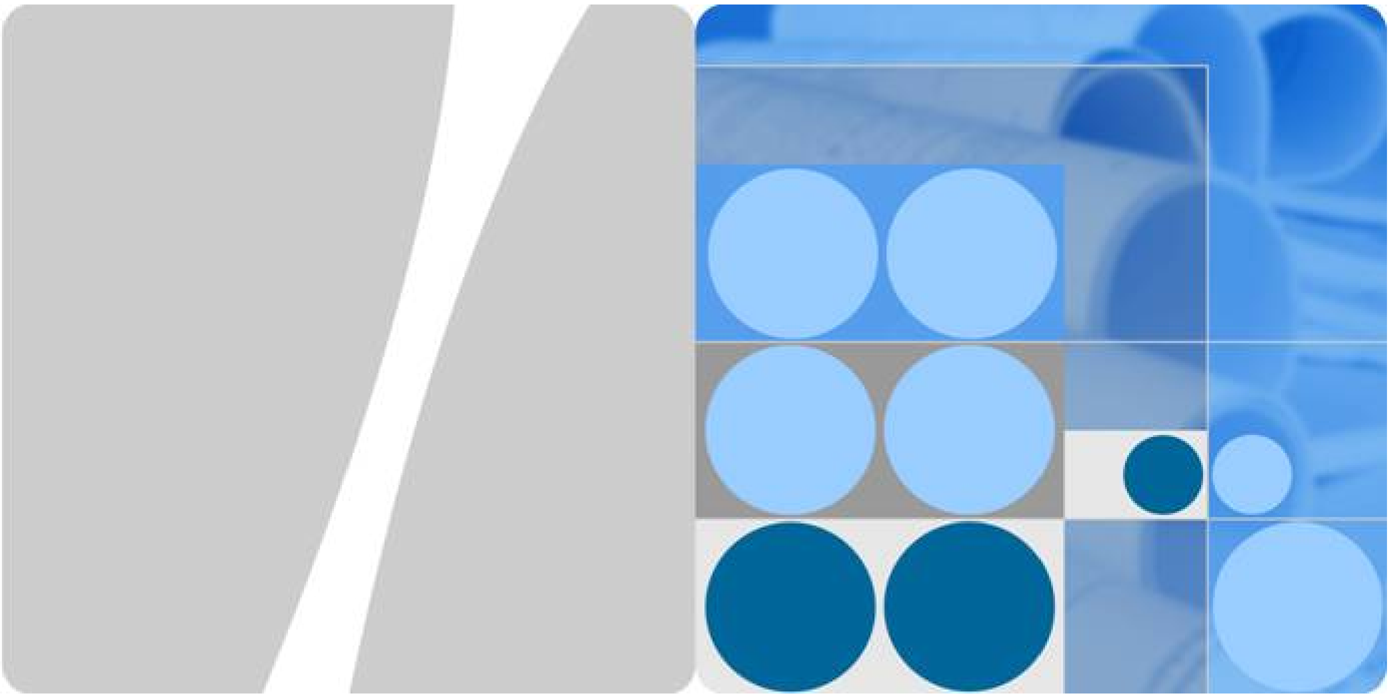


S300, S500, S2700, S5700, and S6700 Series Ethernet Switches

V200R023C00

Command Reference

Issue 02
Date 2024-07-31

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

About This Document

Intended Audience

This document is intended for network engineers responsible for switch configuration and management. You should be familiar with basic Ethernet knowledge and have extensive experience in network deployment and management.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Security Conventions

- Password setting
  - To ensure device security, use ciphertext when configuring a password and change the password periodically.
  - The switch considers all passwords starting and ending with %^%#, %#%#, %@%@ or @%@% as ciphertext and attempts to decrypt them. If you configure a plaintext password that starts and ends with %^%#, %#%#, %@%@ or @%@%, the switch decrypts it and records it into the configuration file (plaintext passwords are not recorded for the sake of security). Therefore, do not set a password starting and ending with %^%#, %#%#, %@%@ or @%@%.
  - When you configure passwords in ciphertext, different features must use different ciphertext passwords. For example, the ciphertext password set for the AAA feature cannot be used for other features.

- Encryption algorithms

  The switch currently supports the 3DES, AES, RSA, SHA1, SHA2, and MD5. 3DES, RSA, and AES are reversible, whereas SHA1, SHA2, and MD5 are irreversible. Using the encryption algorithms DES, 3DES, RSA (RSA-1024 or lower), MD5 (in digital signature scenarios and password encryption), or SHA1 (in digital signature scenarios) is a security risk. If protocols allow, use more secure encryption algorithms, such as AES, RSA (RSA-2048 or higher), SHA2, or HMAC-SHA2.

  An irreversible encryption algorithm must be used for the administrator password. SHA2 is recommended for this purpose.

- Personal data

  Some personal data (such as MAC or IP addresses of terminals) may be obtained or used during operation or fault location of your purchased products, services, features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

- Mirroring

  The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this document are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

- Reliability design declaration

  Network planning and site design must comply with reliability design principles and provide device- and solution-level protection. Device-level protection includes planning principles of dual-network and inter-board dual-link to avoid single point or single link of failure. Solution-level protection refers to a fast convergence mechanism, such as FRR and VRRP. If solution-level protection is used, ensure that the primary and backup paths do not share links or transmission devices. Otherwise, solution-level protection may fail to take effect.

Disclaimer

- This document is designed as a reference for you to configure your devices. Its contents, including web pages, command line input and output, are based on laboratory conditions. It provides instructions for general scenarios, but does not cover all use cases of all product models. The examples given may differ from your use case due to differences in software versions, models, and configuration files. When configuring your device, alter the configuration depending on your use case.
- The specifications provided in this document are tested in a lab environment (for example, a certain type of cards have been installed on the tested device or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values due to factors such as differences in hardware configurations and carried services.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.

Contents

1 Using the Command Query Tool to Query Product Command Information

The **Command Query Tool** can be used to query formats, parameters, and examples of commands by model, version, and command line keyword.

2 Basic Configurations Commands

2.1 CLI Overview Commands

2.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.1.2 assistant task

Function

The **assistant task** command creates an assistant task.

The **undo assistant task** command deletes an assistant task.

By default, no assistant task is created.

Format

assistant task *task-name*

undo assistant task *task-name*

Parameters

Parameter	Description	Value
task-name	Specifies the name of an assistant task.	The value is a string of 1 to 15 characters. It can consist of only underscores (_), letters, and digits, and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

An assistant task is a virtual assistant on a device to realize automatic maintenance and management. After you create an assistant task and bind it to a batch of files to be processed, the device performs operations or configurations when it is unattended. Assistant tasks are mainly used for scheduled system upgrade or configuration.

NOTE

You can create a maximum of five assistant tasks on a device.

Example

Create an assistant task.

```
<HUAWEI> system-view
[HUAWEI] assistant task test
```

2.1.3 command-privilege level

Function

The **command-privilege level** command sets a command privilege level in a specified view.

The **undo command-privilege** command restores the default level.

By default, each command in each view has a default command privilege level.

Format

command-privilege level *level* **view** *view-name command-key*

undo command-privilege [**level** *level*] **view** *view-name command-key*

Parameters

Parameter	Description	Value
level *level*	Specifies a command privilege level.	The value is an integer that ranges from 0 to 15.
view *view-name*	Specifies a view name. You can enter a question mark (?) in the terminal GUI to obtain all view names in the command view. For example: ● shell: user view ● system: system view ● vlan: VLAN view	-
command-key	Specifies a command. The command must be entered manually because automatic command line completion is not supported.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system divides commands into levels for management. Each command in views has a specified level. The device administrator can change a command privilege level as required so that a lower-level user can use certain high-level commands. The device administrator can also increase the command privilege level to a larger value to improve device security.

Precautions

- The rules for using this command to set the command privilege level of a specified view are as follows:
  - When you degrade the target command, all keywords in the command are degraded.
  - When you upgrade the target command, only the last keyword in the command is upgraded.

  - When you set a level for the target command, the levels of all commands (in the same view) starting with this command are changed.
  - When you set a level for the target command, the keyword level in other commands having the same index as the keyword whose level is changed is also changed.
  - If the level of keywords that have the same index is modified for multiple times, the latest configured level takes effect.
- Do not change the default command privilege level. If you need to change it, consult with professional personnel to ensure that routine operation and maintenance are not affected and security risks are avoided.
- If parameters are specified in the command whose privilege level is configured using the **command-privilege level** command, enter these parameters, for example, **command-privilege level 1 view shell tftp 10.1.1.1 get vrpcfg.txt cfcard:/vrpcfg.bak**.

Example

Set the privilege level of the **save** command to 5.

```
<HUAWEI> system-view
[HUAWEI] command-privilege level 5 view shell save
```

2.1.4 command-privilege level rearrange

Function

The **command-privilege level rearrange** command upgrades command privilege levels in batches.

The **undo command-privilege level rearrange** command restores the default command privilege levels in batches.

By default, the command privilege levels assigned by the system during registration are used.

Format

command-privilege level rearrange

undo command-privilege level rearrange

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Each command registered on a device is assigned a default level 0, 1, 2, or 3. These levels correspond to the visit level, monitoring level, configuration level, and management level. You can run the **command-privilege level rearrange** command to upgrade all the level-2 and level-3 commands to level-10 and level-15 commands in batches. The level-0 and level-1 commands remain unchanged.

Precautions

- You can change the levels of the commands that are not separately changed by the **command-privilege level** command. The levels of the commands that are separately changed by the **command-privilege level** command cannot be upgraded.
- You can restore the levels of the commands that are upgraded in batches. The levels of the commands that are separately changed by the **command-privilege level** command cannot be upgraded.
- After the **command-privilege level rearrange** command is run, users at Level 2 to Level 9 are not allowed to run commands defaulted to Level 2, and users at Level 3 to Level 14 are not allowed to run commands defaulted to Level 3. If some users are required to have the same command privilege as that before the command privilege level promotion, you are advised to adjust the levels of all users on the device.
- After the **undo command-privilege level rearrange** command is run, users at level 3 to level 14 are allowed to run commands defaulted to level 3, and users at level 2 to level 9 are allowed to run commands defaulted to level 2. If some users are required to have the same command privilege as that before the command privilege level decrease, you are advised to adjust the levels of all users on the device.
- You can use the **command-privilege level rearrange** command only when your user privilege level is 15.
- After the levels of the commands are upgraded in batches and before the levels of the commands are restored, upgrading the levels of the commands is invalid and does not change the current status of the commands.

Example

Change the levels of the current commands in batches.

```
<HUAWEI> system-view
[HUAWEI] command-privilege level rearrange
```

2.1.5 diagnose

Function

The **diagnose** command enables a device to enter the diagnostic view from the system view.

Format

diagnose

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Diagnostic commands are mainly used for fault diagnosis. However, running certain commands may cause device faults or service interruptions. Therefore, use these diagnostic commands under the instruction of technical support personnel.

Example

Enable a device to enter the diagnostic view.

```
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose]
```

2.1.6 display assistant task history

Function

The **display assistant task history** command displays operation records of assistant tasks.

Format

display assistant task history [*task-name*]

Parameters

Parameter	Description	Value
task-name	Specifies the name of an assistant task.	The value is a string of 1 to 15 characters consisting only of underscores (_), letters, and digits, and must start with a letter.

Views

All views

Default Level

3: Management level

Usage Guidelines

The five latest operations of each assistant task are displayed in order from earliest to latest.

Example

Displays operation records of assistant tasks.

```
<HUAWEI> display assistant task history
-------------------------------------------------------------------------------
Assistant task name: nemo
-------------------------------------------------------------------------------
Assistant task name: song
 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:25:00
 End time       : 2012-07-16 09:25:00
 State          : Finished

 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:24:00
 End time       : 2012-07-16 09:24:00
 State          : Finished

-------------------------------------------------------------------------------
Assistant task name: xu
 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:25:00
 End time       : 2012-07-16 09:25:00
 State          : Finished

 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:24:00
 End time       : 2012-07-16 09:24:00
 State          : Finished

 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:23:00
 End time       : 2012-07-16 09:23:00
 State          : Finished

-------------------------------------------------------------------------------
```

Table 2-1 Description of the **display assistant task history** command output

Item	Description
Assistant task name	Task name. This parameter is configured using the **assistant task** command.
Action type	Operation that an assistant task performs.

Item	Description
Batch file name	Name of the batch file used by an assistant task. This parameter is configured using the **perform batch-file** command.
Start time	Operation start time of an assistant task.
End time	Operation end time of an assistant task.
State	Running status of an assistant task. ● **Running** indicates that the assistant task is in operating. ● **Finished** indicates that the assistant task has finished operating.

2.1.7 display component

Function

The **display component** command displays information about a registered component.

Format

display component [*component-name*] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
component-name	Displays information about a component with a specified ID.	The value ranges from 0 to FFFFFFFF, in hexadecimal notation. **0** indicates brief information about all components, and **FFFFFFFF** indicates detailed information about all components. The default value is **FFFFFFFF**.

Parameter	Description	Value
slot *slot-id*	- Displays information about registered components on a specified slot if stacking is not configured. - Displays information about registered components on a specified stack member device if stacking is configured.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display component** command displays information about a registered component.

Example

Display brief information about all registered components.

```
<HUAWEI> display component 0


********************************************************
 No.   CompID      CompVer         CompName
 0     0x00003391  1.0.0.0         DNS
 1     0x000001f4  1.0.0.0         COMMON
 2     0x00002ee1  1.0.0.0         NSPCOMMON
 3     0x0000332d  1.0.0.0         NSPNOLIBCOMMON
 4     0x000032c9  1.0.0.0         NFPCOMMON
 5     0x00002c89  1.0.0.0         SECAPP
 6     0x000027da  1.0.0.0         TRUNK
 7     0x00002775  1.0.0.0         L2IF
 8     0x00002af9  1.0.0.0         NQAC_BASIC
 9     0x00002b5d  1.0.0.0         NQAS_BASIC
 10    0x00002e19  1.0.0.0         VPLS BASIC
 11    0x000000c8  1.0.0.0         PPMNG
 12    0x000000ce  1.0.0.0         ND
 13    0x000000cf  1.0.0.0         ADDR
 14    0x000000c9  1.0.0.0         ICMP6
 15    0x000000cd  1.0.0.0         PMTU
 16    0x000000df  1.0.0.0         IPSEC6-IPV6
 17    0x000000de  1.0.0.0         IPSEC6-POLICY
 18    0x000000dc  1.0.0.0         IPSEC6-SAPRO
 19    0x000000cb  1.0.0.0         UDP6
 20    0x000000cc  1.0.0.0         RIP6
  ---- More ----
```

Table 2-2 Description of the **display component** command output

Item	Description
No.	Number.
CompID	Component ID.
CompVer	Component version.
CompName	Component name.

2.1.8 display history-command

Function

The **display history-command** command displays the historical commands stored on a device.

Format

display history-command [**all-users**]

Parameters

Parameter	Description	Value
all-users	Displays information about the successfully matched commands that are executed by all users. If *all-users* is not specified, successfully matched historical commands executed by the current user are displayed.	-

Views

All views

Default Level

display history-command: 0: Visit level

display history-command all-users: 3: Management level

Usage Guidelines

Usage Scenario

The terminal automatically saves the history commands entered by the user, that is, records any keyboard entry of the user with **Enter** as the unit.

By default, the **display history-command** command displays a maximum of 10 historical commands. If the number of historical commands is less than 10, the

display history-command command output displays all of them. Run **history-command max-size** command to set the size of the historical command buffer.

Precautions

Commands run by users are automatically saved on the terminal. Any input that ends with **Enter** is saved as a historical command.

NOTE

- Commands are saved in the same format as those users entered. If an entered command is incomplete, the saved command is also incomplete.
- If a command is run several times, only the latest one is saved. If the command is run in different formats, they all saved as different commands.

You can check historical commands using the following methods:

- To check a previous historical command, press the **Up** arrow key or **Ctrl+P**.
- To check a next historical command, press the **Down** arrow key or **Ctrl+N**.

NOTE

To check the previous historical commands on a Windows 9X HyperTerminal, press **Ctrl+P**. The **Up** arrow key does not take effect.

Example

Display the historical commands that have been executed on a terminal.

```
<HUAWEI> display history-command
 system-view
 user-interface vty 0 4
 user privilege level 15
 quit
```

2.1.9 display this

Function

The **display this** command displays the running configurations in the current view.

Format

display this

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configurations are complete in a certain view, run the **display this** command to check the current configurations.

Precautions

If a configuration parameter uses the default value, this parameter is not displayed. Configurations for functions that do not take effect are not displayed.

If you run the **display this** command in an interface view, configurations of the interface view are displayed. If you run this command in a protocol view, configurations of the protocol view are displayed.

Example

Display the running configuration in the current view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
#
return
```

2.1.10 display this include-default

Function

The **display this include-default** command displays the valid configurations in the current view, including the unchanged default configurations.

NOTE

This command does not display the default configurations that are not modified in the WLAN view.

Format

display this include-default

Parameters

None.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can use this command to view the default configurations of physical attributes, basic Ethernet protocols, routing, multicast, QoS, and security features on Ethernet interfaces. The following features are included:

- VLAN management: port-based VLAN assignment, other VLAN assignment methods, PVID, link type, QinQ protocol type, port priority, discard tagged-pkt, and port bridge
- MUX VLAN, voice VLAN, VLAN mapping/stacking, VT enable, and VT miss-drop
- MAC address learning status and priority, port security, sticky MAC, MAC address limiting, and MAC flapping detection
- MSTP, L2PT, DLDP, LLDP, loopback detection, RRPP, SmartLink, SEP, and ERPS
- Ethernet interface physical attributes: speed/duplex, speed auto-negotiation, negotiation, flow control, flow control negotiation, flow-control receive/flow-control negotiation receive, loopback, MDI, jumbo frame, trap/log alarm thresholds, link flapping, EEE, link Up/Down report delay, VCT, inter-frame gap statistics, error packet statistics, URPF, and copper module information
- ARP, ND, Eth-Trunk, and port isolation
- BFD: single-hop BFD, multi-hop BFD, BFD for LSP, and multicast BFD
- Unicast route management, static routes, RIP, OSPF, IS-IS, BGP, and VRRP
- Multicast routing, PIM, IGMP, MLD, IGMP snooping, and MLD snooping
- QoS, ACL, storm suppression, ARP security, IP security, and MFF
- DHCP, DHCPv6, ND Snooping, NAC, and RADIUS

This command can also display the following default global configurations: enabling of the function that sends ICMP host/port unreachable packets, enabling of the function that discards ICMP packets with TTL value 1, rate limit for ARP Miss packets, enabling of ICMP packet rate limiting, and interval for collecting CAR-based traffic statistics. For the support for default settings of the features, see the corresponding device model.

Example

Display the valid configurations and default configurations on VLANIF 10. The following command output is used for reference. The command output on your device may differ from that provided in this example.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 10
[HUAWEI-Vlanif10] display this include-default
#
interface Vlanif10
 undo shutdown
 undo set flow-stat interval
 mtu 1500
 undo arp detect-mode unicast
 arp-fake expire-time 3
 undo arp learning disable
 undo arp purge slowly
 undo ipv6 enable
 icmp host-unreachable send
 icmp redirect send
 icmp port-unreachable send
 icmp ttl-exceeded send
```

```
 undo ip verify source-address
 undo ip forward-broadcast
 undo clear ip df
 undo discard srr
 undo discard rr
 undo discard ra
 undo discard ts
 damping time 0
 arp learning strict trust
 undo ntp-service in-interface disable
 undo mpls
 undo arp-proxy enable
 undo arp-proxy inter-sub-vlan-proxy enable
 undo arp-proxy inner-sub-vlan-proxy enable
 undo arp broadcast disable
 undo rrpp snooping enable
 nd optimized-passby enable
 undo urpf
 diffserv-mode uniform
 undo statistic enable both
 undo ipv4 statistic enable both
 undo ipv6 statistic enable both
 undo arp gratuitous-arp send enable
 undo arp anti-attack entry-check enable
 undo arp learning double-tag disable
 arp optimized-passby enable
 undo dhcp select global
 undo dhcp select interface
 undo dhcp select relay
 undo ip address bootp-alloc
 undo ip address dhcp-alloc
 undo arp learning dhcp-trigger
#
return
```

2.1.11 header

Function

The **header** command configures the header information displayed on a terminal when users log in to a connected device.

The **undo header** command deletes the header information displayed on a terminal when users log in to a connected device.

By default, no header information is displayed on terminals when users log in to a connected device.

Format

header { **login** | **shell** } { **information** *text* | **file** *file-name* }

undo header { **login** | **shell** }

Parameters

Parameter	Description	Value
login	Indicates header information displayed on a terminal when a user logs in to the device and a connection between the terminal and the device is activated.	-
shell	Indicates the header displayed on a terminal when the session is set up after the user logs in to the connected device.	-
information *text*	Specifies the header and content.	The value is a string with spaces and carriage returns supported. The maximum length of the string that can be entered at one time is 480 characters.
file *file-name*	Specifies the file name that the header uses.	The value is a string of 1 to 64 characters without spaces. Only the absolute path is supported. The file name must be in the [drive] [path] [file name] format, where [path] is the absolute path of the file. The maximum header file size that can be configured is 2 KB.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To provide some prompts or alarms to users, run the **header** command to configure a title on the device. If a user logs in to the device, the title is displayed.

Procedure

If **information** is specified, the header text starts and ends with the same character. You can set the header text in either of the following modes:

- Non-interactive: enter the header text behind the start character.

  Use the same character at the beginning and end of the header and press **Enter**. If the start and end characters are inconsistent, the system prompts an error message.
- Interactive: enter the start character and press **Enter** to enter the interactive process.

  The system displays a message asking you to enter the correct header information. After you enter the information, enter the same character as the start character. Press **Enter**. The system quits the interactive process.

  During interaction, you can press **Enter** at any time to enter information in the next line.

Precautions

- Before setting the **login** parameter, you must set login authentication parameters; otherwise, no header information about authentication is displayed.
- Before setting the **file** parameter, ensure that the file containing the header exists; otherwise, the file name cannot be obtained. If you change header information after login, the header information that has been displayed in the system does not change, even if you exit and log in to the system again. The header information changes in either of the following cases:
  - You have successfully changed the header information. Before the system restarts, you run this command again. Then you exit and log in to the system again.
  - You have successfully changed the header information. Then you restart the system.
- If you use SSH1.X to log in to the device, only the shell header is displayed.
- If you use SSH2.0 to log in to the device, both login and shell headers are displayed in the login process.
- If the header command is configured several times, only the latest configuration takes effect.
- After configuring the login header, any user that logs in to the system can view the header.
- In the system view, run the **execute** *batch-filename* batch processing command. If the batch processing command contains the **header** { **login** | **shell** } **information** *text* command and *text* contains line feed character **\r\n**, you need to use third-party software to change the hexadecimal value (0D 0A) of the line feed character **\r\n** to (1B 19).

Example

Configure a shell header in non-interactive mode.

```
<HUAWEI> system-view
[HUAWEI] header shell information &Hello! Welcome to system!&      # Enter the header text behind
the start character '&' and enter '&' at the end of the header text, and press Enter.
```

Display the shell header if the login succeeds.

```
Hello! Welcome to system!
```

Configure a shell header in interactive mode.

```
<HUAWEI> system-view
[HUAWEI] header shell information %      # Press Enter after entering the start character '%' to start the interactive process.
The banner text supports 480 characters max, including the start and the end cha
racter.If you want to enter more than this, use banner file instead.Input banner
 text, and quit with the character '%':
Hello!
Welcome to system!%      # Press Enter after entering the end character '%' to quit the interactive process.
[HUAWEI] quit
<HUAWEI> quit      // Log off.
```

Press **Enter**. The shell header is displayed when the user logs in again.

```
Hello!
Welcome to system!
<HUAWEI>
```

Specify the file that stores a login header.

```
<HUAWEI> system-view
[HUAWEI] header login file flash:/header-file.txt
```

2.1.12 if-match timer cron

Function

The **if-match timer cron** command sets the time to perform an assistant task.

The **undo if-match timer cron** command cancels the time configured for performing an assistant task.

By default, the time to perform an assistant task is not specified.

Format

if-match timer cron *seconds minutes hours days-of-month months days-of-week* [*years*]

undo if-match timer cron

Parameters

Parameter	Description	Value
seconds	Sets second.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). Currently, the device supports only asterisks (*), indicating that the value is accurate to the minute but not the second.

Parameter	Description	Value
minutes	Sets minute.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,).
hours	Sets hour.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,).
days-of-month	Sets date.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). This parameter is exclusive with the *days-of-week* parameter. At least one of the two contains asterisks (*).
months	Sets month.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,).

Parameter	Description	Value
days-of-week	Sets week.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). The parameter is exclusive with the *days-of-month* parameter. At least one of the two contains asterisks (*).
years	Sets year.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). If this parameter is not specified, it refers to all the years between 2000 to 2099.

Views

Assistant task template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **if-match timer cron** command is used to set the time to perform an assistant task. The time is expressed in the cron format defined in UNIX or Linux.

The commonly used time and date format (hh:mm:ss dd-mm-yyyy) can specify only one specific time value. The cron time format is more flexible and can display single or multiple time points, time ranges, and time intervals. The following table describes the expression mode of the cron format.

Expression Mode	Format	Description	Example
Single time point	<time>	<time>: The value is an integer that specifies a specific time value. The value range is dependent on a specific parameter. The range of minutes is 0 to 59. The range of hours is 0 to 23. The range of days-of-month depends on the number of days in a specific month. The range of months is 1 to 12. The range of days-of-week is 0 to 7. The range of years is 2000 to 2099.	Command: if-match timer cron * 0 1 2 5 * 2012 Meaning: perform an assistant task at 1:00 on May 2, 2012.
Multiple time points	<time1>,<time2>,...,<timen>	<timen>: The value is an integer. The value range depends on a specific parameter. Multiple time points are separated by a comma (,) with no space before or after it. The time values in a list can be arranged in any sequence.	Command: if-match timer cron * 0 1,2,3 2 3 * 2012 Meaning: perform an assistant task at the following time points: ● 1:00, March 2, 2012 ● 2:00, March 2, 2012 ● 3:00, March 2, 2012

Expression Mode	Format	Description	Example
Specific time point	<time>/<step>	<time>: The value is an integer that specifies a specific time value. <step>: The value is an integer that specifies the time incremental. The two values are separated by a slash (/) with no space before or after it. The format: <time>,<time>+<step>,<time>+2*<step>,...,<time>+n*<step>. The maximum time (<time>+n*<step>) depends on a specific parameter in the command line.	Command: if-match timer cron * 0 0/10 * 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 10:00, March 1, 2012 ● 20:00, March 1, 2012 ● 0:00, March 2, 2012 ● ... ● 10:00, March 31, 2012 ● 20:00, March 31, 2012
Duration	<time1>-<time2>	<time1> and <time2>: The values are integers, specifying the start and end time respectively. <time2> must be later than or equal to <time1>. The two values are separated by a hyphen (-) with no space before or after it. the <time1>-<time2> is same as <time1>,<time1>+1,<time1>+2,......,<time2>. If <time1> and <time2> are the same, they specify the same time point.	Command: if-match timer cron *0 0-3 1 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 1:00, March 1, 2012 ● 2:00, March 1, 2012 ● 3:00, March 1, 2012

Expression Mode	Format	Description	Example
Period	*	If the parameter in the command line is set to *, the parameter may refer to any time point. By setting the parameter to *, you can configure the system to periodically perform an assistant task every year, week, month, day, hour, or minute.	Command: if-match timer cron * 30 10 * 1 1 2012 Meaning: perform an assistant task at 10:30, Monday every week in January, 2012.
Combination	Combination format	All the expression modes can be combined except "period". The expression modes are separated by a comma (,) with no space before or after it.	Command: if-match timer cron * 0 0/10,2,4-5 1 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 2:00, March 1, 2012 ● 4:00, March 1, 2012 ● 5:00, March 1, 2012 ● 10:00, March 1, 2012 ● 20:00, March 1, 2012

Precautions

- If you run the **if-match timer cron** command multiple times in the same view, only the latest configuration takes effect.
- The *days-of-month* and *days-of-week* parameters are exclusive. Set one or both of them to "*". If one parameter is set to *, the other one specifies a specific date. If both parameters are set to *, they can refer to any date.
- The minimum unit supported is minute, so set the second parameter to *. The specified assistant task works only once every minute.
- Since the system can perform only one assistant task at a time, the time when one assistant task finished working may be later than the time when the next task is schedule to start. There may be a time span between the time when an assistant task is scheduled to work and the time when it actually starts to work. The **if-match timer cron** command specifies the time when an assistant task is scheduled to work.
- When you enter digits, such as 000002012, the numeric string means the same as 2012.

Example

Configure an assistant task to work at 20:00, 2012-05-04.

```
<HUAWEI> system-view
[HUAWEI] assistant task test
[HUAWEI-assistant-task-test] if-match timer cron * 0 20 4 5 * 2012
[HUAWEI-assistant-task-test] perform 1 batch-file sys.bat
```

Cancel the time for an assistant task to start to work.

```
<HUAWEI> system-view
[HUAWEI] assistant task test
[HUAWEI-assistant-task-test] undo if-match timer cron
```

2.1.13 perform batch-file

Function

The **perform batch-file** command configures an assistant task to process a batch file.

The **undo perform** command disables an assistant task from processing a batch file.

By default, no batch file is configured for an assistant task.

Format

perform *priority* **batch-file** *filename*

undo perform *priority*

Parameters

Parameter	Description	Value
priority	Specifies a priority for an assistant task.	The value is fixed at 1 because one assistant task can process only one batch file.
filename	Specifies the name of the batch file processed by the assistant task.	The file is in *.bat file. **NOTE** The file must be stored in the **flash:/user/bat** directory.

Views

Assistant task template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you successfully create an assistant task and specify the execution time, you can run this command to configure the device to process a batch file at the specified time.

Prerequisites

An assistant task has been created using the **assistant task** command and the execution time has been specified using the **if-match timer cron** command.

Precautions

To delete an assistant task that is being executed, stop it first. To delete an assistant task to be executed, directly delete it. The device will not execute the assistant task.

Example

Configure the assistant task **huawei** to process the batch file **sys.bat** at 20:00 on 2012-05-04.

```
<HUAWEI> system-view
[HUAWEI] assistant task huawei
[HUAWEI-assistant-task-huawei] if-match timer cron * 0 20 4 5 * 2012
[HUAWEI-assistant-task-huawei] perform 1 batch-file sys.bat
```

Disable an assistant task from processing a batch file.

```
<HUAWEI> system-view
[HUAWEI] assistant task huawei
[HUAWEI-assistant-task-huawei] undo perform 1
Info: Start to delete the action.
[HUAWEI-assistant-task-huawei] display this
#
assistant task huawei
 if-match timer cron * 0 20 4 5 * 2012
#
return
```

2.1.14 quit

Function

The **quit** command returns a device from the current view to a lower-level view. If the current view is the user view, this command exits from the system.

Format

quit

Parameters

None

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Three types of views are available (listed from a lower level to a higher level):

- User view
- System view
- Service view, such as the interface view

Run the **quit** command to return to a lower-level command view from the current view. Running this command in the user view quits from the system.

Example

Return to the system view from the AAA view and then return to the user view. Quit the system after this.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] quit
[HUAWEI] quit
<HUAWEI> quit
```

2.1.15 reset history-command

Function

The **reset history-command** command deletes historical commands from a device.

Format

reset history-command [**all-users**]

Parameters

Parameter	Description	Value
all-users	Deletes historical commands entered by all users. If this parameter is not specified, the historical commands entered only by the current user are deleted.	-

Views

All views

Default Level

reset history-command: 0: Visit level

reset history-command all-users: 3: Management level

Usage Guidelines

To delete historical commands entered by the current user, run the **reset history-command** command. If a level 3 (or higher) user runs the **reset history-command all-users** command, historical commands entered by all users are deleted.

Example

Delete historical commands entered by the current user.

```
<HUAWEI> reset history-command
```

2.1.16 return

Function

The **return** command returns to the user view from other views (except the user view).

Format

return

Parameters

None

Views

All views

Default Level

0: Visit level

Usage Guidelines

Use the **return** command in other views to return to the user view.

- This command returns to the user view if the current view is another view (but not the user view).
- No change occurs after running this command if the current view is the user view.
- The shortcut keys **Ctrl+Z** functions similarly as the **return** command.

Example

Return to the user view from the user interface view.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] return
<HUAWEI>
```

2.1.17 system-view

Function

The **system-view** command enables you to enter the system view from the user view.

Format

system-view

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You must configure the device in the system view. Run this command in the user view to enter the system view.

Example

Enter the system view.

```
<HUAWEI> system-view
Enter system view, return user view with Ctrl+Z.
[HUAWEI]
```

2.1.18 terminal command forward matched upper-view

Function

The **terminal command forward matched upper-view** command enables forward commands (not in the undo form) to automatically match the upper-level view and return to the upper-level view.

The **undo terminal command forward matched upper-view** command disables forward commands from automatically matching the upper-level view.

By default, forward commands are enabled to automatically match the upper-level view.

Format

terminal command forward matched upper-view

undo terminal command forward matched upper-view

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If forward commands are enabled to automatically match the upper-level view and you run a forward command not registered in the current view, the system automatically switches to the upper-level view to search for the command. If the command is found in that view, the system runs the command. If the command is not found in that view, the system continues the search in the next upper-level view until the system view.

Precautions

The **terminal command forward matched upper-view** command takes effect only for the current login user who runs this command.

Example

Enable forward commands to automatically match the upper-level view.

```
<HUAWEI> terminal command forward matched upper-view
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] sysname ABC
[ABC]
```

Disable forward commands from automatically matching the upper-level view.

```
<HUAWEI> undo terminal command forward matched upper-view
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] sysname ABC
                              ^
Error: Unrecognized command found at '^' position.
```

2.1.19 terminal echo-mode

Function

The **terminal echo-mode** command sets a command output mode.

The default command output mode is **character**.

Format

terminal echo-mode { **character** | **line** }

Parameters

Parameter	Description	Value
character	Specifies a character mode. The system displays the character that you enter in the command line.	-
line	Specifies a line mode. The system displays the character that you enter in the command line only after you press **Enter**, **Tab** or **?**. If you press a shortcut key, such as **Backspace**, **Page Up**, or **Ctrl+A**, it still takes effect.	-

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When operating a device using the NMS, run this command to change the command output mode to **line** to improve operation efficiency. Common users typically use the **character** mode, so use this mode for common users to improve operation efficiency.

Precautions

- After a user runs this command to set the **line** mode, this mode takes effect only for this user. Other users still use the **character** mode.
- After a user changes the command output mode to **line**, the command output mode automatically switches to **character** when the user exits the device or the device restarts or performs an active/standby switchover.

- This command does not affect interactive inputs for the command line.

Example

Set the command output mode to **line**.

```
<HUAWEI> terminal echo-mode line
```

2.2 EasyDeploy Commands

2.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

Switches' support for the commander and client roles in EasyDeploy application is as follows:

Role	Product Model	Version	Maximum Number of Managed Clients
Commander	S12700	V200R005C00 and later	255
	S12700E	V200R019C00 and later	255
	S7700	V200R003C00 and later	255
	S9700	V200R003C00 to V200R013C00	255
	S5700-HI	V200R003C00 to V200R005C00	128
	S5710-HI	V200R003C00 to V200R005C00	128
	S6700-EI	V200R003C00 to V200R005C00	128
	S5700-EI	V200R003C00 to V200R005C00	64
	S5710-EI	V200R003C00 to V200R005C00	64
	S5720-HI	V200R006C00 to V200R019C10	128
	S5720-EI	V200R007C00 to V200R019C10	128

Role	Product Model	Version	Maximum Number of Managed Clients
	S5730-HI	V200R012C00 to V200R019C10	128
	S5731-H	V200R013C02 and later	128
	S5731-S	V200R019C00 and later	128
	S5731S-S	V200R019C00 and later	128
	S5731S-H	V200R019C00 and later	128
	S5732-H	V200R019C00 and later	128
	S6720-EI	V200R008C00 and later	128
	S6720S-EI	V200R009C00 and later	128
	S6720-HI	V200R012C00 to V200R019C10	128
	S6730-H	V200R013C02 and later	128
	S6730S-H	V200R019C10 and later	128
	S6730-S	V200R019C00 and later	128
	S6730S-S	V200R019C00 and later	128
	S6735-S	V200R021C00SPC600 and later	128

Role	Product Model	Version	Maximum Number of Managed Clients
Client	● All fixed switch models except S1720GFR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S1730S-S1, and S1720X-E ● All modular switch models	V200R003C00 and later	-

2.2.2 activate-file

Function

The **activate-file** command sets the file activation mode and time on the Commander.

The **undo activate-file** command restores the default file activation mode and time.

By default, if downloaded files include the system software (*.cc), devices immediately activate all files by resetting. In addition, if the downloaded files in the batch upgrade scenario include the configuration file, the devices also activate files immediately by resetting.

Format

activate-file { **reload** | { **in** *time* | **delay** *delay-time* } } *

undo activate-file [**reload** | **in** [*time*] | **delay** [*delay-time*]]

Parameters

Parameter	Description	Value
reload	Indicates that the device activates files by resetting.	-
in *time*	Indicates the time when the device activates files.	The format is HH:MM, in which HH indicates hour ranging from 0 to 23 and MM indicates minute ranging from 0 to 59.

Parameter	Description	Value
delay *delay-time*	Indicates the delay after which the device activates files.	The value is an integer that ranges from 0 to 86400, in seconds. The default is 0.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If clients use the default method to activate files, network services will be affected. This issue is especially prominent in the batch upgrade scenario where each upgraded device may carry a lot of services. Resetting these devices will interrupt services. Therefore, the devices should activate files when service volume is small.

Precautions

- If the **reload** parameter is specified, the client activates files by resetting regardless of whether downloaded files include the system software.
- The **undo activate-file** command restores the default file activation mode and time. If the **reload**, **in**, and **delay** parameters are specified in the **undo activate-file** command, the default configurations are restored.
- The file activation mode can be set in the Easy-Operation view or group view. If the client matches a group, the configuration in the group view takes effect for the client.

Example

Set the file activation mode to reset.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] activate-file reload
```

Set the file activation delay to one hour.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] activate-file delay 3600
```

Set the file activation mode to reset and time to 1:00 am.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] activate-file in 1:00 reload
```

Set the file activation mode to reset and time to 1:00 am for group F1.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
```

```
[HUAWEI-easyoperation] group custom ip-address F1
[HUAWEI-easyoperation-group-custom-F1] activate-file in 1:00 reload
```

2.2.3 backup configuration interval

Function

The **backup configuration interval** command enables automatic configuration file backup on the Commander and sets the backup interval and method.

The **undo backup configuration** command disables automatic configuration file backup.

By default, the configuration file is not automatically backed up.

Format

backup configuration interval *interval* [**duplicate**]

undo backup configuration [**interval** [*interval*]] [**duplicate**]

Parameters

Parameter	Description	Value
interval	Indicates the backup interval.	The value is an integer that ranges from 0 to 720, in hours. The default value is 0, indicating that clients do not automatically back up configuration files.
duplicate	Indicates that the backup file is saved as a new file, and the original configuration file is not overwritten. If this parameter is not specified, the original configuration file is overwritten by the backup file.	-

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a faulty client is replaced by a new client, the new client needs to obtain the latest configuration file of the faulty client to minimize impact on service.

Therefore, all clients should periodically back up their configuration files to the file server.

NOTE

This function must be configured before any fault occurs. It is recommended that you configure this function when deploying the network.

Prerequisites

The file server information has been configured on the Commander using the **tftp-server/sftp-server/ftp-server** command.

Precautions

- After this function is configured, all clients managed by the Commander will automatically back up configuration files.
- To disable this function, run the **undo backup configuration** [**interval** [*interval*]] or **undo backup configuration interval duplicate** command, or set the file backup interval to 0.
- If you do not want to keep the original configuration files, run the **undo backup configuration duplicate** command to make the backup files overwrite the original files.
- The naming convention of the configuration files is as follows:
  - If the backup files are saved as new files, name the new files in format vrpcfg-MAC address-year-month-day-hour-minute-second.XXX. XXX is the file name extension, which must be the same as the configuration file name extension being used on the client. For example, if the startup configuration file on a client is **vrpcfg.zip**, the backup file is named in format vrpcfg-MAC address-year-month-day-hour-minute-second.zip.
  - If the backup files overwrite the original files, name the backup files in format vrpcfg-MAC address.XXX. XXX is the file name extension, which must be the same as the configuration file name extension being used on the client.

Example

Set the file backup interval to 12 hours and overwrite the original files with backup files.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] backup configuration interval 12
```

Disable automatic configuration file backup.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] backup configuration interval 0
Warning: This command will cancel the function of backing up configuration. Cont
inue?[Y/N]:y
[HUAWEI-easyoperation]
```

2.2.4 batch-cmd begin

Function

The **batch-cmd begin** command starts online command script editing.

Format

batch-cmd begin

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a batch device deployment scenario, you can run this command to start online command script editing. After editing the commands, press **Ctrl**+**C** to exit the editing mode. If you run this command again, the edited commands will be cleared.

Precautions

- Only one network administrator is allowed to edit commands online at one time.
- If no operation is performed in command editing mode within 30 seconds, you automatically exit from the editing mode to the Easy-Operation view.

Example

Start online command script editing.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] batch-cmd begin
Info: Begin to edit batch commands. Press CTRL+C to abort this session.
system-view
vlan batch 10 20
ndp enable
ntdp enable

[HUAWEI-easyoperation]
```

2.2.5 clear topology-error-info

Function

The **clear topology-error-info** command clears faulty link information from the topology.

Format

clear topology-error-info

Parameters

None

Views

Cluster view

Default Level

2: Configuration level

Usage Guidelines

The **clear topology-error-info** command can be run only on the Commander switch.

After a faulty client recovers, run this command to clear faulty link information from the topology. To view the topology information, run the **display cluster-topology-info** command.

Example

Clear information about faulty links and sub-links.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] display cluster-topology-info
The topology information about the cluster:
<-->:normal device        <++>:candidate device        <??>:lost device
--------------------------------------------------------------------------
Total topology node number is 3.
[HUAWEI: Root-00e0-fcb8-d6b6]
|-(GigabitEthernet0/0/2)<??>(GigabitEthernet0/0/1)[00e0-fc67-7f7d]
|-(GigabitEthernet0/0/3)<-->(GigabitEthernet0/0/3)[00e0-fc03-0003]
[HUAWEI-cluster] clear topology-error-info
[HUAWEI-cluster] display cluster-topology-info
The topology information about the cluster:
<-->:normal device        <++>:candidate device        <??>:lost device
--------------------------------------------------------------------------
Total topology node number is 2.
[HUAWEI: Root-00e0-fcb8-d6b6]
|-(GigabitEthernet0/0/3)<-->(GigabitEthernet0/0/3)[00e0-fc03-0003]
```

2.2.6 client

Function

The **client** command adds information to the client database or modifies information in the client database.

The **undo client** command deletes information from the client database.

By default, the client database does not contain client information.

Format

client [*client-id*] { { **mac-address** *mac-address* | **esn** *esn* } | **system-software** *file-name* [*version*] | **patch** *file-name* | **configuration-file** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> } *

undo client *client-id* [**mac-address** [*mac-address*] | **esn** [*esn*] | **system-software** [*file-name* [*version*]] | **patch** [*file-name*] | **configuration-file** [*file-name*] | **web-file** [*file-name*] | **license** [*file-name*] | **custom-file** [*file-name*]]

Parameters

Parameter	Description	Value
client-id	Specifies the client ID, which identifies a client. If this parameter is not specified when you add client information, the system assigns the minimum ID not in use to the client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
mac-address *mac-address*	Specifies the MAC address of the client.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
esn *esn*	Specifies the ESN of the client.	The value is a string of 10 to 32 case-insensitive characters without spaces.
system-software *file-name*	Specifies the name of the system software (*.cc) to be loaded to the client.	The value is a string of 4 to 48 case-insensitive characters without spaces.

Parameter	Description	Value
version	Specifies the version of a system software package, for example, V200R023C00. If the specified software version is the same as the software version running on the client, a software upgrade will not be performed for the client.	The value is a string of 11 to 32 case-insensitive characters without spaces.
patch *file-name*	Specifies the name of the patch file (*.pat) to be loaded to the client.	The value is a string of 5 to 48 case-insensitive characters without spaces.
configuration-file *file-name*	Specifies the name of the configuration file (*.zip or *.cfg) to be loaded to the client.	The value is a string of 5 to 48 case-insensitive characters without spaces.
web-file *file-name*	Specifies the name of the web page file (*.web.7z or *.web.zip) to be loaded to the client.	The value is a string of 8 to 64 case-insensitive characters without spaces.
license *file-name*	Specifies the name of the license file (*.dat) to be loaded to the client. **NOTE** The license file is not supported in the Easy-Operation view. The file does not take effect even if you configure it.	The value is a string of 5 to 64 case-insensitive characters without spaces.
custom-file *file-name*	Specifies the name of the user-defined file to be loaded to the client. A maximum of three user-defined files can be specified. The file names are separated by spaces.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a few zero touch clients need to be deployed on a network, you can run this command multiple times to add client information one by one.

Precautions

- Clients search the matching database by searching for their MAC addresses or ESNs in the database; therefore, the mappings between clients and MAC addresses or ESNs must be configured. When a client finds a matching database, it obtains information mapping its client ID, including system software name and patch file name.
- This command can be executed once or multiple times to configure the mappings between clients and MAC addresses or ESNs and specify information about the files to be downloaded.
- To delete all information about a client, run the **undo client** *client-id* command. To delete an item from a client's information, run the **undo** command with the item specified.

  NOTE

  When parameters are specified in this **undo** command to delete specified information, this command takes effect only for the manually configured clients.
- Each Commander supports a limited number of clients; therefore, the client information that can be added to the client database is also limited.
- You can specify a path for each file.

Example

Add client information in which MAC address is 00e0-fc12-3456, configuration file is **vrpcfg.zip**, and file path is /configfile/.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client mac-address 00e0-fc12-3456 configuration-file configfile/vrpcfg.zip
```

Add client information in which client ID is 3, ESN is 210235165110xxxxxxxx, system software name is **test.cc**, and user-defined file names are **header.txt** and **aaa.bat**.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client 3 esn 210235165110xxxxxxxx
[HUAWEI-easyoperation] client 3 system-software test.cc
[HUAWEI-easyoperation] client 3 custom-file header.txt custom-file aaa.bat
```

Delete the configuration file of the client with client ID 4.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] undo client 4 configuration-file
```

Delete all information about the client with client ID 5.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] undo client 5
```

2.2.7 client aging-time

Function

The **client aging-time** command ages the lost state clients in the client database and specifies the aging time.

The **undo client aging-time** command cancels the configuration.

By default, the lost state clients in the client database are not aged.

Format

client aging-time *aging-time*

undo client aging-time [*aging-time*]

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time for clients in the lost state.	The value is an integer that ranges from 72 to 720, in hours.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Information about clients configured by the network administrator or automatically learned is saved in the client database. The Commander considers that a client to be in the lost state if the client does not respond after two minutes.

The maximum number of clients managed by the Commander depends on the device specifications. If the number of clients exceeds the upper limit, new client information cannot be configured on the Commander. To prevent clients in the lost state from occupying the database resources for a long time, enable the function of aging lost state clients. When the aging time expires, lost state clients are deleted. If some clients in the lost state occupy the database resources for a long time, run the **reset easy-operation client-offline** command to delete these clients.

Precautions

- Automatically learned clients are deleted after their aging time expires.
- Manually configured clients are not deleted but their status changes to unknown.

Example

Enable the function of aging lost state clients and set the aging time to 72 hours.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client aging-time 72
```

2.2.8 client auto-clear enable

Function

The **client auto-clear enable** command enables clients to automatically clear storage space. This command is run on the Commander.

The **undo client auto-clear enable** command disables clients from clearing storage space.

By default, this function is disabled on the Commander.

Format

client auto-clear enable

undo client auto-clear enable

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If storage space on a client is insufficient, the client cannot download files. This command enables clients to automatically clear storage space to ensure a sufficient storage space.

Precautions

- Clients clear storage space only when the storage space is insufficient for a system software package. In addition, they only delete non-startup system software packages to create space.
- This function is invalid for certain file server types. If the file server is a TFTP server, this function does not take effect because the TFTP server does not return file size to clients. If an FTP or SFTP server cannot return file size, this

function does not take effect, either. An S switch serving as an FTP or a TFTP file server does not support the function of returning file size.

Example

Enable clients to automatically clear storage space.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client auto-clear enable
```

2.2.9 client auto-join enable

Function

The **client auto-join enable** command enables clients to automatically join the management domain of a Commander. This command is run on the Commander.

The **undo client auto-join enable** command disables clients from joining the management domain of a Commander.

By default, clients do not automatically join the Commander management domain.

Format

client auto-join enable

undo client auto-join enable

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this function is enabled and the Commander IP address is configured on clients, the Commander automatically learns the basic information about clients, saves the information to the client database, and assigns a client ID to each client.

Client information learned by the Commander includes MAC addresses, ESNs, IP addresses, device types, device models, current system software names, configuration files, and patch files on the clients. The Commander monitors and manages basic information and version files of all clients in the management domain.

In batch upgrade scenario, you can determine the devices to be upgraded according to the client information.

To prevent unknown clients from joining the management domain, disable this function.

Precautions

- In the batch upgrade scenario, run the **easy-operation commander ip-address** command to configure the Commander IP address on the clients.

  In the zero touch device deployment or faulty device replacement scenario, if you require that the clients still be managed by the Commander after completing the EasyDeploy process, add the Commander IP address to the configuration file to be downloaded by the clients.
- To view the client information learned by the Commander, run the **display easy-operation client** command.
- If the learned client information already exists in the client database (statically configured using **client**), the client database is updated.
- After information about a client is stored in the client database, the client status becomes LOST if the client goes offline. When the client goes online, the client joins the management domain again and its status becomes Running.

Example

Enable clients to automatically join the management domain of a Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client auto-join enable
Warning: The commander will create the client information in database automatica
lly when received message from unknown client. Continue? [Y/N]: y
[HUAWEI-easyoperation]
```

2.2.10 client replace

Function

The **client replace** command adds or modifies client replacement information.

The **undo client replace** command deletes client replacement information.

By default, no client replacement information exists.

Format

client *client-id* **replace** { [**mac-address** *mac-address* | **esn** *esn*] | **system-software** *file-name* [*version*] | **patch** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> } *

undo client *client-id* **replace** [**mac-address** [*mac-address*] | **esn** [*esn*] | **system-software** [*file-name* [*version*]] | **patch** [*file-name*] | **web-file** [*file-name*] | **license** [*file-name*] | **custom-file** [*file-name*]]

Parameters

Parameter	Description	Value
client-id	Indicates the ID of a faulty client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
mac-address *mac-address*	Indicates the MAC address of the new client.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
esn *esn*	Indicates the ESN of the new client.	The value is a string of 10 to 32 case-insensitive characters without spaces.
system-software *file-name*	Specifies the name of the system software (*.cc) to be loaded to the new client.	The value is a string of 4 to 48 case-insensitive characters without spaces.
version	Specifies the version of a system software package, for example, V200R023C00. If the specified software version is the same as the software version running on the client, a software upgrade will not be performed for the client.	The value is a string of 11 to 32 case-insensitive characters without spaces.
patch *file-name*	Specifies the name of the patch file (*.pat) to be loaded to the new client.	The value is a string of 5 to 48 case-insensitive characters without spaces.
web-file *file-name*	Specifies the name of the web page file (*.web.7z or *.web.zip) to be loaded to the new client.	The value is a string of 8 to 64 case-insensitive characters without spaces.
license *file-name*	Specifies the name of the license file (*.dat) to be loaded to the new client. **NOTE** The license file is not supported in the Easy-Operation view. The file does not take effect even if you configure it.	The value is a string of 5 to 64 case-insensitive characters without spaces.

Parameter	Description	Value
custom-file *file-name*	Specifies the name of the user-defined file to be loaded to the new client. A maximum of three user-defined files can be specified. The file names are separated by spaces.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a client becomes faulty due to a hardware failure, run this command to add replacement information for the faulty client. After a new client is installed on the network to replace the faulty client, the new client can quickly obtain the configuration file of the faulty client, minimizing impact on services. You can also specify other files that can be loaded on the new client.

Precautions

- A new client finds matching replacement information by searching for its own MAC address or ESN; therefore, the mapping between the new client and MAC address or ESN must be configured. After finding matching information, the new client downloads the configuration file and other specified files of the faulty client from the file server.
- Before replacing the faulty client with a new client, ensure that the EasyDeploy function has been configured on the network and the **backup configuration interval** command has been run on the Commander to enable automatic configuration file backup. If this command has not been run, the new client cannot obtain the latest configuration file of the faulty client.
- This command can be run once or multiple times to configure the mappings between the new client and MAC address or ESN and specify information about the files to be downloaded.
- To delete all replacement information about a client, run the **undo client** *client-id* **replace** command. To delete an item from a client's replacement information, run the **undo** command with the item specified.
- This command is not recorded in the configuration file.

Example

Replace client 3 with a client that has a MAC address xxxx-xxxx-xxxx. The new client only needs to download the configuration file of client 3.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client 3 replace mac-address xxxx-xxxx-xxxx
```

Replace client 3 with a client that has a MAC address xxxx-xxxx-xxxx. The new client needs to download the configuration file, system software, and user-defined file of client 3.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client 3 replace mac-address xxxx-xxxx-xxxx
[HUAWEI-easyoperation] client 3 replace system-software test.cc V200R023C00
[HUAWEI-easyoperation] client 3 replace custom-file header.txt custom-file aaa.bat
```

2.2.11 cluster

Function

The **cluster** command displays the cluster view.

Format

cluster

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After entering the cluster view on the Commander, you can configure a cluster management VLAN and then configure the Commander as the network topology collection device so that the Commander only collects topology information of clients in the VLAN.

Example

Enter the cluster view.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster]
```

2.2.12 cluster enable

Function

The **cluster enable** command enables the cluster function.

The **undo cluster enable** command disables the cluster function.

The **cluster disable** command disables the cluster function.

By default, the cluster function is enabled.

Format

cluster enable

undo cluster enable

cluster disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring the Commander as the network topology collection device, you need to configure a cluster management VLAN in the cluster view on the Commander so that the Commander only collects topology information of clients in the VLAN. Before configuring a cluster management VLAN on an S series switch, you must run the **cluster enable** command to enable the cluster function so that you can enter the cluster view.

Example

Enable the cluster function on a device.

```
<HUAWEI> system-view
[HUAWEI] cluster enable
```

2.2.13 cluster-multimac

Function

The **cluster-multimac** command assigns a multicast address to a cluster.

The **undo cluster-multimac** command restores the default multicast address of the cluster.

By default, the multicast address of the cluster is 0180-C200-000A.

Format

cluster-multimac *mac-address*

undo cluster-multimac

Parameters

Parameter	Description	Value
mac-address	Specifies the multicast MAC address of a cluster.	The value is in the format of H-H-H. Each H stands for a 4-digit hexadecimal number. The value ranges from 0180-C200-0004 to 0180-C200-0007, 0180-C200-0009 to 0180-C200-0010 and 0180-C200-0020 to 0180-C200-002F. The default value is 0180-C200-000A.

Views

Cluster view

Default Level

2: Configuration level

Usage Guidelines

Before setting up a cluster, you need to assign a multicast MAC address to the cluster or use the default multicast MAC address. To enhance the network security or if the default multicast MAC address is being used by other services on the network, you can reassign a multicast MAC address to the cluster within the permitted range. Once the cluster is set up, you cannot change the multicast MAC address of the cluster. All the devices in the cluster must be assigned the same multicast MAC address.

Example

Assign multicast address 0180-c200-0004 to a cluster.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] cluster-multimac 0180-c200-0004
```

Restore the default multicast address of the cluster.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] undo cluster-multimac
```

2.2.14 configuration-file

Function

The **configuration-file** command specifies the configuration file information to be downloaded by clients.

The **undo configuration-file** command deletes information about the configuration file to be downloaded.

Format

configuration-file *file-name*

undo configuration-file [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of the configuration file (*.zip or *.cfg) to be loaded to the client. A file path can be specified.	The value is a string of 5 to 48 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To deploy a zero touch client or reload a configuration file to clients, use this command to specify the configuration file.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

NOTICE

The names of the files to be downloaded cannot be the same as system configuration files. Otherwise, the upgrade fails.

Example

Configure the default configuration file information.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] configuration-file easy/vrpcfg.zip
```

Configure the configuration file information for a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] configuration-file vrpcfg.zip
```

2.2.15 custom-file

Function

The **custom-file** command specifies a user-defined file to be downloaded by clients.

The **undo custom-file** command deletes the configured user-defined file information.

Format

{ **custom-file** *file-name* } &<1-3>

undo custom-file [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a user-defined file to be loaded to the client. A file path can be specified. A maximum of three user-defined files can be specified. The file names are separated by spaces.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to download user-defined files, such as batch processing file and login header file, use this command.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.

- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

NOTICE

The names of the files to be downloaded cannot be the same as system user-defined files. Otherwise, the upgrade fails.

Example

Configure the default user-defined file information.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] custom-file easy/mydoc.bat
```

Configure the user-defined file information for a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] custom-file mydoc.bat custom-file header.txt
```

2.2.16 display easy-operation batch-cmd result

Function

The **display easy-operation batch-cmd result** command displays the batch configuration execution result.

Format

display easy-operation batch-cmd result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the batch configuration execution result, run the **display easy-operation batch-cmd result** command. The result is saved in the memory of clients. If the script contains commands used to clear the client memory, such as the **reboot** command, the result cannot be checked using the **display easy-operation batch-cmd result** command after the commands are delivered to clients.

Example

Display the execution result of batch configuration.

```
<HUAWEI> display easy-operation batch-cmd result
This operation will take some seconds, please wait......
--------------------------------------------------------------
  ID   Total  Successful     Failed     Time
--------------------------------------------------------------
   1      10          10          0    2013-09-12  12:57:02
   2      10          10          0    2013-09-12  12:57:02
   3      10          10          0    2013-09-12  12:57:02
--------------------------------------------------------------
```

Table 2-3 Description of the **display easy-operation batch-cmd result** command output

Item	Description
ID	Client ID.
Total	Total number of commands delivered.
Successful	Number of commands successfully executed.
Failed	Number of commands failed to be executed.
Time	Time when command execution was complete on the client.

2.2.17 display easy-operation client

Function

The **display easy-operation client** command displays client information on the Commander.

Format

display easy-operation client [*client-id* | **mac-address** *mac-address* | **esn** *esn* | **verbose**]

Parameters

Parameter	Description	Value
client-id	Displays detailed information about a client with a specified client ID.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
mac-address *mac-address*	Displays detailed information about a client with a specified MAC address.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
esn *esn*	Displays detailed information about a client with a specified ESN.	The value is a string of 10 to 32 case-insensitive characters without spaces.
verbose	Displays detailed information about all clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays client information that the Commander dynamically obtains from a client, including the client's host name, MAC address, ESN, IP address, device type, and information about the files that have been downloaded to the client.

If the client state is UNKNOWN in the command output, the displayed MAC address and ESN are manually configured. If the client state is not UNKNOWN, the displayed MAC address and ESN values are dynamically obtained from the client. To modify the configuration of a client in a state other than UNKNOWN to match a new device, run the **undo client** *client-id* command to delete the current client configuration first.

If no optional parameter is specified in the command, the command displays brief client information dynamically obtained from the client database.

Example

Display brief client information.

```
<HUAWEI> display easy-operation client
The total number of client is : 4

--------------------------------------------------------------------------------
 ID   Mac address     ESN                             IP address        State
--------------------------------------------------------------------------------
 1    00E0-FC12-ABCD 2102113089P0xxxxxxxx             192.168.150.208   RUNNING
 2    00E0-FC12-0701 -                                -                 INITIAL
 3    -              210235182810xxxxxxxx             192.168.150.210   INITIAL
 4    00E0-FC12-2123 210235276310xxxxxxxx             192.168.150.122   RUNNING
--------------------------------------------------------------------------------
```

Display detailed information about the client with MAC address 0018-1111-2123.

```
<HUAWEI> display easy-operation client mac-address 0018-1111-2123
----------------------------------------------------------------------------
 Client ID                    : 4
 Host name                    : HUAWEI
 Mac address                  : 00e0-fc12-3456
 ESN                          : 210235276310xxxxxxxx
 IP address                   : 192.168.150.122
 Model                        : S5728C-EI
 Device Type                  : S5700-EI
 System-software file         : flash:/s5700-ei-v200r003c00.cc
 System-software version      : V200R003C00
 Configuration file           : flash:/122.cfg
 Patch file                   : -
 WEB file                     : -
 License file                 : -
 System CPU usage             : 6%
 System Memory usage          : 55%
 Backup configuration file    : -
 Backup result                : -
 Last operation result        : -
 Last operation time          : 0000-00-00  00:00:00
 State                        : RUNNING
 Aging time left (hours)      : -
----------------------------------------------------------------------------
```

Table 2-4 Description of the **display easy-operation client** command output

Item	Description
ID/Client ID	Client ID.
Host name	Client host name.
Mac address	Client MAC address.
ESN	Client ESN.
IP address	Client IP address.

Item	Description
State	Client status. - INITIAL: The client is performing initialization. The client information has been added to the Commander, but the client has not obtained an IP address, so the client cannot communicate with the Commander. - UPGRADING: The client is upgrading the software. - RUNNING: The client is running. - LOST: The Commander does not receive the response from the client in 2 minutes. A stack enters the LOST state when its system MAC address changes. - CONFIGURING: Batch configuration status. - UNKNOWN: The client status is unknown. This state rarely appears.
Model	Device model of the client.
Device Type	Device type of the client.
System-software file	Current system software name of the client.
System-software version	Current system version of the client.
Configuration file	Current configuration file name of the client.
Patch file	Current patch file name of the client.
WEB file	Current web page file name of the client.
License file	Current license file name of the client.
System CPU usage	CPU usage of the client.
System Memory usage	Memory usage of the client.
Backup configuration file	Current backup configuration file name of the client.
Last operation result	Last operation result.
Last operation time	Last operation time.
Backup result	File backup result.
Aging time left	Remaining aging time.

2.2.18 display easy-operation client replace

Function

The **display easy-operation client replace** command displays client replacement information on the Commander.

Format

display easy-operation client replace [**verbose**]

display easy-operation client *client-id* **replace**

Parameters

Parameter	Description	Value
verbose	Displays detailed client replacement information.	-
client-id	Displays replacement information about a client with a specified client ID.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display easy-operation client** command displays brief client replacement information.

The replacement information is configured using the **client replace** command.

Example

Display brief client replacement information.

```
<HUAWEI> display easy-operation client replace
The total number of replacement information is :  1

-------------------------------------------------------------
 ID      Replaced Mac      Replaced Esn       Status
```

```
------------------------------------------------------------
 3      00e0-fc12-3456   -               enable
------------------------------------------------------------
```

Display detailed client replacement information.

```
<HUAWEI> display easy-operation client replace verbose
------------------------------------------------------------
 Client ID            : 3
 Mac address          : 00e0-fc12-3456
 ESN                  : -
 System-software file : -
 Configuration file   : 1.cfg
 Patch file           : -
 WEB file             : -
 License file         : -
 Customs file 1       : header.txt
 Customs file 2       : aaa.bat
 Customs file 3       : 1
 Status               : disable
------------------------------------------------------------
```

Display replacement information of client 3.

```
<HUAWEI> display easy-operation client 3 replace
------------------------------------------------------------
 Client ID            : 3
 Mac address          : 00e0-fc12-3456
 ESN                  : -
 System-software file : -
 Configuration file   : 1.cfg
 Patch file           : -
 WEB file             : -
 License file         : -
 Customs file 1       : header.txt
 Customs file 2       : aaa.bat
 Customs file 3       : 1
 Status               : disable
------------------------------------------------------------
```

Table 2-5 Description of the **display easy-operation client replace** command output

Item	Description
ID/Client ID	Faulty client ID.
Replaced Mac/Mac address	New client MAC address.
Replaced Esn/ESN	New client ESN.
System-software file	System software to be downloaded by the new client.
Configuration file	Configuration file to be downloaded by the new client.
Patch file	Patch file to be downloaded by the new client.
WEB file	Web page file to be downloaded by the new client.

Item	Description
License file	License file to be downloaded by the new client.
Customs file 1	First user-defined file to be downloaded by the new client.
Customs file 2	Second user-defined file to be downloaded by the new client.
Customs file 3	Third user-defined file to be downloaded by the new client.
Status	Status of the replacement. ● enable: This function is enabled. ● disable: This function is not enabled.

2.2.19 display easy-operation configuration

Function

The **display easy-operation configuration** command displays the configurations on the Commander.

Format

display easy-operation configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be run on the Commander or clients.

- When the command is run on the Commander, the Commander role, Commander IP address and port number, file server information, and default downloaded file information are displayed.
- When the command is run on a client, the client role and Commander IP address and port number are displayed.

Example

Display EasyDeploy configuration on the Commander.

```
<HUAWEI> display easy-operation configuration
-------------------------------------------------------------------------
 Role                            : Commander
 Commander IP address            : 192.168.150.128
 Commander UDP port              : 60000
 DTLS status                     : Enable
 IP address of file server       : 192.168.150.200
 Type of file server             : SFTP
 Username of file server         : admin
 Default system-software file    : test.cc
 Default system-software version : -
 Default configuration file      : -
 Default patch file              : -
 Default WEB file                : -
 Default license file            : test.dat
 Default custom file 1           : mydoc.pat
 Default custom file 2           : header.txt
 Default custom file 3           : -
 Auto clear up                   : Disable
 Auto join in                    : Disable
 Topology collection             : Enable
 Activating file time            : In 00:00
 Activating file method          : Default
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): -
-------------------------------------------------------------------------
```

Display EasyDeploy configuration on a client.

```
<HUAWEI> display easy-operation configuration
-------------------------------------------------------------------------
 Role                            : Client
 Commander IP address            : 192.168.150.128(dhcp-alloc)
 Commander UDP port              : 60000
 DTLS status                     : Enable
-------------------------------------------------------------------------
```

Table 2-6 Description of the **display easy-operation configuration** command output

Item	Description
Role	Device role in the EasyDeploy service, which can be Commander or client.

Item	Description
Commander IP address	Commander IP address. It can be configured using the **easy-operation commander ip-address** command. If a client starts with a configuration file and obtains an IP address from a DHCP server, the client can also obtain the Commander IP address from the Option 148 field in the DHCP response message sent from the DHCP server. Therefore, the command output on a client shows whether a Commander IP address is configured using the command (configured) or obtained from the DHCP server (dhcp-alloc). If both two types of Commander IP addresses are available, the client uses the configured one. After the configured Commander IP address is deleted, the client uses the Commander IP address obtains from the DHCP server.
Commander UDP port	Port number used for communication between Commander and clients. It can be configured using the **easy-operation commander ip-address** command.
DTLS status	DTLS status.
IP address of file server	File server IP address. It can be configured using the **tftp-server** or **sftp-server** | **ftp-server** command.
Type of file server	File server type.
Username of file server	User name for accessing the file server.
Default system-software file	Default system software. If no default system software is specified, this field is empty. It can be configured using the **system-software** command.
Default system-software version	Default system software version. If no default system software is specified, this field is empty. It can be configured using the **system-software** command.

Item	Description
Default configuration file	Default configuration file. If no default configuration file is specified, this field is empty. It can be configured using the **configuration-file** command.
Default patch file	Default patch file. If no default patch file is specified, this field is empty. It can be configured using the **patch** command.
Default WEB file	Default web page file. If no default web page file is specified, this field is empty. It can be configured using the **web-file** command.
Default license file	Default license file. If no default license file is specified, this field is empty. It can be configured using the **license** command.
Default custom file 1	First default user-defined file. If no default user-defined file is specified, this field is empty. It can be configured using the **custom-file** command.
Default custom file 2	Second default user-defined file. If no default user-defined file is specified, this field is empty. It can be configured using the **custom-file** command.
Default custom file 3	Third default user-defined file. If no default user-defined file is specified, this field is empty. It can be configured using the **custom-file** command.
Auto clear up	Whether clients are enabled to automatically clear storage space. This function is configured using the **client auto-clear enable** command.

Item	Description
Auto join in	Whether clients are enabled to automatically join the management domain of the Commander. This function is configured using the **client auto-join enable** command.
Topology collection	Whether topology information collection is enabled. This function is configured using the **topology enable** command.
Activating file time	File activation time. If default file activation mode is used, this field displays **Immediately**. It can be configured using the **activate-file** command.
Activating file method	File activation mode. If default file activation mode is used, this field displays **Default**. It can be configured using the **activate-file** command.
Aging time of lost client(hours)	Aging time of a client in lost state. It can be configured using the **client aging-time** command.
Backup configuration file mode	Configuration file backup mode. If default mode is used, this field displays **Default**. It can be configured using the **backup configuration interval** command.
Backup configuration file interval(hours)	Configuration file backup interval. If configuration file backup is disabled, this field displays a hyphen (-). It can be configured using the **backup configuration interval** command.

2.2.20 display easy-operation device-information

Function

The **display easy-operation device-information** command displays device information.

Format

display easy-operation device-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check device information, run the **display easy-operation device-information** command. The command output includes the MAC address, ESN, model, type, and active/standby state of the device.

This command can be run on the Commander or clients.

If the client is a stack, the displayed MAC address is the MAC address of the stack (MAC address of the master or backup device) and the displayed ESN is the ESN of the master device.

Example

Display the current device information.

```
<HUAWEI> display easy-operation device-information
System MAC: xxxx-xxxx-xxxx
Slot MAC            ESN                  Model               Device-Type Role
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0    xxxx-xxxx-xxxx 210235404310xxxxxxxx S5701-28X-LI-AC     S5700-X-LI  Master
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Table 2-7 Description of the **display easy-operation device-information** command output

Item	Description
System MAC	System MAC address.
Slot	Slot ID.
MAC	Device MAC address.
ESN	Device ESN.
Model	Device model.
Device-Type	Device type.
Role	Active/standby state.

2.2.21 display easy-operation download-status

Function

The **display easy-operation download-status** command displays file download status of clients on the Commander.

Format

display easy-operation download-status [**client** *client-id* | **verbose**]

Parameters

Parameter	Description	Value
client *client-id*	Displays the file download status of a client with a specified client ID.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
verbose	Displays detailed file download information of clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays file download status of clients, including client information (such as the client ID, MAC address, and IP address), scenario (zero touch device deployment, faulty device replacement, or batch upgrade), downloaded files, file download phase, and current status.

A client downloads files in the following sequence: system software, patch file, license file, web page file, configuration file, and user-defined file.

If the **client** *client-id* or **verbose** parameter is not specified, brief file download information of all clients is displayed.

Example

Display brief file download information of all clients.

```
<HUAWEI> display easy-operation download-status
---------------------------------------------------------------------------
 ID    Mac address     IP address      Method      Phase        Status
---------------------------------------------------------------------------
 1      00e0-fc12-3456 10.10.10.5      Zero-touch  Sys-file      Upgrading
 2      00e0-fc12-3333 10.10.10.6      Upgrade     Config-file   Failed
 3      00e0-fc12-1A52 10.10.10.7      Zero-touch  Patch-file    Waiting
 4      00e0-fc12-4458 10.10.10.8      Zero-touch  Web-file      Upgrading
---------------------------------------------------------------------------
```

Display detailed file download information of client 5.

```
<HUAWEI> display easy-operation download-status verbose
The total number of client in downloading files is : 1

---------------------------------------------------------------------------
 Client ID                    : 5
 Mac address                  : 00e0-fc12-2323
 ESN                          : 210235362912xxxxxxxx
 Host name                    : RTF_1-54
 IP address                   : 192.168.14.252
 Method                       : Zero-touch
 IP address of file server    : 192.168.1.88
 Type of file server          : SFTP
 Username of file server      : 1
 Configuration file           : -
 System-software file         : -
 Patch file                   : -
 WEB file                     : -
 License file                 : -
 Customs file 1               : -
 Customs file 2               : -
 Customs file 3               : -
 Activating file time         : Immediately
 Activating file method       : Default
 Phase                        : Unknown
 DownloadSize(byte)           : 29916738
 Status                       : Upgrading
 Reason                       : The device will enter getting download-information state.
 Description                  : The device will enter getting download-information state.
---------------------------------------------------------------------------
```

Table 2-8 Description of the **display easy-operation download-status** command output

Item	Description
ID/Client ID	Client ID.
Mac address	Client MAC address.
ESN	Client ESN.
Host name	Client host name.
IP address	Client IP address.

Item	Description
Method	EasyDeploy scenario. ● Zero-touch: zero touch device deployment and faulty device replacement. ● Upgrade: batch upgrade.
Phase	File download phase: Sys-file, Config-file, Patch-file, Web-file, License-file, Custom-file, Activating, Rebooting, and Unknown.
Status	File download status. ● Upgrading: The client is downloading a file. ● Waiting: The client is waiting for download. ● Failed: The client fails to download a file because its storage space is insufficient or the file to be downloaded does not exist.
IP address of file server	File server IP address.
Type of file server	File server type.
Username of file server	User name for accessing the file server.
System-software file	System software that is being downloaded.
Configuration file	Configuration file that is being downloaded.
Patch file	Patch file that is being downloaded.
WEB file	Web page file that is being downloaded.
License file	License file that is being downloaded.
Customs file 1	First user-defined file that is being downloaded.
Customs file 2	Second user-defined file that is being downloaded.
Customs file 3	Third user-defined file that is being downloaded.

Item	Description
DownloadSize(byte)	Size of a downloaded file. **NOTE** If the system software is upgraded from V200R009 or an earlier version to V200R010 or a later version, this field displays -.
Activating file time	File activation time. **Immediately** indicates that files are activated immediately after they are downloaded.
Activating file method	File activation mode. **Default** indicates the default activation mode; **Reload** indicates that all files are activated by device resetting.
Reason	File download result. For possible results and solutions, see **Table 2-9**.
Description	Result description. For possible results and measures, see **Table 2-9**.

Table 2-9 Download results and solutions

Reason	Description	Solution
Input has been detected in the console	Input has been detected in the console. EasyOperation will stop	During zero touch device deployment, input is detected on the console interface of the device to be deployed, so EasyOperation stops. You are advised to restart the device to restart the deployment process. Do not input anything on the console interface during EasyOperation.
The USB upgrade is working	The USB upgrade is working. EasyOperation will stop	The device is performing USB-based deployment. USB-based deployment and EasyDeploy are mutually exclusive. You are advised to stop one of the two functions.

Reason	Description	Solution
The uni-mng system is working	The uni-mng system is working. EasyOperation will stop	The device is running SVF. SVF and EasyDeploy are mutually exclusive. You are advised to stop one of the two functions.
The device has in initial state	The device is in initial state. EasyOperation will stop	The device is in web initialization mode. Web initial login mode and EasyDeploy are mutually exclusive. You are advised to stop one of the two functions.
Getting download-information failed. The device will get download-information again	Getting download-information failed. The device will be back to initialization state.	The device to be deployed fails to obtain file download information. ● If the device is deployed using an intermediate file, check whether the intermediate file has the correct content and format, whether the network between the device and server that stores the intermediate file is normal, and whether the configured file server user name and password are correct. ● If the device is deployed using the Commander, check whether the network between the device and Commander is normal and whether the configured download information is correct.
Downloading file failed	The system software file and version are wrong. The device will be back to initialization state	The system software version is specified but the system software file is not specified. You need to specify the system software file.

Reason	Description	Solution
	Downloading the system software file failed. Please check the reason	1. Check whether a network fault occurs during file download. 2. Check whether the file server that stores files is working properly. 3. Check whether the file names of the system software, patch file, configuration file, license file, web file, and user-defined file are valid. 4. Check whether the system software, patch file, configuration file, license file, web file, and user-defined file to be downloaded have the same names as the current system files. 5. Check whether the device to be upgraded has enough disk space.
	Downloading the patch file failed. Please check the reason	
	Downloading the web file failed. Please check the reason	
	Downloading the license file failed. Please check the reason	
	Downloading the configuration file failed. Please check the reason	
	Downloading the custom file 1 failed. Please check the reason	
	Downloading the custom file 2 failed. Please check the reason	
	Downloading the custom file 3 failed. Please check the reason	
The file does not exist in the file server	The file does not exist in the file server	The file to be downloaded does not exist in the file server. Ensure that the file exists in the file server.
There is no enough space on the device	There is no enough space on master device or board	The disk space on the device to be upgraded is insufficient for the system software. Ensure that the device has enough disk space.
The file server is unreachable	The file server is unreachable	Check whether the configured file server IP address is correct and whether the network connection between the device and file server is normal.

Reason	Description	Solution
Authentication on file server fails	Authentication on file server fails	Authentication fails on the file server. Check whether the following configurations are correct: 1. User name and password 2. User management configuration on the file server 3. Other user management configurations
The filename is the same as the system file	The filename of the patch is same as the system patch file	The downloaded patch has the same file name as the system patch file.
	The filename of the system-software is same as the system file	The downloaded patch has the same file name as the system patch file.
Check file failed	System-software crc check error	The CRC check of the downloaded system software fails. Check whether the system software of the file server is correct.
The file is a system file on the other device	The file is system file on other device	The patch to be downloaded is the system file on the standby or slave device.

Reason	Description	Solution
Activate file failed. The device will be back to initialization state after 5 minutes	Activating file failed. The device will be back to initialization state after 5 minutes	File activation because of the following reasons: 1. Failed to set the system software, configuration file, and patch file as next startup files. Check whether these files are available. 2. Failed to start the device. Check whether the device has unsaved configuration, whether next startup files on the master and standby devices are consistent, and whether system files are damaged.
Reboot system failed	The WLAN configuration conflicts with the next startup system software. To prevent configuration loss, use the eDesk tool to convert the configuration, and then specify the new configuration file for next startup	The device has WLAN configurations, which may be lost when the device is upgraded. You need to export the WLAN configurations, use a dedicated tool to convert the configurations, and then import them for use.
Copying file to other device or board failed	Copying file to other device or board failed	Failed to copy files to the standby or slave device. Check whether the file system function is normal and whether boards are installed or removed when files are being copied.
	There is no enough space on other device or board	There is insufficient disk space on the standby or slave device when upgrade files are being copied to the standby or slave device. Ensure that the disk space is enough to store all the upgrade files.

Reason	Description	Solution
The download file was deleted	The download file was deleted in client, please check the environment	The downloaded upgrade files are deleted. Check whether other users have logged in to the device and deleted the files.
Unknown error	Unknown error	An unknown error occurs in the system. Contact technical support personnel.
EasyOperation client operation failed	The file server is not configured. Configure a file server first. Check whether a file server has been configured correctly	Check whether a file server has been configured correctly.

2.2.22 display easy-operation group

Function

The **display easy-operation group** command displays group information on the Commander.

Format

display easy-operation group [**build-in** [*device-type* [**vendor** *vendorname*]] | **custom** [*group-name*]]

Parameters

Parameter	Description	Value
build-in	Displays built-in group information. If the device type is not specified, information about all built-in groups is displayed.	-

Parameter	Description	Value
device-type	Specifies a device type.	The value is an enumerated type and case-insensitive. The following device types are supported: - S2730S-S - S2750-EI - S5700-10P-LI - S5700-EI - S5700-HI - S5700-P-LI - S5700-SI - S5700-TP-LI - S5700-X-LI - S5700S-LI - S5700S-P-LI - S5700S-X-LI - S5710-EI - S5710-HI - S5710-X-LI - S5720-EI - S5720-HI - S5720-LI - S5720-SI - S5720S-LI - S5730-HI - S5730-SI - S5730S-EI - S5731-H - S5731-S - S5731S-H - S5731S-S - S5732-H - S5735-L - S5735-L1 - S5735-L-I - S5735S-L - S5735S-L1 - S5735-S - S5735S-S - S5735S-H

Parameter	Description	Value
		S5736-S S6700-EI S6720-EI S6720-HI S6720-LI S6720-SI S6720S-S S6720S-LI S6720S-SI S6730-H S6730S-H S6730-S S6730S-S S6735-S S9700
vendor *vendorname*	Displays the name of the group created based on the device type of the specified vendor. If no group name is specified, all vendor groups of the corresponding device types are displayed.	The value is a string of case-sensitive characters. It cannot contain spaces.
custom	Displays customized group information. If the group name is not specified, information about all customized groups is displayed.	-
group-name	Specifies the name of a customized group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about groups on the Commander.

If the **build-in** or **custom** parameter is not specified, brief information about all groups on the Commander is displayed.

Example

Display brief information about all groups on the Commander.

```
<HUAWEI> display easy-operation group
The total number of group configured is : 6
The number of build-in group is         : 2
The number of custom group is           : 4

-------------------------------------------------------
 Groupname                       Type     MatchType
-------------------------------------------------------
 AAA                            custom   ip-address
 F1                             custom   ip-address
S5720-HI                         build-in device-type
 test                           custom   mac-address
 test1                          custom   ip-address
-------------------------------------------------------
```

Display information about built-in groups.

```
<HUAWEI> display easy-operation group build-in
---------------------------------------------------------------------------
 Group name                : S5720-HI
 Configuration file        : vrpcfg.zip
 System-software file      : S5720-HI.cc
 Patch file                : -
 WEB file                  : -
 License file              : -
 Customs file 1            : -
 Customs file 2            : -
 Customs file 3            : -
 Activating file time      : Immediately
 Activating file method    : Default
---------------------------------------------------------------------------
```

Display information about the customized group **AAA**.

```
<HUAWEI> display easy-operation group custom AAA
---------------------------------------------------------------------------
 Group name                : AAA
 Configuration file        : -
 System-software file      : -
 Patch file                : -
 WEB file                  : -
 License file              : -
 Customs file 1            : header.txt
 Customs file 2            : -
 Customs file 3            : -
 Activating file time      : Immediately
 Activating file method    : Default
 Ip-address list           :
  Ip-address        Ip-mask
  192.168.150.110   255.255.255.0
  192.168.150.111   255.255.255.0
  192.168.150.112   255.255.255.0
  192.168.150.113   255.255.255.0
  192.168.150.114   255.255.255.0
  192.168.150.115   255.255.255.0
---------------------------------------------------------------------------
```

Table 2-10 Description of the **display easy-operation group** command output

Item	Description
Groupname	Group name.
Type	Group type: build-in or custom.
MatchType	Match type of the group. The match type of a built-in group is configured using the **group build-in** command. The match type of a customized group is configured using the **group custom** command.
Configuration file	System software to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **configuration-file** command.
System-software file	Configuration file to be downloaded by the clients matching the group. If no configuration file is specified, this field displays a hyphen (-). It can be configured using the **system-software** command.
Patch file	Patch file to be downloaded by the clients matching the group. If no patch file is specified, this field displays a hyphen (-). It can be configured using the **patch** command.
WEB file	Web page file to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **web-file** command.
License file	License file to be downloaded by the clients matching the group. If no license file is specified, this field displays a hyphen (-). It can be configured using the **license** command.

Item	Description
Customs file 1	First user-defined file to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **custom-file** command.
Customs file 2	Second user-defined file to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **custom-file** command.
Customs file 3	Third user-defined file to be downloaded by the clients matching the group. If no third user-defined file is specified, this field displays a hyphen (-). It can be configured using the **custom-file** command.
Activating file time	File activation time used by the clients matching the group. If default file activation time is used, this field displays **Immediately**. It can be configured using the **activate-file** command.
Activating file method	File activation mode used by the clients matching the group. If default mode is used, this field displays **Default**. It can be configured using the **activate-file** command.

Item	Description
Ip-address list	Clients match the group based on IP addresses, and all matching IP addresses are displayed. ● If clients match the group based on ESNs, **ESN list** is displayed. ● If clients match the group based on MAC addresses, **Match mac-address list** is displayed. ● If clients match the group based on models, **Product model** is displayed. ● If clients match the group based on types, **Device type** is displayed. The matching rule can be configured using the **match** command.

2.2.23 display easy-operation power

Function

The **display easy-operation power** command displays power consumption information of the Commander and clients.

Format

display easy-operation power [**client** *client-id* | **commander**]

Parameters

Parameter	Description	Value
client *client-id*	Indicates power consumption information of a specified client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
commander	Indicates power consumption information of the Commander.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command used to check power consumption information differs on the Commander and clients.

- On the Commander
  - If no parameter is specified, you can check power consumption information about the Commander and all the clients in initial, upgrade, and normal operating states.
  - If only **client** *client-id* is specified, you can check power consumption information about the specified client.
  - If only **commander** is specified, you can check power consumption information about the Commander.
- On the client

  The parameters **client** *client-id* and **commander** are not supported. You can check power consumption information only about the current client.

Example

Display power consumption information of the Commander and clients.

```
<HUAWEI> display easy-operation power
--------------------------------------------------------------------------------
Role       HostName                    Interface      Usage(W)     Gauge    Mode
--------------------------------------------------------------------------------
Commander       HUAWEI                                  995.0     actual   standard
Client1     HUAWEI                                 511.3      rated   standard
                                GE0/0/1        0.7       actual
Client3     HUAWEI                                 93.0      rated   standard
Client4     HUAWEI                                 100.0      rated   standard
--------------------------------------------------------------------------------
```

Table 2-11 Description of the **display easy-operation power** command output

Item	Description
Role	Device role in the EasyDeploy service, which can be Commander or client.
HostName	Device name.
Interface	Interface name: ● If this parameter is left blank, power consumption of the entire device is displayed. ● If an interface name is specified, power consumption of a power device connected to the corresponding interface is displayed.
Usage(W)	Power consumption, in Watts.

Item	Description
Gauge	Power consumption type: ● actual: indicates real-time power consumption. ● rated: indicates rated power consumption.
Mode	Energy saving mode: ● standard ● basic ● deep

2.2.24 display easy-operation topology

Function

The **display easy-operation topology** command displays network topology information collected by the Commander.

Format

display easy-operation topology

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view network topology information collected by the Commander. Based on the collected information, zero touch device deployment and automatic faulty device replacement can be implemented.

Example

Display network topology information collected by the Commander.

```
<HUAWEI> display easy-operation topology
<-->:normal device         <??>:lost device
Total topology node number: 3
-------------------------------------------------------------------------------
```

```
[HUAWEI: xxxx-xxxx-xxxx](Commander)
|-(GE0/0/8)<-->(GE0/0/38)[HUAWEI: xxxx-xxxx-xxxx](Client 1)
| |-(GE0/0/16)<-->(GE0/0/16)[HUAWEI: xxxx-xxxx-xxxx]  (Client 2)
```

Table 2-12 Description of the **display easy-operation topology** command output

Item	Description
<-->	Clients that are running properly.
<??>	Properly operating clients change to the lost state.
Total topology node number	Number of nodes (including the Commander) in the network topology.

2.2.25 display ndp

Function

The **display ndp** command displays the global NDP information or the NDP information on a specified interface.

Format

display ndp [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] }	Displays the NDP information on a specified interface. ● *interface-type interface-number1* indicates the type and number of the first interface. ● *interface-type interface-number2* indicates the type and number of the last interface. If no interface is specified when you run the **display ndp** command, NDP information about all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you check the NDP information:

- If NDP is not globally enabled, only the current NDP status of a switch is displayed.
- If NDP is globally enabled, the global NDP information and status and the NDP information and status of interfaces on a switch are displayed.

Example

Display the global NDP information and NDP information about all the interfaces.

```
<HUAWEI> display ndp
 Neighbor discovery protocol is enabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 114, Packets Received: 108, Packets Error: 0
    Neighbor 1:  Aging Time: 174(s)
       MAC Address : xxxx-xxxx-xxxx
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.130 V200R023C00
       Device Name : S5720
       Port Duplex : FULL
       Product Ver : S5720 V200R023C00
---- More ----
```

Table 2-13 Description of the **display ndp** command output

Item	Description
Neighbor discovery protocol is *status*	The global NDP function is in *status* state. *status* includes: - disabled: NDP is disabled globally. - enabled: NDP is enabled globally. To set this value, run the **ndp enable (system view)** command.
Neighbor Discovery Protocol Ver	Currently supported NDP versions. Version 1 is currently supported by all devices.
Hello Timer	Interval for sending NDP packets, in seconds. To set this value, run the **ndp timer hello** command.
Aging Timer	Aging time of NDP information, in seconds. To set this value, run the **ndp timer aging** command.
Interface	Interface number of a switch.

Item	Description
Status	NDP status of an interface: - Disabled: NDP is disabled on the interface. - Enabled: NDP is enabled on the interface. To set this value, run the **ndp enable (system view)** or **ndp enable (interface view)** command.
Packets Sent	Number of NDP packets sent from the interface.
Packets Received	Number of NDP packets received by the interface.
Packets Error	Number of incorrect NDP packets received by the interface.
Neighbor 1	Neighboring node 1.
Aging Time	Aging time of NDP information about a neighboring node connected to the interface.
MAC Address	MAC address of the neighboring node.
Port Name	Name of the interface on the neighboring node connected to the interface.
Software Version	Version of the system software on the neighboring node.
Device Name	Host name of the neighboring node.
Port Duplex	Duplex mode of the interface on the neighboring node connected to the local interface. - FULL: full-duplex. - Half: half-duplex.
Product Ver	Type and software version number of the neighboring node.

Display the NDP information of the switch on which NDP is not globally enabled.

```
<HUAWEI> display ndp
 Neighbor discovery protocol is disabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
```

2.2.26 display ntdp

Function

The **display ntdp** command displays NTDP configuration.

Format

display ntdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ntdp** command to check the NTDP configuration of a switch without considering whether NTDP is enabled globally or on interfaces on the switch.

Example

Display the NTDP configuration of a switch.

```
<HUAWEI> display ntdp
Network topology discovery protocol is enabled
Hops      : 8
Timer     : 0 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection: 330 ms
```

Table 2-14 Description of the **display ntdp** command output

Item	Description
Network topology discovery protocol is *status*	The global NTDP function is in *status* state. *status* includes the following types of status: ● disabled: NTDP is disabled globally. ● enabled: NTDP is enabled globally. To set this value, run the **ntdp enable (system view)** command.

Item	Description
Hops	Topology collection range (the number of hops). To set this value, run the **ntdp hop** command.
Timer	Interval for collecting topology information. To set this value, run the **ntdp timer** command.
Hop Delay	Delay for the first interface to forward NTDP topology request packets. To set this value, run the **ntdp timer hop-delay** command.
Port Delay	Delay for other interfaces to forward NTDP topology request packets. To set this value, run the **ntdp timer port-delay** command.
Total time for last collection	Duration for collecting topology information last time.

2.2.27 display ntdp device-list

Function

The **display ntdp device-list** command displays the topology information collected using NTDP.

Format

display ntdp device-list [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed device information. If you run the **display ntdp device-list** command without setting optional parameters, brief information about the device is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the topology information collected using NTDP, run the **display ntdp device-list** command. The topology information can be displayed only after **ntdp explore** command is run in the user view to enable the switch to periodically collect the topology information.

When NTDP is not enabled on interfaces of the switch, only information about the switch itself is collected using NTDP.

Prerequisites

NTDP has been globally enabled on the switch.

Example

Display brief switch information collected using NTDP.

```
<HUAWEI> display ntdp device-list
The device-list of NTDP:
------------------------------------------------------------------------------
 MAC            HOP  IP                PLATFORM
------------------------------------------------------------------------------
 xxxx-xxxx-xxxx  0                     S5700
 xxxx-xxxx-xxxx  1    10.1.1.2/24        S5700
 xxxx-xxxx-xxxx  1    10.1.1.3/24        S5700
```

Table 2-15 Description of the **display ntdp device-list** command output

Item	Description
MAC	MAC address of the device.
HOP	Number of hops from the device to the topology collecting device.
IP	IP address of the device.
PLATFORM	Type of the device.

Display detailed device information collected using NTDP.

```
<HUAWEI> display ntdp device-list verbose
 Hostname  : HUAWEI
 MAC       : xxxx-xxxx-xxxx
 Hop       : 0
 Platform  : S5700
 IP        :
 Version   : Version 5.150 V200R023C00
 Cluster   : Administrator switch of cluster
 Peer MAC        Native Port ID Peer Port ID   N-Index    P-Index    Speed Dup
 xxxx-xxxx-xxxx  GE0/0/4        GE0/0/4        9          9          1000  FULL
 xxxx-xxxx-xxxx  GE0/0/1        GE0/0/1        6          6          1000  FULL


-----------------------------------------------------------------------------

 Hostname  : HUAWEI
 MAC       : xxxx-xxxx-xxxx
 Hop       : 1
```

```
Platform  : S5700
IP        : 10.1.1.2/24
Version   : Version 5.150 V200R023C00
Cluster   : Candidate switch

Peer MAC        Native Port ID Peer Port ID   N-Index    P-Index    Speed Dup
xxxx-xxxx-xxxx  GE0/0/4        GE0/0/4        9          9          1000   FULL

------------------------------------------------------------------------------

Hostname  : HUAWEI
MAC       : xxxx-xxxx-xxxx
Hop       : 1
Platform  : S5700
IP        : 10.1.1.3/24
Version   : Version 5.150 V200R023C00
Cluster   : Candidate switch

Peer MAC        Native Port ID Peer Port ID   N-Index    P-Index    Speed Dup
xxxx-xxxx-xxxx  GE0/0/1        GE0/0/1        6          6          1000   FULL
```

Table 2-16 Description of the **display ntdp device-list verbose** command output

Item	Description
Hostname	Host name of the device.
MAC	MAC address of the device.
Hop	Number of hops from the device to the topology collecting device.
Platform	Model of the device.
IP	Private IP address of the device.
Version	Version of the system software running on the device.
Cluster	Role of the device in the cluster.
Peer MAC	MAC address of the neighboring node.
Native Port ID	Interface of the device connecting to the neighboring node.
Peer Port ID	Interface of the neighboring node connecting to the local device.
N-Index	Index of the local interface.
P-Index	Index of the peer interface.
Speed	Rate of the interface when the neighboring node is connected to the device.
Dup	Duplex mode of the interface when the neighboring node is connected to the local device.

2.2.28 display cluster-topology-info

Function

The **display cluster-topology-info** command displays the topology information about the cluster.

Format

display cluster-topology-info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cluster-topology-info** command on the Commander switch only.

NOTE

If two devices are connected through multiple interfaces, this command displays information only about the link established between a pair of interfaces.

Example

Display the topology information about the cluster.

```
<HUAWEI> display cluster-topology-info
The topology information about the cluster:
<-->:normal device        <++>:candidate device        <??>:lost device
------------------------------------------------------------------------
Total topology node number is 5.
[HUAWEI_0.Administrator: Root-00e0-ad14-c600]
|-(GigabitEthernet0/0/2)<-->(GigabitEthernet0/0/1)[HUAWEI_3.Member-3: xxxx-xxxx-xxxx]
| |-(GigabitEthernet0/0/3)<-->(GigabitEthernet0/0/1)[HUAWEI_2.Member-2: xxxx-xxxx-xxxx]
| | |-(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/1)[HUAWEI_1.Member-1: xxxx-xxxx-xxxx]
|-(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/2)[HUAWEI_4.Member-4: xxxx-xxxx-xxxx]
```

Table 2-17 shows the description of the **display cluster-topology-info** command output.

Table 2-17 Description of the **display cluster-topology-info** command output

Item	Description
<-->	Normal link.

Item	Description
<++>	Candidate link.
<??>	Faulty link.
Total topology node number is	Specifies the number of nodes in the topology of the cluster.
[HUAWEI_0.Administrator: Root-xxxx-xxxx-xxxx]	Specifies the MAC address and host name of the switch. It varies with the name and MAC address of the device.
|-	Indicates the level-1 device that is connected to the root node.
| |-	Indicates the level-2 device which is connected to the level-1 device.
| | |-	Indicates the level-3 device which is connected to the level-2 device.
(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/2)	Specifies the names of the interfaces connecting the two devices. It varies with the interfaces of the devices. The left brackets contain information about the upper-level device. The right brackets contain information about the lower-level device.
[HUAWEI_3.Member-3: xxxx-xxxx-xxxx]	Specifies the MAC address of the member device. It varies with the name and MAC address of the device.

2.2.29 easy-operation

Function

The **easy-operation** command displays the Easy-Operation view.

Format

easy-operation

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To specify the file server, information about files to be downloaded, and file activation mode, or configure other EasyDeploy-related functions, first run the **easy-operation** command to enter the Easy-Operation view.

Prerequisites

You can enter the Easy-Operation view only on the device functions as a Commander.

After choosing a device as the Commander, run the **easy-operation commander ip-address** command on the device to configure the Commander IP address, and then run the **easy-operation commander enable** command to enable the Commander function.

Example

Enter the Easy-Operation view.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation]
```

2.2.30 easy-operation client ftp-server

Function

The **easy-operation client ftp-server** command specifies IP addresses, user names, and passwords for FTP servers on a pre-delivery device.

The **undo easy-operation client ftp-server** command deletes the specified IP addresses, user names, and passwords of FTP servers on a pre-delivery device.

By default, IP addresses, user names, and passwords of FTP servers are not specified on pre-delivery devices.

Format

easy-operation client ftp-server ip-address *ipaddress* &<1-4> [**username** *username* [**password** *password*]]

undo easy-operation client ftp-server ip-address [*ipaddress*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
ip-address *ipaddress*	Specifies the IP address of an FTP server.	The value is in dotted decimal notation.

Parameter	Description	Value
username *username*	Specifies a user name for FTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for FTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client ftp-server** command to specify IP addresses, user names, and passwords for the servers.

Precautions

- The **easy-operation client ftp-server** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client ftp-server** command in the system view to delete the specified IP addresses, user names, and passwords of FTP servers.
- If a user name and a password have been set on a file server, the device must have the same user name and password configured.
- FTP has security risks. Using an SFTP file server is recommended.
- A maximum of four FTP file servers' IP addresses, user names, and passwords can be specified. A device searches for and obtains the desired files from the servers in the sequence in which file servers are configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the IP address, user name, and password of an FTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client ftp-server ip-address 10.1.1.1 username huawei password
```

2.2.31 easy-operation client ftp-server-url

Function

The **easy-operation client ftp-server-url** command specifies URLs, user names, and passwords for FTP servers on a pre-delivery device.

The **undo easy-operation client ftp-server-url** command deletes the specified URLs, user names, and passwords of FTP servers on a pre-delivery device.

By default, URLs, user names, and passwords of FTP servers are not specified on pre-delivery devices.

Format

easy-operation client ftp-server-url *url-address* [**username** *username* [**password** *password*]]

undo easy-operation client ftp-server-url [*url-address*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
url-address	Specifies the URL of an FTP server.	The value is a string of 1 to 64 characters.
username *username*	Specifies a user name for FTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for FTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client ftp-server-url** command to specify URLs, user names, and passwords for the servers.

Precautions

The **easy-operation client ftp-server-url** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client ftp-server-url** command in the system view to delete the specified URLs, user names, and passwords of FTP servers.

You can specify an FTP server using either an IP address or URL.

Example

Delete the URL, user name, and password of an FTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client ftp-server-url www.1234.com username huawei password
```

2.2.32 easy-operation client netfile

Function

The **easy-operation client netfile** command specifies a name for an intermediate file for pre-configured device deployment.

The **undo easy-operation client netfile** command deletes the name of an intermediate file for pre-configured device deployment.

By default, devices use the intermediate file **lswnet.cfg** for pre-configured device deployment.

Format

easy-operation client netfile *filename*

undo easy-operation client netfile [*filename*]

Parameters

Parameter	Description	Value
filename	Specifies the name (*.cfg) of an intermediate file.	The value is a string of 5 to 48 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A pre-configured device obtains version file information from an intermediate file placed on a file server. This information includes an SNMP host's IP address, device's MAC address, ESN or model, and names of files to be downloaded.

If you do not specify an intermediate file, the device uses the **lswnet.cfg** file by default. If you want to use another intermediate file, run the **easy-operation client netfile** command.

Precautions

The **easy-operation client netfile** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use pre-configured device deployment, run the **undo easy-operation client netfile** command in the system view to delete the intermediate file.

The configuration file specified in an intermediate file cannot contain any pre-configured commands.

Example

Delete the intermediate file specified for pre-configured device deployment.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client netfile huawei.cfg
```

2.2.33 easy-operation client sftp-server

Function

The **easy-operation client sftp-server** command specifies IP addresses, user names, and passwords for SFTP servers on a pre-delivery device.

The **undo easy-operation client sftp-server** command deletes the specified IP addresses, user names, and passwords of SFTP servers on a pre-delivery device.

By default, IP addresses, user names, and passwords of SFTP servers are not specified on pre-delivery devices.

Format

easy-operation client sftp-server ip-address *ipaddress* &<1-4> [**username** *username* [**password** *password*]]

undo easy-operation client sftp-server ip-address [*ipaddress*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
ip-address *ipaddress*	Specifies the IP address of an SFTP server.	The value is in dotted decimal notation.

Parameter	Description	Value
username *username*	Specifies a user name for SFTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for SFTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client sftp-server** command to specify IP addresses, user names, and passwords for the servers.

Precautions

- The **easy-operation client sftp-server** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client sftp-server** command in the system view to delete the specified IP addresses, user names, and passwords of SFTP servers.
- If a user name and a password have been set on a file server, the device must have the same user name and password configured.
- A maximum of four SFTP file servers' IP addresses, user names, and passwords can be specified. A device searches for and obtains the desired files from the servers in the sequence in which file servers are configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the IP address, user name, and password of an SFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client sftp-server ip-address 10.1.1.1 username huawei password
```

2.2.34 easy-operation client sftp-server-url

Function

The **easy-operation client sftp-server-url** command specifies URLs, user names, and passwords for SFTP servers on a pre-delivery device.

The **undo easy-operation client sftp-server-url** command deletes the specified URLs, user names, and passwords of SFTP servers on a pre-delivery device.

By default, URLs, user names, and passwords of SFTP servers are not specified on pre-delivery devices.

Format

easy-operation client sftp-server-url *url-address* [**username** *username* [**password** *password*]]

undo easy-operation client sftp-server-url [*url-address*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
url-address	Specifies the URL of an SFTP server.	The value is a string of 1 to 64 characters.
username *username*	Specifies a user name for SFTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for SFTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client sftp-server-url** command to specify URLs, user names, and passwords for the SFTP servers on the device.

Precautions

- The **easy-operation client sftp-server-url** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client sftp-server-url** command in the system view to delete the specified URLs, user names, and passwords of SFTP servers.
- You can specify an SFTP server using either an IP address or URL.
- If a user name and a password have been set on a file server, the device must have the same user name and password configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the URL, user name, and password of an SFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client sftp-server-url www.1234.com username huawei password
```

2.2.35 easy-operation client snmp securityname

Function

The **easy-operation client snmp securityname** command configures a shared key between a pre-delivery device and an SNMP host.

The **undo easy-operation client snmp securityname** command deletes a shared key between a pre-delivery device and an SNMP host.

By default, no shared key is configured between pre-delivery devices and SNMP hosts.

Format

easy-operation client snmp securityname cipher *password*

undo easy-operation client snmp securityname

Parameters

Parameter	Description	Value
cipher *password*	Specifies a shared key.	The value is a string of 1 to 32 characters in plaintext, or 48 or 68 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In pre-configured device deployment, a pre-delivery device sends alarms to an NMS over an SNMP module for deployment monitoring. To configure a shared key between the device and the SNMP host, run the **easy-operation client snmp securityname** command.

Precautions

The **easy-operation client snmp securityname** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client snmp securityname** command in the system view to delete the shared key.

Example

Delete the shared key between a pre-delivery device and an SNMP host.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client snmp securityname
```

2.2.36 easy-operation client tftp-server

Function

The **easy-operation client tftp-server** command specifies IP addresses for TFTP servers on a pre-delivery device.

The **undo easy-operation client tftp-server** command deletes the specified IP addresses of TFTP servers on a pre-delivery device.

By default, IP addresses of TFTP servers are not specified on pre-delivery devices.

Format

easy-operation client tftp-server ip-address *ipaddress* &<1-4>

undo easy-operation client tftp-server ip-address [*ipaddress*]

Parameters

Parameter	Description	Value
ip-address *ipaddress*	Specifies the IP address of a TFTP server.	The value is in dotted decimal notation.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client ftp-server** command to specify IP addresses for the servers.

Precautions

- The **easy-operation client tftp-server** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client tftp-server** command in the system view to delete the specified IP addresses of TFTP servers.
- TFTP has security risks. Using an SFTP file server is recommended.
- A maximum of four TFTP file servers' IP addresses can be specified. A device searches for and obtains the desired files from the servers in the sequence in which file servers are configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the IP address of a TFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client tftp-server ip-address 10.1.1.1
```

2.2.37 easy-operation client tftp-server-url

Function

The **easy-operation client tftp-server-url** command specifies URLs for TFTP servers on a pre-delivery device.

The **undo easy-operation client tftp-server-url** command deletes the specified URLs of TFTP servers on a pre-delivery device.

By default, URLs of TFTP servers are not specified on pre-delivery devices.

Format

easy-operation client tftp-server-url *url-address*

undo easy-operation client tftp-server-url [*url-address*]

Parameters

Parameter	Description	Value
url-address	Specifies the URL of a TFTP server.	The value is a string of 1 to 64 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client tftp-server-url** command to specify URLs for the servers.

Precautions

The **easy-operation client tftp-server-url** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client tftp-server-url** command in the system view to delete the specified URLs of TFTP servers.

You can specify either an IP address or URL for a TFTP server.

Example

Delete the URL of a TFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client tftp-server-url www.1234.com
```

2.2.38 easy-operation client vlan

Function

The **easy-operation client vlan** command specifies the VLAN used in the configured device deployment procedure before device delivery.

The **undo easy-operation client vlan** command deletes the VLAN used in the configured device deployment procedure.

By default, the VLAN used in the configured device deployment procedure is VLAN 1.

Format

easy-operation client vlan *vlanid*

undo easy-operation client vlan

Parameters

Parameter	Description	Value
vlanid	Specifies the VLAN used in the configured device deployment procedure.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

You can use the default VLAN 1 or run this command to specify the VLAN used in the configured device deployment procedure to implement configured device deployment.

Precautions

- This command is an overwritten command.
- The **easy-operation client vlan** command is contained only in a device's pre-delivery configuration file. Users cannot manually run this command. The **undo easy-operation client vlan** command can be manually run.

Example

Delete the VLAN used in the configured device deployment procedure.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client vlan
```

2.2.39 easy-operation client ztp-with-cfg enable

Function

The **easy-operation client ztp-with-cfg enable** command enables pre-configured device deployment.

The **undo easy-operation client ztp-with-cfg enable** command disables pre-configured device deployment.

By default, pre-configured device deployment is disabled.

Format

easy-operation client ztp-with-cfg enable

undo easy-operation client ztp-with-cfg enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before delivery, a device can load a configuration file that contains commands for specifying file server addresses, name of an intermediate file for site deployment, and a shared key between the device and an SNMP host. After simple login configuration, the device can then automatically obtain and load correct configurations, reducing the manual operation cost.

Precautions

The **easy-operation client ztp-with-cfg enable** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not need the pre-configured device deployment function, run the **undo easy-operation client ztp-with-cfg enable** command in the system view to disable this function.

Example

Disable the pre-configured device deployment function on a device.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client ztp-with-cfg enable
```

2.2.40 easy-operation commander enable

Function

The **easy-operation commander enable** command enables the Commander function on a device.

The **undo easy-operation commander enable** command disables the Commander function on a device.

By default, the Commander function is disabled on a device.

Format

easy-operation commander enable

undo easy-operation commander enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To specify a device as the Commander, enable the Commander function on the device. The Commander can enable devices to automatically download files in zero touch device deployment, fault device replacement, and batch upgrade scenarios. On an EasyDeploy network, the Commander manages clients and delivers required information, including file server information, system software name, and configuration file name, to clients. Clients automatically download required files according to information obtained from the Commander.

Prerequisites

The Commander IP address has been configured on the device using the **easy-operation commander ip-address** command.

Precautions

- An EasyDeploy network has only one Commander.
- This command can be used only on the device that functions as the Commander.
- After you run the **undo easy-operation commander enable** command to disable the Commander function, dynamic information in the client database is deleted, and the configuration information is saved in the memory of the device. If the Commander does not restart after the Commander function is disabled, the configuration will be recovered after the Commander function is enabled again.

Example

Enable the Commander function on a device.

```
<HUAWEI> system-view
[HUAWEI] easy-operation commander enable
```

2.2.41 easy-operation commander ip-address

Function

The **easy-operation commander ip-address** command configures the Commander IP address.

The **undo easy-operation commander ip-address** command deletes the Commander IP address.

By default, no Commander IP address is configured.

Format

easy-operation commander ip-address *ip-address* [**udp-port** *udp-port*]

undo easy-operation commander ip-address [*ip-address* [**udp-port** *udp-port*]]

Parameters

Parameter	Description	Value
ip-address	Specifies the Commander IP address.	The value is in dotted decimal notation.
udp-port *udp-port*	Specifies the UDP port number that the Commander uses to communicate with clients.	The value is an integer in the range from 1025 to 65535. The default value is 60000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an IP address is configured for the Commander, clients can communicate with the Commander through this IP address. To implement a batch upgrade, you need to specify the Commander IP address on clients. In zero touch provisioning (ZTP) and faulty device replacement scenarios, clients obtain the Commander IP address from the DHCP server.

Precautions

The configured Commander IP address must exist on the device that functions as the Commander.

The Commander IP address cannot be the IP address of the VLANIF interface bound to a VPN.

After the Commander function is enabled on the switch, changing the Commander IP address is not allowed on the switch. Otherwise, the Commander cannot detect and manage clients.

In batch upgrade scenarios, the Commander and clients must be configured with the same Commander IP address and UDP port number. Otherwise, clients cannot communicate with the Commander.

Example

Configure the Commander IP address.

```
<HUAWEI> system-view
[HUAWEI] easy-operation commander ip-address 10.10.10.5
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
```

Table 2-18 Description of the **easy-operation commander ip-address** command output

Item	Description
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]	Whether to change a pre-shared key. Regardless of whether the pre-shared key is changed, the **easy-operation commander ip-address** command can still be executed, and the Commander IP address can be changed successfully. ● y: The pre-shared key will be changed. ● n: The pre-shared key will not be changed.
Enter the pre-shared key	Enter the ciphertext of the pre-shared key. **NOTE** ● The same pre-shared key must be configured on the Commander and clients simultaneously. ● If the entered pre-shared key is invalid or the two pre-shared keys are different, the pre-shared key will not be changed. The failure to change the pre-shared key does not affect the execution of the **easy-operation commander ip-address** command. That is, the Commander IP address can still be changed successfully.
Confirm the pre-shared key	Confirm the ciphertext of the pre-shared key.

2.2.42 easy-operation dtls disable

Function

The **easy-operation dtls disable** command disables Datagram Transport Layer Security (DTLS) encryption.

The **undo easy-operation dtls disable** command enables DTLS encryption.

By default, DTLS encryption is enabled.

Format

easy-operation dtls disable

undo easy-operation dtls disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is mainly used in the capacity expansion scenario on a live network. If the system software of a client is V200R010C00 or a later version and that of the Commander is a version earlier than V200R010C00, you need to run the **easy-operation dtls disable** command on the client to disable DTLS encryption.

Precautions

- You must enable or disable DTLS encryption on the Commander and client at the same time.
- If the system software of a switch in a version earlier than V200R010C00 is upgraded to V200R010C00 or a later version, an **easy-operation dtls disable** configuration is automatically generated.
- If a client in V200R010C00 or a later version needs to be managed by the Commander in a version earlier than V200R010C00, you need to run the **easy-operation dtls disable** command on the client to disable DTLS encryption.
- If a client in a version earlier than V200R010C00 needs to be managed by the Commander in V200R010C00 or a later version and DTLS encryption is enabled on the Commander, you must upgrade the system software of the

client to V200R010C00 or a later version. Otherwise, the client cannot join the existing network.

- After DTLS encryption is enabled, the shared key configured using the **easy-operation shared-key** command does not take effect.
- After DTLS encryption is enabled, you can run the **easy-operation dtls psk** command to configure the DTLS PSK.

Example

Disable DTLS encryption.

```
<HUAWEI> system-view
[HUAWEI] easy-operation dtls disable
```

2.2.43 easy-operation dtls psk

Function

The **easy-operation dtls psk** command configures the DTLS pre-shared key (PSK).

The **undo easy-operation dtls psk** command restores the default DTLS PSK.

The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

easy-operation dtls psk *psk*

undo easy-operation dtls psk

Parameters

Parameter	Description	Value
psk	Specifies the PSK.	The value is a string of 6 to 32 characters in plain text or a string of 48 or 68 characters in cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DTLS encryption is enabled, you can run this command to change the DTLS PSK.

Precautions

The same PSK must be configured on the Commander and clients simultaneously.

Example

Set the DTLS PSK to **test12345**.

```
<HUAWEI> system-view
[HUAWEI] easy-operation dtls psk test12345
```

2.2.44 easy-operation shared-key

Function

The **easy-operation shared-key** command configures a shared key for the Commander or a client.

The **undo easy-operation shared-key** command deletes the configured shared key of the Commander or client.

By default, no shared key is configured on a Commander or client.

Format

easy-operation shared-key cipher *key-string*

undo easy-operation shared-key

Parameters

Parameter	Description	Value
cipher	Configures a shared key in cipher text.	-
key-string	Specifies a shared key.	The value is a string of case-sensitive characters without spaces. A plain text key contains 1 to 64 characters, and a cipher text key contains 48 to 108 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In batch upgrade and configuration scenarios, to enhance security for communication between the Commander and clients and prevent a bogus Commander from controlling clients, run the **easy-operation shared-key** command to configure the same shared key for the Commander and clients.

Precautions

- The same shared key must be configured on the Commander and clients simultaneously.
- If a shared key has been configured on the Commander, the Commander cannot manage clients running versions earlier than V200R008C00 and clients that have no shared key configured.
- The shared key configuration does not affect zero touch device deployment.
- After DTLS encryption is enabled, the shared key configured using the **easy-operation shared-key** command does not take effect.

Example

Configure a shared key on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation shared-key cipher Easy@huawei
```

2.2.45 execute to

Function

The **execute to** command enables the Commander to deliver commands to clients or client groups.

Format

execute [*script-file*] **to client** { **all** | { *client-id1* [**to** *client-id2*] }&<1-10> }

execute [*script-file*] **to group** { **all** | { **name** *group-name* }&<1-10> }

Parameters

Parameter	Description	Value
script-file	Indicates a script file name. If no script file name is specified, the script made online is delivered.	The value is a string of 5 to 64 characters, depending on the actual situation.

Parameter	Description	Value
client { *client-id1* [**to** *client-id2*] }	Indicates that commands are delivered to a specified client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
client all	Indicates that commands are delivered to all clients.	-
group name *group-name*	Indicates that commands are delivered to a specified client group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.
group all	Indicates that commands are delivered to all client groups.	-

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement a batch configuration of clients on a network supporting EasyDeploy, edit commands to be run, save them as a script, and deliver the edited commands to clients through the Commander.

Example

Enable the Commander to deliver commands to all clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] execute to client all
Warning: This operation will start the batch command executing process to the cl
ients. Continue?[Y/N]:y
Info: This operation will take some seconds, please wait..
```

2.2.46 group build-in

Function

The **group build-in** command configures a built-in group on the Commander and displays the Easy-Operation group view.

The **undo group build-in** command deletes a built-in group.

By default, no built-in group is configured.

Format

group build-in *device-type* [**vendor** *vendorname*]

undo group build-in [*device-type* [**vendor** *vendorname*]]

NOTE

- If clients of the same type from different vendors exist on the network, you need to configure **vendor** *vendorname* to distinguish the clients.
- If **vendor** *vendorname* is specified in the **group build in** command, the device type view of the corresponding vendor is displayed.
- If **vendor** *vendorname* is not specified in the **group build in** command, the vendor type is not specified.

Parameters

Parameter	Description	Value
device-type	Specifies the device type in a group.	The value is an enumerated type and case-insensitive. The following device types are supported: ● S2730S-S ● S2750-EI ● S5700-10P-LI ● S5700-EI ● S5700-HI ● S5700-P-LI ● S5700-SI ● S5700-TP-LI ● S5700-X-LI ● S5700S-LI ● S5700S-P-LI ● S5700S-X-LI ● S5710-EI ● S5710-HI ● S5710-X-LI ● S5720-EI ● S5720-HI ● S5720-LI ● S5720-SI ● S5720S-LI ● S5730-HI ● S5730-SI ● S5730S-EI ● S5731-H ● S5731-S ● S5731S-H ● S5731S-S ● S5732-H ● S5735-L ● S5735-L1 ● S5735-L-I ● S5735S-L ● S5735S-L1 ● S5735-S

Parameter	Description	Value
		- S5735S-S - S5735S-H - S5736-S - S6700-EI - S6720-EI - S6720-HI - S6720-LI - S6720-SI - S6720S-S - S6720S-LI - S6720S-SI - S6730-H - S6730S-H - S6730-S - S6730S-S - S6735-S - S9700
vendor *vendorname*	Displays the group of the device type of the specified vendor.	The value is a character string.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If clients on a network are devices of the same type, run the **group build-in** command to configure a built-in group based on the device type. This group enables these clients to download the same files, such as the system software package and patch file.

Precautions

- If a client matches both a customized group (configured using the **group custom** command) and a built-in group, it prefers the files specified in the customized group.

- A maximum of 256 groups (including both built-in groups and customized groups) can be configured on the Commander.
- If you run the **undo group build-in** command without specifying *device-type*, the command deletes all the built-in groups.

Example

Configure a built-in group and specify the device type as S5732-H.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group build-in s5732-h
[HUAWEI-easyoperation-group-build-in-s5732-h]
```

2.2.47 group custom

Function

The **group custom** command configures a customized group and displays the Easy-Operation group view on the Commander.

The **undo group custom** command deletes a customized group.

By default, no customized group is configured.

Format

group custom { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*

undo group custom [{ **mac-address** | **esn** | **ip-address** | **model** | **device-type** } [*group-name*]]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a customized group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.
mac-address	Configures a MAC address-based group.	-
esn	Configures an ESN-based group.	-
ip-address	Configures an IP address-based group.	-
model	Configures a device model-based group.	-

Parameter	Description	Value
device-type	Configures a device type-based group. This parameter applies when a new device type is not defined for built-in groups on the Commander.	-

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If multiple devices on a network need to download the same file, you can configure a group for the devices on the Commander to simplify device configuration. You can configure various customized groups on the Commander according to the deployment on your network devices.

Precautions

- A maximum of 256 groups (including both built-in groups and customized groups) can be configured on the Commander.
- Customized groups can have matching rules based on MAC address, ESN, IP address, device model, and device type, listed in descending order of priority.
- Running the **undo group custom** command without any parameters will delete all the customized groups.

Example

Configure a MAC address-based customized group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test]
```

2.2.48 license

Function

The **license** command specifies a license file to be downloaded to clients.

The **undo license** command deletes the configured license file information.

Format

license *file-name*

undo license [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file to be downloaded to clients. The file name has an extension .dat and may contain a file path.	The value is a string of 5 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to load a license file, specify the license file on the Commander.

Precautions

You can load a license file only on modular switches. When a fixed switch serves as the client, the license file cannot be loaded even after you specify the license file information.

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

NOTICE

The names of the files to be downloaded cannot be the same as system license files. Otherwise, the upgrade fails.

Example

Specify a default license file for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] license easy/test.dat
```

Specify a license file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] license license.dat
```

2.2.49 match

Function

The **match** command configures a matching rule for a group on the Commander.

The **undo match** command deletes a matching rule for a group on the Commander.

By default, a group has no matching rule.

Format

match mac-address *mac-address* [*mac-mask* | *mac-mask-length*]

match esn *esn*

match ip-address *ip-address* [*ip-mask* | *ip-mask-length*]

match model *model*

match device-type *device-type*

undo match mac-address [*mac-address* [*mac-mask* | *mac-mask-length*]]

undo match esn [*esn*]

undo match ip-address [*ip-address* [*ip-mask* | *ip-mask-length*]]

undo match model [*model*]

undo match device-type [*device-type*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Configures a MAC address-based matching rule. A group can have multiple MAC addresses or MAC address ranges specified. A client matches the group as long as it matches one of MAC addresses.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
mac-mask	Specifies the mask of a MAC address.	The value is in the H-H-H format, where each H contains four hexadecimal digits. By default, the mask is ffff-ffff-ffff.

Parameter	Description	Value
mac-mask-length	Specifies the mask length of a MAC address.	The value is an integer that ranges from 0 to 48. By default, the mask length is 48.
esn *esn*	Configures an ESN-based matching rule. A group can have multiple ESNs specified. A client matches the group as long as it matches one of ESNs.	The value is a string of 10 to 32 case-insensitive characters without spaces.
ip-address *ip-address*	Configures an IP address-based matching rule. A group can have multiple IP addresses or IP address ranges (for example 192.168.110.0) specified. A client matches the group as long as it matches one of IP addresses.	The value is in dotted decimal notation.
ip-mask	Specifies the mask of an IP address.	The value is in dotted decimal notation. By default, the mask is 255.255.255.255.
ip-mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 0 to 32. By default, the mask length is 32.
model *model*	Configures a device model-based matching rule.	The value is a string of 1 to 32 case-insensitive characters without spaces.
device-type *device-type*	Configures a device type-based matching rule.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After configuring a customized group on the Commander, configure matching rules for the group. A client can obtain the files specified in a group only when it matches a rule in the group.

Precautions

- A matching rule can be configured only in a customized group of the corresponding type. For example, the **match mac-address** *mac-address* command can only be used in a MAC address-based customized group.
- A MAC address-based, ESN-based, or IP address-based group each supports a maximum of 256 matching rules. The total number of group rules on the device cannot exceed 256.
- For groups created based on device models, only one matching rule can be defined for each group. The device model specified in a device model-based group must be the same as the actual device model. Otherwise, clients cannot match the group.
- For groups created based on device types, only one matching rule can be defined for each group. The device type specified in a device type-based group must be the same as the actual device type. Otherwise, clients cannot match the group.

Example

Configure two MAC address-based matching rules in a customized group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] match mac-address 00e0-fc12-3456
[HUAWEI-easyoperation-group-custom-test] match mac-address 00e0-fc12-3478
```

2.2.50 mngvlanid

Function

The **mngvlanid** command sets a management VLAN for a cluster.

The **undo mngvlanid** command restores the default management VLAN of a cluster.

By default, the management VLAN is VLAN 1.

Format

mngvlanid *vlan-id*

undo mngvlanid

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

Cluster view

Default Level

2: Configuration level

Usage Guidelines

On a Commander switch, if a management VLAN is changed or the management VLAN and its corresponding VLANIF interface are deleted, the cluster is automatically deleted.

If you change the ID of the management VLAN on a client switch, the client switch automatically withdraws from the cluster.

Use the management VLAN only on the cluster and do not use the VLAN for other services such as the Rapid Ring Protection Protocol (RRPP) and multicast services. Otherwise, service functions will be adversely affected.

Example

Change the management VLAN of the device to VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] mngvlanid 2
```

2.2.51 ndp enable (interface view)

Function

The **ndp enable** command enables NDP on an interface.

The **undo ndp enable** command disables NDP on an interface.

The **ndp disable** command disables NDP on an interface.

By default, NDP is enabled on an interface.

Format

ndp enable

undo ndp enable

ndp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, Eth-Trunk interface view, 100GE interface view, 40GE interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Before you enable network topology collection, run the **ndp enable** command to enable NDP on an interface.

Example

Disable NDP in the GE0/0/1 interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ndp enable
```

2.2.52 ndp enable (system view)

Function

The **ndp enable** command enables NDP globally or on an interface.

The **undo ndp enable** command disables NDP globally or on an interface.

The **ndp disable** command disables NDP globally or on an interface.

By default, NDP is enabled globally.

Format

ndp enable [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

undo ndp enable [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

ndp disable interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

ndp disable

Parameters

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-type interface-number2*]	Specifies the interface on which NDP is enabled or disabled. ● *interface-type interface-number1* indicates the type and number of the first interface. ● *interface-type interface-number2* indicates the type and number of the last interface. If you run the **ndp enable** command or the **undo ndp enable** command without specifying the interface, NDP is enabled or disabled globally.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you enable network topology collection, run the **ndp enable** command to enable NDP.

Configuration Impact

If the **ndp enable** command is run more than once, all configurations take effect.

Example

Enable NDP on the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] ndp enable interface gigabitethernet 0/0/1
```

2.2.53 ndp timer aging

Function

The **ndp timer aging** command configures an aging time for NDP entries on the receiving switch.

The **undo ndp timer aging** command restores the default aging time of NDP entries on the receiving switch.

By default, the aging time of the NDP entries on the receiving switch is 180 seconds.

Format

ndp timer aging *aging-time*

undo ndp timer aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of the NDP entries on the receiving switch.	The value is an integer that ranges from 6 to 255, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the receiving switch does not receive NDP packets from a local switch before the aging time of the NDP entry on the receiving switch expires, the receiving switch automatically deletes the neighbor entry corresponding to the local switch.

Prerequisites

NDP has been enabled on the receiving switch.

Precautions

The aging time of the NDP entries on the receiving switch must be greater than the interval for sending NDP packets.

Example

Set the aging time of NDP entries to 175 seconds.

```
<HUAWEI> system-view
[HUAWEI] ndp timer aging 175
```

2.2.54 ndp timer hello

Function

The **ndp timer hello** command configures the interval for sending NDP packets.

The **undo ndp timer hello** command restores the default interval for sending NDP packets.

By default, the interval for sending NDP packets is 60 seconds.

Format

ndp timer hello *interval*

undo ndp timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NDP packets.	The value is an integer that ranges from 5 to 254, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an interval for sending NDP packets, run the **ndp timer hello** command. The NDP interface then sends NDP packets at the specified interval.

Prerequisites

NDP has been enabled on the switch.

Precautions

The interval for sending NDP packets must be less than the aging time of NDP entries on the switch.

Example

Set the interval for sending NDP packets to 55 seconds.

```
<HUAWEI> system-view
[HUAWEI] ndp timer hello 55
```

2.2.55 ndp trunk-member enable

Function

The **ndp trunk-member enable** command enables trunk member interface-based NDP.

The **undo ndp trunk-member enable** command disables trunk member interface-based NDP.

By default, trunk member interface-based NDP is disabled.

Format

ndp trunk-member enable

undo ndp trunk-member enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a local switch connects to a remote switch through a trunk link, the local switch discovers neighbors and displays NTDP topology information based on the trunk interface. To allow the local switch to obtain link information about trunk member interfaces, run the **ndp trunk-member enable** command to enable trunk member interface-based NDP. The topology information about the trunk member interfaces can then be queried on the NMS.

Prerequisites

NDP has been globally enabled using the **ndp enable** command in the system view.

Example

Enable trunk member interface-based NDP.

```
<HUAWEI> system-view
[HUAWEI] ndp enable
[HUAWEI] ndp trunk-member enable
```

2.2.56 ntdp enable (interface view)

Function

The **ntdp enable** command enables NTDP on an interface.

The **undo ntdp enable** command disables NTDP on an interface.

The **ntdp disable** command disables NTDP on an interface.

By default, NTDP is enabled on an interface.

Format

ntdp enable

undo ntdp enable

ntdp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, Eth-Trunk interface view, 100GE interface view, 40GE interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Before you enable network topology collection, run the **ntdp enable** command to enable NTDP on an interface.

Example

Disable NTDP in the GE0/0/1 interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ntdp enable
```

2.2.57 ntdp enable (system view)

Function

The **ntdp enable** command enables NTDP globally.

The **undo ntdp enable** command disables NTDP globally.

The **ntdp disable** command disables NTDP globally.

By default, NTDP is enabled globally.

Format

ntdp enable

undo ntdp enable

ntdp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before you enable network topology collection, run the **ntdp enable** command to enable NTDP globally.

Example

Enable NTDP globally.

```
<HUAWEI> system-view
[HUAWEI] ntdp enable
```

2.2.58 ntdp explore

Function

The **ntdp explore** command enables you to manually collect topology information.

Format

ntdp explore

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to initiate the process of collecting topology information on an NTDP-capable device. The NTDP-capable device can then effectively manage and monitor devices on the network in real time to reflect the network topology changes.

You can also run the **ntdp timer** command to allow a switch to automatically collect topology information at a specified interval.

Example

Manually start topology information collection.

```
<HUAWEI> ntdp explore
```

2.2.59 ntdp hop

Function

The **ntdp hop** command sets the maximum number of hops for collecting topology information through NTDP.

The **undo ntdp hop** command restores the default maximum number of hops for collecting topology information through NTDP.

By default, the maximum number of hops is 8 for collecting topology information through NTDP.

Format

ntdp hop *max-hop-value*

undo ntdp hop

Parameters

Parameter	Description	Value
max-hop-value	Specifies the maximum number of hops for collecting topology information through NTDP.	The value is an integer that ranges from 1 to 8.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the maximum number of hops for collecting topology information through NTDP is configured, topology information about switches in the hop range can be collected, which avoids collection of infinite topology information. The larger the maximum number of hops is, the more the memory of the topology collection switch is consumed.

Prerequisites

NTDP has been enabled on the switch.

Example

Set the range for collecting topology information through NTDP to 5 hops.

```
<HUAWEI> system-view
[HUAWEI] ntdp hop 5
```

2.2.60 ntdp timer

Function

The **ntdp timer** command sets the interval for collecting topology information through NTDP.

The **undo ntdp timer** command restores the default interval for collecting topology information through NTDP.

By default, the interval for collecting topology information through NTDP is 0 minutes. That means that no topology information is periodically collected.

Format

ntdp timer *interval*

undo ntdp timer

Parameters

Parameter	Description	Value
interval	Specifies the interval for collecting topology information through NTDP.	The value is an integer that ranges from 0 to 65535, in minutes. **NOTE** The Commander collects network topology information at an interval of 5 minutes; therefore, you are advised to set the interval for collecting topology information through NTDP to less than 5 minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the interval for collecting topology information through NTDP is set, the switch collects topology information at this interval.

Prerequisites

NTDP has been enabled on the switch.

Example

Set the interval for collecting topology information to 2 minutes.

```
<HUAWEI> system-view
[HUAWEI] ntdp timer 2
```

2.2.61 ntdp timer hop-delay

Function

The **ntdp timer hop-delay** command sets a delay after which the first interface forwards NTDP topology request packets.

The **undo ntdp timer hop-delay** command restores the default delay.

By default, the first interface forwards NTDP topology request packets after a delay of 200 milliseconds.

Format

ntdp timer hop-delay *hop-delay-time*

undo ntdp timer hop-delay

Parameters

Parameter	Description	Value
hop-delay-time	Specifies the delay after which the first interface forwards NTDP topology request packets.	The value is an integer that ranges from 1 to 1000, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command takes effect only after NTDP is enabled on the switch.

Example

Set the hop delay for forwarding NTDP topology request packets to 300 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] ntdp timer hop-delay 300
```

2.2.62 ntdp timer port-delay

Function

The **ntdp timer port-delay** command sets a delay after which interfaces other than the first one forwards NTDP topology request packets.

The **undo ntdp timer port-delay** command restores the default delay.

By default, interfaces other than the first one forward NTDP topology request packets after a delay of 20 milliseconds.

Format

ntdp timer port-delay *port-delay-time*

undo ntdp timer port-delay

Parameters

Parameter	Description	Value
port-delay-time	Specifies the delay after which interfaces other than the first one forward NTDP topology request packets.	The value is an integer that ranges from 1 to 1000, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ntdp timer port-delay** command takes effect only after NTDP is enabled on the switch.

Example

Set the delay for interfaces other than the first one on the device to forward NTDP topology request packets to 40 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] ntdp timer port-delay 40
```

2.2.63 patch

Function

The **patch** command specifies a patch file to be downloaded to clients.

The **undo patch** command deletes the configured patch file information.

Format

patch *file-name*

undo patch [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a patch file to be downloaded to clients. The file name has an extension .pat and may contain a file path.	The value is a string of 5 to 48 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to load a patch file, specify the patch file on the Commander.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default patch file for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] patch easy/test.pat
```

Specify a patch file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] patch patch.pat
```

2.2.64 reset easy-operation client-database

Function

The **reset easy-operation client-database** command clears the client database on the Commander.

Format

reset easy-operation client-database

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The client database contains client information that is manually configured by the administrator and learned dynamically by the Commander. When the number of clients in the client database exceeds the limit, information about new clients cannot be added to the database. To release space in the client database, use this command to clear the client database after confirming that the manually configured client information can be deleted.

Precautions

This command deletes both manually configured client information and dynamically learned client information. Before running this command, confirm that manually configured client information can be deleted. If the Commander is enabled to learn client information, it continues adding learned client information to the client database after you run this command.

Example

Clear the client database on the Commander.

```
<HUAWEI> reset easy-operation client-database
Warning: All of the database information of client and relative replace in this
device will be cleared. Continue?[Y/N]:y
<HUAWEI>
```

2.2.65 reset easy-operation client-offline

Function

The **reset easy-operation client-offline** command clears lost state clients.

Format

reset easy-operation client-offline

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The maximum number of clients managed by the Commander depends on the device specifications. If the number of clients exceeds the upper limit, information about new clients cannot be configured on the Commander. Delete the clients in the lost state that occupy the database resources for a long time.

Precautions

- If the clients automatically join the management domain of the Commander, they can be deleted.
- If the clients are configured manually, they cannot be deleted but their status changes to unknown.
- If client replacement information is configured using the **client replace** command, client IDs in the client database will not be deleted.

Example

Delete clients in the lost state from the client database.

```
<HUAWEI> reset easy-operation client-offline
Warning: All of clients which are in the lost status will be deleted. Continue?[Y/N]:y
```

2.2.66 reset ndp statistics

Function

The **reset ndp statistics** command clears NDP packet statistics from one or all the interfaces of a device.

Format

reset ndp statistics [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-type interface-number2*]	Clears NDP packet statistics from a specified interface. ● *interface-type interface-number1* specifies the type and number of the first interface. ● *interface-type interface-number2* indicates the type and number of the last interface. When optional parameters are not specified, global statistics on NDP packets are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If you run the **reset ndp statistics** command without setting optional parameters, the NDP packet statistics of all interfaces are cleared.

Example

Delete NDP packet statistics from all the interfaces of the device.

```
<HUAWEI> reset ndp statistics
```

2.2.67 system-software

Function

The **system-software** command specifies the name and version of the system software package to be downloaded to clients.

The **undo system-software** deletes the configured software name and version.

Format

system-software *file-name* [*version*]

undo system-software [*file-name* [*version*]]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a system software package to be downloaded to clients. The file name has an extension .cc and may contain a file path.	The value is a string of 4 to 48 case-insensitive characters without spaces. The string cannot contain the following characters: ~ * : ' " ? < > | [ ] % \ /.
version	Specifies the version of a system software package, for example, V200R023C00. If the specified software version is the same as the software version running on the client, a software upgrade will not be performed for the client.	The value is a string of 11 to 32 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to upgrade their system software, specify the required system software information on the Commander.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default system software package for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] system-software easy/sV200R023C00.cc
```

Specify a system software package in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] system-software V200R023C00.cc V200R023C00
```

2.2.68 tftp-server/sftp-server/ftp-server

Function

The **tftp-server** command configures the TFTP server IP address on the Commander.

The **sftp-server** command configures the SFTP server IP address, user name, and password on the Commander.

The **ftp-server** command configures the FTP server IP address, user name, and password on the Commander.

The **undo tftp-server** command deletes the TFTP server IP address on the Commander.

The **undo sftp-server** command deletes the SFTP server IP address, user name, and password on the Commander.

The **undo ftp-server** command deletes the FTP server IP address, user name, and password on the Commander.

By default, no file server IP address, user name, or password is configured on the Commander.

Format

tftp-server *ip-address*

{ **sftp-server** | **ftp-server** } *ip-address* [**username** *username* [**password** *password*]]

undo tftp-server [*ip-address*]

undo { **sftp-server** | **ftp-server** } [*ip-address*] [**username** *username*] [**password** *password*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a file server (TFTP, SFTP, or FTP server).	The value is in dotted decimal notation.
username *username*	Specifies the user name used to log in to the SFTP or FTP server.	The value is a string of 1 to 64 case-sensitive characters.

Parameter	Description	Value
password *password*	Specifies the password used to log in to the SFTP or FTP server.	The value is a case-sensitive character string. A password in plain text contains 1 to 16 characters, and a ciphertext password contains 48 characters. In the configuration file, the password is displayed in ciphertext regardless of whether it is input in plaintext or ciphertext.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Files that need to be downloaded by clients are saved in a file server. After clients obtain information from the Commander about the necessary files, the clients download the files from the file server specified on the Commander. Therefore, the file server information must be configured on the Commander.

Precautions

- If the file server is an SFTP or FTP server and has a user name and password configured, configure the same user name and password on the Commander.
- Using an SFTP server is recommended because FTP and TFTP have security risks.
- Information about only one file server can be configured. If you run this command multiple times, only the latest configuration takes effect.
- Ensure that the files required for clients have been saved on the specified file server.

Example

Specify the IP address, user name, and password of the SFTP server on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] sftp-server 10.10.10.5 username easyoperation password YsHsjx_202206
```

Specify the TFTP server IP address on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] tftp-server 10.10.10.5
```

2.2.69 topology enable

Function

The **topology enable** command enables the Commander to collect network topology information.

The **undo topology enable** command disables the Commander from collecting network topology information.

By default, the Commander is disabled from collecting network topology information.

Format

topology enable

undo topology enable

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **topology enable** command to enable the Commander to collect network topology information every 5 minutes. Based on the collected information, you can implement zero touch device deployment and automatic faulty device replacement.

Prerequisites

NDP and NTDP have been enabled.

The interval for collecting topology information through NTDP has been set.

Example

Enable network topology information collection on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] topology enable
```

2.2.70 topology save

Function

The **topology save** command saves network topology information collected by the Commander.

Format

topology save

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network topology information collected by the Commander is saved only in the device memory. If the device restarts, the saved information is lost. You can run this command to save the collected network topology information in the flash memory and name it **ezop-topo.xml**.

Prerequisites

Network topology information collection has been enabled.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Save the current network topology information collected by the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] topology save
Warning: This command will record the information of topology. Continue? [Y/N]:y
```

2.2.71 undo group

Function

The **undo group** command deletes all groups.

Format

undo group

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

This command deletes all the groups on a switch, including built-in groups and customized groups.

Example

Delete all groups.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] undo group
Warning: All of the group configuration will be cleared. Continue?[Y/N]:y
```

2.2.72 upgrade group

Function

The **upgrade group** command starts a batch upgrade on the Commander.

Format

upgrade group [*group-name*] &<1-15>

Parameters

Parameter	Description	Value
group-name	Specifies a group name. The Commander starts a batch upgrade for all the clients that match the specified group. A maximum of 15 groups can be specified for a batch upgraded. The group names are separated by a space.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the groups, files to be loaded, and file activation mode are specified on the Commander, you can run this command to start a batch upgrade for clients.

Precautions

- If *group-name* is not specified, a batch upgrade is performed on all clients matching all the groups on the Commander.
- Before running this command, ensure that configurations of the clients have been saved.
- If a client is a stack system, its system MAC address will change after the upgrade, because the master switch changes. In this case, the client ID of the stack system is displayed as LOST on the Commander. To avoid this problem, configure the stack system MAC address to the MAC address of a member switch.

Example

Start a batch upgrade for clients matching all the groups.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] upgrade group
Warning: This command will start the upgrade process of all groups and clients i
n these groups may reboot. Ensure that configurations of the clients have been s
aved. Continue?[Y/N]:y
```

Start a batch upgrade for clients matching specified groups.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] upgrade group test1 test2 test3
Warning: This command will start the upgrade process of the group and clients in
 this group may reboot. Ensure that configurations of the clients have been save
d. Continue?[Y/N]:y
```

2.2.73 web-file

Function

The **web-file** command specifies a web page file to be downloaded to clients.

The **undo web-file** command deletes the configured web page file information.

Format

web-file *file-name*

undo web-file [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a web page file to be downloaded to clients. The file name has an extension .web.7z or .web.zip and may contain a file path.	The value is a string of 8 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to load a web page file, specify the web page file on the Commander.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default web page file for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] web-file easy/test.web.7z
```

Specify a web page file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] web-file test.web.7z
```

2.2.74 module

Function

The **module** command specifies a module file to be downloaded.

The **undo module** command deletes information about the module file to be downloaded.

Format

module *file-name*

undo module [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name (*.mod) of a module file to be loaded to clients. The file path can be specified.	The value is a string of 5 to 48 case-insensitive characters. It cannot contain spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a client needs to load a module file, the module file needs to be specified.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default module file.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] module easy/test.mod
```

Specify a module file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] module test.mod
```

2.3 USB-based Deployment Configuration Commands

2.3.1 Command Support

Only the following switch models support USB-based deployment:

S1730S-S1, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S.

2.3.2 display device usb-deployment configuration

Function

The **display device usb-deployment configuration** command displays the configuration of USB-based deployment.

Format

display device usb-deployment configuration

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the USB-based deployment configuration is completed, you can run this command to view related configuration information, including whether USB-based deployment is enabled, configuration file encryption password, HMAC key, and whether HMAC check is enabled.

Example

Display the configuration of USB-based deployment.

```
<HUAWEI> display device usb-deployment configuration
USB-deployment: disable
Config-file password: ******
HMAC: enable
Hmac-key: --
```

Table 2-19 Description of the **display device usb-deployment configuration** command output

Item	Description
USB-deployment	Whether USB-based deployment is enabled. - disable: indicates that USB-based deployment is disabled on an interface. - enable: indicates that USB-based deployment is enabled on an interface.
Config-file password	Configuration file encryption password. When no password is configured, "--" is displayed.
HMAC	Whether HMAC check is enabled. - disable: indicates that HMAC check is disabled on an interface. - enable: indicates that HMAC check is enabled on an interface.
Hmac-key	HMAC key for HMAC verification. When no HMAC key is configured, "--" is displayed.

2.3.3 set device usb-deployment disable

Function

The **set device usb-deployment disable** command disables the USB-based deployment function.

The **undo set device usb-deployment disable** command enables the USB-based deployment function.

By default, the USB-based deployment function is disabled.

Format

set device usb-deployment disable

undo set device usb-deployment disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the USB-based deployment function is disabled. However, if a device has no configuration, the USB-based deployment function is always enabled.

NOTE

On an unconfigured switch, both the configuration files for current startup and next startup are not specified. That is, the Startup saved-configuration file and Next startup saved-configuration file are NULL in the

display startup command output.

Example

Disable the USB-based deployment function.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment disable
```

Enable the USB-based deployment function.

```
<HUAWEI> system-view
[HUAWEI] undo set device usb-deployment disable
Warning: The function of USB deployment in this device will be enabled. Continue
? [Y/N]:y
```

2.3.4 set device usb-deployment config-file password

Function

The **set device usb-deployment config-file password** command configures an encryption password for the configuration file used in USB-based deployment.

The **undo set device usb-deployment config-file password** command deletes the encryption password for the configuration file used in USB-based deployment.

By default, no encryption password is configured.

NOTE

If upgrade files for USB-based deployment include a configuration file, it is recommended that you run this command to configure an encryption password for the configuration file and compress the configuration file using the configured password before saving it in the USB flash drive. This configuration improves security.

Format

set device usb-deployment config-file password *password*

undo set device usb-deployment config-file password

Parameters

Parameter	Description	Value
password	Specifies the password used for encrypting the configuration file.	The value is a string of 8 to 64 characters or a string of 48 to 108 characters. ● If the password is in plain text, it is a string of 8 to 64 case-sensitive characters and must be a combination of at least two of the following: letters, digits, and special characters. ● If the password is in cipher text, it is a string of 48 to 108 characters. The password is displayed in cipher text in the configuration file regardless of whether you enter it in plain or cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

If a password is configured using the **set device usb-deployment config-file password** *password* command, you need to compress and encrypt the configuration file (if any) with this password and save the compressed file to a specified directory in the USB flash drive. The device cannot compress a .zip configuration file. If such a configuration file is used, decompress the file, use the configured password to compress it, and save it in the USB flash drive.

A user with a level lower than the management level cannot query the password configured using this command. If this user query the configuration file, the password is displayed as asterisks (******).

Example

Set the encryption password for the configuration file used in USB-based deployment to **Pwd123456**.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment config-file password Pwd123456
```

2.3.5 set device usb-deployment hmac-key

Function

The **set device usb-deployment hmac-key** command configures an HMAC key for HMAC verification during USB-based deployment.

The **undo set device usb-deployment hmac-key** command deletes the HMAC key used for HMAC verification during USB-based deployment.

By default, no HMAC key is configured for HMAC verification.

Format

set device usb-deployment hmac-key *hmac-key*

undo set device usb-deployment hmac-key

Parameters

Parameter	Description	Value
hmac-key	Specifies an HMAC key for HMAC verification during USB-based deployment.	The value is a string of 8 to 64 or 68 to 108 characters. ● A cleartext key is a string of 8 to 64 case-sensitive characters. It is recommended that the key be a combination of at least two of the following: uppercase letters A to Z, lowercase letters a to z, digits, and special characters. ● A ciphertext key is a string of 68 to 108 characters. In the configuration file, a password is displayed in cipher text regardless of whether it is entered in clear text or cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

If upgrade files include a configuration file, you can enable HMAC verification to ensure validity of the configuration file to be loaded. After the **set device usb-deployment hmac** command is run to enable HMAC verification for the configuration file during USB-based deployment, run the **set device usb-deployment hmac-key** command to configure an HMAC key for HMAC verification so that the device calculates the HMAC value of the configuration file and then compares the value with the HMAC field value in the index file. If the two values are the same, the configuration file is valid and loaded to the device for USB-based deployment. If the two values are different, the configuration file is invalid and cannot be loaded for USB-based deployment.

A user at a level lower than the management level cannot check the HMAC key configured using this command. If this user checks the configuration file, the HMAC key is displayed as ******.

Example

Configure an HMAC key for HMAC verification during USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment hmac-key huawei@123456852369741236553424654643213
```

2.3.6 set device usb-deployment hmac

Function

The **set device usb-deployment hmac** command enables hashed message authentication code (HMAC) check for the configuration file used for USB-based deployment.

The **undo set device usb-deployment hmac** command disables HMAC check for the configuration file used for USB-based deployment.

By default, HMAC check is disabled.

NOTE

If upgrade files for USB-based deployment include a configuration file, it is recommended that you enable HMAC check to improve security of the configuration file.

Format

set device usb-deployment hmac

undo set device usb-deployment hmac

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Prerequisites

Before enabling the HMAC check function, run the **set device usb-deployment config-file password** command to configure an encryption password for the configuration file used for USB-based deployment.

Applications

If upgrade files for USB-based deployment include a configuration file, you can enable HMAC check to ensure validity of the configuration file to be loaded. After HMAC check is enabled on a device, the device uses the password configured by the **set device usb-deployment config-file password** command to calculate the HMAC for the configuration file, and compares the calculated value with the HMAC field value in the index file. If the two values are the same, the configuration file is considered valid and loaded to the device. If not, the configuration file is considered invalid and cannot be loaded.

Example

Enable HMAC check for the configuration file used for USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment hmac
```

2.3.7 set device usb-deployment password

Function

The **set device usb-deployment password** command sets an authentication password for USB-based deployment.

The **undo set device usb-deployment password** command deletes the authentication password for USB-based deployment.

Format

set device usb-deployment password cipher *password*

set device usb-deployment password *password*

undo set device usb-deployment password

Parameters

Parameter	Description	Value
cipher *password*	Specifies the authentication password for USB-based deployment.	The value is a cipher text string of 8 to 16 or 68 characters.
password	Specifies the authentication password for USB-based deployment.	The value is a cipher text string of 8 to 16 or 68 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

A user with a level lower than the management level cannot query the password configured using this command. If this user query the configuration file, the password is displayed as asterisks (******).

Example

Delete the authentication password for USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] undo set device usb-deployment password
```

2.4 First Login Commands

2.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.4.2 clock datetime

Function

The **clock datetime** command sets the current date and time on a switch.

Format

clock datetime *HH:MM:SS YYYY-MM-DD*

Parameters

Parameter	Description	Value
HH:MM:SS	Specifies the current time on a switch.	*HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. *SS* specifies the second, which is an integer ranging from 0 to 59.
YYYY-MM-DD	Specifies the current date (year, month, and day) on the switch.	*YYYY* specifies the year, which is an integer ranging from 2000 to 2037. *MM* specifies the month, which is an integer ranging from 1 to 12. *DD* specifies the day, which is an integer ranging from 1 to 31.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the scenario where accurate absolute time is required, the current date and time must be set on a switch.

Prerequisite

The time zone and daylight saving time have been configured using the **clock timezone** and **clock daylight-saving-time** commands. If the time zone and daylight saving time are not configured, the **clock datetime** command sets a UTC time.

Precautions

- The specified time must be in 24-hour format. If you do not specify *MM* and *SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- The specified year must be a four-digit number and the specified month and day can be a one-digit number. For example, when you enter 2012-9-1, the time is 2012-09-01.
- If the device is configured to restart at a specified time and if the system time is changed to be more than 10 minutes later than the specified restart time, the scheduled restart function will be disabled.

NOTE

The valid time range is based on the UTC, and this command sets the local time. If the DST or time zone is specified in the current environment, the system automatically converts the local time to the UTC.

For example, if you set the time zone to GMT+8 and the local date to 2000-1-1, the UTC converted equals to the local date minus eight hours, which is 1999-12-31. However, the valid date range is 2000 to 2037. As a result, the validity check fails, and date setting fails.

Example

Set the current time and date of the system to 0:1:2 2012-01-01.

```
<HUAWEI> clock datetime 0:1:2 2012-01-01
```

2.4.3 clock daylight-saving-time

Function

The **clock daylight-saving-time** command sets the name, start time, and end time of the daylight saving time (DST).

The **undo clock daylight-saving-time** command cancels the DST settings.

By default, DST is not used.

Format

clock daylight-saving-time *time-zone-name* **one-year** *start-time start-date end-time end-date offset*

clock daylight-saving-time *time-zone-name* **repeating** *start-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date1* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date1* } *offset* [*start-year* [*end-year*]]

undo clock daylight-saving-time

Parameters

Parameter	Description	Value
time-zone-name	Specifies the name of the DST zone.	The value is a string of 1 to 32 case-sensitive characters without spaces.
one-year	Specifies absolute DST.	-
repeating	Specifies periodic DST.	-
start-time	Specifies the DST start time.	The start time is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, DST starts on the hour. You must enter at least one digit to specify *HH*. For example, when you enter 0, the start time is 00:00.
start-date	Specifies the DST start date.	The start date is in the format *YYYY-MM-DD*. *YYYY* specifies the year, which is an integer ranging from 2000 to 2099, *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.

Parameter	Description	Value
end-time	Specifies the DST end time.	The end time is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, DST starts on the hour. You must enter at least one digit to specify *HH*. For example, when you enter 0, the start time is 00:00.
end-date	Specifies the DST end date.	The end date is in the format *YYYY-MM-DD*. *YYYY* specifies the year, which is an integer ranging from 2000 to 2099, *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
first	Specifies the first workday in a month.	-
second	Specifies the second workday in a month.	-
third	Specifies the third workday in a month.	-
fourth	indicates the fourth workday in a month.	-
last	Specifies the last workday in a month.	-
weekday	Specifies a day of the week.	The value is **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, or **Sun**.
month	Specifies a month.	The value is **Jan**, **Feb**, **Mar**, **Apr**, **May**, **Jun**, **Jul**, **Aug**, **Sep**, **Oct**, **Nov**, or **Dec**.

Parameter	Description	Value
start-date1	Specifies the DST start date.	The start date is in the format *MM-DD*. *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
end-date1	Specifies the DST end date.	The end date is in the format *MM-DD*. *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
offset	Specifies the DST offset.	The offset is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 2. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, the offset is the specified hours. You must enter at least one digit to specify *HH*. The offset should be shorter than or equal to 2 hours.
start-year	Specifies the start year.	The start year is in the format *YYYY* and ranges from 2000 to 2099.
end-year	Specifies the end year.	The end year is in the format *YYYY* and ranges from 2000 to 2099.

Views

User view, system view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

DST, also referred to as summer time, is a convention intended to save resources. In high latitude areas, sunrise time is earlier during summer than it is during winter. To reduce use of incandescent lighting in the evenings and save energy, clocks are adjusted forward one hour.

Users can customize the DST zone according to their countries' or regions' convention. In addition, users can set how far ahead clocks are adjusted forward, usually an hour. With DST enabled, when it is time to start DST, the system time is adjusted according to the user-specified DST. When it is time to end DST, the system time automatically returns to the original time.

Configuration Impact

To configure DST, note the following:

- The time in logs and debugging information uses the local time adjusted based on the time zone and the configured DST.
- The time in the output of the **display** commands uses the local time adjusted based on the time zone and the configured DST.

To remove configurations for DST, note the following:

- If DST has already taken effect when you remove the configurations, the device will adjust its clock by subtracting the value of the *offset* parameter from the current time.
- If DST has not taken effect, removing the configurations will not affect the system time.

Precautions

- The DST is configured in the summer. The DST duration ranges from one day to one year.
- You can configure the start time and end time for periodic DST in one of the following modes: date+date, week+week, date+week, and week+date.
- When you run the **clock daylight-saving-time** command in either the user or system view, the configuration files are both generated in the system view. You are advised to run this command in the system view.

Example

Set periodic DST.

```
<HUAWEI> system-view
[HUAWEI] clock daylight-saving-time bj repeating 0 first sun jan 0 first sun apr 2 2009 2009
```

Set periodic DST by day.

```
<HUAWEI> system-view
[HUAWEI] clock daylight-saving-time bj repeating 12:11 1-1 1:0 3-4 1
```

Set absolute DST.

```
<HUAWEI> system-view
[HUAWEI] clock daylight-saving-time bj one-year 12:11 2010-10-2 1:00 2010-11-4 1
```

2.4.4 clock timezone

Function

The **clock timezone** command sets the local time zone.

The **undo clock timezone** command deletes the local time zone.

By default, the system uses the Coordinated Universal Time (UTC) time zone.

Format

clock timezone *time-zone-name* { **add** | **minus** } *offset*

undo clock timezone

Parameters

Parameter	Description	Value
time-zone-name	Specifies the time zone name.	The name is a string of 1 to 32 case-sensitive characters without spaces.
add	Specifies the offset from the UTC for the time zone specified by *time-zone-name*. That is, the sum of the default UTC time zone and *offset* is equal to the time zone specified by *time-zone-name*.	-
minus	Specifies the offset from the UTC for the time zone specified by *time-zone-name*. That is, the remainder obtained by subtracting *offset* from the default UTC time zone is equal to the time zone specified by *time-zone-name*.	-

Parameter	Description	Value

offset	Specifies the offset from the UTC.	Format: HH:MM:SS
		- *HH* specifies the hour.
		  – If the local time is earlier than the UTC, the value is an integer ranging from 0 to 14.
		  – If the local time is later than the UTC, the value is an integer ranging from 0 to 12.
		- *MM* and *SS* specify the minute and second respectively, and both range from 0 to 59.
		- When *HH* is set to the maximum value, the *MM* and *SS* values must be 0.

Views

User view, System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system clock is the time indicated by the system timestamp. Because the rules governing local time differ in different regions, the system clock can be configured to comply with the rules of any given region.

System clock = UTC + Time zone offset + DST offset

To ensure normal communication between devices, set an accurate system clock. You can run the **clock timezone** and **clock daylight-saving-time** commands to set the time zone and DST offsets.

Configuration Impact

System time adjustment may affect the timing restart function. If you must adjust the system time after the timing restart function is enabled, pay attention to the impact of system time adjustment on the timing restart function:

- If the system time is changed to less than 10 minutes after the scheduled restart time, the system restarts immediately.
- If the system time is changed to 10 minutes or more after the scheduled restart time, the timing restart function is disabled.
- If the system time is changed to 720 hours earlier than the scheduled restart time, the timing restart function is disabled.

Precautions

- The specified time must be in 24-hour format. If you do not specify *MM* and *SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- After configuring the local time zone, run the **display clock** command to view the configuration. The time in logs and diagnostic information uses the local time adjusted based on the time zone and DST.
- When you run the **clock timezone** command in either the user or system view, the configuration files are both generated in the system view. You are advised to run this command in the system view.
- Executing the **clock timezone** command takes about 3 seconds.

Example

Set the local time zone name for Beijing China to BJ.

If the default UTC is London time 2012-12-01 00:00:00, Beijing time is London time plus 08:00 because the offset from UTC is 8 hours.

```
<HUAWEI> clock datetime 0:0:0 2012-12-01
<HUAWEI> system-view
[HUAWEI] clock timezone BJ add 08:00:00
```

2.4.5 display calendar

Function

The **display calendar** command displays the calendar of the current month or a specified month in a specified year.

Format

display calendar [*month* [*year*]]

Parameters

Parameter	Description	Value
month	Specifies the month for which the calendar is displayed.	The value is a character string. The values and their meanings are as follows: - **Jan**: January - **Feb**: February - **Mar**: March - **Apr**: April - **May**: May - **Jun**: June - **Jul**: July - **Aug**: August - **Sep**: September - **Oct**: October - **Nov**: November - **Dec**: December
year	Specifies the year for which the calendar is displayed.	The value is an integer that ranges from 2000 to 2099.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the current date and time on the switch using the **clock datetime** command, you can run the **display calendar** command to view calendar information.

If no month or year is specified, the calendar of the current month is displayed by default. If only month but not year is specified, the calendar of the specified month in the current year is displayed.

Example

Display the calendar of the current month.

```
<HUAWEI> display calendar
     November    2012
 Sun Mon Tue Wed Thu Fri Sat
                  1   2   3
  4   5   6   7   8   9  10
 11  12  13  14  15  16  17
```

```
 18  19  20  21  22  23  24
 25  26  27  28  29  30
Today is 16 November 2012.
```

Display the calendar of May 2008.

```
<HUAWEI> display calendar May 2008
         May    2008
 Sun Mon Tue Wed Thu Fri Sat
                       1   2   3
   4   5   6   7   8   9  10
  11  12  13  14  15  16  17
  18  19  20  21  22  23  24
  25  26  27  28  29  30  31
Today is 16 November 2012.
```

Table 2-20 Description of the **display calendar** command output

Item	Description
Sun	Sunday
Mon	Monday
Tue	Tuesday
Wed	Wednesday
Thu	Thursday
Fri	Friday
Sat	Saturday

2.4.6 display clock

Function

The **display clock** command displays the current date and clock setting.

Format

display clock [**utc**]

Parameters

Parameter	Description	Value
utc	Indicates that the clock is adjusted to the Coordinated Universal Time (UTC).	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display clock** command to view the system date and clock setting and adjust the setting if necessary.

Precautions

The system clock is set using the **clock datetime**, **clock timezone**, and **clock daylight-saving-time** commands.

- If the three commands are not used, the original system clock is displayed after you run the **display clock** command.
- You can use any combination of the three commands to configure the system time. **Table 2-21** lists the formats of the configured time.

The table assumes that the original system time is 08:00:00 on January 1, 2010.

- 1: indicates that the **clock datetime** command is used, in which the current time and date is *date-time*.
- 2: indicates that the **clock timezone** command is used, in which the time zone parameter is set and the time offset is *zone-offset*.
- 3: indicates that the **clock daylight-saving-time** command is used, in which the DST parameters are set and the time offset is *offset*.
- [1]: indicates that the **clock datetime** command is optional.

Table 2-21 System clock setting examples

Action	System Time Configuration	Example
1	*date-time*	Command: **clock datetime 8:0:0 2011-11-12** Configured system time: 2011-11-12 08:00:06 Saturday Time Zone(DefaultZoneName) : UTC
2	Original system time ± *zone-offset*	Command: **clock timezone BJ add 8** Configured system time: 2010-01-01 16:00:30+08:00 Friday Time Zone(BJ) : UTC+08:00
1, 2	*date-time* ± *zone-offset*	Commands: **clock datetime 8:0:0 2011-11-12** and **clock timezone BJ add 8** Configured system time: 2011-11-12 16:00:10+08:00 Saturday Time Zone(BJ) : UTC+08:00

Action	System Time Configuration	Example
[1], 2, 1	*date-time*	Commands: **clock timezone NJ add 8** and **clock datetime 9:0:0 2011-11-12** Configured system time:
3	If the original system time is not in the DST segment, the original system time is displayed.	Command: **clock daylight-saving-time BJ one-year 6:0 2011-8-1 6:0 2011-10-01 1** Configured system time:
	If the original system time is in the DST segment, the configured system time is the original system time plus *offset*.	Command: **clock daylight-saving-time BJ one-year 6:0 2010-1-1 6:0 2010-9-1 2** Configured system time:
1, 3	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock datetime 9:0:0 2011-11-12** and **clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1** Configured system time:

[1], 2, 1

```
2011-11-12 09:00:07+08:00
Saturday
Time Zone(NJ) : UTC+08:00
```

3

```
2010-01-01 08:00:16
Friday
Time Zone(DefaultZoneName) : UTC
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2011
        End year    : 2011
        Start time  : 08-01 06:00:00
        End time    : 10-01 06:00:00
        Saving time : 01:00:00
```

```
2010-01-01 10:00:26+02:00 DST
Friday
Time Zone(BJ) : UTC
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2010
        End year    : 2010
        Start time  : 01-01 06:00:00
        End time    : 09-01 06:00:00
        Saving time : 02:00:00
```

1, 3

```
2011-11-12 09:00:26
Saturday
Time Zone(DefaultZoneName) : UTC
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2012
        End year    : 2012
        Start time  : 08-01 06:00:00
        End time    : 10-01 06:00:00
        Saving time : 01:00:00
```

Action	System Time Configuration	Example
	If *date-time* is in the DST segment, the configured system time is *date-time* +*offset*.	Commands: **clock datetime 9:0:0 2011-11-12** and **clock daylight-saving-time BJ one-year 9:0 2011-11-12 6:0 2011-12-01 2** Configured system time:

```
2011-11-12 11:02:21 DST
Saturday
Time Zone(BJ) : UTC
Daylight saving time :
        Name         : BJ
        Repeat mode : one-year
        Start year  : 2011
        End year    : 2011
        Start time  : 11-12 09:00:00
        End time    : 12-01 06:00:00
        Saving time : 02:00:00
```

Action	System Time Configuration	Example
[1], 3, 1	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1** and **clock datetime 9:0 2011-11-12** Configured system time:

```
2011-11-12 09:00:02
Saturday
Time Zone(DefaultZoneName) : UTC
Daylight saving time :
        Name         : BJ
        Repeat mode : one-year
        Start year  : 2012
        End year    : 2012
        Start time  : 08-01 06:00:00
        End time    : 10-01 06:00:00
        Saving time : 01:00:00
```

Action	System Time Configuration	Example
	If *date-time* is in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2** and **clock datetime 3:0 2011-1-1** Configured system time:

```
2011-01-01 03:00:19 DST
Saturday
Time Zone(BJ) : UTC
Daylight saving time :
        Name         : BJ
        Repeat mode : one-year
        Start year  : 2011
        End year    : 2011
        Start time  : 01-01 01:00:00
        End time    : 09-01 01:00:00
        Saving time : 02:00:00
```

Action	System Time Configuration	Example
2, 3 or 3, 2	If the result of original system time ± *zone-offset* is not in the DST segment, the configured system time is equal to the original system time ± *zone-offset*.	Commands: **clock timezone BJ add 8** and **clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2** Configured system time:
	If the result of original system time ± *zone-offset* is in the DST segment, the configured system time is equal to the original system time ± *zone-offset* ± *offset*.	Commands: **clock daylight-saving-time BJ one-year 1:0 2010-1-1 1:0 2010-9-1 2** and **clock timezone BJ add 8** Configured system time:
1, 2, 3 or 1, 3, 2	If the value of *date-time* ± *zone-offset* is not in the DST segment, the configured system time is equal to *date-time* ± *zone-offset*.	Commands: **clock datetime 8:0:0 2011-11-12**, **clock timezone BJ add 8**, and **clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2** Configured system time:

```
2010-01-01 16:01:29+08:00
Friday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2011
        End year    : 2011
        Start time  : 01-01 06:00:00
        End time    : 09-01 06:00:00
        Saving time : 02:00:00
```

```
2010-01-01 18:05:31+08:00 DST
Friday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2010
        End year    : 2010
        Start time  : 01-01 01:00:00
        End time    : 09-01 01:00:00
        Saving time : 02:00:00
```

```
2011-11-12 08:01:40+08:00
Saturday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2012
        End year    : 2012
        Start time  : 01-01 06:00:00
        End time    : 09-01 06:00:00
        Saving time : 02:00:00
```

Action	System Time Configuration	Example
	If the value of *date-time* ± *zone-offset* is in the DST segment, the configured system time is equal to *date-time* ± *zone-offset* + *offset*.	Commands: **clock datetime 8:0:0 2011-1-1**, **clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2** and **clock timezone BJ add 8** Configured system time:

```
2011-01-01 10:00:43+08:00 DST
Saturday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2011
        End year    : 2011
        Start time  : 01-01 06:00:00
        End time    : 09-01 06:00:00
        Saving time : 02:00:00
```

Action	System Time Configuration	Example
[1], 2, 3, 1 or [1], 3, 2, 1	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2**, **clock timezone BJ add 8**, and **clock datetime 8:0:0 2011-11-12** Configured system time:

```
2011-11-12 08:00:03+08:00
Saturday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2012
        End year    : 2012
        Start time  : 01-01 06:00:00
        End time    : 09-01 06:00:00
        Saving time : 02:00:00
```

Action	System Time Configuration	Example
	If *date-time* is in the DST segment, the configured system time is *date-time*.	Commands: **clock timezone BJ add 8**, **clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2**, and **clock datetime 3:0:0 2011-1-1** Configured system time:

```
2011-01-01 03:00:03+08:00 DST
Saturday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2011
        End year    : 2011
        Start time  : 01-01 01:00:00
        End time    : 09-01 01:00:00
        Saving time : 02:00:00
```

Example

Display the current system date and time.

```
<HUAWEI> display clock
```

```
2013-02-07 15:34:02+08:00
Thursday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2013
        End year    : 2013
        Start time  : 06-01 00:00:00
        End time    : 09-01 00:00:00
        Saving time : 02:00:00
```

Display the UTC of the system.

```
<HUAWEI> display clock utc
2012-04-23 15:11:20
Monday
```

Table 2-22 Description of the **display clock** command output

Item	Description
Time Zone	Time zone.
Daylight saving time	DST.
Name	DST name.
Repeat mode	DST mode. ● one-year: absolute DST ● repeat: periodic DST
Start year	Year from which DST starts.
End year	Year when DST ends.
Start time	Time when DST starts.
End time	Time when DST ends.
Saving time	Storage time.

2.4.7 display sys-netid

Function

The **display sys-netid** command displays the name of a network element (NE).

Format

display sys-netid

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the NE name. If the NE name is not set on the device, the system displays a message indicating that the NE name is not set.

Example

Display the NE name.

```
<HUAWEI> display sys-netid
Info: The NetID is: huawei-1234567890
```

2.4.8 sysname

Function

The **sysname** command sets a device host name.

The **undo sysname** command restores the default device host name.

By default, the device host name is HUAWEI.

Format

sysname *host-name*

undo sysname

Parameters

Parameter	Description	Value
host-name	Specifies a host name.	The value is a string of 1 to 246 case-sensitive characters. It can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Changing the host name of a device affects the CLI prompt. For example, if the host name of the device is HUAWEI, the prompt of the user view is <HUAWEI>.

Example

Set the host name of the device to HUAWEIA.

```
<HUAWEI> system-view
[HUAWEI] sysname HUAWEIA
[HUAWEIA]
```

2.4.9 sys-netid

Function

The **sys-netid** command sets a name for a network element (NE).

The **undo sys-netid** command deletes the NE name.

By default, no NE name is set.

Format

sys-netid *netid*

undo sys-netid

Parameters

Parameter	Description	Value
netid	Specifies the NE name.	The value is a string of 16 to 240 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network management tool needs to obtain the name of an NE, you can run the **sys-netid** command to set the NE name. The NE name is the same as that obtained from the MIB object hwEntitySystemNetID.

Precautions

If you run the **sys-netid** command multiple times, only the latest configuration takes effect.

Example

Set the NE name.

```
<HUAWEI> system-view
[HUAWEI] sys-netid huawei-1234567890
Info: NetID set successfully.
Info: New NetID is: huawei-1234567890.
```

2.5 UI Configuration Commands

2.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.5.2 acl (user interface view)

Function

The **acl** command uses an ACL to restrict login rights of users on a terminal.

The **undo acl** command cancels the configuration.

By default, login rights are not restricted.

Format

acl [**ipv6**] { *acl-number* | *acl-name* } { **inbound** | **outbound** }

undo acl [**ipv6**] [*acl-number* | *acl-name*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv6	Indicates an ACL6 number.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999. ● 2000-2999: restricts the source address using the basic ACL. ● 3000-3999: restricts the source and destination addresses using the advanced ACL.

Parameter	Description	Value
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter. **NOTE** When the number of the ACL configured using the **acl name** command ranges from 2000 to 3999, the *acl-name* parameter can be successfully delivered using the **acl (user interface view)** command. ● 2000-2999: restricts the source address using the basic ACL. ● 3000-3999: restricts the source and destination addresses using the advanced ACL.
inbound	Restricts users with an address or within an address segment from logging in to a device.	-
outbound	Restricts users who have logged in to a device from logging in to other devices.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command restricts the login rights of a user interface based on the source IP address, destination IP address, source port, destination port, VPN instance, or packets whose protocol type is TCP. You can use this command to permit or deny access to a destination or from a source.

Prerequisites

An ACL has been configured using the **acl (system view)** and **rule (basic ACL view)** commands or using **acl (system view)** and **rule (advanced ACL view)** commands.

If no rule is configured, login rights on the user interface are not restricted when the **acl** command is run.

Precautions

After the configurations of the ACL take effect, all users on the user interface are restricted by the ACL.

You can configure all of the following ACL types: IPv4 inbound, IPv4 outbound, IPv6 inbound, and IPv6 outbound on a user interface. Only one ACL of each type can be configured on a user interface, and only the latest configuration of an ACL takes effect.

Console interface does not support this command.

Example

Restrict the Telnet login rights on user interface VTY 0 using an ACL.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule deny tcp destination-port eq telnet
[HUAWEI-acl-adv-3001] quit
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] acl 3001 outbound
```

Remove the restriction on the Telnet login rights on user interface VTY 0.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] undo acl outbound
```

2.5.3 authentication-mode (user interface view)

Function

The **authentication-mode** command configures an authentication mode for accessing the user interface.

The **undo authentication-mode** command deletes the authentication mode for accessing the user interface.

The default authentication mode for console port login users is password authentication. By default, the authentication mode for users using other login modes is not configured using this command. You must configure an authentication mode for accessing the user interface; otherwise, users cannot log in to the device.

Format

authentication-mode { **aaa** | **password** }

undo authentication-mode

Parameters

Parameter	Description	Value
aaa	Indicates the AAA authentication mode.	-
password	Indicates the password authentication mode.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After entering the default user name and password, you must reconfigure the login password and then can log in to the device. After logging in to the device, you can run this command to reconfigure the authentication mode.

Before Telnet or SSH users log in to the device using VTY user interface, they must run the **authentication-mode** command to configure the authentication mode.

Precautions

To ensure that users can log in to the device successfully, configure an authentication mode.

Before setting the Telnet login authentication mode to password authentication, run the **protocol inbound** { **all** | **telnet** } command to configure the VTY user interface to support Telnet. Otherwise, the user authentication mode configuration will fail.

NOTICE

The **none** parameter is not contained in the command. To specify this parameter, install the empty password authentication plug-in. This parameter, however, brings security risks, and the **aaa** or **password** parameter is recommended.

You can search for **Plug-in Usage Guide** at the Huawei technical support website (**Enterprise Network** or **Carrier**), and choose the desired plug-in usage guide based on the switch model and software version. If you do not have permission to access the website, contact technical support personnel.

- After you set the authentication mode to **password**, run the **set authentication password** command to configure an authentication password. Keep the password safe. You need to enter the password when logging in to the device. The levels of commands accessible to a user depend on the level configured for the user interface to which the user logs in.
- After login, the level of the commands the user can run depends on the level of the local user specified in AAA configuration.
- When you run the **undo authentication-mode** command to delete the authentication mode, the device asks you whether to delete the authentication mode.
- In V200R009 and earlier versions, the console port uses non-authentication by default. From V200R010 to V200R019, the console port uses AAA authentication by default. In V200R020C00 and later versions, the console port uses password authentication by default.

- If a device runs a version earlier than V200R010C00 and the authentication mode for accessing the user interface is not configured using this command, the default authentication mode is still non-authentication after the system software is upgraded to V200R010C00 or a later version. The system asks you whether to change the password. To ensure the console port usage security, it is recommended that you configure the login password or set the authentication mode to AAA or password authentication after logging in to the device.
- If a device runs a version earlier than V200R010C00 and the authentication mode for accessing the user interface has been configured using this command, the default authentication mode is still the originally configured authentication mode after the system software is upgraded to V200R010C00 or a later version.

Example

Configure password authentication for users to access the user interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] protocol inbound all
[HUAWEI-ui-vty0] authentication-mode password
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
[HUAWEI-ui-vty0] set authentication password cipher YsHsjx_202206
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
```

2.5.4 auto-execute command

Function

The **auto-execute command** command configures auto-run commands.

The **undo auto-execute command** command cancels auto-run commands.

By default, the auto-run function is disabled.

Format

auto-execute command *command*

undo auto-execute command

Parameters

Parameter	Description	Value
command	Specifies an auto-run command.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **auto-execute command** command to make a device run a command automatically on the corresponding user interface.

You can run the **auto-execute command** command to enable automatic execution of the **Telnet** command.

Precautions

- The **auto-execute command** command applies to the VTY user interface.
- When you log in to a device, the device automatically runs the commands that are configured by the **auto-execute command** command. After command execution, the user's terminal disconnects from the device.
- Before saving the configuration of the **auto-execute command** command, ensure that you can log in to the device to cancel the command configuration.
- If you use the **auto-execute command** command, you cannot configure the device in the user interface view. Therefore, use this command with caution.

Example

Configure the **telnet 10.110.100.1** command to automatically run after a user logs in to the device using the VTY0 interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] auto-execute command telnet 10.110.100.1
Warning: The system will not be configured through ui-vty0.
Continue? [Y/N]: y
```

2.5.5 databits

Function

The **databits** command sets the number of data bits of the user interface.

The **undo databits** command restores the default number of data bits.

By default, the user interface has 8 data bits.

Format

databits { **5** | **6** | **7** | **8** }

undo databits

Parameters

Parameter	Description	Value
5	Indicates that the number of data bits is 5.	-
6	Indicates that the number of data bits is 6.	-
7	Indicates that the number of data bits is 7.	-
8	Indicates that the number of data bits is 8.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Use this command only when necessary. If the number of data bits of a device's user interface is changed, ensure that the same number of data bits is set on the HyperTerminal used for login.

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the number of data bits to 5.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] databits 5
```

2.5.6 display user-interface

Function

The **display user-interface** command displays information about a user interface.

Format

display user-interface [*ui-type ui-number1* | *ui-number*] [**summary**]

Parameters

Parameter	Description	Value
ui-type	Displays information about a specified user interface.	The value can be Console or VTY.

Parameter	Description	Value
ui-number1	Displays information about a user interface with a specified relative number.	The minimum value is 0. The maximum value is the number of user interfaces that the system supports minus 1.
ui-number	Displays information about a user interface with a specified absolute number.	The value is an integer ranging from 0 to 54, 67 to 83. The value varies according to the device type.
summary	Displays the summary of a user interface.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To check detailed configuration information about all user interfaces or a specified user interface, run the **display user-interface** command.

Example

Display detailed information about the user interface with the absolute number 0.

```
<HUAWEI> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi      Auth  Int
  0    CON 0    9600       -     3     -                P     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
     A: Authenticate use AAA.      N: Current UI need not authentication.      P: Authenticate use current
UI's password.
  Int  : The physical location of UIs.
```

Display detailed information about all user interfaces.

```
<HUAWEI> display user-interface
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi       Auth  Int
  0    CON 0    9600          -     3     -              P     -
+ 34   VTY 0               -     3     3            A     -
+ 35   VTY 1               -     1     2            A     -
+ 36   VTY 2               -     3     2            A     -
  37   VTY 3              -     1     -            P     -
  38   VTY 4              -     1     -            A     -
...
UI(s) not in async mode -or- with no hardware support:
```

```
1-32
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.       N: Current UI need not authentication.       P: Authenticate use current
UI's password.
  Int  : The physical location of UIs.
```

Table 2-23 Description of the **display user-interface** command output

Parameter	Description
+	Active user interface.
F	Active user interface in asynchronous mode.
Idx	Absolute number of a user interface.
Type	Type and relative number of a user interface.
Tx/Rx	Data transfer rate of the user interface.
Modem	Type of the modem.
Privi	Authority configured on a user interface.
ActualPrivi	Actual permission of a user interface. In AAA authentication mode, the level of a local user in AAA configuration is the actual permission.
Auth	Authentication mode on a user interface.
Int	User interface.
A	AAA authentication.
N	No authentication on the current user interface.
P	Password authentication.

2.5.7 display user-interface maximum-vty

Function

The **display user-interface maximum-vty** command displays the maximum number of VTY users.

Format

display user-interface maximum-vty

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To check the maximum number of users who are allowed to log in to a device using Telnet or SSH, run the **display user-interface maximum-vty** command. By default, the maximum number of total Telnet and SSH users is five.

Example

Display the maximum number of VTY users.

```
<HUAWEI> display user-interface maximum-vty
Maximum of VTY user : 5
```

Table 2-24 Description of the **display user-interface maximum-vty** command output

Parameter	Description
Maximum of VTY user	Maximum number of VTY users. The maximum number of VTY users can be configured using the **user-interface maximum-vty** command.

2.5.8 display users

Function

The **display users** command displays login information of each user interface.

Format

display users [**all**]

Parameters

Parameter	Description	Value
all	Displays information about all users who log in to a device through user interfaces, including information about user interfaces that are not connected. If the **all** parameter is not used, the command displays information only about user interfaces that have been connected.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about users who are connected to a device. The information includes the user name, IP address, and authentication and authorization information.

NOTE

The user with a level of 0, 1, or 2 can only view related information about users of the same or a lower level. A user with a level of 3 or above can view login information of all users.

Example

Display information about users who log in to the device through user interfaces.

```
<HUAWEI> display users
  User-Intf   Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  34 VTY 0   00:00:00  TEL    10.164.6.10           pass            no
  Username : user1
+ 35 VTY 1   00:00:00  TEL    10.164.6.15           pass            no
  Username : user2
```

Table 2-25 Description of the **display users** command output

Item	Description
+	User interface in use.
User-Intf	The number in the first column under **User-Intf** indicates the absolute number of the user interface, and the number in the second column under **User-Intf** indicates the relative number of the user interface. User Interface type. ● Console: Users who log in through the console port ● VTY: Users who log in using VTY ● LTT: User logs in stack system through the non-master switch console port ● WEB: Users who log in through Web system
Delay	Interval from the user's latest input on the login page to the current time, in seconds.

Item	Description
Type	Connection type. ● Console ● Telnet ● SSH ● Web
Network Address	IP address of the login user.
Username	User name for logging in to the device. If the user name is not specified, **Unspecified** is displayed.
AuthenStatus	Whether the authentication succeeds.
AuthorcmdFlag	Command line authorization status. ● yes: Command line authentication is enabled. ● no: Command line authentication is disabled.

2.5.9 display vty mode

Function

The **display vty mode** command displays the current VTY mode.

Format

display vty mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

VTY modes are classified into the man-to-machine mode and machine-to-machine mode.

Example

Display the VTY mode.

```
<HUAWEI> display vty mode
Current user-interface mode is Human-Machine interface.
```

2.5.10 display vty lines

Function

The **display vty lines** command displays the number of rows that are displayed on the VTY screen.

Format

display vty lines

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the number of rows (configured using **screen-length** command) that are displayed on the VTY screen.

Example

Display the number of rows that are displayed on the VTY screen.

```
<HUAWEI> display vty lines
Current user-interface lines is 24
```

2.5.11 display web welcome-message

Function

The **display web welcome-message** command displays greetings of the web system.

Format

display web welcome-message

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display web welcome-message** command to view greetings of the web system.

Example

Display greetings of the web system.

```
<HUAWEI> display web welcome-message
huawei
```

2.5.12 flow-control

Function

The **flow-control** command configures a flow control mode.

The **undo flow-control** command restores the default flow control mode.

The default flow control mode is **none**, that is, flow control is disabled.

Format

flow-control { **hardware** | **none** | **software** }

undo flow-control

NOTE

Currently, the flow control mode of the device cannot be set to hardware.

Parameters

Parameter	Description	Value
hardware	Specifies hardware flow control.	-
none	Specifies no flow control.	-
software	Specifies software flow control.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The configuration is effective only when the serial interface works in asynchronous interaction mode.

If the flow control mode cannot be configured on a device, the system prompts the message **"Error: Failed to run this command because of internal causes of system malfunctions.**"

Example

Set the flow control mode to software flow control in the user interface view.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] flow-control software
```

2.5.13 free user-interface

Function

The **free user-interface** command disconnects a user from a specified user interface.

Format

free user-interface { *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
ui-number	Specifies the absolute number of a user interface.	The value is an integer ranging from 0 to 54 and 67 to 83. The value varies according to the device type.
ui-type	Specifies the type of a user interface.	The value can be console or VTY.
ui-number1	Specifies the relative number of a user interface.	The minimum value is 0. The maximum value is the number of user interfaces that the system supports minus 1.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a login user does not perform any operation for a long time or needs to be prohibited from configuring the device, run the **free user-interface** command to disconnect the user from the user interface. The device then logs out the user.

Precautions

The **free user-interface** command does not take effect for the current user interface. For example, if the current user interface is VTY 2, the **free user-interface vty 2** command does not take effect, and an error message is displayed.

This command provides the same function as the **kill user-interface** command.

Example

Disconnect the user from user-interface 0.

```
<HUAWEI> free user-interface 0
Warning: User interface Console1 will be freed. Continue? [Y/N]:y
```

2.5.14 kill user-interface

Function

The **kill user-interface** command disconnects a user from a user interface.

NOTE

The **kill user-interface** command can only be executed by users at level 3 or higher. These users can clear any other users.

Format

kill user-interface { *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
ui-number	Specifies the absolute number of a user interface.	The value is an integer ranging from 0 to 54 and 67 to 83. The value varies according to the device type.
ui-type	Specifies the type of a user interface.	The value can be console or VTY.
ui-number1	Specifies the relative number of a specified user interface.	The minimum value is 0. The maximum value is the number of user interfaces that the system supports minus 1.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a login user does not perform any operation for a long time or needs to be prohibited from configuring the device, run the **kill user-interface** command to disconnect the user from the user interface. The device then logs out the user.

Precautions

The **kill user-interface** command does not take effect for the current user interface. For example, if the current user interface is VTY 2, the **kill user-interface vty 2** command does not take effect, and an error message is displayed.

This command provides the same function as the **free user-interface** command.

Example

Disconnect user VTY3 from the device.

```
<HUAWEI> kill user-interface vty 3
Warning: User interface VTY3 will be freed. Continue? [Y/N]:y
Info: User interface VTY3 is free.
```

2.5.15 history-command max-size

Function

The **history-command max-size** command sets the size of the historical command buffer.

The **undo history-command max-size** command restores the default size of the historical command buffer.

By default, a maximum of 10 previously-used commands can be saved in the buffer.

Format

history-command max-size *size-value*

undo history-command max-size

Parameters

Parameter	Description	Value
size-value	Specifies the size of the historical command buffer.	The value is an integer ranging from 0 to 256.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The CLI can automatically save the historical commands that you enter. This function is similar to that of Doskey. You can invoke and run the historical commands at any time.

Precautions

- If the historical command buffer is used up and a new command is entered, the command line interface deletes the earliest command in the buffer in the sequence the commands were entered.
- The formats of the saved historical commands are the same as those of the commands entered by users. If the commands entered by a user are incomplete, the saved historical commands are also incomplete.
- If a user runs the same command several times, only the earliest command is saved as a historical command. However, if the same command is entered with different formats, they are saved as different commands.

Example

Set the size of the historical command buffer to 20.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] history-command max-size 20
```

2.5.16 idle-timeout

Function

The **idle-timeout** command sets a timeout period for users to disconnect from a user interface.

The **undo idle-timeout** command restores the default timeout period.

By default, the timeout period is 10 minutes.

Format

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Parameters

Parameter	Description	Value
minutes	Specifies the idle timeout period, in minutes.	The value is an integer ranging from 0 to 35791.
seconds	Specifies the idle timeout period, in seconds.	The value is an integer ranging from 0 to 59.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an online user does not perform any operation, the user interface where the user logs in is wasted. To resolve this problem, run the **idle-timeout** command to set a timeout period. If the user does not perform any operation before the timeout period expires, the user is disconnected from the user interface.

Precautions

- If you set the timeout period to 0, the user connection remains alive until it is manually cut.
- If you set the timeout period to 0 or a large value, the user will remain in the login state, resulting in security risks. You are advised to run the **lock** command to lock the current connection.
- If the user interface disconnection function is not configured, other users may fail to log in to the device. You are advised to set the timeout period to 10-15 minutes.

NOTE

If AAA authentication is used, the **local-user idle-timeout** *minutes* [*seconds*] command takes precedence. If both the commands are configured, the value configured using the **local-user idle-timeout** command takes effect.

If RADIUS authentication is used, the RADIUS attribute **Idle-Timeout** takes precedence. If both the **Idle-Timeout** attribute and the **idle-timeout** command are configured, value of the RADIUS attribute **Idle-Timeout** takes effect.

Example

Set the timeout period to 1 minute and 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] idle-timeout 1 30
```

2.5.17 mmi-mode enable

Function

The **mmi-mode enable** command enters the machine-to-machine mode.

The **undo mmi-mode enable** command enters the man-to-machine mode.

By default, a VTY user is in man-to-machine mode.

Format

mmi-mode enable

undo mmi-mode enable

Parameters

None

Views

User view, system view

Default Level

0: Visit level

Usage Guidelines

The machine-to-machine mode is used on the NMS. After you enter the machine-to-machine mode using the **mmi-mode enable** command, some important commands that you need to use with caution can be used directly. Therefore, in man-to-machine mode, do not use this command unless necessary.

After you enter the machine-to-machine mode, the maximum number of lines in the screen of the current user interface is restored to the default value (512). You can run the **screen-length** command to change the default value.

Example

Enter the machine-to-machine mode.

```
<HUAWEI> system-view
[HUAWEI] mmi-mode enable
```

2.5.18 parity

Function

The **parity** command sets a parity bit for a user interface.

The **undo parity** command disables the parity check.

By default, no parity check is configured.

Format

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

Parameters

Parameter	Description	Value
even	Specifies even parity check.	-
mark	Specifies Mark parity check.	-
none	Specifies no parity check.	-
odd	Specifies odd parity check.	-
space	Specifies Space parity check.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The setting is valid only when the serial port is configured to work in asynchronous mode.

If the parity bit for a user interface cannot be set on a device, the system prompts the message **"Error: Failed to run this command because of internal causes of system malfunctions.**"

Example

Set the transmission parity bit on the console port to odd parity.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] parity odd
```

2.5.19 protocol inbound

Function

The **protocol inbound** command specifies the protocols that VTY user interfaces support.

The **undo protocol inbound** command restores the default protocols that VTY user interfaces support.

By default, VTY user interfaces support SSH.

Format

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

Parameters

Parameter	Description	Value
all	Indicates that all protocols including SSH and Telnet are supported.	-
ssh	Indicates that only SSH is supported.	-
telnet	Indicates that only Telnet is supported.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To manage and monitor login users, configure VTY user interfaces for login users and run the **protocol inbound** command to configure the protocols that the VTY user interfaces support.

Prerequisites

If SSH is configured for a user interface using the **protocol inbound ssh** command, you must run the **authentication-mode aaa** command to configure AAA authentication. This ensures that a user can successfully log in to the user interface. If password authentication is configured, the **protocol inbound ssh** command does not take effect.

Precautions

- The configuration takes effect at the next login.
- When SSH is specified for the VTY user interface, if the SSH server function is enabled but the RSA, DSA, or ECC key is not configured, a user cannot log in to the SSH server using SSH.
- Telnet is an insecure protocol. Using SSH is recommended.

Example

Configure SSH for user interfaces VTY0 to VTY4.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] protocol inbound ssh
```

2.5.20 screen-length

Function

The **screen-length** command sets the number of lines on each terminal screen.

The **undo screen-length** command restores the default configuration.

By default, the number of lines displayed on a terminal screen is 24.

Format

In the user interface view:

screen-length *screen-length* [**temporary**]

undo screen-length [**temporary**]

In the user view:

screen-length *screen-length* **temporary**

undo screen-length temporary

Parameters

Parameter	Description	Value
screen-length	Specifies the number of lines displayed on a terminal screen.	The value is an integer that ranges from 0 to 512. The value 0 indicates that all command output is displayed on one screen.
temporary	Specifies the number of lines temporarily displayed on a terminal screen.	-

Views

User interface view, user view

Default Level

3: Management level in the user interface view

1: Monitoring level in the user view

Usage Guidelines

If a command output is displayed in more lines than you can see on one screen, run the **screen-length** command to reduce the number of lines displayed on each screen.

In general, you do not need to change the number of lines displayed on each screen. Setting the number of lines to 0 is not recommended. The configuration takes effect after you log in to the system again.

NOTE

In the user view, the **temporary** parameter is mandatory, and this command is at the Monitoring level.

Example

Set the number of lines on each screen of the terminal to 30.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] screen-length 30
```

2.5.21 screen-width

Function

The **screen-width** command sets the number of columns displayed on a terminal screen.

The **undo screen-width** command restores the default configuration.

By default, 80 columns are displayed on a terminal screen.

Format

screen-width *screen-width*

undo screen-width

Parameters

Parameter	Description	Value
screen-width	Specifies the width of a terminal screen.	The value is an integer ranging from 60 to 512.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you log in to the device from a console interface and run the **display interface description** [*interface-type* [*interface-number*]] command to view the interface information, output information does not automatically change to another line, resulting in wrong format of the output information.

To resolve this problem, run the **screen-width** command to adjust the information format. In general, you do not need to adjust the number of columns displayed on the terminal screen. Setting the number of columns displayed on a screen is not recommended.

Precautions

The number of columns set using the **screen-width** command is valid only for the current interface. The setting is not saved after you log out. When you log in to the device from the console interface and configure this command, the number of columns displayed on the terminal screen is valid only for the current console interface, which has no impact on other users who log in to the device from the VTY interface or other interfaces. If you log out of the console interface and log in to the device again, the default width is used for the terminal screen.

This command is valid only for information displayed by the **display interface description** [*interface-type* [*interface-number*]] command.

Example

Configure each line displayed on a terminal screen to have 60 characters.

```
<HUAWEI> screen-width 60
Warning: This command will change the default screen width. Continue? [Y/N]:y
Info: Succeeded in setting the screen width to 60.
```

2.5.22 set authentication password

Function

The **set authentication password** command configures a local authentication password.

The **undo set authentication password** command cancels the local authentication password.

By default, no local authentication password is configured for devices.

Format

set authentication password [**cipher** *password*]

undo set authentication password

Parameters

Parameter	Description	Value
cipher	Indicates a password in cipher text.	-
password	Specifies the password.	The value is a string of 8 to 16 characters or a string of 56 or 68 characters. The password can be in plain or cipher text. ● The password in plain text is a string of 8 to 16 characters. The password must contain at least two types of the following characters: upper-case characters, lower-case characters, digits, and special characters. Special characters do not include the question mark (?) and space. ● The password in cipher text is a string of 56 or 68 characters. The password in cipher text must start with $1a$ and end with $, or start with %^%# and end with %^%#. **NOTE** If the source version supports a ciphertext password that is a string of 24 characters, the target version also supports this type of password. The password is displayed in cipher text in the configuration file regardless of whether it is input in plain text or cipher text.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If password authentication is configured for users, you can run the **set authentication password** command to change the password or set a password in cipher text.

If **cipher** *password* is not specified, the password is entered in interactive mode and can contain 8 to 16 characters. The requirements for the password are the same as the requirements for the password in plain text that is specified using the **cipher** parameter. The password you enter will not be displayed on the screen.

NOTE

If you enter the plain text password when specifying **cipher** *password*, security risks exist. The interactive mode is recommended when users enter the password.

Pre-configuration Tasks

Password authentication has been configured for the user interface.

Precautions

- If a password in cipher text is configured, users must obtain the password in plain text that is required for login authentication.
- You cannot run the **undo set authentication password** command to delete a password. The **undo set authentication password** command is retained for compatibility with other versions.
- If the password authentication is configured but the password is not configured for the user interface, the user cannot log in to the device.
- If the **set authentication password** command is executed multiple times, the latest configuration overrides the previous ones. You can run the **set authentication password** command to change the local authentication password. After the password is changed, a user who wants to log in to the device must enter the latest password for login authentication.
- Users can press **CTRL_C** to cancel password modification in the interaction mode.
- You are advised to change the password periodically to improve device security.

Example

Set a local authentication password for the user interfaces VTY 0-4 in interactive mode.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] set authentication password
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" 
authentication mode.
Please configure the login password (8-16)
Enter Password:
Confirm Password:
[HUAWEI-ui-vty0-4]
```

Set a local authentication password for the user interfaces VTY 0-4.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] set authentication password cipher YsHsjx_202206
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" 
authentication mode.
```

2.5.23 set password min-length

Function

The **set password min-length** command sets the minimum length of passwords in plain text allowed by a device.

The **undo set password min-length** command restores the default minimum length of passwords in plain text allowed by a device.

By default, the minimum length of passwords in plain text allowed by a device is 8 characters.

Format

set password min-length *length*

undo set password min-length

Parameters

Parameter	Description	Value
length	Specifies the minimum length of passwords in plain text allowed by a device.	The value is an integer ranging from 6 to 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command can change the limit on the password length. A longer password length makes the password more complex and improves device security.

Precautions

- The **set password min-length** command limits the length of all passwords in plain text. Only the passwords longer than or equal to the minimum length take effect. The minimum length does not take effect for the following passwords:
  - Passwords configured during configuration restoration
  - Passwords that have taken effect before the minimum length is configured
- This command limits the minimum length of only the passwords in plain text configured using the following commands:
  - **set authentication password**
  - **lock**
  - **local-user**
  - **super password**

  The **set password min-length** command does not limit the minimum length of other types of passwords.

NOTE

If password complexity check has been disabled using the **undo user-password complexity-check** command, the **set password min-length** command does not limit the minimum length of passwords in plain text of local users.

For device security purposes, do not disable the password complexity check function and change the password periodically.

Example

Set the minimum length of passwords in plain text allowed by the local device to 10 characters.

```
<HUAWEI> system-view
[HUAWEI] set password min-length 10
```

2.5.24 shell

Function

The **shell** command enables terminal services on a user interface.

The **undo shell** command disables terminal services on a user interface.

By default, terminal services are enabled on all user interfaces.

Format

shell

undo shell

Parameters

None

Views

User interface view

Default Level

3: Management level

Usage Guidelines

You can use the **shell** command on a user interface to enable terminal services. This command enables users to enter commands through this interface to query device information and configure the device.

You can use the **undo shell** command on the user interface to disable terminal services. This command does not allow users to perform any operations through this interface. After using the **undo shell** command in the VTY view, this user interface does not provide Telnet, STelnet, and SFTP access.

NOTE

The console interface does not support this command.

Example

Disable terminal services on VTY 0 to VTY 4.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] undo shell
Warning: ui-vty0-4 will be disabled. Continue? [Y/N]:y
```

2.5.25 speed (user interface view)

Function

The **speed** command sets the data transfer rate of a user interface.

The **undo speed** command restores the default data transfer rate of a user interface.

By default, the data transfer rate is 9600 bit/s.

Format

speed *speed-value*

undo speed

Parameters

Parameter	Description	Value
speed-value	Specifies the data transfer rate of a user interface.	The value is expressed in bit/s. The asynchronous serial interface supports the following data transfer rates: ● 300 bit/s ● 600 bit/s ● 1200 bit/s ● 4800 bit/s ● 9600 bit/s ● 19200 bit/s ● 38400 bit/s ● 57600 bit/s ● 115200 bit/s

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the data transfer rate of a user interface to 115200 bit/s.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] speed 115200
```

2.5.26 stopbits

Function

The **stopbits** command sets a stop bit for a user interface.

The **undo stopbits** command restores the default stop bit of a user interface.

The default stop bit is 1.

Format

stopbits { **1.5** | **1** | **2** }

undo stopbits

Parameters

Parameter	Description	Value
1.5	Sets the stop bit to 1.5.	-
1	Sets the stop bit to 1.	-
2	Sets the stop bit to 2.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

If the stop bit is 1, the corresponding data bit is 7 or 8.

If the stop bit is 1.5, the corresponding data bit is 5.

If the stop bit is 2, the corresponding data bit is 6, 7, or 8.

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the stop bit of a user interface to 2.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] stopbits 2
```

2.5.27 user privilege

Function

The **user privilege** command configures a user privilege level.

The **undo user privilege** command restores the default user privilege level.

By default, users who log in to a device using the console interface are at level 15, and other users are at level 0.

Format

user privilege level *level*

undo user privilege level

Parameters

Parameter	Description	Value
level *level*	Specifies a user privilege level. **NOTE** A larger value indicates a higher priority.	The value is an integer ranging from 0 to 15.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To limit users' access permissions to a device, the device manages users by level. Users of a specified level can run only commands whose levels are lower than or equal to the user privilege level.

Commands are classified into the visit level, monitoring level, configuration level, and management level that map levels 0, 1, 2, and 3, respectively. **Table 2-26** describes these command privilege levels.

Table 2-26 Command privilege levels

User Privilege Level	Command Privilege Level	Permission	Description
0	0	Visit	Diagnostic commands, such as ping and tracert commands, and commands that are used to access a remote device such as a Telnet client
1	0 and 1	Monitoring	System maintenance commands, such as display commands **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3.
2	0, 1, and 2	Configuration	Service configuration commands
3-15	0, 1, 2, and 3	Management	System basic operation commands that are used to support services, including file system, FTP, TFTP, user management commands, command-level configuration commands, and debugging commands.

Precautions

If refined permission management is required, run the **command-privilege level** command to upgrade command privilege levels.

Example

Set the user privilege level on the VTY0 user interface to 2.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] user privilege level 2
```

Log in to the device using Telnet and view detailed information about the VTY0 user interface.

```
<HUAWEI> display user-interface vty 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
+ 34    VTY 0               -    2     15           N    -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
```

```
Type : Type and relative index of UIs.
Privi: The privilege of UIs.
ActualPrivi: The actual privilege of user-interface.
Auth : The authentication mode of UIs.
    A: Authenticate use AAA.
    N: Current UI need not authentication.
    P: Authenticate use current UI's password.
Int  : The physical location of UIs.
```

Table 2-27 Description of the **user privilege level** command output.

Item	Description
+	Current user interface is active.
F	Current user interface is active and is working in asynchronous mode.
Idx	Absolute index of the user interface.
Type	Type and relative index of the user interface.
Privi	Privilege of the user interface.
ActualPrivi	Actual privilege of the user interface.
Auth	Authentication mode of the user interface.
Int	Physical location of UIs.
A	AAA authentication.
N	None authentication
P	Password authentication

2.5.28 user-interface

Function

The **user-interface** command displays one or multiple user interface views.

Format

user-interface [*ui-type*] *first-ui-number* [*last-ui-number*]

Parameters

Parameter	Description	Value
ui-type	Specifies the type of a user interface. ● If the user interface is specified, the relative number is used. ● If the user interface is not specified, the absolute number is used.	The value can be console or VTY.
first-ui-number	Specifies the number of the first user interface.	● If *ui-type* is set to **console**, the *first-ui-number* value is **0**. ● If *ui-type* is set to **vty**, the *first-ui-number* value ranges from 0 to the maximum number of VTY user interfaces.
last-ui-number	Specifies the number of the last user interface. When you select this parameter, you enter multiple user interface views at the same time. This parameter is valid only when *ui-type* is set to VTY. The *last-ui-number* value must be larger than the *first-ui-number* number. If the maximum number of VTY users has been set using the **user-interface maximum-vty** command in the system view before *ui-type* is selected, the *last-ui-number* value is smaller than or equal to the maximum number of VTY user interfaces minus one.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a network administrator logs in to a device using the console interface, Telnet, or SSH, the network administrator can set parameters, such as an authentication more and user privilege level, on the user interface to allow the device to centrally manage user sessions.

Precautions

Only users at level 15 can use this command.

The user interface varies according to the login mode. The user interface views can be numbered using absolute numbers or relative numbers. **Table 2-28** describes absolute and relative numbers of user interfaces.

NOTE

- The relative numbering uniquely specifies a user interface or a group of user interfaces of the same type.
- The absolute numbering specifies a user interface or a group of user interfaces.

Table 2-28 Absolute and relative numbers of user interfaces

User Interface	Description	Absolute Number	Relative Number
Console user interface	Manages and controls users who log in to the device using the console interface.	0	0
VTY user interface	Manages and controls users who log in to the device using Telnet or SSH.	34 to 48 and 50 to 54	The first one is VTY 0, the second one is VTY 1, and so forth. • Absolute numbers 34 to 48 map relative numbers VTY 0 to VTY 14. • Absolute numbers 50 to 54 map relative numbers VTY 16 to VTY 20. VTY 15 is reserved for the system. VTY 16 to VTY 20 are reserved for the NMS. Only when VTY 0 to VTY 14 are all used, AAA authentication is configured for users, VTY 16 to VTY 20 can be used.

After you log in to the device, you can run the **display user-interface** command to view the supported user interfaces and the corresponding relative and absolute numbers.

Example

Enter the Console 0 user interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0]
```

Enter the VTY 1 user interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 1
[HUAWEI-ui-vty1]
```

Enter the VTY 1 to VTY 3 user interfaces.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 1 3
[HUAWEI-ui-vty1-3]
```

2.5.29 user-interface current

Function

The **user-interface current** command displays the current user interface view.

Format

user-interface current

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enter the current user interface view, run the **user-interface current** command, without the need to run the **display user-interface** command to check the user interface number.

Precautions

Only users at level 15 can use this command.

The user interface varies according to the login mode. The user interface views can be numbered using absolute numbers or relative numbers. **Table 2-28** describes absolute and relative numbers of user interfaces.

NOTE

- The relative numbering uniquely specifies a user interface or a group of user interfaces of the same type.
- The absolute numbering specifies a user interface or a group of user interfaces.

Example

Enter the current user view.

```
<HUAWEI> system-view
[HUAWEI] user-interface current
[HUAWEI-ui-vty1]
```

2.5.30 user-interface maximum-vty

Function

The **user-interface maximum-vty** command configures the maximum number of login users.

The **undo user-interface maximum-vty** command restores the default maximum number of login users.

By default, the maximum number of Telnet and SSH users is 5.

Format

user-interface maximum-vty *number*

undo user-interface maximum-vty

Parameters

Parameter	Description	Value
number	Specifies the maximum number of Telnet and SSH users.	The value is an integer ranging from 0 to 15.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the maximum number of login users, run the **user-interface maximum-vty** command.

Precautions

- If the maximum number that you set is smaller than the number of current online users, a device displays a configuration failure message.
- When the configured maximum number of VTY user interfaces is less than the number of current online users, the system disconnects the users that are not authenticated and occupy VTY channels for more than 15s and allows new users to log in to the device through VTY.
- When the configured maximum number of VTY user interfaces exceeds the maximum number of allowed access users, you need to configure the authentication mode for the excess user interfaces.
- The maximum number of login users set by the **user-interface maximum-vty** command is the total number of Telnet and SSH users.
- If the maximum number of login users is set to 0, users are not allowed to log in to the device using Telnet or SSH.
- When the number of login VTY users has reached the maximum, an NMS user can log in using the reserved VTY numbers 16-20. The NMS user is allowed to log in to the device only after passing the AAA local authentication.

Example

Set the maximum number of Telnet users to 7.

```
<HUAWEI> system-view
[HUAWEI] user-interface maximum-vty 7
```

2.5.31 user-interface password complexity-check disable

Function

The **user-interface password complexity-check disable** command disables the password complexity check function.

The **undo user-interface password complexity-check disable** command enables the password complexity check function.

By default, the password complexity check function is enabled.

Format

user-interface password complexity-check disable

undo user-interface password complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Passwords configured in the interface view must meet the following complexity requirements:

- A password must contain at least 8 characters. If the minimum length set using the **set password min-length** command exceeds 8 characters, the command configuration takes effect.
- A password must contain at least two types of characters: uppercase characters, lowercase characters, digits, and special characters, excluding question marks (?) and spaces.

To disable the password complexity check function, run the **user-interface password complexity-check disable** command. To enable the password complexity check function, run the **undo user-interface password complexity-check disable** command.

Precautions

If the configured password does not meet complexity requirements, it is prone to attacks and cracks from unauthorized users, which affects device security. Therefore, keeping the password complexity check function enabled is recommended.

Example

Disable the password complexity check function.

```
<HUAWEI> system-view
[HUAWEI] user-interface password complexity-check disable
```

2.5.32 web welcome-message

Function

The **web welcome-message** command configures greetings for the web system.

The **undo web welcome-message** command cancels the configuration of greetings for the web system.

By defaults, greetings are not configured for the web system.

Format

web welcome-message *message*

undo web welcome-message

Parameters

Parameter	Description	Value
message	Configures greetings for the web system.	The value is a string of 1 to 242 case-sensitive characters without question mark (?). Spaces are supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **web welcome-message** command to configure greetings for the web system. After the **undo web welcome-message** command is run, no greetings will be displayed on the web system.

Example

Configure greetings of the web system to **huawei**.

```
<HUAWEI> system-view
[HUAWEI] web welcome-message huawei
```

2.6 User Login Configuration Commands

2.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.6.2 configuration exclusive

Function

The **configuration exclusive** command locks the current system configuration. When the system configuration is locked, the user who locks it can query and modify the configuration while other users can only query the configuration.

The **undo configuration exclusive** command unlocks the system configuration.

By default, the system configuration is unlocked.

Format

configuration exclusive

undo configuration exclusive

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device allows several users to log in concurrently to perform manual configurations, which may cause configuration conflicts and service exceptions. To prevent service exceptions, run the **configuration exclusive** command to lock and modify the configuration. Other users can then only query the configuration.

To unlock the configuration, do either of the following:

- Run the **undo configuration exclusive** command.
- Do not modify the configuration in the configured lock interval. The system then automatically unlocks the configuration. To configure the lock interval, run the **configuration-occupied timeout** command.

Precautions

- After you run the **configuration exclusive** command, other users cannot modify the system configuration, so confirm your action before running this command.
- Before you run the **configuration exclusive** command, run the **configuration-occupied timeout** command to configure the maximum lock interval so that the system can automatically unlock the configuration after this interval.

Example

Lock the current system configuration.

```
<HUAWEI> configuration exclusive
```

Unlock the system configuration.

```
<HUAWEI> undo configuration exclusive
```

2.6.3 configuration-occupied timeout

Function

The **configuration-occupied timeout** command sets the interval after which the system automatically unlocks the configuration.

The **undo configuration-occupied timeout** command restores the default automatic unlock interval.

By default, the value is 30 seconds.

Format

configuration-occupied timeout *timeout-value*

undo configuration-occupied timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the interval after which the system automatically unlocks the configuration if no configuration command is run.	The value is an integer that ranges from 1 to 7200, in seconds. By default, the value is 30 seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

The **configuration-occupied timeout** command configures the longest lock interval. If no configuration command is delivered within this interval, the system automatically unlocks the configuration so that other users can modify the configuration.

The usage scenarios for this command are as follows:

- If the user does not have the configuration right, the system displays an error.
- If the configuration is locked by another user, the system displays a message indicating that the modification fails.
- If the configuration is locked by the user who configures the longest lock interval, the modification is valid.

NOTE

Note the following when running the **configuration-occupied timeout** command:

- The interval cannot be too short because the device will automatically unlock the configuration if no configuration command is delivered by the user who configures the interval.
- The interval cannot be too long because other users cannot modify the configuration within this period even if the user who locks the configuration delivers no configuration command within this period.
- The command is valid for all users.

Example

Set the automatic unlock interval to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] configuration-occupied timeout 120
```

2.6.4 console0 disable

Function

The **console0 disable** command disables the console port login function.

The **undo console0 disable** command enables the console port login function.

By default, the console port login function is enabled.

Format

console0 disable

undo console0 disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Application Scenario

By default, the administrator can log in to a switch through the console port. If the console port login function is not required, you can run the **console0 disable** command to disable this function. If this function is required, you can run the **undo console0 disable** command to enable this function.

Precautions

After the **console0 disable** command is run, this command does not take effect for users who have logged in to the device through the console port and takes effect for the users only after they exit from the console port using the **quit** command.

For devices that have the PNP button, you can press and hold the PNP button to enable the function of logging in through the console port.

Example

Disable the console port login function.

```
<HUAWEI> system-view
[HUAWEI] console0 disable
```

2.6.5 display configuration-occupied user

Function

The **display configuration-occupied user** command displays information about the user who locks the configuration.

Format

display configuration-occupied user

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run the **display configuration-occupied user** command to query the user who has the configuration right. If no user locks the system configuration, the system displays a corresponding message.

Example

Display the user who locks the configuration.

```
<HUAWEI> display configuration-occupied user
User Index: 34
User Session Name: VTY0
User Name:**
IP Address: 10.135.19.22
Locked Time: 2012-09-16 15:26:32+10:00 DST
Last Configuration Time: 2012-09-16 15:26:32+10:00 DST
The time out value of configuration right locked is: 30 second(s)
```

Table 2-29 Description of the **display configuration-occupied user** command output

Item	Description
User Index	User index.
User Session Name	User session name. The value is CON0 or ranges from VTY0 to VTY14. snmp-agent: session name of an NMS user.
User Name	Name of a login user. ● If a login user name is **, the user logs in to a device using a serial port or the password authentication mode. ● If the login user name is a community or V3 user name, the user is an NMS user.
IP Address	IP address of the user.
Locked Time	Time when the configuration was locked.
Last Configuration Time	Time when the user delivered the last configuration command.
The time out value of configuration right locked is	Duration for locking the configuration. To configure the duration, run the **configuration-occupied timeout** command.

Display the user who locks the system configuration (when no user locks the system configuration).

```
<HUAWEI> display configuration-occupied user
Info: No user locked the current configuration.
```

2.6.6 display dsa local-key-pair public

Function

The **display dsa local-key-pair public** command displays the public key in the local DSA key pair of the device.

Format

display dsa local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the public key in the local DSA key pair. You can copy the public key in the command output to the DSA public key of the SSH server to ensure that the public keys on the client and server are consistent and that the client can be authenticated by the server.

Example

Display the public key in the client DSA key pair.

```
<HUAWEI> display dsa local-key-pair public
=====================================================
Time of Key pair created:2014-08-27 06:35:16+08:00
Key name     : HUAWEI_Host_DSA
Key modulus : 2048
Key type     : DSA encryption Key
Key fingerprint: b5:82:31:f1:65:0f:97:81:dc:27:95:a8:f8:26:68:c4
=====================================================
Key code:
3081DC
  0240
    AE0AE467 2BF3587F 30FE81FF A14D8070 1FC2930B
    A34004C1 B37824BB D3160595 702901CD 53F0EAE0
    6CC46D2D BE78F6A4 3DC4AAEF C7228E01 9C2EF7CE
    87C63485
  0214
    94FC5624 DCEB09DA E9B88293 2AC88508 AB7C813F
  0240
    91FF0F2C 91996828 BAAD5068 CD2FE83E CEFA1CF4
    7BCA4251 9F04FD24 6CFB50A3 AD78CC0D 335DEFD2
    0B4C3530 DAA25592 DEAFA0EB 61225712 E4AF6139
    C986329F
  0240
    26D21FBE 18A9FCB3 C19A7430 A801D8A1 09CFC6E6
    ACB104F4 B398B3B7 83A059EA BE23AE04 5D7AD134
    4279637B 51AD9ADF 80B627EA 9328C95F 3DFF00EE
    84847039

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAABBAK4K5Gcr81h/MP6B/6FNgHAfwpMLo0AEwbN4JLvTFgWV
cCkBzVPw6uBsxG0tvnj2pD3Equ/HIo4BnC73zofGNIUAAAAVAJT8ViTc6wna6biC
kyrIhQirfIE/AAAAQQCR/w8skZloKLqtUGjNL+g+zvoc9HvKQlGfBP0kbPtQo614
zA0zXe/SC0w1MNqiVZLer6DrYSJXEuSvYTnJhjKfAAAAQCbSH74YqfyzwZp0MKgB
2KEJz8bmrLEE9LOYs7eDoFnqviOuBF160TRCeWN7Ua2a34C2J+qTKMlfPf8A7oSE
cDk=
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-dss AAAAB3NzaC1kc3MAAABBAK4K5Gcr81h/MP6B/6FNgHAfwpMLo0AEwbN4JLvTFgWVcCkBzVPw
6uBsxG0tvnj2pD3Equ/HIo4BnC73zofGNIUAAAAVAJT8ViTc6wna6biCkyrIhQirfIE/AAAAQQCR/w8s
```

```
kZloKLqtUGjNL+g+zvoc9HvKQlGfBP0kbPtQo614zA0zXe/SC0w1MNqiVZLer6DrYSJXEuSvYTnJhjKf
AAAAQCbSH74YqfyzwZp0MKgB2KEJz8bmrLEE9LOYs7eDoFnqviOuBF160TRCeWN7Ua2a34C2J+qTKMlf
Pf8A7oSEcDk= dsa-key
```

Table 2-30 Description of the **display dsa local-key-pair public** command output

Item	Description
Time of Key pair created	Time when the public key was created.
Key name	Name of the public key.
Key modulus	Length of the key.
Key type	Type of the public key.
Key fingerprint	Key fingerprint.
Key code	Content of the key.
Host public key for PEM format code	PEM code of the public key.
Public key code for pasting into OpenSSH authorized_keys file	Public key format in the OpenSSH file.

2.6.7 display dsa peer-public-key

Function

The **display dsa peer-public-key** command displays the DSA public key that has been configured.

Format

display dsa peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information.	-
name *key-name*	Displays the DSA public key with the specified name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays the DSA public key for you to check whether the local and peer public keys are consistent.

Precautions

You must complete the DSA public key configuration before running this command.

Example

Display the DSA public key with the specified name.

```
<HUAWEI> display dsa peer-public-key name amar
=====================================
    Key name: amar
    Encoding type: DER
=====================================
Key Code:
3081DC
  0240
    AE0AE467 2BF3587F 30FE81FF A14D8070 1FC2930B A34004C1 B37824BB D3160595
    702901CD 53F0EAE0 6CC46D2D BE78F6A4 3DC4AAEF C7228E01 9C2EF7CE 87C63485
  0214
    94FC5624 DCEB09DA E9B88293 2AC88508 AB7C813F
  0240
    91FF0F2C 91996828 BAAD5068 CD2FE83E CEFA1CF4 7BCA4251 9F04FD24 6CFB50A3
    AD78CC0D 335DEFD2 0B4C3530 DAA25592 DEAFA0EB 61225712 E4AF6139 C986329F
  0240
    0E7BEFD5 594ECA9C CE574D9D 369BCD0C 19C94725 5FE8666E 73292AD6 908E4E0C
    7F0EA3AF A02F17F7 3A0B1D15 E22420CB B5EC1D2C 8BA77729 276EDEBB 8DA843C7
```

Table 2-31 Description of the **display dsa peer-public-key** command output

Item	Description
Key name	Type of the public key.
Encoding type	Type of the public key encoding format.
Key code	Code of the public key.

2.6.8 display ecc local-key-pair public

Function

The **display ecc local-key-pair public** command displays information about the public key in the local Elliptic Curves Cryptography (ECC) key pair.

Format

display ecc local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **display ecc local-key-pair public** command to check information about the public key in the local ECC key pair on a client and then copy the public key to the server. The public key enables a server to authenticate users and ensures the login of authorized users.

Pre-configuration Tasks

You must run the **ecc local-key-pair create** command to generate a local ECC host key pair before using the command.

Example

Display information about the public key in the local ECC key pair on a client.

```
<HUAWEI> display ecc local-key-pair public
========================================================
Time of Key pair created:2016-10-19 11:50:20+00:00
Key name    : HUAWEI_Host_ECC
Key modulus : 521
Key type    : ECC encryption Key
Key fingerprint:
========================================================
Key code:
   0401CE1E 5EF3B843 CD917648 1D70EF8F CECE8518 5B32ED5F 529E9DC4 D16EDF1A
   5F6E6389 10AAE2D4 74FD9DA7 F05AB123 9AF3EE64 9F0BAF99 A0CBF55B E319B2D1
   8EDEBB01 7C63469B C62A2256 3EAEA0BD 486F9524 8559C7EF 24D969D1 11093BBF
   27F770E7 03E28ABA BB357E5B 28EF04CC EA931C81 C7D7EBD8 5797B1CD 05D9B497
   56D91126 E9

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
```

```
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAHOHl7zuEPN
kXZIHXDvj87OhRhbMu1fUp6dxNFu3xpfbmOJEKri1HT9nafwWrEjmvPuZJ8Lr5mg
y/Vb4xmy0Y7euwF8Y0abxioiVj6uoL1Ib5UkhVnH7yTZadERCTu/J/dw5wPiirq7
NX5bKO8EzOqTHIHH1+vYV5exzQXZtJdW2REm6Q==
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAHOHl7z
uEPNkXZIHXDvj87OhRhbMu1fUp6dxNFu3xpfbmOJEKri1HT9nafwWrEjmvPuZJ8Lr5mgy/Vb4xmy0Y7e
uwF8Y0abxioiVj6uoL1Ib5UkhVnH7yTZadERCTu/J/dw5wPiirq7NX5bKO8EzOqTHIHH1+vYV5exzQXZ
tJdW2REm6Q== ecdsa-key
```

Table 2-32 Description of the **display ecc local-key-pair public** command output

Item	Description
Time of Key pair created	Time when the public key in the local ECC key pair is generated, in the format of YYYY-MM-DD HH:MM:SS±HH:MM.
Key Name	Name of the public key in the local ECC key pair.
Key modulus	Length of the public key in the local ECC key pair on a client.
Key Type	Type of the public key in the local ECC key pair. "ECC encryption Key" indicates an ECC public key.
Key Code	Code of the public key in the local ECC key pair configured using the **ecc local-key-pair create** command.
Host public key for PEM format code	PEM code of the public key in the local ECC key pair on a client.
Public key code for pasting into OpenSSH authorized_keys file	Public key in the local ECC key pair on a client that is used for OpenSSH authorization. This information can be used after being copied to the OpenSSH authorized_keys file.

2.6.9 display ecc peer-public-key

Function

The **display ecc peer-public-key** command displays information about the Elliptic Curves Cryptography (ECC) public key configured on the remote end.

Format

display ecc peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information about the ECC public key configured on the remote end.	-
name *key-name*	Displays information about an ECC public key with a specified name configured on the remote end.	The value is a string of 1 to 30 case-sensitive characters, spaces not supported.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **display ecc peer-public-key** command on a client to check information about the public key configured on the remote end. The public key enables a server to authenticate users and ensures the login of authorized users.

Example

Display the information about the ECC public keys of 127.0.0.1.

```
<HUAWEI> display ecc peer-public-key
====================================
    Key name: 127.0.0.1
    Encoding type: DER
====================================
Key Code:
    04013184 A3311697 89DF558B 7F67BF9D BD95DBD5 280D659F 0E29852C AEC2FFBA
    1913AC2A 88247ADA 46BEBEBE 1829C0DA 3BABC8FC 8F6EAD28 2AE2C6A8 116BAA3A
    540E6B00 34E033D8 9D84841B 0D33DAD8 DEDD1C09 2B70B3DB 5AF0FCB2 37DF1C82
    C4C622A6 85B23698 195DA60F 06858ADB DD743937 B4A29C4C FB28B40B BCEEE036
    1DE61BD2 24
```

Display the brief information about all the ECC public keys.

```
<HUAWEI> display ecc peer-public-key brief
  Bits   Name
----------------------
  521   127.0.0.1
  384   192.168.131.203
```

Table 2-33 Description of the **display ecc peer-public-key** command output

Item	Description
Bits	Length of the ECC public key configured on the remote end.
Name	Name of the ECC public key configured on the remote end.
Key name	Name of the ECC public key configured on the remote end.
Encoding type	Encoding type of the ECC public key configured on the remote end. ● OPENSSH If OpenSSH is specified, data is Base64 encoded. OpenSSH is derived from PEM. ● PEM If PEM is specified, data is Base64 encoded. ● DER If DER is specified, data is Base16 encoded.
Key Code	Code of the public key in the local ECC key pair configured using the **ecc local-key-pair create** command.

2.6.10 display http server

Function

The **display http server** command displays information about the current HTTPS server.

Format

display http server

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can view the HTTPS server information, including the status of HTTPS services, port number, maximum number of users allowed to access the HTTPS server, and number of current online users.

Example

Display information about the current HTTPS server.

```
<HUAWEI> display http server
  HTTP Server Status              : enabled
  HTTP Server Port                : 80(80)
  HTTP Timeout Interval           : 20
  Current Online Users            : 3
  Maximum Users Allowed           : 5
  HTTP Secure-server Status       : enabled
  HTTP Secure-server Port         : 443(443)
  HTTP SSL Policy                 : ssl_server
  HTTP IPv6 Server Status         : disabled
  HTTP IPv6 Server Port           : 80(80)
  HTTP IPv6 Secure-server Status  : disabled
  HTTP IPv6 Secure-server Port    : 443(443)
  HTTP server source interface    : MEth0/0/1
```

Table 2-34 Description of the display http server command output

Item	Description
HTTP Server Status	Status of the HTTP IPv4 server. - Enabled: The HTTP IPv4 service is enabled. - Disabled: The HTTP IPv4 service is disabled. You can configure the HTTP IPv4 server status by running the **http server enable** command.
HTTP Server Port	Port number of the HTTP IPv4 server. The default value is 80. You can configure the port number of the HTTP IPv4 server by running the **http server port** command.
HTTP Timeout Interval	Timeout period of the HTTP/HTTPS server. The default value is 20 minutes. You can configure the timeout period of the HTTP/HTTPS server by running the **http timeout** command.
Current Online Users	Number of current online users.

Item	Description
Maximum Users Allowed	Maximum number of users allowed to access the HTTP server.
HTTP Secure-server Status	Status of the HTTPS IPv4 server. ● Enabled: The HTTPS IPv4 service is enabled. ● Disabled: The HTTPS IPv4 service is disabled. You can configure the HTTPS IPv4 server status by running the **http secure-server enable** command.
HTTP Secure-server Port	Port number of the HTTPS IPv4 server. The default value is 443. You can configure the port number of the HTTPS IPv4 server by running the **http secure-server port** command.
HTTP SSL Policy	HTTPS SSL policy. You can configure the HTTPS SSL policy by running the **ssl policy** command.
HTTP IPv6 Server Status	Status of the HTTP IPv6 server function: ● **enabled**: The HTTP IPv6 server function is enabled. ● **disabled**: The HTTP IPv6 server function is disabled. You can configure the HTTP IPv6 server status by running the **http ipv6 server enable** command.
HTTP IPv6 Server Port	Port number of the HTTP IPv6 server. The default value is 80. You can configure the port number of the HTTPS IPv6 server by running the **http ipv6 server port** command.
HTTP IPv6 Secure-server Status	Status of the HTTPS IPv6 server function: ● **enabled**: The secure HTTPS IPv6 server function is enabled. ● **disabled**: The secure HTTPS IPv6 server function is disabled. You can configure the HTTPS IPv6 server status by running the **http ipv6 secure-server enable** command.

Item	Description
HTTP IPv6 Secure-server Port	Port number of the HTTPS IPv6 server. The default value is 443. You can configure the port number of the HTTPS IPv6 server by running the **http ipv6 secure-server port** command.
HTTP server source interface	The source interface of the HTTPS server. You can configure the source interface of the HTTPS server by running the **http server-source** command.

2.6.11 display http user

Function

The **display http user** command displays information about current online users.

Format

display http user [**username** *username*]

Parameters

Parameter	Description	Value
username *username*	Specifies the name of the current online user.	The value is a string of 1 to 64 case-insensitive characters, with no space or wildcard. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

If **username** is not specified, this command displays summary information about all online users.

If **username** is specified, this command displays detailed information about the specified online user.

Example

Display general information about the current online user.

```
<HUAWEI> display http user
Total online users: 1
-------------------------------------------------------
User name    IP Address           Login Date
-------------------------------------------------------
admin        192.168.0.1          2012-03-23 15:30:55+00:00
```

Display detailed information about the current online user **admin**.

```
<HUAWEI> display http user username admin
Client IP Address: 192.168.0.1
Login Date: 2012-03-19 15:30:55+00:00
User timeouts: 15 minute
```

Table 2-35 Description of the display http user command output

Item	Description
User name	User name.
Client IP Address	IP address of the HTTP client.
Login Date	Login date and time.
User timeouts	Idle timeout duration of online users.

2.6.12 display rsa local-key-pair public

Function

The **display rsa local-key-pair public** command displays the public key in the local key pair.

Format

display rsa local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command on the client and configure the client public key in the command output to the SSH server, which ensures that the SSH client validity check by the SSH server is successful and enables the secure data exchange between the SSH server and client.

Example

Display the public key in the local key pair.

```
<HUAWEI> display rsa local-key-pair public
=====================================================

Time of Key pair created: 2012-08-15 06:41:55+08:00
Key name: HUAWEI_Host
Key type: RSA encryption Key
Key fingerprint: ab:ec:d7:e1:22:5f:e4:e3:6e:f0:d6:1f:99:e4:f2:f3
=====================================================

Key code:
3047
  0240
    D8D10BE8 CD41AA43 862B6C2B 637D1A53
1EBB4015
    96A70B13 72B17A16 84E02168 4061A4C2
A1CDB541
    484F71DB D7271E5F E3C75BEA AF853023
0CDCE55D
    ECCB0461
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDY0QvozUGqQ4YrbCtjfRpTHrtAFZanCxNy

sXoWhOAhaEBhpMKhzbVBSE9x29cnHl/
jx1vqr4UwIwzc5V3sywRh
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys
file :
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDY0QvozUGqQ4YrbCtjfRpTHrtAFZanCxNysXoWhOAhaEBhpMKhzb
VBSE9x29cnHl/jx1vqr4UwIwzc5V3sywRh rsa-key


=====================================================

Time of Key pair created: 2012-08-15 06:42:03+08:00
Key name: HUAWEI_Server
Key type: RSA encryption Key
Key fingerprint: 16:3b:43:4f:74:16:98:b3:5c:51:b5:a3:83:f8:86:19
=====================================================

Key code:
3067
  0260
    F31D5536 26C05536 6703885D E8FCDB00
07C45437
    B3D08086 9E25B7B6 CFE375B2 1AA957EE
24D2DC51
    BAA81ECD 6894F71E 20596754 35653808
C8B74ACB
    DE94C584 1E234FED 840900F0 4A4100FB
C133DFB7
```

```
    12D4B4DB EF0C3E1F E211202A
F45DD5DD
  0203
    010001
```

Table 2-36 Description of the **display rsa local-key-pair public** command output

Item	Description
Time of Key pair created	Time and date when the public key was created.
Key Name	The value can be the host or server public key. The server public key is saved only when the key type is RSA.
Key Type	Type of the public key.
Key fingerprint	Public key fingerprint.
Key Code	Code of the public key.

2.6.13 display rsa peer-public-key

Function

The **display rsa peer-public-key** command displays the peer public key saved on the local host. If no parameter is specified, the command displays detailed information about all peer public keys.

Format

display rsa peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information about all peer public keys.	-
name *key-name*	Specifies the key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to check detailed information about the RSA public key and whether the local and peer public keys are the same.

Precautions

You must complete the RSA public key configuration before running this command.

Example

Display the brief information about all RSA public keys.

```
<HUAWEI> display rsa peer-public-key brief
Address         Bits   Name
---------------------------
                768   rsakey001
```

Table 2-37 Description of the **display rsa peer-public-key brief** command output

Item	Description
Address	Brief information about the public key.
Bits	Bits in the public key.
Name	Name of the public key.

Display the detailed information about the RSA public key named **rsakey001**.

```
<HUAWEI> display rsa peer-public-key name rsakey001
=====================================
    Key name: rsakey001
    Key address:
=====================================
Key Code:
3067
  0260
    A3158E6C F252C039 135FFC45 F1E4BA9B 4AED2D88 D99B2463 3E42E13A 92A95A37
    45CDF037 1AF1A910 AAE3601C 2EB70589 91AF1BB5 BD66E31A A9150911 859CAB0E
    1E10548C D70D000C 55A1A217 F4EA2F06 E44BD438 DA472F14 3FB7087B 45E77C05
  0203
    010001
```

Table 2-38 Description of the **display rsa peer-public-key name** command output

Item	Description
Key name	Name of the public key.
Key address	Brief information about the public key.
Key Code	Code of the public key.

2.6.14 display ssh server

Function

The **display ssh server** command displays the SSH server information.

Format

display ssh server { **status** | **session** }

Parameters

Parameter	Description	Value
status	Displays the global configuration on the SSH server.	-
session	Displays the current session connection information on the SSH server.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the SSH attributes, you can run this command to view the configuration or session connection information on the SSH server to verify that the SSH connection has been established.

Example

Display the global configuration on the SSH server.

```
<HUAWEI> display ssh server status
 SSH version                         :2.0
 SSH connection timeout              :60 seconds
```

```
SSH server key generating interval  :0 hours
SSH authentication retries          :3 times
SFTP IPv4 server                    :Enable
SFTP IPv6 server                    :Enable
STELNET IPv4 server                 :Enable
STELNET IPv6 server                 :Enable
SCP IPv4 server                     :Enable
SCP IPv6 server                     :Enable
SSH server source                   :0.0.0.0
ACL4 number                         :0
ACL6 number                         :0
```

Table 2-39 Description of the **display ssh server status** command output

Item	Description
SSH version	Protocol version used for the SSH session connection.
SSH connection timeout	Timeout interval of SSH server authentication, in seconds. Run the **ssh server timeout** command to set this item.
SSH server key generating interval	Interval for generating an SSH server password, in hours. Run the **ssh server rekey-interval** command to set this item.
SSH authentication retries	Number of times for retrying the SSH session connection. Run the **ssh server authentication-retries** command to set this item.
SFTP IPv4 server	SFTP IPv4 service status. Run the **sftp ipv4 server enable** command to set this item.
SFTP IPv6 server	SFTP IPv6 service status. Run the **sftp ipv6 server enable** command to set this item.
STELNET IPv4 server	STelnet IPv4 service status. Run the **stelnet ipv4 server enable** command to set this item.
STELNET IPv6 server	STelnet IPv6 service status. Run the **stelnet ipv6 server enable** command to set this item.
SCP IPv4 server	SCP IPv4 service status. Run the **scp ipv4 server enable** command to set this item.
SCP IPv6 server	SCP IPv6 service status. Run the **scp ipv6 server enable** command to set this item.

Item	Description
SSH server source	Source address of the SSH server. Run the **ssh server-source** command to set this item.
ACL4 number	ACL4 number of the SSH server. Run the **ssh server acl** *acl-number* command to set this item.
ACL6 number	ACL6 number of the SSH server. Run the **ssh ipv6 server acl** *acl-number* command to set this item.

Display the current session connection information on the SSH server.

```
<HUAWEI> display ssh server session
 Session 1:
     Conn                 : VTY 10
     Version              : 2.0
     State                : started
     Username             : client002
     Retry                : 1
     CTOS Cipher          : aes256-cbc
     STOC Cipher          : aes256-cbc
     CTOS Hmac            : hmac-sha2_256
     STOC Hmac            : hmac-sha2_256
     CTOS Compress        : none
     STOC Compress        : none
     Kex                  : diffie-hellman-group1-sha1
     Public Key           : rsa
     Service Type         : sftp
     Authentication Type  : password
 Session 2:
     Conn                 : VTY 14
     Version              : 2.0
     State                : started
     Username             : client001
     Retry                : 1
     CTOS Cipher          : aes256-cbc
     STOC Cipher          : aes256-cbc
     CTOS Hmac            : hmac-sha2_256
     STOC Hmac            : hmac-sha2_256
     CTOS Compress        : none
     STOC Compress        : none
     Kex                  : diffie-hellman-group1-sha1
     Public Key           : dsa
     Service Type         : stelnet
     Authentication Type  : password
```

Table 2-40 Description of the **display ssh server session** command output

Item	Description
Session	SSH session ID.
Conn	Connection used by the SSH session.
Version	Protocol version used for the SSH session connection.

Item	Description
State	Status of the SSH session connection.
Username	User name for SSH session connection. Run the **ssh user** command to set this item.
Retry	Number of times for retrying the SSH session connection. Run the **ssh server authentication-retries** command to set this item.
CTOS Cipher	Encryption algorithm name from client to server.
STOC Cipher	Encryption algorithm name from server to client.
CTOS Hmac	HMAC algorithm name from client to server.
STOC Hmac	HMAC algorithm name from server to client.
CTOS Compress	Whether data is compressed for transmission from client to server, which can be specified for SCP connection.
STOC Compress	Whether data is compressed for transmission from server to client, which can be specified for SCP connection.
Kex	Exchange algorithm name.
Public Key	Public key algorithm used for server authentication, which can be RSA, DSA, or ECC.
Service Type	Service type for an SSH user. The options are as follows: ● sftp ● stelnet ● all (including SCP, SFTP and STelnet) Run the **ssh user service-type** command to set this item.

Item	Description
Authentication Type	Authentication mode for an SSH user. The options are as follows: ● password ● rsa ● dsa ● ecc ● password-rsa (password and RSA) ● password-dsa (password and DSA) ● password-ecc (password and ECC) ● all (password, ECC, DSA, or RSA) Run the **ssh user authentication-type** command to set this item.

2.6.15 display ssh server-info

Function

The **display ssh server-info** command displays the binding between SSH servers and RSA, DSA, or ECC public keys when the current device works as an SSH client.

Format

display ssh server-info

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When the SSH client needs to authenticate the server, the server public key saved in the local host is used to authenticate the connected SSH server. If the authentication fails, you can run the **display ssh server-info** command to check that the server public key is correct.

Example

Display all bindings between the SSH servers and public keys on the SSH client.

```
<HUAWEI> display ssh server-info
Server Name(IP)              Server Public Key Type  Server public key name
______________________________________________________________________________

192.168.50.207               RSA                     192.168.50.207
192.168.50.204               DSA                     192.168.50.204
192.168.50.208               ECC                     192.168.50.208
```

Table 2-41 Description of the **display ssh server-info** command output

Item	Description
Server Name(IP)	Host name of the SSH server.
Server Public Key Type	Type of the public key on the SSH server.
Server public key name	Name of the public key on the SSH server.

2.6.16 display ssh user-information

Function

The **display ssh user-information** command displays the configuration of all SSH users.

Format

display ssh user-information [*username*]

Parameters

Parameter	Description	Value
username	Displays the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the SSH user name, bound RSA, DSA, or ECC public key name, and service type.

Example

Display the configuration of the SSH user named **client001**.

```
<HUAWEI> display ssh user-information client001
       User Name            : client001
       Authentication-type  : password
       User-public-key-name : -
       User-public-key-type : -
       Sftp-directory       : -
       Service-type         : stelnet
       Authorization-cmd    : No
```

Display the configuration of all SSH users.

```
<HUAWEI> display ssh user-information
  User 1:
       User Name            : client001
       Authentication-type  : password
       User-public-key-name : -
       User-public-key-type : -
       Sftp-directory       : -
       Service-type         : stelnet
       Authorization-cmd    : No
  User 2:
       User Name            : client002
       Authentication-type  : dsa
       User-public-key-name : dsakey001
       User-public-key-type : dsa
       Sftp-directory       : flash:
       Service-type         : sftp
       Authorization-cmd    : No
```

Table 2-42 Description of the **display ssh user-information** command output

Item	Description
User Name	SSH user name. Run the **ssh user** command to set this item.
Authentication-type	Authentication mode for an SSH user. The options are as follows: ● password ● rsa ● dsa ● ecc ● password-rsa (password and RSA) ● password-dsa (password and DSA) ● password-ecc (password and ECC) ● all (password, ECC, DSA, or RSA) Run the **ssh user authentication-type** command to set this item.
User-public-key-name	Peer RSA, DSA, or ECC public key assigned to an SSH user. Run the **rsa peer-public-key**, **dsa peer-public-key**, or **ecc peer-public-key** command to set this item.

Item	Description
User-public-key-type	The public key type for an SSH user can be RSA, DSA, or ECC.
Sftp-directory	SFTP service directory of an SSH user. Run the **ssh user sftp-directory** command to set this item.
Service-type	Service type for an SSH user. The options are as follows: ● sftp ● stelnet ● all: The service types are SFTP and STelnet. Run the **ssh user service-type** command to set this item.
Authorization-cmd	Command line authentication mode configured for an SSH user. Run the **ssh user authorization-cmd aaa** command to set this item.

2.6.17 display telnet server status

Function

The **display telnet server status** command displays the status and configuration of a Telnet server.

Format

display telnet server status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

- To check whether a device functions as a Telnet server, run the **display telnet server status** command.

- If you have set a port number for the Telnet server using the **telnet server port** *port-number* command, run **display telnet server status** command to check the port number.

Example

Display the status and configuration of the Telnet server.

```
<HUAWEI> display telnet server status
 TELNET IPv4 server                    :Enable
 TELNET IPv6 server                    :Enable
 TELNET server port                    :23
 TELNET server source address              :0.0.0.0
 ACL4 number                          :0
 ACL6 number                          :0
```

Table 2-43 Description of the **display telnet server status** command output

Item	Description
TELNET IPv4 server	IPv4 Telnet server.
TELNET IPv6 server	IPv6 Telnet server.
TELNET server port	Listening port number of the Telnet server.
TELNET Server Source address	Source address of the Telnet server
ACL4 number	ACL4 number of the Telnet server
ACL6 number	ACL6 number of the Telnet server

2.6.18 display telnet-client

Function

The **display telnet-client** command displays the source parameters when a device works as a Telnet client.

Format

display telnet-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After setting source parameters of a Telnet client, you can run this command to check the setting result. If you have not run the **telnet client-source** command, the default source IP address is 0.0.0.0.

Example

Display the source parameters of the device functioning as a Telnet client.

```
<HUAWEI> display telnet-client
 The source address of telnet client is 10.1.1.1
```

Table 2-44 Description of the **display telnet-client** command output

Item	Description
The source address of telnet client is 10.1.1.1	The source IP address of the Telnet client is 10.1.1.1.

2.6.19 dsa local-key-pair create

Function

The **dsa local-key-pair create** command generates the local DSA host key pairs.

Format

dsa local-key-pair create

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Compared with RSA, Digital Signature Algorithm (DSA) has a wider application in the SSH protocol. The asymmetric encryption system generates public and private keys to implement secure key exchange, thereby ensuring secure sessions.

If a DSA key exists, when you run this command, the system prompts you to confirm whether to change the original key. If you agree, the key in the new key pair is named ***device name*_Host_DSA**, for example, **HUAWEI_Host_DSA**. The local DSA private key is saved in PKCS#8 format to the hostkey_dsa file in the system NOR FLASH.

After you enter the command, the device prompts you to enter the number of bits in the host key. The length of a host key pair can be 2048. By default, the key length is 2048.

Precautions

This command is not saved in a configuration file and can take effect immediately after being run. After the device restarts, you do not need to run the command again.

To improve security of the device, it is recommended that you use a key pair of 2048 bits.

Example

Generate DSA key pairs on the device.

```
<HUAWEI> system-view
[HUAWEI] dsa local-key-pair create
Info: The key name will be: HUAWEI_Host_DSA.
Info: The key modulus can be any one of the following : 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

2.6.20 dsa local-key-pair destroy

Function

The **dsa local-key-pair destroy** command deletes local DSA host key pairs.

Format

dsa local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

DSA applies to SSH verification. The asymmetric encryption system generates public and private keys to implement secure key exchange, thereby ensuring secure sessions. You can run the **dsa local-key-pair create** command to generate local DSA keys. When local DSA keys are unnecessary, you can run the **dsa local-key-pair destroy** command to delete these keys.

Prerequisite

The local DSA keys have been created.

Configuration Impact

After you run this command, the ****_DSA** file that stores DSA keys on the device is cleared.

Precautions

The **dsa local-key-pair destroy** command takes effect once, and therefore will not be saved in the configuration file.

Example

Delete local DSA keys.

```
<HUAWEI> system-view
[HUAWEI] dsa local-key-pair destroy
Info: The name of the key which will be destroyed is
HUAWEI_Host_DSA.
Warning: These keys will be destroyed. Continue? [Y/N]:y
Info: Succeeded in destroying the DSA host keys.
```

2.6.21 dsa peer-public-key

Function

The **dsa peer-public-key** command configures an encoding format for a DSA public key and displays the DSA public key view.

The **undo dsa peer-public-key** command deletes a DSA public key.

By default, no encoding format is configured for a DSA public key.

Format

dsa peer-public-key *key-name* **encoding-type** { **der** | **openssh** | **pem** }

undo dsa peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the public key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
encoding-type	Specifies an encoding format for a DSA public key.	-
der	Specifies the Distinguished Encoding Rules (DER) format for a DSA public key. DER encodes data in hexadecimal format.	-
openssh	Specifies the OpenSSH format for a DSA public key. OpenSSH encodes data in base-64 format. OpenSSH is an encoding format based on PEM.	-
pem	Specifies the Privacy Enhanced Mail (PEM) format for a DSA public key. PEM encodes data in base-64 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you use a DSA public key for authentication, you must specify the public key of the corresponding client for an SSH user on the server. When the client logs in to the server, the server uses the specified public key to authenticate the client. You can also save the public key generated on the server to the client. Then the client can be successfully authenticated by the server when it logs in to the server for the first time.

Huawei data communications devices support the DER, OpenSSH and PEM formats for DSA keys. If you use a DSA key in non-DER/OpenSSH/PEM format, use a third-party tool to convert the key into a key in DER, OpenSSH or PEM format.

Because a third-party tool is not released with Huawei system software, DSA usability is unsatisfactory. In addition to DER and PEM, DSA keys need to support the OpenSSH format to improve DSA usability.

Third-party software, such as PuTTY, OpenSSH, and OpenSSL, can be used to generate DSA keys in different formats. The details are as follows:

- The PuTTY generate DSA keys in PEM format.
- The OpenSSH generates DSA keys in OpenSSH format.
- The OpenSSL generates DSA keys in DER format.

OpenSSL is an open source software. You can download related documents at the OpenSSL official website.

After you configure an encoding format for a DSA public key, Huawei data communications device automatically generates a DSA public key in the configured encoding format and enters the DSA public key view. Then, you can run the **public-key-code begin** command and manually copy the DSA public key generated on the peer device to the local device.

Follow-up Procedure

After you copy the DSA public key generated on the peer device to the local device, perform the following operations to exit the DSA public key view:

1. Run the **public-key-code end** command to return to the DSA public key view.
2. Run the **peer-public-key end** command to exit the DSA public key view and return to the system view.

Precautions

When you run the **undo dsa peer-public-key** command to delete a DSA public key:

- If the public key has been assigned to an SSH client, run the **undo ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to release the binding between the public key and the SSH client. If you do not release the binding between them, the **undo dsa peer-public-key** command will fail to delete the public key.
- If the name of the host public key of the SSH server to be connected is specified on the SSH client, you need to run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to delete the host public key of the SSH server. Otherwise, the DSA public key cannot be deleted.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Configure an encoding format for a DSA public key and enter the DSA public key view.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key 23 encoding-type der
[HUAWEI-dsa-public-key]
```

2.6.22 ecc local-key-pair create

Function

The **ecc local-key-pair create** command generates a local Elliptic Curves Cryptography (ECC) host key pair.

Format

ecc local-key-pair create

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A local key pair is a prerequisite to a successful SSH login. Compared with the RSA algorithm used by the **rsa local-key-pair create** command, the ECC algorithm shortens the key length, accelerates the encryption, and improves the security. The length of the server key pair and the host key pair can be 256 bits, 384 bits and 521 bits. By default, the length of the key pair is 521 bits.

Precautions

- The generated ECC host key pair is named in the format of switch name_Host_ECC, such as HUAWEI_Host_ECC. The local DSA private key is saved in PKCS#8 format to the hostkey_ecc file in the system NOR FLASH.
- The **ecc local-key-pair create** and **ecc local-key-pair destroy** commands are not saved in the configuration file. They only need to be run once and take effect even after the switch restarts.
- Do not delete the ECC key file from the switch. If the ECC key file is deleted, the ECC key pair cannot be restored after the switch is restarted.

Example

Generate a local ECC host key pair.

```
<HUAWEI> system-view
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The ECC host key named HUAWEI_Host_ECC already exists.
Warning: Do you want to replace it ? [Y/N]: Y
Info: The key modulus can be any one of the following : 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:521
Info: Generating keys...
Info: Succeeded in creating the ECC host keys.
```

Enter a key with incorrect length and re-enter the key with incorrect length for five times, which is the maximum number of retry attempts.

```
<HUAWEI> system-view
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The ECC host key named HUAWEI_Host_ECC already exists.
Warning: Do you want to replace it ?[Y/N]: Y
Info: The key modulus can be any one of the following : 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:123
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:1024
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:512
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:2048
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:4096
Error: Invalid ECC key modulus.
Error: The maximum number of retries has reached, and the command has already been canceled.
```

2.6.23 ecc local-key-pair destroy

Function

The **ecc local-key-pair destroy** command deletes the local Elliptic Curves Cryptography (ECC) keys.

Format

ecc local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you no longer need the local ECC key pairs, run the **ecc local-key-pair destroy** command to delete them.

Configuration Impact

After the **ecc local-key-pair destroy** command is run, the ECC key files on the device are cleared. Exercise caution when running the command.

Precautions

- The **ecc local-key-pair create** and **ecc local-key-pair destroy** commands are not saved in the configuration file. They only need to be run once and take effect even after the switch restarts.
- Do not delete the ECC key file from the switch. If the ECC key file is deleted, the ECC key pair cannot be restored after the switch is restarted.

Example

Delete the local ECC host key pair and server key pair.

```
<HUAWEI> system-view
[HUAWEI] ecc local-key-pair destroy
Info: The name of the key which will be destroyed is HUAWEI_Host_ECC.
Warning: These keys will be destroyed. Continue? [Y/N]:Y
Info: Succeeded in destroying the ECC host keys.
```

2.6.24 ecc peer-public-key

Function

The **ecc peer-public-key** command creates an ECC public key and enters the Elliptic Curves Cryptography (ECC) public key view.

The **undo ecc peer-public-key** command deletes an ECC public key.

By default, no ECC public key is created.

Format

ecc peer-public-key *key-name* **encoding-type** { **der** | **pem** | **openssh** }

undo ecc peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies an ECC public key name.	The value is a string of 1 to 30 case-sensitive characters, spaces not supported.

Parameter	Description	Value
encoding-type	Indicates the encoding type of an ECC public key.	-
der	Specifies DER as the encoding type of an ECC public key. If DER is specified, data is encoded in hexadecimal notation.	-
pem	Specifies PEM as the encoding type of an ECC public key. If PEM is specified, data is Base64 encoded.	-
openssh	Specifies OpenSSH as the encoding type of an ECC public key. If OpenSSH is specified, data is Base64 encoded. OpenSSH is derived from PEM.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When ECC public key authentication is used, a client's public key must be specified on the server for an SSH user. When the client logs in to the server, the server performs authentication on the client based on the public key of the SSH user.

After an ECC public key is created and the ECC public key view is displayed, run the **public-key-code begin** command, then you can manually copy the client's public key to the server.

The client's public key is randomly generated by the client software.

Follow-up Procedure

After copying the client's ECC public key to the server, run the following commands to quit the ECC public key view:

1. Run the **public-key-code end** command to return to the ECC public key view.
2. Run the **peer-public-key end** command to exit the ECC public key view and return to the system view.

Precautions

A maximum of 20 ECC public keys can be created.

When you run the **undo ecc peer-public-key** command to delete an ECC public key:

- If the public key has been assigned to an SSH client, run the **undo ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to release the binding between the public key and the SSH client. If you do not release the binding between them, the **undo dsa peer-public-key** command will fail to delete the public key.
- If the name of the host public key of the SSH server to be connected is specified on the SSH client, you need to run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to delete the host public key of the SSH server. Otherwise, the DSA public key cannot be deleted.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Create an ECC public key and enter the ECC public key view.

```
<HUAWEI> system-view
[HUAWEI] ecc peer-public-key ecc-peer-key encoding-type pem
Info: Enter "ECC public key" view, return system view with "peer-public-key end".
[HUAWEI-ecc-public-key] public-key-code begin
Info: Enter "ECC key code" view, return the last view with "public-key-code end".
[HUAWEI-ecc-key-code] ---- BEGIN SSH2 PUBLIC KEY ----
[HUAWEI-ecc-key-code]
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACDBL5J4v3pqi5S
[HUAWEI-ecc-key-code] ALI9lvLw4cdvtpD2AC6sEJXg9GDCD5vGBnkXlKmnOy6d1TyrXx57ZPNnrSdqVkHC
[HUAWEI-ecc-key-code] sMBa63vSwg1XsVW2qZgx8H57+FJiTPY61b1Vfst9GUif1ymfpB7XrbdYZDownoh0
[HUAWEI-ecc-key-code] FZNadZtIf2CRc0OeiKXbCSPP25dfoT/DTcc=
[HUAWEI-ecc-key-code] ---- END SSH2 PUBLIC KEY ----
[HUAWEI-ecc-key-code] public-key-code end
[HUAWEI-ecc-public-key] peer-public-key end
```

Delete an ECC public key.

```
<HUAWEI> system-view
[HUAWEI] undo ecc peer-public-key ecc-peer-key
Warning: The public key named ecc-peer-key will be deleted. Continue? [Y/N]:Y
```

2.6.25 free http user-id

Function

The **free http user-id** command configures a device to release web users.

Format

free http user-id *user-id*

Parameters

Parameter	Description	Value
user-id	Specifies the VTY ID of a web user to be released. You can run the **display users** command to query the VTY ID.	The value is an integer that ranges from 1 to 256.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A maximum of five web users are supported at present. If one of the five web users is logged out unexpectedly, the user's client keeps connection with the FTP server before the connection expires. During this period, other users cannot log in to the FTP server. To manually release the web user, run the **free http user-id** command.

Precautions

The **free http user-id** command is used only to release web users. **user-id** of web users ranges from 89 to 93, and a maximum of five users are allowed to stay online concurrently. If you set **user-id** to a value smaller than 89 or greater than 93, the message "Error: The specified user does not exist or is not an HTTP user." is displayed.

Example

Release the web user whose VTY ID is 89.

```
<HUAWEI> system-view
[HUAWEI] free http user-id 89
```

2.6.26 http acl

Function

The **http acl** command configures an ACL/ACL6 on the HTTP or HTTPS server.

The **undo http acl** command deletes the ACL/ACL6 on the HTTP or HTTPS server.

By default, no ACL/ACL6 is configured on the HTTP or HTTPS server.

Format

HTTP or HTTPS IPv4:

http acl *acl-number*

undo http acl

HTTP or HTTPS IPv6:

http ipv6 acl *acl6-number*

undo http ipv6 acl

Parameters

Parameter	Description	Value
acl-number	Specifies the ACL number for an HTTP or HTTPS IPv4 server.	The value is an integer that ranges from 2000 to 3999.
acl6-number	Specifies the ACL6 number for an HTTP or HTTPS IPv6 server.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of an HTTP or HTTPS server, you need to configure an ACL/ ACL6 for it to specify clients that can log in to the current HTTP or HTTPS server.

Precautions

- The **http acl** command takes effect only after you run the **rule** command to configure the ACL/ACL6 rule.
- After an ACL/ACL6 rule is modified, the HTTP or HTTPS server does not forcibly log out an online user who matches the ACL/ACL6 rule until the user sends the next login request.
- If the **http acl** command is configured several times, only the latest configuration takes effect.

Example

Set the ACL number to 2000 for the HTTP or HTTPS IPv4 server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule 1 permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] http acl 2000
```

Set the ACL6 number to 2000 for the HTTP or HTTPS IPv6 server.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule 1 permit source fc00:1::1 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] http ipv6 acl 2000
```

2.6.27 http secure-server enable

Function

The **http secure-server enable** command enables the HTTPS service function.

The **undo http secure-server enable** command disables the HTTPS service function.

The **http secure-server disable** command disables the HTTPS service function.

By default, the HTTPS IPv4 service function is enabled, and the HTTPS IPv6 service function is disabled.

Format

http [**ipv6**] **secure-server enable**

undo http [**ipv6**] **secure-server enable**

http [**ipv6**] **secure-server disable**

Parameters

Parameter	Description	Value
ipv6	Enables or disables the HTTPS IPv6 service function. If this parameter is not specified, the HTTPS IPv4 service function is enabled or disabled.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an SSL policy is loaded to an HTTPS server, the HTTPS server provides HTTPS service using SSL. The client and HTTPS server establish an SSL connection to protect user information from theft.

Prerequisites

The web page file has been loaded to the device.

Precautions

- After the HTTPS service is enabled, only authenticated users can use the web browser to access the web network management system to manage devices.
- After the HTTPS service is enabled, the SSL handshake negotiation is triggered.
- After the **http secure-server enable** command is run, the HTTPS server accepts only login requests from MEth0/0/1 or VLANIF1 by default. To allow authorized users to log in to the HTTPS server from other interfaces, you should run the **http server-source** command to specify the source interface of the HTTPS server.
- After the **http ipv6 secure-server enable** command is run, the HTTPS server does not accept login requests from any IPv6 address by default, you should run the **http ipv6 server-source** command to specify the IPv6 source address for the HTTPS server.

Example

Enable the HTTPS IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] http secure-server enable
```

Enable the HTTPS IPv6 service.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 secure-server enable
```

2.6.28 http secure-server port

Function

The **http secure-server port** command sets a port number for an HTTPS server.

The **undo http secure-server port** command restores the default port number of an HTTPS server.

By default, the port number of an HTTPS server is 443.

Format

http [**ipv6**] **secure-server port** *port-number*

undo http [**ipv6**] **secure-server port**

Parameters

Parameter	Description	Value
ipv6	Specifies the port number for an HTTPS IPv6 server. If this parameter is not specified, the command sets the port number for an HTTPS IPv4 server.	-

Parameter	Description	Value
port-number	Specifies the port number of an HTTPS server.	The value is 443 or an integer that ranges from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the port number of an HTTPS server is 443. Attackers may frequently access an HTTPS server through the default port, consuming bandwidth, deteriorating server performance, and causing authorized users unable to access the server. You can run the **http secure-server port** command to specify another port number to prevent attackers from accessing the default port.

Precautions

If the **http secure-server port** command is configured several times, only the latest configuration takes effect.

Example

Set the port number of an HTTPS IPv4 server to 8080.

```
<HUAWEI> system-view
[HUAWEI] http secure-server port 8080
```

Set the port number of an HTTPS IPv6 server to 8080.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 secure-server port 8080
```

2.6.29 http secure-server ssl-policy

Function

The **http secure-server ssl-policy** command configures an SSL policy for the HTTP server.

The **undo http secure-server ssl-policy** command restores the default SSL policy for the HTTP server.

A default SSL policy is available on an HTTP server.

Format

http secure-server ssl-policy *policy-name*

undo http secure-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Traditional HTTP service transmits data in plain text, which can be intercepted and tampered with. User identity cannot be authenticated, and the HTTP server cannot ensure online data security of applications such as the e-commerce and online banks. You can run the **http secure-server ssl-policy** command to configure an SSL policy for the HTTP server to encrypt data, authenticate user identity, and check message integrity to ensure data security during the web access.

Prerequisites

Before running the **http secure-server ssl-policy** command, you must first run the **ssl policy** command to create an SSL policy on the HTTP server.

Precautions

- The device provides a default SSL policy named **Default**. After the web page file is loaded to the device, the default SSL policy is loaded automatically, and you do not need to configure an SSL policy. To enhance device security, it is recommended that you obtain a new digital certificate from the CA and manually configure an SSL policy
- Only one SSL policy can be configured for the HTTP server, and the latest configured SSL policy takes effect.

Example

Configure an SSL policy for the HTTP server.

```
<HUAWEI> system-view
[HUAWEI] http secure-server ssl-policy http_server
```

2.6.30 http server enable

Function

The **http server enable** command enables the HTTP server function.

The **undo http server enable** command disables the HTTP server function.

The **http server disable** command disables the HTTP server function.

By default, the HTTP IPv4 server function is enabled, and the HTTP IPv6 server function is disabled.

Format

http [**ipv6**] **server enable**

undo http [**ipv6**] **server enable**

http [**ipv6**] **server disable**

Parameters

Parameter	Description	Value
ipv6	Enables or disables the HTTP IPv6 server function. If this parameter is not specified, the HTTP IPv4 server function is enabled or disabled.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After running the **http server enable** command to enable the HTTP server, you can use the browser to access the web NMS to manage devices.

If the web page to load does not exist, the HTTP service cannot be enabled.

Prerequisites

The HTTPS service has been enabled using the **http secure-server enable** command.

Precautions

- After the **http server enable** command is run, the HTTPS server accepts only login requests from MEth0/0/1 or VLANIF1 by default. To allow authorized users to log in to the HTTPS server from other interfaces, you should run the **http server-source** command to specify the source interface of the HTTP server.

- After the **http ipv6 server enable** command is run, the HTTP server does not accept login requests from any IPv6 address by default, you should run the **http ipv6 server-source** command to specify the IPv6 source address for the HTTP server.

Example

Enable the HTTP IPv4 server.

```
<HUAWEI> system-view
[HUAWEI] http secure-server enable
[HUAWEI] http server enable
Warning: HTTP is not a secure protocol, and it is recommended to use HTTPS.
Info: Succeeded in starting the HTTP server.
```

Enable the HTTP IPv6 server.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 secure-server enable
[HUAWEI] http ipv6 server enable
Warning: HTTP is not a secure protocol, and it is recommended to use HTTPS.
Info: Succeeded in starting the HTTP IPv6 server.
```

2.6.31 http server load

Function

The **http server load** command loads a web page file.

The **undo http server load** command cancels loading of a specified web page file.

By default, the web page file in the system software has been loaded to the devices.

Format

http server load { *file-name* | **default** }

undo http server load

Parameters

Parameter	Description	Settings
file-name	Specifies the name of the web page file to load. The web page file must be stored in the root directory of the storage device.	The value is a string of 4 to 64 characters without spaces. The file name is in the *.web.7z format.

Parameter	Description	Settings
default	Specifies the web page file in the current system software that is to be loaded.	–

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to manage and maintain devices on the graphical user interface (GUI), configure the Web network management function. When you need to update web page file when using the Web network management function, run this command to load web page file.

Prerequisites

Before loading the web page file using the **http server load** command, ensure that the web page file has been stored to the root directory of the storage device on the device; otherwise, file loading will fail.

Precautions

- If the system software is upgraded from V200R006 or an earlier version to V200R007 or a later version, but the target software version conflicts with the configuration file for next startup, the device will cancel the configuration of loading the web page file in the original system software after the upgrade, and loads the web page file integrated in the new system software by default.
- The web page file contains the SSL certificate, which is used to authenticate the HTTP server during login to ensure information security. When a user attempts to log in to the device through HTTP, the HTTPS login page is pushed to the user. After the user is authenticated, the system returns to the HTTP page. The SSL certificate is also used in the HTTPS login mode to ensure security of user information and data exchanged between the client and server. You can load a new digital certificate to the device.
- If the loaded web page file does not exist, the HTTP service cannot be enabled when the device restarts.
- To disable a loaded web page file, you must load another file.

Example

Load the web page file **web_1.web.7z**.

```
<HUAWEI> system-view
[HUAWEI] http server load web_1.web.7z
```

2.6.32 http server port

Function

The **http server port** command sets the listening port number of the HTTP server.

The **undo http server port** command restores the default listening port number of the HTTP server.

By default, the listening port number of the HTTP server is 80.

Format

http [**ipv6**] **server port** *port-number*

undo http [**ipv6**] **server port**

Parameters

Parameter	Description	Value
ipv6	Specifies a listening port number for an HTTP IPv6 server. If this parameter is not specified, the command configures a listening port number for an HTTP IPv4 server.	-
port-number	Specifies the listening port number of the HTTP server.	The value is 80, or an integer that ranges from 1025 to 55535. The default value is 80.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the listening port number of the security HTTP server is 80. Attackers may frequently access the default listening port, which wastes bandwidth, deteriorates server performance, and prevents authorized users from accessing the HTTP server through the listening port. You can run the **http server port** command to specify another listening port number to prevent attackers from accessing the listening port.

Precautions

If the **http server port** command is configured several times, only the latest configuration takes effect.

Example

Set the listening port number of the HTTP IPv4 server to 1025.

```
<HUAWEI> system-view
[HUAWEI] http server port 1025
```

Set the listening port number of the HTTP IPv6 server to 1500.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 server port 1500
```

2.6.33 http server-source

Function

The **http server-source** command specifies a source interface for an HTTP or HTTPS server.

The **undo http server-source** command cancels the source interface specified for an HTTP or HTTPS server.

By default, the source interface of an HTTP or HTTPS server is MEth0/0/1 or VLANIF 1. The web login is supported after the device enters the initial configuration mode. The source interface of an HTTP or HTTPS server is MEth0/0/1 or VLANIF 1..

Format

http server-source -i *interface-type interface-number*

undo http server-source

http server-source all-interface

Parameters

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface of an HTTP or HTTPS server.	-
all-interface	Indicates that any interface that has an IPv4 address configured can be used as the source interface of an HTTP or HTTPS server.	-

NOTE

In V200R020C00 and later versions, to allow authorized users to log in to the HTTP server through a non-management network port, run a command to specify the source interface of the HTTP server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an HTTP or HTTPS server receives connection requests from all interfaces by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an HTTP or HTTPS server accepts only login requests from MEth0/0/1 or VLANIF1 by default. To allow authorized users to log in to the HTTP or HTTPS server, run either of the following commands to specify the source interface of the HTTP or HTTPS server.

- Run the **http server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the HTTP or HTTPS server.
- Run the **http server-source all-interface** command to configure all interfaces configured with IPv4 addresses as the source interfaces of the HTTP or HTTPS server.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **http server-source** command cannot be successfully executed.

Configuration Impact

Users can log in to an HTTP or HTTPS server only from the specified source interface.

After you run **http server-source** command, the HTTP IPv4 user that has logged in to the server will be forcibly logged out and needs to log in again.

Precautions

After the source interface of an HTTP or HTTPS server is specified using the **http server-source** command, ensure that HTTP or HTTPS users can access the source interface at Layer 3. Otherwise, the HTTP or HTTPS users will fail to log in to the HTTP or HTTPS server.

After the **http server-source all-interface** command is run, the system allows HTTP or HTTPS users to log in to the HTTP or HTTPS server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Specify loopback 0 as the source interface of an HTTP or HTTPS server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] quit
[HUAWEI] http server-source -i loopback 0
Warning: The operation will reboot the HTTP server. Continue? [Y/N]:y
Info: Succeeded in setting the source interface of the HTTP server to
LoopBack0.
Info: Succeeded in starting the HTTP secure server.
Warning: HTTP is not a secure protocol, and it is recommended to use
HTTPS.
Info: Succeeded in starting the HTTP server.
```

2.6.34 http ipv6 server-source

Function

The **http ipv6 server-source** command specifies an IPv6 source address for an HTTP or HTTPS server.

The **undo http ipv6 server-source** command cancels the IPv6 source address specified for an HTTP or HTTPS server.

By default, the IPv6 source address of an HTTP or HTTPS server is not specified.

Format

http ipv6 server-source -a *ipv6_address* [**-vpn-instance** *vpn_name*]

undo http ipv6 server-source

http ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies the IPv6 source address for an HTTP or HTTPS server.	The total length of an IPv6 address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
-vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the HTTP or HTTPS server.	-

NOTE

In V200R020C00 and later versions, to allow authorized users to log in to the HTTP server through a non-management network port, run a command to specify the source interface of the HTTP server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an HTTP or HTTPS server receives connection requests from all interfaces by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an HTTP or HTTPS server does not accept login requests from any interface by default. To allow authorized users to log in to the HTTP or HTTPS server, run either of the following commands to specify the source interface of the HTTP or HTTPS server.

- Run the **http ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure the specified IPv6 address as the IPv6 source address of the HTTP or HTTPS server.
- Run the **http ipv6 server-source all-interface** command to configure all interface IPv6 addresses on the device as the IPv6 source addresses of the HTTP or HTTPS server.

Prerequisites

A VPN instance has been created before you specify it for an HTTP or HTTPS server. Otherwise, the **http ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for an HTTP or HTTPS server, HTTP or HTTPS users can log in to the HTTP or HTTPS server only using this IPv6 address. This configuration applies to the HTTP or HTTPS users who attempt to log in to the server, not to the HTTP or HTTPS users who have logged in to the server.

Precautions

After an IPv6 source address is specified for an HTTP or HTTPS server using this command, ensure that HTTP or HTTPS users can access this IPv6 address at Layer 3. Otherwise, HTTP or HTTPS users will fail to log in to the HTTP or HTTPS server.

If the specified IPv6 source address is bound to a VPN instance, the HTTP or HTTPS server is also bound to the VPN instance.

After the **http ipv6 server-source all-interface** command is run, the system allows HTTP or HTTPS users to log in to the HTTP or HTTPS server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for an HTTP or HTTPS server.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 server-source -a 2001:DB8::
```

2.6.35 http timeout

Function

The **http timeout** command sets the idle timeout duration of the web server.

The **undo http timeout** command restores the default idle timeout duration of the web server.

By default, the idle timeout duration of the web server is 20 minutes.

Format

http timeout *timeout*

undo http timeout

Parameters

Parameter	Description	Value
timeout	Specifies the idle timeout duration of the web server for online users.	The value is an integer that ranges from 1 to 60, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A maximum of five web users are supported at present. When the fifth web user logs in to the web server, any other user cannot log in to the web server even if any of the five users does not perform operations for a long time. The idle timeout duration is configured to release web resources in time. To occupy web channels for a long time, you must set the idle timeout duration to the maximum value.

Precautions

- After you run the **http timeout** command, the idle timeout durations are the same for all web users who log in to the web server. If the idle timeout duration expires, a user is disconnected from the web server and the web server notifies the user only after the user sends the next login request.
- If the **http timeout** command is configured several times, only the latest configuration takes effect.

Example

Set the idle timeout duration of the web server to 6 minutes.

```
<HUAWEI> system-view
[HUAWEI] http timeout 6
```

2.6.36 lock

Function

The **lock** command locks the current user interface to prevent unauthorized users from operating the interface.

By default, the system does not automatically lock the current user interface.

Format

lock

Parameters

None

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Lock the current user interface using this command to prevent other users from operating the interface. The user interface can be console or VTY.

After running the **lock** command, you are prompted to enter a password twice. If you enter the correct password twice, the user interface is locked.

Precautions

- The passwords must meet the following requirements:
  - The password must be a string of 8 to 16 case-sensitive characters.
  - The password must contain at least two types of the following characters: upper-case characters, lower-case characters, digits, and special characters.

    Special characters do not include the question mark (?) and space.
- The password entered in interactive mode is not displayed on the screen.
- You can press **CTRL_C** to cancel the password-based locking operation.
- To unlock the user interface, press **Enter**, and then enter the correct password as prompted.

Example

Lock the current user interface after logging in through the console port.

```
<HUAWEI> lock
Please configure the login password (8-16)
Enter Password:
Confirm Password:
Info: The terminal is locked.
```

To log in to the system again, press **Enter**. The following information is displayed:

```
Enter Password:
```

Enter the correct password and return to the user view.

```
<HUAWEI>
```

2.6.37 matched upper-view

Function

The **matched upper-view** command allows a device to search for the **undo** command in the upper view, and returns to the upper view.

The **undo matched upper-view** command prohibits a device from searching for the **undo** command in the upper view.

By default, a device does not search for the **undo** command in the upper view.

Format

matched upper-view

undo matched upper-view

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If the **matched upper-view** command is run, when you run an **undo** command that is not registered in the current view, a device searches for the **undo** in the upper view. If the device finds the same **undo** command, it executes this command in the upper view. If the device does not find the same **undo** command in the upper view, it continues to search for this command in more upper views till the system view.

Running this command brings security risks. For example, if you run the **undo ftp server** command in the interface view, while this command is not registered in the interface view, the device automatically searches for it in the upper view, that is, the system view, and disables the FTP function.

The **matched upper-view** command is valid only for current login users who run this command.

Example

Allow a device to search for the **undo** command in the upper view.

```
<HUAWEI> system-view
[HUAWEI] matched upper-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ftp server
Info: Succeeded in closing the FTP server.
```

Prohibit a device from searching for the **undo** command in the upper view.

```
<HUAWEI> system-view
[HUAWEI] undo matched upper-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ftp server
                               ^
Error: Unrecognized command found at '^' position.
```

2.6.38 peer-public-key end

Function

The **peer-public-key end** command returns to the system view from the public key view and saves the configured public keys.

Format

peer-public-key end

Parameters

None

Views

Public key view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You must save the public key generated on the remote host to the local host, which ensures that the validity check on the remote end is successful. After editing a public key in the public key view, you can run this command to return to the system view.

Prerequisites

Before you run this command, the **rsa peer-public-key** command has been run to enter the RSA public key view, the **dsa peer-public-key** command has been run to enter the DSA public key view, or the **ecc peer-public-key** command has been run to enter the ECC public key view.

Example

Return to the system view from the public key view.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key dsakey001 encoding-type der
[HUAWEI-dsa-public-key] public-key-code begin
[HUAWEI-dsa-key-code] 308188
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-dsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-dsa-key-code] 171896FB 1FFC38CD
[HUAWEI-dsa-key-code] 0203
[HUAWEI-dsa-key-code] 010001
```

```
[HUAWEI-dsa-key-code] public-key-code end
[HUAWEI-dsa-public-key] peer-public-key end
[HUAWEI]
```

2.6.39 public-key-code begin

Function

The **public-key-code begin** command displays the public key editing view.

Format

public-key-code begin

Parameters

None

Views

Public key view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure that the remote host passes the validity check performed by the local host, the public key generated on the remote host must be saved to the local host. To save the public key, run the **public-key-code begin** command to enter the public key editing view and then enter the key. The key characters can contain spaces. You can also press **Enter** to enter data in another line.

Prerequisite

A key name has been specified using the **rsa peer-public-key**, **dsa peer-public-key**, or **ecc peer-public-key** command.

Precautions

- The public key must be a hexadecimal character string in the public key encoding format, and generated by the client or server that supports SSH.
- The public key displayed using the **display rsa local-key-pair public**, **display dsa local-key-pair public**, or **display ecc local-key-pair public** command can be used as the key data to enter.
- The last line of the key cannot contain only spaces and dsa-key; otherwise, the spaces at the beginning of the lines that are entered will be automatically deleted, and an error will be reported after the **public-key-code end** command is run.

Example

Display the DSA public key editing view and enter the key data.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key dsakey001 encoding-type der
[HUAWEI-dsa-public-key] public-key-code begin
[HUAWEI-dsa-key-code] 308188
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-dsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-dsa-key-code] 171896FB 1FFC38CD
[HUAWEI-dsa-key-code] 0203
[HUAWEI-dsa-key-code] 010001
[HUAWEI-dsa-key-code] public-key-code end
[HUAWEI-dsa-public-key] peer-public-key end
[HUAWEI]
```

2.6.40 public-key-code end

Function

The **public-key-code end** command returns to the public key view from the public key editing view and saves the configured public key.

Format

public-key-code end

Parameters

None

Views

Public key editing view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this command is run, editing the public key ends. Before saving the public key, the system will check the validity of the key.

- If there are illegal characters in the public key configured by the user, the system displays an error prompt. The public key is then discarded, and the configuration fails.
- If the public key configured is valid, it is saved in the public key chain table of the host.

Prerequisites

Before you run this command, the **public-key-code begin** command has been run to enter the public key edit view.

Precautions

- Generally, in the public key view, only the **public-key-code end** command can be used to exit. The **quit** command cannot be used.
- If no valid key coding is input, the key cannot be generated after the **public-key-code end** command is used. The system prompts that key generation fails.
- If the key has been deleted in another window, when you run the **public-key-code end** command, the system prompts that the key does not exist and returns to the system view.

Example

Exit the DSA public key editing view and saves the DSA key configuration.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key dsakey001 encoding-type der
[HUAWEI-dsa-public-key] public-key-code begin
[HUAWEI-dsa-key-code] 308188
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-dsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-dsa-key-code] 171896FB 1FFC38CD
[HUAWEI-dsa-key-code] 0203
[HUAWEI-dsa-key-code] 010001
[HUAWEI-dsa-key-code] public-key-code end
[HUAWEI-dsa-public-key] peer-public-key end
[HUAWEI]
```

2.6.41 rsa local-key-pair create

Function

The **rsa local-key-pair create** command generates the local RSA host and server key pairs.

By default, the local RSA host and server key pairs are not configured.

Format

rsa local-key-pair create

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement secure data exchange between the server and client, run the **rsa local-key-pair create** command to generate a local key pair.

Precautions

If the RSA key pair exists, the system prompts you to confirm whether to replace the original key pair. The keys in the new key pair are named **device name_Server** and **device name_Host**, for example, HUAWEI_Host and HUAWEI_Server. After being encrypted by AES256, the local RSA private key is saved to the hostkey and serverkey files in the system NOR FLASH.

After you run this command, the system prompts you to enter the number of bits in the host key. The difference between the bits in the server and host key pairs must be at least 128 bits. The length of the server or host key pair is 2048 ~ 4096 bits.

After you run this command, the generated key pair is saved in the device and will not be lost after the device restarts.

To improve security of the device, it is recommended that you use a key pair of 4096 bits.

This command is not saved in a configuration file.

Example

Generate the local RSA host and server key pairs.

```
<HUAWEI> system-view
[HUAWEI] rsa local-key-pair create
The key name will be: HUAWEI_Host
The range of public key size is (2048 ~ 4096).
NOTES: If the key modulus is greater than 512,
       it will take a few minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
......................++++++++
.......................................................++++++++
........+++++++++
.....+++++++++
```

2.6.42 rsa local-key-pair destroy

Function

The **rsa local-key-pair destroy** command deletes all local RSA host and server key pairs.

Format

rsa local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete the local key pairs, run **rsa local-key-pair destroy** command. If the host key pair and server key pair of an SSH server are deleted, run the **rsa local-key-pair create** command to create a new host key pair and server key pair for the SSH server.

After you run this command, verify that all local RSA keys are deleted. This command is not saved in a configuration file.

Prerequisite

The local RSA key pairs that can be deleted exist.

Example

Delete all RSA server key pairs.

```
<HUAWEI> system-view
[HUAWEI] rsa local-key-pair destroy
% The name for the keys which will be destroyed is HUAWEI_Host.
% Confirm to destroy these keys? [y/n]:y
Destroying keys............Succeeded.
```

2.6.43 rsa peer-public-key

Function

The **rsa peer-public-key** command configures an encoding format for an RSA public key and displays the RSA public key view.

The **undo rsa peer-public-key** command deletes an RSA public key.

By default, the encoding format is distinguished encoding rules (DER) for an RSA public key.

Format

rsa peer-public-key *key-name* [**encoding-type** { **der** | **openssh** | **pem** }]

undo rsa peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the RSA public key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
encoding-type	Specifies the encoding format of an RSA public key.	-
der	Specifies the DER format of an RSA public key. DER encodes data in hexadecimal format.	-
openssh	Specifies the OpenSSH format of an RSA public key. OpenSSH encodes data in base-64 format. OpenSSH is an encoding format based on PEM.	-
pem	Specifies the PEM format of an RSA public key. PEM encodes data in base-64 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you use an RSA public key for authentication, you must specify the public key of the corresponding client for an SSH user on the server. When the client logs in to the server, the server uses the specified public key to authenticate the client. You can also save the public key generated on the server to the client. Then the client can be successfully authenticated by the server when it logs in to the server for the first time.

Huawei data communications devices support the DER, OpenSSH and PEM formats for RSA keys. If you use an RSA key in non-DER/OpenSSH/PEM format, use a third-party tool to convert the key into a key in DER, OpenSSH or PEM format.

Because a third-party tool is not released with Huawei system software, RSA usability is unsatisfactory. In addition to DER, RSA keys need to support the privacy-enhanced mail (PEM) and OpenSSH formats to improve RSA usability.

Third-party software, such as PuTTY, OpenSSH, and OpenSSL, can be used to generate RSA keys in different formats. The details are as follows:

- The PuTTY generate RSA keys in PEM format.
- The OpenSSH generates RSA keys in OpenSSH format.
- The OpenSSL generates RSA keys in DER format.

OpenSSL is an open source software. You can download related documents at the OpenSSL official website.

After you configure an encoding format for an RSA public key, Huawei data communications device automatically generates an RSA public key in the configured encoding format and enters the RSA public key view. Then you can run the **public-key-code begin** command and manually copy the RSA public key generated on the peer device to the local device.

Prerequisite

The RSA public key in hexadecimal notation on the remote host has been obtained and recorded.

Follow-up Procedure

After you copy the RSA public key generated on the peer device to the local device, perform the following operations to exit the RSA public key view:

1. Run the **public-key-code end** command to return to the RSA public key view.
2. Run the **peer-public-key end** command to exit the RSA public key view and return to the system view.

Precautions

When you run the **undo rsa peer-public-key** command to delete a public key:

- If the public key has been assigned to an SSH client, run the **undo ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to release the binding between the public key and the SSH client. If you do not release the binding between them, the **undo dsa peer-public-key** command will fail to delete the public key.
- If the name of the host public key of the SSH server to be connected is specified on the SSH client, you need to run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to delete the host public key of the SSH server. Otherwise, the DSA public key cannot be deleted.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Display the RSA public key view.

```
<HUAWEI> system-view
[HUAWEI] rsa peer-public-key rsakey001
[HUAWEI-rsa-public-key]
```

Configure an encoding format for an RSA public key and enter the RSA public key view.

```
<HUAWEI> system-view
[HUAWEI] rsa peer-public-key RsaKey001 encoding-type openssh
[HUAWEI-rsa-public-key]
```

2.6.44 run

Function

The **run** command runs a user view command in the system view.

By default, a user view command cannot be run in the system view.

Format

run *command-line*

Parameters

Parameter	Description	Value
command-line	Specifies a command to be run.	-

Views

All views except the user view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Some commands can be run only in the user view. To run these commands, you must return to the user view first. To facilitate command execution, the device allows you to run the **run** command to run such commands in the other views without returning to the user view.

Precautions

- The command specified in the **run** command can be run in the user view.
- When you run the **run** command, the association help function is unavailable.
- When you check the command history on the device using the **display history-command** command, only the commands that you enter are recorded. The command format is **run** *command-line*.

- When you check log information using the **SHELL/5/CMDRECORD** command, only the commands that are actually run are recorded in logs. The command format is **run** *command-line*.

Example

Run the **dir *.cfg** command to check the .cfg file in the system view.

```
<HUAWEI> system-view
[HUAWEI] run dir *.cfg
Directory of flash:/
  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         11,970  Mar 14 2012 19:11:22   31.cfg
    1  -rw-         12,033  Apr 22 2012 17:10:30   31_new.cfg
509,256 KB total (118,784 KB free)
```

2.6.45 send

Function

The **send** command configures a device to send messages to all user interfaces.

Format

send { **all** | *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
all	Specifies that the device sends messages to all user interfaces.	-
ui-number	Specifies the absolute number of a user interface.	The minimum value is 0. The maximum value is the number of the user interfaces that the device supports minus 1.
ui-type	Specifies the type of a user interface.	-
ui-number1	Specifies the relative number of a user interface.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

After you run the **send** command on a device, the device prompts you to enter a message to send. After you confirm to send this message, the user who logs in to the device from a specified user interface can receive this message.

Example

Send a message to the user interface VTY 0.

```
<HUAWEI> send vty 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
Hello, good morning!
Warning: Send the message? [Y/N]: y
```

After you confirm to send the message, the user who logs in to the HUAWEI from VTY 0 can receive this message.

```
<HUAWEI>
Info: Receive a message from VTY2:Hello, good morning!
```

2.6.46 ssh authentication-type default password

Function

The **ssh authentication-type default password** command configures password authentication as the default authentication mode for SSH users.

The **undo ssh authentication-type default password** command cancels the default password authentication mode for SSH users.

By default, the default authentication mode of SSH users is password authentication.

Format

ssh authentication-type default password

undo ssh authentication-type default password

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When there are multiple SSH users, the default password authentication mode simplifies the configuration.

When a TACACS server is used to authenticate a user who uses SSH to log in to a device, the network administrator must specify the SSH user on the TACACS server. In most cases, the SSH server cannot obtain the user information from the TACACS server. In this situation, you can set the authentication mode to **password**. SSH users can then directly log in to the device without additional SSH user configurations on the device.

Precautions

To configure password authentication for a specific SSH user, you can also run the **ssh user** *user-name* **authentication-type password** command.

Example

Configure password authentication as the default authentication mode for SSH users.

```
<HUAWEI> system-view
[HUAWEI] ssh authentication-type default password
```

2.6.47 ssh authorization-type default aaa

Function

The **ssh authorization-type default aaa** command configures the AAA authorization function for the SSH public key authentication user.

The **undo ssh authorization-type default aaa** command cancels the AAA authorization function configured for the SSH public key authentication user.

By default, the AAA authorization function is not configured for the SSH public key authentication user.

Format

ssh authorization-type default aaa

undo ssh authorization-type default aaa

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The SSH public key authentication user is an SSH user that uses the elliptic curve cryptography (ECC), Rivest-Shamir-Adleman (RSA), or digital signature algorithm (DSA) authentication mode.

If the AAA authorization function is not configured for the SSH public key authentication user, the SSH public key authentication user uses the level of the involved VTY channel. After the AAA authorization function is configured for the SSH public key authentication user, if the authorization succeeds, the SSH public key authentication user uses the level returned by the AAA. If the authorization fails, the user still uses the level of the involved VTY channel.

Precautions

AAA authorization configuration succeeds for the SSH public key authentication user if the following conditions are met:

- A local authorization scheme is configured for the default domain of the AAA management user.
- A local user exists, and the SSH access type is configured.

Example

Configure the AAA authorization function for the SSH public key authentication user.

```
<HUAWEI> system-view
[HUAWEI] ssh authorization-type default aaa
```

2.6.48 ssh client assign

Function

The **ssh client assign** command specifies the host public key of an SSH server on an SSH client.

The **undo ssh client assign** command cancels the specified host public key of the SSH server on the SSH client.

By default, the host public key of a server is not specified on clients.

Format

ssh client *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *keyname*

undo ssh client *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }

Parameters

Parameter	Description	Value
servername	Specifies the host name or IP address of an SSH server.	The value is a string of 1 to 255 characters without spaces.

Parameter	Description	Value
rsa-key	Specifies the RSA public key.	-
dsa-key	Specifies the DSA public key.	-
ecc-key	Specifies the ECC public key.	-
keyname	Specifies the SSH server public key name that has been configured on an SSH client.	The value is a string of 1 to 30 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an SSH client connects to an SSH server for the first time and first authentication is not enabled on the SSH client using the **ssh client first-time enable** command, the SSH client must determine whether the server is reliable. To do so, run the **ssh client assign** command to specify the host public key of the SSH server and the mapping between the key and SSH server on the SSH client. The client then uses the correct public key to determine whether the server is reliable based on the mapping.

Precautions

The name of the RSA, DSA, or ECC public key to be assigned to the SSH server must be the same as that configured on the SSH client. This public key must have been configured on the SSH server using the **rsa peer-public-key**, **dsa peer-public-key**, or **ecc peer-public-key** command. If either of the preceding conditions is not met, RSA, DSA, or ECC public key authentication of the SSH server fails on the SSH client.

To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Example

Assign the DSA public key to the SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh client 10.164.39.120 assign dsa-key sshdsakey01
```

Delete the DSA public key of the SSH server.

```
<HUAWEI> system-view
[HUAWEI] undo ssh client 10.164.39.120 assign dsa-key
```

2.6.49 ssh client cipher

Function

The **ssh client cipher** command configures an encryption algorithm list for an SSH client.

By default, the WEAKEA plug-in is not installed; the SSH client supports only the **aes128_ctr** and **aes256_ctr** algorithms; the **undo ssh client cipher** command cannot be used. After the WEAKEA plug-in is installed, the **aes256_cbc**, **aes128_cbc**, **3des_cbc**, and **des_cbc** algorithms are supported, and the **undo ssh client cipher** command can be used.

Format

ssh client cipher { **aes128_ctr** | **aes256_ctr** } *

Parameters

Parameter	Description	Value
aes128_ctr	Specifies the CTR AES128 encryption algorithm.	-
aes256_ctr	Specifies the CTR AES256 encryption algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an encryption algorithm for the packets exchanged between them. You can run the **ssh client cipher** command to configure an encryption algorithm list for the SSH client. After the SSH server receives a packet from the client, the server matches the encryption algorithm list of the client against its local list and selects the first matched encryption algorithm. If no encryption algorithm matches, the negotiation fails.

Precautions

The following encryption algorithms are listed in descending order of security level: **aes256_ctr** and **aes128_ctr**.

The system software does not support the **aes256_cbc**, **aes128_cbc**, **3des_cbc,** and **des_cbc** parameters. To use these parameters, you need to install the

WEAKEA plug-in. To ensure high security, you are advised to configure the **aes256_ctr** or **aes128_ctr** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure CTR encryption algorithms for an SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client cipher aes128_ctr aes256_ctr
```

2.6.50 ssh client first-time enable

Function

The **ssh client first-time enable** command enables the first authentication function on an SSH client.

The **undo ssh client first-time enable** command disables the first authentication function on the SSH client.

By default, the first authentication function is disabled on the SSH client.

Format

ssh client first-time enable

undo ssh client first-time enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSH client accesses an SSH server for the first time and the public host key of the SSH server is not configured on the SSH client, run the **ssh client first-time enable** command to enable the first authentication function. The SSH client then can access the SSH server and save the public host key on the SSH client. When the SSH client accesses the SSH server next time, the saved public host key is used to authenticate the SSH server.

Precautions

To log in to the SSH server successfully at the first time, you can also run the **ssh client assign** command to pre-assign a public host key to the SSH server. When you use STelnet or SFTP to connect to the server, you need to specify the public key authentication algorithm for server authentication as the ECC, RSA, or DSA key algorithm.

Example

Enable the first authentication function on the SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client first-time enable
```

2.6.51 ssh client hmac

Function

The **ssh client hmac** command configures an HMAC algorithm list for an SSH client.

By default, the WEAKEA plug-in is not installed, an SSH client supports only the **sha2_256** algorithm, and the **undo ssh client hmac** command is unavailable. When the WEAKEA plug-in is installed, an SSH client also supports the **sha2_256_96**, **sha1**, **sha1_96**, **md5** and **md5_96** algorithms, and the **undo ssh client hmac** command is available.

Format

ssh client hmac { **sha2_256** }

Parameters

Parameter	Description	Value
sha2_256	Specifies the SHA2_256 algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an HMAC algorithm for the packets exchanged between them. You can run the **ssh client hmac** command to configure an HMAC algorithm list for the SSH client. After the SSH server receives a packet from the client, the server matches the list of the client against its local list and selects the first matched HMAC algorithm. If no matched HMAC algorithms, the negotiation fails.

Precautions

The system software does not support the **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96** parameters. To use these parameters, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2_256** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure the **SHA2_256** algorithm for an SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client hmac sha2_256
```

2.6.52 ssh client key-exchange

Function

The **ssh client key-exchange** command configures a key exchange algorithm list for an SSH client.

By default, the WEAKEA plug-in is not installed, an SSH client supports only the **dh_group14_sha256**, **dh_group15_sha512**, **dh_group16_sha512**, **dh_group_exchange_sha256**, **ecdh_sha2_nistp256**, **ecdh_sha2_nistp384**, and **ecdh_sha2_nistp521** algorithm, and the **undo ssh client key-exchange** command is unavailable. When the WEAKEA plug-in is installed, an SSH client also supports the **dh_group14_sha1**, **dh_group1_sha1**, and **dh_group_exchange_sha1** algorithms, and the **undo ssh client key-exchange** command is available.

Format

ssh client key-exchange { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*

Parameters

Parameter	Description	Value
dh_group14_sha256	Adds the diffie-hellman-group14_sha256 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group15_sha512	Adds the diffie-hellman-group15_sha512 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group16_sha512	Adds the diffie-hellman-group16_sha512 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group_exchange_sha256	Adds the diffie-hellman-group_exchange_sha256 algorithm to the key exchange algorithm list of an SSH client.	-
ecdh_sha2_nistp256	Adds the ecdh_sha2_nistp256 algorithm to the key exchange algorithm list of an SSH client.	-
ecdh_sha2_nistp384	Adds the ecdh_sha2_nistp384 algorithm to the key exchange algorithm list of an SSH client.	-

Parameter	Description	Value
ecdh_sha2_nistp521	Adds the ecdh_sha2_nistp521 algorithm to the key exchange algorithm list of an SSH client.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate a key exchange algorithm for the packets exchanged between them. You can run the **ssh client key-exchange** command to configure a key exchange algorithm list for the SSH client. The server compares the key exchange algorithm list sent by the client with its own key exchange algorithm list, and selects the first key exchange algorithm on the client's list that matches a key exchange algorithm on its own list as the key exchange algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

Precautions

The following key exchange algorithms are listed in descending order of security level: **dh_group_exchange_sha256**, **ecdh_sha2_nistp521**, **ecdh_sha2_nistp384**, **ecdh_sha2_nistp256**, **dh_group16_sha512**, **dh_group15_sha512**, and **dh_group14_sha256**.

The system software does not contain the **dh_group_exchange_sha1**, **dh_group14_sha1**, and **dh_group1_sha1** parameters. To use these parameters, you need to install the WEAKEA plug-in. However, the algorithms specified by these parameters are less secure. For higher security purposes, you are advised to use other parameters. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

NOTICE

The higher the security level of a key exchange algorithm, the longer the time required by the device to calculate the key.

Example

Add two key exchange algorithms **dh_group_exchange_sha256** and **dh_group14_sha256** to the key exchange algorithm list of the SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client key-exchange dh_group_exchange_sha256 dh_group14_sha256
```

2.6.53 ssh client rekey

Function

The **ssh client rekey** command configures key renegotiation parameters for an SSH client.

The **undo ssh client rekey** command restores the default key renegotiation parameter settings of the SSH client.

By default, the interval at which an SSH client triggers key renegotiation is 60 minutes, the maximum size of data sent and received by an SSH client during key renegotiation is 1000 MB, and a maximum of 268435456 (2^28) packets can be sent and received by an SSH client during key renegotiation.

Format

ssh client rekey { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *

undo ssh client rekey { **time** | **data-limit** | **max-packet** } *

Parameters

Parameter	Description	Value
time *rekey-time*	Specifies an interval at which key renegotiation is triggered.	The value is an integer ranging from 30 to 1440, in minutes.
data-limit *data-limit*	Specifies the maximum size of data sent and received during key renegotiation.	The value is an integer ranging from 100 to 10000, in MB.
max-packet *max-packet*	Specifies the maximum number of packets sent and received during key renegotiation.	The value is an integer ranging from 268435456 to 2147483648.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the SSH session duration reaches the specified interval at which key renegotiation is triggered, the system renegotiates a key and uses the new key to establish SSH session connections, improving system security.

If the **time** parameter is configured for an SSH client, the client sends a key renegotiation packet to the server to renegotiate an encryption key when the SSH session duration reaches the specified interval.

If the **data-limit** parameter is configured for an SSH client, the client sends a key renegotiation packet to the server to renegotiate an encryption key when the size of sent and received data exceeds the maximum value.

If the **max-packet** parameter is configured for an SSH client, the client sends a key renegotiation packet to the server to renegotiate an encryption key when the number of sent and received packets exceeds the maximum value.

Precautions

A key renegotiation request is initiated when either an SSH client or server meets the key renegotiation criteria. After one party initiates such a request, the other party responds.

Example

Set the maximum size of data sent and received by the SSH client during key renegotiation to 2000 MB.

```
<HUAWEI> system-view
[HUAWEI] ssh client rekey data-limit 2000
```

2.6.54 ssh server acl

Function

The **ssh server acl** command configures an ACL that the SSH server uses to control the access permission of SSH clients.

The **undo ssh server acl** command cancels the configured ACL of the SSH server.

By default, no ACL is configured for SSH servers.

Format

ssh [**ipv6**] **server acl** *acl-number*

undo ssh [**ipv6**] **server acl**

Parameters

Parameter	Description	Value
acl-number	Specifies an ACL number.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Configure the ACL for the following servers for access control:

- STelnet server: controls which clients can log in to this server through STelnet.
- SFTP server: controls which clients can log in to this server through SFTP.
- SCP server: controls which clients can log in to this server through SCP.

Prerequisites

An ACL has been configured using the **acl (system view)** command in the system view, and an ACL rule has been configured using the **rule (basic ACL view)** or **rule (advanced ACL view)** command.

Precautions

A basic ACL can be configured to restrict source addresses. An advanced ACL can be configured to restrict source and destination addresses.

Example

Configure ACL 2000 on an SSH server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.10 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] ssh server acl 2000
```

2.6.55 ssh server authentication-retries

Function

The **ssh server authentication-retries** command sets the maximum number of authentication retries for an SSH connection.

The **undo ssh server authentication-retries** command restores the default maximum number of authentication retries for an SSH connection.

The default maximum number of authentication retries for an SSH connection is 3.

Format

ssh server authentication-retries *times*

undo ssh server authentication-retries

Parameters

Parameter	Description	Value
times	Specifies the maximum number of authentication retries for an SSH connection.	The value is an integer that ranges from 1 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the maximum number of authentication retries for an SSH connection, run the **ssh server authentication-retries** command. This prevents server overload due to numerous malicious access requests.

Precautions

The configured number of retries takes effect upon the next login.

Example

Set the maximum number of authentication retries to 4.

```
<HUAWEI> system-view
[HUAWEI] ssh server authentication-retries 4
```

2.6.56 ssh server authentication-type keyboard-interactive enable

Function

The **ssh server authentication-type keyboard-interactive enable** command enables keyboard interactive authentication on an SSH server.

The **undo ssh server authentication-type keyboard-interactive enable** command disables keyboard interactive authentication on an SSH server.

By default, keyboard interactive authentication is enabled on SSH servers.

Format

ssh server authentication-type keyboard-interactive enable

undo ssh server authentication-type keyboard-interactive enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To log in to the SSH server in keyboard interactive authentication mode, run the **ssh server authentication-type keyboard-interactive enable** command.

To log in to the SSH server in password authentication mode, run the **undo ssh server authentication-type keyboard-interactive enable** command to disable keyboard interactive authentication.

Example

Enable keyboard interactive authentication on an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server authentication-type keyboard-interactive enable
```

2.6.57 ssh server cipher

Function

The **ssh server cipher** command configures an encryption algorithm list for an SSH server.

By default, the WEAKEA plug-in is not installed; the SSH server supports only the **aes128_ctr** and **aes256_ctr** algorithms; the **undo ssh server cipher** command cannot be used. After the WEAKEA plug-in is installed, the **aes256_cbc**, **aes128_cbc**, **3des_cbc**, and **des_cbc** algorithms are supported, and the **undo ssh server cipher** command can be used.

Format

ssh server cipher { **aes128_ctr** | **aes256_ctr** } *

Parameters

Parameter	Description	Value
aes128_ctr	Specifies the CTR AES128 encryption algorithm.	-
aes256_ctr	Specifies the CTR AES256 encryption algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an encryption algorithm for the packets exchanged between them. You can run the **ssh server cipher** command to configure an encryption algorithm list for the SSH server. After the SSH server receives a packet from the client, the server matches the encryption algorithm list of the client against its local list and selects the first matched encryption algorithm. If no encryption algorithm matches, the negotiation fails.

Precautions

The following encryption algorithms are listed in descending order of security level: **aes256_ctr** and **aes128_ctr**.

The system software does not support the **aes256_cbc**, **aes128_cbc**, **3des_cbc,** and **des_cbc** parameters. To use these parameters, you need to install the WEAKEA plug-in. To ensure high security, you are advised to configure the **aes256_ctr** or **aes128_ctr** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.

- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure CTR encryption algorithms for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server cipher aes256_ctr aes128_ctr
```

2.6.58 ssh server dh-exchange min-len

Function

The **ssh server dh-exchange min-len** command configures the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client.

The **undo ssh server dh-exchange min-len** command restores the default minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client.

By default, the minimum key length supported is 1024 bytes.

Format

ssh server dh-exchange min-len *min-len*

undo ssh server dh-exchange min-len

Parameters

Parameter	Description	Value
min-len	Specifies the minimum Diffie-hellman-group-exchange key length supported on the SSH server.	The value can be either 1024, 2048 or 3072, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Diffie-hellman-group-exchange key of 1024 bytes poses security risks. If the SSH client supports the Diffie-hellman-group-exchange key of more than 1024 bytes, run the **ssh server dh-exchange min-len** command to set the minimum key length to 2048 bytes to improve security.

Precautions

Security risks exist if the minimum Diffie-hellman-group-exchange key length is less than 2048 bytes. You are advised to set the minimum key length to 2048 bytes.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.

```
<HUAWEI> system-view
[HUAWEI] ssh server dh-exchange min-len 2048
```

2.6.59 ssh server hmac

Function

The **ssh server hmac** command configures an HMAC algorithm list for an SSH server.

By default, the WEAKEA plug-in is not installed, an SSH server supports only the **sha2_256** algorithm, and the **undo ssh server hmac** command is unavailable. When the WEAKEA plug-in is installed, an SSH server also supports the **sha2_256_96**, **sha1**, **sha1_96**, **md5** and **md5_96** algorithms, and the **undo ssh server hmac** command is available.

Format

ssh server hmac {**sha2_256** }

Parameters

Parameter	Description	Value
sha2_256	Specifies the SHA2_256 algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an HMAC algorithm for the packets exchanged between them. You can run the **ssh server hmac** command to configure an HMAC algorithm list for the SSH server. After the server receives a packet from the client, the server matches the list of the client against its local list and selects the first matched HMAC algorithm. If no matched HMAC algorithms, the negotiation fails.

Precautions

The system software does not support the **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96** parameters. To use these parameters, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2_256** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure the **SHA2_256** algorithm for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server hmac sha2_256
```

2.6.60 ssh server key-exchange

Function

The **ssh server key-exchange** command configures a key exchange algorithm list for an SSH server.

By default, the WEAKEA plug-in is not installed, an SSH server supports only the **dh_group14_sha256**, **dh_group15_sha512**, **dh_group16_sha512**, **dh_group_exchange_sha256**, **ecdh_sha2_nistp256**, **ecdh_sha2_nistp384**, and **ecdh_sha2_nistp521** algorithm, and the **undo ssh server key-exchange** command is unavailable. When the WEAKEA plug-in is installed, an SSH server also supports the **dh_group14_sha1**, **dh_group1_sha1**, and **dh_group_exchange_sha1** algorithms, and the **undo ssh server key-exchange** command is available.

Format

ssh server key-exchange { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*

Parameters

Parameter	Description	Value
dh_group14_sha256	Adds the diffie-hellman-group14_sha256 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group15_sha512	Adds the diffie-hellman-group15_sha512 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group16_sha512	Adds the diffie-hellman-group16_sha512 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group_exchange_sha256	Adds the diffie-hellman-group_exchange_sha256 algorithm to the key exchange algorithm list of an SSH server.	-
ecdh_sha2_nistp256	Adds the ecdh_sha2_nistp256 algorithm to the key exchange algorithm list of an SSH server.	-
ecdh_sha2_nistp384	Adds the ecdh_sha2_nistp384 algorithm to the key exchange algorithm list of an SSH server.	-

Parameter	Description	Value
ecdh_sha2_nistp521	Adds the ecdh_sha2_nistp521 algorithm to the key exchange algorithm list of an SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate a key exchange algorithm for the packets exchanged between them. You can run the **ssh server key-exchange** command to configure a key exchange algorithm list for the SSH server. The server compares the key exchange algorithm list sent by the client with its own key exchange algorithm list, and selects the first key exchange algorithm on the client's list that matches a key exchange algorithm on its own list as the key exchange algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

Precautions

The following key exchange algorithms are listed in descending order of security level: **dh_group_exchange_sha256**, **ecdh_sha2_nistp521**, **ecdh_sha2_nistp384**, **ecdh_sha2_nistp256**, **dh_group16_sha512**, **dh_group15_sha512**, and **dh_group14_sha256**.

The system software does not contain the **dh_group_exchange_sha1**, **dh_group14_sha1**, and **dh_group1_sha1** parameters. To use these parameters, you need to install the WEAKEA plug-in. However, the algorithms specified by these parameters are less secure. For higher security purposes, you are advised to use other parameters. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Add the **dh_group14_sha256** algorithm to the key exchange algorithm list of the SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server key-exchange dh_group14_sha256
```

2.6.61 ssh server port

Function

The **ssh server port** command configures a listening port number for an SSH server.

The **undo ssh server port** command restores the default listening port number of an SSH server.

The default listening port number of the SSH server is 22.

Format

ssh [**ipv4** | **ipv6**] **server port** *port-number*

undo ssh [**ipv4** | **ipv6**] **server port**

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of the SSH server.	The value is 22 or an integer ranging from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent attackers from attacking the standard SSH listening port number, run the **ssh server port** command to configure a new listening port. This improves security.

Precautions

If the server is listening on port 22, the SSH client can log in successfully with no port specified. If the server is listening on another port, the port number must be specified.

Before changing the current port number, disconnect all devices from the port. After the port number is changed, the server starts to listen on the new port.

After the **ssh server port** *port-number* command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the number of IPv4 port or IPv6 port separately, run the **ssh** { **ipv4** | **ipv6** } **server port** *port-number* command.

Example

Set the listening port number of the SSH server to 1025.

```
<HUAWEI> system-view
[HUAWEI] ssh server port 1025
```

Set the IPv4 port number of the SSH server to 1025.

```
<HUAWEI> system-view
[HUAWEI] ssh ipv4 server port 1025
```

2.6.62 ssh server publickey

Function

The **ssh server publickey** command specifies a public key algorithm for an SSH server.

The **undo ssh server publickey** command restores all the public key algorithms of an SSH server to default settings.

By default, the DSA, ECC, RSA, RSA_SHA2_256, and RSA_SHA2_512 algorithms are enabled.

Format

ssh server publickey { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *

undo ssh server publickey

Parameters

Parameter	Description	Value
dsa	Specifies the DSA algorithm for an SSH server.	-
ecc	Specifies the ECC algorithm for an SSH server.	-
rsa	Specifies the RSA algorithm for an SSH server.	-
rsa_sha2_256	Specifies the RSA_SHA2_256 algorithm for an SSH server.	-
rsa_sha2_512	Specifies the RSA_SHA2_512 algorithm for an SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to specify a public key algorithm for an SSH server. In this case, the SSH server cannot use other public key algorithms, improving device security. The ECC public key algorithm is recommended.

If a public key algorithm is specified in the **ssh server publickey** command, the SSH server can use the specified public key algorithm and cannot use other public key algorithms. For example, if the **ssh server publickey dsa** command is run, the SSH server can use the DSA algorithm and cannot use the ECC and RSA algorithms.

Precautions

A client can log in to an SSH server using a public key algorithm only if the server also uses this public key algorithm.

For security purposes, you are not advised to use the RSA algorithm with the key of less than 2048 bits to authenticate SSH users. Instead, you are advised to use the more secure ECC, RSA_SHA2_256, or RSA_SHA2_512 authentication algorithm.

If this command has been run for multiple times, the latest configuration takes effect.

Example

Configure an SSH server to use the ECC algorithm.

```
<HUAWEI> system-view
[HUAWEI] ssh server publickey ecc
```

2.6.63 ssh server rekey

Function

The **ssh server rekey** command sets key renegotiation parameters for an SSH server.

The **undo ssh server rekey** command restores the default key renegotiation parameter settings of the SSH server.

By default, the interval at which an SSH server triggers key renegotiation is 60 minutes, the maximum size of data sent and received by an SSH server during key renegotiation is 1000 MB, and a maximum of 268435456 (2^28) packets can be sent and received by an SSH server during key renegotiation.

Format

ssh server rekey { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *

undo ssh server rekey { **time** | **data-limit** | **max-packet** } *

Parameters

Parameter	Description	Value
time *rekey-time*	Specifies an interval at which key renegotiation is triggered.	The value is an integer ranging from 30 to 1440, in minutes.
data-limit *data-limit*	Specifies the maximum size of data sent and received during key renegotiation.	The value is an integer ranging from 100 to 10000, in MB.
max-packet *max-packet*	Specifies the maximum number of packets sent and received during key renegotiation.	The value is an integer ranging from 268435456 to 2147483648.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the SSH session duration reaches the specified interval at which key renegotiation is triggered, the system renegotiates a key and uses the new key to establish SSH session connections, improving system security.

After the **time** parameter is configured for an SSH server, the SSH server checks each SSH session. If the session duration reaches the interval, the SSH server sends a key renegotiation packet to the client to renegotiate an encryption key.

After the **data-limit** parameter is configured for an SSH server, the SSH server checks each SSH session. If the size of data sent and received by the SSH server through a session exceeds the maximum value, the SSH server sends a key renegotiation packet to the client to renegotiate an encryption key.

After the **max-packet** parameter is configured for an SSH server, the SSH server checks each SSH session. If the number of packets sent and received by the SSH server through a session exceeds the maximum value, the SSH server sends a key renegotiation packet to the client to renegotiate an encryption key.

Precautions

A key renegotiation request is initiated when either an SSH client or server meets the key renegotiation criteria. After one party initiates such a request, the other party responds.

Example

Set the maximum size of data sent and received by the SSH server during key renegotiation to 2000 MB.

```
<HUAWEI> system-view
[HUAWEI] ssh server rekey data-limit 2000
```

2.6.64 ssh server rekey-interval

Function

The **ssh server rekey-interval** command sets the interval for updating the SSH server key pair.

The **undo ssh server rekey-interval** command restores the default interval for updating the SSH server key pair.

The default interval for updating the SSH server key pair is 0, indicating that the key pair is never updated.

Format

ssh server rekey-interval *hours*

undo ssh server rekey-interval

Parameters

Parameter	Description	Value
hours	Specifies the interval for updating the server key pair.	The value is an integer that ranges from 0 to 24, in hours.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the server key pair is not updated for a long time, the key is easy to decrypt, and the server is insecure. After the interval for updating the SSH server key pair is set using the **ssh server rekey-interval** command, the device will automatically update the key pair at the specified interval.

Precautions

If the client is connected to the server, the server public key on the client is not updated immediately. This key is updated only when the client is reconnected to the server.

This command takes effect only for SSH1.X. However, SSH1.X provides poor security and is therefore not recommended.

Example

Set the interval for updating the SSH server key pair to 2 hours.

```
<HUAWEI> system-view
[HUAWEI] ssh server rekey-interval 2
```

2.6.65 ssh server timeout

Function

The **ssh server timeout** command sets the timeout period for SSH connection authentication.

The **undo ssh server timeout** restores the default timeout period for SSH connection authentication.

The default timeout period for SSH connection authentication is 60 seconds.

Format

ssh server timeout *seconds*

undo ssh server timeout

Parameters

Parameter	Description	Value
seconds	Specifies the timeout period for SSH connection authentication.	The value is an integer ranging from 1 to 120, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user has not logged in successfully before the timeout period for SSH connection authentication expires, the current connection is terminated to ensure security. To query the current timeout period, run the **display ssh server** command.

Precautions

The timeout period setting takes effect upon next login.

NOTE

If a very short timeout period is configured for SSH connection authentication, user login may fail due to a connection timeout. Using the default timeout period is recommended.

Example

Set the timeout period for SSH connection authentication to 90 seconds.

```
<HUAWEI> system-view
[HUAWEI] ssh server timeout 90
```

2.6.66 ssh server-source

Function

The **ssh server-source** command specifies a source interface for an SSH server.

The **undo ssh server-source** command restores the default setting.

By default, no source interface is specified for an SSH server.

Format

ssh server-source -i *interface-type interface-number*

undo ssh server-source

ssh server-source all-interface

Parameters

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface for an SSH server.	-
all-interface	Specifies any interface that has an IPv4 address configured as the source interface of an SSH server.	-

NOTE

In V200R020C00 and later versions, an SSH server does not accept login connection requests from any interface by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an SSH server accepts login connection requests from all interfaces by default, leading to low system security. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an SSH server does not accept login connection requests from any interface by default. To authorize users to log in to the server, run either of the following commands to specify the source interface of the SSH server:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server.
- Run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.

Prerequisites

Before specifying a logical interface as the source interface, ensure that the source interface has been created and has an IPv4 address configured. Otherwise, this command cannot be executed successfully.

Precautions

After this command is run, the new configuration takes effect upon the next login.

After the source interface is specified, the system allows users to log in to the SSH server only using the specified source interface. This configuration applies to the SSH users who attempt to log in to the SSH server, but not to the SSH users who have logged in to the server.

After the source interface of an SSH server is specified using this command, ensure that authorized SSH users can access the source interface at Layer 3. Otherwise, the SSH users will fail to log in to the SSH server.

If the source address or source interface is not specified, there are security risks.

When the **ssh server-source -i** command is run, if a VLANIF interface is specified as the source interface and has a secondary address configured, SSH login using the secondary address is not supported.

After the **ssh server-source all-interface** command is run, the system allows SSH users to log in to the SSH server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Specify Loopback0 as the source interface of an SSH server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] ip address 10.1.1.1 24
[HUAWEI-LoopBack0] quit
[HUAWEI] ssh server-source -i loopback 0
```

2.6.67 ssh ipv6 server-source

Function

The **ssh ipv6 server-source** command specifies an IPv6 source address for an SSH server.

The **undo ssh ipv6 server-source** command cancels the IPv6 source address specified for an SSH server.

By default, the IPv6 source address of an SSH server is not specified.

Format

ssh ipv6 server-source -a *ipv6_address* [**-vpn-instance** *vpn_name*]

undo ssh ipv6 server-source

ssh ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies the IPv6 source address for an SSH server.	The total length of an IPv6 address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.
-vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the SSH server.	-

NOTE

In V200R020C00 and later versions, an SSH server does not accept login connection requests from any interface by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an SSH server accepts connection requests from all IPv6 addresses by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an SSH server does not accept login requests from any IPv6 address by default. To allow authorized users to log in to the SSH server, run either of the following commands to specify an IPv6 source address for the SSH server.

- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure the specified IPv6 address as the IPv6 source address of the SSH server.
- Run the **ssh ipv6 server-source all-interface** command to configure all interface IPv6 addresses on the device as the IPv6 source addresses of the SSH server.

Prerequisites

A VPN instance has been created before you specify it for an SSH server. Otherwise, the **ssh ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for an SSH server, SSH users can log in to the SSH server only using this IPv6 address. This configuration applies to the SSH users who attempt to log in to the SSH server, not to the SSH users who have logged in to the server.

Precautions

After this command is run, the new configuration takes effect upon the next login.

After an IPv6 source address is specified for an SSH server using this command, ensure that SFTP or SSH users can access this IPv6 address at Layer 3. Otherwise, SFTP or SSH users will fail to log in to the SSH server.

If the specified IPv6 source address is bound to a VPN instance, the SSH server is also bound to the VPN instance.

After the **ssh ipv6 server-source all-interface** command is run, the system allows SSH users to log in to the SSH server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh ipv6 server-source -a 2001:DB8::
```

2.6.68 ssh user

Function

The **ssh user** command creates an SSH user.

The **undo ssh user** command deletes an SSH user.

By default, no SSH user is created.

Format

ssh user *user-name*

undo ssh user [*user-name*]

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

System view

Default Level

3: Management level

Usage Guidelines

You can create an SSH user in either of the following ways:

- Run the **ssh user** command.
- Run the **ssh user authentication-type**, **ssh user service-type**, or **ssh user sftp-directory** command with the user name you want to create. If the device

cannot find the user with the name you specified, it automatically creates the user.

Example

Create an SSH user named **testuser**.

```
<HUAWEI> system-view
[HUAWEI] ssh user testuser
```

2.6.69 ssh user assign

Function

The **ssh user assign** command assigns an existing public key to a user.

The **undo ssh user assign** command deletes the mapping between the user and public key.

By default, no public key is assigned to a user.

Format

ssh user *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *key-name*

undo ssh user *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
rsa-key	Specifies an RSA public key.	-
dsa-key	Specifies a DSA public key.	-
ecc-key	Specifies an ECC public key.	-
key-name	Specifies the client public key name.	The value is a string of 1 to 30 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSH client needs to log in to the SSH server in RSA, DSA, or ECC mode, run the **ssh user assign** command to assign a public key to the client. If the client has been assigned keys, the latest assigned key takes effect.

Precautions

The newly configured public key takes effect upon next login.

If the user named *user-name* to whom a public key is assigned does not exist, the device automatically creates an SSH user named *user-name* and performs the configured authentication for the SSH user.

To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Example

Assign key1 to the user named John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john assign rsa-key key1
```

2.6.70 ssh user authorization-cmd aaa

Function

The **ssh user authorization-cmd aaa** command enables command line authorization for an SSH user.

The **undo ssh user authorization-cmd aaa** command restores the default authorization mode.

By default, command line authorization is disabled for an SSH user.

Format

ssh user *user-name* **authorization-cmd aaa**

undo ssh user *user-name* **authorization-cmd aaa**

Parameters

Parameter	Description	Value
user-name	Specifies the name of a valid SSH user defined by the AAA.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

The new setting for command line authorization takes effect upon next login.

This command is valid only for SSH users. The AAA configuration determines whether to configure an authorization mode for the users who log in using passwords.

Example

Enable command line authorization for the user named John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john authorization-cmd aaa
Info: Please make sure that the command line authorization method has been set for the user.
```

2.6.71 ssh user authentication-type

Function

The **ssh user authentication-type** command configures an authentication mode for an SSH user.

The **undo ssh user authentication-type** command restores the default authentication mode for an SSH user.

By default, no authentication mode is configured for an SSH user.

Format

ssh user *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }

undo ssh user *user-name* **authentication-type**

Parameters

Parameter	Description	Value
user-name	Specifies an SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
password	Specifies the password authentication mode.	-
rsa	Specifies the RSA authentication mode.	-
password-rsa	Specifies the password and RSA authentication modes.	-
dsa	Specifies the DSA authentication mode.	-
password-dsa	Specifies the password and DSA authentication modes.	-
ecc	Specifies the ECC authentication mode.	-
password-ecc	Specifies the password and ECC authentication modes.	-

Parameter	Description	Value
all	Specifies the password, ECC, DSA, or RSA authentication mode. **NOTE** In all authentication mode, the user priority depends on the authentication mode that the user selected. - If password authentication is selected, the user priority is the same as that specified on the AAA module. - If RSA/DSA/ECC authentication is selected, the user priority depends on the priority of the VTY interface used during user access. If all authentication is selected and an AAA user with the same name as the SSH user exists, user priorities may be different in password authentication and RSA, DSA, or ECC authentication modes. Set relevant parameters as needed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you configure an authentication mode for an SSH user, if the user does not exist, a device automatically creates an SSH user named *user-name*.

Table 2-45 describes the usage scenarios for different authentication modes.

Table 2-45 Usage scenarios for authentication modes

Authentication Mode	Usage Scenario
RSA	It is a public key encryption architecture and an asymmetric encryption algorithm. RSA is mainly used to transmit the keys of the symmetric encryption algorithm, which improves encryption efficiency and simplify key management. The server checks whether the SSH user, public key, and digital user signature are valid. If all of them are valid, the user is permitted to access the server. If any of them is invalid, the authentication fails, and the user is denied to access the server.
DSA	It is same as RSA authentication in implementation. The server checks whether the SSH user, public key, and digital user signature are valid. If all of them are valid, the user is permitted to access the server. If any of them is invalid, the authentication fails, and the user is denied to access the server. Compared with RSA authentication, DSA authentication uses the digital signature algorithm for encryption and has a wider application scope. ● Many SSH tools only support DSA authentication for servers and clients. ● Based on the latest RFC recommendation for SSH, DSA authentication takes precedence over RSA authentication.

Authentication Mode	Usage Scenario
ECC	Like RSA authentication, the server first checks the validity of the SSH user and whether the public key and the numeric signature are valid. If all of them are consistent with those configured on the server, user authentication succeeds. If any of the three cannot pass authentication, the user access is denied. Compared with the RSA algorithm, the ECC authentication has the following advantages: ● Provides the same security with shorter key length. ● Features a shorter computing process and higher processing speed. ● Requires less storage space. ● Requires lower bandwidth.
password	On the server, the AAA module assigns each authorized user a password for login. The server has the mapping between user names and passwords. When a user requests to access the server, the server authenticates the user name and password. If either of them fails to be authenticated, the access request of the user is denied. The account information of users who are configured with the password authentication mode can be configured on devices or remote authentication servers (for example, RADIUS servers).
password-rsa, password-dsa, and password-ecc	The SSH server authenticates a client by checking both the public key and password. The client can be authenticated only when both the public key and password meet the requirement.
all	The SSH server authenticates a client by checking the public key or password. The client can be authenticated when either the public key or password meets the requirement.

Precautions

A new SSH user cannot log in to the SSH server unless being configured with an authentication mode. The newly configured authentication mode takes effect upon next login.

To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Example

Configure password authentication for the SSH user John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john authentication-type password
```

2.6.72 ssh user service-type

Function

The **ssh user service-type** command configures a service type for an SSH user.

The **undo ssh user service-type** command restores the default service type for an SSH user.

By default, no service type is configured for an SSH user.

Format

ssh user *user-name* **service-type** { **sftp** | **stelnet** | **all** }

undo ssh user *user-name* **service-type**

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
sftp	Specifies the SFTP service type.	-
stelnet	Specifies the STelnet service type.	-
all	Specifies the SFTP and STelnet service types.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure a service type for an SSH user, run the **ssh user service-type** command on a device. If the specified user does not exist, the device creates an SSH user who has the same name as the specified user and uses the configured service type for the SSH user.

Precautions

If the SFTP service type is configured for an SSH user, you need to run the **ssh user sftp-directory** command to set an authorized directory for the user. By default, the SFTP service authorized directory is flash: for the SSH user.

Example

Configure the **all** service type for an SSH user John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john service-type all
```

2.6.73 stelnet

Function

The **stelnet** command enables a user to use the STelnet protocol to log in to another device from the current device.

Format

IPv4 address

stelnet [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [[**-vpn-instance** *vpn-instance-name*] | [**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** }] | [**user-identity-key** { **rsa** | **dsa** | **ecc** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] *

IPv6 address

stelnet ipv6 [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*] [[**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** }] | [**user-identity-key** { **rsa** | **dsa** | **ecc** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*]

| [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **-a** *source-address* and **-i** *interface-type interface-number* parameter in the command.

Parameters

Parameter	Description	Value
-a *source-address*	Specifies the STelnet source IP address.	-
-i *interface-type interface-number*	Specifies the STelnet source interface. If the source interface is specified using **-i** *interface-type interface-number*, the **-vpn-instance** *vpn-instance-name* parameter is not supported.	-
host-ip	Specifies the IP address or host name of the remote IPv4 STelnet server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
host-ipv6	Specifies the IPv6 address or host name of the remote IPv6 STelnet server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
-oi *interface-type interface-number*	Specifies the outbound interface on the local device.	If the IPv6 address of the remote host is linked to a local address, the outbound interface must be specified.
port-number	Specifies the port number that the SSH server is listening on.	The value is an integer that ranges from 1 to 65535. The default value 22 is the standard port number.

Parameter	Description	Value
identity-key	Specifies the public key for server authentication.	The public key algorithm includes dsa, rsa, rsa_sha2_256, rsa_sha2_512 and ecc. By default, the server authentication uses the ECC public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
user-identity-key	Specifies the public key algorithm for the client authentication.	The public key algorithm includes dsa, rsa, and ecc. By default, the client authentication uses the RSA public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
prefer_kex *prefer_key-exchange*	Indicates the preferred key exchange algorithm.	Specifies the preferred key exchange algorithm. The **dh_exchange_group**, **dh_exchange_group_sha256**, **dh_group14_sha1**, **dh_group14_sha256**, **dh_group15_sha512**, and **dh_group16_sha512** algorithms are supported currently. The default key exchange algorithm is dh_group14_sha1.

Parameter	Description	Value
prefer_ctos_cipher *prefer_ctos_cipher*	Specifies the preferred encryption algorithm from the client to the server. The 3des, aes128, aes256, aes128_ctr, and aes256_ctr algorithms are supported currently.	The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr and aes256_ctr algorithms. **NOTE** ● If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. ● If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
prefer_stoc_cipher *prefer_stoc_cipher*	Specifies the preferred encryption algorithm from the server to the client. The 3des, aes128, aes256, aes128_ctr, and aes256_ctr algorithms are supported currently.	The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr and aes256_ctr algorithms. **NOTE** ● If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. ● If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.

Parameter	Description	Value
prefer_ctos_hmac *prefer_ctos_hmac*	Specifies the preferred HMAC algorithm from the client to the server. The sha1, sha1_96, md5, md5_96, sha2_256, and sha2_256_96 algorithms are supported currently.	The default algorithm is sha2_256. To improve security, it is recommended that you use sha2_256 algorithms.
prefer_stoc_hmac *prefer_stoc_hmac*	Specifies the preferred HMAC algorithm from the server to the client. The sha1, sha1_96, md5, md5_96, sha2_256, and sha2_256_96 algorithms are supported currently.	The default algorithm is sha2_256. To improve security, it is recommended that you use sha2_256 algorithms.
-vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the server belongs.	The value must be an existing VPN instance name.
-ki *aliveinterval*	Specifies the interval for sending keepalive packets when no packet is received.	The value is an integer that ranges from 1 to 3600, in seconds.
-kc *alivecountmax*	Specifies the number of times for no reply of keepalive packets.	The value is an integer that ranges from 3 to 10. The default value is 5.

Views

System view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Logins through Telnet bring security risks because Telnet does not provide any authentication mechanism and data is transmitted using TCP in plain text. Compared with Telnet, SSH guarantees secure file transfer on a traditional insecure network by authenticating clients and encrypting data in bidirectional mode. The SSH protocol supports STelnet. You can run this command to use STelnet to log in to another device from the current device.

STelnet is a secure Telnet service. SSH users can use the STelnet service in the same way as the Telnet service.

When a fault occurs in the connection between the client and server, the client needs to detect the fault in real time and proactively release the connection. You need to set the interval for sending keepalive packets and the maximum number of times on the client that logs in to the server through STelnet.

- Interval for sending keepalive packets: If a client does not receive any packet within the specified interval, the client sends a keepalive packet to the server.
- Maximum number of times the server has no response: If the number of times that the server does not respond exceeds the specified value, the client proactively releases the connection.

Precautions

- Before connecting the SSH server using the **STelnet** command, run the **stelnet server enable** command to enable the STelnet service on the SSH server.
- If the server is listening on port 22, the SSH client can log in to the SSH server with no port specified. If the server is listening on another port, the port number must be specified upon login.

Example

Set keepalive parameters when a client logs in to a server through STelnet.

```
<HUAWEI> system-view
[HUAWEI] stelnet 10.164.39.209 -ki 10 -kc 4
```

Remotely connect to the STelnet server that uses an IPv6 address.

```
<HUAWEI> system-view
[HUAWEI] stelnet ipv6 fc00:2001:db8::1 prefer_ctos_cipher aes128
```

2.6.74 stelnet server enable

Function

The **stelnet server enable** command enables the STelnet service on an SSH server.

The **undo stelnet server enable** command disables the STelnet service on an SSH server.

By default, the STelnet service is disabled on SSH servers.

Format

stelnet [**ipv4** | **ipv6**] **server enable**

undo stelnet [**ipv4** | **ipv6**] **server enable**

Parameters

Parameter	Description	Value
ipv4	Configures a device as the STelnet IPv4 server.	-
ipv6	Configure a device as the STelnet IPv6 server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To connect a client to an SSH server through STelnet, you must enable the STelnet service on the SSH server.

Prerequisites

Before enabling the STelnet service, run either of the following commands as required:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server or run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.
- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the SSH server or run the **ssh ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the SSH server.

Precautions

After you disable the STelnet service on the SSH server, all clients that have logged in through STelnet are disconnected.

After the **stelnet server enable** command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the IPv4 or IPv6 port number separately, run the **stelnet** { **ipv4** | **ipv6** } **server enable** command.

Example

Enable the STelnet service.

```
<HUAWEI> system-view
[HUAWEI] stelnet server enable
```

Enable the STelnet IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] stelnet ipv4 server enable
```

2.6.75 super

Function

The **super** command changes the user's current privilege level.

User privilege level indicates the type of the login user. There are 16 user privilege levels. Different from the use of command privilege level, a login user can only use the commands with the levels no higher than the user privilege level.

Format

super [*level*]

Parameters

Parameter	Description	Value
level	Specifies the user privilege level.	The value is an integer ranging from 0 to 15. By default, the level is 3.

Views

User view

Default Level

0: Visit level

Usage Guidelines

User privilege level indicates the type of the login user. There are 16 user privilege levels. Different from the use of command privilege level, a login user can only use the commands with the privilege levels no higher than the user privilege level.

In order to prevent unauthorized users from illegal intrusion, user ID authentication is performed when users at a lower level switch to users at a higher level. In other word, the password of the higher level is needed. You can run the **super password** command to set the password for changing the user from a lower level to a higher level.

For the sake of confidentiality, the password the user inputs is not shown on the screen. The user can switch to the higher level only when inputting the correct password within three times. Otherwise, the original user privilege level remains unchanged.

The passwords must meet the following requirements:

- The password is a string of 8 to 16 case-sensitive characters.
- The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Special character except the question mark (?) and space.

NOTICE

Huawei switches use the combination of user name, password, and level to control users' operation rights. If you use the super command to switch user privilege levels, this right control method will become invalid. Moreover, any user can use the super password of a higher level to obtain high-level operation rights. Therefore, you are not advised to use the super command to switch user privilege levels.

Example

Enable the user to switch to level 3.

```
<HUAWEI> super 3
Password:
Now user privilege is 3 level, and only those commands whose level is equal to or less than this level can
be used.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

2.6.76 super password

Function

The **super password** command sets the password for switching a user from a lower level to a higher level.

The **undo super password** command deletes the password for switching a user from a lower level to a higher level.

By default, no password is configured for switching a user from a lower level to a higher level. A password must be configured for switching a user from a lower level to a higher level. Otherwise, the switching fails.

Format

super password [**level** *user-level*] [**cipher** *password*]

undo super password [**level** *user-level*]

Parameters

Parameter	Description	Value
level *user-level*	Specifies the user privilege level that needs to be changed.	The value is an integer that ranges from 1 to 15. By default, the system sets a password for a user that switches to level 3.

Parameter	Description	Value
cipher *password*	Specifies the password for changing a level.	- When **cipher** is not entered, password input is in man-machine interaction mode, and the system does not display the entered password. The password is a string of 8 to 16 case-sensitive characters. The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Question mark (?) and space characters are not supported. - When **cipher** is entered, the password is displayed in either simple or ciphertext mode during input. – When being input in simple mode, the password requirements are the same as those when **cipher** is not entered. – When being input in ciphertext, the password must be a string of 56 consecutive characters. **NOTE** If the source version supports a ciphertext password which is a string of 24 or 32 characters, the target version also supports this type of password. When setting the password for switching the user privilege level, if the current user privilege level is higher than the specified user privilege level and the password exists, the old password does not need to be verified. If the current user privilege level is lower than the specified user privilege level, enter the correct old password; otherwise, the configuration will fail. The password is displayed in ciphertext in the configuration file regardless of whether it is input in simple or ciphertext mode.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If users' rights are redefined, users need to run the **super** command to change their levels from low to high. For safety, users need to be authenticated when they change their levels. Users can run the **super password** command to set the password of changing their levels from low to high for authentication.

Precautions

- The password entered by a user is saved in ciphertext, irrespective of whether **cipher** is specified. Therefore, if the password is lost, you cannot get it back.
- Users can press **Ctrl+C** to cancel the operation when they run the **super password**.
- When a user with a level lower than the level configured using this command queries the password configured using the **display this** or **display current-configuration** command, the password is displayed as asterisks (******).

Example

Set the password **Abcd@123** for switching a user from a lower level to level 3, with **cipher** configured for the password.

```
<HUAWEI> system-view
[HUAWEI] super password level 3 cipher Abcd@123
Info: The password will be changed, please verify the old password.
Please enter old password:
Info: The password is changed successfully.
```

Set the password **Abcd@123** for switching a user from a lower level to level 3, with **cipher** not configured for the password.

```
<HUAWEI> system-view
[HUAWEI] super password level 3
Please configure the login password (8-16)
Enter Password:
Confirm Password:
Info: The password will be changed, please verify the old password.
Please enter old password:
Info: The password is changed successfully.
```

2.6.77 super password complexity-check disable

Function

The **super password complexity-check disable** command disables password complexity check when a low-level user is switched to a high-level user.

The **undo super password complexity-check disable** command enables password complexity check when a low-level user is switched to a high-level user.

By default, password complexity check is enabled when a low-level user is switched to a high-level user.

Format

super password complexity-check disable

undo super password complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device has the following requirements for the password for switching a low-level user to a high-level user:

- By default, the minimum password length is eight characters. If the password length set by the **set password min-length** command exceeds eight characters, the value set by this command is the minimum password length.
- A password must contain two or more types of characters, such as upper-case letters, lower-case letters, digits, and special characters.

  The special characters exclude question marks (?) and spaces.

To ensure security of the password for switching a low-level user to a high-level user, run the **undo super password complexity-check disable** command to enable password complexity check. In this case, if a specified password fails the password complexity check, the configuration does not take effect. In a scenario where high security is not required, run the **super password complexity-check disable** command to disable password complexity check.

Precautions

If password complexity check is disabled when a low-level user is switched to a high-level user, a simple password will bring security risks.

Example

Disable password complexity check when a low-level user is switched to a high-level user.

```
<HUAWEI> system-view
[HUAWEI] super password complexity-check disable
```

2.6.78 telnet

Function

The **telnet** command enables a user to use the Telnet protocol to log in to another device from the current device.

Format

Log in to another device through Telnet based on IPv4.

telnet [**vpn-instance** *vpn-instance-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*]

Log in to another device through Telnet based on IPv6.

telnet ipv6 [**-a** *source-ip-address*] [**vpn6-instance** *vpn6-instance-name*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*]

(Only S5720I-SI, S5720-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vpn6-instance** *vpn6-instance-name*.)

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN4 instance name of the device to log in through Telnet.	The value must be an existing VPN instance name.
-a *source-ip-address*	Specifies a source IP address through which a server communicates with the device. This improves security. If no source address is specified, a device will use the IP address of the local outbound interface to initiate a Telnet connection.	-
-i *interface-type interface-number*	Specifies the source interface type and number on the local device.	-
vpn6-instance *vpn6-instance-name*	Specifies the name of the VPN6 instance to which the login device belongs.	The value must be an existing VPN instance name.
host-ip	Specifies the IPv4 address or host name of the remote device.	The value is a string of 1 to 255 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Parameter	Description	Value
host-ipv6	Specifies the IPv6 address or host name of the remote device.	The value is a string of 1 to 255 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
-oi *interface-type interface-number*	Specifies the outbound interface on the local device.	If the IPv6 address of the remote host is linked to a local address, the outbound interface must be specified.
port-number	Specifies the number of the TCP port that is used by the remote device to provide the Telnet service.	The value is an integer that ranges from 1 to 65535. The default value is 23.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If multiple devices on a network need to be configured and managed, run the **telnet** command to log in to these devices from your terminal for remote device configuration, facilitating device management.

You can press **Ctrl+K** to terminate an active connection between the local and remote devices.

Precautions

- Before you run the **telnet** command to connect to the Telnet server, the Telnet client and server must be able to communicate at Layer 3 and the Telnet service must be enabled on the Telnet server.
- Logins through Telnet bring security risks because Telnet does not provide any authentication mechanism and data is transmitted using TCP in plain text. The STelnet mode is recommended for networks that have high security requirements.

Example

Connect to a remote device through Telnet.

```
<HUAWEI> telnet 192.168.1.6
```

Use the IPv6 address to connect to a remote device through Telnet.

```
<HUAWEI> telnet ipv6 fc00:0:0:11::158
```

2.6.79 telnet client-source

Function

The **telnet client-source** command specifies a source IP address or source interface for a Telnet client.

The **undo telnet client-source** command restores the default settings.

The default source IP address of a Telnet client is 0.0.0.0, and there is no default source interface.

Format

telnet client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo telnet client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the local switch.	-
-i *interface-type interface-number*	Specifies the source interface of the local switch.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the source IP address is not specified in the **telnet** command, the source IP address specified using the **telnet client-source** is used. If a source IP address is specified in the **telnet** command, the specified setting is used. Check the current Telnet connection on the server. The IP address displayed is the specified source IP address or the primary IP address of the specified interface.

Prerequisites

The source interface specified using the command must exist and have an IP address configured.

Example

Set the source IP address of the Telnet client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] telnet client-source -a 10.1.1.1
```

2.6.80 telnet server acl

Function

The **telnet server acl** command configures an ACL to control the access of clients to the Telnet server.

The **undo telnet server acl** command cancels the configuration of the ACL.

By default, no ACL is configured for Telnet servers.

Format

telnet [**ipv6**] **server acl** *acl-number*

undo telnet [**ipv6**] **server acl**

Parameters

Parameter	Description	Value
ipv6	Specifies a Telnet IPv6 server.	-
acl-number	Specifies an ACL number.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a device functions as a Telnet server, configure an ACL on the device to control the login of the clients to the device.

Prerequisites

An ACL has been configured using the **acl (system view)** command in the system view, and an ACL rule has been configured using the **rule (basic ACL view)** or **rule (advanced ACL view)** command.

Precautions

None.

Example

Configure ACL 2000 on a Telnet server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] telnet server acl 2000
```

2.6.81 telnet server-source

Function

The **telnet server-source** command specifies a source interface for a Telnet server.

The **undo telnet server-source** command restores the default setting.

By default, the source interface of a Telnet server is not specified.

Format

telnet server-source -i *interface-type interface-number*

undo telnet server-source

telnet server-source all-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the source interface of the local device.	-
all-interface	Indicates that any interface that has an IPv4 address configured can be used as the source interface of a Telnet server.	-

NOTE

In V200R020C00 and later versions, a Telnet server does not accept login connection requests from any interface by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, a Telnet server receives connection requests from all interfaces by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, a Telnet server does not accept login requests from any interface by default. To allow authorized users to log in to the Telnet server, run either of the following commands to specify the source interface of the Telnet server.

- Run the **telnet server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the Telnet server.
- Run the **telnet server-source all-interface** command to configure all interfaces configured with IPv4 addresses as the source interfaces of the Telnet server.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **telnet server-source** command cannot be successfully executed.

Precautions

By default, no source interface is specified for an SSH server.

After the source interface is specified, a device allows Telnet users to log in to the Telnet server only through this source interface, and Telnet users logging in through other interfaces are denied. Note that setting this parameter only affects Telnet users who attempt to log in to the Telnet server, and it does not affect Telnet users who have logged in to the server.

After the source interface of a Telnet server is specified using this command, ensure that Telnet users can access the source interface at Layer 3. Otherwise, the Telnet users will fail to log in to the Telnet server.

No source address or source interface is specified, so security risks exist.

After the **telnet server-source all-interface** command is run, the system allows Telnet users to log in to the Telnet server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Specify loopback0 as the source interface of the Telnet server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
```

```
[HUAWEI-LoopBack0] ip address 10.1.1.1 24
[HUAWEI-LoopBack0] quit
[HUAWEI] telnet server-source -i loopback 0
```

2.6.82 telnet ipv6 server-source

Function

The **telnet ipv6 server-source** command specifies an IPv6 source address for a Telnet server.

The **undo telnet ipv6 server-source** command cancels the IPv6 source address specified for a Telnet server.

By default, the IPv6 source address of a Telnet server is not specified.

Format

telnet ipv6 server-source -a *ipv6_address* [**vpn-instance** *vpn_name*]

undo telnet ipv6 server-source

telnet ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies the IPv6 source address for a Telnet server.	The total length of an IPv6 address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the Telnet server.	-

NOTE

In V200R020C00 and later versions, a Telnet server does not accept login connection requests from any IPv6 address by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, a Telnet server accepts connection requests from all IPv6 addresses by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, a Telnet server does not accept login requests from any IPv6 address by default. To allow authorized users to log in to the Telnet server, run either of the following commands to specify an IPv6 source address for the Telnet server.

- Run the **telnet ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*] command to configure the specified IPv6 address as the IPv6 source address of the Telnet server.
- Run the **telnet ipv6 server-source all-interface** command to configure all interface IPv6 addresses on the device as the IPv6 source addresses of the Telnet server.

Prerequisites

A VPN instance has been created before you specify it for a Telnet server. Otherwise, the **telnet ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for a Telnet server, Telnet users can log in to the Telnet server only using this IPv6 address. This configuration applies to the Telnet users who attempt to log in to the server, not to the Telnet users who have logged in to the server.

Precautions

After this command is run, the new configuration takes effect upon the next login.

After an IPv6 source address is specified for a Telnet server using this command, ensure that Telnet users can access this IPv6 address at Layer 3. Otherwise, Telnet users will fail to log in to the Telnet server.

If the specified IPv6 source address is bound to a VPN instance, the Telnet server is also bound to the VPN instance.

After the **telnet ipv6 server-source all-interface** command is run, the system allows Telnet users to log in to the Telnet server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for a Telnet server.

```
<HUAWEI> system-view
[HUAWEI] telnet ipv6 server-source -a 2001:DB8::
```

2.6.83 telnet server enable

Function

The **telnet server enable** command enables the Telnet service.

The **undo telnet server enable** command disables the Telnet service.

The **telnet server disable** command disables the Telnet service.

By default, the Telnet service is disabled.

Format

telnet [**ipv6**] **server enable**

undo telnet [**ipv6**] **server enable**

telnet [**ipv6**] **server disable**

Parameters

Parameter	Description	Value
ipv6	Specifies a Telnet IPv6 server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **telnet server enable** command to enable the Telnet service. A Telnet server can be connected only when it is enabled.

Prerequisites

Before enabling the Telnet service, run either of the following commands as required:

- Run the **telnet server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the Telnet server or run the **telnet server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the Telnet server.
- Run the **telnet ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the Telnet server or run the **telnet ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the Telnet server.

Precautions

If the user who logged in to the server through Telnet is online, the **undo telnet** [**ipv6**] **server enable** command fails to be run on the server.

When a Telnet server is disabled, you can log in to the device only through the console port or SSH.

NOTICE

The Telnet protocol poses a security risk, and therefore using STelnet V2 is recommended.

Example

Enable the Telnet service.

```
<HUAWEI> system-view
[HUAWEI] telnet server enable
```

Disable the Telnet service.

```
<HUAWEI> system-view
[HUAWEI] undo telnet server enable
```

Enable the IPv6 Telnet service.

```
<HUAWEI> system-view
[HUAWEI] telnet ipv6 server enable
```

2.6.84 telnet server port

Function

The **telnet server port** command configures a listening port number for a Telnet server.

The **undo telnet server port** command restores the default listening port of a Telnet server.

The default listening port of a Telnet server is 23.

Format

telnet server port *port-number*

undo telnet server port

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of a Telnet server.	The value is an integer that is 23 or ranges from 1025 to 55535. The default value 23 is the standard Telnet server port number.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent attackers from attacking the standard Telnet listening port number, run the **telnet server port** command to configure a new listening port. This improves security.

Precautions

If the server is listening on port 23, the Telnet client can log in successfully with no port specified. If the server is listening on another port, the port number must be specified.

Before changing the current port number, disconnect all devices from the port. After the port number is changed, the server starts to listen on the new port.

Example

Set the listening port number to 1026.

```
<HUAWEI> system-view
[HUAWEI] telnet server port 1026
```

Restore the listening port number to the default value.

```
<HUAWEI> system-view
[HUAWEI] undo telnet server port
```

2.7 File Management Commands

2.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.7.2 ascii

Function

The **ascii** command sets the file transfer mode to ASCII on an FTP client.

The default file transfer mode is ASCII.

Format

ascii

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files.

Example

Set the file transfer mode to ASCII.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] ascii
200 Type set to A.
```

2.7.3 binary

Function

The **binary** command sets the file transfer mode to binary on an FTP client.

The default file transfer mode is ASCII.

Format

binary

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files.

Example

Set the file transfer mode to binary.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[ftp] binary
200 Type set to I
```

2.7.4 binding cipher-suite-customization

Function

The **binding cipher-suite-customization** command binds a customized SSL cipher suite policy to an SSL policy.

The **undo binding cipher-suite-customization** command unbinds the customized SSL cipher suite policy from an SSL policy.

By default, no customized cipher suite policy is bound to an SSL policy. Each SSL policy uses a default cipher suite.

Format

binding cipher-suite-customization *customization-policy-name*

undo binding cipher-suite-customization

Parameters

Parameter	Description	Value
customization-policy-name	Specifies the name of a customized SSL cipher suite policy.	The value is a string of 1 to 32 case-insensitive characters, spaces not supported.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To bind a customized SSL cipher suite policy to an SSL policy, run the **binding cipher-suite-customization** command. After a customized SSL cipher suite policy is bound to an SSL policy, the device uses an algorithm in the specified cipher suite to perform SSL negotiation.

After a customized cipher suite policy is unbound from an SSL policy, the SSL policy uses one of the following cipher suites supported by default:

- tls1_ck_rsa_with_aes_256_sha
- tls1_ck_rsa_with_aes_128_sha
- tls1_ck_dhe_rsa_with_aes_256_sha
- tls1_ck_dhe_dss_with_aes_256_sha
- tls1_ck_dhe_rsa_with_aes_128_sha
- tls1_ck_dhe_dss_with_aes_128_sha
- tls12_ck_rsa_aes_256_cbc_sha256

Prerequisites

The customized cipher suite policy to be bound to an SSL policy contains cipher suites.

Precautions

If the cipher suite in the customized cipher suite policy bound to an SSL policy contains only one type of algorithm (RSA or DSS), the corresponding certificate must be loaded for the SSL policy to ensure successful SSL negotiation.

Example

Bind customized SSL cipher suite policy named **cipher1** to an SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] binding cipher-suite-customization cipher1
```

2.7.5 bye

Function

The **bye** command terminates the connection with the remote FTP server and enters the user view.

Format

bye

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

This command is equivalent to the **quit** command.

You can use the **close** and **disconnect** commands to terminate the connection with the remote FTP server and retain the FTP client view.

Example

Terminate the connection with the remote FTP server and enter the user view.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] bye
```

```
221 server closing.
<HUAWEI>
```

2.7.6 cd (FTP client view)

Function

The **cd** command changes the working directory of the FTP server.

Format

cd *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a working directory on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

The FTP server authorizes users to access files in certain directories and their subdirectories.

Example

Change the working directory to **d:/temp**.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] cd d:/temp
250 "D:/temp" is current directory.
```

2.7.7 cd (SFTP client view)

Function

The **cd** command changes the working directory of the SFTP server.

Format

cd [*remote-directory*]

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a directory on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- The SFTP server authorizes users to access files in certain directories and their subdirectories.
- The specified working directory must exist on the SFTP server. If the *remote-directory* parameter is not included in the **cd** command, only the current working directory of an SSH user is displayed as the command output.

Example

Change the current working directory of the SFTP server to /bill.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> cd bill
Current directory is:
/bill
```

2.7.8 cd (user view)

Function

The **cd** command changes the current working directory of a user.

By default, the current working directory is flash:.

Format

cd *directory*

Parameters

Parameter	Description	Value
directory	Specifies the current working directory of a user.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] path** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' " For example, a directory name is flash:/selftest/test/.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.

- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

For example, if you change the current working directory flash:/selftest/ to the logfile directory in flash, the absolute path is flash:/logfile/, and the relative path is /logfile/. The logfile directory is not **logfile/** because it is not in the current working directory **selftest**.

Precautions

- The directory specified in the **cd** command must exist; otherwise, the error messages will be displayed:

  You can perform the following operations to rectify faults:

  a. Run the **pwd** command to view the current working directory.
  b. Run the **dir** command to view the current working directory and verify that the directory specified in the **cd** command exists.

Example

Change the current working directory from flash:/temp to flash:.

```
<HUAWEI> pwd
flash:/temp
<HUAWEI> cd flash:
<HUAWEI> pwd
flash:
```

Change the current working directory from flash: to flash:/t1/t2.

```
<HUAWEI> pwd
flash:
<HUAWEI> cd flash:/t1/t2
<HUAWEI> pwd
flash:/t1/t2
```

Change the current working directory from flash:/selftest to flash:/logfile.

```
<HUAWEI> pwd
flash:/selftest
<HUAWEI> cd /logfile/
<HUAWEI> pwd
flash:/logfile
```

Change the current working directory from flash:/selftest to flash:/selftest/test.

```
<HUAWEI> pwd
flash:/selftest
<HUAWEI> cd test/
<HUAWEI> pwd
flash:/selftest/test
```

2.7.9 cdup (SFTP client view)

Function

The **cdup** command changes the current working directory of an SSH user to its parent directory.

Format

cdup

Parameters

None

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **cdup** command to change the current working directory to its parent directory.

Precautions

If the current working directory is the SFTP authorization directory, the command cannot change the current working directory.

Example

Change the current working directory to its parent directory.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> cd dhcp
Current directory is:
/dhcp
sftp-client> cdup
Current directory is:
/
sftp-client> cdup
Error: Failed to change the current directory.
sftp-client>
```

2.7.10 cdup (FTP client view)

Function

The **cdup** command enables you to return to the upper-level directory.

Format

cdup

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To exit from the current directory and return to the upper-level directory, run the **cdup** command.

Precautions

The directories accessible to an FTP user are restricted by the authorized directories configured for the user.

Example

Exit from the current directory and return to the upper-level directory.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] cd security
250 CWD command successfully.
[ftp] cdup
200 CDUP command successfully.
```

2.7.11 certificate load

Function

The **certificate load** command loads a digital certificate for a Secure Sockets Layer (SSL) policy.

The **undo certificate load** command unloads a digital certificate for the SSL policy.

By default, no digital certificate is loaded for an SSL policy.

Format

Load a PEM digital certificate for an SSL policy.

certificate load pem-cert *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*

Load an ASN1 digital certificate for an SSL policy.

certificate load asn1-cert *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*

Load a PFX digital certificate for an SSL policy.

certificate load pfx-cert *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*

Load a PEM certificate chain for an SSL policy.

certificate load pem-chain *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*

Unload a digital certificate for an SSL policy.

undo certificate load

Parameters

Parameter	Description	Value
pem-cert	Loads a PEM digital certificate for the SSL policy. A PEM digital certificate has a file name extension .pem. A PEM digital certificate transfers text data between systems.	-
cert-filename	Specifies the name of a certificate file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
key-pair	Specifies the key pair type.	-
dsa	Sets the key pair type to DSA.	-
rsa	Sets the key pair type to RSA.	-

Parameter	Description	Value
key-file *key-filename*	Specifies the key pair file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code cipher *auth-code*	Specifies the authentication code of the key pair file. The authentication code verifies user identity to ensure that only authorized clients access the server.	The value is a string of case-sensitive characters without spaces. If the value begins and ends with double quotation marks (" "), the string of characters can contain spaces. When the value is displayed in plaintext, its length ranges from 1 to 31. When the value is displayed in ciphertext, its length is 48 or 68. A ciphertext password with the length of 32 or 56 characters is also supported.
asn1-cert	Loads an ASN1 digital certificate for the SSL policy. An ASN1 digital certificate has a file name extension .der. By default, most browsers support the ASN1 digital certificate.	-
pfx-cert	Loads a PFX digital certificate for the SSL policy. A PFX digital certificate has a file name extension .pfx. A digital certificate can be converted from the PFX format to another format.	-

Parameter	Description	Value
mac cipher *mac-code*	Specifies a message authentication code. The message authentication code ensures the packet data reliability and security.	The value is a string of case-sensitive characters without spaces. If the value begins and ends with double quotation marks (" "), the string of characters can contain spaces. When the value is displayed in plaintext, its length ranges from 1 to 31. When the value is displayed in ciphertext, its length is 48 or 68. A ciphertext password with the length of 32 or 56 characters is also supported.
pem-chain	Specifies a PEM certificate chain.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SSL security mechanism includes:

- Data transmission security: Uses the symmetric key algorithm to encrypt data.
- Message integrity: uses the multiplexed analog component (MAC) algorithm to ensure message integrity.
- Identity authentication mechanism: authenticates users based on the digital signatures and certificates.

The Certificate Authority (CA) issues PEM, ASN1, and PFX digital certificates that provide user identity information. Based on digital certificates, users establish trust relationships with partners who require high security.

A digital certificate data includes the applicant information such as the applicant's name, applicant's public key, digital signature of the CA that issues the certificate, and the certificate validity period. The CA can issue a certificate chain along with the digital certificate. After receiving a certificate chain, the receiver owns all the certificates on the chain.

Prerequisites

The **ssl policy** command has been run in the system view to create an SSL policy.

Precautions

You can load a certificate or certificate chain for only one SSL policy. Before loading a certificate or certificate chain, you must unload the existing certificate or certificate chain.

To ensure security, the device automatically saves the key file in the system and deletes the file from the storage medium after a certificate is successfully loaded. It is recommended that you do not delete a certificate or certificate chain that has been successfully loaded; otherwise, services using the SSL policy will be affected.

For device that supports the NOR flash, after the certificate is loaded, the key pair file is stored in the NOR flash, and the file in the **security** directory is deleted. After the SSL policy is deleted, the file in the NOR flash is deleted. To re-load the certificate, upload the key file again.

Example

Load an ASN1 digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] certificate load asn1-cert servercert.der key-pair dsa key-file
serverkey.der
```

Load a PEM digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] certificate load pem-cert servercert.pem key-pair dsa key-file
serverkey.pem auth-code cipher YsHsjx_202206
```

Load a PFX digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pfx-cert servercert.pfx key-pair dsa key-file
serverkey.pfx auth-code cipher YsHsjx_202206
```

Load a PEM certificate chain for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pem-chain chain-servercert.pem key-pair dsa key-file
chain-servercertkey.pem auth-code cipher YsHsjx_202206
```

2.7.12 close

Function

The **close** command terminates the connection with the remote FTP server and retains the FTP client view.

Format

close

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is equivalent to the **disconnect** command.

You can run the **bye** and **quit** commands to terminate the connection with the remote FTP server and enter the user view.

Precautions

To enter the user view from the FTP client view, you can run the **bye** or **quit** command.

Example

Terminate the connection with the remote FTP server and enter the FTP client view.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] close
221 Server closing.

[ftp]
```

2.7.13 copy

Function

The **copy** command copies a file.

The **copy** command allows downloading files from an HTTP/HTTPS server or uploading files to an HTTP/HTTPS server.

NOTE

HTTPS is recommended because it is more secure than HTTP.

Format

copy *source-filename destination-filename* [**all**]

copy { *source-http-urlname destination-filename* | *source-filename destination-http-urlname* } [**username** *user-name* **password** *password*]
(V200R013C00SPC500 or later)

copy { *source-https-urlname destination-filename* | *source-filename destination-https-urlname* } [**username** *user-name* **password** *password*] **ssl-policy** *ssl-policy*
(V200R013C00SPC500 or later)

Parameters

Parameter	Description	Value
source-filename	Specifies the path and name of a source file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
destination-filename	Specifies the path and name of a destination file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
all	Copies a file to all member devices. **NOTE** This parameter is available only in a stack system.	-
username *user-name*	Specifies the user name used to log in to a server.	The value is a string of 1 to 64 characters.
password *password*	Specifies the password used to log in to a server.	The value is a string of 1 to 64 characters.
source-http-urlname	Specifies the URL of an HTTP server from which a file is downloaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.
destination-http-urlname	Specifies the URL of an HTTP server to which a file is uploaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.

Parameter	Description	Value
source-https-urlname	Specifies the URL of an HTTPS server from which a file is downloaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.
destination-https-urlname	Specifies the URL of an HTTPS server to which a file is uploaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.
ssl-policy *ssl-policy*	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file name is not specified, the designation file and the source file have the same name. If the source file and the destination file are in the same directory, you must specify the destination file name. If the destination file name is not specified, you cannot copy the source file.

- If the destination file name is the same as that of an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.

Example

Copy the file **config.cfg** from the root directory of the flash card to flash:/temp. The destination file name is **temp.cfg**.

```
<HUAWEI> copy flash:/config.cfg flash:/temp/temp.cfg
Copy flash:/config.cfg to flash:/temp/temp.cfg?[Y/N]:y
100%  complete.
Info: Copied file flash:/config.cfg to flash:/temp/temp.cfg...Done.
```

If the current directory is the root directory of the flash card, you can perform the preceding configuration using the relative path.

```
<HUAWEI> pwd
flash:
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0   -rw-      6,721,804  Mar 19 2012 12:31:58   devicesoft.cc
    1   -rw-            910  Mar 19 2012 12:32:58   config.cfg
    2   drw-              -  Mar 05 2012 09:54:34   temp
...
65,233 KB total (7,289 KB free)
<HUAWEI> copy config.cfg temp/temp.cfg
Copy flash:/config.cfg to flash:/temp/temp.cfg?[Y/N]:y
100%  complete.
Info: Copied file flash:/config.cfg to flash:/temp/temp.cfg...Done.
```

Copy the file **config.cfg** from the root directory of the flash card to flash:/temp. The destination file name is **config.cfg**.

```
<HUAWEI> pwd
flash:
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0   -rw-      6,721,804  Mar 19 2012 12:31:58   devicesoft.cc
    1   -rw-            910  Mar 19 2012 12:32:58   config.cfg
    2   drw-              -  Mar 05 2012 09:54:34   temp
...
65,233 KB total (7,289 KB free)
<HUAWEI> copy config.cfg temp
Copy flash:/config.cfg to flash:/temp/config.cfg?[Y/N]:y
100%  complete.
Info: Copied file flash:/config.cfg to flash:/temp/config.cfg...Done.
```

Copy the file **backup.zip** to **backup1.zip** in the test directory from the current working directory flash:/test/.

```
<HUAWEI> pwd
flash:/test
<HUAWEI> copy backup.zip backup1.zip
Copy flash:/test/backup.zip to flash:/test/backup1.zip?[Y/N]:y
100%  complete.
Info: Copied file flash:/test/backup.zip to flash:/test/backup1.zip...Done.
```

2.7.14 crl load

Function

The **crl load** command loads the CRL for the SSL policy.

The **undo crl load** command unloads the SSL policy CRL.

By default, the SSL policy CRL is not loaded.

Format

crl load { **pem-crl** | **asn1-crl** } *crl-filename*

undo crl load { **pem-crl** | **asn1-crl** } *crl-filename*

Parameters

Parameter	Description	Value
pem-crl	Loads the CRL in the PEM format for the SSL policy.	-
asn1-crl	Loads the CRL in the ASN1 format for the SSL policy.	-
crl-filename	Specifies the name of a CRL. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 case-insensitive characters without spaces. The file name is the same as that of the uploaded file.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The CA can shorten the validity period of a certificate using a CRL. The CA releases the CRL that specifies a set of invalid certificates. If the CA revokes a certificate in the CRL, the declaration about authorized key pair is revoked before the certificate expires. When the certificate expires, data related to the certificate is cleared from the CRL.

If the certificate key is disclosed or if you need to revoke a certificate due to other reasons, use a third-party tool to revoke released certificates and mark them as invalid, generating a CRL.

Prerequisites

Before running the **crl load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

- When you load the CRL on the FTPS client and access the FTPS server on the FTPS client, the FTPS server checks whether the certificate is declared in the CRL. If the certificate has been declared, the FTPS client and server disconnects.
- A maximum of two CRL files can be loaded in an SSL policy. For the sake of security, deleting the installed CRL file is not recommended; otherwise, services using the SSL policy will be affected.

Example

Load the CRL in the PEM format for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] crl load pem-crl server.pem
```

Load the CRL in the ASN1 format for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] crl load asn1-crl server.der
```

2.7.15 delete (FTP client view)

Function

The **delete** command deletes a file from the FTP server.

Format

delete *remote-filename*

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

A file deleted in the FTP client view cannot be restored.

Example

Delete the file **temp.c**.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] delete temp.c
Warning: File temp.c will be deleted. Continue? [Y/N]: y
250 DELE command successfully.
```

2.7.16 delete (user view)

Function

The **delete** command deletes a specified file in the storage device.

Format

delete [**/unreserved**] [**/quiet**] { *filename* | *devicename* } [**all**]

Parameters

Parameter	Description	Value
/unreserved	Deletes a specified file. The deleted file cannot be restored.	-
/quiet	Deletes a file directly without any confirmation.	-

Parameter	Description	Value
filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
devicename	Deletes all the files in the storage device.	-
all	Deletes files in the specified directory in a batch from all storage devices. **NOTE** This parameter is available only in a stack system.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- The wildcard (*) character can be used in the **delete** command.
- If the parameter **/unreserved** is not included, the file is stored in the recycle bin. To display all files including deleted files that are displayed in square brackets ([ ]), run the **dir /all** command. To restore these files that are displayed in square brackets ([ ]), run the **undelete** command. To clear these files from the recycle bin, run the **reset recycle-bin** command.

NOTICE

If you delete a file using the **/unreserved** parameter, the file cannot be restored.

- If you delete a specified storage device, all files are deleted from the root directory of the storage device.
- If you delete two files with the same name from different directories, the last file deleted is kept in the recycle bin.
- If you attempt to delete a protected file, such as a configuration file, log file, or patch file, a system prompt is displayed.
- If you need to delete protected log files, you can run the **info-center max-logfile-number** command to modify the maximum number of protected log files. When the number of log files exceeds the maximum value, the system will delete the older log files to ensure that the number of log files is less than or equal to the configured value.
- You cannot delete a directory by running the **delete** command. To delete a directory, run the **rmdir (user view)** command.

Example

Delete the file **test.txt** from the **flash:/test/** directory.

```
<HUAWEI> delete flash:/test/test.txt
Delete flash:/test/test.txt?[Y/N]:y
```

Delete the file **test.txt** from the current working directory **flash:/selftest**.

```
<HUAWEI> delete test.txt
Delete flash:/selftest/test.txt?[Y/N]:y
```

2.7.17 dir (user view)

Function

The **dir** command displays information about files and directories in the storage medium.

NOTE

The **dir** command cannot display information about files and directories in a USB flash drive.

Format

dir [**/all**] [*filename* | *directory* | **/all-filesystems**]

Parameters

Parameter	Description	Value
/all	Displays information about all files and directories in the current directory, including files and directories moved to the recycle bin from the current directory.	-

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
directory	Specifies the file directory.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] path** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
/all-filesystems	Display information about files and directories in the root directories of all the storage media on the device.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The wildcard character (*) can be used in this command. If no parameter is specified, this command displays information about files and directories in the current directory.

The following describes the drive name:

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

You can run the **dir /all** command to view information about all files and directories of the storage medium, including those moved to the recycle bin. The name of a file in the recycle bin is placed in square brackets ([]), for example, [test.txt].

Example

Display information about all files and directories in the current directory.

```
<HUAWEI> dir /all
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            889  Feb 25 2012 10:00:58   private-data.txt
    1  -rw-          6,311  Feb 17 2012 14:05:04   backup.cfg
    2  -rw-            836  Jan 01 2012 18:06:20   rr.dat
    3  drw-              -  Jan 01 2012 18:08:20   logfile
    4  -rw-            836  Jan 01 2012 18:06:20   rr.bak
    5  drw-              -  Feb 27 2012 00:00:54   security
    6  -rw-        523,240  Mar 16 2011 11:21:36   bootrom_53hib66.bin
    7  -rw-          2,290  Feb 25 2012 16:46:06   vrpcfg.cfg
    8  -rw-            812  Dec 12 2011 15:43:10   hostkey
    9  drw-              -  Jan 01 2012 18:05:48   compatible
   10  -rw-     25,841,428  Nov 17 2011 09:48:10   basicsoft.cc
   11  -rw-            540  Dec 12 2011 15:43:12   serverkey
   12  -rw-     26,101,692  Dec 21 2011 11:44:52   devicesoft.cc
   13  -rw-          6,292  Feb 14 2012 11:14:32   1.cfg
   14  -rw-          6,311  Feb 17 2012 10:22:56   1234.cfg
   15  -rw-          6,311  Feb 25 2012 17:22:30   [11.cfg]

65,233 KB total (13,632 KB free)
```

Display information about files and directories in the root directories of all the storage media on the devices in a stack.

```
<HUAWEI> dir /all-filesystems
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         10,872  Nov 22 2012 20:26:28   private-data.txt
    1  -rw-            836  Nov 22 2012 20:26:44   rr.dat
    2  -rw-            836  Nov 22 2012 20:26:44   rr.bak
    3  -rw-          1,640  Nov 22 2012 20:24:50   vrpcfg.zip
    4  -rw-             10  Jun 05 2012 09:58:50   dhcp-duid
    5  -rw-        216,399  Nov 22 2012 20:16:52   patch_all_pack.pat
    6  drw-              -  Nov 22 2012 20:06:58   dhcp
    7  drw-              -  Nov 22 2012 20:26:32   compatible
    8  drw-              -  Nov 22 2012 20:28:46   logfile
    9  -rw-          1,399  Oct 25 2012 16:32:12   vrpcfg11.zip
   10  drw-              -  Sep 26 2009 11:02:52   user
   11  -rw-     15,298,556  Nov 20 2012 03:21:16   basicsoft.cc
   12  -rw-        289,596  Nov 16 2012 14:58:00   patch.pat

65,233 KB total (33,632 KB free)

Directory of slot1#flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         10,872  Nov 22 2012 20:28:24   private-data.txt
    1  -rw-            836  Nov 22 2012 20:27:48   rr.dat
    2  -rw-            836  Nov 22 2012 20:27:48   rr.bak
    3  -rw-          1,640  Nov 22 2012 20:24:52   vrpcfg.zip
    4  -rw-             10  Oct 10 2008 22:58:40   dhcp-duid
    5  -rw-        216,399  Nov 22 2012 14:34:36   patch_all_pack.pat
    6  drw-              -  Nov 22 2012 20:28:22   dhcp
    7  drw-              -  Nov 22 2012 20:27:16   compatible
    8  drw-              -  Oct 10 2008 23:00:40   logfile
    9  drw-              -  Nov 24 2012 00:00:18   resetinfo
   10  drw-              -  Sep 26 2009 11:03:02   user
   11  -rw-     15,298,556  Nov 21 2012 14:39:54   basicsoft.cc

65,233 KB total (33,632 KB free)
```

Display information about the file vrpcfg.cfg in the current directory.

```
<HUAWEI> dir vrpcfg.cfg
Directory of flash:/
```

```
  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-          2,290  Feb 25 2012 16:46:06   vrpcfg.cfg

65,233 KB total (13,632 KB free)
```

Display information about all .txt files in the current directory.

```
<HUAWEI> dir *.txt
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            889  Feb 25 2012 10:00:58   private-data.txt

65,233 KB total (13,632 KB free)
```

Table 2-46 Description of the **dir** command output

Item	Description
d	Directory. If this item is not displayed, the corresponding **FileName** field displays a file. For example, **devicesoft.cc** is a file and **security** is a directory.
r	The file or directory is readable.
w	The file or directory is writable.
[ ]	A file moved to the recycle bin.
FileName	● private-data.txt: The file saves service initialization data. Initialization data of some tasks is irrelevant to the configuration and is not recorded in the configuration file. The **private-data.txt** file records initialization data of these tasks, for example, the number of times the device restarts. ● vrpcfg.cfg: configuration file. The file name extension of the configuration file must be .cfg or .zip. ● basicsoft.cc: system software. The file name extension of the system software must be .cc. ● logfile: log file. Some software sub-systems store necessary data in other files in the file system when the device is running properly.

2.7.18 dir/ls (FTP client view)

Function

The **dir** and **ls** commands display all files or specified files that are stored on the FTP server, and save them to a local disk.

Format

dir [*remote-filename* [*local-filename*]]

ls [*remote-filename* [*local-filename*]]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name and directory of a file stored on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of the local file that saves the FTP server file information.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes differences between the **dir** and **ls** commands.

- When you run the **dir** command, detailed file information is displayed, including the file size, date when the file was created, whether the file is a directory, and whether the file can be modified. When you run the **ls** command, only the file name is displayed.
- The **dir** command is used to save detailed file information, while the **ls** command is used to save only the file name even if the file is specified and saved in a local directory.

Precautions

A wildcard character (*) can be used in commands **dir** and **ls**.

Example

Display the name or detailed information about a file that is saved in the test directory.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] cd test
250 CWD command successfully.
```

```
[ftp] dir
200 Port command okay.
150 Opening ASCII mode data connection for *.
drwxrwxrwx   1 noone    nogroup         0 Mar 24 10:48 .
drwxrwxrwx   1 noone    nogroup         0 Mar 26 15:52 ..
drwxrwxrwx   1 noone    nogroup         0 Mar 23 16:04 yourtest
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 10:38 backup.txt
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 10:38 backup1.txt
226 Transfer complete.
[ftp] ls
200 Port command okay.
150 Opening ASCII mode data connection for *.
. ..
yourtest
backup.txt
backup1.txt
226 Transfer complete.
```

Display the detailed information for the file **temp.c**, and save the displayed information in file **temp1**.

```
[ftp] dir temp.c temp1
200 Port command okay.
150 Opening ASCII mode data connection for temp.c.

226 Transfer complete.

[ftp] quit

221 Server closing.

<HUAWEI> more temp1
-rwxrwxrwx  1  noone   nogroup  3929  Apr 27 18:13  temp.c
```

Display the name of file **test.bat**, and save the displayed information in file **test**.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[ftp] ls test.bat test
200 Port command okay.
150 Opening ASCII mode data connection for test.bat.

226 Transfer complete.

[ftp] quit

221 Server closing.

<HUAWEI> more test
test.bat
```

Table 2-47 Description of the dir/ls command output

Item	Description
d	Indicates a directory. If this parameter is not present, the command output indicates a file.
r	Indicates that the file or directory can be read.

Item	Description
w	Indicates that the file or directory can be modified.

2.7.19 dir/ls (SFTP client view)

Function

The **dir** and **ls** commands display a list of specified files that are stored on the SFTP server.

Format

dir [**-l** | **-a**] [*remote-directory*]

ls [**-l** | **-a**] [*remote-directory*]

Parameters

Parameter	Description	Value
-l	Displays detailed information about all files and directories in a specified directory.	-
-a	Displays names of all files and directories in a specified directory.	-
remote-directory	Specifies the name of a directory on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

The **dir** and **ls** commands are equivalent.

- If **-l** and **-a** parameters are not specified, detailed information about all files and directories in a specified directory is displayed when you run the **dir** or **ls** command. The effect is the same as the **dir -l** command output.
- By default, if the *remote-directory* parameter is not specified, the list of current directory files is displayed when you run the **dir** or **ls** command.

Example

Display a list of files in the **test** directory of the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> dir test
drwxrwxrwx   1 noone    nogroup         0 Mar 24 2012 .
drwxrwxrwx   1 noone    nogroup         0 Mar 29 2012 ..
-rwxrwxrwx   1 noone    nogroup         0 Mar 24 2012 yourtest
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 2012 backup.txt
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 2012 backup1.txt
sftp-client> dir -a test
.
..
yourtest
backup.txt
backup1.txt
sftp-client> ls test
drwxrwxrwx   1 noone    nogroup         0 Mar 24 2012 .
drwxrwxrwx   1 noone    nogroup         0 Mar 29 2012 ..
-rwxrwxrwx   1 noone    nogroup         0 Mar 24 2012 yourtest
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 2012 backup.txt
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 2012 backup1.txt
sftp-client> ls -a test
.
..
yourtest
backup.txt
backup1.txt
```

2.7.20 disconnect

Function

The **disconnect** command terminates the connection with the remote FTP server and displays the FTP client view.

Format

disconnect

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

This command is equivalent to the **close** command.

You can run the **bye** and **quit** commands to terminate the connection with the remote FTP server and enter the user view.

To enter the user view from the FTP client view, you can run the **bye** or **quit** command.

Example

Terminate the connection with the remote FTP server and enter the FTP client view.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] disconnect

221 Server closing.

[ftp]
```

2.7.21 display ftp-client

Function

The **display ftp-client** command displays the source IP address configured for the FTP client.

Format

display ftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The default source IP address 0.0.0.0 is used if **ftp client-source** is not configured.

Example

Display the source IP address of the FTP client.

```
<HUAWEI> display ftp-client
The source address of FTP client is 10.1.1.1.
```

Table 2-48 Description of the display ftp-client command output

Item	Description
The source IP address of FTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the FTP client. You can run the **ftp client-source** command to configure the source IP address. If a source IP address has been configured by using the **ftp client-source** command, the message "The source interface of FTP client is LoopBack0" is displayed.

2.7.22 display ftp-server

Function

The **display ftp-server** command displays FTP server parameter settings.

Format

display [**ipv6**] **ftp-server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to display FTP server parameter settings.

Example

Display FTP server parameter settings.

```
<HUAWEI> display ftp-server
  FTP server is running
  Max user number              5
  User count                   1
  Timeout value(in minute)       30
  Listening port               21
  Acl number                   2010
  FTP server's source address     10.1.1.1
  FTP SSL policy
  FTP Secure-server is stopped
```

Display FTP server parameter settings when the secure FTP server function is enabled.

```
<HUAWEI> display ftp-server
  FTP server is stopped
  Max user number              5
  User count                   0
  Timeout value(in minute)       1
  Listening port               21
  Acl number                   0
  FTP server's source interface   LoopBack0
  FTP SSL policy
  FTP Secure-server is running
```

Table 2-49 Description of the display ftp-server command output

Item	Description
FTP server is running	The FTP server starts. You can run the **ftp** [**ipv6**] **server enable** command to start the FTP server.
Max user number	Maximum number of users who can access the FTP server.
User count	Number of users who are accessing the FTP server.
Timeout value(in minute)	Idle timeout duration of FTP users. You can run the **ftp** [**ipv6**] **timeout** command to set the idle timeout duration of FTP users.
Listening port	Number of the listening port on the FTP server. The default value is 21. If the value is not 21, you can run the **ftp** [**ipv6**] **server port** command to configure the listening port number.
Acl number	Number of the ACL of the FTP server. The default value is 0. You can run the **ftp** [**ipv6**] **acl** command to change the ACL number.

Item	Description
FTP server's source address	Source IP address for the FTP server to send packets. The default value is 0.0.0.0. You can run the **ftp server-source** command to configure the source IP address for the FTP server. Here, the source IP address 10.1.1.1 is displayed. If a source interface is configured, this field displays "FTP server's source interface." **NOTE** If you run the **display ipv6 ftp-server** command, the **FTP server's source address** is not displayed.
FTP SSL policy	SSL policy that the secure FTP server function uses. Before enabling the FTP function, you must run the **ftp secure-server ssl-policy** *policy-name* command to configure the SSL policy.
FTP Secure-server is stopped	Whether to enable the secure FTP server function. To enable the secure FTP server function, disable the common FTP function and run the **ftp secure-server enable** command.

2.7.23 display ftp-users

Function

The **display ftp-users** command displays FTP user parameters on the FTP server.

Format

display ftp-users

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can check FTP user parameters on the FTP server, such as the FTP user name, IP address of the client host, port number, idle duration, and the authorized directories.

Example

Display FTP user parameters.

```
<HUAWEI> display ftp-users
 username  host                                  port  idle  topdir
 user      10.138.77.41                          4028  0     flash:/test
 huawei    10.137.217.159                           51156 0     flash:
```

The preceding information indicates that two users are connected to the FTP server.

Table 2-50 Description of the display ftp-users command output

Item	Description
username	FTP user name.
host	IP address of the client host.
port	Port number of the client host.
idle	Idle duration.
topdir	Authorized directory of a user. You can run the **local-user ftp-directory** command to configure the authorized directory.

2.7.24 display scp-client

Function

The **display scp-client** command displays source parameters of the current SCP client.

Format

display scp-client

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display scp-client** command to check source parameters of the SCP client.

If **scp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* } is not configured, source parameters are not displayed.

Example

Display source parameters of the SCP client.

```
<HUAWEI> display scp-client
 The source of SCP ipv4 client: 10.1.1.1
```

2.7.25 display sftp-client

Function

The **display sftp-client** command displays the source IP address configured for the SFTP client.

Format

display sftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display sftp client** command to display the source IP address of the SFTP client. The default source IP address 0.0.0.0 is used if **sftp client-source** is not configured.

Example

Display the source IP address configured for the SFTP client.

```
<HUAWEI> display sftp-client
The source address of SFTP client is 10.1.1.1.
```

Table 2-51 Description of the display sftp-client command output

Item	Description
The source address of SFTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the SFTP client. You can run the **sftp client-source** command to configure the source IP address for the SFTP client. If an IP address has been configured for the source port, the message "The source interface of SFTP client is LoopBack0" is displayed.

2.7.26 display ssl policy

Function

The **display ssl policy** command displays information about an SSL policy.

Format

display ssl policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specific SSL policy. If the SSL policy name is not specified, configurations of all SSL policies are displayed.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ssl policy** command to display the SSL policy configuration when the device functions as a server or client.

After an SSL policy and its certificates are loaded and configured, you can run this command to obtain information such as the SSL policy name, service applications supported by the SSL policy, certificate name, and certificate type so that you can determine whether the existing SSL policy and certificates are available.

Example

Display the configuration of SSL policy **ftp_server**.

```
<HUAWEI> display ssl policy ftp_server
       SSL Policy Name: ftp_server
     Policy Applicants:
         Key-pair Type: DSA
 Certificate File Type: ASN1
      Certificate Type: certificate
  Certificate Filename: servercert.der
     Key-file Filename: serverkey.der
             Auth-code:
                   MAC:
              CRL File:
       Trusted-CA File:
           Issuer Name:
   Validity Not Before:
    Validity Not After:
```

Display the configuration of SSL policy **ftp_client**.

```
<HUAWEI> display ssl policy ftp_client

       SSL Policy Name: ftp_client
     Policy Applicants:
         Key-pair Type: RSA
 Certificate File Type: ASN1
      Certificate Type: certificate
  Certificate Filename: servercert.der
     Key-file Filename: serverkey.der
             Auth-code:
                   MAC:
              CRL File:
       Trusted-CA File:
           Issuer Name:
   Validity Not Before:
    Validity Not After:
```

Table 2-52 Description of the display ssl policy command output

Item	Description
SSL Policy Name	SSL policy name. You can run the **ssl policy** command to configure the SSL policy name.
Policy Applicants	Service using SSL policies. Currently, SSL policies are supported in HTTP, FTP and Syslog services.

Item	Description
Key-pair Type	Type of a key pair. - RSA - DSA - ECC You can run the **certificate load** command to configure the type of a key pair.
Certificate File Type	Certificate format. This parameter is mandatory when the device functions as a server. - PEM - ASN1 - PFX You can run the **certificate load** command to configure the certificate format.
Certificate Type	Certificate type. This parameter is mandatory when the device functions as a server. - certificate - certificate-chain You can run the **certificate load** command to configure the certificate type.
Certificate Filename	Certificate name. This parameter is mandatory when the device functions as a server. You can run the **certificate load** command to configure the certificate name.
Key-file Filename	Key pair file name. This parameter is mandatory when the device functions as a server. You can run the **certificate load** command to configure the key pair file name.
Auth-code	Authentication code of a key file. You can run the **certificate load** command to configure the authentication code of a key file. If an ASN1 certificate is loaded, the authentication code is unavailable.

Item	Description
MAC	Message authentication code. The message authentication code is required only when you load PFX digital certificates. You can run the **certificate load** command to configure the message authentication code.
CRL File	CRL file. You are advised to configure the CRL file for a client. You can run the **crl load** command to configure the CRL file.
Trusted-CA File	File of a trusted CA. This parameter is mandatory when the device functions as a client. ● **Format**: file format. ● **Auth-code**: authentication code of a PFX file. This field is displayed only when a PFX file has been loaded to the device. ● **Filename**: file name. You can run the **trusted-ca load** command to configure the file of a trusted CA.
Issuer Name	Issuer name.
Validity Not Before	Time when validity starts.
Validity Not After	Time when validity ends.

2.7.27 display tftp-client

Function

The **display tftp-client** command displays the source IP address configured for the TFTP client.

Format

display tftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display tftp client** command to query source IP address of the TFTP client. The default source IP address is 0.0.0.0 if **tftp client-source** is not configured.

Example

Display the source IP address configured for the TFTP client.

```
<HUAWEI> display tftp-client
The source address of TFTP client is 10.1.1.1.
```

Table 2-53 Description of the display tftp-client command output

Parameter	Description
The source address of TFTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the TFTP client. You can run the **tftp client-source** command to configure the source IP address for the TFTP client. If the IP address is configured for the source port, the message "The source interface of TFTP client is LoopBack0" is displayed.

2.7.28 execute

Function

The **execute** command executes a specified batch file.

Format

execute *batch-filename*

Parameters

Parameter	Description	Value
batch-filename	Specifies the name of a batch file. *batch-filename* supports file name association. The disk and directory where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk, directory, and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 160 case-sensitive characters. It cannot contain spaces. The file name extension is .bat.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a series of commands are frequently executed, write these commands in a batch file, and store this file in system. In this way, you can only execute this command to run multiple commands which were manually entered before. This command improves maintenance and management efficiency.

NOTE

- The batch file is edited in .txt format. When editing the file, ensure that one command occupies one line. After editing the file, save the file and change the file name extension to .bat.
- Transfer the batch file in file transmission mode to the device.

Prerequisites

Before running the **execute** command, ensure that the batch file to be processed is in the current directory; otherwise, the system cannot find the batch file.

Precautions

- The commands in a batch file are run one by one. A batch file cannot contain invisible characters (control characters or escape characters, such as \r, \n, and \b). If any invisible character is detected, the execute command exits from the current process and no rollback is performed.
- The **execute** command does not ensure that all commands can be run. If the system runs a wrong or immature command, it displays the error and goes to

next command. The **execute** command does not perform the hot backup operation, and the command format or content is not restricted.

- In case of interactive commands, batch file execution waits the device to interact with users before continuing.

NOTE

When processing files in batches, add the **echo off** field in the first line to mask command line prompts. After the **echo off** field is added, the command line prompts and command lines are not displayed when command lines are processed in batches. Comply with the following rules:

- The **echo off** field can be added only to the first line of the files to be processed in batches.
- The **echo off** field is case-insensitive.
- The line where the **echo off** field resides cannot contain any special characters, spaces excluded.

In the batch file, you can enter **wait(*time*)** between commands to set a command execution delay. The value of *time* ranges from 1 to 1800, in seconds. For example, **wait(10)** indicates that the next command is executed 10 seconds later. The value of **wait(*time*)** is case-insensitive. In the line where **wait(*time*)** resides, spaces cannot be placed before or after **wait(*time*)**, or before or after *time*. Other characters are also not allowed.

Example

Execute the **test.bat** file in the directory flash:/. The **test.bat** file contains the following commands: **system-view**, **local-user huawei password irreversible-cipher Helloworld@6789**, and **aaa**.

```
<HUAWEI> system-view
[HUAWEI] execute test.bat
[HUAWEI]
        ^
Error: Unrecognized command found at '^' position.
[HUAWEI]
[HUAWEI-aaa]
 Info: Add a new user
[HUAWEI-aaa]
```

When the system runs the first command **system-view** in the current system view, it displays an error and continues to run the following commands.

The system displays the execution of a batch file in AAA view.

```
[HUAWEI-aaa] display this
 local-user huawei password irreversible-cipher $1a$HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~\#
%iAut}_~O%0L$
```

2.7.29 feat

Function

The **feat** command displays extended commands that the FTP server supports.

Format

feat

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **feat** command to display extended functions that the FTP server supports, such as:

- Authentication transport layer security (AUTH TLS)
- Data channel protection level (PROT)
- Protection buffer size (PBSZ)

Precautions

If no extended command is supported, the message "211 no features" is displayed.

Example

Display extended commands that the FTP server supports.

```
[ftp] feat
211-Extension Supported
AUTH TLS
PROT
PBSZ
211 End
```

Table 2-54 Description of the feat command output

Parameter	Description
211	Value of the FTP relay code. The value is returned in the help information or system status query result.
AUTH TLS	AUTH TLS commands supported.
PROT	PROT commands supported.s
PBSZ	PBSZ commands supported.

2.7.30 file prompt

Function

The **file prompt** command changes the prompt mode when you perform operations on files.

The **undo file prompt** command restores the default prompt mode.

The default prompt mode is alert.

Format

file prompt { **alert** | **quiet** }

undo file prompt quiet

Parameters

Parameter	Description	Value
alert	Display a prompt message before users perform an operation.	-
quiet	Do not display a prompt message before users perform an operation.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

If the prompt mode is set to quiet, the system does not provide prompt messages when operations leading to data loss are executed, such as deleting or overwriting files. Therefore, this prompt mode should be used with caution.

Example

Set the prompt mode to quiet. When you rename a copied file **test.txt** using an existing file name **test1.txt**, no prompt message is displayed.

```
<HUAWEI> system-view
[HUAWEI] file prompt quiet
[HUAWEI] quit
<HUAWEI> copy test.txt test1.txt
```

```
100%  complete
Info: Copied file flash:/test.txt to flash:/test1.txt...Done.
```

Set the prompt mode to alert.

```
<HUAWEI> system-view
[HUAWEI] file prompt alert
[HUAWEI] quit
<HUAWEI> copy test.txt test1.txt
Copy flash:/test.txt to flash:/test1.txt?[Y/N]:y
The file flash:/test1.txt exists. Overwrite it?[Y/N]:y
100%  complete
Info: Copied file flash:/test.txt to flash:/test1.txt...Done.
```

2.7.31 fixdisk

Function

The **fixdisk** command restores a storage device in which the file system fails to run properly.

Format

fixdisk *drive*

Parameters

Parameter	Description	Value
drive	Specifies the name of the storage device to restore.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the storage device name.

- **drive** is the storage device and is named as flash:.
- In a stack system, *devicename* can be set as follows:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

If the file system does not run properly, the system prompts you to restore it. You can run the **fixdisk** command to attempt to restore the file system. You can run the **fixdisk** command to release the space whose usage status is unknown from the storage device.

You can run the **dir** command to display information about a specified file or directory on the storage device. If the command output contains **unknown**, for example, 30,000 KB total (672 KB free, 25,560 KB used, 3,616 KB unknown), you can run the **fixdisk** command to release the space whose usage status is unknown.

Precautions

- The **fixdisk** command is not recommended when the system works properly. This command cannot rectify device-level faults.
- If you are still prompted to restore the storage device after running the **fixdisk** command, the physical medium may have been damaged.
- Running the **fixdisk** command to restore a flash memory requires high CPU usage. Therefore, do not run this command when the CPU usage in the system is high.

Example

Restore the flash memory when an error message indicating that the flash memory is faulty is displayed.

```
Lost chains in flash detected, please use fixdisk to recover them!
<HUAWEI> fixdisk flash:
Fix disk flash: will take long time if needed...
% Fix disk flash: completed.
```

2.7.32 format

Function

The **format** command formats a storage device.

NOTE

In V200R013C00SPC500 and later versions, this command can be run only if you log in to the device through the serial port.

The following models do not support this command:

S300, S500, S2730S-S, S5735-L1, S5735S-L1, S5731-S (S5731-S24P4X, S5731-S24T4X, S5731-S24T4X-A, S5731-S24T4X-D, S5731-S48P4X, S5731-S48T4X, S5731-S48T4X-A), S5731S-S (S5731S-S24P4X-A, S5731S-S24T4X-A, S5731S-S24T4X-A1, S5731S-S48P4X-A, S5731S-S48T4X-A, S5731S-S48T4X-A1), S5731-H, S5731S-H, S5732-H (S5732-H24S6Q, S5732-H24UM2CC, S5732-H48S6Q, S5732-H48UM2CC), S6730-S, S6730S-S, S6730-H (S6730-H24X6C, S6730-H48X6C), S6730S-H

Format

format *drive*

Parameters

Parameter	Description	Value
drive	Specifies the name of the storage device to format.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the storage device name.

- **drive** is the storage device and is named as flash:.
- In a stack system, *devicename* can be set as follows:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

When the file system fault cannot be rectified or the data on the storage device is unnecessary, the storage device can be formatted. When you run the **format** command, all files and directories are cleared from the storage device.

Configuration Impact

When the storage device has the configuration file and system software package required for the next start, do not format the storage device because data on it will be deleted after the format. If the configuration file required for the next start is deleted, the configuration is lost after the switch restarts. If the system software package is deleted, the switch will fail to start.

After the storage is formatted, you can upload the system software through the Enter ethernet submenu option in the Bootload menu. The Modify startup configuration option modifies the startup configuration information and restarts the device.

Precautions

NOTICE

After the **format** command is run, files and directories are cleared from the specified storage device and cannot be restored. Therefore, this command should be used with caution.

If the storage device is still unavailable after the **format** command is run, a physical exception may have occurred.

Example

Format the storage device.

```
<HUAWEI> format flash:
All data(include configuration and system startup file) on flash: will be lost, proceed with format ? [Y/N]:y
%Format flash: completed.
```

2.7.33 format ssd

Function

The **format ssd** command formats the SSD card.

Format

format ssd [**slot** *slot-id*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, and S5731S-S support this command.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Application Scenario

When the file system fault cannot be rectified or all data on the SSD card is unnecessary, the SSD card can be formatted. When this command is run, all files and directories are cleared from the SSD card.

Configuration Impact

If the SSD card contains the configuration file and software package required for the next startup, do not format the card because formatting the SSD card will cause all data on the card to be cleared. As a result, the configuration file for the next startup is deleted, and configurations are lost after the device is restarted; the software package for the next startup is deleted, and the device cannot be started.

Precautions

NOTICE

After this command is run, all files and directories are cleared from the SSD card and cannot be restored. Therefore, exercise caution when running this command.

If the SSD card is still unavailable after this command is run, a physical exception may have occurred.

Example

Format the SSD card.

```
<HUAWEI> format ssd
Warning: The format requires a long time. All data on SSD will be lost, proceed
with format, Continue? [Y/N]:y
Info: Operating, please wait for a moment......................................
....
Info: Succeed in formating the SSD.
```

2.7.34 ftp

Function

The **ftp** command connects the FTP client to the FTP server and enters the FTP client view.

Format

Connect the FTP client to the FTP server based on the IPv4 address.

ftp [[**ssl-policy** *policy-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]]

Connect the FTP client to the FTP server based on the IPv6 address.

ftp [**ssl-policy** *policy-name*] **ipv6** *host-ipv6* [*port-number*]

ftp [**ssl-policy** *policy-name*] **ipv6** *ipv6-linklocal-address* **-oi** { *interface-name* | *interface-type interface-number* } [*port-number*]

Parameters

Parameter	Description	Value
ssl-policy *policy-name*	Specifies the name of the SSL policy that provides the secure FTP function.	The value is a string of 1 to 23 case-insensitive characters without spaces.

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the FTP client. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
port-number	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. The default value is the standard port number 21.
public-net	Specifies the FTP server on the public network. You must set the **public-net** parameter when the FTP server IP address is a public network IP address.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the FTP server is located.	The value must be an existing VPN instance name.

Parameter	Description	Value
host-ipv6	Specifies the IP address or host name of the remote IPv6 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-linklocal-address	Specifies the local link address that is automatically generated by the remote IPv6 FTP server.	-
-oi	Specifies the outbound interface for the local IPv6 link address.	-
interface-name	Specifies the name of the outbound interface for the local IPv6 link address.	-
interface-typeinterface-number	Specifies the number of the outbound interface for the local IPv6 link address.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before accessing the FTP server on the FTP client, you must first run the **ftp** command to connect the FTP client to the FTP server. If an SSL-based secure FTP connection is set up between the device and remote FTP server, you must specify **ssl-policy**. If the connection is a common FTP connection, you do not need to specify this parameter.

Precautions

- Before running the **ftp** command to set up a secure FTP connection, you must perform the following steps on the FTP client:

  a. In the system view, run the **ssl policy** command to create an SSL policy and enter the SSL policy view.
  b. In the SSL policy view, run the **trusted-ca load** command to load a trusted CA.
  c. In the SSL policy view, run the **crl load** command to load a CRL. This step is optional but recommended.
- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified on the IPv4 network. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If no parameter is set in the **ftp** command, only the FTP client view is displayed, and no connection is set up between the FTP server and client.
- If the port number that the FTP server uses is non-standard, you must specify a standard port number; otherwise, the FTP server and client cannot be connected.
- When you run the **ftp** command, the system prompts you to enter the user name and password for logging in to the FTP server. You can log in to the FTP server if the user name and password are correct.
- If the number of login users exceeds the maximum value that the FTP server allows (that is, 5), other authorized users cannot log in to the FTP server. To allow news authorized users to log in to the FTP server, users who have performed FTP services must disconnect their clients from the FTP server. You can run the **bye** or **quit** command to disconnect the FTP client from the FTP server and return to the user view, or run the **close** or **disconnect** command to disconnect the FTP client from the FTP server and retain in the FTP client view.

Example

Connect to the FTP server whose IP address is 10.137.217.201.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

Connect to the remote IPv6 FTP server whose address is fc00:2001:db8::1.

```
<HUAWEI> ftp ipv6 fc00:2001:db8::1
Trying fc00:2001:db8::1
Press CTRL+K to abort
Connected to ftp fc00:2001:db8::1
220 FTP service ready.
User(fc00:2001:db8::1:(none)):huawei
331 Password required for huawei
Enter Password:
230 User logged in.

[ftp]
```

Connect to the FTPS server whose IP address is 10.1.1.2.

```
<HUAWEI> ftp ssl-policy ftp_server 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
234 AUTH command successfully, Security mechanism accepted.
200 PBSZ is ok.
200 Data channel security level is changed to private.
User(10.1.1.2:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

2.7.35 ftp acl

Function

The **ftp acl** command specifies an ACL number for the current FTP server so that the FTP client with the same ACL number can access the FTP server.

The **undo ftp acl** command deletes an ACL number of the current FTP server.

By default, no ACL is configured for FTP server.

Format

ftp [**ipv6**] **acl** *acl-number*

undo ftp [**ipv6**] **acl**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
acl-number	Specifies the number of the ACL.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device functions as an FTP server, you can configure an access control list (ACL) on the device to control the source IP address, destination IP address, source port, destination port, VPN instance, and packets whose protocol type is TCP, allows specific clients to log in to the device through FTP.

Precautions

The **ftp server acl** command takes effect only after you run the **rule** command to configure the ACL rule.

Example

Allow the client whose ACL number is 2000 to log in to the FTP server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] ftp acl 2000
```

2.7.36 ftp client-source

Function

The **ftp client-source** command specifies the source IP address for the FTP client to send packets.

The **undo ftp client-source** command restores the default source IP address for the FTP client to send packets.

The default source IP address for the FTP client to send packets is 0.0.0.0.

Format

ftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo ftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the source interface on the local device.	The value is in dotted decimal notation.

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface of the local device. The IP address configured for the source interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **ftp server-source** command cannot be successfully executed.

Precautions

- You can also run the **ftp** command to configure the source IP address whose priority is higher than that of the source IP address specified by the **ftp client-source** command. If you specify the source IP addresses by running the **ftp client-source** and **ftp** commands, the source IP address specified by the **ftp** command is used for data communication and is available only for the current FTP connection, while the source IP address specified by the **ftp client-source** command is available for all FTP connections.
- The IP address that a user displays on the FTP server is the specified source IP address or source interface IP address.
- No source address or source interface is specified, so security risks exist.

Example

Set the source IP address of the FTP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the FTP client to 10.1.1.1.
```

2.7.37 ftp secure-server enable

Function

The **ftp secure-server enable** command enables the secure FTP server function for FTP users.

The **undo ftp secure-server** command disables the secure FTP server function.

By default, the secure FTP server function is disabled.

Format

ftp [**ipv6**] **secure-server enable**

undo ftp [**ipv6**] **secure-server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After SSL policies are configured on an FTP server, the secure FTP server function is provided based on SSL policies. To use the secure FTP server function, you must run the **ftp secure-server enable** command to enable the secure FTP server function. You can log in to the FTP server with secure FTP function configured from a client, and manage files between the FTP server and client.

Prerequisites

To enable the secure FTP server function, you must disable the common FTP server function.

Precautions

- If the FTP server function is disabled, no user can log in to the FTP server, and users who have logged in to the FTP server cannot perform any operation except logout.
- After the **ftp secure-server enable** command is run, the FTP server does not accept login requests from any interface by default, you should run the **ftp server-source** command to specify the source interface of the FTP server.
- After the **ftp ipv6 secure-server enable** command is run, the FTP server does not accept login requests from any IPv6 address by default, you should run the **ftp ipv6 server-source** command to specify the IPv6 source address for the FTP server.

Example

Enable the secure FTP server function.

```
<HUAWEI> system-view
[HUAWEI] ftp secure-server enable
```

2.7.38 ftp secure-server ssl-policy

Function

The **ftp secure-server ssl-policy** command configures an SSL policy for the FTP server.

The **undo ftp secure-server ssl-policy** command deletes an SSL policy from the FTP server.

By default, no SSL policy is configured for the FTP server.

Format

ftp secure-server ssl-policy *policy-name*

undo ftp secure-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The traditional FTP function transmits data in plain text, which can be intercepted and tampered with. You can run the **ftp secure-server ssl-policy** command to configure an SSL policy for the FTP server to ensure data security so that the FTP server implements session negotiation, sets up connections, and transmits data based on the SSL policy. You can log in to the FTP server from a client and manage files between the FTP server and client.

Prerequisites

Before running the **ftp secure-server ssl-policy** command to configure the SSL policy, you must first run the **ssl policy** command to create an SSL policy for the FTP server.

Precautions

- You must apply for a digital certificate for the FTP client from a trusted CA to authenticate the validity of the FTP server digital certificate.
- Only one SSL policy can be configured for the FTP server, and the latest configured SSL policy takes effect.

Example

Configure an SSL policy for the FTP server.

```
<HUAWEI> system-view
[HUAWEI] ftp secure-server ssl-policy ftp_server
```

2.7.39 ftp server enable

Function

The **ftp server enable** command enables the FTP server function to allow FTP users to log in to the FTP server.

The **undo ftp server** command disables the FTP server function so that FTP users cannot log in to the FTP server.

By default, the FTP function is disabled.

Format

ftp [**ipv6**] **server enable**

undo ftp [**ipv6**] **server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To manage FTP server files on a client, you must run the **ftp server enable** command to enable the FTP server function to allow FTP users to log in to the FTP server.

Prerequisites

Before enabling the FTP service, run either of the following commands as required:

- Run the **ftp server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the FTP server or run the **ftp server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the FTP server.
- Run the **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the FTP server or run the **ftp ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the FTP server.

Precautions

If the FTP server function is disabled, no user can log in to the FTP server, and users who have logged in to the FTP server cannot perform any operation except logout.

NOTICE

The FTP protocol compromises device security. SFTP V2 or FTPS mode is recommended.

Example

Enable the FTP server function.

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Succeeded in starting the FTP server.
```

2.7.40 ftp server max-sessions

Function

The **ftp server max-sessions** command sets the maximum number of sessions supported by the FTP server.

The **undo ftp server max-sessions** command restores the maximum number of sessions supported by the FTP server to the default value.

By default, the FTP server supports a maximum of five sessions.

Format

ftp [**ipv6**] **server max-sessions** *max-sessions-number*

undo ftp [**ipv6**] **server max-sessions**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
max-sessions *max-sessions-number*	Specifies the maximum number of sessions supported by the FTP server.	The value is an integer ranging from 0 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run this command to set the maximum number of sessions supported by the FTP server. When the number of online users is equal to the maximum number of sessions supported by the FTP server, other users cannot log in to the FTP server.

Example

Set the maximum number of sessions supported by the FTP server to 3.

```
<HUAWEI> system-view
[HUAWEI] ftp server max-sessions 3
```

2.7.41 ftp server port

Function

The **ftp server port** command specifies the listening port number of the FTP server.

The **undo ftp server port** command restores the default value of the listening port number.

The default value is 21.

Format

ftp [**ipv6**] **server port** *port-number*

undo ftp [**ipv6**] **server port**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
port *port-number*	Specifies the listening port number of the FTP server.	The value is 21 or an integer that ranges from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the listening port number of the FTP server is 21. Attackers may frequently access the default listening port, which wastes bandwidth, deteriorates server performance, and prevents authorized users from accessing the FTP server through the listening port. You can run the **ftp server port** command to specify another listening port number to prevent attackers from accessing the listening port.

Prerequisites

Before running the **ftp server port** command to specify the listening port number, you must first run the **undo ftp server** command to disable FTP services.

Precautions

- After the **ftp server port** command is executed, the FTP server disconnects all FTP connections and uses the new listening port.

- If the current listening port number is 21, FTP client users do not need to specify the port number for logging in to the FTP server. If the current listening port number is not 21, FTP client users must use the FTP server's listening port number to log in to the FTP server.
- After the listening port number is changed, you must run the **ftp server enable** command to enable FTP services to make the configuration take effect.

Example

Change the port number of the FTP server to 1028.

```
<HUAWEI> system-view
[HUAWEI] undo ftp server
[HUAWEI] ftp server port 1028
```

2.7.42 ftp server-source

Function

The **ftp server-source** command specifies the source IP address for an FTP server to send packets.

The **undo ftp server-source** command restores the default source IP address for an FTP server to send packets.

By default, the source IP address of an FTP server is not specified.

Format

ftp server-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo ftp server-source

ftp server-source all-interface

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the source interface on the local device.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface of the local device. The primary IP address of the source interface is the source IP address for sending packets. If no IP address is configured for the source IP address, the FTP connection cannot be set up.	-

Parameter	Description	Value
all-interface	Indicates that any interface that has an IPv4 address configured can be used as the source interface of an FTP server.	-

NOTE

In V200R020C00 and later versions, the source address for the FTP server to send packets is not specified by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, the default source IP address for the FTP server to send packets is 0.0.0.0, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, the default source IP address for the FTP server to send packets is not specified. To allow authorized users to log in to the FTP server, run either of the following commands to specify the source IP address of the FTP server.

- Run the **ftp server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the FTP server.
- Run the **ftp server-source all-interface** command to configure all interfaces configured with IPv4 addresses as the source interfaces of the FTP server.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **ftp server-source** command cannot be successfully executed.

Precautions

- After the source IP address is specified for the FTP server, you must use the specified IP address to log in to the FTP server.
- If the FTP service has been enabled, the FTP service restarts after the **ftp server-source** command is executed.

- After the **ftp server-source all-interface** command is run, the system allows FTP users to log in to the FTP server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Set the source IP address of the FTP server to **LoopBack0**.

```
<HUAWEI> system-view
[HUAWEI] ftp server-source -i loopback 0
Warning: To make the server source configuration take effect, the FTP server will be restarted. Continue? [Y/
N]: y
Info: Succeeded in setting the source interface of the FTP server to LoopBack0.
Info: Succeeded in starting the FTP server.
```

2.7.43 ftp ipv6 server-source

Function

The **ftp ipv6 server-source** command specifies an IPv6 source address for an FTP server.

The **undo ftp ipv6 server-source** command cancels the IPv6 source address specified for an FTP server.

By default, the IPv6 source address of an FTP server is not specified.

Format

ftp ipv6 server-source -a *ipv6_address* [**vpn-instance** *vpn_name*]

undo ftp ipv6 server-source

ftp ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies an IPv6 source address for an FTP server.	The total length of an IPv6 source address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the FTP server.	-

NOTE

In V200R020C00 and later versions, the source address for the FTP server to send packets is not specified by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, the default source IP address for the FTP server to send packets is ::, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, the default source IP address for the FTP server to send packets is not specified. To allow authorized users to log in to the FTP server, run either of the following commands to specify the source IP address of the FTP server.

- Run the **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*] command to specify the specified IPv6 address as the IPv6 source address of the FTP server.
- Run the **ftp ipv6 server-source all-interface** command to specify all interface IPv6 addresses on the device as the IPv6 source addresses of the FTP server.

Prerequisites

A VPN instance has been created before you specify it for an FTP server. Otherwise, the **ftp ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for an FTP server, FTP users can log in to the FTP server only using this IPv6 address. This configuration applies to the FTP users who attempt to log in to the FTP server, not to the FTP users who have logged in to the server.

Precautions

After an IPv6 source address is specified for an FTP server using this command, ensure that FTP users can access this IPv6 address at Layer 3. Otherwise, FTP users will fail to log in to the FTP server.

If the specified IPv6 source address is bound to a VPN instance, the FTP server is also bound to the VPN instance.

After the **ftp ipv6 server-source all-interface** command is run, the system allows FTP users to log in to the FTP server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for an FTP server.

```
<HUAWEI> system-view
[HUAWEI] ftp ipv6 server-source -a 2001:DB8::
```

2.7.44 ftp timeout

Function

The **ftp timeout** command configures the idle timeout duration of the FTP server.

The **undo ftp timeout** command restores the default idle timeout duration.

By default, the idle timeout duration of the FTP server is 10 minutes.

Format

ftp [**ipv6**] **timeout** *minutes*

undo ftp [**ipv6**] **timeout**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
minutes	Specifies idle timeout duration.	The value is an integer that ranges from 1 to 35791, in minutes. By default, the idle timeout duration is 10 minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

After a user logs in to the FTP server, a connection is set up between the FTP server and the user's client. The idle timeout duration is configured to release the connection when the connection is interrupted or when the user performs no operation for a specified time.

NOTICE

When you use the **get** command in the FTP view to overwrite a file, the operation may fail due to timeout of the FTP connection. To prevent this problem, set a long timeout period for the FTP connection.

Example

Set the idle timeout duration to 36 minutes.

```
<HUAWEI> system-view
[HUAWEI] ftp timeout 36
```

2.7.45 get (SFTP client view)

Function

The **get** command downloads a file from the SFTP server and saves the file to the local device.

Format

get *remote-filename* [*local-filename*]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be downloaded from the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of a downloaded file to be saved to the local device.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **get** command to download files from the FTP server to upgrade devices.

Precautions

- If *local-filename* is not specified on the local device, the original file name is used.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download a file from the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> get test.txt
Remote file: / test.txt --->  Local file: test.txt
Info: Downloading file successfully ended.
```

2.7.46 get (FTP client view)

Function

The **get** command downloads a file from the FTP server and saves the file to the local device.

Format

get *remote-filename* [*local-filename*]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be downloaded from the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of a downloaded file to be saved to the local device.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **get** command to download system software, backup configuration files, and patch files from the FTP server to upgrade devices.

Precautions

- If the downloaded file name is not specified on the local device, the original file name is used.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download the system software **devicesoft.cc** from the FTP server.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] get devicesoft.cc
200 Port command successful. 150 Opening BINARY mode data connection for file transfer. 226 Transfer
complete  FTP: 6482944 byte(s) received in 54.500 second(s) 1117.40Kbyte(s)/sec.
```

2.7.47 help (SFTP client view)

Function

The **help** command displays the help information in the SFTP client view.

Format

help [**all** | *command-name*]

Parameters

Parameter	Description	Value
all	Displays all commands in the SFTP client view.	-
command-name	Displays the format and parameters of a specified command in the SFTP client view.	-

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the SFTP view, you can only enter the question mark (?) to obtain all commands in the SFTP client view. If you enter a command keyword and the question mark (?) to query command parameters, an error message is displayed, as shown in the following:

```
sftp-client> dir ?
Error: Failed to list files.
```

You can run the **help** command to obtain the help information and display all commands or a command format in the SFTP client view.

Precautions

If you specify no parameter when running the **help** command, all commands in the SFTP client view are displayed. This has the same effect as the **help all** command or directly entering the question mark (?) in the SFTP client view.

Example

Display the format of the command **get**.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> help get
get Remote file name STRING<1-64>   [Local file name STRING<1-64>]  Download file
Default local file name is the same with remote file.
```

Display all commands in the SFTP client view.

```
sftp-client> help all
cd
cdup
dir
get
```

```
help
ls
mkdir
put
pwd
quit
rename
remove
rmdir
```

2.7.48 lcd

Function

The **lcd** command displays and changes the local working directory of the FTP client in the FTP client view.

Format

lcd [*local-directory*]

Parameters

Parameter	Description	Value
local-directory	Specifies the local working directory of the FTP client.	The value is a string of 1 to 128 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **lcd** command to display the local working directory of the FTP client when uploading or downloading files, and set the upload or download path to the path of the local working directory.

Precautions

The **lcd** command displays the local working directory of the FTP client, while the **pwd** command displays the working directory of the FTP server. If you specify the parameter *local-directory* in the **lcd** command, you can directly change the local working directory in the FTP client view.

Example

Change the local working directory to **flash:/test**.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] lcd
The current local directory is flash:.
[ftp] lcd flash:/test
The current local directory is flash:/test.
```

2.7.49 mget

Function

The **mget** command downloads multiple files from the remote FTP server to the local device.

Format

mget *remote-filenames*

Parameters

Parameter	Description	Value
remote-filenames	Specifies multiple files to download to the local device. File names are separated using spaces, and the wildcard (*) is supported.	The value is a string of 1 to 255 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **mget** command to download multiple files at the same time.

Precautions

- The command cannot download all files in a directory or subdirectory.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download files **1.txt**, **2.txt**, and **vrp221.cfg** from the remote FTP server.

```
<HUAWEI> ftp 10.10.10.1
Trying 10.10.10.1 ...
Press CTRL+K to abort
Connected to 10.10.10.1.
220 FTP service ready.
User(10.10.10.1:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] mget 1.txt 2.txt vrp221.cfg
200 Port command okay.
150 Opening ASCII mode data connection for 1.txt.

226 Transfer complete.
FTP: 3885 byte(s) received in 0.174 second(s) 22.32Kbyte(s)/sec.

200 Port command okay.
150 Opening ASCII mode data connection for 2.txt.

226 Transfer complete.
FTP: 8721 byte(s) received in 0.179 second(s) 48.72Kbyte(s)/sec.

200 Port command okay.
150 Opening ASCII mode data connection for vrp221.cfg.

226 Transfer complete.
FTP: 6700 byte(s) received in 0.151 second(s) 44.37Kbyte(s)/sec.

[ftp]
```

2.7.50 mkdir (FTP client view)

Function

The **mkdir** command creates a directory on the remote FTP server.

Format

mkdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the directory to be created.	The value is a string of case-insensitive characters without spaces. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

- You can run the **mkdir** command to create a subdirectory in a specified directory, and the subdirectory name must be unique.
- If no path is specified when you create a subdirectory, the subdirectory is created in the current directory.
- The created directory is stored on the FTP server.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Create a directory **test** on the remote FTP server.

```
<HUAWEI> ftp 172.16.104.110
Trying 172.16.104.110 ...
Press CTRL+K to abort
Connected to 172.16.104.110.
220 FTP service ready.
User(172.16.104.110:(none)):huawei
331 Password required for huawei
Enter password:
230 User logged in.

[ftp] mkdir test
257 "test" new directory created.
```

2.7.51 mkdir (SFTP client view)

Function

The **mkdir** command creates a directory on the remote SFTP server.

Format

mkdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the directory to be created.	The value is a string of case-insensitive characters without spaces. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can run the **mkdir** command to create a subdirectory in a specified directory, and the subdirectory name must be unique.
- If no path is specified when you create a subdirectory, the subdirectory is created in the current directory.
- The created directory is stored on the SFTP server.
- After a directory is created, you can run the **dir/ls (SFTP client view)** command to view the directory.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Create a directory on the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> mkdir ssh
Info: Succeeded in creating a directory.
```

2.7.52 mkdir (User view)

Function

The **mkdir** command creates a directory in the current storage device.

Format

mkdir *directory*

Parameters

Parameter	Description	Settings
directory	Specifies a directory or directory and its path.	The value is a string of case-insensitive characters in the **[drive] [path] directory** format. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

If you only the subdirectory name is specified, a subdirectory is created in the current working directory. You can run the **pwd** command to query the current working directory. If the subdirectory name and directory path are specified, the subdirectory is created in the specified directory.

Precautions

- The subdirectory name must be unique in a directory; otherwise, the message "Error: Directory already exists." is displayed.
- A maximum of four directory levels are supported when you create a directory.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Create the subdirectory **new** in the flash card.

```
<HUAWEI> mkdir flash:/new
Info: Create directory flash:/new......Done.
```

2.7.53 more

Function

The **more** command displays the content of a specified file.

Format

more *filename* [*offset*] [**all**]

Parameters

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
offset	Specifies the file offset.	The value is an integer that ranges from 0 to 2147483647, in bytes.
all	Displays all the file content on one screen.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **more** command to display the file content directly on a device.

- The following describes the drive name.
  - **drive** is the storage device and is named as **flash:**.
  - If devices are stacked, **drive** can be named as:
    - flash: root directory of the flash memory of the master switch in the stack.
    - chassis ID#flash: root directory of the flash memory on a device in the stack.

    For example, **slot2#flash:** indicates the flash memory in slot 2.
- The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working

directory. A relative path beginning with a slash (/) is a path relative to the root directory.

  - **flash:/my/test/** is an absolute path.
  - **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
  - **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- You are not advised to use this command to display non-text files; otherwise, the terminal is shut down or displays garbled characters, which is harmless to the system.
- Files are displayed in text format.
- You can display the file content flexibly by specifying parameters before running the **more** command:
  - You can run the **more** *filename* command to view a specified text file. The content of the specified text file is displayed on multiple screens. You can press the spacebar consecutively on the current session GUI to display all content of the file.

    To display the file content on multiple screens, you must ensure that:

    - The number of lines that can be displayed on a terminal screen is greater than 0. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
    - The total number of file lines is greater than the number of lines that can be displayed on a terminal screen. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
  - You can run the **more** *filename offset* command to view a specified file. The content of the specified text file starting from *offset* is displayed on multiple screens. You can press the spacebar consecutively on the current session GUI to display all content of the file.

    To display the file content on multiple screens, you must ensure that:

    - The number of lines that can be displayed on a terminal screen is greater than 0. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
    - The number of lines starting from *offset* in the file is greater than the number of lines that can be displayed on a terminal screen. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
  - You can run the **more** *file-name* **all** command to view a specified file. The file content is displayed on one screen.

Example

Display the content of the file **test.bat**.

```
<HUAWEI> more test.bat
rsa local-key-pair create
```

```
user-interface vty 12 14
authentication-mode aaa
protocol inbound ssh
user privilege level 5
quit
ssh user sftpuser authentication-type password
ssh user sftpuser service-type all
sftp server enable
```

Display the content of the file **log.txt** and set the offset to 100.

```
<HUAWEI> more log.txt 100
:               CHINA HUAWEI TECHNOLOGY LIMITTED CO.,LTD
#   FILE NAME:                 Product Adapter File(PAF)
#   PURPOSE:                   MAKE VRPV5 SUITABLE FOR DIFFERENT PRODUCT IN LIB
#   SOFTWARE PLATFORM:         V6R2C00
#   DETAIL VERSION:            B283
#   DEVELOPING GROUP:          8090 SYSTEM MAINTAIN GROUP
#   HARDWARE PLATFORM:         8090 (512M Memory)
#   CREATED DATE:              2003/05/10
#   AUTH:                      RAINBOW
#   Updation History:          Kelvin dengqiulin update for 8090(2004.08.18)
#                              lmg update for R3(2006.11.7)
#                              fsr update for R5 (2008.1.18)
#                              qj update for R6 (2008.08.08)
#   COPYRIGHT:                 2003---2008
#------------------------------------------------------------------------------------


#BEGIN FOR RESOURCE DEFINATION
[RESOURCE]
FORMAT: SPECS RESOURCE NAME STRING = CONTROLLABLE(1 : ABLE , 0: NOT ABLE),DEFAUL
T VALUE , MAX VALUE , MIN VALUE
#BEGIN  SPECS RESOURCE FOR TE tunnel Nto1 PS MODULE
PAF_LCS_TUNNEL_SPECS_TE_PS_MAX_PROTECT_NUM = 1, 8, 16, 1
PAF_LCS_TUNNEL_SPECS_TE_PS_REBOOT_TIME     = 1, 180000, 3600000, 60000
  ---- More ----
```

2.7.54 move

Function

The **move** command moves the source file from a specified directory to a destination directory.

Format

move *source-filename destination-filename*

Parameters

Parameter	Description	Settings
source-filename	Specifies the directory and name of a source file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Settings
destination-filename	Specifies the directory and name of a destination file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**. If **file prompt** is set to **quiet**, no prompt is displayed.
- The **move** and **copy** commands have different effects:
  - The **move** command moves the source file to the destination directory.
  - The **copy** command copies the source file to the destination directory.

Example

Move a file from **flash:/test/sample.txt** to **flash:/sample.txt**.

```
<HUAWEI> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]: y
%Moved file flash:/test/sample.txt to flash:/sample.txt.
```

2.7.55 mput

Function

The **mput** command uploads multiple files from the local device to the remote FTP server.

Format

mput *local-filenames*

Parameters

Parameter	Description	Value
local-filenames	Specifies files to be uploaded. File names are separated using spaces, and the wildcard (*) is supported.	The value is a string of 1 to 255 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **mput** command to upload multiple files to the remote FTP server at the same time, especially in the upgrade scenario.

Precautions

If the name of the uploaded file is the same as that of an existing file on the FTP server, the system overwrites the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Upload two local files **111.text** and **vrp222.cfg** to the remote FTP server.

```
<HUAWEI> ftp 10.10.10.1
Trying 10.10.10.1 ...
Press CTRL+K to abort
Connected to 10.10.10.1.
220 FTP service ready.
User(10.10.10.1:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] mput 111.txt vrp222.cfg
200 Port command successful.
150 Opening ASCII mode data connection for file transfer.
226 Transfer complete.
FTP: 6556 byte(s) sent in 0.231 second(s) 28.38Kbyte(s)/sec.

200 Port command successful.
150 Opening ASCII mode data connection for file transfer.
226 Transfer complete.
FTP: 4198 byte(s) sent in 0.171 second(s) 24.54Kbyte(s)/sec.

[ftp]
```

2.7.56 open

Function

The **open** command connects the FTP client and server.

Format

Connect the FTP client to the FTP server based on the IPv4 address.

open [**ssl-policy** *policy-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]

Connect the FTP client to the FTP server based on the IPv6 address.

open [**ssl-policy** *policy-name*] **ipv6** *host-ipv6* [*port-number*]

If the connection address is the IPv6 link-local address generated automatically by the interface of the remote IPv6 FTP server, the command format is as follows:

open [**ssl-policy** *policy-name*] **ipv6** *ipv6-linklocal-address* **-oi** *interface-type interface-number* [*port-number*]

Parameters

Parameter	Description	Value
ssl-policy *policy-name*	Specifies the name of the SSL policy that provides the secure FTP function.	The value is a string of 1 to 23 case-insensitive characters without spaces.
-a *source-ip-address*	Specifies the source IP address for connecting to the FTP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
port-number	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. The default value is the standard port number 21.

Parameter	Description	Value
public-net	Specifies the FTP server on the public network. You must set the **public-net** parameter when the FTP server IP address is a public network IP address.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the FTP server is located.	The value must be an existing VPN instance name.
host-ipv6	Specifies the IP address or host name of the remote IPv6 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-linklocal-address	Specifies the IPv6 link-local address generated automatically by the interface of the remote IPv6 FTP server.	-
-oi	Indicates the outbound interface of the IPv6 link-local address.	-
interface-typeinterface-number	Specifies the outbound interface type and number of the IPv6 link-local address.	-

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **open** command in the FTP client view to connect the FTP client to the server to transmit files and manage files and directories of the FTP server.

Precautions

- You can run the **ftp** command in the user view to connect the FTP client and server and enter the FTP client view.
- Before enabling the FTP or FTPS function and specifying the **ssl-policy** *policy-name* parameter, you must first configure an SSL policy.
- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified on the IPv4 network. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If the port number that the FTP server uses is non-standard, you must specify a standard port number; otherwise, the FTP server and client cannot be connected.
- When you run the **open** command, the system prompts you to enter the user name and password for logging in to the FTP server. You can log in to the FTP client and enter the FTP client view if the user name and password are correct.

Example

Connect the FTP client with the FTP server whose IP address is 10.137.217.204.

```
<HUAWEI> ftp
[ftp] open 10.137.217.204
Trying 10.137.217.204 ...
Press CTRL+K to abort
Connected to 10.137.217.204.
220 FTP service ready.
User(10.137.217.204:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

Connect the FTP client with the FTP server whose IP address is fc00:2001:db8::1.

```
<HUAWEI> ftp
[ftp] open ipv6 fc00:2001:db8::1
Trying fc00:2001:db8::1 ...
Press CTRL+K to abort
Connected to fc00:2001:db8::1
220 FTP service ready.
User(fc00:2001:db8::1:(none)):huawei
331 Password required for huawei
Enter Password:
230 User logged in.

[ftp]
```

2.7.57 passive

Function

The **passive** command sets the data transmission mode to passive.

The **undo passive** command sets the data transmission mode to active.

By default, the data transmission mode is active.

Format

passive

undo passive

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

The device supports the active and passive data transmission modes. In active mode, the server initiates a connection request, and the client and server need to enable and monitor a port to establish a connection. In passive mode, the client initiates a connection request, and only the server needs to monitor the corresponding port. This command is used together with the firewall function. When the client is configured with the firewall function, FTP connections are restricted between internal clients and external FTP servers if the FTP transmission mode is active. If the FTP transmission mode is passive, FTP connections between internal clients and external FTP servers are not restricted.

Example

Set the data transmission mode to passive.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] passive
Info: Succeeded in switching passive on.
```

2.7.58 prompt

Function

The **prompt** command enables the prompt function when files are transmitted between the FTP client and server.

The **undo prompt** command disables the prompt function.

By default, the prompt function is disabled.

Format

prompt

undo prompt

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can enable the prompt function as required when transmitting files between the FTP client and server.

Precautions

- The **prompt** command can be used when you run the **put**, **mput**, **get**, and **mget** commands.
- The prompt function can be enabled only for confirming service upload and download.
  - When you run the **put** or **mput** command, the system always overwrites the existing file if the name of the uploaded file is the same as that of an existing file on the FTP server.
  - When you run the **get** or **mget** command, the system always prompts you whether to overwrite the existing file if the name of the uploaded file is the same as an existing file name in the specified directory.

Example

Enable the FTP message prompt function.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
```

```
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] prompt
Info: Succeeded in switching prompt on.
```

Disable the FTP message prompt function.

```
[ftp] undo prompt
Info: Succeeded in switching prompt off.
```

2.7.59 put (FTP client view)

Function

The **put** command uploads a local file to the remote FTP server.

Format

put *local-filename* [*remote-filename*]

Parameters

Parameter	Description	Value
local-filename	Specifies the local file name of the FTP client.	The value is a string of 1 to 64 case-insensitive characters without spaces.
remote-filename	Specifies the name of the file to be uploaded to the remote FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **put** command to upload a local file to the remote FTP server for further check and backup. For example, you can upload the local log file to the FTP server for other users to check, and upload the configuration file to the FTP server as a backup before upgrading the device.

Precautions

- If the file name is not specified on the remote FTP server, the local file name is used.
- If the name of the uploaded file is the same as that of an existing file on the FTP server, the system overwrites the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Upload the configuration file **vrpcfg.zip** to the remote FTP server as a backup, and save it as **backup.zip**.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] put vrpcfg.zip backup.zip
200 Port command successful.
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
FTP: 1098 byte(s) sent in 0.131 second(s) 8.38Kbyte(s)/sec.
```

2.7.60 put (SFTP client view)

Function

The **put** command uploads a local file to a remote SFTP server.

Format

put *local-filename* [*remote-filename*]

Parameters

Parameter	Description	Value
local-filename	Specifies a local file name on the SFTP client.	The value is a case-insensitive character string without spaces. The file name (including the absolute path) contains 1 to 64 characters.
remote-filename	Specifies the name of the file uploaded to the remote SFTP server.	The value is a case-insensitive character string without spaces. The file name (including the absolute path) contains 1 to 64 characters.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command enables you to upload files from the local device to a remote SFTP server to view the file contents or back up the files. For example, you can upload log files of a device to an SFTP server and view the logs in the server. During an upgrade, you can upload the configuration file of the device to the SFTP server for backup.

Precautions

- If *remote-filename* is not specified, the uploaded file is saved on the remote SFTP server with the original file name.
- If the specified *remote-filename* is the same as an existing file name on the SFTP server, the uploaded file overwrites the existing file on the server.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Upload a file to the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> put wm.cfg
local file: wm.cfg --->  Remote file: /wm.cfg
Info: Uploading file successfully ended.
```

2.7.61 pwd (FTP client view)

Function

The **pwd** command displays the FTP client's working directory on the remote FTP server.

Format

pwd

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

After logging in to the FTP server, you can run the **pwd** command to display the FTP client's working directory on the remote FTP server.

If the displayed working directory is incorrect, you can run the **cd** command to change the FTP client's working directory on the remote FTP server.

Example

Display the FTP client's working directory on the remote FTP server.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] pwd
257 "/" is current directory.
```

2.7.62 pwd (SFTP client view)

Function

The **pwd** command displays the SFTP client's working directory on the remote FTP server.

Format

pwd

Parameters

None

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

After logging in to the SFTP server, you can run the **pwd** command to display the SFTP client's working directory on the remote SFTP server.

If the displayed working directory is incorrect, you can run the **cd** command to change the SFTP client's working directory on the remote SFTP server.

Example

Display the SFTP client's working directory on the remote SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> pwd
/
sftp-client> cd test
Current directory is:
/test
sftp-client> pwd
/test
```

2.7.63 pwd (user view)

Function

The **pwd** command displays the current working directory.

Format

pwd

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **pwd** command in any directory to display the current working directory. To change the current working directory, you can run the **cd** command.

Example

Display the current working directory.

```
<HUAWEI> pwd
flash:/test
```

2.7.64 remotehelp

Function

The **remotehelp** command displays the help information about an FTP command when the FTP client and server are connected.

Format

remotehelp [*command*]

Parameters

Parameter	Description	Value
command	Specifies the FTP command.	The value is a string of 1 to 16 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **remotehelp** command to display help information about an FTP command.

- The help information is provided by the remote server. Different remote servers may provide different help information for an FTP command.
- The help information can be displayed for FTP commands **user**, **pass**, **cwd**, **cdup**, **quit**, **port**, **pasv**, **type**, **retr**, **stor**, **dele**, **rmd**, **mkd**, **pwd**, **list**, **nlst**, **syst**, **help**, **xcup**, **xcwd**, **xmkd**, **xpwd**, **xrmd**, **eprt**, **epsv**, and **feat**.

Example

Display the syntax of the **cdup** command.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] remotehelp
```

```
214-The following commands are recognized (Commands marked with '*' are unimplem ented).    USER
PASS   ACCT*  CWD    CDUP   SMNT*  QUIT   REIN*    PORT   PASV   TYPE   STRU*  MODE*  RETR   STOR
STOU*    APPE   ALLO    REST*  RNFR*  RNTO*  ABOR*  DELE   RMD    MKD    PWD    LIST   NLST   SITE*
SYST   STAT*  HELP    NOOP*  XCUP   XCWD   XMKD   XPWD   XRMD   EPRT   EPSV    FEAT 214 Direct
comments to Huawei Tech.

[ftp] remotehelp cdup
214 Syntax: CDUP <change to parent directory>.
```

2.7.65 remove (SFTP client view)

Function

The **remove** command deletes specified files from the remote SFTP server.

Format

remove *remote-filename* &<1-10>

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be deleted from the remote SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can configure a maximum of 10 file names in the command and separate them using spaces and delete them at one time.
- If the file to be deleted is not in the current directory, you must specify the file path.

Example

Delete the file **3.txt** from the server and **backup1.txt** from the **test** directory.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> remove 3.txt test/backup1.txt
Warning: Make sure to remove these files? [Y/N]:y
Info: Succeeded in removing the file /3.txt.
Info: Succeeded in removing the file /test/backup1.txt.
```

2.7.66 rename (SFTP client view)

Function

The **rename** command renames a file or directory stored on the SFTP server.

Format

rename *old-name new-name*

Parameters

Parameter	Description	Value
old-name	Specifies the name of a file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.
new-name	Specifies the new name of the file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **rename** command to rename a file or directory.

Example

Rename the directory **yourtest** on the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> rename test/yourtest test/test
Warning: Rename /test/yourtest to /test/test? [Y/N]:y
Info: Succeeded in renaming file.
sftp-client> cd test
Current directory is:
/test
sftp-client> dir
drwxrwxrwx   1 noone    nogroup         0 Mar 29 2012 .
drwxrwxrwx   1 noone    nogroup         0 Mar 29 2012 ..
drwxrwxrwx   1 noone    nogroup         0 Mar 24 2012 test
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 2012 backup.txt
```

2.7.67 rename (user view)

Function

The **rename** command renames a file or folder.

Format

rename *old-name new-name*

Parameters

Parameter	Description	Settings
old-name	Specifies the name of a file or folder.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] filename** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Settings
new-name	Specifies the new name of the file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] filename** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name:

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.

- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- You must rename a file or directory in its source directory.
- If the renamed file or directory has the same name as an existing file or directory, an error message is displayed.
- If you specify *old-name* or *new-name* without specifying the file path, the file must be saved in your current working directory.

Example

Rename the directory **mytest** to **yourtest** in the directory **flash:/test/**.

```
<HUAWEI> pwd
flash:/test
<HUAWEI> rename mytest yourtest
Rename flash:/test/mytest to flash:/test/yourtest ?[Y/N]:y
Info: Rename file flash:/test/mytest to flash:/test/yourtest ......Done.
```

Rename the file **sample.txt** to **sample.bak**.

```
<HUAWEI> rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak ?[Y/N] :y
Info: Rename file flash:/sample.txt to flash:/sample.bak .......Done.
```

2.7.68 reset recycle-bin

Function

The **reset recycle-bin** command permanently deletes files from the recycle bin.

Format

reset recycle-bin [*filename* | *devicename*]

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' " The wildcard (*) character is supported.
devicename	Specifies the storage device name.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you run the **delete** command without specifying the **/unreserved** parameter, the file is moved to the recycle bin and still occupies the memory. To free up the space, you can run the **reset recycle-bin** command to permanently delete the file from the recycle bin.

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- You can run the **dir /all** command to display all files that are moved to the recycle bin from the current directory, and file names are displayed in square brackets ([ ]).
- If you delete a specified storage device, all files in the root directory of the storage device are deleted.
- If you run the **reset recycle-bin** command directly, all files that are moved to the recycle bin from the current directory are permanently deleted.

Example

Delete the file **test.txt** that is moved to the recycle bin from the directory **test**.

```
<HUAWEI> reset recycle-bin flash:/test/test.txt
Squeeze flash:/test/test.txt?[Y/N]:y
%Cleared file flash:/test/test.txt.
```

Delete files that are moved to the recycle bin from the current directory.

```
<HUAWEI> pwd
flash:/test
<HUAWEI> reset recycle-bin
Squeeze flash:/test/backup.zip?[Y/N]:y
%Cleared file flash:/test/backup.zip.
Squeeze flash:/test/backup1.zip?[Y/N]:y
%Cleared file flash:/test/backup1.zip.
```

2.7.69 rmdir (FTP client view)

Function

The **rmdir** command deletes a specified directory from the remote FTP server.

Format

rmdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies a directory or path on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **rmdir** command to delete a specified directory from the remote FTP server.

Precautions

- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- If no path is specified when you delete a subdirectory, the subdirectory is deleted from the current directory.
- The directory is deleted from the FTP server rather than the FTP client.

Example

Delete the directory **d:/temp1** from the remote FTP server.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] ascii
200 Type set to A.
[ftp] rmdir d:/temp1
250 'D:\temp1': directory removed.
```

2.7.70 rmdir (user view)

Function

The **rmdir** command deletes a specified directory from the storage device.

Format

rmdir *directory*

Parameters

Parameter	Description	Value
directory	Specifies a directory or directory and its path.	The value is a string of case-insensitive characters in the **[drive] [path] directory** format. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- A deleted directory and its files cannot be restored from the recycle bin.

Example

Delete the directory **test** from the current directory.

```
<HUAWEI> rmdir test
Remove directory flash:/test?[Y/N]:y
%Removing directory flash:/test...Done!%Removing directory flash:/test....Done!
```

2.7.71 rmdir (SFTP client view)

Function

The **rmdir** command deletes a specified directory from the remote SFTP server.

Format

rmdir *remote-directory* &<1-10>

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a file on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can configure a maximum of 10 file names in the command and separate them using spaces and delete them at one time.
- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- If the directory to be deleted is not in the current directory, you must specify the file path.

Example

Delete the directory **1** from the current directory, and the directory **2** from the **test** directory.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
```

```
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> rmdir 1 test/2
Warning: Make sure to remove these directories? [Y/N]:y
Info: Succeeded in removing the directory /test/1.
Info: Succeeded in removing the directory /test/test/2.
```

2.7.72 scp

Function

The **scp** command uploads a local file to the remote SCP server or downloads a file from the remote SCP server to a local directory.

Format

Transfer a file between the local client and the remote SCP server based on IPv4.

scp [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | { **-a** *source-address* | **-i** *interface-type interface-number* } | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile*

Transfer a file between the local client and the remote SCP server based on IPv6.

scp ipv6 [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-a** *source-address* | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile* [**-oi** *interface-type interface-number*]

Parameters

Parameter	Description	Value
-port *port-number*	Specifies the port number of the SCP server.	The value is an integer that ranges from 1 to 65535. The default value is 22.
public-net	Indicates that the SCP server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the SCP server is located.	The value must be an existing VPN instance name.

Parameter	Description	Value
identity-key	Specifies the public key algorithm for server authentication.	Public key algorithms include DSA, RSA, RSA_SHA2_256, RSA_SHA2_512 and ECC. By default, ECC is used for server authentication. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
user-identity-key	Specifies the public key algorithm for client authentication.	Public key algorithms include DSA, RSA, and ECC. By default, RSA is used for client authentication. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
-a *source-address*	Specifies the source IP address for connecting to the SCP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface used by the SCP client to set up connections. It consists of the interface type and number. It is recommended that you specify a loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SCP connection cannot be set up.	-

Parameter	Description	Value
-oi *interface-type interface-number*	Specifies an outbound interface on the local device. If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.	-
-r	Uploads or downloads files in batches.	-
-cipher *-cipher*	Specifies the encryption algorithms for uploading or downloading files.	Encryption algorithms **des**, **3des**, **aes256**, **aes128_ctr**, **aes256_ctr**, and **aes128** are supported. The default encryption algorithm is **aes256_ctr**. You are advised to use aes128_ctr and aes256_ctr encryption algorithms to ensure high security. **NOTE** ● If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. ● If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
-c	Compress files when uploading or downloading them.	-
sourcefile	Specifies a source file to be uploaded or downloaded.	The source file format is *username*@*hostname*:[*path*][*filename*].

Parameter	Description	Value
destinationfile	Specifies a destination file to be uploaded or downloaded.	The destination file format is *username*@*hostname*:[*path*][*filename*].

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SCP is an SSH2.0-based secure file transfer protocol. Compared with the SFTP file transfer mode, the SCP file transfer mode allows you to upload or download files when the connection is set up between the SCP client and server.

- You are advised to set the source IP address to the loopback address, or set the outbound interface to the loopback interface using **-a** and **-i**, to improve security.
- When **-r** is specified, you can use the wildcard (*) to upload or download files in batches, for example, *.txt and huawei.*.
- When **-c** is specified, files are compressed before being transmitted. File compression takes a long time and affects file transfer speed; therefore, you are not advised to compress files before transferring them.

Precautions

- The format of uploaded and downloaded files of the SCP server is *username*@*hostname*:[*path*][*filename*]. In the preceding file format, *username* indicates the user name for logging in to the SCP server, *hostname* indicates the SCP server name or IP address, and *path* indicates user's working directory specified on the SCP server, and *filename* indicates the file name. The following describes the preceding parameters when you upload a file to the SCP server:
  - If *filename* and *path* are not specified, the file is transferred to the root directory of the user's working directory.
  - If only *path* is specified, the file is transferred to the specified directory.
  - If only *filename* is specified, the file is named as *filename*, and transferred to the SCP server.
  - To set *hostname* to the IPv6 address, you must add the IPv6 address with square brackets ([ ]), for example, zhangsan@[FC00::/7]:.
- If the destination file name is the same as the name of an existing directory, the file is moved to this directory with the source file name. If the destination

file has the same name as an existing file, the system prompts you whether to overwrite the existing file.

- If an SCP user on the client authenticates the server using an RSA, a DSA, or an ECC public key, the SCP user is prompted to select the key pair for authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Log in through ECC authentication and copy the **xxxx.txt** file to the flash memory of remote SCP server at 10.10.0.114.

```
<HUAWEI> system-view
[HUAWEI] scp identity-key ecc flash:/xxxx.txt root@10.10.0.114:flash:/xxxx.txt
Trying 10.10.0.114 ...
Press CTRL+K to abort
Connected to 10.10.0.114 ...
The server's public key does not match the one catched before.
The server is not authenticated. Continue to access it? [Y/N]:y
Update the server's public key now? [Y/N]: y

Enter password:
flash:/xxxx.txt              100%          12Bytes           1KByte(s)/sec
```

2.7.73 scp client-source

Function

The **scp client-source** command specifies the source IP address for the SCP client to send packets.

The **undo scp client-source** command cancels the source IP address for the SCP client to send packets.

By default, no source IP address is configured on the SCP client.

Format

scp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo scp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address of the SCP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SCP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

The source interface specified using the command must exist and have an IP address configured.

Precautions

The **scp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **scp client-source** command. If you specify source addresses in the **scp client-source** and **scp** commands, the source IP address specified in the **scp** command is used for data communication. The source address specified in the **scp client-source** command applies to all SCP connections. The source address specified in the **scp** command applies only to the current SCP connection.

Example

Set the source IP address of the SCP client to the loopback interface IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] scp client-source -a 10.1.1.1
```

2.7.74 scp server enable

Function

The **scp server enable** command enables the SCP service on the SSH server.

The **undo scp server enable** command disables the SCP service on the SSH server.

By default, the SCP function is disabled.

Format

scp [**ipv4** | **ipv6**] **server enable**

undo scp [**ipv4** | **ipv6**] **server enable**

Parameters

Parameter	Description	Value
ipv4	Indicates that the SCP IPv4 service is enabled on the SSH server.	-
ipv6	Indicates that the SCP IPv6 service is enabled on the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To use SCP for file transfer, you need to first enable the SCP service on the SSH server. The client can establish an SCP connection with the SSH server only after SCP service has been enabled on the SSH server.

Prerequisites

Before enabling the SCP service, run either of the following commands as required:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server or run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.

- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the SSH server or run the **ssh ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the SSH server.

Precautions

After the **scp server enable** command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the number of IPv4 port or IPv6 port separately, run the **scp** [**ipv4** | **ipv6**] **server enable** command.

Example

Enable the SCP service.

```
<HUAWEI> system-view
[HUAWEI] scp server enable
```

Enable the SCP IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] scp ipv4 server enable
```

2.7.75 set cipher-suite

Function

The **set cipher-suite** command configures cipher suites for a customized SSL cipher suite policy.

The **undo set cipher-suite** command deletes cipher suites in a customized SSL cipher suite policy.

By default, no cipher suite is configured for a customized SSL cipher suite policy.

Format

set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }

undo set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }

Parameters

Parameter	Description	Value
tls12_ck_dss_aes_128_gcm_sha256	Configures the TLS12_CK_DSS_AES_128_GCM_SHA256 cipher suite.	-

Parameter	Description	Value
tls12_ck_dss_aes_256_gcm_sha384	Configures the TLS12_CK_DSS_AES_256_GCM_SHA384 cipher suite.	-
tls12_ck_rsa_aes_128_gcm_sha256	Configures the TLS12_CK_RSA_AES_128_GCM_SHA256 cipher suite.	-
tls12_ck_rsa_aes_256_gcm_sha384	Configures the TLS12_CK_RSA_AES_256_GCM_SHA384 cipher suite.	-

Views

Customized SSL cipher suite policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure cipher suites for a customized SSL cipher suite policy, run the **set cipher-suite** command.

Precautions

- If a customized SSL cipher suite policy is being referenced by an SSL policy, the cipher suites in the customized cipher suite policy can be added, modified, or partially deleted. Deleting all of the cipher suites is not allowed.
- The system software does not support the **tls12_ck_rsa_aes_256_cbc_sha256**, **tls1_ck_dhe_dss_with_aes_128_sha**, **tls1_ck_dhe_dss_with_aes_256_sha**, **tls1_ck_dhe_rsa_with_aes_128_sha**, **tls1_ck_dhe_rsa_with_aes_256_sha**, **tls1_ck_rsa_with_aes_128_sha**, and **tls1_ck_rsa_with_aes_256_sha** parameters. To use the **tls12_ck_rsa_aes_256_cbc_sha256**, **tls1_ck_dhe_dss_with_aes_128_sha**, **tls1_ck_dhe_dss_with_aes_256_sha**, **tls1_ck_dhe_rsa_with_aes_128_sha**, **tls1_ck_dhe_rsa_with_aes_256_sha**, **tls1_ck_rsa_with_aes_128_sha**, or **tls1_ck_rsa_with_aes_256_sha** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to use other parameters. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the **tls12_ck_dss_aes_128_gcm_sha256** cipher suite for the customized SSL cipher suite policy named **cipher1**.

```
<HUAWEI> system-view
[HUAWEI] ssl cipher-suite-list cipher1
[HUAWEI-ssl-cipher-suite-cipher1] set cipher-suite tls12_ck_dss_aes_128_gcm_sha256
```

2.7.76 set default ftp-directory

Function

The **set default ftp-directory** command configures the default FTP working directory.

The **undo set default ftp-directory** command disables the default FTP working directory.

By default, no default FTP working directory is configured.

Format

set default ftp-directory *directory*

undo set default ftp-directory

Parameters

Parameter	Description	Value
directory	Specify the default FTP working directory.	The value is a string of 1 to 160 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **set default ftp-directory** command to configure a default FTP working directory for all FTP users at one time.

Precautions

- The **set default ftp-directory** command takes effect only when the device functions as an FTP server and the user function as an FTP client.
- You can run the **local-user ftp-directory** command to configure an authorized working directory for a local user.
- If you have configured the FTP working directory by running the **local-user ftp-directory** command, you must use this FTP working directory.
- You can run the **lcd** command to view the working directory of FTP users.

- If no FTP working directory is specified on the device, FTP users cannot log in to the device, and are prompted that the working directory is unauthorized.

Example

Set the default FTP working directory to **flash:/**.

```
<HUAWEI> system-view
[HUAWEI] set default ftp-directory flash:/
```

2.7.77 set device auto-delete-file disable

Function

The **set device auto-delete-file disable** command disables the automatic file deletion function.

The **undo set device auto-delete-file disable** command enables the automatic file deletion function.

By default, the device is enabled to automatically delete files.

Format

set device auto-delete-file disable

undo set device auto-delete-file disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device periodically checks the storage space. When the space usage exceeds 85%, the device automatically releases the space using the following methods in sequence: empty the recycle bin, delete the system software package, delete patches, and delete logs. If you need to manually delete the files, run this command to disable the automatic file deletion function.

If no command output is displayed, run the **display current-configuration** command to check the parameters that have taken effect on the device and determine whether the automatic file deletion function is enabled.

Example

Disable the automatic file deletion function.

```
<HUAWEI> system-view
[HUAWEI] set device auto-delete-file disable
```

2.7.78 set net-manager vpn-instance

Function

The **set net-manager vpn-instance** command configures the default VPN instance that the NMS uses on the device.

The **undo set net-manager vpn-instance** command deletes the default VPN instance from the device.

By default, no VPN instance is configured on the device.

Format

set net-manager vpn-instance *vpn-instance-name*

undo set net-manager vpn-instance

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the default VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS manages devices on the VPN network, you need to send the device information to the NMS using the VPN instance.

You can run the **set net-manager vpn-instance** command to configure the default VPN instance for the NMS to manage the device so that the device can use this VPN instance to communicate with the NMS.

Precautions

- Before running the **set net-manager vpn-instance** command, you must create VPN instances.
- After running this command, you can successfully run file transfer commands that you have configured based on the FTP, TFTP, SCP, and SFTP commands only in the default VPN instance.
- If the host has been configured as a log host, the NMS can receive device logs from the default VPN instance.
- After you configure a VPN instance using the **set net-manager vpn-instance** command, the FTP, SFTP, SCP, and TFTP clients as well as the Information Center (IC), SNMP, and TACACS modules will use this instance by default.

  If the preceding clients or modules need to use a public network server or a specified VPN server, run the following commands to set parameters. If **public-net** is specified, the device accesses the server on the public network. If **vpn-instance***vpn-instance-name* is specified, the device accesses the server in the specified VPN instance.
  - FTP client: **ftp**
  - SFTP client: **sftp**
  - SCP client: **scp**
  - TFTP client: **tftp**
  - IC module: **info-center loghost**
  - SNMP module: **snmp-agent target-host trap**
  - TACACS module: **hwtacacs-server accounting**, **hwtacacs-server authentication**, **hwtacacs-server authorization**

Example

Set the default VPN instance to v1.

```
<HUAWEI> system-view
[HUAWEI] set net-manager vpn-instance v1
```

2.7.79 sftp

Function

The **sftp** command connects the device to the SSH server so that you can manage files that are stored on the SFTP server.

Format

Connect the SFTP client to the SFTP server based on IPv4.

sftp [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac*| **-ki** *aliveinterval*] | [**-kc** *alivecountmax*] *

Connect the SFTP client to the SFTP server based on IPv6.

sftp ipv6 [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] *

Parameters

Parameter	Description	Value
-a *source-address*	Specifies the source IP address for connecting to the SFTP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SFTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
host-ipv6	Specifies the IPv6 address or host name of the remote IPv6 SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
-oi *interface-type interface-number*	Specifies an outbound interface on the local device. If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.	-
port	Specifies the port number of the SSH server.	The value is an integer that ranges from 1 to 65535. The default port number is 22.
public-net	Specifies the SFTP server on the public network. You must set the **public-net** parameter when the SFTP server IP address is a public network IP address.	-
-vpn-instance *vpn-instance-name*	Name of the VPN instance where the SFTP server is located.	The value must be an existing VPN instance name.
prefer_kex *prefer_key-exchange*	Indicates the preferred key exchange algorithm.	The **dh_exchange_group**, **dh_exchange_group_sha256**, **dh_group14_sha1**, **dh_group14_sha256**, **dh_group15_sha512**, and **dh_group16_sha512** algorithms are supported currently. The default key exchange algorithm is dh_group14_sha1.

Parameter	Description	Value
prefer_ctos_cipher *prefer_ctos_cipher*	Specify an encryption algorithm for transmitting data from the client to the server.	Encryption algorithms 3des, aes128, aes128_ctr, aes256_ctr, and aes256 are supported. The default encryption algorithm is aes256_ctr. You are advised to use aes128_ctr and aes256_ctr encryption algorithms to ensure high security. **NOTE** ● If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. ● If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.

Parameter	Description	Value
prefer_stoc_cipher *prefer_stoc_cipher*	Specify an encryption algorithm for transmitting data from the server to the client	Encryption algorithms 3des, aes128, aes128_ctr, aes256_ctr, and aes256 are supported. The default encryption algorithm is aes256_ctr. You are advised to use aes128_ctr and aes256_ctr encryption algorithms to ensure high security. **NOTE** ● If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. ● If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
prefer_ctos_hmac *prefer_ctos_hmac*	Specify an HMAC algorithm for transmitting data from the client to the server.	HMAC algorithms sha1, sha1_96, md5, sha2_256, sha2_256_96, and md5_96 are supported. The default HMAC algorithm is sha2_256. **NOTE** To enhance security, you are not advised to use the md5 or md5_96 algorithm.
prefer_stoc_hmac *prefer_stoc_hmac*	Specify an HMAC algorithm for transmitting data from the server to the client.	HMAC algorithms sha1, sha1_96, md5, sha2_256, sha2_256_96, and md5_96 are supported. The default HMAC algorithm is sha2_256. **NOTE** To enhance security, you are not advised to use the md5 or md5_96 algorithm.

Parameter	Description	Value
-ki *aliveinterval*	Specifies the interval for sending keepalive packets when no packet is received in reply.	The value is an integer that ranges from 1 to 3600, in seconds.
-kc *alivecountmax*	Specifies the times for sending keepalive packets when no packet is received in reply.	The value is an integer that ranges from 3 to 10. The default value is 5.
identity-key	Specifies the public key for server authentication.	Public key algorithms include dsa, rsa, rsa_sha2_256, rsa_sha2_512 and ecc. By default, the server authentication uses the ECC public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
user-identity-key	Specifies the public key algorithm for the client authentication.	Public key algorithms include dsa, rsa, and ecc. By default, the client authentication uses the RSA public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SFTP is short for SSH FTP that is a secure FTP protocol. SFTP is on the basis of SSH. It ensures that users can log in to a remote device securely for file management and transmission, and enhances the security in data transmission. In addition, you can log in to a remote SSH server from the device that functions as an SFTP client.

When the connection between the SFTP server and client fails, the SFTP client must detect the fault in time and disconnect from the SFTP server. To ensure this, before being connected to the server in SFTP mode, the client must be configured with the interval and times for sending the keepalive packet when no packet is received in reply. If the client receives no packet in reply within the specified interval, the client sends the keepalive packet to the server again. If the maximum number of times that the client sends keepalive packets exceeds the specified value, the client releases the connection. By default, when no packet is received, the function for sending keepalive packets is not enabled.

Precautions

- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- The SSH client can log in to the SSH server with no port number specified only when the port number of the SSH server is 22. If the SSH server uses another port, the port number must be specified when SSH clients log in to the SSH server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If you cannot run the **sftp** command successfully when you configured the ACL on the SFTP client, or when the TCP connection fails, an error message is displayed indicating that the SFTP client cannot be connected to the server.

Example

Set keepalive parameters when the client is connected to the server in SFTP mode.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.164.39.223 -ki 10 -kc 4
Please input the username: client001
Trying 10.164.39.223 ...
Press CTRL+K to abort
Connected to 10.164.39.223 ...
Enter password:
sftp-client>
```

Connect the client to the server using the DSA authentication in SFTP mode.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.164.39.223 identity-key dsa
Please input the username:root
Trying 10.164.39.223 ...
Press CTRL+K to abort
Connected to 10.164.39.223 ...
Enter password:
```

```
sftp-client> quit
Bye
```

2.7.80 sftp client-source

Function

The **sftp client-source** command specifies the source IP address for the SFTP client to send packets.

The **undo sftp client-source** command restores the default source IP address for the SFTP client to send packets.

The default source IP address for the SFTP client to send packets is 0.0.0.0.

Format

sftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo sftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address. Set the value to the IP address of a loopback interface.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the loopback interface as the source interface. The IP address configured for the source interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

The loopback source interface specified using the command must exist and have an IP address configured.

Precautions

- The source interface must be set to the loopback interface. You can query the source IP address or primary IP address of the source interface for the SFTP connection on the SFTP server.
- The **sftp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **sftp client-source** command. If you specify source addresses in the **sftp client-source** and **sftp** commands, the source IP address specified in the **sftp** command is used for data communication. The source address specified in the **sftp client-source** command applies to all SFTP connections. The source address specified in the **sftp** command applies only to the current SFTP connection.

Example

Set the source IP address of the SFTP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] sftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the SFTP client to 10.1.1.1.
```

2.7.81 sftp client-transfile

Function

The **sftp client-transfile** command uploads files to or downloads files from the SFTP server.

Format

Establish an SFTP connection on an IPv4 network.

sftp client-transfile { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

Establish an SFTP connection on an IPv6 network.

sftp client-transfile { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** | **rsa_sha2_256** |

rsa_sha2_512 } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

Parameters

Parameter	Description	Value
get	Downloads files from the SFTP server.	-
put	Uploads files to the SFTP server.	-
-a *source-address*	Specifies the source address of an SFTP client.	-
-i *interface-type interface-number*	Specifies the source interface of an SFTP client.	-
host-ip *host-ipv4*	Specifies the IPv4 address or host name of an SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
port	Specifies the current monitoring port number on the SFTP server. Only when the monitoring port number on the SFTP server is 22, the SFTP client can log in without a port number being specified. If the monitoring port number on the SFTP server is not 22, you must specify a port number for the SFTP client to log in.	The value is an integer ranging from 1 to 65535. The default value is 22.
public-net	Establishes the SFTP connection on a public network.	-

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. The SFTP connection is established on a private network.	The value must be an existing VPN instance name.
prefer_kex *prefer_key-exchange*	Specifies a preferred algorithm for key exchange.	● dh_exchange_group ● dh_exchange_group_sha256 ● dh_group14_sha1 ● dh_group14_sha256 ● dh_group15_sha512 ● dh_group16_sha512 The default algorithm is dh_exchange_group. **NOTE** The **dh_exchange_group** algorithm is recommended.
identity-key	Specifies a public key algorithm for the server authentication.	● dsa ● rsa ● ecc ● rsa_sha2_256 ● rsa_sha2_512 The default algorithm is rsa. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Parameter	Description	Value
prefer_ctos_cipher *prefer_ctos_cipher*	Specifies the preferred encryption algorithm for packets from the client to the server	● 3des ● aes128 ● aes256 ● aes128_ctr(Advanced Encryption Standard 128_ctr) ● aes256_ctr(Advanced Encryption Standard 256_ctr) The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr, and aes256_ctr algorithms. **NOTE** ● If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. ● If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.

Parameter	Description	Value
prefer_stoc_cipher *prefer_stoc_cipher*	Specifies the preferred encryption algorithm for packets from the server to the client.	- 3des - aes128 - aes256 - aes128_ctr - aes256_ctr The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr, and aes256_ctr algorithms. **NOTE** - If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. - If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
prefer_ctos_hmac *prefer_ctos_hmac*	Specifies the preferred HMAC algorithm for packets from the client to the server.	- sha1 - sha1_96 - md5 - md5_96 - sha2_256 - sha2_256_96 The default algorithm is sha2_256.
prefer_stoc_hmac *prefer_stoc_hmac*	Specifies the preferred HMAC algorithm for packets from the server to the client.	- sha1 - sha1_96 - md5 - md5_96 - sha2_256 - sha2_256_96 The default algorithm is sha2_256.

Parameter	Description	Value
-ki *aliveinterval*	Specifies the interval at which the client sends a Keepalive packet to the server. When the connection between the server and the client fails, the client must detect the fault in time and removes the connection proactively. Therefore, when logging in to the server using SFTP, the client must be configured with an interval at which the client sends keepalive packets to the server and the maximum number of times that the server provides no response. If a client does not receive any packet within a specified period, the client sends a Keepalive packet to the server. If the maximum number of times that the server does not respond exceeds the specified value, the client proactively removes the connection. By default, the function of sending Keepalive packets to the server in the case of no data transmission is not configured.	The value is an integer ranging from 1 to 3600, in seconds. The default value is 60 seconds.
-kc *alivecountmax*	Specifies the maximum number of times that the server does not respond.	The value is an integer ranging from 3 to 10. The default value is 5.
username *user-name*	Specifies the user name for an SFTP connection.	The value is a string of 1 to 255 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
password *password*	Specifies the password for an SFTP connection.	The value is a string of 1 to 128 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
sourcefile *source-file*	Specifies the source file to be uploaded to or downloaded from the server.	The absolute path of the file ranges from 1 to 160 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
destination *destination*	Specifies the destination file to be uploaded to or downloaded from the server. If **destination** *destination* is not specified, the name of the file to be downloaded from or uploaded to the server is the same as that on the SFTP server.	The absolute path of the file ranges from 1 to 160 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
ipv6	Specifies an IPv6 SFTP server.	-
-oi *interface-type interface-number*	Specifies the source IPv6 interface of an SFTP client. If *host-ipv6* is a link-local IPv6 address, you must specify the interface name corresponding to the link-local address. If *host-ipv6* is not a link-local IPv6 address, no interface name is required.	-

Parameter	Description	Value
host-ip *host-ipv6*	Specifies the IPv6 address or host name of an SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To upload files to or download files from an SFTP server, run the **sftp client-transfile** command.

Prerequisites

The SFTP function on the SFTP server has been enabled using the **sftp client-transfile** command.

Configuration Impact

After a connection is established between an SFTP client and an SFTP server, they start to intercommunicate.

Precautions

If command execution fails due to ACLs on the SFTP client or the TCP connection fails, the system prompts an error message indicating that the connection to the server fails.

If the **sftp client-transfile** command is run for the device to connect to the SFTP server, only password authentication is supported.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Configure the current monitoring port number 1025 on the SSH server on a private network (SFTP client on the public network), and download the **sample.txt** file to the SFTP client.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile get host-ip 10.137.144.231 1025 -vpn-instance ssh username root
password YsHsjx_202206 sourcefile sample.txt
```

Specify Keepalive parameters for the client that attempts to log in to the server using SFTP and download the **sample.txt** file to the SFTP client.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile get host-ip 10.164.39.209 -ki 10 -kc 4 username root password
YsHsjx_202206 sourcefile sample.txt
```

Configure the client to pass DSA authentication before logging in to the server using SFTP and download the **sample.txt** file to the SFTP client.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile get host-ip 10.100.0.114 identity-key dsa username root password
YsHsjx_202206 sourcefile sample.txt
```

Upload the **sample.txt** file to the IPv6 SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile put host-ip 10.100.0.114 identity-key dsa username root password
YsHsjx_202206 sourcefile sample.txt
```

2.7.82 sftp server enable

Function

The **sftp server enable** command enables the SFTP service on the SSH server.

The **undo sftp server enable** command disables the SFTP service on the SSH server.

By default, the SFTP service is disabled.

Format

sftp [**ipv4** | **ipv6**] **server enable**

undo sftp [**ipv4** | **ipv6**] **server enable**

Parameters

Parameter	Description	Value
ipv4	Indicates that the SFTP IPv4 service is enabled on the SSH server.	-
ipv6	Indicates that the SFTP IPv6 service is enabled on the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To connect the client to the SSH server to transfer files in SFTP mode, you must first enable the SFTP server on the SSH server.

Prerequisites

Before enabling the SFTP service, run either of the following commands as required:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server or run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.
- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the SSH server or run the **ssh ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the SSH server.

Precautions

After the **sftp server enable** command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the number of IPv4 port or IPv6 port separately, run the **sftp** [**ipv4** | **ipv6**] **server enable** command.

Example

Enable the SFTP service.

```
<HUAWEI> system-view
[HUAWEI] sftp server enable
Info: Succeeded in starting the SFTP server.
```

Disable the SFTP service.

```
<HUAWEI> system-view
[HUAWEI] undo sftp server enable
Info: Succeeded in closing the SFTP server.
```

Enable the SFTP IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] sftp ipv4 server enable
```

2.7.83 ssh user sftp-directory

Function

The **ssh user sftp-directory** command configures the SFTP service authorized directory for an SSH user.

The **undo ssh user sftp-directory** command cancels the SFTP service authorized directory for an SSH user.

The default SFTP service authorized directory is flash: for an SSH user.

Format

ssh user *username* **sftp-directory** *directoryname*

undo ssh user *username* **sftp-directory**

Parameters

Parameter	Description	Value
username	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
directoryname	Specifies the directory name on the SFTP server.	The value is a string of 1 to 160 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If there is the default authorized directory for an SFTP user on the device, you can run this command to change the directory.

Precautions

Users can only access the specified directory on the SFTP server. If the *username* user does not exist, the system creates an SSH user named *username* and uses the SFTP service authorized directory configured for the user. If the configured directory does not exist, the SFTP client fails to connect to the SSH server using this SSH user. After a master/backup switchover or device restart is performed, the SFTP client fails to connect to the SSH server if the configured directory does not exist. In this case, check whether the configured directory is valid. If the configured directory is invalid, re-configure it.

Example

Configure the SFTP service authorized directory flash:/ssh for the SSH user **admin**.

```
<HUAWEI> system-view
[HUAWEI] ssh user admin sftp-directory flash:/ssh
```

2.7.84 ssl cipher-suite-list

Function

The **ssl cipher-suite-list** command customizes an SSL cipher suite policy and displays the view of the cipher suite policy. If the SSL cipher suite policy to be customized already exists, the command directly displays the view of this cipher suite policy.

The **undo ssl cipher-suite-list** command deletes a customized SSL cipher suite policy.

By default, no customized SSL cipher suite policy is configured.

Format

ssl cipher-suite-list *customization-policy-name*

undo ssl cipher-suite-list *customization-policy-name*

Parameters

Parameter	Description	Value
customization-policy-name	Sets a name for a customized SSL cipher suite policy.	The value is a string of 1 to 32 case-insensitive characters, spaces not supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve system security, the device supports only secure algorithms by default. However, to improve compatibility, the device also allows you to customize cipher suite policies. To customize a cipher suite policy, run the **ssl cipher-suite-list** command.

Example

Customize an SSL cipher suite policy named **cipher1** and enter the view of the cipher suite policy.

```
<HUAWEI> system-view
[HUAWEI] ssl cipher-suite-list cipher1
[HUAWEI-ssl-cipher-suite-cipher1]
```

2.7.85 ssl minimum version

Function

The **ssl minimum version** command configures a minimum SSL version for an SSL policy.

The **undo ssl minimum version** command restores the default version.

By default, the minimum SSL version used by an SSL policy is TLS1.2.

NOTE

When the minimum SSL version used for an SSL policy is set to TLS1.2, an SSL certificate is required, which is provided by a third-party authoritative certificate authority.

Format

ssl minimum version { **tls1.1** | **tls1.2** }

undo ssl minimum version

Parameters

Parameter	Description	Value
tls1.1	Sets the minimum SSL version to TLS1.1 for an SSL policy.	-
tls1.2	Sets the minimum SSL version to TLS1.2 for an SSL policy.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure a minimum SSL version for an SSL policy, run the **ssl minimum version** command so that service modules can flexibly adopt the SSL policy.

The SSL versions supported by SSL policies include TLS1.1, TLS1.2 in ascending order of security.

Precautions

The system software does not support the tls1.0 parameter. To use the tls1.0 parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the tls1.2 parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the minimum SSL version for the SSL policy **ftp_server** to be TLS1.2.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] ssl minimum version tls1.2
```

2.7.86 ssl policy

Function

The **ssl policy** command creates an SSL policy and displays the SSL policy view. If the SSL policy has been created before you run this command, the command directly displays the SSL policy view.

The **undo ssl policy** command deletes an SSL policy.

By default, no SSL policy is created.

Format

ssl policy *policy-name*

undo ssl policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Traditional FTP and HTTP protocols does not have the security mechanism. Data that is transmitted in plain text can be modified. User identity cannot be authenticated and data security cannot be ensured. The SSL security policy uses the data encryption, user identity authentication, and message integrity check mechanisms to ensure the security of the TCP-based application layer.

Follow-up Procedure

After you have run the **ssl policy** command to display the SSL policy view, perform either of the following operations:

- When the device functions as a server, run the **certificate load** to load the certificate or certificate chain.
- When the device functions as a client, run the **trusted-ca load** and **crl load** commands to load the trusted CA and CRL so that the server validity can be authenticated.

Precautions

- You can run the **ssl policy** command to create an SSL policy for the secure FTP and HTTP servers.
- A maximum of four SSL policies can be created.

Example

Create SSL policy **https_der** and display the SSL policy view.

```
<HUAWEI> system-view
[HUAWEI] ssl policy https_der
[HUAWEI-ssl-policy-https_der]
```

2.7.87 tftp

Function

The **tftp** command uploads a file to the TFTP server or downloads a file to the local device.

Format

Upload a file to the TFTP server or download a file to the local device based on the IPv4 address

tftp [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]

Upload a file to the TFTP server or download a file to the local device based on the IPv6 address

tftp ipv6 [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the TFTP client. You are advised to use the loopback interface IP address.	-

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface used by the TFTP client to set up connections. It consists of the interface type and number. It is recommended that you specify a loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the TFTP connection cannot be set up.	-
-oi *interface-type interface-number*	Specifies an outbound interface on the local device.	If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.
tftp-server	Specifies the IPv4 address or host name for the TFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
tftp-server-ipv6	Specifies the IPv6 address of the IPv6 TFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
public-net	Specifies the TFTP server on the public network.	-
vpn-instance *vpn-instance-name*	Name of the VPN instance where the TFTP server is located.	The value must be an existing VPN instance name.
get	Download a file.	-
put	Upload a file.	-
source-filename	Specifies the source file name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Parameter	Description	Value
destination-filename	Specifies the destination file name.	The value is a string of 1 to 64 case-insensitive characters without spaces. By default, source and destination file names are the same.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading the system, you can run the **tftp** command to upload an important file to the TFTP server or download a system software to the local device.

Precautions

- When you run the **tftp** command to upload a file to the TFTP server in TFTP mode, files are transferred in binary mode by default. The tftp does not support the ASCII mode for file transfer.
- After specifying a source IP address, you can use this IP address to communicate with the server and implement packet filtering to ensure data security.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download file **vrpcfg.txt** from the root directory of the TFTP server to the local device. The IP address of the TFTP server is 10.1.1.1. Save the downloaded file to the local device as file **vrpcfg.bak**.

```
<HUAWEI> tftp 10.1.1.1 get vrpcfg.txt flash:/vrpcfg.bak
```

Upload file **vrpcfg.txt** from the root directory of the storage device to the default directory of the TFTP server. The IP address of the TFTP server is 10.1.1.1. Save file **vrpcfg.txt** on the TFTP server as file **vrpcfg.bak**.

```
<HUAWEI> tftp 10.1.1.1 put flash:/vrpcfg.txt vrpcfg.bak
```

Obtain the link local IP address and interface name from the TFTP server.

```
<HUAWEI> tftp ipv6 FC00::/7 -oi gigabitethernet 0/0/1 get file1 file2
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
100%
TFTP: Downloading the file successfully.
249704 byte(s) received in 10 second(s).
```

2.7.88 tftp client-source

Function

The **tftp client-source** command specifies the source IP address for the TFTP client to send packets.

The **undo tftp client-source** command restores the default source IP address for the TFTP client to send packets.

By default, the TFTP client source address is the IP address of the outbound interface connecting to the TFTP server, and it is displayed as 0.0.0.0.

Format

tftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo tftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address of the TFTP client. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
-i *interface-type interface-number*	Source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the TFTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

The source interface specified using the command must exist and have an IP address configured.

Precautions

- The **tftp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **tftp client-source** command. If you specify source addresses in the **tftp client-source** and **tftp** commands, the source IP address specified in the **tftp** command is used for data communication. The source address specified in the **tftp client-source** command applies to all TFTP connections. The source address specified in the **tftp** command applies only to the current TFTP connection.
- You can query the source IP address or source interface IP address specified in the TFTP connection on the TFTP server.

Example

Set the source IP address of the TFTP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] tftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the TFTP client to 10.1.1.1.
```

2.7.89 tftp-server acl

Function

The **tftp-server acl** command specifies the ACL number for the local device so that the device can access TFTP servers with the same ACL number.

The **undo tftp-server acl** command deletes the ACL number from the local device.

By default, no ACL number is specified on the local client.

Format

tftp-server [**ipv6**] **acl** *acl-number*

undo tftp-server [**ipv6**] **acl**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
ipv6	Specifies the IPv6 address of a specific server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of the local device, you need to run the **tftp-server acl** command to specify an ACL to specify TFTP servers that the local device can access.

Precautions

- The **tftp-server acl** command takes effect only after you run the **rule** command to configure the ACL rule. If no ACL rule is configured, the local device can access a specified TFTP server in TFTP mode.
- The TFTP supports only the basic ACL whose number ranges from 2000 to 2999.

Example

Allow the local device to the access the TFTP server whose ACL number is 2000.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] tftp-server acl 2000
```

2.7.90 trusted-ca load

Function

The **trusted-ca load** command loads the trusted CA file for the SSL policy for the FTP client.

The **undo trusted-ca load** command unloads the trusted CA file of the SSL policy.

By default, no trusted CA file is loaded for the SSL policy.

Format

Load the trusted CA file for the SSL policy in ASN1 format.

trusted-ca load asn1-ca *ca-filename*

Load the trusted CA file for the SSL policy in PEM format.

trusted-ca load pem-ca *ca-filename*

Load the trusted CA file for the SSL policy in PFX format.

trusted-ca load pfx-ca *ca-filename* **auth-code cipher** *auth-code*

Unload the trusted CA file for the SSL policy.

undo trusted-ca load { **asn1-ca** | **pem-ca** | **pfx-ca** } *ca-filename*

Parameters

Parameter	Description	Value
asn1-ca	Load the trusted CA file for the SSL policy in ASN1 format.	-
pem-ca	Load the trusted CA file for the SSL policy in PEM format.	-
pfx-ca	Load the trusted CA file for the SSL policy in PFX format.	-

Parameter	Description	Value
ca-filename	Specifies the name of the trusted CA file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code cipher *auth-code*	Specifies the verification code for the trusted CA file in PFX format. The authentication code verifies user identity to ensure that only authorized users can log in to the server.	The value is a string of case-sensitive characters without spaces. If the value begins and ends with double quotation marks (" "), the string of characters can contain spaces. When the value is displayed in plaintext, its length ranges from 1 to 31. When the value is displayed in ciphertext, its length is 48 or 68. A ciphertext password with the length of 32 or 56 characters is also supported.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

CAs that are widely trusted in the world are called root CAs. Root CAs can authorize other lower-level CAs. The identity information about a CA is provided in the file of a trusted CA. To ensure the communication security and verify the server validity, you must run the **trusted-ca load** command to load the trusted CA file.

Prerequisites

Before running the **trusted-ca load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

A maximum of four trusted CA files can be loaded for an SSL policy. For the sake of security, deleting the installed trusted CA file is not recommended; otherwise, services using the SSL policy will be affected.

Example

Load the trusted CA file for the SSL policy in ASN1 format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load asn1-ca servercert.der
```

Load the trusted CA file for the SSL policy in PEM format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load pem-ca servercert.pem
```

Load the trusted CA file for the SSL policy in PFX format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load pfx-ca servercert.pfx auth-code cipher YsHsjx_202206
```

2.7.91 undelete

Function

The **undelete** command restores a file that has been temporally deleted from or moved to the recycle bin.

Format

undelete { *filename* | *devicename* }

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be restored.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
devicename	Specifies the storage device name.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **undelete** command to restore a file that has been temporally deleted and moved to the recycle bin. However, files that are permanently deleted by running the **delete** or **reset recycle-bin** command with the **/unreserved** parameter cannot be restored.

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- To display information about a temporally deleted file, run the **dir /all** command. The file name is displayed in square brackets ([ ]).
- If the name of a file is the same as an existing directory, the file cannot be restored. If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.

Example

Restore file **sample.bak** from the recycle bin.

```
<HUAWEI> undelete sample.bak
Undelete flash:/sample.bak ?[Y/N]:y
%Undeleted file flash:/sample.bak.
```

Restore a file that has been moved from the root directory to the recycle bin.

```
<HUAWEI> undelete flash:
Undelete flash:/test.txt?[Y/N]:y
%Undeleted file flash:/test.txt.
Undelete flash:/rr.bak?[Y/N]:y
%Undeleted file flash:/rr.bak.
```

2.7.92 unzip

Function

The **unzip** command decompresses a file.

Format

unzip *source-filename destination-filename*

Parameters

Parameter	Description	Value
source-filename	Specifies the name of a source file to be decompressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
destination-filename	Specifies the name of a destination file that is decompressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can decompress files, especially log files that are stored on the storage device and run the **more** command to query the file.

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file path is specified while the file name is not specified, the designation file name is the same as the source file name.
- The source file persists after being decompressed.
- The compressed file must be a .zip file. If a file to be decompressed is not a zip file, the system displays an error message during decompression.
- The source file must be a single file. If you attempt to decompress a directory or multiple files, the decompression cannot succeed.

Example

Decompress log file **logfile-2012-02-27-17-47-50.zip** that is stored in the **logfile** directory and save it to the root directory as file **log.txt**.

```
<HUAWEI> pwd
flash:/logfile
<HUAWEI> unzip logfile-2012-02-27-17-47-50.zip flash:/log.txt
Extract flash:/logfile/logfile-2012-02-27-17-47-50.zip to flash:/log.txt?[Y/N]:y
100%  complete
%Decompressed file flash:/logfile/logfile-2012-02-27-17-47-50.zip to flash
:/log.txt.
```

2.7.93 user

Function

The **user** command changes the current FTP user when the local device is connected to the FTP server.

Format

user *user-name* [*password*]

Parameters

Parameter	Description	Value
user-name	Specifies the name of a login user.	The value is a string of 1 to 255 case-insensitive characters without space.
password	Specifies the login password.	The value is a string of 1 to 255 case-sensitive characters without space, single quotation mark, or question mark.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device accesses the remote FTP server, to switch from the current user to another user, you only need to run the **user** command to log in to the FTP server by using another user name without disconnecting the FTP connection.

Precautions

After you run the **user** command to change the current user, a new FTP connection is set up, which is the same as that you specify using the **ftp** command.

Example

Log in to the FTP server using the user name **tom**.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] user tom
331 Password required for tom.
Enter password:
230 User logged in.
```

2.7.94 verbose

Function

The **verbose** command enables the verbose function on the FTP client.

The **undo verbose** command disables the verbose function.

By default, the verbose function is enabled.

Format

verbose

undo verbose

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

After the verbose function is enabled, all FTP responses are displayed on the FTP client, including FTP protocol information and details about the responses.

Example

Enable the verbose function.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] verbose
Info: Succeeded in switching verbose on.
[ftp] get h1.txt
200 Port command okay.
150 Opening ASCII mode data connection for h1.txt.

226 Transfer complete.
FTP: 69 byte(s) received in 0.160 second(s) 431.25byte(s)/sec.
```

Disable the verbose function.

```
[ftp] undo verbose
Info: Succeeded in switching verbose off.
[ftp] get h1.txt

FTP: 69 byte(s) received in 0.150 second(s) 460.00byte(s)/sec.
```

2.7.95 zip

Function

The **zip** command compresses a file.

Format

zip *source-filename destination-filename*

Parameters

Parameter	Description	Value
source-filename	Specifies the name of a source file to be compressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
destination-filename	Specifies the name of a destination file that is compressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.

  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file path is specified while the file name is not specified, the designation file name is the same as the source file name.
- The source file persists after being compressed.
- Directories cannot be compressed.

Example

Compress file **log.txt** that is stored in the root directory and save it to the **test** directory as file **log.zip**.

```
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            155  Dec 02 2011 01:28:48   log.txt
    1  -rw-          9,870  Oct 01 2011 00:22:46   patch.pat
    2  drw-              -  Mar 22 2012 00:00:48   test
    3  -rw-            836  Dec 22 2011 16:55:46   rr.dat
...

65,233 KB total (7,289 KB free)
<HUAWEI> zip log.txt flash:/test/log.zip
Compress flash:/log.txt to flash:/test/log.zip?[Y/N]:y
100%  complete
%Compressed file flash:/log.txt to flash:/test/log.zip.
<HUAWEI> cd test
<HUAWEI> dir
Directory of flash:/test/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            836  Mar 20 2012 19:49:14   test
    1  -rw-            239  Mar 22 2012 20:57:38   test.txt
    2  -rw-          1,056  Dec 02 2011 01:28:48   log.txt
    3  -rw-            240  Mar 22 2012 21:23:46   log.zip

65,233 KB total (7,288 KB free)
```

2.8 Configuring System Startup Commands

2.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.8.2 check file-integrity

Function

The **check file-integrity** command checks whether a file is consistent with the corresponding signature file.

Format

check file-integrity *filename signature-filename*

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be checked. The file must exist.	The value is a string of 4 to 64 case-insensitive characters without spaces. The file name extension can be .cc, .pat, .zip, .mod, or .7z.
signature-filename	Specifies the name of the signature file corresponding to the file to be checked. The signature file must exist.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name extension must be .asc or .p7s.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to check whether a file is consistent with the corresponding signature file. If the check fails, the file cannot be used as the system software, patch file, web page file, or mod file.

NOTE

Signature files are released with each version. Each valid system software, patch file, web page file, or mod file has a corresponding signature file. You need to upload the signature file to the switch before using this command.

Example

Check whether the system software is consistent with the corresponding signature file.

```
<HUAWEI> system-view
[HUAWEI] check file-integrity S5700-V200R023C00.cc S5700-V200R023C00.cc.asc
```

2.8.3 clear configuration interface

Function

Using the **clear configuration interface** command, you can perform one-touch configuration clearance on an interface.

Format

clear configuration interface { *interface-type-start interface-number-start* [**to** *interface-type-end interface-number-end*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type-start interface-number-start [**to** *interface-type-end interface-number-end*]	Indicates the type and number of the interface where one-touch configuration clearance is performed. • *interface-type-start* specifies the type of the first interface. • *interface-number-start* specifies the number of the first interface. • *interface-type-end* specifies the type of the last interface. • *interface-number-end* specifies the number of the last interface.	At present, the tunnel and stack-port interfaces are not supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure an interface on a device for other use, original configurations on the interface need to be deleted one by one. If the interface has a large number of configurations, deleting these configurations one-by-one takes a long time and increases the maintenance workload. To reduce the maintenance workload and simplify the deletion operation, you can use this command to perform one-touch configuration clearance on an interface.

You can also run the **clear configuration this** command in the system view to delete configurations on a specified interface.

NOTE

The one-touch configuration clearance function cannot delete the **combo-port** command on an interface.

Configuration Impact

After this command is run, all configurations on an interface will be cleared. The status of the interface is **shutdown**.

Precautions

The execution of this command takes a long time. To terminate the running command, press **Ctrl**+**C**.

In general, after the **clear configuration this** command is run on an interface to clear the configuration, the default configuration is restored. If special configurations exist on the interface on which the **clear configuration this** command is run, the configuration may be displayed in the **undo** command format.

Example

Perform one-touch configuration clearance on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 50
#
return
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] clear configuration interface gigabitethernet 0/0/1
Warning: All configurations of the interface will be cleared, and its state will
 be shutdown. Continue? [Y/N] :y...
Info: Total execute 2 command(s), 2 successful, 0 failed.
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 shutdown
#
return
```

2.8.4 clear configuration this

Function

The **clear configuration this** command deletes configurations on an interface at a time to restore the default configurations.

Format

clear configuration this

Parameters

None

Views

Interface view (excluding tunnel interface view, stack-port interface view, and port group view)

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure an interface on a device for other use, original configurations on the interface need to be deleted one by one. If the interface has a large number of configurations, deleting these configurations one-by-one takes a long time and increases the maintenance workload. To reduce the maintenance workload and simplify the deletion operation, you can use this command to perform one-touch configuration clearance on an interface.

You can also run the **clear configuration interface** *interface-type interface-num* command in the system view to delete configurations on a specified interface.

Configuration Impact

After you run the **clear configuration this** command, the system displays a message, asking you whether to delete the configurations on the specified interface. If you enter **Y**, all configurations on the specified interface are deleted and the interface status becomes shutdown.

Running the **clear configuration this** command on an interface is similar to running undo commands on the interface in batches.

Precautions

The execution of this command takes a long time. To terminate the running command, press **Ctrl**+**C**.

In general, after the **clear configuration this** command is run on an interface to clear the configuration, the default configuration is restored. If special configurations exist on the interface on which the **clear configuration this** command is run, the configuration may be displayed in the **undo** command format.

As some commands correlate to each other, if you run the **undo** command to delete the configurations of a command, the configurations of the correlated command are also deleted. After the **clear configuration this** command is run on an interface, the statistics in the command output may be inconsistent with actual clearance results. Refer to the actual clearance results in real-world applications.

Example

Perform one-touch configuration clearance on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 description abc
 port link-type access
#
return
[HUAWEI-GigabitEthernet0/0/1] clear configuration this
Warning: All configurations of the interface will be cleared, and its state will be shutdown. Continue? [Y/
N] :y
Info: Total 2 command(s) executed, 2 successful, 0 failed.
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 shutdown
#
return
```

2.8.5 clear inactive-configuration all

Function

The **clear inactive-configuration all** command clears inactive configurations on the switch.

NOTE

This command can only clear inactive configurations on interfaces.

Format

clear inactive-configuration all

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If a card is removed, the original configurations on the card are saved on the switch. If the standby/slave switch leaves a stack, the configurations on the switch are saved on the master switch. These invalid configurations are called inactive or offline configurations. To view inactive configurations on the switch, run the **display current-configuration inactive** command.

You can run the **clear inactive-configuration all** command to clear all the inactive configurations on the switch to increase available space.

This command can be run by only one user at a time to clear inactive configurations on all interfaces on the device.

NOTICE

Configurations cannot be recovered after clearing. Therefore, exercise caution when deciding to run this command. You are advised to run this command under the guidance of technical support personnel.

Example

Clear inactive configurations on the switch.

```
<HUAWEI> system-view
[HUAWEI] clear inactive-configuration all
Warning: All inactive configurations will be deleted and cannot be restored.
Are you sure you want to continue?[Y/N]y
The command will take a few minutes. Please wait.
Info: There is no inactive configuration.
```

2.8.6 configuration backup local disable

Function

The **configuration backup local disable** command disables the device from backing up the running configurations locally.

The **undo configuration backup local disable** command enables the device to back up the running configurations locally.

By default, the device is enabled to back up the running configurations locally.

Format

configuration backup local disable

undo configuration backup local disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To automatically back up the current running configurations to the local storage after the device configurations are modified, run the **undo configuration backup local disable** command to enable automatic backup of the current running configurations. This function helps check historical records of configuration changes and facilitate fault location.

Precautions

- When the device is enabled to back up the current running configurations, the current running configurations are backed up 2 hours after the device configurations are modified. If saving or automatic saving operation is performed, conflicts may occur. The configuration backup will be triggered every 30 minutes until the backup succeeds.
- If the CPU usage exceeds 60% during the configuration backup, the configuration backup will be triggered every 30 minutes until the backup succeeds.
- Delivering a configuration command fails during the configuration backup.
- If the current configurations are consistent with the configurations saved last time, the device does not repeatedly back up the current configurations to the local storage.

Rules for backup file management:

- The local storage path is **$_backup/running_config/**.
- The format of the backup file name is **yyyymmddhhmmss.sysname.zip**, where **yyyymmdd** indicates the year, month, and day, **hhmmss** indicates the hour, minute, and second, and **sysname** indicates the host name of the device.
- Backup files are aged based on the aging rules each time when the number of backup files exceeds 30, when the total space used by backup files exceeds 10 MB, or when the remaining storage space is less than 30 MB.
- The backup file aging stops when the number of backup files is 5 or less.

Rules for backup file aging:

- A number and an aging priority are specified for a backup file based on the file generation time.

NOTE

File number: The latest file generated is numbered 1, the file generated before the latest file is numbered 2, and so on. A larger number indicates an earlier generation time.

File aging priority: The file with a smaller file number has a higher priority. Files with a lower priority are aged first. Note that files with priority 0 are not aged. If a file has multiple priorities, refer to the highest priority.

  - Priority 0: files numbered from 1 to 5
  - Priority 1: files numbered from 6 to 10
  - Priority 2: the last generated files on each day in the past week
  - Priority 3: the last generated files in each month in the past 5 months
  - Priority 4: other backup files
- Note for backup file aging:
  - The backup files are aged in time sequence based on the priority. A backup file generated earlier is aged first.

Example

Disable the device from backing up the running configurations locally.

```
<HUAWEI> system-view
[HUAWEI] configuration backup local disable
```

2.8.7 configuration copy file to running

Function

The **configuration copy file to running** command executes commands in a specified configuration file.

Format

configuration copy file *file-name* **to running**

Parameters

Parameter	Description	Value
file-name	Specifies the name of a configuration file to be executed.	The value is a string of 4 to 160 characters in the [*drive*] [*path*] *file-name* format. The file name extension must be .cfg or .zip.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To execute an existing configuration file, run the **configuration copy file to running** command. All the commands in the specified configuration file are executed at one time.

Precautions

- Only one user can execute the **configuration copy file to running** command at one time.
- Running this command does not clear the existing configuration.
- If configuration restoration occurs or a batch backup operation is performed, the **configuration copy file to running** command ends.
- If a command fails during the execution of the **configuration copy file to running** command, the system skips it and executes the next command.
- If the configuration file to be executed contains a restart command, the device will restart when the restart command is executed. Therefore, exercise caution when executing the configuration file.
- Do not change the configuration file manually and execute the configuration file. Otherwise, the device may not start normally.

Example

Execute the commands in the **huawei.cfg** file.

```
<HUAWEI> configuration copy file huawei.cfg to running
Warning: This operation may take a long time, press CTRL+C to break. Continue?[Y/N]:y
```

2.8.8 configuration copy startup to file

Function

The **configuration copy startup to file** command backs up the startup configuration file to a specified file.

Format

configuration copy startup to file *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a destination file.	The value is a string of 4 to 160 characters in the [*drive*] [*path*] *file-name* format. The file name extension must be .cfg or .zip. The extension of the destination file and the backup file must be the same.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To back up the startup configuration file, run the **configuration copy startup to file** command.

Precautions

If a file with the same name already exists, the system asks whether to replace the previous file. Press **Y** to replace the file or **N** not to do so.

Example

Back up the startup configuration file to the **huawei.cfg** file.

```
<HUAWEI> configuration copy startup to file huawei.cfg
```

2.8.9 compare configuration

Function

The **compare configuration** compares whether the current configurations (including offline configurations) are identical with the next startup configuration file.

Format

compare configuration [*configuration-file*] [*current-line-number save-line-number*]

Parameters

Parameter	Description	Value
configuration-file	Specifies the name of the configuration file to be compared with the current configurations.	The value is a string of 5 to 48 case-insensitive characters without spaces.
current-line-number	Specifies the line number for comparison in the current configuration.	The value is an integer that ranges from 0 to 65535.

Parameter	Description	Value
save-line-number	Specifies the line number for comparison in the saved configuration.	The value is an integer that ranges from 0 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If *current-line-number* and *save-line-number* are not specified, the configuration files are compared from the first lines. The two parameters can be specified to skip the differences that are found and continue the comparison.

The **compare configuration** command outputs display the current configuration file (including offline configurations) and the saved configuration file from the line that contains differences respectively. By default, the output difference information is restricted to 120 characters.

- If the characters from differences to the end of the configuration file are less than 120, the system displays the output difference information till the end of the configuration file.
- If the characters from differences to the end of the configuration file are more than 120, the system only displays 120 characters.

Precautions

- The execution of this command takes a long time. To terminate the running command, press **Ctrl+C**.
- The configuration file name extension must be .cfg or .zip.
- If *configuration-file* is not specified, the system compares whether the current configurations (including offline configurations) are identical with the next startup configuration file.
- If *configuration-file* is specified, the system compares whether the current configurations (including offline configurations) are identical with the specified startup configuration file.

Example

Compare whether the current configurations (including offline configurations) are identical with the next startup configuration file.

```
<HUAWEI> compare configuration
Info: The system is now comparing the configuration, please wait....
Warning: The current configuration is not the same as the next startup
configuration file. There may be several differences, and the following are some
```

```
configurations beginning from the first:
====== Current configuration line 6 ======
 vlan batch 1 to 2 10 to 11 15 70 to 71 91 to 92 100 111 230 240 901
 vlan batch 911 1111
#
 l2protocol-tunnel vtp group-mac xxxx-xxxx-xxxx

 ====== Configuration file line 6 ======
 vlan batch 1 to 2 10 to 11 15 70 91 to 92 100 111 230 240 901
 vlan batch 911 1111
#
 l2protocol-tunnel vtp group-mac xxxx-xxxx-xxxx
```

2.8.10 display changed-configuration time

Function

The **display changed-configuration time** command displays the time of the last configuration change.

Format

display changed-configuration time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After changing the configuration of the device, you can run the **display changed-configuration time** command to view the time of the last configuration change.

Example

Display the time of the last configuration change.

```
<HUAWEI> display changed-configuration time
```

2.8.11 display configuration recover-result

Function

The **display configuration recover-result** command displays the configuration recovery result.

Format

display configuration recover-result

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use the **display configuration recover-result** command to view the information about the configuration recovery result and records of configuration recovery failures. The records include the command that fails the configuration recovery, the view in which the command resides, the line number of the command in the current startup configuration file, the reason why the command fails, and the execution time of the configuration recovery.

This command displays a maximum of 256 records in time sequence. The latest record is displayed in the last. If the number of commands for configuration recovery exceeds 256, the device no longer records commands that fail the configuration recovery.

Prerequisites

The device has restarted and the configuration recovery is successful.

Example

Display the configuration result.

```
<HUAWEI> display configuration recover-result
The current startup saved-configuration file is flash:/vrpcfg.zip.
The number of failed commands is 2.
-----------------------------------------------------------------------

Command : ip address 10.85.1.1 255.255.255.0
View    : Vlanif85
Line    : 414
Reason  : Failed to parse the command.
Time    : 10:00:06  2012-07-25 UTC+08:00 DST

Command : ip address 10.86.1.1 255.255.255.0
View    : Vlanif86
Line    : 417
Reason  : Failed to parse the command.
Time    : 10:00:06  2012-07-25 UTC+08:00 DST

-----------------------------------------------------------------------
```

Table 2-55 Description of the display configuration recover-result command output

Item	Description
Command	Command that fails the configuration recovery
View	View in which the command resides
Line	Line number of the command in the current startup configuration file
Reason	Reason why the command fails
Time	Execution time of the configuration recovery

2.8.12 display current-configuration

Function

The **display current-configuration** command displays the currently running configuration.

This command does not display parameters that use default settings.

Format

display current-configuration [**configuration** [*configuration-type* [*configuration-instance*]] | **interface** [*interface-type* [*interface-number*]]] [**feature** *feature-name*] [**filter** *filter-expression*]

display current-configuration [**all** | **inactive**]

display current-configuration configuration vpn-instance [*vpn-instance-name*] **related**

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **display current-configuration configuration vpn-instance** [*vpn-instance-name*] **related** command.

Parameters

Parameter	Description	Value
configuration	Displays all configuration information, except for the configuration on interfaces.	-

Parameter	Description	Value
configuration-type	Specifies information about the configuration that is a specified type, except for the configuration on interfaces. The configuration type depends on the existing configuration. For example: ● system: system configuration ● user-interface: user interface configuration ● aaa: AAA configuration	-
configuration-instance	Specifies information about the specified configuration instance, except for the configuration on interfaces. The configuration instance depends on the existing configuration.	The value is a string of 1 to 180 case-insensitive characters without spaces.
interface [*interface-type* [*interface-number*]]	Specifies an interface type. The information on the interface depends on the existing configuration. ● *interface-type*: specifies the type of an interface ● *interface-number*: specifies the number of an interface	-
feature *feature-name*	Specifies the configuration information about the specified feature. The configuration information about the feature depends on the existing configuration.	-

Parameter	Description	Value
filter *filter-expression*	Displays the configuration information that matches a regular expression.	The value is a string of 1 to 255 case-insensitive characters, spaces not supported. The matching starts from the first character of the command. For example, if snmp-agent is specified for *filter-expression*, only commands beginning with snmp-agent are filtered.
all	Displays all the configuration information.	-
inactive	Displays configurations about the cards that are not installed. When a card is not inserted, its configuration information is in the inactive status. The front of these configurations in the inactive state is marked with an asterisk (*).	-
vpn-instance [*vpn-instance-name*]	Displays configurations of a VPN instance with a specified name.	The value must be an existing VPN instance name.
related	Displays configurations of a specified module.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To check whether the configured parameters take effect, run the **display current-configuration** command. The parameters that do not take effect are not displayed.

The command output is relevant to user configuration.

You can use a regular expression to filter the command output. For the regular expression rules, see Filtering Output Information Based on the Regular Expression in "CLI Overview" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Basic Configuration*.

If the configuration is in the offline state, the offline configuration is marked with * in the **display current-configuration all** and **display current-configuration inactive** command output.

Example

Display all configurations that include **vlan**.

```
<HUAWEI> display current-configuration | include vlan
vlan batch 10 77 88
 port trunk allow-pass vlan 10
```

Display the FTP feature configuration.

```
<HUAWEI> display current-configuration feature ftp
#
FTP server enable
#
------------ END ------------
```

2.8.13 display factory-configuration information

Function

The **display factory-configuration information** command displays whether the function of restoring the factory configuration by holding down the Reset button is enabled and the mode of restoring the factory configuration.

NOTE

Only the SS1720GW-E, S1720GWR-E, and S1720GFR-P support this command.

Format

display factory-configuration information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before restoring the factory configuration by holding down the Reset button, you can run this command to check whether the function of restoring the factory configuration by holding down the Reset button is enabled and whether the mode of restoring the factory configuration is deleted or reserved.

Example

Display whether the function of restoring the factory configuration by holding down the Reset button is enabled and the mode of restoring the factory configuration.

```
<HUAWEI> display factory-configuration information
Reset function status: enable
Operate mode: deleted
```

Table 2-56 Description of the **display factory-configuration information** command output

Item	Description
Reset function status	Whether the function of restoring the factory configuration after you hold down the Reset button is enabled. ● enable: When you hold down the Reset button on a device, the device restarts with the factory configuration. ● disable: When you hold down the Reset button on a device, the device restarts without the factory configuration.
Operate mode	Mode of restoring the factory configuration. ● deleted: The system deletes the previous configuration when restoring the factory configuration. ● reserved: The system reserves the previous configuration when restoring the factory configuration.

2.8.14 display factory-configuration reset-result

Function

The **display factory-configuration reset-result** command displays the latest factory configuration restoration result of a switch.

Format

display factory-configuration reset-result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the factory configuration of a switch is restored using the **reset factory-configuration** command, you can run the **display factory-configuration reset-result** command to check the factory configuration restoration result.

Example

Display the latest factory configuration restoration result.

```
<HUAWEI> display factory-configuration reset-result
Slot   Time                         Type                              Result
--------------------------------------------------------------------------------------
0      2017/10/11 15:55:11 [DST]    Startup saved-configuration file     Succeeded
                                    Configuration in flash               Succeeded
                                    Netconf db-configuration             Succeeded
                                    Data file                            Succeeded
```

Table 2-57 Description of the **display factory-configuration reset-result** command output

Item	Description
Slot	Stack ID.
Time	Time for restoring the factory configuration.

Item	Description
Type	Type of the configuration file that needs to be restored to the factory configuration. - Startup saved-configuration file: configurations in the configuration file - Configuration in flash: configurations in the flash, such as the stack configuration - Netconf db-configuration: database files of the NETCONF and NETCONF - Data file: data files in the file system
Result	Result of restoring the factory configuration of the configuration file. - Succeeded: Factory configuration restoration succeeds. - Failed: Factory configuration restoration fails.

2.8.15 display pnp-button mode

Function

The **display pnp-button mode** command displays the device behavior after the PNP button is pressed and held.

Format

display pnp-button mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **pnp-button mode reset-system** command to configure the device behavior after the PNP button is pressed and held, you can run the **display pnp-button mode** command to view the command configuration.

Example

Display the device behavior after the PNP button is pressed and held.

```
<HUAWEI> display pnp-button mode
Pnp configuration mode: reset single switch.
Pnp button enable: enable.
```

Table 2-58 Description of the **display pnp-button mode** command output

Item	Description
Pnp configuration mode	PnP configuration mode: ● reset system: The default settings of the stack will be restored and the stack will automatically restart. ● reset single switch: The default settings of a specific stack member will be restored and the stack member will automatically restart.
Pnp button enable	Whether the PNP button is available: ● enable: The PNP button is available. ● disable: The PNP button is unavailable.

2.8.16 display reboot-info

Function

The **display reboot-info** command displays the device reset information.

Format

display reboot-info [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- Specifies the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	The value is an integer. The value is 0 if stacking is not configured, and varies according to the stacking configuration if stacking is configured.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the type and time of a reset.

This command displays reset information collected by the device, including the reset type and time. The following reset types may be displayed:

- MANUAL: The device was restarted manually using the **reboot** command or the NMS.
- POWER: The device restarted after being powered off (usually because users switch off the power supply).
- SCHEDU: The device restarted at a scheduled time.
- FSP: The device restarted due to a stack split or merge or an incorrect Mod-ID.
- EXCEPTION: The device restarted due to an exception or a dead loop.
- VRP: The device restarted due to an active/standby switchover or a fault on the VRP platform.
- SOFTWARE: The device restarted due to a software fault which is traceable.
- OS: The kernel was abnormal and initiated a reset.
- WATCHDOG: The device restarted due to the hardware watchdog.
- OTHER: Other causes.
  - A hardware component, such as the CPU, flash, or memory, has failed.
  - The device has overheated.
  - The switch was power recycled instantly, for example, when the power cable is in bad contact or when transient overvoltage and loss of voltage occurs. In this case, check whether the power cable is correctly connected to the switch.
  - The reboot was caused by other reasons that cannot be categorized into the preceding types. For example, the switch rebooted after joining a stack.

Example

Display the device reset information.

```
<HUAWEI> display reboot-info
Slot ID   Times         Reboot Type         Reboot Time(DST)
==========================================================================
0           1         POWER              2013/07/18 19:19:56
0           2         SCHEDU             2013/07/18 18:51:04
0           3         SOFTWARE             2013/07/18 18:41:22
0           4         EXCEPTION           2013/07/18 17:38:26
0           5         MANUAL              2013/07/18 17:31:14
0           6         MANUAL              2013/07/18 17:26:01
0           7         EXCEPTION           2013/07/18 17:03:28
==========================================================================
Total   7
```

Table 2-59 Description of the display reboot-info command output

Item	Description
Slot ID	Stack ID if the stacking function is enabled or the slot ID if the stacking function is not enabled.
Times	Number of board resets.
Reboot Type	Types of reset, including MANUAL, POWER, SCHEDU, FSP, EXCEPTION, VRP, SOFTWARE, OS, WATCHDOG, and OTHER.
Reboot Time(DST)	Time when a board was reset. On devices that do not support RTC, the device synchronizes the system clock on the network after the NTP function is configured. During the synchronization, the system time when the device is delivered is displayed. If synchronization fails, the system time when the device is delivered is displayed.

2.8.17 display saved-configuration

Function

The **display saved-configuration** command displays the configuration file to be used for the next startup.

Format

display saved-configuration [**last** | **time** | **configuration**]

Parameters

Parameter	Description	Value
last	Displays the system configurations saved last time.	-

Parameter	Description	Value
time	Displays the recent time when the configurations are saved manually or automatically.	-
configuration	Displays the parameters of the automatic save function.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

If the device has been started and is not working properly, run the **display saved-configuration** command to check the device startup configuration in the file specified by running the **startup saved-configuration** command.

Run the **display saved-configuration last** command to check the system configurations saved last time in the configuration file loaded during the current startup.

Run the **display saved-configuration time** command to check the last time when the system configurations are saved.

Run the **display saved-configuration configuration** command to check the automatic save function parameters including the automatic save interval and CPU usage.

The command output is relevant to user configuration.

Example

Display the configuration file for the next startup.

```
<HUAWEI> display saved-configuration
#
 sysname Switch
...
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.1.3 255.255.255.0
#
interface Vlanif20
 ip address 192.168.4.3 255.255.255.0
...
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
...
```

```
#
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
 idle-timeout 0 0
#
return
```

2.8.18 display schedule reboot

Function

The **display schedule reboot** command displays the configuration of the scheduled restart of the device.

Format

display schedule reboot

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After using the **schedule reboot** command to configure a scheduled restart, you can use this command to view the configuration of the scheduled restart.

Example

Display the configuration of the scheduled restart of the device.

```
<HUAWEI> display schedule reboot
Info:System will reboot at 22:00:00 2013/09/17 (in 1 hours and 43 minutes).
```

Table 2-60 Description of the display schedule reboot command output

Item	Description
System will reboot at	Specific restart time.
in hours and minutes	Time span between the restart time and the current time.

2.8.19 display startup

Function

The **display startup** command displays the system software and configuration files for the current and next startup.

Format

display startup [**slot** *slot-id*]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slot** *slot-id* parameters.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before upgrading or degrading a device, run this command to check whether the files for next startup have been loaded. If the files have been loaded, the device can be upgraded or degraded successfully after it is restarted. You can also run the command to view the system software and files for current startup.

The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.

Example

Display the names of system software for current and next startup.

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:        flash:/basicsoftware.cc
  Startup system software:                   flash:/basicsoftware.cc
  Next startup system software:              flash:/basicsoftware.cc
  Startup saved-configuration file:          flash:/vrpcfg.zip
  Next startup saved-configuration file:     flash:/vrpcfg.zip
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
```

```
Startup license file:                NULL
Next startup license file:           NULL
Startup patch package:               NULL
Next startup patch package:          NULL
```

Table 2-61 Description of the display startup command output

Item	Description
Configured startup system software	System software that is configured for the current startup by running the **startup system-software** command before the system starts.
Startup system software	System software that is used in the current startup.
Next startup system software	System software that is configured for the next startup by running the **startup system-software** command. If no system software for the next startup is configured, the system software used in the current startup is displayed.
Startup saved-configuration file	Configuration file that is used in the current startup.
Next startup saved-configuration file	Configuration file that is configured for the next startup by running the **startup saved-configuration** command. If no configuration file for the next startup is configured, the configuration file used in the current startup is displayed.
Startup paf file	PAF file that is used in the current startup. **default** indicates that no PAF file is specified or the PAF file does not take effect. **NULL** indicates that no PAF file exists on the device.
Next startup paf file	PAF file that is configured for the next startup. If no PAF file is configured, **default** is displayed. **NULL** indicates that no PAF file exists on the device.

Item	Description
Startup license file	License file that is used in the current startup. **default** indicates that no license file is specified or the license file does not take effect. **NULL** indicates that no license file exists on the device.
Next startup license file	License file that is configured for the next startup. If no license file is configured, **default** is displayed. **NULL** indicates that no license file exists on the device.
Startup patch package	Patch package file that is used in the current startup. **NULL** indicates that no patch package file is specified or the patch package file does not take effect.
Next startup patch package	Patch package file that is configured for the next startup by running the **startup patch** command. If no patch package file is configured, **NULL** is displayed.

2.8.20 factory-configuration prohibit

Function

The **factory-configuration prohibit** command disables the function of restoring the factory settings of a device by holding down **reset**.

The **undo factory-configuration prohibit** command enables the function of restoring the factory settings of a device by holding down **reset**.

By default, you can hold down **reset** to restore the factory configuration.

NOTE

Only SS1720GW-E, S1720GWR-E, and support this command.

Format

factory-configuration prohibit

undo factory-configuration prohibit

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you hold down **reset** on a device for more than 5 seconds, the device restarts with the factory settings and all user-defined configurations are lost after the restart. To retain user-defined configurations after you hold down **reset**, run the **factory-configuration prohibit** command to disable this function.

If you want to restore the factory settings of a device by holding down **reset**, run the **undo factory-configuration prohibit** command to enable this function.

Example

Disable the function of restoring the factory configuration of a device by holding down **reset**.

```
<HUAWEI> system-view
[HUAWEI] factory-configuration prohibit
```

2.8.21 pnp-button mode reset-system

Function

The **pnp-button mode reset-system** command configures all member switches in a stack to restore to the default settings and restart after the PNP button is pressed and held.

The **undo pnp-button mode reset-system** command restores the default settings.

By default, a switch in a stack restores to the default settings and automatically restarts after the PNP button is pressed and held on the switch.

Format

pnp-button mode reset-system

undo pnp-button mode reset-system

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To clear all service configurations and data files, press and hold the PNP button for more than 6 seconds to restore the default settings and automatically restart the device. By default, holding the PNP button on any device in a stack will restore the device to the default settings and automatically restart the device. To clear the service configurations and data files of the stack, run the **pnp-button mode reset-system** command to configure the device behavior after the PNP button is pressed and held.

Example

Configure all member switches in a stack to restore to the default settings and automatically restart after the PNP button is pressed and held.

```
<HUAWEI> system-view
[HUAWEI] pnp-button mode reset-system
```

2.8.22 pnp-button disable

Function

The **pnp-button disable** command disables the PNP button function of a device.

The **undo pnp-button disable** command enables the PNP button function of a device.

By default, the PNP button function is enabled on a device.

Format

pnp-button disable

undo pnp-button disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you do not want anyone to use the PNP button to reset the device configuration or restart the device, run the **pnp-button disable** command to disable the PNP button function of the device.

Example

Disable the PNP button function of the device.

```
<HUAWEI> system-view
[HUAWEI] pnp-button disable
```

2.8.23 reboot

Function

The **reboot** command restarts the device.

Format

reboot [**fast** | **save diagnostic-information**]

Parameters

Parameter	Description	Value
fast	Fast restarts the device. In fast restart mode, the configuration file is not saved.	-
save diagnostic-information	Saves the diagnostic information before the restart.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command functions in the same way as a power recycle operation (power off and then restart the device). The command enables you to restart the device remotely.

- If the configuration file for next startup (new configuration file) is the same as the configuration file saved on the device after the **reboot** command is run, the system will not ask you whether to save the configuration before the restart. If the configuration file for next startup (new configuration file) differs from the configuration file saved on the device, the system asks you whether to save the configuration before the restart, and unsaved configuration information will be lost after the restart.

- When the **reboot fast** command is run, the system restart quickly without displaying any message and the configuration is lost.
- After the **reboot save diagnostic-information** command is run, the system will save the diagnostic information to root directory of the storage device before restarting.

Precautions

- If you do not respond to the displayed message within the timeout period after running this command, the system will return to the user view and the device will not be restarted.
- To avoid loss of diagnostic information after a restart, configure the device to save the diagnostic information before restarting.
- This command interrupts services on the entire device. Therefore, do not use this command when the device is running properly.
- Before restarting the device, ensure that the configuration file has been saved.
- If you upgrade the system software to V200R009C00 or a later version and the configuration file contains WLAN configurations, the system displays a message indicating that the configuration file conflicts with the system software for next startup when the device restarts. The system software upgrade fails. If a conflict occurs, you need to use the eDesk tool to convert configurations in the configuration file, and specify the converted configuration file as the configuration file for next startup. If the configuration file is not converted, the configurations will be lost after the system is restarted and upgraded.
- If multiple users run the **reboot save diagnostic-information** command at the same time, a message indicating that the command is locked by another user is displayed.
- If a user runs the **display diagnostic-information** command when another user is running the **reboot save diagnostic-information** command, a message indicating that the command is locked by another user is displayed.
- The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, and S5735S-S support the stacking function since V200R019C10. S5735-L-I supports the stacking function since V200R021C00. If multiple switches set up a stack and the system software package for the next startup is earlier than V200R019C10, the stack will split after the **reboot** command is executed to restart any stack member. If the stacking function is enabled on a single switch, the system software package for the next startup is earlier than V200R019C10, and the **stack slot renumber** command is executed to change the stack ID of the switch to a non-zero value, then the stack configuration of the switch will be cleared and the slot-ID-related configuration cannot be restored after the **reboot** command is executed to restart the switch.
- Due to the component upgrade of some device models, some devices cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about

the first supported version of the device and matching patch version, see the device overview in the "Hardware Description"..

NOTE

After converting configurations in the configuration file using the **eDesk pro** tool, restart the switch without saving the configurations. If the configurations are saved, the converted configuration file is invalid.

Example

Restart the device.

```
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait........
Warning: The configuration has been modified, and it will be saved to the next s
tartup saved-configuration file flash:/204.cfg. Continue? [Y/N]:y
Info: If want to reboot with saving diagnostic information, input 'N' and then e
xecute 'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

Restart the device quickly.

```
<HUAWEI> reboot fast
Info: If want to reboot with saving diagnostic information, input 'N' and then execute 'reboot save
diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

2.8.24 reset factory-configuration

Function

The **reset factory-configuration** command restores the factory settings of the device.

Format

reset factory-configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear all service configurations and data files, run the **reset factory-configuration** command to restore the factory settings.

Precautions

After you run the **reset factory-configuration** command, the system asks you whether to restart the device. After you enter **y**, the device restarts and clears the service configurations and data files on the device. The configurations and files to be cleared include:

- Configurations in the configuration file
- Configurations in the flash memory, such as the stackconfigurations.
- Database files in NETCONF
- Data files in the file system

NOTE

- The next-startup system software package, patch, module, and license file will not be deleted.
- This command will not delete the protected directory and the $_default.cfg file in the protected directory.

NOTICE

Exercise caution and use this command under the supervision of technical support personnel.

Example

Restore the device to factory settings.

```
Warning: The command will delete all the configurations and files (except the startup, patch, module, and
license files) from the de
vice. Continue? [Y/N]:y
Warning: The system will reboot after configurations and files are deleted. Continue? [Y/
N]:y
```

2.8.25 reset saved-configuration

Function

The **reset saved-configuration** command clears the next startup configuration file and cancels the configuration file used for next startup.

Format

reset saved-configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- If the configuration file on the device is incompatible with the upgraded software, run the **reset saved-configuration** command to clear the configuration file and run the **startup saved-configuration** command to specify a new configuration file.
- If the device in use is applied to another scenario and the original configuration file of the device does not meet requirements in the scenario, run the **reset saved-configuration** command to clear the existing configuration file and restart the device to restore its factory configurations.

Precautions

- After you run the **reset saved-configuration** command, the next startup configuration file is cleared and the file is not used for next startup. If the current startup configuration file is the same as the next startup configuration file, the current startup configuration file is also cleared.
- If you do not use the **startup saved-configuration** command to specify a new configuration file or do not save the configuration file after the file is not used for next startup, the device uses default factory configurations for startup.
- If the current configuration file is empty, and the configuration file for the next startup is not empty, running the **reset saved-configuration** command clears the settings for the configuration file for the next startup.
- If the configuration file for the next startup is empty, and the current configuration file is not empty, after the **reset saved-configuration** command is run, the system prompts an error and no settings are cleared.
- Exercise caution when you run the **reset saved-configuration** command.
- Running the **reset saved-configuration** command will clear the content in the configuration file used for the next device startup but not clear the database information on the device. In NETCONF mode, run the **reset netconf db-configuration** command to clear the configuration and database file to prevent the configuration delivery failures caused by residual database files.
- After the **reset netconf db-configuration** or **reset saved-configuration** command is run, the **assign trunk** command configuration is cleared, that is, the default configuration is restored.

Example

Clear the next startup configuration file in the storage device and cancel the configuration file used for next startup.

```
<HUAWEI> reset saved-configuration
Warning: The action will delete the saved configuration in the device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Info: Succeeded in clearing the configuration in the device.
```

2.8.26 reset reboot-info

Function

The **reset reboot-info** command resets the device reset information.

Format

reset reboot-info [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- Specifies the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.

Views

User view

Default Level

3: Management level

Usage Guidelines

The device records information about every restart, including the number of restart events, restart type, and restart time. Run the **display reboot-info** command to view restart information. You can run the **reset reboot-info** command to clear restart information.

Example

Reset the device reset information.

```
<HUAWEI> reset reboot-info
```

2.8.27 save

Function

The **save** command saves the configurations to the default directory.

Format

save [**all**] [**force**] [*configuration-file*]

Parameters

Parameter	Description	Value
all	Saves all configurations to the next startup configuration file of the system. **NOTE** All configurations are saved, including those of the boards that are not running, no matter whether **all** is specified.	-
force	Forcibly saves configurations.	-
configuration-file	Specifies the name of a configuration file.	The value is a string of case-insensitive characters. The absolute path length ranges from 5 to 64 characters. The value cannot contain spaces and the following characters: < > \ ? , : `. Left and right square brackets cannot be used in pairs. The forward slash (/) and period (.) cannot be used together.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to take effect after a restart, save the current configuration in the configuration file before restarting the device.

When a series of configurations are complete and take effect, you must save the current configuration file to the storage device.

- If the *configuration-file* parameter is not specified, the **save** [**all**] command saves the current configuration to the next startup configuration file in the storage device. The "Next startup saved-configuration file:" field displayed in the **display startup** command output indicates the next startup configuration file.

- The **save** [**all**] *configuration-file* command saves the current configuration to the specified directory of the storage device. Generally, the command does not affect the current startup configuration file. Only if the *configuration-file* parameter is the same as the directory and name of the configuration file for the next startup, this command can be used as the same as the **save** command without the *configuration-file* parameter.
- The **save** [**all**] **force** *configuration-file* command saves the current configurations to a file specified by the *configuration-file* parameter on a storage device without user confirmation.

All configurations are saved, no matter whether **all** is specified.

If you do not specify *configuration-file* when saving the configuration file for the first time, the system asks you whether to save the configuration file as **vrpcfg.zip**. The **vrpcfg.zip** file is the default system configuration file with empty configurations in initial state.

Precautions

- If the configuration file to be saved using this command has the same name with the existing configuration file, the existing configuration file is rewritten.
- The configuration file name extension must be .zip or .cfg.
  - .cfg: The file is saved in plain text mode. After the file is specified as the configuration file, all commands in the file are recovered one by one during startup.
  - .zip: The .cfg file is compressed to a .zip file that occupies less space. After being specified as the configuration file, the .zip file is decompressed to the .cfg file and all commands in the .cfg file are recovered one by one during startup.
- When the system is saving configuration files, other users are not allowed to perform configuration. When the current user is performing configuration, other users are not allowed to save configuration files.
- When the controller delivers configurations, the configuration cannot be saved on the device side.
- If you run the **authentication-mode none** command to change the authentication mode of the console port to none authentication, security risks exist. When you save the configuration file, the system displays a message indicating security risks.
- If you run the **undo authentication-mode** command to change the authentication mode of the console port to none authentication, security risks exist. When you save the configuration file, the system displays a message indicating security risks.

Example

Save the current configuration to the default directory when the next startup configuration file is not specified.

```
<HUAWEI> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0.
Save the configuration successfully.
```

Save the current configuration to the next startup configuration file specified.

```
<HUAWEI> save
The current configuration will be written to flash:/vrpcfg.zip.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0.
Info: Save the configuration successfully.
```

2.8.28 schedule reboot

Function

The **schedule reboot** command configures the scheduled restart of a device and sets the specific time when the device restarts or the delay time before the device restarts.

The **undo schedule reboot** command disables the scheduled restart function.

By default, the scheduled restart is disabled.

Format

schedule reboot { **at** *time* | **delay** *interval* [**force**] }

undo schedule reboot

Parameters

Parameter	Description	Value
at *time*	Specifies the device restart time.	The format of *time* is *hh:mm YYYY/MM/DD*. The restart time must be later than the current device time by less than 720 hours. *YYYY/MM/DD* indicates year, month, and date and is optional. • *hh* indicates hour and the value ranges from 0 to 23. • *mm* indicates minute and the value ranges from 0 to 59. • *YYYY* indicates year and the value ranges from 2000 to 2099. • *MM* indicates month and the value ranges from 1 to 12. • *DD* indicates date and the value ranges from 1 to 31.

Parameter	Description	Value
delay *interval*	Specifies the delay time before the device restarts.	The format of *interval* is *hh:mm* or *mm*. The delay time must be no more than 720 hours. ● In *hh:mm*, *hh* indicates hour and the value ranges from 0 to 720 and *mm* indicates minute and the value ranges from 0 to 59. ● *mm* indicates minute and the value ranges from 0 to 43200.
force	Specifies forcible scheduled restart.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading or restarting the device, you can configure the device to restart at time when few services are running to minimize the impact on services.

Precautions

- If the **schedule reboot at** command is used to set a specific date (*YYYY/MM/DD*) and the date is a future date, the device restarts at the specified time. If no date is set, two situations occur: If the specified time is later than the current time, the device restarts at the specified time of the day. If the specified time is earlier than the current time, the device restarts at the set time next day.
- Note that the gap between the specified date and current date must be shorter than or equal to 720 hours. If the scheduled restart has been configured, the latest configuration overrides the previous one.
- Run the **schedule reboot delay** *interval* command to set the delay time before the device restarts. If the **force** parameter is not specified, the system compares the configuration file with the current configuration. If the current configuration is different from the configuration file, the system asks you whether to save the current configuration. After you complete the selection, the system prompts you to confirm the configured restart time. Enter **Y** or **y** to make the configured restart time take effect. If the **force** parameter is specified, the system does not display any message, and the restart time takes effect directly. The current configuration is not compared or saved.
- The scheduled restart function becomes invalid when you use the **clock datetime** command to set the system time to over 10 minutes later than the

restart time set by the **schedule reboot** command. If the time difference is equal to or less than ten minutes, the device immediately restarts and does not save the configuration.

- This command restarts the device at the specified time, interrupting all services on the device. Therefore, do not use this command when the device is running properly.
- Before restarting the device, ensure that the configuration file has been saved.

Example

Configure the device to restart at 22:00.

```
<HUAWEI> schedule reboot at 22:00
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-configuration
file flash:/vrpcfg.zip. C
ontinue? [Y/N]:y
Now saving the current configuration to the slot 0...
Save the configuration successfully.
Info: Reboot system at 22:00:00 2012/06/12 UTC-05:13(in 2 hours and 0 minutes)
confirm?[Y/N]:y
```

2.8.29 set factory-configuration operate-mode

Function

The **set factory-configuration operate-mode** command determines whether to reserve or delete the existing configuration when restoring the factory configuration.

The **undo set factory-configuration operate-mode** command enables the device to reserve the existing configuration when you restore the factory configuration.

By default, the system reserves the previous configuration when restoring the factory configuration.

NOTE

Only SS1720GW-E, and S1720GWR-E support this command.

Format

set factory-configuration operate-mode { **reserve-configuration** | **delete-configuration** }

undo set factory-configuration operate-mode

Parameters

Parameter	Description	Value
reserve-configuration	Reserves current configuration file after factory settings are restored.	-

Parameter	Description	Value
delete-configuration	Deletes current configuration file after factory settings are restored.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **set factory-configuration operate-mode delete-configuration** command to specify the operation as **delete-configuration** for restoring factory settings. This prevents user information leak when the device is lost.

Example

Set the mode of restoring the factory configuration to **delete**.

```
<HUAWEI> system-view
[HUAWEI] set factory-configuration operate-mode delete-configuration
Warning: It may delete your configuration file when executing factory configuration, continue?[Y/N]:y
```

2.8.30 set save-configuration

Function

The **set save-configuration** command enables the function of saving system configurations periodically.

The **undo set save-configuration** command disables the function of saving system configurations periodically.

By default, the system does not periodically save configurations.

Format

set save-configuration [**interval** *interval* | **cpu-limit** *cpu-usage* | **delay** *delay-interval*] *

undo set save-configuration [**interval** | **cpu-limit** | **delay**] *

undo set save-configuration [**interval** *interval* | **cpu-limit** *cpu-usage* | **delay** *delay-interval*] *

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for saving configurations.	The value is an integer that ranges from 30 to 43200, in minutes. The default value is 30.
cpu-limit *cpu-usage*	Specifies the threshold of the CPU usage during the periodic save operation.	The value is an integer that ranges from 1 to 60. The default value is 50.
delay *delay-interval*	Specifies the delay in automatic backup after the configuration changes. **NOTE** If a configuration change occurs within the configured delay time, the device restarts the timer.	The value is an integer that ranges from 1 to 60, in minutes. The default value is five minutes. The value of *delay-interval* must be less than the value of *interval*.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this command enables the function of saving system configurations periodically, the configuration file will not be lost if the device is powered off or restarts.

If the **set save-configuration** command is not executed, the system does not enable the function of saving system configurations periodically.

If the **set save-configuration** command is executed, the system compares the configuration files before saving configurations. If the configurations do not change, the system does not save the configurations.

- You can specify **interval** *interval* to set the interval for periodically saving configurations. The system saves the current configurations only when the configurations have been changed and are not saved. The default interval is 0 seconds, indicating that the system does not save the configurations. After the automatic save function is enabled, the default interval is 30 minutes if *interval* is not specified.
- If **cpu-limit** *cpu-usage* is specified, the automatic save function does not affect system performance. After the automatic save timer is triggered, the system cancels the current automatic save operation if the system CPU usage

  is detected to be higher than the upper limit. The default upper limit of the CPU usage is 50% for the automatic save function.
- After **delay** *delay-interval* is specified, the system saves the changed configurations after the specified delay. The default value is 5 minutes.

The **undo set save-configuration** command disables the automatic save function. The **undo set save-configuration** command with a parameter specified restores the default value of the parameter and the automatic save function still takes effect.

Follow-up Procedure

Run the **display saved-configuration configuration** command to check the configurations about the periodic save function.

Precautions

Before saving configurations, the system compares the configurations with those in the configuration file. Automatic saving of configurations is triggered in the following scenarios:

- The configurations are inconsistent with those saved last time.
- The configurations are the same as those saved last time, but changes have been made. For example, if a command is run and then its configurations are deleted, automatic saving of configurations will still be triggered although configurations are the same as those saved last time.

After the automatic save function is enabled, the configurations are saved in the configuration file for the next startup. The content in the configuration file changes when the configuration changes. The system cancels the automatic save operation when:

- Content is being written into the configuration file.
- The configurations are being recovered.
- The CPU usage is excessively high.

Example

Set the automatic save interval to 60 minutes.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration interval 60
```

Configure the system to save the new configuration 3 minutes after the configuration changes at an interval of 10 hours when the upper limit of the CPU usage is 60%.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration interval 600 delay 3 cpu-limit 60
```

2.8.31 set save-configuration backup-to-server server

Function

The **set save-configuration backup-to-server server** command specifies the server where the system periodically saves the configuration file.

The **undo set save-configuration backup-to-server server** command cancels the server where the system periodically saves the configuration file.

By default, the system does not periodically save configurations to the server.

Format

set save-configuration backup-to-server server *server-ip* [**vpn-instance** *vpn-instance-name*] **transport-type** { **ftp** | **sftp** } [**port** *port-number*] **user** *user-name* **password** *password* [**path** *path*]

set save-configuration backup-to-server server *server-ip* [**vpn-instance** *vpn-instance-name*] **transport-type tftp** [**path** *path*]

undo set save-configuration backup-to-server server [*server-ip* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
server *server-ip*	Specifies the IP address of the server where the system periodically saves the configuration file.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance.	The value must be an existing VPN instance name.
port *port-number*	Specifies the port number of a server.	The value is an integer ranging from 1 to 65535. By default, the port number of the FTP server is 21, and that of the SFTP server is 22.
transport-type	Specifies the mode in which the configuration file is transmitted to the server.	The value can be **ftp**, **sftp**, or **tftp**. To ensure file transfer security, use the SFTP method.
user *user-name*	Specifies the name of the user who saves the configuration file on the server.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
password *password*	Specifies the password of the user who saves the configuration file on the server.	The value is a case-sensitive string without spaces. The value of a simple text password is a string of 1 to 16 characters. The value of a ciphertext password is a string of 24, 32 or 48 characters. When double quotation marks are used around the string, spaces are allowed in the string.
path *path*	Specifies the relative save path on the server. If this parameter is not specified, the FTP, SFTP, or TFTP root path is enabled by default.	The value is a string of 1 to 64 case-sensitive characters without spaces. The path should use forward slashes. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to periodically save the configuration file to the server.

Before periodically saving configurations, the system compares the configuration files. If the configurations do not change, the system does not periodically save them.

Precautions

If the specified path on the server does not exist, configuration files cannot be sent to the server. The system then sends an alarm message indicating the transmission failure to the NMS, and the transmission failure is recorded as a log message on the device.

The user name and password must be the same as those used in FTP or SFTP login mode.

NOTE

- When you run this command to save configuration files to a server, the system supports only the binary transmission mode. Therefore, the server must support the binary transmission mode.
- Before running this command, run the **set save-configuration** command to start the periodic configuration saving function. Otherwise, configuration files are not saved to the server.
- FTP or TFTP is insecure. Therefore, configuring SFTP is recommended.
- A server IP address can be bound to multiple VPN instances. To delete the configurations of a specified VPN instance, you must set *vpn-instance-name*. Otherwise, configurations irrelevant to the VPN instance will be deleted.
- The configuration file saved by running this command is named in the format of yyyy-mm-dd.hh-mm-ss.sysname.zip, where yyyy indicates the year, the first mm indicates the month, dd indicates the day, hh indicates the hour, the second mm indicates the minute, ss indicates the second, and sysname indicates the host name, for example, **2022-07-02.17-23-17.HUAWEI.zip**.

Example

Specify the server to which the system periodically sends the configuration file, and set the transmission mode to SFTP.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration backup-to-server server 10.1.1.1 transport-type sftp user admin1234
password Helloworld@6789
```

Specify the server to which the system periodically sends the configuration file, and set the transmission mode to SFTP, port number to 88, and save path to **d:/sftp**.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration backup-to-server server 10.1.1.1 transport-type sftp port 88 user
admin1234 password Helloworld@6789 path d:/sftp
```

2.8.32 startup saved-configuration

Function

The **startup saved-configuration** command specifies the system configuration file for next startup.

The **undo startup saved-configuration** command deletes the system configuration for next startup.

Format

startup saved-configuration *configuration-file* [**slot** *slot-id*]

undo startup saved-configuration

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slot** *slot-id* parameters.

Parameters

Parameter	Description	Value
configuration-file	Specifies the name of a configuration file. Make sure that the file exists.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name extension can be .zip or .cfg. The file name must not contain %.
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

startup saved-configuration: User view

undo startup saved-configuration: System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the original configuration file cannot be used due to the software upgrade, run the **startup saved-configuration** command to specify another configuration file for next startup. The startup configuration file must be saved in the root directory of the storage device.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- The configuration file specified for the next startup must exist.
- The configuration file name extension must be .zip or .cfg.
  - A configuration file with the file name extension .cfg is a text file, and you can view the file content in the text file. After the file is specified as the configuration file for next startup, the system restores all commands in the file one by one during a startup.
  - A .cfg file is compressed to a .zip file that occupies less space. After being specified as the configuration file, the .zip file is decompressed to the .cfg file and the system restores all commands in the .cfg file one by one during startup.
- If the EasyDeploy function is configured, run the **undo startup saved-configuration** command to clear the configuration file for next startup and delete all the configuration files in the storage device. When the device

restarts, it finds no configuration file available and downloads a configuration file from the file server.

If the EasyDeploy function is not configured, run the **undo startup saved-configuration** command to clear the configuration file for next startup. After the command is run, the device uses empty configuration in next startup.

- The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.
- Do not change the configuration file manually and specify the configuration file for next startup. Otherwise, the device may not start normally.
- Users at level 3 or higher can change the configuration file used for the next startup.
- If the configuration file used for the next startup contains the **authentication-mode none** command that changes the authentication mode of the console port to none authentication, security risks exist. When you configure the configuration file used for the next startup, the system displays a message indicating security risks.
- If the configuration file used for the next startup contains the **undo authentication-mode** command that changes the authentication mode of the console port to none authentication, security risks exist. When you configure the configuration file used for the next startup, the system displays a message indicating security risks.

Example

Cancel the specified configuration file for next startup in the system view.

```
<HUAWEI> system-view
[HUAWEI] undo startup saved-configuration
```

Specify the system configuration file for the next startup.

```
<HUAWEI> startup saved-configuration vrpcfg.cfg
Info: Succeeded in setting the configuration for booting system.
```

2.8.33 startup system-software

Function

The **startup system-software** command specifies the system software for next startup.

Format

startup system-software *system-file* [**all** | **slave-board** | **slot** *slot-id*]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **all**, **slave-board**, or **slot** *slot-id* parameters.

Parameters

Parameter	Description	Value
system-file	Specifies the name of the system software file.	The value is a string of 4 to 64 case-sensitive characters without spaces and %. It is in the format of [*drive-name*] [*file-name*]. If *drive-name* is not specified, the name of the default storage device is used.
all	Specifies all member devices in a stack.	-
slave-board	Specifies the system software for next startup on the slave switch.	-
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In system software upgrade or downgrade, run this command to specify the system software for next startup.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- When the **startup system-software** command is run, the system displays a prompt and the current password is cleared only after the user confirms the operation.
- The system software package must use .cc as the file name extension and be saved to the root directory of the storage device.
- When the system software for next startup is configured using the **startup system-software** command, the system checks the system software integrity. If the digital signature of the system software is invalid, the configuration fails. Therefore, ensure the system software validity.

- If the upgrade or downgrade cannot be performed between versions, the system displays a message, prompting you to perform operations as prompted.
- The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.
- During system software upgrade of fixed PoE switches, powered devices (PDs) will be powered off.
- During the downgrade to an earlier version, the system checks whether the software package of the earlier version contains a complete signature file. If the software package does not contain a complete signature file, the system prompts you whether to continue the downgrade. After confirming that the software package is correct, the downgrade does not affect functions. However, you are advised to upgrade to a more secure version.

NOTE

The system file is authenticated when you configure the file name of the system software used in the next startup. Wait for a while.

Table 2-62 lists the possible causes and troubleshooting methods for failures to load the system software package to the device.

Table 2-62 Possible causes and troubleshooting methods for failures to load the system software package

Failure Cause		Troubleshooting Method
CRC check fails.	The system software package is damaged. Please upload again.	Upload the system software package again.
Version check fails.	The %s only supports the system software package of %s and later versions.	Upload the system software package of the version supported by the device.
Signature verification fails.	Software package verification failed. Please upload again.	Upload the system software package again.
The system software package is corrupted.	The system software package is damaged. Please upload again.	Upload the system software package again.
The system software package is not supported on the device.	The system software package does not match the device.	Upload the system software package that matches the device.
The name of the system software package is incorrect.	The system software package does not exist.	Change the name of the system software package and upload the package again.

Failure Cause		**Troubleshooting Method**
The name of the system software package is too long.	The file name is too long.	Change the name of the system software package and upload the package again.
Stacking is not supported.	The target version does not support CSS card stacking. Disable this stacking function and try later.	Disable the stacking function and upload the system software package again.
The system software package does not match the MPU.	The system software package does not include the MPU software package.	Upload the system software package that matches the MPU.
Failed to set the system software package.	Failed in setting the software for booting system.	Check whether the system software package matches the device type.
The directory where the system software package is uploaded is incorrect.	The file flash:/%.cc doesn't exist in the main board. (Default directory is flash:/)	Upload the system software package to the root directory of the flash memory.
The flash version does not support the system software package to be uploaded.	The flash chip version xxx does not support the new startup system software package. This file cannot be specified as the startup system software package.	Upload the system software package of the version supported by the flash.
The PHY version does not support the system software package to be uploaded.	The PHY chip version xxx does not support the new startup system software package. This file cannot be specified as the startup system software package.	Upload the system software package of the version supported by the PHY.
The LSW version does not support the system software package to be uploaded.	The LSW chip version xxx does not support the new startup system software package. This file cannot be specified as the startup system software package.	Upload the system software package of the version supported by the LSW.

Failure Cause		Troubleshooting Method
The hardware version VER.B does not support the new system software package.	The hardware VER.B does not support the startup software package. You need to configure the matching patch first.	Configure the matching patch first. For details, see the reference document or upgrade guide.

Example

Specify the system software to be loaded for next startup.

```
<HUAWEI> startup system-software basicsoft.cc
```

2.8.34 startup patch

Function

The **startup patch** command specifies the patch file for next startup.

Format

startup patch *patch-name* [**slave-board** | **slot** *slot-id*]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slave-board** parameters.

Parameters

Parameter	Description	Value
patch-name	Specifies the name of the patch file for next startup.	The value is a string of 5 to 64 case-insensitive characters without spaces. It is in the format of [*drive-name*] [*path*] [*file-name*]. If *drive-name* is not specified, the name of the default storage device is used.
slave-board	Specifies the patch file for next startup on slave switch.	-
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To make the patch file take effect after the device restarts, run this command to specify the patch file for next startup.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- A patch file uses .pat as the file name extension and must be saved in the root directory.
- If you use this command to specify another patch for next startup, the previous patch will be overridden.
- After the patch file is specified for next startup, run the **display patch-information** command to view the patch file.
  - If the patch file for next startup is not empty, the device load the patch automatically after next startup.
  - If the patch file for next startup is empty, the device cannot load the patch after next startup.
- After the device restarts, the system loads and runs the patch. If you do not want the system to load the patch file after startup, use either of the following methods to delete the patch file:
  - Run the **patch delete all** command to delete the current patch.
  - Run the **reset patch-configure** [**next-startup**] command to delete the patch file already loaded on the system after startup.
- The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.

Example

Specify the patch file for next startup.

```
<HUAWEI> startup patch patch.pat.........................................
................................
Info: Succeeded in setting main board resource file for system.
```

2.9 Smart Upgrade Commands

2.9.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support Smart Upgrade.

Only the following switch models support Smart AP Upgrade:

S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H

2.9.2 display smart-upgrade information

Function

The **display smart-upgrade information** command displays details about smart upgrade.

Format

display smart-upgrade information

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After smart upgrade is enabled, you can run the **display smart-upgrade information** command to check network connectivity with the HOUP and check whether a new version of software or patch is available for upgrade.

Precautions

This command triggers information exchange between the switch and HOUP. If this command is used frequently, smart upgrade may be affected.

Example

Display details about smart switch or AP upgrade.

```
<HUAWEI> display smart-upgrade information
Info: Loading the information, please wait .

Configuration:
    URL                        : s.houp.huawei.com
    HTTPS port                   : 443
    Bind SSL policy              : houp
```

```
    Verify HTTPS server          : true
Version information:
    Refresh time                 : 2019-01-23 12:24:06
    Check version result         : needUpdate
    Recommended software version : V200R023C00
    Recommended patch version    : V200R020SPH001
    Upgrade description          :
    Firmware and Patch Description in English:1)description:2)CC+SPH

    Software package name        : S5732-H-V200R023C00.cc
    Software package size(B)     : 120101636
    Patch package name           : S5732-H-V200R020SPH001.pat
    Patch package size(B)        : 14910

Upgrade information:
    Upgrade Time                 : 2019-01-23 11:13
    Upgrade status               : success
    Cancellation status          : -
    Software download time       : -
    Software download progress(%): -
    Software download speed(KB/s): -
    Patch download time          : -
    Patch download progress(%)   : -
    Patch download speed(KB/s)   : -
    Last upgrade time            : 2019-01-23 11:13
    Last upgrade result          : success

Local information:
    Device name                  : S5732-H24UM2CC
    ESN                          : 2102351XFR1*********
    Software version             : V200R020C00
    Patch version                : V200R020SPH

Schedule Upgrade Information:
    Download time                : 2020-2-13 20:01:24
    Download triggered           : yes
    Download pre-check result    : succeeded
    Reboot time                  : 2020-2-13 20:01:24
    Reboot triggered             : yes
    Reboot triggered result      : failed
<HUAWEI> display smart-upgrade information
Info: Loading the information, please wait .

Configuration:
    URL                          : s.houp.huawei.com
    HTTPS port                   : 443
    Bind SSL policy              : houp
    Verify HTTPS server          : true
Version information:
    Refresh time                 : 2020-07-23 12:24:06
    Check version result         : needUpdate
    Recommended software version : V200R023C00
    Recommended patch version    : -
    Upgrade description          : -
    Firmware and Patch Description in English: -

    Software package name        : AirEngineX760_V200R023C00.bin
    Software package size(B)     : 120101636
    Patch package name           : xxx.pat
    Patch package size(B)        : 14910

Upgrade information:
    Upgrade Time                 : 2020-01-23 11:13
    Upgrade status               : success
    Cancellation status          : -
    Software download time       : -
    Software download progress(%): -
    Software download speed(KB/s): -
    Patch download time          : -
```

```
    Patch download progress(%)   : -
    Patch download speed(KB/s)   : -
    Last upgrade time            : 2020-01-23 11:13
    Last upgrade result          : success

Local information:
    Device name                  : AirEngine 8760-X1-PRO
    ESN                          : 2102351XFR1*********
    Software version             : V200R019C10
    Patch version                : -

AP information:
    Device Type                  : AirEngine 8760-X1-
PRO

Schedule Upgrade Information:
    Download time                : -
    Download triggered           : no
    Download pre-check result    : -
    Reboot time                  : -
    Reboot triggered             : no
    Reboot triggered result      : -
```

Table 2-63 Description of the **display smart-upgrade information** command output

Item	Description
Configuration	Configuration information.
URL	Configured proxy server.
HTTPS port	HTTPS port number of the proxy server. The default port number is 443.
Bind SSL policy	Name of the bound SSL policy.
Verify HTTPS server	Whether to verify the HTTPS server. ● true: The HTTPS server is verified. ● false: The HTTPS server is not verified.
Version information	Version information.
Refresh time	Time when version information is obtained. Each time the command is run, the time is updated.
Check version result	Version check result. ● needUpdate: An upgrade is required. ● netError: The network is unavailable. ● versionOptimal: The version is optimal.
Recommended software version	Recommended software package version.
Recommended patch version	Recommended patch version.
Upgrade description	Upgrade description.

Item	Description
Firmware and Patch Description in English	Hardware and patch description in English.
Software package name	Software package name.
Software package size(B)	Software package size.
Patch package name	Patch package name.
Patch package size(B)	Patch package size.
Upgrade information	Upgrade information.
Upgrade Time	Upgrade time.
Upgrade status	Upgrade status: ● success: The upgrade succeeds. ● running: The upgrade is ongoing. ● netError: Network error. ● serverSpecUpLimit: The server specification reached the upper limit of the connection. ● CertOutDate: The certificate has expired. ● writeFlashFailed: The system file fails to be saved in the flash memory. ● fileCheckFailed: The file verification fails. ● upgradeCancelled: The upgrade is canceled. ● abnormalReset: The switch is restarted or an active/standby switchover is performed during an upgrade. ● fileNotMatch: The file does not match. ● systemError: System error. ● other: Other status.
Cancellation status	Upgrade cancellation status: ● Initial: The initialization is generally performed when the loading starts. ● Cancelling: The upgrade is being canceled. ● Successful: The upgrade is successfully canceled. ● Failed: The upgrade fails to be canceled.

Item	Description
Software download time	Time when the software package is downloaded to a device.
Software download progress(%)	Software package download progress, in percentage.
Software download speed(KB/s)	Software package download rate.
Patch download time	Time when a patch is downloaded to a device.
Patch download progress(%)	Patch download progress, in percentage.
Patch download speed(KB/s)	Patch download rate.
Last upgrade time	Last upgrade time.
Last upgrade result	Last upgrade result.
Local information	Local device information.
Device name	Device name.
ESN	Device ESN.
Software version	Software version.
Patch version	Patch version.
AP information	AP information.
Device Type	AP type.
Schedule Upgrade Information	Scheduled upgrade information.
Download time	Scheduled time when system files will be downloaded.
Download triggered	Whether system file download is triggered: ● yes: System file download is triggered. ● no: System file download is not triggered.
Download pre-check result	Result of the device status pre-check before system files are downloaded: ● failed: The check fails. ● succeeded: The check is successful.
Reboot time	Scheduled time for a reboot following an upgrade.

Item	Description
Reboot triggered	Check whether the reboot following an upgrade is triggered. ● yes: The reboot following an upgrade is triggered. ● no: The reboot following an upgrade is not triggered.
Reboot triggered result	Result of the device status pre-check before a restart is performed: ● failed: The check fails. ● succeeded: The check is successful.

2.9.3 smart-upgrade { url | https-port }

Function

The **smart-upgrade** { **url** | **https-port** } command configures the URL and HTTPS port number of a proxy server.

The **undo smart-upgrade** { **url** | **https-port** } command cancels the configured URL and HTTPS port number of a proxy server.

By default, the URL and HTTPS port number of a proxy server for connecting to a device are s.houp.huawei.com and 443, respectively.

Format

smart-upgrade { **url** *host* | **https-port** *https-port* }

undo smart-upgrade { **url** | **https-port** }

Parameters

Parameter	Description	Value
host	Specifies the URL or IP address of a proxy server.	The value is a string of 1 to 127 characters.
https-port	Specifies the HTTPS port number of a proxy server.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a device resides on an intranet, it cannot directly access the HOUP (s.houp.huawei.com). You can run this command to configure the URL and HTTPS port number of a proxy server, so that the device can access public networks through the proxy server.

When the device resides on a public network, it cannot directly access the HOUP (s.houp.huawei.com). You can run this command to configure s.houp.huawei.cn as the URL for connecting to the public network.

Example

Configure the URL and HTTPS port number of a proxy server.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade url 10.10.10.20
[HUAWEI] smart-upgrade https-port 10020
```

2.9.4 smart-upgrade download

Function

The **smart-upgrade download** command configures a smart upgrade-enabled switch to download the system file from the HOUP.

Format

smart-upgrade download

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the smart upgrade status of the switch or AP is displayed as **needUpdate**, you can run the **smart-upgrade download** command to configure the switch or AP to download the system file first and then run the **smart-upgrade right-now** command at the right time to implement smart upgrade.

Precautions

Resumable download is supported during system file download for smart upgrade. If the system file fails to be downloaded due to a network exception, run the **smart-upgrade download** command to enable the switch to start downloading the system file from the breakpoint.

During the smart upgrade of an AP, if the upgrade file version of the AP does not match the software version of the switch, the system displays an error message.

Example

Configure a smart upgrade-enabled switch to download the system file from the HOUP.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade download
Info: Getting version information from houp, please wait ...
Info: If you want to stop the download, please press CTRL + C.
Info: Downloading file basic-soft.cc ...
Info: Current percent is 100%.
Info: 83148260 byte(s) received in 160.618 second(s) 505.54 Kbyte(s)/sec.
Info: Downloading file basic-soft.cc.asc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file content is inconsistent with houp, delete and re-download...
Info: Current percent is 100%.
Info: 490 byte(s) received in 0.228 second(s) 2.10 Kbyte(s)/sec.
Info: Start verifying signature ...
Info: Signature verification passed.
Info: Start set next startup file, please wait...
Info: Set next startup file basic-soft.cc successfully.
```

2.9.5 smart-upgrade enable

Function

The **smart-upgrade enable** command enables smart upgrade.

The **undo smart-upgrade enable** command disables smart upgrade.

By default, smart upgrade is disabled on a switch.

Format

smart-upgrade enable

undo smart-upgrade enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After the **smart-upgrade enable** command is run on a switch, the switch queries the latest version information from the HOUP every 24 hours.

Prerequisites

An SSL policy has been bound to smart upgrade using the **smart-upgrade ssl-policy** command.

Follow-up Task

After smart upgrade is enabled, perform the following operations according to the actual situation:

- Run the **display smart-upgrade information** command to check details about smart upgrade.
- Run the **smart-upgrade download** command to configure the switch to download the system file from the HOUP.
- Run the **smart-upgrade right-now** command to perform a smart upgrade immediately.

Example

Enable smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade enable
```

2.9.6 smart-upgrade ap enable

Function

The **smart-upgrade ap enable** command enables smart upgrade for APs.

The **undo smart-upgrade ap enable** command disables smart upgrade for APs.

By default, smart upgrade is disabled for APs.

NOTE

This command is supported only on the following models:

S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H

Format

smart-upgrade ap enable

undo smart-upgrade ap enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To upgrade APs to the latest version more conveniently, you can deploy the smart upgrade function to implement one-click upgrade. After the **smart-upgrade ap enable** command is run to enable smart upgrade for APs, the switch queries the latest version information from the HOUP every 24 hours.

Prerequisites

Smart upgrade has been enabled using the **smart-upgrade enable** command.

Follow-up Task

After the smart upgrade function is enabled for APs, perform the following operations as required:

- Run the **smart-upgrade download** command to download system files.
- Run the **smart-upgrade right-now** command to perform a smart upgrade immediately.
- Run the **display smart-upgrade information** command to check details about smart upgrade.

Example

Enable smart upgrade for APs.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade ap enable
```

2.9.7 smart-upgrade right-now

Function

The **smart-upgrade right-now** command performs smart upgrade on a switch immediately.

Format

smart-upgrade right-now

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the smart upgrade status of a switch is displayed as **needUpdate**, you can run the **smart-upgrade right-now** to implement loading of and upgrade to a new software version in one-click mode.

Before this command is run, you can also run the **smart-upgrade download** command to configure the switch to download the system file from the HOUP first and then run the **smart-upgrade right-now** command at the right time to implement smart upgrade. The wait time in this method is shorter than that when the **smart-upgrade right-now** command is run.

Precautions

Switches cannot be added to or removed from a stack during smart upgrade.

Resumable download is supported during system file download for smart upgrade. If the download is interrupted due to a network exception, run the **smart-upgrade right-now** command to enable the switch to continue the download from the breakpoint.

During the smart upgrade of an AP, if the upgrade file version of the AP does not match the software version of the switch, the system displays an error message.

Example

Perform smart upgrade on a switch immediately.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade right-now
Info: Getting version information from houp, please wait ...
Info: If you want to stop the upgrade, please press CTRL + C.
Info: Downloading file basic-soft.cc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: Resume from the 15728640 bytes breakpoint.
Info: Current percent is 100%.
Info: 104372996 byte(s) received in 197.329 second(s) 516.53 Kbyte(s)/sec.
Info: Downloading file basic-soft.cc.asc ...
Info: Current percent is 100%.
Info: 490 byte(s) received in 0.201 second(s) 2.38 Kbyte(s)/sec.
Info: Downloading file basic-patch.pat ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
Info: Downloading file basic-patch.pat.asc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
```

```
Info: Start verifying signature ...
Info: Signature verification passed.
Info: Set next startup patch basic-patch.pat successfully.
Info: Start set next startup file, please wait...
Info: Set next startup file basic-soft.cc successfully.
Info: System will rebooting for upgrade...
```

2.9.8 smart-upgrade ssl-policy

Function

The **smart-upgrade ssl-policy** command binds an SSL policy to smart upgrade.

The **undo smart-upgrade ssl-policy** command unbinds an SSL policy from smart upgrade.

By default, no SSL policy is bound to smart upgrade.

Format

smart-upgrade ssl-policy *policy-name*

undo smart-upgrade ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

Because a switch where smart upgrade is to be enabled is connected to the HOUP using HTTPS, an SSL policy must be bound to smart upgrade for the switch to establish HTTPS connection with the HOUP before smart upgrade is enabled on the switch.

Example

Bind an SSL policy named **houp** to smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade ssl-policy houp
```

2.9.9 smart-upgrade schedule

Function

The **smart-upgrade schedule** command configures the scheduled smart upgrade function on a switch.

The **undo smart-upgrade schedule** command disables the scheduled smart upgrade function on a switch.

By default, the scheduled smart upgrade function is disabled on a switch.

Format

smart-upgrade schedule download at *download-time* [**reboot at** *reboot-time*]

undo smart-upgrade schedule

Parameters

Parameter	Description	Value
download at *download-time*	Specifies the time when a switch downloads system files.	The format is YYYY-MM-DD HH:MM:SS. ● YYYY indicates the year. The value is an integer in the range from 2000 to 2099. ● MM indicates the month. The value is an integer in the range from 1 to 12. ● DD indicates the day. The value is an integer in the range from 1 to 31. ● HH specifies the hour. The value is an integer in the range from 0 to 23. ● MM indicates the minute. The value is an integer in the range from 0 to 59. ● SS indicates the second. The value is an integer in the range from 0 to 59. **NOTE** The time when a switch downloads system files must be later than the current time of the switch.

Parameter	Description	Value
reboot at *reboot-time*	Specifies the time when a switch restarts after an upgrade.	The format is YYYY-MM-DD HH:MM:SS. ● YYYY indicates the year. The value is an integer in the range from 2000 to 2099. ● MM indicates the month. The value is an integer in the range from 1 to 12. ● DD indicates the day. The value is an integer in the range from 1 to 31. ● HH specifies the hour. The value is an integer in the range from 0 to 23. ● MM indicates the minute. The value is an integer in the range from 0 to 59. ● SS indicates the second. The value is an integer in the range from 0 to 59. **NOTE** ● The time when a switch restarts after an upgrade must be later than the time when the switch downloads system files. ● If you do not specify the time when a switch restarts after an upgrade, the switch only downloads system files. In this case, you need to manually restart the switch to complete the upgrade.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a switch requires a smart upgrade, you can run the **smart-upgrade schedule** command on the switch to configure it to perform a smart upgrade at an off-peak time. This configuration will prevent the upgrade from affecting services running on the switch.

Precautions

- This command takes effect only for smart upgrade of switches instead of APs.
- During a scheduled smart upgrade, if the switch fails to download system files at the scheduled time due to network problems, the switch attempts to download system files again when the scheduled restart time arrives. If the upgrade still fails, the scheduled smart upgrade fails.
- The following operations will disable the scheduled smart upgrade function:

  - Resets a switch.
  - Run the **undo smart-upgrade enable** command to disable smart upgrade.
  - Run the **smart-upgrade download** command to download system files.
  - Run the **smart-upgrade right-now** command to perform a smart upgrade immediately.
  - Download system files immediately through the web system.
  - Perform a smart upgrade immediately through the web system.

Example

Configure the scheduled smart upgrade function.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade schedule download at 2020-12-01 00:00:00
```

2.9.10 smart-upgrade verify-server disable

Function

The **smart-upgrade verify-server disable** command disables the server certificate verification function before a switch is connected to a proxy server for smart upgrade.

The **undo smart-upgrade verify-server disable** command enables the server certificate verification function before a switch is connected to a proxy server for smart upgrade.

By default, the server certificate verification function is enabled before a switch is connected to a proxy server for smart upgrade.

Format

smart-upgrade verify-server disable

undo smart-upgrade verify-server disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When the certificate for smart upgrade is invalid or no certificate for smart upgrade is available, you can run the **smart-upgrade verify-server disable** command to temporarily disable the certificate verification function.

Although the certificate verification function is manually disabled, an SSL policy still needs to be bound to smart upgrade. Therefore, after the certificate verification function is disabled, run the **ssl policy** *policy-name* command to create an empty SSL policy and run the **smart-upgrade ssl-policy** command to bind the SSL policy to smart upgrade.

Example

Disable the function of verifying the HTTPS certificate of the server.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade verify-server disable
```

2.9.11 smart-upgrade web-prompt disable

Function

The **smart-upgrade web-prompt disable** command disables web prompt for smart upgrade.

The **undo smart-upgrade web-prompt disable** command enables web prompt for smart upgrade.

By default, web prompt for smart upgrade is enabled.

Format

smart-upgrade web-prompt disable

undo smart-upgrade web-prompt disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, when smart upgrade is disabled on a switch, the web system prompts the user that this function is disabled. After smart upgrade is enabled on the switch and a new software version is available, the web system prompts the user to upgrade the switch to the new version. If such information is not required, you can run this command to disable web prompt for smart upgrade.

Example

Disable web prompt for smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade web-prompt disable
```

2.10 Upgrade Commands

2.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.10.2 check startup

Function

The **check startup** command checks the correctness of various resource files, including the PAF file, the patch package, the startup software, and the configuration file.

Format

check startup [**crc**] [**next**]

Parameters

Parameter	Description	Value
crc	Performs a CRC check on various resource files.	-
next	Checks various resource files used for next startup.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

After configuring the resource files for next startup, you can run this command to check whether the resource files are complete and whether the formats and versions of the resource files are correct.

Example

Check the correctness of the resource files.

```
<HUAWEI> check startup
Main board:
Check startup software.......ok
Check configuration file.....ok
Check PAF....................ok
Check Patch..................ok
PAF is fitted with startup software
Info: Slave board is not existing.
```

Performs a CRC check on various resource files.

```
<HUAWEI> check startup crc
Warning: This operation will take several minutes! Continue?[Y/N]:y
Check startup software CRC..................................................
ok
Info: Slave board is not existing.
```

2.10.3 display device group-speed license-usage

Function

The **display device group-speed license-usage** command displays the usage of license control items.

NOTE

This command takes effect only on the following devices that have license control items loaded:

S5732-H24UM2CC, S5732-H48UM2CC, and S5736-S24UM4XC

Format

display device group-speed license-usage

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the usage of license control items, run the **display device group-speed license-usage** command.

For details about license control items, see **License Control Items**.

Example

Display the usage of license control items.

```
<HUAWEI> display device group-speed license-usage
Slot LicenseItem      ResourceCount ResourceUsed
-----------------------------------------------
 0   1G->2.5G         4             0
     1G->5G           4             0
     1G->10G          4             3
     2.5G->5G         1             0
     2.5G->10G        1             0
     5G->10G          1             0
```

Table 2-64 Description of the **display device group-speed license-usage** command output

Item	Description
Slot	Slot ID.
LicenseItem	Control item name.
ResourceCount	Number of control Items.
ResourceUsed	Number of used control items.

2.10.4 display last startup information

Function

The **display last startup information** command displays the version of the system software used for the last startup.

Format

display last startup information slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the version of the system software used for the last startup in the MPU slot.	The value must be set according to the device configuration.

Views

All view

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display last startup information** command to check the version of the system software used for the last startup.

Precautions

- If the device is upgraded from V200R020C10SPC100 or an earlier version to V200R020C10SPC500 or a later version, because the source version does not support this command, the system displays a message "Info: The file that records information about the last startup system software is empty." after this command is executed.
- If the device version is V200R020C10SPC500 or later and the system software remains unchanged, the system displays a message "Info: The file that records information about the last startup system software is empty." after this command is executed.

Example

Display the version of the system software used for the last startup.

```
<HUAWEI> system-view
[HUAWEI] display last startup information slot 0
Startup system software : flash:/basicsoft.cc
Software version        : V200R021C01SPC100B236
Software compile time   : Oct 30 2021, 19:32:02
```

2.10.5 display license

Function

The **display license** command displays information about the license file in the system.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license [*file-name* | **verbose**]

Parameters

Parameter	Description	Value
file-name	Displays summary information about the license file with a specified file name. *file-name* supports file name association. The disk where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 case-insensitive characters without spaces.
verbose	Displays detailed information about the current active license file.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A license file dynamically controls the availability of some features. Only one license file is active in the system. Run this command to view detailed information about the active license in the system, including license file name, version, validity period, and control item. Based on the information, you can determine whether to upgrade the system version to support more features.

Precautions

The license of an N1 software package is activated on iMaster NCE-Campus. Therefore, you cannot view the license control items of the N1 software package by running this command on the device.

On the S5732-H24UM2CC, S5732-H48UM2CC, and S5736-S24UM4XC, if these devices set up a stack and the master and non-master devices have inconsistent license control items, run the **display device group-speed license-usage** command to check the usage of license control items in the stack.

Example

Display information about the active license file of the device.

```
<HUAWEI> display license
 Active license     : flash:/LICORTF163673-554BEF51E8.dat
```

```
License state     : Trial
Revoke ticket     : No ticket

RD of Huawei Technologies Co., Ltd.

Product name      : S5700
Product version   : V200R0012
License Serial No : LIC20210401UV9K50
Creator           : Huawei Technologies Co., Ltd.
Created Time      : 2021-04-01 21:22:06
Sns End Data      : 2021-07-01
Feature name      : EHFEA1
Authorize type    : DEMO
Expired date      : PERMANENT
Trial days        : 60

Item name          Item type  Value    Description
-------------------------------------------------------------
ES5SF4512K00       Resource   2        FIB512K
ES5SF4128K00       Resource   6        FIB128K
ES5SWL16AP00       Resource   64       WL16AP
ES5SWL64AP00       Resource   16       WL64AP
ES5SWL128AP0       Resource   8        WL128AP
ES5SWL512AP0       Resource   2        WL512AP

 Master board license state: Trial. The trial days remains 60 days. Apply for authentic license before the
current license expires.
```

Table 2-65 Description of the **display license** command output

Item	Description
Active license	Name and path of the active license file.

Item	Description
License state	Status of a license file: - Normal This state value indicates that a license file is working properly. If the status of the license file on the live network is not **Normal**, check the license file. - Trial – A license file enters the Trial state if the ESN does not match the device. A license file in Trial state can be used only for 60 days. To continue to use a license file after the Trial state, apply for a new license file using the correct ESN. – A temporary license file expires and enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file and activate it. – A license file is revoked and enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file based on the revocation code and activate it. - Demo When you activate a temporary license file, it enters the Demo state. The Demo state exists only for a demo license file used for test and deployment. A license file in Demo state allows you to use normal functions within a specified period. Before the expiration of the license file in Demo state, replace it with a commercial license file. - Emergency In emergency conditions like earthquakes, volcano explosions, and tsunamis, run the **license emergency** command to trigger a license file to enter the emergency

Item	Description
	state. The emergency state stays for seven days, and a license file can enter the emergency state three times. - Default: No license file is activated or a license file expires. If a license file enters the Default state, services will be interrupted. If you want to use services after a license file expires or becomes invalid, apply for a new license file and activate it.
Revoke ticket	License revocation code. **no ticket** indicates that the license is permanently valid.
Product name	Name of the product that runs the license.
Product version	Product version.
License Serial No	Serial number of the license file.
Creator	Creator of the file.
Created Time	Time when the file was created.
Sns End Data	SnS end date in the N1 business model. Only the following models support this field: - S5700 series: S300, S500, S5720-LI, S5720-SI, S5720-HI, S5720-EI, S5720I-SI, S5730-SI, S5730-HI, S5731-S, S5731-H, , S5732-H, S5735-L, S5735-L-I, S5735-L1, S5735-S, S5735-S-I, S5736-S - S6700 series: S6720-LI, S6720-SI, S6735-S, S6720-EI, S6720-HI, S6730-S, S6730-H,
Feature name	Feature name.
Authorize type	Authorization type. - demo: trial authorization. - comm: commercial authorization.

Item	Description
Expired date	License expiration date. **PERMANENT** indicates that the license is permanently valid. A license file enters the trial period after it expires. This does not affect services. When the trial period expires, a license file will be invalid. The services and functions under its control revert to the default values. **NOTE** You need to apply for a new license file and activate it during the trial period. After activation, the new license file replaces the one in the trial period automatically.
Trial days	Trial period of an expired license. - For a license file in the trail state, the trial period is 60 days. The value of this field is displayed as 60. - For a license file that is not in the trail state, this field is meaningless, and its value is displayed as **--**.
Item name	Name of a control item.
Item type	Type of a control item. - Function: function items controlled by a license file - Resource: resource items controlled by a license file
Value	Value of a control item. - When **Item type** displays **Function**, **Value** displays **Yes**, indicating that this function is enabled. - When **Item type** displays **Resource**, **Value** displays a specified value, indicating the maximum number of this resource item. **NOTE** This parameter is displayed in the **display license** command output.
Control value	Values supported by a control item. **NOTE** This parameter is displayed in the **display license verbose** command output.

Item	Description
Used value	Actual used value. **NOTE** This parameter is displayed in the **display license verbose** command output.
Description	Description of a control item.

2.10.6 display license esn

Function

The **display license esn** command displays the equipment serial number (ESN) used for applying a license.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license esn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you need to use licensed resource items or function items, apply for a license file. When applying for a license, you need to provide the device ESN.

ESN is the only identifier of device components, run the **display license esn** command to display the ESN of the current device, and then use the ESN to apply a license file for the device.

The ESN of the chassis must be the same as the ESN in the license to be activated. If they are different, the license file cannot be activated.

Example

Display the ESN used for applying a license.

```
<HUAWEI> display license esn
```

```
ESN: 2102113090P0xxxxxxxx
```

Table 2-66 Description of the **display license esn** command output

Item	Description
ESN	ESN of the device.

2.10.7 display license information

Function

The **display license information** command displays license information about the master, standby, and slave switches in a stack system.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

- If the control items of the license files on the standby/slave and master switches are the same, the standby/slave switch uses its own license file and does not synchronize the license file of the master switch. You can run the **display license** command to check the license control items. An active/standby switchover has no impact on the license files loaded on the master, standby, and slave switches.
- If the control items of the license files on the standby/slave and master switches are different, the standby/slave switch synchronizes the license file of the master switch. The ESN in the synchronized license file will differ from the standby/slave switch's ESN. If so, the license changes to the Trial state and enters the trial period. After an active/standby switchover, the license on the new master switch enters the trial period. You can run the **display license**

information command on the master switch to check whether the switch's ESN is the same as the ESN in the license file.

Precautions

The **display license** command displays license information about the master switch only, whereas the **display license information** command displays license information about the master, standby, and slave switches in the stack system.

If a switch is not in a stack system, the **display license information** command displays license information about the switch only. If a stack system contains the master, standby, and slave switches, the **display license information** command displays license information about the master, standby, and slave switches.

Follow-up Procedure

If the ESN of the standby/slave switch differs from the ESN in the synchronized license file, the license enters the trial period. Apply for a new license file before the trial period expires according to the following process.

1. Run the **license revoke** command on the master switch to obtain the revocation code of the license file on the switch.
2. Run the **display esn** command on the master switch to collect ESNs of the master, standby, and slave switches.
3. Log in to license application website, and use the revocation code and ESNs of the master, standby, and slave switches to apply for a new license file for the stack system.
4. Run the **license active** *license-name* command on the master switch to activate the new license file.

Example

Display license information about the master, standby, and slave switches in a stack system.

```
<HUAWEI> display license information

Slot 0:
Current license file          : flash:/s5720-hi_slot0_full.datSynchronize from master board  : NO
Current license file esn       : 210235859810xxxxxxxx
Current slot esn              : 210235859810xxxxxxxx
License esn match with device  : YES

Slot 1:
Current license file          : flash:/s5720-hi_slot2_full.dat
Synchronize from master board  : YES
Current license file esn       : 210235859810xxxxxxxx
Current slot esn              : 210235859810xxxxxxxx
License esn match with device  : NO

Slot 2:
Current license file          : flash:/s5720-hi_slot2_full.dat
Synchronize from master board  : YES
Current license file esn       : 210235859810xxxxxxxx
Current slot esn              : 210235859810xxxxxxxx
License esn match with device  : YES
```

Table 2-67 Description of the **display license information** command output

Item	Description
Slot	Slot ID.
Current license file	Current license file.
Synchronize from master board	Whether the license file is synchronized from the master switch. For the master switch, the value is YES.
Current license file esn	ESN in the current license file.
Current slot esn	ESN of the switch.
License esn match with device	Whether the ESN in the license file matches the switch's ESN.

2.10.8 display license resource usage

Function

The **display license resource usage** command displays the usage of the resource items defined in a license file.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license resource usage

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display license resource usage** command to check the usage of the resource items defined in the license file, including the number of remaining licenses and the resource usage.

Resource usage refers to the percentage of resources used out of resources defined by the license file. For details about license control items, see **License Control Items**.

Example

Display the usage of licensed resources.

```
<HUAWEI> display license resource usage
Info: Active License on master board: flash:/LICORTF163673-554BEF51E8.dat
 FeatureName     | ConfigureItemName       | ResourceUsage

 ES5FEA1          ES5SF4512K00             0/2
 ES5FEA1          ES5SF4128K00             0/6
 ES5FEA1          ES5SWL16AP00              0/64
 ES5FEA1          ES5SWL64AP00              0/16
 ES5FEA1          ES5SWL128AP0              0/8
 ES5FEA1          ES5SWL512AP0              0/2
```

Table 2-68 Description of the display license resource usage command output

Item	Description
Active License on master board	File name and path of an active license name.
FeatureName	Name of the feature controlled by the license.
ConfigureItemName	Name of a control item.
ResourceUsage	Percentage of used resources.

2.10.9 display license revoke-ticket

Function

The **display license revoke-ticket** command displays the revocation code of the current license file of the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license revoke-ticket

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display license revoke-ticket** command enables you to check the revocation code of a license file that has become invalid on the device. This code proves that the current license file is invalid and is used to apply for a new license.

Precautions

This command displays information only when the license file in current device system is invalid. Otherwise, no command output is displayed.

Example

Display the revocation code of the current invalid license file.

```
<HUAWEI> display license revoke-ticket
 Info: The revoke ticket is: LIC20091103006100:27C1B773ED11D9F877855CDAEE74ABFE60E07126.
```

2.10.10 display license state

Function

The **display license state** command displays the license status on the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the status of the running license, run this command. The command displays the current status of the license and the number of days before the license in this status will expire.

The system supports the following license states:

- Normal: normal license
- Demo: demonstration license
- Trial: trial license that has expired but is still valid during the trial period
- Emergency: emergency license
- Default: default license

This command helps you locate license problems and verify the license status on the device.

Prerequisites

A license file has been stored on the main control board of the device and has been activated. This ensures that valid entries are displayed after the execution of the command. If the license file is not activated, no command output is displayed.

Example

Display the status of the license on the device.

```
<HUAWEI> display license state
Info: Current license state is Trial. 60 days remain.
```

2.10.11 display module-information

Function

The **display module-information** command displays information about dynamically uploaded modules.

Format

display module-information [**verbose** | **next-startup**]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about dynamically uploaded modules.	-
next-startup	Displays information about the module packages to be uploaded at the next startup.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After modules are uploaded, you can run the **display module-information** command to check information about these modules.

Example

Display information about dynamically uploaded modules.

```
<HUAWEI> display module-information

                        Module Information
------------------------------------------------------------------------
Module     Version   InstallTime                   PackageName
------------------------------------------------------------------------
MACSEC     SPH       2011-01-16 16:39:18+00:00     s5720hi.mod

Total = 1
```

Display detailed information about dynamically uploaded modules.

```
<HUAWEI> display module-information verbose

                        Module Information
------------------------------------------------------------------------
Module     Version   InstallTime                   PackageName
------------------------------------------------------------------------
MACSEC     SPH       2011-01-16 16:39:18+00:00     s5720hi.mod

Total = 1
Board Info:

------------------------------------------------------------------------
Slot       Module         State     Count Time(YYYY-MM-DD HH:MM:SS)
------------------------------------------------------------------------
0          MACSEC         Using     1     2011-01-16 16:39:17+00:00

Total = 1
```

Table 2-69 Description of the **display module-information** command output

Item	Description
Module Information	Module information.
Module	Name of a dynamically uploaded module.
Version	Module package version.
PackageName	Module package name.
InstallTime	Time when the module package was uploaded to the memory.
Total	The **Total** field under **Module Information** displays the number of module packages that take effect. The **Total** field under **Board Info** displays the number of boards that have modules installed.

Item	Description
Board Info	Board information.
Slot	Slot ID of the board where a module resides.
State	Status of the module.
Count	Number of modules that take effect on the board.
Time(YYYY-MM-DD HH:MM:SS)	Time when the module took effect, that is, time when the current module was loaded to the current state.

Display information about the next startup modules configured in the system.

```
<HUAWEI> display module-information next-startup
Info: The result will be shown in several minutes. Please wait for a moment......

                   Next startup module packages
Total = 1
------------------------------------------------------------------------
No.  PackageName
------------------------------------------------------------------------
1    flash:/$_install_mod/s5720hi.mod
```

Table 2-70 Description of the **display module-information next-startup** command output

Item	Description
Next startup module packages	Information about module packages to be installed at the next startup.
Total	Number of module packages to be installed at the next startup.
No.	Sequence number of a module package to be installed at the next startup.
PackageName	Name of a module package to be installed at the next startup.

2.10.12 display paf

Function

The **display paf** command displays information about the product adaptive file (PAF) in the system.

Format

display paf { **all** | { **resource** | **service** } *item-name* }

Parameters

Parameter	Description	Value
all	Displays all information about the PAF file.	-
resource	Specifies the value set for a resource item in the PAF file.	-
service	Specifies the value set for a service item in the PAF file.	-
item-name	Specifies the name of a resource item or a service item.	The value is a string of 1 to 64 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

A PAF file provides only required resources and features. This command can display all the specification information about the PAF file.

Example

Display the value set for a resource item in the PAF file.

```
<HUAWEI> display paf resource PAF_LCS_NQA_SPECS_NUM_ENTRY
 PAF_LCS_NQA_SPECS_NUM_ENTRY = 1, 32, 32, 0
```

Display the value set for a service item in the PAF file.

```
<HUAWEI> display paf service PAF_LCS_IPV6_BASE_SPECS_ENABLED
 PAF_LCS_IPV6_BASE_SPECS_ENABLED = 1, 1
```

Table 2-71 Description of the display paf resource command output

Item	Description
PAF_LCS_NQA_SPECS_NUM_ENTRY	Resource item name in the PAF file.
1	Whether a resource item is controlled by a license. ● 1: yes ● 0: no

Item	Description
32	Default value of the resource item in the PAF file.
32	Maximum value of the resource item in the PAF file.
0	Minimum value of the resource item in the PAF file.

Table 2-72 Description of the display paf service command output

Item	Description
PAF_LCS_IPV6_BASE_SPECS_ENABLED	Service item name in the PAF file.
1	Whether a service item is controlled by a license. ● 1: yes ● 0: no
1	Service status. ● 1: enabled ● 0: disabled

2.10.13 display patch-information

Function

The **display patch-information** command displays information about the patch in the current system.

Format

display patch-information [**history**]

Parameters

Parameter	Description	Value
history	Displays historical information about the patch in the current system.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After a patch is loaded or deleted, run this command to view information about the patch, including its version, name, and status.

Example

Display current information about the patch in the system.

```
<HUAWEI> display patch-information
Patch Package Name   :flash:/patch_pack.pat
Patch Package Version:V200R013SPH
The state of the patch state file is: Running
The current state is: Running

****************************************************************************
*           Information about hot patch errors is as follows:          *
****************************************************************************

    Slot            CurrentVersion
------------------------------------------------------------

No hot patch error occurs on any board.


****************************************************************************
*                The hot patch information, as follows:              *
****************************************************************************

 Slot       Type           State     Count Time(YYYY-MM-DD HH:MM:SS)
------------------------------------------------------------------------
 3          C              Running   1     2018-12-03 18:34:25+00:00
 4          C              Running   1     2018-12-04 09:51:43+00:00


****************************************************************************
*              The Kernel patch information, as follows:              *
****************************************************************************

    Slot           Type          State         Count
------------------------------------------------------------
    3              Kernel        Running       1
    4              Kernel        Running       1


****************************************************************************
*              The firmware patch information, as follows:           *
****************************************************************************

    Slot           Type          State         Count
------------------------------------------------------------
    4              BOOTLOAD      Running       1
```

Display historical information about the patch in the system.

```
<HUAWEI> display patch-information history
****************************************************************************
*                The patch command history, as follows:              *
****************************************************************************

 time(Y.M.D/HH:MM:SS)   state        size     patch-package name
 -----------------------------------------------------------------------
```

```
2014.01.29/14:07:39  Startup       827318      patch_all_pack.pat
2014.10.13/11:33:12  Running         8404      patch_all_pack1.pat
2014.10.13/10:48:36     Idle       827318      patch_all_pack2.pat
```

Table 2-73 Description of the display patch-information command output

Item	Description
Patch Package Name	Name of the patch file.
Patch Package Version	Version of the patch.
The state of the patch state file is	Status of the patch file.
The current state is	Current status of the patch.
Slot	Slot ID.
Type	Patch type. ● C: single-core patch. ● BOOTLOAD, CPLD, BOOTROOM, KERNEL, DTB, OSPKG, RAMDISK, FPGA, MCU_POE, or SUBCARD_CPLD: indicates a firmware patch. ● SEFU: multi-core patch type. ● ENP: indicates an ENP patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.) ● Kernel: indicates a kernel patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.) ● BIN: indicates a process patch. ● C-WMP: multi-core WMP patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.) ● C-NAC: multi-core NAC patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.)

Item	Description
State	Running status of the patch. ● Deactive ● Active ● Running ● Idle: no patch in the system ● Startup: indicates the Startup state after the patch to be loaded at the next startup is set. If the next state change is recorded, the current Startup state is overwritten.
Count	Number of patch units. For kernel patches, the number of kernel patches in **Active** and **Running** states is displayed.
Time(YYYY-MM-DD HH:MM:SS)	Time when the patch takes effect.
size	Size of the patch.

2.10.14 display rollback

Function

The **display rollback** { **information** \| **result** } command displays rollback information in the system.

Format

display rollback { **information** | **result** }

Parameters

Parameter	Description	Value
information	Displays version information after the system is rolled back.	-
result	Checks whether the rollback is successful.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If an error occurs during an upgrade and you need to cancel the upgrade, run the **rollback** command to roll back the system to the previous version.

- Before performing a rollback, you can run the **display rollback information** command to preview the version status after the rollback, including the system software, configuration file, and patch file used after the rollback, as well as the remaining time for the rollback function to take effect.
- After completing the rollback, you can run the **display rollback result** command to check whether the rollback is successful.

Example

Display rollback information in the system.

```
<HUAWEI> display rollback information
---------------------------------------------------------------------
MainBoard:
 Software package:        flash:/basicsoft.cc
 Configuration file:      flash:/vrpcfg201506011523.zip
 Patch file:              NULL
 Rollback remain time:    00:16:49
---------------------------------------------------------------------
```

Table 2-74 Description of the **display rollback information** command output

Item	Description
Software package	System software used after the rollback.
Configuration file	Configuration file used after the rollback. This configuration file is the backup configuration file automatically generated by the system after the upgrade. The file name is in the format of **filenameYYYYMMDDhhmm.zip**. • **filename**: indicates the name of the configuration file before the upgrade. • **YYYY**: indicates the year. • **MM**: indicates the month. • **DD**: indicates the day. • **hh**: indicates the hour. • **mm**: indicates the minute. If the file name is too long, the system automatically shortens the file name length to the required length.

Item	Description
Patch file	Patch file used after the rollback.
Rollback remain time	Remaining time for the rollback function to take effect.

Check whether the rollback is successful after the rollback is complete.

```
<HUAWEI> display rollback result
Rollback result: Success.
```

Table 2-75 Description of the **display rollback result** command output

Item	Description
Rollback result	Rollback result: • Success: The rollback is successful. • Fail: The rollback fails. If the rollback fails, the system displays specific rollback failure information: – Software rollback fail: The system software fails to be rolled back. – Configuration rollback fail: The configuration file fails to be rolled back. – Patch rollback fail: The patch file fails to be rolled back.

2.10.15 display virtual license

Function

The **display virtual license** command displays information about the virtual license file in the current system.

Format

display virtual license [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- Specifies the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The controller delivers a virtual license to perform management. You do not need to load the entity license for the switch. This facilitates the management and control of the functions related to the entity license.

You can run this command to check detailed information about the virtual license file in the current system, including the name of the virtual control item, status of the virtual license, and expiration date of the virtual license.

Example

Display information about the virtual license file on the device.

```
<HUAWEI> display virtual license

Slot 0
------------------------------------------------------------------------------
Item       Resource  License     Expired     Trial days  Item
Name         Value     Status     Date        Total       Description
------------------------------------------------------------------------------
VXLAN      1         Demo       2019-08-16  -           VXLAN Control Function
```

Table 2-76 Description of the **display virtual license** command output

Item	Description
Slot	- Specifies the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.

Item	Description
Item Name	Name of a control item in the virtual license. VXLAN: Control over the enhanced VXLAN functions. The enhanced VXLAN functions include the distributed VXLAN gateway function and the BGP EVPN function. **NOTE** The license does not control route exchange between devices, but controls the status of the dynamic VXLAN tunnel established using BGP EVPN. If no license is loaded or the license becomes invalid, the dynamic VXLAN tunnel cannot be established using BGP EVPN.
Resource Value	Resource value of the control item.
License Status	Status of the virtual license. ● Default: By default, no virtual license is installed on a device and the dynamic VXLAN tunnel is in Down status. ● Normal: The commercial virtual license is activated. The device status is changed to Normal after the controller delivers a commercial virtual license to the device. The status can be restored to Default only through online retrieving. ● Demo: The temporary virtual license is activated. The device status is changed to Demo after the controller delivers a temporary virtual license to the device. The status can be restored to Default through online retrieving, and trial keepalive. ● Trial: The license is in keepalive status, indicating that the device status is automatically changed to trial keepalive after the validity period for the device in Demo status expires. The keepalive period is 90 days. After the keepalive period expires, the status is restored to Default and the dynamic VXLAN tunnel is in Down status.
Expired Date	Expiration date of the virtual license.
Trial days Total	Total trial period of the virtual license.
Item Description	Description of a control item in the virtual license.

2.10.16 install-module

Function

The **install-module** command installs module packages.

By default, no module package is installed.

Format

install-module *file-name* [**next-startup**]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a module package to be installed. *file-name* supports file name association. The related file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 case-insensitive characters without spaces.
next-startup	Specifies the name of the module package to be installed during next startup.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Software upgrade is a common method to add new services on a network. This method, however, is complex and affects services. To solve these problems, you can run the **install-module** command to install the module package of a desired function, without upgrading or powering off your device.

- Run the **install-module** *file-name* command to load a module in the module package to the device. The module directly takes effect after being loaded. If the device is in a stack, the module is loaded to all the devices in the stack, including the master, standby, and slave switches.
- Run the **install-module** *file-name* **next-startup** command to add the module package to the next startup module list. The device automatically loads the module next time it starts. Before a module package is installed dynamically, the system checks the module package validity. In the next startup module list, one module can exist in only one module package.

Precautions

- The file name extension of the module package must be .MOD, and the file must be saved in the directory **$_install_mod** on the device.
- The module package version must match the current system software version. Otherwise, the module package will fail to be installed.

- The system allows you to install up to 16 modules.

Example

Load the module package s5720hi.mod.

```
<HUAWEI> install-module s5720hi.mod
Info: Installing the module flash:/$_install_mod/s5720hi.mod..
.
Info: Succeeded in installing the module on the master board....
```

Configure the module package to be loaded during next startup.

```
<HUAWEI> install-module s5720hi.mod next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....
...
Info: Succeeded in setting the next-startup module.
```

2.10.17 license active

Function

The **license active** command activates the license file saved in the storage of the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license active *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file. *file-name* supports file name association. The disk where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Change or upgrade the license file when the current license file is outdated or needs higher specifications and more features. The initial state of a license file is inactive and the license file does not take effect in the system. Run this command to activate the new or updated license file.

The **license active** command can be used to activate a license file in the following situations:

- The license needs to be activated for the first time.

  You can directly run this command to activate a license.
- The current license file needs to be updated.

  If the specifications of the new license file are lower than those of the current license file, the system displays a message asking you whether to continue. If you choose **No**, the system retains the current license file. If you choose **Yes**, the master switch activates the current license file and the system uses the new license file.

NOTICE

If the configuration items of the new license file are lower than those of the current license file, check whether the configuration items required by services exist in the new license file. If not, apply for a correct license file and activate it. Otherwise, services may be interrupted due to lack of dependent license configuration items after the board or the device is restarted.

Prerequisites

The new license file has been uploaded to the device.

Follow-up Procedure

When the system restarts, the system activates the license file that was activated last time to ensure the license files are the same before and after restart.

Precautions

- The license file must use .dat as file name extension and be saved to the default root directory in the storage of the device.
- If no path is specified, the license file in the working path is activated by default.
- If the specifications of the new license file are lower than those of the current license file (some functions are authorized in the current license file, but not

in the new license file, or the new license file allows fewer resources than the current one), the system displays a message asking you whether to continue.

- When the switch is stacked, if the ESN in the license file does not match the ESN of each stack member, activating the license file will prompt that the license file is abnormal. There is a risk that the license file will enter the grace period when the stack master changes.

Example

Activate **license.dat** in the storage of the device.

```
<HUAWEI> license active license.dat
```

Activate the license file **license.dat** in the storage of the stacked device.

```
<HUAWEI> license active license.dat
Verify license passed with minor errors:
    ESN is mismatched with node esn of slot 0.
    ESN is mismatched with node esn of slot 1.
Info: This operation maybe use the trial license instead of current licnese, may be reduce current resource or
functions. Continue?[Y/N]:y
Warning: The ESN in board is different from that in the license file, Update the license file in time.
Continue? [Y/N]y
Info: The license is being activated. Please wait for a moment.
```

2.10.18 license emergency

Function

The **license emergency** command enables the emergency state for the license.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license emergency

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system configuration is classified into maximum configuration, authorized configuration, and minimum configuration.

- In maximum configuration, the maximum number of dynamic resource items are configured. Static resource items and function items are configured according to license configuration.
- Authorization configuration means the functions and resources of the software configured on the basis of contract or special authorization. Authorized configuration depends on feature authorization of license files.
- The minimum configuration is the default configuration when no activated license file exists in the system. The minimum configuration varies according to products.

Configurations are classified to limit the bearer capability of the system in different running status.

When you run the **license emergency** command to enable the emergency state for the license, the system is free from license control. In this case, the system can run with the maximum configuration of dynamic resources and the license-defined configuration of static resources and functions. When the validity period of the emergency state expires, dynamic resources are controlled by the license again. One version is provided with three validity periods of emergency state, each lasting for seven days.

The purpose for enabling the emergency state for the GTL license is disaster tolerance. If an earthquake takes place, for example, this mechanism protects users' services from being affected.

Precautions

- The emergency state cannot be disabled manually.
- The emergency state can only be enabled three times for each license, and the license can keep in emergency state for 7 days each time.
- The next emergency state can be enabled only on the last day when the last emergency state expires.
- After the emergency state is enabled, the device provides maximum number of resource control items contained in the loaded license. The device does not provide resource control items that are not contained in the loaded license even through the emergency state is enabled.

Example

Enable the license emergency state.

```
<HUAWEI> license emergency
Warning: This operation will cause LCS into the EMERGENCY state. Continue? [Y/N]:y
Info: Emergency started cannot be stopped.
```

2.10.19 virtual-license emergency

Function

The **virtual-license emergency** command enables the emergency state of the virtual license.

Format

virtual-license emergency

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **virtual-license emergency** command to enable the emergency state of the virtual license. After the emergency state is enabled, the VXLAN and AP cloud license control items are not controlled by the virtual license. After the validity period of the emergency state expires, the VXLAN and AP cloud license control items are controlled by the license. A version provides three validity periods of the emergency state, each of which lasts for seven days.

Precautions

- The emergency state cannot be disabled manually.
- The emergency state can only be enabled three times for each license, and the license can keep in emergency state for seven days each time.

Example

Enable the emergency state of the virtual license.

```
<HUAWEI> virtual-license emergency
```

2.10.20 license revoke

Function

The **license revoke** command revokes a license file.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license revoke

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

License is an authorization file. You can apply for, upgrade, or activate the license file to get corresponding user rights.

If new devices are deployed, you can purchase new licenses as needed to enable license-controlled features and functions on the devices. This reduces purchase costs. If the capacities of the existing devices need to be expanded, you can update the licenses used on the devices to enable more license-controlled features and functions.

You can upgrade a license file to:

- Add new features.
- Optimizes device performance.
- Fix bugs in the current version.

Before updating a license file, run the **license revoke** command to revoke the existing license. The system then returns a license revocation code. This code is the evidence for license invalidation and is used to apply for a new license.

NOTE

A license revocation code is a character string generated after a license file becomes invalid. You can determine that a license file is invalid based on the corresponding revocation code.

Precautions

- When the existing license is going to expire, apply for a new license, upgrade, and activate the license. If the license has expired, the service modules are disabled and services are interrupted.
- After you run the **license revoke** command, the license file enters the Trial state and cannot be activated again regardless of how long the license file will expire.

Example

Revoke the current license file.

```
<HUAWEI> license revoke
Warning: The license will enter the Trial state and will not be activated again.
 Continue?[Y/N]: y
```

2.10.21 license verify

Function

The **license verify** command verifies the license file of the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license verify *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file. *file-name* supports file name association. The disk where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before running the **license active** command to activate a license file, verify the license file.

The result of the **license verify** command can be the following:

- Major error

  The license file cannot be activated.
- Minor error

  The license file may be unable to be activated.
- Success

  The license file can be activated.

Prerequisites

The license file has been saved on the device.

Example

Verify the license file **license.dat**.

```
<HUAWEI> license verify license.dat
Info: Verify license succeeded.
```

2.10.22 patch active all

Function

The **patch active all** command activates the patches on the current system.

By default, the loaded patches on the current system are inactive.

Format

patch active all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you do not specify the **active** or **run** keyword when running the **patch load** command, run the **patch active all** command to activate all the loaded patches to make them effect.

Prerequisites

Patches have been loaded using the **patch load** command.

Configuration Impact

- After a non-incremental patch is loaded and the **patch active all** command is run, the patches in the current system are activated.
- If an incremental patch is loaded and the previous patch package is running, the previous patch package is still in running state after you run the **patch active all** command. The new patch package is activated.

Follow-up Procedure

After running the **patch active all** command, use the **patch run all** command to run the activated patch.

Precautions

After you run the **patch active all** command:

- If the device is restarted, all the active patches become inactive. To reactivate the patches, run the **patch active all** command.

To make the patches become active, run the **patch active all** command again.

The active state can prevent a patch error from causing continuous faults of the system. If a patch has a bug and the patch is in the active state, restart the device to prevent the patch from taking effect.

Example

Activate all patches.

```
<HUAWEI> patch active all
```

2.10.23 patch configuration-synchronize

Function

The **patch configuration-synchronize** command synchronizes the patch configuration and patch file of the master switch to other member switches in a stack.

Format

patch configuration-synchronize

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After you replace or add a member switch in a stack and start the new member switch, run this command to synchronize the patch configuration and patch file from the master switch if the patch file of the new member switch is incorrect.

Example

Run the following commands on the new member switch to synchronize the patch configurations and patch files to the new member switch.

```
<HUAWEI> patch configuration-synchronize
Info: Finished synchronizing the patch package file and the patch configuration.
```

2.10.24 patch deactive all

Function

The **patch deactive all** command deactivates the patches on the current system.

Format

patch deactive all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

This command does not take effect in the current version. During the operation, if a bug is detected in a patch and the system software problem cannot be solved, run the **patch delete all** command to delete the patches in the patch area in the memory.

Example

Deactivate patches on the current system.

```
<HUAWEI> patch deactive all
Warning: This function is no longer supported in the current version.
```

2.10.25 patch delete all

Function

The **patch delete all** command deletes patches on the current system.

Format

patch delete all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

- If you find errors in patches that have been loaded to the system, run this command to delete the patches to prevent patch errors from affecting system operating.
- Before loading a non-incremental patch, run this command to delete the existing patches (if any). Otherwise, the non-incremental patch cannot be loaded.
- After the patch is deleted, it is recommended that you restart the switch.

Example

Delete all patches.

```
<HUAWEI> patch delete all
Warning: The device needs to restart after the patch is deleted.
This will delete the patch. Are you sure? [Y/N]
```

2.10.26 patch load

Function

The **patch load** command loads the patches to the patch areas in the system.

Format

patch load *filename* **all** [**active** | **run**]

Parameters

Parameter	Description	Value
filename	Specifies the path and file name of a patch package. The path can be an absolute path or a relative path. *file-name* supports file name association. The disk where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name must have an extension of .pat.
all	Loads the patches of all member switches in a stack.	-
active	Activates loaded patches.	-
run	Runs loaded patches.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you load a patch to the current system, the system searches the patch package for a matching patch file according to the attributes of the patch file.

- If a matching patch file is found in the patch package, the system loads the patch.
- If no matching patch file is found in the patch package, the system does not load any patch.

Prerequisites

The patch package has been uploaded to the root directory of the storage device.

Before loading a patch, the system must resolve the patch package, check the validity of the patch files in the patch package, and obtain the attributes such as the patch type and version of the patch file.

Precautions

The patch file cannot be reloaded. When you reload a patch, the system displays an error message.

After this command is run, the system loads all types of patches in the patch package.

- If the **active** parameter is specified, the system activates the loaded patches directly. Then you can use the **patch run all** command to run the patches.
- If the **run** parameter is specified, the system runs the loaded patches directly.

Example

Load the patches to the patch area of the device and run the patches directly.

```
<HUAWEI> patch load patch.pat all run
```

2.10.27 patch run all

Function

The **patch run all** command runs the patches on the current system.

Format

patch run all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device is restarted, the active patches become deactivated and need to be activated again. To enable the active patches to retain in running start after a device restart, use this command to run these active patches.

Prerequisites

Patches have been loaded and activated on the system.

Configuration Impact

After you run this command to run patches on the current system, the patches remain in the running state if a device restart occurs.

After the **patch run all** command is run, the patches enter running state and cannot be restored to the previous state. Confirm the action before you run the command.

Example

Run active patches on the current system.

```
<HUAWEI> patch run all
```

2.10.28 reset patch-configure

Function

The **reset patch-configure** command deletes the configuration of the patch file for next startup.

Format

reset patch-configure [**next-startup**]

Parameters

Parameter	Description	Value
next-startup	Deletes the configuration of the patch file for next startup.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you run the **startup patch** command to specify the patch file for next startup, you can use the **reset patch-configure** command to delete the configuration.

Precautions

If you run the **reset patch-configure** command, the patch file for next startup is empty. When the device restarts, the system does not load and run the patch file.

Example

Delete the configuration of the patch file for next startup.

```
<HUAWEI> reset patch-configure next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....
...
Info: Succeeded in resetting the next-startup patch state.
```

2.10.29 rollback

Function

The **rollback** command rolls back the system to the previous version.

Format

rollback

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an error occurs during an upgrade and you need to cancel the upgrade, run the **rollback** command to roll back the system to the previous version. After the rollback, the configuration of the device is the same as the previous configuration.

Precautions

- The rollback function takes effect only for an upgrade during which the **reboot** command is run to restart the device, and does not support other upgrade modes, such as the EasyDeploy upgrade and smooth stack upgrade. If the **reboot** command is run to complete an upgrade and then the system is upgraded using another mode, you can only run the **rollback** command to roll back the system to the latest version before the upgrade during which the **reboot** command is run. For example, if you run the **reboot** command to restart the device and upgrade the system from V1.0 to V1.1, and then upgrade the system to V1.2 using EasyDeploy, the system can only be rolled back to V1.0 when you run the **rollback** command to perform a system rollback.
- If a device runs continuously for more than 48 hours after being upgraded, the rollback function does not take effect. If the device runs continuously for less than 48 hours and restarts, the system sets the remaining time to zero

and the rollback function does not take effect. You can run the **display rollback information** command to check the remaining time for the rollback function to take effect.

- If the system software, configuration file, or patch file required in the rollback is deleted using the **delete (user view)** command, the system prompts that the rollback function cannot be used when you run the **rollback** command.

NOTICE

If you run the **rollback** command to roll back the system software, the current configuration of the device will be lost. Therefore, exercise caution when deciding to run this command.

Prerequisites

The device contains the system software, configuration file, and patch file that are used after the rollback and displayed in the **display rollback information** command output.

Example

Roll back the system to the previous version.

```
<HUAWEI> rollback
Info: Checking rollback version information...
Rollback software: flash:/basicsoft.cc
Rollback configuration: flash:/vrpcfg.zip
Rollback patch: NULL
Warning: The version running before the last reboot/reboot fast operation is performed will be restored,
and the current configuration will be lost. Continue? [Y/N]:y
```

2.10.30 uninstall-module

Function

The **uninstall-module** command uninstalls module packages.

Format

uninstall-module *file-name* [**next-startup**]

uninstall-module next-startup all

Parameters

Parameter	Description	Value
file-name	Specifies the name of a module package to be uninstalled.	The value is a string of 5 to 64 case-insensitive characters without spaces.
next-startup	Clears the module list for next startup.	-

Parameter	Description	Value
all	Clears the module list for next startup.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If some services or functions are not required, run the **uninstall-module** command to uninstall the corresponding modules running in the system.

Example

Uninstall the module package s5720hi.mod from the system.

```
<HUAWEI> uninstall-module s5720hi.mod
This will uninstall the module. Are you sure? [Y/N]y....
Info: Succeeded in uninstalling the module on the master board.
```

Clear a specified module package in the next startup module list.

```
<HUAWEI> uninstall-module s5720hi.mod next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....
...
Info: Succeeded in resetting the next-startup module.
```

3 Device Management Commands

3.1 Device Status Checking Commands

3.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.1.2 check hardware health

Function

The **check hardware health** command displays health check information about the device.

Format

check hardware health [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before upgrading a device's software package, run this command to check the health check information about the device. Ensure that all check items are normal before the upgrade to prevent a device upgrade failure.

Example

Display health check information about the device.

```
<HUAWEI> check hardware health
--------------------------------------------------------------------
Hardware health information of slot 0
--------------------------------------------------------------------
Board ID                              : Normal
PCB version                           : Normal
Bom ID                                : Normal
Flash read state                      : Normal
NAND bad block check result           : Normal
Remaining space                       : Normal
NOR flash erase state                 : Normal
CPLD erase state                      : Normal
CPLD self-check                       : Normal
DDR single-bit ECC error count        : 0
Cache single-bit ECC error count      : 0
Power PWR1(CML)                       : Normal
Power PWR1(TEMPERATURE)               : Normal
Power PWR1(VIN_UV)                    : Normal
Power PWR1(IOUT_OC)                   : Normal
Power PWR1(VOUT_OV)                   : Normal
```

```
Power PWR1(OFF)                    : Normal
Power PWR1(BUSY)                   : Normal
Power PWR1(UNKNOWN)                : Normal
Power PWR1(OTHER)                  : Normal
Power PWR1(FANS)                   : Normal
Power PWR1(POWER_GOOD)             : Normal
Power PWR1(MFR)                    : Normal
Power PWR1(INPUT)                  : Normal
Power PWR1(IOUT/POUT)              : Normal
Power PWR1(VOUT)                   : Normal
Board corrosion                    : No
```

Table 3-1 Description of the **check hardware health** command output and troubleshooting methods for abnormal devices

Item	Description	Troubleshooting methods for abnormal devices
Hardware health information of slot x	Health check information about the device.	-
Board ID	Status of the Printed circuit board (PCB) check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
PCB version	Status of the PCB version check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Bom ID	Status of the Bom ID check. ● Normal: The status is normal. ● Abnormal: The status is abnormal. **NOTE** This field is not available for the S6720-EI and S6720S-EI.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Flash read state	Status of the flash read/write check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
NAND bad block check result	Status of the bad block check of the NAND flash. ● Normal: The status is normal. ● Abnormal: The status is abnormal. **NOTE** This field is not available for the S6735-S.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Remaining space	Status of the flash remaining space check. ● Normal: The status is normal. ● Abnormal: The status is abnormal.	1. Enter the device directory. a. If the switch has a hard disk, run the **cd hda1:** command to enter the hard disk directory. b. If the switch has a flash rather than a hard disk, run the **cd flash:** command to enter the flash directory. 2. Run the **dir** command to check the size of the remaining storage space. If the remaining space is not enough, run the **delete** command to delete unneeded files. 3. Run the **dir** command to check whether the size of the remaining storage space is greater than the size of the PDF file. ● If so, go to Step 5. ● If not, go to Step 4. 4. Collect log information and configuration information, and then contact technical support personnel. 5. End.

Item	Description	Troubleshooting methods for abnormal devices
NOR flash erase state	Status of the erase and write check of the NOR flash. - Normal: The status is normal. - Abnormal: The status is abnormal. **NOTE** This field is not available for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
CPLD erase state	Status of the CPLD erase and write check. - Normal: The status is normal. - Abnormal: The status is abnormal. **NOTE** This field is not available for the S6720-EI and S6720S-EI.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
CPLD self-check	Status of the CPLD self-check. - Normal: The status is normal. - Abnormal: The status is abnormal.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
DDR single-bit ECC error count	DDR single-bit ECC error frequency.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.
Cache single-bit ECC error count	Cache single-bit ECC error frequency.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(CML)	Whether the communication of the power module is normal: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(TEMPERATURE)	Whether the temperature of the power module is abnormal: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(VIN_UV)	Whether the input voltage of the power module is below the lower threshold: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(IOUT_OC)	Whether the power module has output overcurrent: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(VOUT_OV)	Whether the output voltage of the power module exceeds the upper threshold: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(OFF)	Whether the power module is powered off: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(BUSY)	Whether the power module is busy and does not respond: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(UNKNOWN)	Whether the power module status is unknown: - Normal: The status is normal. - Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(OTHER)	Whether the power module is faulty due to any other reasons: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(FANS)	Whether the fan of the power module is faulty: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(POWER_GOOD)	Whether the output of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(MFR)	Whether a user-defined fault occurs on the power module: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.

Item	Description	Troubleshooting methods for abnormal devices
Power PWR1(INPUT)	Whether the input of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(IOUT/POUT)	Whether the output current or power of the power supply is faulty: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Power PWR1(VOUT)	Whether the output voltage of the power module is normal: ● Normal: The status is normal. ● Abnormal: The status is abnormal. If this parameter is not supported, a hyphen (-) is displayed.	If the power supply is faulty, collect alarm and configuration information, and contact technical support personnel.
Board corrosion	Whether the device is corroded. ● Yes: Corrosion occurs. ● No: Corrosion does not occur. If this parameter is not supported, a hyphen (-) is displayed.	If the device hardware is damaged, collect alarm and configuration information and contact technical support personnel.

3.1.3 display built-in power

Function

The **display built-in power** command displays the built-in power supply status of switches with extended temperature range.

NOTE

Only S5720I-28X-SI-AC and S5720I-28X-PWH-SI-AC support this command.

Format

display built-in power

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display built-in power** command to check whether the built-in power supply status of switches with extended temperature range is normal.

If some member switches do not support this command, the system displays a prompt message.

Example

Display the built-in power supply status of switches with extended temperature range.

```
<HUAWEI> display built-in power
------------------------------------------------------------
 Slot    PowerID     State
------------------------------------------------------------
 1       PWR1        Normal
         PWR2        Abnormal
 2       PWR1        Normal
         PWR2        Abnormal
------------------------------------------------------------
Info: Slot 0 does not support the command.
```

Table 3-2 Description of the **display built-in power** command output

Item	Description
Slot	Slot ID.
PowerID	Power supply ID.
State	Power supply status: - Abnormal - Normal

3.1.4 display battery information

Function

The **display battery information** command displays lithium battery information.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

display battery information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view lithium battery information.

Example

Display lithium battery information.

```
<HUAWEI> display battery information
Info: This operation may take a few seconds. Please wait for a
moment....
------------------------------------------------------------
 Lithium battery information of integrated power
------------------------------------------------------------
Battery group information
```

```
   Battery status                                 : Float charging
   Battery voltage(V)                               : 54.26
   Battery current(A)                               : 0.00
   Total battery capacity(Ah)                          : 200
   Available battery capacity(%)                         : 100.00
   Battery temperature(degC)                            : 29.47
   Battery run time(h)                               : 256.00
   Number of connected ESMUs                             : 2

Battery 1 information
   Battery voltage(V)                               : 54.28
   Battery current(A)                               : 0.00
   Device address                                 : 1
   Battery status                                 : Charging
   Battery SOH(%)                                  : 100.00
   Battery capacity(Ah)                             : 100
   Electrochemical cell package voltage(V)               : 50.99
   Maximum allowable current limiting coefficient(C10) :
0.30
   Electric core(1-16) voltage(V)                      :
       core[1-4]  :3.40 3.40 3.40 3.40
       core[5-8]  :3.40 3.40 3.40 3.40
       core[9-12] :3.38 3.40 3.40 3.40
       core[13-16]:3.40 3.40 3.40 3.40
   Electric core(1-16) degree(degC)                      :
       core[1-4]  :29.00 29.00 29.00 29.00
       core[5-8]  :29.00 29.00 29.00 29.00
       core[9-12] :29.00 29.00 29.00 30.00
       core[13-16]:30.00 30.00 30.00 30.00
   SoftWare version                                 : V116

Battery 2 information
   Battery voltage(V)                               : 54.25
   Battery current(A)                               : 0.00
   Device address                                 : 2
   Battery status                                 : Charging
   Battery SOH(%)                                  : 100.00
   Battery capacity(Ah)                             : 100
   Electrochemical cell package voltage(V)               : 51.28
   Maximum allowable current limiting coefficient(C10) :
0.30
   Electric core(1-16) voltage(V)                      :
       core[1-4]  :3.42 3.42 3.41 3.42
       core[5-8]  :3.42 3.42 3.42 3.42
       core[9-12] :3.42 3.42 3.42 3.42
       core[13-16]:3.42 3.42 3.42 3.42
   Electric core(1-16) degree(degC)                      :
       core[1-4]  :31.00 31.00 31.00 29.00
       core[5-8]  :29.00 29.00 29.00 29.00
       core[9-12] :29.00 29.00 29.00 30.00
       core[13-16]:30.00 30.00 30.00 30.00
   SoftWare version                                 : V116
```

Table 3-3 Description of the **display battery information** command output

Item	Description
Lithium battery information of integrated power	Information about the integrated lithium battery system.
Battery group information	Battery group information.
Battery status	Battery status.
Battery voltage(V)	Battery voltage, in volts (V).

Item	Description
Battery current(A)	Battery current, in amperes (A).
Total battery capacity(Ah)	Total battery capacity, in Ah.
Available battery capacity(%)	Remaining battery capacity, in percentage.
Battery temperature(degC)	Battery temperature, in °C.
Battery run time(h)	Battery backup time, in hours.
Number of connected ESMUs	Number of connected ESMUs.
Device address	Device address.
Battery SOH(%)	Battery string SOH, in percentage.
Battery capacity(Ah)	Battery capacity, in Ah.
Electrochemical cell package voltage(V)	Electrochemical cell package voltage, in volts (V).
Maximum allowable current limiting coefficient(C10)	Maximum allowable current limiting coefficient, in C10.
Electric core(1-16) voltage(V)	Voltage of electrochemical cells 1 to 16, in Volt (V).
Electric core(1-16) degree(degC)	Temperature of electrochemical cells 1 to 16, in degrees Celsius.
SoftWare version	Software version. The value is in ASCII format.

3.1.5 display chip-temperature

Function

The **display chip-temperature** command displays the temperature of chip.

Format

display chip-temperature { **all** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
all	Displays the temperature of chip of all slots.	-

Parameter	Description	Value
slot *slot-id*	Displays the temperature of chip of a specified slot.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A proper temperature range is the prerequisite for stable running of switches. If the temperature of chip is too high or too low, the hardware may be damaged.

Example

Display the temperature of chips of all slots. (The actual output information may differ from the following information.)

```
<HUAWEI> display chip-temperature all
--------------------------------------------------
 Slot      Chip      Status      Current(C)
--------------------------------------------------
 0          LSW       Normal       46
           CPU       Normal       60
           PHY       Normal       52
<HUAWEI> display chip-temperature all
--------------------------------------------------
 Slot      Chip      Status      Current(C)
--------------------------------------------------
 0          LSW1       Normal       46
           LSW2       Normal       50
           CPU       Normal       60
           PHY       Normal       52
```

Table 3-4 Description of the **display chip-temperature** command output

Item	Description
Slot	Slot ID.
Chip	Type of the chip. ● CPU: indicates a CPU chip. ● LSW: indicates a forwarding chip. If there are multiple chips, they are displayed as LSW1, LSW2, ..., and so on. ● PHY: indicates a PHY chip on the backplane. ● PHY1: indicates a PHY chip on a subcard.

Item	Description
Status	Temperature status. ● Normal: The temperature is normal. ● Abnormal: The temperature is abnormal or all interfaces on the device are down.
Current(C)	Current temperature of the chip, in the centigrade scale (°C). The temperature value is displayed as an integer, so there may be a maximum of 1°C error between the displayed value and actual temperature.

3.1.6 display compatible-information

Function

The **display compatible-information** command displays compatible information of a device.

Format

display compatible-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Generally, device versions have matching NMS software. The NMS software needs to apply to all the devices supported by matching versions. Otherwise, the NMS cannot manage devices. If the NMS version is an earlier version but the current device is running a later version that does not match the current NMS version, the NMS cannot manage the current device.

To decouple the NMS version and device version, a compatible device model developed based on an earlier version is defined for each device model. If the NMS cannot manage a device because of version mismatch, obtain information about the device compatible with the current device. The NMS can then use the obtained information to manage the current device.

For example:

S5720-SI_R10 is a device model newly available in V200R010. The NMS software version that matches the device software version is V200R010.

S5720-SI_R8 is a device model newly available in V200R008. The NMS software version that matches the device software version is V200R008.

When you use the NMS of V200R008 to manage S5720-SI_R10, the device cannot be managed because of version mismatch. The NMS then obtains compatibility information about S5720-SI_R10 and learns that it is compatible with S5720-SI_R8. Subsequently, the NMS uses information about S5720-SI_R8 to manage the current device.

If the device does not have a compatible version, the system will display a message, indicating that no compatible information exists after the **display compatible-information** command is executed.

Compatible information of stacked devices can also be displayed.

Example

Display compatible information of a device.

```
<HUAWEI> display compatible-information
SlotID              : 0
Compatible SysOids  : 1.3.6.1.4.1.2011.2.23.331
Compatible Version  : V200R008C00
ProductName         : S5720-52X-SI-AC
```

Table 3-5 Description of the display compatible-information command output

Item	Description
SlotID	The slot ID.
Compatible SysOids	System OID of an old device version.
Compatible Version	Old device version compatible with the current device version.
ProductName	Product name of new devices.

3.1.7 display cpu-usage

Function

The **display cpu-usage** command displays CPU usage statistics.

Format

display cpu-usage [**slave** | **slot** *slot-id*] [**vcpu** *vcpu-index*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
slave	Displays the CPU usage of slave devices in a stack. This parameter is valid only in a stack system.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
vcpu *vcpu-index*	Displays the usage of a specified virtual CPU.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

CPU usage is an important indicator to evaluate device performance. A high CPU usage will cause service faults, for example, BGP route flapping, frequent VRRP active/standby switchover, and even failed device login. You can use the **display cpu-usage** command to view CPU usage to check whether devices are working properly.

When the CPU usage is high, rectify the fault according to "Troubleshooting: High CPU" in ***Huawei S Series Campus Switches Troubleshooting Guide***.

Example

Display the CPU usage on the device.

```
<HUAWEI> display cpu-usage
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 20% Max: 99%
CPU Usage Stat. Time : 2019-10-23  10:04:45
CPU utilization for five seconds: 5%: one minute: 5%: five minutes: 5%
Max CPU Usage Stat. Time : 2019-10-21 16:14:00.

TaskName             CPU  Runtime(CPU Tick High/Tick Low)  Task Explanation
VIDL                80%         0/e3a150c0       DOPRA IDLE
```

```
OS            10%       0/ bfb0440      Operation System
1AGAGT          6%       0/      0      1AGAGT
AAA            2%       0/    1d4a      AAA  Authen Account Authorize
ACL            1%       0/   13362      ACL Access Control List
ADPT            1%       0/      0      ADPT Adapter
AGNT             0%       0/      0      AGNTSNMP agent task
AGT6            0%       0/      0      AGT6SNMP AGT6 task
ALM             0%       0/      0      ALM  Alarm Management
ALS            0%       0/  527a3e      ALS  Loss of Signal
AM             0%       0/   232cf      AM   Address Management
APP            0%       0/      0      APP
ARP            0%       0/   36582      ARP
ASFI           0%       0/      0      ASFI
ASFM             0%       0/      0      ASFM
BATT            0%       0/      0      BATT Main Task
BFD             0%       0/  100f36      BFD Bidirection Forwarding
                                  Detect
BFDA            0%       0/      0      BFDA BFD Adapter
BFDS            0%       0/    5825      BFDS
BOX            0%       0/  1d0097      BOX Output
BPDU            0%       0/    1806      BPDU Adapter
BTRC            0%       0/    60e      BTRC
CDM             0%       0/    9b95      CDM
CFM             0%       0/    6f68      CFM Configuration file
                                  management
CLKI           0%       0/      0      CLKI
DEFD            0%       0/   22ebd      DEFD CPU Defend
DELM             0%       0/    355c      DELMAC FOR STP
DEV            0%       0/      0      DEV  Device Management
DHCP             0%       0/   12188      DHCP Dynamic Host Config
                                  Protocol
DLDP            0%       0/    dc0d      DLDP Protocol
EAP            0%       0/    38a9      EAP  Extensible Authen
                                  Protocol
EFMT            0%       0/   11c70      EFMTEST 802.3AH Test
EOAM             0%       0/    ea8f      EOAM1AG
ESAP            0%       0/      0      ESAP eSap Adapter
ETHA            0%       0/      0      ETHA
EZOP            0%       0/   506f4      EZOP EasyOperation
                                  application
EZPP            0%       0/  1e41f8      EZPP EasyOperation packet
FCAT            0%       0/    6479      FCAT Catch Packets for
                                  debugging
FECD            0%       0/   11d8e      FECD Mod Manage Task
FIB            0%       0/    523b      FIB Forward Information Base
FIB6           0%       0/      0      FIB6IPv6 FIB
FLOW             0%       0/    ce76      FLOW SFLOW
FMAT             0%       0/    7f23      FMATFault Manage task
FTS            0%       0/  125f35      FTS
GEM             0%       0/      0      GEM task
GEMR             0%       0/      0      GEMRun task
GRSA            0%       0/      0      GRSA
GVRP            0%       0/      0      GVRP Protocol
HACK             0%       0/      0      HACKtask for HA ACK
HOTT             0%       0/      0      HOTT
HS2M             0%       0/      0      HS2MHigh available task
HTTP            0%       0/   5d420      HTTP
IFLP           0%       0/    8611      IFLP
IFNT            0%       0/      0      IFNTIfnet task
IFPD            0%       0/ 2177f21      IFPD Ifnet Product Adapter
INFO            0%       0/   70409      INFOInformation center
IP            0%       0/    cb13      IP
IPCK           0%       0/      0      IPCKIPC task for ack message
IPCQ            0%       0/  3c6ffd      IPCQIPC task for single queue
IPCR           0%       0/      0      IPCR IPC Receiver
JOB            0%       0/      0      JOB Schedule
L2            0%       0/   2a6b5      L2
L2IF           0%       0/   b7fbc      L2IF
L2_E           0%       0/   10088      L2_EOAM_Y1731
```

```
L2_P            0%       0/   58a50      L2_PR
L2_R            0%       0/  169c0c      L2_RING
L2_T            0%       0/    1724      L2_TRUNK
L3I4            0%       0/       0      L3I4 LPU Manage IPv4 unicast
                                         FDB
L3IO            0%       0/       0      L3IO LPU Process urpf, vrrp
                                         etc.
L3M4            0%       0/       0      L3M4 MPU Manage IPv4 unicast
                                         FDB
L3MB            0%       0/    4319      L3MB MPU Process urpf, vrrp
                                         etc.
LAGAGT          0%       0/   107dd      LAGAGT
LBDT            0%       0/  1bf810      LBDT Loopback Detect Mpu
LINK            0%       0/       0      LINK
LLDP            0%       0/   70921      LLDP Protocol
LNP             0%       0/       0      LNP task
MAC             0%       0/    564f      MAC Media Access Control
MACL            0%       0/   21954      MACL Access Control List
MAD             0%       0/    dae7      MAD Task
MADP            0%       0/       0      MADP MAD proxy Task
MCSW            0%       0/   12624      MCSW Mulitcast Switch Adapter
MERX            0%       0/   8a774      MERX Meth Receive
METH            0%       0/   f0699      METH Metropolitan Ethernet
MFF             0%       0/    b308      MFF MAC Forced Forwarding
MFIB            0%       0/     beb      MFIBMulticast forward info
MIRR            0%       0/       0      MIRR Capture Packet
MSYN            0%       0/   7245a      MSYN Mac Synchronization
Mirr            0%       0/    4107      Mirror
NDIO            0%       0/       0      NDIO LPU Manage IPv6 unicast
                                         FDB
NDMB            0%       0/       0      NDMB MPU Manage IPv6 unicast
                                         FDB
NFPT            0%       0/   d2dec      NFPTNFP timer task
NTPT            0%       0/       0      NTPT task
OAM1            0%       0/       0      OAM1 EOAM Adapter
PAT             0%       0/       0      PAT
PNGI            0%       0/       0      PNGI
PNGM            0%       0/       0      PNGM MPU Process icmp reply
                                         fast
POE+            0%       0/       0      POE+ PPP Over Ethernet Plus
PPI             0%       0/   58e46      PPI Product Process Interface
PTAL            0%       0/       0      PTAL Portal
RDS             0%       0/       0      RDS  Radius
RMON            0%       0/   11240      RMONRemote monitoring
ROUT            0%       0/  6a6343      ROUTRoute task
RPCQ            0%       0/   22254      RPCQRemote procedure call
RTMR            0%       0/   ed870      RTMR
SAM             0%       0/    2e2d      SAM  Service Agent Module
SAPP            0%       0/    758e      SAPP
SECE            0%       0/  2e6e82      SECE Security
SLAG            0%       0/       0      SLAG
SMAG            0%       0/       0      SMAG Smart Link Agent
SMLK            0%       0/   71827      SMLK Smart Link Protocol
SNPG            0%       0/   d97b7      SNPG Multicast Snooping
SOCK            0%       0/   4bdda      SOCKPacket schedule and
                                         process
SPM             0%       0/   6a1ce      SPM  Smart Power Management
SRM             0%       0/  6bb9b8      SRM  System Resource
                                         Management
SRMI            0%       0/       0      SRMI External Interrupt
SRMT            0%       0/  fe2a46      SRMT System Resource Manage
                                         Timer
STFW            0%       0/       0      STFW Super task forward
STND            0%       0/       0      STNDStandby task
STP             0%       0/  79e590      STP
STRA            0%       0/   1c767      STRA Source Trail
TACH            0%       0/   9817e      TACHWTACACS
TARP            0%       0/       0      TARPING
TICK            0%       0/  7dbef6
```

```
TM              0%       0/      0      TM   Transmission Management
TNQA            0%       0/  83134      TNQAC
TRAP            0%       0/   14d7      TRAPSNMP trap task
TTNQ            0%       0/      0      TTNQAS
TUNL            0%       0/   5c17      TUNL
UCM             0%       0/   3e46      UCM  User Control Management
UTSK            0%       0/      0      UTSK
VCMP            0%       0/      0      VCMP task
VFS             0%       0/      0      VFS Virtual file system
VFSD            0%       0/      0      VFSDVFS flash task for delete
                                        file block
VMON            0%       0/   78d5      VMONSystem monitor
VMSH            0%       0/      0      VMSH
VP              0%       0/   5966      VP  Virtual path task
VPR             0%       0/      0      VPR  VP Receiver
VRPT            0%       0/   39fd      VRPT
VRRP            0%       0/ 152ced      VRRP
VT              0%       0/      0      VT   Virtual Transfer
VT0             0%       0/ 4909c5      VT0 Line user's task
VT1             0%       0/      0      VT1 Line user's task
VTYD            0%       0/  b3282      VTYDVirtual terminal
WEB             0%       0/   1295      WEB  Web
XMON            0%       0/      0      XMONVxworks system monitor
XQOS            0%       0/  12999      XQOS Quality of service
_EXC            0%       0/      0      Exception Agent Task
_TIL            0%       0/      0      Infinite loop event task
bcmCNTR.0       0%       0/ 61077b      tS10
bcmCNTR.1       0%       0/ 605691      tS11
bcmDPC          0%       0/  25d89      tS09
bcmL2X.0        0%       0/ b069d6      tS0c
bcmL2X.1        0%       0/ b2c5f2      tS0f
bcmRX           0%       0/ 1df879      bcmRX
bcmTX           0%       0/   16f2      tS0a
frag_add        0%       0/ 45ecce      tS0d
frag_del        0%       0/      0      tS0e
linkscan        0%       0/ ecce16      tS12
root            0%       0/      0      tS03
soft_learn      0%       0/  7812a      tS0b
tExcTask        0%       0/      0      tS00
tLogTask        0%       0/      0      tS01
tShell          0%       0/      0      tS02
```

Table 3-6 Description of the **display cpu-usage** command output

Item	Description
CPU Usage Stat. Cycle	Interval for collecting CPU usage statistics. The interval is 60 seconds and cannot be configured.
CPU Usage	Average CPU usage in the last 10 seconds.
Max	Highest CPU usage in history.
CPU Usage Stat. Time	Time when the latest CPU usage statistics are collected.
CPU utilization for five seconds	CPU usage in five seconds.
one minute	CPU usage in one minute.
five minutes	CPU usage in five minutes.
Max CPU Usage Stat. Time	Time when the highest CPU usage statistics are collected.

Item	Description
TaskName	Task that is being executed. For details about all the tasks and functions of the device, see "Troubleshooting: High CPU Usage - How to Locate the High CPU Usage Problem - Determining Fault Causes According to CPU Usages of Tasks (Fixed Switches)" and "Troubleshooting: High CPU Usage - Appendix - CPU-related Tasks and Functions for Fixed Switches" in ***Huawei S Series Campus Switches Troubleshooting Guide***.
CPU	Real-time CPU usage of each task.
Runtime(CPU Tick High/Tick Low)	System running time calculated based on CPU tick.
Task Explanation	Explanation to the task.

3.1.8 display cpu-usage configuration

Function

The **display cpu-usage configuration** command displays CPU usage configuration.

Format

display cpu-usage configuration [**slave** | **slot** *slot-id*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Parameters

Parameter	Description	Value
slave	Displays CPU usage configuration of standby switches in a stack.	-
slot *slot-id*	Displays device CPU usage configuration of a specified slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the alarm threshold and recovery threshold.

- When CPU usage reaches the alarm threshold, the system generates a CPU usage alarm.
- When CPU usage falls within the recovery threshold, the system generates a clear alarm.

Example

Display CPU usage configuration.

```
<HUAWEI> display cpu-usage configuration
The CPU usage monitor is turned on.
The current monitor cycle is 60 seconds.
The current monitor warning threshold is 95%.
The current monitor restore threshold is 80%.
```

Table 3-7 Description of the **display cpu-usage configuration** command output

Item	Description
The CPU usage monitor	Whether the CPU usage monitoring function is enabled or disabled. To enable the CPU usage monitoring function, run the **cpu-usage monitor** command.
The current monitor cycle	CPU usage monitoring period, which cannot be configured.
The current monitor warning threshold	Alarm threshold. To set the CPU usage alarm threshold, run the **cpu-usage threshold** *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*] command.
The current monitor restore threshold	Alarm recovery threshold. To set the CPU usage alarm recovery threshold, run the **cpu-usage threshold** *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*] command.

3.1.9 display cpu-usage history

Function

The **display cpu-usage history** command displays CPU usage statistics within a period.

Format

display cpu-usage history [**1hour** | **24hour** | **72hour**] [**slave** | **slot** *slot-id*] [**vcpu** *vcpu-index*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
1hour	Displays CPU usage statistics within the last one hour.	-
24hour	Displays CPU usage statistics within the last 24 hours.	-
72hour	Displays CPU usage statistics within the last 72 hours.	-
slave	Displays the CPU usage statistics of slave devices in a stack. This parameter is valid only in a stack system.	-
slot *slot-id*	Displays the CPU usage statistics of a specified slot ID.	The value varies with the device configuration.
vcpu *vcpu-index*	Displays the CPU usage statistics of a specified virtual CPU.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The system collects CPU usage statistics at a specified interval (usually 60s) and saves them in the historical record table. To check CPU usage statistics within a period, run the **display cpu-usage history** command, and the command output helps you determine whether the CPU is working properly.

In the **display cpu-usage history** command output, the x-coordinate indicates the specified period, and the y-coordinate indicates the CPU usage.

Precautions

If CPU usage is constantly higher than the upper alarm threshold (95% by default) before the feature is deployed on a large scale, check the device to troubleshoot the fault.

Example

Display CPU usage statistics within the last one hour.

```
<HUAWEI> display cpu-usage history 1hour
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|        H
 30%|        H
 25%|        H
 20%|        H
 15%|        H
 10%|        H
  5%|HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH
    ---------+---------+---------+---------+---------+---------+>
             10        20        30        40        50        60
             System cpu-usage last 60 minutes(Per Min)
```

Display CPU usage statistics within the last 24 hours.

```
<HUAWEI> display cpu-usage history 24hour

100%|
 95%|
 90%|
 85%|
 80%|
 75%|*
 70%|*
 65%|*
 60%|*
```

```
 55%|*
 50%|*
 45%|*
 40%|*
 35%|*                 **
 30%|*                 **
 25%|*                 **
 20%|*                 **
 15%|*                 **
 10%|H                  **
  5%|HHHHHHHHHHHHHHHHHHHHHHHHHHHHH
     ---------+---------+---------+---------+-------->
              10        20        30        40
        System cpu-usage last 24 hours(Per Halfhour)
       * = maximum cpu-usage    H = average cpu-usage
```

Display CPU usage statistics within the last 72 hours.

```
<HUAWEI> display cpu-usage history 72hour

100%|
 95%|
 90%|
 85%|
 80%|
 75%|*
 70%|*
 65%|*
 60%|*
 55%|*
 50%|*
 45%|*
 40%|*
 35%|*      *
 30%|*      *
 25%|*      *
 20%|*      *
 15%|*      *
 10%|*      *
  5%|HHHHHHHHHHHHHH
     ---------+---------+---------+---------+---------+---------+---------+-->
              10        20        30        40        50        60        70
                    System cpu-usage last 72 hours(Per Hour)
                   * = maximum cpu-usage    H = average cpu-usage
```

Table 3-8 Description of the **display cpu-usage history** command output

Item	Description
System cpu-usage last 60 minutes(Per Min)	CPU usage statistics within the last one hour, with a step of one minute.
System cpu-usage last 24 hours(Per Halfhour)	CPU usage statistics within the last 24 hours, with a step of half an hour.
System cpu-usage last 72 hours(Per Hour)	CPU usage statistics within the last 72 hours, with a step of an hour.
* = maximum cpu-usage	Maximum CPU usage. For example, the maximum CPU usage in the first hour in the latest 72 hours is 75%.

Item	Description
H = average cpu-usage	Average CPU usage. For example, the average CPU usage in the first hour in the latest 72 hours is 5%.

3.1.10 display device

Function

The **display device** command displays the type and status of the components on a device.

Format

display device [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you need to check whether a switch is working properly, run the **display device** command to view hardware information of the components and device registration status on the switch.

This command can also display the working status of the battery or redundant power supply (RPS) used for a device.

The following product models support the use of an RPS:

- S5720-LI series: S5720-28X-LI-AC, S5720-28X-LI-DC, S5720-28X-PWR-LI-AC, S5720-52X-LI-AC, S5720-52X-LI-DC, S5720-52X-PWR-LI-AC, S5720-28X-LI-24S-AC, S5720-28X-LI-24S-DC, S5720-28X-PWH-LI-AC, S5720-52X-PWR-LI-ACF, S5720-52X-LI-48S-AC, S5720-52X-LI-48S-AC1, S5720-52X-LI-48S-DC1, S5720-52X-LI-24S-AC1 S5720-28X-PWR-LI-ACF
- S5720S-LI series: S5720S-28X-LI-24S-AC and S5720S-52X-LI-24S-AC1

Example

Display information about the components on a device (with a built-in power supply unit or power module).

```
<<HUAWEI> display device
S5720-52P-LI-AC's Device status:
Slot Sub  Type              Online    Power     Register    Status   Role
-------------------------------------------------------------------------------
0    -    S5720-52P-LI       Present   PowerOn    Registered   Normal   Master
```

Display information about components on a device (connected to an RPS).

```
<HUAWEI> display device
S5720-28X-LI-AC's Device status:
Slot  Sub  Type             Online    Power     Register    Status   Role
--------------------------------------------------------------------------------
0     -    S5720-28X-LI      Present   PowerOn    Registered   Normal   Master
         RPS              Present   PowerOn    Registered   Self-powered
```

Display information about components on a device (where ports on the device panel and ports on subcards cannot be used together).

```
<HUAWEI> display device
S6720-32C-PWH-SI-AC's Device status:
Slot Sub  Type               Online    Power    Register    Status   Role
-------------------------------------------------------------------------------
0    -    S6720-32C-PWH-SI      Present   PowerOn  Registered   Normal
Master
     1    -                  Present   PowerOn  Unregistered -       NA
     PWR1 POWER                Present   PowerOn  Registered   Normal
NA
     FAN1 FAN                  Present   PowerOn  Registered   Normal
NA
Info: Slot 0 is in the port-on-card disable mode, so subcard 1 is unavailable and unregistered.
```

Display information about the component in slot 0.

```
<HUAWEI> display device slot 0
*down: administratively down

S5720-52P-LI-AC's Device status:
Slot Sub  Type              Online    Power     Register    Status   Role
-------------------------------------------------------------------------------
0    -    S5720-52P-LI       Present   PowerOn    Registered   Normal   Master
-------------------------------------------------------------------------------
  Board Type        : S5720-52P-LI
  Board Description : 48 Ethernet 10/100/1000 ports,4 Gig SFP,AC 110/220V
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Port      Port     Optic     MDI     Speed    Duplex  Flow-    Port   PoE
          Type     Status            (Mbps)           Ctrl     State  State
------------------------------------------------------------------------------
0/0/1     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/2     GE(C)    Absent    Auto    1000     Full    Disable  Up     -
0/0/3     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/4     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/5     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/6     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/7     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/8     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/9     GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/10    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/11    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/12    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/13    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/14    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/15    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/16    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
0/0/17    GE(C)    Absent    Auto    1000     Full    Disable  Down   -
```

```
0/0/18   GE(C)   Absent   Auto   1000   Full   Disable  Down   -
0/0/19   GE(C)   Absent   Auto   1000   Full   Disable  Down   -
```

Table 3-9 Description of the display device command output

Item	Description
Slot	Slot ID.
Sub	Card ID. The value can be: - –: indicates that the component is a device, not a card. - n: indicates a card. *n* is a digit. - FANn: indicates a fan module. *n* indicates the serial number of the fan module. - PWRn: indicates a power module . *n* indicates the serial number of the power module.
Type	Component type. A component can be a device, RPS, or a card. Subcards are classified into the front subcard, rear subcard, power subcard and fan subcard. - Front card: The command displays the PCB model of a front card. For card classification and details about different cards, see the *Hardware Description*. - Rear card: The command displays the PCB model of a rear card. For card classification and details about different cards, see the *Hardware Description*. - Fan subcards include FAN. - Power subcard is POWER. - Lead-acid battery board: PBB-12AHA Redundant power supply: RPS
Online	Whether a component is available. If the component is available, this field displays Present. If the component is unavailable, it is not displayed in the command output.
Power	Power supply status. The value can be: - PowerOn - PowerOff
Register	Whether the device is registered: - Registered: indicates that the component is registered. - Unregistered: indicates that the component is unregistered.

Item	Description
Status	Status of the component. The value can be: ● Abnormal: indicates that the component is running abnormally or the component does not match the device model. ● Normal: indicates that the component is running normally. ● WarmingUp: indicates that a subcard is performing configuration restoration. If the device is connected to an RPS power supply, the following values may be displayed: ● Non-powered: The RPS power supply is not supplying power to the local device. ● Other-powered: The RPS power supply is supplying power to another device and cannot supply power to the local device. ● Self-powered: The RPS power supply is supplying power to the local device. ● –: The RPS power supply is initializing and has not registered.
Role	Role of a component. ● In a stack, the value can be: Master: The component is the master switch. Standby: The component is the standby switch. Slave: The component is a slave switch. ● On a standalone device, this field displays Master. ● The value NA indicates a card.
Board Type	Device type.
Board Description	Device description.
Port	Number of an interface on a device.
Port Type	Type of an interface. ● If the field value contains (C), this interface is an electrical interface. ● If the field value contains (F), this interface is an optical interface.
Optic Status	Whether an optical module is available on an interface. ● Present: An optical module is present on the interface. ● Absent: No optical module is present on the interface. ● -: Optical module information cannot be obtained.

Item	Description
MDI	Medium dependent interface (MDI) type, which can be any of the following: ● Auto ● Normal ● Across If this field displays -, the MDI type of the interface cannot be obtained.
Speed (Mbps)	Interface speed.
Duplex	Duplex mode of an interface. ● Half: The interface works in half-duplex mode. ● Full: The interface works in full-duplex mode. ● -: The interface duplex mode cannot be obtained. To set the duplex mode for an interface, run the **duplex** command.
Flow-Ctrl	Flow control status on an interface. ● Disable: The flow control and received flow control is disabled on the interface. ● Enable: The flow control function is enabled on the interface. ● Receive enable: The receive flow control is enabled on the interface. ● -: The flow control status cannot be obtained. To configure flow control, run the **flow-control** or **flow-control receive** command.
Port State	Status of an interface: ● down: The interface is physically Down. ● *down: The interface is manually shut down. ● up: The interface is in Up state.
PoE State	Status of the PoE function on an interface. ● Enable: The PoE function is enabled. ● Disable: The PoE function is disabled. ● -: PoE information cannot be obtained.

3.1.11 display device mac-number

Function

The **display device mac-number** command displays the number of MAC addresses of a switch.

Format

display device mac-number [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a device ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

One or more MAC addresses may be configured on a switch before delivery. To check the number of MAC addresses of a switch, run the **display device mac-number** command. If the switch has multiple MAC addresses configured, the MAC addresses of Layer 3 interfaces are different from the system MAC address. If the switch has only one MAC address configured, the MAC addresses of Layer 3 interfaces are the same as the system MAC address. On a switch with one or more MAC addresses configured, the MAC addresses of Layer 2 interfaces are the same as the system MAC address.

If **slot** *slot-id* is not specified in a stack, the **display device mac-number** command displays the number of MAC addresses of the master switch.

Example

Display the number of MAC addresses.

```
<HUAWEI> display device mac-number
The number of MAC address : 1
```

Table 3-10 Description of the **display device mac-number** command output

Item	Description
The number of MAC address	Number of MAC addresses.

3.1.12 display device manufacture-info

Function

The **display device manufacture-info** command displays manufacture information about the device.

Format

display device manufacture-info [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display device manufacture-info** command to view manufacture information about the device, including the serial number and manufacture date. The command output contains information about only service subcards and does not contain information about fans and power modules.

Example

Display manufacture information about the device.

```
<HUAWEI> display device manufacture-info
Slot  Sub  Serial-number          Manu-date
- - - - - - - - - - - - - - - - - - - - - -
0     -    2102353169107C800132   2011-08-24
      1    021ESN1234567890       2000-01-01
```

Display manufacture information about devices in a stack.

```
<HUAWEI> display device manufacture-info
Slot  Sub  Serial-number          Manu-date
- - - - - - - - - - - - - - - - - - - - - -
0     -    2102353169107C800132   2011-08-24
      1    021ESN1234567890       2000-01-01
3     -    2102353170107C800132   2011-08-23
4     -    2102353170107C800132   2011-08-23
      1    020WYG1234567892       2010-12-02
8     -    2102353170107C800235   2000-01-01
```

Table 3-11 Description of the display device manufacture-info command output

Item	Description
slot	Slot ID.
Sub	Subcard number.
Serial-number	Serial number.
Manu-date	Manufacture date of the device.

3.1.13 display diagnostic-information

Function

The **display diagnostic-information** command collects and displays all the current diagnostic information or saves diagnostic information in a specified file.

Format

display diagnostic-information [**acl** | **ap** | **arp** | **bfd** | **cmng** | **decoding** | **defend** | **dhcp | engine | evpn | gpm** | **l2adp** | **l3adp** | **lbdt** | **lldp** | **mcast** | **mpls** | **qos** | **rrpp | rumng | sa** | **sdk** | **smlk** | **srm** | **sta** | **stack** | **stat** | **stp** | **ucm** | **vxlan**] [*file-name*]

NOTE

- Only the S5720I-SI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **bfd**.
- Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730S-H, S6730-S, S6730S-S, and S6730-H support **mpls**.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **sdk**.
- The **stack** parameter is supported on a stack only.
- Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support **ap** and **sta**.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vxlan** and **evpn**.

Parameters

Parameter	Description	Value
acl	Displays ACL information.	-
ap	Displays AP information.	-
arp	Displays ARP information.	-

Parameter	Description	Value
bfd	Displays BFD information.	-
cmng	Displays cloud-based management information.	-
defend	Displays attack defense information.	-
decoding	Displays decoding information.	-
dhcp	Displays DHCP information.	-
engine	Displays engine information.	-
evpn	Displays EVPN information.	-
gpm	Displays GPM information.	-
l2adp	Displays L2 information.	-
l3adp	Displays L3 information.	-
lbdt	Displays LBDT information.	-
lldp	Displays LLDP information.	-
mcast	Displays multicast information.	-
mpls	Displays MPLS information.	-
qos	Displays QoS information.	-
rrpp	Displays RRPP information.	-
sa	Displays SA information.	-
sdk	Displays sdk information.	-
smlk	Displays Smart Link information.	-
stack	Displays stack information.	-

Parameter	Description	Value
srm	Displays device information.	-
sta	Displays STA information.	-
stat	Displays basic statistic information.	-
stp	Displays STP information.	-
ucm	Displays UCM module information.	-
vxlan	Displays VXLAN module information.	-
file-name	Specifies the name of the file where diagnostic information is stored.	The value is a string of 5 to 64 characters. The file name extension must be .txt. The default directory where files are stored is flash:/.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a fault occurs in the system, you can use the **display diagnostic-information** command to collect diagnostic information for fault location.

The **display diagnostic-information** command output includes the output for multiple **display** commands, such as **display clock**, **display version**, and **display current-configuration**. Running the **display diagnostic-information** command is like running these **display** commands in batches.

Precautions

- If the *file-name* parameter is not specified, diagnostic information is only displayed on the screen. If the *file-name* parameter is specified, diagnostic information is only stored to a specified file but not displayed on the screen, and the command level is management level (3).
- The command output does not support split-screen display.

- If this command displays a long output, press **Ctrl+C** to abort this command.
- This command displays diagnostic information, which helps locate faults but may affect system performance. For example, CPU usage may become high. Therefore, do not use this command when the system is running properly.
- Running the **display diagnostic-information** command simultaneously on multiple terminals connected to the device is prohibited. This is because CPU usage of the device may obviously increase and the device performance may be degraded.
- When you run this command, the device obtains or uses some personal data of users, such as the STA MAC address. Delete the personal data immediately after the command is executed to ensure user data security.

Example

Display diagnostic information about the device.

```
<HUAWEI> display diagnostic-information
==========================================================
  ===============display interface brief===============
==========================================================
PHY: Physical
*down: administratively down
#down: LBDT down
(l): loopback
(s): spoofing
(E): E-Trunk down
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(lb): LBDT block
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol  InUti OutUti   inErrors  outErrors
Eth-Trunk5                  down  down         0%     0%          0          0
Eth-Trunk9                  down  down         0%     0%          0          0
GigabitEthernet0/0/1        *down down         0%     0%          0          0
GigabitEthernet0/0/2        *down down         0%     0%          0          0
GigabitEthernet0/0/3        *down down         0%     0%          0          0
GigabitEthernet0/0/4        *down down         0%     0%          0          0
GigabitEthernet0/0/5        up    up           0%     0%          0          0
GigabitEthernet0/0/6        *down down         0%     0%          0          0
GigabitEthernet0/0/7        down  down         0%     0%          0          0
GigabitEthernet0/0/8        *down down         0%     0%          0          0
GigabitEthernet0/0/9        down  down         0%     0%          0          0
GigabitEthernet0/0/10       down  down         0%     0%          0          0
GigabitEthernet0/0/11       up    up           0%     0%          0          0
GigabitEthernet0/0/12       down  down         0%     0%          0          0
GigabitEthernet0/0/13       down  down         0%     0%          0          0
GigabitEthernet0/0/14       down  down         0%     0%          0          0
GigabitEthernet0/0/15       down  down         0%     0%          0          0
GigabitEthernet0/0/16       down  down         0%     0%          0          0
GigabitEthernet0/0/17       down  down         0%     0%          0          0
GigabitEthernet0/0/18       down  down         0%     0%          0          0
GigabitEthernet0/0/19       down  down         0%     0%          0          0
GigabitEthernet0/0/20       *down down         0%     0%          0          0
GigabitEthernet0/0/21       down  down         0%     0%          0          0
GigabitEthernet0/0/22       *down down         0%     0%          0          0
GigabitEthernet0/0/23       down  down         0%     0%          0          0
GigabitEthernet0/0/24       up    up           0%     0%          0          0
......
```

Save diagnostic information to the file **aa.txt** in the flash memory.

```
<HUAWEI> display diagnostic-information aa.txt
Now saving the diagnostic information to the device
```

```
 100%
Info: The diagnostic information was saved to the device successfully.
```

3.1.14 display elabel

Function

The **display elabel** command displays the electronic label of the device.

Format

display elabel [**slot** *slot-id* [*subcard-id*]]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
subcard-id	Specifies the subcard ID the ID of power module.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Electronic labels identify the hardware. You can use the **display elabel** command to view the electronic label information.

No electronic label is displayed for an electrical interface or a combo interface working as an electrical interface.

NOTE

The electronic label version of devices delivered since V200R011 has been updated to version 4.0. This version adds the following fields compared to earlier versions:

- Model indicates the hardware external model of the device.
- ExInfo indicates the hardware extension information of the device. This field is not provided in electronic labels of optical modules.
- ElabelVersion indicates the version of the elabel.

Example

Display the electronic label of the slot 0.

```
<HUAWEI> display elabel slot 0
Warning: It may take a long time to excute this command. Continue? [Y/N]:y
Info: It is executing, please wait...
/$[System Integration Version]
/$SystemIntegrationVersion=3.0


[Slot_0]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]

/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=S5720-28P-LI-AC
BarCode=2102353174107C800132
Item=02353174
Description=S5720-28P-LI-AC Mainframe (24 10/100/1000BASE-T, 4 100/1000BASE-X, AC 110/22
0V)
Manufactured=2011-08-22
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=




[Port_GigabitEthernet0/0/1]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=
BarCode=
Item=
Description=
Manufactured=
/$VendorName=
IssueNumber=
CLEICode=
BOM=
```

Table 3-12 Description of the **display elabel** command output

Item	Description
BoardIntegrationVersion	Version of the board software integration format.
ArchivesInfoVersion	Electronic label information version.
SystemIntegrationVersion	Version of the host software integration format.
BoardType	Vendor's component model of the specified component.
BarCode	Bar code of the specified component.

Item	Description
Item	BOM code of the specified component.
Description	English description of the specified component.
Manufactured	Production date of the specified component.
VendorName	Vendor name of the specified component.
IssueNumber	Issuing number of the specified component.
CLEICode	CLEI code of the specified component.
BOM	Sales BOM code of the specified component, which is an item number.

3.1.15 display esn

Function

The **display esn** command displays the Equipment Serial Number (ESN) of a device.

Format

display esn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ESN uniquely identifies a device.

In a stack, the **display esn** command displays the ESNs of all member devices.

Example

Display the ESN of the device.

```
<HUAWEI> display esn
ESN of slot 0: 21023586001xxxxxxxx
```

Table 3-13 Description of the display esn command output

Item	Description
ESN of slot 0	SN of the device with the slot ID 0.

3.1.16 display fan

Function

The **display fan** command displays the fan status.

Format

display fan [**power**]

NOTE

Only the following models support the power parameter:

S5731-H, S5731S-H, S5732-H, S5735-L, S5735S-L, S5736-S, and S6730-H

Parameters

Parameter	Description	Value
power	Indicates the fan speed of the power module.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Devices can run properly when fans are working properly. If proper heat dissipation cannot be ensured for devices, devices may overheat, damaging the hardware. You can use the **display fan** command to view the fan status.

Different device models may support different numbers of fans.

Example

Display the fan status of the device.

```
<HUAWEI> display fan
-------------------------------------------------------------------------------------------------------
 Slot  FanID   Online    Status    Speed     Mode     Airflow        Auto Min-Speed
Name
-------------------------------------------------------------------------------------------------------
 2        1   Present   Normal      34%     Auto     Front-to-Back              -   FAN-031A-
B
 2        2   Present   Normal      34%     Auto     Front-to-Back              -   FAN-031A-B
```

Table 3-14 Description of the **display fan** command output

Item	Description
Slot	Slot ID.
FAN	Number of a fan.
Online	Whether a fan is available: ● Present: available ● Absent: unavailable
Status	Running status of a fan: ● Normal: The fan is running normally. ● Abnormal: The fan works abnormally. ● -: The fan is not present.
Speed	Percentage of the current fan speed to the full speed. If this field displays -, the fan is not present or the fan works abnormally.
Mode	Working mode of a fan: ● AUTO: The fan speed can be automatically adjusted. ● MANUAL: The fan works at a fixed speed. ● -: The fan is not present or the fan works abnormally.
Airflow	Airflow direction of a fan: ● Back-to-Side: Air flows from the rear to the left and right sides. ● Side-to-Back: Air flows from the left and right sides to the rear. ● Side-to-Side: Air flows from one side to the other side. ● Front-to-Back: Air flows from the front to the rear. ● -: The fan is not present.

Item	Description
Auto Min-Speed	Minimum fan speed in automatic fan speed adjustment mode. To configure the minimum fan speed in automatic fan speed adjustment mode, run the **set fan speed auto min-speed** command. If this field displays -, this command is not supported, or the fan is not present, or the fan works abnormally.
Name	Name of a fan: **NOTE** The information is displayed only for the S5731-H, S5732-H, and S6730-H.

Display the fan speed of the power module.

```
<HUAWEI> display fan power
----------------------------------------
 Slot  FanID   Online    PowerSpeed
----------------------------------------
 1         1   Absent            -
 1         2   Present         46%
```

Table 3-15 display fan power command output

Item	Description
Speed	Fan speed of the power module.

3.1.17 display integrated-power information

Function

The **display integrated-power information** command displays information about the built-in or external power supply of an extended-temperature switch.

NOTE

This command is available only on the following switch models:

S5735-S4T2X-IA150G1, S5735-S8P2X-IA200G1, S5735-S8P2X-IA200H1, S5735-L8P4X-IA1, S5735-L8T4X-IA1

Format

display integrated-power information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command on an extended-temperature switch to check the version and working status of the built-in or external power supply.

Example

Display information about the built-in power supply of the S5735-S4T2X-IA150G1.

```
<HUAWEI> display integrated-power information
------------------------------------------------------------
 Integrated power information
------------------------------------------------------------
General information
   Software version             : 555
   Hardware version             : B
   Power supply mode            : Mains Power 500
   Total input power(W)         : 0.00
   AC input voltage status      : Normal
   12V DC output voltage status : Normal
   24V AC output voltage(V)     : 0.00
   24V AC output current(A)     : 0.00
   53V DC output voltage status : Normal
```

Table 3-16 Description of the **display integrated-power information** command output

Item	Description
Integrated power information	Information about the built-in power supply.
General information	Generic information about the built-in power supply.
Software version	Software version, in hexadecimal notation.
Hardware version	Hardware version, which is an ASCII value.
Power supply mode	Working mode of the built-in power supply.
Total input power(W)	Total input power, in Watt (W).
AC input voltage status	AC input voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.

Item	Description
12V DC output voltage status	12 V DC output voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
24V AC output voltage(V)	24 V AC output voltage, in Volt (V).
24V AC output current(A)	24 V AC output current, in amperes (A).
53V DC output voltage status	53 V DC output voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.

Display information about the built-in power supply of the S5735-S8P2X-IA200H1.

```
<HUAWEI> display integrated-power information
Info: This operation may take a few seconds. Please wait for a
moment..
------------------------------------------------------------
 Integrated power information
------------------------------------------------------------
General information
   Hardware version             : A
   Software version(ASCII)      : V100R021C10SPC000
   Power supply mode            : Hybrid Power 500(B)
   Current power supply mode    : Mains
   Busbar voltage(V)            : 54.26
   AC voltage(V)                : 218.69
   SSU input voltage(V)         : 0.00
   SSU input current(A)         : 0.00
   Total load power(W)          : 0.00
   Total input power(W)         : 0.00
   12V DC output voltage status : Normal
   24V AC output voltage(V)     : 0.00
   24V AC output current(A)     : 0.00
   53V DC output voltage(V)     : 54.50
```

Table 3-17 Description of the **display integrated-power information** command output

Item	Description
Integrated power information	Information about the built-in power supply.
General information	Generic information about the built-in power supply.
Hardware version	Hardware version. The value is in hexadecimal notation.
Software version(ASCII)	Software version. The value is in ASCII format.

Item	Description
Current power supply mode	Working mode of the built-in power supply.
Busbar voltage(V)	Busbar voltage, in volts (V).
AC voltage(V)	AC voltage, in volts (V).
SSU input voltage(V)	Input voltage of the solar supply unit (SSU), in volts (V).
SSU input current(A)	Input current of the SSU, in amperes (A).
Total load power(W)	Total load power, in watts (W).
Total input power(W)	Total input power, in watts (W).
12V DC output voltage status	12 V DC output voltage status: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
24V AC output voltage(V)	24 V AC output voltage, in volts (V).
24V AC output current(A)	24 V AC output current, in amperes (A).
53V DC output voltage(V)	53 V DC output voltage, in volts (V).
53V DC output current(A)	53 V DC output current, in amperes (A).
AC current(A)	AC current, in amperes (A).
Chip1 upgrade status	Upgrade status of chip 1: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
Chip2 upgrade status	Upgrade status of chip 2: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
Chip3 upgrade status	Upgrade status of chip 3: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.
Chip4 upgrade status	Upgrade status of chip 4: ● Normal: The voltage is normal. ● Abnormal: The voltage is abnormal.

Display information about the power supply connected to the S5735-L8P4X-IA1.

```
<HUAWEI> display integrated-power information
------------------------------------------------------------
```

```
 Integrated power information
------------------------------------------------------------
General information
   Hardware version             : B
   Software version             : V1.20
```

Table 3-18 Description of the **display integrated-power information** command output

Item	Description
Integrated power information	Information about the external power supply.
General information	Generic information about the built-in power supply.
Hardware version	Hardware version. The value is in hexadecimal notation.
Software version	Software version.

3.1.18 display memory-usage

Function

The **display memory-usage** command displays the memory usage of the device.

Format

display memory-usage [**slave** | **slot** *slot-id*] [**vcpu** *vcpu-index*]

NOTE

The **slave** parameter is not supported if the switch does not support the stacking function or does not have the stacking function enabled.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
slave	Displays memory usage of a slave switch in a stack. This parameter is valid only when multiple switches form a stack.	-
slot *slot-id*	Displays memory usage of a slot ID.	The value depends on the device configuration.

Parameter	Description	Value
vcpu *vcpu-index*	Specifies the virtual CPU number.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Memory usage is an important index to evaluate device performance. A high memory usage will cause service faults. You can use the **display memory-usage** command to view memory usage to check whether devices are working properly.

The memory usage displayed using the **display memory-usage** command is based on the total available memory of a process.

Example

Display memory usage of the current device.

```
<HUAWEI> display memory-usage
 Memory utilization statistics at 2008-12-15 15:17:42+08:00
 System Total Memory Is: 394152720 bytes
 Total Memory Used Is: 130975664 bytes
 Memory Using Percentage Is: 33%
```

Display memory usage of the virtual CPU 1 in slot 0.

```
<HUAWEI> display memory-usage slot 0 vcpu 1
 Vcpu 1 Memory utilization Info:
 Memory utilization statistics at 2017-08-26 06:11:20+00:00
 System Total Memory Is: 30408904 bytes
 Total Memory Used Is: 22938332 bytes
 Memory Using Percentage Is: 75%
```

Table 3-19 Description of the **display memory-usage** command output

Item	Description
Memory utilization statistics at	Time when memory usage is collected.
System Total Memory	Total memory of the device network operating system.
Total Memory Used	Total used memory of the device network operating system.
Memory Using Percentage	Memory usage.

3.1.19 display memory-usage threshold

Function

The **display memory-usage threshold** command displays the memory usage threshold on the device.

Format

display memory-usage threshold [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the memory usage threshold of a specified slot ID.	The value depends on the device configuration.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can view the memory usage alarm threshold to learn about the conditions for triggering alarms.

- When memory usage reaches the alarm threshold, the system generates an alarm.
- When memory usage falls within the alarm threshold, the system generates a clear alarm.

Example

Display the memory usage threshold on the main control board.

```
<HUAWEI> display memory-usage threshold
 Current memory threshold of the main board is 95%.
```

Table 3-20 Description of the display memory-usage threshold command output

Item	Description
Current memory threshold of the main board is 95%.	The memory usage threshold of the main control board is 95%. To set the memory usage threshold of the main control board, use the **set memory-usage threshold** *threshold-value* command.

3.1.20 display power

Function

The **display power** command displays information about all power supplies on the device.

Format

display power

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the status of all power supplies, and their power.

No information is displayed for built-in power supplies.

Example

Display the current power supply status.

```
<HUAWEI> display power
-----------------------------------------------------------------------
 Slot    PowerID  Online   Mode   State      Power(W)  CurrentPower(W)
-----------------------------------------------------------------------
 0       PWRI     Present  AC     Supply      500.00          70.50
 0       PWRII    Absent   -      -               -             -
```

Table 3-21 Description of the **display power** command output

Item	Description
Slot	• Slot ID if stacking is not configured. The value is 0. • Stack ID if stacking is configured. The value must be set according to the device configuration.

Item	Description
PowerID	ID of a power supply slot: ● PWRI: slot for a power module, or lead-acid battery board ● PWRII: slot for a power module **NOTE** On the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S series switches, the power supply slots are PWR1 and PWR2. If a device has only one power supply slot, only PWR1 is displayed.
Online	Whether a power supply is installed properly. ● Present: indicates that the power supply is installed properly. ● Absent: indicates that the power supply is not installed properly, or the power supply is a fixed power supply.
Mode	Type of the power module, or lead-acid battery board: ● AC: AC power module ● DC: DC power module ● –: Power supply invalid or absent ● PBB: Lead-acid battery board
State	Working status of a power module. ● Supply: Current is output. ● NotSupply: No current is output. ● –: Invalid or absent
Power(W)	Rated power of a power supply. If this field displays –, the power supply is invalid or is not installed properly.
CurrentPower(W)	Real-time power of a power supply. If this field displays –, the power supply is not supported.

3.1.21 display system-software information

Function

The **display system-software information** command displays the software versions supported by the device.

NOTE

Only the S1730S-S1, S200, S2730S-S, S300, S500, S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S5735-L, S5735S-L, S5735-L1, S5735S-L1, S5735S-L-M, S5735-S, S5735-S-I, S5735S-S, S5735S-H, S5736-S, S6730-H, S6730-S, and S6735-S support this command.

Format

display system-software information

Parameters

None

Views

User views

Default Level

3: Management level

Usage Guidelines

Before upgrading a device, you can run this command to check the software versions supported by the device. This helps you select a software package supported by the device. Some models cannot be downgraded due to component upgrade. Before downgrading a device, run this command to check the software versions supported by the device.

Example

Display the software versions supported by the device.

```
<HUAWEI> display system-software information
Slot 0:
Device type        : S5735S-L48T4X-A
Supported versions : V200R021C00 and later versions
```

Table 3-22 Description of the **display system-software information** command output

Item	Description
Slot	Slot ID.
Device type	Device model.

Item	Description
Supported versions	Software versions to which the device can be upgraded.

3.1.22 display software information

Function

The **display software information** command displays information about the current system software package.

Format

display software information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before upgrading a device, you can run this command to check whether the current startup software package is supported by the device.

Example

Display the software version supported by the device.

```
<HUAWEI> display software information
Startup software name      : xxxx.cc
Startup software file name : xxxx.cc
```

Table 3-23 Description of the **display software information** command output

Item	Description
Startup software name	Name of the software package supported by the device.
Startup software file name	Name of the current startup software package.

3.1.23 display transceiver

Function

The **display transceiver** command displays information about the optical module on an interface.

NOTE

The command displays only information about optical interfaces.

Format

display transceiver [**interface** *interface-type interface-number* | **slot** *slot-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
verbose	Displays detailed information about the optical module on an interface, including the general information, manufacture information, alarm information, and diagnostic information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view general information, manufacture information, and alarm information about an optical module. If you specify the **verbose** keyword, diagnostic information is also displayed in addition to the preceding information.

If a device does not support optical modules, a message will be displayed after you run this command.

Some parameters including the current and optical power will be displayed for each lane of the 40GE interfaces.

Example

Display general information, manufacture information, and alarm information about the optical module on a specified interface.

```
<HUAWEI> display transceiver interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 transceiver information:
-------------------------------------------------------------
Common information:
  Transceiver Type              :1000_BASE_SX_SFP
  Connector Type                :LC
  Wavelength(nm)                :850
  Transfer Distance(m)          :0(9um),300(50um),150(62.5um)
  Digital Diagnostic Monitoring  :YES
  Vendor Name                   :HUAWEI
  Vendor Part Number            :02315204
  Ordering Name                 :
-------------------------------------------------------------
Manufacture information:
  Manu. Serial Number           :CD25HP12M
  Manufacturing Date            :2013-06-184
  Vendor Name                   :HUAWEI
-------------------------------------------------------------
```

Display general information, manufacture information, alarm information and diagnostic information about the optical module on a specified interface.

```
<HUAWEI> display transceiver interface gigabitethernet 0/0/3 verbose
GigabitEthernet0/0/3 transceiver information:
-------------------------------------------------------------
Common information:
  Transceiver Type              :GPS_SFP
  Connector Type                :SMA Coaxial Connector
  Wavelength(nm)                :-
  Transfer Distance(m)          :100(copper)
  Digital Diagnostic Monitoring  :NO
  Vendor Name                   :HUAWEI
  Vendor Part Number            :HUAWEI AE 905S A
  Ordering Name                 :
-------------------------------------------------------------
Manufacture information:
  Manu. Serial Number           :031TUX10HB000065
  Manufacturing Date            :2017-11-28
  Vendor Name                   :HUAWEI
-------------------------------------------------------------
Diagnostic information:
  Temperature(°C)               :26.00
  Temp High Threshold(°C)       :85.00
  Temp Low  Threshold(°C)       :-40.00
  Voltage(V)                    :3.29
  Volt High Threshold(V)        :3.64
  Volt Low  Threshold(V)        :2.95
  Bias Current(mA)              :4.57
```

```
  Bias High Threshold(mA)       :9.00
  Bias Low  Threshold(mA)       :2.00
  RX Power(dBM)                 :-40.00
  RX Power High Warning(dBM)    :-1.00
  RX Power Low  Warning(dBM)    :-15.80
  RX Power High Threshold(dBM)  :0.00
  RX Power Low  Threshold(dBM)  :-16.99
  TX Power(dBM)                 :-5.03
  TX Power High Warning(dBM)    :4.00
  TX Power Low  Warning(dBM)    :-4.70
  TX Power High Threshold(dBM)  :-2.22
  TX Power Low  Threshold(dBM)  :-6.99
  Transceiver phony alarm       :Yes
-------------------------------------------------------------

<HUAWEI> display transceiver interface xgigabitethernet 0/0/4 verbose
XGigabitEthernet0/0/4 transceiver information:
-------------------------------------------------------------
Common information:
  Transceiver Type              :GPS_SFP
  Connector Type                :SMA Coaxial Connector
  Wavelength(nm)                :-
  Transfer Distance(m)          :100(copper)
  Digital Diagnostic Monitoring  :NO
  Vendor Name                   :HUAWEI
  Vendor Part Number            :HUAWEI AE 905S A
  Ordering Name                 :
-------------------------------------------------------------
Extended information:
  Longitude(° )                 :118.7662952
  Latitude(° )                  :31.9829019
  Altitude(mm)                  :75051
-------------------------------------------------------------
Manufacture information:
  Manu. Serial Number           :031TUX10HB000065
  Manufacturing Date            :2017-11-28
  Vendor Name                   :HUAWEI
-------------------------------------------------------------
Diagnostic information:
  Transceiver does not support diagnostic information.
-------------------------------------------------------------
```

Table 3-24 Description of the **display transceiver** command output

Item	Description
Common information	Generic information about the optical module.
Transceiver Type	Type of the optical module.
Connector Type	Type of the fiber connector required by the optical module. The value depends on the protocol related to the optical module.
Wavelength (nm)	Wavelength of the optical module. If this field displays -, the optical module does not have wavelength information.

Item	Description
Transfer Distance (m)	Transmission distance of the optical module. 50 um and 62.5 um are fiber diameters. Fibers with a diameter of 50 um or 62.5 um are multimode fibers. Fibers with a diameter of 9 um are single-mode fibers. For a GPS module, this field indicates the maximum length of the antenna between the GPS module and signal receiver. **NOTE** Only the maximum transmission distance of the optical module is displayed if different optical fibers are used.
Digital Diagnostic Monitoring	Whether diagnostic information about the optical module is monitored.
Vendor Name	Vendor name of the optical module. If the system has not determined whether the optical module is a Huawei-customized one, this field displays Judging. If the vendor name of an optical module is not HUAWEI, check whether the optical module is a Huawei-certified optical module. For details, see "How Can I Determine Whether an Optical Module Is Huawei-Certified?" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management – Device Status Query*.
Vendor Part Number	Vendor part number or product name. If the system has not determined whether the optical module is a Huawei-customized one, this field displays Judging.
Ordering Name	External name of the optical module. Currently, this field is not supported and is empty.
Extended information	GPS module information. Only the S5720I-SI and S5735-S-I support this item.
Longitude(°)	Longitude of the location of the GPS module. Only the S5720I-SI and S5735-S-I support this item.
Latitude(°)	Latitude of the location of the GPS module. Only the S5720I-SI and S5735-S-I support this item.
Altitude(mm)	Altitude of the location of the GPS module. Only the S5720I-SI and S5735-S-I support this item.
Manufacture information	Manufacture information of the optical module.
Manu. Serial Number	Vendor sequence number of the optical module.
Manufacturing Date	Manufacturing date of the optical module.

Item	Description
Diagnostic information	Diagnostic information about the optical module.
Temperature (°C)	Current temperature of the optical module.
Temp High Threshold (°C)	Upper temperature threshold for the optical module.
Temp Low Threshold (°C)	Lower temperature threshold for the optical module.
Voltage (V)	Current voltage of the optical module.
Volt High Threshold(V)	Upper voltage threshold for the optical module.
Volt Low Threshold(V)	Lower voltage threshold for the optical module.
Bias Current (mA)	Bias current of the optical module.
Bias High Threshold (mA)	Upper threshold for the bias current of the optical module.
Bias Low Threshold (mA)	Lower threshold for the bias current of the optical module.
RX Power (dBM)	Input power of the optical module. When the Input power is 0 W, **-Inf** is displayed.
RX Power High Warning(dBM)	Upper warning threshold for the receive power of the optical module.
RX Power Low Warning(dBM)	Lower warning threshold for the receive power of the optical module.
RX Power High Threshold (dBM)	Upper input power threshold for the optical module.
RX Power Low Threshold (dBM)	Lower input power threshold for the optical module.
TX Power (dBM)	Output power of the optical module. When the output power is 0 W, **-Inf** is displayed.
TX Power High Warning(dBM)	Upper warning threshold for the transmit power of the optical module.
TX Power Low Warning(dBM)	Lower warning threshold for the transmit power of the optical module.
TX Power High Threshold (dBM)	Upper output power threshold for the optical module.

Item	Description
TX Power Low Threshold (dBM)	Lower output power threshold for the optical module.
Transceiver phony alarm:Yes	The device has generated an alarm on an optical module not certified for Huawei switches. This field is displayed only when the following conditions are met: ● The device is enabled to generate alarms on non-Huawei-customized optical modules. This alarm function is enabled by default. If it is disabled, you can run the **undo transceiver phony-alarm-disable** command to enable it. ● This optical module is a non-Huawei-customized one.

3.1.24 display transceiver diagnosis interface

Function

The **display transceiver diagnosis interface** command displays the diagnosis parameters of an optical module.

Format

display transceiver diagnosis interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display transceiver diagnosis interface** command to view digital diagnostic monitoring (DDM) information about optical modules installed on all interfaces of a device.

If *interface-type interface-number* is specified, only diagnostic information about the optical module installed on the specified interface is displayed.

Example

Display the diagnosis parameters of the optical module installed in GigabitEthernet0/0/4.

```
<HUAWEI> display transceiver diagnosis interface gigabitethernet 0/0/4
Port GigabitEthernet0/0/4 transceiver diagnostic information:
-------------------------------------------------------------------------------------
Item                  Value    HighAlarm     HighWarn     LowAlarm      LowWarn     Status
-------------------------------------------------------------------------------------
TxPower lane0(dBm)      0.23        7.00        4.00       -7.40       -4.40    Normal
TxPower lane1(dBm)     -1.56        7.00        4.00       -7.40       -4.40    Normal
RxPower lane0(dBm)      0.06        7.00        4.00      -11.20       -8.20    Normal
RxPower lane1(dBm)     -1.42        7.00        4.00      -11.20       -8.20    Normal
Current lane0(mA)       7.03       12.00       10.00        3.00        5.00    Normal
Current lane1(mA)       6.04       12.00       10.00        3.00        5.00    Normal
Temperature(C)         47.97       80.00       70.00      -10.00        0.00    Normal
Voltage(V)              3.35        3.63        3.46        2.97        3.13    Normal
LaserTemp(C)               -           -           -           -           -    -
TecCurrent(mA)             -           -           -           -           -    -
MediaSNR(dB)               -           -           -           -           -    -
-------------------------------------------------------------------------------------

Versatile Diagnostics Monitoring:
-------------------------------------------------------------------
Item          Minimum      Maximum      Average      Current PriorPeriod
-------------------------------------------------------------------
Ber          5.56e-10     8.22e-10     6.75e-10     7.07e-10    0.00e+00
Fer          0.00e+00     0.00e+00     0.00e+00     0.00e+00    0.00e+00
-------------------------------------------------------------------
```

NOTE

If the parameter displays **-**, the parameter value cannot be obtained. If the **Status** field displays **-**, this parameter does not support diagnosis.

Table 3-25 Description of the **display transceiver diagnosis interface** command output

Item	Description
Item	Parameter type.
Value	Real-time value of a parameter.
HighAlarm	Upper alarm threshold.
HighWarn	Upper warning threshold.
LowAlarm	Lower alarm threshold.
LowWarn	Lower warning threshold.

Item	Description
Status	Parameter value status: - **Normal**: indicates that the current value is within the normal range, that is, the current value does not exceed the upper alarm threshold or fall below the lower upper alarm threshold. - **Abnormal**: indicates that the current value is not within the normal range.
TxPower lane0(dBm) TxPower lane1(dBm)	Transmit power of an optical module. lane*i* indicates a physical channel. If an optical module has multiple physical channels, this parameter is displayed multiple times.
RxPower lane0(dBm) RxPower lane1(dBm)	Indicates the receiving power of the optical module, in dBm.lane*i* indicates a physical channel. If an optical module has multiple physical channels, this parameter is displayed multiple times.
Current lane0(mA) Current lane1(mA)	Indicates the current of the optical module, in mA. lane*i* indicates a physical channel. If an optical module has multiple physical channels, this parameter is displayed multiple times.
Temperature(C)	Indicates the temperature of the optical module, in degree Celsius.
Voltage(V)	Indicates the voltage of the optical module, in V.
LaserTemp(C)	Laser temperature of an optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
TecCurrent(mA)	Indicates the tec current of the optical module.If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
MediaSNR(dB)	Indicates the media SNR of the optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
Ber	BER of an optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
Fer	FER of an optical module. If an optical module has multiple channels, this parameter is displayed for multiple times for lane 0, lane 1, and so on.
Minimum	Minimum BER and FER of an optical module.

Item	Description
Maximum	Maximum BER and FER of an optical module.
Average	Average BER and FER of an optical module.
Current	Real-time BER and FER of an optical module.
PriorPeriod	BER and FER of an optical module in the previous period.

3.1.25 display temperature

Function

The **display temperature** command displays the working status temperature information of the device's internal components.

Format

display temperature { **all** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
all	Displays the working status temperature information of internal components in all slots on the device.	-
slot *slot-id*	Displays the working status temperature information of internal components on the specified slot.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A high or low device temperature may damage the hardware. This command displays the working status temperature information of internal components instead of the operating temperature that indicates the temperature range of the surrounding environment. When the device temperature exceeds the upper threshold or falls below the lower threshold, the device generates an alarm to alert you that the device temperature is abnormal.

Example

Display the working status temperature information of internal components in all slots.

```
<HUAWEI> display temperature all
-------------------------------------------------------------------------------
 Slot  Card  Sensor Status    Current(C) Lower(C) Lower     Upper(C) Upper
                                          Resume(C)         Resume(C)
-------------------------------------------------------------------------------
0     NA    NA     Normal          44        0        4       72        68
```

Table 3-26 Description of the **display temperature** command output

Item	Description
Slot	Slot ID.
Card	Subcard ID. This field is invalid on the device and displays NA.
Sensor	Number of a sensor on a card. This field is invalid on the device and displays NA.
Status	Temperature status of a device. ● Normal: The device temperature is within the normal range. ● Abnormal: The device temperature is out of the normal range.
Current(C)	Working status temperature information of internal components of a device, expressed in the centigrade scale (°C). The temperature value is displayed as an integer, so there may be a maximum of 1°C error between the displayed value and actual temperature. This field displays - when the sensor is abnormal or the obtained temperature is higher than 200°C or lower than 100°C.
Lower(C)	Low-temperature alarm threshold, expressed in the centigrade scale (°C). To set the low-temperature alarm threshold, run the **temperature threshold** command.
Lower Resume(C)	Low-temperature alarm clear threshold, expressed in the centigrade scale (°C). To set the low-temperature alarm clear threshold, run the **temperature threshold** command. The low-temperature alarm clear threshold is 4°C higher than the low-temperature alarm threshold.

Item	Description
Upper(C)	High-temperature alarm threshold, expressed in the centigrade scale (°C). To set the high-temperature alarm threshold, run the **temperature threshold** command. On the devices that support fan speed adjustment using the **set fan speed-adjust threshold minus** command, the default value of this field changes based on the PoE power load.
Upper Resume(C)	High-temperature alarm clear threshold, expressed in the centigrade scale (°C). To set the high-temperature alarm clear threshold, run the **temperature threshold** command. The high-temperature alarm clear threshold is 4°C lower than the high-temperature alarm threshold.

3.1.26 display version

Function

The **display version** command displays the device version.

Format

display version [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display version** command to view the device version to determine whether the device needs to be upgraded.

Example

Display the device version.

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S6720
V200R023C00)
Copyright (C) 2000-2020 HUAWEI TECH Co.,
Ltd.
HUAWEI S6720-54C-EI-48S-AC Routing Switch uptime is 0 week, 0 day, 0 hour, 5
minutes

ES5D2S50Q002 1(Master)  : uptime is 0 week, 0 day, 0 hour, 2
minutes
DDR             Memory Size : 2048  M bytes
FLASH Total     Memory Size : 512   M bytes
FLASH Available Memory Size : 446   M bytes
Pcb           Version   : VER.B
BootROM       Version   : 020b.0001
BootLoad      Version   : 020b.0001
CPLD          Version   : 0108
Software      Version   : VRP (R) Software, Version 5.170
(V200R023C00)
FLASH         Version   : 0000
CARD1 information
Pcb           Version   : ES5D21Q04Q01 VER.A
CPLD   Version          : 0105
PWR2 information
Pcb           Version   : PWR VER.A
FAN1 information
Pcb           Version   : NA
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5730 V200R023C00)
Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.
HUAWEI S5730-60C-HI-48S Routing Switch uptime is 0 week, 0 day, 13 hours, 49
minutes

ES5D2S52C004 1(Master)  : uptime is 0 week, 0 day, 13 hours, 47
minutes
DDR             Memory Size : 4096  M bytes
FLASH Total     Memory Size : 1024  M bytes
FLASH Available Memory Size : 842   M bytes
SSD             Memory Size : 223   G bytes
Pcb           Version   : VER.A
BootROM       Version   : 020d.0000
BootLoad      Version   : 020d.0000
CPLD          Version   : 0102
Software      Version   : VRP (R) Software, Version 5.170
(V200R023C00)
FLASH         Version   : 0000
CARD1 information
Pcb           Version   : ES5D21X08T00 VER.C
CPLD          Version   : 010c
PWR1 information
Pcb           Version   : PWR VER.A
FAN1 information
Pcb           Version   : NA
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5735 V200R023C00)
Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.
HUAWEI S5735-S8P2X-IA200G1 Routing Switch uptime is 0 week, 0 day, 0 hour, 0 minute

ES5D2V10S005 0(Master)  : uptime is 0 week, 0 day, 0 hour, 0 minute
DDR             Memory Size : 1024  M bytes
FLASH Total     Memory Size : 512   M bytes
FLASH Available Memory Size : 303   M bytes
```

```
Pcb           Version   : VER.A
BootROM       Version   : 0000.03e8
BootLoad      Version   : 0213.0000
CPLD          Version   : 0100
MCU           Version   : 1.9.10.1
Software      Version   : VRP (R) Software, Version 5.170 (V200R023C00)
FLASH         Version   : 0000.0000
Power         Version   : 0555
```

Table 3-27 Description of the display version command output

Item	Description
Huawei Versatile Routing Platform Software	-
VRP (R) software, Version	Versions of the VRP and the software of the device.
Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.	Huawei copyright.
Routing Switch uptime	System power-on time.
ES5D2S50Q002 1(Master) : uptime	Hardware type, role, and startup time of the device. **NOTE** The names in the instance are taken as an example.
DDR Memory Size	Device's physical memory capacity, which stores data when the program is running. The **System Total Memory** field value displayed using the **display memory-usage** command is part of the physical memory capacity and varies depending on the device model.
FLASH Total Memory Size	Total size of the flash memory.
FLASH Available Memory Size	Available flash memory size. This value is the **total** field value displayed using the **dir** command divided by 1024.
Pcb Version	Version of the printed circuit board (PCB).
MAB Version	MAB version information.
BootROM Version	Version of the BootROM software.
BootLoad Version	Version of the BootLoad software.
CPLD Version	Version of the complex programmable logic device (CPLD).

Item	Description
MCU Version	Micro Control Unit (MCU) version. **NOTE** The information is displayed only for the S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, and the PoE devices of S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5732-H, S5735S-H, and S5736-S.
Software Version	Versions of the VRP and the software of the device.
FLASH Version	Version of the flash memory.
Power Version	Firmware version of the power module. **NOTE** The information is displayed only for the PoE devices of S5735-S-I.
CARD1 information	Information about a front card. If no front card is available, this field is not displayed.
CARD2 information	Information about a rear card. If no rear card is available, this field is not displayed.
FAN1 information	Information about a pluggable fan module. If no pluggable fan module is available, this field is not displayed. If a pluggable fan module does not have an electronic label, its PCB version is displayed as NA.
PWR2 information	Information about a pluggable power module. If no pluggable power module is available, this field is not displayed. If a pluggable power module does not have an electronic label, its PCB version is displayed as NA.
RPS Version	RPS management software version. If the device does not support RPS, this information is not displayed.

3.2 Hardware Configuration Commands

3.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.2.2 assign resource-mode

Function

The **assign resource-mode** command configures the resource allocation mode of the device.

The **undo assign resource-mode** command restores the default resource allocation mode of the device.

By default, the resource allocation mode of the S5731-H, S5731S-H, S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,S5735S-L1, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S, S6720-EI, and S6720S-EI is enhanced-arp.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,S5735S-L1, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S, S6720-EI, and S6720S-EI support this command.

Format

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-ipv4** | **ipv4-ipv6 6:1** | **super-arp** } [**slot** *slot-id* | **all**] (S6720-EI and S6720S-EI)

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-ipv4** | **super-arp** } [**slot** *slot-id* | **all**] (S6735-S)

assign resource-mode { **enhanced-arp** | **enhanced-sac** | **enhanced-sipfpm** | **eca** | **sac** } [**slot** *slot-id* | **all**] (S5731-H, S5731S-H, S5731-S, and S5731S-S)

assign resource-mode { **enhanced-arp** | **enhanced-sac** | **enhanced-sipfpm** | **sac** } [**slot** *slot-id* | **all**] (S6730-S, S6730S-S, and S5732-H)

assign resource-mode { **enhanced-mac** | **enhanced-arp** | **enhanced-fib** | **enhanced-sac** | **sac** | **enhanced-sipfpm** } [**slot** *slot-id* | **all**] (S6730-H and S6730S-H)

assign resource-mode { **enhanced-mac** | **enhanced-arp** } **global** (S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,and S5735S-L1)

undo assign resource-mode global (S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,and S5735S-L1)

undo assign resource-mode [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
enhanced-mac	Sets the resource allocation mode to enhanced-mac.	-

Parameter	Description	Value
enhanced-ipv4	Sets the resource allocation mode to enhanced-ipv4.	-
enhanced-ipv6	Sets the resource allocation mode to enhanced-ipv6.	-
enhanced-arp	Sets the resource allocation mode to enhanced-arp.	-
enhanced-fib	Sets the resource allocation mode to enhanced-fib.	-
enhanced-sac	Sets the resource allocation mode to enhanced-sac.	-
enhanced-sipfpm	Sets the resource allocation mode to enhanced-sipfpm.	-
ipv4-ipv6 6:1	Sets the resource allocation mode to ipv4-ipv6 6:1.	-
super-arp	Sets the resource allocation mode to super-arp.	-
eca	Sets the resource allocation mode to eca.	-
sac	Sets the resource allocation mode to sac.	-
slot *slot-id*	● Specifies a slot ID on a standalone switch where stacking is not enabled. ● Specifies a stack ID in a stack.	In a stack, the value is an integer and must be set according to the configuration in the stack. On a standalone switch where stacking is not enabled, the default value is 0.
all	Configures a resource allocation mode for all devices that are present in slots.	-

Parameter	Description	Value
global	Configures the resource allocation mode of the system.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device's MAC address entries, FIB entries, or ARP entries are insufficient to meet service requirements, you can use this command to change the resource allocation mode so as to extend the entry space.

Precautions

- The configured resource allocation mode takes effect only after the configuration is saved and the device is restarted. To view the resource allocation modes that take effect currently and take effect after the device restarts, run the **display resource-mode configuration** command.
- The requirements for different entry spaces will change when service configuration is adjusted. In this case, you can change the resource allocation mode to meet the new service requirements. Subsequently, entry spaces in different resource allocation modes will change. Therefore, before changing the resource allocation mode, consider the benefit and loss that the new mode will bring.
- In versions earlier than V200R012C00, the resource allocation mode used by the device is recorded in only the flash memory but not the configuration file. In V200R012C00 and later versions, the resource allocation mode used by the device is recorded in both the flash memory and configuration file. If the resource allocation mode used by the device is not the default mode, and the **save** command is executed to save the configuration after the device is upgraded to V200R012C00 or later, the corresponding configuration is added to the configuration file.
- In a stack, member switches synchronize MAC addresses with each other. Therefore, the MAC address specifications of the stack are not the sum of MAC address specifications of multiple member switches.
  - If member switches have the same MAC address specifications, the MAC address specifications of the stack are those of any member switch.
  - If member switches have different MAC address specifications, when uplink and downlink traffic is forwarded by the same member switch, the MAC address specifications of the stack are those of the member switch. When uplink and downlink traffic is forwarded across member switches,

the MAC address specifications of the stack are those of the member switch with smaller MAC address specifications.

When the resource allocation mode of the following models is changed, the specifications of MAC, FIB, ARP, ND, or multicast entries will be modified.

Table 3-28 Number of entries supported in different resource allocation modes on the S5731-H and S5731S-H

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
enhanced-sac	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
enhanced-sipfpm	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
eca	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000
sac	288K	512K(share)	64K(share)	128K(share)	64K(share)	16K(share)	16K(share)	10000

NOTE

On the S5731-H and S5731S-H, when the resource allocation mode is set to **enhanced-sipfpm**, the specifications of MAC, FIB, ARP, ND, and multicast entries will not be modified, and NetStream aggregation flows cannot be configured.

Table 3-29 Number of entries supported in different resource allocation modes on the S5731-S and S5731-S-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp	64K	32K	8K	16K	8K	1K	1K	10000

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-sac	64K	32K	8K	16K	8K	1K	1K	10000
enhanced-sipfpm	64K	16K 32K	8K	16K	8K	1K	1K	10000
eca	64K	32K	8K	16K	8K	1K	1K	10000
sac	64K	32K	8K	16K	8K	1K	1K	10000

NOTE

On the S5731-S and S5731-S-S, when the resource allocation mode is set to **enhanced-sipfpm**, the specifications of MAC, FIB, ARP, ND, and multicast entries will not be modified, and NetStream aggregation flows cannot be configured.

Table 3-30 Number of entries supported in different resource allocation modes on the S5732-H

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp (default)	128K	192K (shared)	80K (shared)	140K (shared)	80K (shared)	64K-1 (shared)	4K	10000
sac	96K	192K (shared)	80K (shared)	96K (shared)	80K (shared)	64K-1 (shared)	4K	10000
enhanced-sac	96K	64K(Share)	24K(Share)	96K(Share)	80K(Share)	20(Share)	4K	10000

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-sipfpm	32K	128K(Share)	64K(Share)	128K(Share)	64K(Share)	4K(Share)	4K	10000

NOTE

On the S5732-H, IPv4 FIB, IPv6 FIB, ARP, ND, and Multicast IPv4 share hardware resources. The specifications listed in the preceding table indicate the maximum number of entries of a single type and cannot reach the maximum value simultaneously.

Table 3-31 Number of entries supported in different resource allocation modes on the S500, S5735-S, and S5735S-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp(Default)	16512	8192	3072	8180(share)	3072(share)	1500(Share)	1500(Share)	N/A
enhanced-mac	32896(Share)	128	64	128(share)	64(share)	128	64(Share with Multicast Ipv4)	N/A

Table 3-32 Number of entries supported in different resource allocation modes on the S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735-L-I, S5735-L1,and S5735S-L1

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp(Default)	16512	4096	1024	4096	1024	1500	1500	N/A
enhanced-mac	32896(Share)	128	64	128(share)	64(share)	128	64(Share with Multicast Ipv4)	N/A

Table 3-33 Number of entries supported in different resource allocation modes on the S6720-EI and S6720S-EI

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
enhanced-arp (default)	160K	12K	6K (shared with IPv4 FIB)	1K	48K	44K (shared with ARP)	4000	2K
enhanced-mac	288K	12K	6K (shared with IPv4 FIB)	1K	16K	8K (shared with ARP)	4000	2K
enhanced-ipv4	32K	256000	128K (shared with IPv4 FIB)	0K	16K	8K (shared with ARP)	4000	2K
ipv4-ipv6 6:1	32K	64K	10K	10K	16K	8K (shared with ARP)	4000	2K

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
super-arp	96K	12K	6K (shared with IPv4 FIB)	1K	128K	48K (shared with ARP)	4000	2K

NOTE

- On the S6720-EI and S6720S-EI, ARP and ND share hardware resources. The value listed in the preceding table indicates the maximum number of entries of a single type. Numbers of the two types of entries cannot reach the maximum value simultaneously.
- When the S6720-EI and S6720S-EI work in enhanced-arp, enhanced-mac, enhanced-ipv4, or super-arp mode, IPv4 FIB and IPv6 FIB (0-64 bits mask) share hardware resources. The value listed in the preceding table indicates the maximum number of FIB entries of a single type. Numbers of the two types of FIB entries cannot reach the maximum value simultaneously.
- When the S6720-EI and S6720S-EI work in ipv4-ipv6 6:1 mode, IPv6 FIB (0-64 bits mask) and IPv6 FIB (over 64 bits mask) share hardware resources. The value listed in the preceding table indicates the maximum number of FIB entries of a single type. Numbers of the two types of FIB entries cannot reach the maximum value simultaneously.
- On the S6720-EI and S6720S-EI, if the **assign resource-mode** command sets the resource allocation mode to enhanced-ipv4 or ipv4-ipv6 6:1, and the **ipv4 destination-unreachable drop** or **ipv6 destination-unreachable drop** command has been executed, the function that dropping the packets that do not match routing entries does not take effect.
- On the S6720-EI and S6720S-EI, redirection to a low-priority next hop is not supported in enhanced-ipv4 or ipv4-ipv6 6:1 resource allocation mode.
- On the S6720-EI and S6720S-EI, MPLS and Layer 3 VXLAN Gateway are not supported in super-arp resource allocation mode.

Table 3-34 Number of entries supported in different resource allocation modes on the S6735-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
enhanced-arp (default)	160K	12K	6K (shared with IPv4 FIB)	1K	48K	44K (shared with ARP)	4000	2K

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB (0-64 Bits Mask)	IPv6 FIB (Over 64 Bits Mask)	ARP	ND	Multicast IPv4 &IPv6	Number of NAC Users
enhanced-mac	288K	12K	6K (shared with IPv4 FIB)	1K	16K	8K (shared with ARP)	4000	2K
enhanced-ipv4	32K	256000	128K (shared with IPv4 FIB)	0K	16K	8K (shared with ARP)	4000	2K
super-arp	96K	12K	6K (shared with IPv4 FIB)	1K	128K	48K (shared with ARP)	4000	2K

NOTE

- On the S6735-S, ARP and ND share hardware resources. The value listed in the preceding table indicates the maximum number of entries of a single type. Numbers of the two types of entries cannot reach the maximum value simultaneously.
- When the S6735-S works in enhanced-arp, enhanced-mac, enhanced-ipv4, or super-arp mode, IPv4 FIB and IPv6 FIB (0-64 bits mask) share hardware resources. The value listed in the preceding table indicates the maximum number of FIB entries of a single type. Numbers of the two types of FIB entries cannot reach the maximum value simultaneously.
- On the S6735-S, if the **assign resource-mode** command sets the resource allocation mode to enhanced-ipv4, and the **ipv4 destination-unreachable drop** or **ipv6 destination-unreachable drop** command has been executed, the function that dropping the packets that do not match routing entries does not take effect.
- On the S6735-S, redirection to a low-priority next hop is not supported in enhanced-ipv4 resource allocation mode.
- On the S6735-S, MPLS and Layer 3 VXLAN Gateway are not supported in super-arp resource allocation mode.

Table 3-35 Number of entries supported in different resource allocation modes on the S6730-S and S6730S-S

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp(Default)	64K	64K	32K	64K	32K	4K	4K	N/A
enhanced-sac	64K	64K	32K	64K	32K	4K	4K	N/A
enhanced-sipfpm	64K	64K	32K	64K	32K	4K	4K	N/A

NOTE

On the S6730-S and S6730S-S, when the resource allocation mode is set to **sac**, **enhanced-sipfpm**, or **enhanced-sac**, the specifications of MAC, FIB, ARP, ND, and multicast entries will not be modified.

Table 3-36 Number of entries supported in different resource allocation modes on the S6730-H and S6730S-H

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-arp (default)	128K	192K (shared)	80K (shared)	140K (shared)	80K (shared)	64K-1 (shared)	4K	10000
enhanced-mac	384K	32K	8K	32K (shared with FIBv4)	8K (shared with FIBv6)	4K	4K	8K
enhanced-fib	32K	256K (shared)	80K (shared)	128K (shared)	80K (shared)	4K	4K	8K

Resource Allocation Mode	MAC	IPv4 FIB	IPv6 FIB	ARP	ND	Multicast IPv4	Multicast IPv6	Number of NAC Users
enhanced-sac	96K	148K(Share)	80K(Share)	96K(Share)	80K(Share)	64K-1(Share)	4K	10000
sac	96K	192K (shared)	80K (shared)	96K (shared)	80K (shared)	64K-1 (shared)	4K	10000
enhanced-sipfpm	32K	128K(Share)	64K(Share)	128 K(Share)	64K(Share)	4K	4K	8K

NOTE

On the S6730-H and S6730S-H, the value listed in the preceding table indicates the maximum number of entries of a single type. Numbers of the two types of entries cannot reach the maximum value simultaneously. For example, ARP and FIBv4 share hardware resources, while ND and FIBv6 share hardware resources.

Example

Set the resource allocation mode to enhanced-ipv4.

```
<HUAWEI> system-view
[HUAWEI] assign resource-mode enhanced-ipv4
Info: It is executing, please wait...
Info: The resource mode in slot 0 has been set to enhanced-ipv4
successfully.
Warning: It will take effect after rebooting this device.
```

3.2.3 backup elabel

Function

The **backup elabel** command backs up electronic labels of the device to the flash memory. The default file name format is elabel-slot*slotid*.fls, for example, elabel-slot0.fls.

The **backup elabel ftp** command backs up electronic labels of the device to a specified FTP server.

The **backup elabel sftp** command backs up electronic labels of the device to a specified SFTP server.

Format

backup elabel [**slot** *slot-id* [*subcard-id*]]

backup elabel ftp *ftp-server-address filename username password* [**slot** *slot-id* [*subcard-id*]]

backup elabel sftp *sftp-server-address filename username password* [**slot** *slot-id* [*subcard-id*]]

Parameters

Parameter	Description	Value
ftp-server-address	Specifies the IP address of the FTP server that stores electronic labels.	The value is in dotted decimal notation.
sftp-server-address	Specifies the IP address of the SFTP server that stores electronic labels.	The value is in dotted decimal notation.
filename	Specifies the name of the file that stores electronic labels.	The value is a string of 5 to 28 case-sensitive characters without spaces, in the format of elabel-slot*slotid*.fls, for example, elabel-slot0.fls.
username	Specifies the user name used to log in to the FTP or SFTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password	Specifies the password used to log in to the FTP or SFTP server.	The value is a string of 1 to 16 case-sensitive characters without spaces.
slot *slot-id*	Specifies the slot ID.	The value must be set according to the device configuration.
subcard-id	Specifies the subcard ID.	The value must be set according to the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

When electronic labels are stored on a device, run the **backup elabel** command to save electronic labels to a file. This file can be saved to the flash memory, to the

FTP or SFTP server using FTP or SFTP. FTP cannot ensure secure file transfer. SFTP is recommended on networks that require high security.

Example

Save electronic labels of the device to the **elabel-slot0.fls** file in the flash memory.

```
<HUAWEI> backup elabel slot 0
Info: Output information to file: flash:/elabel-slot0.fls. Please wait for a mom
ent...

Info: Put file to flash successfully.
```

Save electronic labels of the device to FTP server 192.168.12.91. Set the FTP user name to **user** and password to **123**. Save electronic labels in the **elabel-slot0.fls** file.

```
<HUAWEI> backup elabel ftp 192.168.12.91 elabel-slot0.fls user 123
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: It is executing, please wait...

Info: Put file to FTP server successfully.
```

Save electronic labels of the device to SFTP server 192.168.12.91. Set the SFTP user name to **client001** and password to YsHsjx_202206. Save electronic labels in the **elabel-slot0.fls** file.

```
<HUAWEI> backup elabel sftp 192.168.12.91 elabel-slot0.fls client001 YsHsjx_202206
Info: It is executing, please wait...

Info: Put file to SFTP server successfully.
```

3.2.4 cpu-usage monitor

Function

The **cpu-usage monitor** command enables the CPU usage monitoring.

The **undo cpu-usage monitor** command disables the monitoring function.

By default, the CPU usage monitoring is enabled.

Format

cpu-usage monitor [{ **slot** *slot-id* } | **slave**]

undo cpu-usage monitor [{ **slot** *slot-id* } | **slave**]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slave** parameter.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
slave	Indicates information about the CPU usage of the slave device. This Parameter is invalid.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If you want to check the status and performance of the device, run the **cpu-usage monitor** command to enable the CPU usage monitoring, and then run the **display cpu-usage** command to check information about the CPU usage.

Example

Enable the CPU usage monitoring.

```
<HUAWEI> system-view
[HUAWEI] cpu-usage monitor
```

3.2.5 cpu-usage threshold

Function

Using the **cpu-usage threshold** command, you can set the alarm threshold and alarm recovery threshold of CPU usage.

Using the **undo cpu-usage threshold** command, you can restore the alarm threshold and alarm recovery threshold of CPU usage.

By default, the alarm threshold of CPU usage is 95% and alarm recovery threshold is 80%.

Format

cpu-usage threshold *threshold-value* [**restore** *restore-threshold-value*] [**slot** *slot-id*]

undo cpu-usage threshold [*threshold-value* [**restore** [*restore-threshold-value*]]] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold *threshold-value*	Specifies the alarm threshold of CPU usage.	The value is an integer that ranges from 2 to 100. The default value is 95.
restore *restore-threshold-value*	Specifies the alarm recovery threshold of CPU usage.	The value is an integer that ranges from 1 to 99. The alarm recovery threshold must be smaller than the alarm threshold.
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the CPU usage exceeds the alarm threshold, a log is recorded. When the CPU usage reduces by equal to or smaller than 5% and exceeds the threshold again, no log is recorded. A log is recorded only when the CPU usage is reduced by greater than 5% and reaches the threshold again. Through log information, you can know the CPU usage more conveniently.

If **slot** *slot-id* is not configured, the alarm threshold and alarm recovery threshold of CPU usage are set. In addition, the system automatically synchronizes the threshold on the master switch with those on the member switches.

Example

Set the alarm threshold of CPU usage to 85% and alarm recovery threshold to 70% of the switch.

```
<HUAWEI> system-view
[HUAWEI] cpu-usage threshold 85 restore 70
```

3.2.6 clear battery-group esmu communication-failure

Function

The **clear battery-group esmu communication-failure** command clears alarms indicating that a battery module fails to communicate with its connected ESMUs.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

clear battery-group esmu communication-failure

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An Energy Storage System Management Unit (ESMU) is a unit for monitoring lithium batteries. You can run this command to clear alarms indicating that a battery module fails to communicate with its connected ESMUs.

Example

Clear alarms indicating that a battery module fails to communicate with its connected ESMUs.

```
<HUAWEI> system-view
[HUAWEI] clear battery-group esmu communication-failure
```

3.2.7 clear battery-group module-missing alarm

Function

The **clear battery-group module-missing alarm** command clears alarms indicating that a lithium battery group module is lost.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

clear battery-group module-missing alarm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to clear alarms indicating that a lithium battery group module is lost.

Example

Clear alarms indicating that a lithium battery group module is lost.

```
<HUAWEI> system-view
[HUAWEI] clear battery-group module-missing alarm
```

3.2.8 display device dc-output information

Function

The **display device dc-output information** command displays detailed information about DC output on the switch.

NOTE

Only the S5720I-10X-PWH-SI-AC supports this command.

Format

display device dc-output information

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When PDs require DC power supply, run the **display device dc-output information** command to view information about the switch output voltage, current, and power and determine whether the switch meets power supply requirements of PDs.

Example

Display detailed information about DC output on the switch.

```
<HUAWEI> display device dc-output information
-------------------------------------------------------
Output Line    Voltage(V)   Current(mA)   Power(mW)
-------------------------------------------------------
12V            12           147           1762
24V            24           0             0
-------------------------------------------------------
```

Table 3-37 Description of the **display device dc-output information** command output

Item	Description
Output Line	DC output line: - 12V: 12 V output line - 24V: 24 V output line
Voltage(V)	DC output voltage, in volts (V).
Current(mA)	DC output current, in milliamperes (mA).
Power(mW)	DC output power, in milliwatts (mW).

3.2.9 display device ac-output status

Function

The **display device ac-output status** command displays AC output status of the switch.

NOTE

Only the S5735-S8P2X-IA200H1, S5720I-6X-PWH-SI-AC, S5735-S4T2X-IA150G1, and S5735-S8P2X-IA200G1 support this command.

Format

display device ac-output status

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When PDs require AC power supply, check whether the AC output function has been enabled on the switch based on the device AC output status displayed using the **display device ac-output status** command.

Example

Display AC output status of the Switch.

```
<HUAWEI> display device ac-output status
----------------------------------------------------
OutputLine      ConfiguredState      PowerStatus
----------------------------------------------------
 24V            Enable               On
----------------------------------------------------
```

Table 3-38 Description of the **display device ac-output status** command output

Item	Description
OutputLine	AC output line. 24V: 24 V AC output line.
ConfiguredState	AC output configuration: ● Enable: AC output is enabled. ● Disable: AC output is disabled. To enable AC output, run the **set device ac-output 24v enable** command.
PowerStatus	AC output power status: ● On: Power is being supplied. ● Off: No power is supplied.

3.2.10 display device dc-output status

Function

The **display device dc-output status** command displays DC output status of the switch.

NOTE

Only the S5720I-10X-PWH-SI-AC supports this command.

Format

display device dc-output status

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When PDs require DC power supply, check whether the DC output function has been enabled on the switch based on the device DC output status displayed using the **display device dc-output status** command.

Example

Display DC output status of the Switch.

```
<HUAWEI> display device dc-output status
-----------------------------------------------------
OutputLine       ConfiguredState       PowerStatus
-----------------------------------------------------
12V-line1        Enable                On
12V-line2        Disable               Off
24V              Disable               Off
-----------------------------------------------------
```

Table 3-39 Description of the **display device dc-output status** command output

Item	Description
OutputLine	DC output line: • 12V-line1: 12 V line 1 DC output line • 12V-line2: 12 V line 2 DC output line • 24V: 24 V DC output line
ConfiguredState	DC output configuration: • Enable: DC output is enabled. • Disable: DC output is disabled. To enable DC output, run the **set device dc-output enable** command.
PowerStatus	DC output power status: • On: Power is being supplied. • Off: No power is supplied.

3.2.11 display device fault-light

Function

The **display device fault-light** command displays status of fault indicator on a device.

Format

display device fault-light

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After using the **display device fault-light** command to check the fault indicator status, you can determine whether to set the fault indicator on a device to indicate that the device is faulty using the **set device fault-light** command.

Example

Display the fault indicator status.

```
<HUAWEI> display device fault-light
----------------------------------------------------------------
Slot    Status      Keeptime(s)
----------------------------------------------------------------
0       UnderRepair    45
----------------------------------------------------------------
```

Table 3-40 Description of the display device fault-light command output

Item	Description
Slot	Slot ID.
Status	Status of the fault indicator. - Normal: Indicate that the device is running normally. - UnderRepair: Indicate that the device is faulty.

Item	Description
Keeptime(s)	Time during which the fault indicator indicates that the device is faulty. When the **Status** displays **Normal**, the value displays "--".

3.2.12 display fan speed-adjust threshold minus

Function

The **display fan speed-adjust threshold minus** command displays the temperature thresholds for fan speed adjustment.

Format

display fan speed-adjust threshold minus [**slot** *slot-id*]

NOTE

The following switches do not support this command:

- S2730S-S series
- S5720-LI series: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28P-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28X-LI-AC, S5720-28X-LI-DC, and S5720-16X-PWH-LI-AC
- S5735-L, S5735S-L, S5735-L1, S5735S-L1, and S5735S-L-M series: S5735-L12T4S-A, S5735-L24T4S-A, S5735-L24T4S-A1, S5735S-L24T4S-MA, S5735S-L24FT4S-A, S5735S-L12T4S-A, S5735S-L24T4S-A1, S5735-L8T4S-QA1, S5735-L24T4X-QA1, S5735-L24T4S-QA1, and S5735S-L24T4S-A
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720I-SI series: S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-SI-AC, and S5720I-12X-PWH-SI-DC
- S5735-S-I series
- S5731-H series, S5731S-H series, S5731-S series, S5731S-S series, S5732-H series
- S6730-H series, S6730S-H series, S6730-S series, S6730S-S series
- S6735-S

If one of the preceding switches can set up a stack with other switch models that support this command, this switch also supports this command so that this command can be executed and delivered in the stack.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID. If this parameter is not specified, the threshold settings in all slots are displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the temperature thresholds for fan speed adjustment, including the default values and current values.

In some situations, the higher the device temperature, the slower the fan speed may be. This is because the device temperature range when the fan speed increases overlaps with that when the fan speed decreases.

For example, if the threshold for fan speed adjustment is as follows:

- When the fan speed is 55%, the device temperature may be lower than or equal to 60°C.
- When the fan speed is 60%, the device temperature may be in the range from 55°C to 60°C.
- When the fan speed is 65%, the device temperature may be in the range from 56°C to 58°C.
- When the fan speed is 70%, the device temperature may be in the range from 54°C to 56°C.
- When the fan speed is 80%, the device temperature may be in the range from 52°C to 56°C.
- When the fan speed is 90%, the device temperature may be in the range from 53°C to 56°C.
- When the fan speed is 100%, the device temperature may be higher than 54°C.

The fan speed remains at 55% before the device temperature reaches 60°C from the startup temperature. If the temperature exceeds 60°C, the fan speed increases to 60%.

- If the temperature decreases to a value between 55°C and 60°C, the fan speed remains at 60%. If the temperature decreases to lower than 55°C, the fan speed reduces to 55% accordingly.

- If the temperature is still higher than 60°C, the fan speed increases to 65%.

The same rule applies to other temperatures.

Example

Display the temperature thresholds for fan speed adjustment.

```
<HUAWEI> display fan speed-adjust threshold minus
-----------------------------------------------------------
 Slot     Default Range  Current Range  Speed Rate Adjusted
-----------------------------------------------------------
 0          NA - 56         NA - 56        35%
           53 - 58        53 - 58       40%
           55 - 58        55 - 58       45%
           55 - 58        55 - 58       50%
           52 - 57        52 - 57       60%
           54 - 56        54 - 56       70%
           54 - 57        54 - 57       80%
           55 - 58        55 - 58       90%
           56 - NA         56 - NA       100%
```

Table 3-41 Description of the **display fan speed-adjust threshold minus** command output

Item	Description
Slot	Slot ID.
Default Range	Default temperature thresholds, which change based on the PoE power load.
Current Range	Current temperature thresholds. To set temperature thresholds, run the **set fan speed-adjust threshold minus** command. The new thresholds are the fixed temperature thresholds minus the configured value. After this command is executed, both the threshold for increasing the fan speed and the threshold for lowering the fan speed are reduced.
Speed Rate Adjusted	Fan speed adjustment range.

3.2.13 display flash threshold

Function

The **display flash threshold** command displays the alarm threshold for flash memory usage.

Format

display flash threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the configured alarm threshold for flash memory usage, run the **display flash threshold** command.

Example

Display the alarm threshold for flash memory usage.

```
<HUAWEI> display flash threshold
Info: The current flash usage threshold is 80%.
```

3.2.14 display otdr capture history-record interface

Function

The **display otdr capture history-record interface** command displays historical Optical Time Domain Reflectometer (OTDR) test results on an interface.

Format

display otdr capture history-record interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **otdr capture interface** command to perform an OTDR test on a specified interface, you can run the **display otdr capture history-record interface** command to view historical OTDR test results on the interface. Each test result displays reflection distances of 16 optical fibres, and the command output can display the latest 10 OTDR test results at most. If the reflection distance of an optical fiber is 0, the optical module connected to the optical fiber does not support OTDR testing.

After the device is restored to factory settings or the **reset otdr capture history-record** command is executed, historical OTDR test results are cleared and cannot be queried by running the **display otdr capture history-record interface** command.

Example

Display historical OTDR test results on GE0/0/1.

```
<HUAWEI> display otdr capture history-record interface gigabitethernet 0/0/1
----------------------------------------------------------------------------------------------
Index     Reflections Distance(m)                                                  Time
----------------------------------------------------------------------------------------------
 0        2027      0      0      0      0      0      0      0      2019-12-31 
14:34:03
           0      0      0      0      0      0      0      0
 1        2021      0      0      0      0      0      0      0      2019-12-26 
20:14:05
           0      0      0      0      0      0      0      0
 2        2019      0      0      0      0      0      0      0      2019-12-26 
20:14:04
           0      0      0      0      0      0      0      0
 3        2021      0      0      0      0      0      0      0      2019-12-26 
20:14:03
           0      0      0      0      0      0      0      0
 4        2021      0      0      0      0      0      0      0      2019-12-25 
20:14:03
           0      0      0      0      0      0      0      0
 5        2021      0      0      0      0      0      0      0      2019-12-24 
17:15:08
           0      0      0      0      0      0      0      0
 6        2021      0      0      0      0      0      0      0      2019-12-24 
15:26:08
           0      0      0      0      0      0      0      0
 7        2021      0      0      0      0      0      0      0      2019-12-23 
11:22:38
           0      0      0      0      0      0      0      0
 8        2021      0      0      0      0      0      0      0      2019-12-23 
10:46:55
           0      0      0      0      0      0      0      0
 9        2021      0      0      0      0      0      0      0      2019-12-23 
09:33:48
           0      0      0      0      0      0      0      0
```

Table 3-42 Description of the **display otdr capture history-record interface** command output

Item	Description
Index	Sequence number of an OTDR test result.

Item	Description
Reflections Distance(m)	Reflection distance, in meters.
Time	Time when an OTDR test is performed.

3.2.15 display otdr certificate interface

Function

The **display otdr certificate interface** command displays the OTDR test result which is configured as the OTDR birth certificate on an interface.

Format

display otdr certificate interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **otdr certificate interface** command to configure an OTDR test result as the OTDR birth certificate for an interface, you can run the **display otdr certificate interface** command to view the OTDR birth certificate.

After the device is restored to factory settings or the **reset otdr certificate** command is executed, OTDR birth certificates of interfaces are cleared and cannot be queried using the **display otdr certificate interface** command.

Example

Display the OTDR birth certificate on GE0/0/1.

```
<HUAWEI> display otdr certificate interface gigabitethernet 0/0/1
----------------------------------------------------------------------------------------------------
Reflections       Distance(m)                                           Time
----------------------------------------------------------------------------------------------------
```

```
     2021      0      0      0      0      0      0      0           2019-12-31
14:34:03
       0      0      0      0      0      0      0      0
```

Table 3-43 Description of the **display otdr certificate interface** command output

Item	Description
Reflections Distance(m)	Reflection distance, in meters.
Time	Time when an OTDR test is performed.

3.2.16 display resource-mode configuration

Function

The **display resource-mode configuration** command displays the resource allocation mode configuration on the device.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,S5735S-L1, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S, S6720-EI, and S6720S-EI support this command.

Format

display resource-mode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before configuring or modifying the resource allocation mode, run the **display resource-mode configuration** command to check the resource allocation mode configuration.

Example

Display the resource allocation mode.

```
<HUAWEI> display resource-mode configuration
Slot       Current Mode    Next Mode
- - - - - - - - - - - - - - - - - - - - - - -
0          enhanced-mac    enhanced-mac
```

Table 3-44 Description of the display resource-mode configuration command output

Item	Description
Slot	Slot ID.
Current Mode	Current resource allocation mode.
Next Mode	Resource allocation mode configured using the **assign resource-mode** command. **NOTE** If the Next Mode is different from the Current Mode, the device is not restarted after the resource allocation mode is modified.

3.2.17 display root-key configuration

Function

The **display root-key configuration** command displays information about the currently used root key.

Format

display root-key configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use the **display root-key configuration** command to check information about the currently used root key.

Example

Display information about the currently used root key.

```
<HUAWEI> display root-key configuration
Master:
  Current root-key:  User-configured
  Next root-key:     System default
```

Table 3-45 Description of the **display root-key configuration** command output

Item	Specification
Current root-key	Information about the currently used root key: ● User-configured: user-configured root key ● System default: system default root key
Next root-key	Information about the root key used after the device restarts: ● User-configured: user-configured root key ● System default: system default root key To set the root key, run the **set root-key** command.

3.2.18 display service-mode configuration

Function

The **display service-mode configuration** command displays the working mode of the device.

NOTE

This command is supported only by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

display service-mode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the working mode of the device, run the **display service-mode configuration** command.

Example

Display the working mode of the device.

```
<HUAWEI> display service-mode configuration
Service mode status: Normal
```

Display the working mode of the S6730-H.

```
<HUAWEI> display service-mode configuration
Service mode status: BFD-enhanced, OAM-normal, PTP-normal
```

Table 3-46 Description of the **display service-mode configuration** command output

Item	Description
Service mode status	Working mode of the device: ● Normal ● Enhanced ● BFD-normal ● BFD-enhanced ● OAM-normal ● OAM-enhanced ● PTP-normal ● PTP-enhanced To set the working mode, run the **set service-mode** command.

3.2.19 display switchover state

Function

The **display switchover state** command displays information about active/standby switchover, which helps check whether the stack meets switchover requirements.

Format

display switchover state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In a stack containing multiple switches, you can run the **display switchover state** command to view the status of master and standby switches to determine whether to perform an active/standby switchover. When performing active/standby switchover, ensure that the standby switch is in real-time backup state.

Example

Display information about active/standby switchover, which helps check whether the stack meets switchover requirements.

```
<HUAWEI> display switchover state
Slot 1 HA FSM State(master): waiting for the slave to be inserted.
```

Table 3-47 Description of the display switchover state command output

Item	Description
HA FSM State(master)	Master switch status: ● The slave has been inserted: The slave switch has been inserted. ● waiting for the slave to be inserted: The master switch is waiting for the slave switch to be inserted. ● waiting the batch backup request from the slave: The master switch is waiting for the batch backup request from the slave switch. ● batch global data: Backup global data in batch ● batch backup: Backup data in batch ● batch check: Check the backup data in batch ● realtime or routine backup: Backup data periodically or promptly ● data smooth: Synchronize data

Item	Description
HA FSM State(slave)	Standby switch status: • ready: The standby switch is started and ready for receiving the batch backup data. • receiving batch data: The standby switch is receiving the batch backup data. • receiving realtime or routine data: The standby switch is ready for receiving data in real time.

3.2.20 display system resource-template

Function

The **display system resource-template** command displays system resource template information.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S6735-S, S5735S-H, S5736-S, and S6720S-S support this command.

Format

display system resource-template [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	• Specifies a slot ID on a standalone device. • Specifies the stack ID in a stack.	The value is an integer. In a stack, the value must be set according to the device configuration. On a standalone device, the default value is 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display system resource-template** command to view system resource template information, including the resource type, currently running resource template information and resource template for the next startup.

Example

Display information about the system resource template. For example, the S5720-LI.

```
<HUAWEI> display system resource-template
Resource Template Information:
------------------------------------------------------------
 Slot    Type        RunningTemplate     NextTemplate
------------------------------------------------------------
 0       acl-mode    dual-ipv4-ipv6      dual-ipv4-ipv6
------------------------------------------------------------
```

Table 3-48 Description of the **display system resource-template** command output

Item	Description
Slot	Slot ID.
Type	Resource type. Currently, only one system resource template (acl-mode) is supported.
RunningTemplate	Currently running resource template information. To configure a resource template, run the **assign resource-template acl-mode** command.
NextTemplate	Resource template for the next startup.

3.2.21 display wavelength-map

Function

The **display wavelength-map** command displays the mapping between the wavelength channel, wavelength, and frequency.

Format

display wavelength-map

Parameters

None

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

Before using the **wavelength-channel** command to add an optical module to a specific wavelength channel, run the **display wavelength-map** command to view the mapping between the wavelength channel, wavelength, and frequency.

Example

Display the mapping between the wavelength channel, wavelength, and frequency.

```
<HUAWEI> system-view
[HUAWEI] display wavelength-map
-------------------------------------------
Channel     Frequency(THz)    Wavelength(nm)
-------------------------------------------
1          192.10          1560.606
2          192.15          1560.200
3          192.20          1559.794
4          192.25          1559.389
5          192.30          1558.983
6          192.35          1558.578
7          192.40          1558.173
8          192.45          1557.768
9          192.50          1557.363
10          192.55          1556.959
11          192.60          1556.555
12          192.65          1556.151
13          192.70          1555.747
14          192.75          1555.344
15          192.80          1554.940
16          192.85          1554.537
17          192.90          1554.134
18          192.95          1553.731
19          193.00          1553.329
20          193.05          1552.927
21          193.10          1552.524
22          193.15          1552.122
23          193.20          1551.721
24          193.25          1551.319
25          193.30          1550.918
26          193.35          1550.517
27          193.40          1550.116
28          193.45          1549.715
29          193.50          1549.315
30          193.55          1548.915
31          193.60          1548.515
32          193.65          1548.115
33          193.70          1547.715
34          193.75          1547.316
35          193.80          1546.917
36          193.85          1546.518
37          193.90          1546.119
38          193.95          1545.720
39          194.00          1545.322
40          194.05          1544.924
```

```
41        194.10        1544.526
42        194.15        1544.128
43        194.20        1543.730
44        194.25        1543.333
45        194.30        1542.936
46        194.35        1542.539
47        194.40        1542.142
48        194.45        1541.746
49        194.50        1541.349
50        194.55        1540.953
51        194.60        1540.557
52        194.65        1540.162
53        194.70        1539.766
54        194.75        1539.371
55        194.80        1538.976
56        194.85        1538.581
57        194.90        1538.186
58        194.95        1537.792
59        195.00        1537.397
60        195.05        1537.003
61        195.10        1536.609
62        195.15        1536.216
63        195.20        1535.822
64        195.25        1535.429
65        195.30        1535.036
66        195.35        1534.643
67        195.40        1534.250
68        195.45        1533.858
69        195.50        1533.465
70        195.55        1533.073
71        195.60        1532.681
72        195.65        1532.290
73        195.70        1531.898
74        195.75        1531.507
75        195.80        1531.116
76        195.85        1530.725
77        195.90        1530.334
78        195.95        1529.944
79        196.00        1529.553
80        196.05        1529.163
---------------------------------------------
```

Table 3-49 Description of the **display wavelength-map** command output

Item	Description
Channel	Channel ID.
Frequency(THz)	Frequency, in THz.
Wavelength(nm)	Wavelength, in nm.

3.2.22 mib-data optical-module sample-interval

Function

The **mib-data optical-module sample-interval** command sets the sampling interval for optical module information in the MIB performance module.

The **undo mib-data optical-module sample-interval** command restores the default setting.

By default, the interval is 30 seconds.

Format

mib-data optical-module sample-interval *interval-value*

undo mib-data optical-module sample-interval

Parameters

Parameter	Description	Value
interval-value	Specifies a sampling interval for optical module information in the MIB performance module.	The value is an integer in the range from 10 to 300, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It takes a long time for the NMS to query real-time optical module information on a device using hwOpticalModuleInfoTable in the MIB, especially when the device has a large number of optical modules installed. To solve this problem, you can configure devices to periodically sample optical module information. Then, the NMS can directly obtain sampling information about optical modules, which improves efficiency.

Precautions

- When you run the **mib-data optical-module sample-interval** command multiple times, only the latest configuration takes effect.
- The shorter the sampling interval, the higher the CPU usage.

Example

Set the sampling interval of optical module information in the MIB performance module to 35 seconds.

```
<HUAWEI> system-view
[HUAWEI] mib-data optical-module sample-interval 35
```

3.2.23 otdr capture interface

Function

The **otdr capture interface** command triggers an optical time domain reflectometer (OTDR) test on an interface.

Format

otdr capture interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To perform an OTDR test to obtain reflection distances of optical fibers, run the **otdr capture interface** command. The reflection distances are used for fiber fault diagnosis. To query historical OTDR test results, run the **display otdr capture history-record interface** command.

To ensure that historical OTDR test results are not lost after the device is restarted, historical OTDR test results are recorded in the **flash:/otdr_capture.bin** file. This file is set as a system file and cannot be deleted. To clear historical OTDR test results, you need to run the **reset otdr capture history-record** command. After the **reset otdr capture history-record** command is executed and the device is restarted, historical OTDR test results are cleared and cannot be queried by running the **display otdr capture history-record interface** command.

Precautions

- The command can be run multiple times.
- This command can be configured only when a specific optical module is installed on an interface. For details about the optical module, contact Huawei technical support.

Example

Trigger an OTDR test on GE0/0/1.

```
<HUAWEI> otdr capture interface gigabitethernet 0/0/1
```

3.2.24 otdr certificate interface

Function

The **otdr certificate interface** command configures an OTDR test result as the OTDR birth certificate on an interface.

Format

otdr certificate interface *interface-type interface-number capture-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
capture-number	Specifies the sequence number of an OTDR test result.	The value is an integer ranging from 0 to 9.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To configure an OTDR test result as the OTDR birth certificate, run the **otdr certificate interface** command. The OTDR birth certificate is used as a baseline for fault detection. You can run the **display otdr certificate interface** command to view the OTDR birth certificate. By comparing the fiber reflection distances in OTDR test results (in the **display otdr capture history-record interface** command output) and the OTDR birth certificate (in the **display otdr certificate interface** command output), you can determine whether a fault occurs on an optical fiber.

To ensure that birth certificates of interfaces are not lost after the device restarts, the birth certificates are recorded in the **flash:/otdr_certificate.bin** file. This file is set as a system file and cannot be deleted. To clear OTDR birth certificates of interfaces, you need to run the **reset otdr certificate** command. After the **reset otdr certificate** command is executed and the device is restarted, OTDR birth certificates of interfaces are cleared and cannot be queried by running the **display otdr certificate interface** command.

Precautions

- This command can be run multiple times, but the latest configuration takes effect.
- This command can be configured only when a specific optical module is installed on an interface. For details about the optical module, contact Huawei technical support.

Example

Configure the second OTDR test result as the OTDR birth certificate on GE0/0/1.

```
<HUAWEI> otdr certificate interface gigabitethernet 0/0/1 2
port_no=GigabitEthernet0/0/1
capture_no=2
```

3.2.25 reset battery esmu

Function

The **reset battery** command resets ESMUs that monitor a specific battery.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command. This command takes effect only when the backup lithium battery is unavailable.

Format

reset battery *battery-id* **esmu**

Parameters

Parameter	Description	Value
battery-id	Specifies the battery number.	The value is an integer and must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An ESMU is a unit for monitoring a lithium battery. You can run this command to reset ESMUs.

Example

Reset the ESMUs that monitor the battery whose number is 1.

```
<HUAWEI> system-view
[HUAWEI] reset battery 1 esmu
```

3.2.26 reset cpu-usage record

Function

The **reset cpu-usage record** command clears CPU usage records.

Format

reset cpu-usage record [**slot** *slot-id* | **slave** | **all**]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	Set the value according to the device configuration.
slave	Clears CPU usage records on the slave switch.	-
all	Clears CPU usage records on all switches	-

Views

System view, User view

Default Level

3: Management level

Usage Guidelines

If the **slot** *slot-id* or **slave** parameter is not specified, CPU usage records of the master switch is cleared.

Example

Clear CPU usage records of the master switch.

```
<HUAWEI> system-view
[HUAWEI] reset cpu-usage record
Waiting for clearing . . . Done
```

3.2.27 reset integrated-power output

Function

The **reset integrated-power output** command resets the outputs of a PC510 power supply.

Format

reset integrated-power output

NOTE

This command is supported only by the S5735-L8P4X-IA1, S5735-L8T4X-IA1.

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the switch is connected to a PC510 power supply through a network cable, the PC510 power supply can provide 12 V DC and 24 V AC outputs. When the power outputs are abnormal or the downstream devices of the switch need to be restarted, you can run this command on the switch to reset the PC510 power supply outputs.

Resetting the outputs of the PC510 power supply does not reset the output to the switch. Therefore, the switch does not restart.

Precautions

Before running this command, run the **set power protocol modbus** command on the switch to set up a connection with the PC510 power supply. If the connection fails to be set up, this command does not take effect.

Example

Reset the outputs of the PC510 power supply.

```
<HUAWEI> reset integrated-power output
```

3.2.28 reset power-detect status

Function

The **reset power-detect status** command restores the power supply to its factory defaults.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

reset power-detect status

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to restore the power supply to its factory defaults.

Example

Restore the power supply to its factory defaults.

```
<HUAWEI> system-view
[HUAWEI] reset power-detect status
```

3.2.29 reset otdr capture history-record

Function

The **reset otdr capture history-record** command clears historical OTDR test results on an interface.

Format

reset otdr capture history-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **otdr capture interface** command to obtain the fiber reflection distance for fiber fault diagnosis. You can run the **display otdr capture history-record interface** command to view historical OTDR test results.

To ensure that historical OTDR test results are not lost after the device is restarted, historical OTDR test results are recorded in the **flash:/otdr_capture.bin** file. This file is set as a system file and cannot be deleted. To clear historical OTDR test results, you need to run the **reset otdr capture history-record** command. After the **reset otdr capture history-record** command is executed and the device is restarted, historical OTDR test results are cleared and cannot be queried by running the **display otdr capture history-record interface** command.

Example

Clear historical OTDR test results on interfaces.

```
<HUAWEI> reset otdr capture history-record
```

3.2.30 reset otdr certificate

Function

The **reset otdr certificate** command clears the OTDR test results configured as birth certificates on interfaces.

Format

reset otdr certificate

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **otdr certificate interface** command to configure a historical OTDR test result as the OTDR birth certificate for an interface and run the **display**

otdr certificate interface command to view the OTDR birth certificate of an interface.

To ensure that birth certificates of interfaces are not lost after the device restarts, the birth certificates are recorded in the **flash:/otdr_certificate.bin** file. This file is set as a system file and cannot be deleted. To clear OTDR birth certificates of interfaces, you need to run the **reset otdr certificate** command. After the **reset otdr certificate** command is executed and the device is restarted, OTDR birth certificates of interfaces are cleared and cannot be queried by running the **display otdr certificate interface** command.

Example

Clear the OTDR test results used as birth certificates on interfaces.

```
<HUAWEI> reset otdr certificate
```

3.2.31 reset slot

Function

The **reset slot** command resets a device.

Format

reset slot *slot-id* [**cold**]

NOTE

Only the following devices support cold reset. Other devices that support the **cold** parameter do not support cold reset.

- S5735-S8P2X-IA200H1, S5735-L24P4S-A, S5735-L24P4S-A1, S5735S-L24P4S-A, S5735S-L24P4S-A1, S5735S-L24P4S-MA, S5735-L24P4X-A, S5735-L24P4X-A1, S5735S-L24P4X-A, S5735S-L24P4X-A1, S5735-S4T2X-IA150G1, S5735-S8P2X-IA200G1
- Devices that use a 300 W AC power module (PAC300S12-CL)
- Devices that use a 600 W AC power module (PAC600S12-CB, PAC600S12-EB, PAC600S12-DB, and PAC600S56-CB)
- Devices that use a 600 W AC PoE power module (PAC600S56-EB)
- Devices that use a 1000 W DC power module (PDC1000S12-DB)
- Devices that use a 1000 W DC Poe power module (PDC1000S56-CB and PDC1000S56-EB)
- Devices that use a 1000 W AC PoE power module (PAC1000S56-CB, PAC1000S56-EB, and PAC1000S56-DB)

The **cold** parameter is supported only in the user view.

Parameters

Parameter	Description	Value
slot-id	Specifies a slot ID.	The value must be set according to the device configuration.

Parameter	Description	Value
cold	Indicates cold reset.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack, you can restart stack members. Restarting a stack member will interrupt services on this device, but the configuration of this device still exists.

Precautions

- Before commands have been executed, if a master/standby switchover occurs because the **reset slot** command is used to reset the master switch, you need to execute the commands that have not been executed on the new master switch again after the standby switch becomes the new master switch.
- For the S5735-S8P2X-IA200H1, after this command is run, the switch will not restart, but its output power supply will be reset.
- Due to the component upgrade of some device models, some devices cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about the first supported version of the device and matching patch version, see the device overview in the "Hardware Description"..

Example

Restart the switch with the slot ID 0.

```
<HUAWEI> reset slot 0
Warning: Confirm to reset slot 0? [Y/N]:y
Info: The board 0 is reset successfully.
```

Perform a cold reset on the switch with the slot ID 0.

```
<HUAWEI> reset slot 0 cold
Warning: The device in slot 0 will be cold reset. Ensure that the configuration has been saved. Otherwise,
the configuration will be lost after cold restart. Continue? [Y/N]: y
Info: Succeeded in cold resetting the device in slot 0.
```

3.2.32 set battery-group

Function

The **set battery-group** command configures the float charging voltage or equalized charging voltage for the lithium battery group.

The **undo set battery-group** command restores the default float charging voltage or equalized charging voltage of the lithium battery group.

By default, the float charging voltage of the lithium battery group is 54.50 V, and the equalized charging voltage is 56.40 V.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set battery-group { **equalized-charge-voltage** | **float-charge-voltage** } *value*

undo set battery-group { **equalized-charge-voltage** | **float-charge-voltage** }

Parameters

Parameter	Description	Value
equalized-charge-voltage	Configures the float charging voltage.	-
float-charge-voltage	Configures the equalized charging voltage.	-
value	Indicates the voltage value.	The value range is as follows: • **equalized-charge-voltage**: The value ranges from 43.20 to 56.40, in volts (V). • **float-charge-voltage**: The value ranges from 43.20 to 56.40, in volts (V). **NOTE** The equalized charging voltage must be greater than or equal to the float charging voltage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the float charging voltage or equalized charging voltage for the lithium battery group.

Example

Configure the float charging voltage of the lithium battery group to 55.11 V.

```
<HUAWEI> system-view
[HUAWEI] set battery-group equalized-charge-voltage 55.11
```

3.2.33 set battery-group charge current-limit

Function

The **set battery-group charge current-limit** command configures the charge current limiting coefficient for the lithium battery group.

The **undo set battery-group charge current-limit** command restores the default charge current limiting coefficient for the lithium battery group.

By default, the charge current limiting coefficient for the lithium battery group is 0.30.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set battery-group charge current-limit *value*

undo set battery-group charge current-limit

Parameters

Parameter	Description	Value
value	Specifies the charge current limiting coefficient for the lithium battery group.	The value ranges from 0.05 to 1.00, in C10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the charge current limiting coefficient for the lithium battery group.

Example

Set the charge current limiting coefficient of the lithium battery group to 0.61.

```
<HUAWEI> system-view
[HUAWEI] set battery-group charge current-limit 0.61
```

3.2.34 set battery-group install date

Function

The **set battery-group install date** command sets the installation date of the lithium battery group.

The **undo set battery-group date** command restores the default installation date of the lithium battery group.

By default, the installation date of the lithium battery group is 2014-01-01.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set battery-group install date *date-value*

undo set battery-group install date

Parameters

Parameter	Description	Value
date-value	Specifies the installation date of the lithium battery group.	The value is in YYYY-MM-DD format. It ranges from 2014-01-01 to 2037-12-31.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to record the installation date of the lithium battery group.

Example

Set the installation date of the lithium battery group to November 11, 2021.

```
<HUAWEI> system-view
[HUAWEI] set battery-group install date 2021-11-11
```

3.2.35 set device dc-output enable

Function

The **set device dc-output enable** command enables the DC output function on the switch.

The **undo set device dc-output enable** command disables the DC output function on the switch.

By default, the DC output function is enabled on a switch.

NOTE

Only the S5720I-10X-PWH-SI-AC supports this command.

Format

set device dc-output [**12V** [**line1** | **line2**] | **24V**] **enable**

undo set device dc-output [**12V** [**line1** | **line2**] | **24V**] **enable**

Parameters

Parameter	Description	Value
12V	Specifies the DC output voltage as 12 V.	-
line1	Configures DC output of 12 V line 1.	-
line2	Configures DC output of 12 V line 2.	-
24V	Specifies the DC output voltage as 24 V.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PDs require DC power supply, enable DC output on the switch.

Precautions

If you run the **set device dc-output 12V** [**line1** | **line2**] **enable** command to enable the 12 V DC output function of the switch, and then run the **set device dc-output 24V enable** command to enable the 24 V DC output function of the switch, both the 12 V and 24 V DC output functions have been enabled on the switch. To determine the state of each DC output line, run the **display device dc-output status** command.

Example

Enable DC output of 12 V line 1 and set the DC output voltage to 12 V.

```
<HUAWEI> system-view
[HUAWEI] set device dc-output 12V line1 enable
Warning: The total PoE power and DC output power is 0mW, and the remaining power is 175000mW.
Continue? [Y/N]:Y
Warning: After the 12V line1 DC output is enabled, PoE power and DC output power may be disabled if the
total PoE power and DC output power exceeds 175000mW. Continue? [Y/N]:Y
```

Enable DC output of all lines.

```
<HUAWEI> system-view
[HUAWEI] set device dc-output enable
Warning: The total PoE power and DC output power is 731mW, and the remaining power is 174269mW.
Continue? [Y/N]:Y
Warning: After all DC output is enabled, PoE power and DC output power may be disabled if the total PoE
power and DC output power exceeds 175000mW. Continue? [Y/N]:Y
```

3.2.36 set device ac-output 24v enable

Function

The **set device ac-output 24v enable** command enables the 24 V AC output function on a switch.

The **undo set device ac-output 24v enable** command disables the 24 V AC output function on a switch.

By default, the 24 V AC output function is enabled on switches.

NOTE

Only the S5735-S8P2X-IA200H1, S5720I-6X-PWH-SI-AC, S5735-S4T2X-IA150G1, and S5735-S8P2X-IA200G1 support this command.

Format

set device ac-output 24v enable

undo set device ac-output 24v enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PDs require AC power supply, enable the AC output function on the switch.

Precautions

- For the S5720I-6X-PWH-SI-AC, when the sum of the PoE power, DC output power, and AC output power is greater than 150000 mW, the switch restarts.
- For the S5735-S4T2X-IA150G1 and S5735-S8P2X-IA200G1, when the sum of the PoE power, DC output power, and AC output power is greater than 160000 mW, the switch restarts.
- For the S5735-S8P2X-IA200H1, when the sum of the PoE power, DC output power, and AC output power is greater than 200000 mW, the switch restarts.

Example

Enable the 24 V AC output function on a switch.

```
<HUAWEI> system-view
[HUAWEI] set device ac-output 24v enable
Warning: After this command is excuted, the 24V AC output will be enabled. Continue? [Y/N]:y
Warning: After the 24V AC output is enabled, the switch will reboot if the total power of PoE power, DC
output power and AC output power exceed 150000mW. Continue? [Y/N]:y
```

3.2.37 set device fault-light

Function

The **set device fault-light** command sets the fault indicator status on a device.

The **undo set device fault-light** command restores the default fault indicator status.

By default, the fault indicator status of the device is not set. The fault indicator status is displayed based on the current device running status.

Format

set device fault-light { **normal** | **under-repair** [**keeptime** *time*] } [**slot** *slot-id*]

undo set device fault-light [**slot** *slot-id*]

Parameters

Parameter	Description	Value
normal	Displays the fault indicator status based on the current device running status.	-
under-repair	Configures the fault indicator to indicate that the device is faulty.	-
keeptime *time*	Sets the time during which the fault indicator indicates that the device is faulty.	The value is an integer that ranges from 45 to 600, in seconds. The default value is 45.
slot *slot-id*	Specifies a slot ID. If not slot ID is specified in a stack, this command sets the fault indicator status of the stack master.	The value range depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

If a switch is faulty, run the **set device fault-light** command to set the mode indicators or system indicator to the faulty state so that O&M personnel can find the faulty switch onsite.

- For the S500, S5735-S, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

  When the **set device fault-light under-repair** command is executed, the ID indicator is steady blue and turns off after it is steady blue for the time specified by **keeptime** *time* (the default time is 45s if this parameter is not specified). The **set device fault-light normal** command and the **undo set device fault-light** command have the same functions. That is, after either of the two commands is executed, the ID indicator turns off.
- For the S5720I-6X-PWH-SI-AC and S5720I-10X-PWH-SI-AC

  The switch has only one fault indicator, WiFi indicator. When the **set device fault-light under-repair** command is executed, the WiFi indicator blinks red fast and turns off after it blinks red fast for the time specified by **keeptime**

time (the default time is 45s if this parameter is not specified). The **set device fault-light normal** and **undo set device fault-light** commands have the same functions. That is, after either of the two commands is executed, the WiFi indicator turns off.

- For the S5735-S-I

  The switch has only one fault indicator, SYS indicator. When the **set device fault-light under-repair** command is executed, the SYS indicator blinks red fast and returns to the previous state after it blinks red fast for the time specified by **keeptime** *time* (the default time is 45s if this parameter is not specified). The **set device fault-light normal** and **undo set device fault-light** commands have the same functions. That is, after either of the two commands is executed, the SYS indicator returns to the previous state.

- For other switches that support this command

  When the **set device fault-light under-repair** command is executed, the SYS indicator and mode indicators (STAT, SPED, PoE, and STCK) blink red fast. After these indicators blink red fast for the time specified by **keeptime** *time* (the default time is 45s if this parameter is not specified), the SYS indicator returns to the previous state, and the STAT indicator is steady on.

  The **set device fault-light normal** and **undo set device fault-light** commands have the same functions. That is, after either of the two commands is executed, the SYS indicator returns to the previous state, and the STAT indicator is steady on.

  If **slot** *slot-id* is not specified in a stack, the configuration takes effect on indicators on the master switch.

Example

Configure the fault indicator to indicate that the device is faulty.

```
<HUAWEI> system-view
[HUAWEI] set device fault-light under-repair
```

3.2.38 set fan speed auto min-speed

Function

The **set fan speed auto min-speed** command configures the minimum fan speed in automatic fan speed adjustment mode.

The **undo set fan speed auto min-speed** command restores the default minimum fan speed in automatic fan speed adjustment mode.

By default, the minimum fan speed in automatic fan speed adjustment mode is not configured.

NOTE

The following switches do not support this command:

- S2730S-S series
- S5720-LI series: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28P-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28X-LI-AC, S5720-28X-LI-DC, and S5720-16X-PWH-LI-AC
- S5735-L, S5735S-L, S5735-L1, S5735S-L1, and S5735S-L-M series: S5735-L12T4S-A, S5735-L24T4S-A, S5735-L24T4S-A1, S5735S-L24T4S-MA, S5735S-L24FT4S-A, S5735S-L12T4S-A, S5735S-L24T4S-A1, S5735-L8T4S-QA1, S5735-L24T4X-QA1, S5735-L24T4S-QA1, and S5735S-L24T4S-A
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720I-SI series: S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-SI-AC, and S5720I-12X-PWH-SI-DC
- S5735-S-I series
- S5731-H series, S5731S-H series, S5731-S series, S5731S-S series, S5732-H series
- S6730-H series, S6730S-H series, S6730-S series, S6730S-S series
- S6735-S

If one of the preceding switches can set up a stack with other switch models that support this command, this switch also supports this command so that this command can be executed and delivered in the stack.

Format

set fan speed auto min-speed *value* [**slot** *slot-id* | **all**]

undo set fan speed auto min-speed [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
value	Sets the percentage of the minimum fan speed. For example, if this parameter is set to 35, the minimum fan speed in automatic fan speed adjustment mode is 35% of the full fan speed.	The value is an integer that ranges from 1 to 100.
slot *slot-id*	Specifies a slot ID. If this parameter is not specified, the minimum fan speed in automatic fan speed adjustment mode is configured for the fans on the master switch.	The value depends on the device configuration.
all	Specifies all slots.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The fan speed affects the device temperature. When the device temperature is high, increase the fan speed to lower the device temperature. When the device temperature is low, reduce the fan speed to save energy. A proper fan speed ensures stable device operation. By default, fans run in automatic fan speed adjustment mode. In this mode, the system adjusts the fan speed when detecting that the device temperature increases or decreases. To control the fan speed in a timely manner, run the **set fan speed auto min-speed** command to configure the minimum fan speed in automatic speed adjustment mode.

Precautions

- If the automatically calculated fan speed is lower than the configured minimum speed, the configured minimum speed takes effect. If the automatically calculated fan speed is greater than the configured minimum speed, the calculated fan speed takes effect. To obtain the minimum fan speed of a device, view the **Speed Rate Adjusted** field in the **display fan speed-adjust threshold minus** command output.
- To obtain the minimum fan speed in automatic fan speed adjustment mode on a device, view the **Auto Min-speed** field in the **display fan** command output.
- The following assumes that the device can set up a stack with other device models and has the minimum fan speed in automatic fan speed adjustment mode configured before the stack is set up. After the stack is set up, if this device functions as the master switch, the configured minimum fan speed still takes effect. If this device functions as the standby or slave switch, the configured minimum fan speed does not take effect.
- This configuration takes effect only when fan modules work in automatic speed adjustment mode. You can check the **Mode** field in the **display fan** command output to check the fan speed adjustment mode. If a fan module works at a fixed speed, run the **fan speed mandatory** command in the diagnostic view to configure the fan module to work in automatic speed adjustment mode.

Example

Set the minimum fan speed in automatic fan speed adjustment mode to 20% of the full fan speed.

```
<HUAWEI> system-view
[HUAWEI] set fan speed auto min-speed 20
Info: The configuration is successful and takes effect only when the specified value is greater than the value
calculated based on the intelligent fan speed adjustment policy.
```

3.2.39 set fan speed-adjust threshold minus

Function

The **set fan speed-adjust threshold minus** command adjusts the temperature thresholds for fan speed adjustment.

The **undo set fan speed-adjust threshold minus** command restores the default temperature thresholds for fan speed adjustment.

The default temperature thresholds on different devices are different. You can get to run the **display fan speed-adjust threshold minus** command.

NOTE

The following switches do not support this command:

- S2730S-S series
- S5720-LI series: S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28P-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28X-LI-AC, S5720-28X-LI-DC, and S5720-16X-PWH-LI-AC
- S5735-L, S5735S-L, S5735-L1, S5735S-L1, and S5735S-L-M series: S5735-L12T4S-A, S5735-L24T4S-A, S5735-L24T4S-A1, S5735S-L24T4S-MA, S5735S-L24FT4S-A, S5735S-L12T4S-A, S5735S-L24T4S-A1, S5735-L8T4S-QA1, S5735-L24T4X-QA1, S5735-L24T4S-QA1, and S5735S-L24T4S-A
- S5720S-LI series: S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28TP-PWR-LI-AC, and S5720S-28X-LI-AC
- S5720I-SI series: S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-SI-AC, and S5720I-12X-PWH-SI-DC
- S5735-S-I series
- S5731-H series, S5731S-H series, S5731-S series, S5731S-S series, S5732-H series
- S6730-H series, S6730S-H series, S6730-S series, S6730S-S series
- S6735-S

If one of the preceding switches can set up a stack with other switch models that support this command, this switch also supports this command so that this command can be executed and delivered in the stack.

Format

set fan speed-adjust threshold minus *threshold-value* [**slot** *slot-id*]

undo set fan speed-adjust threshold minus [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the deduction to the temperature thresholds.	The value is an integer that ranges from 1 to 20.

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID. If this parameter is not specified, the thresholds in all slots are set.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device uses fixed temperature thresholds to increase and decrease the fan speed by default. The fan speed increases when the device temperature exceeds the upper threshold and decreases when the device temperature falls below the lower threshold. If you want to keep the device working at a lower temperature, you can set deduction for the fixed temperature thresholds. The adjusted temperature threshold is lower than the default temperature threshold.

Precautions

- The new thresholds are the fixed temperature thresholds minus *threshold-value*. After the **set fan speed-adjust threshold minus** command is executed, the thresholds for increasing and lowering the fan speed decrease.
- To view the fixed temperature thresholds, run the **display fan speed-adjust threshold minus** command.

NOTE

If a device uses intelligent fan control, this command reduces the temperature thresholds for starting and stopping the fans. Fans in intelligent heat dissipation mode can only start and stop rotating at a fixed speed that cannot be increased or reduced.

You can run the **display fan speed-adjust threshold minus** command to check temperature thresholds for fan speed adjustment of fans in intelligent heat dissipation mode. Assume you view that the current temperature threshold of the fans is 40-50, in which 40°C is the threshold for stopping the fans, and 50°C is the threshold for starting the fans. When the current device temperature is 45°C, you need to determine whether fans will rotate according to the fan temperature change:

- When the device temperature is increased to 45°C from a lower temperature (30°C for example), fans do not rotate because the device temperature does not reach the threshold for starting the fans.
- When the device temperature is reduced to 45°C from a higher temperature (65°C for example), fans keep rotating because the device temperature does not fall below the threshold for stopping the fans.

Example

Set the deduction to the temperature thresholds to 10.

```
<HUAWEI> system-view
[HUAWEI] set fan speed-adjust threshold minus 10
Info: Succeeded in setting the fan speed-adjust threshold.
```

3.2.40 set fan speed mandatory

Function

The **set fan speed mandatory** command sets a fixed speed for fans on a device.

The **undo set fan speed mandatory** command restores the automatic fan speed mode.

By default, the automatic fan speed mode is used.

Format

set fan speed mandatory { **minimal** | **middle** | **maximal** | **fixed40** | **fixed50** | **fixed60** | *speed* } [**slot** *slot-id*]

undo set fan speed mandatory { **minimal** | **middle** | **maximal** | **fixed40** | **fixed50** | **fixed60** | *speed* } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
minimal	Sets the fan speed to the minimum speed of the device.	-
middle	Sets the fan speed to 70% of the full speed.	-
maximal	Sets the fan speed to the full speed.	-
fixed40	Sets the fan speed to 40% of the full speed.	-
fixed50	Sets the fan speed to 50% of the full speed.	-
fixed60	Sets the fan speed to 60% of the full speed.	-
speed	Specifies the percentage of the fan speed to the full speed.	The value is an integer from 20 to 100.

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The command for manually setting the fan speed is used only for fault locating. Generally, automatic fan speed adjustment is recommended.

Only devices installed with variable-speed fans support this command. Such fans support fan speed adjustment at two or multiple levels. The system can display the matching parameters according to the type of the fan installed on the device, and you do not need to know how many speed levels the fan supports.

Precautions

In a stack, the **set fan speed mandatory minimal** command will set the fan speed of each member switch to the minimum fan speed.

Example

Set the fan speed to 70% of the full speed.

```
<HUAWEI> system-view
[HUAWEI] set fan speed mandatory middle
```

3.2.41 set flash threshold

Function

The **set flash threshold** command sets the alarm threshold for flash memory usage.

The **undo set flash threshold** command restores the default alarm threshold for flash memory usage.

By default, the alarm threshold for flash memory usage is 80.

Format

set flash threshold *value*

undo set flash threshold *value*

Parameters

Parameter	Description	Value
value	Sets the alarm threshold for flash memory usage.	The value is an integer that ranges from 1 to 99.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To ensure that the switch has sufficient flash memory, run the **set flash threshold** command to set the alarm threshold for flash memory usage. When flash memory of the switch is insufficient, the system prompts that flash memory is insufficient so that you can determine the flash memory usage.

Example

Set the alarm threshold for flash memory usage on an MPU to 50%.

```
<HUAWEI> system-view
[HUAWEI] set flash threshold 50
Info: Now the flash usage threshold is 50%.
```

3.2.42 set integrated-power

Function

The **set integrated-power** command configures a voltage threshold for the device.

The **undo set integrated-power** command restores the default voltage threshold of the device.

By default, the DC overvoltage threshold is 58.00 V, the DC undervoltage threshold is 50.00 V, the low-load voltage threshold is 49.00 V, and the 53 V DC output voltage threshold is 53.00 V.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set integrated-power { **53v-dc output-voltage** | **dc-overvoltage** | **dc-undervoltage** | **low-load-voltage** } **threshold** *value*

undo set integrated-power { **53v-dc output-voltage** | **dc-overvoltage** | **dc-undervoltage** | **low-load-voltage** } **threshold**

Parameters

Parameter	Description	Value
53v-dc output-voltage	Configures a 53 V DC output voltage threshold.	-
dc-overvoltage	Configures a DC overvoltage threshold.	-
dc-undervoltage	Configures a DC undervoltage threshold.	-
low-load-voltage	Configures a low-load voltage threshold.	-
threshold *value*	Specifies a voltage threshold.	-
value	Specifies the threshold value.	The value range is as follows: ● **53v-dc output-voltage**: The value ranges from 53 to 56.4, in volts (V). ● **dc-overvoltage**: The value ranges from 53 to 60, in volts (V). ● **dc-undervoltage**: The value ranges from 35 to 57, in volts (V). ● **low-load-voltage**: The value ranges from 35 to 51.49, in volts (V).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure a voltage threshold.

Example

Set the low-load voltage threshold to 39.11 V.

```
<HUAWEI> system-view
[HUAWEI] set integrated-power low-load-voltage threshold 39.11
```

3.2.43 set memory-usage threshold

Function

The **set memory-usage threshold** command sets the memory usage threshold.

The **undo set memory-usage threshold** command restores the default memory usage threshold.

By default, the following describes the memory usage alarm threshold on the S1720GFR:

- If the memory capacity on the device is lower than or equal to 256 MB, the memory usage alarm threshold is 85% and the memory usage alarm recovery threshold is 80%.
- If the memory capacity on the device is larger than 256 MB and smaller than or equal to 512 MB, the memory usage alarm threshold is 90% and the memory usage alarm recovery threshold is 85%.
- If the memory capacity on the device is higher than 512 MB, the memory usage alarm threshold is 95% and the memory usage alarm recovery threshold is 90%.

The following describes the memory usage alarm threshold on other switch models:

- If the memory capacity on the device is lower than or equal to 512 MB, the memory usage alarm threshold is 85% and the memory usage alarm recovery threshold is 80%.
- If the memory capacity on the device is larger than 512 MB and smaller than or equal to 1.5 GB, the memory usage alarm threshold is 90% and the memory usage alarm recovery threshold is 85%.
- If the memory capacity on the device is higher than 1.5 GB, the memory usage alarm threshold is 95% and the memory usage alarm recovery threshold is 90%.

Format

set memory-usage threshold *threshold-value* [**slot** *slot-id*]

undo set memory-usage threshold [*threshold-value*] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the memory usage threshold.	The value is an integer that ranges from 75 to 100.

Parameter	Description	Value
slot *slot-id*	Specifies the memory usage threshold of a specified slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use the **set memory-usage threshold** command to set the memory usage threshold. When memory usage exceeds the threshold, the system logs the event and generates an alarm. By viewing log information, you can learn about memory usage.

Precautions

You are advised to use the default threshold. If the memory usage threshold is set too low, the system frequently generates alarms. If the memory usage threshold is set too high, you cannot learn about memory usage in a timely manner.

Example

Set the memory usage threshold to 85%.

```
<HUAWEI> system-view
[HUAWEI] set memory-usage threshold 85
```

3.2.44 set power protocol modbus

Function

The **set power protocol modbus** command configures the IP address and port number of a PC510 power supply for the switch to connect to.

The **undo set protocol modbus** command deletes the configuration.

By default, the IP address and port number of a PC510 power supply for the switch to connect to are not configured.

NOTE

This command is supported only by the S5735-L8P4X-IA1, S5735-L8T4X-IA1.

Format

set power protocol modbus [**ip-address** *ip-address-value*] [**tcp-port** *port-value*]

undo set power protocol modbus

Parameters

Parameter	Description	Value
ip-address *ip-address-value*	Specifies the IP address of a PC510 power supply.	The value is in dotted decimal notation. The default value is 192.168.18.88.
tcp-port *port-value*	Specifies the port number of a PC510 power supply.	The value is an integer ranging from 0 to 65535. The default value is 502.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PC510 power module provides multiple types of power outputs and can supply power to devices, such as switches and cameras, at the same time. To be powered by a PC510 power supply, the switch needs to set up a connection with the PC510 power supply using the Modbus TCP protocol. After connecting to a PC510 power supply, the switch can manage this power supply, for example, obtain its version information and restart it.

You need to run this command on the switch to configure the IP address and port number of the PC510 power supply so that the switch can set up a connection with it.

Precautions

- After running this command, to ensure that the switch can set up a connection with the power supply successfully, you need to create a VLANIF interface on the switch, configure an IP address on the same subnet as the power supply for the VLANIF interface, and add the interface connecting the switch to the power supply to the VLAN of the VLANIF interface.
- The IP address and port number of a PC510 power module are fixed at 192.168.18.88 and 502, respectively. Therefore, the IP address and port number configured using this command can only be 192.168.18.88 and 502.

Example

Configure the IP address and port number of a PC510 power supply for the switch to connect to.

```
<HUAWEI> system-view
[HUAWEI] set power protocol modbus ip-address 192.168.18.88 tcp-port 502
```

3.2.45 set root-key

Function

The **set root-key** command configures a root key for a switch.

The **undo set root-key** command restores the default root key of a switch.

By default, a switch uses the system default root key.

Format

set root-key [**auto**]

undo set root-key

Parameters

Parameter	Description	Value
auto	Automatically generates the root key of the device.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A root key is located at the bottom of the key management infrastructure to protect confidentiality of upper-layer keys (such as key encryption key). Therefore, a root key is important to data security. A switch's root key is often stored in the system. If attackers illegally obtain the root key, encrypted data will become insecure. To improve data security and prevent attackers from obtaining encrypted packets, configure another root key on the switch. The configured root key will take effect after the switch restarts.

If the device has high security requirements and its configuration file needs to be prevented from being used by other devices, run the **set root-key auto** command to automatically generate a root key for the device. You can run this command to automatically generate a root key only for an unconfigured device.

Precautions

- The root key can only be configured when the switch has no service configuration. If service configuration has been performed on the switch, an error message will be displayed when you configure the root key.
- If you configure a password (not the administrator password) and key after configuring the root key, the password and key configuration will not be restored after the switch software version is changed to V200R009 or an earlier version.
- After the root key is configured and the device is restarted, run the **display root-key configuration** command to check whether the configuration takes effect. After the configuration takes effect on the device, if you export the device's configuration file and apply it to other devices, other devices cannot work properly.
- Do not run this command to set the root key to the weak password preset by running the **load security weak-password-dictionary** command.

Example

Set the root key that meets the length requirements, for example, 98765432109876543210abc. Set this parameter based on the site requirements.

```
<HUAWEI> set root-key
Warning: A new root key can take effect only after the device is restarted. Continue? [Y/N]:y
Please enter a new key of no more than 32 and no less than 20 characters:
Please enter the new key again:
Info: Succeed in setting next root-key on the master board.
```

Configure automatic root key generation.

```
<HUAWEI> set root-key auto
```

3.2.46 set rtc to power

Function

The **set rtc to power** command synchronizes the time of the power supply with the device time.

NOTE

Only the S5735-S8P2X-IA200H1 supports this command.

Format

set rtc to power

undo set rtc to power

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to synchronize the time of the power supply with the device time.

Example

Synchronize the time of the power supply with the device time.

```
<HUAWEI> system-view
[HUAWEI] set rtc to power
```

3.2.47 set service-mode

Function

The **set service-mode** command sets the working mode of the device to enhanced.

The **undo set service-mode** command restores the working mode of the device to normal.

By default, the working mode of the device is normal.

NOTE

This command is supported only by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

Command format on the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H:

set service-mode { **enhanced-bfd** | **enhanced-oam** | **enhanced-ptp** }

undo set service-mode { **enhanced-bfd** | **enhanced-oam** | **enhanced-ptp** }

Command format on other switches:

set service-mode enhanced

undo set service-mode enhanced

Parameters

Parameter	Description	Value
enhanced	Sets the working mode of the device to enhanced.	-

Parameter	Description	Value
enhanced-bfd	Sets the BFD working mode of the device to enhanced.	-
enhanced-oam	Sets the OAM working mode of the device to enhanced.	-
enhanced-ptp	Sets the PTP working mode of the device to enhanced.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In normal mode, the interval for receiving BFD packets must be more than or equal to 100 ms. If the interval cannot meet requirements, run the **set service-mode** command to change the working mode of the switch to enhanced or **enhanced-bfd** mode so that the switch supports a minimum of 3 ms interval.

To implement some OAM functions, you need to run the **set service-mode** command to change the working mode of the switch to enhanced or **enhanced-oam** mode. For more details, see the OAM description.

To configure PTP, you need to run the **set service-mode** command to change the working mode of the switch to enhanced **enhanced-ptp** mode.

Precautions

- Running the **set service-mode** command will reduce the device forwarding performance. Therefore, confirm the action before you use the command.
- If BFD has been enabled before this command is executed, disable BFD first.
- Before changing the working mode from enhanced to normal, disable the PTP function.
- On the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H, you can run the **set service-mode** command multiple times to set the working mode of BFD, PTP, and OAM to enhanced.

Example

Set the working mode of the device to enhanced.

```
<HUAWEI> system-view
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
```

3.2.48 slave restart

Function

Using the **slave restart** command, you can reload the system software of the standby device and then restart it.

NOTE

This function is supported only on member devices in a stack.

Format

slave restart

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the standby switch is not working normally, you can reset it to restore its functions without affecting existing services.

Precautions

Due to the component upgrade of some device models, the devices whose first supported version is V200R021C10 cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about the first supported version of the device and matching patch version, see the device overview in the "Hardware Description".

NOTICE

The command may interrupt services on the device. Therefore, exercise caution when using this command.

Example

Restart the standby device.

```
<HUAWEI> system-view
[HUAWEI] slave restart
```

3.2.49 slave switchover

Function

The **slave switchover** command performs an active/standby switchover.

NOTE

This function is supported only on member devices in a stack.

Format

slave switchover

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack of multiple switches, you can manually perform an active/standby switchover on the master and standby switches during a software upgrade or system maintenance. After the active/standby switchover is complete, the original master switch restarts, becomes the new standby switch or a slave switch, and joins the stack, and the original standby switch becomes the new master switch.

Prerequisites

- The forcible active/standby switchover function has been enabled on devices.
- The **display switchover state** command output shows that system has met requirements for an active/standby switchover. The requirements for an active/standby switchover are met only when the value of **HA FSM State(master)** is **realtime or routine backup** and the value of **HA FSM State(slave)** is **receiving realtime or routine data**. This indicates that data is consistent on the master and standby switches.

Precautions

- You can run the **slave switchover** command to perform an active/standby switchover only in a stack of multiple switches.
- If an unregistered member switch exists in the stack, to prevent the stack from being split, do not run the **slave switchover** command to perform an active/standby switchover.
- If the **slave switchover** command is executed when other commands are being executed, you need to execute the commands that have not taken effect on the new master switch again after the original standby switch becomes the new master switch.
- Due to the component upgrade of some device models, some devices cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about the first supported version of the device and matching patch version, see the device overview in the "Hardware Description"..

Example

Perform an active/standby switchover.

```
<HUAWEI> system-view
[HUAWEI] slave switchover enable
[HUAWEI] slave switchover
Warning: This operation will switch the slave board to the master board. Continue? [Y/N]:y
```

3.2.50 slave switchover { disable | enable }

Function

The **slave switchover** { **disable** | **enable** } command enables or disables forcible master/slave switchover.

undo slave switchover disable command enables forcible master/slave switchover.

By default, master/slave switchover is enabled.

NOTE

This function is supported only on member devices in a stack.

Format

slave switchover { **disable** | **enable** }

undo slave switchover disable

Parameters

Parameter	Description	Value
disable	Disables forcible master/slave switchover.	-

Parameter	Description	Value
enable	Enables forcible master/slave switchover.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **slave switchover** command takes effect only after forcible master/slave switchover is enabled. If forcible master/slave switchover is disabled, the **slave switchover** command does not take effect.

Example

Disable forcible master/slave switchover.

```
<HUAWEI> system-view
[HUAWEI] slave switchover disable
```

3.2.51 system memory-usage monitor disable

Function

The **system memory-usage monitor disable** command disables the function of generating an alarm when the system memory usage reaches the threshold.

The **undo system memory-usage monitor disable** command enables the function of generating an alarm when the system memory usage reaches the threshold.

By default, the function of generating an alarm when the system memory usage reaches the threshold is enabled.

Format

system memory-usage monitor disable

undo system memory-usage monitor disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When the system memory is insufficient, services are abnormal. For example, configurations cannot be delivered or traffic cannot be forwarded. For the Linux operating system, when the system memory usage reaches 90%, the device reports an alarm indicating that the memory usage reaches the threshold by default.

If the memory is sufficient and the memory insufficiency alarm does not need to be reported, you can run this command to disable the function of reporting an alarm when the system memory usage reaches the threshold.

Example

Disable the function of generating an alarm when the system memory usage reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] system memory-usage monitor disable
```

3.2.52 temperature threshold

Function

The **temperature threshold** command sets the temperature alarm thresholds.

The **undo temperature threshold** command restores the default temperature alarm thresholds.

By default, the lower temperature threshold is -40°C on the S5720I-SI and S5735-S-I, and -3°C on the S5731-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S, S5735S-S, S5736-S, and S6730-H, and 0°C on other switch models, and the upper temperature threshold varies according to hardware of various models, ranging from 44°C to 88°C.

Format

temperature threshold slot { *slot-id* | **all** } **lower-limit** *min-temperature* **upper-limit** *max-temperature*

undo temperature threshold slot { *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Parameter	Description	Value
all	Sets the temperature alarm threshold for all member switches in a stack.	-
lower-limit *min-temperature*	Specifies the lower temperature alarm threshold.	The value is an integer that ranges from -40 to 88. *min-temperature* specifies the value of the temperature. The value of *min-temperature* varies according to device models. The minimum value of *min-temperature* is the default lower threshold. In a stack of multiple member switches, when **all** is specified in the **temperature threshold** command and the temperature alarm thresholds of all member switches are set, the *min-temperature* value is the largest value among the lower temperature alarm thresholds of the member switches.

Parameter	Description	Value
upper-limit *max-temperature*	Specifies the upper temperature alarm threshold.	The value is an integer that ranges from -40 to 88. *max-temperature* specifies the value of the temperature. The value of *max-temperature* varies according to device models. The maximum value of *max-temperature* is the default upper threshold. *max-temperature* must be at least 10 greater than *min-temperature*. In a stack of multiple member switches, when **all** is specified in the **temperature threshold** command and the temperature alarm thresholds of all member switches are set, the *max-temperature* value is the smallest value among the upper temperature alarm thresholds of the member switches.

Views

system view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device generates an alarm and records log information when the device temperature falls below the lower threshold or rises above the upper threshold.

Precautions

- If the configured threshold values are out of the allowed range, the configuration fails and the upper and lower thresholds are restored to the maximum values.

- Configuration commands are generated in a configuration file regardless of whether the configured threshold values are default values. These commands can be cleared only when the **undo temperature threshold** command is executed.

Example

Set the lower temperature alarm threshold to 20°C and upper temperature alarm threshold to 60°C.

```
<HUAWEI> system-view
[HUAWEI] temperature threshold slot all lower-limit 20 upper-limit 60
```

3.2.53 transceiver diagnosis threshold rx-power

Function

The **transceiver diagnosis threshold rx-power** command sets the upper and lower thresholds for the receive optical power of the optical transceiver installed in an interface.

The **undo transceiver diagnosis threshold rx-power** command restores the upper and lower thresholds to the default values for the receive optical power of the optical transceiver installed in an interface.

By default, the optical power upper and lower thresholds vary according to optical module vendors.

Format

transceiver diagnosis threshold rx-power { **default** | **low-alarm** *low-alarm* **high-alarm** *high-alarm* }

undo transceiver diagnosis threshold rx-power

Parameters

Parameter	Description	Value
default	Sets the upper and lower thresholds for the receive optical power of the optical transceiver installed in an interface to default values.	-
high-alarm *high-alarm*	Sets the upper threshold for the receive optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.

Parameter	Description	Value
low-alarm *low-alarm*	Sets the lower threshold for the receive optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **transceiver diagnosis threshold rx-power** command to adjust the receive optical power of the optical transceiver.

Example

Set the upper and lower thresholds for the receive optical power of the optical transceiver installed in GigabitEthernet 0/0/2 to default values.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] transceiver diagnosis threshold rx-power default
```

3.2.54 transceiver diagnosis threshold tx-power

Function

The **transceiver diagnosis threshold tx-power** command sets the upper and lower thresholds for the transmit optical power of the optical transceiver installed in an interface.

The **undo transceiver diagnosis threshold tx-power** command restores the upper and lower thresholds for the transmit optical power of the optical transceiver installed in an interface to default values.

By default, the optical power upper and lower thresholds vary according to optical module vendors.

Format

transceiver diagnosis threshold tx-power { **default** | **low-alarm** *low-alarm* **high-alarm** *high-alarm* }

undo transceiver diagnosis threshold tx-power

Parameters

Parameter	Description	Value
default	Sets the upper and lower thresholds for the transmit optical power of the optical transceiver installed in an interface to default values.	-
high-alarm *high-alarm*	Sets the upper threshold for the transmit optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.
low-alarm *low-alarm*	Sets the lower threshold for the transmit optical power of the optical transceiver installed in an interface.	The value varies according to the optical module vendor.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **transceiver diagnosis threshold tx-power** command to adjust the transmit optical power of the optical transceiver.

Example

Set the upper and lower thresholds for the transmit optical power of the optical transceiver installed in GigabitEthernet 0/0/2 to default values.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] transceiver diagnosis threshold tx-power default
```

3.2.55 transceiver phony-alarm-disable

Function

The **transceiver phony-alarm-disable** command disables the alarm function for non-Huawei-certified switch optical modules.

The **undo transceiver phony-alarm-disable** command enables the alarm function for non-Huawei-certified switch optical modules.

By default, the alarm function is enabled for non-Huawei-certified switch optical modules.

Format

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Non-Huawei-certified switch optical modules may fail to work normally. If non-Huawei-certified switch optical modules are used on devices produced since July 1, 2013 (January 1, 2016 for QSFP+ 40GE optical modules), the devices generate a large number of alarms to prompt users to replace these optical modules with Huawei-certified switch optical modules. However, vendor information of optical modules early delivered from Huawei may not be recorded. Therefore, non-Huawei-certified switch optical module alarms are generated. These optical modules can still be used to protect customer investment. In this case, you can disable the alarm function for non-Huawei-certified switch optical modules.

Example

Disable the alarm function for non-Huawei-certified switch optical modules.

```
<HUAWEI> system-view
[HUAWEI] transceiver phony-alarm-disable
Info:Transceiver-phony-alarm disable.
```

Enable the alarm function for non-Huawei-certified switch optical modules.

```
<HUAWEI> system-view
[HUAWEI] undo transceiver phony-alarm-disable
Info:Transceiver-phony-alarm enable.
```

3.2.56 wavelength-channel

Function

The **wavelength-channel** command sets the wavelength channel of a wavelength-tunable optical module.

The **undo wavelength-channel** command restores the default wavelength channel of a wavelength-tunable optical module.

The default wavelength channel of a wavelength-tunable optical module is channel 1.

Format

wavelength-channel *channelnum*

undo wavelength-channel

Parameters

Parameter	Description	Value
channelnum	Specifies a wavelength channel number.	The value is an integer that ranges from 1 to 80.

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To adjust the wavelength of a wavelength-tunable optical module on an interface, run the **wavelength-channel** *channelnum* command on this interface. This command will add the wavelength-tunable optical module to a specified wavelength channel. Each wavelength channel has a fixed center wavelength and frequency. To view the mapping between the wavelength channel, center wavelength, and frequency, run the **display wavelength-map** command.

You can also run the **wavelength-channel frequency** *frequency-value* and **wavelength-channel wavelength** *wavelength-value* commands to set the wavelength and frequency of a wavelength-tunable optical module.

Precautions

- When the **wavelength-channel** command configuration exists on the interface, after the interface has a wavelength-tunable optical module installed, this optical module will automatically adjust its wavelength to the configured wavelength. If a copper module is installed, the command configuration remains but does not take effect. If a non-wavelength-tunable optical module is installed, the command configuration will not take effect and the system displays an alarm.
- Running the **wavelength-channel** command will open and close the laser, resulting in interface flapping.
- The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value*

commands are mutually exclusive with the **wavelength-channel trust sfp** command.

Example

Add a wavelength-tunable optical module to wavelength channel 20 on XGigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel 20
```

3.2.57 wavelength-channel frequency

Function

The **wavelength-channel frequency** command sets the frequency of a wavelength-tunable optical module.

The **undo wavelength-channel frequency** command restores the default frequency of a wavelength-tunable optical module.

The default frequency of a wavelength-tunable optical module is the same as that of wavelength channel 1.

Format

wavelength-channel frequency *frequency-value*

undo wavelength-channel frequency

Parameters

Parameter	Description	Value
frequency-value	Specifies a frequency.	The value is an integer ranging from 0 to 4294967295, in MHz.

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two interfaces installed with optical modules are connected through optical fibers, the wavelengths of the two optical modules must match, and so do their frequencies; otherwise, the interfaces cannot go Up or transmit traffic. When a wavelength-tunable optical module is connected to an optical module with a fixed wavelength and frequency, you need to change the wavelength and frequency of the wavelength-tunable optical module to match with those of its connected optical module, respectively.

You can run the **wavelength-channel frequency** *frequency-value* command to set the frequency of a wavelength-tunable optical module and run the **wavelength-channel wavelength** *wavelength-value* command to set the wavelength of a wavelength-tunable optical module. You can also run the **wavelength-channel** *channelnum* command to set the wavelength channel of a wavelength-tunable optical module. This changes its wavelength and frequency at the same time. To view the mapping between the wavelength channel, wavelength, and frequency, run the **display wavelength-map** command.

Precautions

- When the **wavelength-channel** command configuration exists on the interface, after the interface has a wavelength-tunable optical module installed, this optical module will automatically adjust its wavelength to the configured wavelength. If a copper module is installed, the command configuration remains but does not take effect. If a non-wavelength-tunable optical module is installed, the command configuration will not take effect and the system displays an alarm.
- Running the **wavelength-channel** command will open and close the laser, resulting in interface flapping.
- The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value* commands are mutually exclusive with the **wavelength-channel trust sfp** command.

Example

Set the frequency of the wavelength-tunable optical module on XGigabitEthernet 0/0/2 to 192100000 MHz.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel frequency 192100000
```

3.2.58 wavelength-channel wavelength

Function

The **wavelength-channel wavelength** command sets the wavelength of a wavelength-tunable optical module.

The **undo wavelength-channel wavelength** command restores the default wavelength of a wavelength-tunable optical module.

The default wavelength of a wavelength-tunable optical module is the same as that of wavelength channel 1.

Format

wavelength-channel wavelength *wavelength-value*

undo wavelength-channel wavelength

Parameters

Parameter	Description	Value
wavelength-value	Specifies a wavelength.	The value is an integer ranging from 0 to 4294967295, in pm.

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two interfaces installed with optical modules are connected through optical fibers, the wavelengths of the two optical modules must match, and so do their frequencies; otherwise, the interfaces cannot go Up or transmit traffic. When a wavelength-tunable optical module is connected to an optical module with a fixed wavelength and frequency, you need to change the wavelength and frequency of the wavelength-tunable optical module to match with those of its connected optical module, respectively.

You can run the **wavelength-channel frequency** *frequency-value* command to set the frequency of a wavelength-tunable optical module and run the **wavelength-channel wavelength** *wavelength-value* command to set the wavelength of a wavelength-tunable optical module. You can also run the **wavelength-channel** *channelnum* command to set the wavelength channel of a wavelength-tunable optical module. This changes its wavelength and frequency at the same time. To view the mapping between the wavelength channel, wavelength, and frequency, run the **display wavelength-map** command.

Precautions

- When the **wavelength-channel** command configuration exists on the interface, after the interface has a wavelength-tunable optical module installed, this optical module will automatically adjust its wavelength to the configured wavelength. If a copper module is installed, the command configuration remains but does not take effect. If a non-wavelength-tunable optical module is installed, the command configuration will not take effect and the system displays an alarm.
- Running the **wavelength-channel** command will open and close the laser, resulting in interface flapping.
- The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value*

commands are mutually exclusive with the **wavelength-channel trust sfp** command.

Example

Set the wavelength of the wavelength-tunable optical module on XGigabitEthernet 0/0/2 to 1560606 pm.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel wavelength 1560606
```

3.2.59 wavelength-channel trust sfp

Function

The **wavelength-channel trust sfp** command configures a device to trust the wavelength channel of an optical module.

The **undo wavelength-channel trust sfp** command deletes the configuration.

By default, a device does not trust the wavelength channel of an optical module.

Format

wavelength-channel trust sfp

undo wavelength-channel trust sfp

Parameters

None

Views

XGE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a wavelength-tunable optical module is installed on a device, the device forcibly sets the wavelength channel to the default value 1 or a value configured using the **wavelength-channel** *channelnum* command. This makes the wavelength channel on the local device be different from that of on the remote device. As a result, the two devices fail to communicate. In this case, you can run the **wavelength-channel trust sfp** command to configure the device to trust the wavelength channel of the optical module.

Precautions

The **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, and **wavelength-channel wavelength** *wavelength-value* are mutually exclusive with the **wavelength-channel trust sfp** command. That is:

- After the **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, or **wavelength-channel wavelength** *wavelength-value* command is configured, the **wavelength-channel trust sfp** command cannot be configured.
- After the **wavelength-channel trust sfp** command is configured, the **wavelength-channel** *channelnum*, **wavelength-channel frequency** *frequency-value*, or **wavelength-channel wavelength** *wavelength-value* command cannot be configured.

Example

Configure the device to trust the wavelength channel of the optical module on XGigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/2
[HUAWEI-XGigabitEthernet0/0/2] wavelength-channel trust sfp
```

3.3 Stack Configuration Commands

3.3.1 Command Support

Table 3-50 Applicable product models and versions

Product	Software Version	Stack Connection Mode	Product Model
S200	Not supported	-	All S200 switches do not support stacking.
S300	V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S300 switches support stacking.
S300	V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S500 switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S1720 and S1730	Not supported	-	All S1720 and S1730 switches do not support stacking.
S2700-SI	Not supported	-	All S2700-SI switches do not support stacking.
S2710-SI	V100R006(C03&C05)	Service port connection using ordinary cables	All S2710-SI switches support stacking.
S2700-EI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables	S2700-9TP-EI-AC, S2700-9TP-EI-DC, S2700-9TP-PWR-EI, S2700-18TP-EI-AC, S2700-26TP-EI-AC, S2700-26TP-EI-DC, and S2700-26TP-PWR-EI do not support stacking, whereas other models support.

Product	Software Version	Stack Connection Mode	Product Model
S2720-EI	Versions supporting service port connection using ordinary cables: V200R006C10, V200R009C00, V200R010C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00	Service port connections using ordinary and dedicated cables	All S2720-EI switches support stacking.
S2730S-S	Versions supporting service port connection using ordinary cables: V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S2730S-S switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S2750-EI	Versions supporting service port connection using ordinary cables: V200R003C00, V200R005C00SPC300, V200R006C00, V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	All S2750-EI switches support stacking.
S3700-SI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables	All S3700-SI switches support stacking.
S3700-EI	V100R005C01, V100R006(C00&C01&C03&C05)	Service port connection using ordinary cables	All S3700-EI switches support stacking.
S3700-HI	Not supported	-	All S3700-HI switches do not support stacking.
S5700-EI	V100R005C01, V100R006(C00&C01), V200R001(C00&C01), V200R002C00, V200R003C00, V200R005(C00&C01&C02&C03)	Stack card connection	All S5700-EI switches support stacking.
S5700-SI	V100R005C01, V100R006C00, V200R001C00, V200R002C00, V200R003C00, V200R005C00	Stack card connection	S5700-26X-SI-12S-AC does not support stacking, whereas other models support.

Product	Software Version	Stack Connection Mode	Product Model
S5700-HI	V200R003C00, V200R005C00	Service port connection using ordinary cables	All S5700-HI switches support stacking.
S5700-LI	Versions supporting service port connection using ordinary cables: V200R001C00, V200R002C00, V200R003(C00&C02&C10), V200R005C00SPC300, V200R006C00, V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	S5700-10P-LI-AC, S5700-10P-PWR-LI-AC, S5700-28P-LI-BAT, and S5700-28P-LI-24S-BAT do not support stacking, whereas other models support.
S5700S-LI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	S5700S-28P-LI-AC and S5700S-52P-LI-AC do not support stacking, whereas other models support.
S5710-EI	V200R001C00, V200R002C00, V200R003C00, V200R005(C00&C02)	Service port connection using ordinary cables	All S5710-EI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5710-HI	V200R005C03	Service port connection using ordinary cables	All S5710-HI switches support stacking.
S5710-C-LI	V200R001C00	Stack card connection	All S5710-C-LI switches support stacking.
S5710-X-LI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00 Versions supporting service port connection using dedicated cables: V200R011C10 and V200R012C00	Service port connections using ordinary and dedicated cables	All S5710-X-LI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5720-LI and S5720S-LI	Versions supporting service port connection using ordinary cables: V200R010C00, V200R011C00, V200R011C10, V200R012(C00&C20), V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5720-LI and S5720S-LI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5720-SI and S5720S-SI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S5720-SI and S5720S-SI switches support stacking.
S5720I-SI	V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	S5720I-6X-PWH-SI-AC and S5720I-10X-PWH-SI-AC do not support stacking, whereas other models support.

Product	Software Version	Stack Connection Mode	Product Model
S5720-EI	V200R007C00, V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connection using ordinary cables: S5720-C-EI, S5720-PC-EI Stack card connection: S5720-P-EI, S5720-C-EI, S5720-X-EI, S5720-PC-EI When using the stack card connection mode, note the following: ● S5720-C-EI and S5720-PC-EI series switches use dedicated stack cards to set up stacks. ● S5720-X-EI and S5720-P-EI series switches use stack ports fixed on cards to set up stacks.	All S5720-EI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5720-HI	Versions supporting service port connection using ordinary cables: V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S5720-HI switches support stacking.
S5730-HI	V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S5730-HI switches support stacking.
S5731-H	V200R013C02, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5731-H switches support stacking.
S5731S-H	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5731S-H switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5731-L and S5731S-L	Not supported	-	All S5731-L and S5731S-L switches do not support stacking.
S5731-S and S5731S-S	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5731-S and S5731S-S switches support stacking.
S5732-H	Versions supporting service port connection using ordinary cables: V200R019C00, V200R019C10, V200R019C20, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5732-H switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5730-SI	Versions supporting service port connection using ordinary cables and dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting stack card connection: V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables, and stack card connection	All S5730-SI switches support stacking.
S5730S-EI	Versions supporting service port connection using ordinary cables and dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting stack card connection: V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables, and stack card connection	All S5730S-EI switches support stacking.
S5735-L, S5735S-L, and S5735S-L-M	V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5735-L, S5735S-L, and S5735S-L-M switches support stacking.
S5735-L-I	V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5735-L-I switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S5735-L1 and S5735S-L1	V200R020C10, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	S5735-L8T4S-A1(98011284-001), S5735-L8P4S-A1(98011295-001), S5735-L24T4S-A1(98011306-001), and S5735-L24P4S-A1(98011321-001) do not support stacking, whereas other models support.
S5735-S and S5735S-S	V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S5735-S and S5735S-S switches support stacking.
S5735-S-I	V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	Only the S5735-S24T4X-I switch supports stacking.
S5735S-H	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connection using ordinary cables	All S5735S-H switches support stacking.
S5736-S	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connection using ordinary cables	All S5736-S switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6700-EI	V100R006C00, V200R001(C00&C01), V200R002C00, V200R003C00, V200R005(C00&C01&C02)	Service port connection using ordinary cables	All S6700-EI switches support stacking.
S6720-EI	Versions supporting service port connection using ordinary cables: V200R008C00, V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6720-EI switches support stacking.
S6720-HI	V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S6720-HI switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6720S-EI	Versions supporting service port connection using ordinary cables: V200R009C00, V200R010C00, V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6720S-EI switches support stacking.
S6720S-S	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connection using ordinary cables	All S6720S-S switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6720-SI and S6720S-SI	Versions supporting service port connection using ordinary cables: V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S6720-SI and S6720S-SI switches support stacking.
S6720-LI and S6720S-LI	Versions supporting service port connection using ordinary cables: V200R011C00, V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10 Versions supporting service port connection using dedicated cables: V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10	Service port connections using ordinary and dedicated cables	All S6720-LI and S6720S-LI switches support stacking.
S6730-H	V200R013C02, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6730-H switches support stacking.

Product	Software Version	Stack Connection Mode	Product Model
S6730S-H	V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6730S-H switches support stacking.
S6730-S and S6730S-S	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R021C00, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6730-S and S6730S-S switches support stacking.
S6735-S	V200R021C00SPC600, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00	Service port connections using ordinary and dedicated cables	All S6735-S switches support stacking.

3.3.2 display mad

Function

The **display mad** command displays the multi-active detection (MAD) configuration.

Format

display mad [**proxy** | **verbose**]

Parameters

Parameter	Description	Value
proxy	Displays information about the proxy device.	-
verbose	Displays detailed MAD configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the MAD configuration, run the **display mad** command. If the **verbose** parameter is specified, detailed MAD configuration is displayed, including MAD-enabled interfaces and interfaces excluded from shutdown.

When MAD in relay mode is configured, you can run the **display mad proxy** command on the proxy device to check its MAD configuration.

Example

Display MAD configuration.

```
<HUAWEI> display mad
Current MAD domain: 0
MAD direct detection enabled: YES
MAD relay detection enabled: NO
```

Display detailed MAD configuration.

```
<HUAWEI> display mad verbose
Current MAD domain: 0
Current MAD status: Detect
Mad direct detect interfaces configured:
 GigabitEthernet2/0/8
 GigabitEthernet2/0/9
Mad relay detect interfaces configured:
Excluded ports(configurable):
 GigabitEthernet2/0/4
Excluded ports(can not be configured):
```

Display information about the specified proxy device.

```
<HUAWEI> display mad proxy
Mad relay interfaces configured:
 Eth-Trunk1
```

Table 3-51 Description of the **display mad** command output

Item	Description
Current MAD domain	MAD domain configured in the system. To configure this parameter, run the **mad domain** command.
MAD direct detection enabled	MAD in direct mode is configured. To configure MAD in direct mode, run the **mad detect mode direct** command.
MAD relay detection enabled	MAD in relay mode is configured. To configure MAD in relay mode, run the **mad detect mode relay** command.

Item	Description
Current MAD status	Current MAD status: ● Detect: The stack is running properly. ● Recovery: The switch that fails master switch election in a MAD scenario enters the Recovery state and blocks all of its service ports except those excluded from shutdown.
Mad direct detect interfaces configured	Interface on which MAD in direct mode is configured. To configure MAD in direct mode on an interface, run the **mad detect mode direct** command.
Mad relay detect interfaces configured	Interface on which MAD in relay mode is configured. To configure MAD in relay mode on an interface, run the **mad detect mode relay** command.
Excluded ports(configurable)	Interfaces excluded from shutdown. To configure interfaces excluded from shutdown, run the **mad exclude** command.
Excluded ports(can not be configured)	Interfaces that are excluded from shutdown in the system by default.
Mad relay interfaces configured	Interface on which the relay function is configured. To configure the relay function on an interface, run the **mad relay** command.

3.3.3 display stack

Function

The **display stack** command displays information about the member switches in a stack.

Format

display stack

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check stack information, including stack topology and stack member switches, run the **display stack** command.

This command can be used only after the stack function is enabled (default status).

Example

Display stack information.

```
<HUAWEI> display stack
Stack mode: Service-port
Stack topology type: Link
Stack system MAC: xxxx-xxxx-xxxx
MAC switch delay time: 10 min
Stack reserved VLAN: 4093
Slot of the active management port: 0
Slot   Role        MAC address      Priority   Device type
-------------------------------------------------------------
  0    Master      xxxx-xxxx-xxxx   200        S5720-28P-LI-AC
  1    Standby     xxxx-xxxx-xxxx   150        S5720-28P-LI-AC
```

Table 3-52 Description of the **display stack** command output

Item	Description
Stack mode	Stack connection mode supported by the switch: ● Service-port: Service port connection ● Card: Stack card connection
Stack topology type	Stack topology type: ● Link: chain topology ● Ring: ring topology
Stack system MAC	Stack system MAC address.
MAC switch delay time	Time after which the system MAC address of the stack is switched. To configure this parameter, run the **stack timer mac-address switch-delay** command.

Item	Description
Stack reserved VLAN	Stack reserved VLAN. To configure this parameter, run the **stack reserved-vlan** command.
Active management slot	Slot ID of the effective management interface in the stack. If no member switch in the stack has a management interface or all the management interfaces are Down, this field displays **--**. **NOTE** After a stack is set up, you can log in to the stack through any member switch's management interface or console interface. A stack can have only one effective management interface at a time.
Slot	Stack ID of the member switch.
Role	Member switch role: ● Master ● Standby ● Slave
MAC address	MAC address of the member switch.
Priority	Stack priority. To configure this parameter, run the **stack slot priority** command.
Device Type	Device model of the member switch.

3.3.4 display stack peers

Function

The **display stack peers** command displays information about the neighbors of a member switch.

Format

display stack peers

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check information about the neighbors of a member switch, run the **display stack peers** command.

This command can be used only after the stack function is enabled (default status).

Example

Display information about the neighbors of a member switch.

```
<HUAWEI> display stack peers
(B): Block all
Slot     Port1              Peer1     Port2              Peer2
--------------------------------------------------------------------------
0        STACK 1              1       STACK 2             None
1        STACK 1            None       STACK 2              0
```

Table 3-53 Description of the **display stack peers** command output

Item	Description
(B): Block all	Indicates that the stack port is blocked.
Slot	Stack ID of a member switch.
Port1	Stack port 1.
Peer1	Stack ID of the switch to which stack port 1 connects. If this field displays **ID(B)**, stack port 1 is blocked. If this field displays **None**, there is no peer device.
Port2	Stack port 2.
Peer2	Stack ID of the switch to which stack port 2 connects. If this field displays **ID(B)**, stack port 2 is blocked. If this field displays **None**, there is no peer device.

3.3.5 display stack port

Function

The **display stack port** command displays information about stack ports.

Format

display stack port [**brief** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
brief	Displays summary of stack ports.	-
slot *slot-id*	Displays configuration of stack ports on a specified switch. *slot-id* specifies the stack ID of a switch.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack port** command to check summary and detailed information about stack ports.

Example

Display summary of stack ports on the S5720-LI (service port connection).

```
<HUAWEI> display stack port brief
PHY     :Physical state
Protocol:Stack link protocol state
*down   :administratively down
(r)     :Runts trigger error down
(c)     :CRC trigger error down
(l)     :Link-flapping trigger error down
(m)     :Media mismatch trigger error down
Stack Port              PHY    Protocol  InUti  OutUti    InErrors   OutErrors
------------------------------------------------------------------------------
stack-port0/1            up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/1  up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/2  up     up        0.00%  0.00%     0          0
stack-port0/2            up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/3  up     up        0.00%  0.00%     0          0
  XGigabitEthernet0/0/4  up     up        0.00%  0.00%     0          0
```

Display summary of stack ports on the S6720-EI (service port connection).

```
<HUAWEI> display stack port brief
PHY     :Physical state
Protocol:Stack link protocol state
*down   :administratively down
(r)     :Runts trigger error down
(c)     :CRC trigger error down
(l)     :Link-flapping trigger error down
(m)     :Media mismatch trigger error down
Stack Port              PHY    Protocol  InUti  OutUti    InErrors   OutErrors
------------------------------------------------------------------------------
stack-port0/1
  XGigabitEthernet0/0/1  down   down      0.00%   0.00%          0
0
```

```
unAllocated
  XGigabitEthernet0/0/2  down   --       0.00%   0.00%          0          0
  XGigabitEthernet0/0/3  down   --       0.00%   0.00%          0          0
  XGigabitEthernet0/0/4  down   --       0.00%   0.00%          0          0
```

Table 3-54 Description of the **display stack port brief** command output

Item	Description
Stack Port	Number of a stack port. unAllocated indicates that a service port has become a stack member port but has not been bound to a logical stack port.
PHY	Physical status of an interface: ● down: The interface is physically disabled. ● up: The interface is physically enabled. ● *down: The interface is manually shut down. ● down(r): Runts error continuously occurs on a stack port. ● down(c): There are CRC error packets on a stack port. ● down(l): A stack port repeatedly alternates between Up and Down states. ● down(m): The rate of the optical module installed in a stack member port is not the rate required by the member port. ● down(s): A self-loop occurs on a stack port. **NOTE** Only the S5736-S, S5735-L, S5735S-L, S5735-L-I, S5735-L1,S5735S-L1, S5735S-L-M, S5735-S, S5735-S-I, S5735S-S, S5735S-H, and S6720S-S support this status.
Protocol	Link layer protocol status of the interface: ● down: A stack port does not receive stack link packets. ● up: A stack port can receive stack link detection packets.
InUti	Average inbound bandwidth usage of an interface within the last 300 seconds.
OutUti	Average outbound bandwidth usage within the last 300 seconds.
InErrors	Number of error packets received by an interface.
OutErrors	Number of error packets sent by an interface.

Display detailed information about stack ports (stack card connection).

```
<HUAWEI> display stack port
stack-port1/1:
---------------------------------------------
```

```
Current state : DOWN
Speed : NA

Input:  0 packets, 0 bytes
  Unicast:                        0,  Multicast:                        0
  Broadcast:                      0,  Jumbo:                            0
  Discard:                        0,  Frames:                           0

  Total Error:                    0
  CRC:                            0,  Giants:                           0
  Jabbers:                        0,  Fragments:                        0
  Runts:                          0,  DropEvents:                       0
  Alignments:                     0,  Symbols:                          0
  Ignoreds:                       0

Output:  0 packets, 0 bytes
  Unicast:                        0,  Multicast:                        0
  Broadcast:                      0,  Jumbo:                            0
  Discard:                        0

  Total Error:                    0
  Collisions:                     0,  ExcessiveCollisions:              0
  Late Collisions:                0,  Deferreds:                        0
  Buffers Purged:                 0


stack-port1/2:
--------------------------------------------
Current state : DOWN
Speed : NA

Input:  0 packets, 0 bytes
  Unicast:                        0,  Multicast:                        0
  Broadcast:                      0,  Jumbo:                            0
  Discard:                        0,  Frames:                           0

  Total Error:                    0
  CRC:                            0,  Giants:                           0
  Jabbers:                        0,  Fragments:                        0
  Runts:                          0,  DropEvents:                       0
  Alignments:                     0,  Symbols:                          0
  Ignoreds:                       0

Output:  0 packets, 0 bytes
  Unicast:                        0,  Multicast:                        0
  Broadcast:                      0,  Jumbo:                            0
  Discard:                        0

  Total Error:                    0
  Collisions:                     0,  ExcessiveCollisions:              0
  Late Collisions:                0,  Deferreds:                        0
  Buffers Purged:                 0
```

Table 3-55 Description of the **display stack port** command output (stack card connection)

Item	Description
stack-port1/1	Stack port 1 in slot 1.
Speed	Interface forwarding rate.
current state	Stack port status: - DOWN: The stack port is disabled. - UP: The stack port is enabled.

Item	Description
Input	Total number of packets received by the stack port.
Output	Total number of packets sent by the stack port.
Unicast	Number of unicast packets sent or received by the stack port.
Multicast	Number of multicast packets sent or received by the stack port.
Broadcast	Number of broadcast packets sent or received by the stack port.
Jumbo	Number of jumbo frames sent or received by the stack port.
Discard	Number of packets discarded by the stack port during physical layer detection.
Total Error	Total number of error packets found by the stack port during physical layer detection.
CRC	Number of CRC error packets received by the stack port.
Giants	Number of jumbo frames with correct FCS received by the stack port.
Jabbers	Number of jumbo frames with incorrect FCS received by the stack port.
Fragments	Number of undersized frames with incorrect FCS received by the stack port.
Runts	Number of undersized frames with correct FCS received by the stack port.
DropEvents	Number of received packets that are discarded because the GBP is full or there is back pressure.
Alignments	Number of frames with alignment errors received by the stack port.
Symbols	Number of coding error frames received by the stack port.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Frames	Number of packets with an incorrect 802.3 length received by the stack port.
Collisions	Number of packets that encountered 1 to 15 conflicts and sent by the stack port.
ExcessiveCollisions	Number of packets that encountered 16 conflicts and fail to be sent by the stack port.

Item	Description
Late Collisions	Number of packets sent by the stack port after a delay due to conflicts.
Deferreds	Number of packets sent by the stack port after a delay without any conflict.
Buffers Purged	Number of packets aged due to existence in the buffer for an extended time before being sent out by the stack port.

Display detailed information about stack ports (service port connection).

```
<HUAWEI> display stack port
*down : administratively down
Logic Port         Phy Port                    Online       Status
---------------------------------------------------------------------------
stack-port0/1      XGigabitEthernet0/0/1        present      up
                   XGigabitEthernet0/0/2        present      down
                   XGigabitEthernet0/0/4        present      down
stack-port0/2      XGigabitEthernet0/0/3        present      up
stack-port3/1      XGigabitEthernet3/0/1        present      up
stack-port3/2      XGigabitEthernet3/0/3        present      up
stack-port4/1      XGigabitEthernet4/0/1        present      up
stack-port4/2      XGigabitEthernet4/0/3        present      up
stack-port8/1      XGigabitEthernet8/0/1        present      up
stack-port8/2      XGigabitEthernet8/0/3        present      up
```

Table 3-56 Description of the **display stack port** command output (service port connection)

Item	Description
Logic Port	Number of a stack port.
Phy Port	Type and number of a physical member port.
Online	Presence of a physical member port. ● present: The current installed service card type is consistent with that configured on the switch. ● absent: The current installed service card type is inconsistent with that configured on the switch.

Item	Description
Status	Physical status of an interface: - down: The interface is physically disabled. - up: The interface is physically enabled. - *down: The interface is manually shut down. - down(r): Runts error continuously occurs on a stack port. - down(c): There are CRC error packets on a stack port. - down(l): A stack port repeatedly alternates between Up and Down states. - down(m): The rate of the optical module installed in a stack member port is not the rate required by the member port. - down(s): A self-loop occurs on a stack port. **NOTE** Only the S5736-S, S5735-L, S5735S-L, S5735-L-I, S5735-L1,S5735S-L1, S5735S-L-M, S5735-S, S5735-S-I, S5735S-S, S5735S-H, and S6720S-S support this status.

3.3.6 display stack port auto-cable-info

Function

The **display stack port auto-cable-info** command displays information about dedicated stack cables.

Format

display stack port auto-cable-info slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a member switch.	The value range depends on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack port auto-cable-info** command to check interfaces supporting dedicated stack cables and whether dedicated stack cables have been connected to interfaces.

Example

Display information about dedicated stack cables on the switch with the slot ID 0.

```
<HUAWEI> display stack port auto-cable-info slot 0
Logic Port        Phy Port                   Cable-role
---------------------------------------------------------
stack-port0/1     XGigabitEthernet0/0/1      Slave
stack-port0/1     XGigabitEthernet0/0/2      --
stack-port0/2     XGigabitEthernet0/0/3      --
stack-port0/2     XGigabitEthernet0/0/4      Master
```

Table 3-57 Description of the **display stack port auto-cable-info** command output

Item	Description
Logic Port	Logical stack port.
Phy Port	Physical member port.
Cable-role	Role of a dedicated stack cable: ● Master: The installed dedicated stack cable is the master end. ● Slave: The installed dedicated stack cable is the slave end. ● --: No dedicated stack cable is connected to the current port.

3.3.7 display stack port speed

Function

The **display stack port speed** command displays the stack port working speed.

NOTE

Only the S5720-X-LI, S5720I-SI, S5732-H, and S5720S-X-LI support this command.

The S5720-P-LI does not support this command before the license is loaded and supports this command after the license is loaded and it restarts.

Format

display stack port speed

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack port speed** command to check the stack port's current working speed and working speed taking effect after a restart. To set the stack port working speed, run the **stack port speed** command.

Example

Display the stack port's current working speed and working speed taking effect after a restart.

```
<HUAWEI> display stack port speed
Stack Port                Current Speed    Next Speed
-----------------------------------------------------
stack-port2/1
  XGigabitEthernet2/0/1    10G              12G
stack-port2/2
  XGigabitEthernet2/0/4    10G              12G
stack-port3/1
  XGigabitEthernet3/0/1    10G              12G
  XGigabitEthernet3/0/3    10G              12G
stack-port3/2
  XGigabitEthernet3/0/28   10G              12G
  XGigabitEthernet3/0/30   10G              12G
```

Table 3-58 Description of the **display stack port speed** command output

Item	Description
Stack Port	Stack port.
Current Speed	Stack port's current working speed.
Next Speed	Stack port's working speed taking effect after a restart. To configure the parameter, run the **stack port speed** command.

3.3.8 display stack-port load-balance

Function

The **display stack-port load-balance** command displays the load balancing modes of stack ports.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display stack-port { **global load-balance** | **load-balance** [*slot-id*/*port-id*] }

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
port-id	Specifies the ID of a stack port.	The value is 1 or 2.
global	Displays the global load balancing mode. **NOTE** The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S only support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display stack-port load-balance** command to check the load balancing modes of stack ports and then locate data transmission failures between stack links.

Example

Display the load balancing modes of stack ports.

```
<HUAWEI> display stack-port load-balance
Global load balance mode: ENHANCED
Stack-port0/1 load balance mode: ENHANCED
Stack-port0/2 load balance mode: ENHANCED
Stack-port1/1 load balance mode: DST-MAC
Stack-port1/2 load balance mode: SRC-MAC
Stack-port2/1 load balance mode: DST-IP
Stack-port2/2 load balance mode: SRC-DST-IP
```

Table 3-59 Description of the **display stack-port load-balance** command output

Item	Description
Global load balance mode	Global load balancing mode: - DST-IP: performs load balancing based on destination IP addresses. - DST-MAC: performs load balancing based on destination MAC addresses. - SRC-IP: performs load balancing based on source IP addresses. - SRC-MAC: performs load balancing based on source MAC addresses. - SRC-DST-IP: performs load balancing based on the Exclusive-OR result of source and destination IP addresses. - SRC-DST-MAC: performs load balancing based on the Exclusive-OR result of source and destination MAC addresses. - ENHANCED: enhanced load balancing mode, that is, load balancing based on the Exclusive-OR result of the source and destination MAC addresses. To set the global load balancing mode, run the **stack-port load-balance mode** command in the system view.

Item	Description
Stack-port0/1 load balance mode Stack-port0/2 load balance mode Stack-port1/1 load balance mode Stack-port1/2 load balance mode Stack-port2/1 load balance mode Stack-port2/2 load balance mode	Load balancing mode of a stack port: ● DST-IP: performs load balancing based on destination IP addresses. ● DST-MAC: performs load balancing based on destination MAC addresses. ● SRC-IP: performs load balancing based on source IP addresses. ● SRC-MAC: performs load balancing based on source MAC addresses. ● SRC-DST-IP: performs load balancing based on the Exclusive-OR result of source and destination IP addresses. ● SRC-DST-MAC: performs load balancing based on the Exclusive-OR result of source and destination MAC addresses. ● ENHANCED: enhanced load balancing mode, that is, load balancing based on the Exclusive-OR result of the source and destination MAC addresses. To set the load balancing mode for a stack port, run the **stack-port load-balance mode** command in the stack port view.

3.3.9 display stack configuration

Function

The **display stack configuration** command displays stack configuration commands configured in a stack.

Format

display stack configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the stack commands configured on a stack member switch. *slot-id* specifies the stack ID of the member switch.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Stack configuration will only be written to the flash memory instead of the configuration file. As a result, Stack configuration cannot be obtained through the configuration file. To view stack configuration, run the **display stack configuration** command.

Precautions

- This command is valid only when the stack function is enabled and has taken effect. By default, the stack function is enabled.
- This command displays only the stack commands that have been executed. The displayed command configuration is not necessarily the running stack configuration, because most stack configuration commands take effect after a system restart.

Example

Display the stack configuration commands that have been executed in a stack.

```
<HUAWEI> display stack configuration
*    : Invalid-configuration
#    : Unsaved configuration
---------------Configuration on slot 2
Begin---------------

stack enable
stack slot 0 renumber 2
stack slot 2 priority 150
stack reserved-vlan 4093
stack timer mac-address switch-delay 10

interface stack-port 2/1
 *port interface XGigabitEthernet2/0/1 enable

interface stack-port 2/2
 #port interface XGigabitEthernet2/0/4 enable
---------------Configuration on slot 2 End-----------------
```

- If a stack member port is marked with an asterisk (*), the current configuration does not take effect because of the following reasons:
  - The current configuration is the preconfiguration that has not taken effect.
  - Insert different types of subcards.
  - The stack member port is located on a subcard that is not available.
  - When ports on the device panel and ports on subcards cannot be used together, one of the two port types is configured as stack member ports but not configured as the ports that take effect on the device, and the device is restarted.
- If a stack member port is marked with a number sign (#), the current configuration is automatically generated for dedicated cable stacking but not

saved to the flash memory using the **save stack configuration** or **save** command.

- If a stack member port is marked with *#, the switch is using stack card stacking. In this case, the **display stack configuration** command displays the stack configuration that is automatically generated after dedicated stack cables are installed. To change stack card stacking to dedicated stack cable stacking, run the **save stack configuration** or **save** command to save the stack configuration to the flash memory and then restart the switch.

3.3.10 display stack channel

Function

The **display stack channel all** command displays stack link connections and status.

Format

display stack channel [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Displays stack link connections and status of all the member switches.	-
slot *slot-id*	Displays stack link connections and status of the member switch with a specified stack ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check stack link connections and status, run the **display stack channel all** command. If you do not specify **all** or **slot** *slot-id* in the command, this command displays the stack link connections and status of the master switch.

Example

Display stack link connections and status of all the member switches.

```
<HUAWEI> display stack channel all
!     : Port have received packets with CRC error.
L-Port: Logic stack port
```

```
P-Port: Physical port
Slot  L-Port  P-Port    Speed  State  ||  P-Port    Speed  State  L-Port  Slot
--------------------------------------------------------------------------------
1     1/2     GE1/0/28  2.5G   UP         GE2/0/27  2.5G   UP     2/1     2
2     2/1     GE2/0/27  2.5G   UP         GE1/0/28  2.5G   UP     1/2     1
--------------------------------------------------------------------------------
```

The following output information shows that the physical member port GE1/0/28 works at 2.5 Gbit/s and is in Up state; it is bound to stack port 1/2 and belongs to the member switch with stack ID 1; GE1/0/28 is connected to the physical member port GE2/0/27; GE2/0/27 works at 2.5 Gbit/s and is in Up state; It is bound to stack port 2/1 and belongs to member switch with stack ID 2.

```
1     1/2     GE1/0/28  2.5G   UP         GE2/0/27  2.5G   UP     2/1     2
```

Table 3-60 Description of the **display stack channel** command output

Item	Description
!	A physical member port has received CRC error packets. **NOTE** If a physical member port receives CRC error packets, its **Speed** field displays the speed value and an exclamation mark (!), for example, 2.5G!.
Slot	Stack ID of a device.
L-Port	Number of a stack port.
P-Port	Number of a physical member port.
Speed	Speed of a physical member port.
Status	Status of a physical member port.

3.3.11 display upgrade area

Function

The **display upgrade area** command displays area status and whether a smooth upgrade can start.

Format

display upgrade area

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the stack topology changes after the areas for smooth upgrade are divided, members in the active and backup areas may change, resulting in a smooth upgrade failure. To check whether a smooth upgrade can start in these areas, run the **display upgrade area** command.

If the areas fail the check, re-define the active and backup areas according to the current stack topology.

The active area contains the master switch.

Example

Display the current area status and whether a smooth upgrade can start.

```
<HUAWEI> display upgrade area
Slot      Area         Upgrade-Check
-----------------------------------
   0      backup       passed
   3      active       passed
   4      active       passed
   8      active       passed
```

Table 3-61 Description of the **display upgrade area** command output

Item	Description
Slot	Stack ID of a device.
Area	Area to which a device belongs. ● active ● backup ● unknown: The device does not belong to any area.
Upgrade-Check	Upgrade check result. ● passed ● failed

3.3.12 display upgrade state

Function

The **display upgrade state** command displays the smooth upgrade status of member switches in a stack.

Format

display upgrade state [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of member switches in the active and backup areas before or after a smooth upgrade, run the **display upgrade state** command.

If you specify the **slot** *slot-id* parameter in the command, you can check whether the member switch with this slot ID has been upgraded successfully.

If the master switch of a stack restarts or experiences a master/standby switchover after a smooth upgrade, area information will be deleted from the master switch, and the **Area** field of the master switch will be displayed as **unknown**.

Example

Display the smooth upgrade status of member switches in a stack.

```
<HUAWEI> display upgrade state
Slot      Area          Status
-----------------------------
   0      backup        backup rebooting
   3      backup        backup rebooting
   4      active       backup rebooting
   8      active       backup rebooting
```

Display the smooth upgrade status of the member switch with stack ID 4.

```
<HUAWEI> display upgrade state slot 4
--------------------------------------
  Slot         : 4
  Area         : backup
  Status       : successful
  ErrorCode   : 0
  Description :
--------------------------------------
```

Table 3-62 Description of the **display upgrade state** command output

Item	Description
Slot	Stack ID of a device.

Item	Description
Area	Area to which a device belongs. ● active ● backup ● unknown: The device does not belong to any area.
Status	Upgrade progress of a device. ● idle: The upgrade has not been performed yet. ● backup rebooting: The backup area is upgrading. ● active rebooting: The active area is upgrading. ● failed: The upgrade failed. ● successful: The upgrade succeeded.
ErrorCode	Error code of an upgrade failure. For details, see **3.3.38 upgrade start**. The value 0 indicates that the upgrade succeeded.
Description	Description about the failure if an upgrade fails.

3.3.13 interface stack-port

Function

The **interface stack-port** command displays the stack port view.

NOTE

Only devices supporting service port stacking support this command.

Format

interface stack-port *member-id*/*port-id*

Parameters

Parameter	Description	Value
member-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
port-id	Specifies a stack port number.	The value is 1 or 2.

Views

System view

Default Level

3: Management level

Usage Guidelines

Each member switch has two stack ports, which are named Stack-Port*n*/1 and Stack-Port*n*/2. *n* specifies the stack ID of a member switch. After you run the **interface stack-port** command to enter the view of a stack port, you can configure attributes for the stack port.

Example

Display the view of Stack-Port1/1.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 1/1
[HUAWEI-stack-port1/1]
```

3.3.14 mad backup ip address

Function

The **mad backup ip address** command configures a backup IP address for the management interface in a stack.

The **undo backup ip address** command deletes the backup IP address for the management interface in a stack.

By default, no backup IP address is configured for the management interface in a stack.

Format

mad backup ip address *ip-address* { *mask* | *mask-length* }

undo mad backup ip address

Parameters

Parameter	Description	Value
ip-address	Specifies the backup IP address for the management interface.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the backup IP address for the management interface.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the backup IP address for the management interface.	The value is an integer that ranges from 0 to 32.

Views

MEth0/0/1 management interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When MAD detects a stack split fault, all interfaces (including the management interface) of the member device that fails in the election are shut down to prevent network flapping caused by identical MAC and IP addresses, reducing the impact on the network. After the management interface of the member device is shut down, you cannot remotely log in to and manage the device, and can only log in to the device through the console interface, which is inconvenient for device maintenance.

To prevent this problem, you can configure a backup IP address for the management interface on the device. If the stack splits, the IP address of the management interface on the member device that fails in the election is set to the configured backup IP address. This prevents packet forwarding from being affected due to conflicting management IP addresses upon the stack split. In addition, you can remotely log in to and manage the device, which facilitates device maintenance.

If the stack splits after a backup IP address is configured for the management interface on the device, the management interface on the member device that fails in the election is not shut down, and only the backup IP address is configured as the IP address of the management interface. Other non-reserved service interfaces are still shut down.

Precautions

- This command does not take effect if the device does not have a management interface.
- The backup IP address cannot be on the same network segment as the IP addresses used by other interfaces on the device. Otherwise, the function does not take effect due to address conflicts.
- This command can only be used to configure the IP address of the management interface, regardless of the Up/Down status of the management interface. For example, if the management interface is shut down using a command or the management interface is not connected using a cable, the management interface is Down.

Example

Configure a backup IP address for the management interface in a stack.

```
<HUAWEI> system-view
[HUAWEI] interface meth 0/0/1
[HUAWEI-MEth0/0/1] mad backup ip address 10.1.1.1 24
```

3.3.15 mad detect mode direct

Function

The **mad detect mode direct** command configures multi-active detection (MAD) in direct mode on an interface.

The **undo mad detect** command cancels the configuration.

By default, MAD in direct mode is disabled on an interface.

Format

mad detect mode direct

undo mad detect [**mode direct**]

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, port group view, MultiGE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that only one switch becomes the master switch after a stack splits, thereby enhancing stack stability, run the **mad detect mode direct** command to configure MAD in direct mode on an interface.

Configuration Impact

Configuring MAD in direct mode on an interface blocks the interface. Disabling MAD in direct mode on an interface restores the forwarding function of the interface. If a loop exists on the network, a broadcast storm occurs.

Precautions

The **undo mad detect** command is not supported in the port group view. You can only run the **undo mad detect mode direct** command in the port group view to disable MAD in direct mode.

Example

Configure MAD in direct mode on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] mad detect mode direct
Warning: This command will block the port, and no other configuration running on this port is
recommended. Continue? [Y/N]:y
```

3.3.16 mad detect mode relay

Function

The **mad detect mode relay** command configures multi-active detection (MAD) in relay mode on an interface.

The **undo mad detect** command cancels the configuration.

By default, MAD in relay mode is disabled on an interface.

Format

mad detect mode relay

undo mad detect [**mode relay**]

Parameters

None

Views

Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that only one switch becomes the master switch after a stack splits, thereby enhancing stability of the stack, run the **mad detect mode relay** command to configure MAD in relay mode on an Eth-trunk.

Precautions

The **undo mad detect** command is not supported in the port group view. You can only run the **undo mad detect mode relay** command in the port group view to disable MAD in relay mode.

Example

Configure MAD in relay mode on Eth-Trunk 10.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] mad detect mode relay
```

3.3.17 mad domain

Function

The **mad domain** command sets a MAD domain ID for a stack.

The **undo mad domain** command restores the default MAD domain ID for a stack.

By default, the MAD domain ID of a stack is 0.

Format

mad domain *domain-id*

undo mad domain

Parameters

Parameter	Description	Value
domain-id	Specifies the MAD domain ID for a stack.	The value is an integer that ranges from 0 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In most MAD scenarios, configuring a MAD domain ID for a stack is unnecessary. When two stack systems function as a proxy of each other to implement MAD, configure different MAD domain IDs for the stack systems.

Example

Set the MAD domain ID for a stack to 1.

```
<HUAWEI> system-view
[HUAWEI] mad domain 1
```

3.3.18 mad exclude

Function

The **mad exclude** command excludes specified interfaces of a stack from shutdown.

The **undo mad exclude** command cancels excluding specified interfaces of a stack from shutdown.

By default, only physical member ports are excluded from shutdown.

Format

mad exclude interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo mad exclude interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] }	Specifies the type and number of an interface: ● *interface-type* specifies the type of the interface. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the second interface.	The value of *interface-number2* must be larger than that of *interface-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If MAD detects a stack split, all service ports of the member switch that fails master switch election must be shut down to prevent network flapping caused by MAC or IP address flapping. If some interfaces only transparently transmit packets, they do not affect network operation in a dual-active condition. You can run the **mad exclude** command to exclude these interfaces from shutdown before a stack split occurs.

Precautions

- After an interface is shut down because of MAD, it cannot be enabled if the **mad exclude** command is executed to exclude it from shutdown.
- When the **to** parameter is specified to exclude multiple ports from shutdown, these ports must reside on the same card and the port number following this parameter must be larger than the port number followed by this parameter.

Example

Exclude GigabitEthernet0/0/2 and GigabitEthernet0/0/3 from shutdown.

```
<HUAWEI> system-view
[HUAWEI] mad exclude interface gigabitethernet 0/0/2 to gigabitethernet 0/0/3
```

3.3.19 mad relay

Function

The **mad relay** command enables the relay function on an interface of a proxy device.

The **undo mad relay** command disables the relay function on an interface of a proxy device.

By default, the relay function is disabled on an interface.

Format

mad relay

undo mad relay

Parameters

None

Views

Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

For MAD working in relay mode, run the **mad relay** command to configure the relay function on an Eth-Trunk interface of a proxy device. Member interfaces of the Eth-Trunk interface exchange MAD packets between member switches.

Example

Enable the relay function on Eth-Trunk 10 of a proxy device.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] mad relay
```

3.3.20 mad restore

Function

The **mad restore** command restores all the blocked interfaces of a standby switch that enters the Recovery state after its stack splits.

Format

mad restore

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When MAD detects a multi-active event, the member switch elected as the master switch remains in the Detect state. The elected standby switch enters the Recovery state, shuts down all its service ports except those excluded from shutdown, and stops forwarding service packets.

If the switch in the Detect state fails or is removed before the split stack is restored, run the **mad restore** command on the switch in the Recovery state to restore the interfaces in shutdown state. The switch in the Recovery state then goes to the Detect state. You can then restore the original switch in the Detect state and rectify the faulty stack links. After the faults are rectified, the two switches form a stack again.

Example

Restore all the blocked interfaces of the standby switch that enters the Recovery state after its stack splits.

```
<HUAWEI> system-view
[HUAWEI] mad restore
```

3.3.21 port interface enable

Function

The **port interface enable** command configures a service interface as a physical member port and adds it to a stack port.

The **undo port interface enable** command restores a physical member port to being a service interface.

By default, service interfaces are not used as physical member ports of a stack port.

NOTE

Only the switches supporting service port stacking support this command.

Format

port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **enable**

undo port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **enable**

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies the type and number of an interface: ● *interface-type* specifies the type of the interface. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the second interface.	The value of *interface-number2* must be larger than that of *interface-number1*.

Views

Stack interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In service interface connection mode, run the **port interface enable** command to configure a service interface as a physical member port to implement the stack function.

Configuration Impact

A stack physical member port supports only stack-related functions, and other functions cannot be configured on the interface. All the commands irrelevant to the stack function are masked in the interface view, and only basic configuration commands, such as **description**, are retained.

After configuring a service port of a switch as a physical stack member port, you are advised to save the configuration if this service port has been referenced by other commands. Otherwise, the commands that reference this service port may be retained after the switch restarts.

On the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S the electrical or optical port stack configuration on the front panel is mutually exclusive with the SVF client mode configuration. If electrical or optical ports on the front panel have been configured as stack physical member ports, SVF management VLAN cannot be configured. If an SVF management VLAN has been configured, electrical or optical ports on the front panel cannot be configured as stack physical member ports.

On the S6720-EI, S6735-S, and S6720S-EI, every four of XGE interfaces from the left are added to one group. For example, XGE interfaces numbered 1 to 4 can be added to one group, but XGE interfaces numbered 2 to 5 cannot. That is, the number of the last XGE interface in each group must be the multiple of 4. If you configure any interface in each group as a physical member port, configurations on the other three interfaces in the group will be lost and the three interfaces cannot be used as service ports.

Precautions

- The stack member ports of a logical stack port must be the same type.
- After a UCL group is created on the S5720I-SI, S5720-LI, S5720S-LI, or S5720-SI, using the **ucl-group** command, the **port interface enable** command cannot be used to configure a service interface as a stack member port.
- To restore a physical member port as a service interface, run the **shutdown interface** command in the stack port view and then run the **undo port interface enable** command.
- On the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, after a service interface is configured as a stack member port, the following priority mapping rules apply to packets on this interface:
  - Packets sent to the CPU are mapped to queue 7.
  - Packets with priority 0 or 1 are mapped to queue 0.
  - Packets with priorities 2 to 7 are mapped to queues 1 to 6, respectively.
- If the switch functions as an AS in an SVF system and its downlink service ports have been configured as member ports of an uplink fabric port, all the downlink ports of the AS cannot be configured as stack member ports.

Example

Configure XGigabitEthernet0/0/28 as a physical member port and add it to stack port 0/1.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port interface xgigabitethernet 0/0/28 enable
Warning: Enabling stack function may cause configuration loss on the interface. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait....
```

On the S6720-EI, configure XGigabitEthernet0/0/15 as a physical member port and add it to stack port 0/1.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] port interface xgigabitethernet 0/0/15 enable
Warning: Enabling stack function may cause configuration loss on the interface XGigabitEthernet0/0/13 to
XGigabitEthernet0/0/16. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait....
Info: Ports XGigabitEthernet0/0/13 to XGigabitEthernet0/0/16 in a port group have been configured as
physical stack ports.
```

3.3.22 reset stack configuration

Function

The **reset stack configuration** command clears all stack configuration. That is, this command restores the default stack configuration.

Format

reset stack configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The cleared stack configuration includes: switch slot ID, stack priority, stack reserved VLAN, stack MAC address switching delay, stack port configuration, and stack port rate configuration. For example, when switches are stacked using dedicated stack cables, to ensure that slot IDs are automatically generated for the switches based on the sequence in which dedicated stack cables are connected, run the **reset stack configuration** command to clear all stack configuration.

Precautions

Running this command will cause the stack to split and member switches to restart.

Example

Clear all stack configuration.

```
<HUAWEI> system-view
[HUAWEI] reset stack configuration
Warning: This operation will clear all stack configurations and may lead to the loss of the slot ID
configuration and cause the device to reset immediately. Are you sure you want to continue? [Y/N]:y
```

3.3.23 reset stack port statistics

Function

The **reset stack port statistics** command clears stack port statistics.

Format

reset stack port statistics [*slot-id*/*port-id*]

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
port-id	Specifies the number of a stack port.	The value is 1 or 2.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting interface traffic statistics in a certain period of time, run the **reset stack port statistics** command to clear existing traffic statistics. If you do not specify the port number, statistics on all stack ports are cleared. If you specify the port number, only statistics on the specified port are cleared.

Precautions

The cleared statistics cannot be restored. Therefore, exercise caution when you run the **reset stack port statistics** command.

This command can be used only after the stack function is enabled (default status).

Example

Clear the statistics from all stack ports.

```
<HUAWEI> reset stack port statistics
```

3.3.24 save stack configuration

Function

The **save stack configuration** command saves the stack configuration automatically generated for dedicated cable stacking to the flash memory.

By default, the stack configuration automatically generated for dedicated cable stacking is not saved to the flash memory.

Format

save stack configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After dedicated stack cables are connected to ports, stack configuration is automatically generated but not saved to the flash memory. If these cables are removed or other cables are connected, the stack configuration is automatically deleted. To ensure that the stack configuration still takes effect when these cables are removed or other cables are connected, run the **save stack configuration** command.

Precautions

- Removing dedicated stack cables from ports after this command is executed will cause these ports unable to automatically become service ports.
- No stack configurations can be manually modified before the stack configuration automatically generated for dedicated cable stacking is saved to the flash memory.

Example

Save the stack configuration that is automatically generated for dedicated cable stacking to the flash memory.

```
<HUAWEI> system-view
[HUAWEI] save stack configuration
Warning: This operation will save all stack configurations to flash. Are you sure you want to continue? [Y/
N]:y
```

3.3.25 set l2-traffic fast-recover

Function

The **set l2-traffic fast-recover enable** command enables fast recovery of Layer 2 traffic.

The **undo set l2-traffic fast-recover enable** command disables fast recovery of Layer 2 traffic.

By default, fast recovery of Layer 2 traffic is disabled.

Format

set l2-traffic fast-recover enable

undo set l2-traffic fast-recover enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After fixed switches set up a stack and the standby switch starts, the standby switch restores configurations and then implements batch backup from the master switch.

By default, interfaces on the standby switch become Up when batch backup is complete. In this case, Layer 2 and Layer 3 traffic can be normally forwarded but there is a delay in Layer 2 traffic recovery. To enable fast recovery of Layer 2 traffic, run the **set l2-traffic fast-recover enable** command. Interfaces on the standby switch then immediately go Up when configuration restoration is complete. This way, however, cannot ensure Layer 3 traffic forwarding through the Up interfaces.

Example

Enable fast recovery of Layer 2 traffic.

```
<HUAWEI> system-view
[HUAWEI] set l2-traffic fast-recover enable
```

3.3.26 shutdown interface

Function

The **shutdown interface** command shuts down a physical member interface.

The **undo shutdown interface** command enables a physical member interface.

By default, a physical member interface is enabled after being configured.

NOTE

Only devices supporting service port stacking support this command.

Format

shutdown interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo shutdown interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies the type and number of an interface: ● *interface-type* specifies the type of the interface. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the second interface.	The value of *interface-number2* must be larger than that of *interface-number1*.

Views

Stack interface view

Default Level

3: Management level

Usage Guidelines

To restore a physical member interface to being a service interface, run the **shutdown interface** command in the stack interface view and then run the **undo port interface enable** command.

If there is only one available link on a stack interface, running the **shutdown interface** command will change the stack status or split the stack. After you run the **undo shutdown interface** command on the stack interface, the stack will be set up again when a link on the stack interface becomes available.

Example

Shut down physical member interface XGigabitEthernet0/0/3.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] shutdown interface XGigabitEthernet0/0/3
Warning: Shutting down the last active stack-port will cause a topology change. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait...succeeded.
```

3.3.27 stack authentication

Function

The **stack authentication** command configures the authentication mode and authentication information used when a switch needs to join a stack.

The **undo stack authentication** command deletes the authentication mode and authentication information used when a switch needs to join a stack.

By default, a switch does not need to be authenticated when joining a stack.

Format

stack authentication slot *slot-id* { **mac-address** *mac-address* | **esn** *esn-value* | **shared-key cipher** *shared-key* }

undo stack authentication slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a switch.	The value is an integer that ranges from 0 to 8.
mac-address *mac-address*	Configures MAC-based authentication.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits.
esn *esn-value*	Configures ESN-based authentication.	The value is a string of 10 to 32 characters.
shared-key cipher *shared-key*	Configures shared key-based authentication.	The value is a string of case-sensitive characters without spaces. A plain text key contains 1 to 64 characters, and a cipher text key contains 48 to 108 characters. **NOTE** It is recommended that a shared key contains at least seven characters, including at least two types of lowercase letters, uppercase letters, digits, and special characters. The master switch and the specified slot must configure the same shared key. If a shared key is used for authentication, the master switch and the member switch specified in this command must be configured with the same shared key.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A switch can join a stack without being authenticated. In this situation, an attacker can add any switch to a stack to obtain the configuration file of the stack master switch, resulting in information leak. To solve this problem, configure authentication when a switch needs to join a stack. This configuration ensures that this switch joins the stack only when it is authenticated successfully.

A switch will be authenticated only when its stack ID is the same as that specified in the **stack authentication** command. Otherwise, this switch can join a stack without being authenticated. Therefore, before adding a switch to a stack, you are advised to change the slot ID of the switch to an unused stack ID in the stack and then configure an authentication mode for this stack ID.

Precautions

- This command can be executed only after the stacking function is enabled.
- Only one authentication mode can be configured for a stack ID, and the latest configuration takes effect.
- If a switch to join a stack fails the authentication, this switch will restart repeatedly.

Example

Configure MAC-based authentication to be used when a switch with the stack ID 4 needs to join a stack.

```
<HUAWEI> system-view
[HUAWEI] stack authentication slot 4 mac-address 3-3-3
```

3.3.28 stack led enable

Function

The **stack led enable** command enables a service port indicator to indicate the stack ID of a stack switch.

The **stack led disable** command disables a service port indicator from indicating the stack ID of a stack switch.

By default, a service port indicator does not indicate the stack ID of a stack switch.

NOTE

S6735-S does not support this command.

Format

stack led enable [**duration** *duration-value*]

stack led disable

Parameters

Parameter	Description	Value
duration *duration-value*	Specifies how long a service port indicator indicates the stack ID of a stack switch.	The value is an integer that ranges from 30 to 600, in seconds. By default, a stack ID indicator stays on for 45 seconds.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Stack IDs can be allocated by the master switch when a stack is set up, or you can configure them yourself. If stack IDs are allocated by the master switch, you cannot identify which ID a device maps to. To enable a service port indicator to indicate the stack ID of a stack switch, run the **stack led enable** command.

A service port indicator indicates the stack ID of a stack switch as follows:

- For a switch whose stack ID ranges from 1 to 8: Only the indicator whose serial number matches the stack ID is on. For example, if the stack ID is 1, the first indicator is on. If the stack ID is 2, the second indicator is on.
- For a switch whose stack ID is 0: If the stack contains *N* stack switches, the first *N* indicators are on. For example, if the stack contains 9 stack switches, the first 9 indicators are on, indicating the stack ID is 0.
- After service port indicators are configured to indicate the stack IDs, the service port indicator of the master switch blinks, and that of the slave switch is steady on.

The configuration of this command becomes invalid when port indicators show stack IDs of member switches for the specified time.

Example

Enable a service port indicator to indicate the stack ID of a stack device for a period of 30s.

```
<HUAWEI> stack led enable duration 30
```

3.3.29 stack-port load-balance mode

Function

The **stack-port load-balance mode** command sets a load balancing mode for the physical member ports of a stack port.

The **undo stack-port load-balance mode** command restores the default load balancing mode.

By default, the physical member ports of a stack port perform load balancing in enhanced mode, that is, load balancing based on the Exclusive-OR result of the source and destination MAC addresses.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

stack-port load-balance mode { **dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** }

undo stack-port load-balance mode

Parameters

Parameter	Description	Value
dst-ip	Performs load balancing based on destination IP addresses.	-
dst-mac	Performs load balancing based on destination MAC addresses.	-
src-dst-ip	Performs load balancing based on the Exclusive-OR result of the source and destination IP addresses.	-
src-dst-mac	Performs load balancing based on the Exclusive-OR result of the source and destination MAC addresses.	-
src-ip	Performs load balancing based on source IP addresses.	-

Parameter	Description	Value
src-mac	Performs load balancing based on source MAC addresses.	-

Views

System view

Logical stack port view (The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support the **stack-port load-balance mode** command in this view.)

Default Level

3: Management level

Usage Guidelines

Use Scenario

To transmit traffic from a stack port to a destination over different links, run the **stack-port load-balance mode** command to configure an appropriate load balancing mode for the physical member ports of the stack port. Outgoing traffic is then properly balanced among the physical links, preventing congestion on these links. If you run this command multiple times to set different load balancing modes, the last configuration takes effect. The load balancing mode configured in the system view takes effect globally, and the load balancing mode configured in a stack port view takes effect only on the specified stack port. You can run the **display stack-port** command to view the load balancing mode on a stack port.

Precautions

- If a non-default load balancing mode is configured on a stack port, the configured load balancing mode takes effect. If a stack port uses the default load balancing mode and the global load balancing mode is not the default one, the global load balancing mode takes effect.
- If the source MAC address-based load balancing mode is used, Layer 3 packets forwarded to a downstream device may fail to be balanced among the stack links because the source MAC address of the packets is the fixed system MAC address. If the traffic rate exceeds the bandwidth of a single stack link, some packets may be dropped.

Example

Set the global load balancing mode to **src-ip**.

```
<HUAWEI> system-view
[HUAWEI] stack-port load-balance mode src-ip
```

Set the load balancing mode on stack port 0/1 to **dst-ip**.

```
<HUAWEI> system-view
[HUAWEI] interface stack-port 0/1
[HUAWEI-stack-port0/1] stack-port load-balance mode dst-ip
```

3.3.30 stack port speed

Function

The **stack port speed** command sets the working speed for stack member ports.

The **undo stack port speed** command restores the working speed of stack member ports to the default value.

For the default working speeds of stack member ports on different switch models, see "Stack Support and Version Requirements" in Stack Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

NOTE

Only the S5720-X-LI, S5720I-SI, S5732-H, and S5720S-X-LI support this command.

The S5720-P-LI does not support this command before the license is loaded and supports this command after the license is loaded and it restarts.

Format

stack port speed { **12G** | **2.5G** | **40GE** }

undo stack port speed

Parameters

Parameter	Description	Value
12G	Sets the working speed of stack member ports to 12 Gbit/s. This speed can be set only on the S5720-P-LI, S5720-X-LI, S5720I-SI, and S5720S-X-LI,.	-
2.5G	Sets the working speed of stack member ports to 2.5 Gbit/s. This speed can be set only on the S5720-P-LI, S5720-X-LI, and S5720S-X-LI.	-

Parameter	Description	Value
40GE	Sets the working speed of stack member ports to 40 Gbit/s. This speed can be set only on the S5732-H.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On the S5720-P-LI, S5720-X-LI, S5720I-SI, and S5720S-X-LI,, if optical ports are used as stack member ports and are connected using 1 m or 3 m SFP+ passive copper cables, you can use this command to increase their working speed from 10 Gbit/s to 12 Gbit/s, expanding the stack bandwidth. After their working speed is increased to 12 Gbit/s, switches using these ports cannot set up a stack with switches using ports with the working speed 10 Gbit/s.

If S5720-P-LI, S5720-X-LI, and S5720S-X-LI switches use XGE optical ports to stack with other switches that have GE optical ports, use this command to reduce the working speed of the XGE optical ports from 10 Gbit/s to 2.5 Gbit/s, so that the XGE optical ports can work with the remote GE optical ports.

On the S5732-H, if 100GE and 40GE ports need to be connected using 2 m QSFP28 dedicated stack cables for stack setup, run this command to reduce the working speed of the 100GE ports that function as stack member ports to 40 Gbit/s.

You can run the **display stack port speed** command to check the working speed of stack member ports.

Precautions

After changing the working speed of stack member ports, you need to restart the switch for the new speed to take effect.

Example

Set the working speed of stack member ports to 12 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] stack port speed 12G
```

3.3.31 stack port { crc | link-flap } trigger

Function

The **stack port { crc | link-flap } trigger** command sets the stack port error-down parameters.

The **undo stack port { crc | link-flap } trigger** command restores the default settings of the stack port error-down parameters.

By default, the stack port receives 20 CRC error packets (include Symbols error packets) per minute or alternates between Up and Down states 10 times per minute, the error-down check interval is 3 minutes, and the alarm clearance interval is 0 (not cleared automatically).

Format

stack port { **crc** | **link-flap** } **trigger** { **threshold** *threshold* | **interval** *interval* } *

undo stack port { **crc** | **link-flap** } **trigger** { **threshold** | **interval** }

stack port { **crc** | **link-flap** } **trigger error-down auto-recovery-interval** *auto-recovery-interval*

undo stack port { **crc** | **link-flap** } **trigger error-down auto-recovery-interval**

Parameters

Parameter	Description	Value
crc	Sets the parameters for stack port error-down alarms triggered by CRC error packets (include Symbols error packets).	-
link-flap	Sets the parameters for stack port error-down alarms triggered by port Up/Down transitions.	-
threshold *threshold*	Specifies the error-down alarm threshold.	The value is an integer. It ranges from 1 to 10000 for error-down alarms triggered by CRC error packets (include Symbols error packets) and ranges from 3 to 30 for error-down alarms triggered by port Up/Down transitions. The unit is times per minute.

Parameter	Description	Value
interval *interval*	Specifies the error-down check interval.	The value is an integer that ranges from 3 to 30, in minutes.
auto-recovery-interval *auto-recovery-interval*	Specifies the error-down alarm clearance interval.	The value is an integer that ranges from 3 to 30, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

After the stack port error-down function is enabled, you can run the **stack port { crc | link-flap } trigger** command to adjust the related parameters.

Example

Set the clearance interval of stack port error-down alarms triggered by CRC error packets (include Symbols error packets) to 3 minutes. That is, if the rate of received CRC error packets (include Symbols error packets) stays below the threshold for 3 minutes, the stack port changes to Up state and the error-down alarm is cleared.

```
<HUAWEI> system-view
[HUAWEI] stack port crc trigger error-down auto-recovery-interval 3
```

3.3.32 stack port { crc | link-flap } trigger error-down

Function

The **stack port { crc | link-flap } trigger error-down** command enables the stack port error-down function.

The **undo stack port { crc | link-flap } trigger error-down** command disables the stack port error-down function.

By default, the stack port error-down function is enabled.

Format

stack port { **crc** | **link-flap** } **trigger error-down**

undo stack port { **crc** | **link-flap** } **trigger error-down**

Parameters

Parameter	Description	Value
crc	Enables stack port error-down triggered by CRC error packets (include Symbols error packets).	-
link-flap	Enables stack port error-down triggered by port Up/Down transitions.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a stack system, if a stack port continuously receives CRC error packets (include Symbols error packets) or flaps between Up and Down states, the corresponding stack link cannot forward traffic normally, thereby affecting network services. This command enables the stack port error-down function. This function can shut down a stack port and switch traffic to other stack links if the rate of received CRC error packets (include Symbols error packets) or the number of Up/Down transitions on the stack port reaches the specified threshold, reducing the impact on services. Additionally, the system generates stack port error-down alarms to help in fault location.

Follow-up Procedure

Run the **stack port { crc | link-flap } trigger** command to set stack port error-down parameters.

Precautions

- When one end is a stack port and the other end is a service port, the system does not set the stack port to error-down state or generate an error-down alarm even if this stack port continuously receives CRC error packets (include Symbols error packets).
- The stack port error-down alarm OID is 1.3.6.1.4.1.2011.5.25.183.1.22.59.
- The stack port error-down alarm clearance OID is 1.3.6.1.4.1.2011.5.25.183.1.22.60.

Example

Enable stack port error-down triggered by CRC error packets (include Symbols error packets).

```
<HUAWEI> system-view
[HUAWEI] stack port crc trigger error-down
```

3.3.33 stack reserved-vlan

Function

The **stack reserved-vlan** command configures a reserved VLAN for a stack.

By default, a stack uses VLAN 4093 as the reserved VLAN.

Format

stack reserved-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a reserved VLAN.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, a stack uses VLAN 4093 as the reserved VLAN. A reserved VLAN is used only to exchange stack protocol packets.

To deploy services in VLAN 4093, run the **stack reserved-vlan** command to change the reserved VLAN of the stack.

NOTICE

If the reserved VLAN is used for other services, the stack cannot be set up. You must specify an unused VLAN as the reserved VLAN for a stack.

Example

Configure VLAN 4000 as the reserved VLAN of a stack.

```
<HUAWEI> system-view
[HUAWEI] stack reserved-vlan 4000
Warning: Do not frequently modify the stack reserved VLAN because it will make the stack split. Continue?
[Y/N]:y
```

3.3.34 stack slot priority

Function

The **stack slot priority** command sets a stack priority for a member switch in a stack.

By default, the stack priority of a member switch is 100.

Format

stack slot *slot-id* **priority** *priority*

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.
priority	Specifies a stack priority.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To set a stack priority for a member switch in a stack, run the **stack slot priority** command. A larger priority indicates a higher priority, meaning that a switch is more likely to be selected as a master switch.

Example

Set the stack priority of the member switch with stack ID 4 to 150.

```
<HUAWEI> system-view
[HUAWEI] stack slot 4 priority 150
Warning: Do not frequently modify the priority because it will make the stack split. Continue? [Y/N]:y
```

3.3.35 stack slot renumber

Function

The **stack slot renumber** command changes the stack ID of a specified stack member switch.

Format

stack slot *slot-id* **renumber** *new-slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the current stack ID.	The value is an integer that ranges from 0 to 8.
new-slot-id	Specifies a new stack ID.	The value is an integer that ranges from 0 to 8.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To change the stack ID of a stack member switch, run the **stack slot renumber** command.

Precautions

- After changing the stack ID of a switch, if you do not restart the switch, the switch continues to use the original stack ID, and all physical resources are identified by the original stack ID.
- After changing the stack ID of a switch, if you restarts the switch, the new stack ID takes effect and all physical resources are identified by the new stack ID. In the configuration file, only the global stack configuration and stack priority of the switch continue to take effect. All other configurations related to the old stack ID (such as interface configuration) become invalid and must be reconfigured.

- After a UCL group is created on the S5720I-SI, S5720-LI, S5720S-LI, or S5720-SI, using the **ucl-group** command, the **stack slot renumber** command cannot be used to change the stack ID of a specified stack member switch.

Example

Change the stack ID of a stack member switch from 4 to 5.

```
<HUAWEI> system-view
[HUAWEI] stack slot 4 renumber 5
Warning: All the configurations related to the slot ID will be lost after the slot ID is
modified.
Do not frequently modify the slot ID because it will make the stack split. Continue? [Y/
N]:y
Info: Stack configuration has been changed, and the device needs to restart to make the configuration
effective.
```

3.3.36 stack timer mac-address switch-delay

Function

The **stack timer mac-address switch-delay** command sets a period after which a stack changes its system MAC address.

The **undo stack timer mac-address switch-delay** command configures a stack to change the system MAC address immediately after the owner of the original system MAC address leaves the stack.

By default, a stack changes the system MAC address after 10 minutes.

NOTICE

When a stack is configured to switch the system MAC address immediately, the system begins using the MAC address of the new master switch the moment the previous master switch fails or leaves the stack. This may cause protocols such as LACP and STP to flap, thereby affecting services.

Format

stack timer mac-address switch-delay *delay-time*

undo stack timer mac-address switch-delay

Parameters

Parameter	Description	Value
delay-time	Specifies a period after which a stack changes the system MAC address.	The value ranges from 0 to 60, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a member switch leaves a stack, if you specify the MAC address of the leaving switch as the stack MAC address and it does not rejoin the stack within the time specified by *delay-time*, the master switch changes the stack MAC address to its own MAC address.

The stack MAC address switchover delay time of any member switch in a stack is the same as that of the master switch.

If the value of the MAC address switchover timer is set to 0, no stack MAC address switchover will be performed.

This command can be used only after the stack function is enabled (default status).

Example

Set the MAC address switchover delay of the local switch to 4 minutes.

```
<HUAWEI> system-view
[HUAWEI] stack timer mac-address switch-delay 4
Warning: Do not frequently modify the MAC switching time because it will make the stack split. Continue?
[Y/N]:y
```

3.3.37 upgrade backup-area slot

Function

The **upgrade backup-area slot** command defines the active and backup areas in a stack in preparation for a smooth upgrade.

Format

upgrade backup-area slot *slot-id* **to** *slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the stack ID of a member switch.	The value is an integer that ranges from 0 to 8.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before upgrading a reliable stack with uplinks and downlinks working in redundancy mode, you can divide the stack into an active area and a backup area for redundancy. After an upgrade is started, member switches in the two areas are upgraded in sequence, shortening the service interruption duration and reducing the impact of the upgrade on the network.

Precautions

- Member switches in the active and backup areas form the entire stack. When dividing active and backup areas, note that:
  - The active and backup areas cannot have the same member switch, and both areas must have at least one member switch.
  - The backup area cannot contain the master switch of the stack.
  - Member switches in each area must be directly connected.
- After this command is run, the member switches with specified stack IDs join the backup area. The other member switches automatically join the active area.
- To ensure mutual backup, it is recommended that the two areas have similar quantities of member switches.

Example

Add member switches with stack IDs 0 to 3 to the backup area.

```
<HUAWEI> system-view
[HUAWEI] upgrade backup-area slot 0 to 3
```

3.3.38 upgrade start

Function

The **upgrade start** command starts a smooth upgrade.

Format

upgrade start

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before running this command, run the **upgrade backup-area slot** command to define the active and backup areas and ensure that all member switches in the stack are running the same system software and support smooth upgrades.

If an upgrade fails, error codes and displayed message help locate the cause. Table 3-63 lists the error codes and displayed messages in different upgrade failure scenarios.

Table 3-63 Error codes and displayed messages in different upgrade failure scenarios

Upgrade Failure Scenario	Error Code	Displayed Message
Record in the backup area: The upgrade in the backup area times out and rolls back.	1	Rollback due to timeout.
Record in the active area: The upgrade in the backup area times out and rolls back.	2	
Record in the backup area: The upgrade in the active area times out and rolls back.	3	
Record in the active area: The upgrade in the active area times out and rolls back.	4	
Record in the backup area: Rollback occurs due to a topology change in the backup area.	257	Rollback due to topology changes.
Record in the active area: Rollback occurs due to a topology change in the backup area.	258	

Upgrade Failure Scenario	Error Code	Displayed Message
Record in the backup area: Rollback occurs due to a topology change in the active area.	259	
Record in the active area: Rollback occurs due to a topology change in the active area.	260	
A member switch records that the master switch is not upgraded.	512	Master is not upgraded.
During a backup area upgrade, the master switch instructs switches in the backup area to roll back (after the active area instructs the backup area to upgrade and switches in the backup area restart).	769	Master notifies others of rollback.
During a backup area upgrade, the master switch instructs switches in the backup area to roll back (after the active area instructs the backup area to upgrade and before switches in the backup area restart).	770	
During an active area upgrade, the master switch instructs switches in the active area to roll back (after the backup area instructs the active area to upgrade and before switches in the active area restart).	771	

Upgrade Failure Scenario	Error Code	Displayed Message
During an active area upgrade, the master switch instructs switches in the active area to roll back (after the backup area instructs the active area to upgrade and switches in the active area restart).	772	
During a backup area upgrade, the master switch in the active area instructs switches in the backup area to roll back (after switches in the backup area restart).	1025	Master of the active area notifies others of rollback.
During a backup area upgrade, the master switch in the active area instructs switches in the backup area to roll back (before switches in the backup area restart).	1026	
During an active area upgrade, the master switch in the active area instructs switches in the active area to roll back (before switches in the active area restart).	1027	
During an active area upgrade, the master switch in the active area instructs switches in the active area to roll back (after switches in the active area restart).	1028	
During a backup area upgrade, the master switch in the backup area instructs switches in the backup area to roll back (after switches in the backup area restart).	1281	Master of the backup area notifies others of rollback.

Upgrade Failure Scenario	Error Code	Displayed Message
During a backup area upgrade, the master switch in the backup area instructs switches in the backup area to roll back (before switches in the backup area restart).	1282	
During an active area upgrade, the master switch in the backup area instructs switches in the active area to roll back (before switches in the active area restart).	1283	
During an active area upgrade, the master switch in the backup area instructs switches in the active area to roll back (after switches in the active area restart).	1284	
A load event occurs, and switches in the backup area roll back.	1537	Rollback due to a load event.
A load event occurs, and switches in the active area roll back.	1549	
The system software package is incorrect in the active area.	5	Active startup file is incorrect.
The system software package is incorrect in the backup area.	6	Backup startup file is incorrect.

Example

Start a smooth upgrade.

```
<HUAWEI> system-view
[HUAWEI] upgrade start
Warning: Upgrade will begin. Continue? [Y/N]:y
```

3.4 Intelligent Simplified Campus Network Configuration Commands

3.4.1 Command Support

All commands in this chapter are run on a central switch. The following table lists the device models that can function as central switches.

Table 3-64 Device models that can function as central switches

Series	Sub-series or MPU
S12700E	MPUE, MPUEC
S12700	MPUD
S7700	SRUHX1, SRUE1, SRUH1, SRUHA1, MCUD, SRUHD, SRUED, SRUH, SRUE
S6700	S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S
S5700	S5732-H, S5731-H, S5731S-H, S5731-S, S5731S-S, S5736-S, S5736S-S, S5735S-H, S5735-S, S5735S-S, S5735-S-I, S5720I-SI, S5735-L, S5735S-L, S5735-L1, S5735S-L1, S5735-L-I, S5720-LI, S5720S-LI
S500, S300	-

3.4.2 bind interface

Function

The **bind interface** command binds an interface on the central switch to an RU for interconnection.

The **undo bind** command unbinds the interconnection interface from an RU.

By default, no interconnection interface is bound to an RU.

Format

bind interface *interface-type interface-number*

undo bind

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To deliver configurations to an RU, you need to bind an interface on the central switch to the RU for interconnection. After interface binding, you can run the **remote-unit connect-interface** *interface-type interface-number* command on the central switch to enter the view of an RU by specifying an interconnection interface, and run the **display remote-unit connect-interface** *interface-type interface-number* command to view information about an RU bound to a specific interconnection interface.

Precautions

- An interface can be bound to only one RU.
- An Eth-Trunk physical member interface cannot be bound to an RU.

Example

Bind XGigabitEthernet0/0/1 to the RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] bind interface XGigabitEthernet 0/0/1
```

3.4.3 commit (remote-unit N view)

Function

The **commit** command delivers configurations to a single RU.

Format

commit

Parameters

None

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After configuring an RU by running commands on the central switch, such as configuring the port rate, port isolation, port shutdown, or port negotiation, you need to run the **commit** command to make the configuration take effect.

Precautions

A central switch does not deliver configurations to RUs that fail to be authenticated or are not authenticated.

RUs do not save their configurations. After the central switch or an RU is restarted and works normally, the central switch preferentially delivers the configuration in the single RU view. If no configuration is available in the single RU view, the central switch delivers the configuration in the global RU view.

Example

Deliver configurations to RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] commit
```

3.4.4 commit (remote-unit view)

Function

The **commit** command delivers configurations to RUs.

Format

commit { **all** | **name** *remote-unit-name* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Commits configurations of all RUs.	-

Parameter	Description	Value
name *remote-unit-name*	Specifies the alias of an RU.	The value is a string of 1 to 32 case-sensitive characters without spaces.
interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Views

remote-unit view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After configuring an RU by running commands on the central switch, such as the port rate, port isolation, port shutdown, and port negotiation, you need to run the **commit** command to deliver the configurations to the RU for the configurations to take effect.

The **commit** command can be run to deliver configurations to offline RUs. After an offline RU goes online, the central switch automatically applies the committed configurations to this RU.

Precautions

A central switch does not deliver configurations to RUs that fail to be authenticated or are not authenticated.

RUs do not save their configurations. After the central switch or an RU is restarted and works normally, the central switch preferentially delivers the configuration in the single RU view. If no configuration is available in the single RU view, the central switch delivers the configuration in the global RU view.

Follow-up Procedure

Run the **display remote-unit commit configuration** command to check the configurations that are successfully delivered to RUs, and run the **display remote-unit commit result** command to check configuration delivery results of RUs.

Example

Deliver configurations to the RU connected to XGigabitEthernet0/0/1 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] commit interface XGigabitEthernet 0/0/1
```

3.4.5 description (remote-unit N view)

Function

The **description** command sets a description for an RU.

The **undo description** command restores the default description of an RU.

By default, an RU has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an RU.	The value is a string of 1 to 64 case-sensitive characters, and can contain spaces.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate management and maintenance of RUs, you can set descriptions for RUs to help you understand the usage of each RU.

Precautions

The description is displayed from the first non-space character.

Follow-up Procedure

Run the **display remote-unit commit configuration** command to check the configurations that are successfully delivered to RUs, and run the **display remote-unit commit result** command to check configuration delivery results of RUs.

Example

Set the description of an RU to **ru for office**.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] description ru for office
```

3.4.6 display remote-unit

Function

The **display remote-unit** command displays RU information.

Format

display remote-unit [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*][**verbose**]

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.
verbose	Displays detailed RU information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view RU information, including the ESN, alias, MAC address, device type, online duration, and firmware version of an RU.

Precautions

The central switch does not maintain information about RUs that attempt to go online when the number of connected RUs has reached the upper limit.

The **display remote-unit** command output displays information only about online RUs. You can run the **display current-configuration configuration remote-unit** command to view global configurations of RUs, or run the **display current-configuration configuration remote-unit-n** command to view the configuration of a specific RU.

Example

Display RU information.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit
------------------------------------------------------------------------------------------------------------------------
ESN                     ID        Type                ConnectInterface  Status      VersionMatch  Name
------------------------------------------------------------------------------------------------------------------------
219801176601XXXXXXXX    1         S5731-L8P2HT-RUA    XGE0/0/6          Normal      NO            RU1
219801176601XXXXXXXX    16777214  S5731-L8P2HT-RUA    XGE0/0/7          Normal      NO            RU2
------------------------------------------------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 3-65 Description of the **display remote-unit** command output

Item	Description
ESN	ESN of an RU.
ID	ID of an RU. This field displays a hyphen (-) if an RU is not configured with an ID.
Type	Device type of an RU.
ConnectInterface	Interconnection interface.
Status	Status of an RU: ● **Normal**: The RU is online. ● **Upgrading**: The RU is being upgraded. ● **Configuring**: The RU is being configured. ● **Idle**: The RU is in the initialization state. ● **Abnormal**: The link connecting the RU and central switch is faulty, or the RU is an excess one because the number of connected RUs has reached the upper limit.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.

Item	Description
VersionMatch	Whether the firmware version of the RU matches that of the central switch. ● **YES**: The version matches. ● **NO**: The version does not match. ● **-**: The firmware version of the HUAWEI S5731-L16P2SR-RUA or S5731S-L16P2SR-RUA cannot be upgraded to that of the central switch or that of the patch.
Total: *m*, printed: *n*	Total number of RUs (*m*) and number of RUs whose information is displayed (*n*).

Display detailed RU information.

```
<HUAWEI> display remote-unit verbose
Total number: 2
-------------------------------------------------------------------------
ESN                 :219801177001xxxxxxxx
Name                :-
ID                  :3
Device mac          :xxxx-xxxx-xxxx
Device type         :S5731-L8P2HT-RUA
Item                :98011770
Manufacture Date    :2021-12-17
Up time             :0 day, 6 hours, 25 minutes, 44 seconds
APP version         :220207016
POE version         :7812
BIOS version        :220225001
Connect interface   :Eth-Trunk100
Disk usage          :44%
Memory usage        :22%
Temperature         :37(Celsius)
Mac usage           :0%
Disk space(MB)      :16
Status              :Normal
VersionMatch        :YES
Version support     :YES
Authen Result       :Success
-------------------------------------------------------------------------
ESN                 :219801176801xxxxxxxx
Name                :-
ID                  :2
Device mac          :xxxx-xxxx-xxxx
Device type         :S5731-L8P2HT-RUA
Item                :98011768
Manufacture Date    :2021-12-17
Up time             :0 day, 0 hour, 48 minutes, 39 seconds
APP version         :220123002
POE version         :7812
BIOS version        :220225001
Connect interface   :GigabitEthernet0/0/1
Disk usage          :44%
Memory usage        :22%
Temperature         :39(Celsius)
Mac usage           :0%
Disk space(MB)      :16
Status              :Normal
```

```
VersionMatch       :YES
Version support    :YES
Authen Result      :Success
--------------------------------------------------------------------------
```

Table 3-66 Description of the **display remote-unit verbose** command output

Item	Description
Total number	Total number of RUs.
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
ID	ID of an RU. If an RU is not configured with an ID, a hyphen (-) is displayed.
Device mac	System MAC address of an RU.
Device type	Device type of an RU.
Item	Code of an RU.
Manufacture Date	Manufacture date of an RU.
Up time	Online duration of an RU.
APP version	APP firmware version.
POE version	PoE firmware version.
BIOS version	BIOS firmware version.
Connect interface	Interface connecting the central switch to an RU. If the central switch uses a physical Eth-Trunk member interface to connect to an RU, this field displays the Eth-Trunk interface to which the member interface belongs.
Disk usage	Disk usage of an RU.
Memory usage	Memory usage of an RU.
Temperature	Current temperature of an RU. **NOTE** If the temperature value cannot be read properly, this field displays a hyphen (-). In this case, check whether the central switch receives an alarm from the RU, indicating that the IIC channel is faulty. For details, see the description of the hwRuIICFault alarm.
Mac usage	MAC address table usage of an RU.
Disk space(MB)	Disk size of an RU.

Item	Description
Status	Status of an RU: - **Unknown** - **Idle**: The RU is in the initialization state. - **Normal**: The RU is online. - **Upgrading**: The RU is being upgraded. - **Configuring**: The RU is being configured. - **Abnormal**: The link connecting the RU and central switch is faulty, or the RU is an excess one because the number of connected RUs has reached the upper limit. - **Offline**: The RU is offline.
VersionMatch	Whether the firmware version of the RU matches that of the central device. - **YES**: The version matches. - **NO**: The version does not match.
Version support	Whether the RU supports the firmware of the central switch: - YES: compatible - NO: incompatible
Authen Result	Authentication result of an RU: - **Success** - **Authenticating** - **Fail** - **-**: The RU is not authenticated.

3.4.7 display remote-unit commit configuration

Function

The **display remote-unit commit configuration** command displays the configurations successfully delivered to RUs.

Format

display remote-unit commit configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

RUs do not support web-based management and cannot have commands run on them for configuration. All RU configurations are delivered by the central switch. You can run the **display remote-unit commit configuration** command on the central switch to view the configurations successfully delivered to RUs.

Example

Display the configurations successfully delivered to RUs.

```
<HUAWEI> display remote-unit commit configuration
#
remote-unit 3
 isolate disable
#
#
remote-unit 0
 isolate disable
 undo negotiation auto port 1
 speed 100 port 1
#
```

3.4.8 display remote-unit commit result

Function

The **display remote-unit commit result** command displays configuration delivery results of RUs.

Format

display remote-unit commit result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

RUs do not support web-based management and cannot have commands run on them for configuration. All RU configurations are delivered by the central switch.

You can run the **display remote-unit commit result** command on the central switch to view configuration delivery results of RUs. A maximum of 500 result records are supported.

Example

Display configuration delivery results of RUs.

```
<HUAWEI> display remote-unit commit result
[HUAWEI-remote-unit-0] display remote-unit commit result
------------------------------------------------------------------------------
StartTime            ConnectInterface       CfgType        Result   SendCnt
------------------------------------------------------------------------------
2022/01/27 16:04:02   GE0/0/27              isolate        success  2
2022/01/27 16:04:02   GE0/0/27              shutdown        success  2
2022/01/27 16:04:02   GE0/0/27              negotiation     success  2
2022/01/27 16:04:02   GE0/0/27              speed           success  2
2022/01/27 16:04:02   XGE0/0/1              isolate        success  2
2022/01/27 16:04:02   XGE0/0/1              shutdown        success  2
2022/01/27 16:04:02   XGE0/0/1              negotiation     success  2
2022/01/27 16:04:02   XGE0/0/1              speed           success  2
```

Table 3-67 Description of the **display remote-unit commit result** command output

Item	Description
StartTime	Time when the configuration is delivered.
ConnectInterface	Interconnection interface.
CfgType	Configuration type.
Result	Delivery result: - **success** - **failed**
SendCnt	Number of times that the configurations of the same type are delivered to an RU.

3.4.9 display remote-unit connect record

Function

The **display remote-unit connect record** command displays onboarding and disconnection records of RUs.

Format

display remote-unit connect record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view onboarding and disconnection records of RUs, you can run the **display remote-unit connect record** command. In the command output, you can check when an RU is onboarded or disconnected and the disconnection cause. A maximum of 1024 records are supported.

Example

Display onboarding and disconnection records of RUs.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit connect record
-------------------------------------------------------------------------------------------------------
ESN                          ConnectInterface    Type    Offline Reason         Time
-------------------------------------------------------------------------------------------------------
219801177001XXXXXXXX           GE0/0/27          OnLine  -                   2022-02-08/17:00:36
219801177601XXXXXXXX           GE0/0/25          OnLine  -                   2022-02-08/17:00:39
219801177601XXXXXXXX           XGE0/0/1          OffLine Upgrade                2022-02-08/17:02:32
219801177001XXXXXXXX           GE0/0/27          OffLine Upgrade                2022-02-08/17:02:39
219801177601XXXXXXXX           XGE0/0/1          OnLine  -                   2022-02-08/17:04:09
219801177001XXXXXXXX           GE0/0/27          OnLine  -                   2022-02-08/17:04:33
219801177001XXXXXXXX           GE0/0/27          OffLine Port down              2022-02-09/11:43:06
-------------------------------------------------------------------------------------------------------
Total records: 7
```

Table 3-68 Description of the **display remote-unit record** command output

Item	Description
ESN	ESN of an RU.
ConnectInterface	Interface connecting the central switch to an RU.
Type	Record type: ● **OnLine**: onboarding ● **OffLine**: disconnection

Item	Description
Offline Reason	Disconnection cause: - **Upgrade**: The RU was upgraded and restarted. - **Manual**: The RU was manually restarted. - **No heartbeat**: The RU lost heartbeats and went offline. - **Port down**: The interconnection interface went Down. - **Multi-RU on port**: Multiple RUs were connected to the same interface. - **Abnormal temperature**: The RU goes offline due to abnormal temperature. - **Unknown**
Time	Time when an RU entered this state.
Total records	Total number of records.

3.4.10 display remote-unit poe

Function

The **display remote-unit poe** command displays the global PoE power supply status of an RU.

Format

display remote-unit poe [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Parameter	Description	Value
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view PoE power supply information about an RU, including the configured maximum power, current power consumption, peak power consumption, and PoE firmware status.

Example

Display the global PoE power supply information about the RU connected to XGigabitEthernet0/0/1.

```
<HUAWEI> display remote-unit poe connect-interface XGigabitEthernet 0/0/1
ESN                :21980117760123xxxxxxxx
Name                 :-
Device type          :S5731-L8P2HT-RUA
Connect interface  :XGigabitEthernet0/0/1
-----------------------------------------------------
PSE information    :
  PoE power supply(mW)                              :83000
  Total available power(mW)                         :83000
  Total power consumption(mW)                          :0
  Power peak value(mW)                              :0
  Power voltage(V)                              :54
  PSE reset times                             :0
  PoE failure                               :NO
-----------------------------------------------------
```

Table 3-69 Description of the **display remote-unit poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interface connecting the central switch to an RU.
PoE power supply(mW)	Power supply.

Item	Description
Total available power(mW)	Total available power.
Total power consumption(mW)	Total output power.
Power peak value(mW)	Peak output power.
Power voltage(V)	Output voltage.
PSE reset times	Number of times that the PSE chip is reset.
PoE failure	Whether the PoE firmware is abnormal: ● **NO**: normal ● **YES**: abnormal

3.4.11 display remote-unit poe realtime

Function

The **display remote-unit poe realtime** command displays real-time PoE information about an RU.

Format

display remote-unit poe { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.
interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view real-time PoE information about an RU.

Example

Display real-time PoE information about all interfaces on the RU connected to GigabitEthernet0/0/19 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit poe connect-interface GigabitEthernet 0/0/19 realtime
Info: This operation will take several seconds. Please wait....
ESN              :219801177601XXXXXXXX
Name              :-
Device type        :S5731-L8P2HT-RUA
Connect interface  :GigabitEthernet0/0/19
----------------------------------------------------
PSE information    :
  PoE power supply(mW)                              :83000
  Total available power(mW)                         :46100
  Total power consumption(mW)                          :36900
  Power peak value(mW)                              :50300
  Power voltage(V)                              :53
  PSE reset times                             :0
  PoE failure                               :NO
----------------------------------------------------
```

Table 3-70 Description of the **display remote-unit port poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interface connecting the central switch to an RU.
PoE power supply(mW)	Power supply.
Total available power(mW)	Total available power.
Total power consumption(mW)	Total output power.
Power peak value(mW)	Peak output power.
Power voltage(V)	Output voltage.
PSE reset times	Number of times that the PSE chip is reset.

Item	Description
PoE failure	Whether the PoE firmware is abnormal: - **NO**: normal - **YES**: abnormal

3.4.12 display remote-unit port brief

Function

The **display remote-unit port brief** command displays brief information about interfaces on an RU.

Format

display remote-unit port [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*] **brief**

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor interfaces on an RU or locate faults on interfaces, you can run the **display remote-unit port brief** command to view information about the interfaces, including the physical status, auto-negotiation status, working mode, and rate. If no parameter is specified, brief information about interfaces on all RUs is displayed.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display brief information about interfaces on the RUs connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> display remote-unit port connect-interface Eth-Trunk 10 brief
ESN               :219801177801xxxxxxxx
Name              :-
Device type       :S5731-L8P2HT-RUA
Connect interface :Eth-Trunk10
-------------------------------------------------------------------------------------------
Interface    PHY    Negotiation   Duplex   Mode     Speed(Mbps)   Neighbor-Interface
-------------------------------------------------------------------------------------------
GE1          Up     Enable        Full     Copper   1000          -
GE2          Down   Enable        Full     Copper   1000          -
GE3          Down   Enable        Full     Copper   1000          -
GE4          Down   Enable        Full     Copper   1000          -
GE5          Down   Enable        Full     Copper   1000          -
GE6          Down   Enable        Full     Copper   1000          -
GE7          Down   Enable        Full     Copper   1000          -
GE8          Up     Enable        Full     Copper   1000          -
GE9          Down   Enable        Full     Copper   1000          -
GE10         Up     Enable        Full     Fiber    1000          GE0/0/36
-------------------------------------------------------------------------------------------
```

Table 3-71 Description of the **display remote-unit port brief** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.

Item	Description
Connect interface	Interconnection interface.
Interface	Interface on an RU.
PHY	Physical status of an RU interface: ● **up**: The interface is Up. ● **down**: The interface is Down.
Negotiation	Auto-negotiation status of an RU interface: ● **Enable**: The interface works in auto-negotiation mode. ● **Disable**: The interface works in non-auto negotiation mode.
Duplex	Duplex mode of an RU interface: ● **Full**: The interface works in full-duplex mode. ● **Half**: The interface works in half-duplex mode.
Mode	Working mode of an RU interface: ● **Copper**: electrical mode ● **Fiber**: optical mode
Speed(Mbps)	Rate at which an RU interface works.
Neighbor-Interface	Physical interface used by the central switch for connection with an RU.

3.4.13 display remote-unit port poe

Function

The **display remote-unit port poe** command displays PoE running information about an interface on an RU.

Format

display remote-unit port [*port-id*] **poe** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display remote-unit port poe** command to view PoE running information about interfaces on an RU, including the current power, class of the power device (PD) connected to each interface, reference power of the PD, and power supply status.

If no parameter is specified, the PoE running information about all interfaces on all RUs is displayed.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module. In V200R022C10 and earlier versions, the uplink interface configured with a

GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display the running PoE information about all interfaces on the RU connected to XGigabitEthernet0/0/1 on the central switch.

```
<HUAWEI> display remote-unit port poe connect-interface XGigabitEthernet0/0/1
ESN              :219801177601xxxxxxxx
Name             :-
Device type      :S5731-L4P2HW-RUA
Connect interface  :XGigabitEthernet0/0/1
-----------------------------------------------------
GE1 PoE information:
  PD class                   :-
  PD reference power(mW)       :-
  PD current power(mW)         :0
  PD peak power(mW)            :0
  PD average power(mW)         :0
  Power-up mode                :bt
  Force power                  :Disable
  Power ON/OFF                 :Off
  Power-on delay(s)            :0
  Power status                 :Detecting
  Current(mA)                  :0
  Voltage(V)                   :0

GE2 PoE information:
  PD class                   :-
  PD reference power(mW)       :-
  PD current power(mW)         :0
  PD peak power(mW)            :0
  PD average power(mW)         :0
  Power-up mode                :bt
  Force power                  :Disable
  Power ON/OFF                 :Off
  Power-on delay(s)            :0
  Power status                 :Detecting
  Current(mA)                  :0
  Voltage(V)                   :0

GE3 PoE information:
  PD class                   :0
  PD reference power(mW)       :15400
  PD current power(mW)         :4300
  PD peak power(mW)            :4500
  PD average power(mW)         :4120
  Power-up mode                :bt
  Force power                  :Disable
  Power ON/OFF                 :On
  Power-on delay(s)            :0
  Power status                 :Powered
  Current(mA)                  :80
  Voltage(V)                   :52

GE4 PoE information:
  PD class                   :-
  PD reference power(mW)       :-
  PD current power(mW)         :0
  PD peak power(mW)            :0
  PD average power(mW)         :0
  Power-up mode                :bt
```

```
Force power              :Disable
Power ON/OFF             :Off
Power-on delay(s)        :0
Power status             :Detecting
Current(mA)              :0
Voltage(V)               :0

-------------------------------------------------------
```

Table 3-72 Description of the **display remote-unit port poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interface connecting the central switch to an RU.
PD class	Class of the PD connected to an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD reference power(mW)	Reference power of an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD current power(mW)	Current output power of an interface.
PD peak power(mW)	Peak output power of an interface.
PD average power(mW)	Average output power of an interface.
Power-up mode	Power supply mode of an interface.
Force power	Whether forcible PoE power supply is enabled on an interface. To configure this function, run the **poe force-power port** command.
Power ON/OFF	Whether the interface is supplying power: ● **on**: The interface is supplying power. ● **off**: The interface does not supply power.
Power-on delay(s)	Power supply delay of an interface, in seconds. The value 0 indicates no delay. To set this parameter, run the **poe power-on delay port** command.

Item	Description
Power status	Power supply status of an interface: - **Test mode**: indicates the testing state. - **Detecting**: indicates the detection state. - **Disabled**: indicates that PoE is disabled on the interface. - **Power-deny**: indicates that the reference power is greater than the maximum output power of the interface. - **Classification overcurrent**: indicates that the current of the PDs on the interface exceeds the threshold. - **Unknown**: indicates an unknown class. - **Power overcurrent**: indicates that the interface is in overcurrent condition. - **Power-on failed**: indicates that the interface fails to be powered on. - **Power-ready**: indicates that the interface is ready to be powered on. - **Powering**: indicates that the interface is being powered on. - **Powered**: indicates that the interface has been powered on. - **Overloaded**: indicates that the power is overloaded. - **Time-range power-off**: indicates that the interface is in the power-off time range. - **Unstable voltage**: indicates that the interface voltage is unstable. - **Legacy disable**: indicates that PD compatibility check is disabled on the interface. - **Class mismatch**: indicates that the interface does not support PD classification.
Current(mA)	Output current of an interface.
Voltage(V)	Output voltage of an interface.

3.4.14 display remote-unit port poe realtime

Function

The **display remote-unit port poe realtime** command displays real-time PoE information about an interface on an RU.

Format

display remote-unit port [*port-id*] **poe** { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display remote-unit port poe realtime** command to view real-time power supply information about interfaces on an RU, such as the current power, class of the PD connected to the interface, reference power of the PD, and power supply status.

Example

Display the real-time running PoE information about all interfaces on the RU connected to XGigabitEthernet0/0/1 on the central switch.

```
<HUAWEI> display remote-unit port poe connect-interface XGigabitEthernet0/0/1 realtime
Info: This operation will take several seconds. Please wait.....
ESN                :219801177601xxxxxxxx
Name               :-
Device type        :S5731-L4P2HW-RUA
Connect interface  :XGigabitEthernet0/0/1
-------------------------------------------------------
GE1 PoE information:
  PD class                      :-
  PD reference power(mW)        :-
  PD current power(mW)          :0
  PD peak power(mW)             :0
  PD average power(mW)          :0
  Power-up mode                 :bt
  Force power                   :Disable
  Power ON/OFF                  :Off
  Power-on delay(s)             :0
  Power status                  :Detecting
  Current(mA)                   :0
  Voltage(V)                    :0
  Insertion and removal status :0

GE2 PoE information:
  PD class                      :-
  PD reference power(mW)        :-
  PD current power(mW)          :0
  PD peak power(mW)             :0
  PD average power(mW)          :0
  Power-up mode                 :bt
  Force power                   :Disable
  Power ON/OFF                  :Off
  Power-on delay(s)             :0
  Power status                  :Detecting
  Current(mA)                   :0
  Voltage(V)                    :0
  Insertion and removal status :0

GE3 PoE information:
  PD class                      :-
  PD reference power(mW)        :-
  PD current power(mW)          :4200
  PD peak power(mW)             :0
  PD average power(mW)          :0
  Power-up mode                 :bt
  Force power                   :Disable
  Power ON/OFF                  :Off
  Power-on delay(s)             :0
  Power status                  :Detecting
  Current(mA)                   :83
  Voltage(V)                    :52
  Insertion and removal status :0

GE4 PoE information:
  PD class                      :-
  PD reference power(mW)        :-
  PD current power(mW)          :0
  PD peak power(mW)             :0
  PD average power(mW)          :0
  Power-up mode                 :bt
  Force power                   :Disable
  Power ON/OFF                  :Off
  Power-on delay(s)             :0
  Power status                  :Detecting
  Current(mA)                   :0
  Voltage(V)                    :0
  Insertion and removal status :0

-------------------------------------------------------
```

Table 3-73 Description of the **display remote-unit port poe** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interconnection interface.
PD class	Class of the PD connected to an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD reference power(mW)	Reference power of an interface. This field displays a hyphen (-) if **Power status** is **Detecting**.
PD current power(mW)	Current output power of an interface.
PD peak power(mW)	Peak output power of an interface.
PD average power(mW)	Average output power of an interface.
Power-up mode	Power supply mode of an interface.
Force power	Whether forcible PoE power supply is enabled on an interface. To configure this function, run the **poe force-power port** command.
Power ON/OFF	Whether the interface is providing power: ● **on**: The interface is supplying power. ● **off**: The interface does not supply power.
Power-on delay(s)	Power supply delay of an interface, in seconds. The value 0 indicates no delay. To set this parameter, run the **poe power-on delay port** command.

Item	Description
Power status	Power supply status of an interface: - **Test mode**: indicates the testing state. - **Detecting**: indicates the detection state. - **Disabled**: indicates that PoE is disabled on the interface. - **Power-deny**: indicates that the reference power is greater than the maximum output power of the interface. - **Classification overcurrent**: indicates that the current of the PDs on the interface exceeds the threshold. - **Unknown**: indicates an unknown class. - **Power overcurrent**: indicates that the interface is in overcurrent condition. - **Power-on failed**: indicates that the interface fails to be powered on. - **Power-ready**: indicates that the interface is ready to be powered on. - **Powering**: indicates that the interface is being powered on. - **Powered**: indicates that the interface has been powered on. - **Overloaded**: indicates that the power is overloaded. - **Time-range power-off**: indicates that the interface is in the power-off time range. - **Unstable voltage**: indicates that the interface voltage is unstable. - **Legacy disable**: indicates that PD compatibility check is disabled on the interface. - **Class mismatch**: indicates that the interface does not support PD classification.
Current(mA)	Output current of an interface.
Voltage(V)	Output voltage of an interface.

Item	Description
Insertion and removal status	Whether the interface has PD removal and installation records. ● **0**: initial value, which is meaningless. If an RU is started with a PD, this field displays **0**. ● **1**: indicates that the interface has PD installation records. ● **2**: indicates that the interface has PD removal records. ● **3**: indicates that the interface has PD removal and installation records

3.4.15 display remote-unit port realtime

Function

The **display remote-unit port realtime** command displays real-time information about interfaces on an RU.

Format

display remote-unit port { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor interfaces on a specific RU or locate faults on interfaces, you can run the **display remote-unit port realtime** command to view real-time information about the interfaces, including the physical status, auto-negotiation status, working mode, and rate.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display information about all interfaces on the RUs connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit port connect-interface Eth-Trunk 10 realtime
Info: This operation will take several seconds. Please wait...
ESN                :219801177801xxxxxxxx
Name               :-
Device type        :S5731-L4P2HW-RUA
Connect interface  :Eth-Trunk10
-----------------------------------------------------------------------------------------
Interface    PHY      Negotiation    Duplex    Mode     Speed(Mbps)   Neighbor-Interface
-----------------------------------------------------------------------------------------
GE1          Up       Enable         Full      Copper   1000          -
GE2          Down       Enable         Full      Copper   1000          -
GE3          Down       Enable         Full      Copper   1000          -
GE4          Down       Enable         Full      Copper   1000          -
GE5          Down       Enable         Full      Copper   1000          -
GE6          Up       Enable         Full      Fiber    1000          GE0/0/36
-----------------------------------------------------------------------------------------
```

Table 3-74 Description of the **display remote-unit port brief** command output

Item	Description
ESN	ESN of an RU.

Item	Description
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Connect interface	Interface connecting the central switch to an RU.
Interface	Interface of an RU.
PHY	Status of an RU interface: ● **up**: The interface is Up. ● **down**: The interface is Down.
Negotiation	Auto-negotiation status of an RU interface: ● **Enable**: The interface works in auto-negotiation mode. ● **Disable**: The interface works in non-auto negotiation mode.
Duplex	Duplex mode of an RU interface: ● **Full**: The interface works in full-duplex mode. ● **Half**: The interface works in half-duplex mode.
Mode	Working mode of an RU interface: ● **Copper**: electrical mode ● **Fiber**: optical mode
Speed(Mbps)	Rate at which an RU interface works.
Neighbor-Interface	Physical interface used by the central switch for connection with an RU.

3.4.16 display remote-unit port statistics

Function

The **display remote-unit port statistics** command displays traffic statistics about an interface on an RU.

Format

display remote-unit port [*port-id*] **statistics** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the status and statistics of interfaces on an RU, including the interface physical status, basic configuration, and packet forwarding information. The information is refreshed every 60 seconds. You can use this command to collect traffic statistics or locate faults on an interface. If no index of an RU interface is specified, traffic statistics about all interfaces on the RU are displayed.

Precautions

- An uplink 2.5GE optical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical module. In V200R022C10 and earlier versions, the uplink interface configured with a GE optical module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.
- An uplink 2.5GE hybrid optical-electrical interface of an RU does not support a copper module, and supports only a GE or 2.5GE optical or hybrid module.

In V200R022C10 and earlier versions, the uplink interface configured with a GE optical or hybrid module can connect to a central switch only when it works at the rate of 1 Gbit/s. In V200R023C00 and later versions, the uplink interface configured with a 2.5GE optical or hybrid module can connect to a central switch when it works at the rate of 2.5 Gbit/s. After the rate of the uplink interface is changed, the RU automatically restarts for the change to take effect.

Example

Display traffic statistics on interface 1 of the RU connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> display remote-unit port 1 statistics connect-interface Eth-Trunk 10
ESN               :219801177601XXXXXXXX
Name              :S5731S-4P
Device type       :S5731-L8P2HT-RUA
Connect interface  :Eth-Trunk10
-------------------------------------------------------------------------------
GE1 current state : DOWN
Speed: 1000,  Duplex: Full,  Negotiation: Enable,  Mode: Copper,  Congestion: No
Input rate 0 bits/sec, 0 packets/sec
Output rate 0 bits/sec, 0 packets/sec

Input: 0 packets, 0 bytes
  Unicast:                       0,  Multicast:                       0
  Broadcast:                     0,  Jumbo:                           0
  Discard:                       0,  Pause:                           0
  Frames:                        0

  Total Error:                   0
  CRC:                           0,  Giants:                          0
  Runts:                         0,  DropEvents:                      0
  Alignments:                    0,  Symbols:                         0
  Ignoreds:                      0

Output : 0 packets, 0 bytes
  Unicast:                       0,  Multicast:                       0
  Broadcast:                     0,  Jumbo:                           0
  Discard:                       0,  Pause:                           0

  Total Error:                   0
  Collisions:                    0,  Late Collisions:                 0
  Deferreds:                     0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Last 60 seconds input utility rate : 0.00%
    Last 60 seconds output utility rate: 0.00%

-------------------------------------------------------------------------------
```

Table 3-75 Description of the **display remote-unit port statistics** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.

Item	Description
Device type	Device type of an RU.
Connect interface	Interconnection interface.
GE*n* current state	Physical status of the GE*n* interface on an RU. - **DOWN**: indicates that a fault occurs at the physical layer of the interface. The possible cause can be that no terminal is connected to the interface or the interface is shut down. - **Up**: indicates that the interface is physically Up.
Speed	Current rate of an interface. - In auto-negotiation mode, this field displays the interface rate after auto-negotiation with terminals. - In non-auto-negotiation mode, you can run the **speed** command to configure an interface rate.
Duplex	Duplex mode of an interface: - **Full**: The interface works in full-duplex mode. - **Half**: The interface works in half-duplex mode.
Negotiation	Auto-negotiation status of an interface. To configure auto-negotiation for an interface, run the **negotiation auto** command. - **Enable**: The interface works in auto-negotiation mode. - **Disable**: The interface works in non-auto negotiation mode.
Mode	Working mode of an interface: - **Copper**: electrical mode - **Fiber**: optical mode
Congestion	Congestion status of an RU interface: - **YES**: The RU interface is congested. - **NO**: The RU interface is not congested.
Input rate 0 bits/sec, 0 packets/sec	Rate of incoming packets on an interface.

Item	Description
Output rate 0 bits/sec, 0 packets/sec	Rate of outgoing packets on an interface.
Input	Total number of received packets. **NOTE** ● Packets that are longer than jumbo frames and have correct CRC values are counted in **Jumbo** statistics but not in **Input** statistics. ● An RU can forward a packet with a maximum size of 10240 bytes.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by an interface.
Multicast	Number of multicast packets received or sent by an interface.
Broadcast	Number of broadcast packets that are received or sent by the interface.
Jumbo	Statistics about outgoing packets on an interface. The following packets are counted: ● Ethernet frames longer than 1518 bytes and with correct FCS values Statistics about incoming packets on an interface. The following packets are counted: ● Ethernet frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values ● VLAN frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values ● Packets with the length greater than the maximum jumbo frame length
Discard	Number of packets discarded by an interface during physical layer detection. A possible cause can be interface congestion. **NOTE** Currently, this item is not supported, and the value is displayed as 0.

Item	Description
Frames	Number of packets with the incorrect 802.3 length received by an interface.
Pause	Number of pause frames.
Total Error	Number of error frames found during physical layer detection.
CRC	Number of packets longer than 63 bytes and with incorrect FCS values.
Giants	Number of received packets with the length exceeding the maximum jumbo frame length. **NOTE** Currently, this item is not supported, and the value is displayed as 0. Such packets are counted in the **Jumbo** field.
Runts	Number of received undersized frames with correct CRC values. An undersized frame is a frame that is shorter than 64 bytes, in correct format, and contains a valid CRC field. **NOTE** Packets with incorrect CRC values and the length shorter than 64 bytes are also counted in **Runts**.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors. **NOTE** Currently, this item is not supported, and the value is displayed as 0.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE. **NOTE** If an RU interface receives an **Ignoreds** packet, the packet is not only counted as an Ignoreds packet, but also is counted as a unicast, multicast, or a broadcast packet. The total number of incoming packets on an interface has excluded repeated counts. Therefore, the statistics are correct.

Item	Description
Collisions	Number of collision frames. A collision frame is a frame that is not sent due to a detected collision.
Late Collisions	Number of deferred collision frames. A deferred collision frame is a frame that is delayed to be sent because of a deferred collision detected after the frame's first 512 bits are sent.
Deferreds	Number of deferred packets. A deferred packet refers to a packet that is delayed due to a detected collision.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Last 60 seconds input utility rate	Inbound bandwidth usage within the last 60 seconds.
Last 60 seconds output utility rate	Outbound bandwidth usage within the last 60 seconds.

3.4.17 display remote-unit port statistics realtime

Function

The **display remote-unit port statistics realtime** command displays real-time traffic statistics about an interface on an RU.

Format

display remote-unit port [*port-id*] **statistics** { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and statistics of interfaces on an RU, including the interface physical status, basic configuration, and packet forwarding information. You can run this command when you need to collect real-time traffic statistics or diagnose faults on an interface in real time, or when you cannot locate faults according to the information reported by RUs at an interval of 60s.

Example

Display real-time traffic statistics about interface 1 on the RU connected to XGigabitEthernet0/0/5 on the central switch

```
<HUAWEI> display remote-unit port 1 statistics  connect-interface XGigabitEthernet 0/0/5 realtime
ESN               :219801176601XXXXXXXX
Name              :-
Device type       :S5731-L8P2HT-RUA
Connect interface :XGigabitEthernet 0/0/5
----------------------------------------------------------------------------------
GE1 current state : UP
Speed: 1000,  Duplex: Full,  Negotiation: Enable,  Mode: Copper,  Congestion: No
Input rate 0 bits/sec, 0 packets/sec
Output rate 2294 bits/sec, 2 packets/sec

Input: 0 packets, 0 bytes
  Unicast:                    0,  Multicast:                   0
  Broadcast:                  0,  Jumbo:                       0
  Discard:                    0,  Pause:                       0
  Frames:                     0

  Total Error:                0
  CRC:                        0,  Giants:                      0
  Runts:                      0,  DropEvents:                  0
  Alignments:                 0,  Symbols:                     0
  Ignoreds:                   0

Output : 2719354134 packets, 503308078504 bytes
  Unicast:                    0,  Multicast:               50766
  Broadcast:         2719303368,  Jumbo:                       0
```

```
Discard:                        0,  Pause:                          0

Total Error:                    0
Collisions:                     0,  Late Collisions:                0
Deferreds:                      0

  Input bandwidth utilization threshold : 80.00%
  Output bandwidth utilization threshold: 80.00%
  Last 60 seconds input utility rate : 0.00%
  Last 60 seconds output utility rate: 0.00%

------------------------------------------------------------------------------------------
```

Table 3-76 Description of the **display remote-unit port statistics realtime** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interconnection interface.
GE*n* current state	Physical status of the GE*n* interface on an RU. ● **DOWN**: indicates that a fault occurs at the physical layer of the interface. The possible cause can be that no terminal is connected to the interface or the interface is shut down. ● **Up**: indicates that the interface is physically Up.
Speed	Current rate of an interface. ● In auto-negotiation mode, this field displays the interface rate after auto-negotiation with terminals. ● In non-auto-negotiation mode, you can run the **speed** command to configure an interface rate.
Duplex	Duplex mode of an interface: ● **Full**: The interface works in full-duplex mode. ● **Half**: The interface works in half-duplex mode.

Item	Description
Negotiation	Auto-negotiation status of an interface. To configure auto-negotiation for an interface, you can run the **negotiation auto** command. - **Enable**: The interface works in auto-negotiation mode. - **Disable**: The interface works in non-auto negotiation mode.
Mode	Working mode of an interface: - **Copper**: electrical mode - **Fiber**: optical mode
Congestion	Congestion status of an RU interface: - **YES**: The RU interface is congested. - **NO**: The RU interface is not congested.
Input rate 0 bits/sec, 0 packets/sec	Rate of incoming packets on an interface.
Output rate 0 bits/sec, 0 packets/sec	Rate of outgoing packets on an interface.
Input	Total number of received packets. **NOTE** - Packets that are longer than jumbo frames and have correct CRC values are counted in **Jumbo** statistics but not in **Input** statistics. - An RU can forward a packet with a maximum size of 10240 bytes.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by an interface.
Multicast	Number of multicast packets received or sent by an interface.
Broadcast	Number of broadcast packets that are received or sent by the interface.

Item	Description
Jumbo	Statistics about outgoing packets on an interface. The following packets are counted: ● Ethernet frames longer than 1518 bytes and with correct FCS values Statistics about incoming packets on an interface. The following packets are counted: ● Ethernet frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values ● VLAN frames with the length greater than or equal to 1519 bytes and less than the maximum jumbo frame length and correct FCS values ● Packets with the length greater than the maximum jumbo frame length
Discard	Number of packets discarded by an interface during physical layer detection. A possible cause can be interface congestion. **NOTE** Currently, this item is not supported, and the value is displayed as 0.
Frames	Number of packets with the incorrect 802.3 length received by an interface.
Pause	Number of Pause frames.
Total Error	Number of error frames found during physical layer detection.
CRC	Number of packets longer than 63 bytes and with incorrect FCS values.
Giants	Number of received packets with the length exceeding the maximum jumbo frame length. **NOTE** Currently, this item is not supported, and the value is displayed as 0. Such packets are counted in the **Jumbo** field.

Item	Description
Runts	Number of received undersized frames with correct CRC values. An undersized frame is a frame that is shorter than 64 bytes, in correct format, and contains a valid CRC field. **NOTE** Packets with incorrect CRC values and the length shorter than 64 bytes are also counted in **Runts**.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors. **NOTE** Currently, this item is not supported, and the value is displayed as 0.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE. **NOTE** If an RU interface receives an **Ignoreds** packet, the packet is not only counted as an Ignoreds packet, but also is counted as a unicast, multicast, or a broadcast packet. The total number of incoming packets on an interface has excluded repeated counts. Therefore, the statistics are correct.
Collisions	Number of collision frames. A collision frame is a packet that is not sent due to a detected collision.
Late Collisions	Number of deferred collision frames. A deferred collision frame is a frame that is delayed to be sent because of a deferred collision detected after the transmission of the frame first 512 bits.
Deferreds	Number of deferred packets. A deferred packet refers to a packet that is delayed due to a detected collision.
Input bandwidth utilization threshold	Threshold for the inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for the outbound bandwidth usage.

Item	Description
Last 60 seconds input utility rate	Inbound bandwidth usage within the last 60 seconds.
Last 60 seconds output utility rate	Outbound bandwidth usage within the last 60 seconds.

3.4.18 display remote-unit port transceiver

Function

The **display remote-unit port transceiver** command displays information about the optical module installed on an interface of an RU.

Format

display remote-unit port [*port-id*] **transceiver** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view general, manufacturing, and diagnostic information about the optical module installed on an interface of an RU.

Example

Display information about the optical module installed on the interface with index 6 of all RUs.

```
<HUAWEI> display remote-unit port 6 transceiver
ESN                :219801177001xxxxxxxx
Name               :-
Device type        :S5731-L4P2HW-RUA
Connect interface  :GigabitEthernet0/0/27
-------------------------------------------------------
GE6 transceiver information:
-------------------------------------------------------
Common information:
  Transceiver type                  :1000_BASE_LX_SFP
  Transfer distance(m)              :10000(9um)
  Digital diagnostic monitoring     :YES
  Vendor name                       :WTD
-------------------------------------------------------
Manufacture information:
  Manu. serial Number               :MF213704450083
  Manufacturing date                :2021-10-22
  Vendor name                       :WTD
-------------------------------------------------------
Diagnostic information:
  Temperature(Celsius)              :57.04
  Temp high threshold(Celsius)      :95.00
  Temp low  threshold(Celsius)      :-50.00
  Voltage(V)                        :3.27
  Volt high threshold(V)            :3.63
  Volt low  threshold(V)            :2.97
  Bias current(mA)                  :32.89
  Bias high threshold(mA)           :80.00
  Bias low threshold(mA)            :10.00
  RX power(dBM)                     :-5.52
  RX power high warning(dBM)        :-3.00
  RX power low warning(dBM)         :-19.00
  RX power high threshold(dBM)      :-1.00
  RX power low threshold(dBM)       :-21.02
  TX power(dBM)                     :-4.62
  TX power high warning(dBM)        :-3.00
  TX power low warning(dBM)         :-11.00
  TX power high threshold(dBM)      :-1.00
  TX power low threshold(dBM)       :-13.00

-------------------------------------------------------
ESN                :QU221A000285
Name               :-
Device type        :S5731-L8P2HT-RUA
Connect interface  :GigabitEthernet0/0/1
-------------------------------------------------------
GE10 transceiver information:
-------------------------------------------------------
Common information:
  Transceiver type                  :1000_BASE_LX_SFP
  Transfer distance(m)              :10000(9um)
  Digital diagnostic monitoring     :YES
  Vendor name                       :WTD
-------------------------------------------------------
Manufacture information:
  Manu. serial Number               :MF213704450086
  Manufacturing date                :2021-10-22
```

```
  Vendor name                       :WTD
-------------------------------------------------------
Diagnostic information:
  Temperature(Celsius)              :57.04
  Temp high threshold(Celsius)      :95.00
  Temp low  threshold(Celsius)      :-50.00
  Voltage(V)                        :3.27
  Volt high threshold(V)            :3.63
  Volt low  threshold(V)            :2.97
  Bias current(mA)                  :32.64
  Bias high threshold(mA)           :80.00
  Bias low threshold(mA)            :10.00
  RX power(dBM)                     :-5.99
  RX power high warning(dBM)        :-3.00
  RX power low warning(dBM)         :-19.00
  RX power high threshold(dBM)      :-1.00
  RX power low threshold(dBM)       :-21.02
  TX power(dBM)                     :-4.62
  TX power high warning(dBM)        :-3.00
  TX power low warning(dBM)         :-11.00
  TX power high threshold(dBM)      :-1.00
  TX power low threshold(dBM)       :-13.00

-------------------------------------------------------
```

Table 3-77 Description of the **display remote-unit port transceiver** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Connect interface	Interconnection interface.
GE*n* transceiver information	Information about the optical module installed on the GE*n* interface of an RU.
Common information	General information.
Transceiver type	Type of an optical module.

Item	Description
Transfer distance(m)	Transmission distance of an optical module. ● **OM1**: indicates traditional 62.5 µm/125 µm multimode fibers. ● **OM2**: indicates traditional 50 µm/125 µm multimode fibers. ● **OM3**: indicates next-generation multimode fibers, with longer transmission distances than OM1 and OM2 fibers. For a GPS optical module, this field indicates the maximum length of the antenna between the GPS optical module and signal receiver. **NOTE** The device displays only the maximum transmission distances supported by different optical fibers of an optical module.
Digital diagnostic monitoring	Whether diagnostic information about an optical module is monitored.
Vendor name	Vendor of an optical module.
Manufacture information	Manufacture information.
Manu. serial Number	Manufacturing sequence number of an optical module.
Manufacturing date	Manufacturing date of an optical module.
Diagnostic information	Diagnostic information.
Temperature(Celsius)	Current temperature of an optical module.
Temp high threshold(Celsius)	Upper temperature threshold of an optical module.
Temp low threshold(Celsius)	Lower temperature threshold of an optical module.
Voltage(V)	Current voltage of an optical module.
Volt high threshold(V)	Upper voltage threshold of an optical module.
Volt low threshold(V)	Lower voltage threshold of an optical module.
Bias current(mA)	Bias current of an optical module.

Item	Description
Bias high threshold(mA)	Upper threshold for the bias current of an optical module.
Bias low threshold(mA)	Lower threshold for the bias current of an optical module.
RX power(dBM)	Receive power of an optical module. When the receive power is 0 W, this field displays **-Inf**.
RX power high warning(dBM)	Upper warning threshold for the receive power of an optical module.
RX power low warning(dBM)	Lower warning threshold for the receive power of an optical module.
RX power high threshold(dBM)	Upper receive power threshold of an optical module.
RX power low threshold(dBM)	Lower receive power threshold of an optical module.
TX power(dBM)	Transmit power of an optical module. When the transmit power is 0 W, this field displays **-Inf**.
TX power high warning(dBM)	Upper warning threshold for the transmit power of an optical module.
TX power low warning(dBM)	Lower warning threshold for the transmit power of an optical module.
TX power high threshold(dBM)	Upper transmit power threshold of an optical module.
TX power low threshold(dBM)	Lower transmit power threshold of an optical module.

3.4.19 display remote-unit port transceiver realtime

Function

The **display remote-unit port transceiver** command displays real-time information about the optical module installed on an interface of an RU.

Format

display remote-unit port [*port-id*] **transceiver** { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **realtime**

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If this parameter is not specified, statistics about all interfaces on the RU are displayed.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view real-time information about the optical modules installed on an RU.

Example

Display real-time information about the optical module installed on the interface with index 6 of the RU connected to XGigabitEthernet 0/0/5 on the central switch.

```
<HUAWEI> display remote-unit port 6 transceiver connect-interface XGigabitEthernet 0/0/5 realtime
Info: This operation will take several seconds. Please wait...........
ESN                :219801177002xxxxxxxx
Name               :-
Device type        :S5731-L8P2HT-RUA
Connect interface  :XGigabitEthernet0/0/5
-------------------------------------------------------
GE6 transceiver information:
-------------------------------------------------------
Common information:
  Transceiver type                :1000_BASE_SX_SFP
  Transfer distance(m)            :275(OM1),550(OM2),1000(OM3)
  Digital diagnostic monitoring   :YES
  Vendor name                     :WTD
-------------------------------------------------------
Manufacture information:
  Manu. serial Number             :EC184500011577
```

```
  Manufacturing date              :2018-11-06
  Vendor name                     :WTD
-------------------------------------------------------
Diagnostic information:
  Temperature(Celsius)              :57.04
  Temp high threshold(Celsius)      :95.00
  Temp low  threshold(Celsius)      :-50.00
  Voltage(V)                        :3.31
  Volt High Threshold(V)            :3.63
  Volt Low  Threshold(V)            :2.97
  Bias current(mA)                  :2.78
  Bias high threshold(mA)           :40.00
  Bias low threshold(mA)            :0.00
  RX power(dBM)                     :-5.66
  RX power high warning(dBM)        :0.00
  RX power low warning(dBM)         :-17.01
  RX power high threshold(dBM)      :2.00
  RX power low threshold(dBM)       :-19.03
  TX power(dBM)                     :-5.77
  TX power high warning(dBM)        :0.00
  TX power low warning(dBM)         :-9.50
  TX power high threshold(dBM)      :2.00
  TX power low threshold(dBM)       :-11.51

-------------------------------------------------------
```

Table 3-78 Description of the **display remote-unit port transceiver realtime** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Connect interface	Interface connecting the central switch to an RU.
GE*n* transceiver information	Information about the optical module installed on the GE*n* interface of an RU.
Common information	General information.
Transceiver type	Type of an optical module.

Item	Description
Transfer distance(m)	Transmission distance of an optical module. - **OM1**: indicates traditional 62.5 µm/125 µm multimode fibers. - **OM2**: indicates traditional 50 µm/125 µm multimode fibers. - **OM3**: indicates next-generation multimode fibers, with longer transmission distances than OM1 and OM2 fibers. For a GPS optical module, this field indicates the maximum length of the antenna between the GPS optical module and signal receiver. **NOTE** The device displays only the maximum transmission distances supported by different optical fibers of an optical module.
Digital diagnostic monitoring	Whether diagnostic information about an optical module is monitored.
Vendor name	Vendor of an optical module.
Manufacture information	Manufacture information.
Manu. serial Number	Manufacturing sequence number of an optical module.
Manufacturing date	Manufacturing date of an optical module.
Vendor name	Vendor of an optical module.
Diagnostic information	Diagnostic information.
Temperature(Celsius)	Current temperature of an optical module.
Temp high threshold(Celsius)	Upper temperature threshold of an optical module.
Temp low threshold(Celsius)	Lower temperature threshold of an optical module.
Voltage(V)	Current voltage of an optical module.
Volt high threshold(V)	Upper voltage threshold of an optical module.
Volt low threshold(V)	Lower voltage threshold of an optical module.

Item	Description
Bias current(mA)	Bias current of an optical module.
Bias high threshold(mA)	Upper threshold for the bias current of an optical module.
Bias low threshold(mA)	Lower threshold for the bias current of an optical module.
RX power(dBM)	Receive power of an optical module. When the receive power is 0 W, this field displays **-Inf**.
RX power high warning(dBM)	Upper warning threshold for the receive power of an optical module.
RX power low warning(dBM)	Lower warning threshold for the receive power of an optical module.
RX power high threshold(dBM)	Upper receive power threshold of an optical module.
RX power low threshold(dBM)	Lower receive power threshold of an optical module.
TX power(dBM)	Transmit power of an optical module. When the transmit power is 0 W, this field displays **-Inf**.
TX power high warning(dBM)	Upper warning threshold for the transmit power of an optical module.
TX power low warning(dBM)	Lower warning threshold for the transmit power of an optical module.
TX power high threshold(dBM)	Upper transmit power threshold of an optical module.
TX power low threshold(dBM)	Lower transmit power threshold of an optical module.

3.4.20 display remote-unit upgrade

Function

The **display remote-unit upgrade** command displays RU upgrade information.

Format

display remote-unit upgrade { **record** | **information** }

Parameters

Parameter	Description	Value
record	Displays upgrade records of RUs.	-
information	Displays the upgrade information about the RUs that are being upgraded.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An RU has three types of firmware: APP firmware (controlling the forwarding process, parsing XLDP packets, and processing configurations), PoE firmware, and BIOS firmware. The three types of firmware can all be upgraded. System software packages or patches (containing firmware) of the central switch can be used to upgrade RUs.

You can run this command to view the upgrade information about RUs. The information includes the firmware version of an RU connected to the central switch, information about the RUs that fail to be upgraded and enter the cooldown period, information about RUs which have the firmware package of the new version successfully pre-loaded and wait to be reset, information about RUs that are being upgraded, and the upgrade progress in percentage. After the upgrade is complete, you can run this command to check upgrade records.

If an RU fails to be upgraded, it enters the cooldown period. You can upgrade it again only after the cooldown period ends.

Example

Display RU upgrade information.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit upgrade information
Firmware information:
-------------------------------------------------------------------------------
Type          Version            From              Note
-------------------------------------------------------------------------------
APP           220207016            Startup software    -
POE           -                  -                 -
BIOS          220207016            Startup software    -

Remote-unit during cooling down:
-------------------------------------------------------------------------------
Type          ConnectInterface      FailCnt          CoolDownInSeconds
-------------------------------------------------------------------------------

Waiting for restart to apply new firmware's remote-unit information:
-------------------------------------------------------------------------------
```

```
Type            ConnectInterface        NextVersion(APP/POE/BIOS)
-------------------------------------------------------------------------------

Upgrading remote-unit information:
-------------------------------------------------------------------------------
Type            ConnectInterface        Firmware           Percent
-------------------------------------------------------------------------------
S5731-L8P2HT-RUA  XGigabitEthernet0/0/1    APP                3%
```

Table 3-79 Description of the **display remote-unit upgrade information** command output

Item	Description
Firmware information	Firmware of the RU to be upgraded.
Type	Firmware type. The options include **APP**, **POE**, and **BIOS**.
Version	Firmware version. **NOTE** For an RU of the S5731-L16P2SR-RUA or S5731S-L16P2SR-RUA model, only the following firmware versions are supported: APP firmware: 221207011 PoE firmware: 7701 BIOS firmware: 220225001 The S5731-L8LP2ST-RUA supports only the following firmware versions: APP firmware: 230109001 and later
From	Source file used for upgrading the RU. It can be a patch or software package of the central switch.
Note	Whether the current firmware is successfully signed. ● **-**: The signature is correct. ● **Bad signature**: The firmware patch signature is incorrect. In this case, the firmware will not be upgraded. ● **No signature**: The firmware patch does not have a digital signature. In this case, the firmware will not be upgraded.
Remote-unit during cooling down	RUs that fail to be upgraded and are in the cooldown period. You can end the cooldown period of an RU by resetting the RU.
Type	Device type of an RU.
ConnectInterface	Interconnection interface.
FailCnt	Number of upgrade failures.

Item	Description
CoolDownInSeconds	Remaining seconds in the cooldown period. When the value becomes 0, the RU can be upgraded again.
Waiting for restart to apply new firmware's remote-unit information	Information about the RUs that have new firmware successfully pre-loaded and wait to be reset. **NOTE** If the function of applying new functions after the upgrade at a specified time is enabled, the information about the RUs to be reset at a specified time is displayed. If this function is disabled and an RU cannot be reset in time, the information about the RU is displayed in this field for a short time. After the RU is reset, the corresponding information is automatically cleared.
NextVersion(APP/POE/BIOS)	Version number for the next startup. **NOTE** If the upgrade command is run in the remote-unit view, the version for the next RU startup is displayed. For the firmware not supported by the RU, a hyphen (-) is displayed. If the forcible upgrade command is run in the remote-unit N view, the version number only of the upgraded firmware is displayed. For the firmware not upgraded, a hyphen (-) is displayed.
Upgrading remote-unit information:	Information about the RUs that are being upgraded.
Firmware	Firmware type. The options include **APP**, **POE**, and **BIOS**.
Percent	Upgrade progress, in percentage.

Display upgrade records of RUs.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit upgrade record
------------------------------------------------------------------------------
StartTime            ConnectInterface       Firmware   UpdateResult
------------------------------------------------------------------------------
2021/12/25 03:25:54   XGigabitEthernet0/0/1   APP        Success
2021/12/25 03:30:08   XGigabitEthernet0/0/1   APP        Success
```

Table 3-80 Description of the **display remote-unit upgrade record** command output

Item	Description
StartTime	Start time.
ConnectInterface	Interconnection interface.
Firmware	Firmware type. The options include **APP**, **POE**, and **BIOS**.
UpdateResult	Upgrade result. **Success** indicates that the upgrade is successful. Other values indicate that the upgrade fails.

3.4.21 display remote-unit verbose realtime

Function

The **display remote-unit** command displays detailed real-time information about an RU.

Format

display remote-unit { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **verbose realtime**

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of the interface connecting the central switch to an RU. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view detailed real-time information about an RU, including the ESN, name, MAC address, device type, online duration, and firmware version.

Example

Display detailed real-time information about the RU connected to Eth-Trunk 10 on the central switch.

```
<HUAWEI> system-view
[HUAWEI] display remote-unit connect-interface Eth-Trunk 10 verbose realtime
------------------------------------------------------------------------
ESN                :219801177002xxxxxxxx
Name                 :-
ID                 :10
Device mac          :xxxx-xxxx-xxxx
Device type         :S5731-L4T2S-RUA
Item                :98011768
Manufacture Date   :2021-12-17
Up time             :0 day, 4 hours, 12 minutes, 20 seconds
APP version         :220123020
POE version         :-
BIOS version        :220207016
Connect interface  :Eth-Trunk10
Disk usage          :44%
Memory usage        :40%
Temperature         :34(Celsius)
Mac usage           :0%
Status              :Normal
Authen Result       :-
------------------------------------------------------------------------
```

Table 3-81 Description of the **display remote-unit verbose realtime** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
ID	ID of an RU.
Device mac	System MAC address of an RU.
Device type	Device type of an RU.
Item	Code of an RU.
Manufacture Date	Manufacture date of an RU.
Up time	Online duration of an RU.
APP version	APP firmware version.
POE version	PoE firmware version.
BIOS version	BIOS firmware version.

Item	Description
Connect interface	Interface connecting the central switch to an RU. If the central switch uses a physical Eth-Trunk member interface to connect to an RU, this field displays the corresponding Eth-Trunk interface.
Disk usage	Disk usage of an RU.
Memory usage	Memory usage of an RU.
Temperature	Current temperature of an RU.
Mac usage	MAC address table usage of an RU.
Disk space(MB)	Disk size of an RU.
Status	Status of an RU: ● **Normal**: online ● **Upgrading** ● **Configuring**: the RU is being configured. ● **Abnormal**: The link connecting the RU and central switch is faulty, or the RU is an excess one because the number of connected RUs has reached the upper limit. ● **Idle**: the RU is in the initialization state.
Authen Result	Authentication result of an RU: ● **Success** ● **Fail** ● **-**: the RU is not authenticated.

3.4.22 display remote-unit vlan

Function

The **display remote-unit vlan** command displays VLAN information about interfaces on an RU.

Format

display remote-unit vlan [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

display remote-unit vlan { **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* } **vlan** *vlan-id*

Parameters

Parameter	Description	Value
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer in the range from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An RU supports interface-based VLAN configuration. After the central switch delivers a VLAN to an interface on an RU, you can run this command to view VLAN information about the interface.

Example

Display VLAN information about interfaces on the RU connected to XG0/0/6 of the central switch.

```
<HUAWEI> display remote-unit vlan connect-interface XGigabitEthernet0/0/6
----------------------------------------------------------------------
U:Up            D:Down           TG:Tagged           UT:Untagged
----------------------------------------------------------------------
ESN                :219801176601XXXXXXXX
Name                 :-
Device type         :S5731-L4P2HW-RUA
Remote unit ID      :16777215
Connect interface  :XGigabitEthernet0/0/6
----------------------------------------------------------------------
VlanID            Ports
----------------------------------------------------------------------
1                 UT:GE1(D)    GE2(D)    GE3(D)    GE4(D)
                    GE5(D)    GE6(U)    GE7(D)    GE8(D)
                    GE9(D)    UPLINK(U)
2                 UT:UPLINK(U)
3                 TG:GE1(D)    GE2(D)    GE3(D)    GE4(D)
                    UPLINK(U)
----------------------------------------------------------------------
```

Display information about interfaces in VLAN 3 on the RU connected to XG0/0/6 of the central switch.

```
<HUAWEI> display remote-unit vlan connect-interface XGigabitEthernet0/0/6 vlan 3
----------------------------------------------------------------------
U:Up          D:Down          TG:Tagged          UT:Untagged
----------------------------------------------------------------------
ESN              :219801176601XXXXXXXX
Name               :-
Device type        :S5731-L4P2HW-RUA
Remote unit ID     :16777215
Connect interface  :XGigabitEthernet0/0/6
----------------------------------------------------------------------
VlanID           Ports
----------------------------------------------------------------------
3               TG:GE1(D)    GE2(D)    GE3(D)    GE4(D)
                  UPLINK(U)
----------------------------------------------------------------------
```

Table 3-82 Description of the **display remote-unit vlan** command output

Item	Description
ESN	ESN of an RU.
Name	Alias of an RU. This field displays a hyphen (-) if an RU is not configured with an alias.
Device type	Device type of an RU.
Remote unit ID	ID of an RU. This field displays a hyphen (-) if an RU is not configured with an ID.
ConnectInterface	Interconnection interface.
VlanID	VLAN ID.
Ports	Interface of an RU. GE*n*: downlink interface on the RU. *n* indicates the interface number on the panel of the RU. UPLINK: uplink interface of the RU

3.4.23 display xldp statistics

Function

The **display xldp statistics** command displays statistics about XLDP packets sent and received by a switch.

Format

display xldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about XLDP packets sent and received by a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays statistics about XLDP packets on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To display the XLDP packet statistics within a specified period of time, you need to run the **reset xldp statistics** command to clear the existing statistics first, and then run the **display xldp statistics** command to view new statistics.

Example

Display statistics about XLDP packets sent and received by all interfaces on the central switch.

```
<HUAWEI> display xldp statistics
Statistics for GigabitEthernet0/0/1:
Transmitted frames total      : 27664
  Hello frames                : 27664
  Channel frames              : 0
Received frames total         : 0
  Hello frames                : 0
  Channel ACK frames          : 0
```

Table 3-83 Description of the **display xldp statistics** command output

Item	Description
Statistics for *x*	Statistics about XLDP packets received and sent by interface *x*.
Transmitted frames total	Number of sent XLDP packets.
Received frames total	Number of received XLDP packets.
Hello frames	Number of heartbeat packets.
Channel frames	Number of channel packets.
Channel ACK frames	Number of channel ACK packets.

3.4.24 isolate (remote-unit view)

Function

The **isolate enable** command enables interface isolation on RUs globally.

The **undo isolate enable** command disable interface isolation on RUs globally.

By default, interface isolation is disabled on RUs.

Format

isolate enable

undo isolate enable

Parameters

None

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an RU is delivered, its downlink interfaces are in the same broadcast domain and are not isolated by default. This allows users connected to the same RU to communicate with each other before being authenticated. To prevent this, you can configure interface isolation on RUs. To isolate downlink interfaces on all RUs, run the **isolate enable** command in the remote-unit view.

Follow-up Procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Configure interface isolation on all RUs.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] isolate enable
```

3.4.25 isolate (remote-unit N view)

Function

The **isolate enable** command enables port isolation on an RU.

The **isolate disable** command disables port isolation on an RU.

The **undo isolate** command restores the default configuration.

By default, port isolation is disabled on an RU.

Format

isolate {enable | disable }

undo isolate

Parameters

Parameter	Description	Value
enable	Enables port isolation.	-
disable	Disables port isolation.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an RU is delivered, its downlink interfaces are in the same broadcast domain and are not isolated by default. This allows users connected to the same RU to communicate with each other before being authenticated. To prevent this, you can configure port isolation on RUs. To isolate downlink interface on a single RU, run the **isolate enable** command in the view of the RU.

Precautions

The port isolation configuration specific to an RU has a higher priority than the global port isolation configuration.

Follow-up Procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Disable port isolation on an RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] isolate disable
```

3.4.26 led off (remote-unit view)

Function

The **led off** command turns off indicators on RUs.

The **undo led off** command restores the default status of indicators on RUs.

By default, indicators on RUs are turned on.

Format

led off [**time-range** *time-name*]

undo led off

Parameters

Parameter	Description	Value
time-range *time-name*	Specifies the name of a time range. If no time range is specified, the configuration is always valid.	The specified time range must exist.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When RUs are deployed in places such as hotels and dormitories, the blinking of indicators on the RUs may affect users' rest at night. You can run the **led off** command to turn off indicators on RUs to reduce the impact on users, for example, to turn off the indicators from 8:00 p.m. every day to 7:00 a.m. the next day.

Follow-up Procedure

After you run this command to turn on or off indicators on RUs, you need to run the **commit** command to deliver the configuration to make the configuration take effect.

Precautions

If this command is configured in both the remote-unit view and remote-unit N view, the configuration in the remote-unit N view takes effect.

Example

Turn off indicators on all RUs from 8:00 p.m. every day to 7:00 a.m. the next day.

```
<HUAWEI> system-view
[HUAWEI] time-range test 20:00 to 00:00 daily
[HUAWEI] time-range test 00:00 to 07:00 daily
[HUAWEI] remote-unit
[HUAWEI-remote-unit] led off time-range test
[HUAWEI-remote-unit] commit
```

3.4.27 led (remote-unit N view)

Function

The **led** command sets the time period during which indicators on an RU are turned on or off.

The **undo led off** command restore the default status of indicators on an RU.

By default, indicators on RUs are turned on.

Format

led { **on** | **off** [**time-range** *time-name*] }

undo led off

Parameters

Parameter	Description	Value
time-range *time-name*	Specifies the name of a time range. If no time range is specified, the configuration is always valid.	The specified time range must exist.

Parameter	Description	Value
on	Turns on RU indicators.	-
off	Turns off RU indicators.	-

Views

remote-unit view, remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When RUs are deployed in places such as hotels and dormitories, the blinking of indicators on the RUs may affect users' rest at night. You can run the **led** command to set the time period during which indicators on an RU are turned on or off to reduce the impact on users, for example, to turn off the indicators from 8:00 p.m. every day to 7:00 a.m. the next day.

Follow-up Procedure

After you run this command to configure the time period during which indicators on an RU are turned on or off, you need to run the **commit** command to deliver the configuration to make the configuration take effect.

Precautions

If this command is configured in both the remote-unit view and remote-unit N view, the configuration in the remote-unit N view takes effect.

Example

Turns off indicators on RU 0 from 8:00 p.m. every day to 7:00 a.m. the next day.

```
<HUAWEI> system-view
[HUAWEI] time-range test 20:00 to 00:00 daily
[HUAWEI] time-range test 00:00 to 07:00 daily
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] led off time-range test
[HUAWEI-remote-unit-0] commit
```

3.4.28 loopbacktest internal port

Function

The **loopbacktest internal port** configures an interface on an RU to perform an internal loopback test.

By default, internal loopback testing is not configured for an RU interface.

Format

loopbacktest internal port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the internal forwarding chip of an RU works properly.

Example

Configure internal loopback testing for interface 2 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] loopbacktest internal port 2
```

3.4.29 name

Function

The **name** command configures an alias for an RU.

The **undo name** command deletes the alias of an RU.

By default, no alias is configured for an RU.

Format

name *remote-unit-name*

undo name

Parameters

Parameter	Description	Value
remote-unit-name	Specifies the alias of an RU.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

If a central switch is connected to multiple RUs, you can configure an alias for each RU to facilitate management, since aliases are easier to remember than IDs. In addition, after specifying an alias for an RU, you can run the **remote-unit name** *remote-unit-name* command to enter the view of an RU by its alias directly.

Example

Set the alias of RU 0 to **access_1**.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] name access_1
```

3.4.30 negotiation auto port

Function

The **negotiation auto port** command configures an interface on an RU to work in auto-negotiation mode.

The **undo negotiation auto port** command configures an interface on an RU to work in non-auto-negotiation mode.

By default, an interface on an RU works in auto-negotiation mode.

Format

negotiation auto port { *portid1* [**to** *portid2*] } &<1-32>

undo negotiation auto port { *portid1* [**to** *portid2*] } &<1-32>

Parameters

Parameter	Description	Value
portid1 [**to** *portid2*]	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their operating parameters, including the duplex mode and rate. If the negotiation succeeds, the two interfaces work at the same operating parameters and the transmission capability can reach the maximum value supported by both ends.

Follow-up Procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Configure interface 8 on RU 0 to work in auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] negotiation auto port 8
```

3.4.31 poe anti-interference frequency

Function

The **poe anti-interference frequency** command configures the PoE anti-interference frequency for an RU.

The **undo poe anti-interference frequency** command restores the default configuration.

By default, the PoE anti-interference frequency of an RU is 50 Hz.

NOTE

Only PoE-capable RUs support this command.

Format

poe anti-interference frequency { **50** | **60** }

undo poe anti-interference frequency

Parameters

Parameter	Description	Value
50	Sets the anti-interference frequency to 50 Hz.	-
60	Sets the anti-interference frequency to 60 Hz.	-

Views

remote-unit view, remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The mains frequency varies in different countries and regions. Some are 60 Hz and some are 50 Hz. When RUs provide PoE power supply, incorrect grounding may occur. As a result, industrial frequency interference is coupled to network cables, resulting in abnormal PoE detection classification. You can run the **poe anti-interference frequency** command to modify the filtering algorithm on the PoE port to make the PoE anti-interference frequency become the same as the mains frequency, reducing the impact of the mains frequency on PD detection.

Follow-up Procedure

After configuring the PoE anti-interference frequency for an RU, you need to run the **commit** command to make the configuration take effect.

Precautions

If this command is configured in both the remote-unit view and remote-unit N view, the configuration in the remote-unit N view takes effect.

Example

Set the PoE anti-interference frequency of RU 0 to 60 Hz.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe anti-interference frequency 60
```

3.4.32 poe enable port

Function

The **poe enable port** command sets the power supply mode for an interface on an RU.

The **undo poe enable port** command restores the default power supply mode of a PoE interface on an RU.

By default, interfaces supporting the PoE++ mode provide power in that mode (also referred to as the **bt-inrush** mode). Interfaces that do not support the PoE++ mode provide power in **at-inrush** mode.

Format

poe { *at-inrush* | *af-inrush* } **enable port** *port-id*

undo poe { *at-inrush* | *af-inrush* } **enable port** *port-id*

NOTE

The following RUs work in PoE++ mode by default:

S5731-L4P2HW-RUA, S5731S-L4P2HW-RUA, S5731-L4P2S-RUA, S5731S-L4P2S-RUA, S5731-L4P2ST-RUA, S5731S-L4P2ST-RUA, S5731-L4P2HT-RUA, S5731S-L4P2HT-RUA

The following RUs work in PoE+ mode by default:

S5731-L8P2ST-RUA, S5731S-L8P2ST-RUA, S5731-L8P2HT-RUA, S5731S-L8P2HT-RUA, S5731-L8LP2ST-RUA

Parameters

Parameter	Description	Value
poe *at-inrush*	Sets an RU interface to work in PoE+ power supply mode.	-
poe *af-inrush*	Sets an RU interface to work in 802.3af power supply mode.	-
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To power the PDs requiring the standard power supply mode, you can run the **poe at-inrush enable** command. This command configures PoE interfaces to work in PoE+ power supply mode. Some non-IEEE standard PDs do not support high-current power supply, and instead only support low-current power supply. To power on such non-standard PDs, you can run the **poe af-inrush enable** command to configure PoE interfaces on RUs to work in 802.3af power supply mode.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Precautions

Switching the PoE power supply mode of an RU interface between the at-inrush and bt-inrush modes will cause PDs to be powered off.

Example

Set interface 1 on RU 0 to work in PoE+ power supply mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe at-inrush enable port 1
```

3.4.33 poe force-power port

Function

The **poe force-power port** command enables forcible PoE power supply for an interface on an RU.

The **undo poe force-power port** command disables forcible PoE power supply for an interface on an RU.

By default, forcible PoE power supply is disabled on interfaces of RUs.

Format

poe force-power port *port-id*

undo poe force-power port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the system power is sufficient, you can run this command to enable forcible power supply on RU interfaces connected to non-standard PDs when the RU, as the PSE, cannot detect the PDs.

Precautions

This command forcibly increases the power supplied by the RU. Ensure that the total power of PDs connected to the RU does not exceed the RU's available power.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Enable forcible power supply on interface 1 of RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe force-power port 1
```

3.4.34 poe power-on delay port

Function

The **poe power-on delay port** command sets the power supply delay for an interface on an RU.

The **undo poe power-on delay port** command restores the default power supply delay for an interface on an RU.

By default, the power supply delay for an interface on an RU is 0, which indicates no delay.

Format

poe power-on delay *delay-time* **port** *port-id*

undo poe power-on delay port *port-id*

Parameters

Parameter	Description	Value
delay-time	Specifies the power supply delay for an interface on an RU.	The value is an integer in the range from 1 to 60, in seconds. The default value is 0, indicating no delay.
port-id	Specifies the index of a downlink interface on an RU.	The value is an integer that ranges from 1 to 32. If some of the specified interface indexes are greater than the largest one on the RU, commands concerning these interfaces are not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

As the holding current of a non-standard PD is insufficient at the power-on moment, an RU assumes that the PD has been disconnected and powers it off.

To solve this problem, you can set the power supply delay for RU interfaces on the central switch. When the delay expires, the RUs detect the holding current to ensure that non-standard PDs can be properly powered on.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Precautions

If a PD is connected to an interface configured with a power supply delay, do not replace the PD within the delay. Otherwise, the new PD cannot work properly.

Example

Set the power supply delay to 5 seconds for interface 1 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] poe power-on delay 5 port 1
```

3.4.35 poe xldp-proxy

Function

The **poe xldp-proxy** command binds an optical interface to a MultiGE electrical interface on the central switch.

The **undo poe xldp-proxy** command restores the default configuration.

By default, no optical interface is bound to a MultiGE electrical interface.

Format

poe xldp-proxy interface multige *interface-number*

undo poe xldp-proxy

NOTE

Only the S5732-H48XUM2CC supports this command.

Parameters

Parameter	Description	Value
interface multige *interface-number*	Specifies the number of a MultiGE electrical interface.	-

Views

XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an S5732-H48XUM2CC functions as a central switch and connects to RUs using first-generation hybrid copper-fiber cables (that is, electrical interfaces are used for power supply and optical interfaces are used for communication), the central switch needs to provide PoE power for RUs through its electrical interfaces. To implement this, run the **poe xldp-proxy** command to bind an optical interface to an electrical interface, so that the optical interface can function as a proxy for the electrical interface to provide PoE power for its connected RU.

If this command is not configured, the central switch provides 60 W power for RUs by default.

Precautions

XLDP has been enabled on a 10GE optical interface. By default, XLDP is enabled.

Example

Bind XGE0/0/1 optical interface to MultiGE0/0/1 electrical interface.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] poe xldp-proxy interface MultiGE 0/0/1
```

3.4.36 port default vlan (remote-unit N view)

Function

The **port default vlan** command configures the default VLAN for downlink interfaces on an RU.

The **undo port default vlan** command restores the default setting.

By default, a downlink interface on an RU uses VLAN 1 as its default VLAN.

Format

port { *portid1* [**to** *portid2*] } &<1-32> **default vlan** *vlanid*

undo port { *portid1* [**to** *portid2*] } &<1-32> **default vlan**

Parameters

Parameter	Description	Value
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlanid	Specifies the default VLAN ID for the downlink interfaces on the RU.	The value is an integer in the range from 1 to 4094.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **port default vlan** command to configure a downlink interface on an RU as a hybrid interface and configure the default VLAN for the interface. As such, different VLANs can be configured for downlink interfaces of an RU to carry services of different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Run the **port uplink** { **tagged** | **untagged** } **vlan** *vlan-id1* command to configure the default VLAN of the downlink interfaces on an RU as an allowed VLAN for the RU's uplink interface.

Example

Configure VLAN 2 as the default VLAN for downlink interfaces 1 to 4 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port 1 to 4 default vlan 2
```

3.4.37 port uplink default vlan

Function

The **port uplink default vlan** command configures the default VLAN for the uplink interface on an RU.

The **undo port uplink default vlan** command restores the default setting.

By default, the uplink interface on an RU uses VLAN 1 as its default VLAN.

Format

port uplink default vlan *vlan-id*

undo port uplink default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID for the uplink interface on an RU.	The value is an integer in the range from 1 to 4094.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If terminals connected to an RU run the same service, they can reside in the same service VLAN. In this situation, you can run the **port uplink default vlan** command to configure the service VLAN as the default VLAN for the uplink interface on the RU.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Run the **port uplink untagged vlan** command to configure the default VLAN as an allowed VLAN in untagged mode for the uplink interface.

Example

Set VLAN 10 as the default VLAN for the uplink interface on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port uplink default vlan 10
```

3.4.38 port uplink vlan

Function

The **port uplink vlan** command configures allowed VLANs for the uplink interface on an RU.

The **undo port uplink vlan** command deletes the allowed VLAN configuration of the uplink interface on an RU.

By default, the uplink interface of an RU allows packets from VLAN 1 to pass through.

Format

port uplink { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port uplink { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the uplink interface to forward packets of the specified VLAN in tagged mode.	-
untagged	Configures the uplink interface to forward packets of the specified VLAN in untagged mode.	-
all	Deletes all allowed VLANs from the uplink interface on the RU.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a downlink interface of an RU is configured with a default VLAN, the uplink interface must allow packets of this VLAN to pass through, so that service traffic can be forwarded normally.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure the uplink interface on RU 0 to forward packets of VLAN 10 and VLAN 20 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port uplink tagged vlan  10 20
```

3.4.39 port vlan

Function

The **port vlan** command configures allowed VLANs for downlink interfaces on an RU.

The **undo port vlan** command deletes the allowed VLAN configuration of downlink interfaces on an RU.

By default, a downlink interface of an RU allows packets from VLAN 1 to pass through.

Format

port { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the downlink interfaces to forward packets of the specified VLANs in tagged mode.	-
untagged	Configures the downlink interfaces to forward packets of the specified VLANs in untagged mode.	-
all	Deletes all allowed VLANs from the downlink interfaces on the RU.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **port vlan** command to configure allowed VLANs for downlink interfaces on an RU, so that different service VLANs can be assigned to different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure downlink interfaces 1 to 4 on RU 0 to forward packets of VLAN 2 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] port 1 to 4 tagged vlan 2
```

3.4.40 reboot

Function

The **reboot** command resets an RU.

By default, an RU is not reset.

Format

reboot [**all**]

Parameters

Parameter	Description	Value
all	Resets all RUs.	This parameter is supported only in the remote-unit view.

Views

remote-unit view, remote-unit N view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- You can run this command to reset a faulty RU.
- If an RU fails to be upgraded and enters the cooldown period, you can run the **reboot** command to end the cooldown period.

Precautions

- An RU that has no interconnection interface bound cannot be reset.
- An RU that fails to be authenticated or is not authenticated cannot be reset.
- An RU that encounters a communication error will fail to be reset.
- RUs do not save their configurations. After an RU starts, it goes online on the central switch. After the RU is authenticated successfully, the central switch delivers configurations to the RU for them to take effect. For example, port isolation is required on an RU. After you restart the RU, its downlink interfaces can communicate with each other. The interfaces are isolated after the central switch authenticates the RU successfully and delivers the port isolation configuration.

Example

Reset a single RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] reboot
```

Reset all RUs.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] reboot all
```

3.4.41 remote-unit

Function

The **remote-unit** command displays the remote-unit view.

Format

remote-unit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enter the global RU view to perform global configurations for RUs.

Example

Enter the remote-unit view.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
```

3.4.42 remote-unit N

Function

The **remote-unit** command displays the view of an RU.

The **undo remote-unit** command deletes all configurations of an RU from the central switch.

Format

remote-unit { *id* | **connect-interface** *interface-type interface-number* | **name** *remote-unit-name* }

undo remote-unit *id*

Parameters

Parameter	Description	Value
id	ID of an RU, which is the RU index. The value range does not indicate the number of RUs that can be configured.	The value is an integer ranging from 0 to 16777215.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

System view, remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure or operate a single RU by running this command to enter the view of the specific RU.

Prerequisites

To enter the view of a specific RU by specifying the **name** parameter, ensure that you have configured an alias for this RU by running the **name** command. To enter the view of a specific RU by specifying the interconnection interface, ensure that you have bound an interconnection interface to this RU by running the **bind interface** command.

Example

Enter the view of an RU by specifying the ID of the RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
```

Enter the view of an RU by specifying the interconnection interface.

```
<HUAWEI> system-view
[HUAWEI] remote-unit connect-interface XGigabitEthernet 0/0/1
```

Enter the view of an RU by specifying the RU alias.

```
<HUAWEI> system-view
[HUAWEI] remote-unit name test
```

3.4.43 remote-unit protect-action error-down

Function

The **remote-unit protect-action error-down enable** command enables RU protection by setting interfaces to the Error-Down state.

The **remote-unit protect-action error-down disable** command disables RU protection.

By default, this function is enabled.

Format

remote-unit protect-action error-down { **disable** | **enable** }

undo remote-unit protect-action error-down disable

Parameters

Parameter	Description	Value
disable	Disables RU protection.	-

Parameter	Description	Value
enable	Enables RU protection by setting interfaces to the Error-Down state.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During RU deployment, a configuration error or link fault may occur (for details, see "Usage Guidelines" in **error-down auto-recovery cause remote-unit-link interval**). When the central switch detects the fault, it sets the interface connected to the RU to the Error-Down state.

Prerequisites

XLDP has been enabled on all interfaces of the central switch.

Precautions

The **undo remote-unit protect-action error-down disable** command is equivalent to the **remote-unit protect-action error-down enable** command.

Example

Enable RU protection by setting interfaces to the Error-Down state.

```
<HUAWEI> system-view
[HUAWEI] undo remote-unit protect-action error-down disable
```

3.4.44 remote-unit port default vlan

Function

The **remote-unit port default vlan** command configures the default VLAN for downlink interfaces on RUs in batches.

The **undo remote-unit port default vlan** command restores the default setting.

By default, a downlink interface on an RU uses VLAN 1 as its default VLAN.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> **default vlan** *vlanid*

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> **default vlan**

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* specifies the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlanid	Specifies the default VLAN ID for the downlink interfaces on the RUs.	The value is an integer in the range from 1 to 4094.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **remote-unit port default vlan** command to configure downlink interfaces on RUs as hybrid interfaces in batches and configure default VLANs for the interfaces, so that different VLANs can be configured to carry services of different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Run the **port uplink tagged vlan** command to configure the default VLAN of the downlink interfaces on the RUs as an allowed VLAN in tagged mode for the uplink interfaces on the RUs.

Example

Configure VLAN 2 as the default VLAN for downlink interfaces 1 to 4 on RUs 0 to 4.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] remote-unit 0 to 4 port 1 to 4 default vlan 2
```

3.4.45 remote-unit port uplink default vlan

Function

The **remote-unit port uplink default vlan** command configures the default VLAN for uplink interfaces on RUs in batches.

The **undo remote-unit port uplink default vlan** command restores the default setting.

By default, an uplink interface on an RU uses VLAN 1 as its default VLAN.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port uplink default vlan** *vlanid*

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port uplink default vlan**

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* indicates the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
vlanid	Specifies the default VLAN for uplink interfaces on the RUs.	The value is an integer in the range from 1 to 4094.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If terminals connected to multiple RUs carry the same service and use the same service VLAN, you can run the **remote-unit port uplink default vlan** command to configure the service VLAN as the default VLAN for the uplink interfaces on the RUs in batches.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Set VLAN 10 as the default VLAN for the uplink interfaces on RUs 0 to 4.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] remote-unit 0 to 4 port uplink default vlan 10
```

3.4.46 remote-unit port uplink vlan

Function

The **remote-unit port uplink vlan** command configures allowed VLANs for uplink interfaces on RUs in batches.

The **undo remote-unit port uplink vlan** command deletes the allowed VLAN configuration from uplink interfaces on RUs in batches.

By default, the uplink interface of an RU allows packets from VLAN 1 to pass through.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port uplink** { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8>] **port uplink** { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* indicates the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: *vlan-id1* specifies the first VLAN ID. **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the uplink interfaces to forward packets of the specified VLANs in tagged mode.	-
untagged	Configures the uplink interfaces to forward packets of the specified VLANs in untagged mode.	-
all	Deletes all allowed VLANs from the uplink interfaces on the specified RUs.	-

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **remote-unit port uplink vlan** command to configure allowed VLANs for uplink interfaces on RUs in batches so that different service VLANs can be assigned to different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure uplink interfaces on RUs 0 to 4 to forward packets of VLAN 2 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI] remote-unit 0 to 4 port uplink tagged vlan 2
```

3.4.47 remote-unit port vlan

Function

The **remote-unit port vlan** command configures allowed VLANs for downlink interfaces on RUs in batches.

The **undo remote-unit port vlan** command deletes the allowed VLAN configuration from downlink interfaces on RUs.

By default, a downlink interface of an RU allows packets from VLAN 1 to pass through.

Format

remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo remote-unit { *ruid1* [**to** *ruid2*] } &<1-8> **port** { *portid1* [**to** *portid2*] } &<1-32> { **tagged** | **untagged** } { **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
ruid1 [**to** *ruid2*]	Specifies IDs of RUs: *ruid1* indicates the ID of the first RU. **to** *ruid2* indicates the ID of the last RU. *ruid2* must be greater than or equal to *ruid1*.	*ruid1* is an integer that ranges from 0 to 16777215. *ruid2* is an integer that ranges from 0 to 16777215.
portid1 [**to** *portid2*]	Indicates numbers of downlink interfaces: *portid1* specifies the number of the first interface. **to** *portid2* specifies the number of the last interface. *portid2* must be greater than or equal to *portid1*.	*portid1* is an integer that ranges from 1 to 32. *portid2* is an integer that ranges from 1 to 32.
vlan-id1 [**to** *vlan-id2*]	Specifies allowed VLANs: ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*.	*vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094.
tagged	Configures the downlink interfaces to forward packets of the specified VLANs in tagged mode.	-
untagged	Configures the downlink interfaces to forward packets of the specified VLANs in untagged mode.	-
all	Deletes all allowed VLANs from downlink interfaces on the specified RUs.	-

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. You can run the **remote-unit port vlan** command to configure allowed VLANs for downlink interfaces on RUs in batches so that different service VLANs can be assigned to different terminals.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Prerequisites

You have run the **vlan mode manual** command to configure the manual VLAN mode for the RU.

Follow-up Procedure

After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Example

Configure downlink interfaces 1 to 4 on RUs 0 to 4 to forward packets of VLAN 2 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] remote-unit 0 to 4 port 1 to 4 tagged vlan 2
```

3.4.48 reset xldp statistics

Function

The **reset xldp statistics** command clears XLDP packet statistics on all interfaces or on a specified interface.

Format

reset xldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface where statistics need to be cleared. In the command: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, XLDP packet statistics on all interfaces are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To troubleshoot XLDP faults, you may need to view XLDP packet statistics within a certain period of time. In this case, you need to run this command to clear existing XLDP packet statistics, and run the **display xldp statistics** command to view new XLDP packet statistics.

Example

Clear XLDP packet statistics on all interfaces.

```
<HUAWEI> reset xldp statistics
```

Clear statistics about XLDP packets sent and received by GigabitEthernet0/0/1.

```
<HUAWEI> reset xldp statistics interface gigabitethernet 0/0/1
```

3.4.49 reset remote-unit commit result

Function

The **reset remote-unit commit result** command clears configuration delivery records of RUs.

Format

reset remote-unit commit result

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

RUs do not support web-based management and cannot have commands run on them for configuration. All RU configurations are delivered by the central switch. You can run the **display remote-unit commit result** command on the central switch to view configuration delivery results. To clear configuration delivery records, you can run the **reset remote-unit commit result** command.

After this command is run, configuration delivery records of RUs are cleared and cannot be restored.

Example

Clear configuration delivery records of RUs.

```
<HUAWEI> reset remote-unit commit result
```

3.4.50 reset remote-unit connect record

Function

The **reset remote-unit connect record** command clears onboarding and disconnection records of RUs.

Format

reset remote-unit connect record

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting onboarding and disconnection records of RUs, you can run this command to clear the existing records, and run the **display remote-unit connect record** command after a period of time to view new records.

Precautions

After this command is run, onboarding and disconnection records of RUs are cleared.

Example

Clear onboarding and disconnection records of RUs.

```
<HUAWEI> reset remote-unit connect record
```

3.4.51 reset remote-unit port statistics

Function

The **reset remote-unit port statistics** command clears the statistics on interfaces of an RU.

Format

reset remote-unit port [*port-id*] **statistics** [**connect-interface** *interface-type interface-number* | **name** *remote-unit-name*]

Parameters

Parameter	Description	Value
[*port-id*]	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34.
connect-interface *interface-type interface-number*	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.	-
name *remote-unit-name*	Specifies the alias of an RU.	The value must be an existing RU alias.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting traffic statistics on an RU interface within a period of time, run this command to clear the existing traffic statistics.

Example

Clear the statistics on all interfaces of an RU.

```
<HUAWEI> reset remote-unit port statistics
```

3.4.52 reset remote-unit upgrade record

Function

The **reset remote-unit upgrade record** command clears upgrade records of RUs.

Format

reset remote-unit upgrade record

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear upgrade records of RUs.

Example

Clear upgrade records of RUs.

```
<HUAWEI> reset remote-unit upgrade record
```

3.4.53 restart port

Function

The **restart port** command restarts an interface on an RU.

By default, no interface on an RU will be restarted.

Format

restart port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 34. If the specified number is greater than the largest interface number on the RU, the RU will not execute this command.

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface on an RU is faulty, you can run this command to restart the interface.

Precautions

- If an interface is disabled (in the shutdown state) before the restart, the interface is enabled automatically (in the undo shutdown state) after the restart.
- An RU that has no interconnection interface bound cannot be restarted.

Example

Restart interface 1 on the RU.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] restart port 1
```

3.4.54 shutdown port

Function

The **shutdown port** command shuts down an interface on an RU.

The **undo shutdown port** command enables an interface on an RU.

By default, interfaces on an RU are enabled.

Format

shutdown port { *port-id*1 [**to** *port-id*2] } &<1-32>

undo shutdown port { *port-id*1 [**to** *port-id*2] } &<1-32>

Parameters

Parameter	Description	Value
port-id1 [**to** *port-id2*]	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

When an interface on an RU is not connected to a cable or fiber, you can run the **shutdown** command to shut down the interface to prevent exceptions caused by interference.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Shut down interface 8 on RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] shutdown port 8
```

3.4.55 speed port

Function

The **speed port** command sets a fixed rate for an interface on an RU.

The **undo speed port** command restores the default rate of an interface on an RU.

By default, an interface on an RU works at the rate of 1000 Mbit/s.

Format

speed { **10** | **100** | **1000** } **port** { *portid1* [**to** *portid2*] } &<1-32>

undo speed { **10** | **100** | **1000** } **port** { *portid1* [**to** *portid2*] } &<1-32>

Parameters

Parameter	Description	Value
10	Sets the interface rate to 10 Mbit/s.	-
100	Sets the interface rate to 100 Mbit/s.	-
1000	Sets the interface rate to 1000 Mbit/s.	-
{ *portid1* [**to** *portid2*] }	Specifies the index of an interface on an RU.	The value is an integer that ranges from 1 to 32. If the specified interface index is larger than the largest one on the RU, the command is not issued to the RU.

Views

remote-unit N view

Default Level

3: Management level

Usage Guidelines

In non-auto negotiation mode, if interfaces on two connected devices work at different rates, the two devices cannot communicate with each other. In this case, you need to run this command to change the rates of the interfaces to be the same.

Prerequisites

The **undo negotiation auto port** command has been run to configure the interface to work in non-auto-negotiation mode.

Follow-up procedure

After running this command, run the **commit** command to make the configuration take effect.

Example

Configure interface 2 on RU 0 to work at the rate of 100 Mbit/s in non-auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] undo negotiation auto port 2
[HUAWEI-remote-unit-0] speed 100 port 2
```

3.4.56 upgrade cutoff-time

Function

The **upgrade cutoff-time** command sets the RU deployment end time. After this command is run, the firmware of the RUs that go online before the specified time will be automatically upgraded, and automatic RU firmware upgrade is disabled after the specified time.

The **undo upgrade cutoff-time** command deletes the configuration.

By default, no RU deployment end time is configured.

Format

upgrade cutoff-time *YYYY/MM/DD HH:MM:SS*

undo upgrade cutoff-time

Parameters

Parameter	Description	Value
YYYY/MM/DD	Specifies the date when RUs restart with firmware of the new version.	The value is in the 12-month format of YYYY/MM/DD. YYYY specifies the year, which ranges from 2000 to 2099. MM specifies the month, which ranges from 1 to 12. DD specifies the day, which ranges from 1 to 31.

Parameter	Description	Value
HH:MM:SS	Specifies the time when RUs restart with firmware of the new version.	The value is in the 24-hour format of HH:MM:SS. HH indicates hours, and its value is an integer ranging from 0 to 23; MM indicates minutes, and its value is an integer ranging from 0 to 59; SS indicates seconds, and its value is an integer ranging from 0 to 59.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applicable to the deployment scenario. The deployment process usually lasts for several days, during which RUs may be connected to the central switch successively. You can run this command to specify the deployment end time (based on the system time of the central switch), so that the firmware of all RUs is automatically upgraded when the specified time is reached. As such, you do not need to run the **upgrade right-now** command to upgrade RU firmware each time a new RU is connected to the central switch. After this command is run, the firmware of the RUs that go online before the specified time will be automatically upgraded, and automatic RU firmware upgrade is disabled after the specified time.

Precautions

After you run the **upgrade cutoff-time** command to configure the RU deployment time, other upgrade commands that have been configured are overwritten. That is, all RUs that go online before the specified deployment time will immediately restart with firmware of the new version.

Example

Set the time when RUs restart with firmware of the new version in the deployment scenario.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] upgrade cutoff-time 2022/05/31 00:00:00
```

3.4.57 upgrade force

Function

The **upgrade force** command configures forcible firmware upgrade for RUs.

By default, the function of upgrading RU firmware is disabled.

Format

upgrade { **app** | **bios** | **poe** } **force**

Parameters

Parameter	Description	Value
app	Specifies the APP firmware of RUs.	-
bios	Specifies the BIOS firmware of RUs.	-
poe	Specifies the PoE firmware of RUs.	-

Views

remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an RU fails to be upgraded, it enters the cooldown period and can be upgraded again only after the cooldown period ends. To upgrade the firmware of RUs in the cooldown period, you can run this command to configure forcible upgrade.

Precautions

During the BIOS firmware upgrade of RUs, do not power off or disconnect the RUs. Otherwise, the RUs cannot be started.

The **upgrade force** command upgrades firmware of an RU, regardless of whether the RU has the upgrade function enabled. After this command is run in the view of a single RU, the RU immediately restarts with firmware of the new version.

Example

Configure forcible APP firmware upgrade for RUs.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] upgrade app force
```

3.4.58 upgrade right-now

Function

The **upgrade right-now** command upgrades the firmware of RUs immediately.

By default, the function of upgrading RU firmware is disabled.

Format

upgrade right-now

Parameters

None

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the firmware version of an RU is different from that in the system software package or patch package of the central switch, the central switch does not automatically upgrade the firmware version of the RU. You can run the **upgrade right-now** command to upgrade the firmware of all RUs. After the **upgrade right-now** command is run, the system checks whether the firmware version of an RU is the same as that in the system software package or patch package of the central switch. If not, the RU immediately loads the firmware package of the new version and restarts with new firmware.

Prerequisites

RUs are online and in the normal state.

Precautions

- RUs will restart after loading firmware packages, resulting in service interruption. To prevent this issue, upgrade RUs at a proper time.
- Do not power off RUs during the upgrade. Otherwise, RUs may fail to start.
- Only the firmware of the RUs that go online before the command is run is upgraded. To upgrade RUs that go online later, you need to run this command again.
- This command is executed only once and is not recorded in Buildrun information. You can run the **display remote-unit upgrade information** command to check whether an RU is being upgraded.
- After you run the **upgrade right-now** command, RUs are upgraded immediately. The **upgrade cutoff-time** and **upgrade start-time** upgrade commands that have been configured are overwritten.

Example

Enable RU firmware upgrade.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] upgrade right-now
```

3.4.59 upgrade start-time

Function

The **upgrade start-time** command restarts RUs with firmware of the new version at a specified time.

The **undo upgrade start-time** command deletes the configuration.

By default, no time is set for RUs to restart with firmware of the new version.

Format

upgrade start-time *HH:MM:SS*

undo upgrade start-time

Parameters

Parameter	Description	Value
HH:MM:SS	Specifies the time when RUs restart with firmware of the new version.	The value is in the 24-hour format of HH:MM:SS. HH indicates hours, and its value is an integer ranging from 0 to 23; MM indicates minutes, and its value is an integer ranging from 0 to 59; SS indicates seconds, and its value is an integer ranging from 0 to 59.

Views

remote-unit view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The firmware upgrade of an RU consists of two steps:

1. The RU loads firmware of the new version. In this step, the central switch sends the firmware package of the new version to the RU.
2. The RU restarts to make firmware of the new version take effect.

You can run the **upgrade start-time** command to configure RUs to restart with firmware of the new version at a specified time. This command configures the restart time in step 2.

Precautions

During the BIOS firmware upgrade of RUs, do not power off or disconnect the RUs. Otherwise, the RUs cannot be started.

After you run the **upgrade start-time** command to configure RUs to restart with firmware of the new version at a specified time, other upgrade commands that have been configured are overwritten. That is, RUs will restart with firmware of the new version at the time specified by the **upgrade start-time** command.

Example

Configure RUs to restart with firmware of the new version at midnight.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] upgrade start-time 00:00:00
```

3.4.60 vlan mode

Function

The **vlan mode** command configures the VLAN mode for an RU.

The **undo vlan mode** command restores the default VLAN mode for an RU.

By default, an RU uses the transparent VLAN mode.

Format

vlan mode { **manual** | **transparent** }

undo vlan mode

Parameters

Parameter	Description	Value
manual	Configures the manual VLAN mode. In manual mode, an interface uses VLAN 1 as its default VLAN and joins VLAN 1 in untagged mode.	-
transparent	Configures the transparent VLAN mode.	-

Views

remote-unit view, remote-unit N view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RU can connect to different types of terminals using its downlink interfaces and distinguish terminal services by joining its downlink interfaces to different VLANs. By default, all interfaces on an RU work in transparent VLAN mode. That is, the RU does not change the VLAN IDs of received packets. If services of downlink terminals connected to an RU need to be divided based on VLANs, you need to run the **vlan mode manual** command to configure the RU to work in manual VLAN mode, and then configure default and allowed VLANs for interfaces on the RU.

An RU saves the VLAN configuration delivered by the central switch to it in its flash memory and forwards traffic based on this VLAN configuration after being powered on. After the RU goes online on the central switch, the central switch synchronizes the latest VLAN configuration to the RU's flash memory.

Follow-up Procedure

- Configure default and allowed VLANs for interfaces on the RU.
- After you run the commands for configuring the VLAN mode for an RU and VLANs for RU interfaces, run the **commit** command to deliver the VLAN configuration to the RU or bring the RU offline and then online again for the configuration to take effect.

Precautions

You can configure the VLAN mode of an RU in the remote-unit view or remote-unit N view. If the VLAN mode is configured in both views, the configuration in the remote-unit N view takes effect. If no VLAN mode is configured in the remote-unit N view, the configuration in the remote-unit view takes effect.

Example

Configure all connected RUs to work in manual VLAN mode.

```
<HUAWEI> system-view
[HUAWEI] remote-unit
[HUAWEI-remote-unit] vlan mode manual
```

Configure the manual VLAN mode for the RU 0.

```
<HUAWEI> system-view
[HUAWEI] remote-unit 0
[HUAWEI-remote-unit-0] vlan mode manual
```

3.4.61 xldp enable (interface view)

Function

The **xldp enable** command enables XLDP on an interface.

The **xldp disable** command disables XLDP on an interface.

The **undo xldp disable** command restores the default configuration.

After XLDP is enabled in the system view, all interfaces are enabled with XLDP by default.

Format

xldp enable

xldp disable

undo xldp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After XLDP is enabled on an interface, the interface exchanges XLDP packets with XLDP-enabled neighbors. The interface receives status information from the neighbors and sends the local status information to the neighbors. An intelligent simplified campus network runs based on the XLDP protocol.

Prerequisites

XLDP has been enabled globally using the **xldp enable** in the system view.

Precautions

- XLDP can be enabled in the system view and the interface view.
  - After XLDP is enabled in the system view, all interfaces are enabled with XLDP.
  - After XLDP is disabled in the system view, all XLDP settings are restored to the default settings except the setting of XLDP trap. Therefore, XLDP is also disabled on all interfaces.
  - An interface can send and receive XLDP packets only after XLDP is enabled in both the system view and the interface view.
  - After XLDP is disabled globally, the commands for enabling and disabling XLDP on an interface do not take effect.
  - If some interfaces need to have XLDP enabled but some need to have XLDP disabled, you can globally enable XLDP and run the **xldp disable** command in the interface view to disable XLDP for the required interfaces. To re-enable XLDP on these interfaces, run the **xldp enable** command in the views of these interfaces.
- The **xldp enable (interface view)** command can be run only on an Ethernet interface, regardless of whether it works at Layer 2 or Layer 3 mode, and cannot be run on a logical interface such as a VLANIF or Eth-Trunk interface.

For an Eth-Trunk interface, XLDP can only be enabled on its member interfaces. XLDP-enabled interfaces and XLDP-disabled interfaces can be added to the same Eth-Trunk.

- If a large number of XLDP packets are sent to attack an interface, disable XLDP on the interface so that the interface does not send XLDP packets to the CPU for processing.

Example

Disable XLDP on the Ethernet interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] xldp disable
```

3.4.62 xldp enable (system view)

Function

The **xldp enable** command enables XLDP globally.

The **xldp disable** command disables XLDP globally.

The **undo xldp disable** command restores the default global XLDP configuration.

By default, XLDP is enabled globally.

Format

xldp enable

xldp disable

undo xldp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the status of Layer 2 links connecting the central switch and RUs for analyzing the network topology, you need to run this command to enable XLDP.

Configuration Impact

After XLDP is enabled globally, the device sends its own status information to XLDP-enabled neighbors and receives the status information from the neighbors.

Precautions

After global XLDP is disabled, the XLDP configuration is deleted from all interfaces.

XLDP can be enabled in the system view and the interface view.

- After XLDP is enabled in the system view, all interfaces are enabled with XLDP.
- After XLDP is disabled in the system view, all XLDP settings are restored to the default settings except the setting of XLDP trap. Therefore, XLDP is also disabled on all interfaces.
- An interface can send and receive XLDP packets only after XLDP is enabled in both the system view and the interface view.
- After XLDP is disabled globally, the commands for enabling and disabling XLDP on an interface do not take effect.

Example

Enable XLDP globally.

```
<HUAWEI> system-view
[HUAWEI] xldp enable
```

Disable XLDP globally.

```
<HUAWEI> system-view
[HUAWEI] xldp disable
```

3.5 SVF Configuration Commands

3.5.1 Command Support

NOTE

- When the parent version is earlier than V200R011C10, the AS version must be the same as the parent version. Otherwise, this AS cannot go online. For example, if the parent version is V200R010C00, the AS version must also be V200R010C00. When the parent version is V200R011C10 or later, the parent version and AS version can be different, but the parent version must be higher than or the same as the AS version and the AS version must also be V200R011C10 or later. **Table1** describes the version mapping between parent and AS. **Table2** describes supported Parent and AS switch models in different software versions.
- APs must use the software version matching that of the parent. For details, see "WLAN Service Configuration - Licensing Requirements and Limitations for WLAN" in the *Configuration Guide - WLAN-AC*.
- To check AP device types supported by the parent by default, run the **display ap-type all** command on the parent. The S6735-S, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720S-S,S6730-S, or S6730S-S cannot manage APs when acting as a parent.

Table 3-84 Version mapping between parent and AS

Parent Version	Required AS Version
V200R007C00	V200R007C00
V200R008C00	V200R008C00
V200R009C00	V200R009C00
V200R010C00	V200R010C00
V200R011C00	V200R011C00
V200R011C10	V200R011C10
V200R012C00	V200R011C10, V200R012C00
V200R013C00	V200R011C10, V200R012C00, V200R013C00
V200R019C00	V200R012C00, V200R013C00, V200R019C00
V200R019C10	V200R012C00, V200R013C00, V200R019C00, V200R019C10
V200R020C00	V200R013C00, V200R019C00, V200R019C10, V200R020C00
V200R020C10	V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10
V200R020C30	V200R013C00, V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30
V200R021C00	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30, V200R021C00
V200R021C01	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01
V200R021C10	V200R019C00, V200R019C10, V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10
V200R022C00	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00
V200R022C10	V200R020C00, V200R020C10, V200R020C30, V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10
V200R023C00	V200R021C00, V200R021C01, V200R021C10, V200R022C00, V200R022C10, V200R023C00

Table 3-85 Supported parent and AS switch models

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R007C00	• S12708, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI	S2750-EI, S5700-LI, S5700S-LI, S5720-EI
V200R008C00	• S12704, S12708, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI	• S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-SI, S5720S-SI, S5720-EI • E600
V200R009C00	• S12704, S12708, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI, S6720-EI, S6720S-EI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-SI, S5720S-SI, S5720-EI, S6720-EI, S6720S-EI • E600
V200R010C00	• S12704, S12708, S12710, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S5720-HI, S6720-EI, S6720S-EI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720-EI, S6720-EI, S6720S-EI • E600 • S600-E
V200R011C00	S5720-HI, S6720-EI, S6720S-EI	• S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720-EI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • E600 • S600-E
V200R011C10	• S12704, S12708, S12710, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S9303, S9306, S9310, S9312 • S5720-HI, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720-EI, S5730-SI, S5730S-EI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • E600 • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R012C00	• S12704, S12708, S12710, S12712 • S7703, S7706, S7712 • S9703, S9706, S9712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI	• S2720-EI, S2750-EI, S5700-LI, S5700S-LI, S5710-X-LI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E
V200R013C00	• S12704, S12708, S12710, S12712 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9703, S9706, S9712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI	• S2720-EI, S5720-LI, S5720S-LI, S5720-SI, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E
V200R019C00	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI, S6730-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5735-L, S5735S-L, S5735S-L-M, S5720S-LI, S5720-SI, S5735-S, S5735S-S, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E
V200R019C10	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5720-HI, S5730-HI, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720-HI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5735-L, S5735S-L, S5735S-L-M, S5720S-LI, S5720-SI, S5735-S, S5735S-S, S5735-S-I, S5720S-SI, S5720I-SI, S5720-EI, S5730-SI, S5730S-EI, S5730-HI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6720-LI, S6720S-LI, S6720-SI, S6720S-SI • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R020C00	- S12704, S12708, S12710, S12712 - S12700E-4, S12700E-8, S12700E-12 - S7703, S7703 PoE, S7706, S7706 PoE, S7712 - S9303, S9306, S9310, S9312 - S5731-H, S5731S-H, S5732-H, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	- S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S - S600-E
V200R020C10	- S12704, S12708, S12710, S12712 - S12700E-4, S12700E-8, S12700E-12 - S7703, S7703 PoE, S7706, S7706 PoE, S7712 - S9303, S9306, S9310, S9312 - S5731-H, S5731S-H, S5732-H, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	- S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S - S600-E
V200R020C30	None	S5735-S8P2X-IA200H1, S5736-S48S4X-A, S5736-S48S4X-D
V200R021C00	- S12704, S12708, S12710, S12712 - S12700E-4, S12700E-8, S12700E-12 - S7703, S7703 PoE, S7706, S7706 PoE, S7712 - S9303, S9306, S9310, S9312 - S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	- S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S - S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R021C01	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E
V200R021C10	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E
V200R022C00	• S12704, S12708, S12710, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S,S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S600-E

Software Version	Supported Parent Switch Models	Supported AS Switch Models
V200R022C10	• S12704, S12708, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S • S5531-H	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S5531-H, S5531-S
V200R023C00	• S12704, S12708, S12712 • S12700E-4, S12700E-8, S12700E-12 • S7703, S7703 PoE, S7706, S7706 PoE, S7712 • S9303, S9306, S9310, S9312 • S5731-H, S5731S-H, S5732-H, S6720S-S,S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S • S5531-H	• S2720-EI, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S • S5531-H, S5531-S

3.5.2 acl ipv6 number (AS administrator profile view)

Function

The **acl ipv6 number** command configures an IPv6 ACL rule number in an AS administrator profile.

The **undo acl ipv6 number** command deletes an IPv6 ACL rule number in an AS administrator profile.

By default, no IPv6 ACL rule number is configured in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

acl ipv6 number { *acl-number* } &<1-16>

undo acl ipv6 number { *acl-number* } &<1-16>

Parameters

Parameter	Description	Value
acl-number	Specifies an ACL rule number.	The value is an integer in the range from 3000 to 3999.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS administrator profile, you can run the **acl ipv6 number** command to configure an IPv6 ACL rule number for an AS in the AS administrator profile. After the profile is bound to an AS, the following configuration is generated on the AS:

```
#
acl ipv6 number acl-number
 rule xxx
#
```

Precautions

- In SVF, only 5-tuple information (source IP address, destination IP address, source port, destination port, and protocol type) can be specified in ACL rules.
- The IPv6 ACL used in an AS administrator profile must have been created in the system view, and rules have been configured in the ACL view.
- A maximum of 64 IPv6 ACLs can be configured in an AS administrator profile, and a maximum of 1024 rules can be created in an ACL. The total number of IPv4 and IPv6 ACL rules cannot exceed 4096.

Example

Configure an IPv6 ACL rule number in an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] acl ipv6 number 3000 3002 3010 3011 3012
```

3.5.3 acl number (AS administrator profile view)

Function

The **acl number** command configures an ACL rule number in an AS administrator profile.

The **undo acl number** command deletes an ACL rule number in an AS administrator profile.

By default, no ACL rule number is configured in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

acl number { *acl-number* } &<1-16>

undo acl number { *acl-number* } &<1-16>

Parameters

Parameter	Description	Value
acl-number	Specifies an ACL rule number.	The value is an integer in the range from 3000 to 3900.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS administrator profile, you can run the **acl number** command to configure an ACL rule number for an AS in the AS administrator profile. After the profile is bound to an AS, the following configuration is generated on the AS:

```
#
acl number acl-number
 rule xxx
#
```

Precautions

- In SVF, only 5-tuple information (source IP address, destination IP address, source port, destination port, and protocol type) can be specified in ACL rules.
- The ACL used in an AS administrator profile must have been created in the system view, and rules have been configured in the ACL view.
- A maximum of 64 ACLs can be configured in an AS administrator profile, and a maximum of 1024 rules can be created in an ACL. The total number of IPv4 and IPv6 ACL rules cannot exceed 4096.

Example

Configure an ACL rule number in an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] acl number 3000 3002 3010 3011 3012
```

3.5.4 arp anti-attack check user-bind enable (network enhanced profile view)

Function

The **arp anti-attack check user-bind enable** command configures dynamic ARP inspection (DAI) in a network enhanced profile.

The **undo arp anti-attack check user-bind enable** command disables DAI in a network enhanced profile.

By default, DAI is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

Parameters

None

Views

Network enhanced profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a network enhanced profile, you can configure DAI in the profile. After the profile is bound to an AS port, DAI is automatically enabled on the port. The following configuration is generated on the AS port:

```
#
 arp anti-attack rate-limit enable
 arp anti-attack rate-limit packet 5 interval 1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
```

You can configure DAI to prevent Man in The Middle (MITM) attacks and theft on authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the

ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device allows the packet to pass through. If the ARP packet does not match any binding entry, the device discards the packet.

Prerequisites

DHCP snooping has been enabled in the network enhanced profile using the **dhcp snooping enable** command.

Example

Enable DAI in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] dhcp snooping enable
[HUAWEI-um-net-enhanced-profile_1] arp anti-attack check user-bind enable
```

3.5.5 as-admin-profile (AS group view)

Function

The **as-admin-profile** command binds an AS administrator profile to an AS group.

The **undo as-admin-profile** command unbinds an AS administrator profile from an AS group.

By default, no AS administrator profile is bound to an AS group.

NOTE

This command can only be executed on a parent switch.

Format

as-admin-profile *profile-name*

undo as-admin-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AS administrator profile.	The value must have an existing AS administrator profile name.

Views

AS group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind an AS administrator profile to an AS group to deliver the configurations in the profile to all the member ASs in the AS group.

Prerequisites

The AS administrator profile has been created.

Precautions

AS groups can only be bound to AS administrator profiles. Each AS group can be bound to only one AS administrator profile.

Example

Bind an AS administrator profile to an AS group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] quit
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as-admin-profile profile_1
```

3.5.6 as-admin-profile name

Function

The **as-admin-profile name** command creates an AS administrator profile.

The **undo as-admin-profile name** command deletes an AS administrator profile.

By default, no AS administrator profile is configured.

NOTE

This command can only be executed on a parent switch.

Format

as-admin-profile name *profile-name*

undo as-admin-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AS administrator profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an AS administrator profile, you can configure AS administrator information and the rate limit for outgoing ARP and DHCP packets on an uplink fabric port.

Precautions

You can create a maximum of 16 AS administrator profiles.

Example

Create an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
```

3.5.7 as authentication configuration revert disable

Function

The **as authentication configuration revert disable** command enables the function of retaining the authentication configuration after an AS goes offline.

The **undo as authentication configuration revert disable** command disables the function of retaining the authentication configuration after an AS goes offline.

By default, the authentication configuration is cleared after an AS goes offline.

NOTE

This command can only be executed on a parent switch.

Format

as authentication configuration revert disable

undo as authentication configuration revert disable

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

When an AS goes offline, it automatically clears its authentication configuration to ensure connectivity in the local area network (LAN) connected to it in case of an AS authentication failure. However, clearing the authentication configuration when the AS goes offline will lengthen the time taken for the AS to go online again. If the AS is not connected to a LAN or if the time taken for the AS to go online again needs to be shortened, enable the function of retaining the authentication configuration after the AS goes offline on the parent to shorten the time taken for the AS to go online again.

Example

Enable the function of retaining the authentication configuration after an AS goes offline.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as authentication configuration revert disable
```

3.5.8 as-auth

Function

The **as-auth** command displays the AS authentication view.

NOTE

This command can only be executed on a parent switch.

Format

as-auth

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After entering the AS authentication view, you can configure the AS authentication mode, blacklist, and whitelist.

Example

Enter the AS authentication view.

```
<HUAWEI> system-view
[HUAWEI] as-auth
```

3.5.9 as-group name

Function

The **as-group name** command creates an AS group or displays the AS group view.

The **undo as-group name** command deletes an AS group.

By default, no AS group is created.

NOTE

This command can only be executed on a parent switch.

Format

as-group name *group-name*

undo as-group name *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of an AS group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An AS group contains one or more ASs, which facilitates AS batch configuration.

Follow-up Procedure

Run the **as name** *as-name* or **as name-include** *string* command to add ASs to an AS group.

Precautions

You can create a maximum of 16 AS groups.

AS groups can only be bound to AS administrator profiles. Each AS group can be bound to only one AS administrator profile.

Example

Create an AS group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-group name group_1
```

3.5.10 as access dtls psk

Function

The **as access dtls psk** command configures a pre-shared key for Datagram Transport Layer Security (DTLS) encryption on an access switch (AS).

The **undo as access dtls psk** command deletes a pre-shared key used for DTLS encryption.

The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

This command can only be executed on an AS.

Format

as access dtls psk *psk-value*

undo as access dtls psk

Parameters

Parameter	Description	Value
psk-value	Specifies a pre-shared key.	The value is a string of 6 to 32 case-sensitive characters without spaces. The pre-shared key must be in plain text and contain at least two of the following: letters, digits, and special characters.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To encrypt CAPWAP-encapsulated packets between the parent and an AS, configure the same pre-shared key on the parent and AS. You can run the **as access dtls psk** command to configure a pre-shared key for DTLS encryption on the AS.

Precautions

- The default pre-shared key has security risks. You are advised to change the pre-shared key.
- After an AS has connected to an SVF system, configuring or deleting the pre-shared key for DTLS encryption is not allowed on the AS.

Example

Set the pre-shared key for DTLS encryption to **test@1234**.

```
<HUAWEI> as access dtls psk test@1234
```

3.5.11 as access manage-mac

Function

The **as access manage-mac** command configures the management MAC address of an AS.

The **undo as access manage-mac** command restores the default management MAC address of an AS.

By default, an AS uses the system MAC address as the management MAC address.

NOTE

This command can only be executed on an AS.

Format

as access manage-mac *mac-address*

undo as access manage-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the management MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a Super Virtual Fabric (SVF) system, each AS has a unique management MAC address to identify itself. By default, an AS uses its system MAC address as the management MAC address to connect to an SVF system. When the management MAC address of an AS conflicts with that of another AS, you can run the **as access manage-mac** command to change the management MAC address so as to prevent MAC address conflicts.

Precautions

- Use of this command is not recommended when no MAC address conflict occurs, as an improper management MAC address may affect service operations.
- This command can be used only before an AS connects an SVF system. If an AS has connected to an SVF system, use of this command is not allowed.
- Before using this command to change the management MAC address of an AS, you must run the **undo as access manage-mac** command to delete the existing management MAC address.

Example

Configure the management MAC address of an AS.

```
<HUAWEI> as access manage-mac 00e0-fc91-52a0
```

3.5.12 as auto-replace enable

Function

The **as auto-replace enable** command enables AS automatic replacement.

The **undo as auto-replace enable** command disables AS automatic replacement.

By default, AS automatic replacement is disabled.

NOTE

This command can only be executed on a parent switch.

Format

as auto-replace enable

undo as auto-replace enable

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an SVF system, each AS is identified by its MAC address by default. When a new device is used to replace an AS, the SVF system considers the new device as a new AS because their MAC addresses are different. As a result, the new AS does not inherit services from the previous AS.

You can enable AS automatic replacement to solve this problem. When an AS is replaced by a new device connected to the same fabric port, the SVF system replaces the AS MAC address with the MAC address of the new device in the configuration. Consequently, the new device can inherit services from the AS.

Precautions

- An AS can only be replaced by a device of the same model. If the new device is a different model, the SVF system considers it as a new AS, which then cannot inherit services from the previous AS.
- Only a standalone AS can be replaced. If an AS is a stack, it cannot be replaced.
- AS automatic replacement is not supported when an AS connects to the parent through a network.
- To ensure that a replacement AS can be successfully authenticated, run the **auth-mode none** command to set the AS authentication mode to none, or run the **whitelist mac-address** command to add the management MAC address of the replacement AS to the whitelist. If the replacement AS has no management MAC address configured, its system MAC address is used as the management MAC address.

Example

Enable AS automatic replacement.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as auto-replace enable
```

3.5.13 as-mode disable

Function

The **as-mode disable** command changes the switch working mode to the parent mode.

The **undo as-mode disable** command restores the switch working mode to the AS mode.

Swich models supporting this command and the default working mode of them are as follows:

- S5731-H (excluding S5731-H24HB4XZ, S5731-H48HB4XZ), S5731S-H (excluding S5731S-H24HB4XZ-A, S5731S-H48HB4XZ-A), S5732-H24S6Q, S5732-H48S6Q, S6730S-H, S6730-H: Parent mode
- S5531-H48HB4XZ, S5731-H24HB4XZ, S5731-H48HB4XZ, S5731S-H24HB4XZ-A, S5731S-H48HB4XZ-A, S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S6730-S, S6730S-S, S6720-SI, S6720S-S, S6720S-SI, S6720-EI, S6720S-EI, S6735-S: AS mode

Format

as-mode disable

undo as-mode disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Switch models supporting this command can function as the parent or AS in an SVF system.

Precautions

- After the working mode of a switch is changed, the switch restarts for the new working mode to take effect, and does not use any configuration file at the next startup. As such, the switch restarts without any configuration file. In this case, you are advised to back up the configuration file of the switch before it restarts.
- By default, the following switches work in AS mode: S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC. To enable these switches to

automatically change the working mode to parent during unconfigured device deployment, run the **option 148 ascii** *ascii-string* command to configure Option 148 of the DHCP server. The format of *ascii-string* is svfmode=uc.

Example

Change the switch working mode to the parent mode.

```
<HUAWEI> system-view
[HUAWEI] as-mode disable
Warning: Switching the AS mode will clear current configuration and reboot the system. Continue? [Y/N]:y
```

3.5.14 as all (AS group view)

Function

The **as all** command adds all ASs to an AS group.

The **undo as all** command deletes all ASs from an AS group.

By default, no AS is added to an AS group.

NOTE

This command can only be executed on a parent switch.

Format

as all

undo as all

Parameters

None

Views

AS group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS group, you need to add the ASs that require the same configuration to the AS group. This command adds all ASs to the same AS group.

Precautions

An AS can be added to only one AS group. For example, if you run the **as all** command in group_1 and then in group_2, the system displays a message, saying that the ASs need to be deleted from the previous AS group before they can be added to the new AS group.

Example

Add all ASs to the AS group group_1.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as all
```

3.5.15 as name (AS group view)

Function

The **as name** command adds an AS with a specified name to an AS group.

The **as name-include** command adds an AS of which the name contains a specified string to an AS group.

The **undo as name** command deletes an AS with a specified name from an AS group.

The **undo as name-include** command deletes an AS of which the name contains a specified string from an AS group.

By default, no AS is added to an AS group.

NOTE

This command can only be executed on a parent switch.

Format

as name *as-name*

as name-include *string*

undo as name *as-name*

undo as name-include *string*

Parameters

Parameter	Description	Value
as-name	Specifies the name of an AS.	The value must have an existing AS name.
string	Specifies the string contained in an AS name.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

AS group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS group, add the ASs that need to be configured in a batch to the AS group. You can only add created ASs to an AS group.

Precautions

An AS can be added to only one AS group.

After an AS is added to an AS group, to change the AS group, run the **as name** command to add the AS to another AS group.

Example

Add the AS **as_1** to the AS group **group_1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as name as_1
```

3.5.16 as name interface (port group view)

Function

The **as name interface** command adds ports on the AS with a specified name to a port group.

The **as name-include interface** command adds ports on the AS of which the name contains a specified string to a port group.

The **undo as name interface** command deletes ports on the AS with a specified name from a port group.

The **undo as name-include interface** command deletes ports on the AS of which the name contains a specified string from a port group.

By default, no ports on an AS are added to a port group.

NOTE

This command can only be executed on a parent switch.

Format

as name *as-name* **interface** { { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **all** }

as name-include *string* **interface all**

undo as name *as-name* **interface** { { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **all** }

undo as name-include *string* **interface all**

Parameters

Parameter	Description	Value
as-name	Specifies the name of an AS.	The value must have an existing AS name.
string	Specifies the string contained in an AS name.	The value is a string of 1 to 31 case-insensitive characters without spaces.
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of AS interfaces. • *interface-type* specifies the interface type. • *interface-number1* specifies the first interface number. • *interface-number2* specifies the last interface number.	The following ports cannot be added to a port group: • Fabric port • Eth-Trunk member interface • Uplink port on an AS. You can run the **display port connection-type access all** command to view all downlink ports of the device. The ports that are not displayed in the command output are uplink ports. Note that an uplink port still cannot be added to a port group after it is configured as a downlink port using the **port connection-type access** command.
all	Indicates all downlink ports on an AS.	-

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a port group, add the AS ports that need to be configured in a batch to the port group.

Precautions

A port can be added to only one port group.

After ports on an AS are added to a port group, to change the port group, run the **as name interface** command to add the ports to another port group.

A fabric port in a port group takes effect only for a network QoS profile but not for any network basic profile, network enhanced profile, traffic policy profile, or user access profile.

Example

Add ports on the AS **as1** to the port group **group_1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] as name as1 interface gigabitethernet 0/0/1 to 0/0/5
```

3.5.17 as name (uni-mng view)

Function

The **as name** command configures an AS name or displays the AS view.

The **undo as name** command deletes an AS.

By default, system default name-device MAC address is used as the AS name, for example, **huawei-000a-123d-2200**.

NOTE

This command can only be executed on a parent switch.

Format

as name *as-name* [**model** *as-model* **mac-address** *mac-address*]

undo as { **all** | **name** *as-name* }

Parameters

Parameter	Description	Value
as-name	Specifies the name of an AS.	The value is a string of 1 to 31 case-insensitive characters without spaces.
model *as-model*	Specifies the device model of an AS.	The value is of enumerated type. You can enter a question mark (?) and select a value from the displayed value range.
mac-address *mac-address*	Specifies the management MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Parameter	Description	Value
all	Deletes all ASs.	-

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure a name for an AS and use the name to uniquely identify the AS. This configuration facilitates AS identification and management.

If no AS name is configured, system default name-device MAC address is used as the AS name after the AS connects to an SVF system.

You can change the name of an AS that has connected to an SVF system when the following conditions are met:

1. The AS is not bound to any service profile.
2. The AS is not added to any AS group.
3. Ports of the AS are not added to any port group.

Precautions

- If the **model** *as-model* **mac-address** *mac-address* parameter is not specified, the AS view is displayed. You can enter the view of an AS only when the AS has been created.
- If an AS has connected to an SVF system, the AS leaves the SVF system and restarts after being deleted.
- If the message "A port instance in the AS (xxx) has been added to the PM. Please delete the configuration first." is displayed when you delete an AS, run the **undo binding** command in the PM statistics task view to delete the configuration. This command ensures that the AS can be deleted successfully.

Example

Configure an AS name.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1 model S5720-28P-LI-AC mac-address xxxx-xxxx-xxxx
```

3.5.18 as reset

Function

The **as reset** command restarts an AS.

NOTE

This command can only be executed on a parent switch.

Format

as reset { **all** | **name** *as-name* }

Parameters

Parameter	Description	Value
all	Restarts all ASs.	-
name *as-name*	Restarts an AS with a specified name.	The value must have an existing AS name.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

When an AS is upgraded or working abnormally, you can restart the AS.

Example

Restart the AS **as1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as reset name as1
```

3.5.19 as service-vlan igmp-snooping

Function

The **as service-vlan igmp-snooping** command enables IGMP snooping for a service VLAN on an AS.

The **undo as service-vlan igmp-snooping** command disables IGMP snooping for a service VLAN on an AS.

By default, IGMP snooping is disabled for service VLANs on an AS.

NOTE

This command can only be executed on a parent switch.

Format

as service-vlan igmp-snooping { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

undo as service-vlan igmp-snooping { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies range of service VLANs: - *vlan-id1* specifies the start VLAN ID. - *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. - If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is a service VLAN ID.	The *vlan-id1* and *vlan-id2* are integers ranging from 1 to 4094.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, IGMP snooping is disabled for service VLANs on an AS. If IGMP snooping needs to be enabled on an AS, run the **as service-vlan igmp-snooping** command to deliver the configuration to the AS. After the configuration is delivered successfully, the igmp-snooping enable configuration will be generated in the corresponding VLAN view of the AS.

Precautions

This VLAN cannot be a stack reserved VLAN, SVF management VLAN, super VLAN, or RRPP/SEP/ERPS control VLAN.

Example

Enable IGMP snooping for the service VLAN 10 on an AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as service-vlan igmp-snooping 10
```

3.5.20 as service-vlan authorization

Function

The **as service-vlan authorization** command creates service VLANs on ASs.

The **undo as service-vlan authorization** command deletes service VLANs on ASs.

By default, all interfaces on an AS belong to the default VLAN, that is, VLAN 1.

NOTE

This command can only be executed on a parent switch.

Format

as service-vlan authorization { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

undo as service-vlan authorization { *vlan-id1* [**to** *vlan-id2*] } &<1-16>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies service VLAN IDs in a batch: ● *vlan-id1* specifies the first VLAN ID. ● *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* together determine a VLAN range. ● If you do not specify **to** *vlan-id2*, only one service VLAN is specified by *vlan-id1*.	Values of *vlan-id1* and *vlan-id2* are integers in a range of 1 to 4094.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **as service-vlan authorization** command to deliver service VLANs to ASs in a batch. After these service VLANs are delivered successfully, corresponding VLANs are created on these ASs.

Precautions

This VLAN cannot be a stack reserved VLAN, SVF management VLAN, super VLAN, or RRPP/SEP/ERPS control VLAN.

In versions earlier than V200R019, a maximum of 32 service VLANs can be created. In V200R019 and later versions, a maximum of 1024 service VLANs can be created.

Example

Create the service VLAN 10 for ASs.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as service-vlan authorization 10
```

3.5.21 as type

Function

The **as type** command specifies the file to be loaded during the upgrade of an AS of a specified device type.

The **undo as type** command deletes the file to be loaded during the upgrade of an AS of a specified device type.

By default, the file to be loaded is not specified during the upgrade of an AS of a specified device type.

NOTE

This command can only be executed on a parent switch.

Format

as type *as-type* { **system-software** *system-software* | **patch** *patch* } *

undo as type *as-type* [**system-software** | **patch**]

Parameters

Parameter	Description	Value
as-type	Specifies the device type of an AS.	The value is an enumerated type. You can enter a question mark (?) and select a value from the displayed value range.
system-software *system-software*	Specifies the name of the system software file to be loaded on an AS.	The value is a string of 4 to 48 case-insensitive characters without spaces or special characters, including ~ * : ' " ? < > | [ ] % \ /.
patch *patch*	Specifies the name of the patch file to be loaded on an AS.	The value is a string of 5 to 48 case-insensitive characters without spaces or special characters, including ~ * : ' " ? < > | [ ] % \ /.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS is automatically upgraded after going online, the AS is upgraded using the file specified by the **as type** command.

Precautions

You can run the **as type** command multiple times to specify different files for different types of ASs.

If the system software file is not specified and only the patch file is specified during a patch upgrade, the patch upgrade fails if the patch file does not match the system software.

Follow-up Procedure

Run the **upgrade as** command to upgrade the AS.

Example

Specify the file to be loaded on the AS of the S5720-P-LI type.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as type s5720-p-li system-software S5720-P-LI-V200R022C00SPC500.cc
```

3.5.22 attach as

Function

The **attach as** command allows you to log in to an AS from the parent.

NOTE

This command can only be executed on a parent switch.

Format

attach as name *as-name*

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS for login.	The value must have an existing AS name.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In addition to local login through a console port, you can log in to an AS from the parent. This login mode is supported in two service configuration modes: centralized mode and independent mode.

After you log in to an AS in centralized mode, you can configure only commands related to file management and service diagnosis for fault location.

After you log in to an AS in independent mode, you can use more commands to configure services on the AS.

Prerequisites

In centralized mode, an AS administrator profile has been bound to the AS, and an AS user name and password have been configured.

In independent mode, an AS user name and password have been configured in the uni-mng view using the **independent-as-admin** command.

Precautions

After an AS user name and password are configured, you need to enter the correct user name and password when logging in to an AS through the console port. When you log in to an AS from the parent using the **attach as** command, you can log in to the AS without entering the user name or password.

In versions earlier than V200R011C10, at most one VTY user can log in to an AS at a time. In V200R011C10 and later versions, at most four VTY users can log in to an AS at a time.

Example

In centralized mode, log in to the AS **as1** from the parent.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] user asuser password YsHsjx_202206
[HUAWEI-um-as-admin-profile_1] quit
```

```
[HUAWEI-um] as-group name group_1
[HUAWEI-um-as-group-group_1] as name as1
[HUAWEI-um-as-group-group_1] as-admin-profile profile_1
[HUAWEI-um-as-group-group_1] quit
[HUAWEI-um] commit as all
Info: Commiting the configuration will take a long time. Are you sure you want to commit the
configuration? [Y/N]: y
[HUAWEI-um] attach as name as1
```

In independent mode, log in to the AS **as1** from the parent. Before the login, the independent mode needs to be enabled on the fabric-port connected to the AS **as1**. The following uses a level-1 AS as the AS **as1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] independent-as-admin user asuser password YsHsjx_202206
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port connect independent-as
[HUAWEI-um-fabric-port-1] quit
[HUAWEI-um] attach as name as1
```

3.5.23 authentication access-user maximum (user access profile view)

Function

The **authentication access-user maximum** command configures the maximum number of access users in a user access profile.

The **undo authentication access-user maximum** command deletes the maximum number of access users in a user access profile.

By default, the maximum number of access users is not configured in a user access profile.

NOTE

This command can only be executed on a parent switch.

Format

authentication access-user maximum *max-num*

undo authentication access-user maximum

Parameters

Parameter	Description	Value
max-num	Specifies the maximum number of access users in a user access profile.	The value is an integer that ranges from 1 to 1024. After the value is delivered to an AS, the effective value depends on the AS specifications. For details, see **authentication access-point max-user**.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a user access profile, you can configure the maximum number of access users in the profile. When the profile is bound an AS port, the maximum number of access users is automatically configured for the port. The following configuration is generated on the AS port:

```
#
 authentication access-point max-user max-num
#
```

Precautions

The **authentication access-user maximum** command configuration takes effect only for new users.

Example

Set the maximum number of access users to 100 in the user access profile **profile_1**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] authentication access-user maximum 100
```

3.5.24 auth-mode none

Function

The **auth-mode none** command sets the AS authentication mode to no authentication.

The **undo auth-mode** command restores the default AS authentication mode.

By default, authentication is required when an AS connects to an SVF system.

NOTE

This command can only be executed on a parent switch.

Format

auth-mode none

undo auth-mode

Parameters

None

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

By default, an AS needs to be authenticated using a blacklist or whitelist before connecting to an SVF system. You can also configure no authentication for ASs. In no authentication mode, an AS can connect to an SVF system regardless of whether it is in a blacklist or whitelist.

NOTE

Non-authentication has security risks. Therefore, authentication is recommended.

Example

Configure no authentication for ASs to connect to an SVF system.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] auth-mode none
```

3.5.25 authentication-profile (user access profile view)

Function

The **authentication-profile** command binds an authentication profile to a user access profile.

The **undo authentication-profile** command deletes the authentication profile bound to a user access profile.

By default, no authentication profile is bound to a user access profile.

NOTE

This command can only be executed on a parent switch.

Format

authentication-profile *authentication-profile-name*

undo authentication-profile

Parameters

Parameter	Description	Value
authentication-profile-name	Specifies the name of an authentication profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a user access profile, you can bind an authentication profile to the user access profile. When the user access profile is bound to an AS port, the user access authentication mode specified in the authentication profile is automatically configured on the AS port.

NAC provides three user authentication modes: 802.1X authentication, MAC address authentication, and Portal authentication. To implement user access authentication, run the **dot1x-access-profile name** *access-profile-name*, **mac-access-profile name** *access-profile-name*, and **portal-access-profile name** *access-profile-name* commands in the system view to create an access profile, bind one or multiple of the three user authentication modes to the authentication profile, and then bind the authentication profile to the user access profile in an SVF system.

Precautions

- If Portal authentication is deployed in an SVF system, you must run the **web-auth-server** *server-name* command to specify the Portal server template used in Portal authentication in the Portal access profile view. Additionally, only one Portal server template can be configured in a Portal access profile.
- If the Portal authentication mode has been set to **layer3** in the portal-access-profile bound to the authentication profile, it is not allowed to bind this authentication profile to the user access profile. If an authentication profile has been bound to the user access profile, it is now allowed to set the Portal authentication mode to **layer3**.
- In versions earlier than V200R019C10, user access profiles must be bound to the same authentication profile at any time. In V200R019C10 and later versions, user access profiles can be bound to different authentication profiles. However, if these user access profiles are bound to ASs on the same cascade port, the authentication profiles must be the same.

- The **authentication-profile** and **mac-limit maximum** *max-num* as well as **authentication-profile** and **traffic-limit inbound** { **arp** | **dhcp** } **cir** *cir-value* commands are mutually exclusive and cannot be configured together in a user access profile.
- If many users are connected to the port to which a user access profile is bound, the authentication configuration in the profile may need to take a certain period of time to complete.
- Before changing the authentication profile on the parent, run the **undo authentication-profile** command to delete the existing authentication profile and then run the **commit as** { **name** *as-name* | **all** } command to commit the configuration. You can then create a new authentication profile on the parent.
- After bidirectional flow control is configured in an authentication profile using the **authentication control-direction all** command, this authentication profile cannot be bound to a user access profile.
- In SVF of a version earlier than V200R019, access authentication is not supported for IPv6 users. In SVF of V200R019 or a later version, access authentication is supported for IPv6 users.
- In V200R019 and later versions, the **authentication ipv6-control enable** command configured in an authentication profile can be delivered to ASs. This command can take effect only in the following situations:
  - The parent is S6735-S, S6720-EI, or S6720S-EI, and ASs are S5720-LI, S5720S-LI, S5720I-SI, S5735-S, S5735S-S, S5735S-H, S5736-S, S6735-S, S6720-EI, S6720S-S, or S6720S-EI.
  - The parent is a modular switch and the parent's port to which the authentication profile is bound is not located on the ES0D0G24SA00, ES0D0G24CA00, LE0MG24CA, LE0MG24SA, LE1D2S04SEC0, LE1D2X32SEC0, LE1D2H02QEC0, or X series cards, and ASs are S5720-LI, S5720S-LI, S5720I-SI, S5735-S, S5735S-S, S5735S-H, S5736-S, S6735-S, S6720-EI, S6720S-S, or S6720S-EI.
- In V200R019 and later versions, the **authentication single-stack-control enable** command configured in an authentication profile can be delivered to ASs. This command can take effect only in the following situations:
  - The parent is S5531-H, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, or S6730-H, and ASs are S5531-H, S5531-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, or S6730-H.
  - The parent is a modular switch and the parent's port to which the authentication profile is bound is located on the LE1D2S04SEC0, LE1D2X32SEC0, LE1D2H02QEC0, or X series cards, and ASs are S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, or S6730-H.
- If an interface needs to be unbound from an authentication profile and there are many users on the interface, it takes a long time to unbind the interface from the authentication profile. To shorten the time, run the **authentication speed-limit max-num** command to increase the rate at which a specified AS sends user disassociation request messages.

Example

Bind an authentication profile to the user access profile.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name 1
[HUAWEI-mac-access-profile-1] quit
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] mac-access-profile 1
[HUAWEI-authen-profile-test] quit
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] authentication-profile test
```

3.5.26 blacklist mac-address

Function

The **blacklist mac-address** command adds a specified MAC address to the blacklist.

The **undo blacklist mac-address** command deletes a MAC address from the blacklist.

By default, no MAC address is added to the blacklist. A maximum of 128 MAC addresses can be added to the blacklist.

NOTE

This command can only be executed on a parent switch.

Format

blacklist mac-address *mac-address1* [**to** *mac-address2*]

undo blacklist mac-address { *mac-address1* [**to** *mac-address2*] | **all** }

Parameters

Parameter	Description	Value
mac-address1 [**to** *mac-address2*]	Specifies the MAC address to be added to the blacklist.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.
all	Deletes all the MAC addresses in the blacklist.	-

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SVF system needs to authenticate an AS, the SVF system allows the AS to connect to if the MAC address of the AS is in the whitelist and disallows the AS to connect to if the MAC address is in the blacklist.

Precautions

- A MAC address cannot exist in both the whitelist and blacklist.
- By default, if the MAC address of an AS is neither in the whitelist nor in the blacklist, the AS fails the authentication. You can run the **confirm** { **all** | **mac-address** *mac-address* } command to allow all ASs or a specified AS to pass the authentication.
- If the MAC address of an AS that has connected to an SVF system is added to the blacklist, the AS restarts and exits from the SVF system.

Example

Add the MAC address 00e0-fc12-3456 to the blacklist.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] blacklist mac-address 00e0-fc12-3456
```

3.5.27 broadcast-suppression (network enhanced profile view)

Function

The **broadcast-suppression** command configures broadcast traffic suppression in a network enhanced profile.

The **undo broadcast-suppression** command cancels broadcast traffic suppression in a network enhanced profile.

By default, broadcast traffic suppression is not configured in a network enhanced profile. By default, the percentage of broadcast traffic that can pass through an AS port is 50%.

NOTE

This command can only be executed on a parent switch.

Format

broadcast-suppression packets *packets-per-second*

undo broadcast-suppression

Parameters

Parameter	Description	Value
packets *packets-per-second*	Specifies the packet rate of an interface.	The value is an integer that ranges from 0 to 14881000, in packets per second (PPS). If the configured packet rate on the parent switch is larger than the maximum value on the AS port, the maximum value takes effect on the AS port.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure broadcast traffic suppression in the profile. After the profile is bound to an AS port, broadcast traffic suppression is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 broadcast-suppression packets packets-per-second
#
```

To prevent broadcast storms, you can run the **broadcast-suppression** command to configure the maximum number of broadcast packets that can pass through a port. When the broadcast traffic rate reaches the maximum value, the system discards excess broadcast packets to control the traffic volume within a proper range.

Example

Configure broadcast traffic suppression in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] broadcast-suppression packets 148810
```

3.5.28 clear direct-command

Function

The **clear direct-command** command deletes commands to be directly delivered to an AS from the parent.

NOTE

This command can only be executed on a parent switch.

Format

clear direct-command [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID of a member device in an AS.	The value is an integer that ranges from 0 to 4.

Views

AS view

Default Level

3: Management level

Usage Guidelines

After you run the **direct-command** command to directly deliver commands to an AS, you can run the **clear direct-command** command to delete the commands from the parent.

You can delete directly delivered commands only when the AS is offline. Do not run the **clear direct-command** command when the parent is delivering the commands to an AS.

Example

Delete the commands to be directly delivered to AS1 from the parent.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] clear direct-command
```

3.5.29 commit as

Function

The **commit as** command delivers the service configuration to ASs.

NOTE

This command can only be executed on a parent switch.

Format

commit as { **name** *as-name* | **all** }

Parameters

Parameter	Description	Value
name *as-name*	Delivers the service configuration to an AS with a specified name.	The value must have an existing AS name.
all	Delivers the service configuration to all ASs.	-

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

After configuring or changing services (including service profiles and user authentication-free rules) on the parent, you need to run the **commit as** command to deliver the configuration to ASs to make the configuration take effect.

In versions earlier than V200R020C00, you do not need to configure an AS administrator before configuring an AS in centralized mode. However, in V200R020C00 and later versions, before configuring an AS in centralized mode, you have to configure an AS administrator and deliver it to the AS. Otherwise, the AS configuration will fail to be delivered. For details about how to configure an AS administrator, see Configuring Services for ASs Using an AS Administrator Profile.

Example

Deliver the service configuration to all ASs.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] commit as all
```

3.5.30 confirm

Function

The **confirm** command confirms that unauthenticated ASs pass the authentication.

NOTE

This command can only be executed on a parent switch.

Format

confirm { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Confirms that all ASs pass the authentication.	-
mac-address *mac-address*	Confirms that an AS with a specified MAC address passes the authentication.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

When an AS needs to be authenticated before connecting to an SVF system, the AS fails the authentication if its MAC address is neither in the whitelist nor in the blacklist. You can run the **confirm** command to allow all ASs or a specified AS to pass the authentication.

You can run the **display as unauthorized record** command to check information about the ASs that fail the authentication.

Example

Confirm that the AS with the MAC address 00e0-fc12-3456 passes the authentication.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] confirm mac-address 00e0-fc12-3456
```

3.5.31 description (Fabric-port view)

Function

The **description** command configures the description of a fabric port.

The **undo description** command deletes the description of a fabric port.

By default, no description is configured for a fabric port.

NOTE

This command can only be executed on a parent switch.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description.	The value is a string of 1 to 64 case-sensitive characters with spaces supported.

Views

Fabric-port view

Default Level

2: Configuration level

Usage Guidelines

To facilitate fabric port management and identification, you can configure descriptions for fabric ports. For example, you can describe the name of an AS that connects to a fabric port.

Example

Configure the description of a fabric port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] description To_as1
```

3.5.32 description (port group view)

Function

The **description** command configures the description of a port group.

The **undo description** command deletes the description of a port group.

By default, a port group does not have a description.

NOTE

This command can only be executed on a parent switch.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description.	The value is a string of 1 to 15 case-sensitive characters with spaces supported.

Views

Port group view

Default Level

2: Configuration level

Usage Guidelines

To facilitate identification and management of terminals connected to a port group in the web system, configure the description of the port group.

Example

Configure the description of a specified port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name 1
[HUAWEI-um-portgroup-1] description switch
```

3.5.33 dhcp snooping enable (network enhanced profile view)

Function

The **dhcp snooping enable** command configures DHCP snooping in a network enhanced profile.

The **undo dhcp snooping enable** command cancels DHCP snooping in a network enhanced profile.

By default, DHCP snooping is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

dhcp snooping enable

undo dhcp snooping enable

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure DHCP snooping in the profile. After the profile is bound to an AS port, DHCP snooping is automatically enabled on the AS and AS port. The following configuration is generated on the AS:

```
#
dhcp enable
#
dhcp snooping enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile configuration.

You can run the **dhcp snooping enable** command to enable DHCP snooping on a port so as to improve DHCP security.

Precautions

Before running the **undo dhcp snooping enable** command, ensure that the network enhanced profile view is not configured with IPSG or DAI. To disable IPSG and DAI, run the **undo ip source check user-bind enable (network enhanced profile view)** and **undo arp anti-attack check user-bind enable (network enhanced profile view)** commands respectively.

The **dhcp snooping enable** command configured in the network enhanced profile can only configure a DHCP dynamic binding table but not a DHCP static binding table.

Example

Configure DHCP snooping in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] dhcp snooping enable
```

3.5.34 direct-command

Function

The **direct-command** command configures ASs on the parent. The parent directly delivers the configuration to the ASs, and you do not need to run the **commit as** command.

The **undo direct-command** command cancels the configuration for ASs on the parent.

The following table lists the service configurations that can be delivered using the **direct-command** command. If no configuration dependency and restriction are provided for a command, see the details in the command reference.

NOTE

This command can only be executed on a parent switch.

Format

direct-command view { **system** | **eth-trunk** *trunk-id* | *interface-type interface-number* | **stack-port** *member-id/port-id* } **command** *command-text*

undo direct-command view { **system** | **eth-trunk** *trunk-id* | *interface-type interface-number* | **stack-port** *member-id/port-id* } **command** *command-text*

Parameters

Parameter	Description	Value
view { **system** | **eth-trunk** *trunk-id* | *interface-type interface-number* | **stack-port** *member-id/port-id* }	Specifies the view in which a command is executed. - **system**: system view - *interface-type interface-number*: interface view - **stack-port** *member-id/port-id*: stack port view - **eth-trunk** *trunk-id*: Eth-Trunk interface view	-
command *command-text*	Specifies the command to be delivered to ASs.	The value is a string of 1 to 128 characters. This command does not support auto-completion of keywords by pressing Tab.

Views

AS view

Default Level

3: Management level

Usage Guidelines

- When you configure a directly delivered command on the parent, enter the complete and correct command instead of the abbreviated form. No info message is displayed for confirming your input.
- A directly delivered command supports the help and typeahead functions but not real-time check during input. The system checks the input only after you complete typing a command and press **Enter**. No detailed description is provided in help information. If you fail to configure a command for an AS, an info message is displayed.
- When you configure a directly delivered command, the AS to which the command is to be delivered must be online. If you need to specify a port or *slot-id* in a command, the corresponding member device must be available. If the AS is offline, run the **clear direct-command** command to delete the completed configuration on the parent.
- If a port has the configuration directly delivered using commands, the port cannot be configured as a member port of the Eth-Trunk to which a fabric port is bound. If a port has been configured as a member port of the Eth-Trunk to which a fabric port is bound, the configuration cannot be directly delivered to the port using commands.
- Directly delivering configuration using commands and delivering configuration using service profiles are mutually exclusive and cannot be performed simultaneously.
- In versions earlier than V200R019C00, a maximum of 4096 commands can be configured. In V200R019C00 and later versions, a maximum of 8192 commands can be configured.
- In versions earlier than V200R020C00, you do not need to configure an AS administrator before configuring an AS in centralized mode. However, in V200R020C00 and later versions, before configuring an AS in centralized mode, you have to configure an AS administrator and deliver it to the AS. Otherwise, the AS configuration will fail to be delivered. For details about how to configure an AS administrator, see Configuring Services for ASs Using an AS Administrator Profile.
- The following lists the commands that can be directly delivered to ASs. You can run the **undo direct-command view** { **system** | *interface-type interface-number* } **command** *command-text* command to cancel the configuration or restore default settings. The *command-text* parameter specifies the commands listed in the following table.

Service Category	Format	View	Function	Configuration Dependency and Restriction
Energy-saving management	**port-auto-sleep enable**	Interface view	Enables the port sleeping function on an electrical interface.	Currently, this command can be used on electrical interfaces (excluding MultiGE interfaces) and combo interfaces working as electrical interfaces.
PoE	**poe force-power**	Interface view	Enables forcible PoE power supply on an interface.	-
	poe legacy enable	Interface view	Enables an interface to check compatibility of PDs.	-
	poe priority { **critical** | **high** | **low** }	Interface view	Sets the power supply priority of a PoE interface.	-
	poe af-inrush enable slot *slot-id*	System view	Configures the IEEE 802.3at-compliant device to provide power in accordance with IEEE 802.3af.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	poe high-inrush enable slot *slot-id*	System view	Configures a device to allow high inrush current during power-on.	-
	undo poe enable (supported in V200R011C10 and later versions)	Interface view	Disables the PoE function on an interface.	-
Ethernet interfaces	**undo negotiation auto**	Interface view	Configures an interface to work in non-auto negotiation mode. After you run the **undo direct-command** command, the interface works in auto negotiation mode.	- This command cannot be configured on combo interfaces. - Do not cancel the **undo negotiation auto** command when **speed** or **duplex** is specified.
	speed { **10** | **100** | **1000** | **2500** | **5000** | **10000** }	Interface view	Sets the rate in non-auto negotiation mode.	- This command cannot be configured on combo interfaces. - Ensure that the interface works in non-auto negotiation mode before configuring this command.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	speed auto-negotiation	Interface view	Enables auto-negotiation on a GE optical interface.	- Support for this command varies depending on switch models. For details, see the **speed auto-negotiation** command in the *Command Reference - Interface Management Commands - Ethernet Interface Configuration Commands*. - Ensure that the interface works in auto-negotiation mode before configuring this command.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	duplex { **full** | **half** }	Interface view	Sets the duplex mode for an electrical interface in non-auto negotiation mode.	● This command cannot be configured on combo interfaces. ● Ensure that the interface works in non-auto negotiation mode before configuring this command. ● When the working rate of a GE electrical interface is 1000 Mbit/s, the interface supports only the full duplex mode.
	loopback internal	Interface view	Configures a loopback detection mode on an interface.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	description *description* (supported in V200R011C10 and later versions)	Interface view	Configures the description for an interface.	The description contains a maximum of 52 characters in V200R011C10, and the description contains a maximum of 116 characters in V200R012C00 and later versions.
Eth-Trunk interface	**description** *description* (supported in V200R019C00 and later versions)	Eth-Trunk interface view	Configures the description for an Eth-Trunk interface.	The description contains a maximum of 116 characters. The description can be configured for a service Eth-Trunk interface or an Eth-Trunk interface used in an SVF system to connect upstream and downstream devices. The description cannot be configured for Eth-Trunk0.

Service Category	Format	View	Function	Configuration Dependency and Restriction
Port bridge	**port bridge enable**	Interface view	Enables the bridging function on an interface.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
Port Security (supported in V200R019C00 and later versions)	**port-security max-mac-num** *max-number*	Interface view	Sets the maximum number of secure MAC addresses that can be learned on an interface.	● The **port-security max-mac-num** *max-number* command in direct configuration mode is mutually exclusive with the **mac-limit maximum** *max-num* command configured in a user access profile and cannot be both configured. ● Port security (and sticky MAC if needed) must be enabled in a network enhanced profile, and then run the **direct-command** command to deliver this command.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	port-security mac-address sticky *mac-address* **vlan** *vlan-id*	Interface view	Configures a sticky MAC address entry.	Port security and sticky MAC must be enabled in a network enhanced profile, and then run the **direct-command** command to deliver this command.
	save sticky-mac configuration	System view	Saves the sticky MAC addresses on an AS to a file named unimng-xxxx.ztbl. *xxxx* in the file name represents the management MAC address of the AS.	-
Voice VLAN	**voice-vlan mac-address** *mac-address* **mask** *mask* (supported in V200R011C10 and later versions)	System view	Configures the OUI address of the voice VLAN.	-
LBDT	**loopback-detect enable**	Interface view	Enables loopback detection on an interface.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	loopback-detect packet vlan *vlan-id*	Interface view	Enables loopback detection for a specified VLAN.	If you configure this command multiple times, loopback detection is enabled for multiple VLANs.

Service Category	Format	View	Function	Configuration Dependency and Restriction
ARP rate limiting	**arp speed-limit source-mac maximum** *maximum*	System view	Configures ARP rate limiting based on source MAC addresses.	● Only some models support this command. For details, see the **arp speed-limit source-mac** command in the *Command Reference - Security Commands - ARP Security Configuration Commands*. ● The value of **maximum** *maximum* ranges from 0 to 256. ● This function takes effect only for the ARP packets sent to the CPU.

Service Category	Format	View	Function	Configuration Dependency and Restriction
	arp speed-limit source-ip maximum *maximum*	System view	Configures ARP rate limiting based on source IP addresses.	- The value of **maximum** *maximum* ranges from 0 to 256. - This function takes effect only for the ARP packets sent to the CPU.
Stack	**port interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } **enable** (supported in V200R010 and later versions)	Stack interface view: **stack-port** *member-id/port-id*	Configures a service interface as a stack member port and adds it to a stack port.	Before restoring the stack member ports that are added to a stack port in direct configuration mode as common service interfaces, you do not need to run the **shutdown interface** command in the stack interface view.
	stack slot *slot-id* **priority** *priority* (supported in V200R010 and later versions)	System view	Sets a stack priority for a member switch in a stack.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	stack slot *slot-id* **renumber** *new-slot-id* (supported in V200R011C10 and later versions)	System view	Changes the stack ID of a specified member switch in a stack. **NOTICE** If there are services running, delivering this command may cause service interruptions and configuration loss. Therefore, you are advised to deliver this command when an AS is unconfigured.	A stack ID cannot be changed in the following situations: - The switch is a standalone switch that does not join any stack. - The newly configured stack ID is an existing stack ID of a specified member switch in a stack. - Ports with the specified *slot-id* have been configured as member ports of an uplink fabric port. - Ports with the specified *slot-id* have been configured as member ports of a downlink

Service Category	Format	View	Function	Configuration Dependency and Restriction
				fabric port.

Service Category	Format	View	Function	Configuration Dependency and Restriction
User Access and Authentication (supported in V200R012C00 and later versions)	**access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*	System view	Sets the source IP address and source MAC address of offline detection packets in a VLAN.	- In other V200R012C00 versions except V200R012C00SPC710, this command can be configured only one. If you want to modify the configuration, delete the existing configuration and then perform the configuration again. - In V200R012C00SPC710 and V200R013C00, when **vlan**, **ip-address**, and **mac-address** are all different, multiple configurations of this command can be generated.

Service Category	Format	View	Function	Configuration Dependency and Restriction
				If any one of **vlan**, **ip-address**, and **mac-address** has been configured, delete the existing configuration before reconfiguring them. ● In V200R019 and later versions, multiple configurations of this command can be generated regardless of whether the VLAN, IP address, and MAC address are the same. You do not need to delete the existing configuration. If the newly configured VLAN is the same as the

Service Category	Format	View	Function	Configuration Dependency and Restriction
				existing one, the IP address and MAC address in the original configuration are replaced with the newly configured IP address and MAC address. If the newly configured VLAN is different from the existing one, a new configuration is generated.
	access-user arp-detect default ip-address *ip-address*	System view	Sets the default source IP address of offline detection packets.	-
	undo user-detect	System view	Disables the online user detection function.	-

Service Category	Format	View	Function	Configuration Dependency and Restriction
	authentication speed-limit max-num *max-num-value* **interval** *interval-value* (supported in V200R013C00 and later versions)	System view	Configures the rate limit for an access device to send user association and disassociation request messages.	-
	access-user arp-detect fallback ip-address *mask-length* (supported in V200R013C00 and later versions)	System view	Configures an IP address required for calculating the source address of offline detection packets.	If you run this command multiple times, only the latest configuration takes effect.
	access-user arp-detect delay *delay* (supported in V200R013C00 and later versions)	System view	Configures the delay for sending offline detection packets.	-
	static-user *start-ip-address* [*end-ip-address*] [**mac-address** *mac-address* | **vlan** *vlan-id*] (supported in V200R019C00 and later versions)	System view	Configures a static user.	If the IP address of a static user is set to an IP address range, any IP address in this address range cannot be modified or deleted.

Example

Configure the parent to deliver the **loopback-detect enable** command to GigabitEthernet0/0/1 on **as1** to enable loopback detection on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
```

```
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] direct-command view gigabitethernet 0/0/1 command loopback-detect enable
```

3.5.35 display as

Function

The **display as** command displays information about access switches (ASs).

NOTE

This command can only be executed on a parent switch.

Format

display as { **all** | **name** *as-name* | **mac-address** *mac-address* | **vpn-instance information** }

Parameters

Parameter	Description	Value
all	Displays information about all ASs.	-
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.
vpn-instance information	Displays VPN instance information.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as** command to view information about ASs in an SVF system, including the AS device type, VPN instance information, and access status.

Example

Display information about all ASs.

```
<HUAWEI> display as all
Total: 1, Normal: 1, Fault: 0, Idle: 0, Version mismatch: 0
--------------------------------------------------------------------------------
No.  Type          MAC            IP              State       Name
--------------------------------------------------------------------------------
0    S5720-P-LI     00e0-fcbb-cc92 192.168.11.254  normal       as1
--------------------------------------------------------------------------------
```

Table 3-86 Description of the **display as all** command output

Item	Description
Total	Total number of ASs.
Normal	Number of ASs that are running normally.
Fault	Number of ASs in abnormal running status.
Idle	Number of ASs that have been configured but no gone online.
Version mismatch	Number of ASs of which the software versions do not match the software version of the parent.
No.	Sequence number.
Type	Device type of an AS.
MAC	Management MAC address of an AS.
IP	IP address of an AS.
State	Status of an AS: ● idle: The AS is in initial state. ● normal: The AS has gone online and connected to an SVF system. ● fault: The AS does not connect to an SVF system. ● version mismatch: The V, R, or C versions of the AS and parent are inconsistent.
Name	Name of an AS.

Display information about the AS **as1**.

```
<HUAWEI> display as name as1
-----------------------------------------------------------------------------
Management MAC       : 00e0-fcbb-cc92
System MAC          : 00e0-fcbb-cc92
```

```
ESN                : 210235317310xxxxxxxx
Name                 : as1
Model                : S5720-28P-LI-AC
Device type          : S5720-P-LI
State              : normal
Mode                 : centralized
Slot              : 0
AS group             : group1
Port group           : group2
-------------------------------------------------------------------------------
```

Table 3-87 Description of the **display as name** command output

Item	Description
Management MAC	Management MAC address of an AS. In a Super Virtual Fabric (SVF) system, each AS has a unique management MAC address to identify itself. To set a management MAC address for an AS, run the **as access manage-mac** command. If no management MAC address is configured for an AS, the system MAC address of the AS is used as the management MAC address.
System MAC	System MAC address of an AS, which is the physical MAC address of this AS.
ESN	Sequence number of an AS.
Name	Name of an AS.
Model	Device model of an AS.
Device type	Device type of an AS.
State	Status of an AS: ● idle: The AS is in initial state. ● normal: The AS has gone online and connected to an SVF system. ● fault: The AS does not connect to an SVF system. ● version mismatch: The V, R, or C versions of the AS and parent are inconsistent.
Mode	Service configuration mode of an AS: ● centralized: indicates the centralized mode. ● independent: indicates the independent mode.
Slot	Stack ID of an AS in a stack.
AS group	AS group to which an AS belongs.

Item	Description
Port group	Port group to which an AS port belongs.

Display VPN instance information of ASs.

```
<HUAWEI> display as vpn-instance information
Total: 5
--------------------------------------------------------------------------------
No.  VPN-Instance                    AS Name
--------------------------------------------------------------------------------
0    VPN1                              e-10005(1-1)
1    --                             t-10018(2-2)
2    VPN2                              s-10021(1-1)
3    --                             6-10023(2-1)
4    --                             11-t-16(x-s)
--------------------------------------------------------------------------------
```

Table 3-88 Description of the **display as vpn-instance information** command output

Item	Description
Total	Number of ASs.
No.	AS number.
VPN-Instance	VPN instance name.
AS Name	AS name.

3.5.36 display as access configuration

Function

The **display as access configuration** command displays the access configuration of ASs.

NOTE

Only the switches that function as ASs support this command.

Format

display as access configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as access configuration** command on an AS to check the access configuration of the AS.

Example

Display the access configuration of an AS.

```
<HUAWEI> display as access configuration
   AS mode                              : centralized
   Access interface                     : vlanif11
   Access controller configuration      : --
   Current connected access controller : 192.168.11.1(dynamic)
   Access management MAC                : xxxx-xxxx-xxxx
   Access system MAC                    : xxxx-xxxx-xxxx
   Current connected state              : normal
```

Table 3-89 Description of the **display as access configuration** command output

Item	Description
AS mode	AS mode: - disable: The device works in parent mode. To change the device working mode, run the **as-mode disable** command. - enable: The device works in AS mode, but it does not have the SVF function enabled using the **uni-mng** command. - centralized: The device works in AS mode and the service configuration mode is centralized mode. - independent: The device works in AS mode and the service configuration mode is independent mode.
Access interface	VLANIF interface for the management VLAN of an AS.
Access controller configuration	Parent IP address configured using the **as access controller ip-address** command. If this IP address is configured, the **Current connected access controller** field value contains configured.

Item	Description
Current connected access controller	IP address of the parent to which an AS is connected. If this field contains dynamic, the IP address is obtained through DHCP or in broadcast mode. If this field contains configured, the IP address is statically configured. If an AS does not go online, this field displays --.
Access management MAC	Configured management MAC address of an AS.
Access system MAC	System MAC address of an AS.
Current connected state	Connection status of an AS: ● idle: The AS is in initial state. ● normal: The AS has gone online and connected to an SVF system. ● fault: The AS does not connect to an SVF system. ● version mismatch: The V, R, or C versions of the AS and parent are inconsistent.

3.5.37 display as blacklist

Function

The **display as blacklist** command displays blacklist information of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display as blacklist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as blacklist** command to check blacklist information of an AS.

Example

Display blacklist information of an AS.

```
<HUAWEI> display as blacklist
-------------------------------------------------------------------------------
ID     MAC
-------------------------------------------------------------------------------
0      xxxx-xxxx-xxxx
-------------------------------------------------------------------------------
Total: 1
```

Table 3-90 Description of the **display as blacklist** command output

Item	Description
ID	ID of a blacklist.
MAC	MAC address added to the blacklist. To add a MAC address to a blacklist, run the **blacklist mac-address** command. If no MAC address is specified, no information is displayed.

3.5.38 display as run-info

Function

The **display as run-info** command displays running status information of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display as { **name** *as-name* | **mac-address** *mac-address* } **run-info**

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as run-info** command to check running status information of an AS, including the AS access status, CPU usage, and memory usage.

Example

Display running status information of an AS.

```
<HUAWEI> display as name as1 run-info
Info: This operation may take a few seconds. Please wait...
-------------------------------------------------------------------------------
Software version     : Version 5.170 V200R023C00
Hardware version     : VER.A
Patch version        : --
Patch state          : running
IP address           : 192.168.1.154
IP mask              : 255.255.255.0
Gateway              : 192.168.1.1
VPN-Instance         : --
State                : normal
Online time          : 1 day, 18 hours, 40 minutes, 0 second
CPU usage            : 12%
Memory usage         : 52%
Slot 0               : present
-------------------------------------------------------------------------------
```

Table 3-91 Description of the **display as run-info** command output

Item	Description
Software version	Software version running on an AS.
Hardware version	Hardware version running on an AS.
Patch version	Patch version. This field displays**--** when the patch package is not installed.

Item	Description
Patch state	Patch status. - Running: The patch is running. - not running: The patch is not running.
IP address	IP address of an AS.
IP mask	Subnet mask.
Gateway	Gateway of an AS.
VPN-Instance	Name of a VPN instance.
State	Status of an AS: - idle: The AS is in initial state. - normal: The AS has gone online and connected to an SVF system. - fault: The AS does not connect to an SVF system. - version mismatch: The V, R, or C versions of the AS and parent are inconsistent.
Online time	Online time of an AS.
CPU usage	CPU usage of an AS.
Memory usage	Memory usage of an AS.
Slot 0	Whether an AS member device is present: - present - absent

3.5.39 display as unauthorized record

Function

The **display as unauthorized record** command displays information about the ASs that fail the authentication.

NOTE

This command can only be executed on a parent switch.

Format

display as unauthorized record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as unauthorized record** command to check information about the ASs that fail the authentication.

Example

Display information about the ASs that fail the authentication.

```
<HUAWEI> display as unauthorized record
Unauthorized AS record:
-------------------------------------------------------------------------------
AS type        : S5720-SI
Host name      : host
AS MAC address : xxxx-xxxx-xxxx
AS IP address  : 192.168.1.253
Record time    : 2023-02-20 16:06:10 DST
-------------------------------------------------------------------------------
Total: 1
```

Table 3-92 Description of the **display as unauthorized record** command output

Item	Description
AS type	Device type of an AS.
Host name	Name of the AS.
AS MAC address	MAC address of the AS.
AS IP address	IP address of the AS.
Record time	Time when the AS is authenticated.

3.5.40 display as whitelist

Function

The **display as whitelist** command displays whitelist information of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display as whitelist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display as whitelist** command to check whitelist information of an AS.

Example

Display whitelist information of an AS.

```
<HUAWEI> display as whitelist
--------------------------------------------------------------------------------
ID     MAC
--------------------------------------------------------------------------------
0      00e0-fc07-8282
--------------------------------------------------------------------------------
Total: 1
```

Table 3-93 Description of the **display as whitelist** command output

Item	Description
ID	ID of a whitelist.
MAC	MAC address added to the whitelist.

3.5.41 display uni-mng as-discover packet statistics

Function

The **display uni-mng as-discover packet statistics** command displays AS Discovery packet statistics on a fabric port.

NOTE

This command can be used on the parent or an AS. After running this command, you can check AS Discovery packet statistics on a fabric port of the local device.

Format

display uni-mng as-discover packet statistics interface fabric-port *port-id*

Parameters

Parameter	Description	Value
interface fabric-port *port-id*	Specifies the number of a fabric port.	The value is an integer that ranges from 0 to 63 on an AS and the value range on the parent varies depending on the switch model: ● S12700/S12700E: 0 to 255 ● MCUD/SRUK/MFUX/MPUE/SRUE/SRUHA1/SRUHX1/SRUH: 0 to 255 ● Other switch models: 0 to 63

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as-discover packet statistics** command to check AS Discovery packet statistics on a fabric port.

Example

Display AS Discovery packet statistics on a fabric port.

```
<HUAWEI> display uni-mng as-discover packet statistics interface fabric-port 1
The statistics of AS Discover packet on Fabric-port1:

PortName     Packet-type                  Receive        Send
-------------------------------------------------------------------------------
GE2/0/23     AS Discover Request            0              3
             AS Discover ACK              3              0
             AS Discover ParaSyn Req        0              3
             AS Discover ParaSyn ACK        3              0
             AS Discover HeartBeat Req      0              11238
             AS Discover HeartBeat ACK      11238          0
             AS Discover NAK              0              0
             AS Discover FabricCfg Req      0              0
             AS Discover FabricCfg ACK      0              0
             AS Discover NotifyOffline Req  0              0
             AS Discover NotifyOffline ACK  0              0
-------------------------------------------------------------------------------
```

Table 3-94 Description of the **display uni-mng as-discover packet statistics** command output

Item	Description
PortName	Name of a member port in a fabric port.
Packet-type	Packet type: - AS Discover Request: neighbor discovery request packet - AS Discover Request: neighbor discovery request packet - AS Discover ParaSyn Req: neighbor discovery parameter synchronization packet - AS Discover ParaSyn ACK: neighbor discovery parameter synchronization response packet - AS Discover HeartBeat Req: neighbor discovery heart packet - AS Discover HeartBeat ACK: neighbor discovery heart response packet - AS Discover NAK: neighbor discovery error packet - AS Discover FabricCfg Req: neighbor discovery AS fabric port configuration packet - AS Discover FabricCfg ACK: neighbor discovery AS fabric port configuration response packet - AS Discover NotifyOffline Req: request packet that notifies AS offline - AS Discover NotifyOffline ACK: response packet of the request that notifies AS offline
Receive	Statistics about received packets. Statistics about AS Discover HeartBeat Req and AS Discover HeartBeat ACK packets will be cleared and start from 0 after an active/standby switchover is performed on the device.

Item	Description
Send	Statistics about sent packets. Statistics about AS Discover HeartBeat Req and AS Discover HeartBeat ACK packets will be cleared and start from 0 after an active/standby switchover is performed on the device.

3.5.42 display uni-mng as-group

Function

The **display uni-mng as-group** command displays information about AS groups.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as-group [**name** *group-name* | **verbose**]

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of an AS group.	The value must be an existing an AS group name.
verbose	Displays detailed information about an AS group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as-group** command to check information about created AS groups.

Example

Display brief information about all AS groups.

```
<HUAWEI> display uni-mng as-group

-------------------------------------------------------------------------------
 Number                    AS-group Name
-------------------------------------------------------------------------------
 1                         asgroup
-------------------------------------------------------------------------------
```

Table 3-95 Description of the **display uni-mng as-group** command output

Item	Description
Number	Sequence number.
AS-group Name	AS group name.

Display detailed information about all AS groups.

```
<HUAWEI> display uni-mng as-group verbose

AS-group name: asgroup
-------------------------------------------------------------------------------
AS name list: (Total number = 1)
 as1
-------------------------------------------------------------------------------
AS-admin profile name: admin
-------------------------------------------------------------------------------
```

Table 3-96 Description of the **display uni-mng as-group verbose** command output

Item	Description
AS-group name	AS group name.
AS name list	List of ASs added to an AS group.
AS-admin profile name	Name of the bound AS administrator profile.

3.5.43 display uni-mng as index

Function

The **display uni-mng as index** command displays the index of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as index

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as index** command to check the index, management MAC address, and name of an AS.

Example

Display the index of an AS.

```
<HUAWEI> display uni-mng as index
Total number : 1
-------------------------------------------------------------------------------
Index     MAC-Current          MAC-Saved          Name
-------------------------------------------------------------------------------
1         00e0-fc12-3456       00e0-fc12-3456     as1
-------------------------------------------------------------------------------
```

Table 3-97 Description of the **display uni-mng as index** command output

Item	Description
Index	Index of an AS.
MAC-Current	Management MAC address.

Item	Description
MAC-Saved	MAC address saved in the flash memory. This field indicates the MAC address saved in the flash memory using the **save** command after an AS goes online or the **as name (uni-mng view)** command is configured. ● If this field displays --, the **save** command is not executed after an AS goes online or the **as name (uni-mng view)** command is configured. ● When **MAC-Current** and **MAC-Saved** are inconsistent, the **save** command is not executed after an AS is replaced or the **as name (uni-mng view)** command is configured.
Name	Name of an AS.

3.5.44 display uni-mng as interface brief

Function

The **display uni-mng as interface brief** command displays brief information about AS ports.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as name *as-name* **interface brief**

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng as interface brief** command to check brief information about AS ports.

When an AS is offline or its version is inconsistent with the parent version, this command displays default attributes of ports on this AS.

Example

Display brief information about AS ports.

```
<HUAWEI> display uni-mng as name as1 interface brief
PHY: Physical
*down      : administratively down
*Stack Port: inactive stack port
-------------------------------------------------------------------------------
Interface                 Type            PHY      Online       MSTP state
-------------------------------------------------------------------------------
Eth-Trunk1                Fabric Port     up       present      forwarding
Eth-Trunk40               Service Port    down     present      discarding
GigabitEthernet0/0/1      Service Port    down     present      discarding
GigabitEthernet0/0/2      Service Port    up       present      forwarding
GigabitEthernet0/0/3      Service Port    down     present      discarding
GigabitEthernet0/0/4      Service Port    down     present      discarding
GigabitEthernet0/0/5      Service Port    down     present      discarding
GigabitEthernet0/0/6      Service Port    down     present      discarding
GigabitEthernet0/0/7      Service Port    down     present      discarding
GigabitEthernet0/0/8      Service Port    down     present      discarding
GigabitEthernet0/0/9      Service Port    down     present      discarding
GigabitEthernet0/0/10     Service Port    down     present      discarding
GigabitEthernet0/0/11     Service Port    down     present      discarding
GigabitEthernet0/0/12     Service Port    down     present      discarding
GigabitEthernet0/0/13     Service Port    down     present      discarding
GigabitEthernet0/0/14     Service Port    down     present      discarding
GigabitEthernet0/0/15     Service Port    down     present      discarding
GigabitEthernet0/0/16     Service Port    down     present      discarding
GigabitEthernet0/0/17     Service Port    down     present      discarding
GigabitEthernet0/0/18     Service Port    down     present      discarding
GigabitEthernet0/0/19     Service Port    down     present      discarding
GigabitEthernet0/0/20     Service Port    down     present      discarding
GigabitEthernet0/0/21     Service Port    down     present      discarding
GigabitEthernet0/0/22     Service Port    down     present      discarding
GigabitEthernet0/0/23     Service Port    down     present      discarding
GigabitEthernet0/0/24     Service Port    down     present      discarding
GigabitEthernet0/0/25     Fabric Port     down     present      discarding
GigabitEthernet0/0/26     Fabric Port     up       present      forwarding
GigabitEthernet0/0/27     Fabric Port     down     present      discarding
GigabitEthernet0/0/28     Fabric Port     up       present      discarding
-------------------------------------------------------------------------------
```

Table 3-98 Description of the **display uni-mng as interface brief** command output

Item	Description
Interface	Interface number.

Item	Description
Type	Interface type: ● Service Port: indicates a service port. ● Stack Port: indicates a physical stack member port. ● Fabric Port: indicates a member port of a fabric port. ● *Stack Port: indicates a stack member port that does not take effect.
PHY	Interface status: ● up: The interface is Up. ● down: The interface is Down. ● *down: The administrator shuts down the interface.
Online	Whether the card where the interface resides is present: ● present ● absent
MSTP state	STP forwarding status of the interface: ● disabled ● discarding ● learning ● forwarding ● --: The interface is absent or a physical stack member port. If the interface is an Eth-Trunk member port, this field displays the forwarding state of the Eth-Trunk.

3.5.45 display uni-mng as interface eth-trunk

Function

The **display uni-mng as interface eth-trunk** command displays information about an Eth-Trunk interface of an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng as name *as-name* **interface eth-trunk** *eth-trunk-id*

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.
eth-trunk-id	Specifies the ID of an Eth-Trunk.	The value range varies depending on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you use the **uni eth-trunk** command to create an Eth-Trunk on an AS, you can run the **display uni-mng as interface eth-trunk** command to view information including the Eth-Trunk working mode, member interface, and member interface status.

Example

Display information about Eth-Trunk 40 on AS as1.

```
<HUAWEI> display uni-mng as name as1 interface eth-trunk 40
Eth-Trunk40's state information is:
WorkingMode: NORMAL
Operate status: down
--------------------------------------------------------------------------------
PortName                Status
GigabitEthernet0/0/10     down
GigabitEthernet0/0/11     down
--------------------------------------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 0
```

Table 3-99 Description of the **display uni-mng as interface eth-trunk** command output

Item	Description
Eth-Trunk40's state information is	State information of Eth-Trunk 40.

Item	Description
WorkingMode	Working mode of the Eth-Trunk interface: ● NORMAL: manual mode ● LACP: LACP mode. To set the LACP mode, specify the **mode lacp** parameter when running the **uni eth-trunk** command to create an Eth-Trunk.
Operate status	Status of the Eth-Trunk interface: ● down: The interface is Down. ● up: The interface is Up.
PortName	Eth-Trunk member interface name. To add or delete an Eth-Trunk member interface, run the **port eth-trunk trunkmember** command.
Status	Eth-Trunk member interface status: ● down: The member interface is Down. ● up: The member interface is Up.
The Number of Ports in Trunk	Number of Eth-Trunk member interfaces.
The Number of UP Ports in Trunk	Number of Eth-Trunk member interfaces in Up state.

3.5.46 display uni-mng authen-user

Function

The **display uni-mng authen-user** command displays authenticated user information on an AS.

NOTE

This command can be used on the parent or an AS.

Format

display uni-mng authen-user [**as name** *as-name*]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS. **NOTE** This parameter can be specified only when the command is run on the parent.	The value must be the name of an online AS.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng authen-user** command to view authenticated user information on an AS.

Example

Display authenticated user information on the AS named **test1**.

```
<HUAWEI> display uni-mng authen-user as name test1
Total: 5
-------------------------------------------------------------------------------
MAC Address       VLAN  IP              Interface    AS Name
-------------------------------------------------------------------------------
xxxx-xxxx-xxx1    212   1.1.1.1         Ge1/0/1      test1
xxxx-xxxx-xxx2    212   1.1.1.2         Ge1/0/1      test1
xxxx-xxxx-xxx3    212   1.1.1.3         Ge1/0/1      test1
xxxx-xxxx-xxx4    212   1.1.1.4         Ge1/0/1      test1
xxxx-xxxx-xxx5    212   1.1.1.5         Ge1/0/1      test1
-------------------------------------------------------------------------------
```

Table 3-100 Description of the **display uni-mng authen-user** command output

Item	Description
Total	Total number of authenticated users on an AS.
MAC Address	MAC address of an authenticated user.
VLAN	VLAN that an authenticated user belongs to.
IP	IP address of an authenticated user. **NOTE** If this command is run on an AS, this field is displayed as **--**.

Item	Description
Interface	Interface to which an authenticated user is connected.
AS Name	Name of an AS.

3.5.47 display uni-mng commit-result

Function

The **display uni-mng commit-result** command displays the configuration delivery result.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng commit-result { **profile** | **free-rule** | **as-direct-config** }

Parameters

Parameter	Description	Value
profile	Displays the delivery result of the service profile configuration.	-
free-rule	Displays the delivery result of user authenticate-free rules.	-
as-direct-config	Displays the direct configuration recovery result after an AS goes online.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng commit-result** command to check the result of delivering the configuration to an AS, including the service profiles configured on the parent, user authentication-free rules, and configurations directly delivered to ASs. This command displays only the latest result but not historical information.

Example

Display the result of delivering the service profile configuration to an AS.

```
<HUAWEI> display uni-mng commit-result profile
Result of profile:
--------------------------------------------------------------------------------
 AS Name                        Commit Time              Commit/Execute Result
--------------------------------------------------------------------------------
 as1                        2014-09-16 14:38:03       Success/Success
--------------------------------------------------------------------------------
```

Table 3-101 Description of the **display uni-mng commit-result profile** command output

Item	Description
AS Name	Name of an AS.
Commit Time	Time when the configuration is delivered.
Commit/Execute Result	Commit Result indicates the configuration delivery result: ● Success: The configuration is delivered successfully. ● Failed: The configuration fails to be delivered. ● Committing: The configuration is being delivered. Execute Result indicates the execution result of the delivered configuration: ● Success: The configuration is executed successfully. ● Failed: The configuration fails to be executed. ● Executing: The configuration is being executed.

3.5.48 display uni-mng global

Function

The **display uni-mng global** command displays the global configuration of SVF.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng global** command to view the globally configured service functions of SVF.

Example

Display the global configuration of SVF.

```
<HUAWEI> display uni-mng global
Forward-mode : Centralized
Portal url encode : Disable
IGMP snooping VLAN : 10
Authorization VLAN : 23
Authentication configuration revert : Disabled
```

Table 3-102 Description of the **display uni-mng global** command output

Item	Description
Forward-mode	SVF forwarding mode: - Distributed: distributed forwarding. In distributed forwarding, local traffic of an AS can be forwarded from the AS, and traffic between ASs is sent to the parent for forwarding. - Centralized: centralized forwarding. In centralized forwarding mode, both traffic forwarded by the local AS and traffic forwarded between ASs are sent to the parent for forwarding.
Portal url encode	Whether URL encoding is enabled: - Disable: URL encoding is disabled. - Enable: URL encoding is enabled. To disable URL encoding, run the **portal url-encode disable** command.

Item	Description
IGMP snooping VLAN	Service VLAN in which IGMP snooping is enabled. To configure a service VLAN in which IGMP snooping is enabled, run the **as service-vlan igmp-snooping** command. If no service VLAN is configured, this field is not displayed.
Authorization VLAN	Create the service VLAN for ASs. To create the service VLAN, run **as service-vlan authorization** command.
Authentication configuration revert	Whether the function retaining the authentication configuration after an AS goes offline is enabled. To disable the function, run the **as authentication configuration revert disable** command.

3.5.49 display uni-mng indirect configuration

Function

The **display uni-mng indirect configuration** command displays the indirect connection configuration on ASs.

NOTE

This command can only be executed on an AS.

Format

display uni-mng indirect configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng indirect configuration** command on an AS to check the indirect connection configuration on the AS.

Example

Display the SVF indirect connection configuration on an AS.

```
<HUAWEI> display uni-mng indirect configuration
Uni-mng configuration information:
 Current uni-mng status      : disable
 Next uni-mng status         : enable
 Current management VLAN     : --
 Next management VLAN        : 100
 Current fabric-port members :
 Next fabric-port members    :
  GigabitEthernet0/0/9
```

Table 3-103 Description of the **display uni-mng indirect configuration** command output

Item	Description
Current uni-mng status	Current manually configured client mode.
Next uni-mng status	Next startup manually configured client mode. To configure the client mode and management VLAN, run the **uni-mng indirect mng-vlan** command.
Current management VLAN	Current management VLAN. To configure the client mode and management VLAN, run the **uni-mng indirect mng-vlan** command.
Next management VLAN	Next startup management VLAN.
Current fabric-port members	Current member port configuration in a fabric port. To configure member ports for a fabric port, run the **uni-mng indirect fabric-port** command.
Next fabric-port members	Next startup member port configuration in a fabric port.

3.5.50 display uni-mng execute-failed-record

Function

The **display uni-mng execute-failed-record** command displays execution failure records after the configuration is delivered to an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng execute-failed-record { **profile** | **as-direct-config** } **as name** *as-name*

Parameters

Parameter	Description	Value
profile	Displays records of configurations delivered through profiles.	-
as-direct-config	Displays records of configurations directly delivered through commands.	-
as name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng execute-failed-record** command to check execution failure records after the configuration is delivered to an AS.

Example

Display execution failure records after the configuration is delivered to an AS.

```
<HUAWEI> display uni-mng execute-failed-record as-direct-config as name as1
Info: This operation may take a few seconds. Please wait....done.
--------------------------------------------------------------------------------
View name     : system
Command       : arp speed-limit source-mac maximum
1
Execute time  : 2015-01-19 15:09:23 DST
Failed reason : This device does not support this
command.
--------------------------------------------------------------------------------
```

Table 3-104 Description of the **display uni-mng execute-failed-record as-direct-config** command output

Item	Description
View name	View in which the configuration is executed.
Command	Command that failed to be executed.
Execute Time	Time the configuration is executed.
Failed reason	Cause of the execution failure.

3.5.51 display uni-mng interface fabric-port configuration

Function

The **display uni-mng interface fabric-port configuration** command displays the fabric port configuration.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng interface fabric-port configuration [**parent** | **as name** *as-name*]

Parameters

Parameter	Description	Value
parent	Display the parent-side fabric port configuration.	-
as name *as-name*	Display the AS-side fabric port configuration. If **parent** and *as-name* are not specified, the configurations of all the fabric ports in an SVF system are displayed.	The value must have an existing AS name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng interface fabric-port configuration** command to check the fabric port configuration.

Example

Display the fabric port configuration.

```
<HUAWEI> display uni-mng interface fabric-port configuration
Interface      Direction  Connect-type  Member-name
Location
-------------------------------------------------------------------------------
Fabric-port0   Down       Direct        Eth-Trunk0   Parent
Fabric-port1   Down       Direct        Eth-Trunk1   Parent
Fabric-port3   Down       Direct        Eth-Trunk3   Parent
Fabric-port5   Down       Direct        Eth-Trunk5   Parent
Fabric-port6   Down       Direct        Eth-Trunk6   Parent
Fabric-port7   Down       Direct        Eth-Trunk7   Parent
Fabric-port8   Down       Direct        Eth-Trunk8   Parent
Fabric-port9   Down       Indirect      Eth-Trunk9   Parent
Fabric-port10  Down       Indirect      Eth-Trunk10  Parent
Fabric-port11  Down       Direct        Eth-Trunk11  Parent
Fabric-port15  Down       Direct        Eth-Trunk15  Parent
-------------------------------------------------------------------------------
Total : 11
```

Table 3-105 Description of the **display uni-mng interface fabric-port configuration** command output

Item	Description
Interface	Fabric port name.
Direction	Direction of a fabric port. Down indicates downlink and Up indicates uplink.
Connect-type	Connection mode of a fabric port. Direct indicates the direct connection mode, whereas Indirect indicates the indirect connection mode (connection through an intermediate network).
Member-name	Eth-Trunk to which a fabric port is bound.
Location	Device where a fabric port resides.

3.5.52 display uni-mng interface fabric-port state

Function

The **display uni-mng interface fabric-port state** command displays the fabric port status.

NOTE

This command can be used on the parent or an AS. After running this command, you can check the fabric port status on the local device.

Format

display uni-mng interface fabric-port [*port-id*] **state**

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port. If this parameter is not specified, the status of all fabric ports is displayed.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng interface fabric-port state** command to check the fabric port status.

- If an AS connects to the parent through an intermediate network, peer fabric port information cannot be obtained and displays --.
- If a fabric port is incorrectly connected, the system displays an error summary message to provide the cause of the error.

Example

Display the fabric port status on the parent.

```
<HUAWEI> display uni-mng interface fabric-port state
--------------------------------------------------------------------------------
Fabric-port name             : Fabric-port1
Fabric-port direction        : Down
Fabric-port member name      : Eth-Trunk1

Peer MAC                     : xxxx-xxxx-xxxx
Peer AS name                 : as1
Peer fabric-port member name : Eth-Trunk0

Physical member number       : 1
Local-port    Peer-port    State     Detail                    Exptime(s)
XGE6/0/3      XGE0/0/1     Connected None                            32
--------------------------------------------------------------------------------
```

Table 3-106 Description of the **display uni-mng interface fabric-port state** command output

Item	Description
Fabric-port name	Fabric port name.
Fabric-port direction	Direction of a fabric port. Down indicates downlink and Up indicates uplink.
Fabric-port member name	Eth-Trunk to which a fabric port is bound.
Peer MAC	MAC address of the peer device.
Peer AS name	Name of the peer device.
Peer fabric-port member name	Eth-Trunk to which the peer fabric port is bound.
Physical member number	Number of member ports in a fabric port.
Local-port	Local member port.
Peer-port	Peer member port.
State	Port connection status: ● Init: initialization state ● Config: negotiation state ● Error: negotiation error state ● Connected: connected state ● unknown: unknown state
Detail	Detailed information when the port connection state is Error. For error reasons and solutions, see **Table 3-107**.
Exptime(s)	Timeout period of link heartbeat packets, in seconds.

Table 3-107 Error reasons indicated by the **Detail** field and solutions

Detail Field	Meaning	Solution
Startup cfg file exists	The AS has a startup configuration file.	Clear the startup configuration file and restart the AS.

Detail Field	Meaning	Solution
Console input exists	Input exists on the console interface of an AS.	Restart the AS and do not log in to the console interface immediately after the AS is restarted.
VLAN for VCMP exists	The VLAN for VCMP exists on the AS.	Run the **reset vcmp** command on the AS to restart the AS.
Port not supported	The AS attempts to connect to the parent through an unsupported port.	Connect the AS to the parent through an uplink port or subcard port.
Fabric-port linked to multi-AS	Member ports of the same downlink fabric port connect to two ASs.	Member ports of a downlink fabric port can connect to only one AS, and different ASs must connect to different fabric ports.
Parent exists already	The AS connects to two parent switches.	Disconnect the AS from one parent switch.
Linked to multi fabric-port	The uplink port of the AS connects to multiple fabric ports of the parent.	Ensure that the AS connects to only one fabric port of the parent and disconnect the AS from other fabric ports.
Level-1 AS linked to level-1 AS	The downlink fabric port of a level-1 AS connects to another level-1 AS.	Disconnect the two level-1 ASs from each other.
Parent linked to level-2 AS	The parent directly connects to a level-2 AS.	Disconnect the parent from the level-2 AS.
Downstream fabric-port linked	A downlink fabric port of an AS connects to the parent.	Disconnect the fabric port of the AS from the parent.
No response received	The parent does not receive any response packet.	● Ensure that the parent is a Huawei switch that supports the SVF function. ● Ensure that the AS starts without configuration. ● Ensure that physical ports that connect the AS to the parent are of the same type.

Detail Field	Meaning	Solution
Failed to create Eth-Trunk	Failed to create an Eth-Trunk on an AS.	Disconnect the AS from the parent and then reconnect them.
Failed to bind trunk	Failed to add ports of an AS to an Eth-Trunk.	Disconnect the AS from the parent and then reconnect them.
Force Uni-mng mode	An AS has been configured to work in client mode.	On the parent, configure the indirect connection mode for the fabric port that connects to the AS. Alternative, run the **undo uni-mng enable** command on the AS and restart the AS to enable it exit from the client mode.
Parent linked to parent	The fabric port of the parent connects to another parent.	Disconnect the fabric port from the remote parent.
System is busy on AS	The system is busy on the AS.	Wait until the AS is idle.
Linked to AS with IPv4-hardware	When an S5700-10P-LI, S5700-10P-PWR-LI-AC, or S2750-EI functions as an AS, Layer 3 hardware forwarding for IPv4 packets has been enabled using the **assign forward-mode ipv4-hardware** command.	Disable Layer 3 hardware forwarding for IPv4 packets.
Configurations exist on port	Configurations exist on the port of an AS.	Delete the configurations of the port.
Invalid stack config exists	Downlink service port of AS is configured as a stack port.	Clear the stack configuration of the downlink service port.

3.5.53 display uni-mng port-group

Function

The **display uni-mng port-group** command displays information about port groups.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng port-group [**name** *group-name* | **verbose**]

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a port group.	The value must be an existing a port group name.
verbose	Displays detailed information about a port group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng port-group** command to check information about created port groups.

Example

Display brief information about all port groups.

```
<HUAWEI> display uni-mng port-group

------------------------------------------------------------------------------
 Number              Port-group Name                Port-group Type
------------------------------------------------------------------------------
 1                group1                      connect to user
 2                ap_group1                     connect to AP
------------------------------------------------------------------------------
```

Table 3-108 Description of the **display uni-mng port-group** command output

Item	Description
Number	Sequence number.
Port-group Name	Port group name.

Item	Description
Port-group Type	Port group type: ● connect to user: port connected to a terminal user ● connect to AP: port connected to an AP

Display detailed information about all port groups.

```
<HUAWEI> display uni-mng port-group verbose

-------------------------------------------------------------------------------
Port-group name                  : ap
Port-group type                  : connect to AP
Interface list                   :
 AS name as1 interface Eth-trunk 5 GigabitEthernet 0/0/2
Network-basic profile            : qos
Network-enhanced profile         : net
Network-qos profile              : test
Traffic-policy profile           : test(inbound)
User-access profile              : access_profile
-------------------------------------------------------------------------------
Port-group name                  : group_2
Port-group type                  : connect to user
Interface list                   :
 AS name as1 interface Eth-trunk 4 GigabitEthernet 0/0/10
Network-basic profile            : --
Network-enhanced profile         : --
Network-qos profile              : --
Traffic-policy profile           : --

User-access profile              : --
-------------------------------------------------------------------------------
```

Table 3-109 Description of the **display uni-mng port-group verbose** command output

Item	Description
Port-group name	Port group name.
Port-group type	Port group type: ● connect to user: port connected to a terminal user ● connect to AP: port connected to an AP
Interface list	List of member ports added to a port group.
Network-basic profile	Name of the network basic profile bound to the port group. When no network basic profile is bound to the port group, this field displays --.

Item	Description
Network-enhanced profile	Name of the network enhanced profile bound to the port group. When no network enhanced profile is bound to the port group, this field displays --.
Network-qos profile	Name of the network QoS profile bound to the port group. When no network QoS profile is bound to the port group, this field displays --.
Traffic-policy profile	Name of the traffic policy profile bound to the port group. When no traffic policy profile is bound to the port group, this field displays --.
User-access profile	Name of the user access profile bound to the port group. When no user access profile is bound to the port group, this field displays --.

3.5.54 display uni-mng profile

Function

The **display uni-mng profile** command displays service profile information.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng profile [{ **as-admin** | **network-basic** | **network-enhanced** | **user-access** | **network-qos** | **traffic-policy** } [**name** *profile-name*]]

Parameters

Parameter	Description	Value
as-admin	Displays information about AS administrator profiles.	-
network-basic	Displays information about network basic profiles.	-
network-enhanced	Displays information about network enhanced profiles.	-

Parameter	Description	Value
user-access	Displays information about user access profiles.	-
network-qos	Displays information about network qos profiles.	-
traffic-policy	Displays information about traffic policy profiles.	-
name *profile-name*	Specifies the name of a service profile. If this parameter is specified, you can check information about services configured in a specified profile.	The profile must have an existing profile name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng profile** command to check information about created service profiles.

Example

Display brief information about all service profiles.

```
<HUAWEI> display uni-mng profile

AS-admin profile:
-------------------------------------------------------------------------------
 Number                         Profile Name
-------------------------------------------------------------------------------
 1                          hehe
 2                          profile_1
-------------------------------------------------------------------------------

Network-basic profile:
-------------------------------------------------------------------------------
 Number                         Profile Name
-------------------------------------------------------------------------------
 1                          b_pro
 2                          p
-------------------------------------------------------------------------------

Network-enhanced profile:
-------------------------------------------------------------------------------
 Number                         Profile Name
-------------------------------------------------------------------------------
 1                          enp
```

```
-------------------------------------------------------------------------------

Network-qos profile:
-------------------------------------------------------------------------------
 Number                        Profile Name
-------------------------------------------------------------------------------
 1                          test
-------------------------------------------------------------------------------

Traffic-policy profile:
-------------------------------------------------------------------------------
 Number                        Profile Name
-------------------------------------------------------------------------------
 1                          12341
 2                          123410
 3                          123411
-------------------------------------------------------------------------------

User-access profile:
-------------------------------------------------------------------------------
 Number                        Profile Name
-------------------------------------------------------------------------------
 1                          u_pro
-------------------------------------------------------------------------------
```

Table 3-110 Description of the **display uni-mng profile** command output

Item	Description
Number	Sequence number.
Profile Name	Name of each profile type.
AS-admin profile	AS administrator profile created using the **as-admin-profile name** command.
Network-basic profile	Network basic profile created using the **network-basic-profile name** command.
Network-enhanced profile	Network enhanced profile created using the **network-enhanced-profile name** command.
Network-qos profile	Network qos profile created using the **network-qos-profile name** command.
Traffic-policy profile	Traffic policy profile created using the **traffic-policy-profile name** command.
User-access profile	User access profile created using the **user-access-profile name** command.

Display information about the service profile with a specified name.

```
<HUAWEI> display uni-mng profile network-basic name basic

-------------------------------------------------------------------------------
Profile name: basic
 User-vlan                  : 110
```

```
Voice-vlan              : 114
Pass-vlan               : 1 112 to 113
------------------------------------------------------------------------------
```

Table 3-111 Description of the **display uni-mng profile network-basic name** command output

Item	Description
Profile name	Name of a service profile.
User-vlan	Default VLAN configured in a service profile. To configure a default VLAN, run the **user-vlan** command. By default, VLAN 1 is a default VLAN.
Voice-vlan	Voice VLAN configured in a service profile. To configure a voice VLAN, run the **voice-vlan** command. If no voice VLAN is configured, this field displays --.
Pass-vlan	Allowed VLAN configured in a service profile. To configure an allowed VLAN, run the **pass-vlan** command. By default, only VLAN 1 is allowed.

3.5.55 display uni-mng profile as

Function

The **display uni-mng profile as** command displays the configuration generated after an AS is bound to service profiles.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng profile as name *as-name* [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.
interface *interface-type interface-number*	Displays the configuration of a specified interface: ● *interface-type* specifies the interface type. The interface type can be a physical interface, an Eth-Trunk, or a fabric port. ● *interface-number* specifies the interface number. If this parameter is not specified, the configurations of all the service interfaces on an AS are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng profile as** command to check the configuration generated after an AS is bound to service profiles.

If a fabric port is specified, this command displays only the network QoS profile configuration.

Example

Display the configuration generated on an AS.

```
<HUAWEI> display uni-mng profile as name as1

Global
-------------------------------------------------------------------------------
 Centralized forward mode: disable
-------------------------------------------------------------------------------
 Portal url-encode: enable
-------------------------------------------------------------------------------
 Igmp-vlan                    : --
-------------------------------------------------------------------------------
 Authorization-vlan           : --
-------------------------------------------------------------------------------
AS-group name: xy
 Username: admin
  Privilege-level   : 3
```

```
  Service-type       : terminal ssh
  Bpdu-protection    : --
  Ipv6               : --
  Acl number         : 3000 3002 3011 3012 3013 3014 3015 3016 3017 3018
 Traffic-limit outbound ARP(Kbps)  : 512
 Traffic-limit outbound DHCP(Kbps) : 128
-------------------------------------------------------------------------------

Interface fabric-port 0
-------------------------------------------------------------------------------
Port-group name: --
 Trust Flag                        : --
 Scheduling Profile                : --
 Scheduling Mode                   : --
  Weight of Queue 0                : --
  Weight of Queue 1                : --
  Weight of Queue 2                : --
  Weight of Queue 3                : --
  Weight of Queue 4                : --
  Weight of Queue 5                : --
  Weight of Queue 6                : --
  Weight of Queue 7                : --
-------------------------------------------------------------------------------

Interface GigabitEthernet0/0/1
-------------------------------------------------------------------------------
Port-group name: --
 User-vlan                         : --
 Voice-vlan                        : --
 Pass-vlan                         : --

 Priority-trust                    : disable
 User-access-port                  : disable
 DHCP snooping                     : disable
 IP source check                   : disable
 ARP anti-attack check             : disable
 Unicast-suppression(pps)          : --
 Multicast-suppression(pps)        : --
 Broadcast-suppression(pps)        : --
 Rate-limit(Kbps)                  : --
 Port-security                     : disable
 Mac-address sticky                : disable
 Port-security aging-time          : --

 Trust Flag                        : dscp
 Scheduling Profile                : qos
 Scheduling Mode                   : wrr
  Weight of Queue 0                : --
  Weight of Queue 1                : 6
  Weight of Queue 2                : --
  Weight of Queue 3                : --
  Weight of Queue 4                : --
  Weight of Queue 5                : --
  Weight of Queue 6                : --
  Weight of Queue 7                : --

 Authentication                    : --
 Authentication maximum user-num  : --
 MAC-limit                         : --
 Traffic-limit inbound ARP(Kbps)  : --
 Traffic-limit inbound DHCP(Kbps) : --

 Traffic policy profile            : --
-------------------------------------------------------------------------------

Interface GigabitEthernet0/0/2
-------------------------------------------------------------------------------
Port-group name: --
 User-vlan                         : --
```

```
Voice-vlan                     : --
Pass-vlan                      : --

Priority-trust                 : disable
User-access-port               : disable
DHCP snooping                  : disable
IP source check                : disable
ARP anti-attack check          : disable
Unicast-suppression(pps)       : --
Multicast-suppression(pps)     : --
Broadcast-suppression(pps)     : --
Rate-limit(Kbps)               : --
Port-security                  : disable
Mac-address sticky             : disable
Port-security aging-time       : --

Trust Flag                     : dscp
Scheduling Profile             : qos
Scheduling Mode                : wrr
 Weight of Queue 0             : --
 Weight of Queue 1             : 6
 Weight of Queue 2             : --
 Weight of Queue 3             : --
 Weight of Queue 4             : --
 Weight of Queue 5             : --
 Weight of Queue 6             : --
 Weight of Queue 7             : --

Authentication                 : --
Authentication maximum user-num  : --
MAC-limit                      : --
Traffic-limit inbound ARP(Kbps)  : --
Traffic-limit inbound DHCP(Kbps) : --

Traffic policy profile         : --
-------------------------------------------------------------------------------
......
```

Table 3-112 Description of the **display uni-mng profile as** command output

Item	Description
Global	Global AS configuration.
Centralized forward mode	Whether centralized forwarding is enabled: ● disable: Centralized forwarding is disabled, and distributed forwarding is used currently. ● enable: Centralized forwarding is enabled. To configure centralized forwarding, run the **forward-mode centralized** command. By default, distributed forwarding is used.

Item	Description
Portal url-encode	Whether URL encoding is enabled for an AS: ● disable: URL encoding is disabled for the AS. ● enable: URL encoding is enabled for the AS. To disable URL encoding for an AS, run the **portal url-encode disable** command. By default, URL encoding is enabled for an AS.
Igmp-vlan	VLAN in which IGMP Snooping is enabled. If no VLAN is configured, this field displays --. To configure the VLAN, run the **as service-vlan igmp-snooping** command.
Authorization-vlan	Service VLAN created on an AS. If no VLAN is configured, this field displays --. To configure the service VLAN, run the **as service-vlan authorization** command.
AS-group name	Name of the AS group to which an AS belongs.
Username	AS administrator user name. If no AS administrator user name is configured, this field displays --. AS administrator user name configured in the AS administrator profile bound to an AS group. To configure an AS administrator user name, run the **user password** command.
Privilege-level	User level. The value is 3 and cannot be changed.
Service-type	User access type. The value is terminal ssh and cannot be changed.
Bpdu-protection	BPDU protection status of an AS. If BPDU protection is not configured, this field displays --.
Ipv6	Whether IPv6 is enabled on an AS.
Acl number	ACL number created on an AS.

Item	Description
Traffic-limit outbound ARP(Kbps)	Outbound ARP packet rate limit of the uplink fabric port of an AS, in kbit/s. To set the outbound ARP packet rate limit, run the **traffic-limit outbound** command.
Traffic-limit outbound DHCP(Kbps)	Outbound DHCP packet rate limit of the uplink fabric port of an AS, in kbit/s. To set the outbound ARP packet rate limit, run the **traffic-limit outbound** command.
Interface GigabitEthernet0/0/1 Interface GigabitEthernet0/0/2 Interface fabric-port 0	Interface name.
Port-group name	Name of the port group to which an interface belongs. If an interface is not added to any port group, this field displays -- or disable.
User-vlan	Default VLAN. To configure a default VLAN, run the **user-vlan** command.
Voice-vlan	Voice VLAN. To configure a voice VLAN, run the **voice-vlan** command.
Pass-vlan	Allowed VLAN. To configure an allowed VLAN, run the **pass-vlan** command.
Priority-trust	Whether the priority trust function is enabled: ● disable: The priority trust function is disabled in a network enhanced profile. ● enable: The priority trust function is enabled in a network enhanced profile.

Item	Description
User-access-port	Whether the edge port function is enabled: ● disable: The edge port function is disabled in a network enhanced profile. ● enable: The edge port function is enabled in a network enhanced profile. To enable the edge port function, run the **user-access-port enable** command.
DHCP snooping	Whether DHCP snooping is enabled: ● disable: DHCP snooping is disabled in a network enhanced profile. ● enable: DHCP snooping is enabled in a network enhanced profile. To enable DHCP snooping, run the **dhcp snooping enable** command.
IP source check	Whether the IP packet check function is enabled: ● disable: IP packet check is disabled in a network enhanced profile. ● enable: IP packet check is enabled in a network enhanced profile. To enable IP packet check, run the **ip source check user-bind enable** command.
ARP anti-attack check	Whether the dynamic ARP inspection function is enabled: ● disable: The dynamic ARP inspection function is disabled in a network enhanced profile. ● enable: The dynamic ARP inspection function is enabled in a network enhanced profile. To enable the dynamic ARP inspection function, run the **arp anti-attack check user-bind enable** command.
Unicast-suppression(pps)	Rate limit for unknown unicast traffic, in pps. To set the rate limit for unknown unicast traffic, run the **unicast-suppression** command.

Item	Description
Multicast-suppression(pps)	Rate limit for multicast traffic, in pps. To set the rate limit for multicast traffic, run the **multicast-suppression** command.
Broadcast-suppression(pps)	Rate limit for broadcast traffic, in pps. To set the rate limit for broadcast traffic, run the **broadcast-suppression** command.
Rate-limit(Kbps)	Traffic rate limit, in kbit/s. To set the traffic rate limit, run the **rate-limit** command.
Port-security	Whether port security is enabled. To enable the port security function, run the **port-security enable** command.
Mac-address sticky	Whether the sticky MAC function is enabled on an interface. To enable the sticky MAC function on an interface, run the **port-security mac-address sticky** command.
Port-security aging-time	Aging time of secure dynamic MAC addresses on an interface. To set this parameter, run the **port-security aging-time** command.
Trust Flag	Packet priority mapping flag. To configure priority mapping, run the **trust dscp** command.
Scheduling Profile	Name of a network QoS profile.
Scheduling Mode	Queue scheduling mode. To configure the queue scheduling mode, run the **qos { pq | wrr | drr }** command.

Item	Description
Weight of Queue 0 Weight of Queue 1 Weight of Queue 2 Weight of Queue 3 Weight of Queue 4 Weight of Queue 5 Weight of Queue 6 Weight of Queue 7	Queue scheduling weight. To configure the queue scheduling weight, run the **qos queue** command.
Authentication	User authentication profile created using the **authentication-profile** command.
Authentication maximum user-num	Maximum number of access users configured in a user access profile. To set this parameter, run the **authentication access-user maximum** command.
MAC-limit	MAC address learning limit. To set the MAC address learning limit, run the **mac-limit** command.
Traffic-limit inbound ARP(Kbps)	Inbound ARP packet rate limit of an AS port, in kbit/s. To set the inbound ARP packet rate limit, run the **traffic-limit inbound** command.
Traffic-limit inbound DHCP(Kbps)	Inbound DHCP packet rate limit of an AS port, in kbit/s. To set the inbound ARP packet rate limit, run the **traffic-limit inbound** command.
Traffic policy profile	Name of the traffic policy profile bound to an AS.

3.5.56 display uni-mng topology configuration

Function

The **display uni-mng topology configuration** command displays the SVF network topology collection configuration.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng topology configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng topology configuration** command to check the SVF network topology collection configuration.

Example

Display the SVF network topology collection configuration.

```
<HUAWEI> display uni-mng topology configuration
Explore timer: 10 minutes
Last collection time: 10:03:58 UTC+00:00 2014/09/11
Total time for last collection: 9 ms
```

Table 3-113 Description of the **display uni-mng topology configuration** command output

Item	Description
Explore timer	Network topology collection interval. To set the network topology collection interval, run the **topology explore** command.
Last collection time	Last time the SVF network topology is collected.
Total time for last collection	Time taken to collect the SVF network topology.

3.5.57 display uni-mng topology information

Function

The **display uni-mng topology information** command displays SVF network topology information.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng topology information [**by-name**]

Parameters

Parameter	Description	Value
by-name	Displays SVF network topology information based on the device name. If this parameter is not specified, SVF network topology information is displayed based on the MAC address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng topology information** command to check SVF network topology information.

Example

Display SVF network topology information.

```
<HUAWEI> display uni-mng topology information
The topology information of uni-mng network:
<-->: direct link        <??>: indirect link
T: Trunk ID                *: independent AS
------------------------------------------------------------------------------
 Local MAC       Hop  Local Port      T  ||  T   Peer Port      Peer MAC
------------------------------------------------------------------------------
 00e0-fc12-7890  0    GE6/1/0         11 <-->0   GE0/0/26       00e0-fc12-0008 *
 00e0-fc12-0008  1    GE0/0/2         -- <-->--  GE0/0/0        00e0-fc12-0005
------------------------------------------------------------------------------
Total items displayed : 2
```

Display SVF network topology information based on the device name.

```
<HUAWEI> display uni-mng topology information by-name
The topology information of uni-mng network:
<-->: direct link        <??>: indirect link
T: Trunk ID              *: independent AS
--------------------------------------------------------------------------------------------------------------
 Local Dev                        Hop  Local Port      T  ||  T   Peer Port      Peer Dev
--------------------------------------------------------------------------------------------------------------
 100-S1                           0    GE6/1/0         1  <-->0   GE0/0/26       as1 *
```

```
 as1                          1    GE0/0/2         -- <-->--  GE0/0/0       ap-1
------------------------------------------------------------------------------------------------------------------
Total items displayed : 2
```

Table 3-114 Description of the **display uni-mng topology information** command output

Item	Description
Local MAC	MAC address of the local device. If **by-name** is specified, this field displays **Local Dev**, indicating the device name.
Hop	Hierarchy of a device on the SVF network: ● 0: the parent ● 1: level-1 AS ● 2: level-2 AS
Local Port	Local physical port. When two devices are indirectly connected, port information cannot be displayed because ports are not indirectly connected.
T	ID of the Eth-Trunk to which a physical port belongs.
||	Whether two devices are directly connected: ● <-->: indicates that two devices are directly connected. ● <??>: indicates that two devices are indirectly connected. For example, two devices are connected through other networks.
Peer Port	Peer physical port. When two devices are indirectly connected, port information cannot be displayed because ports are not indirectly connected.
Peer MAC	MAC address of the peer device. If **by-name** is specified, this field displays **Peer Dev**, indicating the device name. If * is displayed, the AS is configured in the independent mode.
Local Dev	Local device name.

Item	Description
Peer Dev	Peer device name. If * is displayed, the AS is configured in the independent mode.

3.5.58 display uni-mng unauthen-user

Function

The **display uni-mng unauthen-user** command displays information about non-authenticated users on an AS.

NOTE

This command can be used on the parent or an AS.

Format

display uni-mng unauthen-user [**as name** *as-name* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS. **NOTE** This parameter is supported only on the parent.	The value is a string of 1 to 31 case-insensitive characters without spaces.
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about non-authenticated users on an AS, run the **display uni-mng unauthen-user** command.

Example

Display information about non-authenticated users on the AS **test1**.

```
<HUAWEI> display uni-mng unauthen-user as name test1
Total: 5
-------------------------------------------------------------------------------
MAC Address      VLAN  IP            Interface    AS Name
-------------------------------------------------------------------------------
xxxx-xxxx-xxx2   212   1.1.1.1       Ge1/0/1      test1
xxxx-xxxx-xxx3   212   1.1.1.2       Ge1/0/1      test1
xxxx-xxxx-xxx4   212   1.1.1.3       Ge1/0/1      test1
xxxx-xxxx-xxx5   212   1.1.1.4       Ge1/0/1      test1
xxxx-xxxx-xxx6   212   1.1.1.5       Ge1/0/1      test1
-------------------------------------------------------------------------------
```

Table 3-115 Description of the **display uni-mng unauthen-user** command output

Item	Description
Total	Number of non-authenticated users on an AS.
MAC Address	MAC address of a non-authenticated user.
VLAN	VLAN to which a non-authenticated user belongs.
IP	IP address of a non-authenticated user. **NOTE** When this command is run on the AS, this field is displayed as --.
Interface	Access interface of a non-authenticated user.
AS Name	Name of an AS.

3.5.59 display uni-mng unauthen-user offline-record

Function

The **display uni-mng unauthen-user offline-record** command displays offline records of non-authenticated users on an AS.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng unauthen-user offline-record [**as name** *as-name* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS.	The value is a string of 1 to 31 case-insensitive characters without spaces.
mac-address *mac-address*	Specifies the MAC address of an AS.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view offline records of non-authenticated users on an AS, run the **display uni-mng unauthen-user offline-record** command.

Example

Display offline records of non-authenticated users on the AS **test1**.

```
<HUAWEI> display uni-mng unauthen-user offline-record as name test1
Total: 2
-------------------------------------------------------------------------------
 AS name               : test1
 User MAC              : 00e0-fc46-b67c
 User VLAN             : 212
 User access interface : Ge1/0/2
 User IP address       : 192.168.1.1
 User offline time     : 2016/01/21 04:59:43
 User offline reason   : As offline
-------------------------------------------------------------------------------
 AS name               : test1
 User MAC              : 00e0-fc46-b67d
 User VLAN             : 212
 User access interface : Ge1/0/3
 User IP address       : 192.168.1.2
 User offline time     : 2016/01/21 05:59:43
 User offline reason   : User offline
-------------------------------------------------------------------------------
```

Table 3-116 Description of the **display uni-mng unauthen-user offline-record** command output

Item	Description
Total	Number of offline records of non-authenticated users on an AS.
AS name	Name of an AS.
User MAC	MAC address of a non-authenticated user.
User VLAN	VLAN to which a non-authenticated user belongs.
User access interface	Access interface of a non-authenticated user.
User IP address	IP address of a non-authenticated user.
User offline time	Time when a non-authenticated user goes offline.
User offline reason	Reason that a non-authenticated user goes offline. ● User offline: The user goes offline. ● AS offline: The AS is offline.

3.5.60 display uni-mng upgrade-info

Function

The **display uni-mng upgrade-info** command displays AS version upgrade information.

NOTE

This command can only be executed on a parent switch.

Format

display uni-mng upgrade-info [**as name** *as-name* | **verbose**]

Parameters

Parameter	Description	Value
as name *as-name*	Specifies the name of an AS.	The value must have an existing AS name.

Parameter	Description	Value
verbose	Displays detailed version upgrade information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng upgrade-info** command to check AS version upgrade information.

Example

Display AS version upgrade information.

```
<HUAWEI> display uni-mng upgrade-info
The total number of AS is : 1
-------------------------------------------------------------------------------
 Name                          Method      Phase      Status      Result
-------------------------------------------------------------------------------
 as1                         --          --         NO-UPGRADE  --
-------------------------------------------------------------------------------
```

Table 3-117 Description of the **display uni-mng upgrade-info** command output

Item	Description
Name	Name of an AS.
Method	AS upgrade mode: ● --: The upgrade task is not started. ● ver-sync: The AS is automatically upgraded when going online. ● upgrade: The AS is manually upgraded after going online.

Item	Description
Phase	Upgrade phase: - --: The upgrade task is not started. - sys-file: The system is determining whether to download the system software or is downloading the system software from the parent. - patch-file: The system is determining whether to download the patch file or is downloading the patch file from the parent. - waiting: The AS is waiting for activation. - activating: The AS is being activated. - rebooting: The AS is restarting.
Status	Whether the AS is being upgraded: - NO-UPGRADE: The AS is not upgraded. - UPGRADING: The AS is being upgraded.
Result	Upgrade result: - --: The upgrade task is not started. - successful: The upgrade is successful. - failed: The upgrade fails.

Display detailed AS version upgrade information.

```
<HUAWEI> display uni-mng upgrade-info verbose
The total number of AS is : 1
-------------------------------------------------------------------------------
 AS name                        : as1
 Work status                    : UPGRADING
 Startup system-software        : flash:/s5720-p-li-v200r021c00.cc
 Startup version                : V200R013C00
 Startup patch                  : --
 Next startup system-software   : flash:/s5720-p-li-v200r022c00spc500.cc
 Next startup patch             : --
 Download system-software       : s5720-p-li-v200r022c00spc500.cc
 Download version               : --
 Download patch                 : --
 Activating file time           : immediately
 Activating file method         : reload
 Method                         : upgrade
 Upgrading phase                : sys-file
 Last operation result          : --
 Error reason                   : --
 Last operation time            : --
-------------------------------------------------------------------------------
```

Display detailed information after an AS version upgrade is complete.

```
<HUAWEI> display uni-mng upgrade-info verbose
The total number of AS is : 1
-------------------------------------------------------------------------------
 AS name                       : as1
 Work status                   : NO-UPGRADE
 Startup system-software       : flash:/s5720-p-li-v200r022c00spc500.cc
 Startup version               : V200R022C00SPC500
 Startup patch                 : --
 Next startup system-software  : --
 Next startup patch            : --
 Download system-software      : --
 Download version              : --
 Download patch                : --
 Method                        : --
 Upgrading phase               : --
 Last operation result         : failed
 Error reason                  : The local file server has not been configured.
 Last operation time           : 2019-10-04  15:51:05
-------------------------------------------------------------------------------
```

Table 3-118 Description of the **display uni-mng upgrade-info verbose** command output

Item	Description
AS name	Name of an AS.
Work status	Whether the AS is being upgraded: ● NO-UPGRADE: The AS is not upgraded. ● UPGRADING: The AS is being upgraded.
Startup system-software	Running system software.
Startup version	Current software version.
Startup patch	Running patch file. If this field displays --, no patch file is running.
Next startup system-software	System software that is configured for the next startup. If this field displays --, no system software is configured for the next startup.
Next startup patch	Patch package file that is configured for the next startup. If this field displays --, no patch package file is configured for the next startup.
Download system-software	Downloaded system software. If this field displays --, the upgrade task is not started.
Download version	Downloaded system software version. If this field displays --, the upgrade task is not started.

Item	Description
Download patch	Downloaded patch file. If this field displays --, the upgrade task is not started.
Activating file time	Activation time after the AS system software is downloaded. ● at **xxx**: The downloaded AS system software is activated at the specified time. ● delay **xxx**: The downloaded AS system software is activated after the specified delay time. ● immediately: The AS system software is activated immediately after being downloaded.
Activating file method	Mode in which the AS system software is activated: ● reload: The AS system software is activated by restarting the AS. ● default: The AS system software is activated without restarting the AS.
Method	AS upgrade mode: ● --: The upgrade task is not started. ● ver-sync: The AS is automatically upgraded when going online. ● upgrade: The AS is manually upgraded after going online.
Upgrading phase	Upgrade phase: ● --: The upgrade task is not started. ● sys-file: The system is determining whether to download the system software or is downloading the system software from the parent. ● patch-file: The system is determining whether to download the patch file or is downloading the patch file from the parent. ● waiting: The AS is waiting for activation. ● activating: The AS is being activated. ● rebooting: The AS is restarting.

Item	Description
Last operation result	Upgrade result: - --: The upgrade task is not started. - successful: The upgrade is successful. - failed: The upgrade fails.
Error reason	Upgrade failure reason.
Last operation time	Last time the AS is upgraded.

3.5.61 display uni-mng up-direction fabric-port

Function

The **display uni-mng up-direction fabric-port** command displays information about AS service ports added to an uplink fabric port.

NOTE

This command can only be executed on an AS.

Format

display uni-mng up-direction fabric-port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display uni-mng up-direction fabric-port** command to check the current and next startup configurations of AS service ports added to an uplink fabric port.

Example

Display information about AS service ports added to an uplink fabric port.

```
<HUAWEI> display uni-mng up-direction fabric-port
Uni-mng up-direction fabric-port configuration:
```

```
Current fabric-port members :
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/4
Next fabric-port members    :
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/4
```

Table 3-119 Description of the **display uni-mng up-direction fabric-port** command output

Item	Description
Uni-mng up-direction fabric-port configuration	Configuration of an uplink fabric port.
Current fabric-port members	Effective member interfaces of the uplink fabric port.
Next fabric-port members	Effective member interfaces of the uplink fabric port after the device's next startup.

3.5.62 down-direction fabric-port

Function

The **down-direction fabric-port** command configures the fabric port that connects a level-1 AS to a level-2 AS.

The **undo down-direction fabric-port** command deletes the fabric port that connects a level-1 AS to a level-2 AS.

By default, no fabric port that connects a level-1 AS to a level-2 AS is configured.

NOTE

This command can only be executed on a parent switch.

Format

down-direction fabric-port *port-id* **member-group interface eth-trunk** *trunk-id*

undo down-direction fabric-port *port-id* **member-group**

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port.	The value is an integer and must be set according to the device configuration.
member-group interface	Specifies the Eth-Trunk to which a fabric port is bound.	-
eth-trunk *trunk-id*	Specifies the ID of an Eth-Trunk.	The value is an integer that ranges from 1 to 63. **NOTE** If an Eth-Trunk has been created and configured on an AS in independent mode, the **eth-trunk** *trunk-id* parameter cannot be the same as the existing Eth-Trunk ID of this AS. Otherwise, this command cannot be delivered.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a level-1 AS needs to connect to a level-2 AS, you need to configure a fabric port on the level-1 AS to connect to the level-2 AS. A downlink port of a level-1 AS becomes Up only after the parent finishes delivering the configuration. A level-2 AS begins to go online only after the downlink port of the level-1 AS becomes Up.

Follow-up Procedure

Run the **port eth-trunk** *trunk-id* **trunkmember interface** *interface-type interface-number1* [**to** *interface-number2*] command to add member ports to the bound Eth-Trunk.

Example

Configure the fabric port that connects a level-1 AS to a level-2 AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] down-direction fabric-port 1 member-group interface eth-trunk 1
```

3.5.63 down-direction fabric-port connect independent-as

Function

The **down-direction fabric-port connect independent-as** command enables the independent mode on the fabric port that connects a level-1 AS to a level-2 AS.

The **undo down-direction fabric-port** command restores the default mode of the fabric port that connects a level-1 AS to a level-2 AS.

By default, the service configuration mode of the fabric port that connects a level-1 AS to a level-2 AS is centralized mode.

NOTE

This command can only be executed on a parent switch.

Format

down-direction fabric-port *port-id* **connect independent-as**

undo down-direction fabric-port *port-id* **connect**

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port.	The value is an integer and must be set according to the device configuration.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In independent mode, you can log in to an AS to configure this AS using commands. After the independent mode is enabled on the fabric port that connects a level-1 AS to a level-2 AS, the level-2 AS can be configured independently.

Prerequisites

The fabric port used to connect a level-1 AS to a level-2 AS has been created using the **down-direction fabric-port** *port-id* **member-group interface eth-trunk** *trunk-id* command in the AS view.

Precautions

Before enabling the independent mode, run the **independent-as-admin** command in the uni-mng view to configure an administrator for AS login. If no administrator is created, you can only log in to an AS through a console port.

If service configurations have been delivered in centralized mode to a level-1 AS port before this port is changed to the independent mode, this port cannot be configured as a fabric port that connects to a level-2 AS. To do so, restore the level-1 AS to the centralized mode and cancel the service configurations of this port on the parent.

In independent mode, when an AS goes offline, traffic on the network attached to an AS port cannot be forwarded if the port has authentication configurations. To enable the traffic to be forwarded normally, manually delete the authentication configurations from the port.

Example

Enable the independent mode on the fabric port that connects a level-1 AS to a level-2 AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] down-direction fabric-port 1 member-group interface eth-trunk 1
[HUAWEI-um-as-as1] down-direction fabric-port 1 connect independent-as
```

3.5.64 forward-mode centralized

Function

The **forward-mode centralized** command sets the forwarding mode of an SVF system to centralized forwarding.

The **undo forward-mode** command restores the default forwarding mode of an SVF system.

By default, the forwarding mode of an SVF system is distributed forwarding.

NOTE

This command can only be executed on a parent switch.

Format

forward-mode centralized

undo forward-mode

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SVF system uses the distributed forwarding mode by default. You can change the forwarding mode to centralized mode.

- In centralized forwarding mode, traffic forwarded by the local AS and forwarded between ASs is sent to the parent for forwarding.
- In distributed forwarding mode, an AS directly forwards local traffic and the parent forwards traffic between ASs.

Precautions

- After changing the SVF forwarding mode, you must run the **commit as** { **name** *as-name* | **all** } command to commit the configuration so that the device can deliver it to ASs.
- In centralized forwarding mode, ports of the ASs connected to the same fabric port of the parent are isolated and so cannot communicate at Layer 2, and need to have proxy ARP in the corresponding VLAN configured using the **arp-proxy inner-sub-vlan-proxy enable** command to communicate at Layer 3.
- In centralized forwarding mode, after an AS goes offline, traffic of its attached network cannot be forwarded by the parent and will be interrupted.
- In distributed forwarding mode, after an AS goes offline, in versions earlier than V200R012C00, downlink ports of the AS are automatically error down. As a result, traffic of the AS attached network will be interrupted. In V200R012C00 and later versions, downlink ports of the AS will not be error down, and traffic of the AS attached network will be forwarded as usual.

Example

Set the SVF forwarding mode to centralized forwarding.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] forward-mode centralized
```

3.5.65 independent-as-admin

Function

The **independent-as-admin** command creates an administrator for AS login in independent mode.

The **undo independent-as-admin** command deletes the administrator for AS login in independent mode.

By default, no administrator is created for AS login in independent mode.

NOTE

This command can only be executed on a parent switch.

Format

independent-as-admin user *user-name* **password** *password*

undo independent-as-admin user

Parameters

Parameter	Description	Value

user *user-name*	Specifies a user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		● Note the following when configuring case sensitivity for user names:
		  ● Only the user name is case-sensitive and the domain name is case-insensitive.
		  ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Parameter	Description	Value
password *password*	Specifies the password.	The value is a string of case-sensitive characters without spaces. A password in plain text is a string of 8 to 128 characters. A password in cipher text is a string of 48 to 188 characters and cannot be generated using the irreversible algorithm. The password is displayed in cipher text in the configuration file regardless of whether the password is input in plain or cipher text. Do not set this password to the weak password preset by running the **load security weak-password-dictionary** command.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the AS service configuration mode is set to independent mode, you need to use this command to configure the administrator account used to log in to ASs. After the configuration is complete, the user name and password used for login are automatically configured on the AS. The following configuration is generated on the AS:

```
#
aaa
 local-user user-name password irreversible-cipher password
 local-user user-name privilege level 3
 local-user user-name service-type terminal ssh
#
```

After an AS user name and password are configured, you need to enter the correct user name and password when logging in to an AS through the console port. When you log in to an AS from the parent using the **attach as name** *as-name* command, you can log in to the AS without entering the user name or password.

Precautions

The user name and password configured using this command take effect after the configuration is generated on ASs. It takes about 5 minutes for the configuration to take effect after you run the command. Do not log in to an AS within this period; otherwise, the configuration may take effect after a longer period of time.

Example

Create an AS administrator user name and password in independent mode.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] independent-as-admin user test password YsHsjx_202206
```

3.5.66 interface fabric-port

Function

The **interface fabric-port** command creates a fabric port and displays the fabric port view.

The **undo interface fabric-port** command deletes a fabric port.

By default, no fabric port exists in the system.

NOTE

This command can only be executed on a parent switch.

Format

interface fabric-port *port-id*

undo interface fabric-port *port-id*

Parameters

Parameter	Description	Value
port-id	Specifies the number of a fabric port.	The value range on the parent varies depending on the switch model: • S12700/S12700E: 0 to 255 • MCUD/SRUK/MFUX/MPUE/SRUE/SRUHA1/SRUHX1/SRUH: 0 to 255 • Other switch models: 0 to 63

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

To set up an SVF system, create fabric ports on the parent switches to allow ASs to connect to the parent switches.

Example

Create a fabric port and enter the fabric port view.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
```

3.5.67 ip source check user-bind enable (network enhanced profile view)

Function

The **ip source check user-bind enable** command configures IP packet checking in a network enhanced profile.

The **undo ip source check user-bind enable** command cancels IP packet checking in a network enhanced profile.

By default, IP packet checking is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

Network enhanced profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a network enhanced profile, you can configure IP packet checking in the profile. After the profile is bound to the port of an AS, IP packet checking is automatically enabled on the port. The following configuration is generated on the AS port:

```
#
 ip source check user-bind enable
 ip source check user-bind alarm enable
#
```

When attackers steal authorized users' IP addresses or MAC addresses to send packets to access or attack networks, authorized users cannot obtain stable and secure network services. After configuring IP packet checking on a device, the device checks received IP packets against the binding table to prevent such attacks.

Prerequisites

DHCP snooping has been enabled in the network enhanced profile using the **dhcp snooping enable** command.

Precautions

When an AS is an S2750-EI, S5700-10P-LI, or S5700-10P-PWR-LI and works in Layer 3 hardware forwarding mode, the **ip source check user-bind enable** command does not take effect on the AS. Because an AS performs only Layer 2 forwarding in an SVF system, you are advised to run the **undo assign forward-mode** command to cancel the Layer 3 hardware forwarding mode and then connect the AS to the SVF system.

Example

Configure IP packet checking in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] dhcp snooping enable
[HUAWEI-um-net-enhanced-profile_1] ip source check user-bind enable
```

3.5.68 ipv6 (AS administrator profile view)

Function

The **ipv6** command enables IPv6 in an AS administrator profile.

The **undo ipv6** command disables IPv6 in an AS administrator profile.

By default, IPv6 is disabled in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

ipv6

undo ipv6

Parameters

None

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

After creating an AS administrator profile, you can run the **ipv6** command to enable IPv6 for ASs in the profile. After an AS administrator profile is bound to an AS, the following configurations are generated globally on the AS:

```
#
ipv6
#
```

Example

Enable IPv6 in the AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] ipv6
```

3.5.69 mac-address flapping action (network enhanced profile view)

Function

The **mac-address flapping action** command configures the action taken on an interface in case of MAC address flapping in a network enhanced profile.

The **undo mac-address flapping action** command deletes the action taken on an interface in case of MAC address flapping in a network enhanced profile.

By default, in a network enhanced profile, the system does not perform any action when detecting MAC address flapping on an interface.

NOTE

This command can only be executed on a parent switch.

Format

mac-address flapping action error-down

undo mac-address flapping action error-down

Parameters

Parameter	Description	Value
error-down	Configures the system to set an interface to the Error-Down state when detecting MAC address flapping on this interface.	-

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure the action taken on an interface when MAC address flapping occurs on the interface in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 mac-address flapping action error-down
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration is determined by the profile configuration.

Example

Configure the system to set an interface to the Error-Down state when detecting MAC address flapping on this interface.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] mac-address flapping action error-down
```

3.5.70 mac-address trap notification (network enhanced profile view)

Function

The **mac-address trap notification** command configures the alarm function for MAC address learning and aging in a network enhanced profile.

The **undo mac-address trap notification** command deletes the alarm function of MAC address learning and aging in a network enhanced profile.

By default, the alarm function for MAC address learning and aging is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

mac-address trap notification all

undo mac-address trap notification

Parameters

Parameter	Description	Value
all	Indicates the alarm function for MAC address learning and aging.	-

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure the alarm function for MAC address learning and aging in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 mac-address trap notification all
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration is determined by the profile configuration.

Example

Configure the alarm function for MAC address learning and aging.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] mac-address trap notification all
```

3.5.71 mac-limit (user access profile view)

Function

The **mac-limit** command configures MAC address learning limiting in a user access profile.

The **undo mac-limit** command cancels MAC address learning limiting in a user access profile.

By default, MAC address learning limiting is not configured in a user access profile.

NOTE

This command can only be executed on a parent switch.

Format

mac-limit maximum *max-num*

undo mac-limit

Parameters

Parameter	Description	Value
maximum *max-num*	Specifies the maximum number of MAC addresses that can be learned on an interface.	The value is an integer that ranges from 0 to 4096. The value 0 indicates that the maximum number of MAC addresses that can be learned is not limited.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a user access profile, you can configure MAC address learning limiting in the profile. When the profile is bound an AS port, MAC address learning limiting is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 mac-limit maximum max-num
#
```

To control the number of access users and protect the MAC address table against attacks, you can limit the maximum number of MAC addresses that can be learned on an interface.

Precautions

The **mac-limit** and **authentication** commands are mutually exclusive and cannot be configured together in a user access profile.

Example

Configure MAC address learning limiting in a user access profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] mac-limit maximum 1024
```

3.5.72 multicast-suppression (network enhanced profile view)

Function

The **multicast-suppression** command configures unknown multicast traffic suppression in a network enhanced profile.

The **undo multicast-suppression** command cancels unknown multicast traffic suppression in a network enhanced profile.

By default, unknown multicast traffic suppression is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

multicast-suppression packets *packets-per-second*

undo multicast-suppression

Parameters

Parameter	Description	Value
packets *packets-per-second*	Specifies the packet rate of an interface.	The value is an integer that ranges from 0 to 14881000, in packets per second (PPS). If the configured packet rate on the parent switch is larger than the maximum value on the AS port, the maximum value takes effect on the AS port.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure unknown multicast traffic suppression in the profile. After the profile is bound to an AS port, unknown multicast traffic suppression is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 multicast-suppression packets packets-per-second
#
```

To prevent broadcast storms, you can run the **multicast-suppression** command to configure the maximum number of unknown multicast packets that can pass through a port. When the unknown multicast traffic rate reaches the maximum value, the system discards excess unknown multicast packets to control the traffic volume within a proper range.

Example

Configure unknown multicast traffic suppression in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] multicast-suppression packets 148810
```

3.5.73 network-basic-profile name

Function

The **network-basic-profile name** command creates a network basic profile.

The **undo network-basic-profile name** command deletes a network basic profile.

By default, no network basic profile is created.

NOTE

This command can only be executed on a parent switch.

Format

network-basic-profile name *profile-name*

undo network-basic-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network basic profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure basic user services in a network basic profile, including the default VLAN, allowed VLAN, and voice VLAN of a port.

Precautions

You can create a maximum of 256 network basic profiles in a version earlier than V200R011C10.

You can create a maximum of 512 network basic profiles in V200R011C10 and later versions.

Example

Create a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
```

3.5.74 network-basic-profile (port group view)

Function

The **network-basic-profile** command binds a network basic profile to a port group.

The **undo network-basic-profile** command unbinds a network basic profile from a port group.

By default, no network basic profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

network-basic-profile *profile-name*

undo network-basic-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network basic profile.	The value must have an existing network basic profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a network basic profile to a port group to deliver the configurations in the profile to all the member ports in the port group.

Prerequisites

The network basic profile has been created.

Precautions

A port group can be bound to only one network basic profile.

Example

Bind a network basic profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] network-basic-profile profile_1
```

3.5.75 network-enhanced-profile name

Function

The **network-enhanced-profile name** command creates a network enhanced profile.

The **undo network-enhanced-profile name** command deletes a network enhanced profile.

By default, no network enhanced profile is created.

NOTE

This command can only be executed on a parent switch.

Format

network-enhanced-profile name *profile-name*

undo network-enhanced-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network enhanced profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure value-added services in a network enhanced profile, such as network security and QoS.

Precautions

- You can create a maximum of 16 network enhanced profiles.
- A network enhanced profile can be bound to only an AS port group but not an AP port group.

Example

Create a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
```

3.5.76 network-enhanced-profile (port group view)

Function

The **network-enhanced-profile** command binds a network enhanced profile to a port group.

The **undo network-enhanced-profile** command unbinds a network enhanced profile from a port group.

By default, no network enhanced profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

network-enhanced-profile *profile-name*

undo network-enhanced-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network enhanced profile.	The value must have an existing network enhanced profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a network enhanced profile to a port group to deliver the configurations in the profile to all the member ports in the port group.

Prerequisites

The network enhanced profile has been created.

Precautions

- A network enhanced profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one network enhanced profile.

Example

Bind a network enhanced profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] network-enhanced-profile profile_1
```

3.5.77 network-qos-profile name

Function

The **network-qos-profile name** command creates a network QoS profile and displays the network QoS profile view.

The **undo network-qos-profile name** command deletes a network QoS profile.

By default, no network QoS profile is created.

NOTE

This command can only be executed on a parent switch.

Format

network-qos-profile name *profile-name*

undo network-qos-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network QoS profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A network QoS profile is used to configure QoS services for ASs on the parent, including the packet priority mapping mode, queue scheduling mode, and queue scheduling weight.

Precautions

- A maximum of 32 network QoS profiles can be created on the parent.
- A maximum of six network QoS profiles can be created on an AS.

Example

Create a network QoS profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test]
```

3.5.78 network-qos-profile (port group view)

Function

The **network-qos-profile** command binds a network QoS profile to a port group.

The **undo network-qos-profile** command unbinds a network QoS profile from a port group.

By default, no network QoS profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

network-qos-profile *profile-name*

undo network-qos-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a network QoS profile.	The value must be an existing network QoS profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a network QoS profile to a port group to deliver the configurations in the profile to all the member ports in the port group in a batch.

Prerequisites

The network QoS profile has been created before being bound to a port group.

Precautions

- A network QoS profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one network QoS profile.

Example

Bind a network QoS profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] trust dscp
[HUAWEI-um-net-qos-test] quit
```

```
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] network-qos-profile test
```

3.5.79 pass-vlan (network basic profile view)

Function

The **pass-vlan** command configures allowed VLANs in a network basic profile.

The **undo pass-vlan** command deletes allowed VLANs in a network basic profile.

By default, no allowed VLANs are configured in a network basic profile, and downlink ports of an AS allow packets from VLAN 1 to pass through.

NOTE

This command can only be executed on a parent switch.

Format

pass-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo pass-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies IDs of VLANs from which packets are allowed to pass through.	The value is an integer that ranges from 1 to 4094. The value cannot be the ID of an SVF management VLAN, a stack management VLAN, an ERPS control VLAN, an RRPP control VLAN, an SEP control VLAN, or a super VLAN.

Views

Network basic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network basic profile, you can configure allowed VLANs in the profile. After the profile is bound to an AS port, the port allows packets from these VLANs to pass through. The following configuration is generated on the AS port:

```
#
 port link-type hybrid
```

```
 port hybrid tagged vlan vlan-id1 to vlan-id2
#
```

Precautions

- The default VLAN, allowed VLANs, and voice VLAN in a network basic profile must be different.
- You can configure a maximum of 32 allowed VLANs in a network basic profile.

Example

Configured allowed VLANs in a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] pass-vlan 10 to 12
```

3.5.80 patch delete as

Function

The **patch delete as** command deletes patches on a specified online AS.

NOTE

This command can only be executed on a parent switch.

Format

patch delete as { **all** | **name** *patch-name* | **name-include** *string* }

Parameters

Parameter	Description	Value
all	Indicates all online ASs.	-
name *patch-name*	Specifies the name of an AS.	The value is a string of 1 to 31 case-insensitive characters without spaces.
name-include *string*	Specifies the string contained in an AS name.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you find errors in the patches loaded to an AS, run this command to delete the patches to prevent system operation failures.

If non-incremental patches need to be loaded to an AS, you need to run the **patch delete as** command to delete the existing patches on the AS first. Otherwise, non-incremental patches will fail to be loaded.

Precautions

If the patch file to be loaded to an AS type has been specified using the **as type** command, patches on this AS type cannot be deleted.

Example

Delete the patches on as1.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] patch delete as name as1
Warning: This command will start to delete the patch of AS. Continue?[Y/N]:y
Info: This operation will take several seconds, please wait...
```

3.5.81 policy (traffic policy profile view)

Function

The **policy** command configures a traffic policy in a traffic policy profile.

The **undo policy** command deletes a traffic policy in a traffic policy profile.

By default, no traffic policy is configured in a traffic policy profile.

NOTE

This command can only be executed on a parent switch.

Format

policy *policy-name* **remark** { **8021p** { *8021p-value* | **inner-8021p** } | **cvlan-id** *cvlan-id* | **dscp** { *dscp-value* | *dscp-name* } | **ip-precedence** *ip-precedence* | **local-precedence** { *local-precedence-value* | *local-precedence-name* } [**green** | **yellow** | **red**] | **vlan-id** *vlan-id* | **flow-id** *flow-id* | **destination-mac** *mac-address* }* **if-match acl** *acl-number*

undo policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value is a string of 1 to 64 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
remark	Specifies re-marking information.	-
8021p	Specifies the 802.1p priority of packets.	-
8021p-value	Specifies the 802.1p priority value of packets.	The value is an integer in the range from 0 to 7. A larger value indicates a higher priority.
inner-8021p	Inherits the 802.1p priority in the inner tag.	-
cvlan-id *cvlan-id*	Re-marks the inner VLAN tag in QinQ packets.	The value is an integer in the range from 1 to 4094.
dscp	Specifies the DSCP priority of packets.	-
dscp-value	Specifies the DSCP priority value of packets.	The value is an integer in the range from 0 to 63. A larger value indicates a higher priority.
dscp-name	Specifies the DSCP priority name of packets.	The value can be: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.
ip-precedence *ip-precedence*	Specifies the IP precedence.	The value is an integer in the range from 0 to 7. A larger value indicates a higher priority.
local-precedence	Specifies the local priority of packets.	-

Parameter	Description	Value
local-precedence-value	Specifies the local priority value.	The value is an integer in the range from 0 to 7. A larger value indicates a higher priority.
local-precedence-name	Specifies the local priority name.	The value can be: **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.
green	Indicates that the packet color corresponding to the local priority is green.	-
yellow	Indicates that the packet color corresponding to the local priority is yellow.	-
red	Indicates that the packet color corresponding to the local priority is red.	-
vlan-id *vlan-id*	Re-marks a VLAN ID in packets.	The value is an integer in the range from 1 to 4094.
flow-id *flow-id*	Specifies the value of a flow ID.	The value is an integer in the range from 1 to 8.
destination-mac *mac-address*	Re-marks the destination MAC address in packets.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
if-match	Specifies an ACL rule for matching packets.	-
acl *acl-number*	Specifies an ACL rule number.	The value is an integer in the range from 3000 to 3900.

Views

Traffic policy profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a traffic policy profile, you can configure traffic behaviors and traffic classifiers in the profile. After the profile is bound to an AS port, the traffic behaviors and traffic classifiers are automatically configured on the port.

The following global configuration is generated on the AS:

```
#
traffic classifier classifier-name operator or
 if-match acl-number
#
traffic behavior behavior-name
 remark xxxx
#
```

The following configuration is generated on the AS port:

```
#
 traffic-policy profile-name inbound
#
```

Or:

```
#
 traffic-policy profile-name outbound
#
```

Precautions

- A maximum of 64 traffic policies can be created in a traffic policy profile.
- **remark 8021p** and **remark local-precedence** cannot be configured in the same traffic policy.
- **remark dsc** and **remark ip-precedence** cannot be configured in the same traffic policy.

Example

Configured allowed VLANs in a traffic policy profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] traffic-policy-profile name profile_1
[HUAWEI-um-traffic-policy-profile_1] policy a remark 8021p 2 if-match acl 3456
```

3.5.82 port connect independent-as

Function

The **port connect independent-as** command enables the independent mode on the fabric port that connects the parent to a level-1 AS.

The **undo port connect** command restores the default mode of the fabric port that connects the parent to a level-1 AS.

By default, the service configuration mode of the fabric port that connects the parent to a level-1 AS is centralized mode.

NOTE

This command can only be executed on a parent switch.

Format

port connect independent-as

undo port connect

Parameters

None

Views

Fabric-port view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In independent mode, you can log in to an AS to configure this AS using commands. After the independent mode is enabled on the fabric port that connects the parent to a level-1 AS, the level-1 AS can be configured independently.

Precautions

- Before enabling the independent mode, run the **independent-as-admin** command in the uni-mng view to configure an administrator for AS login.
- If the AS connected to a fabric port is online, running the **undo port connect** command on the fabric port for mode switching will cause the AS to automatically restart and register with the parent again. Switching from the centralized mode to the independent mode does not cause the AS to restart.
- During mode switching on a fabric port, the parent and AS exchange packets for multiple times. In this process, if faults occur, for example, link or device faults, mode switching may fail. An error message will be displayed on the parent, indicating that mode switching fails. Additionally, the AS may restart and then registers with the parent again. In this situation, run commands on the fabric port again to change the mode after the AS has registered with the parent.
- In independent mode, when an AS goes offline, traffic on the network attached to an AS port cannot be forwarded if the port has authentication configurations. To enable the traffic to be forwarded normally, manually delete the authentication configurations from the port.
- When the service configuration mode of an AS is independent mode, configuring the following commands on the Eth-Trunk bound to or on the member port of a fabric port connected to the AS may cause this AS to go offline.

Table 3-120 Commands that may cause an AS to go offline

Command
loopback internal

Command
traffic-policy
traffic-filter
speed
negotiation
port media-type
port split
training disable
wavelength-channel
undo port hybrid tagged vlan
undo port trunk allow-pass vlan
storm-control action
mac-address flapping action
port-security protect-action

- If the Eth-Trunk bound to a fabric port has other configurations in addition to the following **Table 2** and **Table 3**, you need to manually delete the other configurations before running the **undo port connect** command on this fabric port for mode switching. Otherwise, an error message will be displayed to indicate that mode switching fails.

Table 3-121 Commands that can not be manually deleted in an Eth-Trunk

Command
port link-type hybrid
port hybrid tagged vlan

Table 3-122 Commands that do not need to be manually deleted in an Eth-Trunk

Command
undo port hybrid vlan
stp root-protection
stp edged-port disable
loop-detection disable

Command
mode lacp
mad relay
trust 8021p
authentication-profile
authentication control-point

Example

Enable the independent mode on the fabric port that connects the parent to a level-1 AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port connect independent-as
```

3.5.83 port connect-type indirect

Function

The **port connect-type indirect** command configures the indirect connection mode for a fabric port.

The **undo port connect-type** command restores the default connection mode for a fabric port.

The default connection mode of a fabric port is direct connection.

NOTE

This command can only be executed on a parent switch.

Format

port connect-type indirect

undo port connect-type

Parameters

None

Views

Fabric-port view

Default Level

3: Management level

Usage Guidelines

When the parent connects to an AS across a network, you need to run the **port connect-type indirect** command to configure the indirect connection mode for the fabric port that connects the parent to the AS.

Prerequisites

No Eth-Trunk is bound to the fabric port.

Follow-up Procedure

Run the **port member-group interface** command to bind an Eth-Trunk to the fabric port.

Example

Configure the indirect connection mode for a fabric port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port connect-type indirect
```

3.5.84 port-group name

Function

The **port-group name** command creates an AS port group.

The **port-group connect-ap name** command creates an AP port group.

The **undo port-group name** command deletes an AS port group.

The **undo port-group connect-ap name** command deletes an AP port group.

By default, no AS port group is created.

NOTE

This command can be executed only on a parent switch of models except the S6735-S, S6720-EI, S6720S-EI, S6720-SI, S6720S-SI, S6720S-S,S6730-S, or S6730S-S.

Format

port-group name *group-name*

port-group connect-ap name *group-name*

undo port-group name *group-name*

undo port-group connect-ap name *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a port group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A port group is a set of AS ports. The purpose of a port group is to facilitate batch configuration of AS ports.

Port groups are classified into AS port groups and AP port groups.

- Ports in an AS port group are used to connect an AS to a user terminal. An AS port group can be bound to four types of service profiles (network basic profile, network enhanced profile, user access profile, traffic policy profile, and network qos profile), but only one profile of the same type can be bound.
- Ports in an AP port group are used to connect an AS to an AP. To connect an AP to an AS, you need to add the port that connects the AS to the AP to an AP port group. An AP port group can be bound to only a network basic profile, and only the **pass-vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command configured in the profile takes effect.

Follow-up Procedure

Run the **as name** *as-name* or **as name-include** *string* **interface all** command to add AS ports to a port group.

Precautions

- You can create a maximum of 256 AS port groups in a version earlier than V200R011C10.

  You can create a maximum of 512 AS port groups in V200R011C10 and later versions.
- You can create a maximum of 1 AP port group.

Example

Create a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] port-group name group_1
```

3.5.85 port eth-trunk trunkmember

Function

The **port eth-trunk trunkmember** command adds member ports to the Eth-Trunk.

The **undo port eth-trunk trunkmember** command deletes member ports from an Eth-Trunk.

By default, no member ports are added to the Eth-Trunk.

NOTE

This command can only be executed on a parent switch.

Format

port eth-trunk *trunk-id* **trunkmember interface** *interface-type interface-number1* [**to** *interface-number2*]

undo port eth-trunk *trunk-id* **trunkmember interface** *interface-type interface-number1* [**to** *interface-number2*]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer and the minimum value is 1. The maximum value varies according to the switch model. For a specific switch model, the maximum value is the same as that described in **interface eth-trunk**.
interface *interface-type interface-number1* [**to** *interface-number2*]	Specifies the type and number of the interface added to an Eth-Trunk: ● *interface-type* specifies the interface type. ● *interface-number1* specifies the first interface number. ● *interface-number2* specifies the last interface number.	-

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a downlink fabric port of a level-1 AS is configured using the **down-direction fabric-port** *port-id* **member-group interface eth-trunk** *trunk-id* command, you need to add member ports to the Eth-Trunk to which the fabric port is bound.

When an Eth-Trunk has been created for an AS using the **uni eth-trunk** command, you can run the **port eth-trunk trunkmember** command to add member ports to this Eth-Trunk.

Precautions

AS uplink ports can be used to connect to the parent or level-1 AS or set up a stack and be configured as downlink fabric ports to connect to other ASs.

On the S6720-EI and S6720S-EI, 40GE ports and 10GE ports split from 40GE ports cannot be configured as downlink fabric ports.

Example

Add member ports to the Eth-Trunk to which a fabric port is bound.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] down-direction fabric-port 1 member-group interface eth-trunk 1
[HUAWEI-um-as-as1] port eth-trunk 1 trunkmember interface gigabitethernet 0/0/16
```

Add member ports to the Eth-Trunk configured on the specified AS.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] uni eth-trunk 40
[HUAWEI-um-as-as1] port eth-trunk 40 trunkmember interface GigabitEthernet 0/0/10
```

3.5.86 port member-group interface

Function

The **port member-group interface** command binds a fabric port to an Eth-Trunk.

The **undo port member-group** command unbinds a fabric port from an Eth-Trunk.

By default, no fabric port is bound to an Eth-Trunk.

NOTE

This command can only be executed on a parent switch.

Format

port member-group interface eth-trunk *trunk-id*

undo port member-group

Parameters

Parameter	Description	Value
eth-trunk *trunk-id*	Specifies the ID of the Eth-Trunk to which a fabric port is bound.	The value is an integer that ranges from 0 to 127.

Views

Fabric-port view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a fabric port using the **interface fabric-port** *port-id* command, bind the fabric port to an Eth-Trunk.

Follow-up Procedure

Run the **eth-trunk** *trunk-id* command in the interface view to add interfaces to the bound Eth-Trunk.

Precautions

- After the **port connect independent-as** command is executed to enable the independent configuration mode, you need to run the **undo port connect** command to restore to the centralized configuration mode before unbinding a fabric port from an Eth-Trunk.
- A created Eth-Trunk cannot be bound to a fabric port. When a fabric port is bound to an Eth-Trunk, the system creates the Eth-Trunk.
- You can run the **interface eth-trunk** command to enter the view of the Eth-Trunk to which a fabric port is bound and configure services. Currently, the following commands can be executed in the view of the Eth-Trunk to which a fabric port is bound: **authentication open ucl-policy enable**, **mac-address multiport**, **quit**, and all display commands.
- If physical member interfaces have been added to the Eth-Trunk bound to a fabric port, the **undo port member-group** command cannot be used to unbind the fabric port from the Eth-Trunk.

- Running the **undo port member-group** command will delete the configuration in the Eth-Trunk interface view and delete the Eth-Trunk.
- When a fabric port is bound to an Eth-Trunk, the system creates the Eth-Trunk and performs some service configurations on the Eth-Trunk, for example, the **stp root-protection** and **mad relay** command configurations.

Example

Bind a fabric port to an Eth-Trunk.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] interface fabric-port 1
[HUAWEI-um-fabric-port-1] port member-group interface eth-trunk 11
```

3.5.87 port-security aging-time (network enhanced profile view)

Function

The **port-security aging-time** command sets the aging time of secure dynamic MAC addresses on an interface in a network enhanced profile.

The **undo port-security aging-time** command cancels the configuration.

By default, the aging time of secure dynamic MAC addresses is not configured in a network enhanced profile, that is, secure dynamic MAC addresses will not be aged out.

NOTE

This command can only be executed on a parent switch.

Format

port-security aging-time *time*

undo port-security aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time of secure dynamic MAC address entries.	The value is an integer ranging from 1 to 1440, in minutes.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Application scenario

After creating a network enhanced profile, you can set the aging time of secure dynamic MAC addresses in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 port-security enable
 port-security aging-time 10
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile.

Prerequisites

Before setting the aging time of secure dynamic MAC addresses in a network enhanced profile, ensure that port security is enabled in the profile.

Example

Set the aging time of secure dynamic MAC addresses on an interface to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] port-security enable
[HUAWEI-um-net-enhanced-profile_1] port-security aging-time 10
```

3.5.88 port-security enable (network enhanced profile view)

Function

The **port-security enable** command enables port security in a network enhanced profile.

The **undo port-security enable** command disables port security in a network enhanced profile.

By default, port security is disabled in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

port-security enable

undo port-security enable

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Application scenario

After creating a network enhanced profile, you can enable port security in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 port-security enable
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile.

Prerequisites

- If the **mac-limit** command is configured in the user access profile view on an AS port bound to a network enhanced profile, the port security function cannot be enabled on the AS port.
- The port security function cannot be disabled in a network enhanced profile if other port security configurations exist in the profile.

Example

Enable port security in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] port-security enable
```

3.5.89 port-security mac-address sticky (network enhanced profile view)

Function

The **port-security mac-address sticky** command enables the sticky MAC address function in a network enhanced profile.

The **undo port-security mac-address sticky** command disables the sticky MAC address function in a network enhanced profile.

By default, the sticky MAC address function is disabled in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

port-security mac-address sticky

undo port-security mac-address sticky

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Application scenario

After creating a network enhanced profile, you can enable the sticky MAC address function in the profile. After the profile is bound to an AS port, the configuration is automatically delivered to the AS port. The following configuration is generated on the AS:

```
#
interface GigabitEthernet0/0/1
 port-security enable
 port-security mac-address sticky
#
```

In the preceding configuration, GigabitEthernet0/0/1 is used for reference only. The actual configuration depends on the profile.

Prerequisites

Before enabling the sticky MAC address function in a network enhanced profile, ensure that port security has been enabled in the profile.

Example

Configure the system to set an interface to the Error-Down state when detecting MAC address flapping on the interface.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] port-security enable
[HUAWEI-um-net-enhanced-profile_1] port-security mac-address sticky
```

3.5.90 portal url-encode disable

Function

The **portal url-encode disable** command disables the URL encoding function of ASs.

The **undo portal url-encode disable** command enables the URL encoding function of ASs.

By default, the URL encoding function of AS is enabled.

NOTE

This command can only be executed on a parent switch.

Format

portal url-encode disable

undo portal url-encode disable

Parameters

None

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. After URL encoding is enabled for ASs, special characters in redirect URLs are converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented. By default, URL encoding is enabled in ASs. This function can be disabled using the **portal url-encode disable** command.

Precautions

If the system software is upgraded from a version earlier than V200R009C00SPC500 to V200R009C00SPC500 or a later version, the switch automatically runs the **portal url-encode disable** command to disable URL encoding and decoding.

Example

Disable URL encoding.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] portal url-encode disable
```

3.5.91 qos { pq | wrr | drr } (network QoS profile view)

Function

The **qos** { **pq** | **wrr** | **drr** } command configures the queue scheduling mode for an AS port.

The **undo qos** { **pq** | **wrr** | **drr** } command restores the default queue scheduling mode of an AS port.

By default, no interface queue scheduling mode is configured in the network QoS profile view.

NOTE

This command can only be executed on a parent switch.

Format

qos { **pq** | **wrr** | **drr** }

undo qos { **pq** | **wrr** | **drr** }

Parameters

Parameter	Description	Value
pq	Indicates the PQ scheduling mode.	-
wrr	Indicates the WRR scheduling mode.	-
drr	Indicates the WDRR scheduling mode.	-

Views

Network QoS profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When congestion occurs on a network, configure the interface queue scheduling mode to balance between the delay and jitter of various service packets. In this way, packets of delay-sensitive services, such as voice and video services, can be processed preferentially. Among delay-insensitive services, such as the email service, the packets with the same priority are processed equally and the packets with different priorities are processed based on their weights.

In an SVF system, to change the queue scheduling mode of an AS port, run the **qos** { **pq** | **wrr** | **drr** } command in the network QoS profile view and then bind the profile to the AS port.

Precautions

If the queue scheduling weight has been configured using the **qos queue** command before the queue scheduling mode is configured, delete the configured queue scheduling weight first.

Example

Set the queue scheduling mode of an AS port to WDRR.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] qos drr
```

3.5.92 qos queue (network QoS profile view)

Function

The **qos queue** command configures a queue scheduling weight for an AS.

The **undo qos queue** command restores the default queue scheduling weight of an AS.

By default, the queue scheduling weight is 1.

NOTE

This command can only be executed on a parent switch.

Format

qos queue *queue-index* { **drr** | **wrr** } **weight** *weight*

undo qos queue *queue-index* { **drr** | **wrr** }

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
drr	Specifies the WDRR scheduling weight.	-
wrr	Specifies the WRR scheduling weight.	-
weight *weight*	Specifies the scheduling weight.	The value is an integer that ranges from 0 to 127.

Views

Network QoS profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If congestion occurs during queue scheduling, to ensure that each queue can be scheduled, configure a scheduling weight for each queue so that the device schedules each queue based on the configured scheduling weights.

In an SVF system, to change the queue scheduling weight of an AS port, run the **qos queue** command in the network QoS profile view and then bind the profile to the AS port.

Prerequisites

The queue scheduling mode of an AS port has been set to WRR or WDRR using the **qos { pq | wrr | drr }** command.

Example

Set the WDRR scheduling weight of queue 4 in a network QoS profile to 6.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] qos drr
[HUAWEI-um-net-qos-test] qos queue 4 drr weight 6
```

3.5.93 rate-limit (network enhanced profile view)

Function

The **rate-limit** command configures traffic rate limiting in a network enhanced profile.

The **undo rate-limit** command cancels traffic rate limiting in a network enhanced profile.

By default, traffic rate limiting is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

rate-limit *cir-value*

undo rate-limit

Parameters

Parameter	Description	Value
cir-value	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 1000000, in kbit/s. The packet rate range of an interface depends on the interface bandwidth,If the configured packet rate is larger than the maximum value, the maximum value takes effect.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network enhanced profile, you can configure traffic rate limiting in the profile. After the profile is bound to an AS port, traffic rate limiting is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 qos lr inbound cir cir-value cbs 125*cir-value
#
```

If user traffic is not limited, continuous burst data from numerous users can make the network congested. You can configure traffic rate limiting in inbound direction on an interface to limit traffic entering from the interface within a specified range.

Precautions

When an AS is an S2750-EI, S5700-10P-LI, or S5700-10P-PWR-LI switch and works in Layer 3 hardware forwarding mode, the **rate-limit** *cir-value* command does not take effect on the AS. Because an AS performs only Layer 2 forwarding in an SVF system, you are advised to run the **undo assign forward-mode** command to cancel the Layer 3 hardware forwarding mode and then connect the AS to the SVF system.

Example

Configure traffic rate limiting in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] rate-limit 100000
```

3.5.94 reboot uni-mng

Function

The **reboot uni-mng** command restarts an SVF system.

NOTE

This command can only be executed on a parent switch.

Format

reboot uni-mng

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading or troubleshooting an SVF system, you can restart the SVF system, including the parent and all ASs.

Precautions

- This command can be used only after the SVF function is enabled.
- The next startup software version of the AS must be V200R011C10 or later, and the next startup software version of the parent cannot be earlier than that of the AS.
- Before running this command to restart an SVF system, you must save the configuration of the parent. If an AS is configured in independent mode, you also need to save the configuration of the AS.

Example

Restart an SVF system.

```
<HUAWEI> reboot uni-mng
```

3.5.95 reset uni-mng as-discover packet statistics

Function

The **reset uni-mng as-discover packet statistics** command clears AS Discovery packet statistics on a fabric port.

NOTE

This command can be used on the parent or an AS. After running this command, you can clear AS Discovery packet statistics on a fabric port of the local device.

Format

reset uni-mng as-discover packet statistics interface fabric-port *port-id*

Parameters

Parameter	Description	Value
interface fabric-port *port-id*	Specifies the number of a fabric port.	The value is an integer that ranges from 0 to 63 on an AS and the value range on the parent varies depending on the switch model: • S12700/S12700E: 0 to 255 • MCUD/SRUK/MFUX/MPUE/SRUE/SRUHA1/SRUHX1/SRUH: 0 to 255 • Other switch models: 0 to 63

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting statistics about AS Discovery packets on a fabric port, clear the existing statistics.

Example

Clear AS Discovery packet statistics on a fabric port.

```
<HUAWEI> reset uni-mng as-discover packet statistics interface fabric-port 1
```

3.5.96 shutdown interface

Function

The **shutdown interface** command disables an AS port.

The **undo shutdown interface** command enables an AS port.

By default, an interface is enabled.

NOTE

This command can only be executed on a parent switch.

Format

shutdown interface *interface-type interface-number*

undo shutdown interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. - *interface-type* specifies the interface type. The interface type cannot be an Eth-Trunk interface. - *interface-number* specifies the interface number.	-

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **shutdown interface** command to disable an AS port.

Precautions

Running this command can disable only an AS downlink port but not an AS uplink port. If an uplink port has been configured as a downlink fabric port, this port can be disabled.

If the version of an AS is inconsistent with that of the parent, the **shutdown interface** and **undo shutdown interface** commands do not take effect on the ports of this AS.

If an AS is configured in the independent mode, the **shutdown interface** and **undo shutdown interface** commands do not take effect on the ports of this AS.

Example

Disable an AS port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] shutdown interface gigabitethernet 0/0/1
```

3.5.97 slot

Function

The **slot** command pre-configures a stack ID or changes the pre-configured device model.

The **undo slot** command deletes the pre-configured stack ID or changes the pre-configured device model.

By default, the pre-configured stack ID is 0.

NOTE

This command can only be executed on a parent switch.

Format

slot *slot-id1* **replace-model** *model-name*

undo slot *slot-id1* **replace-model**

slot *slot-id2* [**to** *slot-id3*] [**replace-model** *model-name*]

undo slot *slot-id2* [**to** *slot-id3*] [**replace-model**]

Parameters

Parameter	Description	Value
slot-id1	Specifies the pre-configured stack ID.	The value is 0.
slot-id2 [**to** *slot-id3*]	Specifies the pre-configured stack ID. *slot-id3* must be larger than *slot-id2*.	The value is an integer that ranging from 1 to 4.
replace-model *model-name*	Specifies the device model of which the stack ID needs to be pre-configured.	The value range depends on the device configuration.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS is a stack of multiple member switches, the system pre-configures only stack ID 0 by default. You can only pre-configure services for the member switch with stack ID 0. Before pre-configuring services for another member switch, pre-configure a stack ID for the member switch.

The pre-configured stack ID does not affect the actual stack ID. For example, the pre-configured stack ID is 0 (default value), but the actual stack IDs are 0 and 2. The actual stack IDs remain 0 and 2 except that no services are configured on the device with stack ID 2.

An AS can be a stack of the same device series but different device models. If the stack contains different device models, you need to specify the **replace-model** parameter to change the device model that is different from the other device models in the stack to the actual access device model. If you do not specify the device model of a specified member, by default, the device model of this member is consistent with the pre-configured AS type.

Precautions

If the AS does not support stacking, the **slot** *slot-id* command configuration takes effect on the parent only when slot 0 is configured as the stack ID.

Changing the device models of online devices in a stack is not allowed.

Example

Pre-configure a stack ID.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] slot 1 to 4
```

Change the device model of the switch with stack ID 2 in the AS **as1** to S5720-28X-SI-AC.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name as1
[HUAWEI-um-as-as1] slot 2 replace-model S5720-28X-SI-AC
```

3.5.98 stp bpdu-protection (AS administrator profile)

Function

The **stp bpdu-protection** command configures BPDU protection for ASs in an AS administrator profile.

The **undo stp bpdu-protection** command cancels BPDU protection of ASs in an AS administrator profile.

By default, BPDU protection is not configured for ASs in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

stp bpdu-protection

undo stp bpdu-protection

Parameters

None

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

After creating an AS administrator profile, run the **stp bpdu-protection** command to configure BPDU protection for ASs in the profile. After the profile is bound to an AS, the following configuration is generated on the AS:

```
#
stp bpdu-protection
#
```

Example

Configure BPDU protection for ASs in an AS administrator profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] stp bpdu-protection
```

3.5.99 traffic-limit inbound (user access profile view)

Function

The **traffic-limit inbound** command configures the rate limit for incoming ARP and DHCP packets on an AS port.

The **undo traffic-limit inbound** command restores the default rate limit for incoming ARP and DHCP packets on an AS port.

By default, the forwarding rate of incoming ARP and DHCP packets on an AS port is not limited.

NOTE

This command can only be executed on a parent switch.

Format

traffic-limit inbound { **arp** | **dhcp** } **cir** *cir-value*

undo traffic-limit inbound { **arp** | **dhcp** }

Parameters

Parameter	Description	Value
arp	Specifies the ARP packet.	-
dhcp	Specifies the DHCP packet.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed average rate of traffic that can pass through.	The value is an integer that ranges from 8 to 128, in kbit/s.

Views

User access profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a user access profile is created, you can configure the rate limit for incoming ARP and DHCP packets on an AS port. After the user access profile is bound to the AS port, the following configuration is generated on the AS port:

```
#
 traffic-limit inbound acl 4999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
 traffic-statistic inbound acl 4999
 traffic-limit inbound acl 3999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
 traffic-statistic inbound acl 3999
#
```

Precautions

- This command and the **authentication** command cannot be both run in the user access profile view.
- Do not run the **traffic-limit inbound dhcp** and **dhcp snooping enable (network enhanced profile view)** commands simultaneously on the same port; otherwise, the **traffic-limit inbound dhcp** command does not take

effect. On an AS of the S2750-EI, S5700-LI, S5700S-LI, S5720S-LI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5710-X-LI, S5735S-H, S5736-S, S6720S-S, or S600-E model, running the **dhcp snooping enable (network enhanced profile view)** command on any port may cause the **traffic-limit inbound dhcp** command unable to take effect on all ports. You are advised to shut down the attacked port after detecting DoS attacks.

- Do not run the **traffic-limit inbound arp** and **arp anti-attack check user-bind enable (network enhanced profile view)** commands simultaneously on the same port. Otherwise, the **traffic-limit inbound arp** command may not take effect. On an AS of the S2750-EI, S5700-LI, S5700S-LI, S5720S-LI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5710-X-LI, S5735S-H, S5736-S, S6720S-S, or S600-E model, running the **arp anti-attack check user-bind enable (network enhanced profile view)** command on any port may cause the **traffic-limit inbound arp** command unable to take effect on all ports. You are advised to shut down the attacked port after detecting DoS attacks.

Example

Set the rate limit for incoming ARP packets to 64 on an AS port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] traffic-limit inbound arp cir 64
```

3.5.100 traffic-limit outbound (AS administrator profile view)

Function

The **traffic-limit outbound** command configures the rate limit for outgoing ARP and DHCP packets on an AS uplink fabric port.

The **undo traffic-limit outbound** command restores the default rate limit for outgoing ARP and DHCP packets on an AS uplink fabric port.

By default, the rate limits for outgoing ARP packets and DHCP packets are 32 kbit/s and 128 kbit/s respectively on an AS uplink fabric port.

NOTE

This command can only be executed on a parent switch.

Format

traffic-limit outbound { **arp** | **dhcp** } **cir** *cir-value*

undo traffic-limit outbound { **arp** | **dhcp** }

Parameters

Parameter	Description	Value
arp	Specifies the ARP packet.	-
dhcp	Specifies the DHCP packet.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed average rate of traffic that can pass through.	The value is an integer that ranges from 8 to 512, in kbit/s.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an AS administrator profile is created, you can configure the rate limit for outgoing ARP and DHCP packets on an AS uplink fabric port. After the AS goes online, the following configuration is generated in the AS Eth-Trunk 0 view and system view, regardless of whether the AS administrator profile is bound to the AS:

```
#
acl number 3999
 rule 5 permit udp destination-port eq bootps
#
acl number 4998
 rule 5 permit vlan-id management-vlan
acl number 4999
 rule 5 permit l2-protocol arp destination-mac ffff-ffff-ffff
 rule 10 permit l2-protocol arp
#
interface Eth-Trunk0
 traffic-filter outbound acl 4998
 traffic-statistic outbound acl 3999
 traffic-limit outbound acl 3999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
 traffic-statistic outbound acl 4999
 traffic-limit outbound acl 4999 cir cir-value pir pir-value cbs cbs-value pbs pbs-value
#
```

Example

Set the rate limit for outgoing ARP packets to 64 on an uplink fabric port.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] traffic-limit outbound arp cir 64
```

3.5.101 traffic-policy-profile (port group view)

Function

The **traffic-policy-profile** command binds a traffic policy profile to a port group.

The **undo traffic-policy-profile** command unbinds a traffic policy profile from a port group.

By default, no traffic policy profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

traffic-policy-profile *profile-name* { **inbound** | **outbound** }

undo traffic-policy-profile { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic policy profile.	The profile must have been created.
inbound	Applies a traffic policy profile to the inbound direction of an interface.	-
outbound	Applies a traffic policy profile to the outbound direction of an interface.	-

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a traffic policy profile to a port group to deliver the configurations in the profile to all the member ports in the port group in a batch.

Prerequisites

The traffic policy profile has been created before being bound to a port group.

Precautions

- A traffic policy profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one traffic policy profile.

Example

Bind a traffic policy profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] traffic-policy-profile name profile_1
[HUAWEI-um-traffic-policy-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] traffic-policy-profile profile_1 inbound
```

3.5.102 traffic-policy-profile name

Function

The **traffic-policy-profile name** command creates a traffic policy profile.

The **undo traffic-policy-profile name** command deletes a traffic policy profile.

By default, no traffic policy profile is configured.

NOTE

This command can only be executed on a parent switch.

Format

traffic-policy-profile name *profile-name*

undo traffic-policy-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic policy profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A traffic policy profile is used to configure traffic policy functions for ASs, including the packet re-marking function.

Precautions

You can create at most 32 traffic policy profiles.

Example

Create a traffic policy profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] traffic-policy-profile name profile_1
```

3.5.103 trust dscp (network QoS profile view)

Function

The **trust dscp** command configures an AS to perform priority mapping on packets based on DSCP priorities.

The **undo trust dscp** command cancels configuring an AS to perform priority mapping on packets based on DSCP priorities.

By default, an AS performs priority mapping on packets based on 802.1p priorities.

NOTE

This command can only be executed on a parent switch.

Format

trust dscp

undo trust dscp

Parameters

None

Views

Network QoS profile view

Default Level

3: Management level

Usage Guidelines

By default, a device performs priority mapping on packets based on 802.1p priorities. If packets have the same 802.1p priority, the device cannot provide differentiated services to packets. To solve this problem, configure the device to perform priority mapping on packets based on DSCP priorities. After the **trust dscp** command is configured, the device searches for the priority mapping table based on DSCP priorities and assigns an internal priority to packets so that packets are placed in their corresponding queues.

In an SVF system, you can configure an AS to perform priority mapping on packets based on DSCP priorities by running the **trust dscp** command in the network QoS profile view and then binding the profile to an AS port.

Example

In a network QoS profile, configure an AS to perform priority mapping on packets based on DSCP priorities.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-qos-profile name test
[HUAWEI-um-net-qos-test] trust dscp
```

3.5.104 topology explore

Function

The **topology explore** command triggers SVF network topology collection immediately.

The **topology explore interval** command sets the interval for collecting SVF network topology information.

The **undo topology explore interval** command restores the default interval for collecting SVF network topology information.

By default, the interval for collecting SVF network topology information is 10 minutes.

NOTE

This command can only be executed on a parent switch.

Format

topology explore [**interval** *interval*]

undo topology explore interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for collecting SVF network topology information.	The value is an integer that ranges from 0 to 1440, in minutes. The value 0 indicates that SVF network topology information is not automatically collected.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

You can adjust the interval for collecting SVF network topology information based on SVF network stability. When the network topology is stable, you can increase the interval or disable periodic topology information collection. When the network topology is unstable, you can shorten the interval.

You can also run the **topology explore** command to trigger SVF network topology collection immediately.

Example

Set the SVF network topology collection interval to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] topology explore interval 30
```

3.5.105 undo uni-mng enable

Function

The **undo uni-mng enable** command changes an AS from the client mode to the standalone mode.

NOTE

This command can only be executed on an AS. After this command is executed, the AS restarts.

Format

undo uni-mng enable

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **undo uni-mng enable** command to change an AS from the client mode to the standalone mode.

Example

Change an AS from the client mode to the standalone mode.

```
<HUAWEI> undo uni-mng enable
```

3.5.106 uni eth-trunk

Function

The **uni eth-trunk** command creates an Eth-Trunk interface for an AS.

The **undo uni eth-trunk** command deletes an Eth-Trunk interface of an AS.

By default, no Eth-Trunk interface is created on an AS.

NOTE

This command can only be executed on the parent.

Format

uni eth-trunk *trunk-id* [**mode lacp**]

undo uni eth-trunk *trunk-id* [**mode lacp**]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk interface.	The value is an integer and the minimum value is 1. The maximum value varies according to the switch model. For a specific switch model, the maximum value is the same as that described in **interface eth-trunk**.
mode lacp	Sets the working mode of an Eth-Trunk interface to LACP mode. If this parameter is not specified, the working mode of an Eth-Trunk interface is manual mode.	-

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AP with two network interfaces connects to an SVF system through an AS or to improve access user bandwidth and reliability, you can create an Eth-Trunk interface for this AS.

Precautions

- An Eth-Trunk interface can be created for an AS only when this AS is in centralized mode.
- When an AS works in independent mode and its Eth-Trunk interface needs to be deleted, you need to run the **undo uni eth-trunk** *trunk-id* command in the AS view of the parent and log in to this AS to delete this Eth-Trunk interface.
- To delete an Eth-Trunk interface, ensure that it does not contain member interfaces.
- After an Eth-Trunk interface is created and its working mode is set to LACP, running the **uni eth-trunk** *trunk-id* command will not change the working mode of the Eth-Trunk interface. To change the working mode to manual mode, run the **undo uni eth-trunk** *trunk-id* **mode lacp** command.
- Running the **undo uni eth-trunk** *trunk-id* **mode lacp** command only changes the working mode of an Eth-Trunk interface and will not delete the Eth-Trunk interface. To delete an Eth-Trunk interface, run the **undo uni eth-trunk** *trunk-id* command.
- The Eth-Trunk interface of an AS and Eth-Trunk interfaces bound to fabric ports share the Eth-Trunk interface specifications.
- An Eth-Trunk interface contains a maximum of eight member interfaces.
- An Eth-Trunk interface cannot be created across ASs.

Follow-up Procedure

Run the **port eth-trunk trunkmember** command to add member interfaces to the Eth-Trunk interface.

Example

Create Eth-Trunk 2 in LACP mode for the AS **test**.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name test
[HUAWEI-um-as-test] uni eth-trunk 2 mode lacp
```

3.5.107 uni eth-trunk lacp timeout

Function

The **uni eth-trunk lacp timeout** command configures the LACP timeout time for an Eth-Trunk interface on an AS.

The **undo uni eth-trunk lacp timeout** command restores the default LACP timeout time of an Eth-Trunk interface on an AS.

By default, the LACP timeout time of an Eth-Trunk interface on an AS is 90 seconds.

NOTE

This command can only be executed on a parent switch.

Format

uni eth-trunk *trunk-id* **lacp timeout fast** [**user-defined** *user-defined-timeout*]

undo uni eth-trunk *trunk-id* **lacp timeout**

Parameters

Parameter	Description	Value
trunk-id	Specifies an Eth-Trunk ID.	The value must be an Eth-Trunk ID that has been created using the **uni eth-trunk** command.
fast	Sets the LACP timeout time of an Eth-Trunk interface to 3 seconds. In this situation, the interval at which the remote end sends LACP PDUs is 1 second.	-
user-defined *user-defined-timeout*	Indicates the user-defined LACP timeout time of an Eth-Trunk interface.	The value is an integer that ranges from 3 to 90, in seconds.

Views

AS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, if a member interface of the remote Eth-Trunk interface is faulty, it takes 90 seconds for the local Eth-Trunk interface to detect the remote member interface status change. This results in data traffic loss because the local interface continues to forward data traffic to the faulty remote member interface within 90 seconds. To enable the local interface to detect the remote member interface status change in a timely manner, run the **uni eth-trunk lacp timeout** command to reduce the LACP timeout time.

Prerequisites

The **uni eth-trunk lacp timeout** command can be configured only when the **uni eth-trunk** command has been configured to create an Eth-Trunk interface and set its working mode to LACP mode.

Precautions

The **uni eth-trunk lacp timeout** command is deleted when the **undo uni eth-trunk** command is configured to delete the Eth-Trunk interface.

Example

Set the LACP timeout time of Eth-Trunk 2 on the AS **test** to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as name test
[HUAWEI-um-as-test] uni eth-trunk 2 mode lacp
[HUAWEI-um-as-test] uni eth-trunk 2 lacp timeout fast
```

3.5.108 uni-mng

Function

The **uni-mng** command enables SVF or displays the uni-mng view.

The **undo uni-mng** command disables SVF.

By default, SVF is disabled.

NOTE

This command can only be executed on a parent switch.

Format

uni-mng

undo uni-mng

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When SVF is disabled, the **uni-mng** command enables SVF and displays the uni-mng view. When SVF has been enabled, this command displays the uni-mng view.

Prerequisites

- A source interface used to set up a CAPWAP link has been specified using the **capwap source interface vlanif** *vlan-id* command.
- The STP working mode must be STP or RSTP. If the current working mode is not STP or RSTP, run the **stp mode** { **rstp** | **stp** } command to set the STP working mode to STP or RSTP before enabling SVF. By default, the STP working mode is MSTP. You can run the **display stp** command to check the current STP working mode.
- The default STP/RSTP port path cost algorithm must be used. If the current port path cost algorithm is not the default one, run the **undo stp pathcost-standard** command to restore the default port path cost algorithm before enabling SVF. The default STP/RSTP port path cost algorithm is IEEE 802.1t (**dot1t**). You can run the **display stp** command to check the current port path cost algorithm.
- The default Eth-Trunk specifications are used. If the current Eth-Trunk specifications are not the default value on S5531-H, S5531-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, or S6720S-EI, run the **undo assign trunk** command to restore the default Eth-Trunk specifications before enabling SVF. You can run the **display trunk configuration** command to check the default and configured Eth-Trunk specifications.
- The NAC configuration mode must be the unified mode. If the current mode is not the unified mode, run the **authentication unified-mode** command to set the NAC configuration mode to unified mode. The default NAC configuration mode is unified mode. You can run the **display authentication mode** command to check the current NAC configuration mode.
- Remote authorization is not configured in the system. If remote authorization has been configured, run the **undo remote-authorize** command to disable remote authorization before enabling SVF. By default, remote authorization is not configured in the system. You can run the **display current-configuration** command to check whether remote authorization is configured.

Precautions

- When SVF is enabled on the parent, LLDP is automatically enabled on the parent if LLDP is disabled. When SVF is disabled on the parent, LLDP is not automatically disabled on the parent.

- When SVF is disabled on the parent, the STP priorities of ports change, and STP recalculates the port role and changes the interface status.
- After SVF is enabled on a switch used as the parent, the **stack timer mac-address switch-delay** value changes to 0 (not changing system MAC address) and cannot be changed. After SVF is disabled on this switch, this delay time is still 0, but you can manually change it.

Example

Enable SVF (default Eth-Trunk specifications and default NAC configuration mode).

```
<HUAWEI> system-view
[HUAWEI] vlan batch 11
[HUAWEI] interface Vlanif 11
[HUAWEI-Vlanif11] ip address 192.168.11.1 24
[HUAWEI-Vlanif11] quit
[HUAWEI] capwap source interface vlanif 11
[HUAWEI] stp mode stp
[HUAWEI] uni-mng
Warning: This operation will enable the uni-mng mode and disconnect all ASs. STP calculation may be
triggered and service traffic will be affected. Continue? [Y/N]:y
```

3.5.109 uni-mng indirect fabric-port

Function

The **uni-mng indirect fabric-port** command configures a member port for an uplink fabric port that connects an AS to the parent through a network.

The **undo uni-mng indirect fabric-port** command deletes a member port of an uplink fabric port that connects an AS to the parent through a network.

By default, no member port is configured for an uplink fabric port that connects an AS to the parent through a network.

NOTE

This command can only be executed on an AS.

Format

uni-mng indirect fabric-port member interface *interface-type interface-number*

undo uni-mng indirect fabric-port member interface *interface-type interface-number*

Parameters

Parameter	Description	Value
member interface *interface-type interface-number*	Specifies the type and number of member ports of a fabric port.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS connects to the parent through a network, you must run the **uni-mng indirect fabric-port** command to configure a member port for an uplink fabric port of the AS. You can run this command multiple times to add multiple member ports to the fabric port.

Prerequisites

The **uni-mng indirect mng-vlan** command has been executed to configure the device to work in client mode and configure a management VLAN.

Precautions

- Only AS uplink ports or subcard ports can be added to an uplink fabric port. If you have to add AS downlink ports to uplink fabric ports, run the **uni-mng up-direction fabric-port member interface** *interface-type interface-number* [**to** *interface-number*] command.
- A maximum of eight member ports can be added to a fabric port.
- Ports used to set up a stack cannot be configured as member ports of a fabric port.
- The command that configures the stack ID is mutually exclusive with the command that configures a member port for a fabric port:
  - After the **stack slot** *slot-id* **renumber** *new-slot-id* command is executed in a specified slot, the port in the slot cannot be configured as a member port of a fabric port.
  - After a port in a slot is configured as a member port of a fabric port, the stack ID of the slot cannot be configured using the **stack slot** *slot-id* **renumber** *new-slot-id* command.
- You need to configure a member port of a fabric port according to the network configuration. A member port needs to be reconfigured if the stack ID changes because the stack changes, for example, the stacking function is disabled, or existing stack IDs conflict after member devices are added to the stack.

Example

Configure member ports for an uplink fabric port that connects an AS to the parent through a network.

```
<HUAWEI> uni-mng indirect fabric-port member interface gigabitethernet 0/0/27
<HUAWEI> uni-mng indirect fabric-port member interface gigabitethernet 0/0/28
```

3.5.110 uni-mng indirect mng-vlan

Function

The **uni-mng indirect mng-vlan** command configures a device to work in client mode and configures a management VLAN.

NOTE

This command can only be executed on an AS.

Format

uni-mng indirect mng-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a management VLAN. The VLAN must be consistent with the management VLAN configured on a parent.	The value is an integer that ranges from 2 to 4094. The VLAN cannot be the reserved VLAN (The default is VLAN 4093) of a stack.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AS connects to the parent through a network, you must run the **uni-mng indirect mng-vlan** command to configure the AS to work in client mode and configures a management VLAN.

Precautions

- The VCMP role switching command is mutually exclusive with the command that configures a device to work in client mode. If the current device is not a silent switch in a VCMP domain, the device cannot be configured to work in client mode. You must run the **vcmp role silent** command in the system view to set the VCMP role of the device to silent. After a device is configured to work in client mode, the VCMP role switching command cannot be executed. That is, the device cannot change from the silent role to another role.
- After running the **uni-mng indirect mng-vlan** *vlan-id* command on the device in standalone mode, you must delete the configuration file of the device and restart the device to make the configuration take effect.

- If the device has been configured to work in client mode but has not gone online, you can run the **uni-mng indirect mng-vlan** *vlan-id* command multiple times to change the management VLAN, and the configuration takes effect immediately.
- If the device has been configured to work in client mode and has gone online, the **uni-mng indirect mng-vlan** *vlan-id* command cannot be executed.
- When an AS is an S5700-10P-LI, S5700-10P-PWR-LI-AC, or S2750-EI and Layer 3 hardware forwarding for IPv4 packets has been enabled using the **assign forward-mode ipv4-hardware** command in the system view, the management VLAN cannot be configured. To solve this problem, start the AS in standalone mode and run the **undo assign forward-mode** command in the system view to disable Layer 3 hardware forwarding for IPv4 packets.
- On the S5720-SI, S5735-S, S500, S5735S-S, S5720I-SI, S5735S-H, S5736-S, S6720S-S, or S600-E, the electrical port stack configuration on the front panel is mutually exclusive with the client mode configuration. If electrical ports on the front panel have been configured as stack physical member ports, no management VLAN cannot be configured. If a management VLAN has been configured, electrical ports on the front panel cannot be configured as stack physical member ports.
- If an AS is configured in the independent mode, its management VLAN cannot be configured using this command.
- The slot ID of an AS cannot be greater than or equal to 5. Otherwise, the management VLAN cannot be configured for the AS using the **uni-mng indirect mng-vlan** command.
- The command that changes a stack ID and the command that configures a management VLAN are mutually exclusive.
  - The management VLAN cannot be configured for an AS after the slot ID of the AS is changed using the **stack slot** *slot-id* **renumber** *new-slot-id* command.
  - The slot ID of an AS cannot be changed using the **stack slot** *slot-id* **renumber** *new-slot-id* command after a management VLAN is configured for the AS using the **uni-mng indirect mng-vlan** command.

Example

Configure the device to work in client mode and configure a management VLAN 100.

```
<HUAWEI> uni-mng indirect mng-vlan 100
```

3.5.111 uni-mng up-direction fabric-port

Function

The **uni-mng up-direction fabric-port** command configures AS service ports as an uplink fabric port's members.

The **undo uni-mng up-direction fabric-port** command cancels the configuration.

By default, AS service ports are not configured as members of uplink fabric ports.

NOTE

This command can only be executed on an AS.

Format

uni-mng up-direction fabric-port member interface *interface-type interface-number* [**to** *interface-number*]

undo uni-mng up-direction fabric-port member interface *interface-type interface-number* [**to** *interface-number*]

undo uni-mng up-direction fabric-port member all

Parameters

Parameter	Description	Value
member interface *interface-type interface-number*	Specifies the type and number of an AS service port to be configured as a member of an uplink fabric port.	-
all	Specifies all AS service ports.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure AS service ports as an uplink fabric port's members, run the **uni-mng up-direction fabric-port** command.

Precautions

- A maximum of eight interfaces can be configured as a fabric port's members on an AS.
- Stack ports cannot be configured as members of fabric ports. Similarly, fabric member ports cannot be configured as stack ports.
- After the **uni-mng up-direction fabric-port** command is run on an AS, you must restart the AS to make the configuration take effect. If the AS is a stack, you need to restart all stack members. If a configuration conflicting with this command exists on the parent, the AS may fail to go online.
- The command for configuring a stack ID and the command for configuring a fabric member port are mutually exclusive. Specifically:

  - If you have run the **stack slot** *slot-id* **renumber** *new-slot-id* command in a slot, you are not allowed to configure the service port of this slot as a member of an uplink fabric port.
  - If you have configured a service port of a slot as a member of an uplink fabric port, you are not allowed to run the **stack slot** *slot-id* **renumber** *new-slot-id* command to configure a stack ID in this slot.
- When configuring a service port as a member of a fabric port, pay attention to the stacking configuration. A member port needs to be reconfigured if stack IDs change because the stack changes, for example, the stacking function is disabled, or existing stack IDs conflict after member switches are added to the stack.
- If a downlink service interface of an AS is incorrectly configured as a stack port, other interfaces on the AS cannot be configured as uplink interfaces. In this case, delete the stack port configuration from the downlink service interface.

Example

Configure an AS service port as a member of an uplink fabric port.

```
<HUAWEI> uni-mng up-direction fabric-port member interface gigabitethernet 0/0/3
Warning: After a service port on an AS is configured as an uplink port, the AS needs to be restarted to
make the configuration take effect.
 If the parent has a configuration conflict with the AS, the AS may fail to go online. Continue? [Y/N]:y
```

3.5.112 unicast-suppression (network enhanced profile view)

Function

The **unicast-suppression** command configures unknown unicast traffic suppression in a network enhanced profile.

The **undo unicast-suppression** command cancels unknown unicast traffic suppression in a network enhanced profile.

By default, unknown unicast traffic suppression is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

unicast-suppression packets *packets-per-second*

undo unicast-suppression

Parameters

Parameter	Description	Value
packets *packets-per-second*	Specifies the packet rate of an interface.	The value is an integer that ranges from 0 to 14881000, in packets per second (PPS). If the configured packet rate on the parent switch is larger than the maximum value on the AS port, the maximum value takes effect on the AS port.

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure unknown unicast traffic suppression in the profile. After the profile is bound to an AS port, unknown unicast traffic suppression is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 unicast-suppression packets packets-per-second
#
```

To prevent broadcast storms, you can run the **unicast-suppression** command to configure the maximum number of unknown unicast packets that can pass through a port. When the unknown unicast traffic rate reaches the rate limit, the system discards excess unknown unicast packets to control the traffic volume within a proper range.

Example

Configure unknown unicast traffic suppression in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] unicast-suppression packets 148810
```

3.5.113 upgrade as

Function

The **upgrade as name** command upgrades an AS with a specified name.

The **upgrade as name-include** command upgrades ASs of which the name contains a specified string.

The **upgrade as type** command upgrades ASs of a specified type.

The **upgrade as all** command upgrades all ASs.

undo upgrade as command rolls back ASs to the previous version.

NOTE

This command can only be executed on a parent switch.

Format

upgrade as name *as-name* [**reload** [**at** *time*]]

upgrade as name-include *string* [**reload** [**at** *time*]]

upgrade as type *as-type* [**reload** [**at** *time*]]

upgrade as all [**reload** [**at** *time*]]

undo upgrade as { **all** | **name** *as-name* | **name-include** *string* | **type** *as-type* }

Parameters

Parameter	Description	Value
as-name	Upgrades an AS with a specified name.	The value must have an existing AS name.
string	Upgrades all the ASs of which the name contains a specified string.	The value is a string of 1 to 31 case-insensitive characters without spaces.
as-type	Upgrades ASs of a specified type.	The value is an enumerated type. You can enter a question mark (?) and select a value from the displayed value range.
reload	Configures an AS to restart after upgrade files are downloaded.	-
at *time*	Specifies the AS restart time. If **reload** is specified but *time* is not specified, an AS restarts immediately after loading files. If *time* is specified, the AS restarts at the specified time.	The value is a string of characters in the HH:MM format, where HH:MM indicates the hour and minute. HH ranges from 0 to 23, and MM ranges from 0 to 59.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **upgrade as** command to upgrade online ASs. You can upgrade one AS, ASs of a specified type, or all ASs.

After performing upgrade configuration on an AS, the patch and system software files for the next startup will be the specified ones. You can run the **undo upgrade as** command to cancel the configuration as long as the AS is not restarted. After this command is executed, the patch and system software files for the next startup are consistent with the currently running ones. If the patch has taken effect after upgrade configuration is performed, the patch cannot be rolled back to the previous version.

Precautions

- The patch and system software files used to upgrade ASs are specified in the **as type** command. If no system software file is not specified using the **as type** command, an AS automatically uses the system software of the same version as the parent during an upgrade. If the system software of the same version as the parent does not exist, the AS continues to use the previous system software.
- The **upgrade as** command cannot upgrade an AS if the software file name or patch file name specified in the **as type** command is the same as the current or next startup software file name or patch file name of the AS.
- The **upgrade as** command cannot upgrade an AS if the software file name specified in the **as type** command does not exist.
- When you upgrade an AS using the **upgrade as** command without specifying **reload**:
  - If you specify **patch** *patch* but not **system-software** *system-software* in the **as type** command, the patch file is activated online immediately.
  - If you specify both **patch** *patch* and **system-software** *system-software* in the **as type** command and the specified system software file version is the version running on the AS, the patch file is activated online immediately.
  - If you specify both **patch***patch* and **system-software***system-software* in the **as type** command and the specified system software file version is earlier or later than the version running on the AS, the specified system software file and patch file will be set as next startup files.

Example

Perform an in-service upgrade on an AS of the S5720-P-LI type.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] upgrade as type s5720-p-li reload
```

3.5.114 upgrade { local-ftp-server | local-sftp-server }

Function

The **upgrade** { **local-ftp-server** | **local-sftp-server** } command configures a local file server.

The **undo upgrade** { **local-ftp-server** | **local-sftp-server** } command deletes a local file server.

By default, no local file server is configured.

NOTE

This command can only be executed on a parent switch.

Format

upgrade { **local-ftp-server** | **local-sftp-server** } **username** *username* **password** *password*

undo upgrade { **local-ftp-server** | **local-sftp-server** }

Parameters

Parameter	Description	Value
local-ftp-server	Specifies the file server type as FTP server.	-
local-sftp-server	Specifies the file server type as SFTP server.	-

Parameter	Description	Value

username *username*	Specifies the user name for accessing the file server.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		● Note the following when configuring case sensitivity for user names:
		  ● Only the user name is case-sensitive and the domain name is case-insensitive.
		  ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

password *password*	Specifies the password for accessing the file server.	The value is a string of case-sensitive characters without spaces. By default, the value is a string of 8 to 128 characters or 48 to 188 characters. You can enter a password in plain text or cipher text. The password is displayed in cipher text in the configuration file regardless of whether the password is input in plain or cipher text. ● The password in plain text is a string of 8 to 128 characters. ● The password in cipher text is a string of 48 to 188 characters. The password in cipher text cannot be generated using the irreversible algorithm.

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an AS automatic upgrade or in-service AS batch upgrade, you need to download the version file or patch file from the parent. Before the upgrade, you need to configure the parent as an FTP/SFTP server. The AS then can work as a client to download files from the FTP/SFTP server.

Precautions

- The files used to upgrade an AS are often saved in the root directory unimng/ of the parent. These files can also be saved on an AS when the AS is upgraded or downgraded to the software version that is consistent with that of the parent.
- FTP has potential security risks, and so SFTP is recommended. If you want to use FTP, you are advised to configure ACLs to improve security. For details, see Configure the FTP ACL in "File Management" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Basic Configuration*.
- When the file server is an FTP server, the parent automatically enables the FTP service and creates an FTP user. You only need to run the ftp server-source command to specify the source IP address of the FTP server.
- When the file server type is set to SFTP, the SFTP service is not automatically enabled and no SFTP user is created on the parent. You need to manually pre-configure SFTP on the parent.
- After the **upgrade** { **local-ftp-server** | **local-sftp-server** } command is executed, the same user name and password configuration is also generated in the AAA view. If you modify the configured local user information (the user password for example) in AAA view, the version management function does not take effect.
- If information about a user already exists in the AAA view, you cannot run this command to configure the same user name.
- Running this command multiple times to create new users will delete previous user information. Previous user information can be deleted only when the user level of the user running this command is higher or equal to the user level configured in the AAA view. Otherwise, the command does not take effect.
- If a remote authentication server is used for AAA authentication, the user name and password configured using this command must also be configured on the remote authentication server.
- If a remote authentication server is used for AAA authentication and the remote authentication server does not support FTP or SFTP, ASs will fail to be authenticated. In this case, run the **authentication-scheme** *authentication-scheme-name* command in the AAA view to create an authentication scheme and run the **authentication-mode local** command in the authentication scheme view to set the authentication mode to local authentication. Then, run the **domain** command in the AAA view to create a domain and run the **authentication-scheme** *authentication-scheme-name* command in the AAA

domain view to apply the created authentication scheme to the domain. ASs can be authenticated when they use the newly created domain for local authentication.

Example

Set the local file server type to FTP server.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] upgrade local-ftp-server username test password Pwd@12345
```

3.5.115 upload config

Function

The **upload config** command saves the AS configuration to the flash memory of an AS and uploads the configuration file of the AS to the parent.

NOTE

This command can only be executed on an AS.

Format

upload config

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In independent mode, after services are configured on an AS using commands, you can run the **upload config** command to save the service configuration and upload the configuration file to the parent.

Precautions

- After this command is executed, the AS configuration file uploaded to the parent will be saved to the **flash:/unimng/ind-cfg** directory or the **cfcard:/unimng/ind-cfg** directory on some parent switch models. If the file name format is unimng-xxxx-xxxx-xxxx.zip (xxxx-xxxx-xxxx indicates the management MAC address of an AS), and the service configuration mode of this AS is independent mode, it is not allowed to delete this configuration file.

- After the **upload config** command is executed, the AS configuration file may fail to be uploaded to the parent. The possible causes include insufficient storage space on the parent and a fault of the link between the AS and parent.
- To prevent services from being affected, it is recommended not to delete the configuration file saved on the AS.
- The AS configuration file saved on the parent can ensure configuration integrity for the AS. For example, after an AS goes online again or is replaced, the AS will compare its saved configuration file with that saved on the parent. If the two files are inconsistent, the configuration file saved on the parent will replace the configuration file saved on the AS and take effect after the AS restarts.

Example

Save the AS configuration to the flash memory of the AS and upload the configuration file of the AS to the parent.

```
<HUAWEI> upload config
```

3.5.116 user-access-port enable (network enhanced profile view)

Function

The **user-access-port enable** command configures the edge port function in a network enhanced profile.

The **undo user-access-port enable** command cancels the edge port function in a network enhanced profile.

By default, the edge port function is not configured in a network enhanced profile.

NOTE

This command can only be executed on a parent switch.

Format

user-access-port enable

undo user-access-port enable

Parameters

None

Views

Network enhanced profile view

Default Level

3: Management level

Usage Guidelines

After creating a network enhanced profile, you can configure the edge port function in the profile. After the profile is bound to an AS port, the port becomes an edge port. The following configuration is generated on the AS port:

```
#
 stp edged-port enable
#
```

Ports connected to a Layer 2 STP network do not need to participate in spanning tree calculation. If these ports participate in the calculation, the network topology convergence speed is affected and the status changes of these ports may cause network flapping. After these ports are configured as edge ports, they do not participate in spanning tree calculation. This configuration speeds up network topology convergence and enhances network stability.

Example

Enable the edge port function in a network enhanced profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-enhanced-profile name profile_1
[HUAWEI-um-net-enhanced-profile_1] user-access-port enable
```

3.5.117 user-access-profile name

Function

The **user-access-profile name** command creates a user access profile.

The **undo user-access-profile name** command deletes a user access profile.

By default, no user access profile is configured.

NOTE

This command can only be executed on a parent switch.

Format

user-access-profile name *profile-name*

undo user-access-profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user access profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain letters, digits, and underscores (_).

Views

uni-mng view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a user access profile, you can configure authentication services for user access (for example, the authentication mode), MAC address learning limiting, and the rate limit for incoming ARP and DHCP packets on an AS port.

Precautions

You can create a maximum of 16 user access profiles.

Example

Create a user access profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
```

3.5.118 user-access-profile (port group view)

Function

The **user-access-profile** command binds a user access profile to a port group.

The **undo user-access-profile** command unbinds a user access profile from a port group.

By default, no user access profile is bound to a port group.

NOTE

This command can only be executed on a parent switch.

Format

user-access-profile *profile-name*

undo user-access-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user access profile.	The value must have an existing user access profile name.

Views

Port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can bind a user access profile to a port group to deliver the configurations in the profile to all the member ports in the port group.

Prerequisites

The user access profile has been created.

Precautions

- A user access profile can be bound to only an AS port group but not an AP port group.
- A port group can be bound to only one user access profile.

Example

Bind a user access profile to a port group.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] user-access-profile name profile_1
[HUAWEI-um-user-access-profile_1] quit
[HUAWEI-um] port-group name group_1
[HUAWEI-um-portgroup-group_1] user-access-profile profile_1
```

3.5.119 user-vlan (network basic profile view)

Function

The **user-vlan** command configures the default VLAN in a network basic profile.

The **undo user-vlan** command deletes the default VLAN in a network basic profile.

By default, no default VLAN is configured in a network basic profile, and downlink ports of an AS use VLAN 1 as the default VLAN.

NOTE

This command can only be executed on a parent switch.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094. The value cannot be the ID of an SVF management VLAN, a stack management VLAN, an ERPS control VLAN, an RRPP control VLAN, an SEP control VLAN, or a super VLAN.

Views

Network basic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network basic profile, you can configure the default VLAN in the profile. After the profile is bound to an AS port, the default VLAN is automatically configured on the port. The following configuration is generated on the AS port:

```
#
 port link-type hybrid
 port hybrid pvid vlan vlan-id
 port hybrid tagged vlan 1
 port hybrid untagged vlan vlan-id
#
```

The **user-vlan** command can only configure the default VLAN for a port. To enable this port to allow packets of multiple VLANs to pass through, run the **pass-vlan** command in a network basic profile.

Precautions

The default VLAN, allowed VLANs, and voice VLAN in a network basic profile must be different.

Example

Configure the default VLAN in a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] user-vlan 10
```

3.5.120 user password (AS administrator profile view)

Function

The **user password** command configures an AS administrator in an AS administrator profile.

The **undo user** command deletes an AS administrator in an AS administrator profile.

By default, no AS administrator is configured in an AS administrator profile.

NOTE

This command can only be executed on a parent switch.

Format

user *user-name* **password** *password*

undo user *user-name*

Parameters

Parameter	Description	Value

user-name	Specifies a user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		- During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		- Note the following when configuring case sensitivity for user names:
		  - Only the user name is case-sensitive and the domain name is case-insensitive.
		  - For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  - When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Parameter	Description	Value
password	Specifies the password.	The value is a string of case-sensitive characters without spaces. By default, the value is a string of 8 to 128 characters or 48 to 188 characters. You can enter a password in plain text or cipher text. The password is displayed in cipher text in the configuration file regardless of whether the password is input in plain or cipher text. ● The password in plain text is a string of 8 to 128 characters. ● The password in cipher text is a string of 48 to 188 characters. The password in cipher text cannot be generated using the irreversible algorithm. Do not set this password to the weak password preset by running the **load security weak-password-dictionary** command.

Views

AS administrator profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating an AS administrator profile, you can configure an AS administrator in the profile, including the user name and password. After the profile is bound to an AS, the user name and password for login are automatically configured on the AS. The following configuration is generated on the AS:

```
#
aaa
 local-user user-name password irreversible-cipher password
 local-user user-name privilege level 3
 local-user user-name service-type terminal ssh
#
```

After an AS user name and password are configured, you need to enter the correct user name and password when logging in to an AS through the console port. When you log in to an AS from the parent using the **attach as name** *as-name* command, you can log in to the AS without entering the user name or password.

Precautions

In versions earlier than V200R020C00, when no AS user name and password are configured, you need to enter the default username and password when logging in to an AS through the console port. However, in V200R020C00 and later versions, there is no preset password for logging in to an AS through the console port, therefore, you must configure an AS user name and password before logging in to the AS through the console port.

The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Example

Configure the user name and password for an AS administrator.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] as-admin-profile name profile_1
[HUAWEI-um-as-admin-profile_1] user test password YsHsjx_202206
```

3.5.121 voice-vlan (network basic profile view)

Function

The **voice-vlan** command configures a voice VLAN in a network basic profile.

The **undo voice-vlan** command deletes the voice VLAN in a network basic profile.

By default, no voice VLAN is configured in a network basic profile.

NOTE

This command can only be executed on a parent switch.

Format

voice-vlan *vlan-id* [**include-untagged**]

undo voice-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 2 to 4094. The value cannot be the ID of an SVF management VLAN, a stack management VLAN, an ERPS control VLAN, an RRPP control VLAN, an SEP control VLAN, or a super VLAN.
include-untagged	Adds voice VLAN IDs to untagged packets.	-

Views

Network basic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a network basic profile, you can configure a voice VLAN in the profile. After the profile is bound to an AS port, the voice VLAN is automatically configured on the port. The following configuration is generated on the AS port:

- The **include-untagged** parameter is not specified:

```
#
 port link-type hybrid
 port hybrid tagged vlan vlan-id
 lldp tlv-enable med-tlv network-policy voice-vlan vlan vlan-id
 lldp compliance cdp txrx
#
```

- The **include-untagged** parameter is specified (S6735-S, S6720-EI, and S6720S-EI):

```
#
 port link-type hybrid
 port hybrid untagged vlan vlan-id
 voice-vlan vlan-id enable include-untagged include-tag0
 undo lldp tlv-enable med-tlv network-policy
#
```

- The **include-untagged** parameter is specified (except S6735-S, S6720-EI, and S6720S-EI):

```
#
 port link-type hybrid
 port hybrid untagged vlan vlan-id
 voice-vlan vlan-id enable include-untagged
 undo lldp tlv-enable med-tlv network-policy
#
```

Precautions

The default VLAN, allowed VLANs, and voice VLAN in a network basic profile must be different.

When configuring a voice VLAN on an AS port, ensure that IP phones connected to the AS port support LLDP and have LLDP enabled.

Example

Configure a voice VLAN in a network basic profile.

```
<HUAWEI> system-view
[HUAWEI] uni-mng
[HUAWEI-um] network-basic-profile name profile_1
[HUAWEI-um-net-basic-profile_1] voice-vlan 10
```

3.5.122 whitelist mac-address

Function

The **whitelist mac-address** command adds a specified MAC address to the whitelist.

The **undo whitelist mac-address** command deletes a MAC address from the whitelist.

By default, no MAC address is added to the whitelist. A maximum of 512 MAC addresses can be added to the whitelist.

NOTE

This command can only be executed on a parent switch.

Format

whitelist mac-address *mac-address1* [**to** *mac-address2*]

undo whitelist mac-address { *mac-address1* [**to** *mac-address2*] | **all** }

Parameters

Parameter	Description	Value
mac-address1 [**to** *mac-address2*]	Specifies MAC addresses to be added to a whitelist.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits. The value cannot be all 0s, all Fs, or a multicast MAC address.
all	Deletes all the MAC addresses in a whitelist.	-

Views

AS authentication view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SVF system needs to authenticate an AS, the SVF system allows the AS to connect to if the MAC address of the AS is in the whitelist and disallows the AS to connect to if the MAC address is in the blacklist.

Precautions

- A MAC address cannot exist in both the whitelist and blacklist.
- By default, if the MAC address of an AS is neither in the whitelist nor in the blacklist, the AS fails the authentication. You can run the **confirm** { **all** | **mac-address** *mac-address* } command to allow all ASs or a specified AS to pass the authentication.

Example

Add the MAC address xxxx-xxxx-xxxx to the whitelist.

```
<HUAWEI> system-view
[HUAWEI] as-auth
[HUAWEI-as-auth] whitelist mac-address xxxx-xxxx-xxxx
```

3.6 PoE Configuration Commands

3.6.1 Command Support

NOTE

Whether switches support PoE depends on the hardware. Non-PoE switches cannot be changed to PoE switches through software upgrades. A switch that meets any of the following conditions is a PoE switch:

- The device name contains PWR or PWH.
- The switch is released in V200R013C02 or later versions and provides new downlink interface types XUM, UM, P or U.

Only the following switch models support the PoE function:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731-S, S5731S-S, S5732-H, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-H, S5735S-S, S5735-S-I, S5736-S

3.6.2 display poe device

Function

The **display poe device** command displays information about the device supporting Power over Ethernet (PoE).

Format

display poe device

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before using the PoE function, run the **display poe device** command to check whether the device supports the PoE function. If the command output is displayed, the device supports the PoE function.

Example

Display information about the device supporting PoE.

```
<HUAWEI> display poe device
slot 0   : PoE
```

Table 3-123 Description of the display poe device command output

Item	Description
Slot 0	The device supports PoE.

3.6.3 display poe information

Function

The **display poe information** command displays PoE running information about the device.

Format

display poe information [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE running information in a specified slot ID. If this parameter is not specified, the PoE information about all device is displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information including the maximum output power set by the user, current power consumption, peak power consumption, and power management mode.

Example

Display the PoE running information about the device. (The actual output information may differ from the following information.)

```
<HUAWEI> display poe information
PSE Information of slot 0:
    User Set Max Power(mW)     : 739200
    PoE Power Supply(mW)       : 369600
    Available Total Power(mW)  : 369600
    Total Power Consumption(mW): 0
    Power Peak Value(mW)       : 0
    Power-Management Mode      : auto
    Power High Inrush          : disable
<HUAWEI> display poe information
PSE Information of slot 0:
MCU 1:
    User Set Max Power(mW)     : 739200
    PoE Power Supply(mW)       : 369600
    Available Total Power(mW)  : 369600
    Total Power Consumption(mW): 0
    Power Peak Value(mW)       : 0
    Power-Management Mode      : auto
    Power High Inrush          : disable
MCU 2:
    User Set Max Power(mW)     : 739200
    PoE Power Supply(mW)       : 369600
    Available Total Power(mW)  : 369600
    Total Power Consumption(mW): 0
    Power Peak Value(mW)       : 0
    Power-Management Mode      : auto
    Power High Inrush          : disable
```

Table 3-124 Description of the **display poe information** command output

Item	Description
User Set Max Power(mW)	Maximum output power set by the user. To set the value, run the **poe max-power** command. When the value is not set using the command, this field displays the maximum output power that can be provided by the device.

Item	Description
PoE Power Supply(mW)	PoE total power supply, which is determined by the PoE power module configured on the device. **NOTE** On the S5720I-6X-PWH-SI-AC switch, the total available power includes the power of two 12 V DC outputs and one 24 V AC output. No command is available to view the 12 V DC and 24 V AC output power. On the S5720I-10X-PWH-SI-AC switch, the total available power includes the power of two 12 V DC outputs and one 24 V AC output. To view the DC output power, run the **display device dc-output information** command.
Available Total Power(mW)	Remaining available power
Total Power Consumption(mW)	Total output power.
Power Peak Value(mW)	Peak value of the output power.
Power-Management Mode	Power management mode, including auto and manual modes. To set the mode, run the **poe power-management** command.
Power High Inrush	State of power high inrush function, including enabled and disabled state. By default, the power high inrush function is in disabled state. To set the state, run the **poe high-inrush enable** command.

3.6.4 display poe power

Function

The **display poe power** command displays current power information on interfaces.

Format

display poe power [**slot** *slot-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE power information in a specified slot ID. If this parameter is not specified, the PoE power information of all devices in a stack system or the PoE power information of the device in a non-stack system is displayed.	The value depends on the device configuration.
interface *interface-type interface-number*	Displays the PoE power information about a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If this parameter is not specified, the output power of all interfaces on the device is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe power** command displays information including the current actual power, maximum output power set for an interface, and class, reference power, and average power of PDs on the interface.

If this parameter is not specified, the output power of all interfaces on the device is displayed.

An interface provides 15400 mW power to PDs based on the power class 0 if non-standard PDs are connected to the interface or forcible power supply is configured on the interface of the switches except the S5720-16X-PWH-LI-AC, S5720-28X-

PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H. If you run the **display poe power** command to check the interface power, the PD class is displayed as 0.

Example

Display the power information of interfaces on the device whose ID is 0.

```
<HUAWEI> display poe power slot 0
Codes: REFPW(Reference power), USMPW(User set max power),
       CURPW(Current power), PKPW(Peak power), AVGPW(Average power)

PortName             Class  REFPW(mW) USMPW(mW) CURPW(mW) PKPW(mW)  AVGPW(mW)
-------------------------------------------------------------------------------
GigabitEthernet0/0/1   -     -        15400     0         0         0
GigabitEthernet0/0/2   -     -        15400     0         0         0
GigabitEthernet0/0/3   -     -        15400     0         0         0
GigabitEthernet0/0/4   -     -        15400     0         0         0
GigabitEthernet0/0/5   -     -        15400     0         0         0
GigabitEthernet0/0/6   -     -        15400     0         0         0
GigabitEthernet0/0/7   -     -        15400     0         0         0
GigabitEthernet0/0/8   -     -        15400     0         0         0
GigabitEthernet0/0/9   -     -        15400     0         0         0
GigabitEthernet0/0/10  -     -        15400     0         0         0
GigabitEthernet0/0/11  2     7000     15400     3710      3816      3487
GigabitEthernet0/0/12  2     7000     15400     2968      3180      2960
GigabitEthernet0/0/13  -     -        15400     0         0         0
GigabitEthernet0/0/14  -     -        15400     0         0         0
GigabitEthernet0/0/15  -     -        15400     0         0         0
GigabitEthernet0/0/16  -     -        15400     0         0         0
GigabitEthernet0/0/17  -     -        15400     0         0         0
GigabitEthernet0/0/18  -     -        15400     0         0         0
GigabitEthernet0/0/19  -     -        15400     0         0         0
GigabitEthernet0/0/20  -     -        15400     0         0         0
GigabitEthernet0/0/21  -     -        15400     0         0         0
GigabitEthernet0/0/22  -     -        15400     0         0         0
GigabitEthernet0/0/23  -     -        15400     0         0         0
GigabitEthernet0/0/24  -     -        15400     0         0         0
```

Table 3-125 Description of the display poe power slot command output

Item	Description
PortName	Name of an interface.
Class	Class of a PD on an interface. The system classifies PDs into nine classes, namely, class 0 to class 8, according to their maximum power. If no PD is connected to interface, "-" is displayed.
REFPW(mW)	Reference power of a PD. The system can identify the reference power of each PD. The value varies according to types of PDs.
USMPW(mW)	Maximum output power set for an interface. To set the value, run the **poe power** command.
CURPW(mW)	Current power of the PDs on an interface.

Item	Description
PKPW(mW)	Peak power of the PDs on an interface. The value is a statistical value, which equals the current maximum power consumption of the PDs on the interface.
AVGPW(mW)	Average power of the PDs on an interface. The value is a statistical value, which equals the average power consumption from the power-on of the interface till now.

Display the power of interface GigabitEthernet0/0/3.

```
<HUAWEI> display poe power interface gigabitethernet 0/0/3
PD power(mW)            : 3710
PD class                : 2
PD reference power(mW) : 7000
user set max power(mW) : 15400
PD peak power(mW)       : 3816
PD average power(mW)    : 3487
```

Table 3-126 Description of the display poe power interface command output

Item	Description
PD power(mW)	Output power of an interface.
PD class	Class of a PD on an interface. The system classifies PDs into nine classes, namely, class 0 to class 8, according to their maximum power.
PD reference power(mW)	Reference power of a PD. The system can identify the reference power of each PD. The value varies according to types of PDs.
user set max power(mW)	Maximum output power set for an interface. To set the value, run the **poe power** command.
PD peak power(mW)	Peak power of the PDs on an interface. The value is a statistical value, which equals the current maximum power consumption of the PDs on the interface.
PD average power(mW)	Average power of the PDs on an interface. The value is a statistical value, which equals the average power consumption from the power-on of the interface till now.

3.6.5 display poe power-state

Function

The **display poe power-state** command displays the PoE power supply status of a device.

Format

display poe power-state [**slot** *slot-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE power supply status of a specified slot ID. If the parameter is not specified, the PoE power supply status of all devices in a stack system or the PoE power supply status of a device in a non-stack system is displayed.	The value range depends on the device configuration.
interface *interface-type interface-number*	Displays the PoE power supply status of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the PoE power supply status of all interfaces on the device is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe power-state** command displays information including whether an interface is enabled to check compatibility of non-standard PDs, power supply status on of an interface, class of PDs on an interface, power supply priority, and maximum output power of an interface.

Example

Display the PoE power supply status of GigabitEthernet 0/0/3.

```
<HUAWEI> display poe power-state interface gigabitethernet 0/0/3
Legacy detect           : disable
Power enable state      : enable
Power fast-on state     : -
Single-class state      : disable
Power-up mode           : at
Power-on delay(s)       : 0
PD power auto-neg state : enable
PD power-up mode        : at
PD support mode         : af at
Power ON/OFF            : on
Power status            : Powered
PD class                : 4
Reference power(mW)     : 30000
Power priority          : Low
Max power(mW)           : 30000
Current power(mW)       : 8910
Peak power(mW)          : 10725
Average power(mW)       : 8779
Current(mA)             : 162
Voltage(V)              : 55
```

Table 3-127 Description of the **display poe power-state interface** command output

Item	Description
Legacy detect	Whether an interface is enabled to check compatibility of non-standard PDs. To enable an interface to check compatibility of non-standard PDs, run the **poe legacy enable** command.
Power enable state	Whether PoE is enabled on an interface. To enable PoE on an interface, run the **poe enable** command.
Power fast-on state	Whether PoE fast power-on is enabled on an interface. To enable PoE fast power-on on an interface, run the **poe fast-on enable** command. If this field displays -, the device does not support the **poe fast-on enable** command.
Single-class state	Single-class power supply mode of an interface: ● disable: standard power supply mode ● enable: single-class power supply To set this parameter, run the **poe single-class enable** command.

Item	Description
Power-up mode	Power supply mode of an interface. To set the power supply mode for an interface, run the **poe { at-inrush | pre-bt-inrush | bt-inrush } enable** command. If this field displays -, this interface does not support this configuration.
Power-on delay(s)	Power supply delay of an interface, in seconds. The value 0 indicates that power supply is not delayed. To set the power supply delay, run the **poe power-on delay** command.
PD power auto-neg state	Whether power auto-negotiation is enabled for interfaces. To enable power auto-negotiation for interfaces, run the **poe power auto-neg enable** command. **NOTE** The S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this field.
PD power-up mode	Current power supply standards of the PD connected to an interface: ● af: IEEE 802.3af ● at: IEEE 802.3at **NOTE** The S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this field.

Item	Description
PD support mode	Power supply standards supported by the PD connected to an interface: ● af: IEEE 802.3af ● at: IEEE 802.3at ● af at: both IEEE 802.3af and 802.3at **NOTE** The S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this field.
Power ON/OFF	Whether the interface is providing power: ● on: The interface is providing power. ● off: The interface is not providing power.

Item	Description
Power status	Power supply status of an interface: - Test mode: indicates the testing state. - Detecting: indicates the detection state. - Disabled: indicates that PoE is disabled on the interface. - Power-deny: indicates that the reference power is greater than the maximum output power of an interface. - Classification overcurrent: indicates that the current of the PD connected to the interface exceeds the threshold. - Unknown: indicates that the class of the PD is unknown. - Power overcurrent: indicates that the current of the PD connected to the interface exceeds the maximum current of the interface. - Power-on failed: indicates that the interface fails to provide power. - Power-ready: indicates that the interface is ready to provide power. - Powering: indicates that the PSE starts to power on the interface. - Powered: indicates that the interface is providing power. - Overloaded: indicates that the power is overloaded. - Time-range power-off: indicates that the interface is in the power-off time range. - Unstable voltage: indicates that the interface voltage is unstable. - Legacy disable: indicates that the PSE does not check the capability of PDs. - Class mismatch: indicates that the interface works in standard hierarchical power supply mode.
PD class	Class of a PD connected to an interface. The system classifies PDs into nine classes, namely, class 0 to class 8, according to their maximum power.
Reference power(mW)	Reference power of an interface. The system can identify the maximum power of a PD, classify the PD into a certain level, and define the reference power of each level.

Item	Description
Power priority	Power supply priority of an interface: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **poe priority** command.
Max power(mW)	Maximum output power of an interface. A maximum output power of 15400 mW indicates that the device complies with IEEE 802.3af. A maximum output power of 30000 mW indicates that the device complies with IEEE 802.3at. To set the value, run the **poe power** command.
Current power(mW)	Current output power of an interface.
Peak power(mW)	Peak output power of an interface.
Average power(mW)	Average output power of an interface.
Current(mA)	Output current of an interface.
Voltage(V)	Output voltage of an interface.

Display the PoE power supply status of the device.

```
<HUAWEI> display poe power-state slot 0
PORTNAME            POWERON/OFF  ENABLED  FAST-ON  PRIORITY STATUS
-------------------------------------------------------------------------------
GigabitEthernet0/0/1     off     enable   disable  Low      Detecting
GigabitEthernet0/0/2     off     enable   disable  Low      Detecting
GigabitEthernet0/0/3     off     enable   disable  Low      Detecting
GigabitEthernet0/0/4     off     enable   disable  Low      Detecting
GigabitEthernet0/0/5     off     enable   disable  Low      Detecting
GigabitEthernet0/0/6     off     enable   disable  Low      Detecting
GigabitEthernet0/0/7     off     enable   disable  Low      Detecting
GigabitEthernet0/0/8     off     enable   disable  Low      Detecting
GigabitEthernet0/0/9     off     enable   disable  Low      Detecting
GigabitEthernet0/0/10    off     enable   disable  Low      Detecting
GigabitEthernet0/0/11    off     enable   disable  Low      Detecting
GigabitEthernet0/0/12    off     enable   disable  Low      Legacy disable
```

Table 3-128 Description of the display poe power-state slot command output

Item	Description
PORTNAME	Name of an interface.
POWERON/OFF	Whether the interface is providing power: ● On: The interface is providing power. ● Off: The interface is not providing power.

Item	Description
ENABLED	Whether PoE is enabled on an interface. To enable PoE on an interface, run the **poe enable** command.
FAST-ON	Whether PoE fast power-on is enabled on an interface. To enable PoE fast power-on on an interface, run the **poe fast-on enable** command.
PRIORITY	Power supply priority of an interface: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **poe priority** command.

Item	Description
STATUS	Power supply status of an interface: - Test mode: indicates the testing state. - Detecting: indicates the detection state. - Disabled: indicates that PoE is disabled on the interface. - Power-deny: indicates that the reference power is greater than the maximum output power of an interface. - Classification overcurrent: indicates that the current of the PD connected to the interface exceeds the threshold. - Unknown: indicates that the class of the PD is unknown. - Power overcurrent: indicates that the current of the PD connected to the interface exceeds the maximum current of the interface. - Power-on failed: indicates that the interface fails to provide power. - Power-ready: indicates that the interface is ready to provide power. - Powering: indicates that the PSE starts to power on the interface. - Powered: indicates that the interface is providing power. - Overloaded: indicates that the power is overloaded. - Time-range power-off: indicates that the interface is in the power-off time range. - Unstable voltage: indicates that the interface voltage is unstable. - Legacy disable: indicates that the PSE does not check the capability of PDs. - Class mismatch: indicates that the interface works in standard hierarchical power supply mode.

3.6.6 display poe-power

Function

The **display poe-power** command displays information about the PoE power supply.

Format

display poe-power [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe-power** displays information including the available total PoE power, percentage of the reserved power, power alarm threshold, and PoE power module.

If the stack ID is not specified, information about the PoE power supply of all the stack devices is displayed.

Example

Display information about the PoE power supply of a switch (except S5720I-28X-PWH-SI-AC).

```
<HUAWEI> display poe-power
Slot 0
Total Available PoE Power(mW)  : 246400
Reserved PoE Power Percent     : 20 %
PoE Power Threshold Percent    : 90 %
    PoE Power 1
    Power Value(mW)            : 123200
    Type                       : PSA250-A2
    Supported Mode             : Redundancy, Balance
    PoE Power 2
    Power Value(mW)            : 123200
    Type                       : PSA250-A2
    Supported Mode             : Redundancy, Balance

Slot 1
Total Available PoE Power(mW) : 492800
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %
    PoE Power 1
    Power Value(mW)            : 123200
    Type                       : PSA250-A2
    Supported Mode             : Redundancy, Balance
    PoE Power 2
    Power Value(mW)            : 369600
    Type                       : PSA500-A1
    Supported Mode             : Redundancy, Balance

Slot 2
Total Available PoE Power(mW) : 739200
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %
```

```
    PoE Power 1
    Power Value(mW)           : 369600
    Type                      : PSA500-A1
    Supported Mode            : Redundancy, Balance
    PoE Power 2
    Power Value(mW)           : 369600
    Type                      : PSA500-A1
    Supported Mode            : Redundancy, Balance
```

Display information about the PoE power supply of S5720I-28X-PWH-SI-AC.

```
<HUAWEI> display poe-power
Slot 0
Total Available PoE Power(mW) : 369600
Power backup-mode             : 2+0
MCU 1:
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %
MCU 2:
Reserved PoE Power Percent    : 20 %
PoE Power Threshold Percent   : 90 %

    PoE Power 1
    Power Value(mW)           : 369600
    PoE Power 2
    Power Value(mW)           : -
```

Table 3-129 Description of the display poe-power command output

Item	Description
Total Available PoE Power(mW)	Total power that can be provided for PDs.
Power backup-mode	PoE power supply backup mode: ● 2+0: high power mode ● 1+1: backup mode
MCU 1/MCU 2	MCU ID.
PoE Power 1/PoE Power 2	PoE Power ID.
Reserved PoE Power Percent	Percentage of the reserved power to the total power. To set the percentage, run the **poe power-reserved** command.
PoE Power Threshold Percent	Alarm threshold of the power consumption percentage. To set the threshold, run the **poe power-threshold** command.
Power Value(mW)	Power of a PoE power supply.

Item	Description
Type	Type of a PoE power supply. The value can be: ● PSA250-A1: 250 W non-current-balance power supply ● PSA250-A2: 250 W current balance power supply ● PSA500-A1: 500 W current balance power supply ● PAC1000S56-CB: 1000W AC power supply ● PAC1000S56-DB: 1000W AC power supply ● PDC1000S56-CB: 1000W DC power supply ● PAC600S56-CB: 600W AC & 240V DC power module ● PAC600S56-EB: 600W AC & 240V DC power module ● PAC1000S56-EB: 1000W AC & 240V DC power module ● PDC1000S56-EB: 1000W DC power module
Supported Mode	Supported PoE power supply mode. The value can be: ● Redundancy: redundancy backup mode ● Balance: current balance mode

3.6.7 poe af-inrush enable

Function

The **poe af-inrush enable** command configures the power supply standards of interfaces as 802.3af.

The **undo poe af-inrush enable** command restores the power supply standards of interfaces to the default value.

By default, interfaces on the devices supporting PoE++ comply with 802.3bt, the other interfaces comply with 802.3at.

Format

poe af-inrush enable

undo poe af-inrush enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Switches that comply with 802.3at or 802.3bt cannot power some non-standard PDs that do not support inrush current. To power these PDs, configure the power supply standards of interfaces as 802.3af.

Precautions

- The **poe af-inrush enable** command applies to the scenario where some non-standard PDs cannot be powered on. After this command is executed, some PDs requiring high current may be unable to be powered on.
- After running the **poe af-inrush enable** command, remove non-standard PDs and then install them so that they can be powered on.
- On the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H, the **poe af-inrush enable** and **poe single-class enable** commands are mutually exclusive and cannot be configured on the same interface.
- In an upgrade to V200R011C10 or later, if the **poe af-inrush enable** command is configured in the system view before the upgrade, the **poe af-inrush enable** command configuration is automatically generated on all interfaces after the upgrade.

Example

Configures the power supply standards of interfaces as 802.3af.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe af-inrush enable
Warning: This operation will cause PD to be powered off. Continue?[Y/N]:y
```

3.6.8 poe anti-interference frequency

Function

The **poe anti-interference frequency** command configures the PoE anti-interference frequency of the device.

The **undo poe anti-interference frequency** command restores the default configuration.

By default, the PoE anti-interference frequency of a device is 50 Hz.

NOTE

PoE models in the S5720-LI, S5720S-LI, and S5720I-SI series do not support this command. PoE models in other series support this command.

Format

poe anti-interference frequency { **50** | **60** }

undo poe anti-interference frequency

Parameters

Parameter	Description	Value
50	Sets the anti-interference frequency to 50 Hz.	-
60	Sets the anti-interference frequency to 60 Hz.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The mains frequency varies in different countries and regions. Some are 60 Hz and some are 50 Hz. When a device provide PoE power supply, incorrect grounding may occur. As a result, industrial frequency interference is coupled to network cables, resulting in abnormal PoE detection classification. You can run the **poe anti-interference frequency** command to modify the PoE anti-interference frequency on the device to make that become the same as the mains frequency, reducing the impact of the mains frequency on PoE detection.

Example

Set the PoE anti-interference frequency of a device to 60 Hz.

```
<HUAWEI> system-view
[HUAWEI] poe anti-interference frequency 60
```

3.6.9 poe { at-inrush | pre-bt-inrush | bt-inrush } enable

Function

The **poe { at-inrush | pre-bt-inrush | bt-inrush } enable** command changes the power supply mode of interfaces supporting the PoE++ mode.

The **undo poe { at-inrush | pre-bt-inrush | bt-inrush } enable** command restores the default power supply mode of PoE interfaces.

By default, interfaces supporting the PoE++ mode on devices provide power in PoE ++ mode. That is, the power supply mode is **bt-inrush**, interfaces not supporting the PoE++ mode on devices provide power in **at-inrush** mode.

NOTE

Only the MultiGE interface of an S5720-28X-PWH-LI-AC, the first 12 electrical interfaces of an S5720-16X-PWH-LI-AC, the first 8 electrical interfaces of an S5720I-28X-PWH-SI-AC, and electrical interfaces of the S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-PWH-SI-DC, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731S-H, S5731-S, S5731S-S, and S5732-H support this command.

Format

poe { **at-inrush** | **pre-bt-inrush** | **bt-inrush** } **enable**

undo poe { **at-inrush** | **pre-bt-inrush** | **bt-inrush** } **enable**

Parameters

Parameter	Description	Value
at-inrush	Sets the power supply mode to PoE+.	-
pre-bt-inrush	Sets the power supply mode to PoE++ compatible. That is, except that the PoE power is 60000 mW, interfaces comply with 802.3at. **NOTE** The S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731S-H, S5731-S, and S5731S-S do not support the **pre-bt-inrush**.	-
bt-inrush	Sets the power supply mode to PoE++. **NOTE** The S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731S-H, S5731-S, and S5731S-S do not support the **bt-inrush**.	-

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To power the PDs requiring the standard power supply mode, run the **poe at-inrush enable** command. This command changes the power supply mode of the PoE interface to the PoE+ mode. If most of the parameters supported by the PDs requiring high power comply with 802.3at, run the **poe pre-bt-inrush enable** command to change the power supply mode of these interfaces to PoE++ compatible.

Precautions

- When the **poe bt-inrush enable** command is configured after the **poe af-inrush enable** command is configured in the interface, the **poe af-inrush enable** command configuration is automatically overwritten.
- The **poe { pre-bt-inrush | bt-inrush } enable** and **poe single-class enable** commands are mutually exclusive and cannot be configured on the same interface.
- Changing the power supply mode of a PoE interface will power off the PD connected to this PoE interface.
- After the power supply mode of an interface is set to **bt-inrush**, forcible PoE power supply and PD compatibility check configured on this interface using the **poe force-power** and **poe legacy enable** commands respectively do not take effect on this interface.
- After the power supply mode of an interface is set to **bt-inrush**, and the interface detects that it connects to a non-standard PD, confirm whether this interface is connected to a PD. If so, run the **poe pre-bt-inrush enable** command and the **poe legacy enable** or **poe force-power** command to provide power to this PD.

Example

Set the power supply mode of GE0/0/1 to PoE+.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe at-inrush enable
Warning: This operation will cause the PD to be powered off. Continue?[Y/N]:y
```

Set the power supply mode of GE0/0/1 to PoE++ compatible.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe pre-bt-inrush enable
Warning: This operation will cause the PD to be powered off. Continue?[Y/N]:y
```

3.6.10 poe enable

Function

The **poe enable** command enables the PoE function on an interface.

The **undo poe enable** command disables the PoE function on an interface.

By default, the PoE function is enabled on an interface.

Format

poe enable

undo poe enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

Before providing power for the PD connected to an interface, ensure that the PoE function has been enabled on the interface. If the PoE function is not enabled on the interface, run the **poe enable** command to enable the PoE function on the interface.

In automatic mode, PD power-on and power-off on interfaces are determined by the PoE power and interface power priority. When the PoE power is sufficient, the device does not power off the PD connected to any interface. To stop providing power for a PD, run the **undo poe enable** command on the interface to which the PD is connected.

Precautions

The device only supports PoE power supply on downlink interfaces and does not support PoE power supply on uplink interfaces.

Example

Disable the PoE function on GigabitEthernet0/0/3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3] undo poe enable
```

3.6.11 poe fast-on enable

Function

The **poe fast-on enable** command enables fast power-on for a PoE interface.

The **undo poe fast-on enable** command disables fast power-on for a PoE interface.

By default, fast power-on is disabled on a PoE interface.

NOTE

Only the S5720-28X-PWH-LI-AC, S5720-16X-PWH-LI-AC, S5720I-12X-PWH-SI-DC, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5731-H, S5731S-H, S5731-S, S5731S-S, and S5732-H support this command.

Format

poe fast-on enable

undo poe fast-on enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PoE switch is powered off and then restarts, interfaces on this device can be powered on again only after a certain period. As a result, PDs connected to these interfaces are powered off within this period. To shorten the time during which the PDs are powered off, you can run the **poe fast-on enable** command on the PoE switch. After the PoE switch is powered off and then restarts, PoE interfaces can rapidly resume power supply to PDs.

Precautions

- This command takes effect only during cold startup of the device.
- The **poe fast-on enable** command does not generate any configuration but always takes effect after being executed until the **undo poe fast-on enable** command is executed. To determine whether the fast power-on configuration takes effect, run the **display poe power-state** command to check the **fast-on** field.

Example

Enable fast power-on for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe fast-on enable
Warning: This configuration takes effect only after a cold restart. Continue?[Y/N]:y
Warning: Ensure that the power required by the connected PD does not exceed the rated PoE power
provided by the device. Otherwie, the device may not start normally. Continue?[Y/N]:y
```

Disable fast power-on for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo poe fast-on enable
Warning: This configuration takes effect only after a cold restart. Continue?[Y/N]:y
```

3.6.12 poe force-power

Function

The **poe force-power** command enables forcible powering on a PoE interface.

The **undo poe force-power** command disables forcible powering on a PoE interface.

By default, forcible powering is disabled on a PoE interface.

Format

poe force-power

undo poe force-power

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the power of the system is sufficient, you can run the **poe force-power** command on the interface connected to PDs when the PSE cannot detect the PDs.

Precautions

After the power supply mode of an interface is set to PoE++ using the **poe bt-inrush enable** command, the **poe force-power** command does not take effect on this interface.

The **poe force-power** command and the **poe legacy enable** command are mutually exclusive. When configured on the same interface, the later configured command takes effect and the earlier configured command is cleared.

If the interface connects to a non-PD device, configuring forcible powering on the interface may damage the non-PD device. Exercise caution when using the **poe force-power** command. After forcible powering is configured on a PoE switch, you must delete the forcible powering configuration from the switch if you need to remove the switch from the current networking environment and deploy it in a new networking environment.

Example

Enable forcible powering on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe force-power
Warning: Is there a valid PD connected to this interface? Yes or No?[Y/N]:y
```

3.6.13 poe group management enable

Function

The **poe group management enable** command enables a PoE device's group management of PDs.

The **undo poe group management enable** command disables a PoE device's group management of PDs.

By default, a PoE device's group management of PDs is disabled.

NOTE

Among PoE models, the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5731-H, S5731-S, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5736-S24UM4XC, and S5731S-S do not support this command.

Format

poe group management enable

undo poe group management enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Powering on some PDs may affect other PDs, causing other PDs unable to be detected by a PoE device. After group management of PDs is enabled, a PoE device can detect PDs on a per-group basis and power on these PDs in a batch.

Precautions

- To support a PoE device's group management of PDs, every four interfaces on the left are added to one group. For example, interfaces numbered 1 to 4 or numbered 5 to 8 can be added to one group, but interfaces numbered 2 to 5 cannot. That is, the number of the last interface in each group must be the multiple of 4. If the **poe group management enable** command is configured on any interface in a group, this command is also delivered to the other three interfaces in the same group.

- After group management of PDs is configured on an interface, the other interfaces in the same group use the same power supply priority as this interface and this priority is lower than that of other interfaces that are not added to any group. If some interfaces have this group management function configured, the PoE interface power supply priority configured using the **poe priority** command does not take effect on these interfaces.

Example

Enable group management of PDs on PoE interfaces GE0/0/1 through GE0/0/4.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe group management enable
Info: 'Poe group management enable' will be executed on interface GigabitEthernet0/0/1 to
GigabitEthernet0/0/4. Continue?[Y/N]: y
```

3.6.14 poe high-inrush enable

Function

The **poe high-inrush enable** command configures an interface to allow generation of the high pulse current during power-on.

The **undo poe high-inrush enable** command configures an interface not to allow generation of the high pulse current during power-on.

By default, interfaces do not allow generation of the high pulse current during power-on.

Format

poe high-inrush enable [**slot** *slot-id*]

undo poe high-inrush enable [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

High inrush current is generated when a non-standard PD is powered on. In this case, the PSE cuts off the power of the PD to protect itself. If the PSE is required to provide power for the PD, the PSE must allow high inrush current. The high inrush current may damage device components.

Example

Enable the device to allow generation of the high pulse current during power-on.

```
<HUAWEI> system-view
[HUAWEI] poe high-inrush enable
```

3.6.15 poe { power-off | power-on } interface

Function

The **poe** { **power-off** | **power-on** } **interface** command manually powers on or powers off the PD of an interface.

NOTE

Among PoE models, the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H do not support this command.

Format

poe { **power-off** | **power-on** } **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
power-off	Powers off an interface.	-
power-on	Powers on an interface.	-
interface-type interface-number	Specifies the type and number of the interface that needs to be powered on or powered off manually.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

By default, a PoE device works in automatic power management mode. After a PD is connected to a PoE device, the PoE device automatically provides power for the PD.

After you run the **poe power-management** command to configure the power management mode of a PoE device to manual, the PoE device does not automatically provide power for PDs when PDs are connected to the PoE device. You need to run the **poe power-on interface** command to manually power on the interfaces of the PoE device. Check whether the interface is powered on based on the Power ON/OFF field in the **display poe power-state** command.

Precautions

When the available power of the device is insufficient and the device cannot provide power for a new PD, the **poe power-on interface** command is invalid.

Pre-configuration Tasks

Before powering on or powering off an interface, ensure that:

- The power management mode has been in manual mode through running the **poe power-management** command.
- PDs have been connected to the interface.
- The PoE function of the interface has been enabled.
- The classification of the PDs connected to the interface has finished and the PDs have been ready for being powered on.

Example

Manually power on PDs connected to GigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] poe power-management manual
[HUAWEI] poe power-on interface gigabitethernet 0/0/1
```

3.6.16 poe legacy enable

Function

The **poe legacy enable** command enables the power sourcing equipment (PSE) to check the compatibility of power devices (PDs).

The **undo poe legacy enable** command disables the PSE from checking the compatibility of PDs.

By default, the PSE does not check the capability of PDs.

Format

poe legacy enable

undo poe legacy enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the switch is enabled to check the compatibility of PDs, the switch can detect and provide power to the PDs that do not comply with the 802.3af or 802.3at standard or the standard PDs that are detected as non-standard PDs because of the external environment. If compatibility check is disabled, the switch cannot provide power to the non-standard PDs.

After interfaces are enabled to check the compatibility of PDs, the interfaces can provide power to both standard and non-standard PDs. This configuration does not affect the power supply of standard PDs. That is, the interfaces can still provide power to standard PDs after the **poe legacy enable** command is configured.

Precautions

After the power supply mode of an interface is set to PoE++ using the **poe bt-inrush enable** command, the **poe legacy enable** command does not take effect on this interface.

The **poe force-power** command and the **poe legacy enable** command are mutually exclusive. When configured on the same interface, the later configured command takes effect and the earlier configured command is cleared.

If the interface is connected to a non-PD device, enabling PD compatibility check may damage this non-PD device. Exercise caution when you use this command. After enabling PD compatibility check on a PoE switch, you need to manually disable this function if you need to remove the switch from the current networking environment and deploy it in a new networking environment.

Example

Enable GigabitEthernet0/0/1 to check the compatibility of the PD.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe legacy enable
```

3.6.17 poe lldp-proxy

Function

The **poe lldp-proxy** command configures a 10GE optical port as a proxy for a MultiGE electrical port to perform LLDP negotiation.

The **undo poe lldp-proxy** command restores the default configuration.

By default, a 10GE optical port does not act as a proxy for a MultiGE electrical port to perform LLDP negotiation.

NOTE

Only the S5732-H48XUM2CC supports this command.

Format

poe lldp-proxy interface multige *interface-number*

undo poe lldp-proxy

Parameters

Parameter	Description	Value
interface multige *interface-number*	Specifies the number of a MultiGE electrical port.	It must be a MultiGE electrical port on the panel of an S5732-H48XUM2CC switch.

Views

XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hybrid optical/electrical cables integrate optical fibers and electrical cables and are used to connect S5732-H48XUM2CC switches to APs. Hybrid optical/electrical cables are often used in the following scenarios:

- One end of the RJ45 cable in a hybrid optical/electrical cable is connected to a MultiGE electrical port of a switch, and the other end is connected to the RJ45 power receiving port of an AP. The RJ45 cable is used only for the switch to provide PoE power supply for the AP and does not transmit data.
- One end of the optical fiber in a hybrid optical/electrical cable is connected to a 10GE optical port on a switch, and the other end is connected to an uplink

10GE optical port on an AP. The optical fiber is used for data transmission between the switch and AP.

Since the MultiGE electrical port connected to a hybrid optical/electrical cable stays in the **down** state, to use LLDP to negotiate the power supply capability, you must run the **poe lldp-proxy** command to configure the 10GE optical port on the switch connected to the hybrid optical/electrical cable as a proxy for the MultiGE electrical port to perform LLDP negotiation.

Precautions

- LLDP must be enabled on the 10GE optical port connected to a hybrid optical/electrical cable. This function is enabled by default.
- If an AP requires PoE++ power supply, run the **poe legacy enable** command on the 10GE optical port connected to a hybrid optical/electrical cable to enable compatibility check.

Example

Configure the 10GE 0/0/1 optical port as a proxy for the MultiGE 0/0/1 electrical port to perform LLDP negotiation.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] poe lldp-proxy interface MultiGE 0/0/1
```

3.6.18 poe max-power

Function

The **poe max-power** command sets the maximum output power of the device.

The **undo poe max-power** command restores the default maximum output power of the device.

By default, the maximum output power of a device is the power actually provided by the device. Therefore, the configured maximum output power must be lower than or equal to the total power of PoE power modules. On the S5720I-12X-PWH-SI-DC, the default maximum output power is 220000 mW, and the supported maximum output power is 240000 mW. On the S5720I-10X-PWH-SI-AC, the default maximum output power is 175000 mW. When the 110 V voltage is input, the maximum output power is 175000 mW. When the input voltage is 220 V, the maximum output power is 200000 mW.

Format

poe max-power *max-power* [**slot** *slot-id* [**mcu** *mcu-id*]]

undo poe max-power *max-power* **slot** *slot-id*

undo poe max-power [**slot** *slot-id* [**mcu** *mcu-id*]]

NOTE

Only the S5720I-28X-PWH-SI-AC supports the **mcu** *mcu-id* parameter.

Parameters

Parameter	Description	Value
max-power	Specifies the maximum output power.	The value is an integer that ranges from 15400 to 2880000, in mW.
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
mcu *mcu-id*	Specifies an MCU ID.	The value is 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a stack, if no stack ID is added to the **poe max-power** command, this command sets the maximum output power of all stack member switches.

Precautions

- If the configured maximum output power is lower than the total power required by PDs, lower-priority PDs will be powered off or cannot be powered on manually.
- The configured maximum output power of the device must be lower than the remaining PoE power of the device. Otherwise, the configuration does not take effect.

Example

Set the maximum output power of the device with the ID 0 to 45000 mW.

```
<HUAWEI> system-view
[HUAWEI] poe max-power 45000 slot 0
```

3.6.19 poe power

Function

The **poe power** command sets the maximum output power of an interface.

The **undo poe power** command restores the default maximum output power of an interface.

This default value varies depending on interfaces of switches:

- The electrical interface of an S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5736-S24UM4XC, S5736-S24U4XC, S5736-S48U4XC, S5735S-H24U4XC-A, or S5735S-H48U4XC-A: 90000 mW
- The MultiGE interface of an S5720-28X-PWH-LI-AC: 60000 mW; Other electrical interface of an S5720-28X-PWH-LI-AC: 30000 mW
- First 8 electrical interfaces of an S5720I-28X-PWH-SI-AC: 60000 mW; last 16 electrical interfaces of an S5720I-28X-PWH-SI-AC: 30000 mW
- The electrical interface of an S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-PWH-SI-DC, S5720-16X-PWH-LI-AC, or S5732-H: 60000 mW
- The electrical interface of other PoE devices: 30000 mW

Format

poe power *port-max-power*

undo poe power

Parameters

Parameter	Description	Value
port-max-power	Specifies the maximum output power of an interface.	The value is an integer, in mW. - For a electrical interface of S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5736-S24UM4XC, S5736-S24U4XC, S5736-S48U4XC, S5735S-H24U4XC-A, or S5735S-H48U4XC-A, the value ranges from 0 to 90000. - For a MultiGE interface of S5720-28X-PWH-LI-AC, the value ranges from 0 to 60000. For other an electrical interface of S5720-28X-PWH-LI-AC, the value ranges from 0 to 30000. - For the first 8 electrical interfaces of an S5720I-28X-PWH-SI-AC, the value ranges from 0 to 60000. For the last 16 electrical interfaces of an S5720I-28X-PWH-SI-AC, the value ranges from 0 to 30000. - For an electrical interface of S5720I-6X-PWH-SI-AC, S5720I-10X-PWH-SI-AC, S5720I-12X-PWH-SI-DC, S5720-16X-PWH-LI-AC, S5732-H, or the value ranges from 0 to 60000.

Parameter	Description	Value
		- For electrical interfaces of other PoE devices, the value ranges from 0 to 30000.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The PD negotiation power may be different from the power required by some non-standard PDs or PDs that cannot be classified. You can run the **poe power** command to set the maximum output power of the interface, which prevents power overload for PDs and saves energy.

Prerequisites

The PoE function has been enabled on the interface using the **poe enable** command.

Example

Set the maximum output power on GigabitEthernet0/0/1 to 15400 mW.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power 15400
```

3.6.20 poe power auto-neg enable

Function

The **poe power auto-neg enable** command enables power auto-negotiation for interfaces.

The **undo poe power auto-neg enable** command disables power auto-negotiation for interfaces.

By default, power auto-negotiation is disabled for interfaces.

NOTE

Among PoE models, only the S5731-H(except S5731-H48HB4XZ and S5731-H24HB4XZ), S5731-S, S5731S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-PWR-LI-AC, S5720-52P-PWR-LI-AC, S5720-28X-PWR-LI-AC, S5720-28X-PWR-LI-ACF, S5720-52X-PWR-LI-AC, S5720-52X-PWR-LI-ACF, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-PWR-LI-AC, S5720S-52P-PWR-LI-AC, S5720S-28X-PWR-LI-AC, and S5720S-52X-PWR-LI-AC support this command.

Format

poe power auto-neg enable

undo poe power auto-neg enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch supplies power to the APs connected to interfaces in compliance with IEEE 802.3at (the maximum output power is 30 W). Some APs support both IEEE 802.3at and 802.3af. The switch can supply power to these APs in accordance with IEEE 802.3af (the maximum output power is 15.4 W). When the APs connected to the switch support both IEEE 802.3at and 802.3af, enable power auto-negotiation on the interfaces connected to these APs. When the total available power of the switch is less than 30 W and the switch detects that the current power supply standards of an AP are IEEE 802.3at, the switch can send an LLDP packet to the AP to enable the AP to set its power supply standards to IEEE 802.3af. Power auto-negotiation changes only the power supply standards of APs but not the interfaces to which the APs are connected.

Enabling power auto-negotiation on interfaces will change the power supply standards of the APs connected to the interfaces, reduce the power consumption of the APs, and enable the switch to supply power to more APs when the rated output power of the switch is fixed.

Precautions

- The **poe power auto-neg enable** command is mutually exclusive with the **lldp dot3-tlv power 802.1ab force** and **lldp dot3-tlv power 802.3at** commands and cannot be configured together.
- When the total available power of the switch is less than 30 W, the power supply standards of all the APs connected to the interfaces that have power

auto-negotiation enabled will be set to IEEE 802.3af. When the total available power of the switch is more than the larger value of 60 W and reserved power, the power supply standards of the APs connected to the interfaces will be restored to IEEE 802.3at based on the power supply priority configured on the interfaces. That is, the power supply standards of the AP connected to the interface with a higher priority are restored to IEEE 802.3at. If the power supply priority of these interfaces is the same, the power supply standards of the AP connected to the interface with a smaller interface number are restored to IEEE 802.3at first.

- Disabling power auto-negotiation on an interface will restore the power supply standards of the AP connected to the interface to IEEE 802.3at. This operation will power off the APs connected to some interfaces if the total power of the switch is insufficient.

Example

Enable power auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power auto-neg enable
Warning: This operation will enable PoE power auto-negotiation of the port, which will change the power-
up mode of the PD connected to the port from AT to AF in case of insufficient power. Continue?[Y/N]:y
```

3.6.21 poe power-management

Function

The **poe power-management** command sets the power management mode of the device.

The **undo poe power-management** command restores the default power management mode of the device.

By default, the device uses the automatic power management mode.

NOTE

Among PoE models, the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H do not support this command.

Format

poe power-management { **auto** | **manual** } [**slot** *slot-id*]

undo poe power-management { **auto** | **manual** } **slot** *slot-id*

undo poe power-management [**slot** *slot-id*]

Parameters

Parameter	Description	Value
auto	Specifies the power management mode to automatic mode.	-
manual	Specifies the power management mode to manual mode.	-
slot *slot-id*	Specifies the slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In automatic power management mode, the device first provides power for the interfaces with higher priority and powers off the interfaces of lower priority when the power is insufficient. When the power is sufficient, all interfaces connected to PDs are powered on. To stop providing power for some interfaces, run the **undo poe enable** command to disable the PoE function on the interfaces. If the PoE function is enabled and disabled frequently, faults may occur on the interfaces. To prevent the faults, you can set the power management mode to manual mode. In manual mode, the power-on and power-off of an interface are controlled manually and not affected by the interface power priority.

Precautions

- If all the interfaces are of the same priority, the power supply priority of the interface with a smaller interface number is higher in automatic mode.
- You can view the power management mode by running the **display poe information** command.

Follow-up Procedures

After setting the power management mode to manual, you need to run the **poe { power-off | power-on } interface** command to manually power on or off the PDs connected to interfaces of the device. If the device restarts after being powered off, you need to run the **power-on** command on the interfaces again to power on the PDs connected to the interfaces. If the device restarts without being powered off, you do not need to run the **power-on** command on the interfaces again to power on the PDs.

Example

Set the power management mode of a device to automatic mode.

```
<HUAWEI> system-view
[HUAWEI] poe power-management auto slot 0
```

3.6.22 poe power-off time-range

Function

The **poe power-off time-range** command makes a configured PoE power-off time range effective on an interface.

The **undo poe power-off time-range** command cancels the configuration.

By default, a device is not configured with PoE power-off time range.

Format

poe power-off time-range *time-range-name*

undo poe power-off time-range

Parameters

Parameter	Description	Value
time-range-name	Specifies a name for a PoE power-off time range.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word all cannot be specified as a time range name.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **poe power-off time-range** command makes a PoE power-off time range set in the system view effective on an interface. If the current time is within the specified time range, the PD connected to the interface cannot be powered on.

The **undo poe power-off time-range** command cancels the configuration. The time range does not take effect on the PD connected to the interface; however, the configuration of the time range is still saved.

Pre-configuration Tasks

Before running the **poe power-off time-range** command, you must ensure a PoE power-off time range has been configured through running the **time-range** command in the system view.

Example

Configure a PoE power-off time range from 10:00 to 11:00 for PDs connected to GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] time-range PoE 10:00 to 11:00 daily
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power-off time-range PoE
```

3.6.23 poe power-on delay

Function

The **poe power-on delay** command sets the PoE power supply delay on an interface.

The **undo poe power-on delay** command restores the default PoE power supply delay on an interface.

By default, the PoE power supply delay is 0. That is, the PoE power supply is not delayed.

Format

poe power-on delay *delay-time*

undo poe power-on delay

Parameters

Parameter	Description	Value
delay-time	Specifies the PoE power supply delay.	The value is an integer that ranges from 1 to 60, in seconds.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maintain current of the used PD is insufficient at the power-on moment, so the PoE switch considers that the PD has been disconnected and powers it off.

IEEE standards require that a PD must maintain a current value of more than 10 mA for at least 75 ms in each 325 ms duration. Otherwise, the PoE switch considers that the PD has left and powers off the PD.

To enable the PoE switch to power these non-standard PDs, set the PoE power supply delay on the appropriate interfaces of the switch so that the switch detects the maintain power of the PDs after the specified delay.

Precautions

After the PoE power supply delay is configured on an interface, do not replace the PD connected to this interface within the delay. Otherwise, the new PD cannot work properly.

Example

Set the PoE power supply delay to 5 seconds on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe power-on delay 5
```

3.6.24 poe power-reserved

Function

The **poe power-reserved** command sets the percentage of the reserved PoE power against the total PoE power.

The **undo poe power-reserved** command restores the default percentage of the reserved PoE power against the total PoE power.

By default, the percentage of the reserved PoE power against the total PoE power is 20%.

Format

poe power-reserved *power-reserved* [**slot** *slot-id* [**mcu** *mcu-id*]]

undo poe power-reserved *power-reserved* **slot** *slot-id*

undo poe power-reserved [**slot** *slot-id* [**mcu** *mcu-id*]]

NOTE

Only the S5720I-28X-PWH-SI-AC supports the **mcu** *mcu-id* parameter.

Parameters

Parameter	Description	Value
power-reserved	Specifies the percentage of the reserved PoE power against the total PoE power.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 20.

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
mcu *mcu-id*	Specifies an MCU ID.	The value is 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The device can dynamically allocate power to each interface according to the power consumption of each interface. The power consumption of a PD keeps changing when the PD is running. The system periodically calculates the total power consumption of all the PDs. If the total power consumption exceeds the upper threshold of the device, the system powers off the PDs on the interfaces of low priority. If interfaces have the same priority, the system powers off the PD on the interface with a larger port number.

Sometimes, however, the power consumption increases sharply and the available power of the system cannot support the burst increase of power. At this time, the system has not calculated and found that the total power consumption exceeded the upper threshold; therefore, the system does not cut off power low-priority interfaces in time. As a result, the PoE power supply is shut down for overload protection, and all PDs are powered off.

This problem can be solved by running the **poe power-reserved** command to set proper reserved power. When there is a burst increase in power consumption, the reserved power can support the system running. Then the system has time to power off interfaces of low priority to ensure stable running of other PDs.

Precautions

- The reserved power should not be set greater than 20%. If the reserved PoE power is greater than 20% of the total PoE power, the power capacity of the device is affected.
- To set the maximum output power of a device, run the **poe max-power** command. In this case, the device calculates the reserved power based on the set maximum output power. If the maximum output power is not set, the available PoE power is the power provided by the PoE power module.

Example

Set the percentage of reserved PoE power to the total PoE power to 30%.

```
<HUAWEI> system-view
[HUAWEI] poe power-reserved 30
Warning: The power for new PDs connected to slot 0 may be insufficient after this operation is performed.
Continue?[Y/N]:y
```

3.6.25 poe power-threshold

Function

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage.

The **undo poe power-threshold** command restores the default alarm threshold of the PoE power consumption percentage.

By default, the alarm threshold is 90%. That is, an alarm is generated when the consumed power accounts for 90% of the total power.

Format

poe power-threshold *threshold-value* [**slot** *slot-id* [**mcu** *mcu-id*]]

undo poe power-threshold *threshold-value* **slot** *slot-id*

undo poe power-threshold [**slot** *slot-id* [**mcu** *mcu-id*]]

NOTE

Only the S5720I-28X-PWH-SI-AC supports the **mcu** *mcu-id* parameter.

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold of the PoE power consumption percentage. When the power consumption reaches this value, a PoE power alarm is generated.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 90.
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
mcu *mcu-id*	MCU ID	The value is an integer ranging from 1 to 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage. If the total PoE power is 369.6 W and the alarm threshold is 90%, an alarm is generated when the power consumption is greater than 332.64 W. When the power consumption falls below 332.64 W, the alarm is cleared.

Example

Set the alarm threshold of the PoE power consumption percentage to 80%.

```
<HUAWEI> system-view
[HUAWEI] poe power-threshold 80
```

3.6.26 poe priority

Function

The **poe priority** command sets the power priority of a PoE interface.

The **undo poe priority** command restores the default power priority of a PoE interface.

By default, the power supply priority of an interface is **low**.

Format

poe priority { **critical** | **high** | **low** }

undo poe priority

Parameters

Parameter	Description	Value
critical	Indicates the highest priority.	-
high	Indicates the second highest priority.	-
low	Indicates the lowest priority.	-

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

When the output power of a device is insufficient, the device in automatic power management mode provides power for the interfaces of the higher power supply priorities first and cuts off power of the interfaces of the lower power supply priorities. PoE switches provide power to PDs connected to the interfaces in the sequence in which PDs are connected to them.

Example

Set the power supply priority of GigabitEthernet0/0/1 to critical.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe priority critical
```

3.6.27 poe-power backup-mode

Function

The **poe-power backup-mode** command sets the PoE power supply mode to the backup mode.

The **undo poe-power backup-mode** command restores the PoE power supply mode to the high-power mode.

By default, the PoE power supply mode is the high-power mode.

NOTE

Only the S5720I-28X-PWH-SI-AC supports this command.

Format

poe-power backup-mode *backup-mode* [**slot** *slot-id*]

undo poe-power backup-mode [**slot** *slot-id*]

Parameters

Description	Description	Value
backup-mode	Specifies the backup mode of PoE power supplies.	The value can only be 1.

Description	Description	Value
slot *slot-id*	Specifies a slot ID. If this parameter is not specified in Stack, only the PoE power supply mode of the master switch is modified.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The S5720I-28X-PWH-SI-AC has two built-in power modules, which support two PoE power supply modes:

- High-power mode (default): When two power modules are used, they provide 369.6 W PoE power for the first 8 electrical ports and last 16 electrical ports respectively, and the system provides 739.2 W PoE power. If one of the two power modules is faulty, the first 8 electrical interfaces provide power normally, but the PDs connected to the last 16 electrical ports are powered off and the PoE function becomes unavailable on the last 16 electrical ports. When only one power module is used, only the first 8 electrical interfaces can provide PoE power.
- PoE backup mode: The PoE power supply mode can be manually set to the backup mode using the **poe-power backup-mode** command. The backup mode provides 1+1 redundancy. In backup mode, the system provides 369.6 W PoE power, regardless of whether one or two power modules are used. The 369.6 W PoE power is shared by 24 electrical ports. Setting the PoE power supply mode to the backup mode can improve system stability.

Precautions

Changing the PoE power supply mode will power off the PDs connected to all ports.

Example

Set the PoE power supply mode to the backup mode.

```
<HUAWEI> system-view
[HUAWEI] poe-power backup-mode 1
```

3.6.28 poe single-class enable

Function

The **poe single-class enable** command configures the single-class power supply mode for an interface.

The **undo poe single-class enable** command restores the standard hierarchical power supply mode for an interface.

By default, an interface works in standard hierarchical power supply mode.

NOTE

Format

poe single-class enable

undo poe single-class enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a PoE interface works in standard hierarchical power supply mode. If PoE interfaces provide power to non-standard PDs in standard hierarchical power supply mode, these PDs cannot initiate power requests using LLDP or CDP and can only obtain a low power. As a result, these PDs cannot work normally. To address this issue, run the **poe single-class enable** command to configure the single-class power supply mode for PoE interfaces. These non-standard PDs can then initiate power requests and obtain the standard power supply to work normally.

Precautions

- If a standard PD is connected to the interface, this PD may be unable to work normally after the **poe single-class enable** command is run.
- On the S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, and S5732-H, the **poe af-inrush enable** and **poe single-class enable** commands are mutually exclusive and cannot be configured on the same interface.

Example

Configure the single-class power supply mode for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] poe single-class enable
```

3.6.29 reset poe slot

Function

The **reset poe slot** command resets the PoE chip in a specified slot.

NOTE

Only the S5720-LI, S5731-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S-I, S500, and S5735-S support this command.

Format

reset poe { **all chips** | **chip** *chip-id* } **slot** *slot-id*

Parameters

Parameter	Description	Value
all chips	Specifies all PoE chips.	-
chip *chip-id*	Specifies a chip ID.	The value must be set according to the device configuration.
slot-id	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

If one or multiple PoE chips of a PSE are suspended, the port connected to a PD cannot detect the suspension and fails power the PD. In this case, you can run the **reset poe** { **all chips** | **chip** *chip-id* } **slot** *slot-id* command to reset the PoE chip.

Example

Reset PoE chip 0 in slot 1.

```
<HUAWEI> reset poe chip 0 slot 1
Warning: This command will cause power cycling for the PD connected to port 1,2,3,4. Continue? [Y/N]:y
```

3.7 Monitoring Interface Configuration Commands

3.7.1 Command Support

Only the following switch models support monitoring interfaces:

S5720I-SI (excluding the S5720I-6X-PWH-SI-AC and S5720I-10X-PWH-SI-AC), S5735-S-I

3.7.2 display monitor input

Function

The **display monitor input** command displays the status of an input line connected to a monitoring interface.

NOTE

Only the S5735-S-I supports this command.

Format

display monitor input { *line-id* | **all** } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
line-id	Displays the status of the specified input line.	The value is an integer that ranges from 1 to 2.
all	Displays the status of all input lines.	-
slot *slot-id*	Specifies the stack ID if stacking is configured.	The value is determined based on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display monitor input** command to check the status of an input line connected to a monitoring interface, including the name, the normal level, and the current status of the input line, and whether the monitoring function is enabled.

Example

Display the current status of all input lines.

```
<HUAWEI> display monitor input all

--------------------------------------------------------------------------
LineID  LineName                   Enable  NormalStatus  CurrentStatus
--------------------------------------------------------------------------
1       Input1                     enable  low-level     abnormal
2       Input2                     enable  high-level    normal
--------------------------------------------------------------------------
```

Table 3-130 Description of the display monitor input command output

Item	Description
LineID	ID of the input line connected to a monitoring interface.
LineName	Name of the input line connected to a monitoring interface. To set the name, run the **monitor input** command.
Enable	Whether an input line connected to a monitoring interface is enabled. To set the parameter, run the **monitor input enable** command.
NormalStatus	Normal level of an input line connected to a monitoring interface: ● low-level: The normal level is low level. ● high-level: The normal level is high level. To set the normal level, run the **monitor input** command.
CurrentStatus	Current status of an input line connected to a monitoring interface: ● normal: The input line is in normal state. ● abnormal: The input line is abnormal state.

3.7.3 display monitor output

Function

The **display monitor output** command displays the status of an output line connected to a monitoring interface.

NOTE

Only the S5735-S-I supports this command.

Format

display monitor output { *line-id* | **all** }

Parameters

Parameter	Description	Value
line-id	Displays the status of a specified output line.	The value is 1.
all	Displays the status of all output lines.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **monitor output enable** or **undo monitor output enable** command, you can run the **display monitor output** command to check the status of an output line connected to a monitoring interface, including line ID, the initial status of the monitoring function on the output line, and the current status of the monitoring function on the output line. If the initial status of the monitoring function on the output line is the same as the current status, the maintenance compartment door is closed. If they are inconsistent, the maintenance compartment door is opened.

Example

Display the status of all output lines.

```
<HUAWEI> display monitor output all
----------------------------------
LineID  Config  Current Keeptime(s)
----------------------------------
1       enable  enable  3
----------------------------------
```

Table 3-131 Description of the **display monitor output** command output

Item	Description
LineID	ID of the output line connected to a monitoring interface.

Item	Description
Config	Initial status of the monitoring function on the output line. - enable: The **monitor output enable** command is run. - disable: The **undo monitor output enable** command is run.
Current	Current status of the monitoring function on the output line. If the value of this field is the same as that of **Config**, the maintenance compartment door is closed. If they are inconsistent, the maintenance compartment door is opened.
Keeptime(s)	Hold time of the signals indicating the maintenance compartment door is open or closed when the monitoring function on the output line connecting to a monitoring interface is enabled. The unit is second.

3.7.4 monitor input

Function

The **monitor input** command configures the name and normal level of the input lines connected to a monitoring interface.

The **undo monitor input** command restores the name and normal level of the input lines connected to a monitoring interface to default value.

By default, the name of a monitored input line is **Input1** or **Input2**. The normal level is **low-level**.

NOTE

Only the S5735-S-I supports this command.

Format

monitor input *line-id* **name** *line-name* **normal-state** { **low-level** | **high-level** } [**slot** *slot-id*]

undo monitor input *line-id* [**slot** *slot-id*]

Parameters

Parameter	Description	Value
line-id	Specifies the ID of an input line.	The value is an integer that ranges from 1 to 2.
name *line-name*	Specifies the name of an input line.	The name is a string of 1 to 31 case-sensitive characters without spaces.
normal-state { **low-level** | **high-level** }	Specifies the normal level of input lines connected to a monitoring interface. ● **low-level**: indicates that the normal level is low level. ● **high-level**: indicates that the normal level is high level.	-
slot *slot-id*	Specifies the stack ID if stacking is configured.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **monitor input** command to configure the name and normal level of the input lines connected to a monitoring interface. When the level of the input line changes, the device generates an alarm.

Example

Configure the name of input line 1 as line1 and normal level as **high-level**.

```
<HUAWEI> system-view
[HUAWEI] monitor input 1 name line1 normal-state high-level
```

3.7.5 monitor input enable

Function

The **monitor input enable** command enables the monitoring function on an input line.

The undo monitor input enable command disables the monitoring function on an input line.

By default, the monitoring function on an input line is disabled.

NOTE

Only the S5735-S-I supports this command.

Format

monitor input *line-id* **enable** [**slot** *slot-id*]

undo monitor input *line-id* **enable** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
line-id	Specifies the ID of an input line.	The value is an integer that ranges from 1 to 2.
slot *slot-id*	Specifies the stack ID if stacking is configured.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **monitor input enable** command to enable the monitoring function on an input line so that you can monitor the application environment of the device.

Example

Enable the monitoring function on input line 1.

```
<HUAWEI> system-view
[HUAWEI] monitor input 1 enable
```

3.7.6 monitor output enable

Function

The **monitor output enable** command configures the initial status of the monitoring function on an output line connected to a monitoring interface to enabled.

The **undo monitor output enable** command configures the initial status of the monitoring function on an output line connected to a monitoring interface to disabled.

By default, the initial status of the monitoring function on an output line is not configured.

NOTE

Only the S5735-S-I supports this command.

Format

monitor output *line-id* **enable slot** *slot-id*

undo monitor output *line-id* **enable slot** *slot-id*

Parameters

Parameter	Description	Value
line-id	Specifies the ID of an output line.	The value is 1.
slot *slot-id*	Specifies the slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **monitor output enable** command is run, the initial status of the monitoring function on an output line (DOUT status for short) is configured to enabled. If the maintenance compartment door is opened, the DOUT status changes to disabled. If the maintenance compartment door is closed, the DOUT status changes to enabled. You can monitor whether the maintenance compartment door is opened based on the DOUT status.

Similarly, after the **undo monitor output enable** command is run, the initial DOUT status is configured to disabled. If the maintenance compartment door is opened, the DOUT status changes to enabled. If the maintenance compartment door is closed, the DOUT status changes to disabled.

Example

Configure the initial status of the monitoring function on output line 1 to enabled.

```
<HUAWEI> system-view
[HUAWEI] monitor output 1 enable slot 0
```

3.7.7 monitor output keeptime

Function

The **monitor output keeptime** command sets the hold time of the signals indicating the maintenance compartment door on a device is open or closed when the monitoring function on the output line connecting to a monitoring interface is enabled.

The **undo monitor output keeptime** command restores the default setting.

By default, the hold time of the signals indicating the maintenance compartment door on a device is open or closed is 3 seconds.

NOTE

Only the S5735-S-I supports this command.

Format

monitor output keeptime *time* **slot** *slot-id*

undo monitor output keeptime slot *slot-id*

Parameters

Parameter	Description	Value
time	Specifies the hold time.	The value is an integer ranging from 1 to 3600, in seconds.
slot *slot-id*	Specifies the slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the hold time of the signals indicating the maintenance compartment door on a device is open or closed is three seconds. That is, a camera keeps monitoring the device maintenance compartment door for 3 seconds and then turns to another direction. You can run the **monitor output keeptime** command to change the hold time based on the actual situation of the camera.

Example

Set the hold time to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] monitor output keeptime 10 slot 0
```

3.8 OPS Configuration Commands

3.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.8.2 assistant scheduler suspend

Function

The **assistant scheduler suspend** command disables the OPS maintenance assistant function.

The **undo assistant scheduler suspend** command enables the OPS maintenance assistant function.

By default, the OPS maintenance assistant function is enabled.

Format

assistant scheduler suspend

undo assistant scheduler suspend

Parameters

None

Views

OPS view

Default Level

3: Management level

Usage Guidelines

If the OPS maintenance assistant function is no longer needed, the **assistant scheduler suspend** command applies to the following scenarios:

- Before deleting configured Python script assistants one by one, you can run this command to disable the OPS maintenance assistant function to prevent the assistants from running.

- During system maintenance, you can run this command to disable the OPS maintenance assistant function temporarily.

After you run the **assistant scheduler suspend** command to disable the OPS maintenance assistant function, none of Python script assistants will run again.

Example

Disable the OPS maintenance assistant function.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] assistant scheduler suspend
```

3.8.3 display ops assistant

Function

The **display ops assistant** command displays information about Python script assistants.

Format

display ops assistant { **current** [**verbose**] | **history** } [**name** *assistant-name*]

Parameters

Parameter	Description	Value
current	Displays brief information about the current status of Python script assistants.	-
verbose	Displays detailed information about the current status of Python script assistants.	-
history	Displays historical operation records of Python script assistants.	-
name *assistant-name*	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file for which the script assistant has been configured.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use this command to check the current status and historical operation record of a Python script assistant, including the Python script assistant name, running status, and execution result. The command can display a maximum of 100 latest Python script assistant records.

Example

Display brief information about the current status of Python script assistants.

```
<HUAWEI> display ops assistant current
-----------------------------------------------------
Assistant                   State         Condition
-----------------------------------------------------
subscribe_cli_sync_1.py       ready          cli
user-correlat-10.py          ready         multi
-----------------------------------------------------
```

Table 3-132 Description of the **display ops assistant current** command output

Item	Description
Assistant	Name of a Python script assistant.
State	Current status of the Python script assistant. • ready: The Python script assistant is waiting to be triggered. • pending: The Python script assistant is waiting to run. • waiting: A resident script is waiting to be triggered the second time. • running: The Python script assistant is running. • shutdown: The Python script assistant stops. • suspend: The OPS maintenance assistant function is disabled.

Item	Description
Condition	Triggering condition for a Python script assistant. ● cli: command line event ● device: stack status change event ● iclog: log event ● ifm: interface statistics collection event event ● lldp: LLDP neighbor change event ● multi: complex event ● timer: timer event ● trap: trap event ● URM: routing event

Display detailed information about the current status of Python script assistants.

```
<HUAWEI> display ops assistant current verbose
Assistant information
  Name                          :user-correlat-10.py
  State                         :ready
Running statistics
  Running times                 :0
  Queue size/(free)             :5/(5)
  Skip for queue full           :0
  Skip for delay                :0
  Skip for suppression          :0
Condition information
  Condition tag                 :cli1
    Condition type              :multi
    Threshold                   :1
    Period (s)                  :0
    Hits in period              :0
  Condition tag                 :cli2
    Condition type              :multi
    Threshold                   :1
    Period (s)                  :0
    Hits in period              :0
  Condition tag                 :cli3
    Condition type              :multi
    Threshold                   :1
    Period (s)                  :0
    Hits in period              :0
  Condition tag                 :cli4
    Condition type              :multi
    Threshold                   :1
    Period (s)                  :0
    Hits in period              :0
  Correlate expression          :((cli1 andnot cli2) and (cli3 andnot cli4))
  Trigger control
    Threshold                   :1
    Period (s)                  :30
    Delay (s)                   :0
    Suppress max                :0
    Hits in period              :0
```

Table 3-133 Description of the **display ops assistant current verbose** command output

Item	Description
Assistant information	Information about a Python script assistant.
Name	Name of a Python script assistant.
State	Current status of a Python script assistant. - ready: The Python script assistant is waiting to be triggered. - pending: The Python script assistant is waiting to run. - waiting: A resident script is waiting to be triggered the second time. - running: The Python script assistant is running. - shutdown: The Python script assistant stops. - suspend: The OPS maintenance assistant function is disabled.
Running statistics	Detailed running information about a Python script assistant.
Running times	Number of running times.
Queue size/(free)	Number of buffered Python script assistants. If the number of buffered Python script assistants reaches the maximum value, excessive assistants will be discarded.
Skip for queue full	Number of tasks discarded because the queue is full.
Skip for delay	Number of tasks discarded within the delay.
Skip for suppression	Number of times the triggering of the assistant is suppressed.
Condition information	Condition information about a Python script assistant. The **Condition information** field is displayed only for a complex event script.
Condition tag	Condition name.
Condition type	Type of triggering condition. The value is **multi**.

Item	Description
Threshold	Maximum number of times that tasks are executed. The default value is 1.
Period (s)	Detection period, in seconds. The default value is 30.
Hits in period	Number of times the triggering condition is met in the detection period.
Correlate expression	Condition combination mode.
Trigger control	Trigger control.
Delay (s)	Delay in triggering a working task. The default value is 0 seconds.
Suppress max	Maximum number of times working tasks are triggered within the delay. The default value is 0, indicating that working tasks will not be suppressed.

Display historical operation records of Python script assistants.

```
<HUAWEI> display ops assistant history
Assistant history information
  Name                          :subscribe_cli_sync_1.py
  Running information
    Trigger condition             :cli
    Trigger event name            :cli1
    Trigger time                  :2017-03-25 19:48:51
    Execute start time            :2017-03-25 19:48:51
    Execute end time              :2017-03-25 19:48:53
    Execute result                :normal
```

Table 3-134 Description of the **display ops assistant history** command output

Item	Description
Assistant history information	Historical information about a Python script assistant.
Name	Name of a Python script assistant.
Running information	Running information about a Python script assistant.

Item	Description
Trigger condition	Triggering condition for a Python script assistant. ● cli: command line event ● device: stack status change event ● iclog: log event ● ifm: interface statistics collection event event ● lldp: LLDP neighbor change event ● multi: complex event ● timer: timer event ● trap: trap event ● URM: routing event
Trigger event name	Trigger event name for a Python script assistant.
Trigger time	Triggering time of a Python script assistant.
Execute start time	Execution time of a Python script assistant.
Execute end time	End time of a Python script assistant.
Execute result	Execution result of a Python script assistant. ● normal: The script assistant ends normally. ● abnormal: An exception occurs in the script. ● userCancel: A user stops the script. ● duplicate: The script file name conflicts with the database file name. ● os: The system kills the script process due to a script exception.

3.8.4 display ops environment

Function

The **display ops environment** command displays information about user-defined environment variables.

Format

display ops environment

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display ops environment** command to check information about user-defined environment variables after user-defined environment variables are configured using the **environment** command.

Example

Display user-defined environment variables.

```
<HUAWEI> display ops environment
No.  Name                          Value
1    user                          admin
```

Table 3-135 Description of the **display ops environment** command output

Item	Description
No.	User-defined environment variable number. The value ranges from 1 to 100.
Name	Name of a user-defined environment variable. To configure this parameter, run the **environment** command.
Value	Value of a user-defined environment variable. To configure this parameter, run the **environment** command.

3.8.5 display ops error

Function

The **display ops error** command displays script execution errors.

Format

display ops error [**name** *assistant-name*]

Parameters

Parameter	Description	Value
name *assistant-name*	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file for which the script assistant has been configured.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view execution errors of all scripts or a specified script. According to the errors in the command output, you can modify the script.

Example

Display execution errors of all scripts.

```
<HUAWEI> display ops error
--------------------------------------------------------------------------------
test12.py:
Traceback (most recent call last):
  File ".lib/frame.py", line 114, in <module>
    ret = m.ops_execute(ops)
  File "flash:$_user/test12.py", line 7, in ops_execute
    status, err_context = ops.context.save(varName, value)
NameError: global name 'varName' is not defined

--------------------------------------------------------------------------------
test13.py:
Traceback (most recent call last):
  File ".lib/frame.py", line 114, in <module>
    ret = m.ops_execute(ops)
  File "flash:$_user/test13.py", line 6, in ops_execute
    status, err_log = ops.syslog("Syslog: Hello, World..", ops.CRITICAL, "syslog
")
```

```
AttributeError: 'module' object has no attribute 'syslog'

--------------------------------------------------------------------------------
```

Table 3-136 Description of the **display ops error** command output

Item	Description
test12.py	Python script file name.
Traceback (most recent call last)	Last call error.
File ".lib/frame.py", line 114, in <module>	Stack where an error occurs.
File "flash:$_user/test12.py", line 7, in ops_execute	Information about location where an error occurs, including the Python script name, number of line, and phase when the error occurs.
status, err_context = ops.context.save(varName, value)	Invalid contents.
NameError	A variable error. The system is attempting to access a variable that is not declared.
AttributeError	An attribute error. The system is attempting to access an unknown object attribute.

3.8.6 display ops system-script

Function

The **display ops system-script** command displays system built-in OPS scripts.

Format

display ops system-script

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When associating OIDS with OPS, you need to use OPS scripts to subscribe to OIDS events. The device provides built-in OPS scripts, which removing the need to make scripts or download scripts from websites and import the scripts to the device. To view system built-in OPS scripts, run the **display ops system-script** command.

Precautions

The system built-in OPS scripts are not installed by default.

Example

Display system built-in OPS scripts.

```
<HUAWEI> display ops system-script
ScriptName                  Description
------------------------------------------------------------------------------
oids.py                       The OIDS sample script describes the subscriptio
                            n process. The execution result of the script ha
                            s been recorded to OIDS. You can refer to this s
                            cript to implement the OIDS script process.
```

Table 3-137 Description of the **display ops system-script** command output

Item	Description
ScriptName	Name of a script.
Description	Description of the script.

3.8.7 environment

Function

The **environment** command configures a user-defined environment variable.

The **undo environment** command deletes a user-defined environment variable.

By default, no user-defined environment variable is configured.

Format

environment *variable-name variable-value*

undo environment *variable-name*

Parameters

Parameter	Description	Value
variable-name	Specifies the name of a user-defined environment variable.	The value is a string of 1 to 31 case-sensitive characters without spaces. It starts with a letter and contains only letters, digits, and underscores (_).
variable-value	Specifies the value of a user-defined environment variable.	The value is a string of 1 to 64 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An environment variable consists of a name and a value. In a Python script, you can input an environment variable name in the location where a parameter needs to be input to indicate that an environment variable value needs to be referenced. When the system is running a Python script, it replaces an environment variable name with an environment variable value. To change the value, you can directly change it on the device without having to change and install the Python script. You can define and use user-defined environment variables to simplify the configuration and improve flexibility and feasibility of the Python script.

Precautions

If *variable-name* is specified multiple times, the system will prompt that the configured user-defined environment variable already exists. You can choose whether to overwrite the existing variable value. After overwriting the existing variable value, you need to run the **undo script-assistant python** command to delete the Python script assistant that uses the environment variable and then run the **script-assistant python** command to re-configure the Python script assistant.

A maximum of 100 environment variables can be configured on the device.

To check configured user-defined environment variables, run the **display ops environment** command.

Example

Set the value of the user-defined environment variable **user** to **admin**.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] environment user admin
```

3.8.8 ops

Function

The **ops** command displays the OPS view.

Format

ops

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

You can configure the Python script assistant in the OPS view.

Example

Display the OPS view.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops]
```

3.8.9 ops abort

Function

The **ops abort** command stops all OPS Python scripts.

Format

ops abort

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If commands cannot be entered on the switch due to OPS Python script exceptions, run the **ops abort** command to stop all OPS Python scripts to make the switch work properly.

Prerequisites

Running the **ops abort** command on the master switch will not be captured by the CLI event subscription API (ops.cli.subscribe), but running this command on the standby switch will be captured by this API.

Follow-up Procedure

To restore the OPS function, perform the following operations:

1. Run the **system-view** command to enter the system view.
2. Run the **ops** command to enter the OPS view.
3. Run the **undo script-assistant python** *script-name* command to delete the assistant of the abnormal Python script.
4. Run the **return** command to return to the user view.
5. Run the **ops uninstall file** *script-name* command to uninstall the abnormal Python script.
6. Run the **system-view** command to enter the system view.
7. Run the **ops** command to enter the OPS view.
8. Run the **undo assistant scheduler suspend** command to enable the OPS assistant to restore the OPS function.

Example

Stop all OPS Python scripts.

```
<HUAWEI> ops abort
```

3.8.10 ops install file

Function

The **ops install file** command installs a Python script.

Format

ops install file *file-name* [**destination** *directory*]

Parameters

Parameter	Description	Value
file-name	Specifies the directory and file name of the Python script to be installed. ● To install a Python script stored in the root directory of the device, you can directly specify the file name of the script. ● To install a Python script that is stored a non-root directory, you need to specify both the directory and file name of the script.	The value is a string of 4 to 64 case-insensitive characters. Spaces and special characters |, ;, &, $, >, <, `, \, !, \n, and \0 are not allowed. The file name extension of a Python script file is .py.

Parameter	Description	Value
		NOTE *file-name* cannot be set to the name of a built-in Python script file, including ConfigParser.py, copy_reg.py, locale.py, sre.py, Queue.py, decimal.py, macurl2path.py, sre_compile.py, StringIO.py, dis.py, modulefinder.py, sre_constants.py, UserDict.py, dummy_thread.py, ntpath.py, sre_parse.py, UserList.py, dummy_threading.py, nturl2path.py, stat.py, UserString.py, filecmp.py, numbers.py, string.py, __future__.py, fileinput.py, opcode.py, stringold.py, _abcoll.py, fnmatch.py, os.py, struct.py, _pyio.py, formatter.py, os2emxpath.py, subprocess.py, _strptime.py, fractions.py, pickle.py, sysconfig.py, _threading_local.py, functools.py, pkgutil.py, textwrap.py, _weakrefset.py, genericpath.py, platform.py, threading.py, abc.py, getopt.py, posixpath.py, token.py, argparse.py, getpass.py, pprint.py, tokenize.py, atexit.py, gettext.py, re.py, trace.py, base64.py, glob.py, repr.py, traceback.py, bisect.py, heapq.py, runpy.py, types.py, calendar.py, imputil.py, sched.py, user.py, codecs.py, inspect.py, sets.py, warnings.py, collections.py, io.py, shutil.py, weakref.py, contextlib.py, keyword.py, site.py, xmllib.py, copy.py, linecache.py, socket.py, _cli.py, _device.py, _frame.py, _route.py, _timer.py, _common.py, _environment.py, _iclog.py, _snmp.py, _trap.py, _context.py, _farg.py, _lldp.py, _terminal.py, and ops.py.

Parameter	Description	Value
destination *directory*	Specifies the installation directory of a script.	The value is a string of 1 to 64 case-insensitive characters without any spaces. If this parameter is not specified, the script will be installed in $_user. If this parameter is specified, the script will be installed in $_user/*directory*. If the directory name does not exist, a directory will be created. **NOTE** The total length of *file-name* and the installation directory of the script cannot exceed 118. The total length refers to the storage path + $_user + directory name + file name. The installation directory of the script cannot be huawei_pys. The depth of the path specified by *directory* cannot exceed three levels.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

OPS allows you to run the scripts you make. A script can be executed after the script assistant is configured. Before configuring a script assistant, install the script.

To check information about the scripts installed in $_user, run the **dir (user view)** command.

Precautions

- Before installing a script, upload the script to the root directory of flash: on the device.

- Ensure that the device has sufficient storage space when the script is installed. Otherwise, the script fails to be installed.
- If the specified installation directory does not exist, a directory will be created. A maximum of seven levels of subdirectories can be created in $_user.
- The name of the script to be installed cannot be the same as an existing directory name on the device. After scripts are installed successfully, you cannot create a directory whose name is the same as that of an installed script.
- To install scripts in $_user, you can only run the **ops install file** command. The scripts installed in this directory will be automatically backed up to the standby switch when a stack is configured.
- To modify a script that has been installed, run the **ops uninstall file** command to uninstall the script and the **delete (user view)** command to delete the script file. After modifying the script, upload and reinstalling the script file.
- It is recommended that the total size of files installed in $_user be smaller than 100 MB. If the total size of files exceeds 100 MB, performance of data synchronization between the active and standby cards may deteriorate.

Example

Install the script file config.py in the flash: root directory to the default flash:/$_user.

```
<HUAWEI> ops install file config.py
```

Install the script file config.py in the flash: root directory to the specified flash:/$_user/user.

```
<HUAWEI> ops install file config.py destination user
```

Install the script file config.py in the flash:/admin directory to the default flash:/$_user.

```
<HUAWEI> ops install file admin/config.py
```

3.8.11 ops uninstall file

Function

The **ops uninstall file** command uninstalls a Python script.

Format

ops uninstall file *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of the script file to be uninstalled.	The value must be the name of a script file that has been installed. If a script in a specified installation directory *directory*/*file-name* needs to be deleted, *directory* specifies the installation directory of the script. **NOTE** The total length of *file-name* and the installation directory of the script cannot exceed 118. The total length refers to the storage path + $_user + directory name + file name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can uninstall unnecessary scripts to release storage space on a device. If an installed script needs to be updated, uninstall it first, and reinstall it after the update.

Precautions

This command cannot uninstall a script for which a script assistant has been configured. To uninstall the script, delete the script assistant first.

If the script for which a script assistant has configured invokes another script, the called script can be uninstalled using this command. Therefore, it is recommended that you use one script to implement required functions.

Example

Uninstall the script file config.py in the default directory flash:/$_user.

```
<HUAWEI> ops uninstall file config.py
```

Uninstall the script file config.py in the specified directory flash:/$_user/user.

```
<HUAWEI> ops uninstall file user/config.py
```

3.8.12 script-assistant python

Function

The **script-assistant python** command configures a Python script assistant.

The **undo script-assistant python** command deletes a Python script assistant.

By default, no Python script assistant is configured.

Format

script-assistant python *script-name*

undo script-assistant python *script-name*

Parameters

Parameter	Description	Value
script-name	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file that has been installed.

Parameter	Description	Value
		NOTE *script-name* cannot be set to the file name of a built-in Python script, including ConfigParser.py, copy_reg.py, locale.py, sre.py, Queue.py, decimal.py, macurl2path.py, sre_compile.py, StringIO.py, dis.py, modulefinder.py, sre_constants.py, UserDict.py, dummy_thread.py, ntpath.py, sre_parse.py, UserList.py, dummy_threading.py, nturl2path.py, stat.py, UserString.py, filecmp.py, numbers.py, string.py, __future__.py, fileinput.py, opcode.py, stringold.py, _abcoll.py, fnmatch.py, os.py, struct.py, _pyio.py, formatter.py, os2emxpath.py, subprocess.py, _strptime.py, fractions.py, pickle.py, sysconfig.py, _threading_local.py, functools.py, pkgutil.py, textwrap.py, _weakrefset.py, genericpath.py, platform.py, threading.py, abc.py, getopt.py, posixpath.py, token.py, argparse.py, getpass.py, pprint.py, tokenize.py, atexit.py, gettext.py, re.py, trace.py, base64.py, glob.py, repr.py, traceback.py, bisect.py, heapq.py, runpy.py, types.py, calendar.py, imputil.py, sched.py, user.py, codecs.py, inspect.py, sets.py, warnings.py, collections.py, io.py, shutil.py, weakref.py, contextlib.py, keyword.py, site.py, xmllib.py, copy.py, linecache.py, socket.py, _cli.py, _device.py, _frame.py, _route.py, _timer.py, _common.py, _environment.py, _iclog.py, _snmp.py, _trap.py, _context.py, _farg.py, _lldp.py, _terminal.py, and ops.py.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

As networks are developing rapidly, existing network devices provide only limited functions and predefined services, failing to meet the requirements for diversified services. You can run the script using OPS to implement customized functions.

The device supports a built-in Python script interpreter. You can run the **script-assistant python** command to run a Python script and register the events defined in the script.

Prerequisites

The script has been uploaded to the device and installed using the **ops install file** command in the user view.

Precautions

Only one assistant can be configured for a Python script. A maximum of 100 Python script assistants can be configured on the device.

The system does not check correctness of the Python script.

If you run the **undo script-assistant python** command to uninstall the script assistant, the corresponding Python script will be terminated.

Example

Configure a script assistant for the script config.py.

```
<HUAWEI> ops install file config.py
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] script-assistant python config.py
```

3.8.13 shutdown script-assistant

Function

The **shutdown script-assistant** command stops a Python script assistant.

The **undo shutdown script-assistant** command starts a Python script assistant.

By default, the Python script assistant is started.

Format

shutdown script-assistant *script-name*

undo shutdown script-assistant *script-name*

Parameters

Parameter	Description	Value
script-name	Specifies the name of a Python script assistant, namely, a Python script name for a script assistant.	The value must be the name of a script file for which the script assistant has been configured.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent a Python script of an assistant from running, run the **shutdown script-assistant** command to stop the Python script assistant.

Precautions

Stopping a running assistant interrupts the task of the assistant. Exercise caution when you perform this operation.

Example

Stop a script assistant for the script config.py.

```
<HUAWEI> system-view
[HUAWEI] ops
[HUAWEI-ops] shutdown script-assistant config.py
Info: Succeeded in stopping script assistant config.py.
```

3.9 Energy-saving Configuration Commands

3.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.9.2 als enable

Function

The **als enable** command enables ALS on an interface.

The **undo als enable** command disables ALS on an interface.

By default, ALS is disabled on an interface.

Format

als enable

undo als enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The constraints on ALS are as follows:

- Only optical interfaces support ALS. Electrical interfaces and combo interface do not support ALS.
- When optical interfaces transmit services unidirectionally, they do not support ALS.
- When the copper cable, copper module, or GPON optical module is used on the optical port, the ALS function is not supported. In addition, after the copper cable or GPON optical module is inserted, all the ALS-related commands configured on this interface are cleared.
- When you run the display elabel command to view electronic label information of a port and the command output shows that the component vendor is FCBN410QB1C10-HW, this port does not support ALS.

Example

Enable ALS on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als enable
```

3.9.3 als restart

Function

The **als restart** command manually restarts the laser of an interface.

Format

als restart

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to manually restart the laser of an optical module. After the optical link recovers, the laser is started after a certain interval if the restart mode is automatic restart. To start the laser immediately after the optical link recovers, set the restart mode of the laser to manual restart and run the **als restart** command. If this command is not executed, the laser automatically sends a pulse after receiving a pulse from the remote end.

Prerequisites

ALS has been enabled on the interface using the **als enable** command and the restart mode of the laser has been set to manual restart mode using the **als restart mode manual** command.

Precautions

This command cannot be executed on an interface if the interface has been added to an interface protection group and is in **Protect** state.

Example

Restart lasers on GigabitEthernet0/0/1 manually.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als enable
[HUAWEI-GigabitEthernet0/0/1] als restart mode manual
[HUAWEI-GigabitEthernet0/0/1] als restart
```

3.9.4 als restart mode manual

Function

The **als restart mode manual** command sets the mode of restarting the laser of the optical module to manual.

The **undo als restart mode manual** command restores the mode of restarting the laser of the optical module to automatic.

By default, a laser works in automatic restart mode.

Format

als restart mode manual

undo als restart mode manual

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The laser of an optical module works in automatic restart mode or manual restart mode.

- In automatic restart mode, the laser sends pulses at the interval set using the **als restart pulse-interval** command to detect whether the link is recovered. The pulse width is set through the **als restart pulse-width** command.
- In manual restart mode, you must manually start the laser using the **als restart** command so that the laser can send a pulse. The ALS pulse width is set using the **als restart pulse-width** command.

If the fiber link recovery is detected in time, you can use the manual restart mode so that the laser can send pulses immediately. Therefore, data communication can be recovered rapidly.

Example

Configure lasers on GigabitEthernet0/0/1 to work in manual restart mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als restart mode manual
```

3.9.5 als restart pulse-interval

Function

The **als restart pulse-interval** command sets the ALS pulse interval for the laser of an optical module.

The **undo als restart pulse-interval** command restores the default ALS pulse interval of the laser of an optical module.

By default, the ALS pulse interval of the laser is 100s.

Format

als restart pulse-interval *pulse-interval*

undo als restart pulse-interval

Parameters

Parameter	Description	Value
pulse-interval	Specifies the ALS pulse interval of the laser.	The value is an integer that ranges from 100 to 20000, in seconds.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

In automatic restart mode, the ALS pulse interval affects the frequency of detecting the LOS on the interface. A long ALS pulse interval is beneficial for energy saving, but the fiber link recovery cannot be detected in a timely manner. In contrary, a short ALS pulse interval wastes power but the fiber link recovery can be detected immediately.

Example

Set the ALS pulse interval of lasers on GigabitEthernet0/0/1 to 150s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als restart pulse-interval 150
```

3.9.6 als restart pulse-width

Function

The **als restart pulse-width** command sets the ALS pulse width for the laser of an optical module.

The **undo als restart pulse-width** command restores the default ALS pulse width for the laser of an optical module.

By default, the ALS pulse width of the laser is 2s.

Format

als restart pulse-width *pulse-width*

undo als restart pulse-width

Parameters

Parameter	Description	Value
pulse-width	Specifies the ALS pulse width of the laser.	The value is an integer that ranges from 2 to 200, in seconds.

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The ALS pulse width refers to the period between rising edges of pulses. A short ALS pulse width is beneficial for energy saving, but the fiber link recovery cannot be detected immediately. In contrary, a long ALS pulse width consumes more power but the fiber link recovery can be detected immediately.

Example

Set the ALS pulse width on GigabitEthernet0/0/1 to 3s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] als restart pulse-width 3
```

3.9.7 display als configuration

Function

The **display als configuration** command displays ALS configuration.

Format

display als configuration slot *slot-id*

display als configuration interface *interface-type interface-number*

Parameters

Parameter	Description	Value
slot *slot-id*	Displays ALS configuration in a slot with a specified slot ID.	The value depends on the device configuration.
interface *interface-type interface-number*	Displays ALS configuration on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an optical interface connects to a high-speed cable, this command does not have command output.

Example

Display ALS configuration on GigabitEthernet0/0/1.

```
<HUAWEI> display als configuration interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------
Interface              ALS        Laser      Restart    Interval(s)   Width(s)
                       Status     Status     Mode
-------------------------------------------------------------------------------
GigabitEthernet0/0/1   Disable    On         Auto       100           2
-------------------------------------------------------------------------------
```

Table 3-138 Description of the **display als configuration** command output

Item	Description
Interface	Interface type and number.

Item	Description
ALS Status	Whether ALS is enabled. - Enable: ALS is enabled. - Disable: ALS is disabled. ALS is enabled using the **als enable** command.
Laser Status	Status of the laser on the interface. The value can be: - Off: The laser is shut down. - On: The laser is turned on. - --: No optical module is present on the interface.
Restart Mode	ALS restart mode. - Auto: automatic restart mode. - Manual: manual restart mode. The ALS restart mode is set to manual using the **als restart mode manual** command.
Interval(s)	ALS pulse interval, expressed in seconds. The ALS pulse interval is set using the **als restart pulse-interval** command.
Width(s)	ALS pulse width, expressed in seconds. The ALS pulse width is set using the **als restart pulse-width** command.

3.9.8 display power manage cycle

Function

The **display power manage cycle** command displays the interval for updating power consumption data.

Format

display power manage cycle

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The average power consumption of a device is the average power consumption within a period of time. You can use the **display power manage cycle** command to view the interval for calculating the average power consumption.

Example

Display the interval for updating power consumption data.

```
<HUAWEI> display power manage cycle
 3 : 1 hour
```

Table 3-139 Description of the display power manage cycle command output

Item	Description
3 (1 hour)	The interval for updating power consumption data is 1 hour. You can set the interval to the following values: • 1 : 15 minutes • 2 : 30 minutes • 3 : 1 hour • 4 : 1 day • 5 : 1 week • 6 : 1 month (30 days) To set the interval for updating power consumption data, use the **set power manage cycle** command.

3.9.9 display power manage mode

Function

The **display power manage mode** command displays the energy-saving mode of the device.

Format

display power manage mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display power manage mode** command to check the currently configured energy-saving mode of the device.

Example

Display the energy-saving mode of the device.

```
<HUAWEI> display power manage mode
2 (Standard mode)
```

Table 3-140 Description of the display power manage mode command output

Item	Description
2 (Standard mode)	Standard energy-saving mode. The device supports the following energy-saving modes: ● 1. User-defined mode: user-defined energy-saving mode. ● 2. Standard mode: standard energy-saving mode ● 3. Basic mode: basic energy-saving mode ● 4. Deep mode: depth energy-saving mode ● 5. Standby mode. **NOTE** The device does not support the user-defined mode. Only the S5720-16X-PWH-LI supports the standby mode. You can set the energy-saving mode using the **set power manage mode** command.

3.9.10 display power manage power-information

Function

The **display power manage power-information** command displays the power consumption information of a device.

Format

display power manage power-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display power manage power-information** command enables you to check the system power consumption information, including the accumulative power consumption, average power, real-time power, rated power, and power threshold of the device.

Example

Display the system power consumption information.

```
<HUAWEI> display power manage power-information
The information of net element power:
 --------------------------------------------------
 The total power consumption (Joule) : 3702200060
 The average power consumption (mW)  : 67050
 The current power consumption (mW)  : 65750
 The inbound interface power (mW)    : 81750
 The rated power (mW)                : 229000
 The threshold of power (mW)         : 600000
 The typical power (mW)              : 126000
 --------------------------------------------------
```

Table 3-141 Description of the display power manage power-information command output

Item	Description
The information of net element power	System power consumption information.

Item	Description
The total power consumption (Joule)	Accumulative power consumption, in Joule. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained. **NOTE** The accumulative power consumption is stored in the device memory and will not be lost when the device is powered off. When the device is running, power consumption is accumulated once every 15 minutes. The accumulated power consumption and accumulative power consumption in the memory are added and recorded in the memory once every 24 hours. If there is no accumulative power consumption in the memory, this field displays 0. If the device is powered off within 24 hours after starting, the power consumption accumulated within 24 hours is not added to the accumulative power consumption in the memory.
The average power consumption (mW)	The average power consumption of a device is the average power consumption within a period of time, including the PoE power, in mW. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained.
The current power consumption (mW)	The output power of the system, including the PoE power, in mW. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained.

Item	Description
The inbound interface power (mW)	The input power of the system, including the PoE power, in mW. This field displays NA for PoE-incapable models, including the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I. This field displays NA when the device uses the PDC180S12-CR, PDC260S12-DL, PAC60S12-AR or PAC150S12-R power module of which power information cannot be obtained.
The rated power (mW)	Rated power of the system, excluding the PoE power, in mW. For a stack, the value of this parameter indicates the maximum power consumption of the stack.
The threshold of power (mW)	Power threshold of the power supply unit, in mW. The value is the rated power of the power supply unit used on the device. ● When there are two power supply units on the device, they work in redundancy mode to supply power to the system. The supplied power is not the accumulated power of the two power supply units. When the rated power of both power supply units can be obtained, this field displays the smaller rated power. If the rated power of one power supply unit cannot be obtained, this field displays the obtained rated power. If the rated power of both power supply units cannot be obtained, this field displays the system rated power. ● If a built-in power supply is used, the value is the rated power of the system.
The typical power (mW)	Power of the device when 30% of the line rate is used, excluding the PoE power. The unit is mW.

3.9.11 display power manage sleep configuration

Function

The **display power manage sleep configuration** command displays device dormancy information.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

display power manage sleep configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display power manage sleep configuration** command shows device dormancy information, including the time range, period during which the awakening port status is detected continuously, awakening mode, and non-awakening ports.

Example

Display the device dormancy configuration.

```
<HUAWEI> display power manage sleep configuration
The device sleep function status: enable
The device sleep time-range: night-time
----------------------------------------------
Current time is 16:19:45 5-14-2012 Monday

Time-range: night-time ( Inactive )
20:00 to 00:00 working-day
00:00 to 08:00 working-day
----------------------------------------------
The awaken port state check interval (minutes): 20(default)
The configuration of non-awaken port:
----------------------------------------------
 GigabitEthernet0/0/1     GigabitEthernet0/0/2
 GigabitEthernet0/0/3     GigabitEthernet0/0/4
 GigabitEthernet0/0/5     GigabitEthernet0/0/6
 GigabitEthernet0/0/7     GigabitEthernet0/0/8
 GigabitEthernet0/0/9     GigabitEthernet0/0/10
----------------------------------------------
```

Table 3-142 Description of the display power manage sleep configuration command output

Item	Description
The device sleep function status	Device dormancy mode. - disable: The device dormancy function is disabled. That is, the device energy-saving mode configured using the **set power manage mode** command is not 4. - enable: The device dormancy function is enabled. That is, the device energy-saving mode configured using the **set power manage mode** command is 4.
The device sleep time-range	Dormancy time range name. If no dormancy time range is specified, the whole day takes effect by default. To set a dormancy time range, run the **sleep time-range** command.
Time-range	Dormancy time range. - If the field value contains (Inactive), the current time is not within the dormancy time range. - If the field value contains (Active), the current time is within the dormancy time range.
The awaken port state check interval (minutes)	Period during which the awakening port status is detected continuously. To set the period, run the **set power manage interval** command.
The configuration of non-awaken port	Configured non-awakening ports. To configure non-awakening ports, run the **set power manage non-awaken-port** command.

3.9.12 energy-efficient-ethernet enable

Function

The **energy-efficient-ethernet enable** command enables the Energy Efficient Ethernet (EEE) function on an electrical interface.

The **undo energy-efficient-ethernet enable** command disables the EEE function on an electrical interface.

By default, EEE is disabled on an electrical interface.

Format

energy-efficient-ethernet enable

undo energy-efficient-ethernet enable

Parameters

None

Views

GE interface view, port group view, MultiGE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system provides power for each interface. Even though an interface is idle, it consumes the same power as working interfaces. The **energy-efficient-ethernet enable** command enables the system to reduce the power on an interface when the interface is idle and restore the power when the interface starts to transmit data. This reduces system power consumption.

Prerequisites

If an electrical interface works in non-auto negotiation mode, run the **negotiation auto** command to enable auto-negotiation.

Precautions

- The EEE function can be configured only on electrical interfaces (including combo electrical interfaces). Optical interfaces do not support the EEE function.
- If an electrical interface works at 10 Mbit/s after auto-negotiation, the EEE function does not take effect.
- The S5731-H, S5731-S (except S5731-S32ST4X-A, S5731-S32ST4X-D, S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, and S5731-S32ST4X), S5731S-H, S5731S-S (except S5731S-S32ST4X-A, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, and S5731S-S32ST4X-A1), S6735-S, S6720-EI, and S6720S-EI do not support the EEE function.
- For the S5732-H48XUM2CC, S5732-H24UM2CC and S5732-H48UM2CC, MultiGE interfaces working at 2.5 Gbit/s or 5 Gbit/s do not support the EEE function.
- Enabling or disabling EEE on an interface will trigger re-negotiation. During the negotiation, the interface may change to Down state, which causes short service interruption. Therefore, determine whether the operation is allowed before you run this command.
- If auto-negotiation is disabled on an interface, the EEE configuration is automatically deleted.

Example

Enable the EEE function on electrical interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] energy-efficient-ethernet enable
```

3.9.13 port-auto-sleep enable

Function

The **port-auto-sleep enable** command enables the port dormancy function on an Ethernet electrical port to save energy.

The **undo port-auto-sleep enable** command disables the port dormancy function on an Ethernet electrical port.

By default, the port dormancy function is disabled on an Ethernet electrical port.

Format

port-auto-sleep enable

undo port-auto-sleep enable

Parameters

None

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The **port-auto-sleep enable** command enables electrical port dormancy. If this function is enabled on a port, the port enters the energy-saving mode when no carrier wave signals are transmitted on the port. When carrier wave signals are transmitted on the port, the port exits the energy-saving mode. Port sleep does not affect functioning of the port.

NOTE

Currently, this command can be used on electrical interfaces (excluding MultiGE interfaces) and combo interfaces working as electrical interfaces.

The port sleeping function is enabled by default on the ES5D21X08T00 electrical sub-card supported by the S5731-H, and S5731S-H, and cannot be disabled.

Example

Enable the port dormancy function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-auto-sleep enable
```

3.9.14 set power manage cycle

Function

The **set power manage cycle** command sets the interval for updating power consumption data.

The **undo set power manage cycle** command restores the default interval for updating power consumption data.

By default, the interval for updating power consumption data is 1 hour.

Format

set power manage cycle *cycle-id*

undo set power manage cycle

Parameters

Parameter	Description	Value
cycle-id	Sets the interval for updating power consumption data.	The value is an integer that ranges from 1 to 6. • 1: 15 minutes • 2: 30 minutes • 3: 1 hour • 4: 1 day • 5: 1 week • 6: 30 days

Views

System view

Default Level

3: Management level

Usage Guidelines

The average power consumption of a device is the average power consumption within a period of time. You can use the **set power manage cycle** command to set the interval for calculating the average power consumption. To obtain real-time power consumption, set a short interval.

Example

Set the interval for updating power consumption data to 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] set power manage cycle 1
```

3.9.15 set power manage interval

Function

The **set power manage interval** command sets the period during which the awakening port status is probed continuously.

The **undo set power manage interval** command restores the default period during which the awakening port status is probed continuously.

By default, the period is 20 minutes.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

set power manage interval *interval-time*

undo set power manage interval

Parameters

Parameter	Description	Value
interval-time	Specifies the period during which the awakening port status is probed continuously.	The value is an integer ranging from 5 to 60, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the device does not enter the dormancy state in the specified time range, the device continuously probes the status of all awakening ports. The device enters the dormancy state when the device does not probe any awakening port in Up state within the default 20 minutes. Otherwise, the device continues to probe the awakening ports status.

If no time range is applied to the device, the device probes the status of all awakening ports all round the clock. By default, the device enters the dormancy state when the device does not probe any awakening port in Up state within 20 minutes.

NOTE

In a stack, the **set power manage interval** command cannot set the period during which the awakening port status is detected continuously. However, you can use the **undo set power manage interval** command to delete the configuration in standalone mode.

Example

Set the period during which the awakening port status is probed continuously to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] set power manage interval 10
[HUAWEI] quit
<HUAWEI> save
```

3.9.16 set power manage mode

Function

The **set power manage mode** command sets the energy-saving mode of the device.

The **undo set power manage mode** command restores the default energy-saving mode of the device.

By default, the standard energy-saving mode is used.

Format

set power manage mode *mode-id*

undo set power manage mode

Parameters

Parameter	Description	Value
mode-id	Specifies the energy-saving mode of the device.	The value is an integer that ranges from 1 to 5: • 1: indicates the user-defined energy-saving mode. This mode is not supported currently. • 2: indicates the standard energy-saving mode. • 3: indicates the basic energy-saving mode. • 4: indicates the deep energy-saving mode. • 5: indicates the standby energy-saving mode. **NOTE** Only the S5720-16X-PWH-LI supports the standby energy-saving mode.

Views

System view

Default Level

3: Management level

Usage Guidelines

The **set power manage mode** command sets the energy-saving mode of the device.

The device can run in the following energy-saving modes:

- Standard mode

  Factory mode and default power saving mode.
- Basic mode

  Components not in use are shut down or switched to the sleep mode when no services are configured or users are not online.
- Deep mode

  Power consumption is dynamically adjusted for running services, and components not in use are shut down or switched to the sleep mode according to service requirements.
- Standby mode

  The device enters the low power consumption mode when it does not need to provide PoE power to PDs and shuts down all the interfaces except GE0/0/13 and GE0/0/14.

NOTE

- The ALS, EEE, and port dormancy functions are disabled in standard mode by default. However, the port dormancy function is enabled by default on the ES5D21X08T00 electrical sub-card supported by the S5731-H, and S5731S-H, and cannot be disabled.
- The ALS, EEE, and port dormancy functions are enabled by default in basic or deep mode.
- The deep mode adds the device dormancy function based on functions of the basic mode.
- Only the S5720-16X-PWH-LI supports the standby mode. The interfaces that have been shut down in standby mode cannot be enabled manually using a command. To enable these interfaces manually, ensure that the switch exits the standby mode.
- Before entering the standby mode, the system forcibly saves the configuration to the configuration file that is being used by the device.
- The configuration restoration function is not configured in the standby mode. That is, after the device restarts, the currently configured standby mode of an interface is automatically restored to the default standard mode.
- On the S5720-16X-PWH-LI XGE0/0/1 and XGE0/0/2, installing optical modules and configuring the standby mode are mutually exclusive. That is, the two interfaces cannot have the standby mode configured after they have optical modules installed. When they work in standby mode, installing optical modules into them will restore them to the default standard mode or may even restart the device.
- The minimum interval between configuring and disabling the standby mode is 15s.
- The standby mode cannot be configured in a stack.
- When the device is switched from the basic or deep mode to the standby mode, disabling the EEE function may cause interface flapping. Similarly, when the device is switched from the standby mode to the basic or deep mode, enabling the EEE function may cause interface flapping.

After the energy-saving mode is set to basic or deep mode, loopback test on interfaces is disabled. Therefore, before performing a loopback test, set the energy-saving mode to standard mode.

Example

Set the energy-saving mode of the device to basic mode.

```
<HUAWEI> system-view
[HUAWEI] set power manage mode 3
Warning: Performance of ALS, EEE, Auto sleep will be enabled, and the EEE function may lead to port
flapping. Continue?[Y/N]:y
Info: It will take a few seconds. Please wait...
```

3.9.17 set power manage non-awaken-port

Function

The **set power manage non-awaken-port** command configures a port as a non-awakening port.

The **undo set power manage non-awaken-port** command restores a non-awakening port to be an awakening port.

By default, all ports are awakening ports.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

set power manage non-awaken-port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo set power manage non-awaken-port interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-type interface-number2*]	Specifies the type and number of an interface: ● *interface-type* specifies the type of the interface. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the second interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can use the **set power manage non-awaken-port** command to configure some ports as non-awakening ports so that these ports do not affect device dormancy and awakening. This is because device dormancy and awakening depend on the awakening port status.

NOTE

In a stack, the **set power manage non-awaken-port** command cannot configure a port as a non-awakening port. However, you can use the **undo set power manage non-awaken-port** command to delete the configuration in standalone mode.

Example

Configure interfaces GigabitEthernet0/0/1 to GigabitEthernet0/0/5 as non-awakening interfaces.

```
<HUAWEI> system-view
[HUAWEI] set power manage non-awaken-port interface gigabitethernet 0/0/1 to gigabitethernet
0/0/5
Info: Succeeded in setting the configuration.
[HUAWEI] quit
<HUAWEI> save
```

3.9.18 sleep time-range

Function

The **sleep time-range** command applies a time range to the device in dormancy state.

The **undo sleep time-range** command deletes the time range.

By default, no time range is applied to the device.

NOTE

Only the S500, S5735-S, S5735-S-I, S5735S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-H, and S5736-S series switches support the sleep mode.

Format

sleep time-range *timerange-name*

undo sleep time-range *timerange-name*

Parameters

Parameter	Description	Value
timerange-name	Specifies the name of a time range that applies to the device.	The value is a string of 1 to 32 case-sensitive characters without spaces and must start with an uppercase or lowercase.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A device on an enterprise network is not used at certain time. You can apply a time range to the device in dormancy mode to save power. When dormancy conditions are met, the device automatically enters the dormancy state during the time range. When the time range expires, the device is awakened.

When an awakening interface detects a user, the device in dormancy mode is awakened. User services on the device are not affected.

The device enters the sleeping mode when the following conditions are met:

- The device works in deep mode. By default, the standard energy-saving mode is used.
- A time range applies to the device in sleeping mode.
- During the period for continuously detecting awakening port status, the terminals (switches or PCs) connected to awakening ports are shut down.

  NOTE

  If the terminal is a PC, the device can enter the dormancy state only when the PC is shut down and its network adapter is powered off (this can be set in the power management module of BIOS).

The device is awakened when either of the following conditions is met:

- A user logs in to the device through the serial port and presses Ctrl+W.
- The terminals (switches or PCs) connected to awakening ports are started up.
- The sleeping time range expires (if a time range is configured).
- A user presses the mode switching button.

Prerequisites

- The energy-saving mode of the device has been set to deep mode using the **set power manage mode** command.
- A time range has been specified using the **time-range** command.

NOTE

In a stack, the **sleep time-range** command cannot apply a time range to the device in dormancy state. However, you can use the **undo sleep time-range** command to delete the configuration in standalone mode.

Example

Apply the time range 1:00 to 6:00 am to the device.

```
<HUAWEI> system-view
[HUAWEI] set power manage mode 4
[HUAWEI] time-range test 1:00 to 6:00 daily
[HUAWEI] sleep time-range test
[HUAWEI] quit
<HUAWEI> save
```

3.10 Information Center Configuration Commands

3.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.10.2 display buffer

Function

The **display buffer** command displays statistics about logs cached in the buffer.

Format

display buffer [*feature-name* [*buffer-name*]]

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the buffer dedicated to caching logs of a specific feature.	-
buffer-name	Specifies the name of the buffer.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

On the device, service modules generate logs and control the log volume. The information center processes the received logs.

When the number of logs that are generated within a specified period (T) exceeds the threshold, the service module, with the buffer mechanism, saves extra logs to the buffer and does not send them to the information center.

You can run the **display buffer** command to view statistics about log information in the buffer.

Example

Display statistics about logs cached in the buffer on the service module **L2IF**.

```
<HUAWEI> display buffer L2IF
Feature name : L2IF
Buffer number : 1
Buffer name : CALLBACKFAIL
  Buffer ID                    : 35
```

```
Max length of message        : 256
Max number of message        : 5
Time threshold(s)            : 3600
Store lastest message number : 0
Total receive number         : 76
Total process number         : 5
Max rate record              : 0 / 3600(s)
Max rate timestamp           : 0-00-00 00:00:00
```

Table 3-143 Description of the **display buffer** command output

Item	Description
Feature name	Feature name.
Buffer number	Buffer number.
Buffer name	Buffer name.
Buffer ID	Buffer ID.
Max length of message	Maximum length of a message.
Max number of message	Maximum number of messages.
Time threshold(s)	Time threshold.
Store lastest message number	Number of messages saved to non-volatile memory.
Total receive number	Total receive number
Total process number	Total process number
Max rate record	Maximum rate record.
Max rate timestamp	Maximum rate timestamp.

3.10.3 display channel

Function

The **display channel** command displays the channel configuration.

Format

display channel [*channel-number* | *channel-name*]

Parameters

Parameter	Description	Value
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9. That is, the system has 10 channels. Channels 0 to 5 have default names and the six channels map to six different output directions. **Table 3-144** shows the relationship between channels and output directions.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Table 3-144 Relationship between channel and output directions

Channel Number	Default Channel Name	Output Direction	Description
0	console	console	Console that can receive logs, traps, and debugging messages.
1	monitor	monitor	VTY terminal that can receive logs, traps, and debugging messages, which facilitates remote maintenance.
2	loghost	loghost	Log host that can receive logs, traps, and debugging messages. By default, information is saved on the log host in file format for easy reference.
3	trapbuffer	trapbuffer	Trap buffer that can receive traps.
4	logbuffer	logbuffer	Log buffer that can receive logs.
5	snmpagent	snmpagent	SNMP agent that can receive traps.
6	channel6	Unspecified	Reserved. You can specify to which destination this channel can output information.
7	channel7	Unspecified	Reserved. You can specify to which destination this channel can output information.
8	channel8	Unspecified	Reserved. You can specify to which destination this channel can output information.

Channel Number	Default Channel Name	Output Direction	Description
9	channel9	Unspecified	Reserved. You can specify to which destination this channel can output information.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display channel** command displays the channel configuration.

When using this command, note the following points:

- When *channel-number* or *channel-name* is specified, the **display channel** command displays the specified channel that information passes through and information severity.
- When *channel-number* or *channel-name* is not specified, the **display channel** command displays all the channels that information passes through and information severity.

Example

Display the configuration of channel 0.

```
<HUAWEI> display channel 0
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging
```

Display the configuration of all channels.

```
<HUAWEI> display channel
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging

channel number:1, channel name:monitor
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging

channel number:2, channel name:loghost
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      informational Y      debugging     N      debugging

channel number:3, channel name:trapbuffer
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  N      informational Y      debugging     N      debugging
```

```
channel number:4, channel name:logbuffer
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       N      debugging     N      debugging

channel number:5, channel name:snmpagent
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  N      debugging     Y      debugging     N      debugging

channel number:6, channel name:channel6
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number:7, channel name:channel7
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number:8, channel name:channel8
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number:9, channel name:channel9
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging
```

Table 3-145 Description of the display channel command output

Item	Description
channel number	Channel number, which ranges from 0 to 9.
channel name	Channel name. **Table 3-144** lists default channel names. To set the channel name, run the **info-center channel name** command.
MODU_ID	Module ID. The default value is ffff0000.
NAME	Module name. The default value is **default**. To set the module name, run the **info-center source channel** command.
ENABLE	Whether logs/traps/debugging messages are allowed to pass through a channel: ● Y ● N To specify the channel, run the **info-center source channel** command.

Item	Description
LOG_LEVEL/ TRAP_LEVEL/ DEBUG_LEVEL	Lowest severity of output logs/traps/debugging messages. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging To set the lowest severity of output logs, run the **info-center source channel** command.

3.10.4 display debugging

Function

The **display debugging** command displays debugging messages allowed to be sent by the device.

Format

display debugging [**interface** *interface-type interface-number*] [*module-name*]

display debugging interface all

display debugging slot *slot-id* **vcpu** *vcpu-index*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vcpu** *vcpu-index* parameter.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number.	-
all	Display debugging information on all interfaces.	-

Parameter	Description	Value
module-name	Displays debugging messages sent by a specified module such as the DHCP module. If this parameter is not specified, all debugging messages allowed to be sent are displayed.	Enumerated type. The value depends on the registered module.
slot *slot-id*	Specifies a slot ID.	The value is an integer, and the value range depends on the device configuration.
vcpu *vcpu-index*	Specifies the virtual CPU number.	Specify the *vcpu-index* parameter based on the hardware configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Using the **display debugging** command, you can display the enabled debugging. If no parameters are specified, the **display debugging** command displays global debugging information.

Debugging affects device performance. The **display debugging** command displays debugging messages allowed to be sent by the Switch.

Prerequisites

By default, sending debugging messages is prohibited. The debugging of a specified module has been enabled.

Example

Display debugging messages allowed to be sent by the Switch.

```
<HUAWEI> debugging acl4 all
<HUAWEI> display debugging
ACL4 event debugging switch is on
ACL4 packet debugging switch is on
```

Table 3-146 Description of the **display debugging** command output

Item	Description
ACL4 event debugging switch is on	Event debugging is enabled for the ACL4 module.
ACL4 packet debugging switch is on	Packet debugging is enabled for the ACL4 module.

3.10.5 display info-center

Function

The **display info-center** command displays the output configuration of the information center.

Format

display info-center

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center** command to display all information recorded in the information center.

When a module is specified, you can view all information about the module recorded in the information center.

Example

Display output configuration of the information center.

```
<HUAWEI> display info-center
Information Center:enabled
Log host:
        10.1.1.1, channel number 2, channel name loghost,
language English , host facility local7
Console:
```

```
        channel number : 0, channel name : console
Monitor:
        channel number : 1, channel name : monitor
SNMP Agent:
        channel number : 5, channel name : snmpagent
Log buffer:
        enabled,max buffer size 1024, current buffer size 512,
current messages 512, channel number : 4, channel name : logbuffer
dropped messages 0, overwritten messages 53
Trap buffer:
        enabled,max buffer size 1024, current buffer size 256,
current messages 256, channel number:3, channel name:trapbuffer
dropped messages 0, overwritten messages 6229
Information timestamp setting:
        log - date, trap - date, debug - date millisecond

 Sent messages = 270090, Received messages = 281030

 IO Reg messages = 2 IO Sent messages = 10940
```

Table 3-147 Description of the display info-center command output

Item	Description
Information Center	Information center status: ● enabled ● disabled To enable the information center, run the **info-center enable** command.
Log host	Log host configuration.
10.1.1.1	Log host IP address. To set the log host IP address, run the **info-center loghost** command.
channel number	Number of a channel used to output information. To set the number of a channel used to output information, run the **info-center channel** command.
channel name	Name of a channel used to output information. To set the name of a channel used to output information, run the **info-center channel name** command.
language	Language mode in which information is output to a log host. To set the language mode in which information is output to a log host, run the **info-center loghost** command.
host facility	Logging tool. To configure the logging tool, run the **info-center loghost** command.
Console	Console configuration.
Monitor	Remote terminal configuration.
SNMP Agent	SNMP agent configuration.

Item	Description
Log buffer	Log buffer configuration.
enabled	Whether the Switch is enabled to send logs/traps to the log/trap buffer. - enabled - disabled To enable the Switch to send logs/traps to the log/trap buffer, run the **info-center logbuffer** or **info-center trapbuffer** command.
max buffer size	Maximum number of logs/traps in the log/trap buffer.
current buffer size	Maximum number of logs/traps in the current log/trap buffer. To set the maximum number of logs/traps in the current log/trap buffer, run the **info-center logbuffer size** or **info-center trapbuffer size** command.
current messages	Number of messages recorded in the log/trap buffer.
dropped messages	Number of messages discarded by the log/trap buffer.
overwritten messages	Number of overwritten messages in the log/trap buffer.
Trap buffer	Trap buffer configuration.
Information timestamp setting	Timestamp format of logs, traps, and debugging messages: - boot: indicates that the timestamp is expressed in the format of relative time, a period of time since system start. - date: indicates the current system date and time. It is expressed in mm dd yyyy hh:mm:ss format. - short-date: indicates the short date. This timestamp differs from **date** is that the year is not displayed. - format-date: indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format. - none: indicates that the output information does not contain the timestamp. To configure the timestamp format, run the **info-center timestamp** command.
Sent messages	Number of sent messages output by information center modules.
Received messages	Number of messages sent to information center modules.
IO Reg messages	Number of receive messages by switch.
IO Sent messages	Number of sent messages by switch.

3.10.6 display info-center filter-id

Function

The **display info-center filter-id** command displays information filtered by the information center.

Format

display info-center filter-id [*id* | **bymodule-alias** *modname alias*]

Parameters

Parameter	Description	Value
id	Displays filtered information with the specified ID.	The value is in hexadecimal notation and is a string of 8 digits. The value can contain 0-9, a-f, and A-F.
bymodule-alias *modname alias*	Displays filtered information with the specified module name and mnemonic symbol. ● *modname*: specifies the module name. ● *alias* specifies the mnemonic symbol.	Enumerated type. Set the value according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

ID identifies each function module for log registration. An ID filter list is the aggregation of the shielded IDs.

If *id* or **bymodule-alias** is not specified, all information is filtered.

If you do not want to output a specific log to the log file or log buffer, you can find the ID of the log in the data dictionary and run the **info-center filter-id** command to inject the ID into the filter list. Then, you can run the **display info-center filter-id** command to check whether the ID has become the one to be filtered.

Example

Display all the IDs in the filter list.

```
<HUAWEI> display info-center filter-id
ID              : 0x40394017
Module          : SHELL
Alias           : CMDRECORD
Content         : Recorded command information. (Task=[string], Ip=[string], VpnName=[STRING],
User=[string], AthenticationMethod="[STRING]",
Command="[string]")
Filtered Number : 2

ID              : 0x40394018
Module          : SHELL
Alias           : DISPLAY_CMDRECORD
Content         : Recorded display command information. (Task=[string], Ip=[string], VpnName=[string],
User=[string], AuthenticationMethod="[string]",
Command="[string]")
Filtered Number : 1
```

Table 3-148 Description of the display info-center filter-id command output

Item	Description
ID	Identifier to which each log corresponds. To configure the Switch to filter a log or trap with a specified ID, run the **info-center filter-id** *id* command.
Module	Module name. To configure the Switch to filter a log or trap with a specified module name or alias name, run the **info-center filter-id bymodule-alias** *modname alias* command.
Alias	Alias name. To configure the Switch to filter a log or trap with a specified module name or alias name, run the **info-center filter-id bymodule-alias** *modname alias* command.
Content	Log message to which each log ID corresponds.
Filtered Number	Number of times that the log to which the log ID corresponds is filtered.

3.10.7 display info-center rate-limit record

Function

The **display info-center rate-limit record** command displays the suppression of the log processing rate in the information center.

Format

display info-center rate-limit record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center rate-limit record** command to check suppression information of the log processing rate. Then you can determine whether service logs are suppressed because there are many logs.

Example

Display the suppression of the log processing rate in the information center.

```
<HUAWEI> display info-center rate-limit record
Record No.1
 InfoID                : 417d5000
 Module                  : 6OVER4
 Alias                 : DESTFAIL
 Rate limit threshold : 50
 Total receive number : 1872
 Total drop number    : 922
 Total send number    : 950
 Begin timestamp      : 2009-12-21 11:41:28
```

Table 3-149 Description of the **display info-center rate-limit record** command output

Item	Description
InfoID	Log ID.
Module	Log module name.
Alias	Log mnemonic name.
Rate limit threshold	Maximum number of logs set for the information center to process every second.
Total receive number	Total number of logs that are generated during the latest suppression period.
Total drop number	Total number of logs that are discarded during the latest suppression period.

Item	Description
Total send number	Total number of logs that the information center process during the latest suppression period.
Begin timestamp	Timestamp signifying when the suppression function is enabled for the last time.

3.10.8 display info-center rate-limit threshold

Function

The **display info-center rate-limit threshold** command displays the threshold of the log processing rate (maximum number of logs that the information center can process every second). The threshold information includes the default threshold contained in the released version, the default threshold for the specified log ID, and the threshold set through the command lines after the system startup.

Format

display info-center rate-limit threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center rate-limit threshold** command to check the log processing rate threshold of each module and then adjust the threshold based on service requirements.

Example

Display the threshold of the log processing rate set for the information center.

```
<HUAWEI> display info-center rate-limit threshold
Rate limit threshold(per second):
 Module           Alias                            Default  Config
 default                                        30       30
 IPC            IPCFRGTOOLARGE                       5        5
 IPC            IPCDUMPMEM                          5        5
 IPC            ALLOCINDEXERR                       5        5
 IPC            DRVNOTSTABLE                        2        2
```

```
IPC          NOTIMODFALNOREASM                2        2
IPC          SYNRPCGETSMFAL                5        5
IPC          SYNRPCMODUNREG                  5        5
IPC          SYNRPCRETNULL                5        5
IPC          MODULENOTREG                  5        5
IPC          SENDRETURN                5        5
IPC          GETMTUFAL                5        5
IPC          ALLOCIPCFRGFAL                5        5
IPC          RECVINVALIDMSG                5        5
IPC          RCVNOTIQUEERR                5        5
IPC          NOTIFYQUEERR                5        5
IPC          SENDFINISHRETURN                5        5
IPC          RECVINVALIDMSGTYPE                5        5
SOURCE          UMSGGETSRCOBJFAL                1        1
```

Table 3-150 Description of the **display info-center rate-limit threshold** command output

Item	Description
Module	Log module name.
Alias	Log mnemonic name.
Default	The default threshold of the log processing rate.
Config	The threshold of the log processing rate set for the information center.

3.10.9 display info-center session log status

Function

The **display info-center session log status** command displays the status of the user session logging function.

Format

display info-center session log status

Parameters

None

Views

All views

Level

3: Management level

Usage Guidelines

If no session log file is generated in a VTY window, you can run the **display info-center session log status** command to view the status of the user session logging function and status of the online user session logging function.

Example

Display the status of the user session logging function.

```
<HUAWEI> display info-center session log status
Info-center Session Log Status:
-------------------------------
Global Status: On
-------------------------------
User-Interface    Status
VTY 0             Off
VTY 1             On
VTY 2             On
VTY 3             On
CON 0              On
```

Table 3-151 Description of the **display info-center session log status** command output

Item	Description
Info-center Session Log Status	Status of the user session logging function.
Global Status	Status of the user session logging function: ● On: Recording session logs is enabled. ● Off: Recording session logs is disabled. This function can be configured using the **info-center session log disable** command in the system view.
User-Interface	User UI identifier: ● VTY/CON: indicates the user type. ● 0/1/2/3: indicates online users.
Status	Status of the online user session logging function: ● On: The function is enabled. ● Off: The function is disabled. The online user session logging function is disabled after the **info-center session log disable** command is executed to disable the user session logging function. The online user session logging function is enabled after the **undo info-center session log disable** command is executed to enable the user session logging function.

3.10.10 display info-center statistics

Function

The **display info-center statistics** command displays statistics on the information center.

Format

display info-center statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display info-center statistics** command to view statistics on the information center, including logs, traps, and debugging messages of each module.

Example

Display statistics on the information center.

```
<HUAWEI> display info-center statistics
Information statistics data:
ModuleID    ModuleName       LogSend   LogDrop   DiagSend  DiagDrop  TrapSend
TrapDrop  DebugSend DebugDrop
0x417d0000  6OVER4           0         0         0         0         0
0         0         0
0x41470000  AAA              0         0         0         0         0
0         0         0
0x406c0000  ACL              0         0         0         0         0
0         0         0
0x40ef0000  ACL6             0         0         0         0         0
0         0         0
0xff060000  ACLE             1         0         0         0         0
0         0         0
0xff380000  ADA_BFD          0         0         0         0         0
0         0         0
0x40e70000  ADDR             0         0         0         0         0
0         0         0
0xff2f0000  ADP_RRPP         0         0         114       18        0
0         0         0
0xff950000  ADPIPV4          0         0         253       393       0
0         0         0
  ---- More ----
```

Table 3-152 Description of the display info-center statistics command output

Item	Description
ModuleID	Registered ID of the module.
ModuleName	Name of the module that generates logs.
LogSend	Number of sent logs.
LogDrop	Number of discarded logs.
DiagSend	Number of sent diagnostic messages.
DiagDrop	Number of discarded diagnostic messages.
TrapSend	Number of sent traps.
TrapDrop	Number of discarded traps.
DebugSend	Number of sent debugging messages.
DebugDrop	Number of discarded debugging messages.

3.10.11 display logbuffer

Function

The **display logbuffer** command displays information recorded in the log buffer.

Format

display logbuffer [**size** *size* | **slot** *slot-id* | **module** *module-name* | **security** | **level** { *severity* | *level* }] *

display logbuffer summary [**level** *severity* | **slot** *slot-id*] *

display logbuffer order by module

Parameters

Parameter	Description	Value
size *size*	Displays the specified number of logs recently generated in the log buffer.	The value is an integer that ranges from 1 to 1024.
module *module-name*	Displays logs of a specified module in the log buffer.	Enumerated type. The value depends on the registered module.

Parameter	Description	Value
security	Specifies the security logs.	-
slot *slot-id*	Displays logs in a specified slot.	The value must be set according to the device configuration.
level { *severity* | *level* }	Displays logs of specified severity name or ID. - *severity* specifies the severity ID. - *level* specifies the severity name.	The value of *severity* is an integer that ranges from 0 to 7. - 0: Emergencies - 1: Alert - 2: Critical - 3: Error - 4: Warning - 5: Notification - 6: Informational - 7: Debugging The value of *level* is the enumerated type: - emergencies - alert - critical - error - warning - notification - informational - debugging
summary	Displays the summary of logs in the log buffer.	-

Parameter	Description	Value
order by module	Displays logs in the order of the modules to which they belong to. **NOTE** ● Logs in the log buffer are classified and displayed by the modules they belong to. ● Modules are displayed by the time that the module's first log is generated in the log buffer in descending order. ● Logs in each module are displayed by the time they are generated in descending order.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display logbuffer** command displays the information of recent logs. If the actual number of logs is smaller than the value specified by *size*, the system displays logs of the actual number.

Example

Display all the logs in the log buffer.

```
<HUAWEI> display logbuffer
Logging buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 43

Oct 16 2013 06:06:48 HUAWEI %%01VFS/4/DISKSPACE_NOT_ENOUGH(l)[3]:Disk space is
insufficient. The system begins to delete unused log files.
Oct 10 2013 19:06:48 HUAWEI %%01VFS/4/DISKSPACE_NOT_ENOUGH(l)[4]:Disk space is
insufficient. The system begins to delete unused log files.
Oct  7 2013 16:36:48 HUAWEI %%01VFS/4/DISKSPACE_NOT_ENOUGH(l)[5]:Disk space is
insufficient. The system begins to delete unused log files.
```

```
Oct  5 2013 09:12:22 HUAWEI %%01EZOP/3/PROCESS_STOP(l)[6]:Easy-operation upgrad
e process has been stopped. (Reason=There is a configuration file in this device)
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[7]:Interface XGigabitEther
net0/0/4 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[8]:Interface XGigabitEther
net0/0/3 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[9]:Interface XGigabitEther
net0/0/2 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/IF_ENABLE(l)[10]:Interface XGigabitEthe
rnet0/0/1 has been available.
Oct  5 2013 09:09:29 HUAWEI %%01IFNET/4/CARD_ENABLE(l)[11]:Board 0 card 1 has b
een available.
Oct  5 2013 09:09:24 HUAWEI %%01ALML/4/ENT_PLUG_IN(l)[12]:LS51S24CA frame[1] bo
ard[0]'s card[1] was plugged in.
Oct  5 2013 09:09:22 HUAWEI %%01IFNET/4/IF_ENABLE(l)[13]:Interface GigabitEther
net0/0/24 has been available.
Oct  5 2013 09:09:22 HUAWEI %%01IFNET/4/IF_ENABLE(l)[14]:Interface GigabitEther
net0/0/23 has been available.
Oct  5 2013 09:09:21 HUAWEI %%01IFNET/4/IF_ENABLE(l)[15]:Interface GigabitEther
net0/0/22 has been available.
Oct  5 2013 09:09:21 HUAWEI %%01IFNET/4/IF_ENABLE(l)[16]:Interface GigabitEther
net0/0/21 has been available.
Oct  5 2013 09:09:20 HUAWEI %%01IFNET/4/IF_ENABLE(l)[17]:Interface GigabitEther
net0/0/20 has been available.
Oct  5 2013 09:09:20 HUAWEI %%01IFNET/4/IF_ENABLE(l)[18]:Interface GigabitEther
net0/0/19 has been available.
Oct  5 2013 09:09:20 HUAWEI %%01IFNET/4/IF_ENABLE(l)[19]:Interface GigabitEther
net0/0/18 has been available.
Oct  5 2013 09:09:19 HUAWEI %%01IFNET/4/IF_ENABLE(l)[20]:Interface GigabitEther
net0/0/17 has been available.
Oct  5 2013 09:09:19 HUAWEI %%01IFNET/4/IF_ENABLE(l)[21]:Interface GigabitEther
net0/0/16 has been available.
Oct  5 2013 09:09:18 HUAWEI %%01IFNET/4/IF_ENABLE(l)[22]:Interface GigabitEther
net0/0/15 has been available.
Oct  5 2013 09:09:18 HUAWEI %%01IFNET/4/IF_ENABLE(l)[23]:Interface GigabitEther
net0/0/14 has been available.
  ---- More ----
```

Display logs in the order of the modules they belong to.

```
<HUAWEI> display logbuffer order by module
Logging buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 113

Nov 10 2010 16:16:53 HUAWEI %%01DHCP/4/DHCP_INFO_LOG_DHCP_REMOTEBACKUP_FAILED(l)
[0]:Saving the dynamic binding table to a remot
e server failed. Ensure that the FTP/SFTP server address is reachable and the FTP/SFTP user name and
password and the file path are
correct.
Nov 10 2010 10:38:23 HUAWEI %%01INFO/4/SUPPRESS_LOG(l)[1]:Last message repeated 1 times.
(InfoID=1077493787, ModuleName=SHELL, I
nfoAlias=LOGINFAILED)
Nov 10 2010 10:19:42 HUAWEI %%01SHELL/4/LOGINFAILED(s)[2]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=3, AccessType=
TELNET, VpnName=)
Nov 10 2010 10:19:42 HUAWEI %%01SHELL/4/LOGIN_FAIL_FOR_INPUT_TIMEOUT(s)[3]:Failed to log in due
to timeout.(Ip=10.134.27.157, U
serName=**, Times=3, AccessType=TELNET,
VpnName=)
Nov 10 2010 10:18:02 HUAWEI %%01SHELL/4/LOGINFAILED(s)[4]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=2, AccessType=
TELNET, VpnName=)
Nov 10 2010 10:18:02 HUAWEI %%01SHELL/4/LOGIN_FAIL_FOR_INPUT_TIMEOUT(s)[5]:Failed to log in due
to timeout.(Ip=10.134.27.157, U
serName=**, Times=2, AccessType=TELNET,
VpnName=)
```

```
Nov 10 2010 10:16:27 HUAWEI %%01SHELL/4/LOGINFAILED(s)[6]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=1, AccessType=
TELNET, VpnName=)
Nov 10 2010 10:16:27 HUAWEI %%01SHELL/4/LOGIN_FAIL_FOR_INPUT_TIMEOUT(s)[7]:Failed to log in due
to timeout.(Ip=10.134.27.157, U
serName=**, Times=1, AccessType=TELNET,
VpnName=)
Nov  9 2010 19:51:57 HUAWEI %%01SHELL/4/LOGINFAILED(s)[8]:Failed to login. (Ip=10.134.27.157,
UserName=**, Times=1, AccessType=
TELNET, VpnName=)
```

Table 3-153 Description of the display logbuffer command output

Item	Description
Logging buffer configuration and contents	Whether the device is enabled to output logs to the log buffer: ● enabled ● disabled To configure the device to output logs to the log buffer, run the **info-center logbuffer** command.
Allowed max buffer size	Maximum size of the log buffer.
Actual buffer size	Actual size of the log buffer. To set the log buffer size, run the **info-center logbuffer size** command.
Channel number	Number of the channel used to send logs to the log buffer. To configure the number of a channel used to send logs to the log buffer, run the **info-center channel** command.
Channel name	Name of the channel used to send logs to the log buffer. To configure the name of a channel used to send logs to the log buffer, run the **info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Display the summary of information in the log buffer.

```
<HUAWEI> display logbuffer summary
     SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
        0     0     0     0    36   476     0     0     0
```

Table 3-154 Description of the display logbuffer summary command output

Item	Description
SLOT	ID of the slot where logs are generated.
EMERG	Number of logs of emergency.
ALERT	Number of logs of alert.
CRIT	Number of logs of critical.
ERROR	Number of logs of error.
WARN	Number of logs of warning.
NOTIF	Number of logs of notification.
INFO	Number of logs of informational.
DEBUG	Number of logs of debugging.

3.10.12 display logfile

Function

The **display logfile** command displays information about a log file.

Format

display logfile *file-name* [*offset* | **hex**] *

Parameters

Parameter	Description	Value
file-name	Specifies the log file name, which can contain the drive and path.	The value is a string of case-insensitive characters, spaces not supported. If the parameter value does not contain any path, it is a string of 1 to 64 bytes. Otherwise, it is a string of 1 to 160 bytes.
offset	Displays the log file with the specified offset or byte.	The value is an integer that ranges from 0 to 2147483647.

Parameter	Description	Value
hex	Displays the log file in hexadecimal notation. If the parameter is not specified, the log file is displayed in text format.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

When encountering problems, you can query log information to know about what happened during device operation. This is helpful for fault location.

The file name is generated automatically by the system. The file name extension of the log file is *.log or *.dblg. When the current log file size reaches the specified upper limit, the system compresses the file into a *.log.zip or *.dblg.zip file.

You can view the *.log files or *.log.zip files. When viewing a *.log.zip file, you can press **Ctrl+C** to abort command execution.

When viewing the *.log.zip file, it is recommended that the length of the file name (including the driver and path) not exceed 62 bytes. Otherwise, the content of the file may fail to be viewed.

If the files you filter based on the pipe character are large and no qualified log file is displayed, the command fails to display any output for a long period of time until the command execution finishes.

For details about the log format, see "Log Message Format Description" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Log Reference - Introduction*.

Example

Display log information saved in the log file in a specified path.

```
<HUAWEI> display logfile logfile/log.log
###################################################################
#     This logfile is generated at slot 0
###################################################################

Aug 30 2013 16:18:58-05:13 HUAWEI FSP/4/STANDBY_CHANGE:OID 1.3.6.1.4.1.2011.5.25.183.1.22.3 Slot 2
is designated as standby.
Aug 30 2013 16:19:40-05:13 HUAWEI SNMP/4/WARMSTART:OID 1.3.6.1.6.3.1.1.5.2
warmStart
Aug 30 2013 16:19:15-05:13 HUAWEI %%01ACL/6/INIT_OK(l)[6]:Succeed in mqc
initializtion.
Aug 30 2013 16:19:41-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[7]:Record command information.
(Task=CFM, Ip=**, User=**, Command="vlan
batch 4090", Result=Success)
```

```
Aug 30 2013 16:19:41-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[8]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inter
face Vlanif4090", Result=Success)
Aug 30 2013 16:19:43-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[9]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inter
face Eth-Trunk10", Result=Success)
Aug 30 2013 16:19:43-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[10]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface Eth-Trunk20", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[11]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface Eth-Trunk30", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[12]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface GigabitEthernet0/0/1", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[13]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface GigabitEthernet0/0/2", Result=Success)
Aug 30 2013 16:19:44-05:13 HUAWEI %%01SHELL/5/CMDRECORD(s)[14]:Record command information.
(Task=CFM, Ip=**, User=**, Command="inte
rface GigabitEthernet0/0/3", Result=Success)
```

3.10.13 display log restrain all

Function

The **display log restrain all** command displays all log suppression configurations.

Format

display log restrain all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To check configurations of the log suppression function, run this command.

Example

Display all log suppression configurations.

```
<HUAWEI> display log restrain all
Log restrain                     : enable
Check interval in seconds        : 60
The maximum number of a log per minute : 200

---------------------------------------------------------------------
Description                  InfoId               MaxCount
---------------------------------------------------------------------
```

```
RecordCommand(*)              40394017              NotLimit
RecordCommandResult(*)           40394025              NotLimit
```

Table 3-155 Description of the **display log restrain all** command output

Item	Description
Log restrain	Whether log suppression is enabled.
Check interval in seconds	Statistical period, in seconds.
The maximum number of a log per minute	Maximum number of logs that can be generated every minute.
Description	Description.
InfoId	Log ID.
MaxCount	Maximum number of logs with a specific log ID that can be generated per minutes.

3.10.14 display log restrain statistics

Function

The **display log restrain statistics** command displays all log suppression statistics.

Format

display log restrain statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view all log suppression statistics, run this command.

Example

Display all log suppression statistics.

```
<HUAWEI> display log restrain statistics
Total number of logs                   : 56477
```

```
Average number of logs per minute      : 6
Maximum number of logs per minute      : 1796
Minimum number of logs per minute      : 0
Number of log types in the last minute : 0


-------------------------------------------------------------------
InfoId                         TotalDiscard           MaxCount
-------------------------------------------------------------------
ff51502a                         29                   229
ffd35005                         124                   324
```

Table 3-156 Description of the **display log restrain statistics** command output

Item	Description
Total number of logs	Total number of logs.
Average number of logs per minute	Average number of logs generated per minute.
Maximum number of logs per minute	Maximum number of logs generated per minute.
Minimum number of logs per minute	Minimum number of logs generated per minute.
Number of log types in the last minute	Number of types of the logs generated in the last minute.
InfoId	Log ID.
TotalDiscard	Total number of discarded logs.
MaxCount	Maximum number of logs with a specific log ID generated per minutes.

3.10.15 display trapbuffer

Function

The **display trapbuffer** command displays information recorded in the trap buffer.

Format

display trapbuffer [**size** *value* | **slot** *slot-id* | **module** *module-name* | **level** { *severity* | *level* }] *

display trapbuffer order by module

Parameters

Parameter	Description	Value
size *value*	Displays the specified number of traps recently generated in the trap buffer. If this parameter is not specified, all traps are displayed.	The value is an integer that ranges from 1 to 1024.
module *module-name*	Displays traps of a specified module in the trap buffer.	Enumerated type. The value depends on the registered module.
slot *slot-id*	Displays traps in a specified slot.	The value must be set according to the device configuration.
level { *severity* | *level* }	Displays traps of specified severity name or ID. • *severity* specifies the severity ID. • *level* specifies the severity name.	The value of *severity* is an integer that ranges from 0 to 7. • 0: Emergencies • 1: Alert • 2: Critical • 3: Error • 4: Warning • 5: Notification • 6: Informational • 7: Debugging The value of *level* is the enumerated type: • emergencies • alert • critical • error • warning • notification • informational • debugging

Parameter	Description	Value
order by module	Displays alarms in the order of the modules they belong to. **NOTE** - Alarms in the alarm buffer are classified and displayed by the modules they belong to. - Modules are displayed by the time that the module's first alarm is generated in the alarm buffer in descending order. - Alarms in each module are displayed by the time they are generated in descending order.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display trapbuffer** command displays the information of recent traps. If the number of traps in the trap buffer is smaller than *value*, traps of the actual number are displayed.

Example

Display all traps in the trap buffer.

```
<HUAWEI> display trapbuffer
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 6248
Current messages : 256

#Sep 19 2012 04:38:03+08:00 HUAWEI DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.5.25.191.3.1 configurations have been changed. The current change number is 8,
the change loop count is 0, and the maximum number of records is 4095.
#Sep 19 2012 04:37:39+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.114, UserC
hannel=VTY0)
#Sep 19 2012 04:35:48+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, Use
rChannel=VTY0)
#Sep 19 2012 04:20:54+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, UserC
hannel=VTY0)
#Sep 19 2012 04:08:03+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, Use
rChannel=VTY0)
```

```
#Sep 19 2012 03:54:27+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.143, UserC
hannel=VTY0)
#Sep 19 2012 03:54:18+08:00 HUAWEI LINE/5/VTYUSERLOGINFAIL:OID 1.3.6.1.4.1.2011
.5.25.207.2.3 A user login fail. (UserIndex=34, UserName=VTY, UserIP=10.135.18.1
43, UserChannel=VTY0)
#Sep 19 2012 02:51:03+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=34, UserName=VTY, UserIP=10.135.18.57, User
Channel=VTY0)
#Sep 19 2012 02:50:24+08:00 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.
25.207.2.4 A user logout. (UserIndex=35, UserName=VTY, UserIP=10.135.18.164, Use
rChannel=VTY1)
#Sep 19 2012 02:40:19+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=35, UserName=VTY, UserIP=10.135.18.164, UserC
hannel=VTY1)
#Sep 19 2012 02:35:23+08:00 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.2
5.207.2.2 A user login. (UserIndex=34, UserName=VTY, UserIP=10.135.18.57, UserCh
annel=VTY0)
......
```

Display alarms in the order of the modules they belong to.

```
<HUAWEI> display trapbuffer order by module
Trapping buffer configuration and contents : enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , Channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 79

#Nov 11 2010 11:51:24 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=36, UserName=**, Us
erIP=10.135.19.152, UserChannel=VTY2)
#Nov 10 2010 18:54:06 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=35, UserName=**, Us
erIP=10.135.186.212, UserChannel=VTY1)
#Nov 10 2010 12:07:44 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=34, UserName=**, Us
erIP=10.135.19.157, UserChannel=VTY0)
#Nov 10 2010 11:19:23 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.25.207.2.4 A user logout.
(UserIndex=34, UserName=**,
UserIP=10.134.27.157, UserChannel=VTY0)
#Nov 10 2010 10:48:57 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=34, UserName=**, Us
erIP=10.134.27.157, UserChannel=VTY0)
#Nov 10 2010 10:48:48 HUAWEI LINE/5/VTYUSERLOGOUT:OID 1.3.6.1.4.1.2011.5.25.207.2.4 A user logout.
(UserIndex=34, UserName=**,
UserIP=10.134.27.157, UserChannel=VTY0)
#Nov 10 2010 10:38:23 HUAWEI LINE/5/VTYUSERLOGIN:OID 1.3.6.1.4.1.2011.5.25.207.2.2 A user login.
(UserIndex=34, UserName=**, Us
erIP=10.134.27.157, UserChannel=VTY0)
```

Table 3-157 Description of the display trapbuffer command output

Item	Description
Trapping buffer configuration and contents	Whether the device is enabled to output traps to the trap buffer: ● enabled ● disabled To enable the device to output traps to the trap buffer, run the **info-center trapbuffer** command.

Item	Description
Allowed max buffer size	Maximum size of the trap buffer.
Actual buffer size	Actual size of the trap buffer. To set the size of the trap buffer, run the **info-center trapbuffer size** command.
Channel number	Number of the channel used to send traps to the trap buffer. To set the channel number, run the **info-center channel** command.
Channel name	Name of the channel used to send traps to the trap buffer. To set the channel name, run the **info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

3.10.16 info-center channel

Function

The **info-center channel** command configures channels for outputting information in various directions.

The **undo info-center channel** command restores the default settings.

By default, the system outputs information in various directions through channels listed in the table below.

Table 3-158 Default association between the channel number, channel name, and output direction of information channels

Channel Number	Channel Name	Output Direction
0	console	Console
1	monitor	User terminal
2	loghost	Log host
3	trapbuffer	Trap buffer
4	logbuffer	Log buffer

Channel Number	Channel Name	Output Direction
5	snmpagent	SNMP agent
6	channel6	Unspecified
7	channel7	Unspecified
8	channel8	Unspecified
9	channel9	Log file

Format

info-center { **console** | **logbuffer** | **logfile** | **monitor** | **snmp** | **trapbuffer** } **channel** { *channel-number* | *channel-name* }

undo info-center { { **console** | **monitor** | **snmp** | **logfile** } **channel** | { **logbuffer** | **trapbuffer** } **channel** [*channel-number* | *channel-name*] }

Parameters

Parameter	Description	Value
console	Specifies the channel used to output information to the console.	-
logbuffer	Specifies the channel used to output information to the log buffer.	-
logfile	Specifies the channel used to output information to the log file.	-
monitor	Specifies the channel used to output information to the user terminal.	-
snmp	Specifies the channel used to output information to the SNMP agent.	-
trapbuffer	Specifies the channel used to output information to the trap buffer.	-
channel-number	Specifies the channel number.	The value is an integer ranging from 0 to 9.
channel-name	Specifies the name of a channel, which can be the default channel name or a user-defined name.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center channel** command in the following scenarios: The same information is sent to different directions. For example, the log file and log host record the same content or the trap buffer and the SNMP agent record the same content.

NOTE

The channels should not have the same name.

For details on how to configure a channel for outputting information to a log host, see **info-center loghost**.

The **info-center channel** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Configure the channel used to output information to a console.

```
<HUAWEI> system-view
[HUAWEI] info-center console channel console
```

Configure the channel used to output information to the log buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center logbuffer channel logbuffer
```

Configure the channel used to output information to the user terminal.

```
<HUAWEI> system-view
[HUAWEI] info-center monitor channel monitor
```

Configure the channel used to output information to an SNMP agent.

```
<HUAWEI> system-view
[HUAWEI] info-center snmp channel 5
```

Configure the channel used to output information to the trap buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center trapbuffer channel trapbuffer
```

3.10.17 info-center channel name

Function

The **info-center channel name** command names a channel with a specified number.

The **undo info-center channel** command restores the default channel name.

The following lists default channel names.

Table 3-159 Default channel names

Channel Number	Default Channel Name
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent
6	channel6
7	channel7
8	channel8
9	channel9

Format

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

Parameters

Parameter	Description	Value
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9. That is, the system has 10 channels.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can rename channels, which facilitates memorization and usage.

Precautions

Channel names must be unique. It is recommended that channel names represent channel functions.

Example

Name channel 0 execconsole.

```
<HUAWEI> system-view
[HUAWEI] info-center channel 0 name execconsole
```

3.10.18 info-center enable

Function

The **info-center enable** command enables the information center.

The **undo info-center enable** command disables the information center.

The **info-center disable** command disables the information center.

By default, the information center is enabled.

Format

info-center enable

undo info-center enable

info-center disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During device running, the information center records device operation. The system outputs system information to destinations such as the log host and the console only after the information center is enabled. Network administrators can store and query output information to monitor device running and locate faults.

Precautions

After the **undo info-center enable** or **info-center disable** command is executed, only logfile, logbuffer, and user session record logs, the other channel no longer records logs.

Follow-up Procedure

Configure a rule for outputting information to the terminal or remote server.

Example

Enable the information center.

```
<HUAWEI> system-view
[HUAWEI] info-center enable
Info: Information center is enabled.
```

3.10.19 info-center filter-id

Function

The **info-center filter-id** command configures the Switch to filter a specified log or trap.

The **undo info-center filter-id** command disables the Switch from filtering a specified log or trap.

By default, no log or trap is filtered.

Format

info-center filter-id { *id* | **bymodule-alias** *modname alias* } &<1-50>

info-center filter-id { *id* | **bymodule-alias** *modname alias* } [**bytime** *interval* | **bynumber** *number*]

undo info-center filter-id all

undo info-center filter-id { *id* | **bymodule-alias** *modname alias* } &<1-50>

undo info-center filter-id { *id* | **bymodule-alias** *modname alias* } [**bytime** *interval* | **bynumber** *number*]

Parameters

Parameter	Description	Value
id	Specifies the ID of the log or trap to be filtered. **NOTE** This parameter indicates the ID of a log. If this parameter fails to be configured, the log specified by this ID does not exist.	The value is in hexadecimal notation and contains 8 digits. The value contains 0-9, a-f, and A-F.
bymodule-alias *modname alias*	Specifies the module name and alias name corresponding to the log or trap to be filtered.	Enumerated type. Set the value according to the device configuration.

Parameter	Description	Value
all	Filters all logs or traps.	-
bytime *interval*	Specifies the interval at which logs are sent.	The value is an integer that ranges from 1 to 86400, in seconds.
bynumber *number*	Specifies the number of logs that are discarded between two received logs.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If some logs or traps are unnecessary, configure the Switch not to output the logs and traps. When the filtering function is enabled, the information center does not send the traps with a specified ID that satisfy the filtering condition to any channel. As a result, the trap buffer, console, terminal, or SNMP agent cannot receive the traps with the specified ID.

Precautions

- Currently, the Switch can filter traps with a maximum of 50 IDs. If there are more than 50 log IDs, the system displays a message indicating that the filtering table is full. To configure the filtering function, run the **undo info-center filter-id** { *id* | **bymodule-alias** *modname alias* } &<1-50> [**bytime** *interval* | **bynumber** *number*], or the **undo info-center filter-id all** command to delete original IDs and reconfigure the log ID.
- When both the **bytime** *interval* and **bynumber** *number* parameters are not specified, all the logs with the specified ID will be discarded.
- When the **bytime** *interval* parameter is specified, the interval for sending two allowed logs must be at least the configured time.
- When the **bynumber** *number* parameter is specified, the configured number of logs between two allowed logs must be discarded.
- To add multiple IDs at a time, use a space to separate every two IDs. The result of adding each ID is displayed.
- You cannot add the same ID or alias name repeatedly.
- When you add an unregistered or nonexistent ID or alias name, the system displays a message indicating that the system fails to filter the log or trap with the specified ID or alias name.

- During a software upgrade, if the information filtering function is configured in the old version, but the new version does not support the specified log module and alias, the information filtering configuration of the specified log module and alias will be automatically cleared after the upgrade.
- You are advised to use the module name and alias to filter specified log information. The *id* parameter can be obtained by running the **display info-center register-info** [**module** *module-name*] **log** command in the diagnostic view, and the *modname* and *alias* parameters can be obtained through the command association function.

Example

Filter information by module names and alias names.

```
<HUAWEI> system-view
[HUAWEI] info-center filter-id bymodule-alias CMD CMD_PRI_REARRG
```

Cancel filtering for all logs.

```
<HUAWEI> system-view
[HUAWEI] undo info-center filter-id all
```

Filter the log with the ID of 40394017.

```
<HUAWEI> system-view
[HUAWEI] info-center filter-id 40394017
```

3.10.20 info-center local log-counter disable

Function

The **info-center local log-counter disable** command disables the local log from carrying the sequence number.

The **undo info-center local log-counter disable** command enables the local log to carry the sequence number.

By default, the local log carries the sequence number.

Format

info-center local log-counter disable

undo info-center local log-counter disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device keeps running for a long time, a large number of logs may be generated.

- You can run the **info-center local log-counter disable** command to disable logs sent to the log buffer, log file, console, or terminal from carrying the sequence number, and run the **undo info-centerlocal log-counter disable** command to enable these logs to carry the sequence number.
- You can run the **undo info-center local log-counter disable** command to enable logs to carry the incremental sequence number, checking whether all logs have been sent to the log buffer, log file, console, or terminal.

NOTE

- Logs sent to the console log file, or terminal are counted separately and therefore carry different sequence numbers in ascending order. The sequence number of the earliest log is 0.
- Logs sent to the log buffer carry sequence numbers in descending order. The sequence number of the latest log is 0.

Example

Disable local logs from carrying the sequence number.

```
<HUAWEI> system-view
[HUAWEI] info-center local log-counter disable
```

Enable local logs to carry the sequence number.

```
<HUAWEI> system-view
[HUAWEI] undo info-center local log-counter disable
```

3.10.21 info-center logbuffer

Function

The **info-center logbuffer** command enables the Switch to send logs to the log buffer.

The **undo info-center logbuffer** command disables the Switch from sending logs to the log buffer.

By default, the Switch is enabled to send logs to the log buffer.

Format

info-center logbuffer

undo info-center logbuffer

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To log in to a device and check the faults or problems during operation, run the **info-center logbuffer** command to enable the function to output logs to the log buffer. Then, you can view log information in the log buffer.

By configuring the size of the log buffer using the **info-center logbuffer size** *buffersize* command, you can view information about specified logs.

By configuring the number or name of a channel through which a device sends logs to the log buffer using the **info-center logbuffer channel** { *channel-number* | *channel-name* } command, you can send log information through a specified channel to the log buffer.

Example

Enable the Switch to send logs to the log buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center logbuffer
```

3.10.22 info-center logbuffer size

Function

The **info-center logbuffer size** command sets the maximum number of logs in the log buffer.

The **undo info-center logbuffer size** command restores the default maximum number of logs in the log buffer.

By default, a log buffer can store a maximum of 512 logs.

Format

info-center logbuffer size *logbuffer-size*

undo info-center logbuffer size [*logbuffer-size*]

Parameters

Parameter	Description	Value
logbuffer-size	Specifies the maximum number of logs in the log buffer.	The value is an integer that ranges from 0 to 1024. If *logbuffer-size* is 0, logs are not displayed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the number of logs in the log buffer reaches the maximum value, new logs will replace the existing logs that were placed earlier in the log buffer until all the new logs are stored.

Precautions

When you run the **info-center logbuffer size** command multiple times, only the latest configuration takes effect.

The **info-center logbuffer size** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Set the maximum number of logs in the log buffer to 50.

```
<HUAWEI> system-view
[HUAWEI] info-center logbuffer size 50
```

3.10.23 info-center logfile size

Function

The **info-center logfile size** command sets the log file size.

The **undo info-center logfile size** command restores the default log file size.

By default, the log file size is 8 MB.

Format

info-center logfile size *size*

undo info-center logfile size

Parameters

Parameter	Description	Value
size	Specifies the log file size.	The value is an integer that is 4, 8, 16, or 32, in MB. The default value is 8 MB.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the Switch to export information to a log file, run the **info-center logfile size** command to set the log file size.

Precautions

If you configure the device to export information to a log file, exported information is saved in the **log.log** or **log.dblg** file. When the **log.log** or **log.dblg** file exceeds the specified size, the system compresses the file in to a zip package and names the compressed file *date time*.log.zip or *date time*.dblg.zip.

The **info-center logfile size** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Set the log file size to 32 MB.

```
<HUAWEI> system-view
[HUAWEI] info-center logfile size 32
```

3.10.24 info-center loghost

Function

The **info-center loghost** command configures the device to output information to a log host.

The **undo info-center loghost** command disables the device from outputting information to a log host.

By default, no information is output to the log host.

Format

info-center loghost *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | { **vpn-instance** *vpn-instance-name* | **public-net** } | **local-time** | **log-counter** { **disable** | **enable** } | **port** *port* | **security-log** | **operation-log** | { **source-ip** *source-ip-address* } | **transport** { **udp** | **tcp ssl-policy** *policy-name* [**verify-dns-name** *verify-dns-name*] }] *

info-center loghost ipv6 *ipv6-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | **local-time** | **log-counter** { **disable** | **enable** } | **port** *port* | **security-log** | **operation-log** | **transport** { **udp** | **tcp ssl-policy** *policy-name* [**verify-dns-name** *verify-dns-name*] }] *

undo info-center loghost *ip-address* [**vpn-instance** *vpn-instance-name*]

undo info-center loghost ipv6 *ipv6-address*

info-center loghost domain *domain-name* [**vpn-instance** *vpn-instance-name*] [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | **log-counter** { **disable** | **enable** } | **local-time** | **port** *port* | **security-log** | **operation-log** | **transport** { **udp** | **tcp ssl-policy** *policy-name* [**verify-dns-name** *verify-dns-name*] }] *

undo info-center loghost domain *domain-name* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the log host.	The value is in dotted decimal notation.
channel { *channel-number* | *channel-name* }	Specifies the channel used to send information to a log host. ● *channel-number*: specifies the number of a channel. ● *channel-name*: specifies the name of a channel. The name can be the default or user-defined channel name.	The value of *channel-number* is an integer that ranges from 0 to 9. The value of *channel-name* is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.
facility *local-number*	Specifies a syslog server facility that is used to identify the log information source. You can use this parameter to plan a local value for the log information of a specified device, so that the syslog server can handle received log information based on the parameter.	The value ranges from local0 to local7. The default value is local7.
language *language-name*	Displays the language in which logs are recorded.	Currently, the value can only be English.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	VPN instance.	The value must be an existing VPN instance name. **NOTE** _public_ cannot be specified as a VPN instance name.If the VPN instance is not created, the command does not take effect.
public-net	Indicates that the log host is connected in the public network.	-
local-time	Indicates the local time when logs are sent to the log host.	-
log-counter { **disable** | **enable** }	Disables or enables the log counter function.	-
port *port*	Specifies the port number of a log host.	The value is an integer that ranges from 1 to 65535. By default, when the transport mode is UDP, the port number of the log host is 514; when the transport mode is TCP, the port number of the log host is 6514.
security-log	Configures a device to send security logs to a specified log host.	-
operation-log	Configures a device to send operation logs to a specified log host.	-
source-ip *source-ip-address*	Specifies the source IP address used to send information to the log host.	The value is in dotted decimal notation.
transport	Indicates the information transport mode.	-

Parameter	Description	Value
udp	Indicates the UDP transport mode. **NOTE** The default transport mode is UDP if no transport mode is specified.	-
tcp	Indicates the TCP transport mode. **NOTE** The default transport mode is UDP if no transport mode is specified.	-
ssl-policy *policy-name*	Specifies a Secure Sockets Layer (SSL) policy in the TCP transport mode. This parameter is recommended to improve log transmission security.	The value is a string of 1 to 23 case-insensitive characters without spaces.
verify-dns-name *verify-dns-name*	Verify DNS identifier name.	The value is a string of 1 to 255 case-insensitive characters without spaces.
ipv6 *ipv6-address*	Specifies the IPv6 address of the log host.	The value is a 32-digit hexadecimal number.
domain *domain-name*	Specifies a DNS domain name of a log host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To query information generated on the Switch deployed remotely, configure the Switch to export information to a log host so that you can view device information on the log host. Run the **info-center loghost** command to configure the Switch to export information to a log host.

To configure the Switch to output information to different log hosts using different channels, specify the channels used to send information to the log hosts. For example, you can configure the Switch to output information to log hosts at 192.168.0.1 and 192.168.0.2 using channels 7 and 8 respectively.

Precautions

The Switch can output information to eight log hosts including IPv4 and IPv6 hosts to implement backup among log hosts.

To transfer logs to the log hosts using TCP and encrypt logs using SSL, create an SSL policy first.

If the **set net-manager vpn-instance** command is run to configure the NMS to manage network elements through a VPN instance, either of the following situations occurs.

- If **vpn-instance** is configured, the system accesses the log host in the VPN instance.
- If **public-net** is configured, the system accesses the log host on the public network.

If the **transport tcp ssl-policy** *policy-name* parameters are specified to enable logs to be transmitted in TCP mode through SSL encryption, perform the following operations:

- Run the **ssl-policy** *policy-name* command to configure an SSL policy and enter the SSL policy view.
- Run the **trusted-ca load** command to load trusted-CA files (**cacert** and **rootcert** files) of the SSL client.
- On the log server, load trusted-CA files (**serverkey** and **servercert** files) of the SSL server.
- Run the **display tcp status** command to check that the TCP connection status of port 6514 is **Established**.

Example

Configure a device to use channel 6 to output information to the log host at 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost 10.1.1.1 channel channel6
```

Configure the source IP address used to send information to the log host is Loopback1.

```
<HUAWEI> system-view
[HUAWEI] info-center  loghost source LoopBack1
```

Configure the Switch to send information to the log host at FC00:0:0:3001::1/64.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost ipv6 fc00:0:0:3001::1
```

Configure the Switch to send information to the host with the IPv4 address 192.168.2.2 and VPN instance name **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost 192.168.2.2 vpn-instance vpn1
```

Configure a device to send information to a log host with the domain name set to **www.test.com**.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost domain www.test.com
```

Configure a device to send information to the log host at 192.168.2.2 in TCP mode, using the SSL policy **YsHsjx_202206** that has been created in the system.

```
<HUAWEI> system-view
[HUAWEI] ssl policy YsHsjx_202206
[HUAWEI-ssl-policy-ftps_der] trusted-ca load pem-ca 1_cacert_pem_rsa.pem
[HUAWEI-ssl-policy-ftps_der] trusted-ca load pem-ca 1_rootcert_pem_rsa.pem
[HUAWEI-ssl-policy-ftps_der] quit
```

3.10.25 info-center loghost source

Function

The **info-center loghost source** command configures the source interface used by the Switch to send information to a log host.

The **undo info-center loghost source** command restores the default source interface used by the Switch to send information to a log host.

By default, the source interface for a device to send logs to a log host is the actual interface that sends the logs.

Format

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If multiple devices send log messages to the same log host, you can identify the devices by setting different source interfaces so as to index the received log messages.

The source interface specified in the **info-center loghost source** command for a device to send logs to a log host is not necessarily the actual interface that sends the logs, but the IP address of the specified source interface is carried in logs.

Prerequisites

There is a reachable route between the source interface and the log host.

Example

Specify Loopback0 IP address as the source interface address to send information to a log host.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] ip address 10.1.1.1 255.255.255.0
[HUAWEI-LoopBack0] quit
[HUAWEI] info-center loghost source loopback 0
```

3.10.26 info-center loghost source-port

Function

The **info-center loghost source-port** command configures a source interface through which the device sends information to the log host.

The **undo info-center loghost source-port** command restores the default source interface through which the device sends information to the log host.

By default, the source interface number is 38514.

Format

info-center loghost source-port *source-port*

undo info-center loghost source-port

Parameters

Parameter	Description	Value
source-port	Specifies the number of the source interface through which the device sends information to the log host.	The value is an integer ranging from 1025 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

If the device uses the default source interface to send information to the log host, attackers may keep accessing this interface. As a result, the log host cannot send information. To improve system security, you can run the **info-center loghost source-port** *source-port* command to change the source interface through which the device sends information to the log host so that attackers cannot obtain the new source interface.

Example

Change the number of the source interface through which the device sends information to the log host to 1026.

```
<HUAWEI> system-view
[HUAWEI] info-center loghost source-port 1026
```

3.10.27 info-center max-logfile-number

Function

The **info-center max-logfile-number** command sets the maximum number of log files to be saved.

The **undo info-center max-logfile-number** command restores the default maximum number of log files to be saved.

By default, a maximum of 500 log files can be stored on the S5732-H, S6730-H, S6730-S, S6730S-S, and S6730S-H, and a maximum of 200 log files can be stored on other models.

Format

info-center max-logfile-number *filenumbers*

undo info-center max-logfile-number

Parameters

Parameter	Description	Value
filenumbers	Specifies the maximum number of log files that can be saved.	The value is an integer that ranges from 3 to 500.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If too many log files are saved on the Switch, many disk space resources are occupied. To view log files generated recently, run the **info-center max-logfile-number** command to set the maximum number of log files that can be saved.

Precautions

If the number of log files generated on the Switch exceeds the limit, the system deletes the oldest log file so that the number of log files is not larger than the maximum value.

NOTICE

If the number of saved log files is greater than the default value, more system resources are consumed. The default value is recommended. Excess log files can be deleted automatically. When the system deletes excess log files, high CPU usage may last for a short period.

Example

Set the maximum number of log files to be saved to 100.

```
<HUAWEI> system-view
[HUAWEI] info-center max-logfile-number 100
```

3.10.28 info-center rate-limit except

Function

The **info-center rate-limit except** command cancels the log processing rate limit for logs.

The **undo info-center rate-limit except** command deletes the preceding configuration.

Format

info-center rate-limit except { **byinfoid** *infoID* | **bymodule-alias** *modname alias* }

undo info-center rate-limit except { **byinfoid** *infoID* | **bymodule-alias** *modname alias* }

Parameters

Parameter	Description	Value
byinfoid *infoID*	Specifies the log ID in hexadecimal notation.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to fffffff.
bymodule-alias *modname*	Specifies the log module name.	The value is a string of 1 to 24 case-insensitive characters without spaces.

Parameter	Description	Value
alias	Specifies the log mnemonic name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

When too many logs will never be generated under a specified ID, you can run the **info-center rate-limit except** command to avoid the impact of the suppression of the log processing rate. After this command is run, the configured log processing rate limit will not be effective for logs with the specified ID or module name.

During a software upgrade, if the function that prevents logs from being suppressed by the information center is configured in the old version, but the new version does not support the specified log module and alias, the function configuration of the specified log module and alias will be automatically cleared after the upgrade.

Example

Prevent logs specified by the module name and mnemonic from being suppressed by the information center.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit except bymodule-alias AAA AUTHEN_ERR_EVENT
```

Prevent logs specified by the log ID from being suppressed by the information center.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit except byinfoid ff011015
```

Prevent logs with a specified log ID from being suppressed by the information center.

```
<HUAWEI> system-view
[HUAWEI] undo info-center rate-limit except bymodule-alias AAA AUTHEN_ERR_EVENT
```

3.10.29 info-center rate-limit global-threshold

Function

The **info-center rate-limit global-threshold** command sets the total number of logs that the information center can process every second.

The **undo info-center rate-limit global-threshold** command restores the default value.

By default, the information center processes a maximum of 400 logs in every second.

Format

info-center rate-limit global-threshold *value*

undo info-center rate-limit global-threshold

Parameters

Parameter	Description	Value
value	Specifies the maximum number of logs that the information center can process every second.	The value is an integer that ranges from 100 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center rate-limit global-threshold** command to adjust the processing capability of the information center. If the number of logs to be processed exceeds the processing capability of the information center, the extra logs are discarded.

NOTE

- If the threshold is too low, some logs may be discarded.
- If the threshold is too high, the information center cannot identify the log ID under which too many logs are generated. The number of logs to be processed depends on the current processing capacity of the information center.

Example

Set the number of logs that the information center can process every second to 300.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit global-threshold 300
```

3.10.30 info-center rate-limit monitor-period

Function

The **info-center rate-limit monitor-period** command sets the monitoring period for the information center to suppress the log processing rate.

The **undo info-center rate-limit monitor-period** command restores the default value.

By default, the monitoring period is 3 seconds.

Format

info-center rate-limit monitor-period *value*

undo info-center rate-limit monitor-period

Parameters

Parameter	Description	Value
value	Specifies the monitoring period for the information center to suppress the log processing rate.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

In the monitoring period specified by *value*, if the rate of sending a single log every second exceeds the threshold configured using the **info-center rate-limit threshold** command, the information center will limit the log processing rate. In this situation, the information center discards logs exceeding the threshold.

In the monitoring period that is five times *value*, if the number of a single type of logs that are sent every second is smaller than the threshold configured using the **info-center rate-limit threshold** command, the information center does not limit the log processing rate.

Example

Set the monitoring period for the information center to suppress the log processing rate to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit monitor-period 5
```

3.10.31 info-center rate-limit threshold

Function

The **info-center rate-limit threshold** command sets the maximum number of logs with the same log ID that the information center can process every second.

The **undo info-center rate-limit threshold** command restores the default setting.

By default, the information center processes a maximum of 30 logs with the same log ID in every second.

Format

info-center rate-limit threshold *value* [**byinfoid** *infoID* | **bymodule-alias** *modname alias*]

undo info-center rate-limit threshold [*value*] [**byinfoid** *infoID* | **bymodule-alias** *modname alias*]

Parameters

Parameter	Description	Value
value	Specifies the maximum number of logs with the same log ID that the information center can process every second.	The value is an integer that ranges from 1 to 500.
byinfoid *infoID*	Specifies the log ID.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
bymodule-alias *modname*	Specifies the log of the module name.	The value is a string of 1 to 24 case-insensitive characters without spaces.
alias	Specifies the log of the mnemonic name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center rate-limit threshold** command to set the maximum number of logs with the same log ID that the information center can process every second. The information center monitors the number of logs that are generated every second under the same log ID. When the number of logs that are generated every second under the same log ID exceeds the threshold in the monitoring period, the information center decides that too many logs are generated and suppresses its log processing rate by processing only the conforming traffic (logs within the threshold) and discarding the non-conforming traffic (logs exceeding the threshold). When the number of logs that are generated every second under the same log ID falls below the threshold and remains below the threshold for five monitoring periods, the information center removes the suppression.

By default, the information center processes a maximum of 30 logs with the same log ID in every second. In certain application scenarios, by default, the information center needs to process more than 50 logs with the same log ID in every second. You can set thresholds for logs with different log IDs. Generally, the default threshold is recommended.

- If the threshold is too low, some logs may be discarded.
- If the threshold is too high, the information center cannot identify the log ID under which too many logs are generated.

NOTE

- If the threshold *value1* specified by the parameter **byinfoid** *infoID* or **bymodule-alias** *modname alias* differs from the threshold *value0* specified globally, *value1* takes effect.
- During a software upgrade, if the threshold is configured in the old version, but the new version does not support the specified log module and alias, the threshold configuration of the specified log module and alias will be automatically cleared after the upgrade.

Example

Set the maximum number of logs that the information center can process every second to 60.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit threshold 60
```

Set the maximum number of logs identified by the same module name and mnemonic that the information center can process every second to 30.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit threshold 30 bymodule-alias AAA AUTHEN_ERR_EVENT
```

Set the maximum number of logs with the same log ID that the information center can process every second to 20.

```
<HUAWEI> system-view
[HUAWEI] info-center rate-limit threshold 20 byinfoid ff011015
```

Restore the maximum number of logs that the information center can process every second to the default value.

```
<HUAWEI> system-view
[HUAWEI] undo info-center rate-limit threshold
```

Cancel the restriction on the maximum number of logs with a specified log ID that the information center can process every second.

```
<HUAWEI> system-view
[HUAWEI] undo info-center rate-limit threshold bymodule-alias AAA AUTHEN_ERR_EVENT
```

3.10.32 info-center session log disable

Function

The **info-center session log disable** command disables the user session logging function.

The **undo info-center session log disable** command enables the user session logging function.

By default, the user session logging function is enabled.

Format

info-center session log disable

undo info-center session log disable

Parameters

None

Views

System view

Level

3: Management level

Usage Guidelines

Usage Scenario

The user session logging function saves the user input, device screen output, and time when the device executes the commands entered by users to a session log file. If the device becomes faulty or services become abnormal, you can obtain the user operation records from the saved session log file for fault location.

A session log file is generated in each VTY window and named cli_channel name.log, for example: **cli_vty1.log**. The generated session log files are stored in the sessionlog directory. The file size cannot exceed 1 MB.

If the number of session log files exceed the maximum value 20 (cannot be changed), the system compresses the files into .zip files. The compressed file is named cli_slot ID_timestamp_channel name_host name.log.zip, for example: **cli_11_20171129081148_vty1_huawei.log.zip**.

If the remaining device space is less than 30 MB, the system deletes the earliest log files until the remaining device space is more than 30 MB.

Precautions

Using the **undo info-center enable** or **info-center disable** command disables the information center will not affect the user session logging function. This function can only be enabled or disabled using the **undo info-center session log disable** or **info-center session log disable** command.

Example

Disable the user session logging function.

```
<HUAWEI> system-view
[HUAWEI] info-center session log disable
```

3.10.33 info-center source channel

Function

The **info-center source channel** command configures a rule for outputting information to a channel.

The **undo info-center source channel** command deletes the rules for outputting information to a channel.

The following lists the default rule for outputting information to a channel.

Table 3-160 Default rule for outputting information to a channel

Output Channel	Module Enabled to Output Information	Log		Trap		Debugging Message	
		Status	Lowest Output Severity	Status	Lowest Output Severity	Status	Lowest Output Severity
0 (console)	default	on	warning	on	debugging	on	debugging
1 (remote terminal)	default	on	warning	on	debugging	on	debugging
2 (log host)	default	on	informational	on	debugging	off	debugging
3 (trap buffer)	default	off	informational	on	debugging	off	debugging
4 (log buffer)	default	on	warning	off	debugging	off	debugging
5 (SNMP agent)	default	Not supported	Not supported	on	debugging	Not supported	Not supported
6 (channel 6)	default	on	debugging	on	debugging	off	debugging
7 (channel 7)	default	on	debugging	on	debugging	off	debugging
8 (channel 8)	default	on	debugging	on	debugging	off	debugging
9 (channel 9)	default	on	debugging	on	debugging	off	debugging

Format

info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level** *severity* } * | **trap** { **state** { **off** | **on** } | **level** *severity* } * | **debug** { **state** { **off** | **on** } | **level** *severity* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

Parameters

Parameter	Description	Value
module-name	Specifies the module name.	Enumerated type. The value depends on the registered module.
default	Indicates the default module.	-
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.
log { **state** { **off** | **on** } }	Specifies the log status. - **off**: Logs are not sent. - **on**: Logs are sent. **NOTE** This field does not take effect for diagnostic logs.	-

Parameter	Description	Value
log { **level** *severity* }	Specifies the lowest severity of output logs. **NOTE** This field does not take effect for diagnostic logs.	Logs are classified into eight severities. The following severities are listed in descending order of priority: - emergencies - alert - critical - error - warning - notification - informational - debugging
trap { **state** { **off** | **on** } }	Specifies the trap status: - **off**: Traps are not sent. - **on**: Traps are sent.	-
trap { **level** *severity* }	Specifies the lowest severity of output traps.	Traps are classified into eight severities. The following severities are listed in descending order of priority: - emergencies - alert - critical - error - warning - notification - informational - debugging
debug { **state** { **off** | **on** } }	Specifies the debugging message status. - **off**: Debugging messages are not sent. - **on**: Debugging messages are sent.	-

Parameter	Description	Value
debug { **level** *severity* }	Specifies the lowest severity of output debugging messages.	Debugs are classified into eight severities. The following severities are listed in descending order of priority: - emergencies - alert - critical - error - warning - notification - informational - debugging

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect and query information generated on the Switch, define severities for various types of information that is output to different channels. You can run the **info-center source channel** command to configure a rule for outputting information to a channel.

The following lists information severities.

Table 3-161 Information severities

Value	Severity	Description
0	emergencies	A fault causes the device to fail to run normally unless it is restarted. For example, the device is restarted because of program exceptions or a memory error is detected.
1	alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.

Value	Severity	Description
2	critical	A fault needs to be analyzed and processed. For example, the memory usage falls below the lower threshold; temperature falls below the alarm threshold; BFD detects that a device is unreachable or detects locally generated error messages.
3	error	An improper operation is performed or exceptions occur during service processing. The fault does not affect services but needs to be analyzed. For example, users enter incorrect commands or passwords; error protocol packets are received from other devices.
4	warning	Some events or operations may affect device running or cause service processing faults, which requires full attention. For example, a routing process is disabled; BFD detects packet loss; error protocol packets are detected.
5	notification	A key operation is performed to keep the device running normally. For example, the **shutdown** command is run; a neighbor is discovered; protocol status changes.
6	informational	A normal operation is performed. For example, a **display** command is run.
7	debugging	A normal operation is performed, which requires no attention.

Precautions

Each information channel has a default record with the module name **default**. The default configuration for logs, traps, and debugging messages in different channels may differ.

If a module generates a large number of logs, traps, or debugging messages in a short time, use the following methods to suppress this information:

- Specify **level** *severity* to adjust the channel level. Information with lower severity will be filtered.
- Specify **state off** to disable information sent by a specified module.

NOTICE

After the lowest severity of output information is specified, information lower than the severity will be filtered.

Example

Enable the device to send debugging messages of the CFM module through the log host channel, and set the lowest severity of output debugging messages to warning.

```
<HUAWEI> system-view
[HUAWEI] info-center source CFM channel loghost debug level warning
```

3.10.34 info-center statistic-suppress enable

Function

The **info-center statistic-suppress enable** command enables suppression of statistics about consecutive repeated logs.

The **undo info-center statistic-suppress enable** command disables suppression of statistics about consecutive repeated logs.

The **info-center statistic-suppress disable** command disables suppression of statistics about consecutive repeated logs.

By default, suppression of statistics about consecutive repeated logs is enabled.

Format

info-center statistic-suppress enable

undo info-center statistic-suppress enable

info-center statistic-suppress disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the system, service modules generate logs and control the volume of generated logs. The information center processes the received logs.

A large number of repeated logs are generated in a short time in some scenarios, for example, when ARP and VRRP are enabled. This wastes both the storage space and CPU resources. Generally, users do not want to view the repeated logs. You can run the **info-center statistic-suppress enable** command to suppress statistics on consecutive repeated logs so that the system can still record other logs.

NOTE

Logs that are generated consecutively and with the identical log ID and parameters can be regarded as repeatedly generated logs.

Precautions

Statistics about repeatedly generated logs are first output at the 30th seconds from the time the first log is output, and then statistics about repeatedly generated logs are output at the 120th seconds. After being output two times, statistics about repeatedly generated logs are output every 600 seconds.

By default, once receiving a log, the information center outputs the log. If the information center receives repeatedly generated logs within a period, it outputs the number of these logs and will output logs only when it receives a new log (a log with a different log ID). For example, a module sends logs to the information center in the sequence of A1(T1) A2(T2) A3(T2) B1(T3) B2(T4) B3(T4) C1(T5) C2(T6) A4(T7) B4(T8) B5(T8) B5(T8) B7(T9) A5(T9) B8(T10) D1(T11) A6(T11) A7(T12) A8(T12) A9(T13) A10(T14) A11(T15) A12(T16) A13(T17) A14(T18) B9(T18). A1 to A14 are the same; B1 to B9 are the same; C1, C2 and D1 are different from others; T1 to T18 are sequence numbers. The log information output by the information center is as follows:

```
T1:A1
T3(1): last message repeated 2 times
T3:B1
T5: last message repeated 2 times
T5:C1
T6:C2
T7:A4
T8:B4
T9(1): last message repeated 3 times
T9:A5
T10:B8
T11:D1
T11:A6
T13(2): last message repeated 3 times
T18(2): last message repeated 5 times
T18:B9
```

Logs of the service module received by the information center show that:

- Statistics about repeatedly generated logs are output when either of the following conditions is met:
  - The next log is a different log, as shown in **(1)**.
  - The time period (every 30 seconds, 120 seconds, and 600 seconds) for outputting log statistics expires, as shown in **(2)**.
- Each time the statistics are output, the service module clears the count and starts counting again. For example, during the period from T11 to T18, log A is generated 9 times.
- The information center outputs logs in the same sequence the logs are generated, making the trace of information and scenario easy.

NOTE

Logs with the sequence being A B A B A B A B are alternate logs; therefore, the **info-center statistic-suppress enable** command is unable to suppression the statistics about these logs.

Example

Disable suppression of statistics about consecutive repeated logs.

```
<HUAWEI> system-view
[HUAWEI] undo info-center statistic-suppress enable
```

3.10.35 info-center timestamp

Function

The **info-center timestamp** command sets the timestamp format of logs, traps, and debugging messages.

The **undo info-center timestamp** command restores the default timestamp format of logs, traps, and debugging messages.

By default, the **date** timestamp is used in traps, logs and debugging messages. Debugging messages are accurate to milliseconds, and traps and logs are accurate to seconds.

Format

info-center timestamp { **debugging** | **log** | **trap** } { { **date** | **format-date** | **short-date** } [**precision-time** { **second** | **tenth-second** | **millisecond** }] | **boot** } [**without-timezone**]

undo info-center timestamp { **debugging** | **trap** | **log** }

Parameters

Parameter	Description	Value
debugging	Indicates debugging messages.	-
log	Indicates logs.	-
trap	Indicates traps.	-
boot	Indicates that the timestamp is expressed in the format of relative time, a period of time since the start of the system. The format is xxxxxx.yyyyyy. xxxxxx is the higher order 32 bits of the milliseconds elapsed since the start of the system; yyyyyy is the lower order 32 bits of the milliseconds elapsed since the start of the system.	-
date	Specifies the current date and time. It is expressed in mm dd yyyy hh:mm:ss format.	-
short-date	Indicates the short date. This timestamp differs from **date** is that the year is not displayed.	-
format-date	Indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format.	-
precision-time	Specifies the precision.	-

Parameter	Description	Value
second	Indicates that the precision is accurate to seconds.	-
tenth-second	Indicates that the precision is accurate to 0.1 second.	-
millisecond	Indicates that the precision is accurate to milliseconds.	-
without-timezone	Specifies a timestamp to filter timezone information. **NOTE** If **without-timezone** is configured for logs, traps, or debug information, the log, trap, or debugging information sent to the log host does not carry time zone or DST information.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The **info-center timestamp** command sets the timestamp format of logs, traps, and debugging messages.

The following describes the timestamp in **date** format.

Table 3-162 Description of fields of the timestamp in **date** format

Field	Description	Value
mm	Month	The value can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
dd	Date	1-31. If the date is smaller than 10, add a space in front of the date, For example, " 7".
yyyy	Year	4 digits
hh:mm:ss	Local time	hh ranges from 00 to 23, and mm or ss ranges from 00 to 59.

When the precision of the timestamp is accurate to 0.1 second or milliseconds, the system adds identifiers to the logs generated at the same time based on the sequence.

Prerequisites

The information center has been enabled by using the **info-center enable** command.

Example

Set the timestamp format of traps to **boot**.

```
<HUAWEI> system-view
[HUAWEI] info-center timestamp trap boot
```

Set the timestamp precision of logs, traps, and debugging messages.

```
<HUAWEI> system-view
[HUAWEI] info-center timestamp log date precision-time millisecond
[HUAWEI] info-center timestamp debugging date precision-time tenth-second
[HUAWEI] info-center timestamp trap date precision-time millisecond
```

3.10.36 info-center trapbuffer

Function

The **info-center trapbuffer** command enables the Switch to send traps to the trap buffer.

The **undo info-center trapbuffer** command disables the Switch from sending traps to the trap buffer.

By default, the Switch is enabled to send traps to the trap buffer.

Format

info-center trapbuffer

undo info-center trapbuffer

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To view traps in the trap buffer, run the **info-center trapbuffer** command to enable the Switch to send traps to the trap buffer.

The **info-center trapbuffer** command takes effect only after the information center function has been enabled using the **info-center enable** command.

Example

Enable the Switch to send traps to the trap buffer.

```
<HUAWEI> system-view
[HUAWEI] info-center trapbuffer
```

3.10.37 info-center trapbuffer size

Function

The **info-center trapbuffer size** command sets the maximum number of traps in the trap buffer.

The **undo info-center trapbuffer size** command restores the default maximum number of traps in the trap buffer.

By default, a trap buffer allows a maximum of 256 traps.

Format

info-center trapbuffer size *trapbuffer-size*

undo info-center trapbuffer size [*trapbuffer-size*]

Parameters

Parameter	Description	Value
trapbuffer-size	Specifies the maximum number of traps in the trap buffer.	The value is an integer that ranges from 0 to 1024. If *trapbuffer-size* is 0, traps are not displayed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **info-center trapbuffer size** command sets the maximum number of traps in the trap buffer.

Prerequisites

The Switch has been enabled to output traps to the trap buffer by using the **info-center trapbuffer** command.

Precautions

When you run the **info-center trapbuffer size** command multiple times, only the latest configuration takes effect.

If a small value of *trapbuffer-size* is used, some traps may be not displayed. If a large value of *trapbuffer-size* is used, repeated traps may be displayed. The default value of *trapbuffer-size* is recommended.

Example

Set the maximum number of traps in the trap buffer to 30.

```
<HUAWEI> system-view
[HUAWEI] info-center trapbuffer size 30
```

3.10.38 log restrain disable

Function

The **log restrain disable** command disables log restrainion.

The **undo log restrain disable** command enables log restrainion.

By default, log restrainion is enabled.

Format

log restrain disable

undo log restrain disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When a large number of logs are generated, device resources are wasted, affecting system performance. To prevent this problem, enable log restrainion.

Example

Disable log restrainion.

```
<HUAWEI> system-view
[HUAWEI] log restrain disable
```

3.10.39 log restrain threshold

Function

The **log restrain threshold** command sets the maximum number of logs that can be generated per minute.

The **undo log restrain threshold** command restores the default setting.

By default, a maximum of 200 logs can be generated per minute.

Format

log restrain threshold *threshold-value* [**infoid** *infoid-value* **description** *description-str*]

undo log restrain threshold [**infoid** *infoid-value*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the maximum number of logs that can be generated per minute.	The value is an integer that ranges from 10 to 50000.
infoid *infoid-value*	Specifies a log ID. If this parameter is specified, *threshold-value* specifies the maximum number of logs with the specified ID that can be generated per minute. If this parameter is not specified, *threshold-value* specifies the maximum number of logs that can be generated globally on the device per minute.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
description *description-str*	Specifies the description of the log with the sepecified ID.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

After log restrainion is enabled, if the number of logs generated per minute exceeds the specified threshold, excess logs are discarded.

You can run the **display log restrain all** command to check the configuration of the log suppression function. If the value of **MaxCount** in the command output is **NotLimit**, the log of the corresponding ID is not suppressed.

Example

Set the maximum number of logs that can be generated globally on the device per minute to 100.

```
<HUAWEI> system-view
[HUAWEI] log restrain threshold 100
```

3.10.40 reset info-center statistics

Function

The **reset info-center statistics** command clears statistics on each module.

Format

reset info-center statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect statistics on each module, run the **reset info-center statistics** command to clear all historical statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when you run the **reset info-center statistics** command.

Example

Clear statistics on each module.

```
<HUAWEI> reset info-center statistics
```

3.10.41 reset logbuffer

Function

The **reset logbuffer** command clears logs in the log buffer.

Format

reset logbuffer

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To record logs in the log buffer again, run the **reset logbuffer** command to clear all the information in the log buffer.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the **reset logbuffer** command.

Example

Clear information in the log buffer.

```
<HUAWEI> reset logbuffer
Warning: This command will reset the log buffer. Logs in the buffer will be lost. Continue? [Y/N]:y
```

3.10.42 reset log restrain statistics

Function

The **reset log restrain statistics** command clears all log suppression statistics.

Format

reset log restrain statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To clear all log suppression statistics, run this command.

Example

Clear all log suppression statistics.

```
<HUAWEI> reset log restrain statistics
```

3.10.43 reset trapbuffer

Function

The **reset trapbuffer** command clears Trap information in the trap buffer.

Format

reset trapbuffer

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To record traps in the trap buffer again, run the **reset trapbuffer** command to clear all the information in the trap buffer.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the **reset trapbuffer** command.

Example

Clear information in the trap buffer.

```
<HUAWEI> reset trapbuffer
```

3.10.44 save logfile

Function

The **save logfile** command saves logs in the user log file buffer to a user log file.

Format

save logfile

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The system periodically saves log information in the user log buffer to a user log file. If the log buffer becomes full within the log saving interval, the system immediately saves logs to the user log file. To view the current logs, run the **save logfile** command to save the logs to the user log file.

When you run this command, the device obtains or uses some personal data of users, such as the STA MAC address. Delete the personal data immediately after the command is executed to ensure user data security.

Example

Save logs in the user log file buffer to the user log file.

```
<HUAWEI> save logfile
Info: Save logfile successfully.
```

3.10.45 save logfile all

Function

The **save logfile all** command saves the logs in the user log buffer area and diagnostic log buffer area to the user log file and diagnostic log file, respectively.

Format

save logfile all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The logs in the user log buffer area and diagnostic log buffer area are periodically saved to the user log file and diagnostic log file, respectively. The log saving interval varies with the product. To save the logs in the user log buffer area and diagnostic log buffer area to the user log file and diagnostic log file, respectively, run the **save logfile all** command.

A user log file is saved in a log directory (for example, the **log** or **logfile** directory) and named in the **log.log** format.

A diagnostic log file is saved in a log directory (for example, the **log** or **logfile** directory) and named in the **log.dblg** format.

Example

Save the logs in the user log buffer area and diagnostic log buffer area to the user log file and diagnostic log file, respectively.

```
<HUAWEI> save logfile all
Info: Save logfile successfully.
Info: Save diagnostic logfile successfully.
```

3.10.46 terminal debugging

Function

The **terminal debugging** command enables debugging message display on the user terminal.

The **undo terminal debugging** command disables debugging message display on the user terminal.

By default, debugging message display is disabled on the user terminal.

Format

terminal debugging

undo terminal debugging

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **terminal debugging** command to enable debugging message display on the user terminal to view system debugging message and locate faults.

Prerequisites

The **terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Enable debugging message display on the user terminal.

```
<HUAWEI> terminal debugging
Info: Current terminal debugging is on.
```

3.10.47 terminal echo synchronous

Function

The **terminal echo synchronous** command enables a terminal to display debugging, log, or trap information synchronously.

The **undo terminal echo synchronous** command disables a terminal from displaying debugging, log, or trap information synchronously.

By default, a terminal displays debugging, log, and trap information asynchronously.

Format

terminal echo synchronous [**level** { *severity* | **all** } | **size** *size-number*] *

undo terminal echo synchronous

Parameters

Parameter	Description	Value
level *severity*	Specifies an information severity.	The value is an integer ranging from 0 to 7. The default value is **0**. The information center classifies information into the following severities: - 0: emergency - 1: alert - 2: critical - 3: error - 4: warning - 5: notice - 6: informational - 7: debug A smaller value indicates a higher severity. The information with a severity higher than a specified severity is displayed asynchronously.
all	Displays information of all severities.	-
size *size-number*	Specifies the total number of debugging, log, and trap records.	The value is an integer ranging from 1 to 1024. The default value is **512**.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a device generates debugging, log, or trap information, the information queues in the device process and is sent to a terminal sequentially. This output is called a synchronous output.

A synchronous output provides effectively organized output information, improving user experience. In asynchronous output mode, multiple types of information interlaces, which brings poor readability. An asynchronous output allows you to promptly obtain debugging and diagnosis information and therefore applies to debugging and diagnosis scenarios.

You can run the **terminal echo synchronous** command to enable a synchronous output on a terminal, facilitating subsequent operations.

- When you enter a command, the entered command content is displayed after debugging, log, or trap information is displayed. This function is enabled by default. After a synchronous output is disabled, this function is still supported.
- When no command is entered, the command prompt is displayed after debugging, log, or trap information is displayed. This function is enabled by default. After a synchronous output is disabled, this function is still supported.
- When a command is being run, no debugging, log, or trap information is displayed. After the command is run, debugging, log, or trap information is displayed.
- When you enter **Y** for the message "Are you sure to continue?[Y/N]," the **[Y/N]:** prompt is displayed after debugging, log, or trap information is displayed.
- When you enter the More phase, the **More** prompt is displayed after debugging, log, or trap information is displayed.
- If you run a command, for example, for decompressing or saving a file, the terminal does not display output information until the operation is complete. This process ensures monitoring continuity.

Prerequisites

- Terminal display has been enabled using the **terminal monitor** command.
- The terminal has been enabled to display debugging, log, or trap information using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Example

Enable a terminal to display debugging information synchronously.

```
<HUAWEI> terminal monitor
Info: Current terminal monitor is on.
<HUAWEI> terminal debugging
Info: Current terminal debugging is on.
<HUAWEI> terminal echo synchronous
Info: Current terminal synchronization is on.
<HUAWEI> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]:
Aug 23 2012 12:04:37.790.2 huawei VTY/7/Debug_Stat:
 (0)VTY ACCEPT BEGIN !
Aug 23 2012 12:04:37.790.3 huawei VTY/7/Debug_Stat:
 (1)SOCKET ACCEPT OK !
Aug 23 2012 12:04:37.790.4 huawei VTY/7/Debug_Stat:
 (2)FIND LINE INDEX OK !
[Y/N]:
```

3.10.48 terminal logging

Function

The **terminal logging** command enables log display on the user terminal.

The **undo terminal logging** command disables log display on the user terminal.

By default, log display is enabled on the user terminal.

Format

terminal logging

undo terminal logging

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view logs on a terminal, run the **terminal logging** command to enable log display on the user terminal.

Prerequisites

The **terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Disable log display on the user terminal.

```
<HUAWEI> undo terminal logging
Info: Current terminal logging is off.
```

3.10.49 terminal monitor

Function

The **terminal monitor** command enables display of logs, traps, and debugging message output by the information center on the user terminal.

The **undo terminal monitor** command disables display of logs, traps, and debugging message output by the information center on the user terminal.

By default, console display is enabled and terminal display is disabled.

Format

terminal monitor

undo terminal monitor

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Prerequisites

The information center has been enabled by using the **info-center enable** command.

Follow-up Procedure

Run the **terminal debugging**/**undo terminal debugging**, **terminal logging**/**undo terminal logging**, **terminal trapping**/**undo terminal trapping**/ command to enable or disable terminal debugging message, log, or trap display.

Precautions

Logs, traps, and debugging message are sent to the current terminal only when the **terminal monitor** command is used.

Running the **undo terminal monitor** command is equivalent to running the **undo terminal debugging**, **undo terminal logging**, **undo terminal trapping** command.

Example

Disable display of logs, traps, and debugging message output by the information center on the user terminal.

```
<HUAWEI> undo terminal monitor
Info: Current terminal monitor is off.
```

3.10.50 terminal session-log disable

Function

The **terminal session-log disable** command disables the session logging function for an online user.

The **undo terminal session-log disable** command enables the session logging function for an online user.

By default, the session logging function for an online user is enabled.

Format

terminal session-log disable

undo terminal session-log disable

Parameters

None

Views

User view

Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The session logging function for an online user stores the user input, device output, and time when the device executes user-issued commands to a session log file.

Prerequisites

The session logging function has been enabled globally.

Example

Enable the session logging function for an online user.

```
<HUAWEI> undo terminal session-log disable
```

3.10.51 terminal trapping

Function

The **terminal trapping** command enables trap display on the user terminal.

The **undo terminal trapping** command disables trap display on the user terminal.

By default, trap display is enabled on the user terminal.

Format

terminal trapping

undo terminal trapping

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view traps on a terminal, run the **terminal trapping** command to enable trap display on the user terminal.

Prerequisites

The **terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Disable trap display on the user terminal.

```
<HUAWEI> undo terminal trapping
Info: Current terminal trapping is off.
```

3.11 Fault Management Commands

3.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.11.2 alarm (system view)

Function

Using the **alarm** command, you can enter the alarm view.

Format

alarm

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After running the **alarm** command to enter the alarm view, you can configuration alarm management functions.

Example

Enter the alarm view.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm]
```

3.11.3 alarm-name severity

Function

The **alarm-name severity** command sets the severity for an alarm.

The **undo alarm-name severity** command restores the default setting.

By default, each alarm has a default severity.

Format

alarm-name *alarm-name* **severity** *severity*

undo alarm-name *alarm-name* **severity**

Parameters

Parameter	Description	Value
alarm-name	Specifies the registered alarm name.	The value is a string and varies according to the registered device type. To view registered alarm information, run the **display alarm information** command.

Parameter	Description	Value
severity *severity*	Specifies the alarm severity.	The value is of enumerated type. Alarms are classified into the following severities: • **critical**: indicates that a fault affecting services has occurred and it must be rectified immediately. • **major**: indicates that services are being affected and related measures need to be taken urgently. • **minor**: indicates that a fault occurs but does not affect services. To avoid more serious faults that affect services, related measures must be taken. • **warning**: indicates that a potential or impending service-affecting fault is detected before any significant effect has been felt. Take corrective actions to diagnose and rectify the fault. • **indeterminate**: indicates that the alarm severity cannot be determined. • **cleared**: indicates one or more previous alarm conditions have been cleared.

Views

Alarm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **alarm-name severity** command to raise or lower the level of an alarm based on the severity and emergency of the alarm. However, the level of a clear alarm cannot be changed unless during the configuration restoration period. You can configure filtering conditions to allow the NMS to receive only alarms of specified alarm severity.

Precautions

The default severity of each alarm is different. To view the default severity of an alarm, run the **undo alarm-name severity** and **display alarm information** commands in sequence.

Example

Set the severity of the hwSysSlaveHDError alarm to warning.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] alarm-name hwSysSlaveHDError severity warning
```

3.11.4 clear alarm active

Function

The **clear alarm active** command clears active alarms.

Format

clear alarm active { **all** | **sequence-number** *sequence-number* }

Parameters

Parameter	Description	Value
all	Clears all active alarms.	-
sequence-number *sequence-number*	Specifies the sequence number of an active alarm.	The value is an integer ranging from 1 to 2147483647.

Views

Alarm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on alarms generated on the device again, run the **clear alarm active** to clear active alarms.

Precautions

After the **clear alarm active** command is used, all active alarms on the device are deleted and cannot be restored.

Example

Clear all active alarms on the device.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] clear alarm active all
```

3.11.5 clear alarm manual-clear

Function

The **clear alarm manual-clear** command clears the active alarms that are not reported repeatedly so that these active alarms can be reported again.

Format

clear alarm manual-clear { **all** | **sequence-number** *sequence-number* }

Parameters

Parameter	Description	Value
all	Specifies all the active alarms that are not reported repeatedly.	-
sequence-number *sequence-number*	Specifies the sequence number of the active alarm that is not reported repeatedly. You can run **display alarm manual-clear** get the sequence number of the active alarm.	The value is an integer that ranges from 1 to 2147483647.

Views

Alarm management view

Default Level

3: Management level

Usage Guidelines

After the **mask manual-clear alarm** command is executed to prevent manually cleared active alarms from being reported repeatedly and then the **clear alarm**

active command or MIB table hwAlarmActiveTable is used to manually clear active alarms, active alarms will not be reported repeatedly. To view the active alarms that are not reported repeatedly, run the **clear alarm manual-clear** command.

To ensure that the active alarms that are not reported repeatedly can be reported again, run the **clear alarm manual-clear** command. After the **clear alarm manual-clear** command is executed, running the **display alarm manual-clear** command does not display corresponding alarm information.

Example

Clear the active alarms that are not reported repeatedly.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] clear alarm manual-clear all
```

3.11.6 clear event all

Function

The **clear event all** command clears events on the device.

Format

clear event all

Parameters

None

Views

Event view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on events generated on the device again, run the **clear event all** to clear events.

Precautions

NOTICE

The **clear event all** command clears events on the device and cleared events cannot be restored.

Example

Clear events on the device.

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event] clear event all
```

3.11.7 clear record device-alarm

Function

The **clear record device-alarm** command clears hardware alarms.

Format

clear record device-alarm [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Clears all hardware alarms of the device.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

When current hardware alarms are not required on the device, use the **clear record** command to clear the hardware alarms of the device.

Example

Clear all hardware alarms of the device.

```
<HUAWEI> clear record device-alarm all
```

3.11.8 delay-suppression enable

Function

The **delay-suppression enable** command enables delayed alarm or event reporting.

The **undo delay-suppression enable** command disables delayed alarm or event reporting.

By default, delayed reporting is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-suppression enable

undo delay-suppression enable

Parameters

None

Views

Alarm view or event view

Default Level

3: Management level

Usage Guidelines

In the event that an alarm or an event is repeatedly generated, you can enable delayed reporting to prevent a large number of repeated alarms or events from being reported to the NMS. You can choose to enable or disable delayed reporting:

- Run the **delay-suppression enable** command to enable delayed reporting.
- Run the **undo delay-suppression enable** command to disable delayed reporting.

Run the **delay-suppression enable** command in the alarm view to enable delayed alarm reporting. Run the **delay-suppression enable** command in the event view to enable delayed event reporting.

Example

Enable delayed alarm reporting.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] delay-suppression enable
```

3.11.9 display alarm active

Function

The **display alarm active** command displays active alarms on the device.

Format

display alarm active

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display alarm active** command to view active alarms on the device to locate faults.

Example

Display active alarms on the device.

```
<HUAWEI> display alarm active
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|
nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason
info)
J=RootCause alarm sequence(Only for nonRootCause
alarm)

  92/Independent/2019-08-09 10:44:58/-/0x502001/linkDown/Critical/Start/OID 1.3.6.1.6.3.1.1.5.3 Interface
58 turned into DOWN state.
(AdminStatus=1,OperStatus=2,InterfaceName=40GE0/0/5)
```

Table 3-163 Description of the display alarm active command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Sequence number
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: ● Independent: indicates an alarm for which alarm correlation analysis is not performed. ● RootCause: indicates a root-cause alarm. ● nonRootCause: indicates a non-root-cause alarm.

Item	Description
C=Generating time	Time when an alarm is generated
D=Clearing time	Time when an alarm is cleared
E=ID	Alarm ID
F=Name	Alarm name
G=Level	Alarm severity level You can run the **alarm-name severity** command to set this parameter.
H=State	Alarm status: ● Start ● End
I=Description information for locating(Para info, Reason info)	Alarm description including alarm parameters and causes for triggering alarms
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm (for non-root-cause alarms only)

3.11.10 display alarm history

Function

The **display alarm history** command displays historical alarms on the device.

Format

display alarm history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display alarm history** command to view the alarms that are cleared or generated on the device. The **display alarm history** command displays a maximum of 300 alarm history records.

Example

Display historical alarms on the device.

```
<HUAWEI> display alarm history
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  3/Independent/2010-07-14 09:40:20-08:00/2010-07-14 09:40:23-08:00/0x502001/linkDown/
Critical/End/OID 1.3.6.1.6.3.1.1.5.3 Interface 5 turned into DOWN state.
```

Table 3-164 Description of the display alarm history command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Sequence number
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: ● Independent: indicates an alarm for which alarm correlation analysis is not performed. ● RootCause: indicates a root-cause alarm. ● nonRootCause: indicates a non-root-cause alarm.
C=Generating time	Time when an alarm is generated
D=Clearing time	Time when an alarm is cleared
E=ID	E=ID
F=Name	Alarm ID
G=Level	Alarm severity level You can run the **alarm-name severity** command to set this parameter.

Item	Description
H=State	Alarm status: - Start - End
I=Description information for locating(Para info, Reason info)	Alarm description including alarm parameters and causes for triggering alarms
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm

3.11.11 display alarm information

Function

The **display alarm information** command displays alarm configurations.

Format

display alarm information [**name** *alarm-name*]

Parameters

Parameter	Description	Value
name *alarm-name*	Displays the configuration of a specified alarm. If this parameter is not set, configurations of all alarms are displayed.	The value is a string and varies according to the registered device type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view alarm configurations on the device, run the **display alarm information** command.

If no alarm name is specified, information about all alarms in the system will be displayed.

In addition, to change the severity level of an alarm, you can run the **alarm-name** *alarm-name* **severity** *severity* command.

Example

Display the configuration of the alarm named linkUp.

```
<HUAWEI> display alarm information name linkUp
**********************************
  AlarmName: linkUp
  AlarmType: Resume Alarm
  AlarmLevel: Cleared
  Suppress Period: NA
  CauseAlarmName: linkDown
  Match VB Name: ifIndex
**********************************
```

Table 3-165 Description of the display alarm information command output

Item	Description
AlarmName	Name of an alarm.
AlarmType	Alarm type: ● Alarm: indicates a fault occurs. ● Resume Alarm: indicates a fault is rectified.
AlarmLevel	Alarm severity. To set this parameter, run the **alarm-name severity** command.
Suppress Period	Alarm reporting delay. To set this parameter, run the **suppression alarm-name** command. If this field displays **NA**, this alarm does not support the delayed alarm reporting function.
CauseAlarmName	Name of the root-cause alarm. Name of the root-cause alarm, namely, paired alarm name.
Match VB Name	Matching content of paired alarms.

3.11.12 display alarm manual-clear

Function

The **display alarm manual-clear** command displays the alarms that are not reported repeatedly after being cleared.

Format

display alarm manual-clear

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **mask manual-clear alarm** command is executed to prevent manually cleared active alarms from being reported repeatedly and then the **clear alarm active** command or MIB table hwAlarmActiveTable is used to manually clear active alarms, you can run the **display alarm manual-clear** command to view the active alarms that are not reported repeatedly after being cleared.

Example

Display the alarms that are not reported repeatedly after being cleared.

```
<HUAWEI> display alarm manual-clear
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  2/Independent/2016-05-04 10:38:46-08:00/-/0xff14280c/hwEntityOffline/Major/Start/ OID 1
.3.6.1.4.1.2011.5.25.129.2.1.13 Physical entity changed to the offline state. (E
ntityPhysicalIndex=16842752, BaseTrapSeverity=5, BaseTrapProbableCause=69120, Ba
seTrapEventType=5, EntPhysicalContainedIn=16777216, EntPhysicalName="LPU slot 1"
, RelativeResource="", ReasonDescription="Because of get offline message, the en
tity of SLOT1 changed to offline state")
```

Table 3-166 Description of the **display alarm manual-clear** command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Alarm sequence number.

Item	Description
B=RootKindFlag(Independent| RootCause| nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: - Independent: indicates an alarm for which alarm correlation analysis is not performed. - RootCause: indicates a root-cause alarm. - nonRootCause: indicates a non-root-cause alarm.
C=Generating time	Time when an alarm is generated.
D=Clearing time	Time when an alarm is cleared.
E=ID	Alarm ID.
F=Name	Alarm name.
G=Level	Alarm severity. To set this parameter, run the **alarm-name severity** command.
H=State	Alarm status: - Start - End
I=Description information for locating(Para info, Reason info)	Alarm description.
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of a root-cause alarm (for non-root-cause alarms only)

3.11.13 display alarm urgent

Function

Using the **display alarm urgent** command, you can view hardware alarms on the device.

Format

display alarm urgent [**slot** *slot-id* | **time** *interval*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
time *interval*	Displays hardware alarms generated in the last period of time. *interval* specifies the period.	The value is an integer that ranges from 1 to 10000, in minutes.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the command to view hardware alarms, including alarms about the abnormality of the temperature, the fan, and the chip.

If no parameter is specified, the command displays all the hardware alarms.

Example

Display hardware alarms of the device.

```
<HUAWEI> display alarm urgent
 Alarm:

Alarm                 Slot      Date        Time(DST)      Location
-------------------------------------------------------------------------
Temp normal             1         2000/04/09  04:52:47      Slot 1
Temp low              1         2000/04/09  04:52:14      Slot 1
Temp normal             1         2000/04/09  04:39:05      Slot 1
Temp high             1         2000/04/09  04:37:23      Slot 1
Temp normal             2         2000/04/10  07:13:16      Slot 2
Temp high             2         2000/04/10  07:11:22      Slot 2
```

Table 3-167 Description of the display alarm urgent command output

Item	Description
Alarm	Details about an alarm. - Fan pulled out: A fan module is removed. - Fan plugged in: A fan module is installed. - Fan abnormal: A fan module is not working properly. - Fan normal: A fan module is working properly. - Fan unmatched: A fan module does not match the device model. - Fan matched: A fan module matches the device model. - Power pulled out: A power module is removed. - Power plugged in: A power module is installed. - Power abnormal: A power module is not working properly. - Power normal: A power module is working properly. - PWR Input Vol Low: A power module is in an input power outage or undervoltage condition. - PWR Input Vol Low Resume: A power module recovers from an input power outage or undervoltage condition. - Built-in power Off: A built-in power module does not provide power. - Built-in power On: A built-in power module provides power normally. - Temp high: The temperature is too high. - Temp low: The temperature is too low. - Temp normal: The temperature returns to the normal range. - Temp chip abnormal: A temperature sensor is faulty. - Temp chip normal: A temperature sensor recovers from a failure. - storage abnormal: The storage utilization exceeded 85%.
Slot	Slot ID of the device where alarms are generated.
Date	Date when alarms are generated.
Time(DST)	Time when alarms are generated.
Location	Position where alarms are generated.

3.11.14 display event

Function

The **display event** command displays events on the device.

Format

display event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To obtain the contents of events in the system, you can run the display event command.

Example

Display events on the device.

```
<HUAWEI> display event
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2008-10-12 22:42:28-08:00/-/0x40812000/warmStart/Warning/Start/O
ID 1.3.6.1.6.3.1.1.5.2 warmStart
  2/Independent/2008-10-12 22:42:28-08:00/-/0x41132002/hgmpMemberStatusChange/Wa
rning/Start/OID:1.3.6.1.4.1.2011.6.7.1.0.3, DeviceID:0018-8201-0987, Role:17.
  3/Independent/2008-10-16 17:50:32-08:00/-/0x41b82000/hwCfgChgNotify/Warning/St
art/OID 1.3.6.1.4.1.2011.5.25.191.3.1 configurations have been changed. The curr
ent change number is 2, the change loop count is 0, and the maximum number of re
cords is 4095.
```

Table 3-168 Description of the display event command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Event display format
A=Sequence	Sequence number of an event

Item	Description
B=RootKindFlag(Independent| RootCause| nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm (The value of this field is **Independent** for any event.)
C=Generating time	Time when the event is generated
D=Clearing time	Time when the event is cleared (for non-root-cause alarms only)
E=ID	Event ID
F=Name	Event name
G=Level	Event level
H=State	Event status: ● Start ● End
I=Description information for locating(Para info, Reason info)	Description of an event, including parameters of the event and the reason why the event was triggered.
J=RootCause alarm sequence(Only for nonRootCause alarm)	This parameter is valid only for alarms.

3.11.15 display event information

Function

The **display event information** command displays event configurations.

Format

display event information [**name** *event-name*]

Parameters

Parameter	Description	Value
name *event-name*	Displays the configuration of a specified event. If this parameter is not set, configurations of all events are displayed.	The value is a string and varies according to the registered device type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view event configurations on the device, run the **display event information** command.

If no event name is specified, information about all events in the system will be displayed.

Example

Display registration information about the hwCfgManEventlog event.

```
<HUAWEI> display event information name hwCfgManEventlog
***********************************
  EventName: hwCfgManEventlog
  EventType: Critical Event
  EventLevel: Warning
  Suppress Period: NA
  Match VB Name: hwCfgLogSrcCmd hwCfgLogSrcData hwCfgLogDesData
***********************************
```

Table 3-169 Description of the display event information command output

Item	Description
EventName	Event name.
EventType	Event type.
EventLevel	Event level, which cannot be configured.
Suppress Period	Event report delay period. To set this parameter, run the **suppression event-name** command. If this field displays **NA**, this event does not support the delayed event reporting function.
Match VB Name	Matching content of repeated events.

3.11.16 event

Function

Using the **event** command, you can enter the event view.

Format

event

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After running the **event** command to enter the event view, you can configure event management functions.

Example

Enter the event view.

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event]
```

3.11.17 mask manual-clear alarm

Function

The **mask manual-clear alarm** command prevents manually cleared active alarms from being reported repeatedly.

The **undo mask manual-clear alarm** command restores the default configuration.

By default, active alarms are reported repeatedly after being manually cleared.

Format

mask manual-clear alarm

undo mask manual-clear alarm

Parameters

None

Views

Alarm management view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, after the **clear alarm active** command or MIB table hwAlarmActiveTable is used to manually clear active alarms, active alarms are reported repeatedly when being generated again. To prevent manually cleared active alarms from being reported repeatedly, run the **mask manual-clear alarm** command.

After the **mask manual-clear alarm** command is executed and then the **clear alarm active** command or MIB table hwAlarmActiveTable is used, cleared active alarms will not be reported repeatedly before clear alarms of active alarms are reported. To view all the active alarms that are not reported repeatedly, run the **display alarm manual-clear** command.

Precautions

Before the **mask manual-clear alarm** command is executed, the active alarms manually cleared using the **clear alarm active** command or MIB table hwAlarmActiveTable will be reported repeatedly.

Example

Prevent manually cleared active alarms from being reported repeatedly.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] mask manual-clear alarm
```

3.11.18 reset alarm urgent

Function

The **reset alarm urgent** command clears all alarm messages.

Format

reset alarm urgent slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **reset alarm urgent** command to clear all alarm messages. Confirm the action before you run this command.

Example

Clear all alarm messages of the device that slot id is 0.

```
<HUAWEI> system-view
[HUAWEI] reset alarm urgent slot 0
```

3.11.19 set alarm resend interval

Function

The **set alarm resend interval** command set the alarm reporting interval.

The **undo set alarm resend interval** command restores the default alarm reporting interval.

By default, the alarm interval is 10 minutes.

Format

set alarm resend interval *interval-value*

undo set alarm resend interval

Parameters

Parameter	Description	Value
interval-value	Specifies the alarm interval.	The value is an integer that ranges from 0 to 65535, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **set alarm resend interval** command sets the interval at which alarms are generated. If the periodic alarm reporting function is not required, set the interval to 0.

Precautions

If the alarm reporting interval is set to 0, the system does not report alarms periodically.

Example

Set the alarm reporting interval to 4 minutes.

```
<HUAWEI> system-view
[HUAWEI] set alarm resend interval 4
```

3.11.20 suppression alarm-name

Function

The **suppression alarm-name** command modifies a delay period after which a generated alarm is reported.

The **undo suppression alarm-name** command restores the configured delay period after which a generated alarm is reported.

By default, the system defines a delay period after which a generated alarm is reported. To view this default delay period, run the **undo suppression alarm-name** command and then the **display alarm information** command. If the **Suppress Period** field displays NA for an alarm, this alarm does not support the delayed alarm reporting function.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

suppression alarm-name *alarm-name* { **cause-period** *cause-seconds* | **clear-period** *clear-seconds* }

undo suppression alarm-name *alarm-name* { **cause-period** | **clear-period** }

Parameters

Parameter	Description	Value
alarm-name	Specifies the name of an alarm for which the delay period is set.	The value cannot be the alarm name of which the **Suppress Period** field in the **display alarm information** command output displays NA.
cause-period *cause-seconds*	Specifies the period after which a generated alarm is reported.	The value is an integer ranging from 0 to 600, in seconds. If the value is set to 0s, the alarm management module sends the alarm to the NMS without any delay.
clear-period *clear-seconds*	Specifies the period after which a generated clear alarm is reported.	The value is an integer ranging from 0 to 600, in seconds. If the value is set to 0s, the alarm management module sends the alarm to the NMS without any delay.

Views

Alarm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a certain alarm is repeatedly generated, you can enable delayed alarm reporting and set a period after which the alarm is reported to prevent the alarm from being reported during this period.

After the period is set for a certain alarm:

- If no clear alarm is generated during the period, the alarm is not reported to the NMS until the period expires.
- If a clear alarm is generated during this period, the alarm and its clear alarm are both deleted from the alarm queue and will not be reported to the NMS.

If the delay period is too short, alarm reporting is not efficiently delayed. If the delay period is too long, alarm reporting is postponed and the time when the fault occurs cannot be correctly obtained. For most alarms, the default delay period is recommended. For common alarms, such as alarms about hardware and environment, delayed alarm reporting is not recommended.

The value of **cause-period** *cause-seconds* is irrelevant to the value of **clear-period** *clear-seconds*. The delay in reporting an alarm and the delay in reporting a clear alarm can be configured separately.

Prerequisites

Before running the **suppression alarm-name** command, ensure that delayed alarm reporting has been enabled using the **delay-suppression enable** command.

Precautions

- If the delay period is changed when an alarm is being sent, the changed delay period takes effect on the next alarm to be sent.
- If *alarm-name* specifies an alarm, you can configure only **cause-period** *cause-seconds*. If it specifies a clear alarm, you can configured only **clear-period** *clear-seconds*.

Example

Set the hwsysmasterhderror alarm to be reported 5s after it is generated.

```
<HUAWEI> system-view
[HUAWEI] alarm
[HUAWEI-alarm] delay-suppression enable
[HUAWEI-alarm] suppression alarm-name hwsysmasterhderror cause-period 5
```

3.11.21 suppression event-name

Function

The **suppression event-name** command modifies a delay period after which a generated event is reported.

The **undo suppression event-name** command restores the configured delay period after which a generated event is reported.

By default, the system defines a delay period after which a generated event is reported. To view this default delay period, run the **undo suppression event-name** command and then the **display event information** command. If the **Suppress Period** field displays NA for an alarm, this alarm does not support the delayed alarm reporting function.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

suppression event-name *event-name* **period** *seconds*

undo suppression event-name *event-name* **period**

Parameters

Parameter	Description	Value
event-name	Specifies the name of an event for which the delay period is set.	The value cannot be the event name of which the **Suppress Period** field in the **display event information** command output displays NA.
period *seconds*	Specifies the period after which a generated event is reported.	The value is an integer ranging from 0 to 600, in seconds. If the value is set to 0s, the alarm management module sends the event to the NMS without any delay.

Views

Event view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the case where a certain event is repeatedly generated, you can enable delayed event reporting and set a period after which a generated event is reported.

After the delay period is set for a certain event, if an event is generated several times during the delay period, the system reports only the first one to the NMS when the delay period expires and discards the following ones.

Prerequisites

Before running the **suppression event-name** command, ensure that delayed alarm reporting has been enabled using the **delay-suppression enable** command.

Precautions

If the delay period is changed when an event is being sent, the changed delay period takes effect on the next event to be sent.

Example

Set the delay period to 5s after which a generated hwFlhSyncFailNotification event is reported.

```
<HUAWEI> system-view
[HUAWEI] event
[HUAWEI-event] delay-suppression enable
[HUAWEI-event] suppression event-name hwFlhSyncFailNotification period 5
```

3.12 SAID Configuration Commands

3.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.12.2 display said-node brief

Function

The **display said-node brief** command displays brief information about SAID nodes.

Format

display said-node { **all** | *said-name* } **brief** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Indicates all SAID nodes.	-
said-name	Specifies an SAID node.	The value depends on the device configuration.
slot *slot-id*	Specifies a slot ID. If no slot ID is specified, this command displays brief information about SAID nodes on the active MPU.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display said-node brief** command to view brief information about all supported SAID nodes for fault location.

Example

Display brief information about the SAID node named **mac** in slot 2.

```
<HUAWEI> display said-node mac brief slot 2
------------------------------------------------------------------------------------------
Node  Node            Type    Cycle  Enable   Active      Inactive Reason
ID    Name                    (s)    Status   Status
------------------------------------------------------------------------------------------
2     mac             Restore 1      Enable   Active      -
------------------------------------------------------------------------------------------
```

Table 3-170 Description of the **display said-node brief** command output

Item	Description
Node ID	ID of an SAID node.
Node Name	Name of the SAID node.
Type	Type of the SAID node: ● Detect: diagnostic node ● Restore: self-healing node
Cycle(s)	Detection period of the SAID node, in seconds.
Enable Status	Whether the SAID node is enabled: ● Enable: The SAID node is enabled. ● Disable: The SAID node is disabled.
Active Status	Running status of the SAID node: ● Active: The SAID node is running. ● Inactive: The SAID node is not running.
Inactive Reason	Whether the SAID node is activated: ● -: The SAID node is enabled and activated. ● Node disabled: The SAID node is not activated.

3.12.3 set said-node disable

Function

The **set said-node disable** command disables SAID nodes.

The **undo set said-node disable** command enables SAID nodes.

By default, all SAID nodes are enabled.

Format

set said-node { **all** | *said-name* &<1-6> } **disable**

undo set said-node { **all** | *said-name* &<1-6> } **disable**

Parameters

Parameter	Description	Value
all	Indicates all SAID nodes.	-
said-name	Specifies an SAID node.	The value depends on the device configuration. A maximum of six SAID nodes can be configured at a time. If you need to configure more than six SAID nodes, run the **set said-node disable** command multiple times.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The System of Active Immunization and Diagnosis (SAID) is an intelligent fault diagnosis system that automatically diagnoses and rectifies some faults by simulating human operations in troubleshooting. The SAID system has multiple SAID nodes, which detect, diagnose, and rectify faults of multiple modules. However, if a node processes a large number of services, the processing efficiency of other nodes is affected. In this case, run this command disable this node.

Currently, the switch supports the following SAID nodes listed in **Table 3-171**.

Table 3-171 Supported SAID nodes

Node Name	Node Type
FLASH-WRITE	Diagnostic node
MAC	Self-healing node
STG	Self-healing node

Node Name	Node Type
PORT	Self-healing node
VLAN	Self-healing node
SE-REG **NOTE** Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S support this node.	Self-healing node
SE-TABLE **NOTE** Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S support this node.	Self-healing node
CONFD-MEMORY	Self-healing node
PING	Diagnostic node After this node is enabled, the device periodically sends ICMP ping packets.

Precautions

If some cards do not support a specific SAID node and no cards that support this SAID node are installed on the device, the device displays a message, indicating that the device does not support this SAID node.

Example

Disable the SAID nodes **mac** and **stg**.

```
<HUAWEI> system-view
[HUAWEI] set said-node mac stg disable
```

Disable all SAID nodes.

```
<HUAWEI> system-view
[HUAWEI] set said-node all disable
```

3.13 NTP Configuration Commands

3.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

3.13.2 display ntp-service event clock-unsync

Function

The **display ntp-service event clock-unsync** command displays the last 10 clock unsynchronization reasons.

Format

display ntp-service event clock-unsync

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ntp-service event clock-unsync** command to view information about the last 10 clock unsynchronization reasons in the current system.

Example

Display the last 10 clock unsynchronization reasons.

```
<HUAWEI> display ntp-service event clock-unsync
 1. Clock source   :  10.1.1.1(vrf1)
    Session type   :  client, configured
    Unsync reason  :  Peer reachability lost
    Unsync time    :  2012-07-30 12:24:44+00:00

 2. Clock source   :  10.2.1.1(vrf2)
    Session type   :  bdcast client (Interface: GE0/0/1), dynamic
    Unsync reason  :  Authentication failure
    Unsync time    :  2011-06-15 11:24:44+00:0
```

Display the clock unsynchronization reasons.

Table 3-172 Description of the **display ntp-service event clock-unsync** command output

Item	Description
Clock source	Indicates the IP address of the server clock.

Item	Description
Session type	Indicates the session type of the server clock.
Unsync reason	Indicates the unsynchronization reasons.
Unsync time	Indicates the unsynchronization time.

3.13.3 display ntp-service sessions

Function

The **display ntp-service sessions** command displays all session information maintained by NTP on the local end.

Format

display ntp-service sessions [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about an NTP session. If **verbose** is not specified, only summary information about the NTP session is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor or locate faults on NTP sessions, run the **display ntp-service sessions** command to obtain status information about NTP sessions so that the fault can be located efficiently.

Precautions

- If **verbose** is not specified, summary information about NTP sessions is displayed.

- If **verbose** is specified, detailed information about NTP sessions is displayed.

Example

Display NTP session information of the local device.

```
<HUAWEI> display ntp-service sessions
 clock source: 224.0.1.1
 clock stratum: 1
 clock status: configured, insane, valid, unsynced
 reference clock ID: LOCAL(0)
 reach: 0
 current poll: 64
 now: 9
 offset: 0.0000 ms
 delay: 0.00 ms
 disper: 0.00 ms
```

Table 3-173 Description of the display ntp-service sessions command output

Item	Description
clock source	Address of the clock source.
clock stratum	Stratum of the clock source. The clock stratum determines the precision of the clock, and its value ranges from 1 to 16. The higher the stratum value, the lower the clock precision. The value 1 indicates the highest precision, and the value 16 indicates the lowest precision. The clock with stratum 16 is in the unsynchronized status, and cannot be used as a reference clock.

Item	Description
clock status	Status of a clock, where - configured: indicates that the session is set up by a configuration command. - master: indicates that the clock source corresponding to the session is the primary clock source of the current system. - selected: indicates that the clock source corresponding to the session passes the clock selecting algorithm. - candidate: indicates that the clock source corresponding to the session is a candidate clock source. - sane: indicates that the clock source corresponding to the session passes the saneness test. - insane: indicates that the clock source corresponding to the session does not pass the saneness test. - valid: indicates that the clock source corresponding to the session is valid. The clock source corresponding to the session passes the test, is in a synchronized status and is of an effective stratum. The root delay and the root dispersion are within the normal range. - invalid: indicates that the clock source corresponding to the session is invalid. - unsynced: indicates that the clock source corresponding to the session is not yet synchronized or the stratum is invalid.
reference clock ID	When the local system has been synchronized to a remote NTP server or a clock source, the address of the remote server or the identifier of the clock source is displayed.
reach	Reachability count of the clock source. The value 0 indicates that the clock source is unreachable.
current poll	Poll interval of NTP packets. The interval for sending two successive NTP packets, in seconds. To set the poll interval, run the **ntp-service discard min-interval** command.
now	Interval between the last synchronization and the current time.
offset	Offset to the superior clock source.
delay	Delay to the superior clock source.
disper	Dispersion to the superior clock source.

Display detailed information about NTP sessions on the local device.

```
<HUAWEI> display ntp-service sessions verbose
 clock source: 172.16.12.1
 clock stratum: 1
 clock status: configured, insane, valid, unsynced
 reference clock ID: LOCAL(0)
 local mode: client, local poll: 64, current poll: 64
 peer mode: server, peer poll: 64, now: 21
 offset: -3.2385 ms,delay: 26.97 ms,  disper: 14.85 ms
 root delay: 0.00 ms, root disper: 10.94 ms
 reach: 255, sync dist: 0.058, sync state: 4
 precision: 2^18, version: 3, peer interface: wildcard
 reftime: 10:01:38.546 UTC Sep 5 2005(C6C69602.8C00DA1A)
 orgtime: 10:01:43.463 UTC Sep 5 2005(C6C69607.76ACC921)
 rcvtime: 10:01:43.480 UTC Sep 5 2005(C6C69607.7AF4ADBC)
 xmttime: 10:01:43.452 UTC Sep 5 2005(C6C69607.73F1E8E6)
 filter delay :  0.03   0.02   0.03   0.02   0.02   0.02   0.04   0.02
 filter offset:  0.00  -0.01   0.00   0.01   0.00   0.00   0.00   0.00
 filter disper:  0.03   0.02   0.00   0.11   0.09   0.08   0.06   0.05
 reference clock status: normal
```

Table 3-174 Description of the display ntp-service sessions verbose command output

Item	Description
clock source	Address of the clock source.
clock stratum	NTP stratum on which the local system is located.

Item	Description
clock status	Status of a clock, where ● configured: indicates that the session is set up by a configuration command. ● master: indicates that the clock source corresponding to the session is the primary clock source of the current system. ● selected: indicates that the clock source corresponding to the session passes the clock selecting algorithm. ● candidate: indicates that the clock source corresponding to the session is a candidate clock source. ● sane: indicates that the clock source corresponding to the session passes the saneness test. ● insane: indicates that the clock source corresponding to the session does not pass the saneness test. ● valid: indicates that the clock source corresponding to the session is valid. The clock source corresponding to the session passes the test, is in a synchronized status and is of an effective stratum. The root delay and the root dispersion are within the normal range. ● invalid: indicates that the clock source corresponding to the session is invalid. ● unsynced: indicates that the clock source corresponding to the session is not yet synchronized or the stratum is invalid.
reference clock ID	When the local system has been synchronized to a remote NTP server or a clock source, the address of the remote server or the identifier of the clock source is displayed. When the server is located on a certain VPN, the name of the VPN instance is displayed.
local mode	Local system mode.
peer mode	Peer system mode.
local poll	Local polling mode.
peer poll	Peer polling mode.
offset	Offset to the superior clock source.
delay	Delay to the superior clock source.
disper	Dispersion to the superior clock source.

Item	Description
root delay	Total system delay between the local end and the master reference clock. The default value is 0. If the value of root delay or root disper is large, clock synchronization may fail. A larger value indicates that the packet takes a longer time to reach the local device from the master reference clock. Therefore, the local device cannot determine whether the time in the packet is correct.
root disper	System dispersion of the local end to the master reference clock. The default value is 0. If the value of root delay or root disper is large, clock synchronization may fail. A larger value indicates that the packet takes a longer time to reach the local device from the master reference clock. Therefore, the local device cannot determine whether the time in the packet is correct.
reach	Reachability mark, indicating the reachability to the clock source.
sync dist	Synchronization distance to the superior clock source. This parameter evaluates and describes the clock source, and NTP chooses the clock source with the shortest synchronization distance.
sync state	Synchronization state: ● 0: The clock has never been synchronized. ● 1: Frequency information is obtained from configuration information. ● 2: The clock is set. ● 3: The clock is set, but the frequency is not yet determined. ● 4: The clock is synchronized. ● 5: An error is found.
precision	Precision of a peer clock.
version	NTP version.
peer interface	Peer interface.
reftime	Reference timestamp.
orgtime	Time when an NTP packet is sent for the last time.
rcvtime	Time when an NTP packet is received for the last time.
xmttime	Time when an NTP packet is forwarded for the last time.
filter delay	Filter delays of the 8 packets received for the last time.

Item	Description
filter offset	Filter offsets of the 8 packets received for the last time.
filter disper	Filter dispersions of the 8 packets received for the last time.
reference clock status	The status of the reference clock, including: ● normal: indicates that the peer clock is reachable. ● abnormal: indicates that the peer clock is unreachable.

3.13.4 display ntp-service statistics packet

Function

The **display ntp-service statistics packet** command displays statistics on NTP packets.

Format

display ntp-service statistics packet [**ipv6** | **peer** [*ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6** [*ipv6-address* [**vpn-instance** *vpn-instance-name*]]]]

Parameters

Parameter	Description	Value
ipv6	Displays statistics about global IPv6 NTP packets.	-
peer	Displays statistics on an NTP symmetric peer.	-
ip-address	Specifies the IP address of an NTP symmetric peer.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance related to an NTP symmetric peer.	The value must be an existing VPN instance name.
ipv6	Displays the packet statistics on IPv6 peers.	-
ipv6-address	Displays the NTP packet statistics on the specified IPv6 peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ntp-service statistics packet** command output includes the following information, and can help you to debug NTP packets.

- Number of packets sent and received by an interface
- Number of packets failing authentication
- Number of dropped packets
- Reason for dropping an NTP packet last time

Example

Display the statistics on NTP packets.

```
<HUAWEI> display ntp-service statistics packet
 NTP IPv4 Packet Statistical Information
 ---------------------------------------
 Sent                          : 100
    Send failures                : 10
 Received                      : 1000
    Processed                  : 800
    Dropped                    : 200
       Validity test failures      : 50
          Authentication failures      : 20
       Invalid packets             : 50
       Access denied               : 50
       Rate-limited                : 0
       Processing delay            : 50
       Interface disabled          : 0
       Max dynamic association reached : 0
       Server disabled             : 0
       Others                      : 0
Last 2 packets drop reasons:
  [2011-11-24 12:19:26-08:00] Global drop: NTP service disabled for interface.
  [2011-11-24 12:20:30-08:00] Global drop: NTP service disabled for interface.
```

Table 3-175 Description of the **display ntp-service statistics packet** command output

Item	Description
NTP IPv4 Packet Statistical Information	Statistics on IPv4 NTP packets.
Sent	Number of packets sent.
Send failures	Number of failures in sending packets.
Received	Number of received packets.
Processed	Number of processed packets.
Dropped	Number of dropped packets.

Item	Description
Validity test failures	Number of packets dropped because the packets fail to pass the validity test.
Authentication failures	Number of packets dropped because the packets fail to pass the authentication.
Invalid packets	Number of packets dropped because the packets are invalid.
Access denied	Number of packets dropped for lack of access control authority.
Rate-limited	Number of packets dropped due to rate limit.
Processing delay	Number of packets dropped because processing of the packets is delayed.
Interface disabled	Number of packets dropped because the interface is disabled.
Max dynamic association reached	Number of packets dropped because the maximum number of dynamic sessions is reached.
Server disabled	Indicates the number of packets dropped as server disabled.
Others	Number of packets dropped for other reasons.
Last 2 packets drop reasons	Reason for dropping the last n packets, where the maximum value of n can be 10.

3.13.5 display ntp-service status

Function

The **display ntp-service status** command displays the status of NTP.

Format

display ntp-service status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor or locate faults on the NTP service, run the **display ntp-service status** command to obtain status information about the NTP service, such as the synchronization status of the local clock and the stratum of the clock.

Example

Display the status of the NTP service.

```
<HUAWEI> display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 10.00 ms
reference time: 15:51:36.259 UTC Apr 25 2012(C6179088.426490A3)
synchronization state: spike (clock will be set in 1010 secs)
```

Table 3-176 Description of the display ntp-service status command output

Item	Description
clock status	Indicates the clock status. ● synchronized: indicates that the local clock has been synchronized with an NTP server or the reference clock. ● unsynchronized: indicates that the local clock has not been synchronized with any NTP server.
clock stratum	Indicates the stratum of the reference clock. The value ranges from 1 to 15. A lower the clock stratum indicates higher clock precision. When the client gets synchronized to a session, its stratum is the session stratum plus 1.
reference clock ID	Indicates ID of the reference clock. ● When the local clock has been synchronized with the remote NTP server, ID of the reference clock shows IP address of the remote server. ● When the local clock has been synchronized with the reference clock, it shows ID of the reference clock. ● If the local clock is the reference clock, it shows "Local".
nominal frequency	Indicates the nominal frequency of the local clock, in Hz.
actual frequency	Indicates the actual frequency of the local clock, in Hz.
clock precision	Indicates the precision of the local clock.
clock offset	Indicates the offset between the local clock and the NTP server, in ms.

Item	Description
root delay	Indicates the delay between the local clock and the master reference clock, in ms.
root dispersion	Indicates the dispersion between the local clock and the master reference clock, in ms.
peer dispersion	Indicates the dispersion between the local clock and the peer clock, in ms.
reference time	Indicates reference timestamp.
synchronization state	Indicates the synchronization status of the local clock: ● **clock not set**: Indicates the clock is not updated. ● **frequency set by configuration**: Indicates the clock frequency is set by NTP configuration. ● **clock set**: Indicates the clock is set. ● **clock set but frequency not determined:** Indicates the clock is set but the frequency is not determined. ● **clock synchronized**: Indicates that the clock is synchronized. ● **spike (clock will be set in XXX secs)**: Indicates a time difference of more than 128 milliseconds is detected between NTP server and client clock. The clock change will take effect in XXX seconds.

3.13.6 display ntp-service trace

Function

The **display ntp-service trace** command displays the system to trace the path of reference clock source from the local device.

Format

display ntp-service trace

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display ntp-service trace** command, summary information of NTP servers for synchronizing time on the link from the local device to the reference clock source can be displayed.

Example

Display the summary of each passing NTP server when you trace the reference clock source from the local device.

```
<HUAWEI> display ntp-service trace
server 127.0.0.1,stratum 5, offset 0.024099 s, synch distance 0.06337
server 192.168.1.2,stratum 4, offset 0.028786 s, synch distance 0.04575
server 192.168.2.2,stratum 3, offset 0.035199 s, synch distance 0.03075
server 192.168.10.1,stratum 2, offset 0.039855 s, synch distance 0.01096
refid 127.127.1.0
```

Table 3-177 Description of the display ntp-service trace command output

Item	Description
server	IP address of the NTP server.
stratum	Stratum of the clock on the NTP server.
offset	Offset to the superior reference clock.
synch distance	Synchronization distance to the superior reference clock. This parameter evaluates and describes the reference clock and NTP chooses the reference clock with the shortest synchronization distance.
refid	Reference clock source.

3.13.7 display snmp-agent trap feature-name ntp all

Function

The **display snmp-agent trap feature-name ntp all** command displays the status of NTP traps.

Format

display snmp-agent trap feature-name ntp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name ntp all** command to check status of NTP traps. This status can be configured using the **snmp-agent trap enable feature-name ntp** command.

Example

Display the status of NTP traps.

```
<HUAWEI> display snmp-agent trap feature-name ntp all
------------------------------------------------------------------------------
Feature name: NTP
Trap number : 1
------------------------------------------------------------------------------
Trap name                   Default switch status   Current switch status
hwNtpStateChangeTrap            on                     on
```

Table 3-178 Description of the **display snmp-agent trap feature-name ntp all** command output

Item	Description
Feature name	Name of the module where the trap is generated.
Trap number	Number of traps.
Trap name	Name of a trap.
Default switch status	Default status of a trap: ● on: The trap function is enabled. ● off: The trap function is disabled.
Current switch status	Current status of a trap: ● on: The trap function is enabled. ● off: The trap function is disabled. This status can be configured using the **snmp-agent trap enable feature-name ntp** command.

3.13.8 ntp-service

Function

The **ntp-service** command configures the maximum polling interval, the timestamp difference between packets sent by the clock server and received by the client, the maximum interval at which the clock of the client is synchronized.

The **undo ntp-service** command restores the default value.

By default, the maximum polling interval is 2^{17}s, the timestamp difference between packets sent by the clock server and received by the client is 128 ms, the maximum interval at which the clock of the client is synchronized is 600 seconds.

Format

ntp-service { **max-sys-poll** *max-sys-poll-value* | **spike-offset** *spike-offset-value* | **sync-interval** *interval* } *

undo ntp-service { **max-sys-poll** | **spike-offset** | **sync-interval** } *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **max-sys-poll** *max-sys-poll-value* and **spike-offset** *spike-offset-value* parameters.

Parameters

Parameter	Description	Value
max-sys-poll *max-sys-poll-value*	Specifies the maximum polling rate.	The value is an integer ranging from 6 to 17.
spike-offset *spike-offset-value*	Specifies the timestamp difference between packets sent by the clock server and received by the client.	The value is an integer ranging from 32 to 128, in milliseconds.
sync-interval *interval*	Sets the maximum interval for clock synchronization.	The value is an integer, in seconds. The value ranges from 180 to 600.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NTP polling interval is expressed in nth power of 2 (n is an integer). For example, run the **ntp-service max-sys-poll 6** command, the system sends polling packets every 64s. In other words, the device monitors the clock change on the server every 64s.

To decrease the timestamp difference between packets sent by the clock server and received by the client, run the **ntp-service spike-offset** command. If the time offset of the server is greater than the configured timestamp difference, NTP sets the system clock after the interval for time synchronization elapses.

When the clock of the server changes, the clock of the client is required to be synchronized with the clock of the server. If the clock of the server is unstable, you can run the **ntp-service sync-interval** command on the client to reduce the interval.

The **ntp-service max-distance** command is applied to only the NTP client. The NTP client calculates the distance with each NTP server, and compares the calculated distance with the distance threshold configured using the **ntp-service max-distance** command. If the calculated distance is longer than the threshold, the NTP client does not synchronize the clock from this NTP server.

Precautions

The NTP poll interval must be an integer power of 2; therefore, the interval for the client synchronization is configured as a value closest to the integer power of 2. For example, if the interval configured by the user is 180 seconds, the client is synchronized at any time after 128 seconds.

If you run the **ntp-service** command repeatedly, the latest configuration overrides the previous configurations.

Example

Set the maximum interval to 200 seconds for clock synchronization.

```
<HUAWEI> system-view
[HUAWEI] ntp-service sync-interval 200
```

3.13.9 ntp-service access

Function

The **ntp-service access** command sets the access control authority of the local NTP.

The **undo ntp-service access** command cancels the configured access control authority.

By default, no access control authority is set.

Format

ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } { *acl-number* | **ipv6** *acl6-number* } *

undo ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } [**ipv6** | **all**]

undo ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } [*acl-number* | **ipv6** *acl6-number*] *

Parameters

Parameter	Description	Value
peer	Indicates maximum access authority. Both time request and control query can be performed on the local NTP service, and the local clock can be synchronized to the remote server.	-
query	Indicates minimum access. Only control query can be performed on the local NTP service.	-
server	Indicates that server access and query are permitted. Both time request and control query can be performed on the local NTP service, but the local clock cannot be synchronized to the remote server.	-
synchronization	Indicates that only server access is permitted. Only time request can be performed on the local NTP service.	-
limited	When the rate of NTP packets exceeds the upper limit, the incoming NTP packets are discarded.	-
acl-number	Indicates the number of a basic ACL with IPv4 address specified.	The value is an integer that ranges from 2000 to 2999.
ipv6 *acl6-number*	Indicates the number of an ACL with IPv6 address specified.	The value is an integer that ranges from 2000 to 2999.
all	Indicates all access control authority.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with NTP authentication, **ntp-service access** is simpler to ensure the network security. When an access request reaches the local end, the access request is successively matched with the access authority from the highest one to the lowest one. The first successfully matched access authority takes effect. The matching order is: **peer**, **server**, **synchronization**, **query** and **limited**.

Depending on the access authority to be limited, run the command on different devices accordingly. For details, see the following table.

Table 3-179 Configuration of the NTP access control authority

NTP Operating Mode	Usage Scenario	Device Configured
Unicast NTP server/ client mode	The client is restricted from being synchronized to a server, so that the client will not be synchronized to an unreliable unicast NTP server on the network.	Client
Unicast NTP server/ client mode	The server is restricted from processing the synchronization time request of the client, so that the synchronization range of the server is controlled.	Server
NTP symmetric peer mode	The two ends are restricted from being synchronized with each other to prevent an unreliable symmetric passive peer on the network from synchronizing the client.	Symmetric active peer
NTP symmetric peer mode	The symmetric passive peer is restricted from processing the time request, so that the synchronization range of the symmetric passive peer is controlled.	Symmetric passive peer
NTP multicast mode	The client is restricted from synchronizing to the server to prevent an unreliable multicast NTP server from synchronizing the client.	NTP multicast client
NTP broadcast mode	The client is restricted from being synchronized to a server, so that the client will not be synchronized to an unreliable broadcast NTP server on the network.	NTP broadcast client
NTP manycast client mode	The client is restricted from being synchronized to a server.	NTP manycast client
NTP manycast server mode	The server is restricted from processing the clock synchronization request sent by the client.	NTP manycast server

The **ntp-service access** command ensures the security to the minimal extent. A safer method is to perform identity authentication. See the **ntp-service authentication enable** command for relevant configuration.

Precautions

Before configuring access control authority in ACL, check ACL rule configurations as follows:

- If the ACL rule is set to **permit** or empty, a permit action will be performed.
- If the ACL rule is set to **deny** or the associated peer is not bound to the ACL rule, a deny action will be performed.

Example

Enable the peer matching ACL 2000 to perform time request, query control and time synchronization on the local device.

```
<HUAWEI> system-view
[HUAWEI] ntp-service access peer 2000
```

Enable the server matching ACL 2002 to perform time request and query control on the local device.

```
<HUAWEI> system-view
[HUAWEI] ntp-service access server 2002
```

3.13.10 ntp-service authentication enable

Function

The **ntp-service authentication enable** command enables identity authentication for NTP.

The **undo ntp-service authentication enable** command disables the identity authentication.

By default, identity authentication is disabled.

Format

ntp-service authentication enable

undo ntp-service authentication enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On networks requiring high security, authentication must be enabled for NTP. The NTP client authenticates NTP servers using a password and synchronizes time with only the authenticated server. This improves network security.

Example

Enable identity authentication for NTP.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
```

3.13.11 ntp-service authentication-keyid

Function

The **ntp-service authentication-keyid** command sets NTP authentication key.

The **undo ntp-service authentication-keyid** command removes NTP authentication key.

By default, no authentication key is set.

Format

ntp-service authentication-keyid *key-id* **authentication-mode** { **md5** | **hmac-sha256** } [**cipher**] *password*

undo ntp-service authentication-keyid *key-id*

Parameters

Parameter	Description	Value
key-id	Indicates the key number.	Key ID is an integer and ranges from 1 to 4294967295.
authentication-mode md5	Indicates MD5 authentication mode.	-
authentication-mode hmac-sha256	Indicates HMAC-SHA256 authentication mode.	-
cipher	Indicates that the configured password is displayed in cipher text.	-

Parameter	Description	Value
password	Specifies the authentication password in plain text or in cipher text.	The keyword is a string of case sensitive characters, spaces supported. ● 1 to 255 characters in plain text. ● 20 to 392 characters in cipher text. When quotation marks are used around the string, spaces are allowed in the string. **NOTE** To improve password security, the password must be a combination of at least two of the following: digits, letters, and special characters, and the password length must be equal to or larger than 8. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each password.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network that requires high security, the NTP authentication must be enabled. You can configure password authentication between client and server, which guarantee the client only to synchronize with server successfully authenticated, and improve network security. If the NTP authentication function is enabled, a reliable key should be configured at the same time. Keys configured on the client and the server must be identical.

NOTE

In NTP symmetric peer mode, the symmetric active peer functions as a client and the symmetric passive peer functions as a server.

Follow-up Procedure

You can configure multiple keys for each device. After the NTP authentication key is configured, you need to set the key to reliable using the **ntp-service reliable authentication-keyid** command. If you do not set the key to reliable, the NTP key does not take effect.

Precautions

To ensure security, you are advised to use the HMAC-SHA256 algorithm, which is more secure, for NTP authentication.

You can configure a maximum of 1024 keys for each device.

If the NTP authentication key is a reliable key, it automatically becomes unreliable when you delete the key. You do not need to run the **undo ntp-service reliable authentication-keyid** command.

Example

Set the HMAC-SHA256 identity authentication key. The key ID number is 10, and the key is **Betterkey**.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication-keyid 10 authentication-mode hmac-sha256 BetterKey
```

Set authentication text to **xyz123** in HMAC-SHA256 authentication with cipher option.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication-keyid 10 authentication-mode hmac-sha256 cipher xyz123
```

3.13.12 ntp-service broadcast-client

Function

The **ntp-service broadcast-client** command configures the device to work in NTP broadcast client mode.

The **undo ntp-service broadcast-client** command removes the device from the NTP broadcast client mode.

By default, the device is not configured in the NTP broadcast client mode.

Format

ntp-service broadcast-client

undo ntp-service broadcast-client

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

On a synchronization subnet, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode.

On a specified interface on the broadcast client, run the **ntp-service broadcast-client** command to configure an interface on the local device to receive NTP broadcast packets. When the local device automatically runs in the broadcast client mode, the device can receive the synchronization packets sent by a broadcast server. For the configuration of the broadcast server, see the **ntp-service broadcast-server** command.

When the configuration is complete, you can run the **display ntp-service sessions** command to obtain information about sessions between the broadcast server and the local device.

Example

Enable VLANIF100 to receive NTP broadcast messages.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service broadcast-client
```

Enable GigabitEthernet0/0/1 to receive NTP broadcast messages.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service broadcast-client
```

3.13.13 ntp-service broadcast-server

Function

The **ntp-service broadcast-server** command configures the local device to work in NTP broadcast server mode.

The **undo ntp-service broadcast-server** command removes the device from the NTP broadcast server mode.

By default, the broadcast server mode is not configured.

Format

ntp-service broadcast-server [**version** *number* | **authentication-keyid** *key-id* | **port** *port-number* | **subnet-broadcast**] *

undo ntp-service broadcast-server [**version** *number* | **authentication-keyid** *key-id* | **port** *port-number* | **subnet-broadcast**] *

Parameters

Parameter	Description	Value
version *number*	Indicates the NTP version number. If this parameter is not specified, the version number is a default value.	The value is an integer that ranges from 1 to 4. The default value is 3.
authentication-keyid *key-id*	Indicates the authentication key number used to transmit a message to broadcast clients. If this parameter is not specified, authentication is not performed.	For NTPv1, NTPv2, and NTPv3, the value is an integer ranging from 1 to 4294967295. For NTPv4, the value is an integer ranging from 1 to 65535.
port *port-number*	Specifies the port number to transmit NTP broadcast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.
subnet-broadcast	Specifies the subnet broadcast mode for NTP broadcast server.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a synchronization subnet, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode. On a specified interface on the broadcast server, run the **ntp-service broadcast-server** command to configure an interface on the local device to send NTP broadcast packets. When the local device automatically runs in the broadcast server mode, the device can send synchronization packets to a broadcast client. For the configuration of the broadcast client, see the **ntp-service broadcast-client** command.

- Full broadcast mode: The broadcast server sends NTP packets to the broadcast address 255.255.255.255 periodically.

- Subnet broadcast mode: The broadcast server sends NTP packets to the broadcast address of the network segment to which the interface IP address belongs periodically.

Precautions

The full broadcast mode and subnet broadcast mode cannot be specified at the same time. After configuring either of the two modes, you must run the **undo ntp-service broadcast-server** command to cancel the current mode before configuring the other mode.

Follow-up Procedure

When the configuration is complete, you can run the **display ntp-service sessions** command to obtain information about sessions between the broadcast server and the client.

Example

Enable VLANIF100 to send NTP broadcast packets, with the NTP version as 2 and the key number as 4.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service broadcast-server version 2 authentication-keyid 4
```

Enable GigabitEthernet0/0/1 to send NTP broadcast packets, with the NTP version as 3 and the key number as 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service broadcast-server version 3 authentication-keyid 100
```

3.13.14 ntp-service disable

Function

The **ntp-service disable** command disables the IPv4 and IPv6 NTP function.

The **undo ntp-service disable** command enables the IPv4 and IPv6 NTP function.

By default, the NTP function is enabled.

Format

ntp-service [**ipv6**] **disable**

undo ntp-service [**ipv6**] **disable**

Parameters

Parameter	Description	Value
ipv6	Indicates IPv6 NTP services.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **ntp-service disable** or **ntp-service ipv6 disable** command in the system view to disable the IPv4 or IPv6 NTP service function.

You can run the **ntp-service disable** command in either of the following situations:

- The device does not need to synchronize clock with IPv4 or IPv6 external servers or peers.
- The device does not need to provide reference clock source for IPv4 or IPv6 external clients.

Precautions

Disabling of NTP service will not delete the existing configurations.

After the NTP service is enabled, the system listens to IP address 0.0.0.0 by default. That is, the system listens to all IP addresses, which is prone to security issues. It is recommended that you run the **ntp-service access** { **peer** | **query** | **server** | **synchronization** | **limited** } { *acl-number* | **ipv6** *acl6-number* } * command to configure access control permission on the local NTP service. You can also run the **ntp-service authentication enable** command to configure NTP identify authentication.

Example

Disable the IPv4 NTP service.

```
<HUAWEI> system-view
[HUAWEI] ntp-service disable
```

Disable the IPv6 NTP service.

```
<HUAWEI> system-view
[HUAWEI] ntp-service ipv6 disable
```

3.13.15 ntp-service discard

Function

The **ntp-service discard** command sets the minimum inter-packet interval and the average inter-packet interval of NTP.

The **undo ntp-service discard** command cancels the minimum inter-packet interval and the average inter-packet interval of NTP.

By default, the minimum inter-packet interval is set to the first power of 2 in seconds, namely, 2 seconds, and the average inter-packet interval is set to the fifth power of 2 in seconds, namely, 32 seconds.

Format

ntp-service discard { **min-interval** *min-interval-val* | **avg-interval** *avg-interval-val* } *

undo ntp-service discard

Parameters

Parameter	Description	Value
min-interval *min-interval-val*	Specifies the minimum inter-packet interval of NTP. The actual value of the minimum inter-packet interval of NTP is the value obtained by raising 2 to the power of *min-interval-val*, expressed in seconds.	The value of *min-interval-val* is an integer that ranges from 1 to 8.
avg-interval *avg-interval-val*	Specifies the average inter-packet interval of NTP. The actual value of the average inter-packet interval of NTP is the value obtained by raising 2 to the power of *avg-interval-val*, expressed in seconds.	The value of *avg-interval-val* is an integer that ranges from 1 to 8.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The minimum inter-packet interval and the average inter-packet interval of NTP are set using the **ntp-service discard** command. To generate kiss code RATE, we need to set the minimum inter-packet interval and the average inter-packet interval of NTP.

Example

Set both the minimum inter-packet interval and the average inter-packet interval of NTP to the fourth power of 2, expressed in seconds, namely, 16 seconds.

```
<HUAWEI> system-view
[HUAWEI] ntp-service discard min-interval 4 avg-interval 4
```

3.13.16 ntp-service in-interface disable

Function

The **ntp-service in-interface disable** command disables an interface from receiving NTP packets.

The **undo ntp-service in-interface disable** command enables an interface to receive NTP packets.

By default, an interface is enabled to receive NTP packets.

Format

ntp-service [**ipv6**] **in-interface disable**

undo ntp-service [**ipv6**] **in-interface disable**

Parameters

Parameter	Description	Value
ipv6	Indicates IPv6 NTP services.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo ntp-service** [**ipv6**] **in-interface disable** command provides a method for access control.

You can disable the interface connected to external devices from receiving NTP packets in either of the following situations:

- An unreliable clock server exists on the interface. By default, all the interfaces can receive NTP packets after NTP is enabled on the device. However, an unreliable clock source makes NTP clock data inaccurate.
- The NTP clock data is modified when the interface is attacked maliciously.

Prerequisites

Before an interface is disabled from receiving IPv6 NTP packets, the IPv6 function must be enabled on the interface.

Example

Disable VLANIF100 from receiving NTP packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ntp-service in-interface disable
```

Disable GigabitEthernet0/0/1 from receiving NTP packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service in-interface disable
```

3.13.17 ntp-service kod-enable

Function

The **ntp-service kod-enable** command enables the KOD function.

The **undo ntp-service kod-enable** command disables the KOD functions.

By default, the KOD function is disabled.

Format

ntp-service kod-enable

undo ntp-service kod-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Kiss-o'-Death (KOD) is a brand new access control technology put forward by NTPv4, and the KOD is mainly used for a server to provide information, such as a status report and access control, for a client. After the KOD function is enabled on the server, the server sends the kiss code DENY or RATE to the client according to the operating status of the system.

When the kiss code is generated in a specific situation, run the **ntp-service kod-enable** command.

Follow-up Procedure

After the KOD function is enabled on the server, you can run the **ntp-service access limited** command to enable control on the rate of incoming NTP packets. When the rate of incoming NTP packets reaches the upper threshold, the server sends the kiss code.

Example

Enable the KOD function.

```
<HUAWEI> system-view
[HUAWEI] ntp-service kod-enable
```

3.13.18 ntp-service manycast-client

Function

The **ntp-service manycast-client** command configures the NTP manycast client mode.

The **undo ntp-service manycast-client** command cancels the NTP manycast client mode.

By default, the NTP manycast client mode is disabled.

Format

ntp-service manycast-client [*ip-address* | **ipv6** [*ipv6-address*]] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

undo ntp-service manycast-client [*ip-address* | **ipv6** [*ipv6-address*]] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

Parameters

Parameter	Description	Value
ip-address	Specifies a manycast IPv4 address, which is a class D address.	The default IPv4 address is 224.0.1.1.
ipv6 [*ipv6-address*]	Specifies a manycast IPv6 address.	The default IPv6 address is FF0E::0101.
authentication-keyid *key-id*	Specifies the ID of the authentication key used for sending packets to a manycast server.	The value is an integer that ranges from 1 to 65535.
ttl *ttl-number*	Specifies the TTL value of a manycast packet.	The value is an integer ranges from 1 to 255.

Parameter	Description	Value
port *port-number*	Specifies the port number to transmit NTP manycast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The local device runs in the manycast client mode, and periodically sends manycast packets to manycast servers. After the local device receives the reply packet sent by a manycast server, the local device establishes dynamic C/S association with the server.

NOTE

In the configuration of the manycast client, if the server address is not specified, 224.0.1.1 or FF0E::0101 is adopted as the server address by default.

Example

Configure VLANIF100 to receive NTP manycast packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service manycast-client
```

Configure GigabitEthernet0/0/1 to receive NTP manycast packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service manycast-client
```

3.13.19 ntp-service manycast-server

Function

The **ntp-service manycast-server** command configures the NTP manycast server mode.

The **undo ntp-service manycast-server** command cancels the NTP manycast server mode.

By default, the NTP manycast server mode is not configured.

Format

ntp-service manycast-server [*ip-address* | **ipv6** [*ipv6-address*]]

undo ntp-service manycast-server [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a manycast IPv4 address, which is a class D address.	The default IPv4 address is 224.0.1.1.
ipv6 [*ipv6-address*]	Specifies a manycast IPv6 address.	The default IPv6 address is FF0E::0101.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The manycast server responds to the manycast packets sent by the client. After the manycast client receives the reply packet, the manycast client establishes temporary association with the server and enters C/S mode.

Precautions

If the manycast IP address is not specified when the **undo ntp-service manycast-server** command is run, the local device searches for the default IP address. In IPv4 networks, the default IP address of the manycast server is 224.0.1.1. In IPv6 networks, the default IP address of the manycast server is FF0E::0101. If the local device finds the default IP address, the **undo ntp-service manycast-server** command takes effect; otherwise, the **undo ntp-service manycast-server** does not take effect.

Example

Configure VLANIF100 as an interface of the server. The interface is used for responding to the manycast client request from a manycast address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service manycast-server
```

Configure GigabitEthernet0/0/1 as an interface of the server. The interface is used for responding to the manycast client request from a manycast address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service manycast-server
```

3.13.20 ntp-service max-distance

Function

The **ntp-service max-distance** command configures the maximum distance threshold value.

The **undo ntp-service max-distance** command restores the default value.

By default, the maximum distance threshold value is 1.

Format

ntp-service max-distance *max-distance-value*

undo ntp-service max-distance

Parameters

Parameter	Description	Value
max-distance-value	Indicates the maximum distance threshold value in seconds.	The value is an integer and ranges from 1 to 16, in seconds. The default value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

ntp-service max-distance command is used at the client side. At the client side, NTP will calculate synchronization distance for each server and compare it with synchronization distance threshold value. If the synchronization distance exceeds synchronization distance threshold value, the client will not consider that server for clock synchronization. This command is used in the calculation of synchronization distance threshold value.

Example

Set the NTP maximum distance to 16s.

```
<HUAWEI> system-view
[HUAWEI] ntp-service max-distance 16
```

3.13.21 ntp-service max-dynamic-sessions

Function

The **ntp-service max-dynamic-sessions** command sets the maximum dynamic NTP sessions that can be set up.

The **undo ntp-service max-dynamic-sessions** command restores the maximum dynamic NTP sessions to the default value.

By default, a maximum of 100 NTP dynamic sessions can be set up.

Format

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

Parameters

Parameter	Description	Value
number	Specifies the number of dynamic sessions that can be set up.	The value is an integer that ranges from 0 to 100, and the default value is 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A maximum of 128 sessions can be established on the same device running the NTP service in the same period, including static and dynamic sessions. In both unicast server/client mode and symmetric peer mode, command lines are used to establish static sessions. The dynamic sessions are established in broadcast mode or multicast mode.

Excessive dynamic sessions directly affect the establishment of static sessions. A user can limit the number of local dynamic sessions solve this problem.

Precautions

When the number of local dynamic sessions on the device is limited:

- This command limits the number of only dynamic sessions, not static sessions.
- NTP dynamic sessions established are not affected. That is, when the number of the dynamic sessions exceeds the limit, the dynamic sessions established are not deleted, but a new dynamic session cannot be established.

- The limit on the number of local dynamic sessions allowed should be configured on the client because the server does not record the number of the established NTP sessions.

Example

Set the maximum number of NTP dynamic sessions that can be set up to 50.

```
<HUAWEI> system-view
[HUAWEI] ntp-service max-dynamic-sessions 50
```

3.13.22 ntp-service multicast-client

Function

The **ntp-service multicast-client** command configures the local device to work in NTP multicast client mode.

The **undo ntp-service multicast-client** command cancels the NTP multicast client mode.

By default, the NTP multicast client mode is not configured.

Format

ntp-service multicast-client [*ip-address* | **ipv6** [*ipv6-address*]]

undo ntp-service multicast-client [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Indicates the multicast IP address.	The default IP address is 224.0.1.1.
ipv6 [*ipv6-address*]	Indicates the multicast IPv6 address.	The default IPv6 address is FF0E::0101.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform clock synchronization in multicast mode, you can use the **ntp-service multicast-client** command to specify the current interface on the local device to receive NTP multicast packets. The local device runs in the multicast client mode.

If the valid multicast server is configured, the local device gets synchronized with the multicast server. The local device time is updated with the time of the server.

Follow-up Procedure

When the configuration is complete, run the **display ntp-service sessions** command to obtain session information about the multicast server and the local device.

NOTE

You can configure more than one multicast client with different multicast IP address on the same interface. When multiple multicast clients are configured, the device selects the optimal clock source by selecting a preferred clock.

You can configure a maximum of 1024 multicast clients on the local device, but a maximum of 128 multicast clients can work simultaneously.

Example

Configure VLANIF100 to receive NTP multicast packets. The multicast address of the multicast packets is 224.0.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service multicast-client 224.0.1.2
```

Configure GigabitEthernet0/0/1 to receive NTP multicast packets. The multicast address of the multicast packets is 224.0.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service multicast-client 224.0.1.1
```

3.13.23 ntp-service multicast-server

Function

The **ntp-service multicast-server** command specifies an interface on the local device to send NTP multicast packets. The local device runs in the multicast server mode.

The **undo ntp-service multicast-server** command cancels the NTP multicast server mode.

By default, the multicast server mode is not configured.

Format

ntp-service multicast-server [*ip-address*] [**version** *number* | **authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

ntp-service multicast-server ipv6 [*ipv6-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

undo ntp-service multicast-server [*ip-address*] [**version** *number* | **authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

undo ntp-service multicast-server ipv6 [*ipv6-address*] [**authentication-keyid** *key-id* | **ttl** *ttl-number* | **port** *port-number*] *

Parameters

Parameter	Description	Value
ip-address	Indicates the multicast IP address.	The default address is 224.0.1.1.
ipv6 [*ipv6-address*]	Indicates the multicast IPv6 address.	The default IPv6 address is FF0E::0101.
version *number*	Indicates the NTP version number. If this parameter is not specified, the version number is a default value.	The value is an integer that ranges from 1 to 4. The default value is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when sending messages to the multicast clients. If this parameter is not specified, authentication is not performed.	The value is an integer. It ranges from 1 to 4294967295 when the NTP version number is 1, 2, or 3, and ranges from 1 to 65535 when the version number is 4 or the specified remote server uses an IPv6 address.
ttl *ttl-number*	Indicates the life span of the multicast packet. If this parameter is not specified, the life span of the multicast packet is a default value.	The ttl number is an integer that ranges from 1 to 255. The default value is 255.
port *port-number*	Specifies the port number to transmit NTP multicast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform clock synchronization in the multicast mode, run the **ntp-service multicast-server** command to specify the current interface on the local device to send NTP multicast packets. The local device runs in the multicast server mode, and functions as the multicast server to periodically send multicast packets to the multicast client.

Follow-up Procedure

When the configuration is complete, run the **display ntp-service sessions** command to obtain session information about the multicast server and the local device.

NOTE

You can configure a maximum of 128 multicast servers on the local device.

Example

Configure VLANIF100 to send NTP multicast packets. The multicast IPv4 address is 224.0.1.1, the authentication key ID is 4 and the NTP version number is 3.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] ntp-service multicast-server 224.0.1.1 authentication-keyid 4 version 3
```

Configure GigabitEthernet0/0/1 to send NTP multicast packets. The multicast IPv4 address is 224.0.1.1, the authentication key ID is 4 and the NTP version number is 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ntp-service multicast-server 224.0.1.1 authentication-keyid 4 version 3
```

3.13.24 ntp-service port

Function

The **ntp-service port** command changes the number of the port that sends NTP packets.

The **undo ntp-service port** command restores the default port number.

By default, port 123 sends NTP packets.

Format

ntp-service port *port-value*

undo ntp-service port

Parameters

Parameter	Description	Value
port-value	Specifies the number of the port that sends NTP packets.	The value is an integer ranging from 1025 to 65535. **NOTE** The *port-value* can be set to the default port 123.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To improve security of network packets, run the **ntp-service port** command to configure the number of the port that sends NTP packets. Therefore, the user firewall filters packets based on the port number.

Example

Set the number of the port that sends NTP packets to 5000.

```
<HUAWEI> system-view
[HUAWEI] ntp-service port 5000
```

3.13.25 ntp-service refclock-master

Function

The **ntp-service refclock-master** command sets the local clock to be the NTP primary clock that provides the synchronizing time for other devices.

The **undo ntp-service refclock-master** command cancels the configuration of the NTP primary clock.

By default, no NTP primary clock is specified.

Format

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*] [*stratum*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the local reference clock. When no IP address is assigned, the local clock whose IP address is 127.127.1.0 is set as the default NTP primary clock.	The value of *ip-address* is 127.127.1.u, and **u** ranges from 0 to 3, which represents the number of the selected local clock.
stratum	Specifies the stratum of the NTP primary clock. If this parameter is not specified, the stratum is a default value.	The value of the stratum is an integer that ranges from 1 to 15. The default value is 8. Timer is accurate if the stratum value is small.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local clock is the clock of the device itself. Run the **ntp-service refclock-master** command to set the local clock as the NTP primary clock that provides the synchronization time for other devices.

In NTP, the time synchronization in an NTP synchronization subnet is performed from a smaller level to a larger level, that is, from the 1st level to the 15th level. An authoritative clock is used as a reference time source for the synchronization subnet, and is located at the top of the synchronization subnet. The authoritative clock is stratum0. The current authoritative clock is mostly a Radio Clock or the Global Positioning System. The time of the authoritative clock is synchronized through the broadcast UTC time code other than NTP.

Precautions

A device on the network can perform clock synchronization in the following manners.

- Synchronizing with the local clock: The local clock is used as the reference clock.
- Synchronizing with another device on the network: This device is used as an NTP clock server to provide a reference clock for the local end.

If both manners are configured, the device selects an optimal clock source through selecting a preferred clock. That is, clocks determined in the two manners are compared to determine which clock is a lower stratum. The clock of a lower stratum is the preferred clock source.

Example

Set the local clock to be the NTP primary clock, the stratum of which set to 3.

```
<HUAWEI> system-view
[HUAWEI] ntp-service refclock-master 3
```

3.13.26 ntp-service reliable authentication-keyid

Function

The **ntp-service reliable authentication-keyid** command specifies the authentication key to be reliable.

The **undo ntp-service reliable authentication-keyid** command cancels the current setting.

By default, no authentication key is specified to be reliable.

Format

ntp-service reliable authentication-keyid *key-id*

undo ntp-service reliable authentication-keyid *key-id*

Parameters

Parameter	Description	Value
key-id	Indicates the key number.	Key ID is an integer and ranges from 1 to 4294967295.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the identity authentication is enabled, this command is used to specify that one or more keys are reliable. That is, the client can only be synchronized with the server that provides the reliable key. The client cannot be synchronized with the server that provides unreliable keys.

Example

Enable the identity authentication in NTP and adopt the HMAC-SHA256 encryption mode with key number as 37 and the key as BetterKey. Specify the key to be reliable.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
[HUAWEI] ntp-service authentication-keyid 37 authentication-mode hmac-sha256 cipher BetterKey
[HUAWEI] ntp-service reliable authentication-keyid 37
```

3.13.27 ntp-service server disable

Function

The **ntp-service server disable** command disables NTP server function.

The **undo ntp-service server disable** command enables NTP server function.

By default, NTP server function is disabled.

Format

ntp-service [**ipv6**] **server disable**

undo ntp-service [**ipv6**] **server disable**

Parameters

Parameter	Description	Value
ipv6	Indicates IPv6 NTP services.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For the security purpose, NTP server function can be disabled when the device does not need to act as a server.

By default, NTP server functionality is disabled. To enable NTP server functionality, first configure other NTP functions, such as a clock source, and then run the **undo ntp-service server disable** command to make the NTP server function take effect. If you run the **undo ntp-service** [**ipv6**] **server disable** command alone, the NTP server function cannot take effect.

Example

Disable IPv4 NTP server function.

```
<HUAWEI> system-view
[HUAWEI] ntp-service server disable
```

Disable IPv6 NTP server function.

```
<HUAWEI> system-view
[HUAWEI] ntp-service ipv6 server disable
```

3.13.28 ntp-service source-interface

Function

The **ntp-service source-interface** command specifies the local source interface that sends NTP packets.

The **undo ntp-service source-interface** command cancels the current setting.

By default, the local source interface is not specified for sending NTP packets. The local source interface is automatically determined based on routes.

Format

ntp-service [**ipv6**] **source-interface** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

undo ntp-service [**ipv6**] **source-interface** [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6	Indicates that the network type of the local source interface is IPv6.	-
interface-type interface-number	Indicates the local interface that sends NTP packets.	-
vpn-instance *vpn-instance-name*	Indicates the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configure the local source interface for sending and receiving NTP packets to prevent other interfaces on the device from receiving NTP response packets. This configuration is convenient for a user to subsequently deploy a flow control policy. If no interface is specified, the source IP address of NTP packets is selected according to routes.

If you have specified **vpn-instance** when configuring a source IP address using this command, the source IP address can only be used by the NTP client bound to the specified VPN instance and cannot be used by NTP clients bound to other VPN instances or not bound to any VPN instance.

Precautions

- In broadcast, multicast, and manycast modes, NTP is implemented on a specific interface, and this interface is the source interface. Therefore, the **ntp-service source-interface** command is invalid in broadcast, multicast, and manycast modes.
- This command applies only to the NTP client, but not the NTP server.

Example

Specify VLANIF100 as the source interface to send all NTP packets.

```
<HUAWEI> system-view
[HUAWEI] ntp-service source-interface vlanif 100
```

3.13.29 ntp-service unicast-peer

Function

The **ntp-service unicast-peer** command configures NTP peer mode.

The **undo ntp-service unicast-peer** command cancels the NTP peer mode.

By default, the NTP peer mode is not configured.

Format

ntp-service unicast-peer *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **preempt** | **port** *port-number*] *

ntp-service unicast-peer ipv6 *ipv6-address* [**authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **preempt** | **port** *port-number*] *

undo ntp-service unicast-peer { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Indicates the IPv4 address of the remote peer.	The parameter *ip-address* is a host address and cannot be the broadcast address, the multicast address or the IP address of a reference clock.
ipv6 *ipv6-address*	Indicates the IPv6 address of the remote server.	The value of *ipv6-address* is a unicast address, but cannot be a broadcast address, multicast address, or reference clock's IP address.
version *number*	Indicates the NTP version number. If this parameter is not specified, the default version number is used.	The version number is an integer that ranges from 1 to 4. By default, it is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when transmitting messages to the remote peer. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295 when the NTP version number is from 1 to 3. When the NTP version number is 4, the key ID is integer that ranges from 1 to 65535. When the remote server address is an IPv6 address, the key ID is an integer that ranges from 1 to 65535.
maxpoll *max-number*	Indicates the maximum NTP poll interval.	The value is an integer that ranges from 10 to 17.
minpoll *min-number*	Indicates the minimum NTP poll interval.	The value is an integer that ranges from 3 to 6.

Parameter	Description	Value
source-interface *interface-type interface-number*	Indicates the source interface from which the symmetric active end sends NTP packets to the symmetric passive end. The source IP address of the NTP packets is the IP address of this interface.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.
preference	Indicates the remote peer as the preferred one. By default, the remote peer is not preferred. **NOTE** If you run the **ntp-service unicast-peer** command multiple times to configure multiple remote peers, you can specify the **preference** parameter to configure a peer as the preferred one. This prevents the local device from frequently switching connections with remote peers and prevents frequent time changes and a large number of logs generated on the local device.	-
preempt	Indicates that the symmetric peer is in preemption mode. If any error, for example, an authentication failure, is detected on the association, the symmetric peer in preemption mode is marked as unavailable for selection. However, when no other symmetric peers are available for selection, this symmetric peer is marked as available.	-
port *port-number*	Specifies the port number to transmit NTP unicast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the clock of a device on the network needs to be synchronized in symmetric peer mode, you can run the **ntp-service unicast-peer** command to configure a remote node as the symmetric peer of the device. The local device runs in symmetric active peer mode. In this mode, the device and the remote peer can synchronize clock with each other.

Precautions

- If the same server is specified in at least two commands that are run in sequence to configure the NTP server mode, during the configuration restoration, the last run command takes effect. For example, the **ntp-service unicast-peer 10.10.1.1 source-interface vlanif 10** command and **ntp-service unicast-peer 10.10.1.1** command are run in sequence. During the configuration restoration, only the **ntp-service unicast-peer 10.10.1.1** command takes effect.
- A maximum of 128 peers can be configured for the local device. The optimal symmetric peer is selected as the synchronization source.
- When a PE is synchronized to another PE or CE in a VPN, the parameter **vpn-instance** *vpn-instance-name* needs to be specified.
- When you run the **undo ntp-service unicast-peer** command with a specified **vpn-instance** *vpn-instance-name*, the configuration of the NTP symmetric passive peer with the IP address *ip-address* on the VPN is canceled. If **vpn-instance** *vpn-instance-name* is not specified, the configuration of the NTP symmetric passive peer with the IP address *ip-address* on the public network.

Example

Configure the peer 10.10.1.1 to provide the synchronizing time for the local device. The local device can also provide synchronizing time for the peer. The version number is 3. The IP address of the NTP packets is the address of VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ntp-service unicast-peer 10.10.1.1 version 3 source-interface vlanif 100
```

3.13.30 ntp-service unicast-server

Function

The **ntp-service unicast-server** command configures the NTP server mode.

The **undo ntp-service unicast-server** command cancels the NTP server mode.

By default, the NTP server mode is not configured.

Format

ntp-service unicast-server *ip-address* [**version** *number* | **authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **burst** | **iburst** | **preempt** | **port** *port-number*] *

ntp-service unicast-server ipv6 *ipv6-address* [**authentication-keyid** *key-id* | **source-interface** *interface-type interface-number* | **preference** | **vpn-instance** *vpn-instance-name* | **maxpoll** *max-number* | **minpoll** *min-number* | **burst** | **iburst** | **preempt** | **port** *port-number*] *

undo ntp-service unicast-server { *ip-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Indicates the IPv4 address of the remote server.	The value of *ip-address* must be an IP address of a host, but cannot be a broadcast address, multicast address, or reference clock's IP address.
version *number*	Indicates the NTP version number. If this parameter is not specified, the default version number is used.	The version number is an integer that ranges from 1 to 4. By default, the version number is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when messages are transmitted to the remote server. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295 when the NTP version number is from 1 to 3. When the NTP version number is 4, the key ID is integer that ranges from 1 to 65535. When the remote server address is an IPv6 address, the key ID is an integer that ranges from 1 to 65535.

Parameter	Description	Value
maxpoll *max-number*	Specifies the NTP maximum poll interval. The NTP poll interval of the system floats between the minimum value and maximum value.	It is an integer ranging from 10 to 17, in seconds. The default value is 10 seconds in NTPv1, NTPv2, NTPv3, and NTPv4.
minpoll *min-number*	Specifies NTP minimum poll interval. The NTP poll interval of the system floats between the minimum value and maximum value.	It is an integer ranging from 3 to 6, in seconds. The default value is 6 seconds.
source-interface *interface-type interface-number*	Indicates the source interface from which the unicast client sends NTP packets to the unicast server. The source IP address of the NTP packets is the IP address of this interface.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.
preference	Indicates the remote server as the preferred one. By default, the remote server is not preferred. **NOTE** If you run the **ntp-service unicast-server** command multiple times to configure multiple remote servers, you can specify the **preference** parameter to configure a server as the preferred one. This prevents the local device from frequently switching connections with remote servers and prevents frequent time changes and a large number of logs generated on the local device.	-
burst	Indicates that a burst of packets is sent within a fixed poll period. When the poll interval is long, this method helps measure the time jitter.	-

Parameter	Description	Value
iburst	Indicates that the device sends a burst of packets when receiving a response of an unreachable server. This parameter can be used to accelerate synchronization.	-
preempt	Indicates that the server is in preemption mode. If any error, for example, an authentication failure, is detected on the association, the server marked as "preempt" is marked as unavailable for selection. However, the server is marked as available for selection when no other servers are available for selection on the network and no error occurs on the association of the server.	-
port *port-number*	Specifies the port number to transmit NTP unicast message.	The value is 123 or an integer ranging from 1025 to 65535. The default value is 123.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the clock of a device on the network needs to be synchronized in unicast server/client mode, the command can be run, and the remote server specified by *ip-address* or *ipv6-address* is used as the local clock server. The local device runs in client mode. In this mode, the local client can be synchronized to the remote server, but the remote server cannot be synchronized to the local client.

When the **ntp-service unicast-server** command is run, you can also configure the mode used for the remote server, such as the NTP version, authentication key, and the polling interval.

Precautions

- A maximum of 128 servers can be configured for the local device. The optimal symmetric peer is selected as the synchronization source.

- If the local device works in the client mode, the local device can only be synchronized with the remote server but the remote server cannot be synchronized with the local device.
- When a PE is synchronized to another PE or CE in a VPN, the parameter **vpn-instance** *vpn-instance-name* needs to be specified.
- When the **undo ntp-service unicast-server** command is run, if the parameter **vpn-instance** *vpn-instance-name* is specified, cancel the configuration of the NTP server with the IP address *ip-address* or *ipv6-address* in the VPN. If the parameter **vpn-instance** *vpn-instance-name* is not specified, cancel the configuration of the NTP server with the IP address *ip-address* or *ipv6-address* in the public network.
- Before deleting a VPN instance, check whether the VPN instance is bound to the NTP server. This confirmation is to ensure that the changed configuration meets users' requirements. For example:
  a. Specify an NTP server and bind a VPN instance to the NTP server. You can view the following configurations:
     ```
     <HUAWEI> display current-configuration | begin ntp
     ntp-service unicast-server 10.1.1.1 vpn-instance vpn2
     ntp-service refclock-master
     ```
  b. If the VPN instance named vpn2 is deleted, the VPN instance bound to the NTP server is also deleted.
     ```
     <HUAWEI> display current-configuration | be ntp
     ntp-service unicast-server 10.1.1.1
     ntp-service refclock-master
     ```

Example

Configure the server 10.10.1.1 to provide the synchronizing time for the local device. The NTP version number is 3.

```
<HUAWEI> system-view
[HUAWEI] ntp-service unicast-server 10.10.1.1 version 3
```

Configure the server 10.10.1.1 with VPN instance "abc" to provide the synchronizing time for the local device.

```
<HUAWEI> system-view
[HUAWEI] ntp-service unicast-server 10.10.1.1 vpn-instance abc
```

3.13.31 reset ntp-service statistics packet

Function

The **reset ntp-service statistics packet** command clears statistics on NTP packets.

Format

reset ntp-service statistics packet [**ipv6** | **peer** [*ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6** [*ipv6-address* [**vpn-instance** *vpn-instance-name*]]]]

Parameters

Parameter	Description	Value
ipv6	Clears the statistics about global IPv6 NTP packets.	-
peer	Clears statistics related to NTP peers.	-
ip-address	Specifies the IP address of an NTP peer.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance bound to an NTP peer.	The value must be an existing VPN instance name.
ipv6	Clears the packet statistics on IPv6 peers.	-
ipv6-address	Clears the NTP packet statistics on the specified IPv6 peer.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

When debugging NTP, you can use this command to clear the statistics on NTP.

NOTICE

The statistics on NTP cannot be recovered after being cleared. Confirm before you delete the statistics.

Example

Clear statistics on NTP packets.

```
<HUAWEI> reset ntp-service statistics packet
```

Clear statistics on NTP peers.

```
<HUAWEI> reset ntp-service statistics packet peer
```

3.13.32 snmp-agent trap enable feature-name ntp

Function

The **snmp-agent trap enable feature-name ntp** command enables the trap function for the NTP module.

The **undo snmp-agent trap enable feature-name ntp** command disables the trap function for the NTP module.

By default, the trap function is enabled for the NTP module.

Format

snmp-agent trap enable feature-name ntp [**trap-name hwntpstatechangetrap**]

undo snmp-agent trap enable feature-name ntp [**trap-name hwntpstatechangetrap**]

Parameters

Parameter	Description	Value
trap-name hwntpstatechangetrap	Indicates that NTP synchronization status changed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the NMS to easily manage the NTP module of the device, run the **snmp-agent trap enable feature-name ntp** command to enable the trap function for the NTP module. The command configuration ensures that the traps generated during the device operation are sent to the NMS. Otherwise, NTP traps are not sent to the NMS.

You can run the **snmp-agent trap enable feature-name ntp** command to check the configuration result.

Example

Enable the **hwntpstatechangetrap** trap.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name ntp trap-name hwntpstatechangetrap
```

3.14 PTP Configuration Commands

3.14.1 Command Support

Model	Supported Part Number	Unsupported Part Number
S6730-H24X6C	• 02352FSG, 02352FSG-001, 02352FSG-003, 02352FSG-005, 02352FSG-006 • 02353GFC, 02353GFC-001, 02353GFC-003	• 02352FSG-007, 02352FSG-008 • 02353GFC-004
S6730-H48X6C	• 02352FSF, 02352FSF-003, 02352FSF-005, 02352FSF-007, 02352FSF-008, 02352FSF-011 • 02353FWL, 02353FWL-003, 02353FWL-005	• 02352FSF-009, 02352FSF-010 • 02353FWL-006
S6730-H24X4Y4C	None	No part number supports this model.
S6730-H28Y4C	None	No part number supports this model.
S6730S-H24X6C-A	• 02353HVK, 02353HVK-001, 02353HVK-003	02353HVK-004

3.14.2 display ptp

Function

The **display ptp** command displays information about the Precision Time Protocol (PTP).

Format

display ptp all [**config** | **state**] [**slot** *slot-id*]

display ptp interface *interface-type interface-number*

Parameters

Parameter	Description	Value
all	Displays all the statistics of a PTP device, such as the global configuration parameters, interface where the clock source resides, time trace status, and interface running status.	-

Parameter	Description	Value
config	Displays configurations of all the modules related to PTP on the device.	-
state	Displays the running status of the protocol on all the modules related to PTP on the device.	-
slot *slot-id*	Displays the status information of the protocol on all the modules related to PTP based on a slot ID.	The value must be set according to the device configuration.
interface *interface-type interface-number*	Displays the BMC running status and the number of sent and received PTP packets on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Using the **display ptp** command, you can view the running status of PTP and statistics information about the global configuration parameters, interface where the clock source resides, and clock lock status. In addition, the command also displays the grandmaster clock ID, receiver number, parent clock ID, parent port number, statistics, and status of interfaces or role list.

Precautions

The **display ptp** displays the configuration on the interface only when PTP is enabled globally and in the interface view.

Example

Display the status and statistics of all the modules related to PTP.

```
<HUAWEI> display ptp all slot 0
 Device config info
```

```
 ----------------------------------------------------------------------
 PTP state         :enabled    Domain  value       :0
 Slave only        :no         Device type         :E2ETCOC
 Set port state    :no         Local clock ID      :e468a3fffe552a30
 Virtual clock ID  :no         Time lock success   :no
 PTP profile       :IEEE1588V2

 BMC run info
 ----------------------------------------------------------------------
 Grand clock ID    :9c8fd0fffecf3c87
 Receive number    :XGigabitEthernet0/0/3
 Parent clock ID   :9c8fd0fffecf3c87
 Parent portnumber :256
 Priority1         :1          Priority2           :1
 Step removed      :0          Clock accuracy      :0x21
 Clock class       :6          Time Source         :0xa0
 UTC Offset        :35         UTC Offset Valid    :False
 Timescale         :PTP        Time Traceable      :False
 Leap              :None       Frequence Traceable:True
 Offset scaled     :0xffff


 Clock source info
 Clock Pri1 Pri2 Accuracy Class TimeSrc Signal Switch Direction In-Status
 ----------------------------------------------------------------------
 local 128  128  0x31     187   0xa0     -      -      -         -
```

Display PTP interface status and packet statistics of XGigabitEthernet0/0/3.

```
<HUAWEI> display ptp interface xgigabitethernet 0/0/3
 Port State :faulty
 Port Number :3

 Recv Packet Statistics
 ---------------------------------------------------------------------
 Announce              :0         Sync                     :0
 Req                   :0         Resp                     :0
 Followup              :0         Pdelay_resp_followup      :0

 Send Packet Statistics
 ---------------------------------------------------------------------
 Announce              :0         Sync                     :0
 Req                   :0         Resp                     :0
 Followup              :0         Pdelay_resp_followup      :0

 Discard Packet Statistics
 ---------------------------------------------------------------------
 Announce              :0         Sync                     :0
 Delayreq              :0         Pdelayreq                :0
 Resp                  :0         Pdelayresp               :0
 Followup              :0         Pdelay_resp_followup      :0
```

Table 3-180 Description of the **display ptp** command output

Item	Description
Device config info	
PTP state	Whether PTP is enabled. The value is set through the **ptp enable** command.
Domain value	Domain that the PTP clock belongs to. The value is set through the **ptp domain** command.

Item	Description
Slave only	Whether the **slave only** mode is adopted. The value is set through the **ptp slaveonly** command.
Device-type	Type of the PTP device. The value is set through the **ptp device-type** command.
Set port state	Whether to manually enable tracing for a clock source.
Virtual clock ID	Whether a virtual clock ID is configured.
Time lock success	Whether the device time is locked.
PTP profile	PTP profile the device is using.
Local clock ID	ID of the local clock. The value is set through the **ptp virtual-clock-id** command.
BMC run info	
Grand clock ID	ID of the grandmaster clock.
Receive number	Interface that receives signals of the clock source.
Parent clock ID	ID of the parent clock.
Parent portnumber	Interface that sends signals of the parent clock source.
Priority1	Priority1 of the clock source obtained from the master clock.
Priority2	Priority2 of the clock source obtained from the master clock.
Step removed	Number of communication channels between the local clock and the grandmaster clock, that is, number of BC devices.
Clock-accuracy	Accuracy of the clock source, which is obtained from the master clock.
Clock-class	Class of the clock source, which is obtained from the master clock.
Time Source	Time source of the clock source, which is obtained from the master clock.

Item	Description
UTC Offset	Offset between the Universal Time Coordinated (UTC) and International Atomic Time (TAI).
UTC Offset Valid	Whether the UTC offset takes effect.
Timescale	Time scale used by the PTP clock. The PTP protocol supports two types of time scales: - ARB - PTP
Time Traceable	Whether the time can be traced.
Frequence Traceable	Whether the clock frequency can be traced.
Source port	Clock source of the master clock.
Port info	
Name	Name of the interface enabled with PTP.
State	Status of the interface enabled with PTP: - Faulty: indicates that the interface is faulty. - Listening: indicates that the interface is being monitored. - Master: indicates that the interface is a master interface. - Passive: indicates that the interface is a passive port. - Premaster: indicates that the interface is a standby master interface. - Slave: indicates that the interface is a slave interface.
Delay-mech	Delay measurement mechanism used on an interface. The value is set through the **ptp delay-mechanism** command.
Ann-timeout	Timeout interval for waiting the Announce message. The value is set through the **ptp announce receipt-timeout** command.
Type	Type of an interface, which is usually the same as the type of the device. If the device type is TCandBC, the value is set through the **ptp port-type** command.

Item	Description
Domain	The clock domain of an interface should be the same as the device type. If the device type is TCandBC, the clock domain of the interface is set by the **ptp domain** command.
Clock source info	
Clock	Clock source.
Pri1	Priority1 of the clock source. The value is set through the **ptp clock-source** command.
Pri2	Priority2 of the clock source. The value is set through the **ptp clock-source** command.
Accuracy	Accuracy of the clock source. The value is set through the **ptp clock-source** command.
Class	Class of the clock source. The value is set through the **ptp clock-source** command.
TimeSrc	Time source of the clock source. The value is set through the **ptp clock-source** command.
In-Status	Whether the clock source is normal.
Port State	Port state.
Port Number	Port number of the clock source.
Recv Packet Statistics	Received packet statistics.
Send Packet Statistics	Sent packet statistics.
Discard Packet Statistics	Discarded packet statistics.

3.14.3 display ptp utc

Function

The **display ptp utc** command displays the Universal Time Coordinated (UTC) time.

Format

display ptp utc [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the UTC time based on a slot ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

UTC is also called the Greenwich Mean Time (GMT). The time displayed on the PTP device must be the UTC time.

The command is used to view the synchronization status of the UTC time. After two devices are synchronized, the UTC time should be the same.

The PTP supports two types of time scales: ARB and PTP.

- When the ARB time scale is used, the time can start from any time point and be reset by the management process. The slave clock obtains only the offset between the UTC time and TAI time in seconds. Therefore, the ARB time scale is used only to transmit the offset of the PTP time.
- When the PTP time scale is used, the system time is the UTC time adjusted according to *utc-offset*.

  The origin of the PTP time scale is 00:00:00 of January 1, 1970. The formula for converting the TAI time to the UTC time is: UTC = TAI - *utc-offset*. The *utc-offset* parameter indicates the accumulated offset between the current UTC and the TAI.

Example

Display the UTC time.

```
<HUAWEI> display ptp utc
Non-UTC Time:2009-12-30  20:43:39
```

Table 3-181 Description of the display ptp utc command output

Item	Description
Non-UTC Time	Non-standard UTC time converted according to the ARB time.

3.14.4 ptp announce-drop enable

Function

The **ptp announce-drop enable** command configures the interface of the PTP device to discard Announce messages.

The **undo ptp announce-drop enable** command restores the default mode of processing Announce messages on the interface of the PTP device.

By default, Announce messages are not discarded.

Format

ptp announce-drop enable

undo ptp announce-drop enable

Parameters

None.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Announce messages are advertisement messages in PTP, which are used to establish the master-slave hierarchy between devices. If the interface discards Announce messages, the device where the interface resides cannot receive clock synchronization information from other PTP devices. Usually, the **ptp announce-drop enable** command is configured on the interface at the user side to prevent the interface from receiving and processing Announce messages. This saves system resources.

Example

Configure the mode of processing Announce messages on XGigabitEthernet1/0/1 of the PTP device to **discard**.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 1/0/1
[HUAWEI-XGigabitEthernet1/0/1] ptp announce-drop enable
```

3.14.5 ptp announce-interval

Function

The **ptp announce-interval** command sets the interval for sending Announce packets on an interface of the PTP device.

The **undo ptp announce-interval** command restores the default interval for sending Announce packets on the interface of the PTP device.

By default, the interval for sending Announce packets is 128 ms.

Format

ptp announce-interval *announce-interval*

undo ptp announce-interval

Parameters

Parameter	Description	Value
announce-interval	Indicates that the interval for sending Announce packets on the interface is set to the *n*th power of 2 in milliseconds, where *n* is specified by *announce-interval*.	The value is an integer that ranges from 0 to 20. By default, the interval is 7 (128 ms).

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Announce messages are advertisement messages in PTP, which are used to establish the master-slave hierarchy between devices. Announce packets ensure the exchange of clock synchronization information between PTP devices. If the value of the *announce-interval* is too small, devices frequently exchange PTP packets, which consume excessive bandwidth; if the value of the *announce-interval* is too great, the clock synchronization accuracy cannot be guaranteed. Therefore, while the clock synchronization accuracy is ensured, you should set the *announce-interval* to a larger value.

Example

Set the interval for sending Announce packets on XGigabitEthernet0/0/1 of the PTP device to 256 ms.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp announce-interval 8
```

3.14.6 ptp announce receipt-timeout

Function

The **ptp announce receipt-timeout** command configures the maximum timeout times of receiving Announce messages on an interface.

The **undo ptp announce receipt-timeout** command restores the default maximum timeout times of receiving Announce messages on an interface.

By default, the maximum timeout times of receiving Announce messages is 3.

Format

ptp announce receipt-timeout *timeout-value*

undo ptp announce receipt-timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the maximum timeout times of receiving Announce messages.	The value is an integer that ranges from 2 to 255. The default value is **3**.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Announce messages are advertisement messages in PTP, which are used to establish the master-slave hierarchy between devices. When the maximum timeout times of receiving Announce messages on an interface exceeds the specified threshold:

- In dynamic clock source selection: The local device configures the status of the 1588v2 interface as non-slave. That is, the 1588v2 interface does not synchronize the time with other devices.
- In static clock source selection: The 1588v2 interface status remains unchanged.

Timeout interval for receiving Announce messages on the local interface = Maximum timeout times of receiving Announce messages on the local interface (receipt-timeout) x Interval for sending Announce messages to the peer device (announce-interval) The interval for sending Announce messages to the peer device (announce-interval) is set using the **ptp announce-interval** *announce-interval* command.

If you run this command multiple times, only the latest configuration takes effect.

Example

Set the maximum timeout times of receiving Announce messages on XGigabitEthernet0/0/1 of the PTP device to 4.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp announce receipt-timeout 4
```

3.14.7 ptp asymmetry-correction

Function

The **ptp asymmetry-correction** command sets the delay offset value to ensure accurate time synchronization.

The **undo ptp asymmetry-correction** command restores the default delay offset.

By default, the asymmetry correction value of the PTP packet sent from the interface is not configured.

Format

ptp asymmetry-correction { **positive** | **negative** } *asymmetry-correction*

undo ptp asymmetry-correction

Parameters

Parameter	Description	Value
positive *asymmetry-correction*	Indicates the positive asymmetry correction value.	The value is an integer that ranges from 0 to 2000000, in ns. The default value is 0.
negative *asymmetry-correction*	Indicates the negative asymmetry correction value.	The value is an integer that ranges from 0 to 2000000, in ns. The default value is 0.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

In case of path delay calculation, PTP measures the packet sending path only and considers the delays for sending and receiving packets as the same by default.

If the two delays are different or asymmetric, you need to configure an asymmetry correction value. In this case, the device automatically considers the asymmetry correction value in the path delay calculation complying with the Pdelay or Delay measurement mechanism.

Example

Set the delay offset value to 1 ns on XGigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp asymmetry-correction positive 1
```

3.14.8 ptp clock-source

Function

The **ptp clock-source** command sets the attributes of the clock source and time source.

The **undo ptp clock-source** command cancels the settings.

For default values of the parameters, see the parameter description.

Format

ptp clock-source local { **clock-accuracy** *clock-accuracy* | **clock-class** *clock-class* | **priority1** *priority1* | **priority2** *priority2* | **time-source** *time-source* } **slot** *slot-id*

undo ptp clock-source local { **clock-accuracy** | **clock-class** | **priority1** | **priority2** | **time-source** } **slot** *slot-id*

NOTE

After G.8275.1 is enabled, only the **priority2** *priority2* and **time-source** *time-source* parameters are supported.

Parameters

Parameter	Description	Value
local	Indicates the local clock.	-

Parameter	Description	Value
clock-accuracy *clock-accuracy*	Specifies an attribute defining the accuracy of a clock.	The value of *clock-accuracy* is a hexadecimal number that is in the range of 0 to FF. You can set the value to 20-31 or 80-FD. The default accuracy of the local clock is 31. The accuracy values mapping the values of *clock-accuracy-value* are as follows: ● 20: The time is accurate to within 25 ns. ● 21: The time is accurate to within 100 ns. ● 22: The time is accurate to within 250 ns. ● 23: The time is accurate to within 1 us. ● 24: The time is accurate to within 2.5 us. ● 25: The time is accurate to within 10 us. ● 26: The time is accurate to within 25 us. ● 27: The time is accurate to within 100 us. ● 28: The time is accurate to within 250 us. ● 29: The time is accurate to within 1 ms. ● 2A: The time is accurate to within 2.5 ms.

Parameter	Description	Value
		• 2B: The time is accurate to within 10 ms. • 2C: The time is accurate to within 25 ms. • 2D: The time is accurate to within 100 ms. • 2E: The time is accurate to within 250 ms. • 2F: The time is accurate to within 1s. • 30: The time is accurate to within 10s. • 31: The time is accurate to more than 10s. • 80 to FD: reserved for PTP features.

Parameter	Description	Value
clock-class *clock-class*	Specifies the attribute of an ordinary or boundary clock denotes the traceability of the time or frequency distributed by the grandmaster clock, that is the capability to trace the International Atomic Time (TAI).	The value of *clock-class* is an integer that ranges from 0 to 255. The default value of the local clock is 187. The capabilities to trace the TAI mapping the values of *clock-class-value* are as follows: ● 0, 9, and 10: reserved to enable compatibility with future versions. ● 1-5, 8, 11-12, 15-51, 53-57, 59-67, 123-127, 128-132, 171-186, 188-192, 194-215, 233-247, 249-250, 252-254: reserved. ● 68-122, 133-170, 216-232: used by alternate PTP profiles. ● 6: a clock that is synchronized to a primary reference time source. The timescale distributed is PTP. A clock of class 6 cannot be a slave to another clock in the domain. ● 7: a clock that has previously been designated as class 6 but that has lost the capability to synchronize to a primary reference time source. The PTP system enters the holdover state and does not perform best clock source selection. The timescale distributed is PTP. A clock of class 7 cannot be a slave to

Parameter	Description	Value
		another clock in the domain. - 13: a clock that is synchronized to an application specific source of time. The timescale distributed is ARB. A clock of class 13 cannot be a slave to another clock in the domain. - 14: a clock that has previously been designated as class 13 but that has lost the capability to synchronize to an application specific source of time. The clock is in holdover mode and within holdover specifications. The timescale distributed is ARB. A clock of class 14 cannot be a slave to another clock in the domain. - 52: Degradation alternative A for a clock of class 7 that is not within holdover specification. A clock of class 52 cannot be a slave to another clock in the domain. - 58: Degradation alternative A for a clock of class 14 that is not within holdover specification. A clock of class 58 cannot be a slave to another clock in the domain. - 187: Degradation alternative B for a clock of class 7 that is not within holdover specification. A clock

Parameter	Description	Value
		of class 187 can be a slave to another clock in the domain. - 193: Degradation alternative B for a clock of class 14 that is not within holdover specification. A clock of class 193 can be a slave to another clock in the domain. - 248: This clock class is used if none of the other clock class definitions apply. - 251: Reserved for version 1 compatibility. - 255: clock class of a slave-only clock.
priority1 *priority1*	Specifies a user configurable designation that a clock belongs to an ordered set of clocks from which a master is selected. The attribute priority1 is used in the execution of the best master clock algorithm.	The value of *priority1* is an integer that ranges from 0 to 255. The default value is 128. Lower values take precedence.
priority2 *priority2*	Specifies a user configurable designation that provides finer grained ordering among otherwise equivalent clocks. The attribute priority2 is used in the execution of the best master clock algorithm.	The value of *priority2* is an integer that ranges from 0 to 255. The default value is 128. Lower values take precedence.

Parameter	Description	Value
time-source *time-source*	Specifies the source of time used by the grandmaster clock.	The value of *time-source* is an integer that ranges from 1 to 8. The default value of the local clock is 8 (INTERNAL_OSCILLATOR). The attributes mapping the values of *time-source-value* are as follows: - 1: (0x10) ATOMIC_CLOCK - 2: (0x20) GPS - 3: (0x30) TERRESTRIAL_RADIO - 4: (0x40) PTP - 5: (0x50) NTP - 6: (0x60) HAND_SET - 7: (0x90) OTHER - 8: (0xa0) INTERNAL_OSCILLATOR
slot *slot-id*	Specifies the slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **time-source** parameter specifies the clock source attribute used by the grandmaster clock device and the value is set according to the clock source connected to the device.

When the BMC algorithm is used by the PTP device for master clock selection, **priority1** > **clock-class** > **clock-accuracy** > **priority2** of each candidate time source is compared first. If the **priority1** of candidate time sources is the same, **clock-class** is compared, **clock-accuracy** and **priority2**. The time source with the highest priority is selected as the master clock.

A smaller *clock-class* value indicates a higher clock class. When the *clock-class* of a device is smaller than 128, the device cannot function as a slave clock. Therefore, do not set a high *clock-class* for a slave clock. Otherwise, the PTP interface of the slave clock cannot enter the slave state, and the device cannot synchronize with the master clock.

Example

Configure the time source of the local clock to ATOMIC_CLOCK.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local time-source 1 slot 0
```

Set priority 1 of the local clock to 1.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local priority1 1 slot 0
```

Set priority 2 of the local clock to 1.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local priority2 1 slot 0
```

Set the class of the local clock to 10.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local clock-class 10 slot 0
```

Set the accuracy of the local clock to 31 (accurate to >10s).

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local clock-accuracy 31 slot 0
```

3.14.9 ptp clock-source local local-priority

Function

The **ptp clock-source local local-priority** command sets the local priority for a local PTP clock source or an external clock source.

The **undo ptp clock-source local local-priority** command restores the default local priority of a local or external clock source.

By default, the local priority of a local PTP clock source or an external clock source is 128.

Format

ptp clock-source local local-priority *local-priority-value* **slot** *slot-id*

undo ptp clock-source local local-priority slot *slot-id*

Parameters

Parameter	Description	Value
local-priority *local-priority-value*	Specifies a local priority.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

According to the BMC algorithm in G.8275.1, when the local or external clock source competes with a line clock source and other attributes are the same, the two clock sources are compared against the local priority. The clock source with a lower local priority is preferentially selected.

Example

Set the local priority of a local PTP clock source to 120.

```
<HUAWEI> system-view
[HUAWEI] ptp clock-source local local-priority 120 slot 0
```

3.14.10 ptp clock-step

Function

The **ptp clock-step** command specifies the mode in which PTP packets that are used by PTP devices to perform time synchronization are timestamped.

The **undo ptp clock-step** command resets the mode in which PTP packets that are used by PTP devices to perform time synchronization are timestamped.

By default, the mode in which PTP packets are timestamped is **one-step**.

Format

ptp clock-step { **one-step** | **two-step** }

undo ptp clock-step

Parameters

Parameter	Description	Value
one-step	Indicates the one-step clock mode. In one-step clock mode, Sync messages in Delay mode and Pdelay_Resp messages in Pdelay mode are stamped with the time when they are sent.	-
two-step	Indicates the two-step clock mode. In two-step clock mode, Sync messages in Delay mode and Pdelay_Resp messages in Pdelay mode only record the time when they are generated, but carry no timestamps. The timestamps are carried in subsequent messages, that is, Follow_Up or Pdelay_Resp_Follow_Up messages.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device adopts the one-step mode to timestamp outgoing PTP messages to communicate with other devices, and identify received Follow_Up messages in **two-step** mode. In this way, an interface in one-step clock mode can communicate with another interface in two-step clock mode.

Precautions

After the PTP device type is set to **e2etc**, **e2etcoc**, **p2ptc**, or **p2ptcoc** using the **ptp device-type**, the mode in which PTP messages are timestamped cannot be changed to **two-step** using the **ptp clock-step** command.

Example

Configure the two-step clock mode on XGigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp clock-step two-step
```

3.14.11 ptp delay-mechanism

Function

The **ptp delay-mechanism** command configures the delay measurement mechanism applied on the interface of a PTP device.

The **undo ptp delay-mechanism** command deletes the delay measurement mechanism applied on the interface of the PTP device.

By default, the delay measurement mechanism is only configured on the P2P transparent clock (P2PTC), E2E transparent clock (E2ETC), P2P transparent clock and ordinary clock (P2PTCOC), and E2E transparent clock and ordinary clock (E2ETCOC).

Format

ptp delay-mechanism { **delay** | **pdelay** }

undo ptp delay-mechanism

Parameters

Parameter	Description	Value
delay	Indicates that the delay measurement mechanism applied on the interface is in Delay mode.	-
pdelay	Indicates that the delay measurement mechanism applied on the interface is in Pdelay mode.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

PTP supports two delay measurement mechanisms:

- Delay request-response end to end (E2E) mechanism: calculates the time difference based on the total delay of the link between the master and slave clocks.
- Peer delay peer to peer (P2P) mechanism: calculates the time difference based on the delay of each link between the master and slave clocks.

In the P2P mechanism, the link delay of each interface must be measured separately. Different from the E2E mechanism, the P2P mechanism calculates and accumulates the forwarding delay and link delay to ensure accurate clock synchronization. If the master and slave clocks are far from each other and there are many TCs, the P2P mechanism will greatly reduce the clock synchronization efficiency and affect the clock synchronization effect. Therefore, when there is only one or two TCs, the P2P mechanism is recommended. When there are three or more TCs, the E2E mechanism is recommended.

Precautions

- OC and BC interfaces must be configured with the delay measurement mechanism before PTP is enabled.
- If the delay measurement mechanism is configured on an interface, to configure another delay measurement mechanism, you need to cancel the original configuration first.
- The corresponding delay measurement mechanism is applied on the E2ETC, E2ETCOC, P2PTC, P2PTCOC by default and cannot be modified; therefore, PTP can be directly enabled on interfaces of these devices.

Example

Configure the mode of the delay measurement mechanism of XGigabitEthernet0/0/1 on the PTP device as Delay.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type bc
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp delay-mechanism delay
```

3.14.12 ptp device-type

Function

The **ptp device-type** command configures the device type of a PTP device.

The **undo ptp device-type** command cancels the setting of the device type of a PTP device.

By default, the device type is not configured on a PTP device.

Format

ptp device-type { **bc** | **oc** | **e2etc** | **e2etcoc** | **p2ptc** | **p2ptcoc** | **tcandbc** | **t-bc** } **slot** *slot-id*

undo ptp device-type slot *slot-id*

NOTE

After G.8275.1 is enabled, only the **t-bc** parameter is supported.

Parameters

Parameter	Description	Value
oc	Indicates the ordinary clock (OC). An OC device has only one interface in the PTP domain, through which the local clock synchronizes with the upstream clock or advertises the time to the downstream clock.	-
bc	Indicates the boundary clock (BC). A BC device has multiple interfaces in the PTP domain. One of these interfaces synchronizes time from the upstream device, and the other interfaces advertise the time to the downstream device.	-
e2etc	Indicates the end to end transparent clock (E2ETC). A TC device does not participate in the calculation of the PTP clock and only transparently transmits PTP packets.	-
p2ptc	Indicates that the peer to peer transparent clock (P2PTC).	-
e2etcoc	Indicates the end to end transparent ordinary clock (E2ETCOC). A TCOC device is a special TC node. It synchronizes time in the same way as a TC device and can synchronize the clock frequency with the upstream device according to PTP packets.	-
p2ptcoc	Indicates the peer to peer transparent ordinary clock (P2PTCOC).	-
tcandbc	Indicates the transparent boundary clock.	-
t-bc	Indicates the telecom boundary clock.	-
slot *slot-id*	Specifies the ID of the slot where the PTP device resides.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each device can be configured with only one device type.

The PTP functions and parameters are not affected when you change the device type of the device. The device supports the following functions to simplify the configuration:

- Conversion between the BC, OC, and TCandBC modes
- Conversion between the E2ETC, P2PTC, E2ETCOC, and P2PTCOC modes

The PTP functions and parameters are not affected when you change the device type of the device. Before changing the device type, make sure that the conditions of the new device type are met. For example:

- To change the device type from BC or TCandBC to OC, make sure that the conditions of the OC are met, that is, PTP is enabled on only one interface. Otherwise, the following error information is displayed:
- To change the device type from OC to BC, make sure that the device is not in slave-only state. Otherwise, the following error information is displayed:
- To change the device type from E2ETCOC or P2PTCOC to E2ETC or P2PTC, make sure that no PTP-related configuration exists on the OC interface of the TCOC device. Otherwise, the following error information exists:
- If the original device type is TCandBC and the type of an interface is set to TC, when you switch the device type to OC or BC, the following error information is displayed:
- If the original device type is E2ETC or P2PTC, you can switch the device type to only E2ETCOC, or P2PTCOC. Otherwise, the following error information is displayed:

You set the device type of the PTP device and enable PTP on the device in a random sequence.

Precautions

- Running the **undo ptp device-type** command will clear the PTP configuration in the interface view. If the PTP device type is OC and the **ptp slaveonly slot** *slot-id* command is configured, running the **undo ptp device-type** command will also clear the **ptp slaveonly slot** *slot-id* command configuration. Exercise caution when running the **undo ptp device-type** command.
- When the device type of the device is set to TC, TCOC, or TCandBC (the interface type is TC):
  - Ensure that PTP packets are forwarded at the service layer. For example, on a ring network, you need to use ring network protocols to remove loops at the service layer.
  - On the TC device, the interfaces for receiving and sending PTP packets must be enabled with PTP. Otherwise, the resident time of the device cannot be calculated correctly. In this case, only packets are forwarded.
  - To ensure PTP time synchronization, ensure that PTP packets are first forwarded when the interface reaches the maximum rate.
- After the mode in which PTP messages are timestamped is changed to **two-step** using the **ptp clock-step** command, the **ptp device-type** command

cannot be used to configure the PTP device type to **e2etc**, **e2etcoc**, **p2ptc**, or **p2ptcoc**.

Example

Set the PTP device type to OC.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type oc
```

3.14.13 ptp domain

Function

The **ptp domain** command configures the domain where the PTP device resides.

The **undo ptp domain** command restores the domain where the PTP device resides to the default value.

By default, the domain where the PTP device resides is PTP domain 0.

Format

ptp domain *domain-value*

undo ptp domain

Parameters

Parameter	Description	Value
domain-value	Specifies the domain that the clock source belongs to.	The value is an integer that ranges from 0 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A physical time synchronization network can be logically divided into multiple clock domains. Each clock domain has a synchronization time, to which all devices in the domain are synchronized. Different clock domains have their own synchronization time, which is independent from each other.

Example

Set the value of the domain where the PTP device resides to 4.

```
<HUAWEI> system-view
[HUAWEI] ptp domain 4
```

3.14.14 ptp enable (interface view)

Function

The **ptp enable** command enables PTP on a certain interface of the device.

The **undo ptp enable** command disables PTP on a certain interface of the device.

By default, PTP is not enabled on the interface of the device.

Format

ptp enable

undo ptp enable

Parameters

None

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After PTP is enabled globally, enable PTP on an interface so that PTP can take effect.

Precautions

- Before enabling PTP, ensure that the interface supports PTP.
- The management interface and the sub interface cannot be enabled with PTP.

Pre-configuration tasks

- Before enabling PTP on an interface, you must run the **ptp device-type** command in the system view to set the device type.
- You must use the **ptp port-type** command to configure the clock mode of an interface on the TCandBC device.
- On the OC device, only one interface can be enabled with PTP.
- On the OC or BC device, you must use the **ptp delay-mechanism** command to configure the delay mechanism before enabling PTP.

Example

Enable PTP on XGigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type bc slot 0
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp delay-mechanism delay
[HUAWEI-XGigabitEthernet0/0/1] ptp enable
```

3.14.15 ptp enable (system view)

Function

The **ptp enable** command enables PTP on the device.

The **undo ptp enable** command disables PTP on the device.

By default, PTP is disabled globally.

Format

ptp enable

undo ptp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before using PTP, run the **ptp enable** command in the system view to enable PTP globally.

The **undo ptp enable** command will disable PTP and make all the PTP configuration become ineffective. To use PTP, reconfigure PTP.

Example

Enable PTP globally.

```
<HUAWEI> system-view
[HUAWEI] ptp enable
```

3.14.16 ptp local-priority

Function

The **ptp local-priority** command configures the local priority of a G.8275.1 interface.

The **undo ptp local-priority** command restores the default local priority of a G.8275.1 interface.

By default, the local priority of a G.8275.1 interface is 128.

Format

ptp local-priority *local-priority-value*

undo ptp local-priority [*local-priority-value*]

Parameters

Parameter	Description	Value
local-priority-value	Specifies the local priority of a G.8275.1 interface.	The value is an integer that ranges from 1 to 255.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

According to the BMC algorithm in G.8275.1:

- When two line clock sources are compared and other attributes the same, the interface with a lower local priority is preferentially selected.
- When the local or external clock source competes with a line clock source and other attributes are the same, the two clock sources are compared against the local priority. The clock source with a lower local priority is preferentially selected.

Example

Set the local priority of a local G.8275.1 clock source to 120.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp local-priority 120
```

3.14.17 ptp mac-egress

Function

The **ptp mac-egress** command configures the MAC encapsulation mode for the PTP packets.

The **undo ptp mac-egress** command restores the default MAC encapsulation mode.

By default, PTP packets are encapsulated in MAC multicast mode and do not carry any VLAN tag.

Format

ptp mac-egress { **destination-mac** *destination-mac* | **vlan** *vlan-id* [**priority** *priority-value*] }

undo ptp mac-egress { **destination-mac** | **vlan** [**priority**] }

NOTE

In G.8275.1 mode, only the **destination-mac** *destination-mac* parameter is supported.

Parameters

Parameter	Description	Value
destination-mac *destination-mac*	Indicates the destination MAC address of the PTP packet. If the destination MAC address is not configured, the PTP packet is encapsulated in multicast mode by default and does not carry any VLAN tag.	The value is in the format of H-H-H. An H contains one to four hexadecimal numbers.
vlan *vlan-id*	Specifies the VLAN ID of PTP messages.	The value is an integer that ranges from 1 to 4094.
priority *priority-value*	Specifies the priority of VLAN packets.	The value is an integer that ranges from 0 to 7. The default value is 7, indicating the highest priority.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

You can configure the encapsulation mode for packets based on the Layer 2 network types of devices. If a device resides on a Layer 2 unicast network, configure a MAC address for the device. If a device resides on a multicast network, no MAC address needs to be configured for the device because a default multicast MAC address is defined.

Table 3-182 Default multicast MAC address for delay and Pdelay measurement mechanisms

Packet Type	MAC Address
All except peer delay measurement mechanisms	011B-1900-0000
Peer delay measurement mechanism	0180-C200-000E

Precautions

- This command is invalid for transparently transmitted packets.
- The MAC address cannot be 0000-0000-0000.
- Before configuring MAC encapsulation, delete the UDP encapsulation configuration if UDP encapsulation has been configured.
- MAC encapsulation is required when the VLAN ID to be encapsulated to sent or received packets is configured.
- After G.8275.1 is configured, only the default multicast MAC addresses 011B-1900-0000 and 0180-C200-000E can be configured.

Example

Configure the unicast MAC encapsulation for the PTP packet.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp mac-egress destination-mac 001B-1911-1100
```

Configure the multicast MAC encapsulation for the PTP packet.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp mac-egress vlan 2 priority 2
```

3.14.18 ptp min-delayreq-interval

Function

The **ptp min-delayreq-interval** command sets the minimum interval for sending Delay_Req messages on a 1588v2 interface.

The **undo ptp min-delayreq-interval** command restores the default minimum interval for sending Delay_Req messages on a 1588v2 interface.

By default, the minimum interval for sending 1588v2 Delay_Req messages on a 1588v2 interface is 128 ms, and the minimum interval for sending G.8275.1 Delay_Req messages on a 1588v2 interface is 64 ms.

Format

ptp min-delayreq-interval *min-delayreq-interval*

undo ptp min-delayreq-interval

Parameters

Parameter	Description	Value
min-delayreq-interval	Specifies that the minimum interval for sending Delay_Req messages on a 1588v2 interface is set to the min-pdelayreq-intervalth power of 2, in milliseconds.	The value is an integer that ranges from 0 to 20. In 1588v2 mode, the default value is 7, namely, 128 ms. In G.8275.1 mode, the default value is 6, namely, 64 ms. **Table 3-183** shows the mapping between the *min-delayreq-interval* value and the actual sending interval.

Table 3-183 Mapping between the *min-delayreq-interval* value and the actual sending interval

Value of min-delayreq-interval	Actual Interval
0	1 ms
1	2 ms
2	4 ms
3	8 ms
4	16 ms
5	32 ms
6	64 ms
7	128 ms
8	256 ms

Value of min-delayreq-interval	Actual Interval
9	512 ms
10	1s
11	2s
12	4s
13	8s
14	16s
15	32s
16	64s
17	128s
18	256s
19	512s
20	1024s

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

During 1588v2 clock synchronization, an Announce message is sent to determine the master-slave hierarchy, where the upstream node that advertises the synchronization time is the master device and the downstream node that receives the synchronization time is called the slave device. The master device sends Sync messages to the slave device to transmit performance parameters of time signals. In addition, the delay measurement mechanism can be implemented to ensure the accuracy of time signals.

Because the delay varies according to the network link, the 1588v2 time signals may be inaccurate. During 1588v2 clock synchronization, delay and Pdelay messages are transmitted to measure link delay, and time signals can be corrected based on the link delay. During the delay measurement request process, the local device sends a Delay_Req message and the peer device replies with a Delay_Resp message. There are two types of delay measurement mechanism.

- **delay**: specifies a delay request-response mechanism, in which information about the clock and time is calculated according to the delay of the entire link between the PTP device and the clock source. In this mode, the slave device sends a Delay_Req message to the master device, and the slave device corrects time signals based on the Delay_Resp message replied by the master device.

- **pdelay**: specifies a peer delay mechanism, in which information about the time and clock is calculated according to the delay of each segment of the link between the PTP device and the clock source. In this mode, the slave device and master device exchange Pdelay_Req messages and time signals are corrected based on the Pdelay_Resq messages replied.

If *min-delayreq-interval* is set to a small value, PTP devices frequently exchange Delay_Req messages, occupying many bandwidth resources. If *min-delayreq-interval* is set to a large value, high-precision clock synchronization cannot be guaranteed. If the required clock synchronization accuracy is guaranteed, set *min-delayreq-interval* to a large value.

Example

Set the minimum interval for sending Delay_Req messages on the 1588v2 interface XGigabitEthernet 0/0/1 to 256 ms.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp min-delayreq-interval 8
```

3.14.19 ptp min-pdelayreq-interval

Function

The **ptp min-pdelayreq-interval** command configures the minimum interval for sending Pdelay_Req messages on a 1588v2 interface.

The **undo ptp min-pdelayreq-interval** command restores the default minimum interval for sending Pdelay_Req messages on a 1588v2 interface.

By default, the minimum interval for sending Pdelay_Req message is 128 ms.

Format

ptp min-pdelayreq-interval *min-pdelayreq-interval*

undo ptp min-pdelayreq-interval

Parameters

Parameter	Description	Value
min-pdelayreq-interval	Specifies that the minimum interval for sending Pdelay_Req messages on a 1588v2 interface is set to the **min-pdelayreq-interval** power of 2, in milliseconds.	The value is an integer that ranges from 0 to 20. The default value is 7, that is, 128 milliseconds. **Table 3-184** lists the mapping between the **min-pdelayreq-interval** value and the actual sending interval.

Table 3-184 Mapping between the **min-pdelayreq-interval** value and the actual sending interval

Value of min-pdelayreq-interval	Actual Interval
0	1 ms
1	2 ms
2	4 ms
3	8 ms
4	16 ms
5	32 ms
6	64 ms
7	128 ms
8	256 ms
9	512 ms
10	1s
11	2s
12	4s
13	8s
14	16s
15	32s
16	64s
17	128s
18	256s
19	512s
20	1024s

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During 1588v2 clock synchronization, an Announce message is sent to determine the master-slave hierarchy, where the upstream node that advertises the synchronization time is the master device and the downstream node that receives the synchronization time is called the slave device. The master device sends Sync messages to the slave device to transmit performance parameters of time signals. In addition, the delay measurement mechanism can be implemented to ensure the accuracy of time signals.

Because the delay varies according to the network link, the 1588v2 time signals may be inaccurate. During 1588v2 clock synchronization, delay and Pdelay messages are transmitted to measure link delay, and time signals can be corrected based on the link delay. During the delay measurement request process, the local device sends a Delay_Req message and the peer device replies with a Delay_Resp message. There are two types of delay measurement mechanism.

- **delay**: specifies a delay request-response mechanism, in which information about the clock and time is calculated according to the delay of the entire link between the PTP device and the clock source. In this mode, the slave device sends a Delay_Req message to the master device, and the slave device corrects time signals based on the Delay_Resp message replied by the master device.
- **pdelay**: specifies a peer delay mechanism, in which information about the time and clock is calculated according to the delay of each segment of the link between the PTP device and the clock source. In this mode, the slave device and master device exchange Pdelay_Req messages and time signals are corrected based on the Pdelay_Resq messages replied.

If *min-pdelayreq-interval* is set to a small value, PTP devices frequently exchange Pdelay_Req messages, occupying many bandwidth resources. If *min-pdelayreq-interval* is set to a large value, high-precision clock synchronization cannot be guaranteed. If the required clock synchronization accuracy is guaranteed, set *min-pdelayreq-interval* to a large value.

Example

Set the minimum interval for sending Pdelay_Req messages on the 1588v2 interface XGigabitEthernet 0/0/1 to 128 ms.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp min-pdelayreq-interval 7
```

3.14.20 ptp notslave disable

Function

The **ptp notslave disable** command configures the notslave attribute of a G. 8275.1 interface as false.

The **undo ptp notslave disable** command restores the default notslave attribute of a G.8275.1 interface as true.

By default, the notslave attribute of a G.8275.1 interface is set to true.

Format

ptp notslave disable

undo ptp notslave disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the notslave attribute of a G.8275.1 interface, run the **ptp notslave disable** command. If the notslave attribute of a G.8275.1 interface is true, the G. 8275.1 interface will never work in the slave state. If the notslave attribute of a G. 8275.1 interface is false, the G.8275.1 interface can be in the slave state.

Prerequisites

The PTP device complies with the G.8275.1 profile.

Example

Set the nontslave attribute of a G.8275.1 interface to false.

```
<HUAWEI> system-view
[HUAWEI] ptp notslave disable
```

3.14.21 ptp port-state

Function

The **ptp port-state** command statically configures the status of a PTP interface.

The **undo ptp port-state** command restores the default status of a PTP interface.

By default, a statically specified PTPT interface is in the initializing state.

Format

ptp port-state { **slave** | **passive** | **master** | **premaster** | **listening** | **faulty** | **disabled** | **initializing** }

undo ptp port-state

Parameters

Parameter	Description	Value
slave	Configures the PTP interface status as slave. A slave interface traces external time information. A PTP device can be configured with only one slave interface.	-
passive	Configures the PTP interface status as passive. A passive PTP interface neither traces external time information nor advertises time information. A passive interface can send Pdelay_Req, Pdelay_Resp, delay_Resp_Follow_Up, and signaling messages as well as respond to management messages. If multiple PTP interfaces are detected as master devices in a domain, the PTP interface with the highest priority is selected as the master device and the local interface connected to this PTP interface is in the slave state. In this case, other local interfaces are in the passive state and back up the slave interface.	-
master	Configures the PTP interface status as master. A master PTP interface advertises time information to other devices.	-
premaster	Configures the PTP interface status as premaster. A premaster PTP interface neither traces external time information nor advertises time information. A premaster interface can send Pdelay_Req, Pdelay_Resp, delay_Resp_Follow_Up, and signaling messages as well as respond to management messages.	-
listening	Configures the PTP interface status as listening. A listening PTP interface neither traces external time information nor advertises time information. If a device originally functioning as a master clock is configured to be an OC working in slaveonly mode, or if the device becomes faulty, the status of the PTP interface on the device changes from master to listening.	-
faulty	Configures the PTP interface status as faulty. A faulty interface can only respond to some management messages on a link, instead of sending other PTP messages.	-
disabled	Configures the PTP interface status as disabled. A disabled PTP interface cannot send PTP messages, and discards all PTP messages except for management messages. The disabled status of a PTP interface equals to disabling the PTP function from the interface using the **undo ptp enable** command in the interface view.	-
initializing	Configures the PTP interface status as initializing. An initializing PTP interface initializes the data set, hardware information, and communication device information. In case of an initializing PTP interface, all interfaces on the clock node are prohibited from sending PTP messages.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Static clock source selection and dynamic BMC clock source selection are two independent sets of clock source selection mechanism. The priority of static clock source selection is higher than that of dynamic BMC clock source selection. You can fix the master-slave relationship between clock nodes within a network by statically configuring the status of PTP interfaces on them. In this way, the reference clock source is not selected through BMC algorithm.

Example

Configure the PTP interface to be in the slave state.

```
<HUAWEI> system-view
[HUAWEI] ptp set-port-state enable
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp port-state slave
```

3.14.22 ptp port-type

Function

The **ptp port-type** command configures the clock mode of an interface on a TCandBC device.

The **undo ptp port-type** command deletes the clock mode configured on the interface on a TCandBC device.

By default, the PTP clock mode is not configured on the interface.

Format

ptp port-type { **bc** | **tc** }

undo ptp port-type

Parameters

Parameter	Description	Value
bc	Indicates that the clock mode configured on the interface of the TCandBC is BC.	-

Parameter	Description	Value
tc	Indicates that the clock mode configured on the interface of the TCandBC is TC.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

The device supports the TCandBC clock mode. In this case, you can configure the clock mode of the interface to TC or BC. If the original clock mode of the interface is BC or OC, and the interface is enabled with PTP, the clock mode of the interface changes to BC after the device clock mode is changed to TC and BC mode.

Precautions

- This command is invalid when G.8275.1 is enabled.
- If the interface is enabled with PTP, the **ptp port-type** command is invalid.
- Before delete the clock mode of the interface of the TCandBC device, you must first clear the clock domain of the interface, if the clock mode is TC and the clock domain of the interface is configured.

Example

Configure the clock mode of XGigabitEthernet0/0/1 interface on the TCandBC device to BC.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type tcandbc
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp port-type bc
```

3.14.23 ptp profile g-8275-1 enable

Function

The **ptp profile g-8275-1 enable** command configures PTP to comply with ITU-T G.8275.1.

The **undo ptp profile g-8275-1 enable** command cancels configuring PTP to comply with ITU-T G.8275.1. That is, PTP complies with IEEE 1588v2.

By default, PTP complies with IEEE 1588v2.

Format

ptp profile g-8275-1 enable

undo ptp profile g-8275-1 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

ITU-T G.8275.1 is a new PTP protocol designed for the telecom domain. To switch the 1588v2 profile to the G.8275.1 profile, run the **ptp profile g-8275-1 enable** command. To switch the G.8275.1 profile to the 1588v2 profile, run the **undo ptp profile g-8275-1 enable** command.

Configuration Impact

After the ITU-T G.8275.1 profile is configured, all the configurations related to IEEE 1588v2 in the system view and interface view are deleted, and the PTP configurations are restored to the default values. In addition, the default values of value ranges of the **domain**, **sync-interval**, and **delayreq-interval** parameters are changed. However, the function to globally enable PTP (using the **ptp enable** command) is not affected.

Example

Configure the ITU-T G.8275.1 profile.

```
<HUAWEI> system-view
[HUAWEI] ptp profile g-8275-1 enable
```

3.14.24 ptp set-port-state enable

Function

The **ptp set-port-state enable** command enables the function to statically specify the interface status.

The **undo ptp set-port-state enable** command disables the function to statically specify the interface status.

By default, the function to statically specify the interface status is disabled.

Format

ptp set-port-state enable slot *slot-id*

undo ptp set-port-state enable slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In a 1588v2/G.8275.1 clock synchronization network, all clock nodes work in the master-slave relationship. By default, the master-slave relationship between clock nodes is calculated through the BMC algorithm. To fix the master-slave relationship between clock nodes within a network, run the **ptp set-port-state enable** command to enable the function to statically specify the 1588v2/G.8275.1 interface status and then run the **ptp port-state** command to specify the clock synchronization status of all interfaces (except for the TC interface). After the **ptp set-port-state enable** command is run in the system view, all 1588v2/G.8275.1 interfaces are in the initializing state by default.

The following considerations apply when statically configuring the 1588v2 interface status:

- The status of a TC interface is fixed to be premaster. Therefore, you cannot change the status of TC interfaces, including all the 1588v2 interfaces on the E2ETC and P2PTC devices and TC interfaces on the E2ETCOC and P2PTCOC devices using commands.
- If the status of a 1588v2 interface has been specified and the device mode needs to be switched to E2ETC, P2PTC, E2ETCOC, or 2PTCOC, delete the 1588v2 interface status configuration.
- A 1588v2 device can be configured with only one slave interface.

Ensure that a G.8275.1 device is configured with only one slave interface.

Example

Enable the function to statically specify the interface status.

```
<HUAWEI> system-view
[HUAWEI] ptp set-port-state enable slot 0
```

3.14.25 ptp slaveonly

Function

The **ptp slaveonly** command sets the attribute of the clock source interface of the OC to slave-only.

The **undo ptp slaveonly** command restores the default status of the PTP interface of the OC.

By default, the clock source interface can be a master interface or a slave interface.

Format

ptp slaveonly slot *slot-id*

undo ptp slaveonly slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the ID of the slot where the OC with the PTP interface in the slave state resides.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

When an OC functions as the last clock node, the OC receives clock signals from an upstream device and sends the clock signals to clients. To prevent clock signals of clients from affecting the PTP system, configure the interface status of the OC to slave-only. This configuration ensures that the OC does not synchronize the clock signals of clients.

The OC in a domain has only one PTP interface. If the interface status of the OC is set to slave-only, no interface can switch to the master.

Example

Set the attribute of the clock source interface to slave-only on the OC.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type oc slot 0
[HUAWEI] ptp slaveonly slot 0
```

3.14.26 ptp sync-interval

Function

The **ptp sync-interval** command sets the interval for sending Sync packets from an interface.

The **undo ptp sync-interval** command restores the default interval for sending Sync packets from an interface.

By default, the interval for sending 1588v2 Sync packets is 8 ms, the interval for sending G.8275.1 Sync packets is 64 ms.

Format

ptp sync-interval *sync-interval*

undo ptp sync-interval

Parameters

Parameter	Description	Value
sync-interval	Indicates that the interval for sending Sync packets on an interface is set to the *n*th power of 2 in milliseconds, where *n* is specified by *sync-interval*.	The value is an integer that ranges from 0 to 20. In 1588v2 mode, the default value is 3. That is, the interval is 8 ms. In G.8275.1 mode, the default value is 6. That is, the interval is 64 ms.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

Sync packets are used to generate timestamps when the delay mechanism is used. Based on the generated timestamps, PTP calculates the link delay and implements clock synchronization. The interval for sending Sync packets affects the clock synchronization accuracy. A higher interval indicates a higher clock synchronization accuracy. However, a high packet sending interval will increase the network load. Therefore, configure the interval for sending Sync packets according to networking requirements.

Example

Set the interval for sending Sync packets to 128 ms on XGigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp sync-interval 7
```

3.14.27 ptp tcoc-clock-id

Function

The **ptp tcoc-clock-id** command, you can specify a clock source for an OC interface on the TCOC device to synchronize.

The **undo ptp tcoc-clock-id** command cancels the previous setting.

By default, no clock source is specified for a TCOC device to synchronize.

Format

ptp tcoc-clock-id *clock-source-id* **port-num** *port-num*

undo ptp tcoc-clock-id

Parameters

Parameter	Description	Value
clock-source-id	Specifies the ID of the peer clock source (ID of the static clock source).	The format is HHHHHHHH. H is a two-digit hexadecimal number, such as E0 and FC.

Parameter	Description	Value
port-num *port-num*	Indicates the number of the interface where the peer master clock is located. The value is converted from the x/y/z format of the interface number. x stands for the slot number, y stands for the sub-card number, and z stands for the interface number. To convert the port number from the x/y/z format into an integer, you need to first convert x into a 6-bit binary number; y into a 2-bit binary number; z into an 8-bit binary number. Then, rank these binary numbers in the format of x/y/z to obtain a 16-bit binary number. Convert the 16-bit binary number into a decimal number, which is the *port-num* value. For example, port number 2/0/1 on the master clock is converted into 2049.	The value is an integer that ranges from 0 to 65535.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

The **ptp tcoc-clock-id** command specifies the interface from which the local device synchronizes the clock frequency. The *clock-source-id* and *port-num* parameter of the command specify the port identify. The local device accepts only the PTP packets with specified clock ID and port number.

Precautions

- A TCOC device cannot synchronize the time. It can synchronize only the frequency; therefore, it can be configured with only one interface.
- *clock-source-id* specifies the clock ID of the peer master clock source device and *port-num* specifies the number of the peer master clock interface. If the values of *clock-source-id* and *port-num* are incorrect or the specified master clock source is faulty, synchronization cannot be performed.

Example

Set ID of the clock source for XGigabitEthernet0/0/1 on the TCOC device to 122323FFFE122110.

```
<HUAWEI> system-view
[HUAWEI] ptp device-type e2etcoc slot 0
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp tcoc-clock-id 122323FFFE122110 port-num 1
```

3.14.28 ptp udp-egress

Function

The **ptp udp-egress** command sets the UDP encapsulation mode for PTP packets.

The **undo ptp udp-egress source-ip** command restores the encapsulation mode for PTP packets to MAC encapsulation mode.

Using the **undo ptp udp-egress** { **destination-ip** | **destination-mac** | **dscp** | **vlan** | **priority** } command, you can restore the default configuration of the UDP encapsulation mode.

By default, PTP packets are encapsulated in MAC multicast mode. If UDP encapsulation is configured, multicast UDP encapsulation is used by default.

Format

ptp udp-egress source-ip *source-ip* [**destination-ip** *destination-ip*] [**dscp** *dscp*] [**vlan** *vlan-id* [**priority** *priority*]]

ptp udp-egress destination-mac *destination-mac*

undo ptp udp-egress { **source-ip** | **destination-ip** | **destination-mac** | **dscp** | **vlan** | **priority** }

Parameters

Parameter	Description	Value
source-ip *source-ip*	Indicates the source IP address of the UDP-encapsulated PTP packets.	The value is in dotted decimal notation.
destination-ip *destination-ip*	Indicates the destination IP address of the UDP-encapsulated PTP packets.	The value is in dotted decimal notation.

Parameter	Description	Value
destination-mac *destination-mac*	Indicates the destination MAC address of the UDP-encapsulated PTP packets.	The value is in the format of H-H-H. An H contains one to four hexadecimal numbers.
dscp *dscp*	Indicates the Differentiated Service Code Point (DSCP) priority carried in the UDP-encapsulated PTP packets.	The value is an integer that ranges from 0 to 63. The default value is 56.
vlan *vlan-id*	Indicates the VLAN ID encapsulated in the PTP packets.	The value is an integer that ranges from 1 to 4094.
priority *priority*	Indicates the 802.1p priority carried in the VLAN-encapsulated packet.	The value is an integer that ranges from 0 to 7. The default value is 7, indicating the highest priority.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

By default, PTP packets are encapsulated in multicast MAC mode. You can use the **ptp udp-egress** command to change the encapsulation mode to UDP encapsulation to implement Layer 3 encapsulation.

UDP encapsulation is further classified into unicast UDP encapsulation and multicast UDP encapsulation.

- Unicast encapsulation

  In this encapsulation mode, you need to set the unicast destination IP address of PTP packets.

- Multicast encapsulation

  Table 3-185 shows destination IP addresses that can be used only in the multicast UDP encapsulation.

Table 3-185 Default multicast IP address for delay and Pdelay measurement mechanisms

Delay Mechanism	IP Address
All except peer delay	224.0.1.129
Peer delay	224.0.0.107

In multicast UDP encapsulation mode, you do not need to set the destination IP address.

Precautions

Before using the **ptp udp-egress destination-mac** *destination-mac* command to configure the destination MAC address for UDP encapsulation, configure the source IP address for UDP encapsulation. The destination MAC address cannot be all 0s or a multicast address.

Example

Configure the PTP packet to be encapsulated in UDP unicast mode. Set the source IP address of the PTP packet to 192.168.2.2 and the destination IP address to 192.168.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] ptp udp-egress source-ip 192.168.2.2 destination-ip 192.168.1.1
```

3.14.29 ptp virtual-clock-id

Function

The **ptp virtual-clock-id** command configures the virtual clock ID on the PTP device.

The **undo ptp virtual-clock-id** command restores the automatically generated clock ID on the PTP device.

By default, no virtual clock ID is configured on the PTP device. The clock ID is generated by padding fffe to the middle of the system bridge MAC address. For example, if the system bridge MAC address is 111122223333, the default clock ID is 111122fffe223333.

Format

ptp virtual-clock-id *clock-id-value* **slot** *slot-id*

undo ptp virtual-clock-id slot *slot-id*

Parameters

Parameter	Description	Value
clock-id-value	Specifies the lower four bytes of a virtual clock ID. The lower four bytes of the virtual clock ID are configurable, whereas the higher four bytes are automatically allocated by the system. The value of the higher four bytes automatically allocated by the system is 0x00259e32.	The value range is 00000001-ffffffff in the form of a hexadecimal number.
slot *slot-id*	Specifies the ID of the slot where the involved PTP device resides.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The 8-byte clock ID uniquely identifies a PTP device in the PTP domain. When a PTP device performs the master-slave switchover, the clock ID of the PTP device changes along with the system bridge MAC address. As a result, the clock ID may not uniquely identify the PTP device.

By using the **ptp virtual-clock-id** command, you can specify the clock ID of a PTP device. The specified clock ID does not change in the case of the master-slave switchover, and can therefore uniquely identify the PTP device. The lower four bytes of the virtual clock ID are configurable, whereas the higher four bytes are automatically allocated by the system.

Example

Set the lower four bytes of the virtual clock ID on the PTP device to **00000123**.

```
<HUAWEI> system-view
[HUAWEI] ptp virtual-clock-id 00000123 slot 0
```

3.14.30 reset ptp statistics

Function

The **reset ptp statistics** command clears statistics on PTP packets on the interface of a device.

Format

reset ptp statistics { **all** [**slot** *slot-id*] | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Clears statistics on the received PTP packets of all interfaces.	-
interface *interface-type interface-number*	Clears statistics on the received PTP packets of a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-
slot *slot-id*	Clears statistics on the received PTP packets of all interface with a specified slot ID.	The value range depends on the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can use the **reset ptp statistics** command to clear the statistics on the received PTP packets of a specified interface or all interfaces by restoring the counter.

Example

Clear the statistics on PTP packets on XGigabitEthernet0/0/1.

```
<HUAWEI> reset ptp statistics interface xgigabitethernet 0/0/1
```

3.15 Clock Synchronization Commands

3.15.1 Command Support

Only the following models support synchronous Ethernet:

Model	Supported Part Number	Unsupported Part Number
S6730-H24X6C	- 02352FSG, 02352FSG-001, 02352FSG-003, 02352FSG-005, 02352FSG-006 - 02353GFC, 02353GFC-001, 02353GFC-003	- 02352FSG-007, 02352FSG-008 - 02353GFC-004
S6730-H48X6C	- 02352FSF, 02352FSF-003, 02352FSF-005, 02352FSF-007, 02352FSF-008, 02352FSF-011 - 02353FWL, 02353FWL-003, 02353FWL-005	- 02352FSF-009, 02352FSF-010 - 02353FWL-006
S6730-H24X4Y4C	None	No part number supports this model.
S6730-H28Y4C	None	No part number supports this model.
S6730S-H24X6C-A	- 02353HVK, 02353HVK-001, 02353HVK-003	02353HVK-004

3.15.2 clock alarm-threshold frequency-offset

Function

The **clock alarm-threshold frequency-offset** command configures an alarm threshold for frequency offset.

The **undo clock alarm-threshold frequency-offset** command restores the default alarm threshold of frequency offset.

By default, the alarm threshold of frequency offset is 9200 ppb.

Format

clock alarm-threshold frequency-offset *frequency-offset-value*

undo clock alarm-threshold frequency-offset [*frequency-offset-value*]

Parameters

Parameter	Description	Value
frequency-offset-value	Specifies the alarm threshold of frequency offset.	The value is an integer that ranges from 10 to 92, in 100 ppb. The default value is 92.

Views

System view

Default Level

3: Management level

Usage Guidelines

Frequency offset can be performed on a list of clock sources. If the frequency offset value of a clock source exceeds the specified threshold, the clock source is abnormal and does not participate in clock source selection. To configure an alarm threshold for frequency offset, run the **clock alarm-threshold frequency-offset** command.

Example

Configure the alarm threshold of frequency offset as 6000 ppb.

```
<HUAWEI> system-view
[HUAWEI] clock alarm-threshold frequency-offset 60
```

3.15.3 clock clear

Function

The **clock clear** command restores the automatic clock source selection mode.

Format

clock clear slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To clear configurations of the manual or forcible clock source selection mode and restore the automatic clock source selection mode, run the **clock clear** command.

Example

Restore the automatic clock source selection mode for the clock source in slot 0.

```
<HUAWEI> system-view
[HUAWEI] clock clear slot 0
```

3.15.4 clock ethernet-synchronization enable

Function

The **clock ethernet-synchronization enable** command enables synchronous Ethernet.

The **undo clock ethernet-synchronization enable** command disables synchronous Ethernet.

By default, synchronous Ethernet is not enabled.

Format

clock ethernet-synchronization enable

undo clock ethernet-synchronization enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable synchronous Ethernet, run the **clock ethernet-synchronization enable** command. After synchronous Ethernet is enabled on a switch, the switch selects the clock signal sent through Ethernet interfaces as the clock source.

The synchronous Ethernet function of an interface needs to be enabled both globally and on this interface. If the global synchronous Ethernet configuration is disabled, the synchronous Ethernet configuration on the interface is not deleted, but this function becomes unavailable.

Example

Enable synchronous Ethernet on a switch.

```
<HUAWEI> system-view
[HUAWEI] clock ethernet-synchronization enable
```

3.15.5 clock freq-deviation-detect enable

Function

The **clock freq-deviation-detect enable** command enables frequency offset check on clock signals.

The **undo clock freq-deviation-detect enable** command disables frequency offset check on clock signals.

By default, frequency offset check on clock signals is not enabled.

Format

clock freq-deviation-detect enable

undo clock freq-deviation-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the clock synchronization network has high requirements for frequency offset of clock signals, run the **clock freq-deviation-detect enable** command to enable frequency offset check. After this function is enabled, the system performs frequency offset check on clock signals. If the frequency offset value exceeds the specified threshold, the system considers that the clock source is unreliable and triggers another automatic clock source selection.

Frequency offset check on a clock source helps determine whether the quality of the clock source is good or not. If the frequency offset value of a clock source exceeds the specified threshold, the system clock does not trace this clock source any more. To configure the range of frequency offset check, run the **clock alarm-threshold frequency-offset** *frequency-offset-value* command.

Example

Enable frequency offset check on clock signals.

```
<HUAWEI> system-view
[HUAWEI] clock freq-deviation-detect enable
```

3.15.6 clock map unk

Function

The **clock map unk** command maps a clock source with the SSM quality level of UNK to a new SSM quality level.

Format

clock map unk { **prc** | **ssua** | **ssub** | **sec** | **dnu** }

Parameters

Parameter	Description	Value
prc	Indicates G.811 clock signals with the SSM quality level of PRC.	-
ssua	Indicates G.812 transit node clock signals with the SSM quality level of SSUA.	-
ssub	Indicates G.812 local node clock signals with the SSM quality level of SSUB.	-
sec	Indicates SDH clock source signals with the SSM quality level of SEC.	-
dnu	Indicates that the clock with the SSM quality level of DNU cannot function as a clock source.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the SSM quality level of an upstream clock source is UNK, to allow switches to trace this clock source, run the **clock map unk** command to map the upstream clock source to a new SSM quality level. By default, a clock source with the SSM quality level of UNK is mapped to the SSM quality level of DNU. In this case, if SSM control is enabled also, the clock source does not participate in clock source selection.

By default, when SSM control is enabled, the clock source with the SSM quality level of UNK does not participate in clock source selection.

Example

Map the clock source with the SSM quality level of UNK to the SSM quality level of PRC.

```
<HUAWEI> system-view
[HUAWEI] clock map unk prc
```

3.15.7 clock priority (interface view)

Function

The **clock priority** command sets the priority of a clock source.

The **undo clock priority** command restores the default priority of a clock source.

By default, the priority of a clock source is 0.

Format

clock priority *priority-value*

undo clock priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of a clock source.	The value is an integer that ranges from 1 to 255. A smaller value indicates a higher priority.

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

By default, the priority of a clock source is 0, indicating that the clock source does not participate in clock source selection.

In automatic clock source selection mode, a clock source can participate in clock source selection only when a priority is configured. In manual and forcible clock source selection modes, clock source switching can be performed regardless of the clock source priority. In this case, whether a priority is configured does not affect the switching result. To set the priority of a clock source, run the **clock priority** command.

Example

Set the priority of the clock source on the interface XGE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] clock priority 10
```

3.15.8 clock source ptp priority (system view)

Function

The **clock source ptp priority** command sets the priority of a ptp clock source.

The **undo clock source ptp priority** command restores the default priority of a ptp clock source.

The default priority of a ptp clock source is 0.

Format

clock source ptp priority *priority-value* **slot** *slot-id*

undo clock source ptp priority slot *slot-id*

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of a clock source.	The value is an integer that ranges from 1 to 255. The default value is 0. A smaller value indicates a higher priority.
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When PTP is enabled and the PTP clock is a slave clock, the frequency of the PTP clock can be used as a line clock to participate in clock source selection.

In automatic clock source selection mode, a clock source can participate in clock source selection only when a priority is configured. In manual and forcible clock source selection modes, clock source switching can be performed regardless of the clock source priority. In this case, whether a priority is configured does not affect the switching result. To set the priority of a clock source, run the **clock source priority** command.

Example

Set the priority of the PTP clock source in slot 0 to 15.

```
<HUAWEI> system-view
[HUAWEI] clock source ptp priority 15 slot 0
```

3.15.9 clock run-mode

Function

The **clock run-mode** command configures a clock node to work in free, hold, or normal mode.

By default, a clock node works in normal mode.

Format

clock run-mode { **free** | **hold** | **normal** } **slot** *slot-id*

Parameters

Parameter	Description	Value
free	Indicates that a clock node works in free mode.	-
hold	Indicates that a clock node works in hold mode.	-
normal	Indicates that a clock node works in normal mode.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure the working mode of a clock node, run the **clock run-mode** command.

- In free mode, a clock node does not select a clock source using the clock source selection algorithm.
- In hold mode, a clock node retains the locked frequency.
- In normal mode, a clock node selects a clock source using the clock source selection algorithm. If no clock source is available, the clock node automatically enters the free or hold mode.

A clock node working in free mode cannot enter the hold mode using this command.

Example

Configure the clock node in slot 0 to work in free mode.

```
<HUAWEI> system-view
[HUAWEI] clock run-mode free slot 0
```

3.15.10 clock source

Function

The **clock source** command sets the clock source selection mode to manual or forcible and specifies the master clock source.

By default, the automatic clock source selection mode is used.

Format

clock { **manual** | **force** } **source** { **ptp slot** *slot-id* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
manual	Indicates that the manual clock source selection mode is used.	-
force	Indicates that the forcible clock source selection mode is used.	-
ptp	Indicates that an PTP clock source is used as the clock source.	-
interface *interface-type interface-number*	Specifies the input interface of the clock source. ● *interface-type*: specifies the interface type. ● *interface-number*: specifies the interface number.	-
slot *slot-id*	Specifies the slot ID of the master clock source.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure the clock source selection mode as manual or forcible, run the **clock source** command. In manual clock source selection mode, a clock source can be switched to a clock source with a higher SSM quality level, regardless of the clock source priority. In forcible clock source selection mode, a clock can be selected regardless of the SSM quality level and priority.

Precautions

In manual clock source selection mode, a clock source takes effect only when the following conditions are met:

- The synchronous Ethernet function is enabled.
- The SSM quality level is the highest and not DNU.
- The status of the selected clock source is not abnormal or initial.

In forcible clock source selection mode, a clock source takes effect only when the following conditions are met:

- The synchronous Ethernet function is enabled.

If a clock source in manual clock source selection mode does not meet conditions, the clock source automatically switches to the automatic clock source selection mode. If a clock source in forcible clock source selection mode does not meet conditions, for example, the clock source is abnormal, the clock source automatically switches to the hold mode. After the clock source is restored, it is automatically selected again.

A manually selected clock source is used temporarily and no configuration file is generated. To permanently use a clock source, use the forcible clock source selection mode.

The latest configuration of manual clock source selection overrides the previous configuration of manual clock source selection but not forcible clock source selection. The latest configuration of forcible clock source selection overrides the previous configuration of manual or forcible clock source selection.

Example

Set the clock source selection mode to manual and specify the input interface of the master clock source as XGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] clock manual source interface xgigabitethernet 0/0/1
```

3.15.11 clock source-lost holdoff-time

Function

The **clock source-lost holdoff-time** command configures the holdoff time for the system to consider a clock source lost.

By default, the holdoff time for the system to consider a clock source lost is 1000 ms.

Format

clock source-lost holdoff-time *value*

Parameters

Parameter	Description	Value
value	Specifies the holdoff time for the system to consider a clock source lost.	The value is an integer that ranges from 300 to 1800, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The system considers a clock source lost after a specified holdoff time. Within this period, the system considers that the clock source exists. Setting the holdoff time can avoid some mistakes in determining the clock source caused by occasional signal jitter on the network. To set the holdoff time for the system to consider a clock source lost, run the **clock source-lost holdoff-time** command.

If clock source switching needs to be implemented as soon as possible, set **holdoff-time** to a small value. To prevent frequent clock source switching, set **holdoff-time** to a large value.

Example

Set the holdoff time for the system to consider a clock source lost to 400 ms.

```
<HUAWEI> system-view
[HUAWEI] clock source-lost holdoff-time 400
```

3.15.12 clock source ptp ssm (system view)

Function

The **clock source ptp ssm** command configures the SSM quality level of a clock source.

The **undo clock source ptp ssm** command restores the default SSM quality level of a clock source.

By default, the SSM quality level of a clock source is unknown.

Format

clock source ptp ssm { **unk** | **prc** | **ssua** | **ssub** | **sec** | **dnu** } **slot** *slot-id*

undo clock source ptp ssm slot *slot-id*

Parameters

Parameter	Description	Value
ptp	Indicates a PTP clock source.	-
dnu	Indicates that the clock source is unavailable.	-
prc	Indicates G.811 clock signals with the SSM quality level of PRC.	-
sec	Indicates SDH clock source signals with the SSM quality level of SEC.	-
ssua	Indicates G.812 transit node clock signals with the SSM quality level of SSUA.	-
ssub	Indicates G.812 local node clock signals with the SSM quality level of SSUB.	-
unk	Indicates clock signals with unknown synchronization quality.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When SSM control is enabled using the **clock ssm-control on** command, an SSM quality level needs to be specified for the clock source on an interface. To set the SSM quality level of a clock source, run the **clock source ptp ssm** command.

In switch stacking scenarios, each switch independently runs synchronous Ethernet and PTP. Therefore, this command needs to be configured for the stacked switch in each slot.

Example

Set the SSM quality level of a clock source to PRC.

```
<HUAWEI> system-view
[HUAWEI] clock source ptp ssm prc slot 0
```

3.15.13 clock ssm (interface view)

Function

The **clock ssm** command sets the SSM quality level of a clock source.

The **undo clock ssm** command cancels the configured SSM priority level of a clock source.

By default, no SSM quality level is configured for a clock source. The SSM quality level of a line clock source is transmitted from the peer device.

Format

clock ssm { **unk** | **prc** | **ssua** | **ssub** | **sec** | **dnu** }

undo clock ssm

Parameters

Parameter	Description	Value
dnu	Indicates that the clock source is unavailable.	-
prc	Indicates G.811 clock signals with the SSM quality level of PRC.	-
sec	Indicates SDH clock source signals with the SSM quality level of SEC.	-
ssua	Indicates G.812 transit node clock signals with the SSM quality level of SSUA.	-
ssub	Indicates G.812 local node clock signals with the SSM quality level of SSUB.	-
unk	Indicates clock signals with unknown synchronization quality.	-

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

When SSM control is enabled on a clock source using the **clock ssm-control on** command in the system view, an SSM quality level needs to be specified for the clock source on an interface. To set the SSM quality level of a clock source, run the **clock ssm** command. In switch stacking scenarios, each switch independently runs synchronous Ethernet and PTP. Therefore, this command needs to be configured for the stacked switch in each slot.

Example

Set the SSM quality level of the clock source on the interface XGE0/0/1 as PRC.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] clock ssm prc
```

3.15.14 clock ssm-control

Function

The **clock ssm-control** command enables or disables SSM quality levels are used for automatic clock source selection.

By default, SSM quality levels are used for clock source selection.

Format

clock ssm-control { **on** | **off** }

Parameters

Parameter	Description	Value
on	Enables SSM control.	-
off	Disables SSM control.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the system clock works in automatic clock source selection mode, if SSM control is enabled, the system clock selects the clock source to trace based on SSM quality levels and then the priorities. If SSM control is disabled, the system clock selects the clock source to trace based on priorities. To configure SSM control, run the **clock ssm-control** command.

Example

Enable SSM control.

```
<HUAWEI> system-view
[HUAWEI] clock ssm-control on
```

3.15.15 clock switch

Function

The **clock switch** command configures the recovery mode of a clock node.

By default, clock nodes work in revertive mode.

Format

clock switch { **revertive** | **non-revertive** }

Parameters

Parameter	Description	Value
revertive	Indicates the revertive mode.	-
non-revertive	Indicates the non-revertive mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure a clock source to work in revertive or non-revertive mode, run the **clock switch** command.

- Revertive mode: Switching is performed if the new clock source has a higher SSM quality level. If the new clock source has the same SSM quality level but a higher priority than the old clock source, switching is also performed. In other situations, switching is not performed.
- Non-revertive mode: Switching is performed if the new clock source has a higher SSM quality level. If the new clock source has the same SSM quality level but a higher priority than the old clock source, switching is not performed. In other situations, switching is not performed.

Example

Configure a clock node to work in revertive mode.

```
<HUAWEI> system-view
[HUAWEI] clock switch revertive
```

3.15.16 clock synchronization enable

Function

The **clock synchronization enable** command enables clock synchronization.

The **undo clock synchronization enable** command disables clock synchronization.

By default, clock synchronization is not enabled.

Format

clock synchronization enable

undo clock synchronization enable

Parameters

None

Views

XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

An interface can participate in clock source selection only after clock synchronization is enabled.

Example

Enable clock synchronization on the interface XGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] clock synchronization enable
```

3.15.17 clock source ptp synchronization enable

Function

The **clock source ptp synchronization enable** command enables clock synchronization of a PTP clock source.

The **undo clock source ptp synchronization enable** command disables clock synchronization from a PTP clock source.

By default, clock synchronization is not enabled for a PTP clock source.

Format

clock source ptp synchronization enable slot *slot-id*

undo clock source ptp synchronization enable slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable clock synchronization for a PTP clock source, run the **clock source ptp synchronization enable** command. If a PTP clock source with clock synchronization enabled is selected as the clock source, frequency is transmitted through PTP messages.

An interface can participate in clock source selection after it is enabled with clock synchronization using the **clock synchronization enable** command.

Example

Enable clock synchronization for a PTP clock source.

```
<HUAWEI> system-view
[HUAWEI] clock source ptp synchronization enable slot 0
```

3.15.18 clock wtr

Function

The **clock wtr** command sets the wait-to-restore (WTR) time for a clock source.

By default, the WTR time of a clock source is 5 minutes.

Format

clock wtr *wtr-time*

Parameters

Parameter	Description	Value
wtr-time	Specifies the WTR time of a clock source.	The value is an integer that ranges from 0 to 12, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lost clock source is restored, the system waits for a period of 0 to 12 minutes before considering the clock source available. During this period, the system considers the clock source lost.

Setting the WTR time can avoid some mistakes in determining the clock source caused by occasional signal jitter on the network.

The default WTR time of a clock source is 5 minutes. Generally, you do not need to change the default value. If you want to view the clock source switching result during debugging, set the WTR time to 0.

Example

Set the WTR time to 0.

```
<HUAWEI> system-view
[HUAWEI] clock wtr 0
```

3.15.19 display clock

Function

The **display clock** command displays synchronous Ethernet configurations or the attributes of a PTP clock source.

Format

display clock { **config** | **source** [**ptp**] } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
config	Displays the current clock configurations.	-
source	Displays the attributes of all clock sources.	-

Parameter	Description	Value
ptp	Displays the attributes of a PTP clock source.	-
slot *slot-id*	Displays configurations based on a slot ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a clock source is configured, run the **display clock config** command to view clock configurations. During routing maintenance, run the **display clock source** command to view attributes of the clock source being traced or all clock sources.

Example

Display synchronous Ethernet configurations on a switch.

```
<HUAWEI> display clock config
 ethernet synchronization   :enable
 clock freq deviation detect:disable
 clock unk map              :dnu
 system pll run mode        :normal

 switch config
    sys pll                 :auto mode
    SSM control             :on
    switch mode             :revertive
    wtr                     :5min
    holdoff time            :1000ms

 source config
 ptp
    Sync enable
    Pri(sys)                :1
    SSM                     :unk
 XGigabitEthernet0/0/4
    Sync enable
    Pri(sys)                :10
    SSM                     :sec
```

Table 3-186 Description of the **display clock config** command output

Item	Description
ethernet synchronization	Whether synchronous Ethernet is enabled globally

Item	Description
clock freq deviation detect	Whether frequency offset check is enabled
clock unk map	SSM quality level mapped to the clock source with the SSM quality level of UNK
system pll run mode	PLL running mode
switch config	Switching configuration
sys pll	Clock source selection mode of the system phase-locked loop
SSM control	Whether the SSM quality level is used in clock source selection
switch mode	Switching mode
wtr	WTR time
holdoff time	Holdoff time
source config	Clock source configuration
ptp	PTP clock source
XGigabitEthernet0/0/4	Line clock source
Sync enable	Whether clock synchronization is enabled
Pri(sys)	Priority
SSM	SSM quality level

3.15.20 display clock source freq-deviation

Function

The **display clock source freq-deviation** command displays the frequency offset value of a clock source.

Format

display clock source freq-deviation [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the frequency offset value of a clock source, run the **display clock source freq-deviation** command. If the frequency offset value is greater than or equal to the specified threshold, the frequency offset is abnormal. If the frequency offset value is less than the threshold, the frequency offset is normal.

Precautions

- If frequency offset check is not enabled, this command also displays the frequency offset check result of the clock source. The check result, however, is not used for clock source selection.
- A clock source that does not pass the frequency offset check is tagged "--".

Example

Display the frequency offset result of the clock source in slot 2.

```
<HUAWEI> display clock source freq-deviation slot 2
 Frequence deviation detect:     enable
  Source                              Freq-deviation-value
  -----------------------------------------------------------
    XGE2/0/4                            -0.05ppm(normal)
```

Table 3-187 Description of the **display clock source freq-deviation** command output

Item	Description
Source	Interface clock source or PTP clock source with synchronous Ethernet enabled
Freq-deviation-value	Frequency offset value, which is in the format of symbol (negative sign only) + frequency offset value + unit (ppm) + frequency offset status. If the value is "---", the frequency offset check cannot be performed on the clock source.

4 Interface Management Commands

4.1 Basic Interface Configuration Commands

4.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

4.1.2 collect counters top

Function

The **collect counters top** command sets the parameters for top N interface traffic statistics and enables the function to generate top N interface traffic statistics reports.

Format

collect counters top [*number*] **interface** { *interface-type* | **all** | **layer-2** | **layer-3** } [**sort-by** *statistics-type* | **interval** *interval-value*] *

Parameters

Parameter	Description	Value
number	Specifies the number of busiest interfaces for which traffic statistics reports are to be generated. For example, if the value is 10, a traffic statistics report about top 10 busiest interfaces is generated. If you do not specify this parameter, a traffic statistics report about top 20 busiest interfaces is generated.	The value is an integer ranging from 1 to 50000.
interface { *interface-type* | **all** | **layer-2** | **layer-3** }	Specifies the type of the interfaces for which a top N traffic statistics report is to be generated: ● *interface-type*: indicates a specific type of interface. ● **all**: indicates all interfaces. ● **layer-2**: indicates Layer 2 interfaces. ● **layer-3**: indicates Layer 3 interfaces.	The specified interfaces must be Ethernet physical interfaces or Eth-Trunk interfaces.

Parameter	Description	Value
sort-by *statistics-type*	Specifies the statistics type by which ports are determined to be the busiest. If you do not specify **sort-by** *statistics-type*, statistics are sorted by the total number of bytes in descending order.	The value can be: ● **utilization**: indicates to sort statistics by bandwidth utilization. ● **bytes**: indicates to sort statistics by the total number of bytes. ● **packets**: indicates to sort statistics by the total number of packets. ● **multicast**: indicates to sort statistics by the total number of multicast packets. ● **broadcast**: indicates to sort statistics by the total number of broadcast packets. ● **errors**: indicates to sort statistics by the total number of error packets. ● **discards**: indicates to sort statistics by the total number of dropped packets.
interval *interval-value*	Specifies the interval at which statistics are collected.	The value is an integer ranging from 1 to 999, in seconds. The default value is 30.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The display command allows you to view statistics about the traffic sent and received by each interface on a device, but cannot sort these statistics by traffic volume in descending order. The **display counters top interface** command allows you to view top N interface traffic statistics reports, facilitating interface monitoring. Before you view a top N interface traffic statistics report, run the **collect counters top** command to generate your desired top N interface traffic statistics report. For example, configure the device to generate a top N statistics report about packets dropped on Layer 2 interfaces within 50s.

The top N interface traffic statistics function sorts statistics about inbound and outbound traffic processed by interfaces within a collection interval in descending order and generates a top N interface traffic statistics report. The device stops collecting interface traffic statistics after the collection interval ends. To generate another top N interface traffic statistics report, run the **collect counters top** command again.

Configuration Impact

- After the **collect counters top** command is run, the device collects interface traffic statistics and generates a top N interface traffic statistics report based on the set parameters.
- The **collect counters top** command configuration is not saved in the configuration file.

Follow-up Procedure

To view a top N interface traffic statistics report, run the **display counters top interface** command.

Precautions

- When the master switch in a stack containing multiple member switches is faulty, the top N interface traffic statistics function takes effect only on a master switch. If the master switch encounters a fault and switches to the backup state, run the **collect counters top** command on the new master switch again.
- The **collect counters top** command can be run multiple times in succession with different parameters specified. For example, you can configure a device to generate a top N statistics report about interface multicast packets when the device is still generating a top N statistics report about interface broadcast packets.
- The top N interface traffic statistics function allows a device to generate a maximum of five top N interface traffic statistics reports. If you want the device to generate new top N interface traffic statistics reports when five top N interface traffic statistics reports already exist, run the **reset counters top interface** command to clear existing ones.

Example

Configure a device to generate a statistics report about top 10 Layer 2 interfaces in terms of the number of packets dropped within 40s.

```
<HUAWEI> collect counters top 10 interface layer-2 sort-by discards interval 40
```

4.1.3 bandwidth (Interface view)

Function

The **bandwidth** command sets the interface bandwidth obtained by the NMS from the MIB.

The **undo bandwidth** command restores the default configuration.

By default, the interface bandwidth obtained by the NMS from the MIB depends on the interface type. For example, the bandwidth of a GE interface is 1000 Mbit/s.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

bandwidth *bandwidth* [**kbps**]

undo bandwidth

Parameters

Parameter	Description	Value
bandwidth	Specifies the bandwidth of an interface.	The value is an integer ranging from 1 to 1000000, and the unit is Mbit/s.
kbps	Indicates the unit of an interface bandwidth is kbit/s. If **kbps** is not specified, the unit of an interface bandwidth is Mbit/s.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, GE sub-interface view, XGE sub-interface view, 40GE interface view, 100GE interface view, 40GE sub-interface view, 100GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, tunnel interface view, Eth-Trunk interface view, Eth-Trunk sub-interface view, VLANIF interface view, VE interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **bandwidth** command sets an interface bandwidth obtained by the NMS from the MIB and does not change an interface actual bandwidth. The NMS can check the interface bandwidth through the two objects **ifSpeed** and **ifHighSpeed** in **IF-MIB**.

- If the configured bandwidth is smaller than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as *bandwidth* x 1000 x 1000 and *bandwidth*.
- If the configured bandwidth is equal to or larger than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as 4294967295 (0XFFFFFFFF) and *bandwidth*.

Precautions

For a VLANIF interface, no matter how many physical interfaces are added to the VLAN corresponding to the VLANIF interface, the interface bandwidth obtained by the NMS from the MIB is always 1000 Mbit/s.

Example

Set the bandwidth of GE0/0/1 to 100 Mbit/s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] bandwidth 100
```

4.1.4 description (interface view)

Function

The **description** command configures the description for an interface.

The **undo description** command restores the default description of an interface.

By default, the description of an interface is null.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the interface description.	The value is a string of 1 to 242 characters. The character string is case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate switch management and maintenance, you can configure interface descriptions. An interface description can contain:

Precautions

The interface description is displayed from the first non-space character.

Example

Configure the description of GE0/0/1 as To-[DeviceB]GE-0/0/1, indicating that this device is connected to device B through GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] description To-[DeviceB]GE-0/0/1
```

4.1.5 display counters

Function

The **display counters** command displays traffic statistics on an interface.

Format

display counters [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]] [**nonzero**]

Parameters

Parameter	Description	Value
inbound	Displays incoming traffic statistics on an interface.	-
outbound	Displays outgoing traffic statistics on an interface.	-
interface *interface-type* [*interface-number*]	Displays traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If the interface number is not specified, traffic statistics on all the interfaces of the specified type are displayed.	-

Parameter	Description	Value
nonzero	Displays statistics about interface traffic. If the numbers of bytes, octets packets, unicast packets, multicast packets, and broadcast packets on an interface are all 0s, traffic statistics on this interface are not displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display counters** command to view incoming or outgoing traffic statistics based on the interface type for fault location.

Precautions

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

When a device has a large number of interfaces, you are advised to specify the interface type in the **display counters** command to view only desired information. If you do not specify those parameters, the following faults will occur:

- The displayed information is repeatedly refreshed, causing desired information unable to be obtained.
- The system does not respond because of long-time information traversing and searching.

Example

Display traffic statistics on GE0/0/1.

```
<HUAWEI> display counters interface gigabitethernet 0/0/1
Inbound
Interface          Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1              754918035105    1408179641        15018056      9668635374
Outbound
Interface          Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1              764800451602    1148151623        15086605      9957268821
```

Display traffic statistics on interfaces with at least one of the numbers of bytes, unicast packets, multicast packets, and broadcast packets not 0.

```
<HUAWEI> display counters nonzero
Info: This operation may take a few seconds. Please wait for a moment...
Inbound
Interface          Octets(bytes) Unicast(pkts) Multicast(pkts) Broadcast(pkts)
GE0/0/1                  1467604             0           2902               0
Outbound
```

```
Interface          Octets(bytes)  Unicast(pkts)  Multicast(pkts)  Broadcast(pkts)
GE0/0/1                2703904              0           13750                1
```

Table 4-1 Description of the **display counters** command output

Item	Description
Inbound	Incoming traffic statistics on an interface.
Interface	Interface name.
Octets(bytes)	Total number of incoming or outgoing bytes.
Unicast(pkts)	Number of incoming or outgoing unicast packets.
Multicast(pkts)	Number of incoming or outgoing multicast packets.
Broadcast(pkts)	Number of incoming or outgoing broadcast packets.
Outbound	Outgoing traffic statistics on an interface.

4.1.6 display counters discard

Function

The **display counters discard** command displays statistics about dropped packets.

Format

display counters discard [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
inbound	Displays statistics about incoming packets dropped.	-
outbound	Displays statistics about outgoing packets dropped.	-
interface *interface-type* [*interface-number*]	Specifies the interface type and number of an interface on which statistics about dropped packets are to be displayed. If *interface-number* is not specified, traffic statistics on all interfaces with the type specified by *interface-type* are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view detailed statistics about dropped packets on interfaces of different types, run the **display counters discard** command. When a large number of packets are dropped, this configuration facilitates device maintenance.

Precautions

For the S1730S, S300, S5735-L, S2730S-S, S5735-L-I, S5735-L1,S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, or S5735S-S, if multiple switches set up a stack, statistics about dropped packets on stack ports cannot be viewed.

Example

Display statistics about dropped packets on Ethernet 1/0/1.

```
<HUAWEI> display counters discard interface ethernet 1/0/1
Interface              InDiscards                    OutDiscards
Eth1/0/1                0                          0
```

Table 4-2 Description of the **display counters discard** command output

Item	Description
Interface	Interface name
InDiscards	Number of incoming packets dropped on the interface
OutDiscards	Number of outgoing packets dropped on the interface

4.1.7 display counters error

Function

The **display counters error** command displays error packet statistics.

Format

display counters error [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
inbound	Displays inbound error packet statistics.	-
outbound	Displays outbound error packet statistics.	-
interface *interface-type* [*interface-number*]	Displays error packet statistics on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If interface type and interface number are not specified, the statistics of error packets on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display counters error** command to view detailed error packet statistics on all types of interfaces, which facilitates maintenance when there is a large number of error packets. (The actual output information may differ from the following information.)

Example

Check all error packet statistics on the device.

```
<HUAWEI> display counters error
Inbound
Interface         Total          CRC          Giants        Fragments
GE0/0/1               0            0             0              0
GE0/0/2               0            0             0              0
GE0/0/3               0            0             0              0
GE0/0/4               0            0             0              0
GE0/0/5               0            0             0              0
Interface         Runts     DropEvents       Alignments          Symbols
GE0/0/1               0            0             0              0
GE0/0/2               0            0             0              0
GE0/0/3               0            0             0              0
GE0/0/4               0            0             0              0
GE0/0/5               0            0             0              0
Outbound
Interface         Total     Collisions       Excess-Col   Late Collisions
GE0/0/1               0            0             0              0
GE0/0/2               0            0             0              0
GE0/0/3               0            0             0              0
```

```
GE0/0/4              0           0            0            0
GE0/0/5              0           0            0            0
```

Table 4-3 Description of the **display counters error** command output

Item	Description
Inbound	Inbound error packet statistics.
Outbound	Outbound error packet statistics.
Interface	Interface name.
Total	Total number of inbound and outbound error packets.
CRC	Number of packets with length ranging from 64 bytes to 1518 bytes and incorrect FCS values. For the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For switches, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received packets with length exceeding the maximum jumbo frame size.
Fragments	Number of fragmented packets received by the interface. A fragmented packet is a packet with length less than 64 bytes and incorrect CRC values. On the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720-EI, and S6720S-EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of received undersized frames with correct CRC values. An undersized frame is a frame that is shorter than 64 bytes, in correct format, and contains a valid CRC field. For the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720-EI, and S6720S-EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment error.

Item	Description
Symbols	Number of received frames with coding error.
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. **NOTE** If the command output contains only this field and the Excess-Col field is not displayed, the field also includes the number of frames that are canceled due to consecutive 16 collisions.
Excess-Col	After sixteen successive collisions, the system will take it as excessive collision statistics when another collision occurs. Frames that are not sent due to excessive collisions are counted in this field.
Late Collisions	Number of delay collision frames. A delay collision frame is a frame that is delayed because a collision is detected when the first 512 bits of the frame are sent.

4.1.8 display counters interface

Function

The **display counters interface** command displays traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.

Format

display counters interface *interface-type interface-number* **verbose**

display counters interface verbose [**nonzero**]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Parameter	Description	Value
verbose	Displays detailed traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.	-
nonzero	Displays non-zero traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When diagnosing faults on an interface, run this command to view detailed information about packets received and sent by the interface to determine whether the interface works properly. You can also run this command to view detailed traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues. You can also run this command to view non-zero traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.

Follow-up Procedure

If you want to collect new traffic statistics, run the **reset counters interface** command to clear the current statistics.

Example

Display traffic statistics on an interface, including typical packet statistics and number of packets discarded in queues.

```
<HUAWEI> display counters interface gigabitethernet 0/0/1 verbose
GigabitEthernet0/0/1
InPackets                :                 0
InOctets                 :                 0
InUcastPkts              :                 0
InMcastPkts              :                 0
InBcastPkts              :                 0
OutPackets               :                 0
OutOctets                :                 0
```

```
OutUcastPkts            :               0
OutMcastPkts            :               0
OutBcastPkts            :               0
InJumbo                 :               0
InPause                 :               0
Frames                  :               0
OutJumbo                :               0
OutPause                :               0
InDiscards              :               0
OutDiscards             :               0
InErrors                :               0
OutErrors               :               0
CRC                     :               0
Giants                  :               0
Jabbers                 :               0
Fragments               :               0
Runts                   :               0
DropEvents              :               0
Alignments              :               0
Symbols                 :               0
Ignoreds                :               0
Collisions              :               0
ExcessiveCollisions     :               0
Late Collisions         :               0
Deferreds               :               0
Buffers purged          :               0
InPkts64Octets          :               0
InPkts65to127Octets     :               0
InPkts128to255Octets    :               0
InPkts256to511Octets    :               0
InPkts512to1023Octets   :               0
InPkts1024to1518Octets  :               0
OutPkts64Octets         :               0
OutPkts65to127Octets    :               0
OutPkts128to255Octets   :               0
OutPkts256to511Octets   :               0
OutPkts512to1023Octets  :               0
OutPkts1024to1518Octets :               0
Queue0lostPkts          :               0
Queue1lostPkts          :               0
Queue2lostPkts          :               0
Queue3lostPkts          :               0
Queue4lostPkts          :               0
Queue5lostPkts          :               0
Queue6lostPkts          :               0
Queue7lostPkts          :               0
```

Table 4-4 Description of the **display counters interface** command output

Item	Description
GigabitEthernet0/0/1	The interface type and number.
InPackets	Total number of packets received by the interface.
InOctets	Total number of bytes in packets received by the interface.
InUcastPkts	Number of unicast packets received by the interface.
InMcastPkts	Number of multicast packets received by the interface.
InBcastPkts	Number of broadcast packets received by the interface.
OutPackets	Total number of packets sent by the interface.

Item	Description
OutOctets	Total number of bytes in packets sent by the interface.
OutUcastPkts	Number of unicast packets sent by the interface.
OutMcastPkts	Number of multicast packets sent by the interface.
OutBcastPkts	Number of broadcast packets sent by the interface.
InJumbo	Number of Ethernet frames with length ranging from 1518 bytes to the maximum jumbo frame size and correct FCS values received by the interface, or number of VLAN frames with length ranging from 1522 bytes to the maximum jumbo frame size and correct FCS values received or sent by the interface.
InPause	Number of pause frames received by the interface.
Frames	Number of packets in which the 802.3 length field does not match the actual length received by the interface.
OutJumbo	Number of Ethernet frames with length ranging from 1518 bytes to the maximum jumbo frame size and correct FCS values sent by the interface, or number of VLAN frames with length ranging from 1522 bytes to the maximum jumbo frame size and correct FCS values received or sent by the interface.
OutPause	Number of pause frames sent by the interface.
InDiscards	Number of incoming packets discarded by the interface. The number is detected during physical layer detection.
OutDiscards	Number of outgoing packets discarded by the interface. The number is detected during physical layer detection.
InErrors	Number of incoming error packets on the interface. The number is detected during physical layer detection.
OutErrors	Number of outgoing error packets on the interface. The number is detected during physical layer detection.
CRC	For the S5720-LI, S5731-H, S5731S-H, S5731S-S, S5732-H, S5736-S, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. The value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.

Item	Description
Giants	Number of received packets with length exceeding the maximum jumbo frame size. ● On a 10000M interface, the number of bytes for Giants packets is calculated according to the actual packet length. ● On a 1000M interface, the number of bytes for Giants packets is calculated according to the maximum jumbo frame size. To set the maximum jumbo frame size, run the **jumboframe_enable** command.
Jabbers	The S5720-LI, S5720I-SI, S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-S, and S6730-H do not have the Jabbers field. On the other product models, this field indicates the number of received packets with length exceeding the maximum jumbo frame length and incorrect FCS values.
Fragments	Number of received fragmented packets. A fragmented packet is a packet shorter than 64 bytes and with incorrect CRC values. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value of this field contains the number of undersized frames with the correct CRC values received is displayed. On the S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S6720S-EI, S6735-S, and S6720-EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of undersized frames with correct CRC values received by the interface. For the S5720-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735-L, S300, S2730S-S, S5735-L1, S5735-L-I, S5735S-H, S5736-S, S6720S-S, S6720S-EI, S6735-S, and S6720-EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.

Item	Description
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. **NOTE** If the command output contains only this field and the ExcessiveCollisions field is not displayed, the field also includes the number of frames that are canceled due to consecutive 16 collisions.
ExcessiveCollisions	Number of packets with 16 collisions and fail to be sent.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Buffers Purged	Number of packets aged in the cache.
InOutPkts64Octets	Number of packets shorter than 64 bytes received and sent by the interface.
InOutPkts65to127Octets	Number of packets with length ranging from 65 bytes to 127 bytes received and sent by the interface.
InOutPkts128to255Octets	Number of packets with length ranging from 128 bytes to 255 bytes received and sent by the interface.
InOutPkts256to511Octets	Number of packets with length ranging from 256 bytes to 511 bytes received and sent by the interface.
InOutPkts512to1023Octets	Number of packets with length ranging from 512 bytes to 1023 bytes received and sent by the interface.
InOutPkts1024toMaxOctets	Number of packets with length exceeding 1024 bytes received and sent by the interface.
InPkts64Octets	Number of packets shorter than 64 bytes received by the interface.
InPkts65to127Octets	Number of packets with length ranging from 65 bytes to 127 bytes received by the interface.
InPkts128to255Octets	Number of packets with length ranging from 128 bytes to 255 bytes received by the interface.
InPkts256to511Octets	Number of packets with length ranging from 256 bytes to 511 bytes received by the interface.
InPkts512to1023Octets	Number of packets with length ranging from 512 bytes to 1023 bytes received by the interface.
InPkts1024to1518Octets	Number of packets with length ranging from 1024 bytes to 1518 bytes received by the interface.

Item	Description
OutPkts64Octets	Number of packets shorter than 64 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts65to127Octets	Number of packets with length ranging from 65 bytes to 127 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts128to255Octets	Number of packets with length ranging from 128 bytes to 255 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts256to511Octets	Number of packets with length ranging from 256 bytes to 511 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts512to1023Octets	Number of packets with length ranging from 512 bytes to 1023 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
OutPkts1024to1518Octets	Number of packets with length ranging from 1024 bytes to 1518 bytes sent by the interface. The value **NA** indicates that the interface does not support this field.
Queue0lostPkts	Number of packets discarded in queue 0.
Queue1lostPkts	Number of packets discarded in queue 1.
Queue2lostPkts	Number of packets discarded in queue 2.
Queue3lostPkts	Number of packets discarded in queue 3.
Queue4lostPkts	Number of packets discarded in queue 4.
Queue5lostPkts	Number of packets discarded in queue 5.
Queue6lostPkts	Number of packets discarded in queue 6.
Queue7lostPkts	Number of packets discarded in queue 7.

NOTE

The number (InPkts) of packets received by the interface and the number (OutPkts) of packets sent by the interface can be displayed separately only on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S,S6720S-S, display only the total number (InOutPkts) of packets received and sent by the interface.

4.1.9 display counters rate

Function

The **display counters rate** command displays the incoming or outgoing traffic rate of an interface.

Format

display counters rate [**inbound** | **outbound**] [**interface** *interface-type* [*interface-number*]] [**nonzero**]

Parameters

Parameter	Description	Value
inbound	Displays the incoming traffic rate of an interface.	-
outbound	Displays the outgoing traffic rate of an interface.	-
interface *interface-type* [*interface-number*]	Displays the traffic rate of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If the interface number is not specified, the traffic rates of all the interfaces of the specified type are displayed.	-
nonzero	Displays the traffic rate of an interface. If the numbers of bytes, Octets packets, unicast packets, multicast packets, and broadcast packets on an interface are all 0s, the traffic rate of this interface is not displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display counters rate** command to view the incoming or outgoing traffic rate based on the interface type for fault location.

Precautions

After the system is started, in the case of the first query or when the interval with the last query is longer than 600s, the system re-initiates rate statistics collection. In this case, you need to wait until the rate statistics collection result is displayed.

The minimum statistics collection interval is 5 seconds. If the interval is less than 5 seconds, the data collected last time is displayed.

When a device has a large number of interfaces, you are advised to specify the interface type in the **display counters rate** command to view only desired information. If you do not specify those parameters, the following faults will occur:

- The displayed information is repeatedly refreshed, causing desired information unable to be obtained.
- The system does not respond because of long-time information traversing and searching.

Example

Display the traffic rate of GE0/0/1.

```
<HUAWEI> display counters rate interface gigabitethernet 0/0/1
Inbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                18               0                 0                 0
Outbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                61               0                 0                 0
```

Display the traffic rate of interfaces with at least one of the numbers of bytes, unicast packets, multicast packets, and broadcast packets not 0.

```
<HUAWEI> display counters rate nonzero
Info: This operation may take a few seconds. Please wait for a moment...
Inbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1                82               1                 0                 0
Outbound
Interface   Octets(bytes/s) Unicast(pkts/s) Multicast(pkts/s) Broadcast(pkts/s)
GE0/0/1               224               2                 0                 0
```

Table 4-5 Description of the **display counters rate** command output

Item	Description
Inbound	Incoming traffic rate.
Outbound	Outgoing traffic rate.
Interface	Interface name.
Octets(bytes/s)	Total incoming or outgoing traffic rate, in bytes/s.
Unicast(pkts/s)	Incoming or outgoing rate of unicast packets, in pkts/s.

Item	Description
Multicast(pkts/s)	Incoming or outgoing rate of multicast packets, in pkts/s.
Broadcast(pkts/s)	Incoming or outgoing rate of broadcast packets, in pkts/s.

4.1.10 display counters top interface

Function

The **display counters top interface** command displays top N interface traffic statistics reports.

Format

display counters top interface report [*report-number*]

Parameters

Parameter	Description	Value
report-number	Specifies the number of a top N interface traffic statistics report. If you do not specify this parameter, the command output displays the summary information about all top N interface traffic statistics reports.	The value is an integer ranging from 1 to 5.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **collect counters top** command generates top N interface traffic statistics reports, but does not display these reports. To view the generated reports, run the **display counters top interface report** [*report-number*] command.

Precautions

Before you run the **display counters top interface report** [*report-number*] command, ensure that a top N interface traffic statistics report has been generated using the **collect counters top** command. Otherwise, the "There is no

TOPN interface counters report." message is displayed after you run the **display counters top interface report** [*report-number*] command.

Example

Display the summary information about all top N interface traffic statistics reports.

```
<HUAWEI> display counters top interface report
Id Start Time                 Interval Number Sort-By   Status Interface-Type
-------------------------------------------------------------------------------
1  2012-09-05 09:03:13-08:00    30       20     bytes     doing  GigabitEthernet
```

Table 4-6 Description of the **display counters top interface report** command output

Item	Description
Id	Indicates the number of a top N interface traffic statistics report.
Start Time	Indicates the start time of statistics collection.
Interval	Indicates the statistics collection interval.
Number	Indicates the number of busiest interfaces for which interface statistics reports are to be generated.
Sort By	Indicates the statistics type by which ports are determined to be the busiest, which can be: ● utilization: indicates to sort statistics by bandwidth utilization. ● bytes: indicates to sort statistics by the total number of bytes. ● packets: indicates to sort statistics by the total number of packets. ● multicast: indicates to sort statistics by the total number of multicast packets. ● broadcast: indicates to sort statistics by the total number of broadcast packets. ● errors: indicates to sort statistics by the total number of error packets. ● discards: indicates to sort statistics by the total number of dropped packets.
Status	Indicates the generation status of a top N interface traffic statistics report, which can be: ● doing: The report is being generated. ● done: The report has been generated.

Item	Description
Interface-Type	Indicates the type of interfaces for which the top N interface traffic statistics report is generated, which can be: ● all: indicates all interfaces. ● layer-2: indicates Layer 2 interfaces. ● layer-3: indicates Layer 3 interfaces. ● Specified interface type: indicates Ethernet physical interfaces or Eth-Trunk interfaces.

Display the detailed information about the top N interface traffic statistics report numbered 1.

```
<HUAWEI> display counters top interface report 1
Owner            : RT1(10.1.1.1)
Start Time       : 2012-09-17 13:26:06
End Time         : 2012-09-17 13:26:36
Interface Type   : GigabitEthernet
Sort By          : bytes
Interval         : 30 seconds
Port      Band  Util Bytes      Packets    Broadcast  Multicast  Error
Discards
          width      (In + Out) (In + Out) (In + Out) (In + Out)
-------  ----- ------ ---------- ---------- ---------- ---------- ----- --------
GE0/0/1   1000M   0% 974        4          0          4          0     0
```

Table 4-7 Description of the **display counters top interface report 1** command output

Item	Description
Owner	Indicates the device on which the top N interface traffic statistics report is generated.
Start Time	Indicates the start time of statistics collection.
End Time	Indicates the end time of statistics collection.
Interface Type	Indicates the type of interfaces for which the top N interface traffic statistics report is generated, which can be: ● all: indicates all interfaces. ● layer-2: indicates Layer 2 interfaces. ● layer-3: indicates Layer 3 interfaces. ● Specified interface type: indicates Ethernet physical interfaces or Eth-Trunk interfaces.

Item	Description
Sort By	Indicates the statistics type by which ports are determined to be the busiest, which can be: ● utilization: indicates to sort statistics by bandwidth utilization. ● bytes: indicates to sort statistics by the total number of bytes. ● packets: indicates to sort statistics by the total number of packets. ● multicast: indicates to sort statistics by the total number of multicast packets. ● broadcast: indicates to sort statistics by the total number of broadcast packets. ● errors: indicates to sort statistics by the total number of error packets. ● discards: indicates to sort statistics by the total number of dropped packets.
Interval	Indicates the statistics collection interval.
Port	Indicates the interface name.
Band width	Indicates interface bandwidth.
Util	Indicates bandwidth utilization.
Bytes	Indicates the total number of sent and received bytes.
Packets	Indicates the total number of sent and received packets.
Multicast	Indicates the total number of sent and received multicast packets.
Broadcast	Indicates the total number of sent and received broadcast packets.
Error	Indicates the total number of error packets.
Discards	Indicates the total number of dropped packets.

4.1.11 display interface

Function

The **display interface** command displays the interface running status and statistics.

Format

display interface [*interface-type* [*interface-number* [.*subinterface-number*] | **main**] | **main**]

display interface slot *slot-id* [**main**]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the running status and traffic statistics of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.	-
subinterface-number	Displays the running status and traffic statistics of a sub-interface.	The value is an integer that ranges from 1 to 4096.
main	Displays running status and traffic statistics about an interface. ● If an interface has no sub-interfaces, status and traffic statistics about the interface are displayed whether you specify the **main** parameter or not. ● If an interface has sub-interfaces, status and traffic statistics about the interface and sub-interfaces are displayed if you do not specify the **main** parameter.	-
slot *slot-id*	Specifies the slot ID.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The running status and statistics of an interface includes the physical status, basic configuration, and statistics about forwarded packets on the interface. You can use the **display interface** command to collect traffic statistics or locate faults on an interface.

Precautions

- If no interface type is specified, the running status and statistics of all the interfaces is displayed. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.
- When the XGE service interface of the S5731-H includes Ignoreds, Runts, and Fragments packets, the bytes statistics are incorrect.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Display the running status, basic configuration, and statistics about forwarded packets on GE0/0/1.

```
<HUAWEI> display interface gigabitethernet 0/0/1
GigabitEthernet 0/0/1 current state : UP
Line protocol current state : UP
Description:
Switch Port, Link-type : access(negotiated),
PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc12-3456
Last physical up time   : 2018-07-04 18:59:25
Last physical down time : 2018-07-04 19:02:07
Current system time: 2018-07-10 16:03:43
Port Mode: COMMON COPPER
Speed : 1000,   Loopback: NONE
Duplex: FULL,   Negotiation: ENABLE
Mdi   : AUTO,   Flow-control: DISABLE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 50765440 bits/sec, Record time: 2018-07-04 19:01:29
Output peak rate 748160 bits/sec, Record time: 2018-07-04 19:01:29
Input:  850737 packets, 74865496 bytes
  Unicast:                  850735,  Multicast:                          2
  Broadcast:                     0,  Jumbo:                              0
  Discard:                       0,  Pause:                              0
  Frames:                        0

  Total Error:                   0
  CRC:                           0,  Giants:                             0
  Jabbers:                       0,  Fragments:                          0
  Runts:                         0,  DropEvents:                         0
```

```
  Alignments:                     0,  Symbols:                       0
  Ignoreds:                     0

Output:  11905 packets, 1000668 bytes
  Unicast:                      0,  Multicast:                     3
  Broadcast:                      0,  Jumbo:                        0
  Discard:                      0,  Pause:                     11902

  Total Error:                  0
  Collisions:                   0,  ExcessiveCollisions:              0
  Late Collisions:                 0,  Deferreds:                       0
  Buffers Purged:                  0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Display the running status, basic configuration, and statistics about forwarded packets on 100GE0/0/1.

```
<HUAWEI> display interface 100GE 0/0/1
100GE0/0/1 current state : DOWN
Line protocol current state : DOWN
Description:
Switch Port, Link-type : access(negotiated),
PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is
9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-
fc12-3456
Last physical up time   : -
Last physical down time : 2019-02-26 09:45:16
Current system time: 2019-02-26 09:47:43
Port Mode: COMMON FIBER
Speed : 100000, Loopback: NONE
Duplex: FULL,   Negotiation: DISABLE
Mdi   : -,      Flow-control: DISABLE
FEC   : NONE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: -
Output peak rate 0 bits/sec, Record time: -

Input:  0 packets, 0 bytes
Unicast:                      0,  Multicast:                     0
Broadcast:                      0,  Jumbo:                        0
Discard:                      0,  Pause:                       0

Total Error:                  0
CRC:                          0,  Giants:                      0
Runts:                        0,  Fragments:                      0
Alignments:                     0,  Symbols:                        0
Ignoreds:                     0

Output:  0 packets, 0 bytes
Unicast:                      0,  Multicast:                     0
Broadcast:                      0,  Jumbo:                        0
Discard:                      0,  Pause:                       0

                                                             Input bandwidth utilization
threshold : 80.00%
Output bandwidth utilization threshold: 80.00%
Input bandwidth utilization  :    0%
Output bandwidth utilization :
0%
```

Table 4-8 Description of this command output

Item	Description
current state	Current status of the interface: ● UP: The interface is physically Up. ● DOWN: The interface is physically Down. Protected port: An interface is added to an interface protection group and set to be a protected interface. To add an interface to an interface protection group and set the interface to be a protected interface, run the **port protect-group** and **protect-group member** commands. ● Administratively down: The administrator has run the **shutdown** command on the interface. ● TRIGGER DOWN (BFD): When BFD detects a fault, the physical status of the interface becomes Down according to the OAM association. ● TRIGGER DOWN (3AH): When 3AH detects a fault, the physical status of the interface becomes Down according to the OAM association. ● TRIGGER DOWN (1AG): When 1AG detects a fault, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(auto-defend): When the interface receives packets from an attack source, the physical status of the interface becomes Down. ● ERROR DOWN(efm-threshold-event): When the number of error frames, error codes, or error frame seconds of EFM OAM detected by the interface reaches or exceeds the threshold within a set period, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(efm-remote-failure): When EFM detects a remote failure, the physical status of the interface becomes Down according to the OAM association. ● ERROR DOWN(bpdu-protection): If an edge interface receives RST BPDUs after BPDU protection is enabled, the physical status of the edge interface becomes Down. ● ERROR DOWN(error-statistics): If the system detects that the number of error packets received by the interface exceeds the threshold, the physical status of the interface becomes Down. ● ERROR DOWN(transceiver-power-low): If the system detects that the optical power of the interface falls below the configured lower alarm threshold, the physical status of the interface becomes Down.

Item	Description
	● ERROR DOWN(port-security): When the number of learned MAC address entries reaches the threshold, the interface goes Down. ● ERROR DOWN(mac-address-flapping): When the learned MAC address flaps, the interface goes Down. ● ERROR DOWN(dhcp-packet-overspeed): When the DHCP packet rate of the interface exceeds the threshold, the physical status of the associated interface becomes Down. ● ERROR DOWN(link-flap): When the link flaps, the physical status of the associated interface becomes Down. ● ERROR DOWN(data-integrity-error): The chip memory identifier has a data integrity error and the physical status of the interface becomes Down. ● LOOPBACK-DETECT DOWN: The interface goes Down due to loopback detection. ● LINK-FLAP DOWN: The interface goes physically Down due to automatic link flapping detection. ● UP(E-TRUNK-DOWN): The Eth-Trunk interface goes Down because of E-Trunk negotiation. **NOTE** There is a delay before the interface state is reported, so an interface undergoes a short-time intermediate state before it transitions to the ERROR DOWN state. The intermediate state is ERROR DOWN (ERROR DOWN reason), up. This state does not affect functioning of the interface. When the physical status of the interface is ERROR DOWN(data-integrity-error), perform the following operations: 1. Check whether the **error-down auto-recovery cause data-integrity-error interval** *interval-value* command has been configured on the switch. If the command has been configured, go to step 2. Otherwise, go to step 3. 2. Check whether the interface restores to Up state after the time specified by *interval-value* expires. If the interface does not restore to Up state, go to step 3. 3. Run the **undo shutdown** command in the interface view to enable the interface and check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 4. 4. Run the **reset slot** command to restart the switch. After the switch restarts, check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 5. 5. Replace the switch.

Item	Description
Line protocol current state	Link layer protocol status of the interface: - UP: The link layer protocol of the interface is working properly. - UP (BFD status down): BFD associated with the interface is Down. - UP (Main BFD status down): The BFD session associated with the main interface becomes Down and is associated with the sub-interface status. This state is displayed only for sub-interfaces. - UP (spoofing): The link layer protocol of the interface is always Up with the spoofing feature enabled. - DOWN: The link-layer protocol status of the interface is Down or no IP address is assigned to the interface. For example, if no IP address is assigned to an IP service-capable interface, its protocol status is Down. - DOWN (CFM down): CFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes CFM Down. - DOWN (EFM down): EFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes EFM Down. - DOWN (DLDP down): DLDP detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes DLDP Down. - DOWN (MACsec down): MACsec is not enabled on the peer interface. In this case, the link layer protocol of the interface becomes MACsec Down. **NOTE** DOWN (MACsec down) is displayed only after the MACsec plug-in is installed. You can search for **Plug-in Usage Guide** at the Huawei technical support website (**Enterprise Network** or **Carrier**), and choose the desired plug-in usage guide based on the switch model and software version. If you do not have permission to access the website, contact technical support personnel. - DOWN (Observe-port forwarding down): The interface status becomes Down because the packet forwarding function is disabled on the observing port or in the observing port group where the port resides. - DOWN(BFD status down): indicates that BFD detects a fault and changes the link status of the interface to BFD DOWN. In this state, the interface discards Layer 2 and Layer 3 packets but permits BFD packets.

Item	Description
	- DOWN(Main BFD status down): indicates that BFD detects a fault and changes the link status of the main interface and its sub-interfaces to BFD DOWN. This state is applicable only to sub-interfaces. In this state, Layer 2 and Layer 3 packets are discarded, but BFD packets are permitted.
Description	Interface description. To configure the description for an interface, run the **description** command.
Switch Port	A Layer 2 interface. To switch an interface to the Layer 3 mode, run the **undo portswitch** command. If the interface is a Layer 3 interface, **Route Port** is displayed here.
PVID	Default VLAN ID of the interface.
Link-type	Link type of an interface, which is displayed only when the interface works in Layer 2 mode: ● access(configured): The interface is manually configured as the access type. ● hybrid: The interface is manually configured as the hybrid type. ● trunk(configured): The interface is manually configured as the trunk type. ● dot1q-tunnel: The interface is manually configured as the dot1q-tunnel type. ● access(negotiated): The interface is automatically negotiated as the access type. ● trunk(negotiated): The interface is automatically negotiated as the trunk type. To set the link type for an interface, run the **port link-type** command.
The Maximum Frame Length	Maximum frame length allowed by the interface. To set the maximum frame length, run the **jumboframe enable** command.
TPID	Type of frames that are supported on the interface. By default, this field displays 0x8100, indicating an 802.1Q frame. This field is displayed only for a Layer 2 interface.
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the interface.

Item	Description
Port Mode	Working mode of the interface: ● COMMON COPPER: The interface works as an electrical interface. ● COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: ● COMBO AUTO: The combo interface automatically selects the working mode. ● FORCE FIBER: The combo interface is configured as an optical interface. ● FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Supported rates	Rate supported by the interface. **NOTE** Only the XG electrical interface of MultiGE electrical interfaces and XG electrical interface on the ES5D21X08T00 subcard support this parameter.
Transceiver	Type of the optical module. ● This field is not displayed for electrical interfaces. ● If an optical or copper module is inserted into the optical interface, the field indicates the model of the optical or copper module. ● If an optical or copper module is not inserted into the optical interface, the field is not displayed. ● If the optical interface is connected to the high-speed cable, the field indicates the type of the cable. ● For the S5720-LI, S5720-SI, S5720S-LI, and S5735-S-I, If GPON optical module or a faulty optical module is installed on an optical interface, the field is displayed as ONLINE within 1 minute; the detailed type of the GPON optical module is displayed after 1 minute, and no information about other faulty optical modules is displayed.
Last physical up time	Last time the interface went Up physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.

Item	Description
Last physical down time	Last time the interface went Down physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the summer daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS ±HH:MM format.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto-negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface: ● FULL: The interface works in full-duplex mode. ● HALF: The interface works in half-duplex mode. ● In auto-negotiation mode, the **auto duplex** command configures the duplex mode of an interface. ● In non-auto-negotiation mode, the **duplex** command configures the duplex mode of an interface.
Negotiation	Auto-negotiation mode of the interface. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command. ● ENABLE: The interface works in auto-negotiation mode. ● DISABLE: The interface works in non-auto-negotiation mode. ● DISABLE(Only non-auto-negotiation is supported): The interface does not support the auto-negotiation mode and cannot have the **negotiation auto** command configured. Only the S6735-S supports this parameter.

Item	Description
Mdi	Network cable type of the interface. To configure the network cable type of an interface, run the **mdi** command. The Mdi field displays - for an optical interface.
Flow-control	Whether flow control is enabled: ● ENABLE: Flow control is enabled on the interface. ● DISABLE: Flow control and received flow control is disabled on the interface. ● RECEIVE ENABLE: Receive flow control is enabled on the interface. **NOTE** If the **flow-control** command has been executed to enable flow control on an Ethernet interface, or the **flow-control receive** command has been executed to enable received flow control on an Ethernet interface, this field displays **DISABLE** in the following situations: ● The interface is in Down state. ● The interface works in half-duplex mode.
FEC	Whether FEC is enabled on an interface: ● RS-FEC: RS-FEC is enabled on the interface. ● BASE-R: BASE-R FEC is enabled on the interface. ● NONE: The optical module is not properly installed and FEC is not configured; FEC is disabled; or FEC is not supported because a 40G optical module (except CFP 40GE optical module) is installed on a 100GE interface. When FEC is not configured, whether FEC is enabled on the interface depends on the medium. When a CFP 40GE/100GE optical module is installed on the interface, FEC cannot be configured on the interface and this field displays -.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate 0 bits/sec,Record time	Maximum rate of incoming packets and time when the maximum rate is reached.
Output peak rate 0 bits/sec,Record time	Maximum rate of outgoing packets and time when the maximum rate is reached.
Input	Total number of received packets.
Output	Total number of sent packets.

Item	Description
Unicast	Number of unicast packets that are received or sent by the interface.
Multicast	Number of multicast packets that are received or sent by the interface. For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S the value of this field contains the number of pause frames. For the S5736-S24T4XC, S5736-S24U4XC, S5736-S48T4XC, and S5736-S48U4XC, the value of the Multicast field contains the number of outgoing pause frames on GE electrical interfaces.
Broadcast	Number of broadcast packets that are received or sent by the interface.

Item	Description
Jumbo	This field includes the following values in the outbound direction of an interface: ● Number of sent Ethernet frames that exceed 1517 bytes with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I or number of sent Ethernet frames that exceed 1518 bytes with correct FCS values on other switch models. ● Number of sent VLAN frames that exceed 1517 bytes with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, number of sent VLAN frames that exceed 1522 bytes with correct FCS values on the S6735-S, S6720-EI and S6720S-EI, or number of sent VLAN frames that exceed 1518 bytes with correct FCS values on other switch models. This field includes the following values in the inbound direction of an interface: ● Number of received Ethernet frames with the length ranging from 1518 bytes to the configured maximum jumbo frame length and with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I or number of received Ethernet frames with the length ranging from 1519 bytes to the configured maximum jumbo frame length and with correct FCS values on other switch models. ● Number of received VLAN frames with the length ranging from 1518 bytes to the configured maximum jumbo frame length and with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, number of received VLAN frames with the length ranging from 1523 bytes to the configured maximum jumbo frame length and with correct FCS values on the S6735-S, S6720-EI and S6720S-EI, or number of received VLAN frames with the length ranging from 1519 bytes to the configured maximum jumbo frame length and with correct FCS values on other switch models. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame length configured on the interface and correct CRC values.

Item	Description
	To set the maximum jumbo frame length, run the **jumboframe enable** command. **NOTE** Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support statistics on Jumbo frames.
Discard	Number of packets discarded by the interface during physical layer detection. On the S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, after you run the **reset qos queue statistics** command, the number of packets discarded by the interface is cleared.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of packets with length ranging from 64 bytes to 1518 bytes and incorrect FCS values. For the S5720-LI, S5731-H, S5731S-H, S5731S-S, S5732-H, S5736-S, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-S, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received frames with length exceeding the maximum jumbo frame length.
Jabbers	The S5720-LI, S5720I-SI, S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-S, and S6730-H do not have the Jabbers field. On the other product models, this field indicates the number of received packets with length exceeding the maximum jumbo frame length and incorrect FCS values.

Item	Description
Fragments	Number of received fragmented packets. A fragmented packet is a packet shorter than 64 bytes and with incorrect CRC values. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value of this field contains the number of undersized frames with the correct CRC values received is displayed. On the S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S6720S-EI, S6735-S, and S6720-EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of received undersized frames with correct CRC values. For the S5720-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735-L, S300, S2730S-S, S5735-L1, S5735-L-I, S5735S-H, S5736-S, S6720S-S, S6720S-EI, S6735-S, and S6720-EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Frames	Number of packets with incorrect 802.3 length. **NOTE** Only the S2730S-S, S5735-L-I, S5735-L1, S5735S-L1, S300, S5735-L, S5735-S, S500, S5735-S-I, S6735-S, and S6720-EI support frame statistics collection.
Pause	Number of pause frames. **NOTE** The following interfaces do not support the function of collecting Pause frame statistics when flow control is not enabled: ● Four XGE optical interfaces and last eight GE electrical interfaces on the S5720-56C-HI ● Four XGE optical interfaces on the S5720-32C-HI-24S

Item	Description
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. **NOTE** If the command output contains only this field and the ExcessiveCollisions field is not displayed, the field also includes the number of frames that are canceled due to consecutive 16 collisions.
ExcessiveCollisions	Number of packets with 16 collisions and fail to be sent.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Buffers Purged	Number of packets aged in the cache. The S500, S5735-S, S5735S-S, S5735-S-I, S6720S-EI, S6735-S, and S6720-EI do not have the Buffers Purged field. On other models, the value of this field is always 0.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. For the SS1720GW-E, S1720GWR-E, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5720-LI, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.
Output bandwidth utilization	Outbound bandwidth usage. For the SS1720GW-E, S1720GWR-E, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5720-LI, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.

4.1.12 display interface brief

Function

The **display interface brief** command displays brief information about the status and configuration of interfaces.

Format

display interface brief [**main**]

Parameters

Parameter	Description	Value
main	Displays brief information about an Ethernet main interface, but does not display sub-interface information. If no sub-interface is configured on the main interface, the command output is the same as that without the main parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface brief** command displays brief information about interfaces, including the physical status, link layer protocol status, inbound and outbound bandwidth usage within a certain period, and numbers of sent and received error packets. This information helps locate faults on interfaces.

Precautions

To clear statistics on an interface, run the **reset counters interface** command.

Example

Display brief information about the status and configuration of interfaces.

```
<HUAWEI> display interface brief
PHY: Physical
*down: administratively down
#down: LBDT down

(l): loopback
(s): spoofing
(E): E-Trunk down
(b): BFD down
(e): ETHOAM down
```

```
(dl): DLDP down
(lb): LBDT block
(lp): Loop-detect block
(ms): MACsec down
(o): Observe-port forwarding down
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
GigabitEthernet0/0/1        up    up       0.06%   100%          0   21217388
GigabitEthernet0/0/2        up    up        100%   100%          0          0
GigabitEthernet0/0/3        up    up          0%   100%          0          0
GigabitEthernet0/0/4        up    up        100%   100%          0          0
GigabitEthernet0/0/5        up    up         99%   100%          0          0
GigabitEthernet0/0/6        down  down        0%     0%         10          0
GigabitEthernet0/0/7        down  down        0%     0%         12          0
GigabitEthernet0/0/8        down  down        0%     0%          0          0
GigabitEthernet0/0/9        down  down        0%     0%          0          0
GigabitEthernet0/0/10       down  down        0%     0%          0          0
GigabitEthernet0/0/11       down  down        0%     0%          0          0
GigabitEthernet0/0/12       down  down        0%     0%          0          0
GigabitEthernet0/0/13       down  down        0%     0%          0          0
GigabitEthernet0/0/14       down  down        0%     0%          0          0
GigabitEthernet0/0/15       down  down        0%     0%          0          0
GigabitEthernet0/0/16       down  down        0%     0%          0          0
GigabitEthernet0/0/17       down  down        0%     0%          0          0
GigabitEthernet0/0/18       down  down        0%     0%          0          0
GigabitEthernet0/0/19       down  down        0%     0%          0          0
GigabitEthernet0/0/20       down  down        0%     0%          0          0
GigabitEthernet0/0/21       down  down        0%     0%          0          0
GigabitEthernet0/0/22       down  down        0%     0%          0          0
GigabitEthernet0/0/23       down  down        0%     0%          0          0
GigabitEthernet0/0/24       down  down        0%     0%          0          0
MEth0/0/1                   down  down        0%     0%          0          0
NULL0                       up    up(s)       0%     0%          0          0
```

Table 4-9 Description of the **display interface brief** command output

Item	Description
Interface	Type and number of an interface.

Item	Description
PHY	Physical status of an interface: - up: indicates that the interface is working properly. - down: indicates that the physical layer of the interface fails. - *down: Administratively Down, indicating that the administrator has run the **shutdown** command on the interface. - ^down: indicates that the interface is a backup interface. - #down: LBDT down, indicating that loop detection is enabled on the interface. The interface is shut down when the device detects a loop on the downstream network or between interfaces. - -down: indicates that the interface is shut down due to automatic link flapping detection. - (l): indicates that the loopback function is enabled on the interface. - (b): indicates that the physical layer of the interface is in BFD down state.

Item	Description
Protocol	Link layer protocol status of the interface: - up: indicates that the interface is working properly. - down: indicates that the link layer protocol fails. - up(lp)/down(lp): indicates that the interface status is Block due to the loop detected by the L2VPN loop detection function on the interface. - (s): indicates that the spoofing function is enabled on the interface. - (E): indicating that the Eth-Trunk goes down because of the E-Trunk negotiation failure. - (b): indicates that the link layer of the interface is in BFD down state. - (e): indicates that the link layer of the interface is in ETHOAM down state. - (dl): indicates that the link layer of the interface is in DLDP down state. - (lb): indicates that the interface is blocked due to loops on the downstream network or between interfaces. - (lp): indicates that the interface status becomes Down due to loops in the VLAN where the interface resides. - (ms): indicates that the link layer of the interface is in MACsec down state because MACsec is not enabled on the peer interface. **NOTE** (ms): MACsec down is displayed only after the MACsec plug-in is installed. You can search for **Plug-in Usage Guide** at the Huawei technical support website (**Enterprise Network** or **Carrier**), and choose the desired plug-in usage guide based on the switch model and software version. If you do not have permission to access the website, contact technical support personnel. - (o): indicates that the interface status becomes Down because the packet forwarding function is disabled on the observing port or in the observing port group where the port resides.

Item	Description
InUti	Average inbound bandwidth usage of an interface within the last 300 seconds. Average inbound bandwidth usage within the last 300 seconds = Average inbound traffic rate within the last 300 seconds/Interface bandwidth When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the interface bandwidth becomes lower, for example, the **speed** command is executed to reduce the bandwidth of an Ethernet interface, the bandwidth usage be displayed as 100% because the traffic volume is not adjusted in time. "--" indicates that an interface does not support the display of bandwidth usage.
OutUti	Average outbound bandwidth usage within the last 300 seconds. Average outbound bandwidth usage within the last 300 seconds = Average outbound traffic rate within the last 300 seconds/Interface bandwidth When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the interface bandwidth becomes lower, for example, the **speed** command is executed to reduce the bandwidth of an Ethernet interface, the bandwidth usage may be displayed as 100% because the traffic volume is not adjusted in time. "--" indicates that an interface does not support the display of bandwidth usage.
inErrors	The number of error packets received by an interface. The value ranges from 0 to 4294967295. The count restarts after the value exceeds the upper limit. The value becomes 0 when you run the **reset counters interface** command in the user view or when the number of received packets reaches the maximum value 0xFFFFFFFF.
outErrors	The number of error packets sent by an interface. The value ranges from 0 to 4294967295. The count restarts after the value exceeds the upper limit. The value becomes 0 when you run the **reset counters interface** command in the user view or when the number of sent packets reaches the maximum value 0xFFFFFFFF.

4.1.13 display interface description

Function

The **display interface description** command displays the description of an interface.

Format

display interface description [*interface-type* [*interface-number*]]

display interface description [*interface-type*] **main**

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the description of a specified interface. If an interface type is specified but no interface number is specified, the description of all interfaces of the specified type is displayed.	-
main	Displays the description of the main interface. ● If an interface has no sub-interfaces, description about the interface is displayed regardless of whether you specify the **main** parameter. ● If an interface has sub-interfaces, description about the interface and sub-interfaces is displayed if you do not specify the **main** parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface** command can also display the description of an interface. To quickly view the description of an interface, you are advised to use the **display interface description** command.

Precautions

If no interface type is specified, the description of all interfaces is displayed. If an interface type is specified but no interface number is specified, the description of all interfaces of the specified type is displayed.

If there is a great deal of statistics about traffic on Eth-Trunk interfaces, you are recommended to specify *trunk-id* to filter output information. Otherwise, a problem may occur due to excessive output information: The displayed information is repeatedly refreshed, and therefore required information cannot be located.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Display the description of GE0/0/1.

```
<HUAWEI> display interface description gigabitethernet 0/0/1
PHY: Physical
*down: administratively down
#down: LBDT down
(l): loopback
(s): spoofing
(E): E-Trunk down
(b): BFD down
(e): ETHOAM down
(dl): DLDP down
(lb): LBDT block
(ms): MACsec down
Interface                     PHY     Protocol Description
GE0/0/1                       down    down
```

Table 4-10 Description of the **display interface description** command output

Item	Description
Interface	Type and number of an interface. If the bandwidth of an interface exceeds 1 GB, the bandwidth value is displayed following the interface name.

Item	Description
PHY	Physical status of an interface: ● up: indicates that the interface is working properly. ● down: indicates that the physical layer of the interface fails. ● *down: administratively down, indicating that the administrator has run the **shutdown** command on the interface. ● #down: LBDT down, indicating that loopback detection is enabled on the interface. The interface is shut down when the device detects a loop on the downstream network or between interfaces. ● (l): loopback, indicating that the loopback function is enabled on the interface. ● (b): BFD down, indicating that the physical layer of the interface is in BFD Down state.
Protocol	Link layer protocol status of the interface: ● up: indicates that the interface is working properly. ● down: indicates that the link layer protocol of the interface fails. ● (s): spoofing, indicating that the spoofing function is enabled on the interface. ● (E): E-Trunk down, indicating that the interface goes down because of the E-Trunk negotiation failure. ● (b): indicates that the link layer of the interface is in BFD down state. ● (e): ETHOAM down, indicating that the link layer protocol of the interface is in ETHOAM down state. ● (dl): DLDP down, indicating that the link layer protocol of the interface is in DLDP down state. ● (lb): indicates that the interface is blocked due to loops on the downstream network or between interfaces. ● (ms): MACsec down, indicating that the interface is Down because MACsec is not enabled on the peer interface. **NOTE** (ms): MACsec down is displayed only after the MACsec plug-in is installed. You can search for **Plug-in Usage Guide** at the Huawei technical support website (**Enterprise Network** or **Carrier**), and choose the desired plug-in usage guide based on the switch model and software version. If you do not have permission to access the website, contact technical support personnel.
Description	Interface description.

4.1.14 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Display IP information about VLANIF15.

```
<HUAWEI> display ip interface vlanif 15
Vlanif15 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 766390, bytes : 41540847, multicasts : 681817
output packets : 242239, bytes : 14679482, multicasts : 172333
Directed-broadcast packets:
 received packets:            0, sent packets:            0
 forwarded packets:           0, dropped packets:           0
Internet Address is 10.1.1.119/24
Broadcast address : 10.1.1.255
TTL being 1 packet number:    164035
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
```

Table 4-11 Description of the **display ip interface** command output

Item	Description
Vlanif15 current state	Physical status of the interface: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the administrator has run the **shutdown (interface view)** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: The link layer protocol of the interface is running properly. ● DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface or a serial interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 766390, bytes : 41540847, multicasts : 681817	Total number of packets, bytes, and multicast packets received by the interface.
output packets : 242239, bytes : 14679482, multicasts : 172333	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
Internet Address is	IP address assigned to the interface and mask length.
Broadcast address	Broadcast address of the interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.

Item	Description
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

Display brief IP information about VLANIF15.

```
<HUAWEI> display ip interface brief vlanif 15
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                         IP Address/Mask      Physical   Protocol
Vlanif15                          10.1.1.119/24        up         up
```

Table 4-12 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down	^down: indicates that the interface is a backup interface.
(l): loopback	The letter "l" refers to loopback.

Item	Description
(s): spoofing	The letter "s" refers to spoofing.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
Interface	Interface type and number.
IP Address/Mask	IP address and mask of an interface.
Physical	Physical status of an interface: ● Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. ● Down: indicates that the interface becomes faulty. ● *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. ● !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.
Protocol	Link protocol status of the interface: ● Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. ● Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

4.1.15 display ip interface description

Function

The **display ip interface description** command displays IP-related information (such as the IP address, subnet mask, physical layer status, link layer protocol status, and number of interfaces in different states) and description of an interface.

Format

display ip interface description [*interface-type* [*interface-number*] | *interface-type* &<1-8> | **slot** *slot-number* [**card** *card-number*]]

Parameters

Parameter	Description	Value
interface-type	Indicates the interface type. If no interface type is specified, IP-related configurations and statistics of all interfaces are displayed.	-
interface-number	Indicates the interface number, which is used together with *interface-type* to identify an interface. If no interface number is specified, IP-related configurations and statistics of interfaces in the same type are displayed.	-
interface-type	Indicates that the command can display IP-related information about interfaces of multiple types. The command can display IP-related information about interfaces in a maximum of eight types.	-
slot *slot-number*	Specifies the interface board number.	-
card *card-number*	Indicates the card number. If no card number is specified, IP-related information about all interfaces on all cards in a specified slot is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Instead of running the **display ip interface brief** and **display interface description** commands, you can run the **display ip interface description** command to view both IP-related information and description of an interface, which facilitates the user operation.

The **display ip interface description** command cannot display information about Layer 2 interfaces. When it runs on an Eth-Trunk interface, it displays the status and description of Eth-Trunk member interfaces.

Example

View IP-related information and description of a specified interface.

```
<HUAWEI> display ip interface description
Codes:
      Ana(Analogmodem),       Asy(Async),             Cell(Cellular),
      Dia(Dialer),            Eth(Ethernet)           GE(GigabitEthernet),
      H(Hssi),                Ima(Ima-group),         Loop(LoopBack),
      MTun(MTunnel),          S(Serial),              Tun(Tunnel),
      VE(Virtual-Ethernet),   VT(Virtual-Template)

      d(dampened),            D(down),                *D(administratively down)
      ^D(standby),            l(loopback),            s(spoofing),
      U(up)                   E(E-Trunk down)



------------------------------------------------------------------------------
Number of interfaces whose physical status is Up: 9
Number of interfaces whose physical status is Down: 1
Number of interfaces whose protocol status is Up: 9
Number of interfaces whose protocol status is Down: 1

Interface                   IP Address/Mask    Phy  Prot Description
Loop0                       10.3.0.2/32        U    U(s)
Loop1                       unassigned         U    U(s)
MEth0/0/1                   192.168.150.143/24 U    U
NULL0                       unassigned         U    U(s)
Tun1                        unassigned         U    D
Vlanif10                    unassigned         D    D
Vlanif20                    10.1.2.2/24        D    D
Vlanif30                    10.1.1.1/24        D    D
Vlanif100                   unassigned         *D   D
```

Table 4-13 Description of the **display ip interface description** command output

Item	Description
Codes:	The following information provides the full spelling and explanation of the abbreviated interface names, physical status, and link layer protocols. Full spelling of the abbreviated interface names is as follows: - Ana: Analogmodem interfaces - Asy: Async interfaces - Cell: Cellular interfaces - Dia: Dialer interfaces - Eth: Ethernet interfaces - GE: GigabitEthernet interfaces - H: Hssi interfaces - Ima: IMA-Group interfaces - Loop: Loopback interfaces - MTun: MTunnel interfaces - S: Serial interfaces - Tun: Tunnel interfaces - VE: Virtual-Ethernet interfaces - VT: Virtual-Template interfaces Explanation of the abbreviated physical status of the interface is as follows: - U: indicates that the physical status of the interface is Up.U(l) indicates that the interface is enabled with the loopback function. - D: indicates that the physical status of the interface is Down. - *D: indicates that the network administrator has run the **shutdown** command on the interface. - !D: indicates that the FIB module is in the overload suspension state. The link layer protocol of the interface goes Down. - ^D: indicates that the FIB module is in the standby state. - s: indicates that the interface is in spoofing status. - E: the Eth-Trunk goes Down because of E-Trunk negotiation. Explanation of the abbreviated link layer protocol status is as follows:

Item	Description
	- U: indicates that the status of the link layer protocol on the interface is Up. U(s) indicates that the link layer protocol of the interface is Up even though the interface is not configured with an IP address. (s) is an inherent attribute of the interface and will be displayed when the interface is configured with an IP address. (d) indicates that the protocol module of the interface is dampened. - D: indicates that the link layer protocol of the interface is Down or no IP address is assigned to the interface.
Number of interfaces whose physical status is Up:	Indicates the number of interfaces whose physical status is Up.
Number of interfaces whose physical status is Down:	Indicates the number of interfaces whose physical status is Down.
Number of interfaces whose protocol status is Up:	Indicates the number of interfaces whose link layer protocol is Up.
Number of interfaces whose protocol status is Down:	Indicates the number of interfaces whose link layer protocol is Down.
Interface	Indicates the name and number of an interface.
IP Address/Mask	Indicates the IP address and subnet mask of an interface.
Phy	Indicates the physical status of an interface.
Prot	Indicates the link layer protocol status of an interface.
Description	Indicates the description of an interface, expressed in characters. A maximum of 20 characters can be displayed. When the length of the description is greater than 20 characters, only the first 16 characters are displayed and the last 3 characters are replaced by ellipsis (...). If the description of an interface is the default setting, no information is displayed.

4.1.16 display this interface

Function

The **display this interface** command displays interface information in the current interface view.

Format

display this interface

Parameters

None

Views

Interface view

Default Level

1: Monitoring level

Usage Guidelines

In the interface view, you can run the **display this interface** command to rapidly view the status of the interface and packet statistics on the interface.

Example

Display information about GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this interface
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Description:
Switch Port,Link-type : access(negotiated),
 PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc12-3456
Last physical up time   : -
Last physical down time : 2000-04-01 23:55:43
Current system time: 2012-08-24 00:41:35+08:00
Port Mode: COMMON FIBER, Transceiver: 1000_BASE_SX_SFP
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : -, Flow-control: DISABLE
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec, Record time: 2007-12-26 07:23:14
Output peak rate 0 bits/sec, Record time: 2007-12-26 07:23:14

Input:  0 packets, 0 bytes
  Unicast:                       0,  Multicast:                       0
  Broadcast:                     0,  Jumbo:                           0
  Discard:                       0,  Pause:                           0
  Frames:                        0
```

```
  Total Error:                     0
  CRC:                             0,  Giants:                          0
  Jabbers:                         0,  Fragments:                       0
  Runts:                           0,  DropEvents:                      0
  Alignments:                      0,  Symbols:                         0
  Ignoreds:                        0

Output:  0 packets, 0 bytes
  Unicast:                         0,  Multicast:                       0
  Broadcast:                       0,  Jumbo:                           0
  Discard:                         0,  Pause:                           0

  Total Error:                     0
  Collisions:                      0,  ExcessiveCollisions:             0
  Late Collisions:                 0,  Deferreds:                       0
  Buffers Purged:                  0

    Input bandwidth utilization threshold : 80.00%
    Output bandwidth utilization threshold: 80.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-14 Description of this command output

Item	Description
current state	Current status of the interface: - UP: The interface is physically Up. - DOWN: The interface is physically Down. Protected port: An interface is added to an interface protection group and set to be a protected interface. To add an interface to an interface protection group and set the interface to be a protected interface, run the **port protect-group** and **protect-group member** commands. - Administratively down: The administrator has run the **shutdown** command on the interface. - TRIGGER DOWN (BFD): When BFD detects a fault, the physical status of the interface becomes Down according to the OAM association. - TRIGGER DOWN (3AH): When 3AH detects a fault, the physical status of the interface becomes Down according to the OAM association. - TRIGGER DOWN (1AG): When 1AG detects a fault, the physical status of the interface becomes Down according to the OAM association. - ERROR DOWN(auto-defend): When the interface receives packets from an attack source, the physical status of the interface becomes Down. - ERROR DOWN(efm-threshold-event): When the number of error frames, error codes, or error frame seconds of EFM OAM detected by the interface reaches or exceeds the threshold within a set period, the physical status of the interface becomes Down according to the OAM association. - ERROR DOWN(efm-remote-failure): When EFM detects a remote failure, the physical status of the interface becomes Down according to the OAM association. - ERROR DOWN(bpdu-protection): If an edge interface receives RST BPDUs after BPDU protection is enabled, the physical status of the edge interface becomes Down. - ERROR DOWN(error-statistics): If the system detects that the number of error packets received by the interface exceeds the threshold, the physical status of the interface becomes Down. - ERROR DOWN(transceiver-power-low): If the system detects that the optical power of the interface falls below the configured lower alarm threshold, the physical status of the interface becomes Down.

Item	Description
	- ERROR DOWN(port-security): When the number of learned MAC address entries reaches the threshold, the interface goes Down. - ERROR DOWN(mac-address-flapping): When the learned MAC address flaps, the interface goes Down. - ERROR DOWN(dhcp-packet-overspeed): When the DHCP packet rate of the interface exceeds the threshold, the physical status of the associated interface becomes Down. - ERROR DOWN(link-flap): When the link flaps, the physical status of the associated interface becomes Down. - ERROR DOWN(data-integrity-error): The chip memory identifier has a data integrity error and the physical status of the interface becomes Down. - LOOPBACK-DETECT DOWN: The interface goes Down due to loopback detection. - LINK-FLAP DOWN: The interface goes physically Down due to automatic link flapping detection. - UP(E-TRUNK-DOWN): The Eth-Trunk interface goes Down because of E-Trunk negotiation. **NOTE** There is a delay before the interface state is reported, so an interface undergoes a short-time intermediate state before it transitions to the ERROR DOWN state. The intermediate state is ERROR DOWN (ERROR DOWN reason), up. This state does not affect functioning of the interface. When the physical status of the interface is ERROR DOWN(data-integrity-error), perform the following operations: 1. Check whether the **error-down auto-recovery cause data-integrity-error interval** *interval-value* command has been configured on the switch. If the command has been configured, go to step 2. Otherwise, go to step 3. 2. Check whether the interface restores to Up state after the time specified by *interval-value* expires. If the interface does not restore to Up state, go to step 3. 3. Run the **undo shutdown** command in the interface view to enable the interface and check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 4. 4. Run the **reset slot** command to restart the switch. After the switch restarts, check whether the interface restores to Up state. If the interface does not restore to Up state, go to step 5. 5. Replace the switch.

Item	Description
Line protocol current state	Link layer protocol status of the interface: - UP: The link layer protocol of the interface is working properly. - UP (BFD status down): BFD associated with the interface is Down. - UP (Main BFD status down): The BFD session associated with the main interface becomes Down and is associated with the sub-interface status. This state is displayed only for sub-interfaces. - UP (spoofing): The link layer protocol of the interface is always Up with the spoofing feature enabled. - DOWN: The link-layer protocol status of the interface is Down or no IP address is assigned to the interface. For example, if no IP address is assigned to an IP service-capable interface, its protocol status is Down. - DOWN (CFM down): CFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes CFM Down. - DOWN (EFM down): EFM detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes EFM Down. - DOWN (DLDP down): DLDP detects a fault or receives a fault notification message from its associated module. In this case, the link layer protocol of the interface becomes DLDP Down. - DOWN (MACsec down): MACsec is not enabled on the peer interface. In this case, the link layer protocol of the interface becomes MACsec Down. **NOTE** DOWN (MACsec down) is displayed only after the MACsec plug-in is installed. You can search for **Plug-in Usage Guide** at the Huawei technical support website (**Enterprise Network** or **Carrier**), and choose the desired plug-in usage guide based on the switch model and software version. If you do not have permission to access the website, contact technical support personnel. - DOWN (Observe-port forwarding down): The interface status becomes Down because the packet forwarding function is disabled on the observing port or in the observing port group where the port resides. - DOWN(BFD status down): indicates that BFD detects a fault and changes the link status of the interface to BFD DOWN. In this state, the interface discards Layer 2 and Layer 3 packets but permits BFD packets.

Item	Description
	- DOWN(Main BFD status down): indicates that BFD detects a fault and changes the link status of the main interface and its sub-interfaces to BFD DOWN. This state is applicable only to sub-interfaces. In this state, Layer 2 and Layer 3 packets are discarded, but BFD packets are permitted.
Description	Interface description. To configure the description for an interface, run the **description** command.
Switch Port	A Layer 2 interface. To switch an interface to the Layer 3 mode, run the **undo portswitch** command. If the interface is a Layer 3 interface, **Route Port** is displayed here.
PVID	Default VLAN ID of the interface.
Link-type	Link type of an interface, which is displayed only when the interface works in Layer 2 mode: ● access(configured): The interface is manually configured as the access type. ● hybrid: The interface is manually configured as the hybrid type. ● trunk(configured): The interface is manually configured as the trunk type. ● dot1q-tunnel: The interface is manually configured as the dot1q-tunnel type. ● access(negotiated): The interface is automatically negotiated as the access type. ● trunk(negotiated): The interface is automatically negotiated as the trunk type. To set the link type for an interface, run the **port link-type** command.
The Maximum Frame Length	Maximum frame length allowed by the interface. To set the maximum frame length, run the **jumboframe enable** command.
TPID	Type of frames that are supported on the interface. By default, this field displays 0x8100, indicating an 802.1Q frame. This field is displayed only for a Layer 2 interface.
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the interface.

Item	Description
Port Mode	Working mode of the interface: - COMMON COPPER: The interface works as an electrical interface. - COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: - COMBO AUTO: The combo interface automatically selects the working mode. - FORCE FIBER: The combo interface is configured as an optical interface. - FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Supported rates	Rate supported by the interface. **NOTE** Only the XG electrical interface of MultiGE electrical interfaces and XG electrical interface on the ES5D21X08T00 subcard support this parameter.
Transceiver	Type of the optical module. - This field is not displayed for electrical interfaces. - If an optical or copper module is inserted into the optical interface, the field indicates the model of the optical or copper module. - If an optical or copper module is not inserted into the optical interface, the field is not displayed. - If the optical interface is connected to the high-speed cable, the field indicates the type of the cable. - For the S5720-LI, S5720-SI, S5720S-LI, and S5735-S-I, If GPON optical module or a faulty optical module is installed on an optical interface, the field is displayed as ONLINE within 1 minute; the detailed type of the GPON optical module is displayed after 1 minute, and no information about other faulty optical modules is displayed.
Last physical up time	Last time the interface went Up physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.

Item	Description
Last physical down time	Last time the interface went Down physically. If this field displays "-", the physical status of the interface does not change. If the system is configured with a time zone and is in the summer daylight saving time, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS ±HH:MM format.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto-negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface: ● FULL: The interface works in full-duplex mode. ● HALF: The interface works in half-duplex mode. ● In auto-negotiation mode, the **auto duplex** command configures the duplex mode of an interface. ● In non-auto-negotiation mode, the **duplex** command configures the duplex mode of an interface.
Negotiation	Auto-negotiation mode of the interface. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command. ● ENABLE: The interface works in auto-negotiation mode. ● DISABLE: The interface works in non-auto-negotiation mode. ● DISABLE(Only non-auto-negotiation is supported): The interface does not support the auto-negotiation mode and cannot have the **negotiation auto** command configured. Only the S6735-S supports this parameter.

Item	Description
Mdi	Network cable type of the interface. To configure the network cable type of an interface, run the **mdi** command. The Mdi field displays - for an optical interface.
Flow-control	Whether flow control is enabled: ● ENABLE: Flow control is enabled on the interface. ● DISABLE: Flow control and received flow control is disabled on the interface. ● RECEIVE ENABLE: Receive flow control is enabled on the interface. **NOTE** If the **flow-control** command has been executed to enable flow control on an Ethernet interface, or the **flow-control receive** command has been executed to enable received flow control on an Ethernet interface, this field displays **DISABLE** in the following situations: ● The interface is in Down state. ● The interface works in half-duplex mode.
FEC	Whether FEC is enabled on an interface: ● RS-FEC: RS-FEC is enabled on the interface. ● BASE-R: BASE-R FEC is enabled on the interface. ● NONE: The optical module is not properly installed and FEC is not configured; FEC is disabled; or FEC is not supported because a 40G optical module (except CFP 40GE optical module) is installed on a 100GE interface. When FEC is not configured, whether FEC is enabled on the interface depends on the medium. When a CFP 40GE/100GE optical module is installed on the interface, FEC cannot be configured on the interface and this field displays -.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate 0 bits/sec,Record time	Maximum rate of incoming packets and time when the maximum rate is reached.
Output peak rate 0 bits/sec,Record time	Maximum rate of outgoing packets and time when the maximum rate is reached.
Input	Total number of received packets.
Output	Total number of sent packets.

Item	Description
Unicast	Number of unicast packets that are received or sent by the interface.
Multicast	Number of multicast packets that are received or sent by the interface. For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S the value of this field contains the number of pause frames. For the S5736-S24T4XC, S5736-S24U4XC, S5736-S48T4XC, and S5736-S48U4XC, the value of the Multicast field contains the number of outgoing pause frames on GE electrical interfaces.
Broadcast	Number of broadcast packets that are received or sent by the interface.

Item	Description
Jumbo	This field includes the following values in the outbound direction of an interface: - Number of sent Ethernet frames that exceed 1517 bytes with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I or number of sent Ethernet frames that exceed 1518 bytes with correct FCS values on other switch models. - Number of sent VLAN frames that exceed 1517 bytes with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, number of sent VLAN frames that exceed 1522 bytes with correct FCS values on the S6735-S, S6720-EI and S6720S-EI, or number of sent VLAN frames that exceed 1518 bytes with correct FCS values on other switch models. This field includes the following values in the inbound direction of an interface: - Number of received Ethernet frames with the length ranging from 1518 bytes to the configured maximum jumbo frame length and with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I or number of received Ethernet frames with the length ranging from 1519 bytes to the configured maximum jumbo frame length and with correct FCS values on other switch models. - Number of received VLAN frames with the length ranging from 1518 bytes to the configured maximum jumbo frame length and with correct FCS values on the S200, S1730S-S1, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, number of received VLAN frames with the length ranging from 1523 bytes to the configured maximum jumbo frame length and with correct FCS values on the S6735-S, S6720-EI and S6720S-EI, or number of received VLAN frames with the length ranging from 1519 bytes to the configured maximum jumbo frame length and with correct FCS values on other switch models. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame length configured on the interface and correct CRC values.

Item	Description
	To set the maximum jumbo frame length, run the **jumboframe enable** command. **NOTE** Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support statistics on Jumbo frames.
Discard	Number of packets discarded by the interface during physical layer detection. On the S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, after you run the **reset qos queue statistics** command, the number of packets discarded by the interface is cleared.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of packets with length ranging from 64 bytes to 1518 bytes and incorrect FCS values. For the S5720-LI, S5731-H, S5731S-H, S5731S-S, S5732-H, S5736-S, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value of this field includes the number of received packets longer than the maximum jumbo frame length and with incorrect FCS values. For the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-S, the value of this field contains the number of received packets with length ranging from 1518 bytes to the jumbo frame size configured on the interface and incorrect FCS values.
Giants	Number of received frames with length exceeding the maximum jumbo frame length.
Jabbers	The S5720-LI, S5720I-SI, S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-S, and S6730-H do not have the Jabbers field. On the other product models, this field indicates the number of received packets with length exceeding the maximum jumbo frame length and incorrect FCS values.

Item	Description
Fragments	Number of received fragmented packets. A fragmented packet is a packet shorter than 64 bytes and with incorrect CRC values. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value of this field contains the number of undersized frames with the correct CRC values received is displayed. On the S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S6720S-EI, S6735-S, and S6720-EI, the command output does not contain the Fragments field to display statistics about received fragmented packets.
Runts	Number of received undersized frames with correct CRC values. For the S5720-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735-L, S300, S2730S-S, S5735-L1, S5735-L-I, S5735S-H, S5736-S, S6720S-S, S6720S-EI, S6735-S, and S6720-EI, the value of this field includes the number of received fragmented packets shorter than 64 bytes and with incorrect CRC values.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames whose OpCode is not PAUSE.
Frames	Number of packets with incorrect 802.3 length. **NOTE** Only the S2730S-S, S5735-L-I, S5735-L1, S5735S-L1, S300, S5735-L, S5735-S, S500, S5735-S-I, S6735-S, and S6720-EI support frame statistics collection.
Pause	Number of pause frames. **NOTE** The following interfaces do not support the function of collecting Pause frame statistics when flow control is not enabled: ● Four XGE optical interfaces and last eight GE electrical interfaces on the S5720-56C-HI ● Four XGE optical interfaces on the S5720-32C-HI-24S

Item	Description
Collisions	Number of packets with 1 to 15 collisions during packet forwarding. **NOTE** If the command output contains only this field and the ExcessiveCollisions field is not displayed, the field also includes the number of frames that are canceled due to consecutive 16 collisions.
ExcessiveCollisions	Number of packets with 16 collisions and fail to be sent.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Buffers Purged	Number of packets aged in the cache. The S500, S5735-S, S5735S-S, S5735-S-I, S6720S-EI, S6735-S, and S6720-EI do not have the Buffers Purged field. On other models, the value of this field is always 0.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. For the SS1720GW-E, S1720GWR-E, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5720-LI, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.
Output bandwidth utilization	Outbound bandwidth usage. For the SS1720GW-E, S1720GWR-E, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5720-LI, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, the bandwidth usage of Giants packets is calculated based on the configured jumbo frame length. To set the maximum jumbo frame length, run the **jumboframe enable** command.

4.1.17 interface

Function

The **interface** command displays the interface view or sub-interface view.

The **undo interface** command deletes a sub-interface.

Format

interface *interface-type interface-number*

undo interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character. To create a sub-interface, enter the sub-interface view, or delete a sub-interface, specify *interface-number* in the format of main interface number.sub-interface number. For example, the number of sub-interface 1 on GE0/0/1 is GE0/0/1.1.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the specified interface view is displayed, you can set attributes for the interface.

Precautions

- VLAN termination sub-interfaces cannot be created on a VCMP client.
- You need to set the interface type before creating a sub-interface. Only hybrid and trunk interfaces on the preceding series of cards support Ethernet sub-interface configuration.
- Physical interfaces cannot be created or deleted. You can only run the **interface** *interface-type interface-number* command to enter the view of an existing physical interface.
- Sub-interfaces can be created. Run the **interface** *interface-type interface-number* command to create a sub-interface and enter the sub-interface view.
- Sub-interfaces can be deleted. Run the **undo interface** *interface-type interface-number* command to delete a sub-interface.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Display the view of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1]
```

Create sub-interface GE0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
```

Delete sub-interface GE0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] undo interface gigabitethernet 0/0/1.1
```

4.1.18 mtu (Interface view)

Function

Using the **mtu** command, you can set the maximum transmission unit (MTU) of an interface.

Using the **undo mtu** command, you can restore the default MTU of an interface.

By default, the MTU of an interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of an interface.	- For a physical interface, a VLANIF interface, an Eth-Trunk interface, a physical sub-interface, and an Eth-Trunk sub-interface, the value is an integer that ranges from 128 to 9216, in bytes. - For a VE sub-interface, the value is an integer that ranges from 46 to 1500, in bytes. - For a VBDIF interface, the value is an integer that ranges from 128 to 1560, in bytes. - For a tunnel interface, the value is an integer. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S the value ranges from 128 to 9216. For other switch models, the value ranges from 128 to 1530.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum transmission unit (MTU) determines the maximum number of bytes in IP packets each time a sender can send. The MTU of an IP packet refers to the number of bytes from the IP header of the packet to the data.

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Generally, the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU. If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

The switch checks the MTU of CPU-forwarded IP packets. If the packet length is greater than the MTU, the switch fragments the packets. When the length of an IP packet forwarded by the chip is greater than the MTU, switches of different models and with different configurations process the packet differently.

Table 4-15 Packet processing on switches of different models and with different configurations

Model	Configuration	Packet Type	Result
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S	The **ipv4 fragment enable** command is not configured.	GRE packet	If the packet carries the fragment flag, the switch fragments the packet before forwarding it. Otherwise, the switch discards the packet.
	The **ipv4 fragment enable** command is not configured.	Non-GRE packet	The switch forwards the packet without fragmenting it.
	The **ipv4 fragment enable** command is configured.	GRE packet	If the packet carries the fragment flag, the switch fragments the packet before forwarding it. Otherwise, the switch discards the packet.
	The **ipv4 fragment enable** command is configured.	Non-GRE packet	The switch fragments the packet before forwarding it.
Devices except S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S	NA	All packet types	The switch forwards the packet without fragmenting it.

Prerequisites

Run the **undo portswitch** command to change the working mode of Ethernet physical interfaces from Layer 2 mode to Layer 3 mode.

Precautions

- After changing the maximum transmission unit (MTU) using the **mtu** command on an interface, you need to restart the interface to make the new MTU take effect. To restart the interface, run the **shutdown** command and then the **undo shutdown** command, or run the **restart** command in the interface view.

- If IPv6 is run on a tunnel interface and the MTU set using the **mtu** command on the interface is smaller than 1280, IPv6 works abnormally on this interface. To prevent this problem, set the MTU of a tunnel interface to a value greater than or equal to 1280 if IPv6 runs on the tunnel interface.
- Configuring the MTU of an interface affects the maximum number of bytes for IP packets to be sent by the interface at a time. This configuration also affects the maximum frame length of sent Ethernet packets. The Ethernet packet size cannot exceed the maximum frame length allowed by the peer interface, which can be set using the **jumboframe enable** command.

Example

Set the MTU of GE0/0/1 to 1200 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mtu 1200
[HUAWEI-GigabitEthernet0/0/1] restart
```

Set the MTU of the VLANIF interface to 1492 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] mtu 1492
[HUAWEI-Vlanif100] restart
```

Set the MTU of Tunnel 1 to 1492.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mtu 1492
[HUAWEI-Tunnel1] shutdown
[HUAWEI-Tunnel1] undo shutdown
```

4.1.19 port description

Function

The **port description** command configures description about the device type connected to an interface.

The **undo port description** command restores the default setting.

By default, no description about the device type connected to an interface is configured.

Format

port description { **router** | **switch** | **phone** | **desktop** }

undo port description

Parameters

Parameter	Description	Value
router	Indicates that the interface is connected to a router.	-
switch	Indicates that the interface is connected to a switch.	-
phone	Indicates that the interface is connected to an IP phone.	-
desktop	Indicates that the interface is connected to a desktop terminal, such as a PC.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure description about the device type connected to an interface to facilitate device management and maintenance. For example, you can run **port description router** command to indicate that the interface is connected to a router.

Precautions

After you configure this command on an interface, the interface can still switch between Layer 2 and Layer 3 modes.

Example

Specify description of the Ethernet interface GE0/0/1 to **router** to indicate that the interface is connected to a router.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port description router
```

4.1.20 reset counters if-mib interface

Function

The **reset counters if-mib interface** command clears interface traffic statistics in the Network Management System (NMS).

Format

reset counters if-mib interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Clears traffic statistics on a specified interface in the NMS. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on a specific interface within a period in the NMS, clear existing traffic statistics on this interface in the NMS.

NOTE

For details on how to view interface traffic statistics in the NMS, see the NMS documentation.

Precautions

- If no interface type and number are specified, traffic statistics of all interfaces in the NMS are cleared.
- After you run the **reset counters if-mib interface** command, traffic statistics on all interfaces in the NMS are cleared. Therefore, confirm the action before you run this command.

- Running the **reset counters if-mib interface** command does not affect the interface traffic statistics displayed by the **display interface** command. To clear the interface traffic statistics displayed by the **display interface** command, run the **reset counters interface** command.

Example

Clear traffic statistics on GE0/0/1 in the NMS.

```
<HUAWEI> reset counters if-mib interface gigabitethernet 0/0/1
```

4.1.21 reset counters interface

Function

The **reset counters interface** command clears traffic statistics about a specified interface.

Format

reset counters interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Clears traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on an interface within a certain period, run the **reset counters interface** command to clear existing traffic statistics.

Precautions

- Statistics cannot be restored after being cleared. Therefore, exercise caution before clearing the statistics.
- Traffic accounting is based on the packet statistics on an interface. The clearing of the packet statistics on an interface by using the **reset counters interface** command affects the traffic accounting result. Therefore, do not randomly clear the packet statistics on an interface in a normal application environment.
- If no interface type is specified, traffic statistics on all types of interfaces are cleared. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.
- Running the **reset counters interface** command clears the last part of the **display interface** command output. That is, statistics about received and transmitted packets on the interface are cleared.

Example

Clear traffic statistics on all interfaces.

```
<HUAWEI> reset counters interface
```

Clear traffic statistics on VLANIF10.

```
<HUAWEI> reset counters interface vlanif 10
```

4.1.22 reset counters top interface

Function

The **reset counters top interface** command clears top N interface traffic statistics reports.

Format

reset counters top interface report [*report-number*]

Parameters

Parameter	Description	Value
report-number	Specifies the number of the top N interface traffic statistics report to be deleted. If you do not specify this parameter, the command clears all top N interface traffic statistics reports.	The value is an integer ranging from 1 to 5.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The top N interface traffic statistics function allows a device to generate a maximum of five top N interface traffic statistics reports. If you want to generate new top N interface traffic statistics reports when five top N interface traffic statistics reports already exist, run the **reset counters top interface report** [*report-number*] command to clear existing ones.

Precautions

- After you run the **reset counters top interface report** *report-number* command to clear a specified top N interface traffic statistics report, the numbers of other top N interface traffic statistics reports remain unchanged.
- You can run the **reset counters top interface report** [*report-number*] command even if less than five top N interface traffic statistics reports exist.

Example

Clear all top N interface traffic statistics reports.

```
<HUAWEI> reset counters top interface report
```

Clear the top N interface traffic statistics report numbered 1.

```
<HUAWEI> reset counters top interface report 1
```

4.1.23 restart (interface view)

Function

The **restart** command restarts an interface.

Format

restart

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, Sub-interface view, Tunnel interface view, VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an interface, run the **restart** command to make the modification take effect.

Precautions

- Restarting an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **restart** command.
- Running the **restart** command is equivalent to running the **shutdown** command and the **undo shutdown** command in sequence.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Restart GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] restart
```

4.1.24 set flow-stat interval

Function

The **set flow-stat interval** command sets the interval for collecting the traffic statistics on interfaces.

The **undo set flow-stat interval** command restores the default interval for collecting traffic statistics on interfaces.

By default, the interval for collecting traffic statistics on interfaces is 300 seconds.

Format

set flow-stat interval *interval-time*

undo set flow-stat interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for collecting traffic statistics on interfaces.	The value is an integer that ranges from 10 to 600, in seconds. In addition, the value must be a multiple of 10. The default value is 300s.

Views

System view, Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By using the **set flow-stat interval** command to set the interval for collecting traffic statistics on interfaces, you can collect and analyze traffic statistics according to your needs. You can also take traffic control measures based on the traffic statistics to prevent network congestion and service interruption.

- When congestion occurs, set the interval for collecting traffic statistics on an interface to less than 300 seconds, or 30 seconds if congestion worsens. Then observe the traffic distribution on the interface within a short period of time. If data packets cause congestion, take proper measures to control the rate of the packets.
- When the network bandwidth is sufficient and services are running properly, set the interval for collecting traffic statistics on an interface to more than 300 seconds. If the value of any traffic parameter is not within the specified range, change the interval for collecting traffic statistics to observe the traffic volume in real time.

Precautions

- The interval configured in the system view takes effect on all the interfaces that use the default interval.
- The interval configured in the interface view takes effect only on the current interface.
- The interval configured in the interface view takes precedence over the interval configured in the system view.

Example

Set the interval for collecting traffic statistics on GE0/0/1 to 400s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] set flow-stat interval 400
```

4.1.25 shutdown (interface view)

Function

The **shutdown** command disables an interface.

The **undo shutdown** command enables an interface.

By default, interfaces are enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an interface, run the **shutdown** and **undo shutdown** commands to make the modification take effect.

When an interface is not connected to a cable or fiber, you can use the **shutdown** command to disable the interface to prevent exceptions caused by interference.

Precautions

- When the device supports the autocomplete function, you must enter at least the characters **shut** before the device can automatically complete the **shutdown** command.
- Disabling an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **shutdown** command.
- Some logical interfaces, such as loopback, and null interfaces, do not support the **shutdown** and **undo shutdown** commands.
- If you run the **shutdown** command in the Eth-Trunk interface view, all Eth-Trunk member interfaces are disabled.
- Running the **shutdown** and **undo shutdown** commands is equivalent to running the **restart** command.

- When an interface is configured with a sub-interface, the default interval for running the **shutdown** and **undo shutdown** commands on the main interface is 15 seconds.
- When a physical interface functions as an Eth-Trunk member interface, the default interval for running the **shutdown** and **undo shutdown** commands on this interface is 15 seconds.

Example

Shut down GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] shutdown
```

4.2 Ethernet Interface Configuration Commands

4.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

4.2.2 am isolate

Function

The **am isolate** command isolates the current interface from a specified interface unidirectionally.

The **undo am isolate** command cancels unidirectional isolation between the current interface and a specified interface. If no interface is specified, unidirectional isolation between the current interface and all the other interfaces is canceled.

By default, no unidirectional isolation is configured between the current interface and a specified interface.

Format

am isolate { *interface-type interface-number* }&<1-8>

undo am isolate [*interface-type interface-number*]&<1-8>

am isolate *interface-type interface-number1* [**to** *interface-number2*]

undo am isolate [*interface-type interface-number1* [**to** *interface-number2*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface from which the current interface is isolated unidirectionally. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of the interface from which the current interface is isolated unidirectionally. **to** specifies an interface range, indicating all the interfaces numbered between *interface-number1* and *interface-number2*.	*interface-number2* must be greater than *interface-number1*.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **am isolate** command isolates interfaces unidirectionally. For example, if interface A is isolated from interface B unidirectionally, packets sent from interface A cannot reach interface B, but packets sent from interface B can reach interface A. Unidirectional isolation needs to be configured in the following scenarios:

- When multiple hosts connect to different interfaces of a device and a host sends many broadcast packets to the other hosts, isolate the interface connected to the host from other interfaces unidirectionally. Then the other hosts do not receive packets from the host.

- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate. To isolate interfaces in different port isolation groups, configure unidirectional isolation between these interfaces.

By default, only Layer 2 packets of the current interface are isolated from a specified interface, but Layer 3 packets are not isolated. To isolate both Layer 2 and Layer 3 packets on interfaces unidirectionally, run the **port-isolate mode all** command.

Precautions

An interface can be unidirectionally isolated from another type of interface. However, an interface cannot be unidirectionally isolated from itself or from the management interface. In addition, an Eth-Trunk cannot be unidirectionally isolated from its member interfaces.

NOTE

An interface can be isolated from a maximum of 128 interfaces unidirectionally.

Example

Isolate GE0/0/1 from GE0/0/2 unidirectionally.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] am isolate gigabitethernet 0/0/2
```

4.2.3 assign port-type 100ge

Function

The **assign port-type 100ge** command sets the maximum rate of QSFP28 interfaces to 100 Gbit/s.

The **undo assign port-type 100ge** command restores the maximum rate of QSFP28 interfaces to 40 Gbit/s.

For the S6730-H24X6C (part number: 02352FSG) and S6730-H48X6C (part number: 02352FSF) with the factory version V200R013C02, the default rate of QSFP28 interfaces is 100 Gbit/s. After a version upgrade from V200R013C02 to V200R019C00 or later, the default rate of QSFP28 interfaces is still 100 Gbit/s.

For the S5732-H24S6Q, S5732-H48S6Q, S6730-H24X6C (part number: 02352FSG) and S6730-H48X6C (part number: 02352FSF) with the factory version V200R019C00 or later, the default rate of QSFP28 interfaces is 40 Gbit/s.

The S6730-H24X6C (part number: 02353GFC), S6730S-H24X6C-A, S6730-H48X6C (part number: 02353FWL) and with the factory version V200R013C02 or later, the license has been loaded by default, and the default rate of QSFP28 interfaces is 100 Gbit/s.

NOTE

This command is supported only on the following switch models:

S5732-H24S6Q, S5732-H48S6Q, S6730S-H24X6C-A, S6730-H24X6C, S6730-H48X6C

Format

assign port-type 100ge [**slot** *slot-id* | **all**]

undo assign port-type 100ge [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.
all	Indicates all slots.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For the S5732-H24S6Q, S5732-H48S6Q, S6730-H24X6C (part number: 02352FSG), S6730-H48X6C (part number: 02352FSF), to change the rate of QSFP28 interfaces, apply for and purchase a license from the equipment supplier, activate the license, and then run the **assign port-type 100ge command**. The corresponding license does not need to be activated before the **undo assign port-type 100ge** command is run.

For the S6730-H24X6C (part number: 02353GFC), S6730S-H, S6730-H48X6C (part number: 02353FWL), the license has been loaded by default. To change the rate of QSFP28 interfaces, run the **assign port-type 100ge** command. The corresponding license does not need to be activated before the **undo assign port-type 100ge** command is run.

Precautions

- The corresponding license is required before the **assign port-type 100ge** command is run, whereas no license is required before the **undo assign port-type 100ge** command is run.
- To check the current rate of an interface and the rate that takes effect after a device restart, run the **display device port-type configuration** command.
- After the command is executed, restart the device immediately for the configuration to take effect.
- After the device restarts, the original interface configuration may be lost. Therefore, back up the configuration before the restart. After the restart, check the configuration and modify it if necessary.

- After this command is executed, the maximum rate of QSFP28 interfaces is the configured rate if you restore the factory settings with one click or downgrade the software version.
- After the license expires, the maximum rate of QSFP28 interfaces is the default rate if you restart the device and then restore the factory settings with one click.

Example

Set the maximum rate of QSFP28 interfaces to 100 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] assign port-type 100ge all
Warning: The configuration of 40G interfaces may be lost after the device restart. Therefore, back up their configuration before the
 restart, and check the configuration after the restart is complete. Continue? [Y/N]:y
Info: The current configuration has been modified and takes effect after the device is restarted.
```

4.2.4 assign port-type xge

Function

The **assign port-type xge** command sets the maximum rate of 1000BASE-X interfaces to 10 Gbit/s.

The **undo assign port-type xge** command restores the maximum rate of 1000BASE-X interfaces to 1 Gbit/s.

By default, no license is loaded to a device, and 1000BASE-X interfaces support the maximum rate of 1 Gbit/s.

NOTE

This command is supported only on the following switch models:

S5736-S48S4X-A, S5736-S48S4X-D

Format

assign port-type xge [**slot** *slot-id* | **all**]

undo assign port-type xge [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be the ID of an existing slot on the device.
all	Indicates all slots.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, 1000BASE-X interfaces on a switch work at a maximum rate of 1 Gbit/s. To enable these interfaces to work at a maximum rate of 10 Gbit/s, apply for and purchase a license from the equipment supplier, activate the license, and then run the **assign port-type xge** command to set the maximum rate of 1000BASE-X interfaces to 10 Gbit/s. To restore the maximum rate of 1000BASE-X interfaces to 1 Gbit/s, run the **undo assign port-type xge** command. This command configuration takes effect only after the device is restarted.

Precautions

- A license is required for running the **assign port-type xge** command, whereas no license is required for running the **undo assign port-type xge** command.
- To check the current rate of an interface and the rate that takes effect after a device restart, run the **display device port-type configuration** command.
- After the command is executed, restart the device immediately for the configuration to take effect.
- After the device restarts, the original interface configuration may be lost. Therefore, back up the configuration before the restart. After the restart, check the configuration and modify it if necessary.
- After this command is executed, the maximum rate of SFP interfaces is the configured rate if you restore the factory settings with one click or downgrade the software version.
- After the license expires, the maximum rate of SFP interfaces is the default rate if you restore the factory settings with one click after a device restart.

Example

Set the maximum rate of 1000BASE-X interfaces to 10 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] assign port-type xge all
Warning: The configuration of GE interfaces may be lost after the device restart. Therefore, back up their
configuration before the
restart, and check the configuration after the restart is complete. Continue? [Y/
N]:y
Warning: Running this command will change ports' capability of supporting dedicated stack cables.
Continue? [Y/N]:y
Info: The current configuration has been modified and takes effect after the device is restarted.
```

4.2.5 assign port-type 25ge

Function

The **assign port-type 25ge** command sets the maximum rate of 10GE SFP+ Ethernet optical ports to 25 Gbit/s.

The **undo assign port-type 25ge** command restores the maximum rate of 10GE SFP+ Ethernet optical ports to 10 Gbit/s.

By default, no license is loaded to a device, and 10GE SFP+ Ethernet optical ports work at a maximum rate of 10 Gbit/s.

NOTE

This command is supported only on the S6730-H24X4Y4C.

Format

assign port-type 25ge [**slot** *slot-id* | **all**]

undo assign port-type 25ge [**slot** *slot-id* | **all**]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.
all	Indicates all slots.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, 10GE SFP+ Ethernet optical ports on a device work at a maximum rate of 10 Gbit/s. To enable these ports to work at a maximum rate of 25 Gbit/s, apply for and purchase a license from the equipment supplier, activate the license, and then run the **assign port-type 25ge** command to set the maximum rate of the ports to 25 Gbit/s. To restore the maximum rate of the ports to 10 Gbit/s, run the **undo assign port-type 25ge** command. This command configuration takes effect only after the device is restarted.

Precautions

- A license is required for running the **assign port-type 25ge** command, whereas no license is required for running the **undo assign port-type 25ge** command.
- To check the current rate of an interface and the rate that takes effect after a device restart, run the **display device port-type configuration** command.
- After the command is executed, restart the device immediately for the configuration to take effect.

- After the device restarts, the original interface configuration may be lost. Therefore, back up the configuration before the restart. After the restart, check the configuration and modify it if necessary.
- After this command is executed, the maximum rate of 10GE interfaces is the configured rate if you restore the factory settings with one click or downgrade the software version.
- After the license expires, the maximum rate of 10GE interfaces is the default rate if you restore the factory settings with one click after a device restart.

Example

Increase the maximum rate of all 10GE SFP+ Ethernet optical ports to 25 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] assign port-type 25ge all
Warning: The configuration of XGE interfaces may be lost after the device restart. Therefore, back up their configuration before the
restart, and check the configuration after the restart is complete. Continue? [Y/N]:y
Info: The current configuration has been modified and takes effect after the device is restarted.
```

4.2.6 assign group-speed

Function

The **assign group-speed** command sets the maximum rate of interfaces in a MultiGE interface group.

The **undo assign group-speed** command restores the default maximum rate of interfaces in a MultiGE interface group.

By default, you can run the **display device group-speed configuration** command to check the maximum rate of a MultiGE interface based on the **BaseSpeed** field in the command output.

NOTE

This command is supported only on the following switch models:

S5732-H24UM2CC, S5732-H48UM2CC, S5736-S24UM4XC

Format

assign group-speed [**slot** *slot-id*] **group** *group-number speed*

undo assign group-speed [**slot** *slot-id*] **group** *group-number*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID. In a stack, if no slot ID is specified, the maximum rate of interfaces in the MultiGE interface group on the master switch is configured.	The value must be set according to the device configuration.
group *group-number*	Specifies the number of a MultiGE interface group.	The value is an integer and must be set according to the device configuration. Every 12 MultiGE interfaces form a MultiGE interface group. The number of MultiGE interface groups determines the value range. For example, if a device has 24 MultiGE interfaces, the value is 0 or 1.
speed	Specifies the maximum rate of a MultiGE interface.	The value is of the enumerated type: ● 1000 ● 2500 ● 5000 ● 10000 The unit is Mbit/s. **NOTE** ● The value range of this parameter depends on the loaded license control item. ● The specified MultiGE interface rate cannot be lower than the default MultiGE interface rate.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the S5732-H24UM2CC, S5732-H48UM2CC, S5736-S24UM4XC, every 12 MultiGE interfaces form a MultiGE interface group. To set the maximum rate of interfaces in a specified MultiGE interface group, run the **assign group-speed** command. The maximum rates of interfaces in the same MultiGE interface group are the same, and the maximum rates of interfaces in different MultiGE interface groups can be different.

Precautions

- This command takes effect only on the device to which license control items are loaded. For details about how to use license control items, see Other: How Can I Increase the Rate of Ports Through the RTU License? in the *S1720, S5700, and S6700 Series Switches License Usage Guide*.
- After you run the **assign group-speed** command to set the maximum rate of interfaces in a MultiGE interface group, restart the switch to make the configuration take effect. If you have run the **assign group-speed** command multiple times to set the maximum rate of interfaces in multiple MultiGE interface groups, restart the switch to make these configurations take effect simultaneously.
- After the **assign group-speed** command is run, the maximum rate of interfaces in a MultiGE interface group is restored to the default value if factory settings are restored with one click.
- After the license for a MultiGE interface group expires, if the device is restarted or factory settings are restored with one click, the maximum rate of interfaces in the MultiGE interface group is restored to the default value.

Example

Set the maximum rate of interfaces in MultiGE interface group 0 to 10000 Mbit/s.

```
<HUAWEI> system-view
[HUAWEI] assign group-speed group 0 10000
```

4.2.7 auto duplex

Function

The **auto duplex** command configures the duplex mode on an Ethernet electrical interface in auto-negotiation mode.

The **undo auto duplex** command restores the default duplex mode on an Ethernet electrical interface in auto-negotiation mode.

By default, the duplex mode on an Ethernet electrical interface is negotiated with the peer interface.

NOTE

Physical interfaces of the S5732-H24S6Q, S5732-H48S6Q, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and MultiGE interface of the S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC do not support the half duplex mode and this command is not supported.

Format

auto duplex { **half** | **full** }*

undo auto duplex

Parameters

Parameter	Description	Value
half	Sets the duplex mode on an Ethernet electrical interface in auto-negotiation mode to half-duplex.	-
full	Sets the duplex mode on an Ethernet electrical interface in auto-negotiation mode to full-duplex.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their duplex mode. If the negotiated duplex mode is not the required one, you can run the **auto duplex** command to set the required duplex mode in auto-negotiation mode.

- If service traffic volume of enterprise users is high, interfaces at both ends of a link must work in full-duplex mode. Otherwise, packet loss occurs. You can run the **auto duplex full** command to set the duplex mode to full-duplex. After the auto-negotiation succeeds, the interfaces work in full-duplex mode.
- If service traffic volume of enterprise users is low, interfaces at both ends of a link can meet data transmission requirements when they work in half-duplex mode. You can run the **auto duplex half** command to set the duplex mode to half-duplex. After the auto-negotiation succeeds, the interfaces work in half-duplex mode.

Prerequisites

Run the **negotiation auto** command to configure Ethernet interface to work in auto-negotiation mode.

Precautions

- In auto-negotiation mode, an FE electrical interface negotiates the duplex mode with the peer device on the link.
- In auto-negotiation mode, a GE electrical interface that works at a rate of 1000 Mbit/s only supports the full-duplex mode. If the duplex mode is changed to half-duplex, the GE electrical interface works at a maximum rate of 100 Mbit/s.
- The GE optical interfaces support the duplex mode configuration when they are equipped with GE copper modules.
- The interfaces on both ends of a link must have the same duplex mode.

Example

Configure Ethernet electrical interface GE0/0/1 in auto-negotiation mode to work in half-duplex mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] auto duplex half
```

4.2.8 auto speed

Function

The **auto speed** command configures the auto-negotiation rate of an Ethernet electrical interface.

The **undo auto speed** command restores the default auto-negotiation rate of an Ethernet electrical interface.

By default, Ethernet electrical interfaces on both ends can negotiate to any rate they support.

Format

auto speed { **10** | **100** | **1000** | **2500** | **5000** | **10000** } *

undo auto speed

Parameters

Parameter	Description	Value
10	Sets the auto-negotiation rate of an Ethernet electrical interface to 10 Mbit/s.	-
100	Sets the auto-negotiation rate of an Ethernet electrical interface to 100 Mbit/s.	-

Parameter	Description	Value
1000	Sets the auto-negotiation rate of an Ethernet electrical interface to 1000 Mbit/s. **NOTE** FE electrical interfaces do not support this parameter.	-
2500	Sets the auto-negotiation rate of an Ethernet electrical interface to 2500 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
5000	Sets the auto-negotiation rate of an Ethernet electrical interface to 5000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
10000	Sets the auto-negotiation rate of an Ethernet electrical interface to 10000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-

Views

Ethernet interface view, GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their rate. If the negotiated rate is not the required one, run the **auto speed** command to set the auto-negotiation rate range to limit the negotiated rate.

For example, the network adapter speeds on Server1, Server2, and Server3 that form a server cluster are all 1000 Mbit/s, and the speed of the outbound interface

GE0/0/4 connecting the device to external networks is also 1000 Mbit/s. The servers connect to GE0/0/1, GE0/0/2, and GE0/0/3 respectively. If the auto-negotiation speed is not specified on the device, the speeds negotiated by GE0/0/1, GE0/0/2, and GE0/0/3 with their connected servers are all 1000 Mbit/s. When the servers send data at the speed of 1000 Mbit/s concurrently, the outbound interface GE0/0/4 will be blocked. In this case, you can run the **auto speed 100** command to configure the auto-negotiation speed to 100 Mbit/s for GE0/0/1, GE0/0/2, and GE0/0/3, preventing the outbound interface from being blocked.

Prerequisites

Run the **negotiation auto** command to configure the Ethernet interface to work in auto-negotiation mode.

Precautions

The rate of MultiGE interfaces on the S5732-H24UM2CC, S5732-H48UM2CC, and S5736-S24UM4XC can be increased using the RTU license. After the license is activated, you can run the **assign group-speed** command and restart the device to make the configured maximum rate supported by the interfaces in the MultiGE interface group take effect.

To check the default rate of MultiGE interfaces, run the **display device group-speed configuration** command. The **BaseSpeed** field indicates the default rate.

Example

Configure Ethernet electrical interface GE0/0/1 to work at a rate of 100 Mbit/s in auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] auto speed 100
```

4.2.9 cable-snr-test

Function

The **cable-snr-test** command checks the network cable quality and displays the check result.

NOTE

This command is supported only on the XGE electrical interfaces on the ES5D21X08T00 card of the S5731-H, and S5731S-H, GE electrical interfaces on the S5731-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S (except the S5735-S48S4X), S500, S5735S-S, S5735-S-I, and S5720I-SI, and MultiGE electrical interfaces on the S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5720-28X-PWH-LI-AC, S5720-28X-PWH-LI-ACF, S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S5736-S24UM4XC.

Format

cable-snr-test

Parameters

None

Views

MultiGE interface view, XGE interface view, GE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can check the quality of the network cable on an electrical interface to determine whether the network cable quality meets communication requirements.

Precautions

- This command checks real-time quality of the network cable on an interface, and the network cable quality changes with the external environment.
- A MultiGE electrical interface supports accurate network cable quality check only when it works at the rate of 2.5 Gbit/s or higher.
- An XGE electrical interface supports accurate network cable quality check only when it works at the rate of 10 Gbit/s.
- A GE electrical interface supports accurate network cable quality check only when it works at the rate of 1 Gbit/s.
- An interface does not support the network cable quality check when it is Down or in loopback detection mode.
- After the interface goes Up, wait for several minutes before running this command. Otherwise, the command fails to be delivered.

Example

Check the network cable quality on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cable-snr-test
Info: The current network cable is of good quality.
```

4.2.10 carrier

Function

The **carrier** command configures the delay in reporting an interface status change event.

The **undo carrier** command restores the default delay in reporting an interface status change event.

By default, the delay in reporting an interface Up event is 2000 milliseconds, and the delay in reporting an interface Down event is 0 milliseconds.

Format

carrier { **up-hold-time** | **down-hold-time** } *interval*

undo carrier { **up-hold-time** | **down-hold-time** }

Parameters

Parameter	Description	Value
up-hold-time *interval*	Specifies the delay in reporting an interface Up event.	The value is 0 or an integer that ranges from 50 to 120000, in milliseconds.
down-hold-time *interval*	Specifies the delay in reporting an interface Down event.	The value is 0 or an integer that ranges from 1000 to 120000, in milliseconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The physical status of an Ethernet interface can be Up or Down. When the physical status changes, the system notifies upper-layer protocol modules (such as the routing and forwarding modules) of the change to direct packet receiving and forwarding. The system also automatically generates traps and logs to remind users to perform corresponding operations on physical links. For example, when the physical status of the active interface in an interface protection group changes from Up to Down, the system immediately instructs the upper-layer service forwarding protocol to send service packets from the standby interface.

If frequent physical status changes are reported to the system, extra system costs are generated. You can configure the delay in reporting physical status changes to solve the problem. The system is unaware of the physical status changes on interfaces within the configured delay. If the interface physical status is not recovered after the delay expires, the physical status changes are reported to the system.

You can configure the delay in reporting physical status changes based on the network connection status.

- Setting a long delay

  For example, an interface frequently alternates between Up and Down states at an interval shorter than the IP route convergence time. In this case, the upper-layer protocol does not need to sense the physical status changes. You can set a long delay in reporting physical status changes to avoid unnecessary routing entry refreshing caused by frequent physical status changes.
- Setting a short delay

  For example, when the physical status of the active interface in an interface protection group changes from Up to Down, the system needs to immediately instruct the upper-layer service forwarding protocol to send service packets from the standby interface. In this case, you can set a short delay in reporting physical status changes to ensure real-time service switchover.

Precautions

If you run the **carrier** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the delay in reporting an interface Up event to 1000 milliseconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] carrier up-hold-time 1000
```

4.2.11 clear configuration port-isolate

Function

The **clear configuration port-isolate** command clears all the interface isolation configurations on the device.

By default, interface isolation configurations on the device are not cleared.

Format

clear configuration port-isolate

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To clear all the interface isolation configurations on the device, you need to delete the configurations one by one. If a large number of configurations exist on the device, deleting the configurations takes much time and increases the maintenance workload. To reduce the maintenance workload and operation complexity, run the **clear configuration port-isolate** command in the system view to clear all the interface isolation configurations on the device. The configurations involve the port isolation group, unidirectional port isolation, and isolation mode.

Example

Clear all the interface isolation configurations on the device.

```
<HUAWEI> system-view
[HUAWEI] clear configuration port-isolate
Warning: The port isolate will be cancelled. Continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...done.
```

4.2.12 combo-port

Function

The **combo-port** command configures the working mode of a combo interface.

The **undo combo-port** command restores the default setting.

By default, a combo interface works in auto mode. That is, the combo interface automatically switches between the electrical mode and optical mode.

NOTE

Only combo interfaces support this command. For details about the combo interface supported by the switch, see the Hardware Description or click **Info-Finder**.

Format

combo-port { **auto** | **copper** | **fiber** }

undo combo-port

Parameters

Parameter	Description	Value
auto	Allows a combo interface to automatically select the working mode. The combo interface checks whether an optical module has been installed: ● When a cable is not connected and an optical module is installed, the combo interface works in optical mode. ● When a cable is connected, the interface is in Up state, and an optical module is installed, the combo interface works in electrical mode. After the device restarts, the combo interface works in optical mode. ● When a cable is connected, the interface is in Down state, and an optical module is installed, the combo interface works in optical mode. In summary, when an optical module is installed on the combo optical interface, the combo interface works in optical mode after the device restarts.	-
copper	Configures a combo interface to work in electrical mode so that data is transmitted through network cables.	-

Parameter	Description	Value
fiber	Configures a combo interface to work in optical mode so that data is transmitted through optical fibers.	-

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A combo interface consists of a GE electrical interface and a GE optical interface on the panel. The multiplexed electrical and optical interfaces share one internal forwarding interface and cannot work at the same time. When one interface works, the other interface is disabled. You can use the electrical or optical interface based on the remote interface type. The electrical and optical interfaces share one interface view. When you enable the electrical or optical interface, configure the interface attributes (such as the rate and duplex mode) in the same interface view.

Precautions

This command takes effect only on combo interfaces.

If a combo interface is configured to work in a different mode from the remote interface, the two interfaces cannot communicate.

The electrical interface is used with the optical interface as a combo interface. Combo optical interface does not support GE copper module.

Example

Configure GE0/0/1 to work in electrical mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] combo-port copper
```

4.2.13 display counters protocol

Function

The **display counters protocol** command displays IPv4 and IPv6 packet statistics on an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display counters [**interface** *interface-type interface-number*] **protocol** [**rate**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number.	-
protocol	Displays IPv4 and IPv6 packet statistics.	-
rate	Displays packet rate information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After enabling IPv4 or IPv6 packet statistics collection on an interface, you can run this command to view packet statistics, facilitating fault location and troubleshooting.

Example

Display IPv4 and IPv6 packet statistics on interfaces.

```
<HUAWEI> display counters protocol
-: Statistic not enable
Inbound
Interface       IPv4(bytes)     IPv4(pkts)     IPv6(bytes)     IPv6(pkts)
GE0/0/20                0              0               0              0
GE0/0/21                -              -               0              0
Outbound
Interface       IPv4(bytes)     IPv4(pkts)     IPv6(bytes)     IPv6(pkts)
GE0/0/20                0              0               0              0
GE0/0/21                -              -               0              0
```

Display IPv4 and IPv6 packet rate information on interfaces.

```
<HUAWEI> display counters protocol rate
-: Statistic not enable
Inbound
```

```
Interface      IPv4(bytes/s)   IPv4(pkts/s)   IPv6(bytes/s)   IPv6(pkts/s)
GE0/0/20                  0              0               0              0
GE0/0/21                  -              -              0              0
Outbound
Interface      IPv4(bytes/s)   IPv4(pkts/s)   IPv6(bytes/s)   IPv6(pkts/s)
GE0/0/20                  0              0               0              0
GE0/0/21                  -              -              0              0
```

Table 4-16 Description of the **display counters protocol** command output

Item	Description
-: Statistic not enable	If a field of an interface displays **-**, traffic statistics collection about the corresponding type of packets is disabled.
Inbound	Packet statistics in the inbound direction of an interface.
Outbound	Packet statistics in the outbound direction of an interface.
Interface	Interface name.
IPv4(bytes)	Number of bytes in IPv4 packets.
IPv4(pkts)	Number of IPv4 packets.
IPv6(bytes)	Number of bytes in IPv6 packets.
IPv6(pkts)	Number of IPv6 packets.
IPv4(bytes/s)	Rate of bytes in IPv4 packets.
IPv4(pkts/s)	Rate of IPv4 packets.
IPv6(bytes/s)	Rate of bytes in IPv6 packets.
IPv6(pkts/s)	Rate of IPv6 packets.

4.2.14 display card port-config-mode configuration

Function

The **display card port-config-mode configuration** command displays information about the card interface working mode.

NOTE

The following switch models support this command when equipped with an S7X08000 card:

- S5731-H24T4XC, S5731-H24P4XC, S5731-H48T4XC, S5731-H48P4XC, S5731-H24HB4XZ, S5731-H48HB4XZ
- S5731S-H24T4XC-A, S5731S-H48T4XC-A, S5731S-H24HB4XZ-A, S5731S-H48HB4XZ-A
- S5736-S
- S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC

Format

display card port-config-mode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the card interface working mode or check whether the card interface working mode configured using the **set card port-config-mode 25g-port enable** command takes effect, run the **display card port-config-mode configuration** command.

Example

Display information about the card interface working mode.

```
<HUAWEI> display card port-config-mode configuration
-----------------------------------
 SlotId      Current       Next
-----------------------------------
 1           8*10G         8*10G
-----------------------------------
```

Table 4-17 Description of the **display card port-config-mode configuration** command output

Item	Description
SlotId	Slot ID.
Current	Current interface working mode. **NOTE** (*) indicates that the S7X08000 card is not properly installed or does not support the change of the port working mode.

Item	Description
Next	Interface working mode used at the next startup. **NOTE** (*) indicates that the S7X08000 card is not properly installed or does not support the change of the port working mode.

4.2.15 display device group-speed configuration

Function

The **display device group-speed configuration** command displays information about the rate of interfaces in MultiGE interface groups.

NOTE

This command is supported only on the following switch models:

S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S5736-S24UM4XC

Format

display device group-speed configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the following information:

- Default maximum rates of interfaces in MultiGE interface groups
- Maximum rates of interfaces in MultiGE interface groups, which are configured using the **assign group-speed** command
- Maximum rates of interfaces in MultiGE interface groups during the current device startup
- Maximum rates of interfaces in MultiGE interface groups for the next device startup

Example

Display the rates of interfaces in MultiGE interface groups.

```
<HUAWEI> display device group-speed configuration

-------------------------------------------------------------------------------
Slot Group  Interfaces          BaseSpeed ConfigSpeed CurrentSpeed
NextSpeed
-------------------------------------------------------------------------------
 0    0    MultiGE2/0/1  ~ 2/0/12   1G        10G         10G          10G
      1   MultiGE2/0/13 ~ 2/0/24   1G        -           1G           1G
```

Table 4-18 Description of the **display device group-speed configuration** command output

Item	Description
Slot	Slot ID.
Group	Number of a MultiGE interface group.
Interfaces	Interface number.
BaseSpeed	Default maximum rates of interfaces in MultiGE interface groups The unit is bit/s.
ConfigSpeed	Maximum rates of interfaces in MultiGE interface groups, which are configured using the **assign group-speed** command The unit is bit/s. **NOTE** If this field displays -, **ConfigSpeed** is the same as **BaseSpeed**.
CurrentSpeed	Maximum rates of interfaces in MultiGE interface groups during the current device startup The unit is bit/s.
NextSpeed	Maximum rates of interfaces in MultiGE interface groups for the next device startup The unit is bit/s.

4.2.16 display device port-config-mode status

Function

The **display device port-config-mode status** command displays information about the card interface working mode.

Format

display device port-config-mode status [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

For the S5731-S8UM16UN2Q, S5731S-S8UM16UN2Q-A, S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002) and S5732-H48XUM2CC, you can run the **display device port-config-mode status** command to check the interface working mode and interface split information.

Example

Display the interface working mode and interface split information on the S5732-H24UM2CC.

```
<HUAWEI&gt; display device port-config-mode status
Slot ID        Port-config-mode        Split-port              Status
----------------------------------------------------------------------
0            4*25GE+4*10GE+40GE      XGigabitEthernet0/0/1
enable
                                XGigabitEthernet0/0/2
                                XGigabitEthernet0/0/3
                                XGigabitEthernet0/0/4
----------------------------------------------------------------------
```

Table 4-19 Description of the **display device port-config-mode status** command output

Item	Description
Slot ID	Slot ID.
Port-config-mode	The interface working mode is 4x25GE+4x10GE+40GE mode.
Split-port	If an interface is not split, this field displays -. If an interface is split, this field displays the converted interfaces.
Status	Current status of interface split: ● enable: Interface split is enabled. ● disable: Interface split is disabled.

4.2.17 display device port-type configuration

Function

The **display device port-type configuration** command displays the maximum rate of interfaces on the device.

NOTE

This command is supported only on the following switch models:

S5732-H24S6Q, S5732-H48S6Q, S6730S-H24X6C-A, S6730-H24X6C, S6730-H48X6C, S6730-H24X4Y4C, S5736-S48S4X-A, and S5736-S48S4X-D

Format

display device port-type configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On the S5732-H24S6Q, S5732-H48S6Q, S6730S-H24X6C-A, S6730-H24X6C, S6730-H48X6C, after the maximum rate of QSFP28 interfaces is changed using the **assign port-type 100GE** command, you can run the **display device port-type configuration** command to check the supported maximum rate configuration.

On the S6730-H24X4Y4C, after the maximum rate of a 10GE SFP+ Ethernet optical interface is set to 25 Gbit/s using the **assign port-type 25GE** command, you can run the **display device port-type configuration** command to check the maximum rate configuration.

On the S5736-S48S4X-A, S5736-S48S4X-D, after the maximum rate of 1000BASE-X interfaces is set to 10 Gbit/s using the **assign port-type XGE** command, you can run the **display device port-type configuration** command to check the supported maximum rate configuration.

Precautions

The corresponding license does not need to be activated before this command is run.

Example

Display the maximum rate of 40GE interfaces on a switch.

```
<HUAWEI> display device port-type configuration
-----------------------------------
 SlotId       Current       Next
-----------------------------------
 0           40GE         100GE
 1           40GE         100GE
-----------------------------------
```

Table 4-20 Description of the **display device port-type configuration** command output

Item	Description
Slot	Slot ID.
Current	Current maximum rate of 40GE interfaces.
Next	Configured maximum rate supported by the device. **NOTE** If a switch does not restart after the maximum rate of 40GE interfaces is changed, the **Next** field value will be inconsistent with the **Current** field value.

4.2.18 display error-down recovery

Function

The **display error-down recovery** command displays information about the port in Error-Down state, including the interface name, cause of the Error-Down event, delay for the interface to change from Down to Up, and remaining time for the Up event.

NOTE

An interface enters the error-down state after being shut down due to an error. Currently, errors include the auto-defend protection, threshold crossing event, remote failure event, MAC address flapping, link flapping, low optical power, error packets exceeding the alarm threshold, and BPDU protection.

Format

display error-down recovery [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the specified port in Error-Down state. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The auto recovery function is configured and the delay for an interface to change from Down to Up is set using the **error-down auto-recovery** command. If the interface is in the Error-Down state, you can run the **display error-down recovery** command to view the remaining time for the Up event.

Prerequisites

The auto recovery function has been configured on an interface using the **error-down auto-recovery** command.

Precautions

If **interface** is not specified in this command, the system displays information about all interfaces in error-down state.

Example

Display the delay for the interface to change from Down to Up and the remaining time for the Up event.

```
<HUAWEI> display error-down recovery
interface              error-down cause          recovery   remainder
                                                 time(sec)  time(sec)
----------------------------------------------------------------------------
GigabitEthernet0/0/1   bpdu-protection           30         10
```

Table 4-21 Description of the **display error-down recovery** command output

Item	Description
interface	Interface name.
error-down cause	Cause of the Error-Down event, including: ● as-not-ready: An AS is not in service. ● auto-defend ● efm-threshold-event ● efm-remote-failure ● bpdu-protection ● data-integrity-error ● error-statistics ● storm-control ● port-security ● mac-address-flapping ● transceiver-power-low ● link-flap
recovery time(sec)	Delay for the interface to change from Down to Up, in seconds. If no automatic recovery time is configured, you need to run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to make the interface go Up and the recovery time is displayed as **--**.
remainder time(sec)	Remaining time for the Up event, in seconds. If no automatic recovery time is configured, you need to run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to make the interface go Up and the remaining time is displayed as **--**.

4.2.19 display error-statistics trigger speed-down-grade oui

Function

The **display error-statistics trigger speed-down-grade oui** command displays the terminal MAC addresses that can be identified in automatic rate reduction on interfaces.

NOTE

This command is supported only on the following switch models: S5731-S, S5731S-S, S5731-H, S5731S-H.

Format

display error-statistics trigger speed-down-grade oui

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a GE electrical interface on a device is connected to a specific printer and the interface rate is higher than 10 Mbit/s, the interface can go Up, but the printer cannot work properly. Alignment error packets will be detected on the interface. In this case, you can run the **set error-statistics trigger speed-down-grade** command to enable the device to automatically reduce the interface rate when the number of error packets on the interface reaches the threshold. The device then automatically sets the interface rate to 10 Mbit/s, reports an alarm (hwPortErrPktSpeedDownGrade), and records a log (IFPDT/1/ERRPKT_SPEEDDOWN) when the following conditions are met:

- The interface receives three alignment error packets within 60 seconds.
- The interface is in the auto-negotiation state and works at the rate of 100 Mbit/s.
- Only one MAC address is learned on the interface, and the MAC address starts with 001B-82 or is in the MAC address blacklist configured using this command.

You can run this command to view the terminal MAC addresses that can be identified by the device in addition to the default MAC address.

Example

Display the terminal MAC addresses that can be identified in automatic rate reduction on interfaces.

```
<HUAWEI> display error-statistics trigger speed-down-grade oui
--------------------------------------------------
OuiAddress      Mask            Description
--------------------------------------------------
0001-0000-0000  ffff-0000-0000  printer
```

Table 4-22 Description of the **display error-statistics trigger speed-down-grade oui** command output

Item	Description
OuiAddress	MAC OUI. To set this parameter, run the **error-statistics trigger speed-down-grade** command.
Mask	Mask of the MAC address.
Description	Description of the MAC address.

4.2.20 display interface ethernet brief

Function

The **display interface ethernet brief** command displays brief information about Ethernet interfaces.

Format

display interface ethernet brief [**main**]

Parameters

Parameter	Description	Value
main	Displays brief information about Ethernet main interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display interface ethernet brief** command to view brief information about Ethernet interfaces, including the physical status, auto-negotiation mode, duplex mode, rate, and average inbound and outbound bandwidth usages within the last period of time. This information helps you locate and rectify faults.

Precautions

To clear statistics on an interface, run the **reset counters interface** command.

Example

Display brief information about Ethernet interfaces.

```
<HUAWEI> display interface ethernet brief
PHY: Physical
*down: administratively down
#down: LBDT down
(l): loopback
(b): BFD down
InUti/OutUti: input utility/output utility
Interface                   PHY   Auto-Neg Duplex Bandwidth  InUti OutUti Trunk
GigabitEthernet0/0/1        up    enable   half        100M  0.06%   100%    --
GigabitEthernet0/0/2        up    enable   full       1000M   100%   100%    --
GigabitEthernet0/0/3        up    enable   full       1000M     0%   100%    --
GigabitEthernet0/0/4        up    enable   full       1000M   100%   100%     1
GigabitEthernet0/0/5        up    enable   full       1000M    99%   100%    --
GigabitEthernet0/0/6        down  enable   half       1000M     0%     0%    --
GigabitEthernet0/0/7        down  enable   half       1000M     0%     0%    --
GigabitEthernet0/0/8        down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/9        down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/10       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/11       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/12       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/13       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/14       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/15       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/16       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/17       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/18       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/19       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/20       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/21       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/22       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/23       down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/24       down  enable   full       1000M     0%     0%    --
MEth0/0/1                   down  enable   half        100M     0%     0%    --
```

Table 4-23 Description of the **display interface ethernet brief** command output

Item	Description
Interface	Type and number of an interface. All interfaces are displayed in alphabetical order. Information about the following interfaces can be displayed: ● MEth0/0/1 interface ● FE interface ● GE interface ● XGE interface ● 25GE interface ● MultiGE interface ● 40GE interface ● 100GE interface

Item	Description
PHY	Physical status of an interface: ● up: indicates that the interface works properly. ● down: indicates that the physical layer of the interface fails. ● *down: refers to administratively down, indicating that the administrator has run the **shutdown (interface view)** command on the interface. ● #down: LBDT down, indicating that loop detection is enabled on the interface. The interface is shut down when the device detects a loop on the downstream network or between interfaces. ● (l): refers to loopback, indicating that the loopback function is enabled on the interface. ● (b): indicates that the physical layer of the interface is in BFD down state.
Auto-Neg	Whether auto-negotiation is enabled on an interface: ● enable: indicates that auto-negotiation is enabled on the interface. ● disable: indicates that auto-negotiation is disabled on the interface. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command.
Duplex	Duplex mode of an interface: ● full: indicates the full-duplex mode. ● half: indicates the half-duplex mode. ● In auto-negotiation mode, use the **auto duplex** command to configure the duplex mode of an interface. ● In non-auto negotiation mode, use the **duplex** command to configure the duplex mode of an interface.
Bandwidth	Bandwidth on the interface.
InUti	Average inbound bandwidth usage within the last 5 minutes. Average inbound bandwidth usage = Average inbound rate within the last 5 minutes/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the interface bandwidth becomes smaller, for example, the bandwidth is changed using the **speed** command, or when an Eth-Trunk member interface becomes Down or is removed from the Eth-Trunk, the bandwidth usage be displayed as 100% because the communication traffic is not adjusted in time.

Item	Description
OutUti	Average outbound bandwidth usage within the last 5 minutes. Average outbound bandwidth usage = Average outbound rate within the last 5 minutes/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and greater than 0.005%, the value 0.01% is displayed. When the average bandwidth usage is smaller than 0.005% and greater than 0, the value 0 is displayed. When the interface bandwidth becomes smaller, for example, the bandwidth is changed using the **speed** command, or when an Eth-Trunk member interface becomes Down or is removed from the Eth-Trunk, the bandwidth usage be displayed as 100% because the communication traffic is not adjusted in time.
Trunk	Number of the Eth-Trunk to which an interface is added.

4.2.21 display port-group

Function

The **display port-group** command displays information about permanent port groups and interfaces in these groups.

Format

display port-group [**all** | *port-group-name*]

Parameters

Parameter	Description	Value
all	Displays information about all permanent port groups and interfaces in these groups.	-
port-group-name	Displays information about a specified permanent port group and interfaces in the group.	The value is the name of an existing port group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When using the **display port-group** command, note that:

- If no parameter is configured, names of all permanent port groups are displayed.
- If **all** is configured, information about all permanent port groups and interfaces in these groups is displayed.
- If *port-group-name* is configured, information about a specified permanent port group and interfaces in the group is displayed.

Example

Display information about all port groups and interfaces in these groups.

```
<HUAWEI> display port-group all
Portgroup: 1
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
```

Table 4-24 Description of the **display port-group** command output

Item	Description
Portgroup	Name of a permanent port group.

4.2.22 display port-group member-configuration

Function

The **display port-group member-configuration** command displays the configuration of each member interface in a specified interface group.

Format

display port-group *port-group-name* **member-configuration**

Parameters

Parameter	Description	Value
port-group-name	Specifies the name of an interface group to be queried.	The value is the name of an existing port group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the configuration of each member interface in a specified interface group, run the **display port-group member-configuration** command.

Example

Display the configuration of each member interface in an interface group named group1.

```
<HUAWEI> display port-group group1 member-configuration
Portgroup: group1
#
interface GigabitEthernet0/0/1
 description group1
 shutdown
 stp disable
#
interface GigabitEthernet0/0/2
 description group1
 shutdown
 stp disable
#
```

Table 4-25 Description of the **display port-group member-configuration** command output

Item	Description
Portgroup	Name of a permanent port group.

4.2.23 display port-isolate group

Function

The **display port-isolate group** command displays the configuration of a port isolation group.

Format

display port-isolate group { *group-id* | **all** }

Parameters

Parameter	Description	Value
group-id	Displays the configuration of a specified port isolation group.	The value is an integer that ranges from 1 to 64.

Parameter	Description	Value
all	Displays the configurations of all port isolation groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The port isolation feature isolates interfaces in a VLAN. Run **port-isolate enable** [**group** *group-id*] command to add interfaces to a port isolation group, you can implement Layer 2 isolation between these interfaces. To view the configuration of the port isolation group, run the **display port-isolate group** command.

Example

Display the configurations of all port isolation groups.

```
<HUAWEI> display port-isolate group all
  The ports in isolate group 3:
GigabitEthernet0/0/1
GigabitEthernet0/0/2
  The ports in isolate group 4:
GigabitEthernet0/0/3
GigabitEthernet0/0/4
```

4.2.24 display port link-flap auto-detect recovery

Function

The **display port link-flap auto-detect recovery** command displays information about interfaces that go Down due to link flapping.

Format

display port link-flap auto-detect recovery

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the physical status of an interface is **LINK-FLAP DOWN** in the **display interface** command output, you can run the **display port link-flap auto-detect recovery** command to view the automatic recovery period of the interface.

Example

Display information about interfaces that go Down due to link flapping.

```
<HUAWEI> display port link-flap auto-detect recovery
--------------------------------------------------------------------------
Interface               RecoveryTime(sec)        RemainTime(sec)
--------------------------------------------------------------------------
XGigabitEthernet0/0/1     60                       40
```

Table 4-26 Description of the **display port link-flap auto-detect recovery** command output

Item	Description
Interface	Interface name.
RecoveryTime(sec)	Automatic recovery period after an interface goes Down due to link flapping. To set the automatic recovery period, run the **port link-flap auto-detect recovery interval** command.
RemainTime(sec)	Remaining automatic recovery period after an interface goes Down due to link flapping.

4.2.25 display port protect-group

Function

The **display port protect-group** command displays information about member interfaces in an interface protection group.

Format

display port protect-group { **all** | *protect-group-index* }

Parameters

Parameter	Description	Value
all	Displays information about all interface protection groups and their member interfaces.	-
protect-group-index	Displays information about member interfaces in the specified interface protection group.	The value is an integer that ranges from 0 to 63.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Hosts are usually connected to an external network through a default gateway. If the outbound interface of the default gateway fails, the hosts cannot communicate with the external network, interrupting normal service transmission and degrading device reliability. The port protection function solves this problem. Without changing the networking, you can add two interfaces on the device to a port protection group to implement interface backup in active/standby mode. When the active interface fails, services are immediately switched to the standby interface, ensuring non-stop service transmission.

The **display port protect-group** command displays information about member interfaces in an interface protection group.

Example

Display information about interface protection group 1 and its member interfaces.

```
<HUAWEI> display port protect-group 1
  Group ID : 1
----------------------------------------------
  Protect-group member        Role      State
----------------------------------------------
  GigabitEthernet0/0/1        Master    Work
  GigabitEthernet0/0/2        Standby   Protect
```

Table 4-27 Description of the display port protect-group command output

Item	Description
Group ID	ID of the interface protection group.

Item	Description
Protect-group member	Member name of the interface protection group.
Role	Interface role: ● Master: working interface ● Standby: protected interface
State	Interface status: ● Work: working state ● Protect: protection state ● Down: the interface is physically down

4.2.26 display port split

Function

The **display port split** command displays the current status of a split or merged interface.

NOTE

Only interfaces on the panel of the S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A support interface split and merge.

For the devices that have the S7C02000 or S7Q02001 card installed, interfaces on the card support interface split and merge.

Format

display port split [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is an integer and must be set according to the device configuration.

Views

User view, system view

Default Level

1: Monitoring level

Usage Guidelines

After interfaces are split, you can run this command to view the current status of the split and merged interface.

Example

Display the current status of a split or merged interface.

```
<HUAWEI> display port split
*enable  : Will be enabled after board reset
*disable : Will be disabled after board reset

 Port           Status     Split Port
----------------------------------------------------
 40GE0/0/1      enable     XGigabitEthernet0/0/49
                           XGigabitEthernet0/0/50
                           XGigabitEthernet0/0/51
                           XGigabitEthernet0/0/52
 40GE0/0/2      enable     XGigabitEthernet0/0/53
                           XGigabitEthernet0/0/54
                           XGigabitEthernet0/0/55
                           XGigabitEthernet0/0/56
 40GE0/1/1      disable    -
 40GE0/1/2      enable     XGigabitEthernet0/1/5
                           XGigabitEthernet0/1/6
                           XGigabitEthernet0/1/7
                           XGigabitEthernet0/1/8
 40GE0/1/3      disable    -
 40GE0/1/4      disable    -
```

Table 4-28 Description of the display port split command output

Item	Description
Port	Port that can be split or merged.
Status	Current status of a split or merged interface: ● enable: Interface split is enabled. ● disable: Interface split is disabled. ● *enable: Interface split is enabled after the device is reset. ● *disable: Interface merge is enabled after the device is reset.
Split Port	Interfaces that have been split. If an interface is not split, this field displays as **-**. If an interface is split, converted interfaces are displayed.

4.2.27 display virtual-cable-test

Function

The **display virtual-cable-test** command displays the last cable test result on an Ethernet electrical interface.

NOTE

The service interfaces on the following devices do not support this command:

- MultiGE interfaces on the S5720-28X-PWH-LI-AC and S5736-S24UM4XC
- XGE electrical interfaces on the ES5D21X08T00 card

Format

display virtual-cable-test *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays cable test results on a specified interface. This parameter can be configured after a GE optical interface has a GE copper module installed. This parameter can be configured after an XGE optical interface has a GE copper module installed. After a 25GE optical interface is configured to work at the rate of 1 Gbit/s using the **port mode ge** command and has a GE copper module installed, the **virtual-cable-test** command can be configured on the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A cable test detects faults on the cable connected to an interface. If the cable is working properly, the test result displays the total length of the cable. If the cable cannot work properly, the test result displays the distance between the interface and the failure point.

NOTE

The test result is only for reference and may be inaccurate for cables of some vendors.

Example

Display the cable test result on Ethernet electrical interface GE0/0/1.

```
<HUAWEI> display virtual-cable-test gigabitethernet 0/0/1
VCT test last ran on: 2013-7-12 21:25:13
Pair A length: 189meter(s)
Pair B length: 189meter(s)
Pair C length: 189meter(s)
Pair D length: 189meter(s)
Pair A state: Ok
Pair B state: Ok
Pair C state: Ok
Pair D state: Ok
Info: The test result is only for reference.
```

Table 4-29 Description of the **display virtual-cable-test** command output

Item	Description
VCT test last ran on	Time when the last VCT test was performed on an interface. **NOTE** - When the daylight saving time (DST) is not used, the system displays the following information: VCT test last ran on: 2013-7-12 21:25:13. - When the DST is used, the system displays the following information: VCT test last ran on: 2013-7-12 21:25:13 DST.

Item	Description
Pair A length	Length of a network cable. ● The length is the distance between the interface and the faulty point if a fault occurs. ● The length is the actual length of the cable when the cable works properly. ● The length is the default length 0 m if the interface is not connected to any network cable. The test result of different chips may vary, and the displayed result is for reference only. **NOTE** If the cable length is displayed as Unknown, the cable status is OK, but the cable length test result cannot be used.
Pair A state	Status of a circuit pair of the cable: ● Ok: indicates that the circuit pair is terminated normally. ● Open: indicates that the circuit pair is not terminated. ● Short: indicates that the circuit pair is short-circuited. ● Crosstalk: indicates that the circuit pairs interfere with each other. ● Unknown: indicates that the circuit pair has an unknown fault.

NOTE

Pairs A, B, C, and D are the four pairs in a cable.

4.2.28 device transceiver 1000BASE-X

Function

The **device transceiver 1000BASE-X** command pre-configures the module to be installed as a GE optical module.

The **undo device transceiver 1000BASE-X** command cancels the pre-configuration.

By default, modules to be installed are not pre-configured as GE optical modules.

NOTE

Only XGE interfaces support this command.

Format

device transceiver 1000BASE-X

undo device transceiver 1000BASE-X

Parameters

None

Views

XGE interface

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of switches need to be deployed on the live network, a tool is used to deliver unified configurations in a batch, including the **undo negotiation auto** command configuration on interfaces. Currently, XGE interfaces on Huawei switches do not support the **undo negotiation auto** command when no optical module is installed. As a result, the deployment workload increases.

When no optical module is installed into an XGE interface, you can run the **device transceiver 1000BASE-X** and **undo negotiation auto** commands in sequence on the XGE interface, and then install a GE optical module into the XGE interface. Then the non-auto-negotiation configuration takes effect.

Prerequisites

This command can be delivered when no optical module is installed into the XGE interface or a GE optical module is installed into the XGE interface.

Follow-up Procedure

After this command is delivered, the **undo negotiation auto** command configuration can be delivered when no GE optical module is installed into the XGE interface.

Precautions

None

Example

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet0/0/1
[HUAWEI-XGigabitEthernet0/0/1] device transceiver 1000base-x
[HUAWEI-XGigabitEthernet0/0/1] undo negotiation auto
```

4.2.29 duplex

Function

The **duplex** command sets the duplex mode for an Ethernet electrical interface in non-auto-negotiation mode.

The **undo duplex** command restores the default duplex mode for an Ethernet electrical interface in non-auto-negotiation mode.

By default, the duplex mode of an Ethernet electrical interface is full duplex when the interface works in non-auto-negotiation mode.

NOTE

Physical interfaces of the S5732-H24S6Q, S5732-H48S6Q, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and MultiGE interface of the S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC do not support the half duplex mode and this command is not supported.

Format

duplex { **full** | **half** }

undo duplex

Parameters

Parameter	Description	Value
full	Sets the duplex mode to full duplex for an Ethernet electrical interface in non-auto-negotiation mode.	-
half	Sets the duplex mode to half duplex for an Ethernet electrical interface in non-auto-negotiation mode.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Interfaces can work in the following two duplex modes:

- Half-duplex mode: An interface in this mode only receives or sends data at a time within a specified transmission distance.
- Full-duplex mode: An interface in this mode receives and sends data at the same time. The maximum throughput in full-duplex mode is double that in half-duplex mode, and the transmission distance is not limited.

If the peer device does not support auto-negotiation, you can run this command to manually set the duplex mode for the local interface in non-auto-negotiation mode to ensure that the interface works in the same duplex mode as the peer interface.

Prerequisites

The Ethernet interface has been set to work in non-auto-negotiation mode by running the **undo negotiation auto** command.

Precautions

- When the working rate of a GE electrical interface is 1000 Mbit/s, the interface supports only the full duplex mode and does not need to negotiate the duplex mode with the peer interface.
- When an interface works in half-duplex mode, flow control does not take effect on the interface.
- Interfaces on both ends of a link must have the same duplex mode.

Example

Set the duplex mode to half duplex for Ethernet electrical interface GE0/0/1 in non-auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo negotiation auto
[HUAWEI-GigabitEthernet0/0/1] speed 100
[HUAWEI-GigabitEthernet0/0/1] duplex half
```

4.2.30 error-down auto-recovery

Function

The **error-down auto-recovery** command enables an interface in Error-Down state to go Up and sets the auto recovery delay.

The **undo error-down auto-recovery** command disables an interface in Error-Down state from going Up automatically.

By default, an interface in Error-Down state is not enabled to go Up.

NOTE

An interface enters the Error-Down state after being shut down due to an error. Currently, errors include the auto-defend protection, threshold crossing event, remote failure event, MAC address flapping, link flapping, low optical power, error packets exceeding the alarm threshold, and BPDU protection.

Format

error-down auto-recovery cause { **as-not-ready** | **auto-defend** | **bpdu-protection** | **efm-remote-failure** | **efm-threshold-event** | **error-statistics** | **link-flap** | **mac-address-flapping** | **remote-unit-link** | **remote-unit-misconfig** | **port-security** | **transceiver-power-low** | **storm-control** | **data-integrity-error** } **interval** *interval-value*

undo error-down auto-recovery cause { **auto-defend** | **bpdu-protection** | **efm-remote-failure** | **efm-threshold-event** | **error-statistics** | **link-flap** | **mac-address-flapping** | **remote-unit-link** | **remote-unit-misconfig** | **port-security** | **transceiver-power-low** | **storm-control** | **data-integrity-error** }

Parameters

Parameter	Description	Value
cause	Indicates the cause for an interface in Error-Down state.	-
as-not-ready	Indicates that the AS where the interface resides is not in service.	-
auto-defend	Indicates that the auto-defend function is enabled.	-
bpdu-protection	Indicates that STP BPDU protection is enabled.	-
efm-remote-failure	Indicates that an EFM remote failure event occurs.	-
efm-threshold-event	Indicates that a threshold crossing event occurs.	-
error-statistics	Indicates that the number of error packets exceeds the alarm threshold.	-
link-flap	Indicates that link flapping occurs.	-
storm-control	Indicates that storm control is enabled.	-

Parameter	Description	Value
port-security	Indicates that the number of learned secure MAC addresses exceeds the upper limit or static MAC address flapping is detected.	-
remote-unit-link	Indicates that the link between the RU and central switch is not operational.	-
remote-unit-misconfig	Indicates that the configurations of the RU and central switch are incorrect.	-
mac-address-flapping	Indicates that MAC address flapping occurs.	-
transceiver-power-low	Indicates that the optical power is too low.	-
data-integrity-error	Indicates that the chip memory identifier has a data integrity error. **NOTE** Only the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter.	-
interval *interval-value*	Specifies the auto recovery delay.	The value is an integer that ranges from 30 to 86400, in seconds. ● A smaller value indicates a higher frequency at which an interface alternates between Up and Down states. ● A larger value indicates longer traffic interruption.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an interface can only be resumed by a network administrator after being shut down. To configure the interface to restore to the Up state automatically, run the **error-down auto-recovery** command to set an auto recovery delay. After the delay, the interface goes Up automatically. Alternatively, you can run the **shutdown** and **undo shutdown** commands on the interface in the Error-Down state to restore it to the Up state.

The restored interface is shut down again if the interface receives BPDUs again or the link is considered unavailable in a specified time.

An interface enters the Error-Down state in the following scenarios.

Cause for an Interface in Error-Down State	Scenario	Remarks
as-not-ready	When the device negotiates to the AS mode, its port status becomes Down and then becomes Up after services in the service profiles have been delivered.	-
auto-defend	After the **auto-defend action** command is used to configure actions against attack sources, the interface that receives attack packets is shut down to prevent the device from attacks.	-
bpdu-protection	On an STP-enabled network where BPDU protection is configured on an edge port, if malicious attackers send bogus BPDUs to attack the switching device, the switching device sets the edge port to Down immediately after the edge port receives BPDUs. As a result, all services on the edge port are interrupted.	For details, see **stp bpdu-protection**.

Cause for an Interface in Error-Down State	Scenario	Remarks
efm-remote-failure	The **efm trigger error-down** command associates an error event with an interface. When EFM detects **critical-event**, **dying-gasp**, **link-fault**, or **timeout** faults, the protocol status of the interface becomes Down and all services on the interface are interrupted.	-
efm-threshold-event	When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. You can associate an EFM crossing event with an interface. Then the system sets the administrative status of the interface to Down. In this manner, all services on the interface are interrupted.	-
error-statistics	When an Ethernet interface configured with a backup link receives error packets, faults such as packet loss occur. To ensure nonstop service transmission, when the number of received error packets reaches the alarm threshold, the interface is shut down and services are switched to the backup link.	For details, see **trap-threshold error-statistics** and **error-statistics threshold-event trigger error-down**.

Cause for an Interface in Error-Down State	Scenario	Remarks
link-flap	Network cable faults or active/standby switchovers may cause an interface to alternate between Up and Down. You can configure link flapping protection. When the device receives an interface Up/Down message, it checks the interface flapping count and link flapping detection interval. If the interface flapping count reaches the limit within the specified period, the device shuts down interface.	For details, see **port link-flap protection enable**.
storm-control	After the storm control action is configured as error-down on an interface, the interface is shut down when the average rate of receiving broadcast, multicast, and unknown unicast packets is larger than the specified limit within the interval for detecting storms.	For details, see **storm-control action**.
port-security	After port security is enabled on an interface, MAC addresses learned by the interface change to secure dynamic MAC addresses. If the **port-security protect-action** command sets the security protection action to **shutdown**, the interface is shut down when the number of learned MAC addresses on the interface exceeds the upper limit or static MAC address flapping is detected.	For details, see **port-security protect-action** and **port-security enable**.

Cause for an Interface in Error-Down State	Scenario	Remarks
remote-unit-link	The following link faults may occur when an RU is connected to the central switch: ● A unidirectional fault occurs on the link connecting the central switch to the RU. In this case, the interface on the central switch goes Error-Down. This fault occurs if one of the following conditions is met: – The central switch does not receive heartbeat packets from the RU for three consecutive periods (30s in total). – The heartbeat packets sent by the RU do not carry central switch information in three consecutive periods (30s in total). ● When the central switch is connected to the RU through two links and the interface of one link goes Error-Down due to a unidirectional link fault, the interface of the other link does not enter the Error-Down state even if this link fails.	-

Cause for an Interface in Error-Down State	Scenario	Remarks
remote-unit-misconfig	An interface connecting the central switch to an RU goes Error-Down if one of the following configuration errors occurs: ● The two downlink interfaces on the central switch connected to the same RU are not added to an Eth-Trunk. In this case, the interface connected later goes Error-Down. ● The two downlink interfaces on the central switch connected to the same RU are added to two Eth-Trunks respectively. In this case, the interface connected later goes Error-Down. ● Two central switches are connected to the same RU, and the two central switches do not set up a stack. In this case, the interface with a larger system MAC address on the central switches goes Error-Down.	If member interfaces of an Eth-Trunk on a central switch connect to two or more RUs, the interfaces will not enter the Error-Down state if configurations are incorrect and the alarm hwRuMngPortRuFull is generated.

Cause for an Interface in Error-Down State	Scenario	Remarks
mac-address-flapping	If the user network where the device is deployed does not support loop prevention protocols, configure a loop prevention action for the device to perform when the device detects MAC address flapping. The device shuts down an interface when detecting MAC address flapping on the interface.	For details, see **mac-address flapping detection** and **mac-address flapping action**.
transceiver-power-low	When the optical power of an Ethernet optical interface configured with a backup link is reduced, faults such as packet loss occur. When the optical power is lower than the lower alarm threshold, the interface is triggered to be in Error-Down state and services are switched immediately.	For details, see **transceiver power low trigger error-down**.
data-integrity-error	After the switch runs for a long time, the chip memory identifier has a data integrity error.	-

Precautions

- The **error-down auto-recovery** command is invalid for the interface that has been in Error-Down state. It takes effect for only the interface that enters the Error-Down state after the **error-down auto-recovery** command is executed.
- BPDU protection has been enabled using the **stp bpdu-protection** command in the system view.
- A threshold crossing event has been associated with an interface using the **efm threshold-event trigger error-down** command in the interface view.
- An error event has been associated with an interface using the **efm trigger error-down** command in the interface view.

Example

Set the delay for an interface changes from Down to Up to 50s after the edge port is enabled with BPDU protection on an STP-enabled network.

```
<HUAWEI> system-view
[HUAWEI] error-down auto-recovery cause bpdu-protection interval 50
```

Set the auto recovery delay to 50s after an EFM threshold crossing event is associated with an interface.

```
<HUAWEI> system-view
[HUAWEI] error-down auto-recovery cause efm-threshold-event interval 50
```

Set the auto recovery delay to 50s after an EFM remote failure event is associated with an interface.

```
<HUAWEI> system-view
[HUAWEI] error-down auto-recovery cause efm-remote-failure interval 50
```

4.2.31 error-down-threshold error-percentage

Function

The **error-down-threshold error-percentage** command configures the alarm threshold for received CRC packets causing an interface status to change to Error-Down against all the received packets on the interface and alarm interval.

The **undo error-down-threshold error-percentage** command deletes the configured alarm threshold and interval.

By default, the alarm threshold and interval are not configured.

Format

error-down-threshold error-percentage *threshold-value* **interval** *interval-value*

undo error-down-threshold error-percentage [*threshold-value* **interval** *interval-value*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for the percentage of received CRC packets causing an interface status change to Error-Down against all the received packets on the interface.	The value is an integer that ranges from 1 to 50. **NOTE** You are advised to set the threshold to be greater than or equal to the alarm threshold configured in the **trap-threshold error-percentage** command.
interval *interval-value*	Specifies the interval for calculating the percentage of received CRC packets causing an interface status to change to Error-Down against all the received packets on the interface.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **error-statistics threshold-event trigger error-down** command is run and the number of error packets that the interface receives within a specified period exceeds the threshold, the interface status is triggered to change to Error-Down. By default, if an interface receives three CRC packets within 10 seconds, the interface status is triggered to change to Error-Down. When you want to use the percentage of received CRC packets against all the received packets as the threshold for triggering an interface status to change to Error-Down, run the **error-down-threshold error-percentage** command.

Precautions

- This command is mutually exclusive to the **error-down-threshold error-statistics** command. After this command is configured, the **error-down-threshold error-statistics** command configuration does not take effect.
- This command cannot be configured on stack interfaces.

Example

Set the alarm threshold for the percentage of received CRC packets causing the interface status to change to Error-Down against all the received packets to 10% and the interval for calculating the percentage of received CRC packets against all the received packets to 30 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] error-down-threshold error-percentage 10 interval 30
```

4.2.32 error-down-threshold error-statistics

Function

The **error-down-threshold error-statistics** command configures the alarm threshold for CRC error packets causing an interface status to change to Error-Down and interval for receiving CRC error packets.

The **undo error-down-threshold error-statistics** command restores the default value of the alarm threshold and the alarm interval for CRC error packets that cause the interface status to change to Error-Down.

By default, the alarm threshold for CRC error packets is 3 and the alarm interval is 10 seconds.

Format

error-down-threshold error-statistics *threshold-value* **interval** *interval-value*

undo error-down-threshold error-statistics

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for error packets that cause the interface status to change to Error-Down.	The value is an integer that ranges from 1 to 65535. **NOTE** The threshold is greater than or equal to the alarm threshold for error packets configured by the **trap-threshold error-statistics** command.
interval *interval-value*	Specifies the alarm interval for error packets that cause the interface status to change to Error-Down.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface is configured to transit to the Error-Down state when the number of received CRC error packets exceeds the threshold using the **error-statistics threshold-event trigger error-down** command, the interface transits to the Error-Down state when the number of received error packets exceeds the threshold within the specified interval. By default, an interface transits to the Error-Down state when the number of received error packets exceeds 3 within 10 seconds. Run the **error-down-threshold error-statistics** command to configure the interval and the threshold for received error packets.

Precautions

This command is not supported on the stack interface.

On a switch running a version earlier than V200R009C00, if the alarm threshold has been set to *n* and alarm interval to *m* seconds using the **trap-threshold error-statistics** *threshold-value* **interval** *interval-value* command, the **error-down-threshold error-statistics** *n* **interval** *m* configuration is automatically generated after the system software version is upgraded to V200R009C00 or a later version.

On a switch running a version earlier than V200R009C00, if the **error-down-threshold error-statistics** configuration exists on the switch, the configuration remains unchanged after the system software version is upgraded to V200R009C00 or a later version.

Example

By default, the alarm threshold of CRC error packets that cause the interface status to change to Error-Down is 10 and the alarm interval is 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] error-down-threshold error-statistics 10 interval 30
```

4.2.33 error-statistics threshold-event trigger error-down

Function

The **error-statistics threshold-event trigger error-down** command configures an interface to transit to the error-down state when the number of error packets received on the interface reaches the threshold.

The **undo error-statistics threshold-event trigger error-down** command restores the default setting.

By default, an interface does not transit to the error-down state when the number of error packets received on the interface reaches the threshold.

Format

error-statistics threshold-event trigger error-down

undo error-statistics threshold-event trigger error-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an Ethernet interface receives excessive error packets, faults such as packet loss will occur. Because the interface is still in Up state, traffic is still transmitted on the interface even if a backup link is configured. To avoid impact on services, you can configure the interface to change to the Error-down state when it receives excessive error packets. When the number of received error packets on the interface exceeds the threshold, the system disables the interface and records the interface status as **ERROR DOWN(error-statistics)** state (indicating that the interface is Down because of excessive error packets). Services are then switched to the backup link immediately.

Follow-up Procedure

An interface in Error-down state can be recovered using either of the following methods:

- Manual recovery: If a few interfaces need to be recovered forcibly, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.
- Automatic recovery: If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. You can run the **error-down auto-recovery cause error-statistics interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. An interface in Error-down state automatically recovers when the specified delay time expires.

Example

Configure GE0/0/1 to transit to the error-down state when the number of error packets received on the interface reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] error-statistics threshold-event trigger error-down
```

4.2.34 error-statistics trigger speed-down-grade

Function

The **error-statistics trigger speed-down-grade** command configures the blacklist of terminal MAC addresses that can be identified in automatic rate reduction on interfaces.

The **undo error-statistics trigger speed-down-grade** command deletes the blacklist of terminal MAC addresses that can be identified in automatic rate reduction on interfaces.

By default, the device can identify only MAC addresses starting with 001B-82.

NOTE

This command is supported only on the following switch models: S5731-S, S5731S-S, S5731-H, S5731S-H.

Format

error-statistics trigger speed-down-grade mac-address *mac-address* **mask** *mask* [**description** *description*]

undo error-statistics trigger speed-down-grade mac-address { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the terminal MAC address that can be identified.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits. The value cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
mask *mask*	Specifies the mask of a terminal MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
description *description*	Specifies the description of a terminal MAC address.	The value is a string of 1 to 80 characters. The character string is case sensitive and can contain blanks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GE electrical interface on a device is connected to a specific printer and the interface rate is higher than 10 Mbit/s, the interface can go Up, but the printer cannot work properly. Alignment error packets will be detected on the interface. In this case, you can run the **set error-statistics trigger speed-down-grade** command to enable the device to automatically reduce the interface rate when the number of error packets on the interface reaches the threshold. The device then automatically sets the interface rate to 10 Mbit/s, reports an alarm (hwPortErrPktSpeedDownGrade), and records a log (IFPDT/1/ERRPKT_SPEEDDOWN) when the following conditions are met:

- The interface receives three alignment error packets within 60 seconds.
- The interface is in the auto-negotiation state and works at the rate of 100 Mbit/s.

- Only one MAC address is learned on the interface, and the MAC address starts with 001B-82 or is in the MAC address blacklist configured using this command.

Precautions

This command supports a maximum of 32 terminal MAC address blacklists, excluding the default MAC address blacklist in which MAC addresses start with 001B-82.

Example

Configure the MAC address 1-1-1 in the blacklist of the terminal MAC address that can be identified in automatic rate reduction on interfaces.

```
<HUAWEI> system-view
[HUAWEI] error-statistics trigger speed-down-grade mac-address 1-1-1 mask ffff-0-0 description
printer
```

4.2.35 fast-link-down disable

Function

The **fast-link-down disable** command enables an interface to go Down after a delay.

The **undo fast-link-down disable** command disables an interface from going Down after a delay.

By default, an interface is disabled from going Down after a delay.

NOTE

Only the GE electrical interfaces of the following models support this command:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S6720S-S, S5735-S, S5735-S-I, S5735S-S

Format

fast-link-down disable

undo fast-link-down disable

Parameters

None

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface is enabled to go Down after a delay, the device detects the interface Down event after a delay of hundreds of milliseconds. When the interface alternates between Up and Down states, the interface does not go Down immediately, enhancing the anti-interference capability of the device.

Precautions

- If the **energy-efficient-ethernet enable** command has been executed to enable the EEE function on an electrical interface, the interface cannot be enabled to go Down after a delay. If the **fast-link-down disable** command has been executed to enable the interface to go Down after a delay, you can still run the **energy-efficient-ethernet enable** command to enable the EEE function on the interface.
- If the loopback detection mode has been configured on an interface using the **loopback** command, the interface cannot be enabled to go Down after a delay. If the **fast-link-down disable** command has been executed to enable the interface to go Down after a delay, you can still run the **loopback** command to configure the loopback detection mode for the interface.

Example

Enable an interface to go Down after a delay.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] fast-link-down disable
```

4.2.36 fec mode base-r

Function

The **fec mode base-r** command enables the Base-R FEC function on an interface.

The **fec mode none** command disables the Base-R FEC function on an interface.

The **undo fec mode** command restores the default Base-R FEC configuration on an interface.

By default, the medium on a 25GE interface determines whether the Base-R FEC function is enabled on the interface. For details, see **Table 4-30**.

NOTE

This command is supported on the following: S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S6730-H28Y4C, S6730-H24X4Y4C and S7Y08000 cards.

This command is supported when the interface working mode on the S7X08000 or S7X0800K0 card is set to 25GE using the **set card port-config-mode 25g-port enable** command.

Format

fec mode { **base-r** | **none** }

undo fec mode [**base-r** | **none**]

Parameters

Parameter	Description	Value
base-r	Enables the Base-R FEC function.	-
none	Disables the Base-R FEC function.	-

Views

25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Base-R FEC is a bit error correction technology that adds correction information to data packets at the transmit end, and corrects bit errors generated during data packet transmission at the receive end based on the correction information. You can enable the Base-R FEC function to improve the signal quality.

You can run the **display interface** command in any view or run the **display this interface** command in the interface view to check whether the FEC function is enabled on an interface based on the **Fec** field in the command output.

Prerequisites

You can run this command on an interface only when the following conditions are met:

- Auto-negotiation is disabled on the interface.
- The interface is not a stack member interface.

Precautions

- For the device running a version earlier than V200R019C10, the Base-R FEC function is enabled by default on interfaces and cannot be disabled. If you need to disable the function, upgrade the device to V200R019C10 or a later version.
- In V200R019C10 and later versions: Ensure that the FEC status on both ends of a link is the same. If the Base-R FEC function is enabled on one end, this function also needs to be enabled on the other end to ensure that the Base-R FEC status on both ends of the link is the same.
- The FEC function is mutually exclusive with auto-negotiation and the **port mode ge** command. If FEC has been configured, the FEC configuration will be automatically deleted when auto-negotiation is enabled or the **port mode ge** command is run.
- When an XGE optical module or XGE high-speed cable is installed on a 25GE interface, the interface does not support the Base-R FEC function.

- When a 40GE optical module or 40GE high-speed cable is installed on a 100GE interface, the interface does not support the Base-R FEC function.
- When 25GE interfaces are interconnected, you are advised to enable FEC on both ends of the link to reduce the transmission bit error rate of the physical link. Otherwise, error packets may be generated.

Example

Enable the Base-R FEC function on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface 25ge 0/0/1
[HUAWEI-25GE0/0/1] fec mode base-r
```

4.2.37 fec mode rs

Function

The **fec mode rs** command enables the Reed-Solomon Forward Error Correction (RS-FEC) function on an interface.

The **fec mode none** command disables the RS-FEC function on an interface.

The **undo fec mode** command restores the default RS-FEC configuration on an interface.

By default, the medium on an optical interface determines whether the RS-FEC function is enabled on the interface. For details, see **Table 4-30** and **Table 4-31**.

Table 4-30 FEC function of 25GE interfaces

Interface Type	FEC Requirement	Default Setting
SFP-25G-AOC (5e-5)	RS-FEC	Enabled
SFP-25G-SR	RS-FEC	Enabled
SFP-25G-ACC (5e-5)	RS-FEC	Enabled
25G BASE-CR CA-L	RS-FEC	Auto-negotiation is enabled: 1. Whether to enable FEC through negotiation 2. Whether to enable RS-FEC or Base-R FEC through negotiation
25G BASE-CR CA-S	Base-R FEC	
25G BASE-CR CA-N	None	
SFP-25G-AOC (10e-12)	RS-FEC/Base-R FEC/None	Enabled
SFP-25G-ACC (10e-12)	RS-FEC/Base-R FEC/None	Enabled
10G/25G_BR_SFP28	RS-FEC	Enabled (cannot be modified)

Interface Type	FEC Requirement	Default Setting
25GBASE_ER_SFP28	RS-FEC	Enabled (cannot be modified)

Table 4-31 FEC function of 100GE interfaces

Interface Type	FEC Requirement	Default Setting
QSFP-100G-AOC (5e-5)	RS-FEC	RS-FEC
QSFP-100G-SR4	RS-FEC	RS-FEC
QSFP-100G-LR4	None	None
100GBASE_LR1_QSFP28	None	None
100G Base-ER4	None	None
100G Base-SR10	None	None
QSFP-100G-CWDM4 with FEC	RS-FEC	RS-FEC
QSFP-100G-CWDM4-Lite	RS-FEC	RS-FEC
QSFP-100G-PSM4	RS-FEC	RS-FEC
QSFP-100G-ACC (5e-5)	RS-FEC	RS-FEC
100G Base-CR4	RS-FEC	RS-FEC
QSFP-100G-CLR4	RS-FEC/None	RS-FEC
QSFP-100G-AOC (10e-12)	RS-FEC/None	RS-FEC
QSFP-100G-ACC (10e-12)	RS-FEC/None	RS-FEC
100GBASE_SDLC_QSFP28	None	None

Format

fec mode { **rs** | **none** }

undo fec mode [**rs** | **none**]

Parameters

Parameter	Description	Value
rs	Enables the RS-FEC function.	-

Parameter	Description	Value
none	Disables the RS-FEC function.	-

Views

25GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RS-FEC is a bit error correction technology that adds correction information to data packets at the transmit end, and corrects bit errors generated during data packet transmission at the receive end based on the correction information. RS-FEC improves the signal quality, but increases the signal transmission delay. You can disable this function based on requirements to reduce the signal transmission delay.

You can run the **display interface** command in any view or run the **display this interface** command in the interface view to check whether the FEC function is enabled on an interface based on the **FEC** field in the command output.

Precautions

- For the device running a version earlier than V200R019C00, the RS-FEC function is enabled by default on interfaces and cannot be disabled. If you need to disable the function, upgrade the device to V200R019C00 or a later version.
- In V200R019C00 and later versions, if the RS-FEC function is enabled on one end, this function also needs to be enabled on the other end to ensure that the RS-FEC status on both ends of the link is the same.
- When an XGE optical module or XGE high-speed cable is installed on a 25GE interface, the interface does not support the RS-FEC function.
- When a 40GE optical module or 40GE high-speed cable is installed on a 100GE interface, the interface does not support the RS-FEC function.
- The FEC function is mutually exclusive with auto-negotiation and the **port mode ge** command. If FEC has been configured, the FEC configuration will be automatically deleted when auto-negotiation is enabled or the **port mode ge** command is run.
- When 25GE interfaces are interconnected, you are advised to enable FEC on both ends of the link to reduce the transmission bit error rate of the physical link. Otherwise, error packets may be generated.

Example

Disable the FEC function on 100GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface 100ge 0/0/1
[HUAWEI-100GE0/0/1] fec mode none
```

4.2.38 flow-control (interface view)

Function

The **flow-control** command enables flow control on an Ethernet interface.

The **undo flow-control** command disables flow control on an Ethernet interface.

By default, flow control is disabled on an Ethernet interface.

NOTE

The following interfaces do not support this command:

- S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), and S5732-H48XUM2CC
    - 25G, 40G, and 100G interfaces of the device.
    - Four SFP28 Ethernet optical interfaces (25GE by default) and two QSFP28 Ethernet optical interfaces (40GE by default) have been configured using the **set device port-config-mode enable** command.
    - 8*10GE ports and 2*25GE ports when the S7X08000 card is installed.
    - 8*25GE ports when the S7Y08000 card is installed.
- GE interfaces of the S5735S-H24S4XC-A
- GE interfaces of the S5736-S24S4XC and S5736-S48S4XC
- When the RTU license is not loaded on the S6730-H24X4Y4C, the first eight XGE interfaces numbered 0/0/1 to 0/0/8 do not support flow control. In V200R021C00 and later versions, the RTU license can be loaded. After the license is loaded, the interface rate is increased from 10 Gbit/s to 25 Gbit/s, and the first eight 25GE interfaces numbered 0/1/1 to 0/1/8 do not support flow control.
- First eight 25GE interfaces of the S6730-H28Y4C
- XGE interfaces that have copper modules installed on the S6735-S

Format

flow-control

undo flow-control

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow control prevents packet loss caused by network congestion. If network congestion occurs on the local device after flow control is configured, the local device sends a message to the remote device, requesting the remote device to temporarily stop sending packets. After receiving the message, the remote device temporarily stops sending packets to the local device regardless of the interface working rate. In this case, the device can receive and send pause frames.

Precautions

- If flow control is enabled on an interface, it must also be enabled on the peer interface.
- Flow control and flow control auto-negotiation can be configured on Ethernet interfaces, but they cannot be configured concurrently.
- When an interface works in half-duplex mode, flow control does not take effect on the interface.
- In a scenario where Layer 3 services are deployed, enabling flow control may affect the IP traffic forwarding on the interface. As a result, the interface becomes unavailable. You can run the **undo flow-control** command in the interface view to disable flow control to recover the interface.
- If the flow control configuration is implemented on the S5735S-H and S5736-S using the **flow-control** command, the rate limit for outbound traffic of the GE electrical interface is 200 Mbit/s, and a congestion occurs, the inbound traffic rate cannot be reduced to be the same as the outbound traffic rate on the GE electrical interface. (The inbound traffic rate is about 200 Mbit/s.)
- For the S2730S-S, S5735-L1, S5735-L-I, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the multicast functions (both Layer 2 and Layer 3 multicast functions) conflict with the flow control function.

Example

Enable flow control on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] flow-control
```

4.2.39 flow-control negotiation

Function

The **flow-control negotiation** command enables flow control auto-negotiation on an Ethernet interface.

The **undo flow-control negotiation** command disables flow control auto-negotiation on an Ethernet interface.

By default, flow control auto-negotiation is disabled on an Ethernet interface.

NOTE

The following interfaces do not support this command:

- S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), and S5732-H48XUM2CC
  - 25G, 40G, and 100G interfaces of the device.
  - Four SFP28 Ethernet optical interfaces (25GE by default) and two QSFP28 Ethernet optical interfaces (40GE by default) have been configured using the **set device port-config-mode enable** command.
  - 8*10GE ports and 2*25GE ports when the S7X08000 card is installed.
  - 8*25GE ports when the S7Y08000 card is installed.
- GE interfaces of the S5735S-H24S4XC-A
- GE interfaces of the S5736-S24S4XC and S5736-S48S4XC
- When the RTU license is not loaded on the S6730-H24X4Y4C, the first eight XGE interfaces numbered 0/0/1 to 0/0/8 do not support flow control. In V200R021C00 and later versions, the RTU license can be loaded. After the license is loaded, the interface rate is increased from 10 Gbit/s to 25 Gbit/s, and the first eight 25GE interfaces numbered 0/1/1 to 0/1/8 do not support flow control.
- First eight 25GE interfaces of the S6730-H28Y4C
- XGE interfaces that have copper modules installed on the S6735-S

Format

flow-control negotiation

undo flow-control negotiation

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion causes packet loss. Flow control can prevent packet loss. If congestion occurs on a device, the device sends a message to request the peer device to stop sending packets, which prevents packet loss. Flow control auto-negotiation enables a device to determine whether to enable flow control by negotiating with the peer device.

Prerequisites

Run the **negotiation auto** command to configure the Ethernet interface to work in auto negotiation mode.

Precautions

- Electrical interfaces support flow control auto-negotiation.
- If flow control auto-negotiation is enabled on an interface, it must also be enabled on the peer interface.
- If flow control has been enabled on an Ethernet interface using the **flow-control** command, run the **undo flow-control** command to disable flow control before running the **flow-control negotiation** command. Otherwise, the **flow-control negotiation** command fails to be executed.
- This command can be used on an XGE optical interface that has a GE copper module installed.
- This command can be used on a GE optical interface that has a GE optical module or GE copper module installed.
- This command can be used on an 25GE optical interface that has a GE copper module installed. Before installing a GE copper module on a 25GE optical interface, you need to run the **port mode ge** command to configure the interface to work at the rate of 1 Gbit/s.

NOTE

On the S5720-52P-LI-AC, if interfaces 0 to 23 work as inbound interfaces (or outbound interfaces) and interfaces 24 to 47 work as outbound interfaces (or inbound interfaces), flow control auto-negotiation does not take effect on these interfaces.

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

Example

Enable flow control auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] flow-control negotiation
```

4.2.40 flow-control negotiation receive

Function

The **flow-control negotiation receive** command enables received flow control auto-negotiation on an Ethernet interface.

The **undo flow-control negotiation receive** command disables received flow control auto-negotiation on an Ethernet interface.

By default, received flow control auto-negotiation is disabled on an Ethernet interface.

NOTE

The following interfaces do not support this command:

- S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), and S5732-H48XUM2CC
  - 25G, 40G, and 100G interfaces of the device.
  - Four SFP28 Ethernet optical interfaces (25GE by default) and two QSFP28 Ethernet optical interfaces (40GE by default) have been configured using the **set device port-config-mode enable** command.
  - 8*10GE ports and 2*25GE ports when the S7X08000 card is installed.
  - 8*25GE ports when the S7Y08000 card is installed.
- GE interfaces of the S5735S-H24S4XC-A
- GE interfaces of the S5736-S24S4XC and S5736-S48S4XC
- When the RTU license is not loaded on the S6730-H24X4Y4C, the first eight XGE interfaces numbered 0/0/1 to 0/0/8 do not support flow control. In V200R021C00 and later versions, the RTU license can be loaded. After the license is loaded, the interface rate is increased from 10 Gbit/s to 25 Gbit/s, and the first eight 25GE interfaces numbered 0/1/1 to 0/1/8 do not support flow control.
- First eight 25GE interfaces of the S6730-H28Y4C
- XGE interfaces that have copper modules installed on the S6735-S
- Ethernet optical interfaces on the S5720I-SI, S5720-LI (last four optical interfaces on the S5720-52X-LI-48S-AC), and S5720S-LI

Format

flow-control negotiation receive

undo flow-control negotiation receive

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow control prevents packet loss caused by network congestion. Received flow control auto-negotiation enables a device to determine whether to enable received flow control by negotiating with the peer device. On a unidirectional communication network, you can run the **flow-control negotiation receive** command on the Ethernet interface functioning as the outbound interface at the transmit side to enable received flow control auto-negotiation, and run the **flow-control negotiation** command on the inbound interface at the receive side to enable flow control auto-negotiation. After received flow control auto-negotiation is enabled on the Ethernet interface, if congestion occurs on a device, the device sends a message to request the peer device to stop sending packets, which prevents packet loss.

Prerequisites

The Ethernet interface has been configured to work in auto-negotiation mode using the **negotiation auto** command.

Precautions

- Electrical interfaces support this configuration.
- Received flow control auto-negotiation can be implemented only if flow control auto-negotiation is enabled on the interface of the peer device.
- Flow control, received flow control, flow control auto-negotiation, and received flow control auto-negotiation can be configured on Ethernet interfaces, but cannot be configured together. For example, if received flow control auto-negotiation has been enabled on an Ethernet interface using the **flow-control receive** command, you need to run the **undo flow-control receive** command to disable received flow control and then run the **flow-control negotiation receive** command. Otherwise, the **flow-control negotiation receive** command fails to be executed.
- XGE optical interfaces support this command after GE copper modules are installed on them.
- GE optical interfaces support this command after GE optical or GE copper modules are installed on them.
- This command can be used on an 25GE optical interface that has a GE copper module installed. Before installing a GE copper module on a 25GE optical interface, you need to run the **port mode ge** command to configure the interface to work at the rate of 1 Gbit/s.

NOTE

For the S5720-52P-LI-AC, if received flow control auto-negotiation is configured on the interfaces 0 to 23 that work as inbound interfaces and flow control auto-negotiation is configured on the interfaces 24 to 47 that work as outbound interfaces, received flow control auto-negotiation and flow control auto-negotiation do not take effect.

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

Example

Enable received flow control auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] flow-control negotiation receive
```

4.2.41 flow-control receive

Function

The **flow-control receive** command enables received flow control on an Ethernet interface.

The **undo flow-control receive** command disables received flow control on an Ethernet interface.

By default, received flow control is disabled on an Ethernet interface.

NOTE

The following interfaces do not support this command:

- S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), and S5732-H48XUM2CC
  - 25G, 40G, and 100G interfaces of the device.
  - Four SFP28 Ethernet optical interfaces (25GE by default) and two QSFP28 Ethernet optical interfaces (40GE by default) have been configured using the **set device port-config-mode enable** command.
  - 8*10GE ports and 2*25GE ports when the S7X08000 card is installed.
  - 8*25GE ports when the S7Y08000 card is installed.
- GE interfaces of the S5735S-H24S4XC-A
- GE interfaces of the S5736-S24S4XC and S5736-S48S4XC
- When the RTU license is not loaded on the S6730-H24X4Y4C, the first eight XGE interfaces numbered 0/0/1 to 0/0/8 do not support flow control. In V200R021C00 and later versions, the RTU license can be loaded. After the license is loaded, the interface rate is increased from 10 Gbit/s to 25 Gbit/s, and the first eight 25GE interfaces numbered 0/1/1 to 0/1/8 do not support flow control.
- First eight 25GE interfaces of the S6730-H28Y4C
- XGE interfaces that have copper modules installed on the S6735-S

Format

flow-control receive

undo flow-control receive

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow control prevents packet loss caused by network congestion. On a unidirectional communication network, after received flow control is enabled on the Ethernet interface at the transmit side using the **flow-control receive** command and flow control is enabled on the Ethernet interface at the receive side using the **flow-control** command, if congestion occurs on the device at the receive side, the device sends a message to the device at the transmit side to notify it to stop sending packets. After receiving the message, the device at the transmit side temporarily stops sending packets to the device at the receive side regardless of the interface working rate, preventing congestion. In this case, the device at the transmit side can receive pause frames, but cannot send pause frames; the device at the receive side can receive and send pause frames.

Precautions

- Flow control can be implemented only after flow control is enabled on the peer device.
- Flow control, received flow control, flow control auto-negotiation, and received flow control auto-negotiation can be configured on Ethernet interfaces, but cannot be configured together.
- When an interface works in half-duplex mode, received flow control does not take effect.
- In a scenario where Layer 3 services are deployed, enabling received flow control may affect the IP traffic forwarding on the interface. As a result, the interface becomes unavailable. You can run the **undo flow-control receive** command in the interface view to disable received flow control to recover the interface.
- For the S2730S-S, S5735-L1, S5735-L-I, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the multicast functions (both Layer 2 and Layer 3 multicast functions) conflict with the flow control function.

Example

Enable received flow control on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] flow-control receive
```

4.2.42 group-member

Function

The **group-member** command adds specified Ethernet interfaces to a permanent port group.

The **undo group-member** command deletes specified Ethernet interfaces from a permanent port group.

By default, no Ethernet interface is added to a permanent port group.

Format

group-member { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo group-member { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

undo group-member all-unavailable-interface

Parameters

Parameter	Description	Value
interface-type interface-number1 **to** *interface-type interface-number2*	Adds an Ethernet interface to a permanent port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	*interface-number2* must be greater than *interface-number1*.
all-unavailable-interface	Delete all unavailable interfaces from this port-group.	-

Views

Permanent port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Prerequisite

Prior to running this command, run the **port-group** command in the system view to create a permanent interface group.

Configuration Impact

If the **group-member** command is run more than once, all configurations take effect.

Precautions

- Both physical and logical interfaces can be added to a permanent port group.
- This command has the same function as the **port-group group-member** command that is used in the system view. You can also run the **port-group group-member** command to add interfaces to a temporary port group to configure the interfaces in batches.
- When you specify the keyword **to** in the **group-member** command:
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not used, these limitations do not apply.
  - Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Add GE0/0/1 and GE0/0/2 to port group **portgroup1**.

```
<HUAWEI> system-view
[HUAWEI] port-group portgroup1
[HUAWEI-port-group-portgroup1] group-member gigabitethernet 0/0/1 to gigabitethernet 0/0/2
```

4.2.43 interface (Ethernet interface)

Function

The **interface** command displays the specified interface view or sub-interface view.

The **undo interface** command deletes a sub-interface.

Format

interface { **ethernet** | **gigabitethernet** | **multige** | **xgigabitethernet** | **25ge** | **40ge** | **100ge** } *interface-number*[.*subinterface-number*] [**mode l2**]

undo interface { **ethernet** | **gigabitethernet** | **multige** | **xgigabitethernet** | **25ge** | **40ge** | **100ge** } *interface-number*[.*subinterface-number*]

Parameters

Parameter	Description	Value
ethernet	Displays the view of an FE interface.	-
gigabitethernet	Displays the view of a GE interface.	-
multige	Displays the view of a MultiGE interface. **NOTE** Only the S5720-28X-PWH-LI-AC, S5720-28X-PWH-LI-ACF, S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, and S5736-S24UM4XC support MultiGE interfaces.	-
xgigabitethernet	Displays the view of an XGE interface.	-
25ge	Displays the view of a 25GE interface.	-
40ge	Displays the view of a 40GE interface.	-
100ge	Displays the view of a 100GE interface.	-
interface-number	Specifies the number of an interface.	The value depends on the interface type and slot ID.
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Parameter	Description	Value
mode l2	Configures a sub-interface to work in Layer 2 mode for the VXLAN service. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After entering the specified Ethernet interface view, you can set attributes for the Ethernet interface.

NOTE

- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Layer 2 Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Layer 3 Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

Enter the view of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1]
```

4.2.44 interface range

Function

The **interface range** command creates a temporary interface group and adds specified interfaces to this temporary interface group. Commands configured for a temporary interface group then automatically run on all member interfaces.

By default, no temporary interface group is created.

Format

interface range { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	The value of *interface-number2* must be larger than the value of *interface-number1*. A maximum of 48 temporary port groups can be created on a device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Configuration Impact

If the **interface range** command is run more than once, all configurations take effect.

Precautions

- The **interface range** and **port-group group-member** commands have the same functions. Therefore, use either of the commands for configuration. After exiting from the temporary port group view, the system deletes the temporary port group.
- The **interface range** command is equivalent to the **group-member** command executed in the permanent port group view. Multiple interfaces can be added to a permanent port group in batches using the **group-member** command.
- When you specify the keyword **to** in the **interface range** command:
  - The interfaces specified by *interface-number1* and *interface-number2* must reside on the same member switch. To add contiguous interfaces on different member switches to the same port group, run this command several times or use the keyword **to** several times.
  - The interfaces specified by *interface-number1* and *interface-number2* must be of the same type, for example, both of the interfaces are GE interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not specified, the preceding limitations do not apply.
  - Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Add GE0/0/1, 0/0/2, and 0/0/3 to a temporary port group.

```
<HUAWEI> system-view
[HUAWEI] interface range gigabitethernet 0/0/1 to gigabitethernet 0/0/3
[HUAWEI-port-group]
```

4.2.45 jumboframe enable

Function

The **jumboframe enable** command sets the maximum frame length allowed by an interface.

The **undo jumboframe enable** command restores the default maximum frame length allowed by an interface.

By default, the maximum frame length allowed by the S200, S1730S-S1, S500, S5735-S, S5735S-S, S5735-S-I, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735-L-I, and S5735S-L-M is 10240 bytes, and the maximum frame length allowed by other switches is 9216 bytes.

NOTE

The following switch models do not support this command:

S200, S1730S-S1, S500, S5735-S, S5735S-S, S5735-S-I, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735-L-I, and S5735S-L-M

Format

jumboframe enable [*value*]

undo jumboframe enable

Parameters

Parameter	Description	Value
value	Specifies the maximum frame length allowed by an Ethernet interface.	The value is an integer, in bytes. ● On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S6720S-S the value is an integer that ranges from 1536 to 10240, in bytes. ● On the S5732-H24S6Q, S5732-H48S6Q, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value is an integer that ranges from 1536 to 12288, in bytes. ● On the S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC, S5731-H, S5731S-H, S5731-S, and S5731S-S, the value is an integer that ranges from 1536 to 9600, in bytes. ● On the S6735-S, the value is an integer that ranges from 1536 to 9216, in bytes. **NOTE** On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, *value* cannot be set to an odd number. For GE electrical interfaces on the S5735S-H and S5736-S, *value* can only be set to 10232. If *value* is set to an odd number in a version earlier than V200R008, the value of *value* increases by one automatically after the system software is upgraded to V200R008 or later versions. For example, *value* is set to 8879 in V200R007. After the system software is upgraded to V200R008, the value of *value* is 8880.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When transmitting a large amount of data (such as files and videos), an Ethernet interface may receive jumbo frames. If the jumbo frame length exceeds the default data frame length that can be processed, the device directly discards the jumbo frames. You can set the jumbo frame length allowed on an interface.

After you configure the device to allow jumbo frames, packet forwarding becomes more flexible. If multiple common Ethernet frames are used to transmit a data packet, many redundant contents such as interframe gaps (IFGs) and preambles are also transmitted. If jumbo frames are used to transmit the data packet, fewer frames, as well as fewer IFGs and preambles, are transmitted, improving bandwidth efficiency.

Precautions

If you run the **jumboframe enable** command multiple times in the same interface view to set the maximum frame length allowed by the interface, only the latest configuration takes effect.

If you run the **jumboframe enable** command on an interface without specifying the *value* parameter, the interface allows the default jumbo frame length. By default, the jumbo frame length allowed by Ethernet interfaces of other models is 9216 bytes.

If the length of an outgoing packet exceeds the maximum frame length allowed on an interface, the interface can directly forward the packet.

If the maximum frame length allowed by interfaces is configured in batches through the port group function, the maximum frame length range displayed when the **jumboframe enable ?** command is executed in the port group view is 1536-12288. The actual maximum frame length allowed by the interfaces is defined in **Parameters**. Configure the maximum frame length as required.

Example

Set the maximum frame length allowed by GE0/0/1 to 5000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] jumboframe enable 5000
```

4.2.46 log-threshold input-rate output-rate

Function

The **log-threshold input-rate output-rate** command sets the inbound and outbound bandwidth usage thresholds for generating a log.

The **undo log-threshold input-rate output-rate** command restores the default inbound and outbound bandwidth usage thresholds for generating a log.

The default inbound and outbound bandwidth usage thresholds for generating a log is 80.

Format

log-threshold { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]

undo log-threshold { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Specifies the inbound bandwidth.	-
output-rate	Specifies the outbound bandwidth.	-
bandwidth-in-use	Specifies the bandwidth usage threshold for generating a log.	The value is an integer that ranges from 1 to 100.
resume-rate *resume-threshold*	Specifies the bandwidth usage threshold for clearing a log.	The value is an integer that ranges from 1 to the value of *bandwidth-in-use*. The default value is the value of *bandwidth-in-use*.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Monitoring bandwidth usage helps you know current load on a device. If the bandwidth usage exceeds a threshold, bandwidth resources are insufficient and the device capacity needs to be expanded. For example, if the bandwidth usage exceeds 95%, an alarm is generated, indicating that bandwidth resources are almost exhausted. As a result, some services may be interrupted before device capacity expansion.

You can configure two thresholds: low threshold (log threshold) and high threshold (alarm threshold). The system generates a log when the bandwidth usage exceeds the low threshold and generates an alarm when the bandwidth usage exceeds the high threshold. This configuration ensures that you can expand the device capacity in advance to avoid service interruptions caused by bandwidth exhaustion.

NOTE

Outbound bandwidth usage threshold = (Outbound interface rate/Outbound physical interface bandwidth) x 100

Inbound bandwidth usage threshold = (Inbound interface rate/Inbound physical interface bandwidth) x 100

The **trap-threshold** command is used to set the bandwidth usage threshold for generating a trap.

The **log-threshold input-rate output-rate** command with the following parameters provides various functions:

- **log-threshold input-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the inbound bandwidth usage threshold for generating a log to provide the following functions:
  - If inbound bandwidth usage value exceeds the value of *bandwidth-in-use*, an IFNET_BWRATE_IN_RISING log is generated, indicating that inbound bandwidth usage exceeds the configured threshold.
  - If inbound bandwidth usage value is lower than the value of *resume-threshold*, an IFNET_BWRATE_IN_RESUME log is generated, indicating that inbound bandwidth usage is lower than the configured threshold.
- **log-threshold output-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the outbound bandwidth usage threshold for generating a log to provide the following functions:
  - If outbound bandwidth usage value exceeds the value of *bandwidth-in-use*, an IFNET_BWRATE_OUT_RISING log is generated, prompting for a bandwidth increase request.
  - If outbound bandwidth usage falls below the threshold specified by *resume-threshold*, an IFNET_BWRATE_OUT_RESUME log is generated, indicating that bandwidth usage has been restored.

If the offset between the value of *bandwidth-in-use* and the value of *resume-threshold* is too small, log information may be frequently displayed.

The log threshold must be lower than the trap threshold, providing efficient protection for services. For example, when the inbound bandwidth usage reaches 80%, a log is generated. If the inbound bandwidth usage continues to increase and reaches 95%, a trap is generated. This ensures that a log is generated for inbound bandwidth usage of 80%, and a trap is generated for inbound bandwidth usage of 95%. Either the log or the trap prompts for a bandwidth increase, preventing service interruption.

Example

Configure GE0/0/1 to generate a log when the outbound interface rate exceeds 80% of the bandwidth.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] log-threshold output-rate 80
```

Configure GE0/0/1 to generate a log when the outbound interface rate exceeds 80% of the bandwidth and to clear a log when the outbound interface rate is lower than 60% of the bandwidth.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] log-threshold output-rate 80 resume-rate 60
```

4.2.47 log-threshold input-discard output-discard (interface view)

Function

The **log-threshold input-discard** command sets the log threshold for congestion-triggered packet loss and interval for collecting statistics on discarded packets in the inbound direction of an interface.

The **log-threshold output-discard** command sets the log threshold for congestion-triggered packet loss and interval for collecting statistics on discarded packets in the outbound direction of an interface.

The **undo log-threshold input-discard** command restores the default settings.

The **undo log-threshold output-discard** command restores the default settings.

By default, the log threshold for congestion-triggered packet loss in the inbound or outbound direction of an interface is 3000, and the interval for collecting statistics on discarded packets in the inbound or outbound direction of an interface is 300s.

Format

log-threshold { **input-discard** | **output-discard** } [*threshold-value* **interval** *interval-value*]

undo log-threshold { **input-discard** | **output-discard** }

Parameters

Parameter	Description	Value
input-discard	Records logs about congestion-triggered packet loss in the inbound direction of an interface.	-

Parameter	Description	Value
output-discard	Records logs about congestion-triggered packet loss in the outbound direction of an interface.	-
threshold-value	Specifies the log threshold for congestion-triggered packet loss.	The value is an integer in the range from 100 to 4294967295.
interval *interval-value*	Specifies the interval for collecting statistics on discarded packets due to congestion.	The value is an integer in the range from 60 to 86400, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion during service transmission may cause packet loss. If a lot of packets are discarded, services are affected. To better monitor the number of discarded packets, you can run the **log-threshold output-discard** or **log-threshold input-discard** command to set the threshold for packet loss caused by congestion and interval for collecting statistics on discarded packets in the inbound or outbound direction of an interface. The device generates a log when the number of discarded incoming and outgoing packets on the interface in a specified period exceeds the threshold. Logs help you know the congestion on the interface. You can determine whether to increase the bandwidth or cancel the bandwidth limit on the interface based on the logs. In this way, the congestion problem can be solved.

Precautions

- If the number of discarded incoming and outgoing packets falls below the threshold in a specified period, the device generates a log indicating that the number of discarded packets falls below the threshold.
- If the number of discarded packets exceeds the threshold in an interval for collecting statistics on discarded packets, the device immediately generates a log indicating that the number of discarded packets exceeds the threshold, and enters the next statistics interval. In the next statistics interval, the number of discarded packets on an interface is calculated using the following formula:

Number of discarded packets = Current number of discarded packets - Number of discarded packets in the beginning of the statistics interval

- If the number of discarded packets exceeds the threshold in several consecutive statistics intervals, the device only generates a log in the first statistics interval, indicating that the number of discarded packets exceeds the threshold. If the number of discarded packets falls below the threshold, the device generates a log indicating that the number of discarded packets falls below the threshold. If the number of discarded packets on an interface exceeds the threshold again, the device will generate a log indicating that the number of discarded packets exceeds the threshold.
- If the user log function is disabled in the system view, the user log function no longer takes effect in the interface view. To record user logs, run the **log-threshold** { **input-discard** | **output-discard** }* command in the system view to enable the log function first.

Example

Set the log threshold for congestion-triggered packet loss to 100 and interval for collecting statistics on discarded packets to 60 seconds in the inbound direction of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] log-threshold input-discard 100 interval 60
```

4.2.48 log-threshold

Function

The **log-threshold** command enables the log function for congestion-triggered packet loss on all interfaces of a device.

The **undo log-threshold** command disables the log function for congestion-triggered packet loss on all interfaces of a device.

By default, the log function is enabled for congestion-triggered packet loss on all interfaces of a device.

Format

log-threshold { **input-discard** | **output-discard** }*

undo log-threshold { **input-discard** | **output-discard** }*

Parameters

Parameter	Description	Value
input-discard	Records logs about congestion-triggered packet loss in the inbound direction of an interface.	-

Parameter	Description	Value
output-discard	Records logs about congestion-triggered packet loss in the outbound direction of an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enable or disable the log function for congestion-triggered packet loss on all interfaces of a device in the system view.

Example

Enable the log function for inbound congestion-triggered packet loss on a device.

```
<HUAWEI> system-view
[HUAWEI] log-threshold input-discard
```

4.2.49 loopback

Function

The **loopback** command enables loopback detection on an interface.

The **undo loopback** command disables loopback detection on an interface.

By default, loopback detection is not configured.

Format

loopback internal

undo loopback

Parameters

Parameter	Description	Value
internal	Configures internal loopback detection on a specified interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When testing some special functions, for example, locating an Ethernet fault, you need to enable loopback detection on Ethernet interfaces to check whether the interfaces are working properly. After loopback detection is enabled on an Ethernet interface, the interface is in Up state if it works properly, and is in Down state if it fails.

Follow-up Procedure

Run the **display interface** command to check whether the current status of the interface configured with internal loopback is Up. If the **current status** of the interface is Up, the internal forwarding function works well; otherwise, a fault occurs during internal forwarding.

After loopback detection is enabled on an interface, the **Speed** field in the **display this interface** command output indicates the configured interface rate or the rate of the installed optical module, copper module, or network cable, and the **Bandwidth** field in the **display interface ethernet brief** command output indicates the actual interface rate. Installing and then removing the optical or copper module or restarting the device may affect the actual interface rate.

Precautions

- Loopback detection interrupts the operation of Ethernet interfaces and links. After loopback detection is performed, run the **undo loopback** command to disable loopback detection immediately.
- You cannot run the **loopback** command to perform loopback detection on a fabric port.
- The **loopback** command and the **single-fiber enable** command cannot be configured on the same interface.

Example

Configure loopback detection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback internal
Warning: The configuration may cause loops.
```

4.2.50 loopbacktest

Function

The **loopbacktest** command configures internal loopback detection on an interface.

By default, internal loopback detection is not configured.

Format

loopbacktest internal

Parameters

Parameter	Description	Value
internal	Configures internal loopback detection. Internal loopback detection is used to check whether the internal forwarding chip controls forwarding on the interface correctly. ● If the test packet is received, the internal forwarding chip functions properly. ● If the test packet is not received, the internal forwarding chip is faulty.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

3: Management level

Usage Guidelines

You can run the **loopbacktest** command to check whether the internal forwarding chip functions properly.

NOTE

Loopback detection is not required when an interface is shut down.

Loopback detection is not supported on a service stack interface.

The internal loopback detection result can be used only when no service is configured on the switch.

You cannot run the **loopbacktest** command to perform loopback detection on a fabric port.

After the energy-saving mode is set to basic or deep, loopback detection is disabled on an interface. Therefore, before performing loopback detection, set the energy-saving mode to standard.

Example

Configure internal loopback detection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopbacktest internal
Warning: This command may conflict with other service configurations. It can only be used on a device with
no configuration. Continu
e?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment...................
Info: Loopback packet test succeeded.
```

4.2.51 mdi

Function

The **mdi** command configures the medium dependent interface (MDI) mode of an Ethernet electrical interface.

The **undo mdi** command restores the default MDI mode of an Ethernet electrical interface.

By default, an Ethernet electrical interface automatically identifies the network cable type.

Format

mdi { **across** | **auto** | **normal** }

undo mdi

Parameters

Parameter	Description	Value
across	Sets the MDI mode of an Ethernet electrical interface to **across**.	-

Parameter	Description	Value
auto	Sets the MDI mode of an Ethernet electrical interface to **auto**. An Ethernet electrical interface automatically identifies the network cable type.	-
normal	Sets the MDI mode of an Ethernet electrical interface to **normal**.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Twisted pairs used to connect Ethernet devices include:

- Straight-through cable: connects devices of different types, such as a switch and a PC or a switch and a router.
- Crossover cable: connects devices of the same type, such as two switches, two routers, or two PCs.

Generally, if two interfaces are connected with a twisted-pair cable, the receive pin on the local end must be connected to the transmit pin on the remote end and the transmit pin on the local end must be connected to the receive pin on the remote end so that a link can be Up. According to pin assignment, twisted-pair cables are classified into straight-through and crossover cables. The device must support negotiation and crossover of receive and transmit pins so that Ethernet electrical interfaces can support the two types of twisted-pair cables. The device supports the following medium dependent interface (MDI) modes: auto, normal, and across.

Generally, when interfaces at both ends work in auto mode, devices can communicate regardless of whether the straight-through or crossover cable is used. Set the MDI mode to normal or across only when the device cannot identify the network cable type. When configuring an MDI mode on an interface, pay attention to the following points:

- When a straight-through cable is used, the local and remote interfaces must use different MDI modes, for example, across mode on one end and normal mode on the other end.

- When a crossover cable is used, the local and remote interfaces must use the same MDI mode. For example, both ends must use the across or normal mode, or at least one end uses the auto mode

NOTE

Electrical interfaces support the MDI type configuration.

The XGE electrical interfaces on the ES5D21X08T00 card of the S5731-H, and S5731S-H can only use the auto MDI type.

The MDI type can be configured on an optical interface that has a GE copper module installed. Before installing a GE copper module on a 25GE optical interface, you need to run the **port mode ge** command to configure the interface to work at the rate of 1 Gbit/s.

Example

Set the MDI mode of GE0/0/1 to **across**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mdi across
```

4.2.52 negotiation active

Function

The **negotiation active** command configures an interface to work in slave mode.

The **undo negotiation active** command cancels the slave mode configuration on an interface.

By default, an interface does not work in slave mode.

Format

negotiation active

undo negotiation active

Parameters

None

Views

MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a MultiGE interface on a Huawei switch is connected to an interface on a Cisco AP, the two interfaces may both support 2.5 Gbit/s or higher rates, but cannot negotiate to work in the highest rate. You can configure the MultiGE interface on the Huawei switch to work in slave mode (the interface on the Cisco AP works in master mode). The two interfaces then can negotiate to work in the highest rate supported by both of them to improve the data transmission capability.

Precautions

- It is recommended that you run this command on an interface working in auto-negotiation mode.
- When MultiGE interfaces of two switches are connected, you cannot configure the **negotiation active** command on the MultiGE interfaces simultaneously; otherwise, the MultiGE interfaces cannot go Up.

Example

Configure MultiGE 0/0/1 to work in slave mode.

```
<HUAWEI> system-view
[HUAWEI] interface MultiGE 0/0/1
[HUAWEI-MultiGE0/0/1] negotiation active
```

4.2.53 negotiation auto

Function

The **negotiation auto** command configures an Ethernet interface to work in auto-negotiation mode.

The **undo negotiation auto** command configures an Ethernet interface to work in non-auto negotiation mode.

By default, an Ethernet interface works in auto-negotiation mode.

Format

negotiation auto

undo negotiation auto

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, port group view, Meth interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Earlier Ethernet worked in 10M half-duplex mode and required mechanisms such as Carrier Sense Multiple Access (CSMA)/Collision Detection (CD) to ensure system stability. As Ethernet technology develops, full-duplex Ethernet and 100 Mbit/s Ethernet emerge. This greatly improves Ethernet performance. Auto-negotiation technology allows new Ethernet to be compatible with earlier Ethernet. In auto-negotiation mode, interfaces on both ends of a link negotiate their operating parameters, including the duplex mode and rate. If the negotiation succeeds, the two interfaces work at the same operating parameters.

Precautions

- For details about Ethernet interfaces supporting the auto-negotiation function, see Licensing Requirements and Limitations for Ethernet Interfaces.
- By default, auto-negotiation is enabled on GE optical interfaces and rate auto-negotiation is disabled. You can run the **speed auto-negotiation** command to enable rate auto-negotiation.
- When a GE optical module is installed on an XGE optical interface, the interface works in auto-negotiation mode by default. To configure the interface to work in non-auto-negotiation mode, run the **undo negotiation auto** command. If you replace the GE optical module with an XGE optical module, the interface does not support the auto-negotiation mode and works in non-auto-negotiation mode by default. If you replace the XGE optical module with a GE optical module, the **undo negotiation auto** command configuration becomes ineffective. If you need the interface to still work in non-auto-negotiation mode, reconfigure this command.
- After configuring the auto-negotiation function on an interface, if you remove and install a single optical fiber on the interface, the interface may be Up and the remote interface may be Down. You can run the **shutdown** and **undo shutdown** commands on the remote interface to make the remote interface go Up.

Example

Configure GE0/0/1 to work in non-auto negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo negotiation auto
```

4.2.54 negotiation priority

Function

The **negotiation priority** command configures the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.

The **undo negotiation priority** command restores the default protocol that a MultiGE interface in auto-negotiation mode preferentially uses.

By default, a MultiGE interface in auto-negotiation mode preferentially uses IEEE 802.3bz.

NOTE

Only multi-GE interfaces on the S5720-28X-PWH-LI-AC, S5720-28X-PWH-LI-ACF, S5732-H48XUM2CC, S5736-S24UM4XC, S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002) support this command.

Format

negotiation priority { **802.3bz** | **mgbase-t** }

undo negotiation priority

Parameters

Parameter	Description	Value
802.3bz	Configures IEEE 802.3bz as the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.	-
mgbase-t	Configures Mgbase-t as the protocol that a MultiGE interface in auto-negotiation mode preferentially uses. **NOTE** Only the S5732-H24UM2CC, S5732-H48XUM2CC, and S5732-H48UM2CC do not support this parameter.	-

Views

MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device supports 2.5 Gbit/s or 5 Gbit/s rate when the peer device connects to the MultiGE interface of Huawei switch and the peer device uses the proprietary protocol Mgbase-t of the Broadcom company, the MultiGE interface of the interconnected Huawei switch may fail to be enabled. You can configure Mgbase-t as the protocol that the MultiGE interface on the Huawei switch preferentially uses, so that the MultiGE interface can be properly enabled.

Example

Configure Mgbase-t as the protocol that a MultiGE interface in auto-negotiation mode preferentially uses.

```
<HUAWEI> system-view
[HUAWEI] interface MultiGE 0/0/1
[HUAWEI-MultiGE0/0/1] negotiation priority mgbase-t
```

4.2.55 port clock-mode slave

Function

The **port clock-mode slave** command sets the clock negotiation mode of an XGE electrical interface to the slave mode.

The **undo port clock-mode slave** command restores the clock negotiation mode of an XGE electrical interface to the auto-negotiation mode.

By default, the clock negotiation mode of an XGE electrical interface is the auto-negotiation mode.

NOTE

Only the XGE electrical interfaces of the ES5D21X08T00 cards support this command.

Format

port clock-mode slave

undo port clock-mode slave

Parameters

None

Views

XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a modern communications network, most telecommunications services require that the frequency offset or time difference between devices be in an acceptable range. When an XGE electrical interface on an ES5D21X08T00 card of a Huawei device connects to a non-Huawei device, the clock negotiation mode of the XGE electrical interface on the local device is auto-negotiation by default. The two devices determine the master/slave relationship based on the negotiation result and perform network clock synchronization. When the local device negotiates to become the master device, the interfaces on both ends may fail to go Up or their rate may decrease due to the impact of the non-Huawei device. In this case, run the **port clock-mode slave** command to set the clock negotiation mode of the XGE electrical interface of the local device to the slave mode. This configuration ensures clock synchronization between the two devices.

Precautions

If the interfaces on both ends are configured to work in slave mode, clock negotiation will fail and the interfaces cannot go Up.

Example

Set the clock negotiation mode of an XGE electrical interface to slave.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/1/1
[HUAWEI-XGigabitEthernet0/1/1] port clock-mode slave
```

4.2.56 port link-flap auto-detect protection disable

Function

The **port link-flap auto-detect protection disable** command disables global link flapping protection.

The **undo port link-flap auto-detect protection disable** or **port link-flap auto-detect protection enable** command enables global link flapping protection.

By default, global link flapping protection is enabled.

Format

port link-flap auto-detect protection disable

undo port link-flap auto-detect protection disable

port link-flap auto-detect protection enable

Parameters

Parameter	Description	Value
enable	Enables global link flapping protection.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If network jitter or a link fault occurs on an interface, the physical status of the interface frequently alternates between Up and Down, affecting service traffic forwarding. After global link flapping detection protection is enabled, if the number of times that an interface alternates between Up and Down within a specified period reaches the configured threshold, the system shuts down the interface so that the interface goes Down. This reduces the impact of interface link flaps on services.

By default, global link flapping protection is enabled and the system detects link flaps on all interfaces. If the number of link flaps on an interface reaches the threshold within the link flapping detection period, the system automatically shuts down this interface and records the interface status as **LINK-FLAP DOWN**. That is, the interface goes Down due to link flapping protection. By default, the link flapping detection period is 10 seconds, the threshold for the number of link flaps is 5, and the automatic recovery period is 60 seconds. If an interface alternates between Up and Down five times within 10 seconds, the interface goes Down. After 60 seconds, the interface automatically goes Up. To set the link flapping detection period, run the **port link-flap auto-detect interval** command. To set the threshold for the number of link flaps, run the **port link-flap auto-detect threshold** command. To set the automatic recovery period, run the **port link-flap auto-detect recovery interval** command.

Precautions

- To check whether a link flap occurs on a specified interface, run the **port link-flap protection enable** command on this interface to enable link flapping protection. The link flapping protection function on an interface and the global link flapping protection function are mutually exclusive.
- If link flapping protection is enabled on an interface, global link flapping protection does not take effect on this interface.
- If an interface is set to Down due to link flapping protection, enabling link flapping protection on this interface will restore the interface to Up.
- Stack interfaces do not support link flapping protection.

Example

Disable global link flapping protection.

```
<HUAWEI> system-view
[HUAWEI] port link-flap auto-detect protection disable
```

4.2.57 port link-flap auto-detect interval

Function

The **port link-flap auto-detect interval** command sets the global link flapping detection period.

The **undo port link-flap auto-detect interval** command restores the default global link flapping detection period.

By default, the global link flapping detection period is 10s.

Format

port link-flap auto-detect interval *interval-value*

undo port link-flap auto-detect interval

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the global link flapping detection period.	The value is an integer that ranges from 5 to 600, in seconds. The default value is 10s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the number of link flaps on an interface reaches the threshold within the link flapping detection period, the system automatically shuts down this interface and records the interface status as **LINK-FLAP DOWN**. That is, the interface goes Down due to link flapping protection. By default, the link flapping detection period is 10 seconds, the threshold for the number of link flaps is 5, and the automatic recovery period is 60 seconds. If an interface alternates between Up and Down five times within 10 seconds, the interface goes Down. After 60 seconds, the interface automatically goes Up.

If high network reliability is required, you can run this command to shorten the detection period to quickly detect network flapping. Otherwise, you can increase the detection period.

Example

Set the global link flapping detection period to 50s.

```
<HUAWEI> system-view
[HUAWEI] port link-flap auto-detect interval 50
```

4.2.58 port link-flap auto-detect threshold

Function

The **port link-flap auto-detect threshold** command sets the global threshold for the number of link flaps within a specified period.

The **undo port link-flap auto-detect threshold** command restores the default global threshold for the number of link flaps within a specified period.

By default, the global threshold for the number of link flaps within a specified period is 5.

Format

port link-flap auto-detect threshold *threshold-value*

undo port link-flap auto-detect threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the threshold for the number of link flaps within a specified period.	The value is an integer in the range from 1 to 10. The default value is 5.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the number of link flaps on an interface reaches the threshold within the link flapping detection period, the system automatically shuts down this interface and records the interface status as **LINK-FLAP DOWN**. That is, the interface goes Down due to link flapping protection. By default, the link flapping detection period is 10 seconds, the threshold for the number of link flaps is 5, and the automatic recovery period is 60 seconds. If an interface alternates between Up and Down five times within 10 seconds, the interface goes Down. After 60 seconds, the interface automatically goes Up.

If high network reliability is required, you can run this command to reduce the threshold for the number of link flaps to quickly detect network flapping. Otherwise, you can increase the threshold for the number of link flaps.

Example

Set the threshold for the number of link flaps within a specified period to 5.

```
<HUAWEI> system-view
[HUAWEI] port link-flap auto-detect threshold 5
```

4.2.59 port link-flap auto-detect recovery interval

Function

The **port link-flap auto-detect recovery interval** command sets the automatic recovery period after interfaces go Down due to global link flapping protection.

The **undo port link-flap auto-detect recovery interval** command restores the default automatic recovery period after interfaces go Down due to global link flapping protection.

By default, the automatic recovery period after interfaces go Down due to global link flapping protection is 60 seconds.

Format

port link-flap auto-detect recovery interval *interval-value*

undo port link-flap auto-detect recovery interval

Parameters

Parameter	Description	Value
interval-value	Specifies the automatic recovery period after interfaces go Down due to global link flapping protection.	The value is an integer that ranges from 60 to 86400, seconds. The default value is 60 seconds, and the increment value is 60 seconds. That is, the value must be a multiple of 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the number of link flaps on an interface reaches the threshold within the link flapping detection period, the system automatically shuts down this interface and records the interface status as **LINK-FLAP DOWN**. That is, the interface goes Down due to link flapping protection. By default, the link flapping detection period is 10 seconds, the threshold for the number of link flaps is 5, and the automatic recovery period is 60 seconds. If an interface alternates between Up and Down five times within 10 seconds, the interface goes Down. After 60 seconds, the interface automatically goes Up. To set the automatic recovery period after interfaces go Down due to global link flapping protection, run the **port link-flap auto-detect recovery interval** command.

Example

Set the automatic recovery period after interfaces go Down due to global link flapping protection to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] port link-flap auto-detect recovery interval 120
```

4.2.60 port link-flap interval

Function

The **port link-flap interval** command sets the link flapping detection interval.

The **undo port link-flap interval** command restores the default link flapping detection interval.

By default, the link flapping detection interval is 10s.

Format

port link-flap interval *interval-value*

undo port link-flap interval

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the link flapping detection interval.	The value is an integer that ranges from 5 to 600, in seconds. The default value is 10s.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A link flap occurs when the physical status of an interface frequently alternates between Up and Down due to network flapping or network cable faults. This causes frequent network topology changes and affects user communication. For example, two links work in primary/backup mode. If the interface of the primary link experiences frequent Up/Down transitions, flows are switched between the primary and backup links. Frequent service switchovers increase load of the device and may result in service data loss.

Link flapping protection can solve the problem. To be specific, you can configure link flapping protection globally or on a specified interface. This function disables interfaces that frequently alternate between Up and Down so that the interfaces become Down. This prevents the network topology from changing frequently. When the system detects frequent physical status changes on the interface of the primary link, the system directly disables the interface to trigger a primary/backup link switchover. The backup link then steadily transmits services. The link flapping protection function involves the following parameters:

- Number of link flaps: A link flap refers to an interface Up/Down transition.
- Link flapping detection period: It is a period during which the system counts the number of link flaps.

If the number of link flaps on an interface reaches the threshold within a link flapping detection period, the system disables the interface and records its status as **ERROR DOWN(link-flap)** when link flapping protection is configured on this interface or records its status as **LINK-FLAP DOWN** when link flapping protection is configured globally. By default, after link flapping protection is enabled, an interface goes Down if its status changes five times within 10 seconds.

Prerequisites

The configured interval takes effect only after link flapping protection is enabled using the **port link-flap protection enable** command on the interface.

Precautions

If you run the **port link-flap interval** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the link flapping detection interval to 50s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-flap interval 50
```

4.2.61 port link-flap protection enable

Function

The **port link-flap protection enable** command enables link flapping protection on an interface.

The **undo port link-flap protection enable** command disables link flapping protection on an interface.

By default, link flapping protection is disabled on an interface.

Format

port link-flap protection enable

undo port link-flap protection enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A link flap occurs when the physical status of an interface frequently alternates between Up and Down due to network flapping or network cable faults. This causes frequent network topology changes and affects user communication. For example, two links work in primary/backup mode. If the interface of the primary link experiences frequent Up/Down transitions, flows are switched between the primary and backup links. Frequent service switchovers increase load of the device and may result in service data loss.

Link flapping protection can solve the problem. To be specific, you can configure link flapping protection globally or on a specified interface. This function disables interfaces that frequently alternate between Up and Down so that the interfaces become Down. This prevents the network topology from changing frequently. When the system detects frequent physical status changes on the interface of the primary link, the system directly disables the interface to trigger a primary/backup link switchover. The backup link then steadily transmits services. The link flapping protection function involves the following parameters:

- Number of link flaps: A link flap refers to an interface Up/Down transition.
- Link flapping detection period: It is a period during which the system counts the number of link flaps.

If the number of link flaps on an interface reaches the threshold within a link flapping detection period, the system disables the interface and records its status as **ERROR DOWN(link-flap)** when link flapping protection is configured on this interface or records its status as **LINK-FLAP DOWN** when link flapping protection is configured globally. By default, after link flapping protection is enabled, an interface goes Down if its status changes five times within 10 seconds.

Follow-up Procedure

- Run the **port link-flap interval** *interval-value* command to set the link flapping interval for the interface.
- Run the **port link-flap threshold** *threshold-value* command to set the number of link flappings for the interface.
- An interface in **ERROR DOWN(link-flap)** state can be recovered using either of the following methods:
  - Manual recovery. If a few interfaces need to be recovered forcibly, run the **shutdown** and **undo shutdown** commands in sequence in the interface view. Alternatively, run the **restart** command in the interface view to restart the interface.

– Automatic recovery. If a large number of interfaces need to be recovered, manual recovery is time consuming and error prone. Instead, you can run the **error-down auto-recovery cause link-flap interval** *interval-value* command in the system view to enable automatic interface recovery and set the automatic recovery delay. Interfaces in Error-Down state then automatically recover after the specified delay expires.

Example

Enable link flapping protection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-flap protection enable
```

4.2.62 port link-flap threshold

Function

The **port link-flap threshold** command sets the maximum number of link flapping events on an interface.

The **undo port link-flap threshold** command restores the default maximum number of link flapping events on an interface.

By default, the maximum number of link flapping events is 5.

Format

port link-flap threshold *threshold-value*

undo port link-flap threshold

Parameters

Parameter	Description	Value
threshold *threshold-value*	Specifies the maximum number of link flapping events on an interface.	The value is an integer that ranges from 1 to 10. The default value is 5.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A link flap occurs when the physical status of an interface frequently alternates between Up and Down due to network flapping or network cable faults. This causes frequent network topology changes and affects user communication. For example, two links work in primary/backup mode. If the interface of the primary link experiences frequent Up/Down transitions, flows are switched between the primary and backup links. Frequent service switchovers increase load of the device and may result in service data loss.

Link flapping protection can solve the problem. To be specific, you can configure link flapping protection globally or on a specified interface. This function disables interfaces that frequently alternate between Up and Down so that the interfaces become Down. This prevents the network topology from changing frequently. When the system detects frequent physical status changes on the interface of the primary link, the system directly disables the interface to trigger a primary/backup link switchover. The backup link then steadily transmits services. The link flapping protection function involves the following parameters:

- Number of link flaps: A link flap refers to an interface Up/Down transition.
- Link flapping detection period: It is a period during which the system counts the number of link flaps.

If the number of link flaps on an interface reaches the threshold within a link flapping detection period, the system disables the interface and records its status as **ERROR DOWN(link-flap)** when link flapping protection is configured on this interface or records its status as **LINK-FLAP DOWN** when link flapping protection is configured globally. By default, after link flapping protection is enabled, an interface goes Down if its status changes five times within 10 seconds.

Prerequisites

The **port link-flap threshold** command configuration takes effect only after link flapping protection is enabled using the **port link-flap protection enable** command on the interface.

Precautions

If you run the **port link-flap threshold** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the maximum number of link flapping events on GE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-flap threshold 10
```

4.2.63 port-group

Function

The **port-group** command creates a permanent port group and displays the permanent port group view.

The **undo port-group** command deletes permanent port groups.

By default, no permanent port group is configured.

Format

port-group *port-group-name*

undo port-group { **all** | *port-group-name* }

Parameters

Parameter	Description	Value
port-group-name	Specifies the name of a permanent interface group. The value cannot conflict with the group-member keyword. For example, the name cannot be g, gr, or group-m.	The value is a string of 1 to 32 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** A permanent port group cannot be named **all**. Meanwhile, to avoid a usage conflict between the **port-group group-member** command and *port-group-name*, do not specify g, group-member, or first letters of group-member as the name of a permanent interface group.
all	Deletes all port groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Two types of port groups are available:

- Temporary port group: To temporarily deliver a configuration to multiple interfaces, you can create a temporary port group. After you deliver the configuration and exit from the port group view, the system automatically deletes the temporary port group.
- Permanent port group: To deliver configurations to interfaces multiple times, you can create a permanent port group. After you exit from the port group view, the port group and member interfaces in the group still exist, facilitating subsequent batch configuration for the member interfaces. To delete a permanent port group, run the **undo port-group** { **all** | *port-group-name* } command.

Follow-up Procedure

Run the **group-member** command to add Ethernet interfaces to the created permanent port group.

Precautions

- The system supports a maximum of 32 permanent port groups and each port group supports a maximum of 48 member interfaces.
- Deleting a permanent port group will not clear the configurations of an interface in the port group.

Example

Create port group **portgroup1** and enter the port group view.

```
<HUAWEI> system-view
[HUAWEI] port-group portgroup1
[HUAWEI-port-group-portgroup1]
```

4.2.64 port-group group-member

Function

The **port-group group-member** command creates a temporary port group and adds specified Ethernet interfaces to the temporary port group. Commands configured for a temporary port group will be automatically run on all member interfaces.

By default, no temporary port group is created.

Format

port-group group-member { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	The value of *interface-number2* must be larger than the value of *interface-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same operations on multiple Ethernet interfaces, configuring each interface one by one easily causes incorrect configurations and is labor-intensive.

The port group function easily solves the problem. You can add all the Ethernet interfaces to the same port group. After you run a configuration command once in the port group view, the configuration takes effect on all the Ethernet interfaces in the port group, reducing the configuration workload.

Two types of port groups are available:

- Temporary port group: To temporarily deliver a configuration to multiple interfaces, you can create a temporary port group. After you deliver the configuration and exit from the port group view, the system automatically deletes the temporary port group.
- Permanent port group: To deliver configurations to interfaces multiple times, you can create a permanent port group. After you exit from the port group view, the port group and member interfaces in the group still exist, facilitating subsequent batch configuration for the member interfaces. To delete a permanent port group, run the **undo port-group** { **all** | *port-group-name* } command.

Configuration Impact

If the **port-group group-member** command is run more than once, all configurations take effect.

Precautions

- The **port-group group-member** command is equivalent to the **group-member** command executed in the permanent port group view. Multiple interfaces can be added to a permanent port group in batches using the **group-member** command.

- When you specify the keyword **to** in the **port-group group-member** command:
  - The interfaces specified by *interface-number1* and *interface-number2* must reside on the same member switch. To add contiguous interfaces on different member switches to the same port group, run this command several times or use the keyword **to** several times.
  - The interfaces specified by *interface-number1* and *interface-number2* must be of the same type, for example, both of the interfaces are GE interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not specified, the preceding limitations do not apply.
  - Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Add GE0/0/1, GE0/0/2, and GE0/0/3 to a temporary port group.

```
<HUAWEI> system-view
[HUAWEI] port-group group-member gigabitethernet 0/0/1 to gigabitethernet 0/0/3
[HUAWEI-port-group]
```

4.2.65 port-isolate enable

Function

The **port-isolate enable** command enables port isolation.

The **undo port-isolate enable** command disables port isolation.

By default, port isolation is disabled.

Format

port-isolate enable [**group** *group-id*]

undo port-isolate enable [**group** *group-id*]

Parameters

Parameter	Description	Value
group *group-id*	Specifies the ID of a port isolation group.	The value is an integer that ranges from 1 to 64.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view, , port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement Layer 2 isolation between interfaces, add different interfaces to different VLANs. This, however, wastes VLAN resources. To save VLAN resources, enable port isolation to isolate interfaces in a VLAN. That is, you can add interfaces to a port isolation group to implement Layer 2 isolation between these interfaces. Port isolation provides secure and flexible networking schemes for customers.

Precautions

- After port isolation is configured, ports are isolated at Layer 2 but can communicate at Layer 3 by default. To configure both Layer 2 isolation and Layer 3 isolation, run the **port-isolate mode all** command.
- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate. If *group-id* is not specified, interfaces are added to port isolation group 1 by default.
- There is no limit on the number of members in a port isolation group on the S200, and S1730S-S1. The maximum number of members in a port isolation group on other switch models is 512.
- In the same VLAN, if the **mac-address learning disable** command is run to disable MAC address learning and traffic is forwarded in broadcast mode, the device first copies the traffic received on the inbound interface before checking whether port isolation is configured, though port isolation has been configured. When the copied traffic exceeds the chip performance, the device discards the traffic, resulting in packet loss in forwarding.

Example

Enable port isolation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-isolate enable group 1
```

4.2.66 port-isolate exclude vlan

Function

The **port-isolate exclude vlan** command excludes a VLAN where port isolation needs to be disabled.

The **undo port-isolate exclude vlan** command cancels the configuration.

By default, no VLAN is excluded when port isolation is configured.

Format

port-isolate exclude vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port-isolate exclude vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
vlan-id2	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
vlan-id1 **to** *vlan-id2*	Specifies VLAN IDs in a batch. ● *vlan-id1* specifies the first VLAN ID. ● *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than *vlan-id1*. *vlan-id1* and *vlan-id2* determine a VLAN range. ● If you do not specify **to** *vlan-id2*, only one VLAN is specified.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable communication between users in a VLAN where port isolation needs to be disabled, run the **port-isolate exclude vlan** command to exclude the VLAN.

Only SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Example

Exclude VLAN 10 where port isolation needs to be disabled.

```
<HUAWEI> system-view
[HUAWEI] port-isolate exclude vlan 10
```

4.2.67 protect-group member

Function

The **protect-group member** command adds the specified Ethernet interface to an interface protection group.

The **undo protect-group member** command deletes an Ethernet interface from an interface protection group.

By default, no Ethernet interface is added to an interface protection group.

Format

protect-group member *interface-type interface-number* { **master** | **standby** }

undo protect-group member *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be added to an interface protection group.	-
master	Indicates the working interface.	-
standby	Indicates the protected interface.	-

Views

Interface protection group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts are usually connected to an external network through a default gateway. If the outbound interface of the default gateway fails, the hosts cannot communicate with the external network, interrupting normal service transmission and degrading device reliability. The port protection function solves this problem. Without changing the networking, you can add two interfaces on the device to a port protection group to implement interface backup in active/standby mode. When the active interface fails, services are immediately switched to the standby interface, ensuring non-stop service transmission.

Prerequisites

An interface protection group has been created using the **port protect-group** command.

Precautions

An interface protection group contains only a working interface and a protected interface.

Example

Add GigabitEthernet0/0/1 to an interface protection group.

```
<HUAWEI> system-view
[HUAWEI] port protect-group 1
[HUAWEI-protect-group1] protect-group member gigabitethernet 0/0/1 master
```

4.2.68 port mode 2.5ge

Function

The **port mode 2.5ge** command configures an interface to work at the rate of 2.5 Gbit/s.

The **undo port mode** command restores the default interface rate.

By default, the rate of a GE interface is 1 Gbit/s, and the rate of an XGE interface is 10 Gbit/s.

NOTE

Only the following interfaces on the following models can be configured to work at the rate of 2.5 Gbit/s:

- S5731-S32ST4X, S5731-S32ST4X-A, S5731-S32ST4X-D, S5731S-S32ST4X-A, and S5731S-S32ST4X-A1: 24 downlink GE interfaces
- S5731-S48S4X, S5731-S48S4X-A, S5731S-S48T4X-A, and S5731S-S48T4X-A1: 44 GE interfaces numbered 5 to 48
- S5731-H24HB4XZ and S5731S-H24HB4XZ-A: first 20 downlink GE interfaces and four downlink 10GE interfaces
- S5731-H48HB4XZ and S5731S-H48HB4XZ-A: 28 GE interfaces numbered 1 to 8 and 25 to 44 and four downlink 10GE interfaces

Format

port mode 2.5ge

undo port mode

Parameters

None

Views

GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

GE and XGE interfaces can work at the rate of 2.5 Gbit/s. You can run this command to change the rate of a GE or XGE interface based on networking and bandwidth requirements. After the change, replace the transmission medium to enable the interface to work at the corresponding rate.

The rate of interfaces is changed by group. Every four interfaces form a group. If the rate of any interface in the group is changed, the rate of other interfaces in the same group is changed to be the same. For GE interfaces, the four interfaces in the same group work at the same rate (either all 1 Gbit/s or all 2.5 Gbit/s). For XGE interfaces, the following situations exist: The four interfaces in the same group work at the same rate (all 2.5 Gbit/s, all 1 Gbit/s, or all 10 Gbit/s). The four interfaces in the same group work at different rates, that is, some interfaces work at the rate of 1 Gbit/s, while other interfaces work at the rate of 10 Gbit/s.

Precautions

- After an interface is configured to work at the rate of 2.5 Gbit/s, the interface cannot be configured to work in auto-negotiation mode, and does not support single-fiber communication, MACsec, training, FEC, 100M optical modules, GE optical modules, or optical-to-electrical conversion modules.
- After an interface is configured to work at the rate of 2.5 Gbit/s, it cannot be configured as a stack interface. Similarly, after an interface is configured as a stack interface, it cannot be configured to work at the rate of 2.5 Gbit/s.
- For the S5731-H24HB4XZ, S5731-H48HB4XZ, S5731S-H24HB4XZ-A, and S5731S-H48HB4XZ-A, if the interface rate is changed to 2.5 Gbit/s after a subcard is installed, the subcard becomes unavailable due to insufficient bandwidth. You need to confirm the operation as prompted before changing the interface rate.

Example

Configure a GE interface to work at the rate of 2.5 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] interface ge 0/0/3
[HUAWEI-GigabitEthernet0/0/3] port mode 2.5ge
Warning: The interface(s)(GigabitEthernet0/0/1, GigabitEthernet0/0/2, GigabitEthernet0/0/3,
GigabitEthernet0/0/4) will be converted to 2.5GE mode, Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.....done.
```

4.2.69 port mode ge (25GE interface)

Function

The **port mode ge** command configures a 25GE interface to work at the rate of 1 Gbit/s.

The **undo port mode** command restores the rate of a 25GE interface to 25 Gbit/s.

By default, when a 25GE medium is installed on a 25GE interface, the interface works at the rate of 25 Gbit/s; when an XGE medium is installed on a 25GE interface, the interface works at the rate of 10 Gbit/s; when a GE medium is installed on a 25GE interface, the interface cannot go Up.

NOTE

This command is supported by the following: S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), S5732-H48XUM2CC, S6730-H28Y4C, S6730-H24X4Y4C and S7Y08000 card.

This command is supported when the interface working mode on the S7X08000 or S7X0800K0 card is set to 25GE using the **set card port-config-mode 25g-port enable** command.

Format

port mode ge

undo port mode

Parameters

None

Views

25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 25GE interface can work at the rate of 1 Gbit/s. You can configure the rate as required and replace the transmission medium.

When a 25GE interface is configured to work at the rate of 1 Gbit/s, all interfaces in the interface group to which the 25GE interface belongs are configured to work at the rate of 1 Gbit/s.

- For the S6730-H28Y4C, each group of interfaces numbered 1 to 4, 5 to 8, 9 to 16, 17 to 20, 21 to 24, or 25 to 28 belong to the same interface group.
- Interfaces numbered 1 and 2 on the S7X08000 or S7X0800K0 card belong to the same interface group.
- For the S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), S5732-H48XUM2CC, S6730-H24X4Y4C and S7Y08000 card, each group of interfaces numbered 1 to 4, 5 to 8, or 9 to 12 belong to the same interface group.

Precautions

- Configure the remote interface to work at the same rate as that of the local interface.
- Ensure that all interfaces in the interface group in which the interface rate is to be changed are in Down status before running this command. If the status of an interface is Up, run the **shutdown** command on the interface and then change the interface rate.
- After the **port mode ge** command is run on an interface, if any interface in the same interface group as that interface is Up, the command configuration will not be cleared after the **clear configuration this** or **clear configuration interface** command is run. If all the interfaces in the interface group are Down, the command configuration will be cleared after the **clear configuration this** or **clear configuration interface** command is run.
- 25GE interfaces split from other interfaces cannot work at the rate of 1 Gbit/s.

Example

Configure a 25GE interface to work at the rate of 1 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] interface 25ge 0/1/1
[HUAWEI-25GE0/1/1] port mode ge
Warning:The interface(s)(25GE0/1/1,25GE0/1/2) will be converted to GE mode.[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment....done.
```

4.2.70 port-isolate mode

Function

The **port-isolate mode** command sets the port isolation mode.

The **undo port-isolate mode** command restores the default port isolation mode.

By default, ports are isolated at Layer 2 but can communicate at Layer 3.

Format

port-isolate mode { **l2** | **all** }

undo port-isolate mode

Parameters

Parameter	Description	Value
l2	Indicates that ports are isolated at Layer 2 but can communicate at Layer 3.	-
all	Indicates that ports are isolated at both Layer 2 and Layer 3.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement Layer 2 isolation between interfaces, you can add different interfaces to different VLANs. This wastes VLAN resources. Port isolation can isolate interfaces in the same VLAN. That is, you only need to add interfaces to a port isolation group to implement Layer 2 isolation between these interfaces. Port isolation provides secure and flexible networking schemes.

You can configure the interface isolation mode to **all** to implement Layer 2 and Layer 3 isolation between interfaces in a port isolation group.

NOTE

The S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI support isolation at Layer 2 and interworking at Layer 3, and do not support this command.

Example

Configure Layer 2 isolation and Layer 3 communication.

```
<HUAWEI> system-view
[HUAWEI] port-isolate mode l2
```

4.2.71 port media type (GE interface view)

Function

The **port media type** command determines whether an interface configuration item belongs to an optical or electrical interface.

The **undo port media type** command restores the default settings.

Format

port media type { **copper** | **fiber** }

undo port media type { **copper** | **fiber** }

Parameters

Parameter	Description	Value
copper	Determines that the interface configuration item belongs to a combo interface or GE interface that is equipped with a copper module and works as an electrical interface.	-
fiber	Determines that the interface configuration item belongs to a combo interface or GE interface that is equipped with a copper module and works as an optical interface.	-

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

This command only distinguishes optical interface configuration and electrical interface configuration, and is not configurable.

If you have specified the interface attributes (such as auto-negotiation, speed, and full-duplex mode) on a combo interface, the system automatically generates this command to determine whether an interface configuration item belongs to the optical interface or electrical interface. After this command is generated, the configuration for the other interface type (such as optical interface) will not be lost if the combo interface works as an electrical interface.

For example, after you run the **display this** command on a combo interface, the interface configuration is as follows:

```
#
interface GigabitEthernet0/0/1
 port media type copper
  undo negotiation auto
  speed 100
 port media type fiber
  undo negotiation auto
#
```

The command output shows that there are two configuration items **undo negotiation auto** and **speed 100** when the combo interface works as an electrical interface and one configuration item **undo negotiation auto** when the combo interface works as an optical interface.

Example

None

4.2.72 port media type (XGE interface view)

Function

The **port media type** command determines whether an interface configuration item belongs to the optical or electrical interface.

The **undo port media type** command restores the default settings.

Format

port media type { **copper** | **fiber** }

undo port media type { **copper** | **fiber** }

Parameters

Parameter	Description	Value
copper	Determines the interface configuration item belongs to an XGE interface that is equipped with a copper module and works as an electrical interface.	-

Parameter	Description	Value
fiber	Determines the interface configuration item belongs to an XGE interface that is equipped with a copper module and works as an optical interface.	-

Views

XGE interface view

Default Level

2: Configuration level

Usage Guidelines

This command cannot be manually configured and belongs to internal implementation commands. This command only distinguishes optical interface configuration and electrical interface configuration, and is not configurable.

If you have installed a copper module on an XGE interface and specified the interface attributes (such as auto-negotiation, speed, and full-duplex mode), the system automatically generates this command to determine whether an interface configuration item belongs to the optical or electrical interface.

For example, after you run the **display this** command on an XGE interface, the interface configuration is as follows:

```
#
interface XGigabitEthernet0/0/1
 port media type copper
  mdi across
 port media type fiber
  als enable
#
```

The command output indicates that there is one configuration item **mdi across** when the XGE interface works as an electrical interface and one configuration item **als enable** when the XGE interface works as an optical interface.

Example

None

4.2.73 port media type (25GE interface view)

Function

The **port media type** command determines whether an interface configuration item belongs to an optical or electrical interface.

The **undo port media type** command restores the default settings.

Format

port media type { **copper** | **fiber** }

undo port media type { **copper** | **fiber** }

Parameters

Parameter	Description	Value
copper	Determines the interface configuration item belongs to a 25GE interface that is equipped with a GE copper module and works as an electrical interface.	-
fiber	Determines the interface configuration item belongs to a 25GE interface that is equipped with a GE copper module and works as an optical interface.	-

Views

25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command only distinguishes optical interface configuration and electrical interface configuration, and is not configurable.

If you have run the **port mode ge** command to configure a 25GE interface to work at the rate of 1 Gbit/s, installed a GE copper module on the 25GE interface, and specified the interface attributes (such as auto-negotiation and MDI type) for the 25GE interface, the system automatically generates this command to determine whether an interface configuration item belongs to the optical or electrical interface.

For example, after you run the **display this** command on a 25GE interface, the interface configuration is as follows:

```
#
interface 25GigabitEthernet0/0/1
 port media type copper
  mdi across
 port media type fiber
  als enable
#
```

The command output indicates that there is one configuration item **mdi across** when the 25GE interface works as an electrical interface and one configuration item **als enable** when the 25GE interface works as an optical interface.

Example

None

4.2.74 port protect-group

Function

The **port protect-group** command creates an interface protection group and enters the interface protection group view.

The **undo port protect-group** command deletes the created interface protection group.

By default, no interface protection group is created.

Format

port protect-group *protect-group-index*

undo port protect-group *protect-group-index*

Parameters

Parameter	Description	Value
protect-group-index	Specifies the ID of an interface protection group.	The value is an integer that ranges from 0 to 63.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts are usually connected to an external network through a default gateway. If the outbound interface of the default gateway fails, the hosts cannot communicate with the external network, interrupting normal service transmission and degrading device reliability. The port protection function solves this problem. Without changing the networking, you can add two interfaces on the device to a port protection group to implement interface backup in active/standby mode. When the active interface fails, services are immediately switched to the standby interface, ensuring non-stop service transmission.

Follow-up Procedure

Run the **protect-group member** command to add the specified Ethernet interface to an interface protection group.

Example

Create an interface protection group.

```
<HUAWEI> system-view
[HUAWEI] port protect-group 1
```

4.2.75 port split

Function

The **port split** command splits a specified interface.

The **undo port split** command cancels the split configuration on an interface.

By default, an interface is not split.

NOTE

Only interfaces on the panel of the S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A support interface split and merge.

For the devices that have the S7C02000 or S7Q02001 card installed, interfaces on the card support interface split and merge.

Format

40GE interfaces on the device panel or card

port split split-type 40GE:4*XGE

100GE interfaces on the device panel or card

port split split-type 100GE:4*25GE

10GE and 25GE interfaces split from other interfaces

undo port split

Parameters

Parameter	Description	Value
40GE:4*XGE	Splits a specified 40GE interface into four 10GE interfaces.	-
100GE:4*25GE	Splits a specified 100GE interface into four 25GE interfaces.	-

Views

XGE interface view, 40GE interface view25GE interface view, 100GE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To split an interface, run the **port split split-type** command in the view of the interface. To merge converted interfaces into the original interface, run the **undo port split** command in the view of only one of the converted interfaces.

Precautions

- After configuring interface split using the **port split split-type** command, restart the interface card to make the configuration take effect.
- If interface split or merge is configured on an interface, the original configuration on the interface is lost. Therefore, exercise caution when deciding to perform the interface split or merge operation.
- 10GE interfaces converted from a 40GE interface are numbered based on the number of the last 10GE interface on the switch. For interfaces on the switch panel, if the last 10GE interface is numbered XGE 0/y/m and a 40GE interface to be split is numbered 40GE 0/y/n, the four 10GE interfaces converted from the 40GE interface are numbered XGE 0/y/(m + 4 * (n - 1) + z + 1). For example, if the last 10GE interface on a switch is numbered XGE 0/0/48, the four 10GE interfaces converted from 40GE 0/0/3 are numbered XGE 0/0/57, XGE 0/0/58, XGE 0/0/59, and XGE 0/0/60. For interfaces on a card, m has a fixed value of 0. For example, the four 10GE interfaces converted from 40GE 1/1/1 on a card are numbered XGE 1/1/1, XGE 1/1/2, XGE 1/1/3, and XGE 1/1/4.
  - y: indicates the subcard number.
  - m: indicates the sequence number of the last 10GE interface on the switch.
  - n: indicates the sequence number of the 40GE interface.
  - z: indicates the interface location. The value ranges from 0 to 3.
- 25GE interfaces converted from a 100GE interface are numbered based on the number of the last 25GE interface on the switch. Because only the 100GE interfaces on cards support interface split, if a 100GE interface to be split is

numbered 100GE 0/y/n, the four 25GE interfaces converted from the 100GE interface are numbered 25GE 0/y/(4 * (n - 1) + z + 1). For example, the four 25GE interfaces converted from 100GE 0/1/1 on a card are numbered 25GE 0/1/1, 25GE 0/1/2, 25GE 0/1/3, and 25GE 0/1/4.

  - y: indicates the subcard number.
  - m: indicates the sequence number of the last 10GE interface on the switch.
  - n: indicates the sequence number of the 40GE interface.
  - z: indicates the interface location. The value ranges from 0 to 3.

NOTE

Split interfaces are numbered in the same sequence as the wires of a cable are numbered. For example, in a 1-to-4 cable, the wire numbered 1 corresponds to the interface with the lowest interface number, and the wire numbered 4 corresponds to the interface with the highest interface number.

- After interface split is configured, the interface and converted interfaces cannot be added to a stack interface, regardless of whether the configuration takes effect. If an interface has been added to a stack interface, the interface cannot be split.
- After configuring interface split using the **port split split-type 40GE:4*XGE** command, or using the **undo port split** command, restart the device to make the configuration take effect. You can run the **display port split** command in any view to check the status of a split interface.

Example

Split a 40GE interface into four 10GE interfaces and restart the device to make the configuration take effect.

```
<HUAWEI> system-view
[HUAWEI] interface 40GE 0/0/1
[HUAWEI-40GE0/0/1] port split split-type 40GE:4*XGE
Warning: This command will take effect only after resetting the board. 40GE0/0/1 will be split up into XGE,
and the port configuration will be lost when the port type is changed. Continue? [Y/N]:y
Info: Succeeded in setting the configuration.
[HUAWEI-40GE0/0/1] return
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-configuration
file flash:/device.cfg. Continue? [Y/N]:y
Now saving the current configuration to the slot 0.
Save the configuration successfully.
Info: If want to reboot with saving diagnostic information, input 'N' and then execute 'reboot save
diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

4.2.76 port serdes-mode

Function

The **port serdes-mode** command configures the Serdes mode of a MultiGE interface.

The **undo port serdes-mode** command restores the default Serdes mode of a MultiGE interface.

By default, a MultiGE interface can work in 1G or 10G Serdes mode.

NOTE

This command is supported only on the following switch models:

S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002), S5732-H48XUM2CC (excluding MultiGE interfaces numbered 9 to 12)

Format

port serdes-mode { **2500-base-x** | **5000-base-x** } { **sgmii** | **xfi** }

port serdes-mode sgmii xfi

undo port serdes-mode

Parameters

Parameter	Description	Value
2500-base-x	Configures an interface to work in 2.5G Serdes mode.	-
5000-base-x	Configures an interface to work in 5G Serdes mode.	-
sgmii	Configures an interface to work in 1G Serdes mode.	-
xfi	Configures an interface to work in 10G Serdes mode.	-

Views

MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, when a MultiGE interface works at the rate of 2.5 Gbit/s or 5 Gbit/s, the Serdes mode of the MultiGE interface is 10G. When a Huawei device is connected to a non-Huawei device, if the preamble of packets sent from the non-Huawei device is not fixed, the MultiGE interface connecting the Huawei device to the non-Huawei device discards the packets. To prevent this problem, when a

Huawei device connects to a non-Huawei device and receives the ENTITYTRAP_1.3.6.1.4.1.2011.5.25.219.2.2.3 hwBoardFail alarm with EntityTrapFaultID being 132282, run the **port serdes-mode** command to change the Serdes mode of the MultiGE interface to 2.5G or 5G based on the alarm information.

When a Huawei device connects to a non-Huawei device, the MultiGE interface connecting the Huawei device to the non-Huawei device cannot go Up if its Serdes mode is different from that on the non-Huawei device. To prevent this problem, when a Huawei device connects to a non-Huawei device and receives the ENTITYTRAP_1.3.6.1.4.1.2011.5.25.219.2.2.3 hwBoardFail alarm with EntityTrapFaultID being 132283, run the **port serdes-mode** command to change the Serdes mode of the MultiGE interface to be the same as that on the non-Huawei device based on the alarm information.

Precautions

MultiGE interfaces of different devices can be split into separate interface groups based on rules. MultiGE interfaces in each interface group support only two Serdes modes.

- On the S5732-H24UM2CC (part number: 02353HUC), each group of MultiGE interfaces 1 to 8, 9 to 16, and 17 to 24 forms an interface group.
- On the S5732-H24UM2CC (part number: 02353HUC), each group of MultiGE interfaces 1 to 8, 9 to 16, 17 to 24, 25 to 32, 33 to 36, 37 to 40, 41 to 44, and 45 to 48 forms an interface group.
- On the S5732-H48XUM2CC, each group of MultiGE interfaces 1 to 8, 13 to 20, and 21 to 24 forms an interface group.

Example

Configure a MultiGE interface to work in 2.5G or 10G Serdes mode.

```
<HUAWEI> system-view
[HUAWEI] interface MultiGE 0/0/1
[HUAWEI-MultiGE0/0/1] port serdes-mode 2500-base-x xfi
```

4.2.77 portswitch

Function

The **portswitch** command changes the working mode of Ethernet interfaces from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

Format

portswitch

undo portswitch

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an Ethernet interface on the device works in Layer 2 mode. To enable Layer 3 functions on the interface, run the **undo portswitch** command on the interface.

Precautions

- If an interface has the non-attribute configuration, this command cannot be executed. Before running this command, delete the non-attribute configuration on the interface.
- The minimum interval between running the **portswitch** and **undo portswitch** commands must be 30s.

NOTE

Only interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

Ethernet interfaces working at Layer 3 support IP address configuration.

By default, Ethernet interfaces on the device work at Layer 2 mode and have been added to VLAN 1. You can run the **undo portswitch** command to change the working mode to Layer 3 mode. The Ethernet interfaces are removed from VLAN 1 only after Layer 3 protocols become Up.

Example

Change the working mode of GE0/0/1 from Layer 2 mode to Layer 3 mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 255.255.255.0
```

4.2.78 portswitch batch

Function

The **portswitch batch** command changes the working mode of Ethernet interfaces from Layer 3 mode to Layer 2 mode in batches.

The **undo portswitch batch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode in batches.

By default, the working mode of the interface is Layer 2 mode.

Format

portswitch batch *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

undo portswitch batch *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type *interface-number1* [**to** *interface-number2*]	Specifies interfaces of which the working mode needs to be changed. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. ● If **to** *interface-number2* is not specified, only the working mode of the interface specified by *interface-number1* is changed. **NOTE** You can specify a maximum of 10 interface number ranges at a time. The entered ranges cannot overlap.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **portswitch batch** or **undo portswitch batch** command to change the working mode of interfaces in batches.

Precautions

- The mode switching function takes effect when the interface only has attribute configurations (for example, **shutdown** and **description** configurations). If the service configuration (for example, **port link-type access** configuration) exists on the interface, you must clear the service configuration before running this command.

- The minimum interval between running the **portswitch batch** and **undo portswitch batch** commands must be 30s.

NOTE

Only interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

Ethernet interfaces working at Layer 3 support IP address configuration.

Example

Change the working mode of GE0/0/1, 0/0/2, and 0/0/3 to Layer 2 mode.

```
<HUAWEI> system-view
[HUAWEI] portswitch batch gigabitethernet 0/0/1 0/0/2 0/0/3
```

4.2.79 reset statistics-peak

Function

The **reset statistics-peak** command clears Peak Information Rate (PIR) statistics on an interface.

Format

reset statistics-peak interface *interface-type interface-number*

NOTE

PIR statistics on the management interface cannot be cleared.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears PIR statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the PIR of an interface indicates the maximum rate of the interface in a long time. To check the recent peak rate of an interface, run the **reset statistics-peak** command to clear the previous peak rate record and obtain the new peak rate. To view the peak rate of an interface, run the **display interface** command. The following information is displayed:

```
Input peak rate 244425848 bits/sec,Record time: 2008-01-01 00:16:37
Output peak rate 753496 bits/sec,Record time: 2008-01-15 19:25:12
```

Precautions

PIR statistics on a specified interface cannot be restored after they are cleared. Exercise caution before clearing the statistics.

Example

Clear PIR statistics on GE0/0/1.

```
<HUAWEI> reset statistics-peak interface gigabitethernet 0/0/1
```

4.2.80 reset statistics-peak interface

Function

The **reset statistics-peak interface** command clears peak information rate (PIR) statistics on all the interfaces in one click.

Format

reset statistics-peak interface

NOTE

PIR statistics on management interfaces cannot be cleared.

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the PIR of an interface indicates the maximum rate of the interface in a long time. To check the recent PIR of a specified interface, run the **reset statistics-peak** command to clear the previous PIR statistics and obtain the new PIR. To check recent PIR statistics on multiple or all interfaces, you may need to spend a long time in clearing the PIR statistics, increasing the workload. To reduce the workload, you can run this command in the user view to clear PIR statistics on all the interfaces.

Precautions

PIR statistics on an interface cannot be restored after they are cleared. Exercise caution before clearing the statistics.

Example

Clear PIR statistics on all the interfaces.

```
<HUAWEI> reset statistics-peak interface
```

4.2.81 reset virtual-cable-test

Function

The **reset virtual-cable-test** command deletes cable test results on an interface.

NOTE

The service interfaces on the following devices do not support this command:

- MultiGE interfaces on the S5720-28X-PWH-LI-AC and S5736-S24UM4XC
- XGE electrical interfaces on the ES5D21X08T00 card

Format

reset virtual-cable-test { *interface-type interface-number* | **all** }

Parameters

Parameter	Description	Value
interface-type interface-number	Deletes cable test results on a specified interface. • *interface-type* specifies an interface type. • *interface-number* specifies an interface number.	-
all	Deletes cable test results on all interfaces.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before conducting a cable test on an electrical interface, you can use this command to delete the previous test results.

Precautions

The cable test results cannot be restored after being cleared. Exercise caution before clearing the statistics.

Example

Delete cable test results on GE0/0/1.

```
<HUAWEI> reset virtual-cable-test gigabitethernet 0/0/1
```

4.2.82 set card port-config-mode 25g-port enable

Function

The **set card port-config-mode 25g-port enable** command sets the card interface working mode to 25GE.

The **undo set card port-config-mode 25g-port enable** command restores the default card interface working mode.

By default, the card interface working mode is 10GE.

NOTE

The following switch models support this command when equipped with an S7X08000 card:

- S5731-H24T4XC, S5731-H24P4XC, S5731-H48T4XC, S5731-H48P4XC, S5731-H24HB4XZ, S5731-H48HB4XZ
- S5731S-H24T4XC-A, S5731S-H48T4XC-A, S5731S-H24HB4XZ-A, S5731S-H48HB4XZ-A
- S5736-S
- S5732-H24UM2CC, S5732-H48UM2CC, S5732-H48XUM2CC

Format

set card port-config-mode 25g-port enable slot *slot-id*

undo set card port-config-mode 25g-port enable slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Configures the interface working mode for the card in a specified slot.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the card interface working mode is 10GE, and the number of interfaces is **8*10GE**. To use 25GE interfaces, run the **set card port-config-mode 25g-port enable** command. In this case, the number of interfaces on the card is **2*25GE**, and the last six interfaces are unavailable.

Precautions

- After running this command, you need to confirm the automatic reset of cards as prompted to make the configuration take effect.
- After the interface working mode is changed, replace the connection medium.
- When the interface working mode of a card is being changed, the card cannot be removed and then reinstalled.
- After you run the **reset factory-configuration** command to restore factory settings and restart the device, the card interface working mode is restored to 10GE.
- If there are stack ports on a card, changing the card interface working mode may cause a stack split after the card is reset.

Example

Configure the card interface working mode to 25GE.

```
<HUAWEI> system-view
[HUAWEI] set card port-config-mode 25g-port enable slot 1
Warning: Only the first two ports will be available after the subcard is automatically initialized. Continue?
[Y/N]:y
Warning: The subcard needs to be reset for the new port mode to take effect. Ensure that subcard is
properly installed during re-ini
tialization. Otherwise, port mode switching fails. Continue? [Y/
N]:y
Info: The system is executing the command. Please wait....................................
Info: The port mode is changed successfully.
```

4.2.83 set device port-config-mode enable

Function

The **set device port-config-mode enable** command changes the working mode of SFP28 Ethernet optical ports or MultiGE interfaces on the device panel and changes the working mode of QSFP28 Ethernet optical ports or splits QSFP28 Ethernet optical ports.

The **undo set device port-config-mode enable** command restores the default configuration.

By default, four SFP28 Ethernet optical ports on the panel of the S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002) and S5732-H48XUM2CC work at the rate of 25 Gbit/s, and two QSFP28 Ethernet optical ports work at the rate of 40 Gbit/s. On the panel of the S5731-S8UM16UN2Q and S5731S-S8UM16UN2Q-A, the first 16 MultiGE interfaces work at the rate of 2.5 Gbit/s, the last eight MultiGE interfaces work at the rate of 10 Gbit/s, four SFP+ Ethernet optical ports are unavailable, and two QSFP+ Ethernet optical ports work at the rate of 40 Gbit/s.

NOTE

This command is supported only on the S5731-S8UM16UN2Q, S5731S-S8UM16UN2Q-A, S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002) and S5732-H48XUM2CC.

Format

set device port-config-mode *port-config-mode* **enable** { **all** | **slot** *slot-id* }

undo set device port-config-mode enable { **all** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
port-config-mode	Specifies the working mode of ports on the device panel.	The value is a character string: - **4*25GE+2*40GE** - **4*25GE+4*10GE+40GE** - **4*25GE+40GE+4*10GE** - **4*25GE+8*10GE** - **2*100GE** - **4*25GE+100GE** - **100GE+4*25GE** - **8*25GE** - **8*10G+16*2.5G+2*40G** - **12*10G+12*2.5G+4*10G** **NOTE** The **8*10G+16*2.5G+2*40G** and **12*10G+12*2.5G+4*10G** parameters are supported only on the S5731-S8UM16UN2Q and S5731S-S8UM16UN2Q-A.
all	Indicates all slots.	-
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

There are four SFP28 Ethernet optical ports and two QSFP28 Ethernet optical ports on the panel of S5732-H24UM2CC (part number: 02353HUC/02353HUC-003/02353SJY/02353SJY-001/02353SJY-004/02353SJY-010/02353SJY-011/02353SJY-014/02353SJY-015/02353SJY-016/02353SJY-019/02353SJY-002/02353SJY-003/02353SJY-012/02353SJY-013/02353SJY-017/02353SJY-018), S5732-H48UM2CC (part number: 02353HUB/02353HUB-002/02353SJT/02353SJT-001/02353SJT-003/02353SJT-004/02353SJT-010/02353SJT-011/02353SJT-013/02353SJT-014/02353SJT-015/02353SJT-016/02353SJT-018/02353SJT-002) and S5732-H48XUM2CC. You can run the **set device port-config-mode enable** command to change the working mode of SFP28 Ethernet optical ports on the device panel and change the working mode of QSFP28 Ethernet optical ports or split QSFP28 Ethernet optical ports. The device supports eight types of working mode switching modes or interface split modes:

- **4*25GE+2*40GE**: Four SFP28 Ethernet optical ports work at the rate of 25 Gbit/s, and two QSFP28 Ethernet optical ports work at the rate of 40 Gbit/s.
- **4*25GE+4*10GE+40GE**: Four SFP28 Ethernet optical ports work at the rate of 25 Gbit/s, QSFP28 Ethernet optical port 1 is split into four 10GE ports, and QSFP28 Ethernet optical port 2 works at the rate of 40 Gbit/s.
- **4*25GE+40GE+4*10GE**: Four SFP28 Ethernet optical ports work at the rate of 25 Gbit/s, QSFP28 Ethernet optical port 1 works at the rate of 40 Gbit/s, and QSFP28 Ethernet optical port 2 is split into four 10GE ports.
- **4*25GE+8*10GE**: Four SFP28 Ethernet optical ports work at the rate of 25 Gbit/s, and each of two QSFP28 Ethernet optical ports is split into four 10GE ports.
- **2*100GE**: Four SFP28 Ethernet optical ports are unavailable, and two QSFP28 Ethernet optical ports work at the rate of 100 Gbit/s.
- **4*25GE+100GE**: Four SFP28 Ethernet optical ports are unavailable, QSFP28 Ethernet optical port 1 is split into four 25GE ports, and QSFP28 Ethernet optical port 2 works at the rate of 100 Gbit/s.
- **100GE+4*25GE**: Four SFP28 Ethernet optical ports are unavailable, QSFP28 Ethernet optical port 1 works at the rate of 100 Gbit/s, and QSFP28 Ethernet optical port 2 is split into four 25GE ports.
- **8*25GE**: Four SFP28 Ethernet optical ports are unavailable, and each of two QSFP28 Ethernet optical ports is split into four 25GE ports.

On the panel of the S5731-S8UM16UN2Q and S5731S-S8UM16UN2Q-A, there are 24 MultiGE interfaces, four SPF+ Ethernet optical ports, and two QSFP+ Ethernet optical ports. You can switch the interface working mode as required. The device supports the following working mode switching modes:

- **8*10G+16*2.5G+2*40G**: On the panel, the first 16 MultiGE interfaces work at the rate of 2.5 Gbit/s, the last eight MultiGE interfaces work at the rate of 10 Gbit/s, four SFP+ Ethernet optical ports are unavailable, and two QSFP+ Ethernet optical ports work at the rate of 40 Gbit/s.
- **12*10G+12*2.5G+4*10G**: On the panel, the first 12 MultiGE interfaces work at the rate of 2.5 Gbit/s, the last 12 MultiGE interfaces work at the rate of 10 Gbit/s, four SFP+ Ethernet optical ports work at the rate of 10 Gbit/s, and two QSFP+ Ethernet optical ports are unavailable.

Precautions

- After the working mode of an interface is changed or an interface is split, the configuration on the original interface is lost. Therefore, exercise caution when performing this operation.
- After running this command, you need to confirm the automatic restart of the device as prompted to make the configuration take effect. To prevent configuration loss, save the configuration in advance.
- After interface split is configured, the interface and converted interfaces cannot be added to a stack interface, regardless of whether the configuration takes effect. If an interface has been added to a stack interface, the interface cannot be split.

Example

Configure the two QSFP28 Ethernet optical ports on the device panel to work at the rate of 100 Gbit/s.

```
<HUAWEI> system-view
[HUAWEI] set device port-config-mode 2*100GE enable all
Warning: After the command is run, some ports may become unavailable or their configurations may be
lost, and the device automatically restarts. Continue? [Y/N]:y
Warning: Save the configuration before restart. Otherwise, configuration will be lost and the device will
restart. Continue? [Y/N]:y
```

4.2.84 set ethernet speed down-grade

Function

The **set ethernet speed down-grade** command enables the rate decrease auto-negotiation function on an interface.

The **undo set ethernet speed down-grade** command disables the rate decrease auto-negotiation function on an interface.

By default, rate decrease auto-negotiation is disabled on an interface.

NOTE

The rate decrease auto-negotiation function takes effect only on the following interfaces:

- MultiGE interface
- GE electrical interface
- GE optical interface that has a GE copper module installed
- Last four 10GE electrical interfaces on the ES5D21X08T00 card of the S5731-H and S5731S-H

Format

set ethernet speed down-grade

undo set ethernet speed down-grade

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two devices are connected through two GE electrical interfaces using a network cable. The two GE interfaces are configured to work in rate auto-negotiation mode. The network cable can only work at the rate of 100 Mbit/s or 10 Mbit/s because it deteriorates, but the maximum rate supported by the two GE interfaces is 1000 Mbit/s. The interfaces negotiate the working rate to 1000 Mbit/s, but cannot go Up because the network cable does not support the rate of 1000 Mbit/s.

You can use the rate decrease auto-negotiation function to solve this problem. After rate decrease auto-negotiation is enabled using this command, the two GE interfaces can decrease the negotiated rate to 10 Mbit/s or 100 Mbit/s, and then can go Up.

Prerequisites

The two connected interfaces work in auto-negotiation mode. If an interface works in non-auto-negotiation mode, run the **negotiation auto** command in the interface view to configure it to work in auto-negotiation mode.

Precautions

If rate decrease auto-negotiation is configured on the local interface, but not on the remote interface, the local interface can still decrease the negotiated rate to 100 Mbit/s. If the rate decrease auto-negotiation function is configured on an interface of the S5720-28X-PWH-LI-AC or S5720-28X-PWH-LI-ACF, configure this function on the remote interface; otherwise, the local and remote interfaces may not go Up.

If the network cable quality is low, a MultiGE interface takes longer time to go Up after the rate decrease auto-negotiation function is configured. For example, if the rate is decreased from 10 Gbit/s to 100 Mbit/s, the MultiGE interface takes about 40 seconds to go Up. If the rate is decreased from 2.5 Gbit/s to 100 Mbit/s, the MultiGE interface takes about 20 seconds to go Up. It is recommended that you replace the network cable.

After the rate decrease auto-negotiation function is configured on a MultiGE interface, the interface rate may automatically decrease to 1000 Mbit/s, if a network cable is removed and reinstalled on the interface in Down state continuously or if the **shutdown** and **undo shutdown** commands are frequently run on the interface. To restore the interface rate to 2500 Mbit/s, remove and reinstall the network cable again after the interface goes Up or run the **shutdown** and **undo shutdown** commands on the remote interface.

After the rate decrease auto-negotiation function is configured on a GE interface, the interface rate may automatically decrease to 100 Mbit/s, if a network cable is removed and reinstalled on the interface in Down state continuously or if the **shutdown** and **undo shutdown** commands are frequently run on the interface. To restore the interface rate to 1000 Mbit/s, remove and reinstall the network cable again after the interface goes Up or run the **shutdown** and **undo shutdown** commands on the remote interface.

Example

Configure the rate decrease auto-negotiation function on a GE interface.

```
<HUAWEI> system-view
[HUAWEI] set ethernet speed down-grade
```

4.2.85 set error-statistics trigger speed-down-grade

Function

The **set error-statistics trigger speed-down-grade** command enables the device to automatically reduce the interface rate when the number of error packets on an interface reaches the threshold.

The **undo set error-statistics trigger speed-down-grade** command disables the device from automatically reducing the interface rate when the number of error packets on an interface reaches the threshold.

By default, the device is enabled to automatically reduce the interface rate when the number of error packets on an interface reaches the threshold.

NOTE

This command is supported only on the following switch models: S5731-S, S5731S-S, S5731-H, S5731S-H.

Format

set error-statistics trigger speed-down-grade { **disable** | **enable** }

undo set error-statistics trigger speed-down-grade disable

Parameters

Parameter	Description	Value
disable	Disables the device from automatically reducing the interface rate when the number of error packets on an interface reaches the threshold.	-
enable	Enables the device to automatically reduce the interface rate when the number of error packets on an interface reaches the threshold.	-

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GE electrical interface on a device is connected to a specific printer and the interface rate is higher than 10 Mbit/s, the interface can go Up, but the printer cannot work properly. Alignment error packets will be detected on the interface. In this case, you can enable the device to automatically reduce the interface rate when the number of error packets on the interface reaches the threshold. The device then automatically sets the interface rate to 10 Mbit/s, reports an alarm (hwPortErrPktSpeedDownGrade), and records a log (IFPDT/1/ERRPKT_SPEEDDOWN) when the following conditions are met:

- The interface receives three alignment error packets within 60 seconds.
- The interface is in the auto-negotiation state and works at the rate of 100 Mbit/s.
- Only one MAC address is learned on the interface, and the MAC address starts with 001B-82 or is in the MAC address blacklist configured using **error-statistics trigger speed-down-grade** command.

After the interface rate is set to 10 Mbit/s, the device does not automatically reduce the interface rate if any of the following conditions is met. Instead, the device restores the interface rate to the default value obtained through auto-negotiation, sends a clear alarm (hwPortErrPktSpeedDownGradeResume), and records a log (IFPDT/1/ERRPKT_SPEEDDOWNRECOVER).

- The **set ethernet speed down-grade disable** command is run to disable the device from automatically reducing the interface rate when the number of error packets on an interface reaches the threshold.
- The **auto speed** command is run on the interface to set the auto-negotiation rate.
- The **undo negotiation auto** command is run on the interface to set the working mode of the interface to non-auto-negotiation.
- A new MAC address is learned on the interface, and the number of MAC address entries on the interface is not 1.

To prevent the interface rate reduction information from being lost after the device restarts, the device automatically records the interface rate information in the file named **speeddowngrade.txt** every 10 minutes or you can run the **save** command to record the information in the file named **speeddowngrade.txt**. After the device restarts, the interface rate remains unchanged. Running the **reset saved-configuration** or **reset factory-configuration** command automatically clears the saved files.

Precautions

- After the interface rate is set to 10 Mbit/s, you need to restart the printer so that the printer can work properly.
- When the interface goes Down, the function of automatically reducing the interface rate when the number of error packets on an interface reaches the threshold still takes effect, and the interface rate remains 10 Mbit/s.

Example

Enable the device to automatically reduce the interface rate when the number of error packets on an interface reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] set error-statistics trigger speed-down-grade enable
```

4.2.86 set flow-statistics include-interframe

Function

The **set flow-statistics include-interframe** command configures traffic statistics on an interface to contain the inter-frame gap and preamble.

The **undo set flow-statistics include-interframe** command configures traffic statistics on an interface not to contain the inter-frame gap and preamble.

By default, traffic statistics on an interface contain the inter-frame gap and preamble.

Format

set flow-statistics include-interframe

undo set flow-statistics include-interframe

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display interface** command to view the running status and traffic statistics on an interface. The **Last 300 seconds input rate** or **Last 300 seconds output rate** field in the command output indicates the inbound or outbound traffic rate on the interface in the last 300 seconds.

- If you want to obtain the total number of bytes passing through an interface in a period, configure the device to count the bytes in the interframe gap (IFG) and preamble when collecting traffic statistics on the interface. The interface traffic rate is as follows:

  Interface traffic rate = (Original packet length + IFG + Preamble) x Number of packets passing through the interface every second
- If you want to obtain only the number of packet bytes passing through an interface in a period, configure the device not to count the bytes in the IFG and preamble when collecting traffic statistics on the interface. The interface traffic rate is as follows:

  Interface traffic rate = Original packet length x Number of packets passing through the interface every second

By default, the IFG has a fixed value of 12 bytes and the preamble has a fixed value of 8 bytes.

Example

Configure traffic statistics on GE0/0/1 to contain the inter-frame gap and preamble.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] set flow-statistics include-interframe
```

4.2.87 set flow-change-ratio

Function

The **set flow-change-ratio** { **input-threshold** | **output-threshold** } **upper-limit** command sets the trap threshold for a sudden traffic volume change on interfaces.

The **undo set flow-change-ratio** { **input-threshold** | **output-threshold** } **upper-limit** command restores the default trap threshold for a sudden traffic volume change on interfaces.

By default, the trap threshold for a sudden traffic volume change on interfaces is 50%.

Format

set flow-change-ratio { **input-threshold** | **output-threshold** } **upper-limit** *threshold*

undo set flow-change-ratio { **input-threshold** | **output-threshold** } **upper-limit**

Parameters

Parameter	Description	Value
input-threshold	Specifies the trap threshold for a sudden traffic volume change in the inbound direction of interfaces.	-
output-threshold	Specifies the trap threshold for a sudden traffic volume change in the outbound direction of interfaces.	-
upper-limit *threshold*	Specifies the threshold for the traffic volume change percentage on interfaces.	The value is an integer that ranges from 0 to 100. The default value is 50.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the switch to detect real-time traffic volume changes on interfaces, you can run this command to set the trap threshold for a sudden traffic volume change on interfaces for triggering a trap.

Traffic volume change percentage on interfaces = |Interface rate in the current traffic statistics collection interval - Interface rate in the previous traffic statistics collection interval| / Interface rate in the previous traffic statistics collection interval

Configuration Impact

If the trap function for a sudden traffic volume change is enabled (using the **snmp-agent trap enable feature ifpdt trap-name hwInputRateChangeOverThresholdNotice** or **snmp-agent trap enable feature ifpdt trap-name hwOutputRateChangeOverThresholdNotice** command) after the **set flow-change-ratio** command is enabled, a trap will be generated when the traffic volume change percentage on interfaces exceeds the specified threshold (value of *threshold*) and the bandwidth usage percentage is not lower than the lower threshold (*threshold* configured using the **set flow-change-ratio start-check** command).

Precautions

You can run the **set flow-stat interval** command to configure the traffic statistics collection interval on interfaces. The default interval is 300 seconds.

Example

Set the trap threshold for a sudden traffic volume change in the inbound direction of interfaces to 70%.

```
<HUAWEI> system-view
[HUAWEI] set flow-change-ratio input-threshold upper-limit 70
```

4.2.88 set flow-change-ratio input-broadcast-detect disable

Function

The **set flow-change-ratio input-broadcast-detect disable** command disables detection of a sudden broadcast traffic volume change in the inbound direction of interfaces.

The **undo set flow-change-ratio input-broadcast-detect disable** command enables detection of a sudden broadcast traffic volume change in the inbound direction of interfaces.

By default, detection of a sudden broadcast traffic volume change in the inbound direction of interfaces is enabled.

Format

set flow-change-ratio input-broadcast-detect disable

undo set flow-change-ratio input-broadcast-detect disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch checks whether the volume of broadcast traffic in the inbound direction of interfaces changes suddenly, and generates a trap after detecting a sudden change, facilitating network maintenance.

If the switch has many interfaces, detection of a sudden broadcast traffic volume change in the inbound direction of interfaces consumes some CPU and memory resources. You can run the **set flow-change-ratio input-broadcast-detect disable** command to disable the function.

Precautions

If the system software is upgraded from V200R009C00 or an earlier version to V200R010C00 or a later version, detection of a sudden broadcast traffic volume change in the inbound direction of interfaces is disabled by default.

Example

Disable detection of a sudden broadcast traffic volume change in the inbound direction of interfaces.

```
<HUAWEI> system-view
[HUAWEI] set flow-change-ratio input-broadcast-detect disable
```

4.2.89 set flow-change-ratio start-check

Function

The **set flow-change-ratio start-check bandwidth-usage** command sets the lower threshold of the initial bandwidth usage percentage for triggering a trap.

The **undo set flow-change-ratio start-check bandwidth-usage** command restores the default lower threshold of the initial bandwidth usage percentage for triggering a trap.

By default, the lower threshold of the initial bandwidth usage percentage for triggering a trap is 20%.

Format

set flow-change-ratio start-check bandwidth-usage *bandwidth-usage-threshold*

undo set flow-change-ratio start-check bandwidth-usage

Parameters

Parameter	Description	Value
bandwidth-usage *bandwidth-usage-threshold*	Specifies the lower threshold of the initial bandwidth usage percentage for triggering a trap.	The value is an integer that ranges from 1 to 100. The default value is 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the switch to detect real-time traffic volume changes on interfaces, you can run this command to set the lower threshold of the initial bandwidth usage percentage for triggering a trap.

Configuration Impact

If the trap function for a sudden traffic volume change is enabled (using the **snmp-agent trap enable feature ifpdt trap-name hwInputRateChangeOverThresholdNotice** or **snmp-agent trap enable feature ifpdt trap-name hwOutputRateChangeOverThresholdNotice** command) after the **set flow-change-ratio** command is enabled, a trap will be generated when the traffic volume change percentage on interfaces exceeds the specified threshold (*threshold* configured using the **set flow-change-ratio** command) and the bandwidth usage percentage is not lower than the lower threshold (value of *bandwidth-usage-threshold*).

Precautions

You can run the **set flow-stat interval** command to configure the traffic statistics collection interval on interfaces. The default interval is 300 seconds.

Example

Set the trap threshold for the lower threshold of the initial bandwidth usage percentage to 70%.

```
<HUAWEI> system-view
[HUAWEI] set flow-change-ratio start-check bandwidth-usage 70
```

4.2.90 set if-mib sample-interval

Function

The **set if-mib sample-interval** command configures the interval of collecting traffic statistics on an interface.

The **undo set if-mib sample-interval** command restores the default interval.

The default interval is 60 seconds.

Format

set if-mib sample-interval *interval-value*

undo set if-mib sample-interval [*interval-value*]

Parameters

Parameter	Description	Value
interval-value	Specifies the interval of collecting traffic statistics on an interface.	The value can be 0 or an integer multiple of 10 in the range from 10 to 300, in seconds. The value 0 indicates that the function of periodically collecting traffic statistics on an interface is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the NMS obtains interface traffic statistics through the MIB tables iftable and ifxtable, the time for querying interface traffic statistics in real time is long. When the device has a large number of interfaces, the query efficiency of the NMS is low. To resolve this issue, switches can be configured to periodically collect traffic statistics on interfaces. In this case, the NMS can directly obtain traffic statistics collected on interfaces, improving the query efficiency.

Precautions

- If the command has been run for multiple times, only the latest configuration takes effect.
- When the **undo set if-mib sample-interval** [*interval-value*] command is run, if the interval is specified, the value must be consistent with the current configuration.
- A short interval will cause a high CPU usage.

Example

Set the interval of collecting traffic statistics on an interface to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] set if-mib sample-interval 100
```

4.2.91 set log updown disable

Function

The **set log updown disable** command disables the log function for interface up/down changes.

The **undo set log updown disable** command enables the log function for interface up/down changes.

By default, the log function for interface up/down changes is enabled.

Format

set log updown disable

undo set log updown disable

Parameters

None

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can disable the log function for interface up/down changes in the following situation: A large number of interfaces repeatedly alternate between up and down states and users do not need to pay attention to the up/down changes of these interfaces, for example, interfaces alternate between up and down states when APs connected to the network go online and offline.

Precautions

This command is not supported on an interface that is configured as a stack interface.

Example

Disable the log function for up/down changes on GE**0**/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/0] set log updown disable
```

4.2.92 set port-enable delay

Function

The **set port-enable delay** command sets the delay after which an interface goes Up after a device restart.

The **undo set port-enable delay** command deletes the delay after which an interface goes Up after a device restart.

By default, an interface goes Up immediately after a device restart.

Format

set port-enable delay *delay-timer*

undo set port-enable delay

Parameters

Parameter	Description	Value
delay-timer	Specifies the delay after which an interface goes Up after a device restart.	The value is an integer ranging from 0 to 1800, in seconds. The increment value is 10 seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an unstable network, devices may fail to obtain IP addresses from the expected DHCP server. If devices obtain IP addresses from another DHCP server, the devices cannot obtain IP addresses on the expected network segment for a long time even after the network is recovered. To prevent this problem, you can set the delay after which interfaces go Up after a device restart.

Precautions

- If you run the **shutdown** and **undo shutdown** commands or run the **restart** command on the interface during the delay, the delay does not take effect.
- The configuration takes effect only after the device is restarted.

Example

Set the delay after which GE0/0/1 goes Up after a device restart to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] set port-enable delay 20
Warning: The configuration takes effect only after the card or subcard is restarted.
```

4.2.93 single-fiber enable

Function

The **single-fiber enable** command enables the single-fiber communication function on an optical interface.

The **undo single-fiber enable** command disables the single-fiber communication function on an optical interface.

By default, the single-fiber communication function is disabled on an optical interface.

NOTE

The first four GE optical ports on the S5731-S48S4X, S5731-S48S4X-A, S5731S-S48S4X-A, and S5731S-S48S4X-A1 do not support this configuration.

GE, XGE, 25GE, and 40GE interfaces on the S5731-H24HB4XZ, S5731-H48HB4XZ, S5731S-H24HB4XZ-A, and S5731S-H48HB4XZ-A support this configuration. On other S5731-H, only XGE, 25GE, and 40GE interfaces support this configuration.

On the S5732-H, S6730-H, and S6730S-H, only 25GE, 40GE, and 100GE interfaces support this configuration.

On the S6730-S and S6730S-S, only 40GE interfaces support this configuration.

GE optical interfaces on the following models do not support this command: S5720-52X-LI-24S-AC1, S5720-52X-LI-48S-AC1, S5720-52X-LI-48S-DC1, S5736-S24S4XC, S5736-S48S4XC, S6720S-S24S28X-A.

XGE optical interfaces on the following models support this command after they have GE optical modules installed: S6735-S, S6720-EI, S6720S-EI.

Optical interfaces of other models support this command.

Note the following:

- A GE optical interface supports this command only when it works at the rate of 1000 Mbit/s.
- An XGE optical interface supports this command only when it has no optical module installed or has an XGE optical module installed.
- A 25GE optical interface supports this command only when it has no optical module installed or has a GE, XGE, or 25GE optical module installed.
- A 40GE optical interface supports this command only when it has no optical module installed or has a 40GE optical module installed.
- A 100GE optical interface supports this command only when it has no optical module installed or has a 40GE or 100GE optical module installed.
- The QSFP-40G-SR-BD, QSFP-40G-SDLC-PAM, QSFP-40G-LR4-Lite, QSFP-40G-LX4-MM, and QSFP-40G-eSDLC-PAM optical modules do not support the single-fiber function.

Format

single-fiber enable

undo single-fiber enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network management and maintenance, the administrator may need to send traffic from users to a specified server for analysis and processing. If a server can receive and send packets, there is a possibility that the server forwards user traffic to other devices, causing a security risk. The unidirectional single-fiber communication function can address this issue. A single fiber means that two optical modules are connected by only one fiber, and unidirectional communication means that packets can be sent in only one direction. With this function, a switch can only send but cannot receive packets, and an analysis server can only receive but cannot send packets. Data security on the analysis server is ensured.

Precautions

- The remote interface also works in non-auto negotiation mode and the rate of the peer interface is the same as the rate of the local interface.
- The **single-fiber enable** command and **configuring internal loopback detection** and **MAC SWAP loopback test** cannot be configured on the same interface.
- If this command has been run on an interface, the command configuration is lost in the following situations:
  - The GE optical interface has an FE optical module installed.
  - The GE optical interface does not work at a rate of 1000 Mbit/s.
  - The XGE interface is connected to a cable or has a GE optical module installed.
  - The 25GE interface is connected to a cable.
  - The 40GE interface is connected to a cable.
  - The 100GE interface is connected to a cable.

Example

Enable XGigabitEthernet0/0/1 to send packets through a single fiber.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] single-fiber enable
```

4.2.94 speed

Function

The **speed** command sets the rate for an Ethernet interface in non-auto negotiation mode.

The **undo speed** command restores the default rate of an Ethernet interface in non-auto negotiation mode.

By default, an Ethernet interface works at its highest rate when it works in non-auto negotiation mode.

Format

speed { **10** | **100** | **1000** | **2500** | **5000** | **10000** }

undo speed

Parameters

Parameter	Description	Value
10	Indicates that the interface works at 10 Mbit/s.	-
100	Indicates that the interface works at 100 Mbit/s.	-
1000	Indicates that the interface works at 1000 Mbit/s. **NOTE** FE interfaces do not support this parameter.	-
2500	Sets the auto-negotiation rate of an Ethernet electrical interface to 2500 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
5000	Sets the auto-negotiation rate of an Ethernet electrical interface to 5000 Mbit/s. **NOTE** Only MultiGE interfaces support this parameter.	-
10000	Sets the auto-negotiation rate of an Ethernet electrical interface to 10000 Mbit/s. **NOTE** Only MultiGE interfaces and 25GE interfaces with XGE/25GE dual-rate optical modules installed support this parameter.	-

Views

Ethernet interface view, GE interface view, MultiGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In non-auto negotiation mode, if interfaces on two connected devices work at different rates, use the **speed** command to change the rates of the interfaces to be the same so that the two devices can communicate.

Precautions

- If the remote interface does not support the auto negotiation mode, run the **undo negotiation auto** command on the local interface to configure the interface to work in non-auto negotiation mode. You can then change the rate of the local interface to be the same as the rate of the remote interface to ensure proper communication.
- For details about the rates supported by Ethernet interfaces, see Licensing Requirements and Limitations for Ethernet Interfaces.
- On 25GE interfaces, the **speed 10000** command is mutually exclusive with the following commands:
  - **port mode ge (25GE interface)**
  - **fec mode rs**
  - **fec mode base-r**
- The rate of MultiGE interfaces on the S5732-H24UM2CC, S5732-H48UM2CC, and S5736-S24UM4XC can be increased using the RTU license. After the license is activated, you can run the **assign group-speed** command and restart the device to make the configured maximum rate supported by the interfaces in the MultiGE interface group take effect.

  To check the default rate of MultiGE interfaces, run the **display device group-speed configuration** command. The **BaseSpeed** field indicates the default rate.

Example

Configure GE0/0/1 to work at 100 Mbit/s in non-auto negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo negotiation auto
[HUAWEI-GigabitEthernet0/0/1] speed 100
```

4.2.95 speed auto-negotiation

Function

The **speed auto-negotiation** command enables auto-negotiation on a GE optical interface.

The **undo speed auto-negotiation** command disables auto-negotiation on a GE optical interface.

By default, auto-negotiation is disabled on a GE optical interface.

NOTE

Only the following models do not support this command:

- S200 series
- S300 series
- S500-8T4S, S500-8P4S, S500-24T4S, S500-16T4S, S500-24P4S, S500-16P4S, and S500-48T4S
- S1730S-S8T4S-A1, S1730S-S8P4S-A1, S1730S-S24T4S-A1, S1730S-S24P4S-A1, S1730S-S48T4S-A1, and S1730S-S48P4S-A1
- S2730S-S8FT4S-A, S2730S-S8FP4S-A, S2730S-S16FT4S-A, S2730S-S24FT4S-A, S2730S-S24FP4S-A, and S2730S-S48FT4S-A
- S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28TP-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-ACL, S5720-28P-LI-AC, S5720-28P-PWR-LI-AC, S5720-52P-LI-AC, and S5720-52P-PWR-LI-AC
- S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, S5720S-28P-LI-AC, S5720SV2-28P-LI-AC, S5720S-28P-PWR-LI-AC, S5720S-52P-LI-AC, S5720SV2-52P-LI-AC, and S5720S-52P-PWR-LI-AC
- S5731S-H24T4S-A and S5731S-H48T4S-A
- S5732-H24S6Q and S5732-H48S6Q
- S6720S-S24S28X-A

Format

speed auto-negotiation

undo speed auto-negotiation

Parameters

None

Views

GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an optical interface is configured to work in auto-negotiation mode using the **negotiation auto** command, the interface cannot negotiate the rate with another interface. You can run the **speed auto-negotiation** command to configure the auto-negotiation function on the interface. After auto-negotiation is configured on the interface, if the interface is Down, the device cyclically switches the interface to the auto-negotiated 1000 Mbit/s, forced 1000 Mbit/s, and forced 100 Mbit/s until the interface goes Up.

Prerequisites

Run the **negotiation auto** command to enable auto-negotiation before using the **speed auto-negotiation** command on the interface.

Precautions

- The **speed auto-negotiation** command will make flow control auto-negotiation and internal loopback ineffective.
- After auto-negotiation is configured on an interface, if a single fiber is removed and then inserted or the link is not operational, the interface may be Up and the remote interface may be down. You can run the **shutdown** and **undo shutdown** commands on the remote interface to make the remote interface go Up.
- After auto-negotiation is configured on an interface, if this interface becomes Up and the remote interface becomes Down after the negotiation, run the **shutdown** and **undo shutdown** commands on the remote interface or run the **undo speed auto-negotiation** and **speed auto-negotiation** commands on this interface to enable the two ends to negotiate their rate again.

Example

Enable auto-negotiation on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] negotiation auto
[HUAWEI-GigabitEthernet0/0/1] speed auto-negotiation
```

4.2.96 statistic enable (interface view)

Function

The **statistic enable** command enables IPv4 or IPv6 packet statistics collection on an interface.

The **undo statistic enable** command disables IPv4 or IPv6 packet statistics collection on an interface.

By default, IPv4 or IPv6 packet statistics collection is disabled on an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

{ **ipv4** | **ipv6** } * **statistic enable** { **both** | **inbound** | **outbound** }

undo { **ipv4** | **ipv6** } * **statistic enable** { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv4	Indicates IPv4 packet statistics collection.	-

Parameter	Description	Value
ipv6	Indicates IPv6 packet statistics collection.	-
both	Indicates statistics collection for incoming and outgoing packets.	-
inbound	Indicates statistics collection for incoming packets.	-
outbound	Indicates statistics collection for outgoing packets.	-

Views

Eth-Trunk interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can enable IPv4 or IPv6 packet statistics collection on an interface to collect IPv4 or IPv6 packet statistics on the interface.

Precautions

- If this command and the **traffic-policy (interface view)** command are configured together on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, traffic policy will fail to be applied.
- After the IPv4 or IPv6 packet statistics collection function is enabled on an interface, you can run the **display counters protocol** command to check traffic statistics on the interface.

Example

Enable IPv4 packet statistics collection in the inbound direction of GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv4 statistic enable inbound
```

4.2.97 traffic-pppoe

Function

The **traffic-pppoe** command configures an interface to allow only PPPoE packets to pass through.

The **undo traffic-pppoe** command cancels the configuration.

By default, an interface allows all types of packets to pass through.

NOTE

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support the configuration.

Format

traffic-pppoe { **any** | *source-address* } { **any** | *destination-address* }

undo traffic-pppoe { **any** | *source-address* } { **any** | *destination-address* }

Parameters

Parameter	Description	Value
{ **any** | *source-address* }	Indicates that an interface allows PPPoE packets with a specified source MAC address to pass through. ● **any** indicates that PPPoE packets with any source MAC address can pass through the interface. ● *source-address* indicates that PPPoE packets with a specified source MAC address can pass through the interface.	The value of *source-address* is in the format H-H-H. An H contains 1 to 4 hexadecimal digits.

Parameter	Description	Value
{ **any** | *destination-address* }	Indicates that an interface allows PPPoE packets with a specified destination MAC address to pass through. - **any** indicates that PPPoE packets with any destination MAC address can pass through the interface. - *destination-address* indicates that PPPoE packets with a specified destination MAC address can pass through the interface.	The value of *destination-address* is in the format H-H-H. An H contains 1 to 4 hexadecimal digits.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

If you run the **traffic-pppoe any any** command on an interface, the interface allows only PPPoE packets to pass through and discards other packets.

Example

Configure GE0/0/1 to allow only PPPoE packets to pass through.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-pppoe any any
```

Configure GE0/0/1 to allow only PPPoE packets with source MAC address 1-1-1 to pass through.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-pppoe 1-1-1 any
```

4.2.98 training (40GE interface view)

Function

The **training disable** and **undo training enable** commands disable the training function on a 40GE interface.

The **training enable** and **undo training disable** commands enable the training function on a 40GE interface.

By default, the training function is enabled on a 40GE interface.

NOTE

- The training function can be configured on the 40GE interfaces of the S6720-EI and S6720S-EI.
- The training function can be configured on the 40GE interfaces of the S5735S-H, S5731-H, S5731S-H24T4XC-A, S5731S-H48T4XC-A or S5736-S that has the ES5D21Q02Q00 or ES5D21Q04Q01 card installed.

Format

training { enable | disable }

undo training { enable | disable }

Parameters

None

Views

40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the increase of transmission rate or frequency, attenuation of signal's high-frequency components becomes increasingly severe. To guarantee transmission performance of signals, it is necessary to compensate for signals, and commonly used compensation technologies are pre-emphasis and balancing. The pre-emphasis technology increases high-frequency components of signals at the transmit end of transmission lines to compensate attenuation during the transmission. However, the pre-emphasis technology increases crosstalk while amplifying high-frequency components. To solve this problem, the balancing technology is developed. The balancing technology is used at the receive end of transmission lines to function like a filter for filtering high-frequency crosstalk.

After the training function is enabled on a 40GE interface, the transmit end exchanges frames with the receive end to automatically set the pre-emphasis and balancing parameters, improving processing efficiency of the two technologies. Note that the negotiated parameters for the training function are obtained based on the site environment. If the site environment changes, for example, from high-temperature environment to low-temperature environment, the parameters may be inaccurate. Therefore, bit errors may occur when the training function is enabled. The training function is optional in IEEE802.3 standards, and its implementation on different types of products from various vendors may differ.

When connecting two devices, enable or disable the training function on both ends simultaneously. By default, the training function is enabled on a 40GE interface. If the training function is disabled on the remote device or the remote device does not support the function, run the **training disable** or **undo training enable** command to disable the function.

Precautions

- The **training disable** and **undo training enable** commands can be configured on a 40GE interface only when the interface connects to a high-speed cable and is not a physical member interface in a stack.
- After a cable is installed on a 40GE interface without the **training disable** configuration, the **training enable** configuration is automatically generated on the interface.
- If no cable is installed on an interface, only the **training enable** and **undo training disable** commands can be configured on the interface.
- If the **display this include-default** command is run on an interface to view the training configuration after a cable is installed on the interface, the default **training enable** configuration is always displayed in the command output and does not change with the training configuration change.
- The training configuration on an interface takes effect only after a cable is installed on the interface. If the cable is replaced with an optical module, the **training disable** and **training enable** configurations will be automatically deleted from the interface.
- If a 40GE interface is configured as a physical member interface in a stack system, the **training disable** and **training enable** configurations will be automatically deleted from the interface.
- If a 40GE interface has been configured as a physical member interface in a stack system, the training function is disabled on the interface by default and cannot be enabled.
- If the **training disable** or **undo training enable** command is configured on a 40GE interface of the S6720S-26Q-EI-24S-AC or S6720S-26Q-EI-24S-DC after a cable is installed on the interface, and the interface is connected to a remote interface on which the training function is disabled or a remote interface that does not support the training function, the two interfaces may not go Up or go Up after a delay. Therefore, configure the **training disable** or **undo training enable** command only when the training function is disabled on the remote interface or the remote interface does not support the training function. In other scenarios, it is recommended that you do not disable the training function.
- If the training configuration does not exist on an interface of a switch running V200R008C00 or an earlier version, the **training disable** configuration is automatically generated on the interface after the system software is upgraded to a version later than V200R009C00. If the training configuration

exists on the interface, the configuration remains unchanged after the system software is upgraded to a version later than V200R009C00.

Example

Disable the training function on 40GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface 40ge 0/0/1
[HUAWEI-40GE0/0/1] training disable
Warning: The configuration will cause an abnormality in port running. Continue? [Y/N]:y
```

4.2.99 training (100GE interface view)

Function

The **training disable** and **undo training enable** commands disable the training function on a 100GE interface.

The **training enable** and **undo training disable** commands enable the training function on a 100GE interface.

By default, the training function is enabled on a 100GE interface.

NOTE

Only the S6735-S supports this command.

The **training disable** and **undo training enable** commands can be configured on a 100GE interface only when the interface connects to a 40GE or 100GE cable.

Format

training { enable | disable }

undo training { enable | disable }

Parameters

None

Views

100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the increase of transmission rate or frequency, attenuation of signal's high-frequency components becomes increasingly severe. To guarantee transmission performance of signals, it is necessary to compensate for signals, and commonly used compensation technologies are pre-emphasis and balancing. The pre-emphasis technology increases high-frequency components of signals at the transmit end of transmission lines to compensate attenuation during the transmission. However, the pre-emphasis technology increases crosstalk while amplifying high-frequency components. To solve this problem, the balancing technology is developed. The balancing technology is used at the receive end of transmission lines to function like a filter for filtering high-frequency crosstalk.

After the training function is enabled on a 100GE interface, the transmit end exchanges frames with the receive end to automatically set the pre-emphasis and balancing parameters, improving processing efficiency of the two technologies. Note that the negotiated parameters for the training function are obtained based on the site environment. If the site environment changes, for example, from high-temperature environment to low-temperature environment, the parameters may be inaccurate. Therefore, bit errors may occur when the training function is enabled. The training function is optional in IEEE802.3 standards, and its implementation on different types of products from various vendors may differ.

When connecting two devices, enable or disable the training function on both ends simultaneously. By default, the training function is enabled on a 100GE interface. If the training function is disabled on the remote device or the remote device does not support the function, run the **training disable** or **undo training enable** command to disable the function.

Precautions

- After a 40GE or 100GE cable is installed on a 100GE interface without the **training disable** configuration, the **training enable** configuration is automatically generated on the interface.
- If no cable is installed on an interface, only the **training enable** and **undo training disable** commands can be configured on the interface.
- If the **display this include-default** command is run on an interface to view the training configuration after a cable is installed on the interface, the default **training enable** configuration is always displayed in the command output and does not change with the training configuration change.
- The training configuration on an interface takes effect only after a cable is installed on the interface. If the cable is replaced with an optical module, the **training disable** and **training enable** configurations will be automatically deleted from the interface.

Example

Disable the training function on 100GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface 100ge 0/0/1
[HUAWEI-100GE0/0/1] training disable
Warning: The configuration will cause an abnormality in port running. Continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.......
```

4.2.100 transceiver power low trigger error-down

Function

The **transceiver power low trigger error-down** command enables an Ethernet optical interface to enter the error-down state when the optical power is low.

The **undo transceiver power low trigger error-down** command disabled an Ethernet optical interface from entering the error-down state when the optical power is low.

By default, an Ethernet optical interface does not enter the error-down state when the optical power is low.

Format

transceiver power low trigger error-down

undo transceiver power low trigger error-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Low optical power of the device may cause intermittent service interruption. To ensure that services are running properly, enable an interface to enter the error-down state when the optical power is low so that services can be switched in a timely manner.

Follow-up Procedure

An interface in Error-down state can be recovered using either of the following methods:

- Manual recovery: If a few interfaces need to be recovered forcibly, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.
- Automatic recovery: If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. You can run the **error-down auto-recovery cause transceiver-power-low interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. An interface in Error-down state automatically recovers when the specified delay time expires.

Example

Enable GE0/0/1 to enter the error-down state when the optical power is low.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] transceiver power low trigger error-down
```

4.2.101 trap-threshold

Function

The **trap-threshold** command sets the inbound and outbound bandwidth usage thresholds for generating a trap.

The **undo trap-threshold** command restores the default inbound and outbound bandwidth usage thresholds for generating a trap.

The default inbound or outbound bandwidth usage threshold for generating a trap is 80.

Format

trap-threshold { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]

undo trap-threshold { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Indicates inbound bandwidth.	-
output-rate	Indicates outbound bandwidth.	-
bandwidth-in-use	Specifies the bandwidth usage threshold for generating a trap.	The value is an integer that ranges from 1 to 100.
resume-rate *resume-threshold*	Specifies the bandwidth usage threshold for clearing a trap.	The value is an integer that ranges from 1 to *bandwidth-in-use*. The default value is *bandwidth-in-use*.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring bandwidth usage helps you know current load on a device. If the bandwidth usage exceeds a threshold, bandwidth resources are insufficient and the device capacity needs to be expanded. For example, if the bandwidth usage exceeds 95%, an alarm is generated, indicating that bandwidth resources are almost exhausted. As a result, some services may be interrupted before device capacity expansion.

You can configure two thresholds: low threshold (log threshold) and high threshold (alarm threshold). The system generates a log when the bandwidth usage exceeds the low threshold and generates an alarm when the bandwidth usage exceeds the high threshold. This configuration ensures that you can expand the device capacity in advance to avoid service interruptions caused by bandwidth exhaustion.

NOTE

Outbound bandwidth usage = (Outbound interface rate/Outbound physical interface bandwidth) x 100

Inbound bandwidth usage = (Inbound interface rate/Inbound physical interface bandwidth) x 100

The interval for collecting statistics on the traffic rate on an interface is the value configured using the **set flow-stat interval** command on the interface.

The interface rate and bandwidth are expressed in bits per second.

To set a lower threshold, run the **log-threshold** command.

The **trap-threshold** command sets the bandwidth usage threshold for generating a trap. The **trap-threshold** with the following parameters provides various functions:

- **trap-threshold input-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the inbound bandwidth usage threshold for generating a trap.
  - If inbound bandwidth usage exceeds the threshold specified in *bandwidth-in-use*, an hwIfMonitorInputRateRising trap is generated, indicating that inbound bandwidth usage exceeds the configured threshold.
  - If inbound bandwidth usage falls below the threshold specified in *resume-threshold*, an hwIfMonitorInputRateResume trap is generated, indicating that inbound bandwidth usage falls between the configured threshold for clearing a trap.
- **trap-threshold output-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the outbound bandwidth usage threshold for generating a trap.
  - If outbound bandwidth usage exceeds the threshold specified in *bandwidth-in-use*, an hwIfMonitorOutputRateRising trap is generated, indicating that outbound bandwidth usage exceeds the configured threshold.
  - If outbound bandwidth usage falls below the threshold specified in *resume-threshold*, an hwIfMonitorOutputRateResume trap is generated, indicating that outbound bandwidth usage falls between the configured threshold for clearing a trap.

If the offset between the value of *bandwidth-in-use* and the value of *resume-threshold* is too small, trap information may be frequently displayed.

The log threshold must be lower than the trap threshold, providing efficient protection for services. For example, when the inbound bandwidth usage reaches 80%, a log is generated. If the inbound bandwidth usage continues to increase and reaches 95%, a trap is generated. This ensures that a log is generated for inbound bandwidth usage of 80%, and a trap is generated for inbound bandwidth usage of 95%. Either the log or the trap prompts for a bandwidth increase, preventing service interruption.

Example

Configure GE0/0/1 to generate a trap when the outbound bandwidth usage exceeds 60%.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold output-rate 60
```

Configure GE0/0/1 to generate a trap when the outbound bandwidth usage exceeds 80% and clear the trap when the outbound bandwidth usage falls below 60%.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold output-rate 80 resume-rate 60
```

4.2.102 trap-threshold enable

Function

The **trap-threshold enable** command enables the function of reporting an alarm if packets are discarded on an interface due to a congestion.

The **undo trap-threshold enable** command disables the function of reporting an alarm if packets are discarded on an interface due to a congestion.

By default, this function is disabled.

Format

trap-threshold { **input-discard** | **output-discard** } **enable**

undo trap-threshold { **input-discard** | **output-discard** } **enable**

Parameters

Parameter	Description	Value
input-discard	Enables the function of reporting an alarm if incoming packets are discarded on an interface due to a congestion.	-

Parameter	Description	Value
output-discard	Enables the function of reporting an alarm if outgoing packets are discarded on an interface due to a congestion.	-

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

NOTE

Only the S5736-S equipped with the S7C02000, S7Q02001, ES5D21Q02Q00 or ES5D21Q04Q01 card supports this command in the 40GE interface view.

Default Level

2: Configuration level

Usage Guidelines

If a congestion occurs on a network that is running, packets may be discarded when service flows are transmitted on the network. If a lot of packets are discarded, services are affected. To improve transmission quality of service flows, you can run the **trap-threshold enable** command to enable the function of reporting an alarm if packets are discarded on an interface due to a congestion. The device then reports an alarm if the number of discarded incoming and outgoing packets on the interface in a specified period exceeds the threshold. Such alarms help you know the congestion on the interface. You can determine whether to increase the bandwidth or cancel the bandwidth limit on the interface based on the logs. In this way, the congestion problem can be rectified.

Example

Enable the function of reporting an alarm if incoming packets are discarded on XGE0/0/1 due to a congestion.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] trap-threshold input-discard enable
```

4.2.103 trap-threshold error-percentage

Function

The **trap-threshold error-percentage** command configures the alarm threshold for the percentage of CRC packets against all the received packets on an interface and alarm interval.

The **undo trap-threshold error-percentage** command deletes the configured alarm threshold and interval.

By default, the alarm threshold and interval are not configured.

Format

trap-threshold error-percentage *threshold-value* **interval** *interval-value*

undo trap-threshold error-percentage [*threshold-value* **interval** *interval-value*]

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for the percentage of CRC packets against all the received packets on the interface.	The value is an integer that ranges from 1 to 50. **NOTE** You are advised to set the threshold to be smaller than the alarm threshold configured in the **error-down-threshold error-percentage** command.
interval *interval-value*	Specifies the interval for calculating the percentage of CRC packets against all the received packets on the interface.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface receives too many CRC packets, packet forwarding is affected. To enable the device to report the corresponding alarm if the percentage of received CRC packets against all the received packets within the specified period exceeds the alarm threshold, run this command.

Precautions

This command is mutually exclusive to the **trap-threshold error-statistics** command. After this command is configured, the **trap-threshold error-statistics** command configuration does not take effect.

Example

Set the alarm threshold for the percentage of CRC packets against all the received packets to 10% and the interval for calculating the percentage of CRC packets against all the received packets to 20 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold error-percentage 10 interval 20
```

4.2.104 trap-threshold error-statistics

Function

The **trap-threshold error-statistics** command sets the alarm threshold for error packets and alarm interval.

The **undo trap-threshold error-statistics** command restores the default alarm threshold for error packets and default alarm interval.

By default, the alarm threshold for error packets is 3 and the alarm interval is 10 seconds.

Format

trap-threshold error-statistics *threshold-value* **interval** *interval-value*

undo trap-threshold error-statistics

Parameters

Parameter	Description	Value
threshold-value	Sets the alarm threshold for error packets.	The value is an integer that ranges from 1 to 65535. **NOTE** The value should not be greater than the alarm threshold for error packets that cause the interface status to change to Error-Down configured by the **error-down-threshold error-statistics** command.
interval *interval-value*	Sets the interval for reporting alarms for error packets.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The system generates an alarm when the number of error packets received by an interface within an alarm interval exceeds the alarm threshold. If the number of received error packets is 0 in the next alarm interval, the system displays an alarm clearance message.

Example

Set the alarm threshold for error packets on GE0/0/1 to 10 and the alarm interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trap-threshold error-statistics 10 interval 30
```

4.2.105 trap-threshold interval

Function

The **trap-threshold interval** command sets the interval for reporting an alarm if packets are discarded on an interface due to a congestion.

The **undo trap-threshold interval** command restores the default interval for reporting an alarm if packets are discarded on an interface due to a congestion.

By default, the interval for reporting an alarm if packets are discarded on an interface due to a congestion is 300 seconds.

Format

trap-threshold { **input-discard** | **output-discard** } **interval** *interval-value*

undo trap-threshold { **input-discard** | **output-discard** } **interval**

Parameters

Parameter	Description	Value
input-discard	Enables the function of reporting an alarm if incoming packets are discarded on an interface due to a congestion.	-
output-discard	Enables the function of reporting an alarm if outgoing packets are discarded on an interface due to a congestion.	-

Parameter	Description	Value
interval *interval-value*	Specifies the interval for reporting an alarm.	The value is an integer ranging from 60 to 86400, in seconds. It must be an integer multiple of 10.

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion during service transmission may cause packet loss. If a lot of packets are discarded, services are affected. To improve transmission quality of service flows, you need to enable the device to report alarms to notify users of the current network status if the number of packets discarded due to a congestion in a period of time reaches the specified limit. In this case, you can run the **trap-threshold interval** command to flexibly adjust the interval for reporting an alarm if packets are discarded due to a congestion based on actual service situations. Such alarms help you know the congestion on the interface. You can determine whether to increase the bandwidth or cancel the bandwidth limit on the interface based on the logs. In this way, the congestion problem can be solved.

Precautions

After this command is run, only the interval for reporting an alarm if packets are discarded on an interface due to a congestion is set. The corresponding alarm is triggered only after the function of reporting an alarm if packets are discarded on an interface due to a congestion is enabled using the **trap-threshold enable** command and the number of discarded packets on the interface within a specified period of time reaches the alarm threshold.

If this command is executed multiple times, only the latest configuration takes effect.

Example

Set the interval for reporting an alarm if incoming packets are discarded on XGE0/0/1 due to a congestion to 80 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] trap-threshold input-discard interval 80
```

4.2.106 trap-threshold threshold

Function

The **trap-threshold threshold** command sets the alarm threshold for the number of discarded packets on an interface due to a congestion.

The **undo trap-threshold threshold** command restores the default alarm threshold for the number of discarded on an interface due to a congestion.

By default, the alarm threshold for the number of discarded packets on an interface due to a congestion is 6000.

Format

trap-threshold { **input-discard** | **output-discard** } **threshold** *threshold-value*

undo trap-threshold { **input-discard** | **output-discard** } **threshold**

Parameters

Parameter	Description	Value
input-discard	Enables the function of reporting an alarm if incoming packets are discarded on an interface due to a congestion.	-
output-discard	Enables the function of reporting an alarm if outgoing packets are discarded on an interface due to a congestion.	-
threshold-value	Specifies the alarm threshold for the number of discarded packets on an interface due to a congestion.	The value is an integer that ranges from 100 to 4294967295.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, port group view

NOTE

Only the S5736-S equipped with the S7C02000, S7Q02001, ES5D21Q02Q00 or ES5D21Q04Q01 card supports this command in the 40GE interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion during service transmission may cause packet loss. If a lot of packets are discarded, services are affected. To improve transmission quality of service flows, you need to enable the device to report alarms to notify users of the current network status if the number of packets discarded due to a congestion in a period of time reaches the specified limit. In this case, you can run the **trap-threshold threshold** command to flexibly adjust the alarm threshold for the number of discarded packets on an interface due to a congestion based on actual service situations. Such alarms help you know the congestion on the interface. You can determine whether to increase the bandwidth or cancel the bandwidth limit on the interface based on the logs. In this way, the congestion problem can be solved.

Precautions

- After this command is run, only the interval for reporting an alarm if packets are discarded on an interface due to a congestion is set. The corresponding alarm is triggered only after the function of reporting an alarm if packets are discarded on an interface due to a congestion is enabled using the **trap-threshold enable** command and the number of discarded packets on the interface within a specified period of time reaches the alarm threshold.
- If the number of discarded packets exceeds the threshold in several consecutive statistics intervals, the device only reporting an alarm in the first statistics interval, indicating that the number of discarded packets exceeds the threshold. If the number of discarded packets falls below the threshold, the device reporting an alarm indicating that the number of discarded packets falls below the threshold. If the number of discarded packets on an interface exceeds the threshold again, the device will report an alarm indicating that the number of discarded packets exceeds the threshold.
- If this command is executed multiple times, only the latest configuration takes effect.

Example

Set the alarm threshold for the number of discarded incoming packets on XGE0/0/1 due to a congestion to 200.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] trap-threshold input-discard threshold 200
```

4.2.107 virtual-cable-test

Function

The **virtual-cable-test** command tests the cable connected to an Ethernet electrical interface and displays the test result.

NOTE

The MEth management interfaces on the following devices support this command: S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, S6730S-H, S6735-S.

The service interfaces on the following devices do not support this command:

- MultiGE interfaces on the S5720-28X-PWH-LI-AC and S5736-S24UM4XC
- XGE electrical interfaces on the ES5D21X08T00 card

For the S5731-S24N4X2Q-A, S5731-S24UN4X2Q, S5731-S8UM16UN2Q, S5731S-S24N4X2Q-A1, S5731S-S24UN4X2Q-A, S5731S-S8UM16UN2Q-A, S5732-H24UM2CC (part number: 02353SJY-020, 02353SJY-021, 02353SJY-024), and S5732-H48UM2CC (part number: 02353SJT-020, 02353SJT-021, 02353SJT-023, 02353SJT-024), if the MultiGE interface is configured to work in auto-negotiation mode, and the peer interface is set to 100 Mbit/s, the local check result obtained using the **virtual-cable-test** command is inaccurate.

Format

virtual-cable-test

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the cable is faulty, the interface is in Down state or the interface rate is abnormal even if it is in Up state. You can run the **virtual-cable-test** command to check whether the cable works properly. According to the command output, you can locate and rectify cable faults.

- If the cable works properly, the total length of the cable is displayed.
- If the cable cannot work properly, the distance between the interface and the failure point is displayed.

VCT can be performed in either of the following modes:

- Common mode: The test speed is fast (about 2.5s), but the test precision is low.
- Enhanced mode: The test precision is high, but the test duration is longer (about 8s).

NOTE

For the S5736-S24T4XC, S5736-S48T4XC, S5736-S24U4XC, and S5736-S48U4XC, when ports are Up, VCT operates in common mode; when ports are Down, VCT operates in enhanced mode. Other devices support only VCT in enhanced mode.

Precautions

- The test result is only for reference and may be inaccurate for cables of some vendors.
- If the detection result is **Unknown**, you are advised to use the cable analyzer to perform the test.
- The test result is related to the cable signal attenuation. When the cable length is shorter than 3 m, the cable signal attenuation mostly is resulted from the connector, not the cable. The test result is therefore inaccurate.
- Running the **virtual-cable-test** command may affect services on the interface in a short period of time, and the interface in Up state may alternate between Up and Down.
- Combo electrical interfaces support cable tests, but cable tests are not recommended on combo electrical interfaces because services will be interrupted.
- This command can be used on an XGE optical interface or GE optical interface when the interface has a GE copper module installed.
- After a 25GE optical interface is configured to work at the rate of 1 Gbit/s using the **port mode ge** command and has a GE copper module installed, the **virtual-cable-test** command can be configured on the interface.
- When a GE electrical interface on the S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, S500, S5735-S, S5735S-S, S5735-S-I, and S5720I-SI works at a rate of 1000 Mbit/s or 100 Mbit/s and the interface is up, the detection result is inaccurate.
- On the S6720S-EI, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, and S6720-EI, when a GE electrical interface works at a rate of 100 Mbit/s, the detection result is inaccurate.
- On the S5731-H, S5731S-H, S5731-S, and S5731S-S, when a GE electrical interface works at a rate of 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s and the interface is up, the detection result is inaccurate.
- The test result is inaccurate when the interface is in the Up state or the remote interface is shut down.
- An FE electrical port uses only two pairs of wire pairs. The test result of the two pairs of wire pairs that are not used during the VCT test is inaccurate.
- When a GE electrical port works at a rate of 10 Mbit/s or 100 Mbit/s, only two pairs of cables are used to detect the VCT status. The other two pairs of cables do not detect or return the default result.
- The virtual cable test (VCT) cannot be performed on multiple interfaces of the device at the same time.

Example

Test the cable connected to Ethernet electrical interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] virtual-cable-test
Warning: The command will stop service for a while. Continue? [Y/N]y
Info: This operation may take a few seconds. Please wait for a moment..........done.
Pair A length: 189meter(s)
Pair B length: 189meter(s)
Pair C length: 189meter(s)
Pair D length: 189meter(s)
Pair A state: Ok
Pair B state: Ok
Pair C state: Ok
Pair D state: Ok
Info: The test result is only for reference.
```

Table 4-32 Description of the virtual-cable-test command output

Item	Description
Pair A/B/C/D	Four pairs of circuits in a network cable. A: orange/white and orange B: green/white and green C: blue/white and blue D: brown/white and brown

Item	Description
Pair A length	Length of a network cable: - The length is the distance between the interface and the faulty point if a fault occurs. - The length is the actual length of the cable when the cable works properly. - The length is the default length 0 m if the interface is not connected to any cable. The test result of different chips may vary, and the displayed result is for reference only. **NOTE** If the cable length is displayed as Unknown, the cable status is OK, but the cable length test result cannot be used. If the cable status is Open (indicating open circuit), the cable length in the VCT result can be used. If the remote interface is shut down, the cable length in the VCT result can be used for combo electrical interfaces on the following switches: - S5720I-SI - S5720-12TP-LI-AC, S5720-12TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720S-28TP-PWR-LI-AC, S5720-28TP-PWR-LI-AC, S5720-28TP-LI-AC, S5720-52X-LI-48S-AC, S5720-52X-LI-48S-AC1, S5720-52X-LI-48S-DC1, S5720-52X-LI-24S-AC1 If the remote interface is shut down, the cable length in the VCT result can be used for electrical interfaces on the following switches: - S5731-H - S6730-H - S6730S-H - S5720-16X-PWH-LI-AC, S5720-28X-PWH-LI-AC, S5720-28X-PWH-LI-ACF, S5720-52X-LI-48S-AC, S5720-52X-LI-48S-AC1, S5720-52X-LI-48S-DC1, S5720-52X-LI-24S-AC1

Item	Description
Pair A state	Network cable status: - Ok: indicates that the circuit pair is terminated normally. - Open: indicates that the circuit pair is not terminated. - Short: indicates that the circuit pair is short-circuited. - Crosstalk: indicates that the circuit pairs interfere with each other. - Unknown: Other unknown fault causes are detected or the detection result is inaccurate.

4.3 Logical Interface Configuration Commands

4.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

4.3.2 display interface loopback

Function

Using the **display interface loopback** command, you can view the status and traffic statistics of a loopback interface.

Format

display interface loopback [*loopback-number* | **main**]

Parameters

Parameter	Description	Value
loopback-number	Displays status and traffic statistics about a specified loopback interface. If *loopback-number* is not specified, the status and traffic statistics of all loopback interfaces are displayed.	-

Parameter	Description	Value
main	Displays status and traffic statistics about a Loopback interface. A Loopback interface has no sub-interfaces. Status and traffic statistics about a Loopback interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In the scenario where you need to monitor the status of an interface or locate an interface fault, you can use the **display interface loopback** command to collect the statistics on the interface including the status. Through the displayed information, you can collect the traffic statistics and troubleshoot the interface.

Prerequisite

A loopback interface has been created using the **interface loopback** command.

Example

Display the status and traffic statistics of a specified loopback interface.

```
<HUAWEI> display interface loopback 6
LoopBack6 current state : UP
Line protocol current state : UP (spoofing)
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.3.3/32
Current system time: 2012-02-25 09:56:04
    Last 10 seconds input rate 0 bits/sec, 0 packets/sec
    Last 10 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors,0 unknownprotocol
    Output:0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-33 Description of the **display interface loopback** command output

Item	Description
LoopBack6 current state	Physical status of a loopback interface. The physical status of a loopback interface is always Up after the loopback interface is created.
Line protocol current state	Link layer protocol status of a loopback interface. The link layer protocol status of a loopback interface is always Up after the loopback interface is created.
Description	Indicates the description of the interface, which can be set by using the **description** command.
Route Port,The Maximum Transmit Unit is 1500	Indicates the maximum transmission unit (MTU). The default MTU is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packet is discarded.
Internet Address is	Indicates the IP address of the interface.
Current system time	Indicates the current system time.
Input bandwidth utilization	Indicates the percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate for sending packets to the total bandwidth.

4.3.3 display interface null

Function

Using the **display interface null** command, you can view the status and traffic statistics of a null interface.

Format

display interface null [**0** | **main**]

Parameters

Parameter	Description	Value
0	Displays status and traffic statistics about a specified Null interface.	The value can be 0 only.

Parameter	Description	Value
main	Displays status and traffic statistics about a Null interface. A Null interface has no sub-interfaces. Status and traffic statistics about a Null interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface null** command displays the status of a null interface. The interface status information includes: the physical status, link layer protocol status, description, MTU, IP address, current system time, last time statistics about the null interface are cleared, incoming and outgoing packet rates in bit/s and pps, total numbers of packets and bytes received and sent by the null interface, and percentages of the rates for receiving and sending packets to the total bandwidth.

Precautions

There is only one null interface, namely, NULL 0.

Example

Display the status and traffic statistics of Null 0 interface.

```
<HUAWEI> display interface null 0
NULL0 current state : UP
Line protocol current state : UP (spoofing)
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Physical is NULL DEV
Current system time: 2012-02-25 10:25:59
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors,0 unknownprotocol
    Output:0 packets,0 bytes
           0 unicast,0 broadcast,0 multicast
           0 errors
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-34 Description of the display interface null command output

Item	Description
NULL0 current state	Indicates the physical status of the null interface. The physical status of the null interface is always Up.
Line protocol current state	Indicates the link layer protocol status of the interface. The protocol status of the null interface is always Up.
Description	Indicates the description of the interface, which can be set by using the **description** command.
Route Port	A Layer 3 interface.
The Maximum Transmit Unit	Indicates the MTU of the interface.
Internet protocol processing : disabled	Indicates that the Internet protocol processing is not configured.
Physical is NULL DEV	Indicates that the interface is null.
Current system time	Indicates the current system time.
Last 300 seconds input rate Last 300 seconds output rate	Indicates the rates for sending and receiving the bytes and the packets by the interface in the last five minutes.
Realtime 0 seconds input rate Realtime 0 seconds output rate	Indicates the real-time rates of sending and receiving the bytes and the packets. It refers to the interval between two **display** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. This entry is displayed only when information about a logical interface is viewed.
Input	Indicates the total number of packets and the total number of bytes received by the interface.
Output	Indicates the total number of packets and the total number of bytes sent by the interface.
Input bandwidth utilization	Indicates the percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate for sending packets to the total bandwidth.

4.3.4 display interface virtual-ethernet

Function

The **display interface virtual-ethernet** command displays status and traffic statistics about Virtual Ethernet (VE) interfaces.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display interface virtual-ethernet [*ve-number* | **main**]

Parameters

Parameter	Description	Value
ve-number	Displays status and traffic statistics about a specified VE interface. If no interface number is specified, information about all VE interfaces is displayed.	The sequence number ranges from 0 to 511.
main	Displays status and traffic statistics about a VE interface. If you do not specify the **main** parameter, status and traffic statistics about both a VE interface and VE sub-interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where you need to monitor the status of an interface or locate an interface fault, you can use the **display interface virtual-ethernet** command to collect the statistics on the interface including the status. Through the displayed information, you can collect the traffic statistics and troubleshoot the interface.

Example

Display the status and traffic statistics of VE 0/0/1.

```
<HUAWEI> display interface virtual-ethernet 0/0/1
Virtual-Ethernet0/0/1 current state : UP
```

```
Line protocol current state : UP
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is xxxx-xxxx-xxxx
Current system time: 2017-01-02 02:20:03
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
  Unicast:                    0,  Multicast:                  0
  Broadcast:                  0
Output:  0 packets, 0 bytes
  Unicast:                    0,  Multicast:                  0
  Broadcast:                  0
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 4-35 Description of the **display interface virtual-Ethernet** command output

Item	Description
Virtual-Ethernet0/0/1 current state	Physical status of the VE interface: ● UP: indicates that the interface is Up. ● DOWN: indicates that the interface is Down. ● Administratively DOWN: indicates that the administrator uses the **shutdown** command on the interface.
Line protocol current state	Indicates the link layer protocol status of the interface: ● UP: indicates that the link layer protocol on the interface is Up. ● DOWN: indicates that the link layer protocol on the interface is Down or no IP address is assigned to the interface.
Description	Description of an interface. The information allows users to know about functions of the interface and is used to identify the current interface. You can run the **description** command to configure or modify the description of an interface.
Route Port	Layer 3 interface. If this parameter specifies a Layer 2 interface, the value of this parameter will be displayed as "Switch Port". You can run the **portswitch** command to change the mode of an interface from Layer 3 to Layer 2.
The Maximum Transmit Unit is	MTU of the interface.
Internet protocol processing : disabled	No IP address is configured for the interface. If an IP address is configured for the interface, the interface's IP address and subnet mask are displayed.

Item	Description
IP Sending Frames' Format is	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address is	MAC address of the interface.
Current system time	Current system time. If the system is configured with a time zone and is in the summer daylight saving time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets that are received or sent by the interface.
Broadcast	Number of broadcast packets that are received or sent by the interface.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

4.3.5 interface loopback

Function

The **interface loopback** command creates a loopback interface.

The **undo interface loopback** command deletes a loopback interface.

Format

interface loopback *loopback-number*

undo interface loopback *loopback-number*

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a loopback interface.	The value is an integer. On the S5735S-H, S5736-S, S5735-S, S5735S-S, S5731-H, S5731S-H, S6730-H, and S6720S-S series switches, the value ranges from 0 to 1023. On the SS1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI series switches, the value ranges from 0 to 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A loopback interface is always Up.

The IP address of a loopback interface is usually specified as the source address of packets.

Example

Create loopback interface 5.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 5
[HUAWEI-LoopBack5]
```

4.3.6 interface null

Function

Using the **interface null** command, you can enter the null interface view.

Format

interface null 0

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Null0 interface never forwards or accepts any traffic. All traffic sent to this interface is directly discarded. Unnecessary traffic can be sent to the Null0 interface to avoid using ACLs.

Precautions

There is only one null interface, named null0. This interface is always Up and cannot be shut down or deleted.

Example

Enter the view of the Null0 interface.

```
<HUAWEI> system-view
[HUAWEI] interface null 0
[HUAWEI-NULL0]
```

4.3.7 interface virtual-ethernet

Function

The **interface virtual-ethernet** command displays the view of an existing virtual Ethernet (VE) interface, or creates a VE interface and displays the VE interface view.

The **undo interface virtual-ethernet** command deletes a VE interface.

By default, no VE interface is created.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

interface virtual-ethernet *ve-number*[.*subnumber*]

undo interface virtual-ethernet *ve-number* [.*subnumber*]

Parameters

Parameter	Description	Value
ve-number	Specifies the number of a VE interface.	The sequence number is an integer that ranges from 0 to 511.

Parameter	Description	Value
subnumber	Specifies the number of a VE sub-interface.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A VE interface is a logical interface with Ethernet features on a switch. VE interfaces are mainly used in scenarios where Ethernet over GRE is configured or an L2VPN accesses to an L3VPN. You need to create a VE sub-interface when configuring an L2VPN to access to an L3VPN.

Example

Create VE interface 0//0/1.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1]
```

Create VE sub-interface VE0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l3-access
[HUAWEI-Virtual-Ethernet0/0/1] quit
[HUAWEI] interface virtual-ethernet 0/0/1.1
[HUAWEI-Virtual-Ethernet0/0/1.1]
```

4.3.8 portswitch (VE interface view)

Function

The **portswitch** command changes the working mode of a virtual Ethernet (VE) interface from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of a VE interface from Layer 2 mode to Layer 3 mode.

By default, a VE interface works in Layer 3 mode.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

portswitch

undo portswitch

Parameters

None

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VE interface on the device works in Layer 3 mode. To enable Layer 2 forwarding on the VE interface, run the **portswitch** command to change the working mode to Layer 2 mode.

Precautions

- If an interface has the non-attribute configuration, this command cannot be executed. Before running this command, delete the non-attribute configuration on the interface.
- The minimum interval between running the **portswitch** and **undo portswitch** commands must be 30s.

Example

Change VE0/0/1 to Layer 2 mode.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] portswitch
```

4.3.9 statistic enable (sub-interface view)

Function

The **statistic enable** command enables traffic statistics collection on a sub-interface.

The **undo statistic enable** command disables traffic statistics collection on a sub-interface.

By default, traffic statistics collection is disabled on a sub-interface.

NOTE

This configuration is supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S and S6730S-S.

For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: Configuring traffic statistics collection on sub-interfaces may affect the forwarding performance. For example, some packets may be discarded when all interfaces forward packets at the line rate. Therefore, configure traffic statistics collection on sub-interfaces if necessary.

Format

statistic enable { **both** | **inbound** | **outbound** }

undo statistic enable { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
both	Enables traffic statistics collection for incoming and outgoing traffic.	-
inbound	Enables traffic statistics collection for incoming traffic.	-
outbound	Enables traffic statistics collection for outgoing traffic.	-

Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or troubleshoot network faults, enable traffic statistics collection on a sub-interface. The device then collects traffic statistics on the sub-interface.

Precautions

- After you run the **undo statistic enable** command to disable traffic statistics collection on a sub-interface, traffic statistics collection on the sub-interface is stopped and the collected traffic statistics are cleared.

- Traffic statistics collection on sub-interfaces occupies a device's limited ACL resources. If this function is enabled on too many sub-interfaces, other services may fail to obtain ACL resources.
- Traffic statistics collection on sub-interfaces is unavailable for error packets.
- The device supports traffic statistics collection on a maximum of 4096 sub-interfaces.
- VXLAN Layer 2 sub-interfaces do not support traffic statistics collection.

Example

Enable traffic statistics collection for incoming and outgoing traffic on the sub-interface GigabitEthernet1/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1.1
[HUAWEI-GigabitEthernet1/0/1.1] statistic enable both
```

4.3.10 trigger trap

Function

Using the **trigger trap** command, you can configure an interface to send traps to the NMS.

Format

trigger trap { **linkup** | **linkdown** }

Parameters

Parameter	Description	Value
linkup	Sends the LinkUp trap to the NMS.	-
linkdown	Sends the LinkDown trap to the NMS.	-

Views

Loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traps configured by **trigger trap** are used to check whether the network between the NMS and device functions properly. If the NMS receives a trap sent from the interface, the network between the NMS and device functions properly; otherwise, a fault may occur on the network.

Prerequisites

Run the **snmp-agent trap enable feature-name** command to enable the LinkUp and LinkDown traps.

Precautions

The **trigger trap** command is used on loopback interfaces to check the network between the NMS and device. The interface status does not change according to the meaning of the trap. For example, if the **trigger trap linkdown** command is used, the loopback interface sends a LinkDown trap to the NMS but does not change its status to Down. If you have used the **trigger trap linkdown** command, you must run the **trigger trap linkup** command to clear the LinkDown trap on the NMS.

Example

Configure a loopback interface to send the LinkUp trap to the NMS.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] trigger trap linkup
```

5 Ethernet Switching Configuration Commands

5.1 MAC Address Table Configuration Commands

5.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.1.2 display bridge mac-address

Function

The **display bridge mac-address** command displays the bridge MAC address of a device.

Format

display bridge mac-address

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you need to view the bridge MAC address of a device, run the **display bridge mac-address** command.

Example

Display the bridge MAC address of a device.

```
<HUAWEI> display bridge mac-address
System bridge MAC address: 00e0-fc4b-6d00
```

Table 5-1 Description of the display bridge mac-address command output

Item	Description
System bridge MAC address	Indicates the bridge MAC address of a device.

5.1.3 display mac-address

Function

The **display mac-address** command displays the MAC address table of the switch. A MAC address entry contains the destination MAC address, VLAN ID/VSI/BD, outbound interface, and entry type.

Format

display mac-address [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**]

display mac-address [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in an entry.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter less than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Displays MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays MAC address entries in a specified VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface-type interface-number	Displays the MAC address entries with a specified outbound interface. - *interface-type* specifies the type of the outbound interface. - *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The **display mac-address** command displays all MAC address entries, such as dynamic MAC address entries, static MAC address entries, and blackhole MAC address entries. A MAC address entry contains the destination MAC address, VLAN ID/VSI/BD, outbound interface, and entry type.

Follow-up Procedure

If any MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address static** command to add a correct one.

Precautions

If you run the **display mac-address** command without parameters, all MAC address entries are displayed.

When the switch has a large number of MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all MAC address entries.

```
<HUAWEI> display mac-address
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                  Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc12-3458       100/-/-                      GE0/0/1             dynamic
00e0-fc12-3457       200/-/-                      GE0/0/2             static
-------------------------------------------------------------------------------
Total items displayed = 2
```

Display detailed information about all MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc12-3457          VLAN : 10
Learned-From: GE0/0/2                 Type : dynamic

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 5-2 Description of the **display mac-address** command output

Item	Description
MAC Address	Destination MAC address in a MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.

Item	Description
Type	Type of a MAC address entry. - static: indicates a static MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address static vlan**, **mac-address static vlanif**, **mac-address static vsi**, **mac-address static bridge-domain**, or **mac-address static bridge-domain vni** command. - blackhole: indicates a blackhole MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address blackhole** command. - dynamic: indicates a MAC address entry learned by the switch, which will be aged out when the aging time expires. - security: indicates a MAC address entry that an interface learns after port security is enabled. - sec-config: indicates a static secure MAC address entry configured by using the **port-security mac-address** command. - sticky: indicates a MAC address entry that an interface learns after the sticky MAC function is enabled. - mux: indicates a MAC address entry learned by a MUX VLAN enabled interface. - snooping: indicates a static MAC address entry generated based on the dynamic DHCP snooping binding table. - authen: indicates a MAC address entry corresponding to the NAC authentication user that obtains an IP address (excluding the Layer 3 authentication user of which the MAC address cannot be generated and wireless user in direct forwarding mode). - evpn: indicates a MAC address entry of EVPN. - sticky-config: indicates a MAC address entry configured through the **port-security mac-address sticky-config** command.

5.1.4 display mac-address aging-time

Function

The **display mac-address aging-time** command displays the aging time of dynamic MAC address entries in the MAC address table.

Format

display mac-address aging-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays the aging time of dynamic MAC address entries on the switch. You can check whether the aging time is suitable for network requirements and device performance.

Follow-up Procedure

If the aging time is unsuitable for requirements or device performance, run the **mac-address aging-time** command to set the aging time properly.

Precautions

If the aging time is 0, dynamic MAC addresses will not be aged out. In this case, MAC address entries increase sharply and the MAC address table will be full quickly.

Example

Display the aging time of dynamic MAC address entries.

```
<HUAWEI> display mac-address aging-time
  Aging time: 300 second(s)
```

Table 5-3 Description of the display mac-address aging-time command output

Item	Description
Aging time	Aging time of dynamic MAC address entries, in seconds. To set the aging time, run the **mac-address aging-time** command.

5.1.5 display mac-address blackhole

Function

The **display mac-address blackhole** command displays blackhole MAC address entries.

Format

display mac-address blackhole [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays blackhole MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays blackhole MAC address entries of a specified virtual switch instance (VSI). *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about blackhole MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The MAC address table contains the following MAC address entries:

- Blackhole MAC address entries that are used to discard packets with the specified MAC addresses or destination MAC addresses. Blackhole MAC address entries are manually configured and will not be aged out.
- Static MAC entries that are manually configured and will not be aged out.
- Dynamic MAC address entries that are learned by the switch and will be aged out when the aging time expires.

To check whether blackhole MAC address entries are configured correctly, run this command. These entries ensure communication between authorized users.

Follow-up Procedure

If any blackhole MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address blackhole** command to add a correct one.

Precautions

- If you run the **display mac-address blackhole** command without parameters, all blackhole MAC address entries are displayed.
- If the MAC address table does not contain any blackhole MAC address, no information is displayed.

Example

Display all blackhole MAC address entries.

```
<HUAWEI> display mac-address blackhole
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                 Learned-From         Type
-------------------------------------------------------------------------------
00e0-fc22-0033       100/-/-                   -                  blackhole
00e0-fc00-0001       200/-/-                   -                  blackhole

-------------------------------------------------------------------------------
Total items displayed = 2
```

Display blackhole MAC address entries in VLAN 100.

```
<HUAWEI> display mac-address blackhole vlan 100
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                  Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc22-0033       100/-/-                    -                  blackhole
00e0-fc00-0001       100/-/-                    -                  blackhole

-------------------------------------------------------------------------------
Total items displayed = 2
```

Table 5-4 Description of the display mac-address blackhole command output

Item	Description
MAC Address	Destination MAC address in a blackhole MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	When the type of a MAC address entry is blackhole, "-" is displayed.

Item	Description
Type	Type of a MAC address entry. blackhole: indicates a blackhole MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address blackhole** command.

5.1.6 display mac-address dynamic

Function

The **display mac-address dynamic** command displays dynamic MAC address entries.

Format

display mac-address dynamic [[**slot**] *slot-id*] [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

display mac-address dynamic [[**slot**] *slot-id*] [**vsi** *vsi-name* [**peer** *ip-address*]] [**verbose**]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays dynamic MAC address entries on a specified card.	The value is an integer and must be the slot ID of a running card.
vlan *vlan-id*	Displays dynamic MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays dynamic MAC address entries of a specified virtual switch instance (VSI). *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
peer *ip-address*	Displays the dynamic MAC address entry mapped to a specified peer IPv4 address. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	-
interface-type interface-number	Displays dynamic MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about dynamic MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table needs to be updated constantly because the network topology always changes. You can use this command to view learned MAC addresses in real time.

Follow-up Procedure

If the displayed dynamic MAC address entries are invalid, run the **undo mac-address** command to delete dynamic MAC address entries.

Precautions

If you run the **display mac-address dynamic** command without parameters, all dynamic MAC address entries are displayed.

If the MAC address table does not contain any dynamic MAC address entry, no information is displayed.

When the switch has a large number of dynamic MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all dynamic MAC address entries.

```
<HUAWEI> display mac-address dynamic
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc22-0033       100/-/-                    GE0/0/1           dynamic
00e0-fc00-0001       200/-/-                    GE0/0/2           dynamic

-------------------------------------------------------------------------------
Total items displayed = 2
```

Display all dynamic MAC address entries in VLAN 9.

```
<HUAWEI> display mac-address dynamic  vlan 9
-------------------------------------------------------------------------------
MAC Address      VLAN/VSI/BD                       Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc07-0122   9/-/-                          GE0/0/1            dynamic
00e0-fc07-0106   9/-/-                          GE0/0/1            dynamic
00e0-fc07-0114   9/-/-                          GE0/0/1            dynamic

-------------------------------------------------------------------------------
Total items displayed = 3
```

Display detailed information about all dynamic MAC address entries in VLAN 9.

```
<HUAWEI> display mac-address dynamic vlan 9 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc07-0117           VLAN: 9
Learned-From: GE0/0/1                Type: dynamic

MAC Address : 00e0-fc07-0133           VLAN: 9
Learned-From: GE0/0/1                Type: dynamic

MAC Address : 00e0-fc07-0121           VLAN: 9
Learned-From: GE0/0/1                Type: dynamic

-------------------------------------------------------------------------------
Total items  displayed = 3
```

Table 5-5 Description of the display mac-address dynamic command output

Item	Description
MAC Address	Destination MAC address in a dynamic MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. dynamic: indicates a MAC address entry learned by the switch, which will be aged out when the aging time expires.

5.1.7 display mac-address flapping

Function

The **display mac-address flapping** command displays the configuration of MAC address flapping detection.

Format

display mac-address flapping

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MAC address flapping detection is configured, you can run the **display mac-address flapping** command to check the configuration.

The command output includes the following information:

- Whether MAC address flapping detection is configured.
- Aging time of flapping MAC addresses.
- Delay time before the interface joins a VLAN again after it is removed from the VLAN.

- VLAN that does not require MAC address flapping detection.
- List of VLANs of three security levels defined for MAC address flapping detection

Example

Display the configuration of MAC address flapping detection.

```
<HUAWEI> display mac-address flapping
MAC address Flapping Configurations :
----------------------------------------------------------------------------
  Flapping detection          : Enable
  Aging time(sec)             : 300
  Quit VLAN Recover time(min) : 10
  Exclude VLAN list           : -
  Low level VLAN list         : -
  Middle level VLAN list      : 1 to 4094
  High level VLAN list        : -
----------------------------------------------------------------------------
```

Table 5-6 Description of the display mac-address flapping command output

Item	Description
Flapping detection	MAC address flapping detection status: - Enable: MAC address flapping detection is enabled. - Disable: MAC address flapping detection is disabled. To specify the parameter, run the **mac-address flapping detection** command.
Aging time(sec)	Aging time of flapping MAC addresses. To specify the parameter, run the **mac-address flapping aging-time** command.
Quit VLAN Recover time(min)	Delay time before the interface joins a VLAN again after it is removed from the VLAN. To specify the parameter, run the **mac-address flapping quit-vlan recover-time** command. The default value is 10. If the value is 0, the interface cannot join a VLAN again after it is removed from the VLAN.
Exclude VLAN list	VLAN that does not require MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection exclude vlan** command. If such a VLAN is specified, the VLAN ID is displayed. If the VLAN is not specified, this field is displayed as -.
Low level VLAN list	List of VLANs of low security level defined for MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection vlan security-level** command.

Item	Description
Middle level VLAN list	List of VLANs of middle security level defined for MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection vlan security-level** command.
High level VLAN list	List of VLANs of high security level defined for MAC address flapping detection. To specify the parameter, run the **mac-address flapping detection vlan security-level** command.

5.1.8 display mac-address flapping record

Function

The **display mac-address flapping record** command displays MAC address flapping records.

Format

display mac-address flapping record [**slot** *slot-id*] [**begin** *YYYY/MM/DD HH:MM:SS*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
begin *YYYY/MM/DD HH:MM:SS*	Displays MAC address flapping records generated from the specified time to the current time. *YYYY/MM/DD* indicates year/month/date. *HH:MM:SS* indicates hour:minute:second.	• *YYYY/MM/DD* ranges from 2000/01/01 to 2099/12/31. • *HH:MM:SS* ranges from 00:00:00 to 23:59:59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display mac-address flapping record** command output helps locate the position where MAC address flapping occurs.

Precautions

The command output is displayed only when MAC address flapping has occurred.

Example

Display all MAC address flapping records.

```
<HUAWEI> display mac-address flapping record
 S  : start time
 E  : end time
(Q) : quit VLAN
(D) : error down
-------------------------------------------------------------------------------
Move-Time             VLAN  MAC-Address   Original-Port Move-Ports   MoveNum
-------------------------------------------------------------------------------
S:2011-08-31 17:22:36 300  00e0-fc12-3456 Eth-Trunk1   Eth-Trunk2   81
E:2011-08-31 17:22:44

-------------------------------------------------------------------------------
Total items on slot 0: 1
```

Display MAC address flapping records generated from 2012/06/04 09:00:00 to the current time.

```
<HUAWEI> display mac-address flapping record begin 2012/06/04 09:00:00
 S  : start time
 E  : end time
(Q) : quit VLAN
(D) : error down
-------------------------------------------------------------------------------
Move-Time                 VLAN MAC-Address   Original-Port Move-Ports   MoveNum
-------------------------------------------------------------------------------
S:2012-06-04 17:22:38 300  00e0-fc12-3456 Eth-Trunk2   Eth-Trunk1   5
E:2012-06-04 17:22:42

-------------------------------------------------------------------------------
Total items on slot 0: 1
```

Table 5-7 Description of the display mac-address flapping record command output

Item	Description
Move-Time	Start time and end time MAC address flapping occurs. If the DST is configured, the DST plus the flapping start time or end time is displayed, for example: StartTime: 2012-02-02 15:54:10 DST.
VLAN	VLAN where MAC address flapping occurs.

Item	Description
MAC-Address	Flapping MAC address. **NOTE** Only one MAC address that flaps is displayed for the same VLAN on the same device.
Original-Port	Port that learns the MAC address first.
Move-Ports	Ports that learn the MAC address later.
MoveNum	Number of times the MAC address has flapped. The maximum value is 65535. When the number of times the MAC address has flapped exceeds 65535, the MoveNum field still displays 65535.

5.1.9 display mac-address hash-conflict record

Function

The **display mac-address hash-conflict record** command displays records of MAC address hash conflicts.

Format

display mac-address hash-conflict record [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	Set this parameter based on the actual device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Application Scenarios

When MAC address hash conflicts occur on the network, you can run this command to view conflict records.

Precautions

A maximum of 100 MAC address hash conflict records can be displayed. The latest 100 records are retained in time sequence.

Example

Display MAC address hash conflict records of slot 0.

```
<HUAWEI> display mac-address hash-conflict record slot 0
-----------------------------------------------------------------------------
 Time                   MAC Address         VLAN/VSI/BD     InterfaceName
-----------------------------------------------------------------------------
 2019-11-21 09:25:38     00e0-fc00-0004      4011/-/-        XGE0/0/5
 2019-11-21 09:25:38     00e0-fc00-0009      4011/-/-        XGE0/0/5
 2019-11-21 09:26:40     00e0-fc00-0003      -/-/10         XGE0/0/5
 2019-11-21 09:26:40     00e0-fc00-0008      -/-/10         XGE0/0/5
 2019-11-21 09:26:40     00e0-fc00-0001      -/-/10         XGE0/0/5
-----------------------------------------------------------------------------
Total items on slot 0: 5
```

Table 5-8 Description of the **display mac-address hash-conflict record** command output

Item	Description
Time	Time when a MAC address hash conflict occurs.
MAC Address	MAC address.
VLAN/VSI/BD	ID of the VLAN or name of the VSIor ID of the BD to which the MAC address belongs.
InterfaceName	Interface name.

5.1.10 display mac-address hash-mode

Function

The **display mac-address hash-mode** command displays the running hash mode and configured hash mode on the device.

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

display mac-address hash-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a hash mode is configured, you can run the **display mac-address hash-mode** command to check the configuration.

Precautions

After the hash algorithm is changed, restart the device for the configuration to take effect.

Example

Display the running hash mode and configured hash mode on the device.

```
<HUAWEI> display mac-address hash-mode
  MAC address hash mode status:
--------------------------------------------
 Slot       CurMode         CfgMode
--------------------------------------------
 0         crc16-lower     crc32-lower
--------------------------------------------
```

Table 5-9 Description of the display mac-address hash-mode command output

Item	Description
Slot	Slot ID.
CurMode	Running hash mode on the device. After changing the hash algorithm and saving the configuration, restart the device for the configuration to take effect.
CfgMode	Configured hash mode on the device. To specify the parameter, run the **mac-address hash-mode** command.

5.1.11 display mac-address mux

Function

The **display mac-address mux** command displays MUX MAC address entries.

Format

display mac-address mux [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MUX MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MUX MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about MUX MAC address entries. If this parameter is not specified, brief information about MUX MAC address entries is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. A MUX MAC address entry is learned by a MUX VLAN enabled interface. The learned MUX MAC address entries are deleted after the switch restarts.

After configuring the MUX VLAN function, you can run the **display mac-address mux** command to check whether the learned MUX MAC address entries are correct.

Follow-up Procedure

If the displayed MUX MAC address entries are invalid, run the **undo mac-address** command to delete MUX MAC address entries.

Precautions

If you run the **display mac-address mux** command without parameters, all MUX MAC address entries are displayed.

If the MAC address table does not contain any MUX MAC address entry, no information is displayed.

When the switch has a large number of MUX MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all MUX MAC address entries.

```
<HUAWEI> display mac-address mux
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD               Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc12-3456       100/-/-                   GE0/0/2           mux

-------------------------------------------------------------------------------
Total items displayed = 1
```

Display detailed information about all MUX MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address mux vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc12-3457           VLAN : 10
Learned-From: GE0/0/2                  Type : mux


-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 5-10 Description of the display mac-address mux command output

Item	Description
MAC Address	Destination MAC address in a MUX MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the virtual switch instance (VSI), or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.

Item	Description
Type	Type of a MAC address entry. mux: indicates a MAC address entry learned by a MUX VLAN enabled interface.

5.1.12 display mac-address oam

Function

The **display mac-address oam** command displays information about MAC address entries of the OAM type.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display mac-address oam

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

VPLS data forwarding depends on MAC address learning. Data packets in a VPLS domain can be correctly forwarded only when the MAC addresses of the data packets are correctly learned by PEs.

VPLS MAC diagnostic tools can be used to check whether MAC address learning works properly on the devices in a VPLS domain. VPLS MAC diagnostic tools include MAC populate and MAC purge.

- MAC populate is used to check whether MAC addresses can be learned by devices in a VSI by populating an OAM MAC address into the VPLS domain.

  If the devices in a specified VSI in the VPLS domain have learned the populated MAC address, running the **display mac-address oam** command can display detailed information about the populated OAM MAC address.

- MAC purge is used to purge the populated OAM MAC address.

  If the learned OAM MAC address is purged on the device, running the **display mac-address oam** command can show that the learned OAM MAC address has been purged.

Prerequisites

- Configuring the diagnosis of the OAM MAC address learning capacity is completed before you check detailed information about the populated OAM MAC address.
- Purging the OAM MAC address learned by the devices on the VPLS network is completed before you check whether the OAM MAC has been purged.

Example

Display MAC address entries of the OAM type in the MAC address table.

```
<HUAWEI> display mac-address oam
-------------------------------------------------------------------------------------------
MAC Address     VLAN/VSI/BD             Learned-From          Type
-------------------------------------------------------------------------------------------
00e0-fc00-0010  -/vsi1/-             GigabitEthernet0/0/1  OAM-PU
00e0-fc00-0020  -/vsi1/-             GigabitEthernet0/0/1  OAM-PO

-------------------------------------------------------------------------------------------
Total items displayed = 2
```

Table 5-11 Description of the **display mac-address oam** command output

Item	Description
MAC Address	Indicates the MAC address of the OAM type.
VLAN/VSI/BD	• VLAN: the value is always displayed as "-". • VSI: indicates the VSI to which the MAC addresses of the OAM type belong. • BD: the value is always displayed as "-".
Learned-From	Indicates an interface on which the MAC addresses of the OAM type are configured.
Type	Indicates the OAM type of the MAC address. • **OAM-PU**: indicates the OAM MAC address entry that is used to discard data frames containing a specified destination MAC address, configured by using the **mac-purge** command. • **OAM-PO**: indicates the OAM MAC address entry that is used to test whether the function of learning dynamic MAC addresses is normal on the device. The entry is displayed as the dynamic MAC address on the device. In addition, the entry, the same as a common dynamic MAC address, supports VPLS forwarding, configured by using the **mac-populate** command.

5.1.13 display mac-address static

Function

The **display mac-address static** command displays static MAC address entries.

Format

display mac-address static [**vsi** *vsi-name*] [**verbose**]

display mac-address static [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays static MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays static MAC address entries in a specified VSI. *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Displays the static MAC address entries on a specified interface.	-
verbose	Displays detailed information about static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The MAC address table contains the following MAC address entries:

- Static MAC entries that are manually configured and will not be aged out.
- Blackhole MAC address entries that are used to discard packets with the specified source MAC addresses or destination MAC addresses. Blackhole MAC address entries are manually configured and will not be aged out.
- Dynamic MAC address entries that are learned by the switch and will be aged out when the aging time expires.

To improve network security, configure static MAC address entries to ensure that packets destined for specified MAC addresses are forwarded by the specified interfaces. This prevents attack packets with bogus MAC addresses and guarantees communication between the switch and the upstream device or server. After configuring static MAC address entries, you can run the **display mac-address static** command to verify the configuration.

Follow-up Procedure

If any static MAC address entry is incorrect, run the **undo mac-address** command to delete it.

Precautions

If you run the **display mac-address static** command without parameters, all static MAC address entries are displayed.

If the MAC address table does not contain any static MAC address entry, no information is displayed.

Example

Display all static MAC address entries.

```
<HUAWEI> display mac-address static
-------------------------------------------------------------------------------
MAC Address          VLAN/VSI/BD                 Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc00-0033       100/-/-                     GE0/0/1           static
00e0-fc00-0001       200/-/-                     GE0/0/2           static

-------------------------------------------------------------------------------
Total items displayed = 2
```

Display detailed information about all static MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address static vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc00-0001            VLAN : 10
Learned-From: GE0/0/1                 Type : static

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 5-12 Description of the display mac-address static command output

Item	Description
MAC Address	Destination MAC address in a static MAC address entry.
VLAN/VSI/BD	ID of the VLAN, or name of the VSI, or ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. static: indicates a static MAC address entry, which is manually configured and will not be aged out, configured by using the **mac-address static vlan**, **mac-address static vlanif**, **mac-address static vsi**, **mac-address static bridge-domain**, or **mac-address static bridge-domain vni** command.

5.1.14 display mac-address summary

Function

The **display mac-address summary** command displays statistics on MAC address entries.

Format

display mac-address summary [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays statistics on MAC address entries on a specified card.	The value is an integer and must be the slot ID of a running card.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the device stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

When the switch has many MAC address entries of different types.

Precautions

- If **slot** *slot-id* is specified, this command displays statistics on MAC address entries on the specified card. If this parameter is not specified, this command displays statistics on MAC address entries on all cards.
- If no static or blackhole MAC addresses are configured on the device, statistics about the two types of MAC address entries are 0.
- Blackhole MAC address entries fall into global and VLAN- or VSI-based blackhole MAC address entries. Global blackhole MAC address entries are configured using the **mac-address blackhole** command with only a MAC address specified. They do not occupy the MAC address table space.
- If MAC address learning is disabled on the device, statistics about dynamic MAC address entries are 0.

  Using the **undo mac-address learning disable** command in the Ethernet interface view can enable MAC address learning.

Example

View statistics on all MAC address entries in the system.

```
<HUAWEI> display mac-address summary
Summary information of slot 0:
-----------------------------------
Static        :              2
Blackhole     :              0
Dyn-Local     :              0
Dyn-Remote    :              0
Dyn-Trunk     :              0
Sticky        :              0
Security      :              0
Sec-config    :              0
Authen        :              0
Guest         :              0
Mux           :              0
Snooping      :              0
Pre-Mac       :              0
Evpn          :              0
Sticky-config :              0
In-used       :              5
Capacity      :              32768
-----------------------------------
```

Table 5-13 Description of the **display mac-address summary** command output

Item	Description
Static	Number of static MAC address entries.
Blackhole	Number of blackhole MAC address entries.
Dyn-Local	Number of MAC address entries learned by the local card.

Item	Description
Dyn-Remote	Number of MAC address entries synchronized from other cards.
Dyn-Trunk	Total number of MAC address entries learned by all trunk interfaces.
Sticky	Number of sticky MAC address entries.
Security	Number of secure dynamic MAC address entries.
Sec-config	Number of secure static MAC address entries.
Authen	Number of MAC address entries corresponding to authentication users.
Guest	Number of MAC address entries learned by interfaces in the guest VLAN.
Mux	Number of MAC address entries learned by interfaces enabled with the MUX VLAN function.
Snooping	Number of Snooping MAC address entries.
Pre-Mac	Number of Pre-authen MAC address entries.
Evpn	Number of EVPN MAC address entries.
Sticky-config	Number of MAC address entries of the sticky-config type.
In-used	Total number of existing MAC address entries. **NOTE** Global blackhole MAC address entries do not occupy the MAC address table space. If these MAC address entries are configured on the device, the In-used value may be greater than the Capacity value.
Capacity	Capacity of the MAC address table. The actual value varies according to device models.

5.1.15 display mac-address total-number

Function

The **display mac-address total-number** command displays the number of MAC address entries of a specified type.

Format

display mac-address total-number [**slot** *slot-id*]

display mac-address total-number [**vsi** *vsi-name*]

display mac-address total-number [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number vlan all

display mac-address total-number { **mux** | **security** | **sticky** | **sec-config** | **snooping** | **pre-authen** | **authen** | **sticky-config** } [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number blackhole [**vlan** *vlan-id* | **vsi** *vsi-name*]

display mac-address total-number dynamic [**slot** *slot-id*] [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number dynamic [**slot** *slot-id*] [**vsi** *vsi-name*]

display mac-address total-number static [**vlan** *vlan-id* | *interface-type interface-number*] *

display mac-address total-number static vsi *vsi-name*

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the number of MAC address entries on a specified card.	The value is an integer and must be the slot ID of a running card.
mux	Displays the number of MUX MAC address entries.	-
dynamic	Displays the number of dynamic MAC address entries.	-
security	Displays the number of secure dynamic MAC address entries.	-
sec-config	Displays the number of secure static MAC address entries.	-
snooping	Displays the number of static MAC address entries generated based on the dynamic DHCP snooping binding table.	-
pre-authen	Displays the number of static MAC address entries corresponding to a user in pre-connection state after NAC authentication is enabled.	-

Parameter	Description	Value
authen	Displays the number of static MAC address entries that is generated after a user passes NAC authentication.	-
sticky-config	Displays the number of MAC address entries of the sticky-config type.	-
sticky	Displays the number of sticky MAC address entries.	-
blackhole	Displays the number of blackhole MAC address entries.	-
static	Displays the number of static MAC address entries.	-
vlan *vlan-id*	Displays the number of MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vlan all	Displays the number of MAC address entries in all VLANs.	-
interface-type interface-number	Displays the number of MAC address entries learned by a specified interface.	-
vsi *vsi-name*	Displays the number of MAC address entries in a specified VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

When the switch has many MAC address entries of different types, you can use the **display mac-address total-number** command to view statistics on MAC address entries of a specified type.

Precautions

If no parameter is specified, the total number of MAC address entries in the system is displayed.

If no interface is specified in the **display mac-address total-number** command, the total number of MAC address entries learned by all interfaces is displayed.

If an interface is specified in the **display mac-address total-number** command, the total number of MAC address entries in the VLAN where the interface resides is displayed.

If no VLAN is specified in the **display mac-address total-number** command, the total number of MAC address entries in all VLANs is displayed.

Example

Display the number of dynamic MAC address entries.

```
<HUAWEI> display mac-address total-number dynamic
Total number of MAC address : 20
```

Table 5-14 Description of the **display mac-address total-number** command output

Item	Description
Total number of MAC address	Total number of MAC address entries in the system.

5.1.16 display mac-limit

Function

The **display mac-limit** command displays the rules that limit the number of learned MAC addresses.

Format

display mac-limit [*interface-type interface-number* | **vlan** *vlan-id* | **vsi** *vsi-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the MAC address limiting rule on a specified interface. - *interface-type* specifies the type of the interface. - *interface-number* specifies the number of the interface.	-
vlan *vlan-id*	Displays the MAC address limiting rules in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays the MAC address limiting rules in a specified VSI. *vsi-name* specifies the name of a VSI. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether MAC address limiting rules are configured correctly, run the **display mac-limit** command. If a rule is incorrect, run the **mac-limit** command to modify the rule or run the **undo mac-limit all** command to delete it.

Precautions

If no parameter is specified, MAC address learning limit rules of all interfaces, VSIs, and VLANs are displayed.

Example

Display the MAC address limiting rule on GigabitEthernet0/0/1.

```
<HUAWEI> display mac-limit GigabitEthernet 0/0/1
GigabitEthernet0/0/1 MAC limit:
  Maximum MAC count 1000, used count 0
  Action: forward, Alarm: enable
```

Display all the MAC address limiting rules.

```
<HUAWEI> display mac-limit
MAC Limit is enabled
Total MAC Limit rule count : 1

PORT                VLAN/VSI/SI       SLOT Maximum Rate(ms) Action  Alarm
--------------------------------------------------------------------------------
GE0/0/1              -                 -    100     -        forward enable
```

Table 5-15 Description of the display mac-limit command output

Item	Description
GigabitEthernet 0/0/1 MAC limit:	MAC address limiting rule for the interface. To specify the parameters, run the **mac-limit** command.
Maximum MAC count	Maximum number of MAC addresses that can be learned.
used count	Number of MAC addresses that have been learned.
Total MAC Limit rule count	Number of configured MAC address limiting rules.
PORT	Name of an interface.
VLAN/VSI/SI	ID of a VLAN VSI name, or service instance (SI) name.
SLOT	Slot ID of the card where a MAC address limiting rule is configured.
Maximum	Maximum number of MAC addresses that can be learned. To set the maximum number of MAC addresses, run the **mac-limit** command.
Rate(ms)	Indicates the interval at which MAC addresses are learned.
Action	Action performed on packets when the number of learned MAC addresses exceeds the maximum. The value **forward** indicates that packets are forwarded with new source MAC addresses.

Item	Description
Alarm	Whether an alarm is generated when the number of learned MAC addresses exceeds the maximum. ● enable: indicates that an alarm is generated. ● disable: indicates that an alarm is not generated.

5.1.17 drop illegal-mac alarm

Function

The **drop illegal-mac alarm** command configures the switch to send a trap to the network management system (NMS) when receiving a packet with an all-0 MAC address.

The **undo drop illegal-mac alarm** command deletes the configuration.

By default, the switch does not send a trap to the NMS when receiving a packet with an all-0 MAC address.

Format

drop illegal-mac alarm

undo drop illegal-mac alarm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some legacy computers or network devices may send packets with an all-0 source or destination MAC address when their network adapters fail. The **drop illegal-mac alarm** command configures the switch to send a trap to the NMS when receiving a packet with an all-0 MAC address. You can locate the faulty network adapter according to the trap message.

Precautions

If the alarm function is disabled on the switch, the NMS cannot receive any trap message.

After you run the **drop illegal-mac alarm** command, the switch sends a trap only once after receiving packets with an all-0 MAC address. To configure the switch to send traps continuously, run the **drop illegal-mac alarm** command repeatedly.

This command and IPv6 over IPv4 cannot be configured simultaneously on the S6720S-S, S5735S-H, S5736-S, and S5720I-SI.

Example

Configure the switch to send a trap to the NMS when receiving a packet with an all-0 MAC address.

```
<HUAWEI> system-view
[HUAWEI] drop illegal-mac alarm
```

5.1.18 drop illegal-mac enable

Function

The **drop illegal-mac enable** command enables the switch to discard packets with an all-0 invalid MAC address.

The **undo drop illegal-mac enable** command disables the switch from discarding packets with an all-0 invalid MAC address.

By default, the switch does not discard packets with an all-0 MAC address.

Format

drop illegal-mac enable

undo drop illegal-mac enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some legacy computers or network devices may send packets with an all-0 source or destination MAC address when their network adapters fail. You can run the **drop illegal-mac enable** command to configure the switch to discard such packets. After receiving the packets with an all-0 source or destination MAC address, the switch discards the packets.

This command reduces incorrect MAC address entries on the device.

Precautions

If the alarm function is disabled on the device, the network management system cannot receive any alarm message.

Example

Configure the switch to discard packets with an all-0 invalid MAC address.

```
<HUAWEI> system-view
[HUAWEI] drop illegal-mac enable
```

5.1.19 mac-address aging-time

Function

The **mac-address aging-time** command sets the aging time of dynamic MAC address entries.

The **undo mac-address aging-time** command restores the default aging time of dynamic MAC address entries.

By default, the aging time of dynamic MAC address entries is 300 seconds.

Format

mac-address aging-time *aging-time*

undo mac-address aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of dynamic MAC address entries.	The value is 0 or an integer that ranges from 10 to 1000000, in seconds. The default value is 300. The value 0 indicates that dynamic MAC address entries will not be aged out.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network topology changes frequently, and the switch will learn many MAC addresses. You can run the **mac-address aging-time** command to set a proper aging time for dynamic MAC address entries so that aged MAC address entries are deleted from the MAC address table. This reduces MAC address entries in the MAC address table.

The system starts an aging timer for each dynamic MAC address entry. If a dynamic MAC address entry is not updated within a certain period (twice the aging time), the entry is deleted. If the entry is updated within this period, the aging timer of this entry is reset. If the aging time is short, the switch is sensitive to network changes.

When setting the aging time of dynamic MAC address entries, follow these rules:

- Set a longer aging time on a stable network and a shorter aging time on an unstable network.
- The capacity of the MAC address table on a low-end device is small; therefore, set a relatively short aging time on low end devices to save the MAC address table space.

Precautions

- Dynamic MAC address entries are lost after system restart. Static MAC address entries and blackhole MAC address entries are not aged or lost.
- If the aging time is 0, dynamic MAC address entries will not be aged out. In this case, MAC address entries increase sharply and the MAC address table will be full quickly.
- If you run the **mac-address aging-time** command multiple times, only the latest configuration takes effect.
- If a MAC address entry is always matched to direct traffic forwarding, this entry will not be aged out.

Example

Set the aging time of dynamic MAC address entries to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-address aging-time 500
```

5.1.20 mac-address blackhole

Function

The **mac-address blackhole** command configures a blackhole MAC address entry.

The **undo mac-address blackhole** command deletes a blackhole MAC address entry.

By default, no blackhole MAC address entry is configured.

Format

mac-address blackhole *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name*]

undo mac-address blackhole [*mac-address*] [**vlan** *vlan-id* | **vsi** *vsi-name*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a blackhole MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the VLAN ID in a blackhole MAC address entry.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Specifies the name of a VSI in a blackhole MAC address entry. The VSI must have been created. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device or network against MAC address attacks, configure MAC addresses of untrusted users as blackhole MAC addresses. The device then directly discards the received packets of which the source or destination MAC addresses match the blackhole MAC address entries.

Prerequisites

The network administrator is familiar with the MAC addresses of all devices on the network. If the MAC address of an authorized user is configured as a blackhole MAC address, the user's communications will be interrupted.

Configuration Impact

If the source or destination MAC address of a packet matches a blackhole MAC address entry, the packet will be discarded. After being configured and saved, blackhole MAC address entries are not lost after the system reset.

Precautions

- Blackhole MAC address entries can be added or deleted, and they will not be aged.

  Unlike configuring a static MAC entry, you can configure a blackhole MAC entry without specifying an outbound interface.
- If the specified VLAN is the control VLAN for Rapid Ring Protection Protocol (RRPP), the **mac-address blackhole** command cannot be run.
- Blackhole MAC address entries fall into global and VLAN- or VSI-based blackhole MAC address entries. Global blackhole MAC address entries are configured using the **mac-address blackhole** command with only a MAC address specified. They do not occupy the MAC address table space.
- If you configure a VLAN- or VSI-based blackhole MAC address entry when the MAC address table is full, the device processes the MAC address entry as follows:
  - If a dynamic MAC address entry with the same MAC address and VLAN ID or VSI name exists in the MAC address table, the blackhole MAC address entry replaces the dynamic MAC address entry.
  - If no dynamic MAC address entry with the same MAC address exists in the MAC address table, the system deletes one dynamic MAC address entry and adds the blackhole MAC address entry to the MAC address table.
- You can run the **mac-address blackhole** command multiple times to configure multiple blackhole MAC address entries.
- For the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S switch, if both traffic policy-based redirection action and VLAN-based blackhole MAC address are configured, the switch will not discard the packet if its source or destination MAC address is a blackhole MAC address and the packet matches the redirection policy. For other device models, the switch discards the packet.
- An existing MAC address entry whose MAC address type is **authen**, **pre-authen**, **security**, **sticky**, **static**, or **static-con mac** cannot be configured as a blackhole MAC address entry.
- In a Layer 3 forwarding scenario, if a device has learned an ARP entry and the MAC address in the ARP entry is configured as a VLAN-based blackhole MAC address, the device discards packets with this source MAC address only after the ARP entry ages out.

Example

Add a blackhole MAC address entry to the MAC address table. In the blackhole MAC address entry, the MAC address is 00e0-fc04-0004 and the VLAN ID is VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
```

```
[HUAWEI-vlan5] quit
[HUAWEI] mac-address blackhole 00e0-fc04-0004 vlan 5
```

Configure a global blackhole MAC address entry in which the MAC address is 00e0-fc05-0005.

```
<HUAWEI> system-view
[HUAWEI] mac-address blackhole 00e0-fc05-0005
```

Add a blackhole MAC address entry in which the MAC address is 00e0-fc33-4455 to VSI **a2**. The device directly discards the received frame in which the source or destination MAC address is 00e0-fc33-4455 and the VSI name is **a2**.

```
<HUAWEI> system-view
[HUAWEI] mac-address blackhole 00e0-fc33-4455 vsi a2
```

5.1.21 mac-address destination hit aging enable

Function

The **mac-address destination hit aging enable** command configures the device to age MAC address entries no matter whether the entries match destination MAC addresses of packets.

The **undo mac-address destination hit aging enable** command restores the default configuration.

By default, if MAC address entries match destination MAC addresses of packets, the system recalculates the aging time.

NOTE

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S do not support this command.

Format

mac-address destination hit aging enable

undo mac-address destination hit aging enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user uses one-way services such as the video on demand service, packets are transmitted unidirectionally from the server to the user terminal. When the user terminal is shut down, the server still sends packets. Therefore, the dynamic MAC address entry with the destination MAC address of the packets remains in the MAC address table.

To delete MAC address entries matching one-way service packets after user terminals are shut down, run the **mac-address destination hit aging enable** command to enable the device to age dynamic MAC address entries matching dynamic MAC addresses of received packets.

Configuration Impact

This command is used only when one-way services are deployed on a network.

Precautions

This command only free up space in the MAC address table but cannot save system resources. If the device cannot find the matching entry in the MAC address table, it broadcasts the packets.

Example

Configure the device to age MAC address entries no matter whether the entries match destination MAC addresses of packets.

```
<HUAWEI> system-view
[HUAWEI] mac-address destination hit aging enable
```

5.1.22 mac-address flapping action

Function

The **mac-address flapping action** command configures the action to perform on an interface when MAC address flapping is detected on the interface.

The **undo mac-address flapping action** command deletes the action.

By default, the system does not perform any action when detecting MAC address flapping on an interface.

Format

mac-address flapping action { **error-down** | **quit-vlan** }

undo mac-address flapping action { **error-down** | **quit-vlan** }

Parameters

Parameter	Description	Value
error-down	Shuts down an interface when MAC address flapping is detected on the interface.	-

Parameter	Description	Value
quit-vlan	Removes an interface from the VLAN where MAC address flapping occurs when MAC address flapping is detected on the interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch connects to a user network that does not support loop prevention protocols, configure a loop prevention action for the switch to perform when detecting MAC address flapping. This reduces the impact of MAC address flapping on the user network.

When MAC address flapping occurs on an interface with a loop prevention action configured, the switch performs the configured action. When the action is set to error-down, the switch shuts down the interface. When the action is set to quit-VLAN, the switch removes the interface from the VLAN where MAC address flapping occurs. Only one interface can be shut down during one aging time configured by the **mac-address flapping aging-time** command.

Follow-up Procedure

- When the action is set to **error-down**, the interface cannot be automatically restored after it is shut down. You can only restore the interface by running the **shutdown** and **undo shutdown** commands or the **restart** command in the interface view.

  To enable the interface to go Up automatically, you must run the **error-down auto-recovery cause mac-address-flapping** command in the system view before the interface enters the error-down state. This command enables an interface in error-down state to go Up and sets a recovery time. The interface goes Up automatically after the time expires.
- If the action is set to **quit-vlan**, the interface can be automatically restored after a specified time period after it is removed from the VLAN. The default recovery time is 10 minutes. The recovery delay time can be set using the **mac-address flapping quit-vlan recover-time** *time-value* command in the system view.

Precautions

Do not run the **mac-address flapping action** command on uplink interfaces.

MAC address flapping detection can only detect loops on interfaces, but cannot obtain the entire network topology. If the user network connected to the switch supports loop prevention protocols, use the loop prevention protocols instead of MAC address flapping detection.

If you run the **mac-address flapping action** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure the switch to shut down GE0/0/1 when detecting MAC address flapping on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping action error-down
Info: This command may shut down the interface after MAC address flapping is detected.
```

Configure the switch to remove GE0/0/1 from the VLAN where MAC address flapping occurs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping action quit-vlan
```

5.1.23 mac-address flapping action priority

Function

The **mac-address flapping action priority** command sets the priority for the action against MAC address flapping on an interface.

The **undo mac-address flapping action priority** command restores the default configuration.

By default, the action against MAC address flapping on an interface is 127.

Format

mac-address flapping action priority *priority*

undo mac-address flapping action priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the action against MAC address flapping on an interface.	The value is an integer that ranges from 0 to 255. A larger value indicates a higher priority. The default value is 127.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch connects to a user network that does not support loop prevention protocols, configure a loop prevention action for the switch to perform when detecting MAC address flapping. This reduces the impact of MAC address flapping on the user network. The **mac-address flapping action priority** command sets the priority of the action.

When a MAC address flaps between two interfaces and both the interfaces have an action and priority configured, the switch performs the action (error-down or quit-VLAN) configured on the interface with lower priority. If the two interfaces have the same priority, the switch performs the action on the interface that learns the MAC address later. If the later interface has no action configured, the switch performs the action on the interface that learns the MAC address earlier.

NOTE

The switch compares priorities of the interfaces only when the interfaces have the same action configured. If one interface is configured with the error-down action, and the other is configured with the quit-VLAN action, the switch performs the actions on both interfaces even if their priorities are same.

Precautions

If you run the **mac-address flapping action priority** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the priority of the action against MAC address flapping on GE0/0/1 to 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping action priority 3
```

5.1.24 mac-address flapping aging-time

Function

The **mac-address flapping aging-time** command sets the aging time of flapping MAC addresses.

The **undo mac-address flapping aging-time** command restores the default aging time of flapping MAC addresses.

By default, the aging time of flapping MAC addresses is 300 seconds.

Format

mac-address flapping aging-time *aging-time*

undo mac-address flapping aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of flapping MAC addresses.	The value is an integer that ranges from 60 to 900, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Increasing the aging time of flapping MAC addresses will cause MAC address flapping again and increase the error-down time. To ensure that the system performs MAC address flapping detection in a timely manner, run the **mac-address flapping aging-time** command to shorten the aging time of flapping MAC addresses.

Precautions

If you run the **mac-address flapping aging-time** command multiple times, only the latest configuration takes effect.

Example

Set the aging time of flapping MAC addresses to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping aging-time 500
```

5.1.25 mac-address flapping detection

Function

The **mac-address flapping detection** command enables global MAC address flapping detection.

The **undo mac-address flapping detection** command disables global MAC address flapping detection.

By default, global MAC address flapping detection is enabled.

Format

mac-address flapping detection

undo mac-address flapping detection

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

MAC address flapping occurs when a MAC address is learned by two interfaces in the same VLAN. The MAC address entry learned later replaces the earlier one.

MAC address flapping occurs in the following situations:

- Network cables of switches are connected incorrectly or switches use incorrect configurations.
- Unauthorized users simulate MAC address of valid network devices to attack the network.

Global MAC address flapping detection enables the Switch to check all MAC addresses. When MAC address flapping occurs, the Switch sends a trap message to the NMS. You can locate the fault according to the trap message. You can also run the **display mac-address flapping record** command to view MAC address flapping records.

NOTE

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, it takes several seconds to eliminate MAC address flapping if a large number of MAC address flapping events occur on the network. During this period, the number of MAC address flapping records may increase even if MAC address flapping is eliminated.

Example

Enable global MAC address flapping detection.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection
```

5.1.26 mac-address flapping detection exclude vlan

Function

The **mac-address flapping detection exclude vlan** command excludes a VLAN from MAC address flapping detection.

The **undo mac-address flapping detection exclude vlan** command restores MAC address flapping detection for a VLAN.

By default, the system performs MAC address flapping detection in all VLANs.

Format

mac-address flapping detection exclude vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo mac-address flapping detection exclude vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the ID of a VLAN where MAC address flapping detection is not required. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than *vlan-id1*. You can specify a maximum of 10 VLANs.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Indicates that all VLANs are excluded from MAC address flapping detection.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the system performs MAC address flapping detection in all VLANs. When a switch connected to a load balancing server with dual network adapters, the server's MAC address may be learned by two interfaces on the switch. This is a normal situation where MAC address flapping detection is not required.

You can run the **mac-address flapping detection exclude vlan** command to exclude a VLAN from MAC address flapping detection. If MAC address flapping occurs in this VLAN, the system does not send a trap message or record this event.

Precautions

If you run the **mac-address flapping detection exclude vlan** command multiple times, multiple VLANs are excluded from MAC address flapping detection.

Example

Exclude VLAN 5 from MAC address flapping detection.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection exclude vlan 5
```

5.1.27 mac-address flapping detection vlan security-level

Function

The **mac-address flapping detection vlan security-level** command configures the security level of VLANs for MAC address flapping detection.

The **undo mac-address flapping detection vlan security-level** command restores the default security of VLANs for MAC address flapping detection.

By default, the security level of a VLAN for MAC address flapping detection is middle. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces 10 times.

Format

mac-address flapping detection vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } **security-level** { **high** | **middle** | **low** }

undo mac-address flapping detection vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } **security-level** [**high** | **middle** | **low**]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the VLANs of which the security level needs to be set for MAC address flapping detection. - *vlan-id1* specifies the ID of the first VLAN. - **to** *vlan-id2* specifies the ID of the last VLAN. The value of *vlan-id2* must be larger than the value of *vlan-id1*. You can specify a maximum of 10 VLAN ID ranges in a command.	- The value of *vlan-id1* is an integer that ranges from 1 to 4094. - The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Configures security level of all VLANs for MAC address flapping detection.	-
high	Sets the security level of specified VLANs to high. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces three times.	-
middle	Sets the security level of specified VLANs to middle. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces 10 times.	-
low	Sets the security level of specified VLANs to low. At this security level, the system considers that a MAC address flapping occurs when a MAC address moves between interfaces 50 times.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch considers that a MAC address flapping occurs when a MAC address moves between interfaces 10 times. On an unstable network, it may be a normal situation when a MAC address moves between interfaces 10 times. You can set the security level for VLANs according to the actual situation of your network. The switch reports a MAC address flapping when a MAC address moves between interfaces for the specified number of times.

Example

Set the security level of VLAN 5 to high for MAC address flapping.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection vlan 5 security-level high
```

5.1.28 mac-address flapping mac-syn-suppress disable

Function

The **mac-address flapping mac-syn-suppress disable** command disables real-time MAC address synchronization suppression triggered by MAC address flapping.

The **undo mac-address flapping mac-syn-suppress disable** command enables real-time MAC address synchronization suppression triggered by MAC address flapping.

By default, MAC address synchronization suppression triggered by MAC address flapping is enabled.

Format

mac-address flapping mac-syn-suppress disable

undo mac-address flapping mac-syn-suppress disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, real-time MAC address synchronization suppression is enabled on a device. With this function enabled, if a large number of real-time MAC address synchronization packets are generated due to persistent MAC address flapping, real-time MAC address synchronization suppression will be triggered. This will result in problems such as delay in obtaining DHCP addresses in terminal roaming scenarios. To address such problems, run the **mac-address flapping mac-syn-suppress disable** command to disable real-time MAC address synchronization suppression triggered by MAC address flapping.

Example

Disable real-time MAC address synchronization suppression triggered by MAC address flapping.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping mac-syn-suppress disable
```

5.1.29 mac-address flapping quit-vlan recover-time

Function

The **mac-address flapping quit-vlan recover-time** command sets the delay time an interface waits to join a VLAN again after it is removed from the VLAN due to MAC address flapping.

The **undo mac-address flapping quit-vlan recover-time** command restores the default delay time.

By default, the delay time is 10 minutes.

Format

mac-address flapping quit-vlan recover-time *time-value*

undo mac-address flapping quit-vlan recover-time

Parameters

Parameter	Description	Value
time-value	Specifies the delay time an interface waits to join a VLAN again after it is removed from the VLAN due to MAC address flapping.	The value is an integer ranging from 0 to 1440, in minutes. The default value is 10. The value 0 indicates that the interface cannot join a VLAN again after it is removed from the VLAN.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface is removed from a VLAN because MAC address flapping occurs in the VLAN, the interface can automatically join the VLAN again after a delay.

Precautions

If an interface is removed from multiple VLANs due to MAC address flapping, the system counts the delay time since the interface is removed from the last VLAN.

Example

Set the delay time before an interface joins a VLAN again to 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping quit-vlan recover-time 15
```

Restore the default delay time.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address flapping quit-vlan recover-time
```

5.1.30 mac-address flapping unicast-suppress all disable

Function

The **mac-address flapping unicast-suppress all disable** command globally disables MAC address flapping suppression.

The **undo mac-address flapping unicast-suppress all disable** command cancels the configuration.

By default, unknown unicast traffic suppression is enabled globally.

Format

mac-address flapping unicast-suppress all disable

undo mac-address flapping unicast-suppress all disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if MAC address flapping detection is enabled on a device and MAC address flapping is detected, traffic suppression is triggered on the corresponding interface. As a result, excess traffic is discarded, resulting in packet loss.

To prevent this, disable unknown unicast traffic suppression.

Example

Globally disable unknown unicast traffic suppression.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping unicast-suppress all disable
```

5.1.31 mac-address flapping unicast-suppress disable

Function

The **mac-address flapping unicast-suppress disable** command disables MAC address flapping suppression on an interface.

The **undo mac-address flapping unicast-suppress disable** command cancels the configuration.

By default, unknown unicast traffic suppression is enabled on an interface.

Format

mac-address flapping unicast-suppress disable

undo mac-address flapping unicast-suppress disable

Parameters

None

Views

Interface view

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if MAC address flapping detection is enabled on a device and MAC address flapping is detected, traffic suppression is triggered on the corresponding interface. As a result, excess traffic is discarded, resulting in packet loss.

To prevent this, disable unknown unicast traffic suppression.

Precautions

Unknown unicast traffic suppression takes effect on an interface only when the following conditions are met:

- Global MAC address flapping detection is configured.
- MAC address flapping occurs on the interface.
- Unknown unicast traffic suppression is enabled globally.
- Unknown unicast traffic suppression is enabled on the interface.

Example

Disable unknown unicast traffic suppression on GE0/0/1.

```
<HUAWEI> system-view
<HUAWEI> interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address flapping unicast-suppress disable
```

5.1.32 mac-address hash-bucket-mode

Function

The **mac-address hash-bucket-mode** command sets the hash bucket size of the MAC address table.

The **undo mac-address hash-bucket-mode** command restores the default hash bucket size of the MAC address table.

By default, the hash bucket size of the MAC address table is 4.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

mac-address hash-bucket-mode { **size4** | **size8** | **size12** | **size16** }

undo mac-address hash-bucket-mode

Parameters

Parameter	Description	Value
size4	Indicates that the hash bucket size of the MAC address table is 4.	-

Parameter	Description	Value
size8	Indicates that the hash bucket size of the MAC address table is 8.	-
size12	Indicates that the hash bucket size of the MAC address table is 12.	-
size16	Indicates that the hash bucket size of the MAC address table is 16.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the MAC address forwarding performance, the MAC address table of the device is saved using a hash link. When the same key value is obtained for multiple MAC addresses according to the hash algorithm, some MAC addresses may be not learned. That is, the MAC address hash conflict occurs. When the MAC address hash conflict occurs, traffic with this destination MAC address can only be broadcast. This occupies device bandwidth and resources.

When the MAC address hash conflict aggravates, run this command to increase the hash bucket size of the MAC address table.

Precautions

A larger hash bucket size will lower device forwarding performance.

When the hash bucket size becomes small, you need to restart the device.

Example

Set the hash bucket size of the MAC address table to 16.

```
<HUAWEI> system-view
[HUAWEI] mac-address hash-bucket-mode size16
```

5.1.33 mac-address hash-mode

Function

The **mac-address hash-mode** command configures a MAC hash algorithm on the device.

The **undo mac-address hash-mode** command restores the default MAC hash algorithm on the device.

By default, the hash algorithm on the S6735-S, S6720-EI and S6720S-EI is **crc32-lower**. The hash algorithm on other models is **crc**.

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

On the S6735-S, S6720-EI and S6720S-EI:

mac-address hash-mode { **crc16-lower** | **crc16-upper** | **crc32-lower** | **crc32-upper** | **lsb** | **enhanced** } **slot** *slot-id*

undo mac-address hash-mode [**crc16-lower** | **crc16-upper** | **crc32-lower** | **crc32-upper** | **lsb** | **enhanced**] **slot** *slot-id*

On devices except S6735-S, S6720-EI and S6720S-EI:

mac-address hash-mode { **xor** | **crc** } **slot** *slot-id*

undo mac-address hash-mode [**xor** | **crc**] **slot** *slot-id*

Parameters

Parameter	Description	Value
crc	Indicates the CRC-based hash algorithm.	-
crc16-lower	Indicates the hash algorithm based on low order bits of CRC16.	-
crc16-upper	Indicates the hash algorithm based on high order bits of CRC16.	-
crc32-lower	Indicates the hash algorithm based on low order bits of CRC32.	-
crc32-upper	Indicates the hash algorithm based on high order bits of CRC32.	-

Parameter	Description	Value
lsb	Indicates the hash algorithm based on the lowest bit of the key value.	-
xor	Indicates the Exclusive-Or mode.	-
enhanced	Indicates the enhanced mode.	-
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses a hash algorithm to improve MAC address forwarding performance. If multiple MAC addresses match a key value, a hash conflict occurs.

When a hash conflict occurs, the device may fail to learn many MAC addresses and some traffic can only be broadcast. This results in heavy broadcast traffic on the device. If such a problem occurs, use an appropriate hash algorithm to reduce the hash conflict.

Precautions

- MAC addresses are distributed on a network randomly, so the system cannot determine the best hash algorithm. Generally, the default hash algorithm is the best one, so do not change the hash algorithm unless you have special requirement.
- An appropriate hash algorithm can only reduce hash conflicts, but cannot prevent them.
- After changing the hash algorithm and saving the configuration, restart the device for the configuration to take effect.
- If you run the **mac-address hash-mode** command multiple times, only the latest configuration takes effect.

Example

Set the hash algorithm on the device to **crc**.

```
<HUAWEI> system-view
[HUAWEI] mac-address hash-mode crc slot 0
```

5.1.34 mac-address learning disable (interface view and VLAN view)

Function

The **mac-address learning disable** command disables MAC address learning.

The **undo mac-address learning disable** command enables MAC address learning.

By default, MAC address learning is enabled.

Format

mac-address learning disable [**action** { **discard** | **forward** }] (Interface view)

mac-address learning disable (VLAN view)

undo mac-address learning disable

Parameters

Parameter	Description	Value
action	Indicates the action that the interface takes after MAC address learning is disabled. • This parameter takes effect only in the interface view and port group view, and the specified interface must be a Layer 2 interface. • You can use this parameter to determine whether packets are forwarded when the specified interface does not need to learn MAC addresses. By default, an interface forwards the packets carrying new MAC addresses after MAC address learning is disabled.	-

Parameter	Description	Value
discard	Discards the packets whose source MAC addresses do not match the MAC address table.	-
forward	Forwards the packets according to the MAC address table.	-

Views

VLAN view, 100GE interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want an interface to forward only packets with certain MAC addresses, use this command. For example, if an interface is connected to a server, configure a static MAC address entry with the MAC address of the server, and then disable MAC address learning and set the action to discard on the interface. The configuration prevents other servers or terminals from accessing the interface and improves network stability and security.

When a switch with MAC address learning enabled receives an Ethernet frame, it records the source MAC address and inbound interface of the Ethernet frame in a MAC address entry. When receiving other Ethernet frames destined for this MAC address, the switch forwards the frames through the corresponding outbound interface according to the MAC address entry. MAC address learning reduces broadcast packets on a network.

You can use the **mac-address learning disable** command to disable MAC address learning on an interface. The action performed on received packets can be set to **discard** or **forward**.

By default, the switch takes the forward action after MAC address learning is disabled. That is, the switch forwards packets according to the MAC address table. When the action is set to discard, the switch looks up the source MAC address of the packet in the MAC address table. If the source MAC address is found in the MAC address table, the switch forwards the packet according to the matching MAC address entry. If the source MAC address is not found, the switch discards the packet.

Precautions

- Before running the **mac-address learning disable** command on an Eth-Trunk interface, ensure that the Eth-Trunk interface works in Layer 2 mode; otherwise, the configuration fails. To switch an Eth-Trunk interface from the Layer 3 mode to the Layer 2 mode, you can run the **portswitch** command in the view of the Eth-Trunk interface.
- After MAC address learning is disabled on an interface, the device does not learn new MAC addresses on the interface. Untrusted terminals can still access the network.
- After MAC address learning is disabled on an interface, dynamic MAC address entries learned on the interface are not immediately deleted. These entries will be deleted after the aging time elapses or after you run a command to manually delete the entries. If a MAC address entry is always matched to direct traffic forwarding, this entry will not be aged out.
- On the S6735-S, if the number of MAC addresses learned in the VLAN reaches the upper limit or the MAC address learning function is disabled in the VLAN, the packet discarding function configured using the **mac-address learning disable action discard** command does not take effect on interfaces in the VLAN.

Example

Disable MAC address learning in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] mac-address learning disable
```

5.1.35 mac-address learning disable (traffic behavior view)

Function

The **mac-address learning disable** command disables MAC address learning in a traffic behavior.

The **undo mac-address learning disable** command enables MAC address learning in a traffic behavior.

By default, MAC address learning is enabled in a traffic behavior.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

mac-address learning disable

undo mac-address learning disable

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mac-address learning disable** command is used in the following scenarios:

- When a network is running stably and the MAC address of packets is fixed, a device does not need to learn MAC addresses of other packets. To save MAC addresses and improve device efficiency, apply a traffic policy and disable MAC address learning in all the traffic classifiers bound to the traffic policy.
- Some unauthorized users may change MAC addresses frequently to attack the network. To prevent MAC address overflow and protect device performance, apply a traffic policy and disable MAC address learning in all the traffic classifiers bound to the traffic policy.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of disabling MAC address learning.

Precautions

After the traffic behavior containing **mac-address learning disable** is bound to the specified traffic classifier, the source MAC addresses of packets matching the traffic classifier are not learned. The source MAC addresses of packets that do not match the traffic classifier are still learned by default.

The **mac-address learning disable** command is similar to the **mac-address learning disable** command in the interface view or VLAN view. The difference is that the **mac-address learning disable** command is valid for the packets matching the user-defined traffic classifier and is applied to the system, an interface, or a VLAN by using the traffic policy. The **mac-address learning disable** command is used in the interface view, port group view, or VLAN view and is valid for all the packets in the corresponding view.

To disable MAC address learning on an interface, in a port group, or in a VLAN, run the **mac-address learning disable** command in the corresponding view. To disable MAC address learning for a specified traffic classifier, run the **mac-address learning disable** command in the traffic behavior view.

Example

Disable MAC address learning in the traffic behavior **test**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior test
[HUAWEI-behavior-test] mac-address learning disable
```

5.1.36 mac-address learning self-healing enable

Function

The **mac-address learning self-healing enable** command enables self-healing for MAC address learning.

The **undo mac-address learning self-healing enable** command disables self-healing for MAC address learning.

By default, self-healing is enabled for MAC address learning.

Format

mac-address learning self-healing enable

undo mac-address learning self-healing enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the SAID node is enabled, the switch periodically checks whether MAC address learning of the Eth-Trunk, port security, and MAC address management modules is normal. You can run the **mac-address learning self-healing enable** command to enable self-healing for MAC address learning. After this function is enabled, self-healing is automatically performed upon detection of service status inconsistencies. This ensures that packets are forwarded correctly.

Example

Enable self-healing for MAC address learning.

```
<HUAWEI> system-view
[HUAWEI] mac-address learning self-healing enable
```

5.1.37 mac-address static vlan

Function

The **mac-address static vlan** command configures a static MAC address entry.

The **undo mac-address static vlan** command deletes a static MAC address entry.

By default, no static MAC address entry is configured.

Format

mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id*

undo mac-address static [*interface-type interface-number* | **vlan** *vlan-id*] *

undo mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id*

NOTE

For details on how to configure a VSI-based static MAC address entry, see **mac-address static vlanif** and **mac-address static vsi**.

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a static MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
interface-type interface-number	Specifies the outbound interface in a static MAC address entry.	-
vlan *vlan-id*	Specifies the ID of the VLAN that the outbound interface belongs to.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static MAC address entries are used for the following purposes:

- Improve security. The device directly discards packets sent from unauthorized users using authorized users' MAC addresses.
- Guide unicast forwarding and save bandwidth.

Precautions

- The VLAN in a static MAC address entry must have been created and the outbound interface in the same static MAC address entry has been added to the VLAN.
- If you configure a static MAC address entry when the MAC address table is full, the device processes the MAC address entry as follows:
  - If a dynamic MAC address entry with the same MAC address and VLAN ID exists in the MAC address table, the static MAC address entry replaces the dynamic MAC address entry.
  - If no dynamic MAC address entry with the same MAC address exists in the MAC address table, the system deletes one dynamic MAC address entry and adds the static MAC address entry to the MAC address table.
- You can run the **mac-address static** command multiple times to configure multiple static MAC address entries.
- An existing MAC address entry of the authen, pre-authen, security, or sticky type cannot be configured as a static MAC address entry.

Example

Add a static MAC address entry to the MAC address table. In the MAC address entry, the destination MAC address is 00e0-fc12-3456, the VLAN ID is 4, and the outbound interface is gigabitethernet0/0/2. That is, the device forwards packets with the destination MAC address of 00e0-fc12-3456 from VLAN 4 through gigabitethernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] vlan 4
[HUAWEI-vlan4] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] port link-type access
[HUAWEI-GigabitEthernet0/0/2] port default vlan 4
[HUAWEI-GigabitEthernet0/0/2] quit
[HUAWEI] mac-address static 00e0-fc12-3456 gigabitethernet 0/0/2 vlan 4
```

5.1.38 mac-address threshold-alarm

Function

The **mac-address threshold-alarm** command configures upper and lower alarm thresholds for the MAC address usage.

The **undo mac-address threshold-alarm** command restores the default upper and lower alarm thresholds for the MAC address usage.

By default, the upper and lower alarm thresholds for the MAC address usage are 80% and 70% respectively. An alarm is sent when the MAC address usage is higher than 80% or lower than 70%.

Format

mac-address threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mac-address threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for the MAC address usage, in percentage.	The value is an integer that ranges from 1 to 100. The default value is 80.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for the MAC address usage, in percentage.	The value is an integer that ranges from 1 to 100. The default value is 70. *lower-limit-value* must be smaller than or equal to *upper-limit-value*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MAC address resources are core resources of the device and the device supports limited MAC addresses. The MAC address usage affects device running. You can run the **mac-address threshold-alarm** command to configure upper and lower alarm thresholds for the MAC address usage. When the MAC address usage is larger than the upper alarm threshold or smaller than the lower alarm threshold, an alarm is generated to notify the administrator. The administrator then can learn the MAC address usage in a timely manner.

Precautions

When you run the **mac-address threshold-alarm** command multiple times, only the latest configuration takes effect.

Example

Set upper and lower alarm thresholds for the MAC address usage to 90% and 20% respectively.

```
<HUAWEI> system-view
[HUAWEI] mac-address threshold-alarm upper-limit 90 lower-limit 20
```

5.1.39 mac-address trap hash-conflict enable

Function

The **mac-address trap hash-conflict enable** command enables the trap function for the MAC address hash conflict.

The **undo mac-address trap hash-conflict enable** command disables the trap function for the MAC address hash conflict.

By default, the trap function for the MAC address hash conflict is enabled.

Format

mac-address trap hash-conflict enable

undo mac-address trap hash-conflict enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To improve the MAC address forwarding performance, the MAC address table of the device is saved using a hash link. When the same key value is obtained for multiple MAC addresses according to the hash algorithm, some MAC addresses may be not learned. That is, the MAC address hash conflict occurs.

In this situation, the MAC address table space is not full but the MAC address entry cannot be learned. When the MAC address hash conflict occurs, traffic with this destination MAC address can be only broadcast. This occupies device bandwidth and resources. You can replace the device or network adapter of the terminal.

After the trap function for the MAC address hash conflict is configured, the administrator can immediately discover MAC address hash conflicts.

Example

Enable the trap function for the MAC address hash conflict.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict enable
```

5.1.40 mac-address trap hash-conflict history

Function

The **mac-address trap hash-conflict history** command sets the number of alarms reported at an interval when the MAC address hash conflict occurs.

The **undo mac-address trap hash-conflict history** command restores the default number of alarms reported at an interval when the MAC address hash conflict occurs.

By default, 10 alarms are reported at an interval when the MAC address hash conflict occurs.

Format

mac-address trap hash-conflict history *history-number*

undo mac-address trap hash-conflict history

Parameters

Parameter	Description	Value
history-number	Specifies the number of alarms reported at an interval when the MAC address hash conflict occurs.	The value is an integer that ranges from 1 to 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the trap function for the MAC address hash conflict is enabled, the device reports a maximum of 10 alarms every 60s. Each alarm carries a MAC address for which the hash conflict occurs.

If hash values of more than 10 MAC addresses conflict, reports about subsequent MAC address hash conflicts cannot be reported. You can run this command to set the number of alarms reported at an interval.

Precautions

When you run the **mac-address trap hash-conflict history** command multiple times, only the latest configuration takes effect.

Example

Set the number of alarms reported at an interval to 12 when the MAC address hash conflict occurs.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict history 12
```

5.1.41 mac-address trap hash-conflict interval

Function

The **mac-address trap hash-conflict interval** command sets the interval at which alarms are reported when the MAC address hash conflict occurs.

The **undo mac-address trap hash-conflict interval** command restores the default interval at which alarms are reported when the MAC address hash conflict occurs.

By default, alarms are reported at intervals of 60s when the MAC address hash conflict occurs.

Format

mac-address trap hash-conflict interval *interval-time*

undo mac-address trap hash-conflict interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which alarms are reported when the MAC address hash conflict occurs.	The value is an integer that ranges from 60 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the trap function for the MAC address hash conflict is enabled, the device reports a maximum of 10 alarms every 60s. Each alarm carries a MAC address for which the hash conflict occurs.

If a small interval is used, alarms about MAC address hash conflicts are reported immediately. When there are many MAC address hash conflicts, many alarms are reported.

If a long interval is used and many MAC address hash conflicts occur, alarms will be suppressed. You can adjust the interval according to the requirements.

Precautions

When you run the **mac-address trap hash-conflict interval** command multiple times, only the latest configuration takes effect.

Example

Set the interval at which alarms are reported to 90s when the MAC address hash conflict occurs.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict interval 90
```

5.1.42 mac-address trap hash-conflict threshold

Function

The **mac-address trap hash-conflict threshold** command sets the lower alarm threshold for MAC address hash conflicts.

The **mac-address trap hash-conflict threshold** command restores the default value of the lower alarm threshold for MAC address hash conflicts.

By default, the lower alarm threshold for MAC address hash conflicts is 0.

Format

mac-address trap hash-conflict threshold *threshold-value*

undo mac-address trap hash-conflict threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the lower alarm threshold for MAC address hash conflicts.	The value is an integer that ranges from 0 to 20. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the trap function for MAC address hash conflicts is configured on a switch, the switch sends an alarm if a MAC address hash conflict occurs. This helps you detect and rectify the fault in time.

If a small number of MAC address hash conflicts occur on the network and users do not need to be aware of the conflicts, you can run the **mac-address trap hash-conflict threshold** command on a switch to set the lower alarm threshold for MAC address hash conflicts. The switch sends an alarm only if the number of MAC address hash conflicts exceeds the lower alarm threshold.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

If the lower alarm threshold for MAC address hash conflict is set to 20 on a device, the device does not report MAC address hash conflict alarms regardless of the number of MAC address hash conflict alarms generated during each period.

Example

Set the lower alarm threshold for MAC address hash conflicts to 10.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap hash-conflict threshold 10
```

5.1.43 mac-address trap notification

Function

The **mac-address trap notification** command enables the trap function for MAC address learning or aging.

The **undo mac-address trap notification** command disables the trap function for MAC address learning or aging.

By default, the trap function for MAC address learning or aging is disabled.

Format

mac-address trap notification { **aging** | **learn** | **all** }

undo mac-address trap notification

Parameters

Parameter	Description	Value
aging	Enables the trap function for MAC address aging.	-

Parameter	Description	Value
learn	Enables the trap function for MAC address learning.	-
all	Enables the trap function for MAC address learning and aging.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To learn MAC address change in a timely manner, run the **mac-address trap notification** command to enable the trap function for MAC address learning or aging.

Precautions

When you run the **mac-address trap notification** command multiple times, only the latest configuration takes effect.

The trap function for MAC address learning or aging is not supported for the MAC address entries in a VSI.

Example

Enable the trap function for MAC address learning on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address trap notification learn
```

5.1.44 mac-address trap notification interval

Function

The **mac-address trap notification interval** command sets the interval at which the device checks MAC address learning or aging.

The **undo mac-address trap notification interval** command restores the default interval at which the device checks MAC address learning or aging.

By default, the device checks MAC address learning or aging at intervals of 10s.

Format

mac-address trap notification interval *interval-time*

undo mac-address trap notification interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which the device checks MAC address learning or aging.	The value is an integer that ranges from 10 to 600, in seconds. The default value is 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **mac-address trap notification** command is used to enable the trap function when the device learns MAC addresses or MAC addresses are aged, the device periodically checks whether MAC addresses are learned or aged. You can run the **mac-address trap notification interval** command to set the interval.

Example

Set the interval at which the device checks MAC address learning or aging to 20s.

```
<HUAWEI> system-view
[HUAWEI] mac-address trap notification interval 20
```

5.1.45 mac-address update arp

Function

The **mac-address update arp** command enables the MAC address-triggered ARP entry update function. That is, the Switch is enabled to update outbound interfaces in ARP entries when outbound interfaces in MAC address entries change.

The **undo mac-address update arp** command disables the MAC address-triggered ARP entry update function.

By default, the MAC address-triggered ARP entry update function is disabled.

Format

mac-address update arp

undo mac-address update arp

NOTE

The S200, S1730S-S1 does not support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the Ethernet, MAC address entries are used to guide Layer 2 data forwarding. The ARP entries that define the mapping between IP addresses and MAC addresses guide communication between devices on different network segments.

The outbound interface in a MAC address entry is updated by packets, whereas the outbound interface in an ARP entry is updated after the aging time is reached. In this case, the outbound interfaces in the MAC address entry and ARP entry may be different. To address this issue, run the **mac-address update arp** command to enable the Switch to update outbound interfaces in ARP entries when outbound interfaces in MAC address entries change.

Precautions

This command takes effect only for dynamic ARP entries. Static ARP entries are not updated when the corresponding MAC address entries change.

The **mac-address update arp** command does not take effect after ARP entry fixing is enabled by using the **arp anti-attack entry-check { fixed-mac | fixed-all | send-ack } enable** command.

After the **mac-address update arp** command is run, the Switch updates an ARP entry only if the outbound interface in the corresponding MAC address entry changes.

After this command is executed, the **arp anti-attack gratuitous-arp drop** command becomes invalid and the Switch cannot drop gratuitous ARP packets.

Example

Enable the MAC address-triggered ARP entry update function.

```
<HUAWEI> system-view
[HUAWEI] mac-address update arp
```

5.1.46 mac-learning priority

Function

The **mac-learning priority** command sets the MAC address learning priority of an interface.

The **undo mac-learning priority** command restores the default MAC learning priority of an interface.

By default, the MAC address learning priority of an interface is 0.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Format

mac-learning priority *priority-id*

undo mac-learning priority

Parameters

Parameter	Description	Value
priority *priority-id*	Specifies the MAC address learning priority of an interface.	The value is an integer that ranges from 0 to 3. A larger value indicates a higher priority.

Views

GE interface view, XGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An uplink interface of the switch is connected to a server, and downlink interfaces are connected to users. To prevent unauthorized users from using the server MAC address to connect to the switch, run the **mac-learning priority** command to set the priority of the uplink interface to be higher than the user-side interfaces. When these interfaces learn the same MAC address, the MAC address entry learned by the uplink interface overrides MAC address entries learned by the user-side interfaces. Therefore, the switch will not learn MAC addresses of unauthorized users, and authorized users can access the server and use network resources.

You can run the **undo mac-learning priority allow-flapping** command to forbid MAC address flapping between interfaces with the same priority.

Both the **undo mac-learning priority allow-flapping** command and the **mac-learning priority** command can prevent MAC address flapping. The difference between the two commands is as follows:

- The **undo mac-learning priority allow-flapping** command prevents MAC address flapping between interfaces with the same priority. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch cannot learn the correct server MAC address.
- The **mac-learning priority** command prevents MAC address flapping between interfaces with different priorities. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch can learn the correct server MAC address.

Precautions

If you run the **mac-learning priority** command multiple times in the same interface view, only the latest configuration takes effect.

The function is not supported for the MAC address entries in a VSI.

Example

Set the MAC address learning priority of GigabitEthernet0/0/2 to 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] mac-learning priority 3
```

5.1.47 mac-learning priority allow-flapping

Function

The **mac-learning priority allow-flapping** command allows MAC address flapping between interfaces with the same priority.

The **undo mac-learning priority allow-flapping** command prevents MAC address flapping between interfaces with the same priority.

By default, MAC address flapping between interfaces with the same priority is allowed.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Format

mac-learning priority *priority-id* **allow-flapping**

undo mac-learning priority *priority-id* **allow-flapping**

Parameters

Parameter	Description	Value
priority *priority-id*	Specifies the MAC address learning priority of an interface.	The value is an integer that ranges from 0 to 3. A larger value indicates a higher priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An uplink interface of the switch is connected to a server, and downlink interfaces are connected to users. To prevent unauthorized users from using the server MAC address to connect to the switch, you can run the **undo mac-learning priority allow-flapping** command to forbid MAC address flapping between interfaces with the same priority. MAC address then will not be learned by multiple interfaces. This prevents attackers from using the MAC addresses of valid devices to attack the switch.

Both the **mac-learning priority** command and the **undo mac-learning priority allow-flapping** command can prevent MAC address flapping. The difference between the two commands is as follows:

- The **undo mac-learning priority allow-flapping** command prevents MAC address flapping between interfaces with the same priority. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch cannot learn the correct server MAC address.
- The **mac-learning priority** command prevents MAC address flapping between interfaces with different priorities. If an attacker uses the server MAC address to connect to the switch after the server is powered off, the switch learns the MAC address of the forged server. After the real server is powered on, the switch can learn the correct server MAC address.

Precautions

The function is not supported for the MAC address entries in a VSI.

Example

Forbid MAC address flapping between interfaces with priority 1.

```
<HUAWEI> system-view
[HUAWEI] undo mac-learning priority 1 allow-flapping
```

5.1.48 mac-learning priority flapping-defend action

Function

The **mac-learning priority flapping-defend action** command configures an action to be taken when the switch is configured to prohibit MAC address flapping.

The **undo mac-learning priority flapping-defend action** command restores the default action when the switch is configured to prohibit MAC address flapping.

By default, the action is **forward** when the switch is configured to prohibit MAC address flapping.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Format

mac-learning priority flapping-defend action { **forward** | **discard** }

undo mac-learning priority flapping-defend action

Parameters

Parameter	Description	Value
forward	Packets are forwarded when the switch is configured to prohibit MAC address flapping.	-
discard	Packets are discarded when the switch is configured to prohibit MAC address flapping.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An uplink interface of the switch is connected to a server, and a downlink interface is connected to a user. To prevent a malicious user from using a forged server's MAC address to attack the switch, run the **mac-learning priority** command in the interface view or the **undo mac-learning priority allow-flapping** command in the system view to prohibit MAC address flapping. A MAC address then will not be learned by multiple interfaces, and the malicious user cannot use the MAC address of a valid device to attack the switch. However, packets of the malicious user are still forwarded. You can configure the **discard** action to discard packets from the malicious user when MAC address flapping is prohibited.

Precautions

- If the **mac-learning priority** or **undo mac-learning priority allow-flapping** command is not used, the action specified using this command is invalid.
- This command is invalid for MAC addresses in a VSI.

Example

Configure the switch to discard packets when the switch is configured to prohibit MAC address flapping.

```
<HUAWEI> system-view
[HUAWEI] mac-learning priority flapping-defend action discard
```

5.1.49 mac-limit

Function

The **mac-limit** command configures a rule to limit the number of MAC addresses that can be learned.

The **undo mac-limit** command deletes the rule.

By default, the number of learned MAC addresses is not limited.

Format

mac-limit { **maximum** *max-num* | **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } } * (Interface view)

mac-limit { **maximum** *max-num* | **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } } * (This command is supported in the VLAN view only on the S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S.)

mac-limit { **maximum** *max-num* | **alarm** { **disable** | **enable** } } * (This command is supported in the VLAN view only on the devices except the S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. When the number of learned MAC address entries reaches the limit on a device, the device still forwards packets with new source MAC addresses, but does not add the new MAC addresses to the MAC address table.)

undo mac-limit

Parameters

Parameter	Description	Value
action { **discard** | **forward** }	Indicates the action performed when the number of learned MAC address entries reaches the limit. - **discard**: discards packets with new source MAC addresses. - **forward**: forwards packets with new source MAC addresses but does not add the new MAC addresses to the MAC address table.	If no action is specified in the command, the default action **discard** is used. **NOTE** On the S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, running a version earlier than V200R019C10, the **action** parameter is unavailable. When the number learned of MAC addresses reaches the limit, the system takes the **forward** action by default.
alarm { **disable** | **enable** }	Indicates whether the system generates an alarm when the number of learned MAC address entries reaches the limit. - **disable**: indicates that no alarm is generated when the number of learned MAC addresses reaches the limit. - **enable**: indicates that an alarm is generated when the number of learned MAC addresses reaches the limit.	If you do not set this parameter in the command, the alarm function is enabled by default.

Parameter	Description	Value
maximum *max-num*	Sets the maximum number of MAC addresses that can be learned. **NOTE** If **maximum** is not set, you must run the **mac-limit** command with **maximum** specified. If you have run the **mac-limit** command to set the maximum number of MAC addresses that can be learned, you do not need to set **maximum** *max-num* when running this command again.	The value is a decimal integer that ranges from 0 to 4096. The value 0 indicates that the highest rate of MAC address learning is not limited.

Views

VLAN view, Ethernet interface view, 100GE interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mac-limit** command limits the number of access users and prevents attacks to the MAC address tables. You can enable the function to improve network security.

Precautions

- The **mac-limit** command configuration takes effect only for dynamically learned MAC addresses. If some MAC addresses have been learned, run the **undo mac-address dynamic** command to delete the learned MAC address entries. If you do not delete them, less new MAC addresses can be learned than the value configured using the **mac-limit** command.
- After the **port-security enable** command is configured on an interface, **mac-limit** cannot take effect. Do not configure **mac-limit** and **port-security enable** simultaneously.
- The MAC address limiting function and NAC conflict on an interface; therefore, the **mac-limit** and **mac-authen**, **dot1x enable**, **web-auth-server** or **authentication-profile** commands cannot be used on the same interface.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, a maximum of 32 VLANs can be configured with the **action discard** parameter.

- If you run the **mac-limit** command in the interface view, the command takes effect only for MAC addresses learned from VLANs.
- On the S6735-S, if the number of MAC addresses learned in the VLAN reaches the upper limit or the MAC address learning function is disabled in the VLAN, the packet discarding function configured using the **mac-address learning disable action discard** command does not take effect on interfaces in the VLAN.

Example

Set the maximum number of MAC addresses that can be learned by GigabitEthernet0/0/2 to 30. Configure the device to generate an alarm when the number learned of MAC addresses reaches the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] mac-limit maximum 30 alarm enable
```

5.1.50 mac-spoofing-defend enable (interface view)

Function

The **mac-spoofing-defend enable** command configures an interface as a trusted interface.

The **undo mac-spoofing-defend enable** command restores an interface to an untrusted interface.

By default, an interface is untrusted.

NOTE

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

mac-spoofing-defend enable

undo mac-spoofing-defend enable

Parameters

None

Views

GE interface view, Ethernet interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User behaviors are uncontrollable; therefore, a user device may send bogus packets with the server MAC address to prevent other users from accessing the real server. To prevent such attacks, you can use the **mac-spoofing-defend enable** command to configure the network-side interface connected to the server as a trusted interface. The MAC address learned by the interface will not be learned by other interfaces. This prevents the attacks of bogus packets with the server MAC address.

Prerequisites

The MAC spoofing defense function has been enabled by using the **mac-spoofing-defend enable** command in the system view.

Precautions

- After the device connected to the trusted interface is powered off, the MAC address entry matching the device MAC address is aged out after a certain period. After another device is connected to the interface, the MAC address of this device will not be learned by other interfaces.
- On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, when the TPID configured by the **qinq protocol** command on the inbound interface is different from the TPID in received packets and the **mac-spoofing-defend enable** command is also used on the inbound interface, the MAC address of packets in the VLAN specified by the PVID is learned, but not the MAC address-based VLAN, protocol-based VLAN, IP subnet-based VLAN, or policy VLAN. For example, the TPID on port A is 0x9100, the PVID is 10, MAC address-based VLAN is VLAN 20, received packet A contains VLAN 30 and TPID of 0x8100 that matches the MAC address-based VLAN. Because TPID values are different, the interface considers that packet A is untagged and adds VLAN 20 to packet A. The MAC address in VLAN 20 is therefore learned. If the **mac-spoofing-defend enable** command is configured on port A, the MAC address in VLAN 10 is incorrectly learned.

Example

Configure GigabitEthernet0/0/1 as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-spoofing-defend enable
```

5.1.51 mac-spoofing-defend enable (system view)

Function

The **mac-spoofing-defend enable** command enables global MAC spoofing defense.

The **undo mac-spoofing-defend enable** command disables global MAC spoofing defense.

By default, global MAC spoofing defense is disabled.

NOTE

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

mac-spoofing-defend enable

undo mac-spoofing-defend enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User behaviors are uncontrollable; therefore, a user device may send bogus packets with the server MAC address to prevent other users from accessing the real server. To prevent such attacks, you can use the **mac-spoofing-defend enable** command to configure the network-side interface connected to the server as a trusted interface. The MAC address learned by the interface will not be learned by other interfaces. This prevents the attacks of bogus packets with the server MAC address.

Before configuring an interface as a trusted interface, you must use the **mac-spoofing-defend enable** command to enable global MAC spoofing defense.

Precautions

After you run the **undo mac-spoofing-defend enable** command in the system view to disable global MAC spoofing defense, the **mac-spoofing-defend enable** command cannot be used in the interface view.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after MAC spoofing defense is enabled globally, the real-time performance of MAC address flapping detection on the interfaces that are not enabled with MAC spoofing defense decreases.

On the S300 and S500, after MAC spoofing defense is enabled globally, the real-time performance of MAC address flapping detection on the interfaces that are not enabled with MAC spoofing defense decreases.

Example

Enable global MAC spoofing defense.

```
<HUAWEI> system-view
[HUAWEI] mac-spoofing-defend enable
```

5.1.52 mac-syn realtime enable

Function

The **mac-syn realtime enable** command enables real-time MAC address synchronization.

The **undo mac-syn realtime enable** command disables real-time MAC address synchronization.

By default, real-time MAC address synchronization is disabled.

Format

mac-syn realtime enable { **all** | **slot** *slot-id* }

undo mac-syn realtime enable { **all** | **slot** *slot-id* }

NOTE

This command is supported only on the S6720-EI, S6720S-EI, and S6735-S.

Parameters

Parameter	Description	Value
all	Enables real-time MAC address synchronization in all slots.	-
slot *slot-id*	Enables real-time MAC address synchronization in a specified slot.	The value is an integer and must be the slot ID of a running card.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device connects to a Linux server through an aggregated link, to ensure that services are not affected in the case of an active/standby link switchover on the server, run the **mac-syn realtime enable** command on the device to enable real-time MAC address synchronization.

Prerequisites

Before running the **mac-syn realtime enable** { **all** | **slot** *slot-id* } command, run the **mac-syn receive enable** { **all** | **slot** *slot-id* } command in the diagnostic view.

Example

Enable real-time MAC address synchronization.

```
<HUAWEI> system-view
[HUAWEI] mac-syn realtime enable all
```

5.1.53 port bridge enable

Function

The **port bridge enable** command enables the port bridge function on an interface. The interface then can forward packets whose source and destination MAC addresses are both learned by this interface.

The **undo port bridge enable** command disables the port bridge function.

By default, the port bridge function is disabled on an interface.

Format

port bridge enable

undo port bridge enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

The port bridge function enables an interface to forward packets whose source and destination MAC addresses are both learned on the interface. By default, an interface discards packets whose source and destination MAC addresses are both learned on the interface.

When enabled with the port bridge function, the interface forwards such packets if their destination MAC addresses are found in the MAC address table.

The port bridge function is used in the following scenarios:

- The switch connects to devices that do not support Layer 2 forwarding. When users connected to the devices need to communicate, the devices send user packets to the switch for forwarding. Because source and destination MAC addresses of the packets are learned on the same interface, the port bridge function needs to be enabled on the interface so that the interface can forward such packets.
- The switch is used as an access device in a data center and is connected to servers. For example, take multiple servers hosting multiple virtual machines that need to transmit data to each other. By enabling the port bridge function on the interfaces connected to the servers, you allow the switch to forward data packets between the virtual machines at a higher speed than if the servers perform the switching operations.

Example

Enable the port bridge function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port bridge enable
```

5.1.54 remark destination-mac

Function

The **remark destination-mac** command configures an action of re-marking the destination MAC address in packets in a traffic behavior.

The **undo remark destination-mac** command deletes the configuration.

By default, an action of re-marking the destination MAC address in packets is not configured in a traffic behavior.

NOTE

Only the S6735-S, S6720-EI and S6720S-EI support this command.

Format

remark destination-mac *mac-address*

undo remark destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number with 1 to 4 digits. The value must be a unicast MAC address.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **remark destination-mac** command to re-mark the destination MAC address in packets in a traffic behavior so that the downstream device can identify packets and provide differentiated services.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing destination MAC address re-marking.

Precautions

- In a traffic behavior, the **remark destination-mac** command cannot be used with the **redirect ip-nexthop** or **redirect ip-multihop** command.
- A traffic policy containing **remark destination-mac** cannot be applied to the outbound direction.
- If you run the **remark destination-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure the traffic behavior **b1**: The destination MAC address of packets is re-marked to 00e0-fc07-bed3.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark destination-mac 00e0-fc07-bed3
```

5.1.55 reset mac-address flapping record

Function

The **reset mac-address flapping record** command clears MAC address flapping records.

Format

reset mac-address flapping record

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting MAC address flapping statistics, run the **reset mac-address flapping record** command to clear the current statistics.

Precautions

This command deletes only the historical MAC address flapping records that have been aged.

After clearing MAC address flapping records, you can run the **display mac-address flapping record** command to view current MAC address flapping records.

The cleared MAC address flapping records cannot be restored.

Example

Clear MAC address flapping records.

```
<HUAWEI> reset mac-address flapping record
```

5.1.56 undo mac-address

Function

The **undo mac-address** command deletes one or more MAC address entries.

Format

undo mac-address [**all** | **dynamic**] [*interface-type interface-number* | **vlan** *vlan-id*] *

undo mac-address { **all** | **dynamic** } [**vsi** *vsi-name*]

undo mac-address *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a MAC address entry to be deleted.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
interface-type interface-number	Specifies the interface in a MAC address entry to be deleted.	-
vlan *vlan-id*	Specifies the VLAN ID in a MAC address entry to be deleted.	The value is an integer that ranges from 1 to 4094.
all	Specifies that all MAC address entries excluding DHCP sticky MAC address entries, sticky-config MAC address and NAC MAC address entries are deleted.	-
vsi *vsi-name*	Specifies the name of a VSI. The VSI must have been created. **NOTE** Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this parameter.	-
dynamic	Deletes dynamic MAC address entries, that is, MAC address entries learned by an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A MAC address table saves a limited number of MAC addresses. If the MAC address table is full, the device cannot learn new MAC address entries until old MAC addresses are aged out. Packets matching no MAC address entry are broadcast, wasting bandwidth resources. This command can delete useless MAC address entries to release the MAC address table space.

You can delete some of MAC address entries as required. For example:

- If you do not specify *interface-type interface-number*, the command deletes MAC address entries of the specified type on all interfaces.
- If you do not specify **vlan** *vlan-id*, the command deletes MAC address entries of the specified type in all VLANs.

Precautions

If port security and NAC authentication are enabled on an interface and a user is successfully authenticated on the interface and connects to the network, the **undo mac-address** command cannot delete MAC address entries of the user. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if **authentication mode** is used to set the user access mode to multi-share, the **undo mac-address** command can delete MAC address entries of the user.

MAC address entries of the sticky-config type cannot be deleted through the **undo mac-address** command, and can be deleted only through the **undo port-security mac-address sticky-config** command.

Example

Delete all MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address all
```

Delete all dynamic MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address dynamic
```

Delete all MAC address entries on gigabitethernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address gigabitethernet 0/0/1
```

Delete all MAC address entries in VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address vlan 5
```

Delete all dynamic MAC address entries in the VSI **a2**.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address dynamic vsi a2
```

Delete all MAC address entries in which the MAC address is 00e0-fc04-0004.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address 00e0-fc04-0004
```

5.1.57 undo mac-address temporary

Function

The **undo mac-address temporary** command deletes all the temporary MAC address entries in the system.

Format

undo mac-address temporary

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the interface card is pulled out, the static MAC address entries configured on the interfaces are reserved as temporary MAC address entries. After the interface card is plugged again, the static MAC address entries are restored.

If the interface card is not plugged after being pulled out, the temporary MAC address entries become unnecessary and occupy the system resources. In this case, you can run the **undo mac-address temporary** command to delete all the temporary MAC address entries in the system.

Example

Delete all the temporary MAC address entries in the system.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address temporary
```

5.1.58 undo mac-limit all

Function

The **undo mac-limit all** command deletes all MAC address limiting rules.

Format

undo mac-limit all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command deletes all the rules configured by the **mac-limit** command.

Precautions

Before using this command, run the **display mac-limit** command to check the MAC address limiting rules and confirm your operation.

Example

Delete all MAC address limiting rules.

```
<HUAWEI> system-view
[HUAWEI] undo mac-limit all
```

5.2 Link Aggregation Commands

5.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.2.2 authentication-mode (E-Trunk view)

Function

The **authentication-mode** command configures the E-Trunk authentication and encryption mode.

The **undo authentication-mode** command restores the default E-Trunk authentication and encryption mode.

By default, the E-Trunk authentication and encryption mode is hmac-sha1.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

authentication-mode { **hmac-sha1** | **hmac-sha256** | **enhanced-hmac-sha256** }

undo authentication-mode

Parameters

Parameter	Description	Value
hmac-sha1	Indicates that the E-Trunk authentication and encryption mode is hmac-sha1.	-
hmac-sha256	Indicates that the E-Trunk authentication and encryption mode is hmac-sha256. **NOTE** **hmac-sha256** is more secure than **hmac-sha1**, so you are advised to configure **hmac-sha256** as the E-Trunk authentication and encryption mode.	-
enhanced-hmac-sha256	Indicates that the E-Trunk authentication and encryption mode is **enhanced-hmac-sha256**. **NOTE** **enhanced-hmac-sha256** is more secure than **hmac-sha256** and **hmac-sha1**, so you are advised to configure **enhanced-hmac-sha256** as the E-Trunk authentication and encryption mode.	-

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve system security, run the **authentication-mode** command to configure the E-Trunk authentication and encryption mode.

Precautions

Two devices in an E-Trunk must have the same E-Trunk authentication and encryption mode.

Example

Configure the E-Trunk authentication and encryption mode as **enhanced-hmac-sha256**.

```
<HUAWEI> system-view
```

```
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] authentication-mode enhanced-hmac-sha256
```

5.2.3 assign trunk

Function

The **assign trunk** command sets the maximum number of link aggregation groups (LAGs) and the maximum number of member interfaces in each LAG.

The **undo assign trunk** command restores the default maximum number of LAGs and the default maximum number of member interfaces in each LAG.

Table 5-16 describes the default maximum numbers of LAGs and member interfaces in each LAG on a device.

Table 5-16 Default maximum numbers of LAGs and member interfaces in each LAG

Model	Default Maximum Number of LAGs	Default Maximum Number of Member Interfaces in each LAG
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S	128	32
S6735-S, S6720-EI and S6720S-EI	128	8

NOTE

This command is supported only on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI and S6720S-EI.

Format

assign trunk { **trunk-group** *group-number* | **trunk-member** *member-number* }*

undo assign trunk

Parameters

Parameter	Description	Value
trunk-group*group-number*	Specifies the number of LAGs.	The value is an integer ranging 32 to 512 for the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and 32 to 128 for other models. The value multiplied by *member-number* cannot exceed 2048 on the S6735-S, S6720-EI and S6720S-EI. The value multiplied by *member-number* cannot exceed 8192 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.
trunk-member*member-number*	Specifies the maximum number of member interfaces in each LAG.	The value is an integer that can be 8, 16, 32, or 64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, a switch supports a fixed maximum number of LAGs and a fixed maximum number of member interfaces in each LAG. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the maximum number of LAGs and the maximum number of member interfaces in each LAG, implementing flexible networking and meeting various service requirements.

Precautions

- By default, if the value of *member-number* configured for an Eth-Trunk using the **assign trunk** { **trunk-group** *group-number* | **trunk-member** *member-number* }* command is larger than or equal to 16 on the S6735-S, S6720-EI and S6720S-EI or larger than 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, known unicast packets are load balanced using the enhanced mode, and broadcast, unknown-unicast, and multicast (BUM) packets are load balanced based on their source and destination MAC addresses. Known unicast packets must be load balanced using the enhanced mode (the load balancing mode can be configured using the **load-balance** command). Otherwise, packet loss or uneven load balancing may occur.

- After the Eth-Trunk specifications are modified, save the configuration and restart the switch to make the modification take effect.
- If you use the **assign trunk** command to modify Eth-Trunk specifications, the existing Eth-Trunk configuration will become invalid or be lost. Exercise caution when you run the **assign trunk** command. When the configured Eth-Trunk specifications are reduced and the Eth-Trunks that exceed the specifications are configured, the configuration of excess Eth-Trunks is invalid.
- If an Eth-Trunk interface has been created on a switch and you want to expand the Eth-Trunk specifications, you need to run the **load-balance enhanced profile** command to configure an enhanced load balancing profile for all Eth-Trunks first. After Eth-Trunk specifications are expanded, you are advised not to delete the configured enhanced load balancing profile because this operation will cause uneven load balancing.
- After the **reset netconf db-configuration** or **reset saved-configuration** command is run, the **assign trunk** command configuration is cleared, that is, the default configuration is restored.

Example

Set the maximum number of LAGs to 64 and the maximum number of member interfaces in each LAG to 16.

```
<HUAWEI> system-view
[HUAWEI] assign trunk trunk-group 64 trunk-member 16
```

5.2.4 collect forward-path

Function

The **collect forward-path** command configures the device to collect traffic information.

The **undo collect forward-path** command configures the device not to collect traffic information.

By default, the device does not collect traffic information.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

collect forward-path { { **sip** *source-ip-address* **dip** *destination-ip-address* [**sport** *source-port* **dport** *destination-port* [**protocol** { *protocol-number* | **gre** | **icmp** | **igmp** | **ip** | **ipinip** | **ospf** | **tcp** | **udp** }]] } | { **smac** *source-mac-address* | **dmac** *dest-mac-address* | **vlan** *vlan-id* | **l2-protocol** { *protocol-value* | **arp** | **ip** | **ipv6** | **mpls** | **rarp** } } * } { **ingress** | **egress** | **both** } [**interval** *interval-time*]

undo collect forward-path { { **sip** *source-ip-address* **dip** *destination-ip-address* [**sport** *source-port* **dport** *destination-port* [**protocol** { *protocol-number* | **gre** | **icmp** | **igmp** | **ip** | **ipinip** | **ospf** | **tcp** | **udp** }]] } | { **smac** *source-mac-address* | **dmac** *dest-mac-address* | **vlan** *vlan-id* | **l2-protocol** { *protocol-value* | **arp** | **ip** | **ipv6** | **mpls** | **rarp** } } * } { **ingress** | **egress** | **both** } [**interval** *interval-time*]

Parameters

Parameter	Description	Value
sip *source-ip-address*	Specifies the source IP address.	The value is in dotted decimal notation.
dip *destination-ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
sport *source-port*	Specifies the source port number.	The value is an integer that ranges from 0 to 65535.
dport *destination-port*	Specifies the destination port number.	The value is an integer that ranges from 0 to 65535.
protocol { *protocol-number* | **gre** | **icmp** | **igmp** | **ip** | **ipinip** | **ospf** | **tcp** | **udp** }	Specifies the protocol number or type. ● *protocol-number* specifies the protocol number. ● **gre** indicates that the protocol type is GRE. ● **icmp** indicates that the protocol type is ICMP. ● **igmp** indicates that the protocol type is IGMP. ● **ip** indicates that the protocol type is IP. ● **ipinip** indicates that the protocol type is IPinIP. ● **ospf** indicates that the protocol type is OSPF. ● **tcp** indicates that the protocol type is TCP. ● **udp** indicates that the protocol type is UDP.	The value of *protocol-number* is an integer that ranges from 1 to 255.

Parameter	Description	Value
smac *source-mac-address*	Specifies the source MAC address.	The value is in hexadecimal notation.
dmac *dest-mac-address*	Specifies the destination MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
l2-protocol { *protocol-value* | **arp** | **ip** | **ipv6** | **mpls** | **rarp** }	Specifies the Layer 2 protocol number or type. ● *protocol-value* specifies the protocol number. ● **arp** indicates that the protocol type is ARP and the protocol number is 0x0806. ● **ip** indicates that the protocol type is IP and the protocol number is 0x0800. ● **ipv6** indicates that the protocol type is IPv6 and the protocol number is 0x86dd. ● **mpls** indicates that the protocol type is MPLS and the protocol number is 0x8847. ● **rarp** indicates that the protocol type is RARP and the protocol number is 0x8035.	The value of *protocol-value* is in hexadecimal notation and must start with 0x. The value contains three or six digits.
ingress	Indicates the inbound direction.	-
egress	Indicates the outbound direction.	-
both	Indicates the inbound and outbound directions.	-

Parameter	Description	Value
interval *interval-time*	Indicates the collection duration.	The value is an integer that ranges from 0 to 1440, in minutes. The default value is 10. The value 0 indicates that the device continuously collects inbound and outbound interfaces and traffic information in packets with 5-tuple information.

Views

User view, System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The packet information contains the source and destination IP addresses, source and destination port numbers, source and destination MAC addresses, and protocol type. Traffic transmitted on each device interface contains different information. You can run this command to configure the device to collect traffic information, which helps you locate faults and understand the traffic forwarding path.

Precautions

The device can collect inbound and outbound interfaces and traffic information of a maximum of 8 flows.

In the outbound direction, traffic information collection (with the **egress** or **both** parameter specified) conflicts with a traffic policy or simplified traffic policy. If traffic information collection, traffic policy, or simplified traffic policy are configured, one of them may not take effect.

When the device restarts or an active/standby switchover occurs in a CSS, the collection information and report configured by the **collect forward-path** command will be deleted.

If traffic information collection is no longer required after the collection time ends, run the **undo collect forward-path** command to disable the device from collecting traffic information.

After the **undo collect forward-path** command is run, the collected traffic statistics will be deleted.

If commands for collecting statistics on traffic with the same packet information are configured and the directions in two consecutive commands are the same or overlap, only the previous command takes effect. Examples are as follows:

- Scenarios where **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress interval 20** and **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress interval 30** are configured in sequence: The **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress interval 30** command does not take effect.
- Scenarios where **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress** and **collect forward-path sip 10.1.1.1 dip 10.2.2.2 both** are configured in sequence: The **collect forward-path sip 10.1.1.1 dip 10.2.2.2 both** command does not take effect.
- Scenarios where **collect forward-path sip 10.1.1.1 dip 10.2.2.2 both** and **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress** are configured in sequence: The **collect forward-path sip 10.1.1.1 dip 10.2.2.2 ingress** command does not take effect.

Example

Configure the device to collect traffic information with source IP address 10.1.1.1 and destination IP address 10.2.2.2.

```
<HUAWEI> system-view
[HUAWEI] collect forward-path sip 10.1.1.1 dip 10.2.2.2 both
```

5.2.5 display eth-trunk

Function

The **display eth-trunk** command displays the Eth-Trunk configuration.

Format

display eth-trunk [*trunk-id* [**interface** *interface-type interface-number* | **verbose**]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
interface *interface-type interface-number*	Specifies a member interface. *interface-type* specifies the type of the member interface. *interface-number* specifies the number of the member interface.	-
verbose	Displays the detailed configuration of a specified Eth-Trunk, including the Eth-Trunk traffic statistics.	-

Views

All views

Default Level

1 : Monitoring level

Usage Guidelines

Usage Scenario

After configuring an Eth-Trunk on a device, you can run the **display eth-trunk** command to check whether the Eth-Trunk configuration is correct.

When using the **display eth-trunk** command, pay attention to the following points:

- If no parameter is specified, the **display eth-trunk** command displays the configurations of all Eth-Trunks.
- If only *trunk-id* is specified, the **display eth-trunk** command displays the configuration of a specified Eth-Trunk.
- If *trunk-id* and **interface** *interface-type interface-number* are specified, the configuration of member interfaces of the specified Eth-Trunk is displayed.
- If *trunk-id* is specified and **verbose** is configured, the **display eth-trunk** command displays detailed configuration of a specified Eth-Trunk, including the Eth-Trunk traffic statistics.

Prerequisites

The Eth-Trunk has been correctly configured. If no Eth-Trunk is configured, when you run this command, the system displays an error message.

Precautions

If there are traffic statistics about many Eth-Trunks, you are advised to specify *trunk-id* or **interface** *interface-type interface-number* to filter output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly updated, and required information cannot be located.
- The system does not respond because of long-time information traverse and search.

Example

Display the configurations of all Eth-Trunks.

```
<HUAWEI> display eth-trunk
Eth-Trunk10's state information is:
Local:
LAG ID: 10                WorkingMode: LACP
Preempt Delay Time: 10    Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120      System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up        Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName          Status   PortType PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/2   Selected 1GE      10      262    2609    10111100  1
GigabitEthernet0/0/3   Selected 1GE      10      263    2609    10111100  1
GigabitEthernet0/0/4   Unselect 1GE      32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName          SysPri SystemID       PortPri PortNo PortKey PortState
GigabitEthernet0/0/2   32768  00e0-fc6e-bb11 32768   262    2609    10111100
GigabitEthernet0/0/3   32768  00e0-fc6e-bb11 32768   263    2609    10111100
GigabitEthernet0/0/4   32768  00e0-fc6e-bb11 32768   264    2609    10110000
```

```
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                          Status      Weight
GigabitEthernet0/0/1                Up          1
```

Display the configuration of Eth-Trunk 11 in manual load balancing mode.

```
<HUAWEI> display eth-trunk 11
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                          Status      Weight
GigabitEthernet0/0/1                Up          1
```

Display the configuration of Eth-Trunk 10 in LACP mode.

```
<HUAWEI> display eth-trunk 10
Eth-Trunk10's state information is:
Local:
LAG ID: 10                  WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName                 Status   PortType     PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/2           Selected 1GE          10      262    2609    10111100  1
GigabitEthernet0/0/3           Selected 1GE          10      263    2609    10111100  1
GigabitEthernet0/0/4           Unselect 1GE          32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                 SysPri    SystemID  PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/2           32768  00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet0/0/3           32768  00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet0/0/4           32768  00e0-fc6e-bb11  32768  264   2609      10110000
```

Display the detailed configuration of Eth-Trunk 11 in manual load balancing mode.

```
<HUAWEI> display eth-trunk 11 verbose
Eth-Trunk11's state information is:
WorkingMode: NORMAL         Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1  Max Bandwidth-affected-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 1
--------------------------------------------------------------------------------
PortName                          Status      Weight
GigabitEthernet0/0/1                Up          1

Flow statistic
 Interface GigabitEthernet0/0/1,
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
 Interface Eth-Trunk11
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
```

Display the detailed configuration of Eth-Trunk 10 in LACP mode.

```
<HUAWEI> display eth-trunk 10 verbose
Eth-Trunk10's state information is:
Local:
```

```
LAG ID: 10                  WorkingMode: LACP
Preempt Delay Time: 10      Hash arithmetic: According to SIP-XOR-DIP
System Priority: 120        System ID: 0018-82d4-04c3
Least Active-linknumber: 1  Max Active-linknumber: 2
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName                Status   PortType   PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/2          Selected 1GE        10      262    2609    10111100  1
GigabitEthernet0/0/3          Selected 1GE        10      263    2609    10111100  1
GigabitEthernet0/0/4          Unselect 1GE        32768   264    2609    10100000  1

Partner:
--------------------------------------------------------------------------------
ActorPortName                SysPri   SystemID  PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/2          32768  00e0-fc6e-bb11  32768  262   2609      10111100
GigabitEthernet0/0/3          32768  00e0-fc6e-bb11  32768  263   2609      10111100
GigabitEthernet0/0/4          32768  00e0-fc6e-bb11  32768  264   2609      10110000

Flow statistic
 Interface GigabitEthernet0/0/2,
    Last 300 seconds input rate 32 bits/sec, 0 packets/sec
    Last 300 seconds output rate 32 bits/sec, 0 packets/sec
    148 packets input, 18944 bytes, 0 drops
    246 packets output, 31488 bytes, 0 drops
 Interface GigabitEthernet0/0/3,
    Last 300 seconds input rate 32 bits/sec, 0 packets/sec
    Last 300 seconds output rate 32 bits/sec, 0 packets/sec
    147 packets input, 18816 bytes, 0 drops
    246 packets output, 31488 bytes, 0 drops
 Interface GigabitEthernet0/0/4,
    Last 300 seconds input rate 56 bits/sec, 0 packets/sec
    Last 300 seconds output rate 48 bits/sec, 0 packets/sec
    144 packets input, 18432 bytes, 0 drops
    174 packets output, 22272 bytes, 0 drops
 Interface Eth-Trunk10
    Last 300 seconds input rate 96 bits/sec, 0 packets/sec
    Last 300 seconds output rate 96 bits/sec, 0 packets/sec
    439 packets input, 56192 bytes, 0 drops
    666 packets output, 85248 bytes, 0 drops
```

Table 5-17 Description of the **display eth-trunk** command output

Item	Description
Local	Configuration of the local Eth-Trunk.
LAG ID	ID of the Eth-Trunk.
WorkingMode	Working mode of the Eth-Trunk: ● NORMAL: manual load balancing mode ● LACP: LACP mode
Preempt Delay Time	Preemption delay time: ● If LACP preemption is enabled, the preemption time is displayed and expressed in seconds. ● If LACP preemption is disabled, the value is displayed as Disabled.

Item	Description
Hash arithmetic	Hash algorithm used for load balancing among member interfaces of the Eth-Trunk. The hash algorithm is configured by using the **load-balance** command. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.
SysPri	System LACP priority. To configure the LACP system priority, run the **lacp priority** command.
SystemID	System ID.
Least Active-linknumber	Minimum number of active member links in Up state. To configure the minimum number of active member links in Up state, run the **least active-linknumber** command.
Max Active-linknumber	Maximum number of active member links in Up state. To configure the maximum number of active member links in Up state, run the **max active-linknumber** command.
Max Bandwidth-affected-linknumber	Maximum number of connections that affect the Eth-Trunk bandwidth.
Operate status	Eth-Trunk status: ● UP ● DOWN
Number Of Up Port In Trunk	Number of member interfaces in Up state in the Eth-Trunk.
ActorPortName	Name of a member interface.

Item	Description
Status	Status of the local member interface in LACP mode: • Selected: A member interface in Selected state is active. • Unselect: A member interface in Unselected state is inactive. • ForceFwd: A member interface can forward Layer 2 traffic. Status of the local member interface in manual load balancing mode: • Up: indicates that the interface is properly started. • Down: indicates that the interface is faulty.
PortType	Type of the local member interface.
PortPri	LACP priority of the member interface.
PortNo	Number of the member interface in LACP mode.
PortKey	Key value of the member interface in LACP mode.

Item	Description
PortState	Status variable of the member interface. The status variable is eight bits, such as 10111100. The descriptions of each bit are as follows: - Bit 1: Whether the member interface is an Actor. This bit has a fixed value 1. - Bit 2: Whether the member interface uses a long or short timeout interval to receive LACPDUs. 1: The member interface uses a short timeout interval. 0: The member interface uses a long timeout interval. By default, an Eth-Trunk member interface uses the long timeout interval (90s) to receive LACPDUs. To set the timeout interval, run the **lacp timeout** command. - Bit 3: Whether the system allows the member interface to be aggregated. 1: The system allows the member interface to be aggregated. 0: The system does not allow the member interface to be aggregated. - Bit 4: Whether the member interface is added to the link aggregation group (LAG). 1: The member interface is added to the LAG. 0: The member interface is not added to the LAG. - Bit 5: Whether the member interface can receive LACPDUs. 1: The member interface can receive LACPDUs. 0: The member interface cannot receive LACPDUs. - Bit 6: Whether the member interface can send LACPDUs. 1: The member interface can send LACPDUs. 0: The member interface cannot send LACPDUs. - Bit 7: Whether the LACPDUs contain default parameter values.

Item	Description
	1: The LACPDUs contain default parameter values. 0: The LACPDUs do not contain default parameter values. ● Bit 8: Whether the receive state machine of the Actor is in Expired state. 1: The receive state machine of the Actor is in Expired state. 0: The receive state machine of the Actor is not in Expired state.
Weight	Weight of the member interface.
Partner	Information about member interfaces of the remote Eth-Trunk. The Eth-Trunk must work in LACP mode.
Flow statistic	Eth-Trunk traffic statistics.
Last 300 seconds input/output rate	Rates for sending and receiving bits and packets on the interface in the last 300 seconds.
input/output	Number of packets received or sent by the interface.
packets	Total number of packets that the interface receives or sends.
bytes	Total number of bytes that the interface receives or sends.
drops	Number of packets that the interface drops.

5.2.6 display trunk configuration

Function

The **display trunk configuration** command displays the maximum number of LAGs and the maximum number of member interfaces in each LAG.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI and S6720S-EI support this command.

Format

display trunk configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To facilitate flexible networking, run the **assign trunk** command to set the maximum number of LAGs and the maximum number of member interfaces in each LAG. You can run the **display trunk configuration** command to view the configuration.

Example

Display the maximum number of LAGs and the maximum number of member interfaces in each LAG.

```
<HUAWEI> display trunk configuration
--------------------------------------------------
Item           Default    Current    Configured
--------------------------------------------------
trunk-group     128         64          64
trunk-member     8          16          16
--------------------------------------------------
```

Table 5-18 Description of the **display trunk configuration** command output

Item	Description
Item	The name of item.
Default	Default Eth-Trunk specifications supported by the device.
Current	Current Eth-Trunk specifications supported by the device.
Configured	Configured Eth-Trunk specifications. If the configured Eth-Trunk specifications are different from the current Eth-Trunk specifications, the configured Eth-Trunk specifications take effect after the device restarts. To specify the parameter, run the **assign trunk** command.
trunk-group	Maximum number of Eth-Trunks supported by the device.
trunk-member	Maximum number of member interfaces in each Eth-Trunk.

5.2.7 display eth-trunk load-balance

Function

The **display eth-trunk load-balance** command displays the load balancing mode of an Eth-Trunk.

Format

display eth-trunk [*trunk-id*] **load-balance**

Parameters

Parameter	Description	Value
trunk-id	Displays the load balancing mode of a specified Eth-Trunk. *trunk-id* specifies the ID of the Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the load balancing mode of an Eth-Trunk is configured, you can run this command to view the load balancing mode of the Eth-Trunk. If *trunk-id* is not specified, the load balancing modes of all Eth-Trunks are displayed.

Example

Display the load balancing mode of Eth-Trunk 1.

```
<HUAWEI> display eth-trunk 1 load-balance
Eth-Trunk1's load-balance information:
 Load-balance Configuration: SIP-XOR-DIP
 Load-balance options used per-protocol:
  L2  : Source XOR Destination MAC address, Vlan ID, Ethertype, Ingress-port
  IPv4: Source XOR Destination IP address, Source XOR Destination TCP/UDP port
  IPv6: Source XOR Destination IP address, Source XOR Destination TCP/UDP port
  MPLS: Source XOR Destination IP address, Source XOR Destination TCP/UDP port
```

Table 5-19 Description of the **display eth-trunk load-balance** command output

Item	Description
Load-balance Configuration	Configured load balancing mode. The options are as follows: - SIP: Eth-Trunk load balancing based on source IP addresses. - DIP: Eth-Trunk load balancing based on destination IP addresses. - SIP-XOR-DIP: Eth-Trunk load balancing based on source and destination IP addresses. - SA: Eth-Trunk load balancing based on source MAC addresses. - DA: Eth-Trunk load balancing based on destination MAC addresses. - SA-XOR-DA: Eth-Trunk load balancing based on source and destination MAC addresses. - ENHANCED: Enhanced Eth-Trunk load balancing. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.
Unicast load-balance enhanced mode **NOTE** This information is displayed only when the load balancing mode is set to ENHANCED.	Whether traffic is load balanced based on the inner IP address, outer IP address, or both. - outer: Traffic is load balanced based on the outer IP address. - inner: Traffic is load balanced based on the inner IP address. - inner and outer: Traffic is load balanced based on both the inner and outer IP addresses.
Load-balance enhanced profile **NOTE** This information is displayed only when the load balancing mode is set to ENHANCED.	Name of a load balancing profile.

Item	Description
Load-balance options used per-protocol	Load balancing parameters of different types of packets.

5.2.8 display e-trunk

Function

The **display e-trunk** command displays E-Trunk information.

Format

display e-trunk { **brief** | *e-trunk-id* }

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
brief	Displays brief E-Trunk information.	-
e-trunk-id	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an E-Trunk is configured, you can run the **display e-trunk** command to view information about the E-Trunk.

Example

Display information about E-Trunk 1.

```
<HUAWEI> display e-trunk 1
                        The E-Trunk information
E-TRUNK-ID : 1                          Revert-Delay-Time (s) : 120
```

```
Priority : 10                    System-ID : 00e0-fc12-3456
Peer-IP : 10.1.1.2                 Source-IP : 10.1.1.1
State : Master                     Causation : TIMEOUT
Send-Period (100ms) : 10              Fail-Time (100ms) : 200
Receive : 1                      Send : 1006
RecDrop : 0                       SndDrop : 0
Peer-Priority : -                  Peer-System-ID : -
Peer-Fail-Time (100ms) : -            BFD-Session : 1
Description : -
Sequence : Enable
------------------------------------------------------------------------------
                     The Member information
Type      ID  LocalPhyState  Work-Mode     State   Causation        Remote-
ID
Eth-Trunk 10  Up            auto          Master  ETRUNK_INIT      17
```

Table 5-20 Description of the **display e-trunk** command output

Item	Description
E-TRUNK-ID	E-Trunk ID. To specify the parameter, run the **e-trunk** command.
Revert-Delay-Time	Revertive switching delay of the E-Trunk. To specify the parameter, run the **timer revert delay** command.
Priority	Priority of the E-Trunk. To specify the parameter, run the **priority** command.
System-ID	System ID of the local end. To specify the parameter, run the **lacp e-trunk system-id** command.
Peer-IP/Source-IP	Local and remote IP addresses of the E-Trunk. To specify the parameter, run the **peer-address source-address** command.
State	E-Trunk status: ● 1: Init ● 2: Backup ● 3: Master

Item	Description
Causation	E-Trunk status change cause: - PRI(1): The E-Trunk status is determined by the E-Trunk priority. - TIMEOUT(2): The local device changes from the backup to the master because it does not receive hello packets from the remote device within the timeout interval. - BFD_DOWN(3): The BFD session on the local device detects that the link between the local device and the remote device is Down. - PEER_TIMEOUT(4): The remote device changes from the backup to the master because it does not receive hello packets from the local device within the timeout interval. - PEER_BFD_DOWN(5): The BFD session on the remote device detects that the link between the local device and the remote device is Down. - ALL_MEMBER_DOWN(6): Both the two member devices of the E-Trunk are Down. - INIT(7): The E-Trunk is being initialized.
Send-Period	Interval for sending hello packets. To specify the parameter, run the **timer hello** command.
Fail-Time	Timeout interval for the E-Trunk to receive packets. To specify the parameter, run the **timer hold-on-failure multiplier** command.
Receive/Send	Number of packets received and sent by the E-Trunk.
RecDrop/SndDrop	Number of received and sent packets discarded by the E-Trunk.
Peer-Priority	Priority of the remote device.
Peer-System-ID	System MAC address of the remote device.
Peer-Fail-Time	Timeout interval of the remote device.
BFD-Session	BFD session bound to the E-Trunk. To specify the parameter, run the **e-trunk track bfd-session** command.
Description	Description of the E-Trunk.

Item	Description
Sequence	E-Trunk sequence number check function status: ● Enable ● Disable You can run the **sequence enable** command in the E-Trunk view to configure the E-Trunk sequence number check function or modify its state.
Type	Member type. The value is Eth-Trunk.
ID	Member ID. To add Eth-Trunks with different IDs on two devices to the same E-Trunk, run the **e-trunk** *e-trunk-id* **remote-eth-trunk** *eth-trunk-id* command on the Eth-Trunk interface view of the two devices to specify remote Eth-Trunk IDs to ensure that the E-Trunk works properly.
LocalPhyState	Physical status of a member link: ● 1: Up ● 2: Down
Work-Mode	Working mode of a member interface: ● 1: auto ● 2: force-backup ● 3: force-master To specify the parameter, run the **e-trunk mode** command.
State	Status of a member interface: ● 1: Master ● 2: Backup

Item	Description
Causation	Cause for the member interface status change: ● FORCE_BACKUP(1): The member interface is forcibly to work in backup state. ● FORCE_MASTER(2): The member interface is forcibly to work in master state. ● ETRUNK_INIT(3): The member interface works in automatic state but the E-Trunk is being initialized. ● ETRUNK_BACKUP(4): The member interface works in automatic state but the E-Trunk is in backup state. ● ETRUNK_MASTER(5): The member interface works in automatic state but the E-Trunk is in master state. ● PEER_MEMBER_DOWN(6): The remote device is Down. ● PEER_MEMBER_UP(7): The remote device is Up. ● NO_PEER_MEMBER(8): There is no remote device.
Remote-ID	Eth-Trunk ID of the remote device.

5.2.9 display e-trunk packet-statistics

Function

The **display e-trunk packet-statistics** command displays E-Trunk packet statistics.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display e-trunk packet-statistics [**e-trunk-id** *e-trunk-id*]

Parameters

Parameter	Description	Value
e-trunk-id *e-trunk-id*	Display packet statistics about an E-Trunk. *e-trunk-id* specified the ID of the E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an E-Trunk is successfully configured, you can run the **display e-trunk packet-statistics** command to check packet statistics about the E-Trunk. The command output helps you to determine whether data is normal and to locate faults.

Example

Display E-Trunk packet statistics on the device.

```
<HUAWEI> display e-trunk packet-statistics
E-Trunk-ID errors : 0
Length errors     : 0

E-TRUNK-ID : 10
  Sent packets                               : 355
  Failed to send packets                     : 355
  Received packets                           : 0
  Received packets with priority errors      : 0
  Received packets with fail-time errors     : 0
  Received packets with state errors         : 0
  Received packets with state reason errors  : 0
  Received packets with peer-ip errors       : 0
  Received packets with authentication errors : 0
  Received packets with TLV check errors     : 0
  Received packets with system-id errors     : 1
  Dropped packets with BFD protection        : 0
  Received packets with member errors        : 53
  Received packets with sequence check errors : 0
```

Table 5-21 Description of the **display e-trunk packet-statistics** command output

Item	Description
E-Trunk-ID errors	Number of packets with incorrect E-Trunk IDs.
Length errors	Number of packets with incorrect lengths.
E-TRUNK-ID	E-Trunk ID.
Sent packets	Number of sent E-Trunk packets.
Failed to send packets	Number of E-Trunk packets that fails to be sent.
Received packets	Number of received E-Trunk packets.
Received packets with priority errors	Number of received E-Trunk packets with incorrect priorities.
Received packets with fail-time errors	Number of received E-Trunk packets with timeout errors.

Item	Description
Received packets with state errors	Number of received E-Trunk packets with incorrect states.
Received packets with state reason errors	Number of received E-Trunk packets with incorrect state reasons.
Received packets with peer-ip errors	Number of received E-Trunk packets with incorrect remote IP addresses.
Received packets with authentication errors	Number of received E-Trunk packets with authentication errors.
Received packets with TLV check errors	Number of received E-Trunk packets with TLV check errors.
Received packets with system-id errors	Number of received E-Trunk packets with incorrect system IDs.
Dropped packets with BFD protection	Number of E-Trunk packets dropped during the active/standby switchover because BFD is used.
Received packets with member errors	Number of packets generated when the switch detects that Eth-Trunk member interfaces at both ends are different.
Received packets with sequence check errors	Number of received E-Trunk packets failing the sequence number check.

5.2.10 display e-trunk state-change

Function

The **display e-trunk state-change** command displays the latest 10 status changes of an E-Trunk member interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display e-trunk *e-trunk-id* **state-change member-interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
e-trunk-id	Displays the latest 10 status changes of a specified E-Trunk.	The value is an integer that ranges from 1 to 16.
member-interface *interface-type* *interface-number*	Displays the latest 10 status changes of a specified E-Trunk member interface. *interface-type* can only be Eth-Trunk.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an E-Trunk is configured, you can run the **display e-trunk state-change** command to check the status changes of an E-Trunk member interface.

Prerequisites

An Eth-Trunk has been added to the E-Trunk.

Example

Display the status changes of Eth-Trunk 10 in E-Trunk 1.

```
<HUAWEI> display e-trunk 1 state-change member-interface Eth-Trunk 10
Time                          SourceState    DestState   Reason
-------------------------------------------------------------------------------
2013-07-25 10:41:30-08:00      Backup          Master      PEER_MEMBER_DOWN
```

Table 5-22 Description of the **display e-trunk state-change** command output

Item	Description
Time	Time when the status of the E-Trunk's member Eth-Trunk changed.
SourceState	Status of the E-Trunk's member Eth-Trunk before the status change.
DestState	State of the E-Trunk's member Eth-Trunk after the status change

Item	Description
Reason	Reason for the status change of the E-Trunk's member Eth-Trunk: ● FORCE_BACKUP: The E-Trunk's member Eth-Trunk is forcibly in backup state. ● FORCE_MASTER: The E-Trunk's member Eth-Trunk is forcibly in master state. ● ETRUNK_INIT: The E-Trunk is in initialization state. ● ETRUNK_BACKUP: The E-Trunk is in backup state. ● ETRUNK_MASTER: The E-Trunk is in master state. ● PEER_MEMBER_DOWN: The remote member Eth-Trunk goes Down. ● PEER_MEMBER_UP: The remote member Eth-Trunk goes Up. ● NO_PEER_MEMBER: There is no remote device.

5.2.11 display forward-path

Function

The **display forward-path** command displays collected traffic information.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display forward-path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate faults and understand the traffic forwarding path, run the **collect forward-path** command to configure the device to collect traffic information. To check collected packet information, run the **display forward-path** command.

Prerequisites

The device has been configured to collect traffic information.

Example

Display collected traffic information.

```
<HUAWEI> display forward-path
The brief information of forward-path(s) for L3:
Id       : Report id
SIP      : Source IP address
DIP      : Destination IP address
Sport    : Source port
Dport    : Destination port
Pro      : Protocol type or protocol number
Dir      : Direction
Interval : Interval time (in minutes), 0 means that the system keeps
collecting
------------------------------------------------------------------------------
Id SIP           DIP           Sport Dport Pro    Dir     Interval   Status
------------------------------------------------------------------------------
1  10.1.1.1       10.2.2.2        -     -     -      both    10        done

The brief information of forward-path(s) for L2:
Id       : Report id
SMAC     : Source MAC address
DMAC     : Destination MAC address
VLAN     : VLAN id
Pro      : Protocol type or protocol number
Dir      : Direction
Interval : Interval time (in minutes), 0 means that the system keeps
collecting
------------------------------------------------------------------------------
Id SMAC           DMAC           VLAN   Pro    Dir      Interval     Status
------------------------------------------------------------------------------
2  00e0-fc12-3456   00e0-fc12-3456   10     -     both     10          doing
```

Table 5-23 Description of the **display forward-path** command output

Item	Description
Id	Report ID, that is, number of collected flows. You can run the **display forward-path report** command to view detailed information about inbound and outbound interfaces according to the specified report ID. The IDs are displayed according to the sequence in which the **collect forward-path** command was executed. If an ID is deleted, the existing IDs remain unchanged. The ID configured later is displayed in the position of the deleted ID. For example, IDs 1 and 2 exist on the device. If ID 1 is deleted, ID 2 remains unchanged. If the **collect forward-path** command is used, the new ID is displayed in the position of deleted ID 1. The device can collect inbound and outbound interfaces and traffic information of a maximum of 8 flows.
SIP	Source IP address of collected packets.
DIP	Destination IP address of collected packets.
Sport	Source port number of collected packets.
Dport	Destination port number of collected packets.
Pro	Protocol number or type of collected packets. To configure the protocol number or type of collected packets, run the **collect forward-path** command.
Dir	Direction where packets are collected.
Interval	The collection duration.
Status	Status of collected packets.
SMAC	Source MAC address of collected packets.
DMAC	Destination MAC address of collected packets.
VLAN	VLAN ID of collected packets.

5.2.12 display forward-path report

Function

The **display forward-path report** command displays traffic statistics.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display forward-path report *report-id*

Parameters

Parameter	Description	Value
report-id	Specifies the ID of collected traffic.	The value is an integer that ranges from 1 to 8. The IDs are displayed according to the sequence in which the **collect forward-path** command was executed. If an ID is deleted, the existing IDs remain unchanged. The ID configured later is displayed in the position of the deleted ID. For example, IDs 1 and 2 exist on the device. If ID 1 is deleted, ID 2 remains unchanged. If the **collect forward-path** command is used, the new ID is displayed in the position of deleted ID 1.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate faults and understand the traffic forwarding path, run the **collect forward-path** command to configure the device to collect traffic information. Then run the **display forward-path report** command to check the collection result.

Prerequisites

The device has been configured to collect traffic information.

Example

Display traffic statistics of the report ID 1.

```
<HUAWEI> display forward-path report 1
Source IP address      : 10.1.1.1
Destination IP address : 10.2.2.2
Source port            : -
Destination port       : -
Protocol type          : -
Direction              : both
Interval time          : 10 minute(s)
Status                 : doing
Start time             : 2010-12-30 11:39:11
End time               : -
```

```
--------------------------------------------------------------------------------
Port          Eth-Trunk       Packets         Bytes         Direction
--------------------------------------------------------------------------------
GE0/0/1        1               6555            20           ingress
GE0/0/2        -              6555            20           egress
```

Display traffic statistics of the report ID 2.

```
<HUAWEI> display forward-path report 2
Source MAC address      : 00e0-fc05-0005
Destination MAC address : 00e0-fc06-0006
L2 protocol type        : arp
VLAN id                 : 5
Direction               : both
Interval time           : 1440 minute(s)
Status                  : doing
Start time              : 2015-11-23 17:15:33+02:00
End time                : -
--------------------------------------------------------------------------------
Port          Eth-Trunk       Packets         Bytes         Direction
-------------------------------------------------------------------------------
GE0/0/1        -              46004724        0             ingress
GE0/0/2        -              45999397        0             ingress
```

Table 5-24 Description of the **display forward-path report** command output

Item	Description
Source IP address	Source IP address of collected packets.
Destination IP address	Destination IP address of collected packets.
Source port	Source port number of collected packets.
Destination port	Destination port number of collected packets.
Protocol type	Protocol number or type of collected packets. To configure the protocol number or type of collected packets, run the **collect forward-path** command.
Direction	Direction where packets are collected.
Interval time	The collection duration.
Status	Collected packet status.
Start time	Start time when packets were collected.
End time	End time when packets were collected.
Port	Inbound and outbound interfaces of packets.
Eth-Trunk	Eth-Trunk that interfaces join.
Source MAC address	Source MAC address of collected packets.
Destination MAC address	Destination MAC address of collected packets.
L2 protocol type	Layer 2 protocol type of collected packets.

Item	Description
VLAN id	VLAN ID of collected packets.
Packets	Number of forwarded packets.
Bytes	Number of forwarded bytes.

5.2.13 display interface eth-trunk

Function

The **display interface eth-trunk** command displays status and traffic statistics about Eth-Trunk interfaces.

Format

display interface eth-trunk [*trunk-id* | **main**]

display interface eth-trunk *trunk-id.subnumber*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support *trunk-id.subnumber* parameter.

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: - SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 - S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 - S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
main	Displays the status and traffic statistics of an Eth-Trunk main interface.	-
trunk-id.subnumber	Specifies the number of an Eth-Trunk sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display interface eth-trunk** command to view the status and weight of each Eth-Trunk member interface.

To monitor the status of an interface or locate an interface fault, you can use the **display interface eth-trunk** command to collect the status of and traffic statistics on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

Display status and traffic statistics about Eth-Trunk 10.

```
<HUAWEI> display interface Eth-Trunk 10
Eth-Trunk10 current state : UP
Line protocol current state : DOWN
Description:
Switch Port, Link-type : trunk(negotiated),
PVID :    1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW:
 2G, Current BW: 1000M, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fcd4-36f1
Current system time: 2013-01-14 19:38:12
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
  Unicast:                          0,  Multicast:                          0
  Broadcast:                        0,  Jumbo:                              0
  Discard:                          0,  Pause:                              0
  Frames:                           0

  Total Error:                      0
  CRC:                              0,  Giants:                             0
  Jabbers:                          0,  Fragments:                          0
  Runts:                            0,  DropEvents:                         0
  Alignments:                       0,  Symbols:                            0
  Ignoreds:                         0

Output:  0 packets, 0 bytes
  Unicast:                          0,  Multicast:                          0
  Broadcast:                        0,  Jumbo:                              0
  Discard:                          0,  Pause:                              0

  Total Error:                      0
  Collisions:                       0,  ExcessiveCollisions:                0
  Late Collisions:                  0,  Deferreds:                          0
  Buffers Purged:                   0

    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
-----------------------------------------------------
PortName                      Status      Weight
-----------------------------------------------------
GigabitEthernet0/0/1          DOWN        1
GigabitEthernet0/0/2          UP          1
-----------------------------------------------------
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 1
```

Table 5-25 Description of the **display interface eth-trunk** command output

Item	Description
Eth-Trunk10 current state	Eth-Trunk status: - UP: The interface is Up. - DOWN: The interface becomes faulty. - UP(E-TRUNK-DOWN): The Eth-Trunk goes Down because of E-Trunk negotiation.

Item	Description
Line protocol current state	Link layer protocol status of the Eth-Trunk: - DOWN: The link layer protocol of the interface fails or no IP address is assigned to the interface. - UP: The link layer protocol of the interface is running properly.
Description	Description of the Eth-Trunk. To specify the parameter, run the **description** command.
Switch Port	The Eth-Trunk is a Layer 2 interface. Route Port is displayed if the Eth-Trunk is a Layer 3 interface.
Link-type	Link type of the Layer 2 interface. The parameter is displayed only in Layer 2 mode. The options are as follows: - access (configured): The interface is manually configured as an access interface. - hybrid: The interface is manually configured as a hybrid interface. - trunk (configured): The interface is manually configured as a trunk interface. - dot1q-tunnel: The interface is manually configured as a Dot1q-tunnel interface. - access(negotiated): The interface is used as an access interface through negotiation. - trunk(negotiated): The interface is used as a trunk interface through negotiation. To configure the link type of an interface, run the **port link-type** command.
PVID	Default VLAN ID of the Eth-Trunk.
Hash arithmetic	Hash algorithm used for load balancing among Eth-Trunk member interfaces. The hash algorithm depends on the load balancing mode configured by using the **load-balance** command. The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.
Maximal BW	Maximum bandwidth.
Current BW	Current bandwidth.

Item	Description
The Maximum Frame Length	Maximum frame length allowed by the Eth-Trunk. To specify the parameter, run the **jumboframe enable** command.
IP Sending Frames' Format	Format of frames sent through the IP protocol, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	Device MAC address.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in the format of YYYY/MM/DD HH:MM:SS±HH:MM.
Last 300 seconds input rate	Received packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Sent packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by an Eth-Trunk.
Multicast	Number of multicast packets received or sent by an Eth-Trunk.
Broadcast	Number of broadcast packets received or sent by an Eth-Trunk.
Jumbo	Number of jumbo frames received or sent by the Eth-Trunk.
Discard	Number of packets discarded by the Eth-Trunk during physical layer detection.
Pause	Pause frame.
Total Error	Number of error packets discovered by the Eth-Trunk during physical layer detection.
CRC	Number of CRC error packets received by the Eth-Trunk.
Giants	Number of jumbo frames with the correct FCS received by the Eth-Trunk.
Jabbers	Number of jumbo frames with incorrect FCS received by the Eth-Trunk.
Fragments	Number of fragments received by the Eth-Trunk.

Item	Description
Runts	Number of undersized frames with the correct FCS received by the Eth-Trunk.
DropEvents	Number of received packets that are discarded due to GBP full or back pressure.
Alignments	Number of received frames with alignment errors.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames in which the OpCode is not PAUSE.
Frames	Number of packets with the incorrect 802.3 length.
Collisions	Number of sent packets. During packet transmission, 1 to 15 conflict events were generated.
ExcessiveCollisions	Number of packets that fail to be sent. During packet transmission, 16 conflict events were generated.
Late Collisions	Number of delayed packets sent by the Eth-Trunk. During packet transmission, conflict events were generated.
Deferreds	Number of delayed packets sent by the Eth-Trunk. During packet transmission, no conflict event was generated.
Buffers Purged	Number of packets aged in the cache because packets sent by the Eth-Trunk have been stored in the queue buffer for a long time.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.
PortName	Name of the Eth-Trunk member interface.
Status	Status of the Eth-Trunk member interface. Manual mode: ● Up: indicates that the interface is properly started. ● Down: indicates that the interface becomes faulty. LACP mode: ● Up: indicates that the interface is selected. ● Down: indicates that the interface is not selected.
Weight	Weight of a member interface for load balancing.
The Number of Ports in Trunk	Number of Eth-Trunk member interfaces.

Item	Description
The Number of UP Ports in Trunk	Number of Eth-Trunk member interfaces in Up state.

5.2.14 display lacp brief

Function

The **display lacp brief** command displays brief LACP information, including the LACP system priority and system ID.

Format

display lacp brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Devices at both ends of an Eth-Trunk compare LACP system priorities and system IDs to determine the Actor during LACP negotiation.

- By default, the LACP system priority is 32768, and the device with the smaller LACP system ID is used as the Actor.
- If LACP system priorities are changed using the **lacp priority** command, the device with the smaller LACP system priority is used as the Actor.

The **display eth-trunk** command can be used to check the LACP system priority and system ID only after an Eth-Trunk in LACP mode has been configured. This is inconvenient for network planning. To facilitate network planning, you can run the **display lacp brief** command to check the LACP system priority and system ID when no Eth-Trunk in LACP mode is configured.

Precautions

When two PEs join an E-Trunk, run the **lacp e-trunk system-id** command on the PEs to configure the same E-Trunk LACP system ID so that the CE considers the PEs to be one device. The E-Trunk LACP system ID configurations do not affect

LACP system IDs of Eth-Trunks in LACP mode. The LACP system ID of an Eth-Trunk in LACP mode is the MAC address of the Ethernet interface on the device.

E-Trunk is supported by only the following models: S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Example

Display brief LACP information.

```
<HUAWEI> display lacp brief
System Priority:32768
System ID      :00e0-5958-ef00
```

Table 5-26 Description of the **display lacp brief** command output

Item	Description
System Priority	LACP system priority. To configure the LACP system priority, run the **lacp priority** command.
System ID	System ID, which is the bridge MAC address of the device.

5.2.15 display lacp statistics eth-trunk

Function

The **display lacp statistics eth-trunk** command displays statistics on received and sent Link Aggregation Control Protocol Data Units (LACPDUs) about an Eth-Trunk in LACP mode.

Format

display lacp statistics eth-trunk [*trunk-id* [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be used only when the Eth-Trunk works in LACP mode. To change the working mode of an Eth-Trunk to the LACP mode, run the **mode lacp** command in the Eth-Trunk interface view.

To view the statistics on a specific Eth-Trunk, ensure that the Eth-Trunk has been created. To view the statistics on a specified Eth-Trunk member interface, ensure that the interface is added to the Eth-Trunk.

Example

Display the statistics on LACPDUs sent and received by member interface GigabitEthernet0/0/1 of Eth-Trunk 4.

```
<HUAWEI> display lacp statistics eth-trunk 4
 Eth-Trunk4's PDU statistic is:
 -------------------------------------------------------------------------------
 Port                  LacpRevPdu   LacpSentPdu  MarkerRevPdu  MarkerSentPdu
 GigabitEthernet0/0/2    20683        830          0            0
 GigabitEthernet0/0/3    16356        677          0            0
 GigabitEthernet0/0/1    7213         7213         0            0
```

Display the statistics on LACPDUs sent and received by member interface GigabitEthernet0/0/1 of Eth-Trunk 4.

```
<HUAWEI> display lacp statistics eth-trunk 4 interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1's PDU statistic is:
 -------------------------------------------------------------------------------
 Port                  LacpRevPdu   LacpSentPdu  MarkerRevPdu MarkerSentPdu
 GigabitEthernet0/0/1    7673         7673         0            0
```

Table 5-27 Description of the **display lacp statistics eth-trunk** command output

Item	Description
Port	Current member interface of the Eth-Trunk.
LacpRevPdu	Number of received LACPDUs.
LacpSentPdu	Number of sent LACPDUs.
MarkerRevPdu	Number of received MARKER packets.
MarkerSentPdu	Number of sent MARKER packets.

5.2.16 display load-balance-profile

Function

The **display load-balance-profile** command displays detailed information about a specified load balancing profile.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display load-balance-profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a load balancing profile.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays detailed information about a specified load balancing profile, including the load balancing mode of IPv4, IPv6, Layer 2, and MPLS packets.

Example

Display detailed information about a specified load balancing profile.

```
<HUAWEI> display load-balance-profile abc
Load-balance-profile : abc
Packet    HashField
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
IPV4      sip         dip
IPV6      sip         dip
L2        smac        l2-protocol vlan        sport
MPLS      top-label   2nd-label

Trunk interface
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Eth-Trunk100
```

Table 5-28 Description of the display load-balance-profile command output

Item	Description
Load-balance-profile	Load balancing profile. To specify the parameter, run the **load-balance-profile** command.
Packet	Packet type.
HashField	Load balancing mode in the load balancing profile. You can run the **ipv4 field**, **ipv6 field**, **l2 field**, and **mpls field** commands to configure the load balancing mode for IPv4, IPv6, Layer 2, and MPLS packets respectively.
Trunk interface	Eth-Trunk that uses the load balancing profile, configured by the **load-balance** command.

5.2.17 display load-distribution active-linknumber-change

Function

The **display load-distribution active-linknumber-change** command displays the configuration when the number of interfaces in an Eth-Trunk where load balancing calculation is performed is configured.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

display load-distribution active-linknumber-change [**interface Eth-Trunk** *trunk-id*]

Parameters

Parameter	Description	Value
interface Eth-Trunk *trunk-id*	Specifies the ID of an Eth-Trunk.	The ID of an Eth-Trunk must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **load-distribution active-linknumber-change** command is used to configure the number of interfaces in an Eth-Trunk where load balancing calculation is performed, you can run the **display load-distribution active-linknumber-change** command to check the configuration.

Example

Display the configuration when the number of interfaces in an Eth-Trunk where load balancing calculation is performed is configured.

```
<HUAWEI> display load-distribution active-linknumber-change interface Eth-Trunk 3
--------------------------------------------------------------------------------
Interface    Pre-linknumber    Post-linknumber
--------------------------------------------------------------------------------
Eth-Trunk3       2                   4
--------------------------------------------------------------------------------
```

Table 5-29 Description of the **display load-distribution active-linknumber-change** command output

Item	Description
Interface	Name of the Eth-Trunk.
Pre-linknumber	Number of active interfaces in an Eth-Trunk when the number of interfaces in an Eth-Trunk where load balancing calculation is performed is configured. To configure the number of active interfaces in an Eth-Trunk when the number of interfaces in an Eth-Trunk where load balancing calculation is performed, run the **load-distribution active-linknumber-change** or **load-distribution active-linknumber-change global** command.
Post-linknumber	Number of interfaces in an Eth-Trunk where load balancing calculation is performed when the Eth-Trunk has active interfaces. To configure the number of interfaces in an Eth-Trunk where load balancing calculation is performed when the Eth-Trunk has active interfaces, run the **load-distribution active-linknumber-change** or **load-distribution active-linknumber-change global** command.

5.2.18 display trunk index-map

Function

The **display trunk index-map** command displays the mapping between Eth-Trunk IDs and internal indexes.

Format

display trunk index-map

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ID is manually allocated to an Eth-Trunk during Eth-Trunk creation. For example, the ID of Eth-Trunk 1 is 1. In addition, the device also allocates an internal number, also called the index, to each Eth-Trunk. When allocating indexes, the device traverses indexes in ascending order. The unallocated index is used as the index of an Eth-Trunk; therefore, the mapping between Eth-Trunk IDs and indexes is unordered. You can use **display trunk index-map** to check the mapping between Eth-Trunk IDs and indexes.

Example

Display the mapping between Eth-Trunk IDs and internal indexes.

```
<HUAWEI> display trunk index-map
Index   Interface Name

-----------------------------
1       Eth-Trunk10
2       Eth-Trunk20
3       Eth-Trunk5
```

Table 5-30 Description of the **display trunk index-map** command output

Item	Description
Index	Index of the Eth-Trunk.
Interface Name	Name of the Eth-Trunk.

5.2.19 display trunk resource

Function

The **display trunk resource** command displays trunk resources that have been used on a device.

Format

display trunk resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the number of trunk interfaces configured on a device and the number of member interfaces added to the trunk interfaces, run the **display trunk resource** command. The command output helps you learn about used trunk resources.

Example

Display trunk resources used on a device.

```
<HUAWEI> display trunk resource
Number of configured trunk interfaces is : 4
Interface           Member Count
-----------------------------------------------------------
Eth-Trunk1          2
Eth-Trunk10         0
Eth-Trunk30         0
Eth-Trunk55         0
```

Table 5-31 Description of the **display trunk resource** command output

Item	Description
Number of configured trunk interfaces is	Number of configured trunk interfaces.
Interface	Trunk interface type: - Eth-Trunk
Member Count	Number of member interfaces added to a trunk interface.

5.2.20 display trunkfwdtbl eth-trunk

Function

The **display trunkfwdtbl eth-trunk** command displays the forwarding table of an Eth-Trunk.

Format

display trunkfwdtbl eth-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By default, an Eth-Trunk supports a maximum of eight physical member interfaces, which correspond to eight entries in the forwarding table. The eight entries correspond to HASH-KEY values 0 to 7. The system searches for outbound interfaces among active links based on HASH-KEY values.

NOTE

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Example

Display the forwarding table of Eth-Trunk 1. Eth-Trunk 1 has three active links.

```
<HUAWEI> display trunkfwdtbl eth-trunk 1
 Eth-Trunk1's forwarding table is:
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/1
GigabitEthernet0/0/2
GigabitEthernet0/0/3
GigabitEthernet0/0/1
GigabitEthernet0/0/2
```

Table 5-32 Description of the **display trunkfwdtbl eth-trunk** command output

Item	Description
Eth-Trunk1's forwarding table	Forwarding entry of an Eth-Trunk.

5.2.21 display trunkmembership eth-trunk

Function

The **display trunkmembership eth-trunk** command displays information about Eth-Trunk member interfaces.

Format

display trunkmembership eth-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an Eth-Trunk is successfully configured, you can run the **display trunkmembership eth-trunk** command to view the configuration of the Eth-Trunk and its member interfaces.

To monitor the status of an interface or locate an interface fault, you can use the **display trunkmembership eth-trunk** command to view detailed information about an Eth-Trunk and its member interfaces. The command output helps you can troubleshoot faults and check the member interface configuration.

Prerequisites

An Eth-Trunk has been correctly configured. If the Eth-Trunk is not created, the system displays an error when you run the **display trunkmembership eth-trunk** command.

Precautions

Before running the **display trunkmembership eth-trunk** command to view the configuration of the Eth-Trunk in LACP mode, ensure that the Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command.

Example

Display information about member interfaces of Eth-Trunk 2.

```
<HUAWEI> display trunkmembership eth-trunk 2
Trunk ID: 2
Used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of Up Ports in Trunk = 2
Operate status: up
Interface GigabitEthernet0/0/1, valid, operate up, weight=1
Interface GigabitEthernet0/0/2, valid, operate up, weight=1
```

Table 5-33 Description of the display trunkmembership eth-trunk command output

Item	Description
Trunk ID	ID of the Eth-Trunk.
Used status	Whether the Eth-Trunk is available: ● VALID: The Eth-Trunk is available. ● INVALID: The Eth-Trunk is unavailable.
TYPE	Type of an Eth-Trunk. To specify the parameter, run the **port link-type** command.
Working Mode	Working mode of an Eth-Trunk. ● Normal: manual load balancing mode ● LACP: LACP mode To specify the parameter, run the **mode** command.
Number Of Ports in Trunk	Number of interfaces that are added to the Eth-Trunk.
Number Of Up Ports in Trunk	Number of Up interfaces that are added to the Eth-Trunk.
Operate status	Eth-Trunk status: ● up ● down

Item	Description
Interface, valid, operate, weight	Detailed information about a member interface: - Interface: indicates the interface type and number. - valid: indicates that the interface is available. - operate: indicates the status of the interface. - weight: indicates the weight of the interface for load balancing.

5.2.22 eth-trunk

Function

The **eth-trunk** command adds an interface to an Eth-Trunk.

The **undo eth-trunk** command removes an interface from an Eth-Trunk.

By default, an interface does not belong to any Eth-Trunk.

Format

eth-trunk *trunk-id* [**mode** { **active** | **passive** }]

undo eth-trunk

Parameters

Parameter	Description	Value
trunk-id	Indicates the ID of an Eth-Trunk.	The value is an integer that ranges from 0 to 249. The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Parameter	Description	Value
mode { **active** | **passive** }	Indicates the mode in which an Eth-Trunk member interface sends packets. This parameter is valid for only the Eth-Trunk in LACP mode. By default, the mode an Eth-Trunk member interface sends packets is **active**. ● **active**: indicates that an Eth-Trunk member interface proactively sends negotiation packets. ● **passive**: indicates that an Eth-Trunk member interface sends packets to negotiate with its remote end only after receiving a packet from its remote end.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the connection reliability and increase the bandwidth, you can use the **eth-trunk** command to bind multiple interfaces into an Eth-Trunk.

You can add an interface to an Eth-Trunk only after you run the **interface Eth-Trunk** command to create the Eth-Trunk.

An Eth-Trunk contains a maximum of 32 member interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 member interfaces on the S5735S-H, S5736-S, and S6720S-S, and 8 member interfaces on all other models. Interfaces added to an Eth-Trunk are called member interfaces. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

When you add an Ethernet interface to an Eth-Trunk, the interface must use default settings of some attributes. Otherwise, the interface cannot be added to the Eth-Trunk. The attributes include:

- Link type
- VLAN that the interface belongs to
- VLAN mapping
- VLAN stacking
- QinQ protocol number
- Interface priority
- Whether the interface allows BPDUs to pass through
- MAC address learning
- Adding the interface to a multicast group statically
- Discarding broadcast packets
- Discarding unknown multicast packets
- Discarding unknown unicast packets
- Controllable multicast profile bound to the interface

The attributes on all member interfaces of an Eth-Trunk must be consistent and cannot be changed separately. If the preceding attributes of an Eth-Trunk are changed, the attributes of all the member interfaces are changed accordingly.

It is recommended that you run the **shutdown (interface view)** command to disable an interface before adding the interface to an Eth-Trunk. After adding interfaces at both ends of a link to an Eth-Trunk, run the **undo shutdown (interface view)** command to enable the interfaces. Otherwise, traffic interruption or broadcast storms may occur.

It is recommended that you run the **shutdown (interface view)** command to disable a member interface before running the **undo eth-trunk** command to remove the member interface from an Eth-Trunk.

The number of member interfaces of the Eth-Trunk on devices at both ends must be the same. The interfaces at both ends must be connected with straight-through cables.

Example

Add GigabitEthernet0/0/1 to Eth-Trunk 2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 2
```

5.2.23 e-trunk (Eth-Trunk interface view)

Function

The **e-trunk** command adds an Eth-Trunk in LACP mode to a specified E-Trunk.

The **undo e-trunk** command deletes an Eth-Trunk from a specified E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk *e-trunk-id* [**remote-eth-trunk** *eth-trunk-id*]

undo e-trunk

Parameters

Parameter	Description	Value
e-trunk-id	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.
remote-eth-trunk *eth-trunk-id*	Specifies the Eth-Trunk ID of the remote PE. If the ID of the Eth-Trunk created on a PE is different from the ID of the Eth-Trunk created on the other PE, you must configure **remote-eth-trunk** when adding different Eth-Trunks in LACP mode to an E-Trunk so that the E-Trunk can work properly.	The value is an integer that ranges from 0 to 4294967295.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Only Eth-Trunks in LACP mode can be added to an E-Trunk, and an Eth-Trunk can be added to only one E-Trunk. If an Eth-Trunk is already added to an E-Trunk, you must delete it from the E-Trunk before adding it to another E-Trunk.

NOTE

At most 64 Eth-Trunks in LACP mode can be added to an E-Trunk.

Precautions

- Only Eth-Trunk interfaces in LACP mode can be added to an E-Trunk.
- After an Eth-Trunk interface is added to an E-Trunk, to add the Eth-Trunk interface to another E-Trunk or modify the remote Eth-Trunk ID, first run the **undo e-trunk** command to delete the Eth-Trunk interface from the current E-Trunk and then run the **e-trunk** command.
- If the master Eth-Trunk interface in an E-Trunk encounters a link failure, the backup Eth-Trunk interface goes Down after the master Eth-Trunk interface is removed from the E-Trunk.

Example

Add Eth-Trunk 1 to E-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] e-trunk 1
```

5.2.24 e-trunk mode

Function

The **e-trunk mode** command configures a working mode of an Eth-Trunk in an E-Trunk.

The **undo e-trunk mode** command restores the default working mode of an Eth-Trunk in an E-Trunk.

By default, an Eth-Trunk works in automatic mode in an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk mode { **auto** | **force-master** | **force-backup** }

undo e-trunk mode

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode.	-
force-master	Indicates the forcible master mode.	-
force-backup	Indicates the forcible backup mode.	-

Views

Eth-Trunk interface view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

The **e-trunk mode** command is valid only for the Eth-Trunks added to an E-Trunk. When the Eth-Trunk is deleted from the E-Trunk, the configuration is cancelled.

When the E-Trunk works properly, changing the interval for sending packets or timeout of hello packets will cause the E-Trunk to alternate between the master state and the backup state. You are advised to set the working mode of a member Eth-Trunk to forcible master/backup before changing the interval for sending packets or the timeout of hello packets. After the new configuration takes effect, restore the working mode to automatic.

Example

Set the working mode of Eth-Trunk 1 in an E-Trunk to forcible master.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] e-trunk mode force-master
```

5.2.25 e-trunk port

Function

The **e-trunk port** command configures the UDP port number used to send and receive E-Trunk packets.

The **undo e-trunk port** command restores the default value.

By default, UDP port 1025 is used to send and receive E-Trunk packets.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk port *port-number*

undo e-trunk port

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number used to send and receive E-Trunk packets. If the UDP port number in the range of 1025 to 65535 is used by another protocol, the port number cannot be used to send or receive E-Trunk packets. **NOTE** UDP port numbers 49152 to 65535 are allocated randomly by the socket. Do not configure the UDP port number in this range; otherwise, the E-Trunk cannot work properly.	The value is an integer that ranges from 1025 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

E-Trunk is a Huawei proprietary protocol. UDP port 1025 used to send and receive E-Trunk packets may conflict with the UDP port used by another protocol. To ensure that E-Trunk packets are forwarded correctly, run the **e-trunk port** command to change the UDP port number used to send and receive E-Trunk packets.

Precautions

The port numbers at both ends of an E-Trunk must be consistent. When the E-Trunk works properly, you must change the UDP port number within the timeout of E-Trunk negotiation.

If you change the UDP port number during E-Trunk running, devices at both ends of an E-Trunk may be unable to communicate. If E-Trunk negotiation times out, both devices in the E-Trunk may become master devices.

Example

Configure the UDP port number used to send and receive E-Trunk packets.

```
<HUAWEI> system-view
[HUAWEI] e-trunk port 1026
```

5.2.26 e-trunk (system view)

Function

The **e-trunk** command creates an E-Trunk.

The **undo e-trunk** command deletes an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk *e-trunk-id*

undo e-trunk *e-trunk-id*

Parameters

Parameter	Description	Value
e-trunk-id	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the specified E-Trunk already exists, this command directly displays the view of the specified E-Trunk.

At most 16 E-Trunks can be created on a device.

After an E-Trunk is created, it does not send protocol packets until the remote IP address is configured.

Example

Create an E-Trunk with the ID of 1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1]
```

5.2.27 e-trunk track bfd-session

Function

The **e-trunk track bfd-session** command binds a BFD session to an E-Trunk.

The **undo e-trunk track bfd-session** command unbinds a BFD session from an E-Trunk.

By default, no BFD session is bound to an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

e-trunk track bfd-session session-name *bfd-session-name*

undo e-trunk track bfd-session

Parameters

Parameter	Description	Value
session-name *bfd-session-name*	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. When the string is enclosed with double quotation marks (""), spaces are allowed in the string.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PE1 and PE2 are connected through an E-Trunk. PE1 is in master state and PE2 is in slave state. When PE1 fails and PE2 does not receive any E-Trunk protocol packets from PE1 after the timer expires, PE2 switches from the slave state to the master state.

The status of PE2 changes after the timer expires. During the timeout, user traffic is interrupted. To enable PE2 to rapidly detect the fault and switch its status, run this command to bind a BFD session to an E-Trunk.

After the BFD session is bound to the E-Trunk, the BFD session can rapidly detect the link between PE1 and PE2. If the link fails, the BFD session becomes Down. PE2 then can detect the BFD session status and switch its status to master so that traffic is correctly forwarded.

NOTE

In this scenario, the Eth-Trunk on PE1 and PE2 supports only one member interface.

Prerequisites

Before using this command, pay attention to the following points:

- An E-Trunk and a BFD session must have been configured. BFD for IP must be used; otherwise, the E-Trunk cannot rapidly detect the fault through the BFD session.
- The IP addresses of both ends of the E-Trunk must be reachable; otherwise, the BFD session cannot go Up. That is, the BFD session cannot detect the link between PE1 and PE2.

Precautions

After a BFD session is bound to an E-Trunk and AC interfaces on both devices of the E-Trunk are associated with the BFD session, if the AC interface of the master device fails, the BFD session goes Down and traffic is switched to the standby link. If the AC interface recovers within 60 seconds, traffic is immediately switched back to the active link.

Example

Bind a BFD session named **hello** to E-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] e-trunk track bfd-session session-name hello
```

5.2.28 interface eth-trunk

Function

The **interface eth-trunk** command displays the view of an existing Eth-Trunk or creates an Eth-Trunk and displays its view.

The **undo interface eth-trunk** command deletes an Eth-Trunk.

By default, no Eth-Trunk is created.

Format

interface eth-trunk *trunk-id*[.*subnumber*]

undo interface eth-trunk *trunk-id*[.*subnumber*]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
subnumber	Specifies the ID of an Eth-Trunk sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the specified Eth-Trunk already exists, the **interface eth-trunk** command directly displays the view of the specified Eth-Trunk.

You can delete an Eth-Trunk only when the Eth-Trunk does not contain any member interface.

NOTE

- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Layer 2 Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Layer 3 Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

Create Eth-Trunk 2.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 2
[HUAWEI-Eth-Trunk2]
```

5.2.29 ipv4 field

Function

The **ipv4 field** command configures a load balancing mode of IPv4 packets in a load balancing profile.

The **undo ipv4 field** command deletes a load balancing mode of IPv4 packets or restores the default load balancing mode of IPv4 packets.

By default, load balancing of IPv4 packets is based on the source IP address (**sip**) and destination IP address (**dip**).

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv4 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

undo ipv4 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

NOTE

Only **dip**, **sip**, and **sport** are supported on the S5736-S.

Parameters

Parameter	Description	Value
dip	Performs load balancing based on destination IP addresses in IPv4 packets.	-
l4-dport	Performs load balancing based on transport-layer destination port numbers in IPv4 packets.	-
l4-sport	Performs load balancing based on transport-layer source port numbers in IPv4 packets.	-
protocol	Performs load balancing based on protocol types in IPv4 packets.	-
sip	Performs load balancing based on source IP addresses in IPv4 packets.	-
sport	Performs load balancing based on physical-layer source port numbers in IPv4 packets.	-
vlan	Performs load balancing based on VLAN IDs in IPv4 packets.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo ipv4 field** command with no parameter specified restores the default load balancing mode of IPv4 packets. The **undo ipv4 field** command with a parameter specified deletes a specified load balancing mode of IPv4 packets.

Precautions

If you run the **ipv4 field** command multiple times, only the latest configuration takes effect.

On S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S switches, if **l4-dport** or **l4-sport** is specified for L2TP packets, load balancing is performed based on **session id** and **tunnel id** in L2TP packets rather than **l4-dport** and **l4-sport**.

On S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S switches, if **l4-dport** or **l4-sport** is specified for GTP packets, both outer and inner IP information are parsed when load balancing is performed for GTP packets; if another parameter is specified, only the outer IP information is parsed when load balancing is performed for GTP packets. For other switches, only the outer IP information of GTP packets is parsed when load balancing is performed.

Example

In the load balancing profile **a**, set the load balancing mode of IPv4 packets to **sip** and **protocol**, that is, load balancing based on source IP addresses and protocol types of IPv4 packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] ipv4 field sip protocol
```

5.2.30 ipv6 field

Function

The **ipv6 field** command configures a load balancing mode of IPv6 packets in a load balancing profile.

The **undo ipv6 field** command deletes the load balancing mode of IPv6 packets or restores the default load balancing mode of IPv6 packets.

By default, load balancing of IPv6 packets is based on the source IP address (**sip**) and destination IP address (**dip**).

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv6 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

undo ipv6 field [**dip** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **sport** | **vlan**] *

NOTE

Only **dip**, **l4-dport**, **l4-sport**, **sip**, and **sport** are supported on the S5735S-H, S5736-S, andS6720S-S.

Parameters

Parameter	Description	Value
dip	Performs load balancing based on destination IP addresses in IPv6 packets.	-
l4-dport	Performs load balancing based on transport-layer destination port numbers in IPv6 packets.	-
l4-sport	Performs load balancing based on transport-layer source port numbers in IPv6 packets.	-
protocol	Performs load balancing based on protocol types in IPv6 packets.	-
sip	Performs load balancing based on source IP addresses in IPv6 packets.	-
sport	Performs load balancing based on physical-layer source port numbers in IPv6 packets.	-
vlan	Performs load balancing based on VLAN IDs in IPv6 packets.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo ipv6 field** command with no parameter specified restores the default load balancing mode of IPv6 packets. The **undo ipv6 field** command with a parameter specified deletes a specified load balancing mode of IPv6 packets.

Precautions

If you run the **ipv6 field** command multiple times, only the latest configuration takes effect.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S switches, if **l4-dport** or **l4-sport** is specified for L2TP packets, load balancing is performed based on **session id** and **tunnel id** in L2TP packets rather than **l4-dport** and **l4-sport**.

Example

In the load balancing profile **a**, set the load balancing mode of IPv6 packets to **sip** and **protocol**, that is, load balancing based on source IP addresses and protocol types of IPv6 packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] ipv6 field sip protocol
```

5.2.31 l2 field

Function

The **l2 field** command configures a load balancing mode of Layer 2 packets in a load balancing profile.

The **undo l2 field** command deletes the load balancing mode of Layer 2 packets or restores the default load balancing mode of Layer 2 packets.

By default, load balancing of Layer 2 packets is based on the source MAC address (**smac**) and destination MAC address (**dmac**).

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

l2 field [**dmac** | **l2-protocol** | **smac** | **sport** | **vlan**] *

undo l2 field [**dmac** | **l2-protocol** | **smac** | **sport** | **vlan**] *

NOTE

Only **dmac**, **smac**, and **sport** are supported on the S5735S-H, S5736-S, and S6720S-S.

Parameters

Parameter	Description	Value
dmac	Performs load balancing based on destination MAC addresses in Layer 2 packets.	-

Parameter	Description	Value
l2-protocol	Performs load balancing based on protocol types in Layer 2 packets.	-
smac	Performs load balancing based on source MAC addresses in Layer 2 packets.	-
sport	Performs load balancing based on physical-layer source port numbers in Layer 2 packets.	-
vlan	Performs load balancing based on VLAN IDs in Layer 2 packets.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo l2 field** command with no parameter specified restores the default load balancing mode of Layer 2 packets. The **undo l2 field** command with a parameter specified deletes a specified load balancing mode of Layer 2 packets.

Precautions

If you run the **l2 field** command multiple times, only the latest configuration takes effect.

Example

In the load balancing profile **a**, set the load balancing mode of Layer 2 packets to **l2-protocol**, that is, load balancing based on protocol types of Layer 2 packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] l2 field l2-protocol
```

5.2.32 lacp collector delay

Function

The **lacp collector delay** command configures the value of the **CollectorMaxDelay** field in an LACPDU.

The **undo lacp collector delay** command restores the default value of the **CollectorMaxDelay** field in an LACPDU.

The default value of the **CollectorMaxDelay** field is 0 in an LACPDU.

Format

lacp collector delay *delay-time*

undo lacp collector delay

Parameters

Parameter	Description	Value
delay-time	Specifies the value of the **CollectorMaxDelay** field in an LACPDU.	The value is an integer that ranges from 0 to 65535, in 10 microseconds.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default value of the **CollectorMaxDelay** field in LACPDUs sent by the device of different versions to the connected non-Huawei device is different. This may cause high CPU usage. You can run the **lacp collector delay** command to set the value of the **CollectorMaxDelay** field in LACPDUs.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command.

Precautions

For a Huawei device, the valid value range of the **CollectorMaxDelay** field is 0 to 65535. Even though the member interfaces of the same Eth-Trunk receive LACPDUs with different **CollectorMaxDelay** values, the device can process the LACPDUs without deteriorating its CPU performance.

Example

Set the value of the **CollectorMaxDelay** field to 65535.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp collector delay 65535
```

5.2.33 lacp e-trunk priority

Function

The **lacp e-trunk priority** command sets the LACP priority of an E-Trunk.

The **undo lacp e-trunk priority** command cancels the configuration.

By default, the LACP priority of an E-Trunk is 32768.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp e-trunk priority *priority*

undo lacp e-trunk priority

Parameters

Parameter	Description	Value
priority	Specifies the LACP priority of an E-Trunk.	The value is an integer that ranges from 0 to 65535. A smaller value indicates a higher LACP priority.

Views

System view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The **lacp e-trunk priority** command sets the LACP priority of an E-Trunk. If the LACP priority is set, a member Eth-Trunk sends LACPDUs by using this LACP priority. If the LACP priority is not set, the default LACP priority 32768 is used.

The master and backup devices in an E-Trunk must use the same LACP priority.

When multiple E-Trunks are configured on the device, different LAGs can use different LACP priorities. You need to set the LACP priorities in the Eth-Trunk interface view.

The LACP priority configured in the system view is valid for all Eth-Trunks added to the E-Trunk. The LACP priority configured in the Eth-Trunk view takes effect only on the corresponding Eth-Trunk. If the LACP priorities are configured in both the Eth-Trunk interface view and system view, the LACP priority configured in the interface view takes effect.

NOTE

Ensure that the Eth-Trunk has been added to the E-Trunk before you run the **lacp e-trunk priority** command in the Eth-Trunk interface view.

Example

Set the LACP priority of the E-Trunk to 1.

```
<HUAWEI> system-view
[HUAWEI] lacp e-trunk priority 1
```

5.2.34 lacp e-trunk system-id

Function

The **lacp e-trunk system-id** command sets the LACP system ID of an E-Trunk.

The **undo lacp e-trunk system-id** command cancels the configuration.

By default, the LACP system ID in the system view is the MAC address of the Ethernet interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp e-trunk system-id *mac-address*

undo lacp e-trunk system-id

Parameters

Parameter	Description	Value
system-id *mac-address*	Specifies the LACP system ID of an E-Trunk.	The value is in the format of H-H-H. An H contains 1 to 4 hexadecimal numbers, such as 00e0 and fc01. If you enter fewer than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The LACP system ID cannot be all 0s or all Fs.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **lacp e-trunk system-id** command sets the LACP system ID of an E-Trunk. If the system ID is set, a member Eth-Trunk sends LACPDUs by using this system ID. If the LACP system ID is not set, the MAC address of the Ethernet interface is used as the system ID.

The master and backup devices in an E-Trunk must use the same LACP system ID.

Example

Set the LACP system ID of the E-Trunk to 00E0-FC00-0000.

```
<HUAWEI> system-view
[HUAWEI] lacp e-trunk system-id 00E0-FC00-0000
```

5.2.35 lacp force-switch

Function

The **lacp force-switch** command enables forcible switching when no preemption is configured for an Eth-Trunk interface in LACP mode or preemption is enabled but the delay is not reached.

By default, the switch does not enable forcible switching.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp force-switch

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 5-1 Eth-Trunk interface in LACP mode

As shown in **Figure 5-1**, when no service is bound to the MA (Maintenance Association), an Eth-Trunk interface in LACP mode is configured on two devices. interface1 where the MEP (Maintenance End Point) resides is the interface of the Eth-Trunk interface's primary link. When the **delay-measure two-way trigger if-down** or **loss-measure single-ended-synthetic trigger if-down** command is configured on interface1, interface1 is triggered to go ETHOAM down if Y.1731 detects that the primary link has poor quality. To ensure that services are not interrupted, run the **lacp track interface** command in the Eth-Trunk member interface view to increase the priority of the secondary member interface interface2. The secondary link then preempts the primary state, implementing an automatic primary/secondary link switchover.

When the primary link's quality recovers, run the **lacp force-switch** command to enable forcible switching if no preemption is configured or preemption is enabled but the delay is not reached.

Prerequisites

The **lacp track interface** command has been run to associate the secondary member interface of an Eth-Trunk interface in LACP mode with its primary member interface and to dynamically change the priority of the secondary member interface.

Precautions

An Eth-Trunk interface can have only two member interfaces. The maximum number of active links must be 1.

Example

Enable forcible switching on Eth-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] lacp force-switch
```

5.2.36 lacp force-forward

Function

The **lacp force-forward** command configures an Eth-Trunk member interface in Up state to forward data packets when the remote interface does not join the Eth-Trunk.

The **undo lacp force-forward** command restores the default setting.

By default, an Eth-Trunk member interface in Up state cannot forward data packets when the remote interface does not join the Eth-Trunk.

Format

lacp force-forward

undo lacp force-forward

Parameters

None

Views

Eth-Trunk interface view

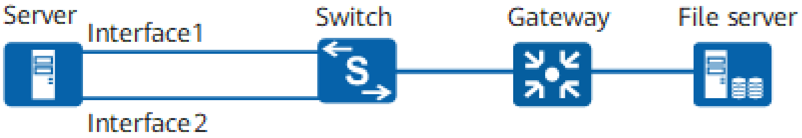
Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 5-2 A switch directly connects to a server



In Figure 5-2, two interfaces of two network adapters on a server are directly connected to a switch. The switch is configured with an Eth-Trunk in LACP mode. The process on the server is as follows:

1. The server configures an IP address for Interface1 based the default configuration during startup, and sends a request to the remote file server through Interface1 and downloads the configuration file from the remote file server.

2. After the configuration file is downloaded successfully, the server aggregates two interfaces according to the configuration file. The server uses the two interfaces as Eth-Trunk member interfaces to perform LACP negotiation with the switch.

Before the server obtains the configuration file, Interface1 is an independent physical interface and is not configured with LACP. As a result, LACP negotiation on the switch interface fails. The switch does not forward traffic on the Eth-Trunk, and the server cannot download the configuration file through Interface1. In this case, the server cannot communicate with the switch.

To address this issue, run the **lacp force-forward** command on the Eth-Trunk of the switch. The Eth-Trunk member interface in Up state can still forward data packets even though the remote device is not enabled with LACP.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode by using the **mode lacp** command.

Precautions

- With this command configured, an Eth-Trunk interface does not support Layer 3 forwarding and cannot be used to forward packets sent to the CPU. Only member interfaces in the ForceFwd state can forward Layer 2 traffic through hardware forwarding. The ForceFwd state is automatically set when LACP negotiation fails, and cannot be changed manually. You can use the **display eth-trunk** command to check the value of the Status field.
- This command applies to only the scenario where an Eth-Trunk joins a VLAN as an access, hybrid, trunk, and dot1q-tunnel interfaces.
- When a spanning tree protocol (for example, STP, RSTP, or MSTP) is used, the member interface in ForceFwd state cannot be blocked. That is, the member interface in ForceFwd state can continue to forward data packets. When other loop prevention protocols such as ERPS and RRPP are used, the member interface in ForceFwd state can be blocked. The blocked member interface in ForceFwd state cannot forward data packets.
- This command cannot be used with E-Trunk. That is, this command cannot be used on the Eth-Trunk that joins an E-Trunk.
- This command cannot be used with **max active-linknumber** or **least active-linknumber**.

Example

Configure an Eth-Trunk member interface in Up state to forward data packets when the remote interface does not join the Eth-Trunk.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp force-forward
```

5.2.37 lacp optimized-converge enable

Function

The **lacp optimized-converge enable** command enables optimized LACP convergence.

The **undo lacp optimized-converge enable** command disables optimized LACP convergence.

By default, optimized LACP convergence is disabled.

Format

lacp optimized-converge enable

undo lacp optimized-converge enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the working mode of an Eth-Trunk interface is set to LACP, Eth-Trunk member interfaces are configured to forward traffic after LACP negotiation and instruct services to reselect a route. Service traffic then can be properly forwarded. However, when multiple cards are restarted at the same time, Eth-Trunk member interfaces negotiate in preemption mode. As a result, Eth-Trunk member interfaces negotiate slowly, causing a large number of service packets to be lost.

After optimized LACP convergence is enabled using the **lacp optimized-converge enable** command, the device increases the LACP negotiation priority so that services can quickly detect Eth-Trunk member interface changes, accelerating Eth-Trunk traffic convergence.

Example

Enable optimized LACP convergence.

```
<HUAWEI> system-view
[HUAWEI] lacp optimized-converge enable
```

5.2.38 lacp preempt delay

Function

The **lacp preempt delay** command sets the LACP preemption delay.

The **undo lacp preempt delay** command restores the default LACP preemption delay.

By default, the LACP preemption delay is 30 seconds.

Format

lacp preempt delay *delay-time*

undo lacp preempt delay

Parameters

Parameter	Description	Value
delay-time	Specifies the LACP preemption delay.	The value is an integer that ranges from 0 to 180 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 10 to 180 on other models, in seconds.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

To use this command, ensure that the following conditions are met:

- The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.
- Priority preemption has been enabled on the Eth-Trunk using the **lacp preempt enable** command in the Eth-Trunk interface view.

Link A replaces link B and becomes active after the preemption delay n the following situation:

1. LACP priority preemption is enabled and the **lacp preempt delay** command is used.

2. The faulty link (link A) with higher priority than that of the current active link (link B) recovers.
3. The number of current active links reaches the upper threshold.

If both devices of an Eth-Trunk use different preemption delays, a longer preemption delay is used. If priority preemption is enabled but the preemption delay is not set, the interface with a higher priority preempts the interface with a lower priority according to the default preemption delay.

Example

Set the LACP preemption delay of Eth-Trunk 1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp preempt delay 20
```

5.2.39 lacp preempt enable

Function

The **lacp preempt enable** command enables priority preemption for an Eth-Trunk in LACP mode.

The **undo lacp preempt enable** command disables priority preemption for an Eth-Trunk in LACP mode.

By default, priority preemption is disabled.

Format

lacp preempt enable

undo lacp preempt enable

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In LACP mode, when one of the active links fails, the system selects the link with the highest priority from backup links to replace the faulty one. When the faulty link recovers, the priority of this link is higher than the priority of the link that replaces itself, and priority preemption is enabled, the link becomes active again.

If priority preemption is disabled, the system does not re-select any active interface. The recovered link functions as the backup one.

When priority preemption is enabled, the system selects an active interface based on the LACP interface priority on the Actor.

Prerequisites

The LACP mode must have been configured using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

To ensure that an Eth-Trunk works properly, enable or disable LACP preemption on both ends of the Eth-Trunk.

Example

Enable priority preemption on Eth-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp preempt enable
```

5.2.40 lacp priority

Function

The **lacp priority** command sets the LACP system or interface priority.

The **undo lacp priority** command restores the default LACP system or interface priority.

By default, the LACP system or interface priority is 32768.

Format

lacp priority *priority*

undo lacp priority

Parameters

Parameter	Description	Value
priority	Specifies the LACP priority. A smaller value indicates a higher LACP priority.	The value is an integer that ranges from 0 to 65535.

Views

System view, Ethernet interface view, GE interface view, 25GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LACP system priority is used to differentiate the local device and the remote device. The device of a higher LACP system priority is selected as the Actor of the link aggregate group (LAG), and active interfaces are selected according to interfaces of the Actor.

The LACP interface priority is used to differentiate interfaces on a device. The interface of a higher priority is selected as the active interface.

If devices at both ends of an Eth-Trunk are not configured with LACP system priorities, the devices use the default LACP system priority 32768 and the device with a smaller MAC address is selected as the Actor.

If priorities of different interfaces on a switch are not set, the default priority of interfaces is all 32768. Active interfaces are selected based on interface numbers and interfaces with smaller interface numbers are preferred.

Prerequisites

The interface has been added to the Eth-Trunk in LACP mode.

You can run the **mode lacp** command in the Eth-Trunk interface view to change the working mode of an Eth-Trunk to LACP.

Precautions

In LACP mode, active interfaces selected by devices at both ends of an Eth-Trunk link must be the same; otherwise, the link aggregation group cannot be set up.

If the **max active-linknumber** command is executed in LACP mode to set the upper threshold for the number of active interfaces, you need to determine the active interfaces when the number of interfaces manually added to an LAG exceeds the upper threshold. Setting the LACP interface priority ensures that interfaces with higher priorities become active ones in LACP mode.

If the **max active-linknumber** command is not used, the upper threshold for the number of active interfaces is 8. When the number of interfaces manually added to an LAG is smaller than 8, you do not need to select active interfaces because all interfaces are active.

If the **max active-linknumber** *link-number* command is run in the Eth-Trunk interface view, you need to run the **lacp preempt enable** command to enable LACP preemption on the current Eth-Trunk interface. Otherwise, interfaces with high LACP priorities may fail to be selected as active interfaces.

Example

Set the LACP system priority to 1.

```
<HUAWEI> system-view
[HUAWEI] lacp priority 1
```

Set the LACP priority of GigabitEthernet0/0/1 to 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] lacp priority 1
```

5.2.41 lacp priority-command-mode

Function

The **lacp priority-command-mode** command sets a Link Aggregation Control Protocol (LACP) system priority configuration mode.

The **undo lacp priority-command-mode** command restores the default LACP system priority configuration mode.

By default, the LACP system priority configuration mode is **default**.

Format

lacp priority-command-mode { **default** | **system-priority** }

undo lacp priority-command-mode

Parameters

Parameter	Description	Value
default	Sets the LACP system priority configuration mode to **default**. In **default** mode, the LACP system priority is configured using the **lacp priority** command in the system view.	-
system-priority	Sets the LACP system priority configuration mode to **system-priority**. In **system-priority** mode, the LACP system priority is configured using the **lacp system-priority** command in the system view.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A change in the LACP system priority will cause LACP renegotiation. During the renegotiation process, Eth-Trunk interfaces in LACP mode will go Down until the renegotiation succeeds, which may interrupt services. If the **lacp priority** command used to set the LACP interface priority is executed in the system view, the Eth-Trunk in LACP mode may alternate between Up and Down. To prevent this situation, run the **lacp priority-command-mode** command in the system view to set the configuration mode of the LACP system priority to **system-priority**. This mode can be used to differentiate the LACP system priority and LACP interface priority.

Precautions

When running the **lacp priority-command-mode** command, note the following points:

- If you specify **default** in the command, the LACP system priority and LACP interface priority configurations still use the same command (**lacp priority** *priority*).
- If you specify **system-priority** in the command, run the **lacp system-priority** *priority* command to configure the LACP system priority and run the **lacp priority** *priority* command to configure the LACP interface priority.

Example

Set the LACP system priority configuration mode to **system-priority**.

```
<HUAWEI> system-view
[HUAWEI] lacp priority-command-mode system-priority
```

5.2.42 lacp selected

Function

The **lacp selected** command configures a mode for selecting active interfaces of an Eth-Trunk in LACP mode.

The **undo lacp selected** command restores the default mode for selecting active interfaces of an Eth-Trunk in LACP mode.

By default, active interfaces are selected based on the LACP interface priority.

Format

lacp selected { **priority** | **speed** }

undo lacp selected

Parameters

Parameter	Description	Value
priority	Indicates that active interfaces are selected based on the LACP interface priority. The interfaces with high priorities are preferentially selected as active interfaces.	-
speed	Indicates that active interfaces are selected based on the interface rate. High-speed interfaces are preferentially selected as active interfaces.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in LACP, active interfaces are selected based on the LACP interface priority by default. If member interfaces of an Eth-Trunk in LACP mode work at different rates, low-speed interfaces may be selected as active interfaces. To enable the device to select high-speed interfaces as active interfaces, run the **lacp selected** command to set the mode of selecting active interfaces to **speed**.

To enable the device to select active interface based on the LACP interface priority, run the **lacp selected priority** command to set the mode of selecting active interfaces to **priority**.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

Active interfaces are selected based on the LACP interface priority by default. Changing the mode for selecting active interfaces may cause service interruptions for a short time. You are advised not to change the mode for selecting active interfaces during service transmission.

You are advised not to bundle interfaces working at different rates into an Eth-Trunk in LACP mode because the priority preemption function may become ineffective.

Example

Configure Eth-Trunk 1 in LACP mode and configure the device to select active interfaces based on the interface rate.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp selected speed
```

5.2.43 lacp src-mac

Function

The **lacp src-mac** command configures an interface or system MAC address as an LACPDU's source MAC address.

The **undo lacp src-mac** command restores the default source MAC address.

By default, the system MAC address is used as an LACPDU's source MAC address.

Format

lacp src-mac { **bridge** | **port** }

undo lacp src-mac

Parameters

Parameter	Description	Value
bridge	Configures the system MAC address as an LACPDU's source MAC address.	-
port	Configures an interface MAC address as an LACPDU's source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a Huawei device connects to a non-Huawei device through Eth-Trunk interfaces in static LACP mode, if the Huawei device uses the default system MAC address, whereas the non-Huawei device uses the MAC addresses of the Eth-Trunk member interfaces as LACPDUs' source MAC addresses, the non-Huawei device may consider the received LACPDUs with the same MAC address invalid and therefore discard them, leading to an LACP negotiation failure.

To ensure a successful LACP negotiation, run the **lacp src-mac port** command to configure the Huawei device to use interface MAC addresses as LACPDUs' source MAC addresses.

Example

Configure interface MAC addresses as LACPDUs' source MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] lacp src-mac port
```

5.2.44 lacp system-id

Function

The **lacp system-id** command configures a Link Aggregation Control Protocol (LACP) system ID for an Eth-Trunk.

The **undo lacp system-id** command restores the default configuration.

By default, the system bridge MAC address functions as the LACP system ID of an Eth-Trunk.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp system-id *mac-address*

undo lacp system-id [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the LACP system ID of an Eth-Trunk.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number. You can enter 1 to 4 digits, such as 00e0 or fc01. If an H contains fewer than four digits, 0s are added ahead. For example, e0 is equal to 00e0. **NOTE** The LACP system ID of an Eth-Trunk cannot be all 0s.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple E-Trunks are configured on the device, the link aggregation groups can use different LACP system IDs. You need to run the **lacp system-id** *mac-address* command to set the LACP system ID.

The LACP system ID configured using the **lacp e-trunk system-id** command in the system view is valid for all Eth-Trunks that are added to the E-Trunk. The LACP system ID configured using the **lacp system-id** *mac-address* command in the Eth-Trunk interface view is valid for only the Eth-Trunk. If the LACP system ID is configured in both the Eth-Trunk interface view and system view, the system ID configured in the Eth-Trunk interface view takes effect.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command.

Example

Configure 00e0-fc00-0000 as the LACP system ID of Eth-Trunk 10.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] mode lacp
[HUAWEI-Eth-Trunk10] lacp system-id 00e0-fc00-0000
```

5.2.45 lacp system-priority

Function

The **lacp system-priority** command configures a Link Aggregation Control Protocol (LACP) system priority.

The **undo lacp system-priority** command restores the default LACP system priority.

The default LACP system priority is 32768.

Format

lacp system-priority *priority*

undo lacp system-priority

Parameters

Parameter	Description	Value
priority	Specifies an LACP system priority.	The value is an integer ranging from 0 to 65535. A smaller value indicates a higher LACP priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system priority is set to differentiate the priority of the local device and the peer device. The system of a higher priority is selected as the Actor of the link aggregate group (LAG), and active interfaces are selected according to interfaces of the Actor.

If the devices on both ends of the Eth-Trunk are not configured with system priorities, the devices use the default priority 32768. In this case, the Actor is selected according to the system MAC. The system with a smaller MAC is selected as the Actor.

A change in the LACP system priority will cause LACP renegotiation. During the renegotiation process, Eth-Trunk interfaces in LACP mode will go Down until the renegotiation succeeds, which may interrupt services. If the **lacp priority** command used to set the LACP interface priority is executed in the system view, the Eth-Trunk in LACP mode may alternate between Up and Down. To prevent this situation, run the **lacp priority-command-mode** command in the system view to set the configuration mode of the LACP system priority to **system-priority**. This mode can be used to differentiate the LACP system priority and LACP interface priority.

When running the **lacp priority-command-mode** command, note the following points:

- If you specify **default** in the command, the LACP system priority and LACP interface priority configurations still use the same command (**lacp priority** *priority*).
- If you specify **system-priority** in the command, run the **lacp system-priority** *priority* command to configure the LACP system priority and run the **lacp priority** *priority* command to configure the LACP interface priority.

Prerequisites

The **lacp priority-command-mode system-priority** command has been executed in the system view to set the configuration mode of the LACP system priority to **system-priority**.

Example

Set the LACP system priority to 10.

```
<HUAWEI> system-view
[HUAWEI] lacp priority-command-mode system-priority
[HUAWEI] lacp system-priority 10
```

5.2.46 lacp timeout

Function

The **lacp timeout** command configures the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs.

The **undo lacp timeout** command restores the default timeout interval.

By default, the timeout interval for an Eth-Trunk to receive LACPDUs is 90s.

Format

lacp timeout { **fast** [**user-defined** *user-defined*] | **slow** }

undo lacp timeout

Parameters

Parameter	Description	Value
fast	Indicates that the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs is 3 seconds. If **fast** is specified, the remote device sends an LACPDU every 1 second. In this mode, the local device can quickly respond to LACPDUs from the remote device but consumes more system resources compared with the **slow** mode.	-
user-defined *user-defined*	Specifies the timeout interval for an Eth-Trunk to receive LACPDUs when **fast** is specified.	The value is an integer that ranges from 3 to 90, in seconds.
slow	Indicates that the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs is 90 seconds. If **slow** is specified, the remote device sends an LACPDU every 30 seconds. In this mode, the local device responds to LACPDUs from the remote device slowly but consumes fewer system resources compared with the **fast** mode. The timeout interval on the two ends can be different. To facilitate maintenance, you are advised to set the same timeout interval at both ends.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two devices are connected through three GE interfaces at each end and the three GE interfaces are bundled into an Eth-Trunk, you can run the **mode lacp** command to configure the Eth-Trunk to work in LACP mode and run the **least active-linknumber** *link-number* command to set the lower threshold for the number of active interfaces to 2.

If the Eth-Trunk on the local device cannot detect a self-loop or fault that occurred on a member interface in the LAG on the remote device, the local Eth-Trunk still has three member interfaces in Up state and the three member interfaces still load balance data, causing packet loss. To ensure reliable data transmission, run the **lacp timeout** command to set the timeout interval for the Eth-Trunk to receive LACPDUs. If a local member interface does not receive any LACPDU within the configured timeout interval, it becomes Down immediately and no longer forwards data.

The number of Up member interfaces does not fall below the configured lower threshold for the number of active interfaces, so the Eth-Trunk is still Up. In this case, data is load balanced between the two member interfaces in Up state and reliably transmitted to the remote end.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

After the timeout interval is successfully configured, pay attention to the following points:

- If **fast** is specified, the remote device sends an LACPDU every 1 second.
- If **slow** is specified, the remote device sends an LACPDU every 30 seconds.

The timeout interval configured on an Eth-Trunk takes effect on all its member interfaces.

Example

Set the timeout interval for Eth-Trunk 1 to receive LACPDUs to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] lacp timeout fast
```

5.2.47 lacp track interface

Function

The **lacp track interface** command associates the secondary member interface of an Eth-Trunk interface in LACP mode with its primary member interface and dynamically changes the priority of the secondary member interface.

The **undo lacp track interface** command restores the default configuration.

By default, the secondary member interface of an Eth-Trunk interface in LACP mode is not associated with its primary member interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

lacp track interface *interface-type interface-number* **priority-reduced** *value*

undo lacp track interface *interface-type interface-number* **priority-reduced** *value*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an associated physical interface.	-
priority-reduced *value*	Specifies a value by which the priority is reduced. **NOTE** The new priority of the secondary member interface is the configured priority minus the value specified by **priority-reduced** *value*. The new priority of the secondary member interface must be less than the priority of the primary member interface.	The value is an integer ranging from 0 to 65535.

Views

Eth-Trunk member interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 5-3 Eth-Trunk interface in LACP mode

As shown in **Figure 5-3**, when no service is bound to the MA, an Eth-Trunk interface in LACP mode is configured on two devices. interface1 where the MEP resides is the interface of the Eth-Trunk interface's primary link. When the **delay-measure two-way trigger if-down** or **loss-measure single-ended-synthetic trigger if-down** command is configured on interface1, interface1 is triggered to go ETHOAM down if Y.1731 detects that the primary link has poor quality.

To ensure that services are not interrupted, run the **lacp track interface** command in the Eth-Trunk member interface view to increase the priority of the secondary member interface interface2. The secondary link then preempts the primary state, implementing an automatic primary/secondary link switchover.

Prerequisites

An Eth-Trunk interface has been configured to work in LACP mode using the **mode lacp** command in the Eth-Trunk interface view.

Precautions

An Eth-Trunk interface can have only two member interfaces. The maximum number of active links must be 1.

The **lacp track interface** command must be configured on the secondary member interface of an Eth-Trunk interface's Actor.

The secondary member interface must not be associated with another interface.

If the **lacp track interface** command has been run and the primary link has poor quality, the primary interface is triggered to go ETHOAM down. If the secondary link also has poor quality, a primary/secondary switchover is also performed because Y.1731 performance detection is not configured for the secondary link.

If the **lacp track interface** command has been run and the primary link has poor quality, the primary interface is triggered to go ETHOAM down. If the **undo lacp track interface** command is run to delete the configuration, two links cannot be selected within the timeout period. As a result, traffic is interrupted. Services can be restored only after the timeout period elapses.

Example

Associate the secondary member interface GE 0/0/1 of an Eth-Trunk interface in LACP mode with its primary member interface GE 0/0/2, and set a value by which the priority is reduced to 100 when the status of the primary member interface changes to ETHOAM down.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] trunkport GigabitEthernet 0/0/1 to 0/0/2
[HUAWEI-Eth-Trunk1] max active-linknumber 1
[HUAWEI-Eth-Trunk1] quit
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lacp track interface GigabitEthernet 0/0/2 priority-reduced 100
```

5.2.48 least active-linknumber

Function

The **least active-linknumber** command sets the lower threshold for the number of active interfaces in an Eth-Trunk.

The **undo least active-linknumber** command restores the default lower threshold for the number of active interfaces in an Eth-Trunk.

By default, the lower threshold for the number of active interfaces in an Eth-Trunk is 1.

Format

least active-linknumber *link-number*

undo least active-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the lower threshold for the number of active interfaces in an Eth-Trunk.	The value is an integer that ranges from 1 to 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 1 to 16 on the S5735S-H, S5736-S, and S6720S-S, and 1 to 8 on other models. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of active interfaces in an Eth-Trunk affects the status and bandwidth of the Eth-Trunk. The bandwidth of an Eth-Trunk is equal to the total bandwidth of all member interfaces in Up state.

The number of Up member links affects the status and bandwidth of an Eth-Trunk. To ensure that the Eth-Trunk functions properly and is less affected by member link status changes, set the following thresholds.

- Lower threshold for the number of active interfaces

  When the number of active interfaces falls below this threshold, the Eth-Trunk goes Down. This guarantees the Eth-Trunk a minimum available bandwidth.

  For example, if the Eth-Trunk is required to provide a minimum bandwidth of 2 Gbit/s and each member link's bandwidth is 1 Gbit/s, the lower threshold for the number of active interfaces must be set to 2 or larger.
- Upper threshold for the number of active interfaces

  When the number of active interfaces reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. This guarantees higher network reliability.

  To set the upper threshold for the number of active interfaces, use the **max active-linknumber** command.

To delete the configured lower threshold or restore the default lower threshold, use the **undo least active-linknumber** or **least active-linknumber 1** command.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

If you run the **least active-linknumber** command multiple times, only the latest configuration takes effect.

After the lower threshold for the number of active interfaces is configured, the following situations may occur:

- The Eth-Trunk goes Down when the number of active interfaces falls below the configured lower threshold.
- The Eth-Trunk goes Up when the number of active interfaces reaches the configured lower threshold.

If the **max active-linknumber** command has been configured before you run the **least active-linknumber** command, ensure that the lower threshold for the number of active interfaces is less than or equal to the upper threshold for the number of active interfaces.

Example

Set the lower threshold for the number of active interfaces to 3.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] least active-linknumber 3
```

5.2.49 load-balance

Function

The **load-balance** command sets a load balancing mode of an Eth-Trunk.

The **undo load-balance** command restores the default load balancing mode of an Eth-Trunk.

The default load balancing mode is **src-dst-ip**.

Format

load-balance { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** | **enhanced profile** *profile-name* }

undo load-balance

NOTE

Only S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S and S6730S-S support **enhanced profile** *profile-name*.

Parameters

Parameter	Description	Value
dst-ip	Indicates load balancing based on destination IP addresses.	-
dst-mac	Indicates load balancing based on destination MAC addresses.	-
src-ip	Indicates load balancing based on source IP addresses.	-
src-mac	Indicates load balancing based on source MAC addresses.	-
src-dst-ip	Indicates load balancing based on source and destination IP addresses.	-
src-dst-mac	Indicates load balancing based on source and destination MAC addresses.	-
enhanced profile *profile-name*	Indicates the name of the profile used to configure enhanced load balancing.	The value is a string of 1 to 31 characters.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure proper load balancing between physical links of an Eth-Trunk and avoid link congestion, use the **load-balance** command to set the load balancing mode of the Eth-Trunk.

Load balancing is valid only for outgoing traffic; therefore, the load balancing modes for the interfaces at both ends of the link can be different and do not affect each other.

You can set the load balancing mode based on traffic models. When a parameter of traffic changes frequently, you can set the load balancing mode based on this parameter to ensure that the traffic is load balanced evenly. For example, if IP addresses in packets change frequently, use the load balancing mode based on **dst-ip**, **src-ip**, or **src-dst-ip** so that traffic can be properly load balanced among physical links. If MAC addresses in packets change frequently and IP addresses are fixed, use the load balancing mode based on **dst-mac**, **src-mac**, or **src-dst-mac** so that traffic can be properly load balanced among physical links.

After the **load-balance** command is run to configure the load balancing mode for an Eth-Trunk, the hash factors used to calculate the outbound interface vary according to the packet type and device model. For example, after you configure load balancing based on the source and destination IP addresses for an Eth-Trunk, Layer 2 packets are load balanced automatically based on the source and destination MAC addresses because Layer 2 packets do not contain the source and destination IP addresses. You can run the **display eth-trunk load-balance** command to check the hash factors used when the outbound interface is calculated.

Prerequisites

Ensure that the **load-balance-profile** *profile-name* command has been executed to create a load balancing profile before you run the **load-balance enhanced profile** *profile-name* command.

Precautions

If you run the **load-balance** command multiple times, only the latest configuration takes effect.

When an inter-device Eth-Trunk is configured in a stack and the local device has Eth-Trunk member interfaces and the member interfaces function properly, only the Eth-Trunk member interfaces on the local device participate in load balancing. To enable Eth-Trunk member interfaces on other devices participate in load balancing, run the **undo local-preference enable** command to configure the Eth-Trunk not to preferentially forward local traffic.

If the value of *member-number* configured for an Eth-Trunk using the **assign trunk** { **trunk-group** *group-number* | **trunk-member** *member-number* }* command is larger than 16 on the S6735-S, S6720-EI and S6720S-EI or larger than 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, only the enhanced mode can be used for load balancing. If the enhanced mode is not used, problems such as packet loss and uneven load balancing may occur.

NOTE

The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S use the **src-dst-ip**, source TCP or UDP port number, and destination TCP or UDP port number in the hash algorithm for load balancing regardless of whether you configure this parameter.

The S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support only one load balancing mode globally. If the load balancing mode of an Eth-Trunk is modified, the modification takes effect on all Eth-Trunks. If an Eth-Trunk is created, the load balancing mode of the Eth-Trunk is the same as that of the original Eth-Trunks on the switch.

On the S6735-S, S6720-EI and S6720S-EI, when the **load-balance** command is run to configure the load balancing mode for an Eth-Trunk, whether the TCP or UDP port number is involved in the hash operation depends on the **ecmp load-balance** command. If the default setting is used or the **port** parameter is specified in the **ecmp load-balance** command, the TCP or UDP port number is involved in the hash operation when the dst-ip, src-ip, or src-dst-ip load balancing mode is configured for an Eth-Trunk.

On the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, when you run the **load-balance** { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** } command to configure the load balancing mode for an Eth-Trunk, regardless of which parameter is specified, packets are load balanced based on physical-layer source port numbers in the packets.

Example

Set the load balancing mode of Eth-Trunk 1 to **dst-mac**.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] load-balance dst-mac
```

5.2.50 load-balance-profile

Function

The **load-balance-profile** command creates a load balancing profile and displays the load balancing profile view.

The **undo load-balance-profile** command deletes a load balancing profile.

By default, there is not a load balancing profile on the device.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

load-balance-profile *profile-name*

undo load-balance-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a load balancing profile.	The value is a string of 1 to 31 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting the load balancing mode, create a load balancing profile.

Only one load balancing profile can be created.

NOTE

If VLAN mapping, VLAN stacking, or VLAN re-marking of the ACL is configured on an inbound interface, and a load balancing profile is configured on an inter-device Eth-Trunk outbound interface, you are advised not to choose the VLAN-based load balancing mode when running the **mpls field**, **l2 field**, **ipv4 field**, and **ipv6 field** commands.

Example

Create a load balancing profile named **a**.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a]
```

5.2.51 load-distribution active-linknumber-change

Function

The **load-distribution active-linknumber-change** command configures the number of interfaces in an Eth-Trunk where load balancing calculation is performed.

The **undo load-distribution active-linknumber-change** command cancels the configuration.

By default, the number of interfaces in an Eth-Trunk where load balancing calculation is performed is the number of active interfaces of the device.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

load-distribution active-linknumber-change *link-number1* **to** *link-number2*

undo load-distribution active-linknumber-change [*link-number1*]

Parameters

Parameter	Description	Value
link-number1	Specifies the number of active interfaces in an Eth-Trunk.	The value is an integer that ranges from 2 to 7.
link-number2	Specifies the number of interfaces in an Eth-Trunk where load balancing calculation is performed.	The value is an integer that ranges from 3 to 8. **NOTE** When this command is used, *link-number2* must be larger than *link-number1*.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the number of interfaces in an Eth-Trunk where load balancing calculation is performed is the number of active interfaces of the device. If the number of active interfaces is smaller than 8 and traffic on an Eth-Trunk is unevenly load balanced, you can run the **load-distribution active-linknumber-change** command to increase the number of interfaces in the Eth-Trunk where load balancing calculation is performed so that traffic can be better load balanced among active links.

The **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* command with different values of *link-number1* can be configured repeatedly. When the number of active interfaces is the same as the value of *link-number1*, the configuration takes effect. If the **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* command with the same value of *link-number1* is configured, only the latest configuration takes effect.

Precautions

When an inter-device Eth-Trunk is configured in a iStack and the **local-preference enable** command is used to configure an Eth-Trunk to preferentially forward local traffic, the number of interfaces in the Eth-Trunk where load balancing calculation is performed is the number of active interfaces.

This command is effective only for known unicast packets.

Example

Set the number of interfaces in Eth-Trunk 1 where load balancing calculation is performed to 8 when Eth-Trunk 1 has four active interfaces.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] load-distribution active-linknumber-change 4 to 8
```

5.2.52 load-distribution active-linknumber-change global

Function

The **load-distribution active-linknumber-change global** command specifies the number of Eth-Trunk interfaces participating in load balancing calculation in the system view.

The **undo load-distribution active-linknumber-change global** command cancels the configuration.

By default, the number of member interfaces that participate in load balancing calculation in all Eth-Trunks is the number of active interfaces in the Eth-Trunks.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, and S5720I-SI support this command.

Format

load-distribution active-linknumber-change *link-number1* **to** *link-number2* **global**

undo load-distribution active-linknumber-change [*link-number1*] **global**

Parameters

Parameter	Description	Value
link-number1	Specifies the number of active interfaces in an Eth-Trunk.	The value is an integer in the range from 2 to 7.
link-number2	Specifies the number of interfaces in an Eth-Trunk where load balancing calculation is performed.	The value is an integer in the range from 3 to 8. **NOTE** When this command is used, *link-number2* must be larger than *link-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the number of interfaces in an Eth-Trunk where load balancing calculation is performed is the number of active interfaces of the device. If the number of active interfaces is smaller than 8 and traffic on an Eth-Trunk is unevenly load balanced, you can run the **load-distribution active-linknumber-change global** command to set the number of Eth-Trunk interfaces participating in load balancing calculation to a larger value in the system view to better load balance traffic.

The **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* **global** command with different values of *link-number1* can be configured repeatedly. When the number of active interfaces is the same as the value of *link-number1*, the configuration takes effect. If the **load-distribution active-linknumber-change** *link-number1* **to** *link-number2* **global** command with the same value of *link-number1* is configured, only the latest configuration takes effect.

Precautions

- When an inter-device Eth-Trunk is configured in an iStack and the **local-preference enable** command is used to configure an Eth-Trunk to preferentially forward local traffic, the number of interfaces in the Eth-Trunk where load balancing calculation is performed is the number of active interfaces.
- This command is effective only for known unicast packets.
- If the number of Eth-Trunk interfaces participating in load balancing calculation is configured in both the system view and Eth-Trunk interface view, the configuration in the Eth-Trunk interface view takes effect.

Example

Set the number of Eth-Trunk interfaces participating in load balancing calculation to 8 when the Eth-Trunks have four active interfaces.

```
<HUAWEI> system-view
[HUAWEI] load-distribution active-linknumber-change 4 to 8 global
```

5.2.53 local-preference enable

Function

The **local-preference enable** command configures an Eth-Trunk to preferentially forward local traffic.

The **local-preference disable** command configures an Eth-Trunk not to preferentially forward local traffic.

The **undo local-preference enable** command configures an Eth-Trunk not to preferentially forward local traffic.

By default, an Eth-Trunk is enabled to preferentially forward local traffic.

NOTE

The S5735-S-I, S5720I-10X-PWH-SI-AC, and S5720I-6X-PWH-SI-AC do not support this configuration.

Format

local-preference { **enable** | **disable** }

undo local-preference enable

NOTE

The S2730S-S, 5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, and S5735S-S do not support the **local-preference disable**.

Parameters

None

Views

System view (S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735-S, S5735S-S, S5735S-L-M, S500)

Eth-Trunk interface view (Other models excluding the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735-S, S5735S-L-M, S500)

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a stack, an Eth-Trunk is configured to be the outbound interface of traffic to ensure reliable transmission. Member interfaces of the Eth-Trunk may be located on different devices. When the stack device forwards traffic, the Eth-Trunk may select an inter-device member interface based on the hash algorithm. This forwarding mode occupies bandwidth resources between devices and reduces traffic forwarding efficiency.

To solve the problem, run the **local-preference enable** command to enable the Eth-Trunk to preferentially forward local traffic. Then traffic arriving at the local device is preferentially forwarded through member interfaces of the local device. If there is no member interface on the local device, member interfaces on another device are used to forward traffic. This forwarding mode effectively saves inter-device bandwidth resources and improves traffic forwarding efficiency.

- When the local device has Eth-Trunk member interfaces and the member interfaces function properly, the Eth-Trunk forwarding table of the local device contains only local Eth-Trunk member interfaces. Therefore, the hash algorithm selects a local member interface, and traffic is forwarded through the local device.

- When the local device does not have any Eth-Trunk member interfaces or all member interfaces fail, the Eth-Trunk forwarding table of the local device contains all available Eth-Trunk member interfaces. The hash algorithm selects a member interface on another device, and traffic is forwarded through this device.

Precaution

Member interfaces of the local Eth-Trunk have sufficient bandwidth to forward local interface traffic, which prevents packet loss.

This function is only valid for known unicast packets, and is invalid for broadcast, unknown-unicast, and multicast (BUM) packets.

Example

Configure an Eth-Trunk not to preferentially forward local traffic.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 10
[HUAWEI-Eth-Trunk10] undo local-preference enable
```

5.2.54 max active-linknumber

Function

The **max active-linknumber** command sets the upper threshold for the number of active interfaces in an Eth-Trunk.

The **undo max active-linknumber** command restores the default upper threshold for the number of active interfaces in an Eth-Trunk.

By default, the upper threshold for the number of active interfaces in an Eth-Trunk is 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 on the S5735S-H, S5736-S, and S6720S-S, and 8 on other models.

Format

max active-linknumber *link-number*

undo max active-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the upper threshold for the number of active interfaces.	The value is an integer that ranges from 1 to 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 1 to 16 on the S5735S-H, S5736-S, and S6720S-S, and 1 to 8 on other models. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of active interfaces in an Eth-Trunk affects the status and bandwidth of the Eth-Trunk. The bandwidth of an Eth-Trunk is equal to the total bandwidth of all member interfaces in Up state.

The number of Up member links affects the status and bandwidth of an Eth-Trunk. To ensure that the Eth-Trunk functions properly and is less affected by member link status changes, set the following thresholds.

- Lower threshold for the number of active interfaces

  When the number of active interfaces falls below this threshold, the Eth-Trunk goes Down. This guarantees the Eth-Trunk a minimum available bandwidth.

  For example, if the Eth-Trunk is required to provide a minimum bandwidth of 2 Gbit/s and each member link's bandwidth is 1 Gbit/s, the minimum number of Up member links must be set to 2 or larger.

  To set the lower threshold for the number of active interfaces, run the **least active-linknumber** command.

- Upper threshold for the number of active interfaces

  When the number of active interfaces reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. The upper threshold is used to improve network reliability with assured bandwidth.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

- If you run the **max active-linknumber** command multiple times, only the latest configuration takes effect.
- The **max active-linknumber** command is valid only in LACP mode.
- If the number of member interfaces added to an Eth-Trunk is less than the upper threshold, there is no backup interface.
- After you run this command, if the number of current active interfaces reaches the upper threshold, new member interfaces function as the backup interfaces.
- If the **least active-linknumber** command has been configured before you run the **max active-linknumber** command, ensure that the maximum number of active member links is greater than or equal to the minimum number of active member links.
- The upper thresholds configured by the **max active-linknumber** command on both ends must be the same; otherwise, the Eth-Trunk status flaps if an active interface fails.
- In the scenario where the Eth-Trunk in 1:N LACP mode is used, the upper threshold for the number of Eth-Trunk member links in Up state is 1. After the active link becomes Down and before the backup link switches to the active link, the Down event of the original active link is not reported to the Eth-Trunk. To prevent route re-calculation caused by the Eth-Trunk Down event, the Down event of the original active link is reported to the Eth-Trunk in any of the following situations:
  - The timeout interval (60s) for reporting the Down event has been expired.
  - The backup link goes Up and becomes the active link.
  - The backup link fails and cannot go Up.

  The preceding implementation is inapplicable to scenarios where association between Eth-Trunk in E-Trunk or LACP mode and VRRP is configured.
- When a Huawei switch connects to a non-Huawei device, if the maximum number of active links at both ends is smaller than the number of all active interfaces of the Eth-Trunk, a link is interrupted suddenly especially in 1:1 mode. As a result, LACP negotiation results at both ends are different and the Eth-Trunk in Down state cannot be restored. It is recommended that LACP preemption be enabled and the same preemption delay be set at both ends or the maximum number of active links be not set at both ends.

  NOTE

  The 1:1 mode indicates that the maximum number of active links at both ends of an Eth-Trunk is 1 and two member interfaces join an Eth-Trunk at both ends.

Example

Set the upper threshold for the number of active interfaces in Eth-Trunk 1 to 3.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
[HUAWEI-Eth-Trunk1] max active-linknumber 3
```

5.2.55 mixed-rate link enable

Function

The **mixed-rate link enable** command adds interfaces with different interface types to the same Eth-Trunk.

The **undo mixed-rate link enable** command disables interfaces with different interface types from being added to the same Eth-Trunk.

By default, interfaces with different interface types are not allowed to be added to the same Eth-Trunk.

Format

mixed-rate link enable

undo mixed-rate link enable

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mixed-rate link enable** command to add interfaces with different rates to the same Eth-Trunk. If a member interface of an Eth-Trunk is a GE interface and the transmission bandwidth needs to be increased, you can enable this function when the GE interface needs to be changed to an XGE interface. During switching, add the XGE interface to the Eth-Trunk and then delete the GE interface. In this way, the service interruption time during the switching process can be reduced.

Precautions

- In LACP mode, if the peer device does not support this function, interfaces with different rates cannot be successfully added to the same Eth-Trunk even if the local device has the function enabled.

- In LACP mode, when Eth-Trunk negotiation succeeds, modifying the configuration of this command triggers a renegotiation, which can cause an LACP flap.
- In manual mode, if the peer device allows only interfaces with the same rate to be added to the same Eth-Trunk, traffic forwarded by all interfaces of the local device can be received only by the interfaces with the same rate, but not by the other interfaces.
- When an Eth-Trunk performs load balancing calculation, the interface rate cannot be used as the calculation weight. When interfaces with different rates are added to the same Eth-Trunk, traffic is evenly load balanced on all the links. Therefore, the bandwidth of member interfaces is calculated by the minimum rate of the member interfaces in the Eth-Trunk. For example, when a GE interface and a 10GE interface are added to the same Eth-Trunk, the rate of the GE interface is used in calculation and the bandwidth of the Eth-Trunk is 2G.
- When the **undo mixed-rate link enable** command is executed, ensure that the Eth-Trunk does not contain member interfaces with different rates.

Example

Set the Eth-Trunk 2 to allow interfaces with different interface types adding.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 2
[HUAWEI-Eth-Trunk2] mixed-rate link enable
```

5.2.56 mode

Function

The **mode** command configures a working mode of an Eth-Trunk.

The **undo mode** command restores the default working mode of an Eth-Trunk.

By default, an Eth-Trunk works in manual load balancing mode.

Format

mode { **lacp** | **manual load-balance** }

undo mode

Parameters

Parameter	Description	Value
lacp	Indicates the LACP mode.	-
manual load-balance	Indicates the manual load balancing mode.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

An Eth-Trunk can use the following working modes:

- LACP mode

  When the devices that are directly connected through an Eth-Trunk support LACP, you can run the **mode lacp** command to configure the Eth-Trunk to work in LACP mode. This mode can implement both load balancing and redundancy.

  In LACP mode, you must manually create an Eth-Trunk and add member interfaces to the Eth-Trunk. The difference between the LACP mode and manual load balancing mode is that active member interfaces are selected by sending LACP data units (LACPDUs). That is, when a group of interfaces are added to an Eth-Trunk, devices at both ends determine active and inactive interfaces by sending LACPDUs to each other.

- Manual load balancing mode

  When one of the devices at the two ends of an Eth-Trunk does not support LACP, run the **mode manual load-balance** command to configure the Eth-Trunk to work in manual load balancing mode. In addition, you can add multiple member interfaces to the Eth-Trunk to increase the bandwidth between the two devices and improve reliability.

  The manual load balancing mode is a basic link aggregation mode. In this mode, you must manually create an Eth-Trunk and add interfaces to the Eth-Trunk. LACP is not used.

  In manual load balancing mode, all active interfaces of the Eth-Trunk forward data and load balance traffic.

Precautions

If you run the **mode** command multiple times, only the latest configuration takes effect.

If an Eth-Trunk interface has member interfaces, you can switch the Eth-Trunk interface's working mode between manual mode and LACP mode. However, if the Eth-Trunk interface is added to an E-Trunk, you cannot change its working mode.

Example

Configure Eth-Trunk 1 to work in LACP mode.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] mode lacp
```

5.2.57 mpls field

Function

The **mpls field** command configures a load balancing mode of MPLS packets in a load balancing profile.

The **undo mpls field** command deletes a specified load balancing mode of MPLS packets or restores the default load balancing modes of MPLS packets.

By default, load balancing of MPLS packets is based on the two outer labels (**top-label** and **2nd-label**) of each packet.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6720S-S, S6730S-H, and S6730-H support this command.

Format

mpls field [**2nd-label** | **3rd-label** | **dip** | **dmac** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **smac** | **sport** | **top-label** | **vlan**] *

undo mpls field [**2nd-label** | **3rd-label** | **dip** | **dmac** | **l4-dport** | **l4-sport** | **protocol** | **sip** | **smac** | **sport** | **top-label** | **vlan**] *

Parameters

Parameter	Description	Value
2nd-label	Performs load balancing based on the second label of MPLS packets.	-
3rd-label	Performs load balancing based on the third label of MPLS packets.	-
dip	Performs load balancing based on destination IP addresses in MPLS packets.	-
dmac	Performs load balancing based on destination MAC addresses in MPLS packets.	-
l4-dport	Performs load balancing based on transport-layer destination port numbers in MPLS packets.	-

Parameter	Description	Value
l4-sport	Performs load balancing based on transport-layer source port numbers in MPLS packets.	-
protocol	Performs load balancing based on protocol types in MPLS packets.	-
sip	Performs load balancing based on source IP addresses in MPLS packets.	-
smac	Performs load balancing based on source MAC addresses in MPLS packets.	-
sport	Performs load balancing based on physical-layer source port numbers.	-
top-label	Performs load balancing based on the top label of MPLS packets.	-
vlan	Performs load balancing based on VLAN IDs.	-

Views

Load balancing profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo mpls field** command with no parameter specified restores the default load balancing modes of MPLS packets. The **undo mpls field** command with a parameter specified deletes a specified load balancing mode of MPLS packets.

The **mpls field 3rd-label** command implements flow label-based load balancing on L2VPN networks.

Precautions

- If you run the **mpls field** command multiple times, only the latest configuration takes effect.

- Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support the **3rd-label**, **l4-dport**, **l4-sport**, and **protocol** load balancing mode.
- Only **2nd-label**, **dmac**, **smac**, **sport**, and **top-label** are supported on the S5735S-H, S5736-S, and S6720S-S.
- Load balancing based on MPLS labels takes effect for only labeled packets on the ingress.
- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H, MPLS packets can be load balanced based on source or destination IP addresses on the P and tunnel egress on an L2VPN network. If original data packets are Layer 2 packets and the **sip** or **dip** parameter is specified, MPLS packets are load balanced based on source or destination MAC addresses. For other models, load balancing based on source or destination IP addresses for MPLS packets does not take effect on the P and tunnel egress on an L2VPN network. You are advised to configure the **2nd-label**, **3rd-label**, or **top-label** load balancing mode.

Example

In the load balancing profile **a**, set the load balancing mode of MPLS packets to **2nd-label**, that is, load balancing based on the second label of MPLS packets.

```
<HUAWEI> system-view
[HUAWEI] load-balance-profile a
[HUAWEI-load-balance-profile-a] mpls field 2nd-label
```

5.2.58 peer-address source-address

Function

The **peer-address source-address** command configures the local and remote IP addresses of an E-Trunk.

The **undo peer-address** command cancels the configuration.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer-address *peer-ip-address* **source-address** *source-ip-address*

undo peer-address

Parameters

Parameter	Description	Value
peer-address *peer-ip-address*	Specifies the remote IP address of an E-Trunk.	The value is in dotted decimal notation.

Parameter	Description	Value
source-address *source-ip-address*	Specifies the local IP address of an E-Trunk.	The value is in dotted decimal notation.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

The remote IP address of the local device is the local IP address of the remote device. For example, an E-Trunk is created between device A and device B. On device A, the remote IP address is 10.2.2.2 and the local IP address is 10.1.1.1. On device B, the remote IP address is 10.1.1.1 and the local IP address is 10.2.2.2.

When changing the local or remote IP address on a device, you must change the corresponding address on the remote device. Otherwise, LACPDUs are discarded.

Example

Set the remote IP address of E-Trunk 1 to 10.2.2.2 and the local IP address to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] peer-address 10.2.2.2 source-address 10.1.1.1
```

5.2.59 priority (E-Trunk view)

Function

The **priority** command sets the priority of an E-Trunk.

The **undo priority** command restores the default priority of an E-Trunk.

By default, the priority of an E-Trunk is 100.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

priority *priority*

undo priority

Parameters

Parameter	Description	Value
priority *priority*	Specifies the priority of an E-Trunk.	The value is an integer that ranges from 1 to 254. The default value is 100. A smaller value indicates a higher priority.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

An E-Trunk determines the master/backup status of the two devices according to the priority and system ID. The device with a higher priority is the master.

If the two devices have the same priority, the device with a smaller system ID is the master.

If the two devices have the same priority and system ID, the E-Trunk considers the configuration incorrect and discards LACPDUs.

Example

Set the priority of E-Trunk 1 to 10.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] priority 10
```

5.2.60 reset e-trunk packet-statistics

Function

The **reset e-trunk packet-statistics** command clears packet statistics about an E-Trunk.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset e-trunk packet-statistics [**e-trunk-id** *e-trunk-id*]

Parameters

Parameter	Description	Value
e-trunk-id *e-trunk-id*	Specifies the ID of an E-Trunk.	The value is an integer that ranges from 1 to 16.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting packet statistics about an E-Trunk in a given period, run the **reset e-trunk packet-statistics** command to clear the existing statistics. Then run **display e-trunk** command to view packet statistics.

Example

Clear packet statistics about E-Trunk 1.

```
<HUAWEI> reset e-trunk packet-statistics e-trunk-id 1
```

5.2.61 reset lacp statistics eth-trunk

Function

The **reset lacp statistics eth-trunk** command clears statistics about LACPDUs on all Eth-Trunks in LACP mode, a specified Eth-Trunk in LACP mode, or a specified member interface.

Format

reset lacp statistics eth-trunk [*trunk-id* [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer. The value varies according to device model: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720I-SI, S5720-LI, and S5720S-LI: 0-119 ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 0-127 ● S5735S-H, S5736-S, S6720S-S: 0-249 On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.
interface *interface-type interface-number*	Specifies an Eth-Trunk member interface. *interface-type*: specifies the type of the interface. *interface-number*: specifies the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics about LACPDUs on a specific interface within a given period of time, you need to run the **reset lacp statistics eth-trunk** command to clear the existing statistics about LACPDUs on the interface.

When using the **reset lacp statistics eth-trunk** command, pay attention to the following points:

- If no parameter is specified, statistics about LACPDUs on all Eth-Trunks in LACP mode are cleared.
- If only *trunk-id* is specified, statistics about LACPDUs on the specified Eth-Trunk in LACP mode are cleared.
- If both *trunk-id* and **interface** *interface-type interface-number* are specified, statistics about LACPDUs on the specified member interface of the specified Eth-Trunk in LACP mode are cleared.

Prerequisites

- The Eth-Trunk has been created and configured to work in LACP mode.
- Member interfaces have been added to the Eth-Trunk.

Precautions

The **reset lacp statistics eth-trunk** command clears statistics about sent and received LACPDUs on all Eth-Trunks in LACP mode, a specified Eth-Trunk in LACP mode, or a specified member interface. The cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Clear statistics about LACPDUs on all Eth-Trunks in LACP mode.

```
<HUAWEI> reset lacp statistics eth-trunk
```

Clear the statistics about LACPDUs on the member interface GigabitEthernet0/0/1 of Eth-Trunk 1 in LACP mode.

```
<HUAWEI> reset lacp statistics eth-trunk 1 interface gigabitethernet 0/0/1
```

5.2.62 revert disable

Function

The **revert disable** command disables revertive switching on an E-Trunk.

The **undo revert disable** command enables revertive switching on an E-Trunk.

By default, revertive switching is enabled on an E-Trunk and the revertive switching delay is 120s.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

revert disable

undo revert disable

Parameters

None

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On devices of an E-Trunk, when the faulty master device recovers, to prevent loss of traffic that is switched back, run the **revert disable** command to disable revertive switching on the E-Trunk.

Prerequisites

The E-Trunk has been correctly configured.

Follow-up Procedure

Run the **undo revert disable** command to enable revertive switching on an E-Trunk. When the faulty master device recovers, services are switched back to the original active device after 120s by default. Run the **timer revert delay** *delay-value* command to set the revertive switching delay.

Example

Disable revertive switching on the E-Trunk.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] revert disable
```

5.2.63 security-key

Function

The **security-key** command sets an encrypted password for an E-Trunk.

The **undo security-key** command restores the default password of an E-Trunk.

By default, no encryption password is configured.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

security-key { **simple** *simple-key* | **cipher** *cipher-key* }

undo security-key

Parameters

Parameter	Description	Value
simple *simple-key*	Indicates the password in plain text.	The value is a string of 1 to 255 case-sensitive characters without spaces and question mark (?). When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *cipher-key*	Indicates the password in cipher text.	The value is a case-sensitive character string without spaces and question mark (?). When double quotation marks are used around the string, spaces are allowed in the string. When the cipher text is used, the password can be entered in plain or cipher text. The length depends on the input mode: ● The password in plain text is a string of 1 to 255 characters, but the cipher-text password of 32 to 392 characters is displayed during query. ● The password in plain text is a string of 24 or 32 to 392 characters. **NOTE** ● It is recommended that the password in plain text be used. If the password in cipher text is used, the password must comply with the encryption algorithm. ● If the cipher-text password of 24 characters is supported before upgrade, the password is compatible during upgrade.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

NOTICE

If **simple** is specified, the password is saved in the configuration file in plain text. This brings security risks. Therefore, it is recommended that you specify **cipher** to save the password in cipher text.

You can encrypt the password with the plain text or cipher text.

- When the password is encrypted in plain text, it can be displayed in the configuration file.
- When the password is encrypted in cipher text, it is displayed as unidentifiable characters.

An encrypted password must be configured to enhance the system security. The encrypted passwords configured on the two devices of an E-Trunk must be the same.

Example

Set the password of E-Trunk 1 to YsHsjx_202206 and encrypt the password in cipher mode.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] security-key cipher YsHsjx_202206
```

5.2.64 sequence enable

Function

The **sequence enable** command enables the E-Trunk sequence number check function.

The **undo sequence enable** command disables the E-Trunk sequence number check function.

By default, the E-Trunk sequence number check function is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

sequence enable

undo sequence enable

Parameters

None

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the master device in an E-Trunk fails, an attacker can obtain the E-Trunk packet sent by the master device and attack the backup device, causing service interruptions. To resolve this problem, run the **sequence enable** command to enable the E-Trunk sequence number check function.

Configuration Impact

After the E-Trunk sequence number check function is enabled, the E-Trunk sequence number of packets is checked to protect against attacks and enhance E-Trunk security.

Precautions

The **sequence enable** command must be run on both the master and backup devices in an E-Trunk. Otherwise, the E-Trunk sequence number check function fails, causing dual master devices in the E-Trunk.

Example

Enable the E-Trunk sequence number check function on E-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] sequence enable
```

5.2.65 timer hello (E-Trunk view)

Function

The **timer hello** command sets the interval at which an E-Trunk sends hello packets.

The **undo timer hello** command restores the default interval for sending hello packets.

By default, the value of *hello-times* is 10, in 100 ms. That is, the default interval for sending hello packets is 1s.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

timer hello *hello-times*

undo timer hello

Parameters

Parameter	Description	Value
hello *hello-times*	Specifies the interval for sending hello packets.	The value is an integer that ranges from 5 to 100. The unit is 100 ms. The default value is 10.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

The **timer hello** command sets the interval at which the master and backup devices of an E-Trunk send hello packet. If the backup device receives no hello packet from the master device after certain number of intervals (specified by the **timer hold-on-failure multiplier** command for detecting hello packets), the backup device becomes the master.

Configuring a timeout period longer than 5 minutes is recommended, so that the Eth-Trunk packets can be sent to the peer device within the timeout period when a master/backup switchover is performed.

Example

Set the interval for sending hello packets to 9.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] timer hello 9
```

5.2.66 timer hold-on-failure multiplier

Function

The **timer hold-on-failure multiplier** command sets the time multiplier for an E-Trunk to detect hello packets.

The **undo timer hold-on-failure multiplier** command restores the default time multiplier.

By default, the time multiplier for detecting hello packets is 20.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

timer hold-on-failure multiplier *multiplier*

undo timer hold-on-failure multiplier

Parameters

Parameter	Description	Value
multiplier *multiplier*	Specifies the time multiplier for detecting hello packets.	The value is an integer that ranges from 3 to 300. The default value is 20.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

After the time multiplier for detecting hello packets is set, the local device is triggered to send hello packets. The remote device checks the timeout of the local device according to the timeout interval in the received packet. If the remote device is the backup device and does not receive hello packets from the local device within the timeout interval, the remote device becomes the master device.

Timeout interval = Interval for sending hello packets x Time multiplier

It is recommended that you set the time multiplier to 3 or larger.

The timeout interval configured on the local device is used by the remote device to check the timeout of the local device. If the hello packet from the remote device does not contain the timeout interval, the timeout interval of the local device is used.

Example

Set the time multiplier for detecting hello packets to 3.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] timer hold-on-failure multiplier 3
```

5.2.67 timer revert delay

Function

The **timer revert delay** command sets the revertive switching delay of an E-Trunk.

The **undo timer revert delay** command restores the default revertive switching delay of an E-Trunk.

By default, the revertive switching delay of an E-Trunk is 120 seconds.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

timer revert delay *delay-value*

undo timer revert delay

Parameters

Parameter	Description	Value
delay-value	Specifies the revertive switching delay of an E-Trunk.	The value is an integer that ranges from 0 to 3600, in seconds.

Views

E-Trunk view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the member Eth-Trunk on the master device goes Down, the member Eth-Trunk on the remote device becomes Up after LACP negotiation. Then the remote device becomes the master device, and the local device becomes the backup device. When the local device recovers, it becomes the master device again in the subsequent LACP negotiation.

If an E-Trunk works with other services, after the master device recovers from a fault, the status of the member Eth-Trunk on the master device may be restored before other services are restored. If traffic is immediately switched back to the master device, service traffic will be interrupted. To solve this problem, you need to set the revertive switching delay for the E-Trunk.

After you run the **timer revert delay** command to set the revertive switching delay for an E-Trunk, the local Eth-Trunk can become Up only after the delay timer times out. This delays the revertive switching of the service traffic, ensuring nonstop services.

Precautions

The revert delay of an E-Trunk must be greater than the PW recovery time. This ensures that services are not interrupted when traffic is reverted back to the master device.

In E-Trunk B2B scenarios where there are four PE devices and an E-Trunk is configured between each two PEs, to ensure that services can be switched back to the master device when a fault is rectified, configure the master device in one E-Trunk to immediately switch traffic back and the master device in the other E-Trunk to switch traffic back after a delay.

Example

Set the revertive switching delay of E-Trunk 1 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] e-trunk 1
[HUAWEI-e-trunk-1] timer revert delay 100
```

5.2.68 trunkport

Function

The **trunkport** command adds a member interface in the Eth-Trunk interface view.

The **undo trunkport** command deletes a member interface in the Eth-Trunk interface view.

By default, no member interface is added to an Eth-Trunk.

Format

trunkport *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-16> [**mode** { **active** | **passive** }]

undo trunkport *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-16>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-
mode { **active** | **passive** }	Indicates the mode in which an Eth-Trunk member interface sends packets. This parameter is valid for only the Eth-Trunk in LACP mode. By default, the mode an Eth-Trunk member interface sends packets is **active**. ● **active**: indicates that an Eth-Trunk member interface proactively sends negotiation packets. ● **passive**: indicates that an Eth-Trunk member interface sends packets to negotiate with its remote end only after receiving a packet from its remote end.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

An Eth-Trunk contains a maximum of 32 member interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 member interfaces on the S5735S-H, S5736-S, and S6720S-S and 8 member interfaces on other models.

NOTE

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Example

Add GigabitEthernet0/0/1 to Eth-Trunk 1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] trunkport gigabitethernet 0/0/1
```

5.2.69 unknown-unicast load-balance

Function

The **unknown-unicast load-balance** command configures a load balancing mode for broadcast, unknown-unicast, and multicast (BUM) traffic.

The **undo unknown-unicast load-balance** command restores the default load balancing mode for BUM traffic.

By default, BUM traffic is load balanced based on source and destination MAC addresses of packets.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

unknown-unicast load-balance { **dmac** | **smac** | **smacxordmac** | **enhanced** [**lbid**] }

undo unknown-unicast load-balance

Parameters

Parameter	Description	Value
dmac	Load balances the BUM traffic based on destination MAC addresses of packets.	-
smac	Load balances BUM traffic based on source MAC addresses of packets.	-
smacxordmac	Load balances BUM traffic based on source and destination MAC addresses of packets.	-
enhanced [**lbid**]	Load balances BUM traffic based on the enhanced load balancing profile. **NOTE** Only the S6735-S, S6720-EI and S6720S-EI support the **lbid** parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the traffic policy contains a traffic behavior that defines the action of re-marking destination MAC addresses of packets, load balancing of BUM traffic must be based on source MAC addresses of packets.

On a VPLS network or a VXLAN network, when the S6735-S, S6720-EI or S6720S-EI switches form a stack, if the outbound interface of BUM traffic is an inter-device Eth-Trunk interface, you need to configure run the **unknown-unicast load-balance enhanced lbid** to configure the load balancing mode. Otherwise, packet loss may occur or there may be duplicate packets.

Example

Configure the device to load balance BUM traffic based on source MAC addresses of packets.

```
<HUAWEI> system-view
[HUAWEI] unknown-unicast load-balance smac
```

5.2.70 unicast load-balance enhanced

Function

The **unicast load-balance enhanced** command configures a load balancing mode for known unicast packets based on the inner or outer IP address.

The **undo unicast load-balance enhanced** commands restores the default loading balancing mode for known unicast packets.

By default, load balancing for known unicast packets is based on the outer IP address.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

unicast load-balance enhanced { **inner-ip** | **outer-ip** } *

undo unicast load-balance enhanced

Parameters

Parameter	Description	Value
inner-ip	Indicates that load balancing for known unicast packets is based on the inner IP address.	-
outer-ip	Indicates that load balancing for known unicast packets is based on the outer IP address.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When configuring enhanced Eth-Trunk load balancing, you can run the **unicast load-balance enhanced** command to configure known unicast packets, such as GRE packets, to be load balanced based on the inner IP address, outer IP address, or both.

- In IPv4 over GRE or IPv6 over GRE scenarios, if **inner-ip** is specified, known unicast packets are load balanced based on the inner source IP address, inner destination IP address, or both. Similarly, you can configure known unicast packets to be load balanced based on the outer source IP address, outer destination IP address, or both. Additionally, known unicast packets can be load balanced based on the inner and outer source IP addresses, inner and outer destination IP addresses, or both.

- In Ethernet over GRE scenarios, if **inner-ip** is specified, known unicast packets are load balanced based on the inner source MAC address, inner destination MAC address, or both. If **outer-ip** is specified, known unicast packets are load balanced based on the outer source IP address, outer destination IP address, or both. If both **inner-ip** and **outer-ip** are specified, known unicast packets are load balanced based on the outer source IP address and inner source MAC address, outer destination IP address and inner destination MAC address, or both.
- In PPPoE scenarios, if **inner-ip** is specified, known unicast packets are load balanced based on the inner source IP address, inner destination IP address, or both. If **outer-ip** is specified, known unicast packets are load balanced based on the outer source MAC address, outer destination MAC address, or both. If both **inner-ip** and **outer-ip** are specified, known unicast packets are load balanced based on the inner source IP address and outer source MAC address, inner destination IP address and outer destination MAC address, or both.

Example

Configure an Eth-Trunk interface to perform load balancing for known unicast packets based on the inner IP address.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] unicast load-balance enhanced inner-ip
```

5.3 VLAN Configuration Commands

5.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.3.2 damping time

Function

The **damping time** command sets the VLAN damping time on a VLANIF interface, that is, the delay before reporting a VLAN Down event to the VLANIF interface.

The **undo damping time** command restores the default damping time.

The default damping time on a VLANIF interface is 0 seconds. That is, the VLANIF interface is notified immediately after the VLAN becomes Down.

Format

damping time *delay-time*

undo damping time

Parameters

Parameter	Description	Value
delay-time	Specifies the delay before reporting the VLAN Down event to a VLANIF interface.	The value ranges from 0 to 20, in seconds. The default value is 0.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Software upgrade or active/standby switchover on the switch may cause frequent status changes on VLANIF interfaces. To prevent network flapping, run the **damping time** command on VLANIF interfaces to configure the VLAN damping function.

When all interfaces in a VLAN become Down, the switch waits for a period specified by *delay-time* and then reports the VLAN Down event to the VLANIF interface.

Precautions

If any interface in the VLAN becomes Up within the delay time, the VLANIF interface remains Up.

You can use the **display interface vlanif** command to view the VLAN damping time.

If you run the **damping time** command multiple times in the same VLANIF interface view, only the latest configuration takes effect.

Example

Set the VLAN damping time on VLANIF 10 to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] damping time 10
```

5.3.3 description (VLAN view)

Function

The **description** command sets the description of a VLAN.

The **undo description** command restores the default description of a VLAN.

By default, the description of a VLAN shows the VLAN ID. For example, the description of VLAN 2 is "VLAN 0002".

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VLAN.	It is a string of 1 to 80 characters. The characters are case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command is used to set the description of a VLAN, which is convenient for identifying, memorizing, and maintaining the VLAN.

The **display vlan** *vlan-id* **verbose** command can display the description of a specified VLAN.

Precautions

Set different descriptions for VLANs to distinguish.

If you run the **description** command multiple times in the same VLAN view, only the last configuration takes effect.

Example

Set the description of VLAN 2 as "huawei".

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] description huawei
```

5.3.4 description (VLANIF interface view)

Function

The **description** command set the description of a VLANIF interface.

The **undo description** command restores the default description of a VLANIF interface.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VLANIF interface.	The value is a string of 1 to 242 characters. The character string is case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage VLANIF interfaces conveniently, use the **description** command to set VLANIF interface descriptions. The description of a VLANIF interface helps you identify the VLANIF interface and know its functions.

You can use the **display interface vlanif** command to view the description of a VLANIF interface.

Precautions

The description of a VLANIF interface should provide useful information.

Set different descriptions for VLANIF interfaces to distinguish VLANIF interfaces.

If you run the **description** command multiple times in the same VLANIF interface view, only the latest configuration takes effect.

Example

Set the description of VLANIF 2 to huawei.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] description huawei
```

5.3.5 display default-parameter vlan

Function

The **display default-parameter vlan** command displays the default parameters of a VLAN.

Format

display default-parameter vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Displays the default parameters of a specified VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A great number of VLANs are created on a device, and different features are configured for every VLAN. To know the default parameters of a VLAN, run the **display default-parameter vlan** command to specify the VLAN and view its default parameters.

Prerequisites

The specified VLAN has been created.

Precautions

The default parameters of a VLAN do not change with the VLAN configuration.

Example

Display the default parameters of VLAN 10.

```
<HUAWEI> display default-parameter vlan 10
  VLAN ID              : 10
  Type                 : Common
  Status               : undo shutdown
  Broadcast            : Forward
  Unknown-Multicast    : Forward
  Unknown-Unicast      : Forward
  Statistics           : Disable
  MAC learning         : Enable
  Property             : Default
  Description          : VLAN 0010
```

Table 5-34 Description of the **display default-parameter vlan** command output

Item	Description
VLAN ID	VLAN ID.
Type	VLAN type. The value can be: Common: indicates an ordinary VLAN.
Status	VLAN status. The value can be: undo shutdown: The VLAN is enabled.
Broadcast	Method to deal with broadcast packets. Forward: forwards broadcast packets.
Unknown-Multicast	Method to deal with unknown multicast packets. Forward: forwards unknown multicast packets.
Unknown-Unicast	Method to deal with unknown unicast packets. Forward: forwards unknown unicast packets.
Statistics	Whether collecting statistics about VLAN packets is enabled. The value can be: Disable: Collecting statistics about VLAN packets is disabled.
MAC learning	Whether MAC address learning is enabled. The value can be: Enable: MAC address learning is enabled.
Property	VLAN attribute. The value can be: Default: indicates an ordinary VLAN.
Description	Description of a VLAN.

5.3.6 display interface vlanif

Function

The **display interface vlanif** command displays the status and configuration of a VLANIF interface.

Format

display interface vlanif [*vlan-id* | **main**]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer and the value range depends on the range of existing VLANIF interfaces. You can enter the question mark (?) to obtain the range of VLAN IDs.
main	Displays status and traffic statistics about a VLANIF interface. A VLANIF interface has no sub-interfaces. Status and traffic statistics about a VLANIF interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor an interface or locate an interface fault, you can use the **display interface vlanif** command to view the interface status, interface configuration, and traffic statistics on the interface.

Prerequisites

The specified VLANIF interface has been created.

Precautions

If *vlan-id* is not specified, the **display interface vlanif** command displays information about all VLANIF interfaces in the system.

Example

Display the status and configuration of VLANIF 3.

```
<HUAWEI> display interface vlanif 3
Vlanif3 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-08-03 03:54:16
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc12-3456
Current system time: 2012-02-10 11:24:14
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  0 packets, 0 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Table 5-35 Description of the display interface vlanif command output

Item	Description
current state	Status of a VLANIF interface. The value is UP or Down.
Line protocol current state	Status of the link-layer protocol on a VLANIF interface. The value is UP or Down.
Last line protocol up time	The last time the line protocol is up.
Description	Description of a VLANIF interface. To specify the parameter, run the **description** command.
Route Port	Indicates that the interface is a Layer 3 interface.
The Maximum Transmit Unit	Specifies the MTU of a VLANIF interface. To specify the parameter, run the **mtu** command.
Internet Address	IP address of a VLANIF interface. If the VLANIF interface does not have an IP address, the system displays "Internet protocol processing: disabled." To specify the parameter, run the **ip address** command.
IP Sending Frames' Format	Encapsulation format of IP packets, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the VLANIF interface.

Item	Description
Last 300 seconds input/output rate	Rates of incoming and outgoing packets in the last 300 seconds, expressed in bytes per second and packets per second. **NOTE** On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S- this field is displayed only when the traffic statistics function is enabled on the VLAN view using the **statistic enable** command. On other models, this field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Current system time	Indicates the current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS±HH:MM.
Input/Output	Number of bytes and packets sent and received by the VLANIF interface. **NOTE** On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S- this field is displayed only when the traffic statistics function is enabled on the VLAN view using the **statistic enable** command. On other models, this field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Input/Output bandwidth utilization	Inbound/outbound bandwidth utilization on an interface.

5.3.7 display ip-subnet-vlan vlan

Function

The **display ip-subnet-vlan vlan** command displays information about IP subnets associated with VLANs.

Format

display ip-subnet-vlan vlan { **all** | *vlan-id1* [**to** *vlan-id2*] }

Parameters

Parameter	Description	Value
all	Displays IP subnets associated with all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Displays IP subnets associated with specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only the IP subnet associated with *vlan-id1* is displayed.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring IP subnet-based VLAN assignment, you can run the **display ip-subnet-vlan vlan** command to verify the configuration.

This command displays the VLAN ID, IP subnet index, IP subnet address, IP subnet mask, and 802.1p priority of the VLAN mapping an IP subnet.

When using the **display ip-subnet-vlan vlan** command, pay attention to the following points:

- If **all** is specified, IP subnets associated with all VLANs are displayed.
- If **vlan** *vlan-id* is specified, the IP subnet associated with the specified VLAN is displayed.
- If *vlan-id1* **to** *vlan-id2* is specified, IP subnets associated with the specified VLANs are displayed.

Precautions

If no VLAN is associated with any IP subnet by using the **ip-subnet-vlan** command, the **display ip-subnet-vlan vlan** command does not display any information.

Example

Display information about IP subnets associated with all VLANs.

```
<HUAWEI> display ip-subnet-vlan vlan all
----------------------------------------------------------------
 Vlan    Index   IpAddress           SubnetMask          Priority
 ----------------------------------------------------------------
 2       12      192.168.1.1         255.255.255.0       3
 ----------------------------------------------------------------
 ip-subnet-vlan count: 1                 total count: 1
```

Table 5-36 Description of the **display ip-subnet-vlan vlan** command output

Item	Description
Vlan	ID of an IP subnet-based VLAN. To specify the parameter, run the **ip-subnet-vlan** command.
Index	Index of an IP subnet. To specify the parameter, run the **ip-subnet-vlan** command.
IpAddress	IP subnet address. To specify the parameter, run the **ip-subnet-vlan** command.
SubnetMask	IP subnet mask. To specify the parameter, run the **ip-subnet-vlan** command.
Priority	802.1p priority of the VLAN associated with an IP address or subnet. To specify the parameter, run the **ip-subnet-vlan** command.

5.3.8 display lnp

Function

The **display lnp interface** command displays LNP negotiation information on a Layer 2 Ethernet interface.

Format

display lnp { **interface** *interface-type interface-number* | **summary** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays LNP negotiation information on a specified Layer 2 Ethernet interface.	-
summary	Displays LNP negotiation information on all Ethernet interfaces of a Layer 2 device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you want to check the link type and traffic statistics of a Layer 2 Ethernet interface after enabling LNP negotiation, run the **display lnp** command.

To monitor the status of or locate the fault on an LNP-enabled Layer 2 Ethernet interface, run the **display lnp** command to obtain the status information and statistics about user packets. This information provides a basis for fault locating.

Example

Display LNP negotiation information on a specified Layer 2 Ethernet interface.

```
<HUAWEI> display lnp interface gigabitethernet0/0/1
LNP information for GigabitEthernet0/0/1:
  Port link type: trunk
  Negotiation mode: desirable
  Hello timer expiration(s): 19
  Negotiation timer expiration(s): 0
  Trunk timer expiration(s): 289
  FSM state: trunk

  Packets statistics
  4 packets received
    0 packets dropped
      bad version: 0, bad TLV(s): 0, bad port link type: 0,
      bad negotiation state: 0, other: 0
  5 packets output
    0 packets dropped
      other: 0
```

Table 5-37 Description of the display lnp interface command output

Item	Description
LNP information for	Layer 2 Ethernet interface on which LNP negotiation information is displayed

Item	Description
Port link type	Link-type of the Layer 2 Ethernet interface ● Trunk ● Access ● Hybrid ● dot1q-tunnel
Negotiation mode	Negotiation mode on the Layer 2 Ethernet interface, which can be configured using the **port link-type** command ● desirable ● auto ● on ● off
Hello timer expiration(s)	Timeout period for the Hello timer
Negotiation timer expiration(s)	Timeout period for the negotiation timer
Trunk timer expiration(s)	Timeout period for the Trunk timer
FSM state	Status of the LNP state machine
Packets statistics	Statistics about LNP packets
packets received	Number of received LNP packets
packets dropped	Number of dropped LNP packets
bad version	Number of LNP packets dropped due to incorrect versions
bad TLV(s)	Number of LNP packets dropped due to incorrect TLVs
bad port link type	Number of LNP packets dropped due to incorrect negotiation results
bad negotiation state	Number of LNP packets dropped due to incorrect negotiation states
other	Number of LNP packets dropped due to other causes
packets output	Number of sent LNP packets

Display LNP negotiation information on all Ethernet interfaces of a Layer 2 device.

```
<HUAWEI> display lnp summary
Global LNP : Negotiation enable
-------------------------------------------------------------------------------
C: Configured; N: Negotiated; *: Negotiation disable;
Port         link-type(C)   link-type(N)   InDropped   OutDropped  FSM
-------------------------------------------------------------------------------
```

```
GE0/0/1      access        access              0            0  off
GE0/0/2      desirable      access              0            0  off
GE0/0/3      desirable      access              0            0  off
GE0/0/4      desirable      access              0            0  off
GE0/0/6      desirable      access              0            0  off
GE0/0/7      desirable      access              0            0  off
GE0/0/8      desirable      access              0            0  off
GE0/0/9      desirable      access              0            0  off
GE0/0/10     desirable      access              0            0  off
```

Table 5-38 Description of the display lnp summary command output

Item	Description
Global LNP	Whether LNP is enabled globally, which can be configured using the **lnp disable** command
Port	Layer 2 Ethernet interface on which LNP negotiation information is displayed
link-type(C)	Negotiation mode on the Layer 2 Ethernet interface, which can be configured using the **port link-type** command
link-type(N)	Negotiation result on the Layer 2 Ethernet interface
InDropped	Number of incoming LNP packets that are dropped on the Layer 2 Ethernet interface
OutDropped	Number of outgoing LNP packets that are dropped on the Layer 2 Ethernet interface
FSM	Status of the LNP state machine ● access ● trunk ● on ● off

5.3.9 display mac-vlan

Function

Using the **display mac-vlan** command, you can view the configuration of MAC address-based VLAN assignment.

Format

display mac-vlan { **mac-address** { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] } | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays VLANs associated with all MAC addresses.	-
mac-address *mac-address*	Displays the VLAN associated with a specified MAC address.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
mac-address-mask	Specifies the mask of a MAC address.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. The default value is FFFF-FFFF-FFFF.
mac-address-mask-length	Specifies the mask length of a MAC address.	The value is an integer that ranges from 1 to 48. The default value is 48.
vlan *vlan-id*	Displays the configuration of a specified MAC address-based VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring MAC address-based VLAN assignment, you can run the **display mac-vlan** command to verify the configuration.

When using the **display mac-vlan** command, pay attention to the following points:

- If **mac-address** *mac-address* is specified, the VLAN associated with the specified MAC address is displayed.
- If **mac-address all** is specified, all VLANs associated with MAC addresses are displayed.
- If **vlan** *vlan-id* is specified, configuration of the specified MAC address-based VLAN is displayed.

Example

Display the configuration of all MAC address-based VLANs.

```
<HUAWEI> display mac-vlan mac-address all
-------------------------------------------------------------
MAC Address      MASK            VLAN    Priority
-------------------------------------------------------------
00e0-fc12-0006  ffff-ffff-ffff  200     0

Total MAC VLAN address count: 1
```

Table 5-39 Description of the display mac-vlan command output

Item	Description
MAC Address	MAC address associated with a VLAN. To specify the parameter, run the **mac-vlan mac-address** command.
MASK	Mask of a MAC address. To specify the parameter, run the **mac-vlan mac-address** command.
VLAN	ID of the VLAN associated with a MAC address. To specify the parameter, run the **mac-vlan mac-address** command.
Priority	802.1p priority of the VLAN associated with the MAC address. To specify the parameter, run the **mac-vlan mac-address** command.

5.3.10 display policy-vlan

Function

Using the **display policy-vlan** command, you can view the configuration of policy-based VLAN assignment.

Format

display policy-vlan { **all** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all policy-based VLANs.	-

Parameter	Description	Value
vlan *vlan-id*	Displays the configuration of a specified policy-based VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After associating MAC address and IP address binding policies to VLANs, you can use the **display policy-vlan** command to verify the configuration. The command displays the source MAC address, source IP address, interface where a policy-based VLAN is configured, VLAN ID, and VLAN priority.

When using the **display policy-vlan** command, pay attention to the following points:

- If **all** is specified, configuration of all policy-based VLANs is displayed.
- If **vlan** *vlan-id* is specified, configuration of the specified policy-based VLAN is displayed.

Precautions

If no policy-based VLAN is configured by using the **policy-vlan** command, the **display policy-vlan** does not display any information.

Example

Display configuration of policy-based VLAN assignment.

```
<HUAWEI> display policy-vlan all
 -----------------------------------------------------------------------
 MacAddress      IPAddress       Port                 Vlan   Priority
 -----------------------------------------------------------------------
 00e0-fc03-0003  10.2.2.2        GigabitEthernet0/0/1  6       4
 00e0-fc02-0002  10.1.1.1        NA                    8       6
 -----------------------------------------------------------------------
Total Policy-VLAN count: 2
```

Table 5-40 Description of the display policy-vlan command output

Item	Description
MacAddress	Source MAC address bound to a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.
IPAddress	Source IP address bound to a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.
Port	Interface where the MAC address and IP address are bound. To specify the parameter, run the **policy-vlan** command.
Vlan	ID of a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.
Priority	802.1p priority of a policy-based VLAN. To specify the parameter, run the **policy-vlan** command.

5.3.11 display port vlan

Function

The **display port vlan** command displays information about interfaces of the VLAN.

Format

display port vlan [*interface-type interface-number* | **active**] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface in the VLAN. If this parameter is not specified, information about all interfaces in the VLAN is displayed.	-

Parameter	Description	Value
active	Indicates the interface information of dynamic entries in the VLAN. The dynamic mappings between VLANs and ports are identified by services such as voice VLAN service or protocols such as GARP VLAN registration protocol (GVRP).	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display port vlan** command to view information about interfaces of the VLAN and check whether the VLAN is assigned by the command, protocols, or services. If a fault occurs on an interface, you can locate the fault based on the information about the interface and VLAN.

Prerequisite

A VLAN has been created and the Layer 2 interface has joined the VLAN.

Precautions

If a large number of mappings between interfaces and VLANs exist on the device, you are advised to specify the interface or **active** to filter the command output. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, causing required information to fail to be obtained.
- The system does not respond because of long-time information traverse and search.

Example

Display information about interfaces that belong to each VLAN on the device.

```
<HUAWEI> display port vlan
Port                    Link Type    PVID  Trunk VLAN List
-------------------------------------------------------------------------------
GigabitEthernet0/0/1    hybrid       1     -
GigabitEthernet0/0/2    hybrid       1     -
```

Display information about all dynamic entries.

```
<HUAWEI> display port vlan active
T=TAG U=UNTAG
-------------------------------------------------------------------------------
Port            Link Type    PVID    VLAN List
-------------------------------------------------------------------------------
GE0/0/3           hybrid      2        T: 10
GE0/0/4           trunk       10       T: 100
```

NOTE

When the stack is set up through service interfaces and service interfaces are configured as physical member interfaces, the physical member interfaces are not displayed in **display port vlan** and **display port vlan active** command outputs.

Table 5-41 Description of the display port vlan command output

Item	Description
Port	Indicates the type and number of the interface.
Link Type	Types of the interface link: ● access ● trunk ● hybrid ● dot1q-tunnel ● desirable ● auto To specify the parameter, run the **port link-type** command. **NOTE** For the Eth-Trunk member interface, the value is displayed as -.
PVID	Indicates the default VLAN ID of the interface. By default, VLAN 1 is the default VLAN of all interfaces. For interfaces of the access and dot1q types and those interfaces negotiated as the access type, you can run the **port default vlan** command to configure the default VLAN. For interfaces of the hybrid type, you can run the **port hybrid pvid vlan** command to configure the default VLAN. For interfaces of the trunk type and those interfaces negotiated as the trunk type, you can run the **port trunk pvid vlan** command to configure the default VLAN. **NOTE** For the Eth-Trunk member interface, the value is displayed as 0.
Trunk VLAN List	Indicates the VLAN IDs of packets that are statically configured to pass through an interface.

Item	Description
VLAN List	- Indicates the VLAN IDs that are dynamically added by an interface. - Indicates the VLAN IDs of packets that are statically configured to pass through an interface.

5.3.12 display protocol-vlan interface

Function

The **display protocol-vlan interface** command displays the protocol-based VLAN configuration on a specified interface or all interfaces.

Format

display protocol-vlan interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays the protocol-based VLANs configured on all interfaces.	-
interface-type interface-number	Displays the protocol-based VLAN configured on a specified interface. - *interface-type* specifies the type of an interface. - *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After associating an interface with a protocol-based VLAN, you can use the **display protocol-vlan interface** command to verify the configuration.

Precautions

If no protocol-based VLAN is configured by using the **protocol-vlan vlan** command, the **display protocol-vlan interface** command displays no information.

Example

Display the protocol-based VLAN associated with GE0/0/1.

```
<HUAWEI> display protocol-vlan interface gigabitethernet 0/0/1
-------------------------------------------------------------------------------
 Interface              VLAN    Index       Protocol Type          Priority
-------------------------------------------------------------------------------
 GigabitEthernet0/0/1     2       2          ipv4                4
```

Table 5-42 Description of the display protocol-vlan interface command output

Item	Description
Interface	Interface associated with a protocol-based VLAN. To specify the parameter, run the **protocol-vlan vlan** command.
VLAN	ID of a protocol-based VLAN. To specify the parameter, run the **protocol-vlan vlan** command.
Index	Index of a protocol. To specify the parameter, run the **protocol-vlan vlan** command.
Protocol Type	Type of a protocol. To specify the parameter, run the **protocol-vlan** command.
Priority	802.1p priority of the VLAN associated with a protocol. To specify the parameter, run the **protocol-vlan** command.

5.3.13 display protocol-vlan vlan

Function

The **display protocol-vlan vlan** command displays the types and indexes of the protocols associated with VLANs.

Format

display protocol-vlan vlan { **all** | *vlan-id1* [**to** *vlan-id2*] }

Parameters

Parameter	Description	Value
all	Displays the protocols associated with all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Displays the protocols associated with specified VLANs. - *vlan-id1* specifies the start VLAN ID. - *vlan-id2* specifies the end VLAN ID.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. *vlan-id2* is an integer that ranges from 1 to 4094. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring protocol-based VLANs, you can use the **display protocol-vlan vlan** command to verify the configuration.

Example

Display types and indexes of protocols associated with VLANs.

```
<HUAWEI> display protocol-vlan vlan all
-------------------------------------------------------------------
 VLAN          Protocol Index    Protocol Type
-------------------------------------------------------------------
 2             2                 ipv4
```

Table 5-43 Description of the display protocol-vlan vlan command output

Item	Description
VLAN	ID of a protocol-based VLAN. To specify the parameter, run the **protocol-vlan** command.
Protocol Index	Index of a protocol. To specify the parameter, run the **protocol-vlan** command.

Item	Description
Protocol Type	Type of a protocol. To specify the parameter, run the **protocol-vlan** command.

5.3.14 display vlan

Function

The **display vlan** command displays information about VLANs.

Format

display vlan [*vlan-id* [**verbose** \| **statistics** [**slot** *slot-id*] \| **port-info**]]

display vlan [*vlan-id1* [**to** *vlan-id2*]]

display vlan summary [**slot** *slot-id*]

display vlan vlan-name *vlan-name* [**statistics** \| **verbose**]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
vlan-id1 [**to** *vlan-id2*]	Specifies a range of VLAN IDs. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only information about the VLAN specified by *vlan-id1* is displayed.	• The value of *vlan-id1* is an integer that ranges from 1 to 4094. • The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Parameter	Description	Value
statistics	Displays traffic statistics on interfaces in a specified VLAN. If traffic statistics is enabled in the VLAN view, the **display vlan** *vlan-id* **statistics** command can be used to view VLAN traffic statistics.	-
slot *slot-id*	Displays VLAN traffic statistics or summary in a specified slot.	The value is an integer and must be the slot ID of a running card.
summary	Displays summary of all VLANs.	-
verbose	Displays detailed information about a specified VLAN. If **verbose** is not specified, only brief information about the VLAN is displayed.	-
vlan-name *vlan-name*	Specifies a VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
port-info	Displays information about all interfaces in a specified VLAN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display vlan** command displays VLAN configuration or packet statistics on interfaces in a VLAN.

The **display vlan** *vlan-id* command displays the ports that actually take effect, and the **display vlan** *vlan-id* **verbose** command displays the configured ports.

Prerequisites

Before using the **display vlan** *vlan-id* **statistics** command, run the **statistic enable (vlan view)** command in the corresponding VLAN view to enable the traffic statistics function in the VLAN.

Precautions

If no parameter is specified, brief information about all VLANs is displayed.

Example

Display brief information about all VLANs.

```
<HUAWEI> display vlan
The total number of VLANs is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type    Ports
--------------------------------------------------------------------------------
1    common  UT:GE0/0/1(D)
9    common  TG:GE0/0/2(D)      Eth-Trunk1(D)
40   common

VID  Status  Property      MAC-LRN Statistics Description
--------------------------------------------------------------------------------
1    enable  default       enable  disable    VLAN 0001
9    enable  default       enable  disable    VLAN 0009
40   enable  default       enable  disable    VLAN 0040
```

Display detailed information about VLAN 100.

```
<HUAWEI> display vlan 100 verbose
* : Management-VLAN
---------------------
  VLAN ID                 : 100
  VLAN Name               :
  VLAN Type               : Common
  Description             : VLAN 0100
  Status                  : Enable
  Broadcast               : Enable
  MAC Learning            : Enable
  Smart MAC Learning      : Disable
  Current MAC Learning Result : Enable
  Statistics              : Disable
  Property                : Default
  VLAN State              : Down
  ----------------
  Tagged        Port: GigabitEthernet0/0/1
  ----------------
  Active  Tag   Port: GigabitEthernet0/0/1
-------------------
Interface           Physical
GigabitEthernet0/0/1                  DOWN
```

Display interface traffic statistics in VLAN 10 on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. If no interface is added to VLAN 10, **Slot** information is not displayed.

```
<HUAWEI> display vlan 10 statistics
 Total
 VLAN : 10
 -------------------------------------------------------------------------------
 Item                                      Packets                    Bytes
                                            pps                      bps
 -------------------------------------------------------------------------------
 Inbound                                         0                        0
                                            0                        0
 Outbound                                         0                        0
                                            0                        0
 -------------------------------------------------------------------------------
 Slot : 0                                                                            VLAN :
10
-------------------------------------------------------------------------------
Item                                      Packets
Bytes                                                                          pps
bps
-------------------------------------------------------------------------------
Inbound                                         0
0                                                                         0
0                                            Outbound                           0
0                                                                         0
0                                            -------------------------------------------------------------------------------
```

Display interface traffic statistics in VLAN 10 on other devices except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. If no interface is added to VLAN 10, **Slot** information is not displayed.

```
<HUAWEI> display vlan 10 statistics
 Total
 VLAN : 10
 -------------------------------------------------------------------------------
 Item                                      Packets                    Bytes
                                            pps                      bps
 -------------------------------------------------------------------------------
 Inbound                                         0                        -
                                            0                        -
 Outbound                                         0                        -
                                            0                        -
 Inbound unknown-unicast                              -                        -
                                            -                        -
 Inbound multicast                                    0                        -
                                            0                        -
 Inbound broadcast                                     0                        -
                                            0                        -
 Inbound drop                                     -                        -
                                            -                        -
 -------------------------------------------------------------------------------
 Inbound drop-percentage                             -                        -
 -------------------------------------------------------------------------------
 Slot : 0                                                                            VLAN :
10
-------------------------------------------------------------------------------
Item                                      Packets
Bytes                                                                          pps
bps
-------------------------------------------------------------------------------
Inbound                                         0
-                                                                         0
-                                            Outbound                           0
-                                                                         0
-                                            Inbound unknown-unicast                 -
-                                                                         -
-                                            Inbound multicast                  0
```

```
-                                                          0
-                                  Inbound broadcast               0
-                                                          0
-                                  Inbound drop                      -
-                                                          -
-
--------------------------------------------------------------------------------
Inbound drop-percentage                 -                    -
--------------------------------------------------------------------------------
```

Display summary of all VLANs.

```
<HUAWEI> display vlan summary
Static VLAN:
Total 3 static VLAN.
  1 9 to 10

Dynamic VLAN:
Total 0 dynamic VLAN.

Reserved VLAN:
Total 5 reserved VLAN.
  Rrpp reserved:
  3000 to 3001
  Sep reserved:
  3100

Stack-VLAN:   212 to 213
```

Display interface information of a specific VLAN.

```
<HUAWEI> display vlan 1 port-info
VLAN  Interface              PHY      Auto-Neg   Duplex  Bandwidth
1     GigabitEthernet0/0/1   UP       enable     full    1000M
1     GigabitEthernet0/0/2   DOWN     enable     full    1000M
1     GigabitEthernet0/0/3   DOWN     disable    full    1000M
```

Table 5-44 Description of the display vlan command output

Item	Description
VID, VLAN, or VLAN ID	ID of a VLAN.
Type or VLAN Type	Type of a VLAN: ● mux: principal VLAN used in the MUX VLAN function ● mux-sub: subordinate VLAN used in the MUX VLAN function ● super: super-VLAN used for VLAN aggregation ● sub: sub-VLAN used for VLAN aggregation ● Common: common VLAN ● *Common: management VLAN ● dynamic: dynamic VLAN
Ports	Interfaces in a VLAN.
VLAN Name	Name of a VLAN.
Description	Description of a VLAN.

Item	Description
Status	Status of a VLAN. The value is always **Enable**.
Broadcast	Whether the broadcast function is enabled in a VLAN: ● Disable: The broadcast function is disabled. ● Enable: The broadcast function is enabled.
MAC Learning/MAC-LRN	Whether MAC address learning is enabled: ● Disable: MAC address learning is disabled. ● Enable: MAC addresses learning is enabled.
Smart MAC Learning	Whether smart MAC address learning is enabled: ● Disable: Smart MAC address learning is disabled. ● Enable: Smart MAC addresses learning is enabled.
Current MAC Learning Result	MAC address learning result.
Statistics	Whether the traffic statistics function is enabled in a VLAN: ● Disable: Traffic statistics function is disabled. ● Enable: Traffic statistics function is enabled.
Property	Property of a VLAN: ● Default: default VLAN ● MulticastVlan: multicast VLAN ● UserVlan: user VLAN
VLAN State	Status of the VLAN: ● Up ● Down The status of a VLAN is determined by the status of member interfaces in the VLAN. A VLAN is Up only when at least one member interface in the VLAN is Up.
Tagged/Untagged Port	Interfaces that are manually added to a VLAN in tagged or untagged mode.
Active Tag/Active Untag Port	Active interfaces that join a VLAN in tagged or untagged mode.
Inbound	Total incoming traffic volume.
Outbound	Total outgoing traffic volume.
Inbound unknown-unicast	Number of incoming unknown unicast packets.

Item	Description
Inbound multicast	Number of incoming multicast packets.
Inbound broadcast	Number of incoming broadcast packets.
Inbound drop	Number of discarded incoming packets. **NOTE** For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, if the **statistic enable** command is configured in a VLAN and the **port discard tagged-packet** command is configured on an interface and the interface is configured to allow packets from the specified VLAN to pass through, this item does not take effect.
Inbound drop-percentage	Percentage of discarded incoming packets. **NOTE** For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, if the **statistic enable** command is configured in a VLAN and the **port discard tagged-packet** command is configured on an interface and the interface is configured to allow packets from the specified VLAN to pass through, this item does not take effect.
Static VLAN	VLANs that are created manually.
Dynamic VLAN	VLANs that are learned dynamically.
Reserved VLAN	VLANs that are reserved for certain functions.
Rrpp reserved	VLANs used by the Rapid Ring Protection Protocol (RRPP). This field is displayed only when RRPP is configured on the switch.
Sep reserved	VLANs used by the Smart Ethernet Protocol (SEP). This field is displayed only when SEP is configured on the switch.
Stack-VLAN	VLANs configured in a stack. This field is displayed only when the switch is in a stack.
Interface	The name and number of an interface. All interfaces are displayed in the alphabetical order.
PHY	The physical status of the interface, including: ● UP: The physical layer of this interface works properly. ● DOWN: The physical layer of this interface becomes faulty.

Item	Description
Auto-Neg	Indicates whether auto-negotiation is enabled on the interface. The value can be: - enable: indicates that the interface is enabled with auto-negotiation. - disable: indicates that the interface is disabled with auto-negotiation.
Duplex	Duplex mode of the interface: - half: The interface works in half-duplex mode. - full: The interface works in full-duplex mode. - auto: The interface works in auto-negotiation mode.
Bandwidth	Indicates the bandwidth of the interface.

5.3.15 interface vlanif

Function

The **interface vlanif** command creates a VLANIF interface and displays the VLANIF interface view.

The **undo interface vlanif** command deletes a VLANIF interface.

By default, VLANIF interfaces are not created.

Format

interface vlanif *vlan-id*

undo interface vlanif *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN that a VLANIF interface belongs to.	- S2710-SI/S5710-C-LI: 1 - S2700-SI/S2700-EI/S5710-X-LI: 8 - S2720-EI (V200R006C10, V200R009C00, V200R010C00): 8 - S2720-EI (V200R011C10, V200R012C00, V200R013C00, V200R019C00, V200R019C10): 1024 - S2730S-S: 1024 - S3700-SI/S3700-EI/S3700-HI/S5700-SI/S5700-EI: 256 - S5700-HI/S5730-SI/S5735S-H/S5736-S/S5730S-EI/S5720-EI/S5731-S/S5731S-S/S5710-HI/S5720I-SI/S5720-SI/S5720S-SI/S5720-LI/S5720S-LI/S6730-S/S6730S-S/S6720-LI/S6720S-LI/S6720-SI/S6720S-S/S6720S-SI/S6735-S/S6720-EI/S6720S-EI: 1024 - S5720-HI/S5730-HI/S5731-H/S5731S-H/S5732-H/S6720-HI/S6730-H/S6730S-H: 1024 in versions earlier than V200R019C10 and 4096 in V200R019C10 and later versions - S5735-L/S5735S-L/S5735S-L-M/S5735-S/S5735-S-I/S5735S-S: 1019 in versions earlier than V200R019C10 and

Parameter	Description	Value
		1024 in V200R019C10 and later versions - S5735-L-I/S5735-L1/S5735S-L1/S500/S300: 1024 **NOTE** On the S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L1, S5735-L-I and S5735S-L1 running V200R020C10 or a later version, if the resource allocation mode is set to **enhanced-mac**, a maximum of eight VLANIF interfaces can be configured. - S2750-EI/S5700-LI/S5700S-LI: 1 in versions earlier than V200R005 and 8 in V200R005 and later versions - S5710-EI/S6700-EI: 256 in versions earlier than V200R005 and 1024 in V200R005

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device needs to communicate with devices at the network layer, you can create a logical interface based on a VLAN on the device, namely, a VLANIF interface. A VLANIF interface is a network layer interface and can be configured with an IP address. The device then users the VLANIF interface to communicate with devices at the network layer.

Follow-up Procedure

Run the **ip address** to assign an IP address to the VLANIF interface.

Precautions

- A VLANIF interface goes Up only after the following conditions are met:
  - The corresponding VLAN must have been created.
  - A physical interface or Eth-Trunk in Up state has been added to the corresponding VLAN.
- After a VLANIF interface is configured, the corresponding VLAN cannot be configured as a VLAN for Dot1q termination sub-interfaces or an outer VLAN for QinQ termination sub-interfaces.
- If the specified VLANIF interface exists, the **interface vlanif** command displays the VLANIF interface view directly.
- When a VLANIF interface is used as a management VLANIF interface where you can telnet to the device, the user VLAN ID cannot be the same as the management VLAN ID; otherwise, you will fail to telnet to the device.
- For the S500, S5735-S, S300, S5735-L, S5735S-L, S5735-S-I, S5735S-L-M, S5735S-S, S5735-L-I, S5735-L1,and S5735S-L1, if the resource allocation mode is set to **enhanced-mac** using the **assign resource-mode enhanced-mac global** command, a maximum of eight VLANIF interfaces can be created; if the device has already more than eight VLANIF interfaces configured, after the **enhanced-mac** resource allocation mode is configured, only the eight VLANIF interfaces with the smallest VLAN IDs are reserved.

Example

Create VLANIF 2 and enter the VLANIF interface view.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2]
```

5.3.16 ip-subnet-vlan

Function

Using the **ip-subnet-vlan** command, you can associate an IP subnet with a VLAN.

Using the **undo ip-subnet-vlan** command, you can disassociate an IP subnet from a VLAN.

By default, a VLAN is not associated with any IP subnet.

Format

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* { *mask* | *mask-length* } [**priority** *priority*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

Parameters

Parameter	Description	Value
ip-subnet-index	Specifies the index of an IP subnet. It can be set manually or automatically generated by the system according to the order in which IP subnets were associated with a VLAN.	The value is an integer that ranges from 1 to 12.
ip *ip-address* { *mask* | *mask-length* }	Specifies the source IP address or network segment associated with a VLAN. - *ip-address* specifies the source IP address or IP subnet. - *mask* specifies the subnet mask. - *mask-length* specifies the mask length.	- *ip-address* is in dotted decimal notation. - *mask* is in dotted decimal notation. - *mask-length* is an integer that ranges from 0 to 32.
priority *priority*	Specifies the 802.1p priority of the VLAN associated with an IP address or subnet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.
to *ip-subnet-end*	Specifies the end subnet index.	The value is an integer that ranges from 1 to 12 and must be greater than or equal to *ip-subnet-index*.
all	Disassociates all the IP subnets from a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip-subnet-vlan** command associates IP subnets with VLANs so that packets from different subnets are transmitted in different VLANs. On a network, if only one service is deployed on each subnet, you can associate IP subnets with VLANs to simplify VLAN configuration. In addition, you can add, modify, and move users on subnets without changing the VLAN configuration.

Follow-up Procedure

Add an interface to the VLAN and enable IP subnet-based VLAN assignment on the interface.

Precautions

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI, when the **ip error-packet-check disable** command is used to disable IP packet check, IP subnet-based VLAN assignment and policy-based VLAN assignment do not take effect.

If you run the **ip-subnet-vlan** command multiple times in the same VLAN view, all the specified IP subnets are associated with the VLAN.

NOTE

- The control VLAN of an RRPP ring cannot be associated with IP subnets.
- The IP subnet or the IP address associated with a VLAN cannot be a multicast network segment or multicast address.

Example

Associate VLAN 3 with network segment 10.10.10.0/24 so that the packets originated from this segment can be transmitted in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] vlan 3
[HUAWEI-vlan3] ip-subnet-vlan ip 10.10.10.0 255.255.255.0
```

5.3.17 ip-subnet-vlan enable

Function

The **ip-subnet-vlan enable** command enables IP subnet-based VLAN assignment on an interface.

The **undo ip-subnet-vlan enable** command disables IP subnet-based VLAN assignment on an interface.

By default, IP subnet-based VLAN assignment is disabled on an interface.

Format

ip-subnet-vlan enable

undo ip-subnet-vlan enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP subnets can be associated with VLANs so that packets from different subnets are transmitted in different VLANs. On a network, if only one service is deployed on each subnet, you can associate IP subnets with VLANs to simplify VLAN configuration. In addition, you can add, modify, and move users on subnets without changing the VLAN configuration.

If IP subnet-based VLAN assignment is enabled on an interface:

- When receiving an untagged packet, the interface searches for the VLAN entry matching the source IP address of the packet. If a matching entry is found, the interface forwards the packet based on the matching VLAN ID and priority. If no matching entry is found, the interface uses other matching rules to forward the packet.
- When receiving a tagged packet, the interface forwards the packet based on the port-based VLAN configuration.

Precautions

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI, when the **ip error-packet-check disable** command is used to disable IP packet check, IP subnet-based VLAN assignment and policy-based VLAN assignment do not take effect.

On access and trunk interfaces, IP subnet-based VLAN assignment can be used only when the IP subnet-based VLAN is the same as the PVID. It is recommended that IP subnet-based VLAN assignment be configured on hybrid interfaces.

When multiple VLAN assignment methods are configured on the device, the device assigns VLANs based on priorities of these methods.

Example

Enable IP subnet-based VLAN assignment.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] ip-subnet-vlan enable
```

5.3.18 lnp disable

Function

The **lnp disable** command disables LNP negotiation on a device.

The **undo lnp disable** command enables LNP negotiation on a device.

By default, LNP negotiation is enabled on all interfaces of a device.

Format

lnp disable

undo lnp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If an LNP-capable Layer 2 device is connected to an LNP-incapable Layer 2 device, the LNP-capable device keeps sending LNP packets, wasting bandwidth resources. To disable LNP negotiation on all interfaces of a Layer 2 device, run the **lnp disable** or **undo lnp enable** command.

To disable LNP negotiation on a Layer 2 Ethernet interface, run the **port negotiation disable** command in the interface view.

Precautions

- When the switch is upgraded from an earlier version of V200R005C00 to V200R005C00 or later, the link type auto-negotiation function is automatically disabled globally.
- By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If you run the **lnp disable** command in the system view to disable LNP negotiation on all interfaces of a Layer 2 device. LNP negotiation cannot be enabled on a Layer 2 Ethernet interface by running the **undo port negotiation disable** command in the interface view.
- The **lnp disable** command has no impact on services before the device restarts. However, after the device restarts, Layer 2 forwarding can be performed only for the manually configured VLANs. The **port default vlan 1**

command is configured by default, so only packets of VLAN 1 can be forwarded at Layer 2.

- For LNP negotiation to take effect, LNP negotiation must be enabled on both the device and Layer 2 Ethernet interfaces.
- This command is not supported in NETCONF mode.

Example

Disable LNP negotiation on a device.

```
<HUAWEI> system-view
[HUAWEI] lnp disable
```

5.3.19 mac-learning smart vlan enable

Function

The **mac-learning smart vlan enable** command enables flexible MAC address learning in a specified VLAN.

The **undo mac-learning smart vlan enable** command disables flexible MAC address learning in a specified VLAN.

By default, flexible MAC address learning is disabled in a VLAN.

Format

mac-learning smart vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **enable**

undo mac-learning smart vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **enable**

Parameters

Parameter	Description	Value
vlan-id1	Specifies the start VLAN ID.	The value is an integer ranging from 1 to 4094.
to *vlan-id2*	Specifies the end VLAN ID.	The value is an integer ranging from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enterprises usually adopt the ring or tree network topology to construct enterprise networks. Both network topologies require that devices at the convergence layer be able to learn a large number of MAC addresses in the case of enormous number of attached users.

As the number of attached users keeps growing, the specification of MAC entries supported by the devices cannot meet the need. As a result, MAC addresses of some users cannot be learned, and the packets of these users are broadcast in the VLAN, wasting network bandwidth and affecting the network performance.

To prevent the preceding problem, you can run the **mac-learning smart vlan enable** command in the system view to enable flexible MAC address learning in a VLAN. When less than three interfaces in the VLAN are Up, the system automatically disables MAC address learning in the VLAN, avoiding unnecessary resource consumption due to MAC address learning.

Prerequisites

The command takes effect only when the following operations are complete.

1. Run the **vlan** command to create a VLAN. If the device supports the dynamic VLAN function, you do not need to run the **vlan** command to create the VLAN.
2. Run the **undo mac-address learning disable** command in the VLAN view to enable MAC address learning.

Precautions

The system will delete the MAC entries after enabling flexible MAC address learning in the specified VLAN. When the number of Up interfaces in the VLAN exceeds 2, the system automatically enables MAC address learning in the VLAN. If a VLAN is configured as a MUX VLAN or is used as the outer VLAN in VLAN stacking or VLAN mapping configuration, flexible MAC address learning does not take effect in the VLAN.

If the **mac-learning smart vlan** command is run more than once, all configurations take effect.

Example

Configure the system to automatically disable MAC address learning in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] undo mac-learning smart vlan 10 enable
```

5.3.20 mac-vlan enable

Function

The **mac-vlan enable** command enables MAC address-based VLAN assignment on an interface.

The **undo mac-vlan enable** command disables MAC address-based VLAN assignment on an interface.

By default, MAC address-based VLAN assignment is disabled on an interface.

Format

mac-vlan enable

undo mac-vlan enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If user devices move frequently on a network, you can use the **mac-vlan mac-address** command to associate MAC addresses with VLANs. When a user moves, you do not need to assign a VLAN to the user again. This improves security and access flexibility on the network. To enable an interface to forward packets based on associations between MAC addresses and VLANs, you must run the **mac-vlan enable** command to enable MAC address-based assignment on the interface.

If MAC address-based assignment is enabled on an interface:

- When receiving an untagged packet, the interface searches for the VLAN entry matching the source MAC address of the packet. If a matching entry is found, the interface forwards the packet using the VLAN ID and priority in the entry. If no matching entry is found, the interface uses other matching rules to forward the packet.
- When receiving a tagged packet, the interface forwards the packet based on the port-based VLAN configuration.

Precautions

On access and trunk interfaces, MAC address-based VLAN assignment can be used only when the MAC address-based VLAN is the same as the PVID. It is recommended that MAC address-based VLAN assignment be configured on hybrid interfaces.

The MUX VLAN function and MAC address-based VLAN assignment cannot be enabled on the same interface.

MAC address-based VLAN assignment and MAC address authentication cannot be enabled on the same interface.

When multiple VLAN assignment methods are configured on the switch, the switch assigns VLANs based on priorities of these methods.

MAC address-based VLAN assignment on an interface and NAC conflict on an interface; therefore, the **mac-vlan enable** and **mac-authen**, **dot1x enable**, **web-auth-server** or **authentication-profile** commands cannot be used on the same interface.

Example

Enable MAC address-based VLAN assignment on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] mac-vlan enable
```

5.3.21 mac-vlan mac-address

Function

The **mac-vlan mac-address** command associates a MAC address with a VLAN.

The **undo mac-vlan mac-address** command cancels the association between MAC addresses and VLANs.

By default, the MAC addresses are not associated with VLANs.

Format

mac-vlan mac-address *mac-address* [*mac-address-mask* | *mac-address-mask-length*] [**priority** *priority*]

undo mac-vlan mac-address { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] }

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address to be associated with a VLAN.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter less than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or a multicast MAC address.
mac-address-mask	Specifies the mask of a MAC address.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. The default value is FFFF-FFFF-FFFF.

Parameter	Description	Value
mac-address-mask-length	Specifies the length of a MAC address mask.	The value is an integer that ranges from 1 to 48. The default value is 48.
priority *priority*	Specifies the 802.1p priority of the VLAN to be associated with a MAC address.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.
all	Specifies all the MAC addresses associated with a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If user devices move frequently on a network, you can use the **mac-vlan mac-address** command to associate MAC addresses with VLANs. The switch then assigns VLANs to packets based on source MAC addresses of packets. Before forwarding a packet, the switch tags the packet with the VLAN associated with the source MAC address. When a user device moves, you do not need to assign a VLAN to the user device again. This improves security and access flexibility on the network.

You can specify the 802.1p priority of the VLAN to be associated with the specific MAC address. In this manner, when the switching device is congested, the switching device preferentially sends frames with high priorities.

Follow-up Procedure

Add an interface to the VLAN and enable MAC address-based VLAN assignment on the interface.

Precautions

- When the **mac-vlan mac-address** command with the same MAC address specified is executed multiple times, MAC-VLAN entries take effect according to the longest match principle. On the S6735-S, S6720-EI and S6720S-EI, MAC-VLAN entries take effect according to the longest match principle only when the subnet mask has 47 bits or less than 47 bits. A MAC-VLAN entry with a 48-bit subnet mask has the lowest priority.
- After a MAC address is associated with a VLAN, it cannot be associated with other VLANs.

- If you run the **mac-vlan mac-address** command multiple times in the same VLAN view, all the specified MAC addresses are associated with the VLAN.
- The total number of MAC-VLAN entries is the number of configured MAC-VLAN entries multiplied by the number of interfaces where MAC-VLAN entries are delivered. On different models, the number of MAC-VLAN entries is different:
  - The S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support a maximum of 1024 MAC-VLAN entries and a maximum of 64 MAC-VLAN entries with the mask.
  - The SS1720GW-E, S1720GWR-E, S500S5720S-LI, S5735S-H, S5736-S, S6720S-S, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, and S5735S-L-M support a maximum of 512 MAC-VLAN entries and a maximum of 64 MAC-VLAN entries with the mask.
  - Other models support a maximum of 512 MAC-VLAN entries and a maximum of 32 MAC-VLAN entries with the mask.

Example

Associate MAC address 22-33-44 with VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-vlan mac-address 22-33-44
```

5.3.22 management-vlan

Function

Using the **management-vlan** command, you can configure a VLAN as a management VLAN.

Using the **undo management-vlan** command, you can cancel the configuration.

By default, no VLAN is configured as a management VLAN.

Format

management-vlan

undo management-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a network management system to manage multiple devices, create a VLANIF interface on each device and configure a management IP address for the VLANIF interface. You can then log in to a device and manage it using its management IP address. If a user-side interface is added to the VLAN, users connected to the interface can also log in to the device. This brings security risks to the device.

After a VLAN is configured as a management VLAN, no access interface or dot1q-tunnel interface can be added to the VLAN. An access interface or a dot1q-tunnel interface is connected to users. The management VLAN forbids users connected to access and dot1q-tunnel interfaces to log in to the device, improving device performance.

Follow-up Procedure

Create a VLANIF interface corresponding to the VLAN and configure a management IP address on the VLANIF interface.

Precautions

VLAN 1 cannot be configured as a management VLAN.

You can run the **display vlan** command to view the management VLAN configuration. In the command output, the VLAN marked with a * is the management VLAN.

After a VLAN is configured as a management VLAN, only trunk and hybrid interfaces can be added to the VLAN.

VCMP will be disabled if a managedment VLAN is configured.

Example

Configure VLAN 100 as a management VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] management-vlan
```

5.3.23 name (VLAN view)

Function

The **name** command configures a name for a VLAN.

The **undo name** command deletes a configured VLAN name.

By default, a VLAN does not have a name.

Format

name *vlan-name*

undo name

Parameters

Parameter	Description	Value
vlan-name	Specifies the VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

If a device is configured with multiple VLANs for transmitting different services, you can name the VLANs in their corresponding VLAN views to facilitate service management. In this manner, you can check the deployed services of a VLAN by the VLAN name.

After VLANs are named, you can run the **vlan vlan-name** command in the system view to enter the view of a specific VLAN, and then check or modify the configuration of the VLAN.

Example

Create VLAN 2, which is used to transmit voice services, and name it as voice.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] name voice
```

5.3.24 ping mac

Function

The **ping mac** command enables the system to monitor connectivity between the local device and the destination device. This detection is called GMAC ping.

Format

ping mac *mac-address* **vlan** *vlan-id* [**interface** *interface-type interface-number* | **-c** *count* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of the destination node. An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	The destination node can be a MEP or a MIP. The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies the outbound interface on the local device for sending ping packets. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is specified and the interface is in the specified VLAN, the device sends ping packets through the interface. If this parameter is not specified, the device searches the MAC address table based on the specified destination MAC address and VLAN ID. ● If the forwarding entry is found, the device sends ping packets according to the entry. ● If the forwarding entry is not found, the device broadcasts ping packets in the VLAN.	-

Parameter	Description	Value
-c *count*	Specifies the number of ping attempts.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-s *packetsize*	Specifies the size of a ping packet. On the device running IEEE 802.1ag Draft 7, the value does not contain the length of the Layer 2 packet header. On the device running IEEE Standard 802.1ag-2007, the value is the size of a ping packet.	The value is an integer that ranges from 95 to 9000, in bytes. The default value is 95.
-t *timeout*	Specifies the timeout interval for waiting for a response packet.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
-p *priority-value*	Specifies the priority of ping packets.	The value is an integer that ranges from 0 to 7. The default value is 7.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To use GMAC ping to detect connectivity, use the **ping mac** command.

Prerequisites

GMAC ping has been enabled using the **ping mac enable** command.

Precautions

A MEP is not required to initiate GMAC ping. The destination node can be not a MEP or MIP. You can perform GMAC ping without configuring the MD, MA, or MEP on the source device, intermediate device, and destination device. You must specify the VLAN on which the destination node resides.

NOTE

The two devices must be configured with IEEE 802.1ag of the same version. If the local device is configured with IEEE 802.1ag Draft 7 and the peer device is configured with IEEE Standard 802.1ag-2007, the **ping mac** command does not take effect. That is, the local device cannot ping the peer device.

Example

Ping the device with the MAC address of 00e0-fc00-0204. Send two ping packets with the size of 112 bytes each. The device is in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] ping mac enable
[HUAWEI] ping mac 00e0-fc00-0204 vlan 10 -c 2 -s 112
Pinging 00e0-fc00-0204 with 112 bytes of data:
Reply from 00e0-fc00-0204: byte = 112 time = 9ms
Reply from 00e0-fc00-0204: byte = 112 time = 11ms
Packets: Sent = 2, Received = 2, Lost = 0 (0% Loss)
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 5-45 Description of the ping mac command output

Item	Description
Reply from 00e0-fc00-0204: byte = 112 time = 9ms	Size and response time of ping packets returned from the destination device. When the response time is less than 1 ms, "time < 1ms" is displayed.
Packets: Sent = 2, Received = 2, Lost = 0 (0% Loss)	Number of sent ping packets, number of received reply packets, and number and percentage of discarded packets.
Minimum	Minimum round-trip time (RTT).
Maximum	Maximum RTT.
Average	Average RTT.

5.3.25 ping mac enable

Function

The **ping mac enable** command enables GMAC ping.

The **undo ping mac enable** command disables GMAC ping.

By default, GMAC ping is disabled.

Format

ping mac enable

undo ping mac enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement the following functions, use the **ping mac enable** command:

- Implement GMAC ping.
- Enable the device to respond to received GMAC ping packets.

Example

Enable GMAC ping.

```
<HUAWEI> system-view
[HUAWEI] ping mac enable
```

5.3.26 policy-vlan

Function

The **policy-vlan** command configures policy-based VLAN assignment by associating a MAC address and IP address binding policy to a VLAN and setting the 802.1p priority of the VLAN.

The **undo policy-vlan** command disassociates a MAC address and IP address binding policy from a VLAN.

By default, a VLAN is not associated with any MAC address and IP address binding policy.

Format

policy-vlan mac-address *mac-address* **ip** *ip-address* [**interface** *interface-type interface-number*] [**priority** *priority*]

undo policy-vlan { **all** | **mac-address** *mac-address* **ip** *ip-address* [**interface** *interface-type interface-number*] }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the source MAC address associated with a VLAN.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter fewer than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or a multicast MAC address.
ip *ip-address*	Specifies the IP address associated with a VLAN.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the interface where the MAC address and IP address binding policy is applied. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. If this parameter is not specified, the binding policy is applied to all the interfaces in the VLAN. If this parameter is specified, the binding policy is applied to the specified interface.	-
priority *priority*	Specifies the 802.1p priority of the VLAN associated with the MAC address and IP address.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.
all	Disassociates all MAC address and IP address binding policies from a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Policy-based VLAN assignment is a method to assign VLANs based on source MAC addresses and IP addresses of packets. This method is applicable to networks where high security is required and user devices move frequently.

When receiving an untagged packet, an interface matches the source IP address and source MAC address of the packet with the entries in the policy-based VLAN table.

- If a matching entry is found, the interface forwards the packet based on the matching VLAN ID and priority.
- If no matching entry is found, the interface uses other matching rules to forward the packet.

Policy-based VLAN assignment takes effect only for untagged packets, whereas tagged packets are forwarded based on port-based VLANs.

Precautions

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI, when the **ip error-packet-check disable** command is used to disable IP packet check, IP subnet-based VLAN assignment and policy-based VLAN assignment do not take effect.

After a MAC address or IP address is associated with a VLAN, it cannot be associated with other VLANs.

If you run the **policy-vlan** command multiple times in the same VLAN view, all the specified IP addresses and MAC addresses are associated with the VLAN.

Example

Bind MAC address 0-1-1 and IP address 10.1.1.1 to VLAN 2, and set the 802.1p priority of the VLAN to 7.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] policy-vlan mac-address 0-1-1 ip 10.1.1.1 priority 7
```

5.3.27 port

Function

The **port** command configures a VLAN as the default VLAN of an interface and adds the interface to the VLAN.

The **undo port** command restores the default VLAN of an interface to the default setting.

By default, VLAN 1 is the default VLAN of all interfaces.

Format

port *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

undo port *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type { *interface-number1* [**to** *interface-number2*] }	Configures the default VLAN for multiple interfaces. • *interface-type* specifies the type of interfaces. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. The *interface-number1* and *interface-number2* parameters identify a range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. You can specify 10 interface ranges at one time.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from a user device are untagged, and frames sent from a remote device may also be untagged. However, the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

After the default VLAN is specified for an access interface or a QinQ interface, packets passing through the interface are processed as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN ID.
- When the interface receives a tagged packet:
  - If the interface is an access interface, it compares the VLAN ID of the packet with the default VLAN ID. If they are the same, the interface forwards the packets; otherwise, the interface discards the packets.
  - If the interface is a QinQ interface, it adds an outer tag with the default VLAN ID to the packet.
- Before forwarding tagged packets, access and QinQ interfaces remove VLAN tags from the packets.

Prerequisites

The link-type of specified interfaces cannot be hybrid or trunk before you run the **port** command.

Precautions

A super VLAN cannot be configured as the default VLAN of interfaces.

The **undo port** command deletes the default VLAN of the specified interfaces only if the current VLAN is the default VLAN of these interfaces.

If you run the **port** command multiple times in the same VLAN view, the VLAN is configured as the default VLAN of all the specified interfaces.

You can also run the **port default vlan** command in the interface view to configure the default VLAN for an interface. The two commands have the same function.

Example

Configure VLAN 3 as the default VLAN of interfaces GE0/0/1 to GE0/0/4.

```
<HUAWEI> system-view
[HUAWEI] vlan 3
[HUAWEI-vlan3] port gigabitethernet 0/0/1 to 0/0/4
```

5.3.28 port default vlan

Function

The **port default vlan** command configures the default VLAN of an interface and adds the interface to the VLAN.

The **undo port default vlan** command restores the default VLAN of an interface to the default setting.

By default, VLAN 1 is the default VLAN of all interfaces.

Format

port default vlan *vlan-id* [**step** *step-number* [**increased** | **decreased**]]

undo port default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the default VLAN.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
step *step-number* [**increased** | **decreased**]	Specifies that the interface added to an interface group can be bound to VLANs starting from the one identified by *vlan-id* in an ascending or descending order at a step specified by *step-number*. **increased** specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id* at a step specified by *step-number* to add the interfaces to the VLANs. Whereas **decreased** specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id* at a step specified by *step-number* to add the interfaces to the VLANs. For example, you can configure **increased**, and set *vlan-id* to 10 and *step-number* to 20 in the **port default vlan** command. After this configuration, interface 1 joins VLAN 10; interface 2 joins VLAN 30... By analogy, interface 10 joins VLAN 190. **NOTE** ● This parameter can only be used in the port group view. ● When using **step** and *vlan-id* in the command, ensure that all interfaces added to the VLAN are available. ● If this parameter is not specified, all interfaces in an interface group are added into the same VLAN, that is, VLAN *vlan-id*.	The value is an integer that ranges from 1 to 4093.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from a user device are untagged, and frames sent from a remote device may also be untagged. However, the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

After the default VLAN is specified for an access interface or a QinQ interface, packets passing through the interface are processed as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN tag.
- When the interface receives a tagged packet:
  - If the interface is an access interface, it compares the VLAN ID of the packet with the default VLAN ID. If they are the same, the interface forwards the packet; otherwise, the interface discards the packet.
  - If the interface is a QinQ interface, it adds an outer tag with the default VLAN ID to the packet.
- Before forwarding tagged packets, access and QinQ interfaces remove VLAN tags from the packets.

Prerequisites

The interface type is negotiation-desirable, negotiation-auto, access or QinQ. If not, run the **port link-type** command to change the interface type. The interface where **negotiation-desirable** or **negotiation-auto** is configured must be negotiated as an access interface so that the default VLAN configured by the **port default vlan** command takes effect.

Precautions

- If the ID of a nonexistent VLAN is configured as the PVID, VLAN 1 is added to the untagged packets. After the PVID is configured globally, the PVID of the interface is changed to the configured one.
- You can also run the **port** command in the VLAN view to configure the default VLAN of an interface. The two commands have the same function.
- A super VLAN cannot be configured as the default VLAN of interfaces.
- This command is invalid on a member interface of an Eth-Trunk.

- If you run the **port default vlan** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure VLAN 3 (an existing VLAN) as the default VLAN of GE0/0/1 (an access interface).

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 3
```

5.3.29 port discard tagged-packet

Function

The **port discard tagged-packet** command configures an interface to discard incoming tagged frames.

The **undo port discard tagged-packet** command configures an interface not to discard incoming tagged frames.

By default, an interface does not discard incoming tagged frames.

Format

port discard tagged-packet

undo port discard tagged-packet

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from user devices are untagged, so user-side interfaces on a switch should not receive tagged frames. If a user connects a switching device to a user-side interface without permission, the user-side interface may receive tagged frames. The **port discard tagged-packet** command enables the user-side interface to discard untagged frames, preventing unauthorized access.

Precautions

The **port discard tagged-packet** command cannot function when dot1q-tunnel interfaces are configured on switches except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Use this command only on interfaces connected to user devices. If you run this command on a network-side interface, users in the same VLAN may fail to communicate.

Example

Configure GE0/0/1 to discard incoming tagged frames.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port discard tagged-packet
```

5.3.30 port hybrid pvid vlan

Function

The **port hybrid pvid vlan** command specifies the default VLAN ID of a hybrid interface.

The **undo port hybrid pvid vlan** command restores the default VLAN ID of a hybrid interface to the default setting.

By default, VLAN 1 is the default VLAN ID of all interfaces.

Format

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a hybrid interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface may receive untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

A hybrid interface processes Ethernet frames as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN ID. If the default VLAN ID is allowed by the interface, the interface accepts the frame. Otherwise, the interface discards the frame.
- When the interface receives a tagged frame, it accepts the frame if the VLAN ID of the frame is in the list of allowed VLAN IDs. Otherwise, the interface discards the frame.
- If the VLAN ID of a frame is allowed by the interface, the interface forwards the frame.

Prerequisites

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

- If the ID of a nonexistent VLAN is configured as the PVID, VLAN 1 is added to the untagged packets. After the PVID is configured globally, the PVID of the interface is changed to the configured one.
- This command is invalid on a member interface of an Eth-Trunk.
- The **port hybrid pvid vlan** command only specifies the default VLAN for an interface but does not add the interface to the default VLAN.
- If you run the **port hybrid pvid vlan** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Specify VLAN 5 as the default VLAN of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid pvid vlan 5
```

5.3.31 port hybrid tagged vlan

Function

The **port hybrid tagged vlan** command adds a hybrid interface to the specified VLANs. Frames of the VLANs then pass through the hybrid interface in tagged mode.

The **undo port hybrid vlan** command removes a hybrid interface from the specified VLANs.

By default, a hybrid interface is added to VLAN 1 in untagged mode.

Format

port hybrid tagged vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port hybrid [**tagged**] **vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view) **port hybrid tagged vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view) **undo port hybrid vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a hybrid interface to specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a hybrid interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port hybrid tagged vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.

Parameter	Description	Value
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hybrid interface can connect to either a user device or a switch. This command adds a hybrid interface to VLANs in tagged mode so that the hybrid interface allows frames from the VLANs to pass.

After a hybrid interface is added to VLANs in tagged mode, the interface forwards frames without removing VLAN tags of frames.

Prerequisites

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

- This command is invalid on a member interface of an Eth-Trunk.
- A super VLAN cannot be specified in the command.
- If you run the **port hybrid tagged vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.
- Running the **undo port hybrid tagged vlan** command on a hybrid interface removes the interface from specific VLANs it joins using the **port hybrid tagged vlan** command.

Example

Add GE0/0/1 to VLAN 3 to VLAN 5 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 3 to 5
```

5.3.32 port hybrid untagged vlan

Function

The **port hybrid untagged vlan** command adds a hybrid interface to the specified VLANs. Frames of the VLANs then pass through the hybrid interface in untagged mode.

The **undo port hybrid vlan** command removes a hybrid interface from the specified VLANs.

By default, a hybrid interface is added to VLAN 1 in untagged mode.

Format

port hybrid untagged vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port hybrid [**untagged**] **vlan**{ { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view) **port hybrid untagged vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view) **undo port hybrid vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a hybrid interface to specified VLANs. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a hybrid interface to all VLANs.	-

Parameter	Description	Value
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port hybrid untagged vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.

Parameter	Description	Value
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hybrid interface can connect to either a user device or a switch. When a hybrid interface is connected to a user device, it must be added to VLANs in untagged mode so that it sends untagged frames. When a hybrid interface is connected to a switch, it can receive and forward frames with the same VLAN tag (in the tagged VLAN or untagged VLAN list) from the switch.

After a hybrid interface is added to VLANs in untagged mode, the interface removes VLAN tags of frames before sending frames.

Prerequisites

The link type of the interface has been changed to hybrid using the **port link-type hybrid** command.

Precautions

- This command is invalid on a member interface of an Eth-Trunk.
- A super VLAN cannot be specified in the command.
- If you run the **port hybrid untagged vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

- Running the **undo port hybrid untagged vlan** command on a hybrid interface removes the interface from specific VLANs it joins using the **port hybrid untagged vlan** command.

Example

Add GE0/0/1 to VLAN 3 to VLAN 5 in untagged mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 3 to 5
```

5.3.33 port hybrid vlan 1

Function

The **port hybrid vlan 1** command adds a Hybrid port to VLAN 1 in untagged mode.

The **undo port hybrid vlan 1** command deletes a Hybrid port from VLAN 1.

Format

port hybrid vlan 1

undo port hybrid vlan 1

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All interfaces on the device join VLAN 1 by default, and the hybrid interface joins VLAN 1 in untagged mode by default. When there are unknown unicast packets, multicast packets, or broadcast packets of VLAN 1, broadcast storms may occur. For the hybrid interface that does not need to join VLAN 1, you need to run the **undo port hybrid vlan 1** command to delete the hybrid interface from VLAN 1 to prevent loops. When the network changes and the hybrid interface needs to join VLAN 1 in untagged mode, run the **port hybrid vlan 1** command.

Prerequisites

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

This command cannot be used for a physical interface that has been added to an Eth-Trunk interface.

Example

Add GE 0/0/1 to VLAN 1 in Untagged mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid vlan 1
```

5.3.34 port link-type

Function

The **port link-type** command sets the link type of an interface.

The **undo port link-type** command restores the default link type of an interface.

By default, the link type of an interface on the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, S6720S-S is **negotiation-auto**, and the link type of an interface on other models is **negotiation-desirable**.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support VE interfaces. You can configure the link type for a VE interface only after the VE interface is switched to Layer 2 mode using the **portswitch** command. The default link type is hybrid.

Format

port link-type { **access** | **dot1q-tunnel** | **hybrid** | **trunk** | **negotiation-desirable** | **negotiation-auto** }

undo port link-type

Parameters

Parameter	Description	Value
access	Sets the link type of an interface to access.	-
dot1q-tunnel	Sets the link type of an interface to QinQ.	-
hybrid	Sets the link type of an interface to hybrid.	-

Parameter	Description	Value
trunk	Sets the link type of an interface to trunk.	-
negotiation-desirable	Sets LNP negotiation mode for a Layer 2 Ethernet interface to negotiation-desirable. **NOTE** This parameter is not supported in the VE interface view.	-
negotiation-auto	Sets the LNP negotiation mode for a Layer 2 Ethernet interface to negotiation-auto. **NOTE** This parameter is not supported in the VE interface view.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Access, hybrid, trunk, and dot1q-tunnel link types are statically configured, and the LNP negotiation mode of **negotiation-desirable** or **negotiation-auto** is dynamically negotiated. The interface where **negotiation-desirable** or **negotiation-auto** is configured is negotiated as the access or trunk interface.

Characteristics of different interfaces are:

- An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. If the default VLAN is configured for an access interface, the interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the default VLAN ID. The access link transmits only the packets with the default VLAN ID.
- A trunk interface connects to a switch and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.

- A hybrid interface can connect to either a user device or a switch, and it can connect to an access link or a trunk link. A hybrid interface allows frames from multiple VLANs to pass and can remove VLAN tags of outgoing frames.
- A QinQ interface connects to a switch and can process double-tagged frames.
- The interface configured with **negotiation-desirable** can actively send negotiation packets, while the interface configured with **negotiation-auto** cannot actively send negotiation packets. The interface where **negotiation-desirable** or **negotiation-auto** is configured is negotiated as the access or trunk interface through LNP and added to a VLAN. **Table 5-46** describes the negotiation result when the local and remote ends use different negotiation modes.

Table 5-46 LNP negotiation

Local LNP Negotiation Mode	Remote Link Type or LNP Negotiation Mode	Locally Negotiated Link Type	Remotely Negotiated Link Type	Link Type When Negotiation Fails
negotiation-desirable/ negotiation-auto	Access (negotiate on)	Access	Access	Access
	Hybrid (negotiate on)	Trunk	Hybrid	Access
	Dot1q-tunnel (negotiate on)	Access	Dot1q-tunnel	Access
	Trunk (negotiate on)	Trunk	Trunk	Access
	LNP negotiation not supported or negotiate off	Access	N/A	Access
negotiation-desirable	negotiation-desirable	Trunk	Trunk	Access
negotiation-desirable	negotiation-desirable	Trunk	Trunk	Access
negotiation-auto	negotiation-desirable	Access	Access	Access

negotiate on: LNP negotiation is enabled. negotiate off: LNP negotiation is disabled. N/A: The link type is uncertain.

Prerequisites

LNP has been enabled.

Follow-up Procedure

Add the interface to VLANs.

Precautions

This command is invalid on a member interface of an Eth-Trunk.

Starting from V200R005C00, the default link type of an interface is not hybrid. Before upgrading the device of an earlier version of V200R005C00 to V200R005C00 or later, the **port link-type hybrid** command configuration is generated.

If you run the **port link-type** command multiple times in the same interface view, only the latest configuration takes effect.

After VLAN-related configurations are configured on an interface, the **[undo] port link-type** command is an interactive command. You need to enter confirmation information.

When using LNP negotiation, pay attention to the following points:

- If a Layer 2 Ethernet interface is Down, it does not participate in LNP negotiation.
- If the two ends of an Eth-Trunk link have different numbers of member interfaces, LNP negotiation may fail.
- If the link type of the Layer 2 Ethernet interface is configured as access, hybrid, trunk, or dot1q-tunnel using the **port link-type** command, LNP does not take effect on the interface.
- The interface configured with **negotiation-desirable** or **negotiation-auto** is negotiated as an access or trunk interface. By default, the negotiated access interface joins VLAN 1, and the negotiated trunk interface allows all VLANs and uses default VLAN 1. **port default vlan** and **port trunk allow-pass only-vlan** can be simultaneously used on the interface configured with **negotiation-desirable** or **negotiation-auto**. If the interface is negotiated as an access interface, **port default vlan** takes effect. If the interface is negotiated as a trunk interface, **port trunk allow-pass only-vlan** takes effect.

Before changing the link type of an interface, you do not need to restore the default VLAN configuration. However, if the link type of the interface is changed, the VLAN configuration of the interface is deleted. Exercise caution when you perform this configuration.

There are limitations on the interface where **negotiation-desirable** or **negotiation-auto** is configured:

- The sub-interface cannot be created.
- No MUX VLAN can be enabled.
- No voice VLAN in auto mode can be configured.

Dot1q-tunnel interfaces do not support the voice VLAN function.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after the **port link-type dot1q-tunnel** command is run on an interface, IP packets cannot be forwarded on the interface.

If the device works in VBST mode, changing the link type of an interface may cause a loop on the network, resulting in a traffic storm. If the link type of an interface must be changed, disable the interfaces on both ends and then change the link type of these interfaces.

Example

Set the link type of GE0/0/1 to trunk.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
```

5.3.35 port negotiation disable

Function

The **port negotiation disable** command disables LNP negotiation on a Layer 2 Ethernet interface.

The **undo port negotiation disable** command enables LNP negotiation on a Layer 2 Ethernet interface.

By default, LNP negotiation is enabled on a Layer 2 Ethernet interface.

Format

port negotiation disable

undo port negotiation disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If an LNP-capable Layer 2 device is connected to an LNP-incapable Layer 2 device, the LNP-capable device keeps sending LNP packets, wasting bandwidth resources. In this situation, you can run the **port negotiation disable** command to disable LNP negotiation on the Layer 2 Ethernet interface connected to the LNP-incapable Layer 2 device.

To disable LNP negotiation on all interfaces of a Layer 2 device, run the **lnp disable** command in the system view.

Prerequisites

The interface must be a layer 2 interface before using the **port negotiation disable** command. Use the **portswitch** command to switch a layer 3 interface to a Layer 2 interface.

Precautions

By default, LNP negotiation is enabled for all interfaces on a Layer 2 device. If you run the **lnp disable** command in the system view to disable LNP negotiation on all interfaces of a Layer 2 device. LNP negotiation cannot be enabled on a Layer 2 Ethernet interface by running the **undo port negotiation disable** command in the interface view.

For LNP negotiation to take effect, LNP negotiation must be enabled on both the device and Layer 2 Ethernet interfaces.

Example

Disable LNP negotiation on a Layer 2 Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port negotiation disable
```

5.3.36 port trunk allow-pass vlan

Function

The **port trunk allow-pass vlan** command adds a trunk interface to the specified VLANs.

The **undo port trunk allow-pass vlan** command deletes a trunk interface from the specified VLANs.

By default, a trunk interface is in VLAN 1.

Format

port trunk allow-pass vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port trunk allow-pass vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view) **port trunk allow-pass vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view) **undo port trunk allow-pass vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a trunk interface to specified VLANs. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a trunk interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port trunk allow-pass vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.

Parameter	Description	Value
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A trunk interface can join multiple VLANs and connects to a network device. To allow all packets from one or more VLANs to pass through a trunk interface, the trunk interface must be added to the VLANs using the **port trunk allow-pass vlan** command.

Prerequisites

The link type of the interface has been set to trunk or negotiation.

Precautions

If a specified VLAN does not exist, the configuration does not take effect.

The command cannot be used on a member interface of an Eth-Trunk.

If you run the **port trunk allow-pass vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

If a port is configured with a PVID VLAN, run the **port trunk allow-pass vlan** *pvid-vlan* command to add the PVID VLAN to the port.

Example

Add GE0/0/1 to VLANs 10 to 30.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 to 30
```

5.3.37 port trunk allow-pass only-vlan

Function

The **port trunk allow-pass only-vlan** command configures VLANs allowed by the interface that is configured as a trunk interface through LNP negotiation.

The **undo port trunk allow-pass only-vlan** command restores the default VLANs allowed by the interface that is configured as a trunk interface through LNP negotiation.

By default, if the Layer 2 Ethernet interface is negotiated as a trunk interface, the interface allows all VLANs.

Format

port trunk allow-pass only-vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **none** }

undo port trunk allow-pass only-vlan

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies VLANs on a Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation. ● *vlan-id1* specifies the first VLAN. ● **to** *vlan-id2* specifies the last VLAN. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* can be configured for the Layer 2 Ethernet interface. In one **port trunk allow-pass only-vlan** command, a maximum of 10 VLAN ranges can be specified using **to**.	The value is an integer ranging from 1 to 4094.

Parameter	Description	Value
none	Specifies that the Layer 2 Ethernet interface cannot forward packets for any VLAN after the LNP negotiation.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link-type Negotiation Protocol (LNP) dynamically negotiates the link type of an Ethernet interface. The negotiated link type can be access or trunk.

In routine maintenance, if the network administrator wants to update the VLANs on a Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation, perform the following operations in the corresponding interface view.

1. Run the **port trunk allow-pass vlan all** command to delete all VLANs from the Layer 2 Ethernet interface.
2. Run the **port trunk allow-pass only-vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **none** } to update VLANs on the Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation.

Alternatively, to simplify configurations and reduce the network administrator's maintenance workload, run the **port trunk allow-pass only-vlan** to update VLANs on the Layer 2 Ethernet interface so that the interface forwards only packets for these VLANs after LNP negotiation.

Prerequisites

The LNP function is supported on the Layer 2 Ethernet interface, and the Layer 2 Ethernet interface is configured to work in auto-negotiation mode using the **port link-type negotiation** command.

Example

Configure VLANs 10 to 20 on the interface so that the interface forwards only packets for these VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass only-vlan 10 to 20
```

5.3.38 port trunk pvid vlan

Function

The **port trunk pvid vlan** command specifies the default VLAN for a trunk interface.

The **undo port trunk pvid vlan** command restores the default VLAN of a trunk interface to the default setting.

By default, VLAN 1 is the default VLAN of trunk interfaces.

Format

port trunk pvid vlan *vlan-id*

undo port trunk pvid vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a trunk interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface may receive untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

Follow-up Procedure

Add the trunk interface to the default VLAN.

Precautions

- If the ID of a nonexistent VLAN is configured as the PVID, VLAN 1 is added to the untagged packets. After the PVID is configured globally, the PVID of the interface is changed to the configured one.

- The **port trunk pvid vlan** command only specifies the default VLAN of a trunk interface but does not add the trunk interface to the default VLAN. A trunk interface forwards frames with the default VLAN ID only after it is added to the default VLAN using the **port trunk allow-pass vlan** command.
- If you run the **port trunk pvid vlan** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Specify VLAN 5 as the default VLAN of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk pvid vlan 5
```

5.3.39 protocol-transparent

Function

Using the **protocol-transparent** command, you can enable transparent transmission of protocol packets in a VLAN.

Using the **undo protocol-transparent** command, you can disable transparent transmission of protocol packets in a VLAN.

By default, transparent transmission of protocol packets is disabled in a VLAN.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

protocol-transparent

undo protocol-transparent

Parameters

None

Views

VLAN view, VLAN-Range view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device used as the gateway or Layer 2 switches is enabled with snooping functions such as DHCP/IGMP/MLD snooping, the device needs to parse and process protocol packets such as ARP, DHCP, and IGMP packets. The interface sends protocol packets without differentiating VLANs. That is, if any of the preceding snooping functions are deployed, protocol packets from all VLANs are sent to the CPU for processing.

If the device is a gateway of some VLANs or snooping functions is deployed in some VLANs, the device does not need to process protocol packets in other VLANs. After the protocol packets in other VLANs are sent to the CPU, the CPU needs to forward them to other devices. This mechanism is called software forwarding. Software forwarding affects the forwarding speed and efficiency of protocol packets because protocol packets need to be processed.

To address this issue, deploy transparent transmission of protocol packets in VLANs where protocol packets do not need to be processed. This function enables the device to transparently transmit the protocol packets in the VLANs to other devices, which improves the forwarding speed and efficiency.

The switch can transparently transmit the following protocol packets: CFM/ARP/BFD/DHCP/DHCPV6/HTTP/IGMP/MLD/ND/PIM/PIMv6/PPPoE/TACACS.

Precautions

- Before running the **protocol-transparent** command, ensure that IGMP snooping or MLD snooping has been disabled in the VLAN. Otherwise, the configuration fails.
- After the **protocol-transparent** command is executed in a VLAN view, the switch does not participate in protocol calculation in this VLAN.

Example

Enable transparent transmission of protocol packets in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] protocol-transparent
```

Enable transparent transmission of protocol packets in VLAN 10 to 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 to 20
[HUAWEI] vlan range 10 to 20
[HUAWEI-vlan-range] protocol-transparent
```

5.3.40 protocol-vlan

Function

The **protocol-vlan** command associates a protocol with a VLAN.

The **undo protocol-vlan** command disassociates a protocol from a VLAN.

Format

protocol-vlan [*protocol-index*] { **at** | **ipv4** | **ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii-etype** *etype-id1* | **llc dsap** *dsap-id* **ssap** *ssap-id* | **snap-etype** *etype-id2* } }

undo protocol-vlan { **all** | *protocol-index1* [**to** *protocol-index2*] }

Parameters

Parameter	Description	Value
protocol-index	Specifies the index of a protocol. If no protocol index is set, the switch generates an index based on the order in which protocols were associated with a VLAN.	The value is an integer that ranges from 0 to 15. The value range varies according to the device type. ● S1720GW-E,S1720GWR-E,S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S: 0 to 11 ● S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: 0 to 7 ● other models: 0 to 15
at	Associates the AppleTalk protocol with a VLAN.	-
ipv4	Associates the IPv4 protocol with a VLAN.	-
ipv6	Associates the IPv6 protocol with a VLAN.	-
ipx	Associates the Internetwork Packet Exchange (IPX) protocol with a VLAN. The encapsulation type of IPX packets can be Ethernet II, Logical Link Control (LLC), raw, or Subnetwork Access Protocol (SNAP).	-
ethernetii	Indicates that the encapsulation format of Ethernet frames is Ethernet II.	-

Parameter	Description	Value
llc	Indicates that the encapsulation format of Ethernet frames is LLC.	-
raw	Indicates that the encapsulation format of Ethernet packets is raw.	-
snap	Indicates that the encapsulation format of Ethernet packets is SNAP.	-
mode	Indicates a user-defined protocol.	-
ethernetii-etype *etype-id1*	Specifies the protocol type ID that matches the Ethernet II encapsulation format.	The value ranges from 0x600 to ffff, excluding 800, 809b, 8137, and 86dd.
dsap *dsap-id*	Specifies the destination service access point.	The value ranges from 0x0 to ff.
ssap *ssap-id*	Specifies the source service access point.	The value ranges from 0x0 to ff.
snap-etype *etype-id2*	Specifies the protocol type ID that matches the SNAP encapsulation format.	The value ranges from 0x600 to ffff, excluding 800, 809b, 8137, and 86dd.
all	Disassociates all protocols from a VLAN.	-

Parameter	Description	Value
protocol-index1	Specifies the start protocol index.	The value is an integer that ranges from 0 to 15. The value range varies according to the device type. ● S1720GW-E,S1720GWR-E,S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S: 0 to 11 ● S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: 0 to 7 ● other models: 0 to 15
protocol-index2	Specifies the end protocol index.	The value of *protocol-index2* must be greater than or equal to the value of *protocol-index1*.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Protocol-based VLAN assignment is a method to associate protocols with VLANs. After a protocol is associated with a VLAN, packets of this protocol are transmitted in the associated VLAN. This function allows different protocol packets to be transmitted on different paths.

Follow-up Procedure

Add interfaces to the VLAN associated with protocols, and then associate the interfaces with the VLAN.

Precautions

The control VLAN of an RRPPor ERPS ring cannot be associated with protocols.

The AppleTalk, IPv4, and IPv6 protocols can be associated with VLANs directly. When associating other protocols with a VLAN, set the encapsulation format.

When specifying the source and destination service access points, pay attention to the following points:

- The *dsap-id* and *ssap-id* parameters cannot be set to 0xaa (indicating the SNAP encapsulation format) simultaneously.
- The *dsap-id* and *ssap-id* parameters cannot be set to 0xe0 (indicating the LLC encapsulation format) simultaneously.
- The *dsap-id* and *ssap-id* parameters cannot be set to 0xff (indicating the raw encapsulation format) simultaneously.

If you run the **protocol-vlan** command multiple times in the same VLAN view, all the specified protocols are associated with the VLAN.

Example

Associate IPv4 with VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] vlan 3
[HUAWEI-vlan3] protocol-vlan ipv4
```

5.3.41 protocol-vlan vlan

Function

The **protocol-vlan vlan** command associates an interface with a protocol-based VLAN.

The **undo protocol-vlan vlan** command disassociates an interface from a VLAN.

By default, an interface is not associated with any protocol-based VLAN.

Format

protocol-vlan vlan *vlan-id* { **all** | *protocol-index1* [**to** *protocol-index2*] } [**priority** *priority*]

undo protocol-vlan { **all** | **vlan** *vlan-id* { **all** | *protocol-index1* [**to** *protocol-index2*] } }

Parameters

Parameter	Description	Value
all	The **all** keywords in the command have different meanings: ● The one followed by *protocol-index1* indicates all protocols. ● The one followed by **vlan** indicates all protocol-based VLANs.	-
vlan *vlan-id*	Specifies the ID of a protocol-based VLAN.	The value is an integer that ranges from 1 to 4094.
protocol-index1 [**to** *protocol-index2*]	Specifies the start protocol index. If no protocol index is set, the switch generates an index based on the order in which protocols were associated with a VLAN.	The value is an integer that ranges from 0 to 15. The value range varies according to the device type. ● S1720GW-E,S1720GWR-E,S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S: 0 to 11 ● S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: 0 to 7 ● other models: 0 to 15
priority *priority*	Specifies the 802.1p priority of a VLAN.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The default value is 0.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Protocol-based VLAN assignment is a method to associate protocols with VLANs. After a protocol is associated with a VLAN, packets of this protocol are transmitted in the associated VLAN. This function allows different protocol packets to be transmitted on different paths.

After an interface is associated with a protocol-based VLAN:

- When receiving an untagged packet, the interface searches for the VLAN entry matching the protocol type of the packet. If a matching entry is found, the interface forwards the packet based on the matching VLAN ID and priority. If no matching entry is found, the interface uses other matching rules to forward the packet.
- When receiving a tagged packet, the interface forwards the packet based on the port-based VLAN configuration.

Prerequisites

The VLAN has been associated with a protocol using the **protocol-vlan** command.

Precautions

On access and trunk interfaces, protocol-based VLAN assignment can be used only when the protocol-based VLAN is the same as the PVID. It is recommended that protocol-based VLAN assignment be configured on hybrid interfaces.

After an interface is associated with a protocol-based VLAN, the switch checks the protocol type of a received packet and forwards the packet in the VLAN associated with the protocol.

Example

Associate GE0/0/1 with VLAN 2, which is associated with the protocol with index 0.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] protocol-vlan vlan 2 0
```

5.3.42 reset lnp statistics

Function

The **reset lnp statistics** command clears statistics on LNP packets.

Format

reset lnp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics on LNP packets on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect statistics about LNP packets for a specified period of time, run the **reset lnp statistics** command to clear existing statistics and allow the system to re-collect them.

Configuration Note

Cleared statistics on LNP packets cannot be restored. Exercise caution when running this command.

Example

Clear statistics about LNP packets.

```
<HUAWEI> reset lnp statistics interface gigabitethernet 0/0/1
```

5.3.43 reset vlan statistics

Function

Using the **reset vlan statistics** command, you can clear traffic statistics in a specified VLAN.

Format

reset vlan *vlan-id* **statistics**

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is used when you need to collect new packet statistics in a VLAN. After this command is executed, the packet count in the VLAN becomes 0.

Prerequisites

The traffic statistics function has been enabled in the VLAN by using the **statistic enable (VLAN view)** command.

Precautions

⚠ CAUTION

Traffic statistics cannot be restored after they are cleared. Exercise caution when you use the command.

Example

Clear traffic statistics in VLAN 3.

```
<HUAWEI> reset vlan 3 statistics
```

5.3.44 shutdown (VLANIF interface view)

Function

Using the **shutdown** command, you can shut down a VLANIF interface.

Using the **undo shutdown** command, you can enable a VLANIF interface.

By default, a VLANIF interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VLANIF interface fails or is not needed, you can run the **shutdown** command on the VLANIF interface.

Precautions

A VLANIF interface is Up as long as an interface in the corresponding VLAN is Up.

After the VLANIF interface is shut down, the interface status changes to Down even if physical interfaces in the corresponding VLAN are Up.

After a VLANIF interface is shut down, none of the users who use the VLANIF interface address as the gateway address can communicate at Layer 3. In addition, the VLANIF interface address cannot be used in route calculation.

After a VLANIF interface is shut down, the dynamic ARP entry corresponding to the VLANIF interface starts aging in the ARP table. If the VLANIF interface address is in a static ARP entry, the ARP entry is not deleted.

Example

Enable VLANIF 2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] undo shutdown
```

5.3.45 statistic enable (VLAN view)

Function

The **statistic enable** command enables the traffic statistics function in a VLAN.

The **undo statistic enable** command disables the traffic statistics function in a VLAN.

By default, the traffic statistics function is disabled in a VLAN.

Format

statistic enable

undo statistic enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable the traffic statistics function in a VLAN.

After the traffic statistics function is enabled in a VLAN, the device collects statistics on unicast packets, broadcast packets, and broadcast packets transmitted in the VLAN.

Precautions

- On different models, the number of VLANs where the traffic statistics function can be configured is different:
  - S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 256
  - S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S: 64
  - Other models: 16
- Traffic statistics are accumulative and cannot be cleared by the system. To clear traffic statistics in a VLAN, run the **reset vlan statistics** command in the VLAN.
- The traffic statistics function occupies system resources. If system resources are insufficient, the configuration may fail. Disable this function when traffic statistics do not need to be collected.
- After enabling the traffic statistics function in a VLAN, you can use the **display vlan** *vlan-id* **statistics** command to view traffic statistics in the VLAN.
- On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S if the traffic policy is bound to the traffic behavior containing traffic statistics and is applied to an interface in the inbound direction, and the **statistic enable** command is enabled in the VLAN that the interface joins, the **statistic enable** command cannot collect statistics on packets in the inbound direction of the interface.
- For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, configuring traffic statistics collection on VLANs and VLANIF interfaces may affect forwarding performance. For example, some packets may be discarded during line-rate forwarding on all ports. Configure this function if necessary.

Example

Enable the traffic statistics function in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] statistic enable
```

5.3.46 statistic enable (VLANIF interface view)

Function

The **statistic enable** command enables the traffic statistics function on a VLANIF interface.

The **undo statistic enable** command disables the traffic statistics function on a VLANIF interface.

By default, the traffic statistics function is disabled on a VLANIF interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

[**ipv4** | **ipv6**] * **statistic enable** { **both** | **inbound** | **outbound** }

undo [**ipv4** | **ipv6**] * **statistic enable** { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv4	Indicates IPv4 packet statistics collection.	-
ipv6	Indicates IPv6 packet statistics collection.	-
both	Enables the traffic statistics function for incoming and outgoing traffic.	-
inbound	Enables the traffic statistics function for incoming traffic.	-
outbound	Enables the traffic statistics function for outgoing traffic.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable the traffic statistics function on VLANIF interfaces. The switch then collects traffic statistics on the VLANIF interfaces.

Precautions

- On the S6735-S, S6720S-EI and S6720-EI, if the traffic statistics function is enabled in the VLAN corresponding to the VLANIF interface, the traffic statistics function is invalid on the VLANIF interface in the **outbound** direction.
- After you run the **undo statistic enable** command on a VLANIF interface, the switch stops collecting traffic statistics on the VLANIF interface, and the collected traffic statistics are deleted.
- The switch uses ACL resources when collecting traffic statistics. If the traffic statistics function is enabled on too many VLANIF interfaces, other services may fail to obtain ACL resources. The device supports traffic statistics on a maximum of 100 VLANIF interface.
- Traffic statistics on VLANIF interfaces is unavailable for error packets.
- On the VLANIF interface enabled with the traffic statistics function, the packets such as ping packets sent from the device cannot be counted.
- After enabling the traffic statistics function in a VLANIF, you can use the **display interface vlanif** command to view traffic statistics in the VLANIF.
- The traffic statistics function on VLANIF interfaces is unavailable for MPLS packets.
- A higher number of VLANIF interfaces configured with the traffic statistics function leads to higher CPU usage.
- For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, configuring traffic statistics collection on VLANs and VLANIF interfaces may affect forwarding performance. For example, some packets may be discarded during line-rate forwarding on all ports. Configure this function if necessary.

Example

Enable the traffic statistics function for incoming and outgoing traffic on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] statistic enable both
```

5.3.47 trace mac

Function

The **trace mac** command locates a link connectivity fault between the local device and the destination device. The operation is called GMAC trace.

Format

trace mac *mac-address* **vlan** *vlan-id* [**interface** *interface-type interface-number* | **-t** *timeout* | **-h**]*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of the destination node. The destination node can be a MEP or a MIP. An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
interface *interface-type* *interface-number*	Specifies the outbound interface on the local device for sending trace packets. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● If this parameter is specified, the device sends trace packets directly through the interface. ● If this parameter is not specified, the device searches the MAC address table based on the specified destination MAC address and VLAN ID. If the forwarding entry is found, the device sends trace packets according to the entry. If the forwarding entry is not found but there is one interface in the VLAN, the device sends trace packets from this interface. If there is more than one interface in the VLAN, the device discards trace packets directly.	-
-t *timeout*	Specifies the timeout interval for waiting for an LTR.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
-h	Specifies the host name and IP address of a device that an LTM passes through.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To perform GMAC trace, run this command.

Prerequisites

GMAC trace has been enabled using the **trace mac enable** command.

Precautions

A MEP is not required to initiate GMAC trace. The destination node can be not a MEP or MIP. That is, GMAC trace can be implemented without configuring the MD, MA, or MEP on the source device, intermediate device, and the destination device. All the intermediate devices can respond with an LTR.

NOTE

The two devices must be configured with IEEE 802.1ag of the same version. If the local device is configured with IEEE 802.1ag Draft 7 and the peer device is configured with IEEE Standard 802.1ag-2007, the **trace mac** command does not take effect. That is, the connectivity fault cannot be located.

-h is only supported by the device running IEEE Standard 802.1ag-2007.

Example

Trace the destination device with the MAC address as 00e0-fc12-3456. The device belongs to VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] trace mac enable
[HUAWEI] trace mac 00e0-fc12-3456 vlan 2
Tracing the route to 00e0-fc12-3456 over a maximum of 255 hops:
 Hops  Ingress MAC    Ingress Port              Ingress Action    Relay Action
       Egress MAC     Egress Port               Egress Action
 1     00e0-fc12-3456 GigabitEthernet0/0/1      IngOK             RlyHit
       --             --                        --
Info: Succeed in tracing the destination address 00e0-fc12-3456.
```

Trace the destination device with the MAC address as 00e0-fc12-3455. The device belongs to VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] trace mac enable
[HUAWEI] trace mac 00e0-fc12-3455 vlan 2 -h
Tracing the route to 00e0-fc12-3455 over a maximum of 255 hops:
 Hops  Host Name (IP Address)
       Ingress MAC    Ingress Port              Ingress Action    Relay Action
       Egress MAC     Egress Port               Egress Action
 1     173 (10.10.10.173)
       00e0-fc12-3455 GigabitEthernet0/0/1      IngOK             RlyHit
       --             --                        --
Info: Succeed in tracing the destination address 00e0-fc12-3455.
```

Table 5-47 Description of the trace mac command output

Item	Description
Hops	Number of hops.
Ingress Action	Action taken by the inbound interface to process LTMs: ● IngOK: The inbound interface forwards LTMs successfully. ● If this field is empty, the inbound interface fails to forward LTMs.

Item	Description
Relay Action	Action taken by the device to process LTMs: ● RlyFDB: The device forwards LTMs to the next hop device. ● RlyHit: The device forwards LTMs to the destination device.
Egress Action	Action taken by the outbound interface to process trace packets: ● EgrOK: The outbound interface forwards LTMs successfully. ● If this field is empty, the outbound interface does not or fails to forward LTMs.

5.3.48 trace mac enable

Function

The **trace mac enable** command enables GMAC trace.

The **undo trace mac enable** command disables GMAC trace.

By default, GMAC trace is disabled (except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S).

Format

trace mac enable

undo trace mac enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement the following functions, use the **trace mac enable** command:

- Implement GMAC trace.
- Enable the device to respond to LTMs of MAC trace.

Example

Enable GMAC trace.

```
<HUAWEI> system-view
[HUAWEI] trace mac enable
```

5.3.49 unknown-flow drop

Function

The **unknown-flow drop** command configures unknown packet isolation in a VLAN.

The **undo unknown-flow drop** command cancels unknown packet isolation in a VLAN.

By default, unknown packet isolation is not configured in a VLAN.

NOTE

This function is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

unknown-flow drop

undo unknown-flow drop

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To isolate unknown packets in a VLAN, run the **unknown-flow drop** command. This function applies to large- and medium-sized campus networks where aggregation and access switches go online through Option 148.

Example

Configure unknown packet isolation in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] unknown-flow drop
```

5.3.50 vlan

Function

The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN exists, the VLAN view is displayed.

The **undo vlan** command deletes a VLAN.

By default, all interfaces belong to the default VLAN, named VLAN 1.

Format

vlan *vlan-id*

vlan batch { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan *vlan-id*

undo vlan batch { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer ranging from 1 to 4094.
batch	Configures VLANs in batches.	-
vlan-id1 **to** *vlan-id2*	Specifies range of VLANs to be configured in batches: • *vlan-id1* specifies the start VLAN ID. • *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. • If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is created.	The *vlan-id1* and *vlan-id2* are integers ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce broadcast domains and enhance security on a complex network, VLANs can be created on the network to isolate the hosts that do not need to communicate with each other. The **vlan batch** command creates multiple VLANs at one time, simplifying VLAN configuration.

Follow-up Procedure

Assign VLANs according to network requirements.

Precautions

- VLAN 1 is the default VLAN, which cannot be deleted and does not need to be created.
- The **vlan** command can be used to create a VLAN and enter the VLAN view. If a VLAN has been created, the VLAN view is displayed after this command is used. You can repeat the **vlan** command for multiple times. If a VLAN has been created, this command cannot be used to create the same VLAN or modify the configurations of the VLAN.
- The **vlan batch** command can be used to create multiple VLANs in batches. If a VLAN has been created, this command cannot be used to create the same VLAN or modify the configurations of the VLAN. If you run the **vlan batch** command multiple times, all the specified VLANs are created.
- The allowed VLANs on a sub-interface cannot be created in the system view or be displayed by the display command.

Example

Create VLAN 100 and enter the VLAN 100 view. If VLAN 100 exists, the VLAN 100 view is displayed directly.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100]
```

5.3.51 vlan configuration

Function

The **vlan configuration** command creates and enters the configuration view of a VLAN. When the VLAN is not created, this command does not create the VLAN.

The **undo vlan** *vlan-id* **configuration** command deletes the configuration view of a VLAN.

By default, no VLAN configuration view is created.

Format

vlan *vlan-id* **configuration**

undo vlan *vlan-id* **configuration**

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the following scenarios:

- If you need to perform configurations in a VLAN without creating the VLAN on VCMP clients, create the VLAN on the VCMP server and run the **vlan configuration** command on VCMP clients to enter the VLAN configuration view.
- After a VLAN is deleted on the VCMP server, VCMP clients delete the local VLAN but do not delete configurations in the VLAN. To delete or modify configurations in a VLAN without creating the VLAN, run the **vlan configuration** command to enter the VLAN configuration view to delete or modify configurations.

The **vlan** *vlan-id* **configuration** command completes the VLAN configuration when the VLAN is not created.

Precautions

The **vlan configuration** command only enters the VLAN configuration view. Neither the corresponding VLAN or configurations in the VLAN take effect. To make configurations in the VLAN take effect, create the VLAN using the **vlan** command.

The **vlan** *vlan-id* **configuration** command configuration is displayed in the following situations:

- The **vlan** *vlan-id* **configuration** command displays the VLAN view and services are configured in the VLAN.
- The VLAN is deleted using VCMP.

Example

Enter the configuration view of VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10 configuration
[HUAWEI-vlan10]
```

5.3.52 vlan precedence

Function

The **vlan precedence** command configures the device to preferentially use a VLAN assignment mode when both MAC address-based and IP subnet-based VLAN assignment modes are matched.

The **undo vlan precedence** command restores the default VLAN assignment mode on an interface when both MAC address-based and IP subnet-based VLAN assignment modes are matched.

By default, MAC address-based VLAN assignment takes precedence over IP subnet-based VLAN assignment.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6735-S, S6720-EI, S6720S-EI, and S6720S-S support this command.

Format

vlan precedence { **ip-subnet-vlan** | **mac-vlan** }

undo vlan precedence

Parameters

Parameter	Description	Value
ip-subnet-vlan	Indicates that IP subnet-based VLAN assignment takes precedence over MAC address-based VLAN assignment.	-
mac-vlan	Indicates that MAC address-based VLAN assignment takes precedence over IP subnet-based VLAN assignment.	-

Views

system view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, MultiGE interface view, port group view

NOTE

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support the **vlan precedence** command only in the system view. Other switches support the **vlan precedence** command only in the interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure all the VLAN assignment methods simultaneously on the switch. By default, the priority order of VLAN assignment methods is: policy-based VLAN > MAC address-based > IP subnet-based > protocol-based > port-based.

The **vlan precedence** command changes the priority order of MAC address-based VLAN assignment and IP subnet-based VLAN assignment. For example, the **vlan precedence ip-subnet-vlan** command makes IP subnet-based VLAN assignment take precedence over MAC address-based VLAN assignment.

Currently, port-based VLAN assignment is used most widely.

Precautions

This command does not change the priority order of the other VLAN assignment methods.

Packets may be transmitted in a different VLAN after the priority order of MAC address-based VLAN assignment and IP subnet-based VLAN assignment changes. This may cause a traffic forwarding failure in the VLAN.

When the command is used on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S to adjust the priority, the command is valid for MAC-VLAN entries with the mask and without the mask. The command is valid for only MAC-VLAN entries without the mask on other models.

If you run the **vlan precedence** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Specify that IP subnet-based VLAN assignment takes precedence over MAC address-based VLAN assignment.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vlan precedence ip-subnet-vlan
```

5.3.53 vlan range

Function

The **vlan range** command creates a temporary VLAN range and displays the VLAN-Range view.

By default, no temporary VLAN ranges are created.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vlan range { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies VLAN IDs to be created in batches: - *vlan-id1* specifies the start VLAN ID. - *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and **to** *vlan-id2* specify a VLAN range. - If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is configured.	The value is an integer ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Manually configuring and maintaining VLANs is challenging on a large Layer 2 network. Configuration inconsistency may also occur. To improve maintenance efficiency and simplify configurations, run the **vlan range** command to create a temporary VLAN range. You can then configure services in the VLAN-Range view. Configured services will be delivered in batches to all the VLANs in the VLAN range.

Precautions

The **vlan range** command configuration is not saved in the configuration file. If services are configured in the VLAN-Range view, the service configurations of all the VLANs in the VLAN range will be saved in the configuration file.

A temporary VLAN range fails to be created if the specified VLAN is a dynamic VLAN or is not created. VLANs that have been added to a temporary VLAN range will automatically leave the VLAN range after being deleted.

Configuration Impact

If the **vlan range** command is run more than once, all configurations take effect.

Example

Create a VLAN range 10 to 20 and enter the VLAN-Range view.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 to 20
[HUAWEI] vlan range 10 to 20
[HUAWEI-vlan-range]
```

5.3.54 vlan statistics

Function

The **vlan statistics** command configures the way to collect VLAN traffic statistics.

The **undo vlan statistics** command restores the default way to collect VLAN traffic statistics.

By default, VLAN traffic statistics are collected by packets.

Format

vlan statistics { **by-bytes** | **by-packets** }

undo vlan statistics { **by-bytes** | **by-packets** }

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S support this command.

Parameters

Parameter	Description	Value
by-bytes	Collects VLAN traffic statistics by bytes.	-
by-packets	Collects VLAN traffic statistics by packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable (VLAN view)** command to enable traffic statistics collection in VLANs.

After traffic statistics collection is enabled in a VLAN, the switch collects statistics on unicast packets, broadcast packets, and broadcast packets transmitted in the VLAN.

The **vlan statistics** { **by-bytes** | **by-packets** } command configures whether traffic statistics are collected by packet s or bytes.

Example

Configure the system to collect VLAN traffic statistics by bytes.

```
<HUAWEI> system-view
[HUAWEI] vlan statistics by-bytes
```

5.3.55 vlan statistics interval

Function

The **vlan statistics interval** command sets the interval for collecting VLAN traffic statistics.

The **undo vlan statistics interval** command restores the default interval for collecting VLAN traffic statistics.

By default, VLAN traffic statistics are collected at an interval of 300 seconds.

Format

vlan statistics interval *interval-time*

undo vlan statistics interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for collecting VLAN traffic statistics.	The value is an integer that ranges from 60 to 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable (VLAN view)** command to enable traffic statistics collection in VLANs.

After traffic statistics collection is enabled in a VLAN, the switch collects statistics on unicast packets, broadcast packets, and broadcast packets transmitted in the VLAN.

You can use the **vlan statistics interval** command to specify the interval at which traffic statistics are collected.

Example

Set the interval for collecting VLAN traffic statistics to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] vlan statistics interval 500
```

5.3.56 vlan vlan-name

Function

The **vlan vlan-name** command displays the view of a VLAN with the specified VLAN name.

The **undo vlan vlan-name** command deletes a VLAN with the specified VLAN name. After the command is used, the VLAN name is also deleted.

Format

vlan vlan-name *vlan-name*

undo vlan vlan-name *vlan-name*

Parameters

Parameter	Description	Value
vlan-name	Specifies the VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **name** command is run to set a VLAN name, you can run the **vlan vlan-name** command in the system view to enter the corresponding VLAN view.

Assume that a device has multiple VLANs and each VLAN has a name. If you need to delete the VLAN that is used to transmit voice services but cannot remember the ID of the VLAN, you can run the **undo vlan vlan-name** command to delete the VLAN by inputting the VLAN name.

Prerequisites

Before running the **vlan vlan-name** command, ensure that the **name** command is run to set the VLAN name.

Precautions

When you run the **undo vlan vlan-name** command to delete a VLAN, services configured for the VLAN are deleted at the same time. The deleted services cannot be restored even if you recreate the VLAN. Therefore, exercise caution when running the **undo vlan vlan-name** command.

Example

Enter the view of the VLAN named **user1**.

```
<HUAWEI> system-view
[HUAWEI] vlan vlan-name user1
[HUAWEI-vlan2]
```

5.4 VLAN Aggregation Configuration Commands

5.4.1 Command Support

Only the following switch models support VLAN aggregation:

S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S5735-S, S5735S-S, S5735-S-I, S6720S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

5.4.2 access-vlan

Function

The **access-vlan** command adds one or more sub-VLANs to a super-VLAN.

The **undo access-vlan** command removes one or more sub-VLANs from a super-VLAN.

By default, no sub-VLAN is added to the super-VLAN.

Format

access-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo access-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies a range of sub-VLAN IDs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only one VLAN is added to the super-VLAN. You can specify a maximum of 10 VLAN ID ranges at a time. The ranges cannot overlap.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VLAN technology is widely applied to packet switching networks because it controls broadcast domains flexibly and is easy to deploy. Generally, a Layer 3 switch usually uses a Layer 3 logical interface in each VLAN to allow user hosts in different broadcast domains to communicate. This wastes IP addresses. The VLAN aggregation function is introduced to save IP addresses while implementing communication between VLANs.

The VLAN aggregation function associates a super-VLAN with multiple sub-VLANs. A VLANIF interface can be created in the super-VLAN and be configured with an IP address. Interfaces in all the sub-VLANs use this IP address as the gateway address to communicate with interfaces in other VLANs. This reduces subnet IDs, subnet default gateway addresses, and subnet broadcast IP addresses. In a word, the VLAN aggregation function allows different broadcast domains to use the same subnet address, implements flexible addressing, and saves IP addresses.

Prerequisites

The super-VLAN has been configured using the **aggregate vlan** command.

Before running the **access-vlan** command, delete VLANIF interfaces from all the sub-VLANs.

Follow-up Procedure

Configure the sub-VLANs to implement Layer 2 communication between them.

Precautions

The super-VLAN must be different from all its sub-VLANs.

A VLAN can be added to only one super-VLAN.

If you run the **access-vlan** command multiple times in the same VLAN view, all the specified VLANs are added to the super-VLAN.

Example

Add sub-VLAN20 and sub-VLAN30 to super-VLAN2.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] aggregate-vlan
[HUAWEI-vlan2] access-vlan 20 30
```

5.4.3 aggregate-vlan

Function

The **aggregate-vlan** command configures a VLAN as a super-VLAN.

The **undo aggregate-vlan** command cancels the configuration.

By default, no VLAN is configured as a super-VLAN.

Format

aggregate-vlan

undo aggregate-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VLAN technology is widely applied to packet switching networks because it controls broadcast domains flexibly and is easy to deploy. Generally, a Layer 3 switch usually uses a Layer 3 logical interface in each VLAN to allow user hosts in different broadcast domains to communicate. This wastes IP addresses. The VLAN aggregation function is introduced to save IP addresses while implementing communication between VLANs.

The VLAN aggregation function associates a super-VLAN with multiple sub-VLANs. A VLANIF interface can be created in the super-VLAN and be configured with an IP address. Interfaces in all the sub-VLANs use this IP address as the gateway address to communicate with interfaces in other VLANs. This reduces subnet IDs, subnet default gateway addresses, and subnet broadcast IP addresses. In a word, the VLAN aggregation function allows different broadcast domains to use the same subnet address, implements flexible addressing, and saves IP addresses.

Prerequisites

Before configuring a VLAN as a super-VLAN, delete all physical interfaces from the VLAN.

Precautions

VLAN 1 cannot be configured as a super-VLAN.

If a VLAN has been configured as a guest VLAN, it cannot be configured as a super-VLAN.

If a VLAN or the VLAN pool to which a VLAN belongs has been configured as a service VLAN for the WLAN network, the VLAN cannot be configured as a super-VLAN. Similarly, if a VLAN has been configured as a super-VLAN, the VLAN or the VLAN pool to which the VLAN belongs cannot be configured as a service VLAN for the WLAN network. In addition, if a VLAN pool has been configured as a service VLAN for a WLAN network, a super-VLAN cannot be added to the VLAN pool.

The super-VLAN must be different from all its sub-VLANs.

After a VLAN is configured as a super-VLAN, no physical interface can be added to the VLAN.

If too many sub-VLANs are added to the super-VLAN, the ARP broadcast storm degrades the system performance and affects the ARP learning.For S6730-H, S6730-S, S6730S-H, S6730S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, and S5732-H, the number of sub-VLANs that are added to a super-VLAN cannot exceed 24. For other models, the number cannot exceed 16.

Example

Configure VLAN 2 as a Super-VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 2
[HUAWEI-vlan2] aggregate-vlan
```

5.4.4 display sub-vlan

Function

The **display sub-vlan** command displays information about sub-VLAN entries.

Format

display sub-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a sub-VLAN. When multiple VLANs are configured on a device, you are recommended to specify the VLAN ID so that you can view information about a specific sub-VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VLAN aggregation is configured on a device, you can determine whether VLAN aggregation has been correctly configured by running the **display sub-vlan** command to check information about sub-VLANs and check which sub-VLANs are contained in a super-VLAN.

When using the **display sub-vlan** command, note the following issues:

- If *vlan-id* is not specified, information about all sub-VLANs on the device is displayed.
- If *vlan-id* is specified, information about a specific sub-VLAN is displayed.

Before running the **display sub-vlan** command, ensure that the device is configured with sub-VLANs. Otherwise, no command output is displayed.

Example

Display information about all sub-VLANs.

```
<HUAWEI> display sub-vlan
```

```
VLAN ID   Super-VLAN
------------------------
10        40
20        40
30        40
```

Table 5-48 Description of the **display sub-vlan** command output

Item	Description
VLAN ID	Existing sub-VLAN on the device. To specify the parameter, run the **access-vlan** command.
Super-VLAN	Super-VLAN that the sub-VLAN belongs to. To specify the parameter, run the **aggregate-vlan** command.

5.4.5 display super-vlan

Function

The **display super-vlan** command displays information about super-VLAN entries.

Format

display super-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a super-VLAN. When multiple VLANs are configured on a device, you are recommended to specify the VLAN ID so that you can view information about a specific super-VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VLAN aggregation is configured on a device, you can determine whether VLAN aggregation has been correctly configured by running the **display super-vlan** command to check information about super-VLANs and check which sub-VLANs are contained in a super-VLAN.

When using the **display super-vlan** command, note the following issues:

- If *vlan-id* is not specified, information about all super-VLANs on the device is displayed.
- If *vlan-id* is specified, information about a specific super-VLAN is displayed.

Before running the **display super-vlan** command, ensure that the device is configured with super-VLANs. Otherwise, no command output is displayed.

Example

Display information about all super-VLANs.

```
<HUAWEI> display super-vlan
VLAN ID   Sub-VLAN
------------------------
40        10 20 30
```

Table 5-49 Description of the **display super-vlan** command output

Item	Description
VLAN ID	Existing super-VLAN on the device. To specify the parameter, run the **aggregate-vlan** command.
Sub-VLAN	Sub-VLAN in the super-VLAN. To specify the parameter, run the **access-vlan** command.

5.5 MUX VLAN Configuration Commands

5.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.5.2 display mux-vlan

Function

Using the **display mux-vlan** command, you can view the MUX VLAN configuration.

Format

display mux-vlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring the MUX VLAN function, you can use the **display mux-vlan** command to verify the configuration. This command displays the principal VLAN ID, subordinate VLAN ID, VLAN type, and interfaces in each VLAN.

Precautions

If no MUX VLAN is configured by using the **mux-vlan** command, the **display mux-vlan** command does not display any information.

Example

Display the MUX VLAN configuration.

```
<HUAWEI> display mux-vlan
Principal Subordinate Type      Interface
----------------------------------------------------------------------------
100       -          principal
100       120          separate    GigabitEthernet0/0/1
100       130          group       GigabitEthernet0/0/2
100       140          group       GigabitEthernet0/0/3
----------------------------------------------------------------------------
```

Table 5-50 Description of the display mux-vlan command output

Item	Description
Principal	ID of a principal VLAN. To specify the parameter, run the **mux-vlan** command.
Subordinate	ID of a subordinate VLAN To specify the parameter, run the **subordinate group**, or **subordinate separate** command.
Type	Type of a VLAN. ● principal: indicates a principal VLAN, configured by the **mux-vlan** command. ● group: indicates a subordinate group VLAN, configured by the **subordinate group** command. ● separate: indicates a subordinate separate VLAN, configured by the **subordinate separate** command.
Interface	Interfaces in a VLAN.

5.5.3 mux-vlan

Function

The **mux-vlan** command configures a VLAN as a principal VLAN.

The **undo mux-vlan** command cancels the configuration.

By default, no VLAN is configured as a principal VLAN.

Format

mux-vlan

undo mux-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.
  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

Prerequisites

The VLAN to be configured as a principal VLAN is not a super-VLAN, a sub-VLAN, or a subordinate VLAN.

Follow-up Procedure

Configure subordinate VLANs for the principal VLAN and enable the MUX VLAN function on interfaces.

Precautions

The VLAN ID assigned to a principal VLAN cannot be used to configure the super-VLAN or sub-VLAN. Additionally, it is not recommended that this VLAN ID be used to configure VLAN mapping and VLAN stacking.

If a VLAN has been configured as a principal VLAN, it cannot be configured as a subordinate VLAN of another principal VLAN.

Example

Configure VLAN 5 as a principal VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] mux-vlan
```

5.5.4 port mux-vlan enable

Function

The **port mux-vlan enable** command enables the MUX VLAN function on an interface.

The **undo port mux-vlan enable** command disables the MUX VLAN function on an interface.

By default, the MUX VLAN function is disabled on an interface.

Format

port mux-vlan enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port mux-vlan enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo port mux-vlan enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables MUX VLAN for specified VLANs. For principal VLANs, a VLAN ID range can be specified. For subordinate group VLANs or separate VLANs, only one VLAN ID can be specified.	The value is an integer ranging from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, VE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves a MUX VLAN and several subordinate VLANs. Subordinate VLANs are classified into subordinate group VLANs and subordinate separate VLANs. Subordinate VLANs can communicate with the principal VLAN but cannot communicate with each other. Interfaces in a subordinate group VLAN can communicate with each other, and interfaces in a subordinate separate VLAN are isolated from each other.

The MUX VLAN function takes effect only after it is enabled on an interface.

Prerequisites

Before enabling the MUX VLAN function, ensure that the interface has been added to a principal or subordinate VLAN as an access, hybrid, or trunk interface.

Precautions

- Disabling MAC address learning or limiting the number of learned MAC addresses on an interface affects the MUX VLAN function on the interface.
- The MUX VLAN and port security functions conflict on an interface; therefore, the **port mux-vlan enable** and **port-security enable** commands are not advised to be used on the same interface.
- The MUX VLAN and MAC address authentication conflict on an interface; therefore, the **port mux-vlan enable** and **mac-authen** commands are not advised to be used on the same interface.
- The MUX VLAN and 802.1x authentication conflict on an interface; therefore, the **port mux-vlan enable** and **dot1x enable** commands are not advised to be used on the same interface.

- You can create a VLANIF interface for a principal VLAN, but cannot create a VLANIF interface for a subordinate group VLAN or separate VLAN.
- The **port mux-vlan enable** command is not supported on a **negotiation-auto** or **negotiation-desirable** port.
- When the interface is enabled with MUX VLAN and configured with the PVID using the **port trunk pvid vlan** command, do not configure the PVID as the ID of the principal VLAN or subordinate VLAN of the MUX VLAN. For example, VLAN 10 is the principal VLAN, VLAN 11 is a subordinate group VLAN, and VLAN 12 is a subordinate separate VLAN. After the **port mux-vlan enable vlan 10** command is used on the interface to enable MUX VLAN, do not run the **port trunk pvid vlan** command to set the PVID to VLAN 11 or VLAN 12.

Example

Enable the MUX VLAN function in VLAN 2 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port mux-vlan enable vlan 2
```

5.5.5 subordinate group

Function

The **subordinate group** command configures subordinate group VLANs for a principal VLAN.

The **undo subordinate group** command removes subordinate group VLANs from a principal VLAN.

By default, a principal VLAN does not have any subordinate group VLAN.

Format

subordinate group { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo subordinate group { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies a range of VLAN IDs. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. If **to** *vlan-id2* is not specified, only one subordinate group VLAN is configured.	- The value of *vlan-id1* is an integer that ranges from 1 to 4094. - The value of *vlan-id2* is an integer that ranges from 1 to 4094 and must be greater than or equal to the value of *vlan-id1*.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.
  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

After interfaces using by employees are added to the subordinate group VLAN, employees can access servers of the enterprise and communicate with one another.

Prerequisites

The specified subordinate group VLANs are not super-VLANs and do not have any VLANIF interface.

Before configuring a VLAN as a subordinate group VLAN, run the **undo subordinate group** command to delete all its member interfaces.

Follow-up Procedure

Add interfaces to subordinate group VLANs and enable the MUX VLAN function on the interfaces.

Precautions

Before configuring a VLAN as a subordinate separate VLAN, ensure that the VLAN and its principal VLAN have been created. Otherwise, this command does not take effect even if it is executed successfully.

Subordinate VLANs must be different from the principal VLAN.

A VLAN cannot be configured as a subordinate group VLAN and a subordinate separate VLAN simultaneously.

If you run the **subordinate group** command multiple times in the same VLAN view, all the specified VLANs are configured as subordinate group VLANs. A maximum of 128 subordinate group VLANs can be configured in a primary VLAN.

The VLAN ID assigned to a group VLAN cannot be used to configure a VLANIF interface, super-VLAN, or sub-VLAN. Additionally, it is not recommended that this VLAN ID be used to configure VLAN mapping and VLAN stacking.

When you configure a subordinate VLAN using the **subordinate group** or **subordinate separate** command or create a VLAN with an ID same as an existing subordinate VLAN, the device deletes existing dynamic MAC address entries and duplicated MUX MAC address entries of the principal VLAN of this subordinate VLAN.

Example

Configure VLAN 7 as the subordinate group VLAN of VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] subordinate group 7
```

5.5.6 subordinate separate

Function

The **subordinate separate** command configures a subordinate separate VLAN for a principal VLAN.

The **undo subordinate separate** command removes the subordinate separate VLAN from a principal VLAN.

By default, a principal VLAN does not have any subordinate separate VLAN.

Format

subordinate separate *vlan-id*

undo subordinate separate

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of an existing VLAN.	The value is an integer that ranges from 1 to 4094.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate

separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.

  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

After interfaces using by customers are added to the subordinate separate VLAN, customers can neither communicate with each other nor access servers of the enterprise.

Prerequisites

The specified subordinate separate VLANs are not super-VLANs and do not have any VLANIF interface.

Before configuring a VLAN as a subordinate separate VLAN, run the **undo subordinate separate** command to delete all its member interfaces.

Follow-up Procedure

Add interfaces to the subordinate separate VLAN and enable the MUX VLAN function on the interfaces.

Precautions

Before configuring a VLAN as a subordinate separate VLAN, ensure that the VLAN and its principal VLAN have been created. Otherwise, this command does not take effect even if it is executed successfully.

Subordinate VLANs must be different from the principal VLAN.

A VLAN cannot be configured as a subordinate group VLAN and a subordinate separate VLAN simultaneously.

A principal VLAN can be configured with only one subordinate separate VLAN. Before configuring another VLAN as the subordinate separate VLAN, run the **undo subordinate separate** command to delete the previous one.

The VLAN ID assigned to a separate VLAN cannot be used to configure a VLANIF interface, super-VLAN, or sub-VLAN. Additionally, it is not recommended that this VLAN ID be used to configure VLAN mapping and VLAN stacking.

When you configure a subordinate VLAN using the **subordinate group** or **subordinate separate** command or create a VLAN with an ID same as an existing subordinate VLAN, the device deletes existing dynamic MAC address entries and duplicated MUX MAC address entries of the principal VLAN of this subordinate VLAN.

Example

Configure VLAN 6 as the subordinate separate VLAN of VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] vlan 5
[HUAWEI-vlan5] subordinate separate 6
```

5.6 VLAN Termination Configuration Commands

5.6.1 Command Support

Only the following switch models support VLAN termination:

S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

5.6.2 arp broadcast enable

Function

The **arp broadcast enable** command enables ARP broadcast on a VLAN tag termination sub-interface.

The **undo arp broadcast enable** command disables ARP broadcast on a VLAN tag termination sub-interface.

By default, ARP broadcast is disabled on a VLAN tag termination sub-interface.

Format

arp broadcast enable

undo arp broadcast enable

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN tag termination sub-interfaces discard broadcast packets after receiving the packets. To permit a VLAN tag termination sub-interface to forward broadcast packets, run the **arp broadcast enable** command on the sub-interface to enable ARP broadcast.

Configuration Impact

When IP packets need to be sent out from the termination sub-interface and there is no corresponding ARP entry on the device, the following situations may occur:

- If ARP broadcast is not enabled on the termination sub-interface, the system does not send or forward broadcast ARP packets to learn ARP entries (gratuitous ARP packets will still be sent normally). In this case, the IP packets are discarded directly.
- The system tags an ARP broadcast packet and forwards it through the VLAN tag termination sub-interface when ARP broadcast is enabled run on the VLAN tag termination sub-interface.

Precautions

When you enable or disable ARP broadcast on a VLAN tag termination sub-interface, the routing status of the sub-interface becomes Down and then Up. This may result in route flapping on the entire network, affecting services.

After the ARP broadcast function is enabled using the **arp broadcast enable** command, if a service packet is sent from a termination sub-interface but does not have an ARP entry, an ARP request is copied and sent in all VLANs of the sub-interface. If a large number of VLANs are configured, the number of ARP requests to be copied and sent is large, which may bring a heavy burden on the peer devices that receive the ARP requests. Consequently, the peer devices may encounter exceptions, such as high CPU usage and broadcast suppression. The local device may also fail to immediately send ARP requests as it is busy in processing packet copying, leading to ARP learning failures. To prevent this issue, you are advised to reduce the number of VLANs configured on sub-interfaces.

Example

Enable ARP broadcast on XGigabitEthernet0/0/1.1.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] dot1q termination vid 10
[HUAWEI-XGigabitEthernet0/0/1.1] arp broadcast enable
```

5.6.3 display dot1q information

Function

The **display dot1q information termination** command displays the configuration of a dot1q sub-interface.

Format

display dot1q information termination [**interface** *interface-type interface-number* [.*subinterface-number*]]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring dot1q termination on sub-interfaces, run the **display dot1q information termination** command to view the sub-interfaces where dot1q termination is configured and configuration of the dot1q sub-interfaces.

Example

Display the configuration of all dot1q sub-interfaces.

```
<HUAWEI> display dot1q information termination
 XGigabitEthernet0/0/1.3
   Total QinQ Num: 1
   dot1q  termination vid 3
   Total vlan-group Num: 0
```

Table 5-51 Description of the display dot1q information command output

Item	Description
XGigabitEthernet0/0/1.3	Sub-interface name.
Total QinQ Num	Number of QinQ entries configured for user packets on a sub-interface.

Item	Description
dot1q termination vid 3	VLAN allowed by a sub-interface. To specify the parameter, run the **dot1q termination vid** command.
Total vlan-group Num	Number of VLAN groups configured on a sub-interface.

5.6.4 display qinq information

Function

The **display qinq information** command displays the configuration of all the sub-interfaces configured with QinQ termination, QinQ stacking, or QinQ mapping.

Format

display qinq information { **termination** | **stacking** | **mapping** } [**interface** *interface-type interface-number* [.*subinterface-number*]]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
termination	Displays all the sub-interfaces configured with QinQ termination.	-
stacking	Displays all the sub-interfaces configured with QinQ stacking.	-
mapping	Displays all the sub-interfaces configured with QinQ mapping.	-
interface *interface-type interface-number*	Displays whether all the sub-interfaces of the specified main interface are configured with QinQ termination, QinQ stacking, or QinQ mapping. *interface-type* specifies the interface type. *interface-number* specifies the number of the main interface.	-

Parameter	Description	Value
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring QinQ termination, QinQ stacking, and QinQ mapping, run the **display qinq information** command to view the configuration and the sub-interfaces configured with these functions.

When a large number of QinQ termination, QinQ stacking, and QinQ mapping entries are configured, it is recommended that you specify a QinQ function, a main interface, a sub-interface, or a pipe operator (|) to filter the output. Otherwise, too much information is displayed, which has the following negative effects:

- The displayed information is updated continuously on the display terminal and the required information cannot be obtained.
- The system traverses and retrieves information for a long time. As a result, the system does not respond to any request.

When using this command, note the following points:

- If you specify only **termination** in the command, all sub-interfaces configured with QinQ termination are displayed.
- If you specify **termination** and **interface** *interface-type interface-number*, the sub-interface configured with QinQ termination on the specified main interface is displayed.
- If you specify **termination** and **interface** *interface-type interface-number.subinterface-number*, the specified sub-interface configured with QinQ termination is displayed.
- If you specify only **stacking** in the command, all sub-interfaces configured with QinQ stacking are displayed.
- If you specify **stacking** and **interface** *interface-type interface-number*, the sub-interface configured with QinQ stacking on the specified main interface is displayed.
- If you specify **stacking** and **interface** *interface-type interface-number.subinterface-number*, the specified sub-interface configured with QinQ stacking is displayed.
- If you specify only **mapping** in the command, all sub-interfaces configured with QinQ mapping are displayed.

- If you specify **mapping** and **interface** *interface-type interface-number*, the sub-interface configured with QinQ mapping on the specified main interface is displayed.
- If you specify **mapping** and **interface** *interface-type interface-number.subinterface-number*, the specified sub-interface configured with QinQ mapping is displayed.

Example

Display all the sub-interfaces configured with QinQ termination.

```
<HUAWEI> display dot1q information termination
 XGigabitEthernet0/0/1.30
   Total QinQ Num: 1
   qinq termination pe-vid 300 ce-vid 200
   Total vlan-group Num: 0
```

Display all the sub-interfaces configured with QinQ stacking.

```
<HUAWEI> display qinq information stacking
 XGigabitEthernet0/0/1.4
   Total QinQ Num: 1
     qinq stacking vid 25 pe-vid 35
   Total vlan-group Num: 0
```

Display all the sub-interfaces configured with QinQ mapping.

```
<HUAWEI>display qinq information mapping
 XGigabitEthernet0/0/1.5
   Total QinQ Num: 1
     qinq mapping vid 55 map-vlan vid 65
   Total vlan-group Num: 0
```

Table 5-52 Description of the display qinq information command output

Item	Description
XGigabitEthernet0/0/1.30	Sub-interface name.
Total QinQ Num	Number of QinQ entries configured for user packets on a sub-interface.
Total vlan-group Num	Number of VLAN groups configured on a sub-interface.

5.6.5 dot1q termination vid

Function

The **dot1q termination vid** command sets the single VLAN ID for Dot1q termination on a sub-interface.

The **undo dot1q termination vid** command deletes the single VLAN ID for Dot1q termination on a sub-interface.

By default, the single VLAN ID for Dot1q termination is not set on a sub-interface.

Format

dot1q termination vid *low-pe-vid* [**to** *high-pe-vid*]

undo dot1q termination vid *low-pe-vid* [**to** *high-pe-vid*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
low-pe-vid	Specifies the minimum value of the VLAN tag in user packets.	The value is an integer that ranges from 2 to 4094.
high-pe-vid	Specifies the maximum value of the VLAN tag in user packets. The value of *high-pe-vid* must be greater than or equal to the value of *low-pe-vid*.	The value is an integer that ranges from 2 to 4094.

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- Communication between VLANs

  VLANs are widely used because they can separate Layer 2 packets. A physical LAN is divided into multiple logical broadcast domains. Hosts in the same VLAN can communicate with each other but the hosts of different VLANs cannot. The Layer 3 routing technology is used for communication between hosts of different VLANs in the following two methods:

  - Through the VLANIF interface on the Layer 3 switch.
  - Through the Layer 3 Ethernet interface on the Layer 3 switch.

    However, when a traditional Layer 3 Ethernet interface receives VLAN packets, the VLAN packets are discarded. To enable communication between hosts of different VLANs, you can create an Ethernet sub-interface on the Layer 3 Ethernet interface and enable QinQ termination on the sub-interface to remove the tag from the VLAN packet.

- Communication between a LAN and a WAN

  Most packets on a LAN have VLAN tags, but some WAN protocols such as ATM, FR, and PPP, cannot identify VLAN packets. To send a VLAN packet from LAN to WAN, the device records VLAN information in the packet, removes the VLAN tag, and forwards the packet.

Based on the number of tags, VLAN packets can be classified into Dot1q packets and QinQ packets. A Dot1q packet carries a single-layer VLAN tag and a QinQ packet carries a double-layer VLAN tag. Accordingly, there are two VLAN tag termination modes:

- Dot1q termination, which terminates tags carried in Dot1q packets

  To configure Dot1q termination, run the **dot1q termination vid** command.
- QinQ termination, which terminates tags carried in QinQ packets.

  To configure QinQ termination, run the **qinq termination pe-vid ce-vid** command in the sub-interface view.

After the **dot1q termination vid** command is run, the sub-interface for VLAN tag termination processes the packet in the following procedures:

- The sub-interface removes the tag in the VLAN packet when receiving the packet and forwards the packet on Layer 3. The outbound interface determines whether the forwarded VLAN packet carries tags.
- The sub-interface adds VLAN information to the packet and then sends the packet.

Precautions

- The tag values of the user packet received by the sub-interface must be in the range of *low-pe-vid* to *high-pe-vid* specified in the command; otherwise, the packet is discarded.
- The VLANs allowed by a sub-interface cannot be created globally or on main interfaces, and their information cannot be displayed either.The VLANs allowed by a sub-interface cannot be the same as the default VLAN of its main interface.
- When the sub-interface is used for Layer 3 forwarding, it is recommended that there should be a maximum of 128 VLANs in the VLAN range. When there are more than 128 VLANs, IPv4 addresses can be configured but IPv6 addresses cannot be configured.
- If the **dot1q termination vid** command is run more than once, all configurations take effect.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

Set the encapsulation mode on XGigabitEthernet0/0/1.1 to Dot1q and allow the packets with the VLAN tag 100 to pass through.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
```

```
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] dot1q termination vid 100
```

5.6.6 qinq termination l2

Function

The **qinq termination l2** command configures the mode in which a sub-interface for QinQ VLAN tag termination connects to a Pseudo-Wire Emulation Edge to Edge (PWE3)/Virtual Leased Line (VLL)/Virtual Private LAN Service (VPLS) network.

The **undo qinq termination l2** command deletes the mode configured for a sub-interface for QinQ VLAN tag termination in which the sub-interface connects to a PWE3/VLL/VPLS network.

By default, access attributes are not configured on a sub-interface for QinQ VLAN tag termination.

Format

qinq termination l2 { **symmetry** | **asymmetry** }

undo qinq termination l2

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this configuration.

Parameters

Parameter	Description	Value
symmetry	Configures the sub-interface for QinQ VLAN tag termination to connect to a PWE3/VLL/VPLS network in symmetry mode.	-
asymmetry	Configures the sub-interface for QinQ VLAN tag termination to connect to a PWE3/VLL/VPLS network in asymmetry mode.	-

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

More QinQ encapsulation and termination modes are provided to differentiate users and services and save VLAN resources. These modes are widely used for refined operation.

If users communicate over an L2VPN (a PWE3, VLL, or VPLS network), you can run the **qinq termination l2** command on the sub-interfaces for QinQ VLAN tag termination of L2VPN edge devices to configure the mode in which the sub-interfaces connect to the L2VPN.

Prerequisites

A VLL, PWE3, or VPLS network-side has been deployed.

For VLL, PWE3, or VPLS configurations, see VLL Configuration, PWE3 Configuration, and VPLS Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - VPN*.

When a sub-interface for QinQ VLAN tag termination is connected to the L2VPN, the PE processes packets based on the QinQ termination configuration, attributes of the sub-interface for QinQ VLAN tag termination when the sub-interface connects to the PWE3, VLL, or VPLS network, and encapsulation mode.

NOTE

Select the encapsulation mode according to **encapsulation (VSI view)** or **mpls l2vc**.

Table 5-53 Packet processing on the inbound interface in the VPLS scenario

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Symmetrical mode	Removes the outer tag.	Reserves double tags. No action is required.
Asymmetrical mode	Removes double tags.	Removes the outer tag.
Default	Removes double tags.	Reserves double tags. No action is required.

Table 5-54 Packet processing on the outbound interface in the VPLS scenario

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Symmetrical mode	Removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.	If packets carry the inner tag: removes the MPLS label and replaces the outer tag with the tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination. If packets do not carry the inner tag: removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Asymmetrical mode	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry one inner tag: removes the MPLS label, removes one inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry double inner tags: removes the MPLS label, removes double inner tags, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Ethernet Encapsulation	VLAN Encapsulation
Default	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H and S6730-H: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.	Removes the MPLS label and transparently transmits packets.

Table 5-55 Packet processing on the inbound interface in the VLL or PWE3 scenario

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Symmetrical mode	Removes the outer tag.	Reserves double tags. No action is required.
Asymmetrical mode	Removes double tags.	Removes the outer tag.
Default	Removes the outer tag.	Reserves double tags. No action is required.

Table 5-56 Packet processing on the outbound interface in the VLL or PWE3 scenario

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Symmetrical mode	Removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.	If packets carry the inner tag: removes the MPLS label and replaces the outer tag with the tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination. If packets do not carry the inner tag: removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Asymmetrical mode	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.	S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6730S-H, and S6730-H: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry the inner tag: removes the MPLS label, removes the inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. Other models: If packets do not carry the inner tag: removes the MPLS label and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry one inner tag: removes the MPLS label, removes one inner tag, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination. If packets carry double inner tags: removes the MPLS label, removes double inner tags, and adds double tags according to **ce-vid** and **pe-vid** configured on the sub-interface for QinQ VLAN tag termination.

Inbound Interface Type	Raw Encapsulation	Tagged Encapsulation
Default	Removes the MPLS label and adds the outer tag specified by **pe-vid** that is configured on the sub-interface for QinQ VLAN tag termination.	If packets carry the inner tag: removes the MPLS label and replaces the outer tag with the tag specified by **pe-vid** on the sub-interface for QinQ VLAN tag termination. If packets do not carry the inner tag: removes the MPLS label and adds the outer tag specified by **pe-vid** on the sub-interface for QinQ VLAN tag termination.

Example

Configure the sub-interface for QinQ VLAN tag termination XGigabitEthernet0/0/1.1 to connect to an L2VPN in asymmetry mode.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq termination l2 asymmetry
[HUAWEI-XGigabitEthernet0/0/1.1] qinq termination pe-vid 100 ce-vid 200
[HUAWEI-XGigabitEthernet0/0/1.1] quit
```

5.6.7 qinq termination pe-vid ce-vid

Function

The **qinq termination pe-vid ce-vid** command configures QinQ termination on a sub-interface.

The **undo qinq termination pe-vid ce-vid** command cancels QinQ termination on a sub-interface.

By default, QinQ termination is disabled on a sub-interface.

Format

qinq termination pe-vid *pe-vid* **ce-vid** *ce-vid1* [**to** *ce-vid2*]

undo qinq termination pe-vid *pe-vid* **ce-vid** *ce-vid1* [**to** *ce-vid2*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the outer VLAN ID.	The value is an integer that ranges from 2 to 4094.
ce-vid *ce-vid1* [**to** *ce-vid2*]	Specifies the inner VLAN ID. ● *ce-vid1*: specifies the lower threshold of the inner VLAN tag in the user packet. ● *ce-vid2*: specifies the upper threshold of the outer VLAN tag in the user packet. ● The value of *ce-vid2* must be greater than or equal to the value of *ce-vid1*.	The value of *ce-vid1* is an integer that ranges from 1 to 4094. The value of *ce-vid2* is an integer that ranges from 1 to 4094.

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- Communication between VLANs

  VLANs are widely used because they can separate Layer 2 packets. A physical LAN is divided into multiple logical broadcast domains. Hosts in the same VLAN can communicate with each other but the hosts of different VLANs cannot. The Layer 3 routing technology is used for communication between hosts of different VLANs in the following two methods:

  - Through the VLANIF interface on the Layer 3 router.
  - Through the Layer 3 Ethernet interface on the router.

    However, when a traditional Layer 3 Ethernet interface receives VLAN packets, the VLAN packets are discarded. To enable communication between hosts of different VLANs, you can create an Ethernet sub-interface on the Layer 3 Ethernet interface and enable QinQ termination on the sub-interface to remove the tag from the VLAN packet.

- Communication between a LAN and a WAN

  Most packets on a LAN have VLAN tags, but some WAN protocols such as ATM, FR, and PPP, cannot identify VLAN packets. To send a VLAN packet from LAN to WAN, the device records VLAN information in the packet, removes the VLAN tag, and forwards the packet.

Based on the number of tags, VLAN packets can be classified into Dot1q packets and QinQ packets. A Dot1q packet carries a single-layer VLAN tag and a QinQ packet carries a double-layer VLAN tag. Accordingly, there are two VLAN tag termination modes:

- Dot1q termination, which terminates tags carried in Dot1q packets

  To configure Dot1q termination, run the **dot1q termination vid** command in the sub-interface view.
- QinQ termination, which terminates tags carried in QinQ packets.

  To configure Dot1q termination, run the **qinq termination pe-vid ce-vid** command.

After the **qinq termination pe-vid ce-vid** command is run, the sub-interface for VLAN tag termination processes the packet in the following procedures:

- The sub-interface removes the tag in the VLAN packet when receiving the packet and forwards the packet on Layer 3. Whether the forwarded VLAN packet carries tags is determined by the outbound interface.
- The sub-interface adds VLAN information to the packet and then sends the packet.

Precautions

- The tag values of the user packet received by the sub-interface must be in the range specified in the command; otherwise, the packet is discarded.
- The allowed VLANs on a sub-interface cannot be created in the system view or be displayed by the display command.
- When the sub-interface is used for Layer 3 forwarding, it is recommended that there should be a maximum of 128 VLANs in the VLAN range. When there are more than 128 VLANs, IPv4 addresses can be configured but IPv6 addresses cannot be configured.

Example

Set the encapsulation mode on XGigabitEthernet0/0/1.1 to QinQ and allow the packets with the outer VLAN tag 100 and inner VLAN tag 200 to pass through.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq termination pe-vid 100 ce-vid 200
```

5.7 Voice VLAN Configuration Commands

5.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.7.2 display voice-vlan oui

Function

The **display voice-vlan oui** command displays the OUI address and OUI attributes of a voice VLAN.

Format

display voice-vlan oui

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the OUI address, OUI mask, and OUI description of the voice VLAN.

Example

Display the OUI address of the voice VLAN.

```
<HUAWEI> display voice-vlan oui
----------------------------------------------------
OuiAddress       Mask             Description
----------------------------------------------------
00e0-fc00-0000   ffff-ff00-0000   PhoneA
00e0-fc00-0000   ffff-ff00-0000   PhoneB
```

Table 5-57 Description of the display voice-vlan oui command output

Item	Description
OuiAddress	OUI address of the packets that can pass through the device. You can run the **voice-vlan mac-address** command to configure the OUI address.

Item	Description
Mask	OUI mask of the packets that can pass through the device. To specify the parameter, run the **voice-vlan mac-address** command.
Description	Description of the OUI address. To specify the parameter, run the **voice-vlan mac-address** command.

5.7.3 display voice-vlan status

Function

The **display voice-vlan status** command displays information about the current voice VLAN.

Format

display voice-vlan [*vlan-id*] **status**

Parameters

Parameter	Description	Value
vlan-id	Displays information about a specified voice VLAN. If *vlan-id* is not specified, information about all voice VLANs is displayed.	The value is an integer that ranges from 2 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the voice VLAN function is enabled, you can run the **display voice-vlan status** command to check the voice VLAN configuration.

Example

Display information about the current voice VLAN, such as the working status, secure mode, the 802.1p priority, DSCP value, and information about an interface that is enabled with voice VLAN.

```
<HUAWEI> display voice-vlan status
Voice VLAN Configurations:
----------------------------------------------------------
Voice VLAN ID            : 2
Voice VLAN status         : Enable
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
----------------------------------------------------------
Port Information:
------------------------------------------------------------------------------
Port            Add-Mode  Security-Mode  Legacy  PribyVLAN  Untag
Tag0
------------------------------------------------------------------------------
GE0/0/4         Manual    Normal         Disable Enable     Disable Disable
```

Table 5-58 Description of the display voice-vlan status command output

Item	Description
Voice VLAN ID	ID of the voice VLAN.
Voice VLAN status	Status of the voice VLAN function. The value can be: - Enable - Disable You can run the **voice-vlan enable** command to configure the voice VLAN status.
Voice VLAN 8021p remark	802.1p priority of the voice VLAN. You can run the **voice-vlan remark** command to configure the 802.1p priority of the voice VLAN.
Voice VLAN dscp remark	DSCP value of the voice VLAN. You can run the **voice-vlan remark** command to configure the DSCP value of the voice VLAN.
Port	Number of the interface on which the voice VLAN function is enabled.
Add-Mode	Working mode of the voice VLAN. The value can be: - Manual: indicates the manual mode. - Auto: indicates the automatic mode. You can run the **voice-vlan mode** command to configure the working mode of the voice VLAN.

Item	Description
Security-Mode	Security mode of the voice VLAN on the interface. The value can be: ● Security: indicates the secure mode. ● Normal: indicates the normal mode. You can run the **voice-vlan security enable** command to configure the secure mode of the voice VLAN.
Legacy	Whether the interface can communicate with voice devices of other vendors. The value can be: ● Enable: indicates that the interface can communicate with voice devices of other vendors. ● Disable: indicates that the interface cannot communicate with voice devices of other vendors. You can run the **voice-vlan legacy enable** command to enable an interface to communicate with voice devices of other vendors.
PribyVLAN	Whether the interface increases the priority of voice packets based on VLAN IDs ● Enable: The priority of voice packets is increased based on VLAN IDs. ● Disable: The priority of voice packets is increased based on MAC addresses. To specify the parameter, run the **voice-vlan remark-mode** command.
Untag	Whether the interface adds voice VLAN IDs to untagged packets ● Enable: The interface adds voice VLAN IDs to untagged packets. ● Disable: The interface adds PVID to untagged packets. To specify the parameter, run the **voice-vlan enable** command.
Tag0	Whether the interface changes VLAN 0 in packets to the voice VLAN ID: ● Enable: The interface changes VLAN 0 in packets to the voice VLAN ID. ● Disable: The interface changes VLAN 0 in packets to the PVID of the interface. To specify the parameter, run the **voice-vlan enable** command. **NOTE** Only the S6735-S, S6720-EI and S6720S-EI support this parameter.

5.7.4 voice-vlan enable

Function

The **voice-vlan enable** command configures the specified VLAN as a voice VLAN and enables the voice VLAN function on an interface.

The **undo voice-vlan enable** command disables the voice VLAN function on an interface.

By default, the voice VLAN function is disabled on an interface.

Format

voice-vlan *vlan-id* **enable** [**include-untagged** | **include-tag0**]*

undo voice-vlan enable (port group view)

undo voice-vlan [*vlan-id*] **enable** (other interface views except the port group view)

NOTE

Only the S6735-S, S6720-EI and S6720S-EI support **include-tag0**.

Parameters

Parameter	Description	Value
vlan-id	Configures a specified VLAN as a voice VLAN.	The value is an integer that ranges from 2 to 4094.
include-untagged	Adds voice VLAN IDs to untagged packets. When an interface receives untagged packets, the interface determines whether to add voice VLAN tags to the packets according to the OUI address configured by the **voice-vlan mac-address** command. When IP phones send untagged voice packets, this parameter is mandatory.	-

Parameter	Description	Value
include-tag0	Changes the VLAN ID in packets from VLAN 0 to the voice VLAN ID. When an interface receives packets tagged with VLAN 0, the interface checks whether the packets match the OUI address configured by the **voice-vlan mac-address** command and determines whether to change the VLAN ID in packets. When IP phones send packets tagged with VLAN 0, this parameter is mandatory.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After voice VLAN is enabled on a device, based on the mode in which the priority of voice packets is increased by the **voice-vlan remark-mode** command, the device increases the priority of voice packets according to the VLAN or MAC address to ensure that voice packets are sent first.

Precautions

- If the voice VLAN configured on an interface works in automatic mode, you need to run the **port link-type** command to set the interface type to trunk or hybrid.
- To ensure normal transmission of different services, assign different VLAN IDs to the voice VLAN and default VLAN on the interface.
- Only one VLAN on an interface can be configured as a voice VLAN at a time.

- The guest VLAN, restrict VLAN, or critical VLAN on an interface cannot be configured as a voice VLAN.
- A user group VLAN configured using the **user-vlan** command cannot be specified as a voice VLAN.
- Dot1q-tunnel interfaces do not support the voice VLAN function.
- When you run the **voice-vlan enable** command multiple times, only the latest configuration takes effect.
- On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S **include-untagged** is valid for both untagged packets and packets tagged with VLAN 0. On other models, **include-untagged** is valid only for untagged packets. If the voice VLAN is valid for packets tagged with VLAN 0, **include-untagged** and **include-tag0** must be configured.
- On the S6735-S, S6720-EI and S6720S-EI, after a VLAN is associated with a BD or VSI and is specified as a voice VLAN, the VXLAN or MPLS function will not take effect.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, or S6730S-S, after a VLAN is associated with a BD or VSI, if this VLAN needs to be specified as a voice VLAN, you need to run the **lldp tlv-enable med-tlv network-policy voice-vlan vlan** *vlan-id* [**cos** *cvalue* | **dscp** *dvalue*]* command to configure the voice VLAN capability of LLDP on an interface.
- When a voice VLAN is configured together with VLAN Mapping, VLAN Stacking, or a Traffic Policy on the same interface, the configurations may not take effect.

Example

Configure VLAN 2 as a voice VLAN and enable the voice VLAN function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan 2 enable
```

5.7.5 voice-vlan legacy enable

Function

The **voice-vlan legacy enable** command enables CDP-compatible Voice VLAN function so that the switch encapsulates voice VLAN information in CDP packets and sends them to connected IP phones.

The **undo voice-vlan legacy enable** command disables CDP-compatible Voice VLAN function.

By default, CDP-compatible function is disabled.

Format

voice-vlan legacy enable

undo voice-vlan legacy enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can encapsulate voice VLAN information into LLDPDUs and send them to connected IP phones. However, IP phones of some vendors send Cisco Discovery Protocol (CDP) packets. You can run the **voice-vlan legacy enable** command to enable CDP-compatible function so that the switch encapsulates voice VLAN information in CDP packets and sends them to connected IP phones.

Prerequisites

The voice VLAN function has been enabled using the **voice-vlan enable** command.

Example

Enable CDP-compatible Voice VLAN function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan 10 enable
[HUAWEI-GigabitEthernet0/0/1] voice-vlan legacy enable
```

5.7.6 voice-vlan mac-address

Function

The **voice-vlan mac-address** command sets the OUI address of the voice VLAN.

The **undo voice-vlan mac-address** command cancels the setting of the OUI address.

By default, no OUI address is set.

Format

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Specifies the OUI address of voice packets that can be transmitted in the voice VLAN.	The value is in the format of H-H-H. H is a hexadecimal number that contains 1 to 4 digits, such as 00e0 and fc01. The address cannot be all 0s, multicast address, or broadcast address.
mask *oui-mask*	Specifies the mask of the OUI address.	The value is in the format of H-H-H. H is a 4-digit hexadecimal number that can be f or 0. The value in binary notation must start with consecutive 1s and end with consecutive 0s.
description *text*	Indicates the description of the OUI address.	The value is a string of 1 to 80 case-sensitive characters, spaces supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An OUI is the first 24 bits of a 48-bit MAC address assigned to each vendor by the Institute of Electrical and Electronics Engineers (IEEE). Voice packets sent by IP phones can be identified by the MAC address ranges requested by IP phone vendors.

In voice VLAN, the OUI is user-defined and not necessarily 24 bits long. The OUI is the result of the AND operation between the MAC address and mask in the **voice-vlan mac-address** command.

Precautions

- The *mac-address* value cannot be all 0s or a multicast or broadcast address.
- The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support a maximum

of 100 OUIs. When the switch is configured with 100 OUIs, subsequent configurations will not take effect. Other models support a maximum of 32 OUIs. When the switch is configured with 32 OUIs, subsequent configurations will not take effect.

When you run the **undo voice-vlan mac-address** command to delete an OUI MAC address, set *mac-address* to the result of the logical AND operation between the OUI and the OUI mask that you set.

Example

Allow the voice packets coming from Phone A, an IP phone, to be identified by the voice VLAN. The MAC address of Phone A is 00e0-fc04-0004 and the OUI mask address is ffff-ff00-0000.

```
<HUAWEI> system-view
[HUAWEI] voice-vlan mac-address 00e0-fc04-0004 mask ffff-ff00-0000 description PhoneA
```

5.7.7 voice-vlan mode

Function

The **voice-vlan mode** command sets the working mode of the voice VLAN on an interface.

The **undo voice-vlan mode** command restores the mode in which an interface is added to a voice VLAN to the default.

By default, the voice VLAN of an interface works in manual mode.

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this configuration.

Format

voice-vlan mode { **auto** | **manual** }

undo voice-vlan mode { **auto** | **manual** }

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode of the voice VLAN. The automatic mode of the voice VLAN is not supported on the negotiation-auto or negotiation-desirable port.	-

Parameter	Description	Value
manual	Indicates the manual mode of the voice VLAN.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

NOTE

The **undo voice-vlan mode manual** command is not supported in the port group view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ports can be added to a voice VLAN in either of the following modes:

- Automatic mode

  A voice VLAN-enabled port learns source MAC addresses of frames from voice devices, adds ports connecting the device to voice devices to a voice VLAN.

  In auto mode, you cannot manually add ports to a voice VLAN.

  NOTE

  The automatic mode takes effect only when the **voice-vlan remark-mode mac-address** command is configured to increase the priority of voice packets based on MAC addresses and the **voice-vlan enable** command without **include-untagged** specified is configured to enable voice VLAN on the interface and add voice VLAN IDs to only tagged packets.

- Manual mode

  After the voice VLAN function is enabled, ports connected to voice devices must be manually added to a voice VLAN. Otherwise, the voice VLAN function does not take effect.

Pre-configuration Tasks

Before configuring a port to work in automatic mode, run the **voice-vlan enable** command to enable the voice VLAN function and run the **voice-vlan remark-mode mac-address** command to increase the priority of voice packets based on MAC addresses.

In auto mode, access, negotiation-auto, or negotiation-desirable interfaces cannot be added to a voice VLAN. To add the interface to the voice VLAN, run the **port link-type** command to change the link type of the interface to trunk or hybrid.

Precautions

The working mode of the voice VLAN on an interface does not affect the working mode of the voice VLAN on another interface. That is, voice VLANs on different interfaces can adopt different working modes.

Example

On GE0/0/1, configure the voice VLAN to work in manual mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] voice-vlan 10 enable
[HUAWEI-GigabitEthernet0/0/1] voice-vlan remark-mode mac-address
[HUAWEI-GigabitEthernet0/0/1] voice-vlan mode manual
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 10
```

5.7.8 voice-vlan remark

Function

The **voice-vlan remark** command changes the 802.1p priority and DSCP value for a voice VLAN.

The **undo voice-vlan remark** command restores the 802.1p priority and DSCP value to their default values for a voice VLAN.

By default, the 802.1p priority and DSCP value for a voice VLAN are 6 and 46 respectively.

Format

voice-vlan remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

undo voice-vlan remark { **8021p** | **dscp** } *

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority. The 802.1p priority is indicated by the value in the 3-bit PRI field in each 802.1Q VLAN frame. This field determines the transmission priority for data packets when a switching device is congested.	The value is an integer that ranges from 0 to 7. The default value 6. The larger the value, the higher the priority.

Parameter	Description	Value
dscp *dscp-value*	Specify the DSCP value. The DSCP value is indicated by the 6 bits in the ToS field in the IPv4 packet header. DSCP, as the signaling for DiffServ, is used for QoS guarantee on IP networks. The traffic controller on the network gateway takes actions merely based on the information carried by the 6 bits.	The value is an integer that ranges from 0 to 63. The default value is 46.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When voice VLAN is deployed on a network, voice service must be transmitted with a shorter delay than data service. Therefore, voice data packets need to be transmitted with a higher priority than other service data packets to reduce the transmission delay. You can run the **voice-vlan remark** command to change the 802.1p and DSCP priorities of a voice VLAN to allow voice data packets to be transmitted with a high priority.

Precautions

The **voice-vlan** *vlan-id* **enable** command has been run on an interface to specify a VLAN as a voice VLAN, and the voice VLAN function has been enabled on the interface.

If the **voice-vlan remark** command has been run multiple times, the last configuration overrides the previous configurations.

When the **remark** and **voice-vlan remark** commands are used together to modify the user packet priority, if the services conflict:

- For S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the priority configured using the **remark** command takes effect.
- For S6720-EI, S6720S-EI, the priority configured using the **voice-vlan remark** command takes effect.

Example

Set the DSCP value for a voice VLAN to 20.

```
<HUAWEI> system-view
[HUAWEI] voice-vlan remark dscp 20
```

5.7.9 voice-vlan remark-mode

Function

The **voice-vlan remark-mode** command configures a mode to increase the priority of voice packets.

The **undo voice-vlan remark-mode** command restores the default configuration.

By default, the priority of voice packets is increased based on VLAN IDs.

Format

voice-vlan remark-mode { **vlan** | **mac-address** }

undo voice-vlan remark-mode

Parameters

Parameter	Description	Value
vlan	Specifies that the priority of voice packets is increased based on VLAN IDs.	-
mac-address	Specifies that the priority of voice packets is increased based on MAC addresses.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After voice VLAN is enabled on an interface, the device determines whether a data flow consists of voice packets based on the VLAN ID by default. In this situation, even if you do not run the **voice-vlan mac-address** command to configure the OUI of the voice VLAN, you can use the voice VLAN function. Therefore, the voice VLAN configuration is more flexible and simple. Specifically, you can configure voice VLAN in the following methods:

- If you want to increase the priority of voice packets based on MAC addresses, run the **voice-vlan remark-mode mac-address** and **voice-vlan mac-address** commands.
- If you want to increase the priority of voice packets based on VLAN IDs, run the **voice-vlan remark-mode vlan** command.

Prerequisites

Voice VLAN has been enabled on the interface using the **voice-vlan enable** command.

Example

Configure GE0/0/1 to increase the priority of voice packets based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan remark-mode mac-address
```

5.7.10 voice-vlan security enable

Function

The **voice-vlan security enable** command enables the secure mode of the voice VLAN.

The **undo voice-vlan security enable** command disables the secure mode of the voice VLAN.

By default, the secure mode of the voice VLAN is disabled.

Format

voice-vlan security enable

undo voice-vlan security enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the data filtering mechanism, a voice VLAN works in either secure or normal mode:

- Secure mode

  A voice VLAN-enabled inbound port transmits only frames of which the source MAC addresses match OUIs configured on the device, discards the voice data not belong to the current voice VLAN and the other data can be forwarded normally.

The secure mode prevents a voice VLAN from being attacked by malicious data flows, but consumes system resources to check frames.

NOTE

The secure mode takes effect only when the **voice-vlan remark-mode mac-address** command is configured to increase the priority of voice packets based on MAC addresses.

- Normal mode

  A voice VLAN-enabled inbound port transmits both voice and non-voice data. The port does not compare source MAC addresses in received frames with configured OUIs, exposing a voice VLAN to malicious attacks.

Pre-configuration Tasks

Voice VLAN has been enabled using the **voice-vlan enable** command.

Run the **voice-vlan remark-mode mac-address** command to increase the priority of voice packets based on MAC addresses.

Precautions

When a voice VLAN works in secure mode, only voice packets in the VLAN can be transmitted in the voice VLAN.

To allow both voice packets and data packets to be transmitted in the voice VLAN, configure the voice VLAN to work in normal mode.

Example

Disable the secure mode of the voice VLAN on GigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] voice-vlan remark-mode mac-address
[HUAWEI-GigabitEthernet0/0/1] undo voice-vlan security enable
```

5.8 QinQ Configuration Commands

5.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.8.2 add-tag vlan-id

Function

The **add-tag vlan-id** command configures an action of adding an outer VLAN tag in a traffic behavior.

The **undo add-tag** command deletes the action.

By default, no action of adding an outer VLAN tag is configured in a traffic behavior.

NOTE

Only the S5735S-H, S5736-S, and S6720S-S support this command.

Format

add-tag vlan-id *vlan-id*

undo add-tag

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID in the outer VLAN tag.	The value is an integer that ranges from 1 to 4094.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the downstream device needs to provide services based on the outer VLAN tag, run the **add-tag vlan-id** command to configure the device to add an outer VLAN tag to packets matching the traffic classifier.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of adding an outer VLAN tag.

Precautions

- After the **add-tag vlan-id**, **remark 8021p**, **remark cvlan-id** or **remark vlan-id** command is used, the system modifies the VLAN tag of packets according to its configuration. The behavior configured through these commands is called VLAN-based action.

  To apply a VLAN-based action and a non-VLAN-based action to the same upstream traffic policy, configure the VLAN-based action and non-VLAN-based action in different traffic behaviors bound to the same traffic policy.
- In the scenario where a traffic policy is bound to multiple pairs of traffic classifiers and traffic behaviors, a traffic behavior contains **add-tag vlan-id**,

and a traffic classifier bound to another traffic behavior that does not define any VLAN-specific actions defines **if-match vlan-id**, the VLAN ID specified by **add-tag vlan-id** is matched. If another traffic behavior defines **if-match cvlan-id**, the VLAN ID in the packets is matched.

- The **add-tag vlan-id** command is invalid for double-tagged VLAN packets.
- When **port vlan-stacking**, **port vlan-stacking untagged**, or **port link-type dot1q-tunnel** is configured on an interface to add a VLAN tag to packets so that packets carry double VLAN tags, the **add-tag vlan-id** command is invalid for the double-tagged VLAN packets.
- If you run the **add-tag vlan-id** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure an action of adding an outer VLAN tag for traffic behavior **tb** to 100.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior tb
[HUAWEI-behavior-tb] add-tag vlan-id 100
```

5.8.3 display spare-bucket resource

Function

The **display spare-bucket resource** command displays the usage of backup resources when VLAN translation resources conflict.

Format

display spare-bucket resource [**slot** *slot-number*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
slot *slot-number*	Specifies the slot ID where the usage of backup resources is displayed.	The value is an integer and must be the ID of an existing slot on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays the usage of backup VLAN translation resources, including the total number of backup VLAN translation resources, and the numbers of used and remaining backup VLAN translation resources. The command output helps you manage backup VLAN translation resources and locate the problem of ineffective VLAN mapping due to insufficient resources.

When no slot ID is specified, the usage of backup VLAN translation resources in all slots is displayed.

Example

Display the usage of backup VLAN translation resources in slot 0.

```
<HUAWEI> display spare-bucket resource slot 0
--------------------------------------------------------------
 Slot               Used          Free          Total
--------------------------------------------------------------
 0                  0            66            66
```

Table 5-59 Description of the **display spare-bucket resource** command output

Item	Description
Slot	Slot ID
Used	Number of used backup VLAN translation resources.
Free	Number of remaining backup VLAN translation resources.
Total	Total number of backup VLAN translation resources.

5.8.4 display vlan-translation resource

Function

The **display vlan-translation resource** command displays VLAN translation resource usage.

Format

display vlan-translation resource [**slot** *slot-number*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
slot *slot-number*	Displays VLAN translation resource usage in a specified slot.	The value is an integer and must be an existing slot on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display vlan-translation resource** command displays VLAN translation resource usage, including the total number of inbound/outbound VLAN translation resources, the number of used VLAN translation resources, and the number of remaining VLAN translation resources. The command output helps you manage VLAN translation resources, and locate faults of insufficient VLAN translation resources caused by VLAN Mapping or Selective QinQ.

Example

Display VLAN translation resource usage.

```
<HUAWEI> display vlan-translation resource slot 0
 Interface:
   GigabitEthernet0/0/1 to GigabitEthernet0/0/48
-------------------------------------------------
 Type      Total      Configured      Remaining
-------------------------------------------------
 Ingress   65536      0               65536
 Egress    65536      0               65536
```

Table 5-60 Description of the display vlan-translation resource command output

Item	Description
Interface	Interface where VLAN translation is performed.
Type	VLAN translation resource type, which can be **Ingress** or **Egress**.
Total	Total number of VLAN translation resources.
Configured	Number of used VLAN translation resources.
Remaining	Number of remaining VLAN translation resources.

5.8.5 port add-tag acl

Function

The **port add-tag acl** command adds an outer tag to the packet that matches an ACL rule on an interface.

The **undo port add-tag acl** command cancels the configuration.

By default, the device does not add an outer tag to the packet that matches an ACL rule.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

port add-tag acl { *acl-number* | **name** *acl-name* } [**rule** *rule-id*] **vlan** *vlan-id* { **priority-inherit** | **remark-8021p** *8021p-value* }

undo port add-tag acl { *acl-number* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

port add-tag acl *l2-acl* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | **name** *acl-name* } [**rule** *rule-id*]] **vlan** *vlan-id* { **priority-inherit** | **remark-8021p** *8021p-value* }

port add-tag acl { *basic-acl* | *advance-acl* } [**rule** *rule-id*] [**acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]] **vlan** *vlan-id* { **remark-8021p** *8021p-value* | **priority-inherit** }

port add-tag acl name *acl-name* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]] **vlan** *vlan-id* { **remark-8021p** *8021p-value* | **priority-inherit** }

undo port add-tag acl *l2-acl* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | **name** *acl-name* } [**rule** *rule-id*]]

undo port add-tag acl { *basic-acl* | *advance-acl* } [**rule** *rule-id*] [**acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]]

undo port add-tag acl name *acl-name* [**rule** *rule-id*] [**acl** { *basic-acl* | *advance-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 4999. The value ranges of different types of ACLs are as follows: ● The value of a basic ACL ranges from 2000 to 2999. ● The value of an advanced ACL ranges from 3000 to 3999. ● The value of a Layer 2 ACL ranges from 4000 to 4999.
rule-id	Specifies the ID of an ACL rule.	The value of an IPv4 ACL ranges from 0 to 4294967294. ● When the rule ID is specified and the rule associated with the rule ID exists, the new rule takes effect. ● If the rule associated with the rule ID does not exist, you can create a rule with a specified rule ID and add the rule according to the rule ID. **NOTE** The number of ACL rules assigned automatically by the device starts from the step. The default step is 5. With this step, the device creates ACL rules with the numbers of 5, 10, 15, and so on.
name *acl-name*	Specifies a named ACL.	The value must the name of an existing ACL.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
l2-acl	Specifies the number of a Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
basic-acl	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
advance-acl	Specifies the number of an advance ACL.	The value is an integer that ranges from 3000 to 3999.
priority-inherit	Indicates that the outer VLAN tag inherits the priority in the inner VLAN tag.	-
remark-8021p *8021p-value*	Specifies the re-marked priority of the added outer VLAN tag. *8021p-value* specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, MultiGEinterface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device interface adds the specified outer tag to a packet based on the VLAN tag, MAC address, IP protocol, source address, destination address, priority, or port number of an application of a user.

Precautions

- After you run the **port add-tag acl** command, the following situations may occur:
  - The device does not take the original forwarding action to forward the packet that matches an ACL rule. Instead, the device adds an outer tag to the packet and forwards the packet in the VLAN specified by the added outer tag.
  - The device adds an outer tag to the packet that does not match an ACL rule based on the default VLAN of an interface.

- A Layer 2 ACL and a Layer 3 ACL can be set in the **port add-tag acl** command simultaneously. The Layer 3 ACL and its rules can be configured only after the Layer 2 ACL and its rules are configured. The Layer 2 ACL number ranges from 4000 to 4999 and the Layer 3 ACL number ranges from 2000 to 2999 and 3000 to 3999.
- This command is invalid for packets tagged with VLAN 0. If packets tagged with VLAN 0 need to be processed, configure a traffic policy on the switch.
- For the S6735-S, The **port add-tag acl** command is invalid for double-tagged VLAN packets.

Example

Add the outer tag of VLAN 1001 to the packet that matches the source IP address of 192.168.0.0/16 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl name test 2000
[HUAWEI-acl-basic-test] rule 1 permit source 192.168.0.0 0.0.255.255
[HUAWEI-acl-basic-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan all
[HUAWEI-GigabitEthernet0/0/1] port add-tag acl 2000 rule 1 vlan 1001 priority-inherit
```

5.8.6 port vlan-stacking

Function

The **port vlan-stacking** command configures VLAN stacking.

The **undo port vlan-stacking** command cancels the configuration.

By default, VLAN stacking is not configured.

Format

port vlan-stacking vlan *vlan-id1* [**to** *vlan-id2*] **stack-vlan** *vlan-id3* [**remark-8021p** *8021p-value1*]

port vlan-stacking vlan *vlan-id1* **stack-vlan** *vlan-id3* [**remark-8021p** *8021p-value1*] **map-vlan** *vlan-id4* [**remark-inner-8021p** *8021p-value2*]

undo port vlan-stacking vlan *vlan-id1* [**to** *vlan-id2*] [**stack-vlan** *vlan-id3*]

undo port vlan-stacking all

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the VLAN ID in a received tagged frame. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be larger than the value of *vlan-id1*. *vlan-id1* and *vlan-id2* identify a VLAN range.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
stack-vlan *vlan-id3*	Specifies the outer VLAN ID added to a frame.	The value is an integer that ranges from 1 to 4094.
remark-8021p *8021p-value1*	Specifies the re-marked 802.1p priority in the outer tag added to a frame.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
map-vlan *vlan-id4*	Specifies the mapped VLAN ID in the stacked inner tag.	The value is an integer that ranges from 1 to 4094.
remark-inner-8021p *8021p-value2*	Specifies the re-marked 802.1p priority in the mapped inner tag.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
all	Deletes all VLAN stacking configurations on the interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN stacking, also called selective QinQ, is a Layer 2 technology that enables a device to add outer VLAN tags based on VLAN IDs.

When frames are transmitted on the ISP network, the frames are differentiated based on user applications, access sites, or access devices. A device enabled with VLAN stacking adds outer tags to user frames based on the inner tags or priorities in the user frames so that traffic from different users are differentiated. A VLAN stacking interface has the following features:

- A VLAN stacking port can be configured with multiple outer VLAN tags so that the port can add different outer VLAN tags to different VLAN frames.
- A VLAN stacking interface can add the outer tag to received frames. After an interface joins the stacked VLAN in untagged mode, the interface removes the outer tag from outgoing frames.

When a network edge device needs to act as a user-side device and the received single-tagged packets are from one type of service, the same service from different users needs to be sent in different VLANs. That is, 1:1 VLAN mapping is implemented. After mapped VLAN tags enter the carrier network, VLAN stacking needs to be enabled on the network edge device to distinguish different users and services, because the number of VLANs that can be provided by the carrier network is limited. In addition, specified tags need to be added to packets of different users and services. Outer tags are the same as those provided by the carrier network and can be transmitted over the carrier network, and inner tags are transparently transmitted over the carrier network, enabling communication between different users. You need to run the **port vlan-stackingvlan***vlan-id1***stack-vlan***vlan-id2* [**remark-8021p***8021p-value1*] **map-vlan***vlan-id4* [**remark-inner-8021p***8021p-value2*] command to enable both VLAN mapping and VLAN stacking functions. **remark-8021p***8021p-value1* and **remark-inner-8021p***8021p-value2* specify 802.1p priorities of inner and outer VLAN tags.

If you want to implement both VLAN mapping and VLAN stacking, you cannot enable them separately by running the corresponding commands. This is because the VLAN ID that is mapped based on VLAN mapping cannot be mapped again based on VLAN stacking. For example, if **port vlan-stacking vlan 210 stack-vlan 2010** and **port vlan-mapping vlan 10 map-vlan 210** are configured on a device, the device maps VLAN 10 to VLAN 210 based on **port vlan-mapping vlan 10 map-vlan 210**. However, VLAN 210 after mapping will not be mapped to VLAN 2010 based on **port vlan-stacking vlan 210 stack-vlan 2010**. To implement both VLAN stacking and VLAN mapping, run the **port vlan-stacking vlan***vlanid1***stack-vlan***vlanid2***map-vlan***vlanid3* command.

When **remark-8021p** *8021p-value* is not specified:

- On the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, the 802.1p priority in the outer VLAN tag is the same as the interface priority. If **trust 8021p** is configured on the interface, the 802.1p priority in the outer VLAN tag is the same as the 802.1p priority in the inner VLAN tag.
- On other models, the 802.1p priority in the outer VLAN tag is the same as the 802.1p priority in the inner VLAN tag.

Precautions

When you configure selective QinQ, note the following points:

- Selective QinQ is recommended to be enabled on a hybrid interface. Selective QinQ can take effect on the interface only in the inbound direction.
- The outer VLAN must be created before VLAN stacking is performed.
- When an interface configured with VLAN stacking needs to remove the outer tag from outgoing frames, the interface must join the VLAN specified by **stack-vlan** in untagged mode. If the outer VLAN does not need to be removed, the interface must join the VLAN specified by **stack-vlan** in tagged mode.
- When **map-vlan** *vlan-id4* is configured to perform VLAN stacking and VLAN mapping concurrently, on switches other than the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, the same outer VLAN tag cannot be added to packets from different user VLANs. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, the same outer VLAN tag cannot be added to packets from different user VLANs, and different inner VLAN tags in packets from different user VLANs cannot be matched to the same VLAN tag. For example, if packets containing VLAN IDs 10 and 20 respectively are received on an interface, the **port vlan-stacking vlan 10 stack-vlan 100 map-vlan 200** and **port vlan-stacking vlan 20 stack-vlan 100 map-vlan 200** commands cannot be configured together.
- On the S6735-S, the **qinq protocol** and **port vlan-stacking** commands cannot be run simultaneously on an interface.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after the **port vlan-stacking** command is run on an interface, IP packets cannot be forwarded on the interface.
- On the S6735-S, after the **port vlan-stacking** command is run on an interface, the inner VLAN tag of packets is not removed and the outer VLAN tag is replaced during Layer 3 forwarding.

Example

On GE0/0/1, configure selective QinQ and outer VLAN tag 100 to the tagged frames with the inner VLAN tags 10 to 13.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking vlan 10 to 13 stack-vlan 100
```

5.8.7 port vlan-stacking untagged

Function

The **port vlan-stacking untagged** command configures a device to add double VLAN tags to an untagged frame.

The **undo port vlan-stacking untagged** command cancels the configuration.

By default, the device does not add double tags to an untagged frame.

Format

port vlan-stacking untagged stack-vlan *vlan-id1* **stack-inner-vlan** *vlan-id2*

undo port vlan-stacking untagged

Parameters

Parameter	Description	Value
stack-vlan *vlan-id1*	Specifies the outer VLAN tag added to an untagged frame.	The value of *vlan-id1* is an integer that ranges from 1 to 4094.
stack-inner-vlan *vlan-id2*	Specifies the inner VLAN tag added to an untagged frame.	The value of *vlan-id2* is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If double tags need to be added to packets, two devices are required. The **port vlan-stacking untagged** command adds double tags to packets on one device or untagged packets received on a Layer 2 interface to differentiate services or users.

For outgoing packets:

- S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and S6720S-S:
  - Double-tagged packets: The switch removes tags, as long as the outer VLAN ID is matched (regardless of whether the inner VLAN ID is matched).
  - Single-tagged packets: If QinQ (doltq or VLAN stacking) is configured on the inbound interface and the outer VLAN ID in QinQ is the same as the outer VLAN ID specified by the **port vlan-stacking untagged stack-vlan** *vlan-id1* **stack-inner-vlan** *vlan-id2* command, the VLAN ID of outgoing packets is the VLAN ID of original packets.
- Other models: When only the outer VLAN ID is matched and the VLAN is configured on the interface in untagged mode, the outer VLAN tag is removed and the inner VLAN tag is reserved.

Precautions

To enable an interface to add double VLAN tags to an untagged packet, you need to set the link type of the interface to hybrid, and add the interface to the VLAN specified by **stack-vlan** on the S6720S-S, S5735S-H, S5736-S, S5720S-LI, S5720-LI, S5720I-SI. On other devices, you need to set the link type of the interface to hybrid or trunk, and add the interface to the VLAN specified by **stack-vlan**.

When the interface PVID is not VLAN 1, restore the PVID to VLAN 1 before the **port vlan-stacking untagged** command is executed.

Adding double VLAN tags to untagged frames is port-based VLAN assignment. Different VLAN assignment modes are in the following order of priority: policy-based VLAN assignment > MAC address-based VLAN assignment > IP subnet-based VLAN assignment > protocol-based VLAN assignment > interface-based VLAN assignment.

On the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S if the **port vlan-stacking untagged** *vlan-id1* **stack-inner-vlan** *vlan-id2* command is used on an interface, the VLAN specified by *vlan-id1* cannot be configured as the outer VLAN in the **port vlan-stacking** command.

If the **port vlan-stacking untagged** command is used on an interface, the interface processes the received packets with VLAN tag 0 as untagged packets.

Example

Add double VLAN tags to untagged frames received on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
 [HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
 [HUAWEI-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[HUAWEI-GigabitEthernet0/0/1] port vlan-stacking untagged stack-vlan 100 stack-inner-vlan 200
```

5.8.8 qinq mapping pe-vid ce-vid

Function

The **qinq mapping pe-vid ce-vid** command configures a sub-interface to map the outer VLAN tag of a frame.

The **undo qinq mapping pe-vid ce-vid** command cancels the configuration.

By default, VLAN mapping is not configured on a sub-interface.

Format

qinq mapping pe-vid *vlan-id1* **ce-vid** *vlan-id2* [**to** *vlan-id3*] **map-vlan vid** *vlan-id4*

undo qinq mapping pe-vid *vlan-id1* **ce-vid** *vlan-id2* [**to** *vlan-id3*] **map-vlan vid** *vlan-id4*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
pe-vid *vlan-id1*	Specifies the outer VLAN tag in a received frame.	The value is an integer that ranges from 2 to 4094.
ce-vid *vlan-id2* [**to** *vlan-id3*]	Specifies the inner VLAN tag in a received frame. ● *vlan-id2*: specifies the start inner VLAN tag. ● *vlan-id3*: specifies the end inner VLAN tag. ● The value of *vlan-id3* must be greater than or equal to the value of *vlan-id2*. *vlan-id2* and *vlan-id3* identify a VLAN range.	The value of *vlan-id2* is an integer that ranges from 1 to 4094. The value of *vlan-id3* is an integer that ranges from 1 to 4094.
map-vlan vid *vlan-id4*	Specifies the VLAN ID in the mapped outer tag.	The value is an integer that ranges from 1 to 4094.

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

QinQ mapping is generally deployed on edge devices of a metro Ethernet and often used to map the VLAN tag carried in a frame to a specified VLAN tag before the frame is transmitted on the public network. QinQ mapping can be applied to the following scenarios:

- The VLAN IDs deployed in new sites and old sites conflict, but new sites need to communicate with old sites.
- The VLAN ID planning of each site on the public network is different. As a result, the VLAN IDs conflict. However, the sites do not need to communicate.

- The VLAN IDs on both ends of the public network are different.

When a network edge device receives double-tagged frames, the inner tags indicate users and outer tags indicates services. To differentiate services on the ISP network, you can configure 2 to 1 QinQ mapping on network edge devices. The double tags of frames are mapped to a specified S-VLAN tag so that the outer tag can be transparently transmitted on the ISP network.

The **qinq mapping pe-vid ce-vid** command on a sub-interface has similar functions with the **port vlan-mapping vlan inner-vlan** command on the main interface. The differences are as follows:

- QinQ mapping on a sub-interface is mainly used to access the L2VPN.
- QinQ mapping used on the main interface is used for interconnection on the Layer 2 MAN so that users of different VLANs can communicate with each other.
- QinQ mapping saves a large number of physical ports.

Precautions

The **qinq mapping pe-vid ce-vid** command maps the outer VLAN tags of the frames on a sub-interface, but does not change the inner VLAN tags. This command takes effect for only incoming frames.

The original VLAN IDs specified for QinQ mapping on a sub-interface cannot be globally created or displayed by display commands.

VLAN mapping or VLAN stacking cannot be configured for the same VLAN on the main interface and its sub-interfaces.

The mapped VLAN IDs specified in QinQ mapping configuration must be different from the control VLAN IDs for ring protocols such as SEP, RRPP, and ERPS. Otherwise, an error message will be displayed, indicating that the configuration fails.

Example

On XGigabitEthernet0/0/1.1, set the outer VLAN tag 10 of frames with the inner VLAN tag 20 to outer VLAN tag 30.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq mapping pe-vid 10 ce-vid 20 map-vlan vid 30
```

5.8.9 qinq mapping vid map-vlan

Function

The **qinq mapping vid map-vlan** command configures 1 to 1 QinQ mapping on a sub-interface.

The **undo qinq mapping vid map-vlan** command cancels the configuration.

By default, 1 to 1 QinQ mapping is not configured on a sub-interface.

Format

qinq mapping vid *vlan-id1* [**to** *vlan-id2*] **map-vlan vid** *vlan-id3*

undo qinq mapping vid *vlan-id1* [**to** *vlan-id2*] **map-vlan vid** *vlan-id3*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
vid *vlan-id1* **to** *vlan-id2*	Specifies the VLAN ID of the tag carried in the received packet. ● *vlan-id1*: specifies the start inner VLAN tag. ● *vlan-id2*: specifies the end inner VLAN tag. ● The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. *vlan-id1* and *vlan-id2* identify a VLAN range.	*vlan-id1* is an integer that ranges from 2 to 4094. *vlan-id2* is an integer that ranges from 2 to 4094.
map-vlan vid *vlan-id3*	Specifies the VLAN ID in the mapped outer tag.	The value is an integer that ranges from 1 to 4094.

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

QinQ mapping is often deployed on edge devices of a metro Ethernet and is used to map the frames sent from the user side. The devices map the VLAN IDs in user packets to specified VLAN IDs before forwarding the packets to the public network. QinQ mapping can be applied to the following scenarios:

- The VLAN IDs deployed in new sites and old sites conflict, but new sites need to communicate with old sites.

- The VLAN ID planning of each site on the public network is different. As a result, the VLAN IDs conflict. However, the sites do not need to communicate.
- The VLAN IDs on both ends of the public network are different.

The **qinq mapping vid map-vlan** command on a sub-interface has similar functions with the **port vlan-mapping vlan inner-vlan** command on the main interface. The differences are as follows:

- QinQ mapping on a sub-interface is mainly used to access the L2VPN.
- QinQ mapping used on the main interface is used for interconnection on the Layer 2 MAN so that users of different VLANs can communicate with each other.
- QinQ mapping saves a large number of physical ports.

Precautions

The **qinq mapping vid map-vlan** command maps the single tags in frames on a sub-interface. This command takes effect only for incoming packets.

The original VLAN IDs specified for QinQ mapping on a sub-interface cannot be globally created or displayed by display commands.

VLAN mapping or VLAN stacking cannot be configured for the same VLAN on the main interface and its sub-interfaces.

The mapped VLAN IDs specified in QinQ mapping configuration must be different from the control VLAN IDs for ring protocols such as SEP, RRPP, and ERPS. Otherwise, an error message will be displayed, indicating that the configuration fails.

Example

Configure QinQ mapping on XGigabitEthernet0/0/1.1 to map outer VLAN tag 100 to inner VLAN tag 200.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq mapping vid 100 map-vlan vid 200
```

5.8.10 qinq protocol

Function

The **qinq protocol** command sets the TPID value in the outer VLAN tag of an interface.

The **undo qinq protocol** command restores the default TPID value in the outer VLAN tag.

By default, the TPID value in the outer VLAN tag is 0x8100.

Format

qinq protocol *protocol-id*

undo qinq protocol

Parameters

Parameter	Description	Value
protocol-id	Specifies the TPID value in the outer VLAN tag.	The value is a 4-digit hexadecimal integer that ranges from 0x0600 to 0xFFFF. The default TPID value is 0x8100.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable devices from different vendors to interoperate, set the same TPID value in outer VLAN tags on the devices. Devices from different vendors or in different network plans may use different Tag Protocol Identifier (TPID) values in VLAN tags of VLAN packets. The switch supports configuration of the TPID value in outer VLAN tags so that it can interoperate with devices from different vendors or operate seamlessly on an existing network.

Precautions

- In earlier versions of V200R010, this command can be configured on Eth-Trunk member interfaces but not the Eth-Trunk. In V200R010 and later versions, this command can be configured on the Eth-Trunk but not Eth-Trunk member interfaces.
- When the device is upgraded from an earlier version of V200R010 to V200R010 or later and the **qinq protocol** command is configured on Eth-Trunk member interfaces, the following situations may occur:
  - If the same **qinq protocol** command has been configured on all Eth-Trunk member interfaces, the **qinq protocol** command configuration takes effect on the Eth-Trunk after the upgrade.
  - If different **qinq protocol** commands are configured on Eth-Trunk member interfaces, the **qinq protocol** command configuration takes effect on the Eth-Trunk member interfaces after the upgrade and there is the configuration on the Eth-Trunk member interfaces. To configure the **qinq protocol** command in the Eth-Trunk interface view, first manually run the **undo qinq protocol** command on Eth-Trunk member interfaces to delete the configuration. In this situation, automatic completion of the

undo qinq protocol command is not supported. You must manually enter the **undo qinq protocol** command.

- The device directly connected to an interface must be able to identify the TPID value in the outer VLAN tag on the interface.
- On the S6735-S, the **qinq protocol** and **port vlan-stacking** commands cannot be run simultaneously on an interface.
- The **qinq protocol** command identifies incoming frames, and adds or changes the TPID value of outgoing frames.
- The **qinq protocol** command can also change the TPID value in the VLAN tag of a single-tagged packet.
- The TPID value specified by the **qinq protocol** command must be different from TPID values of specific protocols. Otherwise, the interface cannot correctly classify protocol packets. The TPID value cannot be any of the values in the following table.

Table 5-61 Description of protocol types and values

Protocol Type	Value
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

Example

Set the TPID value in the outer VLAN tag of a QinQ frame to 0x9100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] qinq protocol 9100
```

5.8.11 qinq stacking

Function

The **qinq stacking** command configures VLAN stacking on a sub-interface.

The **undo qinq stacking** command cancels the configuration.

By default, VLAN stacking is not configured on a sub-interface.

Format

qinq stacking vid *vlan-id1* [**to** *vlan-id2*] **pe-vid** *vlan-id3*

undo qinq stacking vid *vlan-id1* [**to** *vlan-id2*] **pe-vid** *vlan-id3*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this configuration.

Parameters

Parameter	Description	Value
vid *vlan-id1* [**to** *vlan-id2*]	Specifies the outer VLAN ID range. - *vlan-id1* specifies the start VLAN ID. - **to***vlan-id2* specifies the end VLAN ID. The *vlan-id1* and *vlan-id2* id value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*entify a VLAN range.	The value of *vlan-id1* is an integer that ranges from 2 to 4094. The value of *vlan-id2* is an integer that ranges from 2 to 4094.
pe-vid *vlan-id3*	Specifies the outer VLAN tags added to a frame.	The value is an integer that ranges from 1 to 4094.

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **qinq stacking** command adds an outer VLAN tag to the packets on a sub-interface.

Precautions

- The original VLAN IDs specified for QinQ mapping on a sub-interface cannot be globally created or displayed by display commands.
- VLAN mapping or VLAN stacking cannot be configured for the same VLAN on the main interface and its sub-interfaces.
- When a QinQ stacking sub-interface receives a packet, the interface checks whether the packet carries a VLAN tag. If not, the packet is directly dropped. If the packet carries one or two VLAN tags, the interface processes the packet as follows:
  - If the packet carries one VLAN tag and the VLAN ID in the tag matches the VLAN range specified by **vid** *vlan-id1* [**to** *vlan-id2*] in the **qinq stacking vid** command, the interface adds an outer VLAN tag with a VLAN ID in the specified range to the packet. If the VLAN ID in the tag carried by the packet does not match the specified VLAN range, the packet is dropped.
  - If the packet carries two VLAN tags and the VLAN ID in the outer VLAN tag matches the VLAN range specified by **vid** *vlan-id1* [**to** *vlan-id2*] in the **qinq stacking vid** command, the interface adds another outer VLAN tag with a VLAN ID in the specified range to the packet and forwards the packet. In this case, the inner VLAN tag is transmitted transparently. If the VLAN ID in the outer VLAN tag carried by the packet does not match the specified VLAN range, the packet is dropped.

Example

Configure VLAN stacking on XGigabitEthernet0/0/1.1 and add an outer VLAN tag 100 to frames with the inner VLAN tags 10 to 13.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-XGigabitEthernet0/0/1] quit
[HUAWEI] interface xgigabitethernet 0/0/1.1
[HUAWEI-XGigabitEthernet0/0/1.1] qinq stacking vid 10 to 13 pe-vid 100
```

5.8.12 qinq stacking vlan

Function

The **qinq stacking vlan** command configures QinQ stacking on a VLANIF interface.

The **undo qinq stacking vlan** command cancels the configuration.

By default, QinQ stacking is not configured on a VLANIF interface.

Format

qinq stacking vlan *vlan-id*

undo qinq stacking vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the outer VLAN tag added to a frame.	The value is an integer that ranges from 1 to 4094.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Assume that the local device A is connected to the remote device B over the ISP network.

The ID of the management VLAN on device B is the same as the ID of VLAN for users connected to device A. However, the S-VLAN ID is different from the management VLAN ID.

To log in to device B to manage it from local device A, you can use the qinq stacking vlan command on device B to configure QinQ stacking on the VLANIF interface corresponding to the management VLAN. In addition, you need to configure QinQ on the user-side interface of device A.

- Packets sent from device A to device B are processed as follows:

  The user-side interface of device A sends double-tagged packets to the ISP network. The outer VLAN tag is assigned by the carrier so that the packets can be transparently transmitted over the ISP network to SwitchB.

  When device B receives double-tagged packets, it compares the VLAN tags of the packets with the VLAN tags configured on the VLANIF interface. If the outer tag of the packets is the same as the outer tag configured on the VLANIF interface, device B removes the outer tag and sends the packets to the IP layer for processing.
- Packets sent from device B to device A are processed as follows:

  When the VLANIF interface of SwitchB receives data packets, device B adds a VLAN tag to the packets according to the QinQ stacking configuration. The new outer VLAN tag is assigned by the carrier so that the double-tagged data packets can be transparently transmitted across the ISP network to device A. Device A removes the outer VLAN tag, and then forwards the packets to users.

NOTE

- When configuring QinQ stacking on a VLANIF interface, ensure that the VLANIF interface corresponds to the management VLAN. VLANIF interfaces corresponding to other VLANs do not support QinQ stacking.
- To change the configured outer VLAN, run the **undo qinq stacking vlan** command to disable QinQ stacking, and then run the **qinq stacking vlan** command to configure a new outer VLAN.
- The **qinq stacking vlan** command conflicts with the **icmp host-unreachable send** command. Therefore, you must run the **undo icmp host-unreachable send** command before using the **qinq stacking vlan** command.
- The outer VLAN added to packets must be an existing VLAN without VLANIF interface configured.

Example

Configure QinQ stacking on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] management-vlan
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] undo icmp host-unreachable send
[HUAWEI-Vlanif10] qinq stacking vlan 20
```

5.8.13 qinq vlan-translation enable

Function

The **qinq vlan-translation enable** command enables VLAN translation on an interface.

The **undo qinq vlan-translation enable** command disables VLAN translation on an interface.

By default, VLAN translation is disabled on an interface.

Format

qinq vlan-translation enable

undo qinq vlan-translation enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

You can configure VLAN mapping and selective QinQ on an interface only after VLAN translation is enabled on it.

Example

Enable VLAN translation on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
```

5.8.14 qinq vlan-translation miss-drop

Function

The **qinq vlan-translation miss-drop** command configures an interface to discard the packets that do not match any VLAN Stacking, VLAN mapping, and entry.

The **undo qinq vlan-translation miss-drop** command cancels the configuration.

By default, an interface does not discard the packets that do not match any VLAN Stacking, VLAN mapping, and entry.

NOTE

This command does not take effect for untagged packets.

Format

qinq vlan-translation miss-drop

undo qinq vlan-translation miss-drop

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After VLAN Stacking and VLAN mapping, are configured on an interface, you can run the **qinq vlan-translation miss-drop** command to configure the interface to discard the received packets that do not match any VLAN Stacking, VLAN mapping, and entry.

Example

Configure GE0/0/1 to discard the packets that do not match any VLAN Stacking, VLAN mapping, and entry.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation miss-drop
```

5.9 VLAN Mapping Configuration Commands

5.9.1 Command Support

Table 5-62 Products supporting the function of VLAN mapping

VLAN Mapping Mode	Supported Model
1:1 mode for 1 to 1 VLAN mapping	All models.
N:1 mode for 1 to 1 VLAN mapping	S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735-S, S500, S5735-S-I, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-S, S6735-S, S6720-EI, S6720S-S, S6720S-EI, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S
1:1 mode for 2 to 1 VLAN mapping	S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S
N:1 mode for 2 to 1 VLAN mapping	S6735-S, S6720-EI, S6720S-S, S5736-S, S5735S-H S6720S-EI, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S
2 to 2	S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

5.9.2 port vlan-mapping ingress

Function

The **port vlan-mapping ingress** command configures VLAN mapping in the inbound direction.

The **undo port vlan-mapping ingress** command cancels the configuration.

By default, VLAN mapping is valid for both inbound and outbound directions.

NOTE

This command is only supported by S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S.

Format

port vlan-mapping ingress

undo port vlan-mapping ingress

Parameters

None

Views

Ethernet interface view, GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **port vlan-mapping vlan** *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*] command is used on an interface, *vlan-id1* [**to** *vlan-id2*] is mapped to *vlan-id3* in the inbound direction, and *vlan-id3* is mapped to *vlan-id1* [**to** *vlan-id2*] in the outbound direction.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, outbound VLAN mapping cannot be used with a traffic policy containing CAR. You can run the **port vlan-mapping ingress** command to configure VLAN mapping in the inbound direction. The interface configured with VLAN mapping maps *vlan-id1* [**to** *vlan-id2*] to *vlan-id3* in the inbound direction, and does not map *vlan-id3* to *vlan-id1* [**to** *vlan-id2*] in the outbound direction.

Prerequisites

The **qinq vlan-translation enable** command has been executed.

Precautions

To make VLAN mapping take effect in the inbound direction only, configure the **port vlan-mapping ingress** and **port vlan-mapping vlan map-vlan** commands in sequence. To delete the VLAN mapping configuration, delete the **port vlan-mapping vlan map-vlan** and **port vlan-mapping ingress** commands in sequence.

Example

Configure VLAN mapping in the inbound direction on GE0/0/1 to map VLAN 100 in received frames to VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping ingress
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 100 map-vlan 10
```

5.9.3 port vlan-mapping vlan inner-vlan

Function

The **port vlan-mapping vlan inner-vlan** command enables the interface to replace the outer VLAN tag or both VLAN tags of a double-tagged packet.

The **undo port vlan-mapping vlan inner-vlan** command disables the interface to replace the outer VLAN tag or both VLAN tags of a double-tagged packet.

By default, the interface does not map tags of packets.

NOTE

Only the S6735-S, S6720-EI, S6720S-EI, S6720S-S, S5736-S, S5735S-H, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, S5731S-S support this command.

Format

port vlan-mapping vlan *vlan-id1* **inner-vlan** *vlan-id2* [**to** *vlan-id3*] **map-vlan** *vlan-id4* [**remark-8021p** *8021p-value*]

port vlan-mapping vlan *vlan-id1* **inner-vlan** *vlan-id2* **map-vlan** *vlan-id4* [**map-inner-vlan** *vlan-id5*] [**remark-8021p** *8021p-value*]

undo port vlan-mapping { **all** | **vlan** *vlan-id1* **inner-vlan** *vlan-id2* [**to** *vlan-id3*] [**map-vlan** *vlan-id4*] }

undo port vlan-mapping vlan *vlan-id1* **inner-vlan** *vlan-id2* **map-vlan** *vlan-id4* **map-inner-vlan** *vlan-id5*

Parameters

Parameter	Description	Setting
vlan *vlan-id1*	Specifies the VLAN ID of the outer tag in a received packet.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Setting
inner-vlan *vlan-id2* [**to** *vlan-id3*]	Specifies the VLAN ID of the inner tag in a received packet. ● *vlan-id2*: specifies the start value of the VLAN ID range of the inner tag in the received packet. ● *vlan-id3*: specifies the end value of the VLAN ID range of the inner tag in the received packet. *vlan-id3* is optional. The value of *vlan-id3* must be greater than that of *vlan-id2*.	The value of *vlan-id2* or *vlan-id3* is an integer that ranges from 1 to 4094.
map-vlan *vlan-id4*	Specifies the VLAN ID that replaces the VLAN ID of the outer tag in a packet.	The value is an integer that ranges from 1 to 4094.
map-inner-vlan *vlan-id5*	Specifies the VLAN ID that replaces the VLAN ID of the inner tag in a packet. If the parameter **map-inner-vlan** is configured, the interface maps the VLAN ID of the inner tag in the packet to the value of *vlan-id5* specified by users.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Setting
remark-8021p *8021p-value*	Specifies the re-marked 802.1p priority of the outer tag. The 802.1p priority is specified by a 3-bit PRI (priority) field in an 802.1Q packet. When congestion occurs on a switch, packets with a higher priority are sent first. If the parameter **remark-8021p** is configured, the interface changes the 802.1p priority in the packet to the value of *8021p-value* specified by users.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
all	Specifies all VLAN mapping entries configured on the primary interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, MultiGE interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When provider edges (PEs) receive double-tagged packets, the inner tag in the packets indicates the user, and the outer tag indicates the service. To differentiate services entering the ISP network, you can configure 2 to 1 VLAN mapping on PEs. To allow users to communicate with each other, the interface maps tags of different services to outer tags, and inner tags are transparently transmitted to the ISP network.

This command allows an interface to map the VLAN ID in a tagged packet to an S-VLAN ID.

Precautions

VLAN mapping can only be configured on trunk or hybrid ports. Hybrid ports on switches except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S must be added to the mapped VLAN in tagged mode. On the S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if a trunk port is added to the mapped VLAN in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

Interfaces configured with N:1 VLAN mapping must be added to the original VLAN in tagged mode. On switches except the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730-S, S6730S-S, and S6730S-H, if a trunk port is configured with N:1 VLAN mapping and its PVID is the mapped VLAN ID or it is added to mapped VLANs in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

When **inner-vlan** is set to a VLAN ID range, the interface cannot replace the VLAN ID of the inner tag in packets.

If VLAN mapping and DHCP are configured on the same interface, the interface must be added to the original VLANs (VLANs before mapping) in tagged mode.

When the VLAN tags of a packet match both a single-tag VLAN mapping entry and a double-tag VLAN mapping entry, the double-tag VLAN mapping takes effect.

If DHCP snooping is enabled on the device, do not configure 2:2 VLAN mapping. Otherwise, DHCP users cannot go online.

For the S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first and MAC address learning is enabled on interfaces and in VLANs. If packets are sent from an S-VLAN first or MAC address learning is disabled on interfaces or in VLANs, the C-VLAN to be mapped cannot be determined because no VLAN mapping information is recorded in MAC address entries. As a result, the packets are discarded. In addition, VLAN mapping cannot be configured together with VPLS or VXLAN tunnels.For the others, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first. In this case, if packets are sent from an S-VLAN first, the C-VLAN to be mapped cannot be determined because no ACL entry is generated. As a result, the packets are discarded.

Example

Configure 2 to 1 VLAN mapping, map VLAN 10 in the outer tag of a packet (with VLAN 10 in the outer tag and VLAN 20 in the inner tag) to VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 10 inner-vlan 20 map-vlan 100
```

5.9.4 port vlan-mapping vlan map-vlan

Function

The **port vlan-mapping vlan map-vlan** command enables the interface to map single tags of packets.

The **undo port vlan-mapping** command cancels the interface to map single tags of packets.

By default, the interface does not map tags of packets.

Format

port vlan-mapping vlan *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*]

undo port vlan-mapping { **all** | **vlan** *vlan-id1* [**to** *vlan-id2*] [**map-vlan** *vlan-id3*]}

NOTE

N:1 VLAN mapping is supported on :

S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735-S, S500, S5735-S-I, S5735S-L, S5735S-L1, S5735S-L-M, S5735S-S, S6735-S, S6720-EI, S6720S-S, S6720S-EI, S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S

Parameters

Parameter	Description	Setting
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the VLAN ID in a received packet. • *vlan-id1*: specifies the start value of the VLAN ID range of the tag. • **to** *vlan-id2*: specifies the end value of the VLAN ID range of the tag. The value of *vlan-id2* must be greater than that of *vlan-id1*.	The value of *vlan-id1* or *vlan-id2* is an integer that ranges from 1 to 4094.
map-vlan *vlan-id3*	Specifies the VLAN ID in the mapped tag.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Setting
remark-8021p *8021p-value*	Specifies the re-marked 802.1p priority of the mapped tag. The 802.1p priority is specified by a 3-bit PRI (priority) field in an 802.1Q packet. When congestion occurs on a switch, packets with a higher priority are sent first. If the parameter **remark-8021p** is configured, the interface changes the 802.1p priority in the packet to the value of *8021p-value* specified by users.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
all	Specifies all VLAN mapping entries configured on the interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN mapping, also called VLAN translation, implements communication between different VLANs. VLAN mapping takes effect after outbound interfaces on a switch forward the packets received by inbound interfaces. This command allows an interface to map the VLAN ID in a tagged packet to an S-VLAN ID.

After the **port vlan-mapping vlan** *vlan-id1* [**to** *vlan-id2*] **map-vlan** *vlan-id3* [**remark-8021p** *8021p-value*] command is used on an interface, *vlan-id1* [**to** *vlan-id2*] is mapped to *vlan-id3* in the inbound direction, and *vlan-id3* is mapped to *vlan-id1* [**to** *vlan-id2*] in the outbound direction.

Precautions

VLAN mapping can only be configured on trunk or hybrid ports. Hybrid ports on switches except the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S must be added to the mapped VLAN in tagged mode. On the S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if a trunk port is added to the mapped VLAN in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

Interfaces configured with N:1 VLAN mapping must be added to the original VLAN in tagged mode. On switches except the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730-S, S6730S-S, and S6730S-H, if a trunk port is configured with N:1 VLAN mapping and its PVID is the mapped VLAN ID or it is added to mapped VLANs in untagged mode, the port forwards reverse traffic without VLAN tags. As a result, VLAN mapping may not take effect.

When N:1 VLAN mapping is configured (VLAN IDs can be incontiguous before mapping), the interface needs to be added to these VLANs in tagged mode, and the VLAN specified by **map-vlan** cannot be a VLAN corresponding to a VLANIF interface.

If VLAN mapping and DHCP are configured on the same interface, it is recommended to add the interface to the original VLANs (VLANs before mapping) in tagged mode.

For the S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first and MAC address learning is enabled on interfaces and in VLANs. If packets are sent from an S-VLAN first or MAC address learning is disabled on interfaces or in VLANs, the C-VLAN to be mapped cannot be determined because no VLAN mapping information is recorded in MAC address entries. As a result, the packets are discarded. In addition, VLAN mapping cannot be configured together with VPLS or VXLAN tunnels.For the others, N:1 VLAN mapping takes effect only when the packets with original VLANs are sent first. In this case, if packets are sent from an S-VLAN first, the C-VLAN to be mapped cannot be determined because no ACL entry is generated. As a result, the packets are discarded.

N:1 VLAN mapping is not supported in a stack scenario.

A maximum of 16 original VLAN IDs can be specified on an interface.

If the VLANs before and after mapping are the same, return packets may fail to be forwarded. To solve the problem, map the VLAN to itself. For example, packets with VLAN 10 and VLAN 20 (before mapping) need to be sent to the network side and S-VLAN 20 (after mapping) is assigned to users, run the **port vlan-mapping vlan 10 map-vlan 20** command. To ensure that return packets are correctly forwarded, run the **port vlan-mapping vlan 20 map-vlan 20** command.

The S6730-H, S6730-S, S6730S-S, S6730S-H, S5732-H, S5731-H, S5731S-H, S5731-S, and S5731S-S do not support N:1 VLAN mapping on Eth-Trunk interfaces.

Example

Configure VLAN mapping on the GE0/0/1 and map VLAN 100 of a received packet to VLAN 10 before the packet is forwarded.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] qinq vlan-translation enable
[HUAWEI-GigabitEthernet0/0/1] port vlan-mapping vlan 100 map-vlan 10
```

5.9.5 remark cvlan-id

Function

The **remark cvlan-id** command configures an action of re-marking the inner VLAN tag in QinQ packets in a traffic behavior.

The **undo remark cvlan-id** command deletes the configuration.

By default, an action of re-marking the inner VLAN tag in QinQ packets is not configured in a traffic behavior.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

remark cvlan-id *cvlan-id*

undo remark cvlan-id

Parameters

Parameter	Description	Value
cvlan-id	Specifies the inner VLAN tag of QinQ packets to be re-marked.	The value is an integer that ranges from 1 to 4094.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **remark cvlan-id** command to re-mark the inner VLAN tag in QinQ packets in a traffic behavior so that the downstream device can identify packets and provide differentiated services.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of re-marking the inner VLAN tag in QinQ packets.

Precautions

The **remark cvlan-id** command is valid for only QinQ packets that carry two or more layers of tags.

After the **remark cvlan-id**, **remark 8021p**, **add-tag vlan-id**, and **remark vlan-id** commands are used, the system modifies VLAN tags of packets according to the configuration. These actions are called VLAN-based actions.

You must configure the VLAN-based action and non-VLAN-based action in different traffic behaviors bound to the same traffic policy.

If you run the **remark cvlan-id** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Re-mark the inner VLAN tag in packets with 5 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark cvlan-id 5
```

5.9.6 remark vlan-id

Function

The **remark vlan-id** command configures an action of re-marking the VLAN tag in VLAN packets in a traffic behavior.

The **undo remark vlan-id** command deletes the configuration.

By default, an action of re-marking the VLAN tag in VLAN packets is not configured in a traffic behavior.

Format

remark vlan-id *vlan-id*

undo remark vlan-id

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN tag of packets in a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **remark vlan-id** command to re-mark the VLAN tag in VLAN packets in a traffic behavior so that the downstream device can identify packets and provide differentiated services.

The **remark vlan-id** command re-marks only the outer VLAN tag of double-tagged packets.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing VLAN tag re-marking.

Precautions

If the **remark vlan-id** command is used on an inbound interface, on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, add the outbound interfaces to the replaced VLAN and the original VLAN. Otherwise, packets cannot be forwarded correctly. On other models, add the inbound and outbound interfaces to the replaced VLAN and the original VLAN. Otherwise, packets cannot be forwarded correctly.

If a traffic policy containing **remark vlan-id** is applied to the outbound direction on an interface, the VLAN that the interface belongs to must work in tag mode.

After the **remark vlan-id**, **remark 8021p**, **remark cvlan-id** command is used, the system modifies the VLAN tag of packets based on the device configuration. The behavior configured through these commands is called VLAN-based action.

To perform VLAN-based actions and non-VLAN-based actions in an upstream traffic policy, you need to configure VLAN-based actions and non-VLAN-based actions in different traffic behaviors.

If you run the **remark vlan-id** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the VLAN tag of packets in a VLAN to 200.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior tb
[HUAWEI-behavior-tb] remark vlan-id 200
```

5.9.7 set inner-vlan tag0-remove

Function

The **set inner-vlan tag0-remove** command configures whether interfaces retain the inner VLAN tag 0 when forwarding double-tagged frames.

The **undo set inner-vlan tag0-remove disable** command restores the default configuration.

By default, interfaces remove the inner VLAN tag 0 when forwarding double-tagged frames.

NOTE

This command is supported only on the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S.

Format

set inner-vlan tag0-remove { **disable** | **enable** }

undo set inner-vlan tag0-remove disable

Parameters

Parameter	Description	Value
disable	Configures interfaces to retain the inner VLAN tag 0 when forwarding double-tagged frames.	-
enable	Configures interfaces to remove the inner VLAN tag 0 when forwarding double-tagged frames.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, a QinQ interface removes the inner VLAN tag 0 when forwarding double-tagged frames. You can run the **set inner-vlan tag0-remove disable** command to configure interfaces to retain the inner VLAN tag 0 when forwarding double-tagged frames.

Example

Configure interfaces to retain the inner VLAN tag 0 when forwarding double-tagged frames.

```
<HUAWEI> system-view
[HUAWEI] set inner-vlan tag0-remove disable
```

5.10 GVRP Configuration Commands

5.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.10.2 display garp statistics

Function

The **display garp statistics** command displays statistics about the Generic Attribute Registration Protocol (GARP) on an interface.

Format

display garp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about GARP on the specified interface. - *interface-type* specifies the type of an interface. - *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the GARP VLAN Registration Protocol (GVRP) is enabled on an interface, the system collects statistics about GVRP packets sent, received, and discarded on the interface. You can view the statistics to check whether the GVRP function on the interface is normal.

When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system displays statistics about GARP packets on all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system displays statistics about GARP packets on the specified interface.

Example

Display statistics about GARP packets on a specified interface.

```
<HUAWEI> display garp statistics interface gigabitethernet 0/0/1

 GARP statistics on port GigabitEthernet0/0/1
   Number of GVRP frames received       : 0
   Number of GVRP frames transmitted    : 0
   Number of frames discarded           : 0
```

Table 5-63 Description of the display garp statistics command output

Item	Description
Number of GVRP frames received	Number of GVRP packets received by an interface.
Number of GVRP frames transmitted	Number of GVRP packets sent by an interface.
Number of frames discarded	Number of packets discarded by an interface.

5.10.3 display garp timer

Function

The **display garp timer** command displays the values of GARP timers.

Format

display garp timer [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the GARP timers of the specified interface. - *interface-type* specifies the type of an interface. - *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display garp timer** command displays the values of GARP timers. When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system displays GARP timers of all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system displays GARP timers of the specified interface.

Example

Display the values of the GARP timers of the specified interface.

```
<HUAWEI> display garp timer interface gigabitethernet 0/0/1

 GARP timers on port GigabitEthernet0/0/1
   GARP JoinTime              : 80 centiseconds
   GARP LeaveTime             : 240 centiseconds
   GARP LeaveAllTime          : 1000 centiseconds
   GARP HoldTime              : 40 centiseconds
```

Table 5-64 Description of the display garp timer command output

Item	Description
GARP JoinTime	Value of the Join timer. You can run the **garp timer** command to set the Join timer.
GARP LeaveTime	Value of the Leave timer. You can run the **garp timer** command to set the Leave timer.

Item	Description
GARP LeaveAllTime	Value of the LeaveAll timer. You can run the **garp timer leaveall** command to set the LeaveAll timer.
GARP HoldTime	Value of the Hold timer. You can run the **garp timer** command to set the Hold timer.

5.10.4 display gvrp state

Function

The **display gvrp state** command displays information about the GVRP state machine.

Format

display gvrp state interface *interface-type interface-number* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the GVRP state machine of the specified interface. - *interface-type* specifies the type of an interface. - *interface-number* specifies the number of an interface.	-
vlan *vlan-id*	Displays information about the state machine of the specified VLAN.	The value is an integer that ranges from 2 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The GVRP function has two types of state machines: Applicant state machine and Registrar state machine.

An applicant implements declaration of attributes. If no message is lost during transmission, an applicant can ensure that all registrars have registered an attribute after it sends a Join message or receives a JoinIn message. To ensure reliable transmission of messages, the applicant needs to send two Join messages or send a Join message and receive a JoinIn message to confirm that all registrars have registered an attribute. Therefore, a simple counter is used. The counter starts from 0 and increases by 1 every time the applicant sends a Join message or receives a JoinIn message. The maximum value of the counter is 2. If the applicant receives a JoinEmpty, Empty, Leave, or LeaveAll message, the counter is reset to 0. This indicates that the applicant can send PDUs only when the value of the counter is smaller than 2.

The Join timer controls the interval for sending Join messages, but not every attribute has its own Join timer. A GVRP participant uses a Join timer. The value of the Join timer must be long enough to ensure that all the attributes can be packaged in a message and transmitted in a declaration.

- Anxious applicants

  Depending on the value of the applicant counter, an applicant may be in either of the following states:

  - V (very anxious): The value of the counter is 0, indicating that the applicant does not send a Join message or receive a JoinIn message.
  - A (anxious): The value of the counter is 1, indicating that no message is lost and all the registrars have registered the attribute.
  - Q (quiet): The value of the counter is 2, indicating that the applicant does not need to send Join messages.

- Members and observers

  The preceding states are applicable to normal situations. In special cases, for example, when some terminals do not need to send registration messages and only need to retain all the GARP state machines, these terminals must be separated from other entities. Therefore, the concept of member and observer is introduced. A member refers to an entity that tries to declare or retain an attribute value or an entity that has not sent a Leave message yet. An observer refers to an entity that traces the states of attributes but does not declare attributes.

  Multiple entities may actively join or leave the same attribute. To minimize the number of Join or Leave messages in this situation, members are classified into active members and passive members. Therefore, the following states are introduced:

  - A: Active member
  - P: Passive member
  - O: Observer

In addition, when an active member must send a Leave message to cancel a declaration, the active member enters the leaving state. Considering all these states, the state machine of an applicant has multiple state combinations, as shown in the following table.

State Combination	Very Anxious	Anxious	Quiet	Leaving
Active Member	VA	AA	QA	LA
Passive Member	VP	AP	QP	-
Observer	VO	AO	QO	LO

When a passive member needs to cancel a declaration, it can switch to the observer state. Therefore, the leaving passive member state does not exist.

A registrar has a Leave timer and three states: IN (attribute registered), MTR (attribute deregistered), and LV (attribute being deregistered). If a registrar in LV state does not receive the declaration of an attribute within the timeout interval of the Leave timer, the registrar enters the MTR state.

A registrar changes to different states depending on the received message:

- When receiving a Join message, the registrar changes to the IN state.
- When receiving a Leave or LeaveAll message, the registrar changes from the IN state to the LV state and starts the Leave timer. If the registrar is not in IN state, it does not change its state after receiving a Leave or LeaveAll message.
- The registrar does not change its state after receiving an Empty message.

Example

Display information about the GVRP state machine.

```
<HUAWEI> display gvrp state interface gigabitethernet 0/0/1 vlan 100
   GVRP state of VLAN 100 on port GigabitEthernet0/0/1

       Applicant state machine :    VP
       Registrar state machine :    MTR
```

Table 5-65 Description of the display gvrp state command output

Item	Description
Applicant state machine	State machine of the applicant.
Registrar state machine	State machine of the registrar.

5.10.5 display gvrp statistics

Function

The **display gvrp statistics** command displays statistics about GVRP on an interface.

Format

display gvrp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about GVRP on the specified interface. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface. If no interface is specified, the system displays statistics about GVRP on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display gvrp statistics** command displays statistics about GVRP on an interface, including the GVRP status, number of GVRP registration failures, source MAC address of the last GVRP PDU, and registration mode of the interface.

Example

Display the statistics about GVRP on an interface.

```
<HUAWEI> display gvrp statistics interface gigabitethernet 0/0/1
```

```
GVRP statistics on port GigabitEthernet0/0/1
  GVRP status                   : Enabled
  GVRP registrations failed      : 0
  GVRP last PDU origin           : 0000-0000-0000
  GVRP registration type         : Normal
```

Table 5-66 Description of the display gvrp statistics command output

Item	Description
GVRP status	GVRP state. The value can be: ● Enabled ● Disabled To specify the parameter, run the **gvrp** command.
GVRP registrations failed	Number of GVRP registration failures.
GVRP last PDU origin	Source MAC address of the last GVRP PDU.
GVRP registration type	GVRP registration type of an interface, which is configured by the **gvrp registration** command. The registration type can be: ● Fixed ● Forbidden ● Normal

5.10.6 display gvrp status

Function

The **display gvrp status** command displays whether global GVRP is enabled.

Format

display gvrp status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device with GVRP enabled can dynamically register VLANs or deregister VLANs from an interface. You can run the **display gvrp status** command to check whether GVRP is enabled.

Example

Display the enabling status of global GVRP.

```
<HUAWEI> display gvrp status
GVRP status: disabled
```

Table 5-67 Description of the display gvrp status command output

Item	Description
GVRP status	The status of global GVRP. To specify the parameter, run the **gvrp** command.

5.10.7 display gvrp vlan-operation

Function

The **display gvrp vlan-operation** command displays the operation of adding a specified interface to dynamic VLANs.

Format

display gvrp vlan-operation interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays operations related to dynamic VLANs performed on the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display gvrp vlan-operation** command displays the dynamic VLANs to which an interface is added.

Example

Display the operation of adding an interface to dynamic VLANs.

```
<HUAWEI> display gvrp vlan-operation interface GigabitEthernet 0/0/1
  Dynamic VLAN operations on port GigabitEthernet0/0/1

      Operations of adding VLAN to TRUNK              : none
```

Table 5-68 Description of the display gvrp vlan-operation command output

Item	Description
Operations of adding VLAN to TRUNK	Operation of adding a trunk interface to dynamic VLANs.

5.10.8 garp timer

Function

The **garp timer** command sets GARP timers.

The **undo garp timer** command restores the default values of GARP timers.

By default, the value of the Hold timer is 10 centiseconds, the value of the Join timer is 20 centiseconds, and the value of the Leave timer is 60 centiseconds.

Format

garp timer { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** } [*timer-value*]

Parameters

Parameter	Description	Value
hold *timer-value*	Sets the value of the GARP Hold timer.	- Lower limit: 10 centiseconds - Upper limit: less than or equal to half the value of the Join timer, changing with the value of the Join timer - The value can be exactly divided by 5, in centiseconds.
join *timer-value*	Sets the value of the GARP Join timer.	- Lower limit: greater than or equal to two times the value of the Hold timer, changing with the value of the Hold timer - Upper limit: smaller than half the value of the Leave timer, changing with the value of the Leave timer - The value can be exactly divided by 5, in centiseconds.
leave *timer-value*	Sets the value of the GARP Leave timer.	- Lower limit: greater than two times the value of the Join timer, changing with the value of the Join timer - Upper limit: smaller than the value of the LeaveAll timer, changing with the value of the LeaveAll timer - The value can be exactly divided by 5, in centiseconds.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 100GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can set the following GARP timers:

- Join timer: controls sending of Join messages including JoinIn messages and JoinEmpty messages.
- Hold timer: controls sending of Join messages (JoinIn messages and JoinEmpty messages) and Leave messages (LeaveIn messages and LeaveEmpty messages).
- Leave timer: controls attribute deregistration.

You can set the GARP timers to control sending of GARP protocol packets.

Prerequisite

The physical port has been added to the port group before running the **garp timer** command in the port group view.

Before setting garp timers on an interface, you must enable GVRP globally and on the interface.

Precautions

When using the **garp timer** command to set the GARP timers, pay attention to the following points:

- The **garp timer** can be used only on trunk interfaces.
- The **undo garp timer** command restores the default values of GARP timers. If the default value of a timer is out of the valid range, the **undo garp timer** command does not take effect.
- The value range of each timer changes with the values of the other timers. If a value you set for a timer is not in the allowed range, you can change the value of the timer that determines the value range of this timer.
- To restore the default values of all the GARP timers, restore the Hold timer to the default value, and then restore the Join timer, Leave timer, and LeaveAll timer to the default values in sequence.

When many dynamic VLANs need to be registered or the network radius is large, using default values of timers may cause VLAN flapping and high CPU usage. In this case, increase values of the timers. The following values are recommended depending on the number of VLANs.

Table 5-69 Relationship between GARP timer values and number of dynamic VLANs that need to be registered

Timer	Number of Dynamic VLANs to Be Registered (N)			
	N <= 500	500 < N <= 1000	1000 < N <= 1500	N > 1500
GARP Hold timer	100 centiseconds (1 second)	200 centiseconds (2 seconds)	800 centiseconds (8 seconds)	1000 centiseconds (10 seconds)
GARP Join timer	600 centiseconds (6 seconds)	1200 centiseconds (12 seconds)	4000 centiseconds (40 seconds)	6000 centiseconds (1 minute)

Timer	Number of Dynamic VLANs to Be Registered (N)			
	N <= 500	500 < N <= 1000	1000 < N <= 1500	N > 1500
GARP Leave timer	3000 centiseconds (30 seconds)	6000 centiseconds (1 minute)	20000 centiseconds (3 minutes and 20 seconds)	30000 centiseconds (5 minutes)
GARP LeaveAll timer	12000 centiseconds (2 minutes)	24000 centiseconds (4 minutes)	30000 centiseconds (5 minutes)	32765 centiseconds (5 minutes and 27.65 seconds)

Example

Set the Leave timer of GigabitEthernet 0/0/1 to 800 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] garp timer leave 800
```

Set the Join timer of GigabitEthernet 0/0/1 to 300 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] garp timer join 300
```

Set the Hold timer of GigabitEthernet 0/0/1 to 100 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] garp timer hold 100
```

5.10.9 garp timer leaveall

Function

The **garp timer leaveall** command sets the GARP LeaveAll timer.

The **undo garp timer leaveall** command restores the default value of the GARP LeaveAll timer.

The default value of the LeaveAll timer is 1000 centiseconds (10 seconds).

Format

garp timer leaveall *timer-value*

undo garp timer leaveall [*timer-value*]

Parameters

Parameter	Description	Value
timer-value	Specifies the value of the GARP LeaveAll timer.	The value is an integer that ranges from 65 to 32765 and that can be exactly divided by 5, in centiseconds. The value of the LeaveAll timer must be greater than the values of Leave timers on all the interfaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. Then the LeaveAll timer restarts.

Devices on a network may have different settings for the LeaveAll timer. In this case, all the devices use the smallest LeaveAll timer value on the network. When the LeaveAll timer of a device expires, the device sends LeaveAll messages to other devices. After other devices receive the LeaveAll messages, they reset their LeaveAll timers. Therefore, only the LeaveAll timer with the smallest value takes effect even if devices have different settings for the LeaveAll timer.

Prerequisites

Before setting LeaveAll timers, you must enable GVRP globally.

Precautions

The Leave timer length on an interface is restricted by the global LeaveAll timer length. When configuring the global LeaveAll timer, ensure that all the interfaces that have a GARP Leave timer configured are working properly.

Example

Set the LeaveAll timer to 2000 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] garp timer leaveall 2000
```

5.10.10 gvrp

Function

The **gvrp** command enables GVRP globally or on an interface.

The **undo gvrp** command disables GVRP globally or on an interface.

By default, GVRP is disabled globally and on each interface.

Format

gvrp

undo gvrp

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device with GVRP enabled can dynamically register VLANs or deregister VLANs from an interface. To make GVRP take effect, run the **gvrp** command both in the system view and interface view.

Precautions

When configuring GVRP, pay attention to the following points:

- If you run the **gvrp** command in the system view, GVRP is enabled globally. If you run this command in the interface view, GVRP is enabled on the interface.
- Before enabling GVRP on an interface, you must enable GVRP globally.
- Before enabling GVRP on an interface, you must set the link type of the interface to trunk.
- GVRP and Port security conflict on an interface; therefore, the **port-security enable** and **gvrp** commands cannot be used on the same interface.
- When GVRP is enabled globally, manually change values of timers based on the network scale.

Table 5-70 Relationship between GARP timer values and number of dynamic VLANs that need to be registered

Timer	Number of Dynamic VLANs to Be Registered (N)			
	N <= 500	500 < N <= 1000	1000 < N <= 1500	N > 1500
GARP Hold timer	100 centiseconds (1 second)	200 centiseconds (2 seconds)	800 centiseconds (8 seconds)	1000 centiseconds (10 seconds)
GARP Join timer	600 centiseconds (6 seconds)	1200 centiseconds (12 seconds)	4000 centiseconds (40 seconds)	6000 centiseconds (1 minute)
GARP Leave timer	3000 centiseconds (30 seconds)	6000 centiseconds (1 minute)	20000 centiseconds (3 minutes and 20 seconds)	30000 centiseconds (5 minutes)
GARP LeaveAll timer	12000 centiseconds (2 minutes)	24000 centiseconds (4 minutes)	30000 centiseconds (5 minutes)	32765 centiseconds (5 minutes and 27.65 seconds)

Example

Enable GVRP globally.

```
<HUAWEI> system-view
[HUAWEI] gvrp
```

Enable GVRP on GigabitEthernet 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] gvrp
```

5.10.11 gvrp registration

Function

The **gvrp registration** command sets the registration mode of a GVRP interface.

The **undo gvrp registration** command restores the default registration mode of a GVRP interface.

By default, the registration mode of a GVRP interface is **normal**.

Format

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration [**fixed** | **forbidden** | **normal**]

Parameters

Parameter	Description	Value
fixed	Indicates the fixed registration mode.	-
forbidden	Indicates the forbidden registration mode.	-
normal	Indicates the normal registration mode.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A GVRP interface supports three registration modes:

- Normal: In this mode, the GVRP interface can dynamically register and deregister VLANs, and transmit dynamic VLAN registration information and static VLAN registration information.
- Fixed: In this mode, the GVRP interface is disabled from dynamically registering and deregistering VLANs and can transmit only the static VLAN registration information. If the registration mode of a trunk interface is set to **fixed**, the interface allows only the manually configured VLANs to pass even if it is configured to allow all the VLANs to pass.
- Forbidden: In this mode, the GVRP interface is disabled from dynamically registering and deregistering VLANs and can transmit only information about VLAN 1. If the registration mode of a trunk interface is set to **forbidden**, the interface allows only VLAN 1 to pass even if it is configured to allow all the VLANs.

Pre-configuration Tasks

Before setting the registration mode of an interface, you must enable GVRP globally and configure the interface as a trunk interface.

Example

Set the registration mode of GE0/0/1 to **fixed**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] gvrp
[HUAWEI-GigabitEthernet0/0/1] gvrp registration fixed
```

5.10.12 reset garp statistics

Function

The **reset garp statistics** command clears statistics about GARP packets on an interface.

Format

reset garp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears the statistics about GARP packets on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting GARP traffic statistics on a specific interface within a certain period, you need to clear the existing GARP traffic statistics on this interface.

When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system clears statistics about GARP packets on all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system clears statistics about GARP packets on the specified interface.

Precautions

GVRP statistics cannot be restored after being cleared. Confirm your action before using this command.

Example

Clear statistics about GARP packets on GE0/0/1.

```
<HUAWEI> reset garp statistics interface gigabitethernet 0/0/1
```

5.11 VCMP Configuration Commands

5.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.11.2 display vcmp counters

Function

The **display vcmp counters** command displays statistics on VCMP packets.

Format

display vcmp counters

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If VCMP configured on a switch does not take effect, run the **display vcmp counters** command to view statistics on VCMP packets. The statistics helps you determine whether data on the switch is incorrect and locate faults.

Example

Display statistics on VCMP packets.

```
<HUAWEI> display vcmp counters
VCMP statistics:
```

```
Received summary packets                   : 0
Received request packets                   : 0
Received subset packets                    : 0
Sent summary packets                       : 0
Sent request packets                       : 0
Sent subset packets                        : 0
Received packets with ethheader error      : 0
Received packets with version error        : 0
Received packets with type error           : 0
Received packets with digest error         : 0
Received packets with domain error         : 0
Received packets with deviceid error       : 0
Failed to receive packets for bad vcmp state    : 0
Failed to send packets for bad vcmp state       : 0
Failed to receive packets for bad vlan          : 0
Failed to send packets for bad vlan             : 0
Failed to receive packets for bad link state    : 0
Failed to send packets for bad link state       : 0
Failed to receive packets for bad link type     : 0
Failed to send packets for bad link type        : 0
Failed to receive packets for bad forward state : 0
Failed to send packets for bad forward state    : 0
Failed to receive packets for bad length        : 0
Failed to receive packets for other             : 0
```

Table 5-71 Description of the display vcmp counters command output

Item	Description
VCMP statistics	Statistics on VCMP packets.
Received summary packets	Number of received VCMP Summary-Advert packets.
Received request packets	Number of received VCMP Advert-Request packets.
Received subset packets	Number of received VCMP subset packets.
Sent summary packets	Number of sent VCMP Summary-Advert packets.
Sent request packets	Number of sent VCMP Advert-Request packets.
Sent subset packets	Number of sent VCMP subset packets.
Received packets with ethheader error	Number of received VCMP packets with an incorrect Ethernet header.
Received packets with version error	Number of received VCMP packets with an incorrect protocol version.
Received packets with type error	Number of received VCMP packets of an incorrect type.
Received packets with digest error	Number of received VCMP packets with an incorrect digest.

Item	Description
Received packets with domain error	Number of received VCMP packets with an incorrect VCMP domain name.
Received packets with deviceid error	Number of received VCMP packets with an incorrect device ID.
Failed to receive packets for bad vcmp state	Number of packets that failed to be received due to incorrect VCMP status.
Failed to send packets for bad vcmp state	Number of packets that failed to be sent due to incorrect VCMP status.
Failed to receive packets for bad vlan	Number of packets that failed to be received due to incorrect VLAN information.
Failed to send packets for bad vlan	Number of packets that failed to be sent due to incorrect VLAN information.
Failed to receive packets for bad link state	Number of packets that failed to be received due to incorrect link status.
Failed to send packets for bad link state	Number of packets that failed to be sent due to incorrect link status.
Failed to receive packets for bad link type	Number of packets that failed to be received due to an incorrect link type.
Failed to send packets for bad link type	Number of packets that failed to be sent due to an incorrect link type.
Failed to receive packets for bad forward state	Number of packets that failed to be received due to incorrect forwarding status of the Layer 2 Ethernet interface.
Failed to send packets for bad forward state	Number of packets that failed to be sent due to incorrect forwarding status of the Layer 2 Ethernet interface.
Failed to receive packets for bad length	Number of packets that failed to be received because their lengths are incorrect.
Failed to receive packets for other	Number of packets that failed to be received due to other causes.

5.11.3 display vcmp interface brief

Function

The **display vcmp interface brief** command displays the VCMP status on Layer 2 Ethernet interfaces.

Format

display vcmp interface brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By default, VCMP is enabled on all Layer 2 Ethernet interfaces of a switch. You can run the **display vcmp interface brief** command to view the VCMP status on Layer 2 Ethernet interfaces.

Example

Display the VCMP status on Layer 2 Ethernet interfaces.

```
<HUAWEI> display vcmp interface brief
Vcmp interface number:2
Interface                    Vcmp State
--------------------------------------------
GigabitEthernet0/0/1              disable
GigabitEthernet0/0/2              enable
```

Table 5-72 Description of the display vcmp interface brief command output

Item	Description
Vcmp interface number	Number of Layer 2 Ethernet interfaces supporting VCMP.
Interface	Name and number of a Layer 2 Ethernet interface on which VCMP can run.
Vcmp State	VCMP status on a Layer 2 Ethernet interface. To specify the parameter, run the **vcmp disable** command.

5.11.4 display vcmp status

Function

The **display vcmp status** command displays the VCMP configuration, including the VCMP domain name, VCMP role, device ID, configuration revision number, and VCMP domain authentication password.

Format

display vcmp status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VCMP is configured on a switch, you can run the **display vcmp status** command to view the VCMP configuration.

Example

Display the VCMP configuration.

```
<HUAWEI> display vcmp status
VCMP information:
Domain                  : VLAN
Role                    : Server
Server ID               : VLAN
Configuration Revision  : 0x846a0000
Password                : ******
```

Table 5-73 Description of the display vcmp status command output

Item	Description
VCMP information	VCMP information.
Domain	VCMP domain name. To change the VCMP domain name, run the **vcmp domain** command.
Role	VCMP role of the switch in the VCMP domain. To change the VCMP role, run the **vcmp role** command.
Server ID	ID of the switch functioning as the VCMP server. To change the device ID, run the **vcmp device-id** command.

Item	Description
Configuration Revision	Configuration revision number.
Password	VCMP domain authentication password. To change the authentication password, run the **vcmp authentication** command. If no authentication password is configured, this parameter is left empty.

5.11.5 display vcmp track

Function

The **display vcmp track** command displays VLAN changes on a device functioning as a client.

Format

display vcmp track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If VLAN changes, including creating VLANs, deleting VLANs, modifying VLAN names, and modifying VLAN descriptions, are made on a device functioning as a server, the device functioning as a client synchronizes its VLAN information with that on the server by exchanging VCMP packets. To view VLAN changes, run the **display vcmp track** command on the client.

Example

Display VLAN changes on the client.

```
<HUAWEI> display vcmp track
Operate Flags: A - Add, D - Delete, VN - VLAN Name , VD - VLAN Description
-------------------------------------------------------------------------------
Op System-Time              Operate-VLAN
-------------------------------------------------------------------------------
A  03-19 19:32:27           103
```

```
A  03-19 19:30:57          10
D  03-19 19:15:52          20
VD 03-19 19:12:20           100
VN 03-19 19:12:06           100
A  03-19 19:10:48          101
A  03-19 19:09:45          100
```

Table 5-74 Description of the **display vcmp track** command output

Item	Description
Operate Flags	Operation flag: ● A: Newly created VLANs ● D: Deleted VLANs ● VN: VLANs whose names were modified ● VD: VLANs whose descriptions were modified
Op System-Time	System time
Operate-VLAN	Operated VLAN

5.11.6 reset vcmp

Function

The **reset vcmp** command clears the VCMP domain name and device ID learned on a VCMP client.

Format

reset vcmp

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The VCMP domain ID and device ID learned by a VCMP client remain unchanged. The VCMP client needs to learn VCMP information again when the VCMP server in the local VCMP domain is changed. Therefore, clear learned VCMP information before the VCMP client learns VCMP information.

Configuration Impact

After the **reset vcmp** command is executed, the learned VCMP information is cleared and cannot be restored. Therefore, exercise caution when you run the **reset vcmp** command.

Example

Clear the VCMP domain name and device ID learned on a VCMP client

```
<HUAWEI> reset vcmp
```

5.11.7 reset vcmp counters

Function

The **reset vcmp counters** command clears statistics on VCMP packets.

Format

reset vcmp counters

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting statistics on VCMP packets in a specified period, run the **reset vcmp counters** command to clear existing statistics on VCMP packets.

Configuration Impact

After the **reset vcmp counters** command is executed, statistics on VCMP packets are cleared cannot be restored. Therefore, exercise caution when you run the **reset vcmp counters** command.

Example

Clear statistics on VCMP packets.

```
<HUAWEI> reset vcmp counters
```

5.11.8 reset vcmp track

Function

The **reset vcmp track** command deletes VLAN changes on a device functioning as a client.

Format

reset vcmp track

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before viewing VLAN changes on a client using the **display vcmp track** command, run the **reset vcmp track** command to delete existing VLAN changes.

Configuration Impact

After you run the **reset vcmp track** command, the deleted information cannot be restored. Therefore, exercise caution when running the **reset vcmp track** command.

Example

Delete existing VLAN changes on the client.

```
<HUAWEI> reset vcmp track
```

5.11.9 vcmp authentication

Function

The **vcmp authentication** command sets a VCMP domain authentication password.

The **undo vcmp authentication** command deletes the VCMP domain authentication password.

By default, no VCMP domain authentication password is set and VCMP packets pass without authentication.

Format

vcmp authentication sha2-256 password *password*

undo vcmp authentication

Parameters

Parameter	Description	Value
sha2-256	Enables SHA2-256 authentication for a VCMP domain.	-
password *password*	Specifies a VCMP domain authentication password.	The value a string of case-sensitive characters, spaces not supported. Passwords are saved in ciphertext in the configuration file. Either of the following passwords can be set: ● A simple text password is a string of 1 to 8 characters. ● A ciphertext password is a string of 48 characters. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** A 32-character ciphertext password configured in an earlier version is also supported in this version.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance security for a VCMP domain, you can run the **vcmp authentication** command to set a VCMP domain authentication password on each switch for authenticating packets exchanged between the switches in the VCMP domain.

Precautions

All switches in a VCMP domain must use the same VCMP domain authentication password.

Example

Set the VCMP domain authentication password to **huawei**.

```
<HUAWEI> system-view
[HUAWEI] vcmp authentication sha2-256 password huawei
```

5.11.10 vcmp device-id

Function

The **vcmp device-id** command sets the device ID of the VCMP server.

The **undo vcmp device-id** command deletes the device ID of the VCMP server.

By default, no device ID is set for the VCMP server.

Format

vcmp device-id *device-name*

undo vcmp device-id

Parameters

Parameter	Description	Value
device-name	Specifies a device ID.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device ID identifies the VCMP server so that other roles in a VCMP domain can identify the VCMP server.

Prerequisites

The **vcmp role server** command has been executed to configure a server role for a switch in a VCMP domain. The device ID can be set only for the VCMP server.

Example

Set the device ID of the VCMP server.

```
<HUAWEI> system-view
[HUAWEI] vcmp device-id VLAN
```

5.11.11 vcmp disable

Function

The **vcmp disable** command disables VCMP on an interface.

The **undo vcmp disable** command enables VCMP on an interface.

By default, VCMP is enabled on all interfaces of a switch.

Format

vcmp disable

undo vcmp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, VCMP is enabled on all interfaces of a switch. If an edge switch in a VCMP domain requires VCMP management but its peer end does not require VCMP management, run the **vcmp disable** command on the edge switch Layer 2 interface connected to the peer end to disable VCMP. The peer end then does not receive VCMP packets.

Prerequisites

The interface connected to the peer end has been configured as a Layer 2 interface using the **portswitch** command.

Example

Disable VCMP on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vcmp disable
```

5.11.12 vcmp domain

Function

The **vcmp domain** command configures a VCMP domain.

The **undo vcmp domain** command deletes a VCMP domain.

By default, no VCMP domain is created.

Format

vcmp domain *domain-name*

undo vcmp domain

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a VCMP domain.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLANs created and deleted on the VCMP server are synchronized to VCMP clients in the local VCMP domain by sending VCMP packets.

A VCMP domain specifies the scope for managed switches. All VCMP clients are managed by the VCMP server. You can run the **vcmp domain** command to configure a VCMP domain.

Precautions

All switches in a VCMP domain must use the same domain name either through manual configuration or automatic learning. If the domain name is not set on a VCMP client, the VCMP client learns the domain name in the first received VCMP packet.

Each switch can be added to only one VCMP domain. Switches in different VCMP domains cannot synchronize VLAN information.

Example

Configure a VCMP domain named **VLAN**.

```
<HUAWEI> system-view
[HUAWEI] vcmp domain VLAN
```

5.11.13 vcmp role

Function

The **vcmp role** command configures a role for a switch in a VCMP domain.

The **undo vcmp role** command restores the default role of a switch in a VCMP domain.

By default, switches in a VCMP domain are VCMP silent.

Format

vcmp role { **client** | **server** | **silent** | **transparent** }

undo vcmp role

Parameters

Parameter	Description	Value
client	Indicates the client role in a VCMP domain. As a managed role, a VCMP client synchronizes VLAN information with the VCMP server. After the VCMP server is specified on a Layer 2 network, VCMP clients in the same domain learn VLAN information in VCMP packets from the VCMP server and synchronize the VLAN information. You can create and delete VLAN information on VCMP clients. Local VLAN information on VCMP clients, however, are overwritten by VLAN information synchronized from the VCMP server.	-
server	Indicates the server role in a VCMP domain. You can create and delete VLAN information on the VCMP server. The VCMP server synchronizes VLAN information to other switches in the local VCMP domain by sending VCMP packets.	-

Parameter	Description	Value
silent	Indicates the silent role in a VCMP domain. Deployed at the edge of a VCMP domain, a VCMP silent switch prevents VCMP packets in a VCMP domain from being transmitted to other VCMP domains, saving unnecessary costs of devices in other VCMP domains. A VCMP silent switch directly discards received VCMP packets.	-
transparent	Indicates the transparent role in a VCMP domain. A VCMP transparent switch does not affect other switches in the local VCMP domain and is not affected by VCMP management behaviors such as VLAN creation and deletion. The VCMP transparent switch transparently forwards VCMP packets. Only trunk or hybrid interfaces in VLAN 1 can receive and forward VCMP packets. VLANs created and deleted on a VCMP transparent switch are not synchronized to other switches.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLANs created and deleted on the VCMP server are synchronized to VCMP clients in the local VCMP domain by sending VCMP packets.

You can run the **vcmp role** command to set roles of switches in a VCMP domain.

Precautions

In V200R021C10 and earlier versions, the VCMP role is **Client** by default. In V200R022C00 and later versions, the VCMP role is **Silent** by default. If a device is upgraded from V200R021C10 or an earlier version to V200R022C00 or a later version, the VCMP role does not change after the upgrade.

In V200R021C10 and earlier versions:

- The VCMP role of a device is Client by default and the device configuration file does not contain the vcmp role client command. After the device is upgraded to V200R022C00 or a later version, the device configuration file contains the vcmp role client command.
- If the vcmp role silent command has been run on a device to set the VCMP role to Silent, the device configuration file contains the vcmp role silent

command. After the device is upgraded to V200R022C00 or a later version, the device configuration file does not contain the vcmp role silent command.

Example

Configure a switch as the VCMP server in a VCMP domain.

```
<HUAWEI> system-view
[HUAWEI] vcmp role server
Warning: Change the VCMP role from client to server.Continue? [Y/N]:y
```

5.12 STP/RSTP/MSTP/VBST Configuration Commands

5.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.12.2 active region-configuration

Function

The **active region-configuration** command activates the configuration of a multiple spanning tree (MST) region.

Format

active region-configuration

Parameters

None

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring MST region parameters, especially VLAN mapping tables for MST regions, is likely to cause network topology flapping. To reduce network flapping, make sure that newly configured MST region parameters take effect only after the **active region-configuration** command is run.

Precautions

Before running the **active region-configuration** command, you are recommended to run the **check region-configuration** command to check whether the region configurations that have not taken effect are correct. If the region configurations that have not taken effect are correct, run the **active region-configuration** command.

After the **active region-configuration** command is run, the configured MST region parameters will take effect and all spanning trees in the MST region will be recalculated.

If the VLAN to be mapped to an MSTP instance is the control VLAN for the SEP segment, the newly configured parameters of the MST region cannot be activated.

Example

Map VLAN 5 to the spanning tree instance 2 and activate the configuration.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] instance 2 vlan 5
[HUAWEI-mst-region] active region-configuration
```

5.12.3 check region-configuration

Function

The **check region-configuration** command displays the configuration of an MST region such as the region name, revision level, and VLAN mapping table.

Format

check region-configuration

Parameters

None

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each region is called an MST region and each spanning tree is called a multiple spanning tree instance (MSTI).

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- MST region revision level
- Mappings between MSTIs and VLANs

To ensure that MST region configurations on each switching device are correct, you are recommended to run the **check region-configuration** command to check the MST region configurations before running the **active region-configuration** command. If the MST region configurations are correct, run the **active region-configuration** command to activate them.

Precautions

By default, VLANs that are not mapped to any instances with non-zero IDs using the **instance** command are mapped to instance 0.

Example

Display the configuration of an MST region.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] check region-configuration
 Admin configuration
   Format selector    :0
   Region name        :00b010000001
   Revision level     :0

   Instance   VLANs Mapped
     0       1 to 9, 11 to 4094
    16       10
```

Table 5-75 Description of the check region-configuration command output

Item	Description
Format selector	Selection factor defined by MSTP
Region name	Name of the MST region. To configure the name for an MST region, run the **region-name** command.
Revision level	Revision level of the MST region. To set the revision level of the MST region, run the **revision-level** command.
Instance VLANs Mapped	Mapping between MSTIs and VLANs. To configure the mapping between MSTIs and VLANs, run the **instance** or **vlan-mapping modulo**.

5.12.4 display ethernet-loop-protection ignored-vlan

Function

The **display ethernet-loop-protection ignored-vlan** command displays information about configured ignored VLANs.

Format

display ethernet-loop-protection ignored-vlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After you configure an ignored VLAN using the **ethernet-loop-protection ignored-vlan** command, the **display ethernet-loop-protection ignored-vlan** command can be used to display information about the configured ignored VLAN.

Prerequisites

An ignored VLAN has been configured using the **ethernet-loop-protection ignored-vlan** command.

Example

Display information about the configured ignored VLAN.

```
<HUAWEI> display ethernet-loop-protection ignored-vlan
 Ethernet-loop-protection ignored-vlan : 3 to 4
```

Table 5-76 Description of the **display ethernet-loop-protection ignored-vlan** command output

Item	Description
Ethernet-loop-protection ignored-vlan	ID of a configured ignored VLAN To specify the parameter, run the **ethernet-loop-protection ignored-vlan** command.

5.12.5 display stp

Function

The **display stp** command displays the status of and statistics on a spanning tree instance.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] [**brief**]

VBST: **display stp** [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] [**brief**]

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. If **process** *process-id* is not specified, the status and statistics of an MSTP process with the ID 0 will be displayed.	The value is a decimal integer ranging from 1 to 31.
instance *instance-id*	Displays the status and statistics of a spanning tree instance. If **instance** *instance-id* is not specified, the status and statistics of all spanning tree instances will be displayed in the sequence of the interface numbers.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
interface *interface-type interface-number*	Displays the information of a spanning tree on a specified interface. If **interface** *interface-type interface-number* is not specified, the status and statistics of all interfaces will be displayed in the sequence of the interface numbers.	-
brief	Displays the brief status.	-
slot *slot-id*	Displays the status of and statistics on a spanning tree instance in a specified slot.	The value is an integer and must be an existing slot on the device.

Parameter	Description	Value
vlan *vlan-id*	Displays spanning tree configurations in a specified VLAN. If **vlan** *vlan-id* is not specified, configurations of spanning trees in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only VBST spanning tree configurations in a specified VLAN are displayed.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display stp** command is used to check whether STP/RSTP/MSTP/VBST is run in the existing switching device or specified interface.

- If the **Protocol Status** field value is **Disabled**, STP/RSTP/MSTP/VBST is not run.
- If STP/RSTP/MSTP has been run, information such as the working mode of STP/RSTP/MSTP/VBST will be displayed.

When the network planner has deployed STP/RSTP/MSTP/VBST on the network, you can run the **display stp** command to check the configurations and calculation result.

Precautions

- If you run this command in the system view without specifying an MSTP process, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process, information about the MSTP process in this view is displayed by default.
- In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.
- If a non-0 instance is mapped to a VLAN to which no interface is added, the following information is displayed when you query the status and statistics of the spanning tree instance:

```
Info: No instance information is available.
```

NOTE

For description about MSTP process 0, see **stp process**.

Example

When the **stp enable** command does not run, the status and statistics of STP are displayed.

```
<HUAWEI> display stp
 Protocol Status       :Disabled
 Protocol Standard     :IEEE 802.1s
 Version               :3
 CIST Bridge Priority  :32768
 MAC address           :00e0-6343-6800
 Max age(s)            :20
 Forward delay(s)      :15
 Hello time(s)         :2
 Max hops              :20
 Share region-configuration :Enabled
```

Table 5-77 Description table of the display stp command output

Item	Description
Protocol Status	Status of the protocol. - Disabled - Enabled
Protocol Standard	Standards of the protocol.
Version	Protocol version: - 0: STP - 2: RSTP - 3: MSTP To set the protocol version, run the **stp mode** command.
CIST Bridge Priority	Priority of the switch in the CIST. To set the STP priority, run the **stp priority** command.
MAC address	MAC address of the switch.
Max age (s)	Maximum TTL of a BPDU. To set the value of Max Age, run the **stp timer max-age** command.
Forward delay (s)	Time taken by interface status transition. To set the value of Forward Delay, run the **stp timer forward-delay** command.
Hello time (s)	Interval for sending BPDUs from the root switch. To set the hello time, run the **stp timer hello** command.
Max hops	Maximum number of hops in an MST region. To set the maximum number of hops, run the **stp max-hops** command.
Share region-configuration	Status of sharing the region configuration of process 0. The status is fixed at Enable.

Display the status of and statistics on a spanning tree instance when the **stp enable** command is configured.

```
<HUAWEI> display stp brief
 MSTID   Port                     Role  STP State      Protection
   0     GigabitEthernet0/0/1      DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/2      DESI  FORWARDING      NONE
   0     GigabitEthernet0/0/4      ROOT  FORWARDING      NONE
```

Table 5-78 Description of the display stp brief command output

Item	Description
MSTID	MSTP instance ID.
Port	-
Role	Interface role: ● DESI: Designated port ● ROOT: Root port ● ALTE: Alternate port ● BACK: Backup port ● MAST: Master port ● DISA: The interface is in initialization state.
STP State	Interface status. In the CIST region, the statuses of interfaces are as follows: ● FORWARDING ● LEARNING ● DISCARDING
Protection	Protection function: ● ROOTPROTECTION ● LOOPPROTECTION ● NONE ● LOOPBACK: loopback detection ● PVIDCONSISTENCY: The PVID of the directly connected interface is inconsistent.

Displays spanning tree configurations when VBST is running.

```
<HUAWEI> display stp
-------[VLAN 20 Global Info][Mode VBST]-------
Bridge ID           :32788.00e0-f068-0600
Bridge Diameter     :7
Config Times        :Hello 2s MaxAge 20s FwDly 15s
Active Times        :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC       :20   .00e0-c959-e700 / 20
RootPortId          :128.2 (GigabitEthernet0/0/2)
Root Type           :Normal
BPDU-Protection     :Disabled
```

```
STP Converge Mode   :Normal
Time since last TC  :0 days 0h:10m:46s
Number of TC        :1
Last TC occurred    :GigabitEthernet0/0/1
 ----[Port1(GigabitEthernet0/0/1)][DISCARDING]----
 Port Role          :Alternate Port
 Port Priority      :128
 Port Cost(Legacy)  :Config=20000 / Active=20000
 Desg. Bridge/Port  :32788.00e0-2539-c700 / 128.3
 Port Edged         :Config=Default / Active=Disabled
 Point-to-point     :Config=Auto / Active=true
 Transit Limit      :6 packets/hello
 Protection Type    :None
 Port STP Mode      :VBST
 BPDU Encapsulation :Config=VBST / Active=VBST
 BPDU Sent          :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received      :0
          TCN: 0, Config: 0, RST: 0
```

Table 5-79 Description of the **display stp** command output

Item	Description
Bridge ID	Bridge ID.
Bridge Diameter	VBST network diameter.
Config Times	Time values in manually configured bridge protocol information: ● Hello: indicates the interval for sending BPDUs. ● MaxAge: indicates the maximum lifetime of BPDUs. ● FwDly: indicates the delay for port status transition.
Active Times	Time values in actual bridge protocol information: ● Hello: indicates the interval for sending BPDUs. ● MaxAge: indicates the maximum lifetime of BPDUs. ● FwDly: indicates the delay for port status transition.
Root ID / RPC	Root switch ID in a VLAN or external path cost from the local switch to the CIST root switch.
RootPortId	ID of the root port in a VLAN. The value 0.0 indicates that the switch is the root switch without the root port.
Root Type	Root bridge type.

Item	Description
BPDU-Protection	BPDU protection function: - Disabled - Enabled
STP Converge Mode	STP converge mode
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Port Role	Role of the port.
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Legacy)	Port path cost calculated using Huawei proprietary algorithm: - Config: indicates the manually configured path cost. - Active: indicates the actual path cost.
Desg. Bridge/Port	Designated bridge or port.
Port Edged	Edge port specified by the administrator: - enabled: indicates that the edge port is enabled. - disabled: indicates that the edge port is not enabled. Config indicates the value configured by the **stp edged-port** command; Active indicates the actual value.
Point-to-point	Link type of the port. Config indicates the link type configured by the **stp point-to-point** command; Active indicates the actual link type.
Transit Limit	Maximum number of BPDUs sent by the current interface in each Hello time. To set the maximum number of BPDUs sent per second on a port, run the **stp transmit-limit (interface view)** command.

Item	Description
Protection Type	Protection type: ● root-protection ● loop-protection ● None ● LoopBack: loopback detection
Port STP Mode	STP mode on an interface.
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface. In STP/RSTP/MSTP mode, the value is stp. In VBST mode, the value is VBST.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: ● TCN: topology change notification ● Config: STP packets ● RST: RSTP packets ● MST: MSTP packets
BPDU Received	Statistics about the packets received by BPDU.

Display the status of and statistics on the spanning tree instance 0 on GE0/0/1.

```
<HUAWEI> display stp instance 0 interface gigabitethernet 0/0/1
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :32768.00e0-fc0e-a421
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc0e-a421 / 0 (This bridge is the root)
CIST RegRoot/IRPC   :32768.00e0-fc0e-a421 / 0 (This bridge is the root)
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 23h:9m:30s
Number of TC        :1
Last TC occurred    :GigabitEthernet0/0/1
----[Port3(GigabitEthernet0/0/1)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Legacy)   :Config=auto / Active=19
 Designated Bridge/Port   :32768.00e0-fc0e-a421 / 128.1229
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :3 packets/hello-time
 Protection Type     :None
 Port STP Mode       :MSTP
 Config-digest-snoop :snooped=false
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
```

```
TC or TCN send      :0
TC or TCN received  :0
BPDU Sent           :147
         TCN: 0, Config: 0, RST: 0, MST: 147
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
```

Table 5-80 Description of the display stp instance command output

Item	Description
CIST Global Info	CIST global information.
Mode MSTP	The operation mode is MSTP. By default, the mode is MSTP. To set the operation mode, run the **stp mode** command.
CIST Bridge	ID of the CIST bridge. ● The previous 16 bits are the priority of the switch in CIST. ● The latter 48 bits is the MAC address of the switch. **NOTE** CIST Bridge is displayed when STP/RSTP/MSTP is running. Bridge ID is displayed when VBST is running.
Config Times	Value that is configured manually in the bridge protocol information: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● MaxHop: the maximum hops in the MST region.
Active Times	Value that is used actually in the bridge protocol information: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● MaxHop: the maximum hops in the MST region.
CIST Root/ERPC	CIST root bridge ID/External path cost (the path cost from the switch to the CIST root bridge.) **NOTE** CIST Root/ERPC is displayed when STP/RSTP/MSTP is running. Root ID / RPC is displayed when VBST is running.
CIST RegRoot/IRPC	Region root bridge ID/Internal path cost (the path cost from the switch to region root bridge.)

Item	Description
CIST RootPortId	CIST root port ID. "0.0" indicates the switch is a root bridge and has no root port. **NOTE** CIST RootPortId is displayed when STP/RSTP/MSTP is running. RootPortId is displayed when VBST is running.
BPDU-Protection	BPDU protection function: ● Disabled ● Enabled
TC or TCN received	Number of the received TC or TCN packets.
TC count per hello	Number of TC packets received within a hello interval.
STP Converge Mode	STP converge mode
Share region-configuration	The status of sharing the region configuration of process 0.
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Last TC occurred	Interface which causes the last topology change **NOTE** This parameter does not appear when **Number of TC** is **0**.
Port Protocol	The status of the port protocol is as follows: ● Enable: STP is enabled on the port. ● disable: STP is disabled on the port.
Port Role	The port roles are as follows: ● Root Port ● Designated Port ● Alternate Port ● Backup Port ● Master port ● Disabled Port
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Legacy)	Path cost of the port. It is calculated by dot1t algorithm. ● config: refers to the path cost that is configured manually. ● active: refers to the path cost actually.

Item	Description
Designated Bridge/ Port	ID of the designated switch and port. The first 16 bits of the switch ID represent the priority of the switch in the CIST region; the last 48 bits represent the MAC address of the switch. The first 4 bits of the port ID represent the priority and the last 12 bits represent the port number.
Port Edged	Edged port that is specified by the administrator: - enabled - disabled **Config** indicates that the value is configured by using the **stp edged-port** command. **Active** indicates the actual value.
Point-to-point	Link type of the port. **Config** indicates that the link type is configured by running the **stp point-to-point** command. **Active** indicates the actual link type.
Transit Limit	Limit of the BPDUs sent by the current port during each Hello time. To set the limit of the BPDUs sent by the current port during each Hello time, run the **stp transmit-limit (interface view)** command.
Protection Type	The protection type is as follows: - root protection - loop protection - None - LoopBack: loopback detection
Port STP Mode	STP mode on an interface.
Config-digest-snoop	The configuration digest snooping function. The command output is displayed only after the **stp config-digest-snoop** command is configured and the configuration digest snooping function is enabled on the port. If the port is not enabled with the function, the command output is not displayed: - snooped=false: The configuration digest of the packets on the remote end is the same as that on the local end. - snooped=true: The configuration digest of the packets on the remote end is different from that on the local end.

Item	Description
Port Protocol Type	Format of the packets that the interface receives and sends. The formats are as follows: ● auto ● legacy ● dot1s The default value is **auto**. **Config** indicates that the packet format is configured by running the **stp compliance** command. **Active** indicates the actual packet format.
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface. In STP/RSTP/MSTP mode, the value is stp. In VBST mode, the value is VBST.
PortTimes	Values in the bridge protocol information of the interface: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● RemHop: the maximum hops in the MST region.
TC or TCN send	Number of BPDUs with TC flags or TCN BPDUs sent by the port.
TC or TCN received	Number of BPDUs with TC flags or TCN BPDUs received by the port.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: ● TCN: topology change notification ● Config: STP packets ● RST: RSTP packets ● MST: MSTP packets
BPDU Received	Statistics about the packets received by BPDU.

5.12.6 display stp abnormal-interface

Function

The **display stp abnormal-interface** command displays information about abnormal interfaces running the Spanning Tree Protocol (STP).

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] **abnormal-interface**

VBST: **display stp** [**vlan** *vlan-id*] **abnormal-interface**

Parameters

Parameter	Description	Value
process *process-id*	Displays the ID of a specified multi service transport platform (MSTP) process. If **process** *process-id* is not specified, the status and statistics of the MSTP process with ID 0 will be displayed.	The value is an integer in the range 1 to 31.
instance *instance-id*	Displays the status and statistics of a specified spanning tree instance. If **instance** *instance-id* is not specified, the status and statistics of all spanning tree instances will be displayed in the sequence of the interface numbers.	The value is an integer in the range 0 to 4094. The value **0** indicates a common and internal spanning tree (CIST) instance. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
vlan *vlan-id*	Displays information about abnormal ports running STP in a specified VLAN. If **vlan** *vlan-id* is not specified, information about abnormal ports running STP in all VLANs is displayed. **NOTE** If **vlan** *vlan-id* is specified, only information about abnormal ports running VBST is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a device has many interfaces and the **display stp** command output displays vast information, viewing information about abnormal interfaces running STP is difficult.

You can use the **display stp abnormal-interface** command to view information about abnormal interfaces running STP.

Precautions

- If you run this command in the system view without specifying an MSTP process, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process, information about the MSTP process in this view is displayed by default.
- In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

Display information about abnormal interfaces in process 0 running STP

```
<HUAWEI> display stp instance 0 abnormal-interface
MSTID    Interface                    Status          Reason
   0     GigabitEthernet0/0/0         DISCARDING      LOOP-Protected
   0     GigabitEthernet0/0/1         DOWN            BPDU-Protected
   0     GigabitEthernet0/0/2         DISCARDING      ROOT-Protected
   0     GigabitEthernet0/0/3         DISCARDING      LOOP-Detected
```

Display information about abnormal ports running VBST in VLAN 5.

```
<HUAWEI> display stp vlan 5 abnormal-interface
VLAN    Interface                    Status          Reason
  5     GigabitEthernet0/0/0         DISCARDING      LOOP-Protected
  5     GigabitEthernet0/0/1         DOWN            BPDU-Protected
  5     GigabitEthernet0/0/2         DISCARDING      ROOT-Protected
  5     GigabitEthernet0/0/3         DISCARDING      LOOP-Detected
```

Table 5-81 Description of the **display stp abnormal-interface** command output

Item	Description
MSTID	MSTP instance ID
Interface	Interface type
Status	Status of an interface after the STP protection takes effect ● **DOWN**: indicates that the physical status of the interface is Down (including error-down). ● **DISCARDING**: indicates the blocked interface after the topology of the spanning tree becomes stable.

Item	Description
Reason	An interface running STP becomes abnormal due to one of the following: • **ROOT-Protected**: indicates that the root protection takes effect. • **LOOP-Protected**: indicates that the loop protection takes effect. • **BPDU-Protected**: indicates that the BPDU protection takes effect. • **LOOP-Detected**: indicates that the loop detection takes effect. • **PVID-Inconsistency**: The PVID of the directly connected interface is inconsistent.
VLAN	VLAN ID.

5.12.7 display stp active

Function

The **display stp active** command displays the status of and statistics on spanning trees of all Up interfaces.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] **active**

VBST: **display stp** [**vlan** *vlan-id*] **active**

Parameters

Parameter	Description	Value
process *process-id*	Multiple Spanning Tree Protocol (MSTP) process ID If **process** *process-id* is not specified, the status of and statistics on process 0 will be displayed.	The value is an integer ranging from 1 to 31.

Parameter	Description	Value
vlan *vlan-id*	Displays details and statistics about spanning trees of all ports in Up state in a specified VLAN. If **vlan** *vlan-id* is not specified, details and statistics about spanning trees of all ports in Up state in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only details and statistics about spanning trees of all ports in Up state in a specified VLAN are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display stp active** command displays information about spanning trees of Up interfaces only.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.
- In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

Display information about spanning trees of all Up interfaces of MSTP process 0 when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp active
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :61440.781d-ba56-f06c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :61440.781d-ba56-f06c / 0 (This bridge is the root)
CIST RegRoot/IRPC   :61440.781d-ba56-f06c / 0 (This bridge is the root)
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :85
```

```
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 9h:10m:8s
Number of TC        :13
Last TC occurred    :GigabitEthernet0/0/4
----[Port18(GigabitEthernet0/0/10)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :61440.781d-ba56-f06c / 128.18
 Port Edged          :Config=default / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :10 packets/s
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :5
 TC or TCN received  :0
 BPDU Sent           :178445
          TCN: 0, Config: 0, RST: 0, MST: 178445
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 Last forwarding time: 2012/04/19 16:58:37 UTC+08:00
----[Port19(GigabitEthernet0/0/17)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :61440.781d-ba56-f06c / 128.19
 Port Edged          :Config=default / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :10 packets/s
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 BPDU Encapsulation  :Config=stp / Active=stp
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :5
          TCN: 0, Config: 0, RST: 0, MST: 5
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0, MST: 0
 Last forwarding time: 2012/04/23 20:06:08 UTC+08:00

-------[MSTI 1 Global Info]-------
MSTI Bridge ID      :61440.781d-ba56-f06c
MSTI RegRoot/IRPC   :61440.781d-ba56-f06c / 0(This bridge is the root)
MSTI RootPortId     :0.0
Master Bridge       :61440.781d-ba56-f06c
Cost to Master      :0
TC received         :2
TC count per hello  :0
Time since last TC  :0 days 9h:10m:8s
Number of TC        :9
Last TC occurred    :GigabitEthernet0/0/4
```

Display details and statistics about spanning trees of all ports in Up state in VLAN 10 when VBST is running.

```
<HUAWEI> display stp vlan 10 active
-------[VLAN 10 Global Info][Mode VBST]-------
Bridge ID             :10   .00e0-5553-9900
Bridge Diameter        :7
Config Times           :Hello 2s MaxAge 20s FwDly 15s
Active Times           :Hello 2s MaxAge 20s FwDly 15s
```

```
Root ID / RPC          :10   .00e0-5553-9900 / 0 (This bridge is the root)
RootPortId             :0.0
Root Type              :Primary
BPDU-Protection        :Disabled
STP Converge Mode      :Normal
Time since last TC     :0 days 0h:10m:46s
Number of TC           :1
 ----[Port1(GigabitEthernet0/0/1)][FORWARDING]----
 Port Role             :Designated Port
 Port Priority         :128
 Port Cost(Legacy)     :Config=Auto / Active=20
 Desg. Bridge/Port     :10   .00e0-5553-9900 / 128.1
 Port Edged            :Config=Default / Active=Disabled
 Point-to-point        :Config=Auto / Active=True
 Port Revert Slow      :Disabled
 Port Agreement Legacy :Disabled
 Transit Limit         :6 packets/hello
 Protection Type       :None
 Port STP Mode         :VBST
 BPDU Encapsulation    :Config=VBST / Active=VBST
 BPDU Sent             :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received         :0
          TCN: 0, Config: 0, RST: 0
```

Table 5-82 Description of the **display stp active** command output

Item	Description
CIST Bridge Bridge ID	CIST bridge: Bridge ID: **NOTE** CIST Bridge is displayed when STP/RSTP/MSTP is running. Bridge ID is displayed when VBST is running.
Bridge Diameter	VBST network diameter.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which Bridge Protocol Data Units (BPDUs) are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command. ● **MaxHop**: maximum number of hops in the MST region. To specify the parameter, run the **stp max-hops** command.
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region

Item	Description
CIST Root/ERPC Root ID/RPC	CIST Root/ERPC indicates the CIST root bridge ID/ external path cost from the switch to the root bridge. Root ID/RPC indicates the root bridge ID in a VLAN/ external path cost from the switch to the root bridge. **NOTE** CIST Root/ERPC is displayed when STP/RSTP/MSTP is running. Root ID/RPC is displayed when VBST is running.
CIST RegRoot/IRPC	ID of the CIST region root bridge or cost of the path from the switch to the CIST region root switch.
CIST RootPortId RootPortId	CIST RootPortId indicates the CIST root port ID. "0.0" indicates that the switch is the root switch without the root port. RootPortId indicates the root port ID in a VLAN. "0.0" indicates that the switch is the root switch without the root port. **NOTE** CIST RootPortId is displayed when STP/RSTP/MSTP is running. RootPortId is displayed when VBST is running.
BPDU-Protection	Whether BPDU protection is enabled: ● **Disabled**: BPDU protection is disabled. ● **Enabled**: BPDU protection is enabled. To specify the parameter, run the **stp bpdu-protection** command.
TC or TCN received	Number of received topology change (TC) or topology change notification (TCN) BPDUs.
TC count per hello	Number of TC BPDUs received per Hello time.
STP Converge Mode	Convergence mode of the Spanning Tree Protocol (SPT), which can be **fast** or **normal**. For details, see **stp converge**.
Share region-configuration	The status of sharing the region configuration of process 0. The status is fixed as Enabled.
Time since last TC	Time since the last topology change.
Number of TC	Number of topology changes.
Last TC occurred	Interface which causes the last topology change. **NOTE** This parameter does not appear when **Number of TC** is **0**.

Item	Description
Port Protocol	STP status on the interface: ● **Enabled**: STP is enabled on the interface. ● **Disabled**: STP is disabled on the interface. To specify the parameter, run the **stp enable** command.
Port Role	Role of an interface: ● Root Port ● Designated Port ● Alternate Port ● Backup Port ● Master port ● Disabled Port
Port Priority	Interface priority. To configure the interface priority, run the **stp port priority** command.
Port Cost(Dot1T)	Path cost (calculated by dot1t) of an interface: ● **Config**: configured path cost ● **Active**: path cost that is being used To specify the parameter, run the **stp pathcost-standard** and **stp cost** commands.
Designated Bridge/ Port	Switch ID/Port ID The first 16 bits represent the switch's priority in the CIST region, and the last 48 bits represent the switch's MAC address. The first 4 bits of the port ID represent the port's priority, and the last 12 bits represent the port number.
Port Edged	Whether the edge interface (specified by the administrator) is enabled: ● **enabled**: The edge interface is enabled. ● **disabled**: The edge interface is disabled. **Config** indicates the value that is specified in the **stp edged-port** command, and **Active** indicates the value in use.
Point-to-point	Link type of the interface. **Config** indicates the link type that is specified in the **stp point-to-point** command, and **Active** indicates the link type that is being used.

Item	Description
Port Revert Slow	Delay in revertive switching during VBST calculation. - Enabled: The delay in revertive switching during VBST calculation is enabled on the interface. You can run the **stp revertive slow** command to enable this function. - Disabled: The delay in revertive switching during VBST calculation is disabled on the interface.
Port Agreement Legacy	Whether to discard non-standard STP/RSTP packets sent by a HanDreamnet switch. - Enabled: The interface discards non-standard STP/RSTP packets sent by a Handreamnet switch. You can run the **stp agreement-legacy** command to configure the interface to discard non-standard STP/RSTP packets sent by a HanDreamnet switch. - Disabled: The interface does not discard non-standard STP/RSTP packets sent by a Handreamnet switch.
Transit Limit	Maximum number of BPDUs that the current interface can send per second. For details, see **stp transmit-limit**.
Protection Type	Protection type, which can be: - Root: Enable the root protection. Protection takes effect only on the specified interface.To specify the parameter, run the **stp root-protection** command. - Loop: Enable loop protection. Protection takes effect only on the root interface or alternate interface.To specify the parameter, run the **stp loop-protection** command. - None. - Loopback: Enable loopback detection.
Port STP Mode	STP mode of the interface. To specify the parameter, run the **stp mode** command.
Port Protocol Type	Format of BPDUs sent and received on the interface, which can be: - auto - legacy - dot1s The default value is **auto**. **Config** indicates the packet format that is specified in the **stp compliance** command, and **Active** indicates the packet format in use.

Item	Description
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface. In STP/RSTP/MSTP mode, the value is stp. In VBST mode, the value is VBST.
PortTimes	Bridge protocol parameters of the interface: ● **Hello**: interval at which BPDUs are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command. ● **RemHop**: maximum number of hops in the MST region. To specify the parameter, run the **stp max-hops** command.
TC or TCN send	Number of TC or TCN BPDUs sent on the interface.
TC or TCN received	Number of TC or TCN BPDUs received on the interface.
BPDU Sent	Statistics on sent BPDUs, including: ● **TCN**: TCN BPDUs ● **Config**: STP BPDUs ● **RST**: Rapid Spanning Tree Protocol (RSTP) BPDUs ● **MST**: MSTP BPDUs
BPDU Received	Statistics on received BPDUs.
MSTI Bridge ID	Multiple Spanning Tree instance (MSTI) bridge ID.
MSTI RegRoot/IRPC	MSTI root bridge ID/Cost of the internal path (path from the switch to the MSTI root switch).
MSTI RootPortId	ID of the MSTI root interface. **0.0** indicates that the switch is the root switch and does not provide any root interface.
Master Bridge	ID of the bridge where the master interface is located. ● The first 16 bits represent the switch's priority in the CIST. ● The last 48 bits represent the switch's MAC address.
Cost to Master	Cost of the path from the switch to the bridge where the master interface is located. **0** indicates that the master interface is located at the current bridge.
TC received	Number of received TC BPDU.

5.12.8 display stp bridge

Function

The **display stp bridge** command displays details about the spanning tree of a bridge.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] **bridge** { **root** | **local** }

VBST: **display stp** [**vlan** *vlan-id*] **bridge** { **root** | **local** }

Parameters

Parameter	Description	Value
process *process-id*	Multiple Spanning Tree Protocol (MSTP) process ID If **process** *process-id* is not specified, details about the spanning tree of MSTP process 0 will be displayed.	The value is an integer ranging from 1 to 31.
root	Displays details about the spanning tree of the root bridge.	-
local	Displays details about the spanning tree of the local bridge.	-
vlan *vlan-id*	Displays details about the spanning tree of a bridge in a specified VLAN. If **vlan** *vlan-id* is not specified, details about the spanning trees of bridges in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only information about bridges running VBST is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a device provides many interfaces, running the **display stp** command displays a large amount of information, and it is difficult to find information about the spanning trees of the root and local bridges.

Using the **display stp bridge** command, you can easily view details about the spanning trees of the root and local bridges.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.

Example

Display details about the spanning tree of the root bridge of MSTP process 0 when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp bridge root
MSTID             Root ID  Root Cost Hello Max Forward Root Port
                                     Time  Age   Delay
----- ------------------- ---------- ----- --- ------- -----------------
    0 61440.781d-ba56-f06c         0     2  20      15
    1 61440.781d-ba56-f06c         0     2  20      15
```

Display details about the spanning tree of the root bridge running VBST in VLAN 5.

```
<HUAWEI> display stp vlan 5 bridge root
 VLAN-ID          Root ID  Root Cost Hello Max Forward Root
Port
                                     Time  Age   Delay
----- ------------------- ---------- ----- --- ------- -----------------
    5 32773.5489-9876-a2b0     20000     2  20      15 GigabitEthernet0/0/5
```

Table 5-83 Description of the **display stp bridge** command output

Item	Description
MSTID	MSTP instance ID
Root ID	Root bridge ID
Root Cost	Root path cost
Hello Time	Interval at which Bridge Protocol Data Units (BPDUs) are sent from the root switch. To specify the parameter, run the **stp timer hello** command
Max Age	Maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command
Forward Delay	Delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command
Root Port	Root interface
VLAN-ID	VLAN ID.

5.12.9 display stp error packet

Function

The **display stp error packet** command displays the statistics about error packets received by MSTP and the contents of recently received packets.

Format

display stp error packet

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device on a Layer 2 network runs MSTP is attacked by MSTP error packets, the **display stp error packet** command can be used to view recently received MSTP error packets. Check the cause at the peer end.

Example

Display the statistics about error packets received by MSTP and the contents of recently received packets.

```
<HUAWEI> display stp error packet
 4 error-packet(s) have been received and the last one is received at 2011/05/02 12:45:31.
01 80 C2 00 00 00 38 AA D2 11 11 10 00 69 42 42
03 00 00 03 02 7C 00 00 38 AA D2 11 11 10 00 00
00 00 00 00 38 AA D2 11 11 10 80 01 00 00 14 00
02 00 0F 00 00 00 40 00 33 38 61 61 64 32 31 31
31 31 31 30 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 AC 36 17 7F 50 28
3C D4 B8 38 21 D8 AB 26 DE 62 00 00 00 00 00 00
38 AA D2 11 11 10 14
```

5.12.10 display stp global

Function

The **display stp global** command displays global Spanning Tree Protocol (STP) information.

Format

display stp [**process** *process-id*] **global**

Parameters

Parameter	Description	Value
process *process-id*	Multiple Spanning Tree Protocol (MSTP) process ID If **process** *process-id* is not specified, the global STP information of MSTP process 0 will be displayed. VBST does not support processes. Therefore, this parameter cannot be specified when the spanning tree protocol is VBST.	The value is an integer ranging from 1 to 31.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a device provides many interfaces, the **display stp** command output contains a large amount of information, and it is difficult to find the desired information quickly and view global information at a glance. The **display stp brief** command output, by comparison, displays information about spanning trees on interfaces, but not global information.

Using the **display stp global** command, you can view global STP information conveniently.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.

Example

Display brief STP information about MSTP process 0 when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp global
Protocol Status            : Enabled
Bpdu-filter default        : Disabled
Tc-protection              : Enabled
Tc-protection threshold    : 1
Tc-protection interval     : 2s
Edged port default         : Enabled
Pathcost-standard          : Dot1t
```

```
Timer-factor              : 3
Transmit-limit            : 10
Bridge-diameter           : 7
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :61440.781d-ba56-f06c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :61440.781d-ba56-f06c / 0
CIST RegRoot/IRPC   :61440.781d-ba56-f06c / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :85
TC count per hello  :0
STP Converge Mode   :Normal
Share region-configuration :Enabled
Time since last TC  :0 days 9h:12m:34s
Number of TC        :13
Last TC occurred    :GigabitEthernet0/0/4
```

Display brief STP information when VBST is running.

```
<HUAWEI> display stp global
Protocol Status            : Enabled
Bpdu-filter default        : Disabled
Tc-protection              : Enabled
Tc-protection threshold    : 1
Tc-protection interval     : 2s
Edged port default         : Disabled
Pathcost-standard          : Dot1t
Timer-factor               : 3
Transmit-limit             : 6
STP Converge Mode          : Normal
```

Table 5-84 Description of the **display stp global** command output

Item	Description
Protocol Status	Spanning Tree Protocol (STP) status: ● **Enabled**: STP is enabled. ● **Disabled**: STP is disabled. To specify the parameter, run the **stp enable** command.
Bpdu-filter default	Whether the function of configuring device interfaces as Bridge Protocol Data Unit (BPDU) filter interfaces is enabled: ● **Enabled**: The function is enabled. ● **Disabled**: The function is disabled. To specify the parameter, run the **stp bpdu-filter default** command.
Tc-protection	Topology change (TC) protection status. This function is permanently enabled.
Tc-protection threshold	Threshold of TC packets that the device can handle and immediately refresh forwarding entries in a given period. To specify the parameter, run the **stp tc-protection threshold** command.

Item	Description
Tc-protection interval	Time the MSTP takes to handle a given number of TC packets and immediately refresh forwarding entries. To specify the parameter, run the **stp tc-protection interval** command.
Edged port default	Whether the function of configuring all ports of the switch as edge ports is enabled: - **Enabled**: The function is enabled. - **Disabled**: The function is disabled. To specify the parameter, run the **stp edged-port default** command.
Pathcost-standard	Method of calculating the MSTP path cost To specify the parameter, run the **stp pathcost-standard** command.
Timer-factor	Multiplier of Hello time To specify the parameter, run the **stp timer-factor** command.
Transmit-limit	Maximum number of BPDUs that the current interface can send per Hello time. For details, see **stp transmit-limit**.
Bridge-diameter	Network diameter of the MSTP To specify the parameter, run the **stp bridge-diameter** command.
CIST Bridge	Common and internal spanning tree (CIST) bridge ID - The first 16 bits represent the switch's priority in the CIST. - The last 48 bits represent the switch's MAC address.
Config Times	Configured bridge protocol parameters: - **Hello**: interval at which BPDUs are sent. To specify the parameter, run the **stp timer hello** command. - **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. - **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command. - **MaxHop**: maximum number of hops in the MST region. To specify the parameter, run the **stp max-hops** command.

Item	Description
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region
CIST Root/ERPC	CIST root switch ID/Cost of the external path (path from the switch to the CIST root switch)
CIST RegRoot/IRPC	ID of the CIST region root bridge/Cost of the internal path (path from the switch to the CIST region root switch)
CIST RootPortId	ID of the CIST root interface. **0.0** indicates that the switch is the root switch and does not provide any root interface.
BPDU-Protection	Whether BPDU protection is enabled: ● **Disabled**: BPDU protection is disabled. ● **Enabled**: BPDU protection is enabled. To specify the parameter, run the **stp bpdu-protection** command.
TC or TCN received	Number of received TC or topology change notification (TCN) packets
TC count per hello	Number of TC packets received per Hello time
STP Converge Mode	Convergence mode of the Spanning Tree Protocol (SPT), which can be **fast** or **normal**. For details, see **stp converge**.
Share region-configuration	The status of sharing the region configuration of process 0. The status is fixed as Enabled.
Time since last TC	Time since the last topology change
Number of TC	Number of topology changes
Last TC occurred	Interface which causes the last topology change **NOTE** This parameter does not appear when **Number of TC** is **0**.

5.12.11 display stp region-configuration

Function

The **display stp region-configuration** command displays the effective configuration of the MST region on the switching device. The configuration includes the region name, revision level and mapping relationship between VLANs and spanning tree instances.

Format

display stp [**process** *process-id*] **region-configuration** [**digest**]

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. VBST does not support processes. Therefore, this parameter cannot be specified when the spanning tree protocol is VBST.	The value is an integer ranging from 1 to 31.
digest	Displays brief information about the effective MST region.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an MST region is configured and takes effect on the network running MSTP, you can run the **display stp region-configuration** command to view the name, revision level, STP instance, and inter-VLAN mapping of the MST region.

Precautions

- If you run this command in the system view without specifying an MSTP process, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process, information about the MSTP process in this view is displayed by default.

NOTE

For description about MSTP process 0, see **stp process**.

Example

Display the configuration of MST regions when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp region-configuration
Oper configuration
```

```
  Format selector :0
  Region name     :huawei
  Revision level  :0
  Instance   VLANs Mapped
     0       21 to 4094
     1       1 to 10
     2       11 to 20
```

Display brief information about the effective MST region when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp region-configuration digest
 Oper configuration
  Format selector    :0
  Region name        :huawei
  Revision level     :0
  Digest             :0xAC36177F50283CD4B83821D8AB26DE62
```

Display the mapping between VLANs and MSTIs when VBST is running.

```
<HUAWEI> display stp region-configuration
 Oper configuration
  Format selector    :0
  Region name        :00e055539900
  Revision level     :0

  Instance Mode    VLANs Mapped
     0     default 1 to 9, 11 to 19, 21 to 29, 31 to 39, 41 to 4094
    10     static  10
    20     static  20
    30     static  30
    40     static  40
```

Table 5-85 Description of the display stp region-configuration command output

Item	Description
Format selector	Selection factors defined by the MSTP protocol.
Region name	Name of the MST region. For the related commands, see **region-name**.
Revision level	Revision level of the MST region. For the related commands, see **revision-level**.
Instance VLANs Mapped	Mapping between the spanning tree instance and VLANs of the MST region. For the related commands, see **instance** or **vlan-mapping modulo**. If the mapping is incorrect, run the **instance** command to re-map the specified VLAN to the specified MSTI and run the **active region-configuration** command to activate the mapping.
Digest	Brief information about the MST region.

Item	Description
Mode	Mode for the mapping between MSTIs and VLANs: ● Static ● Dynamic ● Default **NOTE** The mapping between MSTIs and VLANs can be statically configured or dynamically specified. The configuration of **instance** is static. The system dynamically allocates an instance ID to a new VLAN in ascending order. If an instance ID is statically configured for this VLAN, the statically configured one takes effect. That is, static configuration takes precedence over dynamic configuration.

5.12.12 display stp tc-bpdu statistics

Function

The **display stp tc-bpdu statistics** command displays statistics of sent and received topology change (TC) and topology change notification (TCN) BPDUs on interfaces.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] **tc-bpdu statistics**

VBST: **display stp** [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*] **tc-bpdu statistics**

Parameters

Parameter	Description	Value
process *process-id*	Specifies the ID of an MSTP process of which statistics of TC and TCN BPDUs are displayed. If the parameter **process** *process-id* is not specified, statistics of TC and TCN BPDUs in MSTP process 0 are displayed.	The value is an integer ranging from 1 to 31.

Parameter	Description	Value
instance *instance-id*	Specifies the ID of an MSTP instance of which statistics of TC and TCN BPDUs are displayed. If the parameter **instance** *instance-id* is not specified, statistics of TC and TCN BPDUs on all interfaces are displayed in the sequence of the interface numbers.	The value is an integer that ranges from 0 to 4094. The value 0 indicates a CIST instance. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
interface *interface-type interface-number*	Specifies the interface on which statistics of TC and TCN BPDUs are displayed. If the parameter **interface** *interface-type interface-number* is not specified, statistics of TC and TCN BPDUs on all interfaces are displayed in the sequence of the interface numbers.	-
slot *slot-id*	Displays the statistics of TC and TCN BPDUs on a spanning tree instance in a specified slot.	The value is an integer and must be an existing slot on the device.
vlan *vlan-id*	Display statistics on sent and received TC and TCN BPDUs on ports in a specified VLAN. If **vlan** *vlan-id* is not specified, statistics on sent and received TC and TCN BPDUs on ports in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only statistics on sent and received TC and TCN BPDUs on ports running VBST are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you need to know whether a fault has occurred on interfaces that send and receive TC/TCN BPDUs, you can run this command to view statistics of these BPDUs and locate the fault.

Prerequisites

In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

Display the statistics of TC/TCN BPDUs on interfaces of an MSTP instance when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp tc-bpdu statistics
 ------------------------- STP TC/TCN information -------------------------
 MSTID Port                    TC(Send/Receive)      TCN(Send/Receive)
 0     GigabitEthernet0/0/9            3/2                 0/0
 0     GigabitEthernet0/0/10           1/0                 0/0
 1     GigabitEthernet0/0/9            14/9                -/-
 1     GigabitEthernet0/0/10           8/10                -/-
 2     GigabitEthernet0/0/9            3/2                -/-
 2     GigabitEthernet0/0/10           1/0                 -/-
```

Display statistics on sent and received TC and TCN BPDUs on ports running VBST.

```
<HUAWEI> display stp vlan 5 tc-bpdu statistics
 ------------------------- STP TC/TCN information
--------------------------
 VLAN-ID  Port                    TC(Send/Receive)      TCN(Send/
Receive)
       5  GigabitEthernet0/0/5        1/615                0/0
```

Table 5-86 Description of the **display stp tc-bpdu statistics** command output

Item	Description
MSTID	ID of an MSTP instance.
Port	Interface name.
TC(Send/Receive)	Statistics of sent and received TC BPDUs.
TCN(Send/Receive)	Statistics of send and received TCN BPDUs. ("-" indicates that MSTP instances except MSTP instance 0 do not have TCN BPDUs sent and received.)
VLAN-ID	VLAN ID.

5.12.13 display stp topology-change

Function

The **display stp topology-change** command displays the statistics about topology changes.

Format

STP/RSTP/MSTP: **display stp** [**process** *process-id*] [**instance** *instance-id*] **topology-change**

VBST: **display stp** [**vlan** *vlan-id*] **topology-change**

Parameters

Parameter	Description	Value
process *process-id*	Displays statistics about the topology changes of a specified MSTP process. If this parameter is not specified, the statistics about the topology changes of MSTP process 0 are displayed.	The value is an integer ranging from 1 to 31.
instance *instance-id*	Displays statistics about the topology changes of a specified STP instance. If this parameter is not specified, the statistics about the topology changes of a CIST instance are displayed.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
vlan *vlan-id*	Displays statistics on topology changes in a specified VLAN. If **vlan** *vlan-id* is not specified, statistics on topology changes in all VLANs are displayed. **NOTE** If **vlan** *vlan-id* is specified, only statistics on topology changes of VBST are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On a Layer 2 network running MSTP, a device clears ARP entries and MAC entries after receiving topology change packets. If a device receives too many topology change packets, the device will frequently clear ARP entries and MAC entries, causing high CPU usage. As a result, network traffic is instable.

The **display stp topology-change** command can be used to display the statistics about MSTP/VBST topology changes. If the statistics increase, network flapping occurs.

Prerequisites

In the case of a non-zero process, the **stp process** *process-id* command must be used to create a process.

Example

Display statistics about MSTP topology changes when MSTP is running.

```
<HUAWEI> display stp topology-change
CIST topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(detected)    :GigabitEthernet0/0/1
   Topology change last received from     :00e0-5b3c-c100
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 1 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(detected)    :GigabitEthernet0/0/2
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 2 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(notified)    :GigabitEthernet0/0/3
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 3 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
```

Display statistics on topology changes in VLAN 5 when VBST is running.

```
<HUAWEI> display stp vlan 5 topology-change
 VLAN 5 topology change information
   Number of topology changes             :316
   Topology change initiator(notified)    :GigabitEthernet0/0/5
   Time since last topology change        :0 days 0h:3m:18s
   Topology change last received from     :5489-9876-a2b0
```

Table 5-87 Description of the display stp topology-change command output

Item	Description
Number of topology changes	Total number of topology changes since initialization. **NOTE** The number of received and sent TC BPDUs in each VLAN may be different during topology convergence, so the number of topology changes in each VLAN may be different.
Time since last topology change	Time since the last topology change.

Item	Description
Topology change initiator(detected)	Interface that initiates a topology change because the interface status changes to detected.
Topology change initiator(notified)	Interface that initiates a topology change after receiving a topology change packet.
Topology change last received from	Source bridge MAC address contained in a topology change packet.
Number of generated topologychange traps	Total number of generated topology-change traps.
Number of suppressed topologychange traps	Total number of suppressed topology-change traps.

5.12.14 display stp vlan

Function

The **display stp vlan** command displays the STP status on an interface added to a specified VLAN.

Format

display stp vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Displays the STP status on an interface added to a specified VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an interface is added to a VLAN, the **display stp vlan** command can be used to the display the STP status on the interface. In this case, the mapping between VLANs and instances does not need to be concerned with.

Prerequisites

In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

Display the STP status on an interface added to a specified VLAN when STP/RSTP/MSTP is running.

```
<HUAWEI> display stp vlan 1
     ProcessId   InstanceId   Port                    Role  State
 ---------------------------------------------------------------------
        0           0        GE0/0/1                 DESI  FORWARDING
```

Table 5-88 Description of the **display stp vlan 1** command output

Item	Description
ProcessId	Process ID
InstanceId.	Instance ID
Port	Interface
Role	Interface role: ● DESI: Designated port ● ROOT: Root port ● ALTE: Alternate port ● BACK: Backup port ● MAST: Master port ● DISA: The interface is in initialization state.
State	Interface status: ● FORWARDING ● DISCARDING

Display the spanning tree status on a port in a specified VLAN when VBST is running.

```
<HUAWEI> display stp vlan 20
-------[VLAN 20 Global Info][Mode VBST]-------
Bridge ID               :32788.4c1f-cc6b-c208
Bridge Diameter         :7
Config Times            :Hello 2s MaxAge 20s FwDly 15s
Active Times            :Hello 2s MaxAge 20s FwDly 15s
Root ID / RPC           :20   .781d-bacc-8bc0 / 199
RootPortId              :128.191 (GigabitEthernet0/0/7)
Root Type               :Normal
BPDU-Protection         :Disabled
STP Converge Mode       :Normal
Time since last TC      :0 days 0h:10m:46s
Number of TC            :1
 ----[Port190(GigabitEthernet0/0/6)][DISCARDING]----
 Port Role              :Designated Port
 Port Priority          :128
```

```
Port Cost(Legacy)      :Config=20000 / Active=20000
Desg. Bridge/Port      :32788.4c1f-cc6b-c208 / 128.190
Port Edged             :Config=Default / Active=Disabled
Point-to-point         :Config=Auto / Active=true
Port Revert Slow       :Disabled
Port Agreement Legacy :Disabled
Transit Limit          :6 packets/hello
Protection Type        :None
Port STP Mode          :VBST
BPDU Encapsulation     :Config=VBST / Active=VBST
BPDU Sent              :0
         TCN: 0, Config: 0, RST: 0
BPDU Received          :0
         TCN: 0, Config: 0, RST: 0
```

Table 5-89 Description of the **display stp vlan** command output

Item	Description
VLAN	VLAN ID.
Bridge ID	Bridge ID: ● The first 16 bits represent the switch's priority. ● The last 48 bits represent the switch's MAC address.
Bridge Diameter	VBST network diameter. To specify the parameter, run the **stp bridge-diameter** command.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which Bridge Protocol Data Units (BPDUs) are sent. To specify the parameter, run the **stp timer hello** command. ● **MaxAge**: maximum TTL of a BPDU. To specify the parameter, run the **stp timer max-age** command. ● **FwDly**: delay in interface status transition. To specify the parameter, run the **stp timer forward-delay** command.
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition
Root ID / RPC	Root switch ID or external cost of the path from the switch to the root switch.
RootPortId	Root port ID. The value 0.0 indicates that the root switch has no root port.
Root Type	Root bridge type.

Item	Description
BPDU-Protection	BPDU protection function: ● Disabled ● Enabled To specify the parameter, run the **stp bpdu-protection** command.
STP Converge Mode	STP converge mode. To specify the parameter, run the **stp converge** command.
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Port Role	Role of a port: ● Root Port ● Designated Port ● Alternate Port ● Backup Port ● Disabled Port
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Legacy)	Path cost of the port, which is calculated using Huawei proprietary algorithm: ● config: indicates the path cost that is manually configured. ● active: indicates the path cost that is actually used. To specify the parameter, run the **stp pathcost-standard** and **stp cost** commands.
Desg. Bridge/Port	IDs of the designated switch and designated port. In the switch ID, the first 16 bits represent the switch's priority, and the last 48 bits represent the switch's MAC address. In the port ID, the first 4 bits represents the port priority, and the last 12 bits represent the port number.
Port Edged	Status of the edge port that is specified by the administrator: ● enabled: The edge port is enabled. ● disabled: The edge port is disabled. Config indicates the value configured using the **stp edged-port** command, and Active indicates the actual value.
Point-to-point	Link type of the port. Config indicates link type configured using the **stp point-to-point** command, and Active indicates the actual link type.

Item	Description
Port Revert Slow	The delay in revertive switching during VBST calculation on a port: - enabled: The delay in revertive switching is enabled. - disabled: The delay in revertive switching is disabled. To specify the parameter, run the **stp revertive slow** command.
Port Agreement Legacy	Whether the interface discards non-standard STP/RSTP packets sent by the HanDreamnet switch: - enabled: The interface discards non-standard STP/RSTP packets sent by the HanDreamnet switch - disabled: The interface does not discard non-standard STP/RSTP packets sent by the HanDreamnet switch
Transmit Limit	Maximum number of BPDUs sent by the port per second. To set the maximum number of BPDUs sent by the port per second, run the **stp transmit-limit (interface view)** command.
Protection Type	Protection type of the port: - root-protection: takes effect only on the designated port. - loop-protection: takes effect only on the root port or alternate port. To specify the parameter, run the **stp root-protection** or **stp loop-protection** command.
Port STP Mode	STP mode on an interface. To specify the parameter, run the **stp mode** command.
BPDU Encapsulation	Format of BPDUs that are sent and received on the interface.In VBST mode, the value is VBST.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: - TCN: topology change notification - Config: STP packets - RST: RSTP packets
BPDU Received	Statistics about the packets received by BPDU.

5.12.15 display vbst bpdu-statistics

Function

The **display vbst bpdu-statistics** command displays VBST BPDU statistics.

Format

display vbst bpdu-statistics [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **slot** *slot-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays VBST BPDU statistics in a specified VLAN. If **vlan** *vlan-id* is not specified, VBST BPDU statistics in all VLANs are displayed.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays VBST BPDU statistics on a specified interface.	-
slot *slot-id*	Displays VBST BPDU statistics on a specified card.	The value is an integer and must be the slot ID of a running card.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check statistics on BPDUs on the switch running VBST, run the **display vbst bpdu-statistics** command.

Prerequisites

In VBST, if NAC authentication is configured but user authentication fails on a port that is configured as an edge port and is in Active state, information about the port is not displayed.

Example

Display VBST BPDU statistics in VLAN 2.

```
<HUAWEI> display vbst bpdu-statistics vlan 2
-------[VLAN 2 ]-------
 ----[Port1010(GigabitEthernet0/0/17)]---
 BPDU Sent           :0
          TCN: 0, Config: 0, RST: 0
 BPDU Received       :0
          TCN: 0, Config: 0, RST: 0
```

```
----[Port1011(GigabitEthernet0/0/18)]---
BPDU Sent           :0
         TCN: 0, Config: 0, RST: 0
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0
----[Port1012(GigabitEthernet0/0/19)]---
BPDU Sent           :0
         TCN: 0, Config: 0, RST: 0
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0
----[Port1031(GigabitEthernet0/0/20)]---
BPDU Sent           :0
         TCN: 0, Config: 0, RST: 0
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0
----[Port1033(GigabitEthernet0/0/21)]---
BPDU Sent           :14664
         TCN: 0, Config: 0, RST: 14664
BPDU Received       :3
         TCN: 0, Config: 0, RST: 3
----[Port1047(GigabitEthernet0/0/22)]---
BPDU Sent           :14643
         TCN: 0, Config: 0, RST: 14643
BPDU Received       :0
         TCN: 0, Config: 0, RST: 0
```

Table 5-90 Description of the **display vbst bpdu-statistics** command output

Item	Description
VLAN	VLAN ID.
Port	Port name.
BPDU Sent	Number of sent BPDUs. The number of sent BPDUs contains the number of sent TCP BPDUs, configuration BPDUs, and RST BPDUs.
TCN	Number of sent/received TCN BPDUs.
Config	Number of sent/received configuration BPDUs.
RST	Number of sent/received RST BPDUs.
BPDU Received	Number of received BPDUs. The number of received BPDUs contains the number of received TCP BPDUs, configuration BPDUs, and RST BPDUs.

5.12.16 display vbst port-vlan statistics

Function

The **display vbst port-vlan statistics** command displays statistics about the PV number of VBST.

Format

display vbst port-vlan statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The PV number is the total number of VLANs in which VBST has been enabled and into which all VBST-enabled interfaces are added. For example, if VBST is enabled on 10 interfaces and each interface is added into 100 VLANs in which VBST is enabled, the number of PVs occupied by all interfaces on the switch is 1000. If the number of occupied PVs exceeds the specifications, the CPU usage may be high. As a result, the switch cannot process tasks in a timely manner, protocol calculation is affected, and the switch cannot be managed by the NMS.

After VBST is enabled on a switch, you can run the **display vbst port-vlan statistics** command to check statistics on the PV number, including the number of occupied PVs and the maximum number of PVs supported by the switch.

Example

Display statistics on the PV number after VBST is enabled on a switch.

```
<HUAWEI> display vbst port-vlan statistics
  Statistics on Eth-Trunk:
--------------------------------------------------
Current PV Num : 6
Support PV Num : 1200
--------------------------------------------------
  Statistics on Slots:
--------------------------------------------------
Slot      Current PV Num      Support PV Num
--------------------------------------------------
0         317                 1200
```

Table 5-91 Description of the **display vbst port-vlan statistics** command output

Item	Description
Statistics on Eth-Trunk	Statistics on the PV number of Eth-Trunks.
Current PV Num	Number of PVs occupied by Eth-Trunks.
Support PV Num	Maximum number of PVs that can be occupied by Eth-Trunks on a switch.
Statistics on Slots	Statistics on the PV number of physical interfaces.

Item	Description
Slot	Slot ID.
Current PV Num	On a standalone switch, this field indicates the number of PVs occupied by physical interfaces. In a stack, this field indicates the number of PVs occupied by physical interfaces of member switches.
Support PV Num	On a standalone switch, this field indicates the maximum number of PVs that can be occupied by physical interfaces. In a stack, this field indicates the maximum number of PVs that can be occupied by physical interfaces of member switches.

5.12.17 ethernet-loop-protection ignored-vlan

Function

The **ethernet-loop-protection ignored-vlan** command configures ignored VLANs for a device. Through the loop protocol calculation, the interface on which the ignored VLAN is configured does not enter the blocked state but stays in the forwarding state.

The **undo ethernet-loop-protection ignored-vlan** command restores the ignored VLAN to the default setting.

By default, no ignored VLAN is configured for a device.

Format

ethernet-loop-protection ignored-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo ethernet-loop-protection ignored-vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1	Specifies the ID of a start VLAN.	The value is an integer ranging from 1 to 4094.
to *vlan-id2*	Specifies the ID of an end VLAN. *vlan-id2* and *vlan-id1* together specify a VLAN range. If you do not specify **to** *vlan-id2*, only the VLAN with ID of *vlan-id1* is configured to the ignored VLAN.	The value is an integer ranging from 1 to 4094. The value of *vlan-id2* must be greater than that of *vlan-id1*.

Parameter	Description	Value
all	Restore all the ignored VLAN to the default setting.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device uses a specific VLAN to create a VLANIF interface and configure it as the management network port, Layer 2 loop protocols (MSTP/RRPP/SEP/ERPS/Smart Link) are enabled on the device to prevent network loops. After the device starts or the Layer 2 loop protocols are enabled, the VLANIF interface enters the blocked state and needs to wait a long time to enter the forwarding state through the protocol calculation. During this period, services are interrupted, and users who use the VLANIF interface cannot operate the device.

To resolve the problem, the **ethernet-loop-protection ignored-vlan** command can be used to configure the specific VLAN to an ignored VLAN. Through loop protocol calculation, the interface on which the ignored VLAN is configured does not enter the blocked state but stays in the forwarding state.

Precautions

If the **ethernet-loop-protection ignored-vlan** command is run more than once, all configurations take effect.

If an ignored VLAN is configured on a ring network, a loop occurs. Therefore, you cannot configure an ignored VLAN in a ring topology.

After the **ethernet-loop-protection ignored-vlan** command is executed, the configuration file shows that STP has been disabled in the VLAN, for example, **stp vlan 100 disable**.

After the **undo ethernet-loop-protection ignored-vlan** command is executed, the system checks whether the number of instances exceeds the limit. If so, the system restores the VBST status in the VLAN. If not, the system displays a message about a failure to restore the VBST status in the VLAN.

Example

Configure VLAN 2 as an ignored VLAN.

```
<HUAWEI> system-view
[HUAWEI] ethernet-loop-protection ignored-vlan 2
Warning: This operation may result in bridging loops. Please make sure there are
 no bridging loops in the VLAN(s). Continue?[Y/N]:Y
```

5.12.18 instance

Function

The **instance** command maps a VLAN to a spanning tree instance.

The **undo instance** command deletes the mapping between a VLAN and a spanning tree instance.

By default, all VLANs are mapped to CIST, that is, instance 0.

Format

instance *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo instance *instance-id* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
instance-id	Specifies the number of a spanning tree instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
vlan *vlan-id1*	Specifies a start VLAN ID.	The value is an integer ranging from 1 to 4094. The start VLAN ID must be smaller than the end VLAN ID.
to *vlan-id2*	Specifies an end VLAN ID. **NOTE** ● VBST maps one VLAN to one instance. Therefore, this parameter cannot be specified when the spanning tree protocol is VBST. ● The 1:1 mapping between MSTIs and VLANs are used only by the switch to determine the VBST forwarding status. This does not mean that VBST supports multi-instance. **instance** in other commands cannot be specified when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **instance** command is used to set mappings between spanning tree instances and VLANs.

Precautions

When using the **undo instance** command, note the following points:

- After the mapping between specified VLANs and a specified spanning tree instance is deleted, these VLANs will be mapped to a CIST, namely, instance 0.
- If no VLAN is specified, all VLANs that have established mappings with the spanning tree instance will be mapped to a CIST.

If the **instance** command is run more than once, all configurations take effect.

A VLAN cannot be mapped to different spanning tree instances. If the **instance** command is run several times, the latest configuration overrides the previous one.

To map the MUX VLAN to a spanning tree instance, you are advised to configure the principal VLAN, subordinate group VLAN, and subordinate separate VLAN in the MUX VLAN in the same spanning tree instance.

Example

Map VLAN 2 to spanning tree instance 1.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] instance 1 vlan 2
```

5.12.19 max bandwidth-affected-linknumber

Function

The **max bandwidth-affected-linknumber** command sets the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.

The **undo max bandwidth-affected-linknumber** command restores the default upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.

By default, the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk is 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 16 on the S5735S-H, S5736-S, and S6720S-S, and 8 on other models.

Format

max bandwidth-affected-linknumber *link-number*

undo max bandwidth-affected-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.	The value is an integer that ranges from 1 to 32 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, 1 to 16 on the S5735S-H, S5736-S, and S6720S-S, and 1 to 8 on other models. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, and S6720S-EI, you can run the **assign trunk** command to set the value, and run the **display trunk configuration** command to check the configuration.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk is used for STP calculation.

For example, device A and device B are connected by two Eth-Trunks. Eth-Trunk1 has three member links that are Up; the Eth-Trunk2 has two member links that are Up. The bandwidth of each member link is 1 Gbit/s, so the bandwidth of Eth-Trunk1 is 3 Gbit/s and the bandwidth of Eth-Trunk2 is 2 Gbit/s. If device A is the root bridge during STP calculation, Eth-Trunk1 on device B is the root port and Eth-Trunk2 is the alternate port. You can run this command to set the upper threshold to 1. Then the bandwidth of Eth-Trunk1 becomes 1 Gbit/s during STP calculation. Bandwidth decrease affects the interface cost, causing STP recalculation. The **max bandwidth-affected-linknumber** command does not affect traffic forwarding on the Eth-Trunk. The bandwidth used to forward traffic is still 3 Gbit/s.

Example

Set the upper threshold to 3.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] max bandwidth-affected-linknumber 3
```

5.12.20 region-name

Function

The **region-name** command configures the MST region name of the switching device.

The **undo region-name** command restores the default name.

By default, the MST region name is the MAC address of the bridge MAC of the switching device.

Format

region-name *name*

undo region-name

Parameters

Parameter	Description	Value
name	Specifies the region name of the switching device.	The value is a case-sensitive string of 1 to 32 characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **region-name** command is used to configure MST region names in order to identify different regions.

VBST does not support regions. Therefore, this command does not take effect when the spanning tree protocol is VBST.

Follow-up Procedure

After configuring MST region parameters, run the **active region-configuration** command to activate the MST region configurations.

Precautions

If an MST region name is changed several times, only the last configuration activated using the **active region-configuration** command takes effect.

Example

Set the MST region name of the switch to "huawei".

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] region-name huawei
```

5.12.21 reset stp error packet statistics

Function

The **reset stp error packet statistics** command clears the statistics of error STP packets.

Format

reset stp error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

You can use the **reset stp error packet statistics** command to clear the history statistics when you need to observe the statistics of error STP packets in a period from the current time.

Precautions

The **reset stp error packet statistics** command clears the statistics about error STP packets are cleared and cannot be restored. Therefore, confirm the action before you use the command.

Example

Clear the statistics about error STP packets.

```
<HUAWEI> reset stp error packet statistics
```

5.12.22 reset stp statistics

Function

The **reset stp statistics** command clears the statistics of a spanning tree.

Format

reset stp [**interface** *interface-type interface-number*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface type and the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Sometimes, traffic statistics within a certain period are needed. In this situation, clear the existing statistics before restarting the count.

When you run the **reset stp statistics** command:

- If you specify an interface, you can clear the statistics of a spanning tree on the interface.
- If you do not specify an interface, you can clear the statistics of spanning trees on all interfaces.

Example

Clear the statistics of spanning trees on GE0/0/1.

```
<HUAWEI> reset stp interface gigabitethernet 0/0/1 statistics
```

5.12.23 reset vbst bpdu-statistics

Function

The **reset vbst bpdu-statistics** command clears VBST BPDU statistics.

Format

reset vbst bpdu-statistics [**interface** *interface-type interface-number* | **slot** *slot-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears BPDU statistics on a specified interface running VBST.	-
slot *slot-id*	Clears BPDU statistics on interfaces running VBST on the card in a specified slot.	The value is an integer and must be an existing slot on the device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting VBST BPDU statistics on a specified interface or on the card in a specified slot in a specified period of time, run the **reset vbst bpdu-statistics** command to clear existing VBST BPDU statistics.

Configuration Impact

The cleared VBST BPDU statistics on a specified interface or on the card in a specified slot cannot be restored. Exercise caution when running the **reset vbst bpdu-statistics** command.

Example

Clear VBST BPDU statistics on GE 0/0/1.

```
<HUAWEI> reset vbst bpdu-statistics interface gigabitethernet 0/0/1
```

5.12.24 revision-level

Function

The **revision-level** command configures the revision level of MST region of a switching device.

The **undo revision-level** command restores the default level.

By default, the revision level of MST region is 0.

Format

revision-level *level*

undo revision-level

Parameters

Parameter	Description	Value
level	Specifies the revision level of the MST region.	The value is an integer ranging from 0 to 65535.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each region is called an MST region and each spanning tree is called a multiple spanning tree instance (MSTI).

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name

- Mappings between MSTIs and VLANs
- MST region revision level

To perform tree calculation in an MST region, multiple devices in this region must have the same value for the three parameters. If the parameters are changed after MSTP is deployed, the change will cause spanning tree recalculation and route flapping on the network. As a result, you are advised not to change the MST region parameters after MSTP is deployed.

If two switching devices have the same region name and VLAN mapping table, the **revision-level** command can be used to set different revision levels for the two devices so that the two devices belong to different MST regions.

MSTP is a standard protocol; therefore, the MSTP revision level of a device is 0 by default. If the revision level of some devices from a specified manufacturer is not 0, you must change the MSTP revision level of devices to be the same to facilitate tree calculation in an MST region.

VBST does not support regions. Therefore, this command does not take effect when the spanning tree protocol is VBST.

Follow-up Procedure

After configuring MST region parameters, run the **active region-configuration** command to activate the MST region configurations.

Precautions

If an MST region revision level is changed several times, only the latest configuration activated using the **active region-configuration** command takes effect.

Example

Set the MSTP revision level of the switching device to 5.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] revision-level 5
```

5.12.25 stp agreement-legacy

Function

The **stp agreement-legacy** command configures an interface to discard non-standard STP/RSTP packets sent by the HanDreamnet switch.

The **undo stp agreement-legacy** command cancels the configuration.

By default, an interface does not discard non-standard STP/RSTP packets sent by the HanDreamnet switch.

Format

stp agreement-legacy

undo stp agreement-legacy

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Huawei datacom device and HanDreamnet switch are deployed on the VBST network, non-standard STP/RSTP packets sent by the HanDreamnet switch may cause temporary loops. You can run the **stp agreement-legacy** command to configure the interface to discard non-standard STP/RSTP packets to prevent temporary loops.

Example

Configure the GE0/0/1 to discard non-standard STP/RSTP packets sent by the HanDreamnet switch.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp agreement-legacy
```

5.12.26 stp binding process

Function

The **stp binding process** command adds the current interface to a specified MSTP process.

The **undo stp binding process** command removes the current interface from the specified MSTP process.

By default, the interface belongs to MSTP process with ID 0.

Format

stp binding process *process-id*

undo stp binding process *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an MSTP process.	The value is an integer ranging from 1 to 31.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an MSTP device properly starts, each port of this device belongs to MSTP process 0 by default. Links connecting MSTP devices and access rings are called access links. If multiple processes are required to isolate services on access rings, the **stp binding process** command can be used to add ports on access links to specified MSTP processes.

Prerequisites

The **stp process** command has been run to configure the corresponding MSTP process. This means that the MSTP process to which a port will be added already exists.

Precautions

A port on an access link can be added to only one MSTP process. If the **stp binding process** command is run several times to add a port to different MSTP processes, only the latest configuration takes effect.

Example

Add a port to MSTP process 1.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp binding process 1
```

5.12.27 stp binding process link-share

Function

The **stp binding process link-share** command adds an interface to multiple MSTP processes for status calculation.

The **undo stp binding process** command removes the interface from status calculation of a certain MSTP process.

By default, an interface enabled with MSTP participates only in the status calculation of MSTP process 0.

Format

stp binding process *process-id1* [**to** *process-id2*] **link-share**

undo stp binding process *process-id1* [**to** *process-id2*]

Parameters

Parameter	Description	Value
process-id1	Specifies the ID of the start MSTP process.	The value is an integer ranging from 1 to 31.
to *process-id2*	Specifies the ID of the end MSTP process.	The value is an integer ranging from 1 to 31.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running MSTP, the link shared by multiple access rings is called a public link. A port on a public link participates in the spanning tree calculation for multiple MSTP processes and access rings. As a result, the port may have multiple statuses. Which spanning tree status can be used as the port status cannot be determined. To prevent this situation, the **stp binding process link-share** command can be used to add this port to an MSTP process. Then, the port always uses its status in MSTP process 0 after participating in the calculation for multiple MSTP processes.

Precautions

After the **stp binding process link-share** command is run on a port, the port will perform the following operations:

- Participates in the status calculation of a specified MSTP process without affecting packet forwarding of this MSTP process.
- Participates in the status calculation of MSTP process 0, affecting packet forwarding of this MSTP process.

If the **stp binding process link-share** command is run more than once, all configurations take effect.

The port configured with the **stp binding process link-share** command must be a port on the public link between devices configured with MSTP multi-process, but not a port that connects an access ring and a device.

If a process has a public link, the **stp enable** command must be run in the view of this process to enable MSTP globally.

For a port that is added to the process in link-share mode, you must run the **stp enable** command in the interface view to enable MSTP.

For a port that is added to the process in link-share mode, the port participates in status calculation of MSTP process 0. Therefore, you must run the **stp enable** command to enable MSTP for process 0.

Example

Configure the port to participate in the status calculation of MSTP process 1 and MSTP process 2.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] quit
[HUAWEI] stp process 2
[HUAWEI-mst-process-2] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp binding process 1 to 2 link-share
```

5.12.28 stp bpdu-filter

Function

The **stp bpdu-filter enable** command specifies a port as a BPDU-filter port.

The **stp bpdu-filter disable** command specifies a port as a non-BPDU-filter port.

The **undo stp bpdu-filter** command restores the default attribute of a BPDU-filter port.

By default, a port is a non-BPDU-filter port.

Format

stp bpdu-filter { **enable** | **disable** }

undo stp bpdu-filter

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, if the **stp edged-port enable** command is used to configure a port as an edge port, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability. This port, however, will still send BPDUs. This may cause BPDUs to be sent to other networks. As a result, these networks flap.

The **stp bpdu-filter enable** command can be used on the port to address this problem. After the **stp bpdu-filter enable** command is used on the port, the port will become a BPDU-filter port, and will not process BPDUs.

NOTICE

If the **stp bpdu-filter enable** command is run on a port, the port will not transmit or process BPDUs. The port cannot negotiate the STP status with the directly connected port on the remote device. Therefore, exercise cautions when using the **stp bpdu-filter enable** command. Running the **stp bpdu-filter enable** command only on edge ports is recommended.

Running the **stp bpdu-filter enable** command in the interface view configures only the current port as a BPDU-filter port. If multiple BPDU-filter ports are required on a device, the **stp bpdu-filter default** command can be used in the system view to configure all the ports as BPDU-filter ports. If some ports need to participate in spanning tree calculation but do not need to be configured as BPDU-filter ports, the **stp bpdu-filter disable** command can be used in the view of these ports to configure them as non-BPDU-filter ports. Similarly, if the **stp bpdu-filter disable** command has been run on a port, the non-BPDU filter port attributes of the port will not change after the **stp bpdu-filter default** command is run.

Precautions

After the **stp bpdu-filter disable** command is run on a port, the port becomes a non-BPDU-filter port. The port is still a non-BPDU-filter port even if the **stp bpdu-filter default** command is run in the system view. After the **undo stp bpdu-filter** command is run on the port, the BPDU-filter attributes of the port restore to the default ones.

Example

On a network edge device, specify GE0/0/1 as a non-BPDU-filter port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp bpdu-filter disable
```

On a network edge device, specify GE0/0/1 as a BPDU-filter port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] stp bpdu-filter enable
```

5.12.29 stp bpdu-filter default

Function

The **stp bpdu-filter default** command specifies all edge ports of a device as BPDU filter ports.

The **undo stp bpdu-filter default** command specifies all edge ports of a device as non-BPDU filter ports.

By default, a port is a non-BPDU filter port.

Format

stp bpdu-filter default

undo stp bpdu-filter default

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, if the **stp edged-port enable** command is used to configure a port as an edge port, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability. This port, however, will still send BPDUs. This may cause BPDUs to be sent to other networks. As a result, these networks flap.

The **stp bpdu-filter enable** command can be used on the port to address this problem. After the **stp bpdu-filter enable** command is used on the port, the port will become a BPDU filter port, and will not process BPDUs.

Running the **stp bpdu-filter enable** command in the interface view configures only the current edge port as a BPDU filter port. If multiple BPDU filter ports are required on a device, the **stp bpdu-filter default** command can be used in the system view to configure all edge ports as BPDU filter ports. Then run the **stp bpdu-filter disable** command in the interface view to change the interfaces that do not need to be configured as BPDU filter interfaces into non-BPDU filter interfaces.

Precautions

After the **stp bpdu-filter default** command is run, a port that has been configured with the **undo stp bpdu-filter** command will become a BPDU filter port. After the **stp bpdu-filter disable** command is run, the port that has been configured with the **undo stp bpdu-filter** command, however, will still serve as a non-BPDU filter port.

NOTICE

After the **stp bpdu-filter default** and **stp edged-port default** commands are run in the system view, none of the ports on the device will initiate any BPDUs or initiate a negotiation with the remote device, and all the ports are in the forwarding state. This may lead to a loop and cause a broadcast storm. Exercise caution when using the **stp bpdu-filter default** and **stp edged-port default** commands in the system view.

Example

On a network edge device, specify all ports as BPDU filter ports.

```
<HUAWEI> system-view
[HUAWEI] stp bpdu-filter default
```

5.12.30 stp bpdu-protection

Function

The **stp bpdu-protection** command enables BPDU protection on a switching device.

The **undo stp bpdu-protection** command disables BPDU protection on a switching device.

By default, the BPDU protection is disabled.

Format

stp bpdu-protection

undo stp bpdu-protection

Parameters

None.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp bpdu-protection** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **stp bpdu-protection** command to configure BPDU protection on a switching device.

Configuration Impact

After BPDU protection is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. The attributes of the edge port are not changed.

Precautions

After BPDU protection is enabled, a switching device sets an edge port to error down state if the edge port receives a BPDU and retains the port as an edge port. To configure the edge port in error-down state to automatically restore to the Up state, run the **error-down auto-recovery cause bpdu-protection interval** *interval-value* command in the system view.

By default, an interface cannot automatically restore to Up state after it is shut down. To restore the interface, run the **shutdown** and **undo shutdown** commands on the interface in sequence. Alternatively, run the **restart** command on the interface to restart the interface.

To configure the interface to go Up automatically, run the **error-down auto-recovery cause bpdu-protection interval** *interval-value* command in the system view to set a recovery delay. After the delay, the interface goes Up automatically.

The edge port generated by automatic detection is not protected by BPDUs. When the edge port receives BPDUs, the port is not shutdown.

Example

Enable the BPDU protection on the switching device.

```
<HUAWEI> system-view
[HUAWEI] stp bpdu-protection
```

5.12.31 stp bridge-diameter

Function

The **stp bridge-diameter** command configures the diameter of the spanning tree.

The **undo stp bridge-diameter** command restores the default diameter.

By default, the diameter of the spanning tree is 7.

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **bridge-diameter** *diameter*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **bridge-diameter**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Configures the diameter of a spanning tree in VLANs. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. - If **to** *vlan-id2* is not specified, the diameter is configured only for the VLAN specified by *vlan-id1*. In the **stp bridge-diameter** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
diameter	Specifies the diameter.	The value is an integer ranging from 2 to 7.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp bridge-diameter** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, the network diameter is the maximum number of devices between two switching devices. If the network diameter is improperly set, network converge may slow down, affecting users' normal communication.

The **stp bridge-diameter** command can be used to set a proper network diameter based on the network scale. This helps to accelerate network convergence.

The following time parameters are related to the network scale:

- Hello Time
- Forward Delay
- Max Age

Precautions

After the **stp bridge-diameter** command is used on a switching device, the switching device will automatically set proper values for Hello Time, Forward Delay, and Max Age based on the configured network diameter.

On an MSTP network, the network diameter configured using the **stp bridge-diameter** command is valid only for CISTs.

Example

Set the network diameter to 5 when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp bridge-diameter 5
```

Set the diameter to 5 for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 bridge-diameter 5
```

5.12.32 stp compliance

Function

The **stp compliance** command configures the format for the MSTP packets that are received and sent on the switching device.

The **undo stp compliance** command restores the default format for the MSTP packets that are received and sent on the switching device.

By default, the MSTP packet format is **auto**.

Format

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

Parameters

Parameter	Description	Value
auto	Indicates that the protocol format is self-adaptive.	-
dot1s	Indicates that the format is standard IEEE 802.1s.	-
legacy	Indicates the private packet format.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP protocol packets have two formats: dot1s (IEEE 802.1s standard packets) and legacy (proprietary protocol packets). The **stp compliance** command can be used on a device to set an MSTP packet format based on the format of the MSTP packet received from a remote device so that this device can better communicate with the remote device.

The auto mode is set to allow a port to automatically switch to the MSTP protocol packet format used by the remote end based on the MSTP protocol packet format received from the remote end. This enables the two interfaces to use the same MSTP protocol packet format.

Precautions

If you configure different packet formats on the same interface in the system view and the interface view, the latest configuration overrides the previous one.

If the **auto** parameter is set, the device preferentially sends IEEE·802.1s-compliant MSTP packets and can process IEEE·802.1s-compliant and vendor-specific MSTP packets. After an interface receives an MSTP packet from a non-Huawei device, the interface automatically switches to the packet format supported by the peer device based on the format of the received packet.

If the **dot1s** parameter is set, the device preferentially sends IEEE·802.1s-compliant MSTP packets and can process IEEE·802.1s-compliant and vendor-specific MSTP packets. After an interface receives an MSTP packet from a non-Huawei device, the interface automatically switches to the packet format supported by the peer device based on the format of the received packet.

If the **legacy** parameter is set, the device preferentially sends vendor-specific MSTP packets and can process IEEE·802.1s-compliant and vendor-specific MSTP packets. After an interface receives an MSTP packet from a non-Huawei device, the interface automatically switches to the packet format supported by the peer device based on the format of the received packet.

Example

Set the format of the MSTP packets to the standard format of the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp compliance dot1s
```

Restore the self-adaptive format of the MSTP packets that are received and sent by the switching device.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo stp compliance
```

5.12.33 stp config-digest-snoop

Function

The **stp config-digest-snoop** command enables digest snooping.

The **undo stp config-digest-snoop** command disables digest snooping.

By default, the digest snooping is disabled.

Format

stp config-digest-snoop

undo stp config-digest-snoop

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

On an MSTP network where Huawei and non-Huawei devices are interconnected, if the Huawei and non-Huawei devices have the same region name, revision level, and VLAN mapping table but have different BPDU keys, you can run this command to enable the Huawei and non-Huawei devices to exchange BPDUs.

Example

Enable digest snooping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp config-digest-snoop
```

5.12.34 stp converge

Function

The **stp converge** command sets the converging mode of a spanning tree protocol.

The **undo stp converge** command restores the default mode.

By default, the converging mode of the spanning tree protocol is **normal**.

Format

stp converge { **fast** | **normal** }

undo stp converge

Parameters

Parameter	Description	Value
fast	Indicates ARP entries that will be directly deleted.	-
normal	Indicates ARP entries that will age quickly.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, if the topology of a spanning tree instance changes, the forwarding paths of VLANs that are mapped to this instance change. As a result, ARP entries related to these VLANs need to be updated. Based on methods for processing ARP entries, the converging modes of a spanning tree protocol are classified into fast and normal:

- In fast mode, entries that need to be updated in an ARP table are directly deleted.
- In normal mode, entries that need to be updated in an ARP table quickly age. A switching device sets the EXPIRE time of these ARP entries to 0 in order to age them. If the number of detection times for aging out ARP entries is

greater than 0, the switching device detects these ARP entries before deleting them.

The **stp converge** command can be used to set a converging mode based on the method for processing ARP entries.

Precautions

If the **stp converge fast** command is run on a switching device and the topology of a spanning tree instance changes, the switching device will directly delete the ARP entries that need to be updated in the ARP table.

If the **stp converge normal** command is run on a switching device and the topology of a spanning tree instance changes, the switching device will age the ARP entries that need to be updated in the ARP table.

Setting the converging mode of a spanning tree protocol to **normal** is recommended. If the fast mode is used, frequent ARP entry deletion will affect services and even may cause the CPU usage of the device to reach 100%. As a result, packet processing will time out, causing network flapping.

In either fast or normal mode, MAC address entries that need to be updated are deleted.

Example

Set the converging mode of the spanning tree protocol on the Ethernet switch as normal.

```
<HUAWEI> system-view
[HUAWEI] stp converge normal
```

5.12.35 stp cost

Function

The **stp cost** command sets the path cost of a port in a spanning tree.

The **undo stp cost** command restores the default path cost.

By default, the path cost of a port in a spanning tree is the path cost corresponding to the port rate.

Format

STP/RSTP/MSTP: **stp** [**process** *process-id*] [**instance** *instance-id*] **cost** *cost*

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **cost** *cost*

STP/RSTP/MSTP: **undo stp** [**process** *process-id*] [**instance** *instance-id*] **cost**

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **cost**

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. If **process** *process-id* is not specified, the status and statistics of an MSTP process with the ID 0 will be displayed.	The value is a decimal integer ranging from 1 to 31.
instance *instance-id*	Specifies the number of a spanning tree instance. If **instance** *instance-id* is not specified, it indicates the path cost of an interface in CIST.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
cost	Specifies the path cost of an interface.	According to different calculation standards, the value ranges are as follows: ● Huawei legacy standard: 1 to 200,000 ● IEEE 802.1d-1998 standard: 1 to 65535 ● IEEE 802.1t standard: 1 to 200,000,000
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the port path cost is set. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the port path cost is configured only for the VLAN specified by *vlan-id1*. In the **stp cost** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The path cost of a port is an important basis for calculating a spanning tree. Path costs determine root port selection. In a spanning tree, the port with the lowest path cost to the root bridge is selected as a root port.

If different path costs are set for a port on an MSTP device in different spanning tree instances, traffic of different VLANs will be forwarded along different physical links and VLAN-based load balancing can be carried out.

Path costs depend on path cost calculation standards. After the path cost calculation standard is determined, set a relatively small path cost within a specified range for a port that has a high link rate. In the Huawei legacy standard, default path costs for ports with different link rates are different, as shown in the following table.

Table 5-92 Mappings between link rates and path costs (Huawei legacy standard)

Link Rate	Recommended Value Default, Value	Recommended Value Range	Value Range
10 Mbit/s	2000	200-20000	1-200,000
100 Mbit/s	200	20-2000	1-200,000
1 Gbit/s	20	2-200	1-200,000
10 Gbit/s	2	2-20	1-200,000
Over 10 Gbit/s	1	1-2	1-200,000

Prerequisites

A path cost calculation standard has been set using the **stp pathcost-standard** command.

Precautions

If the path cost of a port, the spanning tree where the port resides needs to be recalculated.

If the **stp pathcost-standard** command is used to change the path cost calculation standard, the path cost set using the **stp cost** command for a port will be restored to the default value.

Example

Set the path cost of GE0/0/1 in spanning tree instance 2 to 200 when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp instance 2 cost 200
```

Set the path cost of GE0/0/1 in VLAN 10 to 300 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp vlan 10 cost 300
```

5.12.36 stp edged-port

Function

The **stp edged-port enable** command sets the current port as an edge port.

The **stp edged-port disable** command sets the current port as a non-edge port.

The **undo stp edged-port** command restores the default attribute of an edge port.

By default, all the ports on the switching device are non-edge ports.

NOTE

After STP is enabled on a port, edge-port detecting is started automatically. If the port fails to receive BPDU packets within (2 x Hello Timer + 1) seconds, the port is set to an edge port. Otherwise, the port is set to a non-edge port. If the **stp edged-port enable** or **stp edged-port disable** command is executed in the interface view or the **stp edged-port default** command is configured in the system view, automatic detection of the edge port becomes invalid.

Format

stp edged-port { **enable** | **disable** }

undo stp edged-port

Parameters

Parameter	Description	Value
enable	Sets the current port as an edge port.	-
disable	Sets the current port as a non-edge port.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

Precautions

An edge port does not participate in spanning tree calculation. The edge port can transition from Disable to Forwarding state immediately without a delay. The switch automatically configures an edge port as a non-edge port once the edge port receives a configuration BPDU. Then the spanning tree is recalculated.

After the **stp edged-port default** command is run, a port that has been configured with the **undo stp edged-port** command will become an edge port. After the **stp edged-port disable** command is run, the port that has been configured with the **undo stp edged-port** command, however, will still serve as a non-edge port.

NOTE

The device supports automatic detection of the edge port. When the port connected to the terminal changes from Down to Up, the port enters the forwarding state after (2 x Hello Timer + 1) seconds. If automatic detection is not configured, the port enters the forwarding state after 30s.

A device configured with automatic edge port detection may fail to detect edge ports when the CPU usage is high. Therefore, you are advised to manually configure edge ports when the device's CPU usage is high.

Example

Configure GE0/0/1 as an edge port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp edged-port enable
```

5.12.37 stp edged-port default

Function

The **stp edged-port default** command configures the ports on a switching device as edge ports.

The **undo stp edged-port default** command restores the default setting.

By default, the ports on a switching device are non-edge ports.

NOTE

After STP is enabled on a port, edge-port detecting is started automatically. If the port fails to receive BPDU packets within (2 x Hello Timer + 1) seconds, the port is set to an edge port. Otherwise, the port is set to a non-edge port.

Format

stp edged-port default

undo stp edged-port default

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

NOTICE

After the **stp edged-port default** command is run on a device, all ports of the device will be become edge ports. During network topology calculation, running the **stp edged-port default** command may cause a loop. Exercise caution when using this command.

Precautions

If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree.

To prevent attackers from forging BPDUs to change edge ports on a switching device to non-edge ports, you can run the **stp bpdu-protection** command in the system view to configure BPDU protection on the switching device. After BPDU protection is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. The attributes of the edge port are not changed.

After the **stp edged-port default** command is run, a port that has been configured with the **undo stp edged-port** command will become an edge port. After the **stp edged-port disable** command is run, the port that has been configured with the **undo stp edged-port** command, however, will still serve as a non-edge port.

Example

Configure all ports on an edge device as edge ports.

```
<HUAWEI> system-view
[HUAWEI] stp edged-port default
```

5.12.38 stp enable

Function

The **stp enable** command enables STP/RSTP/MSTP/VBST on a switching device or an interface.

The **undo stp enable** command disables STP/RSTP/MSTP/VBST on a switching device or an interface.

The **stp disable** command disables STP/RSTP/MSTP/VBST on a switching device or an interface.

The **undo stp disable** command enables STP/RSTP/MSTP/VBST on a switching device or an interface.

By default, STP/RSTP/MSTP/VBST is enabled globally and on an interface.

Format

stp enable

undo stp enable

stp disable

undo stp disable

Parameters

None

Views

System view, MSTP process view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a complex Layer 2 network, to prevent loops or break loops, STP/RSTP/MSTP/VBST can be configured on switching devices.

Running the **stp enable** command enables STP/RSTP/MSTP/VBST. The devices running STP/RSTP/MSTP/VBST discover loops on the network by exchanging information with each other and trim the ring topology into a loop-free tree topology by blocking a certain interface. In this manner, replication and circular propagation of packets are prevented on the network. In addition, the processing performance of devices is prevented from deteriorating.

Enabling STP/RSTP/MSTP/VBST consumes system resources so that you can run the **stp disable** command to disable STP/RSTP/MSTP/VBST on devices or interfaces that do not participate in the spanning tree calculation.

NOTE

To prevent the CPU from being affected and faults such as network flapping from occurring, the following lists the recommended maximum number of STP-enabled ports in Up state for different models:

SS1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S, S6720S-S, S5720I-SI, S5735-S, S500, S5735S-S, and S5735-S-I: 128

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 256

Pre-configuration Tasks

After STP/RSTP/MSTP is enabled on a ring network, STP/RSTP/MSTP immediately calculates spanning trees on the network. Configurations on a switching device, such as, the switching device priority and port priority, will affect spanning tree calculation. Any change of the configurations may cause network flapping. Therefore, to ensure rapid and stable spanning tree calculation, before enabling STP/RSTP/MSTP, perform basic configurations on the switching device and its interfaces. For example:

- Run the **stp mode** { **mstp** | **rstp** | **stp** } command to set the working mode of the switching device.
- Run the **stp** [**instance** *instance-id*] **priority** *priority* command to set the priority of the switching device in the spanning tree.
- Run the **stp** [**process** *process-id*] [**instance** *instance-id*] **port priority** *priority* command to set the priority of the interface in the spanning tree instance.

- Run the **stp** [**instance** *instance-id*] **root primary** command to set the switching device as the primary root bridge of the spanning tree.
- Run the **stp** [**instance** *instance-id*] **root secondary** command to set the switching device as the secondary root bridge of the spanning tree.
- Run the **stp** [**process** *process-id*] [**instance** *instance-id*] **cost** *cost* command to set the path cost of the interface in the spanning tree instance.
- If the spanning tree protocol is MSTP, run the **region-name** *name*, **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>, **vlan-mapping modulo**, and **revision-level** *level* commands to configure the MST region.

When VBST is enabled on a ring network, VBST immediately starts spanning tree calculation. Parameters such as the switch priority and port priority affect spanning tree calculation, and change of these parameters may cause network flapping. To ensure fast and stable spanning tree calculation, perform basic configurations on the switch and ports before enabling VBST.

- Run the **stp mode vbst** command to set the working mode of the switch.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **priority** *priority* command to set the priority of the switch in the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **port priority** *priority* command to set the priority of the port in the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root primary** command to set the switch as the root bridge of the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root secondary** command to set the switch as the secondary root bridge of the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **cost** *cost* command to set the path cost of the port in the spanning tree instance.
- Run the **instance** *instance-id* **vlan** *vlan-id* command to configure 1:1 mapping between MSTIs and VLANs.

Other configurations are needed based on real-world situations.

Precautions

- If STP/RSTP/MSTP/VBST is enabled on an interface, the interface participates in the spanning tree calculation and determines whether it is in the forwarding state according to the calculation result.
- If STP/RSTP/MSTP/VBST is disabled on an interface, the interface does not participate in the spanning tree calculation and it is always in the forwarding state.
- STP/RSTP/MSTP/VBST must be enabled on all interfaces that participate in the spanning tree calculation. Otherwise, a loop may occur.
- Spanning tree calculation may result in network flapping. Before network convergence, packets cannot be correctly forwarded. In this case, if the DHCP server is configured on a VLANIF interface, DHCP clients obtain IP addresses slowly. To solve the problem, disable STP or configure the device interface connected to a terminal as the edge interface.
- If the **undo stp enable** or **stp disable** command is run in the system view, the global STP function is disabled, which may cause a loop.
- If the **undo stp enable** or **stp disable** command is run in the MSTP process view, the STP function in the MSTP process is disabled, which may cause a loop in the MSTP process.

Follow-up Procedure

After STP is enabled globally and on an interface, run the **stp vlan enable** command to enable STP in a VLAN so that VBST can take effect.

Example

Enable STP/RSTP/MSTP/VBST on a switching device.

```
<HUAWEI> system-view
[HUAWEI] stp enable
```

Disable STP/RSTP/MSTP/VBST on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp disable
```

5.12.39 stp link-share-protection

Function

The **stp link-share-protection** command enables the shared-link protection for an MSTP process.

The **undo stp link-share-protection** command disables the shared-link protection of an MSTP process.

By default, the shared-link protection of an MSTP process is disabled.

Format

stp link-share-protection

undo stp link-share-protection

Parameters

None

Views

MSTP process view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In networking with a switching device dual-homed to an upper-layer network, if a public link becomes faulty, rings that the public link accesses may unblock their blocked ports. As a result, a permanent network loop is generated.

The **stp link-share-protection** command can be used to enable shared-link protection in a specified process in order to prevent this problem. Then, when a public link becomes faulty, the working mode of each device on the public link will be forcibly switched to RSTP. After shared-link protection and root protection are deployed, a port will still be in blocked state even after receiving packets of a higher priority from a downstream device. This prevents network loops.

Precautions

Shared-link protection is valid only in processes. Before running the **stp link-share-protection** command, check that relevant ports have been correctly bound to the corresponding process using the **stp binding process** command.

Example

Enable the shared-link protection for MSTP process 1.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] stp link-share-protection
```

5.12.40 stp loop-protection

Function

The **stp loop-protection** command enables loop protection on the current port.

The **undo stp loop-protection** command disables loop protection on the current port.

By default, loop protection on ports is disabled.

Format

stp loop-protection

undo stp loop-protection

Parameters

None.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, a switching device maintains the status of the root port and blocked port by continually receiving BPDUs from the upstream switching device. If ports cannot receive BPDUs from the upstream switching device due to link congestion or unidirectional link failures, the switching device will re-select a root port. Then, the previous root port becomes a designated port and the previous blocked port enters the Forwarding state. As a result, loops may occur on the network.

To prevent the preceding problems, deploy loop protection. If the root port or alternate port does not receive BPDUs from the upstream device for a long time, the switch enabled with loop protection sends a notification to the NMS. If the root port is used, the root port enters the Discarding state and becomes the designated port. If the alternate port is used, the alternate port keeps blocked and becomes the designated port. In this case, loops will not occur. After the link is not congested or unidirectional link failures are rectified, the port receives BPDUs for negotiation and restores its original role and status.

NOTE

- An alternate port is the backup of the root port. When the root port can normally send and receive BPDUs, the alternate port is in the blocked state.
- Between two interconnected switching devices in a spanning tree, the switching device nearer to the root bridge is the upstream device of the other devices.

Precautions

Loop protection and root protection cannot be configured on the same interface simultaneously.

If loop protection needs to be configured on an interface in a process with a non-zero ID, the **stp binding process** command must have been run to bind this interface to the process.

Example

Enable loop protection on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp loop-protection
```

5.12.41 stp max-hops

Function

The **stp max-hops** command sets the maximum hops of a spanning tree in an MST region.

The **undo stp max-hops** command restores the default value of the maximum hops of a spanning tree.

By default, the maximum hops in an MST region is 20.

Format

stp max-hops *hop*

undo stp max-hops

Parameters

Parameter	Description	Value
hop	Specifies the maximum hops.	The value ranges from 1 to 40.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp max-hops** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Switching devices on a Layer 2 network running MSTP communicate with each other by exchanging MST BPDUs. An MST BPDU has a field that indicates the number of remaining hops.

- The number of remaining hops in a BPDU sent by the root switching device equals the maximum number of hops.
- The number of remaining hops in a BPDU sent by a non-root switching device equals the maximum number of hops minus the number of hops from the non-root switching device to the root switching device.
- If a switching device receives a BPDU in which the number of remaining hops is 0, the switching device will discard the BPDU.

Therefore, the maximum number of hops of a spanning tree in an MST region determines the network scale. The **stp max-hops** command can be used to set the maximum number of hops in an MST domain so that the network scale of a spanning tree can be controlled.

Precautions

In an MST region, the maximum number of hops set on the root switching device in a CIST or an MSTI is the maximum number of hops in the CIST or MSTI.

Example

Set the maximum hops in the MST region to 35.

```
<HUAWEI> system-view
[HUAWEI] stp max-hops 35
```

5.12.42 stp mcheck

Function

The **stp mcheck** command configures a port to switch from the STP mode back to the RSTP/MSTP/VBST mode.

By default, a port transitions from the STP mode to the RSTP/MSTP/VBST mode by receiving BPDUs. A port that does not receive BPDUs cannot transition from the STP mode to the RSTP/MSTP/VBST mode.

Format

stp mcheck

Parameters

None

Views

System view, MSTP process view, Ethernet interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, 25GE interface view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp mcheck** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a port of an RSTP/MSTP/VBST switching device is directly connected to an STP switching device, the port automatically switches to the STP mode and then sends BPDUs. This ensures that the two switching devices properly communicate with each other. If the STP switching device is powered off or removed, the port on the RSTP/MSTP/VBST switching device cannot switch back to the RSTP/MSTP/VBST mode. As a result, the RSTP/MSTP/VBST device cannot communicate with other RSTP/MSTP/VBST switching devices.

The **stp mcheck** command can be used to address this problem. After this command is run on a port, the port will switch from the STP mode back to the RSTP/MSTP/VBST mode.

When a VBST-enabled switch connects to an MSTP-enabled switch, the connected port of the MSTP-enabled switch automatically switches to the RSTP mode through negotiation. When the VBST-enabled switch switches to the MSTP mode, the connected ports of the two switches may still work in RSTP mode due to the time sequence problem. You can perform the following operations to manually switch the ports to the MSTP mode.

Prerequisites

If a port in a process with a non-zero ID needs to be configured to switch from the STP mode back to the RSTP/MSTP mode, the port must have been bound to the corresponding process using the **stp binding process** *process-id* command.

Precautions

This command does not take effect on a port in Down state.

Running the **stp mcheck** command in the system view configures all ports on the device to switch back to the RSTP/MSTP/VBST mode.

Running the **stp mcheck** command in the MSTP process view configures all ports bound to the current MSTP process to switch back to the RSTP/MSTP mode.

Running the **stp mcheck** command in the interface view configures only the current port to switch back to the RSTP/MSTP/VBST mode.

Example

Perform MCheck on GE0/0/1 and switch it to the MSTP mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp mcheck
```

5.12.43 stp mode (MSTP process view)

Function

The **stp mode** command sets the operation mode of spanning tree protocol for the current MSTP process.

The **undo stp mode** command restores the default operation mode of the current MSTP process.

By default, the operation mode of spanning tree protocol for the current MSTP process is MSTP.

Format

stp mode { **mstp** | **rstp** | **stp** }

undo stp mode

Parameters

Parameter	Description	Value
mstp	Indicates the MSTP operation mode for the ports bound to the current MSTP process.	-
rstp	Indicates the RSTP operation mode for the ports bound to the current MSTP process.	-

Parameter	Description	Value
stp	Indicates the STP operation mode for the ports bound to the current MSTP process.	-

Views

MSTP process view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an MSTP process is created on an MSTP network, all ports bound to the MSTP process operate in MSTP mode by default. These ports may be connected to STP/RSTP devices. As a result, spanning trees cannot be properly calculated, because devices running different spanning tree protocols cannot exchange packets.

To address this problem, the **stp mode** command can be set an operation mode for a switching device. The operation mode can be MSTP, RSTP, or STP.

By default, if a port on a switching device is bound to a process and is connected to an STP switching device, the switching device automatically sets the operation mode of this port to STP and the operation mode of the other ports to MSTP.

Precautions

- After the **stp mode mstp** command is run in an MSTP process, all ports that are running MSTP and are bound to the MSTP process, excluding the ports directly connected to STP switching devices, operate in MSTP mode and can send MST BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode rstp** command is run in an MSTP process, all ports that are running MSTP and are bound to the MSTP process, excluding the ports directly connected to STP switching devices, operate in RSTP mode and can send RST BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode stp** command is run in an MSTP process, all ports bound to the MSTP process operate in STP mode and send configured BPDUs.

A port operating in MSTP mode can communicate with a port operating in RSTP mode.

Running the **stp mode rstp** command on a device that supports MSTP is not recommended. The function of the **stp mode rstp** command can be implemented by the **stp mode mstp** command by default.

Example

Set the operation mode of MSTP process 1 to the STP mode.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] stp mode stp
```

5.12.44 stp mode (system view)

Function

The **stp mode** command sets the operation mode of the spanning tree protocol on a switching device.

The **undo stp mode** command restores the default operation mode of the spanning tree protocol.

By default, the switching device operates in MSTP mode.

Format

stp mode { **mstp** | **rstp** | **stp** | **vbst** }

undo stp mode

Parameters

Parameter	Description	Value
mstp	Indicates the MSTP mode.	-
rstp	Indicates the RSTP mode.	-
stp	Indicates the STP mode.	-
vbst	Indicates the VBST mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the network running a spanning tree protocol, switches running different spanning tree protocols cannot communicate with each other. As a result, spanning trees cannot be properly calculated. A switch has four operation modes: VBST, MSTP, RSTP, and STP.

The **stp mode** command can be used to set a proper operation mode for a spanning tree protocol on a switching device and enables the switching device to identify BPDUs sent by a switching device that runs a different spanning tree protocol during communication.

By default, all ports on a switching device operate in MSTP mode. When a switching device finds that it is directly connected to an STP switching device, it automatically switches the operation mode and the port directly connected to the STP switching device to STP.

Configuration Impact

- After the **stp mode vbst** command is run on a switch, all ports running VBST on the switch, excluding the ports directly connected to STP switches, operate in VBST mode and can send VBST BPDUs. The ports directly connected to STP switches operate in STP mode.
- After the **stp mode mstp** command is run on a switching device, all ports running MSTP on the switching device, excluding the ports directly connected to STP switching devices, operate in MSTP mode and can send MSTP BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode rstp** command is run on a switching device, all ports running RSTP on the switching device, excluding the ports directly connected to STP switching devices, operate in RSTP mode and can send RSTP BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode stp** command is run on a switching device, all ports of the switching device operate in STP mode and send configured BPDUs.

Precautions

- A port operating in MSTP mode can communicate with a port operating in RSTP mode.
- VBST BPDUs and RST BPDUs can be used at the same time.
- The **stp mode rstp** command can be used to enable a switch that does not support MSTP to communicate with an STP switch.
- In VBST mode, the MAC address 0100-0CCC-CCCD is displayed in the **display bpdu mac-address** command output. In STP/RSTP/MSTP mode, the MAC address 0100-0CCC-CCCD is not displayed unless the **bpdu mac-address** command specifies the MAC address as 0100-0CCC-CCCD.
- An Eth-Trunk on the S6735-S, S6720-EI, and S6720S-EI can meet at most three of the following conditions simultaneously:
  - The Eth-Trunk is a Layer 2 interface, or the working mode of the Eth-Trunk is changed from Layer 3 to Layer 2 using the **portswitch** or **portswitch batch** command.
  - The Eth-Trunk is configured as a Layer 2 remote observing port using the **observe-port** command.
  - The operating mode of the spanning tree protocol is set to VBST on the switch using the **stp mode** command.
  - VBST is enabled on the Eth-Trunk using the **stp enable** command.

Example

Set the operation mode of the switching device to the STP mode.

```
<HUAWEI> system-view
```

```
[HUAWEI] stp mode stp
```

5.12.45 stp no-agreement-check

Function

The **stp no-agreement-check** command configures the common fast transition mechanism on an interface.

The **undo stp no-agreement-check** command restores the default fast transition mechanism on an interface.

STP does not support fast transition. By default, for RSTP, MSTP, and VBST, fast transition in enhanced mode is used on a port.

Format

stp no-agreement-check

undo stp no-agreement-check

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Huawei and non-Huawei data communication devices are deployed on a network running a spanning tree protocol, the Huawei devices and non-Huawei devices may fail to communicate with each other, because they have different Proposal/Agreement mechanisms. To address this problem, the **stp no-agreement-check** command can be used to set a common fast transition mechanism or an enhanced transition mechanism on a port.

- Running the **stp no-agreement-check** command configures a common fast transition mechanism on a port.
- Running the **undo stp no-agreement-check** command configures an enhanced fast transition mechanism on a port.

Precautions

The fast transition mechanism is also called the Proposal/Agreement mechanism. The device currently supports the following modes:

- Enhanced mode: The current interface counts a root port when it computes the synchronization flag bit.
  a. An upstream device sends a Proposal message to a downstream device requesting fast transition. After receiving the message, the downstream device sets the port connected to the upstream device as the root port and blocks all non-edge ports.
  b. The upstream device then sends an Agreement message to the downstream device. After the downstream device receives the message, the root port transitions to the Forwarding state.
  c. The downstream device then responds with an Agreement message. After receiving the message, the upstream device sets the port connected to the downstream device as the designated port, and then the status of the designated port changes to Forwarding.
- Common mode: The current interface ignores the root port when it computes the synchronization flag bit.
  a. An upstream device sends a Proposal message to a downstream device requesting fast transition. After receiving the message, the downstream device sets the port connected to the upstream device as the root port and blocks all non-edge ports. Then, the status of the root port changes to Forwarding.
  b. The downstream device then responds with an Agreement message. After receiving the message, the upstream device sets the port connected to the downstream device as the designated port, and then the status of the designated port changes to Forwarding.

NOTE

Between two interconnected switching devices in a spanning tree, the switching device nearer to the root bridge is the upstream device of the other devices.

Example

Configure the common fast transition mechanism for the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp no-agreement-check
```

5.12.46 stp pathcost-standard

Function

The **stp pathcost-standard** command sets the standard used to calculate the path cost.

The **undo stp pathcost-standard** command restores the default standard used to calculate the path cost.

By default, the IEEE 802.1t is used to calculate the path cost.

Format

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

Parameters

Parameter	Description	Value
dot1d-1998	Indicates IEEE 802.1D standard that is used to calculate the path cost.	-
dot1t	Indicates IEEE 802.1t standard that is used to calculate the path cost.	-
legacy	Indicates Huawei legacy standard that is used to calculate the path cost.	-

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp pathcost-standard** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A path cost is a port parameter, and is used by a spanning tree protocol to select a link. By calculating path costs, a spanning tree protocol selects stable links, blocks redundant paths, and trims a network into a loop-free network. The path cost range is determined by the path cost calculation standard.

Table 5-93 lists path costs defined by the IEEE 802.1D-1998 standard, IEEE 802.1t standard, and Huawei legacy standard. Different vendors use different standards.

Table 5-93 Path cost list

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1t Standard	Huawei Legacy Standard
0	-	65535	200,000,000	200,000
10 Mbit/s	Half-Duplex	100	2,000,000	2000
	Full-Duplex	99	1,999,999	1999

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1t Standard	Huawei Legacy Standard
	Aggregated Link 2 Ports	95	1,000,000	1800
	Aggregated Link 3 Ports	95	666,666	1600
	Aggregated Link 4 Ports	95	500,000	1400
100 Mbit/s	Half-Duplex	19	200,000	200
	Full-Duplex	18	199,999	199
	Aggregated Link 2 Ports	15	100,000	180
	Aggregated Link 3 Ports	15	66,666	160
	Aggregated Link 4 Ports	15	50,000	140
1000 Mbit/s	Full-Duplex	4	20,000	20
	Aggregated Link 2 Ports	3	10,000	18
	Aggregated Link 3 Ports	3	6666	16
	Aggregated Link 4 Ports	3	5000	14
2500 Mbit/s	Full-Duplex	3	8000	17
	Aggregated Link 2 Ports	3	4000	12
	Aggregated Link 3 Ports	3	2666	7
	Aggregated Link 4 Ports	2	2000	2
10 Gbit/s	Full-Duplex	2	2000	2
	Aggregated Link 2 Ports	1	1000	1
	Aggregated Link 3 Ports	1	666	1

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1t Standard	Huawei Legacy Standard
	Aggregated Link 4 Ports	1	500	1
40 Gbit/s	Full-Duplex	1	500	1
	Aggregated Link 2 Ports	1	250	1
	Aggregated Link 3 Ports	1	166	1
	Aggregated Link 4 Ports	1	125	1

Precautions

If the path cost calculation standard is changed on a port, the path cost of the port is restored to the default value. The **stp cost** command can be used to set a path cost for a port.

Usually, all switching devices on the same network use the same path cost calculation standard.

Example

Use the IEEE 802.1d-1998 to calculate the path cost.

```
<HUAWEI> system-view
[HUAWEI] stp pathcost-standard dot1d-1998
```

5.12.47 stp point-to-point

Function

The **stp point-to-point** command sets the link type of a port.

The **undo stp point-to-point** command restores the default link type.

By default, the link type of the ports on the switching device is **auto**. That is, the spanning tree protocol detects whether a port is connected to a P2P link.

Format

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

Parameters

Parameter	Description	Value
force-true	Indicates the link type is P2P.	-
force-false	Indicates the link type is non-P2P.	-
auto	Indicates that the spanning tree protocol detects automatically whether the port is connected to a P2P link.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, if a port of a switching device is connected to a non-P2P link, the port cannot perform fast status transition.

If a port works in full-duplex mode, the port is connected to a P2P link, and **force-true** can be set in the **stp point-to-point** command.

If a port works in half-duplex mode, the **stp point-to-point force-true** command can be used to forcibly set the type of the link to which the port is connected to P2P, implementing rapid network convergence.

Precautions

The **stp point-to-point** command configuration on a port takes effect in all spanning tree instances where the port resides.

Example

Set the link type of GE0/0/1 as P2P.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp point-to-point force-true
```

5.12.48 stp port priority

Function

The **stp port priority** command sets the priority of a port in a spanning tree.

The **undo stp port priority** command restores the default priority.

By default, the priority of a port in a spanning tree is 128.

Format

STP/RSTP/MSTP: **stp** [**process** *process-id*] [**instance** *instance-id*] **port priority** *priority*

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **port priority** *priority*

STP/RSTP/MSTP: **undo stp** [**process** *process-id*] [**instance** *instance-id*] **port priority**

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **port priority**

Parameters

Parameter	Description	Value
process *process-id*	Indicates the ID of an MSTP process. If **process** *process-id* is not specified, the status and statistics of an MSTP process with the ID 0 will be displayed.	The value is an integer ranging from 1 to 31.
instance *instance-id*	Specifies the spanning tree instance. If this parameter is not specified, the statistics about the topology changes of a CIST are displayed.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
priority	Specifies the priority of a port.	The priority ranks from 0 to 240 in descending order. The value is an integer multiple of 16, such as, 0, 16, and 32.
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the port priority is configured. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the port priority is configured only for the VLAN specified by *vlan-id1*. In the **stp priority** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When ports participate in spanning tree calculation, the PIDs of these ports on switching devices may affect the designated port election result. During spanning tree calculation, the port with the smallest PID is elected as the designated port.

NOTE

A PID is the ID of a port, and consists of a 4-bit priority and a 12-bit port number.

The **stp port priority** command can be used to change the priority of a port. This affects the PID of the port and determines whether the port can be elected as the designated port.

Precautions

When the priority of a port changes, a spanning tree protocol recalculates the role of the port and performs status transition for the port.

The priority of a port determines the role of the port in a specified spanning tree instance and process. You can set different priorities for a port in different spanning tree instances or processes so that user traffic can be forwarded along different links and traffic load balancing can be implemented.

Enabling MSTP on a ring network immediately triggers spanning tree calculation. If basic configurations are not performed on switches and interfaces before MSTP is enabled, network flapping may occur upon changes to parameters such as device priority and interface priority.

Example

Set the priority of GE0/0/1 to 16 in the spanning tree instance 2 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp instance 2 port priority 16
```

Set the priority of GE 0/0/1 in VLAN 10 to 32 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp vlan 10 port priority 32
```

5.12.49 stp priority

Function

The **stp priority** command sets the priority of the switching device in a spanning tree.

The **undo stp priority** command restores the default priority.

By default, the priority of the switching device in a spanning tree is 32768.

Format

STP/RSTP/MSTP: **stp** [**instance** *instance-id*] **priority** *priority*

STP/RSTP/MSTP: **undo stp** [**instance** *instance-id*] **priority**

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **priority** *priority*

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **priority**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of a spanning tree instance. If the parameter **instance** *instance-id* is not specified, the configuration takes effect on a CIST instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
priority	Specifies the priority of the switching device in a spanning tree. The smaller the value is, the higher the switch priority is.	The priority ranks from 0 to 61440. The value is an integer multiple of 4096, such as 0, 4096 and 8192. The default is 32768.

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the switch priority is configured. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, the switch priority is configured only for the VLAN specified by *vlan-id1*. In the **stp priority** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp priority** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge.

On an STP/RSTP/MSTP/VBST network, each spanning tree has only one root bridge, which is responsible for sending BPDUs. Owning to the importance of the root bridge, the switching device with high performance and network hierarchy is generally chosen as the root bridge. The priority of such a switching device, however, may not be that high. Therefore, setting a high priority for the switching device is necessary so that the device can function as a root bridge.

Other devices with low performance and network hierarchy are not fit to be a root bridge. Therefore, set low priorities for these devices.

On an MSTP network, each switching device can be set with a distinct priority in each spanning tree instance. On a VBST network, each switch can be set with a priority for the spanning tree in each VLAN.

Precautions

The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

If a switching device has been configured as the primary or secondary root bridge, before changing the priority of the switching device, run the **undo stp** [**instance** *instance-id*] **root** command to disable the root bridge or secondary root bridge function.

If the **stp root primary** command is run to set a switching device as the primary root bridge, the priority value of the switching device is 0.

If the **stp root secondary** command is run to set a switching device as the secondary root bridge, the priority value of the switching device is 4096.

Enabling MSTP on a ring network immediately triggers spanning tree calculation. If basic configurations are not performed on switches and interfaces before MSTP is enabled, network flapping may occur upon changes to parameters such as device priority and interface priority.

Example

Set the priority of the switching device in spanning tree instance 1 to 4096 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 1 priority 4096
```

Set the priority of the switch in VLAN 10 to 4096 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 priority 4096
```

5.12.50 stp process

Function

The **stp process** command has the following functions:

- Create an MSTP process with a specified ID and enter the MSTP process view if the specified MSTP process does not exist.
- Display the MSTP process view if the specified MSTP process exists.

The **undo stp process** command deletes a specified MSTP process.

By default, all MSTP configurations on a device belong to MSTP process 0.

Format

stp process *process-id*

undo stp process *process-id*

Parameters

Parameter	Description	Value
process-id	Indicates the ID of an MSTP process.	The value is an integer ranging from 1 to 31.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network where MSTP is run, if devices belong to multiple access rings that are isolated from each other and these access rings do not need intercommunication, MSTP cannot be used to calculate one spanning tree for all these access rings. Instead, MSTP must be enabled on each access ring to calculate the spanning trees independently.

Each switching device on these access rings can be configured with multiple MSTP processes. After ports of each switching device are bound to different MSTP processes, they participate in the MSTP calculations of different MSTP processes. MSTP calculations in different MSTP processes are independent of each other.

Follow-up Procedure

After an MSTP process is created, run the **stp binding process** command to bind relevant interfaces to the MSTP process.

Precautions

After a switching device that runs MSTP starts correctly, MSTP process 0 exists by default. MSTP configurations in the system view and interface view both belong to this process.

VBST does not support processes. Therefore, this command does not take effect when the spanning tree protocol is VBST. If this command has been run in MSTP mode, switching the MSTP mode to VBST mode fails, and the system displays a message indicating switching failure.

Example

Create MSTP process 1.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
```

5.12.51 stp pvid-consistency protection mode

Function

The **stp pvid-consistency protection mode** command configures a protection mode for PVID inconsistency between directly connected ports in VLAN-based Spanning Tree (VBST).

The **undo stp pvid-consistency protection mode** command deletes the protection mode for PVID inconsistency between directly connected ports in VBST.

By default, no protection mode is configured for PVID inconsistency between directly connected ports. That is, the switch only prints log information when the PVIDs of directly connected ports are different.

Format

stp pvid-consistency protection mode block

undo stp pvid-consistency protection mode

Parameters

Parameter	Description	Value
block	Specifies the block mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VBST checks whether PVIDs of two directly connected ports are the same. If they are different, the processing method varies as follows:

- If the protection mode is **block**, VBST will block the PVIDs.
- If no protection mode is configured, VBST will print log information but not block the PVIDs.

Precautions

When the PVID of the interface is inconsistent and the PVID needs to be blocked, the **stp pvid-consistency protection mode** command must be configured on the two directly connected ports and their link types must be both trunk.

Example

Set the protection mode for PVID inconsistency between directly connected ports to **block**.

```
<HUAWEI> system-view
[HUAWEI] stp pvid-consistency protection mode block
```

5.12.52 stp region-configuration

Function

The **stp region-configuration** command displays the MST region view.

The **undo stp region-configuration** command restores the default configuration of the MST region.

The default parameters of the MST regions are as follows:

- MST region name: MAC address of the switching device.
- MSTP revision level 0.
- VLAN mapping table: all VLANs are mapped to CIST.

Format

stp region-configuration

undo stp region-configuration

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees and these spanning trees are independent of each other. Each spanning tree is called a multiple spanning tree instance (MSTI) and each region is called a multiple spanning tree (MST) region.

Two switching devices belong to the same MST region if they have the following parameters the same:

- MST region name
- Mappings between VLANs and MSTIs

- Revision level of the MST region

If the preceding parameters need to be set for the current switching device or the current process, run the **stp region-configuration** command to enter the MST region view first.

Follow-up Procedure

After the **stp region-configuration** command is run to enter the MST region view, run the following commands:

- Run the **region-name** command to set the MST region name.
- Run the **instance** or the **vlan-mapping modulo** command to set the mappings between VLANs and MSTIs.
- Run the **revision-level** name command to set the revision level of the MST region.

After entering the MST region view and setting the preceding parameters, run the **active region-configuration** command to activate the configurations of the MST region.

Precautions

Modifying the configuration in the MST region view will cause STP recalculation.

Example

Enter the MST region view.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region]
```

5.12.53 stp revertive slow

Function

The **stp revertive slow** command enables the delay in revertive switching during VBST calculation on a port.

The **undo stp revertive slow** command disables the delay in revertive switching during VBST calculation on a port.

By default, the delay in revertive switching disabled during VBST calculation on a port.

Format

stp revertive slow

undo stp revertive slow

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VBST-enabled switch interworks with a PVST-enabled third-party device that does not support P/A negotiation, negotiation is asynchronous. As a result, the network convergence time is long. If the remote device is the root bridge and the VBST-enabled switch provides the alternate port in addition to the interconnected port, you can enable the delay in revertive switching on the interconnected interface. The delay is calculated as follows: 2 * Forward Delay + 8s After the delay function is enabled, the remote interface first completes spanning tree calculation when the port status changes. Then the local interface performs spanning tree status switching. During status switching, services are not interrupted.

Precautions

After the delay in revertive switching is enabled on a port, this function takes effect for all VLANs that the interface join. If there is no alternate port in the VLAN where the interconnected port belongs, the port needs to wait for the delay for recovery. Exercise caution when you run this command in this situation.

Example

```
<HUAWEI> system-view
[HUAWEI] stp mode vbst
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp revertive slow
```

5.12.54 stp root

Function

The **stp root** command configures the switch as a root bridge or secondary root bridge of a spanning tree.

The **undo stp root** command cancels the configuration.

By default, the switch does not function as the root bridge or secondary root bridge of a spanning tree.

Format

STP/RSTP/MSTP: **stp** [**instance** *instance-id*] **root** { **primary** | **secondary** }

STP/RSTP/MSTP: **undo stp** [**instance** *instance-id*] **root**

VBST: **stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **root** { **primary** | **secondary** }

VBST: **undo stp** [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **root**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of a spanning tree instance. If the parameter **instance** *instance-id* is not specified, the configuration takes effect on a CIST instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Each process supports a maximum of 65 instances.
primary	Indicates that the switch functions as the root bridge of a spanning tree.	-
secondary	Indicates that the switch functions as the secondary root bridge of a spanning tree.	-
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the VLAN to which the switch used as the root bridge or secondary root bridge belongs. ● *vlan-id1* specifies the first VLAN to which the switch used as the root bridge or secondary root bridge belongs. ● **to** *vlan-id2* specifies the last VLAN to which the switch used as the root bridge or secondary root bridge belongs. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* determine a VLAN range. ● If **to** *vlan-id2* is not specified, the VLAN specified by *vlan-id1* is used. In the **stp root secondary** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp root** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a spanning tree protocol network, each spanning tree has only one root bridge, which is responsible for sending BPDUs. Owning to the importance of the root bridge, the switch with high performance and network hierarchy is generally chosen as a root bridge. The priority of such a device, however, may be not that high. Therefore, setting a high priority for the switch is necessary so that the switch can function as a root bridge.

To ensure nonstop traffic transmission, run the **stp root** command to configure the switch as the secondary root bridge. When the root bridge is faulty or is powered off, the secondary root bridge becomes the root bridge during spanning tree calculation.

NOTE

After the **stp root primary** command is run to set the switch to be the primary root bridge, the priority value of the switch is 0 in the spanning tree and the priority cannot be modified.

The secondary root bridge specified using the **stp root secondary** command has the priority value of 4096 and the priority cannot be modified.

Precautions

A spanning tree has only one root bridge.

A switch in a spanning tree cannot function both as the primary root bridge and as the secondary root bridge.

If multiple secondary root bridges are set in a spanning tree, the one with the smallest MAC address functions as the secondary root bridge of the spanning tree.

When the device connects to a non-Huawei device, you are advised to run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **priority** *priority* command to set the device priority to ensure that the root bridge is selected correctly.

When multiple MSTIs are configured, the root bridges in MSTI 0 and all other MSTIs must be specified. When the root bridge of MSTI 0 is not configured and is preempted by another device, the MSTP status of all MSTIs other than MSTI 0 will be re-converged, causing MSTP flapping.

Example

Configure the switch as the root bridge of spanning tree instance 1 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 1 root primary
```

Configure the switch as the root bridge in VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 root primary
```

Configure the switch as the secondary root bridge of spanning tree instance 4 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 4 root secondary
```

Configure the switch as the secondary root bridge in VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 root secondary
```

5.12.55 stp root-protection

Function

The **stp root-protection** command enables root protection at the current port.

The **undo stp root-protection** command restores the default setting of root protection.

By default, root protection is disabled at all ports.

Format

stp root-protection

undo stp root-protection

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Owning to incorrect configurations or malicious attacks on the network, a root bridge may receive BPDUs with a higher priority. Consequently, the root bridge is no longer able to serve as the root bridge, and the network topology is changed, triggering a spanning tree recalculation. This spanning tree recalculation may transfer traffic from high-speed links to low-speed links, causing traffic congestion.

If a designated port is enabled with the root protection function, the port role cannot be changed. Once a designated port that is enabled with root protection receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority before a period (generally two Forward Delay periods) expires, the port automatically enters the Forwarding state.

NOTE

You can run the **stp timer forward-delay** command to set the Forward Delay period.

Precautions

The root protection function takes effect only on a designated port. In addition, configuring the root protection function on a port that functions as the designated port in all instances is recommended. Generally, root protection is configured on the interfaces of the root bridge.

If the **stp root-protection** command is run on other types of ports, the root protection function does not take effect.

Loop protection and root protection cannot be configured on the same interface.

Example

Enable the root protection function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp root-protection
```

5.12.56 stp tc-notify process 0

Function

The **stp tc-notify process 0** command enables the current MSTP process to notify the specified STP instances in MSTP process 0 of receiving a TC message.

The **undo stp tc-notify process 0** command forbids the current MSTP process from notifying the specified STP instances in MSTP process 0 of receiving a TC message.

By default, the current MSTP process is disabled from notifying the STP instances in MSTP process 0 of receiving a TC message.

Format

stp tc-notify process 0

undo stp tc-notify process 0

Parameters

None

Views

MSTP process view

Default Level

2: Configuration level

Usage Guidelines

After the **stp tc-notify process 0** command is run, the current MSTP process, after receiving a TC message, notifies the MSTIs in MSTP process 0 to update MAC entries and ARP entries. This prevents user services from being interrupted.

Example

Configure MSTP process 1 to notify MSTP process 0 of receiving a TC message.

```
<HUAWEI> system-view
[HUAWEI] stp process 1
[HUAWEI-mst-process-1] stp tc-notify process 0
```

5.12.57 stp tc-protection interval

Function

The **stp tc-protection interval** command sets the time for a device to process the maximum number of TC BPDUs.

The **undo stp tc-protection interval** command restores the default value.

By default, the time is the Hello timer length.

NOTE

When STP works in VBST mode, the default time for the device to process the maximum number of TC BPDUs is 10s.

Format

stp tc-protection interval *interval-value*

undo stp tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the time for a device to process the maximum number of TC BPDUs.	The value is an integer ranging from 1 to 600, in seconds.

Views

System view or MST process region view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp tc-protection interval** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a device deletes MAC address entries and ARP entries after receiving TC packets. Frequent entry deletion may cause high CPU usage.

The TC attack defense function is enabled by default. You can configure the time, which the device takes to handle a given number of TC packets and immediately refresh forwarding entries, by running the **stp tc-protection interval** command. Within the time specified by *interval-value*, the device handles a given number of TC packets. Excess TC packets are processed by the device at once after the timer (whose length is the configured time) expires. This mechanism ensures that the device does not frequently delete its MAC entries and ARP entries, and therefore does not have excessive CPU usage.

NOTE

You can specify the maximum number of TC packets that the device processes can handle in the specified time by running the **stp tc-protection threshold** command.

Example

Configure the time that MSTP takes to handle a given number of TC packets and immediately refreshes forwarding entries, to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] stp tc-protection interval 10
```

5.12.58 stp tc-protection threshold

Function

The **stp tc-protection threshold** command sets the number of times that a device handles received TC BPDUs and updates forwarding entries within a unit time.

The **undo stp tc-protection threshold** command restores the default setting.

By default, after a device receives TC BPDUs, the default number of times that the device handles the TC BPDUs and updates forwarding entries is 1 within a unit time.

Format

stp tc-protection threshold *threshold*

undo stp tc-protection threshold

Parameters

Parameter	Description	Value
threshold	Indicates the number of times that a device handles the TC BPDU and updates forwarding entries per unit of time.	The value is an integer ranging from 1 to 255.

Views

System view or MST process region view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp tc-protection threshold** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network where MSTP is run, a switching device that receives TC BPDUs will delete the corresponding MAC entries and ARP entries. Frequent deletion operations will greatly affect the CPU, leading to a high CPU usage.

The TC attack defense function is enabled by default, the number of times that TC BPDUs are processed by the switching device within a unit time is configurable (the default unit time is 2s, and the default number of times is 1). If the number of TC BPDUs that the switching device receives within a unit time exceeds the specified threshold, the switching device handles TC BPDUs only for the specified number of times. Additional TC BPDUs are processed by the switching device as a whole for once after the timer (that is, the specified time period) expires. In this manner, the switching device is prevented from frequently deleting its MAC entries and ARP entries so that the CPU is protected against overburden.

NOTE

The value of the unit time is consistent with the Hello time and can be set using the **stp timer hello** command.

Example

Set the threshold update forwarding entries to 5.

```
<HUAWEI> system-view
[HUAWEI] stp tc-protection threshold 5
```

5.12.59 stp tc-restriction enable

Function

The **stp tc-restriction enable** command enables the TC restriction function.

The **undo stp tc-restriction enable** command disables the TC restriction function.

By default, the TC restriction function is disabled.

Format

stp tc-restriction enable

undo stp tc-restriction enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If link flapping occurs on an STP-enabled Layer 2 network, the flapping port sends BPDUs carrying the TC flag (or TCN flag in STP mode) to instruct other devices on the Layer 2 network to update ARP and MAC entries. In special scenarios, however, the customer does not want a port to update ARP or MAC entries after it receives TC or TCN packets. In this case, you can run the **stp tc-restriction enable** command on the port to enable the TC restriction function. After this function is enabled, the port neither updates its local ARP or MAC entries after receiving TC or TCN packets, nor advertises the TC or TCN information to other devices through other ports.

Precautions

After the command is run, ARP and MAC entries may fail to be updated correctly, causing a long packet loss duration in the case of topology changes. Therefore, exercise caution when you run this command.

Example

Enable the TC restriction function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp tc-restriction enable
```

5.12.60 stp timer forward-delay

Function

The **stp timer forward-delay** command sets the value of the Forward Delay of a switching device.

The **undo stp timer forward-delay** command restores the default value of the Forward Delay.

By default, the value of the Forward Delay of a switching device is 1500 centiseconds (15 seconds).

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer forward-delay** *forward-delay*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer forward-delay**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the Forward Delay value is set. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. - If **to** *vlan-id2* is not specified, the Forward Delay value is configured for only the VLAN specified by *vlan-id1*. In the **stp timer forward-delay** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
forward-delay	Specifies the value of the Forward Delay.	The value ranges from 400 to 3000 centiseconds by a step of 100.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer forward-delay** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

The **stp timer forward-delay** command is used to set the Forward Delay timer.

Precautions

The value of the Forward Delay timer set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the value of the Forward Delay timer of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and MaxAge are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

Set the Forward Delay to 2000 centiseconds (20 seconds) when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp timer forward-delay 2000
```

Set the Forward Delay value to 2000 centiseconds (20 seconds) for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 timer forward-delay 2000
```

5.12.61 stp timer hello

Function

The **stp timer hello** command sets the interval of the switching device to send BPDUs, that is, the value of the Hello Time.

The **undo stp timer hello** command restores the default setting.

By default, the interval of the switch to send BPDUs is 200 centiseconds (2 seconds).

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer hello** *hello-time*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer hello**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the Hello timer value is set. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. - If **to** *vlan-id2* is not specified, the Hello timer value is configured for only the VLAN specified by *vlan-id1*. In the **stp timer hello** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
hello-time	Specifies the interval of the switch to send BPDUs.	The value ranges from 100 to 1000, in centiseconds by a step of 100.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer hello** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device periodically sends BPDUs to other devices in the same spanning tree at the interval of the Hello Time. Sending BPDUs periodically ensures that the spanning tree is stable. The **stp timer hello** command can be used to set the BPDU sending interval, that is, the Hello Time.

If no BPDUs are received by the switching device within the timeout period (timeout period = Hello Time x 3 x Timer Factor), the spanning tree is calculated again.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

The value of the Hello Time set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the value of the Hello Time of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree works properly only if the relationships are correctly established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

Set the Hello Time to 400 centiseconds (4 seconds) when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp timer hello 400
```

Set the Hello time to 400 centiseconds (4 seconds) for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 timer hello 400
```

5.12.62 stp timer max-age

Function

The **stp timer max-age** command sets the Max Age of a switching device, that is, the BPDU aging time on a port of the switching device.

The **undo stp timer max-age** command restores the default setting.

By default, the Max Age of a switching device is 2000 centiseconds (20 seconds).

Format

stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer max-age** *max-age*

undo stp [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>] **timer max-age**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which the Max Age value is set. - *vlan-id1* specifies the start VLAN ID. - **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. - If **to** *vlan-id2* is not specified, the Max Age value is configured only for the VLAN specified by *vlan-id1*. In the **stp timer max-age** command, you can specify a maximum of 10 VLAN ranges. **NOTE** VLANs can be specified only when VBST is running.	The value is an integer that ranges from 1 to 4094.
max-age	Specifies the BPDU aging time on a port of the switch.	The value ranges from 600 to 4000 in centiseconds with a step of 100.

Views

System view or MST process region view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer max-age** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device checks whether the BPDUs received from an upstream switching device time out based on the set Max Age value. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs. Then, the switching device sends the BPDUs with the switching device as the root bridge. This aging mechanism effectively controls the diameter of the spanning tree. After the **stp timer max-age** command is run, the Max Age value is set to control the timeout period of received BPDUs.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

The value of the Max Age set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the MaxAge value of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) ≥ Max Age
- Max Age ≥ 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

Set the Max Age to 1000 centiseconds (10 seconds) when STP/RSTP/MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp timer max-age 1000
```

Set the Max Age value to 1000 centiseconds (10 seconds) for VLAN 10 when VBST is running.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 10 timer max-age 1000
```

5.12.63 stp timer-factor

Function

The **stp timer-factor** command sets the timer factor of the timeout period of a switching device to the Hello Time.

The **undo stp timer-factor** command restores the default setting.

By default, the timer factor is 3.

NOTE

If a switching device does not receive BPDUs from an upstream device within the timeout period (timeout period = Hello Time × 3 × Timer Factor), the spanning tree is calculated again.

Format

stp timer-factor *factor*

undo stp timer-factor

Parameters

Parameter	Description	Value
factor	Specifies the timer factor.	The value ranges from 1 to 10.

Views

System view or MSTP process view

NOTE

VBST does not support processes. When VBST is running, you cannot run the **stp timer-factor** command in the MSTP process view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, if a switching device does not receive BPDUs from an upstream device within the timeout period, it considers that the upstream device becomes faulty, and will recalculate the spanning tree.

Sometimes, however, the failure of the upstream device to send BPDUs within the timeout period is only because it is busy processing services. In this case, the spanning tree cannot be calculated. Therefore, you can set a long timeout period on a stable network to avoid the waste of network resources.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

If the parameter *factor* is set smaller, the timeout period of the switching device to re-calculate the spanning tree is shorter. In this case, there is a higher probability that the switching device incorrectly considers the upstream device as being faulty.

If the parameter *factor* is set larger, the timeout period of the switching device to re-calculate the spanning tree is longer. In this case, there is a higher probability that the traffic becomes interrupted because the upstream device has become faulty.

Example

Set the timer factor of the switching device to 6.

```
<HUAWEI> system-view
[HUAWEI] stp timer-factor 6
```

5.12.64 stp transmit-limit (interface view)

Function

The **stp transmit-limit** command sets the maximum number of BPDUs that the current port can send in a specified period.

The **undo stp transmit-limit** command restores the default maximum BPDUs.

By default, the maximum number of BPDUs that a port sends is 6 per second.

Format

stp transmit-limit *packet-number*

undo stp transmit-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum number of BPDUs that a port can send in a specified period.	The value is an integer that ranges from 1 to 255.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device periodically sends BPDUs to other devices in the same spanning tree with the interval of the Hello Time. Sending BPDUs periodically ensures that the spanning tree is stable. If the number of sent BPDUs is great in a specified period, excessive system and bandwidth resources will be consumed.

To prevent this problem from occurring, run the **stp transmit-limit** command to set the maximum number of BPDUs that can be sent by an interface in a specified period. In this manner, the BPDU sending speed is controlled, preventing excessive use of system and bandwidth resources by MSTP when the network topology flaps.

Precautions

After the **stp transmit-limit** command is configured, the maximum number of BPDUs sent in a specified period by the interface is determined by the set value.

Example

Set the maximum BPDUs that GE0/0/1 can send in a specified period to 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp transmit-limit 5
```

5.12.65 stp transmit-limit (system view)

Function

The **stp transmit-limit** command configures the maximum number of Bridge Protocol Data Units (BPDUs) that each interface of the local device can send per second.

The **undo stp transmit-limit** command restores the maximum number of BPDUs, which can be sent by each interface of the local device per second, to the default value.

By default, each interface can send a maximum of 6 BPDUs per second.

Format

stp transmit-limit *packet-number*

undo stp transmit-limit

Parameters

Parameter	Description	Value
packet-number	Maximum number of BPDUs that each interface of the local device can send per second	The value is an integer ranging from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running the Spanning Tree Protocol (STP), a switch sends BPDUs to other devices in the same spanning tree at the interval of the Hello time, to maintain the spanning tree stability. If a large number of BPDUs are sent every second, system and bandwidth resources will be greatly consumed.

NOTE

You can configure the Hello time by using the **stp timer hello** command. The Hello time is the length of the Hello timer and specifies the interval at which the switch sends BPDUs.

To prevent excessive usage of system and bandwidth resources, you can run the **stp transmit-limit** command to configure the maximum number of BPDUs that each interface of the local device can send per second. This configuration controls the BPDU sending rate and prevents the Multiple Spanning Tree Protocol (MSTP) from consuming too many system and bandwidth resources when topology flapping occurs.

Precautions

After the **stp transmit-limit** command is executed, *packet-number* controls the maximum number of BPDUs that each interface can send per second.

You can also configure the maximum number of BPDUs that a specific interface can send per second by running the **stp transmit-limit (interface view)** command in the view of this interface. The **stp transmit-limit (interface view)** command configuration in the interface view takes precedence over the **stp transmit-limit** command configuration in the system view. That is, if the **stp transmit-limit (interface view)** command is configured in the view of an interface, the **stp transmit-limit** command configuration in the system view does not take effect for this interface.

Example

Configure the maximum number of BPDUs that each interface of the local device can send per second to **5**.

```
<HUAWEI> system-view
[HUAWEI] stp transmit-limit 5
```

5.12.66 stp vlan enable

Function

The **stp vlan enable** command enables VBST in a VLAN on the switch.

The **stp vlan disable** command disables VBST in a VLAN on the switch.

The **undo stp vlan disable** command restores the default VBST status in a VLAN on the switch.

By default, VBST is enabled in a VLAN on the switch.

Format

stp vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **enable**

stp vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **disable**

undo stp vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **disable**

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies one or more VLANs in which VBST is enabled. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id2* and *vlan-id1* specify a VLAN range. ● If **to** *vlan-id2* is not specified, VBST is enabled only for the VLAN specified by *vlan-id1*. In the **stp enable** command, you can specify a maximum of 10 VLAN ranges.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a complex Layer 2 network, to prevent or eliminate loops and allow traffic in different VLANs to be forwarded along spanning trees to implement load balancing, deploy VBST on the switch.

Spanning tree calculation occupies system resources. Therefore, run the **stp vlan disable** command to disable VBST in a VLAN where spanning tree calculation does not need to be performed.

Pre-configuration Tasks

When VBST is enabled on a ring network, VBST immediately starts spanning tree calculation. Parameters such as the switch priority and port priority affect spanning tree calculation, and change of these parameters may cause network flapping. To ensure fast and stable spanning tree calculation, perform basic configurations on the switch and ports before enabling VBST.

- Run the **stp mode vbst** command to set the working mode of the switch.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **priority** *priority* command to set the priority of the switch in the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **port priority** *priority* command to set the priority of the port in the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root primary** command to set the switch as the root bridge of the spanning tree instance.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **root secondary** command to set the switch as the secondary root bridge of the spanning tree.
- Run the **stp vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> **cost***cost* command to set the path cost of the port in the spanning tree instance.
- Run the **instance** *instance-id* **vlan** *vlan-id* command to configure 1:1 mapping between MSTIs and VLANs.

Configurations are needed based on real-world situations.

Precautions

When VBST is enabled globally and in a VLAN, the interface that belongs to the VLAN participates in spanning tree calculation. Whether the interface is in forwarding state depends on the calculation result.

When VBST is disabled in a VLAN, the interface that belongs to the VLAN does not participate in spanning tree calculation and is in forwarding state in the VLAN.

VBST cannot be enabled in the ignored VLAN or control VLAN used by ERPS, RRPP, SEP, or Smart Link.

If VLAN mapping or VLAN stacking is configured on an interface corresponding to the VLAN, VBST negotiation for this VLAN will fail.

Example

Enable VBST in VLAN 5.

```
<HUAWEI> system-view
[HUAWEI] stp vlan 5 enable
```

Disable VBST in VLAN 5.

```
<HUAWEI> system-view
```

```
[HUAWEI] stp vlan 5 disable
```

5.12.67 stp vpls-subinterface enable

Function

The **stp vpls-subinterface enable** command enables a main interface to notify its sub-interface bound to a VSI of the received TC BPDUs.

The **undo stp vpls-subinterface enable** command disables a main interface from notifying its sub-interface bound to a VSI of the received TC BPDUs.

By default, a main interface is disabled from notifying its sub-interface bound to a VSI of the received TC BPDUs.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

stp vpls-subinterface enable

undo stp vpls-subinterface enable

Parameters

None.

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an MSTP-enabled interface has a sub-interface configured with L2VPN, you can run the **stp vpls-subinterface enable** command to enable the main interface to notify its sub-interface bound to a VSI of the received TC BPDUs. After the main interface receives TC BPDUs, the main interface can notify the sub-interface bound to the VSI of updating MAC address entries and ARP entries. This function ensures nonstop services. When the **stp vpls-subinterface enable** command is used and the main interface is in Discarding state, the sub-interface bound to the VSI enters the flowdown state. This prevents loops on a VPLS network when CEs are dual-homed to PEs.

This command does not take effect when VBST is running. If this command has been run in STP/RSTP/MSTP mode, switching the STP/RSTP/MSTP mode to VBST mode fails, and the system displays a message indicating switching failure

Precautions

When the forwarding status of an interface moves to Discarding, its VSI-bound sub-interfaces will move to the Discarding state to prevent loops on the VPLS network on which a CE is dual-homed to two PEs.

The **stp vpls-subinterface enable** and **erps vpls-subinterface enable** commands are mutually exclusive on the same interface.

Example

Enable the 40GE0/0/1 to notify its sub-interface bound to a VSI of the received TC BPDUs.

```
<HUAWEI> system-view
[HUAWEI] interface 40ge 0/0/1
[HUAWEI-40GE0/0/1] stp vpls-subinterface enable
```

5.12.68 vlan-mapping modulo

Function

The **vlan-mapping modulo** command enables VLAN-to-instance mapping assignment based on a default algorithm.

The **undo vlan-mapping modulo** command restores the default mapping.

By default, all VLANs are mapped to CIST, namely, spanning tree instance 0.

Format

vlan-mapping modulo *modulo*

undo vlan-mapping modulo

Parameters

Parameter	Description	Value
modulo	Specifies the value of a module.	The value is an integer ranging from 1 to 64.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **vlan-mapping modulo** command is used to enable VLAN-to-instance mapping assignment based on a default algorithm.

NOTE

In the command, **vlan-mapping modulo** indicates that the formula (VLAN ID-1)%modulo +1 is used. In the formula, (VLAN ID-1)%modulo means the remainder of (VLAN ID-1) divided by the value of modulo. This formula is used to map a VLAN to the corresponding MSTI. The calculation result of the formula is ID of the mapping MSTI. For example, if the modulus is 16, the switch maps VLAN 1 to MSTI 1, VLAN 2 to MSTI 2 VLAN 16 to MSTI 16, VLAN 17 to MSTI 1, and so on.

Precautions

The **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10> command is recommended because VLAN-to-instance mapping assignments cannot meet actual mapping requirements.

VBST does not support regions. Therefore, this command does not take effect when the spanning tree protocol is VBST.

Example

Map all VLANs to spanning tree instances modulo 16.

```
<HUAWEI> system-view
[HUAWEI] stp region-configuration
[HUAWEI-mst-region] vlan-mapping modulo 16
```

5.13 SEP Configuration Commands

5.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.13.2 block port

Function

The **block port** command configures the mode in which an interface is blocked on the device where the primary edge interface resides.

The **undo block port** command restores the default mode in which an interface is blocked on the device where the primary edge interface resides.

By default, the system selects a blocked interface from the interfaces on both ends of the link that is established last or the link that recovers from a fault last.

Format

block port { **sysname** *sysname* **interface** *interface-type interface-number* | **hop** *hop-id* | **optimal** | **middle** }

undo block port

Parameters

Parameter	Description	Value
sysname *sysname*	Specifies the name of the device where the interface to be blocked resides.	The value is a string of 1 to 20 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the interface to be blocked. *interface-type* indicates the type of the interface to be blocked. After SEP is enabled, **sysname** *sysname* and **interface** { *interface-type interface-number* } specify the interface to be blocked. Before configuring the mode in which an interface is blocked, run the **display sep topology verbose** command to view detailed information about the topology of the current ring and obtain information about all the interfaces in the topology. Then, you can specify the device and interface names.	-

Parameter	Description	Value
hop *hop-id*	Specifies the interface with the specified hop count from the primary edge interface as the blocked interface. *hop-id* specifies the hop count. If *hop-id* is set to 1, the primary edge interface is blocked. If *hop-id* is set to 2, the neighboring interface of the primary edge interface is blocked. The hop count increases by steps of 1 in the downstream direction of the primary edge interface.	The value is an integer that ranges from 1 to 128.
optimal	Specifies the interface with the highest priority as the blocked interface. SEP compares interface priorities as follows: 1. A larger value set using the **sep segment priority** command indicates a higher priority. 2. If interfaces have the same priority value, a smaller bridge MAC address indicates a higher priority. 3. If interfaces have the same priority value and the same bridge MAC address, a smaller interface number indicates a higher priority.	-
middle	Specifies the interface in the middle of the SEP segment as the blocked interface.	-

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some interfaces are blocked to prevent loops. Any interface in a SEP segment may be blocked if no interface is specified for blocking. A complete SEP segment contains only one blocked interface.

You can specify the blocked interface according to network requirements or your reference. The specified interface is not blocked immediately. Normally, the blocked interface is one of the two interfaces that complete neighbor negotiations last. The specified interface preempts to be the blocked interface only after the preemption mechanism takes effect.

The SEP segment must have been created before the **block port** command is used.

To make the **block port** command configuration take effect, complete the following tasks before using the **block port** command.

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **control-vlan (SEP segment view)** command to configure the control VLAN of the SEP segment.
- Run the **sep segment (interface view)** command to add the interface to the SEP segment and configure the interface as the primary edge interface.

Example

On the device where the primary edge interface is located, specify the device and interface names to block the specified interface.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port sysname HUAWEI interface gigabitethernet 0/0/1
```

On the device where the primary edge interface is located, specify the interface with the specified hop count from the primary edge interface as the interface to be blocked.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port hop 3
```

On the device where the primary edge interface is located, specify the interface with the highest priority as the interface to be blocked.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port optimal
```

On the device where the primary edge interface is located, specify the interface in the middle of the SEP segment as the interface to be blocked.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] block port middle
```

5.13.3 control-vlan (SEP segment view)

Function

The **control-vlan** command configures the control VLAN of a SEP segment for SEP packet transmission.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in a SEP segment.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the control VLAN in a SEP segment.	The value is an integer that ranges from 1 to 4094.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a SEP segment is created, run the **control-vlan** command to create a control VLAN for the SEP segment.

Compared with a data VLAN, a control VLAN forwards only SEP packets but not service packets in a SEP segment, which improves SEP security.

Precautions

- Devices in the same SEP segment must be configured with the same control VLAN to fast forward SEP packets. Different SEP segments can use the same control VLAN.
- In the absence of neighbors, devices that are not in a SEP segment cannot be added to the control VLAN of the SEP segment. Otherwise, network loops occur.
- The control VLAN must be not created, and is not used by other features. In addition, no interface is added to the control VLAN.
- To check whether the control VLAN is created or view the control VLAN where SEP packets are transmitted, run the **display sep interface** command and specify the **verbose** parameter.
- You must configure the control VLAN of a SEP segment before adding interfaces to the SEP segment.
  - If the SEP segment contains an interface, the control VLAN cannot be deleted. To delete the configured control VLAN, run the **undo sep segment** command in the interface view to remove the interface from the SEP segment, and then run the **undo control-vlan** command.
  - If the SEP segment contains no interface, you can configure the control VLAN multiple times. Only the latest configuration takes effect.
  - After the control VLAN is created, the configuration file automatically displays the command for creating the VLAN.

    Each SEP segment must have a control VLAN. After an interface is added to a SEP segment that has a control VLAN, the interface is automatically added to the control VLAN.

  - If the interface type is trunk, in the configuration file, the **port trunk allow-pass vlan** command is displayed in the view of the interface added to the SEP segment.
  - If the interface type is hybrid, in the configuration file, the **port hybrid tagged vlan** command is displayed in the view of the interface added to the SEP segment.

Example

Configure control VLAN 5 for SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] control-vlan 5
```

5.13.4 deal smart-link-flush

Function

The **deal smart-link-flush** command enables a device in a SEP segment to process SmartLink Flush packets.

The **undo deal smart-link-flush** command disables a device in a SEP segment from processing SmartLink Flush packets.

By default, a device in a SEP segment is disabled from processing SmartLink Flush packets.

Format

deal smart-link-flush

undo deal smart-link-flush

Parameters

None

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a host is connected to a SEP network through a SmartLink group, the host sends SmartLink Flush packets to the connected devices in the SEP segment, if the active/standby switchover of member interfaces in the SmartLink group occurs. In this situation, the **deal smart-link-flush** command must be used to enable the devices in the SEP segment to process SmartLink Flush packets.

Prerequisites

Interfaces have been added to the SEP segment.

Precautions

After the **deal smart-link-flush** command is used, the device that receives a SmartLink Flush packet in the SEP segment floods the forwarding database (FDB) to notify the other devices in the SEP segment of topology changes. The other devices then refresh their MAC address entries to ensure reliable traffic transmission.

The **deal smart-link-flush** command must be run on the device that receives SmartLink Flush packets and the interfaces on the device have been added to the SEP segment.

Example

Enable a device in SEP segment 1 to process SmartLink Flush packets.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] deal smart-link-flush
```

5.13.5 description (SEP segment view)

Function

The **description** command configures the description of the SEP segment.

The **undo description** command restores the default setting.

By default, the description of a SEP segment is null.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a SEP segment	The value is a string of 1 to 255 case-sensitive characters with spaces supported.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running SEP, you can run the **description** command to configure the description of the SEP segment, such as the SEP segment ID. Configuring the description of a SEP segment facilitates the maintenance of the SEP segment.

Precautions

After being configured in the SEP-Segment view, the description command takes effect only on the local device.

Example

Configure the description **It's segment 10** for SEP segment 10.

```
<HUAWEI> system-view
[HUAWEI] sep segment 10
[HUAWEI-sep-segment10] description It's segment 10
```

5.13.6 display sep error packet

Function

The **display sep error packet** command displays the statistics about error packets received by SEP and the contents of recently received packets.

Format

display sep error packet

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device on a Layer 2 network runs SEP is attacked by SEP error packets, the **display sep error packet** command can be used to view recently received MSTP error packets.

Example

Display the statistics about error packets received by SEP and the contents of recently received packets.

```
<HUAWEI> display sep error packet
4 error-packets have been received and the last

one is received at 2012/05/02 12:45:31 UTC+08:00 :



01 80 c2 00 00 02 00 e0 fc 8e 0b 34 88 09 01 01
01 14 80 00 00 e0 fc 8e 0b 34 01 21 80 00 09 06
47 00 00 00 02 14 00 00 00 00 00 00 00 00 00 00
00 00 00 00 c7 00 00 00 03 10 ff ff 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
```

5.13.7 display sep interface

Function

The **display sep interface** command displays information about the interfaces in a SEP segment.

Format

display sep interface [*interface-type interface-number* | **segment** *segment-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays SEP information on a specified interface. *interface-type* specifies the type of an interface. *interface-number* specifies the number of an interface.	-
segment *segment-id*	Displays information about the interfaces in a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
verbose	Displays detailed SEP information on a specified interface, including traffic statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the status of an interface or locate an interface fault, use this command to collect statistics and the status of the interface. Then you can locate the interface fault according to the statistics.

When using the **display sep interface** command:

- If no parameter is specified, this command displays information about all the interfaces in SEP segments.
- If only *interface-type interface-number* is specified, this command displays information about a specified interface in SEP segments.
- If only **segment** *segment-id* is specified, this command displays information about all the interfaces in a specified SEP segment.
- If only **verbose** is specified, this command displays detailed information about all the interfaces in SEP segments.
- If *interface-type interface-number* and **verbose** are specified, this command displays detailed information about a specified interface in SEP segments.
- If **segment** *segment-id* and **verbose** are specified, this command displays detailed information about a specified interface in a specified SEP segment.

NOTE

Before running this command, complete the following tasks:

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **sep segment (interface view)** command in the Ethernet interface view to add an interface to a SEP segment and set the role of the interface as required.

Example

Display information about all the interfaces in SEP segments.

```
<HUAWEI> display sep interface
SEP segment 1
----------------------------------------------------------------
Interface        Port Role      Neighbor Status           Port Status
----------------------------------------------------------------
GE0/0/1            *secondary    up                 forwarding
GE0/0/2            common        up                 forwarding
```

Display information about a specified interface in SEP segments.

```
<HUAWEI> display sep interface gigabitethernet 0/0/1
SEP segment 1
----------------------------------------------------------------
Interface          Port Role     Neighbor Status     Port Status
----------------------------------------------------------------
GE0/0/1            common        up                 forwarding
```

Display detailed information about a specified interface in a specified SEP segment.

```
<HUAWEI> display sep interface segment 1 verbose
SEP segment 1
Control-vlan           :3
```

```
Preempt Delay Timer    :15
TC-Notify Propagate to :stp
----------------------------------------------------------------
Interface              :GE0/0/1
Port Role              :Config = *primary / Active =  *secondary
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :NULL
NBR TLV            rx :0                 tx :0
LSP INFO TLV       rx :0                 tx :0
LSP ACK TLV        rx :0                 tx :0
PREEMPT REQ TLV    rx :0                 tx :0
PREEMPT ACK TLV    rx :0                 tx :0
TC Notify          rx :0                 tx :0
EPA                rx :0                 tx :0
Interface              :GE0/0/2
Port Role              :Config = common / Active =  common
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :LSW3 - GE0/0/1 (00e0-ff7c-6400.0000)
NBR TLV            rx :51820             tx :51882
LSP INFO TLV       rx :50380             tx :5776
LSP ACK TLV        rx :5749              tx :50296
PREEMPT REQ TLV    rx :0                 tx :1
PREEMPT ACK TLV    rx :4                 tx :0
TC Notify          rx :22                tx :3
EPA                rx :0                 tx :0
```

Table 5-94 Description of the **display sep interface** command output

Item	Description
SEP segment	ID of a SEP segment. To specify the parameter, run the **sep segment** command.
Interface	Interface name.
Port Role	Role of an interface in a SEP segment: ● common: common interface ● primary: primary edge interface ● secondary: secondary edge interface ● *primary: no-neighbor primary edge interface ● *secondary: no-neighbor secondary edge interface
Neighbor Status	Status of the neighbor state machine: ● up: Neighbor negotiations succeed and the protocol status of the interface is Up. ● down: Neighbor negotiations fail and no neighbor relationship is established between the local interface and its peer interface. ● init: The local interface receives packets from the peer interface and neighbor negotiations start. ● conflict: The local interface receives packets from multiple peer interfaces and the protocol status of the interface is Conflict.

Item	Description
Port Status	Current status of the interface: - discarding: The interface is blocked and can forward SEP packets but not data packets. - forwarding: The interface is in Forwarding state and can forward both data packets and SEP packets.
Port Priority	Interface priority. It is an integer that ranges from 1 to 128. By default, the interface priority is 64. To specify the parameter, run the **sep segment priority** command.
Control-vlan	ID of a control VLAN. A control VLAN is used to forward SEP packets in the local SEP segment. To specify the parameter, run the **control-vlan** command.
Preempt Delay Timer	Delay in preempting the blocked interface after the faulty link recovers, in seconds. To specify the parameter, run the **preempt** command.
TC-Notify Propagate to	Object to be notified of a topology change. To specify the parameter, run the **tc-notify** command.
Neighbor Port	Neighbor interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no neighbor, the value is NULL.
NBR TLV	Neighbor information packet: - rx: indicates the number of received neighbor information packets. - tx: indicates the number of sent neighbor information packets.
LSP INFO TLV	LSA packets: - rx: indicates the number of received LSA packets. - tx: indicates the number of sent LSA packets.
LSP ACK TLV	ACK packets in response to LSA packets: - rx: indicates the number of received ACK packets in response to LSA packets. - tx: indicates the number of sent ACK packets in response to LSA packets.
PREEMPT REQ TLV	Preemption packets: - rx: indicates the number of received preemption packets. - tx: indicates the number of sent preemption packets.
PREEMPT ACK TLV	ACK packets in response to preemption packets: - rx: indicates the number of received ACK packets in response to preemption packets. - tx: indicates the number of sent ACK packets in response to preemption packets.

Item	Description
TC Notify	Packets reporting topology changes: ● rx: indicates the number of received packets reporting topology changes. ● tx: indicates the number of sent packets reporting topology changes.
EPA	Packets reporting edge port selection: ● rx: indicates the number of received packets reporting edge port selection. ● tx: indicates the number of sent packets reporting edge port selection.

5.13.8 display sep segment

Function

The **display sep segment** command displays the configurations of SEP segments.

Format

display sep segment {*segment-id* | **all** }

Parameters

Parameter	Description	Value
segment-id	Displays the configuration of a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
all	Displays the configurations of all SEP segments.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After SEP is configured, you can run the **display sep segment** command to view the configuration of a specified SEP segment or all SEP segments on the network.

Example

Display the configuration of SEP segment 2.

```
<HUAWEI> display sep segment 2
-----------------------------------------------------------------
SEP Segment ID         :2
SEP Control-vlan       :3
Protected-instance     :0 to 5 9 12 to 13 16 to 17 20 to 21
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected    :Eth-Trunk2
Name of Port Member    :Eth-Trunk3
TC-Notify Propagate to :segment 6
```

Display the configurations of all SEP segments.

```
<HUAWEI> display sep segment all
-----------------------------------------------------------------
SEP Segment ID         :1
SEP Control-vlan       :10
Protected-instance     :0 to 48
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected    :Eth-Trunk2
Name of Port Member    :GE0/0/1
TC-Notify Propagate to :segment 6
-----------------------------------------------------------------
SEP Segment ID         :2
SEP Control-vlan       :3
Protected-instance     :0 to 5 9 12 to 13 16 to 17 20 to 21
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected    :Eth-Trunk2
Name of Port Member    :Eth-Trunk3
TC-Notify Propagate to :segment 6
-----------------------------------------------------------------
Total number of segment configured = 2
```

Table 5-95 Description of the **display sep segment** command output

Item	Description
SEP Segment ID	ID of a SEP segment. To specify the parameter, run the **sep segment** command.
SEP Control-vlan	Control VLAN for transmitting SEP packets. To specify the parameter, run the **control-vlan** command.
Protected-instance	ID of a protected instance. To specify the parameter, run the **protected-instance** command.
Preempt Delay Timer(s)	Delay in preemption. ● Configured: configured value of the Preempt Delay Timer (s). ● Remaining: remaining value of the Preempt Delay Timer (s). If the timer does not start, 0 is displayed. If preemption is not configured for a SEP segment, one of the two interfaces that complete neighbor negotiation last remains to be blocked even though a network fault is rectified. Consequently, the interface specified to be blocked is not blocked. To specify the parameter, run the **preempt** command.
Block Port Expected	Specified blocked interface. To specify the parameter, run the **block port** command.

Item	Description
Name of Port Member	Name of a member interface.
TC-Notify Propagate to	Object to which topology changes are reported. To specify the parameter, run the **tc-notify** command.

5.13.9 display sep topology

Function

The **display sep topology** command displays the topologies of SEP segments.

Format

display sep topology [**segment** *segment-id*] [**verbose**]

Parameters

Parameter	Description	Value
segment *segment-id*	Displays the topology of a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
verbose	Displays detailed information about the topology of a SEP segment.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After SEP is configured, you can run the **display sep topology** command to view the topologies of SEP segments, including device names, names of the interfaces added to SEP segments, and roles of the interfaces in a SEP segment.

When running the **display sep topology** command:

- If no parameter is specified, this command displays brief information about the topologies of all the SEP segments on the device.
- If only **segment** *segment-id* is specified, this command displays brief information about the topology of a specified SEP segment.

- If only **verbose** is specified, this command displays detailed information about the topologies of all SEP segments on the device.
- If **segment** *segment-id* and **verbose** are specified, this command displays detailed information about the topology of a specified SEP segment on the device.

NOTE

Before running this command, complete the following tasks:

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **sep segment (interface view)** command in the Ethernet interface view to add an interface to the SEP segment and set the role of the interface as required.

  Edge interfaces must be configured in the SEP segment; otherwise, the SEP topology is incomplete and the system displays an error message.

Example

Display the topologies of all SEP segments on the device.

```
<LSW1> display sep topology
SEP segment 1
SEP detects a segment failure that may be caused by an incomplete topology
-----------------------------------------------------------------------
System Name      Port Name          Port Role       Port Status     Hop
-----------------------------------------------------------------------
LSW1            GE0/0/1           *secondary      forwarding      1
LSW1            GE0/0/2           common          forwarding      2
LSW3            GE0/0/1           common          forwarding      3
LSW3            GE0/0/2           common          forwarding      4
LSW2            GE0/0/1           common          forwarding      5
LSW2            GE0/0/2           *secondary      discarding      6
```

Display detailed topology information in SEP segment 1.

```
<LSW1> display sep topology segment 1 verbose
SEP segment 1
---------------------------------------------------------------
System Name     :LSW1
Port Name       :GE0/0/1
Port Role       :Config = primary / Active =  primary
PortID          :00e0-9e62-6100.0000
Port Priority   :64
Port Status     :forwarding
Link Status     :up
Neighbor Status :up
Age Time        :60(s)
Sequence Number :0x8000000e
Neighbor Port   :LSW2 - GE0/0/2 (00e0-8830-fe00.0000)
Brother Port    :LSW1 - GE0/0/3 (00e0-9e62-6100.0001)
```

Table 5-96 Description of the **display sep topology** command output

Item	Description
SEP segment	ID of a SEP segment. To specify the parameter, run the **sep segment** command.
System Name	Device name.
Port Name	Name of an interface added to the SEP segment.

Item	Description
Port Role	Role of an interface in the SEP segment: ● common: common interface ● primary: primary edge interface ● secondary: secondary edge interface ● *primary: no-neighbor primary edge interface ● *secondary: no-neighbor secondary edge interface Config: indicates the configured role of an interface in a SEP segment. Active: indicates the running role of an interface in a SEP segment. **NOTE** In normal situations, a SEP segment has a primary edge interface, a secondary edge interface, and common interfaces.
Port Status	Current status of an interface: ● discarding: The interface is blocked and can forward SEP packets but not data packets. ● forwarding: The interface is in Forwarding state and can forward both data packets and SEP packets.
PortID	Interface ID. It is in the format of 6-byte system MAC address +2-byte interface number.
Port Priority	Interface priority. It is an integer that ranges from 1 to 128. By default, the interface priority is 64. To specify the parameter, run the **sep segment priority** command.
Link Status	Link status: ● up: The link is Up. ● down: The link is Down.
Neighbor Status	Status of the neighbor state machine: ● up: Neighbor negotiations succeed and the protocol status of the interface is Up. ● down: Neighbor negotiations fail and no neighbor relationship is established between the local interface and its peer interface. ● init: The local interface receives packets from the peer interface and neighbor negotiations start. ● conflict: The local interface receives packets from multiple peer interfaces and the protocol status of the interface is Conflict.
Age Time	Aging time of the LSA.
Sequence Number	Sequence number of the LSA.

Item	Description
Neighbor Port	Neighbor interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no neighbor, the value is NULL.
Brother Port	Brother interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no brother, the value is NULL.

5.13.10 preempt (SEP segment view)

Function

The **preempt** command configures the blocked interface preemption mode on the device where the primary edge interface is located.

The **undo preempt delay** command cancels the configuration of delayed preemption on the primary edge interface.

By default, the SEP preemption mode is not configured.

Format

preempt { **manual** | **delay** *seconds* }

undo preempt delay

Parameters

Parameter	Description	Value
manual	Indicates the manual preemption mode.	-
delay	Indicates the delayed preemption mode.	-
seconds	Specifies the preemption delay. You can configure a preemption delay to prevent network flapping. When link faults are rectified, the specified interface waits until the delay timer expires, and then preempts to be the blocked interface.	The value is an integer that ranges from 15 to 600, in seconds.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some ports are blocked to prevent loops.

When a link in the SEP segment fails, the blocked interface in Up state changes to the Forwarding state after receiving a fault notification packet. If the preemption mode is not configured, when all link faults are rectified or the last two interfaces enabled with SEP complete neighbor negotiations, interfaces send blocking status packets to each other. The interface with the highest priority is then blocked, and the other interfaces enter the Forwarding state.

NOTE

The blocked interface is determined by the administrative priority and user-defined priority of each interface. The priority value of an interface contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user. The value of the lower 8 bits ranges from 1 to 128, and the default value is 64. The interface with the highest priority is blocked.

If the preemption mode is configured on the device where the primary edge interface is located, the specified interface transitions to the Blocking state and sends blocking status packets to other ports.

SEP supports the following preemption modes:

- Delayed preemption

  After all interface faults are rectified, the faulty interface does not send any fault notification packet. If the primary edge interface does not receive any fault notification packet within 3 seconds, it starts the delay timer. When the delay timer expires, the devices in the SEP segment initiate blocked interface preemption.

  NOTE

  You must set the preemption delay when delayed preemption is used because there is no default delay time.

  After delay preemption is configured, you can run the **undo preempt delay** command in the SEP segment view to delete the configuration of delay preemption.

- Manual preemption

  In this mode, if the link status databases of the primary and secondary edge interfaces are complete, the primary edge interface sends preemption packets to block the specified interface. Then the specified interface sends blocking status packets to request the original blocked interface to transition to the Forwarding state.

  NOTE

  - Manual preemption is a one-off operation and will not take effect again after the preemption is complete on the SEP segment. To change the blocked interface, run the **preempt** command and specify the **delay** parameter to configure delayed preemption.
  - Manual preemption causes a short link disconnection in the SEP segment.

Blocked interface preemption is triggered when the following conditions are met:

- The primary edge interface in the SEP segment is selected.

To configure interface roles, run the **sep segment** *segment-id* [**edge** [**no-neighbour**] { **primary** | **secondary** }] command in the interface view.

- The method of selecting the interface to block is configured on the device where the primary edge interface is located.

  To configure the method of selecting the interface to block, run the **block port** { **sysname** *sysname* **interface** *interface-type interface-number* | **hop** *hop-id* | **optimal** | **middle** } command in the SEP segment view.
- The topology of the SEP segment must be complete.

Example

Configure the manual preemption mode on the device where the primary edge port is located.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] preempt manual
```

Configure the delayed preemption mode on the device where the primary edge port is located.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] preempt delay 100
```

5.13.11 protected-instance

Function

The **protected-instance** command configures protected instances in a SEP segment.

The **undo protected-instance** command deletes the protected instances in a SEP segment.

By default, no protected instance is configured in a SEP segment.

Format

protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> }

undo protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
all	Indicates all protected instances in a SEP segment.	-

Parameter	Description	Value
instance-id1 [**to** *instance-id2*]	Specifies the IDs of protected instances in a SEP segment. The keyword **to** connecting two instance IDs, indicating an ID range from *instance-id1* to *instance-id2*. The value of *instance-id2* must be greater than the value of *instance-id1*. **&<1-10>** indicates that the parameter before the sign (&) can be repeated 1 to 10 times.	The value is an integer in the range 0 to 4094. Each device supports a maximum of 65 instances.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In common SEP networking, a physical ring can be configured with only one SEP segment in which only one interface can be blocked. If an interface in a complete SEP segment is blocked, all service data is transmitted only along the path where the primary edge interface is located. The path where the secondary edge interface is located remains idle, wasting bandwidth.

SEP multi-instance is used to improve bandwidth efficiency, allowing each physical interface on a ring network to be added to two SEP segments. A physical ring can be configured with two logical rings, allowing packets carrying different VLAN IDs to pass through. Load balancing is then implemented between the two logical rings. This implementation requires logical rings to be configured with different protected instances and mappings between protected instances and VLANs to be configured. The **protected-instance** command can be used to configure protected instances for a SEP segment.

Prerequisites

The protected instance IDs configured for SEP segments do not overlap. If different SEP segments have duplicate protected instance IDs, replan protected instance IDs.

Follow-up Procedure

Complete the following tasks to configure mappings between protected instances and VLANs:

1. Run the **stp region-configuration** command to enter the MST region view.

2. Run the **instance** *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command to configure mappings between protected instances and VLANs.

   The value of *instance-id* specified in this command must be the same as the value of *instance-id* specified in the **protected-instance** command.
3. Run the **active region-configuration** command to activate the configured mappings between protected instances and VLANs.

Precautions

If you run the **protected-instance** command multiple times in the same SEP segment, multiple instances are configured.

After the **protected-instance** command is run to configure different protected instances for SEP segments and mappings between protected instances and VLANs are set, topology changes affect only corresponding VLANs. This ensures reliable data transmission.

Before adding an interface to a SEP segment, ensure that the SEP segment has been configured with protected instances; otherwise, the interface cannot be added to the SEP segment.

Example

Configure protected instances for SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] protected-instance all
```

5.13.12 reset sep error packet statistics

Function

The **reset sep error packet statistics** command clears the statistics of error sep packets.

Format

reset sep error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

You can use the **reset sep error packet statistics** command to clear the history statistics when you need to observe the statistics of error sep packets in a period from the current time.

Precautions

The **reset sep error packet statistics** command clears the statistics about error sep packets are cleared and cannot be restored. Therefore, confirm the action before you use the command.

Example

Clear the statistics about error sep packets.

```
<HUAWEI> reset sep error packet statistics
```

5.13.13 reset sep interface statistics

Function

The **reset sep interface statistics** command clears SEP packet statistics on a specified interface in a SEP segment.

Format

reset sep interface *interface-type interface-number* **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears SEP packet statistics on a specified interface in a SEP segment. *interface-type* specifies the type of the interface in a SEP segment. *interface-number* specifies the number of the interface in a SEP segment.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Before collecting SEP packet statistics on an interface within a certain period, clear existing traffic statistics on this interface. In such a situation, you can run the **reset sep interface statistics** command.

NOTE

- Before the **reset sep interface statistics** command is run, the SEP segment must be created and the interface must be added to the SEP segment.
- After the **reset sep interface statistics** command is run, SEP packet statistics on the specified interface in the SEP segment are cleared and cannot be restored. Confirm your action before you use this command.

Example

Clear SEP packet statistics on GE 0/0/1 in the SEP segment.

```
<HUAWEI> reset sep interface gigabitethernet 0/0/1 statistics
```

5.13.14 sep segment

Function

The **sep segment** command creates a SEP segment and displays the SEP segment view. If the specified SEP segment has been created, you can directly enter the SEP segment view.

The **undo sep segment** command deletes the existing SEP segment.

Format

sep segment *segment-id*

undo sep segment *segment-id*

Parameters

Parameter	Description	Value
segment-id	Specifies the ID of a SEP segment.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On a Layer 2 switching network, packets will be transmitted infinitely once a loop occurs, causing a broadcast storm. The broadcast storm occupies all the bandwidth on the network, causing network congestion or even breakdown of the entire network. To prevent loops on a Layer 2 switching network, Huawei develops the Smart Ethernet Protection (SEP) protocol.

SEP is a ring network protocol specially used for the Ethernet link layer. It blocks redundant links to prevent loops. It can run on a network together with STP, RSTP, MSTP, and RRPP and supports display of the network topology. When the devices of other vendors are used on the network, SEP can also prevent loops, but does not need to be configured on these devices.

A SEP segment consists of interconnected Layer 2 switching devices configured with the same SEP segment ID and control VLAN ID. A SEP segment is the basic unit for SEP.

The switches support a maximum of 48 SEP segments.

NOTE

A maximum of two interfaces on a Layer 2 switching device can be added to the same SEP segment.

Before enabling SEP, run the **sep segment** command to create a SEP segment. Then run the **control-vlan (SEP segment view)** command in the SEP segment view to configure a control VLAN.

A SEP segment can be deleted only when it does not contain any interface. If the SEP segment contains interfaces, run the **undo sep segment** *segment-id* command in the corresponding interface views to delete the interfaces from the SEP segment one by one.

Example

Create SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1]
```

5.13.15 sep segment (interface view)

Function

The **sep segment** command adds an Ethernet interface to a specified SEP segment and configures the role of the Ethernet interface.

The **undo sep segment** command removes an Ethernet interface from a specified SEP segment and deletes the interface role configuration.

By default, an Ethernet interface is not added to a specified SEP segment and is not configured with a role.

Format

sep segment *segment-id* [**edge** [**no-neighbor**] { **primary** | **secondary** }]

undo sep segment *segment-id*

Parameters

Parameter	Description	Value
segment-id	Specifies the ID of the SEP segment to which an Ethernet interface is added.	The value is an integer that ranges from 1 to 1024.
edge	Specifies the Ethernet interface added to the SEP segment as an edge interface.	-
no-neighbor	Specifies the Ethernet interface as a no-neighbor edge interface.	-
primary	Specifies the Ethernet interface as a primary edge interface.	-
secondary	Specifies the Ethernet interface as a secondary edge interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 interface can forward SEP packets only after being added to a SEP segment. Each Layer 2 switching device in a SEP segment is a node. Each node can have at most two Layer 2 interfaces added to the same SEP segment.

When using the **sep segment** command:

- If no parameter is specified, this command adds an Ethernet interface to a specified SEP segment and configures the interface as a common interface.

  In a SEP segment, all interfaces except edge interfaces and blocked interfaces are common interfaces.

  A common interface monitors the status of the directly-connected SEP link. When the link status changes, the interface sends a topology change notification message to notify its neighbors. Then the topology change notification message is flooded on the link until it finally reaches the primary edge interface. The primary edge interface determines how to process the link change.

- If **edge** and **primary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the primary edge interface.

  A SEP segment has only one primary edge interface, which is determined by the configuration and primary edge interface election. The primary edge interface initiates blocked interface preemption, terminates packets, and sends topology change notification messages to other networks.
- If **edge** and **secondary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the secondary edge interface.

  A SEP segment has only one secondary edge interface, which is determined by the configuration and secondary edge interface election. The secondary edge interface terminates packets and sends topology change notification messages to other networks.
- If **edge**, **no-neighbor**, and **primary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the no-neighbor primary edge interface.

  An interface at the edge of a SEP segment is a no-neighbor edge interface. There are two types of no-neighbor edge interface: no-neighbor primary edge interface and no-neighbor secondary edge interface. You can configure the role of a no-neighbor edge interface. A no-neighbor edge interface terminates packets and sends topology change notification messages to other networks. It is commonly used to interconnect Huawei devices and non-Huawei devices or interconnect Huawei devices and devices that do not support SEP.
- If **edge**, **no-neighbor**, and **secondary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the no-neighbor secondary edge interface.

To view the role of an interface added to a SEP segment, run the **display sep topology** or **display sep interface** command.

Precautions

- You have created a SEP segment and configured a control VLAN and protected instances.
- To add an interface to a SEP segment, configure the interface as a hybrid or trunk interface.
- If **no-neighbor** is not specified, the interface to be added to the SEP segment is not an STP or RRPP interface.
- Two interfaces at the edge of a SEP segment must be configured as edge interfaces. The roles of the interfaces are defined by users.
- All the interfaces on the network are Up so that the SEP segment is complete and the displayed topology information is correct.

Example

Add GE 0/0/1 to SEP segment 1 and configure the interface as the no-neighbor secondary edge interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
```

```
[HUAWEI-GigabitEthernet0/0/1] sep segment 1 edge no-neighbor secondary
```

5.13.16 sep segment priority

Function

The **sep segment priority** command configures the priority of an Ethernet interface in a specified SEP segment.

The **undo sep segment priority** command restores the default priority of an Ethernet interface in a specified SEP segment.

By default, the priority of an Ethernet interface in a specified SEP segment is 64.

Format

sep segment *segment-id* **priority** *priority*

undo sep segment *segment-id* **priority**

Parameters

Parameter	Description	Value
segment-id	Specifies the ID of the SEP segment to which an Ethernet interface is added.	The value is an integer that ranges from 1 to 1024.
priority	Specifies the priority of an Ethernet interface in a specified SEP segment. A larger value indicates a higher priority. When the link fault is rectified, the interface with the highest priority is likely to become the blocked interface.	The value is an integer that ranges from 1 to 128. The default value is 64.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, 25GE interface view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some interfaces are blocked to prevent loops. Any interface in a SEP segment may be blocked if no interface is specified for blocking. A complete SEP segment contains only one blocked interface.

If you run the **block port optimal** command to select the blocked interface according to the port priority, the interface priority set using the **sep segment**

priority command determines whether the interface will be blocked when an interface fault is rectified.

The blocked interface is determined by the administrative priority and user-defined priority of each interface. The priority value of an interface contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user. A higher interface priority indicates a higher probability that the interface is blocked.

SEP compares interface priorities as follows:

1. Compares configured interface priority values. A larger value indicates a higher priority.
2. Compares bridge MAC addresses of interfaces with same priority values. A smaller bridge MAC address indicates a higher priority.
3. Compares interface numbers of interfaces with identical bridge MAC addresses. A smaller interface number indicates a higher priority.

Before using the **sep segment priority** command, ensure that the interface is added to the specified SEP segment using the **sep segment** (interface view) command.

Example

Set the priority of GE 0/0/1 added to SEP segment 1 to 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] sep segment 1
[HUAWEI-GigabitEthernet0/0/1] sep segment 1 priority 10
```

5.13.17 tc-notify

Function

The **tc-notify** command configures a SEP segment to report topology changes to other SEP segments or networks running other ring network protocols.

The **undo tc-notify** command disables a SEP segment from reporting topology changes to other SEP segments or networks running other ring network protocols.

By default, a SEP segment does not send topology change notifications.

Format

tc-notify { **segment** { *segment-id1* [**to** *segment-id2*] } &<1-10> | **stp** | **rrpp** | **smart-link send-packet vlan** *vlan-id* | **vpls** }

undo tc-notify { **segment** { *segment-id1* [**to** *segment-id2*] } &<1-10> | **stp** | **rrpp** | **smart-link send-packet vlan** | **vpls** }

NOTE

Only S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H support **vpls** parameter.

Parameters

Parameter	Description	Value
segment *segment-id1* [**to** *segment-id2*]	Specifies the SEP segments to which topology changes of the local SEP segment need to be reported. Topology changes of the local SEP segment are reported to other SEP segments, but not the local SEP segment. The keyword **to** connecting two instance IDs, indicating an ID range from *instance-id1* to *instance-id2*. The value of *instance-id2* must be greater than the value of *instance-id1*.	The value is an integer that ranges from 1 to 1024.
stp	Indicates that the local SEP segment reports topology changes to STP networks.	-
rrpp	Indicates that the local SEP segment reports topology changes to RRPP networks.	-
smart-link	Indicates that the local SEP segment reports topology changes to an upper-layer network using SmartLink Flush packets. When the local SEP segment is connected to an upper-layer network through a no-neighbor edge interface, this parameter must be specified in the **tc-notify** command.	-
send-packet vlan *vlan-id*	Specifies the ID of a VLAN used to transmit SmartLink Flush packets.	The value is an integer that ranges from 1 to 4094.
vpls	Indicates that the local SEP segment reports topology changes to VPLS networks.	-

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If topology changes in a SEP segment are not reported to the upper-layer Layer 2 network in time, devices on the upper-layer network retain the original MAC address entries, causing traffic interruption. To ensure uninterrupted traffic transmission, run the **tc-notify** command to configure the local SEP segment to report topology changes to other SEP segments or networks running other ring network protocols.

Prerequisites

The **sep segment** command has been used to create SEP segments.

Precautions

When the topology of a SEP segment changes, the SEP segment sends topology change notification messages to other SEP segments or networks running other ring network protocols. If the specified segment or network does not exist, the **tc-notify** command configuration does not take effect.

After receiving topology change notification messages from a SEP segment, devices on the upper layer network send Flush FDB packets on the network. Then, all the devices on the upper-layer network delete the original MAC addresses and learn new MAC addresses to ensure normal traffic transmission.

The **tc-notify** command is used on the device connecting a lower-layer network and an upper-layer network.

Example

Configure SEP segment 1 to report topology changes to SEP segments 10 to 20.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify segment 10 to 20
```

Configure SEP segment 1 to report topology changes to STP networks.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify stp
```

Configure SEP segment 1 to report topology changes to RRPP networks.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify rrpp
```

Configure SEP segment 1 to report topology changes to upper-layer networks using SmartLink Flush packets.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify smart-link send-packet vlan 3
```

Configure SEP segment 1 to report topology changes to VPLS networks.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-notify vpls
```

5.13.18 tc-protection interval

Function

The **tc-protection interval** command sets the interval for suppressing topology change (TC) notification packets.

The **undo tc-protection interval** command restores the default interval for suppressing TC notification packets.

By default, the interval for suppressing TC notification packets is 2s.

Format

tc-protection interval *interval-value*

undo tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for suppressing TC notification packets. A longer interval ensures stable SEP operating but deteriorates convergence performance.	The value is an integer that ranges from 1 to 10, in seconds.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that a host is connected to an upstream network through three or more SEP networks. If the topology of the SEP network nearest to the host changes, doubled TC notification packets are flooded on the upper-layer SEP network. Each time TC notification packets pass through a SEP segment, TC notification packets will be doubled. The upstream network will receive multiple duplicate TC notification packets.

Frequent topology change notifications reduce the CPU packet processing capability, and cause devices in the SEP segments to frequently refresh MAC address entries, which consumes bandwidth resources. To address the problem, run the **tc-protection interval** command to suppress TC notification packets.

Prerequisites

The **sep segment** command has been used to create SEP segments.

Precautions

After this command is used, the upstream network only needs to process one TC notification packet but not multiple duplicate TC notification packets. In addition, this function protects devices on the SEP segment against TC attacks.

Example

Set the interval for suppressing TC notification packets to 3s in SEP segment 1.

```
<HUAWEI> system-view
[HUAWEI] sep segment 1
[HUAWEI-sep-segment1] tc-protection interval 3
```

5.14 RRPP Configuration Commands

5.14.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support RRPP.

Only the S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support RRPP Snooping.

5.14.2 control-vlan

Function

The **control-vlan** command configures the control VLAN in an RRPP domain.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in an RRPP domain.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the control VLAN ID in an RRPP domain. The VLAN must be a VLAN that has not been created.	The value is an integer that ranges from 1 to 4093. **NOTE** VLAN 1 is the default VLAN and cannot be configured as the control VLAN.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VLAN that transmits RRPP packets in an RRPP domain is called a control VLAN.

An RRPP domain is configured with two control VLANs, that is, the major control VLAN and sub-control VLAN. You need to specify only the major control VLAN. The VLAN whose ID is one greater than the ID of the major control VLAN becomes the sub-control VLAN.

Precautions

- The control VLAN must be included in the protected VLANs; otherwise, the RRPP ring cannot be configured.
- The control VLAN specified by *vlan-id* must be a VLAN that has not been created, and not been used by other features. The sub-control VLAN specified by *vlan-id* plus one must be a VLAN that has not been created, and not been used by other features.
- The control VLAN is deleted when the RRPP domain is deleted using the **undo rrpp domain** command.

Example

Set the control VLAN ID in RRPP Domain 1 to 100.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
```

5.14.3 description (RRPP domain view)

Function

The **description** command configures the description of the RRPP domain.

The **undo description** command restores the default setting.

By default, the description of an RRPP domain is null.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an RRPP domain.	The value is a string of 1 to 255 case-sensitive characters.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running RRPP, you can run the **description** command to configure the description of the RRPP domain, such as the RRPP domain ID. Configuring the description of an RRPP domain facilitates the maintenance of the RRPP domain.

Precautions

After being configured in the RRPP domain view, the description command takes effect only on the local device.

Example

Configure the description **It's RRPP Domain 10** for RRPP domain 10.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 10
[HUAWEI-rrpp-domain-region10] description It's RRPP Domain 10
```

5.14.4 display rrpp brief

Function

The **display rrpp brief** command displays summary information about all RRPP domains configured on the device.

Format

display rrpp brief [**domain** *domain-id*]

Parameters

Parameter	Description	Value
domain *domain-id*	Displays summary information about a specified RRPP domain. If this parameter is not specified, the command displays summary information about all RRPP domains.	The value is an integer that ranges from 1 to 64.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rrpp brief** command on the RRPP-enabled device to view summary information about RRPP domains configured on the device. The command output shows whether RRPP is enabled, the configuration of RRPP domains, and information about the configured rings in the RRPP domains.

Example

Display summary information about RRPP.

```
<HUAWEI> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status: Disable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec (0 sec default)
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 30    sub 31
Protected VLAN : Reference Instance 10
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

 Ring   Ring    Node     Primary/Common            Secondary/Edge       Is
 ID     Level   Mode     Port                      Port                 Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/2      GigabitEthernet0/0/3 No
```

Display summary information about RRPP Domain 1.

```
<HUAWEI> display rrpp brief domain 1
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge
```

```
RRPP Protocol Status: Disable
RRPP Working Mode: HW
RRPP Linkup Delay Timer: 1 sec (0 sec default)
Number of RRPP Domains: 1

Domain Index   : 1
Control VLAN   : major 30    sub 31
Protected VLAN : Reference Instance 10
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)

 Ring   Ring    Node     Primary/Common           Secondary/Edge       Is
 ID     Level   Mode     Port                     Port                 Enabled
 ------------------------------------------------------------------------------
 1      0       M        GigabitEthernet0/0/2     GigabitEthernet0/0/3     No
```

Table 5-97 Description of the display rrpp brief command output

Item	Description
Abbreviations for Switch Node Mode	Abbreviations of node modes. The value can be: - M-Master: indicates the master node. - T-Transit: indicates the transit node. - E-Edge: indicates the edge node. - A-Assistant-Edge: indicates the assistant edge node.
RRPP Protocol Status	Status of RRPP. - Enable: indicates that RRPP is enabled. - Disable: indicates that RRPP is disabled. To enable RRPP, run the **rrpp enable** command.
Number of RRPP Domains	Number of RRPP domains configured.
Domain Index	ID of the RRPP domain. To specify the parameter, run the **rrpp domain** command.
RRPP Working Mode	RRPP working mode: - GB: indicates RRPP defined by the national standard of China. - HW: indicates RRPP defined by Huawei.
RRPP Linkup Delay Timer	Delay time before the master node becomes Complete. To set the delay time before the master node becomes Complete, run the **rrpp linkup-delay-timer** command.
Control VLAN : major 30 sub 31	Control VLAN IDs of the RRPP domain. **major** indicates the master control VLAN and **sub** indicates the sub-control VLAN. To specify the parameter, run the **control-vlan** command.

Item	Description
Protected VLAN	ID of the instance bound to the protected VLAN in the RRPP domain. To specify the parameter, run the **protected-vlan** command.
Hello Timer	Hello timer in the RRPP domain, in seconds. To set the value of the Hello timer, run the **timer (RRPP domain view)** command.
Fail Timer	Fail timer in the RRPP domain, in seconds. To set the value of the Fail timer, run the **timer (RRPP domain view)** command.
Ring ID	ID of the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Ring Level	Level of the RRPP ring. ● Level 0 indicates the major ring. ● Level 1 indicates the sub-ring. To specify the parameter, run the **ring node-mode** command.
Node Mode	Mode of a node. For modes of a node, see the preceding item **Abbreviations for Switch Node Mode**. To specify the parameter, run the **ring node-mode** command.
Primary/Common Port	Primary interface or common interface on the master node or transit node of an RRPP ring. To specify the parameter, run the **ring node-mode** command.
Secondary/Edge Port	Secondary interface or edge interface on the master node or transit node of an RRPP ring. To specify the parameter, run the **ring node-mode** command.
Is Enabled	Whether a ring is enabled. To enable a ring, run the **ring enable** command.

5.14.5 display rrpp error packet

Function

The **display rrpp error packet** command displays statistics about recently-received RRPP error packets.

Format

display rrpp error packet

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device receives RRPP attack packets on a network, you can run the **display rrpp error packet** command to collect statistics about recently-received RRPP error packets to locate the problem.

Example

Display statistics about recently-received RRPP error packets.

```
<HUAWEI> display rrpp error packet
4 error-packets have been received and the last

one is received at 2010/01/02 12:45:31 UTC+00:00 :


00 0f e2 07 82 17 00 18 82 99 fc 22 81 00 e0 01
00 48 aa aa 03 00 e0 2b 00 bb 99 0b 00 40 01 05

00 01 00 01 00 00 00 18 82 99 fc 22 00 01 00 03

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00.
```

5.14.6 display rrpp ring-group

Function

The **display rrpp ring-group** command displays the configuration about an RRPP ring group.

Format

display rrpp ring-group [*ring-group-id*]

Parameters

Parameter	Description	Value
ring-group *ring-group-id*	Specifies the ID of an RRPP ring group. If this parameter is not specified, configurations about all the RRPP ring groups are displayed.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rrpp ring-group** command on an RRPP-enabled device to view configurations about RRPP ring groups and learn their running status.

Precautions

If the RRPP-enabled device is an edge node, the ring that sends Edge-Hello packets is displayed.

If the RRPP-enabled device is an assistant edge node, the ring that receives Edge-Hello packets is displayed.

Example

Display configurations about all ring groups.

```
<HUAWEI> display rrpp ring-group
 Ring Group 1:
 domain 1 ring 1 to 3, 5
 domain 2 ring 1 to 3, 5
 domain 1 ring 1 send Edge-Hello packet

 Ring Group 2:
 domain 1 ring 4, 6 to 7
 domain 2 ring 4, 6 to 7
```

Check the configuration about Ring Group 2.

```
<HUAWEI> display rrpp ring-group 2
 Ring Group 2:
 domain 1 ring 4, 6 to 7
 domain 2 ring 4, 6 to 7
```

Table 5-98 Description of the display rrpp ring-group command output

Item	Description
Ring Group	ID of the RRPP ring group. To specify the parameter, run the **rrpp ring-group** command.
domain xx ring xx	Sub-rings in the ring group. To specify sub-rings in a ring group, run the **domain** command.
domain xx ring xx send Edge-Hello packet	Sub-ring that sends Edge Hello packets in the RRPP ring group.

5.14.7 display rrpp snooping enable

Function

The **display rrpp snooping enable** command displays information about an interface where RRPP snooping is enabled.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display rrpp snooping enable { **all** | **interface vlanif** *interface-number* }

display rrpp snooping enable { **all** | **interface** *interface-type interface-number* [*.subinterface-number*] }

Parameters

Parameter	Description	Value
all	Displays information about all interfaces where RRPP snooping is enabled.	-
interface vlanif *interface-number*	Displays information about a VLANIF interface where RRPP snooping is enabled. *interface-number* specifies the number of the VLANIF interface.	-

Parameter	Description	Value
interface *interface-type* *interface-number* [.*subinterface-number*]	Displays information about an interface where RRPP snooping is enabled. *interface-type* specifies the type of the interface, *interface-number* specifies the number of the interface, and *subinterface-number* specifies the number of the sub-interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display rrpp snooping enable** command to view information about interfaces where RRPP snooping is enabled.

Example

Display information about all interfaces where RRPP snooping is enabled.

```
<HUAWEI> display rrpp snooping enable all
 Port                         VsiName          Vlan
-------------------------------------------------------
 Vlanif100                       name1            100
 Vlanif200                       name2            200
```

Display information about interfaces where RRPP snooping is enabled.

```
<HUAWEI> display rrpp snooping enable interface vlanif 100
 Port                         VsiName          Vlan
-------------------------------------------------------
 Vlanif100                       name1            100
```

Table 5-99 Description of the display rrpp snooping enable command output

Item	Description
Port	Name of the interface where RRPP snooping is enabled. To specify the parameter, run the **rrpp snooping enable** command.
VsiName	Name of the VSI that is bound to the interface. To specify the parameter, run the **rrpp snooping vsi** command.
Vlan	VLAN that is associated with the interface. It refers to the control VLAN of the RRPP ring.

5.14.8 display rrpp snooping vsi

Function

The **display rrpp snooping vsi** command displays the VSI that is associated with RRPP snooping.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display rrpp snooping vsi { **all** | **interface vlanif** *interface-number* }

display rrpp snooping vsi { **all** | **interface** *interface-type interface-number* [*.subinterface-number*] }

Parameters

Parameter	Description	Value
all	Displays all VSIs that are associated with RRPP snooping.	-
interface vlanif *interface-number*	Displays the VSI associated with RRPP snooping on the specified VLANIF interface. *interface-number* specifies the VLANIF interface number.	-

Parameter	Description	Value
interface *interface-type interface-number* [*.subinterface-number*]	Displays the VSI associated with RRPP snooping on the specified interface. *interface-type* specifies the type of the interface, *interface-number* specifies the number of the interface, *subinterface-number* specifies the number of the sub-interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command on an RRPP snooping-enabled device to view VSIs that are associated with RRPP snooping.

Example

Display VSIs associated with RRPP snooping on all interfaces.

```
<HUAWEI> display rrpp snooping vsi all
 Port                         VsiName
----------------------------------------------
 Vlanif100                      name1
 Vlanif100                      name2
 Vlanif200                      name1
 Vlanif200                      name2
```

Display the VSI associated with RRPP snooping on the specified interface.

```
<HUAWEI> display rrpp snooping vsi interface vlanif 100
 Port                         VsiName
----------------------------------------------
 Vlanif100                      name1
 Vlanif100                      name2
```

Table 5-100 Description of the display rrpp snooping vsi command output

Item	Description
Port	Name of the interface that is bound to a VSI. To specify the parameter, run the **rrpp snooping enable** command.
VsiName	Name of the VSI that is associated with the interface. To specify the parameter, run the **rrpp snooping vsi** command.

5.14.9 display rrpp statistics

Function

The **display rrpp statistics** command displays statistics on RRPP packets.

Format

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id*	Specifies the ID of an RRPP ring. If *ring-id* is not specified, statistics on packets of all the rings in a specified RRPP domain are displayed.	The value is an integer that ranges from 1 to 64.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view statistics on RRPP packets on each interface to locate network faults.

Example

Display the statistics on packets on RRPP Ring 1 in Domain 1.

```
<HUAWEI> display rrpp statistics domain 1 ring 1
RRPP Ring     : 1
Ring Level    : 0
Node Mode     : Master
Is Active     : Yes
Primary port  : GigabitEthernet0/0/1
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB       FDB        HELLO   FAULT    Total
 --------------------------------------------------------------------------------
 Send    386     0       0         0           0        0        386
 Rcv     0       0       0         0           0        0        0
Secondary port: GigabitEthernet0/0/2
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB       FDB        HELLO   FAULT    Total
 --------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
```

Display the statistics on packets on all RRPP rings in Domain 3.

```
<HUAWEI> display rrpp statistics domain 3
RRPP Ring     : 3
Ring Level    : 0
Node Mode     : Transit
Is Active     : Yes
Primary port  : GigabitEthernet0/0/1
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB       FDB        HELLO   FAULT    Total
 --------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
Secondary port: GigabitEthernet0/0/2
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB       FDB        HELLO   FAULT    Total
 --------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
RRPP Ring     : 4
Ring Level    : 1
Node Mode     : Assistant-edge
Is Active     : Yes
Common port   : GigabitEthernet0/0/3
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB       FDB        HELLO   FAULT    Total
 --------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
Edge port     : GigabitEthernet0/0/4
 Packet         LINK    COMMON    COMPLETE    EDGE    MAJOR    Packet
 Direct  HEALTH  DOWN     FDB       FDB        HELLO   FAULT    Total
 --------------------------------------------------------------------------------
 Send    0       0       0         0           0        0        0
 Rcv     0       0       0         0           0        0        0
```

Table 5-101 Description of the display rrpp statistics command output

Item	Description
RRPP Ring	ID of the RRPP ring.

Item	Description
Ring Level	Level of the RRPP ring. ● Level 0 indicates the major ring. ● Level 1 indicates the sub-ring.
Node Mode	Mode of a node on the RRPP ring. ● Master: indicates the master node. ● Transit: indicates the transit node. ● Edge: indicates the edge node. ● Assistant Edge: indicates the assistant edge node that is supported by RRPP defined by Huawei.
Is Active	Whether the RRPP ring is activated. The RRPP ring can be activated only when RRPP and the RRPP ring are enabled. To activate an RRPP ring, run the **rrpp enable** and **ring enable** commands.
Primary port	Primary interface on the RRPP ring.
Secondary port	Secondary interface on the RRPP ring.
Common port	Common interface on the edge node or assistant edge node of the RRPP sub-ring.
Edge port	Edge interface on the edge node or assistant edge node of the RRPP sub-ring.
Packet Direct	Direction of RRPP packets. ● Send: indicates the packets sent from the interface. ● Rcv: indicates the packets received by the interface.
HEALTH	Number of Hello packets sent by the master node to check the loop integrity.
LINK DOWN	Number of LinkDown packets. LinkDown packets are sent by the transit node, edge node, or assistant edge node to notify the master node that the status of the link on the ring becomes Down and the physical ring does not exist. Only statistics on received packets are collected on the master node and statistics on sent packets are collected on other nodes.
COMMON FDB	Number of common FDB packets used to refresh the FDB. Common FDB packets are sent from the master node to request the transit node, edge node, and assistant edge node to update their MAC address forwarding entries and ARP entries. Only statistics on sent packets are collected on the master node and statistics on received packets are collected on other nodes.

Item	Description
COMPLETE FDB	Number of Complete FDB packets used to update the FDB after the ring network recovers. Complete FDB packets are sent from the master node to request the transit node, edge node, and assistant edge node to update their MAC address forwarding entries and ARP entries. These packets are also used to request the transit node to unblock the temporarily blocked interfaces. Only statistics on sent packets are collected on the master node and statistics on received packets are collected on other nodes.
EDGE HELLO	Number of Edge-Hello packets used to check the integrity of the major ring. Edge-Hello packets are sent from the edge node of the sub-ring to the assistant edge node of the same sub-ring. The sub-ring checks the integrity of the major ring in the same domain through the Edge-Hello packets. Only statistics on sent packets are collected on the edge node and statistics on received packets are collected on the assistant edge node.
MAJOR FAULT	Number of Major-Fault packets used to notify faults on the major ring. Major-Fault packets are sent by the assistant edge interface on a sub-ring. If the assistant edge node does not receive the Edge-Hello packet from the edge interface within a specified period, the assistant edge node sends the Major-Fault packet to the edge interface to notify that the packets cannot be transparently transmitted on the major ring. Only statistics on received packets are collected on the edge node and statistics on sent packets are collected on the assistant edge node.
Packet Total	Total number of sent or received packets.

5.14.10 display rrpp verbose

Function

The **display rrpp verbose** command displays detailed configuration about RRPP on the device.

Format

display rrpp verbose [**domain** *domain-id* [**ring** *ring-id*]]

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id*	Specifies the ID of an RRPP ring. If this parameter is not specified, detailed configurations about all the rings in a specified domain is displayed.	The value is an integer that ranges from 1 to 64.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check detailed configuration about RRPP. The command output helps you analyze the link status of the network and locate network faults.

Example

Display detailed configuration about the master node on Ring 1 in RRPP Domain 1.

```
<HUAWEI> display rrpp verbose domain 1 ring 1
Domain Index   : 1
Control VLAN   : major 400    sub 401
Protected VLAN : Reference Instance 30
Hello Timer    : 1 sec(default is 1 sec)  Fail Timer : 6 sec(default is 6 sec)
RRPP Ring      : 1
Ring Level     : 0
Node Mode      : Master
Ring State     : Complete
Is Enabled     : Enable                   Is Active : Yes
Primary port   : GigabitEthernet0/0/1               Port status: UP
Secondary port : GigabitEthernet0/0/2               Port status: BLOCKED
```

Table 5-102 Description of the display rrpp verbose command output

Item	Description
Domain Index	ID of the RRPP domain. To specify the parameter, run the **rrpp domain** command.
Control VLAN : major 400 sub 401	Control VLAN IDs of the RRPP domain. **major** indicates the master control VLAN and **sub** indicates the sub-control VLAN. To specify the parameter, run the **control-vlan** command.
Protected VLAN	Instance mapping the protected VLANs of the RRPP domain. To specify the parameter, run the **protected-vlan** command.
Hello Timer	Value of the Hello timer, in seconds. To set the value of the Hello timer, run the **timer (RRPP domain view)** command.
Fail Timer	Value of the Fail timer, in seconds. To set the value of the Fail timer, run the **timer (RRPP domain view)** command.
RRPP Ring	ID of the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Ring Level	Level of the RRPP ring. ● Level 0 indicates the major ring. ● Level 1 indicates the sub-ring. To specify the parameter, run the **ring node-mode** command.
Node Mode	Role of a node on the RRPP ring. The value can be: ● Master: indicates the master node. ● Transit: indicates the transit node. ● Edge: indicates the edge node. ● Assistant Edge: indicates the assistant edge node. To specify the parameter, run the **ring node-mode** command.

Item	Description
Ring State	Status of the RRPP ring. The value can be: ● Complete: indicates that the ring is complete. Only the master node can be in Complete state. ● Failed: indicates that the ring fails. Only the master node can be in Failed state. ● Unknown: indicates that the status of the ring is unknown. The Unknown state occurs when RRPP or the RRPP ring is enabled. ● LinkUp: indicates that the link is Up. Only transit nodes can be in LinkUp state. ● LinkDown: indicates that the link is Down. Only transit nodes can be in LinkDown state. ● Preforwarding: indicates that the link is in Preforwarding state. Only transit nodes can be in Preforwarding state.
Is Enabled	Whether the ring is enabled. To enable a ring, run the **ring enable** command.
Is Active	Whether the RRPP ring is activated. The RRPP ring can be activated only when RRPP and the RRPP ring are enabled. To activate an RRPP ring, run the **rrpp enable** and **ring enable** commands.
Primary port	Primary interface on the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Secondary port	Secondary interface on the RRPP ring. To specify the parameter, run the **ring node-mode** command.
Port status	Status of an interface on the RRPP ring. The value can be: ● UNKNOWN: indicates that the device is not properly installed in a stack. ● UP: indicates that the interface is in Up state and can forward packets. ● DOWN: indicates that the interface is not connected. ● BLOCKED: indicates that the interface is in Up state but cannot forward packets.

5.14.11 domain (RRPP ring group view)

Function

The **domain** command adds sub-rings to an RRPP ring group.

The **undo domain** command deletes the sub-rings from the RRPP ring group.

Format

domain *domain-id* **ring** { *ring-id1* [**to** *ring-id2*] } &<1-10>

undo domain *domain-id* **ring** { *ring-id1* [**to** *ring-id2*] } &<1-10>

Parameters

Parameter	Description	Value
domain-id	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id1* **to** *ring-id2*	Specifies the ID of an RRPP sub-ring. ● *ring-id1* specifies the first sub-ring ID. ● **to** *ring-id2* specifies the last sub-ring ID. The value of *ring-id2* must be larger than the value of *ring-id1*. *ring-id1* and *ring-id2* identify a range of instances. If **to** *ring-id2* is not specified, only *ring-id1* is specified.	The value is an integer that ranges from 1 to 64.

Views

RRPP ring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple RRPP rings exist, you can add sub-rings to the ring group to reduce the number of Edge-Hello packets, improving system performance.

Precautions

A maximum of 15 sub-rings can be added to a ring group.

If the **domain** command is run more than once, all configurations take effect.

- Only an edge node or an assistant edge node on a sub-ring can be added to a ring group. The edge nodes on the sub-rings are configured on the same device. Similarly, the assistant edge nodes are on the same device.
- A sub-ring can belong to only one ring group.
- All the sub-rings in a ring group must be on the same type of nodes, that is, edge nodes or assistant edge nodes.
- To add an activated sub-ring to a ring group, add the sub-ring to the ring group on the assistant edge node, and then perform the same operation on the edge node.

- To delete an activated sub-ring from a ring group, delete the sub-ring from the ring group on the edge node, and then perform the same operation on the assistant edge node.
- All the sub-rings in a ring group must have the same primary ring link; otherwise, the ring group cannot work properly.
- The configuration and activation status of a ring group must be the same on the edge node and assistant edge node.

Example

Add sub-rings to Ring Group 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp ring-group 1
[HUAWEI-rrpp-ring-group1] domain 1 ring 1 to 3 5
```

5.14.12 protected-vlan

Function

The **protected-vlan** command configures a list of protected VLANs in an RRPP domain.

The **undo protected-vlan** command deletes the list of protected VLANs in an RRPP domain.

Format

protected-vlan reference-instance { **all** | { { *instance-id1* [**to** *instance-id2*] } &<1-10> } }

undo protected-vlan reference-instance { **all** | { { *instance-id1* [**to** *instance-id2*] } &<1-10> } }

Parameters

Parameter	Description	Value
reference-instance	Indicates the instance imported by a specified RRPP domain.	-
all	Indicates that VLANs in all the instances are protected VLANs. **all** can be configured successfully only when instances 0 to 64 are created. This task is performed to create an instance and configure the mapping between the instance and VLANs.	-

Parameter	Description	Value
instance-id1 **to** *instance-id2*	Specifies the ID of a protected instance. ● *instance-id1* specifies the first instance ID. The value is an integer that ranges from 0 to 4094. ● **to** *instance-id2* specifies the last instance ID. *instance-id2* is an integer that ranges from 0 to 4094. The value of *instance-id2* must be larger than the value of *instance-id1*. *instance-id1* and *instance-id2* identify a range of instances. If **to** *instance-id2* is not specified, only *instance-id1* is specified.	The value is an integer that ranges from 0 to 4094.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The control VLAN transmits RRPP protocol packets and the data VLAN transmits data packets. The control VLAN and data VLANs must be configured as the protected VLANs so that RRPP takes effect for these VLAN packets. Otherwise, VLAN packets may cause broadcast storms on the ring network. This will cause the network to be unavailable.

Precautions

When you configure the list of protected VLANs, note the following points:

- Protected VLANs must be configured before you configure an RRPP ring.
- You can delete or change existing protected VLANs before configuring an RRPP ring. The protected VLANs cannot be changed after the RRPP ring is configured.
- In the same physical topology, the control VLAN of a domain cannot be configured as a protected VLAN of another domain.
- The control VLAN must be configured as a protected VLAN; otherwise, the RRPP ring cannot be configured.
- The control VLAN can be mapped to other instances before the RRPP ring is created. After the RRPP ring is created, the mapping cannot be changed unless you delete the RRPP ring.
- When an RRPP domain is deleted, the protected VLANs in the RRPP domain are deleted automatically.
- When the mapping between an instance and VLANs changes, the protected VLANs of the RRPP domain also change.
- All the VLANs allowed by an RRPP interface must be configured as protected VLANs.

If the **protected-vlan** command is run more than once, all configurations take effect.

Example

Configure the VLANs mapping instances 0 as the protected VLANs in Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
```

5.14.13 reset rrpp error packet statistics

Function

The **reset rrpp error packet statistics** command clears statistics on RRPP error packets.

Format

reset rrpp error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to check statistics on RRPP error packets from the current time, you can run this command to clear historical statistics on RRPP error packets.

Configuration Impact

The statistics on all the RRPP error packets are cleared and cannot be restored after you run the command. Exercise caution when you run the command.

Example

Clear statistics on all the RRPP error packets.

```
<HUAWEI> reset rrpp error packet statistics
```

5.14.14 reset rrpp statistics

Function

The **reset rrpp statistics** command clears statistics on all RRPP packets.

Format

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.
ring *ring-id*	Specifies the ID of an RRPP ring. If *ring-id* is specified, statistics on RRPP packets on the primary and secondary interfaces of the specified ring in the domain of the switch are cleared. If *ring-id* is not specified, statistics on all the RRPP packets on the RRPP interfaces of all rings are cleared.	The value is an integer that ranges from 1 to 64.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command clears statistics on all the RRPP packets so that you can collect new statistics to analyze the network.

Precautions

The statistics on RRPP packets cannot be restored after you clear them. Exercise caution before you run the command.

Example

Clear the statistics on RRPP packets on Ring 1 in Domain 1.

```
<HUAWEI> reset rrpp statistics domain 1 ring 1
```

Clear the statistics on RRPP packets all the rings in Domain 1.

```
<HUAWEI> reset rrpp statistics domain 1
```

5.14.15 ring enable

Function

The **ring enable** command enables an RRPP ring.

The **undo ring enable** command disables an RRPP ring.

By default, an RRPP ring is disabled.

Format

ring *ring-id* **enable**

undo ring *ring-id* **enable**

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an RRPP ring.	The value is an integer that ranges from 1 to 64.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RRPP ring cannot be activated using the **ring enable** command. You also need to run the **rrpp enable** command to enable RRPP so that the RRPP ring can be activated.

Example

Activate ring 1 in Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 1 node-mode transit primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 1
[HUAWEI-rrpp-domain-region1] ring 1 enable
```

Disable Ring 1 in Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] undo ring 1 enable
```

5.14.16 ring node-mode

Function

The **ring node-mode** command configures the node mode and specifies the interfaces for nodes.

The **undo ring** command deletes an RRPP ring.

NOTE

Deleting the RRPP ring can delete the mode configured on the node and interfaces on the node.

Format

ring *ring-id* **node-mode** { **master** | **transit** } **primary-port** *interface-type interface-number* **secondary-port** *interface-type interface-number* **level** *level-value*

ring *ring-id* **node-mode** { **assistant-edge** | **edge** } **common-port** *interface-type interface-number* **edge-port** *interface-type interface-number*

undo ring *ring-id*

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an RRPP ring to be created or deleted.	The value is an integer that ranges from 1 to 64.
master	Specifies the current device as the master node on the RRPP ring to be created. You need to specify the primary and secondary interfaces on the master node, and the level of the ring.	-
transit	Specifies the current device as a transit node on the RRPP ring to be created. You need to specify the primary and secondary interfaces on the transit node, and the level of the ring.	-

Parameter	Description	Value
primary-port	Specifies the primary interface on the node.	-
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary-port	Specifies the secondary interface of the node.	-
level-value	Specifies the level on an RRPP ring.	The value can be 0 or 1. ● 0: indicates a major ring. ● 1: indicates a sub-ring.
assistant-edge	Specifies the current device as the assistant edge node on the RRPP ring to be created.	-
edge	Specifies the current device as the edge node on the RRPP ring to be created.	-
common-port *interface-type interface-number*	Specifies the common interface of the sub-ring and major ring. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
edge-port *interface-type interface-number*	Specifies the edge interface of the sub-ring. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RRPP specifies devices and interfaces on the ring network as nodes and interfaces of different roles on the RRPP ring to implement RRPP functions.

Prerequisites

An RRPP domain has been created using the **rrpp domain** command, and STP has been enabled using the **stp disable** command on the interfaces that want to join the RRPP domain.

Precautions

- The rings in the same RRPP domain must use different ring IDs.
- After the RRPP ring is enabled, to delete the RRPP ring using the **undo ring** *ring-id* command, you must run the **undo ring** *ring-id* **enable** command to disable the RRPP ring first.
- After the **control-vlan** command is used to configure the control VLAN in an RRPP domain, the ID of the sub-control VLAN is the control VLAN ID plus one. If the protected VLAN list specified by **protected-vlan** does not contain the control VLAN or sub-control VLAN, the system displays an error message when you run the **ring node-mode** command.

Example

Configure the master node of Ring 10 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 10 node-mode master primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 0
```

Configure the transit node of Ring 10 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 10 node-mode transit primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 0
```

Configure the master node of Ring 20 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
```

```
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 20 node-mode master primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 1
```

Configure the transit node of Ring 20 in Domain 1, with GE0/0/5 as the primary interface and GE0/0/6 as the secondary interface.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] control-vlan 100
[HUAWEI-rrpp-domain-region1] protected-vlan reference-instance 0
[HUAWEI-rrpp-domain-region1] ring 20 node-mode transit primary-port gigabitethernet 0/0/5
secondary-port gigabitethernet 0/0/6 level 1
```

Delete Ring 10.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] undo ring 10 enable
[HUAWEI-rrpp-domain-region1] undo ring 10
```

5.14.17 rrpp domain

Function

The **rrpp domain** command creates an RRPP domain.

The **undo rrpp domain** command deletes an RRPP domain.

By default, the RRPP domain is not created.

Format

rrpp domain *domain-id*

undo rrpp domain *domain-id*

Parameters

Parameter	Description	Value
domain *domain-id*	Specifies the ID of an RRPP domain.	The value is an integer that ranges from 1 to 64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Other RRPP configurations can be performed only after an RRPP domain is created.

Precautions

Before you delete a domain, ensure that no RRPP ring is configured in the domain. If a ring exists in the domain, the domain cannot be deleted.

Example

Create RRPP Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1]
```

Delete RRPP Domain 1.

```
<HUAWEI> system-view
[HUAWEI] undo rrpp domain 1
```

5.14.18 rrpp enable

Function

The **rrpp enable** command enables RRPP.

The **undo rrpp enable** or **rrpp disable** command disables RRPP.

By default, RRPP is disabled.

Format

rrpp enable

undo rrpp enable

rrpp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RRPP ring cannot be activated using the **rrpp enable** command. You also need to run the **ring enable** command to enable RRPP so that the RRPP ring can be activated.

NOTE

Running the **undo rrpp enable** or **rrpp disable** command may cause network loops. Therefore, exercise caution when running these commands.

Example

Enable RRPP.

```
<HUAWEI> system-view
[HUAWEI] rrpp enable
```

Disable RRPP.

```
<HUAWEI> system-view
[HUAWEI] undo rrpp enable
```

Disable RRPP.

```
<HUAWEI> system-view
[HUAWEI] rrpp disable
```

5.14.19 rrpp linkup-delay-timer

Function

The **rrpp linkup-delay-timer** command sets the value of a LinkUp timer.

The **undo rrpp linkup-delay-timer** command restores the default value of a LinkUp timer.

By default, the value of a LinkUp timer is 0.

Format

rrpp linkup-delay-timer *linkup-delay-timer-value*

undo rrpp linkup-delay-timer

Parameters

Parameter	Description	Value
linkup-delay-timer-value	Sets the value of the LinkUp timer.	The value is an integer that ranges from 0 to 1000, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the link recovers, transmission paths of the traffic are switched frequently if the link status changes frequently on a ring. As a result, link flapping occurs and system performance deteriorates. To address this problem, a LinkUp timer is used to set the period after which the status of the master node changes to Complete.

Precautions

After a LinkUp timer is set, the status of the Blocked interface on the RRPP link is changed only after the period set using the *linkup-delay-timer-value* command. This prevents link flapping.

The value set by the *linkup-delay-timer-value* command must be no larger than the value of the Fail timer minus twice the value of the Hello timer.

The **rrpp linkup-delay-timer** command is valid only for the master node.

Configure the LinkUp timer on the master node on the RRPP ring.

In scenarios where RRPP packets are transparently transmitted, running the **rrpp linkup-delay-timer** command on the master node of the major ring is not recommended. If you do so, temporary loops may occur due to RRPP packet interruption or loss.

Example

Set the value of the LinkUp timer to 2 seconds.

```
<HUAWEI> system-view
[HUAWEI] rrpp linkup-delay-timer 2
```

5.14.20 rrpp ring-group

Function

The **rrpp ring-group** command creates an RRPP ring group and enters the RRPP ring group view.

The **undo rrpp ring-group** command deletes an RRPP ring group.

By default, the RRPP ring group is not created.

Format

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

Parameters

Parameter	Description	Value
ring-group *ring-group-id*	Specifies the ID of an RRPP ring group.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can create an RRPP ring group to reduce the number of Edge-Hello packets, improving system performance.

Precautions

A maximum of 16 ring groups are supported on each node.

When running the **rrpp ring-group** command to add a subring to a ring group, add the subring to the ring group on the assistant edge node and then on the edge node.

To delete a ring group, delete it on the edge node first, and then perform the same operation on the assistant edge node.

Example

Create Ring Group 1 and enter its view.

```
<HUAWEI> system-view
[HUAWEI] rrpp ring-group 1
[HUAWEI-rrpp-ring-group1]
```

5.14.21 rrpp snooping enable

Function

The **rrpp snooping enable** command enables RRPP snooping on an interface.

The **undo rrpp snooping enable** command disables RRPP snooping on an interface.

By default, RRPP snooping is disabled on an interface.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

rrpp snooping enable

undo rrpp snooping enable

Parameters

None

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an RRPP ring accesses the virtual private LAN service (VPLS) network in which devices are connected using PWs, the device cannot respond to RRPP protocol packets directly. Therefore, the VPLS network cannot sense the status change of the RRPP ring. When the RRPP ring topology changes, each node in the VPLS network forwards downstream data according to the MAC address table generated before the RRPP ring topology changes. As a result, the downstream traffic cannot be forwarded. When RRPP snooping is configured on sub-interfaces or VLANIF interfaces, the VPLS network can transparently transmit RRPP protocol packets, detect the changes on the RRPP rings, and upgrade the forwarding entries to ensure that traffic is switched in time to a congestion-free path.

When an RRPP network and a VPLS network are connected to form a network, you can run the **rrpp snooping enable** command to enable RRPP snooping on interfaces of the devices deployed on the network.

Precautions

Before running the **rrpp snooping enable** command, ensure that the following configurations are completed on the sub-interface or VLANIF interface:

- Binding the sub-interface or VLANIF interface to a VSI using the **l2 binding vsi** *vsi-name* command in the interface view.
- Specifying that the sub-interface or VLANIF interface permits only the packets in the control VLAN of the RRPP domain to pass through.

After you run the **rrpp snooping enable** command, RRPP snooping is automatically associated with the VSI bound to this interface.

When RRPP snooping is enabled on the interface, the status of the RRPP ring can be detected through RRPP control packets. When the RRPP ring status changes, the VSI can receive a notification and update the MAC address table.

RRPP and RRPP snooping cannot be simultaneously configured on the same interface.

Example

Enable RRPP snooping on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rrpp snooping enable
```

5.14.22 rrpp snooping vsi

Function

The **rrpp snooping vsi** command associates RRPP snooping on an interface with a VSI that is not bound to the interface.

The **undo rrpp snooping vsi** command cancels the configuration.

By default, the RRPP snooping-enabled interface is not associated with other VSIs on the device.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

rrpp snooping vsi *vsi-name*

undo rrpp snooping vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario of RRPP and VPLS association, when the RRPP ring fails, the RRPP snooping-enabled interface clears the forwarding entries on the associated VSI and the remote VPLS device, and relearns the entries. In this way, downstream traffic can be forwarded through a normal path.

Precautions

Before running the **rrpp snooping vsi** command, you must enable RRPP snooping using the **rrpp snooping enable** command.

The VSI specified in the **rrpp snooping vsi** command is bound to other sub-interfaces or VLANIF interfaces, instead of the interface where RRPP snooping is enabled.

After you run the **rrpp snooping vsi** command, the change of the RRPP ring status is reported to the VSI that is bound to the interface so that the VSI can update its MAC address table.

Example

Associate RRPP snooping with VSI **abc**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rrpp snooping vsi abc
```

5.14.23 rrpp snooping all-vsi

Function

The **rrpp snooping all-vsi** command associates a sub-interface with the VSI that all the other sub-interfaces connected to the same primary interface are bound to.

The **undo rrpp snooping all-vsi** command cancels the association.

By default, a sub-interface is not associated with the VSI that all the other sub-interfaces connected to the same primary interface are bound to.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

rrpp snooping all-vsi

undo rrpp snooping all-vsi

Parameters

None

Views

GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, MultiGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario of RRPP and VPLS association, when the RRPP ring fails, the RRPP snooping-enabled sub-interface clears the forwarding entries on the associated VSI and the remote VPLS device, and relearns the entries. In this way, downstream traffic can be forwarded through a normal path.

You can run the **rrpp snooping all-vsi** command on the RRPP snooping-enabled sub-interface to associate the sub-interface with the VSI that all the other sub-interfaces connected to the same primary interface are bound to. The sub-interface clears all the forwarding entries of associated VSIs when the preceding fault occurs.

Prerequisites

RRPP snooping has been enabled using the **rrpp snooping enable** command.

Precautions

- You must run the **l2 binding vsi** *vsi-name* command to bind other interfaces connected to the same primary interface to the VSI before associating the VSI using the **rrpp snooping all-vsi** command on the current sub-interface.
- You can run the **undo rrpp snooping all-vsi** command to cancel all the associations between the current sub-interface and the VSIs bound to other interfaces connected to the same primary interface.
- You do not need to enable RRPP snooping on other sub-interfaces connected to the same primary interface.

Example

Associate the sub-interface with VSIs that all the other sub-interfaces connected to the same primary interface are bound to.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] rrpp snooping enable
[HUAWEI-GigabitEthernet0/0/1.1] rrpp snooping all-vsi
```

5.14.24 timer (RRPP domain view)

Function

The **timer** command sets the values of the Hello timer and Fail timer.

The **undo timer** command restores the default values of the Hello timer and Fail timer.

By default, the value of the Hello timer is 1 second and that of the Fail timer is 6 seconds.

Format

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

Parameters

Parameter	Description	Value
hello-timer *hello-value*	Specifies the value of the Hello timer.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 1.
fail-timer *fail-value*	Specifies the value of the Fail timer.	The value is an integer that ranges from 3 to 1200, in seconds. The default value is 6. The value of *fail-value* must be three times the value of *hello-value* or larger.

Views

RRPP domain view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the values of the Hello timer and Fail timer as required.

Precautions

You need to run the **timer** command only on the master node, edge node, and assistant edge node.

The value of the Fail timer must be three times the value of the Hello timer or larger.

By default, the value of the Hello timer on an edge node is half of the value of the Hello timer on the master node of the major ring.

The values of the Hello timer and Fail timer must be the same on the nodes in an RRPP domain; otherwise, the edge interface on the edge node may be unstable.

You are advised to set the value of the Fail timer to 30 seconds, because the default value may cause temporary loops. For example, when RRPP multi-instance is enabled, multiple RRPP domains are configured on the same ring. If the value of the Fail timer is set to the default value, loops may occur.

Example

Set the Hello timer and Fail timer in RRPP Domain 1 to 2s and 7s respectively.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] timer hello-timer 2 fail-timer 7
```

Restore the default values of the timers in RRPP Domain 1.

```
<HUAWEI> system-view
[HUAWEI] rrpp domain 1
[HUAWEI-rrpp-domain-region1] undo timer
```

5.15 ERPS (G.8032) Configuration Commands

5.15.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.15.2 clear (ERPS ring view)

Function

The **clear** command clears the port blocking mode of an ERPS ring.

Format

clear

Parameters

None

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To clear the FS or MS mode configured by the **erps ring protect-switch** command, run the **clear** command. The **clear** command also provides the following functions:

- Triggers revertive switching before the WTR or WTB timer expires in the case of revertive switching operations.
- Triggers revertive switching in the case of non-revertive operations.

Precautions

The **clear** command is supported in both ERPSv1 and ERPSv2.

Example

Clear the port blocking mode of ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] clear
```

5.15.3 control-vlan (ERPS ring view)

Function

The **control-vlan** command configures a control VLAN for an ERPS ring to forward RAPS PDUs.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in an ERPS ring.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a control VLAN for an ERPS ring.	The value is an integer that ranges from 1 to 4094.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ERPS ring is created, run the **control-vlan** command to create the control VLAN. Unlike a data VLAN, a control VLAN is used only to forward ERPS protocol packets but not forward service packets in an ERPS ring, which improves the security of the ERPS protocol.

Precautions

- If you run the **control-vlan** command multiple times, only the latest configuration takes effect.
- After a control VLAN is created, the **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command used to create common VLANs is displayed in the configuration file.
- After a port is added to an ERPS ring configured with a control VLAN, the port is added to the control VLAN.
  - If the port is a trunk port, the **port trunk allow-pass vlan** *vlan-id* command is displayed in the record of the port that has been added to the ERPS ring in the configuration file.
  - If the port is a hybrid port, the **port hybrid tagged vlan** *vlan-id* command is displayed in the record of the port that has been added to the ERPS ring in the configuration file.
- All the devices in an ERPS ring must use the same control VLAN in an ERPS ring, and different ERPS rings must use different control VLANs.
- The control VLAN must be not created, and is not used by other features. In addition, no interface is added to the control VLAN.
- If ports have been added to an ERPS ring, the control VLAN cannot be modified. To delete the configured control VLAN, run the **undo erps ring** command in the interface view or the **undo port** command in the ERPS ring view to delete ports from the ERPS ring, and run the **undo control-vlan** command to delete the control VLAN.
- Run the **display erps** command to check whether the control VLAN is configured or which VLAN is configured as the control VLAN.

Example

Configure control VLAN 5 in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] control-vlan 5
```

5.15.4 description (ERPS ring view)

Function

The **description** command configures the description of an ERPS ring.

The **undo description** command restores the default description of an ERPS ring.

By default, the description of an ERPS ring is the name of the ERPS ring. For example, if the name of an ERPS ring is Ring1, the default description of the ring is Ring 1.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an ERPS ring.	The value is a string of 1 to 80 case-sensitive characters.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **description** command on the ERPS-enabled device to configure the description of an ERPS ring. The description contains information such as the ID of the ERPS ring, which facilitates maintenance.

Precautions

If you run the **description** command multiple times, only the latest configuration takes effect.

After the description is configured in the ERPS ring view, the description only takes effect on the device.

Example

Configure the description of the ERPS ring 10 as **huawei Ring 1** on the device.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] description huawei Ring 1
```

5.15.5 display erps

Function

The **display erps** command displays ports that are added to an ERPS ring and information about the ERPS ring.

Format

display erps [**ring** *ring-id*] [**verbose**]

Parameters

Parameter	Description	Value
ring *ring-id*	Displays information about an ERPS ring and the ports that are added to the ERPS ring.	The value is an integer that ranges from 1 to 255.
verbose	Displays detailed information about an ERPS ring and the ports that are added to the ERPS ring.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display erps** command on the ERPS-enabled device to view ports added to the ERPS ring and information about the ERPS ring. The command output facilitates ERPS management and helps you learn the running status of ports.

Prerequisites

To view information about ports that have been added to a specified ERPS ring and the ERPS ring, ensure that the ERPS ring has already been created.

Precautions

If **ring** *ring-id* is not specified, information about all the ERPS rings and ports added to the ERPS rings is displayed.

Example

Display information about all ERPS rings and ports that are added to the ERPS rings.

```
<HUAWEI> display erps
D  : Discarding
F  : Forwarding
R  : RPL Owner
N  : RPL Neighbour
FS : Forced Switch
MS : Manual Switch
Total number of rings configured = 4
Ring  Control  WTR Timer  Guard Timer  Port 1              Port 2
ID    VLAN     (min)      (csec)
-------------------------------------------------------------------------------
   1     100         1          50  (D)GE0/0/1          (F,R)GE0/0/2
   2     200         2          50  (D)GE0/0/3          (F)GE0/0/4
   3     300         3          50  (F)ETH-TRUNK3       (D)ETH-TRUNK4
```

```
   4     400         5          50  (F,R)ETH-TRUNK1      (D)ETH-TRUNK2
--------------------------------------------------------------------------------
```

Display information about ERPS ring 1 and ports that are added to ERPS ring 1.

```
<HUAWEI> display erps ring 1
D  : Discarding
F  : Forwarding
R  : RPL Owner
N  : RPL Neighbour
FS : Forced Switch
MS : Manual Switch
Ring  Control  WTR Timer  Guard Timer  Port 1              Port 2
ID    VLAN     (min)      (csec)
--------------------------------------------------------------------------------
   1     100         1          50  (D)GE0/0/1          (F,R)GE0/0/2
--------------------------------------------------------------------------------
```

Display detailed information about all ERPS rings and ports that are added to the ERPS rings.

```
<HUAWEI> display erps verbose
Ring ID                           : 101
Description                       : Ring 101
Control Vlan                      : 1001
Protected Instance                : 4091
Service Vlan                      : 200 to 400
WTR Timer Setting (min)           : 1      Running (s)          : 0
Guard Timer Setting (csec)        : 200    Running (csec)       : 0
Holdoff Timer Setting (deciseconds) : 0      Running (deciseconds) : 0
WTB Timer Running (csec)          : 0
Ring State                        : Idle
RAPS_MEL                          : 7
Revertive Mode                    : Revertive
R-APS Channel Mode                : -
Version                           : 2
Sub-ring                          : No
Forced Switch Port                : -
Manual Switch Port                : -
TC-Notify                         : -
Time since last topology change     : 0 days 0h:31m:49s
--------------------------------------------------------------------------------
Port              Port Role     Port Status     Signal Status
--------------------------------------------------------------------------------
GE0/0/1           Common        Discarding      Non-failed
GE0/0/2           Common        Forwarding      Non-failed

Ring ID                           : 102
Description                       : Ring 102
Control Vlan                      : 1002
Protected Instance                : 4092
Service Vlan                      : 500 to 600
WTR Timer Setting (min)           : 1      Running (s)          : 0
Guard Timer Setting (csec)        : 200    Running (csec)       : 0
Holdoff Timer Setting (deciseconds) : 0      Running (deciseconds) : 0
WTB Timer Running (csec)          : 0
Ring State                        : Idle
RAPS_MEL                          : 7
Revertive Mode                    : Revertive
R-APS Channel Mode                : -
Version                           : 2
Sub-ring                          : No
Forced Switch Port                : -
Manual Switch Port                : -
TC-Notify                         : -
Time since last topology change     : 0 days 4h:12m:20s
--------------------------------------------------------------------------------
Port              Port Role     Port Status     Signal Status
--------------------------------------------------------------------------------
```

```
GE0/0/1             Common        Forwarding       Non-failed
GE0/0/2             RPL Owner     Discarding      Non-failed
```

Display detailed information about ERPS ring 1 and ports that are added to ERPS ring 1.

```
<HUAWEI> display erps ring 1 verbose
Ring ID                             : 1
Description                          : Ring 102
Control Vlan                         : 1002
Protected Instance                   : 4092
Service Vlan                         : 500 to 600
WTR Timer Setting (min)              : 1      Running (s)          : 0
Guard Timer Setting (csec)           : 200    Running (csec)        : 0
Holdoff Timer Setting (deciseconds) : 0      Running (deciseconds) : 0
WTB Timer Running (csec)             : 0
Ring State                           : Idle
RAPS_MEL                             : 7
Revertive Mode                       : Revertive
R-APS Channel Mode                   : -
Version                              : 2
Sub-ring                             : No
Forced Switch Port                   : -
Manual Switch Port                   : -
TC-Notify                            : -
Time since last topology change      : 0 days 4h:13m:40s
--------------------------------------------------------------------------------
Port                Port Role      Port Status      Signal Status
--------------------------------------------------------------------------------
GE0/0/1             Common        Forwarding       Non-failed
GE0/0/2             RPL Owner     Discarding      Non-failed
```

Table 5-103 Description of the display erps command output

Item	Description
D: Discarding	The port is in discarding state.
F: Forwarding	The port is in forwarding state.
R: RPL Owner	The port is the RPL Owner port.
N : RPL Neighbour	The port is the RPL neighbor port.
FS : Forced Switch	The port is blocked by an FS operation.
MS : Manual Switch	The port is blocked by an MS operation.
Total number of rings configured	Number of ERPS rings.
Ring ID	ID of the ERPS ring. To configure an ERPS ring, run the **erps ring** command.
Control VLAN	Control VLAN. To configure a control VLAN, run the **control-vlan** command.
WTR Timer (min)	Value of the WTR timer. To set the value of the WTR timer, run the **wtr-timer** command.
Guard Timer (csec)	Value of the Guard timer. To set the value of the Guard timer, run the **guard-timer** command.

Item	Description
Port 1	A port that is added to the specified ERPS ring.
Port 2	Another port that is added to the specified ERPS ring.
Description	Description of an ERPS ring. To configure the description, run the **description** command.
Protected Instance	ERPS instance. To configure an ERP instance, run the **protected-instance** command.
Service Vlan	Service VLAN associated with ERPS. A service VLAN is mapped to an ERP instance, and is not the control VLAN.
WTR Timer Setting (min) Running (s)	Value of the WTR timer. Setting indicates the configured value and Running indicates the actual value. To set the value of the WTR timer, run the **wtr-timer** command.
Guard Timer Setting (csec) Running (csec)	Value of the Guard timer. Setting indicates the configured value and Running indicates the actual value. To set the value of the Guard timer, run the **guard-timer** command.
Holdoff Timer Setting (deciseconds) Running (deciseconds)	Value of the Holdoff timer. Setting indicates the configured value and Running indicates the actual value. To set the value of the Holdoff timer, run the **holdoff-timer** command.
WTB Timer Running (csec)	Value of the WTB timer.
Ring State	Status of the ERPS ring: ● Idle: indicates that the current blocking point is the RPL Owner port. ● Protection: indicates that a fault has occurred on a link or a device. ● Pending: indicates a transition state during ERPS ring negotiation. For example, the blocking point is being switched back to the RPL Owner port. ● ForcedSwitch: The FS mode is used to block an ERPS port. ● ManualSwitch: The MS mode is used to block an ERPS port.
RAPS_MEL	MEL value. To set the MEL value, run the **raps-mel** command.

Item	Description
Revertive Mode	Revertive or non-revertive switching mode to be used after a faulty ERPS link recovers: ● Revertive: re-blocks the RPL owner port after a faulty ERPS link recovers. ● Non-revertive: retains the RPL owner port status and still blocks the port of the faulty link after a faulty ERPS link recovers. To configure the revertive or non-revertive switching mode, run the **revertive** command.
R-APS Channel Mode	RAPS PDU transmission mode in a sub-ring: ● -: The current ring is not a sub-ring. ● Virtual Channel: VCs are used to transmit RAPS PDUs. ● Non-virtual-channel: NVCs are used to transmit RAPS PDUs. To configure an RAPS PDU transmission mode in a sub-ring, run the **virtual-channel** command.
Version	ERPS version: ● 1: ERPSv1 ● 2: ERPSv2 To configure an ERPS version, run the **version** command.
Sub-ring	ERPS sub-ring ID. To configure an ERPS sub-ring ID, run the **sub-ring** command.
Forced Switch Port	Port that has been blocked by an FS operation. A hyphen (-) indicates that no port has been blocked by an FS operation. To configure an FS mode, run the **erps ring protect-switch** command.
Manual Switch Port	Port that has been blocked by an MS operation. A hyphen (-) indicates that no port has been blocked by an MS operation. To configure a port blocking mode for an ERPS port, run the **erps ring protect-switch** command.
TC-Notify	The ERPS ring is configured to notify other ERPS rings of its topology change. A hyphen (-) indicates that the ERPS ring does not notify other ERPS rings when its topology changes. To configure an ERPS ring to notify other ERPS rings of its topology change, run the **tc-notify erps ring** command.
Time since last topology change	Period since the last ERPS ring topology change.

Item	Description
Port	Port that is added to the ERPS ring.
Port Role	Port role: - RPL Owner - Common - RPL Neighbour
Port Status	Port status: - Forwarding - Discarding
Signal Status	Signal status: - Failed: A fault occurs. - Non-failed: No fault occurs.

5.15.6 display erps interface

Function

The **display erps interface** command displays ERPS information of a port that has been added to an ERPS ring.

Format

display erps interface *interface-type interface-number* [**ring** *ring-id*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays ERPS information of a specified port that has been added to an ERPS ring. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ring *ring-id*	Specifies the ID of the ERPS ring to which the port has been added.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the running status of ports that have been added to an ERPS ring, run the **display erps interface** command.

Example

Display ERPS information about GigabitEthernet0/0/1.

```
<HUAWEI> display erps interface gigabitethernet 0/0/1
Interface State                   : Up
--------------------------------------------------------------------------------
Ring ID                           : 1
Flush Logic
    Remote Node ID                : 0000-0000-0000
    Remote BPR                    : 0
Track Link Detect Protocol        : 1AG
    MD Name                       : 1
    MA Name                       : 1
    MEP ID                        : 2270
    RMEP ID                       : 2260
    CFM State                     : Failed
```

Table 5-104 Description of the **display erps interface** command output

Item	Description
Interface State	Physical status of the port.
Ring ID	ID of the ERPS ring to which the port has been added.
Flush Logic	Whether the FDB logic is updated.
Remote Node ID	ID of the remote node.
Remote BPR	Blocked port reference of the remote node.
Track Link Detect Protocol	Protocol associated with ERPS on the port. The hyphen (-) indicates that no protocol is associated with ERPS on the port.
MD Name	Name of the maintenance domain for which Ethernet CFM is associated with ERPS.
MA Name	Name of the maintenance association (MA) where Ethernet CFM is associated with ERPS.
MEP ID	ID of the maintenance association end point (MEP) where Ethernet CFM is associated with ERPS.
RMEP ID	ID of the remote maintenance association end point (RMEP) where Ethernet CFM is associated with ERPS.

Item	Description
CFM State	Status of the protocol associated with ERPS on the port.

5.15.7 display erps statistics

Function

The **display erps statistics** command displays statistics about sent and received ring auto protection switching (RAPS) protocol data units (PDUs) on the ports that have been added to ERPS rings.

Format

display erps [**ring** *ring-id*] **statistics**

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an ERPS ring. If this parameter is not specified, this command displays statistics about sent and received RAPS PDUs on ports that are added to all ERPS rings.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On a Layer 2 network running ERPS, the **display erps statistics** command displays statistics about sent and received RAPS PDUs on the ports that are added to ERPS rings. The command output helps you analyze the network situation, learn the network running status, and maintain devices.

Prerequisites

To query statistics about sent and received RAPS PDUs on the ports that have been added to a specified ERPS ring, ensure that the ERPS ring has been created.

Example

Display statistics about sent and received RAPS PDUs on the ports that are added to ERPS rings.

```
<HUAWEI> display erps statistics
-------------------------------------------------------------------------------
Ring Port           RX/TX     SF      NR     NRRB      FS      MS    EVENT
-------------------------------------------------------------------------------
   1 Eth-Trunk1      RX        0       0      552       0       0       0
   1 Eth-Trunk1      TX        0      68        0     326       0       6
   1 GE0/0/1         RX        0       6      552       0       0       0
   1 GE0/0/1         TX        4      63        0     326       0       6
  10 GE0/0/2         RX        0       1        0       0       0       0
  10 GE0/0/2         TX        4      74        0       0       0       0
```

Display statistics about sent and received RAPS PDUs on the ports that are added to ERPS ring 2.

```
<HUAWEI> display erps ring 2 statistics
-------------------------------------------------------------------------------
Ring  Port          RX/TX     SF      NR     NRRB      FS      MS    EVENT
-------------------------------------------------------------------------------
   2  GE0/0/1        RX       0       1       0       0       0       0
   2  GE0/0/1        TX       4      74       0       0       0       0
```

Table 5-105 Description of the display erps statistics command output

Item	Description
Ring	ID of the ERPS ring. To configure an ERPS ring, run the **erps ring** command.
Port	Port that is added to the ERPS ring.
RX/TX	RAPS PDU forwarding: ● RX: RAPS PDUs are received. ● TX: RAPS PDUs are sent.
SF	Statistics about RAPS (SF) messages.
NR	Statistics about RAPS (NR) messages.
NRRB	Statistics about RAPS (NR, RB) messages.
FS	Statistics about RAPS (FS) messages.
MS	Statistics about RAPS (MS) messages.
EVENT	Statistics about RAPS Event messages.

5.15.8 encapsulate-ring-id enable

Function

The **encapsulate-ring-id enable** command enables ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets.

The **undo encapsulate-ring-id enable** command disables ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets.

By default, ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets is disabled.

Format

encapsulate-ring-id enable

undo encapsulate-ring-id enable

Parameters

None

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Huawei device cannot communicate with a non-Huawei device that sends ERPS protocol packets whose destination MAC addresses carry ERPS ring IDs. To enable the Huawei device to communicate with such a non-Huawei device, run the **encapsulate-ring-id enable** command to enable ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets sent by the Huawei device.

Precautions

The **encapsulate-ring-id enable** command and its undo form fail to be run in the view of an ERPS ring that has an interface added. To resolve this issue, remove the interface from the ERPS ring by running the **undo erps ring** *ring-id* command in the interface view or **undo port** *interface-type interface-number* command in the ERPS ring view.

Example

Enable ERPS ring ID encapsulation in the destination MAC addresses of ERPS protocol packets.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] encapsulate-ring-id enable
```

5.15.9 erps ring

Function

The **erps ring** command creates an ERPS ring and displays the view of the ERPS ring, or directly displays the view of an existing ERPS ring.

The **undo erps ring** command deletes a created ERPS ring.

By default, no ERPS ring is created.

Format

erps ring *ring-id*

undo erps ring *ring-id*

Parameters

Parameter	Description	Value
ring-id	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ethernet Ring Protection Switching (ERPS) is a standard protocol issued by the ITU-T to prevent loops on ring networks. ERPS implements fast convergence of carrier-class reliability standards. It allows all ERPS-capable devices on a ring network to communicate.

To enable ERPS on the device, run the **erps ring** command to create an ERPS ring and enter the ERPS ring view.

To configure parameters such as the control VLAN and the protected instance for an ERPS ring, run the **erps ring** command to enter the ERPS ring view.

Follow-up Procedure

Run the **control-vlan (ERPS ring view)** command to configure a control VLAN for the ERPS ring.

Run the **protected-instance (ERPS ring view)** command to configure an ERP instance for the ERPS ring.

Precautions

To delete an ERPS ring, ensure that no ports are added to the ERPS ring. If any port is added to the ERPS ring, the system displays a message indicating a failure to delete the ERPS ring. To delete an ERPS ring where ports are added, run the **undo erps ring** command in the interface view or the **undo port** command in the ERPS ring view to remove the port, and run the **undo erps ring** command to delete the ERPS ring.

Example

Create ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1]
```

5.15.10 erps ring (interface view)

Function

The **erps ring** command adds a port to an ERPS ring and specifies a role for the port.

The **undo erps ring** command deletes a port from an ERPS ring and cancels the port role.

By default, a port is not added to an ERPS ring, and no port role is specified.

Format

erps ring *ring-id* [**rpl** { **owner** | **neighbour** }]

undo erps ring *ring-id*

Parameters

Parameter	Description	Value
ring-id	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.
rpl { **owner** | **neighbour** }	Specifies the port to be added to an ERPS ring as the RPL owner port or RPL neighbor port.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ERPS ring is created, run the **erps ring** command in the interface view to add Layer 2 ports to the ERPS ring so that RAPS PDUs can be correctly forwarded. Each device in an ERPS ring is a node, and a maximum of two Layer 2 ports on each node can be added to the same ERPS ring.

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- RPL owner port

  An RPL owner port is responsible for blocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.

  When the node on which the RPL owner port resides receives an RAPS PDU indicating a link or node fault in an ERPS ring, the node unblocks the RPL owner port. Then the RPL owner port can send and receive traffic to ensure nonstop traffic forwarding.

  The link where the RPL owner port resides is the RPL.

- RPL neighbor port

  An RPL neighbor port is directly connected to an RPL owner port.

  Both the RPL owner port and RPL neighbor ports are blocked in normal situations to prevent loops.

  If an ERPS ring fails, both the RPL owner and neighbor ports are unblocked.

  The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port resides.

- Common port

  Common ports are ring ports other than the RPL owner and neighbor ports.

  A common port monitors the status of the directly connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Prerequisites

An ERPS ring has been created using the **erps ring** command.

- The control VLAN and ERP instance have been configured using the **control-vlan** and **protected-instance** commands respectively in the ERPS ring view.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- Spanning Tree Protocol (STP), Rapid Ring Protection Protocol (RRPP), Smart Ethernet Protection (SEP), or Smart Link is not enabled on the port.
  - If the port has STP enabled, run the **stp disable** command in the interface view to disable STP.
  - If the port has RRPP enabled, run the **undo ring** *ring-id* command in the RRPP domain view to disable RRPP.
  - If the port has SEP enabled, run the **undo sep segment** *segment-id* command in the interface view to disable SEP.
  - If the port has Smart Link enabled, run the **undo port** command in the Smart Link group view to disable Smart Link.

- ERPSv2 has been specified in the ERPS ring using the **version v2** command if the port is specified as an RPL neighbor port.

Precautions

- Before running the **undo erps ring** command to delete a port from an ERPS ring, run the **shutdown (interface view)** command to shut down the port. The port can be enabled again according to the actual situation.
- If ports added to an ERPS ring are all ordinary ports, any port on the device with the largest MAC address will be blocked.
- If an RPL neighbor port is configured for a non-virtual channel of a sub-ring, network convergence may fail to meet requirements because SF packets are discarded on the port in the case of a link fault.

Example

Add GE0/0/1 to ERPS ring 2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 2
```

5.15.11 erps ring protect-switch

Function

The **erps ring protect-switch** command configures a port blocking mode for an ERPS port.

Format

erps ring *ring-id* **protect-switch** { **force** | **manual** }

Parameters

Parameter	Description	Value
ring-id	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.
force	Forcibly blocks a port immediately after FS is configured, irrespective of whether link failures have occurred.	-
manual	Indicates the MS mode for blocking an ERPS port.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Because the Ring Protection Link (RPL) may have high bandwidth, you can block the low-bandwidth link so that user traffic can be transmitted on the RPL. ERPSv2 supports both Forced Switch (FS) and Manual Switch (MS) modes for blocking an ERPS port:

- FS: forcibly blocks a port immediately after FS is configured, irrespective of whether link failures have occurred.
- MS: blocks a port on which MS is configured when the ERPS ring is in Idle or Pending state.

FS takes precedence over MS.

Prerequisites

- The **erps ring** or **port (ERPS ring view)** command has been executed to add the port to an ERPS ring.
- The **version v2** command has been executed to specify ERPSv2.

Configuration Impact

After an ERPS port is blocked in FS or MS mode, the node on which the ERPS port resides sends RAPS (FS) or RAPS (MS) messages to the other nodes in the ERPS ring. As a result, ERPS performs recalculation and finally unblocks the RPL owner port.

Precautions

The ERPS ring specified by *ring-id* must be the one to which the port belongs; otherwise, the command does not take effect.

To change the port blocking mode from MS to FS, run the **erps ring** *ring-id* **protect-switch force** command to set the FS mode. To change the port blocking mode from FS to MS, run the **clear** command in the ERPS ring view to delete the FS mode, and then run the **erps ring** *ring-id* **protect-switch manual** command to set the MS mode.

You can delete the manual port blocking mode only by using the **clear** command in the ERPS ring view.

The **erps ring protect-switch** command is not saved in the configuration file.

Example

Specify the FS mode to block GigabitEthernet0/0/1 in ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 5
[HUAWEI-GigabitEthernet0/0/1] erps ring 5 protect-switch force
```

5.15.12 erps track cfm

Function

The **erps track cfm** command associates ERPS with Ethernet CFM to fast detect link failures.

The **undo erps track cfm** command disassociates ERPS from Ethernet CFM.

By default, ERPS is not associated with Ethernet CFM.

Format

erps ring *ring-id* **track cfm md** *md-name* **ma** *ma-name* **mep** *mep-id* **remote-mep** *rmep-id*

undo erps ring *ring-id* [**track cfm**]

Parameters

Parameter	Description	Value
ring *ring-id*	Specifies the ID of an ERPS ring.	The value is an integer that ranges from 1 to 255.
md *md-name*	Specifies the name of a maintenance domain (MD).	The value is a string of 1 to 43 case-sensitive characters. Spaces and question marks (?) are not supported. MD names on a device must be unique. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of a maintenance association (MA).	The value is a string of 1 to 43 case-sensitive characters. Spaces and question marks (?) are not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
mep *mep-id*	Specifies the ID of a maintenance association end point (MEP).	The value is an integer that ranges from 1 to 8191.

Parameter	Description	Value
remote-mep *rmep-id*	Specifies the ID of a remote maintenance association end point (RMEP).	The value is an integer that ranges from 1 to 8191.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect faults, implement fast convergence, and shorten traffic interruptions, run the **erps track cfm** command to associate ERPS with Ethernet CFM on a port added to an ERPS ring.

Prerequisites

- STP, RRPP, or SEP is not enabled on the port.
  - If the port has STP enabled, run the **stp disable** command in the interface view to disable STP.
  - If the port has RRPP enabled, run the **undo ring** *ring-id* command in the RRPP domain view to disable RRPP.
  - If the port has SEP enabled, run the **undo sep segment** *segment-id* command in the interface view to disable SEP.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- The ERPS ring specified by **ring** *ring-id* must be the one to which the port belongs.
- Ethernet CFM has not been applied to other ports in the ERPS ring.

Precautions

This command is supported in both ERPSv1 and ERPSv2.

The association between ERPS and CFM takes effect only when the interface has ERPS associated with CFM and has an interface-based MEP created using the **mep mep-id** command.

Example

Associate ERPS with Ethernet CFM on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 5
[HUAWEI-GigabitEthernet0/0/1] erps ring 5 track cfm md md1 ma ma1 mep 1 remote-mep 2
```

5.15.13 erps vpls-subinterface enable

Function

The **erps vpls-subinterface enable** command enables topology change notification of an interface to instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

The **undo erps vpls-subinterface enable** command disables topology change notification of an interface.

By default, the interface does not instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6720-EI, S6720S-EI, S6730S-H, S6730-H support this command.

Format

erps vpls-subinterface enable

undo erps vpls-subinterface enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, when an ERPS ring topology changes, the ERPS ring reselects a blocked interface, and accordingly all devices will update MAC address entries. However, if an ERPS-enabled interface has VSI-bound sub-interfaces or VLANIF interfaces, which cannot detect topology changes immediately, the MAC address entries will not be updated on the VPLS network in time. To resolve this problem, run the **erps vpls-subinterface enable** command to enable an interface to instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

Prerequisites

An interface has been added to an ERPS ring using the **erps ring (interface view)** command.

Configuration Impact

After the **erps vpls-subinterface enable** command has been run, when the forwarding status of an interface changes to Discarding, its VSI-bound sub-interfaces or VLANIF interfaces will change to the Flowdown state to prevent loops on the VPLS network on which a CE is dual-homed to PEs.

Precautions

The **erps vpls-subinterface enable** and **stp vpls-subinterface enable** commands are mutually exclusive on the same interface.

If an interface is deleted from all ERPS rings using the **undo erps ring** command, the **erps vpls-subinterface enable** command configuration on the interface is also deleted.

If a user is delivering the ERPS configuration, the **erps vpls-subinterface enable** command fails to be run.

Example

Enable GE0/0/1 to instruct VSI-bound sub-interfaces or VLANIF interfaces to update MAC address entries promptly after the ERPS ring topology changes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] erps ring 1
[HUAWEI-GigabitEthernet0/0/1] erps vpls-subinterface enable
```

5.15.14 guard-timer (ERPS ring view)

Function

The **guard-timer** command sets the Guard timer in an ERPS ring.

The **undo guard-timer** command restores the default value of the Guard timer.

By default, the Guard timer is 200 centiseconds in an ERPS ring.

Format

guard-timer *time-value*

undo guard-timer

Parameters

Parameter	Description	Value
time-value	Specifies the value of the Guard timer in an ERPS ring.	The value is an integer that ranges from 1 to 200, in centiseconds.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running ERPS, after a faulty link or node recovers, the device sends RAPS PDUs to inform the other nodes of link or node recovery and starts the Guard timer. Before the Guard timer expires, the device does not receive any RAPS PDU. If the device receives out-of-date RAPS PDUs indicating that the link or node fails, the local port may be blocked again. After the Guard timer expires, if the device receives an RAPS PDU indicating that another port fails, the local port enters the Forwarding state.

Precautions

If the value of the Guard timer is too small, network loops may occur. The default value (200 centiseconds) is recommended.

Example

Set the Guard timer to 180 centiseconds in ERPS ring 10.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] guard-timer 180
```

5.15.15 holdoff-timer (ERPS ring view)

Function

The **holdoff-timer** command sets the Holdoff timer in an ERPS ring.

The **undo holdoff-timer** command restores the default value of the Holdoff timer.

By default, the Holdoff timer is 0 deciseconds in an ERPS ring.

Format

holdoff-timer *time-value*

undo holdoff-timer

Parameters

Parameter	Description	Value
time-value	Specifies the value of the Holdoff timer in an ERPS ring.	The value is an integer that ranges from 0 to 100, in deciseconds.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On Layer 2 networks running ERPS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. That is, protection switching is not performed immediately.

You can run the **holdoff-timer** command to set the Holdoff timer. When a fault occurs, the fault is not immediately reported to ERPS. Instead, the Holdoff timer starts. If the fault persists after the timer expires, the fault will be reported to ERPS.

Precautions

If you run the **holdoff-timer** command multiple times, only the latest configuration takes effect.

Example

Set the Holdoff timer to 10 in ERPS ring 10.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] holdoff-timer 10
```

5.15.16 port (ERPS ring view)

Function

The **port** command adds a port to an ERPS ring and specifies a role for the port.

The **undo port** command deletes a port from an ERPS ring and cancels the port role.

By default, a port is not added to an ERPS ring, and no port role is specified.

Format

port *interface-type interface-number* [**rpl** { **owner** | **neighbour** }]

undo port *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the port to be added to an ERPS ring. *interface-type* specifies the interface type and *interface-number* specifies the interface number.	-
rpl { **owner** | **neighbour** }	Specifies the port to be added to an ERPS ring as the RPL owner port or RPL neighbor port.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ERPS ring is created, run the **port** command to add Layer 2 ports to the ERPS ring so that RAPS PDUs can be correctly forwarded. Each device in an ERPS ring is a node, and a maximum of two Layer 2 ports on each node can be added to the same ERPS ring.

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- RPL owner port

  An RPL owner port is responsible for blocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.

  When the node on which the RPL owner port resides receives an RAPS PDU indicating a link or node fault in an ERPS ring, the node unblocks the RPL owner port. Then the RPL owner port can send and receive traffic to ensure nonstop traffic forwarding.

  The link where the RPL owner port resides is the RPL.

- RPL neighbor port

  An RPL neighbor port is directly connected to an RPL owner port.

  Both the RPL owner port and RPL neighbor ports are blocked in normal situations to prevent loops.

  If an ERPS ring fails, both the RPL owner and neighbor ports are unblocked.

  The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port resides.

- Common port

  Common ports are ring ports other than the RPL owner and neighbor ports.

  A common port monitors the status of the directly connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Prerequisites

- The control VLAN and ERP instance have been configured using the **control-vlan** and **protected-instance** commands respectively in the ERPS ring view.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- Spanning Tree Protocol (STP), Rapid Ring Protection Protocol (RRPP), Smart Ethernet Protection (SEP), or Smart Link is not enabled on the port.
  - If the port has STP enabled, run the **stp disable** command in the interface view to disable STP.
  - If the port has RRPP enabled, run the **undo ring** *ring-id* command in the RRPP domain view to disable RRPP.
  - If the port has SEP enabled, run the **undo sep segment** *segment-id* command in the interface view to disable SEP.
  - If the port has Smart Link enabled, run the **undo port** command in the Smart Link group view to disable Smart Link.
- ERPSv2 has been specified in the ERPS ring using the **version v2** command if the port is specified as an RPL neighbor port.

Precautions

Before deleting a port from an ERPS ring or changing the port role, use the **shutdown (interface view)** command to disable the port. Then remove the port or change the port role and run the **undo shutdown (interface view)** command to enable the port. Otherwise, traffic forwarding may fail.

If ports added to an ERPS ring are all ordinary ports, any port on the device with the largest MAC address will be blocked.

Example

Add GE0/0/1 to ERPS ring 10, and set the port to the RPL owner port.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] port gigabitethernet 0/0/1 rpl owner
```

5.15.17 protected-instance (ERPS ring view)

Function

The **protected-instance** command configures Ethernet ring protection (ERP) instances in an ERPS ring.

The **undo protected-instance** command deletes ERP instances from an ERPS ring.

By default, no ERP instance is configured in an ERPS ring.

Format

protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] &<1-10> } }

undo protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] &<1-10> } }

Parameters

Parameter	Description	Value
instance-id1 **to** *instance-id2*	Specifies the ID of an ERP instance. - *instance-id1* specifies the first ERP instance ID. - **to** *vlan-id2* specifies the last ERP instance ID. The value of *instance-id2* must be greater than the value of *instance-id1*. *instance-id1* and *instance-id2* identify a range of ERP instances. If **to** *instance-id2* is not specified, only *instance-id1* is specified.	The value is an integer that ranges from 0 to 4094.
all	Indicates all ERP instances.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running ERPS, the VLAN where ERPS PDUs and data packets are transmitted must be mapped to an ERP instance. Otherwise, VLAN packets may cause broadcast storms on the ring network. As a result, the network may become unavailable.

Precautions

- If the **stp mode (system view)** command is used to set the STP working mode to VLAN-based Spanning Tree (VBST), the ERP instance specified by the **protected-instance** command must be the created static instance.
- If you run the **protected-instance** command multiple times in the same ERPS ring, multiple ERP instances are configured.
- If ports have been added to the ERPS ring, the ERP instance cannot be modified. To delete the configured ERP instance, run the **undo erps ring** command in the interface view or the **undo port** command in the ERPS ring view to delete ports from the ERPS ring, and run the **undo protected-instance** command to delete the ERP instance.

Follow-up Procedure

Configure the mapping between protected instances and VLANs. The specific procedures are as follows:

1. Run the **stp region-configuration** command to enter the MST region view.

2. Run the **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10> command to configure the mapping relationship between the protected instance and the VLAN.

   The parameter *instance-id* in this command must the same as the parameter *instance-id* in the **protected-instance** command.
3. Run the **active region-configuration** command to activate the protected instance and the mapping relationship between the protected instance and the VLAN.

Example

Configure ERP instance 5 in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] protected-instance 5
```

5.15.18 raps-mel

Function

The **raps-mel** command sets the value of the MEL field in Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs).

The **undo raps-mel** command restores the default value of the MEL field.

By default, the value of the MEL field in RAPS PDUs is 7.

Format

raps-mel *level-id*

undo raps-mel

Parameters

Parameter	Description	Value
level-id	Specifies the value of the MEL field in RAPS PDUs.	The value is an integer that ranges from 0 to 7.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running ERPS, if another fault detection protocol is enabled, the MEL field in RAPS PDUs is used to determine whether the RAPS PDUs can be forwarded. If the MEL value in an ERPS ring is smaller than the MEL value of the fault detection protocol, the RAPS PDUs have a lower priority and are discarded. If the MEL value in an ERPS ring is larger than the MEL value of the fault detection protocol, the RAPS PDUs can be forwarded. You can run the **raps-mel** command to set the value of the MEL field in RAPS PDUs.

In addition, the MEL value can also be used for interworking with other vendors' devices in an ERPS ring. The same MEL value ensures smooth communication between devices.

Precautions

If you run the **raps-mel** command multiple times, only the latest configuration takes effect.

Example

Set the value of the MEL field to 5 in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] raps-mel 5
```

5.15.19 reset erps statistics

Function

The **reset erps statistics** command clears packet statistics in an ERPS ring.

Format

reset erps [**ring** *ring-id*] **statistics**

Parameters

Parameter	Description	Value
ring *ring-id*	Clears packet statistics in a specified ERPS ring.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on a specific interface in a given period of time, clear the existing statistics on the interface by using the **reset erps** command.

Prerequisites

The ERPS ring has been created, and ports have been added to the specified ERPS ring.

Precautions

The cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Clear packet statistics in ERPS ring 2.

```
<HUAWEI> reset erps ring 2 statistics
```

5.15.20 revertive

Function

The **revertive** command configures revertive switching or non-revertive switching in an ERPS ring. The switching mode determines whether the RPL owner port is blocked again after a link fault is rectified.

The **undo revertive disable** command restores the default configuration.

By default, ERPS rings use revertive switching.

Format

revertive { **enable** | **disable** }

undo revertive disable

Parameters

Parameter	Description	Value
enable	Enables revertive switching in an ERPS ring.	-
disable	Disables revertive switching. That is, non-revertive switching is used in an ERPS ring.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After link faults in an ERPS ring are rectified, re-blocking the RPL owner port depends on the switching mode:

- In revertive switching, the RPL owner port is re-blocked after the WTR timer expires, and the RPL is blocked.
- In non-revertive switching, the WTR timer is not started, and the original faulty link is still blocked.

Prerequisites

The **version v2** command has been executed to specify ERPSv2.

Example

Configure non-revertive switching in ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] revertive disable
```

5.15.21 sub-ring

Function

The **sub-ring** command configures an ERPS ring as a sub-ring.

The **undo sub-ring** command restores the default configuration.

By default, all ERPS rings are major rings.

Format

sub-ring

undo sub-ring

Parameters

None

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ERPS has two versions: ERPSv1 and ERPSv2. ERPSv2 supports multi-ring topologies such as intersecting ring topologies in addition to single-ring topologies.

To deploy ERPS on a multi-ring network, run the **sub-ring** command to configure some rings as sub-rings.

NOTE

Major rings are closed, and sub-rings are open.

Prerequisites

- The **version v2** command has been executed to specify ERPSv2.
- The ERPS ring does not have any port. If the ERPS ring has a port, run the **undo erps ring** *ring-id* or **undo port** *interface-type interface-number* command to delete the port from the ERPS ring.

Precautions

If a sub-ring uses the VC mode to transmit RAPS PDUs, you must run the **virtual-channel disable** command to restore the RAPS PDU transmission mode to NVC before running the **undo sub-ring** command to restore the sub-ring to a major ring.

Example

Configure ERPS ring 5 as a sub-ring.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] sub-ring
```

5.15.22 tc-notify erps ring

Function

The **tc-notify erps ring** command configures an ERPS ring to notify other ERPS rings of its topology change.

The **undo tc-notify erps ring** command disables the topology change notification function.

By default, an ERPS ring does not notify other ERPS rings of its topology change.

Format

tc-notify erps ring { *ring-id1* [**to** *ring-id2*] } &<1-10>

undo tc-notify erps ring { *ring-id1* [**to** *ring-id2*] } &<1-10>

Parameters

Parameter	Description	Value
ring-id1	Specifies the start ring ID of the ERPS ring that will be notified of the topology change.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
to *ring-id2*	Specifies the end ring ID of the ERPS ring that will be notified of the topology change. *ring-id1* and *ring-id2* specify a ring range. If **to** *ring-id2* is not specified, an ERPS ring notifies only the ERPS ring specified by *ring-id1* of its topology change. **NOTE** You can specify the ring range for a maximum of 10 times, and the ring ranges can overlap.	The value is an integer that ranges from 1 to 255 and must be greater than or equal to *ring-id1*.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the topology of the local ERPS ring changes and other ERPS rings is not notified of the topology change, the MAC address entries remain unchanged on the other ERPS rings and therefore user traffic is interrupted. To ensure nonstop traffic transmission, run the **tc-notify erps ring** command to specify ERPS rings to which topology change notifications are sent.

Prerequisites

The **version v2** command has been executed to specify ERPSv2.

Precautions

- The **tc-notify erps ring** command takes effect only on ERPS sub-rings.
- If an ERPS ring topology changes, the ERPS ring notifies the specified ERPS rings of its topology change. If the ERPS ring that has been specified to receive the topology change notification does not exist, the configuration does not take effect.
- After other ERPS rings receive the topology change notification from an ERPS ring, they send Flush-FDB messages on their separate rings to instruct their nodes to update MAC addresses. This ensures nonstop traffic transmission.
- If the **tc-notify erps ring** command is run more than once, all configurations take effect.

Example

Configure ERPS ring 5 to notify ERPS rings 1 through 3 of its topology change.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] tc-notify erps ring 1 to 3
```

5.15.23 tc-notify sep

Function

The **tc-notify sep** command configures the device to notify a SEP segment of topology changes in the ERPS ring so that the SEP segment can update the FDB in a timely manner.

The **undo tc-notify sep** command disables the topology change notification function.

By default, the device does not notify a SEP segment of topology changes in the ERPS ring.

Format

tc-notify sep { **segment** *segment-id* | **all-segment** }

undo tc-notify sep { **segment** *segment-id* | **all-segment** }

Parameters

Parameter	Description	Value
segment *segment-id*	Specifies the ID of a SEP segment.	The value is an integer in the range from 1 to 1024.
all-segment	Indicates all SEP segments.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

When the topology of the ERPS ring changes and SEP segments are not notified of the topology change, the MAC address entries remain unchanged on the SEP segments and therefore user traffic is interrupted. To ensure nonstop traffic transmission, you can run the **tc-notify sep** command to specify the objects to which ERPS ring topology change notifications are sent.

Example

Configure the device to notify a SEP segment of topology changes in the ERPS ring.

```
<HUAWEI> system-view
[HUAWEI] sep segment 2
[HUAWEI-sep-segment2] quit
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] tc-notify sep segment 2
```

5.15.24 tc-protection interval (ERPS ring view)

Function

The **tc-protection interval** command sets the topology change protection interval at which topology change notification messages are sent.

The **undo tc-protection interval** command restores the default topology change protection interval.

By default, the topology change protection interval is 2s.

Format

tc-protection interval *interval-value*

undo tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the topology change protection interval. A longer interval ensures stable ERPS operation, but may cause slow convergence.	The value is an integer that ranges from 1 to 600, in seconds.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user terminal connects to an upper-layer network through multiple ERPS rings and the topology of the ERPS ring closest to the user terminal changes, topology change notifications will be multiplied by 2 each time they pass through a ring until they reach the upper-layer network. As a result, the upper-layer network receives many identical topology change notifications.

In addition, if an ERPS ring frequently receives topology change notifications, its nodes will have lower CPU processing capability and repeatedly update Flush-FDB packets, consuming much bandwidth. To prevent this problem, run the **tc-protection interval** command to set the topology change protection interval at which the maximum number of topology change notifications specified in the **tc-protection threshold** command are processed. Then, during the topology change protection interval, the device processes only the specified maximum number of topology change notification messages. If there are excess notifications, the device processes all the excess notifications once after the topology change protection interval elapses. For example, if the topology change protection interval is set to 10 seconds and the maximum number is set to 5, when a device receives topology change notifications, the device processes only the first 5 topology change notifications within 10 seconds and processes the subsequent topology change notifications only after 10s. This prevents the device from frequently deleting MAC address entries and ARP entries.

Prerequisites

The **erps ring** command has been executed to create an ERPS ring.

Precautions

Suppressing topology change notification transmission allows the upper-layer network to receive and process only one notification during the topology change protection interval and protects ERPS nodes against topology change (TC) attacks.

Example

Set the topology change protection interval to 3s in ERPS ring 1.

```
<HUAWEI> system-view
[HUAWEI] erps ring 1
[HUAWEI-erps-ring1] tc-protection interval 3
```

5.15.25 tc-protection threshold (ERPS ring view)

Function

The **tc-protection threshold** command sets the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval.

The **undo tc-protection threshold** command restores the default number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval.

By default, ERPS parses topology change notifications and updates forwarding entries three times in the topology change protection interval.

Format

tc-protection threshold *threshold-value*

undo tc-protection threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval.	The value is an integer that ranges from 1 to 255.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a switching device in an ERPS ring network receives topology change notifications, the device updates MAC address entries and ARP entries. Frequent updates will cause a high CPU usage.

To prevent frequent MAC address and ARP entry updates, run the **tc-protection threshold** command to set the maximum number of topology change notifications that can be processed during the topology change protection interval specified by the **tc-protection interval** command. Then, during the topology change protection interval, the device processes only the specified maximum number of topology change notification messages. If there are excess notifications, the device processes all the excess notifications once after the topology change protection interval elapses. For example, if the topology change protection interval is set to 10 seconds and the maximum number is set to 5, when a device receives topology change notifications, the device processes only the first 5 topology change notifications within 10 seconds and processes the subsequent topology change notifications only after 10s. This prevents the device from frequently deleting MAC address entries and ARP entries.

Prerequisites

The **version v2** command has been run to specify ERPSv2.

Example

Set the number of times ERPS parses topology change notifications and updates forwarding entries in the topology change protection interval to 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] tc-protection threshold 5
```

5.15.26 version (ERPS ring view)

Function

The **version** command configures an ERPS version.

The **undo version** command restores the default ERPS version.

By default, ERPSv1 is used.

Format

version { **v1** | **v2** }

undo version

Parameters

Parameter	Description	Value
v1	Specifies ERPSv1.	-
v2	Specifies ERPSv2.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ERPS has two versions: ERPSv1 released by the ITU-T in June and ERPSv2 released in August, 2010. ERPSv2 that is compatible with ERPSv1 provides the following enhanced functions:

- Multi-ring topologies, such as intersecting rings
- RAPS PDU transmission on virtual channels (VCs) and non-virtual-channels (NVCs) in sub-rings
- Forced Switch (FS) and Manual Switch (MS)
- Revertive and non-revertive switching

To configure an ERPS version, run the **version** command.

Precautions

Before specifying ERPSv1 for an ERPSv2-enabled device, delete all ERPS configurations that ERPSv1 does not support. Otherwise, the version cannot be changed.

Example

Specify ERPSv2 for ERPS ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] version v2
```

5.15.27 virtual-channel

Function

The **virtual-channel enable** command configures the virtual channel (VC) mode for RAPS PDU transmission in a sub-ring.

The **virtual-channel disable** command configures the non-virtual-channel (NVC) mode for RAPS PDU transmission in a sub-ring.

The **undo virtual-channel enable** command configures the non-virtual-channel (NVC) mode for RAPS PDU transmission in a sub-ring.

By default, RAPS PDUs are transmitted in NVC mode in a sub-ring.

Format

virtual-channel { **enable** | **disable** }

undo virtual-channel enable

Parameters

Parameter	Description	Value
enable	Enables the VC mode for RAPS PDU transmission in a sub-ring.	-
disable	Disables the VC mode for RAPS PDU transmission in a sub-ring. That is, the NVC mode is used.	-

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ERPSv2 supports both single- and multi-ring topologies.

In multi-ring topologies, the VC or NVC mode can be used to transmit RAPS PDUs in a sub-ring:

- VC mode: RAPS PDUs in a sub-ring are transmitted to the major ring by the intersecting node. The RPL owner port of the sub-ring blocks both RAPS PDUs and data traffic.
- NVC mode: RAPS PDUs in a sub-ring are terminated on the intersecting nodes. The RPL owner port of the sub-ring blocks data traffic but not RAPS PDUs.

You can run the **virtual-channel** command to configure the RAPS PDU transmission mode in a sub-ring.

Prerequisites

- The **version v2** command has been executed to specify ERPSv2.
- The **sub-ring** command has been executed to configure an ERPS ring as a sub-ring.

Configuration Impact

If a sub-ring uses the VC mode to transmit RAPS PDUs, you must run the **virtual-channel disable** or **undo virtual-channel enable** command to restore the RAPS PDU transmission mode to NVC before running the **undo sub-ring** command to restore the sub-ring to a major ring.

Example

Configure the VC mode for RAPS PDU transmission in ERPS sub-ring 5.

```
<HUAWEI> system-view
[HUAWEI] erps ring 5
[HUAWEI-erps-ring5] version v2
[HUAWEI-erps-ring5] sub-ring
[HUAWEI-erps-ring5] virtual-channel enable
```

5.15.28 wtr-timer (ERPS ring view)

Function

The **wtr-timer** command sets the WTR timer in an ERPS ring.

The **undo wtr-timer** command restores the default value of the WTR timer.

By default, the WTR timer is 5 minutes in an ERPS ring.

Format

wtr-timer *time-value*

undo wtr-timer

Parameters

Parameter	Description	Value
time-value	Specifies the value of the WTR timer in an ERPS ring.	The value is an integer that ranges from 1 to 12, in minutes.

Views

ERPS ring view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **wtr-timer** command is applied to RPL owner ports. If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. To prevent the RPL owner port from alternating between the Up and Down states, the node where the RPL owner port resides starts the WTR timer after receiving an RAPS PDU indicating the link or node recovery:

- If the node receives an RAPS PDU indicating that another port fails before the timer expires, the node disables the WTR timer and enables the RPL owner port.
- If the node does not receive any RAPS PDUs indicating that another port fails before the timer expires, the node blocks the RPL owner port when the WTR timer expires and sends an RAPS PDU indicating that the RPL owner port is blocked. After receiving the RAPS PDU, other nodes set their recovering ports to the Forwarding state in the ring.

Precautions

If you run the **wtr-timer** command multiple times, only the latest configuration takes effect.

Example

Set the WTR timer to 10 minutes in ERPS ring 10.

```
<HUAWEI> system-view
[HUAWEI] erps ring 10
[HUAWEI-erps-ring10] wtr-timer 10
```

5.16 Loopback Detection Configuration Commands

5.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.16.2 display loopback-detect

Function

The **display loopback-detect** command displays the loopback detection configuration and status of loopback detection enabled interfaces.

Format

display loopback-detect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to check the loopback detection configuration and status of each interface on which loopback detection is enabled.

Example

Display the loopback detection configuration and status of loopback detection enabled interfaces.

```
<HUAWEI> display loopback-detect
Loopback-detect sending-packet interval:  5

(A): Auto Loopback-detect
----------------------------------------------------------------
Interface                   RecoverTime  Action     Status
----------------------------------------------------------------
GigabitEthernet0/0/1           30          quitvlan(A) NORMAL
----------------------------------------------------------------
```

Table 5-106 Description of the display loopback-detect command output

Item	Description
Loopback-detect sending-packet interval	Interval between sending loopback detection packets, in seconds. For details, see **loopback-detect packet-interval**.
Interface	Interface on which loopback detection is enabled.
RecoverTime	Interface recovery time, in seconds. For details, see **loopback-detect recovery-time**.

Item	Description
Action	Action performed when a loopback is detected on an interface: ● block: blocks the interface. After the interface is blocked, it is isolated from other interfaces and does not forward received data packets to other interfaces. ● nolearn: disables MAC address learning on the interface. When a loopback is detected on the interface, the interface stops learning MAC addresses. ● shutdown: shuts down the interface. When a loopback is detected on an interface, the interface is shut down. ● trap: only sends a trap. When a loopback is detected on an interface, the interface only sends a trap. ● trap(A): only sends a trap. (A) indicates that automatic loopback detection is performed on an interface. ● quitvlan: quits VLANs. When a loopback is detected on an interface, the interface exits from the VLAN in which a loop occurs. ● quitvlan(A): quits VLANs. (A) indicates that automatic loopback detection is performed on an interface. To specify the parameter, run the **loopback-detect action or loopback-detect auto action** command.
Status	Status of a loopback detection enabled interface: ● NORMAL: No loopback is detected on the interface. ● BLOCK: A loopback is detected on the interface and the interface is blocked. ● NOLEARN: A loopback is detected on the interface and the MAC address learning is disabled on the interface. ● SHUTDOWN: A loopback is detected on the interface and the interface is shut down. ● TRAP: A loopback is detected on the interface and a trap is sent. ● QUITVLAN: A loopback is detected on the interface and the interface exits from the VLAN in which a loop occurs.

5.16.3 display loopback-detect interface

Function

display loopback-detect interface command displays the LBDT configuration and status of LBDT-enabled interfaces.

Format

display loopback-detect interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to check the loopback detection configuration and status of each interface on which loopback detection is enabled.

Example

Display the LBDT configuration and status of interfaces that are enabled with LBDT manually.

```
<HUAWEI> display loopback-detect interface GigabitEthernet 0/0/1
LBDT mode   : Manual
Detect VLAN : Untag
Looped VLAN :
Action      : shutdown
Status      : NORMAL
Recover Time: 15
```

Display the LBDT configuration and status of interfaces that are enabled with LBDT automatically.

```
<HUAWEI> display loopback-detect interface GigabitEthernet 0/0/1
LBDT mode    : Auto
PVID VLAN    :
  VLAN ID           : 1
  Trap only VLAN ID : -
Mac-flap VLAN:
  Total NUM         : 0
  VLAN ID           : -
```

```
Trap only VLAN NUM: 0
Trap only VLAN ID : -
Quit-vlan VLAN NUM: 0
Quit-vlan VLAN ID : -
```

Table 5-107 Description of the **display loopback-detect interface** command output

Item	Description
LBDT mode	Mode in which LBDT is enabled: - Manual: LBDT is enabled manually. To enable LBDT on an interface, run the **loopback-detect enable (interface view)** command. - Auto: LBDT is enabled automatically. To enable automatic LBDT on the device, run the **undo loopback-detect auto disable** command.
Detect VLAN	VLAN where LBDT is configured to detect loops. To configure a VLAN where LBDT is configured to detect loops, run the **loopback-detect packet vlan** command.
Looped VLAN	VLAN where loops are detected.
Action	Action performed when a loopback is detected on an interface: - block: blocks the interface. After the interface is blocked, it is isolated from other interfaces and does not forward received data packets to other interfaces. - nolearn: disables MAC address learning on the interface. When a loopback is detected on the interface, the interface stops learning MAC addresses. - shutdown: shuts down the interface. When a loopback is detected on an interface, the interface is shut down. - trap: only sends a trap. When a loopback is detected on an interface, the interface only sends a trap. - quitvlan: quits VLANs. When a loopback is detected on an interface, the interface exits from the VLAN in which a loop occurs. To configure an action performed when a loopback is detected, run the **loopback-detect action** command.

Item	Description
Status	Status of a loopback detection enabled interface: - NORMAL: No loopback is detected on the interface. - BLOCK: A loopback is detected on the interface and the interface is blocked. - NOLEARN: A loopback is detected on the interface and the MAC address learning is disabled on the interface. - SHUTDOWN: A loopback is detected on the interface and the interface is shut down. - TRAP: A loopback is detected on the interface and a trap is sent. - QUITVLAN: A loopback is detected on the interface and the interface exits from the VLAN in which a loop occurs.
Recover Time	Restoration time of an interface, in seconds. To configure the restoration time of an interface, run the **loopback-detect recovery-time** command.
PVID VLAN	VLAN that is specified by the PVID and where automatic LBDT is enabled.
VLAN ID	Default VLAN of the interface. To configure the default VLAN of an interface, run the **port default vlan** command.
Trap only VLAN ID	VLAN that is specified by the PVID and where loops are detected. The value is displayed as - if there is no such a VLAN.
Mac-flap VLAN	VLAN where MAC address flapping detection is enabled automatically.
Total NUM	Total number of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping.
VLAN ID	List of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping.
Trap only VLAN NUM	Total number of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **trap**.
Trap only VLAN ID	List of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **trap**.

Item	Description
Quit-vlan VLAN NUM	Total number of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **quit-vlan**.
Quit-vlan VLAN ID	List of VLANs where MAC address flapping detection is enabled automatically to detect MAC address flapping and the action is **quit-vlan**.

5.16.4 loopback-detect action

Function

The **loopback-detect action** command configures an action to be taken when a loopback is detected on an interface.

The **undo loopback-detect action** command restores the default action.

By default, an interface is shut down when a loopback is detected on the interface.

Format

loopback-detect action { **block** | **nolearn** | **shutdown** | **trap** | **quitvlan** }

undo loopback-detect action [**block** | **nolearn** | **shutdown** | **trap** | **quitvlan**] (Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 25GE interface view, 100GE interface view, Eth-Trunk interface view)

undo loopback-detect action (port group view)

Parameters

Parameter	Description	Value
block	Blocks an interface when a loopback is detected.	-
nolearn	Disables MAC address learning on an interface when a loopback is detected on the interface.	-
shutdown	Shuts down an interface when a loopback is detected on the interface.	-

Parameter	Description	Value
trap	Only sends a trap message when a loopback is detected.	-
quitvlan	The interface exits from the VLAN in which a loop occurs when a loopback is detected on an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals. When a loopback is detected on the interface, the system performs an action to minimize the impact on the entire network. The **loopback-detect action** command configures the action.

The system performs any of the following actions after detecting a loopback on an interface:

- **block**: blocks the interface. After the interface is blocked, it is isolated from other interfaces and does not forward received data packets to other interfaces.
- **nolearn**: disables MAC address learning on the interface. When a loopback is detected on the interface, the interface stops learning MAC addresses.
- **shutdown**: shuts down the interface.
- **trap**: only sends a trap.
- **quitvlan**: When a loopback is detected on an interface, the interface exits from the VLAN in which a loop occurs.

Prerequisites

Enable loopback detection in the interface view or system view.

Follow-up Procedure

- If the action is set to **block**, **nolearn**, **trap** or **quitvlan**, you can run the **loopback-detect recovery-time** command to set the interface recovery time.

- If the action is set to **shutdown**, the shutdown interface cannot be automatically restored after a loopback is eliminated. You must run the **shutdown** and **undo shutdown** commands or run the **restart** command to enable the interface again. In addition to the preceding methods, the interface that is manually shut down or enters the Error-Down state due to other protocols will be automatically restored after the recovery time. However, the interface that is disabled only by LBDT cannot be restored after the recovery time.

Example

Configure the system to shut down GigabitEthernet0/0/1 when a loopback occurs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback-detect action shutdown
```

5.16.5 loopback-detect auto action

Function

The **loopback-detect auto action** command specifies an action when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

The **undo loopback-detect auto action** command restores the default action when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

By default, the action is **trap** when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

Format

loopback-detect auto action { **trap** | **quitvlan** }

undo loopback-detect auto action

Parameters

Parameter	Description	Value
trap	Indicates that the interface only sends a trap when loops are detected.	-
quitvlan	Indicates that the interface is removed from the VLAN where MAC address flapping is detected.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

When the switch is configured with MAC address flapping detection and automatic LBDT, if MAC address flapping is detected in a VLAN, automatic LBDT is triggered to detect loops in the VLAN. Then you can run the **loopback-detect auto action** command to configure an action on the interface to minimize the impact of loops on the entire network.

When automatic LBDT is triggered to automatically detect loops in the VLAN where MAC address flapping is detected, you can configure either of the following actions on the interface:

- **trap**: The interface only sends a trap.
- **quitvlan**: The interface is removed from the VLAN where a loop occurs.

Prerequisites

- MAC address flapping detection has been enabled. For details on how to configure MAC address flapping detection, see Configuring MAC Address Flapping Detection.
- Automatic LBDT has been enabled using the **undo loopback-detect auto disable** command.

Follow-up Procedure

Run the **loopback-detect recovery-time** command to configure the recovery time of the problematic interface.

Precautions

The **quitvlan** action that is configured using this command takes effect only in the scenario where automatic LBDT is triggered to detect a loop between interfaces in the VLAN where MAC address flapping is detected. The **trap** action is used in the scenario where automatic LBDT is triggered to detect a loop on the downstream network or device in the VLAN where MAC address flapping is detected.

Example

Configure the **quitvlan** action when automatic LBDT is triggered to detect loops in the VLAN where MAC address flapping is detected.

```
<HUAWEI> system-view
[HUAWEI] mac-address flapping detection
[HUAWEI] undo loopback-detect auto disable
[HUAWEI] loopback-detect auto action quitvlan
```

5.16.6 loopback-detect auto disable

Function

The **loopback-detect auto disable** command disables automatic LBDT.

The **undo loopback-detect auto disable** command enables automatic LBDT.

By default, automatic LBDT is enabled.

Format

loopback-detect auto disable

undo loopback-detect auto disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface changes from Down to Up, a loop may occur. You can enable automatic LBDT. The device then immediately detects loops and reports the corresponding alarm. When the switch is enabled with MAC address flapping detection, if MAC address flapping is detected, LBDT is triggered automatically to detect loops in the VLAN where MAC address flapping occurs.

Precautions

- When the switch is upgraded from an earlier version to V200R009 or later, automatic loop detection is disabled by default.
- The device enabled with automatic LBDT automatically reports an alarm when detecting a loop. After the loop is eliminated, the device automatically reports a clear alarm. The time for reporting a clear alarm is one or two times the recovery time. The recovery time can be configured using the **loopback-detect recovery-time** command. The default value is three detection intervals, that is, 15s.
- When automatic LBDT is enabled, all interfaces where the **loopback-detect enable** command is not configured periodically to send detection packets with the PVID to detect loops, consuming CPU resources. If no loop occurs on a network, run the **loopback-detect auto disable** command to disable automatic LBDT to reduce resource consumption.

Example

Enable automatic LBDT.

```
<HUAWEI> system-view
[HUAWEI] undo loopback-detect auto disable
```

5.16.7 loopback-detect enable (system view)

Function

The **loopback-detect enable** command enables loopback detection on all interfaces.

The **undo loopback-detect enable** command disables loopback detection on all interfaces.

By default, loopback detection is disabled on all interfaces.

Format

loopback-detect enable

undo loopback-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

When loopback detection needs to be enabled on all or most of interfaces on a device, you can use the **loopback-detect enable** command to simplify configuration.

Precautions

After you run the **loopback-detect enable** command in the system view, the CPU usage increases because all interfaces send broadcast loopback detection packets at intervals.

Loopback detection occupies CPU resources; therefore, disable this function when it is not required.

Follow-up Procedure

If loopback detection is not required on an interface, run the **undo loopback-detect enable** command in the interface view to disable loopback detection.

Example

Enable loopback detection on all interfaces.

```
<HUAWEI> system-view
[HUAWEI] loopback-detect enable
```

5.16.8 loopback-detect enable (interface view)

Function

The **loopback-detect enable** command enables loopback detection on an interface.

The **undo loopback-detect enable** command disables loopback detection on an interface.

By default, loopback detection is disabled on an interface.

Format

loopback-detect enable

undo loopback-detect enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, 25GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The **loopback-detect enable** command enables loopback detection on an interface. This function enables the system to detect a loopback on the downstream network quickly and shut down an interface to minimize the impact of the loopback on the entire network.

Precautions

After loopback detection is enabled on an interface, the interface sends loopback detection packets at intervals.

A large number of broadcast packets are sent during loopback detection, occupying CPU resources; therefore, disable loopback detection if it is not required.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, manual LBDT can be configured on a maximum of 64 Eth-Trunks; on other models, manual LBDT can be configured on a maximum of 32 Eth-Trunks.

Example

Enable loopback detection for the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback-detect enable
```

5.16.9 loopback-detect packet vlan

Function

The **loopback-detect packet vlan** command configures loopback detection in a specified VLAN.

The **undo loopback-detect packet vlan** command cancels the configuration.

By default, loopback detection is disabled in a VLAN.

Format

loopback-detect packet vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-8>

undo loopback-detect packet vlan [{ *vlan-id1* [**to** *vlan-id2*] } &<1-8>]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the VLAN IDs of loopback detection packets. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094. ● Each interface can send detection packets with a maximum of 32 VLAN IDs.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, 25GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, loopback detection is disabled in VLANs. After the **loopback-detect packet vlan** command is executed on an interface, the interface sends multiple copies of tagged loopback detection packets with the specified VLAN tags.

Prerequisites

The specified VLANs exist and the interface has been added to the VLANs in tagged mode.

Before running this command, check whether loopback detection is enabled. If not, run the **loopback-detect enable (interface view)** command to enable loopback detection.

Precautions

If you run the **loopback-detect packet vlan** command multiple times in the same interface view, multiple VLAN IDs are specified.

Each interface can send detection packets with a maximum of 32 VLAN IDs.

Example

Configure loopback detection in VLAN30 on the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] vlan 30
[HUAWEI-vlan30] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 30
[HUAWEI-GigabitEthernet0/0/1] loopback-detect enable
[HUAWEI-GigabitEthernet0/0/1] loopback-detect packet vlan 30
```

5.16.10 loopback-detect packet-interval

Function

The **loopback-detect packet-interval** command sets the interval between sending loopback detection packets on all interfaces.

The **undo loopback-detect packet-interval** command restores the default interval between sending loopback detection packets on all interfaces.

By default, the interval between sending loopback detection packets is 5 seconds.

Format

loopback-detect packet-interval *packet-interval-time*

undo loopback-detect packet-interval [*packet-interval-time*]

Parameters

Parameter	Description	Value
packet-interval-time	Specifies the interval between sending loopback detection packets.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

After loopback detection is enabled on an interface, the interface sends loopback detection packets at the interval specified by the **loopback-detect packet-interval** command. You can run the **loopback-detect packet-interval** command to adjust the interval between sending loopback detection packets according to service requirements. If a shorter interval is set, the system sends more loopback detection packets in a certain period. This enables the system to detect loopbacks more quickly and accurately, but more system sources are consumed.

Precautions

If you run the **loopback-detect packet-interval** command multiple times, only the latest configuration takes effect.

After a loopback detection-enabled interface recovers from Down to Up, the interface sends loopback detection packets immediately.

Example

Set the interval between sending loopback detection packets on all interfaces to 10s.

```
<HUAWEI> system-view
[HUAWEI] loopback-detect packet-interval 10
```

5.16.11 loopback-detect recovery-time

Function

The **loopback-detect recovery-time** command sets the interface recovery time after a loopback is detected.

The **undo loopback-detect recovery-time** command restores the interface recovery time after a loopback is detected.

The default recovery time is three times the loopback detection interval.

Format

loopback-detect recovery-time *recovery-time*

undo loopback-detect recovery-time [*recovery-time*] (Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 25GE interface view, 100GE interface view, Eth-Trunk interface view)

undo loopback-detect recovery-time (port group view)

Parameters

Parameter	Description	Value
recovery-time	Interface recovery time.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, 100GE interface view, 25GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

After loopback detection is enabled on an interface, the device sends loopback detection packets at intervals through the interface, performs the preconfigured action on the interface after a loopback is detected, and starts timing. You can configure the interface recovery time. After the configured interface recovery time, the system will attempt to recover the interface. If the loopback is removed on the interface, the system recovers the interface from the error-down state.

Precautions

If you run the **loopback-detect recovery-time** command multiple times, only the latest configuration takes effect.

After a loop is eliminated, the interface recovery time is the same as the value of *recovery-time* or two times the value of *recovery-time*.

It is recommended that the interface recovery time be three times the packet sending interval. If the packet sending interval has been set to a small value, the interface recovery time should be at least 10 seconds longer than the packet sending interval.

If the action is set to **shutdown**, the shutdown interface cannot be automatically restored after a loopback is eliminated. You must run the **shutdown** and **undo shutdown** commands or run the **restart** command to enable the interface again. In addition to the preceding methods, the interface that is manually shut down or enters the Error-Down state due to other protocols will be automatically restored after the recovery time. However, the interface that is disabled only by LBDT cannot be restored after the recovery time.

NOTE

The default recovery time is three times the loopback detection interval and is not restricted by the value ranging from 1 to 1000. If you configure the command manually, the recovery time can only be set to a value from 1 to 1000.

Example

Sets the recovery time of the GE0/0/1 interface to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback-detect recovery-time 50
```

5.16.12 loopback-detect untagged mac-address

Function

The **loopback-detect untagged mac-address** command sets the destination MAC address of untagged loopback detection packets.

The **undo loopback-detect untagged mac-address** command restores the default destination MAC address of untagged loopback detection packets.

By default, the destination MAC address of untagged loopback detection packets is **0180-C200-000A**.

Format

loopback-detect untagged mac-address *mac-address*

undo loopback-detect untagged mac-address [*mac-address*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the destination MAC address of untagged loopback detection packets.	The destination MAC address can only be a broadcast MAC address or a multicast MAC address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **loopback-detect untagged mac-address** command applies to scenarios with self-loops and loops on the downstream network. When the connected interfaces are access interfaces, run the **loopback-detect packet vlan** command to configure the device to detect loops in a specified VLAN. This is because untagged packets are processed only when the transmit interface receives them. If the device is not configured to detect loops in a specified VLAN, run the **loopback-detect untagged mac-address** command.

Prerequisites

Loopback detection has been enabled using the **loopback-detect enable (system view)** command.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

You are not advised to set the destination MAC address of untagged loopback detection packets to a destination MAC address of other protocols but to the broadcast MAC address **FFFF-FFFF-FFFF**.

Example

Set the destination MAC address of untagged loopback detection packets to **FFFF-FFFF-FFFF**.

```
<HUAWEI> system-view
[HUAWEI] loopback-detect enable
[HUAWEI] loopback-detect untagged mac-address ffff-ffff-ffff
```

5.17 Layer 2 Protocol Tunneling Commands

5.17.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

5.17.2 bpdu

Function

The **bpdu** command configures an interface to send received BPDUs to the CPU or discard BPDUs.

By default, an interface sends received BPDUs to the CPU.

Format

bpdu { **disable** | **enable** }

undo bpdu disable

Parameters

Parameter	Description	Value
disable | **enable**	Indicates the action that an interface performs on BPDUs. ● **disable**: The interface discards BPDUs. ● **enable**: The interface sends BPDUs to the CPU.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

After you run the **bpdu enable** command on an interface, the interface forwards a packet to the CPU if the destination MAC address of the packet is the BPDU MAC address. You can use the **display bpdu mac-address** command to view the BPDU MAC address.

NOTE

This command is not supported by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, an interface directly discards BPDUs by default. If BPDUs of a protocol need to be sent to the CPU for processing, enable the function of this protocol. For example, if STP BPDUs need to be sent to the CPU for processing, enable STP globally and on interfaces.

On the S200, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S, an interface directly discards BPDUs except EAPoL packets by default. If BPDUs of a protocol need to be sent to the CPU for processing, enable the function of this protocol. For example, if STP BPDUs need to be sent to the CPU for processing, enable STP globally and on interfaces. EAPoL packets are forwarded by default. To enable a switch to discard EAPoL packets, run the **bpdu packet-type eapol discard** command on the switch.

Example

Enable Eth-Trunk 1 to send received BPDUs to the CPU.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] bpdu enable
```

5.17.3 bpdu dmac

Function

The **bpdu dmac** command configures actions taken on packets with a specified destination MAC address and protocol number.

The **undo bpdu dmac** command restores the default configurations.

By default, no action is taken on packets with a specified destination MAC address and protocol number.

NOTE

S1730S-S1, S200, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Format

bpdu dmac *mac-address* **eth-type** *type* **action encapsulate**

undo bpdu dmac *mac-address* **eth-type** *type* **action** [**encapsulate**]

Parameters

Parameter	Description	Value
dmac *mac-address*	Specifies a destination MAC address.	The value is in H-H-H format. An H contains four hexadecimal digits. The value cannot be 0000-0000-0000.
eth-type *type*	Specifies the protocol type of Ethernet packets.	The value is a hexadecimal integer that ranges from 0 to FFFF.
action	Specifies the action taken on received packets.	-
encapsulate	Encapsulates packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To be compatible with devices of other vendors, run this command to configure actions taken on packets with a specified destination MAC address and protocol number. Actions is encapsulating packets.

Example

Configure the device to forward packets with the destination MAC address 0100-0ccc-cccc and protocol number 0101.

```
<HUAWEI> system-view
[HUAWEI] bpdu dmac 0100-0ccc-cccc eth-type 0101 action encapsulate
```

5.17.4 bpdu mac-address

Function

The **bpdu mac-address** command sets the MAC address of BPDUs.

The **undo bpdu mac-address** command cancels the configuration.

Format

bpdu mac-address *mac-address* [*mac-address-mask*]

undo bpdu mac-address *mac-address* [*mac-address-mask*]

Parameters

Parameter	Description	Value
mac-address [*mac-address-mask*]	Specifies the MAC address and mask of BPDUs.	The first digit of the MAC address must be 0 and the second digit must be an odd number, for example, 03XX-XXXX-XXXX and 0fXX-XXXX-XXXX. The mask of the MAC address must consist of consecutive fs and 0s, for example, ffff-ffff-ff00 and ffff-fff0-0000. **NOTE** ● To enable the device to forward packets destined for 0100-0ccc-cccc by using hardware, run the **undo bpdu mac-address** command to cancel the BPDU MAC address configuration. ● Only addresses of 0100-0ccc-cccc, 0100-0ccc-cccd, and 0118-8255-5555 can be configured as BPDU MAC addresses on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Bridge Protocol Data Unit (BPDU) uses a special reserved multicast MAC address. An interface can send and receive BPDUs regardless of whether the interface is blocked. By default, the switch does not forward BPDUs at Layer 2.

NOTE

Sometimes, bridge protocol packets of the devices from other vendors need to be processed as BPDUs. You can set the MAC address of such packets to the MAC address of BPDUs.

Prerequisites

Before running the **undo bpdu mac-address** *mac-address* [*mac-address-mask*] command to delete a specified BPDU MAC address, delete all BPDU mac-addresses on the network segment. Then, run the **bpdu mac-address mac-address** [*mac-address-mask*] command to add the bpdu mac-address that does not need to be deleted.

Example

Set the MAC address of BPDUs to 0100-0ccc-cccd.

```
<HUAWEI> system-view
[HUAWEI] bpdu mac-address 0100-0ccc-cccd
```

Delete the MAC address 0180-c200-0003 as the BPDU MAC address.

```
<HUAWEI> system-view
[HUAWEI] undo bpdu mac-address 0180-c200-0000 ffff-ffff-fff0
[HUAWEI] bpdu mac-address 0180-c200-0000 FFFF-FFFF-FFFE
[HUAWEI] bpdu mac-address 0180-c200-0002 FFFF-FFFF-FFFF
[HUAWEI] bpdu mac-address 0180-c200-0004 FFFF-FFFF-FFFC
[HUAWEI] bpdu mac-address 0180-c200-0008 FFFF-FFFF-FFF8
```

5.17.5 bpdu packet-type eapol discard

Function

The **bpdu packet-type eapol discard** command configures the switch to discard EAPoL packets.

The **undo bpdu packet-type eapol discard** command configures the switch to transparently transmit EAPoL packets.

By default, the switch transparently transmits EAPoL packets.

NOTE

Only the following switch models support this command:

S200, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

Format

bpdu packet-type eapol discard

undo bpdu packet-type eapol discard

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that the 802.1X authentication point is deployed at the aggregation or upper layer and the access device functions only as a Layer 2 transparent transmission access device. In such networking, to enable the access device to transparently transmit EAPoL packets to the upper-layer authentication point device, run the **undo bpdu packet-type eapol discard** command on the access device. If the access device does not need to transparently transmit EAPoL packets to the upper-layer authentication point device, run the **bpdu packet-type eapol discard** command on the access device.

Precautions

The **l2protocol-tunnel enable** command takes precedence over the **bpdu packet-type eapol discard** command. If the **bpdu packet-type eapol discard** command is run on a device to discard EAPoL packets and then the **l2protocol-tunnel enable** command is run on an interface to enable the interface to transparently transmit Layer 2 protocol packets, this interface can transparently transmit EAPoL packets.

Example

Enable the device to discard EAPoL packets.

```
<HUAWEI> system-view
[HUAWEI] bpdu packet-type eapol discard
```

5.17.6 bpdu-tunnel stp bridge role provider

Function

The **bpdu-tunnel stp bridge role provider** command configures the switch as a provider on the network.

The **undo bpdu-tunnel stp bridge role provider** command configures the switch as a customer on the network.

By default, the switch is a customer on the network.

NOTE

Only the S6720S-S, S5735S-H, S5736-S, S5720I-SI, S5735-S, S5735S-S, and S5735-S-I support this command.

Format

bpdu-tunnel stp bridge role provider

undo bpdu-tunnel stp bridge role provider

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the switch is configured as a customer, the well-known destination MAC address of the transmitted BPDU packets is 01-80-C2-00-00-00.

If the switch is configured as a provider, the well-known destination MAC address of the transmitted BPDU packets is 01-80-C2-00-00-08. The provider directly forwards the BPDU packets created by the customer, instead of sending the packets to the CPU.

If the **bpdu-tunnel stp bridge role provider** and **l2protocol-tunnel** commands are configured simultaneously, the **l2protocol-tunnel** command preferentially takes effect.

Example

Configure the switch as a provider on the network.

```
<HUAWEI> system-view
[HUAWEI] bpdu-tunnel stp bridge role provider
```

5.17.7 display bpdu mac-address

Function

The **display bpdu mac-address** command displays the MAC addresses of BPDUs.

Format

display bpdu mac-address

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A Bridge Protocol Data Unit (BPDU) uses a special reserved multicast MAC address. An interface can send and receive BPDUs regardless of whether the interface is blocked. By default, the switch does not forward BPDUs at Layer 2.

Sometimes, bridge protocol packets of the devices from other vendors need to be processed as BPDUs. You can set the MAC address of such packets to the MAC address of BPDUs.

This command displays the MAC addresses of BPDUs.

Example

Display the MAC addresses of BPDUs.

```
<HUAWEI> display bpdu mac-address
 Remaining configurable number: 126
 ------------------------------------------------------------------------------
 (001) 0100-0ccc-cccc                  (002) 0100-0ccc-cccd
```

Table 5-108 Description of the display bpdu mac-address command output

Item	Description
Remaining configurable number	Number of remaining MAC addresses that you can specify for BPDUs.

5.17.8 display bpdu-tunnel global config

Function

The **display bpdu-tunnel global config** command displays the role of a device on the network and the multicast MAC address of STP BPDUs.

NOTE

Only the S6720S-S, S5735S-H, S5736-S, S5720I-SI, S5735-S, S5735S-S, and S5735-S-I support this command.

Format

display bpdu-tunnel global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the role of a device on the network and the multicast MAC address of STP BPDUs, you can use the **display bpdu-tunnel global config** command.

Example

Display the role of a device on the network and multicast MAC address of STP BPDUs.

```
<HUAWEI> display bpdu-tunnel global config
BridgeRole      customer
GroupMac        0100-5e00-0011
```

Table 5-109 Description of the display bpdu-tunnel global config command output

Item	Description
BridgeRole	Device role on a network. The roles are classified into two types: ● Customer: The well-known destination MAC address of the BPDUs generated by the customer is 01-80-C2-00-00-00. This is the default type. ● Provider: The well-known destination MAC address of the BPDUs generated by the provider is 01-80-C2-00-00-08. To specify the parameter, run the **bpdu-tunnel stp bridge role provider** command.
GroupMac	Multicast MAC address of STP BPDUs. To specify the parameter, run the **l2protocol-tunnel group-mac** command.

5.17.9 display l2protocol-tunnel group-mac

Function

The **display l2protocol-tunnel group-mac** command displays transparent transmission information about all standard Layer 2 protocols or a specified Layer 2 protocol.

Format

display l2protocol-tunnel group-mac { **all** | *protocol-type* | **user-defined-protocol** *protocol-name* }

Parameters

Parameter	Description	Value
all	Displays transparent transmission information about all standard Layer 2 protocols and user-defined Layer 2 protocols.	-

Parameter	Description	Value
protocol-type	Displays transparent transmission information about a specified Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC)

Parameter	Description	Value
user-defined-protocol *protocol-name*	Displays transparent transmission information about a user-defined protocol. *protocol-name* specifies the name of a user-defined protocol.	The name is in the format of character strings. It is case-insensitive without spaces. The value ranges from 1 to 31. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring Layer 2 protocol tunneling, you can run this command to check transparent transmission information about all standard Layer 2 protocols or a specified Layer 2 protocol.

Example

Display transparent transmission information about the STP protocol.

```
<HUAWEI> display l2protocol-tunnel group-mac stp
Protocol  EncapeType  ProtocolType   Protocol-MAC    Group-MAC       Pri
------------------------------------------------------------------------------------------
stp       llc          dsap 0x42    0180-c200-0000   0100-0ccd-cdd0  0
                      ssap 0x42
```

Table 5-110 Description of the display l2protocol-tunnel group-mac command output

Item	Description
Protocol	Name of a Layer 2 protocol whose packets are transparently transmitted.
EncapeType	Encapsulation types of protocols. At present, the encapsulation types of protocol packets can be Ethernet II, SNAP and LLC.
ProtocolType	Type of a Layer 2 protocol whose packets are transparently transmitted.

Item	Description
Protocol-MAC	Multicast destination MAC address of transparently transmitted Layer 2 protocol packets.
Group-MAC	Group MAC address of transparently transmitted Layer 2 protocol packets. It is a multicast MAC address that replaces the original multicast destination MAC address of transparently transmitted Layer 2 protocol packets.
Pri	Priority of transparently transmitted Layer 2 protocol packets.

5.17.10 display l2protocol-tunnel statistics

Function

The **display l2protocol-tunnel statistics** command displays statistics about Layer 2 protocol packets that are transparently transmitted on a specified interface.

Format

display l2protocol-tunnel statistics *interface-type interface-number* [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics about Layer 2 protocol packets that are transparently transmitted on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. When specifying an interface in the command, ensure that Layer 2 protocol tunneling is enabled on the interface.	-

Parameter	Description	Value
protocol-type	Displays statistics about a specified protocol.	The protocol type can be: - Spanning Tree Protocol (STP) - Link Aggregation Control Protocol (LACP) - Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) - Link Layer Discovery Protocol (LLDP) - GARP VLAN Registration Protocol (GVRP) - GARP Multicast Registration Protocol (GMRP) - HUAWEI Group Management Protocol (HGMP) - VLAN Trunking Protocol (VTP) - Unidirectional Link Detection (UDLD) - Port Aggregation Protocol (PAGP) - Cisco Discovery Protocol (CDP) - Per VLAN Spanning Tree Plus (PVST+) - Shared Spanning Tree Protocol (SSTP) - Dynamic Trunking Protocol (DTP) - Device Link Detection Protocol (DLDP) - Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Displays statistics about transparently transmitted packets of a user-defined protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring Layer 2 protocol tunneling, you can run this command to view statistics about transparently transmitted packets of a specified Layer 2 protocol. The command output includes:

- Number of Layer 2 protocol packets received by the inbound interface
- Number of Layer 2 protocol packets sent from the outbound interface
- Number of Layer 2 protocol packets discarded when the threshold is exceeded

According to the output information, you can collect traffic statistics and locate faults on the interface.

When an interface transparently transmits packets of multiple Layer 2 protocols, it is recommended that you specify the optional parameters or a regular expression in the command to filter the output information. Otherwise, too much information will be displayed, causing the following problems:

- The displayed information is repeatedly refreshed, causing desired information unable to be located.
- The system does not respond because of prolonged information traversing and searching.

When using this command, pay attention to the following points:

- If no optional parameter is specified, statistics about all Layer 2 protocol packets transparently transmitted on the specified interface are displayed.
- If *protocol-type* is specified, statistics about packets of the specified Layer 2 protocol that are transparently transmitted on the specified interface are displayed.
- If **user-defined-protocol** is specified, statistics about packets of the specified user-defined Layer 2 protocol that are transparently transmitted on the specified interface are displayed.

Example

Display statistics about transparently transmitted STP and HGMP protocol packets.

```
<HUAWEI> display l2protocol-tunnel statistics GigabitEthernet 0/0/1 stp hgmp
--------------------------------------------------------------------------------
Port              Protocol        Drop       Input      Output     Drop
                               Threshold  Packets    Packets    Packets
--------------------------------------------------------------------------------
GE0/0/1            stp            100       12345      67890      1235
```

Table 5-111 Description of the display l2protocol-tunnel statistics command output

Item	Description
Port	Name of an interface on which Layer 2 protocol tunneling is enabled.
Protocol	Name of a Layer 2 protocol whose packets are transparently transmitted.
Drop Threshold	Drop threshold of transparently transmitted Layer 2 protocol packets. The drop threshold is set by using the **l2protocol-tunnel drop-threshold** command. The unit is packet per second (pps). When the rate of incoming Layer 2 protocol packets on an interface exceeds the threshold, the interface discards excess packets.
Input Packets	Number of incoming Layer 2 protocol packets on the interface enabled with Layer 2 protocol tunneling.
Output Packets	Number of outgoing Layer 2 protocol packets on the interface enabled with Layer 2 protocol tunneling.
Drop Packets	Number of Layer 2 protocol packets discarded on the interface after the traffic rate exceeds the drop threshold.

5.17.11 display l2protocol-tunnel statistics group-mac

Function

The **display l2protocol-tunnel statistics group-mac** command displays statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified destination MAC address (group MAC address) on an interface.

Format

display l2protocol-tunnel statistics group-mac *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface on which the statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address are to be displayed. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring Layer 2 protocol tunneling based on an interface, VLAN, or QinQ on a device, you can run the **display l2protocol-tunnel statistics group-mac** command to check statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on an interface. The command output includes:

- Number of Layer 2 PDUs received by the interface
- Number of Layer 2 PDUs dropped by the interface due to queue resource exhaustion
- Number of Layer 2 PDUs dropped by the interface due to queue execution timeout

The command output helps you locate interface faults.

Example

Display statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on GE 0/0/1.

```
<HUAWEI> display l2protocol-tunnel statistics group-mac GigabitEthernet 0/0/1
------------------------------------------------------------------------------------------
 Port                  Group-Mac          Input           QueueFull          TimeOut
                                        Packets         DropPackets        DropPackets
 -----------------------------------------------------------------------------------------
 GE0/0/1              0100-0ccd-cdd0      8942             0                 8651
                  0100-0ccd-cd2d      232              0                 161
                  0100-0ccd-cd29      242              0                 181
                  0100-0ccd-cd26      228              0                 166
                  0100-0ccd-cd22      277              0                 206
                  0100-0ccd-cd19      254              0                 184
                  0100-0ccd-cd0c      278              0                 203
```

Table 5-112 Description of the **display l2protocol-tunnel statistics group-mac** command output

Item	Description
Port	Interface name
Group-Mac	Multicast MAC address
Input Packets	Number of Layer 2 PDUs received by the interface
QueueFull DropPackets	Number of Layer 2 PDUs dropped by the interface due to queue resource exhaustion
TimeOut DropPackets	Number of Layer 2 PDUs dropped by the interface due to queue execution timeout

5.17.12 l2protocol-tunnel

Function

The **l2protocol-tunnel enable** command enables Layer 2 protocol tunneling on an interface.

The **undo l2protocol-tunnel enable** command disables Layer 2 protocol tunneling on an interface.

The **l2protocol-tunnel disable** command disables Layer 2 protocol tunneling on an interface.

By default, Layer 2 protocol tunneling is disabled on an interface.

Format

l2protocol-tunnel { **all** | { *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name* } **enable**

l2protocol-tunnel { **all** | { *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name* } **disable**

undo l2protocol-tunnel { { *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name* } **enable**

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-

Parameter	Description	Value
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC)

Parameter	Description	Value
		NOTE - You can select one or more preceding protocols. - By default, the packets with the destination MAC address of 0100-0CCC-CCCD are not BPDUs. PVST+ BPDUs are transparently transmitted by default, and other protocol packets are not transparently transmitted by default. - If PVST BPDUs need to be transparently transmitted, use PVST+. SSTP can be used to transparently transmit the packets with the destination MAC address of 0100-CCCC-CCCD, regardless of the packet protocol.
user-defined-protocol *protocol-name*	Enables or disables transparent transmission of packets of a specified user-defined Layer 2 protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocol tunneling is often configured on an interface connecting the PE and CE. After Layer 2 protocol tunneling is enabled, Layer 2 protocol packets received from the user network need to be sent to the CPU and the destination MAC address in the packets needs to be replaced. On the ISP network, Layer 2 protocol packets are directly forwarded.

Generally, the **l2protocol-tunnel** command is run on user-side interfaces of PEs.

Prerequisites

- The **l2protocol-tunnel vlan** command **enable**s an interface to transparently transmit Layer 2 protocol packets from the specified VLANs. The **l2protocol-tunnel** command **enable**s an interface to transparently transmit all Layer 2 protocol packets.
- The **l2protocol-tunnel vlan** and **l2protocol-tunnel** commands cannot specify the same protocol type on the same interface; otherwise, the configurations conflict.
- Before specifying a user-defined protocol in the **l2protocol-tunnel enable** command, run the **l2protocol-tunnel user-defined-protocol** command to define characteristic information about the Layer 2 protocol.
- STP packets have a default group MAC address for replacing the original destination MAC address. For packets of other Layer 2 protocols, you need to configure a global group MAC address to replace the destination MAC address. For details, see **l2protocol-tunnel group-mac**.
- To improve system performance, do not add service-irrelevant interfaces to the VLAN on which Layer 2 protocol tunneling is enabled.
- When an interface is enabled to transparently transmit the packets of a certain protocol, these packets do not participate in protocol processing. For example, after an interface is enabled to transparently transmit STP packets, the interface does not participate in STP calculation. Therefore, you are advised not to enable a protocol and the transparent transmission of this protocol on the same interface.
- You can configure the **l2protocol-tunnel enable** command on Layer 3 main interfaces and sub-interfaces only when the interfaces are on the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H and these interfaces are bound to VSIs.

Example

Configure GE0/0/1 to transparently transmit STP BPDUs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] stp disable
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
```

5.17.13 l2protocol-tunnel drop-threshold

Function

The **l2protocol-tunnel drop-threshold** command sets the drop threshold of Layer 2 protocol packets that are transparently transmitted on an interface.

The **undo l2protocol-tunnel drop-threshold** command cancels the setting of the drop threshold.

By default, the drop threshold of Layer 2 protocol packets that are transparently transmitted on an interface is 0 pps. The rate of Layer 2 protocol packets is not limited on the interface.

Format

l2protocol-tunnel drop-threshold *rate* [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

undo l2protocol-tunnel drop-threshold [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

undo l2protocol-tunnel drop-threshold *rate* { *protocol-type* | **user-defined-protocol** *protocol-name* }

Parameters

Parameter	Description	Value
rate	Specifies the drop threshold of Layer 2 protocol packets that are transparently transmitted on an interface.	The value is an integer that ranges from 1 to 4096, in pps.

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol. The interface discards excess packets of this type of protocol when the rate of these packets exceeds the drop threshold. **NOTE** You can specify multiple protocols in the command.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Sets the drop threshold of packets of a user-defined Layer 2 protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After enabling Layer 2 protocol tunneling on an interface, you can run the **l2protocol-tunnel drop-threshold** command on this interface to set the drop threshold of protocol packets.

After Layer 2 protocol tunneling is enabled and the drop threshold of Layer 2 protocol packets is set on an interface, the interface drops excess Layer 2 protocol packets when the drop threshold is exceeded. If the trap function is enabled, the device sends a trap message to the NMS to notify the network administrator.

When using the **l2protocol-tunnel drop-threshold** command, pay attention to the following points:

- If no Layer 2 protocol is specified, the drop threshold applies to all Layer 2 protocol packets that need to be transparently transmitted.
- If a Layer 2 protocol is specified, the interface discards excess packets of the protocol when the rate of these packets exceeds the drop threshold.
- If you run this command without specifying a protocol, and then run the command with a specified protocol, the drop threshold that you set the second time takes effect.

Example

Set the drop threshold of STP packets that are transparently transmitted on GE0/0/1 to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel stp enable
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel drop-threshold 10 stp
```

5.17.14 l2protocol-tunnel group-mac

Function

The **l2protocol-tunnel group-mac** command enables the switch to replace the multicast destination MAC address of Layer 2 protocol packets with a specified multicast MAC address.

The **undo l2protocol-tunnel** command disables the group MAC function for Layer 2 protocol tunneling. After you run this command, the switch deletes a configured multicast destination MAC address of Layer 2 protocol packets except STP packets that uses the default multicast destination address or restores the default multicast destination MAC address of STP packets.

By default, the multicast destination MAC address of STP packets is replaced by 0100-0ccd-cdd0. For other Layer 2 protocol packets, there is not a default multicast MAC address for replacing their multicast destination MAC addresses.

Format

l2protocol-tunnel *protocol-type* **group-mac** { *group-mac* | **default-group-mac** }

undo l2protocol-tunnel *protocol-type*

Parameters

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC)

Parameter	Description	Value
group-mac	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.
default-group-mac	Specifies the default MAC address of a multicast group, which is 0100-0ccd-cdd0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocols running between user networks, such as MSTP, HGMP, and LACP, must traverse a backbone network to perform Layer 2 protocol calculation.

Generally, the destination MAC addresses in Layer 2 protocol packets of the same Layer 2 protocol are the same. For example, the MSTP PDUs are BPDUs with the destination MAC address 0180-C200-0000. Therefore, when a Layer 2 protocol packet reaches an edge device on a backbone network, the edge device cannot identify whether the Layer 2 protocol packet comes from a user network or the backbone network and sends the Layer 2 protocol packet to the CPU to calculate a spanning tree. As a result, the user network devices calculate a spanning tree with backbone network edge devices but not with user network devices.

To resolve this problem, run the **l2protocol-tunnel group-mac** command on backbone network edge devices to replace the multicast destination MAC addresses in Layer 2 protocol packets with a specified multicast MAC address (group MAC address). This configuration allows Layer 2 protocol packets to be tunneled so that user network devices can calculate a spanning tree.

After this command is run, run the **display l2protocol-tunnel statistics group-mac** command to check statistics about the group-mac packets transparently transmitted by a specified interface.

Precautions

Layer 2 protocols with the same protocol type (For example, the LACP and DLDP protocol types are both 0x8809.) Do not configure the same group-mac. Otherwise, Layer 2 protocol transparent transmission may fail.

When configuring Layer 2 protocol tunneling, do not use the following multicast MAC addresses to replace the destination MAC address of Layer 2 protocol packets:

- Reserved multicast MAC addresses: 0180-C200-0000 to 0180-C200-002F
- Special multicast MAC addresses: 0100-0CCC-CCCC and 0100-0CCC-CCCD
- Destination MAC address of Smart Link packets: 010F-E200-0004
- Multicast MAC addresses that have been used on the network.
- Destination MAC address of VRRP packets: 0100-5E00-0012

NOTE

Do not replace the destination MAC addresses of SSTP, STP, GVRP, and GMRP packets with the same multicast MAC address.

Example

Configure a device to replace the destination MAC address of STP packets with 0100-0100-0100 before tunneling the STP BPDUs.

```
<HUAWEI> system-view
[HUAWEI] l2protocol-tunnel stp group-mac 0100-0100-0100
```

5.17.15 l2protocol-tunnel protocol-type match disable

Function

The **l2protocol-tunnel protocol-type match disable** command disables a device from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type.

The **undo l2protocol-tunnel protocol-type match disable** command cancels the configuration.

By default, a device matches Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type.

Format

l2protocol-tunnel protocol-type match disable

undo l2protocol-tunnel protocol-type match disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To disable a device from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type, run the **l2protocol-tunnel protocol-type match disable** command. After this command is run, the device can transparently transmit Layer 2 protocol packets with more than three tags.

Precautions

After the device is disabled from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type, the device checks only these packets' destination MAC addresses, not their protocol types. Packets with the same destination MAC address but different protocol types are all transparently transmitted. The user-defined Layer 2 protocol type configured using the **l2protocol-tunnel user-defined-protocol** *protocol-name* **protocol-mac** *protocol-mac* **encap-type ethernetii protocol-type** *protocol-type* command does not take effect.

Example

Disable a device from matching Layer 2 protocol tunneling packets to be sent to the CPU against the protocol type.

```
<HUAWEI> system-view
[HUAWEI] l2protocol-tunnel protocol-type match disable
Info: The specified BPDU tunnel configuration of all interface will be updated. Please wait.
```

5.17.16 l2protocol-tunnel user-defined-protocol

Function

The **l2protocol-tunnel user-defined-protocol** command defines characteristic information about a user-defined Layer 2 protocol, including the protocol name, Ethernet encapsulation format, destination MAC address, and MAC address that replaces the destination MAC address of Layer 2 protocol packets.

The **undo l2protocol-tunnel user-defined-protocol** command deletes characteristic information about a user-defined Layer 2 protocol.

By default, no characteristic information about a user-defined Layer 2 protocol exists on the device.

Format

l2protocol-tunnel user-defined-protocol *protocol-name* **protocol-mac** *protocol-mac* [**encap-type** { { **ethernetii** | **snap** } **protocol-type** *protocol-type-value* | **llc dsap** *dsap-value* **ssap** *ssap-value* }] **group-mac** { *group-mac* | **default-group-mac** }

undo l2protocol-tunnel user-defined-protocol *protocol-name*

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a user-defined Layer 2 protocol.	The value is a string of 1 to 31 characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
protocol-mac *protocol-mac*	Specifies the multicast destination MAC address of the user-defined protocol packets.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits.
encap-type	Indicates the encapsulation format of transparently transmitted Layer 2 protocol packets. ● **ethernetii**: indicates Ethernet_II, the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **snap**: indicates Sub-Network Access Protocol (SNAP), the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **llc**: indicates Logical Link Control (LLC), the encapsulation format for Layer 2 protocol packets that are transparently transmitted.	-
dsap *dsap-value*	Specifies the destination service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.
ssap *ssap-value*	Specifies the source service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.

Parameter	Description	Value
protocol-type *protocol-type-value*	Indicates the Ethernet encapsulation format.	The value is a hexadecimal integer. ● The value ranges from 600 to FFFF for Ethernet II encapsulation type. ● The value ranges from 0 to FFFF for SNAP encapsulation type.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.
default-group-mac	Replaces the destination MAC address of Layer 2 protocol packets with the default multicast MAC address 0100-0ccd-cdd0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When Layer 2 protocol packets with a specified multicast destination MAC address need to be transparently transmitted on an ISP network, you can define characteristic information about the Layer 2 protocol on devices on the ISP network.

When configuring Layer 2 protocol tunneling, do not use the following multicast MAC addresses to replace the destination MAC address of Layer 2 protocol packets:

- Reserved multicast MAC addresses: 0180-C200-0000 to 0180-C200-002F
- Special multicast MAC addresses: 0100-0CCC-CCCC and 0100-0CCC-CCCD
- Destination MAC address of Smart Link packets: 010F-E200-0004
- Common multicast MAC addresses that have been used on the device

Before running the **l2protocol-tunnel** or **l2protocol-tunnel vlan** command to enable transparent transmission of user-defined Layer 2 protocol packets, run the **l2protocol-tunnel user-defined-protocol** command to define characteristic information about the Layer 2 protocol.

Example

Define a Layer 2 protocol named **huawei**. Set the destination MAC address of its packets to 0180-c200-0022 and use multicast MAC address 0100-0100-0100 to replace the destination MAC address of its packets.

```
<HUAWEI> system-view
[HUAWEI] l2protocol-tunnel user-defined-protocol huawei protocol-mac 0180-c200-0022 group-mac
0100-0100-0100
```

5.17.17 l2protocol-tunnel vlan

Function

The **l2protocol-tunnel vlan** command enables VLAN-based Layer 2 protocol tunneling on an interface.

The **undo l2protocol-tunnel vlan** command disables VLAN-based Layer 2 protocol tunneling on an interface.

By default, VLAN-based Layer 2 protocol tunneling is disabled on an interface.

Format

l2protocol-tunnel { **all** | { *protocol-type* } &<1-15> | **user-defined-protocol** *protocol-name* } **vlan** { *low-id* [**to** *high-id*] } &<1-10>

undo l2protocol-tunnel { **all** | { *protocol-type* } &<1-15> | **user-defined-protocol** *protocol-name* } **vlan** { *low-id* [**to** *high-id*] } &<1-10>

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-

Parameter	Description	Value
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol.	The protocol type can be: ● Spanning Tree Protocol (STP) ● Link Aggregation Control Protocol (LACP) ● Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) ● Link Layer Discovery Protocol (LLDP) ● GARP VLAN Registration Protocol (GVRP) ● GARP Multicast Registration Protocol (GMRP) ● HUAWEI Group Management Protocol (HGMP) ● VLAN Trunking Protocol (VTP) ● Unidirectional Link Detection (UDLD) ● Port Aggregation Protocol (PAGP) ● Cisco Discovery Protocol (CDP) ● Per VLAN Spanning Tree Plus (PVST+) ● Shared Spanning Tree Protocol (SSTP) ● Dynamic Trunking Protocol (DTP) ● Device Link Detection Protocol (DLDP) ● Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Enables or disables transparent transmission of packets of a user-defined Layer 2 protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
low-id	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be smaller than the end VLAN ID.
high-id	Specifies the end VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be greater than the start VLAN ID.

Views

Ethernet interface view, GE interface view, XGE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, port group view, 25GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

After a user-side interface of a PE on an ISP network is enabled to transparently transmit Layer 2 protocol packets, the interface directly forwards Layer 2 protocol packets sent from a user network instead of sending the packets to the CPU. In this way, Layer 2 protocol packets are transparently transmitted through the ISP network.

The **l2protocol-tunnel vlan** command is usually used on user-side interfaces of PEs.

The **l2protocol-tunnel vlan** command enables an interface to transparently transmit Layer 2 protocol packets from the specified VLANs. The **l2protocol-tunnel** command enables an interface to transparently transmit all Layer 2 protocol packets.

The **l2protocol-tunnel vlan** and **l2protocol-tunnel** commands cannot specify the same protocol type on the same interface. Otherwise, the configurations conflict.

Before specifying a user-defined protocol in the **l2protocol-tunnel vlan** command, run the **l2protocol-tunnel user-defined-protocol** command to define characteristic information about the Layer 2 protocol.

STP packets have a default MAC address for replacing the original destination MAC address. For packets of other Layer 2 protocols, you need to configure a global group MAC address to replace the destination MAC address. For details, see **l2protocol-tunnel group-mac**.

In addition, the VLAN specified in the command must be the static VLAN, but not the VLAN dynamically created by GVRP or VCMP.

If the **l2protocol-tunnel vlan** command is run more than once, all configurations take effect.

Example

Enable GE0/0/1 to transparently transmit LACP packets with VLAN tags ranging from 100 to 200.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100 to 200
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 200
[HUAWEI-GigabitEthernet0/0/1] l2protocol-tunnel lacp vlan 100 to 200
```

5.17.18 reset l2protocol-tunnel statistics

Function

The **reset l2protocol-tunnel statistics** command clears statistics about Layer 2 protocol packets that are transparently transmitted on an interface.

Format

reset l2protocol-tunnel statistics *interface-type interface-number* [{ *protocol-type* } &<1-16> | **user-defined-protocol** *protocol-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Clears statistics about Layer 2 protocol packets that are transparently transmitted on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. The specified interface must be enabled with Layer 2 protocol tunneling.	-

Parameter	Description	Value
protocol-type	Clears statistics about transparently transmitted packets of a specified protocol.	The protocol type can be: • Spanning Tree Protocol (STP) • Link Aggregation Control Protocol (LACP) • Ethernet Operation, Administration, and Maintenance 802.3ah (EOAM3ah) • Link Layer Discovery Protocol (LLDP) • GARP VLAN Registration Protocol (GVRP) • GARP Multicast Registration Protocol (GMRP) • HUAWEI Group Management Protocol (HGMP) • VLAN Trunking Protocol (VTP) • Unidirectional Link Detection (UDLD) • Port Aggregation Protocol (PAGP) • Cisco Discovery Protocol (CDP) • Per VLAN Spanning Tree Plus (PVST+) • Shared Spanning Tree Protocol (SSTP) • Dynamic Trunking Protocol (DTP) • Device Link Detection Protocol (DLDP) • Ethernet Synchronization Message Channel (ESMC) You can select one or more Layer 2 protocols.

Parameter	Description	Value
user-defined-protocol *protocol-name*	Clears statistics about transparently transmitted packets of a user-defined protocol. *protocol-name* specifies the name of a user-defined protocol.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect statistics about Layer 2 protocol packets transparently transmitted on an interface in a specified period, you must reset original statistics on the interface.

When using the **reset l2protocol-tunnel statistics** command, pay attention to the following points:

- If you specify an interface but do not specify any protocol, statistics about all Layer 2 protocol packets on the interface are reset.
- If you specify an interface and a protocol, statistics about packets of the specified protocol are reset.

NOTE

Statistics about Layer 2 protocol packets cannot be restored after being deleted. Confirm your action before you use this command.

Example

Reset statistics about all Layer 2 protocol packets on GE0/0/1.

```
<HUAWEI> reset l2protocol-tunnel statistics gigabitethernet 0/0/1
```

Reset statistics about STP packets on GE0/0/2.

```
<HUAWEI> reset l2protocol-tunnel statistics gigabitethernet 0/0/2 stp
```

5.17.19 reset l2protocol-tunnel statistics group-mac

Function

The **reset l2protocol-tunnel statistics group-mac** command clears statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with destination MAC addresses (group MAC address) on an interface.

Format

reset l2protocol-tunnel statistics group-mac [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface on which the statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address are to be cleared. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After Layer 2 protocol tunneling is configured on a device, if you need to collect statistics within a specified period about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on an interface, first run the **reset l2protocol-tunnel statistics group-mac** command to clear existing statistics on the interface, and then enable the interface to collect statistics within that period.

Example

Clear statistics about transparently transmitted Layer 2 PDUs whose multicast destination MAC addresses are replaced with a specified group MAC address on GE 0/0/1.

```
<HUAWEI> reset l2protocol-tunnel statistics group-mac Gigabitethernet 0/0/1
```

5.17.20 stp bpdu vlan

Function

The **stp bpdu vlan** command configures the STP packets sent from an interface to contain the specified VLAN ID.

The **undo stp bpdu vlan** command cancels the configuration.

By default, the STP packets sent from an interface do not contain VLAN IDs.

Format

stp bpdu vlan *vlan-id*

undo stp bpdu vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID contained in the STP packets sent from an interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 100GE interface view, 40GE interface view, MultiGE interface view, port group view, 25GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When multiple user networks connect to the interfaces of the same PE, the PE interface needs to distinguish STP packets from different user networks. In this case, you need to configure the STP packets sent from each CE interface to contain the specified VLAN ID. In addition, the STP packets sent to the CE interface must also contain the specified VLAN ID.

On the CE interface, run the **stp bpdu vlan** *vlan-id* command to configure the STP packets sent to the PE to contain the specified VLAN ID. On the PE interface connected to the CE, run the **l2protocol-tunnel vlan** command to enable the STP packets with the specified VLAN ID to traverse the ISP network.

Before running the **stp bpdu vlan** command on a CE interface, ensure that the CE interface has been added to the specified VLAN.

The **stp bpdu vlan** command is usually configured on the network interface of the CE.

Example

Configure the STP packets sent from GE0/0/1 to contain VLAN ID 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
```

```
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] stp bpdu vlan 100
```

5.17.21 stp snooping enable

Function

The **stp snooping enable** command enables STP snooping.

The **undo stp snooping enable** command disables STP snooping.

By default, STP snooping is disabled on interfaces.

Format

stp snooping enable

undo stp snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **l2protocol-tunnel** command to enable transparent transmission of Layer 2 protocol packets on untagged interfaces or the **l2protocol-tunnel vlan** command to enable transparent transmission of Layer 2 protocol packets on tagged interfaces, the untagged or tagged interfaces directly forward Layer 2 protocol packets sent from user networks over the ISP network but not send them to the CPU for processing. When a device enabled with Layer 2 protocol tunneling receives TC packets, the device clears the MAC entries and ARP entries and updates the forwarding table after the **stp snooping enable** command is executed.

Example

Enable STP snooping.

```
<HUAWEI> system-view
[HUAWEI] stp snooping enable
```

6 IP Service Commands

6.1 IPv4 Configuration Commands

6.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

6.1.2 ip address

Function

The **ip address** command configures an IP address for an interface.

The **undo ip address** command deletes an IP address from an interface.

By default, the IP address 192.168.1.253 255.255.255.0 is configured on VLANIF1 of the S1720GW-E and S1720GWR-E. On other switches, no IP address is configured for an interface.

Format

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an interface.	The value is in dotted decimal notation.
mask	Specifies a subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
sub	Configures a secondary IP address for an interface. This parameter is optional. To implement communication between multiple subnets of an interface, configure secondary IP addresses for the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip address** command configures IP addresses for interfaces on the switch so that the switch can communicate with different network segments. To connect an interface to multiple network segments, configure multiple IP addresses for the interface. Among these IP addresses, one is the primary IP address and the others are secondary IP addresses. If you configure a new primary IP address for the interface, the new IP address overrides the original one.

The following conditions are prohibited for different interfaces on the same switch:

- The IP addresses are the same.
- The broadcast addresses (with the host number field containing all 1s in the binary mode) corresponding to the IP addresses are the same. For example, if the IP address of interface A is 10.1.1.1/16 and its corresponding broadcast address is 10.1.255.255 and the IP address of interface B is 10.1.1.2/24 and its corresponding broadcast address is 10.1.1.255, the configuration is successful. However, if the IP address of interface B is also 10.1.1.2/16 and its corresponding broadcast address is also 10.1.255.255, the configuration fails.
- The IP address of an interface is the same as the broadcast address of another interface. For example, if the IP address of interface A is 10.1.2.1/28 and its broadcast address is 10.1.2.15 and the IP address of interface B is 10.1.2.15/26, the configuration fails.

When you run the **undo ip address** command:

- The **undo ip address** command deletes all IP addresses from an interface.
- The **undo ip address** *ip-address* { *mask* | *mask-length* } command deletes the primary IP address of an interface.
- The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command deletes a secondary IP address.

Precautions

You can configure a secondary IP address only after configuring a primary IP address on the interface. You must delete all secondary IP addresses before deleting the primary IP address.

You can configure multiple IP addresses for a Layer 3 interface on the switch, one as the primary IP address, and the others as secondary IP addresses. Each Layer 3 interface can have a maximum of 31 secondary IP addresses.

The subnet IP address cannot be used as the IP address on an interface.

On the S1720GW-E and S1720GWR-E, if no IP address is configured, VLANIF1 uses the IP address 192.168.1.253 255.255.255.0 by default. After VLANIF1 obtains an IP address through DHCP successfully, the IP address 192.168.1.253 255.255.255.0 is deleted.

NOTE

- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Layer 2 Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Layer 3 Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Example

Configure a primary IP address 10.1.0.1 and a secondary IP address 10.2.0.1 for VLANIF10, with subnet mask 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.0.1 255.255.255.0
[HUAWEI-Vlanif10] ip address 10.2.0.1 255.255.255.0 sub
```

Configure a primary IP address 10.1.0.1 and a secondary IP address 10.2.0.1 for GE0/0/1, with subnet mask 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.0.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] ip address 10.2.0.1 255.255.255.0 sub
```

6.1.3 ip address unnumbered

Function

The **ip address unnumbered** command configures IP unnumbered on an interface so that the interface can borrow the IP address from another interface.

The **undo ip address unnumbered** command cancels the IP unnumbered configuration on an interface.

By default, an interface does not borrow the IP address from another interface.

Format

ip address unnumbered interface *interface-type interface-number* [**all-address**]

undo ip address unnumbered

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the numbered interface from which the IP address will be borrowed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
all-address	Enables an interface to borrow all IP addresses of another interface. This parameter can be configured only in the VLANIF interface view.	-

Views

GE interface view, GE sub-interface view, XGE interface view, XGE sub-interface view, 25GE interface view, 25GE sub-interface view, 40GE interface view, 40GE sub-interface view, 100GE interface view, 100GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, VLANIF interface view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

An IP unnumbered interface can be a VLANIF interface , an Ethernet interface, an Ethernet sub-interface, or a Tunnel interface.

- An Ethernet interface and an Ethernet sub-interface can only borrow the IP address of a loopback interface. If one end is configured with IP address unnumbered and the other end is configured with an IP address in non-borrow mode, inter-network segment ARP learning must be enabled on both ends.
- A VLANIF interface can only borrow the IP address of a loopback interface. You can set **all-address** to configure a VLANIF interface to borrow all the IP addresses of a loopback interface.
- A Tunnel interface can borrow the IP address of an Ethernet interface, a loopback interface, an Eth-Trunk interface, a VLANIF interface, or a Tunnel interface.

The interface from which the IP address is borrowed must be a Layer 3 interface.

If the interface assigned to an IP unnumbered interface has no IP address, the IP unnumbered interface obtains the IP address 0.0.0.0.

The **ip address unnumbered** command only configures an interface to borrow the IP address from another interface. Other attributes of the interface that borrows an IP address, such as the enablement of routing protocols, need to be configured separately.

Example

Configure Tunnel1 to borrow the IP address from LoopBack0.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] ip address unnumbered interface loopback 0
```

Configure VLANIF 10 to borrow the IP address from LoopBack1.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address unnumbered interface loopback 1
```

6.1.4 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-

Parameter	Description	Value
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Display IP information about VLANIF15.

```
<HUAWEI> display ip interface vlanif 15
Vlanif15 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 766390, bytes : 41540847, multicasts : 681817
```

```
output packets : 242239, bytes : 14679482, multicasts : 172333
Directed-broadcast packets:
 received packets:            0, sent packets:            0
 forwarded packets:           0, dropped packets:          0
Internet Address is 10.1.1.119/24
Broadcast address : 10.1.1.255
TTL being 1 packet number:    164035
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
```

Table 6-1 Description of the **display ip interface** command output

Item	Description
Vlanif15 current state	Physical status of the interface: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the administrator has run the **shutdown (interface view)** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: The link layer protocol of the interface is running properly. ● DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface or a serial interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 766390, bytes : 41540847, multicasts : 681817	Total number of packets, bytes, and multicast packets received by the interface.

Item	Description
output packets : 242239, bytes : 14679482, multicasts : 172333	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
Internet Address is	IP address assigned to the interface and mask length.
Broadcast address	Broadcast address of the interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

Display brief IP information about VLANIF15.

```
<HUAWEI> display ip interface brief vlanif 15
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                         IP Address/Mask      Physical   Protocol
Vlanif15                          10.1.1.119/24        up         up
```

Table 6-2 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down	^down: indicates that the interface is a backup interface.
(l): loopback	The letter "l" refers to loopback.
(s): spoofing	The letter "s" refers to spoofing.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
Interface	Interface type and number.
IP Address/Mask	IP address and mask of an interface.
Physical	Physical status of an interface: ● Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. ● Down: indicates that the interface becomes faulty. ● *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. ● !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.

Item	Description
Protocol	Link protocol status of the interface: - Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. - Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

6.2 ARP Configuration Commands

6.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

6.2.2 arp auto-scan enable

Function

The **arp auto-scan enable** command enables automatic ARP scanning on a sub-interface.

The **undo arp auto-scan enable** command disables automatic ARP scanning on a sub-interface.

By default, automatic ARP scanning is disabled on a sub-interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp auto-scan enable

undo arp auto-scan enable

Parameters

None

Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After automatic ARP scanning is enabled on a sub-interface of which the IP address mask is greater than or equal to 24 bits and the protocol status is Up, the switch scans IP addresses on the network segment where the sub-interface's primary IP address belongs and learns ARP entries of the remote device immediately.

Precautions

Automatic ARP scanning can be enabled on a maximum of 512 sub-interfaces of a switch simultaneously. If automatic ARP scanning is enabled on multiple interfaces simultaneously and the protocol status of the sub-interfaces are Up, the switch sends detection packets to the sub-interfaces, causing a high CPU usage.

To prevent the delay of the interface Up event caused by loop detection, the switch enabled with automatic ARP scanning sends detection packets after a delay of 10s.

When both the interface and protocol status are Up, automatic ARP scanning is performed only once, instead of being performed periodically.

Example

Enable automatic ARP scanning.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.10
[HUAWEI-GigabitEthernet0/0/1.10] arp auto-scan enable
```

6.2.3 arp broadcast disable (VLANIF interface view)

Function

The **arp broadcast disable** command disables a VLANIF interface from broadcasting ARP packets.

The **undo arp broadcast disable** command enables a VLANIF interface to broadcast ARP packets.

By default, VLANIF interfaces are enabled to broadcast ARP packets.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp broadcast disable

undo arp broadcast disable

Parameters

None

Views

VLANIF interface view

Default Level

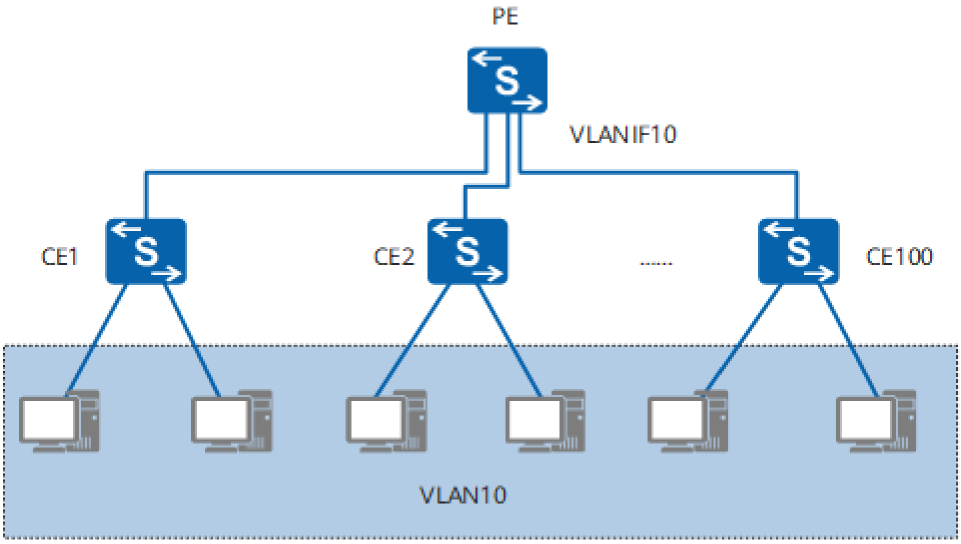
2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VLANIF interface broadcasts ARP packets in a VLAN. For example, on the large Layer 2 aggregation network shown in **Figure 6-1**, user hosts connect to CE1 through CE100 to access the aggregation device PE that has VLANIF10 configured as the user gateway. As VLANIF10 by default broadcasts ARP packets, these ARP packets are flooded on the user network, consuming a large number of network resources, which affects services and gateway performance.

Figure 6-1 Layer 2 aggregation network



To ensure user services and aggregation gateway performance, run the **arp broadcast disable** command to disable the aggregation gateway's VLANIF interface from broadcasting ARP packets.

Precautions

Exercise caution when disabling a VLANIF interface from broadcasting ARP packets because this affects the following scenarios in the following ways:

- Proxy ARP scenarios, including intra-VLAN proxy ARP and inter-VLAN proxy ARP

  After a VLANIF interface is disabled from broadcasting ARP packets, the proxy does not forward ARP Request messages from a host to their destinations even if all proxy conditions are met. As a result, proxy ARP fails.

- Scenarios in which hosts send unicast packets

  For example, in ping operations, ICMP Echo Request messages must be encapsulated with MAC addresses mapped to the destination IP addresses. If the host does not have ARP entries, it must send ARP Request messages to learn the MAC address mapped to the destination IP address. However, the VLANIF interface is disabled from broadcasting ARP packets, and therefore cannot send ARP Request messages. Subsequently, the host cannot obtain the MAC address mapped to the destination IP address, causing a ping operation failure. This problem also occurs in other scenarios in which hosts send unicast packets.

- Strict ARP learning scenarios

  In a strict ARP learning scenario, a device learns MAC addresses only of ARP Reply messages in response to ARP Request messages that it sends. If the VLANIF interface is disabled from broadcasting ARP packets, it cannot actively send ARP Request messages. As a result, strict ARP learning fails.

- VLAN aggregation scenarios

  If the VLANIF interface is disabled from broadcasting ARP packets, the super VLAN will not broadcast ARP packets to all its sub-VLANs.

After a VLANIF interface is disabled from broadcasting ARP packets, gratuitous ARP packets will still be sent normally.

Switching between enabling and disabling the ARP broadcasting function on a VLANIF interface will cause the direct routes to flap temporarily.

Example

Disable VLANIF 10 from broadcasting ARP packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp broadcast disable
Warning: This operation will cause the device to fail to send ARP broadcast packets, continue?[Y/N]:y
```

6.2.4 arp detect-mode unicast

Function

The **arp detect-mode unicast** command configures an interface to send ARP aging probe packets in unicast mode.

The **undo arp detect-mode unicast** command restores the default ARP aging probe mode on an interface.

By default, an interface broadcasts only the last ARP aging probe packet, and unicasts other ARP aging probe packets.

Format

arp detect-mode unicast

undo arp detect-mode unicast

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the aging time of a dynamic ARP entry on an interface expires, the switch sends an aging probe packet (ARP Request packet, and the detection interval is 5 seconds.) from the interface. If the switch receives an ARP Reply packet, it updates this dynamic ARP entry and the aging probe ends. If the switch does not receive an ARP Reply packet after the configured aging probe attempts, it deletes the dynamic ARP entry and the aging probe ends. The aging probe packet can be a unicast or broadcast packet.

If a non-Huawei device receives an ARP aging probe packet with the destination MAC address as the broadcast address from a switch, but the ARP entry of the switch already exists in its ARP table, the non-Huawei device discards the ARP aging probe packet. Failing to receive an ARP Reply to the ARP aging probe packet, the switch deletes the corresponding ARP entry. As a result, the traffic from the network side is interrupted. To resolve this problem, the switch must be configured to send ARP aging probe packets in unicast mode, and the non-Huawei device must be configured to respond to unicast ARP aging probe packets.

Precautions

If the IP address of the peer device remains the same but the MAC address changes frequently, configuring an interface to send ARP aging probe packets in broadcast mode is recommended.

If the MAC address of the peer device remains the same, the network bandwidth is insufficient, and the aging time of ARP entries is set to a small value, configuring an interface to send ARP aging probe packets in unicast mode is recommended.

Example

Configure the interface VLANIF 100 to unicast ARP aging probe packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp detect-mode unicast
```

6.2.5 arp detect-times

Function

The **arp detect-times** command sets the number of aging probes for dynamic ARP entries.

The **undo arp detect-times** command restores the default number of aging probes for dynamic ARP entries.

The default number of aging probes for dynamic ARP entries is 3.

Format

arp detect-times *detect-times*

undo arp detect-times

Parameters

Parameter	Description	Value
detect-times	Specifies the number of aging probes for dynamic ARP entries.	The value is an integer that ranges from 0 to 10. The default value is 3.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In case that the mapping relationship between the IP address and the MAC address of the peer device exists in the ARP table of the local device, the local device will directly send data packets rather than ARP request packets to the peer device because the MAC address of the peer device exists in the ARP entry of the local device. If the peer device fails to work but the local device is not informed of the fault or change, the local device will send data packets to its original destination MAC address. This causes the traffic to be interrupted.

Therefore, to enhance the communication reliability, run the **arp detect-times** command to set the aging probe times of a dynamic ARP entry to update the dynamic ARP entry.

After the aging time of a dynamic ARP entry on an interface expires, the switch sends an aging probe packet (ARP Request packet, and the detection interval is 5 seconds.) from the interface. If the switch receives an ARP Reply packet, it updates this dynamic ARP entry and the aging probe ends. If the switch does not receive an ARP Reply packet after the configured aging probe attempts, it deletes the dynamic ARP entry and the aging probe ends.

Precautions

- If the number of aging probes is set to 0, the device directly deletes expired dynamic ARP entries.
- In VM migration scenarios with distributed gateways, you are advised to set the number of aging probes to 0 to reduce packet loss.
- The **arp detect-times** command can be configured globally or on the specified interface. If the command is not configured on the interface, the aging detection times of a dynamic ARP entry will be the one configured globally. If the command is both configured globally and on the specified interface, the aging detection times of a dynamic ARP entry will be the one configured on the interface.

Example

Set the number of aging probes for dynamic ARP entries on VLANIF 100 to 5.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp detect-times 5
```

6.2.6 arp direct-route enable

Function

The **arp direct-route enable** command enables the ARP module to send ARP Vlink direct routes to the route management (RM) module.

The **undo arp direct-route enable** command disables the ARP module from sending ARP Vlink direct routes to the RM module.

By default, the ARP module is disabled from sending ARP Vlink direct routes to the RM module.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp direct-route enable

undo arp direct-route enable

Parameters

None

Views

VLANIF interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, Eth-Trunk sub-interface view, 100GE sub-interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ARP Vlink direct routes are 32-bit host routes that are generated based on ARP entries statically configured or dynamically learned.

In most cases, ARP Vlink direct routes are only used to guide local forwarding. To control the scale and maintain the stability of the routing table, the ARP module does not send ARP Vlink direct routes to the RM module.

In some scenarios, however, the device needs to perform operations based on specific routes of users. For example, the device needs to directly send the network traffic to specific user terminals, or route filtering is used to restrict inter-device communication.

In these scenarios, run the **arp direct-route enable** command to enable the ARP module to send ARP Vlink direct routes to the RM module. This configuration allows the device to select ARP Vlink direct routes based on longest match first to guide traffic forwarding, and accordingly accurately control downstream traffic, which improves the forwarding efficiency.

Follow-up Procedure

If you want the device to advertise ARP Vlink direct routes to upstream devices after you enable the ARP module to send ARP Vlink direct routes to the RM module, perform the following operations in sequence:

1. Run the **arp vlink-direct-route advertise** command to configure the device to advertise ARP Vlink direct routes.
2. Configure the device to import the ARP Vlink direct routes to the routing tables of the routing protocols running on the device for the ARP Vlink direct routes to be advertised.

Precautions

Currently, the ARP module can only send ARP Vlink direct routes of sub-interfaces and VLANIF interfaces to the RM module.

Example

Enable the ARP module to send ARP Vlink direct routes to the RM module.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] arp direct-route enable
```

6.2.7 arp expire-time

Function

The **arp expire-time** command sets the aging time of dynamic ARP entries.

The **undo arp expire-time** command restores the default aging time of dynamic ARP entries.

By default, the aging time of dynamic ARP entries is 1200 seconds, that is, 20 minutes.

Format

arp expire-time *expire-time*

undo arp expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of dynamic ARP entries.	The value is an integer that ranges from 30 to 62640, in seconds. The default value is 1200 seconds, that is, 20 minutes.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure communication reliability, you need to update ARP entries when they are invalid. A dynamic ARP entry has a life cycle. If a dynamic ARP entry is not updated before its life cycle ends, this dynamic ARP entry will be deleted from the ARP table. The life cycle is called aging time. If the entry is updated before its life cycle expires, the aging time of the entry is recalculated.

You can run the **arp expire-time** command to configure the aging time of dynamic ARP entries, ensuring that dynamic ARP entries are updated in time.

After the aging time of a dynamic ARP entry on an interface expires, the switch sends an aging probe packet (ARP Request packet, and the detection interval is 5 seconds.) from the interface. If the switch receives an ARP Reply packet, it updates this dynamic ARP entry and the aging probe ends. If the switch does not receive an ARP Reply packet after the configured aging probe attempts, it deletes the dynamic ARP entry and the aging probe ends.

Precautions

- If the aging time set for a dynamic ARP entry is short, the refreshment for the ARP entry will consume huge number of system resources, causing adverse impacts on other services, a network flapping and even traffic forwarding.
- If the aging time set for a dynamic ARP entry is long, the ARP entry will not be promptly updated when it is invalid. For example, if a device fails to work or a network card is changed but the invalid ARP entry has not updated yet, the device sends packets to the peer device based on the existing ARP entry. As a result, the service will be interrupted.

To ensure system stability, use the default value of 20 minutes for a dynamic ARP entry.

If a new aging time is set on an interface that has already learned ARP entries, the new aging time will not take effect on the ARP entries that have been learned, but will take effect on the ARP entries to be learned.

After proxy ARP is enabled on the device, the aging time of ARP entries on user hosts connected to the device should be shortened so that invalid ARP entries on the hosts can be deleted as soon as possible. This decreases packet forwarding failures on the device.

You can adjust the aging parameters of dynamic ARP entries in both the system view and interface view.

- If you configure the parameters only in the system view, the configuration takes effect for the dynamic ARP entries learned on all interfaces of the device.
- If you configure the parameters in both the system and interface views, the configuration in the interface view takes effect only for the dynamic ARP entries learned on the interface specified.
- You cannot adjust the aging parameters of dynamic ARP entries on sub-interfaces. If you configure the parameters on the master interface, the configuration takes effect for the dynamic ARP entries learned on the sub-interfaces. If you do not configure the parameters on the master interface, the configuration in the system view takes effect for the dynamic ARP entries learned on the sub-interfaces.

Example

Set the aging time of dynamic ARP entries to 600 seconds on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp expire-time 600
```

6.2.8 arp fixup

Function

The **arp fixup** command configures fixed ARP and converts the dynamic ARP entries learned by the device into static ARP entries.

Format

arp fixup

Parameters

None

Views

VLANIF interface view, GE interface view, GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, 40GE interface view, 40GE sub-interface view, XGE interface view, 25GE interface view, XGE sub-interface view, 25GE sub-interface view, 100GE interface view, 100GE sub-interface view, Eth-Trunk interface view, or Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent attackers from forging ARP packets and modifying dynamic ARP entries on the device, you can run the **arp fixup** command on interfaces to configure fixed ARP and convert the dynamic ARP entries learned by the device into static ARP entries.

Fixed ARP is used together with ARP automatic scanning. Run the **arp scan** command to configure ARP automatic scanning so that the device can obtain the dynamic ARP entries from the devices in the network. Then run the **arp fixup** command to configure fixed ARP so that the device converts the obtained dynamic ARP entries to static ARP entries to prevent network attacks.

Prerequisites

On an Ethernet interface working in Layer 2 mode, the **undo portswitch** command has been run to switch the interface to Layer 3 mode.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

Precautions

- The number of static ARP entries converted through fixed ARP depends on the number of static ARP entries supported on the device. When the number of dynamic ARP entries exceeds the maximum value supported on the device, excess dynamic ARP entries will not be converted and the system displays an error message.
- The static ARP entries converted through fixed ARP are the same as the configured ARP entries. You can run the **undo arp static** command to delete each entry or **reset arp static** to delete all the entries.

Example

Configure fixed ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp fixup
Warning: This operation may generate configuration of static ARP, and take a long time, press CTRL+C to
break. Continue?[Y/N]:y
```

6.2.9 arp ip-conflict-detect enable

Function

The **arp ip-conflict-detect enable** command enables the switch to log IP address conflicts during IP address conflict detection.

The **undo arp ip-conflict-detect enable** command disables the switch from logging IP address conflicts during IP address conflict detection.

By default, IP address conflicts during IP address conflict detection are not logged.

Format

arp ip-conflict-detect enable

undo arp ip-conflict-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the IP addresses of devices on the network conflict, the CPU usage becomes excessively high and routes on the devices flap frequently. This greatly affects user services and even results in service interruption. You can run the **arp ip-conflict-detect enable** command to enable the switch to log IP address conflicts during IP address conflict detection. In this way, the device IP addresses can be properly managed, reducing the impact of IP address conflicts on user services.

When a device enabled with IP address conflict detection receives a non-gratuitous ARP packet from a user, the device compares the source IP address and source MAC address of the packet with the ARP entries that the device has learned. If the source IP address matches an ARP entry but the MAC address matches no ARP entry, the IP address conflict occurs. The device then generates log information to inform the user.

Precautions

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable the switch to log IP address conflicts during IP address conflict detection.

```
<HUAWEI> system-view
[HUAWEI] arp ip-conflict-detect enable
```

6.2.10 arp learning double-tag disable

Function

The **arp learning double-tag disable** command disables ARP learning for packets with double VLAN tags.

The **undo arp learning double-tag disable** command enables ARP learning for packets with double VLAN tags.

ARP learning is disabled for packets with double VLAN tags.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp learning double-tag disable

undo arp learning double-tag disable

Parameters

None

Views

VLANIF interface view

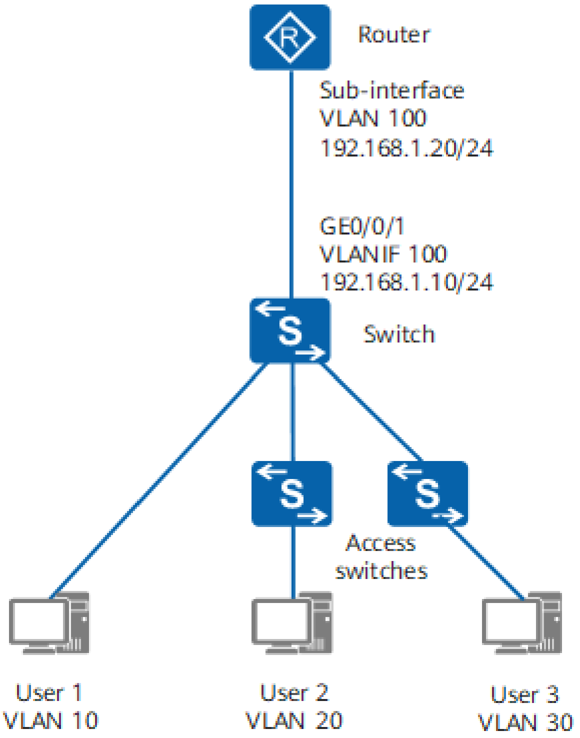
Default Level

2: Configuration level

Usage Guidelines

In **Figure 6-2**, users belong to different VLANs and are connected to the gateway router through the switch. The switch is connected to the sub-interface for VLAN termination on the router through VLANIF 100. GE0/0/1 on the switch is configured as a hybrid interface, added to VLAN 10 in untagged mode, and added to VLAN 20 and VLAN 30 in tagged mode. Static ARP binding is configured for user 2 and user 3 on the router, and the inner and outer VLANs are specified.

Figure 6-2 Networking of disabling ARP learning for packets with double VLAN tags



When the router pings the IP address 192.168.1.10 of VLANIF 100 on the switch, the switch learns an ARP entry containing the IP address 192.168.1.20 and VLAN ID 100 of the router's sub-interface.

When the router sends ARP probe packets to a user (for example, user 2) who is not directly connected to the switch, the source IP address in the probe packets is the IP address 192.168.1.20 of the router's sub-interface, and the probe packets contain double VLAN tags. The outer VLAN ID is 100 and the inner VLAN ID is 20. When the probe packets pass through the switch, the switch updates the original ARP entry, and records the outer VLAN ID 100 and inner VLAN ID 20.

By default, the fast ICMP reply function is enabled on the switch. When receiving ICMP request packets, the receiving interface on the switch does not send the packets to the CPU for processing, and instead, directly replies with ICMP reply packets. When the router pings the IP address 192.168.1.10 of VLANIF 100 on the switch, ICMP reply packets match the ARP entry containing the IP address 192.168.1.20, and the ARP entry corresponds to the outer VLAN ID 100 and inner VLAN ID 20. Therefore, ICMP reply packets sent by the switch contain double VLAN tags. When checking the VLAN in received packets, the router detects that the packets contain double VLAN tags instead of one VLAN tag, and discards the packets. Therefore, the router fails to ping the IP address 192.168.1.10 of VLANIF 100 on the switch.

You can run the **arp learning double-tag disable** command on the switch to disable ARP learning for packets with double VLAN tags. After this function is disabled, the switch does not learn ARP entries from ARP probe packets with double VLAN tags sent from the router to a user, and does not update the learned ARP entry containing the IP address 192.168.1.20 and VLAN ID 100. The router can always ping the IP address 192.168.1.10 of VLANIF 100 on the switch.

Example

Disable ARP learning for packets with double VLAN tags on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp learning double-tag disable
```

6.2.11 arp learning ip-network-cross enable

Function

The **arp learning ip-network-cross enable** command enables inter-network segment ARP learning on interfaces.

The **undo arp learning ip-network-cross enable** command disables inter-network segment ARP learning on interfaces.

By default, inter-network segment ARP learning is disabled on interfaces.

Format

arp learning ip-network-cross enable

undo arp learning ip-network-cross enable

Parameters

None

Views

System view

Default Level

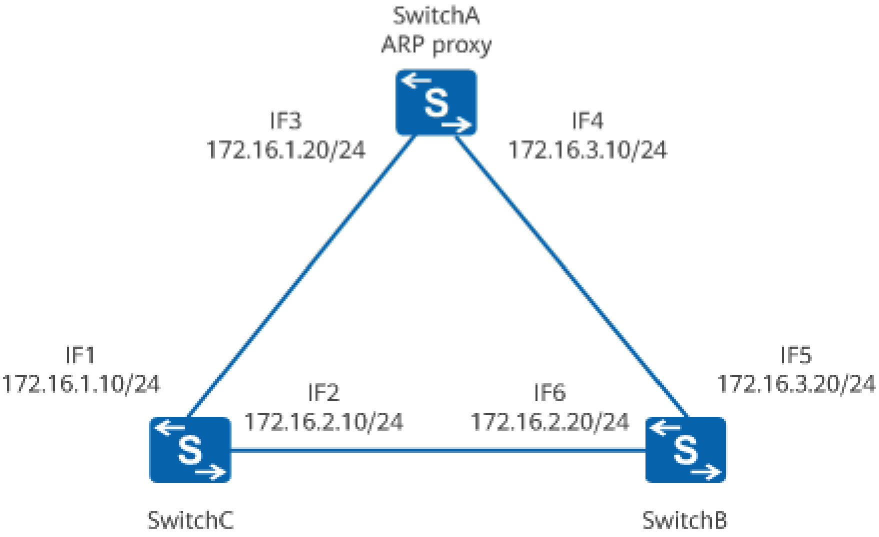
2: Configuration level

Usage Guidelines

Usage Scenario

In **Figure 6-3**, a loop prevention protocol has been configured on each switch. SwitchC can learn the ARP entry with the destination IP address 172.16.2.20 (IP address of interface IF6 on SwitchB) through interface IF2. After proxy ARP is enabled on SwitchA, SwitchC can learn ARP entries on another network segment, and interface IF1 on SwitchC can also learn the ARP entry with the destination IP address 172.16.2.20. As a result, the ARP entry learned through interface IF2 is overwritten by that learned through interface IF1, and SwitchC cannot communicate with SwitchB. In this case, you can run the **undo arp learning ip-network-cross enable** command to disable inter-network segment ARP learning on interface IF1 of SwitchC.

Figure 6-3 Networking for disabling inter-network segment ARP learning



If a switch is upgraded from a version earlier than V200R010C00 to V200R020C00 or a later version, inter-network segment ARP learning is enabled on interfaces by default after the upgrade. In addition, the **undo arp learning ip-network-cross enable** command can be run on such switches, but not the **arp learning ip-network-cross enable** command. If a switch is upgraded from V200R010C00 or a later version to V200R020C00 or a later version, inter-network segment ARP learning is disabled on interfaces by default after the upgrade, and the **arp learning ip-network-cross enable** and **undo arp learning ip-network-cross enable** commands can be run on such switches.

Precautions

In versions earlier than V200R020C00, this command can be used only for configuration restoration and cannot be manually configured after the configuration is restored.

Example

Disable inter-network segment ARP learning on interfaces.

```
<HUAWEI> system-view
[HUAWEI] undo arp learning ip-network-cross enable
```

6.2.12 arp learning multicast disable

Function

The **arp learning multicast disable** command disables an interface from learning ARP entries with multicast MAC addresses.

The **undo arp learning multicast disable** command enables an interface to learn ARP entries with multicast MAC addresses.

By default, if a device is globally enabled to learn ARP entries with multicast MAC addresses, this function is enabled on all the interfaces. If a device is globally disabled from learning ARP entries with multicast MAC addresses, this function is disabled on all the interfaces.

Format

arp learning multicast disable

undo arp learning multicast disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP address may map a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. After a device is enabled to learn ARP entries with multicast MAC addresses, the device can generate dynamic ARP entries. This reduces a network administrator's workload and decreases network operation and maintenance costs.

After a device is globally enabled to learn ARP entries with multicast MAC addresses, all the interfaces will learn ARP entries when receiving ARP packets with the multicast MAC addresses as source MAC addresses. This increases system resource consumption and affects user service running. You can run the **arp learning multicast disable** command on an interface to disable the interface from learning ARP entries with multicast MAC addresses.

Precautions

After an interface is disabled from learning ARP entries with multicast MAC addresses, the interface directly discards ARP packets with the multicast MAC addresses as source MAC addresses, which may result in service interruption.

In the multicast service scenario, if the mapping between IP addresses and multicast MAC addresses is not specified using the **arp static** command, do not disable the specified interface from learning ARP entries with multicast MAC addresses to ensure normal running of the multicast service.

After an interface is disabled from learning ARP entries with multicast MAC addresses using the **arp learning multicast disable** command, you can run the **undo arp learning multicast disable** or **arp learning multicast enable** command on the interface to enable it to learn multicast MAC addresses. The differences between the two commands are as follows:

- After you run the **arp learning multicast enable** command, the configuration on the interface takes effect.
- After you run the **undo arp learning multicast disable** command, the global configuration takes effect.

Example

Disable an interface from learning ARP entries with multicast MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp learning multicast disable
```

6.2.13 arp learning multicast enable (interface view)

Function

The **arp learning multicast enable** command enables an interface to learn ARP entries with multicast MAC addresses.

The **undo arp learning multicast enable** command disables an interface from learning ARP entries with multicast MAC addresses.

By default, if a device is globally enabled to learn ARP entries with multicast MAC addresses, this function is enabled on all the interfaces. If a device is globally disabled from learning ARP entries with multicast MAC addresses, this function is disabled on all the interfaces.

Format

arp learning multicast enable

undo arp learning multicast enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP address may map a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. After a device is enabled to learn ARP entries with multicast MAC addresses, the device can generate dynamic ARP entries. This reduces a network administrator's workload and decreases network operation and maintenance costs.

Precautions

After a device is enabled to learn ARP entries with multicast MAC addresses, the device may be attacked by ARP attack packets with multicast MAC addresses.

To prevent the device from being attacked, multicast MAC address learning adopts the most precise matching rule:

- When the function is enabled globally and on an interface, the configuration on the interface takes effect.
- When the function is disabled on an interface, the global configuration takes effect.
- When the function is disabled globally, the configuration on the interface takes effect.

If you run the **undo arp learning multicast enable** command on an interface when the function is enabled globally and on the interface, the global configuration takes effect and the function is still enabled. To completely disable the interface from learning ARP entries with multicast MAC addresses, run the **arp learning multicast disable** command on the interface.

Example

Enable GigabitEthernet0/0/1 to learn ARP entries with multicast MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp learning multicast enable
```

6.2.14 arp learning multicast enable (system view)

Function

The **arp learning multicast enable** command globally enables a device to learn ARP entries with multicast MAC addresses.

The **undo arp learning multicast enable** command globally disables a device from learning ARP entries with multicast MAC addresses.

By default, a device is globally disabled from learning ARP entries with multicast MAC addresses.

Format

arp learning multicast enable

undo arp learning multicast enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP address may map a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. After a device is enabled to learn ARP entries with multicast MAC addresses, the device can generate dynamic ARP entries. This reduces a network administrator's workload and decreases network operation and maintenance costs.

Precautions

After a device is enabled to learn ARP entries with multicast MAC addresses, the device may be attacked by ARP attack packets with multicast MAC addresses.

The **arp learning multicast enable** and **arp learning multicast disable** commands can be used together on an interface to precisely control the range of ARP entries with multicast MAC addresses to be learned.

Example

Globally enable a device to learn ARP entries with multicast MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] arp learning multicast enable
```

6.2.15 arp learning priority high

Function

The **arp learning priority high** command sets the ARP learning priority of an interface to high.

The **undo arp learning priority high** command sets the ARP learning priority of an interface to low.

By default, the ARP learning priority of an interface is low.

Format

arp learning priority high

undo arp learning priority high

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the ARP resources of a card are limited, you can configure a high ARP learning priority for VLANIF interfaces that carry important services and reserve certain ARP resources. When the remaining ARP resources of a card are less than or equals the number of reserved ARP entries, only VLANIF interfaces with a high priority can deliver the ARP entries.

- To check the ARP specification based on the value of **HOST4**, run the **display adp-l3 ability** [**slot** *slot-number*] command in the diagnostic view.
- To check the number of reserved ARP entries based on the value of **Reserved ARP number**, run the **display adp-ipv4 statistics arp** [**slot** *slot-id*] command in the diagnostic view.

Pre-configuration Tasks

The **assign arp reserved number** *number-value* command has been run in the system view to configure the number of reserved ARP entries for all cards. The number of reserved ARP entries of each card is displayed as the value of *number-value*.

Precautions

If you run the **arp learning priority high** command on multiple VLANIF interfaces of a card, these interfaces share the number of reserved ARP entries of the card.

Example

Set the ARP learning priority of VLANIF 10 to high.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
```

```
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp learning priority high
```

6.2.16 arp periodic-refresh disable

Function

The **arp periodic-refresh disable** command disables the function of updating ARP entries every 10 hours.

The **undo arp periodic-refresh disable** command enables the function of updating ARP entries every 10 hours.

By default, the function of updating ARP entries every 10 hours is enabled.

NOTE

For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: To disable the function of periodically updating ARP entries, run both the **arp periodic-refresh disable** and **undo arp regularly-refresh enable** commands.

Format

arp periodic-refresh disable

undo arp periodic-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, a device runs a timer to update its ARP entries every 10 hours. To reduce the load on the device, you can run this command to disable the device from updating ARP entries every 10 hours.

Example

Disable the device from updating ARP entries every 10 hours.

```
<HUAWEI> system-view
[HUAWEI] arp periodic-refresh disable
```

6.2.17 arp purge slowly

Function

The **arp purge slowly** command enables a device to delete dynamic ARP entries after a delay when a VLANIF member interface goes Down.

The **undo arp purge slowly** command restores the default setting.

By default, a device deletes dynamic ARP entries immediately when a VLANIF member interface goes Down.

Format

arp purge slowly

undo arp purge slowly

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, when a VLANIF member interface goes Down, a device immediately deletes the dynamic ARP entries learned by the member interface. At this time, the VLANIF interface needs to relearn ARP entries to forward user traffic. However, in some special networking scenarios, such as the ring or dual-homed networking, a VLANIF member interface going Down does not necessarily mean that its interconnected interface is deleted. The outbound interfaces of ARP entries may change. In this situation, it will take a long time for the device to relearn ARP entries, interrupting user service traffic.

To minimize the preceding impact and accelerate user traffic convergence, run the **arp purge slowly** command to enable the device to delete dynamic ARP entries after a delay when a VLANIF member interface goes Down.

After the **arp purge slowly** command is configured, the device does not immediately delete dynamic ARP entries learned by a VLANIF member interface after it goes Down. Instead, it sends ARP probe packets and then deletes or updates ARP entries depending on whether it receives ARP Reply packets within the ARP aging time:

- If the device does not receive ARP Reply packets, it deletes the dynamic ARP entries.

- If the device receives ARP Reply packets, it updates ARP entries based on information contained in the ARP Reply packets.

Precautions

To update ARP entries, a better alternative to ARP aging mechanism is enabling the MAC address-triggered ARP entry update function, because the device learns MAC address entries faster. Therefore, to accelerate user traffic convergence, you are advised to enable ARP entry delayed deletion and the MAC address-triggered ARP entry update function using the **mac-address update arp** command.

The **arp purge slowly** and **arp detect-mode unicast** commands are mutually exclusive on the same VLANIF interface. If they are both run on the same VLANIF interface, the **arp purge slowly** command fails to take effect.

Example

Enable a device to delete dynamic ARP entries after a delay when a member interface of VLANIF 100 goes Down.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp purge slowly
```

6.2.18 arp regularly-refresh cycle-interval

Function

The **arp regularly-refresh cycle-interval** command sets the interval for updating ARP entries in the device hardware table.

The **undo arp regularly-refresh cycle-interval** command restores the default interval for updating ARP entries in the device hardware table.

By default, the interval for updating ARP entries in the device hardware table is 1 minute.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp regularly-refresh cycle-interval *cycle-interval*

undo arp regularly-refresh cycle-interval

Parameters

Parameter	Description	Value
cycle-interval	Specifies the interval for updating ARP entries in the device hardware table.	The value is an integer in the range from 1 to 1440, in minutes. The default value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally. You can set the interval for updating ARP entries in the device hardware table as required.

Precautions

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

Example

Set the interval for updating ARP entries in the device hardware table to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh cycle-interval 5
```

6.2.19 arp regularly-refresh enable

Function

The **arp regularly-refresh enable** command enables the function of periodically updating ARP entries in the device hardware table.

The **undo arp regularly-refresh enable** command disables the function of periodically updating ARP entries in the device hardware table.

By default, the function of periodically updating ARP entries in the device hardware table is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp regularly-refresh enable

undo arp regularly-refresh enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally.

Precautions

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

Example

Enable the function of periodically updating ARP entries in the device hardware table.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh enable
```

6.2.20 arp regularly-refresh entry-number

Function

The **arp regularly-refresh entry-number** command sets the number of ARP entries in the hardware table updated each time.

The **undo arp regularly-refresh entry-number** command restores the default number of ARP entries in the hardware table updated each time.

By default, the number of ARP entries in the hardware table updated each time is 50.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp regularly-refresh entry-number *entry-number*

undo arp regularly-refresh entry-number

Parameters

Parameter	Description	Value
entry-number	Specifies the number of ARP entries in the hardware table updated each time.	The value is an integer in the range from 1 to 100. The default value is 50.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally. You can set the number of ARP entries in the hardware table updated each time as required.

Precautions

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

Example

Set the number of ARP entries in the hardware table updated each time to 25.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh entry-number 25
```

6.2.21 arp regularly-refresh scan-interval

Function

The **arp regularly-refresh scan-interval** command sets the scan interval for updating ARP entries in the device hardware table.

The **undo arp regularly-refresh scan-interval** command restores the default scan interval for updating ARP entries in the device hardware table.

By default, the scan interval for updating ARP entries in the device hardware table is 1 second.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp regularly-refresh scan-interval *scan-interval*

undo arp regularly-refresh scan-interval

Parameters

Parameter	Description	Value
scan-interval	Specifies the scan interval for updating ARP entries in the device hardware table.	The value is an integer in the range from 1 to 300, in seconds. The default value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally. You can set the scan interval for updating ARP entries in the device hardware table as required.

Precautions

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

Example

Set the scan interval for updating ARP entries in the device hardware table.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh scan-interval 10
```

6.2.22 arp scan

Function

The **arp scan** command configures ARP automatic scanning. This function enables the device to learn ARP entries by sending ARP Request packets to the network segment of the interface IP address.

Format

arp scan [*start-ip-address* **to** *end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address for ARP automatic scanning. The start IP address must be smaller than or equal to the end IP address.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address for ARP automatic scanning. The end IP address must be greater than or equal to the end IP address.	The value is in dotted decimal notation.

Views

VLANIF interface view, GE interface view, GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, 40GE interface view, 40GE sub-interface view, XGE interface view, 25GE interface view, XGE sub-interface view, 25GE sub-interface view, 100GE interface view, 100GE sub-interface view, Eth-Trunk interface view, or Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **arp scan** command to configure ARP automatic scanning so that the device can quickly learn ARP entries of the neighbors in the same network segment.

ARP automatic scanning is used together with fixed ARP. Run the **arp scan** command to enable the device to obtain dynamic ARP entries from all devices in the network. Then run the **arp fixup** command to configure the device to convert the obtained dynamic ARP entries to static ARP entries to prevent network attacks.

Prerequisites

On an Ethernet interface working in Layer 2 mode, the **undo portswitch** command has been run to switch the interface to Layer 3 mode.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

Precautions

- The start and end IP addresses for ARP automatic scanning must be in the same network segment with the IP address of the interface, and the start IP address must be smaller than or equal to the end IP address.
- If the IP address range is not specified, the device scans only the neighbors within the same network segment as the primary IP address of the interface.
- The device does not scan the IP addresses in ARP entries.
- ARP automatic scanning consumes a large number of system resources. You are advised to perform scanning when the resource usage is low and avoid other operations during scanning.
- A VLAN must be configured on a sub-interface, and only one VLAN can be configured.
- Automatic ARP scanning takes a long time if there is a large number of neighbors within the same network segment as the primary IP address of the interface. You can press **Ctrl+C** to stop scanning. The device generates dynamic ARP entries based on the ARP Reply packets received from neighbors before you stop the scanning. You can run the **display arp dynamic** command in any view to check all the dynamic ARP entries that the device has learned.

Example

Enable ARP automatic scanning.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp scan
Warning: This operation may take a long time, press CTRL+C to break. Continue?[Y/N]:y
```

6.2.23 arp send-packet

Function

The **arp send-packet** command configures the ARP unicast probe function.

Format

arp send-packet *ip-address mac-address* **interface** *interface-type interface-number*[*.subinterface-number*] [**vid** *vid* [**cevid** *cevid*]]

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **cevid** and *subinterface-number* parameter.

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address of a unicast ARP Request packet.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address of a unicast ARP Request packet.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits. The value cannot be set to FFFF-FFFF-FFFF.
interface *interface-type interface-number*[*.subinterface-number*]	Specifies the outbound interface for a unicast ARP Request packet. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● *subinterface-number* specifies the sub-interface number.	-
vid *vid*	Specifies the outer VLAN tag of a unicast ARP Request packet.	The value is an integer that ranges from 1 to 4094.
cevid *cevid*	Specifies the inner VLAN tag of a unicast ARP Request packet.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **arp send-packet** command triggers the device to send a unicast ARP Request packet to the user with the specified IP address and MAC address. You can determine whether the peer exists by checking whether the device receives an ARP Reply packet from the peer.

- If the device receives an ARP Reply packet from the peer, the peer exists. The device then generates or updates the ARP entry based on the ARP Reply packet.
- If the device does not receive an ARP Reply packet from the peer, the peer does not exist. The device does not generate an ARP entry in this case.

Example

Configure the device to send a unicast ARP Request packet with the destination IP address 10.10.10.1 and destination MAC address 00e0-fc12-3456 from VLANIF 100.

```
<HUAWEI> arp send-packet 10.10.10.1 00e0-fc12-3456 interface vlanif 100
```

6.2.24 arp static

Function

The **arp static** command configures a static ARP entry.

The **undo arp static** command deletes a static ARP entry.

By default, the ARP table is empty and address mappings are obtained using dynamic ARP.

Format

arp static *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]

arp static *ip-address mac-address* **interface** *interface-type interface-number*[*.subinterface-number*]

arp static *ip-address mac-address* **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number*[*.subinterface-number*]

undo arp static *ip-address* [*mac-address*] [**vpn-instance** *vpn-instance-name*]

undo arp static *ip-address mac-address* **interface** *interface-type interface-number*[*.subinterface-number*]

undo arp static *ip-address* [*mac-address*] **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number*[*.subinterface-number*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **cevid** *ce-vid* and *subinterface-number*.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address in a static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address in a static ARP entry.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** After the name of a VPN instance is specified, the device can automatically learn the outbound interface, with no need for specifying it.	The value must be an existing VPN instance name.
interface *interface-type interface-number*[*.subinterface-number*]	Specifies the outbound interface in a static ARP entry. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● *subinterface-number* specifies the sub-interface number. **NOTE** If the IP address corresponding to the specified ARP entry belongs to the VPN, an outbound interface cannot be specified.	-
vid *vlan-id*	Specifies the ID of the VLAN to which a static ARP entry belongs.	The value is an integer that ranges from 1 to 4094.
cevid *ce-vid*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, devices on a network can use ARP to dynamically learn ARP entries and age or update the generated dynamic ARP entries. However, when a network encounters an ARP attack, the dynamic ARP entries may be incorrectly updated or aged. As a result, the communication between authorized users becomes abnormal.

Static ARP entries can be neither aged nor overwritten by dynamic ARP entries, ensuring communication security. If a static ARP entry is configured on a device, the device can communicate with the peer device using only the specified MAC address. Network attackers cannot modify the mapping between the IP and MAC addresses using ARP packets, ensuring communication between the two devices. Static ARP entries are generally configured on gateways.

Static ARP entries are applicable when:

- Networks contain critical devices such as servers. In this case, static ARP entries can be configured on the switch. As such, network attackers cannot update the ARP entries containing IP addresses of the critical devices on the switch using ARP attack packets, thereby ensuring communication between users and the critical devices.
- Networks contain user devices with multicast MAC addresses. In this case, static ARP entries can be configured on the switch. In doing so, a device, by default, does not learn ARP entries when the source MAC addresses of received ARP packets are multicast MAC addresses.
- A network administrator wants to prevent an IP address from accessing devices. In this case, static ARP entries can be configured on the switch to bind the IP address to an unavailable MAC address.

An ARP entry includes the IP address, the MAC address, and the outbound interface as well as the outer and inner VLAN tags. The switch can add two VLAN tags to the packets according to the ARP entry during packet forwarding.

Precautions

When you configure a static ARP entry, note that:

- When the outbound interface is a Layer 2 Ethernet interface, run the **arp static** *ip-address mac-address* **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number* [*.subinterface-number*] command.

  When a static ARP entry is configured for a QinQ termination sub-interface, **vid** specified in this command must be the same as **pe-vid** in the **qinq termination pe-vid ce-vid** command, and **cevid** in this command must be within the value range of **ce-vid** in the **qinq termination pe-vid ce-vid** command.
- When the outbound interface is a Layer 3 Ethernet interface, run the **arp static** *ip-address mac-address* **interface** *interface-type interface-number* command.

- When the VPN instance mapping the ARP entries needs to be specified, run the **arp static** *ip-address mac-address* **vpn-instance** *vpn-instance-name* command.
- When short static ARP entries need to be configured (for example, if the device is connected to an NLB cluster and multi-interface ARP is used), run the **arp static** *ip-address mac-address* command.

The IP address specified by *ip-address* must be in the same network segment as the IP address of the outbound interface specified by **interface** *interface-type interface-number*.

If a new static ARP entry is duplicate with an existing one, the system updates the entry.

You can run the **arp static** command multiple times to configure static ARP entries one by one, or run the **arp scan** and **arp fixup** commands to configure multiple static ARP entries at one time.

Example

Configure a static ARP entry that maps the IP address 10.0.0.1 to the MAC address 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] arp static 10.0.0.1 00e0-fc12-3456
```

Configure a static ARP entry that maps the IP address 10.1.1.1 to the MAC address 00e0-fc12-3457. This entry belongs to VLAN 10 and its outbound interface is GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] arp static 10.1.1.1 00e0-fc12-3457 vid 10 interface gigabitethernet 0/0/1
```

Configure a static ARP entry that maps the IP address 10.1.1.1 to the MAC address 00e0-fc12-3457. This entry belongs to the VPN instance **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] arp static 10.1.1.1 00e0-fc12-3457 vpn-instance vpn1
```

6.2.25 arp topology-change disable

Function

The **arp topology-change disable** command disables the device from responding to TC BPDUs. That is, the device does not age or delete ARP entries when receiving TC BPDUs.

The **undo arp topology-change disable** command enables the device to respond to TC BPDUs.

By default, the device is enabled to respond to TC BPDUs. The device ages or deletes ARP entries when receiving TC BPDUs.

Format

arp topology-change disable

undo arp topology-change disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When STP detects network topology changes, the device sends TC BPDUs to instruct the ARP module to age or delete ARP entries. The device then needs to relearn ARP entries.

If the network topology changes frequently or there are many ARP entries on the network, ARP entry relearning will cause excess ARP packets to be generated. As a result, a large number of system resources are occupied and services are affected. To address this issue, run the **arp topology-change disable** command to disable the device from responding to TC BPDUs. The device does not age or delete ARP entries even if the network topology changes.

Precautions

After the device is disabled from responding to TC BPDUs using the **arp topology-change disable** command, it does not age or delete ARP entries when the network topology changes. If the MAC address-triggered ARP entry update function is not enabled, user services may be interrupted because the device does not update the saved ARP entries in real time. In this case, you are advised to run the **mac-address update arp** command to enable the MAC address-triggered ARP entry update function.

Example

Disable the device from aging or deleting ARP entries when the network topology changes.

```
<HUAWEI> system-view
[HUAWEI] arp topology-change disable
```

6.2.26 arp-miss message-cache disable

Function

The **arp-miss message-cache disable** command disables the device from packetizing ARP Miss messages.

The **undo arp-miss message-cache disable** command enables the device to packetize ARP Miss messages.

By default, the device is enabled to packetize ARP Miss messages.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp-miss message-cache disable

undo arp-miss message-cache disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a host sends an IP packet with an irresolvable destination IP address to the device (there is a routing entry matching the destination IP address but there is no ARP entry matching the next hop of the routing entry), ARP Miss messages are generated on the device. By default, the device packetizes ARP Miss messages and sends them to the CPU, improving the efficiency in processing ARP Miss messages.

When the device is enabled to packetize ARP Miss messages, the device cannot send ICMP Host Unreachable packets or ICMP Redirect packets. To enable these cards to send ICMP Host Unreachable packets and ICMP Redirect packets, run the **arp-miss message-cache disable** command to disable the device from packetizing ARP Miss messages.

Example

Disable the device from packetizing ARP Miss messages.

```
<HUAWEI> system-view
[HUAWEI] arp-miss message-cache disable
```

6.2.27 arp-proxy enable

Function

The **arp-proxy enable** command enables routed proxy ARP on an interface.

The **undo arp-proxy enable** command disables routed proxy ARP on an interface.

By default, routed proxy ARP is disabled on an interface.

Format

arp-proxy enable

undo arp-proxy enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the hosts not configured with the default gateways are located on the same network segment but different physical networks (different broadcast domains), you can run the **arp-proxy enable** command on the device connected to the hosts to enable routed proxy ARP, implementing IP address resolution between the hosts.

Precautions

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable routed proxy ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy enable
```

Enable routed proxy ARP on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-Gigabitethernet0/0/1] undo portswitch
[HUAWEI-Gigabitethernet0/0/1] arp-proxy enable
```

6.2.28 arp-proxy inner-sub-vlan-proxy enable

Function

The **arp-proxy inner-sub-vlan-proxy enable** command enables intra-VLAN proxy ARP.

The **undo arp-proxy inner-sub-vlan-proxy enable** command disables intra-VLAN proxy ARP.

By default, intra-VLAN proxy ARP is disabled.

Format

arp-proxy inner-sub-vlan-proxy enable

undo arp-proxy inner-sub-vlan-proxy enable

Parameters

None

Views

VLANIF interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When hosts are located on the same network segment and belong to the same VLAN configured with port isolation, you can run the **arp-proxy inner-sub-vlan-proxy enable** command on the device connected to the hosts to enable intra-VLAN proxy ARP, implementing IP address resolution between the hosts.

Precautions

QinQ sub-interfaces, Dot1q sub-interfaces, QinQ Stacking sub-interfaces and QinQ Mapping sub-interfaces do not support proxy ARP within a VLAN.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable intra-VLAN proxy ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy inner-sub-vlan-proxy enable
```

6.2.29 arp-proxy inter-sub-vlan-proxy enable

Function

The **arp-proxy inter-sub-vlan-proxy enable** command enables inter-VLAN proxy ARP or enables proxy ARP on a sub-interface.

The **undo arp-proxy inter-sub-vlan-proxy enable** command disables inter-VLAN proxy ARP or disables proxy ARP on a sub-interface.

By default, inter-VLAN proxy ARP is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support inter-VLAN proxy ARP.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interface.

Format

arp-proxy inter-sub-vlan-proxy enable

undo arp-proxy inter-sub-vlan-proxy enable

Parameters

None

Views

VLANIF interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When hosts are located on the same network segment but belong to different VLANs, you can run the **arp-proxy inter-sub-vlan-proxy enable** command on interfaces to enable inter-VLAN proxy ARP, implementing IP address resolution between the hosts.

When hosts are located on the same network segment but belong to different sub-VLANs, you can enable inter-VLAN proxy ARP on the VLANIF interface in a super VLAN.

If inter-VLAN proxy ARP is enabled on a sub-interface, the users on the sub-interface who belong to the same network segment but different VLANs can communicate with each other.

Precautions

After inter-VLAN proxy ARP is enabled and packets are sent from different VLANs but do not have the corresponding ARP entries, ARP packets are replicated in all VLANs on the involved sub-interface. If a lot of VLANs are configured, a large number of ARP packets need to be replicated, causing heavy burden on the peer device and abnormalities (such as high CPU usage and broadcast suppression) on downstream devices. In addition, the local device may fail to send ARP packets in time due to the replication of a large number of packets, which may lead to ARP learning failures. Therefore, do not configure too many VLANs on an interface.

After inter-VLAN proxy ARP is enabled on a sub-interface or VLANIF interface, whether packets sent by the sub-interface or VLANIF interface carry tags depends on the link type of the corresponding Layer 2 Ethernet interface, regardless of the mode in which the Layer 2 Ethernet interface is added to a VLAN. For example, packets sent from a sub-interface or VLANIF interface on a trunk interface carry VLAN tags.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable inter-VLAN proxy ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy inter-sub-vlan-proxy enable
```

6.2.30 arp-suppress enable

Function

The **arp-suppress enable** command enables ARP suppression.

The **undo arp-suppress** command disables ARP suppression.

By default, ARP suppression is disabled and applicable only to VLANIF interfaces.

Format

arp-suppress enable

undo arp-suppress

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On a special network or in the case of ARP attacks, the system receives multiple ARP packets with the same source IP address at a time. The system needs to update ARP entries repeatedly. To ensure system performance, you can enable ARP suppression. This function enables the system to only respond to ARP Request packets but not update ARP entries when the system receives multiple ARP packets with the same IP address in one second.

If ARP suppression is enabled for all interfaces, ARP entries on some interfaces cannot be updated temporarily. ARP suppression is applicable only to VLANIF and Eth-Trunk interfaces. By default, ARP suppression always takes effect on VLANIF interfaces. It can be configured on other logical interfaces.

After you run the **undo arp-suppress** command, ARP suppression is enabled only on VLANIF interfaces.

Example

Enable ARP suppression.

```
<HUAWEI> system-view
[HUAWEI] arp-suppress enable
```

6.2.31 assign arp reserved number

Function

The **assign arp reserved number** command configures the number of reserved ARP entries.

The **undo assign arp reserved number** command cancels the configuration of the number of reserved ARP entries.

By default, the number of reserved ARP entries is 0.

Format

assign arp reserved number *number-value*

undo assign arp reserved number

Parameters

Parameter	Description	Value
number-value	Specifies the number of reserved ARP entries.	The value is an integer that ranges from 0 to 2000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the ARP resources of a card are limited, you can set the ARP learning priorities and the number of reserved ARP entries. When the remaining ARP resources of a card are less than or equals the reserved ARP entries, only interfaces with a high priority can deliver ARP entries.

- Run the **display adp-l3 ability** [**slot** *slot-number*] command in the diagnostic view to check the ARP specification based on the value of **HOST4**.
- Run the **display adp-ipv4 statistics arp** [**slot** *slot-id*] command in the diagnostic view to check the number of reserved ARP entries based on the value of **Reserved ARP number**.

Follow-up Procedure

Run the **arp learning priority high** command in the VLANIF interface view to set the ARP learning priority of the VLANIF interface to high.

Example

Set the number of reserved ARP entries of each card to 1000.

```
<HUAWEI> system-view
[HUAWEI] assign arp reserved number 1000
```

6.2.32 dhcp snooping arp security enable

Function

The **dhcp snooping arp security enable** command enables the egress ARP inspection (EAI) function.

The **undo dhcp snooping arp security enable** command disables the EAI function.

By default, EAI is disabled.

Format

dhcp snooping arp security enable

undo dhcp snooping arp security enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

EAI applies to the following scenario: A device is deployed between an upstream Layer 3 switch and user hosts. The user hosts belong to the same VLAN, connect to the network through user-side interfaces of the device, and obtain IP addresses through DHCP.

If the device broadcasts ARP Request packets in the VLAN, the traffic volume in the VLAN increases. To reduce network loads in the VLAN, enable EAI in this VLAN on the device. The EAI function must be used together with DHCP snooping.

After EAI is enabled, the device matches the destination IP address of a received ARP Request packet with DHCP snooping binding entries to determine the outbound interface for the packet.

- If the destination IP address matches an entry, the device directly sends the packet to the mapping outbound interface. (However, if the outbound interface is the same as the inbound interface of the packet, the device discards the packet.)
- If the destination IP address does not match an entry, the device determines whether the packet is sent from a trusted interface. (In DHCP snooping, the interfaces connecting the device to the DHCP server are deployed as trusted interfaces.)
  - If the packet is sent from a trusted interface, the device forwards the packet from other trusted interfaces. (If there is no other trusted interface, the device discards the packet.)
  - If the packet is not sent from a trusted interface, the device forwards the packet from a trusted interface.

NOTE

DHCP snooping allows a physical interface to be configured as a trusted or untrusted interface. The interfaces connected to the authorized DHCP server are configured as trusted interfaces, and other interfaces as untrusted interfaces. After DHCP snooping is enabled, all interfaces are considered as untrusted interfaces by default.

Precautions

Because the EAI function must be used together with the DHCP snooping function, run the **dhcp snooping enable** command to enable the DHCP snooping function.

After EAI is enabled, the device sends all the received ARP packets to the CPU for software forwarding, which degrades the ARP packet forwarding performance.

The MFF function is implemented based on ARP proxy, whereas the EAI function is implemented based on ARP request packet forwarding. Therefore, the two functions conflict with each other. If you have enabled both MFF and EAI in the same VLAN, the MFF function takes effect.

EAI enabled in a super VLAN does not take effect.

If a VLANIF interface is created for a VLAN enabled with EAI, EAI does not take effect on the VLAN.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable EAI.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI-vlan100] dhcp snooping arp security enable
```

6.2.33 dhcp snooping arp security isolate-forwarding-trust

Function

The **dhcp snooping arp security isolate-forwarding-trust** command enables the device to forward ARP packets to trusted interfaces when port isolation is enabled on both inbound and outbound interfaces of the device.

The **undo dhcp snooping arp security isolate-forwarding-trust** command disables the device from forwarding packets to trusted interfaces.

By default, the device is disabled from forwarding packets to trusted interfaces when port isolation is enabled on both inbound and outbound interfaces of the device.

Format

dhcp snooping arp security isolate-forwarding-trust

undo dhcp snooping arp security isolate-forwarding-trust

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This function applies to the following scenario: A device is deployed between an upstream Layer 3 switch and user hosts. The user hosts belong to the same VLAN, connect to the network through user-side interfaces of the device, and obtain IP addresses through DHCP. Port isolation is configured on the interfaces of the user hosts and intra-VLAN ARP proxy is configured on the Layer 3 switch. This implements Layer 2 isolation and Layer 3 communication between isolated users in the VLAN.

If EAI is also configured on the device, when receiving an ARP Request packet from a user host requesting for another user host, the device matches the destination IP address of the packet with dynamic DHCP snooping binding entries to determine the outbound interface of the packet. If the destination IP address matches an entry, the device directly sends the packet to the destination interface (that is, the interface on the requested user host). If the destination interface is isolated from the inbound interface of the packet, the device discards the packet and the isolated users cannot communicate with each other.

To address this problem, run the **dhcp snooping arp security isolate-forwarding-trust** command. The device then directly forwards the ARP packet to a trusted interface (that is, the interface on the Layer 3 switch). In this case, the intra-VLAN ARP proxy function on the Layer 3 switch allows the isolated users to communicate with each other.

Prerequisites

EAI has been enabled using the **dhcp snooping arp security enable** command.

Example

Enable the device to forward ARP packets to trusted interfaces in VLAN 100 when port isolation is enabled on both inbound and outbound interfaces of the device.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI-vlan100] dhcp snooping arp security enable
[HUAWEI-vlan100] dhcp snooping arp security isolate-forwarding-trust
```

6.2.34 display arp

Function

The **display arp** command displays all ARP entries.

Format

display arp [**all**]

Parameters

Parameter	Description	Value
all	Displays all ARP entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check ARP entries mapping a specified IP address. For example, to check ARP entries mapping the IP address 10.1.1.1, run the **display arp all** | **include** *10.1.1.1* command.

Example

Display all ARP entries.

```
<HUAWEI> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN(SIP/DIP)
------------------------------------------------------------------------------
192.168.50.166  xxxx-xxxx-xxxx            I -         MEth0/0/1
192.168.50.1    xxxx-xxxx-xxx1  20        D-0         MEth0/0/1
192.168.50.165  xxxx-xxxx-xxx2  19        D-0         MEth0/0/1
192.168.50.171  xxxx-xxxx-xxx3  19        D-0         MEth0/0/1
------------------------------------------------------------------------------
Total:4         Dynamic:3       Static:0     Interface:1
```

Table 6-3 Description of the **display arp all** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.

Item	Description
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. ● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. ● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. ● After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating a dynamic ARP entry ● S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries for the interface.

6.2.35 display arp dynamic

Function

The **display arp dynamic** command displays dynamic ARP entries.

Format

display arp dynamic [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the dynamic ARP entries learned in a specified VLAN. If this parameter is not specified, all the dynamic ARP entries learned by the device are displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp dynamic** command to check dynamic ARP entries.

Example

Display all dynamic ARP entries.

```
<HUAWEI> display arp dynamic
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                      VLAN/CEVLAN(SIP/DIP)
------------------------------------------------------------------------------
192.168.50.166  xxxx-xxxx-xxxx            I -  MEth0/0/1
192.168.50.1    xxxx-xxxx-xxx1  13        D-0  MEth0/0/1
192.168.50.165  xxxx-xxxx-xxx2  19        D-0  MEth0/0/1
192.168.50.171  xxxx-xxxx-xxx3  12        D-0  MEth0/0/1
------------------------------------------------------------------------------
Total:4         Dynamic:3       Static:0     Interface:1
```

Table 6-4 Description of the **display arp dynamic** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. ● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. ● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. ● After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.

Item	Description
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating a dynamic ARP entry ● S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries for the interface.

6.2.36 display arp error packet

Function

The **display arp error packet** command displays the last received 10 ARP error packets.

Format

display arp error packet

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device cannot learn ARP entries, you can run this command to check the last received ARP error packets. The ARP error packets help locate the fault.

Example

Display the last received 10 ARP error packets.

```
<HUAWEI> display arp error packet
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:53]:
 00 01 08 00 06 04 00 01 00 25 9E 4B 1F 75 0A 8A
 4E 02 00 00 00 00 00 00 0A 8A 4E FF 00 00 00 00
 00 00 00 00 00 00 FF FF FF FF FF FF 00 25
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:54]:
 00 01 08 00 06 04 00 01 00 13 72 FD E7 1C 0A 8A
 4E 98 00 00 00 00 00 00 0A 8A 4E 30 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:55]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:05]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:05]:
 00 01 08 00 06 04 00 01 00 E0 FC 8F B2 DD 0A 8A
 4E 01 00 00 00 00 00 00 0A 8A 4F FA 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:08]:
 00 01 08 00 06 04 00 01 00 0F E2 5C 8C EA AC 12
 3E FE 00 00 00 00 00 00 AC 12 3E FE 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:11]:
 00 01 08 00 06 04 00 01 00 1B B9 78 25 2E 0A 8A
 4E A5 00 00 00 00 00 00 0A 8A 4E 2D 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:15]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:19]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
--------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:22]:
 00 01 08 00 06 04 00 01 00 E0 FC 8F B2 DD 0A 8A
 4E 01 00 00 00 00 00 00 0A 8A 4F FA 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Table 6-5 Description of the **display arp error packet** command output

Item	Description
interface	Interface name.
time	Time when an ARP error packet is received.

6.2.37 display arp interface

Function

The **display arp interface** command displays ARP entries for a specified interface.

Format

display arp interface *interface-type interface-number*[*.subinterface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number[*.subinterface-number*]	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. • *subinterface-number* specifies the sub-interface number. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the *subinterface-number* parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp interface** command to view contents of ARP entries when you need to monitor dynamic ARP entries or locate the faults in ARP.

Example

Display all ARP entries for VLANIF 10.

```
<HUAWEI> display arp interface Vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                      VLAN/CEVLAN(SIP/DIP)
------------------------------------------------------------------------------
10.1.0.1        xxxx-xxxx-xxxx            I -         Vlanif10
------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0     Interface:1
```

Table 6-6 Description of the **display arp interface** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. ● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. ● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. ● After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating a dynamic ARP entry ● S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries for the interface.

6.2.38 display arp ip-conflict track

Function

The **display arp ip-conflict track** command displays records about IP address conflicts detected.

Format

display arp ip-conflict track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IP address conflicts on a network will result in frequent route flapping on the device and greatly affect user services.

To quickly locate the conflicting IP addresses and better manage device IP addresses, you can run the **display arp ip-conflict track** command to check records about IP address conflicts detected.

Example

Display records about IP address conflicts detected.

```
<HUAWEI> display arp ip-conflict track
  Conflict type       : Remote IP conflict
  IP address          : 10.1.1.1
  System time         : 2013-04-07 11:22:29
  Conflict count      : 1
  Suppress count      : 0
  Old interface       : GE0/0/1
  Receive interface   : GE0/0/2
  Old VLAN/CEVLAN     : 100/0
  Receive VLAN/CEVLAN : 100/0
  Old MAC             : 00e0-fc12-3456
  Receive MAC         : 00e0-fc12-3457

  Conflict type       : Local IP conflict
  IP address          : 192.168.10.1
  System time         : 2013-04-07 11:21:10
  Conflict count      : 1
  Suppress count      : 0
  Local interface     : Vlanif10
  Receive interface   : GE0/0/3
  Receive VLAN/CEVLAN : 10/0
  Receive MAC         : 00e0-fc12-3458
```

Table 6-7 Description of the **display arp ip-conflict track** command output

Item	Description
Conflict type	IP address conflict type: - Local IP conflict occurs between a local device and another device. - Remote IP conflict occurs between devices and users attached to a local access device.
IP address	Conflicting IP address.
System time	System time when an IP address conflict occurs.
Conflict count	Number of IP address conflicts. **NOTE** If the ARP entry mapping the IP address is aged or deleted, this field is set to zero.

Item	Description
Suppress count	Number of IP address conflict suppressions. **NOTE** If the ARP entry mapping the IP address is aged or deleted, this field is set to zero.
Old interface	Interface recorded in the ARP entry mapping the IP address before a conflict.
Local interface	Interface in the ARP entry of the conflicting IP address.
Receive interface	Interface that receives ARP packet during a conflict.
Old VLAN/CEVLAN	VLAN and CE VLAN recorded in the ARP entry mapping the IP address before a conflict.
Receive VLAN/CEVLAN	VLAN and CE VLAN that receive ARP packets during a conflict.
Old MAC	MAC address recorded in the ARP entry mapping the IP address before a conflict.
Receive MAC	Source MAC address in the ARP packet received during a conflict.

6.2.39 display arp network

Function

The **display arp network** command displays ARP entries of a specified network segment.

Format

display arp network *net-number* [*net-mask* | *mask-length*] [**dynamic** | **static**]

Parameters

Parameter	Description	Value
net-number	Specifies the network ID.	The value is in dotted decimal notation.

Parameter	Description	Value
net-mask	Specifies the subnet mask. If *net-mask* and *mask-length* are not specified, the default mask length is 32.	This value is in dotted decimal notation.
mask-length	Specifies the mask length. If *net-mask* and *mask-length* are not specified, the default mask length is 32.	The value is an integer that ranges from 1 to 32.
dynamic	Displays dynamic ARP entries of a specified network segment.	-
static	Displays static ARP entries of a specified network segment.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp network** command to check ARP entries of a specified network segment.

Example

Display all ARP entries of the network segment with network ID 10.10.0.0 and subnet mask 255.255.0.0.

```
<HUAWEI> display arp network 10.10.0.0 255.255.0.0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                      VLAN/CEVLAN(SIP/DIP)
------------------------------------------------------------------------------
10.10.20.9      xxxx-xxxx-xxxx            I -         Vlanif10
10.10.10.6      xxxx-xxxx-xxxx            I -         Vlanif20
------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0     Interface:2
```

Table 6-8 Description of the **display arp network** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. ● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. ● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. ● After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating a dynamic ARP entry ● S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries for the interface.

6.2.40 display arp packet statistics

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to view the statistics on ARP packets.

This command displays the ARP packet statistics on the active switch in a stack system.

Example

Display the statistics on ARP packets.

```
<HUAWEI> display arp packet statistics
ARP Pkt Received: sum 420066
ARP Received In Message-cache: sum 0
ARP-Miss Msg Received: sum 0
ARP Learnt Count: sum 5
ARP Pkt Discard For Limit: sum 0
ARP Pkt Discard For SpeedLimit: sum 0
ARP Pkt Discard For Proxy Suppress: sum 179578
ARP Pkt Discard For Other: sum 90347
ARP-Miss Msg Discard For SpeedLimit: sum 0
ARP Discard In Message-cache For SpeedLimit: sum 0
ARP-Miss Msg Discard For Other: sum 0
```

Table 6-9 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Received In Message-cache	Number of ARP packets received within each second when a switch encapsulates multiple ARP request packets into one packet.
ARP-Miss Msg Received	Total number of ARP Miss messages triggered by ARP Miss packets sent to the CPU.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit. To configure the maximum number of dynamic ARP entries that an interface can learn, run the **arp-limit** command.
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit. To configure a rate limit for ARP packets based on the source IP address, run the **arp speed-limit source-ip** command.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.

Item	Description
ARP-Miss Msg Discard For SpeedLimit	Number of ARP Miss messages discarded when the number of ARP Miss messages triggered by IP packets from a specified source IP address exceeds the limit.
ARP Discard In Message-cache For SpeedLimit	Number of ARP packets discarded due to software rate limit when a switch encapsulates multiple ARP request packets into one packet. To configure a rate limit for ARP Miss messages based on the source IP address, run the **arp-miss speed-limit source-ip** command.
ARP-Miss Msg Discard For Other	Number of the ARP Miss messages discarded due to other causes.

6.2.41 display arp static

Function

The **display arp static** command displays all static ARP entries.

Format

display arp static

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp static** command to check static ARP entries.

You can run the **arp static** command multiple times to configure static ARP entries one by one, or run the **arp scan** and **arp fixup** commands to configure multiple static ARP entries at one time.

Example

Display all static ARP entries.

```
<HUAWEI> display arp static
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN(SIP/DIP)
------------------------------------------------------------------------------
10.1.2.1        00e0-fc12-3456            S--
------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:1     Interface:0
```

Table 6-10 Description of the **display arp static** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. ● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. ● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. ● After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: - I: Interface, indicating the MAC address of the interface - D: Dynamic, indicating a dynamic ARP entry - S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries for the interface.

6.2.42 display arp statistics

Function

The **display arp statistics** command displays ARP entry statistics.

Format

display arp statistics { **all** | **interface** *interface-type interface-number* | **slot** *slot-id* }

Parameters

Parameter	Description	Value
all	Displays ARP entry statistics of the device.	-
interface *interface-type interface-number*	Displays ARP entry statistics of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
slot *slot-id*	Displays ARP entry statistics of a specified slot.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor ARP entries or locate the faults in ARP, you can run the **display arp statistics** command to check ARP entry statistics.

Example

Display ARP entry statistics of the device.

```
<HUAWEI> display arp statistics all
Dynamic:1       Static:0
```

Display ARP entry statistics of slot 0.

```
<HUAWEI> display arp statistics slot 0
Capacity: 98304       In-used: 0
```

Table 6-11 Description of the **display arp statistics** command output

Item	Description
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Capacity	Maximum number of ARP entries of the device. The ARP entry specifications of a device vary according to the device version and model.
In-used	Number of current ARP entries on the device.

6.2.43 display arp status

Function

The **display arp status** command displays the delivery status of ARP entries on a device.

Format

display arp status *ip-address* [**vpn-instance** *vpn-instance-name*] **slot** *slot-id*

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
slot *slot-id*	Specifies a slot ID.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp status** command to check the delivery status of ARP entries with a specified IP address on a device.

Example

Display the delivery status of ARP entries on card 0.

```
<HUAWEI> display arp status 10.137.216.1 slot 0
TYPE : D - Dynamic, I - Interface, S - Static
IP ADDRESS      MAC ADDRESS       EXPIRE(M) TYPE       INTERFACE   VPN-
INSTANCE
                             VLAN/CEVLAN                STATE
------------------------------------------------------------------------------
10.137.216.1    xxxx-xxxx-xxxx  20       D-0       GE0/0/1
                             4094/-              Available
------------------------------------------------------------------------------
```

Table 6-12 Description of the **display arp status** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.

Item	Description
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. ● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. ● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. ● After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating a dynamic ARP entry ● S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.
STATE	Whether the ARP entry has been delivered to the chip. ● Available: The ARP entry has been delivered to the chip. ● Unavailable: The ARP entry has not been delivered to the chip.

6.2.44 display arp track

Function

The **display arp track** command displays changes of outbound interfaces in ARP entries learned by a VLANIF interface.

Format

display arp track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the outbound interfaces change in ARP entries learned by a VLANIF interface, traffic may be interrupted. In this case, run the **display arp track** command to check changes of outbound interfaces and the change time.

Precautions

After the **display arp track** command is executed, changes of ARP entries are displayed in the following situations:

- Outbound interfaces in dynamic ARP entries learned by the VLANIF interface change to other interfaces.
- No outbound interface is specified in the static ARP entries. The outbound interfaces change to other interfaces.
- Dynamic ARP entries or static ARP entries in which no VLAN ID and outbound interface are specified are deleted.

Changes of ARP entries cannot be displayed in the following situations:

- ARP entries change on a non-VLANIF interface.
- New ARP entries are learned.
- The VLAN ID and outbound interface are manually specified in static ARP entries.

Example

Display changes of outbound interfaces in ARP entries.

```
<HUAWEI> display arp track
Operate Flags: M - Modify, D - Delete
------------------------------------------------------------------------------
Op IP-Address  MAC-Address     VLAN   Old-Port   New-Port   System-Time
------------------------------------------------------------------------------
M  10.1.1.1    xxxx-xxxx-xxxx  1000   GE0/0/1    GE0/0/2    2017-08-19 12:10:12
D  10.2.1.100  xxxx-xxxx-xxx1  300               GE0/0/3    2017-08-19 12:12:12
```

Table 6-13 Description of the **display arp track** command output

Item	Description
Op	Operation code. ● M: Modify, indicating that the outbound interface changes. ● D: Delete, indicating that the ARP entry is deleted.
IP-Address	IP address in the ARP entry
MAC-Address	MAC address in the ARP entry
VLAN	ID of the VLAN to which the VLANIF interface belongs.
Old-Port	Original outbound interface in the ARP entry.
New-Port	New outbound interface in the ARP entry.
System-Time	System time when the outbound interface changes.

6.2.45 display arp vpn-instance

Function

The **display arp vpn-instance** command displays ARP entries of a specified VPN instance.

Format

display arp vpn-instance *vpn-instance-name* [**dynamic** | **static**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance name.	The value must be an existing VPN instance name.
dynamic	Displays dynamic ARP entries.	-
static	Displays static ARP entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp vpn-instance** command to check ARP entries of a specified VPN instance.

Example

Check all ARP entries learned by the VPN instance **r1**.

```
<HUAWEI> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                      VLAN/CEVLAN(SIP/DIP)
------------------------------------------------------------------------------
192.168.1.11    00e0-fc12-3456            I -         Vlanif10       r1
192.168.1.1     00e0-fc12-3455  12        D-0         Vlanif10       r1
------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

Table 6-14 Description of the **display arp vpn-instance** command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. **NOTE** If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment. - When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered. - When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry. - After the temporary ARP entry is aged out, the device deletes this entry. You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes. If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged.

Item	Description
TYPE	Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: - I: Interface, indicating the MAC address of the interface - D: Dynamic, indicating a dynamic ARP entry - S: Static, indicating a static ARP entry The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB table has been updated. If the entry is not reported to the routing module, this field displays -. For the ARP entry with the type as I, this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -.
INTERFACE	Type and number of the interface that has learned ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. To configure the VPN instance name, run the **ip vpn-instance** command.

Item	Description
VLAN/CEVLAN	ID of the VLAN/CEVLAN to which the ARP entry belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries for the interface.

6.2.46 display mac-address multiport

Function

The **display mac-address multiport** command displays MAC address entries configured for multiple outbound interfaces.

Format

display mac-address multiport *mac-address* **vlan** *vlan-id*

display mac-address multiport [**vlan** *vlan-id*] [**total-number**]

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN.	The value is an integer that ranges from 1 to 4094.
total-number	Specifies the number of MAC address entries mapping multiple outbound interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mac-address multiport** command to check MAC address entries configured for multiple outbound interfaces. If no parameter is specified, all MAC address entries configured for multiple outbound interfaces are displayed. To configure MAC address entries mapping multiple outbound interfaces, run the **mac-address multiport interface** or **mac-address multiport** command.

Example

Display MAC address entries configured for multiple outbound interfaces in VLAN 10.

```
<HUAWEI> display mac-address multiport vlan 10
-------------------------------------------------------------------------------
MAC Address       VLANID    Out-Interface             Status
-------------------------------------------------------------------------------
XXXX-XXXX-XXXX    10        GigabitEthernet0/0/1        Active
                              1 port(s)
-------------------------------------------------------------------------------
 Total Group(s) : 1
```

Table 6-15 Description of the **display mac-address multiport** command output

Item	Description
MAC Address	-
VLANID	VLAN that the outbound interface mapping the destination MAC address belongs to.
Out-Interface	Outbound interface mapping the destination MAC address.

Item	Description
Status	Current VLAN status, including: ● InActive: indicates that no VLAN is created or a VLAN is created but no physical interface is added to the VLAN. ● Active: indicates that a VLAN has been created and physical interfaces are added to the VLAN.
Total Group(s)	Total number of MAC address entries mapping multiple outbound interfaces.

6.2.47 l2-topology detect enable

Function

The **l2-topology detect enable** command enables Layer 2 topology detection.

The **undo l2-topology detect enable** command disables Layer 2 topology detection.

By default, Layer 2 topology detection is disabled.

Format

l2-topology detect enable

undo l2-topology detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **l2-topology detect enable** command is executed, all ARP entries mapping the VLAN to which the Layer 2 interface belongs are updated if the Layer 2 interface turns Up.

NOTE

When an active/standby switchover is performed in a stack, all ARP entries mapping the VLAN to which the Layer 2 interface belongs are updated.

Example

Enable Layer 2 topology detection.

```
<HUAWEI> system-view
[HUAWEI] l2-topology detect enable
```

6.2.48 mac-address multiport

Function

The **mac-address multiport** command configures MAC address entries mapping multiple outbound interfaces in the interface view.

The **undo mac-address multiport** command deletes the MAC address entries mapping multiple outbound interfaces in the interface view.

By default, no MAC address entries on the device map multiple outbound interfaces.

Format

mac-address multiport *mac-address* **vlan** *vlan-id*

undo mac-address multiport *mac-address* **vlan** *vlan-id*

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Specifies a VLAN that interfaces belong to.	The value is an integer that ranges from 1 to 4094.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The servers in an NLB server cluster use the same IP address (cluster IP address) and MAC address (cluster MAC address). When a device functioning as the access gateway connects to the NLB server cluster, the device needs to send the packet destined to the cluster IP address to each server in the cluster. In this case, run the **mac-address multiport** or **mac-address multiport interface** command to configure MAC address entries mapping multiple outbound interfaces, and run the **arp static** command to configure short static ARP entries. By configuring short static ARP entries, you can determine the MAC address and VLAN mapping the cluster IP address. Query the MAC address table based on the MAC address and VLAN to determine multiple outbound interfaces, and then connect the interfaces to the NLB server cluster.

Precautions

The VLAN specified in the **mac-address multiport** command cannot be a MAC VLAN, super VLAN, leased line VLAN, or control VLAN of Smart Ethernet Protection (SEP) and Rapid Ring Protection Protocol (RRPP).

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the outbound interfaces are Eth-Trunk interfaces, you must run the **unknown-unicast load-balance enhanced** command to configure enhanced load balancing for unknown unicast packets. Otherwise, the configuration is invalid.

Example

Configure entries of the destination MAC address XXXX-XXXX-XXXX mapping multiple outbound interfaces in VLAN 100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address multiport XXXX-XXXX-XXXX vlan 100
```

Configure entries of the destination MAC address XXXX-XXXX-XXXX mapping multiple outbound interfaces in VLAN 100 on Eth-Trunk 6.

```
<HUAWEI> system-view
[HUAWEI] unknown-unicast load-balance enhanced
[HUAWEI] interface eth-trunk 6
[HUAWEI-Eth-Trunk6] mac-address multiport XXXX-XXXX-XXXX vlan 100
```

6.2.49 mac-address multiport interface

Function

The **mac-address multiport interface** command configures MAC address entries mapping multiple outbound interfaces in the system view.

The **undo mac-address multiport interface** command deletes the MAC address entries mapping multiple outbound interfaces in the system view.

By default, no MAC address entries on the device map multiple outbound interfaces.

Format

mac-address multiport *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **vlan** *vlan-id*

undo mac-address multiport *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **vlan** *vlan-id*

undo mac-address multiport { **all** | [*mac-address*] **vlan** *vlan-id* }

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the first interface number mapping a MAC address entry. ● *interface-number2* specifies the last interface number mapping a MAC address entry. The value of *interface-number2* must be greater than that of *interface-number1*, and *interface-number1* and *interface-number2* determine an interface range.	-
vlan *vlan-id*	Specifies a VLAN that interfaces belong to.	The value is an integer that ranges from 1 to 4094.
all	Specifies all MAC address entries mapping multiple outbound interfaces.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The servers in an NLB server cluster use the same IP address (cluster IP address) and MAC address (cluster MAC address). When a device functioning as the access gateway connects to the NLB server cluster, the device needs to send the packet destined to the cluster IP address to each server in the cluster. In this case, run the **mac-address multiport interface** or **mac-address multiport** command to configure MAC address entries mapping multiple outbound interfaces, and run the **arp static** command to configure short static ARP entries. By configuring short static ARP entries, you can determine the MAC address and VLAN mapping the cluster IP address. Query the MAC address table based on the MAC address and VLAN to determine multiple outbound interfaces, and then connect the interfaces to the NLB server cluster.

Precautions

The VLAN specified in the **mac-address multiport interface** command cannot be a MAC VLAN, super VLAN, leased line VLAN, or control VLAN of Smart Ethernet Protection (SEP) and Rapid Ring Protection Protocol (RRPP).

On the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, when the outbound interfaces are Eth-Trunk interfaces, you must run the **load-balance** command to configure load balancing based on IP addresses. Otherwise, the configuration is invalid.

Example

Configure entries of the destination MAC address 00e0-fc00-2200 mapping the outbound interfaces GE0/0/1-GE0/0/4 in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mac-address multiport 00e0-fc00-2200 interface gigabitethernet 0/0/1 to gigabitethernet
0/0/4 vlan 100
```

Configure entries of the destination MAC address 00e0-fc00-2200 mapping the outbound interfaces Eth-Trunk 4-Eth-Trunk 6 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] unknown-unicast load-balance enhanced
[HUAWEI] mac-address multiport 00e0-fc00-2200 interface eth-trunk 4 to eth-trunk 6 vlan 10
```

6.2.50 reset arp

Function

The **reset arp** command clears ARP entries and related packet statistics.

Format

reset arp { **dynamic** [**ip** *ip-address* [**vpn-instance** *vpn-instance-name*]] | **interface** *interface-type interface-number*[*.subinterface-number*] [**ip** *ip-address*] | **static** }

Parameters

Parameter	Description	Value
dynamic	Clears dynamic ARP entries	-
interface *interface-type interface-number*[*.subinterface-number*]	Specifies the interface type and number. ● *interface-type* specifies the type of the interface. ● *interface-number*[*.subinterface-number*] specifies the number of the interface or sub interface.	-
ip *ip-address*	Clears dynamic ARP entries with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.
static	Static ARP entries cannot be restored after being cleared. Exercise caution when you clear static ARP entries.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an attacked device learns a large number of invalid ARP entries, ARP entries of valid users may fail to be saved and these users may fail to access the network. The **reset arp** command can be used to delete ARP entries. After that, the device relearns ARP entries to ensure that users can access the network.

To delete ARP entries based on a certain IP address, you can run the **reset arp dynamic ip** *ip-address* [**vpn-instance** *vpn-instance-name*] or **reset arp interface** *interface-type interface-number*[*.subinterface-number*] **ip** *ip-address* command.

Precautions

- The **reset arp** command deletes mappings between IP addresses and MAC addresses. As a result, users may fail to access some network devices and services may be interrupted.
- The minimum interval for running the command (only the **reset arp** command in which **ip** *ip-address* is not specified) to clear ARP entries is 20 seconds.

Example

Clear dynamic ARP entries.

```
<HUAWEI> reset arp dynamic
```

Clear dynamic ARP entries of VLANIF 100.

```
<HUAWEI> reset arp interface vlanif 100
```

Clear the dynamic ARP entry corresponding to the IP address of 10.1.1.1 in VPN 1.

```
<HUAWEI> reset arp dynamic ip 10.1.1.1 vpn-instance vpn1
```

6.2.51 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics on the active switch in a stack system.

Example

Clear the statistics on all ARP packets.

```
<HUAWEI> reset arp packet statistics
```

6.3 DHCP Configuration Commands

6.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

Layer 3 ethernet interface, VLANIF interface, and sub-interface all support the DHCP function.

6.3.2 alarm ip-used percentage

Function

The **alarm ip-used percentage** command configures the percentage of the alarms indicating that the addresses in an address pool are used up, and the percentage of the clear alarms.

The **undo alarm ip-used percentage** command restores the default percentages of the alarms and clear alarms.

By default, the percentage of the alarms indicating that the addresses in an IP address pool are used up is 100%, and the percentage of the clear alarms is 50%.

Format

alarm ip-used percentage *alarm-resume-percentage alarm-percentage*

undo alarm ip-used percentage

Parameters

Parameter	Description	Value
alarm-resume-percentage	Specifies the percentage of the clear alarms.	The value is an integer that ranges from 1 to 100. The default value is **50**. **NOTE** The percentage of the clear alarms cannot exceed that of the alarms.

Parameter	Description	Value
alarm-percentage	Specifies the percentage of the alarms indicating that the addresses in an address pool are used up.	The value is an integer that ranges from 1 to 100. The default value is **100**.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the addresses in an IP address pool are used up, alarms are sent to notify the administrator.

Precautions

The percentage of the clear alarms cannot exceed that of the alarms.

Example

Configure the percentage of the alarms indicating that the addresses in an address pool are used up, and the percentage of the clear alarms in the IP address pool view.

```
<HUAWEI> system-view
[HUAWEI] ip pool p1
[HUAWEI-ip-pool-p1] alarm ip-used percentage 80 90
```

6.3.3 bootfile

Function

The **bootfile** command configures the name of the startup configuration file for a DHCP client.

The **undo bootfile** command deletes the configured name of the startup configuration file for a DHCP client.

By default, the startup configuration file name is not configured for a DHCP client.

Format

bootfile *bootfile*

undo bootfile

Parameters

Parameter	Description	Value
bootfile	Specifies the name of the startup configuration file for a DHCP client.	The value is a string of 1 to 127 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP clients. After the startup configuration file name is configured using the **bootfile** command, the Offer and ACK packets sent from the DHCP server carry this file name. The DHCP client can acquire the startup configuration file from the specified server based on the file name.

Precautions

Usually, the startup configuration file is saved on a specified file server. Therefore, the route between the DHCP client and the file server must be reachable and the ip address or name of the file server must be specified.

Example

In the IP address pool view, configure the name of the startup configuration file as **start.ini** for the DHCP client.

```
<HUAWEI> system-view
[HUAWEI] ip pool p1
[HUAWEI-ip-pool-p1] bootfile start.ini
```

In the DHCP Option template view, configure the name of the startup configuration file as **start.ini** for the DHCP client.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] bootfile start.ini
```

6.3.4 conflict auto-recycle interval

Function

The **conflict auto-recycle interval** command enables automatic reclaim of conflicting IP addresses in the global address pool and configures the interval for the automatic reclaim.

The **undo conflict auto-recycle interval** command disables automatic reclaim of conflicting IP addresses in the global address pool and deletes the configured interval for the automatic reclaim.

By default, automatic reclaim of conflicting IP addresses in the global address pool is disabled.

Format

conflict auto-recycle interval day *day* [**hour** *hour* [**minute** *minute*]]

undo conflict auto-recycle interval

Parameters

Parameter	Description	Value
day *day*	Specifies the interval for the automatic reclaim, in days.	The value is an integer that ranges from 0 to 999, in days. The default value is 0.
hour *hour*	Specifies the interval for the automatic reclaim, in hours.	The value is an integer that ranges from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the interval for the automatic reclaim, in minutes.	The value is an integer that ranges from 0 to 59, in minutes. The default value is 0.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When a DHCP server allocates IP addresses to clients, IP address conflict may occur because IP addresses of some hosts have been manually configured. In this case, the DHCP server considers these IP addresses as conflicting IP addresses, and allocates available IP addresses from the conflicting IP addresses to clients only after available IP addresses in the address pool are used up. To reclaim conflicting IP addresses promptly, the administrator can run the **conflict auto-recycle interval** command to enable automatic reclaim and specify the reclaim interval.

Prerequisites

The global address pool has been created using the **ip pool** command.

Example

Enable automatic reclaim for conflicting IP addresses in the global address pool **global1**, and set the interval for automatic reclaim to one day.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] conflict auto-recycle interval day 1
```

6.3.5 dhcp anti-attack check duplicate option

Function

The **dhcp anti-attack check duplicate option** command enables the device to check and discard DHCP messages with duplicate options.

The **undo dhcp anti-attack check duplicate option** command disables the device from checking and discarding DHCP messages with duplicate options.

By default, the device is disabled from checking and discarding DHCP messages with duplicate options.

Format

dhcp anti-attack check duplicate option [*option-start* [**to** *option-end*]] &<1-254>

undo dhcp anti-attack check duplicate option [*option-start* [**to** *option-end*]] &<1-254>

Parameters

Parameter	Description	Value
option-start [**to** *option-end*]	Specifies the option value. - *option-start*: Specifies the start value of an option in a DHCP packet. - *option-end*: Specifies the end value of an option in a DHCP packet.	The value is an integer in the range 1 to 254. For an option, the end value must be larger than the start value.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp anti-attack check duplicate option** command applies to DHCP servers, DHCP relay agents, DHCP clients, and DHCP snooping-enabled devices. To discard DHCP messages with duplicate options 1 to 254, run the **dhcp anti-attack check duplicate option** command.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Configure the device to discard DHCP messages with duplicate options.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp anti-attack check duplicate option
```

6.3.6 dhcp anti-attack check udp-checksum

Function

The **dhcp anti-attack check udp-checksum** command enables the function of checking the UDP header checksum in a DHCP packet and discarding a DHCP packet with an incorrect checksum.

The **undo dhcp anti-attack check udp-checksum** command disables the function of checking the UDP header checksum in a DHCP packet.

By default, a device checks the UDP header checksum in a DHCP packet and discards a DHCP packet with an incorrect checksum.

Format

dhcp anti-attack check udp-checksum

undo dhcp anti-attack check udp-checksum

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp anti-attack check udp-checksum** command applies to DHCP servers, DHCP relay agents, DHCP clients, and DHCP snooping-enabled devices. Devices from different vendors may use different DHCP implementation mechanisms. After checking the UDP header checksum in a received DHCP packet, a device may not allow the DHCP packet to pass through and discards the packet. As a result, DHCP becomes unavailable. To solve this problem, you can run the **undo dhcp anti-attack check udp-checksum** command to disable the function of checking the UDP header checksum in a DHCP packet, so that a DHCP packet with an incorrect UDP header checksum can be properly forwarded.

Prerequisites

DHCP has been enabled on the device using the **dhcp enable** command.

Example

Disable the function of checking the UDP header checksum in a DHCP packet.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] undo dhcp anti-attack check udp-checksum
```

6.3.7 dhcp anti-attack check magic-cookie

Function

The **dhcp anti-attack check magic-cookie** command enables the function of checking the magic-cookie field in a DHCP packet and discarding a DHCP packet with an incorrect value in the magic-cookie field.

The **undo dhcp anti-attack check magic-cookie** command disables the function of checking the magic-cookie field in a DHCP packet.

By default, a device does not check the magic-cookie field in a DHCP packet but directly forwards a DHCP packet with an incorrect value in the magic-cookie field.

Format

dhcp anti-attack check magic-cookie

undo dhcp anti-attack check magic-cookie

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp anti-attack check magic-cookie** command applies to DHCP servers, DHCP relay agents, DHCP clients, and DHCP snooping-enabled devices. Devices from different vendors may use different DHCP implementation mechanisms. After checking the magic-cookie field in a received DHCP packet, a device may not allow the DHCP packet to pass through and discards the packet. As a result, DHCP becomes unavailable. To solve this problem, you can run the **undo dhcp anti-attack check magic-cookie** command to disable the function of checking the magic-cookie field in a DHCP packet, so that a DHCP packet with an incorrect value in the magic-cookie field can be properly forwarded.

Prerequisites

DHCP has been enabled on the device using the **dhcp enable** command.

Example

Disable the function of checking the magic-cookie field in a DHCP packet.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] undo dhcp anti-attack check magic-cookie
```

6.3.8 dhcp broadcast suppress enable

Function

The **dhcp broadcast suppress enable** command enables the DHCP broadcast suppression function.

The **undo dhcp broadcast suppress enable** command disables the DHCP broadcast suppression function.

By default, the DHCP broadcast suppression function is disabled.

Format

dhcp broadcast suppress enable

undo dhcp broadcast suppress enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DHCP relay or DHCP server function is enabled on a VLANIF interface of a device, the DHCP broadcast messages (DHCP Discover and DHCP Request messages) received on the VLANIF interface are broadcast among all the physical interfaces in the corresponding VLAN. If a large number of DHCP clients go online, each physical interface receives a large number of DHCP broadcast messages, affecting the device performance. In this case, you can run the **dhcp broadcast suppress enable** command to enable the DHCP broadcast suppression function, so that the DHCP broadcast messages are not broadcast among the interfaces that do not receive these messages.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

In VRRP master/backup scenarios, DHCP broadcast suppression must be disabled so that the backup device can broadcast received DHCP traffic to the master device and IP addresses can be allocated to users through DHCP.

Example

Enable the DHCP broadcast suppression function.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp broadcast suppress enable
```

6.3.9 dhcp client class-id (interface view)

Function

The **dhcp client class-id** command sets the Option60 field in the DHCP request packet sent by the DHCP client.

The **undo dhcp client class-id** command deletes the configured Option60 field in the DHCP request packet sent by the DHCP client.

By default, no Option60 field is configured.

Format

dhcp client class-id *class-id*

undo dhcp client class-id

Parameters

Parameter	Description	Value
class-id	Indicates the value of the Option60 field.	The value is a string of 1 to 64 case-sensitive characters.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server identifies the devices according to the Option60 field in the DHCP request packet. You can run the **dhcp client class-id** *class-id* command to customize the Option60 field in the DHCP request packet sent from the DHCP client.

After you run the **dhcp client class-id** *class-id* command in the VLANIF interface view, the device that functions as the DHCP client fills the set Option60 in the DHCP request packet on the VLANIF interface.

Example

Set the class-id of a DHCP client to **test** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client class-id test
```

Set the class-id of a DHCP client to **test** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client class-id test
```

6.3.10 dhcp client class-id (system view)

Function

The **dhcp client class-id** command is used to set the Option60 field in the DHCP request packet sent by the DHCP client.

The **undo dhcp client class-id** command is used to restore the default value of the Option60 field.

By default, the default value of the Option60 field depends on the device type, which is "huawei *Device Model*".

Format

dhcp client class-id *class-id*

undo dhcp client class-id

Parameters

Parameter	Description	Value
class-id	Indicates the value of the Option60 field.	The value is a string of 1 to 64 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server identifies the devices according to the Option60 field in the DHCP request packet. You can run the **dhcp client class-id** *class-id* command to customize the Option60 field in the DHCP request packet sent from the DHCP client.

Configuration information of the Option60 field is saved in the *storage device*:/dhcp-client.options file. By default, the storage device needs to provide more than 80-byte storage space. You can run the **more dhcp-client.options** command in the user view to check configuration information of the Option60 field.

After you run the **dhcp client class-id** *class-id* command in the system view, the device that functions as the DHCP client fills the set Option60 in the DHCP request packet sent from all of the interfaces.

Example

Set the class-ID of a DHCP client to **test**.

```
<HUAWEI> system-view
[HUAWEI] dhcp client class-id test
```

6.3.11 dhcp client client-id

Function

The **dhcp client client-id** command configures an identifier for a DHCP client.

The **undo dhcp client client-id** command restores the default identifier of a DHCP client.

By default, the identifier of a DHCP client is the client's MAC address.

Format

dhcp client client-id *client-id*

undo dhcp client client-id

Parameters

Parameter	Description	Value
client-id	Specifies the identifier of a DHCP client.	The value is a string of 2 to 64 case-sensitive characters without spaces.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp client client-id** command configures an identifier for a DHCP client. The identifier is encapsulated into a DHCP Request message. When a DHCP client requests an IP address from a DHCP server, the DHCP server obtains the identifier of the DHCP client and assigns an IP address to the DHCP client with the specified identifier.

Example

Set the identifier of the DHCP client to **test_client** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client client-id test_client
```

Set the identifier of the DHCP client to **test_client** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client client-id test_client
```

6.3.12 dhcp client default-route preference

Function

The **dhcp client default-route preference** command configures the default route preference that a DHCP server delivers to a DHCP client.

The **undo dhcp client default-route preference** command restores the default value of the default route preference that a DHCP server delivers to a DHCP client.

By default, the default route preference that a DHCP server delivers to a DHCP client is 60.

Format

dhcp client default-route preference *preference-value*

undo dhcp client default-route preference

Parameters

Parameter	Description	Value
preference-value	Specifies the default route preference.	The value is an integer that ranges from 1 to 255. A smaller value indicates a higher preference.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

A DHCP client can obtain the default route through the DHCP server to dynamically update the routing table. The next-hop address of the default route is the DHCP client's gateway address carried in Option3.

The default route that a DHCP server delivers is the user network router (UNR) route with the default preference 60. You can run the **dhcp client default-route preference** command to change the default route preference.

Example

In the view of VLANIF100, set the default route preference that a DHCP server delivers to a DHCP client to 30.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client default-route preference 30
```

In the view of GE0/0/1, set the default route preference that a DHCP server delivers to a DHCP client to 30.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client default-route preference 30
```

6.3.13 dhcp client expected-lease

Function

The **dhcp client expected-lease** command enables expected lease on a DHCP client.

The **undo dhcp client expected-lease** command disables expected lease on a DHCP client.

By default, expected lease is disabled on the DHCP client.

Format

dhcp client expected-lease *time*

undo dhcp client expected-lease

Parameters

Parameter	Description	Value
time	Specifies an expected lease for a DHCP client.	The value is an integer that ranges from 60 to 864000, in seconds.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp client expected-lease** command applies to DHCP clients. An expected lease can be contained in Option 51 of a DHCP Request message sent to the server. The server compares the expected lease with the lease in the address pool and assigns a shorter lease to the client.

Example

Set the expected lease to 7200s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client expected-lease 7200
```

Set the expected lease to 7200s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client expected-lease 7200
```

6.3.14 dhcp client gateway-detect

Function

The **dhcp client gateway-detect** command enables gateway detection on a DHCP client.

The **undo dhcp client gateway-detect** command disables gateway detection on a DHCP client.

By default, gateway detection is disabled on a DHCP client.

Format

dhcp client gateway-detect period *period* **retransmit** *retransmit* **timeout** *time*

undo dhcp client gateway-detect

Parameters

Parameter	Description	Value
period *period*	Specifies an interval for gateway detection on a DHCP client.	The value is an integer that ranges from 1 to 86400, in seconds.
retransmit *retransmit*	Specifies the retransmission count of gateway detection on a DHCP client.	The value is an integer that ranges from 1 to 10.

Parameter	Description	Value
timeout *time*	Specifies the timeout period of gateway detection on a DHCP client.	It is an integer that ranges from 300 to 2000, in milliseconds.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp client gateway-detect** command applies to DHCP clients. After a DHCP client obtains an IP address, the **dhcp client gateway-detect** command enables the DHCP client to detect the status of the gateway being used. If the gateway has an incorrect address or the gateway device fails, the DHCP client requests a new IP address from the DHCP server.

Precautions

Gateway detection applies to dual-homed scenarios.

Example

Enable gateway detection on VLANIF100 of the DHCP client. Set the detection interval to 3600s, retransmission count to 3, and timeout period to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client gateway-detect period 3600 retransmit 3 timeout 500
```

Enable gateway detection on GE0/0/1 of the DHCP client. Set the detection interval to 3600s, retransmission count to 3, and timeout period to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client gateway-detect period 3600 retransmit 3 timeout 500
```

6.3.15 dhcp client hostname

Function

The **dhcp client hostname** command configures a host name for a DHCP/BOOTP client.

The **undo dhcp client hostname** command deletes the configured host name of a DHCP/BOOTP client.

By default, no host name is configured for a DHCP/BOOTP client.

Format

dhcp client hostname *hostname*

undo dhcp client hostname

Parameters

Parameter	Description	Value
hostname	Specifies the name of a DHCP/BOOTP client.	The value is a string of 1 to 64 case-sensitive characters.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A DHCP server must obtain the host name of a client before assigning an IP address to the client. To configure a host name for a DHCP/BOOTP client, run the **dhcp client hostname** command. The host name is used to match the local domain name of the DHCP/BOOTP client.

Follow-up Procedure

After DHCP/BOOTP client is enabled, the device can use DHCP to obtain an IP address.

Example

Set the host name of a DHCP/BOOTP client to **gateway1** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client hostname gateway1
```

Set the host name of a DHCP/BOOTP client to **gateway1** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client hostname gateway1
```

6.3.16 dhcp client renew

Function

The **dhcp client renew** command renews the lease of the IP address obtained by a DHCP client.

Format

dhcp client renew

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

This command applies to the following scenarios:

- Manually renewing the lease

  If a DHCP server assigns the original IP address to the client, only the lease is renewed. If another DHCP server assigns an IP address to the client, the client obtains a new IP address and related network parameters.
- Updating the IP address

  When the DHCP client is migrated from a network segment to another network segment and the original IP address lease does not expire, the client needs to update the IP address.

After the **dhcp client renew** command is run, the DHCP client sends a lease renewal request to the DHCP server.

- If the DHCP client receives a positive reply from the server, the client updates the parameters such as the lease duration.
- If the DHCP client receives a negative reply from the server, the client releases the applied parameters and re-applies to the DHCP server for an IP address and other network parameters.

- If no reply is received, the client does not perform any operation.

The **dhcp client renew** command can be normally run only after the DHCP client function is enabled on the interface and an IP address is obtained.

Example

Renew the IP address lease on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client renew
```

Renew the IP address lease on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client renew
```

6.3.17 dhcp client request option-list exclude

Function

The **dhcp client request option-list exclude** command configures a list of default request options that are not carried in the Option55 field of DHCP Request messages.

The **undo dhcp client request option-list exclude** command deletes the list of default request options that are not carried in the Option55 field of DHCP Request messages.

By default, the device does not configure the option to be excluded from the DHCP client request list.

Format

dhcp client request option-list exclude *option-code* &<1-8>

undo dhcp client request option-list exclude *option-code* &<1-8>

Parameters

Parameter	Description	Value
option-code	Specifies a list of default request options that are excluded from the Option55 field.	The value is of enumerated type and can be 3, 6, 15, 28, 33, 44, 121, and 184.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The Option55 field in DHCP Request messages is used to set the request option list. DHCP clients use this option to specify network configuration parameters that need to be obtained from the DHCP server. You can run the **dhcp client request option-list exclude** command to configure a list of default options that are excluded from the Option55 field based on network requirements.

For option meanings, see *DHCP Options* in *Configuration- IP Service Configuration Guide - DHCP Configuration*.

Example

Configure the default request option 3 to be excluded from the Option55 field in DHCP Request messages on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client request option-list exclude 3
```

6.3.18 dhcp client request option-list

Function

The **dhcp client request option-list** command configures a list of request options that the Option55 field in DHCP Request packets carries besides the default options.

The **undo dhcp client request option-list** command deletes a list of request options that the Option55 field in DHCP Request packets carries besides the default options.

By default, the Option 55 field in DHCP Request packets carries only default request options.

Format

dhcp client request option-list *option-code* &<1-9>

undo dhcp client request option-list *option-code* &<1-9>

Parameters

Parameter	Description	Value
option-code	Specifies a list of request options that the Option55 field carries besides the default options.	The value is of enumerated type and can be 4, 7, 17, 42, 43, 66, 67, 120, and 129.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The Option55 field in DHCP Request packets is used to set the request option list. DHCP clients use this option to specify network configuration parameters that need to be obtained from the DHCP server. Besides the default options, you can run the **dhcp client request option-list option-code** command to set a list of other request options that the Option55 field carries.

For option meanings, see *DHCP Options* in *Configuration- IP Service Configuration Guide - DHCP Configuration*.

Example

Configure the Option55 field in DHCP Request packets to carry option 4 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client request option-list 4
```

6.3.19 dhcp enable

Function

The **dhcp enable** command enables the DHCP function.

The **undo dhcp enable** command disables the DHCP function.

By default, the DHCP function is disabled.

NOTE

When a device of any of the following models does not work as a DHCP server or DHCP relay, do not configure this command; otherwise, users may go online slowly: S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S.

Format

dhcp enable

undo dhcp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the network scale expands and the network complexity increases, network configurations become more and more complex. For example, computers frequently change their locations, and IP addresses are insufficient for these computers. The DHCP protocol is developed to address these problems. The **dhcp enable** command enables the DHCP function on the device.

Precautions

The **dhcp enable** command is the prerequisite for configuring DHCP-related functions, including DHCP relay, DHCP snooping, and DHCP server. These functions take effect only after the **dhcp enable** command is run. After the **undo dhcp enable** command is run, all DHCP-related configurations of the device are deleted. After DHCP is enabled again using the **dhcp enable** command, all DHCP-related configurations of the device are restored to the default configurations.

Example

Enable the DHCP function on the device.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
```

6.3.20 dhcp relay anycast gateway re-route enable

Function

The **dhcp relay anycast gateway re-route enable** command enables the re-routing function for the DHCP relay agent on a distributed gateway.

The **undo dhcp relay anycast gateway re-route enable** command disables the re-routing function for the DHCP relay agent on a distributed gateway.

By default, the re-routing function for the DHCP relay agent on a distributed gateway is disabled.

NOTE

This command is supported on the following devices: S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI.

Format

dhcp relay anycast gateway re-route enable

undo dhcp relay anycast gateway re-route enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a distributed VXLAN gateway scenario, the DHCP relay function is configured on VBDIF interfaces of distributed gateways. The value of the GIADDR field carried in a request packet sent from a DHCP relay agent to the DHCP server is the IP address of the VBDIF interface. When returning a response packet, the DHCP server figures out the network segment on which the DHCP client resides based on information of this field. However, the response packet from the DHCP server may be forwarded to other distributed gateways (rather than the device that sends the request packet) because IP addresses of VBDIF interfaces on distributed gateways are the same. As a result, the user cannot obtain an IP address.

To resolve the preceding problem, you can enable the re-routing function for DHCP relay agents on VBDIF interfaces of the distributed gateways. After this function is enabled, when a DHCP relay agent sends a request packet, the VTEP IP address of the local device, functioning as the return IP address, is carried in the Option82 field; when a DHCP relay agent returns a response packet, the VTEP IP address of the local device is also carried in the packet. When processing a response packet from the DHCP server, the DHCP relay agent figures out whether the response packet corresponds to the request packet sent from the local device based on the return IP address carried in the packet. If so, the DHCP relay agent forwards the packet to the client. If not, the DHCP relay agent performs re-routing based on the return IP address to forward the response packet to the corresponding distributed gateway through a VXLAN tunnel.

Prerequisites

The DHCP relay function has been enabled using the **dhcp select relay** command in the VBDIF interface view.

Precautions

Because the return IP address is carried in the Option82 field, you need to perform the following operations:

1. Run the **dhcp option82 vendor-specific format vendor-sub-option 2 ip-address** *ip-address* command in the system view to use the Sub Option2 field that is customized by the vendor in the Option82 field to carry the VTEP IP address of the local device.
2. Run the **dhcp option82 encapsulation vendor-specific-id** command in the BD view to insert the sub-option customized by the vendor into the Option82 field.
3. Run the **dhcp option82** { **insert** | **rebuild** } **enable** command in the BD view to configure the Option82 field to be inserted into DHCP packets.
4. (Optional) Run the **dhcp relay information enable** command in the VBDIF interface view to enable the Option 82 function for the DHCP relay agent.

Example

Enable the re-routing function for the DHCP relay agent on VBDIF100 of a distributed gateway.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] bridge-domain 100
[HUAWEI-bd100] quit
[HUAWEI] interface vbdif 100
[HUAWEI-Vbdif100] dhcp select relay
[HUAWEI-Vbdif100] dhcp relay anycast gateway re-route enable
```

6.3.21 dhcp option template

Function

The **dhcp option template** command creates a DHCP Option template and enters the DHCP Option template view.

The **undo dhcp option template** command deletes a configured DHCP Option template.

By default, no DHCP Option template is created on the device.

Format

dhcp option template *template-name*

undo dhcp option template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of the DHCP Option template.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain digits, letters, underscores (_), hyphens (-), and dots (.), but cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. During network deployment, a DHCP server dynamically allocates IP addresses with leases to clients or allocates fixed IP addresses to some clients. For example, laptops or terminals are often moved to different places in enterprises, and they can obtain IP addresses using the dynamic allocation mode. However, IP addresses obtained dynamically are randomly allocated, and cannot be set to specified IP addresses. To allocate fixed IP addresses to some fixed terminals (such as IP phones), run the **static-bind** command in the global address view to bind IP addresses to MAC addresses of the clients so that the clients are allocated fixed IP addresses.

In some cases, you need to allocate other network configuration parameters except IP addresses to fixed static terminals. For example, besides obtaining an IP address, an IP phone needs information such as the startup configuration file to register normally. In this case, you can configure a DHCP Option template and configure network configuration parameters except the IP address required by the client in the DHCP Option template. Then bind the DHCP Option template to the fixed terminal in the global address pool. The DHCP server then allocates the IP address and other parameters to the terminal.

Precautions

Network parameters configured in the DHCP Option template view take effect only for static clients. A DHCP Option template can be bound to multiple clients.

Run the **static-bind ip-address** *ip-address* **mac-address** *mac-address* [**option-template** *template-name*] command to configure a DHCP Option template that is bound to static clients.

Example

Create a DHCP Option template named **test**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template test
```

6.3.22 dhcp relay gateway-switch enable

Function

The **dhcp relay gateway-switch enable** command enables automatic gateway switching on the DHCP relay agent.

The **undo dhcp relay gateway-switch enable** command disables automatic gateway switching on the DHCP relay agent.

By default, automatic gateway switching is disabled on the DHCP relay agent.

Format

dhcp relay gateway-switch enable

undo dhcp relay gateway-switch enable

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp relay gateway-switch enable** command is used on DHCP relay agents. This command allows a DHCP relay agent to use a secondary IP address as the gateway address to apply for IP addresses for users when it has failed to use the primary IP address to apply for user IP addresses.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command in the system view. DHCP relay has been enabled on an interface by using the **dhcp select relay** command.

Precautions

- After VRRP is configured, if the interface (enabled with DHCP relay) has a primary IP address and several secondary IP addresses, the DHCP relay agent by default uses the virtual IP address first configured for the VRRP group to apply for IP addresses for users. If IP addresses fail to be applied for, the DHCP relay agent tries other virtual IP addresses of the VRRP group one by one based on the VRRP virtual IP address configuration sequence until users successfully obtain IP addresses.
- The DHCP relay agent switches the gateway address from the primary to a secondary IP address only when it has failed to apply an IP address for a user using the primary IP address at least three times and the interval between the first and last failures exceeds 24 seconds.
- Before running this command on an interface, ensure that the interface has a primary IP address and at least one secondary IP address.
- An interface can have a primary IP address and several secondary IP addresses. The system tries the secondary IP addresses one by one based on the IP address configuration sequence until users successfully obtain IP addresses.

Example

Enable automatic gateway switching on DHCP relay-enabled VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 192.168.30.1 255.255.255.0
[HUAWEI-Vlanif10] ip address 192.168.31.1 255.255.255.0 sub
[HUAWEI-Vlanif10] dhcp select relay
[HUAWEI-Vlanif10] dhcp relay server-ip 192.168.20.1
[HUAWEI-Vlanif10] dhcp relay gateway-switch enable
```

Enable automatic gateway switching on DHCP relay-enabled GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.30.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.31.1 255.255.255.0 sub
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip 192.168.20.1
[HUAWEI-GigabitEthernet0/0/1] dhcp relay gateway-switch enable
```

6.3.23 dhcp relay giaddr source-interface

Function

The **dhcp relay giaddr source-interface** command configures a source interface for relayed DHCP messages and fills the primary IP address of the source interface in the giaddr field of these messages.

The **undo dhcp relay giaddr source-interface** command restores the default configuration.

By default, no source interface for relayed DHCP messages is configured, and the IP address of the DHCP relay agent is filled in the giaddr field of these messages.

NOTE

This command is supported on the following devices: S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI.

Format

dhcp relay giaddr source-interface *interface-type interface-number*

undo dhcp relay giaddr source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies a source interface for relayed DHCP messages. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network with distributed VXLAN gateways where VBDIF interfaces are enabled with the DHCP relay function, a distributed gateway (as a DHCP relay agent) fills the IP address of its VBDIF interface in the giaddr field of a DHCP DISCOVER message to be sent to DHCP servers. When replying with a DHCP OFFER message, a DHCP server sets the destination IP address to the IP address of the VBDIF interface in the giaddr field carried in its received DHCP DISCOVER message. However, since the IP addresses of VBDIF interfaces on different distributed gateways are the same, the DHCP OFFER message from a DHCP server may be forwarded to a distributed gateway rather than the one relaying the DHCP DISCOVER message received by the server. As a result, the user sending the DHCP DISCOVER message cannot obtain an IP address.

To resolve this issue, you can configure a source interface for relayed DHCP messages on VBDIF interfaces of all distributed gateways. The distributed gateways (as DHCP relay agents) then fill the primary IP address of the specified source interface in the giaddr field of DHCP DISCOVER messages to be relayed to DHCP servers. Since the primary IP address of the source interface configured on each VBDIF interface is unique among all distributed gateways, as long as this IP address is reachable to DHCP servers, the DHCP OFFER messages from DHCP servers can be sent to the correct distributed gateways.

Prerequisites

DHCP relay has been enabled using the **dhcp select relay** command in the VBDIF interface view.

Follow-up Procedure

By default, a DHCP server selects an IP address from the address pool on the network segment specified in the giaddr field of its received DHCP DISCOVER messages. After this command is run to configure a source interface for relayed DHCP messages on a DHCP relay-enabled interface (which is the gateway for its downlink DHCP clients), the primary IP address of the specified source interface is filled in the giaddr field of DHCP DISCOVER messages destined for DHCP servers. If DHCP servers still select an IP address from the address pool on the network segment specified in the giaddr field, DHCP clients cannot access the network after obtaining IP addresses. This is because the primary IP address of the source interface is on a different network segment from that of the DHCP relay-enabled interface. To resolve the preceding problem, you need to run the **dhcp relay information link-selection insert enable** command to insert the Link-selection sub-option of the Option82 field into relayed DHCP DISCOVER messages, and to fill the IP address of the DHCP relay-enabled interface in the Link-selection suboption. In this case, DHCP servers select IP addresses from the address pool on the network segment specified in the Link-selection sub-option of the Option 82 field of their received DHCP DISCOVER messages.

Precautions

- The primary IP address of the source interface for relayed DHCP messages must be reachable to DHCP servers.
- The source interface and VBDIF interfaces enabled with the DHCP relay function can be bound to different VPNs.
- The DHCP server must be able to parse the Link-selection sub-option.

Example

On VBDIF 100, configure Loopback 1 as the source interface for relayed DHCP messages.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.1.1 24
[HUAWEI-LoopBack1] quit
[HUAWEI] dhcp enable
[HUAWEI] bridge-domain 100
[HUAWEI-bd100] quit
[HUAWEI] interface vbdif 100
[HUAWEI-Vbdif100] dhcp select relay
[HUAWEI-Vbdif100] dhcp relay giaddr source-interface loopback 1
```

6.3.24 dhcp relay information enable

Function

The **dhcp relay information enable** command enables the Option 82 function for the DHCP relay agent.

The **undo dhcp relay information enable** command disables the Option 82 function for the DHCP relay agent.

By default, the Option 82 function is disabled for the DHCP relay agent.

Format

dhcp relay information enable

undo dhcp relay information enable

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP relay agent. When DHCP Request messages carry Option 82 information, the DHCP server can locate user positions accurately and assign IP addresses to users using different policies. After the Option 82 function is enabled on the DHCP relay agent, the device checks the Option 82 field contained in the packets and processes the packets using corresponding policies.

Prerequisites

DHCP has been enabled by running the **dhcp enable** command in the system view.

DHCP relay has been enabled by running the **dhcp select relay** command in the interface view.

Precautions

If you run the **dhcp relay information enable** command on an interface and the **dhcp option82** { **insert** | **rebuild** } **enable** command in the VLAN view or on a physical interface in the VLAN simultaneously, only the **dhcp relay information enable** command takes effect.

Follow-up Tasks

Run the **dhcp relay information strategy** { **drop** | **keep** | **replace** } command in the interface view to configure strategies for the DHCP relay agent to process Option 82 information.

Example

Enable the Option 82 function for the DHCP relay agent on the VLANIF100 interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] dhcp relay information enable
```

Enable the Option 82 function for the DHCP relay agent on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay information enable
```

6.3.25 dhcp relay information strategy

Function

The **dhcp relay information strategy** command configures the strategies used by a DHCP relay agent to process Option 82 information.

The **undo dhcp relay information strategy** command restores the default setting.

By default, the strategy used by a DHCP relay agent to process Option 82 information is **replace**.

Format

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

Parameters

Parameters	Description	Value
drop	Configures the DHCP relay agent to drop Option 82 information.	-

Parameters	Description	Value
keep	Configures the DHCP relay agent to keep Option 82 information.	-
replace	Configures the DHCP relay agent to replace Option 82 information.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP relay agent. When DHCP Request messages carry Option 82 information, the DHCP server can locate user positions accurately and assign IP addresses to users using different policies. When a DHCP relay agent receives DHCP Request messages, it uses one of the following strategies to process Option 82 information:

- Drop:
  - If the received DHCP message does not carry an Option 82 field, the DHCP relay agent forwards the message directly without processing it.
  - If the received DHCP message carries an Option 82 field, the DHCP relay agent drops the Option 82 field and forwards the message.
- Keep:
  - If the received DHCP message does not carry an Option 82 field, the DHCP relay agent forwards the message directly without processing it.
  - If the received DHCP message carries an Option 82 field, the DHCP relay agent keeps the Option 82 field and forwards the message.
- Replace:
  - If the received DHCP message does not carry an Option 82 field, the DHCP relay agent inserts an Option 82 field configured by the administrator into the received message and forwards the message.
  - If the received DHCP message carries an Option 82 field, the DHCP relay agent replaces it with the Option 82 field configured by the administrator and forwards the message.

Prerequisites

DHCP has been enabled by running the **dhcp enable** command in the system view.

DHCP relay has been enabled by running the **dhcp select relay** command in the interface view.

The Option 82 function has been enabled for the DHCP relay agent by using the **dhcp relay information enable** command.

Example

Configure the DHCP relay agent to drop Option 82 information on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] dhcp relay information enable
[HUAWEI-Vlanif100] dhcp relay information strategy drop
```

Configure the DHCP relay agent to drop Option 82 information on the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay information enable
[HUAWEI-GigabitEthernet0/0/1] dhcp relay information strategy drop
```

6.3.26 dhcp relay information link-selection insert enable

Function

The **dhcp relay information link-selection insert enable** command inserts the Link-selection sub-option of the Option82 field into DHCP messages.

The **undo dhcp relay information link-selection insert enable** command restores the default configuration.

By default, the Link-selection sub-option of the Option82 field is not inserted into DHCP messages.

NOTE

This command is supported on the following devices: S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI.

Format

dhcp relay information link-selection insert enable

undo dhcp relay information link-selection insert enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network with VXLAN distributed gateways as DHCP relay agents, to ensure that the DHCP OFFER messages from DHCP servers can arrive at the correct distributed gateways, you need to run the **dhcp relay giaddr source-interface** command on the distributed gateways to configure a source interface for relayed DHCP messages and fill the primary IP address of the source interface in the giaddr field. By default, DHCP servers select IP addresses from the address pool on the network segment specified in the giaddr field of their received DHCP DISCOVER messages. After the preceding command is run, since the primary IP address of the source interface is on a different network segment from that of the DHCP relay-enabled interface (which is the gateway for its downlink DHCP clients), if DHCP servers still select IP addresses from the address pool on the network segment specified in the giaddr field, DHCP clients cannot access the network after obtaining IP addresses.

To solve the preceding problem, run the **dhcp relay information link-selection insert enable** command to insert the Link-selection sub-option of the Option82 field into DHCP DISCOVER messages forwarded by the DHCP relay agent, and to fill in the IP address of the DHCP relay-enabled interface in the Link-selection sub-option. In this case, DHCP servers select IP addresses from the address pool on the network segment specified in the Link-selection sub-option of the Option 82 field of their received DHCP DISCOVER messages.

Prerequisites

DHCP relay has been enabled using the **dhcp select relay** command in the VBDIF interface view.

Precautions

- DHCP servers must be able to parse the Link-selection sub-option.
- After the **dhcp relay information link-selection insert enable** command is run, the Link-selection sub-option is added to DHCP messages, removing the need to configure policies for Option 82 insertion and processing. A DHCP relay agent processes the Link-selection sub-option in different ways depending on the policies for Option 82 insertion and processing:
  - Without policies for Option 82 insertion and processing: The DHCP relay agent inserts the Option 82 field with the Link-selection sub-option into DHCP messages. When forwarding a DHCP message with the Option 82 field, the DHCP relay agent deletes the original Option 82 field and inserts the locally configured Option 82 field with the Link-selection sub-option.
  - With policies for Option 82 insertion and processing: How the DHCP relay agent inserts the Link-selection sub-option into DHCP messages is

determined by the configured policies. For example, if the Option 82 insertion mode is set to **insert**, the DHCP relay agent does not insert the Link-selection sub-option into DHCP messages when receiving DHCP messages carrying the Option 82 field.

You can run the **dhcp option82** { **insert** | **rebuild** } **enable** command to configure the Option 82 insertion mode, and run the **dhcp relay information enable** and **dhcp relay information strategy** { **drop** | **keep** | **replace** } commands to configure an Option 82 processing policy.

Example

On VBDIF 100, configure the function of inserting the Link-selection sub-option of the Option82 field into DHCP messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] bridge-domain 100
[HUAWEI-bd100] quit
[HUAWEI] interface vbdif 100
[HUAWEI-Vbdif100] dhcp select relay
[HUAWEI-Vbdif100] dhcp relay information link-selection insert enable
```

6.3.27 dhcp relay release

Function

The **dhcp relay release** command configures a DHCP relay agent to send a release message to a DHCP server for releasing the IP address assigned to a DHCP client.

Format

In the system view:

dhcp relay release *client-ip-address mac-address* [**vpn-instance** *vpn-instance-name*] [*server-ip-address*]

In the interface view:

dhcp relay release *client-ip-address mac-address* [*server-ip-address*]

Parameters

Parameter	Description	Value
client-ip-address	Specifies the IP address of a DHCP client.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address of a DHCP client.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
server-ip-address	Specifies the IP address of a DHCP server. If this parameter is specified, a DHCP relay agent sends a release message to the specified DHCP server for releasing the IP address assigned to a DHCP client.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified DHCP server releasing IP addresses belongs.	The value must be an existing VPN instance name.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. In some situations, for example, a user is forced to go offline, the user's IP address is no longer used. However, the user cannot access the network, and will not send a DHCP release message to the DHCP server to release the IP address assigned by the DHCP server. Before the IP address lease expires, the DHCP server will not assign the user's IP address to another client, wasting IP addresses. In this case, you can run the **dhcp relay release** command to configure a DHCP relay agent to send a DHCP release message to the DHCP server. After receiving the message, the DHCP server sets the status of the IP address to idle. The DHCP server then can assign the released IP address to another client.

If a DHCP server IP address is specified, the DHCP relay agent sends an address release request only to the specified DHCP server. If no DHCP server address is specified, the following situations occur:

- When the **dhcp relay release** command is run in the system view, the DHCP relay agent sends an address release request to DHCP servers on all the interfaces working in DHCP relay mode.

- When the **dhcp relay release** command is run in the interface view, the DHCP relay agent sends an address release request to all DHCP servers on the VLANIF interface.

Precautions

The **dhcp relay release** command only releases the IP addresses dynamically assigned by DHCP servers.

When multiple DHCP relay agents are connected between the DHCP client and server, this command must be executed on the first DHCP relay agent.

Example

Configure a DHCP relay agent to send a release message to the DHCP server at 10.1.1.1 for releasing the IP address 192.168.1.1 assigned to the DHCP client whose MAC address is 00e0-fc34-2000.

```
<HUAWEI> system-view
[HUAWEI] dhcp relay release 192.168.1.1 00e0-fc12-3456 10.1.1.1
```

6.3.28 dhcp relay request server-match enable

Function

The **dhcp relay request server-match enable** command configures a DHCP relay agent to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

The **undo dhcp relay request server-match enable** command configures a DHCP relay agent not to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

By default, a DHCP relay agent checks the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

Format

dhcp relay request server-match enable

undo dhcp relay request server-match enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the four-message exchange process, the DHCP Offer message sent by a DHCP server carries the DHCP server identifier (Option54) to identify the server. After receiving the DHCP Offer message, the DHCP client records the DHCP server identifier and carries it in the DHCP Request message to be replied to indicate which DHCP server is selected. When the DHCP relay agent forwards the DHCP Request message, it checks the DHCP server identifier in the message and forwards the message only to the corresponding DHCP server.

If multiple DHCP servers are deployed on the network and the design of a server does not comply with standards, the DHCP server identifier carried in the DHCP Offer message to be sent by the server is not its identifier. As a result, the DHCP server identifier carried in the DHCP Request message is incorrect, the DHCP relay agent forwards the message to an incorrect DHCP server rather than the matching DHCP server, and the client fails to obtain an IP address.

To resolve this issue, you can run the **undo dhcp relay request server-match enable** command, so that the DHCP relay agent does not check the DHCP server identifier (Option54) in the DHCP Request message to be forwarded and forwards the message to all relayed DHCP servers, ensuring that the matching DHCP server can receive the DHCP Request message.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Configure a DHCP relay agent not to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] undo dhcp relay request server-match enable
```

6.3.29 dhcp relay reply forward all enable

Function

The **dhcp relay reply forward all enable** command configures a DHCP relay agent to forward all DHCP ACK messages.

The **undo dhcp relay reply forward all enable** command restores the default setting.

By default, a DHCP relay agent forwards only the first received DHCP ACK message.

Format

dhcp relay reply forward all enable

undo dhcp relay reply forward all enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in RFC2131, the DHCP server that provides only IP addresses for DHCP clients replies with DHCP ACK messages. After receiving a DHCP ACK message, a DHCP relay agent searches for the entry based on the DHCP client's MAC address contained in the message, forwards the message to the corresponding client, and then immediately deletes the entry matching the client.

If multiple DHCP servers are deployed on the network, the design of a server does not comply with standards, and a DHCP client requests for an IP address, the server does not provide an IP address for the DHCP client but replies with a DHCP ACK message. If the DHCP relay agent first receives the DHCP ACK message replied by the server, it incorrectly forwards the message to the client and deletes the corresponding entry. After the DHCP relay agent receives the correct DHCP ACK message, it cannot forward the message because the entry matching the client has been deleted. As a result, the client cannot obtain an IP address.

To resolve this issue, you can run the **dhcp relay reply forward all enable** command, so that the DHCP relay agent does not immediately delete the entry matching a client after forwarding a DHCP ACK message to the client. Instead, the DHCP relay agent deletes the entry that has been aged out to ensure that the subsequently received DHCP ACK messages can be forwarded to the client.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Configure a DHCP relay agent to forward all DHCP ACK messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp relay reply forward all enable
```

6.3.30 dhcp relay server-ip

Function

The **dhcp relay server-ip** command configures a DHCP server address on an interface enabled with DHCP relay.

The **undo dhcp relay server-ip** command deletes the configured DHCP server addresses on an interface enabled with DHCP relay.

By default, no DHCP server IP address is configured on an interface enabled with DHCP relay.

Format

dhcp relay server-ip [**vpn-instance** *vpn-name* | **public-net**] *ip-address*

undo dhcp relay server-ip { [**vpn-instance** *vpn-name* | **public-net**] *ip-address* | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-name*	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.
public-net	Indicates that the public network is used to forward packets.	-
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.
all	Deletes all the DHCP server IP addresses configured on an interface.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. When a DHCP client needs to send a DHCP DISCOVER message to a DHCP server on a different network segment through a DHCP relay agent, you must configure the DHCP server IP address on the DHCP relay agent. If the DHCP server and DHCP client are not in the same VPN, you also need to specify the VPN where the DHCP server resides.

When a DHCP relay agent forwards a DHCP DISCOVER message, it does not check whether the DHCP server is Down. If multiple DHCP server addresses are configured on an interface, multiple DHCP servers respond with DHCP OFFER messages to the DHCP client. However, the DHCP client uses the first received DHCP OFFER message. As a result, IP addresses in the IP address pool on the first DHCP server are insufficient, but available IP addresses in the IP address pools on the other DHCP servers are not allocated. To make each DHCP server allocate the same number of IP addresses, a DHCP relay agent changes the forwarding order each time it forwards a DHCP DISCOVER message, so that load balancing is implemented among DHCP servers. A DHCP relay agent forwards a DHCP DISCOVER message as follows:

- The DHCP relay agent forwards the message to all DHCP servers by default, and changes the forwarding order each time it forwards a DHCP DISCOVER message.
- You can configure the **ip relay address cycle** command to reduce the number of messages received by a DHCP server and lessen the load of a DHCP server. After this command is configured, the DHCP relay agent forwards a received DHCP DISCOVER message to one DHCP server at a time, and forwards the DHCP DISCOVER message to a different DHCP server each time it receives the message.

Prerequisites

DHCP relay has been enabled on the interface using the **dhcp select relay** command.

Precautions

To configure multiple DHCP server IP addresses, run this command for multiple times.

Each interface enabled with DHCP relay can be configured with a maximum of 20 DHCP server IP addresses.

If the interface enabled with DHCP relay is bound to a VPN instance but no VPN instance is specified for the DHCP server served by the DHCP relay agent, the DHCP relay agent sends packets through the VPN instance to which the interface belongs by default. If a VPN instance is specified for the DHCP server, the DHCP relay agent sends packets through the VPN instance specified for the DHCP server.

Example

Configure DHCP relay and three DHCP server IP addresses on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] dhcp select relay
[HUAWEI-Vlanif10] dhcp relay server-ip 10.1.1.2
[HUAWEI-Vlanif10] dhcp relay server-ip vpn-instance temp 10.1.1.3
[HUAWEI-Vlanif10] dhcp relay server-ip public-net 192.0.2.1
```

Configure DHCP relay and three DHCP server IP addresses on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip vpn-instance temp 10.1.1.3
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip public-net 192.0.2.1
```

6.3.31 dhcp relay server-select

Function

The **dhcp relay server-select** command configures a DHCP server group for a DHCP relay agent.

The **undo dhcp relay server-select** command deletes the configured DHCP server group of a DHCP relay agent.

By default, no DHCP server group is configured.

Format

dhcp relay server-select *group-name*

undo dhcp relay server-select

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp relay server-select** command applies to DHCP relay agents. When a DHCP client needs to send DHCP requests to a DHCP server using a DHCP relay agent, you can run the **dhcp relay server-select** command to specify a DHCP server group for the DHCP relay agent and configure the DHCP server address.

Prerequisites

1. A DHCP server group has been created using the **dhcp server group** command.
2. The DHCP relay function has been enabled using the **dhcp select relay** command so that the system can forward DHCP packets to the specified DHCP server.

Precautions

- Multiple interfaces can be configured with the same DHCP server group, and one interface can be configured with only one DHCP server group.
- If you run the **dhcp relay server-select** command in the same interface view for multiple times, only the latest configuration takes effect. If a specified DHCP server group does not exist, the configuration fails; however, the latest configured DHCP server group still takes effect.

Example

Configure the DHCP server group of a DHCP relay agent as **group1** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server group group1
[HUAWEI-dhcp-server-group-group1] dhcp-server 10.10.10.10
[HUAWEI-dhcp-server-group-group1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] dhcp relay server-select group1
```

Configure the DHCP server group of a DHCP relay agent as **group1** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server group group1
[HUAWEI-dhcp-server-group-group1] dhcp-server 10.10.10.10
[HUAWEI-dhcp-server-group-group1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-select group1
```

6.3.32 dhcp relay trust option82

Function

The **dhcp relay trust option82** command enables Option 82 on the DHCP relay agent.

The **undo dhcp relay trust option82** command disables Option 82 on the DHCP relay agent.

By default, Option 82 is enabled on the DHCP relay agent.

Format

dhcp relay trust option82

undo dhcp relay trust option82

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP relay agent to enable the Option 82 function. After receiving a DHCP packet that carries the Option 82 field but the giaddr field of the packet is 0, the DHCP relay agent processes the packet by default. Using the **undo dhcp relay trust option82** command, the DHCP relay agent discards the packet.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Example

Enable Option 82 trusted of the DHCP relay agent.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp relay trust option82
```

6.3.33 dhcp select global

Function

The **dhcp select global** command enables an interface to use the global address pool.

The **undo dhcp select global** command disables an interface from using the global address pool.

By default, an interface is disabled from using the global address pool.

Format

dhcp select global

undo dhcp select global

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select global** command applies to DHCP servers. After receiving a DHCP Request message from a DHCP client, a DHCP server assigns an IP address from the local address pool to the client. Run the **dhcp select global** command to configure the device to assign IP addresses from the global address pool. When no interface address pool is created for the DHCP server, the DHCP server assigns an IP address from the global address pool to an online user.

The device can also assign IP addresses from an interface address pool using the **dhcp select interface** command in the interface view.

Prerequisites

- DHCP has been enabled using the **dhcp enable** command in the system view.

Precautions

- When the device is configured as a DHCP server, if the server's real IP address is configured as the DHCP server IP address on a DHCP relay agent, the server's Layer 3 interface that receives relayed DHCP messages can process these messages, without the need of running the **dhcp select global** command on the interface.
- When the device is configured as a DHCP server, if the VRRP virtual IP address of the server's Layer 3 interface that does not receive DHCP messages is configured as the DHCP server IP address on the DHCP relay agent, the DHCP server cannot process messages relayed by the DHCP relay agent. The DHCP server can process messages relayed by the DHCP relay agent only if the VRRP virtual IP address of the server's Layer 3 interface that receives DHCP messages is configured as the DHCP server IP address on the DHCP relay agent and the **dhcp select global** command is configured on this Layer 3 interface.

Example

Enable VLANIF100 to use the global address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select global
```

Enable GE0/0/1 to use the global address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select global
```

6.3.34 dhcp select interface

Function

The **dhcp select interface** command enables an interface to use the interface address pool.

The **undo dhcp select interface** command disables an interface from using the interface address pool.

By default, the DHCP server function using the interface address pool is disabled on an interface.

Format

dhcp select interface

undo dhcp select interface

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select interface** command applies to DHCP servers. After receiving a DHCP Request message from a DHCP client, a DHCP server assigns an IP address from the local address pool to the client. Run the **dhcp select interface** command to configure a DHCP server to assign IP addresses from the interface address pool to clients.

The device can also assign IP addresses from a global address pool using the **dhcp select global** command.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

An IP address has been configured for an interface using the **ip address** command. The IP addresses assigned by the address pool and configured on the interface are on the same network segment.

Example

Enable VLANIF100 to use the interface address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.2 24
[HUAWEI-Vlanif100] dhcp select interface
```

Enable GE0/0/1 to use the interface address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
```

6.3.35 dhcp select relay

Function

The **dhcp select relay** command enables the DHCP relay function.

The **undo dhcp select relay** command disables the DHCP relay function.

By default, the DHCP relay function is disabled.

Format

dhcp select relay

undo dhcp select relay

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select relay** command applies to DHCP relay agents. If the DHCP server and client are on the same network segment, they can directly communicate with each other using DHCP. In this case, no DHCP relay agent is needed. If the DHCP server and client are on different network segments, the DHCP relay function must be enabled to forward DHCP messages.

Prerequisites

The DHCP function has been enabled using the **dhcp enable** command in the system view.

Follow-up Tasks

- To ensure that a DHCP relay agent can forward DHCP packets to a DHCP server, run the **dhcp relay server-select** or **dhcp relay server-ip** command on the DHCP relay-enabled interface to configure the correct IP address of the DHCP server.
- To ensure that a DHCP server can forward DHCP packets to a DHCP relay agent, you must configure a route to the DHCP relay agent on the DHCP server.

Precautions

- The DHCP server must select an IP address in the same network segment with the DHCP relay agent from the global address pool to ensure that the DHCP client obtains an IP address on the local network segment. No interface address pool can be configured on the interface that connects the DHCP server and relay agent.

Example

Enable the DHCP relay function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
```

Enable the DHCP relay function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
```

6.3.36 dhcp server alarm ip-used percentage

Function

The **dhcp server alarm ip-used percentage** command configures the percentage of used addresses in an interface address pool at which an address exhaustion alarm is generated and the percentage at which the alarm is cleared.

The **undo dhcp server alarm ip-used percentage** command restores the default percentage of used addresses in an interface address pool at which an address exhaustion alarm is generated and the default percentage at which the alarm is cleared.

By default, an alarm is generated when the percentage of used addresses in an interface address pool reaches 100%, and the alarm is cleared when the percentage is 50%.

Format

dhcp server alarm ip-used percentage *alarm-resume-percentage alarm-percentage*

undo dhcp server alarm ip-used percentage

Parameters

Parameter	Description	Value
alarm-resume-percentage	Specifies the percentage of used addresses in an interface address pool at which an address exhaustion alarm is cleared.	The value is an integer that ranges from 1 to 100. The default value is 50. **NOTE** The percentage of used addresses in an interface address pool at which the address exhaustion alarm is cleared cannot exceed the percentage at which an address exhaustion alarm is generated.
alarm-percentage	Specifies the percentage of used addresses in an interface address pool at which an address exhaustion alarm is generated.	The value is an integer that ranges from 1 to 100. The default value is 100.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the addresses in an interface address pool are used up, an address exhaustion alarm is generated to notify the administrator. The alarms corresponding to this command are as follows:

- When the number of used IP addresses in an IP address pool reaches the alarm threshold, the alarm hwUsedIPReachThreshold with ID 1.3.6.1.4.1.2011.6.8.2.2.0.6 is generated.
- When the number of used IP addresses in an IP address pool falls below the alarm clear threshold, the alarm hwUsedIPReachThresholdResume with the ID 1.3.6.1.4.1.2011.6.8.2.2.0.7 is generated.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

The percentage of used addresses in an interface address pool at which the address exhaustion alarm is cleared cannot exceed the percentage at which an address exhaustion alarm is generated.

Example

Configure the percentage of used IP addresses in the interface address pool of VLANIF 100 at which an address exhaustion alarm is generated and the percentage at which the alarm is cleared.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.10.10.10 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server alarm ip-used percentage 80 90
```

Configure the percentage of used IP addresses in the interface address pool of GE0/0/1 at which an address exhaustion alarm is generated and the percentage at which the alarm is cleared.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server alarm ip-used percentage 80 90
```

6.3.37 dhcp server bootfile

Function

The **dhcp server bootfile** command configures the name of the startup configuration file for a DHCP client.

The **undo dhcp server bootfile** command deletes the configured name of the startup configuration file for a DHCP client.

By default, the startup configuration file name is not configured for a DHCP client.

Format

dhcp server bootfile *bootfile*

undo dhcp server bootfile

Parameters

Parameter	Description	Value
bootfile	Specifies the name of the startup configuration file for a DHCP client.	The value is a string of 1 to 127 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP clients. After the name of the startup configuration file is configured using the **dhcp server bootfile** command, the Offer and ACK packets sent from the DHCP server carry this file name. The DHCP client can acquire the startup configuration file from the specified server based on the file name.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.

3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Configure the name of the startup configuration file as **start.ini** for the DHCP client on the Vlanif100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 255.255.255.0
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server bootfile start.ini
```

Configure the name of the startup configuration file as **start.ini** for the DHCP client on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server bootfile start.ini
```

6.3.38 dhcp server bootp

Function

Using the **dhcp server bootp** command, you can enable a DHCP server to respond to a Bootstrap Protocol (BOOTP) request.

Using the **undo dhcp server bootp** command, you can disable a DHCP server from responding to a BOOTP request.

By default, a DHCP server does not respond to a BOOTP request.

Format

dhcp server bootp

undo dhcp server bootp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A DHCP server and a BOOTP server may reside on the same network segment. The BOOTP server assigns static IP addresses to BOOTP clients. As defined in the DHCP protocol, a DHCP server can also respond to BOOTP requests to assign IP addresses to BOOTP clients. BOOTP clients may obtain IP addresses from the DHCP server but not the BOOTP server.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Follow-up Procedure

Using the **dhcp server bootp automatic** command in the system view, you can enable the DHCP server to allocate IP addresses to BOOTP clients.

Example

Enable a DHCP server to respond to a BOOTP request.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server bootp
```

6.3.39 dhcp server bootp automatic

Function

The **dhcp server bootp automatic** command enables the DHCP server to dynamically allocate IP addresses to BOOTP clients.

The **undo dhcp server bootp automatic** command disables the DHCP server from dynamically allocating IP addresses to BOOTP clients.

By default, a DHCP server does not dynamically allocate IP addresses to BOOTP clients.

Format

dhcp server bootp automatic

undo dhcp server bootp automatic

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When BOOTP clients need to obtain their IP addresses, DNS server's IP address, and gateway IP address from a DHCP server, you need to run the **dhcp server bootp automatic** command to enable the DHCP server to dynamically allocate IP addresses to BOOTP clients.

Prerequisites

- DHCP has been enabled globally using the **dhcp enable** command in the system view.
- The DHCP server has been enabled to respond to BOOTP requests by using the **dhcp server bootp** command, or **dhcp server bootp automatic** cannot take effect.

Precautions

When the device functions as the DHCP server, the device can allocate IP addresses to BOOTP clients if the BOOTP clients reside on the same network as the DHCP server. You can run the **dhcp server bootp automatic** command to dynamically allocate IP addresses. You can also run the **static-bind** command or the **dhcp server static-bind** command to allocate IP addresses to BOOTP clients in the static binding mode.

Example

Enable the DHCP server to allocate IP addresses to BOOTP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server bootp
[HUAWEI] dhcp server bootp automatic
```

6.3.40 dhcp server conflict auto-recycle interval

Function

The **dhcp server conflict auto-recycle interval** command enables automatic reclaim of conflicting IP addresses in the interface address pool and configures the interval for the automatic reclaim.

The **undo dhcp server conflict auto-recycle interval** command disables automatic reclaim of conflicting IP addresses in the interface address pool and deletes the configured interval for the automatic reclaim.

By default, automatic reclaim of conflicting IP addresses in the interface address pool is disabled.

Format

dhcp server conflict auto-recycle interval day *day* [**hour** *hour* [**minute** *minute*]]

undo dhcp server conflict auto-recycle interval

Parameters

Parameter	Description	Value
day *day*	Specifies the interval for the automatic reclaim, in days.	The value is an integer that ranges from 0 to 999, in days. The default value is 0.
hour *hour*	Specifies the interval for the automatic reclaim, in hours.	The value is an integer that ranges from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the interval for the automatic reclaim, in minutes.	The value is an integer that ranges from 0 to 59, in minutes. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When a DHCP server allocates IP addresses to clients, IP address conflict may occur because IP addresses of some hosts have been manually configured. In this case, the DHCP server considers these IP addresses as conflicting IP addresses, and allocates available IP addresses from the conflicting IP addresses to clients only after available IP addresses in the address pool are used up. To reclaim conflicting IP addresses promptly, the administrator can run this command to enable automatic reclaim and specify the reclaim interval.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Enable automatic reclaim for conflicting IP addresses in the address pool on VLANIF 100, and set the interval for automatic reclaim to one day.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server conflict auto-recycle interval day 1
```

Enable automatic reclaim for conflicting IP addresses in the address pool on GE0/0/1, and set the interval for automatic reclaim to one day.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server conflict auto-recycle interval day 1
```

6.3.41 dhcp server database

Function

The **dhcp server database** command enables the function to save the current DHCP data to storage devices.

The **undo dhcp server database** command disables the function to save the DHCP data to storage devices.

By default, DHCP data is not saved to storage devices.

Format

dhcp server database { **enable** | **recover** | **write-delay** *interval* }

undo dhcp server database { **enable** | **recover** | **write-delay** }

Parameters

Parameter	Description	Value
enable	Enables the function to save DHCP data to storage devices.	-
recover	Recovers DHCP configurations using DHCP data in storage device.	-
write-delay *interval*	Specifies the interval at which DHCP data is saved.	The value is an integer ranging from 300 to 86400, in seconds. The default value is 7200 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCP server, run the **dhcp server database enable** command to enable the device to save DHCP data to storage devices. This avoids data loss caused by device faults. Then the system generates **lease.txt** and **conflict.txt** files in the storage device. The two files save address lease information and address conflict information respectively. Run the **display dhcp server database** command to check the storage device for saving DHCP data. After the **dhcp server database enable** command is run, current DHCP data is automatically saved at the specified interval, and previous data files are overwritten. The interval can be set using the **dhcp server database write-delay** *interval* command.

If a fault occurs on the device, run the **dhcp server database recover** command to recover DHCP data from storage devices during the system restarts.

Prerequisites

The **dhcp server database enable** command has been run to enable the device to save DHCP data to storage devices, and ensure that the storage devices work properly.

Precautions

- The lease.txt and conflict.txt files are overwritten periodically; therefore, you are advised to back up and save the two files to other locations.
- The time displayed in the lease.txt and conflict.txt files is the UTC time rather than the system time, and you do not need to pay attention to time zone information.
- During the interval, if the device restarts unexpectedly, DHCP data generated at the interval is lost. Users can only recover the last successfully saved DHCP data from storage device files.

Example

Enable the device to save the current DHCP data to storage devices and set the interval at which DHCP data is saved to 2000s.

```
<HUAWEI> system-view
[HUAWEI] dhcp server database enable
[HUAWEI] dhcp server database write-delay 2000
```

Recover DHCP configuration using the DHCP data saved on storage devices.

```
<HUAWEI> system-view
[HUAWEI] dhcp server database recover
```

6.3.42 dhcp server dns-list

Function

The **dhcp server dns-list** command configures DNS server addresses for an interface address pool.

The **undo dhcp server dns-list** command deletes the specified DNS server addresses from an interface address pool.

By default, no DNS server address is configured in an interface address pool.

Format

dhcp server dns-list { *ip-address* &<1-8> | **unnumbered interface** *interface-type interface-number* }

undo dhcp server dns-list { **all** | *ip-address* | **unnumbered interface** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the DNS server. You can configure up to eight IP addresses for the DNS servers and separate two IP addresses with a space.	The value is in dotted decimal notation.
unnumbered interface *interface-type interface-number*	Borrows the DNS server address obtained by the interface as the DNS server IP address.	-
all	Deletes all IP addresses of DNS servers specified for the client.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If user hosts access hosts on the network through the domain name, user hosts need to send DNS Request messages to the DNS server and resolve the domain name. To enable DNS services on the DHCP client, specify the DNS server address for the interface address pool on the DHCP server. The DHCP server can assign both the specified DNS server address and an IP address to the client. To configure DNS server addresses for a global address pool, run the **dns-list** command.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- Each address pool can be configured with a maximum of eight DNS server addresses. If multiple DNS server addresses are configured, the first DNS server address assigned to the DHCP client functions as the primary address and other addresses are secondary addresses.
- To specify multiple DNS servers, enter multiple DNS server addresses in the **dhcp server dns-list** command.

Example

Specify a DNS server at 10.10.1.254 for domain name resolution when IP addresses in the interface address pool on VLANIF100 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server dns-list 10.10.1.254
```

Specify a DNS server at 192.168.1.254 for domain name resolution when IP addresses in the interface address pool on GE0/0/1 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server dns-list 192.168.1.254
```

6.3.43 dhcp server domain-name (interface view)

Function

The **dhcp server domain-name** command configures a DNS domain name assigned to a DHCP client.

The **undo dhcp server domain-name** command deletes a specified domain name.

By default, no domain name is configured for the DHCP client.

Format

dhcp server domain-name *domain-name*

undo dhcp server domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name that the DHCP server assigns to the client.	The value is a string of 1 to 63 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Run the **dhcp server domain-name** command on a DHCP server to specify a domain name for each interface address pool. When allocating IP addresses to clients, the DHCP server also sends the domain names to the clients.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

If no domain name is specified for an interface address pool, a DHCP server does not send a domain name to clients, and users cannot access the Web service by using a domain name.

To configure a domain name for the global address pool, run the **domain-name** command.

Example

Set the domain name assigned by the DHCP address pool on the interface to **example.com**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server domain-name example.com
```

Specify the domain name in the address pool on GE0/0/1 as **example.com**.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server domain-name example.com
```

6.3.44 dhcp server excluded-ip-address

Function

The **dhcp server excluded-ip-address** command specifies the range of IP addresses that cannot be automatically assigned to clients from an interface address pool.

The **undo dhcp server excluded-ip-address** command deletes the specified range of IP addresses that cannot be automatically assigned to clients from an interface address pool.

By default, all IP addresses in an address pool can be automatically assigned to clients.

Format

dhcp server excluded-ip-address *start-ip-address* [*end-ip-address*]

undo dhcp server excluded-ip-address *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address of the IP address segment where addresses cannot be automatically assigned to clients.	The value is in dotted decimal notation.

Parameter	Description	Value
end-ip-address	Specifies the end IP address of the IP address segment where addresses cannot be automatically assigned to clients. If *end-ip-address* is not specified, only the IP address corresponding to *start-ip-address* cannot be automatically assigned.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server excluded-ip-address** command applies to DHCP servers. Fixed IP addresses are allocated to some specific hosts (such as the WWW server) on the network for a long time. If these hosts' IP addresses are overlapped with IP addresses in the address pool and the DHCP server allocates these overlapped IP addresses to other hosts, IP address conflicts may occur. To prevent such IP address conflicts, you need to exclude these IP addresses from being automatically assigned in the address pool.

You can run the **dhcp server excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the interface address pool.

You can run the **excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the global address pool.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.

3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- IP addresses that cannot be automatically assigned must be in the address pool. If IP address range in the address pool is changed using the **dhcp server ip-range** command, IP addresses that are configured not to be automatically assigned must be within the new IP address range.
- You do not need to exclude the gateway address configured using the **dhcp server gateway-list** command from being automatically allocated. The device automatically adds the gateway address into the list of IP addresses that cannot be automatically allocated.

  You do not need to exclude the IP address of a server's interface connecting to a client from being automatically allocated. The device automatically sets the status of the interface IP address to Conflict during address assignment.
- If you run this command multiple times, you can specify multiple IP addresses or ranges of IP addresses that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check the IP addresses in use in the current address pool, so that you can exclude the unused IP addresses from being automatically assigned to clients. If you need to exclude IP addresses in Used and Conflict states from being automatically assigned to clients after address reclamation, you can also run the **excluded-ip-address** command. If an IP address has been bound to a specific MAC address, adding the IP address to the IP address list in which IP addresses are not automatically assigned to clients will unbind the IP address from the MAC address.

Example

Disable IP addresses 192.168.1.1 to 192.168.1.20 from being automatically assigned to clients from the address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server excluded-ip-address 192.168.1.1 192.168.1.20
```

Disable IP address 192.168.1.30 in Used state from being automatically assigned to clients from the address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server excluded-ip-address 192.168.1.30
Warning: The address is in used or conflict state. Are you sure to continue excluding the address?[Y/N]:y
```

Disable IP addresses 10.10.10.11 to 10.10.10.20 from being automatically assigned to clients from the address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server excluded-ip-address 10.10.10.11 10.10.10.20
```

6.3.45 dhcp server force insert option

Function

The **dhcp server force insert option** command configures a DHCP server to forcibly insert an Option field specified in the interface address pool to a DHCP Response packet that it sends to a DHCP client.

The **undo dhcp server force insert option** command deletes the Option field forcibly inserted to a DHCP Response packet that a DHCP server sends to a DHCP client.

By default, a DHCP server does not forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Format

dhcp server force insert option *code* &<1-254>

undo dhcp server force insert option *code* &<1-254>

Parameters

Parameter	Description	Value
code	Specifies the code for a forcibly replied option. You can configure a DHCP server to forcibly reply one or more options.	The value is an integer that ranges from 1 to 254.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In general, when a DHCP client applies for an IP address from a DHCP server, parameters contained in the DHCP Request packet specify the options the client requires. The DHCP server inserts the required options to a DHCP Response packet.

Sometimes, a device, functioning as a DHCP server, receives a DHCP Request packet that contains no parameter specifying the options the client requires. However, the client still wants to obtain the options configured on the interface address pool. You can run the **dhcp server force insert option** *code* &<1-254> command to configure the DHCP server to forcibly insert an Option field to the DHCP Response packet.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
4. The Option field has been configured in the interface address pool using the **dhcp server option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command in the interface view.

Example

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server option 4 hex 11 22
[HUAWEI-Vlanif100] dhcp server force insert option 4
```

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option 4 hex 11 22
[HUAWEI-GigabitEthernet0/0/1] dhcp server force insert option 4
```

6.3.46 dhcp server force response

Function

The **dhcp server force response** command forces a DHCP server to reply with a DHCP NAK message.

The **undo dhcp server force response** command disables the function of forcing a DHCP server to reply with a DHCP NAK message.

By default, a DHCP server is not forced to reply with a DHCP NAK message.

Format

dhcp server force response

undo dhcp server force response

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

When a DHCP client goes online in two steps, the IP address requested by the DHCP client is in the IP address pool, but no lease record of the DHCP client is found in the address pool. For example, after obtaining an IP address from another DHCP server, a wireless user roams to the current DHCP server and the original IP address is in the address pool of the current DHCP server. Alternatively, the address pool is reset and the original user needs to go online again. In this case, when receiving a DHCP Request message from the DHCP client, the DHCP server keeps silent and does not reply the DHCP client with a DHCP NAK message. The DHCP client can apply for an IP address to go online again in four steps only after the two steps for the client to go online time out. As a result, the DHCP client is slow in obtaining an IP address. To force the DHCP server to reply with a DHCP NAK message, you can run the **dhcp server force response** command, so that the DHCP client can quickly enter the four-step process for going online and apply for an IP address again.

Prerequisites

DHCP has been enabled on the device using the **dhcp enable** command.

Example

Force a DHCP server to reply with a DHCP NAK message.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server force response
```

6.3.47 dhcp server gateway-list

Function

The **dhcp server gateway-list** command sets the default gateway IP address that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server gateway-list** command deletes the configured default gateway IP address.

By default, the default gateway IP address that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server gateway-list *ip-address* &<1-8>

undo dhcp server gateway-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address. You can configure a maximum of eight gateway addresses, which are separated by spaces.	The value is in decimal dotted notation.
all	Indicates all IP addresses.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To load balance traffic and improve network reliability, you can configure multiple default gateway addresses.

NOTICE

The default gateway address allocated to the DHCP client can only be a class A, B, or C address, and cannot be a broadcast address, a host address, or a class A address whose network address is 0.

If the VRRP virtual IP address is configured on the interface and no gateway address is pre-allocated to the DHCP client using the **dhcp server gateway-list** command, the DHCP server uses the first VRRP virtual IP address as the gateway address to be allocated to the client. If no VRRP virtual IP address is configured on the interface, the DHCP server uses the physical IP address of the interface as the gateway address to be allocated to the client.

If the **dhcp server gateway-list** command is not configured, the gateway address allocated by the DHCP server to the DHCP client may fail to be displayed in trace information during fault diagnosis. Therefore, you are advised to configure this command if the DHCP server function based on an interface address pool is used.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Enable a DHCP server on a VLANIF100 to pre-allocate default gateway address 10.1.1.1 to DHCP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server gateway-list 10.1.1.1
```

Enable a DHCP server on GE0/0/1 to pre-allocate default gateway address 10.1.1.1 to DHCP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server gateway-list 10.1.1.1
```

6.3.48 dhcp server group

Function

The **dhcp server group** command creates a DHCP server group and displays the DHCP server group view or directly displays the view of the existing DHCP server group.

The **undo dhcp server group** command deletes an existing DHCP server group.

By default, no DHCP server group is configured.

Format

dhcp server group *group-name*

undo dhcp server group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces. It can contain digits, letters, and special characters such as underscores (_), hyphens (-), and periods (.). It cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. Generally, a DHCP relay agent serves multiple DHCP servers. To manage these DHCP servers in a unified manner, run the **dhcp server group** command to create a DHCP server group. The DHCP server group then assigns IP addresses to users using the DHCP relay agent.

Follow-up Procedure

- Run the **dhcp-server** command to add DHCP servers to the DHCP server group.
- Run the **dhcp relay server-select** command in the interface view to specify a DHCP server group for the DHCP relay agent.

Precautions

You can configure a maximum of 32 DHCP server groups in the system, and a maximum of 20 DHCP servers in a DHCP server group.

Example

Create a DHCP server group named **dhcp-srv1**.

```
<HUAWEI> system-view
[HUAWEI] dhcp server group dhcp-srv1
```

6.3.49 dhcp server ip-range

Function

The **dhcp server ip-range** command sets the range of IP addresses that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server ip-range** command deletes the configured IP address range.

By default, the range of IP addresses that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server ip-range *start-ip-address end-ip-address*

undo dhcp server ip-range

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address.	The value is in decimal dotted notation.
end-ip-address	Specifies the end IP address.	The value is in decimal dotted notation.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **dhcp server ip-range** *start-ip-address end-ip-address* command to change the range of IP addresses in an address pool based on actual usage of IP addresses.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Enable a DHCP server on a VLANIF100 to pre-allocate IP addresses 192.168.1.2 to 192.168.1.100 to DHCP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server ip-range 192.168.1.2 192.168.1.100
```

Enable a DHCP server on GE0/0/1 to pre-allocate IP addresses 192.168.1.2 to 192.168.1.100 to DHCP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server ip-range 192.168.1.2 192.168.1.100
```

6.3.50 dhcp server lease

Function

The **dhcp server lease** command specifies the IP address lease for addresses in an interface address pool.

The **undo dhcp server lease** command restores the default IP address lease of addresses in an interface address pool.

By default, the IP address lease of addresses in an interface address pool is one day.

Format

dhcp server lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo dhcp server lease

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer that ranges from 0 to 999. The default value is 1.

Parameter	Description	Value
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer that ranges from 0 to 23. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer that ranges from 0 to 59. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment.

DHCP clients require different IP address leases.

- If a host (such as the DNS server) needs to use a fixed IP address for a long time, run the **dhcp server lease unlimited** command to configure the IP address lease as unlimited.
- If a host (such as a portable computer) needs to use a temporary IP address, run the **dhcp server lease** command to specify an IP address lease. After the lease expires, the DHCP server withdraws the IP address and assigns the address to other clients. In scenarios with high user mobility, new clients may fail to obtain IP addresses if allocated addresses are not reclaimed for a long time. As such, shortening the DHCP lease is recommended. For example, in Wi-Fi access scenarios of an airport or station, you can change the DHCP lease to 30 minutes.

When a DHCP client starts and 50% or 87.5% of its IP address lease has passed, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease.

- If the IP address can still be assigned to the client, the DHCP server informs the client of a renewed IP address lease.

- If the IP address can no longer be assigned to the client, the DHCP server informs the client that the IP address lease cannot be renewed.

You can run the **display ip pool** command to view information about the IP address lease. The values of the **lease** and **left** fields in the command output indicate the configured lease time and remaining lease time, respectively.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

Different IP address leases can be specified for different interface address pools on a DHCP server. All IP addresses in an interface address pool have the same lease.

If the IP address lease of an address pool is changed using this command, newly assigned IP addresses use the new IP address lease. IP addresses assigned before the change still use the original IP address lease before the lease is updated, and use the new lease after the lease is updated.

Example

Set the IP address lease of the address pool on VLANIF100 to 2 days 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.10.10.10 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server lease day 2 hour 2 minute 30
```

Set the IP address lease of the address pool on GE0/0/1 to 2 days 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server lease day 2 hour 2 minute 30
```

6.3.51 dhcp server logging

Function

The **dhcp server logging** command enables the logging function during IP address allocation of the DHCP server in the interface view.

The **undo dhcp server logging** command disables the logging function during IP address allocation of the DHCP server in the interface view.

By default, the logging function during IP address allocation of the DHCP server is disabled.

Format

dhcp server logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

undo dhcp server logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

Parameters

Parameter	Description	Value
allocation-fail	Displays logs when address allocation fails.	-
allocation-success	Displays logs when address allocation succeeds.	-
release	Displays logs when addresses are released.	-
renew-fail	Displays logs when address lease renewal fails.	-
renew-success	Displays logs when address lease renewal succeeds.	-
detect-conflict	Displays logs when address conflict occurs.	-
recycle-conflict	Displays logs when conflicting addresses are reclaimed.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When the DHCP server allocates IP addresses to clients, it records address allocation information to facilitate routine maintenance and fault location. After the logging function during IP address allocation of the DHCP server is configured using the **dhcp server logging** command, the DHCP server records logs about address allocation, conflict, lease renewal, and release.

Run the **display ip pool interface** *interface-pool-name* command to check the status of the logging function during IP allocation of the DHCP server.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- With this logging function enabled, if a large number of DHCP clients request IP addresses from the DHCP server, the server frequently records logs. The server performance may therefore be affected.
- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration in the *CLI-based Configuration - Device Management Configuration Guide*.

  For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the logging function during IP address allocation of the DHCP server on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server logging
```

Enable the logging function during IP address allocation of the DHCP server on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server logging
```

6.3.52 dhcp server mask

Function

The **dhcp server mask** command sets the subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server mask** command deletes the configured subnet mask.

By default, the subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server mask { *mask* | *mask-length* }

undo dhcp server mask

Parameters

Parameter	Description	Value
mask	Specifies a subnet mask.	The value is in decimal dotted notation.
mask-length	Specifies the length of the subnet.	The value is an integer ranging from 0 to 32.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the DHCP server function on an interface, you can configure the range and subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients. Run the **dhcp server ip-range** command to configure the IP address range and run the **dhcp server mask** command to configure the subnet mask of the IP addresses.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Set the subnet mask of IP addresses that a DHCP server on a VLANIF100 pre-allocates to DHCP clients to 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server mask 255.255.255.0
```

Set the subnet mask of IP addresses that a DHCP server on GE0/0/1 pre-allocates to DHCP clients to 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server mask 255.255.255.0
```

6.3.53 dhcp server nbns-list

Function

The **dhcp server nbns-list** command configures Network Basic Input Output System (NetBIOS) server addresses for an interface address pool.

The **undo dhcp server nbns-list** command deletes the NetBIOS server address from an interface address pool.

By default, no NetBIOS server address is configured for an interface address pool.

Format

dhcp server nbns-list *ip-address* &<1-8>

undo dhcp server nbns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the NetBIOS server address.	The value is in dotted decimal notation.
all	Deletes all NetBIOS server addresses.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before hosts communicate with each other, a NetBIOS server needs to resolve the accessed NetBIOS hostname to an IP address. To enable hosts to communicate with each other, run the **dhcp server nbns-list** command to configure NetBIOS server addresses for an interface address pool. When assigning IP addresses to clients, a DHCP server also assigns the configured NetBIOS server addresses to clients. To configure NetBIOS server addresses for a global address pool, run the **nbns-list** command.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

Each interface can be configured with a maximum of eight NetBIOS server addresses. The first assigned address functions as the primary address, and other addresses function as secondary addresses.

Example

Specify a NetBIOS server at 192.168.1.99 for domain name resolution when IP addresses in the interface address pool on VLANIF100 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.10.10.10 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server nbns-list 192.168.1.99
```

Specify a NetBIOS server at 192.168.1.99 for domain name resolution when IP addresses in the interface address pool on GE0/0/1 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server nbns-list 192.168.1.99
```

6.3.54 dhcp server netbios-type

Function

The **dhcp server netbios-type** command specifies the NetBIOS node type for a DHCP client connecting to an interface.

The **undo dhcp server netbios-type** command deletes the specified NetBIOS node type of a DHCP client connecting to an interface.

By default, no NetBIOS node type is specified for a DHCP client connecting to an interface.

Format

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo dhcp server netbios-type

Parameters

Parameter	Description	Value
b-node	Indicates a node in broadcast mode. A b-node obtains the mapping in broadcast mode.	-
h-node	Indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.	-
m-node	Indicates a node in mixed mode. An m-node is a p-type node with some broadcast features.	-
p-node	Indicates a node in peer-to-peer mode. This node obtains mappings by communicating with the NetBIOS server.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When DHCP clients use NetBIOS on the WAN to communicate, their host names and IP addresses need to be mapped. You can run the **dhcp server netbios-type** command to configure the NetBIOS node type for an interface address pool. When assigning an IP address to the client, the DHCP server also sends the specified NetBIOS node type to the client.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

To specify the NetBIOS node type for a client in the global address pool, run the **netbios-type** command.

Example

Set the NetBIOS node type for a client in the address pool on VLANIF100 to **p-node**.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.10.10.10 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server netbios-type p-node
```

Set the NetBIOS node type for a client in the address pool on GE0/0/1 to **p-node**.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server netbios-type p-node
```

6.3.55 dhcp server next-server

Function

The **dhcp server next-server** command specifies a server IP address for DHCP clients.

The **undo dhcp server next-server** command cancels the configuration.

By default, no server IP address is specified by the DHCP Server for DHCP clients.

Format

dhcp server next-server *ip-address*

undo dhcp server next-server

Parameters

Parameter	Description	Value
ip-address	Specifies a server IP address.	The value is in dotted decimal notation.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server next-server** command is used on DHCP servers. When assigning a DHCP client an IP address, a DHCP server can also assign the DHCP client an IP address of the server that provides network services for the client. For example, some clients like IP phones still need other configuration parameters after automatically obtaining IP addresses. You can run the **dhcp server next-server** command to specify the server address used after a client obtains an IP address. The client then requests the configuration parameters from the specified server after obtaining an IP address.

If users use addresses in the interface address pool, run the **dhcp server next-server** command to specify the DHCP server IP address. If users use addresses in the global address pool, run the **next-server** command to specify the DHCP server IP address.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- The **dhcp server next-server** command takes effect for only users who use addresses in the interface address pool.
- If you run the **dhcp server next-server** command multiple times, only the latest configuration takes effect.

Example

Specify the server IP address 192.168.1.2 in the interface address pool on VLANIF100 used to provide services for terminal users.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.2 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server next-server 192.168.1.2
```

Specify the server IP address 192.168.1.2 in the interface address pool on GE0/0/1 used to provide services for terminal users.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server next-server 192.168.1.2
```

6.3.56 dhcp server option

Function

The **dhcp server option** command sets user-defined option for an interface address pool.

The **undo dhcp server option** command deletes user-defined option from an interface address pool.

By default, no user-defined option is configured in an interface address pool.

Format

dhcp server option *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }

undo dhcp server option [*code* [**sub-option** *sub-code*]]

Parameters

Parameter	Description	Value
code	Specifies the code for a user-defined option.	The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 120, 121 and 184. **NOTE** ● The format of option82, Option121 and Option184 are different from the other codes of a customized option. ● There are well-known options and customized options. For details about well-known options, see RFC 2132. ● When the switch functions as a DHCP client, Option 148 can be used in an EasyDeploy scenario and is not recommended in other scenarios.
sub-option *sub-code*	Specifies the code of a user-defined sub-option.	The value is an integer that ranges from 1 to 254. For details about well-known options, see RFC 2132.
ascii *ascii-string*	Specifies the user-defined option code as an ASCII character string.	The value is a string of 1 to 255 characters when **sub-option** is not specified, or a string of 1 to 253 characters when **sub-option** is specified.

Parameter	Description	Value
hex *hex-string*	Specifies the user-defined option code as a hexadecimal string.	The value is a hexadecimal string with an even number of digits, for example, hh or hhhh. If **sub-option** is not specified, the even number is in the range of 2 to 254. If **sub-option** is specified, the even number is in the range of 2 to 252. The value can be a combination of digits (0-9) and letters (A-F and a-f).
cipher *cipher-string*	Specifies the user-defined option code as a ciphertext character string.	The value is a string, you can enter a character string in explicit text or cipher text. ● The character string in explicit text is a string of 1 to 64 characters. ● The character string in cipher text is a string of 32 to 104 characters. No matter whether the character string is entered in explicit or cipher text, the character string is displayed in cipher text in the configuration file and in explicit text in packets.
ip-address *ip-address*	Specifies the user-defined option code as an IP address.	The value is in dotted decimal notation.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. The Option field in a DHCP packet carries control information and parameters, including basic information such as the DNS service, NetBIOS service, and IP address lease. If a DHCP server is configured with option, when a DHCP client applies for an IP address from an interface address pool, the client can obtain configurations in the Option field of the DHCP response packet from the DHCP server without having to configure the DNS service, NetBIOS service, or IP address lease separately.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and special characters. In addition, the password must consist of six or more than eight characters.
- The **dhcp server option** command configures basic functions, such as the NetBIOS service and IP address lease. The system also provides commands to configure these functions separately. These commands take precedence over the **dhcp server option** command.
- To set user-defined option for a global address pool, run the **option** command.
- When users on an enterprise's intranet use a proxy server to connect to the Internet, you need to configure proxy server parameters so that users can use browsers to access the network. The Web Proxy Auto-Discovery Protocol (WPAD) implements automatic configuration of these parameters. The administrator does not need to manually configure these parameters on each client. To implement the WPAD function, the administrator needs to deploy the configuration file of the proxy server in advance, and then run the **dhcp server option 252 ascii** *ascii-string* command to specify the URL of the configuration file. The *ascii-string* parameter specifies the URL of the configuration file, in the format of https://*xxx*/proxy.pac. Set *ascii-string* according to the actual location of the configuration file. When a browser accesses the network, the browser requests the DHCP server to send the URL of the configuration file on the proxy server, and then downloads the configuration file to conduct automatic configuration. After the configuration is completed, the browser can access the network.

NOTE

The value of *ascii-string* cannot be enclosed in double quotation marks as "*ascii-string*". Otherwise, terminals cannot parse Option252.

Example

Set Option64 to 0x11 (a hexadecimal number) for the interface address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.10.10.10 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server option 64 hex 11
```

Set Option64 to 0x11 (a hexadecimal number) for the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option 64 hex 11
```

6.3.57 dhcp server option121

Function

The **dhcp server option121** command configures a classless static route allocated by a DHCP server to a client.

The **undo dhcp server option121** command deletes a classless static route allocated by a DHCP server to a client.

By default, the classless static route allocated to a client is not configured.

Format

dhcp server option121 ip-address { *ip-address mask-length gateway-address* } &<1-8>

undo dhcp server option121 [**ip-address** *ip-address mask-length gateway-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
gateway-address	Specifies the gateway address of a route.	The value is in dotted decimal notation.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server option121 ip-address** command applies to only the DHCP server. The **dhcp server option121 ip-address** command configures Option 121 that defines a classless static route allocated to a client from an interface address pool.

mask-length and *gateway-address* specify a classless static route. The **dhcp server option121 ip-address** command configures a maximum of eight classless static routes.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
4. The **undo dhcp server option121** command will delete all classless static routes. To delete one classless static route, run the **undo dhcp server option121 ip-address** *ip-address mask-length gateway-address* command.

Example

Configure a classless static route allocated by a DHCP server to a client in the interface address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.2 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server option121 ip-address 10.10.10.10 24 192.168.11.11
```

Configure a classless static route allocated by a DHCP server to a client in the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option121 ip-address 10.10.10.10 24 192.168.11.11
```

6.3.58 dhcp server option125 vendor-specific

Function

The **dhcp server option125 vendor-specific** command configures the vendor ID in Option 125 delivered by a DHCP server to a client.

The **undo dhcp server option125 vendor-specific** command deletes the vendor ID in Option 125 delivered by a DHCP server to a client.

By default, no vendor ID is configured in Option 125 delivered by a DHCP server to a client.

Format

dhcp server option125 vendor-specific *vendor-id*

undo dhcp server option125 vendor-specific

Parameters

Parameter	Description	Value
vendor-id	Indicates the vendor ID, which is assigned by the IANA. 2011 indicates Huawei.	The value is an integer in the range from 1 to 4294967295.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a DHCP client sends a DHCP Discover message carrying a vendor ID to a DHCP server, the DHCP server needs to exchange the vendor information with the client using Option 125. You can run the **dhcp server option 125** [**sub-option** *sub-code*] **ascii** *ascii-string* command to configure the vendor ID in Option 125 delivered by a DHCP server to a client. However, it is complex to convert the vendor ID into an ASCII character string.

To simplify the configuration, you can run the **dhcp server option125 vendor-specific** *vendor-id* command to specify the vendor ID in Option 125 of packets sent from a DHCP server to a client.

Prerequisites

1. IP addresses have been configured in an interface address pool using the **ip address** command.
2. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
3. Fields except **Vendor-ID** in Option 125 have been configured for the interface address pool using the **dhcp server option 125 ascii** *ascii-string* command. The **Vendor-ID** field in Option 125 occupies four bytes. Therefore, the *ascii-string* value is a string of 1 to 251 bytes.
4. (Optional) The **dhcp server force insert option 125** command has been used to configure the DHCP server to insert the Option 125 field specified for the interface address pool into the DHCP response packet sent from a DHCP server to a client. This resolves the problem in the following situation: The device functions as a DHCP server, and the DHCP request packet sent by a DHCP client does not carry Option 125. However, the DHCP client still expects the DHCP server to deliver Option 125 configured for the interface address pool.

Precautions

This command and the **dhcp server option 125 sub-option** *sub-code* **ascii** *ascii-string* are mutually exclusive on an interface.

Example

Configure the VLAN and vendor information in Option 125 for the interface address pool on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.2 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server option 125 ascii id:vlan=100
[HUAWEI-Vlanif100] dhcp server option125 vendor-specific 2011
```

Configure the VLAN and vendor information in Option 125 for the interface address pool on GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option 125 ascii id:vlan=10
[HUAWEI-GigabitEthernet0/0/1] dhcp server option125 vendor-specific 2011
```

6.3.59 dhcp server option184

Function

The **dhcp server option184** command configures Option 184 allocated by a DHCP server to a client.

The **undo dhcp server option184** command deletes Option 184 allocated by a DHCP server to a client.

By default, Option 184 allocated by a DHCP server to a client is not configured.

Format

dhcp server option184 { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* }

undo dhcp server option184 [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

Parameters

Parameter	Description	Value
ncp-ip *ip-address*	Specifies the IP address of the network call processor (NCP).	The value is in dotted decimal notation.
as-ip *ip-address*	Specifies the IP address of the backup NCP.	The value is in dotted decimal notation.
fail-over *ip-address*	Specifies the IP address in the failover route.	The value is in dotted decimal notation.
dialer-string	Specifies the dialer string.	The value is a string of 1 to 64 characters.
voice-vlan *vlan-id*	Specifies the ID of a voice VLAN.	The value is an integer that ranges from 1 to 4094.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server option184** command applies to only the DHCP server and configures Option 184 allocated by a DHCP server to a client in an interface address pool.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Configure Option 184 allocated by a DHCP server to a client in the interface address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.2 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server option184 as-ip 10.10.10.10
```

Configure Option 184 allocated by a DHCP server to a client in the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option184 as-ip 10.10.10.10
```

6.3.60 dhcp server ping

Function

The **dhcp server ping** command sets the maximum number of ping packets to be sent and the maximum response time of a ping packet.

The **undo dhcp server ping** command restores the default setting.

By default, the DHCP server sends 2 ping packets and the maximum response time is 500 ms.

Format

dhcp server ping { **packet** *number* | **timeout** *milliseconds* } *

undo dhcp server ping { **packet** | **timeout** }

Parameters

Parameter	Description	Value
packet *number*	Specifies the maximum number of ping packets to be sent.	The value is an integer ranging from 0 to 10. The value 0 indicates that no ping operation is performed.

Parameter	Description	Value
timeout *milliseconds*	Specifies the maximum response time of a ping packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The value 0 indicates that no ping operation is performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Repetitive IP address assignment will cause IP address conflicts. To solve this problem, before assigning an IP address to a client, the DHCP server needs to send ping packets using the **dhcp server ping** command to check whether the IP address is in use. Address detection checks whether the DHCP server receives any response within a certain period of time. If there is no response within a certain period of time, the DHCP server continues to send ping packets to this address until the number of ping packets reaches the maximum value. If there is still no response, it indicates that the IP address is not in use. This ensures that the IP address assigned to the client is unique.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Set the maximum number of ping packets to 3 and the maximum response time to 400 ms.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server ping packet 3
[HUAWEI] dhcp server ping timeout 400
```

6.3.61 dhcp server sip-server

Function

The **dhcp server sip-server** command configures the SIP server IP address assigned to a DHCP client on an interface address pool.

The **undo dhcp server sip-server** command deletes the configured SIP server IP address assigned to a DHCP client on an interface address pool.

By default, the SIP server IP address assigned to a DHCP client on an interface address pool is not configured.

Format

dhcp server sip-server { **ip-address** *ip-address* &<1-2> | **list** *domain-name* &<1-2> }

undo dhcp server sip-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address for the SIP server.	The value is in dotted decimal notation.
list *domain-name*	Specifies the domain name of the SIP server.	The value is a string of 1 to 63 characters.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP server. To enable DHCP clients to normally access the Internet, the DHCP server needs to specify the SIP server IP address in the interface address pool when assigning IP addresses to the clients.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- A maximum of two SIP server addresses can be configured in each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- Before specifying the IP address or name for a SIP server, ensure that the SIP server exists.
- If you run this command repeatedly, the latest configuration overrides the previous ones.

Example

Specify 10.1.1.1 as the IP address of the SIP server when addresses in the interface VLANIF100 address pool are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server sip-server ip-address 10.1.1.1
```

Specify 10.1.1.1 as the IP address of the SIP server when addresses in the interface GE0/0/1 address pool are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server sip-server ip-address 10.1.1.1
```

6.3.62 dhcp server sname

Function

The **dhcp server sname** command configures the name of the server where the DHCP client obtains the startup configuration file.

The **undo dhcp server sname** command deletes the configured name of the server where the DHCP client obtains the startup configuration file.

By default, the name of the server where the DHCP client obtains the startup configuration file is not configured.

Format

dhcp server sname *sname*

undo dhcp server sname

Parameters

Parameter	Description	Value
sname	Specifies the name of the server where the DHCP client obtains the startup configuration file.	The value is a string of 1 to 63 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP clients. After the name of the server where the DHCP client obtains the startup configuration file is configured using the **dhcp server sname** command, the DHCP client obtains the startup configuration file from this server.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
4. The startup configuration file name has been configured for the DHCP client using the **dhcp server bootfile**.

Follow-up Procedures

Ensure that the route between the DHCP client and the file server where the DHCP client obtains the startup configuration file is reachable.

Example

Configure the name of the server where the DHCP client obtains the startup configuration file as **Test** in the interface address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 255.255.255.0
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server bootfile start.ini
[HUAWEI-Vlanif100] dhcp server sname Test
```

Configure the name of the server where the DHCP client obtains the startup configuration file as **Test** in the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server bootfile start.ini
[HUAWEI-GigabitEthernet0/0/1] dhcp server sname Test
```

6.3.63 dhcp server static-bind

Function

The **dhcp server static-bind** command binds an IP address in an interface address pool to a MAC address.

The **undo dhcp server static-bind** command unbinds the IP address in an interface address pool from a MAC address.

By default, an IP address in an interface address pool is not bound to any MAC address.

Format

dhcp server static-bind ip-address *ip-address* **mac-address** *mac-address* [**description** *description*]

undo dhcp server static-bind [**ip-address** *ip-address* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address to be bound. The IP address must be valid in an interface address pool.	The value is in dotted decimal notation.

Parameter	Description	Value
mac-address *mac-address*	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
description *description*	Specifies the user description.	The value is a string of 1 to 256 case-sensitive characters. It can contain spaces.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server static-bind** command applies to DHCP servers. When planning a network, you need to allocate fixed IP addresses to some important hosts to ensure reliability. In this case, you can bind IP addresses in the address pool to the MAC addresses of these hosts. After the preceding configuration is complete, if the host of the MAC address to which the IP address is bound request an IP address from the DHCP server, the DHCP server finds the bound IP address based on the host's MAC address and allocates this IP address to the host, ensuring that the IP address obtained by the host is fixed.

You can run the **dhcp server static-bind** command to bind an IP address in an interface address pool to a MAC address.

You can run the **static-bind** command to bind an IP address in a global address pool to a MAC address.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **dhcp server excluded-ip-address** command.
- IP addresses that are used can also be statically bound to MAC addresses or unbound from MAC addresses. When an IP address is statically bound to a MAC address, ensure that the MAC address to be bound is the same as the MAC address of the user who actually uses the IP address.
- The DHCP server preferentially allocates the IP address that has been statically bound to the client's MAC address.
- After an IP address is bound to a MAC address, the IP address does not expire. After an automatically allocated IP address is statically bound to a MAC address, the lease time of the IP address becomes unlimited. After the static binding between the IP address and the MAC address is deleted, the lease time of the IP address becomes the same as that configured in the address pool.

Example

Configure a DHCP server to assign a fixed IP address 10.10.10.20 in the interface address pool on vlanif 100 to a host with the MAC address 00e0-fcf3-2a3b.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.10.10.10 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server static-bind ip-address 10.10.10.20 mac-address 00e0-fcf3-2a3b
```

Configure a DHCP server to assign a fixed IP address 10.10.10.20 in the interface address pool on GE0/0/1 to a host with the MAC address 00e0-fcf3-2a3b.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server static-bind ip-address 10.10.10.20 mac-address 00e0-
fcf3-2a3b
```

6.3.64 dhcp server trust option82

Function

The **dhcp server trust option82** command enables Option 82 on the DHCP server.

The **undo dhcp server trust option82** command disables Option 82 on the DHCP server.

By default, the DHCP server trusts Option 82.

Format

dhcp server trust option82

undo dhcp server trust option82

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server to enable the Option 82 function. After receiving a DHCP packet that carries the Option 82 field but the giaddr is 0, the DHCP server processes the packet by default. Using the **undo dhcp server trust option82** command, the DHCP server discards the packet.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Example

Enable Option 82 of the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp server trust option82
```

6.3.65 dhcp-server

Function

The **dhcp-server** command adds DHCP servers to a DHCP server group.

The **undo dhcp-server** command deletes DHCP servers from a DHCP server group.

By default, no DHCP server is configured in a DHCP server group.

Format

dhcp-server [**vpn-instance** *vpn-name* | **public-net**] *ip-address* [*ip-address-index*]

undo dhcp-server { [**vpn-instance** *vpn-name* | **public-net**] *ip-address* | *ip-address-index* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-name*	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.
public-net	Indicates that the public network is used to forward packets.	-
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.
ip-address-index	Specifies an index for a DHCP server IP address. If you do not specify the server index, the system assigns an idle index to the server.	The value is an integer that ranges from 0 to 19.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp-server** command applies to DHCP relay agents. To ensure that the DHCP relay agent can forward messages to multiple DHCP servers, configure multiple DHCP servers in a DHCP server group.

Precautions

- Each DHCP server group can be configured with a maximum of 20 DHCP servers. You can delete a DHCP server by specifying *ip-address-index*.
- If a VPN instance is bound to an interface, the DHCP server group must be bound to this VPN instance.
- If the interface enabled with DHCP relay is bound to a VPN instance but no VPN instance is specified for a DHCP server in a DHCP server group, the DHCP relay agent sends packets through the VPN instance to which the interface belongs by default. If a VPN instance is specified for a DHCP server in a DHCP server group, the DHCP relay agent sends packets through the VPN instance specified for the DHCP server.

Example

Add the DHCP server at 10.10.78.56 to the DHCP server group **dhcp-srv1**.

```
<HUAWEI> system-view
[HUAWEI] dhcp server group dhcp-srv1
[HUAWEI-dhcp-server-group-dhcp-srv1] dhcp-server 10.10.78.56
```

6.3.66 dhcp set ttl

Function

The **dhcp set ttl** command sets the TTL value for DHCP Discover messages after they are forwarded by the DHCP relay agent at Layer 3.

The **undo dhcp set ttl** command restores the default setting.

By default, the TTL value of DHCP Discovery messages decreases by 1 after they are forwarded by the DHCP relay agent at Layer 3.

Format

dhcp set ttl { **unvaried** | *ttl-value* }

undo dhcp set ttl

Parameters

Parameter	Description	Value
unvaried	Indicates that the TTL value of DHCP Discovery messages remains unchanged after the messages are forwarded by the DHCP relay agent at Layer 3. That is, the device does not reduce the TTL value by 1.	-
ttl-value	Specifies a fixed TTL value for DHCP Discovery messages after they are forwarded by the DHCP relay agent at Layer 3.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp set ttl** command is used on DHCP relay agents. When a DHCP relay agent forwards DHCP Discovery messages at Layer 3, it reduces the TTL value of the messages by 1 by default. Assume that the TTL value of a DHCP Discovery message received by the DHCP relay agent is 1. If the DHCP relay agent reduces the TTL value by 1, the TTL value changes to 0. The next-hop routing device will discard the message as its TTL value is 0. As a result, the DHCP server cannot receive the DHCP Discovery message forwarded by the DHCP relay agent. To ensure that the DHCP server can receive the DHCP Discovery message sent from the client, run the **dhcp set ttl** command to set the TTL value of the DHCP Discovery message to a non-zero value after the message is forwarded at Layer 3.

NOTE

If the DHCP relay agent connects to a special client whose TTL value of DHCP Discovery messages is 1, and if there are routing devices between the DHCP relay agent and DHCP server, run the **dhcp set ttl** *ttl-value* command to specify a fixed TTL value (16 is recommended) for DHCP Discovery messages after they are forwarded by the DHCP relay agent at Layer 3.

Prerequisites

The DHCP function has been enabled globally using the **dhcp enable** command.

Example

Set the TTL value of DHCP Discovery messages to 16 after the messages are forwarded by the DHCP relay agent at Layer 3.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp set ttl 16
```

6.3.67 dhcp speed-limit auto

Function

The **dhcp speed-limit auto** command enables dynamic rate limiting on DHCP packets.

The **undo dhcp speed-limit auto** command disables dynamic rate limiting on DHCP packets.

By default, dynamic rate limiting is disabled on DHCP packets.

Format

dhcp speed-limit auto

undo dhcp speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security or facilitate management, users may require that the DHCP packet processing rate should be limited. If the rate is not limited, CPU and memory resources can be used up due to malicious attacks.

Table 6-16 and **Table 6-17** list the mapping between the DHCP packet rate and CPU/memory usage after dynamic rate limiting on DHCP packets is enabled.

Table 6-16 DHCP packet rate and CPU usage

CPU Usage (%)	DHCP Packet Rate (packets/second)
(70–85)	100
[85–100)	50
100	10

Table 6-17 DHCP packet rate and memory usage

Memory Usage (%)	DHCP Packet Rate (packets/second)
(65–75)	100
[75–85)	50
[85–100)	10

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Precautions

- When the CPU usage is higher than 70% or the memory usage is higher than 65%, the DHCP packet processing rate is limited.
- The DHCP packet processing rate is the same as the smaller rate among the rates corresponding to the CPU or memory usage. For example, when the CPU usage is 80% and the memory usage is 80%, the DHCP packet rate is 50.

Example

Enable dynamic rate limiting on DHCP packets.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp speed-limit auto
```

6.3.68 dhcp udp-checksum enable

Function

The **dhcp udp-checksum enable** command enables a device to add the UDP header checksum to DHCP packets to be sent.

The **undo dhcp udp-checksum enable** command disables a device from adding the UDP header checksum to DHCP packets to be sent.

By default, the UDP header checksum carried in DHCP packets sent by a device is 0, and the peer device does not verify the checksum.

Format

dhcp udp-checksum enable

undo dhcp udp-checksum enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device does not comply with protocol standards, the peer device still verifies the UDP header checksum when the checksum carried in DHCP packets is 0. In this case, you can run the **dhcp udp-checksum enable** command to enable the device to add the UDP header checksum to DHCP packets to be sent.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

A device can add the UDP header checksum to DHCP packets to be sent only if the device functions as a DHCP server.

Example

Enable a device to add the UDP header checksum to DHCP packets to be sent.

```
<HUAWEI> system-view
[HUAWEI] dhcp udp-checksum enable
```

6.3.69 display dhcp client

Function

The **display dhcp client** command displays DHCP/BOOTP client lease information.

Format

display dhcp client [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP/BOOTP client lease information on a specified interface: ● *interface-type*: specifies the interface type. ● *interface-number*: specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device functions as a DHCP/BOOTP client, you can run this command to view DHCP/BOOTP client lease information.

Example

Display DHCP client lease information.

```
<HUAWEI> display dhcp client
DHCP client lease information on interface Vlanif119 :
 Current machine state         : Bound
 Internet address assigned via : DHCP
 Physical address              : 00e0-fccd-a896
 IP address                    : 192.168.119.254
 Subnet mask                   : 255.255.255.0
 Gateway ip address            : 192.168.119.1
                                 192.168.119.3
                                 192.168.119.2
 DHCP server                   : 192.168.119.1
 Lease obtained at             : 2008-10-01 04:35:10
 Lease expires at              : 2008-10-01 04:36:10
 Lease renews at               : 2008-10-01 04:35:40
 Lease rebinds at              : 2008-10-01 04:36:03
 Classless static route        : 192.168.0.0/16 via 192.168.119.1
                                 10.10.0.0/16 via 192.168.119.2
```

```
Host name                    : client    Request option list           : 1 3 6 15 28 33 44 121 184
Class identifier             : huawei
Client identifier            : 00e0-fccd-a896
```

Table 6-18 Description of the **display dhcp client** command output

Item	Description
DHCP client lease information on interface *if1*	DHCP client lease information on the interface if1.
Current machine state	Current device status. The value can be: - **Halt**: indicates the state of stopping applying for IP addresses. - **Init**: indicates the initialization state. - **Waiting offer**: indicates the state of waiting for an OFFER message. - **Selecting**: indicates the state that the state machine enters after DHCP DISCOVER messages are sent to search for DHCP servers. In this state, the device is waiting for response messages from DHCP servers. - **Requesting**: indicates the state that the state machine enters after DHCP REQUEST messages are sent to request IP addresses. In this state, the device is waiting for response messages from DHCP servers. - **Bound**: indicates the state that the state machine enters after the device successfully obtains an IP address by receiving the DHCP ACK message from a DHCP server. - **Renewing**: indicates the state that the state machine enters after T1 timer times out. - **Rebind**: indicates the state that the state machine enters after T2 timer times out.
Internet address assigned via	Indicates that the device IP address is obtained through DHCP or BOOTP.
Physical address	Device MAC address.
IP address	Device IP address.
Subnet mask	Mask of the device IP address.

Item	Description
Gateway ip address	Gateway address of the DHCP or BOOTP server.
DHCP server	IP address of the DHCP server (no value for a BOOTP client).
Lease obtained at	Time the lease is obtained.
Lease expires at	Time the lease expires (no value for a BOOTP client).
Lease renews at	Lease renewal timer, which is 50% of the lease (no value for a BOOTP client).
Lease rebinds at	Rebinding timer, which is 87.5% of the lease (no value for a BOOTP client).
Classless static route	Classless static route.
Host name	Information in Option 12, which is the host name of the client.
Request option list	Information in Option 55, which is the parameter list requested by the client.
Class identifier	Information in Option 60, which is the vendor class identifier of the client.
Client identifier	Information in Option 61, which is the client identifier.

6.3.70 display dhcp client statistics

Function

The **display dhcp client statistics** command displays message statistics on a DHCP/BOOTP client.

Format

display dhcp client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays packet statistics on a specified interface of the DHCP/BOOTP client: - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as the DHCP client, the **display dhcp client statistics** command displays message statistics.

Example

Display message statistics on a DHCP/BOOTP client.

```
<HUAWEI> display dhcp client statistics
DHCP message statistics on interface GigabitEthernet0/0/1GigabitEthernet0/0/1 :
Input: total 0 packets
  Bootp reply            :          0
  Offer                  :          0
  Ack                    :          0
  Nak                    :          0
  Dropped untrusted reply :          0
Output: total 0 packets
  Bootp request          :          0
  Discover               :          0
  Request                :          0
    Request of init-reboot:          0
    Request of selecting  :          0
    Request of renewing   :          0
    Request of rebinding  :          0
  Decline                :          0
  Release                :          0
```

Table 6-19 Description of the **display dhcp client statistics** command output

Item	Description
Input	Total number of DHCP messages received by the client.
Bootp reply	Number of BOOTP replies received by the client from the server.
Offer	Number of Offer messages received by the client from the server.
Ack	Number of ACK messages received by the client from the server.
Nak	Number of NAK messages received by the client from the server.
Dropped untrusted reply	Number of untrusted reply messages discarded by the device.
Output	Total number of messages forwarded by the client.
Bootp request	Number of BOOTP requests received by the server from the client.
Discover	Number of Discover messages received by the server from the client.
Request	Number of Request messages received by the server from the client.
Request of init-reboot	Number of Request of init-reboot messages received by the server from the client.
Request of selecting	Number of Request of selecting messages received by the server from the client.
Request of renewing	Number of Request of renewing messages received by the server from the client.
Request of rebinding	Number of Request of rebinding messages received by the server from the client.
Decline	Number of Decline messages received by the server from the client.
Release	Number of Release messages received by the server from the client.

6.3.71 display dhcp configuration

Function

The **display dhcp configuration** command displays the configuration of a DHCP public module.

Format

display dhcp configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the configuration of a DHCP public module.

Example

Display the configuration of a DHCP public module.

```
<HUAWEI> display dhcp configuration
  DHCP global running information :
  DHCP                                      : Enable
  DHCP speed limit                          : Disable  (default)
  DHCP anti-attack check duplicate option   : Disable  (default)
  DHCP broadcast suppress                   : Disable  (default)
  DHCP anti-attack check udp-checksum       : Enable   (default)
  DHCP anti-attack check magic-cookie       : Disable  (default)
  DHCP udp-checksum                         : Disable  (default)
```

Table 6-20 Description of the **display dhcp configuration** command output

Item	Description
DHCP global running information	Global configuration of a DHCP public module.

Item	Description
DHCP	Whether DHCP is enabled. The value can be: - Enable: DHCP is enabled. - Disable (default): DHCP is disabled. By default, DHCP is disabled. To configure this parameter, run the **dhcp enable** command.
DHCP speed limit	Whether dynamic DHCP packet rate limiting is enabled. The value can be: - Enable: This function is enabled. - Disable (default): This function is disabled. By default, dynamic DHCP packet rate limiting is disabled. To configure this parameter, run the **dhcp speed-limit auto** command.
DHCP anti-attack check duplicate option	Whether the function of checking and discarding DHCP packets with duplicate options is enabled. The value can be: - Enable: This function is enabled. - Disable (default): This function is disabled. By default, the function of checking and discarding DHCP packets with duplicate options is disabled. To configure this parameter, run the **dhcp anti-attack check duplicate option** command.
DHCP broadcast suppress	Whether DHCP broadcast suppression is enabled. The value can be: - Enable: This function is enabled. - Disable (default): This function is disabled. By default, DHCP broadcast suppression is disabled. To configure this parameter, run the **dhcp broadcast suppress enable** command.

Item	Description
DHCP anti-attack check udp-checksum	Whether the function of checking the UDP header checksum in a DHCP packet and discarding a DHCP packet with an incorrect checksum is enabled. The value can be: ● Enable (default): This function is enabled. By default, a device checks the UDP header checksum in a DHCP packet and discards a DHCP packet with an incorrect checksum. ● Disable: This function is disabled. To configure this parameter, run the **dhcp anti-attack check duplicate option** command.
DHCP anti-attack check magic-cookie	Whether the function of checking the magic cookie field in a DHCP packet and discarding a DHCP packet with an incorrect magic cookie field value is enabled. The value can be: ● Enable: This function is enabled. ● Disable (default): This function is disabled. By default, a device does not check the magic cookie field in a DHCP packet but directly forwards a DHCP packet with an incorrect magic cookie field value. To configure this parameter, run the **dhcp anti-attack check magic-cookie** command.
DHCP udp-checksum	Whether a device is enabled to add the UDP header checksum to DHCP packets to be sent. The value can be: ● Enable: The device is enabled to add the UDP header checksum to DHCP packets to be sent. ● Disable (default): The device is disabled from adding the UDP header checksum to DHCP packets to be sent. By default, the UDP header checksum carried in DHCP packets sent by a device is 0, and the peer device does not verify the checksum. To configure this parameter, run the **dhcp udp-checksum enable** command.

6.3.72 display dhcp option template

Function

The **display dhcp option template** command displays the configuration of a DHCP Option template.

Format

display dhcp option template [**name** *template-name*]

Parameters

Parameter	Description	Value
name *template-name*	Displays the configuration of a specified DHCP Option template.	The template must be an existing DHCP Option template.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a DHCP Option template, you can run the **display dhcp option template** command to view the configuration of the DHCP Option template, including the template name, number, IP address of a server configured for the client after the client automatically obtains the IP address, domain name, and values of customized options.

Example

Display the configuration of the DHCP Option template named **test**.

```
<HUAWEI> display dhcp option template name test
 -------------------------------------------------------------------------------
  Template-Name  : test
  Template-No    : 1
  Next-server    : 192.168.1.5
  Domain-name    : example.com
  DNS-server0    : 192.168.2.7
  DNS-server1    : 192.168.2.8
  NBNS-server0   : 192.168.1.7
  NBNS-server1   : 192.168.1.8
```

```
 Netbios-type   : b-node
 Gateway-0      : 192.168.1.10
```

Display the configurations of all DHCP Option templates.

```
<HUAWEI> display dhcp option template
 -------------------------------------------------------------------------------
 Template-Name  : template1
 Template-No    : 0
 Next-server    : 10.1.1.4
 Domain-name    : -
 DNS-server0    : -
 NBNS-server0   : -
 Netbios-type   : -
 Gateway-0      : -

 -------------------------------------------------------------------------------
 Template-Name  : template2
 Template-No    : 1
 Next-server    : 192.168.1.5
 Domain-name    : example.com
 Option-code      : 64
   Option-subcode : 3
     Option-type  : hex
     Option-value : 11
 DNS-server0    : 192.168.2.7
 DNS-server1    : 192.168.2.8
 NBNS-server0   : 192.168.2.7
 NBNS-server1   : 192.168.2.8
 Netbios-type   : b-node
 Gateway-0      : 192.168.1.10
```

Table 6-21 Description of the **display dhcp option template** command output

Item	Description
Template-Name	Name of the DHCP Option template. To specify the parameter, run the **dhcp option template** command.
Template-No	Index value of the DHCP Option template.
Next-server	IP address of a server configured for the client after the client automatically obtains the IP address. To specify the parameter, run the **next-server** command in the DHCP Option template view.
Domain-name	Name of a domain. To specify the parameter, run the **domain-name** command in the DHCP Option template view.
Option-code	Code for a customized option. To specify the parameter, run the **option** command in the DHCP Option template view.

Item	Description
Option-subcode	Code for a customized sub-option. To specify the parameter, run the **option** command in the DHCP Option template view.
Option-type	Character string type for a customized option. To specify the parameter, run the **option** command in the DHCP Option template view.
Option-value	Character string value for a customized option. To specify the parameter, run the **option** command in the DHCP Option template view.
DNS-server0	Address of the DNS server. Currently, a maximum of eight DNS server addresses can be configured. Values 0 and 1 indicate the first and second DNS server addresses respectively. To specify the parameter, run the **dns-list** command in the DHCP Option template view.
NBNS-server0	Address of the NetBIOS server. Currently, a maximum of eight NetBIOS server addresses can be configured in a DHCP Option template. Values 0 and 1 indicate the first and second NetBIOS server addresses respectively. To specify the parameter, run the **nbns-list** command in the DHCP Option template view.
Netbios-type	NetBIOS node type. To specify the parameter, run the **netbios-type** command in the DHCP Option template view.
Gateway-0	Gateway address. Currently, a maximum of eight gateway addresses can be configured. The value 0 indicates the first gateway address. To specify the parameter, run the **gateway-list** command in the DHCP Option template view.

6.3.73 display dhcp relay

Function

The **display dhcp relay** command displays configuration information about a DHCP relay agent.

Format

display dhcp relay { **configuration** | **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
configuration	Displays configuration information about DHCP relay agents configured globally and on all interfaces.	-
all	Displays configuration information about DHCP relay agents configured on all interfaces.	-
interface *interface-type interface-number*	Displays configuration information about a DHCP relay agent configured on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration information about DHCP relay agents configured globally and on interfaces.

Example

Display configuration information about DHCP relay agents on all interfaces.

```
<HUAWEI> display dhcp relay configuration
  DHCP relay global running information :
  DHCP relay address cycle           : Disable (default)
  DHCP relay trust option82          : Enable  (default)
  DHCP relay request server-match    : Enable  (default)
  DHCP relay reply forward all       : Disable (default)
 DHCP relay agent running information of interface
Vbdif100 :
 Server IP address [00] : 10.1.1.1
 Gateway address in use : 10.10.1.10
 Anycast gateway re-route: disable
 GIADDR source interface : LoopBack1
 Link-selection insert  : enable
 DHCP relay agent running information of interface Vlanif5 :
 Server group name      : group1
 Gateway address in use : 10.100.100.1
 Gateway switch         : enable
 DHCP relay agent running information of interface Vlanif100 :
 Server IP address [00] : 10.2.2.3
 VPN instance      [00] : vpn1
 Gateway address in use : 10.2.2.2
```

Table 6-22 Description of the **display dhcp relay configuration** command output

Item	Description
DHCP relay global running information	Configuration information about DHCP relay agents configured globally.
DHCP relay address cycle	Whether the DHCP server polling function is enabled on a DHCP relay agent. - Enable: The DHCP server polling function is enabled on a DHCP relay agent. - Disable: The DHCP server polling function is disabled on a DHCP relay agent. To configure this item, run the **ip relay address cycle** command.
DHCP relay trust option82	Whether Option 82 is enabled on a DHCP relay agent. - Enable: Option 82 is enabled on a DHCP relay agent. - Disable: Option 82 is disabled on a DHCP relay agent. To configure this item, run the **dhcp relay trust option82** command.

Item	Description
DHCP relay request server-match	Whether a DHCP relay agent is enabled to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded. ● Enable: A DHCP relay agent is enabled to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded. ● Disable: A DHCP relay agent is disabled from checking the DHCP server identifier (Option54) in a DHCP Request message to be forwarded. To configure this item, run the **dhcp relay request server-match enable** command.
DHCP relay reply forward all	Whether a DHCP relay agent is enabled to forward all DHCP ACK messages. ● Enable: A DHCP relay agent is enabled to forward all DHCP ACK messages. ● Disable: A DHCP relay agent is disabled from forwarding all DHCP ACK messages. To configure this item, run the **dhcp relay reply forward all enable** command.
DHCP relay agent running information of interface *if*	DHCP relay agent configuration of the *if* interface.
Server group name	Group name of the DHCP Server. To specify the parameter, run the **dhcp relay server-select** command.
Server IP address [x]	IP address of a DHCP server in the DHCP server group. The value x is the index of a DHCP server. To specify the parameter, run the **dhcp-server** command.
VPN instance [xx]	VPN instance bound to the interface. The value xx indicates the index of the VPN instance. **NOTE** This field is displayed in the command output only when a VPN instance is specified using the **dhcp relay server-ip** command.
Gateway address in use	IP address of the DHCP gateway. To specify the parameter, run the **gateway** command in the DHCP server group view.

Item	Description
Anycast gateway re-route	Whether the re-routing function for the DHCP relay agent is enabled. The value can be: - Enable: The re-routing function for the DHCP relay agent is enabled. - Disable: The re-routing function for the DHCP relay agent is disabled. To configure this item, run the **dhcp relay anycast gateway re-route enable** command.
GIADDR source interface	Source interface of DHCP relayed packets. To configure this item, run the **dhcp relay giaddr source-interface** command.
Link-selection insert	Whether the function of inserting the Link-selection suboption of the Option82 field into DHCP packets is enabled. The value can be: - Enable: The function of inserting the Link-selection suboption of the Option82 field into DHCP packets is enabled. - Disable: The function of inserting the Link-selection suboption of the Option82 field into DHCP packets is disabled. To configure this item, run the **dhcp relay information link-selection insert enable** command.
Gateway switch	Whether automatic gateway switchover is enabled on a DHCP relay agent. The value can be: - Enable: The automatic gateway switchover on a DHCP relay agent is enabled. - Disable: The automatic gateway switchover on a DHCP relay agent is disabled. To configure this item, run the **dhcp relay gateway-switch enable** command.

6.3.74 display dhcp relay statistics

Function

The **display dhcp relay statistics** command displays message statistics on a DHCP relay agent.

Format

display dhcp relay statistics [**server-group** *group-name*]

Parameters

Parameter	Description	Value
server-group *group-name*	Displays message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. If this parameter is not specified, message statistics on DHCP relay agents connected to all DHCP servers are displayed.	The value must be an existing DHCP server group on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dhcp relay statistics** command to view the statistics about the packets received and sent by a DHCP relay agent, so as to check whether the client is correctly configured or the network is connected.

- Run the **display dhcp relay statistics server-group** *group-name* command to check message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. The DHCP server group name needs to be specified.
- Run the **display dhcp relay statistics** command to check message statistics on all DHCP relay agents besides DHCP relay agents connected to DHCP servers in the DHCP server group.

Follow-up Procedure

After detecting incorrect message statistics on a DHCP relay agent, run the **reset dhcp relay statistics** [**server-group** *group-name*] command to clear message statistics on the DHCP relay agent.

Example

Display message statistics on a DHCP relay agent.

```
<HUAWEI> display dhcp relay statistics
 The statistics of DHCP RELAY:
   DHCP packets received from clients         : 0
      DHCP DISCOVER packets received         : 0
      DHCP REQUEST packets received          : 0
      DHCP RELEASE packets received          : 0
      DHCP INFORM packets received           : 0
      DHCP DECLINE packets received          : 0
   DHCP packets sent to clients              : 0
      Unicast packets sent to clients        : 0
      Broadcast packets sent to clients      : 0
   DHCP packets received from servers         : 0
      DHCP OFFER packets received            : 0
      DHCP ACK packets received              : 0
      DHCP NAK packets received              : 0
   DHCP packets sent to servers              : 0
   DHCP Bad packets received                 : 0
```

Table 6-23 Description of the **display dhcp relay statistics** command output

Item	Description
DHCP packets received from clients	DHCP messages received from clients.
DHCP DISCOVER packets received	DHCP Discover messages received from clients.
DHCP REQUEST packets received	DHCP Request messages received from clients.
DHCP RELEASE packets received	DHCP Release messages received from clients.
DHCP INFORM packets received	DHCP Inform messages received from clients.
DHCP DECLINE packets received	DHCP Decline messages received from clients.
DHCP packets sent to clients	DHCP messages sent to clients.
Unicast packets sent to clients	Unicast packets sent to clients.
Broadcast packets sent to clients	Broadcast packets sent to clients.
DHCP packets received from servers	DHCP messages received from servers.
DHCP OFFER packets received	DHCP Offer messages received from servers.
DHCP ACK packets received	DHCP ACK messages received from servers.
DHCP NAK packets received	DHCP NAK messages received from servers.
DHCP packets sent to servers	DHCP messages sent to servers.

Item	Description
DHCP Bad packets received	DHCP error messages received.

6.3.75 display dhcp server configuration

Function

The **display dhcp server configuration** command displays DHCP server configuration.

Format

display dhcp server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the Switch functions as a DHCP server, you can run the **display dhcp server configuration** command to check DHCP server configuration.

Example

Display DHCP server configuration.

```
<HUAWEI> display dhcp server configuration
  DHCP server global running information :
  DHCP server bootp                : Disable (default)
  DHCP server bootp automatic      : Disable (default)
  DHCP server ping packet          : 2       (default)
  DHCP server ping timeout         : 500     (default)
  DHCP server trust option82       : Enable  (default)
  DHCP server force response       : Disable (default)

  DHCP server running information for interface Vlanif10 :
  DHCP server mode                 : Interface

  DHCP server running information for interface
Vlanif20 :
  DHCP server mode                 : Global
```

Table 6-24 Description of the **display dhcp server configuration** command output

Item	Description
DHCP server global running information	Global DHCP server configuration.
DHCP server bootp	Whether the DHCP server is enabled to respond to BOOTP requests. To configure this item, run the **dhcp server bootp** command.
DHCP server bootp automatic	Whether the DHCP server is enabled to dynamically assign IP addresses to BOOTP clients. To configure this item, run the **dhcp server bootp automatic** command.
DHCP server ping packet	Maximum number of ping packets sent by the DHCP server. To configure this item, run the **dhcp server ping** command.
DHCP server ping timeout	Maximum time to wait for a response to the ping packet sent by the DHCP server. To configure this item, run the **dhcp server ping** command.
DHCP server trust option82	Whether the DHCP server is enabled to trust the Option 82 field. To configure this item, run the **dhcp server trust option82** command.
DHCP server force response	Whether the DHCP server is enabled to reply with DHCP NAK messages. To configure this item, run the **dhcp server force response** command.
DHCP server running information for interface *ifn*	DHCP server configuration on an interface.
DHCP server mode	DHCP server mode. The value can be: ● Interface: indicates a DHCP server based on an interface address pool. To configure this item, run the **dhcp select interface** command. ● Global: indicates a DHCP server based on the global address pool. To configure this item, run the **dhcp select global** command.

6.3.76 display dhcp server database

Function

The **display dhcp server database** command displays information about the DHCP database.

Format

display dhcp server database

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display dhcp server database** command displays the storage path and file name of DHCP data on a DHCP server. This information helps to check:

- Whether the function that saves DHCP data to the storage device is enabled. If this function is not enabled, run the **dhcp server database** command to enable it.
- Whether the interval at which DHCP data is saved is proper.
- Whether the function that recovers DHCP data from the storage device after the system restarts is enabled.

Precautions

The function that saves DHCP data to storage devices and the function that recovers DHCP data from storage devices can be enabled in any sequence.

Example

Display information about the DHCP database.

```
<HUAWEI> display dhcp server database
 Status: disable
 Recover from files after reboot: disable
 File saving lease items: flash:/dhcp/lease.txt
 File saving conflict items: flash:/dhcp/conflict.txt
 Save Interval: 300 (seconds)
```

Table 6-25 Description of the **display dhcp server database** command output

Item	Description
Status	Whether to save the data to the storage device: ● disable ● enable The value is set using the **dhcp server database** command.
Recover from files after reboot	Whether to recover data from the file on the storage device after the system restarts: ● disable ● enable The value is set using the **dhcp server database** command.
File saving lease items	File name and path of the file for storing address lease information.
File saving conflict items	File name and path of the file for storing address conflict information.
Save Interval	Interval at which DHCP data is saved, in seconds. The value is set using the **dhcp server database** command.

6.3.77 display dhcp server group

Function

The **display dhcp server group** command displays the configuration of a DHCP server group.

Format

display dhcp server group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified DHCP server group.	The value must be an existing DHCP server group on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display dhcp server group** command displays information about all the DHCP server groups of a DHCP relay agent and the number of DHCP servers in the DHCP server groups. If *group-name* is specified, the **display dhcp server group** *group-name* command displays DHCP server addresses and the number of DHCP servers in a specified DHCP server group.

Prerequisites

A DHCP server group has been created on a DHCP relay agent using the **dhcp server group** command.

Example

Display the configuration of the DHCP server group **myServers**.

```
<HUAWEI> display dhcp server group myServers
 Group-name          : myServers
   (0)  Server-IP    : 10.1.1.1
        VPN instance : vpn1
  Gateway            : 10.10.10.1
```

Table 6-26 Description of the **display dhcp server group** command output

Item	Description
Group-name	Name of a DHCP server group. To specify the parameter, run the **dhcp server group** command.
(x) Server-IP	IP addresses of DHCP servers in a DHCP server group. x is the index of the IP addresses and ranges from 0 to 19. To specify the parameter, run the **dhcp-server** command.
VPN instance	VPN instance to which the DHCP server group belongs. **NOTE** This field is displayed in the command output only when a VPN instance is specified using the **dhcp-server** command.

Item	Description
Gateway	Gateway address of the DHCP server in the DHCP server group. To specify the parameter, run the **gateway** command in the DHCP server group view.

6.3.78 display dhcp server statistics

Function

The **display dhcp server statistics** command displays statistics on a DHCP server.

Format

display dhcp server statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the display dhcp server statistics command to check whether the client is correctly configured or the network is connected.

Follow-up Procedure

After detecting incorrect message statistics on a DHCP server, run the **reset dhcp server statistics** command to clear message statistics on the DHCP server.

Example

Display statistics on the DHCP server.

```
<HUAWEI> display dhcp server statistics
 DHCP Server Statistics:

 Client Request:              6
  Dhcp Discover:              1
  Dhcp Request:               4
  Dhcp Decline:               0
  Dhcp Release:               1
```

```
 Dhcp Inform:            0
Server Reply:            4
 Dhcp Offer:             1
 Dhcp Ack:               3
 Dhcp Nak:               0
Bad Messages:            0
```

Table 6-27 Description of the **display dhcp server statistics** command output

Item	Description
DHCP Server Statistics	Statistics on the DHCP server.
Client Request	Number of DHCP messages sent from the DHCP client to the DHCP server.
Dhcp Discover, Dhcp Request, Dhcp Decline, Dhcp Release, Dhcp Inform	Numbers of different types of DHCP messages sent from the DHCP client to the DHCP server.
Server Reply	Number of DHCP messages sent from the DHCP server to the DHCP client.
Dhcp Offer, Dhcp Ack, Dhcp Nak	Numbers of different types of DHCP messages sent from the DHCP server to the DHCP client.
Bad Messages	Number of unknown messages.

6.3.79 display dhcp statistics

Function

The **display dhcp statistics** command displays DHCP message statistics.

Format

display dhcp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp statistics** command displays statistics about sent and received DHCP messages.

Example

Display DHCP message statistics.

```
<HUAWEI> display dhcp statistics
Input: total 172 packets, discarded 0 packets
  Bootp request          :          0,  Bootp reply            :          0
  Discover               :          0,  Offer                  :        172
  Request                :          0,  Ack                    :          0
  Release                :          0,  Nak                    :          0
  Decline                :          0,  Inform                 :          0

  Rx buffers full        :       2978,  L2fdb lookup failed    :         38

Output: total 172 packets, discarded 0 packets
```

Table 6-28 Description of the **display dhcp statistics** command output

Item	Description
Bootp request	Number of BOOTP requests sent by the device that functions as the client.
Bootp reply	Number of BOOTP replies received by the client from the server.
Discover	Number of Discover messages received by the server from the client.
Offer	Number of Offer messages received by the client from the server.
Request	Number of BOOTP requests received by the server from the client.
Ack	Number of ACK messages received by the client from the server.
Release	Number of Release messages received by the server from the client.
Nak	Number of NAK messages received by the client from the server.
Decline	Number of Decline messages sent by the client.
Inform	Number of Inform messages sent by the client.

Item	Description
Rx buffers full or L2fdb lookup failed	Information displayed when the DHCP service is abnormal. The displayed information includes: - Rx buffers full: Total number of DHCP packets discarded because the remaining queue length is shorter than the reserved threshold. - L2fdb lookup failed: Total number of DHCP ACK packets discarded because the DHCP snooping module fails to find user-side interfaces. - High cpu occupancy: Total number of DHCP packets discarded because the CPU usage is excessively high. - Port blocked: Total number of DHCP packets discarded because the inbound interface is blocked. - Bad vlan id: Total number of DHCP packets discarded because the interfaces receiving the DHCP packets are not added to the VLANs corresponding to the VLAN tags carried in the packets or the DHCP packets received on interfaces carry VLAN tags not in the range from 1 to 4094. - Memory exhausted: Total number of DHCP packets discarded because the memory is exhausted. - L3if protocol down: Total number of DHCP packets discarded because the Layer 3 protocol of the source interface goes Down. - Rate limit: Total number of DHCP packets discarded because rates of the packets exceed the limit, when the **dhcp snooping check dhcp-rate enable** command is configured. - Bad packet length: Total number of DHCP packets discarded because the packet length is not in the range of 50 to 2048 bytes. - Bad ip header length: Total number of DHCP packets discarded because the IP header length is not in the range of 20 to 60 bytes

Item	Description
	- Bad ip header checksum: Total number of DHCP packets discarded because the checksum of the IP header is incorrect. - Bad udp checksum: Total number of DHCP packets discarded because the checksum of the UDP header is incorrect. - Hops exceeded: Total number of DHCP request packets discarded by the DHCP relay agent because the hop count exceeds 16. - Bad magic cookie: Total number of DHCP packets discarded because the magic-cookie field is incorrect. - Duplicate option: Total number of DHCP packets discarded because the option fields are duplicate. - Bad option length: Total number of DHCP packets discarded because the option field length is incorrect. - End option absent: Total number of DHCP packets discarded because of the incorrect end option. - Dest-port equals source: Total number of DHCP packets discarded because the source interface is also the outbound interface. - Bad chaddr: Total number of DHCP packets discarded due to incorrect client MAC addresses. A DHCP packet is discarded due to an incorrect client MAC address if a DHCP relay agent finds that the MAC address in the CHADDR field of the DHCP packet is not a unicast address, a DHCP snooping-enabled device finds that the MAC address in the CHADDR field of the DHCP request packet is different from the source MAC address, or the MAC address in the CHADDR field of the DHCP packet conflicts with the DHCP server MAC address. - Bad giaddr: Total number of DHCP packets discarded due to incorrect values in the GIADDR field, when

Item	Description
	the **dhcp snooping check dhcp-giaddr enable** command is configured to check whether the GIADDR field in received DHCP packets is 0 or carries an invalid IP address, such as a loopback address. ● Bad request: Total number of invalid DHCP request packets that are discarded, when the **dhcp snooping check dhcp-request enable** command is configured to check the validity of DHCP packets. ● Bad reply: Total number of DHCP response packets discarded by untrusted interfaces configured with the **dhcp snooping enable** command. ● Bad dest udp-port: Total number of DHCP request packets discarded by the DHCP relay agent because the destination port number is UDP port 68. ● Bad message type: Total number of DHCP packets discarded because they are neither requests nor responses. ● Max-user limit: Total number of DHCP packets discarded because the maximum number of users (configured by using the **dhcp snooping max-user-number** command) is exceeded. ● Add bindtable failed: Total number of DHCP packets discarded because dynamic binding entries are added. New dynamic binding entries may be added if the user-side interface is Down, or IPSG is configured but ACL resources are insufficient. ● Client transferred: Total number of DHCP packets discarded because the **undo dhcp snooping user-transfer enable** command is configured to disable location transition for DHCP snooping users.

Item	Description
	- Other error: Total number of DHCP packets discarded due to other reasons.

6.3.80 display ip pool

Function

The **display ip pool** command displays configured IP address pool information.

Format

display ip pool

display ip pool interface *interface-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]

display ip pool name *ip-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** [**user-type** { **dhcp** | **l2tp** | **ipsec** | **ssl-vpn** }]]

display ip pool vpn-instance *vpn-instance-name*

display ip pool global interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-pool-name*	Displays the configuration of the specified interface address pool. **NOTE** An interface address pool is often specified using the interface type and interface number, which are not separated by spaces.	The interface address pool must exist on the device.
name *ip-pool-name*	Displays the configuration of the specified global address pool.	The global address pool must exist on the device.
start-ip-address [*end-ip-address*]	Displays the IP addresses within the range specified by the start IP address in an IP address pool. If *end-ip-address* is specified, the end IP address is also specified.	The value is in dotted decimal notation.

Parameter	Description	Value
all	Displays information about all IP addresses in an IP address pool.	-
conflict	Displays information about conflicting IP addresses in an address pool. (If an IP address that the DHCP server prepares to assign to a user exists on the network, the IP address will be added to the conflict list. This problem occurs when a static IP address is configured or an active/standby switchover occurs in a VRRP group if the range of IP addresses in the address pools on the master and backup devices overlap.)	-
expired	Displays information about expired and idle IP addresses in an IP address pool.	-
used [**user-type** { **dhcp** | **l2tp** | **ipsec** | **ssl-vpn** }]	Displays information about used IP addresses of the specified user type in an IP address pool: ● **dhcp** indicates users who obtain IP addresses through DHCP. ● **l2tp** indicates L2TP users. ● **ipsec** indicates IPSec users. ● **ssl-vpn** indicates SSL VPN users.	-
vpn-instance *vpn-instance-name*	Displays information about the address pool in a specified VPN instance.	The value must be an existing VPN instance name.
global interface *interface-type interface-number*	Displays information about the address pool on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip pool** command to view information about configured IP address pools and IP addresses in them, including the IP address pool name, lease, lock status, and IP address status.

Example

Display information about conflicting addresses in the IP address pool named **test**.

```
<HUAWEI> display ip pool name test conflict
 Pool-name        : test
 Pool-No          : 1
 Lease            : 1 Days 0 Hours 0 Minutes
 Domain-name      : -
 Option-code      : 60
  Option-subcode : --
  Option-type    : cipher
  Option-value   : %^%#5g)NPN1M,$M;pQ-lT\P>Al6QN4#ldIVVjD69XlCN%^%#
 DNS-server0      : -
 NBNS-server0     : -
 Netbios-type     : -
 Position         : Local
 Status           : Unlocked
 Gateway-0        : -
 Network          : 192.168.0.0
 Mask             : 255.255.255.0
 VPN instance     : --
 Bootfile         : 43534
 Logging          : Enable
 Conflicted address recycle interval: 1 Days 0 Hours 0 Minutes
 Address Statistic: Total       :254       Used        :1
                    Idle        :252       Expired     :2
                    Conflict    :1         Disabled    :0


 -----------------------------------------------------------------------------
 Network section
       Start           End       Total    Used Idle(Expired) Conflict Disabled
 -----------------------------------------------------------------------------
    192.168.0.1   192.168.0.254     254       1        252(2)       1     0
 -----------------------------------------------------------------------------
 Client-ID format as follows:
  DHCP  : mac-address                PPPoE   : mac-address
  IPSec : user-id/portnumber/vrf      PPP     : interface index
  L2TP  : cpu-slot/session-id        SSL-VPN : user-id/session-id
 -----------------------------------------------------------------------------
 Index              IP            Client-ID    Type       Left   Status
 -----------------------------------------------------------------------------
   109   192.168.0.110                     -       -          -   Conflict
 -----------------------------------------------------------------------------
```

Table 6-29 Description of the **display ip pool** command output

Item	Description
Pool-name	Name of an IP address pool. To configure this parameter, run the **ip pool (system view)** command.
Pool-No	Index of the IP address pool.

Item	Description
Lease	Lease of the IP address pool. To configure this parameter, run the **lease** command.
Domain-name	Domain name. To configure this parameter, run the **domain-name** command.
Option-code	Value of a customized option. To configure this parameter, run the **option** command.
Option-subcode	Value of a customized sub-option. To configure this parameter, run the **option** command.
Option-type	Type of a customized option code: ● ascii: indicates that the customized option code is an ASCII character string. ● hex: indicates that the customized option code is a hexadecimal string. ● cipher: indicates that the customized option code is a ciphertext character string. To configure this parameter, run the **option** command.
Option-value	Content of a customized option. To configure this parameter, run the **option** command.
DNS-server0	Address of the DNS server. Currently, an IP address pool can be configured with up to eight DNS servers. The value 0 indicates the first DNS server address and the value 1 indicates the second DNS server address. To configure this parameter, run the **dns-list** command.
NBNS-server0	Address of the NetBIOS server. Currently, an address pool can be configured with up to eight NetBIOS server addresses. The value 0 indicates the first NetBIOS server address. To configure this parameter, run the **nbns-list** command.

Item	Description
Netbios-type	NetBIOS type. To configure this parameter, run the **netbios-type** command.
Position	Position of the IP address pool.
Status (First)	Status of the IP address pool. To configure this parameter, run the **lock (IP address pool view)** command.
Gateway-0	Gateway address. Currently, a maximum of eight gateway addresses can be configured in an IP address pool. The value 0 indicates the first gateway address. To configure this parameter, run the **gateway-list** command.
Network	Network segment of the IP address pool.
Mask	Subnet mask of the IP address pool. To configure this parameter, run the **network (IP address pool view)** command.
Bootfile	Name of the startup configuration file configured for the DHCP client. To configure this parameter, run the **bootfile** command.
VPN instance	Name of a VPN instance.
Logging	Status of the logging function when the DHCP server assigns IP addresses. ● Enable ● Disable To configure this parameter, run the **logging** or **dhcp server logging** command.
Conflicted address recycle interval	Interval for automatically reclaiming conflicting IP addresses in the IP address pool. To configure this parameter, run the **conflict auto-recycle interval day** *day* [**hour** *hour* [**minute** *minute*]] command.

Item	Description
Address Statistic	Statistics about IP addresses in the IP address pool.
Start	Start IP address of the IP address pool.
End	End IP address of the IP address pool.
Total	Total number of IP addresses in the IP address pool. Total = Used + Idle(Expired) + Conflict + Disable
Used	Number of used IP addresses in the IP address pool.
Idle(Expired)	Number of idle (expired) IP addresses in the address pool. **NOTE** If the mask length of the address pool is shorter than that of the interface IP address on the DHCP server, users may fail to go online even when there are idle IP addresses in the address pool.
Conflict	Number of conflicting IP addresses in the IP address pool. **NOTE** If there are many conflicting IP addresses in the address pool, it is recommended that you configure the **conflict auto-recycle interval** command to reclaim conflicting IP addresses periodically. This configuration reduces occupation of idle IP addresses in the address pool and prevents IP address conflicts on the network.
Disabled	Number of disabled IP addresses in the IP address pool.

Item	Description
Client-ID format as follows	Client ID format: ● DHCP: mac-address. The client ID format of DHCP users is a MAC address. ● PPPoE: mac-address. The client ID format of PPPoE users is a MAC address. ● IPSec: user-id/portnumber/vrf. The client ID format of IPSec users is a user ID, port number, or VPN index. ● PPP: interface index. The client ID format of PPP users is an interface index. ● L2TP: cpu-slot/session-id. The client ID format of L2TP users is a CPU ID-slot ID or session ID. ● SSL-VPN: user-id/session-id. The client ID format of SSL-VPN users is a user ID or session ID.
Index	Index.
IP	IP address.
Client-ID	DHCP client ID.
Type	DHCP client type. The types include DHCP, PPPoE, IPSec, PPP, L2TP, and SSL-VPN.
Left	Remaining lease of an IP address. When the result of the calculation formula ([**Lease** – **Left**]/**Lease**) is 50% or 87.5%, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease. If the renewal succeeds, the value of the **Left** field is recounted. If the renewal fails, the DHCP client requests an IP address again and the status of its original IP address is set to **Expired**.

Item	Description
Status (Second)	Status of an IP address: - Used: indicates that the IP address is used. - Idle: indicates that the IP address is idle. - Expired: indicates that the lease of the IP address expires and the IP address is idle. - Conflict: indicates that the IP address conflicts with another IP address on the network. - Disable: indicates that the IP address cannot be used. - Static-bind: indicates that the IP address is bound to a MAC address. - Static-bind used: indicates that the IP address is bound to a MAC address and used.

6.3.81 dns-list

Function

The **dns-list** command configures the DNS server address for the DHCP client.

The **undo dns-list** command deletes a configured DNS server address.

By default, no DNS server address is configured.

Format

IP address pool view

dns-list { *ip-address* &<1-8> | **unnumbered interface** *interface-type interface-number* }

undo dns-list { *ip-address* | **unnumbered interface** | **all** }

DHCP Option template view

dns-list *ip-address* &<1-8>

undo dns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the DNS server address.	The value is in dotted decimal notation. A maximum of eight DNS server addresses can be configured. These IP addresses are separated by spaces.
unnumbered interface *interface-type interface-number*	Borrows the DNS server address obtained by the interface as the DNS server IP address.	-
all	Deletes all DNS server addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If user hosts access hosts on the network by domain names, user hosts need to send DNS requests to the DNS server and resolve the domain name to access for communication. To connect a DHCP client to the network, configure a DHCP server address so that the DHCP server can assign both the specified DNS server address and an IP address to the client. To configure DNS server addresses for an interface address pool, run the **dhcp server dns-list** command.

Precautions

In the IP address pool view and DHCP Option template view, a device can be configured with a maximum of eight DNS server addresses respectively. The address first assigned to the clients functions as the primary address, and the other seven addresses function as secondary addresses.

Example

In the IP address pool view, set the IP address of the DNS server to 10.10.10.10.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] dns-list 10.10.10.10
```

In the DHCP Option template view, set the IP address of the DNS server to 10.10.10.10.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] dns-list 10.10.10.10
```

6.3.82 domain-name

Function

The **domain-name** command configures the domain name suffix for DHCP clients.

The **undo domain-name** command deletes a configured domain name suffix.

By default, no domain name suffix is configured for DHCP clients.

Format

domain-name *domain-name*

undo domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies a domain name to be assigned to a DHCP client.	The value is a string of 1 to 63 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

This command applies to DHCP servers. When allocating an IP address to a client, a DHCP server can also assign a domain name suffix to the client. You can run the **domain-name** command on the DHCP server to specify the domain name suffix for clients. After this command is run, the DHCP server will send the domain name suffix to a client when allocating an IP addresses to the client.

To configure a domain name for an interface address pool, run the **dhcp server domain-name (interface view)** command.

Example

In the IP address pool view, configure the domain name suffix assigned to the DHCP client as **example.com**.

```
<HUAWEI> system-view
[HUAWEI] ip pool test
[HUAWEI-ip-pool-test] domain-name example.com
```

In the DHCP Option template, configure the domain name suffix assigned to the DHCP client as **example.com**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] domain-name example.com
```

6.3.83 excluded-ip-address

Function

The **excluded-ip-address** command specifies the range of IP addresses that cannot be automatically assigned to clients from an address pool.

The **undo excluded-ip-address** command deletes the specified range of IP addresses that cannot be automatically assigned to clients from an address pool.

By default, all IP addresses in an address pool can be automatically assigned to clients.

Format

excluded-ip-address *start-ip-address* [*end-ip-address*]

undo excluded-ip-address *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address of the IP address segment where addresses cannot be automatically assigned to clients.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address of the IP address segment where addresses cannot be automatically assigned to clients. If *end-ip-address* is not specified, only the IP address corresponding to *start-ip-address* cannot be automatically assigned.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **excluded-ip-address** command applies to DHCP servers. Fixed IP addresses are allocated to some specific hosts (such as the WWW server) on the network for a long time. If these hosts' IP addresses are overlapped with IP addresses in the address pool and the DHCP server allocates these overlapped IP addresses to other hosts, IP address conflicts may occur. To prevent such IP address conflicts, you need to exclude these IP addresses from being automatically assigned in the address pool.

You can run the **excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the global address pool.

You can run the **dhcp server excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the interface address pool.

Prerequisites

Network segment addresses that can be assigned from the global address pool have been configured using the **network (IP address pool view)** command.

Precautions

- The excluded IP address or IP address segment must be in the local address pool.
- You do not need to exclude the gateway address configured using the **gateway-list** command from being automatically allocated. The device automatically adds the gateway address into the list of IP addresses that cannot be automatically allocated.

  You do not need to exclude the IP address of a server's interface connecting to a client from being automatically allocated. The device automatically sets the status of the interface IP address to Conflict during address assignment.
- If you run the **excluded-ip-address** command multiple times, you can specify multiple IP addresses or ranges of IP addresses that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check the IP addresses in use in the current address pool, so that you can exclude the unused IP addresses from being automatically assigned to clients. If you need to exclude IP addresses in Used and Conflict states from being automatically assigned to clients after address reclamation, you can also run the **excluded-ip-address** command. If an IP address has been bound to a specific MAC address, adding the IP address to the IP address list in which IP addresses are not

automatically assigned to clients will unbind the IP address from the MAC address.

Example

Disable IP addresses 10.10.10.10 to 10.10.10.20 from being automatically assigned to clients from the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] network 10.10.10.0 mask 24
[HUAWEI-ip-pool-global1] excluded-ip-address 10.10.10.10 10.10.10.20
```

Disable IP address 10.10.10.30 in Used state from being automatically assigned to clients from the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] network 10.10.10.0 mask 24
[HUAWEI-ip-pool-global1] excluded-ip-address 10.10.10.30
Warning: The address is in used or conflict state. Are you sure to continue excluding the address?[Y/N]:y
```

6.3.84 force insert option

Function

The **force insert option** command configures a DHCP server to forcibly insert an Option field specified in the global address pool or DHCP Option template to a DHCP Response packet that it sends to a DHCP client.

The **undo force insert option** command deletes the Option field forcibly inserted to a DHCP Response packet that a DHCP server sends to a DHCP client.

By default, a DHCP server does not forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Format

force insert option *code* &<1-254>

undo force insert option *code* &<1-254>

Parameters

Parameter	Description	Value
code	Specifies the code for a forcibly replied option. You can configure a DHCP server to forcibly reply one or more options.	The value is an integer that ranges from 1 to 254.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a DHCP client applies for an IP address from a DHCP server, parameters contained in the DHCP Request packet specify the options the client requires. The DHCP server inserts the required options to a DHCP Response packet.

Sometimes, the DHCP server on the existing network receives a DHCP Request packet that contains no parameter specifying the options the client requires. However, the client still wants to obtain the options configured on the global address pool. You can run the **force insert option** *code* &<1-254> command to configure the DHCP server to forcibly insert an Option field to the DHCP Response packet.

Prerequisites

The Option field has been configured in the global address pool by running the **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command in the global address pool view.

Example

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet in the address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] option 4 hex 11 22
[HUAWEI-ip-pool-pool1] force insert option 4
```

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet in the DHCP Option template **template1**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] option 4 hex 11 22
[HUAWEI-dhcp-option-template-template1] force insert option 4
```

6.3.85 gateway (DHCP server group view)

Function

The **gateway** command specifies an egress gateway address of the DHCP server in the DHCP server group view.

The **undo gateway** command restores the default setting.

By default, no egress gateway address is specified.

Format

gateway *ip-address*

undo gateway

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an egress gateway.	The value is in dotted decimal notation.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. If a DHCP server and its DHCP relay agent are on different network segments, you can run the **gateway** command to specify an egress gateway address for the DHCP relay agent. In this way, the DHCP relay agent can communicate with the DHCP server. Run the **gateway-list** command to configure an egress gateway for the DHCP server.

Precautions

- If an egress gateway is not configured for a DHCP relay agent using the **gateway** command, the DHCP relay agent uses the VLANIF interface address as the gateway address to communicate with the DHCP server.
- When two switch devices function as the DHCP server and DHCP relay agent respectively, they must use the same egress gateway address.

Example

Specify the egress gateway address of the server group **myServers** as 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] dhcp server group myServers
[HUAWEI-dhcp-server-group-myServers] gateway 10.10.10.1
```

6.3.86 gateway-list

Function

The **gateway-list** command configures an egress gateway address for a DHCP client.

The **undo gateway-list** command deletes a configured egress gateway address.

By default, no egress gateway address is configured.

Format

gateway-list *ip-address* &<1-8>

undo gateway-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an egress gateway.	The value is in dotted decimal notation.
all	Deletes all gateway addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If a DHCP server and its client are on different network segments, you can run the **gateway-list** command to specify an egress gateway address. In this way, the DHCP server and client can communicate with each other. Then the DHCP server can assign both an IP address and the specified egress gateway address to the client. You can configure multiple gateways in a global address pool to load balance traffic and improve network reliability.

To configure an egress gateway for a DHCP relay agent, run the **gateway (DHCP server group view)** command.

Configuration Impact

If a gateway address is configured on the DHCP server, a DHCP client will obtain the gateway address from the DHCP server and automatically generates a default route to the gateway address. If you run the **option121** command on the DHCP server to allocate classless static routes to DHCP clients, the DHCP client uses an allocated classless static route and does not automatically generate a default route to the gateway address.

Precautions

- The IP addresses specified in the **excluded-ip-address** command cannot be configured as a gateway address.
- After an IP address is configured as a gateway address, the device adds the IP address to the list of IP addresses that cannot be automatically allocated, removing the need to run the **excluded-ip-address** command.
- In the IP address pool view or DHCP Option template view, a maximum of eight egress gateway addresses can be configured on the device. These gateway addresses cannot be subnet broadcast addresses.
- When configuring an egress gateway address for the global address pool of a DHCP server, ensure that this egress gateway address is the same as that of the DHCP relay agent.

Example

In the IP address pool view, set the egress gateway address for the DHCP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] gateway-list 10.1.1.1
```

In the DHCP Option template view, set the egress gateway address for the DHCP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] gateway-list 10.1.1.1
```

6.3.87 ip address bootp-alloc

Function

The **ip address bootp-alloc** command enables the BOOTP client function on an interface.

The **undo ip address bootp-alloc** command disables the BOOTP client function from an interface.

By default, the BOOTP client function is disabled on an interface.

Format

ip address bootp-alloc [**unicast**]

undo ip address bootp-alloc

Parameters

Parameter	Description	Value
unicast	Indicates that the client requests the server to unicast response packets to the client.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP is developed based on the BOOTP protocol. The device supports both DHCP and BOOTP and allows hosts to obtain IP addresses by BOOTP.

To enable an interface to obtain IP addresses using BOOTP, you can enable the BOOTP client function on the interface. A BOOTP client requests for an IP address from the server using BOOTP. The BOOTP client has two functions:

- Sends BOOTP Request messages to the server.
- Processes BOOTP Reply messages from the server.

To obtain an IP address, the BOOTP client sends a BOOTP Request message to the server. When the server receives the BOOTP Request message, it sends a BOOTP response message to the BOOTP client. The BOOTP client obtains the assigned IP address from the response message.

Precautions

Interfaces of the Switch can have IP addresses statically configured using the **ip address** command or dynamically obtain IP addresses using the **ip address bootp-alloc** command. A static IP address takes precedence over a dynamic IP address. If the interface has dynamically obtained an IP address after the **ip address bootp-alloc** command is executed, running the **undo ip address** command deletes the IP address and the **ip address bootp-alloc** command. If the interface does not obtain an IP address after the **ip address bootp-alloc** command is executed, running the **undo ip address** command does not delete the **ip address bootp-alloc** command.

Example

Enable the BOOTP client function on VLANIF100 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address bootp-alloc
```

Enable the BOOTP client function on GE0/0/1 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address bootp-alloc
```

6.3.88 ip address dhcp-alloc

Function

The **ip address dhcp-alloc** command enables the DHCP client function on an interface.

The **undo ip address dhcp-alloc** command disables the DHCP client function on an interface.

By default, the DHCP client function is enabled on VLANIF 1 of the S1720GW-E and S1720GWR-E. On other devices, the DHCP client function is disabled on an interface.

Format

ip address dhcp-alloc [**unicast**]

undo ip address dhcp-alloc

Parameters

Parameter	Description	Value
unicast	Indicates that the client requests the server to unicast response packets.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable an interface on the Switch to obtain an IP address using DHCP, enable the DHCP client function on the interface. A DHCP client applies for an IP address from the server using DHCP. The DHCP client has two functions:

- Sends DHCPREQUEST messages to the server.
- Processes DHCPACK messages from the server.

To obtain an IP address, the DHCP client sends a DHCPREQUEST message to the server. After the server receives the DHCPREQUEST message, it sends a DHCPACK message to the DHCP client. The DHCP client obtains the assigned IP address from the DHCPACK message.

Precautions

Interfaces of the device can have IP addresses statically configured using the **ip address** command or dynamically obtain IP addresses using the **ip address dhcp-alloc** command. A static IP address takes precedence over a dynamic IP address. If the interface has dynamically obtained an IP address after the **ip address dhcp-alloc** command is executed, running the **undo ip address** command deletes the IP address and the **ip address dhcp-alloc** command configuration. If no IP address is obtained through the **ip address dhcp-alloc** command, running the **undo ip address** command does not delete the **ip address dhcp-alloc** command configuration.

For the S1720GW-E and S1720GWR-E, if no IP address is configured on the device, VLANIF 1 uses the IP address 192.168.1.253 255.255.255.0 by default, and the **ip address dhcp-alloc unicast** command is configured on the interface by default. After VLANIF 1 obtains an IP address through DHCP successfully, the IP address 192.168.1.253 255.255.255.0 is deleted. If the DHCP client function is enabled on another VLANIF interface, the VLANIF interface cannot obtain the IP address in the same network segment as that of VLANIF 1, which prevents address conflict.

Example

Enable the DHCP client function on VLANIF100 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address dhcp-alloc
```

Enable the DHCP client function on GE0/0/1 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address dhcp-alloc
```

6.3.89 ip pool (system view)

Function

The **ip pool** command creates a global address pool.

The **undo ip pool** command deletes a global address pool.

By default, no global address pool is created.

Format

ip pool *ip-pool-name*

undo ip pool *ip-pool-name*

Parameters

Parameter	Description	Value
ip-pool-name	Specifies the name for an IP address pool.	The value is a string of 1 to 64 case-insensitive characters without spaces. It can contain digits, letters, and special characters such as underscores (_), hyphens (-), and periods (.). It cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When configuring a DHCP server, run the **ip pool** command in the system view to create a global IP address pool and set parameters for the global IP address pool, including a gateway address, the IP address lease, and a VPN instance. Then the configured DHCP server can assign IP addresses in the IP address pool to clients.

Precautions

A maximum of 128 address pools, including global address pools and interface address pools, can be created on the device.

Follow-up Procedure

Run the **network** command in the IP address pool view to specify the range of the IP addresses that can be allocated in the pool.

Example

Create a global address pool named **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
```

6.3.90 ip relay address cycle

Function

The **ip relay address cycle** command enables the DHCP server polling function on a DHCP relay agent.

The **undo ip relay address cycle** command disables the DHCP server polling function on a DHCP relay agent.

By default, DHCP server polling is disabled on a DHCP relay agent.

Format

ip relay address cycle

undo ip relay address cycle

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. When multiple DHCP server addresses are configured on a DHCP relay agent, the DHCP relay agent forwards DHCP Discover messages to all servers by default. As a result, DHCP servers need to process a large number of messages, leading to heavy loads of servers. To solve this problem, configure the **ip relay address cycle** command. After this command is configured, the DHCP relay agent forwards a received DHCP Discover message to one DHCP server at a time, and forwards the DHCP Discover message to a different DHCP server each time it receives the message. Multiple DHCP servers then can allocate the same number of IP addresses, implementing load balancing among DHCP servers.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

After the **ip relay address cycle** command is run, the DHCP relay agent forwards a received DHCP Discover message to a different DHCP server each time in the sequence in which DHCP servers were configured. You can run the **display dhcp relay** command to view DHCP server IP addresses in the **Server IP address** field to determine the sequence in which DHCP servers were configured.

Example

Enable DHCP server polling on the switch in the system view.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ip relay address cycle
```

6.3.91 ip route dhcp

Function

The **ip route dhcp** command configures a routing entry delivered by the DHCP server to a DHCP client.

The **undo ip route dhcp** command cancels the configuration.

By default, no routing entry is delivered by the DHCP server to a DHCP client.

Format

ip route *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]

undo ip route *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length. The 32-bit mask is represented by consecutive 1s, and the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer that ranges from 0 to 32.
interface-type interface-number	Specifies the type and number of the interface that forwards packets.	-
dhcp	Indicates that the DHCP client obtains routing entries using DHCP.	-
preference-value	Specifies the priority of the routing protocol.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ip route dhcp** command is used on DHCP clients. After the **ip route** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*] command is run, a route with the gateway address as the next-hop IP address is automatically generated when a DHCP client obtains an IP address from the DHCP server through a DHCP request.

Example

Configure a routing entry to be obtained in DHCP mode on the DHCP client, and specify VLANIF100 as the outbound interface for forwarding packets and 30 as the routing protocol priority.

```
<HUAWEI> system-view
[HUAWEI] ip route 10.1.1.1 24 vlanif 100 dhcp 30
```

6.3.92 lease

Function

The **lease** command sets the lease for IP addresses in a global IP address pool.

The **undo lease** command restores the default lease of IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo lease

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer that ranges from 0 to 999. The default value is 1.
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer that ranges from 0 to 23. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer that ranges from 0 to 59. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment.

Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, run the **lease** command to set the IP address lease of the current global address pool to **unlimited**. If some hosts such as a portable computer just need to use temporary IP addresses, run the **lease** command to set the IP address lease of the current global address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts and 50% or 87.5% of its IP address lease has passed, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease.

- If the IP address can be assigned to the client, the DHCP server informs the client that the IP address lease can be renewed.
- If the IP address can no longer be assigned to the client, the DHCP server informs the client that the IP address lease cannot be renewed. The client needs to request for another IP address.

You can run the **display ip pool** command to view information about the IP address lease. The values of the **lease** and **left** fields in the command output indicate the configured lease time and remaining lease time, respectively.

Prerequisites

A global IP address pool has been created using the **ip pool** command.

Precautions

Different IP address leases can be specified for different global address pools on a DHCP server. In a global address pool, all addresses have the same lease.

To specify the IP address lease for an interface address pool, run the **dhcp server lease** command.

If the IP address lease of an address pool is changed using this command, newly assigned IP addresses use the new IP address lease. IP addresses assigned before the change still use the original IP address lease before the lease is updated, and use the new lease after the lease is updated.

Example

Set the lease of a global address pool **global1** to 2 days 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] lease day 2 hour 2 minute 30
```

6.3.93 lock (IP address pool view)

Function

The **lock** command locks an IP address pool.

The **undo lock** restores the default configuration.

By default, no IP address pool is locked.

Format

lock

undo lock

Parameters

None

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

After the **lock** command is run, the specified IP address pool is locked and IP addresses in this address pool cannot be assigned to clients. When a DHCP server needs to be redeployed, you need to migrate address pools on the DHCP server to another DHCP server on the live network. To retain the addresses that have been assigned to clients from a global address pool, run the **lock** command to lock the global address pool. When new users get online after the address pool migration, they apply for IP addresses from a new address pool.

Example

Lock the IP address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] lock
```

6.3.94 logging (IP address pool view)

Function

The **logging** command enables the logging function during IP address allocation of the DHCP server in the IP address pool view.

The **undo logging** command disables the logging function during IP address allocation of the DHCP server in the IP address pool view.

By default, the logging function during IP address allocation of the DHCP server is disabled.

Format

logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

undo logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

Parameters

Parameter	Description	Value
allocation-fail	Displays logs when address allocation fails.	-
allocation-success	Displays logs when address allocation succeeds.	-
release	Displays logs when addresses are released.	-
renew-fail	Displays logs when address lease renewal fails.	-
renew-success	Displays logs when address lease renewal succeeds.	-
detect-conflict	Displays logs when address conflict occurs.	-
recycle-conflict	Displays logs when conflicting addresses are reclaimed.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When the DHCP server allocates IP addresses to clients, it records address allocation information to facilitate routine maintenance and fault location. After the logging function during IP address allocation of the DHCP server is configured using the **logging** command, the DHCP server records logs about address allocation, conflict, lease renewal, and release.

Run the **display ip pool name** *ip-pool-name* command to check the status of the logging function during IP address allocation of the DHCP server.

Prerequisites

The global address pool has been created using the **ip pool (system view)** command.

Precautions

- With this logging function enabled, if a large number of DHCP clients request IP addresses from the DHCP server, the server frequently records logs. The server performance may therefore be affected.

- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration in the *CLI-based Configuration - Device Management Configuration Guide*.

  For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the logging function during IP address allocation of the DHCP server in the IP address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] logging
```

6.3.95 nbns-list

Function

The **nbns-list** command configures the NetBIOS server address for the DHCP client.

The **undo nbns-list** command deletes a configured NetBIOS server address.

By default, no NetBIOS server address is configured.

Format

nbns-list *ip-address* &<1-8>

undo nbns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a NetBIOS server.	The value is in dotted decimal notation. A maximum of eight NetBIOS server addresses can be configured. These IP addresses are separated by spaces.
all	Deletes all NetBIOS server addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before hosts communicate with each other, a NetBIOS server needs to resolve the accessedNetBIOS hostname to an IP address. To enable hosts to communicate with each other, run the **nbns-list** command to configure NetBIOS server addresses. When assigning IP addresses to clients, a DHCP server also assigns the configured NetBIOS server addresses to clients. To configure NetBIOS server addresses for an interface address pool, run the **dhcp server nbns-list** command.

Precautions

In the IP address pool view and DHCP Option template view, a device can be configured with a maximum of eight NetBIOS server addresses respectively. The first assigned address functions as the primary address, and the other seven addresses function as secondary addresses.

Example

In the IP address pool view, set the IP address of the NetBIOS server to 192.168.1.1.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] nbns-list 192.168.1.1
```

In the DHCP Option template view, set the IP address of the NetBIOS server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] nbns-list 10.1.1.1
```

6.3.96 netbios-type

Function

The **netbios-type** command configures the NetBIOS node type for the DHCP client.

The **undo netbios-type** command deletes a configured NetBIOS node type.

By default, no NetBIOS node type for the DHCP client is configured.

Format

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Parameters

Parameter	Description	Value
b-node	Indicates a node in broadcast mode. A b-node obtains the mapping between host names and IP addresses in broadcast mode.	-
h-node	Indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.	-
m-node	Indicates a node in mixed mode. An m-node is a p-type node with some broadcast features.	-
p-node	Indicates a node in peer-to-peer mode. A p-node obtains the mapping between host names and IP addresses by communicating with a NetBIOS server.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When a DHCP client uses NetBIOS for communication, its host name needs to be mapped to an IP address, and the NetBIOS node type needs to be specified for it using the **netbios-type** command. When a DHCP server assigns an IP address to clients, it also sends the specified NetBIOS node type to clients.

Prerequisites

To specify the NetBIOS node type for a client in the interface address pool, run the **dhcp server netbios-type** command.

Example

In the IP address pool view, set the NetBIOS node type for the DHCP client to **b-node**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] netbios-type b-node
```

In the DHCP Option template view, set the NetBIOS node type for the DHCP client to **b-node**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] netbios-type b-node
```

6.3.97 network (IP address pool view)

Function

The **network** command sets a network segment address for a global address pool.

The **undo network** command restores the default network segment address.

By default, the range of IP addresses that can be dynamically allocated is not configured.

Format

network *ip-address* [**mask** { *mask* | *mask-length* }]

undo network

Parameters

Parameter	Description	Value
ip-address	Specifies a network segment address.	The value is in dotted decimal notation.
mask	Specifies the mask of the network segment address. If this parameter is not specified, the natural mask is used.	-
mask	Specifies the mask of the network segment address.	The value is in dotted decimal notation.
mask-length	Specifies the network mask length.	The value is an integer that ranges from 0 to 32.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before a DHCP server assigns IP addresses to clients from a global address pool, run the **network** command to set a network segment address for the global address pool so that the DHCP server can select and assign IP addresses on this network segment to clients. When a DHCP server assigns an IP address to the client from the interface address pool, the network segment of the interface IP address is that of the interface address pool.

Precautions

- Each IP address pool can be configured with only one network segment. If the system needs multiple address segments, multiple IP address pools are required.
- The size of an address pool can be controlled by setting the mask length. The mask length is in reverse proportion to the address pool size.
- When configuring an address pool, ensure that IP addresses on the network address segment must be class A, B, or C IP addresses, and the mask cannot be set to 0 to 7, 31, or 32.
- If you need to assign IP addresses with a 16-bit mask in the network segment 10.1.1.0 to clients, the number of IP addresses in an IP address pool is 64K after the **network 10.1.1.0 mask 16** command is executed in the view of the IP address pool. If the number of IP addresses in the IP address pool is less than 64K, the **network 10.1.1.0 mask 16** command cannot be executed in the view of the IP address pool. In this case, perform the following operations:

  Run the following commands in the IP address pool view:

  ```
  [HUAWEI-ip-pool-test] ip pool test
  [HUAWEI-ip-pool-test] section 0 10.1.1.2 10.1.1.254  // The section command specifies the range of IP addresses to be allocated.
  [HUAWEI-ip-pool-test] network 10.1.1.1 mask 16  // The network command specifies the mask of IP addresses to be allocated using the mask parameter.
  ```

  Enable the DHCP server function on a specific interface.

  ```
  [HUAWEI-Vlanif10] ip address 10.1.1.1 16
  [HUAWEI-Vlanif10] dhcp select global
  ```
- The size of the IP address pool cannot be larger than 16K.

Example

Set the network segment address of the IP address pool **global1** to 192.168.1.0 and mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] network 192.168.1.0 mask 24
```

6.3.98 next-server

Function

The **next-server** command configures the IP address of a server for the DHCP client after the client automatically obtains the IP address.

The **undo next-server** command deletes a configured IP address of a server for the DHCP client after the client automatically obtains the IP address.

By default, no IP address of a server is configured for the DHCP client after the client automatically obtains the IP address.

Format

next-server *ip-address*

undo next-server

Parameters

Parameter	Description	Value
ip-address	Specifies a server IP address.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **next-server** command is used on DHCP servers. When assigning a client an IP address, a DHCP server can also assign the client an IP address of the server that provides network services for the client. For example, after obtaining IP addresses, clients such as IP phones need parameters such as the startup configuration file to work normally. You can run the **next-server** command to specify the server address used after a client obtains an IP address. The client then requests the configuration parameters from the specified server after obtaining an IP address.

If users use addresses in the interface address pool, run the **dhcp server next-server** command to specify the DHCP server IP address. If users use addresses in the global address pool, run the **next-server** command to specify the DHCP server IP address.

Precautions

- Only one IP address of a server that provides network services can be configured in each IP address pool view or DHCP Option template view. If the system needs multiple IP addresses of servers that provide network services, configure multiple IP address pools or DHCP Option templates.
- If you run the **next-server** command multiple times, only the latest configuration takes effect.

Example

In the IP address pool view, set the IP address of a server for the DHCP client after the client automatically obtains the IP address to 10.1.2.2.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] next-server 10.1.2.2
```

In the DHCP Option template view, set the IP address of a server for the DHCP client after the client automatically obtains the IP address to 10.1.2.2.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] next-server 10.1.2.2
```

6.3.99 option

Function

The **option** command configures the user-defined option that a DHCP server assigns to a DHCP client.

The **undo option** command deletes the user-defined option that a DHCP server assigns to a DHCP client.

By default, no user-defined option that a DHCP server assigns to a DHCP client is configured.

Format

option *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }

undo option [*code* [**sub-option** *sub-code*]]

Parameters

Parameter	Description	Value
code	Specifies the code of a user-defined option.	The value is an integer that ranges from 1 to 254, except the values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 120, 121, and 184. **NOTE** There are well-known options and user-defined options. For details about well-known options, see RFC 2132. When the switch functions as a DHCP client, Option 148 can be used in an EasyDeploy scenario and is not recommended in other scenarios.
sub-option *sub-code*	Specifies the code of a user-defined sub-option.	The value is an integer that ranges from 1 to 254. For details about well-known options, see RFC 2132.
ascii *ascii-string*	Specifies the user-defined option code as an ASCII character string.	The value is a string of case-sensitive characters with spaces supported. If **sub-option** is not specified, the value is a string of 1 to 255 characters. If **sub-option** is specified, the value is a string of 1 to 253 characters.

Parameter	Description	Value
hex *hex-string*	Specifies the user-defined option code as a hexadecimal character string.	The value is a hexadecimal string with an even number of characters, for example, hh or hhhh. If **sub-option** is not specified, the value without spaces ranges from 1 to 254 characters; if **sub-option** is specified, the value without spaces ranges from 1 to 252. The value can be a combination of digits (0-9), uppercase letters (A-F), and lowercase letters (a-f).
cipher *cipher-string*	Specifies the user-defined option code as a ciphertext character string.	The value is a character string either in plain text or cipher text. ● The character string in plain text is a string of 1 to 64 characters. ● The character string in cipher text is a string of 32 to 108 characters. No matter whether the character string is entered in plain or cipher text, the character string is displayed in cipher text in the configuration file and in plain text in packets.
ip-address *ip-address*	Specifies the user-defined option code as an IP address.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. The option field in a DHCP packet carries control information and parameters. If a DHCP server is configured with options, when a DHCP client applies for an IP address, the client can obtain the configurations in the option field of the DHCP response packet from the DHCP server. To configure user-defined options for an interface address pool, run the **dhcp server option** command.

Precautions

- To ensure configuration accuracy, read the Request For Comments (RFC) before configuring options.
- When an option contains a password, the option code of the **ascii** or **hex** type is insecure. You are advised to set the option code type to **cipher**. For security purposes, a password must contain at least two types of the following: lowercase letters, uppercase letters, digits, and special characters. In addition, the password must consist of at least eight characters.
- Note the following if the **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command is not executed for the first time:
  - If the new *code* is different from the existing *code*, both the new and existing configurations take effect.
  - If the new *code* is the same as the existing *code*, the following situations may occur:
    - When a *sub-code* is specified in the existing command, the new configuration overrides the existing configuration if the new and existing *sub-code*s are the same, and both the new and existing configurations take effect if the new and existing *sub-code*s are different. If no *sub-code* is specified in the new command, the new configuration overrides the existing configuration.
    - When no *sub-code* is specified in the existing command, the new configuration overrides the existing configuration.
- If the device functions as the DHCP server to assign IP addresses to APs, and the AC and APs are on different network segments, you need to configure the Option 43 field to specify the AC IP address for the APs. Otherwise, the APs cannot discover the AC. Run the **option 43** { **hex** *hex-string* | [**sub-option** 1 **hex** *hex-string* | **sub-option** 2 **ip-address** *ip-address* &<1-8> | **sub-option** 3 **ascii** *ascii-string*] } command to configure the device to specify the AC IP address for APs in one of the following methods:

  a. Run the **option 43 hex 031D3139322e3136382e3139342e35302c3139322e3136382e3139342e3534** command to configure the device to specify AC IP addresses 192.168.194.50 and 192.168.194.54 for APs. In this command, **03** indicates that the sub-option value of Option43 is an ASCII value; **1D** indicates that the length of IP addresses (192.168.194.50,192.168.194.54) including dots (.) and the comma (,) is 29, and multiple IP addresses are separated by the comma (,); **3139322e3136382e3139342e3530** indicates the ASCII value of 192.168.194.50; **2C** indicates the ASCII value of the comma (,); **3139322e3136382e3139342e3534** indicates the ASCII value of 192.168.194.54.

b. Run the **option 43 sub-option 1 hex C0A80001C0A80002** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs. In the command, **C0A80001** indicates the hexadecimal format of 192.168.0.1, and **C0A80002** indicates the hexadecimal format of 192.168.0.2.

c. Run the **option 43 sub-option 2 ip-address 192.168.0.1 192.168.0.2** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs.

d. Run the **option 43 sub-option 3 ascii 192.168.0.1,192.168.0.2** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs.

NOTE

If you need to configure multiple IP addresses when the option is specified as an ASCII character string, use commas (,) to separate the IP addresses.

If the AC and APs are on the same network segment, you do not need to configure the Option 43 field, and the APs can discover the AC in broadcast mode. After Option 43 is configured, the APs unicast Discover Request packets to the IP address carried in Option 43 to discover the AC. If the APs do not receive any Discovery Response packet after sending unicast Discovery Request packets, the APs then broadcast packets to discover the AC.

- When users on an enterprise's intranet use a proxy server to connect to the Internet, you need to configure proxy server parameters so that users can use browsers to access the network. The Web Proxy Auto-Discovery Protocol (WPAD) implements automatic configuration of these parameters. The administrator does not need to manually configure these parameters on each client. To implement the WPAD function, the administrator needs to deploy the configuration file of the proxy server in advance, and then run the **option 252 ascii** *ascii-string* command to specify the URL of the configuration file. The *ascii-string* parameter specifies the URL of the configuration file, in the format of https://*xxx*/proxy.pac. Set *ascii-string* according to the storage path of the configuration file. When a browser accesses the network, the browser requests the DHCP server to send the URL of the configuration file on the proxy server, and then downloads the configuration file to conduct automatic configuration. After the configuration is completed, the browser can access the network.

NOTE

The value of *ascii-string* cannot be enclosed in double quotation marks as "*ascii-string*". Otherwise, terminals cannot parse Option252.

Example

In the global address pool **global1**, configure Option64 to 0x11 (a hexadecimal number).

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] option 64 hex 11
```

In the DHCP Option template **template1**, configure Option64 to 0x11 (a hexadecimal number).

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] option 64 hex 11
```

6.3.100 option121

Function

The **option121** command configures the classless static route for the DHCP client.

The **undo option121** command deletes a configured classless static route.

By default, no classless static route is configured.

Format

option121 ip-address { *ip-address mask-length gateway-address* } &<1-8>

undo option121 [**ip-address** *ip-address mask-length gateway-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
gateway-address	Specifies the gateway address of a route.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **option121** command applies to only the DHCP server. The **option121** command configures Option 121 that defines a classless static route allocated to a client.

mask-length and *gateway-address* specify a classless static route. The **option121** command configures a maximum of eight classless static routes.

Precautions

- To configure multiple classless static routes, run the **option121** command repeatedly.
- The **undo option121** command will delete all classless static routes. To delete one classless static route, run the **undo option121 ip-address** *ip-address mask-length gateway-address* command.

Example

In the IP address pool view, configure classless static routes delivered by the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] option121 ip-address 10.10.10.10 24 10.11.11.11
```

In the DHCP Option template view, configure classless static routes delivered by the DHCP server.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] option121 ip-address 10.10.10.10 24 10.11.11.11
```

6.3.101 option125 vendor-specific

Function

The **option125 vendor-specific** command configures the vendor ID in Option 125 for a DHCP client.

The **undo option125 vendor-specific** command deletes the vendor ID in Option 125 for a DHCP client.

By default, no vendor ID is configured in Option 125.

Format

option125 vendor-specific *vendor-id*

undo option125 vendor-specific

Parameters

Parameter	Description	Value
vendor-id	Indicates the vendor ID, which is assigned by the IANA. 2011 indicates Huawei.	The value is an integer in the range from 1 to 4294967295.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a DHCP client sends a DHCP Discover message carrying a vendor ID to a DHCP server, the DHCP server needs to exchange the vendor information with the client using Option 125. You can run the **option 125** [**sub-option** *sub-code*] **ascii** *ascii-string* command to configure the vendor ID in Option 125 delivered by a DHCP server to a client. However, it is complex to convert the vendor ID into an ASCII character string.

To simplify the configuration, you can run the **option125 vendor-specific** *vendor-id* command to specify the vendor ID in Option 125 of packets sent from a DHCP server to a client.

Prerequisites

1. A global address pool has been created using the **ip pool** command in the system view, and the IP address pool view is displayed.
2. Fields except **Vendor-ID** in Option 125 have been configured for the global address pool using the **option 125 ascii** *ascii-string* command. The **Vendor-ID** field in Option 125 occupies four bytes. Therefore, the *ascii-string* value is a string of 1 to 251 bytes.
3. (Optional) The **force insert option 125** command has been used to configure the DHCP server to insert the Option 125 field specified for the global address pool into the DHCP response packet sent from a DHCP server to a client. This resolves the problem in the following situation: The device functions as a DHCP server, and the DHCP request packet sent by a DHCP client does not carry Option 125. However, the DHCP client still expects the DHCP server to deliver Option 125 configured for the global address pool.

Precautions

This command and the **option 125 sub-option** *sub-code* **ascii** *ascii-string* command are mutually exclusive in an IP address pool.

Example

Configure the VLAN and vendor information in Option 125 in the IP address pool view.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] option 125 ascii id:vlan=10
[HUAWEI-ip-pool-global1] option125 vendor-specific 2011
```

6.3.102 option184

Function

The **option184** command configures the Option 184 field for the DHCP client.

The **undo option184** command deletes a configuration in the Option 184 field.

By default, no content in the Option 184 field is configured.

Format

option184 { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* }

undo option184 [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

Parameters

Parameter	Description	Value
ncp-ip *ip-address*	Specifies the IP address of the network call processor (NCP).	The value is in dotted decimal notation.
as-ip *ip-address*	Specifies the IP address of the backup NCP.	The value is in dotted decimal notation.
fail-over *ip-address*	Specifies the IP address in the failover route.	The value is in dotted decimal notation.
dialer-string	Specifies the dialer string.	The value is a string of 1 to 64 characters.
voice-vlan *vlan-id*	Specifies the ID of a voice VLAN.	The value is an integer that ranges from 1 to 4094.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

The **option184** command applies to only the DHCP server and configures Option 184 allocated by a DHCP server to a client in a global address pool.

Example

In the IP address pool view, configure the Option 184 field.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] option184 as-ip 192.168.1.10
```

In the DHCP Option template view, configure the Option 184 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] option184 as-ip 10.10.10.10
```

6.3.103 reset dhcp client statistics

Function

The **reset dhcp client statistics** command clears packet statistics about a DHCP client.

Format

reset dhcp client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clear packet statistics about the DHCP client of the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset dhcp client statistics** command is applicable to DHCP client. During DHCP troubleshooting, statistics about the packets sent and received within a specified period need to be checked. Therefore, before collecting packet statistics, run the **reset dhcp client statistics** command to clear the existing packet statistics. Then you can run the **display dhcp client statistics** command to check packet statistics about the DHCP client.

Precautions

The **reset dhcp client statistics** command can be run multiple times at any interval.

Example

Clear packet statistics about the DHCP client.

```
<HUAWEI> reset dhcp client statistics
```

6.3.104 reset dhcp relay statistics

Function

The **reset dhcp relay statistics** command clears message statistics on a DHCP relay agent.

Format

reset dhcp relay statistics [**server-group** *group-name*]

Parameters

Parameter	Description	Value
server-group *group-name*	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. Collecting statistics on the DHCP messages sent and received within a specified period helps you locate DHCP faults. Run the **reset dhcp relay statistics** [**server-group** *group-name*] command to clear original statistics on DHCP messages, and run the **display dhcp relay statistics** [**server-group** *group-name*] command to view packet statistics about the DHCP relay agent.

- Run the **reset dhcp relay statistics server-group** *group-name* command to clear message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. The DHCP server group name needs to be specified.
- Run the **reset dhcp relay statistics** command to clear message statistics on all DHCP relay agents besides DHCP relay agents connected to DHCP servers in the DHCP server group.

Precautions

The **reset dhcp relay statistics** command can be run multiple times at any interval.

Example

Clear message statistics on the DHCP relay agent.

```
<HUAWEI> reset dhcp relay statistics
```

6.3.105 reset dhcp server statistics

Function

The **reset dhcp server statistics** command clears statistics on the DHCP server.

Format

reset dhcp server statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Collecting statistics on the DHCP messages sent and received within a specified period helps you locate DHCP faults. Run the **reset dhcp server statistics** command to clear original statistics on DHCP messages and then run the **display dhcp server statistics** to view message statistics on the DHCP server.

Precautions

The **reset dhcp server statistics** command can be run multiple times at any interval.

Example

Clear message statistics on the DHCP server.

```
<HUAWEI> reset dhcp server statistics
```

6.3.106 reset dhcp statistics

Function

The **reset dhcp statistics** command clears packet statistics about a DHCP.

Format

reset dhcp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

During DHCP troubleshooting, statistics about the packets sent and received within a specified period need to be checked. Therefore, before collecting packet statistics, run the **reset dhcp statistics** command to clear the existing packet statistics. Then you can run the **display dhcp statistics** command to view DHCP message statistics.

Example

Clear packet statistics about the DHCP.

```
<HUAWEI> reset dhcp statistics
```

6.3.107 reset ip pool

Function

The **reset ip pool** command resets the IP address pool configured on the device.

Format

reset ip pool { **interface** *interface-name* | **name** *ip-pool-name* } { *start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** }

Parameters

Parameter	Description	Value
interface *interface-name*	Specifies the name of the interface address pool to be reset, which is represented by the type and number of an interface.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.
name *ip-pool-name*	Specifies the name of the global address pool to be reset.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.
start-ip-address	Specifies the start IP address of the IP address pool to be reset.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address of the IP address pool to be reset.	The value is in dotted decimal notation.
all	Indicates that all the IP addresses need to be reset.	-
conflict	Indicates that the conflicting IP addresses need to be reset.	-
expired	Indicates that the expired IP addresses need to be reset.	-
used	Indicates that the used IP addresses need to be reset.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset ip pool** command resets the IP addresses that cannot be released in an IP address pool. If an IP address conflict occurs because two clients use the same IP address, run the **reset ip pool** command to reset the specified IP address pool.

Precautions

If a user's IP address is within the IP address range specified when this command is run, the user cannot continue to use the IP address after this command is run, and needs to send an IP address application request again.

The address pool status cannot be restored after this command is run. Therefore, exercise caution when deciding to run this command.

User information cannot be restored after you clear it. Exercise caution when running the **reset ip pool** command. DHCP clients must release their old IP addresses before obtaining new IP addresses.

Follow-up Procedure

After the address pool is set to idle, the client can obtain an IP address from the global address pool.

Example

Reset the conflicting IP addresses in the IP address pool **mypool**.

```
<HUAWEI> reset ip pool name mypool conflict
```

6.3.108 section (IP address pool view)

Function

The **section** command configures an IP address range in an IP address pool.

The **undo section** command deletes a configured IP address range from an IP address pool.

By default, no IP address range is configured in an IP address pool.

Format

section *section-id start-address* [*end-address*]

undo section *section-id*

Parameters

Parameter	Description	Value
section-id	Specifies the ID of an address range in an IP address pool.	The value is an integer in the range from 0 to 255.

Parameter	Description	Value
start-address	Specifies the start IP address of the address range.	The value is in dotted decimal notation.
end-address	Specifies the end IP address of the address range. **NOTE** The end IP address must be greater than or equal to the start IP address. If the end IP address is not specified, the IP address range contains only one IP address.	The value is in dotted decimal notation.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

An IP address pool consists of one or more IP address ranges. The IP addresses in the IP address ranges cannot overlap.

Example

Configure an IP address range 10.1.1.10 to 10.1.1.15 in the IP address pool **abc**, and set the ID of the IP address range to 0.

```
<HUAWEI> system-view
[HUAWEI] ip pool abc
[HUAWEI-ip-pool-abc] section 0 10.1.1.10 10.1.1.15
```

6.3.109 sip-server (IP address pool view)

Function

The **sip-server** command configures the SIP server IP address assigned to a DHCP client in a global address pool.

The **undo sip-server** command deletes the configured SIP server IP address assigned to a DHCP client in a global address pool.

By default, the SIP server IP address assigned to a DHCP client in a global address pool is not configured.

Format

sip-server { **ip-address** *ip-address* &<1-2> | **list** *domain-name* &<1-2> }

undo sip-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address for the SIP server.	The value is in dotted decimal notation.
list *domain-name*	Specifies the domain name of the SIP server.	The value is a string of 1 to 63 characters.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP server. To enable DHCP clients to normally access the Internet, the DHCP server needs to specify the SIP server IP address in the address pool when assigning IP addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured in each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- Before specifying the IP address or name for a SIP server, ensure that the SIP server exists.
- If you run this command repeatedly, the latest configuration overrides the previous ones.

Example

Specify 192.168.1.1 as the IP address of the SIP server when addresses in the global address pool **global1** are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] sip-server ip-address 192.168.1.1
```

6.3.110 sname

Function

The **sname** command configures the name of the server from which the DHCP client obtains the startup configuration file.

The **undo sname** command deletes the configured name of the server from which the DHCP client obtains the startup configuration file.

By default, no name is configured for the server from which the DHCP client obtains the startup configuration file.

Format

sname *sname*

undo sname

Parameters

Parameter	Description	Value
sname	Specifies the name of the server where the DHCP client obtains the startup configuration file.	The value is a string of 1 to 63 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP client. After the name of the server from which the DHCP client obtains the startup configuration file is configured using the **sname** command, the DHCP client obtains the startup configuration file from this server.

Precautions

Ensure that the route between the DHCP client and the file server from which the DHCP client obtains the startup configuration file is reachable.

Example

In the IP address pool view, configure the name of the server from which the DHCP client obtains the startup configuration file as **example**.

```
<HUAWEI> system-view
[HUAWEI] ip pool p1
[HUAWEI-ip-pool-p1] sname example
```

In the DHCP Option template view, configure the name of the server from which the DHCP client obtains the startup configuration file as **example**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] sname example
```

6.3.111 static-bind

Function

The **static-bind** command binds an IP address in a global address pool to a MAC address of a client.

The **undo static-bind** command unbinds the IP address in a global address pool from a MAC address.

By default, the IP address in a global address pool is not bound to any MAC address.

Format

static-bind ip-address *ip-address* **mac-address** *mac-address* [**option-template** *template-name* | **description** *description*]

undo static-bind [**ip-address** *ip-address* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address to be bound. The IP address must be a valid IP address in the global address pool.	The value is in dotted decimal notation.
mac-address *mac-address*	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
option-template *template-name*	Specifies the name of the DHCP Option template. To allocate network configuration parameters except IP addresses to static clients, specify the parameter. Before specifying the parameter, run the **dhcp option template** command to create a DHCP option template, and configure network parameters for static clients in the DHCP Option template view.	The name is a string of 1 to 31 case-sensitive characters without spaces.
description *description*	Specifies the user description.	The value is a string of 1 to 256 case-sensitive characters. It can contain spaces.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind** command applies to DHCP servers. When planning a network, you need to allocate fixed IP addresses to some important hosts to ensure reliability. In this case, you can bind IP addresses in the address pool to the MAC addresses of these hosts. After the preceding configuration is complete, if the host of the MAC address to which the IP address is bound request an IP address from the DHCP server, the DHCP server finds the bound IP address based on the host's MAC address and allocates this IP address to the host, ensuring that the IP address obtained by the host is fixed.

You can run the **static-bind** command to bind an IP address in a global address pool to a MAC address.

You can run the **dhcp server static-bind** command to bind an IP address in an interface address pool to a MAC address.

Prerequisites

Network segment addresses that can be assigned from the global address pool have been configured using the **network (IP address pool view)** command.

Precautions

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **excluded-ip-address** command.
- IP addresses that are used can also be statically bound to MAC addresses or unbound from MAC addresses. When an IP address is statically bound to a MAC address, ensure that the MAC address to be bound is the same as the MAC address of the user who actually uses the IP address.
- The DHCP server preferentially allocates the IP address that has been statically bound to the client's MAC address.
- After an IP address is bound to a MAC address, the IP address does not expire. After an automatically allocated IP address is statically bound to a MAC address, the lease time of the IP address becomes unlimited. After the static binding between the IP address and the MAC address is deleted, the lease time of the IP address becomes the same as that configured in the address pool.

Example

Configure a DHCP server to assign a fixed IP address 192.168.1.10 in the global address pool **global1** to a host with the MAC address 00e0-fc96-e4c0.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] network 192.168.1.10 mask 24
[HUAWEI-ip-pool-global1] static-bind ip-address 192.168.1.10 mac-address 00e0-fc96-e4c0
```

6.3.112 vpn-instance (global address pool view)

Function

The **vpn-instance** command binds an IP address pool to a VPN instance.

The **undo vpn-instance** command restores the default setting.

By default, an IP address pool is not bound to any VPN instance.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

Global address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To apply DHCP services in a VPN instance, you need to run the **vpn-instance** command to bind the created IP address pool to the VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

- The VPN instance bound to the IP address pool on the DHCP server must be the same as the VPN instance bound to the DHCP server group on the DHCP relay agent; otherwise, users in the IP address pool cannot go online using this DHCP server group.
- If an IP address pool is bound to a VPN instance, IP addresses assigned from this address pool are VPN addresses.
- To bind an interface address pool to a VPN instance, run the **ip binding vpn-instance** command in the interface view.

Example

Bind the address pool **global1** to the VPN instance **example**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance example
[HUAWEI-vpn-instance-example] ipv4-family
[HUAWEI-vpn-instance-example-af-ipv4] quit
[HUAWEI-vpn-instance-example] quit
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] vpn-instance example
```

6.4 DHCP Policy VLAN Configuration Commands

6.4.1 Command Support

Only the following switch models support DHCP policy VLAN:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

6.4.2 dhcp policy-vlan generic

Function

The **dhcp policy-vlan generic** command configures the generic DHCP policy VLAN.

The **undo dhcp policy-vlan generic** command deletes the generic DHCP policy VLAN.

By default, the function of generic DHCP policy VLAN is disabled on the device.

Format

dhcp policy-vlan generic [**priority** *priority*]

undo dhcp policy-vlan generic

Parameters

Parameter	Description	Value
priority *priority*	Specifies the 802.1p priority of DHCP messages.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure three types of DHCP policy VLAN on the device at the same time. They are listed in descending order based on priorities as follows:

- DHCP policy VLAN based on MAC addresses
- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

On a network supporting VLAN assignment based on IP subnets, upon receiving an untagged packet from a host, a switch adds a VLAN ID to the packet based on the source IP address of the packet. A host that accesses the network for the first time does not have a valid IP address. Therefore, the switch cannot add the host to the VLAN and the host cannot obtain a valid IP address or network settings. To make the host obtain a valid IP address from the DHCP server, run the **dhcp policy-vlan generic** command to configure the generic policy VLAN.

Hosts that access the network for the first time apply the generic DHCP policy VLAN only when they cannot apply DHCP policy VLAN based on MAC addresses or interfaces.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Precautions

If you run this command in multiple VLAN views, only the latest configuration takes effect.

Example

Configure the generic DHCP policy VLAN, associate DHCP packets that match no MAC address or interface to VLAN 100, and set the 802.1p priority of the packets to 5.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp policy-vlan generic priority 5
```

6.4.3 dhcp policy-vlan mac-address

Function

The **dhcp policy-vlan mac-address** command configures the MAC address-based DHCP policy VLAN.

The **undo dhcp policy-vlan mac-address** command deletes the MAC address-based DHCP policy VLAN.

By default, the function of DHCP policy VLAN based on MAC addresses is disabled on the device.

Format

dhcp policy-vlan mac-address *mac-address1* [**to** *mac-address2*] [**priority** *priority*]

undo dhcp policy-vlan mac-address *mac-address1* [**to** *mac-address2*]

Parameters

Parameter	Description	Value
mac-address1 [**to** *mac-address2*]	Specifies the MAC addresses of user hosts that access the network for the first time. - *mac-address1* specifies the start MAC address. - **to** *mac-address2* specifies the end MAC address. *mac-address2* must be greater than *mac-address1*. *mac-address2* and *mac-address1* specify the MAC address range. If **to** *mac-address2* is not specified, DHCP policy VLAN based on only the MAC address specified by *mac-address1* is configured.	*mac-address1* and *mac-address2* are in the format of H-H-H. An H contains one to four hexadecimal numbers. **NOTE** The range specified by *mac-address1* and *mac-address2* cannot contain multicast MAC addresses, broadcast MAC addresses, and all 0 address. The number of MAC addresses cannot exceed 512.
priority *priority*	Specifies the 802.1p priority of DHCP messages.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure three types of DHCP policy VLAN on the device at the same time. They are listed in descending order based on priorities as follows:

- DHCP policy VLAN based on MAC addresses
- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

On a network supporting VLAN assignment based on IP subnets, upon receiving an untagged packet from a host, a switch adds a VLAN ID to the packet based on the source IP address of the packet. A host that accesses the network for the first time does not have a valid IP address. Therefore, the switch cannot add the host to the VLAN and the host cannot obtain a valid IP address or network settings. To make the host obtain a valid IP address from the DHCP server, run the **dhcp policy-vlan mac-address** command to configure the MAC address-based DHCP policy VLAN.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Precautions

If you run this command based on the same MAC address in multiple VLAN views, only the latest configuration takes effect.

Example

Configure the MAC address-based DHCP policy VLAN, associate DHCP packets from the host with the MAC address 00e0-fc01-0001 to VLAN 100, and set the 802.1p priority of the packets to 5.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp policy-vlan mac-address 1-1-1 priority 5
```

6.4.4 dhcp policy-vlan port

Function

The **dhcp policy-vlan port** command configures the interface-based DHCP policy VLAN.

The **undo dhcp policy-vlan port** command deletes the interface-based DHCP policy VLAN.

By default, the function of DHCP policy VLAN based on interfaces is disabled on the device.

Format

dhcp policy-vlan port *interface-type interface-number1* [**to** *interface-number2*] &<1-10> [**priority** *priority*]

undo dhcp policy-vlan port *interface-type interface-number1* [**to** *interface-number2*] &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-number2*] &<1-10>	Specifies the interface type and interface number. - *interface-type* specifies the type of an interface. - *interface-number1* specifies the number of the start interface. - **to** *interface-number2* specifies the number of the end interface. *interface-number2*must be greater than *interface-number1*. *interface-number2* and *interface-number1* specify the interface range. If **to** *interface-number2* is not specified, DHCP policy VLAN based on only the interface specified by *interface-number1* is configured. **NOTE** The interface cannot be a stack interface.	-
priority *priority*	Specifies the 802.1p priority of DHCP messages.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure three types of DHCP policy VLAN on the device at the same time. They are listed in descending order based on priorities as follows:

- DHCP policy VLAN based on MAC addresses

- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

On a network supporting VLAN assignment based on IP subnets, upon receiving an untagged packet from a host, a switch adds a VLAN ID to the packet based on the source IP address of the packet. A host that accesses the network for the first time does not have a valid IP address. Therefore, the switch cannot add the host to the VLAN and the host cannot obtain a valid IP address or network settings. To make the host obtain a valid IP address from the DHCP server, run the **dhcp policy-vlan port** command to configure the interface-based policy VLAN.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Precautions

If you run this command on an interface in multiple VLAN views, only the latest configuration takes effect.

NOTE

The interface-based DHCP policy VLAN takes effect only for hybrid interfaces. If an interface is not hybrid, run the **port link-type hybrid** command to configure it as a hybrid interface.

Example

Configure the interface-based DHCP policy VLAN, associate DHCP packets received on GigabitEthernet0/0/1 with VLAN 100, and set the 802.1p priority of the packets to 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI--GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI--GigabitEthernet0/0/1] quit
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp policy-vlan port gigabitethernet 0/0/1 priority 5
```

6.5 DNS Configuration Commands

6.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

6.5.2 display dns dynamic-host

Function

The **display dns dynamic-host** command displays dynamic DNS entries.

Format

display dns dynamic-host [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays dynamic DNS entries of a specified VPN instance.	The value must be an existing VPN instance name.
all	Displays all dynamic DNS entries, including both public and private DNS entries. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public dynamic DNS entries are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dns dynamic-host** command to view dynamic DNS entries and check whether domain names match the mapping entries.

Example

Display dynamic DNS entries.

```
<HUAWEI> display dns dynamic-host
No  Domain-name         IpAddress      TTL    Alias
1   www.example.com     10.1.1.1       3521
2   www.huawei.com     10.1.2.1       3000
```

Display dynamic DNS entries of the VPN instance vpn1.

```
<HUAWEI> display dns dynamic-host vpn-instance vpn1
No  Domain-name                        Alias                 IpAddress           TTL      VPN-Instance
1   www.example.com                                          10.1.3.1            3521     vpn1
2   www.huawei.com                                          10.1.4.1            3000     vpn1
```

Table 6-30 Description of the **display dns dynamic-host** command output

Item	Description
No	Number of a dynamic DNS entry.
Domain-name	Domain name.
IpAddress	IP addresses of the host.
TTL	Remaining lifetime of DNS entries (in seconds).
Alias	Alias of a host.
VPN-Instance	VPN instance name.

6.5.3 display dns domain

Function

The **display dns domain** command displays information about the domain name suffixes.

Format

display dns domain [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about domain name suffixes of a specified VPN instance.	The value must be an existing VPN instance name.
all	Displays information about all domain name suffixes, including both public and private domain name suffixes. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only information about public domain name suffixes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dns domain** command displays the configuration of domain name suffixes and the order in which they are configured.

Example

Display the list of domain name suffixes.

```
<HUAWEI> display dns domain
No                    Domain-name
1                    com
2                    net
```

Display the list of domain name suffixes of the VPN instance vpn1.

```
<HUAWEI> display dns domain vpn-instance vpn1
No          Domain-name         VPN-Instance
1           com.cn              vpn1
```

Table 6-31 Description of the **display dns domain** command output

Item	Description
No	Indicates the domain name suffix numbers, that is, the configuration sequence of domain name suffixes.
Domain-name	Indicates the configured domain name suffix. If there are multiple domain name suffixes in the list, during DNS resolution, the first suffix is added and sent to the DNS server. If the DNS server gives no response, the query message is resent; if the DNS server still gives no response, the query message is resent for a third time; if the DNS server still does not respond, the next suffix is added and sent to the DNS server for searching for the mapped address. The value is set using the **dns domain** command.
VPN-Instance	VPN instance name. The value is set using the **dns domain** command.

6.5.4 display dns server

Function

The **display dns server** command displays information about DNS servers.

Format

display dns server [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about DNS servers of a specified VPN instance.	The value must be an existing VPN instance name.
all	Displays information about all DNS servers, including both public and private DNS servers. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only information about public DNS servers is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring DNS server addresses, you can run the **display dns server** command to view the configuration and sequence of DNS servers.

Example

Display information about DNS servers.

```
<HUAWEI> display dns server
IPv4 Dns Servers :
Domain-server        IpAddress
    1               10.16.1.1
    2               10.17.1.1

IPv6 Dns Servers :
Domain-server        Ipv6Address                          (Interface Name)
    1               FC00:1::1
```

Display information about the DNS servers of the VPN instance vpn1.

```
<HUAWEI> display dns server vpn-instance vpn1
IPv4 Dns Servers :
Domain-server        IpAddress           VPN-Instance
    1               172.16.1.1          vpn1
    2               172.16.1.2          vpn1

IPv6 Dns Servers :
No configured servers.
```

Table 6-32 Description of the **display dns server** command output

Item	Description
IPv4 Dns Servers	IPv4 DNS server configuration.
Domain-server	DNS server number, indicating the order in which they were configured.
IpAddress	IP address of the DNS server. During DNS resolution, the first DNS server is used. If this server fails to resolve packets, the second DNS server is used. The value is set using the **dns server** command.
IPv6 Dns Servers	IPv6 DNS server configuration.
Ipv6Address	IPv6 address of the IPv6 DNS server. The value is set using the **dns server ipv6** command.
Interface Name	Interface name, which only corresponds to the local IPv6 link address. The value is set using the **dns server ipv6** command.
VPN-Instance	VPN instance name. The value is set using the **dns server** command.

6.5.5 display ip host

Function

The **display ip host** command displays the static DNS entries.

Format

display ip host [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays static DNS entries of a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all	Displays all static DNS entries, including both public and private static DNS entries. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public static DNS entries are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **ip host** command to configure static DNS entries, you can run this command to check whether mappings between host names and IP addresses are correct. You can run the **display ip host** command to view static DNS entries.

Example

Display static DNS entries.

```
<HUAWEI> display ip host
Host                  Age        Flags  Address
www.3322.org          0          static 10.1.1.1
members.3322.org      0          static 10.1.2.1
checkip.dyndns.com    0          static 10.1.3.1
members.dyndns.org    0          static 10.1.4.1
```

Display static DNS entries of VPN instance vpn1.

```
<HUAWEI> display ip host vpn-instance vpn1
Host           Age         Flags      Address        VPN-Instance
RTB            0           static     10.1.5.1       vpn1
```

Table 6-33 Description of the **display ip host** command output

Item	Description
Host	Host name. The value is set using the **ip host** command.
Age	Aging time. The value 0 indicates a static DNS entry. Static entries are not aged out.
Flags	Status of the domain name. The value static indicates a static domain name.

Item	Description
Address	IP address mapping the domain name. The value is set using the **ip host** command.
VPN-Instance	VPN instance name. The value is set using the **ip host** command.

6.5.6 dns domain

Function

The **dns domain** command configures a domain name suffix.

The **undo dns domain** command deletes a domain name suffix.

By default, no domain name suffix is configured.

Format

dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

undo dns domain [*domain-name* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
domain-name	Specifies the suffix of a domain name.	The value is a string of 1 to 63 characters without spaces. A combination of digits, letters, underscores (_), hyphens (-), and dots (.) is allowed.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Many servers or hosts have the same suffix. In this case, you can configure domain name suffixes. For example, you can configure a suffix com.cn for the host whose domain name is huawei. When a DNS client accesses the host, it enters only "huawei" to send a query message to the DNS server. The DNS client automatically adds the suffix com.cn. Then the DNS server searches for the IP address mapped to "huawei.com.cn" first. If receiving no response, the DNS client sends a query message containing "huawei" to the DNS server to search for the mapped IP address.

Precautions

The switch supports a maximum of 10 domain name suffixes. To configure multiple domain name suffixes, you can run the **dns domain** command repeatedly.

If the name of the suffix to be deleted is specified, the specified suffix is deleted. Otherwise, all the suffixes are deleted.

If **vpn-instance** *vpn-instance-name* is specified, the specified domain name suffix can be used to search for the IP address corresponding to a domain name only when users access the domain name from the specified VPN instance.

Example

Configure a domain name suffix as com.cn.

```
<HUAWEI> system-view
[HUAWEI] dns domain com.cn
```

6.5.7 dns resolve

Function

The **dns resolve** command enables dynamic domain name resolution.

The **undo dns resolve** command disables dynamic domain name resolution.

By default, dynamic domain name resolution is disabled.

Format

dns resolve

undo dns resolve

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To obtain IP addresses mapping domain names using the DNS server, run the **dns resolve** command to enable dynamic domain name resolution on the device.

Example

Enable dynamic domain name resolution.

```
<HUAWEI> system-view
[HUAWEI] dns resolve
```

6.5.8 dns server

Function

The **dns server** command configures the IP address of a DNS server.

The **undo dns server** command deletes the IP address of a DNS server.

By default, no IP addresses of DNS servers are configured.

Format

dns server *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns server *ip-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DNS server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic domain name resolution, the DNS client can send a query packet to the DNS server, requesting for the IP address of the specified domain name. The DNS client sends a domain name resolution request to the DNS servers according to the order in which they were configured. If the domain name resolution request on the first DNS server times out, the device sends the request to the second DNS server.

If **vpn-instance** *vpn-instance-name* is specified, the system sends domain name resolution requests only to the DNS server bound to the specified VPN instance.

Precautions

A maximum of six DNS server IP (IPv4 and IPv6) addresses can be configured on the switch.

Example

Configure two DNS servers with the IP addresses 172.16.1.1 and 10.10.10.10.

```
<HUAWEI> system-view
[HUAWEI] dns server 172.16.1.1
[HUAWEI] dns server 10.10.10.10
```

6.5.9 dns server source-ip

Function

The **dns server source-ip** command configures the source IP address for the DNS client to communicate with a server.

The **undo dns server source-ip** command deletes the source IP address for the DNS client to communicate with a server.

By default, no source IP address is configured for the DNS client to communicate with a server.

Format

dns server source-ip *ip-address* [**vpn-instance** *vpn-instance-name*]

undo dns server source-ip [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for the DNS client to communicate with a server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the DNS client communicates with a server, the administrator can specify a source IP address for the client to ensure the communication security. The route from the DNS server to the specified source IP address must be reachable. The DNS server uses the specified source IP address as the destination address and sends a DNS response packet to the client.

If **vpn-instance** *vpn-instance-name* is specified, the specified source IP address is used only when the device communicates with the DNS server bound to the specified VPN instance.

Example

Specify the source IP address 172.16.1.1 for the DNS client to communicate with a server.

```
<HUAWEI> system-view
[HUAWEI] dns server source-ip 172.16.1.1
```

6.5.10 ip host

Function

The **ip host** command configures a static DNS entry.

The **undo ip host** command deletes a static DNS entry.

By default, no static DNS entry is configured.

Format

ip host *host-name ip-address* [**vpn-instance** *vpn-instance-name*]

undo ip host *host-name* [*ip-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 255 case-sensitive characters without any space. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
ip-address	Specifies the IP address mapping the host name.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A static domain name resolution table is manually set up using the **ip host** command, describing the mappings between host names and IP addresses. In addition, some common host names are added to the table. Then, static host name resolution can be performed according to the static domain name resolution table. When requiring the IP address corresponding to a host name, the client first searches the static host name resolution table for the specified host name and obtains the corresponding IP address. In this manner, the efficiency of host name resolution is improved.

Precautions

The **ip host** command configures a maximum of 50 static DNS entries. Each host name can be mapped to only one IP address. When one host name is mapped to multiple IP addresses, only the latest configuration takes effect.

Example

Configure a static DNS entry.

```
<HUAWEI> system-view
[HUAWEI] ip host www.example.com 10.10.10.4
```

6.5.11 reset dns dynamic-host

Function

The **reset dns dynamic-host** command clears dynamic DNS entries.

Format

reset dns dynamic-host [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears dynamic DNS entries of a specified VPN instance.	The value must be an existing VPN instance name.
all	Clears all dynamic DNS entries, including both public and private DNS entries. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public dynamic DNS entries are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After confirming the action of deleting dynamic DNS entries, you can run the **reset dns dynamic-host** command to delete them.

Precautions

Dynamic DNS entries cannot be restored after being deleted. Confirm the action before you run the command.

Example

Delete all dynamic DNS entries.

```
<HUAWEI> reset dns dynamic-host all
```

6.6 mDNS Gateway Configuration Commands

6.6.1 Command Support

Only the following switch models support mDNS Gateway:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

6.6.2 display mdns gateway

Function

The **display mdns gateway** command displays the mDNS gateway configuration.

Format

display mdns gateway

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the mDNS gateway is configured, you can run the **display mdns gateway** command to view the mDNS gateway configuration.

Example

Display the mDNS gateway configuration.

```
<HUAWEI> display mdns gateway
mDNS Information:
--------------------------------------------------------------------------------
 mDNS Gateway Status         :  Enable
 mDNS Source IP              :  -
--------------------------------------------------------------------------------
 Gateway Probe Vlan   :  vlan50  vlan101
--------------------------------------------------------------------------------
```

Table 6-34 Description of the display mdns gateway command output

Item	Description
mDNS Gateway Status	mDNS gateway status: ● Enable ● Disable To enable the mDNS gateway, run the **mdns gateway enable** command.
mDNS Source IP	Source IP address in outgoing mDNS request packets when the mDNS gateway is configured to periodically discover services. To specify the source IP address in outgoing mDNS request packets when the mDNS gateway is configured to periodically discover services, run the **mdns source ip** command.
Gateway Probe Vlan	ID of the VLAN where the mDNS gateway is enabled to periodically discover services. To specify the ID of the VLAN where the mDNS gateway is enabled to periodically discover services, run the **mdns probe interval** command.

6.6.3 display mdns gateway statistics

Function

The **display mdns gateway statistics** command displays statistics on the mDNS gateway.

Format

display mdns gateway statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During routine maintenance and fault location, you can run the **display mdns gateway statistics** command to view statistics on mDNS packets received and sent by the mDNS gateway in a given period of time.

To query statistics again, run the **reset mdns gateway statistics** command to clear existing statistics.

NOTICE

Cleared statistics on the mDNS gateway cannot be restored. Exercise caution when you use the **reset mdns gateway statistics** command.

Example

Display statistics on the mDNS gateway.

```
<HUAWEI> display mdns gateway statistics
mDNS Gateway Statistics:
------------------------------------
 Received        : 1120
  Query          : 411
  Response       : 707
  Discarded      : 29                    Query TimeOut : 22                    Bad source IP :
2
   Bad Pkt Length: 3
   Others        : 2
 Sent            : 681
  Query          : 678
  Response       : 3
```

Table 6-35 Description of the **display mdns gateway statistics** command output

Item	Description
Received	Number of mDNS packets received by the mDNS gateway.
Query	Number of mDNS query packets received by the mDNS gateway.
Response	Number of mDNS response packets received by the mDNS gateway.
Discarded	Number of mDNS packets discarded by the mDNS gateway. **NOTE** This field is displayed only when the value is not 0.
Query TimeOut	Number of packets that are discarded after being accumulated in a queue for more than 5 seconds.

Item	Description
Bad source IP	Number of unicast packets that are sent by untrusted mDNS relay agents and discarded by the mDNS gateway. **NOTE** This field is displayed only when the value of the **Discarded** field is not 0.
Bad Pkt Length	Number of mDNS packets discarded because the packet length exceeds the upper limit. **NOTE** This field is displayed only when the value of the **Discarded** field is not 0.
Others	Number of mDNS packets discarded because of other reasons. **NOTE** This field is displayed only when the value of the **Discarded** field is not 0.
Sent	Number of mDNS packets sent by the mDNS gateway.
Query	Number of mDNS query packets sent by the mDNS gateway.
Response	Number of mDNS response packets sent by the mDNS gateway.

6.6.4 display mdns group

Function

The **display mdns group** command displays mDNS group information.

Format

display mdns group [**name** *group-name* | **user-vlan** *vlan-id*]

Parameters

Parameter	Description	Value
name *group-name*	Displays mDNS group information with a specified name. If the mDNS group with the specified name is not created on the device, no information is displayed.	The mDNS group name must have been created.
user-vlan *vlan-id*	Displays mDNS group information with a specified user VLAN. If the specified user VLAN is not used any mDNS group, no information is displayed.	The user VLAN must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device functioning as the mDNS gateway maintains service information lists of all service provisioning devices on a network, and it can use mDNS groups to isolate service resources to provide refined service management. You can run this command to check mDNS group information including the VLANs of the users and service provisioning devices added to the mDNS group.

If **name** *group-name* or **user-vlan** *vlan-id* is not specified in the command, the information about all mDNS groups is displayed.

Example

Display the information about all mDNS groups.

```
<HUAWEI> display mdns group
mDNS Group Information:
--------------------------------------------------------------------------------
 Group Name   :  group1
 User Vlan    :  10
 Service Vlan :  20  30

 Group Name   :  group2
 User Vlan    :  20  30
 Service Vlan :  20  40
--------------------------------------------------------------------------------
Total: 2
```

Table 6-36 Description of the **display mdns group** command output

Item	Description
Group Name	Name of an mDNS group. To configure the mDNS group name, run the **mdns group** command.
User Vlan	VLAN that users in an mDNS group belong to. To configure the VLAN that users in an mDNS group belong to, run the **user-vlan** command.
Service Vlan	VLAN that service provisioning devices in an mDNS group belong to. To configure the VLAN that service provisioning devices in an mDNS group belong to, run the **service-vlan** command.
Total	Number of mDNS groups that have been configured on the device.

6.6.5 display mdns service

Function

The **display mdns service** command displays service information recorded on the mDNS gateway.

Format

display mdns service { **all** [**verbose**] | **name** *name* | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays all service information recorded on the mDNS gateway.	-
name *name*	Displays information about a specified service name recorded on the mDNS gateway.	The service name must have been created.

Parameter	Description	Value
vlan *vlan-id*	Displays service information provided by a specified service VLAN, which is recorded on the mDNS gateway. The VLAN ID indicates the VLAN that the service provisioning device belongs to.	The service VLAN must have been created.
verbose	Displays detailed service information recorded on the mDNS gateway. If this parameter is not specified, the summary of service information recorded on the mDNS gateway is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device functioning as the mDNS gateway maintains service information lists of all service provisioning devices on a network. You can run this command to check service information recorded on the device.

NOTE

When a service name begins with a space or contains a question mark (?), the **name** parameter cannot be specified in this command.

Example

Display the summary of all services recorded on the mDNS gateway.

```
<HUAWEI> display mdns service all
MDNS Service Info:

Service name : Officejet Pro 8100 [C12FFA] (7)._printer._tcp.local
  SRV Info:
      Domain Name : HPC12FFA-156.local
      Port        : 515
      Vlan Id     : 200
  A Info:
      Domain Name : HPC12FFA-156.local
      IP Address  : 10.1.1.254
```

```
      Vlan Id     : 200
  TXT Info:
      Vlan Id     : 200
      Data Length : 297
Total service: 1
```

Display the details of all services recorded on the mDNS gateway.

```
<HUAWEI> display mdns service all verbose
MDNS Service Info:

Service name : Officejet Pro 8100 [C12FFA] (7)._printer._tcp.local
  SRV Info:
      Domain Name : HPC12FFA-156.local
      Port        : 515
      Vlan Id     : 10
      Cache Flush : 1
      Class       : 1
      TTL         : 120
      Aging Time  : 95
      Data Length : 264
      Priority    : 0
      Weight      : 0
  A Info:
      Domain Name : HPC12FFA-156.local
      IP Address  : 10.1.1.254
      Vlan Id     : 10
      Cache Flush : 1
      Class       : 1
      TTL         : 120
      Aging Time  : 115
  TXT Info:
      Vlan Id     : 10
      Data Length : 297
      Cache Flush : 1
      Class       : 1
      TTL         : 4500
      Aging Time  : 3400
      Text        : ***
Total service: 1
```

Table 6-37 Description of the **display mdns service** command output

Item	Description
MDNS Service Info	Service information recorded on the mDNS gateway.
Service name	Service name recorded on the mDNS gateway.
SRV Info	SRV type information, indicating service record information.
Domain Name	Domain name corresponding to the service name.
Port	Number of the port that provides the service.
A Info	A type information, indicating host record information.

Item	Description
IP Address	IP address corresponding to the domain name.
TXT Info	TXT type information, indicating the description of service record information.
Data Length	TXT data length.
PTR Info	PTR type information, indicating that information is searched reversely; that is, the service provisioning device is searched based on the service type. **NOTE** This field is displayed only when the **display mdns service** command is run in the diagnostic view.
Total	Number of services recorded on the mDNS gateway. ● When you query all service information or service information provided by a specified service VLAN recorded on the mDNS gateway, this field displays the total number of service names. ● When you query service information about a specified service name recorded on the mDNS gateway, this field displays the sum of the SRV Info, TXT Info, and PTR Info field values. Type A information and type AAAA information are excluded because they are not service information.
Cache Flush	Cache information about services. The value can be 0 or 1. ● The value 1 indicates that the information is cached information. ● The value 0 indicates that the information is not cached information.
Class	Service type. ● 1: indicates the Internet type. ● 255: indicates any type.
TTL	TTL of the service.

Item	Description
Aging Time	Time elapsed after the mDNS gateway records the service information, in seconds.
Priority	Service priority.
Weight	Service weight.
Text	Service text.
Vlan Id	Service VLAN ID, indicating the VLAN that the service provisioning device belongs to.

6.6.6 mdns gateway enable

Function

The **mdns gateway enable** command enables the mDNS gateway.

The **undo mdns gateway enable** command disables the mDNS gateway.

By default, the mDNS gateway is disabled.

Format

mdns gateway enable

undo mdns gateway enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Bonjour technology proposed by Apple uses mDNS. The destination multicast address of 224.0.0.251 used by mDNS is only valid in a Layer 2 broadcast domain. That is, information can be forwarded in a VLAN only, but cannot be forwarded across VLANs or Layer 3 devices. Run the **mdns gateway enable** command on the device to enable the mDNS gateway so that the device can discover services across VLANs or Layer 3. The mDNS gateway records all available service lists and responds to service requests from Bonjour-compliant terminals.

Precautions

The device cannot function as both mDNS relay and gateway. A protection failure will occur if the **mdns relay enable** and **mdns gateway enable** commands are both configured on the device.

Example

Enable the mDNS gateway.

```
<HUAWEI> system-view
[HUAWEI] mdns gateway enable
```

6.6.7 mdns group

Function

The **mdns group** command creates an mDNS group and displays the mDNS group view.

The **undo mdns group** command deletes the created mDNS group.

By default, no mDNS group is created.

Format

mdns group *group-name*

undo mdns group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of an mDNS group.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the mDNS gateway queries service information lists of all service provisioning devices when receiving an mDNS request packet from a user requesting for a service. The mDNS gateway then replies to the user with a message containing the service provisioning devices that can provide the service. All the service provisioning devices mapping the service are visible to the user; therefore, service resources cannot be isolated. You can configure an mDNS group on the mDNS gateway to implement service resource isolation and refined service management. After receiving an mDNS request packet from a user requesting for a service, the mDNS gateway queries the mDNS group based on the user VLAN. If the user VLAN is added to a certain mDNS group, the gateway queries and replies with the requested service from the service list provided by the service VLAN mapping the mDNS group. If no mDNS group is specified for the user VLAN or no service VLAN is configured in the mDNS group, the gateway queries and replies with the requested service from the service lists provided by all service VLANs.

Follow-up Procedure

- Run the **user-vlan** command to configure the user VLAN for the mDNS group.
- Run the **service-vlan** command to configure the service VLAN to provide services for the users in the mDNS group.

Precautions

The device supports a maximum of 4096 mDNS groups.

Example

Create an mDNS group named **group1**.

```
<HUAWEI> system-view
[HUAWEI] mdns group group1
```

6.6.8 mdns probe interval

Function

The **mdns probe interval** command enables the device to periodically discover services and sets the discovery interval.

The **undo mdns probe interval** command disables the device from periodically discovering services and deletes the discovery interval.

By default, the device is not enabled to periodically discover services and the discovery interval is not set.

Format

mdns probe interval *interval*

undo mdns probe interval

Parameters

Parameter	Description	Value
interval	Specifies the discovery interval.	The value is an integer that ranges from 60 to 38400, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on an mDNS gateway or mDNS relay. The mDNS gateway maintains service information lists of all service provisioning devices on the network. A service information list records the service name, service type, TTL, host name, and IP address of each service. The TTL is provided by a service provisioning device to the mDNS gateway, and represents the aging time of a service. If the mDNS gateway receives mDNS response packets from a service provisioning device within the aging time, the mDNS gateway updates its service information. If the mDNS gateway does not receive mDNS response packets from a service provisioning device within the aging time, the mDNS gateway deletes its service information. If an mDNS gateway already exists on the network, a service provisioning device connected to the network advertises service information to the mDNS gateway through the mDNS relay. If a service provisioning device already exists before an mDNS gateway connects to the network, the service provisioning device does not advertise service information to the mDNS gateway.

If the device works as an mDNS gateway, you can run the **mdns probe interval** command to enable the periodical service discovery function and set the service discovery interval. The device then sends a service query message at the specified interval, and updates the service information list after receiving a response message from the service provisioning device.

If the device works as an mDNS relay and the **mdns probe interval** command is run, the device sends a service query message at the specified interval to request available service update in its VLAN, and forwards the response message from the service provisioning device to the mDNS gateway, ensuring that service information lists on the mDNS gateway are updated immediately.

Precautions

When the device as the mDNS gateway and service provisioning device are located on different network segments, the mDNS relay but not the mDNS gateway needs to be configured to periodically update service lists.

Only the following types of services can be discovered:

- _services._dns-sd._udp.local
- _raop._tcp.local
- _airplay._tcp.local
- _printer._tcp.local
- _device-info._tcp.local
- _rfb._tcp.local
- _sftp-ssh._tcp.local
- _ssh._tcp.local
- _smb._tcp.local
- _afpovertcp._tcp.local
- _universal._sub._ipp._tcp.local

Example

Enable the device to periodically discover services in VLAN 100 and set the discovery interval to 150s.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mdns probe interval 150
```

6.6.9 mdns permit service-type

Function

The **mdns permit service-type** command configures the service type that can be recorded by an mDNS gateway.

The **undo mdns permit id** command cancels the configured service type that can be recorded by an mDNS gateway.

By default, an mDNS gateway can record all service types.

Format

mdns permit service-type *service-type* **id** *id*

undo mdns permit id *id*

Parameters

Parameter	Description	Value
service-type *service-type*	Specifies a service type.	The value can be any service type that service provider devices can provide. The value is a string of characters, including digits, case-insensitive letters, and special characters visible on the keyboard, such as underscores (_), periods (.), and hyphens (-).
id *id*	Specifies a service type ID.	The value is an integer that ranges from 0 to 99.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, an mDNS gateway records all service types on the network and generates a service list. Because a service list size is limited, some uncommonly used services occupy the list space, which may cause entries unable to be generated for commonly used services such as airplay and printer. To reduce the number of service entries in the service list, run the **mdns permit service-type** command. This command allows service entries to be generated for only the specified service type, reduces the number of service entries in the service list.

NOTE

- An mDNS gateway can be configured to record airplay and printer services (a maximum of 64 airplay and printer devices are allowed), meeting the requirements in high-density WLANs and enterprise office WLANs as well as the requirements in manufacturing, finance, and government sectors.
- An mDNS gateway can be configured to record airplay and printer services (a maximum of 256 airplay and printer devices are allowed), meeting the requirements in scenarios where the number of VLANs to which concurrent users belong is less than 36.

Example

Configure the service type that can be recorded by the mDNS gateway.

```
<HUAWEI> system-view
[HUAWEI] mdns permit service-type _raop._tcp.local id 0
[HUAWEI] mdns permit service-type _airplay._tcp.local id 1
```

```
[HUAWEI] mdns permit service-type _printer._tcp.local id 2
[HUAWEI] mdns permit service-type _device-info._tcp.local id 3
[HUAWEI] mdns permit service-type _rfb._tcp.local id 4
[HUAWEI] mdns permit service-type _sftp-ssh._tcp.local id 5
[HUAWEI] mdns permit service-type _ssh._tcp.local id 6
[HUAWEI] mdns permit service-type _smb._tcp.local id 7
[HUAWEI] mdns permit service-type _afpovertcp._tcp.local id 8
[HUAWEI] mdns permit service-type _universal._sub._ipp._tcp.local id 9
```

6.6.10 mdns source ip

Function

The **mdns source ip** command configures the source IP address in mDNS packets sent by the device that functions as an mDNS gateway or mDNS relay.

The **undo mdns source ip** command deletes the configuration of the source IP address in mDNS packets sent by the device.

By default, no source IP address is configured.

Format

mdns source ip *ip-address*

undo mdns source ip

Parameters

Parameter	Description	Value
ip-address	Specifies a source IP address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication with user terminals and service provisioning devices, run this command to specify the source IP address in mDNS packets sent by the mDNS gateway or mDNS relay.

NOTE

When the device works as an mDNS relay, it is recommended that the IP address of the interface connecting the device to the mDNS gateway be used as the source IP address.

User terminals and service provisioning devices will ignore the source IP address of multicast mDNS packets received from the mDNS gateway or mDNS relay. As such, the source IP address configured by this command does not need to be on the same network segment as the user terminals or service provisioning devices.

When the device functions as an mDNS gateway, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS gateway is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- If an mDNS relay is deployed, the mDNS gateway exchanges packets with the mDNS relay in unicast mode. When sending packets to the mDNS relay, the mDNS gateway uses the next-hop IP address of the outbound interface as the source IP address of the packets based on the routing table. If this command is configured, the device preferentially uses the configured IP address as the source IP address of packets.
- When receiving a request to discover services from a terminal, the mDNS gateway uses the IP address configured by this command as the source IP address of the response packet. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN to which the response packet belongs as the source IP address of the response packet.

When the device functions as an mDNS relay, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS relay is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS relay uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- When the device acting as the mDNS relay forwards mDNS packets to an mDNS gateway, it uses the next-hop IP address of the outbound interface as the source IP address of packets based on the routing table. If this command is configured, the device preferentially uses the configured IP address as the source IP address of packets.

Precautions

When the device acting as an mDNS gateway is configured to periodically discover services, the device periodically sends mDNS query packets to all mDNS service provisioning devices in the VLAN, which are expected to return response packets. The destination IP address is the multicast address 224.0.0.251.

Before the mDNS service TTL expires, the mDNS gateway sends mDNS query packets to service provisioning devices that are expected to return response packets. If an mDNS service is advertised through an mDNS relay, the destination IP address of the query packets is the IP address of the mDNS relay. If an mDNS service is not advertised through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

When the device acting as an mDNS gateway receives mDNS requests from terminals and the requested services are available, the device returns mDNS response packets. If the mDNS request packets are forwarded through an mDNS relay, the destination IP address of the response packets is the IP address of the mDNS relay. If mDNS request packets are not forwarded through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

Example

Specify the source IP address of 10.1.1.1 in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device functioning as the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] mdns source ip 10.1.1.1
```

6.6.11 mdns whitelist source-ip

Function

The **mdns whitelist source-ip** command enables the trusted mDNS relay agent function and configures the IP address of the trusted mDNS relay agent.

The **undo mdns whitelist source-ip** command deletes the IP address of the trusted mDNS relay agent.

By default, the trusted mDNS relay agent function is disabled.

Format

mdns whitelist source-ip *ip-address*

undo mdns whitelist source-ip { **all** | *ip-address* }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the trusted mDNS relay agent.	The value is in dotted decimal notation.
all	Deletes IP addresses of all trusted mDNS relay agents.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Bogus mDNS relay agents may exist on the network and forge mDNS packets, threatening network security. To prevent this problem, run the **mdns whitelist source-ip** command on the device functioning as the mDNS gateway to enable the trusted mDNS relay agent function and configure the IP address of the trusted mDNS relay agent. The device then only processes unicast packets from the trusted mDNS relay agent, and discards unicast packets from untrusted mDNS relay agents. If the mDNS relay agent and mDNS gateway are on different network segments, you need to run the **mdns whitelist source-ip** *ip-address* command on the mDNS gateway to specify the IP address of the mDNS relay agent.

Example

Configure the IP address 192.168.1.1 for the trusted mDNS relay agent.

```
<HUAWEI> system-view
[HUAWEI] mdns whitelist source-ip 192.168.1.1
```

6.6.12 reset mdns gateway statistics

Function

The **reset mdns gateway statistics** command clears statistics on the mDNS gateway.

Format

reset mdns gateway statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

During routine maintenance and fault location, you can view statistics on mDNS packets received and sent by the mDNS gateway in a given period of time. Before viewing the statistics, run the **reset mdns gateway statistics** command to delete existing statistics. Then the mDNS gateway recollects statistics on received and sent mDNS packets. You can run the **display mdns gateway statistics** command to view statistics on mDNS packets received and sent by the mDNS gateway.

NOTICE

Cleared statistics on the mDNS gateway cannot be restored. Exercise caution when you use the **reset mdns gateway statistics** command.

Example

Clear statistics on the mDNS gateway.

```
<HUAWEI> reset mdns gateway statistics
```

6.6.13 service-vlan

Function

The **service-vlan** command configures service VLANs (that the service provisioning devices belong to) to provide services for users in an mDNS group.

The **undo service-vlan** deletes the service VLANs that provide services for users in an mDNS group.

By default, no service VLAN is configured to provide services for users in an mDNS group.

Format

service-vlan *vlan-id* &<1-32>

undo service-vlan { *vlan-id* &<1-32> | **all** }

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN that the service provisioning devices belong to.	The value is an integer in the range from 1 to 4094.
all	Specifies all service VLANs.	-

Views

mDNS group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device functioning as an mDNS gateway maintains service information lists of all service provisioning devices on a network, and it can use mDNS groups to isolate service resources to provide refined service management. You can run the **service-vlan** command to configure service VLANs to provide services for users in the mDNS group. The users (specified using the **user-vlan** command in the mDNS group view) in the mDNS group can only obtain services from the service list provided by the service VLAN mapping the mDNS group.

Prerequisites

An mDNS group has been created using the **mdns group** command.

Precautions

- You can add at most 32 service VLANs to an mDNS group.
- You can add a service VLAN to multiple mDNS groups to provide services for the users in these groups.
- The service VLAN cannot be configured as a reserved VLAN for a stack.

Example

Configure the service provisioning devices in VLAN 10 to provide services for the mDNS group **group1**.

```
<HUAWEI> system-view
[HUAWEI] mdns group group1
[HUAWEI-mdns-group-group1] service-vlan 10
```

6.6.14 user-vlan (mDNS group view)

Function

The **user-vlan** command configures user VLANs for an mDNS group.

The **undo user-vlan** command deletes user VLANs for the mDNS group.

By default, no user VLAN is configured for an mDNS group.

Format

user-vlan *vlan-id* &<1-32>

undo user-vlan { *vlan-id* &<1-32> | **all** }

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN that users belong to.	The value is an integer that ranges from 1 to 4094.
all	Specifies all user VLANs.	-

Views

mDNS group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device functioning as the mDNS gateway maintains service information lists of all service provisioning devices on a network, and it can use mDNS groups to isolate service resources to provide refined service management. You can run the **user-vlan** command to configure user VLANs for an mDNS group. The intra-VLAN users who join the mDNS group can only obtain services from the service list provided by the service VLAN (specified using the **service-vlan** command) mapping the mDNS group.

Prerequisites

An mDNS group has been created using the **mdns group** command.

Precautions

- You can add at most 32 user VLANs to an mDNS group.
- A user VLAN can belong to only one mDNS group.
- If no mDNS group is specified for the user VLAN or no service VLAN is configured in the mDNS group, the gateway queries and replies with the requested service from the service lists provided by all service VLANs.

Example

Add the users in VLAN 10 to the mDNS group **group1**.

```
<HUAWEI> system-view
[HUAWEI] mdns group group1
[HUAWEI-mdns-group-group1] user-vlan 10
```

6.7 mDNS Relay Configuration Commands

6.7.1 Command Support

Only the following switch models support mDNS Relay:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

6.7.2 display mdns relay

Function

The **display mdns relay** command displays the mDNS relay configuration.

Format

display mdns relay

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the mDNS relay is configured, you can run the **display mdns relay** command to view the mDNS relay configuration.

Example

Display the mDNS relay configuration.

```
<HUAWEI> display mdns relay
MDNS Relay Information:
--------------------------------------------------------------------------------
 MDNS Gateway IP   :  10.1.1.2
 MDNS Source IP    :  192.168.1.1
--------------------------------------------------------------------------------
 Relay Enable Vlan :  vlan100
--------------------------------------------------------------------------------
 Relay Probe Vlan  :  vlan100
--------------------------------------------------------------------------------
```

Table 6-38 Description of the display mdns relay command output

Item	Description
MDNS Gateway IP	IP address of the mDNS gateway specified on the device as the mDNS relay. To specify the IP address of the mDNS gateway on the device as the mDNS relay, run the **mdns gateway ip** command.
MDNS Source IP	Source IP address in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device as the mDNS relay. To specify the source IP address in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device as the mDNS relay, run the **mdns source ip** command.
Relay Enable Vlan	ID of the VLAN where the mDNS relay is enabled. To enable the mDNS relay, run the **mdns relay enable** command.
Relay Probe Vlan	ID of the VLAN where the mDNS relay is enabled to periodically discover services. To specify the ID of the VLAN where the mDNS relay is enabled to periodically discover services, run the **mdns probe interval** command.

6.7.3 display mdns relay statistics

Function

The **display mdns relay statistics** command displays statistics on the mDNS relay.

Format

display mdns relay statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During routine maintenance and fault location, you can run the **display mdns relay statistics** command to view statistics on mDNS packets received, sent and dropped by the mDNS relay in a given period of time.

To query statistics again, run the **reset mdns relay statistics** command to clear existing statistics.

NOTICE

Cleared statistics on the mDNS relay cannot be restored. Exercise caution when you use the **reset mdns relay statistics** command.

Example

Display statistics on the mDNS relay.

```
<HUAWEI> display mdns relay statistics
MDNS relay statistics:
------------------------------------
 Received  : 100
 Sent      : 100
 Dropped   : 0
  Bad Pkt Length : 0
  Other          : 0
------------------------------------
```

Table 6-39 Description of the display mdns relay statistics command output

Item	Description
Received	Number of mDNS packets received by the mDNS relay.
Sent	Number of mDNS packets sent by the mDNS relay.
Dropped	Number of mDNS packets dropped by the mDNS relay.
Bad Pkt Length	Number of mDNS packets discarded because the packet length exceeds the upper limit.
Other	Number of mDNS packets discarded because of other reasons.

6.7.4 mdns gateway ip

Function

The **mdns gateway ip** command specifies the IP address of the mDNS gateway on the device as the mDNS relay.

The **undo mdns gateway ip** command deletes the configured IP address of the mDNS gateway on the device as the mDNS relay.

By default, the IP address of the mDNS gateway is not specified on the device as the mDNS relay.

Format

mdns gateway ip *ip-address*

undo mdns gateway ip

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the mDNS gateway.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device as the mDNS relay needs to forward mDNS packets from Bonjour-compliant terminals or service provisioning devices to the mDNS gateway. After the **mdns gateway ip** command is used to specify the IP address of the mDNS gateway on the mDNS relay, the mDNS relay converts mDNS packets from Bonjour-compliant terminals or service provisioning devices into unicast packets and sends them to the mDNS gateway.

Example

Specify the IP address of the mDNS gateway as 10.1.1.1 on the device as the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] mdns gateway ip 10.1.1.1
```

6.7.5 mdns probe interval

Function

The **mdns probe interval** command enables the device to periodically discover services and sets the discovery interval.

The **undo mdns probe interval** command disables the device from periodically discovering services and deletes the discovery interval.

By default, the device is not enabled to periodically discover services and the discovery interval is not set.

Format

mdns probe interval *interval*

undo mdns probe interval

Parameters

Parameter	Description	Value
interval	Specifies the discovery interval.	The value is an integer that ranges from 60 to 38400, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on an mDNS gateway or mDNS relay. The mDNS gateway maintains service information lists of all service provisioning devices on the network. A service information list records the service name, service type, TTL, host name, and IP address of each service. The TTL is provided by a service provisioning device to the mDNS gateway, and represents the aging time of a service. If the mDNS gateway receives mDNS response packets from a service provisioning device within the aging time, the mDNS gateway updates its service information. If the mDNS gateway does not receive mDNS response packets from a service provisioning device within the aging time, the mDNS gateway deletes its service information. If an mDNS gateway already exists on the network, a service provisioning device connected to the network advertises service information to the mDNS gateway through the mDNS relay. If a service provisioning device already exists before an mDNS gateway connects to the network, the service provisioning device does not advertise service information to the mDNS gateway.

If the device works as an mDNS gateway, you can run the **mdns probe interval** command to enable the periodical service discovery function and set the service discovery interval. The device then sends a service query message at the specified interval, and updates the service information list after receiving a response message from the service provisioning device.

If the device works as an mDNS relay and the **mdns probe interval** command is run, the device sends a service query message at the specified interval to request available service update in its VLAN, and forwards the response message from the service provisioning device to the mDNS gateway, ensuring that service information lists on the mDNS gateway are updated immediately.

Precautions

When the device as the mDNS gateway and service provisioning device are located on different network segments, the mDNS relay but not the mDNS gateway needs to be configured to periodically update service lists.

Only the following types of services can be discovered:

- _services._dns-sd._udp.local
- _raop._tcp.local
- _airplay._tcp.local
- _printer._tcp.local
- _device-info._tcp.local
- _rfb._tcp.local
- _sftp-ssh._tcp.local
- _ssh._tcp.local
- _smb._tcp.local
- _afpovertcp._tcp.local
- _universal._sub._ipp._tcp.local

Example

Enable the device to periodically discover services in VLAN 100 and set the discovery interval to 150s.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mdns probe interval 150
```

6.7.6 mdns relay enable

Function

The **mdns relay enable** command enables the mDNS relay.

The **undo mdns relay enable** command disables the mDNS relay.

By default, the mDNS relay is disabled.

Format

mdns relay enable

undo mdns relay enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Bonjour technology proposed by Apple uses mDNS. The destination multicast address of 224.0.0.251 used by mDNS is only valid in a Layer 2 broadcast domain. That is, information can be forwarded in a VLAN only, but cannot be forwarded across VLANs or Layer 3 devices. The mDNS relay and mDNS gateway solution implements service discovery across Layer 3. The device can function as the mDNS relay to forward mDNS packets exchanged between Bonjour-compliant terminals or service provisioning devices and mDNS gateway, implementing service discovery across Layer 3. The **mdns relay enable** command enables the mDNS relay.

Precautions

The device cannot function as both mDNS relay and gateway. A protection failure will occur if the **mdns relay enable** and **mdns gateway enable** commands are both configured on the device.

Example

Enable the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mdns relay enable
```

6.7.7 mdns source ip

Function

The **mdns source ip** command configures the source IP address in mDNS packets sent by the device that functions as an mDNS gateway or mDNS relay.

The **undo mdns source ip** command deletes the configuration of the source IP address in mDNS packets sent by the device.

By default, no source IP address is configured.

Format

mdns source ip *ip-address*

undo mdns source ip

Parameters

Parameter	Description	Value
ip-address	Specifies a source IP address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication with user terminals and service provisioning devices, run this command to specify the source IP address in mDNS packets sent by the mDNS gateway or mDNS relay.

NOTE

When the device works as an mDNS relay, it is recommended that the IP address of the interface connecting the device to the mDNS gateway be used as the source IP address.

User terminals and service provisioning devices will ignore the source IP address of multicast mDNS packets received from the mDNS gateway or mDNS relay. As such, the source IP address configured by this command does not need to be on the same network segment as the user terminals or service provisioning devices.

When the device functions as an mDNS gateway, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS gateway is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- If an mDNS relay is deployed, the mDNS gateway exchanges packets with the mDNS relay in unicast mode. When sending packets to the mDNS relay, the mDNS gateway uses the next-hop IP address of the outbound interface as the source IP address of the packets based on the routing table. If this command

is configured, the device preferentially uses the configured IP address as the source IP address of packets.

- When receiving a request to discover services from a terminal, the mDNS gateway uses the IP address configured by this command as the source IP address of the response packet. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN to which the response packet belongs as the source IP address of the response packet.

When the device functions as an mDNS relay, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS relay is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS relay uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- When the device acting as the mDNS relay forwards mDNS packets to an mDNS gateway, it uses the next-hop IP address of the outbound interface as the source IP address of packets based on the routing table. If this command is configured, the device preferentially uses the configured IP address as the source IP address of packets.

Precautions

When the device acting as an mDNS gateway is configured to periodically discover services, the device periodically sends mDNS query packets to all mDNS service provisioning devices in the VLAN, which are expected to return response packets. The destination IP address is the multicast address 224.0.0.251.

Before the mDNS service TTL expires, the mDNS gateway sends mDNS query packets to service provisioning devices that are expected to return response packets. If an mDNS service is advertised through an mDNS relay, the destination IP address of the query packets is the IP address of the mDNS relay. If an mDNS service is not advertised through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

When the device acting as an mDNS gateway receives mDNS requests from terminals and the requested services are available, the device returns mDNS response packets. If the mDNS request packets are forwarded through an mDNS relay, the destination IP address of the response packets is the IP address of the mDNS relay. If mDNS request packets are not forwarded through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

Example

Specify the source IP address of 10.1.1.1 in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device functioning as the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] mdns source ip 10.1.1.1
```

6.7.8 reset mdns relay statistics

Function

The **reset mdns relay statistics** command clears statistics on the mDNS relay.

Format

reset mdns relay statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

During routine maintenance and fault location, you can view statistics on mDNS packets received and sent by the mDNS relay in a given period of time. Before viewing the statistics, run the **reset mdns relay statistics** command to delete existing statistics. Then the mDNS relay recollects statistics on received and sent mDNS packets. You can run the **display mdns relay statistics** command to view statistics on mDNS packets received and sent by the mDNS relay.

NOTICE

Cleared statistics on the mDNS relay cannot be restored. Exercise caution when you use the **reset mdns relay statistics** command.

Example

Clear statistics on the mDNS relay.

```
<HUAWEI> reset mdns relay statistics
```

6.8 UDP Helper Configuration Commands

6.8.1 Command Support

Only the following switch models support UDP helper:

S5720I-SI, S5735-S, S5735-L, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

6.8.2 display udp-helper port

Function

The **display udp-helper port** command displays the configured UDP ports to which packets need to be relayed on the device.

Format

display udp-helper port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the configured UDP ports to which packets need to be relayed, run this command. If the UDP helper function is not enabled, the system displays the following information:

```
Info: Udp-helper has not been enabled, please enable udp-helper first.
```

Example

Display the UDP ports to which packets need to be relayed.

```
<HUAWEI> display udp-helper port
Udp-Port-Number       Description
-------------------------------------------------------------
      1              TCP Port Service Multiplexer
     37              Time
     49              Login Host Protocol
     53              Domain Name Server
     69              Trivial File Transfer
    137              NETBIOS Name Service
    138              NETBIOS Datagram Service
```

Table 6-40 Description of the **display udp-helper port** command output

Item	Description
Udp-Port-Number	UDP ports to which packets need to be relayed. UDP ports are classified into the following types: ● Well-known port: The well-known port numbers range from 0 to 1023. These ports are used by standard TCP/UDP protocols. ● Registered port: The registered port numbers range from 1024 to 49151. They are vendor-specific ports. ● Dynamic/Static port: The dynamic or static port numbers range from 49152 to 65535. These ports can be used as required and may conflict on a network. To configure the UDP ports, run the **udp-helper port** command.
Description	UDP port description.

6.8.3 display udp-helper server

Function

The **display udp-helper server** command displays the VLANIF interface, destination server address, and number of relayed UDP packets.

Format

display udp-helper server [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays statistics about UDP broadcast packets relayed on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The interface type must be VLANIF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays statistics about packets relayed by UDP helper. The statistics help you monitor the UDP helper function.

If no parameter is specified, statistics about relayed packets on all VLANIF interfaces are displayed.

NOTE

This command collects statistics on only the packets forwarded by the UDP helper server. Successful packet forwarding depends on the reachable route.

Example

Display statistics about relayed packets on VLANIF 100.

```
<HUAWEI> display udp-helper server interface vlanif 100
vlan-interface       Server-Ip                packet-num
Vlanif100          10.10.10.10                         0
```

Table 6-41 Description of the **display udp-helper server** command output

Item	Description
vlan-interface	VLANIF interface on which UDP packets are relayed.

Item	Description
Server-Ip	Destination server address. You can run the **udp-helper server** command to set the destination server address.
packet-num	Number of packets sent to the destination server.

6.8.4 reset udp-helper packet

Function

The **reset udp-helper packet** command clears statistics about packets relayed by UDP helper.

Format

reset udp-helper packet

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

This command clears statistics about packets relayed by UDP helper. Before collecting packet statistics in a certain period, run this command to clear existing statistics first.

NOTICE

UDP helper statistics cannot be restored after being cleared. Exercise caution when you run the **reset udp-helper packet** command.

Example

Clear statistics about packets relayed by UDP helper.

```
<HUAWEI> reset udp-helper packet
Warning: This command will delete the packet statistics of udp-helper.Continue?[Y/N]y
```

6.8.5 udp-helper enable

Function

The **udp-helper enable** command enables the UDP Helper function.

The **undo udp-helper enable** command disables the UDP Helper function.

By default, the UDP Helper function is disabled.

Format

udp-helper enable

undo udp-helper enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts on an enterprise intranet may need to obtain the network configuration or resolve host names by sending UDP broadcast packets to the server. If the host and the server are located in different broadcast domains, broadcast packets cannot reach the server and the host cannot obtain the configuration from the server. The switch provides the UDP Helper function to solve this problem. UDP Helper can relay the UDP broadcast packets with specified destination ports. It converts the broadcast packets into unicast packets and sends the unicast packets to the specified destination servers.

The packets that can be forwarded by UDP Helper must meet the following requirements:

- The destination MAC address is the broadcast MAC address (ffff-ffff-ffff).
- The Time-to-Live (TTL) is larger than 1.
- The protocol type is UDP.
- The destination port is a specified UDP port.

Precautions

UDP helper enables a device to relay DHCP packets destined for UDP port 67 (that is, DHCP packets sent to the DHCP server).

However, a UDP helper-enabled device cannot relay DHCP packets destined for UDP port 68 (that is, DHCP packets sent to the DHCP client). To relay this type of DHCP packets, you must enable the DHCP relay function.

After the UDP Helper function is enabled, the switch relays broadcast packets destined for the following UDP ports by default.

Protocol	UDP Port Number
Trivial File Transfer Protocol (TFTP)	69
Domain Name System (DNS)	53
Time Service	37
NetBIOS Name Service (NetBIOS-NS)	137
NetBIOS Datagram Service (NetBIOS-DS)	138
Terminal Access Controller Access Control System (TACACS)	49

After UDP Helper is disabled, all specified UDP ports and default ports are canceled.

NOTE

After the UDP Helper function is enabled, the switch automatically relays the UDP broadcast packets on six default ports. If you want to relay the packets on only one default port, run the **undo udp-helper port** { **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** } command to disable packet relay on other five ports.

Example

Enable UDP Helper.

```
<HUAWEI> system-view
[HUAWEI] udp-helper enable
```

6.8.6 udp-helper port

Function

The **udp-helper port** command specifies the UDP ports to which UDP broadcast packets are relayed.

The **undo udp-helper port** command deletes the UDP ports to which packets are relayed.

By default, no UDP port is specified. After UDP helper is enabled, the switch relays broadcast packets destined for ports 37, 49, 53, 69, 137, and 138 by default.

Format

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Parameters

Parameter	Description	Value
port-number	Specifies the UDP ports to which packets are relayed.	The value is an integer that ranges from 1 to 65535, excluding 68.
dns	Relays the UDP broadcast packets sent by DNS. The UDP port number is 53.	-
netbios-ds	Relays the UDP broadcast packets sent by NetBIOS-DS. The UDP port number is 138.	-
netbios-ns	Relays the UDP broadcast packets sent by NetBIOS-NS. The UDP port number is 137.	-
tacacs	Relays the UDP broadcast packets sent by TACACS. The UDP port number is 49.	-
tftp	Relays the UDP broadcast packets sent by TFTP. The UDP port number is 69.	-
time	Relays the UDP broadcast packets sent by time service. The UDP port number is 37.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After UDP helper is enabled and the UDP ports are specified, the switch relays the received UDP broadcast packets destined for the specified ports.

Precautions

The **udp-helper port** command takes effect globally. That is, if the switch is configured to relay packets destined for a UDP port, all the interfaces configured with the destination server address will relay such packets.

UDP helper enables a device to relay DHCP packets destined for UDP port 67 (that is, DHCP packets sent to the DHCP server).

However, a UDP helper-enabled device cannot relay DHCP packets destined for UDP port 68 (that is, DHCP packets sent to the DHCP client). To relay this type of DHCP packets, you must enable the DHCP relay function.

The switch supports a maximum of 16 UDP ports.

Example

Configure the switch to relay the broadcast packets destined for UDP port 100.

```
<HUAWEI> system-view
[HUAWEI] udp-helper enable
[HUAWEI] udp-helper port 100
```

6.8.7 udp-helper server

Function

The **udp-helper server** command configures the destination server to which UDP packets are relayed.

The **undo udp-helper server** command deletes the destination server to which UDP packets are relayed.

By default, no destination server is configured for UDP Helper.

Format

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a destination server. The IP address can be a unicast address or a subnet broadcast address, but cannot be 255.255.255.255. Otherwise, the configuration fails.	The value is in dotted decimal notation.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If UDP Helper is enabled and the destination server is configured on an interface, when the interface receives the UDP broadcast packets destined for the specified port, it converts the broadcast packets into unicast packets with the destination address *ip-address* and sends them to the specified server.

Precautions

- A maximum of 20 destination servers can be configured on an interface. If multiple destination servers are configured on an interface, the switch converts the broadcast packets into unicast packets and sends them to all these servers.
- When specifying the IP address of a destination server, ensure that the switch has a reachable route to the network segment where the destination server is located. If no route is reachable, packets cannot be forwarded.
- When the **undo udp-helper server** command is used without parameter specified, all the configured destination servers on the interface are deleted.

Example

Configure destination server 10.1.1.2 on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] udp-helper server 10.1.1.2
```

6.9 IP Performance Optimization Configuration Commands

6.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

6.9.2 clear ip df

Function

The **clear ip df** command enables fragmentation for outgoing control-plain IP packets on an interface.

The **undo clear ip df** command disables fragmentation for outgoing control-plain IP packets on an interface.

By default, fragmentation for outgoing control-plain IP packets on an interface is disabled.

Format

clear ip df

undo clear ip df

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP header contains a Don't Fragment (DF) bit to identify whether packet fragmentation is allowed. Commonly, if the DF bit of a packet is set to 1, the packet cannot be fragmented. When the remote device or intermediate forwarding device receives IP packets, if it checks the packet length and discards packets whose length is longer than the Maximum Transmission Unit (MTU) on the interface, network communication is interrupted. You can run the **clear ip df** command to enable fragmentation for outgoing control-plane IP packets so that packets with the DF bit set to 1 are fragmented based on the MTU value on the interface.

After fragmentation for outgoing control-plain IP packets is enabled on an interface, the device sets the Don't Fragment (DF) field to 0 and fragments IP packets that meet the following conditions:

- The value of the DF field in the IP packet header is 1.
- The packet length is larger than the MTU value of the interface that sends the packets.

Precautions

This command takes effect only for the control-plain packets but not for the forwarding-plain packets.

Example

Enable fragmentation for outgoing IP packets on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] clear ip df
```

Enable fragmentation for outgoing IP packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] clear ip df
```

6.9.3 discard { ra | rr | srr | ts }

Function

The **discard { ra | rr | srr | ts }** command configures the device to discard the packets that contain the route alert option, route record option, source route option, or timestamp option on interfaces.

The **undo discard { ra | rr | srr | ts }** command configures the device to process the packets that contain the route alert option, route record option, source route option, or timestamp option on interfaces.

By default, the device processes packets sent to the CPU based on route options contained in these packets.

Format

discard { ra | rr | srr | ts }

undo discard { ra | rr | srr | ts }

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP packets can carry route options including the route alert option (**ra**), route record option (**rr**), source route option (**srr**), and timestamp option (**ts**).

These route options are used to diagnose network paths and temporarily transmit special services. These options, however, may be used by attackers to spy on the network structure for initiating attacks. This degrades network security and device performance. To solve this problem, you can run the **discard { ra | rr | srr | ts }** command to configure the device to discard the IP packets that contain the route options.

Precautions

The **discard { ra | rr | srr | ts }** command only takes effect for the packets on inbound interfaces.

The **discard { ra | rr | srr | ts }** command only takes effect for packets sent to the CPU. For packets that are not sent to the CPU, the device processes and forwards them using the same method of processing packets without route options regardless of whether the **discard { ra | rr | srr | ts }** command is configured or not.

Example

Configure the device to discard the packets that contain the route alert option on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] discard ra
```

Configure the device to discard the packets that contain the route alert option on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] discard ra
```

6.9.4 display icmp statistics

Function

The **display icmp statistics** command displays ICMP traffic statistics.

Format

display icmp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about ICMP packet sending and receiving, run the **display icmp statistics** command.

Example

Display ICMP traffic statistics.

```
<HUAWEI> display icmp statistics
  Input: bad formats          0          bad checksum            0
         echo                10         destination unreachable 0
         source quench        0          redirects               0
         echo reply          25         parameter problem       0
         timestamp request    0          information request     0
         mask requests        0          mask replies            0
         time exceeded        0          timestamp reply         0
         Mping request        0          Mping reply             0
  Output:echo                25          destination unreachable 0
         source quench        0          redirects               0
         echo reply          10         parameter problem       0
         timestamp request    0          information reply       0
         mask requests        0          mask replies            0
         time exceeded        0          timestamp reply         0
         Mping request        0          Mping reply             0
```

Table 6-42 Description of the **display icmp statistics** command output

Item	Description
Input	Received packets.
Output	Sent packets.
bad formats	Number of packets in incorrect format.
bad checksum	Number of packets with checksum errors.
echo	Number of echo request packets.
destination unreachable	Number of unreachable packets.
source quench	Number of source quench packets.
redirects	Number of redirection packets.
echo reply	Number of echo reply packets.

Item	Description
parameter problem	Number of packets with incorrect parameters.
timestamp request	Number of timestamp request packets.
information request	Number of information request packets.
information reply	Number of information reply packets.
mask requests	Number of mask request packets.
mask replies	Number of mask reply packets.
time exceeded	Number of expired packets.
timestamp reply	Number of timestamp reply packets.
Mping requests	Number of multicast ping request packets.
Mping reply	Number of multicast ping reply packets.

6.9.5 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-

Parameter	Description	Value
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Example

Display IP information about VLANIF15.

```
<HUAWEI> display ip interface vlanif 15
Vlanif15 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 766390, bytes : 41540847, multicasts : 681817
```

```
output packets : 242239, bytes : 14679482, multicasts : 172333
Directed-broadcast packets:
 received packets:            0, sent packets:            0
 forwarded packets:           0, dropped packets:           0
Internet Address is 10.1.1.119/24
Broadcast address : 10.1.1.255
TTL being 1 packet number:    164035
TTL invalid packet number:          0
ICMP packet input number:          0
  Echo reply:                     0
  Unreachable:                    0
  Source quench:                  0
  Routing redirect:               0
  Echo request:                   0
  Router advert:                  0
  Router solicit:                 0
  Time exceed:                    0
  IP header bad:                  0
  Timestamp request:              0
  Timestamp reply:                0
  Information request:            0
  Information reply:              0
  Netmask request:                0
  Netmask reply:                  0
  Unknown type:                   0
```

Table 6-43 Description of the **display ip interface** command output

Item	Description
Vlanif15 current state	Physical status of the interface: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the administrator has run the **shutdown (interface view)** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: The link layer protocol of the interface is running properly. ● DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface or a serial interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 766390, bytes : 41540847, multicasts : 681817	Total number of packets, bytes, and multicast packets received by the interface.

Item	Description
output packets : 242239, bytes : 14679482, multicasts : 172333	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
Internet Address is	IP address assigned to the interface and mask length.
Broadcast address	Broadcast address of the interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

Display brief IP information about VLANIF15.

```
<HUAWEI> display ip interface brief vlanif 15
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                     IP Address/Mask      Physical   Protocol
Vlanif15                      10.1.1.119/24        up         up
```

Table 6-44 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down	^down: indicates that the interface is a backup interface.
(l): loopback	The letter "l" refers to loopback.
(s): spoofing	The letter "s" refers to spoofing.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
Interface	Interface type and number.
IP Address/Mask	IP address and mask of an interface.
Physical	Physical status of an interface: ● Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. ● Down: indicates that the interface becomes faulty. ● *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. ● !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.

Item	Description
Protocol	Link protocol status of the interface: - Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. - Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

6.9.6 display ip forwarding status

Function

The **display ip forwarding status** command displays whether IPv4 Layer 3 unicast forwarding is enabled on a switch.

Format

display ip forwarding status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether IPv4 Layer 3 unicast forwarding is enabled on a switch.

Example

Display whether IPv4 Layer 3 unicast forwarding is enabled on the switch.

```
<HUAWEI> display ip forwarding status
Current IP forwarding status: Open
```

Table 6-45 Description of the **display ip forwarding status** command output

Item	Description
Current IP forwarding status	Whether IPv4 Layer 3 unicast forwarding is enabled: ● Open: The function is enabled. ● Closed: The function is disabled. To configure IPv4 Layer 3 unicast forwarding, run the **ip forwarding disable** command.

6.9.7 display ip socket

Function

The **display ip socket** command displays information about the created IPv4 sockets.

Format

display ip socket [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **socket-type** *socket-type*]

Parameters

Parameter	Description	Value
monitor	Displays information about the socket monitor. Information about the socket monitor is displayed together with information about the socket.	-
task-id *task-id*	Displays socket information of the task with a specified ID.	The value must be an existing task ID.
socket-id *socket-id*	Displays information about the socket with a specified ID.	The value must be an existing socket ID.
socket-type *socket-type*	Displays information about a socket of a specified type.	The value is an integer. **Table 6-46** shows the value range.

Table 6-46 Value range of **socket-type** *socket-type*

Value	Description
1	TCP socket
2	UDP socket
3	RAWIP socket
4	RAWLINK socket

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A socket monitor monitors and records each connection. A RawLink also monitors interfaces. The socket monitor records specific protocol events that occur during operations. In addition, it logs information in the disk space.

The socket monitor is similar to a black box of the system. It records specific events that happen during system operations. When the system fails, you can use information recorded by the socket monitor to locate faults.

You can also set the filtering rules, such as the task ID, socket ID, and socket type so that only the information matching the rules is displayed. This reduces information output and helps you locate faults accurately and efficiently.

Example

Display information about the IP sockets.

```
<HUAWEI> display ip socket monitor
SOCK_STREAM:
Task = VTYD(30), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SENDVPNID(23553)
SO_SETKEEPALIVE SO_SETACL,
socket state = SS_PRIV SS_ASYNC
                        Socket Monitor:
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 cram time = 0000-00-00 00:00:00+08:00, lost msg= 0, msg type=0x00000000;
Nothing else has been captured!
SOCK_DGRAM:
Task = DHCP(54), socketid = 2, Proto = 17,
LA = 0.0.0.0:67, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_BROADCAST SO_REUSEPORT SO_UDPCHECKSUM SO_SENDVPNID(14849),
socket state = SS_PRIV
                        Socket Monitor:
Statistics:
```

```
 input packets = 6,recv packets = 6,output packets = 0;
Rcvbuf status:
 cram time = 0000-00-00 00:00:00+00:00, full times = 0,dropped packets = 0;
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 smb input = 0, smb output = 0, smooth over = 0,
 cram time = 0000-00-00 00:00:00+00:00, lost msg = 0, msg type = 0x00000000;
```

Display the information about the IP socket with the task ID as 23 and socket ID as 1.

```
<HUAWEI> display ip socket monitor task-id 23 socket-id 1
Task = RSVP(23), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
                        Socket Monitor:
Statistics:
 input packets = 0,recv packets = 0,output packets = 0;
Rcvbuf status:
 cram time = 00H00M00S: full times = 0,dropped packets = 0;
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 smb input = 0, smb output = 0, smooth over = 0,
 cram time = 00H00M00S, lost msg = 0, msg type = 0x00000000;
```

Display information about the IP socket with the socket type as TCP.

```
<HUAWEI> display ip socket monitor socket-type 1
SOCK_STREAM:
Task = VTYD(30), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_REUSEPORT SO_SENDVPNID(14849)
SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC
                        Socket Monitor:
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 cram time = 0000-00-00 00:00:00+00:00, lost msg= 0, msg type=0x00000000;
Nothing else has been captured!
```

Table 6-47 Description of the **display ip socket** command output

Item	Description
SOCK_STREAM	Socket types. There are the following socket types: ● SOCK_STREAM ● SOCK_DGRAM ● SOCK_RAWLINK ● SOCK_RAWIP
Task	Type and ID of the task that invokes the socket. For example, Task = VTYD(30) indicates that the task named VTYD uses the socket, with the task ID being 30.
socketid	Socket ID.

Item	Description
Proto	Protocol number.
LA	Local address/port number.
FA	Remote address/port number.
sndbuf	Maximum socket send buffer size. The value is in bytes.
rcvbuf	Maximum socket receive buffer size. The value is in bytes.
sb_cc	Number of sent packets. The value is in bytes and is valid only when TCP caches data packets.
rb_cc	Number of received packets. The value is in bytes.

Item	Description
socket option	Set socket options. There are the following socket options: - SO_DEBUG: indicates that debugging is enabled. - SO_ACCEPTCONN: indicates that the socket is the server and is responsible for monitoring. - SO_REUSEADDR: indicates that addresses are overlapped. After the option is set, multiple identical addresses can be bound to an interface. - SO_KEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up. - SO_DONTROUTE: indicates that a socket must choose the direct route to the destination when setting up a connection. - SO_BROADCAST: indicates that an interface can send broadcast packets. - SO_REUSEPORT: indicates that interfaces are overlapped. After the option is set, multiple identical interfaces can be bound to the local interface. This option is often set on servers. - SO_UDPCHECKSUM: indicates that the socket calculates the checksum of UDP packets. - SO_SENDVPNID: indicates an exclusive option for VPNs. - SO_SETKEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up. - SO_SETACL: indicates that an ACL can be configured on the interface. - SO_USELOOPBACK: indicates that a socket can use a loopback interface to receive or send data. - SO_LINGER: indicates the time for closing a TCP connection. If the time is not set to 0, a TCP connection is closed after the timer expires. If the time is set to 0, a TCP connection is closed immediately.

Item	Description
	- SO_OOBINLINE: indicates out-band data. When receiving data, a socket processes the out-band data first. - SO_SENDDATAIF: indicates that a socket uses the specified interface to receive or send data. - SO_SENDDATAIF_DONTSETTTL: indicates that a socket uses the specified interface to receive or send data but does not set the TTL value. - SO_SETSRCADDR: indicates that a socket sets the source address of outgoing packets. - SO_SENDBY_IF_NEXTHOP: indicates that a socket sets the outbound interface and next hop address of outgoing packets.

Item	Description
socket state	Socket status. There are the following socket states: ● SS_NOFDREF: indicates that the socket ID is deleted. ● SS_ISCONNECTED: indicates that a TCP connection is set up. ● SS_ISCONNECTING: indicates that a TCP connection is being set up. ● SS_ISDISCONNECTING: indicates that a TCP connection is being closed. ● SS_CANTSENDMORE: indicates that a socket cannot send data. ● SS_CANTRCVMORE: indicates that a socket cannot receive data. ● SS_RCVMARK: indicates that a socket sets the receiving option in the received packet. ● SS_NBIO: indicates that the type of a socket is non-blocking. ● SS_ISCONFIRMING: indicates that the upper-layer application will complete processing a connection. ● SS_BLOCKING: indicates that congestion occurs during packet receiving and sending. ● SS_RECALL: indicates that the message notification method is set by an asynchronous socket. ● SS_PRIV: indicates the option transferred from the Unix. The option is invalid in the current socket. ● SS_ASYNC: indicates the status identifier of an asynchronous socket.
Asyn Que status	Current asynchronous queue status.
read	Number of messages read by the asynchronous queue.
write	Number of messages written by the asynchronous queue.
connect	Number of connection messages in the asynchronous queue.
close	Number of messages about closed connections in the asynchronous queue.

Item	Description
peer close	Number of messages about connections closed by the remote end in the asynchronous queue.
accept	Number of messages received by the asynchronous queue.
keep alive down	Number of keepalivedown messages in the asynchronous queue.
cram time	Time for the asynchronous queue to become full.
lost msg	Number of asynchronous messages discarded by the asynchronous queue.
msg type	Current asynchronous message type.
smb input	Number of times of notifying the application layer to read received packets on the backup board.
smb output	Number of times of notifying the application layer to read sent packets on the backup board.
smooth over	Number of times of notifying the application layer that the smoothing is over.

6.9.8 display ip socket register-port

Function

The **display ip socket register-port** command displays non-well-known port numbers that have been assigned to services on the device.

Format

display ip socket register-port

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

As defined in RFC standards, port numbers larger than 1024 are non-well-known port numbers and can be assigned to desired services, such as NQA and SSH services. However, a non-well-known port number can be assigned to only one service on the same device. If you assign a non-well-known port number to two or more services, this port number takes effect for only the latest configured service. As a result, the other services using this port number will fail.

Before you assign a non-well-known port number to a service, run the **display ip socket register-port** command to check non-well-known port numbers that have been assigned to other services, preventing service failures caused by conflicts of non-well-known port numbers.

Example

Display non-well-known port numbers that have been assigned to services on the device.

```
<HUAWEI> display ip socket register-port
Port      Task        Type
5247      CWP_FWD     UDP4
31009     MPLSFW      UDP4
38514     INFO        UDP4
60000     EZOP        UDP4
65030     ipfpm       UDP4
65531     CWP_FWD     UDP4
65532     CWP_FWD     UDP4
65533     CWP_FWD     UDP4
65534     CWP_FWD     UDP4
3232      mdt         UDP6
3503      MPLSFW      UDP6
3784      BFD         UDP6
4784      BFD         UDP6
5246      CWP_FWD     UDP6
5247      CWP_FWD     UDP6
31009     MPLSFW      UDP6
38514     INFO        UDP6
60000     EZOP        UDP6
65531     CWP_FWD     UDP6
65532     CWP_FWD     UDP6
65533     CWP_FWD     UDP6
65534     CWP_FWD     UDP6
```

Table 6-48 Description of the **display ip socket register-port** command output

Item	Description
Port	Non-well-known port number that has been assigned to a service.
Task	Name of the task to which a non-well-known port number is assigned.
Type	Port type, including TCP and UDP.

6.9.9 display ip statistics

Function

The **display ip statistics** command displays IP traffic statistics.

Format

display ip statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IP traffic statistics include statistics about received packets (including discarded packets that carry source-route options), sent packets, fragmented packets, and reassembled packets. If a large number of bad protocol and no route fields is displayed in the command output, the device receives a large volume of IP packets of unknown protocol types and IP packets for which no routes can be found. In this situation, the device may be attacked by the connected devices.

Example

Display IP traffic statistics.

```
<HUAWEI> display ip statistics
 Input:     sum                263482      local               263473
            bad protocol            0      bad format               1
            bad checksum            0      bad options              0
            discard srr             0      discard rr               0
            discard ra              0      discard ts               0
            TTL exceeded            0
 Output:    forwarding              0      local               303399
            dropped             56479      no route               225
 Fragment:  input                   0      output                   0
            dropped                 0
            fragmented              0      couldn't fragment        0
 Reassembling:sum                   0      timeouts                 0
```

Table 6-49 Description of the **display ip statistics** command output

Item	Description
Input	Received packets.
sum	Total number of packets.

Item	Description
local	Number of packets sent to the upper-layer protocol.
bad protocol	Number of received IP packets of unknown protocol types. The protocol field in the IP header cannot be identified by the upper-layer protocol.
bad format	Number of packets in incorrect format.
bad checksum	Number of packets with checksum errors.
bad options	Number of packets with incorrect options.
discard srr	Number of discarded packets with source route options.
discard rr	Indicates the number of packets that are received and then discarded because of record-route options.
discard ra	Indicates the number of packets that are received and then discarded because of alert-route options.
discard ts	Indicates the number of packets that are received and then discarded because of time stamps options.
TTL exceeded	Number of packets discarded because the TTL expires.
Output	Sent packets.
forwarding	Number of forwarded packets.
local	Number of generated packets.
dropped	Number of discarded packets.
no route	Number of packets for which no correct route can be found, including the packets sent and forwarded by the local device.
Fragment	Number of packet fragments.
input	Number of received fragments.
output	Number of sent fragments.
dropped	Number of discarded fragments.
fragmented	Number of successfully fragmented packets.
couldn't fragment	Number of packets that cannot be fragmented.

Item	Description
Reassembling:sum	Number of successfully reassembled fragments.
timeouts	Number of expired fragments.

6.9.10 display load-balance mode

Function

The **display load-balance mode** command displays the load balancing mode on a switch.

Format

display load-balance mode [**packet** | **flow** | **slot** *slot-number*]

Parameters

Parameter	Description	Value
packet	Displays information about the switch adopting the per packet load balancing mode.	-
flow	Displays information about the switch adopting the per flow load balancing mode.	-
slot *slot-number*	Specifies the ID of a slot. After the slot ID is specified, the load balancing mode on a specified switch is displayed.	The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display load-balance mode packet** or the **display load-balance mode flow** command displays information about the switch adopting the specified load balancing mode.

The **display load-balance mode slot** *slot-number* command displays the load balancing mode on a specified switch.

If neither the slot ID nor load balancing mode is specified in the **display load-balance mode** command, by default, load balancing mode on the switch is displayed.

Example

Display the load balancing modes on the switch.

```
<HUAWEI> display load-balance mode
load-balance flow slot 0
```

Table 6-50 Description of the **display load-balance mode** command output

Item	Description
load-balance	Load balancing mode: ● packet: per packet load balancing ● flow: per flow load balancing
slot	Slot ID.

6.9.11 display network status

Function

Running the **display network status** command, you can check the network status of a device.

Format

display network status { **all** \| **tcp** \| **udp** \| **port** *port-number* }

Parameters

Parameter	Description	Value
all	Displays all the network information.	-
tcp	Displays TCP.	-

Parameter	Description	Value
udp	Displays UDP.	-
port *port-number*	Specifies the number of an interface.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display network status** command to check the network status, such as the running ports and services on the network. For example, when you find that a port is being used by an unknown module during a security scan, run the **display network status** command to check out the module.

Example

Display all information about the network status.

```
<HUAWEI> display network status all
Proto Task/SockId Local Addr&Port          Foreign Addr&Port        State
TCP   VTYD/1      0.0.0.0:23               0.0.0.0:0                Listening
TCP   HTTP/2      0.0.0.0:80               0.0.0.0:0                Listening
TCP   HTTP/1      0.0.0.0:443              0.0.0.0:0                Listening
TCP   VTYD/59     192.168.50.166:23        10.135.19.141:60445      Established
TCP6  VTYD/2      ::->23                   ::->0                    Listening
UDP   AGNT/1      0.0.0.0:161              0.0.0.0:0
UDP   SLAG/1      0.0.0.0:1025             0.0.0.0:0
UDP   RDS /1      0.0.0.0:1812             0.0.0.0:0
UDP   CMRE/1      0.0.0.0:65311            0.0.0.0:0
UDP6  AGT6/1      ::->161                  ::->0
UDP6  RDS /2      ::->1812                 ::->0
```

Table 6-51 Description of the **display network status** command output

Item	Description
Proto	Protocol

Item	Description
Task/SockId	Task and Socket ID - VTYD: Process login requests of all users. - HTTP: Transfer hypertext from WWW servers to local browsers - AGNT: Implement the IPv4 SNMP protocol. - SLAG: Implement E-Trunk. - RDS: Implement the RADIUS protocol, manage the protocol state machine, and maintain protocol databases. - CMRE: Register with the iMaster NCE-Campus for authentication and establishes NETCONF transmission channels. - AGT6: Implement the IPv6 SNMP protocol.
Local Addr&Port	Local IP address and Port number
Foreign Addr&Port	Remote IP address and Port number
State	Connection status

6.9.12 display priority

Function

Using the **display priority** command, you can view the 802.1p priority and DSCP priority that are set in the system.

Format

display priority { **8021p** | **dscp** }

Parameters

Parameter	Description	Value
8021p	Displays the 802.1p priority.	-
dscp	Displays the DSCP priority.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the 802.1p priority and DSCP priority that are set in the system.

The **display priority** command displays information only after the **set priority** command is executed to set the 802.1p priority or DSCP priority.

Example

Set the DSCP priority to 10, and display the DSCP priority set in the system.

```
<HUAWEI> system-view
[HUAWEI] set priority dscp 10
[HUAWEI] quit
<HUAWEI> display priority dscp
 The dscp priority is 10
```

6.9.13 display rawip statistics

Function

The **display rawip statistics** command displays RawIP traffic statistics.

Format

display rawip statistics [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed RawIP traffic statistics based on the ICMP, RSVP, OSPF, and Others protocols.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The statistics about RawIP packets include the number of sent RawIP packets and the number of received RawIP packets.

RSVP, OSPF, and ICMP packets are encapsulated into RawIP packets to be sent. During the ping operation, for example, you can run the **display rawip statistics** command to view the number of RawIP packets sent by the local device to check whether the abnormality on the network is caused by abnormal sending and receiving of RawIP packets.

If you want to diagnose problems and monitor information of specific applications, configure **verbose** in the **display rawip statistics** command to display application-specific RawIP packet statistics. The applications can be ICMP, RSVP, OSPF, and others.

Precautions

The number of packets received by a switch includes the number of forwarded packets, packets sent to the upper layer, and discarded packets.

RawIP traffic statistics are collected based on the well-known protocol number. The protocol number is identified by the protocol field in the IP packet header.

- The protocol number of ICMP statistics is 1.
- The protocol number of OSPF statistics is 89.
- The protocol number of RSVP statistics is 46.
- Statistics about packets with other protocol numbers are collected into the Others field.

Example

View the statistics about RawIP packets.

```
<HUAWEI> display rawip statistics
Received packets:
  dropped packets because the socket buffer is full   : 0
  dropped packets because no matching socket is found : 0

Sent packets:
  dropped packets : 0
```

Table 6-52 Description of the **display rawip statistics** command output

Item	Description
Received packets	Indicates the number of received packets.
dropped packets because the socket buffer is full	Indicates the number of RawIP packets that are discarded because the socket buffer is full.
dropped packets because no matching socket is found	Indicates the number of RawIP packets that are discarded because the socket of the receiver does not match with that of the sender.
Sent packets	Indicates the number of sent packets.
dropped packets	Indicates the number of discarded packets.

6.9.14 display tcp statistics

Function

The **display tcp statistics** command displays TCP traffic statistics.

Format

display tcp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays TCP traffic statistics including different types of received and sent packets. For example, duplicate received packets and packets with checksum errors. In addition, connection-related statistics are displayed, for example, times of accepted connections, the number of retransmitted packets, and the number of keepalive packets.

Most of the preceding statistics are expressed in number of packets, and some of them are expressed in number of bytes.

Example

Display TCP traffic statistics.

```
<HUAWEI> display tcp statistics
Received packets:
     Total: 0
     Total(64bit high-capacity counter): 0
     packets in sequence: 0 (0 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 0 (0 bytes)
     packets of data after window: 0 (0 bytes)
     packets received after close: 0

     ACK packets: 0 (0 bytes)
     duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
    Total: 0
     Total(64bit high-capacity counter): 0
     urgent packets: 0
     control packets: 0 (including 0 RST)
     window probe packets: 0, window update packets: 0
```

```
    data packets: 0 (0 bytes),    data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 0 (0 delayed)

Other information:
    Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
    Keep alive timeout: 0, keep alive probe: 0,     Keep alive timeout, so connections disconnected : 0
    Initiated connections: 0,     accepted connections: 0, established connections: 0
    Closed connections: 0 (    dropped: 0, initiated dropped: 0)
    Packets dropped with MD5 authentication: 0
    Packets permitted with MD5 authentication: 0
    Send Packets permitted with Keychain authentication: 0
    Receive Packets permitted with Keychain authentication: 0
    Receive Packets Dropped with Keychain authentication: 0
```

Table 6-53 Description of the **display tcp statistics** command output

Item	Description
Received packets	Statistics about received packets.
Total	Total number of packets.
Total (64bit high-capacity counter)	Total number of packets, using the 64-bit counter.
packets in sequence (bytes)	Number of bytes in the packets that arrive in order.
window probe packets	Number of window probe packets.
window update packets	Number of window update packets.
checksum error	Number of packets with checksum errors.
offset error	Number of packets with offset errors.
short error	Number of packets whose length is too short.
duplicate packets (bytes)	Number of bytes in the duplicate packets.
partially duplicate packets (bytes)	Number of bytes in partially duplicate packets.
out-of-order packets (bytes)	Number of bytes in the out-of-order packets.
packets of data after window (bytes)	Number of bytes in the packets whose size is greater than the window size.
packets received after close	Number of packets that arrive after a connection is closed.
ACK packets (bytes)	Number of acknowledged packets, in bytes.
duplicate ACK packets	Number of re-acknowledged packets.
too much ACK packets	Number of acknowledged packets with no data sent.

Item	Description
Sent packets	Number of sent packets.
urgent packets	Number of urgent packets.
control packets (RST)	Number of control packets (RST packets).
data packets	Number of data packets.
data packets retransmitted (0 bytes)	Number of bytes in the retransmitted packets.
ACK only packets (delayed)	Number of acknowledged packets that are delayed.
Other information	Other information.
Retransmitted timeout	Timeout interval of the retransmission timer.
connections dropped in retransmitted timeout	Number of connections discarded because the number of retransmission times exceeds the threshold.
Keep alive timeout	Timeout interval of the keepalive timer.
keep alive probe	Number of sent keepalive packets.
Keep alive timeout, so connections disconnected	Number of connections discarded because keepalive probe fails.
Initiated connections	Number of initiated connections.
accepted connections	Number of accepted connections.
established connections	Number of established connections.
Closed connections (dropped, initiated dropped)	Number of closed connections (number of discarded packets after a connection is set up or before a connection is set up).
Packets dropped with MD5 authentication	Number of packets that fail to pass MD5 authentication.
Packets permitted with MD5 authentication	Number of packets that pass MD5 authentication.
Send Packets permitted with Keychain authentication	Number of sent packets that carry keychain options.
Receive Packets permitted with Keychain authentication	Number of received packets that pass keychain authentication.
Receive Packets Dropped with Keychain authentication	Number of received packets that fail to pass keychain authentication.

6.9.15 display tcp status

Function

The **display tcp status** command displays current TCP connection status.

Format

display tcp status [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ip-address*] [**local-port** *local-port-number*] [**remote-ip** *ip-address*] [**remote-port** *remote-port-number*]]

Parameters

Parameter	Description	Value
task-id *task-id*	Displays the TCP connection status of the task with a specified ID.	The value must be an existing task ID.
socket-id *socket-id*	Displays the TCP connection status of the socket with a specified ID.	The value must be an existing socket ID.
local-ip *ip-address*	Displays the TCP connection status of a specified local IP address.	The value is in dotted decimal notation.
local-port *local-port-number*	Displays the TCP connection status of a specified local port ID.	The value must be an existing local port ID.
remote-ip *ip-address*	Displays the TCP connection status a specified remote IP address.	The value is in dotted decimal notation.
remote-port *remote-port-number*	Displays the TCP connection status of a specified remote port ID.	The value must be an existing remote port ID.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The transmission control protocol defined in RFC 793 ensures high reliability of transmission between hosts. TCP provides reliable and connection-oriented services in full duplex mode. Run the **display tcp status** command to monitor the TCP connection status. The following information is displayed.

- ID of the TCP task control block.
- ID of the IPv4 TCP task and socket.
- Local IPv4 address and port ID.
- Remote IPv4 address and port ID.
- ID of the VPN instance to which the TCP connection belongs.
- IPv4 TCP connection status.

You can set filtering rules based on the Task ID, socket ID, IP address and port number of the local device, and IP address and port number of the remote device so that only the information matching the rules is displayed. This prevents unnecessary information from being displayed and helps you locate faults accurately and efficiently.

Precautions

The command output is null if there is no TCP connection.

Example

Display the TCP connection status on the local device.

```
<HUAWEI> display tcp status
TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
0a5d560c 30 /1    0.0.0.0:23            0.0.0.0:0             14849 Listening
```

Display the status of the TCP connection originated from the local IP address 0.0.0.0 and port 23.

```
<HUAWEI> display tcp status local-ip 0.0.0.0 local-port 23
TCPCB    Tid/Soid Local Add:port        Foreign Add:port      VPNID  State
0a5d560c 30 /1    0.0.0.0:23            0.0.0.0:0             14849 Listening
```

Table 6-54 Description of the **display tcp status** command output

Field	Description
TCPCB	ID of the TCP task control block.
Tid/Soid	Task ID and socket ID.
Local Add: port	IP address and port number of the local device. If the value of Local Add is 0.0.0.0, TCP connections of all IP addresses are monitored. If the value of port is 0, the TCP connection of all ports is monitored.

Field	Description
Foreign Add: port	IP address and port number of the remote device. If the value of Foreign Add is 0.0.0.0, the TCP connection of all IP addresses is monitored. If the value of port is 0, TCP connections of all ports are monitored.
VPNID	ID of the VPN instance to which the TCP connection belongs. ● -1: indicates all VPNs. ● 0: indicates the public VPN. ● Other values: indicates the private VPN. The VPNID is defined by users.
State	TCP connection status: ● Closed: indicates that the TCP connection is closed. ● Listening: indicates that the TCP connection is being monitored. ● Syn_Rcvd: indicates that a packet with the SYN flag is received. ● Syn_Sent: indicates that a SYN packet is sent. ● Established: indicates that the TCP connection has been set up. ● Close_Wait: indicates that a user sends a packet with the FIN flag to the server to close the TCP connection in Established state. The server then sends an ACK packet to the user after receiving the packet and enters the Close_Wait state. ● Fin_Wait1: indicates that a user sends a packet with the FIN flag to the server to close the TCP connection and enter this state. ● Fin_Wait2: indicates that a user receives an ACK packet that responds to the sent packet with the FIN flag. ● Time_Wait: indicates that TCP enters this state after the TCP connection is closed. When TCP has been in Time_Wait state two times the lifetime of the longest packets, records about the closed connection are deleted. ● Closing: indicates that the user and server close the TCP connection simultaneously.

6.9.16 display udp statistics

Function

The **display udp statistics** command displays UDP traffic statistics.

Format

display udp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays UDP traffic statistics including different types of received and sent packets. For example, packets with checksum errors. In addition, connection-related statistics are displayed, for example, the number of broadcast packets. The preceding statistics are expressed in number of packets.

Example

Display UDP traffic statistics.

```
<HUAWEI> display udp statistics
Received packets:
    Total: 0
    Total(64bit high-capacity counter): 0
    checksum error: 0
    shorter than header: 0
    data length larger than packet: 0
    unicast(no socket on port): 0
    broadcast/multicast(no socket on port): 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0

Sent packets:
    Total: 0
    Total(64bit high-capacity counter): 0
```

Table 6-55 Description of the **display udp statistics** command output

Item	Description
Received packet: Total Total (64bit high-capacity counter)	Total number of received UDP packets. Total number of received UDP packets (using the 64-bit counter).
checksum error	Number of packets with checksum errors.
shorter than header	Number of packets whose length is shorter than the packet header.

Item	Description
data length larger than packet	Number of packets whose data length is greater than the packet length.
unicast (no socket on port)	Number of unicast packets.
broadcast/multicast (no socket on port)	Number of broadcast and multicast packets.
not delivered, input socket full	Number of packets that are not sent out because the socket buffer is full.
input packets missing pcb cache	Number of sent packets that are not found in the PCB cache.
Sent packets: Total Total (64bit high-capacity counter)	Total number of sent UDP packets. Total number of sent UDP packets (using the 64-bit counter).

6.9.17 drop illegal-dst-ip enable

Function

The **drop illegal-dst-ip enable** command enables the device to discard IP packets with invalid destination IP addresses and record logs.

The **undo drop illegal-dst-ip enable** command disables the device from discarding IP packets with invalid destination IP addresses and recording logs.

By default, a device is disabled from discarding IP packets with invalid destination IP addresses and recording logs.

Format

drop illegal-dst-ip enable

undo drop illegal-dst-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The following three types of IP addresses are invalid destination IP addresses and should not be used on the network:

- IP address with all 0s, that is, 0.0.0.0
- IP addresses with a network ID of 127, that is, 127.0.0.0 to 127.255.255.255
- Class E IP addresses except 255.255.255.255, that is, 240.0.0.0 to 255.255.255.254

After the **drop illegal-dst-ip enable** command is run on a device, the device discards the IP packets destined to invalid IP addresses and reports statistics about the discarded packets through logs. This reduces the device burden and prevents these packets from occupying network bandwidth.

NOTE

- Devices of the following models will discard IP packets destined to 0.0.0.0, 127.0.0.0 to 127.255.255.255, and 240.0.0.0 to 255.255.255.254 only after this function is configured:

  S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S
- Devices of other models discard the IP packet destined to an IP address that does not match any routing entry. Since there is no routing entry matching 0.0.0.0, 127.0.0.0 to 127.255.255.255, or 240.0.0.0 to 255.255.255.254, devices will discard IP packets destined to these IP addresses by default.

Example

Enable the device to discard IP packets with invalid destination IP addresses and record logs.

```
<HUAWEI> system-view
[HUAWEI] drop illegal-dst-ip enable
```

6.9.18 drop illegal-ip disable

Function

The **drop illegal-ip disable** command disables a device from discarding IPv4 and IPv6 packets sourced from the all-zero address.

The **undo drop illegal-ip disable** command enables a device to discard IPv4 and IPv6 packets sourced from the all-zero address.

By default, the function of discarding IPv4 and IPv6 packets sourced from the all-zero address is enabled.

NOTE

The **drop illegal-ip disable** and **undo drop illegal-ip disable** commands are supported only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. The other device models discard IPv4 and IPv6 packets sourced from the all-zero address by default, and this function cannot be disabled on those models.

Format

drop illegal-ip disable

undo drop illegal-ip disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IPv4 and IPv6 packets sourced from the all-zero address are typical attack packets. You can run the **undo drop illegal-ip disable** command to enable a device to discard these packets.

Example

Enable a device to discard IPv4 and IPv6 packets sourced from the all-zero address.

```
<HUAWEI> system-view
[HUAWEI] undo drop illegal-ip disable
```

6.9.19 icmp blackhole unreachable send

Function

The **icmp blackhole unreachable send** command enables the switch to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

The **undo icmp blackhole unreachable send** command disables the switch from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

By default, the switch is disabled from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

Format

icmp blackhole unreachable send

undo icmp blackhole unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If static IPv4 blackhole routes are configured on the switch configured with the user access and authentication function, when a user goes offline, only the IPv4 blackhole route corresponding to the user's address segment exists on the switch. When a tracert packet matches the IPv4 blackhole route, the switch discards the packet. As a result, an initiator cannot detect that the user has gone offline.

After you run the **icmp blackhole unreachable send** command, the switch sends a Destination Unreachable ICMP packet to an initiator, notifying the initiator that the user has gone offline if a user goes offline and a tracert packet matches the IPv4 blackhole route.

Example

Enable the switch to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

```
<HUAWEI> system-view
[HUAWEI] icmp blackhole unreachable send
```

6.9.20 icmp host-unreachable send

Function

The **icmp host-unreachable send** command enables the switch to send ICMP Host Unreachable packets.

The **undo icmp host-unreachable send** command disables the switch from sending ICMP Host Unreachable packets.

By default, the function of sending ICMP Host Unreachable packets is enabled.

Format

icmp host-unreachable send

undo icmp host-unreachable send

Parameters

None

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

After you run the **undo icmp host-unreachable send** command, the device does not send ICMP Host Unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

Precautions

The **icmp host-unreachable send** command can be run in the system view or interface view.

- After the function of sending ICMP Host Unreachable packets is disabled in the system view, all interfaces do not send ICMP Host Unreachable packets. Even if the function is enabled on an interface, the interface does not send ICMP Host Unreachable packets.
- After the function of sending ICMP Host Unreachable packets is enabled in the system view, all interfaces send ICMP Host Unreachable packets because the function is enabled on all interfaces by default. You can run the **undo icmp host-unreachable send** command in interface view to disable the function on a specified interface.

If the function of sending ICMP Host Unreachable packets is disabled, the switch does not send ICMP Host Unreachable packets in any situations.

This command needs to be configured on the inbound interface of ICMP packets in the interface view.

Example

Enable the switch to send ICMP Host Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp host-unreachable send
```

Enable VLANIF100 to send ICMP Host Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp host-unreachable send
```

Enable GE0/0/1 to send ICMP Host Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp host-unreachable send
```

6.9.21 icmp port-unreachable send

Function

The **icmp port-unreachable send** command enables the device to send ICMP Port Unreachable packets.

The **undo icmp port-unreachable send** command disables the device from sending ICMP Port Unreachable packets.

By default, the device sends ICMP Port Unreachable packets.

Format

icmp port-unreachable send

undo icmp port-unreachable send

Parameters

None

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

After you run the **undo icmp port-unreachable send** command, the device does not send ICMP Port Unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

Precautions

The **icmp port-unreachable send** command can be run in the system view or interface view.

- After the function of sending ICMP Port Unreachable packets is disabled in the system view, all interfaces do not send ICMP Port Unreachable packets. Even if the function is enabled on an interface, the interface does not send ICMP Port Unreachable packets.
- After the function of sending ICMP Port Unreachable packets is enabled in the system view, all interfaces send ICMP Port Unreachable packets because the function is enabled on all interfaces by default. You can run the **undo icmp port-unreachable send** command in interface view to disable the function on a specified interface.

If the function of sending ICMP Port Unreachable packets is disabled, the switch does not send ICMP Port Unreachable packets in any situations.

Example

Enable the device to send ICMP Port Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp port-unreachable send
```

Enable the device to send ICMP Port Unreachable packets on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp port-unreachable send
```

Enable the device to send ICMP Port Unreachable packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp port-unreachable send
```

6.9.22 icmp protocol-unreachable send

Function

The **icmp protocol-unreachable send** command enables the function of sending ICMP Protocol Unreachable packets.

The **undo icmp protocol-unreachable send** command disables the function of sending ICMP Protocol Unreachable packets.

By default, the function of sending ICMP Protocol Unreachable packets is enabled.

Format

icmp protocol-unreachable send

undo icmp protocol-unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

After you run the **icmp protocol-unreachable send** command, the device does not send ICMP Protocol Unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

Example

Enable the function of sending ICMP Protocol Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp protocol-unreachable send
```

6.9.23 icmp receive

Function

The **icmp receive** command enables a switch to receive ICMP packets with the local IP address as the destination IP address.

The **undo icmp receive** command disables a switch from receiving ICMP packets with the local IP address as the destination IP address.

By default, switches are enabled to receive ICMP packets with the local IP address as the destination IP address.

Format

icmp { **type** *icmp-type* **code** *icmp-code* | **name** *icmp-name* | **all** } **receive**

undo icmp { **type** *icmp-type* **code** *icmp-code* | **name** *icmp-name* | **all** } **receive**

Parameters

Parameter	Description	Value
type *icmp-type*	Specifies the type number of an ICMP packet.	The value is an integer ranging from 0 to 255.
code *icmp-code*	Specifies the code of an ICMP packet.	The value is an integer ranging from 0 to 255.

Parameter	Description	Value
name *icmp-name*	Specifies the name of an ICMP packet.	The value is a string of case-insensitive characters, with spaces not supported. The value can be any of the following: ● echo ● echo-reply ● fragmentneed-dfset ● host-redirect ● host-tos-redirect ● host-unreachable ● information-reply ● information-request ● net-redirect ● net-tos-redirect ● net-unreachable ● parameter-problem ● port-unreachable ● protocol-unreachable ● reassembly-timeout ● source-quench ● source-route-failed ● timestamp-reply ● timestamp-request ● ttl-exceeded
all	Specifies all ICMP packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- On secure networks, the device can normally receive ICMP packets. In the case of heavy traffic on the network, if hosts or ports are frequently unreachable, the device will receive a large number of ICMP packets, which causes heavier traffic burdens over the network and degrades the performance of the device.

- On insecure networks, network attackers often use ICMP error packets to probe on the internal structure of the network.

To improve network performance or enhance security, run the **undo icmp receive** command to disable switches from receiving ICMP packets with the local IP address as the destination IP address.

After network performance improves, you can run the **icmp receive** command to enable switches to receive ICMP packets with the local IP address as the destination IP address.

Precautions

After the **undo icmp receive** command is run, the device no longer process ICMP packets of a certain type, causing the host to fail to ping the device.

Example

Disable the switch from receiving ICMP packets with the local IP address as the destination IP address whose type number is 3 and code number is 1.

```
<HUAWEI> system-view
[HUAWEI] undo icmp type 3 code 1 receive
```

6.9.24 icmp redirect send

Function

The **icmp redirect send** command enables the switch to send ICMP redirect packets.

The **undo icmp redirect send** command disables the switch from sending ICMP redirect packets.

The function of sending ICMP Redirect packets is enabled.

Format

icmp redirect send

undo icmp redirect send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

ICMP Redirect packets are a type of ICMP error packets.

When a host starts, there may be only one default route to the gateway in its routing table. In the following situations, the device functions as a gateway to send an ICMP Redirect packet to the source host, requesting the host to select another next hop address for subsequent packet forwarding:

- The interface that receives the data packet is the same as the interface used to forward the packet.
- The device needs to forward a received packet. After looking up the routing table, the device finds that the next hop IP address is on the same network segment with the destination address of the packet.

After the device sends ICMP Redirect packets to the host that has only a few routes, the host can enrich the routing table and find out the optimal route.

The ICMP error packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP error packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Redirect function increases the number of routes in the host's routing table. When many routes are added, the host performance will be degraded.

You need to decide whether to enable ICMP Redirect packet sending according to network situation.

Precautions

The command is used on the interface that receives ICMP packets.

Example

Enable VLANIF100 to send ICMP Redirect packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp redirect send
```

Enable GE0/0/1 to send ICMP Redirect packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp redirect send
```

6.9.25 icmp time-exceed

Function

The **icmp time-exceed** command specifies the format of ICMP Time Exceeded packets.

The **undo icmp time-exceed** command restores the default format of ICMP Time Exceeded packets.

By default, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

icmp time-exceed { **extension** { **compliant** | **non-compliant** } | **classic** }

undo icmp time-exceed

Parameters

Parameter	Description	Value
extension	Indicates that ICMP Time Exceeded packets carry extension headers.	-
compliant	Indicates that ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.	-
non-compliant	Indicates that ICMP Time Exceeded packets carry extension headers in non-compliant mode and original datagrams are of fixed length.	-
classic	Indicates that ICMP Time Exceeded packets do not carry extension headers.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When using the **tracert** command to check the network connectivity, you can run the **icmp time-exceed** command to specify the format of ICMP Time Exceeded packets.

- When the **icmp time-exceed** command carry the parameter **extension compliant**, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length. ICMP Time Exceeded packets carry as many original datagrams as possible. Lengths of original datagrams carried in ICMP Time Exceeded packets are recorded in ICMP headers.
- When the **icmp time-exceed** command carry the parameter **extension non-compliant**, ICMP Time Exceeded packets carry extension headers in non-compliant mode and original datagrams are of fixed length. If the length of original datagrams is less than 128 bytes, the system automatically fills the length to 128 bytes.
- When the **icmp time-exceed** command carry the parameter **classic**, ICMP Time Exceeded packets do not carry extension headers.

Example

Configure ICMP Time Exceeded packets to carry extension headers in compliant mode.

```
<HUAWEI> system-view
[HUAWEI] icmp time-exceed extension compliant
```

6.9.26 icmp ttl-exceeded drop

Function

The **icmp ttl-exceeded drop** command enables the device to discard the ICMP packets whose TTL values are 1.

The **undo icmp ttl-exceeded drop** command disables the device from discarding the ICMP packets whose TTL values are 1.

By default, the function of discarding ICMP packets with TTL values of 1 is disabled on the device.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

icmp ttl-exceeded drop { **slot** *slot-id* | **all** }

undo icmp ttl-exceeded drop { **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Indicates the slot ID.	The value is determined based on the device configuration.
all	Indicates all the devices. This parameter is used when you need to enable all the devices to discard or disable all the devices from discarding the ICMP packets whose TTL values are 1.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TTL is a field in an IP packet that limits the lifespan of the IP packet on the network. The TTL value is set by the sender, and is reduced by 1 every time the packet passes a device. If a forwarding device receives an IP packet of which the TTL is 0 and the destination address is not the local address, the device discards this packet and returns an ICMP packet to the sender.

ICMP packets are encapsulated into IP packets. When receiving an ICMP packet of which the destination address is not the local address and the TTL value is 1, the device discards the packet and returns an ICMP Time Exceeded.

When receiving a packet of which the TTL value is 1, the switch sends the packet to the CPU. The **tracert** function implements hop-by-hop detection using the packets with TTL value 1. If an attacker sends a large number of IP packets with TTL value 1 to a target device, the CPU of the target device is busy handling these IP packets and returns ICMP Destination Unreachable packets. Therefore, the CPU usage becomes high.

If a switch is configured to discard the ICMP packets with TTL value 1, the pressure on the switch can be reduced and network attacks can be prevented.

Precautions

After the function is enabled on the device, the **tracert** command does not take effect.

Example

Enable the device to discard the ICMP packets whose TTL values are 1.

```
<HUAWEI> system-view
[HUAWEI] icmp ttl-exceeded drop slot 0
```

6.9.27 icmp ttl-exceeded send

Function

The **icmp ttl-exceeded send** command enables an interface to send ICMP Time Exceeded packets.

The **undo icmp ttl-exceeded send** command disables an interface from sending ICMP Time Exceeded packets.

By default, an interface is enabled to send ICMP Time Exceeded packets.

Format

icmp ttl-exceeded send

undo icmp ttl-exceeded send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If the destination address of a received IP packet is not the local address and the TTL value is 1, a timeout error occurs. In this situation, the device discards the packet and returns an ICMP Time Exceeded packet to the source.

When replying with an ICMP Time Exceeded packet, an interface adds its IP address as the source IP address in the ICMP Time Exceeded packet, exposing the interface itself to attackers. In addition, after being attacked, the interface replies with numerous ICMP Time Exceeded packets, consuming CPU resources and degrading system performance. To resolve these problems, run the **undo icmp ttl-exceeded send** command to disable the interface from replying with ICMP Time Exceeded packets.

Example

Enable VLANIF100 to send ICMP Time Exceeded packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp ttl-exceeded send
```

Enable GE0/0/1 to send ICMP Time Exceeded packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp ttl-exceeded send
```

6.9.28 icmp unreachable drop

Function

The **icmp unreachable drop** command enables the function of discarding ICMP Destination Unreachable packets.

The **undo icmp unreachable drop** command disables the function of discarding the ICMP Destination Unreachable packets.

By default, the function of discarding ICMP Destination Unreachable packets is disabled.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

icmp unreachable drop

undo icmp unreachable drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

The switch sends ICMP Destination Unreachable packets to the CPU for processing. When a large number of such packets are received, the CPU may be overloaded. To reduce the number of ICMP packets on the network, you can enable the switch to discard ICMP Destination Unreachable packets. After the configuration, the workload on the switch is reduced and malicious attacks can be prevented.

Example

Enable the function of discarding ICMP Destination Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp unreachable drop
```

6.9.29 icmp with-options drop

Function

The **icmp with-options drop** command enables the device to discard ICMP packets that carry options.

The **undo icmp with-options drop** command disables the device from discarding ICMP packets that carry options.

By default, the function of discarding ICMP packets with TTL values of 1 is disabled on the device.

Format

icmp with-options drop { **slot** *slot-id* | **all** }

undo icmp with-options drop { **slot** *slot-id* | **all** }

NOTE

Only the S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
slot *slot-id*	The value is an integer. It must be the slot ID of the device that is inserted into the chassis.	The value is determined based on the device configuration.
all	Indicates all the stacking devices. This parameter is used when you need to enable all the devices to discard or disable all the devices from discarding the ICMP packets that carry options.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the **ping -r** command is run to detect network connectivity, the IP packet is forwarded by Layer 3 routing devices. Every Layer 3 device fills its own IP address into the option field of the IP packet. When the IP packet reaches the destination, the ICMP Echo Reply packet should contain the IP addresses of all passing devices, including the devices on the forward and return paths. When the ping program receives the reply packet, it can display the IP addresses of all passing Layer 3 devices.

If the length of IP packet encapsulating the ICMP packet exceeds the interface MTU, this IP packet is fragmented. Only the IP header of the first fragment includes the option field. The fragment carrying the option field is sent to the protocol stack and processed by the CPU.

When malicious attacks are initiated using ICMP packets, the device needs to process a large number of fragments carrying the option field, so the forwarding performance of the device degrades. To reduce impact on the forwarding performance and prevent ICMP packet attacks, you can enable the device to discard the ICMP fragments carrying option fields.

Example

Enable the device to discard the ICMP packets that carry options.

```
<HUAWEI> system-view
[HUAWEI] icmp with-options drop slot 0
```

6.9.30 icmp-reply fast

Function

The **icmp-reply fast** command enables the fast ICMP reply function.

The **undo icmp-reply fast** command disables the fast ICMP reply function.

By default, the fast ICMP reply function is enabled.

Format

icmp-reply fast

undo icmp-reply fast

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ping program is used to check network connectivity. If two hosts cannot ping each other, they cannot set up a connection. The ping program uses the ICMP protocol. It encapsulates ICMP Echo Request packets into IP packets, and sends the packets to the destination host. The destination host returns an ICMP Echo Reply packet to the source host. If the source host receives a reply within a certain period, the source host considers that the destination host is reachable.

In normal situations, after an interface receives an ICMP Echo Request packet, this packet is sent to the protocol stack and handled by the CPU.

After fast ICMP reply is enabled, if an interface receives an ICMP Echo Request packet of which the destination address is the local address, the packet is not sent to the protocol stack for handing by the CPU, but handled by the physical interface. This improves forwarding performance of the device.

Precautions

The fast ICMP reply function is not supported for fragmented packets, packets with IP options, and MPLS-encapsulated packets.

On the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, fast ICMP reply is not supported for packets whose TTL is 1.

A switch does not support fragmentation of the ICMP Echo Reply packets processed based on the fast ICMP reply mechanism to be sent to the remote end. The packets will not be discarded even if their length is greater than the MTU of the outbound interface.

For the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-S, S6735-S, S6720-EI, S6720S-EI:

- The fast ICMP reply function does not take effect on VBDIF interfaces.
- When a routed main interface (supporting Layer 2 and Layer 3 mode switching) is bound to a VPN instance, the fast ICMP reply function does not take effect on the interface.
- When a sub-interface is bound to a VPN instance, the fast ICMP reply function does not take effect on the interface.
- After VLAN mapping is configured, the VLANIF interface corresponding to the mapped VLAN does not support the fast ICMP reply function.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, after fast ICMP reply is enabled, the ping detection cannot be blocked by the blacklist. This is because after the fast ICMP reply function is enabled, the ICMP Echo Request packets received on an interface of the device are not sent to the protocol stack or processed by the CPU. Instead, the interface directly processes the packets.

Example

Enable the fast ICMP reply function.

```
<HUAWEI> system-view
[HUAWEI] icmp-reply fast
```

6.9.31 ip error-packet-check disable

Function

The **ip error-packet-check disable** command disables the IP packet checking function.

The **undo ip error-packet-check disable** command enables the IP packet checking function.

By default, the IP packet checking function is enabled.

NOTE

Only following model switches support this function:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S

Format

ip error-packet-check disable

undo ip error-packet-check disable

Parameters

None

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the link type of an interface is QinQ or the VLAN mapping or VLAN stacking function is configured on the interface, the system checks IP packets so that the device cannot transparently transmit IP error packets. In addition, during Layer 2 forwarding, devices cannot transparently transmit packets with the same source and destination IP addresses. To enable the device to transparently transmit IP error packets, you can run the **ip error-packet-check disable** command to disable the IP packet checking function.

Precautions

When the IP packet checking function is disabled, the IP subnet-based VLAN assignment, policy-based VLAN assignment, and IPv6 over IPv4 tunnel functions do not take effect. Therefore, confirm your action before disabling this function.

Example

Disable the IP packet checking function on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip error-packet-check disable
```

6.9.32 ip forward-broadcast

Function

Using the **ip forward-broadcast** command, you can enable an interface to forward directed broadcast packets.

Using the **undo ip forward-broadcast** command, you can disable an interface from forwarding directed broadcast packets.

By default, disable the interface from forwarding directed broadcast packets.

Format

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999. - The number of a basic ACL ranges from 2000 to 2999. - The number of an advanced ACL ranges from 3000 to 3999.

Views

VE sub-interface view, VBDIF interface view, VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Directed broadcast packets are sent to a specified network. In the destination IP address of a directed broadcast packet, the network number is that of the specified network and the host number is all 1s.

Hackers use directed broadcast packets to attack networks, which threatens the network security. Therefore, directed broadcast packets are isolated by Layer 3 switches in normal cases. However, in some scenarios, the device needs to receive or forward these directed broadcast packets. For example, when Wake on LAN (WOL) is configured on a PC, the command can be run to enable the interface to forward directed broadcast packets. (WOL enables a PC in dormancy or shutdown state to wake up from dormancy state to running state or turn from shutdown state to power-on state through the instruction from the peer of the network.)

The device can also be enabled to receive and forward a certain type of directed broadcast packets based on ACLs. For example, if the basic ACL is used, run the **acl (system view)** and **rule (basic ACL view)** commands to define the directed broadcast packets to be received and forwarded as **permit**, and then run the **ip forward-broadcast** command to bind this ACL.

Only broadcast packets that match the permit action defined in the ACL are forwarded. Broadcast packets that match the deny action defined in the ACL or do not match any ACL rules are not forwarded.

Precautions

By default, the device identifies directed broadcast packets as malformed packets, and intercepts and discards them because the attack defense function of malformed packets is enabled on the device. In this case, the interface on the device cannot forward the directed broadcast packets.

To solve this problem, use either of the following methods:

- Run the **anti-attack abnormal disable** command to disable the attack defense function of malformed packets. However, after this command is configured, other malformed packets will not be intercepted and discarded, which brings certain security risks. Use this command with caution.
- Run the **anti-attack disable** command to disable all attack defense functions. However, after this command is configured, not only malformed packets but also fragmented, tcp-syn, udp-flood, and icmp-flood attack packets will not be intercepted and discarded, which brings certain security risks. Use this command with caution.

This command does not apply to VPN scenarios, IP address unnumbered scenarios, and scenarios of conflicts between host routes and subnet broadcast routes due to network segment overlapping.

Example

Enable VLANIF100 to forward directed broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip forward-broadcast
```

Enable GE0/0/1 to forward directed broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip forward-broadcast
```

6.9.33 ip forwarding converge normal

Function

The **ip forwarding converge normal** command disables the device to perform Layer 2 forwarding for IP traffic during ring network switchover.

The **undo ip forwarding converge** command enables the device from performing Layer 2 forwarding for IP traffic during ring network switchover.

By default, the device is enabled from performing Layer 2 forwarding for IP traffic during ring network switchover.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ip forwarding converge normal

undo ip forwarding converge

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device deployed with the ring network protocols (STP, RSTP, MSTP, SEP, ERPS, RRPP, VBST, and Smart Link) performs link switchover due to a link fault, the ARP entries need to be learned again. This deteriorates the Layer 3 convergence performance of IP traffic. If the device is enabled to perform Layer 2 forwarding for IP traffic during the switchover, the convergence performance can be improved. By default, the device is enabled from performing Layer 2 forwarding for IP traffic during ring network switchover.

Precautions

After the device is enabled to perform Layer 2 forwarding for IP traffic, it will forward the IP traffic in broadcast mode during ring network switchover. Therefore, the IP traffic increases within a short time.

Example

Disable the device from performing Layer 2 forwarding for IP traffic during ring network switchover.

```
<HUAWEI> system-view
[HUAWEI] ip forwarding converge normal
```

6.9.34 ip forwarding disable

Function

The **ip forwarding disable** command disables IPv4 Layer 3 unicast forwarding on a switch.

The **undo ip forwarding disable** command enables IPv4 Layer 3 unicast forwarding on a switch.

By default, IPv4 Layer 3 unicast forwarding is enabled on a switch.

Format

ip forwarding disable

undo ip forwarding disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to disable IPv4 Layer 3 unicast forwarding on a switch.

After IPv4 Layer 3 unicast forwarding is disabled on a switch, the IPv4 routing function becomes ineffective on the switch, and the switch cannot forward Layer 3 packets based on the IPv4 routing table and FIB table.

Precautions

Running this command on a switch disables IPv4 Layer 3 packet forwarding at the hardware layer and CPU software layer.

Example

Disable IPv4 Layer 3 unicast forwarding on the switch.

```
<HUAWEI> system-view
[HUAWEI] ip forwarding disable
Warning: This operation will close IPv4 forwarding function and affect IPv4 traffic forwarding. Continue?
[Y/N]:y
```

6.9.35 ip ttl-expired drop

Function

The **ip ttl-expired drop** command enables the switch to discard IP packets with expired TTL.

The **undo ip ttl-expired drop** command disables the switch from discarding IP packets with expired TTL.

By default, the function of discarding IP packets with expired TTL is disabled.

Format

ip ttl-expired drop

undo ip ttl-expired drop

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TTL is a field in an IP packet that limits the lifespan of the IP packet on the network. The TTL value is set by the sender, and is reduced by 1 every time the packet passes a device. If a forwarding device receives an IP packet of which the TTL is 0 and the destination address is not the local address, the device discards this packet.

If a device receives many IP packets with TTL value 1, the device may undergo an attack. Run the **ip ttl-expired drop** command to enable the device to discard the IP packets with expired TTL. Then the device discards the packets with TTL value 1, but does not send them to the CPU.

Precautions

After the **ip ttl-expired drop** command is run, some packets that have the TTL value 1 but need to be processed by the CPU are also discarded. Therefore, after the attack is removed, run the **undo ip ttl-expired drop** command to disable the device from discarding the IP packets with expired TTL.

Example

Enable the switch to discard IP packets with expired TTL.

```
<HUAWEI> system-view
[HUAWEI] ip ttl-expired drop
```

6.9.36 ip verify source-address

Function

The **ip verify source-address** command enables an interface to check validity of source IP addresses of received packets.

The **undo ip verify source-address** command disables an interface from checking validity of source IP addresses of received packets.

By default, an interface does not check validity of source IP addresses of received packets.

Format

ip verify source-address

undo ip verify source-address

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Configuring source IP address verification enables an interface to check validity of source IP addresses of received packets. Packets with invalid addresses are discarded, which improves the network security.

The following IP addresses are illegal source addresses:

- Addresses with all 0s or 1s
- Multicast addresses (class D addresses)
- Class E addresses
- Loopback addresses that are not generated on local hosts (in 127.x.x.x format)
- Broadcast addresses of classes A, B, and C
- Subnet broadcast addresses that are on the same network segment as the address of the inbound interface

The interface only checks validity of source IP addresses of the packets that need to be forwarded to the CPU, and does not check validity of source IP addresses of the packets that will be directly forwarded according to the FIB table.

If the mask in the IP address of the received packet is of 31 bits, the receiver considers it as a valid source address without checking the broadcast address of the subnet.

Run the **display this** command in the interface view to check configuration of checking validity of source IP addresses.

Example

Enable VLANIF100 to check validity of source IP addresses of received packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip verify source-address
```

Enable GE0/0/1 to check validity of source IP addresses of received packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip verify source-address
```

6.9.37 ipv4 destination-unreachable drop

Function

The **ipv4 destination-unreachable drop** command enables the function of discarding IP packets that match no routing entry.

The **undo ipv4 destination-unreachable drop** command disables the function of discarding IP packets that match no routing entry.

By default, the function of discarding IP packets that match no routing entry is enabled.

Format

ipv4 destination-unreachable drop

undo ipv4 destination-unreachable drop

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the switch receives an IP packet that matches no routing entry in the local routing table, it sends the packet to the CPU. If a lot of IP packets match no routing entry because of an attack or incorrect network configuration, the CPU is busy. To prevent this problem, run the **ipv4 destination-unreachable drop** command to configure the switch to discard these packets.

Precautions

If you run the **ipv4 destination-unreachable drop** command, the switch does not respond to ICMP error packets when a route fails to match the routing policies. To enable the switch to respond to these ICMP packets, you need to run the **undo ipv4 destination-unreachable drop** command.

On the S6720-EI, S6735-S, and S6720S-EI, when both the **ipv4 destination-unreachable drop** command and the traffic policy command are run, both the drop action and the redirection action take effect. The ICMP redirection packets are discarded because the drop action has a higher priority than the redirection action. This leads to a redirection failure for ICMP packets. To make the redirection action for ICMP packets effective, run the **undo ipv4 destination-unreachable drop** command to disable the drop action. However, disabling the drop action will degrade the attack defense performance of the system. You must configure the two actions properly according to the network requirements.

For the S6720-EI, S6735-S and S6720S-EI, if the resource allocation mode is set to **enhanced-ipv4** or **ipv4-ipv6 6:1** using the **assign resource-mode** command, the **ipv4 destination-unreachable drop** command does not take effect.

Example

Enable the function of discarding IP packets that match no routing entry.

```
<HUAWEI> system-view
[HUAWEI] ipv4 destination-unreachable drop
```

6.9.38 ipv4 fragment enable

Function

The **ipv4 fragment enable** command enables fragmentation for outgoing forwarding-plain IP packets.

The **undo ipv4 fragment enable** command disables fragmentation for outgoing forwarding-plain IP packets.

By default, fragmentation for outgoing forwarding-plain IP packets is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv4 fragment enable

undo ipv4 fragment enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, only packets on the control plane can be fragmented according to the MTU on an interface. Packets on the forwarding plane can be forwarded normally without limited by the MTU. When the remote device or intermediate forwarding device receives IP packets, if it checks the packet length and discards packets whose length is longer than the MTU on the interface, network communication is interrupted. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, you can run the **ipv4 fragment enable** command to enable fragmentation for outgoing forwarding-plane IP packets so that packets on the forwarding plane are fragmented based on the MTU on the interface.

Precautions

Before configuring the **ipv4 fragment enable** command, set a proper MTU. If the MTU is small, there may be many fragments of IP packets, causing the Layer 3 forwarding performance of IP packets to deteriorate.

Example

Enable fragmentation for outgoing IP packets.

```
<HUAWEI> system-view
[HUAWEI] ipv4 fragment enable
```

6.9.39 ipv6 destination-unreachable drop

Function

The **ipv6 destination-unreachable drop** command enables the switch to discard the packets that do not match IPv6 routing entries.

The **undo ipv6 destination-unreachable drop** command disables the switch from discarding the packets that do not match IPv6 routing entries.

By default, the device discards the packets that do not match IPv6 routing entries.

Format

ipv6 destination-unreachable drop

undo ipv6 destination-unreachable drop

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the device sends the IPv6 packets that do not match routing entries to the CPU for processing. If many IPv6 packets do not match routing entries because of an attack or improper network configurations, the CPU is busy. To prevent this situation, run the **ipv6 destination-unreachable drop** command to configure the switch to discard these packets.

Precautions

If the **ipv6 destination-unreachable drop** command is used and a traffic policy with the redirect action is configured, both the drop action and the redirect action take effect. Because the drop action has a higher priority than the redirect action, ICMPv6 Redirect packets are discarded. This leads to a redirection failure. To make the redirect action take effect, run the **undo ipv6 destination-unreachable drop** command to disable the drop action. However, disabling the drop action will degrade the attack defense performance of the system. You must configure the two actions properly according to network requirements.

After the **ipv6 destination-unreachable drop** command is used, the switch does not respond to the ICMPv6 Error packets caused when IPv6 packets do not match routing entries until the drop action is disabled.

For the S6720-EI, S6735-S and S6720S-EI, if the resource allocation mode is set to **enhanced-ipv4** or **ipv4-ipv6 6:1** using the **assign resource-mode** command, the **ipv6 destination-unreachable drop** command does not take effect.

Example

Configure the switch to discard the packets that do not match IPv6 routing entries.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 destination-unreachable drop
```

6.9.40 ipv6 with-options drop

Function

The **ipv6 with-options drop** command enables the switch to discard IPv6 packets destined for the switch and containing specified extension headers.

The **undo ipv6 with-options drop** command disables the switch from discarding IPv6 packets destined for the switch and containing specified extension headers.

By default, the switch is disabled from discarding IPv6 packets destined for the switch and containing specified extension headers.

Format

ipv6 with-options drop

undo ipv6 with-options drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IPv6 packets may contain the following extension headers:

- Routing header: An IPv6 source node uses this header to specify the intermediate nodes that a packet must pass through on the way to its destination.
- Fragment header: The length of IPv6 packets to be forwarded cannot exceed the maximum transmission unit (MTU) specified on interfaces of devices along the forwarding path. When the packet length exceeds the MTU, the packet needs to be fragmented. In IPv6, the fragment header is used by an IPv6 source node to send a packet larger than the MTU. Fragmentation in IPv6 is performed only by source nodes, not by intermediate nodes along the path a packet traverses.
- Destination options header: This header carries information that only the destination node of a packet processes.

Malicious attacks can be initiated using these IPv6 extension headers. For example, the routing header can be used to specify a node that packets must pass through. The fragment header can be used to set the MTU to a small value on the source node, leading to a large number of data fragments. The destination options header can specify destination devices to process IPv6 packets. If attackers send a large number of such IPv6 packets to the switch, the switch is busy handling these packets, degrading the forwarding performance. To prevent malicious network attacks and reduce impact on the forwarding performance, you can enable the switch to discard IPv6 packets destined for the switch and containing specified extension headers.

Example

Enable the switch to discard IPv6 packets destined for the switch and containing specified extension headers.

```
<HUAWEI> system-view
[HUAWEI] ipv6 with-options drop
```

6.9.41 load-balance (system view)

Function

The **load-balance** command configures a load balancing mode for public IP packet forwarding.

The **undo load-balance** command restores the load balancing mode for public IP packet forwarding to the default configuration.

By default, flow-based load balancing is used for public IP packet forwarding

Format

load-balance { **flow** | **packet** } [**all** | **slot** *slot-id*]

undo load-balance packet [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
flow	Indicates flow-based load balancing.	-
packet	Indicates packet-based load balancing.	-
all	In a stack, the configuration is applied to all devices in the stack. On a stand-alone switch, the configuration is applied to the local device.	-
slot *slot-id*	Indicates that the configuration is applied to the device with the specified stack ID.	The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

If flow-based load balancing is used, the hash algorithm is used to calculate a value for selecting a link to forward packets. The value is calculated based on the protocol type, source IP address, destination IP address, source port number, and destination port number.

If packet-based load balancing is used, packets are forwarded through different links. Packet-based load balancing can be implemented only for packets forwarded by the CPU such as protocol packets.

Precautions

The **load-balance** command takes effect on packets delivered by the local device and IP/MPLS packets processed by the CPU.

Example

Configure packet-based load balancing for public IP packet forwarding.

```
<HUAWEI> system-view
[HUAWEI] load-balance packet
```

6.9.42 load-balance vpn

Function

The **load-balance vpn** command configures a load balancing mode for private IP packet forwarding.

The **undo load-balance vpn** command restores the load balancing mode for private IP packet forwarding to the default configuration.

By default, packet-based load balancing is used for private IP packet forwarding

Format

load-balance { **flow** | **packet** } **vpn**

undo load-balance flow vpn

Parameters

Parameter	Description	Value
flow	Indicates flow-based load balancing.	-
packet	Indicates packet-based load balancing.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

If flow-based load balancing is used, the hash algorithm is used to calculate a value for selecting a link to forward packets. The value is calculated based on the protocol type, source IP address, destination IP address, source port number, and destination port number.

If packet-based load balancing is used, packets are forwarded through different links. Packet-based load balancing can be implemented only for packets forwarded by the CPU such as protocol packets.

Precautions

The **load-balance vpn** command takes effect on packets delivered by the local device and IP/MPLS packets processed by the CPU.

Example

Configure flow-based load balancing for private IP packet forwarding.

```
<HUAWEI> system-view
[HUAWEI] load-balance flow vpn
```

6.9.43 management-port icmp-reply fast disable

Function

The **management-port icmp-reply fast disable** command disables the fast ICMP reply function on the management Ethernet port.

The **undo management-port icmp-reply fast disable** command enables the fast ICMP reply function on the management Ethernet port.

By default, the fast ICMP reply function is enabled on the management Ethernet port.

NOTE

The following models support this command: S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S5735-S, S5735-S-I, S5735S-H, S5735-L, S5736-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-S, S6720S-EI.

Format

management-port icmp-reply fast disable

undo management-port icmp-reply fast disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ping program is used to check network connectivity. If two hosts cannot ping each other, they cannot set up a connection. The ping program uses the ICMP protocol. It encapsulates ICMP Echo Request packets into IP packets, and sends the packets to the destination host. The destination host returns an ICMP Echo Reply packet to the source host. If the source host receives a reply within a certain period, the source host considers that the destination host is reachable.

In normal situations, after the management Ethernet port of a device receives an ICMP Echo Request packet, this packet is sent to the protocol stack and handled by the CPU.

After fast ICMP reply is enabled, if the management Ethernet port receives an ICMP Echo Request packet of which the destination address is the local address, the packet is not sent to the protocol stack for handing by the CPU, but handled by the management Ethernet port. This improves forwarding performance of the device.

Precautions

The fast ICMP reply function is not supported for fragmented packets, packets with IP options, and MPLS-encapsulated packets.

Example

Enable the fast ICMP reply function on the management Ethernet port.

```
<HUAWEI> system-view
[HUAWEI] undo management-port icmp-reply fast disable
```

6.9.44 reset ip socket monitor

Function

The **reset ip socket monitor** command clears information in a socket monitor.

Format

reset ip socket monitor [**task-id** *task-id* **socket-id** *socket-id*]

Parameters

Parameter	Description	Value
task-id *task-id*	Clears information about the task with a specified ID in the socket monitor.	The value must be an existing task ID.
socket-id *socket-id*	Clears information about the socket with a specified ID in the socket monitor.	The value must be an existing socket ID.

Views

User view

Default Level

3: Management level

Usage Guidelines

A socket monitor monitors and records each connection. A RawLink monitor also monitors interfaces. The socket monitor records specific protocol events that occur during operations and logs information in the disk space.

You can specify the task ID and socket ID for deleting information about the socket monitor that meets the filtering condition.

Example

Clear information in a socket monitor.

```
<HUAWEI> reset ip socket monitor
```

6.9.45 reset ip socket pktsort

Function

The **reset ip socket pktsort** command resets statistics on the dual receive buffer of the socket.

Format

reset ip socket pktsort task-id *task-id* **socket-id** *socket-id*

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a task.	The value must be an existing task ID.
socket-id *socket-id*	Specifies the ID of a socket.	The value must be an existing socket ID.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics on the dual receive buffer of the socket and restarts the count. Therefore, confirm your action before running the command.

Example

Reset statistics on the dual receive buffer of the socket with the task ID of 2 and the socket ID of 6.

```
<HUAWEI> reset ip socket pktsort task-id 2 socket-id 6
```

6.9.46 reset ip statistics

Function

The **reset ip statistics** command clears IP traffic statistics on an interface.

Format

reset ip statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and ID of an interface. If no optional parameter is specified, all the IP statistics will be deleted.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect IP traffic statistics on an interface in a period of time, you must clear the existing traffic statistics and collect IP statistics after a period of time. Run the **display ip statistics** command to display information.

If no parameter is specified, the command clears IP traffic statistics on all boards.

Example

Clear IP statistics on all interfaces.

```
<HUAWEI> reset ip statistics
```

Clear IP statistics on VLANIF10.

```
<HUAWEI> reset ip statistics interface vlanif 10
```

6.9.47 reset rawip statistics

Function

The **reset rawip statistics** command clears RawIP packet statistics.

Format

reset rawip statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You need to clear the existing statistics about RawIP packets before using the **display rawip statistics** command to view the statistics about RawIP packets in a specified period.

The **reset rawip statistics** command clears RawIP packet statistics. Confirm your action before running this command.

Example

Clear RawIP packet statistics.

```
<HUAWEI> reset rawip statistics
```

6.9.48 reset tcp statistics

Function

The **reset tcp statistics** command deletes TCP traffic statistics.

Format

reset tcp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete TCP packet statistics, run the **reset tcp statistics** command. To view TCP packet statistics, run the **display tcp statistics** [**verbose**] command. The command output contains the number of sent packets, the number of received packets, or the number of TCP packets for each protocol (verbose). You can run the **reset tcp statistics** command to delete existing statistics and then run the **display tcp statistics** command to collect statistics. The statistics help you check whether TCP packet counts are correct or help you diagnose faults.

Precautions

The **reset tcp statistics** command deletes TCP traffic statistics. Confirm your action before running this command.

Example

Delete TCP traffic statistics.

```
<HUAWEI> reset tcp statistics
```

6.9.49 reset udp statistics

Function

The **reset udp statistics** command deletes UDP traffic statistics.

Format

reset udp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete UDP packet statistics, run the **reset udp statistics** command. To view UDP packet statistics, run the **display udp statistics** [**verbose**] command. The command output contains the number of sent packets, the number of received packets, or the number of UDP packets for each protocol (verbose). You can run the **reset udp statistics** command to delete existing statistics and then run the **display udp statistics** command to collect statistics. The statistics help you check whether UDP packet counts are correct or help you diagnose faults.

Precautions

The **reset udp statistics** command deletes UDP traffic statistics. Confirm your action before running this command.

Example

Delete UDP traffic statistics.

```
<HUAWEI> reset udp statistics
```

6.9.50 set priority

Function

The **set priority** command sets the 802.1p priority or DSCP priority of packets.

The **undo set priority** command cancels the settings of the 802.1p priority or DSCP priority of packets.

By default, the 802.1p priority or DSCP priority of packets is not set.

Format

set priority 8021p *8021p-number*

undo set priority 8021p

set priority dscp *dscp-number* [**if-match acl** *acl-number*]

undo set priority dscp [**if-match acl** *acl-number*]

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **if-match acl** *acl-number*.

Parameters

Parameter	Description	Value
8021p *8021p-number*	Specifies the 802.1p priority of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-number*	Specifies the DSCP priority of packets. This parameter takes effect only for IPv4 packets.	The value is an integer that ranges from 0 to 63.
if-match acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **set priority** command to set the 802.1p priority or DSCP priority of packets sent by the switch.

To change the DSCP priority of protocol packets that meet specified characteristics and are sent by the switch, you can use an ACL to match these packets.

Precautions

This command takes effect only for IPv4 but not for IPv6.

If the packet priority has been specified in the protocol, the **set priority 8021p** command does not take effect.

If you use ACLs to match packets whose DSCP priority is to be changed, you can specify up to eight ACLs, each of which supports a maximum of 32 rules. The following fields can be matched:

- ICMP packets: source IP address, destination IP address, protocol number, icmp-type, icmp-code, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range
- TCP packets: source IP address, destination IP address, protocol number, source port, destination port, tcp-flag, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range
- UDP packets: source IP address, destination IP address, protocol number, source port, destination port, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range
- Other protocol packets: source IP address, destination IP address, protocol number, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range

The switch cannot use ACL-based matching to change the DSCP priority of the following protocol packets:

- Protocol packets that are not sent from the protocol stack, such as fast ICMP reply packets and NetStream packets
- Protocol packets whose priority can be configured using a command (for example, you can run the **tos** command to set the priority of NQA packets)

Example

Set the DSCP priority to 10.

```
<HUAWEI> system-view
[HUAWEI] set priority dscp 10
```

6.9.51 tcp min-mss

Function

The **tcp min-mss** command sets the minimum value of maximum segment size (MSS) for a TCP connection.

The **undo tcp min-mss** command restores the default minimum value of the MSS for a TCP connection.

The default minimum MSS value for a TCP connection is 216 bytes.

Format

tcp min-mss *mss-value*

undo tcp min-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the minimum MSS value for a TCP connection.	The value ranges from 32 bytes to 1500 bytes. By default, the value is 216 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. The TCP client on a network may send a request packet for establishing a TCP connection carrying a small MSS value. For example, the MSS value is 1. After the TCP server receives the request packet carrying the MSS value, the TCP connection is established. The TCP client then may send large numbers of requests to the server by an application, causing the TCP server to generate large numbers of reply packets. This may burden the TCP server or network, causing denial of service (DoS) attacks. To resolve this problem, run the **tcp min-mss** command to set the minimum MSS value for a TCP connection. This configuration prevents a server from receiving packets carrying a small MSS value.

Precautions

The minimum MSS value configured using this command is not the negotiation parameter value carried in the MSS option. The negotiation parameter value carried in the MSS option of packets sent by the local device is calculated based on the MTU value.

The minimum MSS value configured using the **tcp min-mss** command must be less than the maximum MSS value configured using the **tcp max-mss** command.

If the **tcp min-mss** command is run more than once in the same view, the latest configuration overrides the previous one.

Configure the parameters under the guidance of the technical personnel.

Example

Set the minimum MSS value for a TCP connection to 512 bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp min-mss 512
```

6.9.52 tcp max-mss

Function

The **tcp max-mss** command configures the maximum Maximum Segment Size (MSS) value for a TCP connection.

The **undo tcp max-mss** command deletes the maximum MSS value of a TCP connection.

By default, the maximum MSS value is not configured for TCP connections.

Format

tcp max-mss *mss-value*

undo tcp max-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the maximum MSS value for a TCP connection.	The value is an integer ranging from 32 to 9600, in bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. This length is the TCP payload length, excluding that of the TCP header. If the path MTU is unavailable on one end of a TCP connection, this end cannot adjust the TCP packet size based on the MTU. As a result, this end may send TCP packets that are longer than the MTUs on intermediate devices, which will discard these packets. To prevent this problem, run the **tcp max-mss** command on either end of a TCP connection to set the maximum MSS value of TCP packets. Then the MSS value negotiated by both ends will not exceed this maximum MSS value, and accordingly TCP packets sent from both ends will not be longer than this maximum MSS value and can travel through the intermediate network.

Precautions

The maximum MSS value configured using the **tcp max-mss** command must be greater than the minimum MSS value configured using the **tcp min-mss** command.

Example

Set the maximum MSS value for a TCP connection to 1024 bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp max-mss 1024
```

6.9.53 tcp send-trap bind-port

Function

The **tcp send-trap bind-port** command configures a TCP port number list.

The **undo tcp send-trap bind-port** command restores the default TCP port number list.

By default, no TCP port number list is configured.

Format

tcp send-trap bind-port { *port-number* } &<1-10>

undo tcp send-trap bind-port { { *port-number* } &<1-10> | **all** }

Parameters

Parameter	Description	Value
port-number	Specifies a TCP port number.	The value is an integer in the range from 1 to 65535.
all	Indicates all TCP port numbers in a TCP port number list.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to pay special attention to some TCP port numbers, you can run this command to add them to a TCP port number list. If port numbers in a TCP port number list are bound to services or an attempt is made to bind such numbers to services, the device sends an event alarm so that you can monitor the TCP port numbers.

Precautions

When the **undo tcp send-trap bind-port all** command is run, the system prompts you for confirmation.

Example

Configure a TCP port number list.

```
<HUAWEI> system-view
[HUAWEI] tcp send-trap bind-port 20 21 23 80
```

6.9.54 tcp timer fin-timeout

Function

The **tcp timer fin-timeout** command configures the value of the TCP FIN-Wait timer.

The **undo tcp timer fin-timeout** command restores the default value of the TCP FIN-Wait timer.

By default, the value of the TCP FIN-Wait timer is 675s.

Format

tcp timer fin-timeout *interval*

undo tcp timer fin-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP FIN-Wait timer.	The value is an integer that ranges from 76 to 3600, in seconds. The default value is 675s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a TCP connection changes from FIN_WAIT_1 to FIN_WAIT_2, the TCP FIN-Wait timer is started. If no response packet is received after the TCP FIN-Wait timer expires, the TCP connection is closed.

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the value of the TCP FIN-Wait timer to 400s.

```
<HUAWEI> system-view
[HUAWEI] tcp timer fin-timeout 400
```

6.9.55 tcp timer syn-timeout

Function

The **tcp timer syn-timeout** command configures the value of the TCP SYN-Wait timer.

The **undo tcp timer syn-timeout** command restores the default value of the TCP SYN-Wait timer.

By default, the value of the TCP SYN-Wait timer is 75s.

Format

tcp timer syn-timeout *interval*

undo tcp timer syn-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP SYN-Wait timer.	The value is an integer ranging from 2 to 600, in seconds. The default value is 75s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an SYN packet is sent, the TCP SYN-Wait timer is started. If no response packet is received after the TCP SYN-Wait timer expires, the TCP connection is closed.

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the value of the TCP SYN-Wait timer to 100s.

```
<HUAWEI> system-view
[HUAWEI] tcp timer syn-timeout 100
```

6.9.56 tcp window

Function

The **tcp window** command configures the size of the receive or send buffer of a connection-oriented socket.

The **undo tcp window** command restores the default size of the receive or send buffer of a connection-oriented socket.

By default, the size of the receive or send buffer of a connection-oriented socket is 8k bytes.

Format

tcp window *window-size*

undo tcp window

Parameters

Parameter	Description	Value
window-size	Specifies the size of the receive or send buffer of a connection-oriented socket.	The value is an integer that ranges from 1 to 32, in k bytes. The default value is 8k bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the size of the receive or send buffer of a connection-oriented socket to 3K bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp window 3
```

6.10 Basic IPv6 Configuration Commands

6.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

6.10.2 display default-parameter tcp6

Function

The **display default-parameter tcp6** command displays the default values of all configurable parameters on the TCP6 module.

Format

display default-parameter tcp6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter tcp6** command displays the default values of all configurable parameters on the TCP6 module.

Example

Display the default values of all configurable parameters on the TCP6 module.

```
<HUAWEI> display default-parameter tcp6
---------------------------------
  SYN Timeout Value(sec) : 75
  FIN Timeout Value(sec) : 600
  Window Size(KBytes)    : 8
---------------------------------
```

Table 6-56 Description of the display default-parameter tcp6 command output

Item	Description
SYN Timeout Value(sec)	TCP SYN-Wait timer value. To configure this parameter, run the **tcp ipv6 timer syn-timeout** command.
FIN Timeout Value(sec)	TCP FIN-Wait timer value. To configure this parameter, run the **tcp ipv6 timer fin-timeout** command.
Window Size(KBytes)	TCP6 slide window size. To configure this parameter, run the **tcp ipv6 window** command.

6.10.3 display icmpv6 statistics

Function

The **display icmpv6 statistics** command displays ICMPv6 traffic statistics.

Format

display icmpv6 statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the ICMPv6 traffic statistics on the specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display icmpv6 statistics** command to view ICMPv6 packet statistics, including statistics about received and sent ICMPv6 error packets and statistics about four types of ICMPv6 packets (RS, RA, NS, and NA packets) used in the neighbor discovery mechanism.

When you ping an IPv6 address from a device, run the **display icmpv6 statistics** command on the device to check whether the total number of sent and received packets is correct.

Precautions

The total number of packets received by the device includes the number of packets forwarded, number of packets delivered to upper-layer network devices, and number of packets discarded.

Example

Display ICMPv6 traffic statistics on the device.

```
<HUAWEI> display icmpv6 statistics interface vlanif 100
ICMPv6 protocol:

 Sent packets:
  Total              : 2
  Unreached          : 0          Prohibited          : 0
  Hop count exceeded : 0          Parameter problem   : 0
  Too big            : 0          Echoed              : 0
  Echo replied       : 0          Router solicit      : 0
  Router advert      : 0          Neighbor solicit    : 1
  Neighbor advert    : 1          Redirected          : 0
  Rate limited       : 0          Cert path advert    : 0

 Received packets:
  Total              : 0          Format error        : 0
  Checksum error     : 0          Too short           : 0
  Bad code           : 0          Bad length          : 0
  Unknown info type  : 0          Unknown error type  : 0
  Unreached          : 0          Prohibited          : 0
  Hop count exceeded : 0          Parameter problem   : 0
  Too big            : 0          Echoed              : 0
  Echo replied       : 0          Router solicit      : 0
  Router advert      : 0          Neighbor solicit    : 0
  Neighbor advert    : 0          Redirected          : 0
  Rate limited       : 0          Cert path solicit   : 0
```

Table 6-57 Description of the display icmpv6 statistics command output

Item	Description
ICMPv6 protocol	ICMPv6 packet statistics.
Sent packets	Statistics about sent ICMPv6 packets.
Total	Total number of sent packets.
Unreached	Total number of sent ICMPv6 Destination Unreachable packets.
Prohibited	Total number of sent ICMPv6 Administratively Prohibited Unreachable packets.
Hop count exceeded	Total number of sent ICMPv6 packets whose hops exceed the limit.
Parameter problem	Total number of sent ICMPv6 Parameter Problem packets.

Item	Description
Too big	Total number of sent ICMPv6 Packet Too Big packets.
Echoed	Total number of sent ICMPv6 Echo Request packets.
Echo replied	Total number of sent ICMPv6 Echo Reply packets.
Router solicit	Total number of sent Router Solicitation (RS) packets.
Router advert	Total number of sent Router Advertisement (RA) packets.
Neighbor solicit	Total number of sent Neighbor Solicitation (NS) packets.
Neighbor advert	Total number of sent Neighbor Advertisement (NA) packets.
Redirected	Total number of sent ICMPv6 Redirect packets.
Rate limited	Total number of ICMPv6 packets that fail to be sent because of the rate limit.
Cert path advert	Total number of sent CPS packets. This parameter is not supported currently and displayed as 0.
Received packets	Statistics about received ICMPv6 packets.
Total	Total number of received packets.
Format error	Total number of received ICMPv6 packets with format errors.
Checksum error	Total number of received ICMPv6 packets with checksum errors.
Too short	Total number of received ICMPv6 packets that are too short.
Bad code	Total number of received ICMPv6 packets with code errors.
Bad length	Total number of received ICMPv6 packets with packet length errors.
Unknown info type	Total number of received ICMPv6 packets with an unknown information type.
Unknown error type	Total number of received ICMPv6 packets with an unknown error type.
Unreached	Total number of received ICMPv6 Destination Unreachable packets.

Item	Description
Prohibited	Total number of received ICMPv6 Administratively Prohibited Unreachable packets.
Hop count exceeded	Total number of received ICMPv6 packets whose hops exceed the limit.
Parameter problem	Total number of received ICMPv6 Parameter Problem packets.
Too big	Total number of received ICMPv6 packets that are oversized.
Echoed	Total number of received ICMPv6 Echo Request packets.
Echo replied	Total number of received ICMPv6 Echo Reply packets.
Router solicit	Total number of received RS packets.
Router advert	Total number of received RA packets.
Neighbor solicit	Total number of received NS packets.
Neighbor advert	Total number of received NA packets.
Redirected	Total number of received ICMPv6 Redirect packets.
Rate limited	Total number of ICMPv6 packets that fail to be received because of the rate limit.
Cert path solicit	Total number of received CPA packets. This parameter is not supported currently and displayed as 0.

6.10.4 display ipv6 attack-source overlapping-fragment

Function

The **display ipv6 attack-source overlapping-fragment** displays source information about overlapping fragment attacks.

Format

display ipv6 attack-source overlapping-fragment

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device suffers from overlapping fragment attacks, the administrator can run this command to view source information about attack packets. Source information includes the source and destination IP addresses of the packets, interface receiving the packets, source VLAN, source CE VLAN, and VPN to which the packets belongs. The administrator can take proper actions on the attack source.

Example

Display source information about overlapping fragment attacks.

```
<HUAWEI> display ipv6 attack-source overlapping-fragment
Attack-source overlapping fragment table:

------------------------------------------------------------------------------
  Source IP           : FC00::1
  Destination IP      : FC00::2
  Interface name      : Vlanif2
  VPN name            :
  VLAN                : 0                          CEVLAN: 0
  Attacked time       : 2011-09-29 01:01:28
------------------------------------------------------------------------------

Total: 1
```

Table 6-58 Description of the display ipv6 attack-source overlapping-fragment command output

Item	Description
Source IP	Source IPv6 address of an overlapping fragment attack packet.
Destination IP	Destination IPv6 address of the overlapping fragment attack packet.
Interface name	Interface that receives the overlapping fragment attack packet.
VPN name	Name of the VPN to which the overlapping fragment attack packet belongs.
VLAN	VLAN to which the overlapping fragment attack packet belongs.
CEVLAN	CE VLAN to which the overlapping fragment attack packet belongs.
Attacked time	Duration of the overlapping fragment attack.
Total	Number of pieces of source information about overlapping fragment attacks.

6.10.5 display ipv6 interface

Function

The **display ipv6 interface** command displays IPv6 information on an interface.

Format

display ipv6 interface [*interface-type interface-number* | **brief**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays IPv6 information on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If no interface is specified, IPv6 information on all interfaces configured with IPv6 addresses is displayed.	-
brief	Displays brief information about the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, ensure that the interface is configured with an IPv6 address. If no IPv6 address is assigned to the interface, no interface information is displayed.

Example

Display IPv6 information on VLANIF 2.

```
<HUAWEI> display ipv6 interface vlanif 2
Vlanif2 current state : DOWN
IPv6 protocol current state : DOWN
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00 [TENTATIVE]
  Global unicast address(es):
    FC00::1, subnet is FC00::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
```

```
  FF02::1:FF04:5D00
  FF02::2
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
ND stale time is 1200 seconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisement max interval 600 seconds, min interval 200 seconds
ND router advertisements live for 1800 seconds
ND router advertisements hop-limit 64
ND default router preference medium
Hosts use stateless autoconfig for addresses
```

Table 6-59 Description of the **display ipv6 interface** command output

Item	Description
Vlanif2 current state	Current physical status of VLANIF 2. ● UP: enabled ● DOWN: disabled
IPv6 protocol current state	Current protocol status of the interface. ● UP: enabled ● DOWN: disabled
IPv6 is enabled	IPv6 is enabled.
link-local address	Link-local address on the interface. After an IPv6 address is configured on the interface, the system automatically assigns a link-local address for the interface. To manually configure a link-local address for an interface, run the **ipv6 address link-local** command.
Global unicast address(es)	Global unicast address configured on the interface. To configure a global unicast address for an interface, run the **ipv6 address** command.
Joined group address(es)	Addresses of all multicast groups that the interface joins.
TENTATIVE	When the interface is in DOWN state, the IPv6 address is TENTATIVE.
MTU	MTU of the interface. To configure the MTU for an interface, run the **ipv6 mtu** command.
ND DAD is enabled	NS packets are sent when the system performs Duplicate Address Detection (DAD).

Item	Description
number of DAD attempts	Number of times duplicate address detection is performed.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Retransmission interval of NS packets.
ND stale time	Aging time of ND entries in STALE state.
ND advertised reachable time	Reachable time of NA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND advertised retransmit interval	Retransmission interval of NA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisement max interval 600 seconds, min interval 200 seconds	Maximum and minimum interval of RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisements live for	Router lifetime in RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisements hop-limit	Hop limit of RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND default router preference	Default route priority in RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses by means of stateless auto-configuration. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.

Display brief IPv6 information about all interfaces.

```
<HUAWEI> display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                 Physical             Protocol
LoopBack0                   up                   up(s)
[IPv6 Address] Unassigned
Vlanif2                   down                 down
[IPv6 Address] 2001:db8:1::1 [TENTATIVE]
```

Table 6-60 Description of the **display ipv6 interface brief** command output

Item	Description
*down	Reason that interface is physically Down. **administratively down** indicates that the network administrator has executed the **shutdown (interface view)** command on the interface.
(l)	This interface is enabled with the loopback function.
(s)	This interface is enabled with the spoofing function.
Interface	Name of an interface.
Physical	Physical status of the interface.
Protocol	Link layer protocol status of the interface.
IPv6 Address	IPv6 address configured for the interface. If no IPv6 address is assigned to the interface, this field displays Unassigned.
TENTATIVE	When the interface is in Down state, the IPv6 address is TENTATIVE.

6.10.6 display ipv6 interface tunnel

Function

The **display ipv6 interface tunnel** command displays IPv6 information on a tunnel interface.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display ipv6 interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Displays the tunnel interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ipv6 interface tunnel** command displays IPv6 information on a tunnel interface.

Example

Display IPv6 information on Tunnel1.

```
<HUAWEI> display ipv6 interface tunnel 1
Tunnel1 current state : UP
IPv6 protocol current state : DOWN
IPv6 is enabled, link-local address is FE80::2E0:9FF:FE87:7890 [TENTATIVE]
  Global unicast address(es):
    FC00:1::1, subnet is FC00:1::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF87:7890
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

Table 6-61 Description of the **display ipv6 interface tunnel** command output

Item	Description
Tunnel1 current state	Current status of the tunnel interface: ● UP: enabled ● DOWN: disabled When working properly, an IPv6 over IPv4 tunnel is in Up state.

Item	Description
IPv6 protocol current state	Current status of the link layer protocol: - UP: enabled - DOWN: disabled When working properly, an IPv6 over IPv4 tunnel is in Up state.
IPv6 is enabled	IPv6 is enabled.
link-local address	Link-local address on the interface. After an IPv6 address is configured on the interface, the system automatically assigns a link-local address for the interface. To manually configure a link-local address for an interface, run the **ipv6 address link-local** command.
Global unicast address(es)	IPv6 global unicast address. To configure an IPv6 global unicast address, run the **ipv6 address** command.
Joined group address(es)	Addresses of multicast groups that the interface joins.
TENTATIVE	When the interface is in DOWN state, the IPv6 address is TENTATIVE.
MTU	MTU of the interface. To configure the MTU of the interface, run the **ipv6 mtu** command.
ND reachable time	Reachable time of ND packets.
ND retransmit interval	Interval for retransmitting ND packets.
ND stale time	Time period for the neighbor to keep the STALE state.
ND advertised reachable time	Reachable time of NA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND advertised retransmit interval	Retransmission interval of NA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.

Item	Description
ND router advertisement max interval 600 seconds, min interval 200 seconds	Maximum and minimum interval of RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisements live for	Router lifetime in RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisements hop-limit	Hop limit of RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND default router preference	Default route priority in RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses by means of stateless auto-configuration. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.

6.10.7 display ipv6 nd track

Function

The **display ipv6 nd track** command displays information about the changes in the outbound interfaces of ND entries on VLANIF interfaces.

Format

display ipv6 nd track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the outbound interfaces of ND entries learned by a VLANIF interface change, traffic is intermittently interrupted. To keep track of the outbound interface changes, run the **display ipv6 nd track** command to display the change time.

Prerequisites

A VLANIF interface has ND entries, and their outbound interfaces have changed.

Precautions

After the **display ipv6 nd track** command is run, the following types of changes are displayed:

- The outbound interface of a dynamic ND entry learned by the VLANIF interface changes to another interface.
- The outbound interface of a static ND entry configured on the VLANIF interface is changed to another interface.
- A dynamic or static ND entry on the VLANIF interface is deleted.

The following types of changes are not displayed:

- ND entries on a non-VLANIF interface change.
- A new ND entry is learned.
- A new static ND entry is configured.

Example

Display information about the changes in the outbound interfaces of ND entries on VLANIF interfaces.

```
<HUAWEI> display ipv6 nd track
Operate Flag : Modify
IPv6-Address : 2001:db8::1
MAC-Address  : 00e0-fc12-3456
VLAN         : 1000
Old-Port     : GE0/0/1
New-Port     : GE0/0/11
System-Time  : 2017-10-19 12:10:12

Operate Flag : Modify
IPv6-Address : 2001:db8:2::2
MAC-Address  : 00e0-fc12-3456
VLAN         : 1000
Old-Port     : GE0/0/1
New-Port     : GE0/0/11
System-Time  : 2017-09-19 12:13:12

Operate Flag : Delete
IPv6-Address : 2001:db8:3::3
MAC-Address  : 00e0-fc12-3455
VLAN         : 300
Old-Port     : GE0/0/2
New-Port     :
System-Time  : 2017-08-19 12:12:12
```

Table 6-62 Description of the **display ipv6 nd track** command output

Item	Description
Operate Flag	Operation flag. - Modify: indicates that the outbound interface changes. - Delete: indicates that the ND entry is deleted.
IPv6-Address	IPv6 address of the ND entry.
MAC-Address	MAC address of the ND entry.
VLAN	VLAN ID of the VLANIF interface.
Old-Port	Original outbound interface of the ND entry.
New-Port	New outbound interface of the ND entry.
System-Time	Time when the outbound interface changed.

6.10.8 display ipv6 neighbors

Function

The **display ipv6 neighbors** command displays information about neighbor entries.

Format

display ipv6 neighbors [*ipv6-address* | [**vid** *vid*] *interface-type interface-number* | **vpn-instance** *vpn-instance-name*]

display ipv6 neighbors [*interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **cevid** *cevid*.

Parameters

Parameter	Description	Value
ipv6-address	Displays neighbor entries of a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
vid *vid*	Displays neighbor entries of a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays neighbor entries on a specified interface.	-
vpn-instance *vpn-instance-name*	Displays neighbor entries of a specified VPN instance.	The value must be an existing VPN instance name.
cevid *cevid*	Specifies the inner tag.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ipv6 neighbors** command displays information about dynamic and static ND entries. The information helps you:

- Check whether the local routing device has learned MAC addresses from neighbors.
- Check the neighbor status of the local routing device, including neighbor unreachable, neighbor reachable, or unknown.

You can run one of the following commands as required:

- To view neighbor entries based on the neighbor IPv6 address, run the **display ipv6 neighbors** [*ipv6-address*] command.
- To view neighbor entries based on the neighbor interface number, run the **display ipv6 neighbors** *interface-type interface-number* command.

  To view neighbor entries on a VLANIF interface, run the **display ipv6 neighbors** [[**vid** *vlan-id*] *interface-type interface-number*] command or the **display ipv6 neighbors** [*interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]] command.
- To view the neighbor entry on a sub-interface for QinQ VLAN tag termination or Dot1q VLAN tag termination, run the **display ipv6 neighbors** [*interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]] command.

If no parameter is specified, the **display ipv6 neighbors** command displays all neighbor entries.

Example

Display neighbor entries of IPv6 address FC00::2.

```
<HUAWEI> display ipv6 neighbors fc00::2
------------------------------------------------------------------------------
IPv6 Address : FC00::2
Link-layer   : 00e0-fc89-fe6e          State : STALE
Interface    : GE0/0/1                 Age   : 00h19m12s
VLAN         : -                     CEVLAN: -
VPN name     :                         Is Router: FALSE
------------------------------------------------------------------------------
Total: 1        Dynamic: 1          Static: 0
```

Display neighbor entries on a specified interface.

```
<HUAWEI> display ipv6 neighbors vlanif 11
------------------------------------------------------------------------------
IPv6 Address : FC00::3
Link-layer   : 0001-0001-0012                   State : INCMP
Interface    : GE0/0/1                          Age   : 00h19m12s
VLAN         : 11                             CEVLAN: -
VPN name     : v1                               Is Router: TRUE

------------------------------------------------------------------------------
Total: 1       Dynamic: 0       Static: 1
```

View the neighbor entries on the QinQ termination sub-interface GE0/0/1.1.

```
<HUAWEI> display ipv6 neighbors gigabitethernet 0/0/1.1 vid 1 cevid 1
------------------------------------------------------------------------------
IPv6 Address : 2001:db8::2
Link-layer   : 00e0-3602-8100                   State : REACH
Interface    : GE0/0/1.1                        Age   : -
VLAN         : 1                              CEVLAN: 1
VPN name     :                                Is Router: TRUE
------------------------------------------------------------------------------
Total: 1       Dynamic: 0       Static: 1
```

Table 6-63 Description of the **display ipv6 neighbors** command output

Item	Description
IPv6 Address	IPv6 address of a neighbor.
Link-layer	Link layer address (MAC address) of the neighbor.

Item	Description
State	Status of a neighbor entry: - INCMP: indicates that the neighbor is unreachable. When the address is being resolved, the link layer address of the neighbor is not detected. If resolution succeeds, the neighbor entry is in REACH state. - REACH: indicates that the neighbor is reachable within a specified period. By default, the neighbor is reachable within 30s. If the period expires and the entry remains unused, the neighbor entry is in STALE state. - STALE: indicates that whether the neighbor is reachable is unknown. The entry remains unused within a specified period. By default, the neighbor is reachable within 30s. A device does not detect neighbor reachability unless it needs to send packets to a neighbor. - DELAY: indicates that whether the neighbor is reachable is unknown. A device has sent a packet to a neighbor. If the device does not receive any response from the neighbor within the specified period, the neighbor entry is in PROBE state. - PROBE: indicates that whether the neighbor is reachable is unknown. A device has sent a packet to a neighbor to detect whether the neighbor is reachable. If the device receives a response from the neighbor within a specified period, the neighbor entry is in REACH state. Otherwise, the neighbor entry is in INCMP state.
Interface	Name of the interface to which the neighbor entry belongs.
Age	Aging time of the neighbor entry: - The aging time of static entries is displayed as "-". - The aging time of dynamic entries is the time that the reachable state lasts. "#" indicates non-reachable (only for dynamic entries).
VLAN	ID of the VLAN to which the neighbor belongs.
CEVLAN	ID of the CEVLAN to which a neighbor belongs. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter.
VPN name	Name of a VPN instance to which the neighbor belongs.

Item	Description
Is Router	Whether an NA packet carries the R flag: - If the NA packet carries the R flag, "TRUE" is displayed. In this case, the neighbor is a routing device. - If the NA packet carries no R flag, "FALSE" is displayed. In this case, the neighbor may be a PC or a routing device that sends an NA packet carrying no R flag.
Total	Number of total neighbor entries.
Dynamic	Number of dynamic neighbor entries.
Static	Number of static neighbor entries.

6.10.9 display ipv6 pathmtu

Function

The **display ipv6 pathmtu** command displays information about PMTU entries.

Format

display ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { *ipv6-address* | **all** | **dynamic** | **static** }

Parameters

Parameter	Description	Value
ipv6-address	Displays PMTU entries that match a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
all	Displays all PMTU entries.	-
dynamic	Displays all dynamic PMTU entries.	-
static	Displays all static PMTU entries.	-
vpn-instance *vpn-instance-name*	Displays PMTU entries of a specified IPv6 VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the MTU on the outbound interface of an intermediate routing device is smaller than the MTU of the source host, the path MTU (PMTU) discovery mechanism determines the maximum size of packets that can be transmitted on a path.

The **display ipv6 pathmtu** command displays information about dynamic and static PMTU entries. The device then fragments packets into a size smaller than the PMTU and forwards the fragmented packets.

Precautions

If no PMTU is set using the **ipv6 pathmtu** command, no static PMTU entry is displayed after the **display ipv6 pathmtu** command is run.

If a static PMTU entry is displayed, the remaining lifetime displays "-".

Example

Display all PMTU entries.

```
<HUAWEI> display ipv6 pathmtu all
IPv6 Destination Address               ZoneID PathMTU LifeTime(M) Type    FF
FC00::2                                0      1500    -           Static  NO
-------------------------------------------------------------------------------
Total: 1      Dynamic: 0     Static: 1
```

Table 6-64 Description of the display ipv6 pathmtu command output

Item	Description
IPv6 Destination Address	Destination IPv6 address.
ZoneID	Zone ID.
PathMTU	PMTU of an IPv6 address. To configure the PMTU for an IPv6 address, run the **ipv6 pathmtu** command.
LifeTime(M)	Remaining lifetime, in minutes. The update interval is 1 minute. This field displays "-" for static entries.

Item	Description
Type	Type of the PMTU entry: - Dynamic: dynamic entries - Static: static entries (configured through CLI)
FF	Fragmentation flag: - YES: Packets are fragmented, and a fragment header is added to a packet. - NO: Packets are not fragmented.
Total	Total number of PMTU entries.
Dynamic	Number of dynamic PMTU entries.
Static	Number of static PMTU entries.

6.10.10 display ipv6 socket

Function

The **display ipv6 socket** command displays information about IPv6 sockets.

Format

display ipv6 socket [**socktype** *socket-type* | **task-id** *task-id* **socket-id** *socket-id*]

Parameters

Parameter	Description	Value
socktype *socket-type*	Specifies the type of a socket. The value can be: - 1: indicates SOCK_STREAM, corresponding to the TCP-based socket. - 2: indicates SOCK_DGRAM, corresponding to the UDP-based socket. - 3: indicates SOCK_RAW, corresponding to the RawIP-based socket.	The value is an integer that ranges from 1 to 3.
socket-id *socket-id*	Specifies the socket ID.	The value is an integer that ranges from 1 to 131072.

Parameter	Description	Value
task-id *task-id*	Specifies the task ID.	The value is an integer and the range depends on the task configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate a fault, you can use this command to view detailed information about sockets of all types or a specified type.

Precautions

If there is no socket information, no information is displayed.

If no parameter is specified, this command displays information about all types of sockets.

Example

Display information about all types of sockets.

```
<HUAWEI> display ipv6 socket
SOCK_STREAM:
Task = VTYD(102), socketid = 3, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_KEEPALIVE SO_LINGER SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC

Task = VTYD(102), socketid = 2, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = TRAP(105), socketid = 2, Proto = 17,
LA = ::->49152, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_ZONEID(-1),
socket state = SS_PRIV

Task = AGT6(106), socketid = 1, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 17941, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC
```

```
Task = RDS(123), socketid = 2, Proto = 17,
LA = ::->1812, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_ZONEID(-1),
socket state = SS_PRIV SS_RECALL

SOCK_DGRAM:
SOCK_RAW:
```

Display information about the socket with socket type 1.

```
<HUAWEI> display ipv6 socket socktype 1
SOCK_STREAM:
Task = VTYD(102), socketid = 3, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_KEEPALIVE SO_LINGER SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC

Task = VTYD(102), socketid = 2, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC
```

Table 6-65 Description of the **display ipv6 socket** command output

Item	Description
SOCK_STREAM	One type of socket. Sockets are classified into the following types: ● SOCK_STREAM ● SOCK_DGRAM ● SOCK_RAW
Task = VTYD	Type and ID of the task that invokes the socket. For example, **Task = VTYD(48)** shows that the task named VTYD uses the socket, with task ID 48.
socketid	Socket ID.
Proto	Protocol ID.
LA	Local address and local port number.
FA	Remote address and remote port number.
sndbuf	Upper limit of the send buffer, in bytes.
rcvbuf	Upper limit of the receive buffer, in bytes.
sb_cc	Total number of sent bytes.
rb_cc	Total number of received bytes.
socket option	Socket option that has been set.
socket state	Socket status.

6.10.11 display ipv6 statistics

Function

The **display ipv6 statistics** command displays IPv6 traffic statistics.

Format

display ipv6 statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays IPv6 traffic statistics on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipv6 statistics** command to view statistics on received and sent IPv6 packets.

During packet transmission, if the source node has fragmented packets, you can run this command to view the total number of IPv6 packets that are successfully fragmented and the total number of fragmented packets that have been sent, and then check whether the number of fragmented packets received by the destination node is correct.

Precautions

The total number of packets received by the device includes the number of forwarded packets, number of packets delivered by the routing device to the upper layer, and number of discarded packets.

Example

Display IPv6 traffic statistics on the device.

```
<HUAWEI> display ipv6 statistics
IPv6 Protocol:

 Sent packets:
  Total             : 0
  Local sent out     : 0         Forwarded          : 0
  Raw packets        : 0         Discarded          : 0
  Fragmented         : 0         Fragments          : 0
  Fragments failed   : 0         Multicast          : 0

 Received packets:
  Total             : 0         Local host         : 0
  Hop count exceeded : 0         Header error       : 0
  Too big            : 0         Routing failed     : 0
  Address error      : 0         Protocol error     : 0
  Truncated          : 0         Option error       : 0
  Fragments          : 0         Reassembled        : 0
  Reassembly timeout : 0         Multicast          : 0
  Fragments overlap  : 0
  Extension header:
    Hop-by-hop options   : 0              Mobility header       : 0
    Destination options  : 0              Routing header        : 0
    Fragment header      : 0              Authentication header : 0
    Encapsulation header : 0              No header             : 0
    TLV length error     : 0              Header length error   : 0
    Unknown header type  : 0              Unknown TLV type      : 0
```

Table 6-66 Description of the **display ipv6 statistics** command output

Item	Description
Sent packets	Statistics about sent packets.
Total	Total number of sent packets.
Local sent out	Total number of packets sent by the local device.
Forwarded	Number of forwarded packets.
Raw packets	Total number of packets sent through the raw socket, such as ping or tracert packets.
Discarded	Total number of discarded packets.
Fragmented	Total number of IPv6 packets that are successfully fragmented.
Fragments	Total number of sent fragmented packets.
Fragments failed	Total number of IPv6 packets that fail to be fragmented.
Multicast	Total number of sent multicast packets.
Received packets	Statistics about received packets.
Total	Total number of received packets.

Item	Description
Local host	Total number of packets received by the local device.
Hop count exceeded	Total number of packets whose hops exceed the upper limit.
Header error	Total number of packets with incorrect packet header.
Too big	Total number of received packets that fail to be forwarded because of excessive size.
Routing failed	Total number of packets that fail to be routed.
Address error	Total number of packets with incorrect IP addresses.
Protocol error	Total number of packets with the incorrect protocol.
Truncated	Total number of packets discarded because the actual packet length is shorter than that specified in the packet length field.
Option error	Total number of packets that carry incorrect options.
Fragments	Total number of received fragmented packets.
Reassembled	Total number of packets that are successfully reassembled.
Reassembly timeout	Total number of packets that fail to be reassembled due to timeout.
Multicast	Total number of received multicast packets.
Fragments overlap	Total number of received fragmented packets that are overlapped.
Extension Header	Total number of the IPv6 extension headers.
Hop-by-Hop Options	Total number of the hop-by-hop options headers.
Mobility Header	Total number of the mobility headers.
Destination Options	Total number of the destination options headers.

Item	Description
Routing Header	Total number of the routing options headers.
Fragment Header	Total number of the fragment headers.
Authentication Header	Total number of the authentication headers.
Encapsulation Header	Total number of the encapsulation headers.
No header	Total number of the packets without headers.
TLV Length error	Total number of the extension headers in which the TLV length field is wrong.
Header Length error	Total number of the extension headers in which the length field is wrong.
Unknown header type	Total number of the unknown extension header types.
Unknown TLV type	Total number of the unknown TLV types.

6.10.12 display nd optimized-passby status

Function

The **display nd optimized-passby status** command displays whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect.

Format

display nd optimized-passby status interface vlanif *vlanif-id* **slot** *slot-id*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface vlanif *vlanif-id*	Displays whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect on a specified VLANIF interface.	The value is an integer and the value range depends on the range of existing VLANIF interfaces. You can enter ? to obtain the range of VLANIF interface numbers.
slot *slot-id*	Displays whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect in a specified slot.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an interface receives a large number of NS packets whose destination IPv6 addresses are different from the IPv6 address of this interface and sends these NS packets to the CPU for processing, the CPU usage is high and the CPU cannot process services properly.

To prevent this issue, you can configure the device to directly forward NS packets destined for other devices without sending them to the CPU. This improves the device's capability of defending against packet attacks.

When the device is configured not to send NS packets destined for other devices to the CPU, the configuration does not take effect if a conflict configuration exists on the device. You can use the **display nd optimized-passby status** command to check whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect. For details about conflict configurations, see **nd optimized-passby enable**.

Example

Display whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect on VLANIF 100.

```
<HUAWEI> display nd optimized-passby status interface Vlanif 100 slot 0
Current configuration: Enable
Actual          status: Inactive
Inactive        Reason: The interface protocol status is down.
```

Table 6-67 Description of the **display nd optimized-passby status** command output

Item	Description
Current configuration	Whether the device is configured not to send NS packets destined for other devices to the CPU. - Enable: The device is configured not to send NS packets destined for other devices to the CPU. - Disable: The device is configured to send NS packets destined for other devices to the CPU.
Actual status	Whether the configuration of disabling the device from sending NS packets destined for other devices to the CPU takes effect. - Inactive - Active
Inactive Reason	Conflict configuration.

6.10.13 display nd optimized-reply statistics

Function

The **display nd optimized-reply statistics** command displays statistics on optimized ND Reply packets.

Format

display nd optimized-reply statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on optimized ND Reply packets after the optimized ND reply function is enabled on the device.

Example

Display statistics on optimized ND Reply packets.

```
<HUAWEI> display nd optimized-reply statistics
Slot          Received           Processed            Dropped
---------------------------------------------------------------
0                  11                 9                 7
```

Table 6-68 Description of the display nd optimized-reply statistics command output

Item	Description
Slot	Stack ID.
Received	Number of ND Request packets entering the processing procedure of the optimized ND reply function.
Processed	Number of optimized ND Reply packets.
Dropped	Number of ND Request packets discarded. **NOTE** When the optimized ND reply function is enabled, the device does not optimize the responses to the ND Request packets whose destination IPv6 address is not the IPv6 address of a local interface on the switch.

6.10.14 display nd optimized-reply status

Function

The **display nd optimized-reply status** command displays the status of the optimized ND reply function.

Format

display nd optimized-reply status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the status of the optimized ND reply function.

Example

Check the status of the optimized ND reply function.

```
<HUAWEI> display nd optimized-reply status
Current configuration:Disable
Actual          status:Inactive
Related configuration:
   nd optimized-reply disable
```

Table 6-69 Description of the display nd optimized-reply status command output

Item	Description
Current configuration	Configuration of the optimized ND reply function. - Enable - Disable To set this field, run the **nd optimized-reply disable** command.
Actual status	Status of the optimized ND reply function. - Active - Inactive
Related configuration	Configuration that results in the invalid optimized ND reply function. If the optimized ND reply function has taken effect, this field is not displayed.

6.10.15 display rawip ipv6 statistics

Function

The **display rawip ipv6 statistics** command displays Raw IPv6 packet statistics.

Format

display rawip ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rawip ipv6 statistics** command to view Raw IPv6 packet statistics, including:

- Statistics about received and sent Raw IPv6 packets
- Statistics about discarded Raw IPv6 packets

Example

Display Raw IPv6 packet statistics.

```
<HUAWEI> display rawip ipv6 statistics
 Received packets:
     total: 20
     packets sent for external pre processing: 0
     packets for which checksum has to be calculated: 0
     packets with invalid checksum : 0
     dropped packets due to socket buffer is full: 0
     dropped packets due to no matching socket: 20
     dropped multicast packets due to no matching socket: 0
 Sent packets:
     total (excluding ICMP6 packets): 0
```

Table 6-70 Description of the display rawip ipv6 statistics command output

Item	Description
total	Total number of received and sent packets.
packets sent for external pre processing	Number of received Raw IPv6 packets for external preprocessing.
packets for which checksum has to be calculated	Number of received Raw IPv6 packets for which checksum has been calculated.
packets with invalid checksum	Number of discarded Raw IPv6 packets with checksum errors.
dropped packets due to socket buffer is full	Number of Raw IPv6 packets that are discarded because the socket buffer is full.

Item	Description
dropped packets due to no matching socket	Number of discarded Raw IPv6 packets that do not match the receiving socket.
dropped multicast packets due to no matching socket	Number of discarded Raw IPv6 packets destined to a multicast address that do not match the receiving socket.

6.10.16 display tcp ipv6 authentication-statistics

Function

The **display tcp ipv6 authentication-statistics** command displays authentication statistics of a specified TCP6 connection.

Format

display tcp ipv6 authentication-statistics src-ip *src-ip* **src-port** *src-port* **dest-ip** *dest-ip* **dest-port** *dest-port*

Parameters

Parameter	Description	Value
src-ip *src-ip*	Specifies the source IPv6 address.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
src-port *src-port*	Specifies the source port.	The value is an integer that ranges from 0 to 65535.
dest-ip *dest-ip*	Specifies the destination IPv6 address.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
dest-port *dest-port*	Specifies the destination port.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display tcp ipv6 authentication-statistics** command to view authentication statistics of a specified TCP6 connection, including:

- Number of TCP6 packets with MD5 Option
- Number of TCP6 packets with Enhanced Authentication Option

Example

Display authentication statistics of a specified TCP6 connection.

```
<HUAWEI> display tcp ipv6 authentication-statistics src-ip fc00::1 src-port 3456 dest-ip fc00::5 dest-port 5678
MD5 Signature Option (MSO)is enabled |
 Enhanced Authentication Option (EAO)is enabled
Received packets:
     total: 0
     packets received with MSO: 0
     packets received with EAO: 0
     packets dropped due to MD5 authentication failure: 0
     packets dropped due to absence of MSO: 0
     packets dropped due to presence of MSO: 0
     packets dropped due to MAC authentication failure: 0
     packets dropped due to absence of active receive key: 0
     packets dropped due to invalid receive algorithm id: 0
     packets dropped due to absence of EAO: 0

Sent packets:
     total: 0
     packets sent with MSO: 0
     packets sent with EAO: 0
     packets not sent due to absence of active send key: 0
```

Table 6-71 Description of the **display tcp ipv6 authentication-statistics** command output

Item	Description
total (received packets)	Total number of received and discarded TCP6 packets.
packets received with MSO	Total number of received TCP6 packets with MD5 Option.
packets received with EAO	Total number of received TCP6 packets with Enhanced Authentication Option.
packets dropped due to MD5 authentication failure	Total number of TCP6 packets discarded due to MD5 authentication failure.
packets dropped due to absence of MSO	Total number of TCP6 packets discarded due to absence of MD5 Option.
packets dropped due to presence of MSO	Total number of TCP6 packets discarded due to presence of MD5 Option.

Item	Description
packets dropped due to MAC authentication failure	Total number of TCP6 packets discarded due to MAC authentication failure.
packets dropped due to absence of active receive key	Total number of TCP6 packets discarded due to absence of active receive key.
packets dropped due to invalid receive algorithm id	Total number of TCP6 packets discarded due to invalid receive algorithm ID.
packets dropped due to absence of EAO	Total number of TCP6 packets discarded due to absence of Enhanced Authentication Option.
total (sent packets)	Total number of sent and unsent TCP6 packets.
packets sent with MSO	Total number of sent TCP6 packets with MD5 Option.
packets sent with EAO	Total number of sent TCP6 packets with Enhanced Authentication Option.
packets not sent due to absence of active send key	Total number of TCP6 packets discarded due to absence of active send key.

6.10.17 display tcp ipv6 statistics

Function

The **display tcp ipv6 statistics** command displays TCP6 traffic statistics.

Format

display tcp ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can check the network connection status according to the items in the command output, for example:

- Established connections: indicates the number of established connections, helping you determine whether to continue deploying services such as BGP services or adjust the load.
- Duplicate ACK packets: indicates whether the device is attacked by unknown ACK packets. If the device receives a large number of unknown ACK packets, the device may be attacked.
- Out-of-order packets: allows you to check network performance. If the network is in poor condition, a lot of out-of-order packets are generated.

Precautions

- The total number of received packets includes the number of forwarded packets, number of packets delivered to the upper layer, and number of discarded packets.
- Before running this command to view TCP6 statistics within a specified period, run the **reset tcp ipv6 statistics** command to clear existing statistics.

Example

Display TCP6 packet statistics.

```
<HUAWEI> display tcp ipv6 statistics
Received packets:
    total: 0
    total(64bit high-capacity counter): 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0
    window update packets: 0
    checksum error: 0
    offset error: 0
    short error: 0
    duplicate packets: 0 (0 bytes)
    partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0
    too much ACK packets: 0
    packets dropped due to MD5 authentication failure: 0
    packets dropped due to absence of MSO: 0
    packets dropped due to presence of MSO: 0
    packets received with MD5 Signature Option: 0

Sent packets:
    total: 0
    urgent packets: 0
    total(64bit high-capacity counter): 0
    control packets: 0 (including 0 RST)
    window probe packets: 0
    window update packets: 0
    data packets: 0 (0 bytes)
    data packets retransmitted: 0 (0 bytes)
    ACK only packets: 0 (0 delayed)
    packets sent with MD5 Signature Option: 0

Other Statistics:
    retransmitted timeout: 0
    connections dropped in retransmitted timeout: 0
    keepalive timeout: 0
    keepalive probe: 0
```

```
    keepalive timeout, so connections disconnected: 0
    initiated connections: 0
    accepted connections: 0
    established connections: 0
    closed connections: 1 (dropped: 0, initiated dropped: 0)
```

Table 6-72 Description of the **display tcp ipv6 statistics** command output

Item	Description
Received packets: total	Total number of received packets.
packets in sequence	Number of packets received in sequence.
window probe packets	Number of received window probe packets.
window update packets	Number of received window update packets.
checksum error	Number of received packets received with invalid checksum.
offset error	Number of received packets with incorrect TCP header length.
short error	Number of received packets with total length shorter than the set value in the packet header.
duplicate packets	Number of received duplicate packets.
partially duplicate packets	Number of received partially duplicate packets.
out-of-order packets	Number of received out-of-order packets.
packets with data after window	Number of received packets exceeding the receive window.
packets after close	Number of packets received after the connection is closed.
ACK packets	Number of received ACK packets.
duplicate ACK packets	Number of received duplicate ACK packets.
too much ACK packets	Number of received ACK packets with too large ACK values.
Sent packets: total	Total number of sent packets.
urgent packets	Number of sent packets with the urgent pointer.
control packets	Number of sent control packets.
window probe packets	Number of sent window probe packets.

Item	Description
window update packets	Number of sent window update packets.
data packets	Number of sent data packets.
data packets retransmitted	Number of retransmitted data packets.
ACK only packets	Number of sent ACK only packets.
Other Statistics	Other statistics.
retransmitted timeout	Number of retransmission timeout packets.
connections dropped in retransmitted timeout	Number of disconnected connections during the retransmission timeout.
keepalive timeout	Number of Keepalive timeouts.
keepalive probe	Number of Keepalive probes.
keepalive timeout, so connections disconnected	Number of connections disconnected due to Keepalive timeout.
initiated connections	Number of initiated connections.
accepted connections	Number of accepted connections.
established connections	Number of established connections.
closed connections	Number of closed connections.
dropped	Number of disconnected connections.
initiated dropped	Number of initiated and disconnected connections.

6.10.18 display tcp ipv6 status

Function

The **display tcp ipv6 status** command displays the status of all TCP6 connections.

Format

display tcp ipv6 status [**local-ip** *ipv6-address*] [**local-port** *local-port-number*] [**remote-ip** *ipv6-address*] [**remote-port** *remote-port-number*]

display tcp ipv6 status [**task-id** *task-id* [**sock-id** *sock-id*]]

Parameters

Parameter	Description	Value
local-ip *ipv6-address*	Displays the TCP6 connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the local device.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
remote-ip *ipv6-address*	Displays the TCP6 connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the remote device.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
local-port *local-port-number*	Displays the TCP6 connection status of the specified port number. *local-port-number* specifies the port number of the local device.	The value is an integer that ranges from 0 to 65535.
remote-port *remote-port-number*	Displays the TCP6 connection status of the specified port number. *remote-port-number* specifies the port number of the remote device.	The value is an integer that ranges from 0 to 65535.
task-id *task-id*	Displays the status of the TCP6 connection with the specified task ID. *task-id* specifies the task ID.	The value is an integer that ranges from 1 to 200.
sock-id *sock-id*	Displays the TCP6 connection status with the specified socket ID. *sock-id* specifies the socket ID.	The value is an integer that ranges from 1 to 131072.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display tcp ipv6 status** command to view all valid TCP6 control blocks, including the following information:

- TCP6 socket ID
- Local IPv6 address and port number
- Remote IPv6 address and port number
- TCP6 connection status
- VPN ID

To view the status of all valid TCP6 connections, run the **display tcp ipv6 status** [**local-ip** *ipv6-address*] [**local-port** *local-port-number*] [**remote-ip** *ipv6-address*] [**remote-port** *remote-port-number*] command.

To view the status of the TCP6 connection with a specified socket ID, run the **display tcp ipv6 status** [**task-id** *task-id* [**sock-id** *sock-id*]] command.

Precautions

If there is no TCP connection, no information is displayed.

Example

Display the status of TCP6 connections.

```
<HUAWEI> display tcp ipv6 status
* - MD5 Authentication is enabled.
TCP6CB   TID/SoID  Local Address       Foreign Address      State        VPNID
0be58fa8 102/3     ::->22              ::->0                Listening    0
0d109448 102/2     ::->23              ::->0                Listening    0
```

Table 6-73 Description of the **display tcp ipv6 status** command output

Item	Description
TCP6CB	Address of a TCP6 control block, in hexadecimal notation.
TID/SoID	Task ID and socket ID.
Local Address	Local IPv6 address and port number.
Foreign Address	Remote IPv6 address and port number.

Item	Description
State	Status of a TCP6 connection: - Closed: indicates that the TCP connection is closed. - Listening: indicates that the TCP connection is being listened on. - Syn_Rcvd: indicates that a TCP packet with the SYN flag is received. - Syn_Sent: indicates that a TCP packet with the SYN flag is sent. - Established: indicates that the TCP connection has been set up. - Close_Wait: indicates that a user host sends a packet with the FIN flag to the server, requesting the server to close the TCP connection in Established state. The server then sends an ACK packet to the user host after receiving the packet and enters the Close_Wait state. - Fin_Wait1: indicates that a user host sends a packet with the FIN flag to the server, requesting the server to close the TCP connection and enters the Fin_Wait1 state. - Fin_Wait2: indicates that a user host receives an ACK packet in a response to the sent packet with the FIN flag and enters the Fin_Wait2 state. - Time_Wait: indicates that TCP enters this state after the TCP connection is closed. When TCP has been in Time_Wait state two times the longest packet lifetime, records about the closed connection are deleted. - Closing: indicates that the two ends close the TCP connection simultaneously. - LAST_ACK: indicates that the local end waits for acknowledging the TCP connection teardown request sent to the remote end.
VPNID	VPN ID.

6.10.19 display this ipv6 interface

Function

The **display this ipv6 interface** command displays IPv6 information on the current interface.

Format

display this ipv6 interface

Parameters

None

Views

Interface view

Default Level

1: Monitoring level

Usage Guidelines

After an IPv6 address is configured in the interface view, you can run the **display this ipv6 interface** command to check IPv6 information on the interface.

Example

Display IPv6 information on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] display this ipv6 interface
Vlanif10 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:4AFF:FE3D:9801 [TENTATIVE]
  Global unicast address(es):
    FC00::1, subnet is FC00::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF3D:9801
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

Display IPv6 information on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00:1::1 64
[HUAWEI-GigabitEthernet0/0/1] display this ipv6 interface
GigabitEthernet0/0/1 current state : DOWN
IPv6 protocol current state : DOWN
IPv6 is enabled, link-local address is FE80::225:9EFF:FEF4:ABCD
[TENTATIVE]
  Global unicast address(es):
    FC00:1::1, subnet is FC00:1::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FFF4:ABCD
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

Table 6-74 Description of the **display this ipv6 interface** command output

Item	Description
Vlanif10 current state	Current physical status of VLANIF 10. - UP: enabled - DOWN: disabled
GigabitEthernet0/0/1 current state	Current physical status of GigabitEthernet0/0/1. - UP: enabled - DOWN: disabled
IPv6 protocol current state	Current protocol status of the interface. - UP: enabled - DOWN: disabled
link-local address	Link-local address on the interface. After an IPv6 address is configured on the interface, the system automatically assigns a link-local address for the interface. To manually configure a link-local address for an interface, run the **ipv6 address link-local** command.

Item	Description
Global unicast address(es)	Global unicast address configured on the interface. To configure a global unicast address for an interface, run the **ipv6 address** command.
Joined group address(es)	Addresses of all multicast groups that the interface joins.
TENTATIVE	When the interface is in DOWN state, the IPv6 address is TENTATIVE. When the IPv6 address is duplicate with another, this field is DUPLICATE. In normal cases, this field is not displayed.
MTU	MTU of the interface. To configure the MTU for an interface, run the **ipv6 mtu** command.
ND DAD is enabled	Duplicate address detection (DAD) has been enabled.
number of DAD attempts	Number of times duplicate address detection is performed.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Retransmission interval.
ND stale time	Aging time of ND entries in STALE state.
ND advertised reachable time	Reachable time of NA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND advertised retransmit interval	Retransmission interval of NA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisement max interval 600 seconds, min interval 200 seconds	Maximum and minimum interval of RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND router advertisements live for	Router lifetime in RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.

Item	Description
ND router advertisements hop-limit	Hop limit of RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
ND default router preference	Default route priority in RA packets. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses by means of stateless auto-configuration. **NOTE** This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface.

6.10.20 display udp ipv6 statistics

Function

The **display udp ipv6 statistics** command displays UDP6 packet statistics.

Format

display udp ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The User Datagram Protocol (UDP) is a simple protocol that exchanges packets on the Internet. You can run the **display udp ipv6 statistics** command to view statistics about sent and received UDP6 packets.

Precautions

The total number of packets received by the device includes the number of forwarded packets, number of packets delivered by the device to the upper layer, and number of discarded packets.

Example

Display UDP6 packet statistics.

```
<HUAWEI> display udp ipv6 statistics
Received packets:
     total: 0
     total(64bit high-capacity counter): 0
     checksum error: 0
     shorter than header: 0
     invalid message length: 0
     no socket on port: 0
     no multicast port: 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
     packets sent for external pre processing: 1

Sent packets:
     total: 0
     total(64bit high-capacity counter): 0
```

Table 6-75 Description of the display udp ipv6 statistics command output

Item	Description
Received packets	Number of received packets.
total	Total number of received and sent packets.
checksum error	Total number of packets with invalid checksum.
shorter than header	Total number of UDP6 packets with the length shorter than the packet header.
invalid message length	Total number of packets whose data length is longer than the packet length.
no socket on port	Number of packets without corresponding sockets on the interface.
no multicast port	Number of received packets carrying nonexistent multicast interfaces.
not delivered, input socket full	Number of unprocessed packets when the buffer is full.
input packet missing pcb cache	Number of received packets failing to find the PCB cache.
packets sent for external pre processing	Number of received packets for external preprocessing.
Sent packets	Number of sent packets.

6.10.21 eth-trunk (tunnel interface view)

Function

The **eth-trunk** command associates a specified tunnel interface with an Eth-Trunk interface enabled with service loopback.

The **undo eth-trunk** command disassociates a specified tunnel interface from an Eth-Trunk interface enabled with service loopback.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

eth-trunk *trunk-id*

undo eth-trunk

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk interface associated with the tunnel interface.	S5720I-SI, S5735-S, S500, S5735-S-I, and S5735S-S: The value ranges from 0 to 119. S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: The value ranges from 0 to 127. S5735S-H, S5736-S, and S6720S-S: The value ranges from 0 to 249.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Before associating a specified tunnel interface with an Eth-Trunk interface, run the **service type tunnel** command to enable service loopback on the Eth-Trunk interface.

Example

Associate Tunnel1 with the Eth-Trunk interface enabled with service loopback.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] eth-trunk 1
```

6.10.22 ipv6

Function

The **ipv6** command enables the device to forward IPv6 unicast packets, including sending and receiving local IPv6 packets.

The **undo ipv6** command disables the device from forwarding IPv6 unicast packets.

By default, a device is disabled from forwarding IPv6 unicast packets.

Format

ipv6

undo ipv6

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You must run the **ipv6** command in the system view before performing IPv6 configurations.

NOTE

The **undo ipv6** command disables the device from forwarding IPv6 unicast packets. Therefore, confirm your action before running this command.

When system resources are insufficient, the **ipv6** command does not take effect and an alarm is generated. The alarm ID is 1.3.6.1.4.1.2011.5.25.227.2.1.7.

Example

Enable the device to forward IPv6 unicast packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

Disable the device from forwarding IPv6 unicast packets.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6
Warning: This operation will interrupt all IPv6 services. Continue?[Y/N]:y
```

6.10.23 ipv6 address

Function

The **ipv6 address** command configures a site-local address or global unicast address for an interface.

The **ipv6 address** *dhcpv6-prefix* command configures an IPv6 address bound to the DHCPv6 PD prefix for an interface.

The **undo ipv6 address** command deletes a global unicast address from an interface.

The **undo ipv6 address** *dhcpv6-prefix* command deletes the IPv6 address bound to the DHCPv6 PD prefix for an interface.

By default, no global unicast address is configured for an interface.

By default, no IPv6 address bound to the DHCPv6 PD prefix is configured for an interface.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

ipv6 address *dhcpv6-prefix* { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*]

undo ipv6 address *dhcpv6-prefix*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
prefix-length	Specifies the prefix length of an IPv6 address. An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.	The value is an integer that ranges from 1 to 128.
dhcpv6-prefix	Specifies the prefix assigned to a DHCPv6 PD client.	The value must be an existing prefix assigned to a DHCPv6 PD client.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A global unicast address is similar to an IPv4 public network address. Global unicast addresses are used on the links that can be summarized, and are provided for the Internet Service Providers (ISPs). These addresses allow route prefix summarization, limiting global routing entries. A global unicast address consists of a 48-bit route prefix managed by carriers, a 16-bit subnet ID managed by local nodes, and a 64-bit interface ID.

The switch is required to function as a DHCPv6 PD client and obtain an IPv6 address prefix from the DHCPv6 PD server. You can run the **ipv6 address** *dhcpv6-prefix* { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } command to configure an IPv6 address is bound to the DHCPv6 PD prefix. After you run this command, the switch uses the prefix assigned to the DHCPv6 PD client and the IPv6 address to form an RA prefix for the interface only when the switch functions as a DHCPv6 PD client and obtains a prefix. The prefix must be a 64-digit number. If not, the host cannot use this prefix for automatic assignment of IPv6 addresses.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The following conditions are prohibited for different interfaces on the same switch:

- The IPv6 addresses are the same.
- The network prefixes of the IPv6 addresses are the same. For example, if the IPv6 address of interface A is 2001:db8::1/12 and its network prefix is 200::

and the IPv6 address of interface B is 2001:db8::1/127 and its network prefix is 2001:db8::, the configuration succeeds. If the IPv6 address of interface B is also 2002:db8::1/12 and its network prefix is also 200::, the configuration fails.

A maximum of 10 global unicast addresses can be configured for an interface.

An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.

The following IPv6 addresses cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- IPv4-mapped IPv6 address (0:0:0:0:0:FFFF:IPv4-address)

A 128-bit IPv6 address has two formats:

- X:X:X:X:X:X:X:X

  In this format, a 128-bit IPv6 address is written as eight groups of four hexadecimal digits (0 to 9, A to F), where each group is separated by a colon (:). Every X represents a group of hexadecimal numbers.
- X:X:X:X:X:X:d.d.d.d

  In this format, "X:X:X:X:X:X" represent the high-order six groups of numbers, and each X stands for 16 bits that are represented by four hexadecimal characters. "d.d.d.d" represents the low-order four groups of numbers, and each d stands for 8 bits that are represented by decimal numbers. "d.d.d.d" stands for a standard IPv4 address.

An IPv6 address has two parts:

- Network prefix: corresponds to the network ID of an IPv4 address. It is of n bits.
- Interface identifier: corresponds to the host ID of an IPv4 address. It is of 128-n bits.

If the **ipv6 address** command has been run to configure an IPv6 address for an interface, but no link-local address is configured for the interface, the system generates a link-local address for the interface.

If no parameter (IPv6 address or prefix length) is specified in the **undo ipv6 address** command, running the **undo ipv6 address** command deletes all IPv6 addresses.

Example

Configure a global unicast address for VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address fc00::1/64
```

Configure a global unicast address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00::1/64
```

Configure an IPv6 address bound to the DHCPv6 PD prefix for VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address prefix1 ::1:0:0:0:1/64
```

6.10.24 ipv6 address anycast

Function

The **ipv6 address anycast** command configures an IPv6 anycast address.

The **undo ipv6 address** command deletes an IPv6 anycast address.

By default, no IPv6 anycast address is configured.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } **anycast**

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An anycast address identifies a group of interfaces, which usually belong to different nodes. Packets sent to an anycast address are delivered to the nearest interface that is identified by the anycast address, depending on the routing protocols.

To implement communication between a 6to4 network and a local (native) IPv6 network using a 6to4 tunnel, configure an anycast address with prefix 2002:c058:6301:: for the tunnel interface of a 6to4 relay agent. If an anycast address is used, you need to configure the same address for the tunnel interfaces of all devices. In this manner, the number of addresses is reduced.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If no parameter is specified in the **undo ipv6 address** command, all IPv6 addresses except link-local addresses are deleted.

An anycast address cannot be used as the source address of a packet. Therefore, a global unicast address must be configured when a device needs to send packets.

An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.

Example

Configure anycast address 2002:c058:6301::/48 for VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address 2002:c058:6301:: 48 anycast
```

Configure anycast address 2002:c058:6301::/48 for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address 2002:c058:6301:: 48 anycast
```

6.10.25 ipv6 address auto global

Function

The **ipv6 address auto global** command enables a device to generate an IPv6 global address through stateless autoconfiguration.

The **undo ipv6 address auto global** command disables a device from generating an IPv6 global address through stateless autoconfiguration.

By default, the device is disabled from generating an IPv6 global address through stateless autoconfiguration.

Format

ipv6 address auto global [**default**]

undo ipv6 address auto global

Parameters

Parameter	Description	Value
default	Indicates that the device learns the default route.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ipv6 address auto global** command is run, a device automatically generates an IPv6 global unicast address on the interface that receives a RA packet. The generated IPv6 address contains the address prefix in the received RA packet and interface identifier of the device. If the device does not receive RA packets, the device can only automatically configure a link-local address to interconnect with local nodes.

After the **ipv6 address auto global default** command is run, a device generates an IPv6 address based on the received RA packet and learns the source address in the RA packet. The device then uses the source IPv6 address as the next hop address of the default IPv6 route.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After the **ipv6 address auto global** command is run, if an interface receives a new RA packet, a new IPv6 address is generated for the interface based on the received RA packet, but the default routes learned by the interface are not deleted.

If an interface has been configured with an IPv6 address, the original IPv6 address is not deleted after the interface receives an RA packet and generates a new IPv6 address. If the interface receives no RA packet and the generated IPv6 address expires, the interface deletes the generated IPv6 address and uses the original IPv6 address.

A device learns a maximum of three default routes based on RA packets. New routes cannot override the existing three routes, and extra routes will be discarded. If multiple default routes have the same priority, packets are forwarded in load balancing mode.

Example

Enable a device to generate an IPv6 global address through stateless autoconfiguration on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto global
```

Enable a device to generate an IPv6 global address through stateless autoconfiguration on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto global
```

6.10.26 ipv6 address auto link-local

Function

The **ipv6 address auto link-local** command configures an interface to automatically generate a link-local address.

The **undo ipv6 address auto link-local** command deletes the automatically generated link-local address on a specified interface.

By default, no link-local address is automatically generated on an interface.

Format

ipv6 address auto link-local

undo ipv6 address auto link-local

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link-local addresses are used for communications between link-local nodes in either the neighbor discovery or stateless auto-configuration process. A packet with a link-local address set to a source or destination address will not be forwarded to another link. That is, link-local addresses are valid only on local links.

After the **ipv6 address auto link-local** command is run, a device uses the link-local address prefix FE80::/10 (1111 1110 10) and IEEE EUI-64 interface identifier go generate a link-local address for an interface. An IEEE EUI-64 interface identifier is converted from an interface link layer address, for example a MAC address.

1. The hexadecimal number FFFE (1111 1111 1111 1110 in binary) is inserted in the middle of a MAC address.
2. The U/L bit (the leftmost seventh bit) is set to 1.
3. The interface ID in EUI-64 format then is obtained.

After an interface automatically obtains a link-local address, it can implement neighbor discovery and automatically configure a global unicast address or a unique local address.

Prerequisites

Before running this command, run the **ipv6 enable** command in the interface view to enable the IPv6 function.

Precautions

Only a single link-local address can be assigned to each interface. If an automatically allocated link-local address has already been configured on an interface, running the **ipv6 address link-local** command will overwrite the existing link-local address.

The **undo ipv6 address auto link-local** command can only delete a link-local address that is automatically generated by an interface. To delete a manually configured link-local address, run the **undo ipv6 address link-local** command.

Example

Configure VLANIF2 to automatically generate a link-local address.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 address auto link-local
```

Configure GE0/0/1 to automatically generate a link-local address.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
```

6.10.27 ipv6 address eui-64

Function

The **ipv6 address eui-64** command configures a site-local address or global unicast address in EUI-64 format for an interface.

The **undo ipv6 address eui-64** command deletes a site-local address or global unicast address in EUI-64 format from an interface.

By default, no site-local address or global unicast address in EUI-64 format is configured for an interface.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IPv6, any IPv6 unicast address needs an interface identifier. The interface identifier is globally unique, similar to a 48-bit MAC address.

The interface identifier of an IPv6 host address uses the IEEE EUI-64 format. A 64-bit interface identifier is generated based on an existing MAC address; therefore, such an interface identifier is globally unique. These 64-bit interface identifiers are globally valid for addressing and uniquely identify each network interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The following conditions are prohibited for different interfaces on the same switch:

- The IPv6 addresses are the same.
- The network prefixes of the IPv6 addresses are the same. For example, if the IPv6 address of interface A is 2001:db8::1/12 and its network prefix is 200:: and the IPv6 address of interface B is 2001:db8::1/127 and its network prefix is 2001:db8::, the configuration succeeds. If the IPv6 address of interface B is also 2002:db8::1/12 and its network prefix is also 200::, the configuration fails.

A maximum of 10 global unicast addresses can be configured for an interface.

The following IPv6 addresses in EUI-64 format cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- IPv4-mapped IPv6 address (0:0:0:0:0:FFFF:IPv4-address)

The **ipv6 address** command is used to specify a 128–bit IPv6 address. Using the **ipv6 address eui-64** command, you can specify the high-order 64 bits of an IPv6 address. The low-order 64 bits of an IPv6 address are automatically generated in the EUI-64 format. Even when the low-order 64 bits are manually specified, the automatically generated ones will override them.

Example

Configure an IPv6 address in EUI-64 format for VLANIF 2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 address fc00::1/64 eui-64
```

Configure an IPv6 address in EUI-64 format for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00::1/64 eui-64
```

6.10.28 ipv6 address link-local

Function

The **ipv6 address link-local** command manually configures a link-local address for a specified interface.

The **undo ipv6 address link-local** command deletes the manually configured link-local address on an interface.

By default, no link-local address is configured for an interface.

Format

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. When a link-local address is being configured, the prefix of the specified IPv6 address must match FE80::/10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link-local addresses are used for the communication between nodes on the same local link in neighbor discovery or stateless autoconfiguration. The packet with a link-local address being the source or destination address will not be forwarded to other links. That is, link-local addresses are valid only on local links.

You can run the **ipv6 address link-local** command to manually configure a link-local address for an interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Avoid changing link-local addresses.

You can configure multiple IPv6 addresses but only one link-local address for an interface.

The link-local address configured using the **ipv6 address link-local** command will override the link-local address automatically generated by the system.

The **undo ipv6 address link-local** command deletes only the link-local address manually configured for an interface. To delete the automatically generated link-local address, run the **undo ipv6 address auto link-local** command.

If an interface is being unbound from the VPN instance that has IPv6 address family enabled, the system displays a message, indicating that this command cannot be run.

The following IPv6 addresses cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address

Example

Manually configure a link-local address for VLANIF 2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 address fe80::1 link-local
```

Manually configure a link-local address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fe80::1 link-local
```

6.10.29 ipv6 enable (interface view)

Function

The **ipv6 enable** command enables the IPv6 function on an interface.

The **undo ipv6 enable** command disables the IPv6 function on an interface.

By default, the IPv6 function is disabled on an interface.

Format

ipv6 enable

undo ipv6 enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can perform IPv6 configurations on an interface only when the interface has the IPv6 function enabled.

Prerequisites

The **ipv6** command has been run in the system view.

Follow-up Procedure

Configure IPv6 addresses and ND parameters. ND parameters include the M flag, O flag, RA halt flag, interval for sending RA packets, lifetime of RA packets, interval for sending NS packets, DAD counts, period during which the IPv6 neighbor keeps reachable, prefix carried in the RA packet, and static ND entries.

Precautions

After the IPv6 function is disabled on an interface, IPv6 configurations on the interface are deleted.

- After the IPv6 function is disabled on an interface, IPv6 addresses of the interface are deleted and IPv6 commands cannot be configured on the interface.
- After the IPv6 function is disabled on an interface, IS-IS IPv6 and RIPng are disabled on the interface. That is, the **isis ipv6 enable** and **ripng enable** commands become ineffective.

When system resources are insufficient, the **ipv6 enable** command does not take effect and an alarm is generated. The alarm ID is 1.3.6.1.4.1.2011.5.25.227.2.1.22.

Example

Enable the IPv6 function on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
```

Enable the IPv6 function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
```

6.10.30 ipv6 icmp-error

Function

The **ipv6 icmp-error** command sets the rate limit for sending ICMPv6 error packets.

The **undo ipv6 icmp-error** command restores the default rate limit for sending ICMPv6 error packets.

By default, the size of the token buckets is 10 and the limit rate is 100 milliseconds.

Format

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

Parameters

Parameter	Description	Value
bucket *bucket-size*	Specifies the maximum number of tokens the bucket can hold.	The value is an integer that ranges from 1 to 200. The default value is 10, which is recommended.
ratelimit *interval*	Specifies the interval for placing tokens into the bucket.	The value is an integer that ranges from 0 to 2147483647, in milliseconds. The default value is 100, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a network is not attacked, a routing device can correctly send ICMPv6 error packets to notify other devices of exceptions in packet transmission. If an attacker frequently sends ICMPv6 packets to network devices, the network devices will be busy responding with ICMPv6 packets. This affects system throughput and CPU usage. To prevent the system from sending a great number of ICMPv6 packets, run the **ipv6 icmp-error** command to limit the rate at which ICMPv6 packets are sent.

The token bucket algorithm is used to count ICMPv6 packets. One token represents an ICMPv6 error packet. The system places tokens into the virtual bucket at a certain interval until the number of tokens in the bucket reaches the upper limit. Once the number of ICMPv6 packets exceeds the maximum number of tokens that the bucket can contain, excess packets are discarded. You can limit the rate at which ICMPv6 packets are sent by setting the bucket size and the interval for placing tokens into the bucket.

Precautions

If you run the **ipv6 icmp-error** command multiple times, only the latest configuration takes effect.

If the interval for placing tokens into the bucket is 0, there is no limit on the interval.

Example

Set the rate limit for sending ICMPv6 error packets to 100.

```
<HUAWEI> system-view
[HUAWEI] ipv6 icmp-error ratelimit 100
```

Set the bucket size of ICMPv6 to 50.

```
<HUAWEI> system-view
[HUAWEI] ipv6 icmp-error bucket 50
```

Set the rate limit for sending ICMPv6 error packets to 100 and the bucket size to 50.

```
<HUAWEI> system-view
[HUAWEI] ipv6 icmp-error bucket 50 ratelimit 100
```

6.10.31 ipv6 icmp blackhole unreachable send

Function

The **ipv6 icmp blackhole unreachable send** command enables the switch to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

The **undo ipv6 icmp blackhole unreachable send** command disables the switch from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

By default, the switch is disabled from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

Format

ipv6 icmp blackhole unreachable send

undo ipv6 icmp blackhole unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If static IPv6 blackhole routes are configured on the switch configured with the user access and authentication function, when a user goes offline, only the IPv6 blackhole route corresponding to the user's address segment exists on the switch. When a tracert packet matches the IPv6 blackhole route, the switch discards the packet. As a result, an initiator cannot detect that the user has gone offline.

After you run the **ipv6 icmp blackhole unreachable send** command, the switch sends a Destination Unreachable ICMP packet to an initiator, notifying the initiator that the user has gone offline if a user goes offline and a tracert packet matches the IPv6 blackhole route.

Pre-configuration Tasks

Static IPv6 blackhole routes have been configured on the switch.

Example

Enable the switch to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

```
<HUAWEI> system-view
[HUAWEI] ipv6 icmp blackhole unreachable send
```

6.10.32 ipv6 icmp port-unreachable send

Function

The **ipv6 icmp port-unreachable send** command enables an interface to send ICMPv6 Port Unreachable messages.

The **undo ipv6 icmp port-unreachable send** command disables the function.

By default, the enabling status of the function that the interface sends ICMPv6 Port Unreachable messages is the same as that of the function that the system sends ICMPv6 Port Unreachable messages.

Format

ipv6 icmp port-unreachable send

undo ipv6 icmp port-unreachable send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a router receives a TCP6/UDP6 packet but cannot find the corresponding socket entry, the router replies with an ICMPv6 Port Unreachable message. This ICMPv6 error message carries the IPv6 address of the router as its source IPv6 address, which exposes the IPv6 address of the router and brings security risks. If the router is attacked by flooding packets, the router keeps replying with ICMPv6 Port Unreachable messages, causing high CPU usage and affecting device performance. To address this problem, run the **undo ipv6 icmp port-unreachable send** command on the inbound interface of ICMPv6 packets to disable the transmission of ICMPv6 Port Unreachable message.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Example

Enable VLANIF100 to send ICMPv6 Port Unreachable messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 icmp port-unreachable send
```

Enable interface GE0/0/1 to send ICMPv6 Port Unreachable messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 icmp port-unreachable send
```

6.10.33 ipv6 icmp hop-limit-exceeded send

Function

The **ipv6 icmp hop-limit-exceeded send** command enables an interface to send ICMPv6 Hop Limit Exceeded messages.

The **undo ipv6 icmp hop-limit-exceeded send** command disables the function.

By default, the enabling status of the function that the interface sends ICMPv6 Hop Limit Exceeded messages is the same as that of the function that the system sends ICMPv6 Hop Limit Exceeded messages.

Format

ipv6 icmp hop-limit-exceeded send

undo ipv6 icmp hop-limit-exceeded send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If a router receives a packet with a hop limit of 1, it replies with an ICMPv6 Hop Limit Exceeded message. This ICMPv6 error message carries the IPv6 address of the router as its source IPv6 address, which exposes the IPv6 address of the router and brings security risks. If the router is attacked by flooding packets, the router keeps replying with ICMPv6 Hop Limit Exceeded messages, causing high CPU usage and affecting device performance. To address this problem, run the **undo ipv6 icmp hop-limit-exceeded send** command on the inbound interface of ICMPv6 packets to disable the transmission of ICMPv6 Hop Limit Exceeded messages.

Example

Disable VLANIF100 from sending ICMPv6 Hop Limit Exceeded messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 icmp hop-limit-exceeded send
```

Disable interface GE0/0/1 from sending ICMPv6 Hop Limit Exceeded messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 icmp hop-limit-exceeded send
```

6.10.34 ipv6 icmp receive

Function

The **ipv6 icmp receive** command enables the system to receive ICMPv6 messages with the local address as the destination address.

The **undo ipv6 icmp receive** command disables the system from receiving ICMPv6 messages with the local address as the destination address.

By default, the system receives ICMPv6 messages with the local address as the destination address.

Format

ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **receive**

undo ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **receive**

Parameters

Parameter	Description	Value
icmpv6-type	Specifies the type of ICMPv6 messages.	The value is an integer in the range from 0 to 255.
icmpv6-code	Specifies the code of ICMPv6 messages.	The value is an integer in the range from 0 to 255.
icmpv6-name	Specifies the name of ICMPv6 messages.	ICMPv6 messages are classified into the following types: ● echo: Echo packet ● echo-reply: Echo Reply packet ● err-header-field: Packet with an error header ● frag-time-exceeded: Fragmentation Timeout packet ● hop-limit-exceeded: Packet whose hop count exceeds the limit ● host-admin-prohib: Packet that is rejected by a host ● host-unreachable: ICMPv6 Host Unreachable packet ● neighbor-advertisement: Neighbor Advertisement packet ● neighbor-solicitation: Neighbor Solicitation packet ● network-unreachable: ICMPv6 Network Unreachable packet ● packet-too-big: Packet Too Big packet ● port-unreachable: ICMPv6 Port Unreachable packet ● redirect: Redirected packets ● router-advertisement: Router Advertisement packet ● router-solicitation: Router Solicitation packet ● unknown-ipv6-opt: Error packet with unknown options ● unknown-next-hdr: Error packet with unknown next header
all	Indicates all ICMPv6 messages.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal cases, a switch can properly receive ICMPv6 messages. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the switch receives a large number of ICMPv6 messages, which burdens the network and degrades device performance. In addition, attackers usually use ICMPv6 error messages to probe the internal network topology.

To improve network performance and security, run the **undo ipv6 icmp receive** command to disable the system from receiving ICMPv6 Echo Reply packets, Host Unreachable packets, and Port Unreachable packets with the local address as the destination address.

Precautions

When the network is in good performance again, you can run the **ipv6 icmp receive** command to enable the system to receive ICMPv6 messages with the local address as the destination address.

After the **undo ipv6 icmp receive** command is run, main interfaces are disabled from processing these ICMPv6 messages. In addition, the system does not collect statistics on these messages that are received but collects statistics on discarded messages.

Example

Disable the system from receiving ICMPv6 Echo packets with the local address as the destination address.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 icmp echo receive
```

6.10.35 ipv6 icmp send

Function

The **ipv6 icmp send** command enables the system to send ICMPv6 packets.

The **undo ipv6 icmp send** command disables the system from sending ICMPv6 packets.

By default, the system is enabled to send ICMPv6 packets.

Format

ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **send**

undo ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **send**

Parameters

Parameter	Description	Value
icmpv6-type	Specifies the type of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-code	Specifies the code of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-name	Specifies the name of ICMPv6 packets.	ICMPv6 packets are classified into the following types: ● echo: Echo packet ● echo-reply: Echo Reply packet ● err-header-field: Packet with an error header ● frag-time-exceeded: Fragmentation Timeout packet ● hop-limit-exceeded: Packet whose hop count exceeds the limit ● host-admin-prohib: Packet that is rejected by a host ● host-unreachable: ICMPv6 Host Unreachable packet ● neighbor-advertisement: Neighbor Advertisement packet ● neighbor-solicitation: Neighbor Solicitation packet ● network-unreachable: ICMPv6 Network Unreachable packet ● packet-too-big: Packet Too Big packet ● port-unreachable: ICMPv6 Port Unreachable packet ● redirect: Redirected packets ● router-advertisement: Router Advertisement packet ● router-solicitation: Router Solicitation packet ● unknown-ipv6-opt: Error packet with unknown options ● unknown-next-hdr: Error packet with unknown next header

Parameter	Description	Value
all	Indicates all ICMPv6 packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is in good performance, routing devices can send or receive ICMPv6 packets. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the routing devices send a large number of ICMPv6 packets, which burdens the network and degrades the performance of the routing devices. In addition, attackers may use ICMPv6 error packets to probe the internal network topology.

To improve network performance and security, run the **undo ipv6 icmp send** command to disable the system from sending ICMPv6 packets.

Precautions

When the network is in good performance again, you can run the **ipv6 icmp send** command to enable the system to send ICMPv6 packets.

Example

Disable the system from sending all ICMPv6 packets.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 icmp all send
```

6.10.36 ipv6 icmp too-big-rate-limit

Function

The **ipv6 icmp too-big-rate-limit** command enables a device to limit oversized ICMPv6 error packets.

The **undo ipv6 icmp too-big-rate-limit** command disables a device from limiting oversized ICMPv6 error packets.

By default, a device limit oversized ICMPv6 error packets.

Format

ipv6 icmp too-big-rate-limit

undo ipv6 icmp too-big-rate-limit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a host sends a large number of packets in a path with a small MTU, it may receive a large number of ICMPv6 error packets, affecting the processing of valid packets. This command limits the number of ICMPv6 error packets, ensuring host performance.

Example

Enable the device to limit oversized ICMPv6 error packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6 icmp too-big-rate-limit
```

6.10.37 ipv6 mtu

Function

The **ipv6 mtu** command sets the MTU on the interface for sending IPv6 packets.

The **undo ipv6 mtu** command restores the default MTU of IPv6 packets on an interface.

By default, the MTU of IPv6 packets on an interface is 1500 bytes.

NOTE

For the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H, this command does not take effect on the IPv6 packets matching ND entries. That is, the MTU of IPv6 packets matching ND entries on the devices is always 1500 bytes.

Format

ipv6 mtu *mtu*

undo ipv6 mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU value.	- For GE interfaces, GE sub-interfaces, XGE interfaces, XGE sub-interfaces, MultiGE interfaces, MultiGE sub-interfaces, 25GE interfaces, 25GE sub-interfaces, tunnel interfaces, and VLANIF interfaces, the value is an integer that ranges from 1280 to 9600, in bytes. - For other interfaces, the value is an integer that ranges from 1280 to 1500, in bytes. The default value is 1500.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the traffic processing capability of a link connecting the source and destination ends changes, you can use this command to set the MTU of IPv6 packets on an interface. If the packet length is larger than the IPv6 MTU of the interface, the system fragments the packet based on the configured MTU value before forwarding the packet.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The directly-connected interfaces must be configured with the same IPv6 MTU values.

Example

Set the MTU of IPv6 packets on VLANIF2 to 1280 bytes.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 mtu 1280
```

Set the MTU of IPv6 packets on GE0/0/1 to 1280 bytes.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 mtu 1280
```

6.10.38 ipv6 nd autoconfig managed-address-flag

Function

The **ipv6 nd autoconfig managed-address-flag** command sets the M flag of stateful autoconfiguration in an RA packet.

The **undo ipv6 nd autoconfig managed-address-flag** command deletes the M flag of stateful autoconfiguration in an RA packet.

By default, the "managed address configuration" flag (M flag) is not set in the RA message.

Format

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the M flag is set, a host obtains an IPv6 address through stateful autoconfiguration.
- If the M flag is not set, a host uses stateless autoconfiguration to obtain an IPv6 address, that is, the host generates an IPv6 address based on the prefix information in the RA packet.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After the **ipv6 nd autoconfig managed-address-flag** command is run, a host can obtain configurations (excluding an IPv6 address) such as the router lifetime, neighbor reachable time, retransmission interval, and PMTU by means of stateful autoconfiguration even if the **ipv6 nd autoconfig other-flag** command is not run.

After the **display ipv6 interface** command is run, the command output shows that the attached hosts obtain IPv6 addresses through stateful autoconfiguration or stateless autoconfiguration.

Example

Set the M flag of stateful autoconfiguration in an RA packet on VLANIF2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 nd autoconfig managed-address-flag
```

Set the M flag of stateful autoconfiguration in an RA packet on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd autoconfig managed-address-flag
```

6.10.39 ipv6 nd autoconfig other-flag

Function

The **ipv6 nd autoconfig other-flag** command sets the "other configuration" flag (O flag) of stateful autoconfiguration in an RA packet.

The **undo ipv6 nd autoconfig other-flag** command deletes the O flag of stateful autoconfiguration in an RA packet.

By default, the O flag is not set in the RA packet.

Format

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the O flag is set, a host uses stateful autoconfiguration to obtain other configuration parameters (excluding an IPv6 address), including the router lifetime, neighbor reachable time, retransmission interval, and PMTU.
- If the O flag is not set, a host uses stateless autoconfiguration to obtain other configuration parameters, including the router lifetime, neighbor reachable time, retransmission interval, and PMTU. That is, the host obtains other configuration parameters through the RA packet advertised by routers.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Example

Set the O flag of stateful autoconfiguration on VLANIF2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 nd autoconfig other-flag
```

Set the O flag of stateful autoconfiguration on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd autoconfig other-flag
```

6.10.40 ipv6 nd dad attempts

Function

The **ipv6 nd dad attempts** command sets the number of times NS packets are sent when the system performs Duplicate Address Detection (DAD).

The **undo ipv6 nd dad attempts** command restores the default value.

By default, the number of times NS packets are sent when the system performs DAD is 1.

Format

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

Parameters

Parameter	Description	Value
value	Specifies the number of times NS packets are sent when the system performs DAD.	The value is an integer that ranges from 0 to 600. The default value is 1, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure an IPv6 address (a global unicast address or a link-local address) for an interface, check whether other interfaces connected to this interface have used the IPv6 address to be configured to prevent address conflicts. The default number of detection times is recommended. If there is a long link delay, you can increase the number of detection times. When a loopback address is configured for an interface, the loopback address may fail the address conflict detection. In this case, you can set the number of detection times to 0 to disable detection, allowing the loopback address to be used.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If the number of times NS packets are sent when the system performs DAD is set 0, DAD is prohibited.

If the physical link connected to an interface fails, DAD cannot be performed on the interface.

If the **ipv6 nd dad attempts** command has been run, running the **ipv6 nd ra** command will change the number of configured detection times.

DAD transmits node configuration variables. The system automatically determines the time to send neighbor request messages while DAD is performed to detect a tentative unicast IPv6 address.

Example

Set the number of times NS packets are sent when the system performs DAD to 20 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd dad attempts 20
```

Set the number of times NS packets are sent when the system performs DAD to 20 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd dad attempts 20
```

6.10.41 ipv6 nd hop-limit

Function

The **ipv6 nd hop-limit** command sets hop limit for IPv6 unicast packets initially sent by a device.

The **undo ipv6 nd hop-limit** command restores the hop limit for IPv6 unicast packets to the default value.

By default, the IPv6 unicast packets initially sent by a device can travel 64 hops.

Format

ipv6 nd hop-limit *limit*

undo ipv6 nd hop-limit

Parameters

Parameter	Description	Value
limit	Specifies the hop limit.	The value is an integer that ranges from 1 to 255. The default value is 64, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hop limit on a device provides the following functions:

- Limiting the number of hops through which IPv6 unicast packets are allowed to travel.

- Functioning as a parameter in an RA packet to help a host automatically configure a hop limit (a limit on the number of hops through which IPv6 unicast packets initially sent by a host are allowed to travel).

Precautions

The hop limit for unicast packets is set using the **ipv6 nd hop-limit** command in the system view.

The hop limit for RA packets depends on the configuration of the **ipv6 nd hop-limit** command in the system view and the configuration of the **ipv6 nd ra hop-limit** command in the interface view.

- If the hop limit for RA packets is not set in the interface view or in the system view, the hop limit for RA packets is 64 by default.
- If the hop limit for RA packets is not set in the interface view, the value set using the **ipv6 nd hop-limit** command in the system view is used as the hop limit for RA packets.
- If the **ipv6 nd ra hop-limit** command is run in the interface view, the configuration in the interface view takes effect, no matter whether the hop limit is set in the system view.

The hop limit set for IPv6 unicast packets is the same as that set for RA packets. In the following cases, however, the hop limit for IPv6 unicast packets is 64, while the hop limit for RA packets is 0.

- No hop limit is set for IPv6 unicast packets. The default value takes effect.
- The **undo ipv6 nd hop-limit** command is run to restore the default hop limit set for IPv6 unicast packets.

After a host receives an RA packet with the hop limit of 0, it sets its hop limit to the default value 64, consistent with the default hop limit on the device.

Example

Set the hop limit for IPv6 unicast packets initially sent by a device to 100.

```
<HUAWEI> system-view
[HUAWEI] ipv6 nd hop-limit 100
```

6.10.42 ipv6 nd learning strict

Function

The **ipv6 nd learning strict** command enables IPv6 neighbor discovery (ND) strict learning.

The **undo ipv6 nd learning strict** command disables IPv6 ND strict learning.

By default, IPv6 ND strict learning is disabled.

Format

In the system view:

ipv6 nd learning strict

undo ipv6 nd learning strict

In the interface view:

ipv6 nd learning strict { **force-disable** | **force-enable** | **trust** }

undo ipv6 nd learning strict

Parameters

Parameter	Description	Value
force-disable	Disables IPv6 ND strict learning forcibly.	-
force-enable	Enables IPv6 ND strict learning forcibly.	-
trust	Inherits the global setting of IPv6 ND strict learning.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, Eth-Trunk sub-interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a device uses neighbor advertisement (NA) packets to establish neighbor entries. Run the **ipv6 nd learning strict** command to enable IPv6 ND strict learning. After you enable IPv6 ND strict learning on a device, the device uses NA packets only in response to neighbor solicitation (NS) packets to establish neighbor entries.

Prerequisites

Before using the **ipv6 nd learning strict** command to enable IPv6 neighbor discovery (ND) strict learning on an interface, ensure that the IPv6 function has been enabled on the interface using the **ipv6 enable** command.

Precautions

Before running this command in an Eth-Trunk view, run the **undo portswitch** command to switch the Eth-Trunk to a Layer 3 interface. For the models supporting switching between Layer 2 and Layer 3 modes, see **portswitch**.

After you run the **ipv6 nd learning strict** command on a device, the device synchronizes fake entries. Synchronizing a large number of fake entries affects device performance. Therefore, you are advised to use the command only for protocol consistency tests.

Example

Enable IPv6 ND strict learning globally.

```
<HUAWEI> system-view
[HUAWEI] ipv6 nd learning strict
```

Enable IPv6 ND strict learning on VLANIF 100 forcibly.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd learning strict force-enable
```

6.10.43 ipv6 nd link-local-entry-learn enable

Function

The **ipv6 nd link-local-entry-learn enable** command enables the device to learn the ND entry containing the link-local address of a peer interface.

The **undo ipv6 nd link-local-entry-learn enable** command disables the device from learning the ND entry containing the link-local address of a peer interface.

By default, the device is disabled from learning the ND entry containing the link-local address of a peer interface.

Format

ipv6 nd link-local-entry-learn enable

undo ipv6 nd link-local-entry-learn enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, on a network where IPv6 routes are learnt through RIPng, a device can learn the link-local address of a peer interface only through packets. If a device does not learn the link-local address of a peer interface but needs to forward a packet with the next hop being this address, the packet will be lost.

The **ipv6 nd link-local-entry-learn enable** command helps solve this issue. With this command run on a device on a RIPng network, the device learns the ND entry containing the link-local address of a peer interface, when it learns the ND entry containing the global unicast address of the peer interface. If you do not require this function, you are advised to disable this function to reduce the memory occupied by ND entries.

Example

Enable the device to learn the ND entry containing the link-local address of a peer interface.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ipv6 nd link-local-entry-learn enable
```

6.10.44 ipv6 nd neighbor-limit

Function

The **ipv6 nd neighbor-limit** command configures the maximum number of dynamic neighbor entries that can be learned by an interface.

The **undo ipv6 nd neighbor-limit** command restores the default maximum number of dynamic neighbor entries that can be learned by an interface.

By default, the maximum of dynamic neighbor entries that an interface can learn is 212 for the S300, 1748 for the S500, 1000 for the SS1720GW-E, S1720GWR-E, S5720-LI, and S5720S-LI, 1024 for the S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, and S5735S-L-M, 2048 for the S5720I-SI, and 3072 for the S5735-S, S5735-S-I, and S5735S-S, 8192 for the S5731-S, S5731S-S, and 64000 for the 65536 for the S5731S-H and S5731-H, 10240 for the S5735S-H, S5736-S and 49152 for the S6720-EI, S6735-S and S6720S-EI, and 32768 for the S5732-H, S6730-S, S6730-H, S6730S-H, and S6730S-S.

Format

ipv6 nd neighbor-limit *limit-number*

undo ipv6 nd neighbor-limit

Parameters

Parameter	Description	Value
limit-number	Specifies the maximum number of dynamic neighbor entries that can be learned by a specified interface.	The value is an integer. ● The value ranges from 2 to 212 for the S300. ● The value ranges from 2 to 1748 for the S500. ● The value ranges from 2 to 1000 for the SS1720GW-E, S1720GWR-E, S5720-LI, and S5720S-LI. ● The value ranges from 2 to 1024 for the S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, and S5735S-L-M. ● The value ranges from 2 to 2048 for the S5720I-SI. ● The value ranges from 2 to 3072 for the S5735-S, S5735-S-I, and S5735S-S. ● The value ranges from 2 to 8192 for the S5731-S, and S5731S-S. ● The value ranges from 2 to 65536 for the S5731S-H and S5731-H. ● The value ranges from 2 to 10240 for the S5735S-H, S5736-S. ● The value ranges from 2 to 49152 for the S6720-EI, S6735-S and S6720S-EI. ● The value ranges from 2 to 32768 for the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H.

Views

VLANIF interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface learns too many neighbor entries, the processing load for the device will be increased and the performance of the device will be degraded. You can run the **ipv6 nd neighbor-limit** command to configure the maximum number of dynamic neighbor entries that can be learned by a specified interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command.

Example

Set the maximum number of dynamic neighbor entries that can be learned by the VLANIF100 interface to 10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd neighbor-limit 10
```

6.10.45 ipv6 nd ns multicast-enable

Function

The **ipv6 nd ns multicast-enable** command enables a termination sub-interface to send NS multicast packets.

The **undo ipv6 nd ns multicast-enable** command disables a termination sub-interface from sending NS multicast packets.

By default, a termination sub-interface is disabled from sending NS multicast packets.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv6 nd ns multicast-enable

undo ipv6 nd ns multicast-enable

Parameters

None

Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A termination sub-interface can send NS multicast packets to actively learn ND entries or respond to NS packets to passively learn ND entries.

When a termination sub-interface needs to send multicast NS packets to learn ND entries but there is no corresponding ND entry, you need to run this command to enable a termination sub-interface to send NS multicast packets.

Prerequisites

Run the **ipv6 enable** command in the sub-interface view to enable IPv6 on a termination sub-interface.

Run the **dot1q termination vid** command in the sub-interface view to set the single VLAN ID for Dot1q termination. Or run the **qinq termination pe-vid ce-vid** command in the sub-interface view to configure a QinQ termination sub-interface to terminate double VLAN tags.

Precautions

- If this command is not run on the termination sub-interface, the system discards the NS multicast packets.
- If this command is run on the termination sub-interface, the system tags an NS multicast packet and forwards it through the termination sub-interface.

Sending multicast NS packets consumes CPU resources. Therefore, when the CPU performance of the system is rather low, you are advised not to enable a termination sub-interface to send NS multicast packets to actively learn ND entries but to respond to NS packets to passively learn ND entries.

VLAN termination sub-interfaces cannot be created on a VCMP client. You can run the **vcmp role** command to configure the role for a switch in a VCMP domain.

Example

Enable the Dot1q termination sub-interface GigabitEthernet0/0/1.1 to send NS multicast packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1.1] dot1q termination vid 100
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 nd ns multicast-enable
```

6.10.46 ipv6 nd ns retrans-timer

Function

The **ipv6 nd ns retrans-timer** command sets the interval for sending NS packets.

The **undo ipv6 nd ns retrans-timer** command restores the interval for sending NS packets to the default value.

By default, the interval for sending NS packets is 1000 ms.

Format

ipv6 nd ns retrans-timer *interval*

undo ipv6 nd ns retrans-timer

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NS packets.	The value is an integer that ranges from 1000 to 4294967295, in milliseconds. The default value is 1000 milliseconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting the interval for sending NS packets provides the following functions:

- Controlling the interval at which a local routing device detects neighbor reachability.
- Controlling the interval at which a local routing device performs DAD.
- Functioning as a parameter in an RA packet to instruct hosts to specify this interval as their own interval for sending NS packets.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Frequently sending NS packets causes high CPU usage, which affects the system performance. Therefore, you are advised to set the interval for sending NS packets to a larger value. The default interval, 1000 milliseconds, is recommended.

If you run the **ipv6 nd ns retrans-timer** command multiple times, only the latest configuration takes effect.

The interval for sending NS packets is the same as that for sending RA packets. In the following cases, however, the interval for sending NS packets is the default value1000 ms, while the interval for sending RA packets is 0 ms.

- No interval for sending NS packets is set. The default value takes effect.
- The **undo ipv6 nd ns retrans-timer** command is run to restore the interval for sending NS packets to the default value.

After a host receives an RA packet of which the sending interval is 0 ms from a device, the host sets the interval for sending NS packet to 1000 ms, the same as that on the device.

Example

Set the interval for sending NS packets to 10000 milliseconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ns retrans-timer 10000
```

Set the interval for sending NS packets to 10000 milliseconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ns retrans-timer 10000
```

6.10.47 ipv6 nd nud reachable-time

Function

The **ipv6 nd nud reachable-time** command sets the IPv6 neighbor reachable time.

The **undo ipv6 nd nud reachable-time** command restores the IPv6 neighbor reachable time to the default value.

By default, the IPv6 neighbor reachable time is 30000 ms.

Format

ipv6 nd nud reachable-time *value*

undo ipv6 nd nud reachable-time

Parameters

Parameter	Description	Value
value	Specifies the IPv6 neighbor reachable time.	The value is an integer that ranges from 1 to 3600000, in milliseconds. The default value is 30000 ms, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting the IPv6 neighbor reachable time provides the following functions:

- Controlling the aging time of neighbor entries on a local routing device.
- Being a parameter in an RA packet to enable a host to configure the neighbor reachable time.

Each RA packet sent by a routing device carries the neighbor reachable time. This allows all nodes along the same link to use the same neighbor reachable time.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

A shorter neighbor reachable time enables a routing device to detect neighbor reachability more quickly. However, this consumes more network bandwidth and CPU resources. Therefore, a short neighbor reachable time is not recommended on an IPv6 network. The default value, 30000 ms, is recommended.

If you run the **ipv6 nd nud reachable-time** command multiple times, only the latest configuration takes effect.

The neighbor reachable time set on a routing device is the same as that carried in an RA packet. In the following cases, however, the neighbor reachable time set on a routing device is the default value 30000 ms while the neighbor reachable time carried in the RA packet is 0 millisecond:

- No neighbor reachable time is set on the routing device. The default value takes effect.
- The **undo ipv6 nd nud reachable-time** command is run to restore the neighbor reachable time to the default value.

After a host receives an RA packet in which the neighbor reachable time is 0 ms, the host sets the neighbor reachable time to 30000 ms, the same as that on the device.

Example

Set the neighbor reachable time to 10000 ms on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd nud reachable-time 10000
```

Set the neighbor reachable time to 10000 ms on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd nud reachable-time 10000
```

6.10.48 ipv6 nd proxy inner-access-vlan enable

Function

The **ipv6 nd proxy inner-access-vlan enable** command enables intra-VLAN ND proxy on a VLANIF interface.

The **undo ipv6 nd proxy inner-access-vlan enable** command disables intra-VLAN ND proxy on a VLANIF interface.

By default, intra-VLAN ND proxy is disabled.

Format

ipv6 nd proxy inner-access-vlan enable

undo ipv6 nd proxy inner-access-vlan enable

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

On an IPv6 network, if port isolation is configured in a VLAN, users in the VLAN cannot communicate with each other. Configure intra-VLAN ND proxy on the VLAN-associated interface to enable Layer 3 communication among users.

Prerequisites

In the VLANIF interface view:

1. Run the **ipv6 enable** command to enable the IPv6 function.
1. Run the **ipv6 address** command to configure an IPv6 address for the interface. The IPv6 address must be in the same network segment as the IPv6 addresses of all hosts in the VLAN.

Example

Enable intra-VLAN ND proxy on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address fc00::1/64
[HUAWEI-Vlanif100] ipv6 nd proxy inner-access-vlan enable
```

6.10.49 ipv6 nd proxy inter-access-vlan enable

Function

The **ipv6 nd proxy inter-access-vlan enable** command enables inter-VLAN ND proxy on a VLANIF interface.

The **undo ipv6 nd proxy inter-access-vlan enable** command disables inter-VLAN ND proxy on a VLANIF interface.

By default, inter-VLAN ND proxy is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S supports this command.

Format

ipv6 nd proxy inter-access-vlan enable

undo ipv6 nd proxy inter-access-vlan enable

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

In a VLAN aggregation scenario on an IPv6 network, if hosts in different sub-VLANs need to communicate at Layer 3, enable inter-VLAN ND proxy on the VLANIF interface corresponding to the super-VLAN. In this way, all sub-VLANs in the super-VLAN are reachable to each other.

Prerequisites

In the VLANIF interface view:

1. Run the **ipv6 enable** command to enable the IPv6 function.
2. Run the **ipv6 address** command to configure an IPv6 address for the interface. The IPv6 address must be in the same network segment as the IPv6 addresses of all sub-VLAN hosts.

Example

Configure inter-VLAN ND proxy on VLANIF 30, the VLANIF interface corresponding to super-VLAN 30.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 30
[HUAWEI-Vlanif30] ipv6 enable
[HUAWEI-Vlanif30] ipv6 address fc00::1/64
[HUAWEI-Vlanif30] ipv6 nd proxy inter-access-vlan enable
```

6.10.50 ipv6 nd ra

Function

The **ipv6 nd ra** command sets the interval for sending Router Advertisement packets.

The **undo ipv6 nd ra** command restores the interval for sending RA packets to the default value.

By default, the maximum interval is 600s and the minimum interval is 200s.

NOTE

If *min-interval* is not specified, the minimum interval varies depending on the maximum interval specified by *max-interval* (the minimum is 1/3 of the maximum). If *min-interval* is specified, the minimum interval is the value configured.

Format

ipv6 nd ra { **max-interval** *maximum-interval* | **min-interval** *minimum-interval* }

undo ipv6 nd ra { **max-interval** | **min-interval** }

Parameters

Parameter	Description	Value
max-interval *maximum-interval*	Specifies the maximum interval for sending RA packets.	The value is an integer that ranges from 4 to 1800, in seconds. The default value is 600 seconds, which is recommended. The maximum interval cannot be less than the minimum interval.
min-interval *minimum-interval*	Specifies the minimum interval for sending RA packets.	The value is an integer that ranges from 3 to 1350, in seconds. The default value is 200 seconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A routing device periodically sends RA packets. An RA packet carries both the IPv6 address prefix and the flag of stateful address autoconfiguration.

You can run the **ipv6 nd ra** command to change the interval for sending RA packets. To reduce the number of RA messages being transmitted on a link, you can set a longer interval. To speed up router discovery, you can set a shorter interval.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Running the **ipv6 nd ra** command changes the interval for sending RA packets during DAD. Therefore, you are advised to use the default interval, that is, the maximum value is 600s and the minimum value is 200s.

If the **ipv6 nd ra** command is run multiple times, the latest configuration takes effect.

The interval for sending RA packets cannot be longer than the lifetime of the RA packets. The default lifetime of the RA packets is 1800s and, you can run the **ipv6 nd ra router-lifetime** command to change the value.

The actual interval for sending RA packets is a random value between *min-interval* and *max-interval*.

Example

Set the maximum interval for sending RA packets to 1000s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra max-interval 1000
```

Set the maximum interval for sending RA packets to 1000s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra max-interval 1000
```

Set the minimum interval for sending RA packets to 300s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra min-interval 300
```

Set the minimum interval for sending RA packets to 300s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra min-interval 300
```

6.10.51 ipv6 nd ra dns-server

Function

The **ipv6 nd ra dns-server** command configures a DNS server address for RA packets.

The **undo ipv6 nd ra dns-server** command deletes the DNS server address configured for RA packets.

By default, RA packets do not contain a DNS server address.

Format

ipv6 nd ra dns-server *ipv6-address* [*valid-lifetime*]

undo ipv6 nd ra dns-server [*ipv6-address* [*valid-lifetime*]]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a DNS server.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
valid-lifetime	Specifies a valid lifetime.	The value is an integer ranging from 1 to 4294967295, in seconds. The default value is three times the maximum interval for advertising RA packets. The maximum interval for advertising RA packets can be configured using the **ipv6 nd ra max-interval** *maximum-interval* command.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where IPv6 ND stateless address auto-configuration is used or DHCPv6 is not configured, run the **ipv6 nd ra dns-server** command to configure a DNS server address for RA packets so that the host can implement the DNS service using the DNS server address in RA packets.

Prerequisites

The IPv6 function has been enabled on an interface using the **ipv6 enable** command in the interface view.

Precautions

A maximum of eight DNS server addresses can be configured for the RA packets transmitted on the same interface.

Example

Configure a DNS server address for the RA packets transmitted on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra dns-server 2001:db8:1::2 1000
```

6.10.52 ipv6 nd ra dns-suffix

Function

The **ipv6 nd ra dns-suffix** command sets a DNS suffix in RA packets.

The **undo ipv6 nd ra dns-suffix** command deletes the DNS suffix configured for RA packets.

By default, RA packets do not contain a DNS suffix.

Format

ipv6 nd ra dns-suffix *domain-suffix* [*valid-lifetime*]

undo ipv6 nd ra dns-suffix [*domain-suffix* [*valid-lifetime*]]

Parameters

Parameter	Description	Value
domain-suffix	Specifies a DNS suffix.	The value is a string of 1 to 64 characters and can contain digits, letters, hyphens (-), underscores (_), and periods (.), but not spaces.

Parameter	Description	Value
valid-lifetime	Specifies a valid lifetime.	The value is an integer ranging from 1 to 4294967295, in seconds. The default value is three times the maximum interval for advertising RA packets. The maximum interval for advertising RA packets can be configured using the **ipv6 nd ra max-interval** *maximum-interval* command.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a host use a DNS domain name with a suffix upon receipt of RA packets, run the **ipv6 nd ra dns-suffix** command to configure a DNS suffix for RA packets.

Prerequisites

The IPv6 function has been enabled on an interface using the **ipv6 enable** command in the interface view.

Precautions

Only one DNS suffix can be configured for the RA packets transmitted on the same interface. If the **ipv6 nd ra dns-suffix** command is run more than once for the same interface, the latest configuration overrides the previous one.

Example

Configure a DNS suffix for the RA packets transmitted on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra dns-suffix example.com 1000
```

6.10.53 ipv6 nd ra halt

Function

The **ipv6 nd ra halt** command disables the system from sending RA packets.

The **undo ipv6 nd ra halt** command enables the system to send RA packets.

By default, the system is disabled from sending RA packets.

Format

ipv6 nd ra halt

undo ipv6 nd ra halt

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When a device is connected to a host, it periodically sends RA packets to the host. An RA packet carries the IPv6 address prefix and flag information of stateful autoconfiguration. You can run the **undo ipv6 nd ra halt** command to enable the device to send RA packets.
- When a device is connected to another device, that is, there is no host on the network, sending RA packets is not required. The default configuration is recommended.

Prerequisites

The IPv6 function has been enabled in the interface view using the **ipv6 enable** command.

Precautions

After the **ipv6 nd ra halt** command is run, the device does not send RA packets. In such a case, the hosts on the network cannot periodically receive information about updated IPv6 prefixes.

You can run the **display icmpv6 statistics** command to check whether a local device has sent RA packets.

Example

Disable VLANIF100 from sending RA packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra halt
```

Disable GE0/0/1 from sending RA packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra halt
```

6.10.54 ipv6 nd ra hop-limit

Function

The **ipv6 nd ra hop-limit** command sets the hop limit for RA packets.

The **undo ipv6 nd ra hop-limit** command restores the hop limit for RA packets to the default value.

By default, the hop limit for RA packets is 64.

Format

ipv6 nd ra hop-limit *limit*

undo ipv6 nd ra hop-limit

Parameters

Parameter	Description	Value
limit	Specifies the hop limit for RA packets.	The value is an integer that ranges from 0 to 255. The default value is 64, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a parameter in an RA packet, the hop limit enables a host to automatically configure a hop limit (a limit on the number of hops through which IPv6 unicast packets initially sent by a host are allowed to travel).

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After this command is run on the switch, the device discards the RA packet whose hop limit is different from its configuration.

- If the **ipv6 nd ra hop-limit** command is run on an interface, the hop limit for RA packets is determined by the interface configuration.
- If the **ipv6 nd ra hop-limit** command is not run on an interface, the hop limit for RA packets is determined by the hop limit configured using the **ipv6 nd hop-limit** command.

Example

Set the hop limit for RA packets sent by VLANIF100 to 126.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra hop-limit 126
```

Set the hop limit for RA packets sent by GE0/0/1 to 126.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra hop-limit 126
```

6.10.55 ipv6 nd ra preference

Function

The **ipv6 nd ra preference** command configures the default router priority value in the RA packets.

The **undo ipv6 nd ra preference** command restores the default router priority value in RA packets to be the default value.

By default, the router priority of RA packets is medium.

Format

ipv6 nd ra preference { **high** | **medium** | **low** }

undo ipv6 nd ra preference

Parameters

Parameter	Description	Value
high	Specifies the default router priority to be high.	-
medium	Specifies the default router priority to be medium.	-
low	Specifies the default router priority to be low.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If there are multiple switches on the links connected to a host, the host needs to select suitable switches based on different destination addresses of the packets to be forwarded. Each switch advertises its default router priority and specific route information to the host so that the host can enhance its own capability of selecting suitable forwarding switches based on different IP addresses of the packets to be forwarded.

After receiving an RA message that contains the default router priority, the host updates its own default router list. If the host does not have any route to select when sending packets to other devices, the host will search the updated router list for the switch with the highest priority. If the switch with the highest priority becomes faulty, the host selects another switch in descending order of priority.

To set a default router priority in RA messages, run the **ipv6 nd ra preference** command. This setting allows the switch with the highest priority to function as the gateway for hosts.

Prerequisites

Before running this command, run the **ipv6 enable** command on the interface view to enable the IPv6 function.

By default, the switch does not advertise RA packets. Therefore, to allow the default router priority to be advertised to the host, you need to run the **undo ipv6 nd ra halt** command to enable the function of advertising RA packets for the device.

Precautions

If the system is deleting the binding relationship between an interface and an IPv6 address family VPN instance, you are prompted not to run the **ipv6 nd ra preference** command.

Example

Configure the default router priority value in RA packets on VLANIF100 to be high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra preference high
```

Configure the default router priority value in RA packets on GE0/0/1 to be high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
```

```
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 nd ra halt
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra preference high
```

6.10.56 ipv6 nd ra prefix

Function

The **ipv6 nd ra prefix** command configures the prefix in an RA packet.

The **undo ipv6 nd ra prefix** command deletes the prefix in an RA packet.

By default, an RA packet carries only the address prefix configured using the **ipv6 address** command.

Format

ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig**] [**off-link**]

undo ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

ipv6 nd ra prefix default no-advertise

undo ipv6 nd ra prefix default no-advertise

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address carried in the RA packet.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128. You can calculate the IPv6 prefix carried in the RA packet based on the IPv6 address and prefix length. When stateless autoconfiguration is used, specify the length of address prefix as 64; otherwise, the address will be invalid and RA packets are discarded.

Parameter	Description	Value
valid-lifetime	Specifies the valid lifetime of the prefix. The valid lifetime decides the prefix on-link status.	The value is an integer that ranges from 0 to 4294967295, in seconds.
preferred-lifetime	Specifies the preferred lifetime of the prefix. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred. The preferred lifetime cannot be larger than the valid lifetime.	The value is an integer that ranges from 0 to 4294967295, in seconds.
no-autoconfig	Deletes the A-Flag. If **no-autoconfig** is specified, a configured prefix cannot be used in stateless address allocation. A-Flag indicates the autonomous address configuration in the prefix option of RA packet.	-
off-link	Specifies the L-Flag. If **off-link** is specified, indicates that this prefix can be used for on-link determination. When **off-link** is not specified, the advertisement makes no statement about on-link or off-link properties of the prefix. In other words, if the L flag is not set a host MUST NOT conclude that an address derived from the prefix is off-link. That is, it MUST NOT update a previous indication that the address is on-link.	-
default no-advertise	Specifies that RA packets do not carry the default prefix generated based on the interface IPv6 address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a prefix has been configured using the **ipv6 nd ra prefix** command, the device advertises both prefixes configured using the **ipv6 nd ra prefix** and **ipv6 address** commands.

By default, RA packets carry the default prefix generated based on the interface IPv6 address. If the default setting is not required, run the **ipv6 nd ra prefix default no-advertise** command.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After a host receives the RA packet with the prefix configured using the **ipv6 nd ra prefix** command, the host updates the local prefix information.

The prefix configured using the **ipv6 nd ra prefix** command cannot be fe80:: (prefix of a link-local address), ff00:: (prefix of a multicast address), :: (prefix of an unspecified address), or the prefix that has been used by another interface (including the interface address prefix and prefix carried in RA packets).

The prefix configuring using the **ipv6 nd ra prefix** command takes precedence over the default prefix generated based on the interface IPv6 address. An RA message can carry a maximum of 10 prefixes. If exactly 10 prefixes have been manually configured, the default prefix will not be carried.

In the DHCPv6 stateful address autoconfiguration scenario, the lifetime of the PD prefixes advertised in RA packets is the default value defined in DHCPv6. If the prefixes in RA packets remain unchanged, you can run the **ipv6 nd ra prefix** command to configure static prefixes and specify their lifetime. If the prefixes in RA packets change, you need to specify the lifetime of the changed prefixes.

Example

Configure the prefix in the RA packet on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra prefix fc00:1::100 128 1000 400 no-autoconfig
[HUAWEI-Vlanif100] ipv6 nd ra prefix fc00:2::100 64 1000 400 off-link
```

Configure the prefix in the RA packet on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 nd ra halt
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra prefix fc00:1::100 128 1000 400 no-autoconfig
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra prefix fc00:2::100 64 1000 400 off-link
```

Configure RA packets on VLANIF100 not to carry the default prefix.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra prefix default no-advertise
```

6.10.57 ipv6 nd ra route-information

Function

The **ipv6 nd ra route-information** command configures route information in RA packets.

The **undo ipv6 nd ra route-information** command deletes route information in RA packets.

By default, there is no route information in RA packets.

Format

ipv6 nd ra route-information *ipv6-address prefix-length* **lifetime** *route-lifetime* [**preference** { **high** | **medium** | **low** }]

undo ipv6 nd ra route-information *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address.	The prefix is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
lifetime *route-lifetime*	Specifies the lifetime of a route.	The value is an integer ranging from 0 to 4294967295, in seconds.
preference	Specifies the priority of a route.	-
high	Specifies the route priority to be high.	-
medium	Specifies the route priority to be medium.	-
low	Specifies the route priority to be low.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RA packet includes route information. The switch sends the specified routes to the hosts on the local network segment by using this information. The hosts can send packets by using these routes.

When receiving the RA packets carrying route information, a host updates its routing table. When sending the RA packets to another device, a host queries the routing table and selects proper route for sending packets.

Prerequisites

Before running this command, run the **ipv6 enable** command on the interface view to enable the IPv6 function of an interface.

By default, the switch does not send RA packets. Therefore, to send the routes to the host, you need to run the **undo ipv6 nd ra halt** command to enable the function of advertising RA packets for the device.

Precautions

A maximum of 17 route options are supported on each interface.

When this command is to be run, the value of *ipv6-address* cannot be a loopback address.

Example

Configure the route information of RA packets on VLANIF100: The lifetime of the route with the destination address of 2001:db8::2/64 is 1550 seconds, and the priority of this route is high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra route-information 2001:db8::2 64 lifetime 1550 preference high
```

Configure the route information of RA packets on GE0/0/1: The lifetime of the route with the destination address of 2001:db8::2/64 is 1550 seconds, and the priority of this route is high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 nd ra halt
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra route-information 2001:db8::2 64 lifetime 1550 preference
high
```

6.10.58 ipv6 nd ra router-lifetime

Function

The **ipv6 nd ra router-lifetime** command sets the lifetime of RA packets.

The **undo ipv6 nd ra router-lifetime** command restores the lifetime of RA packets to the default value.

By default, the lifetime of an RA packet is 1800s.

Format

ipv6 nd ra router-lifetime *ra-lifetime*

undo ipv6 nd ra router-lifetime

Parameters

Parameter	Description	Value
ra-lifetime	Specifies the lifetime of RA packets.	The value is an integer and can be 0 or ranges from 4 to 9000, in seconds. The default value is 1800 seconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device adds the lifetime value to an RA packet before sending the RA packet to the host on the local network segment.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If a host receives an RA packet with the lifetime field being 0, the host does not add the address of the switch to its default router table.

The lifetime of the RA packets cannot be smaller than the interval for sending RA packets. By default, the maximum interval for sending RA packets is 600s and the minimum interval is 200s. You can run the **ipv6 nd ra** command to set the interval. If the set lifetime value of the RA packets is smaller than the set interval for sending RA packets, the system displays an error. In such a case, you need to reset the lifetime value.

Example

Set the lifetime of the RA packets on VLANIF100 to 1000s.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra router-lifetime 1000
```

Set the lifetime of the RA packets on GE0/0/1 to 1000s.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra router-lifetime 1000
```

6.10.59 ipv6 nd stale-timeout

Function

The **ipv6 nd stale-timeout** command sets the aging time of ND entries in STALE state.

The **undo ipv6 nd stale-timeout** command restores the aging time of ND entries in STALE state to the default value.

By default, the aging time of ND entries in STALE state is 1200s.

Format

ipv6 nd stale-timeout *timeout-value*

undo ipv6 nd stale-timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the aging time of ND entries in STALE state.	The value is an integer that ranges from 60 to 172800, in seconds. The default value is 1200s, which is recommended.

Views

System view, Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The STALE state of an ND entry indicates that whether the neighbor is reachable is unknown. A device does not detect the neighbor reachability unless packets need to be sent to a neighbor.

The aging time of ND entries in STALE state is configurable. To quickly clear invalid ND entries, set the aging time to a smaller value using the **ipv6 nd stale-timeout** command. This speeds up entry aging.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If the aging time is not configured on an interface, the aging time configured in system view is used for the interface. If the aging time is configured on an interface, the interface configuration takes effect.

After the **ipv6 nd stale-timeout** command is run, the status of ND entries can be updated after the aging time of ND entries in STALE state expires. That is, the new aging time configuration takes effect after the last aging time expires.

The system checks the validity of ND entries after the aging time of ND entries in STALE state expires. If the neighbor is reachable, the ND entry status changes to REACH; otherwise, the ND entry is deleted.

Example

Set the aging time of ND entries in STALE state to 3600s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd stale-timeout 3600
```

Set the aging time of ND entries in STALE state to 3600s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd stale-timeout 3600
```

6.10.60 ipv6 neighbor

Function

The **ipv6 neighbor** command configures static neighbor entries.

The **undo ipv6 neighbor** command deletes static neighbor entries.

By default, no static neighbor entry is configured.

Format

VLANIF interface view:

ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id interface-type interface-number*

undo ipv6 neighbor *ipv6-address*

Ethernet interface view, Eth-Trunk interface view, Ethernet sub-interface view, and Eth-Trunk sub-interface view:

ipv6 neighbor *ipv6-address mac-address* [**vid** *vlan-id* [**cevid** *cevid*]]

undo ipv6 neighbor *ipv6-address*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the command in Ethernet interface view and Ethernet sub-interface view.

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a static neighbor entry.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
mac-address	Specifies the MAC address of a static neighbor entry.	The value is in the H-H-H format. An H contains one to four hexadecimal numbers.
vid *vlan-id*	Specifies the ID of the outer VLAN to which the interface belongs.	The value is an integer that ranges from 1 to 4094.
cevid *cevid*	Specifies the ID of the inner VLAN to which the interface belongs.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Specifies the interface type and number of a physical interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To filter invalid packets, you can create static neighbor entries, binding the destination IPv6 addresses of these packets to nonexistent MAC addresses.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

A neighbor entry enters the REACHABLE state after being created, indicating that the interface connected to this neighbor is Up.

The static neighbor entries overwrite the neighbor entries dynamically learnt by device. That is, static neighbor entries are of higher priorities than dynamically learnt neighbor entries.

If the IPv6 address or MAC address specified in the **ipv6 neighbor** command is incorrect, communication with this neighbor fails.

Example

Configure static neighbor entries on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 neighbor fc00::1 00e0-fc12-3456 vid 2 gigabitethernet 0/0/1
```

Configure static neighbor entries on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 neighbor fc00::1 00e0-fc12-3456
```

6.10.61 ipv6 packet-too-big drop

Function

The **ipv6 packet-too-big drop** configures the switch to discard packets with the length larger than the IPv6 MTU of the outbound interface, and enables IPv6 PMTU discovery.

The command **undo ipv6 packet-too-big drop** restores the default policy for processing packets with the length larger than the IPv6 MTU of the outbound interface.

By default, the switch properly forwards packets with the length larger than the IPv6 MTU of the outbound interface and IPv6 PMTU discovery is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv6 packet-too-big drop

undo ipv6 packet-too-big drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch functions as an intermediate node on an IPv6 network, you can configure the **ipv6 packet-too-big drop** command to discard packets with the length larger than the IPv6 MTU of the outbound interface and enable IPv6 PMTU discovery.

In an IPv4 network, oversized packets need to be fragmented. When a transit device receives a packet exceeding the maximum transmission unit (MTU) size of its outbound interface from a source node, the transit device fragments the packet before forwarding it to the destination node. In an IPv6 network, however, only the source node can fragment packets, which reducing pressure on transit devices. When an interface on a transit device receives a packet whose size exceeds the MTU, the transit device discards the packet and sends an ICMPv6 Packet Too Big message to the source node. The ICMPv6 Packet Too Big message contains the MTU value of the outbound interface. The source node fragments the packet based on the MTU and resends the packet, increasing traffic overhead. The Path MTU Discovery protocol dynamically discovers the MTU value of each link on the transmission path, reducing excessive traffic overhead.

The PMTU Discovery protocol is implemented through ICMPv6 Packet Too Big messages. A source node first uses the MTU of its outbound interface as the PMTU and sends a probe packet. If a smaller PMTU exists on the transmission path, the transit device sends a Packet Too Big message to the source node. The Packet Too Big message contains the MTU value of the outbound interface on the transit device. After receiving this message, the source node changes the PMTU value to the received MTU value and sends packets based on the new MTU. This process repeats until packets are sent to the destination address. The source node obtains the PMTU of the destination address.

Precautions

The switch supports IPv6 MTU discovery, but does not support IPv6 packet fragmentation when it functions as an intermediate node. IPv6 packets can be fragmented only on source nodes.

Example

Configure the switch to discard packets with the length larger than the IPv6 MTU of the interface, and enable IPv6 PMTU discovery.

```
<HUAWEI> system-view
[HUAWEI] ipv6 packet-too-big drop
Warning: This operation will affect IPv6 traffic forwarding. Continue? [Y/N]:y
```

6.10.62 ipv6 pathmtu

Function

The **ipv6 pathmtu** command sets the PMTU for a specified destination IPv6 address.

The **undo ipv6 pathmtu** command deletes the PMTU for a specified destination IPv6 address.

Format

ipv6 pathmtu *ipv6-address* [**vpn-instance** *vpn-instance-name*] [*path-mtu*]

undo ipv6 pathmtu *ipv6-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for which a PMTU is to be set. **NOTE** The link-local address does not take effect.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance for which a PMTU is to be set.	The value must be an existing VPN instance name.
path-mtu	Specifies the path MTU, that is, the maximum size of IPv6 packets allowed to be sent along the path.	The value is an integer that ranges from 1280 to 10000, in bytes. The default value is 1500, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PMTU is used to determine the proper size of packets to be transmitted along the path from a source to a destination. Usually, a device fragments and forwards packets based on the dynamically learnt PMTU. Packets that are sent using this PMTU do not need to be fragmented during transmission. This reduces pressure on routing devices and optimizes network resource utilization to obtain the maximum throughput.

In some special cases, however, to protect devices on the network and avoid large-size packet attacks, you can run the **ipv6 pathmtu** command to set a static PMTU for the specified destination IPv6 address to control the maximum size of packets that can be transmitted between the source and the destination.

Precautions

On the path along which packets are transmitted, a node discards the received packets if its MTU is smaller than the PMTU of the received packets. Therefore, in most cases, dynamic PMTU learning is recommended unless there are security vulnerabilities on the network. You can use the default PMTU value instead of running the **ipv6 pathmtu** command to set a static PMTU.

Example

Set the PMTU of a specified IPv6 destination address to 1300 bytes.

```
<HUAWEI> system-view
[HUAWEI] ipv6 pathmtu fc00::12 1300
```

Set the PMTU of the address fc00::1 of the IPv6 VPN instance to 1600 bytes.

```
<HUAWEI> system-view
[HUAWEI] ipv6 pathmtu fc00::1 vpn-instance vpn6 1600
```

6.10.63 ipv6 pathmtu age

Function

The **ipv6 pathmtu age** command sets the aging time of dynamic PMTU entries.

The **undo ipv6 pathmtu age** command restores the aging time of dynamic PMTU entries to the default value.

By default, the aging time of dynamic PMTU entries is 10 minutes.

Format

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Parameters

Parameter	Description	Value
age-time	Specifies the aging time of dynamic specified PMTU entries.	The value is an integer that ranges from 10 to 100, in minutes. The default value is 10 minutes, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The lifetime of a dynamic PMTU entry can be changed by setting an aging time for dynamic PMTU entries.

To slow down PMTU aging, run the **ipv6 pathmtu age** command to set the aging time of dynamic PMTU entries to a larger value.

Precautions

This command changes only the aging time of dynamic PMTUs but not static PMTUs because static PMTU entries never age.

The priority of a static PMTU is higher than that of a dynamic PMTU. If the static PMTU exists, the dynamic PMTU does not take effect.

The aging time for the PMTU is valid only for the dynamic PMTU entries generated after this configuration, instead of the PMTU entries generated before this configuration.

Example

Set the aging time of dynamic PMTU entries to 40 minutes.

```
<HUAWEI> system-view
[HUAWEI] ipv6 pathmtu age 40
```

6.10.64 nd optimized-passby enable

Function

The **nd optimized-passby enable** command configures the device not to send NS packets destined for other devices to the CPU.

The **undo nd optimized-passby enable** command configures the device to send NS packets destined for other devices to the CPU.

By default, a device does not send NS packets destined for other devices to the CPU.

Format

nd optimized-passby enable

undo nd optimized-passby enable

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface receives a large number of NS packets whose destination IPv6 addresses are different from the IPv6 address of this interface and sends these NS packets to the CPU for processing, the CPU usage is high and the CPU cannot process services properly.

To prevent this issue, you can configure the device to directly forward NS packets destined for other devices without sending them to the CPU. This improves the device's capability of defending against packet attacks.

Precautions

If the **nd snooping enable** is executed in system view, or if IPv6 protocol is **Down** on the VLANIF interface, the configuration of disabling the device from sending NS packets destined for other devices to the CPU does not take effect on the VLANIF interface.

Example

Configure the device to send NS packets destined for other devices to the CPU.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo nd optimized-passby enable
```

6.10.65 nd optimized-reply disable

Function

The **nd optimized-reply disable** command disables the optimized ND reply function.

The **undo nd optimized-reply disable** command enables the optimized ND reply function.

By default, the optimized ND reply function is enabled.

Format

nd optimized-reply disable

undo nd optimized-reply disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stack functions as an access gateway, it receives a large number of ND Request packets that request the switch to reply with its local interface MAC address. If all these ND Request packets are sent to the master switch, the CPU usage of the master switch increases, and other services are affected.

The optimized ND reply function addresses this issue. After this function is enabled, the switch receiving an ND Request packet returns an ND Reply packet if the ND Request packet is destined for a local interface on the switch of the stack, and discards the ND Request packet if the packet is not destined for a local interface on the switch of the stack.

By default, the optimized ND reply function is enabled. After receiving an ND Request packet, the switch checks whether an ND entry corresponding to the source IPv6 address of the ND Request packet exists.

- If the corresponding ND entry exists and the packet information is the same as the saved ND entry information, the switch performs optimized ND reply to this ND Request packet.
- If the corresponding ND entry exists but the packet information differs from the saved ND entry information, the switch does not perform optimized ND reply to this ND Request packet.
- If the corresponding ND entry does not exist, the switch does not perform optimized ND reply to this ND Request packet.

Precautions

- The optimized ND reply function takes effect for ND Request packets sent by wireless users.

- The optimized ND reply function takes effect for ND Request packets received on VLANIF interfaces and VBDIF interfaces enabled with IPv6. VLANIF interfaces of Group VLANs and Separate VLANs in MUX VLANs, VLANIF interfaces of mapped VLANs, and VLANIF interfaces of super-VLANs do not perform optimized ND reply.
- If the number of global unicast IPv6 addresses on a VLANIF interface or VBDIF interface enabled with IPv6 exceeds 1, the switch does not perform optimized ND reply for NS packets received on this interface.
- If the ND snooping function is enabled on a switch, the switch does not perform optimized ND reply to received ND Request packets.
- The switch does not perform optimized ND reply to the following received packets:
  - NS packets with the source IPv6 address :: (that is, Duplicate Address Detection packets)
  - Packets with IPv6 extension headers

Example

Disable the optimized ND reply function.

```
<HUAWEI> system-view
[HUAWEI] nd optimized-reply disable
```

6.10.66 nd trap hash-conflict enable

Function

The **nd trap hash-conflict enable** command enables the trap function for hash conflicts of ND entries.

The **undo nd trap hash-conflict enable** command disables the trap function for hash conflicts of ND entries.

By default, the trap function for hash conflicts of ND entries is enabled.

Format

nd trap hash-conflict enable

undo nd trap hash-conflict enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the trap function for hash conflicts of ND entries is configured, the switch sends traps when a hash conflict of ND entries occurs so that you can obtain the status of ND entries promptly. ND entry resources are key resources on the switch. Monitoring the ND entry status effectively ensures proper running of the switch.

To improve the IPv6 forwarding performance, the switch saves ND entries using hash links. When multiple ND entries obtain the same key based on the hash algorithm, the ND entries cannot be saved. This is a hash conflict of ND entries.

When a hash conflict of ND entries occurs, the switch has available ND entry space but cannot save ND entries. The switch cannot forward IPv6 traffic matching the ND entries with a hash conflict.

You can enable the trap function for hash conflicts of ND entries to detect hash conflicts of ND entries promptly.

Example

Enable the trap function for hash conflicts of ND entries.

```
<HUAWEI> system-view
[HUAWEI] nd trap hash-conflict enable
```

6.10.67 nd trap hash-conflict history

Function

The **nd trap hash-conflict history** command sets the number of traps reported within each interval when a hash conflict of ND entries occurs.

The **undo nd trap hash-conflict history** command restores the default number of traps reported within each interval when a hash conflict of ND entries occurs.

By default, a switch reports a maximum of 10 traps within each interval when a hash conflict of ND entries occurs.

Format

nd trap hash-conflict history *history-number*

undo nd trap hash-conflict history

Parameters

Parameter	Description	Value
history-number	Specifies the number of traps reported within each interval when a hash conflict of ND entries occurs.	The value is an integer that ranges from 10 to 30. The default value is 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the trap function for hash conflicts of ND entries is enabled, the switch reports a maximum of 10 traps within 60 seconds by default. Each trap contains an IPv6 address that has a hash conflict.

If hash conflicts of more than 10 ND entries occur within an interval, traps for the eleventh and following ND entries that have hash conflicts cannot be reported. To solve this problem, you can run the **nd trap hash-conflict history** command to set the number of traps reported within each interval when a hash conflict of ND entries occurs.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Configure the switch to report a maximum of 15 traps within each interval when a hash conflict of ND entries occurs.

```
<HUAWEI> system-view
[HUAWEI] nd trap hash-conflict history 15
```

6.10.68 nd trap hash-conflict interval

Function

The **nd trap hash-conflict interval** command sets the interval at which the switch reports traps when a hash conflict of ND entries occurs.

The **undo nd trap hash-conflict interval** command restores the default interval at which the switch reports traps when a hash conflict of ND entries occurs.

By default, a switch reports traps at an interval of 60 seconds when a hash conflict of ND entries occurs.

Format

nd trap hash-conflict interval *interval-time*

undo nd trap hash-conflict interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which the switch reports traps when a hash conflict of ND entries occurs.	The value is an integer that ranges from 30 to 3600, in seconds. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the trap function for hash conflicts of ND entries is enabled, the switch reports a maximum of 10 traps within 60 seconds by default. Each trap contains an IPv6 address that has a hash conflict.

If the trap report interval is set to a small value, the switch reports traps for hash conflicts of ND entries more promptly. When many hash conflicts of ND entries occur, the switch reports a lot of traps.

If the trap report interval is set to a large value, the switch reports traps for hash conflicts of ND entries less promptly. When many hash conflicts of ND entries occur, the switch suppresses traps to be reported.

You can run the **nd trap hash-conflict interval** command to adjust the trap report interval based on actual requirements.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Configure the switch to report traps at an interval of 90 seconds when a hash conflict of ND entries occurs.

```
<HUAWEI> system-view
[HUAWEI] nd trap hash-conflict interval 90
```

6.10.69 nd-miss message-cache disable

Function

The **nd-miss message-cache disable** command disables the ND Miss message sending function.

The **undo nd-miss message-cache disable** command enables the ND Miss message sending function.

By default, the ND Miss message sending function is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

nd-miss message-cache disable

undo nd-miss message-cache disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a user sends an IPv6 packet with an irresolvable destination IPv6 address to the device (that is, if the device has a route to the destination IPv6 address of the IPv6 packet but has no ND entry matching the next hop of the route), the device generates an ND Miss message. By default, the device sends the ND Miss messages to the CPU. This improves the efficiency of processing the ND Miss messages.

When the ND Miss message sending function is enabled, a device cannot reply to ICMPv6 host unreachable packets. To enable the device to reply to ICMPv6 host unreachable packets, you can run the **nd-miss message-cache disable** command to disable the ND Miss message sending function.

Example

Disable the ND Miss message sending function.

```
<HUAWEI> system-view
[HUAWEI] nd-miss message-cache disable
```

6.10.70 reset ipv6 attack-source overlapping-fragment

Function

The **reset ipv6 attack-source overlapping-fragment** command clears statistics on overlapping fragment attack packets.

Format

reset ipv6 attack-source overlapping-fragment

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After overlapping fragment attack packets are processed manually, run the **reset ipv6 attack-source overlapping-fragment** command to clear statistics on overlapping fragment attack packets.

Example

Clear statistics on IPv6 overlapping fragment attack packets.

```
<HUAWEI> reset ipv6 attack-source overlapping-fragment
```

6.10.71 reset ipv6 neighbors

Function

The **reset ipv6 neighbors** command clears neighbor entries.

Format

reset ipv6 neighbors { **all** | **dynamic** | **static** | **vid** *vlan-id* [*interface-type interface-number*] | *interface-type interface-number* [**dynamic** | **static**] }

Parameters

Parameter	Description	Value
all	Clears neighbor entries on all interfaces.	-
dynamic	The first **dynamic** indicates that dynamic neighbor entries on all interfaces are cleared. The second **dynamic** indicates that dynamic neighbor entries on the current interface are cleared.	-

Parameter	Description	Value
static	The first **static** indicates that static neighbor entries on all interfaces are cleared. The second **static** indicates that static neighbor entries on the current interface are deleted.	-
vid *vlan-id*	Clears neighbor entries of a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Clears all neighbor entries on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of neighbor entries exceeds the upper limit, run the **reset ipv6 neighbors** command to clear excessive neighbor entries.

Precautions

The **reset ipv6 neighbors** command clears specified neighbor entries, which affects IPv6 packet forwarding. Therefore, confirm your action before running this command.

Example

Clear all neighbor entries on all interfaces.

```
<HUAWEI> reset ipv6 neighbors all
Warning: This operation will delete all static and dynamic IPv6 ND entries and the configurations of all
static IPv6 ND. Continue?[Y/N]:y
```

Clear all neighbor entries on the specified interface VlANIF 10.

```
<HUAWEI> reset ipv6 neighbors vlanif 10
```

6.10.72 reset ipv6 pathmtu

Function

The **reset ipv6 pathmtu** command clears PMTU entries.

Format

reset ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { **all** | **dynamic** | **static** }

Parameters

Parameter	Description	Value
all	Clears all PMTU entries in the cache.	-
dynamic	Clears all dynamic PMTU entries in the cache.	-
static	Clears all static PMTU entries in the cache.	-
vpn-instance *vpn-instance-name*	Clears all PMTU entries of a specified IPv6 VPN instance.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect statistics on PMTU entries within a specified period, use the **reset ipv6 pathmtu** command to clear the existing statistics on PMTU entries before running the **display ipv6 pathmtu** command to check information about PMTU entries.

Precautions

The **reset ipv6 pathmtu all** command clears all PMTU entries. Therefore, confirm your action before running this command.

Example

Clear all PMTU entries.

```
<HUAWEI> reset ipv6 pathmtu all
Warning: This operation will reset all static and dynamic IPv6 PMTU entries, and clear the configurations of
all static IPv6 PMTU, continue?[Y/N]:y
```

6.10.73 reset ipv6 socket pktsort

Function

The **reset ipv6 socket pktsort** command clears statistics on the dual receive buffer of an IPv6 socket.

Format

reset ipv6 socket pktsort task-id *task-id* **socket-id** *socket-id*

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a task.	The value is an integer and the range depends on the task configuration.
socket-id *socket-id*	Specifies the ID of a socket.	The value is an integer that ranges from 1 to 131072.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics on the dual receive buffer of an IPv6 socket and the count restarts. Therefore, confirm your action before running this command.

Example

Clear statistics on the dual receive buffer of the IPv6 socket with the task ID 2 and the socket ID 4.

```
<HUAWEI> reset ipv6 socket pktsort task-id 2 socket-id 4
```

6.10.74 reset ipv6 statistics

Function

The **reset ipv6 statistics** command clears IPv6 traffic statistics.

Format

reset ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect IPv6 traffic statistics within a specified period, clear the existing IPv6 traffic statistics before running the **display ipv6 statistics** command to display IPv6 traffic statistics.

Precautions

The **reset ipv6 statistics** command clears the specified IPv6 traffic statistics. Therefore, confirm your action before running this command.

Example

Clear IPv6 traffic statistics.

```
<HUAWEI> reset ipv6 statistics
```

6.10.75 reset nd optimized-reply statistics

Function

The **reset nd optimized-reply statistics** command clears statistics on optimized ND Reply packets.

Format

reset nd optimized-reply statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Before collecting statistics on optimized ND Reply packets on the device, you can run the **reset nd optimized-reply statistics** command to clear statistics on optimized ND Reply packets of the device.

Example

Clears statistics on optimized ND Reply packets.

```
<HUAWEI> reset nd optimized-reply statistics
```

6.10.76 reset rawip ipv6 statistics

Function

The **reset rawip ipv6 statistics** command clears all Raw IPv6 packet statistics.

Format

reset rawip ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You need to run this command to clear the existing statistics on Raw IPv6 packets before running the **display rawip ipv6 statistics** command to view statistics on Raw IPv6 packets in a specified period.

The **reset rawip ipv6 statistics** command clears statistics on Raw IPv6 packets. Therefore, confirm your action before running this command.

Example

Clear all Raw IPv6 packet statistics.

```
<HUAWEI> reset rawip ipv6 statistics
```

6.10.77 reset tcp ipv6 authentication-statistics

Function

The **reset tcp ipv6 authentication-statistics** command clears authentication statistics of a specified TCP6 connection.

Format

reset tcp ipv6 authentication-statistics src-ip *src-ip* **src-port** *src-port* **dest-ip** *dest-ip* **dest-port** *dest-port*

Parameters

Parameter	Description	Value
src-ip *src-ip*	Specifies the source IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
src-port *src-port*	Specifies the source port.	The value is an integer that ranges from 0 to 65535.
dest-ip *dest-ip*	Specifies the destination IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
dest-port *dest-port*	Specifies the destination port.	The value is an integer that ranges from 0 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset tcp ipv6 authentication-statistics** command clears authentication statistics of a TCP6 connection. Therefore, confirm your action before running this command.

Example

Clear authentication statistics of a TCP6 connection.

```
<HUAWEI> reset tcp ipv6 authentication-statistics src-ip fc00:1::1 src-port 3456 dest-ip fc00:3::5 dest-port 5678
```

6.10.78 reset tcp ipv6 statistics

Function

The **reset tcp ipv6 statistics** command clears TCP6 packet statistics.

Format

reset tcp ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete TCP6 packet statistics displayed using the **display tcp ipv6 statistics** command, run the **reset tcp ipv6 statistics** command. The TCP6 packet statistics include the number of both sent and received packets, the number of discarded packets, the number of redirected packets, the threshold-crossing status of TCP6 connections, network attack status, and network quality. You can run the **reset tcp ipv6 statistics** command to delete existing statistics and then run the **display tcp ipv6 statistics** command to collect statistics. The statistics help you check whether TCP6 packet counts are correct or help you diagnose faults.

Precautions

The **reset tcp ipv6 statistics** command clears TCP6 packet statistics. Therefore, confirm your action before running this command.

Example

Clear TCP6 packet statistics.

```
<HUAWEI> reset tcp ipv6 statistics
```

6.10.79 reset udp ipv6 statistics

Function

The **reset udp ipv6 statistics** command clears UDP6 packet statistics.

Format

reset udp ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete UDP6 packet statistics displayed using the **display udp ipv6 statistics** command, run the **reset udp ipv6 statistics** command. The statistics include the number of both the sent and received packets, the number of discarded packets, and the number of redirected packets. You can run the **reset udp ipv6 statistics** command to delete existing statistics and then run the **display udp ipv6 statistics** command to collect statistics. The statistics help you check whether UDP6 packet counts are correct or help you diagnose faults.

Precautions

The **reset udp ipv6 statistics** command clears UDP6 packet statistics. Therefore, confirm your action before running this command.

Example

Clear UDP6 packet statistics.

```
<HUAWEI> reset udp ipv6 statistics
```

6.10.80 segment-routing ipv6 head pop

Function

The **segment-routing ipv6 head pop** command enables SRv6 packet decapsulation.

The **undo segment-routing ipv6 head pop** command disables SRv6 packet decapsulation.

By default, SRv6 packet decapsulation is disabled.

NOTE

This command is supported only on the following models:

S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

segment-routing ipv6 head pop

undo segment-routing ipv6 head pop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Segment Routing over IPv6 (SRv6) is designed to forward IPv6 packets on a network through source routing. SRv6 is based on the IPv6 forwarding plane. With SRv6, a segment routing header (SRH) is added to IPv6 packets. If the downstream device of a switch cannot process SRv6 packets, run the **segment-routing ipv6 head pop** command on the switch to enable SRv6 packet decapsulation and then configure MQC- or ACL-based redirection. In this case, the switch will forward the decapsulated IPv6 packets to the downstream device.

The following actions are taken to decapsulate SRv6 packets:

- Change the value in the **Next Header** field in the IPv6 header to the value in the **Next Header** field in the SRH.
- Change the value in the **Destination Address** field in the IPv6 header to the first IPv6 address (that is, segment list [0]) in the SRH.
- Remove the SRH from the packet.
- Subtract the SRH length from the **Payload Length** field in the IPv6 header.

Follow-up Procedure

Configure MQC- or ACL-based redirection to redirect decapsulated packets to other devices.

Precautions

After the **segment-routing ipv6 head pop** command is run, SRv6 packets cannot be mirrored or sampled, or sent to the CPU.

Example

Enable SRv6 packet decapsulation.

```
<HUAWEI> system-view
[HUAWEI] segment-routing ipv6 head pop
```

6.10.81 service type tunnel

Function

The **service type tunnel** command enables service loopback on an Eth-Trunk interface to loop service packets back to tunnel interfaces.

The **undo service type tunnel** command disables service loopback on an Eth-Trunk interface.

By default, service loopback is disabled on an Eth-Trunk interface.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

service type tunnel

undo service type tunnel

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward packets using tunnel interfaces, you need to bind the tunnel interfaces to an Eth-Trunk interface. Before binding the tunnel interfaces to the Eth-Trunk interface, run the **service type tunnel** command to enable service loopback on the Eth-Trunk interface to loop service packets back to tunnel interfaces.

Precautions

After being configured as a service loopback interface, an Eth-Trunk interface can only be used to loop service packets back to tunnel interfaces.

A device can be configured with only one service loopback interface.

You cannot configure both the **service type tunnel** command and the URPF function on the same Eth-Trunk.

On an Eth-Trunk enabled with the service loopback function, the STP function is automatically disabled. After the service loopback function is disabled on the Eth-Trunk, the STP function is automatically enabled.

- The configurations allowed on an Eth-Trunk to be configured as a loopback interface include **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **traffic-policy (interface view)**, and **trust**. If other configurations exist on the Eth-Trunk, the Eth-Trunk cannot be configured as a loopback interface.
- After an Eth-Trunk is configured as a loopback interface, the Eth-Trunk supports only the following configurations: **authentication open ucl-policy enable**, **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **statistic enable (interface view)**, **traffic-policy (interface view)**, **vcmp disable**, and **trust**.
- Before running the **undo service type tunnel** command, delete all the member interfaces of the Eth-Trunk interface on the device.

After the Eth-Trunk interface is configured as the service loopback interface, other service configurations cannot be performed on the Eth-Trunk interface by invoking the MIB through the NMS. Otherwise, the service loopback interface function or the service configurations delivered through the MIB may be invalid.

Example

Enable service loopback on the interface **Eth-Trunk 0**.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 0
[HUAWEI-Eth-Trunk0] service type tunnel
```

6.10.82 tcp ipv6 max-mss

Function

The **tcp ipv6 max-mss** command sets the maximum value of Maximum Segment Size (MSS) for a TCP6 connection.

The **undo tcp ipv6 max-mss** command deletes the maximum MSS value of a TCP6 connection.

By default, the maximum MSS value is not configured for TCP6 connections.

Format

tcp ipv6 max-mss *mss-value*

undo tcp ipv6 max-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the maximum MSS value for a TCP6 connection.	The value is an integer ranging from 32 to 9600, in bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP6 connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. If the path MTU is unavailable on one end of a TCP6 connection, this end cannot adjust the TCP6 packet size based on the MTU. As a result, this end may send TCP6 packets that are longer than the MTUs on intermediate devices, which will discard these packets. To prevent this problem, run the **tcp ipv6 max-mss** command on either end of a TCP6 connection to set the maximum MSS value of TCP6 packets. Then the MSS value negotiated by both ends will not exceed this maximum MSS value, and accordingly TCP6 packets sent from both ends will not be longer than this maximum MSS value and can travel through the intermediate network.

Precautions

The maximum MSS value configured using the **tcp ipv6 max-mss** command must be greater than the minimum MSS value configured using the **tcp ipv6 min-mss** command.

Example

Set the maximum MSS value for a TCP6 connection to 1024 bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp ipv6 max-mss 1024
```

6.10.83 tcp ipv6 min-mss

Function

The **tcp ipv6 min-mss** command sets the minimum value of maximum segment size (MSS) for a TCP6 connection.

The **undo tcp ipv6 min-mss** command restores the default minimum value of the MSS for a TCP6 connection.

The default minimum MSS value for a TCP6 connection is 216 bytes.

Format

tcp ipv6 min-mss *mss-value*

undo tcp ipv6 min-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the minimum MSS value for a TCP6 connection.	The value ranges from 32 bytes to 1500 bytes. By default, the value is 216 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP6 connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. The TCP6 client on a network may send a request packet for establishing a TCP6 connection carrying a small MSS value. For example, the MSS value is 1. After the TCP6 server receives the request packet carrying the MSS value, the TCP6 connection is established. The TCP6 client then may send large numbers of requests to the server by an application, causing the TCP6 server to generate large numbers of reply packets. This may burden the TCP6 server or network, causing denial of service (DoS) attacks. To resolve this problem, run the **tcp ipv6 min-mss** command to set the minimum MSS value for a TCP6 connection. This configuration prevents a server from receiving packets carrying a small MSS value.

Precautions

The minimum MSS value configured using the **tcp ipv6 min-mss** command must be less than the maximum MSS value configured using the **tcp ipv6 max-mss** command.

If the **tcp ipv6 min-mss** command is run more than once in the same view, the latest configuration overrides the previous one.

Configure the parameters under the guidance of the technical personnel.

Example

Set the minimum MSS value for a TCP6 connection to 512 bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp ipv6 min-mss 512
```

6.10.84 tcp ipv6 timer fin-timeout

Function

The **tcp ipv6 timer fin-timeout** command sets the value of the TCP6 FIN-Wait timer.

The **undo tcp ipv6 timer fin-timeout** command restores the default value of the TCP6 FIN-Wait timer.

By default, the value of the TCP6 FIN-Wait timer is 600s.

Format

tcp ipv6 timer fin-timeout *interval*

undo tcp ipv6 timer fin-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP6 FIN-Wait timer.	The value is an integer that ranges from 76 to 3600, in seconds. The default value is 600s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a TCP6 connection changes from FIN_WAIT_1 to FIN_WAIT_2, the TCP FIN-Wait timer is started. If the local device does not receive a packet with the FIN flag after the TCP6 FIN-Wait timer expires, the TCP6 connection is closed.

Precautions

If you run the **tcp ipv6 timer fin-timeout** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the value of the TCP6 FIN-Wait timer to 800s.

```
<HUAWEI> system-view
[HUAWEI] tcp ipv6 timer fin-timeout 800
```

6.10.85 tcp ipv6 timer syn-timeout

Function

The **tcp ipv6 timer syn-timeout** command sets the value of the TCP6 SYN-Wait timer.

The **undo tcp ipv6 timer syn-timeout** command restores the default value of the TCP6 SYN-Wait timer.

By default, the value of the TCP6 SYN-Wait timer is 75s.

Format

tcp ipv6 timer syn-timeout *interval*

undo tcp ipv6 timer syn-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP6 SYN-Wait timer.	The value is an integer that ranges from 2 to 600, in seconds. The default value is 75s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an SYN packet is sent, the TCP6 SYN-Wait timer is started. If no response packet is received when the TCP6 SYN-Wait timer expires, the TCP6 connection is closed.

Precautions

If you run the **tcp ipv6 timer syn-timeout** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the value of the TCP6 SYN-Wait timer to 100s.

```
<HUAWEI> system-view
[HUAWEI] tcp ipv6 timer syn-timeout 100
```

6.10.86 tcp ipv6 window

Function

The **tcp ipv6 window** command sets the size of the packet receive or send buffer of a connection-oriented socket.

The **undo tcp ipv6 window** command restores the default size of the packet receive or send buffer of a connection-oriented socket.

By default, the size of the packet receive or send buffer of a connection-oriented socket is 8K bytes.

Format

tcp ipv6 window *window-size*

undo tcp ipv6 window

Parameters

Parameter	Description	Value
window-size	Specifies the size of the packet receive or send buffer of a connection-oriented socket.	The value is an integer that ranges from 1 to 32, in K bytes. The default value is 8K bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command changes the default size of the packet receive or send buffer. The device uses the default size to establish a TCP6 session.

Precautions

If you run the **tcp ipv6 window** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the size of the packet receive or send buffer of a connection-oriented socket to 4K bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp ipv6 window 4
```

6.11 DHCPv6 Configuration Commands

6.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

Layer 3 Ethernet interface, VLANIF interface, and sub-interface all support the DHCPv6 function.

6.11.2 address prefix

Function

The **address prefix** command configures the network prefix and lifetime in the IPv6 address pool view.

The **undo address prefix** command deletes the network prefix and lifetime that are configured in the IPv6 address pool view.

By default, no network prefix and lifetime are configured in the IPv6 address pool view.

Format

address prefix *ipv6-prefix/ipv6-prefix-length* [**eui-64**] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

address prefix *ipv6-prefix/ipv6-prefix-length* [**eui-64**] [**life-time preferred-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]] **valid-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]]

address prefix *ipv6-prefix/ipv6-prefix-length* [**lock**]

undo address prefix *ipv6-prefix/ipv6-prefix-length* [**lock**]

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the network prefix and prefix length.	*ipv6-prefix*: The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 1 to 128.
eui-64	Generates the interface ID based on the user MAC address according to the EUI-64 specifications. This method can be used to allocate addresses only when the client DUID type is LL or LLT.	-
life-time	Specifies the network prefix lifetime.	-
valid-lifetime	Specifies the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

Parameter	Description	Value
preferred-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the preferred lifetime of the IPv6 prefix. The time must be no less than 1 minute.	- *days*: indicates days. The value is an integer that ranges from 0 to 1999. - *hours*: indicates hours. The value is an integer that ranges from 0 to 23. - *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. - *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
valid-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the valid lifetime of the IPv6 prefix. The time must be no less than 1 minute and cannot be less than the preferred lifetime.	- *days*: indicates days. The value is an integer that ranges from 0 to 1999. - *hours*: indicates hours. The value is an integer that ranges from 0 to 23. - *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. - *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
lock	Locks the address prefix.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 server, run the **address prefix** command to configure the network prefix in an IPv6 address pool. If IPv6 addresses in an

IPv6 address pool have been assigned to DHCPv6 clients, only the value of life-time can be modified.

Precautions

If no DHCPv6 relay agent exists between the DHCPv6 server and client, the length of the network prefix configured to the DHCPv6 server address pool must be longer than or equal to the prefix length of IPv6 addresses of Layer 3 interfaces on the DHCPv6 server.

Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Example

Bind the network prefix fc00:1::/64 to the DHCPv6 server address pool pool1 and set the lifetime to infinite.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] address prefix fc00:1::/64 life-time infinite infinite
```

6.11.3 capwap-ac (IPv6 address pool view)

Function

The **capwap-ac** command configures the AC's IPv6 address in the IPv6 address pool view.

The **undo capwap-ac** command deletes the AC's IPv6 address configured in the IPv6 address pool view.

By default, the AC's IPv6 address is not configured in the IPv6 address pool view.

Format

capwap-ac *ipv6-address*

undo capwap-ac *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for an AC.	The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters. The format is X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the AC+Fit AP scenario, the AC needs to establish connections with APs. The device functioning as a DHCPv6 server can specify the AC's IPv6 address for an AP. The AP then can connect to the specified AC. The device uses Option52 to carry the AC address.

If the AC and AP are located in the same network segment, the AP sends a broadcast packet to automatically discover the AC. In this case, the configuration of the **capwap-ac** command is optional. If the AC and AP are located in different network segments, you must configure the **capwap-ac** command.

Prerequisites

The IPv6 address pool is created using the **dhcpv6 pool** command.

Precautions

You can run the **capwap-ac** command multiple times to configure the IPv6 addresses of several ACs, and the AC's IPv6 address that is configured first takes precedence over the one configured later.

Example

Specify the AC's IPv6 address to fc00:1::1 in pool1 of the DHCPv6 server.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] capwap-ac fc00:1::1
```

6.11.4 conflict-address expire-time

Function

The **conflict-address expire-time** command sets the aging time for conflicted addresses in the IPv6 address pool.

The **undo conflict-address expire-time** command restores the default aging time of conflicted addresses in the IPv6 address pool.

By default, the aging time of conflicted addresses is 172800s (two days).

Format

conflict-address expire-time *expire-time*

undo conflict-address expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time for the conflicted addresses in the address pool.	The value is an integer that ranges from 60 to 4294967295, in seconds.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **conflict-address expire-time** command is used on DHCPv6 servers. If the IPv6 address in the address pool is marked as a conflicted address, it cannot be allocated. To use these conflicted addresses, the administrator needs to mark these addresses as assignable. After the aging time configured using the **conflict-address expire-time** command expires, the conflicted addresses automatically become assignable.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Example

Set the aging time of conflicted addresses in global address pool global1 to 36000s.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] conflict-address expire-time 36000
```

6.11.5 dhcpv6 client information-request

Function

The **dhcpv6 client information-request** command enables an interface to obtain configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

The **undo dhcpv6 client information-request** command disables an interface from obtaining configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

By default, the interface is disabled from obtaining configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

Format

dhcpv6 client information-request

undo dhcpv6 client information-request

Parameters

None

Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 client information-request** command is used on the DHCPv6 client. After you run the **dhcpv6 client information-request** on the device that functions as a DHCPv6 client, IPv6 addresses are generated based on the Route Advertisement (RA) packets. The DHCPv6 server provides other configuration parameters such as IP addresses of the DNS, and SNTP servers except for IPv6 addresses and the interval for updating configuration parameters.

Prerequisites

1. IPv6 functions have been enabled globally using the **ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **ipv6 enable** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local** or **ipv6 address** *ipv6-address* **link-local** command in the interface view.

Example

Configure the DHCPv6 client to obtain configuration parameters using stateless DHCPv6 address autoconfiguration on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto link-local
[HUAWEI-Vlanif100] dhcpv6 client information-request
```

Configure the DHCPv6 client to obtain configuration parameters using stateless DHCPv6 address autoconfiguration on the interface

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 client information-request
```

6.11.6 dhcpv6 client pd

Function

The **dhcpv6 client pd** command configures the DHCPv6 PD client function.

The **undo dhcpv6 client pd** command disables the DHCPv6 PD client function.

By default, the DHCPv6 PD client function is disabled.

Format

dhcpv6 client pd *prefix-name* [**hint** *ipv6-prefix/ipv6-prefix-length*] [**rapid-commit**] [**unicast-option**]

undo dhcpv6 client pd

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of an IPv6 address prefix name.	The value is a string of 1 to 63 case-sensitive characters without spaces.
hint *ipv6-prefix/ipv6-prefix-length*	Specifies the required IPv6 address prefix and prefix length.	*ipv6-prefix*: The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 1 to 128.
rapid-commit	Indicates that the DHCPv6 PD client requests an IPv6 address prefix using the two-message exchange.	-
unicast-option	Indicates that the DHCPv6 PD client requests an IPv6 address prefix using the unicast mode.	-

Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 client pd** command is used on the DHCPv6 PD client. After the **dhcpv6 client pd** is executed on the device that functions as a DHCPv6 PD client, the device requests an IPv6 address prefix in the DHCPv6 mode. The requested prefix is bound to the configured prefix name. You can specify the **hint** *ipv6-prefix/ipv6-prefix-length* parameter to set the required IPv6 address prefix and prefix length.

Prerequisites

1. IPv6 functions have been enabled globally using the **ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **ipv6 enable** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local**, or **ipv6 address** *ipv6-address* **link-local** command in the interface view. Or the IPv6 global unicast IPv6 address has been configured using the **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } command in the interface view.

Configuration Precautions

When configuring the DHCPv6 PD client function, you cannot set *prefix-name* to **a**, **au**, **aut**, or **auto**. These prefix names cannot be applied to interfaces.

Example

Configure the DHCPv6 PD client to obtain IPv6 address prefix using stateless DHCPv6 address autoconfiguration on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto link-local
[HUAWEI-Vlanif100] dhcpv6 client pd example
```

Configure the DHCPv6 PD client to obtain IPv6 address prefix using stateless DHCPv6 address autoconfiguration on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 client pd example
```

6.11.7 dhcpv6 client renew

Function

The **dhcpv6 client renew** command updates the IPv6 address or prefix applied by a DHCPv6 client.

Format

dhcpv6 client renew

Parameters

None

Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcpv6 client renew** command applies to only the DHCP client and updates the IPv6 address or prefix applied by the DHCPv6 client.

Example

Manually update the applied IPv6 address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 address auto dhcp
[HUAWEI-Vlanif100] dhcpv6 client renew
```

Manually update the applied IPv6 prefix.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcpv6 client pd myprefix
[HUAWEI-Vlanif100] dhcpv6 client renew
```

6.11.8 dhcpv6 duid

Function

The **dhcpv6 duid** command configures a DUID for the DHCPv6 device.

By default, the device generates a DUID based on the link-layer (LL) address.

Format

dhcpv6 duid { **ll** | **llt** | *duid* }

Parameters

Parameter	Description	Value
ll	Configures the device to generate a DUID based on the link-layer address (MAC address).	-

Parameter	Description	Value
llt	Configures the device to generate a DUID based on the link-layer address (MAC address) plus time.	-
duid	Specifies the DUID of the device.	The value is a hexadecimal string with an even number (in the range of 8 to 28) of characters. The value contains only combinations of digits 0 to 9, uppercase letters A to F, and lowercase letters a to f.

Views

System view

Default Level

3: Management level

Usage Guidelines

A DUID identifies a DHCPv6 device. Each DHCPv6 server or client has a unique DUID. Servers use DUIDs to identify clients and clients use DUIDs to identify servers. When this command is run, a new DUID is stored in the :/dhcp/dhcp-duid.txt file of the storage device. You can run the **display dhcpv6 duid** command to check the DUID of the device.

Example

Configure the device to generate a DUID based on the link-layer address.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 duid ll
Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it? [Y/
N]y
```

6.11.9 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 00e0-fc12-3456, the Interface-ID generated during the system parsing process is 0011.0022.00e0fc123456:vlanif100.	-
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: ● Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 6-76**. ● Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. ● Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

Table 6-76 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.

Keyword	Description
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 interface-id format user-defined "%mac"
```

6.11.10 dhcpv6 interface-id insert enable

Function

The **dhcpv6 interface-id insert enable** command enables the function of adding the Interface-ID option in DHCPv6 packets.

The **undo dhcpv6 interface-id insert enable** command disables the function of adding the Interface-ID option in DHCPv6 packets.

By default, the function of adding the Interface-ID option in DHCPv6 packets is enabled.

NOTE

This command is supported only on the following models: S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6735-S, S6720-EI, S6720S-EIS5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720S-S.

Format

dhcpv6 interface-id insert enable

undo dhcpv6 interface-id insert enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID option records user access information such as the inbound interface of the DHCPv6 Request packets sent from the clients to the device. The user access information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. When the device functions as a DHCPv6 relay agent or lightweight DHCPv6 relay agent (LDRA), and the device receives the Request packets sent from the DHCPv6 clients and forwards the packets to the DHCPv6 server, the device adds the Interface-ID option in the packets to identify location information of the DHCPv6 clients by default. If the DHCPv6 server interconnected to the device does not support the Interface-ID option, you can run the **undo dhcpv6 interface-id insert enable** command to configure the device not to add the Interface-ID option in DHCPv6 packets to flexibly control option information obtained by the DHCPv6 server.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Enable the function of adding the Interface-ID option in DHCPv6 packets on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 interface-id insert enable
```

6.11.11 dhcpv6 packet-rate

Function

The **dhcpv6 packet-rate** command enables rate limit of DHCPv6 messages and sets the rate threshold for DHCPv6 messages.

The **undo dhcpv6 packet-rate** command disables rate limit of DHCPv6 messages and deletes the rate threshold for DHCPv6 messages.

By default, rate limit of DHCPv6 messages is disabled.

Format

dhcpv6 packet-rate *packet-rate*

undo dhcpv6 packet-rate

Parameters

Parameter	Description	Value
packet-rate	Specifies the rate threshold for DHCPv6 messages.	The value is an integer that ranges from 0 to 400, in pps. If the value is 0, rate limit of DHCPv6 messages is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent clients from sending a large number of messages to attack the device, the device limits the rate of DHCPv6 messages. After the DHCPv6 packet rate limit is enabled and the rate threshold is configured using the **dhcpv6 packet-rate** command, the DHCPv6 packets are discarded when the packet rate exceeds the rate threshold.

Prerequisites

DHCP functions have been enabled globally using the **dhcp enable** command.

Precautions

When the value of *packet-rate* is greater than 200, you need to run the **car packet-type dhcpv6-reply cir** *cir-value* command to increase the maximum rate of DHCPv6 Reply messages.

Example

Enable rate limit of DHCPv6 messages and set the rate threshold for DHCPv6 messages to 200 pps.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 packet-rate 200
```

6.11.12 dhcpv6 packet-rate drop-alarm enable

Function

The **dhcpv6 packet-rate drop-alarm enable** command enables the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit.

The **undo dhcpv6 packet-rate drop-alarm enable** command disables the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit.

By default, the alarm function for discarding DHCPv6 messages is disabled when the rate of DHCPv6 messages exceeds the limit.

Format

dhcpv6 packet-rate drop-alarm enable

undo dhcpv6 packet-rate drop-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of DHCPv6 messages discarded is enabled using the **dhcpv6 packet-rate drop-alarm enable** command, the device records alarm information when the number of DHCPv6 packets that are discarded exceeds the alarm threshold. The alarm threshold can be set using the **dhcpv6 packet-rate drop-alarm threshold** command.

Prerequisites

1. DHCP functions have been enabled globally using the **dhcp enable** command.
2. The DHCPv6 packet rate limit has been enabled using the **dhcpv6 packet-rate** command.

Example

Enable the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds rate limit.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 packet-rate 200
[HUAWEI] dhcpv6 packet-rate drop-alarm enable
```

6.11.13 dhcpv6 packet-rate drop-alarm threshold

Function

The **dhcpv6 packet-rate drop-alarm threshold** command sets the alarm threshold for the number of DHCPv6 messages discarded when the rate of DHCPv6 messages exceeds the rate limit.

The **undo dhcpv6 packet-rate drop-alarm threshold** command restores the default alarm threshold of the number of DHCPv6 messages discarded.

By default, the alarm threshold is 100 packets when the alarm function of DHCPv6 messages discarded is enabled.

Format

dhcpv6 packet-rate drop-alarm threshold *threshold*

undo dhcpv6 packet-rate drop-alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCPv6 messages discarded when the rate of DHCPv6 messages exceeds the rate limit.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of DHCPv6 messages discarded is enabled using the **dhcpv6 packet-rate drop-alarm enable** command, the device records alarm information when the number of DHCPv6 packets that are discarded exceeds the alarm threshold.

Prerequisites

1. The DHCP function has been enabled globally using the **dhcp enable** command.
2. The DHCPv6 packet rate limit has been enabled using the **dhcpv6 packet-rate** *packet-rate* command.
3. The alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit has been enabled using the **dhcpv6 packet-rate drop-alarm enable** command.

Example

Configure the device to generate an alarm when the number of DHCPv6 messages discarded exceeds 150 packets.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 packet-rate 200
[HUAWEI] dhcpv6 packet-rate drop-alarm enable
[HUAWEI] dhcpv6 packet-rate drop-alarm threshold 150
```

6.11.14 dhcpv6 pool

Function

The **dhcpv6 pool** command creates an IPv6/IPv6 PD address pool or displays the IPv6/IPv6 PD address pool view.

The **undo dhcpv6 pool** command deletes the created IPv6/IPv6 PD address pool.

By default, no IPv6/IPv6 PD address pool is created.

Format

dhcpv6 pool *pool-name*

undo dhcpv6 pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of an IPv6/IPv6 PD address pool.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value contains digits, letters, underscores (_), and dots (.).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **dhcpv6 pool** command is used on DHCPv6/DHCPv6 PD servers. When configuring the DHCPv6/DHCPv6 PD server, run the **dhcpv6 pool** command to create an IPv6/IPv6 PD address pool for the DHCPv6/DHCPv6 PD server to assign IPv6 addresses or prefixes to DHCPv6/DHCPv6 PD clients.

Example

Create an IPv6 address pool **DHCPv6POOL**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool DHCPv6POOL
```

6.11.15 dhcpv6 relay advertise prefix-delegation route

Function

The **dhcpv6 relay advertise prefix-delegation route** command enables a DHCPv6 relay agent to forward routing information of DHCPv6 prefix delegation (DHCPv6 PD) terminals.

The **undo dhcpv6 relay advertise prefix-delegation route** command disables a DHCPv6 relay agent from forwarding routing information of DHCPv6 PD terminals.

By default, a DHCPv6 relay agent does not forward routing information of DHCPv6 PD terminals.

Format

dhcpv6 relay advertise prefix-delegation route

undo dhcpv6 relay advertise prefix-delegation route

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 relay advertise prefix-delegation route** command is used on DHCPv6 relay agents. DHCPv6 PD terminals cannot advertise IPv6 routes. This command enables a DHCPv6 relay agent to add routes of DHCPv6 PD terminals to the routing table when DHCPv6 PD terminals apply for IP addresses from the DHCPv6 server through the DHCPv6 relay agent. The DHCPv6 relay agent then forwards the routing information to the DHCPv6 server.

Prerequisites

The DHCPv6 relay function has been enabled on the interface using the **dhcpv6 relay** { **destination** *ipv6-address* | **interface** *interface-type interface-number* } or **dhcpv6 relay server-select** *group-name* command.

Precautions

This command takes effect only for the first-hop DHCPv6 relay agent connected to DHCPv6 PD terminals.

Example

Enable VLANIF10 to forward routing information of DHCPv6 PD terminals.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] dhcpv6 relay destination FC00::1:3
[HUAWEI-Vlanif10] dhcpv6 relay advertise prefix-delegation route
```

6.11.16 dhcpv6 relay prefix-delegation route

Function

The **dhcpv6 relay prefix-delegation route** command saves routing information forwarded by a relay agent into a specified file.

The **undo dhcpv6 relay prefix-delegation route** command cancels the configuration.

By default, routing information forwarded by a relay agent into a specified file is not saved.

Format

dhcpv6 relay prefix-delegation route autosave *file-name*

undo dhcpv6 relay prefix-delegation route autosave

Parameters

Parameter	Description	Value
autosave	Backs up routing information learned from DHCPv6 PD terminals to the flash memory.	-

Parameter	Description	Value
file-name	Specifies the path and file name of the file where routing information of DHCPv6 PD terminals is to be saved, for example, flash:/*.pdr.	The value is a string of 1 to 51 case-insensitive characters and is a combination of digits, letters, and characters. It cannot contain spaces. **NOTE** The file name cannot contain any less than sign (<), greater than sign (>), question mark (?), asterisk (*), comma (,), back quote (`), slash (/), backslash (\), single quotation mark ('), colon (:), or double quotation mark ("), and the left square bracket ([) and right square bracket (]) cannot exist in pairs.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 relay prefix-delegation route** command is used on DHCPv6 relay agents. This command saves routing information forwarded by a relay agent into a specified file.

After this command is run, the system immediately saves routing information, and then saves routing information again every two hours. The interval at which the system saves routing information cannot be set.

Prerequisites

The DHCP function has been enabled using the **dhcp enable** command in the system view.

Example

Save routing information forwarded by a relay agent into a specified file.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 relay prefix-delegation route autosave flash:/dhcpv6-pd.pdr
Info: The operation may take a few seconds, Please wait for a moment.done.
```

6.11.17 dhcpv6 relay destination

Function

The **dhcpv6 relay destination** command enables the DHCPv6 relay function on interfaces and configures the IPv6 address of the DHCPv6 server or next-hop relay agent.

The **undo dhcpv6 relay destination** command disables the DHCPv6 relay function on an interface.

By default, the DHCPv6 relay function is disabled on an interface.

Format

dhcpv6 relay { **destination** *ipv6-address* | **interface** *interface-type interface-number* }

undo dhcpv6 relay { **destination** *ipv6-address* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
ipv6-address	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of the outbound interface of relay messages. The specified interface can only be a Layer 2 interface.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a client applies to a DHCPv6 server on a different network segment for an IPv6 address, you need to deploy a relay agent between the client and the DHCPv6 server. In this manner, the relay agent transmits DHCPv6 messages exchanged between the client and the DHCPv6 server.

You can run the **dhcpv6 relay destination** *ipv6-address* command to enable the DHCPv6 relay function on an interface.

When the client and the server are in the same VLAN, you can run the **dhcpv6 relay interface** *interface-type interface-number* command to specify the outbound interface of relay messages.

Prerequisites

The DHCP function has been enabled using the **dhcp enable** command in the system view.

Precautions

- When you run the **dhcpv6 relay interface** *interface-type interface-number* command in the VLANIF interface view to specify the outbound interface of relay messages, the specified interface can only be a Layer 2 interface. If the specified outbound interface is not in the VLAN corresponding to the VLANIF interface, add the interface to the VLAN.
- When both the **dhcpv6 relay destination** *ipv6-address* and **dhcpv6 relay interface** *interface-type interface-number* commands are configured, relay messages are preferentially sent to the configured IPv6 address based on routes.

Example

Enable the DHCPv6 relay function on VLANIF100 and set the destination address of relay messages to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay destination fc00:1::1
```

Enable the DHCPv6 relay function on GE0/0/1 and set the destination address of relay messages to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay destination fc00:1::1
```

6.11.18 dhcpv6 relay server-select

Function

The **dhcpv6 relay server-select** command configures a DHCPv6 server group for a DHCPv6 relay agent.

The **undo dhcpv6 relay server-select** command deletes a DHCPv6 server group for a DHCPv6 relay agent.

By default, no DHCPv6 server group is configured.

Format

dhcpv6 relay server-select *group-name*

undo dhcpv6 relay server-select

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCPv6 server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6 relay server-select** command is used on DHCPv6 relay agents. When a DHCPv6 client sends DHCPv6 Request packets to a DHCPv6 server through a DHCPv6 relay agent, you can run the **dhcp relay server-select** command to specify a DHCPv6 server group for the DHCPv6 relay agent and configure the IPv6 address of the DHCPv6 server.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.

2. A DHCPv6 server group has been created using the **dhcpv6 server group** command.
3. The IPv6 function has been enabled using the **ipv6 enable** command in the interface view.

Precautions

- Each DHCPv6 server group can be bound to multiple interfaces, but each interface can only be bound to one DHCPv6 server group.
- IP addresses of servers in a DHCPv6 server group cannot be on the same network segment with IP addresses of interfaces on the DHCPv6 relay agent.
- If you run the **dhcpv6 relay server-select** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure the DHCPv6 server group named group 1 for the DHCPv6 relay agent on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 server group group1
[HUAWEI-dhcpv6-server-group-group1] dhcpv6-server fc00:1::1
[HUAWEI-dhcpv6-server-group-group1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay server-select group1
```

Configure the DHCPv6 server group named group 1 for the DHCPv6 relay agent on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 server group group1
[HUAWEI-dhcpv6-server-group-group1] dhcpv6-server fc00:1::1
[HUAWEI-dhcpv6-server-group-group1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay server-select group1
```

6.11.19 dhcpv6 relay source-interface

Function

The **dhcpv6 relay source-interface** command configures the IPv6 address of an interface as the source IPv6 address of packets.

The **undo dhcpv6 relay source-interface** command restores the default setting.

By default, the IPv6 address of an interface is not configured as the source IPv6 address of packets.

Format

dhcpv6 relay source-interface *interface-type interface-number*

undo dhcpv6 relay source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. - *interface-type*: specifies the interface type. Currently, only loopback interfaces are supported. - *interface-number*: specifies the interface number.	-

Views

System view, VBDIF interface view, VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, MultiGE sub-interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When forwarding packets from a DHCPv6 client, a DHCPv6 relay agent uses the IPv6 address of the packet inbound interface as the source IPv6 address of the packets. Therefore, you need to configure an IPv6 address for each interface on the DHCPv6 relay agent. As a result, the configuration is complex and IPv6 addresses may be wasted. You can run the **dhcpv6 relay source-interface** *interface-type interface-number* command on the DHCPv6 relay agent to specify the IPv6 address of the loopback interface as the source IPv6 address of the DHCPv6 relayed packets, simplifying the configuration and saving IPv6 addresses.

In addition, VBDIF interfaces functioning as gateways on distributed gateway devices use the same IPv6 address. If Layer 3 VXLAN gateways are distributed gateways and the IPv6 address is used to communicate with the server, the response packets from the server are forwarded to the incorrect distributed gateways (devices that do not send DHCPv6 request packets). To resolve this issue, you need to run the **dhcpv6 relay source-interface** *interface-type interface-number* command on each distributed gateway to specify the IPv6 address of the loopback interface as the source IPv6 address of the DHCPv6 relayed packets for ensuring that response packets from the server can be forwarded to the correct distributed gateways.

Prerequisites

Before you run this command in the system view, the first four conditions must be met. Before you run this command in the interface view, all the following conditions must be met.

- The device has been enabled to forward IPv6 unicast packets using the **ipv6** command.
- A loopback interface has been created using the **interface loopback** *loopback-number* command.
- An IPv6 address has been configured for the loopback interface using the **ipv6 address** command.
- DHCP has been enabled globally using the **dhcp enable** command.
- In the interface view:
  - The IPv6 function has been enabled on the interface using the **ipv6 enable** command.
  - The DHCPv6 relay function has been enabled on the interface using the **dhcpv6 relay** { **destination** *ipv6-address* | **interface** *interface-type interface-number* } or **dhcpv6 relay server-select** *group-name* command.

Precautions

If an IPv6 address is configured for the inbound interface that receives packets from DHCPv6 clients, the IPv6 address is used as the source IPv6 address of packets.

This command takes effect on all interfaces of the device if it is configured in the system view, and takes effect only on an interface if it is configured in the interface view. If this command is configured in both the interface view and system view, the configuration in the interface view takes effect.

If the DHCPv6 relay agent connects to the DHCPv6 server over a VPN network, you need to run the **ip binding vpn-instance** command to bind the loopback interface specified in the **dhcpv6 relay source-interface** command to the corresponding VPN instance.

Example

In the system view, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface loopback 5
[HUAWEI-LoopBack5] ipv6 enable
[HUAWEI-LoopBack5] ipv6 address fc01:1::1/128
[HUAWEI-LoopBack5] quit
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 relay source-interface loopback 5
```

On VLANIF100, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface loopback 5
[HUAWEI-LoopBack5] ipv6 enable
[HUAWEI-LoopBack5] ipv6 address fc01:1::1/128
[HUAWEI-LoopBack5] quit
[HUAWEI] dhcp enable
```

```
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay destination fc00:1::1
[HUAWEI-Vlanif100] dhcpv6 relay source-interface loopback 5
```

On GE0/0/1, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface loopback 5
[HUAWEI-LoopBack5] ipv6 enable
[HUAWEI-LoopBack5] ipv6 address fc01:1::1/128
[HUAWEI-LoopBack5] quit
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay destination fc00:1::1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay source-interface loopback 5
```

6.11.20 dhcpv6 relay option79 insert enable

Function

The **dhcpv6 relay option79 insert enable** command inserts the Option79 field into DHCPv6 messages.

The **undo dhcpv6 relay option79 insert enable** command restores the default setting.

By default, the Option79 field is not inserted into DHCPv6 messages.

Format

dhcpv6 relay option79 insert enable

undo dhcpv6 relay option79 insert enable

Parameters

None

Views

System view, VBDIF interface view, VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

The MAC address is used to identify the DHCPv4 client on the IPv4 network and the DUID is used to identify the DHCPv6 client on the IPv6 network. In an IPv4 and IPv6 dual-stack service deployment scenario, the administrator wants to establish connections between clients' MAC addresses and IPv4 or IPv6 addresses obtained by the clients and perform unified management over dual-stack clients based on the MAC address. However, the MAC address of the DHCPv6 client cannot be identified using the DUID currently.

As defined in RFC, a DHCPv6 relay agent can fill the link address and link type of a client into the Option79 field. When a device functions as a DHCPv6 relay agent, you can run the **dhcpv6 relay option79 insert enable** command to insert the Option79 field into DHCPv6 messages for enabling the DHCPv6 server to obtain the clients' MAC addresses. When this command is run and the DHCPv6 relay agent receives a Request message from a client, it inserts the Option79 field into the Request message and forwards the message to the DHCPv6 server. The DHCPv6 server then obtains the MAC address of the client by parsing the Option79 field.

Prerequisites

- Before the **dhcpv6 relay option79 insert enable** command is configured, DHCP has been globally enabled using the **dhcp enable** command in the system view and IPv6 has been globally enabled using the **ipv6** command.
- Before the **dhcpv6 relay option79 insert enable** command is configured in the interface view, the DHCPv6 relay function has been enabled in the interface view.

Precautions

- Only the first-hop DHCPv6 relay agent supports this function.
- This function takes effect for all interfaces if it is configured in the system view, and takes effect for a specified interface if it is configured in the view of the interface. If this command is configured in both the interface view and system view, the configuration in the interface view takes effect.

Example

Insert the Option79 option into DHCPv6 messages in the system view.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] dhcpv6 relay option79 insert enable
```

Insert the Option79 field into DHCPv6 messages in the interface view.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay destination fc00:1::1
[HUAWEI-Vlanif100] dhcpv6 relay option79 insert enable
```

6.11.21 dhcpv6 remote-id format

Function

The **dhcpv6 remote-id format** command sets the format of the Remote-ID in DHCPv6 messages.

The **undo dhcpv6 remote-id format** command restores the default format of the Remote-ID in DHCPv6 messages.

By default, the default format of the Remote-ID in DHCPv6 messages is used.

Format

dhcpv6 remote-id format { **default** | **user-defined** *text* }

undo dhcpv6 remote-id format

Parameters

Parameter	Description	Value
default	Indicates to adopt the default format of the remote ID. The default format of the remote ID is %duid %portname:%04svlan.%04cvlan, where the values of the outer VLAN ID and inner VLAN ID are integers and composed of four characters. If the length is shorter than four characters, 0s are prefixed to the value. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is GE0/0/1, and the client DUID is 0003000180FB063545B3, the Remote-ID option generated during the system parsing process is 0003000180FB063545B3 GigabitEthernet 0/0/1:0011.0022.	-

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Remote-ID format. A user-defined format can be: - Format defined by keywords: The Remote-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Remote-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 6-77**. - Format defined by common character strings: The Remote-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Remote-ID can be directly defined as N8. - Mixed format: The Remote-ID is defined by both the keywords and common character strings. For	The value is a string of 3 to 247 case-sensitive characters with spaces.

Parameter	Description	Value
	example, the Remote-ID can be defined as %sysname N8.	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The Remote-ID records user access information such as the DUID of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Remote-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 remote-id format** command to configure the format of the Remote-ID inserted into DHCPv6 packets.

Table 6-77 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.

Keyword	Description
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

The DHCP function has been enabled using the **dhcp enable** command in the system view.

Follow-up Procedure

When the device functions as a DHCPv6 relay, you must run the **dhcpv6 remote-id insert enable** or **dhcpv6 remote-id rebuild enable** command to enable the function of inserting the Remote-ID into DHCPv6 relay packets after running the **dhcpv6 remote-id format** command to configure the Remote-ID format in DHCPv6 packets.

NOTE

When the device functions as an LDRA, the Remote-ID is inserted into DHCPv6 relay packets by default and the function does not need to be enabled.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:

- The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
- An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Set the customized format for the remote ID carried in DHCPv6 messages and encapsulate the MAC address of the device into the remote ID.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 remote-id format user-defined "%mac"
```

6.11.22 dhcpv6 remote-id insert enable

Function

Using the **dhcpv6 remote-id insert enable** command, you can enable the function of appending the remote ID to DHCPv6 relay messages.

Using the **undo dhcpv6 remote-id insert enable** command, you can disable the function of appending the remote ID to DHCPv6 relay messages.

By default, the function of appending the remote ID to DHCPv6 relay messages is disabled.

Format

dhcpv6 remote-id insert enable

undo dhcpv6 remote-id insert enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The remote ID carries information about a client and identifies a client. The DHCPv6 server can make decisions about address allocation, parameter setting, and prefix agent according to the remote ID. The remote ID is defined by the vendor. Usually, the remote ID carries the phone number of the caller in dialing, user name, IP address of the peer in a point-to-point connection, and access interface.

Prerequisite

DHCP has been enabled globally using the **dhcp enable** command.

Example

Enable the function of appending the remote ID to DHCPv6 relay messages on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 remote-id insert enable
```

6.11.23 dhcpv6 remote-id rebuild enable

Function

Using the **dhcpv6 remote-id rebuild enable** command, you can enable the function of appending the remote ID to DHCPv6 relay messages.

Using the **undo dhcpv6 remote-id rebuild enable** command, you can disable the function of appending the remote ID to DHCPv6 relay messages.

By default, the function of appending the remote ID to DHCPv6 relay messages is disabled.

Format

dhcpv6 remote-id rebuild enable

undo dhcpv6 remote-id rebuild enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The remote ID carries information about a client and identifies a client. The DHCPv6 server can make decisions about address allocation, parameter setting, prefix agent according to the remote ID. The format of the remote ID is defined by the vendor. Usually, the remote ID carries the phone number and user name in a dial-up connection, or the peer IP address and access interface in a point-to-point connection.

Before running the **dhcpv6 remote-id rebuild enable** command, you must run the **dhcp enable** command to enable DHCP globally.

Example

Enable the function of appending the remote ID to DHCPv6 relay messages on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 remote-id rebuild enable
```

6.11.24 dhcpv6 server (system view)

Function

The **dhcpv6 server** command enables the DHCPv6 server or DHCPv6 PD server function in the system view.

The **undo dhcpv6 server** command disables the DHCPv6 server or DHCPv6 PD server function in the system view.

By default, the DHCPv6 server or DHCPv6 PD server function is disabled in the system view.

Format

dhcpv6 server { **allow-hint** | **preference** *preference-value* | **rapid-commit** | **unicast** } *

undo dhcpv6 server { **allow-hint** | **preference** | **rapid-commit** | **unicast** } *

Parameters

Parameter	Description	Value
allow-hint	Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests. If the **allow-hint** parameter is specified, the server preferentially allocates addresses, prefixes, and prefix lengths based on the client requests. If the address, prefix, and prefix length requested by a client are not within the address pool or have been allocated to another client, the server ignores the client request and allocates another available address, prefix, and prefix length to the client.	-
preference *preference-value*	Specifies the server priority in the Advertise packet sent by the device. The DHCPv6 client selects the server with the highest priority based on the server priority in the Advertise packet to assign IPv6 addresses or prefixes.	The value is an integer that ranges from 0 to 255. By default, the value is 0. A larger value indicates a higher server priority.
rapid-commit	Indicates that the device supports fast address or prefix assignment, that is, two-message exchange.	-
unicast	Specifies unicast communication between the client and server during the address lease renewal process.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 or DHCPv6 PD server, the DHCPv6 or DHCPv6 PD server function can be enabled in the system view or interface view. If the DHCPv6 or DHCPv6 PD server function is enabled in the interface view, the configuration information only takes effect on the interfaces and only one IPv6 address pool can be specified on an interface.

The DHCPv6 or DHCPv6 PD server and DHCPv6 clients are in different link scopes and a DHCPv6 relay exists. If the DHCPv6 or DHCPv6 PD server function is enabled in the interface view, configuration parameters such as IPv6 addresses or prefixes are assigned only to the clients in one network segment connected to the DHCPv6 relay, because only one IPv6 address pool can be specified on an interface. If configuration parameters such as IPv6 addresses or prefixes need to be assigned to the DHCPv6 clients in multiple network segments through the DHCPv6 relay, enable the DHCPv6 or DHCPv6 PD server function in the system view.

The configuration method of enabling the DHCPv6 or DHCPv6 PD server function in the interface view is affected by the physical interface status. If the interface status is Down, the DHCPv6 or DHCPv6 PD server cannot successfully assign network configuration parameters to clients through the DHCPv6 relay. When the DHCPv6 or DHCPv6 PD server function is enabled in the system view and there are multiple reachable routes between the DHCPv6 relay and DHCPv6 or DHCPv6 PD server, configuration parameters such as IPv6 addresses can be assigned to clients through the DHCPv6 relay as long as one route between the DHCPv6 relay and DHCPv6 or DHCPv6 PD server is reachable. This improves reliability of the configuration information obtained by the clients. In addition, no configuration is required on the interface, which reduces the administrator's maintenance workload.

When functioning as a DHCPv6 or DHCPv6 PD server, the device may be configured with multiple IPv6 address pools. After receiving the DHCPv6 request packets, the DHCPv6 or DHCPv6 PD server chooses the IPv6 address pool based on the following rules:

- When the device functions as the DHCPv6 server:
  - If a relay exists, the server chooses the address pool that belongs to the same link scope with the configured network prefix (using the **link-address** command or **address prefix**) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - When the DHCPv6 server is enabled in the system view, the DHCPv6 server cannot assign network parameters (such as IPv6 addresses, DNS, NIS, and SNTP servers) to clients if no relay exists. To enable the DHCPv6

server to assign network parameters, enable the DHCPv6 server function in the interface view.

- When the device functions as the DHCPv6 PD server:
  - If a relay exists, choose the address pool in the same link scope with the configured network prefix (using the **link-address** command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the DHCPv6 PD server function cannot be enabled in the system view and can be enabled in the interface view, using the **dhcpv6 server** command.

Prerequisites

1. The DHCP function has been enabled globally using the **dhcp enable** command.
2. The IPv6 function has been enabled globally using the **ipv6** command.

Example

Enable the DHCPv6 server function in the system view, and configure the server priority to 255.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] dhcpv6 server preference 255
```

6.11.25 dhcpv6 server (interface view)

Function

The **dhcpv6 server** command enables the DHCPv6 server function on an interface.

The **undo dhcpv6 server** command disables the DHCPv6 server function on an interface.

By default, the DHCPv6 server function on an interface is disabled.

Format

dhcpv6 server *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit** | **unicast**] *

undo dhcpv6 server

Parameters

Parameter	Description	Value
pool-name	Specifies the name of the DHCPv6 address pool configured on an interface.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain digits, letters, underscores (_), and periods (.).
allow-hint	Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests. If the **allow-hint** parameter is specified, the server preferentially allocates addresses, prefixes, and prefix lengths based on the client requests. If the address, prefix, and prefix length requested by a client are not within the address pool or have been allocated to another client, the server ignores the client request and allocates another available address, prefix, and prefix length to the client.	-
preference *preference-value*	Specifies the priority of the DHCPv6 server carried in the Advertise message sent by the DHCPv6 server. The DHCPv6 client chooses to obtain an IPv6 address or prefix from the DHCPv6 server with the highest priority based on the server priority carried in the Advertise message.	The value is an integer that ranges from 0 to 255. The default value is 0. A larger value indicates a higher priority of the DHCPv6 server.
rapid-commit	Configures the DHCPv6 server to support fast address prefix allocation.	-

Parameter	Description	Value
unicast	Specifies the unicast communication between the DHCPv6 client and DHCPv6 server during IPv6 address lease.	-

Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 server** command is used on DHCP servers. If an IPv6 address pool is referenced by an interface, the interface assigns addresses or address prefixes in the address pool to clients after receiving the DHCPv6 Request messages.

Prerequisites

- DHCP functions have been enabled globally using the **dhcp enable** command.
- IPv6 functions have been enabled globally using the **ipv6** command.
- IPv6 functions have been enabled using the **ipv6 enable** command in the interface view.

Precautions

- The DHCPv6 client function, DHCPv6 relay function, and DHCPv6 server function cannot be enabled on the same interface simultaneously.
- Only one ipv6 address pool can be referenced by an interface.
- If the ipv6 address pool referenced by the interface does not exist, the DHCPv6 server function does not take effect.

Example

Associate DHCPv6 address pool Pool1 with VLANIF100 and set the priority of pool1 to 255.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
```

```
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 server pool1 preference 255
```

Associate DHCPv6 address pool pool1 with GE0/0/1 and set the priority of Pool1 to 255.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 server pool1 preference 255
```

6.11.26 dhcpv6-server (DHCPv6 server group view)

Function

The **dhcpv6-server** command adds a DHCPv6 server or a next-hop relay agent to a DHCPv6 server group.

The **undo dhcpv6-server** command deletes a DHCPv6 server or a next-hop relay agent that is configured in a DHCPv6 server group.

By default, no DHCPv6 server or next-hop relay agent is configured in a DHCPv6 server group.

Format

dhcpv6-server *ipv6-address* [**interface** *interface-type interface-number*]

undo dhcpv6-server *ipv6-address* [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a DHCPv6 server or a next-hop relay agent.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of an outbound interface for DHCPv6 packets. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface.	-

Views

DHCPv6 server group view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6-server** command is used on DHCPv6 relay agents. To ensure that the DHCPv6 relay agent can send DHCPv6 packets to multiple DHCPv6 servers, you can configure multiple DHCPv6 servers in a DHCPv6 server group. Multiple DHCPv6 servers can allocate IPv6 addresses and other network configuration information to DHCPv6 clients through the DHCPv6 relay agent.

A DHCPv6 client and a DHCPv6 server can have multiple DHCPv6 relay agents connected in between. A device functions as a DHCPv6 relay agent. If the device is connected to a DHCPv6 server, you need to specify the IPv6 address for the DHCPv6 server. If the device is connected to a next-hop relay agent, you need to specify the IPv6 address for the next-hop relay agent and specify the IPv6 address of the remote DHCPv6 server or the next-hop relay agent on the next-hop relay agent.

Prerequisites

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. A DHCPv6 server group has been created using the **dhcpv6 server group** command.

Precautions

If a DHCPv6 relay agent is connected to multiple DHCPv6 servers or next-hop relay agents, repeat this step. A maximum of 20 DHCPv6 servers or next-hop relay agents can be connected to the device.

Example

Add the DHCPv6 server at fc00:1::1 to the DHCPv6 server group named dhcp-srv1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 server group dhcp-srv1
[HUAWEI-dhcpv6-server-group-dhcp-srv1] dhcpv6-server fc00:1::1
```

6.11.27 dhcpv6 server database

Function

The **dhcpv6 server database** command enables the device to save DHCPv6 data to storage devices.

The **undo dhcpv6 server database** command disables the device from saving DHCPv6 data to storage devices.

By default, the device is disabled from saving DHCPv6 data to storage devices.

Format

dhcpv6 server database *url* [**write-delay** *interval*]

undo dhcpv6 server database *url*

Parameters

Parameter	Description	Value
url	Specifies the path and name of the file that data is saved to.	The value is a string of 1 to 63 case-insensitive characters without spaces.
write-delay *interval*	Specifies the interval at which DHCPv6 data is saved.	The value is an integer ranging from 300 to 86400, in seconds. The default value is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 or DHCPv6 PD server, run the **dhcpv6 server database** command to enable the device to save DHCPv6 data to storage devices. This avoids data loss caused by device faults. DHCPv6 data includes the last data recording time, address pool name, client DUID, IAID, address and prefix bound to the client DUID and IAID, conflicted address, and conflict detection time.

The device automatically saves current DHCPv6 data at the specified interval, and previous data files are overwritten. The interval can be set using the **write-delay** *interval* parameter.

Precautions

If the DHCPv6 client requests for lease renewal when the device (functioning as the DHCPv6 server) restarts, the device cannot receive the renewal request and the client fails to renew the lease.

Example

Configure the device to save DHCP data to the path flash:/dhcpv6.tbl and set the interval for saving data to 36000s.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 server database flash:/dhcpv6.tbl write-delay 36000
```

6.11.28 dhcpv6 server group

Function

The **dhcpv6 server group** command creates a DHCPv6 server group and enters the DHCPv6 server group view, or enters the view of a DHCPv6 server group that has been created.

The **undo dhcpv6 server group** command deletes a created DHCPv6 server group.

By default, no DHCPv6 server group is created.

Format

dhcpv6 server group *group-name*

undo dhcpv6 server group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCPv6 server group.	The value is a string of 1 to 32 case-sensitive characters without spaces. It can contain digits, letters, and special characters such as underscores (_), hyphens (-), and periods (.). It cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6 server group** command is used on DHCPv6 relay agents. Generally, a DHCPv6 relay agent serves multiple DHCPv6 servers. You can run the **dhcpv6**

server group command to create a DHCPv6 server group to manage all the DHCPv6 servers that share the DHCPv6 relay agent. The DHCPv6 server group allocates IPv6 addresses and other network configuration information to users connected to the DHCPv6 relay agent.

Follow-up Procedure

- After a DHCPv6 server group is configured, run the **dhcpv6-server** command to add DHCPv6 servers to the DHCPv6 server group.
- When configuring IP address for DHCPv6 servers, run the **dhcpv6 relay server-select** command on an interface to select the DHCPv6 server group of the DHCPv6 relay agent.

Precautions

A maximum of 32 DHCPv6 server groups can be configured on the device. A maximum of 20 DHCPv6 servers can be added to a DHCPv6 server group.

Example

Create a DHCPv6 server group named DHCPv6-srv1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 server group DHCPv6-srv1
[HUAWEI-dhcpv6-server-group-DHCPv6-srv1]
```

6.11.29 display dhcpv6 client

Function

The **display dhcpv6 client** command displays DHCPv6 client information.

Format

display dhcpv6 client [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the DHCPv6 client with the specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dhcpv6 client** command on the DHCPv6 client to check the address that is applied.

Example

Display the DHCPv6 client information.

```
<HUAWEI> display dhcpv6 client
Vlanif10 is in stateful DHCPv6 client mode.
Stateful DHCPv6 client is in BOUND state.
Preferred server DUID   : 000300060819A6CDA894
  Reachable via address : FE80::A19:A6FF:FECD:A897
IA NA IA ID 0x00000051 T1 43200 T2 69120
  Obtained     : 2018-04-18 15:08:49
  Renews       : 2018-04-18 15:09:19
  Rebinds      : 2018-04-18 15:09:37
  Address      : FC00:3::2
    Lifetime valid 120 seconds, preferred 60 seconds
    Expires at 2018-04-18 15:10:49(99 seconds left)
DNS server     : FC00:4::1
```

Table 6-78 Description of the display dhcpv6 client command output

Item	Description
Vlanif10 is in stateful DHCPv6 client mode.	The VLANIF10 interface is in stateful DHCPv6 client mode.
Stateful DHCPv6 client is in BOUND state.	The DHCPv6 client is in BOUND state.
Preferred server DUID	DUID of a DHCPv6 server.
Reachable via address	Source IPv6 address from which a DHCPv6 client receives packets.
Obtained	Time at which the DHCPv6 client obtains an IPv6 address.
Renews	Time (T1) at which the DHCPv6 client updates the lease extension time.
Rebinds	Time (T2) at which the DHCPv6 client rebinds the lease extension time.
Address	IPv6 address that the DHCPv6 client obtains.
Lifetime valid 120 seconds, preferred 60 seconds	The valid lifetime is 120 seconds and preferred lifetime is 60 seconds.
Expires at 2018-04-18 15:10:49(99 seconds left)	The address used by the DHCPv6 client will expire at 2018-04-18 15:10:49, and there are 99 seconds left.
DNS server	IPv6 address of the DNS server that the DHCPv6 client obtains.

6.11.30 display dhcpv6 client prefix

Function

The **display dhcpv6 client prefix** command displays the IPv6 address prefix obtained by the device.

Format

display dhcpv6 client prefix [**name** *prefix-name*]

Parameters

Parameter	Description	Value
name *prefix-name*	Specifies the IPv6 address prefix name.	The value must be an existing IPv6 address prefix name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display dhcpv6 client prefix** command to view IPv6 address prefixes on the device that functions as the DHCPv6 client.

Example

Display information about IPv6 prefix named **aaa** obtained by the device.

```
<HUAWEI> display dhcpv6 client prefix name aaa
Prefix name       : aaa
  Prefix          : FC00:3::/64
    Life time(sec): valid 172800 preferred 86400
```

Table 6-79 Description of the **display dhcpv6 client prefix** command output

Item	Description
Prefix name	IPv6 address prefix name.
Prefix	IPv6 address prefix.

Item	Description
Life time(sec)	- valid: Period during which an IPv6 address prefix is valid. - preferred: Period during which an IPv6 address prefix is valid since its lease is renewed.

6.11.31 display dhcpv6 client statistics

Function

The **display dhcpv6 client statistics** command displays DHCPv6 message statistics on the DHCPv6 client.

Format

display dhcpv6 client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCPv6 message statistics on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as a DHCPv6 client, you can run this command to view DHCPv6 message statistics.

Example

Display DHCPv6 message statistics on the DHCPv6 client.

```
<HUAWEI> display dhcpv6 client statistics
 Message statistics of interface Vlanif10:
   Message                 Received
   Advertise               1
   Reply                   1
   Reconfigure             0
   Invalid                 0
```

```
Dropped untrusted reply  0

Message                 Sent
Solicit                1
Request                 1
Confirm                 0
Renew                   0
Rebind                 0
Release                0
Decline                0
Information-request      0
```

Table 6-80 Description of the **display dhcpv6 client statistics** command output

Item	Description
Message	Message type.
Received	Number of received messages.
Advertise	Number of Advertise messages received by the DHCPv6 client.
Reply	Number of Reply messages received by the DHCPv6 client.
Reconfigure	Number of Reconfigure messages received by the DHCPv6 client.
Invalid	Number of unknown-type messages received by the DHCPv6 client.
Dropped untrusted reply	When the **dhcp snooping check local-reply enable** command is configured on a device that functions as a DHCP client, the **dhcp snooping trusted** command must be configured on the interface connected to the DHCP server. Otherwise, the DHCP client discards response messages from the DHCP server.
Sent	Number of sent messages.
Solicit	Number of Solicit messages sent by the DHCPv6 client.
Request	Number of Request messages sent by the DHCPv6 client.
Confirm	Number of Confirm messages sent by the DHCPv6 client.
Renew	Number of Renew messages sent by the DHCPv6 client.
Rebind	Number of Rebind messages sent by the DHCPv6 client.

Item	Description
Release	Number of Release messages sent by the DHCPv6 client.
Decline	Number of Decline messages sent by the DHCPv6 client.
Information-request	Number of Information-request messages sent by the DHCPv6 client.

6.11.32 display dhcpv6 duid

Function

The **display dhcpv6 duid** command displays the DHCP unique identifier of a DHCPv6 device.

Format

display dhcpv6 duid

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A DUID identifies a DHCPv6 device. Each DHCPv6 server or client has a DUID. The **display dhcpv6 duid** command displays the DUID of a device.

Example

Display the DUID of a DHCPv6 device.

```
<HUAWEI> display dhcpv6 duid
The device's DHCPv6 unique identifier: 0001000117C667C280FB063545B3
```

6.11.33 display dhcpv6 relay configuration

Function

The **display dhcpv6 relay configuration** command displays configuration information about a DHCPv6 relay agent.

Format

display dhcpv6 relay configuration [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays configuration information about the DHCPv6 relay agent with the specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command on a DHCPv6 relay agent to check configuration information about a DHCPv6 relay agent including the source interface information and whether the Option79 field is inserted into DHCP messages.

Example

Display configuration information about a DHCPv6 relay agent.

```
<HUAWEI> display dhcpv6 relay configuration
DHCPv6 relay running information: global
Source interface:       -
Option79 insert:        enable
DHCPv6 relay running information: Vlanif10
Source interface:       -
Option79 insert:        enable
```

Table 6-81 Description of the **display dhcpv6 relay configuration** command output

Item	Description
DHCPv6 relay running information	Configuration information about a DHCPv6 relay agent, including configuration information in the global view and interface view.
Source interface	Specifies the interface IPv6 address as the source IPv6 address for sending messages. To configure this item, run the **dhcpv6 relay source-interface** command.
Option79 insert	Whether to insert the Option79 field into DHCPv6 messages. The value can be: ● enable: The Option79 field is inserted into DHCPv6 messages. ● disable: The Option79 field is not inserted into DHCPv6 messages. To configure this item, run the **dhcpv6 relay option79 insert enable** command.

6.11.34 display dhcpv6 relay prefix-delegation

Function

Using the **display dhcpv6 relay prefix-delegation** command, you can view DHCPv6 PD routing information forwarded by the DHCPv6 Relay.

Format

display dhcpv6 relay prefix-delegation { **client** [**interface** *interface-type interface-number*] | **route** [**interface** *interface-type interface-number*] }

Parameters

Parameter	Description	Value
client	Displays information about DHCPv6 PD clients.	-
interface *interface-type interface-number*	Specifies the type and the number of an interface.	-

Parameter	Description	Value
route	Displays routing information learned from DHCPv6 PD clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 relay prefix-delegation** command is used on DHCPv6 relay agents. This command displays routing information that DHCPv6 relay agents learn from DHCPv6 PD terminals, including the destination IPv6 address, next hop address, outbound interface, and protocol type of each route. You can also use this command to view DHCPv6 PD routing information forwarded by the DHCPv6 Relay.

Example

Display DHCPv6 PD routing information forwarded by the DHCPv6 Relay.

```
<HUAWEI> display dhcpv6 relay prefix-delegation route
-------------------------------------------------------------------------------
 Destination   : FC00:1::/96
 Next-hop      : FC00:2::1
 Interface     : Vlanif62
 Protocol type : Unr
 Destination   : FC00:2::/96
 Next-hop      : FC00:2::2
 Interface     : Vlanif62
 Protocol type : Unr
-------------------------------------------------------------------------------
 Total count : 1  Print count : 1
```

Table 6-82 Description of the display dhcpv6 relay prefix-delegation route command output

Item	Description
Destination	Destination network segment of a route.
Next-hop	Next hop address of a route.
Interface	Outbound interface of a route.
Protocol type	Protocol type used by a route.
Total count	Number of routes displayed.

Item	Description
Print count	Number of routes printed. A maximum of 512 routes can be printed.

Display information about DHCPv6 PD terminals.

```
<HUAWEI> display dhcpv6 relay prefix-delegation client
-------------------------------------------------------------------------------
 DUID_EN       : 000612E978E600E04C774E5A
 Interface     : Vlanif62
 IPv6 address  : FC00:1::4E5A
     IA PD     : IA ID 1, T1 600, T2 900,
         IA Prefix: FC00:3::/96
            preferred lifetime 900 , valid lifetime 1200
            expired at 2010.02.21 15:01:54
         IA Prefix: FC00:4::/96
            preferred lifetime 900 , valid lifetime 1200
            expired at 2010.02.21 15:01:54
-------------------------------------------------------------------------------
 Total count : 1  Print count : 1
```

Table 6-83 Description of the display dhcpv6 relay prefix-delegation client command output

Item	Description
DUID_EN	DHCPv6 unique identifier (DUID) of a client, which is defined by the vendor.
Interface	Interface to which a client is connected.
IPv6 address	IPv6 address of a client.
IA PD	IPv6 prefix contained in the packet sent from a client.
Total count	Number of client records displayed.
Print count	Number of client records printed. A maximum of 512 records can be printed.

6.11.35 display dhcpv6 relay statistics

Function

Using the **display dhcpv6 relay statistics** command, you can view the statistics about DHCPv6 messages passing through the DHCPv6 relay agent.

Format

display dhcpv6 relay statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If no interface is specified, the statistics about all the DHCPv6 messages are displayed. If the interface is specified, the statistics about DHCPv6 messages on the specified interface are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is enabled with the DHCPv6 relay function, the system takes the statistics about DHCPv6 messages passing through the DHCP relay agent. After this command is run, you can view the statistics about DHCPv6 messages passing through the DHCP relay agent.

Example

Display the statistics about DHCPv6 messages on VLANIF 10.

```
<HUAWEI> display dhcpv6 relay statistics interface vlanif 10
 Interface Vlanif10 :
 MessageType           Receive        Send           Error
 Solicit               0              0              0
 Advertise             0              0              0
 Request               0              0              0
 Confirm               0              0              0
 Renew                 0              0              0
 Rebind                0              0              0
 Reply                 0              0              0
 Release               0              0              0
 Decline               0              0              0
 Reconfigure           0              0              0
 Information-request   0              0              0
 Relay-forward         0              0              0
 Relay-reply           0              0              0
 UnknownType           0              0              0
```

Table 6-84 Description of the display dhcpv6 relay statistics command output

Item	Description
Interface	Interface enabled with related DHCPv6 functions.
MessageType	Type of DHCPv6 messages.
Receive	Number of received DHCPv6 messages.
Send	Number of sent DHCPv6 messages.
Error	Number of DHCPv6 messages that fail to be parsed.

6.11.36 display dhcpv6 pool

Function

The **display dhcpv6 pool** command displays the IPv6 address pool configurations.

Format

display dhcpv6 pool [*pool-name* [**allocated** { **address** | **prefix** } | **binding** [*duid*] | **conflict address** | *ipv6-address* | *ipv6-prefix/prefix-length*]]

Parameters

Parameter	Description	Value
pool *pool-name*	Specifies the IPv6 address pool name.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allocated { **address** | **prefix** }	Specifies IPv6 addresses or IPv6 address prefixes that have been assigned.	-
binding [*duid*]	Specifies addresses that are bound to DUIDs.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
conflict address	Specifies the conflicted IPv6 addresses in the IPv6 address pool.	-

Parameter	Description	Value
ipv6-address	Specifies IPv6 addresses in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix/prefix-length	Specifies IPv6 prefixes in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 1 to 128.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 pool** command is used on DHCPv6 servers. The **display dhcpv6 pool** command displays information about IPv6 address pool configurations and dynamic address allocation.

Example

Display information about the IPv6 address pool **pool1**.

```
<HUAWEI> display dhcpv6 pool pool1
DHCPv6 pool: pool1
  Address prefix: FC00:1::/64
    Lifetime valid 4294967295 seconds, preferred 4294967295 seconds
    0 in use, 0 conflicts
  Prefix delegation: FC00:3::/60 64
    Lifetime valid 172800 seconds, preferred 86400 seconds
    0 in use
  Information refresh time: 10000
  DNS server address: FC00:4::1
  SIP server address: FC00:3::1
  NIS server address: FC00:1::2
  NISP server address: FC00:1::2
  SNTP server address: FC00:1::1
  Domain name: example.com
  SIP server domain name: sip.com
  NIS server domain name: nis.com
  NISP server domain name: nisp.com
  Vendor-specific option:
    Enterprise ID: 2011
      Suboption 10 address FC00:1::5
  conflict-address expire-time: 61
  renew-time-percent : 55
  rebind-time-percent : 85
  Active normal clients: 0
  Active pd clients: 0    Logging : Enable
```

Table 6-85 Description of the **display dhcpv6 pool** command output

Item	Description
DHCPv6 pool	Name of the IPv6 address pool.
Address prefix	Prefix bound to the IPv6 address pool. You can set the prefix using the **address prefix** command.
Prefix delegation	Agent prefix bound to the IPv6 address pool. You can set the agent prefix using the **prefix-delegation** command.
Information refresh time	Time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration. You can set the time using the **information-refresh** command.
DNS server address	DNS server address configured for the IPv6 address pool. You can configure the DNS server address using the **dns-server** command.
SIP server address	SIP server address configured for the IPv6 address pool. You can configure the SIP server address using the **sip-server** command.
NIS server address	NIS server address configured for the IPv6 address pool. You can configure the NIS server address using the **nis-server** command.
NISP server address	NISP server address configured for the IPv6 address pool. You can configure the NISP server address using the **nisp-server** command.
SNTP server address	SNTP server address configured for the IPv6 address pool. You can configure the SNTP server address using the **sntp-server** command.

Item	Description
Domain name	Domain name suffix allocated by the DHCPv6 server to the client. You can configure the domain name suffix using the **dns-domain-name** command.
SIP server domain name	SIP domain name suffix allocated by the DHCPv6 server to the client. You can configure the SIP domain name suffix using the **sip-domain-name** command.
NIS server domain name	NIS domain name suffix allocated by the DHCPv6 server to the client. You can configure the NIS domain name suffix using the **nis-domain-name** command.
NISP server domain name	NISP domain name suffix allocated by the DHCPv6 server to the client. You can configure the NISP domain name suffix using the **nisp-domain-name** command.
Vendor-specific option	Vendor-defined options. You can configure the vendor-defined options using the **vendor-specific** and **suboption** commands.
conflict-address expire-time	Aging time of conflicted addresses. You can set the aging time using the **conflict-address expire-time** command.
renew-time-percent	The percentage of the lease renewal time in the preferred lifetime. You can set the percentage of the lease renewal time in the preferred lifetime using the **renew-time-percent rebind-time-percent** command.
rebind-time-percent	The percentage of the lease rebinding time in the preferred lifetime. You can set the percentage of the lease rebinding time in the preferred lifetime using the **renew-time-percent rebind-time-percent** command.

Item	Description
Active normal clients	Number of DHCP clients.
Active pd clients	Number of DHCPv6 PD clients.
Logging	Whether the function of recording a log when the DHCPv6 or DHCPv6 PD server allocates an IPv6 address or prefix is enabled. The value can be: ● Enable: The function is enabled. ● Disable: The function is disabled. To configure this item, run the **logging** command.

6.11.37 display dhcpv6 relay

Function

The **display dhcpv6 relay** command displays the configuration of the interface enabled with the DHCPv6 relay function.

Format

display dhcpv6 relay [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the configuration of the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface is specified, the configuration of all the interfaces enabled with the DHCPv6 relay function is displayed.

Example

Display the configurations of all interfaces enabled with the DHCPv6 relay function.

```
<HUAWEI> display dhcpv6 relay
Interface               Mode           Destination
-------------------------------------------------------------------------
GigabitEthernet0/0/1     Relay         FC00:4::3
Vlanif10                Relay         FC00:1::1:1
-------------------------------------------------------------------------------
 Print count : 2                  Total count : 2
```

Table 6-86 Description of the **display dhcpv6 relay** command output

Item	Description
Interface	Interface enabled with DHCPv6 relay functions.
Mode	DHCPv6 function mode.
Destination	Destination address of DHCPv6 relay messages. Address pointing to the DHCPv6 server, address of the next-hop DHCPv6 relay, or DHCPv6 server group. To configure the address, run the **dhcpv6 relay destination** or **dhcpv6 relay server-select** command.
Print count	The number of interfaces enabled with DHCPv6 relay functions that are displayed.
Total count	The total number of interfaces enabled with DHCPv6 relay functions.

6.11.38 display dhcpv6 server

Function

The **display dhcpv6 server** command displays information about the DHCPv6 server function.

Format

display dhcpv6 server [**database** | [**statistics**] [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
database	Displays database configurations.	-
statistics	Displays message statistics on the DHCPv6 server.	-
interface *interface-type interface-number*	Displays information about the DHCP server with a specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 server** command is used on DHCPv6 servers. The **display dhcpv6 server** command displays information about the DHCPv6 server function.

Example

Display information about the DHCPv6 server function.

```
<HUAWEI> display dhcpv6 server
 Interface                          DHCPv6 pool
 Vlanif10                           pool1
```

Table 6-87 Description of the **display dhcpv6 server** command output

Item	Description
Interface	Interface enabled with the DHCPv6 server function.
DHCPv6 pool	Name of the IPv6 pool that is configured on the interface. You can configure the IPv6 pool name using the **dhcpv6 server** command.

6.11.39 display dhcpv6 server group

Function

The **display dhcpv6 server group** command displays the configuration of a DHCPv6 server group.

Format

display dhcpv6 server group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified DHCPv6 server group. If this parameter is not specified, the configuration of all DHCPv6 server groups is displayed.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use Scenario

The **display dhcpv6 server group** command is used on DHCPv6 relay agents. You can run the **display dhcpv6 server group** command to view the configuration of DHCPv6 server groups created on a DHCPv6 relay agent.

Prerequisites

DHCPv6 server groups have been configured on the DHCPv6 relay agent using the **dhcpv6 server group** command.

Example

View the configuration of the DHCPv6 server group named group1 on the DHCPv6 relay agent.

```
<HUAWEI> display dhcpv6 server group group1
 DHCPv6 Group-name   : group1
   (0)   server-ip   : FC00:1::1
```

View the configuration of all the DHCPv6 server groups on the DHCPv6 relay agent.

```
<HUAWEI> display dhcpv6 server group
dhcpv6 server group
-------------------------------------------------------------------------------
 DHCPv6 Group-name   : g1
   (0)   server-ip   : FC00:2::1
   (1)   server-ip   : FC00:2::2
   (2)   server-ip   : FC00:2::3
   (3)   server-ip   : FC00:2::4
   (4)   server-ip   : FC00:2::5
   (5)   server-ip   : FC00:4::1
 DHCPv6 Group-name   : g2
   (0)   server-ip   : FC00:3::111
   (1)   server-ip   : FC00:3::122
   (2)   server-ip   : FC00:3::123
   (3)   server-ip   : FC00:3::124
   (4)   server-ip   : FC00:3::125
   (5)   server-ip   : FC00:3::126
   (6)   server-ip   : FC00:3::127
 DHCPv6 Group-name   : g3
   (0)   server-ip   : FC00:3::1
   (1)   server-ip   : FC00:3::2
   (2)   server-ip   : FC00:3::3
   (3)   server-ip   : FC00:3::4
   (4)   server-ip   : FC00:3::5
   (5)   server-ip   : FC00:3::6
   (6)   server-ip   : FC00:3::7
-------------------------------------------------------------------------------
 Total count : 3
```

Table 6-88 Description of the display dhcpv6 server group command output

Item	Description
DHCPv6 Group-name	Name of a DHCPv6 server group. To set this parameter, run the **dhcpv6 server group** command.
server-ip	IPv6 address of a DHCPv6 server in a DHCPv6 server group. To set this parameter, run the **dhcpv6-server (DHCPv6 server group view)** command.

6.11.40 display dhcpv6 statistics

Function

The **display dhcpv6 statistics** command displays DHCPv6 packet statistics.

Format

display dhcpv6 statistics [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays statistics about socket packet sending failures.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device may become faulty when running the DHCPv6 service. Some fault location methods are required for administrators or device maintenance personnel to locate faults quickly. The most convenient and effective method is to provide statistics about packets and packet loss reasons. Run the **display dhcpv6 statistics** command to view DHCPv6 packet statistics.

Example

Display DHCPv6 packet statistics.

```
<HUAWEI> display dhcpv6 statistics
Input: total 10 packets, discarded 0 packets
  Solicit               :         10,  Advertise             :          0
  Request               :          0,  Confirm               :          0
  Renew                 :          0,  Rebind                :          0
  Reply                 :          0,  Release               :          0
  Decline               :          0,  Reconfigure           :          0
  Information-request   :          0,  Relay-forward         :          0
  Relay-reply           :          0,  Leasequery            :          0
  Leasequery-reply      :          0,

  Max-user limit        :        831,  Add bindtable failed  :        100
Output: total 0 packets, discarded 0 packets
```

Table 6-89 Description of the **display dhcpv6 statistics** command output

Item	Description
Input: total x packets, discarded y packets	Statistics about DHCPv6 packets received by the device. The number of received DHCPv6 packets is x and the number of discarded DHCPv6 packets is y.
Solicit	Number of SOLICIT packets received by the device.

Item	Description
Advertise	Number of ADVERTISE packets received by the device.
Request	Number of REQUEST packets received by the device.
Confirm	Number of CONFIRM packets received by the device.
Renew	Number of RENEW packets received by the device.
Rebind	Number of REBIND packets received by the device.
Reply	Number of REPLY packets received by the device.
Release	Number of RELEASE packets received by the device.
Decline	Number of DECLINE packets received by the device.
Reconfigure	Number of RECONFIGURE packets received by the device.
Information-request	Number of INFORMATION-REQUEST packets received by the device.
Relay-forward	Number of RELAY-FORW packets received by the device.
Relay-reply	Number of RELAY-REPL packets received by the device.
Leasequery	Number of LEASEQUERY packets received by the device.
Leasequery-reply	Number of LEASEQUERY-REPLY packets received by the device.

Item	Description
Max-user limit or Add bindtable failed	Information displayed if the DHCPv6 service is abnormal. The displayed information includes: ● Max-user limit: Total number of DHCPv6 messages discarded because the maximum number of users (configured by running the **dhcp snooping max-user-number** command) is exceeded. ● Add bindtable failed: Total number of DHCPv6 packets discarded because dynamic binding entries are added. New dynamic binding entries may be added if the user-side interface is Down, or IPSG is configured but ACL resources are insufficient. ● High cpu occupancy: Total number of DHCPv6 packets discarded because the CPU usage is excessively high. ● Port blocked: Total number of DHCPv6 packets discarded because the inbound interface is blocked. ● Rx buffers full: Total number of DHCPv6 packets discarded because the remaining queue length is shorter than the reserved threshold. ● L2fdb lookup failed: Total number of DHCPv6 Reply packets discarded because the DHCP snooping module fails to find user-side interfaces. ● Bad vlan id: Total number of DHCPv6 packets discarded because the interfaces receiving the DHCPv6 packets are not added to the VLANs corresponding to the VLAN tags carried in the packets or the DHCPv6 packets received on interfaces carry VLAN tags not in the range from 1 to 4094. ● Memory exhausted: Total number of DHCPv6 packets discarded because the memory is exhausted. ● L3if protocol down: Total number of DHCPv6 packets discarded because

Item	Description
	the Layer 3 protocol of the source interface goes Down. ● Rate limit: Total number of DHCPv6 packets discarded because rates of the messages exceed the limit, when the **dhcpv6 packet-rate** or **dhcp snooping check dhcpv6-rate enable** command is configured. ● Bad packet length: Total number of DHCPv6 packets discarded because the packet length is not in the range of 50 to 2048 bytes. ● Bad ip header checksum: Total number of DHCPv6 packets discarded because the checksum of the IP header is incorrect. ● Bad request: Total number of invalid DHCPv6 request packets that are discarded, when the **dhcp snooping check dhcp-request enable** or **dhcp snooping check dhcpv6-request mac** command is configured to check the validity of DHCPv6 request packets. ● Bad reply: Total number of DHCPv6 response packets discarded by untrusted interfaces configured with the **dhcp snooping enable** command. ● Client transferred: Total number of DHCPv6 packets discarded because the **undo dhcp snooping user-transfer enable** command is configured to disable interface flapping. ● Other error: Total number of DHCPv6 packets discarded due to other reasons.
Output: total x packets, discarded y packets	Statistics about DHCPv6 packets sent by the device. The number of sent DHCPv6 packets is x and the number of discarded DHCPv6 packets is y.

6.11.41 dns-domain-name

Function

The **dns-domain-name** command configures the DNS domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo dns-domain-name** command deletes the assigned domain name suffix.

By default, no DNS domain name suffix is configured for the DHCPv6 client.

Format

dns-domain-name *dns-domain-name*

undo dns-domain-name *dns-domain-name*

Parameters

Parameter	Description	Value
dns-domain-name	Specifies the DNS domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to only hyphens (-) or hyphens (--).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies a domain name suffix when allocating IPv6 addresses for clients. You can use the **dns-domain-name** command on the DHCPv6 server to specify a domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffix to the clients.

Precautions

A maximum of four different DNS domain names can be configured for an IPv6 address pool.

Example

Configure the domain name suffix assigned to the DHCPv6 client as **example.com** for the address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] dns-domain-name example.com
```

6.11.42 dns-server (IPv6 address pool view)

Function

The **dns-server** command configures a DNS server address for the DHCPv6 address pool.

The **undo dns-server** command deletes the configured DNS server address.

By default, no DNS server address is configured for the IPv6 address pool.

Format

dns-server *ipv6-address*

undo dns-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	DNS server IPv6 address configured for the DHCPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-server** command is used on DHCPv6 servers. Before a host accesses the Internet, a DNS server needs to resolve the accessed domain name to an IP address. The DHCPv6 server needs to specify the IPv6 address of the DNS server for the global address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the DNS server when allocating IPv6 addresses to the clients.

Precautions

- To specify multiple DNS servers, run the **dns-server** command to configure multiple DNS server addresses.
- A maximum of two DNS server addresses can be configured for each IPv6 address pool. The first assigned DNS server address is used as a primary address. The priority of the first configured DNS server is higher than that of the other DNS server.

Example

Specify a DNS server with the IPv6 address fc00:1::1 for domain name resolution when IP addresses in the address pool **global1** are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] dns-server fc00:1::1
```

6.11.43 excluded-address

Function

The **excluded-address** command specifies the range of the IPv6 addresses that cannot be automatically assigned to clients from the IPv6 address pool.

The **undo excluded-address** command deletes the specified range of the IPv6 addresses that cannot be automatically assigned to clients from the address pool.

By default, all IPv6 addresses in the address pool can be automatically assigned to clients.

Format

excluded-address *start-ipv6-address* [**to** *end-ipv6-address*]

undo excluded-address *start-ipv6-address* [**to** *end-ipv6-address*]

Parameters

Parameter	Description	Value
start-ipv6-address	Specifies the start IPv6 address that cannot be automatically assigned.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
to *end-ipv6-address*	Specifies the end IPv6 address that cannot be automatically assigned.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *end-ipv6-address* and *start-ipv6-address* must be on the same network segment and *end-ipv6-address* must be greater than *start-ipv6-address*. If *end-ipv6-address* is not specified, only the *start-ipv6-address* cannot be automatically assigned.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **excluded-address** command is used on DHCPv6 servers. In an address pool, some IPv6 addresses need to be reserved for other services, and some IPv6 addresses are statically assigned to certain hosts (such as the DNS server and Web server) and cannot be automatically assigned to clients. You can run the **excluded-address** command to specify the range of the IPv6 addresses that cannot be automatically assigned to clients from the IPv6 address pool.

Prerequisites

1. An address pool has been created by using the **dhcpv6 pool** command.
2. Bind an IPv6 address prefix to an address pool by using the **address prefix**

Precautions

- The excluded IPv6 address or IPv6 address segment must be in the local address pool.
- The excluded IPv6 address or IPv6 address segment cannot be automatically assigned to clients from a local address pool.

- If you run the **excluded-address** command multiple times, you can specify multiple IPv6 addresses or IPv6 address segments that cannot be automatically assigned to clients.

Example

Specify IPv6 addresses fc00:1::1 to fc00:1::10 not to be automatically allocated from the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] address prefix fc00:1::/64
[HUAWEI-dhcpv6-pool-global1] excluded-address fc00:1::1 to fc00:1::10
```

6.11.44 information-refresh

Function

The **information-refresh** command configures the time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.

The **undo information-refresh** command restores the default time for updating IPv6 address pool configurations.

By default, the time for updating IPv6 address pool configurations is 86400s (24 hours).

Format

information-refresh *time*

undo information-refresh

Parameters

Parameter	Description	Value
time	Specifies the time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.	The value is an integer that ranges from 600 to 4294967295, in seconds.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

The **information-refresh** command is used on DHCPv6 servers. When the DHCPv6 server assigns configuration parameters such as the DNS, NIS, and SNTP server addresses to the DHCPv6 clients through stateless autoconfiguration, you can use the **information-refresh** command to configure the time for updating these configuration parameters.

NOTE

If a Huawei device functions as a DHCPv6 client and the time configured using the **information-refresh** command on the DHCPv6 server is larger than three days (259200 seconds), the time for updating DHCPv6 client configuration information is three days. If the time configured using the **information-refresh** command on the DHCPv6 server is less than or equal to three days, the time for updating DHCPv6 client configuration information is the actually configured value.

Example

Set the time for updating configuration parameters assigned to clients to 10000s in the address pool pool1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] information-refresh 10000
```

6.11.45 ipv6 address auto dhcp

Function

The **ipv6 address auto dhcp** command enables an interface to obtain IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

The **undo ipv6 address auto dhcp** command disables an interface from obtaining IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

By default, the interface is disabled from obtaining IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

Format

ipv6 address auto dhcp [**hint** *ipv6-address*] [**rapid-commit**] [**unicast-option**]

undo ipv6 address auto dhcp

Parameters

Parameter	Description	Value
hint *ipv6-address*	Specifies the IPv6 address applied by a DHCPv6 client.	The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters. The format is X:X:X:X:X:X:X:X.
rapid-commit	Specifies that a DHCPv6 client applies for an IPv6 address using two-message exchange.	-
unicast-option	Specifies that a DHCPv6 client applies for an IPv6 address using a unicast option.	-

Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **ipv6 address auto dhcp** [**rapid-commit**] command on the device that functions as a DHCPv6 client, the client uses stateful DHCPv6 address autoconfiguration to obtain IPv6 addresses and other configuration parameters, such as addresses of the DNS and SNTP servers, from the DHCPv6 server.

Prerequisites

1. IPv6 functions have been enabled globally using the **ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **ipv6 enable** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local** or **ipv6 address** *ipv6-address* **link-local** command in the interface view.
4. The interface has been configured to automatically learn the IPv6 default route using the **ipv6 address auto global default** command in the interface view.

Precautions

The DHCPv6 server assigns an IPv6 address and other configuration parameters to a DHCPv6 client using two-message exchange only when two-message exchange is configured on both the server and client. If two-message exchange is not configured on the server or client, the server assigns an IPv6 address and other configuration parameters to the client using four-message exchange. Two-message exchange applies to the scenarios with one DHCPv6 server, while four-message exchange applies to the scenarios with multiple DHCPv6 servers.

Example

Configure the interface VLANIF100 to obtain IPv6 addresses and other configuration parameters from the DHCPv6 server using DHCPv6 stateful address autoconfiguration.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto link-local
[HUAWEI-Vlanif100] ipv6 address auto dhcp
```

Configure the interface GE0/0/1 to obtain IPv6 addresses and other configuration parameters from the DHCPv6 server using DHCPv6 stateful address autoconfiguration.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto dhcp
```

6.11.46 link-address

Function

The **link-address** command configures the network prefix in the IPv6 address pool view.

The **undo link-address** command deletes the network prefix configured in the IPv6 address pool view.

By default, no network prefix is configured in the IPv6 address pool view.

Format

link-address *ipv6-prefix/ipv6-prefix-length*

undo link-address *ipv6-prefix/ipv6-prefix-length*

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the network prefix and prefix length.	*ipv6-prefix*: The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 16 to 128.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DHCPv6 client needs to apply for network configuration information (for example, the IP address of the DNS server) except for the IPv6 address from the DHCPv6 server. If the **address prefix** is not configured in the IPv6 address pool, you can run the **link-address** command to configure the network prefix in the IPv6 address pool view.

When functioning as a DHCPv6 or DHCPv6 PD server, the device may be configured with multiple IPv6 address pools. After receiving the DHCPv6 request packets, the DHCPv6 or DHCPv6 PD server chooses the IPv6 address pool based on the following rules:

- When the device functions as the DHCPv6 server:
  - If a relay exists, the server chooses the address pool that belongs to the same link scope with the configured network prefix (using the **link-address** or **address prefix** command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - When the DHCPv6 server is enabled in the system view, the DHCPv6 server cannot assign network parameters (such as IPv6 addresses, DNS, NIS, and SNTP servers) to clients if no relay exists. To enable the DHCPv6 server to assign network parameters, enable the DHCPv6 server function in the interface view.
- When the device functions as the DHCPv6 PD server:
  - If a relay exists, choose the address pool in the same link scope with the configured network prefix (using the **link-address** command) based on

the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.

- If no relay exists, the DHCPv6 PD server function cannot be enabled in the system view and can be enabled in the interface view, using the **dhcpv6 server** command.

Prerequisites

Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).

Example

Bind the IPv6 address prefix fc00:1::/64 to the DHCPv6 server address pool named pool1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] link-address fc00:1::/64
```

6.11.47 lock (IPv6 address pool view)

Function

The **lock** command locks the IPv6 address pool.

The **undo lock** command unlocks the address pool.

By default, the IPv6 address pool is unlocked.

Format

lock

undo lock

Parameters

None

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **lock** command is used on DHCPv6 servers. When a DHCPv6 server needs to be migrated, you simply need to migrate address pools on the DHCPv6 server to another DHCPv6 server on the live network. To retain the addresses that have been assigned to clients from a global address pool, run the **lock** command to lock the global address pool. When new users get online, they apply for IPv6 addresses from a new address pool.

Precautions

After the **lock** command is executed, the IPv6 address pool is locked. The locked IPv6 address pool does not assign addresses or extend address lease but only release addresses.

Example

Lock the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] lock
```

6.11.48 logging (IPv6 address pool view)

Function

The **logging** command enables the function of recording a log when the DHCPv6 or DHCPv6 PD server allocates an IPv6 address or prefix in the IPv6 address pool view.

The **undo logging** command disables the function of recording a log when the DHCPv6 or DHCPv6 PD server allocates an IPv6 address or prefix in the IPv6 address pool view.

By default, this function is disabled.

Format

logging [**allocation-address-success** | **allocation-prefix-success** | **detect-address-conflict** | **release-address-success** | **release-prefix-success** | **renew-address-success** | **renew-prefix-success**] *

undo logging [**allocation-address-success** | **allocation-prefix-success** | **detect-address-conflict** | **release-address-success** | **release-prefix-success** | **renew-address-success** | **renew-prefix-success**] *

Parameters

NOTE

If the following parameters are not specified, the function of recording related logs is enabled or disabled.

Parameter	Description	Value
allocation-address-success	Displays a log when an IPv6 address is successfully allocated.	-
allocation-prefix-success	Displays a log when an IPv6 prefix is successfully allocated.	-
detect-address-conflict	Displays a log when an IPv6 address conflict is detected.	-
release-address-success	Displays a log when an IPv6 address is released.	-
release-prefix-success	Displays a log when an IPv6 prefix is released.	-
renew-address-success	Displays a log when an IPv6 address is renewed.	-
renew-prefix-success	Displays a log when an IPv6 prefix is renewed.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applied to the DHCPv6 or DHCPv6 PD server. After the **logging** command is configured, the server records a log if an IPv6 address or prefix is allocated, renewed, or released, or an IPv6 address or prefix conflict is detected, facilitating routine maintenance and fault locating.

You can run the **display dhcpv6 pool** command to check the status of the log recording function on the server.

Prerequisites

An IPv6 address pool has been created using the **dhcpv6 pool** command.

Precautions

- After the log recording function is enabled, the server may frequently record logs if a large number of clients request for IPv6 addresses or prefixes, deteriorating device performance.
- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default

settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration in the *CLI-based Configuration - Device Management Configuration Guide*.

For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the function of recording a log when the server allocates an IPv6 address or prefix in the IPv6 address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] logging
```

6.11.49 nis-domain-name

Function

The **nis-domain-name** command configures the NIS domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo nis-domain-name** command deletes the NIS domain name suffix assigned to the DHCPv6 client.

By default, no NIS domain name suffix is configured for the DHCPv6 client.

Format

nis-domain-name *nis-domain-name*

undo nis-domain-name *nis-domain-name*

Parameters

Parameter	Description	Value
nis-domain-name	Specifies the NIS domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to a single hyphen (-) or consecutive hyphens (--).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nis-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an NIS domain name suffix when allocating IPv6 addresses for clients. You can use the **nis-domain-name** command on the DHCPv6 server to specify a NIS domain name suffix for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the NIS domain name suffix to the clients.

Precautions

A maximum of four different NIS domain names can be configured for an IPv6 address pool.

Example

Configure the NIS domain name assigned to the DHCPv6 client as **nis.com** for the address pool pool1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] nis-domain-name nis.com
```

6.11.50 nisp-domain-name

Function

The **nisp-domain-name** command configures the NISP domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo nisp-domain-name** command deletes the assigned NISP domain name suffix.

By default, no NISP domain name suffix is configured for the DHCPv6 client.

Format

nisp-domain-name *nisp-domain-name*

undo nisp-domain-name *nisp-domain-name*

Parameters

Parameter	Description	Value
nisp-domain-name	Specifies the NISP domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to only hyphens (-) or hyphens (--).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nisp-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an NISP domain name suffix when allocating IPv6 addresses for clients. You can use the **nisp-domain-name** command on the DHCPv6 server to specify a NISP domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffix to the clients.

Precautions

A maximum of four different NISP domain name suffixes can be configured for an IPv6 address pool.

Example

Configure the NISP domain name assigned to the DHCPv6 client as **nisp.com** for the address pool pool1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] nisp-domain-name nisp.com
```

6.11.51 nisp-server

Function

The **nisp-server** command configures the NISP server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo nisp-server** command deletes the configured NISP server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no NISP server address is configured for the IPv6 address pool.

Format

nisp-server *ipv6-address*

undo nisp-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Indicates the NISP server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nisp-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the NISP server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the NISP server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two NISP server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple NISP servers are specified, you need to run the **nisp-server** repeatedly to configure multiple addresses.

Example

Specify fc00:1::2 as the IPv6 address of the NISP server when the IPv6 addresses in the address pool global1 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] nisp-server fc00:1::2
```

6.11.52 nis-server

Function

The **nis-server** command configures the NIS server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo nis-server** command deletes the configured NIS server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no NIS server address is configured for the IPv6 address pool.

Format

nis-server *ipv6-address*

undo nis-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Indicates the NIS server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nis-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the NIS server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the NIS server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two NIS server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple NIS servers are specified, you need to run the **nis-server** repeatedly to configure multiple addresses.

Example

Specify fc00:1::2 as the IPv6 address of the NIS server when IPv6 addresses in the address pool **global1** are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] nis-server fc00:1::2
```

6.11.53 prefix-delegation

Function

The **prefix-delegation** command configures an agent prefix in the address pool view.

The **undo prefix-delegation** command deletes the agent prefix in the address pool view.

By default, no IPv6 address agent prefix is configured in the address pool view.

Format

prefix-delegation *ipv6-prefix/ipv6-prefix-length assign-prefix-length* [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

prefix-delegation *ipv6-prefix/ipv6-prefix-length assign-prefix-length* [**life-time preferred-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]] **valid-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]]

prefix-delegation *ipv6-prefix/ipv6-prefix-length* **lock**

undo prefix-delegation *ipv6-prefix/ipv6-prefix-length* [**lock**]

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the address prefix and the prefix length bound to an IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 1 to 128.

Parameter	Description	Value
assign-prefix-length	Specifies the default prefix length. **NOTE** If the DHCPv6 server has been configured to allocate prefix lengths based on the DHCPv6 client requests, and the client-requested prefix length is within the range from *ipv6-prefix-length* to *assign-prefix-length*, the server allocates the prefix length based on the client request. If the client-requested prefix length is not within the preceding range or the server is not configured to allocate prefix lengths based on the DHCPv6 client requests, the server allocates the default prefix length. You can run the **dhcpv6 server allow-hint** or **dhcpv6 server** *pool-name* **allow-hint** command to configure the server to allocate prefix lengths based on the DHCPv6 client requests.	The value is an integer that ranges from 1 to 128. The *assign-prefix-length* must be greater than or equal to *ipv6-prefix-length*. The difference between the *assign-prefix-length* and *ipv6-prefix-length* must be less than or equal to 16.
life-time	Specifies the lifetime of the address prefix bound to an IPv6 address pool.	-
valid-lifetime	Specifies the valid lifetime.	The value ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

Parameter	Description	Value
preferred-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the preferred lifetime of the IPv6 prefix. The time must be no less than 1 minute.	● *days*: indicates days. The value is an integer that ranges from 0 to 1999. ● *hours*: indicates hours. The value is an integer that ranges from 0 to 23. ● *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. ● *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
valid-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the valid lifetime of the IPv6 prefix. The time must be no less than 1 minute and cannot be less than the preferred lifetime.	● *days*: indicates days. The value is an integer that ranges from 0 to 1999. ● *hours*: indicates hours. The value is an integer that ranges from 0 to 23. ● *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. ● *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
lock	Locks the address prefix.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 PD server, run the **prefix-delegation** command to configure an agent prefix in the address pool view. The DHCPv6 PD client divides the obtained prefix into prefixes of subnet segments and sends an RA message on the network segment that hosts directly connect to or exchange information with hosts using the DHCPv6 protocol. The RA message contains the prefixes of subnet segments. This enables hosts to automatically configure addresses.

Precautions

- Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).
- The agent prefix cannot be overlapped.
- The agent prefix cannot be overlapped with the address prefix.
- The agent prefix cannot be overlapped with the prefix statically specified by a certain user.
- When the prefix pool is deleted, all prefix leases are deleted.
- Only one agent prefix can be configured for an address pool.

Example

Configure the agent prefix of the DHCPv6 server as fc00:1::/30 for the address pool pool1, set the prefix length to 42 and the lifetime to infinite.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] prefix-delegation fc00:1::/30 42 life-time infinite infinite
```

6.11.54 renew-time-percent rebind-time-percent

Function

The **renew-time-percent rebind-time-percent** command configures the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime of an IPv6 address pool.

The **undo renew-time-percent rebind-time-percent** command restores the default percentage of the lease renewal time and the default percentage of the rebinding time in the preferred lifetime of an IPv6 address pool.

By default, the percentage of the lease renewal time in the preferred lifetime of an IPv6 address pool is 50%, and the percentage of the rebinding time is 80%.

Format

renew-time-percent *renew-time-percent* **rebind-time-percent** *rebind-time-percent*

undo renew-time-percent rebind-time-percent

Parameters

Parameter	Description	Value
renew-time-percent	Specifies the percentage of the lease renewal time in the preferred lifetime of an IPv6 address pool.	The value is an integer that ranges from 10 to 89. The default value is 50.
rebind-time-percent	Specifies the percentage of the rebinding time in the preferred lifetime of an IPv6 address pool. The value of *rebind-time-percent* must be greater than that of *renew-time-percent*, and the difference between the values must be greater than or equal to 10.	The value is an integer that ranges from 20 to 99. The default value is 80.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to change the lease renewal time and rebinding time in an IPv6 address pool.

NOTE

When planning the lease renewal time and rebinding time, you can run the **address prefix** and **renew-time-percent rebind-time-percent** commands to configure the preferred lifetime and the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime respectively. If the lease renewal time and rebinding time are too short, the lease and renewal time (T1 and T2) of IPv6 addresses allocated to DHCPv6 clients by the DHCPv6 server are too short. As a result, DHCPv6 clients send lease renewal packets frequently. It is recommended that you set the lease renewal time and rebinding time based on the actual usage scenario.

Example

Configure the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime of the IPv6 address pool **test**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool test
[HUAWEI-dhcpv6-pool-test] renew-time-percent 55 rebind-time-percent 85
```

6.11.55 reset dhcpv6 client statistics

Function

The **reset dhcpv6 client statistics** command clears DHCPv6 message statistics on the DHCPv6 client.

Format

reset dhcpv6 client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears DHCPv6 message statistics on a specified interface. If no interface is specified, all message statistics on the DHCPv6 client are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the DHCPv6 client. Collecting statistics about the DHCPv6 messages sent and received within a specified period helps you locate DHCPv6 faults. Before collecting new statistics, run the **reset dhcpv6 client statistics** [**interface** *interface-type interface-number*] command to clear the existing message statistics. After clearing existing statistics, run the **display dhcpv6 client statistics** [**interface** *interface-type interface-number*] command to view latest message statistics.

Example

Clear message statistics on the DHCPv6 client.

```
<HUAWEI> reset dhcpv6 client statistics
```

6.11.56 reset dhcpv6 pool

Function

The **reset dhcpv6 pool** command clears the IPv6 address pool configured on the device.

Format

reset dhcpv6 pool *pool-name* [**allocated** { **address** | **prefix** } | **binding** [*duid*] | **conflict address** | *ipv6-address* [**to** *ipv6-address*] | *ipv6-prefix/prefix-length*]

Parameters

Parameter	Description	Value
pool *pool-name*	Specifies the IPv6 address pool name.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allocated { **address** | **prefix** }	Deletes IPv6 addresses or IPv6 address prefixes that have been assigned.	-
binding [*duid*]	Deletes addresses that are bound to DUIDs.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
conflict address	Resets the conflicted IPv6 addresses in the IPv6 address pool.	-
ipv6-address [**to** *ipv6-address*]	Resets IPv6 addresses in the IPv6 address pool. If only one IPv6 address is entered, only the entered IPv6 address is reset.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix/prefix-length	Resets IPv6 prefixes in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 16 to 128

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset dhcpv6 pool** command resets the address pool status. If an IPv6 address conflict occurs because two clients use the same IPv6 address, you need to set the IPv6 address pool to idle.

Precautions

If a user's IPv6 address is within the IPv6 address range specified when this command is run, the user cannot continue to use the IPv6 address after this command is run, and needs to send an IPv6 address application request again.

The address pool status cannot be restored after this command is run. Therefore, exercise caution when deciding to run this command.

Example

Set the status of all the conflicted IPv6 addresses in the IPv6 address pool mypool to idle.

```
<HUAWEI> reset dhcpv6 pool mypool conflict address
```

6.11.57 reset dhcpv6 relay prefix-delegation route

Function

The **reset dhcpv6 relay prefix-delegation route** command deletes routing information learned from DHCPv6 PD terminals on a DHCPv6 relay agent.

Format

reset dhcpv6 relay prefix-delegation route [**vpn6-instance** *vpn-instance-name*] *ipv6-address mask-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the destination IPv6 address of the routes to be deleted.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.

Parameter	Description	Value
mask-length	Specifies the mask length of the IPv6 address.	The value is an integer ranging from 0 to 128
vpn6-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset dhcpv6 relay prefix-delegation route** command is used on DHCPv6 relay agents. Before collecting routing information about a specified IPv6 address, run the **reset dhcpv6 relay prefix-delegation route** command to delete the existing routing information.

Example

Delete routing information with destination IPv6 address fc00:1::1 learned from DHCPv6 PD terminals.

```
<HUAWEI> reset dhcpv6 relay prefix-delegation route fc00:1::1 64
```

6.11.58 reset dhcpv6 relay statistics

Function

The **reset dhcpv6 relay statistics** command clears DHCPv6 message statistics on the DHCPv6 relay agent.

Format

reset dhcpv6 relay statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If no interface is specified, all the DHCPv6 message statistics are cleared. If an interface is specified, DHCPv6 message statistics on the specified interface are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If a device is enabled with the DHCPv6 relay function, the system takes the statistics about DHCPv6 messages passing through the DHCP relay agent. You can use the **reset dhcpv6 relay statistics** command to clear current message statistics on the DHCPv6 relay agent.

Example

Clear the DHCPv6 message statistics on VLANIF 10.

```
<HUAWEI> reset dhcpv6 relay statistics interface vlanif 10
```

6.11.59 reset dhcpv6 server statistics

Function

The **reset dhcpv6 server statistics** command clears DHCPv6 message statistics on the DHCPv6 server.

Format

reset dhcpv6 server statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If a device is enabled with the DHCPv6 server function, the system takes the statistics about DHCPv6 messages passing through the DHCPv6 server. You can use the **reset dhcpv6 server statistics** command to clear current message statistics on the DHCPv6 server.

If no interface is specified, all the DHCPv6 message statistics are cleared. If an interface is specified, DHCPv6 message statistics on the specified interface are cleared.

Example

Clear DHCPv6 message statistics.

```
<HUAWEI> reset dhcpv6 server statistics
```

6.11.60 reset dhcpv6 statistics

Function

The **reset dhcpv6 statistics** command clears DHCPv6 packet statistics.

Format

reset dhcpv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Collecting statistics about the DHCPv6 messages sent and received within a specified period helps you locate DHCPv6 faults. Before collecting new statistics, run the **reset dhcpv6 statistics** command to clear the existing message statistics. After clearing existing statistics, run the **display dhcpv6 statistics** command to view latest message statistics.

Example

Clear DHCPv6 packet statistics.

```
<HUAWEI> reset dhcpv6 statistics
```

6.11.61 sip-domain-name

Function

The **sip-domain-name** command configures the SIP domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo sip-domain-name** command deletes the assigned SIP domain name suffix.

By default, no SIP domain name suffix is configured for the DHCPv6 client.

Format

sip-domain-name *sip-domain-name*

undo sip-domain-name *sip-domain-name*

Parameters

Parameter	Description	Value
sip-domain-name	Specifies the SIP domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to a single hyphen (-) or consecutive hyphens (--).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sip-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an SIP domain name when allocating IPv6 addresses for clients. You can use the **sip-domain-name** command on the DHCPv6 server to specify a SIP domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffixes to the clients.

Precautions

A maximum of four SIP domain name suffixes can be configured for an IPv6 address pool.

Example

Configure the SIP domain name assigned to the DHCPv6 client as **sip.com** for the address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] sip-domain-name sip.com
```

6.11.62 sip-server (IPv6 address pool view)

Function

The **sip-server** command configures the SIP server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo sip-server** command deletes the configured SIP server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no SIP server address is configured for the IPv6 address pool.

Format

sip-server *ipv6-address*

undo sip-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	SIP server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sip-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the SIP server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the SIP server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured for each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple SIP servers are specified, you need to run the **sip-server** repeatedly to configure multiple addresses.

Example

Specify fc00:3::1 as the IPv6 address of the SIP server when the assigned IPv6 address belongs to the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] sip-server fc00:3::1
```

6.11.63 sntp-server

Function

The **sntp-server** command configures the SNTP server IPv6 address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo sntp-server** command deletes the configured SNTP server IPv6 address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no SNTP server IPv6 address is configured for the IPv6 address pool.

Format

sntp-server *ipv6-address*

undo sntp-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an SNTP server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sntp-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the SNTP server for the IPv6 address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the SNTP server when allocating IPv6 addresses to the clients. After the clients receive the IPv6 address of the SNTP server, the clients synchronize the system time with the specified SNTP server.

Precautions

- A maximum of two SNTP server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple SNTP servers are specified, you need to run the **sntp-server** command repeatedly to configure multiple addresses.

Example

Specify fc00:1::1 as the IPv6 address of the SNTP server when IPv6 addresses in the address pool **global1** are assigned.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] sntp-server fc00:1::1
```

6.11.64 static-bind address

Function

The **static-bind address** command statically binds an IPv6 address to the client DUID in the DHCPv6 address pool view.

The **undo static-bind address** command deletes the statically bound entries between the IPv6 address and the client DUID in the DHCPv6 address pool view.

By default, no IPv6 address is bound to the client DUID in the address pool view.

Format

static-bind address *ipv6-address* **duid** *client-duid* [**iaid** *iaid*] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

undo static-bind address *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address statically bound to an address pool.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.
duid *client-duid*	Configures the DUID of the DHCPv6 client that is statically bound to the IPv6 address.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
iaid *iaid*	Specifies IA identifier value.	The value is an integer that ranges from 1 to 4294967295.
life-time	Specifies the lifetime of the bound entries.	-
valid-lifetime	Specifies the valid lifetime of the bound entries.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime of the bound entries.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.

Parameter	Description	Value
infinite	Sets the lifetime of the bound entries to infinite.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind address** command is used on DHCPv6 servers. If some special clients need to be statically assigned with fixed IPv6 addresses, bind the DUIDs of these clients to the IPv6 addresses. When receiving a request from a special client for requesting an IPv6 address, a DHCPv6 server assigns the fixed IPv6 address bound to the client DUID to this client.

Prerequisites

1. An address pool has been created by using the **dhcpv6 pool** command.
2. Bind an IPv6 address prefix to an address pool by using the **address prefix**

Example

Bind the IPv6 address fc00:1::2 with the client with DUID abcdef in address pool pool1 and set the lifetime to infinite.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] address prefix fc00:1::/64
[HUAWEI-dhcpv6-pool-pool1] static-bind address fc00:1::2 duid abcdef life-time infinite infinite
```

6.11.65 static-bind prefix

Function

The **static-bind prefix** command statically binds an IPv6 address prefix to the DHCPv6 PD client in the DHCPv6 address pool view.

The **undo static-bind prefix** command unbinds the IPv6 address prefixes from the DHCPv6 PD clients in the DHCPv6 address pool view.

By default, no IPv6 address prefix is bound to the DHCPv6 PD client in the address pool view.

Format

static-bind prefix *ipv6-prefix/ipv6-prefix-length* **duid** *client-duid* [**iaid** *iaid-value*] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

undo static-bind prefix *ipv6-prefix/ipv6-prefix-length*

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the IPv6 address prefix that is statically bound to an address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M.
duid *client-duid*	Specifies the DUID of the DHCPv6 PD client that is statically bound to the IPv6 address prefix.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
iaid *iaid-value*	Specifies the IAID of the DHCPv6 PD client that is statically bound to the IPv6 address prefix.	The value is an integer that ranges from 1 to 4294967295.
life-time	Specifies the lifetime of the bound entries.	-
valid-lifetime	Specifies the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind prefix** command is used on DHCPv6 PD servers. If some special DHCPv6 PD clients need to be statically assigned with fixed IPv6 address prefixes, bind the DUIDs and IAIDs of these clients to the IPv6 address prefixes. When receiving a request for applying for an IP address prefix from a special DHCPv6 PD client, a DHCPv6 PD server assigns the fixed IPv6 address prefix bound to the DUIDs and IAIDs to this client.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Precautions

- When assigning addresses for DHCPv6 PD clients, bind the address prefix to the DUID of the client. The IAID of the client cannot be specified.
- The statically bound prefix cannot be overlapped with the prefix that is configured using the **prefix-delegation** command.

Example

Bind the IPv6 address prefix fc00:1::/64 to the DHCPv6 PD client with DUID abcdef and IAID 12 in address pool pool1 and set the lifetime of the binding entries to infinite.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] static-bind prefix fc00:1::/64 duid abcdef iaid 12 life-time infinite infinite
```

6.11.66 suboption

Function

The **suboption** command configures vendor-defined DHCPv6 sub-options.

The **undo suboption** command deletes vendor-defined DHCPv6 sub-options.

By default, no vendor-defined DHCPv6 sub-option is configured.

Format

suboption *suboption-code* { **address** *ipv6-address* &<1-4> | **ascii** *ascii-string* | **hex** *hex-string* }

undo suboption *suboption-code*

Parameters

Parameter	Description	Value
suboption-code	Specifies the code of the vendor-defined DHCPv6 sub-options.	The value is an integer that ranges from 1 to 65535.
address *ipv6-address*	Specifies the vendor-defined option code as the IPv6 address type.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
ascii *ascii-string*	Specifies the vendor-defined option code as an ASCII character string.	The value is a string of 1 to 255 characters.
hex *hex-string*	Specifies the vendor-defined option code as a hexadecimal string.	The value is a hexadecimal numeral string with an even number of characters (such as aa or aaaa). The even number ranges from 2 to 128.

Views

Vendor-defined mode view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **suboption** command is used on DHCPv6 servers. Run the **vendor-specific** command to enter the vendor-defined mode. In this mode, configure the vendor-defined DHCPv6 options. The DHCPv6 device can carry vendor-defined options such as the TFTP server name and address, and the configuration file of the device.

The **suboption** command configures vendor-defined DHCPv6 sub-options.

Precautions

A maximum of 16 vendor-defined sub-options can be configured in the vendor-defined mode view.

Example

Set Huawei-defined sub-option 10 to fc00:1::5 in the IPv6 address pool pool1 view.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] vendor-specific 2011
[HUAWEI-dhcpv6-pool-pool1-vs-2011] suboption 10 address fc00:1::5
```

6.11.67 vendor-specific

Function

The **vendor-specific** command configures vendor-defined options for the IPv6 address pool and enter the vendor-defined mode view.

The **undo vendor-specific** command deletes vendor-defined options configured for the IPv6 address pool.

By default, no vendor-defined option is configured.

Format

vendor-specific *vendor-id*

undo vendor-specific *vendor-id*

Parameters

Parameter	Description	Value
vendor-id	Indicates the ID of the vendor, which is assigned by the IANA. 2011 is the identifier for Huawei.	The value is an integer that ranges from 1 to 4294967295.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vendor-specific** command is used on DHCP servers. You can use the **vendor-specific** command to enter the vendor-defined mode. In this mode, you can configure the vendor-defined DHCPv6 options. The DHCPv6 device can carry vendor-defined options such as the TFTP server name and address, and the configuration file of the device.

Precautions

A maximum of eight vendor-defined modes are configured for one IPv6 address pool.

Example

Configure Huawei-defined options for the IPv6 address pool pool1.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] vendor-specific 2011
```

6.12 IPv6 DNS Configuration Commands

6.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

6.12.2 display dns ipv6 dynamic-host

Function

The **display dns ipv6 dynamic-host** command displays IPv6 dynamic DNS entries.

Format

display dns ipv6 dynamic-host [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IPv6 dynamic DNS entries of a specified VPN instance.	The value must be an existing VPN instance name.
all	Displays all IPv6 dynamic DNS entries, including both public and private DNS entries. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public IPv6 dynamic DNS entries are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dns ipv6 dynamic-host** command to view IPv6 dynamic DNS entries and check whether domain names match the mapping entries.

Example

Display IPv6 dynamic DNS entries.

```
<HUAWEI> display dns ipv6 dynamic-host
No  Domain-name       Ipv6Address     TTL
1   example           FC00:1::1       6
```

Display IPv6 dynamic DNS entries of the VPN instance vpn1.

```
<HUAWEI> display dns ipv6 dynamic-host vpn-instance vpn1
No      Domain-name                              Ipv6Address         TTL          VPN-Instance
1       example                                  2001:db8::2         6            vpn1
```

Table 6-90 Description of the **display dns ipv6 dynamic-host** command output

Item	Description
No	Sequence number of a dynamic IPv6 DNS entry.
Domain-name	Domain name.
Ipv6Address	IPv6 address mapping the domain name.
TTL	TTL value of the dynamic domain names in the cache (in seconds).
VPN-Instance	VPN instance name.

6.12.3 display ipv6 host

Function

The **display ipv6 host** command displays the IPv6 static DNS entries.

Format

display ipv6 host [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IPv6 static DNS entries of a specified VPN instance.	The value must be an existing VPN instance name.
all	Displays all IPv6 static DNS entries, including both public and private static DNS entries. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public IPv6 static DNS entries are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **ipv6 host** command to configure IPv6 static DNS entries, you can run this command to check whether mappings between host names and IPv6 addresses are correct.

Example

Display IPv6 static DNS entries.

```
<HUAWEI> display ipv6 host
Host                Age      Flags         IPv6Address(es)
www.example.com      0         static          FC00:1::8
www.sohu.com         0         static          FC00:1::9
```

Display IPv6 static DNS entries of the VPN instance vpn1.

```
<HUAWEI> display ipv6 host vpn-instance vpn1
Host          Age        Flags       IPv6Address(es)        VPN-Instance
RTB           0          static      2001:db8::1            vpn1
```

Table 6-91 Description of the **display ipv6 host** command output

Item	Description
Host	Host name. The value is set using the **ipv6 host** command.

Item	Description
Age	Aging time. The value 0 indicates that the entry is not aged out.
Flags	Identifiers. The value static indicates a static domain name.
IPv6Address(es)	IPv6 address mapping the domain name. The value is set using the **ipv6 host** command.
VPN-Instance	VPN instance name. The value is set using the **ipv6 host** command.

6.12.4 dns server ipv6

Function

The **dns server ipv6** command configures the IPv6 address of a DNS server.

The **undo dns server ipv6** command deletes the IPv6 address of a DNS server.

By default, no IPv6 addresses of DNS servers are configured.

Format

dns server ipv6 *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for a DNS server.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an outbound interface that communicates with the DNS server.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DNS client must work with the DNS server to implement dynamic domain name resolution. You can run the **dns server ipv6** command to specify the IPv6 address of the DNS server. The DNS client sends requests to the specified DNS server for domain name resolution.

During dynamic domain name resolution, the switch sends a domain name resolution request to the DNS servers according to the order in which they were configured. If the domain name resolution request on the first DNS server times out, the device sends the request to the next DNS server.

Precautions

The IPv6 address of the DNS server must be a global unicast address or link-local address.

- If a link-local address is configured as the IPv6 address of the DNS server, specify the outbound interface for communicating with the DNS server.
- If a global unicast address is configured as the IPv6 address of the DNS server, do not specify the outbound interface for communicating with the DNS server.

A maximum of six DNS server IP (IPv4 and IPv6) addresses can be configured on the switch.

If **vpn-instance** *vpn-instance-name* is specified, the system sends domain name resolution requests only to the DNS servers bound to the specified VPN instance.

Example

Configure the IPv6 address of the DNS server to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dns server ipv6 fc00:1::1
```

6.12.5 dns server ipv6 source-ip

Function

The **dns server ipv6 source-ip** command configures the source IPv6 address for the local end functioning as the DNS client to communicate with the DNS server.

The **undo dns server ipv6 source-ip** command deletes the source IPv6 address used for the local end functioning as the DNS client to communicate with the DNS server.

By default, no source IPv6 address is configured for the local end functioning as the DNS client to communicate with the DNS server.

Format

dns server ipv6 source-ip *ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo dns server ipv6 source-ip [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address for the local end functioning as the DNS client to communicate with the DNS server.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source IPv6 address is specified, the DNS client uses the specified IPv6 address to communicate with the DNS server. This ensures communication security. If no source IPv6 address is specified, the DNS client needs to select a source IPv6 address according to the destination address each time it sends an IPv6 DNS request.

Precautions

If only one route from the DNS server to the client with an IPv6 address is reachable, you need to specify the source IPv6 address in the DNS query message when the DNS client sends a DNS query to the server.

If **vpn-instance** *vpn-instance-name* is specified, the specified source IPv6 address is used only when the device communicates with the DNS server bound to the specified VPN instance.

Example

Configure the source IPv6 address that the DNS client uses to communicate with the DNS server to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dns server ipv6 source-ip fc00:1::1
```

6.12.6 ipv6 host

Function

The **ipv6 host** command configures an IPv6 static DNS entry.

The **undo ipv6 host** command deletes an IPv6 static DNS entry.

By default, no IPv6 static DNS entry is configured.

Format

ipv6 host *host-name ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo ipv6 host *host-name* [*ipv6-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 255 case-sensitive characters without any space. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address mapping the host name.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When requesting the IPv6 address mapping a domain name, the DNS client searches for the specified domain name in the static DNS table to obtain the corresponding IPv6 address. The **ipv6 host** command configures an IPv6 static DNS entry.

Precautions

Each domain name supports a maximum of eight IPv6 addresses.

Example

Configures an IPv6 static DNS entry mapping the host named **www.example.com**.

```
<HUAWEI> system-view
[HUAWEI] ipv6 host www.example.com fc00:1::8
```

6.12.7 reset dns ipv6 dynamic-host

Function

The **reset dns ipv6 dynamic-host** command clears IPv6 dynamic DNS entries.

Format

reset dns ipv6 dynamic-host [**vpn-instance** *vpn-instance-name* | **all**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears IPv6 dynamic DNS entries of a specified VPN instance.	The value must be an existing VPN instance name.
all	Clears all IPv6 dynamic DNS entries, including both public and private DNS entries. **NOTE** If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public IPv6 dynamic DNS entries are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After confirming the action of deleting IPv6 dynamic DNS entries, you can run the **reset dns ipv6 dynamic-host** command to delete them.

Precautions

IPv6 dynamic DNS entries cannot be restored after being deleted. Confirm the action before you run the command.

Example

Clear all IPv6 dynamic DNS entries.

```
<HUAWEI> reset dns ipv6 dynamic-host all
```

6.13 IPv6 over IPv4 Tunnel Configuration Commands

6.13.1 Command Support

Only the following switch models support the IPv6 over IPv4 Tunnel:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

6.13.2 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Establish a manual IPv6 over IPv4 tunnel between VLANIF 10 at 10.1.1.1 on switch HUAWEI1 and VLANIF 20 at 10.2.1.1 on switch HUAWEI2.

```
<HUAWEI1> system-view
[HUAWEI1] interface tunnel 1
[HUAWEI1-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI1-Tunnel1] source 10.1.1.1
[HUAWEI1-Tunnel1] destination 10.2.1.1
<HUAWEI2> system-view
[HUAWEI2] interface tunnel 1
[HUAWEI2-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI2-Tunnel1] source 10.2.1.1
[HUAWEI2-Tunnel1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel1 to 10.1.1.1 that belongs to vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] destination vpn-instance vpn1 10.1.1.1
```

6.13.3 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is an integer that ranges from 0 to 2047 .

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

Follow-up Procedure

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Example

Create a tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1]
```

6.13.4 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel. The following types of interfaces are often used: VLANIF and loopback.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the source address of the local tunnel interface is the destination address of the remote tunnel interface, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Example

Set the tunnel type of Tunnel1 to IPv6 over IPv4 of manual mode and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI-Tunnel1] source 10.1.1.1
```

Configure Tunnel1 of GRE and use Loopback1 address as the interface address.

```
<HUAWEI> system-view
[HUAWEI] interface Loopback 1
[HUAWEI-LoopBack1] ip address 10.2.1.1 32
[HUAWEI-LoopBack1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] source loopback 1
```

6.13.5 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** | **ipv6-ipv4** [**6to4** | **isatap**] | **ipv4-ipv6** | **mpls te** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicate that the GRE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameters.	-
ipv4-ipv6	Indicate that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameter.	-
ipv6-ipv4 [**6to4** | **isatap**]	Configure the tunnel protocol of the tunnel interface as ipv6-ipv4: ● **ipv6-ipv4**: use a manual IPv6 over IPv4 tunnel ● **ipv6-ipv4 6to4** : using 6to4 tunnel ● **ipv6-ipv4 isatap** : using isatap tunnel **NOTE** Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support these parameter.	-

Parameter	Description	Value
mpls te	Indicate that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730-S, S6730S-S, and S6730S-H support the parameter.	-
none	Indicate that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface.

Example

Set the tunnel encapsulation mode of Tunnel2 to GRE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 2
[HUAWEI-Tunnel2] tunnel-protocol gre
```

6.14 IPv4 over IPv6 Tunnel Configuration Commands

6.14.1 Command Support

Only the following switch models support IPv4 over IPv6 Tunnel:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S

6.14.2 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command. You can run this command to obtain tunnel interface information when configuring tunnels or when locating the fault on these tunnels.

Prerequisites

Before run **display interface tunnel**, please ensure that tunnel interface has been created using the **interface tunnel** command.

Example

Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-11-16 19:16:33 UTC+08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.2.1.2 (Vlanif1234), destination 10.2.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2012-11-16 19:17:39+08:00
Last 300 seconds input rate 16 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  5 packets, 650 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 6-92 Description of the display interface tunnel command output

Item	Description
Tunnel1 current state	Physical layer status of the tunnel interface: - UP: The interface is in normal state. - Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.

Item	Description
Line protocol current state	Link protocol status: ● UP: The link layer protocol of the tunnel interface works normally. ● Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time the link layer protocol of the tunnel interface goes UP. **NOTE** This field is displayed only when the link layer protocol status of the tunnel interface is UP.
Description	Description of the tunnel interface.
Route Port	Indicates the Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.3.1.2/24	IP address of the tunnel interface is 10.3.1.2. The mask is 24 bits, that is, 255.255.255.0.
Encapsulation is TUNNEL,	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.2.1.2 (Vlanif1234)	The source address of the tunnel is 10.2.1.2. That is, the IP address of the VLANIF 1234 interface sending packets at the source side is 10.2.1.2.
destination 10.2.1.1	Destination address of the tunnel.
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.

Item	Description
keepalive enable period 5 retry-times 3	The keepalive function of GRE.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization : --	Input bandwidth usage.
Output bandwidth utilization : --	Output bandwidth usage.

6.14.3 tunnel ipv4-ipv6 encapsulation-limit

Function

The **tunnel ipv4-ipv6 encapsulation-limit** command configures the maximum number of times that IPv6 encapsulation can be performed on embedded nodes of the IPv4 over IPv6 tunnel after an IPv4 packet is encapsulated the first time.

The **undo tunnel ipv4-ipv6 encapsulation-limit** command closes the function of IPv6 encapsulation on embedded nodes of the IPv4 over IPv6 tunnel.

By default, a maximum of four times of IPv6 encapsulation can be performed on embedded nodes of the IPv4 over IPv6 tunnel.

Format

tunnel ipv4-ipv6 encapsulation-limit *encapsulation-limit*

undo tunnel ipv4-ipv6 encapsulation-limit

Parameters

Parameter	Description	Value
encapsulation-limit	Specifies the maximum number of times for performing IPv6 encapsulation on embedded nodes of the IPv4 over IPv6 tunnel.	The value is an integer that ranges from 0 to 255.

Views

System view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum number of times that IPv6 encapsulation can be performed on embedded nodes of the IPv4 over IPv6 tunnel is the value of the tunnel encapsulation limit option carried in the destination option extension header in the IPv6 tunnel header.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Prerequisites

Before running the **tunnel ipv4-ipv6 encapsulation-limit** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

Precautions

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

When Huawei devices communicate with non-Huawei devices, you must run the **undo tunnel ipv4-ipv6 encapsulation-limit** command to restore the maximum number of times that IPv6 encapsulation on embedded nodes of the IPv4 over IPv6 tunnel can be performed after an IPv4 packet is encapsulated the first time to the default value.

Example

Set the maximum number of times of IPv6 encapsulation to be performed on the embedded nodes of the specified IPv4 over IPv6 tunnel to 3.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 encapsulation-limit 3
```

Set the maximum number of times of IPv6 encapsulation to be performed on the embedded nodes of all specified IPv4 over IPv6 tunnels to 3 on the local device.

```
<HUAWEI> system-view
[HUAWEI] tunnel ipv4-ipv6 encapsulation-limit 3
```

6.14.4 tunnel ipv4-ipv6 flow-label

Function

The **tunnel ipv4-ipv6 flow-label** command sets the flow label value.

The **undo tunnel ipv4-ipv6 flow-label** command restores the default flow label value.

The default flow label value is 0.

Format

tunnel ipv4-ipv6 flow-label *label-value*

undo tunnel ipv4-ipv6 flow-label

Parameters

Parameter	Description	Value
label-value	Specifies the flow label value.	The value is an integer that ranges from 0 to 1048575.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

The flow label value of the tunnel refers to the value specified in the flow label field in the IPv6 packet header on the inbound interface of the tunnel.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 flow-label** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the flow label value of a specified IPv4 over IPv6 tunnel to 10.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 flow-label 10
```

Set the flow label value of all the IPv4 over IPv6 tunnels on the local device to 10.

```
<HUAWEI> system-view
[HUAWEI] tunnel ipv4-ipv6 flow-label 10
```

6.14.5 tunnel ipv4-ipv6 hop-limit

Function

The **tunnel ipv4-ipv6 hop-limit** command sets the hop limit of the IPv6 tunnel packets.

The **undo tunnel ipv4-ipv6 hop-limit** command restores the hop limit of the IPv6 tunnel packets to the default value.

By default, the hop limit of the IPv6 tunnel packets is 64.

Format

tunnel ipv4-ipv6 hop-limit *hop-limit*

undo tunnel ipv4-ipv6 hop-limit

Parameters

Parameter	Description	Value
hop-limit	Specifies the hop limit of the IPv6 tunnel packets.	The value is an integer that ranges from 1 to 255.

Views

system view, Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Setting the hop limit of the IPv6 tunnel packets can terminate the packet transmission when routing loops occur on the IPv6 tunnel. To make IPv6 tunnel packets reach the egress of the tunnel, the tunnel hop limit cannot be set too small.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.

- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 hop-limit** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the hop limit of the specified tunnel interface to 100.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 hop-limit 100
```

6.14.6 tunnel ipv4-ipv6 traffic-class

Function

The **tunnel ipv4-ipv6 traffic-class** command sets the traffic level of the IPv4 over IPv6 tunnel.

The **undo tunnel ipv4-ipv6 traffic-class** command restores the traffic level to the default value.

By default, the traffic level of the IPv4 over IPv6 tunnel is 0.

Format

tunnel ipv4-ipv6 traffic-class { **original** | *class-value* }

undo tunnel ipv4-ipv6 traffic-class

Parameters

Parameter	Description	Value
original	Indicates that the value of the Traffic Class field in the IPv6 field of the IPv4 over IPv6 tunnel header uses the value in Traffic Class field of the original packet.	-
class-value	Specifies the traffic level of the IPv4 over IPv6 tunnel.	The value is an integer that ranges from 0 to 255.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traffic level of the IPv4 over IPv6 tunnel packets refers to the value of the traffic class field in the tunnel packet header of the ingress on the tunnel.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Prerequisites

Before running the **tunnel ipv4-ipv6 traffic-class** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

Precautions

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the traffic level of the specified IPv4 over IPv6 tunnel to 10.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 traffic-class 10
```

Set the traffic level of all the IPv4 over IPv6 tunnels on the local device to 10.

```
<HUAWEI> system-view
[HUAWEI] tunnel ipv4-ipv6 traffic-class 10
```

7 IP Unicast Routing Commands

7.1 Static Route Configuration Commands

7.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.1.2 ip route recursive-lookup bgp-vpnv4-route

Function

The **ip route recursive-lookup bgp-vpnv4-route enable** command enables a device to recurse static routes to cross routes on the remote VPN.

The **ip route recursive-lookup bgp-vpnv4-route disable** command disables a device from recursing static routes to cross routes on the remote VPN.

The **undo ip route recursive-lookup bgp-vpnv4-route disable** command enables a device to recurse static routes to cross routes on the remote VPN.

By default, a static route can recurse to a cross route on the remote VPN.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

ip route recursive-lookup bgp-vpnv4-route { **enable** | **disable** }

undo ip route recursive-lookup bgp-vpnv4-route disable

Parameters

Parameter	Description	Value
enable	Enables a device to recurse static routes to cross routes on the remote VPN.	-
disable	Disables a device from recursing static routes to cross routes on the remote VPN.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Recursion is required if next hops of static routes are not directly reachable. You can run the **ip route recursive-lookup bgp-vpnv4-route enable** command to enable the device to recurse a static route to a cross route on the remote VPN. The static route can then inherit the Label and Token information about the cross route. The device can forward data through the tunnel to which the static route recurses.

Precautions

The **ip route recursive-lookup bgp-vpnv4-route enable** command and the **undo ip route recursive-lookup bgp-vpnv4-route disable** command have the same function and do not generate configurations in the configuration file.

This command allows IPv4 static routes to recurse to cross routes on the remote VPN, not applicable to IPv6 static routes.

Example

Enable a device to recurse static routes to a cross route on the remote VPN.

```
<HUAWEI> system-view
[HUAWEI] ip route recursive-lookup bgp-vpnv4-route enable
```

Disable a device from recursing static routes to a cross route on the remote VPN.

```
<HUAWEI> system-view
[HUAWEI] ip route recursive-lookup bgp-vpnv4-route disable
```

Enable a device to recurse static routes to a cross route on the remote VPN.

```
<HUAWEI> system-view
[HUAWEI] undo ip route recursive-lookup bgp-vpnv4-route disable
```

7.1.3 ip route recursive-lookup blackhole protocol static

Function

The **ip route recursive-lookup blackhole protocol static disable** command disables a device from recursing static routes to blackhole routes.

The **ip route recursive-lookup blackhole protocol static enable** command allows a device to recurse static routes to blackhole routes.

The **undo ip route recursive-lookup blackhole protocol static disable** command allows a device to recurse static routes to blackhole routes.

By default, static routes can recurse to blackhole routes.

Format

ip route recursive-lookup blackhole protocol static { **disable** | **enable** }

undo ip route recursive-lookup blackhole protocol static disable

Parameters

Parameter	Description	Value
disable	Disables a device from recursing static routes to blackhole routes.	-
enable	Allows a device to recurse static routes to blackhole routes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If IGP, static, and blackhole routes exist on a network and a link fault occurs, services may be interrupted because static routes may recurse to blackhole routes and remain active. To ensure uninterrupted services, run the **ip route recursive-lookup blackhole protocol static disable** command. This command will prevent static routes from recursing to blackhole routes so that static routes will become inactive and IGP routes will be selected.

Precautions

The **ip route recursive-lookup blackhole protocol static enable** and **undo ip route recursive-lookup blackhole protocol static disable** commands have the same function. You only need to run one of them.

Example

Disable a device from recursing static routes to blackhole routes.

```
<HUAWEI> system-view
[HUAWEI] ip route recursive-lookup blackhole protocol static disable
```

Allow a device to recurse static routes to blackhole routes.

```
<HUAWEI> system-view
[HUAWEI] ip route recursive-lookup blackhole protocol static enable
```

Allow a device to recurse static routes to blackhole routes.

```
<HUAWEI> system-view
[HUAWEI] undo ip route recursive-lookup blackhole protocol static disable
```

7.1.4 ip route recursive-lookup inherit-label-route enable

Function

The **ip route recursive-lookup inherit-label-route enable** command allows a device to recurse routes to cross routes on the remote VPN.

The **undo ip route recursive-lookup inherit-label-route enable** command disables a device from recursing routes to cross routes on the remote VPN.

By default, routes except static routes cannot recurse to cross routes on the remote VPN.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

ip route recursive-lookup inherit-label-route enable

undo ip route recursive-lookup inherit-label-route enable

Parameters

None

Views

System view

Default Level

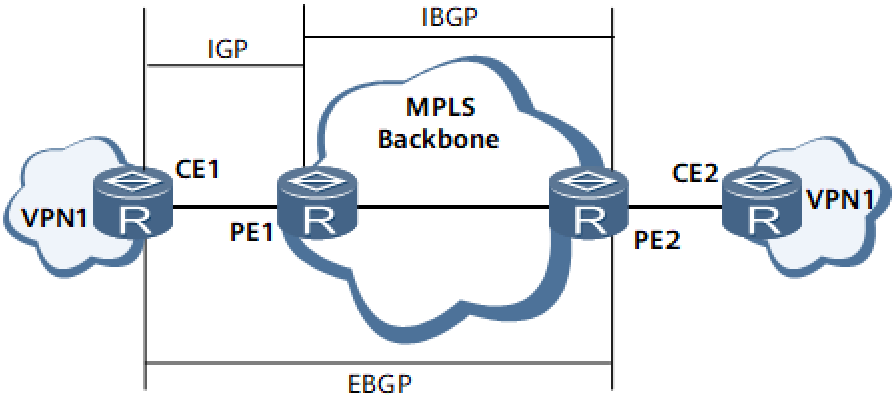
2: Configuration level

Usage Guidelines

Recursion is required if the next hop of a route is unreachable. To allow routes to recurse to cross routes on the remote VPN, run the **ip route recursive-lookup inherit-label-route enable** command. After the command is run, routes inherit the labels and tokens of the cross routes on the remote VPN, ensuring correct traffic forwarding. This command mainly applies to BGP/MPLS IP VPN scenarios.

In **Figure 7-1**, PE1 and PE2 are IBGP peers, and CE1 and PE1 are IGP neighbors. PE2 learns the IP address of CE1's loopback interface, and an EBGP peer relationship is established between CE1 and PE2 using loopback interface IP addresses. By default, the BGP routes that PE2 learns from CE1 through the EBGP peer connection cannot recurse to cross routes on the remote VPN. As a result, traffic fails to be forwarded. To address this problem, run the **ip route recursive-lookup inherit-label-route enable** command to allow the BGP routes to recurse to cross routes on the remote VPN. After the BGP routes inherit the labels and tokens of the cross routes, traffic can be correctly forwarded.

Figure 7-1 Basic BGP/MPLS IP VPN networking



Example

Allow a device to recurse routes to cross routes on the remote VPN.

```
<HUAWEI> system-view
[HUAWEI] ip route recursive-lookup inherit-label-route enable
```

7.1.5 ip route-static

Function

The **ip route-static** command configures a unicast static route.

The **undo ip route-static** command deletes a unicast static route.

By default, no unicast static route is configured.

Format

ip route-static *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-instance-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * [**track** { **route-monitor-group** *route-monitor-group-name* | **bfd-session** *cfg-name* | **efm-state** *interface-type interface-number* | **nqa** *admin-name test-name* } | **permanent**] [**description** *text*]

ip route-static *ip-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name* [**preference** *preference* | **tag** *tag*] * [**description** *text*] (supported only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

undo ip route-static *ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** | **efm-state** } | **permanent**]

undo ip route-static [**track bfd-session**] **all**

undo ip route-static *ip-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name* (supported only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation.
mask	Specifies a subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length. The 1s in each 32-bit mask must be consecutive. Therefore, a mask in dotted decimal notation can be presented by a mask length.	The value is an integer in the range from 0 to 32.

Parameter	Description	Value
nexthop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of an interface that forwards packets.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. If a VPN instance name is specified, the device searches the routing table of the VPN instance for a static route according to *nexthop-address*. If the *nexthop-address* parameter is not specified, the device searches a specified VPN instance forwarding table if the device fails to find a forwarding path in the public network forwarding table.	The value is a string of 1 to 31 case-sensitive characters with spaces. The string can contain spaces if it is enclosed with double quotation marks (").
preference *preference*	Specifies the preference of a static route. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255. The default value is 60.
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.
track route-monitor-group *route-monitor-group-name*	Binds a static route to a route monitoring group for fast fault detection.	The value is a string of 1 to 31 case-sensitive characters.
track bfd-session *cfg-name*	Binds a static BFD session to a static route for fast fault detection.	*cfg-name* is a string of 1 to 15 characters without spaces. The string can contain spaces if it is enclosed with double quotation marks (").

Parameter	Description	Value
track efm-state *interface-type interface-number*	Detects the EFM OAM state of a specified interface.	-
track nqa *admin-name test-name*	Specifies the administrator name of an NQA test instance bound to a static route, and the name of the test instance.	The values of *admin-name* and *test-name* are both a string of 1 to 32 case-sensitive characters without spaces.
permanent	Configures permanent advertisement of static routes.	-
description *text*	Configures a description for a static route.	The value is a string of 1 to 80 characters that can contain spaces.
all	Deletes all IPv4 unicast static routes.	-

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **track bfd-session** *cfg-name* parameter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a simple network, you can configure static routes to ensure network connectivity. If a switch cannot use dynamic routing protocols for network connectivity, static routes can be configured on the switch.

Precautions

When configuring unicast static routes, note the following:

- Only public routes support tunnel recursion.
- If no preference is set for a static route, the static route uses the default preference 60.

- When both the destination IP address and the mask are set to 0.0.0.0, a default route is configured. If the switch cannot find a route in the routing table to forward packets, the switch uses the default route to forward packets.
- By setting different preferences, you can implement different routing management policies. For example, if multiple routes to the same destination are configured with the same preference, load balancing can be implemented. If multiple routes to the same destination are configured with different preferences, route backup can be implemented.
- You can specify the **description** *text* parameter to add a description for a static route so that the administrator can easily check and maintain the static route. You can run the **display this** command in the system view or run the **display current-configuration** command to view the descriptions of static routes.
- When configuring static routes, you can specify outbound interfaces or next-hop addresses based on the outbound interface type. For example, you can specify only outbound interfaces for static routes on P2P interfaces and specify only next hops for static routes on NBMA interfaces, and you must specify next hops for static routes on broadcast interfaces.
- Static routes with the next hop associated with DHCP cannot work in load balancing mode with static routes with the same prefix and not associated with DHCP.
- In some cases, for example, the link layer protocol is PPP and the peer IP address is unknown, you can also specify outbound interfaces when configuring a switch. In this manner, you do not need to modify the switch configuration when the peer IP address changes.
- When a static route to be configured is a supernet route, you need to specify both the outbound interface and next-hop address for it. Otherwise, this route cannot be activated. A route that meets either of the following conditions is a supernet route:
  - When bitwise AND operations are performed on the destination address mask with the destination address and next hop address, the two obtained network addresses are the same, and the destination address mask is greater than or equal to the next hop address mask.
  - When bitwise AND operations are performed on the destination address mask with the destination address and next hop address, the two obtained network addresses are different. When bitwise AND operations are performed on the next hop address mask with the destination address and next hop address, however, the two obtained network addresses are the same.

Example

Set a static route with the destination address and mask are both 0.0.0.0 and the next-hop address 172.16.0.1.

```
<HUAWEI> system-view
[HUAWEI] ip route-static 0.0.0.0 0.0.0.0 172.16.0.1
```

7.1.6 ip route-static default-preference

Function

The **ip route-static default-preference** command sets a default preference for an IPv4 static route.

The **undo ip route-static default-preference** command restores the default preference of IPv4 static routes.

By default, the default preference of IPv4 static routes is 60.

Format

ip route-static default-preference *preference*

undo ip route-static default-preference

Parameters

Parameter	Description	Value
preference	Specifies a default preference for IPv4 static routes. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can change the status of a route by changing the preference of the route. You can use the **ip route-static default-preference** command to change the default preference of all the new IPv4 static routes.

Configuration Impact

After the **ip route-static default-preference** command is used, all the new IPv4 static routes that use the default preference are restored to a new default preference.

Precautions

After a default preference is specified, the new default preference is valid for subsequent rather than existing IPv4 static routes.

Example

Set the default preference of IPv4 static routes to 70.

```
<HUAWEI> system-view
[HUAWEI] ip route-static default-preference 70
```

7.1.7 ip route-static track bfd-session admindown invalid

Function

The **ip route-static track bfd-session admindown invalid** command disables a switch from selecting a static route if the BFD session associated with the route is in the AdminDown state.

The **undo ip route-static track bfd-session admindown invalid** command restores the default configuration.

By default, a static route can participate in route selection even if its bound BFD session is in the AdminDown state.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ip route-static track bfd-session session-name *bfd-name* **admindown invalid**

undo ip route-static track bfd-session session-name *bfd-name* **admindown invalid**

undo ip route-static track bfd-session admindown invalid

Parameters

Parameter	Description	Value
session-name *bfd-name*	Specifies a BFD session bound to a static route.	The value is a string of 1 to 15 case-insensitive characters without spaces. If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if a BFD session associated with a static route is in the AdminDown state, the route can participate in route selection on Huawei switches, but is not allowed for route selection on some non-Huawei devices. As a result, Huawei switches cannot communicate with such non-Huawei devices.

To address this problem, run the **ip route-static track bfd-session admindown invalid** command to configure the device not to select the static route if its bound BFD session is in the AdminDown state.

Prerequisites

The BFD session specified by *bfd-name* has been created.

Example

Disable a switch from selecting a static route if the BFD session associated with the route is in AdminDown state.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd bfda bind peer-ip 1.1.1.1
[HUAWEI-bfd-session-bfda] discriminator local 20
[HUAWEI-bfd-session-bfda] discriminator remote 10
[HUAWEI-bfd-session-bfda] commit
[HUAWEI-bfd-session-bfda] quit
[HUAWEI] ip route-static track bfd-session session-name bfda admindown invalid
```

7.1.8 ip route-static vpn-instance

Function

The **ip route-static vpn-instance** command configures a static route for a VPN instance.

The **undo ip route-static vpn-instance** command deletes static routes from a VPN instance.

By default, no static route is configured for a VPN instance.

Format

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } { *nexthop-address* [**public**] | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-destination-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** *cfg-name* | **efm-state** *interface-type interface-number* | **nqa** *admin-name test-name* } | **permanent**] [**description** *text*]

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } { **public** | **vpn-instance** *vpn-destination-name* } [**preference** *preference* | **tag** *tag*] * [**description** *text*] (supported only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

undo ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** | **efm-state** } | **permanent**]

undo ip route-static vpn-instance *vpn-source-name* **all**

undo ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } { **public** | **vpn-instance** *vpn-destination-name* } (supported only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
vpn-instance *vpn-source-name*	Specifies the name of the source VPN instance. Each VPN instance has its own routing table. The configured static routes are added to the routing table of the specified VPN instance.	The value must be an existing VPN instance name.
destination-address	Specifies the destination IP address of a static route.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	The value is an integer that ranges from 0 to 32.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the outbound interface of a static route.	-
nexthop-address	Specifies the next-hop address of a static route. If the outbound interface of a static route is a broadcast interface, the next-hop address must be specified for the static route.	The value is in dotted decimal notation.
public	Specifies the next-hop address as a public network address but not an address in the source VPN instance. If the *nexthop-address* parameter is not specified, a device searches another outbound interface in the public IP routing table if the device fails to find a forwarding path in the current VPN instance forwarding table.	-
preference *preference*	Specifies the preference of a static route.	The value is an integer that ranges from 1 to 255. If this parameter is not specified, the default preference of a static route is 60.
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.
track bfd-session *cfg-name*	Binds a static BFD session to a static route for fast fault detection.	*cfg-name* is a string of 1 to 15 characters without spaces.
track efm-state *interface-type interface-number*	Detects the EFM OAM state of a specified interface.	-

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the administrator name of an NQA test instance bound to a static route, and the name of the test instance.	The values of *admin-name* and *test-name* are both a string of 1 to 32 case-sensitive characters without spaces.
permanent	Configures permanent advertisement of static routes.	-
description *text*	Specifies the description of a static route. You can specify **description** to add a description for static routes, facilitating static route query and maintenance.	The value is a string of 1 to 80 characters that can contain spaces.
vpn-instance *vpn-destination-name*	Specifies the name of the destination VPN instance. The system searches the routing table of the VPN instance for the outbound interface of a static route according to the configured next-hop address. If the *nexthop-address* parameter is not specified, a device searches another specified VPN instance forwarding table if the device fails to find a forwarding path in the current VPN instance forwarding table. If **vpn-instance** *vpn-destination-name* is specified, devices can communicate with each other between VPNs.	The value is a string of 1 to 31 case-sensitive characters with spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all	Deletes all static routes from a VPN instance.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to configure static routes for a VPN instance on a PE in the following scenarios:

- The PE connects to a CE.
- The specified VPN connects to the Internet.

Follow-up Procedure

After a static route is configured, import the static route to BGP running between PEs if the static route needs to be sent to the peer PE.

Precautions

- During the configuration of a static route for a VPN instance, the next-hop address can belong to the VPN instance or a public network. When the next-hop address of the static route is a public network address, specify **public** after *nexthop-address*.
- If the outbound interface of a static route is a broadcast interface, you must specify the next-hop address for the static route.
- You can specify **description** *text* to add a description for a static route so that the administrator can easily query and maintain the static route. To view the description of static routes, run the **display this** command in the system view or run the **display current-configuration** command.
- If two static routes with the same destination IP address are configured, one of the routes is specified with a next hop IP address or outbound interface, and the other static route is configured with a next-hop VPN instance, without an outbound interface or next hop IP address, the latest configuration overwrites the previous one.

Example

Configure a static route for VPN instance named **vpn1**, and set the destination address of the static route to 10.1.1.0/24 and next-hop address to 192.168.1.2 (IP address of VPN instance **vpn2**).

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] route-distinguisher 100:200
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] ip vpn-instance vpn2
[HUAWEI-vpn-instance-vpn2] route-distinguisher 300:400
[HUAWEI-vpn-instance-vpn2-af-ipv4] quit
[HUAWEI-vpn-instance-vpn2] quit
[HUAWEI] ip route-static vpn-instance vpn1 10.1.1.0 24 vpn-instance vpn2 192.168.1.2
```

7.1.9 ipv6 route recursive-lookup inherit-label-route enable

Function

The **ipv6 route recursive-lookup inherit-label-route enable** command allows a device to recurse IPv6 routes to VPN remote cross routes.

The **undo ipv6 route recursive-lookup inherit-label-route enable** command disables a device from recursing IPv6 routes to VPN remote cross routes.

By default, IPv6 routes cannot recurse to VPN remote cross routes.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

ipv6 route recursive-lookup inherit-label-route enable

undo ipv6 route recursive-lookup inherit-label-route enable

Parameters

None

Views

System view

Default Level

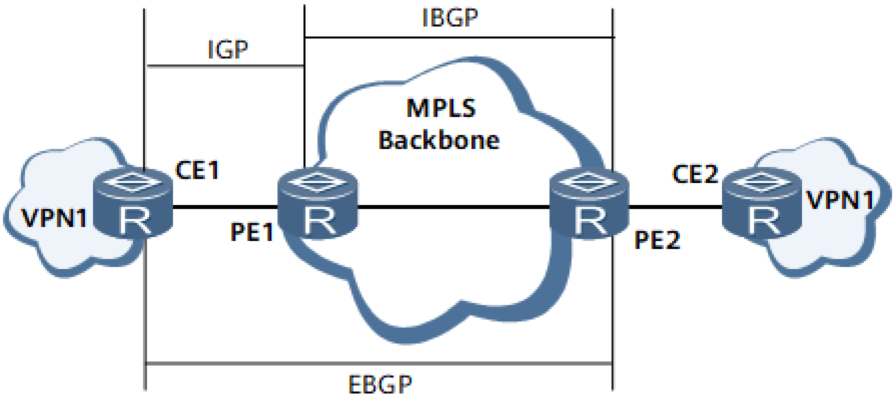
2: Configuration level

Usage Guidelines

Recursion is required if the next hop of a route is unreachable. To allow IPv6 routes to recurse to VPN remote cross routes, run the **ipv6 route recursive-lookup inherit-label-route enable** command. After the command is run, IPv6 routes inherit the labels and tokens of the VPN remote cross routes, ensuring correct traffic forwarding. This command mainly applies to BGP/MPLS IPv6 VPN scenarios.

In **Figure 7-2**, PE1 and PE2 are IBGP peers, and CE1 and PE1 are IGP neighbors. PE2 learns the IP address of CE1's loopback interface, and an EBGP peer relationship is established between CE1 and PE2 using loopback interface IP addresses. By default, the BGP routes that PE2 learns from CE1 through the EBGP peer connection cannot recurse to VPN remote cross routes. As a result, traffic fails to be forwarded. To address this problem, run the **ipv6 route recursive-lookup inherit-label-route enable** command to allow the BGP4+ routes to recurse to VPN remote cross routes. After the BGP4+ routes inherit the labels and tokens of the VPN remote cross routes, traffic can be correctly forwarded.

Figure 7-2 Basic BGP/MPLS IPv6 VPN networking



Example

Allow a device to recurse IPv6 routes to VPN remote cross routes.

```
<HUAWEI> system-view
[HUAWEI] ipv6 route recursive-lookup inherit-label-route enable
```

7.1.10 ipv6 route-static

Function

The **ipv6 route-static** command configures an IPv6 static route.

The **undo ipv6 route-static** command deletes configured IPv6 static routes.

By default, no IPv6 static route is configured.

Format

ipv6 route-static *dest-ipv6-address prefix-length* { *interface-type interface-number* [*nexthop-ipv6-address*] | *nexthop-ipv6-address* | **vpn-instance** *vpn-destination-name nexthop-ipv6-address* } [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** *cfg-name* | **nqa** *admin-name test-name* }] [**description** *text*]

ipv6 route-static *dest-ipv6-address prefix-length* **vpn-instance** *vpn-destination-name* [**preference** *preference* | **tag** *tag*] * [**description** *text*] (support only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

undo ipv6 route-static *dest-ipv6-address prefix-length* [*interface-type interface-number* [*nexthop-ipv6-address*] | *nexthop-ipv6-address*] [**preference** *preference* | **tag** *tag*] * [**track bfd-session**]

undo ipv6 route-static [**track bfd-session**] **all**

undo ipv6 route-static *dest-ipv6-address prefix-length* **vpn-instance** *vpn-destination-name* [**preference** *preference* | **tag** *tag*] * (support only by the

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
dest-ipv6-address	Specifies a destination IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the length of an IPv6 prefix.	The value is an integer that ranges from 0 to 128.
interface-type interface-number	Specifies the type and number of an outbound interface.	-
vpn-instance *vpn-destination-name*	Specifies the name of a VPN instance. If the VPN instance name is specified, a switch searches the routing table of the VPN instance for the outbound interface of a static route according to the configured next-hop address. If the *nexthop-ipv6-address* parameter is not specified, a device searches a specified VPN instance forwarding table to find a forwarding path.	The value is a string of 1 to 31 case-sensitive characters with spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
nexthop-ipv6-address	Specifies the next-hop IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
preference *preference*	Specifies the preference of an IPv6 static route.	The value is an integer that ranges from 1 to 255. The default value is 60.
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.

Parameter	Description	Value
track bfd-session *cfg-name*	Binds a static BFD session to a static route for fast fault detection.	*cfg-name* is a string of 1 to 15 characters without spaces. The string can contain spaces if it is enclosed with double quotation marks (").
track nqa *admin-name test-name*	Specifies the administrator name of an NQA test instance bound to a static route, and the name of the test instance.	The values of *admin-name* and *test-name* are both a string of 1 to 32 case-sensitive characters without spaces.
description *text*	Specifies the description of a static route.	The value is a string of 1 to 80 characters that can contain spaces.
all	Deletes all IPv6 static routes.	-

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **track bfd-session** *cfg-name* parameters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a simple network, you can configure static routes to ensure network connectivity. If a device cannot use dynamic routing protocols for network connectivity, static routes can also be configured on the device.

You can specify **description** *text* to add a description for a static route so that the administrator can easily query and maintain the static route. To view the description of static routes, run the **display this** command in the system view or run the **display current-configuration** command.

Precautions

When configuring unicast static routes, note the following:

- If no preference is set for a static route, the static route uses the default preference 60.

- If the destination address and mask of a static route are all 0s, the static route is a default route.
- For an IPv6 static route, the next hop can be set to either an IP address/ outbound interface or a VPN instance. Only the most recent configuration takes effect.

Example

Configure an IPv6 static route on a public network.

```
<HUAWEI> system-view
[HUAWEI] ipv6 route-static fc00:0:0:2001::1 128 fc00:0:0:2002::2
```

7.1.11 ipv6 route-static default-preference

Function

The **ipv6 route-static default-preference** command sets a default preference for an IPv6 static route.

The **undo ipv6 route-static default-preference** command restores the default preference of IPv6 static routes.

By default, the default preference of IPv6 static routes is 60.

Format

ipv6 route-static default-preference *preference*

undo ipv6 route-static default-preference

Parameters

Parameter	Description	Value
preference	Specifies the default preference of IPv6 static routes. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can change the activation status of routes by changing their preference. To change the default preference of a new IPv6 static route, run the **ipv6 route-static default-preference** command.

Configuration Impact

After the **ipv6 route-static default-preference** command is used, the default preference of all the new IPv6 static routes is changed.

The new default preference is valid only for new IPv6 static routes but not for existing IPv6 static routes.

Example

Set the default preference of IPv6 static routes to 70.

```
<HUAWEI> system-view
[HUAWEI] ipv6 route-static default-preference 70
```

7.1.12 ipv6 route-static track bfd-session admindown invalid

Function

The **ipv6 route-static track bfd-session admindown invalid** command disables a switch from selecting an IPv6 static route if the BFD session associated with the route is in the AdminDown state.

The **undo ipv6 route-static track bfd-session admindown invalid** command restores the default configuration.

By default, an IPv6 static route can participate in route selection even if the BFD session associated with it is in the AdminDown state.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ipv6 route-static track bfd-session session-name *bfd-name* **admindown invalid**

undo ipv6 route-static track bfd-session [**session-name** *bfd-name*] **admindown invalid**

Parameters

Parameter	Description	Value
session-name *bfd-name*	Specifies a BFD session bound to an IPv6 static route.	The value is a string of 1 to 15 case-insensitive characters without spaces. The string can contain spaces if it is enclosed with double quotation marks (").

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if a BFD session associated with an IPv6 static route is in the AdminDown state, the route can participate in route selection on Huawei switches, but is not allowed for route selection on some non-Huawei devices. As a result, Huawei switches cannot communicate with such non-Huawei devices.

To address this problem, run the **ipv6 route-static track bfd-session admindown invalid** command to configure the switch not to select the IPv6 static route if the BFD session associated with it is in the AdminDown state.

Prerequisites

The BFD session specified by *bfd-name* has been created.

Precautions

The **undo ipv6 route-static track bfd-session admindown invalid** command enables all IPv6 static routes to participate in route selection even if the BFD sessions associated with them are in the AdminDown state.

Example

Disable a switch from selecting an IPv6 static route if the BFD session associated with the route is in the AdminDown state.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd bfda bind peer-ipv6 2001:db8:1::1
[HUAWEI-bfd-session-bfda] discriminator local 20
[HUAWEI-bfd-session-bfda] discriminator remote 10
[HUAWEI-bfd-session-bfda] commit
[HUAWEI-bfd-session-bfda] quit
[HUAWEI] ipv6 route-static track bfd-session session-name bfda admindown invalid
```

7.1.13 ipv6 route-static vpn-instance

Function

The **ipv6 route-static vpn-instance** command configures an IPv6 static route for a VPN instance.

The **undo ipv6 route-static vpn-instance** command deletes IPv6 static routes from a VPN instance.

By default, no IPv6 static routes are configured for VPN instances.

Format

ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length* { [*interface-type interface-number* [*nexthop-ipv6-address*]] | *nexthop-ipv6-address* [**public**] | **vpn-instance** *vpn-destination-name nexthop-ipv6-address* } [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** *cfg-name* | **nqa** *admin-name test-name* }] [**description** *text*]

ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length* { **public** | **vpn-instance** *vpn-destination-name* } [**preference** *preference* | **tag** *tag*] * [**description** *text*] (support only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

undo ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length* [*interface-type interface-number*] [*nexthop-ipv6-address*] [**preference** *preference* | **tag** *tag*] *[**track bfd-session**]

undo ipv6 route-static vpn-instance *vpn-instance-name* [**track bfd-session**] **all**

undo ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length* { **public** | **vpn-instance** *vpn-destination-name* } [**preference** *preference* | **tag** *tag*] * (support only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. Each VPN instance has its own unicast routing table. The configured static routes are added to the routing table of the specified VPN instance.	The value must be an existing VPN instance name.
dest-ipv6-address	Specifies a destination IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.

Parameter	Description	Value
prefix-length	Specifies the length of an IPv6 prefix. The length equals the number of consecutive 1s in the mask.	The value is an integer that ranges from 0 to 128.
interface-type	Specifies the type of an interface.	-
interface-number	Specifies the number of an interface.	-
nexthop-ipv6-address	Specifies the next-hop IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
vpn-instance *vpn-destination-name*	Specifies the name of the destination VPN instance. If the name of the destination VPN instance is specified, a static route searches the destination VPN instance for an outbound interface according to the configured next-hop address. If the *nexthop-ipv6-address* parameter is not specified, a device searches the destination VPN instance forwarding table to find a forwarding path. If **vpn-instance** *vpn-destination-name* is specified, devices can communicate with each other between VPNs.	The value is a string of 1 to 31 case-sensitive characters with spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
public	Specifies a public network address as the next-hop address.	-
preference *preference*	Specifies the preference of a static route.	The value is an integer that ranges from 1 to 255.
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.

Parameter	Description	Value
track bfd-session *cfg-name*	Binds a static BFD session to a static route for fast fault detection.	*cfg-name* is a string of 1 to 15 characters without spaces. The string can contain spaces if it is enclosed with double quotation marks (").
track nqa *admin-name test-name*	Specifies the administrator name of an NQA test instance bound to a static route, and the name of the test instance.	The values of *admin-name* and *test-name* are both a string of 1 to 32 case-sensitive characters without spaces.
description *text*	Specifies the description of a static route.	The value is a string of 1 to 80 characters that can contain spaces.
all	Deletes all the IPv6 static routes configured for the specified VPN instance.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a simple IPv6 VPN network, you can run the **ipv6 route-static vpn-instance** command to configure static routes for this VPN.

- To configure VPN users to access a public network, you can perform network address translation (NAT) or run the **ipv6 route-static vpn-instance** command with the keyword **public** specified to configure a public network address as the VPN route's next-hop address.
- You can specify **description** *text* to add a description for a static route so that the administrator can easily query and maintain the static route. To view the description of static routes, run the **display this** command in the system view or run the **display current-configuration** command.

Precautions

If a network fault occurs or the network topology changes, static routes cannot automatically change. Therefore, configure static routes with caution.

If the destination address and the prefix length are set to all 0s, a default route is configured.

Example

Configure a default route with next-hop address FC00:0:0:2001::1.

```
<HUAWEI> system-view
[HUAWEI] ipv6 route-static vpn-instance vpn1 :: 0 fc00:0:0:2001::1
```

7.2 RIP Configuration Commands

7.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.2.2 bfd all-interfaces enable(RIP)

Function

The **bfd all-interfaces enable** command enables BFD on all the interfaces in a RIP process.

The **undo bfd all-interfaces enable** command disables BFD on all the interfaces in a RIP process.

By default, BFD is disabled in a RIP process.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

bfd all-interfaces enable

undo bfd all-interfaces enable

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

If BFD parameters are configured, but the **bfd all-interfaces enable** command is not configured, BFD sessions cannot be established.

NOTE

- The BFD priority on an interface is higher than the BFD priority on a RIP process.
- If the **rip bfd block** command is configured on an interface, the **bfd all-interfaces enable** command cannot be used to enable BFD on the interface.

Example

Enable BFD on all interfaces in a RIP process.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] rip
[HUAWEI-rip-1] bfd all-interfaces enable
```

7.2.3 bfd all-interfaces(RIP)

Function

The **bfd all-interfaces** command sets BFD session parameters.

The **undo bfd all-interfaces** command restores BFD session parameters to default values.

By default, the minimum intervals for receiving and sending BFD packets are 1000 ms and the detection time multiplier is 3.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

bfd all-interfaces { **min-rx-interval** *min-receive-value* | **min-tx-interval** *min-transmit-value* | **detect-multiplier** *detect-multiplier-value* } *

undo bfd all-interfaces { **min-rx-interval** [*min-receive-value*] | **min-tx-interval** [*min-transmit-value*] | **detect-multiplier** [*detect-multiplier-value*] } *

Parameters

Parameter	Description	Value
min-rx-interval *min-receive-value*	Specifies the minimum interval for receiving BFD packets from the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *min-transmit-value*	Specifies the minimum interval for sending BFD packets to the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *detect-multiplier-value*	Indicates the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The priority of BFD configured on an interface is higher than that configured for a RIP process. If BFD is enabled on an interface, BFD sessions are established using the BFD parameters set on the interface.

Actual interval at which BFD packets are transmitted on the local device = Max { transmit-value on the local device, receive-value on the peer}.

Actual interval at which BFD packets are received on the local device = Max { transmit-value on the peer, receive-value on the local device}.

Local BFD detection time = Actual interval at which BFD packets are received on the local device x detect-multiplier-value on the peer.

Prerequisites

BFD has been enabled on all the interfaces using the **bfd all-interfaces enable** command in the RIP view.

Example

Configure BFD for a RIP process and set the minimum interval for sending BFD packets to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] rip
[HUAWEI-rip-1] bfd all-interfaces enable
[HUAWEI-rip-1] bfd all-interfaces min-tx-interval 500
```

7.2.4 checkzero (RIP)

Function

The **checkzero** command enables the device to check the zero fields in RIP-1 packets.

The **undo checkzero** command disables the device from checking the zero fields in RIP-1 packets.

By default, the device checks the zero fields in RIP-1 packets.

Format

checkzero

undo checkzero

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a RIP-1 packet, the values of some fields must be zero. These fields are zero fields. After zero field check is enabled, the device checks the zero fields in the RIP-1 packets and discards the packets in which the zero field values are not 0.

The **checkzero** command is valid only for RIP-1 packets.

Run the **undo checkzero** command to reduce CPU usage if there is no zero field to check (all neighbors are trusted).

Configuration Impact

By default, devices reject all RIP-1 packets in which the zero fields are not 0.

RIP-1 implementations vary with device manufacturers. If the third-party peer device allows zero fields in RIP-1 packets to carry non-zero values, run the **undo checkzero** command on the local device. The **undo checkzero** command causes potential security risks to network, so it is not recommended.

Example

Enable the device to check zero fields in RIP-1 packets.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] checkzero
```

7.2.5 default-cost (RIP)

Function

The **default-cost** command changes the default metric of imported routes.

The **undo default-cost** command restores the default metric of imported routes.

By default, the metric of imported routes is 0.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Specifies the default metric of imported routes.	The value is an integer that ranges from 0 to 15. The default value is 0.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

You can run one of the following commands to set the metric of imported routes. The following commands are listed in descending order of priorities.

- Run the **apply cost** command to set the metric of imported routes.
- Run the **import-route** (RIP) command to set the metric of imported routes.
- Run the **default-cost** (RIP) command to set the default metric of imported routes.

Example

Set the default metric for imported routes to 2.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] default-cost 2
```

7.2.6 default-route originate

Function

The **default-route originate** command configures RIP to originate a default route or advertise the default route in the routing table to neighbors.

The **undo default-route originate** command restores the default configuration.

By default, the device does not advertise the default route to neighbors.

Format

default-route originate [**cost** *cost* | { **match default** | **route-policy** *route-policy-name* } [**avoid-learning**]]*

undo default-route originate

Parameters

Parameter	Description	Value
cost *cost*	Specifies the metric of the default route.	The value is an integer that ranges from 0 to 15. The default value is 0.
match default	Indicates that the device advertises the default route imported from another routing protocol or RIP process in the routing table to neighbors.	-
avoid-learning	Disables RIP from importing default routes. If a default route in active state already exists in the routing table, the default route is set to inactive after this parameter is used.	-
route-policy *route-policy-name*	Specifies the name of the routing policy. RIP will originate the default route only if route permitted by the route policy is present as active in the routing table.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a routing table, the destination address and mask of a default route are all 0s. If the destination address of a packet does not match any entry in the routing table of the switch, the switch sends the packet along the default route.

If no default route exists and the destination address of the packet does not match any entry in the routing table, the switch discards the packet and sends an Internet Control Message Protocol (ICMP) packet, informing the originating host that the destination address or network is unreachable.

Default routes are originated unconditionally, or based on the configured routing policy or **match default**. When default routes are originated based on the configuration, default routes learned from RIP neighbors will be deleted.

- When the **default-route originate** command is configured without any parameter, the default route is originated unconditionally regardless of whether the default route exists in the IP routing table.
- When the **default-route originate** command is configured with **route-policy**, RIP will originate the default route only if the route that matches **route-policy** is active in the IP routing table.
- When the **default-route originate** command is configured with **match default**, RIP will originate the default route only if a default route learned by another routing protocol or RIP process is present in the IP routing table.
- When the **default-route originate** command is configured with **avoid-learning**, RIP will not learn the default route advertised by RIP peers.

Prerequisites

A RIP process has been created, and the RIP view is displayed using the **rip** command.

Example

Set the metric for the default route to 2.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] default-route originate cost 2
```

7.2.7 description (RIP)

Function

The **description** command configures a description for a RIP process.

The **undo description** command deletes the description of a RIP process.

By default, there is no description for a RIP process.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies a description for a RIP process.	It is a string of 1 to 80 case-sensitive characters. Spaces are supported.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring descriptions for RIP processes, you can easily identify RIP processes.

Configuration Impact

If the **description** command is run multiple times, only the latest configuration takes effect.

Example

Configure a description for RIP process 100.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] description this process configure the poison reverse process
```

7.2.8 display default-parameter rip

Function

The **display default-parameter rip** command displays the default RIP configuration.

Format

display default-parameter rip

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the default RIP configuration is modified, running the **display default-parameter rip** command still displays the default configuration during RIP initialization.

Example

Display the default RIP configuration.

```
<HUAWEI> display default-parameter rip
```

```
-------------------------------------------
 Protocol Level Default Configurations
-------------------------------------------
       RIP version   : 1
       Preference    : 100
       Checkzero     : Enabled
       Default-cost  : 0
       Auto Summary  : Enabled
       Host-route    : Enabled
       Maximum Balanced Paths : 16
       Update time   : 30 sec              Age time : 180 sec
       Garbage-collect time : 120 sec
       Default-route     : Disabled
       Verify-source     : Enabled
       Graceful restart  : Disabled
-------------------------------------------
 Interface Level Default Configurations
-------------------------------------------
  Metricin                 : 0
  Metricout                : 1
  Input Packet Processing : Enabled
  Output Packet Processing: Enabled
  Poison Reverse          : Disabled
  Replay Protect          : Disabled
  Split Horizon
   For Broadcast and P2P Interfaces :  Enabled
   For NBMA Interfaces              :  Disabled
  Packet Transmit Interval          :  200 msecs
  Packet Transmit Number            :  50
  RIP Protocol Version              :  RIPv1 Compatible (Non-Standard)
```

Table 7-1 Description of the display default-parameter rip command output

Item	Description
Protocol Level Default Configurations	Default RIP protocol-level configuration.
RIP version	Default global RIP version.
Preference	Default RIP preference.
Checkzero	Whether zero fields in RIP-1 packets are checked by default.
Default-cost	Default metric of routes imported from other routing protocols.
Auto Summary	Whether RIP summarization is enabled by default.
Host-route	Whether host routes are added to routing tables by default.
Maximum Balanced Paths	Default maximum number of equal-cost routes for load balancing.
Update time	Default interval for sending Update packets.
Age time	Default aging time of RIP routes.

Item	Description
Garbage-collect time	Default Garbage-collect time of RIP routes.
Default-route	Whether the default route is used if no entries in the routing table match packets.
Verify-source	Whether source address check is enabled by default.
Graceful restart	Whether RIP GR is enabled by default.
Interface Level Default Configurations	Default RIP configuration on the interface.
Metricin	Default metric added to routes when RIP packets are received.
Metricout	Default metric added to routes when RIP packets are sent.
Input Packet Processing	Whether an interface is allowed to receive RIP packets by default.
Output Packet Processing	Whether an interface is allowed to send RIP packets by default.
Poison Reverse	Whether poison reverse is enabled by default.
Replay Protect	Whether replay-protect is enabled by default.
Split Horizon	Whether split horizon is enabled for the following interfaces: ● Broadcast and P2P interfaces ● NBMA interfaces
Packet Transmit Interval	Default interval for forwarding packets, in milliseconds.
Packet Transmit Number	Default number of forwarded packets.
RIP Protocol Version	Default RIP version on the interface.

7.2.9 display rip

Function

The **display rip** command displays the status and configuration of a RIP process.

Format

display rip [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Displays the status and configuration of a specified RIP process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the status and configuration of a RIP process with the specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rip** command to check the status and configuration of a RIP process.

Example

Display the status and configuration of a RIP process. The command output shows that two VPN instances are running. One is a public instance and another one is a VPN instance named **VPN-Instance-1**.

```
<HUAWEI> display rip
Public VPN-instance
    RIP process : 1
       RIP version   : 1
       Preference    : 100
       Checkzero     : Enabled
       Default-cost  : 0
       Summary       : Enabled
       Host-route    : Enabled
       Maximum number of balanced paths : 8
       Update time   : 30 sec              Age time : 180 sec
       Garbage-collect time : 120 sec
       Graceful restart  : Disabled
       BFD               : Disabled
       Silent-interfaces : None
       Default-route     : Disabled
       Verify-source     : Enabled
       Networks          : None
       Configured peers             : None
       Number of routes in database : 0
       Number of interfaces enabled : 0
       Triggered updates sent       : 0
```

```
      Number of route changes      : 0
      Number of replies to queries : 0
      Number of routes in ADV DB   : 0

Private VPN-instance name : VPN-Instance-1
    RIP process : 100
      RIP version   : 1
      Preference    : 100
      Checkzero     : Enabled
      Default-cost  : 0
      Summary       : Enabled
      Host-route    : Enabled
      Maximum number of balanced paths : 8
      Update time   : 30 sec              Age time : 180 sec
      Garbage-collect time : 120 sec
      Graceful restart  : Disabled
      BFD               : Disabled
      Silent-interfaces : None
      Default-route     : Disabled
      Verify-source     : Enabled
      Networks          : None
      Configured peers             : None
      Number of routes in database : 0
      Number of interfaces enabled : 0
      Triggered updates sent       : 0
      Number of route changes      : 0
      Number of replies to queries : 0
      Number of routes in ADV DB   : 0

  Total count for 2 process :
      Number of routes in database : 0
      Number of interfaces enabled : 0
      Number of routes sendable in a periodic update : 0
      Number of routes sent in last periodic update : 0
```

Table 7-2 Description of the display rip command output

Item	Description
RIP process	Running RIP process. To create a RIP process, run the **rip** command.
RIP version	Global RIP version. To set the RIP version, run the **version** command.
Preference	RIP preference. To set the RIP preference, run the **preference** command.
Checkzero	Whether zero fields in RIP-1 packets are checked. To check zero fields in RIP-1 packets, run the **checkzero** command.
Default-cost	Default metric for the routes imported from other routing protocols. To set the default metric, run the **default-cost** command.
Summary	Whether RIP summarization is enabled. To enable RIP summarization, run the **summary** command.
Host-route	Whether host routes are added to routing tables. To add host routes to routing tables, run the **host-route** command.

Item	Description
Maximum number of balanced paths	Maximum number of equal-cost routes for load balancing. To set the maximum number of equal-cost routes, run the **maximum load-balancing** command.
Update time	Interval for sending RIP Update packets. To set the interval for sending RIP Update packets, run the **timers rip** command.
Age time	Aging time of RIP routes. To set the RIP aging time, run the **timers rip** command.
Garbage-collect time	Garbage-collect time of RIP routes. To set the Garbage-collect time, run the **timers rip** command.
Graceful restart	Whether graceful restart is enabled for RIP routes.
BFD	Whether RIP is associated with BFD.
Silent-interfaces	Suppressed RIP interface, which only receives but does not send RIP packets. To specify the suppressed interface, run the **silent-interface** command.
Default-route	Whether RIP originates default routes. To configure RIP to originate default routes, run the **default-route originate** command.
Verify-source	Whether the source addresses of received RIP Update packets are checked. To check the source addresses of received RIP Update packets, run the **verify-source** command.
Networks	Network segment running RIP. To enable RIP for a network segment, run the **network** command.
Configured peers	RIP neighbors. To configure a RIP neighbor, run the **peer** command.
Number of routes in database	Number of routes in the RIP database.
Number of interfaces enabled	Number of interfaces running RIP.
Triggered updates sent	Number of RIP packets triggering update.
Number of route changes	Number of changed routes in the RIP database.
Number of replies to queries	Number of response packets to RIP requests.
Number of routes in ADV DB	Number of routes in each Update packet.

Item	Description
Number of routes sendable in a periodic update	Number of routes sent in each Update interval.
Number of routes sent in last periodic update	Number of routes sent in last Update interval.

7.2.10 display rip bfd session

Function

The **display rip bfd session** command displays information about BFD sessions.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

display rip *process-id* **bfd session** { **interface** *interface-type interface-number* | *neighbor-id* | **all** }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
interface *interface-type interface-number*	Specifies the type and number of the interface on which the BFD session is configured.	-
neighbor-id	Specifies the RIP neighbor ID on which the BFD session is configured.	The value is in dotted decimal notation.

Parameter	Description	Value
all	Displays information about BFD sessions established on all BFD-enabled interfaces in the RIP process.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display rip bfd session** command can be used to view the following information in a RIP process:

- BFD sessions of a specified process
- BFD sessions on a specified interface
- BFD sessions on a specified neighbor

Example

Display information about BFD sessions in all RIP processes with IDs of 1.

```
<HUAWEI> display rip 1 bfd session all
 LocalIp      :10.1.0.1         RemoteIp :10.1.0.2        BFDState  :Up
 TX           :1000             RX       :1000            Multiplier:3
 BFD Local Dis:8192             Interface:Vlanif10
 Diagnostic Info: No diagnostic information
 LocalIp      :10.2.0.1         RemoteIp :10.2.0.2        BFDState  :Up
 TX           :1000             RX       :1000            Multiplier:3
 BFD Local Dis:8193             Interface:Vlanif20
 Diagnostic Info: No diagnostic information
```

Table 7-3 Description of the display rip bfd session all command output

Item	Description
LocalIp	Local IP address
RemoteIp	Remote IP address
BFDState	A BFD session status can be either Up or Down.
TX	Minimum interval at which BFD packets are sent
RX	Minimum interval at which BFD packets are received
Multiplier	Remote detection multiplier

Item	Description
BFD Local Dis	Local discriminator dynamically assigned by BFD
Interface	Local interfaces on which BFD sessions are configured
Diagnostic Info	Diagnostic information

7.2.11 display rip database

Function

The **display rip database** command displays all the active routes in the RIP database. These routes are sent in RIP Update packets.

Format

display rip *process-id* **database** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about the routes in the RIP database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rip database** command to check all the active routes in the RIP database. These routes are sent in RIP Update packets.

Example

Display the RIP database.

```
<HUAWEI> display rip 100 database
---------------------------------------------------
Advertisement State : [A] - Advertised
                      [I] - Not Advertised/Withdraw
---------------------------------------------------
```

```
10.0.0.0/8, cost 0, ClassfulSumm
   10.1.1.0/24, cost 0, [A], Imported
   10.10.10.0/24, cost 0, [A], Rip-interface
   10.137.220.0/23, cost 1, [A], nexthop 10.10.10.2
```

Table 7-4 Description of the display rip database command output

Item	Description
Advertisement State	Route status. ● [A]: Advertised ● [I]: Not Advertised/Withdraw
ClassfulSumm	Classful route summarization.
Imported	Routes imported from other routing protocols.
Rip-interface	Routes learned on the RIP interface.
nexthop	Next-hop address.

7.2.12 display rip graceful-restart

Function

The **display rip graceful-restart** command displays the GR status of RIP.

Format

display rip *process-id* **graceful-restart** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about GR status.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After receiving the GR abort notification from the helper or detecting a network topology change, the restarter stops the GR process.

Example

Display the GR status in RIP process 1.

```
<HUAWEI> display rip 1 graceful-restart
Restart mode     : Restarting
Restart status   : In Progress - Waiting for updates
Last complete reason : None
Update progress summary:
------------------------
Restart capable peers  : 0
 Completed: 0    Inprogress: 0
Restart incapable peers: 1
 Completed: 0    Inprogress: 1
Update period finishes in 293 seconds
```

Table 7-5 Description of the display rip graceful-restart command output

Item	Description
Restart mode	Role of a switch: ● Restarting: indicates the restarter. ● Helper: indicates the helper. ● None: indicates a common switch that does not participate in GR.
Restart status	GR status: ● In Progress - waiting for updates: indicates that the switch is waiting for Update packets. ● In Progress - calculating active routes: indicates that the switch is calculating RIP routes. ● Aborted - calculating active routes: indicates that the route exits from GR abnormally. ● GR completed: indicates that GR is complete.
Last complete reason	Reason that the switch exits from GR for the last time: ● Unknown: indicates an unknown reason. ● Abort: indicates that the switch exits from GR abnormally. ● Period Expired: indicates that GR period expires. ● Successful: indicates that the switch exits from GR normally. ● None: indicates that the switch does not perform GR.
Update progress summary	Title bar indicating the updated RIP progress summary

Item	Description
Restart capable peers	Number of neighbors that help the local switch to perform GR
Completed	Number of neighbors that have sent all Update packets
Inprogress	Number of neighbors that have not sent all Update packets
Restart incapable peers	Number of neighbors that cannot help the local switch to perform GR
Update period finishes in 293 seconds	Time to finish GR: 293 seconds

7.2.13 display rip interface

Function

The **display rip interface** command displays information about RIP interfaces.

Format

display rip *process-id* **interface** [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the type and the number of an interface.	-
verbose	Displays detailed information about a RIP interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display rip interface** command output displays the configuration and operating status of RIP, which facilitate fault location and configuration verification.

Example

Display information about RIP on VLANIF100.

```
<HUAWEI> display rip 1 interface vlanif 100
 -------------------------------------------------------------------------
 Interface                IP Address      State    Protocol           MTU
 -------------------------------------------------------------------------
 Vlanif 100                10.1.1.2        UP       RIPv1 Compatible    500
```

Table 7-6 Description of the display rip interface command output

Item	Description
Interface	RIP-enabled interfaces
IP Address	IP address of the interface
State	Status of the interface: ● UP ● DOWN
Protocol	Version of RIP running on the interface: ● RIPv1 Compatible ● RIPv2 Multicast ● RIPv2 Broadcast To set the version of RIP, run the **rip version** command.
MTU	MTU value of the link

Display detailed information about RIP on VLANIF100.

```
<HUAWEI> display rip 1 interface vlanif 100 verbose
 Vlanif100 (10.1.1.1)
  State    :   UP            MTU : 500
  Metricin : 0
  Metricout : 1
  Input    : Enabled         Output : Enabled
  Protocol : RIPv1 Compatible (Non-Standard)
  Send version     : RIPv1 Packets
  Receive version  : RIPv1 Packets, RIPv2 Multicast and Broadcast Packets
  Poison-reverse                : Disabled
  Split-Horizon                 : Enabled
  Authentication type           : None
  Replay Protection   : Disabled
  BFD                 : Enabled (Static)
  Transmit-Interval   : 1000 ms
  Receive-Interval    : 1000 ms
  Detect-Multiplier   : 3
  Summary Address (es):  10.1.0.0/16
```

Table 7-7 Description of the display rip interface verbose command output

Item	Description
State	Status of the interface: - UP - DOWN
MTU	Maximum Transmission Unit
Metricin	Metric that is added to the route when the interface receives a RIP packet. To set the metric, run the **rip metricin** command.
Metricout	Metric that is added to the route when the interface sends a RIP packet. To set the metric, run the **rip metricout** command.
Input	Whether receiving packets is enabled. To enable the specified interface to receive RIP packets, run the **rip input** command.
Output	Whether sending packets is enabled. To enable the specified interface to send RIP packets, run the **rip output** command.
Protocol	Protocol running on the interface: - RIPv1 Compatible (Non-Standard) - RIPv1 - RIPv2 Multicast - RIPv2 Broadcast To set the version of RIP, run the **rip version** command.
Send version	Type of packets sent on the interface: - RIPv1 packets - RIPv2 Multicast Packets - RIPv2 Broadcast Packets
Receive version	Type of packets received on the interface: - RIPv1 packets - RIPv2 Multicast and Broadcast Packets
Poison-reverse	Whether poison reverse is enabled on the interface. To enable poison reverse, run the **rip poison-reverse** command.

Item	Description
Split-Horizon	Whether split horizon is enabled on the interface. To enable split horizon, run the **rip split-horizon** command.
Authentication type	Authentication type configured on the interface. To set the authentication mode and authentication parameters, run the **rip authentication-mode** command.
Replay Protection	Whether replay-protect is enabled on the interface. To enable the replay-protect function, run the **rip replay-protect** command.
BFD	Whether BFD is enabled on the interface: ● Enabled (Dynamic): indicates dynamic BFD is enabled on the interface. To enable BFD on the specified interface, run the **rip bfd enable** command. ● Blocked: indicates BFD is blocked on the interface. To block BFD on a specified interface, run the **rip bfd block** command.
Transmit-Interval	Interval for sending BFD packets to the peer on the interface. To set BFD session parameters on the specified interface, run the **rip bfd** command.
Receive-Interval	Interval for receiving BFD packets from the peer on the interface. To set BFD session parameters on the specified interface, run the **rip bfd** command.
Detect-Multiplier	BFD detect multiplier value configured on the interface. To set BFD session parameters on the specified interface, run the **rip bfd** command.
Summary Address (es)	Summary address

7.2.14 display rip neighbor

Function

The **display rip neighbor** command displays information about RIP neighbors.

Format

display rip *process-id* **neighbor** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about a RIP neighbor.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rip neighbor** command to check information about RIP neighbors.

Example

Display information about the neighbor in RIP process 1.

```
<HUAWEI> display rip 1 neighbor
---------------------------------------------------------------
 IP Address      Interface        Type   Last-Heard-Time
---------------------------------------------------------------
 10.1.1.1        Vlanif100        RIP     0:0:7
 Number of RIP routes:1
```

Table 7-8 Description of the display rip neighbor command output

Item	Description
IP Address	IP address of the neighboring interface
Interface	Interface type
Type	Protocol used to establish adjacencies with neighbors
Last-Heard-Time	Time since the last time packets are received from neighbors
Number of RIP routes	Number of RIP routes

Display detailed information about the neighbor in RIP process 1.

```
<HUAWEI> display rip 1 neighbor verbose
---------------------------------------------------------------
 IP Address      Interface        Type   Last-Heard-Time
---------------------------------------------------------------
 10.1.1.1        Vlanif100    RIP    0:0:17
   Number of Active routes       : 1
   Number of routes in garbage   : 0
   Last Received Sequence Number : 0x0
```

Table 7-9 Description of the display rip neighbor verbose command output

Item	Description
Number of Active routes	Number of routes in the active state
Number of routes in garbage	Number of routes in the garbage state
Last Received Sequence Number	Sequence number of last received packet from neighbor

7.2.15 display rip neighbor last-nbr-down

Function

The **display rip neighbor last-nbr-down** command displays information about the last neighbor that goes Down in a RIP process.

Format

display rip *process-id* **neighbor last-nbr-down**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display rip neighbor last-nbr-down** command can be used to view information about the last 10 RIP neighbor that goes down and the reason why the neighbor goes down.

Example

View information about the last neighbor that goes Down in a RIP process.

```
<HUAWEI> display rip 1 neighbor last-nbr-down
 Neighbor IP Address            : 10.2.2.2
 Interface                      : Vlanif10
 Reason for Neighbor down       : Interface Down
 Time at which neighbor went down : 2011-06-02 11:53:50
```

Table 7-10 Description of the display rip neighbor last-nbr-down command output

Item	Description
Neighbor IP Address	IP address of a neighbor
Interface	Interface connected to a neighbor
Reason for Neighbor down	Reason that a neighbor goes Down: ● Unknown ● Interface Down ● Configuration Change ● Time Out (Normal) ● Time Out (Message Processing Failed) ● BFD Session Down ● Invalid Packet Received ● Received Worst Metric Routes ● Received NQA Down Notification
Time at which neighbor went down	Time when a neighbor goes Down

7.2.16 display rip route

Function

The **display rip route** command displays all the RIP routes that are learned from other switches and view the values of different timers related to each route.

Format

display rip *process-id* **route**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a RIP process is enabled on all devices that need to run RIP and the **network** command is run to enable RIP on the related network segment, the **display rip route** command can be used to view RIP routing information.

Example

Display all the RIP routes and the values of different timers related to each route.

```
<HUAWEI> display rip 1 route
 Route Flags: R - RIP
              A - Aging, G - Garbage-collect
 -------------------------------------------------------------------------
 Peer 192.168.5.1  on Vlanif100
      Destination/Mask        Nexthop     Cost   Tag     Flags   Sec
        172.16.0.0/16       192.168.5.1    1     0       RA      15
      192.168.14.0/24        192.168.5.1    2     0       RA      15
```

Table 7-11 Description of the display rip route command output

Item	Description
Route Flags	Route flags. First character indicating that the route is a RIP or TRIP route, Second character indicating the status of the route: ● RA: indicates that a RIP route is active. ● RG: indicates that a RIP route is inactive and that the Garbage-Collect timer has been started.
Destination/ Mask	Destination IP Address and its mask value
Nexthop	Next hop of the route
Cost	Metric value of the route

Item	Description
Tag	Tag that is used to differentiate internal RIP routes from external routes ● 0: indicates that a RIP route is internal route. ● 1: indicates that a RIP route is external route.
Sec	Time during which a route remains in a specific state

7.2.17 display rip statistics interface

Function

The **display rip statistics interface** command displays statistics on a RIP interface, including the number of packets sent and received on the interface.

Format

display rip *process-id* **statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ip-address*] }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
all	Displays the statistics of all interfaces.	-
interface-type interface-number	Specifies the type and number of an interface.	-
verbose	Displays detail information about interface statistics.	-
neighbor *neighbor-ip-address*	Specifies the IP address of a neighbor.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rip statistics interface** command to check packet statistics on a RIP interface, including the number of packets sent and received on the interface.

Example

Display statistics on VLANIF100 in RIP process 1.

```
<HUAWEI> display rip 1 statistics interface vlanif 100
Vlanif100(10.0.0.11)
Statistical information         Last min     Last 5 min    Total
----------------------------------------------------------------
Periodic updates sent           5            23            259
Triggered updates sent          5            30            408
Response packets sent           10           34            434
Response packets received       15           38            467
Response packets ignored        0            0             0
Request packets sent            1            3             8
Request packets received        4            20            40
Request packets ignored         0            0             0
Bad packets received            0            0             0
Routes received                 0            0             0
Routes sent                     0            0             0
Bad routes received             0            0             0
Packet authentication failed    0            0             0
Packet send failed              0            0             0
```

Table 7-12 Description of the display rip statistics interface command output

Item	Description
Statistical information	Packet type
Last min	Statistics within the last 1 minute
Last 5 min	Statistics within the last 5 minutes
Total	Total number of packets
Periodic updates sent	Number of periodic Update packets that are sent on the interface
Triggered updates sent	Number of triggered Update packets that are sent on the interface
Response packets sent	Number of RIP Response packets that are sent on the interface
Response packets received	Number of RIP Response packets that are received on the interface
Response packets ignored	Number of RIP Response packets that are ignored on the interface
Request packets sent	Number of RIP Request packets that are sent on the interface
Request packets received	Number of RIP Request packets that are received on the interface

Item	Description
Request packets ignored	Number of RIP Request packets that are ignored on the interface
Bad packets received	Number of received packets that cannot be parsed correctly
Routes received	Number of received routes
Routes sent	Number of sent routes
Bad routes received	Number of received routes that cannot be parsed correctly
Packet authentication failed	Number of packets that fail to pass authentication
Packet send failed	Number of RIP packets that fail to be sent

7.2.18 filter-policy export (RIP)

Function

The **filter-policy export** command configures egress filtering policy for RIP routes.

The **undo filter-policy export** command deletes the filtering policy.

By default, no filtering policy is configured.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*] **export** [*protocol* [*process-id*] | *interface-type interface-number*]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL that is used to filter the destination addresses of routes.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the ACL filtering route destination addresses.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that is used to filter the destination addresses of routes.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol process-id	Specifies the name of the routing protocol that exports the routes and the protocol process ID. The imported route type can be **static**, **direct**, **rip**, **ospf**, **bgp**, **unr** and **isis**. The process ID must be specified when routes are imported from **isis**, **rip** or **ospf**.	The value is an integer that ranges from 1 to 65535.
interface-type interface-number	Specifies type and number of the interface based on which routes are filtered.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Only filtered routes can be added to routing tables and advertised in Update packets.

When you remove an interface-based filtering policy, you must specify *interface-type interface-number* in the **undo filter-policy export** command. The policy on only one interface can be deleted each time.

This command runs in the RIP view. If the filtering policy is based on interfaces or protocols, each interface or protocol can be configured with only one filtering policy. If the interface or protocol is not specified, a global filtering rule is configured. Only one global filtering rule can be configured each time. If you run the command again when a global rule exists, the new policy overwrites the old one.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Filter the imported static routes based on the IP prefix list named abc. Then, only the routes that match the filtering policy are added into the RIP routing table and then sent through RIP Update packets.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] filter-policy ip-prefix abc export static
```

Filter the routes imported from IS-IS process 1 based on ACL 2002. Only the routes that match the filtering policy are added into the RIP routing table and then sent through RIP Update packets.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] filter-policy 2002 export isis 1
```

7.2.19 filter-policy import (RIP)

Function

The **filter-policy import** command filters the received RIP routes.

The **undo filter-policy import** command cancels route filtering.

By default, no filtering policy is configured.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*]] **import** [*interface-type interface-number*]

undo filter-policy [**gateway** *ip-prefix-name*] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL that is used to filter the destination addresses of routes.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the ACL filtering route destination addresses.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
interface-type interface-number	Indicates the type and the number of the interface based on which routes are filtered.	-
ip-prefix	Filters routes by using the IP prefix list.	-
ip-prefix-name	Specifies the address prefix list used to filter route destination addresses.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
gateway	Filters routes based on the gateway.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

The **filter-policy import** command filters received RIP routes, including:

- Filtering a specified route in the packet
- Not monitoring the Update packets from the device

To cancel route filtering, run the **undo filter-policy import** command. When you remove an interface-based filtering policy, you must specify *interface-type interface-number*. The policy on only one interface can be deleted each time.

This command runs in the RIP view. If the filtering policy is based on interfaces, each interface can be configured with only one filtering policy. If the interface is not specified, a global filtering policy is configured. Only one global filtering policy can be configured. If you run the command again when a global policy exists, the new policy overwrites the old one.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.

Example

Filter the RIP Update packets that are received from all the interfaces according to the IP prefix list named **abc**.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] filter-policy ip-prefix abc import
```

7.2.20 graceful-restart (RIP)

Function

The **graceful-restart** command enables RIP GR on the restarter.

The **undo graceful-restart** command disables RIP GR on the restarter.

By default, RIP GR is disabled.

Format

graceful-restart [**period** *period* | **wait-time** *time* | **planned-only** *time*] *

undo graceful-restart

Parameters

Parameter	Description	Value
period *period*	Specifies the period of GR.	It is an integer ranging from 30 to 3600, in seconds. The default value is 180 seconds.
wait-time *time*	Specifies the period of GR performed between the restarter and the neighbors that do not support GR. The value of **wait-time** *time* cannot be greater than the value of **period** *period*.	It is an integer ranging from 1 to 3600, in seconds. The default value is 45 seconds.
planned-only *time*	Specifies the period of GR performed between the restarter and the neighbors that support GR.	It is an integer ranging from 5 to 3600, in seconds. The default value is 60 seconds.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Planned GR indicates the master/slave switchover triggered through the command. Unplanned GR indicates the master/slave switchover triggered because of a fault.

When most switches on a network do not support RIP GR, you are advised to set **wait-time** *time* to a larger value. This ensures that the restarter has enough time to learn correct routes.

If the restart switch completes GR before the period specified by **period** *period* expires, the restart switch automatically exits from GR. If the restart switch does not complete GR after the period specified by **period** *period* expires, the restart switch is forced to exit from GR.

If the period of GR performed between the restarter and the neighbors that do not support GR depends on **wait-time**, the restarter does not exit from GR regardless of whether GR is finished within **wait-time**. After **wait-time** expires, however, the restarter is forced to exit from GR.

Example

Enable RIP GR and set the GR period to 200s.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] graceful-restart period 200
```

7.2.21 host-route

Function

The **host-route** command adds host routes with 32 bits into the routing table.

The **undo host-route** command disables host routes with 32 bits from being added into the routing table.

By default, host routes can be added into the routing table.

Format

host-route

undo host-route

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

This command applies to RIP-1. In RIP-2, host routes are added to the routing table, regardless of whether the command is run.

Example

Add host routes into the routing table.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] host-route
```

7.2.22 import-route (RIP)

Function

The **import-route** command configures RIP to import routes from other routing protocols.

The **undo import-route** command disables RIP from importing routes from other routing protocols.

By default, RIP does not import routes from other routing protocols.

Format

import-route bgp [**permit-ibgp**] [**cost** { *cost* | **transparent** } | **route-policy** *route-policy-name*] *

import-route { { **static** | **direct** | **unr** } | { { **rip** | **ospf** | **isis** } [*process-id*] } } [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route { { **static** | **direct** | **bgp** | **unr** } | { { **rip** | **ospf** | **isis** } [*process-id*] } }

Parameters

Parameter	Description	Value
bgp | **static** | **direct** | **rip** | **ospf** | **isis** | **unr**	Specifies the routing protocol from which RIP imports routes.	-
permit-ibgp	Imports routes from IBGP to RIP.	-
process-id	Specifies a process ID. The process ID can be specified when you import routes from RIP, OSPF, or IS-IS to RIP.	The value is an integer that ranges from 1 to 65535.
cost *cost*	Specifies the metric for imported routes.	The value is an integer that ranges from 0 to 15.

Parameter	Description	Value
cost transparent	This parameter is valid only when RIP imports routes from BGP. The metric of the imported routes is the MED of the BGP routes.	-
route-policy *route-policy-name*	Specifies the routing policy for importing routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

After you run the **import-route** command to set a routing policy, RIP can import only the specified routes and sets the route attributes.

To import routes from RIP, or IS-IS, you can specify the process ID. If the process ID is specified, RIP imports routes only from the specified process. If no process ID is specified, RIP imports routes from all processes. When a static or direct route is imported, the process ID cannot be specified.

You can run one of the following commands to set the metric of the imported routes. The following commands are listed in the descending order of priorities.

- Run the **apply cost** command to set route metric.
- Run the **import-route** (RIP) command to set the metric for imported routes.
- Run the **default-cost (RIP)** command to set the default metric for routes.

NOTE

- RIP defines a 16-bit tag, while other routing protocols define 32-bit tags. If the routes of other protocols are imported to RIP and the tag is used in the routing policy, the tag value cannot exceed 65535. If the tag value exceeds 65535, the routing policy becomes invalid or the matching result is incorrect.
- After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the RIP routing table. Therefore, use this command with caution.
- The **permit-ibgp** parameter cannot be set for the RIP VPN instance.
- Importing IBGP routes to RIP may cause routing loops.

Example

Import IBGP routes, which are filtered by policy abc, to RIP process 1 and set the metric to 5.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] import-route bgp permit-ibgp cost 5 route-policy abc
```

7.2.23 maximum load-balancing (RIP)

Function

The **maximum load-balancing** command configures the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the maximum number of equal-cost routes on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S6720S-S, and S5736-S is 8, and the maximum number of equal-cost routes on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S is 16.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

maximum load-balancing *number*

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the number of equal-cost routes.	The value is an integer that ranges from 1 to 8 on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S and S6720S-S. The value ranges from 1 to 16 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

If a network has multiple redundant links, the maximum number of equal-cost routes can be configured to implement load balancing. With load balancing, network resources are fully utilized, situations where some links are overloaded while others are idle can be avoided, and delay in packet transmissions is shortened.

Example

Set the maximum number of equal-cost routes to 4.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] maximum load-balancing 4
```

7.2.24 network (RIP)

Function

The **network** command enables RIP for the interface on the specified network segment.

The **undo network** command disables RIP for the interface on the specified network segment.

By default, RIP is disabled for the interface on the specified network segment.

Format

network *network-address*

undo network *network-address*

Parameters

Parameter	Description	Value
network-address	Specifies the network address on which RIP is enabled. It must be the address of the natural network segment.	The value is in dotted decimal notation.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

An interface can be associated with only one RIP process.

Example

Enable RIP routes for the interface on the specified network segment.

```
<HUAWEI> system-view
[HUAWEI] rip
[HUAWEI-rip-1] network 10.0.0.0
```

7.2.25 peer (RIP)

Function

The **peer** command specifies the IP addresses of the RIP neighbors. After this command is configured, Update packets are sent to the peer in unicast instead of multicast or broadcast mode.

The **undo peer** command deletes the specified neighbor IP address.

By default, no RIP neighbor address is specified.

Format

peer *ip-address*

undo peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor.	The value is in dotted decimal notation.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Generally, you are advised to use the **peer** command because an interface may receive the same packets both in multicast (or broadcast) and unicast mode. You are advised to change the mode of the interface to the silent mode when configuring the **peer** command.

Example

Specify the IP address of the neighbor to 10.0.0.1.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] peer 10.0.0.1
```

7.2.26 preference (RIP)

Function

The **preference** command sets the preference for RIP routes.

The **undo preference** command restores the default preference of RIP routes.

The default preference for RIP routes is 100.

Format

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Parameters

Parameter	Description	Value
preference	Specifies the preference for routes.	The value is an integer ranging from 1 to 255. By default, it is 100.
route-policy *route-policy-name*	Specifies the routing policy that sets preference for the routes meeting conditions.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

A small value indicates a high preference. To enable RIP routes to have a higher preference than the routes learned by other IGP protocols, you need to configure a smaller preference value for the RIP routes. The preference determines the algorithm through which the optimal route is obtained among the routes in the IP routing table.

Example

Set the preference of RIP routes to 120.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] preference 120
```

Set the preference of RIP routes that match the routing policy named **rt-policy1** to 120.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] preference 120 route-policy rt-policy1
```

7.2.27 reset rip configuration

Function

The **reset rip configuration** command resets system parameters for a specified RIP process. When a RIP process starts, all the parameters of the process retain the default values.

Format

reset rip *process-id* **configuration**

Parameters

Parameter	Description	Value
process-id	Specifies a RIP process ID.	The value is an integer that ranges from 1 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Restarting RIP processes may interrupt services. Exercise caution when you run this command.

After the command is executed, RIP neighbor relationships are set up again and learned routes are deleted.

Example

Reset the parameters of RIP process 100.

```
<HUAWEI> reset rip 100 configuration
```

7.2.28 reset rip statistics

Function

The **reset rip statistics** command resets the counter that is maintained by a particular RIP process. This command allows you to repeatedly record statistics during debugging.

Format

reset rip *process-id* **statistics** [**interface** { **all** | *interface-type interface-number* [**neighbor** *neighbor-ip-address*] }]

Parameters

Parameter	Description	Value
process-id	Specifies a RIP process ID.	The value is an integer ranging from 1 to 65535.
all	Clears statistics of all RIP processes.	-
interface all	Clears statistics on all the interfaces of a specified RIP process.	-
interface *interface-type interface-number*	Clears statistics on the interface with specified number and type.	-
neighbor *neighbor-ip-address*	Clears statistics on the RIP process between the local RIP interface and the specified neighbor.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Statistics cannot be restored after being cleared. Exercise caution when you run this command.

Example

Clear statistics in RIP process 100.

```
<HUAWEI> reset rip 100 statistics
```

Clear statistics on all interfaces in RIP process 100.

```
<HUAWEI> reset rip 100 statistics interface all
```

7.2.29 rip

Function

The **rip** command starts the specified RIP in the system view.

The **undo rip** command stops the specified RIP process.

By default, no RIP process is started.

Format

rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer that ranges from 1 to 65535. The default value is 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If no VPN instance is specified, a RIP process is run globally or in the default VPN instance. Before configuring each global RIP parameter, you need to start RIP. This restriction is not applicable when you configure interface-related parameters.

Example

Start RIP process 1.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1]
```

Start RIP process 100 in the VPN instance named **abc**.

```
<HUAWEI> system-view
[HUAWEI] rip 100 vpn-instance abc
[HUAWEI-rip-100]
```

7.2.30 rip authentication-mode

Function

The **rip authentication-mode** command sets the RIP-2 authentication mode and authentication parameters. Only one authentication password is used for each authentication. If multiple authentication passwords are configured, the latest one takes effect.

The **undo rip authentication-mode** command cancels authentication.

By default, no authentication is configured.

Format

rip authentication-mode simple { **plain** *plain-text* | [**cipher**] *password-key* }

rip authentication-mode keychain *keychain-name*

rip authentication-mode md5 usual { **plain** *plain-text* | [**cipher**] *password-key* }

rip authentication-mode md5 nonstandard { **keychain** *keychain-name* | { **plain** *plain-text* | [**cipher**] *password-key* } *key-id* }

rip authentication-mode hmac-sha256 { **plain** *plain-text* | [**cipher**] *password-key* } *key-id*

undo rip authentication-mode

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
simple	Specifies simple authentication. **NOTE** Simple authentication mode carries potential risks. HMAC-SHA256 ciphertext authentication is recommended.	-
md5	Specifies MD5 authentication. **NOTE** MD5 ciphertext authentication carries potential risks. HMAC-SHA256 ciphertext authentication is recommended.	-
usual	Indicates that MD5 ciphertext authentication packets use the universal format (private standard).	-
nonstandard	Indicates that MD5 ciphertext authentication packets use non-standard packet format (IETF standard).	-
plain	Indicates that only plain text can be entered and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. You are advised to select **cipher** to save the password in cipher text.	-

Parameter	Description	Value
plain-text	Specifies the authentication password that is displayed in plain text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. When the authentication mode is **simple** or **md5 usual**, the password consists of 1 to 16 characters. When the authentication mode is **md5 nonstandard** or **hmac-sha256**, the password consists of 1 to 255 characters.
cipher	Indicates that either plain text or cipher text can be entered and cipher text is displayed when the configuration file is viewed.	-
password-key	Specifies the authentication password that is displayed in cipher text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. ● When the authentication mode is **simple** or **md5 usual**, the password is in plain text (1 to 16 characters) or in cipher text (24 or 32 or 48 characters). If the source version supports a ciphertext password which is a string of 24 or 32 characters, the target version also supports this type of password. ● When the authentication mode is **md5 nonstandard** or **hmac-sha256**, the password is in plain text (1 to 255 characters) or in cipher text (20 to 392 characters).
keychain *keychain-name*	Specifies keychain authentication.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Parameter	Description	Value
key-id	Specifies the identifier of Cryptographic authentication.	The value is an integer that ranges from 1 to 255.
hmac-sha256	Indicates Keyed-Hash Message Authentication Code (HMAC) for Secure Hash Algorithm 256 (SHA256).	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Keychain authentication improves UDP connection security. Keychain authentication must be configured on both ends of a link. Encryption algorithms and passwords configured on both ends must be the same; otherwise, the UDP connection cannot be set up and RIP messages cannot be transmitted.

Example

Set HMAC-SHA256 authentication on VLANIF100, with the authentication password **YsHsjx_202206** and key-id **255**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip authentication-mode hmac-sha256 cipher YsHsjx_202206 255
```

Set HMAC-SHA256 authentication on GE0/0/1, with the authentication password **YsHsjx_202206** and key-id **255**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip authentication-mode hmac-sha256 cipher YsHsjx_202206 255
```

7.2.31 rip bfd

Function

The **rip bfd** command sets BFD session parameters on the specified interface.

The **undo rip bfd** command restores BFD session parameters set on the specified interface.

By default, the minimum intervals for receiving and sending BFD packets are 1000 ms and the detection time multiplier is 3.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

rip bfd { **min-rx-interval** *min-receive-value* | **min-tx-interval** *min-transmit-value* | **detect-multiplier** *detect-multiplier-value* } *

undo rip bfd { **min-rx-interval** [*min-receive-value*] | **min-tx-interval** [*min-transmit-value*] | **detect-multiplier** [*detect-multiplier-value*] } *

Parameters

Parameter	Description	Value
min-rx-interval *min-receive-value*	Specifies the minimum interval at which BFD packets are received from the remote device.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *min-transmit-value*	Specifies the minimum interval at which BFD packets are sent to the remote device.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
detect-multiplier *detect-multiplier-value*	Specifies the local detection multiplier.	The value is an integer ranging from 3 to 50.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The *min-receive-value* value is obtained after the local **min-rx-interval** value and a neighbor's **min-tx-interval** value are negotiated. For detailed negotiation policies, see **bfd all-interfaces**. If the switch does not receive BFD packets from the neighbor at the interval of *min-receive-value* x *detect-multiplier-value*, the neighbor will go Down.

Prerequisites

Enable BFD globally and run the **rip bfd enable** command before establishing a BFD session.

Precautions

BFD session parameters configured in a RIP process take effect only after BFD is enabled on the interface.

The BFD priority configured on an interface is higher than the BFD priority configured in a RIP process. If BFD session parameters are configured on an interface, establish a BFD session based on the configured parameters.

Example

Enable BFD on VLANIF100 and set the minimum sending interval to 600 ms and local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip bfd enable
[HUAWEI-Vlanif100] rip bfd min-tx-interval 600 detect-multiplier 4
```

Enable BFD on GE0/0/1 and set the minimum sending interval to 600 ms and local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] rip bfd enable
[HUAWEI-GigabitEthernet0/0/1] rip bfd min-tx-interval 600 detect-multiplier 4
```

7.2.32 rip bfd block

Function

The **rip bfd block** command blocks BFD on a specified interface.

The **undo rip bfd block** command disables the blocking function.

By default, the blocking function is disabled.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

rip bfd block

undo rip bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be used to block the specified interface from enabling BFD on some links where no BFD session is needed.

Precautions

The **rip bfd block** and **rip bfd enable** commands are mutually exclusive. If both of them are configured, only the later configured one takes effect.

Example

Block BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip bfd block
```

Block BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip bfd block
```

7.2.33 rip bfd enable

Function

The **rip bfd enable** command enables BFD on the specified interface to establish a BFD session with default parameters.

The **undo rip bfd enable** command disables BFD on the specified interface.

By default, BFD is disabled on a RIP interface.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

rip bfd enable

undo rip bfd enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If BFD is not enabled globally, you can set BFD parameters on the specified interface but you cannot establish a BFD session on this interface.

The **rip bfd block** and **rip bfd enable** commands are mutually exclusive. If both of them are configured, only the later configured one takes effect.

Example

Enable BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip bfd enable
```

Disable BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo rip bfd enable
```

Enable BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip bfd enable
```

Disable BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] undo rip bfd enable
```

7.2.34 rip bfd static

Function

The **rip bfd static** command enables static BFD on a specified RIP interface.

The **undo rip bfd static** command disables static BFD on a specified RIP interface.

By default, static BFD is disabled on a RIP interface.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

rip bfd static

undo rip bfd static

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network deployed with high-speed data services, if a fault occurs on a link, a large amount of data is lost because it takes too long time for RIP to detect the fault. Deploying BFD for RIP to accelerate fault detection is necessary.

The **rip bfd static** command is used to enable BFD for RIP on a specified link to rapidly detect the fault on the link.

In addition, because many devices do not support BFD on the live network, this command can be also used to implement BFD between a BFD-capable device and a BFD-incapable device.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

If **rip bfd static**, **rip bfd enable**, and **rip bfd block** are simultaneously configured, the latest configuration overrides the previous ones.

Example

Enable static BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] bfd
```

```
[HUAWEI-bfd] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip bfd static
```

Enable static BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip bfd static
```

7.2.35 rip input

Function

The **rip input** command enables the specified interface to receive RIP packets.

The **undo rip input** command disables the specified interface from receiving RIP packets.

By default, interfaces can receive RIP packets.

Format

rip input

undo rip input

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The priority of **silent-interface** is higher than the priority of **rip input** or **rip output** configured in the interface view. By default, an interface does not work in the silent state.

Example

Enable the specified interface VLANIF100 to receive RIP packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip input
```

Enable the specified interface GE0/0/1 to receive RIP packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip input
```

7.2.36 rip metricin

Function

The **rip metricin** command sets the metric that is added to the route when an interface receives a RIP packet.

The **undo rip metricin** command restores the additional metric to the default value.

By default, there is no metric added to the route when an interface receives a RIP packet.

Format

rip metricin { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } *value1* }

undo rip metricin

Parameters

Parameter	Description	Value
value	Specifies the metric that is added to the received route.	The value is an integer ranging from 0 to 15. By default, it is 0.
acl-number	Specifies the basic ACL number.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the ACL name.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
value1	Specifies the metric that is added to the route that passes the filtering of the ACL or IP prefix list.	The value is an integer ranging from 1 to 15.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When an interface receives a route, RIP adds the additional metric of the interface to the route, and then installs the route into the routing table. Therefore, increasing the metric of an interface also increases the metric of the RIP route received by the interface.

Adjust RIP route selection by increasing the metrics of received routes.

Example

Set the additional metric to 12 when VLANIF100 receives RIP routes.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip metricin 12
```

Set the additional metric to 12 when GE0/0/1 receives RIP routes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip metricin 12
```

Set the additional metric to 12 using acl-name.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip metricin acl-name abcd 12
```

Set the additional metric to 12 using ip-prefix.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip metricin ip-prefix ip1 12
```

7.2.37 rip metricout

Function

The **rip metricout** command sets the metric that is added to the route when an interface sends a RIP packet.

The **undo rip metricout** command restores the additional metric to the default value.

By default, the metric that is added to the route when an interface sends a RIP packet is 1.

Format

rip metricout { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } *value1* }

undo rip metricout

Parameters

Parameter	Description	Value
value	Specifies the metric that is added to the sent route.	The value is an integer ranging from 1 to 15. By default, it is 1.
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list. The name must be exclusive.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
value1	Specifies the metric that is added to the route that passes the filtering of the ACL or IP prefix list.	The value is an integer ranging from 2 to 15.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a RIP route is advertised, the additional metric is added to the route. Therefore, increasing the metric of an interface also increases the metric of the RIP route sent on the interface. However, the metric of the route in the routing table remains unchanged.

You can specify the metric to be added to the RIP route that passes the filtering of the ACL or IP prefix list by specifying *value1*. If a RIP route does not pass the filtering, its metric is increased by 1.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Set the metric that is added when the interface sends RIP routes to 12.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip metricout 12
```

Set the metric that is added when the interface sends RIP routes to 12.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip metricout 12
```

Increase the metric of a RIP route that passes the filtering of ACL 2050 by 12.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip metricout 2050 12
```

Increase the metric of a RIP route that passes the filtering of ACL 2050 by 12.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip metricout 2050 12
```

Increase the metric of a RIP route that passes the filtering of the IP prefix list named **p1** by 12.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix p1 permit 10.10.10.1 24
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip metricout ip-prefix p1 12
```

Increase the metric of a RIP route that passes the filtering of the IP prefix list named **p1** by 12.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip metricout ip-prefix p1 12
```

7.2.38 rip mib-binding

Function

The **rip mib-binding** command sets the binding between the Management Information Base (MIB) and RIP process ID, and specifies the ID of the RIP process that receives SNMP requests.

The **undo rip mib-binding** command cancels the binding.

By default, there is no binding between the Management Information Base and RIP process ID.

Format

rip mib-binding *process-id*

undo rip mib-binding

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535. The default value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All SNMP requests are sent to the bound RIP process.

Prerequisites

A RIP process has been created using the **rip** command.

Example

Configure RIP process 100 to receive SNMP requests.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] quit
[HUAWEI] rip mib-binding 100
```

7.2.39 rip output

Function

The **rip output** command enables an interface to send RIP packets.

The **undo rip output** command disables an interface from sending RIP packets.

By default, an interface can send RIP packets.

Format

rip output

undo rip output

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a device running RIP is connected to a network running other routing protocols, you can run the **rip output** command on the interface that connects the device to the network to prevent the interface from sending useless packets to the network.

The priority of **silent-interface** is higher than the priority of **rip input** or **rip output** that is configured in the interface view. By default, an interface does not work in the silent state.

Example

Enable the interface VLANIF100 to send RIP packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip output
```

Enable the interface GE0/0/1 to send RIP packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip output
```

7.2.40 rip pkt-transmit

Function

The **rip pkt-transmit** command sets the interval for sending Update packets and the number of packets sent each time on the specified interface.

The **undo rip pkt-transmit** command restores the default values on an interface.

By default, the interval for sending RIP Update packets is 200 ms and 50 packets are sent each time.

Format

rip pkt-transmit { **interval** *interval* | **number** *pkt-count* } *

undo rip pkt-transmit

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for sending Update packets.	The value is an integer ranging from 50 to 500, in milliseconds. The default value is 200.
number *pkt-count*	Specifies the number of packets sent each time.	The value is an integer and ranges from 25 to 100. The default value is 50.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **rip pkt-transmit** command can be used on an interface to control the interval for sending Update packets and the number of sent packets. This improves RIP performance.

Example

Set the interval for sending packets on VLANIF100 to 100 milliseconds and the number of the packets sent each time to 50.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip pkt-transmit interval 100 number 50
```

Set the interval for sending packets on GE0/0/1 to 100 milliseconds and the number of the packets sent each time to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip pkt-transmit interval 100 number 50
```

7.2.41 rip poison-reverse

Function

The **rip poison-reverse** command enables poison reverse.

The **undo rip poison-reverse** command disables poison reverse.

By default, poison reverse is disabled.

Format

rip poison-reverse

undo rip poison-reverse

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After poison reverse is enabled, RIP sets the cost of the routes learned from a specified interface to 16 (indicating unreachable), and then sends the routes to neighbors through the same interface.

When both split horizon and poison reverse are configured, only poison reverse takes effect.

Example

Enable poison reverse.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip poison-reverse
```

Enable poison reverse on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip poison-reverse
```

7.2.42 rip replay-protect

Function

The **rip replay-protect** command enables the replay-protect function.

The **undo rip replay-protect** command disables the replay-protect function.

By default, the replay-protect function is disabled.

Format

rip replay-protect [*window-range*]

undo rip replay-protect

Parameters

Parameter	Description	Value
window-range	Specifies the size of the connection-oriented transmission buffer.	It is an integer ranging from 50 to 50000. The default value is 50.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If the Identification field in the last RIP packet sent before a RIP interface goes Down is X, after the interface goes Up, the Identification field in the RIP packet sent by this interface becomes 0. If the remote end does not receive the RIP packet with the Identification field being 0, subsequent RIP packets will be discarded until the remote end receives the RIP packet with the Identification field being X+1. As a result, RIP routing information of both ends is inconsistent. To solve this problem, you need to configure the **rip replay-protect** command so that RIP can obtain the Identification field in the RIP packet sent before the RIP packet goes Down and increases the Identification field of the subsequently sent RIP packet by one.

Before configuring the **rip replay-protect** command, you need to configure the **rip authentication-mode** command in the RIP interface view to configure the authentication mode and authentication parameters of RIP-2.

NOTE

If you configure the **rip replay-protect** command in the same view for multiple times, only the last configuration takes effect.

Example

Enable the replay-protect function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip replay-protect
```

Enable the replay-protect function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip replay-protect
```

7.2.43 rip split-horizon

Function

The **rip split-horizon** command enables split horizon.

The **undo rip split-horizon** command disables split horizon.

By default, split horizon is enabled.

Format

rip split-horizon

undo rip split-horizon

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If a route is advertised through the interface from which the route is learned, the route is blocked by split horizon. Split horizon is used to avoid routing loops between neighboring devices.

Generally, it is not recommended that you disable split horizon.

If split horizon is enabled on the interface that is configured with secondary IP addresses, RIP Update packets may not be sent by each secondary address. An Update packet does not regard every network as the source unless split horizon is disabled.

If an interface is connected to a Non Broadcast Multiple Access (NBMA) network, split horizon on the interface is disabled by default.

If both poison reverse and split horizon are configured, simple split horizon (the route is suppressed by the interface through which the route is learned) is substituted by poison reverse. Here, simple split horizon means that the route is suppressed when it is advertised through the interface from which it is learned.

Example

Enable split horizon.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip split-horizon
```

Enable split horizon.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip split-horizon
```

7.2.44 rip summary-address

Function

The **rip summary-address** command configures a RIP switch to advertise a local summarized IP address.

The **undo rip summary-address** command disables a RIP switch from advertising a local summarized IP address.

By default, a RIP switch does not advertise local summarized IP addresses.

Format

rip summary-address *ip-address mask* [**avoid-feedback**]

undo rip summary-address *ip-address mask*

Parameters

Parameter	Description	Value
ip-address	Specifies the network IP address to be summarized.	The value is in dotted decimal notation.
mask	Specifies the network mask.	The value is in dotted decimal notation.
avoid-feedback	Specifies that learning the same summarized route from an interface is not allowed.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After the keyword **avoid-feedback** is specified, an interface no longer learns the summarized route with the same IP address as the advertised summarized IP address. This avoids routing loops.

Example

Configure the switch to advertise a local summarized IP address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip summary-address 10.0.0.0 255.0.0.0
```

Configure the switch to advertise a local summarized IP address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip summary-address 10.0.0.0 255.0.0.0
```

7.2.45 rip valid-ttl-hops

Function

The **rip valid-ttl-hops** command enables the RIP GTSM functions and sets the TTL value to be detected.

The **undo rip valid-ttl-hops** command cancels the function.

By default, the RIP GTSM functions are disabled.

Format

rip valid-ttl-hops *valid-ttl-hops-value* [**vpn-instance** *vpn-instance-name*]

undo rip valid-ttl-hops [*valid-ttl-hops-value*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
valid-ttl-hops-value	Specifies the number of TTL hops to be detected. The valid TTL range of the detected packets is [255 -*valid-ttl-hops-value* + 1, 255].	The value is an integer ranging from 1 to 255.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance. If this parameter is used, you need only to specify the TTL value to be detected by the VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a network demanding higher security, you can enable GTSM to improve the security of the RIP network. GTSM defends against attacks by checking the TTL value. If an attacker simulates RIP unicast packets and keeps sending them to a switch, a switch receives the packets and directly sends them to the main control board for RIP processing, without checking the validity of the packets. In this case, the switch is busy processing these packets, causing high usage of the CPU. GTSM protects the routers and enhances the system security by checking whether the TTL value in the IP packet header is in a pre-defined range.

The **rip valid-ttl-hops** command is used to enable RIP GTSM.

Precautions

GTSM configurations must be symmetrical. That is, GTSM must be enabled on devices at both ends.

If GTSM is enabled on a device, after the device receives a RIP packet, it checks whether the TTL value in the packet is in a pre-defined range. If the TTL value is beyond the pre-defined range, the device considers the packet as an attack packet and discards it.

Example

Enable the RIP GTSM functions, and configure the maximum number of TTL hops to 5 for the packets that a switch is allowed to receive.

```
<HUAWEI> system-view
[HUAWEI] rip valid-ttl-hops 5
```

7.2.46 rip version

Function

The **rip version** command sets the RIP version of an interface.

The **undo rip version** command restores the default setting.

By default, an interface sends only RIP-1 packets, but it can receive both RIP-1 and RIP-2 packets.

Format

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

Parameters

Parameter	Description	Value
1	Indicates RIP-1 packets.	-
2	Indicates RIP-2 packets.	-

Parameter	Description	Value
broadcast	Indicates that RIP-2 packets are sent in broadcast mode.	-
multicast	Indicates that RIP-2 packets are sent in multicast mode. **NOTE** By default, RIP-2 packets are sent in multicast mode.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The versions of the request packets and response packets vary with the configured RIP version.

- If the version of RIP is not set, a device sends RIP-1 packets in broadcast mode and receives the RIP-1 and RIP-2 packets that are sent in broadcast mode.
- If the RIP version is set to RIP-1, a device sends only RIP-1 packets in broadcast mode and receives the RIP-1 packets that are sent in broadcast mode.
- If the RIP version is set to RIP-2, a device sends only RIP-2 packets in multicast mode and receives RIP-2 packets that are sent in multicast or broadcast mode.
- If the RIP version is set to multicast RIP-2, a device sends RIP-2 packets in multicast mode and receives RIP-2 packets that are sent in multicast mode.
- If the RIP version is set to broadcast RIP-2, a device sends RIP-2 packets in broadcast mode and receives RIP-1 and RIP-2 packets.

Precautions

You can also set a RIP version in a RIP process, but the RIP version that is set on an interface has a higher priority.

Example

Send RIP-2 packets in broadcast mode.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip version 2 broadcast
```

Send RIP-2 packets in broadcast mode.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] rip version 2 broadcast
```

7.2.47 silent-interface (RIP)

Function

The **silent-interface** command controls an interface only to receive packets to update its routing table and prevent it from sending RIP packets.

The **undo silent-interface** command enables an RIP interface to send Update packets.

The **silent-interface disable** command enables an RIP interface to send Update packets.

The **undo silent-interface disable** command controls an interface only to receive packets to update its routing table and prevent it from sending RIP packets.

By default, silent interface not enabled.

Format

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

silent-interface disable *interface-type interface-number*

undo silent-interface disable *interface-type interface-number*

Parameters

Parameter	Description	Value
all	Indicates that all interfaces are suppressed.	-
interface-type interface-number	Specifies the type and the number of the interface.	-
disable	Disables the suppression of the RIP interface so that the interface can send Update packets.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switch running RIP is connected to a network running other routing protocols, you can run the **silent-interface** command on the interface that connects the switch to the network to prevent the interface from sending useless packets to the network.

The **silent-interface** command is used together with the **peer (RIP)** command to advertise routes to the specified equipment.

Configuration Impact

If an interface is suppressed, the direct routes of the network segment where the interface resides can still be advertised to other interfaces.

Precautions

When the **silent-interface** command is used to suppress the specified interface, the priority of the **silent-interface** command is higher than the priority of the **rip input** and **rip output** command that is configured in the interface view.

NOTE

After you configure all interfaces as silent interfaces, you can run the **silent-interface disable** *interface-type interface-number* command to activate a specified silent interface.

Example

Configure all the interfaces as silent interfaces.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] silent-interface all
```

Configure the RIP interface VLANIF100 as a silent interface and enable it to send routes to the neighbor with the IP address of 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] silent-interface vlanif 100
[HUAWEI-rip-100] peer 10.1.1.1
```

Configure all interfaces as silent interfaces, and then activate the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] silent-interface disable vlanif 100
```

7.2.48 summary (RIP)

Function

The **summary** command enables RIP classful summarization. The summarized routes are advertised using natural masks.

The **undo summary** command disables classful summarization so that routing between subnets can be performed. The subnet information is then advertised. Route summarization reduces the routing table size.

By default, classful summarization is enabled for RIP-2.

Format

summary [**always**]

undo summary

Parameters

Parameter	Description	Value
always	Enables classful summarization no matter whether split horizon is configured.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

RIP-1 does not support classful summarization. When using RIP-2, you can use the **undo summary** command to disable classful summarization.

RIP-2 route summarization improves scalability and efficiency on large networks. IP address summarization means that there is no sub-routing entry in the routing table. That is, there is no routing entry composed of single IP address. In addition to reducing the routing table size, route summarization enables the switch to handle more routes.

When classful summarization is enabled, the switch summarizes subnet addresses to the natural network segment border while advertising routes to the natural network segment border. When split horizon or poison reverse is enabled, route summarization will be invalid if the **always** parameter is not specified. When summarized routes are sent outside the natural network segment, split horizon or poison reverse must be disabled.

NOTE

- By default, classful summarization is enabled for RIP-2. If split horizon or poison reverse has been configured, classful summarization is invalid. When summarized routes are sent to the network border, split horizon and poison reverse must be disabled.
- The **summary always** command can enable classful summarization no matter whether split horizon or poison reverse is enabled.
- The summarization preference on interfaces is higher than the summarization preference in RIP processes. That is, the preference of **rip summary-address** is higher than the preference of **summary**. When summarization is configured on both interface and RIP process, the summarized route is advertised only when a few specific routes are beyond the summarization range configured on the interface.

Example

Enable RIP-2 classful summarization.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] version 2
[HUAWEI-rip-1] summary
```

Enable RIP-2 classful summarization when split horizon is enabled.

```
<HUAWEI> system-view
[HUAWEI] rip 1
[HUAWEI-rip-1] summary always
```

7.2.49 timers rip

Function

The **timers rip** command sets the values of RIP timers.

The **undo timers rip** command restores the values of RIP timers to the default value.

By default, the interval for sending Update packets is 30s, the time for aging routes is 180s, the time for deleting a route from the routing table is 120s.

Format

timers rip *update age garbage-collect*

undo timers rip

Parameters

Parameter	Description	Value
update	Specifies the interval for sending Update packets.	The value is an integer ranging from 1 to 86400, in seconds.
age	Specifies the time for aging routes.	The value is an integer ranging from 1 to 86400, in seconds.
garbage-collect	Specifies the time for deleting a route from the routing table, that is, the standard garbage collection time.	The value is an integer ranging from 1 to 86400, in seconds.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

By adjusting the RIP timers, you can improve routing protocol performance to meet network requirements. If the values of the preceding three timers are set improperly, route flapping occurs.

The relationship of the values of the three timers is: *update* < *age* and *update* < *garbage-collect*. For example, if the update time is longer than the aging time, switches cannot inform neighbors on time if RIP routes change during the update time.

NOTE

Generally, the default values of the timers do not need to be changed, and thus the **timers rip** command must be used with caution.

Example

Set values for RIP timers.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] timers rip 35 170 240
```

7.2.50 verify-source (RIP)

Function

The **verify-source** command enables check on source IP addresses in RIP Update packets.

The **undo verify-source** command disables check on source IP addresses in RIP Update packets.

By default, the source IP addresses in RIP Update packets are checked.

Format

verify-source

undo verify-source

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **verify-source** command is executed, RIP checks whether the IP addresses of interfaces that send and receive the Update packets are on the same network segment. If not, the device does not process the packets.

NOTE

It is not recommended that you disable source address check.

Example

Enable source address check in RIP 100.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] verify-source
```

7.2.51 version (RIP)

Function

The **version** command specifies a global RIP version.

The **undo version** command restores the default global RIP version.

By default, an interface sends only RIP-1 packets, and receives both RIP-1 and RIP-2 packets.

Format

version { **1** | **2** }

undo version

Parameters

Parameter	Description	Value
1	Sets the global RIP version to RIP-1.	-
2	Sets the global RIP version to RIP-2.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Two versions are available for RIP: RIP-1 and RIP-2. RIP-2 is an extension to RIP-1. You can run the **version** command to specify a global RIP version.

Example

Send and receive RIP-2 packets.

```
<HUAWEI> system-view
[HUAWEI] rip 100
[HUAWEI-rip-100] version 2
```

7.3 RIPng Configuration Commands

7.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.3.2 checkzero (RIPng)

Function

The **checkzero** command enables zero field check for RIPng packets.

The **undo checkzero** command disables zero field check for RIPng packets.

By default, zero field check is enabled for RIPng packets.

Format

checkzero

undo checkzero

Parameters

None

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

After zero field check is enabled, the switch refuses to process the RIPng packets in which zero fields are not 0. If all RIPng packets are reliable and no zero field needs to be checked, run the **undo checkzero** command to reduce CPU usage.

Example

Disable zero field check for RIPng packets.

```
<HUAWEI> system-view
[HUAWEI] ripng 1
[HUAWEI-ripng-1] undo checkzero
```

7.3.3 default-cost (RIPng)

Function

The **default-cost** command sets the default cost for imported routes.

The **undo default-cost** command restores the default value 0.

By default, the default cost of RIPng routes is 0.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Sets the default cost of imported routes.	The value is an integer that ranges from 0 to 15.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

You can run one of the following commands to set the cost of imported routes. The following commands are listed in descending order of priorities.

- Run the **apply cost** command to set the cost of routes.
- Run the **import-route** command to set the cost of imported routes.
- Run the **default-cost** (RIPng) command to set the default cost of imported routes.

Example

Set the default cost of imported routes to 2.

```
<HUAWEI> system-view
[HUAWEI] ripng 100
[HUAWEI-ripng-100] default-cost 2
```

7.3.4 description (RIPng)

Function

The **description** command configures a description for a RIPng process.

The **undo description** command deletes the configured description of a RIPng process.

By default, there is no description for a RIPng process.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Configures a description for a RIPng process.	The description is a string of 1 to 80 case-sensitive characters that can contain spaces.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring descriptions for RIPng processes helps identify and configure RIPng processes.

Precautions

If you run the **description** command multiple times, only the latest configuration takes effect.

Example

Configure a description for RIPng process 100.

```
<HUAWEI> system-view
[HUAWEI] ripng 100
[HUAWEI-ripng-100] description this process configure the poison reverse process
```

7.3.5 display default-parameter ripng

Function

The **display default-parameter ripng** command displays the default RIPng configuration.

Format

display default-parameter ripng

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the default RIPng configuration is modified, you can use the **display default-parameter ripng** command to view the default RIPng configuration used when RIPng is initialized.

Example

Display the default RIPng configuration.

```
<HUAWEI> display default-parameter ripng
--------------------------------------------
 Protocol Level Default Configurations
--------------------------------------------
       Preference    : 100
       Checkzero     : Enabled
       Default-cost  : 0
       Maximum Balanced Paths : 8
       Update time   : 30 sec      Age time   : 180 sec
       Garbage-collect time            : 120 sec
--------------------------------------------
 Interface Level Default Configurations
--------------------------------------------
    Metricin                 : 0
    Metricout                : 1
    Input Packet Processing : Enabled
    Output Packet Processing: Enabled
    Poison Reverse           : Disabled
    Split Horizon
     For Broadcast and P2P Interfaces     :  Enabled
     For NBMA Interfaces and LoopBack     :  Disabled
    Default Route                          :  Disabled
    Packet Transmit Interval              :  200 msecs
    Packet Transmit Number                 :  30
```

Table 7-13 Description of the display default-parameter ripng command output

Item	Description
Protocol Level Default Configurations	Default RIPng process configuration.
Preference	RIPng route preference.

Item	Description
Checkzero	Whether zero field check is enabled for RIPng packets.
Default Cost	Default cost of routes imported by RIPng from other routing protocols.
Maximum Balanced Paths	Maximum number of equal-cost routes for load balancing.
Update time	Interval for sending Update packets.
Age time	Aging time of RIPng routes.
Garbage-Collect time	Time from when a route is marked invalid until the route is removed from the routing table.
Interface Level Default Configurations	Default RIPng configuration on an interface.
Metricin	Metric that is added to a route when a RIPng packet is received.
Metricout	Metric that is added to a route when a RIPng packet is sent.
Poison Reverse	Whether poison reverse is enabled.
Split Horizon	Whether split horizon is enabled: ● For Broadcast and P2P Interfaces: broadcast and P2P interfaces ● For NBMA Interfaces and LoopBack: NBMA and loopback interfaces
Default-route	Default route. This route is used when no matching entry can be found for a packet in the routing table.
Packet Transmit Interval	Interval for forwarding packets, in milliseconds.
Packet Transmit Number	Number of forwarded packets.
Input Packet Processing	Whether this interface is enabled to receive RIPng packets
Output Packet Processing	Whether this interface is enabled to send RIPng packets

7.3.6 display ripng

Function

The **display ripng** command displays the current operating status and configuration of RIPng processes.

Format

display ripng [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Displays the current operating status and configuration of the specified RIPng process. If this parameter is not specified, the configurations of all RIPng processes are displayed.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the status and configuration of a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ripng** command to check the current operating status and configuration of RIPng processes.

Example

Display information about a specified RIPng process.

```
<HUAWEI> display ripng 100
Public vpn-instance
    RIPng process : 100
       Preference : 100
       Checkzero : Enabled
       Default-cost : 0
       Maximum number of balanced paths : 8
       Update time   : 30 sec   Age time  : 180 sec
       Garbage-collect time : 120 sec
       Number of periodic updates sent : 0
       Number of trigger updates sent : 1
       Number of routes in database : 1
       Number of interfaces enabled : 1
       Total number of routes : 3
```

```
    Total number of routes in ADV DB is : 0
```

Table 7-14 Description of the display ripng command output

Item	Description
Public vpn-instance	Public VPN.
RIPng process	RIPng process ID.
Preference	RIPng process preference. To set the preference for RIPng routes, run the **preference (RIPng)** command.
Checkzero	Whether zero field check is enabled for RIPng packets.
Default-cost	Default cost of routes imported by RIPng from other routing protocols.
Maximum number of balanced paths	Maximum number of equal-cost routes for load balancing. To set the preference for RIPng routes, run the **maximum load-balancing (RIPng)** command.
Update time	Interval for sending Update packets.
Age time	Aging time of RIPng routes.
Garbage-collect time	Time from when a route is marked invalid until the route is removed from the routing table.
Number of periodic updates sent	Number of RIPng Update packets sent periodically.
Number of trigger updates sent	Number of triggered RIPng Update packets.
Number of routes in database	Number of routes in the RIPng database.
Number of interfaces enabled	Number of RIPng interfaces.
Total number of routes	Total number of routes of a RIPng process.
Total number of routes in ADV DB is	Total number of advertised routes in the database.

7.3.7 display ripng database

Function

The **display ripng database** command displays all the active routes in the RIPng database.

Format

display ripng *process-id* **database** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Displays all the active routes of the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
verbose	Displays detailed information about the routes in the RIPng database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ripng database** command to check all the active routes in the RIPng database.

Example

Display routes in the RIPng database.

```
<HUAWEI> display ripng 100 database
1::/64,
      via FE80::82FB:6FF:FE35:45B6, Vlanif200, cost 0, Imported
  2::/64,
      Vlanif100, cost 0, RIPng-interface
  3::/64,
      via FE80::82FB:6FF:FE35:45B6, Vlanif200, cost 16
  3::/64,
      Vlanif200, cost 0, RIPng-interface
  4::/64,
      via FE80::82FB:6FF:FE35:45B6, Vlanif200, cost 1
```

Table 7-15 Description of the display ripng database command output

Item	Description
1::/64	Destination IPv6 address of a route.
via	Next-hop link-local address.
cost	Cost of a route.
Imported	Route imported from other routing protocols.

Item	Description
RIPng-interface	Route generated by RIPng.

7.3.8 display ripng interface

Function

The **display ripng interface** command displays information about RIPng interfaces.

Format

display ripng *process-id* **interface** [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Displays interface information in the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
interface-type interface-number	Displays information on the interface with the specified type and number.	-
verbose	Displays detailed information about RIPng interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the configuration and operating status of RIPng. The information is helpful in fault location and configuration verification.

Example

Display information about VLANIF100 of the specified RIPng process.

```
<HUAWEI> display ripng 1 interface vlanif 100
 Vlanif100
    FE80::A0A:200:1
    State : UP, Protocol : RIPNG, MTU : 1440
```

Table 7-16 Description of the display ripng interface command output

Item	Description
FE80::A0A:200:1	Link-local address of the interface.
State	Status of the interface: ● UP ● DOWN
Protocol	Routing protocol running on the interface.
MTU	Link MTU.

Display detailed information about VLANIF100 of the specified RIPng process.

```
<HUAWEI> display ripng 1 interface vlanif100 verbose
 VLANIF100
    FE80::A0A:200:1
    State : UP, Protocol : RIPNG, MTU : 1440
    Metricin        : 0
    Metricout       : 1
    Input           : Enabled      Output : Enabled
    Default Route  : Disabled
    Poison Reverse : Disabled
    Split Horizon  : Enabled
```

Table 7-17 Description of the display ripng interface verbose command output

Item	Description
FE80::A0A:200:1	Link-local address of the interface.
State	Status of the interface: ● UP ● DOWN
Protocol	Routing protocol running on the interface.
MTU	Link MTU.
Metricin	Metric added to a received route. To set the metric, run the **ripng metricin** command.
Metricout	Metric added to a sent route. To set the metric, run the **ripng metricout** command.
Input	Indicates whether this interface is enabled to receive RIPng packets. To enable the specified interface to receive RIPng packets, run the **ripng input** command.
Output	Indicates whether this interface is enabled to send RIPng packets. To enable an interface to send RIPng packets, run the **ripng output** command.

Item	Description
Default Route	Whether the interface is enabled to advertise default routes. To generate a default route to the RIPng routing domain, run the **ripng default-route** command.
Poison Reverse	Whether poison reverse is enabled on the interface. To enable poison reverse for RIPng, run the **ripng poison-reverse** command.
Split Horizon	Whether split horizon is enabled on the interface. To enable split horizon for RIPng, run the **ripng split-horizon** command.

7.3.9 display ripng neighbor

Function

The **display ripng neighbor** command displays information about RIPng neighbors.

Format

display ripng *process-id* **neighbor** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Displays neighbor information in the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
verbose	Displays detailed information about RIPng neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ripng neighbor** command to check information about RIPng neighbors.

Example

Display neighbor information in RIPng process 1.

```
<HUAWEI> display ripng 1 neighbor
 Neighbor : FE80::A0A:201:1 Vlanif100
    Protocol : RIPNG
```

Table 7-18 Description of the display ripng neighbor command output

Item	Description
Neighbor	IPv6 address and interface type of the neighbor interface.
Protocol	Routing protocol.

Display detailed neighbor information in RIPng process 1.

```
<HUAWEI> display ripng 1 neighbor verbose
 Neighbor : FE80::A0A:201:1 VLANIF100
    Protocol : RIPNG
    Number of Active routes      : 1
    Number of routes in garbage  : 0
```

Table 7-19 Description of the display ripng neighbor verbose command output

Item	Description
Number of Active routes	Number of active routes.
Number of routes in garbage	Number of garbage routes.

7.3.10 display ripng neighbor last-nbr-down

Function

The **display ripng neighbor last-nbr-down** command displays information about the last neighbor that goes Down in a RIPng process.

Format

display ripng *process-id* **neighbor last-nbr-down**

Parameters

Parameter	Description	Value
process-id	Displays information about the last neighbor that goes Down in the specified RIPng process.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ripng neighbor last-nbr-down** command can be used to view information about the last neighbor that goes Down in a RIPng process and the reason why the neighbor goes Down.

Example

Display information about the last neighbor that goes Down in a RIPng process.

```
<HUAWEI> display ripng 1 neighbor last-nbr-down
 Neighbor down index              : 1
 Neighbor Link local Address      : FE80::2E0:B7FF:FE5B:8242
 Interface                        : vlanif 100
 Reason for Neighbor down         : Interface Down
 Time at which neighbor went down : 2011-06-02 12:03:40+03:00 DST
```

Table 7-20 Description of the display ripng neighbor last-nbr-down command output

Item	Description
Neighbor down index	Index of the neighbor that goes Down.
Neighbor link local Address	IPv6 link-local address of the neighbor interface.
Interface	Interface connecting to the neighbor.
Reason for Neighbor down	Reason that a neighbor goes Down ● Interface Down ● Configuration Change ● Time Out (Normal) ● Time Out (Authentication Failed)
Time at which neighbor went down	Time the neighbor goes Down.

7.3.11 display ripng route

Function

The **display ripng route** command displays all the RIPng routes that the switch learns from other switches.

Format

display ripng *process-id* **route**

Parameters

Parameter	Description	Value
process-id	Displays the RIPng routes of the specified RIPng process that the switch learns from other switches.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ripng route** command is useful for debugging and testing protocols.

Example

Display all active and inactive RIPng routes and timers of each route.

```
<HUAWEI> display ripng 100 route
   Route Flags: R - RIPng
               A - Aging, G - Garbage-collect
 ----------------------------------------------------------------

 Peer 2000::1  on vlanif100
 Dest 2001:DB8:1::1/32,
     via 2000::1, cost  2, tag 0, RA, 6 Sec
 Dest 2001:DB8:1::2/64,
     via 2000::1, cost  2, tag 0, RA, 6 Sec
 Dest 2001:DB8:1::3/64,
     via 2000::1, cost  2, tag 0, RA, 6 Sec
 Dest 2001:DB8:1::4/64,
     via 2000::1, cost  2, tag 0, RA, 6 Sec
```

Table 7-21 Description of the display ripng route command output

Item	Description
Route Flags	Route tag. The first character indicates the type of the route, namely, a RIPng route; the second character indicates the status of the route: ● RA: The RIPng route is in aging state. ● RG: The RIPng route is in garbage collection state.
Peer	Neighbor connecting to the interface.
Dest	Destination IPv6 address.
via	Next-hop IPv6 address.
cost	Cost of a route.
tag	Route tag.
Sec	Time during which a route remains in the state indicated by the route tag.

7.3.12 display ripng statistics interface

Function

The **display ripng statistics interface** command displays statistics about packets received and sent by interfaces in a RIPng process.

Format

display ripng *process-id* **statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ipv6-address*] }

Parameters

Parameter	Description	Value
process-id	Displays statistics on the interface of the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
all	Displays statistics on all interfaces.	-
interface-type interface-number	Displays statistics on the specified interface.	-
verbose	Displays detailed statistics.	-

Parameter	Description	Value
neighbor *neighbor-ipv6-address*	Displays statistics about the specified neighbor.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the configuration and operating status of RIPng. The information is helpful in fault location and configuration verification.

Example

Display statistics about VLANIF100 of RIPng process 1.

```
<HUAWEI> display ripng 1 statistics interface vlanif 100
Vlanif100(FE80::2E0:B9FF:FE7F:1A01)
Statistical information         Last min     Last 5 min    Total
------------------------------------------------------------------
Periodic updates sent           5            23            259
Triggered updates sent          5            30            408
Response packets sent           10           34            434
Response packets received       15           38            467
Response packets ignored        0            0             0
Request packets sent            1            3             8
Request packets received        4            20            40
Request packets ignored         0            0             0
Bad packets received            0            0             0
Routes received                 2            10            0
Routes sent                     1            4             4
Bad routes received             0            0             0
Packets send failed             0            0             0
```

Table 7-22 Description of the display ripng statistics interface command output

Item	Description
Statistical information	Packet type.
Last min	Statistics within the last minute.
Last 5 min	Statistics within the last 5 minutes.
Total	Total statistics.
Periodic updates sent	Number of periodically sent Update packets.
Triggered updates sent	Number of triggered sent Update packets.
Response packets sent	Number of sent RIPng Response packets.

Item	Description
Response packets received	Number of received RIPng Response packets.
Response packets ignored	Number of ignored RIPng Response packets.
Request packets sent	Number of sent RIPng Request packets.
Request packets received	Number of received RIPng Request packets.
Request packets ignored	Number of ignored RIPng Request packets.
Bad packets received	Number of received packets that cannot be parsed.
Bad routes received	Number of received routes that cannot be parsed.
Routes received	Number of received routes.
Routes sent	Number of sent routes.
Packets send failed	Number of RIPng packets that fail to be sent.

7.3.13 filter-policy export (RIPng)

Function

The **filter-policy export** command specifies the filtering policy for sent routes.

The **undo filter-policy export** command cancels the configuration.

By default, no filtering policy is configured.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL, which is case sensitive.	The name is a string of 1 to 64 case-sensitive characters without spaces.

Parameter	Description	Value
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the name of a routing protocol from which routes are imported.	The value can be **bgp**, **direct**, **isis**, **unr**, **ripng**, **static** or **ospfv3**.
process-id	Specifies the process ID of **IS-IS**, **RIPng** or **OSPFv3**.	The value is an integer that ranges from 1 to 65535.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

In some cases, you need to precisely control the advertisement of RIPng routes to meet complicated network requirements. RIPng can use an IPv6 prefix list, route policy and ACL to filter imported routes, allowing only the routes matching the IPv6 prefix list, route policy and ACL to be advertised to RIPng neighbors.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Use IPv6 prefix list **Filter2** to filter the RIPng Update packets that need to be advertised.

```
<HUAWEI> system-view
[HUAWEI] ripng 100
[HUAWEI-ripng-100] filter-policy ipv6-prefix Filter2 export
```

7.3.14 filter-policy import (RIPng)

Function

The **filter-policy import** command specifies the filtering policy for received routes. Only the routes that match the filtering policy can be received.

The **undo filter-policy import** command cancels the configuration.

By default, no filtering policy is configured.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL, which is case sensitive.	The name is a string of 1 to 64 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

In some cases, you need to precisely control the receiving of RIPng routes to meet complicated network requirements. RIPng can use an IPv6 prefix list, route policy and ACL to filter received RIPng routes, allowing only the routes matching the IPv6 prefix list, route policy and ACL to be added to RIPng routing tables.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Use IPv6 prefix list **Filter1** to filter received RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ripng 1
[HUAWEI-ripng-1] filter-policy ipv6-prefix Filter1 import
```

7.3.15 import-route (RIPng)

Function

The **import-route** command imports routes.

The **undo import-route** command cancels importing routes.

By default, no route is imported.

Format

import-route { { **ripng** | **isis** | **ospfv3** } [*process-id*] | **bgp** [**permit-ibgp**] | **unr** | **direct** | **static** } [[**cost** *cost* | **inherit-cost**] | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

Parameters

Parameter	Description	Value
protocol	Specifies the routing protocol from which routes are imported.	The value can be **direct**, **static**, **ripng**, **isis**, **unr**, **bgp**, or **ospfv3**.
ripng	Imports RIPng routes.	-
isis	Imports IS-IS routes.	-
ospfv3	Imports OSPFv3 routes.	-
process-id	Specifies the process ID of imported routes.	The value is an integer that ranges from 1 to 65535.
bgp	Imports BGP routes.	-

Parameter	Description	Value
permit-ibgp	Imports IBGP routes in a public network instance. **NOTE** - Import of IBGP routes in RIPng process can lead to routing loops. Administrators should take care of routing loops before configuring **permit-ibgp**.	-
unr	Imports UNR routes.	-
direct	Imports direct routes.	-
static	Imports static routes.	-
cost *cost*	Specifies the cost of imported routes. If no cost is specified, the default cost configured using the **default-cost (RIPng)** command is used.	The value is an integer that ranges from 0 to 15.
inherit-cost	Specifies to retain the original cost of the imported route.	-
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

You can configure a route-policy to allow RIPng to import only the routes that match the rout-policy and set attributes for imported routes.

You can run one of the following commands to set the cost of imported routes. The following commands are listed in descending order of priorities.

- Run the **apply cost** command to set the cost of routes.
- Run the **import-route** (RIPng view) command to set the cost of imported routes.
- Run the **default-cost (RIPng)** command to set the default cost of imported routes.

NOTE

After the **import-route direct** command is executed, routes to the network segment where the IPv6 address of the management interface belongs are also imported in the RIPng routing table. Therefore, use this command with caution.

Example

Import routes from IS-IS process 7 and set the cost of imported routes to 7.

```
<HUAWEI> system-view
[HUAWEI] ripng 1
[HUAWEI-ripng-1] import-route isis 7 cost 7
```

Import the IBGP routes matching route-policy **abc** to RIPng process 1 and set the cost of imported routes to 5.

```
<HUAWEI> system-view
[HUAWEI] ripng 1
[HUAWEI-ripng-1] import-route bgp permit-ibgp cost 5 route-policy abc
```

7.3.16 ipsec sa (RIPng)

Function

The **ipsec sa** command enables Internet Protocol Security (IPSec) authentication in a RIPng process.

The **undo ipsec sa** command disables IPSec authentication in a RIPng process.

By default, IPSec authentication is disabled in a RIPng process.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ipsec sa *sa-name*

undo ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of a Security Association (SA)	The value is an existing SA name.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ipsec sa** command enables IPSec authentication in a RIPng process. IPSec authenticates received and sent RIPng packets by using the specified SA (including the security algorithm and key). This improves the security of the RIPng network.

If the **ipsec sa** command is run for a RIPng process, all packets of the process will be authenticated by using the SA specified in the command. This means that the IPSec authentication configuration takes effect on all interfaces in the RIPng process.

If IPSec authentication needs to be enabled only on a certain RIPng interface, run the **ripng ipsec sa** command in the view of the interface.

Prerequisites

An IPSec SA has been configured.

Precaution

The **ripng ipsec sa** command takes precedence over the **ipsec sa** command. If both commands are run in respective views and different SA names are specified, only the configuration of the **ripng ipsec sa** command takes effect.

Example

Enable IPSec in a RIPng process and specify sa1 as the SA name.

```
<HUAWEI> system-view
[HUAWEI] ripng 1
[HUAWEI-ripng-1] ipsec sa sa1
```

7.3.17 maximum load-balancing (RIPng)

Function

The **maximum load-balancing** command configures the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the maximum number of equal-cost routes is 8.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

maximum load-balancing *number*

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes for load balancing.	The value is an integer that ranges from 1 to 8. The default value is 8.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

If there are multiple links on the network, you can set the maximum number of equal-cost routes for load balancing. This prevents some links from being heavily loaded and improves network resource efficiency.

Example

Set the maximum number of equal-cost routes to 4.

```
<HUAWEI> system-view
[HUAWEI] ripng 1
[HUAWEI-ripng-1] maximum load-balancing 4
```

7.3.18 preference (RIPng)

Function

The **preference** command specifies the preference for RIPng routes.

The **undo preference** command restores the default setting.

By default, the preference of RIPng routes is 100.

Format

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Parameters

Parameter	Description	Value
preference	Specifies the preference of RIPng routes.	The value is an integer that ranges from 1 to 255.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

A smaller value indicates a higher preference. To make RIPng routes take precedence over other IGP routes, set a smaller preference value for RIPng routes. The preference values also determine which routing protocol's routes are optimal routes in an IPv6 routing table.

Example

Set the preference of RIPng routes to 120.

```
<HUAWEI> system-view
[HUAWEI] ripng 100
[HUAWEI-ripng-100] preference 120
```

Set the preference of the RIPng routes matching route-policy **policy1** to 60.

```
<HUAWEI> system-view
```

```
[HUAWEI] ripng 100
[HUAWEI-ripng-100] preference route-policy policy1 60
```

7.3.19 reset ripng statistics

Function

The **reset ripng statistics** command clears statistics in a specified RIPng process.

Format

reset ripng *process-id* **statistics** [**interface** { **all** | *interface-type interface-number* [**neighbor** *neighbor-ipv6-address*] }]

Parameters

Parameter	Description	Value
process-id	Specifies a RIPng process ID.	The value is an integer that ranges from 1 to 65535.
interface all	Clears statistics on all interfaces.	-
interface *interface-type interface-number*	Clears statistics on the specified interface.	-
neighbor *neighbor-ipv6-address*	Clears statistics in the RIPng process with the specified neighbor.	The value is a 32-digit hexadecimal number, in the common format of X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use the **reset ripng statistics** command in the user view to clear statistics in a specified RIPng process and re-collect statistics for debugging.

NOTICE

Statistics about a RIPng process cannot be restored after being cleared. So, exercise caution when using this command.

Example

Clear statistics on all the interfaces in RIPng process 100.

```
<HUAWEI> reset ripng 100 statistics interface all
Warning:The RIPNG statistics will be reset. Continue? [Y/N] y
```

7.3.20 ripng

Function

The **ripng** command creates a RIPng process.

The **undo ripng** command deletes a RIPng process.

By default, no RIPng process is created.

Format

ripng [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ripng *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies a RIPng process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring RIPng functions, run the **ripng** command to create a RIPng process.

When a RIPng process is deleted, the **ripng enable** command needs to be run again on interfaces.

Example

Create a specified RIPng process.

```
<HUAWEI> system-view
[HUAWEI] ripng 100
```

```
[HUAWEI-ripng-100]
```

7.3.21 ripng default-route

Function

The **ripng default-route** command generates a default route to the RIPng routing domain.

The **undo ripng default-route** command disables advertising RIPng default routes and forwarding IPv6 default routes.

By default, there is no default route in the RIPng routing domain.

Format

ripng default-route { **only** | **originate** } [**cost** *cost*]

undo ripng default-route

Parameters

Parameter	Description	Value
only	Advertises only IPv6 default routes (::/0) and suppresses the advertisement of other routes.	-
originate	Advertises IPv6 default routes (::/0) without affecting the advertisement of other routes.	-
cost *cost*	Specifies the cost of default routes.	The value is an integer that ranges from 0 to 15. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The generated default RIPng route is forcibly advertised in an Update packet through the specified interface, regardless of whether this route already exists in the IPv6 routing table.

This command can take effect only after IPv6 is enabled for the interface by the **ipv6 enable** command.

Example

Advertise only default routes in Update packets through an interface.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng default-route only
```

Advertise only default routes in Update packets through an interface.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng default-route only
```

Advertise default routes together with other routes in Update packets through an interface.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng default-route originate
```

Advertise default routes together with other routes in Update packets through an interface.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng default-route originate
```

7.3.22 ripng enable

Function

The **ripng enable** command enables RIPng on an interface.

The **undo ripng** command disables RIPng on an interface.

By default, RIPng process is disabled.

Format

ripng *process-id* **enable**

undo ripng

Parameters

Parameter	Description	Value
process-id	Specifies a RIPng process ID.	The value is an integer that ranges from 1 to 65535.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command can take effect only after IPv6 is enabled for the RIPng process and interfaces.

Example

Enable RIPng process 100 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ripng 100
[HUAWEI-ripng-100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address fc00:0:0:1::1/64
[HUAWEI-Vlanif100] ripng 100 enable
```

Enable RIPng process 100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ripng 100
[HUAWEI-ripng-100] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00:0:0:1::1/64
[HUAWEI-GigabitEthernet0/0/1] ripng 100 enable
```

7.3.23 ripng input

Function

The **ripng input** command enables the specified interface to receive RIPng packets.

The **undo ripng input** command disables the specified interface from receiving RIPng packets.

By default, interfaces can receive RIPng packets.

Format

ripng input

undo ripng input

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a device running RIPng is connected to a network running other routing protocols, you can run the **undo ripng input** command on the interface that connects the device to the network to prevent the interface from receiving RIPng packets from the network.

Example

Disable VLANIF100 interface to receive RIPng packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo ripng input
```

7.3.24 ripng ipsec sa

Function

The **ripng ipsec sa** command enables Internet Protocol Security (IPSec) authentication on a RIPng interface.

The **undo ripng ipsec sa** command disables IPSec authentication on a RIPng interface.

By default, IPSec authentication is disabled on a RIPng interface.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ripng ipsec sa *sa-name*

undo ripng ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of a Security Association (SA).	The value is an existing SA name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ripng ipsec sa** command enables IPSec on a RIPng interface. IPSec authenticates received and sent RIPng packets by using the specified SA (including the security algorithm and key). This improves the security of the RIPng network.

The command can take effect only after IPv6 is enabled for the interface by the **ipv6 enable** command.

If the **ripng ipsec sa** command is run on an interface, all RIPng packets received and sent by the interface will be authenticated by using the SA specified in the command.

Prerequisites

An IPSec SA has been configured.

Precaution

The **ripng ipsec sa** command takes precedence over the **ipsec sa** command. If both commands are run in respective views and different SA names are specified, only the configuration of the **ripng ipsec sa** command takes effect.

Example

Enable IPSec authentication on a RIPng interface and specify sa3 as the SA name.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ripng ipsec sa sa3
```

7.3.25 ripng metricin

Function

The **ripng metricin** command sets the metric that is added to the RIPng route received by an interface.

The **undo ripng metricin** command restores the default metric added to a received RIPng route.

By default, an interface does not add the metric to a received RIPng route.

Format

ripng metricin *value*

undo ripng metricin

Parameters

Parameter	Description	Value
value	Specifies the value of the metric to be added to a received RIPng route.	The value is an integer that ranges from 0 to 15. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When an interface receives a valid RIPng route, the interface adds a metric to the route before adding the route to the routing table. The metric of this route is changed in the routing table. That is, increasing the metric of an interface also increases the metric of the RIPng route received by the interface.

Before running the **ripng metricin** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Set the metric that is added to a received RIPng route to 12.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng metricin 12
```

Set the metric that is added to a received RIPng route to 12.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng metricin 12
```

7.3.26 ripng metricout

Function

The **ripng metricout** command sets the metric that is added to the RIPng route sent by an interface.

The **undo ripng metricout** command restores the default setting.

By default, the metric that is added to the RIPng route sent by an interface is 1.

Format

ripng metricout { *value* | { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } *value1* }

undo ripng metricout

Parameters

Parameter	Description	Value
value	Specifies the metric added to a sent route.	The value is an integer that ranges from 1 to 15. The default value is 1.
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL.	The name is a string of 1 to 64 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
value1	Specifies the metric added to the route matching the IPv6 prefix list.	The value is an integer that ranges from 2 to 15.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

An interface adds a metric to a route before advertising the route. Therefore, increasing the metric of an interface also increases the metric of the RIPng routes sent by the interface. The metric of the route in the routing table, however, remains unchanged.

Before running the **ripng metricout** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Set the metric that is added to a route sent on an interface to 12.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng metricout 12
```

Set the metric that is added to a route sent on an interface to 12.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng metricout 12
```

Set the metric that is added to the RIPng route matching IPv6 prefix list **p1** to 12.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ip ipv6-prefix p1 permit fc00:0:0:1::1 128
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng metricout ipv6-prefix p1 12
```

7.3.27 ripng output

Function

The **ripng output** command enables an interface to send RIPng packets.

The **undo ripng output** command disables an interface from sending RIPng packets.

By default, an interface can send RIPng packets.

Format

ripng output

undo ripng output

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a device running RIPng is connected to a network running other routing protocols, you can run the **undo ripng output** command on the interface that connects the device to the network to prevent the interface from sending RIPng packets to the network.

Example

Disable VLANIF100 interface to send RIPng packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo ripng output
```

7.3.28 ripng pkt-transmit

Function

The **ripng pkt-transmit** command sets the interval for sending Update packets and the number of packets sent each time on a specified interface.

The **undo ripng pkt-transmit** command restores the default value.

By default, the interval for sending Update packets is 200 ms and the number of packets sent each time is 30 on the RIPng interface.

Format

ripng pkt-transmit { **interval** *interval* | **number** *pkt-count* } *

undo ripng pkt-transmit

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for sending Update packets.	The value is an integer that ranges from 50 to 500, in milliseconds. The default value is 200.
number *pkt-count*	Specifies the number of packets sent each time.	The value is an integer that ranges from 25 to 100. The default value is 30.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Running the **ripng pkt-transmit** command in the interface view as required can accurately control the interval for sending packets and the number of sent packets. RIPng performance is then improved.

Before running the **ripng pkt-transmit** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Set the interval for sending Update packets on VLANIF100 to 100 ms and the number of packets sent each time to 50.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng pkt-transmit interval 100 number 50
```

Set the interval for sending Update packets on GE0/0/1 to 100 ms and the number of packets sent each time to 50.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng pkt-transmit interval 100 number 50
```

7.3.29 ripng poison-reverse

Function

The **ripng poison-reverse** command enables poison reverse for RIPng.

The **undo ripng poison-reverse** command disables poison reverse for RIPng.

By default, poison reverse is disabled for RIPng.

Format

ripng poison-reverse

undo ripng poison-reverse

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After poison reverse is configured, the route learned from an interface is also sent to the neighboring device through the same interface. The metric of this route is set to 16, indicating that the route is unreachable.

When split horizon and poison reverse are configured on the same interface, only poison reverse takes effect.

Before running the **ripng poison-reverse** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Enable poison reverse for RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng poison-reverse
```

Enable poison reverse for RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng poison-reverse
```

Disable poison reverse for RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ripng poison-reverse
```

7.3.30 ripng split-horizon

Function

The **ripng split-horizon** command enables split horizon for RIPng.

The **undo ripng split-horizon** command disables split horizon for RIPng.

By default, split horizon is enabled except on the NBMA network.

Format

ripng split-horizon

undo ripng split-horizon

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After split horizon is enabled, a route is blocked if the route is advertised through the interface that learns the route. The split horizon mechanism avoids routing loops between adjacent neighbors.

When poison reverse and split horizon are configured on the same interface, only poison reverse takes effect.

Before running the **ripng split-horizon** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Enable split horizon for RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ripng split-horizon
```

Enable split horizon for RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ripng split-horizon
```

Disable split horizon for RIPng Update packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ripng split-horizon
```

7.3.31 ripng summary-address

Function

The **ripng summary-address** command configures a RIPng device to advertise summarized IPv6 addresses on an interface.

The **undo ripng summary-address** command deletes this configuration.

By default, a RIPng switch does not advertise summarized IPv6 addresses.

Format

ripng summary-address *ipv6-address prefix-length* [**avoid-feedback**]

undo ripng summary-address *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies a summarized IPv6 address.	The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
avoid-feedback	Disables an interface from learning the same summarized route.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If the prefix and prefix length of a route match the defined IPv6 prefix, the defined IPv6 prefix is advertised instead of the route. As a result, multiple routes are replaced by a single route that has a lower metric.

After the keyword **avoid-feedback** is specified, an interface no longer learns the summarized route with the same IP address as the advertised summarized IP address. This avoids routing loops.

This command can take effect only after IPv6 is enabled for the RIPng process and interfaces.

Example

Configure IPv6 address FC00:200::3EFF:FE11:6770 for VLANIF100, set the prefix length to 64 bits, and summarize the configured IPv6 address as an IPv6 address with prefix FC00:200::/35 in RIPng process 100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ripng 100
[HUAWEI-ripng-100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address fc00:200::3EFF:FE11:6770/64
```

```
[HUAWEI-Vlanif100] ripng 100 enable
[HUAWEI-Vlanif100] ripng summary-address fc00:200:: 35
```

Configure IPv6 address FC00:200::3EFF:FE11:6770 for GE0/0/1, set the prefix length to 64 bits, and summarize the configured IPv6 address as an IPv6 address with prefix FC00:200::/35 in RIPng process 100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ripng 100
[HUAWEI-ripng-100] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00:200::3EFF:FE11:6770/64
[HUAWEI-GigabitEthernet0/0/1] ripng 100 enable
[HUAWEI-GigabitEthernet0/0/1] ripng summary-address fc00:200:: 35
```

7.3.32 timers ripng

Function

The **timers ripng** command configures RIPng timers.

The **undo timers ripng** command restores the default values of timers.

By default, the interval for sending RIPng Update packets is 30s, the aging time of routes is 180s, and the time for deleting routes from an IPv6 routing table is 120s.

Format

timers ripng *update age garbage-collect*

undo timers ripng

Parameters

Parameter	Description	Value
update	Specifies the interval for sending Update packets. This parameter is the basic timing parameter of routing protocols.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 30 seconds.
age	Specifies the aging time of routes. The value of *age* must be at least three times the value of *update*. If no Update packet of a route is received within the aging time, the route becomes invalid (unreachable).	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 180 seconds.
garbage-collect	Specifies the time from when a route is found invalid until it is deleted from the routing table.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 120 seconds.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

The basic timing parameters of RIPng can be adjusted because RIPng adopts a distributed asynchronous routing algorithm. On the network, these parameters on switches need to be consistent with those on access servers.

The command can take effect only after the global IPv6 is enabled.

If the values of the preceding four timers are set improperly, route flapping occurs. The relationship of the values of the four timers is: *update* < *age* and *update* < *garbage-collect*. For example, if the update time is longer than the aging time, switches cannot inform neighbors on time if RIPng routes change during the update time.

Example

Set values for RIPng timers.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ripng 100
[HUAWEI-ripng-100] timers ripng 5 15 30
```

7.4 OSPF Configuration Commands

7.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.4.2 abr-summary (OSPF area)

Function

The **abr-summary** command configures route summarization on an area border router (ABR).

The **undo abr-summary** command disables route summarization on an ABR.

By default, route summarization is not configured on ABRs.

Format

abr-summary *ip-address mask* [**cost** { *cost* | **inherit-minimum** } | [**advertise** [**generate-null0-route**] | **not-advertise** | **generate-null0-route** [**advertise**]]] *

undo abr-summary *ip-address mask*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a summarized route.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address of the summarized route.	The value is in dotted decimal notation.
advertise | **not-advertise**	Indicates whether to advertise the summarized route. By default, the summarized route is advertised.	-
cost *cost*	Specifies the cost of the summarized route. By default, the highest cost of specific routes is used as the cost of the summarized route.	The value is an integer that ranges from 0 to 16777214.
inherit-minimum	Indicates that the smallest cost of specific routes is used as the cost of the summarized route.	-
generate-null0-route	Generates a blackhole route to prevent routing loops.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale OSPF network, route search speed may decrease due to a large routing table size. Route summarization can be configured to reduce the size of the routing table and simplify management.

Route summarization aggregates multiple routes with the same IP prefix into one. If a link connected to a device within a summarized IP address range alternates between Up and Down states, the link status change is not advertised to the devices outside that IP address range. This prevents route flapping and improves network stability.

When the ABR sends routing information to other areas, it originates Type 3 LSAs for each network segment. If any contiguous segments exist in this area, run the **abr-summary** command to summarize these segments into one. The ABR then sends just one summarized LSA, and no LSAs that belong to the summarized network segment specified by the command. Therefore, the routing table size is reduced, and switch performance is improved.

Prerequisites

The **network** command has been run to specify the segments that need to be summarized before configuring route summarization.

Precautions

- This command applies only to ABRs for intra-area route summarization. The **asbr-summary** command configures AS Boundary Routers (ASBRs) to summarize the routes imported by OSPF.
- Route summarization cannot be configured on ABRs in different areas of the same process.

Example

In OSPF 100 area 1, summarize routes in two network segments, 10.42.10.0 and 10.42.110.0, into one route 10.42.0.0, and advertise the summarized route to other areas.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] network 10.42.10.0 0.0.0.255
[HUAWEI-ospf-100-area-0.0.0.1] network 10.42.110.0 0.0.0.255
[HUAWEI-ospf-100-area-0.0.0.1] abr-summary 10.42.0.0 255.255.0.0
```

7.4.3 advertise mpls-lsr-id

Function

The **advertise mpls-lsr-id** command configures OSPF to advertise MPLS LSR IDs to multiple areas as intra-area routes.

The **undo advertise mpls-lsr-id** command cancels the configuration.

By default, OSPF does not advertise MPLS LSR IDs to multiple areas as intra-area routes.

NOTE

Only the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H support this command.

Format

advertise mpls-lsr-id [**cost** *cost*]

undo advertise mpls-lsr-id

Parameters

Parameter	Description	Value
cost *cost*	Specifies the cost of the advertised route.	The value is an integer that ranges from 0 to 65535. By default, it is 0.

Views

OSPF view

Usage Guidelines

Usage Scenario

The prerequisite of a valid tunnel is that an intra-area route to the egress is reachable. When an ABR serves as the egress of tunnels in two areas, OSPF considers that only one tunnel is valid, because there is only one intra-area route to the egress, namely the IP address of the ABR's loopback interface (used as an MPLS LSR ID for tunnel establishment). To the other areas, this route is an inter-area route. To allow the tunnels in both areas to take effect, run the **advertise mpls-lsr-id** command to configure OSPF to advertise the intra-area route to the MPLS LSR ID to all areas connected to this device.

Prerequisites

Before running this command, the **mpls te** command has been run to enable MPLS TE globally.

Configuration Impact

Running this command may have the following impacts:

- If the OSPF area where the local switch resides does not have the interface whose IP address is the MPLS LSR ID, the type of the OSPF routes (with the destination address being the MPLS LSR ID) on the other devices in this OSPF area will be changed from inter-area to intra-area, and the cost will also be changed.
- If an OSPF NSSA has the interface whose IP address is the MPLS LSR ID and the forwarding address of the NSSA LSAs advertised in this area is the MPLS LSR ID, the forwarding address of these NSSA LSAs will be changed and the NSSA LSAs will be re-advertised, thus causing route calculation.

Example

Configure OSPF to advertise MPLS LSR IDs to multiple areas as intra-area routes.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] advertise mpls-lsr-id
```

7.4.4 area (OSPF)

Function

The **area** command creates an OSPF area and displays the OSPF area view.

The **undo area** command deletes a specified area.

By default, the system does not creates any OSPF area.

Format

area *area-id*

undo area *area-id*

Parameters

Parameter	Description	Value
area-id	Specifies an area ID. The area with the *area-id* of 0 is the backbone area.	The value can be a decimal integer or in dotted decimal notation. When the value is an integer, the value ranges from 0 to 4294967295.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of devices increases with the expansion of a network. This leads to a large LSDB on every OSPF-enabled device on a large-scale network. Route flapping frequently occurs and as such, a large number of OSPF packets are transmitted on the network. This wastes bandwidth resources.

OSPF resolves this problem by partitioning an AS into different areas. An area is regarded as a logical group, and each group is identified by a unique area ID.

Configuration Impact

After OSPF partitions the AS into different areas, the functions of multiple devices in the same area, such as the timer, filter, and summarization, can be planned and configured uniformly in the area. Therefore, the size of the LSDB is reduced, and network performance is improved.

Prerequisites

An OSPF process has been started using the **ospf** command.

Precautions

- At the border of an area resides a switch instead of a link.
- A network segment or a link belongs to only one area. Specify the area to which each OSPF interface belongs.
- The backbone area is responsible for forwarding inter-area routing information. The routing information between the non-backbone areas must be forwarded through the backbone area.
- All non-backbone areas must maintain connectivity with the backbone area. The backbone area must also maintain connectivity within itself.

Example

Enter the view of an OSPF area.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 0
[HUAWEI-ospf-100-area-0.0.0.0]
```

7.4.5 asbr-summary (OSPF)

Function

The **asbr-summary** command configures an AS Boundary Router (ASBR) to summarize the routes imported by OSPF.

The **undo asbr-summary** command disables an ASBR from summarizing the routes imported by OSPF.

By default, ASBRs do not summarize the routes imported by OSPF.

Format

asbr-summary *ip-address mask* [[**not-advertise** | **generate-null0-route**] | **tag** *tag* | **cost** *cost* | **distribute-delay** *interval*] *

asbr-summary type nssa-trans-type-reference [**cost nssa-trans-cost-reference**]

undo asbr-summary type

undo asbr-summary *ip-address mask*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a summarized route.	The value is in dotted decimal notation.

Parameter	Description	Value
mask	Specifies the mask of the IP address of the summarized route.	The value is in dotted decimal notation.
not-advertise	Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised.	-
generate-null0-route	Generates a blackhole route to prevent routing loops.	-
tag *tag*	Specifies the tag of the summarized route.	The value is an integer that ranges from 0 to 4294967295. The default value is 1.
cost *cost*	Specifies the cost of the summarized route. By default, for Type 1 external routes, the cost of the summarized route is the highest cost of specific routes; for Type 2 external routes, the cost of the summarized route equals the highest cost of specific routes plus 1.	The value is an integer that ranges from 0 to 16777214.
distribute-delay *interval*	Specifies the delay in advertising the summarized route.	The value is an integer that ranges from 1 to 65535, in seconds.
type nssa-trans-type-reference	Enables OSPF to consider Type 5 LSAs that have been translated from Type 7 LSAs when it sets types for summary routes on ASBRs. By default, when OSPF sets types for summary routes on ASBRs, OSPF does not consider Type 5 LSAs that have been translated from Type 7 LSAs.	-

Parameter	Description	Value
cost nssa-trans-cost-reference	Enables OSPF to consider Type 5 LSAs that have been translated from Type 7 LSAs when it sets costs for summary routes on ASBRs. If the **asbr-summary type nssa-trans-type-reference cost nssa-trans-cost-reference** command is not run, OSPF does not consider Type 5 LSAs that have been translated from Type 7 LSAs when setting types and costs for summary routes on ASBRs.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale OSPF network, route search speed may decrease due to a large routing table size. Configure route summarization to reduce the routing table size and simplify management.

Route summarization aggregates multiple routes with the same IP prefix into one. If a link connected to a device within a summarized IP address range alternates between Up and Down states, the link status change is not advertised to the devices outside the IP address range. This prevents route flapping and improves network stability.

Imported routes with the same prefix can be summarized into one and advertised as one route using the **asbr-summary** command. Route summarization reduces routing information and routing table size, improving device performance.

After route summarization is implemented, if the local device:

- If a local router is an ASBR in an NSSA, the local router summarizes all imported Type 5 LSAs within the summary address range.
- If the local router is an ASBR in an NSSA, the local router summarizes all imported Type 7 LSAs within the summary address range.
- If the local router functions as both an ASBR and an ABR in an NSSA, the local router summarizes all imported Type 7 LSAs within the address range. It also summarizes the Type 5 LSAs that are translated from Type 7 LSAs.

Precautions

When a large number of routes are summarized, specify the **distribute-delay** parameter to set a delay in advertising the summarized routes. This ensures that the advertised summarized routes contain more valid routes and avoids network flapping and incorrect routing information.

Example

Configure route summarization for the imported routes.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 not-advertise tag 2 cost 100
```

Cancel route summarization for the imported routes.

```
[HUAWEI-ospf-100] undo asbr-summary 10.2.0.0 255.255.0.0
```

7.4.6 authentication-mode (OSPF area)

Function

The **authentication-mode** command sets an authentication mode and a password for an OSPF area.

The **undo authentication-mode** command cancels the authentication mode configured for an OSPF area.

By default, no authentication mode is configured.

Format

authentication-mode simple [**plain** *plain-text* | [**cipher**] *cipher-text*]

authentication-mode { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]

authentication-mode keychain *keychain-name*

undo authentication-mode

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
simple	Sets simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
plain	Sets a plaintext password. If this parameter is specified, you can only enter a plaintext password, which is then displayed in plain text when the configuration file is viewed. **NOTICE** If **plain** is specified, the password is saved in the configuration file in plain text. This carries security risks. You are advised to specify **cipher** to save the password in cipher text.	-
plain-text	Sets a plaintext password.	The value is a string of case-sensitive characters that can be letters or digits without spaces. In **simple** authentication, the value is a string of 1 to 8 characters. In **md5**, **hmac-md5** or **hmac-sha256** authentication, the value is a string of 1 to 255 characters.
cipher	Sets a ciphertext password. Either a plaintext or ciphertext password can be entered, and cipher text is displayed when the configuration file is viewed.	When **cipher** is configured, the password can only be entered in cipher text. Then, the password is displayed in cipher text in configuration files. MD5 authentication, HMAC-SHA256 authentication or HMAC-MD5 authentication defaults to use the password in cipher text.

Parameter	Description	Value
cipher-text	Specifies the ciphertext password.	The value is a string of case-sensitive characters that can be letters or digits without spaces. In **simple** authentication, the value is a string of 1 to 8 characters in plain text, or a string of 24 or 32 or 48 characters in cipher text. In **md5**, **hmac-sha256** or **hmac-md5** authentication, the value is a string of 1 to 255 characters in plain text, or a string of 20 to 392 characters in cipher text.
md5	Indicates MD5 authentication using the ciphertext password. **NOTICE** MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates HMAC MD5 authentication using the ciphertext password. **NOTICE** HMAC-MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates HMAC-SHA256 authentication.	-
key-id	Specifies authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, only the **HMAC-MD5**, **SM3**, and **HMAC-SHA256** algorithms can be used in OSPF.	-
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF authentication can be configured to improve network security to meet high security demands. When area authentication is used, interfaces on all devices in an area must have the same area authentication mode and the password.

Precautions

The priority of area authentication is lower than the priority of interface identification. The **ospf authentication-mode** command can be used to change the priority of interface authentication.

Example

Configure HMAC-SHA256 authentication for OSPF area 0.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
```

```
[HUAWEI-ospf-100] area 0
[HUAWEI-ospf-100-area-0.0.0.0] authentication-mode hmac-sha256
```

7.4.7 bandwidth-config enable

Function

The **bandwidth-config enable** command enables a device to calculate the cost of an OSPF interface based on the configured interface bandwidth.

The **undo bandwidth-config enable** command disables a device from calculating the cost of an OSPF interface based on the configured interface bandwidth.

By default, a device is not enabled to calculate the cost of an OSPF interface based on the configured interface bandwidth.

Format

bandwidth-config enable

undo bandwidth-config enable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

External factors may affect the physical bandwidth of a link and change the physical bandwidth of an interface, thereby deteriorating network performance. To enable a device to adjust and optimize the route selection rules, run the **bandwidth** *bandwidth* command in the OSPF interface to adjust the interface bandwidth and run the **bandwidth-config enable** command to enable the device to calculate the cost of an OSPF interface based on the configured interface bandwidth. The calculation formula is as follows: Cost of the interface = Bandwidth reference value/Interface bandwidth.

Precautions

- If the **bandwidth** command is not configured, the OSPF interface cost is calculated based on the physical bandwidth of the interface.
- If the **bandwidth-config enable** command is not configured, the OSPF interface cost is calculated based on the physical bandwidth of the interface.

Example

Enable a device to calculate the cost of an OSPF interface based on the configured interface bandwidth.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] bandwidth-config enable
```

7.4.8 bandwidth-reference (OSPF)

Function

The **bandwidth-reference** command sets a bandwidth reference value that is used to calculate interface costs.

The **undo bandwidth-reference** command restores the default bandwidth reference value.

The default bandwidth reference value is 100 Mbit/s.

Format

bandwidth-reference *value*

undo bandwidth-reference

Parameters

Parameter	Description	Value
value	Specifies a bandwidth reference value for link cost calculation.	The value is an integer ranging from 1 to 2147483648, in Mbit/s. The default value is 100 Mbit/s.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The calculation formula is as follows: Interface cost = Bandwidth reference value/ Interface bandwidth. The integer of the calculated result is the interface cost. If the calculated result is smaller than 1, the interface cost value is 1. If the **bandwidth-reference** command is executed to configure a new bandwidth reference value, the interface cost will be changed. As a result, OSPF will re-select routes.

The default bandwidth reference value is 100 Mbit/s. The interface cost value is 100000000 divided by the interface bandwidth value.

Precautions

- After the **bandwidth-reference** command is configured in a process view, bandwidth reference values of all interfaces in the process are changed to the specified value.
- If the **bandwidth-reference** command is run on an Eth-Trunk interface, the bandwidth of the Eth-Trunk interface is equal to the total bandwidth of all its member interfaces.

Example

Set the bandwidth reference value to 1000 Mbit/s.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] bandwidth-reference 1000
```

7.4.9 bfd all-interfaces (OSPF)

Function

The **bfd all-interfaces** command enables bidirectional forwarding detection (BFD) in an OSPF process and sets the parameter values of a BFD session.

The **undo bfd all-interfaces** command disables BFD in an OSPF process and restores the default parameter values of a BFD session.

By default, BFD is disabled in an OSPF process.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

bfd all-interfaces enable

undo bfd all-interfaces enable

bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } *

undo bfd all-interfaces { **min-rx-interval** | **min-tx-interval** | **detect-multiplier**| **frr-binding** } *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **frr-binding** parameter.

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Indicates the minimum interval at which BFD packets are received from the remote end.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *transmit-interval*	Indicates the minimum interval at which BFD packets are sent to the remote end.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Indicates the local detection multiplier.	The value is an integer ranging from 3 to 50. By default, it is 3.
frr-binding	Binds the BFD status to the link status of an interface.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device communicates with its neighbors, BFD can fast detect faults to minimize the fault impact on services.

You can bind a BFD session to an interface or an OSPF process. If a BFD session is bound to both an interface and an OSPF process, the BFD session bound to an interface takes precedence over that bound to an OSPF process.

Precautions

- *receive-interval* is negotiated based on the **min-rx-interval** value on the local end and the **min-tx-interval** value on the remote end. The local end uses the larger one between the **min-rx-interval** value on the local end and the **min-tx-interval** value on the remote end as the remote **min-tx-interval**. If the local end does not receive any BFD packets within the interval of *receive-interval* × *multiplier-value* (local detection multiplier), it declares that the remote end is unreachable.
- An OSPF device sets up BFD sessions with only the neighbors in Exstart state. Two ends can set up a BFD session only when the **bfd** command is run on both ends to configure BFD globally and the **bfd all-interfaces enable** command is run.
- The **bfd all-interfaces** command and the **ospf bfd block** command are mutually exclusive.

Example

Configure BFD in an OSPF process and set the minimum interval for sending BFD packets to 400 ms.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] bfd all-interfaces enable
[HUAWEI-ospf-1] bfd all-interfaces min-tx-interval 400
```

7.4.10 default (OSPF)

Function

The **default** command configures default parameters for OSPF-imported external routes. The parameters include the cost, type (Type 1 or Type 2), tag, and number of imported routes.

The **undo default** command restores the default setting.

By default, the default cost of the imported external routes is 1; the upper limit of the imported external routes is 2147483647; the type of the imported external routes is Type 2; the default tag value is 1.

Format

default { **cost** { *cost-value* | **inherit-metric** } | **limit** *limit* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **limit** | **tag** | **type** } *

Parameters

Parameter	Description	Value
cost *cost-value*	Specifies the default cost of the external routes imported by OSPF.	The value is an integer ranging from 0 to 16777214. By default, it is 1.
inherit-metric	Indicates that the cost of the imported route is the cost that the route itself carries. If no cost is specified, the default cost set using the **default** command is used.	-
limit *limit*	Specifies the default upper limit of the external routes to be imported within a given period.	The value is an integer ranging from 1 to 2147483647.
tag *tag*	Specifies the tag of the external routes.	The value is an integer ranging from 0 to 4294967295. By default, it is 1.
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. ● 1: Type 1 external route ● 2: Type 2 external route

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The imported external routes carry various parameters that can change the priorities and next hops of those routes in the OSPF routing table.

By setting default parameters for OSPF-imported external routes, you can change OSPF routing policies.

The route tag is used to identify protocol-related information. For example, it can be used to differentiate AS numbers when OSPF receives BGP routes. It also allows you to apply OSPF routing policies to tagged routes.

Follow-up Procedure

The priority of the **default (OSPF)** command is the lowest. Thus, ensure that no other commands are configured when configuring this command. Otherwise, this command cannot take effect.

Precautions

You can run any of the following commands to set a cost for an imported route. The following commands are listed in the descending order of priority.

- **apply cost**
- **import-route (OSPF)**
- **default (OSPF)**

Example

Set the default values for the cost, type, and tag of imported routes.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] default cost 10 tag 100 type 2
```

7.4.11 default-cost (OSPF Area)

Function

The **default-cost** command sets a cost for the Type3 default route that is transmitted to a stub or NSSA by OSPF.

The **undo default-cost** command restores the default setting.

By default, the cost of the Type3 default route transmitted to a stub or NSSA is 1.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Specifies the cost of the Type3 default route transmitted to a stub or NSSA by OSPF.	The value is an integer ranging from 0 to 16777214.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring a cost for a default route can change OSPF route selection, improving networking flexibility.

This command is applicable to area border routers (ABRs) connected to stubs or NSSAs.

Prerequisites

A default route exists in the local routing table.

Example

Set Area 1 as a stub area, and set the cost of the Type 3 default route transmitted to this stub area to 20.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] stub
[HUAWEI-ospf-100-area-0.0.0.1] default-cost 20
```

7.4.12 default-route-advertise (OSPF)

Function

The **default-route-advertise** command advertises default routes to a common OSPF area.

The **undo default-route-advertise** command disables advertisement of default routes to a common OSPF area.

By default, OSPF devices in a common OSPF area do not generate default routes.

Format

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name* [**match-any**]] *

default-route-advertise summary cost *cost*

undo default-route-advertise

Parameters

Parameter	Description	Value
always	Generates and advertises an LSA that describes the default route, regardless of whether there are active default routes of other OSPF processes in the routing table of the host. - If **always** is configured, the switch does not calculate the default routes from other switches. - If **always** is not configured, an LSA for advertising a default route can be generated only when there are active default routes of other OSPF processes in the routing table of the local device.	-
permit-calculate-other	Generates and advertises an ASE LSA that describes the default route only when there are active default routes of other OSPF processes in the routing table of the local device. The device still calculates the default routes from other devices. **NOTE** If neither **always** nor **permit-calculate-other** is configured, - When there are active default routes of other OSPF processes in the routing table of the local device, the device does not calculate the default routes from other devices. - When there are no active default routes of other OSPF processes in the routing table of the local device, the device still calculates the default routes from other devices.	-
cost *cost*	Specifies the cost of the ASE LSA.	The value is an integer that ranges from 0 to 16777214. The default value is 1.

Parameter	Description	Value
type *type*	Specifies the type of the external routes.	The value is 1 or 2. The default value is 2. ● 1: Type 1 external route ● 2: Type 2 external route
route-policy *route-policy-name*	Specifies the name of a routing policy. The device advertises default routes according to the parameters of the configured routing policy when there are matched default routes of other OSPF processes in the routing table of the device.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
summary	Advertises the Type 3 summary LSA of the specified default route. Before specifying this parameter, ensure that a VPN is enabled. Otherwise, routes cannot be advertised.	-
match-any	Indicates that a device matches the routing entry in the routing table against a routing policy and then advertises the default route according to the parameters set through the routing policy.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **import-route (OSPF)** command cannot be used to import a default route from another AS. Running the **default-route-advertise** command on an ASBR can advertise a non-OSPF default route in a common OSPF area.

If the ASBR has a default route, the **default-route-advertise** command enables the ASBR to advertise the default route 0.0.0.0 to the OSPF area.

If the ASBR has no default route, the **default-route-advertise always** command or the **default-route-advertise** command can be used:

- With **always** configured: The ASBR can advertise the default route 0.0.0.0 even if there is no default route. This allows the default route to remain in the routing table and prevents the ASBR from using a default route sent by another device.
- Without **always** configured: The ASBR generates an LSA. It describes a default route only when the local routing table contains an activated non-OSPF default route (except BGP route).

  If the local routing table contains an activated default BGP route, the default route can be injected to the OSPF routing table based on the following situations:
  - Whether the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command is run together with the **vpn-instance-capability simple** command:
    - If the two commands are executed together, to inject an activated default EBGP route into the OSPF routing table, run the **default-route-advertise** command. To inject an activated default IBGP route to the OSPF routing table, run the **import-route bgp permit-ibgp** command before you run the **default-route-advertise** command.
    - If only the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command is run, to inject an activated default EBGP or IBGP route into the OSPF routing table, run the **default-route-advertise** command.
  - If the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command is not run, to inject an activated default EBGP route into the OSPF routing table, run the **default-route-advertise** command. To inject an activated default IBGP route to the OSPF routing table, run the **import-route bgp permit-ibgp** command before you run the **default-route-advertise** command.

NOTICE

Injecting an IBGP route into the OSPF routing table may cause a routing loop. Exercise caution when you perform this step.

If a routing policy is configured with **match-any**, and multiple routes match the policy, a default LSA will be generated based on the optimal route. The principles for optimal route selection are as follows:

1. A route configured with **type** takes precedence over that not configured with **type**. A route configured with a smaller **type** value takes precedence over that configured with a larger **type** value.
2. A route configured with **cost** takes precedence over that not configured with **cost**. A route configured with a smaller **cost** value takes precedence over that configured with a larger **cost** value.
3. A route configured with **tag** takes precedence over that not configured with **tag**. A route configured with a smaller **tag** value takes precedence over that configured with a larger **tag** value.

Prerequisites

Before advertising a default route, OSPF compares the priorities of default routes in an OSPF area and then advertises a default route with the highest priority. If a static default route is configured on an OSPF device, check the priority of the static default route. The priority must be lower than that of the default route to be advertised by OSPF. This ensures that the default route advertised by OSPF will be added to the routing table of the OSPF device.

Configuration Impact

After the **default-route-advertise** command is configured on the ASBR, the ASBR will generate a Type 5 ASE LSA with a link state ID of 0.0.0.0 and mask of 0.0.0.0. In addition, it will advertise the ASE LSA in an entire OSPF area.

If a routing policy is configured, default routes are advertised based on the following principles:

- If a default route matches the routing policy, a default route is generated on an OSPF device based on the parameters configured in the routing policy. Parameters such as **cost**, **tag**, and **type** can be configured in the routing policy.
- If the default route does not match the routing policy, and **always** is configured, the default route is still advertised.
  - If **always** is not configured, the OSPF device will not advertise the default route.
  - If **always** is configured, OSPF devices will advertise the default route. In addition, only **always** configured in the **default-route-advertise** command takes effect on advertisement of default routes.

Precautions

In different OSPF areas, OSPF advertises default routes using different modes. This **default-route-advertise** command can be used to advertise default routes to a common OSPF area. In a stub, totally stub, or totally NSSA area, default routes are advertised automatically. In an NSSA, the **nssa default-route-advertise** command is used to advertise default routes.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the device advertises the default route as long as a default route that is not generated by the current OSPF process exists in the local routing table.

If the **default-route-advertise command** is used in multiple OSPF processes to generate default routes, routing loops tend to occur. To prevent this issue, you are advised to configure route-policies to filter routes so that default routes will not be learned from these OSPF processes.

Example

Configure an ASBR to advertise the ASE LSA of the default route to common OSPF areas when it has no default route.

```
<HUAWEI> system-view
```

```
[HUAWEI] ospf 1
[HUAWEI-ospf-1] default-route-advertise always
```

7.4.13 description (OSPF)

Function

The **description** command configures a description for an OSPF process.

The **undo description** command deletes the description.

By default, there is no description for any OSPF process.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an OSPF process.	The value is a string of 1 to 80 case-sensitive characters, spaces supported.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An OSPF process description helps identify special processes, facilitating network maintenance.

Configuration Impact

If the **description** command is run multiple times, the latest configuration overrides the previous one.

Example

Configure a description for an OSPF process.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] description this process contains 3 areas
```

7.4.14 description (OSPF Area)

Function

The **description** command configures a description for an OSPF area.

The **undo description** command deletes the description.

By default, there is no description for any OSPF area.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an OSPF area.	The value is a string of 1 to 80 case-sensitive characters, spaces supported.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

An OSPF area description helps identify special areas, facilitating network maintenance.

Example

Configure a description for OSPF area 1.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] description this is a stub area
```

7.4.15 display default-parameter ospf

Function

The **display default-parameter ospf** command displays the default OSPF configuration.

Format

display default-parameter ospf

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display default-parameter ospf** command to check the default OSPF configuration during OSPF initialization. After the OSPF configuration is modified, this command still displays the default OSPF configuration during OSPF initialization.

Example

Display the default OSPF configuration.

```
<HUAWEI> display default-parameter ospf
 Process View:
 -------------------------------------------------------
   Default Metric                                  : 1
   Default Tag                                     : 1
   Default Type                                    : 2
   SPF Intelligent-timer Max-interval(msec)      : 10000
   SPF Intelligent-timer Start-interval(msec)   : 500
   SPF Intelligent-timer Hold-interval(msec)    : 1000
   Lsa Maxage (sec)                               : 3600
   Lsa Refresh Time(sec)                          : 1800
   Lsa Maxagediff Interval (sec)                 : 900
   Minimum Lsa Arrival Interval(sec)             : 1
   Minimum Lsa Originate Interval(sec)           : 5
   Sham Link Cost                                  : 1
   VPN Domain ID                                   : 0
   VPN Router Tag                                  : 0
   Route Preference for Internal Routes          : 10
   Route Preference for External Routes          : 150
 -------------------------------------------------------

 Area View:
 -------------------------------------------------------
   Default Stub Cost                               : 1
 -------------------------------------------------------

 Interface View:
 -------------------------------------------------------
   P2P&Broadcast Hello Interval(sec)             : 10
   P2MP&NBMA Hello Interval(sec)                  : 30
   P2P&Broadcast Dead Interval(sec)              : 40
   P2MP&NBMA Dead Interval(sec)                   : 120
   Poll Interval(sec)                              : 120
   Router DR Priority                              : 1
   Retransmit Interval(sec)                        : 5
```

```
 Transmit Delay(sec)                   : 1
--------------------------------------------------------
```

Table 7-23 Description of the **display default-parameter ospf** command output

Item	Description
Process View	Process view.
Default Metric	Default metric of the imported external route.
Default Tag	Default tag value of the imported external route.
Default Type	Default type of the imported external route.
SPF Intelligent-timer Max-interval(msec)	Default maximum interval of SPF calculation.
SPF Intelligent-timer Start-interval(msec)	Default start interval of SPF calculation.
SPF Intelligent-timer Hold-interval(msec)	Default hold interval of SPF calculation.
Lsa Maxage(sec)	Default maximum age of the LSA.
Lsa Refresh Time(sec)	Default maximum interval for generating an LSA. If the LS age of the LSAs generated by the device reaches the LSA Refresh Time, a new instance must be generated for the LSAs.
Lsa Maxagediff Interval(sec)	Default value difference in the MaxAge fields of LSAs. If the value difference in the MaxAge fields of two LSAs is greater than MaxAgeDiff Interval, the two LSAs are considered to belong to different instances of the same LSA.
Minimum Lsa Arrival Interval(sec)	Default minimum interval for receiving the same LSA.
Minimum Lsa Originate Interval(sec)	Default minimum interval for sending the same LSA.
Sham Link Cost	Default cost of the sham link.
VPN Domain ID	Default domain ID of the VPN.
VPN Router Tag	Default router tag of the VPN.
Route Preference for Internal Routes	Default preference of the internal route.
Route Preference for External Routes	Default preference of the external route.
Area View	Area view.
Default Stub Cost	Default cost of a route in the stub area.

Item	Description
Interface View	Interface view.
P2P&Broadcast Hello Interval(sec)	Default interval for sending Hello packets on a P2P or broadcast network.
P2MP&NBMA Hello Interval(sec)	Default interval for sending Hello packets on a P2MP or NBMA network.
P2P&Broadcast Dead Interval(sec)	Default interval for declaring a neighbor to be Down after no Hello packets are received on a P2P or broadcast network.
P2MP&NBMA Dead Interval(sec)	Default interval for declaring a neighbor to be Down after no Hello packets are received on a P2MP or NBMA network.
Poll Interval(sec)	Default interval for the local device to send Hello packets to a neighbor in the Down state on the NBMA network. The value of Poll Interval is greater than the value of Hello Interval.
Router DR Priority	Default priority of the DR.
Retransmit Interval(sec)	Default interval for retransmitting packets.
Transmit Delay(sec)	Default estimated time for transmitting an LSU packet over this interface. LSAs in the LSU packet must have their age incremented by this amount before transmission.

7.4.16 display gtsm statistics

Function

The **display gtsm statistics** command displays GTSM statistics on a device.

Format

display gtsm statistics all

Parameters

Parameter	Description	Value
all	Displays GTSM statistics on a device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display gtsm statistics** command to view GTSM statistics, including the total number of BGP, BGPv6, OSPF, LDP, OSPFv3, and RIP packets, the number of packets that have passed, and the number of discarded packets on a device.

Example

Display GTSM statistics on the device.

```
<HUAWEI> display gtsm statistics all
GTSM Statistics Table
----------------------------------------------------------------
SlotId  Protocol  Total Counters  Drop Counters  Pass Counters
----------------------------------------------------------------
 0      BGP       0               0              0
 0      BGPv6     0               0              0
 0      OSPF      0               0              0
 0      LDP       0               0              0
 0      OSPFv3    0               0              0
 0      RIP       0               0              0
----------------------------------------------------------------
```

Table 7-24 Description of the **display gtsm statistics** command output

Item	Description
SlotId	Slot ID.
Protocol	Protocol type: ● Software-based forwarding: protocol differentiated, displaying BGP, BGPv6, OSPF, LDP, OSPFv3, or RIP ● Hardware-based forwarding: protocol undifferentiated, displaying -----
Total Counters	Total number of packets.
Drop Counters	Total number of dropped packets.
Pass Counters	Total number of packets that have passed.

7.4.17 display ospf abr-asbr

Function

The **display ospf abr-asbr** command displays information about the ABRs and ASBRs of OSPF.

Format

display ospf [*process-id*] **abr-asbr** [*router-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
router-id	Specifies the router ID of an ABR or ASBR.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An area border router (ABR) can belong to two or more areas. One of the areas must be a backbone area. An ABR is used to connect the backbone area and non-backbone areas. The connection with the backbone area can be physically or logically.

An AS boundary router (ASBR) exchanges routing information with other ASs. An ASBR may not reside at the boundary of an AS. It can be an internal device or an ABR. If an OSPF device imports external routes, the device is an ASBR.

This command can view information about the ABRs and ASBRs of OSPF.

Example

Display information about the ABRs and ASBRs of OSPF.

```
<HUAWEI> display ospf abr-asbr

        OSPF Process 1 with Router ID 1.1.1.1
               Routing Table to ABR and ASBR

 RtType      Destination       Area       Cost  Nexthop         Type
 Intra-area  10.10.10.11       0.0.0.0    1     10.2.0.3        ABR
```

Table 7-25 Description of the **display ospf abr-asbr** command output

Item	Description
RtType	Intra-area or inter-area router.
Destination	Router ID of the ABR or ASBR.
Area	Area ID.

Item	Description
Cost	Cost of the route from the local device to the ABR or ASBR.
NextHop	Next hop address through which packets are transmitted to the ABR or ASBR.
Type	ABR or ASBR.

7.4.18 display ospf asbr-summary

Function

The **display ospf asbr-summary** command displays information about OSPF route summarization.

Format

display ospf [*process-id*] **asbr-summary** [*ip-address mask*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
ip-address	Specifies the summary IP address.	The value is in dotted decimal notation.
mask	Specifies the mask of the summary IP address. If no IP address or mask is specified, summarization information of all the imported routes is displayed.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an AS is divided into areas, configuring route aggregation can reduce routing information transmitted between areas. This reduces the size of the routing table and improves route performance. After the **asbr-summary (OSPF)** command is run to configure OSPF route summarization on an ASBR, you can run the **display ospf asbr-summary** command to view information about OSPF route summarization on the ASBR.

Example

Display summarization information about all the imported OSPF routes.

```
<HUAWEI> display ospf asbr-summary
         OSPF Process 1 with Router ID 192.168.1.2
                 Summary Addresses
 Total summary address count: 1
                 Summary Address
 net         : 10.0.0.0
 mask         : 255.0.0.0
 tag         : 10
 status      : Advertise
 Cost        : 0 (Not Configured)
 delay       : 30 (Configured)
 The Count of Route is : 2
 Destination     Net Mask       Proto      Process   Type     Metric
 10.1.0.0        255.255.0.0     Static     1         2        10
 10.2.0.0        255.255.0.0     Static     1         2        10
```

Table 7-26 Description of the **display ospf asbr-summary** command output

Item	Description
Total summary address count	Number of routes that are being summarized through the **asbr-summary** command.
net	Network address of the summary route.
mask	Network mask of the summary route.
tag	Tag of the summary route.
status	Advertisement status of the summary route: ● Advertise: indicates that the summary route is advertised. ● DoNotAdvertise: indicates that the summary route is not advertised.
Cost	Cost of the summarized route.
delay	Delay for advertising the summary route.
The Count of Route is	Number of routes that are being summarized.
Destination	Destination address of the routes that are being summarized.
Net Mask	Mask of the routes that are being summarized.
Proto	Protocol of the routes that are being summarized.
Process	Process ID.

Item	Description
Type	Type of the imported AS external route, which can be Type 1 or Type 2.
Metric	Metric of the routes that are being summarized.

7.4.19 display ospf bfd session

Function

The **display ospf bfd session** command displays information about the BFD-enabled neighbor.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

display ospf [*process-id*] **bfd session** *interface-type interface-number* [*router-id*]

display ospf [*process-id*] **bfd session** { *router-id* | **all** }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the type and number of an interface.	-

Parameter	Description	Value
router-id	Specifies the router ID of the neighbor.	The value is in dotted decimal notation.
all	Indicates all the OSPF-enabled interfaces in the OSPF process.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A BFD session can be associated with OSPF to fast detect a link fault and notifies OSPF of the fault. This speeds up OSPF's response to the change of the network topology.

The **display ospf bfd session** command displays information about the BFD-enabled neighbor.

Example

Display information about the BFD-enabled neighbor.

```
<HUAWEI> display ospf bfd session all
          OSPF Process 1 with Router ID 10.3.3.3
  Area 0.0.0.0 interface 192.168.1.1(Vlanif100)'s BFD Sessions
 NeighborId:10.2.2.2          AreaId:0.0.0.0           Interface:Vlanif100
 BFDState:up                  rx    :1000              tx       :1000
 Multiplier:3                 BFD Local Dis:8198       LocalIpAdd:10.1.1.1
 RemoteIpAdd:10.1.1.2         Diagnostic Info:No diagnostic information
```

Table 7-27 Description of the **display ospf bfd session all** command output

Item	Description
NeighborId	Router ID of the neighbor.
AreaId	Area ID.
Interface	Interface through which the local device establishes a BFD session with the neighbor.
BFDState	BFD status: - up - down - unknown

Item	Description
rx	Negotiated minimum interval for receiving BFD packets.
tx	Negotiated minimum interval for sending BFD packets.
Multiplier	Remote detection multiplier.
BFD Local Dis	Local discriminator dynamically assigned by BFD.
LocalIpAdd	Local IP address.
RemoteIpAdd	Remote IP address.
Diagnostic Info	Diagnostic information: ● Init: indicates that the BFD session is in the Initiate state. ● Admin down: indicates that the **shutdown** command is run on the local BFD session. ● BFD global disable: indicates that BFD is not enabled globally. ● BFD session number exceed: indicates that the number of BFD sessions exceeds the limit. ● Detect down: indicates that the local link becomes Down. ● Receive admin down: indicates that the remote link becomes Down. ● BFD is in rearranging: indicates that the board of the BFD session changes, and the data of the BFD session is transferred to another board. ● No diagnostic information: indicates that no diagnostic information exists. ● No BFD packets were received: indicates that detection expires because no BFD packets are received within a specified period. ● administrator down event received: indicates that the device receives an event that the BFD session is set Down by the network administrator.

7.4.20 display ospf brief

Function

The **display ospf brief** command displays OSPF brief information.

Format

display ospf [*process-id*] **brief**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, brief information about all the OSPF processes is displayed.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In addition to OSPF brief information, running this command also displays the following information:

- Configured Router ID
- Configured VPN domain ID

When locating OSPF faults, you can run the **display ospf brief** command to obtain OSPF brief information. You can then analyze OSPF faults according to the brief information.

Example

Display OSPF brief information.

```
<HUAWEI> display ospf brief
          OSPF Process 1 with Router ID 10.5.5.5
                  OSPF Protocol Information

 RouterID: 10.5.5.5         Border Router:  AREA
 Multi-VPN-Instance is not enabled
 Opaque Capable
 Global DS-TE Mode: Non-Standard IETF Mode
 Graceful-restart capability: disabled
 Helper support capability  : enabled
        filter capability   : disabled
```

```
       policy capability   : strict lsa check, planned and un-planned
Applications Supported: MPLS Traffic-Engineering
Spf-schedule-interval: max 10000ms, start 500ms, hold 1000ms
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 99
RFC 1583 Compatible
Retransmission limitation is disabled
Import routes limitation is enabled, the maximal limitation value: 4294967295
Area Count: 3   Nssa Area Count: 0
ExChange/Loading Neighbors: 0
Process total up interface count: 1
Process valid up interface count: 0
Flush protect mode: false

Area: 0.0.0.0          (MPLS TE not enabled)
Authtype: None   Area flag: Normal
SPF scheduled Count: 94
ExChange/Loading Neighbors: 0
Router ID conflict state: Normal
Area interface up count: 1

Interface: 172.16.16.5 (Vlanif1001)
Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
Priority: 1
Designated Router: 172.16.16.2
Backup Designated Router: 172.16.16.5
Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1

Area: 0.0.0.1
Authtype: Simple   Area flag: Normal
SPF scheduled Count: 83
ExChange/Loading Neighbors: 0
Router ID conflict state: Normal
Area interface up count: 0

Area: 0.0.0.2
Authtype: None   Area flag: Normal
SPF scheduled Count: 81
ExChange/Loading Neighbors: 0
Router ID conflict state: Normal
Area interface up count: 0

Interface: 10.100.100.100 (LoopBack100)
Cost: 0       State: P-2-P     Type: P2P       MTU: 1500
Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

Table 7-28 Description of the **display ospf brief** command output

Item	Description
RouterID	Current router ID.
Border Router	Border router: ● AS: autonomous system border router (ASBR). ● AREA: area border router (ABR). ● NSSA: ABR of an NSSA.
Multi-VPN-Instance is not enabled	The current process does not support multi-VPN-instance.

Item	Description
Opaque Capable	Opaque-LSA capability is enabled. To enable the Opaque-LSA capability, run the **opaque-capability enable** command.
Global DS-TE Mode	Globally configured DS-TE mode: ● Non-Standard IETF Mode: The IETF mode is not supported. ● Standard IETF Mode: The IETF mode is supported.
Graceful-restart capability	Whether graceful restart is enabled: ● disabled: Graceful restart is disabled. ● planned only: Planned-GR is supported. ● un-planned: Unplanned-GR is supported. ● totally: Totally GR is supported. ● planned and un-planned: Planned-GR and unplanned-GR are supported. To enable the GR function, run the **graceful-restart (OSPF)** command.
Helper support capability	Whether the Helper mode is enabled: ● enabled: The Helper mode is enabled. ● not configured: The Helper mode is disabled. To configure a device as a GR helper, run the **graceful-restart helper-role (OSPF)** command.
filter capability	Whether the filtering rule of the Helper mode is enabled: ● ip-prefix: The IP prefix filtering rule of the Helper mode is enabled. ● acl-number: The basic ACL filtering rule of the Helper mode is enabled. ● acl-name: The named ACL filtering rule of the Helper mode is enabled. ● disabled: The filtering rule of the Helper mode is disabled.

Item	Description
policy capability	Whether a policy is configured for the Helper mode: ● strict lsa check: The Helper checks all LSAs. To prevent the Helper from checking AS external LSAs, run the **graceful-restart helper-role ignore-external-lsa** command. ● ignore external lsa check: The Helper does not check AS external LSAs. ● planned and un-planned: The Helper supports planned-GR and unplanned-GR. To configure the Helper to support only planned-GR, run the **graceful-restart helper-role planned-only** command. ● planned: The Helper supports only planned-GR.
Applications Supported: MPLS Traffic-Engineering	OSPF supports Traffic Engineering (TE).
Spf-schedule-interval	Interval for performing SPF calculation. To set the interval for OSPF to calculate routes, run the **spf-schedule-interval** command.
Route Preference	Preference of the default route.
ASE Route Preference	Priority of the external route.
Default ASE parameters	Default parameters of the external LSA. ● Metric: default metric of the external LSA. ● Tag: default tag of the external LSA. ● Type: default type of the external LSA.
SPF Computation Count	Number of times that SPF calculation is performed.
RFC 1583 Compatible	Whether RFC 1583 compatibility is enabled. To convert rules defined in RFC 2328 into rules defined in RFC 1583, run the **rfc1583 compatible** command.
Retransmission limitation is disabled	Retransmission limit is disabled. To enable retransmission limit and set the maximum number of retransmissions, run the **retransmission-limit** command.

Item	Description
Import routes limitation is enabled, the maximal limitation value	Maximum number of imported routes is restricted and that the maximum value is displayed.
Area Count	Number of areas in the current process.
Nssa Area Count	Number of NSSAs in the current process.
Process total up interface count	Number of interfaces that are up.
Process valid up interface count	Number of interfaces that are valid.
Flush protect mode	Whether master/slave board switching triggered by abnormal OSPF LSA aging is enabled: ● false: Master/Slave board switching triggered by abnormal OSPF LSA aging is disabled. ● true: Master/Slave board switching triggered by abnormal OSPF LSA aging is enabled.
ExChange/Loading Neighbors	Number of neighbors in the ExChange/Loading state.
Area	Information about each area in the current process, including ID of the current area in dotted decimal notation.
Authtype	Area authentication type, including none-authentication, simple authentication, MD5 authentication, HMAC-SHA256 authentication, and HMAC-MD5 authentication.
Area flag	Flag used to describe the area attributes, including Transit/Vlink/Stub/Nssa/Normal.
SPF scheduled Count	Number of times that SPF calculation is performed.
Interface	Interface information in the area.
Cost	Cost of an OSPF interface. To set the cost for an OSPF on an interface, run the **ospf cost** command.

Item	Description
State	Interface status: ● Down ● Waiting ● Loopback ● P-2-P ● DR ● BDR ● DROTHER DR and BDR DROTHER exist in only broadcast and NBMA networks, and P-2-P exists in only P2P and P2MP Vlinks.
Type	Interface type, including P2P, broadcast, NBMA, and P2MP.
MTU	MTU value of the interface.
Priority	Interface priority.
Designated Router	(Optional) the current interface is not the DR.
Backup Designated Router	(Optional) the current interface is not the BDR.
Timers	Interval of the timer.
Hello	Interval of the Hello timer. To set the interval for sending Hello packets on an interface, run the **ospf timer hello** command.
Dead	Interval of the Dead timer. To set the dead interval after which an interface considers its OSPF neighbor invalid, run the **ospf timer dead** command.
Poll	Interval of the Poll timer. To set the poll interval for sending Hello packets on NBMA networks, run the **ospf timer poll** command.
Retransmit	Interval of the Retransmit timer. To set the interval for retransmitting LSA on an interface, run the **ospf timer retransmit** command.

Item	Description
Transmit Delay	(Optional) delay for transmitting LSAs on the interface. To add the transmission delay to LSAs before they are sent by an interface, run the **ospf trans-delay** command.
Router ID conflict state	Status of the automatic recovery function. The value can be one of the following: ● Normal: The automatic recovery function is properly detecting router ID conflict. ● Wait select: The automatic recovery function delays defining a new router ID if the device starts after an unexpected delay (two hours by default). ● Selecting: The automatic recovery function restarts the OSPF process with the router ID and waits for the restarted OSPF process to take effect. ● RtrId Changed: The automatic recovery function determines whether router ID conflict occurs after the new router ID takes effect and returns to the Normal state if no new router ID conflict is detected. ● Suspend: If the maximum number of conflict times is reached, automatic recovery function does not define a new router ID any longer. The maximum number of conflict times is three by default.
Area interface up count	The number of interfaces up in the area.

7.4.21 display ospf cumulative

Function

The **display ospf cumulative** command displays OSPF statistics.

Format

display ospf [*process-id*] **cumulative**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, statistics of all the OSPF processes are displayed.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output helps you troubleshoot OSPF faults.

Example

Display OSPF statistics.

```
<HUAWEI> display ospf cumulative
          OSPF Process 1 with Router ID 10.1.1.1
                  Cumulations

  IO Statistics
             Type        Input     Output
            Hello           26         62
   DB Description            3          2
   Link-State Req            1          1
Link-State Update            5          5
   Link-State Ack            3          3
  ASE: 2  Checksum Sum: 233779
  LSAs originated by this router

  Router: 1
  Network: 0
  Sum-Net: 0
  Sum-Asbr: 0
  External: 3
  NSSA: 0
  Opq-Link: 0
  Opq-Area: 0
  Opq-As: 0
  LSAs Originated: 4  LSAs Received: 14

  Routing Table:
    Intra Area: 2  Inter Area: 0  ASE: 2

  Up Interface Cumulate: 2

      Neighbor Cumulate:
  =======================================================

      Neighbor cumulative data. (Process 1)
  -------------------------------------------------------
  Down:       0 Init:        0 Attempt:    0 2-Way:    0
```

```
Exstart:    0 Exchange:    0 Loading:    0 Full:     1
Retransmit Count: 0

    Neighbor cumulative data. (Total)
-------------------------------------------------------
Down:       0 Init:        0 Attempt:    0 2-Way:    0
Exstart:    0 Exchange:    0 Loading:    0 Full:     1
Retransmit Count: 0
```

Table 7-29 Description of the **display ospf cumulative** command output

Item	Description
IO Statistics	Statistics of the transmitted packets and LSAs.
Type	OSPF packet type.
Input	Number of received packets.
Output	Number of sent packets.
Hello	OSPF Hello packet.
DB Description	OSPF Database Description packet.
Link-State Req	OSPF Link State Request packet.
Link-State Update	OSPF Link State Update packet.
Link-State Ack	OSPF Link State Acknowledgement packet.
Checksum Sum	Checksum of the AS external LSA.
ASE	Number of ASE routes (If there are no ASE routes, **Disabled** is displayed.).
LSAs originated by this router	Detailed statistics of the transmitted LSAs.
Router	Router LSA.
Network	Network LSA.
Sum-Net	Type 3 summary LSA.
Sum-Asbr	Type 4 summary LSA.
External	AS external LSA.
NSSA	NSSA.
Opq-Link	Number of Type 9 Opaque LSAs.
Opq-Area	Number of Type 10 Opaque LSAs.
Opq-As	Number of Type 11 Opaque LSAs
LSAs Originated	Generated LSAs.
LSAs Received	Received LSAs.

Item	Description
Routing Table	Routing table.
Intra Area	Number of intra-area routes.
Inter Area	Number of inter-area routes.
Up Interface Cumulate	Statistics of up state interface.
Neighbor Cumulate	Statistics of neighbors.
Neighbor cumulative data	Detailed statistics of neighbors: ● Down ● Init ● Attempt ● 2-Way ● Exstart ● Exchange ● Loading ● Full
Retransmit Count	Total number of nodes in the retransmission list.

7.4.22 display ospf error

Function

The **display ospf error** command displays OSPF error information.

Format

display ospf [*process-id*] **error** [**lsa** | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, error information of all OSPF processes is displayed.	The value is an integer ranging from 1 to 65535.
lsa	Displays the OSPF LSA errors.	-

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating OSPF faults, you can run the **display ospf error** command to obtain OSPF error information. You can then analyze OSPF faults according to the OSPF error information.

Example

Display OSPF error information.

```
<HUAWEI> display ospf error
          OSPF Process 1 with Router ID 10.1.1.1
                  OSPF error statistics

General packet errors:
 0     : IP: received my own packet     0     : Bad packet
 0     : Bad version                    0     : Bad checksum
 0     : Bad area id                    0     : Drop on unnumbered interface
 1     : Bad virtual link               0     : Bad authentication type
 0     : Bad authentication key         0     : Packet too small
 0     : Packet size > ip length        0     : Transmit error
 0     : Interface down                 0     : Unknown neighbor
 0     : Bad net segment                0     : Extern option mismatch
 0     : Router id confusion            0     : Bad authentication sequence number

HELLO packet errors:
 0     : Netmask mismatch               0     : Hello timer mismatch
 0     : Dead timer mismatch            0     : Virtual neighbor unknown
 0     : NBMA neighbor unknown          0     : Invalid Source Address

DD packet errors:
 0     : Neighbor state low             0     : Unknown LSA type
 0     : MTU option mismatch

LS ACK packet errors:
 0     : Neighbor state low             0     : Unknown LSA type

LS REQ packet errors:
 0     : Neighbor state low             0     : Empty request
 0     : Bad request

LS UPD packet errors:
 0     : Neighbor state low             0     : Newer self-generate LSA
 0     : LSA checksum bad               0     : Received less recent LSA
 0     : Unknown LSA type

Opaque errors:
```

```
 0     : 9-out of flooding scope        0     : 10-out of flooding scope
 0     : 11-out of flooding scope       0     : Unknown TLV type

Retransmission for packet over Limitation errors:
 0     : Number for DD Packet           0     : Number for Update Packet
 0     : Number for Request Packet

Receive Grace LSA errors:
 0     : Number of invalid LSAs         0     : Number of policy failed LSAs
 0     : Number of wrong period LSAs

Configuration errors:
0     : Tunnel cost mistake
```

Table 7-30 Description of the **display ospf error** command output

Item	Description
General packet errors	Indicates general packet errors.
IP: received my own packet	Indicates that the packet sent by its own interface is received and therefore the packet is not processed.
Bad packet	Indicates that the parsed packet is incorrect, including the checksum of the length field.
Bad version	Indicates that the OSPF version is incorrect, that is, it is not version 2.
Bad checksum	Indicates that the OSPF checksum is incorrect.
Bad area id	Indicates that the area ID in the received packet does not match the local area ID. (Vlink can receive packets from only Area 0 and its own area.)
Drop on unnumbered interface	Indicates that the unnumbered rather than P2P interface receives packets (the interface must be of the P2P type).
Bad virtual link	Indicates that the Vlink receives invalid packets.
Bad authentication type	Indicates that packet authentication is incorrect. If the value of this field keeps increasing, the OSPF authentication types of the two devices that establish the neighbor relationship are inconsistent. In this case, run the **area-authentication-mode** command to configure the same authentication type for the two devices.
Bad authentication key	Packet authentication key is incorrect.
Packet too small	Indicates that the length of the received packet does not equal the sum of the IP header length and the packet length.
Packet size > ip length	Indicates that the length of the OSPF packet is greater than the permitted length of the IP packet.

Item	Description
Transmit error	Indicates that sending packets to the socket fails.
Interface down	Indicates the number of times that the OSPF interface goes Down.
Unknown neighbor	Indicates that OSPF packets are received from non-OSPF neighbors on NBMA networks, virtual links, and sham links.
HELLO packet errors	Indicates Hello packet errors.
Netmask mismatch	Indicates that the address mask does not match the local address mask.
Hello timer mismatch	Indicates that the Hello intervals on the two ends are inconsistent. If the value of this field keeps increasing, the value of the Hello timers on the two devices that establish the neighbor relationship are inconsistent. In this case, check the interface configurations of the two devices and run the **ospf timer hello** command to set the same value for the Hello timers.
Dead timer mismatch	Indicates that the Dead intervals on the two ends are inconsistent. If the value of this field keeps increasing, the values of the dead timers on the two devices that establish the neighbor relationship are inconsistent. In this case, check the interface configurations of the two devices and run the **ospf timer dead** command to set the same value for the dead timers.
Extern option mismatch	Indicates that the extension attributes of the Hello packets on the two ends are inconsistent. If the value of this field keeps increasing, the area types of the two devices that establish the neighbor relationship are inconsistent (the area type of one device is common area, and the area type of the other device is stub area or NSSA). In this case, configure the same area type for the two devices (in the OSPF area view, the **stub** command indicates the area type is stub and the **stub** command indicates the area type is nssa).
Bad net segment	The source address of received packets is not on the same network segment as the IP address of the interface that receives packets.
Router id confusion	Indicates that the router IDs on the two ends are the same.

Item	Description
Bad authentication sequence number	Indicates bad authentication sequence number errors.
Virtual neighbor unknown	Indicates that the router ID of the packet is inconsistent with that of the neighbor that is configured by the virtual link.
NBMA neighbor unknown	Indicates that the status of the NBMA neighbor is not active.
Invalid Source Address	Indicates that the source address of LSA is invalid.
DD packet errors	Indicates DD packet errors.
Neighbor state low	Indicates the following situations: ● A DD packet is received but its neighbor status is lower than 2-way. ● An LSR packet is received but its neighbor status is lower than Exchange. ● An LSU packet is received but its neighbor status is lower than Exchange. ● An LSAck packet is received but its neighbor status is lower than Exchange.
Unknown LSA type	Indicates the unknown LSA type.
MTU option mismatch	Indicates that the MTU check of the OSPF interface is enabled and the MTU of the DD packet received by the interface is greater than the MTU of the interface.
LS ACK packet errors	Indicates LSAck packet errors.
Bad ack	Indicates the number of times that incorrect LSAck packets are received.
Duplicate ack	Indicates the number of times that duplicate LSAck packets are received.
LS REQ packet errors	Indicates LSR packet errors.
Empty request	Indicates empty LSR packets.
Bad request	Indicates the BadRequest event in the protocol.
LS UPD packet errors	Indicates LSU packet errors.
Newer self-generate LSA	Indicates the number of new self-generated LSAs. This field is reserved for future use.
LSA checksum bad	Indicates that the LSA checksum is incorrect.
Received less recent LSA	Indicates that the LSA older than the local LSA is received.

Item	Description
Opaque errors	Indicates opaque errors.
9-out of flooding scope	Indicates the number of Type 9 LSAs that exceed the flooding scope.
10-out of flooding scope	Indicates the number of Type 10 LSAs that exceed the flooding scope.
11-out of flooding scope	Indicates the number of Type 11 LSAs that exceed the flooding scope.
Unknown TLV type	Indicates the unknown TLV type.
Retransmission for packet over Limitation errors	Indicates the number of times that retransmitting packets expires.
Number for DD Packet	Indicates the number of times that retransmitting DD packets expires.
Number for Update Packet	Indicates the number of times that retransmitting LSU packets expires.
Number for Request Packet	Indicates the number of times that retransmitting LSR packets expires.
Receive Grace LSA errors	Indicates the number of received incorrect Grace LSAs.
Number of invalid LSAs	Indicates the total number of invalid LSAs.
Number of policy failed LSAs	Indicates the total number of policy failed LSAs.
Number of wrong period LSAs	Indicates the total number of wrong period LSAs.
Configuration errors	Indicates configuration errors.
Tunnel cost mistake	Indicates the number of times that the cost of the OSPF tunnel interface is smaller than 1. This count increases by one each time the cost of the OSPF tunnel interface is smaller than one. If the cost is smaller than one, the cost is calculated as one.

Display the OSPF LSA errors.

```
<HUAWEI> display ospf error lsa
 OSPF Process  1  with Router ID 10.1.1.14

 Last Received Bad LSA Header
    LS Age             : 36
    Link State Type    : 0x0008
    Link State ID      : 0.0.1.66
    Advertising Router : 10.10.10.22
    LS Sequence Number : 0x80000002
    LS Checksum        : 0x00bd2e
    Length             : 96
```

```
  Interface          : Vlanif100
  Recv Time            : 2011-05-27 14:37:17
```

Table 7-31 Description of the display ospf error lsa command output

Item	Description
Last Received Bad LSA Header	Bad LSA information received last time.
LS Age	Aging time of the LSA.
Link State Type	LSA type.
Link State ID	LSA state ID.
Advertising Router	Router that advertises or generates LSAs.
LS Sequence Number	Sequence number in the LSA header.
LS Checksum	LSA checksum.
Length	Size of the LSA.
Interface	LSA receiving interface.
Recv Time	LSA receiving time.

7.4.23 display ospf global-statistics

Function

The **display ospf global-statistics** command displays global OSPF statistics. If no OSPF process ID is specified, brief information about all the OSPF processes is displayed.

Format

display ospf global-statistics { **process** *process-id* | **vpn-instance** *vpn-instance-name* | **public-instance** | **timewheel** | **brief** }

Parameters

Parameter	Description	Value
process *process-id*	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
public-instance	Displays the statistics of all the public network instances.	-
timewheel	Displays the number of updated or aged LSAs in different periods.	-
brief	Displays brief information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospf global-statistics** command to check global OSPF statistics for fault location.

Example

Display global OSPF statistics, including statistics of neighbors, processes, and instances.

```
<HUAWEI> display ospf global-statistics brief
  Neighbor cumulative data (OSPF total statistics):
  ---------------------------------------------------------
  Down:              0        Init:                 0      Attempt:     0    2-Way:     0
  Exstart:           0        Exchange:             0      Loading:     0    Full:   2400
  Instance Numer:     1        Process Number:        2
  HighSocketExpire:   27       HighSocketEmpty:  526275
  Total Neighbor Number:                   0
  Total Press:   LOW
```

Table 7-32 Description of the **display ospf global-statistics brief** command output

Item	Description
Neighbor cumulative data (OSPF total statistics)	Neighbor statistics.
Instance Number	Number of instances, including public network instances and VPN instances.
Process Number	Number of OSPF processes running on the device.
HighSocketExpire	Number of unprocessed messages in high-priority queues.
HighSocketEmpty	Number of processed messages in high-priority queues.

Item	Description
Total Neighbor Number	Total number of OSPF neighbors.
Total Press	Total pressure of the current service. In most cases, the Total Press field is **LOW**. If the number of retransmission timers or the number of LSAs being flooded in the OSPF processes exceeds a certain value (default 300), or the number of OSPF neighbors exceeds 300, the Total Press field is **HIGH**. If the number of retransmission timers and the number of LSAs being flooded in the OSPF processes fall below a certain value (default 300), or the number of OSPF neighbors falls below 300, the Total Press field is **LOW**.

Display global statistics of OSPF process 1.

```
<HUAWEI> display ospf global-statistics process 1
  OSPF 1 statistics data:
  -----------------------------------------
  LSA NUM of Flood cache:          0
  Packet NUM of FloodUpdt Hash:          0
  Packet NUM of Flood Queue:          0
```

Table 7-33 Description of the **display ospf global-statistics process 1** command output

Item	Description
LSA NUM of Flood cache	Number of LSAs being flooded in the OSPF process.
Packet NUM of FloodUpdt Hash	Number of Update packets waiting to be flooded in the OSPF process, and the total size of the Update packets does not reach the MTU.
Packet NUM of Flood Queue	Number of Update packets waiting to be flooded in the OSPF process, and the total size of the Update packets reaches the MTU.

Display OSPF time wheel information.

```
<HUAWEI> display ospf global-statistics timewheel
 ================== TimeWheel Info Begin ===================
 TimeWheel current index is 2845, datanode count is 8
 Bucket Number: 3596, Expiry time: 1306(s), Datanode Count: 0
 High expiry time: 0, Low expiry time 527742(s)
```

```
Bucket Number: 3597, Expiry time: 1307(s), Datanode Count: 0
High expiry time: 0, Low expiry time 527743(s)
Bucket Number: 3598, Expiry time: 1308(s), Datanode Count: 0
```

Table 7-34 Description of the **display ospf global-statistics timewheel** command output

Item	Description
TimeWheel current index	Current index of the time wheel.
datanode count	Total number of nodes in the time wheel.
Bucket Number	Total number of indexes of the time wheel.
Expiry time	Expiry time of the index.
High expiry time	High expiry time corresponding to the index in the time wheel after the system starts.
Low expiry time	Low expiry time corresponding to the index in the time wheel after the system starts.

7.4.24 display ospf graceful-restart

Function

The **display ospf graceful-restart** command displays the status of OSPF GR.

Format

display ospf [*process-id*] **graceful-restart** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about OSPF GR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospf graceful-restart** command to view details and statistics of the GR.

Example

Display OSPF GR information.

```
<HUAWEI> display ospf graceful-restart

         OSPF Process 1 with Router ID 10.1.1.1
 Graceful-restart capability     : enabled
 Graceful-restart support        : planned and un-planned, totally
 Helper-policy support           : planned and un-planned, strict lsa check
 Current GR state                : normal
 Graceful-restart period         : 120 seconds

 Number of neighbors under helper:
  Normal neighbors    : 0
  Virtual neighbors   : 0
  Sham-link neighbors : 0
  Total neighbors     : 0

 Number of restarting neighbors : 0

 Last exit reason:
  On graceful restart : successful exit
  On Helper           : none
```

Display detailed information about OSPF GR.

```
<HUAWEI> display ospf graceful-restart verbose

         OSPF Process 1 with Router ID 10.1.1.1
 Graceful-restart capability     : enabled
 Graceful-restart support        : planned and un-planned, totally
 Helper-policy support           : planned and un-planned, strict lsa check
 Current GR state                : normal
 Graceful-restart period         : 120 seconds

 Number of neighbors under helper:
  Normal neighbors    : 0
  Virtual neighbors   : 0
  Sham-link neighbors : 0
  Total neighbors     : 0
 Number of restarting neighbors : 0

 Last exit reason:
  On graceful restart : successful exit
  On Helper           : none

 All area count      : 1

                Area ID    : 0.0.0.0

 Authtype       : None     Area flag : Normal

 Normal interface count: 1

 Interface: 10.1.1.1 (Vlanif100)
 GR state : normal                  State: P-2-P          Type: P2P
 Last Helper Exit reason: none
 Neighbor count of this interface : 1

 Neighbor          IP address        GR state    Last Helper Exit reason
 10.2.2.2          10.1.1.2          Normal      none
```

Table 7-35 Description of the **display ospf graceful-restart** command output

Item	Description
Graceful-restart capability	Whether IETF GR is enabled: ● enabled ● disabled
Graceful-restart support	IETF GR mode that is supported currently: ● planned: indicates that only planned-GR is supported. ● planned and un-planned: indicates that both planned GR and unplanned GR are supported. ● totally: indicates that totally GR is supported. ● partial: indicates that partial GR is supported.
Helper-policy support	Policy that supports the Helper: ● planned: indicates that the Helper supports only planned GR. ● planned and un-planned: indicates the Helper supports both planned GR and unplanned GR. ● strict lsa check: indicates that the Helper supports strict external LSA check. ● ignore external lsa check: indicates that the Helper does not check external LSAs. ● never: indicates that the device does not support the Helper mode.
Current GR state	Current GR status: ● Normal: indicates that GR is in the Normal state. ● Under GR: indicates that the device enters the Restarter mode. ● Under Helper: indicates that the device enters the Helper mode.
Graceful-restart period	GR period.

Item	Description
Number of neighbors under helper	Number of neighbors in the Helper state: ● Normal neighbors: indicates the number of normal neighbors. ● Virtual neighbors: indicates the number of virtual neighbors. ● Sham-link neighbors: indicates the number of sham link neighbors. ● Total neighbors: indicates the total number of neighbors.
Number of restarting neighbors	Number of restarted devices displayed on the Helper.
Last exit reason	Reason why a device exits from GR last time: ● On graceful restart: indicates the reason that the Restarter exits from GR. ● On Helper: indicates the reason that the Helper exits from GR.
On graceful restart	Reason why the Restarter exits from GR: ● 1-way hello received: indicates that 1-way Hello packets are received. ● back-link check failed: indicates that the back link check fails. ● DR election fail: indicates that DR election fails. ● grace period expired: indicates that the GR period expires. ● interface state change: indicates that the interface state machine changes. ● none: indicates that the device never performs GR since startup. ● successful exit: indicates that the Restarter successfully exits from GR. ● two Grace-LSAs received: indicates that two Grace LSAs are received.

Item	Description
On Helper	Reason why the Helper exits from GR: ● flooding change LSA: indicates that the changed LSAs are received. ● grace period expired: indicates that the GR period expires. ● graceful restart unconfigured at process level: indicates that the GR function of the OSPF process is disabled. ● interface state change: indicates that the interface state machine changes. ● policy check failed for received grace LSA: indicates the policy that mismatches the Helper. ● received 1-way hello packet: indicates that 1-way Hello packets are received. ● received flushed grace LSA: indicates that flushed Grace LSAs are received. ● received multiple grace LSA: indicates that multiple Grace LSAs are received. ● neighbor reset: indicates that GR is disabled when neighbors are in the Helper mode. ● none: indicates that the device never enters the Helper mode since startup. ● successful exit: indicates that the Helper successfully exits from GR.
All area count	Number of areas in the process.
Area ID	Area ID.
Authtype	Authentication type.
Area flag	Area attributes: ● Normal ● NSSA ● Stub
Normal interface count	Number of interfaces in the area.
Interface	IP address of the interface.

Item	Description
GR state	GR status of the interface: - Normal: indicates that the device is in the Normal state. - Restarter: indicates that the device enters the Restarter mode. - Helper: indicates that the device enters the Helper mode.
State	Interface status: - P-2-P - DR - BDR - DROther - Waiting - Down
Type	Interface type: - P2P - P2MP - NBMA - Broadcast

Item	Description
Last Helper Exit reason	Reason why the neighbor exits from the Helper mode the last time: ● none: indicates that the device never enters the Helper mode since startup. ● successful exit: indicates that the neighbor successfully exits from the Helper mode. ● grace period expired: indicates that the GR period expires. ● received flushed grace LSA: indicates that flushed Grace LSAs are received. ● flooding change LSA: indicates that the changed LSAs are received. ● received multiple grace LSA: indicates that multiple Grace LSAs are received. ● received 1-way hello packet: indicates that 1-way Hello packets are received. ● policy check failed for received grace LSA: indicates the policy that mismatches the Helper. ● neighbor reset: indicates that the network topology changes after the **reset** command is run on the neighbor of the Helper. ● interface state change: indicates that the interface state machine changes. ● graceful restart unconfigured at process level: indicates that the neighbor is not configured with the GR function.
Neighbor count of this interface	Total number of neighbors of this interface.
Neighbor	Router ID of the neighbor.
IP address	IP address of the neighboring interface.
GR state	GR status of the neighbor: ● Normal: indicates that the neighbor is in the Normal state. ● Restarter: indicates that the neighbor enters the Restarter mode. ● Helper: indicates that the neighbor enters the Helper mode.

7.4.25 display ospf interface

Function

The **display ospf interface** command displays information about OSPF interfaces.

Format

display ospf [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
all	Displays information about all OSPF interfaces.	-
interface-type interface-number	Specifies the interface type and the interface number.	-
verbose	Displays verbose configuration information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ospf interface** command output displays the configuration and operating status of OSPF, which facilitate fault location and configuration verification.

Example

Display OSPF interface information.

```
<HUAWEI> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0         (MPLS TE not enabled)
 IP Address      Type         State    Cost  Pri    DR              BDR
 192.168.1.2     Broadcast    DR        1     1     192.168.1.2     192.168.1.3

 Area: 0.0.0.1         (MPLS TE not enabled)
```

```
IP Address      Type         State     Cost  Pri   DR             BDR
172.16.0.1      Broadcast    DR        1     1     172.16.0.1     172.16.0.2
```

Table 7-36 Description of the **display ospf interface** command output

Item	Description
Area	ID of the area to which the interface belongs.
IP Address	IP address of the interface (regardless of whether TE is enabled on the interface).
Type	Interface type: P2P, PTMP, broadcast, or NBMA.
State	Status of the interface, which is determined by the OSPF interface state machines: ● Down: The status of the interface is Down. If an interface is Down, the interface is unavailable and cannot be used to transmit traffic. ● Loopback: The interface connecting to the network on the device is in the Loopback state. The loopback interface cannot be used to transmit data but can collect interface information by performing the ICMP ping operation or bit error detection. ● Waiting: The device is determining the DR and BDR on the network. The DR or BDR election mechanism should not be implemented until the waiting period ends. This prevents unnecessary changes in the DR and BDR roles. ● P-2-P: The interface is connected to a P2P network or a virtual link. ● DROther: The device itself is not elected as the DR or BDR. Instead, another device connecting to the broadcast network or NBMA network is elected as the DR. The device starts to set up adjacency with the DR and BDR (if existing). ● BDR: The device functions as the BDR on the network, and will turn into a DR when the current DR fails. The device sets up adjacency with other devices that access the network. ● DR: The device functions as the DR on the network. The device sets up adjacency with other devices that access the network.
Cost	Cost of the interface.

Item	Description
Pri	Priority of the device interface during the DR and BDR election The greater the value, the higher the priority.
DR	DR of the network where the interface resides.
BDR	BDR of the network where the interface resides.
Timer Hello	Interval for sending Hello packets.

Display detailed information about an OSPF interface.

```
<HUAWEI> display ospf interface Vlanif 501 verbose

         OSPF Process 1 with Router ID 192.168.2.1
                 Interfaces


 Interface: 192.168.100.2 (Vlanif501)
 Cost: 1       State: BDR       Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 192.168.100.1
 Backup Designated Router: 192.168.100.2
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
  IO Statistics
             Type        Input     Output
            Hello           11         10
   DB Description            3          2
   Link-State Req            1          1
Link-State Update            4          3
   Link-State Ack            2          3
 ALLSPF GROUP
 ALLDR GROUP
 OpaqueId: 0   PrevState: Waiting
 Effective cost: 1, enabled by OSPF Protocol
 Suppress flapping peer: enable(flapping-count: 0, threshold: 10)
```

Table 7-37 Description of the **display ospf interface verbose** command output

Item	Description
IO Statistics	Statistics about received and sent OSPF packets.
Type	OSPF packet type.
Input	Number of OSPF packets that the interface receives.
Output	Number of OSPF packets sent by the interface.
DB Description	Statistics about received and sent OSPF DD packets.

Item	Description
Link-State Req	Statistics about received and sent OSPF LSR packets.
Link-State Update	Statistics about received and sent OSPF LSU packets.
Link-State Ack	Statistics about received and sent OSPF LSAck packets.
ALLSPF GROUP	ALLSPF GROUP that the interface joins.
ALLDR GROUP	ALLDR GROUP that the interface joins.
OpaqueId	Opaque ID of the interface.
PrevState	Previous state of the interface.
Effective cost	Effective cost of the interface: ● enabled by OSPF Protocol: default value or the one configured using the **ospf cost** command. ● enabled by RUI: RUI route cost. ● enabled by IGP_LDP: interface cost configured in LDP. ● enabled by BGP_IGP: interface cost configured in BGP. ● enabled by Tunnel: cost generated after a TE Tunnel is configured.

Item	Description

Suppress flapping peer	Status of OSPF neighbor relationship flapping suppression:
	● enable: OSPF neighbor relationship flapping suppression is enabled.
	– flapping-count: number of valid flapping_events
	If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count is incremented by 1. To change *detecting-interval*, run the **ospf suppress-flapping peer detecting-interval** *detecting-interval* command.
	– threshold: flapping suppression threshold
	When the flapping_count reaches or exceeds **threshold**, flapping suppression takes effect. To configure the threshold, run the **ospf suppress-flapping peer threshold** *threshold* command.
	● disable: OSPF neighbor relationship flapping suppression is disabled. In this case, the following information is displayed, without flapping-count or threshold:
	`Suppress flapping peer: disable`
	● hold-down: OSPF neighbor relationship flapping suppression works in Hold-down mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-down(start: 2016-01-02 09:58:41, remain-interval: 476 sec)`
	– start: time when the flapping suppression started
	– remain-interval: remaining time of the flapping suppression
	● hold-max-cost: OSPF neighbor relationship flapping suppression works in Hold-max-cost mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-max-cost(start: 2016-01-02 09:58:41, remain-interval: 476 sec)`

7.4.26 display ospf lsdb

Function

The **display ospf lsdb** command displays an OSPF Link State Database (LSDB).

Format

display ospf [*process-id*] **lsdb** [**brief**]

display ospf [*process-id*] **lsdb** [{ **router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as** } [*link-state-id*]] [**originate-router** [*advertising-router-id*] | **self-originate**] [**age** { **min-value** *min-age-value* | **max-value** *max-age-value* } *]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
brief	Displays brief information about the LSDB.	-
router	Displays information about the router LSA.	-
network	Displays information about the network LSA.	-
summary	Displays information about the network summary LSA.	-
asbr	Displays information about the ASBR summary LSA.	-
ase	Displays information about the AS external LSA.	-
nssa	Displays information about the status of external links in the NSSA.	-
opaque-link	Displays information about the opaque link LSA.	-
opaque-area	Displays information about the opaque area LSA.	-

Parameter	Description	Value
opaque-as	Displays information about the opaque AS LSA.	-
originate-router	Displays the LSA of the advertising router.	-
link-state-id	Specifies the ID of an LSA.	The value is an IP address in dotted decimal notation.
advertising-router-id	Specifies the router ID of the device that advertises the LSA.	The value is an IP address in dotted decimal notation.
self-originate	Displays information about the self-originated LSA.	-
age	Displays the LSAs that meet the age filtering rule.	-
min-value *min-age-value*	Displays information about only LSAs with the **age** value greater than or equal to the *min-age-value* value.	The value is an integer ranging from 0 to 3600.
max-value *max-age-value*	Displays information only about LSAs with the **age** value less than or equal to the *max-age-value* value.	The value is an integer ranging from 0 to 3600.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check information about the LSDB, run the **display ospf lsdb** command. You can choose to view:

- Brief information about the LSDB
- LSAs of a specified type
- LSAs of the originating device
- Locally originated LSAs

The command output helps you troubleshoot OSPF faults.

Example

Display information about the OSPF LSDB.

```
<HUAWEI> display ospf lsdb
         OSPF Process 1 with Router ID 10.1.1.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    10.1.1.1        10.1.1.1          1348  48    800007C9    10000
 Router    10.1.1.2        10.1.1.2          1078  60    80000654       0
 Network   192.168.10.1    192.168.10.1      1349  32    80000060       0

                 AS External Database
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 External  0.0.0.0         10.1.1.2          1743  36    800005FE       1
```

Table 7-38 Description of the **display ospf lsdb** command output

Item	Description
Area	Area whose LSDB information needs to be displayed.
Type	LSA type: Router, Network, Sum-Net, Sum-Asbr, NSSA, External, Opq-Link, Opq-Area, and Opq-As.
LinkState ID	Link State ID in the LSA header.
AdvRouter	Device that advertises or generates LSAs.
Age	Aging time of the LSA.
Len	Size of the LSA.
Sequence	Sequence number in the LSA header.
Metric	Metric.
AS External Database	LSDB that contains external LSAs.

Display brief information about the OSPF LSDB.

```
<HUAWEI> display ospf lsdb brief
        OSPF Process 1 with Router ID 10.1.1.1
                LS Database Statistics

 Area ID         Stub   Router   Network  S-Net   S-ASBR   Type-7   | Subtotal
 0.0.0.0         0      3        2        0       0        0        | 5
 Total           0      3        2        0       0        0        |
-----------------------------------------------------------------+---------
 Area ID         Opq-9  Opq-10                                   | Subtotal
 0.0.0.0         0      0                                        | 0
 Total           0      0                                        |
-----------------------------------------------------------------+---------
                 ASE    Opq-11                                   | Subtotal
 Total           0      0                                        | 0
-----------------------------------------------------------------+---------
                                                                 | Total
                                                                 | 5
```

Table 7-39 Description of the **display ospf lsdb brief** command output

Item	Description
Area ID	Area to which the device belongs.
Stub	Number of stub networks.
Router	Number of Router LSAs.
Network	Number of network LSAs.
S-Net	Number of Sum-Net LSAs.
S-ASBR	Number of Sum-Asbr LSAs.
Type-7	Number of Type 7 LSAs.
Opq-9	Number of Opq-Link LSAs.
Opq-10	Number of Opq-Area LSAs.
ASE	Number of ASE routes.
Opq-11	Number of Opq-As LSAs.
Subtotal	Total number of sub-items.
Total	Total quantity.

Display information about router LSAs in the LSDB.

```
<HUAWEI> display ospf lsdb router
          OSPF Process 1 with Router ID 10.1.1.1
                          Area: 0.0.0.0
                  Link State Database

  Type      : Router
  Ls id     : 10.2.2.2
  Adv rtr   : 10.2.2.2
  Ls age    : 52
  Len       : 48
  Options   :  E
  seq#      : 80000006
  chksum    : 0xbf5a
  Link count: 2
     Link ID: 10.2.1.2
     Data   : 10.2.1.2
     Link Type: TransNet
     Metric : 1
     Link ID: 10.2.2.2
     Data   : 255.255.255.255
     Link Type: StubNet
     Metric : 0
     Priority : Medium
```

Table 7-40 Description of the **display ospf lsdb router** command output

Item	Description
Ls id	Link State ID in the LSA header.

Item	Description
Adv rtr	Device that advertises or generates LSAs.
Ls age	Aging time of the LSA.
Len	Size of the LSA.
Options	Options field: - E: allows Flood AS-external-LSAs. - MC: forwards IP multicast packets. - N/P: processes Type-7 LSAs. - DC: processes the required links.
seq#	Sequence number, which is used to check the order of LSAs.
chksum	LSA checksum.
Link count	Number of links.
Link ID	Link ID of the router LSA, which is classified according to the link type. - If the type of link is **Point-to-Point**, **Link ID** indicates the router ID of a neighbor. - If the type of link is **TransNet**, **Link ID** indicates IP address of DR. - If the type of link is **Stub**, **Link ID** indicates IP address. - If the type of link is **Virtual Link**, **Link ID** indicates the router ID of a neighbor.
Data	Link data of the router LSA. - If the type of link is Point-to-Point, TransNet, or Virtual Link, **Data** indicates IP address. - If the type of link is Stub, **Data** indicates mask of IP address.
Link Type	Link type of the router LSA: P-2-P, TransNet, StubNet, or Virtual.
Metric	Link metric of the router LSA.

Item	Description
Priority	OSPF convergence priorities: - Critical: indicates that the convergence priority of OSPF routes is critical. - High: indicates that the convergence priority of OSPF routes is high. - Medium: indicates that the convergence priority of OSPF routes is medium. - Low: indicates that the convergence priority of OSPF routes is low.

Display information about network LSAs in the LSDB.

```
<HUAWEI> display ospf 1 lsdb network 10.1.1.1
         OSPF Process 1 with Router ID 10.1.1.1
                         Area: 0.0.0.0
                 Link State Database

  Type      : Network
  Ls id     : 10.1.1.1
  Adv rtr   : 10.1.1.1
  Ls age    : 167
  Len       : 32
  Options   :  E
  seq#      : 80000002
  chksum    : 0x3408
  Net mask  : 255.255.255.0

  Attached Router    10.2.2.2
  Attached Router    10.1.1.1
```

Table 7-41 Description of the **display ospf lsdb network** command output

Item	Description
Net mask	Network mask of the network LSA.
Attached Router	Device that is connected to the network.

Display information about network summary LSAs in the LSDB.

```
<HUAWEI> display ospf 1 lsdb summary 10.20.1.0
         OSPF Process 1 with Router ID 10.1.1.1
                   Area: 0.0.0.0
                 Link State Database

  Type      : Sum-Net
  Ls id     : 10.1.1.0
  Adv rtr   : 10.2.2.2
  Ls age    : 419
  Len       : 28
  Options   :  E
  seq#      : 80000001
  chksum    : 0x1d21
```

```
 Net mask  : 255.255.255.0
 Tos 0  metric: 1
 Priority  : Medium
```

Table 7-42 Description of the **display ospf lsdb summary** command output

Item	Description
Net mask	Network mask of the network summary LSA.
Tos	Type of service of the network summary LSA.
Metric	Metric or cost of the route from the advertising router to the network, which is carried in the network summary LSA.
Priority	OSPF convergence priorities: ● Critical: indicates that the convergence priority of OSPF routes is critical. ● High: indicates that the convergence priority of OSPF routes is high. ● Medium: indicates that the convergence priority of OSPF routes is medium. ● Low: indicates that the convergence priority of OSPF routes is low.

Display information about ASBR summary LSAs in the LSDB.

```
<HUAWEI> display ospf 1 lsdb asbr 10.2.2.2
          OSPF Process 1 with Router ID 10.1.1.1
                    Area: 0.0.0.2
                  Link State Database

 Type      : Sum-Asbr
 Ls id     : 10.2.2.2
 Adv rtr   : 10.1.1.1
 Ls age    : 90
 Len       : 28
 Options   :  E
 seq#      : 80000001
 chksum    : 0xec62
 Tos 0  metric: 1
```

Display information about AS external LSAs in the LSDB.

```
<HUAWEI> display ospf 100 lsdb ase 10.1.1.0
OSPF Process 1 with Router ID 10.1.1.1
Link State Database

 Type      : External
 Ls id     : 10.1.1.0
 Adv rtr   : 10.2.2.2
 Ls age    : 569
 Len       : 36
 Options   :  E
 seq#      : 80000002
 chksum    : 0x90d0
 Net mask  : 255.255.255.0
```

```
Tos 0  Metric: 1
E type    : 2
Forwarding Address : 0.0.0.0
Tag       : 1
Priority  : Medium
```

Table 7-43 Description of the **display ospf lsdb ase** command output

Item	Description
Net mask	Network mask of the ASE or NSSA LSA.
Tos	Type of service of the ASE or NSSA LSA.
Metric	Metric or cost of the route from the advertising router to the network, which is carried in the ASE or NSSA LSA.
E type	E type of the ASE or NSSA LSA.
Forwarding Address	Forwarding address of the ASE or NSSA LSA.
Tag	32-bit tag, which is carried in Type 5 and Type 7 LSAs to avoid routing loops
Priority	OSPF convergence priorities: ● Critical: indicates that the convergence priority of OSPF routes is critical. ● High: indicates that the convergence priority of OSPF routes is high. ● Medium: indicates that the convergence priority of OSPF routes is medium. ● Low: indicates that the convergence priority of OSPF routes is low.

Display information about NSSA external LSAs in the LSDB.

```
<HUAWEI> display ospf 1 lsdb nssa 192.168.1.0
         OSPF Process 1 with Router ID 10.1.1.1
                   Area: 0.0.0.1
                 Link State Database

  Type      : NSSA
  Ls id     : 10.1.1.0
  Adv rtr   : 10.2.2.2
  Ls age    : 521
  Len       : 36
  Options   : None
  seq#      : 80000005
  chksum    : 0x9ea7
  Net mask  : 255.255.255.0
  Tos 0  Metric: 1
  E type    : 2
  Forwarding Address : 10.1.1.2
  Tag       : 1
  Priority  : Medium
```

Display information about Opaque-link LSAs in the LSDB.

```
<HUAWEI> display ospf 1 lsdb opaque-link
          OSPF Process 1 with Router ID 10.1.1.1
Area: 0.0.0.0                                                    Link State Database
 Link State Database for interface 10.1.1.1 (Vlanif200) Type: Broadcast

  Type      : Opq-Link
  Ls id     : 10.0.0.0
  Adv rtr   : 10.2.2.2
  Ls age    : 12
  Len       : 44
  Options   :  E
  seq#      : 80000001
  chksum    : 0x9579
         Opaque type : 3, Opaque ID : 0
         Grace LSA TLV information:
         Grace Period        : 1800
         GR reason           : 1
         IP address          : 10.1.1.2
```

Table 7-44 Description of the **display ospf lsdb opaque-link** command output

Item	Description
Opaque type	Opaque-link LSA.
Opaque ID	Opaque ID of an Opaque-link LSA (Link state ID in the LSA header consists of Opaque type and Opaque ID.).
Grace LSA TLV information:	GR information.
Grace Period	GR waiting period.
GR reason	Cause of GR: ● 0: unknown ● 1: software ● 2: upgrade ● 3: switchover
IP address	Address of the interface that performs GR on the switch.

Display information about Opaque-area LSAs in the LSDB.

```
<HUAWEI> display ospf 1 lsdb opaque-area
OSPF Process 1 with Router ID 10.1.1.1
Area: 0.0.0.0                                                    Link State Database
  Type      : Opq-Area
  Ls id     : 10.0.0.1
  Adv rtr   : 10.1.1.1
  Ls age    : 639
  Len       : 200
  Options   :  E
  seq#      : 80000001
  chksum    : 0x2175
  Opaque Type: 1
  Opaque Id: 1
  Opaque lsa information:
```

```
00 02 00 b0 00 01 00 01 02 00 00 00 00 02 00 04
0a 01 01 01 00 03 00 04 0a 01 01 01 00 04 00 04
00 00 00 00 00 05 00 04 00 00 00 01 80 02 00 04
00 00 00 01 00 06 00 04 00 00 00 00 00 07 00 04
00 00 00 00 80 00 00 04 00 00 00 00 00 09 00 04
00 00 00 00 00 08 00 20 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 80 01 00 20 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 09
00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 04
00 01 00 01
```

7.4.27 display ospf mesh-group

Function

The **display ospf mesh-group** command displays brief information about OSPF mesh groups.

Format

display ospf [*process-id*] **mesh-group** [**brief**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no process ID is specified, brief information about mesh groups in all OSPF processes is displayed.	The value is an integer ranging from 1 to 65535.
brief	Displays brief information about mesh groups in each OSPF area.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When concurrent links exist between a switch and its neighbor, run the **mesh-group enable** command to enable the mesh group function and identify the mesh group using the router ID of the switch. When receiving LSAs, the switch will select a primary link to flood LSAs. The link interface does not flood in reverse. This avoids repeated flooding, reducing link load and saving resources.

Running the **display ospf mesh-group** command allows you to check brief information about mesh groups in a specified process in an OSPF area.

Example

Display brief information about OSPF mesh groups.

```
<HUAWEI> display ospf mesh-group

    OSPF Process 1 with Router ID 10.1.1.1
                  Mesh-Groups

Area 0.0.0.0
       Mesh-Group ID:10.2.2.2

    Interface              IP Address/Mask      Nbr State
    Vlanif100               10.11.10.202/24      Exchange
    Vlanif200               10.22.20.202/24      Loading
    Vlanif300               10.33.30.202/24      Full
    Count of Interface in this Mesh-Group: 1
    Count of Mesh-Group in this Area: 1
```

Table 7-45 Description of the **display ospf mesh-group** command output

Item	Description
Area	OSPF area.
Mesh-Group ID	Key ID of a mesh group, namely, the router ID of a neighbor.
Interface	Interface enabled with the mesh-group feature.
IP Address/Mask	IP address and mask of the interface enabled with the mesh-group feature.
Nbr State	Neighbor status on the interface.
Count of Interface in this Mesh-Group	Number of interfaces in the mesh group.
Count of Mesh-Group in this Area	Number of mesh groups in the area.

7.4.28 display ospf migp-routing

Function

The **display ospf migp-routing** command displays OSPF Multicast IGP (MIGP) routing information.

Format

display ospf [*process-id*] **migp-routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
mask	Specifies a subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
interface-type interface-number	Specifies the type and number of an interface.	-
nexthop *nexthop-address*	Displays the route with a specified next hop IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When both multicast and MPLS TE tunnels are configured on a network and the TE tunnels are configured with IGP Shortcut, the outbound interface that an IGP calculates for a route may be not a physical interface but a TE tunnel interface. Based on a unicast route to a multicast source address, a switch can send a Join message through a TE tunnel interface. In this case, devices spanned by the TE tunnel cannot detect the Join message so that they do not create any multicast forwarding entry.

To solve this problem, you can run the **local-mt enable** command to configure local multicast topology (MT). MT allows multicast routing entries to be created correctly.

If local MT is enabled and the outbound interface of the calculated route is a TE tunnel interface of IGP Shortcut type, the route management (RM) module creates a separate Multicast IGP (MIGP) routing table for the multicast protocol, calculates the physical outbound interface of the route, and adds the IP address of the physical outbound interface to the MIGP routing table.

Running the **display ospf migp-routing** command allows you to view the physical outbound interface of the route with the outbound interface of the TE tunnel interface. The physical outbound interface is OSPF routing information in the MIGP routing table.

Precautions

- Local MT supports only OSPF processes of public network instances.
- Local MT does not support forwarding adjacency (FA).

Example

Display OSPF MIGP routing information.

```
<HUAWEI> display ospf migp-routing
          OSPF Process 1 with Router ID 10.2.2.2
                   MIGP Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 192.168.3.0/24     4     Stub       10.0.1.1        10.5.5.5        0.0.0.0
 10.0.3.0/24        3     Transit    10.0.1.1        10.5.5.5        0.0.0.0

 Total Nets: 4
 Intra Area: 4  Inter Area: 0  ASE: 0  NSSA: 0
```

Table 7-46 Description of the **display ospf migp-routing** command output

Item	Description
Destination	Destination IP address.
Cost	Cost of the route to the destination address.
Type	Router types are as follows: - Inter-area: Indicates routes between areas. - Stub: indicates routes within an area, including routes advertised based on router LSAs, and direct routes to non-broadcast and non-NBMA networks. - Transit: indicates routes within an area, including routes advertised based on network LSAs.
NextHop	Next hop address to the destination address.
AdvRouter	Advertising router.
Area	Area ID.
Total Nets	Total number of networks in an area, between areas, in ASE areas, and in NSSAs.
Intra Area	Total number of intra-area routes (that is, stub routes and transit routes).
Inter Area	Total number of inter-area routes.
ASE	Total number of routes in the ASE area.

Item	Description
NSSA	Total number of routes in the NSSA.

Display OSPF MIGP routing information with the specified next hop address.

```
<HUAWEI> display ospf migp-routing nexthop 10.0.1.1
         OSPF Process 1 with Router ID 10.2.2.2

 Destination : 192.168.3.0/24
 AdverRouter : 10.5.5.5                  Area       : 0.0.0.0
 Cost        : 4                  Type       : Stub
 NextHop     : 10.0.1.1                  Interface : Vlanif10
 Priority    : Low

 Destination : 10.4.4.4/32
 AdverRouter : 10.4.4.4                  Area       : 0.0.0.0
 Cost        : 3                  Type       : Stub
 NextHop     : 10.0.1.1                  Interface : Vlanif20
 Priority    : Medium
```

Table 7-47 Description of the **display ospf migp-routing nexthop** command output

Item	Description
Priority	OSPF convergence priorities: ● Critical: indicates that the convergence priority of OSPF routes is critical. ● High: indicates that the convergence priority of OSPF routes is high. ● Medium: indicates that the convergence priority of OSPF routes is medium. ● Low: indicates that the convergence priority of OSPF routes is low.

7.4.29 display ospf nexthop

Function

The **display ospf nexthop** command displays OSPF next hop information.

Format

display ospf [*process-id*] **nexthop**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can display information about all the OSPF next hops, which helps you troubleshoot OSPF faults.

Example

Display OSPF next hop information.

```
<HUAWEI> display ospf nexthop
          OSPF Process 100 with Router ID 10.0.0.1
              Routing Nexthop information
Next hops:
Address         Type      Refcount  IntfAddr       Intf Name
----------------------------------------------------------------------
10.0.0.1        Local     3         10.0.0.1       Vlanif100
10.0.0.2        Local     5         10.0.0.1       Vlanif100
```

Table 7-48 Description of the **display ospf nexthop** command output

Item	Description
Next hops	Detailed information about the next hop.
Address	Address of the next hop.
Type	Type of the route passing through the next hop. Local indicates that the route is destined for the local network segment.
Refcount	Number of OSPF routes that use the next hop.
IntfAddr	IP address of the interface.
Intf Name	Name of the interface.

7.4.30 display ospf peer

Function

The **display ospf peer** command displays information about neighbors in each OSPF area.

Format

display ospf [*process-id*] **peer** [[*interface-type interface-number*] [*neighbor-id*] | **brief** | **last-nbr-down**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the interface type and the interface number.	-
neighbor-id	Specifies the neighbor's router ID.	It is in dotted decimal notation.
brief	Displays brief information about neighbors in each OSPF area.	-
last-nbr-down	Displays brief information about the last neighbor that went Down in the OSPF area.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can display information about OSPF neighbors, and help you troubleshoot OSPF faults, verify the configurations of OSPF neighbors, and check whether the neighbor performs Graceful Restart (GR).

Example

Display information about the OSPF neighbor.

```
<HUAWEI> display ospf peer
         OSPF Process 1 with Router ID 10.1.1.2
                 Neighbors

 Area 0.0.0.0 interface 10.1.1.2(Vlanif100)'s neighbors
 Router ID: 10.1.1.1          Address: 10.1.1.1           GR State: Normal
   State: Full  Mode:Nbr is Slave  Priority: 1
   DR: 10.1.1.2  BDR: 10.1.1.1    MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:05
   Authentication Sequence: [ 0 ]
```

Table 7-49 Description of the **display ospf peer** command output

Item	Description
Area	Area to which the neighbor belongs.
interface	Interface that connects to the neighbor.
Router ID	Router ID of the neighbor.
Address	Address of the neighboring interface.
GR State	GR status after OSPF GR is enabled: ● Normal: indicates that a switch is in the Normal state and does not perform GR. ● Doing GR: indicates that a switch is performing GR. ● Complete GR: indicates that a switch finishes GR. ● Helper: indicates that the neighbor is the Helper when a switch is performing GR.

Item	Description
State	Neighbor status: - Down: It is the initial status of the neighbor, indicating that the neighbor does not receive any information. On an NBMA network, when the neighbor is in the Down state, Hello packets can still be transmitted at the poll interval, which is longer than the Hello interval. - Attempt: It exists only on an NBMA network, indicating that two ends are attempting to establish the neighbor relationship. The interval for sending Hello packets is the Hello interval, which is shorter than the poll interval. - Init: It indicates that the Hello packet has been received from the neighbor. - 2-Way: It indicates that the Hello packet has been received from the neighbor, and the neighbor list of the Hello packet contains the local Router ID. That is, the two ends can interwork. - ExStart: It is the first step of establishing adjacencies. In this step, the master and slave relationship and DD sequence number are negotiated. - Exchange: It indicates that the LSDBs start to be synchronized. In this process, DD packets, LSR packets, and LSU packets are exchanged. - Loading: It indicates that the LSDBs are being synchronized. In this process, LSR packets and LSU packets are exchanged. - Full: It indicates that the LSDB of the neighbor is already synchronized, and the Full adjacency is established between both ends.
Mode	Master or slave in the process of exchanging DD packets: - Nbr is Master: indicates that the neighbor is the master and actively sends DD packets. - Nbr is Slave: indicates that the neighbor is the slave and cooperates with the master to send DD packets.
Priority	Priority of the neighboring device.
DR	Designated router.
BDR	Backup designated router.
MTU	MTU value of the neighboring interface.

Item	Description
Dead timer due in 35 sec	The dead timer due in 35 seconds.
Retrans timer interval	Interval for retransmitting LSAs, in seconds.
Neighbor is up for	Time during which the neighbor remains Up.
Authentication Sequence	Authentication sequence number.

Display brief information about OSPF neighbors.

```
<HUAWEI> display ospf 1 peer brief
        OSPF Process 1 with Router ID 10.10.10.1
                 Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id         Interface                  Neighbor id      State
 0.0.0.0         Vlanif10                   10.10.10.3       Full
 ----------------------------------------------------------------------------
 Total Peer(s):     1
```

Table 7-50 Description of the **display ospf peer brief** command output

Item	Description
Area Id	Area to which the neighbor belongs.
Interface	Interface that connects to the neighbor.
Neighbor id	Router ID of the neighbor.
Total Peer(s)	Number of neighbors.

Display information about the OSPF neighbor that went Down for the last time.

```
<HUAWEI> display ospf 1 peer last-nbr-down
         OSPF Process 1 with Router ID 10.1.1.1

                      Last Down OSPF Peer

        Neighbor Ip Address : 10.2.1.2
        Neighbor Area   Id  : 0.0.0.0
        Neighbor Router Id  : 2.2.2.2
        Interface           : Vlanif100
        Immediate Reason    : Neighbor Down Due to Kill Neighbor
        Primary Reason      : Logical Interface State Change
        Down Time           : 2012-09-14 17:17:7
```

Table 7-51 Description of the **display ospf peer last-nbr-down** command output

Item	Description
Neighbor Ip Address	Address of the neighboring interface.

Item	Description
Neighbor Area Id	Area to which the neighbor belongs.
Neighbor Router Id	Router ID of the neighbor.
Interface	Interface that connects to the neighbor.
Immediate Reason	Immediate reason that the neighbor went Down: ● Neighbor Down Due to Inactivity: indicates that the inactivity timer times out. ● Neighbor Down Due to LL Down: indicates that the link is Down. For example, the interface went Down from Up or the IP address of the link is deleted. ● Neighbor Down Due to Kill Neighbor: indicates that the kill neighbor event is generated on the neighbor state machine. ● Neighbor Down Due to 1-Wayhello: indicates that the neighbor went Down because it receives a 1-way packet. ● Received: indicates that the AdjOK? event is generated on this interface. ● Neighbor Down Due to SequenceNum Mismatch: indicates that the SequenceNum Mismatch event is generated on the neighbor state machine. ● Neighbor Down Due to BadLSreq: indicates that the BadLSreq event is generated on the neighbor state machine.

Item	Description
Primary Reason	Primary reason that the neighbor went Down: ● Hello Not Seen: indicates that no Hello packet is received. ● Interface Parameter Mismatch: indicates that the parameters set on both ends of the link do not match. ● Logical Interface State Change: indicates that the status of the logical interface changes. ● Physical Interface State Change: indicates that the status of the physical interface changes. ● OSPF Process Reset: indicates that the OSPF process restarts. ● Area reset: indicates that the area restarts because the area type changes. ● Area Option Mis-match: indicates that the area options of the interfaces on both ends of the link do not match. ● Vlink Peer Not Reachable: indicates that the neighbor on the virtual link is not reachable. ● Sham-Link Unreachable: indicates that the neighbor on the sham link is not reachable. ● Undo Network Command: indicates that the **network** command is deleted. ● Undo NBMA Peer: indicates that the neighbor configuration on the NBMA interface is deleted. ● Passive Interface Down: indicates that the neighbor relationship went Down because the **silent-interface** command is configured on the local interface. ● Opaque Capability Enabled: indicates that Opaque capability is enabled. ● Opaque Capability Disabled: indicates that Opaque capability is disabled. ● Virtual Interface State Change: indicates that the status of a virtual link interface changes. ● BFD Session Down: indicates that the BFD session went Down. ● Down Retransmission Limit Exceed: indicates that the number of retransmission times reaches the limit. ● 1-Wayhello Received: indicates that the device receives 1-way hello packets. ● Router State Change from DR or BDR to DROTHER: indicates that the interface state machine changes to DROTHER from DR or BDR.

Item	Description
	- Neighbor State Change from DR or BDR to DROTHER: indicates that the neighbor state machine changes to DROTHER from DR or BDR. - NSSA Area Configure Change: indicates that the configuration of the NSSA area changes. - Stub Area Configure Change: indicates that the configuration of the Stub area changes. - Received Invalid DD Packet: indicates that invalid DD packets are received. - Not Received DD during RouterDeadInterval: indicates that no DD packet is received during the time when the Dead timer starts. - M,I,MS bit or SequenceNum Incorrect: indicates that the M, I, and MS bits do not comply with specifications in the protocol. - Unable Opaque Capability,Find 9,10,11 Type Lsa: indicates that Type9, Type10, and Type11 LSAs are received and Opaque capability is disabled. - Not NSSA,Find 7 Type Lsa in Summary List: indicates that this area is not an NSSA area and Type7 LSAs are found in the summary table. - LSrequest Packet,Unknown Reason: indicates that LSR packets are received with the reason unknown. - NSSA or STUB Area,Find 5 ,11 Type Lsa: indicates that this area is an NSSA or Stub area and Type5 and Type11 LSAs are found. - LSrequest Packet,Request Lsa is Not in the Lsdb: indicates that the neighbor sends an LSR to this process or area to request an LSA and this LSA does not exist in the LSDB of this process. - LSrequest Packet, exist same lsa in the Lsdb: indicates that this process receives an LSA that is same as that in the LSDB and the LSA is found in the request list of the neighbor. - LSrequest Packet, exist newer lsa in the Lsdb: indicates that this process receives a new LSA that exists in the local LSDB and the LSA is found in the request list of the neighbor. - Neighbor state was not full when LSDB overflow: indicates that the LSDB overflows and the neighbor state machine is not Full. - Filter LSA configuration change: indicates that the configuration of LSA filter changes. - ACL changed for Filter LSA: indicates that the ACL configuration of LSA filter changes.

Item	Description
	- Reset Ospf Peer: indicates that the OSPF neighbor is restarted.
Down Time	Time when the neighbor went Down.

7.4.31 display ospf request-queue

Function

The **display ospf request-queue** command displays the OSPF request list.

Format

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the interface type and number.	-
neighbor-id	Specifies the neighbor's router ID.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output helps you troubleshoot OSPF faults.

Example

Display the OSPF request list.

```
<HUAWEI> display ospf request-queue
 OSPF Process 1 with Router ID 10.1.1.1
 OSPF Request List
  The Router's Neighbor is Router ID 10.4.4.4         Address 172.16.4.2
  Interface 172.16.4.1        Area 0.0.0.2
  Request list:
```

```
     Type       LinkState ID      AdvRouter         Sequence   Age
     Router     10.1.1.1          10.1.1.1         8000001b    677
```

Table 7-52 Description of the **display ospf request-queue** command output

Item	Description
The Router's Neighbor is Router ID	Router ID of the neighbor.
Address	IP address of the neighboring interface.
Interface	IP address of the interface.
Area	Area to which the local device belongs.
Request list	Request list.
Type	LSA type: Router LSA, network LSA, network summary LSA, ASBR summary LSA, AS external LSA, NSSA LSA, and opaque LSA
LinkState ID	Link state ID in the LSA header.
AdvRouter	Advertising router in the LSA header.
Sequence	Sequence number in the LSA header.
Age	Aging time in the LSA header.

7.4.32 display ospf retrans-queue

Function

The **display ospf retrans-queue** command displays the OSPF retransmission list.

Format

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*] [**low-level-of-retrans-times-range** *min-time*] [**high-level-of-retrans-times-range** *max-time*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the interface type and number.	-
neighbor-id	Specifies the neighbor's router ID.	It is in dotted decimal notation.

Parameter	Description	Value
low-level-of-retrans-times-range *min-time*	Specifies the minimum number of allowed LSA retransmission.	The value is an integer ranging from 0 to 65535.
high-level-of-retrans-times-range *max-time*	Specifies the maximum number of allowed LSA retransmission.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output helps you troubleshoot OSPF faults.

Example

Display the OSPF retransmission list.

```
<HUAWEI> display ospf retrans-queue

        OSPF Process 1 with Router ID 10.1.1.1
                OSPF Retransmit List

  The Router's Neighbor is Router ID 10.2.2.2  Address 192.168.0.2
  Interface 192.168.0.1      Area 0.0.0.0
  Retransmit list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     10.1.1.1          10.1.1.1          80000002   533
```

Table 7-53 Description of the **display ospf retrans-queue** command output

Item	Description
The Router's Neighbor	Basic information about the neighboring switch.
Router ID	Router ID of the neighbor.
Address	IP address of the neighboring interface.
Interface	IP address of the interface.
Area	Area ID.
Retransmit List	Retransmission list.

Item	Description
Type	LSA type: Router LSA, network LSA, network summary LSA, ASBR summary LSA, AS external LSA, NSSA LSA, and opaque LSA
LinkState ID	Link state ID in the LSA header.
AdvRouter	Advertising router in the LSA header.
Sequence	Sequence number in the LSA header.
Age	Aging time in the LSA header.

7.4.33 display ospf routing

Function

The **display ospf routing** command displays an OSPF routing table.

Format

display ospf [*process-id*] **routing router-id** [*router-id*]

display ospf [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
router-id *router-id*	Specifies the router ID of a destination router.	The value is in dotted decimal notation.
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
mask	Specifies a subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
nexthop *nexthop-address*	Displays the route with a specified next hop IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By using this command with different parameters, you can view the routes of a specified interface or next hop.

The command output helps you troubleshoot OSPF faults.

Example

Display the OSPF routing table.

```
<HUAWEI> display ospf routing
         OSPF Process 1 with Router ID 10.2.2.9
                  Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.12.12.0/24      1     Transit    10.12.12.10     10.2.2.9        0.0.0.1
 10.13.13.0/24      1     Stub       10.13.13.1      10.2.2.9        0.0.0.0
 10.11.11.0/24      2     Transit    10.12.12.11     10.0.0.1        0.0.0.1

 Routing for ASEs
 Destination        Cost      Type       Tag      NextHop         AdvRouter
 10.0.0.0/8         1         Type2      1        10.12.12.11     10.0.0.1

 Total Nets: 4
 Intra Area: 3  Inter Area: 0  ASE: 1  NSSA: 0
```

Table 7-54 Description of the **display ospf routing** command output

Item	Description
Destination	Destination network.
Cost	Cost of the route to the destination address.

Item	Description

Type	- Type 1 external route:
	When the cost of external routes equals that of AS internal routes, and can be compared with the cost of OSPF routes, these external routes have a high reliability and can be configured as Type 1 external routes.
	- Type 2 external route:
	When the cost of the routes from an ASBR to the destination outside an AS is much greater than the cost of the internal routes to the ASBR, these external routes have a low reliability and can be configured as Type 2 external routes.
	Type of the destination network:
	- Inter-area: indicates inter-area routes.
	- Intra-area: indicates intra-area routes.
	  – Stub: indicates the routes advertised by router LSAs, which correspond to the direct routes of non-broadcast and non-NBMA networks.
	  – Transit: indicates the routes advertised by network LSAs.

NextHop	Next hop address to the destination address.
AdvRouter	Device that advertises LSAs.
Area	Area ID.
Tag	Tag of the external route.
Total Nets	Total number of networks in an area, between areas, in ASE areas, and in NSSAs.
Intra Area	Total number of intra-area networks (that is, stub networks and transit networks).
Inter Area	Total number of inter-area networks.
ASE	Total number of networks in the ASE area.
NSSA	Total number of networks in the NSSA.

7.4.34 display ospf sham-link

Function

The **display ospf sham-link** command displays the sham links of an OSPF area.

If no OSPF process ID or area ID is specified, all sham links are displayed.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

display ospf [*process-id*] **sham-link** [**area** *area-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the ID of an OSPF area.	The value is an integer ranging from 0 to 4294967295 or in the IPv4 address format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospf sham-link** command to check information about the sham links of an OSPF area. The information helps determine the establishment of sham links.

Example

Display all OSPF sham links.

```
<HUAWEI> display ospf sham-link
          OSPF Process 100 with Router ID 10.1.1.2
 Sham Link:
 Area       NeighborId     Source-IP      Destination-IP   State   Cost
 0.0.0.1    10.1.1.2       10.3.3.3       10.5.5.5         P-2-P   10
```

Display the OSPF sham link of Area 1.

```
<HUAWEI> display ospf sham-link area 1
         OSPF Process 100 with Router ID 10.1.1.2
  Sham-Link: 10.3.3.3 --> 10.5.5.5
  Neighbor ID: 10.1.1.2,    State: Full
  Area: 0.0.0.1
  Cost: 10  State: P-2-P, Type: Sham
  Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 7-55 Description of the **display ospf sham-link** command output

Item	Description
Area	OSPF area that the sham link belongs to.
NeighborId	Neighbor ID of the switch.
Source-IP	Source IP address of the sham link.
Destination-IP	Destination IP address of the sham link.
State	Interface status of the sham link. P-2-P indicates the point-to-point link.
Cost	Cost of the sham link.
Type	Connection type.
Timers	Information about the following items: the interval for sending Hello messages, Dead time, retransmission interval, and transmission delay on the interface.

7.4.35 display ospf spf-statistics

Function

The **display ospf spf-statistics** command displays route calculation statistics in OSPF processes.

Format

display ospf [*process-id*] **spf-statistics** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, brief information about route calculation statistics in all processes is displayed.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
verbose	Displays detailed information about route calculation statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ospf spf-statistics** command displays route calculation statistics in OSPF processes, including the time when route calculation occurs, cause of route calculation, and number of changed routes.

When identifying the cause of OSPF route flapping, you can run this command to obtain OSPF route calculation statistics, and then identify the cause according to the command output.

Example

Display brief information about route calculation statistics in OSPF process 1.

```
<HUAWEI> display ospf 1 spf-statistics

          OSPF Process 1 with Router ID 10.2.2.2
Routing table change statistics:
Date          Time           Intra       Inter    External    Reason
2008-08-14    10:17:16        17          17       17          LSA
2008-08-14    09:16:47        77          62       127          Other
2008-08-14    08:16:37        0          0        0          LSA
2008-08-14    07:04:40        24          230      108          LSA
2008-08-14    06:03:15        204          230      18          Other
2008-08-14    05:02:55        34          236      128          LSA
2008-08-14    04:01:49        54          130      158          LSA
2008-08-14    03:01:48        44          220      138          LSA
2008-08-14    02:01:43        22          233      158          LSA
2008-08-14    01:00:53        977          897      907          LSA
```

Table 7-56 Description of the **display ospf spf-statistics** command output

Item	Description
Date	Date when route calculation occurs.
Time	Time when route calculation occurs.
Intra	Number of intra-area routes in the routing table, which are changed because of route calculation.
Inter	Number of inter-area routes in the routing table, which are changed because of route calculation.

Item	Description
External	Number of external routes in the routing table, which are changed because of route calculation.
Reason	Cause of route calculation: - LSA: indicates that route calculation is caused by LSAs. - Other: indicates that route calculation is caused by other causes. For example, the configuration changes; or the interface goes Down.

Display detailed information about route calculation statistics in OSPF process 1.

```
<HUAWEI> display ospf 1 spf-statistics verbose

          OSPF Process 1 with Router ID 10.10.10.2
Routing table change statistics:
Index: 1
          Time     : 2008-11-29,17:36:59
          Intra    : 0 Added,0 Deleted, 0 Modified
          Inter    : 0 Added,0 Deleted, 0 Modified
          External : 10 Added,0 Deleted, 0 Modified
          The reason of calculation is:LSA
          NO.     Type          LS ID           Adv Router
          1       External      10.1.5.0        10.10.10.1
          2       External      10.1.3.0        10.10.10.1
          3       External      10.1.9.0        10.10.10.1
          4       External      10.1.4.0        10.10.10.1
          5       External      10.1.2.0        10.10.10.1
          6       External      10.1.8.0        10.10.10.1
          7       External      10.1.7.0        10.10.10.1
          8       External      10.1.6.0        10.10.10.1
          9       External      10.1.10.0        10.10.10.1
          10       External      10.1.1.0        10.10.10.1
```

Table 7-57 Description of the **display ospf spf-statistics verbose** command output

Item	Description
Time	Date and time when route calculation occurs.
Intra	Number of intra-area routes in the routing table, which are added and deleted because of route calculation.
Inter	Number of inter-area routes in the routing table, which are added and deleted because of route calculation.
External	Number of external routes in the routing table, which are added and deleted because of route calculation.

Item	Description
The reason of calculation is	Cause of route calculation: ● LSA: indicates that route calculation is caused by LSAs. ● Other: indicates that route calculation is caused by other causes. For example, the configuration changes; or the interface goes Down.
No.	Sequence number of the LSA that causes route calculation, which ranges from 1 to 10.
Type	Type of the LSA that causes route calculation, including Router, Network, Sum-Net, External, and NSSA.
LS ID	Link state ID of the LSA that causes route calculation.
Adv Router	Router ID of the switch that generates the LSA that causes route calculation.

7.4.36 display ospf statistics updated-lsa

Function

The **display ospf statistics updated-lsa** command displays the frequent updates of the LSAs that the LSDB receives.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

display ospf [*process-id*] **statistics updated-lsa** [**originate-router** *advertising-router-id* | **history**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, this command displays brief information about the route calculation statistics in all processes.	The value is an integer ranging from 1 to 65535.
originate-router	Specifies the link status of the advertising switch.	-
advertising-router-id	Specifies the ID of the advertising switch.	The value is in dotted decimal notation
history	Specifies the change history of LSAs that the LSDB receives.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display ospf statistics updated-lsa** command displays the frequent updates of LSAs, facilitating the location of the cause for a routing flapping.

- If the **history** parameter is not configured, the **display ospf statistics updated-lsa** command only displays the updates of LSAs within the latest hour.
- If the **history** parameter is configured, the **display ospf statistics updated-lsa** command displays the change history of LSAs within the last 24 hours.

Precautions

- If you run the **reset ospf** command to restart the OSPF process, the real-time and historical statistics on the process will be cleared.
- The **display ospf statistics updated-lsa** command is used only to display the frequent updates of LSAs. The updated LSAs are compared with the LSAs in the local LSDB, and those with the **age** greater than 900 will not be displayed except those with the **age** of 3600.

Example

Display the LSA updates within the last one hour.

```
<HUAWEI> display ospf statistics updated-lsa
          OSPF Process 1 with Router ID 10.1.1.1
               Statistics of Received LSAs

 Begin time: 2011-04-25 11:37:32

 AdvRouter          Total        Updated at
 10.1.1.1           18           11:37:40/2011/04/25
 10.2.2.2           5            11:37:40/2011/04/25
 10.3.3.3           5            11:37:41/2011/04/25
 10.4.4.4           5            11:37:41/2011/04/25
 10.5.5.5           2            11:37:40/2011/04/25
 10.6.6.6           3            11:37:40/2011/04/25
 10.7.7.7           5            11:37:40/2011/04/25
 10.8.8.8           6            11:37:41/2011/04/25
```

Table 7-58 Description of the **display ospf statistics updated-lsa** command output

Item	Description
Begin time	Start time of collecting statistics.
AdvRouter	Advertising switch.
Total	Total update times of LSAs.
Updated at	Latest update time.

Display the LSA updates of the specified advertising switch.

```
<HUAWEI> display ospf statistics updated-lsa originate-router 10.1.1.1
          OSPF Process 1 with Router ID 10.2.2.2
               Statistics of Received LSAs

 Begin time: 2011-04-25 11:37:32

 AdvRouter       : 10.1.1.1
 Total           : 6                Updated at       : 2011-04-25 11:37:41
 Router(1)       : 3                Network(2)       : 2
 Summary-Net(3)  : 0                Summary-Asbr(4)  : 0
 External(5)     : 1                NSSA(7)          : 0
 Opaque-link(9)  : 0                Opaque-area(10)  : 0
 Opaque-AS(11)   : 0
```

Table 7-59 Description of the **display ospf statistics updated-lsa originate-router** command output

Item	Description
Router(1)	Update times of Router LSAs.
Network(2)	Update times of Network LSAs.
Summary-Net(3)	Update times of Network Summary LSAs.

Item	Description
Summary-Asbr(4)	Update times of ASBR Summary LSAs.
External(5)	Update times of AS External LSAs.
nssa(7)	Update times of Type7 LSAs.
Opaque-link(9)	Update times of Type9 LSAs.
Opaque-area(10)	Update times of Type10 LSAs.
Opaque-AS(11)	Update times of Type11 LSAs.

Display the change history of LSAs.

```
<HUAWEI> display ospf statistics updated-lsa history
         OSPF Process 1 with Router ID 10.1.1.1
         History Information for Received LSAs

 Record  1:
 Begin time: 2011-04-25 11:39:32
 End   time: 2011-04-25 11:41:32

 no Record

 Record  2:
 Begin time: 2011-04-25 11:37:32
 End   time: 2011-04-25 11:39:32

 AdvRouter      : 10.1.1.1          Total           : 18
 Router(1)      : 0                 Network(2)      : 0
 Summary-Net(3) : 0                 Summary-Asbr(4) : 18
 External(5)    : 0                 NSSA(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0

 AdvRouter      : 10.2.2.2          Total           : 5
 Router(1)      : 3                 Network(2)      : 2
 Summary-Net(3) : 0                 Summary-Asbr(4) : 0
 External(5)    : 0                 NSSA(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0

 AdvRouter      : 10.3.3.3          Total           : 5
 Router(1)      : 3                 Network(2)      : 2
 Summary-Net(3) : 0                 Summary-Asbr(4) : 0
 External(5)    : 0                 NSSA(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0

 AdvRouter      : 10.4.4.4          Total           : 5
 Router(1)      : 2                 Network(2)      : 2
 Summary-Net(3) : 0                 Summary-Asbr(4) : 0
 External(5)    : 1                 NSSA(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0
```

Table 7-60 Description of the **display ospf statistics updated-lsa history** command output

Item	Description
Record	Record number.
End time	End time of collecting statistics.

7.4.37 display ospf vlink

Function

The **display ospf vlink** command displays OSPF virtual links.

Format

display ospf [*process-id*] **vlink**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output helps you troubleshoot OSPF faults.

Example

Display OSPF virtual links.

```
<HUAWEI> display ospf vlink
          OSPF Process 1 with Router ID 10.1.1.1
                  Virtual Links
 Virtual-link Neighbor-id  -> 10.2.2.2, Neighbor-State: Full
 Interface: 10.1.1.1 (Vlanif10)
 Cost: 1  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
 GR State: Normal
```

Table 7-61 Description of the **display ospf vlink** command output

Item	Description
Virtual-link Neighbor-id	ID of the neighboring switch that is connected through the virtual link.
Neighbor-State	Neighbor status, such as Down, Init, 2-Way, ExStart, Exchange, Loading, and Full.
Interface	Information about interfaces in the area, that is, IP address and name of the primary interface (If the interface is a serial interface, **Unknown** is displayed.)
Cost	Cost.
State	Interface status.
Type	Interface type.
Transit Area	Transit area ID if the current interface is a virtual link.
Timers	Information about the following items: the interval for sending Hello messages, Dead time, retransmission interval, and transmission delay on the interface.
GR State	GR status: ● Normal: indicates that a switch is in the Normal state and does not perform GR. ● Doing GR: indicates that a switch is performing GR. ● Complete GR: indicates that a switch finishes GR. ● Helper: indicates that the neighbor is the Helper when a switch is performing GR.

7.4.38 dn-bit-set

Function

The **dn-bit-set disable** command disables OSPF from setting the DN bit in LSAs.

The **undo dn-bit-set disable** command enables OSPF to set the DN bit in LSAs.

By default, OSPF is enabled to set the DN bit in LSAs.

Format

dn-bit-set disable { **summary** | **ase** | **nssa** }

undo dn-bit-set disable { **summary** | **ase** | **nssa** }

Parameters

Parameter	Description	Value
summary	Specifies that the DN bit is not set in summary LSAs.	-
ase	Specifies that the DN bit is not set in ASE LSAs.	-
nssa	Specifies that the DN bit is not set in NSSA LSAs.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dn-bit-set disable** command can be used in the following scenarios:

- In the VPN option A scenario, the local PE imports BGP routes to generate LSAs and advertise the generated LSAs to the peer PE. According to RFC 4577, setting of the DN bit is restricted. The peer PE may fail to calculate a route. In this situation, the **dn-bit-set disable** command can be used to set the DN bit on or remove the setting of the DN bit from the local PE.
- When a PE is connected to an MCE, the MCE needs to calculate routes advertised by the PE. By default, the MCE does not check the DN bit. In this situation, the **dn-bit-set disable** command can be used to set the DN bit on or remove the setting of the DN bit from the local PE.

NOTE

To prevent routing loops, the OSPF multi-instance process uses a bit as a flag. The bit is called DN bit.

Configuration Impact

When the **dn-bit-set disable** command is used to disable OSPF from setting the DN bit in LSAs, routing loops may occur. If the parameter **ase** or **nssa** is specified, the DN bit in ASE LSAs or NSSA LSAs is not set. You can use the **route-tag** command to set the same tag value to prevent routing loops. Therefore, it is recommended that the **dn-bit-set disable** command be used in only the scenarios specified in **Usage Scenario**.

If the **dn-bit-set disable ase** command is configured, the DN bit is not set in type 5 LSAs that are converted from type 7 LSAs even if the DN bit is set in type 7 LSAs.

Precautions

The **dn-bit-set disable** command can be configured for only private OSPF processes. The configuration of this command takes effect only on the PEs.

The **dn-bit-check disable** command can be used to control whether OSPF running on the peer PE checks the DN bit when calculating routes.

Example

Disable OSPF from setting the DN bit in ASE LSAs.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance test
[HUAWEI-vpn-instance-test] route-distinguisher 100:1
[HUAWEI-vpn-instance-test-af-ipv4] quit
[HUAWEI-vpn-instance-test] quit
[HUAWEI] ospf 100 vpn-instance test
[HUAWEI-ospf-100] dn-bit-set disable ase
```

7.4.39 dn-bit-check

Function

The **dn-bit-check disable** command disables OSPF from checking the DN bit in LSAs.

The **undo dn-bit-check disable** command enables OSPF to check the DN bit in LSAs.

By default, OSPF is enabled to check the DN bit in LSAs.

Format

dn-bit-check disable { **summary** [**router-id** *router-id*] | **ase** | **nssa** }

undo dn-bit-check disable { **summary** [**router-id** *router-id*] | **ase** | **nssa** }

Parameters

Parameter	Description	Value
summary	Specifies that the DN bit in summary LSAs is not checked.	-
router-id *router-id*	Specifies the ID of a device on which the DN bit in summary LSAs is checked.	-
ase	Specifies that the DN bit in ASE LSAs is not checked.	-
nssa	Specifies that the DN bit in NSSA LSAs is not checked.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the VPN option A scenario, the local PE imports BGP routes to generate LSAs and advertise the generated LSAs to the peer PE. According to RFC 4577, setting of the DN bit is restricted. The peer PE may fail to calculate a route. In this situation, you need to use the **dn-bit-check disable** command to disable OSPF from checking the DN bit in LSAs.

NOTE

To prevent routing loops, the OSPF multi-instance process uses a bit as a flag. The bit is called DN bit.

Configuration Impact

When the **dn-bit-check disable** command is run, routing loops may occur. If the parameter **ase** or **nssa** is specified, the DN bit in ASE LSAs or NSSA LSAs is not checked. You can use the **route-tag** command to set the same tag value to prevent routing loops. Therefore, run the **dn-bit-check disable** command only in the scenario specified in **Usage Scenario**.

Precautions

When a PE is connected to an MCE, the MCE does not check the DN bit by default.

The **dn-bit-check disable** command can be configured only for private OSPF processes. The configuration of this command takes effect only on the PEs.

In this scenario, you can run the **dn-bit-set disable** command to set the DN bit on or remove the setting of the DN bit from the local PE.

Example

Disable OSPF from checking the DN bit in summary LSAs.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance test
[HUAWEI-vpn-instance-test] route-distinguisher 100:1
[HUAWEI-vpn-instance-test-af-ipv4] quit
[HUAWEI-vpn-instance-test] quit
[HUAWEI] ospf 100 vpn-instance test
[HUAWEI-ospf-100] dn-bit-check disable summary router-id 10.1.1.1
```

7.4.40 domain-id (OSPF)

Function

The **domain-id** command sets an ID for an OSPF domain.

The **undo domain-id** command restores the default setting.

By default, the domain ID is null.

Format

domain-id { **null** | *domain-id* [**type** *type* **value** *value* | **secondary**] * }

undo domain-id [*domain-id* [**type** *type* **value** *value*]]

Parameters

Parameter	Description	Value
domain-id	Specifies the ID of an OSPF domain.	The value can be an integer or in dotted decimal notation. ● If it is an integer, the value ranges from 0 to 4294967295, and it is converted to dotted decimal notation when the ID is displayed. ● If it is in dotted decimal notation, it is displayed as entered.
null	Indicates that the OSPF domain ID is null.	-
type *type*	Specifies the type of the OSPF domain ID.	It can be 0005, 0105, 0205, or 8005. By default, it is 0005.
value *value*	Specifies the value of the type of the OSPF domain ID.	The value is a hexadecimal number that ranges from 0x0 to 0xffff, and the default value is 0x0.
secondary	Indicates the ID of a secondary domain.	The maximum number of **domain-id secondary** in each OSPF process is 1000.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Domain IDs are used to identify domains.

If the local OSPF area and an OSPF area of a remote VPN attempts to exchange Type 3 LSAs, the two areas must be in the same OSPF domain. You can run the **domain-id** command to configure the same domain ID for the two OSPF areas.

The routes that are imported from a PE switch are advertised using External-LSAs. The routes destined for different nodes in the same OSPF domain are advertised based on Type 3 LSAs. This requires that the nodes in the same OSPF domain be configured with the same domain ID.

If the **undo domain-id** command without any parameter is executed, the primary domain ID will be deleted.

NOTE

OSPF direct routes to the PE do not carry the domain ID, while BGP direct routes to the PE carry the domain ID.

Configuration Impact

Before sending routes to a remote CE switch, a PE switch sends Type 3 LSAs or Type 5 LSAs to the CE based on domain ID. If local domain IDs are the same as or compatible with remote domain IDs in BGP routes, the PE advertises Type 3 routes. If local domain IDs are different from or incompatible with remote domain IDs in BGP routes, the PE advertises Type 5 routes.

Precautions

- Each OSPF domain has one or multiple domain IDs. One of them is a primary ID and the others are secondary IDs.
- If an OSPF instance does not have a specific domain ID, its ID is considered as null.
- If the value of the domain ID is 0, **secondary** cannot be configured.
- The maximum number of **domain-id secondary** items configured in an OSPF process is 1000.
- The **domain-id** command is forbidden in public networks.

Example

Set an OSPF domain ID.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] domain-id 234
```

7.4.41 eca-route-type compatible

Function

The **eca-route-type compatible** command sets the route type of the extended community attribute of OSPF VPN to 0x8000.

The **undo eca-route-type compatible** command restores the route type of the extended community attribute of OSPF VPN to 0x0306.

By default, the route type of the extended community attribute of OSPF VPN is 0x0306.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

eca-route-type compatible

undo eca-route-type compatible

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **eca-route-type compatible** command is used in OSPF VPN scenarios.

- For the switch supporting RFC 4577, you can set the route type of the extended community attribute of OSPF VPN to 0x0306 and configure the switch to identify both 0x0306 and 0x8000 route types.
- For the switch that does not support RFC 4577, you can set the route type of the extended community attribute of OSPF VPN to 0x8000 and configure the switch to identify only the 0x8000 route type.

The **eca-route-type compatible** command enables different switches to communicate with each other and avoid the failure in parsing the route type because the route type of the extended community attribute of OSPF VPN is unrecognized.

Precautions

The **eca-route-type compatible** command is forbidden in public network.

Example

Set the route type of the extended community attribute of OSPF VPN to 0x8000.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance test
[HUAWEI-vpn-instance-test] route-distinguisher 100:1
[HUAWEI-vpn-instance-test-af-ipv4] quit
[HUAWEI-vpn-instance-test] quit
[HUAWEI] ospf 1 vpn-instance test
[HUAWEI-ospf-1] eca-route-type compatible
```

7.4.42 enable log

Function

The **enable log** command enables the logging function.

The **undo enable log** command disables the logging function.

By default, the logging function is disabled.

Format

enable log [**config** | **error** | **state** | **snmp-trap**]

undo enable log [**config** | **error** | **state** | **snmp-trap**]

Parameters

Parameter	Description	Value
config	Enables the configuration log.	-
state	Enables the state log.	-
error	Enables the error log.	-
snmp-trap	Enables the SNMP trap log.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **enable log** command can enable the logging function. You can view running status of devices based on logs, facilitating device maintenance.

If the **undo enable log** command is executed, the logging function will be disabled. Then, running status of devices will be not displayed. This is inconvenient for network maintenance.

Precautions

Configuring different parameters in the **enable log** command can display different log information. If no parameter is not specified, the command output displays all log information.

Example

Enable the OSPF logging function.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] enable log
```

7.4.43 filter export (OSPF Area)

Function

The **filter export** command filters the outgoing Type3 LSAs of the local area.

The **undo filter export** command restores the default setting.

By default, the outgoing Type3 LSAs of the local area are not filtered.

Format

filter { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export**

undo filter [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the LSDB and speed up network convergence.

Configuration Impact

After filtering conditions are set for the outgoing summary LSAs to be advertised using the **filter export** command, only the outgoing Type3 LSAs that pass the filtering can be advertised.

Precautions

- The command can be configured only on an ABR.
- For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.
- Run the **filter import** command to set filtering conditions for the incoming Type3 LSAs to be advertised.
- Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, OSPF advertises all Type 3 LSAs.
- Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, OSPF advertises all Type 3 LSAs.

Example

Configure OSPF to filter outgoing Type 3 LSAs.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] area 1
[HUAWEI-ospf-1-area-0.0.0.1] filter 2000 export
```

7.4.44 filter import (OSPF Area)

Function

The **filter import** command filters the incoming Type3 LSAs of the local area.

The **undo filter import** command restores the default setting.

By default, the incoming Type3 LSAs are not filtered.

Format

filter { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After filtering conditions are set for the incoming summary LSAs to be advertised using the **filter import** command, only the incoming Type3 LSAs that pass the filtering can be received.

Configuration Impact

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the LSDB and speed up network convergence.

Precautions

- The command can be configured only on an ABR.
- For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effect only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.
- Run the **filter export** command to set filtering conditions for the outgoing Type3 LSAs to be advertised.
- Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, OSPF receives all Type 3 LSAs.
- Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, OSPF receives all Type 3 LSAs.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all the routes learned by the specified protocol are imported to the OSPF routing table.

Example

Configure an ABR to filter incoming Type 3 LSAs of the area where the ABR resides.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
```

7.4.45 filter-lsa-out peer

Function

The **filter-lsa-out peer** command configures a switch to filter the LSAs that are sent by specified neighbors on a P2MP network.

The **undo filter-lsa-out peer** command cancels the configuration.

By default, the LSAs that are sent by specified neighbors on a P2MP network are not filtered.

Format

filter-lsa-out peer *ip-address* { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }] | **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** { *acl-number* | *acl-name* }] } * }

undo filter-lsa-out peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a P2MP neighbor. This parameter is configured by the neighbor using the **ip address** command.	The value is in dotted decimal notation.
all	Filters all the outgoing LSAs except Grace LSAs.	-
summary	Filters the outgoing network summary LSAs (Type 3).	-
acl *acl-number*	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ase	Filters the outgoing AS external LSAs (Type 5).	-
nssa	Filters the outgoing NSSA LSAs (Type 7).	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a P2MP network, when multiple P2MP links exist between two devices, you can configure the local device to filter the outgoing LSAs on the specified link. This reduces unnecessary LSA retransmission attempts and saves bandwidth resources.

For an ACL, when the **rule** command is used to configure filtering rules, only the source address range that is specified by the **source** parameter and the period of time that is specified by the **time-range** parameter take effect.

Prerequisites

OSPF does not regard a network as a P2MP network by default regardless of any link layer protocol. A P2MP network is forcibly changed from the network of another type using the **ospf network-type p2mp** command.

Configuration Impact

This command is valid for all the interfaces of the OSPF process.

Follow-up Procedure

Configure a device to filter the outgoing LSAs on the specified OSPF interface by using the **ospf filter-lsa-out** command.

Example

On a P2MP network, configure a switch to filter all the LSAs (except Grace LSAs) sent to neighbor 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] filter-lsa-out peer 10.1.1.1 all
```

7.4.46 filter-policy export (OSPF)

Function

The **filter-policy export** command filters the imported routes when these routes are advertised based on a filtering policy.

The **undo filter-policy export** command restores the default setting.

By default, the imported routes to be advertised are not filtered.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol process-id	Filters imported routes of a specified protocol. The value can be **direct**, **rip**, **isis**, **bgp**, **ospf**, **unr**, or **static**. When the routing protocol is RIP, IS-IS, or OSPF, you can specify a process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After OSPF imports external routes using the **import-route** command, you can use the **filter-policy export** command to filter the imported routes to be advertised. Only the external routes that pass the filtering can be converted into AS-external LSAs and advertised.

The *protocol* or *process-id* parameter can be specified to determine a specified protocol or process. If the *protocol* or *process-id* parameter is not specified, OSPF filters all imported routes.

Precautions

- This command can be configured only on ASBRs because AS-external-LSAs are generated by ASBRs.
- For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified

by the **source** parameter and the time period is specified by the **time-range** parameter.

- Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all external routes imported to OSPF are converted to Type 5 LSAs (AS-external-LSAs) or Type 7 LSAs (NSSA-external-LSAs) and then are advertised to neighbors.
- Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all external routes imported to OSPF are converted to Type 5 LSAs (AS-external-LSAs) or Type 7 LSAs (NSSA-external-LSAs) and then are advertised to neighbors.

Example

Filter the routes that are imported from RIP and advertised by OSPF based on a filtering policy.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] import-route rip
[HUAWEI-ospf-100] filter-policy 2000 export
```

7.4.47 filter-policy import (OSPF)

Function

The **filter-policy import** command configures a filtering policy to filter routes received by OSPF.

The **undo filter-policy import** command restores the default setting.

By default, OSPF does not filter received routes.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**] } **import**

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**]] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the basic ACL number.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the route policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
secondary	Selects a secondary route.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **filter-policy import** command is used to set a filtering policy for received routes. Only the routes that pass the filtering can be added to the routing table. The routes that fail to pass the filtering cannot be added to the routing table but can be advertised.

The OSPF routing information is recorded in the LSDB. Instead of filtering the received or sent LSAs, the device filters routes calculated by OSPF using the **filter-policy import** command.

Precautions

For an ACL configured using the **acl** command, when the **rule** command is used to configure a filtering rule, the filtering rule takes effect only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes received by OSPF are delivered to the IP routing table.

Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all routes received by OSPF are delivered to the IP routing table.

Example

Configure OSPF to filter received routes.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] filter-policy 2000 import
```

7.4.48 flooding-control

Function

The **flooding-control** command restricts the flooding of updated LSAs.

The **undo flooding-control** command cancels the restriction on the flooding of updated LSAs.

By default, this function is enabled when the number of neighbors exceeds 256.

Format

flooding-control [**number** *transmit-number* | **timer-interval** *transmit-interval*] *

undo flooding-control [**number** | **timer-interval**] *

Parameters

Parameter	Description	Value
number *transmit-number*	Sets the number of updated LSAs to be flooded each time.	The value is an integer ranging from 1 to 1000. By default, the value is 50.
timer-interval *transmit-interval*	Sets the interval for flooding updated LSAs.	The value is an integer that ranges from 30 to 100000, in milliseconds. By default, the value is 30.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple neighbors are configured or a large number of updated LSAs are flooded, a switch may receive a large number of updated LSAs in a short period. If the switch is busy processing these update packets and discards the Hello packets that maintain neighbor relationships, neighbor relationships may be interrupted. During the reestablishment of neighbor relationships, more packets need to be exchanged, which deteriorates the processing of packets.

To avoid the preceding problem, you can run the **flooding-control** command to restrict the flooding of updated LSAs to keep stable neighbor relationships.

Configuration Impact

After the **flooding-control** command is run, the flooding of updated LSAs is immediately restricted.

Precautions

By default, a switch spends 50 ms in flooding updated LSAs each time. If not all the updated LSAs are flooded within 50 ms, the switch floods the remaining LSAs after the time specified by *transmit-interval*.

Example

Set the number of updated LSAs to be flooded each time to 100.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] flooding-control number 100
```

7.4.49 frr (OSPF)

Function

The **frr** command creates and then displays the OSPF FRR view.

The **undo frr** command deletes the OSPF FRR view.

By default, the OSPF FRR view does not exist.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

frr

undo frr

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF IP FRR allows devices to fast switch traffic from faulty links to back up links without interrupting traffic. This function protects traffic and greatly improves the reliability of OSPF networks. OSPF IP FRR must be configured in the OSPF FRR view. The **frr** command run in the OSPF view creates and displays the OSPF FRR view.

Follow-up Procedure

The **frr** command run in the OSPF view creates and displays the OSPF FRR view only, but cannot enable the OSPF IP FRR function. Run the **loop-free-alternate** command in the OSPF view to enable OSPF IP FRR to create the loop-free backup route.

Example

Create and display the OSPF FRR view.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] frr
[HUAWEI-ospf-1-frr]
```

7.4.50 frr-policy route (OSPF)

Function

The **frr-policy route** command configures a filtering policy for the OSPF IP FRR backup routes. The filtering policy determines what kind of OSPF backup route can be added to the routing table.

The **undo frr-policy route** command cancels the filtering function.

By default, the filtering function is disabled.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

frr-policy route route-policy *route-policy-name*

undo frr-policy route

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the policy used to filter OSPF backup routes.	The value must be an existing route-policy.

Views

OSPF FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF IP FRR allows devices to fast switch traffic on fault links to back up links without interrupting traffic. This protects traffic and greatly improves the reliability of OSPF networks.

After the filtering policy is configured using the **frr-policy route** command, only the OSPF backup route that satisfies filtering rules can be delivered to the forwarding table.

Configuration Impact

To protect the traffic over a specific OSPF route, you can configure a filtering policy *route-policy-name* that the OSPF route matches to ensure that the backup route can be added to the forwarding table. When this route fails, OSPF can fast switch the traffic to a backup route.

Precautions

The **frr-policy route** command is cyclic in nature, and only the latest configuration takes effect.

If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, OSPF adds all backup routes to the IP routing table.

Example

Configure OSPF to add the OSPF backup routes that match the named ACL **abc** to the IP routing table.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] frr
[HUAWEI-ospf-1-frr] loop-free-alternate
[HUAWEI-ospf-1-frr] frr-policy route route-policy abc
```

7.4.51 frr-priority static low

Function

The **frr-priority static low** command enables dynamic backup links to take preference over static backup links so that the LFA algorithm is used to calculate the nexthop and outbound interface.

The **undo frr-priority static** command disables this function.

By default, this function is disabled, static backup links take preference over dynamic backup links during route selection.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

frr-priority static low

undo frr-priority static

Parameters

None

Views

OSPF FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The nexthop and outbound interface of an OSPF loop-free backup link can be obtained using either of the following methods:

- For a static backup link, after IP FRR is enabled using the **ip frr** command in the system view or VPN instance view, configure a nexthop and an outbound interface for the static backup link.
- For a dynamic backup link, after OSPF IP FRR is enabled using the **loop-free-alternate** command, enable the device to use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link.

By default, static backup links take preference over dynamic backup links during route selection. However, static backup links are less flexible than dynamic backup links. If a link failure occurs, static backup links cannot update automatically, but dynamic backup links can. Therefore, to ensure automatic link updates, run the **frr-priority static low** command to enable dynamic backup links to take preference over static backup links so that the LFA algorithm is used to calculate the nexthop and outbound interface.

Prerequisites

The OSPF IP FRR view has been displayed using the **frr** command.

Example

Enable the device to use the LFA algorithm to calculate the backup nexthop and outbound interface.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] frr
[HUAWEI-ospf-1-frr] frr-priority static low
```

7.4.52 graceful-restart (OSPF)

Function

The **graceful-restart** command enables the GR function.

The **undo graceful-restart** command disables the GR function.

By default, OSPF GR is disabled.

Format

graceful-restart [**period** *period* | **planned-only** | **partial**] *

undo graceful-restart [**period** | **planned-only** | **partial**] *

Parameters

Parameter	Description	Value
period *period*	Specifies the duration of GR.	It is an integer ranging from 1s to 1800s. The default value is 120s.
planned-only	Indicates that the switch supports only the planned GR. By default, the switch supports both the planned GR and unplanned GR.	-
partial	Indicates that the switch partially supports the GR. By default, the switch totally supports the GR.	-

NOTE

Planned GR: indicates that a device manually restarts or performs a master/slave device switchover by using the command. Before the device restarts or performs a master/slave device switchover, Restarter will send a grace LSA.

Unplanned GR: indicates that a device restarts or performs a master/slave device switchover because of faults. A device directly performs a master/slave device switchover without sending a grace LSA, and then enters GR after the slave device goes Up. It is different from the planned GR.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent traffic interruption caused by route flapping after an active/standby switchover, you can run the **graceful-restart** command to enable OSPF GR. After the **graceful-restart** command is run to enable GR for a switch, the Helper function is also enabled.

Prerequisites

Opaque LSAs provide a generic mechanism for OSPF extension:

- OSPF supports GR using Type 9 LSAs.
- OSPF supports TE using Type 10 LSAs.

Before configuring OSPF GR, you must enable opaque LSA capability running the **opaque-capability enable** command.

Configuration Impact

After an OSPF process is restarted using GR, the Restarter switch and the Helper switch reestablish the neighbor relationship, exchange routing information, synchronize the LSDB, and update the routing table and forwarding table. This implements OSPF fast convergence, prevents traffic interruption, and stabilizes the network topology.

Precautions

If there are special requirements on the GR Helper, run the **graceful-restart helper-role** command to configure the requirements.

You are advised not to enable OSPF GR if BFD is enabled for a stack of fixed switches. This is because the time taken for smooth data switching during a master/standby switchover in the stack may be longer than the BFD timeout interval, in which situation BFD sessions go Down and OSPF GR fails.

Example

Enable OSPF GR and set the GR period to 200s.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] opaque-capability enable
[HUAWEI-ospf-1] graceful-restart period 200
```

7.4.53 graceful-restart helper-role (OSPF)

Function

The **graceful-restart helper-role** command configures a device as a GR helper.

The **undo graceful-restart helper-role** command cancels the configuration.

By default, the device does not function as a GR helper.

Format

graceful-restart [**period** *period* | **partial** | **planned-only**] * **helper-role** { [{ **ip-prefix** *ip-prefix-name* | **acl-number** *acl-number* | **acl-name** *acl-name* } | **ignore-external-lsa** | **planned-only**] * | **never** }

undo graceful-restart [**period** | **partial** | **planned-only**] * **helper-role** [[{ **ip-prefix** | **acl-number** | **acl-name** } | **ignore-external-lsa** | **planned-only**] * | **never**]

Parameters

Parameter	Description	Value
period *period*	Specifies the duration of GR.	The value is an integer that ranges from 1 to 1800, in seconds. The default value is 120.
planned-only	Configures the device to support only planned GR. By default, the device supports both the planned GR and unplanned GR.	-
partial	Configures the device to support partial GR. By default, the device supports totally GR.	-
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list. The name is a string.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl-number *acl-number*	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ignore-external-lsa	Indicates that the device does not check Type 5 and Type 7 LSAs.	-
planned-only	Indicates that the device supports only planned GR.	By default, the device supports both planned GR and unplanned GR.
never	Indicates that the device does not support the Helper mode.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an OSPF neighbor supports GR and can be a restarter, the current device needs to be set to helper mode, and the neighbor is assisted to complete the GR process.

After the **graceful-restart** command is run to enable GR for a switch, the Helper function is also enabled.

Prerequisites

OSPF supports GR using Type 9 LSAs. So before configuring GR, run the **opaque-capability enable** command to enable opaque LSA capability.

Example

Configure a device as an OSPF GR helper and configure the helper to support only planned GR.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] graceful-restart helper-role planned-only
```

7.4.54 gtsm default-action

Function

The **gtsm default-action** command sets the default action that is performed on the packets that do not match the GTSM policies.

The **undo gtsm default-action drop** command restores the default setting.

By default, the packets that do not match the GTSM policies can pass the filtering.

Format

gtsm default-action { **drop** | **pass** }

undo gtsm default-action drop

Parameters

Parameter	Description	Value
drop	Indicates that the packets that do not match the GTSM policies cannot pass the filtering. The packets are dropped.	-
pass	Indicates that the packets that do not match the GTSM policies can pass the filtering.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a network demanding high security, you can configure Generalized TTL Security Mechanism (GTSM) to improve the security of the OSPF network. GTSM defends against attacks by checking the Time-to-Live (TTL) value. If an attacker simulates real OSPF packets and keeps sending them to a switch, a switch receives the packets and directly sends them to the main control board for OSPF processing, without checking the validity of the packets. In this case, the switch is busy in processing these packets, causing high usage of the CPU. GTSM function protects the switch by checking whether the TTL value in the IP packet header is in a pre-defined range to improve the system security.

GTSM only checks the TTL values of the packets that match the GTSM policy. The packets that do not match the GTSM policy can pass the filtering using the **undo gtsm default-action drop** command or using the **gtsm default-action** command to set the **pass** parameter, or be dropped after the **gtsm default-action** command is run to set the **drop** parameter.

Configuration Impact

If the default action to be taken on GTSM packets is drop, the connection cannot be established by the switch. Therefore, GTSM improves security but reduces the ease of use.

Precautions

You can enable the log function by using the **gtsm log drop-packet** command to record the information about dropped packets for further fault location.

If you configure the default action by using the **gtsm default-action** command but not configure GTSM policy (the **drop** or **pass** parameter), GTSM does not take effect.

Example

Set the default action performed on the packets that do not match the GTSM policies to **drop**.

```
<HUAWEI> system-view
[HUAWEI] gtsm default-action drop
```

Set the default action performed on the packets that do not match the GTSM policy to pass the filtering.

```
<HUAWEI> system-view
[HUAWEI] undo gtsm default-action drop
```

7.4.55 gtsm log drop-packet all

Function

The **gtsm log drop-packet** command configures a GTSM-capable switch to record logs when it drops packets.

The **undo gtsm log drop-packet** command configures a GTSM-capable switch not to record logs when it drops packets.

By default, a GTSM-capable switch does not record logs when dropping packets.

Format

gtsm log drop-packet all

undo gtsm log drop-packet all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a network demanding higher security, you can configure Generalized TTL Security Mechanism (GTSM) to improve the security of the OSPF network. GTSM defends against attacks by checking the Time-to-Live (TTL) value. If an attacker simulates real OSPF packets and keeps sending them to a device, an interface board on the device receives the packets and directly sends them to the main control board for OSPF processing, without checking the validity of the packets. In this case, the device is busy in processing these packets, causing high usage of the CPU. GTSM function protects the device by checking whether the TTL value in the IP packet header is in a pre-defined range to improve the system security.

GTSM only checks the TTL values of the packets that match the GTSM policy. The packets that do not match the GTSM policy can be allowed or dropped by using the **gtsm default-action** command.

You can also enable the logging function by using the **gtsm log drop-packet** command to record the information about dropped packets for further fault location.

Prerequisites

The **gtsm default-action drop** command has been run.

Example

Enable all GTSM-capable boards to record logs when they drop packets.

```
<HUAWEI> system-view
[HUAWEI] gtsm default-action drop
[HUAWEI] gtsm log drop-packet all
```

7.4.56 import-route (OSPF)

Function

The **import-route** command imports routes learned by other protocols.

The **undo import-route** command cancels the configuration.

By default, routes learned by other protocols are not imported.

Format

import-route { **limit** *limit-number* | { **bgp** [**permit-ibgp**] | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf** [*process-id-ospf*] } [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * }

undo import-route { **limit** | **bgp** | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf** [*process-id-ospf*] }

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **bgp** [**permit-ibgp**] and **isis** [*process-id-isis*] parameter.

Parameters

Parameter	Description	Value
bgp	Specifies the BGP protocol whose routes are imported. **NOTE** If this parameter is specified, only EBGP routes can be imported; IBGP routes cannot be imported.	-
permit-ibgp	IBGP routes that are permitted to be imported. **NOTE** The import of IBGP routes may cause route loops. Therefore, this command must not be configured unless it is necessary.	-

Parameter	Description	Value
direct	Specifies the direct protocol whose routes are imported.	-
unr	Specifies the imported source routing protocol as **unr**. User Network Route (UNR) is allocated if dynamic routing protocols cannot be used when users are getting online.	-
rip	Specifies the RIP protocol whose routes are imported.	-
process-id-rip	Specifies the process ID of the protocol whose routes are imported.	The value is an integer ranging from 1 to 65535. The default value is 1.
static	Specifies the static protocol whose routes are imported.	-
isis	Specifies the IS-IS protocol whose routes are imported.	-
process-id-isis	Specifies the process ID of the protocol whose routes are imported.	The value is an integer ranging from 1 to 65535. The default value is 1.
ospf	Specifies the OSPF protocol whose routes are imported.	-
process-id-ospf	Specifies the process ID of the protocol whose routes are imported.	The value is an integer ranging from 1 to 65535. The default value is 1.
limit *limit-number*	The maximum number of external routes that can be imported into an OSPF process.	The value is an integer that ranges from 1 to 4294967295.
cost *cost*	Indicates the route cost.	The value is an integer ranging from 0 to 16777214. For details about the default value, see **default (OSPF)**.

Parameter	Description	Value
route-policy *route-policy-name*	Imports only the route that meets the requirements of the specified route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the tag of the external LSA.	The value is an integer ranging from 0 to 4294967295. For details about the default value, see **default (OSPF)**.
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. For details about the default value, see **default (OSPF)**. ● 1: Type 1 external route ● 2: Type 2 external route

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Importing routes discovered by other routing protocols can enrich OSPF routing information.

OSPF routes are classified into the following types in the descending order of priorities:

- Intra-area routes: refer to the routes in an area within an autonomous system.
- Inter-area routes: refer to the routes between different areas of the same AS. Intra-area routes and area external routes are internal routes of an AS.
- Type 1 external routes: When the cost of external routes equals that of AS internal routes, and can be compared with the cost of OSPF routes, these external routes have a high reliability and can be configured as Type 1 external routes.
- Type 2 external routes: When the cost of the routes from an ASBR to the destination outside an AS is much greater than the cost of the internal routes

to the ASBR, these external routes have a low reliability and can be configured as Type 2 external routes.

On a non-PE device, only EBGP routes are imported after the **import-route bgp** command is configured. IBGP routes are also imported after the **import-route bgp permit-ibgp** command is configured. If IBGP routes are imported, routing loops may occur. To prevent loops, run the **preference (OSPF)** and **preference (BGP)** commands to specify preferences for OSPF and BGP routes. If IBGP routes need to be imported, run the **import-route bgp permit-ibgp** command, and run the **preference (OSPF)** and **preference (BGP)** commands to set the preference of OSPF ASE routes lower than that of IBGP routes (preference value of OSPF ASE routes larger than that of IBGP routes).

On a PE, configuring the **import-route bgp** command imports both EBGP routes and IBGP routes, regardless of whether the **import-route bgp permit-ibgp** command is configured or not. If the **import-route bgp permit-ibgp** command and the **default-route-advertise (OSPF)** command are both configured, the active IBGP default routes can be imported into OSPF.

Prerequisites

To import certain external routes using a route-policy, a route-policy must have been created using the **route-policy** command before running the **import-route** command.

Configuration Impact

After a route-policy is configured, the OSPF process imports only routes that satisfy certain conditions. This prevents devices from receiving unrequired routes.

Precautions

You can use the **default (OSPF)** command to configure default parameters for external routes imported by OSPF, including the cost, type (Type 1 or Type 2), tag, and number of routes.

NOTE

The **import-route (OSPF)** command cannot import the default route of an external protocol. To enable a device to advertise the default route of an external protocol it learns when updating the OSPF routing table to other devices within the area, run the **default-route-advertise (OSPF)** command.

After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the OSPF routing table. Therefore, use this command with caution.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all the routes learned by the specified protocol are imported to the OSPF routing table.

Example

Import Type 2 RIP routes, with the process 40, the tag being 33 and cost being 50.

```
<HUAWEI> system-view
```

```
[HUAWEI] ospf 100
[HUAWEI-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

7.4.57 local-mt enable (OSPF)

Function

The **local-mt enable** command enables OSPF Local Multicast-Topology (MT).

The **undo local-mt enable** command disables OSPF local MT.

By default, OSPF local MT is disabled.

NOTE

Only the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-Hsupport this command.

Format

local-mt enable

undo local-mt enable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast and an MPLS TE tunnel are configured on a network and the TE tunnel is configured with IGP Shortcut, the outbound interface of the route calculated by an IGP is not an actual physical interface but a TE tunnel interface. The device uses a unicast route to the multicast source address to send multicast Join messages from the TE tunnel interface. The device spanned by the TE tunnel, however, cannot sense the multicast Join messages. As a result, multicast forwarding entries will not be created on these devices.

To avoid the preceding problem, you can run the **local-mt enable** command to enable OSPF local Multicast-Topology (MT). MT allows the multicast routing entries to be correct created to guide the forwarding of multicast traffic.

After OSPF local MT is enabled, if the outbound interface of the calculated route is a TE tunnel interface of the IGP Shortcut type, the route management (RM) module creates a separate MIGP routing table for the multicast protocol, calculates the actual physical outbound interface for the route, and adds the physical interface to the MIGP routing table for multicast forwarding.

Prerequisites

IGP Shortcut feature has been enabled using the **enable traffic-adjustment** command.

Precautions

- To control the number of entries in the MIGP routing table and speed up the MIGP routing table search, you can run the **local-mt filter-policy** command to configure a policy for filtering multicast source address. Then only the multicast source address that matches the policy to be added to the MIGP routing table. Configure the routing policy before enabling local MT. This can prevent excessive routes to non-multicast source address from being added to the MIGP routing table and keeps the number of routes in the MIGP routing table within the upper limit.
- Local MT is applicable only to the OSPF process of a public network instance.
- OSPF local MT does not support forwarding adjacency (FA).

Example

Enable local MT on OSPF process 1.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] local-mt enable
```

7.4.58 local-mt filter-policy (OSPF)

Function

The **local-mt filter-policy** command configures the filtering policy of OSPF Local Multicast-Topology (MT).

The **undo local-mt filter-policy** command deletes the filtering policy of OSPF local MT.

By default, the filtering policy of OSPF local MT is not configured.

Format

local-mt filter-policy { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }

undo local-mt filter-policy

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of the basic access control list (ACL).	The value is an integer ranging from 2000 to 2999.

Parameter	Description	Value
acl *acl-name*	Specifies the name of a Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the route policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast and an MPLS TE tunnel are configured on a network and the TE tunnel is configured with IGP Shortcut, the outbound interface of the route calculated by an IGP is not an actual physical interface but a TE tunnel interface. The device uses a unicast route to the multicast source address to send multicast Join messages from the TE tunnel interface. The device through which the TE tunnel passes, however, cannot sense the multicast Join messages. As a result, multicast forwarding entries will not be created.

To avoid the preceding problem, you can create a proper multicast routing table to guide the forwarding of multicast packets by configuring local MT. After OSPF local MT is enabled, if the outbound interface of the calculated route is a TE tunnel interface of the IGP Shortcut type, the route management (RM) module creates a separate MIGP routing table for the multicast protocol, calculates the actual physical outbound interface for the route, and adds the physical interface to the MIGP routing table for multicast forwarding.

To control the number of entries in the MIGP routing table and speed up the MIGP routing table search, you can configure filtering conditions by using the **local-mt filter-policy** command to allow only the matching routes to the multicast source address to be added to the MIGP routing table.

Prerequisites

OSPF local MT has been enabled using the **local-mt enable** command.

Precautions

You are recommended to configure the routing policy before enabling local MT. This can prevent the excessive routes to the not-multicast source address from being added to the MIGP routing table and keeps the number of routes in the MIGP routing table within the upper limit.

When the rule command is used to configure filtering rules for an ACL configured using the **acl** command, only the source address range that is specified by the **source** parameter and the period of time that is specified by the **time-range** parameter take effect.

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all OSPF routes are added to the MIGP routing table.

Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all OSPF routes are added to the MIGP routing table.

Example

Configure the filtering policy of OSPF local MT.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] local-mt enable
[HUAWEI-ospf-1] local-mt filter-policy acl 2000
```

7.4.59 loop-free-alternate (OSPF)

Function

The **loop-free-alternate** command enables OSPF IP FRR to enable the device to use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link.

The **undo loop-free-alternate** command disables OSPF IP FRR.

By default, this function is disabled.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

loop-free-alternate

undo loop-free-alternate

Parameters

None

Views

OSPF FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **frr** command run in the OSPF view creates and displays the OSPF FRR view only, but cannot enable the OSPF IP FRR function. You must run the **loop-free-alternate** command in the OSPF view to enable OSPF IP FRR use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link to create the loop-free backup route.

Follow-up Procedure

Run the **frr-policy route** command in the OSPF view to configure a filtering policy for OSPF IP FRR. Only the OSPF backup route that satisfies specific rules can be delivered to the forwarding table.

Example

Enable OSPF IP FRR to create the loop-free backup route.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] frr
[HUAWEI-ospf-1-frr] loop-free-alternate
```

7.4.60 lsa-arrival-interval

Function

The **lsa-arrival-interval** command sets an interval for receiving LSAs.

The **undo lsa-arrival-interval** command restores the default interval for receiving LSAs.

By default, the interval for receiving LSA packets is one second.

Format

lsa-arrival-interval { *interval* | **intelligent-timer** *max-interval start-interval hold-interval* }

undo lsa-arrival-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for receiving LSAs.	The value is an integer ranging from 0 to 10000, in ms.
intelligent-timer	Enables an intelligent timer to receive LSAs.	-
max-interval	Specifies the maximum interval for receiving LSAs.	The value is an integer ranging from 1 to 120000, in ms. The default value is 1000.
start-interval	Specifies the initial interval for receiving LSAs.	The value is an integer ranging from 0 to 60000, in ms. The default value is 500.
hold-interval	Specifies the Holdtime interval for receiving LSAs.	The value is an integer ranging from 1 to 60000, in ms. The default value is 500.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent frequent LSA updates caused by network connection or frequent route flapping, you can set the interval for receiving LSAs using this command. A router receives LSAs only when it meets the set interval.

In a stable network where routes need to be fast converged, you can set the interval for receiving LSAs at millisecond level to receive and update LSAs in time. The change of the topology or the route, therefore, can be immediately detected, and LSDB synchronization speed is improved.

If there is no special requirement for the network, using the default value is recommended.

Configuration Impact

After this command is configured, the interval for receiving LSAs is as follows:

1. The initial interval for receiving LSAs is specified by the parameter *start-interval*.
2. The interval for receiving LSAs for the nth (n≥2) time is equal to *hold-interval* × $2^{(n-2)}$.
3. When the interval specified by *hold-interval* x $2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Precautions

You are advised to set the receiving interval specified by **lsa-arrival-interval** to be a value smaller than or equal to the Holdtime interval specified by**lsa-originate-interval**.

Example

Set the interval for receiving LSAs to 0 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] lsa-arrival-interval 0
```

7.4.61 lsa-originate-interval

Function

The **lsa-originate-interval** command sets an interval for updating LSAs.

The **undo lsa-originate-interval** command restores the default interval for updating LSAs.

By default, the interval for updating LSA packets is 5 seconds.

Format

lsa-originate-interval { **0** | { **intelligent-timer** *max-interval start-interval hold-interval* | **other-type** *interval* } * }

undo lsa-originate-interval

Parameters

Parameter	Description	Value
0	Sets an interval for updating LSAs to 0 ms, that is, deletes the initial interval (5000 ms) for updating LSAs.	-

Parameter	Description	Value
intelligent-timer	Enables an intelligent timer to update OSPF router LSAs and network LSAs.	-
max-interval	Specifies the maximum interval for updating OSPF LSAs.	The value is an integer ranging from 1 to 120000, in ms. The default value is 5000.
start-interval	Specifies the initial interval for updating OSPF LSAs.	The value is an integer that ranges from 0 to 60000, in ms. The default value is 500.
hold-interval	Specifies the Holdtime interval for updating OSPF LSAs.	The value is an integer ranging from 1 to 60000, in ms. The default value is 1000.
other-type	Sets the interval for updating the LSAs other than the OSPF router LSAs and network LSAs.	-
interval	Specifies the interval for updating LSAs.	The value is an integer ranging from 0 to 10, in seconds. The default value is 5.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent frequent LSA updates caused by network connection or frequent route flapping, you can set the interval for receiving LSAs using this command. A router receives LSAs only when it meets the set interval.

In a stable network where routes need to be fast converged, you can set the interval for receiving LSAs at millisecond level to update LSAs in time. The change of the topology or the route, therefore, can be immediately detected, and LSDB synchronization speed is improved.

If there is no special requirement for the network, using the default value is recommended.

Configuration Impact

After this command is configured, the interval for updating LSAs is as follows:

1. The initial interval for updating LSAs is specified by the parameter *start-interval*.
2. The interval for updating LSAs for the nth ($n \geq 2$) time is equal to *hold-interval* × $2^{(n-2)}$.
3. When the interval specified by *hold-interval* x $2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Precautions

You are advised to set the updating interval specified by **lsa-originate-interval** to be a value longer than or equal to the Holdtime interval specified by **lsa-arrival-interval**.

Example

Set the interval for updating LSAs to 0 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] lsa-originate-interval 0
```

7.4.62 lsdb-overflow-limit

Function

The **lsdb-overflow-limit** command sets the maximum number of external LSAs in an OSPF LSDB.

The **undo lsdb-overflow-limit** command restores the default configuration.

By default, the maximum number of external LSAs is not set.

Format

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of external LSAs in an LSDB.	The value is an integer ranging from 1 to 1000000.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of external LSAs (Type 5 and Type 7 LSAs) imported by OSPF exceeds the limit, the excessive external LSAs cannot be processed properly and are discarded.

To avoid the preceding problem, you can set the maximum number of external LSAs in the LSDB to adjust and optimize OSPF networks.

Prerequisites

If **OSPF is in LSDB overflow status** is displayed in the **display ospf lsdb brief** command output, you must run the **lsdb-overflow-limit** command to set the maximum number of external LSAs imported by OSPF.

Precautions

The configuration of this command must be consistent in the entire AS.

Example

Set a maximum number of 400000 external LSAs allowed in an LSDB.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] lsdb-overflow-limit 400000
```

7.4.63 maximum load-balancing (OSPF)

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the maximum number of equal-cost routes on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S6720S-S, and S5736-S is 8, and the maximum number of equal-cost routes on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S is 16.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

maximum load-balancing *number*

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes.	The value is an integer that ranges from 1 to 8 on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S and S6720S-S. The value ranges from 1 to 16 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a routing protocol discovers multiple routes with the same cost to a single destination, traffic can be balanced among these routes. The **maximum load-balancing** command sets the maximum number of equal-cost routes that can carry out load balancing. This optimizes the routing policy and ensures traffic forwarding on a complex network.

Configuration Impact

Packets will be balanced among multiple equal-cost routes to a single destination.

Follow-up Procedure

If more existing equal-cost OSPFv3 routes than the value set using the **maximum load-balancing** command are available, valid routes are selected for load balancing based on the following criteria:

- Route preference: Routes with lower preferences are selected for load balancing.
- Interface index: If routes have the same priorities, routes with higher interface index values are selected for load balancing.
- Next hop IP address: If routes have the same priorities and interface index values, routes with larger IP address are selected for load balancing.

The **nexthop** command allows routes with a specified weight to carry out load balancing.

Precautions

To disable load balancing, set the value of *number* to 1.

Example

Set the maximum number of the equal-cost routes.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] maximum load-balancing 2
```

Restore the default maximum number of equal-cost routes for carrying out load balancing.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] undo maximum load-balancing
```

7.4.64 maximum-routes

Function

The **maximum-routes** command sets the maximum number of routes of different types that OSPF supports.

The **undo maximum-routes** command restores the default maximum number of routes of different types that OSPF supports.

Format

maximum-routes { **external** | **inter** | **intra** } *number*

undo maximum-routes { **external** | **inter** | **intra** }

Parameters

Parameter	Description	Value
external	Indicates the maximum number of AS external routes that OSPF supports.	-
inter	Indicates the maximum number of inter-area routes that OSPF supports.	-
intra	Indicates the maximum number of intra-area routes that OSPF supports.	-
number	Specifies the maximum number of routes of different types.	The value is an integer. ● When the **external** parameter is specified, the value of *number* is an integer ranging from 100 to 5000000. ● When the **inter** parameter is specified, the value of *number* is an integer ranging from 100 to 1000000. ● When the **intra** parameter is specified, the value of *number* is an integer ranging from 100 to 100000.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the real world situation of a network, such as the convergence speed, you can run the **maximum-routes** command to configure the maximum number of routes of different types. This ensures full use of network resources and improves network performance.

Precautions

The maximum number of routes supported by OSPF cannot exceed the maximum number of all routes supported by the switch.

The **maximum-routes** command configuration limits the maximum number of routes that can be locally calculated. Therefore, the command configuration affects the maximum number of routes that can be sent, but does not affect the maximum number of LSAs that can be received.

Example

Set the maximum number of routes that OSPF supports.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] maximum-routes intra 500
```

7.4.65 mesh-group enable

Function

The **mesh-group enable** command enables the mesh-group function.

The **undo mesh-group enable** command disables the mesh-group function.

By default, the mesh-group function is disabled.

Format

mesh-group enable

undo mesh-group enable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When concurrent links exist between the device and its neighbor, the **mesh-group enable** command enables the mesh-group function. The router ID of a neighboring device uniquely identifies a mesh group. After LSAs are received, the device selects a primary link to flood the received LSAs, without performing reverse flooding. This prevents repeated flooding, reduces the load on the links, and saves system resources.

Device interfaces that meet the following conditions can form a mesh group:

- The interfaces belong to the same area and OSPF process.
- The neighbor status is Exchange or Full.
- Each interface is connected only to one neighbor.

Precautions

After the device is enabled with the mesh-group function, if the router IDs of the directly connected neighbor are the same, the LSDBs of the entire network cannot be synchronized and routes cannot be calculated correctly. In this case, you need to reconfigure the router ID of the neighbors, and then restart the neighbors to validate the configured router ID.

Example

Enable the mesh-group function on the switch.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] mesh-group enable
```

7.4.66 network (OSPF area)

Function

The **network** command specifies the interface that runs OSPF and the area to which the interface belongs.

The **undo network** command deletes the interface that runs OSPF.

By default, an interface does not belong to any area.

Format

network *network-address wildcard-mask* [**description** *text*]

undo network *network-address wildcard-mask*

Parameters

Parameter	Description	Value
network-address	Specifies the address of the network segment where the interface resides.	The value is in dotted decimal notation.
wildcard-mask	Specifies the wildcard mask of an IP address, which is the reverse form of the mask of the IP address. For example, 0.0.0.255 indicates that the mask length is 24 bits. **NOTE** When configuring a short mask, ensure that the area does not contain many interface addresses and secondary addresses. Otherwise, the neighbor relationship may fail to be established due to excessively long router-LSAs.	The value is in dotted decimal notation.

Parameter	Description	Value
description *text*	Specifies the description of the specified OSPF network segment.	The value is a string of 1 to 80 case-sensitive characters with spaces supported.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating an OSPF process, you can run the **network** command to configure the network segments in an area and specify *network-address* and *wildcard-mask* to configure one or multiple interfaces in an area. To run OSPF on an interface, ensure that the primary IP address of this interface is in the network segment range specified in the **network** (OSPF) command. If the secondary IP address of the main interface is in the network segment range specified in this command, the main interface cannot run OSPF.

OSPF can run on an interface only when the following two conditions are met:

- The mask length of the interface's IP address is not less than that specified in the **network** command. OSPF uses a reverse mask. For example, 0.0.0.255 indicates that the mask length is 24 bits.

  NOTE

  When the *wildcard-mask* parameter in the **network** command is set to all 0s, OSPF runs on the interface if its IP address is the IP address specified in the **network** *network-address* command.

- The primary address of the interface must be within the network segment range specified in the **network** command.

Precautions

- OSPF neighbor relationships cannot be established using the secondary IP addresses of interfaces.
- After the **network** 0.0.0.0 0.0.0.0 command is configured, the device automatically changes the command to **network** 0.0.0.0 255.255.255.255. That is, all interfaces (including the management interface) will run OSPF. Therefore, exercise caution when configuring this command.
- For the same **network** *address wildcard-mask*, the last description configured by **description** takes effect.

- On a loopback interface, by default, OSPF advertises its IP address in the form of a 32-bit host route, independent of the mask length of the IP address on the interface.
- To advertise the network segment route of a loopback interface, you need to run the **ospf network-type** command to set the network type to broadcast or NBMA.
- When an OSPF sham link is configured, the local address cannot be advertised through the OSPF process of a private network.
- Two areas that overlap cannot be configured between different processes in the same instance, or between different areas in the same process.
- The **ospf enable** command configuration takes precedence over the **network** command configuration.

Example

Configure the primary IP address of the interface that runs OSPF to be in the network segment of 192.168.1.0/24, set the ID of the OSPF area where the interface resides to 2, and configure the description for the network segment.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 2
[HUAWEI-ospf-100-area-0.0.0.2] network 192.168.1.0 0.0.0.255 description this network is connected to
Beijing
```

7.4.67 nexthop (OSPF)

Function

The **nexthop** command sets a preference for equal-cost routes. After OSPF calculates the equal-cost routes, the next hop is chosen from these equal-cost routes based on the value of weights. A smaller value indicates a higher preference.

The **undo nexthop** command cancels the preference of these equal-cost routes.

By default, the value of weight is 255. Equal-cost routes have no preference, and they forward packets at the same time. Load balancing is performed among them.

Format

nexthop *ip-address* **weight** *value*

undo nexthop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Indicates the IP address of the next hop.	The value is in dotted decimal notation.

Parameter	Description	Value
weight *value*	Indicates the weight of the next hop. A smaller value indicates a higher preference.	It is an integer that ranges from 1 to 254.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

You can run the **nexthop** command to set a high preference for specified valid routes if both of the following conditions are met:

- The number of equal-cost routes on a network is larger than the value configured using the **maximum load-balancing** command.
- Valid routes must be specified for load balancing.

Example

Set a preference for equal-cost routes in OSPF.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] nexthop 10.0.0.3 weight 1
```

7.4.68 nssa (OSPF Area)

Function

The **nssa** command configures an NSSA.

The **undo nssa** command cancels the configuration of an NSSA.

By default, no OSPF area is configured as an NSSA.

Format

nssa [{ **default-route-advertise** [**backbone-peer-ignore**] | **suppress-default-route** } | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding** | **translator-strict**] *

undo nssa [**flush-waiting-timer** *interval-value*]

Parameters

Parameter	Description	Value
default-route-advertise	Generates default Type7 LSAs on the ASBR and then advertises them to the NSSA. **NOTE** If the backbone-peer-ignore parameter is not configured, the ABR automatically generates a default NSSA LSA (Type7 LSA) and advertises it in the NSSA when an interface in the backbone area is in Up state and an OSPF neighbor relationship in Full state exists on the ABR. Type 7 LSAs carrying the default route will be generated only when the default route 0.0.0.0/0 exists in the routing table on the ASBR.	-
backbone-peer-ignore	Prevents the ABR from checking the neighbor status when the ABR generates default Type 7 LSAs and advertises them to the NSSA. Specifically, the ABR generates default Type 7 LSAs and advertises them to the NSSA as long as an interface that is Up exists in the backbone area.	-
suppress-default-route	Generates default Type-7 LSAs on the ASBR or ABR and then not advertises them to the NSSA.	-
flush-waiting-timer *interval-value*	Indicates the interval for an ASBR to send aged Type 5 LSAs. The parameter takes effect only when it is set.	The value is an integer that ranges from 1 to 40, in seconds.
no-import-route	Indicates that no external route is imported to an NSSA.	-
no-summary	Indicates that an ABR is prohibited from sending summary LSAs to the NSSA.	-
set-n-bit	Sets the N-bit in DD packets.	-
suppress-forwarding-address	Sets the FA of the Type 5 LSAs translated from Type 7 LSAs by the NSSA ABR to 0.0.0.0.	-
translator-always	Specifies an ABR in an NSSA as an all-the-time translator. Multiple ABRs in an NSSA can be configured as translators.	-

Parameter	Description	Value
translator-interval *interval-value*	Specifies the timeout period of a translator.	The value is an integer ranging from 1 to 120, in seconds. The default value is 40.
zero-address-forwarding	Sets the FA of the generated NSSA LSAs to 0.0.0.0 when external routes are imported by the ABR in an NSSA.	-
translator-strict	Configures the translator to perform strict check on the P-bit flag. The translator determines whether to translate Type 7 LSAs into Type 5 LSAs based on the P-bit flag.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NSSA is configured in the scenario where AS external routes are to be imported but not forwarded to save system resources. AS external routes can be imported to an NSSA and transmitted to the entire NSSA.

All switches in the NSSA must be configured with NSSA attributes using the **nssa** command.

The **nssa** command is applicable to the following scenarios:

- The **default-route-advertise** parameter is configured to advertise Type 7 LSAs carrying the default route on the ASBR to the NSSA.

  Regardless of whether the default route 0.0.0.0/0 exists in the routing table on the ABR, Type 7 LSAs carrying the default route will be generated. However, Type 7 LSAs carrying the default route will be generated on the ASBR only when the default route 0.0.0.0/0 exists in the routing table on the ASBR.

- When the area to which the ASBR belongs is configured as an NSSA, invalid Type 5 LSAs from other switches in the area where LSAs are flooded will be reserved. These LSAs will be deleted only when the aging time reaches 3600s. The switch performance is affected because the forwarding of a large number of LSAs consumes the memory resources. To resolve such a problem, you can set the parameter **flush-waiting-timer** to the maximum value 3600s for Type 5 LSAs. This ensures that the invalid Type 5 LSAs from other switches can be deleted in time.

NOTE

- When the LS age field value (aging time) in the header of an LSA reaches 3600s, the LSA is deleted.
- If an ASBR also functions as an ABR, **flush-waiting-timer** does not take effect. This prevents Type 5 LSAs in the non-NSSAs from being deleted.

- If an ASBR also functions as an ABR, the **no-import-route** parameter is configured to prevent external routes imported using the **import-route** command from being advertised to the NSSA.
- The **no-summary** parameter is configured on an ABR to reduce the number of LSAs that are transmitted to the NSSA. This implementation prevents the ABR from transmitting Type 3 LSAs to the NSSA.

  NOTE

  After the **nssa default-route-advertise backbone-peer-ignore no-summary** command is run, the ABR generates default Type 7 and Type 3 LSAs as long as an interface that is Up exists in the backbone area. The default Type 3 LSAs preferentially take effect.
- After the **set-n-bit** parameter is configured, the N-bit is set in the database description (DD) packets during the synchronization between the switch and neighboring switches.
- If multiple ABRs are deployed in the NSSA, the system automatically selects an ABR (generally the switch with the largest router ID) as a translator to convert Type 7 LSAs into Type 5 LSAs. You can configure the **translator-always** parameter on an ABR to specify the ABR as an all-the-time translator. To specify two ABRs for load balancing, configure the **translator-always** parameter on the chosen ABRs to specify the ABRs as all-the-time translators. You can use this command to pre-configure a fixed translator to prevent LSA flooding caused by translator role changes.
- The **translator-interval** parameter is used to ensure uninterrupted services when translator roles change. The value of *interval-value* must be greater than the flooding period.

Configuration Impact

Configuring or deleting NSSA attributes will trigger routing updates in the area. A second configuration of NSSA attributes can be implemented or canceled only after a routing update is complete.

Precautions

It is recommended that a loopback address be configured for a device in the NSSA and be enabled in the corresponding OSPF area, so that the loopback address can be automatically selected as the FA. If other switches have routes of the same cost to the switch in the NSSA, load balancing is performed.

When the last ordinary area (other than a stub area or NSSA) under an OSPF process is deleted, useless Type 5 LSAs originated by the local switch in the area where LSAs are flooded will be deleted immediately. The local switch still reserves useless Type 5 LSAs from other switches. These useless Type 5 LSAs will be deleted only when the aging time reaches 3600s.

Example

Configure area 1 as an NSSA.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] area 1
[HUAWEI-ospf-1-area-0.0.0.1] nssa
```

7.4.69 opaque-capability enable

Function

The **opaque-capability enable** command enables the Opaque-LSA capability so that an OSPF process can generate Opaque LSAs and receive Opaque LSAs from neighbors.

The **undo opaque-capability** command disables the Opaque-LSA capability.

By default, the Opaque-LSA capability is disabled.

Format

opaque-capability enable

undo opaque-capability

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Opaque LSAs provide a generic mechanism for OSPF extension:

- OSPF supports GR using Type 9 LSAs.
- OSPF supports TE using Type 10 LSAs.

Before configuring OSPF GR or OSPF TE, you must enable opaque LSA capability running the **opaque-capability enable** command.

Configuration Impact

Enabling or disabling the opaque LSA function may delete and re-establish all sessions and instances.

Example

Enable OSPF opaque-lsa.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] opaque-capability enable
```

7.4.70 ospf

Function

The **ospf** command creates and runs an OSPF process.

The **undo ospf** command terminates an OSPF process.

By default, OSPF is disabled, that is, no OSPF process runs.

Format

ospf [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *

undo ospf *process-id* [**flush-waiting-timer** *time*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535. By default, it is 1.
router-id *router-id*	Specifies a router ID.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
flush-waiting-timer *time*	Indicates the interval for generating aged LSAs. The parameter takes effect only when it is set.	The value is an integer that ranges from 1 to 40, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set OSPF parameters only after creating an OSPF process.

OSPF supports multi-process. More than one OSPF process can run on the same device and are independent of each other. Route interaction between different OSPF processes is similar to route interaction between different routing protocols.

An OSPF router ID can be manually configured or automatically selected. To ensure OSPF stability, you are advised to manually configure the IP address of a loopback interface as the router ID.

If no OSPF router ID is manually configured for a router, the router selects the global router ID as its OSPF router ID. If both the OSPF router ID and global router ID are not configured, the router selects a router ID based on IP addresses of current interfaces:

- If there are loopback interfaces that have IP addresses configured, the device selects the largest IP address among loopback interface addresses as the global router ID.
- If no loopback interface is configured or loopback interfaces do not have IP addresses configured, the device selects the largest IP address among interface addresses as the global router ID without considering the Up/Down state of interfaces.

In any of the following situations, the router ID is re-selected:

- The **ospf** command is run to re-configure an OSPF router ID, and the OSPF process is restarted.
- The global router ID is re-configured, and the OSPF process is restarted.
- The IP address of the original global router ID is deleted, and the OSPF process is restarted.

Configuration Impact

After an OSPF process is disabled using **undo ospf** command, the receive end still maintains the LSAs generated by this OSPF process. These invalid LSAs occupy the system memory and are deleted only when the LS age field (aging time) reaches 3600 seconds. When the **undo ospf** *process-id* **flush-waiting-timer** *time* command is used to delete an OSPF process, the switch regenerates an LSA in the set time and sets the LS age field to 3600 seconds. After other switches receive the LSA with the LS age field as 3600 seconds, they delete the LSA immediately. If the host does not send all the LSAs in the set time, other switches still reserve invalid LSAs.

NOTE

When the LS age field (aging time) in the LSA header reaches 3600 seconds, this LSA is deleted.

Precautions

An interface on a device belongs to only one OSPF process.

If a VPN instance is specified, the OSPF process specified in this command belongs to this VPN instance. If no VPN instance is specified, the OSPF process specified in this command belongs to the global VPN instance. *vpn-instance-name* cannot be changed after being specified.

NOTE

The router ID of each OSPF process must be unique on the entire network; otherwise, the OSPF neighbor relationship cannot be set up and routing information is incorrect. Configuring a unique router ID for each OSPF process on each OSPF device is recommended.

Example

Run an OSPF process.

```
<HUAWEI> system-view
[HUAWEI] ospf 100 router-id 10.10.10.1 vpn-instance test
```

7.4.71 ospf authentication-mode

Function

The **ospf authentication-mode** command sets an authentication mode and password used between neighboring nodes.

The **ospf authentication-mode null** command configures the null authentication mode on an interface.

The **undo ospf authentication-mode** command deletes the authentication mode on an interface.

By default, an interface does not authenticate OSPF packets.

Format

ospf authentication-mode { **simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | **null** }

ospf authentication-mode { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]

ospf authentication-mode keychain *keychain-name*

undo ospf authentication-mode

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
simple	Indicates simple authentication. **NOTICE** Simple authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	In simple authentication, the password type is **cipher** by default.
plain	Indicates plain authentication. Only plain text can be entered, and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This carries security risks. Selecting **cipher** to save the password in cipher text is recommended.	-
plain-text	Specifies a plain text password.	*plain-text* is a string of 1 to 8 characters without spaces when **simple** is configured, and is a string of 1 to 255 characters without spaces when **md5**, **hmac-md5** or **hmac-sha256** is configured.
cipher	Indicates cipher authentication. Either plain text or cipher text can be entered, and cipher text is displayed when the configuration file is viewed.	When **cipher** is configured, enter only the password in cipher text. Then, the password is displayed in cipher text in configuration files. MD5 authentication, HMAC-SHA256 authentication or HMAC-MD5 authentication uses the password in cipher text by default.

Parameter	Description	Value
cipher-text	Specifies a cipher text password.	The value is a string of characters without spaces. In simple authentication, a plain text password is a string of 1 to 8 characters and a cipher text password is a string of 24 or 32 or 48 characters. In MD5 authentication, HMAC-SHA256 authentication or HMAC-MD5 authentication, a plain text password is a string of 1 to 255 characters and a cipher text password is a string of 20 to 392 characters.
md5	Indicates MD5 authentication. **NOTICE** MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates HMAC-MD5 authentication. **NOTICE** HMAC-MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates HMAC-SHA256 authentication.	-
key-id	Specifies the authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, OSPF supports only HMAC-MD5 and HMAC-SHA256 algorithms.	-
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
null	Indicates null authentication.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to the defects and non-strict implementation of the TCP/IP protocol suite and increasing attacks on TCP/IP networks, the impact generated by attacks on the network may become more serious. Attacks on network devices may lead to a network crash. To improve OSPF network security, configure authentication.

Configuration Impact

Interface authentication is used to set the authentication mode and password used between neighboring devices. It takes precedence over area authentication.

Precautions

Null authentication is an authentication method. It does not indicate that no authentication is configured.

The authentication mode and password configured for interfaces on the same network segment must be the same.

OSPF does not support the configuration on a null interface.

An authentication password cannot contain spaces.

Example

Configure OSPF HMAC-SHA256 authentication on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf authentication-mode hmac-sha256
```

Configure OSPF HMAC-SHA256 authentication on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf authentication-mode hmac-sha256
```

7.4.72 ospf bfd

Function

The **ospf bfd** command enables BFD on an OSPF interface or sets parameter values for a BFD session.

The **undo ospf bfd** command deletes BFD on an OSPF interface or restores the default parameter values of a BFD session.

By default, BFD is not enabled on any OSPF interfaces.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ospf bfd enable

undo ospf bfd enable

ospf bfd { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } *

undo ospf bfd { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **frr-binding** parameter.

Parameters

Parameter	Description	Value
enable	Enables BFD.	-
min-rx-interval *receive-interval*	Indicates the minimum interval at which BFD packets are received from the remote end.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *transmit-interval*	Indicates the minimum interval at which BFD packets are sent to the remote end.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Specifies the local detection multiplier.	The value is an integer ranging from 3 to 50. By default, it is 3.

Parameter	Description	Value
frr-binding	Binds the BFD status to the link status of an interface. That is, when the BFD status goes Down, the link status of the interface also goes Down. This enables traffic to be switched to the backup path.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A link failure or topology change causes devices to recalculate routes. Therefore, the convergence of routing protocols must be sped up to improve network performance.

Link faults are unavoidable. Therefore, a feasible solution is required to detect faults faster and notify routing protocols of the faults immediately. If BFD is associated with routing protocols and a link fault occurs, BFD can speed up the convergence of routing protocols.

Prerequisites

The configured parameters of the BFD session are valid on an interface only when BFD is enabled on the interface.

Procedure

The *receive-interval* is obtained through the negotiation between the local end and peer end by comparing the values of the local **min-rx-interval** and the peer **min-tx-interval**. If the local end fails to receive a BFD packet from the peer end within an interval of *receive-interval* x *multiplier-value*, it considers that the neighbor is Down.

Configuration Impact

If global BFD is not enabled, you can enable BFD on an interface but cannot set up BFD sessions. Similarly, if only parameters of a BFD session are set but the **ospf bfd enable** command is not used, the BFD session cannot be set up.

BFD configured on an interface takes precedence over BFD configured in a process. If BFD is enabled on an interface, the BFD parameters on the interface are used to establish BFD sessions.

Precautions

- After BFD is enabled, BFD sessions can be created only between the two ends that have set up an OSPF neighbor relationship and the relationship is in the Exstart state.
- The **ospf bfd enable** command and the **ospf bfd block** command are mutually exclusive.
- After BFD is disabled from an interface through the **undo ospf bfd enable** command, the parameters for setting up BFD sessions remain on this interface but do not take effect.

Example

Enable BFD on VLANIF100 and set the minimum interval for receiving BFD packets to 400 ms and the local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf bfd enable
[HUAWEI-Vlanif100] ospf bfd min-rx-interval 400 detect-multiplier 4
```

Enable BFD on GE0/0/1 and set the minimum interval for receiving BFD packets to 400 ms and the local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf bfd enable
[HUAWEI-GigabitEthernet0/0/1] ospf bfd min-rx-interval 400 detect-multiplier 4
```

7.4.73 ospf bfd block

Function

The **ospf bfd block** command prevents an interface from dynamically setting up a BFD session.

The **undo ospf bfd block** command cancels the configuration.

By default, the device does not prevent an interface from dynamically setting up a BFD session.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ospf bfd block

undo ospf bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **bfd all-interfaces enable** command is used for an OSPF process, BFD sessions are created on all OSPF interfaces whose neighbor status is Full. If you do not want some interfaces to have BFD sessions created, run the **ospf bfd block** command to prevent these interfaces from dynamically setting up BFD sessions.

Prerequisites

BFD has been enabled on interfaces.

Precautions

The **ospf bfd enable** command and the **ospf bfd block** command are mutually exclusive.

Example

Prevent VLANIF100 from dynamically setting up a BFD session.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf bfd block
```

Prevent GE0/0/1 from dynamically setting up a BFD session.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf bfd block
```

7.4.74 ospf cost

Function

The **ospf cost** command sets a cost for an OSPF on an interface.

The **undo ospf cost** command restores the default cost for OSPF.

By default, OSPF automatically calculates its cost based on its interface bandwidth. The default cost of the loopback interface is 0.

Format

ospf cost *cost*

undo ospf cost

Parameters

Parameter	Description	Value
cost	Specifies the cost of an OSPF-enabled interface.	The value is an integer ranging from 1 to 65535. By default, it is 1.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, OSPF automatically calculates the link cost for an interface based on the bandwidth of the interface. You can modify the interface cost using the **ospf cost** command. For example, when you configure load balancing, you can run this command to modify the interface cost of the routes if conditions are satisfied for load balancing.

If no cost is set for an OSPF interface using the **ospf cost** command, OSPF automatically calculates its cost based on the interface bandwidth. The calculation formula is as follows: Cost of the interface = Bandwidth reference value/Interface bandwidth. The integer of the calculated result is the cost of the interface. If the calculated result is smaller than 1, the cost is 1. Changing the bandwidth reference value or interface bandwidth change the cost of an interface:

- To use the bandwidth reference value to determine the interface cost, run the **bandwidth-reference** command.
- To use the interface bandwidth to determine the interface cost, run the **bandwidth** command to set configuration bandwidth for an interface, and then run the **bandwidth-config enable** command to enable the device to calculate the cost for the interface based on the configuration bandwidth of the interface.
- To use both the bandwidth reference value and interface bandwidth to determine the interface cost, run the preceding three commands.

Precautions

- The **ospf cost** command cannot run on null interfaces.
- No default cost is configured for trunk interfaces, because a trunk interface has multiple member interfaces that are in constant change.

Example

Set the cost of VLANIF100 that runs OSPF to 65.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf cost 65
```

Set the cost of GE0/0/1 that runs OSPF to 65.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf cost 65
```

7.4.75 ospf dr-priority

Function

The **ospf dr-priority** command sets a priority for an interface that participates in the DR election.

The **undo ospf dr-priority** command restores the default setting.

By default, the priority is 1.

Format

ospf dr-priority *priority*

undo ospf dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of an interface that participates in the DR or BDR election. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DR priority of an interface determines whether it is qualified to be a DR. The interface with the highest DR priority is elected as the DR. If the DR priority of an interface on a device is 0, the device cannot be elected as a DR or a BDR. On a broadcast or NBMA network, you can set a DR priority for an interface to determine whether it is qualified to be a DR or a BDR.

Configuration Impact

When the DR and BDR are elected on a network segment, they send DD packets to all neighboring nodes and set up adjacencies with all neighboring nodes.

Precautions

NOTICE

Restarting or shutting down an interface will interrupt the OSPF adjacency between devices. Therefore, perform the operation with caution.

If the DR priority of a device is re-configured, the DR or BDR on the network will not be re-elected. You can re-elect a DR or a BDR by using either of the following methods. This, however, will interrupt the OSPF adjacency between devices. Therefore, use the following methods with caution.

- Restart the OSPF processes on all devices.
- Run the **shutdown** and then **undo shutdown** commands on the interfaces where OSPF adjacencies are set up.

In OSPF, the DR priority cannot be configured for null interfaces.

Example

Set the priority of VLANIF100 that participates in the DR election to 8.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf dr-priority 8
```

Set the priority of GE0/0/1 that participates in the DR election to 8.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf dr-priority 8
```

7.4.76 ospf enable

Function

The **ospf enable** command enables OSPF on an interface.

The **undo ospf enable** command disables OSPF on an interface.

By default, the interface does not run OSPF.

Format

ospf enable [*process-id*] **area** *area-id*

undo ospf enable [*process-id*] **area** *area-id*

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535. The default value is 1.
area *area-id*	Specifies an area ID.	The value can be a decimal integer or an IP address. When the value is an integer, the value ranges from 0 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ospf enable** command configuration takes precedence over the **network** command configuration.

After the **undo ospf enable** command is run to disable OSPF on an interface, the **network** configuration takes effect on the interface automatically.

Configuration Impact

The interface will alternate between Up and Down when the **ospf enable** command and the **network** command are run on the interface repeatedly.

Precautions

An interface can be configured with only one OSPF process.

The configured interface and the OSPF process must be in the same VPN.

- The **ospf enable** command can be configured on an interface before an OSPF process is created. The interface specified by the **ospf enable** command and the created OSPF process must be in the same VPN.
- If a process is created before the **ospf enable** command is run on an interface, the process of the interface and existing process must belong to the same VPN. Otherwise, the **ospf enable** command cannot be run.
- If no OSPF process is created, interfaces that belong to different VPN instances cannot be added to the same OSPF process.

Example

Enable VLANIF100 in the specified OSPF area.

```
<HUAWEI> system-view
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf enable 1 area 0
```

Enable GE0/0/1 in the specified OSPF area.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf enable 1 area 0
```

7.4.77 ospf filter-lsa-out

Function

The **ospf filter-lsa-out** command configures an OSPF interface to filter outgoing LSAs.

The **undo ospf filter-lsa-out** command disables an OSPF interface from filtering outgoing LSAs.

By default, outgoing LSAs are not filtered.

Format

ospf filter-lsa-out { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }] | **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** { *acl-number* | *acl-name* }] } * }

undo ospf filter-lsa-out

Parameters

Parameter	Description	Value
all	Filters all outgoing LSAs except grace LSAs.	-
summary	Filters outgoing network summary LSAs (Type3).	-
ase	Filters outgoing AS external LSAs (Type5).	-
nssa	Filters outgoing NSSA LSAs (Type7).	-
acl *acl-number*	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between two switches, you can run the **ospf filter-lsa-out** command to configure the local switch to filter the outgoing LSAs based on the filtering policy before the device sends these LSAs along specified links. This reduces the unnecessary retransmission of LSAs and saves bandwidth resources.

Configuration Impact

Filtering the outgoing LSAs on the specified OSPF interface can prevent useless LSAs from being sent to neighbors. This can reduce the size of the LSDB of neighbors and speed up the network convergence.

NOTE

- After the command is configured on an interface, the OSPF neighbor relationship of the interface will automatically re-establish.
- When the rule in the ACL changes, the OSPF neighbor relationship of the interface will automatically re-establish.

Precautions

When the **rule** command is used to configure the filtering rules for an ACL configured using the **acl** command, only the source address range that is specified by the **source** parameter and the period of time that is specified by the **time-range** parameter take effect.

Grace LSAs are used to inform the neighbor of the Graceful Restart (GR) time, cause, and interface instance ID when GR starts and ends. The command is not used to filter the grace LSAs.

Example

Configure VLANIF100 to filter all outgoing LSAs except grace LSAs.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf filter-lsa-out all
```

Configure GE0/0/1 to filter all outgoing LSAs except grace LSAs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf filter-lsa-out all
```

7.4.78 ospf frr block

Function

The **ospf frr block** command disables the OSPF IP FRR function on a specified interface.

The **undo ospf frr block** command restores the OSPF IP FRR function on the specified interface.

By default, the OSPF IP FRR function is enabled on a specific interface.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ospf frr block

undo ospf frr block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

OSPF IP FRR can be disabled using the **ospf frr block** command on an interface of a specific device that is running important services and resides on an FRR backup link. This setting prevents the device connected to this interface from being a part of a backup link and being burdened after FRR switches traffic to the backup link.

Example

Disable the OSPF IP FRR function on the interface VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ospf frr block
```

7.4.79 ospf maxage-lsa auto-protect disable

Function

The **ospf maxage-lsa auto-protect disable** command disables master/slave board switching triggered by abnormal OSPF LSA aging.

The **undo ospf maxage-lsa auto-protect disable** command enables master/slave board switching triggered by abnormal OSPF LSA aging.

By default, master/slave board switching triggered by abnormal OSPF LSA aging is enabled.

Format

ospf maxage-lsa auto-protect disable

undo ospf maxage-lsa auto-protect disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the local device clock is faster than usual and the aging timer expires abnormally, the local device incorrectly clears all Router LSAs from the peer device, which causes route flapping and service interruptions. To resolve this issue, master/slave board switching triggered by abnormal OSPF LSA aging is automatically enabled. Master/Slave board switching is triggered to restore network connections and service traffic when the following condition is met:

(Number of incorrectly cleared Router LSAs/Total number of Router LSAs) x 100% ≥ 80% (Router LSAs are those sent by the peer device to the local device)

Example

Disable master/slave board switching triggered by abnormal OSPF LSA aging.

```
<HUAWEI> system-view
```

```
[HUAWEI] ospf maxage-lsa auto-protect disable
```

7.4.80 ospf mib-binding

Function

The **ospf mib-binding** command binds an OSPF process to SNMP and enables OSPF to respond to SNMP requests.

The **undo ospf mib-binding** command cancels the binding.

By default, OSPF processes are not bound to SNMP.

Format

ospf mib-binding *process-id*

undo ospf mib-binding

Parameters

Parameter	Description	Value
process-id	Specifies an OSPF process ID.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The OSPF MIB is a virtual database of the device status maintained by the managed devices.

Before performing read and write operations on the OSPF MIB, you must run the **ospf mib-binding** *process-id* command to bind a specified OSPF process to SNMP.

Prerequisites

An OSPF process has been created using the **ospf** command in the system view.

Example

Bind OSPF process 100 to SNMP.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] quit
```

```
[HUAWEI] ospf mib-binding 100
```

Cancel the binding.

```
<HUAWEI> system-view
[HUAWEI] undo ospf mib-binding
```

7.4.81 ospf mtu-enable

Function

The **ospf mtu-enable** command enables an interface to add its actual MTU in DD packets to be sent and check whether the MTU in a received DD packet is greater than the local MTU.

The **undo ospf mtu-enable** command restores the default settings.

By default, an interface adds the MTU 0 (not the actual MTU) in DD packets to be sent and does not check the MTUs in received DD packets.

Format

ospf mtu-enable

undo ospf mtu-enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve compatibility with a non-Huawei device, an OSPF-enabled Huawei device adds the MTU 0 in DD packets to be sent and does not check the MTUs in received DD packets, allowing an OSPF neighbor relationship to be set up even if the two ends have different MTU settings.

However, under the default configuration, the non-Huawei device may discard an OSPF packet received from the Huawei device if the packet's actual MTU is greater than the MTU of the non-Huawei device. If the discarded packet is an LSU, an OSPF neighbor relationship can still be set up, but the route carried in the LSU fails to be learned, causing service interruptions.

To resolve this issue, run the **ospf mtu-enable** command to configure an interface to add the actual MTU in DD packets to be sent and check whether the MTU in a received DD packet is greater than the local MTU. If the interface MTU settings of the local and remote ends are different, an OSPF neighbor relationship cannot enter the Full state. In this manner, MTU inconsistency can then be identified in time.

Precautions

OSPF does not support the configuration on a null interface.

After the command is configured, the system automatically restarts the OSPF process.

Example

Set Vlanif100 to fill in the MTU field when sending DD packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf mtu-enable
```

Set GigabitEthernet0/0/1 to fill in the MTU field when sending DD packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf mtu-enable
```

7.4.82 ospf network-type

Function

The **ospf network-type** command sets a network type for an OSPF interface.

The **undo ospf network-type** command restores the default network type of the OSPF interface.

By default, the network type of an interface is determined by the physical interface. The network type of Ethernet interfaces is **broadcast**.

Format

ospf network-type { **broadcast** | **nbma** | **p2mp** | **p2p** [**peer-ip-ignore**] }

undo ospf network-type

Parameters

Parameter	Description	Value
broadcast	Indicates that the network type of the interface is changed to broadcast.	-
nbma	Indicates that the network type of the interface is changed to NBMA.	-
p2mp	Indicates that the network type of the interface is changed to point-to-multipoint.	-

Parameter	Description	Value
p2p	Indicates that the network type of the interface is changed to point-to-point.	-
peer-ip-ignore	Disables network segment check when IP address unnumbered is not configured for a P2P interface changed from a broadcast interface and the interface tries to establish an OSPF neighbor relationship. By default, if **peer-ip-ignore** is not specified in the command, OSPF checks the network segment of the two ends during which an OSPF neighbor relationship is to be established. Specifically, OSPF performs an AND operation on the local subnet mask and the local IP address, and on the local subnet mask and the remote IP address. An OSPF neighbor relationship can be established only when the results on the two ends are the same.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link layer protocols remain unchanged, you can change network types and configure OSPF features to flexibly build networks.

- In the broadcast network, if there is a device that does not support multicast address, you can change the network type of the interface to NBMA.
- If the network type of the interface is NBMA, when the interface type is changed to broadcast, neighbor relationships do not need to be configured.

The condition for changing an NBMA network to broadcast network is that there must be a direct virtual circuit between any two devices, and the network must be a full mesh network.

If a network does not meet the preceding conditions, you must change the type of network to point-to-multipoint. In this manner, two indirect devices can communicate with the help of one device directly connected to the two devices. Instead of configuring the neighboring device, you can change the network type of the interface to point-to-multipoint.

If there are only two devices that run OSPF in the same network segment, the network type of an interface can be changed to p2p.

Precautions

- OSPF does not support the configuration on a null interface.
- When the network type of an interface is NBMA or the network type of an interface is changed to NBMA manually, you must run the **peer** command to configure the neighbor.
- If the network type of an OSPF interface is NBMA, OSPF does not advertise the interface's information to RSVP-TE, and TE tunnels passing through this interface fail to go Up.
- Generally, the network type of two OSPF interfaces on both ends of the link must be identical. Otherwise, the two interfaces cannot set up the neighbor relationship.

  Only when the network type of one OSPF interface is broadcast and the network type of the other OSPF interface is P2P or P2MP, the two interfaces can still set up the neighbor relationship, but cannot learn the OSPF routing information each other.

Example

Set network type of VLANIF100 to NBMA.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf network-type nbma
```

Set network type of GE0/0/1 to NBMA.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf network-type nbma
```

7.4.83 ospf p2mp-mask-ignore

Function

The **ospf p2mp-mask-ignore** command disables a device from checking the network mask on a Point-to-Multipoint (P2MP) network.

The **undo ospf p2mp-mask-ignore** command configures the device to check the network mask on a P2MP network.

By default, devices on a P2MP network do not check the network mask.

Format

ospf p2mp-mask-ignore

undo ospf p2mp-mask-ignore

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF checks the network masks carried in Hello packets. If the network mask carried in a received Hello packet is not the same as the network mask of the local device, the Hello packet is discarded.

On a P2MP network, when the mask lengths of devices are different, you can use the **ospf p2mp-mask-ignore** command on devices to disable them from checking the network mask in Hello packets. In this manner, the OSPF neighbor relationship can be established.

Prerequisites

Because P2MP is not a link layer protocol, each P2MP network is forcibly changed from a network of another type. A common P2MP network is changed from a non-fully connected non-broadcast multiple access (NBMA) network through the **ospf network-type p2mp** command.

Example

Disable a device from checking the network mask on a P2MP network.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf network-type p2mp
[HUAWEI-Vlanif100] ospf p2mp-mask-ignore
```

Disable a device from checking the network mask on a P2MP network.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf network-type p2mp
[HUAWEI-GigabitEthernet0/0/1] ospf p2mp-mask-ignore
```

7.4.84 ospf router-id auto-recover disable

Function

The **ospf router-id auto-recover disable** command disables a device from performing automatic recovery after detecting router ID conflict.

The **undo ospf router-id auto-recover disable** command enables a device to perform automatic recovery after detecting router ID conflict.

By default, a device performs automatic recovery after detecting router ID conflict.

Format

ospf router-id auto-recover disable

undo ospf router-id auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If router ID conflict occurs in an OSPF area, the system can define a new router ID, preventing route flapping and reducing route calculation operations. Other protocols will not go Down when the CPU usage is controlled.

NOTE

- If the automatic recovery function is enabled and a router ID conflict occurs between indirectly connected routers in one OSPF area, the system replaces the conflicted router ID with a newly calculated one. The automatic recovery function takes effect on both configured and automatically generated router IDs.
- The system can replace a router ID in a maximum of three attempts in case the router ID conflict persists.

Example

Disable a device from performing automatic recovery after detecting router ID conflict.

```
<HUAWEI> system-view
[HUAWEI] ospf router-id auto-recover disable
```

7.4.85 ospf smart-discover

Function

The **ospf smart-discover** command enables smart-discover on an interface.

The **undo ospf smart-discover** command disables smart-discover on an interface.

By default, smart-discover is disabled on interfaces.

Format

ospf smart-discover

undo ospf smart-discover

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, devices periodically send Hello packets through OSPF interfaces. By sending Hello packets, devices set up and maintain neighbor relationships, and elect the DR and BDR on the multi-access network (broadcast or NBMA network). When setting up neighbor relationships or electing the DR and BDR on the multi-access network, interfaces send Hello packets only when the Hello timer expires. This slows down the establishment of neighbor relationships and election of the DR and BDR.

After smart-discover is configured, when the status of the neighbor relationship changes or the DR and BDR on the multi-access network changes, the device sends Hello packets to its neighbor immediately without waiting for the expiration of the Hello timer.

Procedure

On broadcast and NBMA networks, neighbor relationships can be rapidly set up and a DR and a BDR can be rapidly elected.

- When the neighbor status becomes 2-way for the first time or returns to Init from the 2-way or higher state, the smart-discover-enabled interface sends Hello packets to a neighbor without waiting for the expiration of the Hello timer when detecting that the neighbor status changes.
- When the status of the interface functioning as the DR or BDR on the multi-access network changes, the smart-discover-enabled interface actively sends Hello packets on the network segment and then participates in the DR or BDR election.

The principle of setting up adjacencies rapidly on P2P or P2MP networks is the same as that on broadcast and NBMA networks.

Configuration Impact

The interval for sending Hello packets on an interface is determined by the interval for sending Hello packets set on the interface.

Precautions

The default interval for sending Hello packets varies with the network type.

Example

Enable smart-discover on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf smart-discover
```

Enable smart-discover on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf smart-discover
```

7.4.86 ospf suppress-flapping peer

Function

The **ospf suppress-flapping peer** command configures detection parameters for OSPF neighbor relationship flapping suppression.

The **undo ospf suppress-flapping peer** command restores the default detection parameters.

By default, the detection interval of OSPF neighbor relationship flapping suppression is 60s, the suppression threshold is 10, and the interval for exiting from suppression is 120s.

Format

ospf suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

undo ospf suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

Parameters

Parameter	Description	Value
detecting-interval *detecting-interval*	Specifies a detection interval for OSPF neighbor relationship flapping suppression. Each OSPF interface on which OSPF neighbor relationship flapping suppression is enabled starts a flapping counter. If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count is incremented by 1.	The value is an integer ranging from 1 to 300, in seconds. The default value is 60s.
threshold *threshold*	Specifies the threshold of OSPF neighbor relationship flapping suppression. When the flapping-count reaches or exceeds *threshold*, flapping suppression takes effect.	The value is an integer ranging from 1 to 1000. The default value is 10.

Parameter	Description	Value
resume-interval *resume-interval*	Specifies an interval for exiting from OSPF neighbor relationship flapping suppression. If the interval between two successive neighbor status changes from Full to a non-Full state is longer than *resume-interval*, the flapping-count is reset. **NOTE** The value of *resume-interval* must be greater than that of *detecting-interval*.	The value is an integer ranging from 2 to 1000, in seconds. The default value is 120s.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure detection parameters for OSPF neighbor relationship flapping suppression on an interface, run the **ospf suppress-flapping peer** command. However, keeping the default configurations is recommended.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you configure detection parameters for it. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the detection parameters.

Example

Set the detection interval of OSPF neighbor relationship flapping suppression to 5s, the suppression threshold to 40, and the interval for exiting from suppression to 20s on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf suppress-flapping peer detecting-interval 5 threshold 40 resume-interval 20
```

7.4.87 ospf suppress-flapping peer disable

Function

The **ospf suppress-flapping peer disable** command disables OSPF neighbor relationship flapping suppression on an interface.

The **undo ospf suppress-flapping peer disable** command enables OSPF neighbor relationship flapping suppression on an interface.

By default, OSPF neighbor relationship flapping suppression is enabled on all interfaces.

Format

ospf suppress-flapping peer disable

undo ospf suppress-flapping peer disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, OSPF neighbor relationship flapping suppression is enabled on all interfaces in the same OSPF process. To disable the function on one of the interfaces, run the **ospf suppress-flapping peer disable** command.

NOTE

When an interface enters the flapping suppression state, all neighbor relationships on the interface enter the state accordingly.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you enable the function on an interface using the **undo ospf suppress-flapping peer disable** command. By default, the function is enabled globally. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it.

Example

Disable OSPF neighbor relationship flapping suppression on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf suppress-flapping peer disable
```

7.4.88 ospf suppress-flapping peer hold-down

Function

The **ospf suppress-flapping peer hold-down** command configures the Hold-down mode and sets a duration for this mode.

The **undo ospf suppress-flapping peer hold-down** command cancels the Hold-down mode.

By default, the Hold-down mode is disabled.

Format

ospf suppress-flapping peer hold-down *interval*

undo ospf suppress-flapping peer hold-down [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies a duration for the Hold-down mode.	The value is an integer ranging from 1 to 600, in seconds. The default value is 60.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set a duration for this mode, run the **ospf suppress-flapping peer hold-down** command.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you configure the Hold-down mode and set a duration for this mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it.

Example

Configure the Hold-down mode and set its duration to 200s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf suppress-flapping peer hold-down 200
```

7.4.89 ospf suppress-flapping peer hold-max-cost disable

Function

The **ospf suppress-flapping peer hold-max-cost disable** command disables the Hold-max-cost mode.

The **undo ospf suppress-flapping peer hold-max-cost disable** command enables the Hold-max-cost mode.

By default, the Hold-max-cost mode is enabled.

Format

ospf suppress-flapping peer hold-max-cost disable

undo ospf suppress-flapping peer hold-max-cost disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set a duration for this mode, run the **ospf suppress-flapping peer hold-down** *interval* command.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you configure duration for the Hold-max-cost mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it.

Precautions

The Hold-max-cost mode takes effect only unidirectionally. If a remote device does not support OSPF neighbor relationship flapping suppression, bidirectional traffic between the local and remote devices may travel along different paths.

Example

Disable the Hold-max-cost mode on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf suppress-flapping peer hold-max-cost disable
```

7.4.90 ospf suppress-reachability

Function

The **ospf suppress-reachability** command suppresses the advertisement of the IP addresses of a specified interface.

The **undo ospf suppress-reachability** command restores the default configuration.

By default, all OSPF interfaces advertise their IP addresses.

Format

ospf suppress-reachability [**disable**]

undo ospf suppress-reachability [**disable**]

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To suppress the advertisement of the IP addresses of a specified interface so that the IP addresses can be reused, run the **ospf suppress-reachability** command.

Configuration Impact

Suppressing the advertisement of the IP addresses of all interfaces in an OSPF process reduces the number of IP prefixes carried in LSAs and the number of OSPF routes on the network, and improves network security and OSPF performance.

Precautions

If the advertisement of the IP addresses of virtual-link interfaces is suppressed, involved virtual-link neighbors cannot reach the Full state.

The interface IP addresses whose advertisement is suppressed are not used as the forwarding addresses (FAs) of the routes imported by OSPF. As a result, external routes may fail to be calculated.

Running the **ospf suppress-reachability** command suppresses the advertisement of primary and secondary IP addresses, without affecting the advertisement of loopback interfaces' IP addresses.

Example

Suppress the advertisement of IP addresses on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf suppress-reachability
```

7.4.91 ospf timer dead

Function

The **ospf timer dead** command sets a dead interval after which an interface considers its OSPF neighbor invalid.

The **undo ospf timer dead** command restores the default dead interval of the neighbor.

By default, for a P2P or broadcast interface, the dead interval for OSPF neighbors is 40 seconds; for an NBMA or P2MP interface, it is 120 seconds.

Format

ospf timer dead *interval*

undo ospf timer dead

Parameters

Parameter	Description	Value
interval	Specifies the dead interval of the OSPF neighbors.	The value is an integer ranging from 1 to 235926000, in seconds. Setting the dead interval of an OSPF neighbor to be longer than 20s is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface does not receive any Hello packet from its neighbor within the dead interval, the interface considers its neighbor invalid. The dead interval on an OSPF interface must be greater than the transmission interval of Hello messages. In addition, the dead intervals of devices on the same network segment must be the same.

By default, the dead interval of OSPF neighbors is four times the transmission interval of Hello messages.

Precautions

OSPF does not support the configuration on a null interface.

If the dead interval of an OSPF neighbor is shorter than 20s, the session may be closed. Therefore, if **dead** *interval* is shorter than 20s, the actual dead interval of an OSPF neighbor is not shorter than 20s.

Example

Set the dead interval on VLANIF100 to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf timer dead 60
```

Set the dead interval on GE0/0/1 to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf timer dead 60
```

7.4.92 ospf timer hello

Function

The **ospf timer hello** command sets an interval for sending Hello packets on an interface.

The **undo ospf timer hello** command restores the default value of the interval.

By default, for a P2P or broadcast interface, the interval for sending Hello packets is 10 seconds; for an NBMA or P2MP interface, it is 30 seconds.

Format

ospf timer hello *interval* [**conservative**]

undo ospf timer hello

Parameters

Parameter	Description	Value
interval	Specifies an interval for sending the Hello packet on an interface.	The value is an integer ranging from 1 to 65535, in seconds. Setting *interval* to be longer than or equal to 5s is recommended.
conservative	Indicates the conservative mode of the dead timer. If the conservative mode is configured, the value configured for the dead timer using the **ospf timer dead** command takes effect even when the value is less than 20s.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello packets are periodically sent on OSPF interfaces to establish and maintain neighbor relationships. A Hello packet contains information about timers, DRs, BDRs, and known neighbors.

The smaller the **hello** *interval* is, the faster the changing speed of the network topology is. The cost of routes, however, becomes greater. Ensure that the parameters of this interface and the adjacent routers are consistent.

Precautions

OSPF does not support the configuration on a null interface.

If **hello** *interval* is set but a dead interval is not set using the **ospf timer dead** command, the dead interval of an OSPF neighbor is four times the value of **hello** *interval*. If the dead interval of an OSPF neighbor is shorter than 20s, the session may be closed. Therefore, if **hello** *interval* is shorter than 5s, the actual dead interval of an OSPF neighbor is not shorter than 20s.

Example

Set the interval for sending Hello packets on VLANIF100 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf timer hello 20
```

Set the interval for sending Hello packets on GE0/0/1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf timer hello 20
```

7.4.93 ospf timer poll

Function

The **ospf timer poll** command sets a poll interval for sending Hello packets on NBMA networks.

The **undo ospf timer poll** command restores the default poll interval.

By default, it is 120 seconds.

Format

ospf timer poll *interval*

undo ospf timer poll

Parameters

Parameter	Description	Value
interval	Specifies the poll interval for sending Hello packets.	The value is an integer ranging from 1 to 3600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an NBMA network, after a device's neighbor becomes invalid, the device periodically sends Hello packets to the neighbor according to the poll interval set in the **ospf timer poll** command. The poll interval should be at least 4 times that of the **Hello** interval.

Precautions

OSPF does not support the configuration on a null interface.

Example

Set the poll interval for sending Hello packets on VLANIF100 to 130 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf timer poll 130
```

Set the poll interval for sending Hello packets on GE0/0/1 to 130 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf timer poll 130
```

7.4.94 ospf timer retransmit

Function

The **ospf timer retransmit** command sets an interval for retransmitting LSA on an interface.

The **undo ospf timer retransmit** command restores the default interval for retransmitting LSA on an interface.

By default, the interval time is 5 seconds.

Format

ospf timer retransmit *interval*

undo ospf timer retransmit

Parameters

Parameter	Description	Value
interval	Specifies interval for retransmitting LSA on an interface.	The value is an integer ranging from 1 to 3600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device transmits an LSA to its neighbor, it has to wait for the ACK packet from the neighbor. If no ACK packet is received from the neighbor in the LSA retransmission interval, this LSA is retransmitted.

Do not set LSA retransmission intervals too short between adjacent routers. Otherwise, it leads to unnecessary retransmission.

Precautions

OSPF does not support the configuration on a null interface.

Example

Specify the interval for retransmitting LSAs between VLANIF100 and the adjacent device to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf timer retransmit 8
```

Specify the interval for retransmitting LSAs between GE0/0/1 and the adjacent device to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf timer retransmit 8
```

7.4.95 ospf trans-delay

Function

The **ospf trans-delay** command adds a transmission delay to LSAs before they are sent by an interface.

The **undo ospf trans-delay** command restores the default transmission delay of LSAs on an interface.

By default, the transmission delay is 1 second.

Format

ospf trans-delay *interval*

undo ospf trans-delay

Parameters

Parameter	Description	Value
interval	Specifies a transmission delay to be added to LSAs before they are sent by an interface.	The value is an integer ranging from 1 to 500, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LSAs age (increase by 1 each second) in LSDBs but do not age during transmission in the network. To ensure that the aging time of LSAs transmitted to the remote device is correct, run the **ospf trans-delay** command to add a transmission delay to LSAs before they are sent by a local interface. This configuration is especially important to low-speed networks.

Precautions

OSPF does not support the configuration on a null interface.

Example

Add a transmission delay of 3 seconds to LSAs before they are sent by a VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf trans-delay 3
```

Add a transmission delay of 3 seconds to LSAs before they are sent by a GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf trans-delay 3
```

7.4.96 ospf valid-ttl-hops

Function

The **ospf valid-ttl-hops** command enables OSPF GTSM and sets a TTL value to be checked.

The **undo ospf valid-ttl-hops** command disables OSPF GTSM.

By default, OSPF GTSM is disabled.

Format

ospf valid-ttl-hops *hops* [**nonstandard-multicast**] [**vpn-instance** *vpn-instance-name*]

undo ospf valid-ttl-hops [*hops* [**nonstandard-multicast**]] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
hops	Specifies a TTL value to be checked.	The value is an integer that ranges from 1 to 255. The default value is 255.
nonstandard-multicast	Specifies the GTSM configuration is also valid for multicast packets. When the **nonstandard-multicast** parameter is configured: ● The TTL values of the multicast packets which will be sent are set as 255. ● The received multicast packets will be checked for the TTL value 1 or in the range of [255-*hops*+1, 255].	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. If the parameter is specified, only the TTL value of the packets in the specified VPN instance needs to be checked.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a network demanding higher security, you can enable GTSM to improve the security of the OSPF network. GTSM defends against attacks by checking the TTL value. If an attacker simulates and keeps sending OSPF unicast packets to a switch, the switch receives and directly sends the packets to the main control board for OSPF processing, without checking the validity of the packets. In this case, the switch is busy processing these packets, causing high CPU usage. GTSM protects the switches and enhances the system security by checking whether the TTL value in the IP packet header is within a pre-defined range.

The **ospf valid-ttl-hops** command is used to enable OSPF GTSM. To check the TTL value of packets that match the GTSM policy, the **vpn-instance** parameter must be specified in the command.

For example, running the **ospf valid-ttl-hops** command enables OSPF GTSM on both the public network and the private network. If you run the **ospf valid-ttl-hops 5 vpn-instance** *vpn1* command:

- OSPF GTSM is enabled on both the public network and the private network.
- The TTL value of OSPF packets in the VPN instance named *vpn1* is detected.
- The default action is performed for packets that are from the public network and other VPN instances and do not match the GTSM policy.

Precautions

- If a VPN instance is specified in the **ospf valid-ttl-hops** command and the interface is bound to the VPN instance, all the unicast packets sent to this interface are dropped when the set number of TTL hops is smaller than the actual number of hops on the network.
- If a virtual link or sham link is configured, the actual TTL value and the configured TTL value must be the same. That means that the number of virtual links or sham links that pass through the switch is calculated. Otherwise, packets sent from neighbors of a virtual link or a sham link will be dropped.
- GTSM only checks the TTL values of the packets that match the GTSM policy. If the packets do not match the GTSM policy, you can set the **pass** parameter or **drop** parameter in the **gtsm default-action** command to pass or drop these packets.
- If only a private or public network policy is configured, run the **gtsm default-action** command to set the default behavior for processing the packets unmatched with the GTSM policy to **pass** to prevent the OSPF packets of other instances from being discarded.

Example

Enable OSPF GTSM. Set the maximum number of TTL hops to 5 for the packets that can be received from the public network.

```
<HUAWEI> system-view
[HUAWEI] ospf valid-ttl-hops 5
```

7.4.97 p2mp-peer

Function

The **p2mp-peer** command sets a cost for an OSPF route to a specified neighbor on a P2MP network.

The **undo p2mp-peer** command restores the default value.

By default, the cost of an OSPF route to a neighbor in a P2MP network equals the interface cost.

Format

p2mp-peer *ip-address* **cost** *cost*

undo p2mp-peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor on a P2MP network.	The value is in dotted decimal notation.
cost *cost*	Sets a cost for an OSPF route to a specified neighbor on a P2MP network.	The value is an integer ranging from 1 to 65535.

Views

OSPF process view

Default Level

2: Configuration level

Usage Guidelines

By default, the cost of an OSPF route to a neighbor equals the interface cost on a P2MP network. If this default cost is not suitable, run the **p2mp-peer** command to set a desired cost.

The interface cost calculation formula is as follows: Cost of an interface = Bandwidth reference value/Interface bandwidth. The integer of the calculated result is used as the interface cost, and 1 is used as the interface cost if the calculated result is smaller than 1. The bandwidth reference value is set using the **bandwidth-reference** command, with the default value being 100 Mbit/s.

Example

Set the cost to 100 for the OSPF route to the neighbor 10.1.1.1 in OSPF process 100 on a P2MP network.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] p2mp-peer 10.1.1.1 cost 100
```

7.4.98 peer (OSPF)

Function

The **peer** command sets an IP address and a DR priority for the adjacent switch on an NBMA network.

The **undo peer** command cancels the IP address of the adjacent switch on an NBMA network.

By default, the IP address and DR priority for the adjacent switch on an NBMA network are not set.

Format

peer *ip-address* [**dr-priority** *priority*]

undo peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the adjacent switch.	The value is in dotted decimal notation.
dr-priority *priority*	Sets a DR priority for the adjacent switch.	The value of the priority is an integer that ranges from 0 to 255. By default, it is 1.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

On an NBMA network (such as an X.25 or FR network), the entire network can be fully meshed based on the mapping configuration. This means that there is a virtual link between any two devices. In this case, the network running OSPF can be considered as a broadcast network where a DR or a BDR can be selected. However, you must run the **peer** command to manually specify an IP address and a DR priority for an adjacent switch. This is necessary because it is impossible to find the adjacent devices dynamically by broadcasting Hello packets.

Example

Set the IP address of the adjacent switch to 10.1.1.1 on an NBMA network.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] peer 10.1.1.1
```

7.4.99 preference (OSPF)

Function

The **preference** command sets a preference for an OSPF route.

The **undo preference** command restores the default preference of OSPF routes.

By default, the preference of OSPF routes is 10 and that of ASE routes is 150.

Format

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Parameters

Parameter	Description	Value
ase	Indicates the preference of an AS external route.	-
preference	Specifies the preference of an OSPF route. The smaller the preference value, the higher the preference.	The value is an integer ranging from 1 to 255.
route-policy *route-policy-name*	Specifies the name of a route policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Multiple dynamic routing protocols can run on a switch at the same time. This creates a problem of route sharing and selecting among routing protocols. The system sets a default preference for each routing protocol. If different protocols have routes to the same destination, the protocol with a higher preference is selected to forward IP packets. To set a preference for an OSPF route, run the **preference** command.

You can create a route-policy to set a preference for a specific route by setting the **route-policy** parameter in the **preference** command:

- If the **apply preference** clause is configured for the route-policy, route preference is determined as follows:
  - Route matching the route-policy: Its preference is determined by the **apply** clause.

  - Route that does not match the route-policy: Its preference is determined by the **preference** command.

  In the following example, the preference of the route matching the route-policy **abc** is set to 50 and the preference of the route that does not match the route-policy is set to 30.

```
#
route-policy abc permit node 1
 if-match cost 20
 apply preference 50
#
ospf 1
 preference 30 route-policy abc
```

- If the **apply preference** clause is not included in the route-policy, the preference of routes is set by the **preference** command.

  In the above example, if the **apply preference 50** clause is not included in the policy **abc**, the preference of all routes is set to 30.

Configuration Impact

When there are routes discovered by multiple routing protocols on the same switch, you can make the switch prefer OSPF routes by setting a high preference for them.

Precautions

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured priority applies to all OSPF routes.

Example

Set the preference of routes in OSPF process 100 to 150.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] preference 150
```

Set the preference of external routes in OSPF process 200 to 130.

```
<HUAWEI> system-view
[HUAWEI] ospf 200
[HUAWEI-ospf-200] preference ase 130
```

7.4.100 prefix-priority (OSPF)

Function

The **prefix-priority** command sets a convergence priority for OSPF routes.

The **undo prefix-priority** command restores the default convergence priority of OSPF routes.

By default, the convergence priority of public 32-bit host routes is **medium**, and the convergence of other OSPF routes is **low**.

Format

prefix-priority { **critical** | **high** | **medium** } **ip-prefix** *ip-prefix-name*

undo prefix-priority { **critical** | **high** | **medium** }

Parameters

Parameter	Description	Value
critical	Sets the convergence priority of OSPF routes to critical.	-
high	Sets the convergence priority of OSPF routes to high.	-
medium	Sets the convergence priority of OSPF routes to medium.	-
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **prefix-priority** command sets a convergence priority for OSPF routes according to a specified IP prefix list name. It takes effect on the public network only.

After the **prefix-priority** command is run in the OSPF view, OSPF route calculation, link-state advertisement (LSA) flooding, and LSDB synchronization can be implemented according to the configured priority, which accelerates route convergence.

Prerequisites

An IP prefix list has been created using the **ip ip-prefix** command in the system view.

Configuration Impact

When an LSA meets multiple priorities, the highest priority takes effect.

With the **prefix-priority** command, OSPF can calculate and flood LSAs, and synchronize LSDBs according to priorities. This speeds up route convergence. OSPF calculates LSAs in the sequence of intra-area routes, inter-area routes, and AS external routes. This command makes OSPF calculate the three types of routes separately according to the specified route calculation priorities. Convergence priorities are critical, high, medium, and low. To speed up the processing of LSAs with the higher priority, during LSA flooding, the LSAs need to be placed into the corresponding critical, high, medium, and low queues according to priorities.

Precautions

By default, the convergence priorities of public OSPF host routes, direct routes, static routes, and other protocol (such as BGP and RIP) routes are **medium**, **high**, **medium**, and **low** respectively. In the public network, OSPF 32-bit host routes are uniformly identified as **medium**.

Example

Set the convergence priority of OSPF routes of 10.0.0.0/8 to critical.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix critical-prefix index 10 permit 10.0.0.0 8
[HUAWEI] ospf 1
[HUAWEI-ospf-1] prefix-priority critical ip-prefix critical-prefix
```

7.4.101 reset gtsm statistics

Function

The **reset gtsm statistics** command clears GTSM statistics.

Format

reset gtsm statistics all

Parameters

Parameter	Description	Value
all	Clears GTSM statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting the GTSM statistic within a certain period, you need to clear the existing statistics.

Example

Clear GTSM statistics.

```
<HUAWEI> reset gtsm statistics all
```

7.4.102 reset ospf counters

Function

The **reset ospf counters** command resets OSPF counters.

Format

reset ospf [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

Parameters

Parameter	Description	Value
process-id	Indicates an OSPF process ID. If the parameter is not specified, all OSPF processes are restarted.	The value is an integer ranging from 1 to 65535.
neighbor	Specifies neighbor information of an interface.	-
interface-type interface-number	Specifies the type and the number of an interface.	-
router-id	Specifies the router ID of the neighbor.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

When the switch restarts an OSPF process, the neighboring switch always reserves invalid LSAs. This occupies the memory of the system. These LSAs are deleted only when they expire, which happens when the LS age field in the LSA reaches 3600 seconds. After the **reset ospf** is used to restart an OSPF process and only when the router ID is changed, the switch generates an LSA in the set time and sets the LS age field to 3600 seconds. After receiving the LSA, other switches delete the LSA immediately from their LSDBs. If a switch does not send all the LSAs within the set time, other neighboring switches still store some invalid LSAs.

Clearing OSPF statistics does not affect the normal operation of OSPF services.

NOTICE

Once deleted, statistics cannot be restored. Therefore, exercise caution when deleting statistics.

Example

Reset OSPF counters.

```
<HUAWEI> reset ospf counters
```

7.4.103 reset ospf process

Function

The **reset ospf process** command restarts an OSPF process.

Format

reset ospf [*process-id*] **process** [**flush-waiting-timer** *time* | **graceful-restart**]

Parameters

Parameter	Description	Value
process-id	Indicates an OSPF process ID. If the parameter is not specified, all OSPF processes are restarted.	The value is an integer ranging from 1 to 65535.
flush-waiting-timer *time*	Specified the time when the LSA is generated. The parameter takes effect only when it is set.	The value is an integer that ranges from 1 to 40, in seconds.
graceful-restart	Indicates that graceful restart is enabled.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset ospf process** command can be used to clear OSPF information to reset the board.

NOTICE

If OSPF connections are reset, OSPF neighbor relationships will be interrupted and the original information cannot be restored. Exercise caution before running the **reset ospf process** command.

Configuration Impact

After the **reset ospf process** command is used to restart OSPF, the following situations may occur:

- If a router ID is changed, a new router ID will take effect after the command is run.
- Re-elect a DR and BDR.
- OSPF configuration will not be lost after OSPF restarts.

Precautions

Configuring the **flush-waiting-timer** parameter when OSPF starts allows you to clear invalid LSAs within the set time before LSAs time out.

Whether all invalid LSAs on other switches can be deleted depends on the set time.

When the switch restarts an OSPF process, the neighboring switch always reserves invalid LSAs. This occupies the memory of the system. These LSAs are deleted only when they expire, which happens when the LS age field in the LSA reaches 3600 seconds. After the **reset ospf** is used to restart an OSPF process and only when the router ID is changed, the switch generates an LSA in the set time and sets the LS age field to 3600 seconds. After receiving the LSA, other switches delete the LSA immediately from their LSDBs. If a device does not send all the LSAs within the set time, other neighboring switches still store some invalid LSAs.

Example

Restart all OSPF processes.

```
<HUAWEI> reset ospf process
Warning: The OSPF process will be reset. Continue? [Y/N]: y
```

7.4.104 reset ospf redistribution

Function

The **reset ospf redistribution** command re-imports OSPF routes.

Format

reset ospf [*process-id*] **redistribution**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If this parameter is not specified, all OSPF processes are restarted.	The value is an integer that ranges from 1 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset ospf redistribution** command re-imports OSPF routes to generate Type 5 or Type 7 LSAs.

Example

Re-import OSPF routes in OSPF process 1.

```
<HUAWEI> reset ospf 1 redistribution
```

7.4.105 reset ospf suppress-flapping peer

Function

The **reset ospf suppress-flapping peer** command forces an interface to exit from OSPF neighbor relationship flapping suppression.

Format

reset ospf *process-id* **suppress-flapping peer** [*interface-type interface-number*] [**notify-peer**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies an interface type and number.	-
notify-peer	Instructs neighbors to exit from OSPF neighbor relationship flapping suppression too.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Interfaces exit from flapping suppression in any of the following scenarios:

- The suppression timer expires.
- The corresponding OSPF process is reset.
- The **reset ospf suppress-flapping peer** command is run.
- OSPF neighbor relationship flapping suppression is disabled globally using the **suppress-flapping peer disable** command in the OSPF view.

If **notify-peer** is specified when the **reset ospf suppress-flapping peer** command is run on a device, the device sends Hello packets in which **HelloInterval** and **RouterDeadInterval** are 0s to its neighbors to instruct the neighbors to exit from OSPF neighbor relationship flapping suppression too. If the neighbors fail to receive such Hello packets, the function of **notify-peer** does not take effect. To force the neighbors to exit from OSPF neighbor relationship flapping suppression, run the **reset ospf suppress-flapping peer** command on them.

Example

Force interfaces to exit from OSPF neighbor relationship flapping suppression.

```
<HUAWEI> reset ospf 1 suppress-flapping peer
```

7.4.106 retransmission-limit

Function

The **retransmission-limit** command enables retransmission limit and sets the maximum number of retransmissions.

The **undo retransmission-limit** command disables retransmission limit.

By default, retransmission limit is disabled.

Format

retransmission-limit [*max-number*]

undo retransmission-limit

Parameters

Parameter	Description	Value
max-number	Indicates the maximum number of retransmissions.	The value is an integer that ranges from 2 to 255. The default value is 30.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **retransmission-limit** command can be used to enable Retransmission Limitation for OSPF (RL-for OSPF) to prevent dead loops caused by repeated transmissions if neighbors cannot receive packets.

Configuration Impact

The OSPF retransmission limit can be used in the following packets:

- DD packets
- LSU packets
- LSR packets

Limit the maximum number of retransmissions. If the preceding three types of packets cannot be responded within the allowed retransmission times, disconnect neighbor relationships.

Example

Enable OSPF retransmission limit and set the maximum number of retransmissions to 40.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] retransmission-limit 40
```

7.4.107 route-tag

Function

The **route-tag** command sets a tag value for imported VPN routes.

The **undo route-tag** command restores the default setting.

By default, the tag value of a VPN route is calculated based on the AS number of BGP. If no BGP is configured, the default tag value is 0.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

route-tag { *tag* | **disable** }

undo route-tag

Parameters

Parameter	Description	Value
tag	Specifies the tag value of the imported VPN routes.	The value is an integer ranging from 0 to 4294967295.
disable	Disables a device from using a VPN route tag to detect loops.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **route-tag** command can be used only in VPN scenarios to prevent loops on Type-5 and Type-7 LSAs when a CE is dual-homed to two PEs.

In a networking where a CE is dual-homed to two PEs, PE1 generates Type-5 and Type-7 LSAs based on the imported BGP routes and sends the LSAs to the CE, then to PE2. Because OSPF routes have higher priorities over BGP routes, OSPF routes will replace BGP routes on PE2, causing loops. After the **route-tag** command is run, if the tag value of the PE and an LSA are the same, the PE will neglect the LSA, and a loop is prevented.

By default, the first two bytes of the tag value are fixed as 0xD000, while the last two bytes are the AS number of the local BGP. If a BGP AS number is greater than 65535, the default tag 0 is used. You can use the command to change the tag in this case.

Precautions

- Configuring the same VPN route tag on the PEs within the same area is recommended.
- Different OSPF processes can be configured with the same VPN route tag.

The tags set by the **route-tag** command or other commands are different only in preference.

1. The preference of the tag configured using the **import-route** command is the highest.
2. The preference of the tag configured using the **route-tag** command is medium.
3. The preference of the tag configured using the **default tag** command is the lowest.

Example

Set the route tag for OSPF process 100 to 100 in a VPN instance named **test**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance test
[HUAWEI-vpn-instance-test] route-distinguisher 100:1
[HUAWEI-vpn-instance-test-af-ipv4] quit
[HUAWEI-vpn-instance-test] quit
[HUAWEI] ospf 100 vpn-instance test
[HUAWEI-ospf-100] route-tag 100
```

7.4.108 rfc1583 compatible

Function

The **rfc1583 compatible** command converts rules defined in RFC 2328 into rules defined in RFC 1583.

The **undo rfc1583 compatible** command converts rules defined in RFC 1583 into rules defined in RFC 2328.

By default, OSPF supports the routing rule of RFC 1583.

Format

rfc1583 compatible

undo rfc1583 compatible

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

RFC 2328 and RFC 1583 define different OSPF route selection rules. When enabling OSPF, configure the same route selection rules on all devices in the same OSPF area. For example, in scenarios where an OSPF device uses the default route selection rules defined in RFC 1583, if the other switches in the same OSPF area use route selection rules defined in RFC 2328, you need to run the **undo rfc1583 compatible** command.

Example

Converts rules defined in RFC 1583 into rules defined in RFC 2328.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] undo rfc1583 compatible
```

7.4.109 sham-hello enable (OSPF)

Function

The **sham-hello enable** command enables the sham-hello function of OSPF.

The **undo sham-hello** command disables the sham-hello function.

By default, the sham-hello feature is disabled.

Format

sham-hello enable

undo sham-hello

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the device maintains neighbor relationships through both the Hello packets and also all OSPF protocol packets. This accurately senses the existence of OSPF neighbors and stabilizes neighboring relations.

Example

Enable the sham-hello function.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] sham-hello enable
```

7.4.110 sham-link (OSPF Area)

Function

The **sham-link** command configures a sham link or sets parameter values for a sham link.

The **undo sham-link** command deletes a sham link or restores the default parameter values of a sham link.

By default, no sham link is configured for OSPF.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

sham-link *source-ip-address destination-ip-address* [[**simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] | **authentication-null** | **keychain** *keychain-name*] | **smart-discover** | **cost** *cost* | **dead** *dead-interval* | **hello** *hello-interval* | **retransmit** *retransmit-interval* | **trans-delay** *trans-delay-interval*] *

undo sham-link *source-ip-address destination-ip-address* [[**simple** | **md5** | **hmac-md5** | **hmac-sha256** | **authentication-null** | **keychain**] | **smart-discover** | **cost** | **dead** | **hello** | **retransmit** | **trans-delay**] *

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source IP address.	The value is in dotted decimal notation.
destination-ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
smart-discover	Indicates that Hello packets are sent automatically and immediately.	-
simple	Indicates simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
plain	Indicates plain authentication. Only plain text can be entered, and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This carries security risks. You are advised to select **cipher** to save the password in cipher text.	-
plain-text	Specifies a plain text password.	● In **simple** authentication, the value is a string of 1 to 8 characters without spaces. ● In **md5**, **hmac-sha256** or **hmac-md5** authentication, the value is a string of 1 to 255 characters.

Parameter	Description	Value
cipher	Indicates cipher authentication. Either plain text or cipher text can be entered, and cipher text is displayed when the configuration file is viewed.	-
cipher-text	Specifies a cipher text password.	- In **simple** authentication, the value is a string of 1 to 8 plain text characters and 48 cipher text characters. - In **md5**, **hmac-sha256** or **hmac-md5** authentication, the value is a string of 1 to 255 plain text characters and 20 to 392 cipher text characters.
md5	Indicates MD5 authentication. **NOTICE** MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates **hmac-md5** authentication. **NOTICE** HMAC-MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates **HMAC-SHA256** authentication.	-
key-id	Specifies the authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.
authentication-null	Indicates that no authentication is used.	-

Parameter	Description	Value
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, only the **HMAC-MD5**, **SM3**, and **HMAC-SHA256** algorithms can be used in OSPF.	-
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
cost *cost*	Specifies the cost of the sham link.	The value of the cost is an integer that ranges from 1 to 65535. The default value is 1.
dead *dead-interval*	Specifies the dead interval. This value must be equal to *dead-interval* of the switch that sets up a virtual link with the local switch, and must be at least four times that of *hello-interval*.	The value of the interval is an integer that ranges from 1 to 235926000, in seconds.
hello *hello-interval*	Specifies an interval for transmitting Hello packets on an interface. This value must be equal to *hello-interval* of the switch that sets up a virtual link with the local switch.	The value is an integer that ranges from 1 to 65535, in seconds.

Parameter	Description	Value
retransmit *retransmit-interval*	Specifies an interval for retransmitting the LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds.
trans-delay *trans-delay-interval*	Specifies the delay in transmitting LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sham-link** command can be used only in VPN scenarios.

This command can create a sham link to allow VPN traffic to be preferentially forwarded through routes within the backbone area. This prevents traffic from the same VPN in the same OSPF area from being forwarded through intra-area OSPF routes.

Before enabling neighbors of a sham link to set up adjacencies quickly, configure the **smart-discover** parameter to actively send Hello packets immediately.

Configuration Impact

After a sham link is configured between two PEs, the sham link is considered as an intra-area OSPF route. This configuration enables a route passing through an MPLS VPN backbone network to become an intra-area OSPF route, preventing VPN traffic from being transmitted through this route. A 32-bit loopback interface address is specified as the source and destination addresses of the sham link. The loopback interface must be bound to a VPN instance and advertised using BGP.

Precautions

The route to the endpoint address of a sham link cannot be advertised to the remote PE using an OSPF process in a private network. Otherwise, two routes to the endpoint address of the sham link exist on the remote PE. One route is learned from the OSPF process and the other is learned using MP-BGP. OSPF routes have higher priorities over BGP routes. As such, the remote PE selects an incorrect OSPF route. As a result, the sham link cannot be created.

Example

Create a sham link with the source address 10.1.1.1 and destination address 10.2.2.2 in a VPN instance named **test**.

```
<HUAWEI> system-view
[HUAWEI] ospf 1 vpn-instance test
[HUAWEI-ospf-1] area 1
[HUAWEI-ospf-1-area-0.0.0.1] sham-link 10.1.1.1 10.2.2.2
```

7.4.111 silent-interface (OSPF)

Function

The **silent-interface** command disables an interface from receiving and sending OSPF packets.

The **undo silent-interface** command restores the default setting.

By default, the interface is permitted to receive or send OSPF packet.

Format

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type* [*interface-number*] }

Parameters

Parameter	Description	Value
all	Indicates all interfaces in a specified process.	-
interface-type interface-number	Specifies the interface type and interface number.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that OSPF routing information is not obtained by the devices of a certain network and the local device does not receive routing update information advertised by other devices, you can run the **silent-interface** command to disable an interface from receiving and sending OSPF packets, thereby preventing routing loops.

Configuration Impact

After an OSPF interface is set to be in the silent state, the interface can still advertise its direct routes. Hello packets on the interface, however, will be blocked and no neighbor relationship can be established on the interface. This can enhance the networking adaptability of OSPF and reduce the consumption of system resources.

Example

Disable VLANIF200 from sending or receiving OSPF packets.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] silent-interface vlanif 200
```

7.4.112 spf-schedule-interval

Function

The **spf-schedule-interval** command sets an interval for OSPF to calculate routes.

The **undo spf-schedule-interval** command restores the default setting.

By default, the intelligent timer is enabled. The interval for the SPF calculation is expressed in milliseconds. The maximum interval for the SPF calculation is 10000 ms, the initial interval is 500 ms, and the Holdtime interval is 1000 ms.

Format

spf-schedule-interval { *interval1* | **intelligent-timer** *max-interval start-interval hold-interval* | **millisecond** *interval2* }

undo spf-schedule-interval

Parameters

Parameter	Description	Value
interval1	Specifies an interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 10, in seconds.
intelligent-timer	Sets an interval for OSPF SPF calculation through an intelligent timer.	-
max-interval	Specifies a maximum interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 120000, in milliseconds. The default value is 10000.
start-interval	Specifies the initial interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 60000, in milliseconds. The default value is 500.

Parameter	Description	Value
hold-interval	Specifies the Holdtime interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 60000, in milliseconds. The default value is 1000.
millisecond *interval2*	Specifies an interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 10000, in milliseconds.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the LSDB, the device that runs OSPF calculates the SPT with itself as the root based on the SPF arithmetic, and determines the next hop to the destination network according to the SPT. When the OSPF LSDB changes, the shortest path needs to be recalculated. Frequent network changes and continual calculation of the shortest path consume many system resources and affect the efficiency of the devices. You can configure an intelligent timer and set a proper interval for the SPF calculation to prevent the excessive consumption of device memory and bandwidth resources.

On a network where the convergence time of routes is required to be shorter, set millisecond as the unit of interval to increase the frequency of calculating routes. This increases route convergence. In other networking environments, the default value is recommended.

Configuration Impact

After this command is configured, the interval for the SPF calculation is as follows:

1. The initial interval for the SPF calculation is specified by the parameter *start-interval*.
2. The interval for the SPF calculation for the nth (n≥2) time is equal to *hold-interval* x $2^{(n-2)}$.
3. When the interval specified by *hold-interval* x $2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Example

Set the interval for OSPF to calculate routes to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] spf-schedule-interval 6
```

7.4.113 stub (OSPF area)

Function

The **stub** command sets an area to a stub area.

The **undo stub** command cancels the settings.

By default, no area is set to a stub area.

Format

stub [**no-summary** | **default-route-advertise backbone-peer-ignore**] *

undo stub

Parameters

Parameter	Description	Value
no-summary	Disables an ABR from sending non-default Type 3 LSAs to the stub area. This parameter applies only to ABRs of stub areas. If the parameter is configured on an ABR, the ABR advertises only one default Type 3 LSA (no other Type 3 LSAs) to the stub area. In this case, this area is also called a totally stub area.	-
default-route-advertise	Configures an ABR to advertise a default Type 3 LSA to the stub area. This parameter applies only to ABRs of stub areas.	-
backbone-peer-ignore	Prevents an ABR from checking the neighbor status when the ABR generates a default Type 3 LSA and advertises it to the stub area. This parameter applies only to ABRs of stub areas. If the parameter is configured on an ABR, the ABR generates a default Type 3 LSA and advertises it to the stub area as long as an interface is Up in the backbone area.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two configuration commands for stub areas: **stub** and **default-cost**. The stub area attribute must be configured on all switches in a stub area using the **stub** command.

The **default-cost** command takes effect only when it is configured on an ABR. The command is used to specify the cost of the default summary route transmitted by the ABR to the stub area.

- If the **stub** command is run on an ABR, without parameters specified, the ABR advertises a default Type 3 LSA and advertises it to the stub area as long as an OSPF neighbor in the full state exists in the backbone area.
- If the **stub no-summary** command is run on an ABR, the ABR is disabled from sending non-default Type 3 LSAs to the stub area connected to the ABR.
- If the **stub default-route-advertise backbone-peer-ignore** command is run on an ABR, the ABR generates a default Type 3 LSA and advertises it to the stub area as long as an interface is Up in the backbone area.

Precautions

The backbone area (area 0) cannot be configured as a stub area.

Example

Set OSPF area 1 as a stub area.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] stub
```

7.4.114 stub-router (OSPF)

Function

The **stub-router** command configures a stub router.

The **undo stub-router** command restores the default configuration.

By default, no device is configured as a stub router.

Format

stub-router [**on-startup** [*interval*]]

undo stub-router

Parameters

Parameter	Description	Value
on-startup [*interval*]	Specifies the interval during which a device acts as a stub router when the device is restarted or faulty. ● If **on-startup** is not specified, the device is always a stub router, even if the cost of all routes advertised by the device is 65535. ● If **on-startup** is specified, the device works as a stub router only when it restarts or is faulty. The hold time of the stub router state is determined by *interval* parameter. If the *interval* parameter is not configured, the default interval (500 seconds) is used.	The value is an integer that ranges from 5 to 65535, in seconds. By default, the value is 500 seconds.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

After the **stub-router** command is configured on a device, the device informs other devices not to use this stub router to forward data by increasing the metric to 65535 of the links in the LSA that is generated by the device. As the metric is not infinite, there can still be a route to this stub router. The metric of the LSA links that are generated by the stub router is very high.

Example

Configure the device as a stub router.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] stub-router
```

7.4.115 suppress-flapping peer disable (OSPF)

Function

The **suppress-flapping peer disable** command disables OSPF neighbor relationship flapping suppression globally.

The **undo suppress-flapping peer disable** command enables OSPF neighbor relationship flapping suppression globally.

By default, OSPF neighbor relationship flapping suppression is enabled globally.

Format

suppress-flapping peer disable

undo suppress-flapping peer disable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

If an OSPF interface alternates between Up and Down, OSPF neighbor relationship flapping occurs on the interface. During the flapping, OSPF frequently sends Hello packets to reestablish the neighbor relationship, synchronizes LSDBs, and recalculates routes. In this process, a large number of packets are exchanged, adversely affecting neighbor relationship stability, OSPF services, and other OSPF-dependent services, such as LDP and BGP. OSPF neighbor relationship flapping suppression can address this problem by delaying OSPF neighbor relationship reestablishment or preventing service traffic from passing through flapping links.

By default, OSPF neighbor relationship flapping suppression is enabled globally. To disable this function globally, run the **suppress-flapping peer disable** command.

Example

Disable neighbor relationship flapping suppression globally.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] suppress-flapping peer disable
```

7.4.116 suppress-reachability (OSPF)

Function

The **suppress-reachability** command suppresses the advertisement of the IP addresses of all interfaces in an OSPF process.

The **undo suppress-reachability** command restores the default configuration.

By default, all interfaces in an OSPF process advertise their IP addresses.

Format

suppress-reachability

undo suppress-reachability

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To suppress the advertisement of the IP addresses of all interfaces in an OSPF process so that the IP addresses can be reused, run the **suppress-reachability** command.

Configuration Impact

Suppressing the advertisement of the IP addresses of all interfaces in an OSPF process reduces the number of IP prefixes carried in LSAs and the number of OSPF routes on the network, and improves network security and OSPF performance.

Precautions

If the advertisement of the IP addresses of virtual-link interfaces is suppressed, involved virtual-link neighbors cannot reach the Full state.

The interface IP addresses whose advertisement is suppressed are not used as the forwarding addresses (FAs) of the routes imported by OSPF. As a result, external routes may fail to be calculated.

Running the **suppress-reachability** command suppresses the advertisement of primary and secondary IP addresses, without affecting the advertisement of loopback interfaces' IP addresses.

Example

Suppress the advertisement of the IP addresses of all interfaces in OSPF process 100.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] suppress-reachability
```

7.4.117 vlink-peer (OSPF area)

Function

The **vlink-peer** command creates and configures a virtual link.

The **undo vlink-peer** command deletes the virtual link or restores the default setting.

By default, no virtual link is configured for OSPF.

Format

vlink-peer *router-id* [**dead** *dead-interval* | **hello** *hello-interval* | **retransmit** *retransmit-interval* | **smart-discover** | **trans-delay** *trans-delay-interval* | [**simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] | **authentication-null** | **keychain** *keychain-name*]] *

undo vlink-peer *router-id* [**dead** | **hello** | **retransmit** | **smart-discover** | **trans-delay** | **simple** | **md5** | **hmac-md5** | **hmac-sha256** | **authentication-null** | **keychain**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
router-id	Specifies the switch ID of virtual link neighbor.	-
dead *dead-interval*	Specifies a dead interval. This value must be equal to *dead-interval* of the Switch that sets up a virtual link with the interface and must be at least 4 times that of *hello-interval*.	The value is an integer that ranges from 1 to 235926000, in seconds. The default value is 40 seconds.
hello *hello-interval*	Specifies an interval for transmitting Hello packets on an interface. This value must be equal to *hello-interval* value of the Switch that sets up a virtual link with the interface. The default value is 10 seconds.	The value ranges from 1 to 65535 seconds. The default value is 10 seconds.
retransmit *retransmit-interval*	Specifies an interval for retransmitting the LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds. The default value is 5 seconds.
smart-discover	Automatically sends Hello packets	-

Parameter	Description	Value
trans-delay *trans-delay-interval*	Specifies the delay in transmitting LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds. The default value is 1 second.
simple	Indicates simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
plain	Indicates plain authentication. Only plain text can be entered, and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This carries security risks. Select **cipher** to save the password in cipher text for increased security.	-
plain-text	Specifies a plain text password.	● In **simple** mode, the value is a string of 1 to 8 characters without spaces. ● In **md5**, **hmac-sha256** or **hmac-md5** mode, the value is a string of 1 to 255 characters without spaces.
cipher	Indicates cipher authentication. Either plain text or cipher text can be entered, and cipher text is displayed when the configuration file is viewed.	-

Parameter	Description	Value
cipher-text	Specifies a cipher text password.	- In **simple** mode, the value is a string of 1 to 8 characters (plaintext password) or 48 characters (ciphertext password) without spaces. - In **md5**, **hmac-sha256** or **hmac-md5** mode, the value is a string of 1 to 255 (plain text password) and 20 to 392 characters (cipher text password) without spaces.
md5	Indicates MD5 authentication. In MD5 authentication, the password type is **cipher** by default. **NOTICE** MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates HMAC-MD5 authentication. In HMAC-MD5 authentication, the password type is **cipher** by default. **NOTICE** HMAC-MD5 authentication carries potential security risks. As such, HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates HMAC-SHA256 authentication. In HMAC-SHA256 authentication, the password type is **cipher** by default.	-
key-id	Specifies the authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
authentication-null	Indicates that no authentication is used.	-
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, only the **HMAC-MD5**, **SM3**, and **HMAC-SHA256** algorithms can be used in OSPF.	-
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

After OSPF areas are defined, OSPF route updates between non-backbone areas are transmitted through a backbone area. Therefore, OSPF requires that all non-backbone areas be directly connected to the backbone area and devices within the backbone area keep connected as well. However, these requirements may not be met due to various limitations. OSPF virtual links can be configured to solve the problem.

Follow-up Procedure

After virtual links are established, devices provided by different vendors may use different default MTUs. To ensure consistent MTUs on the devices, run the **undo**

ospf mtu-enable command to set the default MTU in DD packets sent by interfaces to 0.

NOTICE

Configuring the MTU in DD packets will cause the neighbor relationship to be re-established.

Precautions

When configuring parameters, pay attention to the following:

- A smaller **hello** value indicates faster detection of changes in network topology and higher network resource usage.
- A **retransmit** value that is too small leads to unnecessary retransmission of LSAs. On a low-speed network, set a large **retransmit** value.
- The authentication mode of a virtual link must be the same as that in the backbone area.

Example

Configure a virtual link with the peer device's router ID 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 2
[HUAWEI-ospf-100-area-0.0.0.2] vlink-peer 10.1.1.1
```

7.4.118 vpn-instance-capability simple (OSPF)

Function

The **vpn-instance-capability simple** command directly calculates a route instead of conducting the routing loop detection.

The **undo vpn-instance-capability** command detects the DN bit to avoid routing loops.

By default, the routing-loop check is enabled.

Format

vpn-instance-capability simple

undo vpn-instance-capability

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If OSPF VPN multi-instance is deployed on a Multi-VPN-Instance CE (MCE), routes cannot be calculated based on Type3, Type5, or Type7 LSAs with the DN bit. Therefore, OSPF detects routing loops when calculating routes. In this case, the **vpn-instance-capability simple** command is used to disable OSPF routing loop detection and enable OSPF to calculate routes based on received LSAs without checking the DN bit and route-tag in the LSAs. The route-tag is restored to the default value 1.

Prerequisites

OSPF VPN multi-instance has been deployed on an MCE using the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command.

Configuration Impact

- If there is no ABR and the **vpn-instance-capability simple** command is run on an MCE, the MEC cannot become an ABR.
- After the **vpn-instance-capability simple** command is run, OSPF routes that have been imported by BGP do not carry any OSPF domain ID, route tag, or router ID.
- By default, when BGP imports an OSPF route, it uses the cost of the OSPF route plus 1 as the MED value. The MED in BGP is similar to the cost in an IGP in terms of functions. After the **vpn-instance-capability simple** command is run, BGP uses the cost of an OSPF route as the MED when it imports the OSPF route. Therefore, MED values change after the command is run, which may affect the route selection result.

Precautions

NOTE

The **undo vpn-instance-capability** command cannot be used to enable OSPF routing loop detection in a scenario without MCEs.

Example

Disable the OSPF routing-loop check.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
[HUAWEI] ospf 100 vpn-instance vrf1
[HUAWEI-ospf-100] vpn-instance-capability simple
```

7.5 OSPFv3 Configuration Commands

7.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.5.2 abr-summary (OSPFv3 Area)

Function

The **abr-summary** command configures IPv6 route summarization on an ABR.

The **undo abr-summary** command cancels IPv6 route summarization on an ABR.

By default, IPv6 route summarization is not configured on ABRs.

Format

abr-summary *ipv6-address prefix-length* [**cost** *cost* | **not-advertise**] *

undo abr-summary *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the address range of IPv6 routes to be summarized.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length.	The value is an integer that ranges from 1 to 128.
cost *cost*	Specifies the cost of a summarized route. By default, the cost of a summarized route is the maximum cost among those of routes that are summarized.	The value is an integer that ranges from 1 to 16777214.
not-advertise	Indicates that the summarized IPv6 routes that match a specified IPv6 address prefix or prefix length are not advertised.	-

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

This command applies only to the ABR of the current area. The ABR transmits only one summarized route to other areas.

An area can be configured with multiple summarized network segments. Thus OSPFv3 can summarize multiple network segments.

Example

Summarize two routes FC00:0:0:1::/64 and FC00:0:0:2::/64 of OSPFv3 area 1 into route FC00:0:0::/48 with the cost being 400, and advertise it to other areas.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 1
[HUAWEI-ospfv3-1-area-0.0.0.1] abr-summary fc00:0:0:: 48 cost 400
```

7.5.3 area (OSPFv3)

Function

The **area** command displays the OSPFv3 area view.

Format

area *area-id*

Parameters

Parameter	Description	Value
area-id	Specifies an OSPFv3 area ID.	The value can be an integer in the decimal format or in the IPv4 address format. If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of devices increases with the expansion of the network. This leads to a large LSDB on every OSPFv3-enabled device on a large-scale network. Consequently, route flapping frequently occurs and thus a large number of OSPF packets are transmitted on the network, which wastes bandwidth resources.

OSPFv3 addresses the preceding problem by logically partitioning an AS into different areas.

Prerequisites

The OSPFv3 process view has been entered.

Precautions

After an AS is partitioned into different areas, not all areas are equal. The area with ID 0 is a backbone area. The backbone area is responsible for forwarding inter-area routes. In addition, the routing information between non-backbone areas must be forwarded through the backbone area.

The first time the **area** command is run, an OSPFv3 area is created, and the OSPFv3 area view is displayed. Running the **area** command later enters the OSPFv3 area view only.

Example

Enter the OSPFv3 area 0 view.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 0
[HUAWEI-ospfv3-1-area-0.0.0.0]
```

7.5.4 asbr-summary (OSPFv3)

Function

The **asbr-summary** command enables an autonomous system border router (ASBR) to summarize the routes imported by OSPFv3.

The **undo asbr-summary** command disables an ASBR from summarizing the routes imported by OSPFv3.

By default, ASBRs do not summarize the routes imported by OSPFv3.

Format

asbr-summary *ipv6-address prefix-length* [**cost** *cost* | **tag** *tag* | **distribute-delay** *dist-delay-interval* | **not-advertise**] *

undo asbr-summary *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address prefix-length	Specifies the IPv6 address and prefix length of a summary IPv6 route.	● The IPv6 address is a 32-digit hexadecimal number in the X:X:X:X:X:X:X:X format. ● The prefix length ranges from 1 to 128.
cost *cost*	Specifies the cost of a summary route. By default, for Type 1 external routes, the cost of the summarized route is the highest cost of specific routes; for Type 2 external routes, the cost of the summarized route equals the highest cost of specific routes plus 1.	The value is an integer in the range from 1 to 16777214.
tag *tag*	Indicates the tag used to control route advertisement based on routing policies.	The value is an integer in the range from 0 to 4294967295. The default value is 1.
distribute-delay *dist-delay-interval*	Specifies the delay in advertising summary routes.	The value is an integer in the range from 1 to 65535, in seconds.
not-advertise	Indicates that the summary IPv6 routes that match a specified IPv6 address prefix or prefix length are not advertised.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

An ASBR connects to more than one autonomous system (AS) and generates AS external LSAs.

You can run the **asbr-summary** command to enable an ASBR to summarize the imported routes with the same prefix into a single summary route and advertise the summary route.

Multiple summary routes can be configured on an ASBR. Therefore, multiple network segments can be summarized in OSPFv3.

Example

Enable an ASBR to summarize the routes imported by OSPFv3.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] asbr-summary fc00::1 64 cost 20 tag 100
```

7.5.5 authentication-mode (OSPFv3)

Function

The **authentication-mode** command configures an authentication mode and a password for an OSPFv3 process or area.

The **undo authentication-mode** command deletes the authentication mode and password configured for an OSPFv3 process or area.

By default, no authentication mode or password is configured for any OSPFv3 process or area.

Format

authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }

authentication-mode keychain *keychain-name*

undo authentication-mode hmac-sha256 key-id *key-id*

undo authentication-mode keychain

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
hmac-sha256	Configures HMAC-SHA256 authentication.	-
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
plain	Configures the plaintext password type. Only a plaintext password can be entered, and the password is displayed in plaintext in the configuration file. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
plain-text	Specifies a plaintext password.	The value is a string of 1 to 255 characters without spaces.
cipher	Configures the ciphertext password type. You can enter either a plaintext or ciphertext password, but the password is displayed in ciphertext in the configuration file.	-
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for plaintext passwords and 20 to 392 characters for ciphertext passwords without spaces.
keychain	Configures keychain authentication. **NOTE** Before configuring this parameter, you must run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, the OSPF authentication will fail.	-
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters without spaces.

Views

OSPFv3 view, OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to inherent defects and flawed implementation of the TCP/IP protocol suite, there are an increasing number of attacks, which poses greater threats on TCP/IP networks than ever before. The attacks on network devices may lead to network failures. To configure an authentication mode and a password for an OSPFv3 process or area to improve OSPFv3 network security, run the **authentication-mode** command.

Precautions

If you use area authentication, the authentication and password configurations on the interfaces of all the routers in the area must be the same.

OSPFv3 area authentication has a lower priority than OSPFv3 interface authentication.

To configure OSPFv3 interface authentication, run the **ospfv3 authentication-mode** command.

Example

Configure HMAC-SHA256 authentication for OSPFv3 process 100.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 100
[HUAWEI-ospfv3-100] authentication-mode hmac-sha256 key-id 10 cipher test
```

Configure HMAC-SHA256 authentication for OSPFv3 area 0.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 100
[HUAWEI-ospfv3-100] area 0
[HUAWEI-ospfv3-100-area-0.0.0.0] authentication-mode hmac-sha256 key-id 10 cipher test
```

7.5.6 bandwidth-reference (OSPFv3)

Function

The **bandwidth-reference** command sets a bandwidth reference value for link cost calculation.

The **undo bandwidth-reference** command restores the default setting.

By default, the bandwidth reference value of the link cost is 100 Mbit/s. That is, the link cost is 100000000/bandwidth.

Format

bandwidth-reference *value*

undo bandwidth-reference

Parameters

Parameter	Description	Value
value	Specifies a bandwidth reference value for link cost calculation.	The value is an integer that ranges from 1 to 2147483648, in Mbit/s. The default value is 100 Mbit/s.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

To set a cost for an interface that runs OSPFv3, you can run the **ospfv3 cost** command. If the link cost is not set, OSPFv3 calculates the link cost according to the link bandwidth (Cost = Reference Value/Bandwidth). The priority of the cost set using the **ospfv3 cost** command is higher than that set using the **bandwidth-reference** command.

The **bandwidth-reference** command has the same function on Eth-Trunk interfaces and physical interfaces. If the command is run on an Eth-Trunk interface, the bandwidth of the Eth-Trunk interface is the total bandwidth of all its member interfaces.

The **bandwidth** *bandwidth* command can only set an interface bandwidth obtained by the NMS from the MIB. It cannot change an interface actual bandwidth and interface cost.

Example

Set the bandwidth reference value of the link cost to 1000.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] bandwidth-reference 1000
```

7.5.7 bfd all-interfaces (OSPFv3)

Function

The **bfd all-interfaces** command enables BFD for OSPFv3 or configures BFD parameters for OSPFv3.

The **undo bfd all-interfaces** command disables BFD for OSPFv3 or deletes the configured BFD parameters for OSPFv3.

By default, BFD is not enabled or configured for OSPFv3 processes.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

bfd all-interfaces { **enable** | { **min-transmit-interval** *min-transmit-value* | **min-receive-interval** *min-receive-value* | **detect-multiplier** *detect-multiplier-value* } * }

undo bfd all-interfaces { **enable** | { **min-transmit-interval** [*min-transmit-value*] | **min-receive-interval** [*min-receive-value*] | **detect-multiplier** [*detect-multiplier-value*] } * }

Parameters

Parameter	Description	Value
enable	Enables BFD for OSPFv3.	-
min-transmit-interval *min-transmit-value*	Specifies the minimum interval for sending BFD packets to the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. • After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. • After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
min-receive-interval *min-receive-value*	Specifies the minimum interval for receiving BFD packets from the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *detect-multiplier-value*	Indicates the local detection multiplier.	The value is an integer in the range from 3 to 50. The default value is 3.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- To allow OSPFv3 to quickly detect device faults and recalculate routes, run the **bfd all-interfaces** command to enable BFD and configure BFD session parameters for OSPFv3. This speeds up OSPFv3 route convergence. If an OSPFv3 neighbor relationship goes Down, the BFD session between the OSPFv3 neighbors is dynamically deleted.

After OSPFv3 establishes a BFD session, the default parameter values are used. BFD session parameters can also be modified as required.

- Actual interval at which BFD packets are transmitted on the local device = Max { configured interval *min-transmit-value* at which BFD packets are transmitted on the local device, configured interval *min-receive-value* at which BFD packets are received on the peer device }
- Actual interval at which BFD packets are received on the local device = Max { configured interval *min-transmit-value* at which BFD packets are transmitted on the peer device, configured interval *min-receive-value* at which BFD packets are received on the local device }
- Actual period for BFD detection on the local device = Actual interval at which BFD packets are received on the local device x Detection multiplier *detect-multiplier-value* configured on the peer device

For example:

- On the local device, the configured interval at which BFD packets are transmitted is 200 ms; the interval at which BFD packets are received is 300 ms; the detection multiplier is 4.
- On the peer device, the configured interval at which BFD packets are transmitted is 100 ms; the interval at which BFD packets are received is 600 ms; the detection multiplier is 5.

Then:

- On the local device, the actual interval at which BFD packets are transmitted is 600 ms calculated by using the formula max {200 ms, 600 ms}; the interval at which BFD packets are received is 300 ms calculated by using the formula max {100 ms, 300 ms}; the detection period is 1500 ms calculated by multiplying 300 ms by 5.
- On the peer device, the actual interval at which BFD packets are transmitted is 300 ms calculated by using the formula max {100 ms, 300 ms}, the actual interval at which BFD packets are received is 600 ms calculated by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms calculated by multiplying 600 ms by 4.

Prerequisites

BFD has been enabled globally using the **bfd** command.

After BFD in the OSPFv3 process is enabled using the **bfd all-interfaces enable** command, OSPFv3 establish BFD sessions only with neighbors whose status is Full.

Follow-up Procedure

- Configure a BFD session on a specified interface.

  If you need to configure BFD on a specified interface, or if global BFD for OSPFv3 is configured but you want a specific interface to detect link faults faster, run the **ospfv3 bfd** command to configure BFD on the specified interface.
- Prevent an interface from dynamically creating a BFD session.

  If you do not want to enable BFD on a specified interface, run the **ospfv3 bfd block** command to disable the interface from dynamically creating a BFD session.

Precautions

The **bfd all-interfaces** command and the **ospfv3 bfd block** command are mutually exclusive.

BFD cannot be enabled on VBDIF interfaces.

Example

Enable BFD for OSPFv3 process 1.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] bfd all-interfaces enable
```

7.5.8 default (OSPFv3)

Function

The **default** command sets default parameters for the external routes that are imported by OSPFv3. The default parameters include the cost, tag and type (Type 1 or Type 2).

The **undo default** command restores the default values of the parameters of the external routes that are imported by OSPFv3.

By default, the cost, tag value, and type of the external routes is 1, 1, and Type 2, respectively.

Format

default { **cost** *cost* | **tag** *tag* | **type** *type* } *

undo default { **cost** [*cost*] | **tag** [*tag*] | **type** [*type*] } *

Parameters

Parameter	Description	Value
cost *cost*	Specifies the default cost of the external route that is imported by OSPFv3.	The value is an integer that ranges from 1 to 16777214. By default, the value is 1.
tag *tag*	Specifies the tag value of the external route that is imported by OSPFv3.	The value is an integer that ranges from 0 to 4294967295. By default, the value is 1.
type *type*	Specifies the type of the external route that is imported by OSPFv3.	The value is an integer that ranges from 1 to 2. By default, it is 2. ● 1: Type 1 external route ● 2: Type 2 external route

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Since OSPFv3 can import external routes and advertise them to the entire AS, it is necessary to specify a default cost for these external routes.

If multiple OSPFv3 processes are enabled, the **default** command takes effect only on the present process.

Example

Set the default cost of the external routes that are imported by OSPFv3 to 10.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] default cost 10
```

7.5.9 default-cost (OSPFv3 Area)

Function

The **default-cost** command specifies a cost for the default route that is sent to the stub area by OSPFv3.

The **undo default-cost** command restores the default cost of the default route.

By default, the cost of the Type 3 default route transmitted to the stub area is 1.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Specifies the cost of the default route that is sent to the stub area by OSPFv3.	The value ranges from 0 to 16777214. By default, the value is 1.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

The **default-cost** command applies only to the ABR that is connected to the stub area.

Before setting the cost of the default route that is transmitted to the stub area by OSPFv3, run the **stub** command to configure the local area as a stub area.

If multiple OSPFv3 processes are enabled, the **default-cost** command takes effect only on the present process.

Example

Set area 1 as the stub area and the cost of the default route that is sent to the stub area to 60.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 1
[HUAWEI-ospfv3-1-area-0.0.0.1] stub
[HUAWEI-ospfv3-1-area-0.0.0.1] default-cost 60
```

7.5.10 default-route-advertise (OSPFv3)

Function

The **default-route-advertise** command advertises default routes into an OSPFv3 routing domain.

The **undo default-route-advertise** command cancels advertising default routes.

Format

default-route-advertise [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name* [**match-any**]]*

undo default-route-advertise [**always** | **cost** [*cost*] | **type** [*type*] | **tag** [*tag*] | **route-policy** [*route-policy-name*] [**match-any**]]*

Parameters

Parameter	Description	Value
always	Generates and advertises an LSA that describes a default route, regardless of whether the local device has active default routes from processes other than the local OSPFv3 process. The switch that has **always** configured does not calculate default routes of other switches. If **always** is not specified, an LSA is generated only when there are active non-OSPFv3 default routes in the routing table of the local device.	-
cost *cost*	Specifies the cost of an advertised default route.	The value is an integer that ranges from 1 to 16777214. The default value is 1.
type *type*	Specifies the type of an external route.	The value is 1 or 2. The default value is 2. ● 1: Type 1 external route ● 2: Type 2 external route

Parameter	Description	Value
tag *tag*	Specifies the tag value of an advertised default route.	The value is an integer that ranges from 0 to 4294967295. The default value is 1.
route-policy *route-policy-name*	Specifies the name of a route-policy. The device advertises default routes according to the parameters configured in the route-policy when there are matched non-OSPFv3 default routes in the routing table.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
match-any	Indicates that through a route-policy, the device advertises default routes according to the parameters configured in the route-policy when there are matched routes in the routing table.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a static default route has been configured on an OSPFv3-capable switch, OSPFv3 compares the preferences of default routes before advertising a default route. To add the default route advertised by OSPFv3 to the current routing table, ensure that the preference of the static default route is lower than that of the default route advertised by OSPFv3.

Default routes that are imported using the **import-route** command cannot be advertised. To advertise default routes, run the **default-route-advertise** command. The cost of a generated default route is determined by the **cost** and **type** parameters in the **default-route-advertise** command, and the default **tag** value is 1. If the local routing table does not contain non-OSPFv3 default routes, specify the **always** parameter to generate an ASE LSA of a default route.

A route-policy is only used to filter existing active non-OSPFv3 default routes of the local device, and match routes according to the following rules:

- If a default route matches the policy, the local device generates a default route according to the parameters configured in the route-policy, such as the cost, tag, and type.

- If a default route does not match the policy and **always** is not specified, the local device does not generate any default route.
- If a default route does not match the policy and **always** is specified, the switch generates a default route. The parameters of the generated default route are determined by the **default-route-advertise** [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*]* command.

NOTE

The preferences of parameters of the default route configured in a route-policy are higher than those of parameters configured in the **default-route-advertise** [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * command.

Precautions

Creating a route-policy before it is referenced is recommended. If a nonexistent route-policy is referenced using the command, the device advertises the default IPv6 route as long as a default IPv6 route that is not generated by the current OSPFv3 process exists in the local routing table.

Example

Advertise the ASE LSA that describes a default route into an OSPFv3 routing domain. The local device does not have a default route.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] default-route-advertise always
```

7.5.11 description (OSPFv3 Area)

Function

The **description** command configures a description for an OSPFv3 area.

The **undo description** command deletes the configured description of an OSPFv3 area.

By default, there is no description for any OSPFv3 areas.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies a description for an OSPFv3 area.	The value is a string of 1 to 80 case-sensitive characters, spaces supported.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

By configuring a description for an OSPFv3 area, you can identify different OSPFv3 areas easily.

Example

Configure a description for OSPFv3 area 0.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 0
[HUAWEI-ospfv3-1-area-0.0.0.0] description main area
```

7.5.12 description (OSPFv3)

Function

The **description** command configures a description for an OSPFv3 process.

The **undo description** command deletes the configured description of an OSPFv3 process.

By default, there is no description for any OSPFv3 processes.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies a description for an OSPFv3 process.	The value is a string of 1 to 80 case-sensitive characters, spaces supported.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

By configuring a description for an OSPFv3 process, you can identify different OSPFv3 processes easily.

Example

Configure a description for OSPFv3 process 1.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] description main process
```

7.5.13 display default-parameter ospfv3

Function

The **display default-parameter ospfv3** command displays the default OSPFv3 configuration.

Format

display default-parameter ospfv3

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the default configurations, regardless of whether the configurations about OSPFv3 parameters are changed.

Example

Display the default OSPFv3 configuration.

```
<HUAWEI> display default-parameter ospfv3

OSPFv3 Default Values:

Process View:
----------------------------------------------------
  Maximum ECMP Count                    : 8
  SPF Delay Time(sec)                   : 5
  SPF Hold Time(sec)                    : 10
  SPF Max Time(millisec)                : 10000
  SPF Start Time(millisec)              : 500
  SPF ExpHold Time(millisec)            : 2000
```

```
  LSA Reorig Time(sec)                    : 5
  Wait Interval for stub-router on-startup   : 500
  Grace Period(sec)                       : 120
  Retransmit-Interval for Grace LSAs(sec)    : 5
  Ack wait-time for Grace LSAs(sec)          : 15
  Helper Max Grace Period Support(sec)       : 1800
  Bandwidth-Reference(Mbps)                  : 100
  Sham Link Cost                          : 1
  VPN Domain ID                           : 0
  VPN Router Tag                          : 0
  Default Metric                          : 1
  Default Tag                             : 1
  Default Type                            : 2
  Route Preference for Internal Routes       : 10
  Route Preference for External Routes       : 150
  Suppress flapping peer                  : Enable
-----------------------------------------------------

Area View:
-----------------------------------------------------
  Default Stub Cost                       : 1
  NSSA Translator Stability Index(sec)       : 40
-----------------------------------------------------

Interface View:
-----------------------------------------------------
  Hello Interval(sec)                     : 10
  NBMA Hello Interval(sec)                   : 30
  Dead Interval(sec)                      : 40
  NBMA Dead Interval(sec)                    : 120
  Poll Interval(sec)                      : 120
  Retransmit Interval(sec)                   : 5
  Transmit Delay(sec)                      : 1
  Router DR Priority                      : 1
  Suppress flapping peer                  : Enable
  Suppress flapping detect interval          : 60
  Suppress flapping detect threshold         : 10
  Suppress flapping Resume interval          : 120
  Suppress flapping mechanism                : Hold-max-cost
  Hold-max-cost interval                  : 120
```

Table 7-62 Description of the **display default-parameter ospfv3** command output

Item	Description
OSPFv3 Default Values	Default values of OSPFv3
Process View	Process view
Area View	Area view
Interface View	Interface view
Maximum ECMP Count	Maximum number of equal-cost routes
SPF Delay Time(sec)	Default delay for SPF calculation
SPF Hold Time(sec)	Hold time interval between two consecutive SPF calculations
SPF Max Time(millisec)	Maximum delay time between two consecutive SPF calculations
SPF Start Time(millisec)	Initial SPF schedule delay

Item	Description
SPF ExpHold Time(millisec)	Minimum hold time between two consecutive SPF calculations
LSA Reorig Time(sec)	Interval at which LSAs are updated
Wait Interval for stub-router on-startup	Default period during which a router remains to be a stub router during master/slave switchover
Grace Period(sec)	GR period
Retransmit-Interval for Grace LSAs(sec)	Default interval for retransmitting Grace LSAs, in seconds
Ack wait-time for Grace LSAs(sec)	Default time during which a router waits to reply the received Grace LSA with an LSAck message If the switch does not receive any Grace LSA within the default waiting time, the switch does not send the LSAck message.
Helper Max Grace Period Support(sec)	Default GR period of the helper router
Bandwidth-Reference(Mbps)	Default bandwidth reference value used to calculate the link cost, in Mbit/s
Default Metric	Default metric of the imported external route
Default Type	Default type of the imported external route
Route Preference for Internal Routes	Default preference of the internal route
Route Preference for External Routes	Default preference of the external route
Default Stub Cost	Default cost of a stub area
NSSA Translator Stability Index(sec)	Default dead time of a translator
Hello Interval(sec)	Default interval for sending Hello packets on a P2P or a broadcast network
NBMA Hello Interval(sec)	Default interval for sending Hello packets on an NBMA network
Dead Interval(sec)	Default interval for declaring a neighbor to be Down after no Hello packets are received on a P2P or broadcast network

Item	Description
NBMA Dead Interval(sec)	Default interval for declaring a neighbor to be Down after no Hello packets are received on an NBMA network
Poll Interval(sec)	Default poll interval for sending Hello packets on an NBMA network
Retransmit Interval(sec)	Default interval for retransmitting packets
Transmit Delay(sec)	Default estimated time for transmitting an LSU over this interface Before packet transmission, the estimated time needs to be added to the time limit of each LSA. The estimated time should be added to the transmission delay of the inbound interface.
Router DR Priority	Default priority of the DR
Suppress flapping peer	Whether OSPFv3 neighbor relationship flapping suppression is enabled
Suppress flapping detect interval	Default detection interval of OSPFv3 neighbor relationship flapping suppression
Suppress flapping detect threshold	Default threshold of OSPFv3 neighbor relationship flapping suppression
Suppress flapping Resume interval	Default interval for exiting from OSPFv3 neighbor relationship flapping suppression
Suppress flapping mechanism	Default mode of OSPFv3 neighbor relationship flapping suppression
Hold-max-cost interval	Default duration of the Hold-max-cost mode

7.5.14 display ospfv3

Function

The **display ospfv3** command displays brief information about OSPFv3.

Format

display ospfv3 [*process-id*]

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID. If process-id is not specified, the brief information of all OSPFv3 processes is displayed in the ascending order of the process ID.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3** command to check brief information about OSPFv3. The information helps learn about the OSPFv3 configuration and status.

Example

Display brief information about OSPFv3.

```
<HUAWEI> display ospfv3

 Routing Process "OSPFv3 (1)" with ID 0.0.0.0
 Route Tag: 0
 Multi-VPN-Instance is not enabled
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 LSA Origination interval 5 secs
 LSA Arrival interval 1 sec
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Stub router capability: enabled
 Number of AS-External LSA 0. AS-External LSA's Checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0. AS-Scoped Unknown LSA's Checksum Sum 0x0000
 Number of FULL neighbors 0
 Number of Exchange and Loading neighbors 0
 Number of LSA originated 0
 Number of LSA received 0
 SPF Count          : 0
 Non Refresh LSA    : 0
 Non Full Nbr Count : 0
 Number of areas in this router is 0
```

Table 7-63 Description of the **display ospfv3** command output

Item	Description
Route Tag	Tag value for the imported VPN route.
Multi-VPN-Instance is not enabled	The current process does not support Multi-VPN instance.

Item	Description
SPF schedule delay	Delay of SPF calculation after the SPF calculation is scheduled.
Hold time between SPFs	Interval between two SPF calculation.
LSA Origination interval	Minimum interval for producing the same LSA.
LSA Arrival interval	Minimum interval for receiving the same LSA.
Default ASE parameters	Default parameters for AS external LSA: ● Metric: cost of the route ● Tag: tag value ● Type: type of LSA (1 or 2)
Stub router capability	Stub router capability. If **on-startup** is not specified when the **stub-router** command is run, information about this field is always displayed. If **on-startup** is specified when the stub-router command is run, information about this field is displayed only in the valid period during which the device keeps serving as a stub router after being restarted.
Number of AS-External LSA	Number of LSA originated for routes outside an AS.
AS-External LSA's Checksum Sum	Checksum of LSA originated for routes outside an AS.
Number of AS-Scoped Unknown LSA	Number of unknown LSA with the flooding range of an entire AS.
AS-Scoped Unknown LSA's Checksum Sum	Checksum of unknown LSA with the flooding range of an entire AS.
Number of FULL neighbors	Number of Full neighbors.
Number of Exchange and Loading neighbors	Number of neighbors in the Exchange state and neighbors in the Loading state.
Number of LSA originated	Number of generated LSAs.
Number of LSA received	Number of received LSAs.
SPF Count	Number of the events triggered by the SPF calculation.
Non Refresh LSA	Number of LSAs that are not updated in the retransmission list during GR.

Item	Description
Non Full Nbr Count	Number of neighbors in the Exchange state and neighbors in the Loading state during GR.
Number of areas in this router is	Number of areas on a switch.

7.5.15 display ospfv3 abr-summary-list

Function

The **display ospfv3 abr-summary-list** command displays information about the summarization of the routes imported by OSPFv3.

If the IP address and mask are not specified, information about the summarization of all the routes imported by OSPFv3 is displayed.

Format

display ospfv3 [*process-id*] **abr-summary-list** [*ipv6-address prefix-length*]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
ipv6-address	Specifies the matched IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of the route prefix.	The value is an integer ranging from 1 to 128.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 abr-summary-list** command to check information about the summarization of the routes imported by an ABR. If the IP address and mask are not specified, information about the summarization of all the routes imported by the ABR is displayed.

Example

Display information about the summarization of all the routes imported by OSPFv3.

```
<HUAWEI> display ospfv3 abr-summary-list
OSPFv3 Process (1)
Area ID  :  0.0.0.1
Prefix           Prefix-Len  Matched       Status
FC00:0:0:2001::  16          2[Active]     Advertise
FC00:0:0:3001::  16          0[NotActive]  Advertise
FC00:0:0:4001::  16          0[NotActive]  Advertise
```

Table 7-64 Description of the **display ospfv3 abr-summary-list** command output

Item	Description
OSPFv3 Process (1)	OSPFv3 process ID
Area ID	Area ID
Prefix	IPv6 prefix
Prefix-Len	Length of the prefix
Matched	Status of the summarized routes
Status	Advertisement status of the summarized routes: ● Advertise: Advertise after the summarization. ● NotAdvertise: Do not advertise after the summarization.

7.5.16 display ospfv3 area

Function

The **display ospfv3 area** command displays OSPFv3 area information.

Format

display ospfv3 [*process-id*] **area** [*area-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID for an OSPFv3 process.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
area-id	Specifies the area ID for the area to be displayed.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 area** command to check OSPFv3 area information. The information helps determine the status and parameters of each area.

Example

Display OSPFv3 area information.

```
<HUAWEI> display ospfv3 area
OSPFv3 Process (1)

Area 0.0.0.0(BACKBONE)  InActive
Number of interfaces in this area is 1
 SPF algorithm executed 0 times
 Number of LSA 0. Checksum Sum 0x0000
 Number of Unknown LSA 0
 Area Bdr Router count: 0
 Area ASBdr Router count: 0
 Next SPF Trigger Time 500 millisecs
 Router ID conflict state : Normal
```

Table 7-65 Description of the display ospfv3 area command output

Item	Description
Number of interfaces in this area	Number of active interfaces.
SPF algorithm executed	Number of SPF calculations.
Number of LSA	Number of LSAs in this area.
Checksum	Area checksum.
Number of Unknown LSA	Number of unknown LSAs in the area.
Area Bdr Router count	Number of ABRs in the area.
Area ASBdr Router count	Number of ASBRs in the area.
Next SPF Trigger Time	Interval for SPF calculations in the area.

Item	Description
Router ID conflict state	Status of the automatic recovery function. The value can be one of the following: ● Normal: The automatic recovery function is properly detecting router ID conflict. ● Wait select: The automatic recovery function delays defining a new router ID if the device starts after an unexpected delay (two hours by default). ● Selecting: The automatic recovery function restarts the OSPF process with the router ID and waits for the restarted OSPF process to take effect. ● RtrId Changed: The automatic recovery function determines whether router ID conflict occurs after the new router ID takes effect and returns to the Normal state if no new router ID conflict is detected. ● Suspend: If the maximum number of conflict times is reached, automatic recovery function does not define a new router ID any longer. The maximum number of conflict times is three by default.

7.5.17 display ospfv3 asbr-summary

Function

The **display ospfv3 asbr-summary** command displays OSPFv3 route summarization information.

Format

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies an OSPFVv3 process ID.	The value is an integer in the range from 1 to 65535.

Parameter	Description	Value
ipv6-address prefix-length	Specifies an IPv6 address and route prefix length. If both *ipv6-address* and *prefix-length* are not specified, all OSPFv3 route summarization information is displayed.	- The IPv6 address is a 32-digit hexadecimal number in the X:X:X:X:X:X:X:X format. - The prefix length ranges from 1 to 128.
verbose	Displays detailed information about OSPFv3 route summarization.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view OSPFv3 route summarization information, run the **display ospfv3 asbr-summary** command.

Example

Display detailed information about OSPFv3 route summarization.

```
<HUAWEI> display ospfv3 asbr-summary verbose

      OSPFv3 Process (1)
 Total summary address count :1

          Summary Address

 Prefix        : 10::
 Prefix length : 32
 Tag           : 0 (Not Configured)
 Status        : Advertised
 Cost          : 10 (Configured)
 Delay         : (Not Configured)
 Type          : 2 (Larger than any link state path)
 The Count of Route is: 3

Destination      Mask        Protocol      Proc       Type     Metric
    10::0         64         Static        0          2        1
    10::2         128        Static        0          2        1
    10::3         128        Static        0          2        1
```

Table 7-66 Description of the **display ospfv3 asbr-summary** command output

Item	Description
OSPFv3 Process	OSPFv3 process ID.

Item	Description
Total Summary address count	Number of summary routes. To configure summary routes, run the **asbr-summary** command.
Summary Address	Detailed information about summary routes.
Prefix	Prefix of a summary route.
Prefix length	Prefix length.
Tag	Tag of a summary route.
Status	Whether summary routes are advertised: ● Advertised: Summary routes will be advertised. ● NotAdvertised: Summary routes will not be advertised.
Cost	Cost of a summary route.
Delay	Delay in advertising summary routes.
Type	AS external route type: ● 1: Type 1 external route ● 2: Type 2 external route
The Count of Route is	Number of routes that are summarized.
Destination	Destination address of a summary route.
Mask	Mask of a summary route.
Protocol	Protocol of a summary route.
Proc	Protocol process ID of a summary route.
Metric	Cost of a summary route.

7.5.18 display ospfv3 bfd session

Function

The **display ospfv3 bfd session** command displays bidirectional forwarding detection (BFD) session information of all OSPFv3 processes.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

display ospfv3 [*process-id*] **bfd session** [*interface-type interface-number*] [*neighbor-id*] [**verbose** | **all**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID for an OSPFv3 process. If the process number is not specified, information about all OSPFv3 processes is displayed in an ascending order.	The value is an integer that ranges from 1 to 65535.
interface-type interface-number	Specifies the name, type and the number of the interface.	-
neighbor-id	Specifies router ID of the neighbor.	-
verbose	Displays detailed information of the neighbor.	-
all	Displays all the BFD sessions configured in OSPFv3.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

BFD can provide millisecond-level fault detection. BFD can work with OSPFv3 to rapidly detect faults on neighboring devices, and instruct OSPFv3 to recalculate routes for correct packet forwarding. You can run the command to check BFD session parameters in OSPFv3 processes.

Example

Display BFD session information of all OSPFv3 processes.

```
<HUAWEI> display ospfv3 bfd session
```

```
* - STALE

OSPFv3 Process (1)
 Neighbor-Id      Interface                    BFD-Status
 10.3.3.3         GE0/0/1                     Up
 10.1.1.1         GE0/0/2                     Up
```

Table 7-67 Description of the **display ospfv3 bfd session** command output

Item	Description
* - STALE	Stale BFD session
OSPFv3 Process	ID of the OSPFv3 process
Neighbor-Id	Neighbor ID
Interface	Interface to which this session is associated
BFD-Status	BFD session status: ● Up ● Down

Display the BFD session information for process 1.

```
<HUAWEI> display ospfv3 1 bfd session verbose

* - STALE

OSPFv3 Process (1)

 Neighbor-Id: 10.3.3.3
 BFD Status: Up
 Interface: GE0/0/1
 IPv6-Local-Address: FE80::201:FF:FE01:1
 IPv6-Remote-Address: FE80::225:9EFF:FEFB:BFF1
 BFD Module preferred timer values
     Transmit-Interval(ms): 100
     Receive-Interval(ms): 100
     Detect-Multiplier: 4
 OSPFv3 Module preferred timer values
     Transmit-Interval(ms): 100
     Receive-Interval(ms): 100
     Detect-Multiplier: 4
 Configured timer values
     Transmit-Interval(ms): 100
     Receive-Interval(ms): 100
     Detect-Multiplier: 4
```

Table 7-68 Description of the **display ospfv3 bfd session** command output

Item	Description
IPv6-Local-Address	Local IPv6 address to which this session is associated

Item	Description
IPv6-Remote-Address	Remote IPv6 address to which this session is associated
BFD Module preferred timer values	Actual BFD parameter values which are negotiated by BFD Module for the established session
Transmit-Interval(ms)	Minimum interval for sending BFD packets
Receive-Interval(ms)	Minimum interval between received BFD packets
Detect-Multiplier	Detection multiplier
OSPFv3 Module preferred timer values	Preferred BFD parameter values across the processes sharing the session
Configured timer values	Configured BFD parameter values for the neighbor

Display all the BFD sessions in OSPFv3.

```
<HUAWEI> display ospfv3 bfd session all

* - STALE

BFD Session (1)
 BFD Status: Up
 Interface: GE0/0/1
 IPv6-Local-Address: FE80::201:FF:FE01:1
 IPv6-Remote-Address: FE80::225:9EFF:FEFB:BFF1
 Process-Id  Neighbor-Id
      1      10.3.3.3

BFD Session (2)
 BFD Status: Up
 Interface: GE0/0/2
 IPv6-Local-Address: FE80::201:FF:FE01:1
 IPv6-Remote-Address: FE80::200:13FF:FE82:4569
 Process-Id  Neighbor-Id
      1      10.1.1.1
```

Table 7-69 Description of the **display ospfv3 bfd session all** command output

Item	Description
BFD Session	BFD session number configured in OSPFv3
Process-Id	Configured OSPFv3 process ID
Neighbor-Id	Neighbor ID

7.5.19 display ospfv3 black-box neighbor-down

Function

The **display ospfv3 black-box neighbor-down** command displays detailed information about OSPFv3 neighbors in the Down state.

Format

display ospfv3 black-box neighbor-down [*number*]

Parameters

Parameter	Description	Value
number	Specifies the number of OSPFv3 neighbors in the Down state to be displayed.	The value is an integer ranging from 1 to 10.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *number* is not specified, the **display ospfv3 black-box neighbor-down** command displays detailed information about the latest 10 OSPFv3 neighbors in the Down state.

Example

Display the latest 2 OSPFv3 neighbors in the Down state.

```
<HUAWEI> display ospfv3 black-box neighbor-down 2
 Neighbor Router-id                    : 10.11.11.99
 Interface                             : Vlanif10
 Process ID                            : 99
 Instance ID                           : 1
 Reason for Neighbor down              : Interface down
 Time at which neighbor went down      : 2010-12-28 12:45:20+08:00
 Neighbor Router-id                    : 10.11.11.99
 Interface                             : Vlanif10
 Process ID                            : 99
 Instance ID                           : 1
 Reason for Neighbor down              : One-way received
 Time at which neighbor went down      : 2010-12-28 12:45:20+08:00
```

Table 7-70 Description of the **display ospfv3 black-box neighbor-down** command output

Item	Description
Neighbor Router-id	Router ID of a neighbor whose neighbor relationship becomes Down
Interface	Interface of a device involved in a neighbor relationship
Process ID	ID of the OSPFv3 process to which the neighbor relationship belongs
Instance ID	ID of the OSPFv3 instance to which the neighbor relationship belongs
Reason for Neighbor down	Reason why a neighbor relationship becomes Down: ● Interface down ● Dead timer expired ● Sequence number mismatch ● One-way received ● Forced down ● Bad LS request ● DR or BDR has changed
Time at which neighbor went down	Date and time at which the neighbor went Down.

7.5.20 display ospfv3 error

Function

The **display ospfv3 error** command displays the OSPFv3 errors.

Format

display ospfv3 [*process-id*] **error** [**lsa**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID. If no OSPFv3 process number is specified, errors of all OSPFv3 processes are displayed.	The value ranges from 1 to 65535.
lsa	Display the OSPFv3 LSA errors	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

While analyzing the faults of OSPFv3, you can obtain information of errors using the command. You can then diagnose the faults of OSPFv3 according to information.

Example

Display the errors of OSPFv3.

```
<HUAWEI> display ospfv3 error
         OSPFv3 Process 1 with Router ID 0.0.0.0
                 OSPFv3 Error Statistics

General Packet Errors :
 0          : Bad packet                    0          : Bad version
 0          : Bad area ID                   0          : Bad virtual link
 0          : Packet too small              0          : Transmit error
 0          : Bad Instance ID               0          : Interface down
 0          : Unknown neighbor              0          : Authentication failure
 0          : AuthSeqNum mismatch           0          : AuthKeyId mismatch
 0          : IPv6: received my own packet  0          : Bad Checksum

Hello Packet Errors :
 0          : Hello timer mismatch          0          : Dead timer mismatch
 0          : Extern option mismatch        0          : Router ID confusion
 0          : Virtual neighbor unknown

DD Packet Errors :
 0          : Neighbor state low            0          : Extern option mismatch
 0          : Unknown LSA Type              0          : MTU option mismatch
 0          : Router ID confusion

LS ACK packet Errors :
 0          : Neighbor state low            0          : Bad ACK
 0          : Duplicate ACK                 0          : Unknown LSA type

LS REQ packet Errors :
 0          : Neighbor state low            0          : Bad request
 0          : Empty Request

LS UPD packet Errors :
 0          : Neighbor state low            0          : LSA checksum bad
 0          : Received less recent LSA      0          : Unknown LSA type
 0          : Newer self-generate LSA
 0          : Received LSA within LSA Arrival interval

Receive Grace LSA errors :
 0          : Number of invalid LSAs
 0          : Number of policy failed LSAs
 0          : Number of wrong period LSAs

License Errors :
 0          : Max external routes reached   0          : Max NBRs reached
```

Table 7-71 Description of the **display ospfv3 error** command output

Item	Description
General Packet Errors	General packet errors.
Bad packet	The analyzed packet errors, including the verification of the length field.
Bad version	OSPFv3 version errors, that is, it is not version 3.
Bad area ID	Area ID in the received packet does not match. That is, when the area IDs in the received packets are different from the local area ID, except area 0, other area IDs are considered incorrect.
Bad virtual link	V-link receives illegal packets.
Packet too small	Length of the received packet is less than the sum of length of IP header and the length field of the packet.
Transmit error	Transmitting packets to socket fails.
Bad Instance ID	The Instance ID errors
Interface down	Times that the OSPFv3 interface goes Down.
Unknown neighbor	For NBMA, sham-link, and V-link networks, the device receives OSPFv3 packets from neighbors that are not enabled with OSPFv3.
Authentication failure	Times that the authentication fails.
AuthSeqNum mismatch	Number of packets with a sequence number different from the local one
AuthKeyId mismatch	Number of packets with key IDs different from the local one
IPv6: received my own packet	Number of IPv6 packets received from self.
Bad Checksum	Number of packets that fail in the check and calculation
Hello Packet Errors	Hello packet errors.
Hello timer mismatch	The Hello interval is not consistent.
Dead timer mismatch	The Dead interval is not consistent.
Extern option mismatch	The extension attributes of Hello packets are not consistent.
Router ID confusion	Router id is configured to the same.

Item	Description
Virtual neighbor unknown	Router id of the packet is inconsistent with that of the neighbor that is configured by the V-link.
DD Packet Errors	DD packet errors.
Neighbor state low	Cases of error: ● DD packet is received but its neighbor status is lower than 2-way. ● LSR packet is received but its neighbor status is lower than Exchange. ● LSU packet is received but its neighbor status is lower than Exchange. ● ACK packet is received but its neighbor status is lower than Exchange.
Extern option mismatch	Option of the DD packets is not matched.
Unknown LSA Type	The router receives unknown LSA type from neighbors that are not enabled with OSPFv3.
MTU option mismatch	MTU check of the interface on which OSPFv3 is enabled. The MTU value of the DD packet that is received on the interface is greater than that of this interface.
LS ACK packet Errors	LS ACK packet errors.
Bad ACK	The count of receiving incorrect ACK packets.
Duplicate ACK	The count of receiving repeat ACK packets.
LS REQ packet Errors	Title bar: LS REQ packet errors.
Bad request	BadRequest event in the protocol.
Empty Request	Number of Empty Request.
LS UPD packet Errors	LS UPD packet error.
LSA checksum bad	LSA checksum not proper
Received less recent LSA	Receiving older LSA than the local copy.
Newer self-generate LSA	LSA recently generated by self.
Received LSA within LSA Arrival interval	Received LSA within arrival interval.
Receive Grace LSA errors	Title bar: Grace LSA error.
Number of invalid LSAs	Number of LSAs that are invalid.
Number of policy failed LSAs	Number of LSAs with policy failure.

Item	Description
Number of wrong period LSAs	Number of LSAs with wrong period.
License Errors	License errors.
Max external routes reached	Number of external routes reached the maximum value.
Max NBRs reached	Number of neighbors reached the maximum value.

7.5.21 display ospfv3 graceful-restart-information

Function

The **display ospfv3 graceful-restart-information** command displays the status of OSPFv3 GR.

Format

display ospfv3 [*process-id*] **graceful-restart-information**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process number. If the process number is not specified, brief information about all OSPFv3 processes is displayed in an ascending order.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 graceful-restart-information** command to check the status of OSPFv3 GR.

Example

Display the status of OSPFv3 GR.

```
<HUAWEI> display ospfv3 graceful-restart-information
```

```
          OSPFv3 Router with ID (10.0.0.0) (Process 1)

Graceful-restart capability      : enabled
Graceful-restart support         : planned and unplanned, strict lsa check
Grace-Period Configured            : 120 Sec
Last Restart-exit Reason         : none

Helper capability                : enabled
  Last Helper-exit Reason          : none
```

Table 7-72 Description of the **display ospfv3 graceful-restart-information** command output

Item	Description
Graceful-restart capability	Whether GR is enabled: ● enabled ● disabled
Graceful-restart support	GR configuration feature. ● planned: indicates that only the planned GR is supported. ● unplanned: indicates that only the unplanned GR is supported. ● strict lsa check: indicates that the Helper supports strict external LSA check.
Grace-Period Configured	GR period.

Item	Description
Last Restart-exit Reason	Reason for the Restart device exiting from GR last time: ● none: indicates that no GR is performed. ● successful: indicates that the device is successfully restarted through GR, and then exits from GR. ● topology change: indicates that the network topology changes. ● grace lsa not recv: indicates that no Grace-LSAs are received. ● grace period exp: indicates that the GR period expires. ● process reset: indicates that a parameter of the OSPFv3 process is reset during GR. ● hold timer expire: indicates that the hold timer expires. ● interface address deleted: indicates that the interface address is deleted. ● interface down: indicates that the interface goes Down. ● DR/BDR change on network: indicates that the DR or BDR on the network changes. ● Received route uninstall notification: indicates that the message indicating that OSPFv3 routes are not installed to the RM is received.
Helper capability	Whether Helper is enabled: ● enabled ● disabled

Item	Description
Last Helper-exit Reason	Reason for the Helper device exiting from GR last time: ● none: indicates that the switch never enters the Helper mode since it starts. ● successful: indicates that the Helper successfully exits from GR. ● topology change: indicates that the network topology changes. ● interface id change: indicates that the interface ID changes. ● grace period exp: indicates that GR period expires. ● hold timer expire: indicates that the hold timer expires. ● interface address deleted: indicates that the interface address is deleted.

7.5.22 display ospfv3 interface

Function

The **display ospfv3 interface** command displays information about OSPFv3 interfaces.

Format

display ospfv3 [*process-id*] **interface** [**area** *area-id*] [*interface-type interface-number*]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID. The value of the area ID can be a decimal integer or in the IPv4 address format.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of the interface. If the interface is not specified, information of all OSPFv3 interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 interface** command to check information about OSPFv3 interfaces.

Example

Display information about OSPFv3 VLANIF 10.

```
<HUAWEI> display ospfv3 interface vlanif 10
 Vlanif10 is up, line protocol is up
 Interface ID 0x45
 Interface MTU 1500
 IPv6 Prefixes
 FE80::2E0:13FF:FE96:1600 (Link-Local Address)
 FC00:0:0:4000::1/64
 OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
       Router ID 10.5.5.5, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State Backup, Priority 1
   No designated router on this link
   No backup designated router on this link
   Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:08
   Neighbor Count is 1, Adjacent neighbor count is 1
   Interface Event: 2, Lsa Count: 2, Lsa Checksum: 0x9b74
   Interface Physical BandwidthHigh 0, BandwidthLow 1000000000
```

Display information about VLANIF 10 after OSPFv3 neighbor relationship flapping suppression is configured.

```
<HUAWEI> display ospfv3 interface Vlanif 10
 Vlanif10 is up, line protocol is up
  Interface ID 0x7
  Interface MTU 1500
  IPv6 Prefixes
    FE80::2E0:74FF:FE00:8201 (Link-Local Address)
    FC00:3::1/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 4.4.4.4
    Interface Address FE80::2E0:4FF:FE09:8201
    Backup Designated Router (ID) 1.1.1.1
    Interface Address FE80::2E0:74FF:FE00:8201
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
       Hello due in 00:00:09
```

```
  Neighbor Count is 1, Adjacent neighbor count is 1
  Interface Event 3, Lsa Count 2, Lsa Checksum 0x15084
  Interface Physical BandwidthHigh 0, BandwidthLow 100000000
  Suppress flapping peer: enable(flapping-count: 0, threshold: 3)
```

Table 7-73 Description of the **display ospfv3 interface** command output

Item	Description
Interface ID	Interface ID
Interface MTU	MTU value
IPv6 Prefixes	IPv6 prefixes
Link-Local Address	Address of local link
OSPFv3 Process	OSPFv3 process ID
Area	Area that the interface belongs to
Instance ID	ID of the instance that the interface belongs to
Router ID	Router ID
Network Type	Network type of the interface that can be displayed as Point-to-Point, NBMA, Point-To-Multipoint and Broadcast
Cost	Cost of the interface. To set the cost of the interface in different instances, run the **ospfv3 cost** command.
Transmit Delay	Transmission delay
State	State of the interface
Priority	Priority of the interface
Designated Router (ID)	Designated router on the link
Backup Designated Router (ID)	Backup designated router on the link

Item	Description
Timer interval configured	Configured interval - Hello: Interval for sending Hello packets. To set the interval for sending Hello packets on the interface instance, run the **ospfv3 timer hello** command. - Dead: Interval of the Dead timer. To set the dead interval of the OSPFv3 neighbor of the instance on the interface, run the **ospfv3 timer dead** command. - Wait: Interval of the Wait timer - Retransmit: Retransmission interval. To set interval for retransmitting the LSA on the interface instance, run the **ospfv3 timer retransmit** command.
Hello due in	Time remaining to send Hello packet
Neighbor Count	Number of neighbors
Adjacent neighbor count	Number of adjacency
Interface Event	Number of events on this interface
Lsa Count	Total number of LSA in the interface scope database
Lsa Checksum	Checksum of all the LSAs in the database
Interface Physical BandwidthHigh	Maximum physical bandwidth on the interface
BandwidthLow	Minimum physical bandwidth on the interface

Item	Description

Suppress flapping peer	Status of OSPFv3 neighbor relationship flapping suppression:
	● enable: OSPFv3 neighbor relationship flapping suppression is enabled.
	– flapping-count: number of valid flapping_events
	If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count is incremented by 1. To change *detecting-interval*, run the **ospfv3 suppress-flapping peer detecting-interval** *detecting-interval* command.
	– threshold: flapping suppression threshold
	When the flapping_count reaches or exceeds **threshold**, flapping suppression takes effect. To configure the threshold, run the **ospfv3 suppress-flapping peer threshold** *threshold* command.
	● disable: OSPFv3 neighbor relationship flapping suppression is disabled. In this case, the following information is displayed, without flapping-count or threshold:
	`Suppress flapping peer: disable`
	● hold-down: OSPFv3 neighbor relationship flapping suppression works in Hold-down mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-down(start: 2016-01-29 12:09:36-08:00, remain-interval: 500s)`
	– start: time when the flapping suppression started
	– remain-interval: remaining time of the flapping suppression
	● hold-max-cost: OSPFv3 neighbor relationship flapping suppression works in Hold-max-cost mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-max-cost(start: 2016-01-29 12:09:36-08:00, remain-interval: 476s)`

7.5.23 display ospfv3 lsdb

Function

The **display ospfv3 lsdb** command displays the OSPFv3 LSDB.

Format

display ospfv3 [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** | **nssa** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** | **grace** } [*link-state-id*]]

display ospfv3 [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]

display ospfv3 [*process-id*] **lsdb statistics**

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID. The value of the area ID can be a decimal integer or in the IPv4 address format.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.
external	Displays the AS-external LSA in the LSDB. If the **area** parameter is selected, the **external** parameter cannot be selected.	-
grace	Displays the Grace-LSA in the LSDB.	-
inter-prefix	Displays the Inter-area-prefix LSA in the LSDB.	-
nssa	Displays the NSSA in the LSDB.	-
inter-router	Displays the Inter-area-router LSA in the LSDB.	-

Parameter	Description	Value
intra-prefix	Displays the Intra-area-prefix LSA in the LSDB.	-
link	Displays the Link-local LSA in the LSDB.	-
network	Displays the Network-LSA in the LSDB.	-
router	Displays the Router-LSA in the LSDB.	-
link-state-id	Indicates the link state ID.	The value is in dotted decimal notation.
originate-router *advertising-router-id*	Specifies the Router ID of the switch that advertises LSA packet.	The value is in dotted decimal notation.
asbr-router *asbr-router-id*	Specifies the router ID of the ASBR.	The value is in dotted decimal notation.
self-originate	Displays LSAs in the LSDB that are advertised by the local switch.	-
ipv6-address prefix-length	Specifies the IPv6 destination address and the length of the prefix.	*ipv6-address* is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X. *prefix-length* is an integer ranging from 0 to 128.
statistics	Indicates the statistics of the LSDB.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 lsdb** command to check the OSPFv3 LSDB.

Example

Display the OSPFv3 LSDB.

```
<HUAWEI> display ospfv3 lsdb
* indicates STALE LSA

         OSPFv3 Router with ID (10.5.5.5) (Process 1)
            Link-LSA (Interface Vlanif1002)

Link State ID   Origin Router    Age   Seq#       CkSum  Prefix
0.0.0.71        10.2.2.2         0995  0x8000000c 0xa44c      1
0.0.0.69        10.5.5.5         0621  0x8000000f 0x20ff      1

            Router-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum    Link
0.0.0.0         10.2.2.2         0565  0x8000008b 0xa54f      1
0.0.0.0         10.5.5.5         0616  0x80000014 0x243c      1

            Network-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.71        10.2.2.2         0565  0x8000000a 0x585c

            Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         10.2.2.2         0320  0x8000000c 0x6a0f
0.0.0.2         10.2.2.2         1637  0x8000000b 0xe1a3
0.0.0.1         10.5.5.5         0616  0x8000000d 0x81f7

            Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum  Prefix  Reference
0.0.0.1         10.2.2.2         0564  0x8000000e 0x79a6      1  Network-LSA

            Router-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum    Link
0.0.0.0         10.5.5.5         0621  0x8000000b 0x8c84      0

            Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         10.5.5.5         0621  0x8000000a 0x8f08
0.0.0.2         10.5.5.5         0612  0x8000000a 0x105d
0.0.0.3         10.5.5.5         0612  0x8000000a 0x85f2

            Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum  Prefix  Reference
0.0.0.1         10.5.5.5         0621  0x8000000b 0xab89      1  Router-LSA

            Router-LSA (Area 0.0.0.3)

Link State ID   Origin Router    Age   Seq#       CkSum    Link
0.0.0.0         10.5.5.5         0621  0x8000000b 0x8092      0

            Inter-Area-Prefix-LSA (Area 0.0.0.3)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         10.5.5.5         0617  0x8000000b 0x85f5
0.0.0.2         10.5.5.5         0621  0x8000000a 0x8511
0.0.0.3         10.5.5.5         0612  0x8000000a 0x0666
0.0.0.4         10.5.5.5         0612  0x8000000a 0x7bfb

            NSSA-external-LSA (Area 0.0.0.3)
```

```
Link State ID   Origin Router    Age   Seq#       CkSum  Type
0.0.0.1         10.5.5.5         0626  0x8000000a 0xe72a E2
```

Table 7-74 Description of the **display ospfv3 lsdb** command output

Item	Description
Link-LSA	Description of the Link-LSA
Router-LSA	Description of the Router-LSA
Network-LSA	Description of the Network-LSA
Inter-Area-Prefix-LSA	Description of the Inter-Area-Prefix-LSA
NSSA-external-LSA	Description of the NSSA-external-LSA
Intra-Area-Prefix-LSA	Description of the Intra-Area-Prefix-LSA
AS-External-LSA	Description of the AS-external-LSA
Link State ID	Link state ID in LSA header
Origin Router	switch that generates LSA
Age	Aging time of LSA
Seq#	Sequence number of LSA (from LSA header)
CkSum	Checksum of LSA
Link	Number of links in router LSA
Prefix	Number of prefixes in Link LSA
Reference	The Reference for Intra Area Prefix LSA, including Router-LSA and Network-LSA
Type	The type of the external routes: ● E1: Type 1 external route ● E2: Type 2 external route

Display the Link-local LSA in the LSDB.

```
<HUAWEI> display ospfv3 lsdb link
          OSPFv3 Router with ID (10.2.2.2) (Process 1)

             Link-LSA (Interface Vlanif10)
 LS age: 11
 LS Type: Link-LSA
 Link State ID: 0.0.2.6
 Originating Router: 10.2.2.2
 LS Seq Number: 0x80000002
 Retransmit Count: 0
 Checksum: 0xEFFA
 Length: 56
 Priority: 1
 Options: 0x000013 (-|R|-|-|E|V6)
 Link-Local Address: FE80::1441:0:E213:1
```

```
Number of Prefixes: 1

  Prefix: 2000:1::/64
   Prefix Options: 0 (-|-|-|-|-)
```

Table 7-75 Description of the **display ospfv3 lsdb link** command output

Item	Description
LS age	Aging time of LSA
LS Type	Type of LSA: - Router-LSA - Network-LSA - Inter-Area-Prefix-LSA - Inter-Area-Router-LSA - AS-external-LSA - Link-LSA - Intra-Area-Prefix-LSA - NSSA-LSA
Link State ID	Link state ID in LSA header
Originating Router	Router that generates LSA
LS Seq Number	Sequence number of LSA (from LSA header)
Retransmit Count	Total number of nodes in the retransmission list
Checksum	Checksum of LSA
Length	Length of the LSA
Priority	Priority of the interface that corresponds to the link
Options	Value of options of the link
Link-Local Address	Link local address
Number of Prefixes	Number of IPv6 prefixes in the LSA
Prefix	IPv6 prefix
Prefix Options	Value of options of the prefix

7.5.24 display ospfv3 next-hop

Function

The **display ospfv3 next-hop** command displays the next-hop routing table of OSPFv3.

Format

display ospfv3 [*process-id*] **next-hop**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 next-hop** command to check the next-hop routing table of OSPFv3.

Example

Display the next-hop routing table of OSPFv3 process 1.

```
<HUAWEI> display ospfv3 1 next-hop
OSPFv3 Process (1)
Neighbor-Id     Next-Hop                          Interface   RefCount
10.3.3.9        FE80::2E0:FCFF:FE01:814F             Vlanif10    1
```

Table 7-76 Description of the **display ospfv3 next-hop** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Neighbor-Id	Neighbor ID
Next-Hop	Next hop address
Interface	Egress
RefCount	Number of routes using the next hop

7.5.25 display ospfv3 path

Function

The **display ospfv3 path** command displays the paths to a destination address.

Format

display ospfv3 [*process-id*] **path**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the process ID is not specified, paths in all processes are displayed.

Example

Display all OSPFv3 paths.

```
<HUAWEI> display ospfv3 path
OSPFv3 Process (1)
Type        AreaId/LSACost   PathCost
Intra       0.0.0.1          2
Inter       0.0.0.1          2
External    0.0.0.10              1
```

Table 7-77 Description of the **display ospfv3 path** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Type	Path type: ● Intra: indicates the intra-area routes. ● Inter: indicates the inter-area routes. ● External: indicates the AS-external routes.
AreaId/LSACost	● Area ID in case of an intra-area or inter-area path. ● LSA cost in case the path type is External. ● Cost in case of a path to a destination outside an AS
PathCost	Cost of the path

7.5.26 display ospfv3 peer

Function

The **display ospfv3 peer** command displays the qualified OSPFv3 neighbor.

Format

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [*interface-type interface-number* | *neighbor-id*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the neighbor of the specific area.	*area-id* can be a decimal integer or in IPv4 address format. The integer ranges from 0 to 4294967295.
interface-type interface-number	Indicates the type and the number of the interface.	-
neighbor-id	Specifies router ID of the neighbor.	The value is in dotted decimal notation.
verbose	Displays detailed information of the neighbor of each area.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 peer** command to check qualified OSPFv3 neighbor information.

Example

Display neighbor information about OSPFv3 process 1 on Vlanif10.

```
<HUAWEI> display ospfv3 1 peer vlanif 10
```

```
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri  State           Dead Time Interface           Instance ID
10.1.1.1          1  Full/DR         00:00:30  Vlanif10                  0
```

Display the detailed neighbor information of OSPFv3 process 100 on Vlanif10.

```
<HUAWEI> display ospfv3 100 peer vlanif 10 verbose
OSPFv3 Process (100)
 Neighbor 10.1.1.1 is Full, interface address FE80::3D43:0:8C14:1
    In the area 0.0.0.1 via interface Vlanif10
    DR Priority is 1 DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)
    Dead timer due in 00:00:29
    Neighbour is up for 18:40:40
    Database Summary Packets List 0
    Link State Request List 0
    Link State Retransmission List 0
    Neighbour Event: 6
    Neighbour If Id: 0x1017
```

Table 7-78 Description of the **display ospfv3 peer** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process.
OSPFv3 Area	ID of the OSPFv3 area.
Neighbor ID	Neighbor ID.
Pri	Priority of the neighbor switch.
State	State of the neighbor / DR or BDR. State of the neighbor: includes Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, and Full. DR or BDR: includes DR and Backup.
Dead Time	Dead time of the neighbor.
Interface	Interface that connects with the neighbor.
Instance ID	ID of the instance that the neighbor belongs to.
Neighbor	Neighbor ID.
interface address	Link address of the neighbor interface.
In the area 0.0.0.1 via interface Vlanif10	Vlanif10 of the neighbor is in Area 1.
DR Priority	Priority of DR.
DR	Designated router.
BDR	Backup designated router.
Options	Options of the neighbor.
Dead timer due in 00:00:29	The time before the neighbor dies.

Item	Description
Neighbour is up for 18:40:40	The up time of the neighbour.
Database Summary Packets List	Number of packets in the database summary list of the neighbor.
Link State Request List	Number of LSAs in the request list of the neighbor.
Link State Retransmission List	Number of LSAs in the retransmission list of the neighbor.
Neighbour Event	Number of times NFSM (Neighbor Finite State Machine) state changed.
Neighbour If Id	Interface ID of the neighbor.

7.5.27 display ospfv3 request-list

Function

The **display ospfv3 request-list** command displays the statistics of the request list of OSPFv3.

Format

display ospfv3 [*process-id*] **request-list** [[**area** *area-id* | **interface** *interface-type interface-number* | **peer** *router-id*]* | **statistics**]

Parameters

Parameter	Description	Value
process-id	Specifies the process ID of OSPFv3.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID.	The integer ranges from 0 to 4294967295. The value of the area ID can be a decimal integer or in the IPv4 address format.
interface *interface-type interface-number*	Specifies the type and number of the interface.	-
peer *router-id*	Indicates the Router ID of a neighbor.	It is in dotted decimal notation.

Parameter	Description	Value
statistics	Displays the statistics of the request list of OSPFv3.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The display of the command is used to diagnose faults.

Example

Display the statistics of the request list in OSPFv3.

```
<HUAWEI> display ospfv3 request-list
   OSPFv3 Process (1)
   Interface  FC00:0:0:1::2        Area-ID   0.0.0.1
   Nbr-ID   10.254.255.255
   LS-Type               LS-ID           AdvRouter       SeqNum       Age
   Link-LSA              0.0.2.2         10.254.255.255  0x80000001   151
   Router-LSA            0.0.0.0         10.254.255.255  0x80000005   46
   Intra-Area-Prefix-LSA 0.0.0.1         10.254.255.255  0x80000001   45
   AS-External-LSA       0.0.0.1         10.254.255.255  0x80000001   113
   AS-External-LSA       0.0.0.2         10.254.255.255  0x80000001   113
```

Table 7-79 Description of the **display ospfv3 request-list** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Interface	Interface that connects with the neighbor
Area-ID	ID of the area that the interface belongs to
Nbr-ID	Router ID of the neighbor

Item	Description
LS-Type	LSA type: ● Link-LSA: is generated by the switch for each link and is advertised in the local link. ● Router-LSA: is generated by each switch and advertised in the area whether the switch resides. It describes the link state and cost of the switch. ● Intra-Area-Prefix-LSA: – An LSA generated on a router describes the IPv6 address prefix associated with the Router LSA. – An LSA generated on a DR describes the IPv6 address prefix associated with the network LSA. ● AS-External-LSA: is generated by the ASBR and is advertised to the entire AS (except the stub area). It describes the routes that reach other ASs.
LS-ID	Link State ID (from LSA header)
AdvRouter	Advertising router (from LSA header)
SeqNum	Sequence number (from LSA header)
Age	Aging time (from LSA header)

7.5.28 display ospfv3 retrans-list

Function

The **display ospfv3 retrans-list** command displays the statistics of the retransmission list in OSPFv3.

Format

display ospfv3 [*process-id*] **retrans-list** [[**area** *area-id* | **interface** *interface-type interface-number* | **peer** *router-id*]* | **statistics**]

Parameters

Parameter	Description	Value
process-id	Specifies the process ID of OSPFv3.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
area *area-id*	Specifies the OSPFv3 area ID.	The integer ranges from 0 to 4294967295. The value of the area ID can be a decimal integer or in the IPv4 address format.
interface *interface-type interface-number*	Specifies the type and number of the interface.	-
peer *router-id*	Indicates the Router ID of a neighbor.	It is in dotted decimal notation.
statistics	Displays the statistics of the retransmission list in OSPFv3.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The display of the command is used to diagnose faults.

Example

Display the statistics of the retransmission list in OSPFv3.

```
<HUAWEI> display ospfv3 retrans-list

    OSPFv3 Process (1)
    Interface  FC00:0:0:1::2        Area-ID   0.0.0.1
    Nbr-ID   10.22.2.255
    LS-Type                LS-ID           AdvRouter       SeqNum       Age
    Network-LSA            0.0.2.2         10.254.255.255  0x80000002   1
    Intra-Area-Prefix-LSA 0.0.0.2          10.254.255.255  0x80000002   1
```

Table 7-80 Description of the **display ospfv3 retrans-list** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Interface	Interface that connects with the neighbor
Area-ID	ID of the area that the interface belongs to

Item	Description
Nbr-ID	Router ID of the neighbor
LS-Type	LSA type: ● Network-LSA: is generated by the DR of a broadcast network or an NBMA network and is advertised in the area where the DR resides. It describes the link state of the network segment. ● Intra-Area-Prefix-LSA: – An LSA generated on a router describes the IPv6 address prefix associated with the Router LSA. – An LSA generated on a DR describes the IPv6 address prefix associated with the network LSA.
LS-ID	Link State ID (from the LSA header)
AdvRouter	Advertising router (from LSA header)
SeqNum	Sequence number (from LSA header)
Age	Aging time (from LSA header)

7.5.29 display ospfv3 routing

Function

The **display ospfv3 routing** command displays the OSPFv3 routing table.

Format

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length* | **abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes** | [**statistics**] [**uninstalled**]]

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
ipv6-address	Indicates the IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
prefix-length	Specifies the length of the prefix.	The value is an integer ranging from 0 to 128.
abr-routes	Displays the routing table of ABR in OSPFv3.	-
asbr-routes	Displays routing table of ASBR in OSPFv3.	-
intra-routes	Displays the statistics of OSPFv3 routes in an area.	-
inter-routes	Displays the statistics of OSPFv3 routes between areas.	-
ase-routes	Displays the statistics of OSPFv3 routes outside an AS.	-
nssa-routes	Displays the statistics of OSPFv3 routes in an NSSA.	-
statistics	Displays the statistics of all routing tables.	-
uninstalled	Displays the routes are not installed into the RM.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By using this command with different parameters, you can view the routes of a specified interface or next hop.

The command output can help you troubleshoot OSPFv3 faults.

Example

Display the OSPFv3 routing table.

```
<HUAWEI> display ospfv3 routing
Codes : E2 - Type 2 External, E1 - Type 1 External, IA - Inter-Area,
        N - NSSA, U - Uninstalled, D - Denied by Import Policy
```

```
OSPFv3 Process (1)
   Destination                                              Metric
     Next-hop
     FC00:0:0:3::1/128                                        0
      directly connected, LoopBack1
  IA FC00:0:0:4::1/128                                        1
       via FE80::200:FF:FE00:DC00, Vlanif1002
  IA FC00:0:0:5::1/128                                        1
       via FE80::200:FF:FE00:DC00, Vlanif1002
     FC00:0:0:6::/64                                            1
      directly connected, Vlanif1002
```

Table 7-81 Description of the **display ospfv3 routing** command output

Item	Description
Codes	The following information provides the full spelling and explanation: ● E2: Type 2 external route ● E1: Type 1 external route ● IA: Inter-area route ● N: NSSA route ● U: OSPFv3 routes that are not advertised to the IPv6 routing table ● D: OSPFv3 routes denied by import route policy
OSPFv3 Process	OSPFv3 process
Destination	Destination address
Metric	Metric to the destination
Next-hop	Next hop to the destination

Displays the routes are not installed into the RM.

```
<HUAWEI> display ospfv3 routing uninstalled
Codes : E2 - Type 2 External, E1 - Type 1 External, IA - Inter-Area,N - NSSA, U - Uninstalled

OSPFv3 Process (1)
   Destination                                                Metric
     Next-hop
  N    via FE80:1000:2000:3000:4000:5000:6000:7000, Vlanif10
  U E2 FC00:0:0:1::1/128                                        5
```

Table 7-82 Description of the **display ospfv3 routing uninstalled** command output

Item	Description
N	NSSA

Display statistics about the OSPFv3 routes that are not installed into the RM.

```
<HUAWEI> display ospfv3 routing statistics uninstalled
OSPFv3 Process (1) UNINSTALLED ROUTES STATISTICS
     Intra-area-routes   :   2
     Inter-area-routes   :   0
     External-routes     :   1
```

Table 7-83 Description of the **display ospfv3 routing statistics uninstalled** command output

Item	Description
Intra-area-routes	Number of intra-area routes
Inter-area-routes	Number of inter-area routes
External-routes	Number of external routes

7.5.30 display ospfv3 sham-link

Function

The **display ospfv3 sham-link** command displays information about sham links in an OSPFv3 area.

Format

display ospfv3 [*process-id*] **sham-link** [**area** *area-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID.	The integer ranges from 0 to 4294967295. The value of the area ID can be a decimal integer or in the IPv4 address format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the process ID and area ID are not specified, information about all the configured sham links is displayed.

Example

Display all sham link information of OSPFv3.

```
<HUAWEI> display ospfv3 sham-link
 OSPFv3 Process (10)
 Sham Link SHAM-LINK1 to router 0.0.0.0 is down
 Area 0.0.0.1, via Interface *, Instance ID 0, cost 1
 Source address 2001:db8:1::1
 Destination address 2001:db8:2::1
 Interface ID 0x80000001
 Sham-Link Interface Events: 24
 Sham-Link Interface LsaCount: 0
 Sham-Link Interface Lsa Checksum: 0x0
 Transmit Delay is 1 sec, State Down
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:00
 Adjacency state Down
 IP security association configured: sa1
 IP security association applied: sa1
```

Table 7-84 Description of the **display ospfv3 sham-link** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Area	ID of the OSPFv3 area to which the sham link belongs
via Interface	Interface of the sham link
Instance ID	ID of the instance
cost	Cost of the sham link
Source address	Source IPv6 address of the sham link
Destination address	Destination IPv6 address of the sham link
Interface ID	Interface ID
Sham-Link Interface Events	Number of interface events of the sham-link
Sham-Link Interface LsaCount	Number of LSAs sent from all sham-link interfaces
Sham-Link Interface Lsa Checksum	Checksum of the LSA sent from the sham-link interface
Transmit Delay	Delay for an interface to send Update packets
State	Interface status of the sham link ● Down ● Point-To-Point

Item	Description
Timer intervals configured	Values of the following timers: ● Hello ● Dead ● Retransmit ● Wait
Adjacency state	Adjacency of the sham link ● Down ● Init ● Exch ● Start ● Exchange ● Loading ● Full
IP security association configured	IP security association configured on a sham link
IP security association applied	IP security association applied on a sham link

7.5.31 display ospfv3 topology

Function

The **display ospfv3 topology** command displays the OSPFv3 area topology.

Format

display ospfv3 [*process-id*] **topology** [**area** *area-id*]

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the area ID.	The value of the area ID can be a decimal integer or in the IPv4 address format. The integer ranges from 0 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 topology** command to check the OSPFv3 area topology.

Example

Display the topology of OSPFv3 area 1.

```
<HUAWEI> display ospfv3 topology area 1
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)       Bits      Metric    Next-Hop        Interface
Rtr   1.1.1.1                   --
Rtr   10.2.2.2                   1         10.2.2.2        Vlanif10
Net   10.2.2.2(268435842)          1         0.0.0.0         Vlanif10
```

Table 7-85 Description of the **display ospfv3 topology** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
OSPFv3 Area	ID of the OSPFv3 area
Type	SPF type: ● Rtr: Router ● Net: Network
ID (If-Index)	Router ID (If-Index) is the interface ID of the DR in the network type.
Bits	B bit and E bit indicate the switch type: ● B bit: ABR ● E bit: ASBR
Metric	Metric of path to the node
Next-Hop	Next hop of the path to the node
Interface	Egress of the path to the node

7.5.32 display ospfv3 vlink

Function

The **display ospfv3 vlink** command displays the OSPFv3 virtual links.

Format

display ospfv3 [*process-id*] **vlink**

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospfv3 vlink** command to check the OSPFv3 virtual links.

Example

Display OSPFv3 virtual links.

```
<HUAWEI> display ospfv3 vlink
OSPFv3 Process (100)

Virtual Link VLINK1 to router 10.2.2.2 is up
 Transit area 0.0.0.1 via interface Vlanif10, instance ID 0
 Local address FC00:0:0:2000::1
 Remote address FC00:0:0:1001::2
 Interface ID 0x80000001
 VirtualInterface Event: 1
 VirtualInterface LsaCount: 0
 VirtualInterface Lsa Checksum: 0x0
 Transmit Delay is 1 sec, State Point-To-Point, Cost 1562
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:04
   Adjacency state Init
```

Table 7-86 Description of the **display ospfv3 vlink** command output

Item	Description
Transit area	If the current interface is the V-link interface, the transfer area ID is displayed
via interface	Interface of the V-link
instance ID	Instance ID
Local address	Local address
Remote address	Remote address
Interface ID	Interface ID

Item	Description
VirtualInterface Event	Number of interface events of the V-link
VirtualInterface LsaCount	Number of LSAs sent from all V-link interfaces
VirtualInterface Lsa Checksum	Checksum of the LSA sent from the V-link interface
Transmit Delay	Transmission delay of the interface
State	Interface state: - Down - Point-To-Point
Cost	Cost
Timer intervals configured	Timers: - Hello: Hello interval - Dead: Interval of Dead timer - Wait: Interval of Wait timer. It is pointless to use a virtual link. - Retransmit: Retransmission interval
Adjacency state	State of the V-link: - Down - Init - Exch - Start - Exchange - Loading - Full

7.5.33 domain-id (OSPFv3)

Function

The **domain-id** command sets an OSPFv3 domain ID.

The **undo domain-id** command restores the default setting.

By default, the domain ID is null.

Format

domain-id { **null** | *domain-id* [**type** *type* **value** *value* | **secondary**] * }

undo domain-id { *domain-id* [**type** *type* **value** *value*] }

Parameters

Parameter	Description	Value
null	Specifies that the OSPFv3 domain ID is null.	-
domain-id	Specifies an OSPFv3 domain ID.	The value can be an integer or expressed in dotted decimal notation. If the domain ID is an integer, its value ranges from 0 to 4294967295; it is converted to the dotted decimal notation and carried 1 with 256 when being displayed. If the domain ID is in dotted decimal notation format, it is displayed as originally entered.
type *type*	Specifies the type of the OSPFv3 domain ID.	The value is an integer that can be 0005, 0105, 0205, or 8005. The default value is 0005.
value *value*	Specifies the value of the OSPFv3 domain ID type.	The value is a hexadecimal number that ranges from 0 to FFFF. The default value is 0.
secondary	Specifies the ID of a secondary domain.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Generally, the routes that are imported from a PE are advertised as External-LSAs. However, such routes that belong to different nodes of the same OSPFv3 domain should be advertised as Type 3 LSAs (intra-domain routes). This requires that different nodes in the same OSPFv3 domain have the same domain ID.

Values 0 and null indicate different meanings.

The maximum number of secondary domain IDs in each OSPFv3 process is 10. The maximum number of secondary domain IDs may vary with products.

The parameter **secondary** can be configured only when the primary domain ID is configured. When the **undo domain-id** command is run, if no parameter is specified, the primary domain ID is deleted.

Example

Set the VPN domain ID in OSPFv3 VPN extension.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance test
[HUAWEI-vpn-instance-test] ipv6-family
[HUAWEI-vpn-instance-test-af-ipv6] route-distinguisher 100:1
[HUAWEI-vpn-instance-test-af-ipv6] quit
[HUAWEI-vpn-instance-test] quit
[HUAWEI] ospfv3 1 vpn-instance test
[HUAWEI-ospfv3-1] domain-id 234
```

7.5.34 filter export (OSPFv3)

Function

The **filter export** command filters the outgoing Type3 LSAs of the local area.

The **undo filter export** command restores the default setting.

By default, the outgoing Type3 LSAs of the local area are not filtered.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

filter { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export**

undo filter [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of neighbors' LSDBs and speed up network convergence.

Configuration Impact

After filtering conditions are set for the outgoing Type3 LSAs to be advertised using the **filter export** command, only the outgoing Type3 LSAs that pass the filtering can be advertised.

Precautions

- The command can be configured only on ABRs.
- When the **rule** command is used to configure a filtering rule for an ACL, only the source address range specified by the parameter **source** and the time range specified by the parameter **time-range** in the **rule** command take effect.
- To set filtering conditions for the incoming Type3 LSAs to be advertised, run the **filter import (OSPFv3)** command.
- Creating an ACL6, IPv6 prefix list, or route-policy before it is referenced is recommended. If a nonexistent ACL6, IPv6 prefix list, or route-policy is referenced using the command, OSPFv3 advertises all Type 3 LSAs.

Example

Configure OSPFv3 to filter the outgoing Type3 LSAs.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 100
[HUAWEI-ospfv3-100] area 1
```

```
[HUAWEI-ospfv3-100-area-0.0.0.1] filter 2000 export
```

7.5.35 filter import (OSPFv3)

Function

The **filter import** command filters the incoming Type3 LSAs of the local area.

The **undo filter import** command restores the default setting.

By default, the incoming Type3 LSAs are not filtered.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

filter { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **filter import** command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the neighbors' LSDBs and speed up network convergence.

Configuration Impact

After filtering conditions are set for the incoming Type3 LSAs to be advertised using the **filter import** command, only the incoming Type3 LSAs that pass the filtering can be received and advertised.

Precautions

- The command can be configured only on ABRs.
- When the **rule** command is used to configure a filtering rule for an ACL, only the source address range specified by the parameter **source** and the time range specified by the parameter **time-range** in the **rule** command take effect.
- To set filtering conditions for the outgoing Type3 LSAs to be advertised, run the **filter export (OSPFv3)** command.
- Creating an ACL6, IPv6 prefix list, or route-policy before it is referenced is recommended. If a nonexistent ACL6, IPv6 prefix list, or route-policy is referenced using the command, OSPFv3 receives all Type 3 LSAs.

Example

Configure OSPFv3 to filter the incoming Type3 LSAs within the local area.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 100
[HUAWEI-ospfv3-100] area 1
[HUAWEI-ospfv3-100-area-0.0.0.1] filter ipv6-prefix my-prefix-list import
```

7.5.36 filter-policy export (OSPFv3)

Function

The **filter-policy export** command filters imported routes.

The **undo filter-policy export** command restores the default setting.

By default, imported routes are not filtered.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl6-number	Specifies the ACL6 number.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of the IPv6 address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the protocol from which the route is imported. You can use this parameter to filter the imported routes of specific protocols. If this parameter is not specified, all imported routes are filtered.	The value may be **bgp, direct**, **isis, ospfv3, ripng**, **static**, or **unr**. The specific value varies depending on the routing protocol supported by the device.
process-id	Specifies the process ID of the protocol.	The value is an integer ranging from 1 to 65535.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **filter-policy export** command is only valid for the routes that are imported using the **import-route** command.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all external routes imported to OSPFv3 are converted to Type 5 LSAs (AS-external-LSAs) or Type 7 LSAs (NSSA-external-LSAs) and then are advertised to neighbors.

Example

Filter the imported routes based on the rule defined by ACL6 2002.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] filter-policy 2002 export
```

7.5.37 filter-policy import (OSPFv3)

Function

The **filter-policy import** command filters received routes.

The **undo filter-policy import** command restores the default setting.

By default, received routes are not filtered.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the ACL6 number.	The value is an integer ranging from 2000 to 2999.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of the IPv6 address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **filter-policy import** command only filters the routes calculated by OSPFv3. Routes that do not pass the filtering are neither added to the OSPFv3 routing table nor advertised.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes received by OSPFv3 are delivered to the IPv6 routing table.

Example

Filter the received routes based on the IPv6 address prefix list named **abc**.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] filter-policy ipv6-prefix abc import
```

7.5.38 frr (OSPFv3)

Function

The **frr** command creates and then displays the OSPFv3 FRR view.

The **undo frr** command deletes the OSPFv3 FRR view.

By default, the OSPFv3 FRR view does not exist.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

frr

undo frr

Parameters

None

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPFv3 IP FRR allows devices to fast switch traffic from faulty links to back up links without interrupting traffic. This function protects traffic and greatly improves the reliability of OSPFv3 networks. OSPFv3 IP FRR must be configured in the OSPFv3 FRR view. The **frr** command run in the OSPFv3 view creates and displays the OSPFv3 FRR view.

Follow-up Procedure

The **frr** command run in the OSPFv3 view creates and displays the OSPFv3 FRR view only, but cannot enable the OSPFv3 IP FRR function. Run the **loop-free-alternate** command in the OSPFv3 view to enable OSPFv3 IP FRR to create the loop-free backup route.

Example

Create and display the OSPFv3 FRR view.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] frr
[HUAWEI-ospfv3-1-frr]
```

7.5.39 frr-policy route (OSPFv3)

Function

The **frr-policy route** command configures a filtering policy for the OSPFv3 IP FRR backup routes. The filtering policy determines what kind of OSPFv3 backup route can be added to the routing table.

The **undo frr-policy route** command cancels the filtering function.

By default, the filtering function is disabled.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

frr-policy route route-policy *route-policy-name*

undo frr-policy route

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the policy used to filter OSPFv3 backup routes.	The value must be an existing route-policy.

Views

OSPFv3 FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPFv3 IP FRR allows devices to fast switch traffic on fault links to back up links without interrupting traffic. This protects traffic and greatly improves the reliability of OSPFv3 networks.

After the filtering policy is configured using the **frr-policy route** command, only the OSPFv3 backup route that satisfies filtering rules can be delivered to the forwarding table.

Configuration Impact

To protect the traffic over a specific OSPFv3 route, you can configure a filtering policy *route-policy-name* that the OSPFv3 route matches to ensure that the backup route can be added to the forwarding table. When this route fails, OSPFv3 can fast switch the traffic to a backup route.

Precautions

The **frr-policy route** command is cyclic in nature, and only the latest configuration takes effect.

If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, OSPFv3 adds all backup routes to the IPv6 routing table.

Example

Configure OSPFv3 to add the OSPFv3 backup routes that match the named ACL **abc** to the IPv6 routing table.

```
<HUAWEI> system-view
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] frr
[HUAWEI-ospfv3-1-frr] loop-free-alternate
[HUAWEI-ospfv3-1-frr] frr-policy route route-policy abc
```

7.5.40 graceful-restart (OSPFv3)

Function

The **graceful-restart** command enables GR of the OSPFv3 process.

The **undo graceful-restart** command disables GR of the OSPFv3 process.

By default, OSPFv3 GR is not enabled.

Format

graceful-restart [**period** *period* | **ack-time** *time* | **retransmit-interval** *interval* | **lsa-checking-ignore** | **planned-only**] *

undo graceful-restart [**period** [*period*] | **ack-time** [*time*] | **retransmit-interval** [*interval*] | **lsa-checking-ignore** | **planned-only**] *

Parameters

Parameter	Description	Value
period *period*	Specifies the GR period.	The value is an integer ranging from 1 to 1800, expressed in seconds. By default, the value is 120 seconds.
ack-time *time*	Specifies the period during which a switch waits for the Grace-LSA Ack message from its neighbor.	The value is an integer ranging from 1 to 30, expressed in seconds. By default, the value is 15 seconds.
retransmit-interval *interval*	Specifies the interval for retransmitting Grace-LSAs.	The value is an integer ranging from 1 to 5, expressed in seconds. By default, the value is 5 seconds.
lsa-checking-ignore	Indicates that strict check is not performed on LSAs. By default, switches perform strict check on received LSAs.	-
planned-only	Indicates that switches support Planned-GR only. By default, switches support Planned-GR and Unplanned-GR.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

ack-time is an optional parameter. After the parameter is specified, the restarter can discover more neighbors in *ack-time* period.

Example

Enable GR of the OSPFv3 process.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] graceful-restart
```

7.5.41 helper-role (OSPFv3)

Function

The **helper-role** command configures a switch to support the GR Helper mode.

The **undo helper-role** command cancels GR Helper mode.

By default, the switch is not enabled to support GR Helper mode.

Format

helper-role [{ **ip-prefix** *ip-prefix-name* | **acl-number** *acl-number* | **acl-name** *acl-name* } | **max-grace-period** *period* | **planned-only** | **lsa-checking-ignore**]*

undo helper-role [[**ip-prefix** [*ip-prefix-name*] | **acl-number** [*acl-number*] | **acl-name** [*acl-name*]] | **max-grace-period** *period* | **planned-only** | **lsa-checking-ignore**]*

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl-number *acl-number*	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a IPv6 Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
max-grace-period *period*	Specifies the permitted maximum restart period.	The value is an integer ranging from 1 to 1800, expressed in seconds. By default, the value is 1800 seconds.
planned-only	Indicates that switches support Planned-GR only. By default, switches support Planned-GR and Unplanned-GR.	-

Parameter	Description	Value
lsa-checking-ignore	Indicates that strict check is not performed on LSAs. By default, switches perform strict check on received LSAs.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Switches cannot use the helper mode during the GR process.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Configure a switch to support the helper mode.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] helper-role acl-number 2001 max-grace-period 250 planned-only lsa-checking-
ignore
```

7.5.42 import-route (OSPFv3)

Function

The **import-route** command imports an external route. Before the routes are imported, the OSPFv3 process of the route must be active.

The **undo import-route** command stops importing external routes.

By default, no route of other protocols is imported.

Format

import-route { **bgp** [**permit-ibgp**] | **unr** | **direct** | **ripng** *help-process-id* | **static** | **isis** *help-process-id* | **ospfv3** *help-process-id* } [{ **cost** *cost* | **inherit-cost** } | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*]*

undo import-route { **bgp** | **unr** | **direct** | **ripng** *help-process-id* | **static** | **isis** *help-process-id* | **ospfv3** *help-process-id* }

Parameters

Parameter	Description	Value
bgp	Specifies the protocol from which routes are imported, as **bgp**.	-
permit-ibgp	IBGP routes that are permitted to be imported. The import of IBGP routes may cause route loops. Therefore, this command must not be configured unless it is necessary.	-
unr	Specifies the imported source routing protocol as **unr**. User Network Route (UNR) is allocated if dynamic routing protocols cannot be used when users are getting online.	-
direct	Specifies the imported source routing protocol as **direct**.	-
ripng	Specifies the protocol from which routes are imported, as **ripng**.	-
static	Specifies the imported source routing protocol as **static**.	-
isis	Specifies the protocol from which routes are imported, as **isis**.	-
ospfv3	Specifies the protocol from which routes are imported, as **ospfv3**.	-
help-process-id	Specifies the process ID of the imported source protocol.	The value is an integer ranging from 1 to 65535.
cost *cost*	Indicates the cost of the imported route.	The value is an integer ranging from 1 to 16777214. For details about the default value, see **default (OSPFv3)**.
inherit-cost	Indicates the original cost of the imported routes.	-

Parameter	Description	Value
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. For details about the default value, see **default (OSPFv3)**. - 1: Type 1 external route - 2: Type 2 external route
tag *tag*	Specifies the tag value of the imported routes.	The value is an integer that ranges from 0 to 4294967295. For details about the default value, see **default (OSPFv3)**.
route-policy *route-policy-name*	Specifies the name of the routing policy. Only the routes that match the *route-policy-name* are imported.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a non-PE device, only EBGP routes are imported after the **import-route bgp** command is configured. IBGP routes are also imported after the **import-route bgp permit-ibgp** command is configured. If IBGP routes are imported, routing loops may occur. In this case, run the **preference (OSPFv3)** and **preference (BGP)** commands to prevent loops by specifying preferences of OSPFv3 and BGP routes. If IBGP routes need to be imported, configure the **import-route bgp permit-ibgp** command, and run the **preference (OSPFv3)** and **preference (BGP)** commands to set the preference of OSPFv3 ASE routes lower than that of IBGP routes (preference value of OSPFv3 ASE routes larger than that of IBGP routes).

On a PE, configuring the **import-route bgp** command imports both EBGP routes and IBGP routes, no matter whether the **import-route bgp permit-ibgp** command is configured or not. If the **import-route bgp permit-ibgp** command and the **default-route-advertise (OSPFv3)** command are both configured, the active IBGP default routes can be imported into OSPFv3.

NOTE

After the **import-route direct** command is executed, routes to the network segment where the IPv6 address of the management interface belongs are also imported in the OSPFv3 routing table. Therefore, use this command with caution.

Precautions

Creating a route-policy before it is referenced is recommended. If a nonexistent route-policy is referenced using the command, all the routes learned by the specified protocol are imported to the OSPFv3 routing table.

Example

Import the RIPng route of type 2. The cost of the route is 50.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] import-route ripng 1 type 2 cost 50
```

OSPFv3 process 100 imports the routes discovered by OSPFv3 process 160.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 100
[HUAWEI-ospfv3-100] import-route ospfv3 160
```

7.5.43 ipsec sa (OSPFv3)

Function

The **ipsec sa** command configures a Security Association (SA) in the OSPFv3 area or OSPFv3 process.

The **undo ipsec sa** command deletes the SA configured in the OSPFv3 area or OSPFv3 process.

By default, no SA is configured in the OSPFv3 area or OSPFv3 process.

Format

ipsec sa *sa-name*

undo ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	The value is an existing SA name.

Views

OSPFv3 view or OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SA defines a set of security algorithms and keys to ensure IP security. Incoming and outgoing OSPFv3 packets are authenticated and encrypted based on the rules defined by the SA.

The **ipsec sa** *sa-name* command run in the OSPFv3 process view is used to authenticate packets of the OSPFv3 process. An SA applied in an OSPFv3 process is used to authenticate the packets of the process. After an OSPFv3 process is associated with an OSPFv3 area, the SA applied in the OSPFv3 process is also applied to the OSPFv3 area.

The **ipsec sa** *sa-name* command run in the OSPFv3 area view is used to authenticate packets of the OSPFv3 area.

NOTE

- The SA applied in an OSPFv3 area takes precedence over that applied in an OSPFv3 process.
- If the SA applied in the OSPFv3 area is deleted, the SA applied in the OSPFv3 process is used to authenticate packets.

Example

Configure an SA named **sa1** in the OSPFv3 process. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] ipsec sa sa1
```

Configure an SA named **sa2** in the OSPFv3 area. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 10.0.0.0
[HUAWEI-ospfv3-1-area-10.0.0.0] ipsec sa sa2
```

7.5.44 loop-free-alternate (OSPFv3)

Function

The **loop-free-alternate** command enables OSPFv3 IP FRR to enable the device to use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link.

The **undo loop-free-alternate** command disables OSPFv3 IP FRR.

By default, this function is disabled.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

loop-free-alternate

undo loop-free-alternate

Parameters

None

Views

OSPFv3 FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **frr** command run in the OSPFv3 view creates and displays the OSPFv3 FRR view only, but cannot enable the OSPFv3 IP FRR function. You must run the **loop-free-alternate** command in the OSPFv3 view to enable OSPFv3 IP FRR use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link to create the loop-free backup route.

Follow-up Procedure

Run the **frr-policy route** command in the OSPFv3 view to configure a filtering policy for OSPFv3 IP FRR. Only the OSPFv3 backup route that satisfies specific rules can be delivered to the forwarding table.

Example

Enable OSPFv3 IP FRR to create the loop-free backup route.

```
<HUAWEI> system-view
[HUAWEI] ospfv3
```

```
[HUAWEI-ospfv3-1] frr
[HUAWEI-ospfv3-1-frr] loop-free-alternate
```

7.5.45 lsa-forwarding-address

Function

The **lsa-forwarding-address** command enables the OSPFv3 forwarding address (FA) function.

The **undo lsa-forwarding-address** command disables the OSPFv3 FA function.

By default, the OSPFv3 FA function is disabled.

Format

lsa-forwarding-address { **standard** | **zero-translate** }

undo lsa-forwarding-address

Parameters

Parameter	Description	Value
standard	Indicates that the function is compatible with RFC 3101.	-
zero-translate	Allows the Type 7 LSAs with the P-bit set and the FA being 0 to be translated to Type 5 LSAs.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For an OSPFv3 Type 5 or Type 7 LSA:

- When there is no FA, other switches consider how to reach the ASBR (the switch that generates this LSA) and then reach an external network through this ASBR.
- When there is an FA, other switches consider how to reach the device to which this FA belongs and then reach an external network through this device.

In this situation, if no FA is available, an additional next hop may be generated when a switch within an OSPF domain first reaches an ASBR before reaching an external network.

Therefore, the FA in an OSPFv3 Type 5 or Type 7 LSA provides a faster next hop to reach an external network.

Precautions

If the FA in an OSPFv3 Type 5 or Type 7 LSA is not 0, the corresponding route is calculated only when the **lsa-forwarding-address** command is configured.

Example

Enable the OSPFv3 FA function that is compatible with RFC 3101.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] lsa-forwarding-address standard
```

7.5.46 maximum load-balancing (OSPFv3)

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for carrying out load balancing.

The **undo maximum load-balancing** command restores the default setting.

The default maximum number of equal-cost OSPFv3 routes for carrying out load balancing is 8.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

maximum load-balancing *number*

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes.	The value is an integer ranging from 1 to 8.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

If a routing protocol discovers multiple routes with the same cost to a single destination, they can carry out load balancing. The **maximum load-balancing** command sets the maximum number of equal-cost routes that can carry out load balancing. This optimizes the routing policy and ensures traffic forwarding on a complex network.

Effect

Packets will be load-balanced by multiple equal-cost routes to a single destination.

NOTE

Load balancing is performed in either per-flow or per-packet mode. By default, packets are load-balanced in per-flow mode.

Follow-up Procedure

If more existing equal-cost OSPFv3 routes than the value set using the **maximum load-balancing** command are available, valid routes are selected for load balancing based on the following criteria:

- Route preference: Routes with lower preferences are selected for load balancing.
- Interface index: If routes have the same priorities, routes with higher interface index values are selected for load balancing.
- Next hop IP address: If routes have the same priorities and interface index values, routes with larger IP address are selected for load balancing.

The **nexthop** command allows routes with a specified weight to carry out load balancing.

Precautions

To disable load balancing, set the value of *number* to 1.

Example

Set the maximum number of equal-cost routes that OSPFv3 can support to 3.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] maximum load-balancing 3
```

Restore the default maximum number of equal-cost routes for carrying out load balancing.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] undo maximum load-balancing
```

7.5.47 nexthop (OSPFv3)

Function

The **nexthop** command sets the preference for equal-cost routes.

The **undo nexthop** command cancels the preference of equal-cost routes.

By default, the preference is not set for equal-cost routes. That is, equal-cost routes forward packets at the same time for load balancing.

Format

nexthop *router-id interface-type interface-number* **weight** *value*

undo nexthop *router-id interface-type interface-number*

Parameters

Parameter	Description	Value
router-id	Specifies the router ID of a neighbor.	It is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of an interface.	-
weight *value*	Specifies the weight of the next hop. The smaller the weight is, the higher the route preference is.	It is an integer ranging from 1 to 254.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

After OSPFv3 calculates equal-cost routes, you can run the **nexthop** command to select the route with the highest preference from the equal-cost routes as the next hop. OSPFv3 selects a next hop from these equal-cost routes according to the weight. The smaller the weight is, the higher the route preference is.

Example

Set the preference for equal-cost routes in OSPFv3.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] quit
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] nexthop 10.2.2.2 vlanif 10 weight 240
```

7.5.48 nssa (OSPFv3 Area)

Function

The **nssa** command configures an OSPFv3 area as an NSSA.

The **undo nssa** command cancels the configuration.

By default, no OSPFv3 area is configured as an NSSA.

Format

nssa [**default-route-advertise** [**cost** *cost* | **type** *type* | **tag** *tag*] * | **no-import-route** | **no-summary** | **translator-always** | **translator-interval** *translator-interval* | **set-n-bit** | **suppress-forwarding-address**] *

undo nssa

Parameters

Parameter	Description	Value
default-route-advertise	Generates default Type7 LSAs on the ASBR and then advertises them to the NSSA. **NOTE** The ABR generates a default NSSA LSA (Type7 LSA) automatically and advertises it in the NSSA.	-
cost *cost*	Specifies the default cost of Type 7 LSAs.	It is an integer ranging from 1 to 16777214. The default value is 1.

Parameter	Description	Value
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. - 1: Type 1 external route - 2: Type 2 external route
tag *tag*	Specifies the tag value of the OSPFv3 route imported to an NSSA.	It is an integer ranging from 0 to 4294967295. The default value is 0.
no-import-route	Indicates that no external routes are imported to NSSAs.	-
no-summary	Disables ABRs from sending summary LSAs to NSSAs.	-
translator-always	Specifies the ABR in an NSSA as the translator. Multiple ABRs in an NSSA can be configured as translators.	-
translator-interval *translator-interval*	Specifies the timeout period of a translator.	It is an integer ranging from 1 to 120, in seconds. The default value is 40 seconds.
set-n-bit	Indicates that the N-bit is set in DD packets.	-
suppress-forwarding-address	Enables the device to suppress the forwarding address of a Type 5 LSA translated from a Type 7 LSA.	-

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

If an area is configured to the nssa area, all switches of the area must be configured with the NSSA attribute.

The area will be updated after NSSA attributes are configured or deleted. Thus, the NSSA attributes can be re-configured or deleted only after the last update of NSSA attributes is complete.

The keyword **default-route-advertise** is used to generate default Type 7 LSAs. Regardless of whether there is route ::/0 in the routing table on an ABR, a Type 7 LSA default route is generated. A Type 7 LSA default route can be generated only when there is route ::/0 in the routing table on an ASBR.

When an ASBR is also an ABR, you can specify **no-import-route** to disable OSPFv3 from advertising the external routes imported through the **import-route** command to NSSAs. To reduce the number of LSAs to be transmitted to NSSAs, you can specify **no-summary** on an ABR to disable the ABR from transmitting summary LSAs (Type 3 LSAs) to NSSAs.

NOTE

- When the LS age field (aging time) in the LSA header reaches 3600 seconds, this LSA is deleted.
- After the keyword **set-n-bit** is set, a switch re-establishes neighbor relationships with switches directly connected to it in the NSSA.

Example

Configure Area 1 as an NSSA, and set the timeout period of the translator to 20s.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 1
[HUAWEI-ospfv3-1-area-0.0.0.1] nssa translator-interval 20
```

7.5.49 ospfv3

Function

The **ospfv3** command enables an OSPFv3 process.

The **undo ospfv3** command disables the OSPFv3 process.

By default, the system does not support OSPFv3.

Format

ospfv3 [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ospfv3 *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535. By default, it is 1.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Only when you configure the Route ID in the OSPFv3 view, the OSPFv3 process can run normally. Otherwise, the OSPFv3 process can be viewed but cannot generate LSAs.

If a VPN instance is specified, the OSPFv3 process belongs to the VPN instance. If no VPN instance is specified, the OSPFv3 process is a global instance.

NOTE

Before configuring OSPFv3-related parameters, you must enable OSPFv3.

Example

Enable the OSPFv3 protocol.

```
<HUAWEI> system-view
[HUAWEI] ospfv3
```

7.5.50 ospfv3 area

Function

The **ospfv3 area** command enables the OSPFv3 process on an interface and specifies the area the process belongs to.

The **undo ospfv3 area** command disables the OSPFv3 process on the interface.

By default, the OSPFv3 protocol is not enabled on the interface.

Format

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID.	The value of the area ID can be a decimal integer or in the IPv4 address format. The integer ranges from 0 to 4294967295.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ipv6 enable** command to enable IPv6 in the interface view.

Example

Enable OSPFv3 on an interface and enable OSPFv3 in area 1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
```

Enable OSPFv3 in GE0/0/1, and enable OSPFv3 in area 1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
```

7.5.51 ospfv3 authentication-mode

Function

The **ospfv3 authentication-mode** command configures an authentication mode and a password for an OSPFv3 interface.

The **undo ospfv3 authentication-mode** command deletes the authentication mode and password configured for an OSPFv3 interface.

By default, no authentication mode or password is configured for any OSPFv3 interface.

Format

ospfv3 authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* } [**instance** *instance-id*]

ospfv3 authentication-mode keychain *keychain-name* [**instance** *instance-id*]

undo ospfv3 authentication-mode hmac-sha256 key-id *key-id* [**plain** *plain-text* | **cipher** *cipher-text*] [**instance** *instance-id*]

undo ospfv3 authentication-mode keychain [*keychain-name*] [**instance** *instance-id*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
hmac-sha256	Configures the HMAC-SHA256 authentication mode.	N/A
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
plain	Configures the plaintext password type. Only a plaintext password can be entered, and the password is displayed in plaintext in the configuration file. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	N/A
plain-text	Specifies a plaintext password.	The value is a string of 1 to 255 characters, spaces not supported.
cipher	Configures the ciphertext password type. You can enter either a plaintext or ciphertext password, but the password is displayed in ciphertext in the configuration file.	N/A
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for plaintext passwords and 20 to 392 characters for ciphertext passwords, spaces not supported.
keychain	Configures keychain authentication. **NOTE** Before you configure keychain authentication, run the **keychain** command to configure a keychain, the **key-id** command to configure a key ID, the **key-string** command to configure a password, and the **algorithm** command to configure an algorithm. If these commands are not run, OSPFv3 authentication fails.	N/A

Parameter	Description	Value
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
instance *instance-id*	Specifies the ID of a VLAN to which the specified interface belongs.	The value ranges from 0 to 255, with default value 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to inherent defects and flawed implementation of the TCP/IP protocol suite, there are an increasing number of attacks, which poses greater threats on TCP/IP networks than ever before. The attacks on network devices may lead to network failures. To configure an authentication mode and a password for an OSPFv3 interface to improve OSPFv3 network security, run the **ospfv3 authentication-mode** command.

Precautions

OSPFv3 interface authentication takes precedence over OSPFv3 area authentication.

To configure OSPFv3 area authentication, run the **authentication-mode** command.

Example

Configure OSPFv3 HMAC-SHA256 authentication on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ospfv3 1 area 0
```

```
[HUAWEI-Vlanif100] ospfv3 authentication-mode hmac-sha256 key-id 10 cipher test
```

Configure OSPFv3 HMAC-SHA256 authentication on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 0
[HUAWEI-GigabitEthernet0/0/1] ospfv3 authentication-mode hmac-sha256 key-id 10 cipher test
```

7.5.52 ospfv3 bfd

Function

The **ospfv3 bfd** command enables the bidirectional forwarding detection (BFD) on the specified interface enabled with OSPFv3, or sets the parameter values of a BFD session.

The **undo ospfv3 bfd** command deletes the BFD on the specified interface, or restores the default parameter values of a BFD session.

By default, BFD is not enabled on OSPFv3 interfaces.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

ospfv3 bfd enable [**instance** *instance-id*]

ospfv3 bfd { **min-transmit-interval** *min-transmit-value* | **min-receive-interval** *min-receive-value* | **detect-multiplier** *detect-multiplier-value* } * [**instance** *instance-id*]

undo ospfv3 bfd enable [**instance** *instance-id*]

undo ospfv3 bfd { **min-transmit-interval** [*min-transmit-value*] | **min-receive-interval** [*min-receive-value*] | **detect-multiplier** [*detect-multiplier-value*] } * [**instance** *instance-id*]

Parameters

Parameter	Description	Value
enable	Enables BFD for OSPFv3 on the specified interface.	-
min-transmit-interval *min-transmit-value*	Specifies the minimum interval for sending BFD packets to the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-receive-interval *min-receive-value*	Specifies the minimum interval for receiving BFD packets from the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *detect-multiplier-value*	Indicates the local detection multiplier.	The value is an integer in the range from 3 to 50. The default value is 3.
instance *instance-id*	Specifies an interface instance ID.	The value is an integer in the range from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A link fault or a topology change causes devices to recalculate routes. Therefore, the convergence of routing protocols must be as fast as possible to improve network performance.

Link faults are inevitable. Therefore, quickly detecting faults and notifying routing protocols of the faults is a feasible solution to immediately rectify link faults. If BFD is associated with routing protocols, BFD can speed up the convergence of routing protocols when a link fault occurs.

After OSPFv3 establishes a BFD session, the default parameter values are used. BFD session parameters can also be modified as required.

- Actual interval at which BFD packets are transmitted on the local device = Max { configured interval *min-transmit-value* at which BFD packets are transmitted on the local device, configured interval *min-receive-value* at which BFD packets are received on the peer device }
- Actual interval at which BFD packets are received on the local device = Max { configured interval *min-transmit-value* at which BFD packets are transmitted on the peer device, configured interval *min-receive-value* at which BFD packets are received on the local device }
- Actual period for BFD detection on the local device = Actual interval at which BFD packets are received on the local device x Detection multiplier *detect-multiplier-value* configured on the peer device

For example:

- On the local device, the configured interval at which BFD packets are transmitted is 200 ms; the interval at which BFD packets are received is set to 300 ms; the detection multiplier is 4.
- On the peer device, the configured interval at which BFD packets are transmitted is 100 ms; the interval at which BFD packets are received is 600 ms; the detection multiplier is 5.

Then:

- On the local device, the actual interval at which BFD packets are transmitted is 600 ms calculated by using the formula max {200 ms, 600 ms}; the interval at which BFD packets are received is 300 ms calculated by using the formula max {100 ms, 300 ms}; the detection period is 1500 ms calculated by multiplying 300 ms by 5.
- On the peer device, the actual interval at which BFD packets are transmitted is 300 ms calculated by using the formula max {100 ms, 300 ms}, the actual interval at which BFD packets are received is 600 ms calculated by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms calculated by multiplying 600 ms by 4.

Prerequisites

The set BFD session parameters take effect only when BFD is enabled on the interface.

Configuration Impact

If the global BFD is not configured, BFD on the interface can be configured but the BFD session cannot be set up. Similarly, if the parameters of a BFD session are set but the **ospfv3 bfd enable** command is not configured, the BFD session cannot be set up.

The priority of BFD configured on an interface is higher than that configured in a process. If the BFD is enabled on the interface, the BFD session is set up by using the parameters of the BFD configured on the interface.

Precautions

- After BFD is configured, OSPFv3 establishes BFD sessions only with neighbors.
- The **ospfv3 bfd enable** command and the **ospfv3 bfd block** command are mutually exclusive.
- After BFD is disabled on the interface using the **undo ospfv3 bfd enable** command, the configurations of the parameters of the BFD session on the interface still exist.
- BFD cannot be enabled on VBDIF interfaces.

Example

Enable BFD for OSPFv3 on interface Vlanif10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ospfv3 bfd enable instance 1
```

Configure BFD parameters for OSPFv3 on interface Vlanif10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ospfv3 bfd min-transmit-interval 100 min-receive-interval 100 detect-multiplier 3
instance 1
```

7.5.53 ospfv3 bfd block

Function

The **ospfv3 bfd block** command blocks the bidirectional forwarding detection (BFD) dynamically created by an interface.

The **undo ospfv3 bfd block** command cancels the feature.

By default, BFD is not blocked.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ospfv3 bfd block [**instance** *instance-id*]

undo ospfv3 bfd block [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Indicates the interface instance id.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the **bfd all-interfaces enable** command is run in the OSPFv3 process, all neighbors that enable OSPFv3 and the neighbor relationship is in Full state create BFD sessions. To prevent specific interfaces from being enabled with BFD, you can disable their interfaces from dynamically creating BFD sessions.

Prerequisites

BFD has been enabled on these interfaces.

Before configuring this command, you must run the **ipv6 enable** command in the interface view to enable IPv6.

Precautions

The **ospfv3 bfd enable** command and the **ospfv3 bfd block** command are mutually exclusive.

Example

Block the BFD dynamically created by Vlanif100 when configured the BFD for OSPF3 of all interfaces in the OSPF3 process.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif100
[HUAWEI-Vlanif100] ospfv3 bfd block instance 1
```

7.5.54 ospfv3 cost

Function

The **ospfv3 cost** command sets the cost of the interface in different instances.

The **undo ospfv3 cost** command restores the default cost of the interface in different instances.

By default, the cost of an interface running OSPF is calculated using the following formula: **Interface cost = Bandwidth reference value/Interface bandwidth** where, the bandwidth reference value can be changed using the **bandwidth-reference** command.

Format

ospfv3 cost *cost* [**instance** *instance-id*]

undo ospfv3 cost [*cost*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
cost	Specifies the cost for running OSPFv3.	The value is an integer ranging from 1 to 65535.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the cost for public instances to run OSPFv3 on VLANIF 10 to 33.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

```
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 cost 33
```

Set the cost for public instances to run OSPFv3 on GE0/0/1 to 33.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 cost 33
```

7.5.55 ospfv3 dr-priority

Function

The **ospfv3 dr-priority** command sets the priority of an interface that takes part in the DR or BDR election.

The **undo ospfv3 dr-priority** command restores the default value.

By default, the priority of an interface that takes part in the DR or BDR election is 1.

Format

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [*priority*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
priority	Specifies the priority of the interface that candidates for DR or BDR.	The value is an integer ranging from 0 to 255. The default value is 1.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The priority of the interface determines the qualification of the interface when electing DR or BDR. The interface with the higher priority is preferred. The router whose priority is 0 cannot be elected as a DR or a BDR.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the priority of public instance for electing DR or BDR to 8 on Vlanif10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 dr-priority 8
```

Set the priority of public instance for electing DR or BDR to 8 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 dr-priority 8
```

7.5.56 ospfv3 frr block

Function

The **ospfv3 frr block** command disables the OSPFv3 IP FRR function on a specified interface.

The **undo ospfv3 frr block** command restores the OSPFv3 IP FRR function on the specified interface.

By default, the OSPFv3 IP FRR function is enabled on a specific interface.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ospfv3 frr block [**instance** *instance-id*]

undo ospfv3 frr block [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

OSPFv3 IP FRR can be disabled using the **ospfv3 frr block** command on an interface of a specific device that is running important services and resides on an FRR backup link. This setting prevents the device connected to this interface from being a part of a backup link and being burdened after FRR switches traffic to the backup link.

Example

Disable the OSPFv3 IP FRR function on the interface VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ospfv3 frr block
```

7.5.57 ospfv3 ipsec sa

Function

The **ospfv3 ipsec sa** command configures an SA in the OSPFv3 interface.

The **undo ospfv3 ipsec sa** command deletes the SA configured in the OSPFv3 interface.

By default, no SA is configured in the OSPFv3 interface.

Format

ospfv3 ipsec sa *sa-name*

undo ospfv3 ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	The value is an existing SA name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an SA is configured on an interface, OSPFv3 uses the SA to authenticate and encrypt packets sent and received by the interface.

If no SA is configured on the interface or the configured SA is deleted from the interface, OSPFv3 uses the SA configured in the process or the area where the interface resides to authenticate packets sent and received by the interface.

NOTE

- The SA configured in the interface view takes precedence over that configured in the OSPFv3 area view or the OSPFv3 process view.
- The **ospfv3 ipsec sa** command can be used on all the OSPFv3 instances of an interface.

Example

Configure an SA named **sa3** for the interface VLANIF10. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 0
[HUAWEI-Vlanif10] ospfv3 ipsec sa sa3
```

7.5.58 ospfv3 mib-binding

Function

The **ospfv3 mib-binding** command binds an OSPFv3 process to SNMP and makes OSPFv3 respond to SNMP requests.

The **undo ospfv3 mib-binding** command disables the binding.

By default, there is no binding between the OSPFv3 process and SNMP.

Format

ospfv3 mib-binding *process-id*

undo ospfv3 mib-binding

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value ranges from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When multiple OSPFv3 processes are enabled, you can bind OSPFv3 MIB to a process so that this process can be processed.

Before running this command, run the **ospfv3** command in the system view to create an OSPFv3 process.

NOTE

Only after **ospfv3 mib-binding** *process-id* command is run on a device, can the trap associated with the specified process ID be triggered on the device.

Example

Bind OSPFv3 process to SNMP.

```
<HUAWEI> system-view
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] quit
[HUAWEI] ospfv3 mib-binding 100
```

Disable the binding.

```
<HUAWEI> system-view
```

```
[HUAWEI] undo ospfv3 mib-binding
```

7.5.59 ospfv3 mtu-ignore

Function

The **ospfv3 mtu-ignore** command disables the MTU check on DD packets.

The **undo ospfv3 mtu-ignore** command restores the default value.

By default, the MTU check on DD packets is enabled.

Format

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Disable OSPFv3 from checking the MTU of the DD packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 mtu-ignore
```

Disable OSPFv3 from checking the MTU of the DD packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

```
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 mtu-ignore
```

7.5.60 ospfv3 network-type

Function

The **ospfv3 network-type** command sets the network type of the OSPFv3 interface.

The **undo ospfv3 network-type** command restores the default network type of the OSPFv3 interface.

By default, the network type of an interface is determined by the physical interface. The network type of Ethernet interface is **broadcast**.

Format

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p**] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
broadcast	Indicates that the network type of the interface is changed to broadcast.	-
nbma	Indicates that the network type of the interface is changed to NBMA.	-
p2mp	Indicates that the network type of the interface is changed to point-to-multipoint.	-
non-broadcast	Indicates that the network type of the interface is changed to non-broadcast point-to-multipoint.	-
p2p	Indicates that the network type of the interface is changed to point-to-point.	-
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set network type of Vlanif10 to NBMA.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 network-type nbma
```

Set network type of GE0/0/1 to NBMA.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 network-type nbma
```

7.5.61 ospfv3 peer router-id

Function

The **ospfv3 peer router-id** command sets the DR priority and IPv6 addresses for adjacent switches on an NBMA network.

The **undo ospfv3 peer router-id** command cancels the setting.

By default, IPv6 addresses are not configured for the adjacent switches on an NBMA network.

Format

ospfv3 peer router-id *router-id ipv6-address* [**dr-eligible** | **cost** *cost* | **poll** *interval* | **instance** *instance-id*]*

undo ospfv3 peer router-id *router-id* [*ipv6-address*] [**dr-eligible** | **cost** [*cost*] | **poll** [*interval*] | **instance** *instance-id*]*

Parameters

Parameter	Description	Value
router-id	Specifies the router ID of the adjacent switch.	The value is in dotted decimal notation.
ipv6-address	Specifies the link-local address of the adjacent node.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
dr-eligible	Specifies the neighbor switch that can take part in DR election on the NBMA network.	-
cost *cost*	Specifies the cost of the interface on the neighbor switch of the NBMA network.	The value is an integer ranging from 1 to 65535.
poll *interval*	Specifies the interval for sending polling Hello packets on the neighbor switch on the NBMA network.	The value is an integer ranging from 1 to 65535.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ospfv3 peer router-id** command to set the DR priority and IPv6 addresses for adjacent switches on an NBMA network.

Example

On Vlanif10, specify the peer end to take part in DR selection.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
```

```
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 peer router-id 10.1.1.1 FE80::1 dr-eligible
```

On GE0/0/1, specify the peer end to take part in DR selection.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 peer router-id 10.1.1.1 FE80::1 dr-eligible
```

7.5.62 ospfv3 router-id auto-recover disable

Function

Using the **ospfv3 router-id auto-recover disable** command, you can disable automatic recovery that will take effect after router ID conflict is detected.

Using the **undo ospfv3 router-id auto-recover disable** command, you can enable automatic recovery that will take effect after router ID conflict is detected.

By default, automatic recovery takes effect after router ID conflict occurs.

Format

ospfv3 router-id auto-recover disable

undo ospfv3 router-id auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If router ID conflict occurs in an OSPFv3 area, the system can define a new router ID, preventing route flapping and reducing route calculation operations. Other protocols will not go Down when the CPU usage is controlled.

NOTE

- After the automatic recovery function is restored and router ID conflict occurs in an OSPFv3 area, the switch changes the conflicted router ID to its own IP address. Even the router ID that is manually configured will be changed.
- After the router ID is changed, the system defines a new router ID for a maximum of three times by default if router ID conflict persists.

Example

Disable automatic recovery that will take effect after router ID conflict is detected.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 router-id auto-recover disable
```

7.5.63 ospfv3 suppress-flapping peer

Function

The **ospfv3 suppress-flapping peer** command configures detection parameters for OSPFv3 neighbor relationship flapping suppression.

The **undo ospfv3 suppress-flapping peer** command restores the default detection parameters.

By default, the detection interval of OSPFv3 neighbor relationship flapping suppression is 60s, the suppression threshold is 10, and the interval for exiting from suppression is 120s.

Format

ospfv3 suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } * [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } * [**instance** *instance-id*]

Parameters

Parameter	Description	Value
detecting-interval *detecting-interval*	Specifies the detection interval of OSPFv3 neighbor relationship flapping suppression. Each OSPFv3 interface on which OSPFv3 neighbor relationship flapping suppression is enabled starts a flapping counter. If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count is incremented by 1.	The value is an integer ranging from 1 to 300, in seconds. The default value is 60s.

Parameter	Description	Value
threshold *threshold*	Specifies the threshold of OSPFv3 neighbor relationship flapping suppression. When the flapping_count reaches or exceeds *threshold*, flapping suppression takes effect.	The value is an integer ranging from 1 to 1000. The default value is 10.
resume-interval *resume-interval*	Specifies the interval for exiting from OSPFv3 neighbor relationship flapping suppression. If the interval between two successive neighbor status changes from Full to a non-Full state is longer than *resume-interval*, the flapping_count is reset. **NOTE** The value of *resume-interval* must be greater than that of *detecting-interval*.	The value is an integer ranging from 2 to 1000, in seconds. The default value is 120s
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure detection parameters for OSPFv3 neighbor relationship flapping suppression on an interface, run the **ospfv3 suppress-flapping peer** command. However, keeping the default configurations is recommended.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you configure detection parameters for it. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the detection parameters.

Example

Set the detection interval of OSPFv3 neighbor relationship flapping suppression to 5s, the suppression threshold to 40, and the interval for exiting from suppression to 20s on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospfv3 suppress-flapping peer detecting-interval 5 threshold 40 resume-interval
20
```

7.5.64 ospfv3 suppress-flapping peer disable

Function

The **ospfv3 suppress-flapping peer disable** command disables OSPFv3 neighbor relationship flapping suppression from an interface.

The **undo ospfv3 suppress-flapping peer disable** command enables OSPFv3 neighbor relationship flapping suppression on an interface.

By default, OSPFv3 neighbor relationship flapping suppression is enabled on all interfaces.

Format

ospfv3 suppress-flapping peer disable [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer disable [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, OSPFv3 neighbor relationship flapping suppression is enabled on all interfaces in the same OSPFv3 process. To disable the function from one of the interfaces, run the **ospfv3 suppress-flapping peer disable** command.

NOTE

When an interface enters the flapping suppression state, all neighbor relationships on the interface enter the state accordingly.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you enable the function on an interface using the **undo ospfv3**

suppress-flapping peer disable command. By default, the function is enabled globally. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it first.

Example

Disable OSPFv3 neighbor relationship flapping suppression from VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospfv3 suppress-flapping peer disable
```

7.5.65 ospfv3 suppress-flapping peer hold-down

Function

The **ospfv3 suppress-flapping peer hold-down** command configures the Hold-down mode and sets duration for this mode.

The **undo ospfv3 suppress-flapping peer hold-down** command cancels the Hold-down mode.

By default, the Hold-down mode is disabled.

Format

ospfv3 suppress-flapping peer hold-down *interval* [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer hold-down *interval* [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Specifies the duration of the Hold-down mode.	The value is an integer ranging from 1 to 600, in seconds.
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **ospfv3 suppress-flapping peer hold-down** *interval* command.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you configure the Hold-down mode and set duration for this mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the Hold-down mode and set duration for this mode.

Example

Configure the Hold-down mode and set its duration to 200s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospfv3 suppress-flapping peer hold-down 200
```

7.5.66 ospfv3 suppress-flapping peer hold-max-cost disable

Function

The **ospfv3 suppress-flapping peer hold-max-cost disable** command disables the Hold-max-cost mode.

The **undo ospfv3 suppress-flapping peer hold-max-cost disable** command enables the Hold-max-cost mode.

By default, the Hold-max-cost mode is enabled.

Format

ospfv3 suppress-flapping peer hold-max-cost disable [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer hold-max-cost disable [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **ospfv3 suppress-flapping peer hold-down** *interval* command.

NOTE

The Hold-max-cost mode can prevent a device from being isolated from the network. If a device on a key path is isolated from the network due to OSPFv3 neighbor relationship flapping, the network is separated into two isolated parts. To prevent this problem, use the Hold-max-cost mode on the key path.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you configure duration for the Hold-max-cost mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure duration for the Hold-max-cost mode.

Precautions

The Hold-max-cost mode takes effect only unidirectionally. If a remote device does not support OSPFv3 neighbor relationship flapping suppression, bidirectional traffic between the local and remote devices may travel along different paths.

Example

Disable the Hold-max-cost mode on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospfv3 suppress-flapping peer hold-max-cost disable
```

7.5.67 ospfv3 timer dead

Function

The **ospfv3 timer dead** command sets the dead interval of the OSPFv3 neighbor of the instance on the interface.

The **undo ospfv3 timer dead** command restores the default value.

By default, the dead interval of OSPFv3 neighbor is 40 seconds for the interface of P2P or Broadcast type. The dead interval of OSPFv3 neighbor is 120 seconds for the interface of P2MP or NBMA type.

Format

ospfv3 timer dead *interval* [**instance** *instance-id*]

undo ospfv3 timer dead [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the dead interval of OSPFv3.	The value is an integer ranging from 1 to 65535, in seconds.
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Dead interval of OSPFv3 neighbor refers to that the neighbor is invalid if the neighbor does not receive the Hello packets from its neighbor in the interval. The dead interval of switches in the same network segment must be consistent.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

By default, the dead interval of OSPF neighbors is four times the Hello packet interval. After the Hello packet interval is configured in the instance of the interface using the **ospfv3 timer hello** command, the default dead interval of the OSPFv3 neighbor of the instance on the interface is changed to be four times the Hello packet interval.

Example

Set the dead interval of the neighbor to 80 seconds for Vlanif10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 timer dead 80
```

Set the dead interval of the neighbor to 80 seconds for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 timer dead 80
```

7.5.68 ospfv3 timer hello

Function

The **ospfv3 timer hello** command specifies the interval for sending Hello packets on the interface instance.

The **undo ospfv3 timer hello** command restores the default interval.

By default, for the interface of the P2P and broadcast type, the interval for sending Hello packets is 10 seconds. For the interface of the P2MP and NBMA type, the interval for sending Hello packets is 30 seconds.

Format

ospfv3 timer hello *interval* [**conservative**] [**instance** *instance-id*]

undo ospfv3 timer hello [*interval* [**conservative**]] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the interval for an interface to send the Hello packets.	The value is an integer ranging from 1 to 65535, in seconds.
conservative	Indicates the conservative mode of the dead timer. If the conservative mode is configured, the value configured for the dead timer using the **ospfv3 timer dead** command takes effect even when the value is less than 10s.	-
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the interval for sending Hello packets on Vlanif10 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 timer hello 20
```

Set the interval for sending Hello packets on GE0/0/1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
```

```
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 timer hello 20
```

7.5.69 ospfv3 timer poll

Function

The **ospfv3 timer poll** command sets the polling interval for sending Hello packets on NBMA network.

The **undo ospfv3 timer poll** command restores the default polling interval.

By default, the polling interval for sending Hello packets on NBMA network is 120 seconds.

Format

ospfv3 timer poll *interval* [**instance** *instance-id*]

undo ospfv3 timer poll [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Specifies the polling interval of Hello packets.	The value is an integer ranging from 1 to 65535, in seconds.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

On the NBMA network, if a neighbor is invalid, you can configure switches to send Hello packet based on the polling interval that is set by the **ospfv3 timer poll** command. The polling interval should be at least 4 times that of the Hello interval.

OSPFv3 does not support the configuration on a null interface.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the polling interval for sending Hello packets on the Vlanif10 to 130 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 timer poll 130
```

Set the polling interval for sending Hello packets on the GE0/0/1 to 130 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 timer poll 130
```

7.5.70 ospfv3 timer retransmit

Function

The **ospfv3 timer retransmit** command specifies the interval for retransmitting the LSA on the interface instance.

The **undo ospfv3 timer retransmit** command restores the default value.

By default, the interval for retransmitting LSAs is 5 seconds.

Format

ospfv3 timer retransmit *interval* [**instance** *instance-id*]

undo ospfv3 timer retransmit [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the interval for retransmitting LSAs.	The value is an integer ranging from 1 to 3600, in seconds.
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After sending an LSA to its neighbor, a switch needs to wait for the Ack packet from the neighbor. If the switch does not receive the Ack packet in the retransmission interval, the switch retransmits the LSA.

The interval for retransmitting LSA between the neighboring switches should not be set too short. Otherwise, it leads to unnecessary retransmission.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the interval for retransmitting the LSA between VLANIF 10 and its neighboring switch to 12 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 timer retransmit 12
```

Set the interval for retransmitting the LSA between GE0/0/1 and its neighboring switch to 12 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 timer retransmit 12
```

7.5.71 ospfv3 trans-delay

Function

The **ospfv3 trans-delay** command sets the delay for transmitting LSA on an interface instance.

The **undo ospfv3 trans-delay** command restores the default value.

By default, the delay for transmitting LSA is 1 second.

Format

ospfv3 trans-delay *interval* [**instance** *instance-id*]

undo ospfv3 trans-delay [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the delay for transmitting LSA on an interface.	The value is an integer ranging from 1 to 800, in seconds. By default, it is 1 second.
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The LSA in the LSDB of the local switch ages with time. The aging of the LSA increases by 1 per second, but the aging of the LSA does not change in the transmission process. Therefore, it is necessary to add the delay to the aging time of the LSA before the LSA is sent.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the delay for transmitting LSA on VLANIF 10 to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ospfv3 1 area 1
[HUAWEI-Vlanif10] ospfv3 trans-delay 3
```

Set the delay for transmitting LSA on GE0/0/1 to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ospfv3
[HUAWEI-ospfv3-1] router-id 10.1.1.1
[HUAWEI-ospfv3-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ospfv3 1 area 1
[HUAWEI-GigabitEthernet0/0/1] ospfv3 trans-delay 3
```

7.5.72 ospfv3 valid-ttl-hops

Function

The **ospfv3 valid-ttl-hops** command enables OSPFv3 GTSM and sets a TTL value.

The **undo ospfv3 valid-ttl-hops** command disables OSPFv3 GTSM.

By default, OSPFv3 GTSM is disabled.

Format

ospfv3 valid-ttl-hops *valid-ttl-hops-value* [**vpn-instance** *vpn-instance-name*]

undo ospfv3 valid-ttl-hops [*valid-ttl-hops-value*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
valid-ttl-hops-value	Specifies a TTL.	The value is an integer ranging from 1 to 255.
vpn-instance *vpn-instance-name*	Indicates the name of a VPN instance. If this parameter is specified, only the TTL values of the packets in the specified VPN instance are checked.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an OSPFv3 network requires high security, you can configure OSPFv3 GTSM and an authentication mode to improve network security. During network attacks, attackers may simulate OSPFv3 packets and continuously send them to a device. If the packets are destined for the device, it directly sends them to the control plane for processing without validating them. As a result, the increased processing workload on the control plane results in high CPU usage. GTSM protects devices against potential attacks and improves system security by checking whether the TTL value in each IP packet header is within a pre-defined range.

To enable OSPFv3 GTSM, run the **ospfv3 valid-ttl-hops**. To check the TTL values of packets that match a GTSM policy in a specified VPN instance, specify **vpn-instance** in the command.

The **ospfv3 valid-ttl-hops** command enables OSPFv3 GTSM on both the public network and VPNs. For example, if you run the **ospfv3 valid-ttl-hops 5 vpn-instance** *vpn1* command, OSPFv3 GTSM takes effect on both the public network and VPN 1, the TTL values of the OSPFv3 packets in the VPN 1 are checked, and the default action is performed on the packets that fail to match the GTSM policy.

Follow-up Procedure

GTSM checks the TTL values of only the packets that match a GTSM policy. For packets that do not match the GTSM policy, you can specify **pass** in the **gtsm default-action** command to allow these packets to pass the filtering or specify **drop** in the command to discard them.

Precautions

- If a VPN instance is specified in the **ospfv3 valid-ttl-hops** command and an interface is bound to the VPN instance, the interface discards all received unicast packets if the set TTL value is less than the actual hop count on the network.
- If a virtual link or sham link is deployed, configure a TTL value based on the actual hop count on the network (the number of routers through which the virtual link or sham link passes) to prevent the local switch from discarding packets from neighbors over the virtual link or sham link.
- Therefore, if you want to apply the configured TTL value to packets only in a VPN or the public network, specify **pass** in the **gtsm default-action** command to prevent the OSPFv3 packets in other instances from being discarded incorrectly.

Example

Enable OSPFv3 GTSM and set the maximum number of TTL hops to 5 for the packets that can be received from the public network.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 valid-ttl-hops 5
```

7.5.73 preference (OSPFv3)

Function

The **preference** command sets the preference for an OSPFv3 route.

The **undo preference** command restores the default setting.

By default, the preference of the OSPFv3 route is 10. When ASE is specified, the default value is 150.

Format

preference [**ase**] { *preference* | **route-policy** *route-policy-name* }*

undo preference [**ase**]

Parameters

Parameter	Description	Value
ase	Sets the preference for an AS external route or an NSSA route.	-
preference	Specifies the preference for OSPFv3 routes.	It is an integer ranging from 1 to 255.
route-policy *route-policy-name*	Specifies the name of a routing policy and sets the preference for specified routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The smaller the preference value, the higher the preference.

Multiple dynamic routing protocols may be run on a switch at the same time. Consequently, there is a problem of sharing and selecting routing information among routing protocols. Therefore, the system sets a default reference for each routing protocol. If different routing protocols find multiple routes to the same destination, the route discovered by the routing protocol with a higher preference is selected to forward IP packets.

Precautions

Creating a route-policy before it is referenced is recommended. If a nonexistent route-policy is referenced using the command, the configured priority applies to all OSPFv3 routes.

Example

Set the preference for OSPFv3 routes.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] preference 5
```

7.5.74 reset ospfv3

Function

The **reset ospfv3** command restarts the OSPFv3 process.

The **reset ospfv3 counters** command resets OSPFv3 statistics.

Format

reset ospfv3 { *process-id* | **all** } [**graceful-restart** [**extend-period** *period*]]

reset ospfv3 { *process-id* | **all** } **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process number.	The value is an integer that ranges from 1 to 65535.
all	Restarts all OSPFv3 processes.	-
graceful-restart	Restarts the OSPFv3 process in GR mode.	-
extend-period *period*	Prolongs the current GR period.	The value is an integer that ranges from 1 to 1800, expressed in seconds.
neighbor	Resets neighbor statistics.	-
interface-type interface-number	Specifies the type and number of the interface.	-
router-id	Specifies the router ID of a neighbor.	It is in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can choose general restart or graceful restart through the parameters.

By setting **extend-period**, you can prolong the current GR period. The prolonged GR period becomes invalid after the process restarts. This parameter takes effect for one time. That is, after the switch performs GR next time, the value of the period returns to the one set by using **graceful-restart** [**extend-period** *period*].

NOTICE

If OSPFv3 connections are reset, OSPFv3 neighbor relationships will be interrupted and the original information cannot be restored. Exercise caution before running the **reset ospfv3** command.

Example

Reset OSPFv3 statistics.

```
<HUAWEI> reset ospfv3 1 counters
```

7.5.75 reset ospfv3 suppress-flapping peer

Function

The **reset ospfv3 suppress-flapping peer** command forces an interface to exit from OSPFv3 neighbor relationship flapping suppression.

Format

reset ospfv3 *process-id* **suppress-flapping peer** [*interface-type interface-number*] [**notify-peer**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies an interface type and number.	-
notify-peer	Instructs neighbors to exit from OSPFv3 neighbor relationship flapping suppression.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Interfaces exit from flapping suppression in the following scenarios:

- The suppression timer expires.
- The corresponding OSPFv3 process is reset.
- An OSPFv3 neighbor is reset using the **reset ospfv3** command.
- The **reset ospfv3 suppress-flapping peer** command is run.
- OSPFv3 neighbor relationship flapping suppression is disabled globally using the **suppress-flapping peer disable (OSPFv3)** command in the OSPFv3 view.

If **notify-peer** is specified when the **reset ospfv3 suppress-flapping peer** command is run on a device, the device sends Hello packets in which **HelloInterval** and **RouterDeadInterval** are 0s to its neighbors to instruct the neighbors to exit from OSPFv3 neighbor relationship flapping suppression too. If the neighbors fail to receive such Hello packets, the function of **notify-peer** does not take effect. To force the neighbors to exit from OSPFv3 neighbor relationship flapping suppression, run the **reset ospfv3 suppress-flapping peer** command on them.

Example

Force interfaces to exit from OSPFv3 neighbor relationship flapping suppression.

```
<HUAWEI> reset ospfv3 1 suppress-flapping peer
```

7.5.76 rfc1583 compatible (OSPFv3)

Function

The **rfc1583 compatible** command converts rules defined in RFC 5340 into rules defined in RFC 1583.

The **undo rfc1583 compatible** command converts rules defined in RFC 1583 into rules defined in RFC 5340.

By default, OSPFv3 supports the routing rule of RFC 5340.

Format

rfc1583 compatible

undo rfc1583 compatible

Parameters

None

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

RFC 5340 and RFC 1583 define different OSPFv3 route selection rules. When enabling OSPFv3, configure the same route selection rules on all devices in the same OSPFv3 area. For example, an OSPFv3 device supports route selection rules defined in RFC 5340 by default. If the other routers in the same OSPFv3 area support route selection rules defined in RFC 1583, run the **rfc1583 compatible** command.

Example

Converts rules defined in RFC 5340 into rules defined in RFC 1583.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] rfc1583 compatible
```

7.5.77 route-tag (OSPFv3)

Function

The **route-tag** command sets the tag value for imported VPN routes.

The **undo route-tag** command restores the default setting.

By default, the first two bytes of the tag value are fixed as 0xD000, and the last two bytes are the local BGP AS number. For example, if the local BGP AS number is 100, the default tag value in decimal notation is 3489661028.

Format

route-tag *tag-value*

undo route-tag

Parameters

Parameter	Description	Value
tag-value	Specifies the tag value for the imported VPN route.	It is an integer ranging from 0 to 4294967295.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

On a PE, the VPN instance associated with an OSPFv3 instance is configured with a VPN route tag. This route tag must be carried in Type 5 or Type 7 LSAs. You are advised to configure the same route tag for PEs in the same area. Not transmitted in BGP extended community attributes, the VPN route tag is configured and takes effect only on the PEs that receive BGP routes and generate OSPFv3 LSAs. Different OSPFv3 processes can be configured with the same route tag.

If a BGP AS number is greater than 65535, the default tag 0 is used. You can use the command to change the tag in this case.

The only difference between the tag value set through the **route-tag** command and the tag value set through other commands is the preference:

- The preference of the tag value set through the **import-route** command is the highest.
- The preference of the tag value set through the **route-tag** command is medium.
- The preference of the tag value set through the **default tag** *tag* command is the lowest.

If a Type 5 or Type 7 LSA whose tag is the same as the local tag is received, this LSA is ignored during route calculation.

Example

Set the tag value of the imported VPN routes in OSPFv3 process 100 to 100.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance test
[HUAWEI-vpn-instance-test] ipv6-family
[HUAWEI-vpn-instance-test-af-ipv6] route-distinguisher 100:1
[HUAWEI-vpn-instance-test-af-ipv6] quit
[HUAWEI-vpn-instance-test] quit
[HUAWEI] ospfv3 100 vpn-instance test
[HUAWEI-ospfv3-100] route-tag 100
```

7.5.78 router-id (OSPFv3)

Function

The **router-id** command sets the Router ID for the switch that runs OSPFv3.

The **undo router-id** command deletes the Router ID that is set for OSPFv3 switch.

By default, there is no Router ID for the switch that runs OSPFv3.

Format

router-id *router-id*

undo router-id

Parameters

Parameter	Description	Value
router-id	Indicates the switch ID.	It is in dotted decimal notation.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The Router ID of an OSPFv3 process is unique in an AS. If no Router ID is set, the OSPFv3 process does not run.

When you set a switch ID, ensure that the Router IDs of any two processes are different in an AS.

NOTE

Multiple OSPFv3 processes can run on a switch by setting the different process ID. In this case, you need to specify different Router IDs for different processes.

Example

Set the Router ID of the OSPFv3 process 1 to 10.1.1.3.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] router-id 10.1.1.3
```

7.5.79 sham-hello enable (OSPFv3)

Function

The **sham-hello enable** command enables OSPFv3 to regard the LSU packets and the LSAck packets the same as the Hello packets.

The **undo sham-hello** command disables the operation.

By default, the sham-hello feature is disabled.

Format

sham-hello enable

undo sham-hello

Parameters

none

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The **sham-hello enable** command, OSPFv3 can regard the LSU packets and the LSAck packets the same as the Hello packets. After receiving this kind of packets, OSPFv3 refreshes the timeout timer of the neighbors to maintain the integrity of their relationship.

Example

Enable sham-hello.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] sham-hello enable
```

7.5.80 sham-link (OSPFv3)

Function

The **sham-link** command configures a sham link.

The **undo sham-link** command deletes a sham link or restores the default setting. If no optional parameters are specified, a sham link is deleted; if optional parameters are specified, the default values of the parameters are restored.

Format

sham-link *source-address destination-address* [**cost** *cost* | **dead** *dead-interval* | **hello** *hello-interval* | **instance** *instance-id* | **retransmit** *retransmit-interval* | **trans-delay** *trans-delay-interval* | { **authentication-mode** { **hmac-sha256 key-id** *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* } | **keychain** *keychain-name* } | **ipsec sa** *sa-name* }] *

undo sham-link *source-address destination-address* [**cost** [*cost*] | **dead** [*dead-interval*] | **hello** [*hello-interval*] | **retransmit** [*retransmit-interval*] | **trans-delay** [*trans-delay-interval*] | { **authentication-mode** { **hmac-sha256 key-id** *key-id* | **keychain** } | **ipsec sa** [*sa-name*] }] *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
source-address	Specifies the source IPv6 address.	-
destination-address	specifies the destination IPv6 address.	-
cost *cost*	Specifies the cost of a sham link	The value is an integer ranging from 1 to 65535. By default, it is 1.
dead *dead-interval*	Specifies the dead interval. This value must be equal to the *dead-interval* of the switch that sets up a sham link with the local switch, and must be at least four times that of *hello-interval*.	The value is an integer ranging from 1 to 65535, in seconds.
hello *hello-interval*	Specifies the interval for sending Hello packets on an interface. This value must be equal to the *hello-interval* of the switch that sets up the sham link with the local switch.	The value is an integer ranging from 1 to 65535, in seconds.
instance *instance-id*	Specifies the instance ID of a sham link.	The value is an integer ranging from 0 to 255.
retransmit *retransmit-interval*	Specifies the interval for retransmitting LSAs on an interface.	The value is an integer ranging from 1 to 3600, in seconds.
trans-delay *trans-delay-interval*	Specifies the delay for sending LSAs on an interface.	The value is an integer ranging 1 to 800, in seconds.
authentication-mode	Indicates the authentication mode over the sham link.	-
hmac-sha256	Sets the HMAC-SHA256 authentication mode.	-
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
plain	Configures the plaintext password type. Only a plaintext password can be entered, and the password is displayed in plaintext in the configuration file. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
plain-text	Specifies a plaintext password.	The value is a string of 1 to 255 characters, spaces not supported.
cipher	Configures the ciphertext password type. You can enter either a plaintext or ciphertext password, but the password is displayed in ciphertext in the configuration file.	-
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for plaintext passwords and 20 to 392 characters for ciphertext passwords, spaces not supported.
keychain	Configures keychain authentication. **NOTE** Before you configure keychain authentication, run the **keychain** command to configure a keychain, the **key-id** command to configure a key ID, the **key-string** command to configure a password, and the **algorithm** command to configure an algorithm. If these commands are not run, OSPFv3 authentication fails.	-

Parameter	Description	Value
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
ipsec sa *sa-name*	Specifies the name of an SA configured for an OSPFv3 sham link.	The value is an existing SA name.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

The **sham-link** command can be configured only in the OSPFv3 VPN process. If two PEs belong to the same area and have an intra-area route, you can set up a sham link between the two PEs so that the VPN backbone route is preferred over the intra-area route.

Example

Create an OSPFv3 sham link with the source address being FC00:0:0:1001::1 and destination address being FC00:0:0:2001::1.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1 vpn-instance vrf1
[HUAWEI-ospfv3-1] area 1
[HUAWEI-ospfv3-1-area-0.0.0.1] sham-link fc00:0:0:1001::1 fc00:0:0:2001::1
```

7.5.81 silent-interface (OSPFv3)

Function

The **silent-interface** command suppresses the specified interface from sending and receiving OSPFv3 packets.

The **undo silent-interface** command restores the default setting.

By default, the interface is permitted to send or receive OSPFv3 packets.

Format

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Indicates all interfaces in a process.	-
interface-type interface-number	Indicates the interface type and interface number.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

To prevent OSPFv3 routing information of a switch from being obtained by other switches on a certain network and prevent the switch from receiving routing information from other switches, you can disable an OSPFv3 interface on the switch from sending or receiving OSPFv3 packets.

After an interface on a switch is disabled from sending or receiving OSPFv3 packets, the direct route of the interface can still be advertised by the switch through an Intra-Area-Prefix-LSA, but no OSPFv3 neighbor relationship will be established on the interface. This enhances OSPFv3 adaptability.

In different processes, you can suppress the same interface from sending and receiving OSPFv3 packets. However, the **silent-interface** command takes effect only in the specified process of an interface, not all processes associated with the interface.

Example

Suppress Vlanif10 from sending and receiving OSPFv3 packets.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] silent-interface vlanif 10
```

7.5.82 spf timers

Function

The **spf timers** command sets the interval for calculating OSPFv3 routes by a common SPF timer.

The **undo spf timers** command restores the default setting.

By default, the interval for calculating OSPFv3 routes by a common SPF timer is not set.

Format

spf timers *delay-interval hold-interval*

undo spf timers

Parameters

Parameter	Description	Value
delay-interval	Specifies the delay for OSPFv3 from receiving network changes to performing SPF calculation.	The value is an integer ranging from 0 to 65535 seconds.
hold-interval	Specifies the holding interval between two consecutive SPF calculations.	The value is an integer ranging from 0 to 65535 seconds.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

According to the local LSDB, the switch that runs OSPFv3 can calculate an SPT with itself as the root and determines the next hop to the destination network according to the SPT. Adjusting SPF calculation interval can avoid the exhaustion of bandwidth and switch sources caused by frequent change of the network.

Precautions

- By default, the intelligent SPF timer takes effect.
- The **spf timers** *delay-interval hold-interval* and **spf-schedule-interval** *delay-interval hold-interval* commands have the same functions.
- The configurations of the **spf timers** *delay-interval hold-interval*, **spf-schedule-interval** *delay-interval hold-interval*, and **spf-schedule-interval intelligent-timer** *max-interval start-interval hold-interval-1* commands will override each other, and only the configuration of the last executed command takes effect.

Example

Set both the OSPFv3 route calculation interval and the hold interval to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] spf timers 6 6
```

7.5.83 spf-schedule-interval (OSPFv3)

Function

The **spf-schedule-interval** command sets the interval for OSPFv3 to calculate routes.

The **undo spf-schedule-interval** command restores the default setting.

By default, the intelligent timer is enabled. The interval for the SPF calculation is expressed in milliseconds. The maximum interval for the SPF calculation is 10000 ms, the initial interval is 500 ms, and the Holdtime interval is 2000 ms.

Format

spf-schedule-interval { *delay-interval hold-interval* | **intelligent-timer** *max-interval start-interval hold-interval-1* }

undo spf-schedule-interval

Parameters

Parameter	Description	Value
delay-interval	Specifies the delay from the time when OSPFv3 receives a route change to the time when the SPF calculation is performed.	The value is an integer ranging from 0 to 65535, in seconds.
hold-interval	Specifies the hold interval between two consecutive SPF calculations.	The value is an integer ranging from 0 to 65535, in seconds.
intelligent-timer	Specifies the SPF calculation interval set through an intelligent timer.	-
max-interval	Specifies the maximum interval for performing the SPF calculation.	The value is an integer ranging from 1 to 20000, in milliseconds. The default value is 10000.
start-interval	Specifies the initial interval for performing the OSPFv3 SPF calculation.	The value is an integer ranging from 1 to 1000, in milliseconds. The default value is 500.

Parameter	Description	Value
hold-interval-1	Specifies the hold interval for performing the OSPFv3 SPF calculation.	The value is an integer ranging from 1 to 5000, in milliseconds. The default value is 2000.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the local LSDB, a device that runs OSPFv3 uses the SPF algorithm to calculate the shortest path tree with itself as the root, and determines the next hop to the destination network based on the shortest path tree. Adjusting the interval at which the SPF calculation is performed can prevent too many bandwidth resources and device resources from being consumed due to frequent network changes.

Precautions

- The **spf timers** *delay-interval hold-interval* and **spf-schedule-interval** *delay-interval hold-interval* commands have the same functions.
- The configurations of the **spf timers** *delay-interval hold-interval*, **spf-schedule-interval** *delay-interval hold-interval*, and **spf-schedule-interval intelligent-timer** *max-interval start-interval hold-interval-1* commands will override each other, and only the configuration of the last executed command takes effect.

Configuration Impact

After the **spf-schedule-interval intelligent-timer** command is configured, the interval for the SPF calculation is as follows:

1. The initial interval for the SPF calculation is specified by the parameter *start-interval*.
2. The interval for the SPF calculation for the nth (n≥2) time is equal to *hold-interval-1*$\times 2^{(n-2)}$.
3. When the interval specified by *hold-interval-1*$\times 2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPFv3 performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Example

Set the delay interval at which OSPFv3 route calculation is performed to 5s and the hold interval at which OSPFv3 route calculation is performed to 6s.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] spf-schedule-interval 5 6
```

Set the maximum interval for performing the SPF calculation to 10000 ms, the initial interval to 700 ms, and the hold interval to 4000 ms.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] spf-schedule-interval intelligent-timer 10000 700 4000
```

7.5.84 stub (OSPFv3 Area)

Function

The **stub** command sets an OSPFv3 area to the stub area.

The **undo stub** command cancels the settings.

By default, no area is set to the stub area.

Format

stub [**no-summary** | **default-route-advertise backbone-peer-ignore**] *

undo stub

Parameters

Parameter	Description	Value
no-summary	Disables an ABR from sending non-default Type 3 LSAs to the stub area. This parameter applies only to ABRs of stub areas. If the parameter is configured on an ABR, the ABR advertises only one default Type 3 LSA (no other Type 3 LSAs) to the stub area. In this case, this area is also called a totally stub area.	-
default-route-advertise	Configures an ABR to advertise a default Type 3 LSA to the stub area. This parameter applies only to ABRs of stub areas.	-
backbone-peer-ignore	Prevents an ABR from checking the neighbor status when the ABR generates a default Type 3 LSA and advertises it to the stub area. This parameter applies only to ABRs of stub areas. If the parameter is configured on an ABR, the ABR generates a default Type 3 LSA and advertises it to the stub area as long as an interface is Up in the backbone area.	-

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The stub area attribute must be configured on all switches in a stub area.

- If the **stub** command is run on an ABR, without parameters specified, the ABR advertises a default Type 3 LSA and advertises it to the stub area as long as an OSPFv3 neighbor in the full state exists in the backbone area.
- If the **stub no-summary** command is run on an ABR, the ABR is disabled from sending non-default Type 3 LSAs to the stub area connected to the ABR.
- If the **stub default-route-advertise backbone-peer-ignore** command is run on an ABR, the ABR generates a default Type 3 LSA and advertises it to the stub area as long as an interface is Up in the backbone area.

Precautions

The backbone area cannot be configured as a stub area.

Example

Set the OSPFv3 area 1 to the stub area.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] area 1
[HUAWEI-ospfv3-1-area-0.0.0.1] stub
```

7.5.85 stub-router (OSPFv3)

Function

The **stub-router** command configures a device as stub router.

The **undo stub-router** command restores the default configuration.

By default, no stub router exists.

Format

stub-router [**on-startup** [*interval*]]

undo stub-router

Parameters

Parameter	Description	Value
on-startup [*interval*]	Specifies the interval during which a device acts as a stub router when the device is restarted or faulty. ● If **on-startup** is not specified, the device is always a stub router, even if the cost of all routes advertised by the device is 65535. ● If **on-startup** is specified, the device works as a stub router only when it restarts or is faulty. The hold time of the stub router state is determined by *interval* parameter. If the *interval* parameter is not configured, the default interval (500 seconds) is used.	The value is an integer ranging from 5 to 65535, in seconds. By default, it is 500 seconds.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

After the **stub-router** command is configured on a switch, the stub router informs other OSPFv3 devices not to use this stub router for data forwarding by increasing the metrics of the links in the Router-LSA generated by the switch. Since the metric is not infinite, the devices to this stub router still exist. The metrics of all links in the device Router-LSAs generated by the stub router are set to 65535.

Example

Configure the device as a stub router.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] stub-router
```

7.5.86 suppress-flapping peer disable (OSPFv3)

Function

The **suppress-flapping peer disable** command disables OSPFv3 neighbor relationship flapping suppression globally.

The **undo suppress-flapping peer disable** command enables OSPFv3 neighbor relationship flapping suppression globally.

By default, OSPFv3 neighbor relationship flapping suppression is enabled globally.

Format

suppress-flapping peer disable

undo suppress-flapping peer disable

Parameters

None

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

If an interface carrying OSPFv3 services alternates between Up and Down, OSPFv3 neighbor relationship flapping occurs on the interface. During the flapping, OSPFv3 frequently sends Hello packets to reestablish the neighbor relationship, synchronizes LSDBs, and recalculates routes. In this process, a large number of packets are exchanged, adversely affecting neighbor relationship stability, OSPFv3 services, and other OSPFv3-dependent services, such as LDP and BGP. OSPFv3 neighbor relationship flapping suppression can address this problem by delaying OSPFv3 neighbor relationship reestablishment or preventing service traffic from passing through flapping links.

By default, OSPFv3 neighbor relationship flapping suppression is enabled globally. To disable this function globally, run the **suppress-flapping peer disable** command.

Example

Disable neighbor relationship flapping suppression globally.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
[HUAWEI-ospfv3-1] suppress-flapping peer disable
```

7.5.87 vlink-peer (OSPFv3 Area)

Function

The **vlink-peer** command creates and configures a virtual link.

The **undo vlink-peer** command removes the existing virtual link.

By default, no virtual link is configured on OSPFv3.

Format

vlink-peer *router-id* [**hello** *hello-interval* | **retransmit** *retransmit-interval* | **trans-delay** *trans-delay-interval* | **dead** *dead-interval* | **instance** *instance-id* |

{ **authentication-mode** { **hmac-sha256 key-id** *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* } | **keychain** *keychain-name* } | **ipsec sa** *sa-name* }] *

undo vlink-peer *router-id* [**hello** [*hello-interval*] | **retransmit** [*retransmit-interval*] | **trans-delay** [*trans-delay-interval*] | **dead** [*dead-interval*] | { **authentication-mode** { **hmac-sha256 key-id** *key-id* | **keychain** } | **ipsec sa** [*sa-name*] }] *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
router-id	Specifies the switch ID of a virtual link neighbor.	The value is in dotted decimal notation.
hello *hello-interval*	Specifies the interval for sending Hello packets on an interface. This value must be equal to the *hello-interval* value of the switch that sets up a virtual link with the interface.	The value is an integer ranging from 1 to 65535 seconds. By default, it is 10 seconds.
retransmit *retransmit-interval*	Specifies the interval for retransmitting the LSA packets on an interface.	The value is an integer ranging from 1 to 3600 seconds. By default, it is 5 seconds.
trans-delay *trans-delay-interval*	Specifies the delay for sending LSA packets on an interface.	The value is an integer ranging from 1 to 800 seconds. By default, it is 1 second.
dead *dead-interval*	Specifies the dead interval of the neighbor. This value must be equal to *dead-interval* of the switch that sets up the virtual link with it and must be at least four times that of the *hello-interval*.	The value is an integer ranging from 1 to 65535 seconds. By default, it is 40 seconds.
instance *instance-id*	Specifies the instance ID of the virtual link.	The value is an integer ranging from 0 to 255. By default, it is 0.
authentication-mode	Indicates the authentication mode over the virtual link.	N/A

Parameter	Description	Value
hmac-sha256	Sets the HMAC-SHA256 authentication mode.	N/A
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer ranging from 1 to 65535.
plain	Configures the plaintext password type. Only a plaintext password can be entered, and the password is displayed in plaintext in the configuration file. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	N/A
plain-text	Specifies a plaintext password.	The value is a string of 1 to 255 characters, spaces not supported.
cipher	Configures the ciphertext password type. You can enter either a plaintext or ciphertext password, but the password is displayed in ciphertext in the configuration file.	N/A
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for plaintext passwords and 20 to 392 characters for ciphertext passwords, spaces not supported.

Parameter	Description	Value
keychain	Configures keychain authentication. **NOTE** Before you configure keychain authentication, run the **keychain** command to configure a keychain, the **key-id** command to configure a key ID, the **key-string** command to configure a password, and the **algorithm** command to configure an algorithm. If these commands are not run, OSPFv3 authentication fails.	N/A
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
ipsec sa *sa-name*	Specifies the name of an SA configured for an OSPFv3 virtual link.	The value is an existing SA name.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

You can use the **vlink-peer** command to set up a logical connection for non-backbone area which does not connect to the backbone area directly or discontinuous backbone area.

The virtual link can be regarded as a common interface on which OSPFv3 is enabled, because the principles of **hello**, **retransmit,** and **trans-delay** that are configured on the virtual link are similar.

Example

Create an OSPFv3 virtual link to 10.110.0.3.

```
<HUAWEI> system-view
[HUAWEI] ospfv3 1
```

```
[HUAWEI-ospfv3-1] area 10.0.0.0
[HUAWEI-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

7.5.88 vpn-instance-capability simple (OSPFv3)

Function

The **vpn-instance-capability simple** command disables loop detection and calculates routes directly.

The **undo vpn-instance-capability** command enables the DN-bit check to prevent routing loops.

By default, loop detection is enabled.

Format

vpn-instance-capability simple

undo vpn-instance-capability

Parameters

None

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

If a Multi-VPN-Instance CE (MCE) needs to support the VPN multi-instance, loop detection needs to be disabled. The **vpn-instance-capability simple** command takes effect only in the OSPFv3 VPN instance.

Example

Disable loop detection.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn1] ipv6-family
[HUAWEI-vpn1-af-ipv6] route-distinguisher 100:1
[HUAWEI-vpn1-af-ipv6] quit
[HUAWEI] ospfv3 100 vpn-instance vpn1
[HUAWEI-ospfv3-100] vpn-instance-capability simple
```

7.6 IPv4 IS-IS Configuration Commands

7.6.1 Command Support

Only the following switch models support IPv4 IS-IS:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

7.6.2 adjacency-strict-check enable

Function

The **adjacency-strict-check enable** command enables IS-IS adjacency strict-check.

The **undo adjacency-strict-check enable** command disables IS-IS adjacency strict-check.

The **adjacency-strict-check disable** command disables IS-IS adjacency strict-check.

By default, IS-IS adjacency strict-check is disabled when IS-IS establishes neighbor relationships.

Format

adjacency-strict-check enable

undo adjacency-strict-check [**enable**]

adjacency-strict-check disable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the establishment of IS-IS neighbor relationships, if both IPv4 and IPv6 are configured at both ends, both IPv4 and IPv6 neighbors are established. By default, IPv4 and IPv6 share the standard topology. When the faulty link is restored, IPv4 goes Up faster than IPv6. After the IS-IS router receives a message indicating that IPv4 goes Up, it considers that both IPv4 and IPv6 neighbors are established. If IPv6 packets are being transmitted at that time, some of these IPv6 packets are discarded.

To resolve this problem, run the **adjacency-strict-check enable** command to enable IS-IS adjacency strict-check to ensure that an IS-IS neighbor is established only when both IPv4 and IPv6 go Up.

Prerequisites

You have created an IS-IS process and entered the IS-IS view using the **isis** command.

Configuration Impact

After you run the **adjacency-strict-check enable** command on a broadcast network, the basic topology becomes Down if the IP protocol enabled on the local router is different from that on its neighbors.

After you run the **adjacency-strict-check enable** command on a P2P network, neighbor relationships cannot be established if the IP protocol enabled on the local router is different from that on its neighbors and only the basic topology is available for the local router.

Precautions

undo adjacency-strict-check [**enable**] and **undo adjacency-strict-check** commands have the same function, **enable** is just provide convenience for users.

Example

Enable adjacency strict-check on IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] adjacency-strict-check enable
```

7.6.3 area-authentication-mode

Function

The **area-authentication-mode** command configures an IS-IS area to authenticate received Level-1 packets (LSPs and SNPs) using the specified authentication mode and password or adds authentication information to Level-1 packets to be sent.

The **undo area-authentication-mode** command restores the default configuration.

By default, the system neither encapsulates generated Level-1 packets with authentication information nor authenticates received Level-1 packets.

Format

area-authentication-mode { { **simple** { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } | **md5** { [**cipher**] *plain-cipher-text* | **plain** *plain-text* } } [**ip** | **osi**] | { **keychain** *keychain-name* } } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

area-authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

undo area-authentication-mode

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
simple	Transmits the password in plain text. NOTICE Simple authentication has potential risks. HMAC-SHA256 ciphertext authentication is recommended.	-
plain *plain-text*	Specifies the authentication password in plain text. You can enter only the password in plain text. When you view the configuration file, the password is displayed in plain text. NOTICE If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters.
cipher *plain-cipher-text*	Specifies the authentication password in cipher text. You can enter the password in plain or cipher text. When you view the configuration file, the password is displayed in cipher text. By default, the password is in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters in plain text or a string of 32 or 48 characters in cipher text. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters in plain text or a string of 20 to 392 characters in cipher text.

Parameter	Description	Value
md5	Transmits the password that is encrypted using MD5. **NOTICE** MD5 authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
ip	Indicates the IP authentication password. This parameter cannot be configured when keychain authentication is used.	-
osi	Indicates the OSI authentication password. This parameter cannot be configured when keychain authentication is used. When neither **osi** nor **ip** is specified, the default parameter **osi** is used.	-
keychain *keychain-name*	Indicates the keychain that changes with time and is encrypted using MD5. This parameter takes effect only when *keychain-name* is set using the **keychain** command. Currently, IS-IS supports only HMAC-MD5 and HMAC-SHA256 algorithms.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
snp-packet	Authenticates SNPs.	-
authentication-avoid	Encapsulates generated LSPs but not SNPs with authentication information and authenticates received LSPs but not SNPs.	-
send-only	Encapsulates generated LSPs and SNPs with authentication information, and authenticates received LSPs but not SNPs.	-

Parameter	Description	Value
all-send-only	Encapsulates generated LSPs and SNPs with authentication information, but does not authenticate received LSPs and SNPs.	-
hmac-sha256	Encapsulates generated packets with the HMAC-SHA256 authentication and a password encrypted by the HMAC-SHA256 algorithm and authenticates received packets.	-
key-id *key-id*	Indicates key ID of the HMAC-SHA256 algorithm.	The value is an integer ranging from 0 to 65535.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IS-IS packets to be sent are not encapsulated with authentication information, and the received packets are not authenticated. If a user sends malicious packets to attack a network, information on the entire network may be stolen. Therefore, you can configure IS-IS authentication to improve the network security.

The area authentication password is encapsulated into Level-1 IS-IS packets. Only the packets that pass the area authentication can be accepted. Therefore, you can configure IS-IS area authentication to authenticate the Level-1 area.

Precautions

The **area-authentication-mode** command is valid only on Level-1 or Level-1-2 routers.

By using this command enables IS-IS to discard all the Level-1 LSPs and SNPs whose area authentication passwords are not consistent with the one set by this command. At the same time, IS-IS inserts the configured area authentication password into all the Level-1 routing packets (LSPs and SNPs) sent from the local node. The establishment of the Level-1 neighbor relationship is not affected, regardless of whether the packets pass the area authentication.

The authentication takes effect only on the peer configured with authentication. The peer with no authentication configured can still receive the LSP and SNP packet with the password.

Example

Set the area authentication mode to keychain and keychain name to **test**.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] area-authentication-mode keychain test
```

7.6.4 attached-bit advertise

Function

The **attached-bit advertise** command configures a rule for setting the ATT bit in Link state Protocol Data Units (LSPs).

The **undo attached-bit advertise** command restores the default setting rule.

By default, the Level-1-2 device sets the ATT bit in LSPs using the default rule.

Format

attached-bit advertise { **always** | **never** }

undo attached-bit advertise

Parameters

Parameter	Description	Value
always	Indicates that the ATT bit is set to 1.	-
never	Indicates that the ATT bit is set to 0.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ATT bit is a field in link state packets. An ATT bit identifies whether Level-1 area is attached to other areas. A Level-1-2 device sets the ATT bit to 1 to notify the devices in Level-1 area of its attachment to a Level-2 backbone area. After a Level-1 device receives the LSPs carrying the ATT bit 1 from the Level-1-2 device, the Level-1 device generates a route with the same destination address as the default route of the Level-1-2 device. Traffic can be forwarded along this route.

The preceding rule is the default rule for setting the ATT bit in the Intermediate System to Intermediate System (IS-IS) protocol. You can run the **attached-bit advertise** command to configure a rule for setting the ATT bit as required.

- If you want the ATT bit in LSPs to be set to 1, run the **attached-bit advertise always** command.
- If you want to disable the Level-1 device connected to the Level-1-2 device from advertising default routes when the ATT bit is set to 1, run either of the following commands:
  - Run the **attached-bit advertise never** command on the Level-1-2 device to disable the device from sending LSPs with the ATT bit 1.
  - Run the **attached-bit avoid-learning** command on the Level-1 device that is connected to the Level-1-2 device.

  Running the **attached-bit advertise never** command applies to all Level-1 devices that receive LSPs with the ATT bit 0. Therefore, it is more convenient.

Precautions

The ATT bit is defined in both Level-1 and Level-2 LSPs, but it can be set to 1 only in Level-1 LSPs. Additionally, only the Level-1-2 device can set the ATT bit. Therefore, running the **attached-bit avoid-learning** command takes effect only on the Level-1-2 device.

Example

Enable the Level-1-2 device to set the ATT bit to 1 in the LSPs sent in IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] attached-bit advertise always
```

7.6.5 attached-bit avoid-learning

Function

The **attached-bit avoid-learning** command disables a device from advertising default routes to a routing table when the ATT bit is set to 1.

The **undo attached-bit avoid-learning** command restores the device to generate default routes when the ATT bit is set to 1.

By default, a device advertises default routes when the ATT bit is set to 1.

Format

attached-bit avoid-learning

undo attached-bit avoid-learning

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

An ATT bit is a field in link state packets. An ATT bit identifies whether Level-1 area is attached to other areas. A Level-1-2 device sets the ATT bit to 1 to notify the devices in Level-1 area of its attachment to a Level-2 backbone area. After a Level-1 device receives the LSPs carrying the ATT bit 1 from the Level-1-2 device, the Level-1 device generates a route with the same destination address as the default route of the Level-1-2 device. Traffic can be forwarded along this route.

To prevent the Level-1 device from advertising the default route when the ATT bit is set to 1, run the **attached-bit avoid-learning** command.

To prevent the Level-1 device from advertising default routes to the routing table, run either of the following commands:

- Run the **attached-bit advertise never** command on the Level-1-2 device to disable the device from sending LSPs with the ATT bit 1.
- Run the **attached-bit avoid-learning** command on the Level-1 device that is connected to the Level-1-2 device.

The difference between the preceding commands lies in that the **attached-bit avoid-learning** command applies to a specified device.

Example

Disable IS-IS-enabled device from advertising default routes to a routing table when the ATT bit is set to 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] attached-bit avoid-learning
```

7.6.6 auto-cost enable

Function

The **auto-cost enable** command enables IS-IS to automatically calculate the interface cost based on the interface bandwidth.

The **undo auto-cost enable** command disables IS-IS from automatically calculating the interface cost based on the interface bandwidth.

By default, IS-IS is disabled from automatically calculating the interface cost based on the interface bandwidth.

Format

auto-cost enable [**compatible**]

undo auto-cost enable

Parameters

Parameter	Description	Value
compatible	Specifies the IS-IS to calculate the cost of an interface based on the bandwidth of the interface automatically in compatible.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is run, if the cost of an IS-IS interface is not set in the interface view and no cost is set in the IS-IS view, the system automatically calculates a cost for the interface.

If the cost style of the system is wide or wide-compatible:

When **auto-cost enable** command is configured, Interface cost = (Bandwidth-reference/Link-bandwidth) x 10.

The cost style is set by the **cost-style** command. The Bandwidth-reference is set by the **bandwidth-reference** command. The Link-bandwidth is the interface bandwidth.

If the cost style of the system is narrow, narrow-compatible or compatible, the cost of each interface is based on the following table.

Table 7-87 Relationship between the IS-IS interface cost and the bandwidth

Cost	Range of the Interface Bandwidth
60	Interface bandwidth =< 10 Mbit/s
50	10 Mbit/s < Interface bandwidth ≤ 100 Mbit/s
40	100 Mbit/s < Interface bandwidth ≤ 155 Mbit/s
30	155 Mbit/s < Interface bandwidth ≤ 622 Mbit/s

Cost	Range of the Interface Bandwidth
20	622 Mbit/s < Interface bandwidth ≤ 2.5 Gbit/s
10	2.5 Gbit/s < Interface bandwidth

Precautions

The priority of the cost value of the global configured by the **circuit-cost** command is higher than the auto cost value.

The **auto-cost enable** command cannot change the cost of the loopback interface.

Example

Enable IS-IS to automatically calculate the interface cost.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] auto-cost enable
```

7.6.7 bandwidth-reference (IS-IS)

Function

The **bandwidth-reference** command sets the bandwidth reference value that is used in automatic IS-IS interface cost calculation.

The **undo bandwidth-reference** command restores the default bandwidth reference value that is used in automatic IS-IS interface cost calculation.

By default, the bandwidth reference value is 100 Mbit/s.

Format

bandwidth-reference *value*

undo bandwidth-reference

Parameters

Parameter	Description	Value
value	Specifies the bandwidth reference value used in automatic IS-IS interface cost calculation.	The value is an integer that ranges from 1 to 2147483648, in Mbit/s.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the set link cost of IS-IS routes reflect the actual link cost, configure a proper link cost for all interfaces or enable automatic interface cost calculation. To enable automatic interface cost calculation, set a proper bandwidth reference value.

You can run the **bandwidth-reference** command to set a proper bandwidth reference value. After automatic interface cost calculation is enabled, and the cost type is wide or wide-compatible, the system calculates the cost of each interface with the following formula: Interface cost = (Bandwidth-reference/Interface bandwidth) x 10. If the interface cost calculated through this formula is greater than 16777214, 16777214 is used as the interface cost for route calculation. That is, the interface cost will never be greater than 16777214.

The **bandwidth** *bandwidth* command can only set an interface bandwidth obtained by the NMS from the MIB. It cannot change an interface actual bandwidth and interface cost.

After the **auto-cost enable** command enables automatic IS-IS interface cost calculation, the system automatically calculates the interface cost based on the bandwidth reference value set using the **bandwidth-reference** command.

The **bandwidth-reference** command can be operated on Eth-Trunk interfaces as same with on physical interfaces. If the command is run on an Eth-Trunk interface, the bandwidth of the Eth-Trunk interface is equal to the total bandwidth of all its member interfaces.

Precautions

Rules for automatically calculating the IS-IS interface cost vary according to the cost style of the IS-IS interface:

- The bandwidth reference value set using the **bandwidth-reference** command takes effect only when the cost style is wide or wide-compatible. In this case, the interface cost is calculated using the following formula:

  Interface cost = (Bandwidth-reference/Interface bandwidth) × 10.
- If the cost style of the system is narrow, narrow-compatible or compatible, the cost of each interface is based on the following table.

Table 7-88 Relationship between the IS-IS interface cost and the bandwidth

Cost	Range of the Interface Bandwidth
60	Interface bandwidth =< 10 Mbit/s
50	10 Mbit/s < Interface bandwidth =< 100 Mbit/s

Cost	Range of the Interface Bandwidth
40	100 Mbit/s < Interface bandwidth =< 155 Mbit/s
30	155 Mbit/s < Interface bandwidth =< 622 Mbit/s
20	622 Mbit/s < Interface bandwidth =< 2.5 Gbit/s
10	2.5 Gbit/s < Interface bandwidth

Example

Set the reference value of the system bandwidth to 1000 Mbit/s.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] bandwidth-reference 1000
```

7.6.8 bfd all-interfaces (IS-IS)

Function

The **bfd all-interfaces** command sets values for BFD session parameters used in BFD for IS-IS.

The **undo bfd all-interfaces** command restores the default values of BFD session parameters used in BFD for IS-IS.

By default, the minimum intervals for receiving and sending BFD packets are 1000 ms and the detection time multiplier is 3.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } *

undo bfd all-interfaces { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } *

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Specifies the minimum interval for receiving BFD packets from the peer end. The interval for receiving BFD packets between determines the BFD session detection time. On an unstable link, a smaller receive interval may result in BFD session flapping. To prevent BFD session flapping, increase the receive interval.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *transmit-interval*	Specifies the minimum interval for transmitting BFD packets to the peer end. The interval for transmitting BFD packets determines the BFD session detection time. On a stable link, you can increase the transmit interval to prevent frequent link status detection.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Specifies the local detection multiplier. On a stable link, you can increase the BFD detection multiplier to prevent frequent link status detection.	The value is an integer that ranges from 3 to 50. The default value is 3.

Parameter	Description	Value
frr-binding	Binds the BFD session status to IS-IS Auto FRR. When BFD detects a link fault on an interface, the BFD session goes Down, triggering FRR on the interface. Then traffic is switched from the faulty link to the backup link to ensure traffic forwarding.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the establishment of a BFD session, you can adjust the interval for transmitting BFD packets, interval for receiving BFD packets, and local detection multiplier according to network and performance requirements.

Precautions

The value of *receive-interval* is obtained by negotiating the local **min-rx-interval** value and the remote **min-tx-interval** value. If a router does not receive any BFD packet from its peer in the *receive-interval* × *multiplier-value* period, the router advertises that its peer is Down.

If only parameters of a BFD session are set but the **bfd all-interfaces enable** command is not used, the BFD session cannot be set up.

NOTE

The BFD priority of the interface is higher than the BFD priority of the process. If BFD of the interface is enabled, the BFD session is set up based on the BFD parameters on the interface.

Example

Enable BFD in an IS-IS process and set the minimum interval for transmitting BFD packets to 600 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] isis
[HUAWEI-isis-1] bfd all-interfaces enable
[HUAWEI-isis-1] bfd all-interfaces min-tx-interval 600
```

7.6.9 bfd all-interfaces enable

Function

The **bfd all-interfaces enable** command enables BFD in an IS-IS process.

The **undo bfd all-interfaces enable** command disables BFD in an IS-IS process.

By default, BFD is disabled in an IS-IS process.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

bfd all-interfaces enable

undo bfd all-interfaces enable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If global BFD is not enabled, you can configure IS-IS BFD but cannot set up the BFD session. Before establishing BFD sessions, you need to enable BFD on the two ends.

Precautions

When BFD is enabled in the process using the **bfd all-interfaces enable** command, the interface does not set up a BFD session in the following cases:

- The **isis bfd block** command is used on the interface. The command suppresses the BFD capability of the interface. To set up a session on the interface, run the **undo isis bfd block** command.
- When the **isis bfd static** command is used on the interface, the interface does not set up the BFD session. To set up a session on the interface, run the **undo isis bfd static** command.

NOTE

The BFD priority of the interface is higher than the BFD priority of the process. If BFD of the interface is enabled, a BFD session is set up based on the BFD parameters on the interface.

Example

Enable BFD in an IS-IS process.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] isis
[HUAWEI-isis-1] bfd all-interfaces enable
```

7.6.10 circuit-cost

Function

The **circuit-cost** command sets the link cost for all IS-IS interfaces during SPF calculation.

The **undo circuit-cost** command deletes the configured link cost of all IS-IS interfaces.

By default, no link cost is set for IS-IS interfaces.

Format

circuit-cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo circuit-cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the interface cost used in SPF calculation.	If the IS-IS cost style is wide or wide-compatible, the cost of imported routes ranges from 1 to 1677721416777214; otherwise, the cost ranges from 1 to 63.
maximum	Sets the link cost of IS-IS interfaces to 16777215. **NOTE** You can configure this parameter only when the IS-IS cost style is wide or wide-compatible. After the interface cost is set to 16777215, the neighbor TLV generated on the link can only be used to transmit TE information but cannot be used for route calculation.	-
level-1	Specifies the link cost for all Level-1 interfaces. If no level is specified, the link cost is set for Level-1-2 interfaces.	-

Parameter	Description	Value
level-2	Specifies the link cost for all Level-2 interfaces. If no level is specified, the link cost is set for Level-1-2 interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large network, there are often multiple valid routes to the same destination. IS-IS can use the SPF algorithm to calculate the optimal route to forward traffic. This may cause the following problems:

- All traffic is forwarded along the optimal path, resulting in load unbalance.
- If the optimal path is intermittently disconnected, traffic is still forwarded along the optimal path, resulting in traffic loss.

To solve the preceding problems, run the **circuit-cost** command to change the cost of all IS-IS interfaces so that traffic can be forwarded along different physical links.

Precautions

The **isis cost** command takes precedence over the **circuit-cost** command. The **circuit-cost** command cannot change the cost of loopback interfaces.

Changing the link cost of interfaces will cause routes of the entire network to be recalculated and change the forwarding path of traffic.

Example

Set the default cost of all Level-1-2 interfaces to 30.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] circuit-cost 30
```

Set the link cost of all IS-IS interfaces to 16777215.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] circuit-cost maximum
```

7.6.11 circuit default-tag

Function

The **circuit default-tag** command sets the administrative tag value for all interfaces in an IS-IS process.

The **undo circuit default-tag** command restores the default administrative tag value for all interfaces in an IS-IS process.

By default, the administrative tag value of all IS-IS interfaces is 0.

Format

circuit default-tag *tag* [**level-1** | **level-2**]

undo circuit default-tag [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag value for all interfaces in an IS-IS process.	The value is an integer that ranges from 1 to 4294967295.
level-1	Specifies the administrative tag value for all Level-1 interfaces in an IS-IS process. If no interface level is specified, the administrative tag values of Level-1 and Level-2 interfaces are set.	-
level-2	Specifies the administrative tag value for all Level-2 interfaces in an IS-IS process. If no interface level is specified, the administrative tag values of Level-1 and Level-2 interfaces are set.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrative tag carries management information about IP address prefixes to control the import of routes of different levels and areas. You can use the administrative tag to control the advertisement of IP address prefixes in an IS-IS routing domain to simplify route management.

The **circuit default-tag** command allows you to set the administrative tag value for all routes in an IS-IS process. You can filter routes based on the configured administrative tag value.

The administrative tag for an interface is advertised along with routing information.

- When the cost style of IS-IS is narrow or narrow-compatible, the administrative tag value is neither advertised nor takes effect in the LSP.
- When the cost style of IS-IS is wide, wide-compatible, or compatible, the administrative tag value is advertised in the LSP.

Precautions

The value of the administrative tag configured through the**circuit default-tag** command is the global administrative tag. The priority of the interface administrative tag configured by the **isis tag-value** command is higher than the priority of the global administrative tag.

Example

Set the administrative tag value of Level-1 interfaces to 30.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] circuit default-tag 30 level-1
```

7.6.12 cost-style

Function

The **cost-style** command sets the cost style of routes received and sent by an IS-IS device.

The **undo cost-style** command restores the default cost style of routes received and sent by an IS-IS device.

By default, the cost style of routes received and sent by an IS-IS device is narrow.

Format

cost-style { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

Parameters

Parameter	Description	Value
narrow	Configures an IS-IS device to receive and send only routes with cost style narrow. When the cost style is narrow, the cost of routes ranges from 1 to 63.	-
wide	Configures an IS-IS device to receive and send only routes with cost style wide. When the cost style is wide, the cost of routes ranges from 1 to 16777215.	-
wide-compatible	Configures an IS-IS device to receive routes with cost style narrow or wide and sent only routes with cost style wide.	-
compatible	Configures an IS-IS device to receive and send routes with cost style narrow or wide.	-

Parameter	Description	Value
narrow-compatible	Configures an IS-IS device to receive routes with cost style narrow or wide and sent only routes with cost style narrow.	-
relax-spf-limit	Configures an IS-IS device to receive routes with cost higher than 1023. If this parameter is specified, there is no restriction on the link costs of interfaces or route costs. The cost of a received route is the actual cost. If this parameter is not specified, the following situations occur: ● If the cost of a route is smaller than or equal to 1023, and the link cost of each interface through which the route passes is smaller than or equal to 63: The cost of the route is the sum of link costs of all interfaces through which the route passes. ● If the cost of a route is smaller than or equal to 1023, and the link costs of certain interfaces through which the route passes are larger than 63: An IS-IS device can learn only the routes imported by the interfaces and direct routes of the network segment where the interfaces reside. The costs of these routes are the actual cost. ● If the cost of a route is larger than 1023: The device can receive only the routes of the network segment where the interface with link cost smaller than 1023 resides. If the cost of a route is larger than 1023, the cost is calculated as 1023.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the cost style of IS-IS routes is narrow, indicating that only routes with the cost ranging from 1 to 63 can be received and sent. LSPs carrying tag information to be filtered by a routing policy cannot be flooded when the cost style is narrow. The **cost-style** command can be used to change the cost style of IS-IS routes so that they can be transmitted successfully.

To implement extended IS-IS functions, setting the cost style of IS-IS routes to **wide** is recommended.

Precautions

When the cost style of a route is changed from wide to narrow, transmission of the route may be interrupted.

If you want to change the cost style of IS-IS routes, running the command while configuring basic IS-IS functions is recommended. If the cost style of IS-IS routes is changed during network operation, the IS-IS process is restarted and neighbors are disconnected.

Example

Configure an IS-IS device to send only the packets with cost style narrow and to receive the packets with cost style narrow or wide.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] cost-style narrow-compatible
```

7.6.13 default-route-advertise (IS-IS)

Function

The **default-route-advertise** command configures IS-IS devices to generate default routes.

The **undo default-route-advertise** command disables IS-IS devices from generating default routes.

By default, IS-IS devices do not generate default routes.

Format

default-route-advertise [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost* | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] * [**avoid-learning**]

undo default-route-advertise

Parameters

Parameter	Description	Value
always	Configures an IS-IS device to unconditionally advertise default routes with itself as the next hop.	-
match default	Advertises a default route through an LSP if the default route is generated by other routing protocols or other IS-IS processes in the routing table. If this default route is deleted from the routing table, it is not advertised through an LSP.	-

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy. A Level-1-2 device advertises default routes to the IS-IS routing domain only when there are external routes matching the route-policy in the routing table of the device. This prevents routing blackhole when link faults make some important external routes unavailable but default routes are still advertised. This route-policy does not affect external route import in IS-IS.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cost *cost*	Specifies the cost of default routes.	The value is an integer. The value range varies according to the cost style. When the cost style is narrow, narrow-compatible, or compatible, the value ranges from 0 to 63. When the cost style is wide or wide-compatible, the value ranges from 0 to 4261412864.
tag *tag*	Specifies the tag value of advertised default routes. Advertised LSPs carry the tag value only when the IS-IS cost style is wide, wide-compatible, or compatible.	The value is an integer that ranges from 1 to 4294967295.
level-1	Sets the level of default routes to Level-1. If no level is specified, Level-2 default routes are generated by default.	-
level-2	Sets the level of default routes to Level-2. If no level is specified, Level-2 default routes are generated by default.	-
level-1-2	Sets the level of default routes to Level-1-2. If no level is specified, Level-2 default routes are generated by default.	-
avoid-learning	Prevents an IS-IS process from learning default routes or adding them to the routing table. If existing default routes in the routing table are active, set the default route that needs to be added to the routing table to inactive.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IS-IS and other routing protocols are running on a network, use either of the following methods to allow the traffic within the IS-IS domain to be transmitted to other routing domains:

- Configure a boundary router in the IS-IS domain to advertise default routes to the IS-IS domain.
- Configure a boundary router in the IS-IS domain to import routes from the other routing domains to the IS-IS domain.

The first method is simpler, because the routers in the IS-IS domain do not need to learn routes imported form the other routing protocols.

Precautions

You can specify **always** to allow default routes to be advertised unconditionally; in this case, the device still calculates default routes from other devices.

NOTE

If **always** is configured on multiple devices within the same area, a routing loop may occur.

After this command is run on an IS-IS router, all traffic in an IS-IS domain will be forwarded by this IS-IS router to a destination outside the domain. Compared with configuring a static default route on each router in an IS-IS domain, running this command simplifies configurations, because this command only needs to be run on a boundary router in the IS-IS domain. In addition, you can specify different parameters to allow default routes to be advertised in different ways.

If this command is run on a Level-1 router, the router advertises default routes only to the Level-1 area.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, an ABR advertises the default route to the IS-IS domain as long as the local routing table contains external routes.

Example

Configure the current IS-IS device to advertise the IPv4 default routes that match route-policy **filter** and set the cost of these default routes to 15.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] default-route-advertise route-policy filter cost 15
```

7.6.14 description (IS-IS)

Function

The **description** command configures a description for an IS-IS process.

The **undo description** command deletes the description of an IS-IS process.

By default, no description is configured for an IS-IS process.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Configures a description for an IS-IS process.	The value is a string of 1 to 80 case-sensitive characters. Spaces are supported.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring descriptions for IS-IS processes helps identify and maintain IS-IS processes.

IS-IS process description that is configured through the **description** command is not advertised in an LSP.

IS-IS process description that is configured through the **is-name** command is advertised in an LSP.

Precautions

If you run the **description** command multiple times, only the latest configuration takes effect.

Example

Configure description for IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
```

```
[HUAWEI-isis-1] description this process configure the area-authentication-mode
```

7.6.15 display default-parameter isis

Function

The **display default-parameter isis** command displays the default IS-IS configuration.

Format

display default-parameter isis

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display default-parameter isis** command to check the default IS-IS configuration in IS-IS initialization.

Example

Display the default IS-IS configuration.

```
<HUAWEI> display default-parameter isis

                        Default Configurations For Process
                        ----------------------------------
   Cost-Style                          : Narrow
   Circuit-Cost <IPv4>                 : L1 10 L2 10
   Circuit-Cost <IPv6>                 : L1 10 L2 10
   IS-Level                            : L12
   LSP-Originate-Length                : 1497
   LSP-Receive-Length                  : 1497
   LSP-Max-Age <s>                     : 1200
   LSP-Generation-IntelliTimer <s,ms,ms> : L1 Max 2 Init 0 Incr 0
                                         L2 Max 2 Init 0 Incr 0
   LSP-Refresh-Interval <s>            : 900
   Preference                          : IPv4 15 IPv6 15
   SPF-IntelliTimer <s,ms,ms>          : Max 5 Init 50 Incr 200

                      Default Configurations For Interfaces
                      -------------------------------------
   Circuit-Level                       : L12
   CSNP-Interval <s>                   : L1 10 L2 10
   Cost <IPv4>                         : L1 10 L2 10
   Cost <IPv6>                         : L1 10 L2 10
   DIS-Priority                        : L1 64 L2 64
   Hello-Interval <s>                  : L1 10 L2 10
```

```
 Holding-Multiplier                  : L1 3 L2 3
 LSP-Retransmit <s>                  : 5
 LSP-Throttle <ms>                   : 50 count 10
 PPP-Negotiation                     : 3-Way
 Peer Suppress-Flapping <s>            : Detect-Interval 60
                                   Resume-Interval 120
                                   Threshold       10
```

Table 7-89 Description of the display default-parameter isis command output

Item	Description
Default Configurations For Process	Default configuration of an IS-IS process.
Cost-Style	IS-IS cost style: ● narrow ● wide ● wide-compatible ● compatible ● narrow-compatible To set the IS-IS cost style, run the **cost-style** command.
Circuit-Cost <IPv4>	Cost of all IS-IS IPv4 interfaces. To set the cost of IS-IS IPv4 interfaces, run the **circuit-cost** command.
Circuit-Cost <IPv6>	Cost of all IS-IS IPv6 interfaces. To set the cost of IS-IS IPv6 interfaces, run the **ipv6 circuit-cost** command.
IS-Level	Level of an IS-IS device: ● L1: Level-1 device ● L2: Level-2 device ● L12: Level-1-2 device To set the level of an IS-IS device, run the **is-level** command.
LSP-Originate-Length	Maximum length of an LSP generated by IS-IS. To set the maximum length of an LSP generated by IS-IS, run the **lsp-length** command.
LSP-Receive-Length	Maximum length of an LSP received by IS-IS. To set the maximum length of an LSP received by IS-IS, run the **lsp-length** command.

Item	Description
LSP-Max-Age <s>	Maximum lifetime of an LSP generated by an IS-IS process, in seconds. To set the maximum lifetime of an LSP generated by an IS-IS process, run the **timer lsp-max-age** command.
LSP-Generation-IntelliTimer <s,ms,ms>	Delay in generating LSPs: ● L1: delay for a Level-1 router to generate LSPs ● L2: delay for a Level-2 router to generate LSPs ● Max: maximum delay in generating LSPs, in seconds ● Init: initial delay in generating LSPs, in milliseconds ● Incr: incremental delay in generating LSPs, in milliseconds To set the delay in generating LSPs, run the **timer lsp-generation** command.
LSP-Refresh-Interval <s>	Interval for refreshing LSPs, in seconds. To set the interval for refreshing LSPs, run the **timer lsp-refresh** command.
Preference	Protocol preference of IS-IS routes. To set the protocol preference of IS-IS routes, run the **preference** command.
SPF-IntelliTimer <s,ms,ms>	Delay in SPF calculation: ● Max: maximum delay in SPF calculation, in seconds ● Init: initial delay in SPF calculation, in milliseconds ● Incr: incremental delay in SPF calculation, in milliseconds To set the delay in SPF calculation, run the **timer spf** command.
Default Configurations For Interfaces	Default configuration of IS-IS interfaces.
Circuit-Level	IS-IS interface level. To set the IS-IS interface level, run the **isis circuit-level** command.
CSNP-Interval <s>	Interval for sending CSNPs, in seconds. To set the interval for sending CSNPs, run the **isis timer csnp** command.

Item	Description
Cost <IPv4>	Cost of IS-IS interfaces in an IPv4 topology. To set the cost of IS-IS interfaces in an IPv4 topology, run the **isis cost** command.
Cost <IPv6>	Cost of IS-IS interfaces in an IPv6 topology. To set the cost of IS-IS interfaces in an IPv6 topology, run the **isis ipv6 cost** command.
DIS-Priority	Priority for DIS election. To set the priority for DIS election, run the **isis dis-priority** command.
Hello-Interval <s>	Interval for sending Hello packets, in seconds. To set the interval for sending Hello packets, run the **isis timer hello** command.
Holding-Multiplier	Number of consecutive Hello packets that are not received before the neighbor is declared Down. To set this value, run the **isis timer holding-multiplier** command.
LSP-Retransmit <s>	Interval for retransmitting LSPs on a P2P link, in seconds. To set the retransmit interval, run the **isis timer lsp-retransmit** command.
LSP-Throttle <ms>	Interval for sending LSPs or CSNPs, in milliseconds, and number of LSPs or CSNPs that are sent each time. To set the two values, run the **isis timer lsp-throttle** command.
PPP-Negotiation	PPP negotiation type during the establishment of IS-IS adjacencies: ● 2-way ● 3-way ● only To set the PPP negotiation type during the establishment of IS-IS adjacencies, run the **isis ppp-negotiation** command.

Item	Description
Peer Suppress-Flapping <s>	Detection parameters for IS-IS neighbor relationship flapping suppression on an interface: ● Detect-Interval: detection interval of IS-IS neighbor relationship flapping suppression ● Resume-Interval: interval for exiting from IS-IS neighbor relationship flapping suppression ● Threshold: threshold of IS-IS neighbor relationship flapping suppression

7.6.16 display isis cost interface

Function

The **display isis cost interface** command displays costs of an interface and how they are generated.

Format

display isis cost interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis cost interface** command to check costs of an IS-IS interface, including the link cost and route prefix cost that the interface uses in each topology, and how the costs are generated.

Example

Display costs of VLANIF 100 and how they are generated.

```
<HUAWEI> display isis cost interface vlanif 100
Interface: Vlanif 100
                            Level-2 interface cost
 Topology base(0):
  Link effective cost: 10(A)                          enabled by circuit cost
  IP prefix effective cost:
   10.10.7.0/24                    cost: 10           enabled by circuit cost
   10.10.8.0/24                    cost: 10           enabled by circuit cost
   10.10.9.0/24                    cost: 10           enabled by circuit cost
 Topology red(7):
  Link effective cost: 87(A)                          enabled by circuit cost
  IP prefix effective cost:
   10.10.7.0/24                    cost: 87           enabled by circuit cost
   10.10.8.0/24                    cost: 87           enabled by circuit cost
   10.10.9.0/24                    cost: 87           enabled by circuit cost

                   Flags: R-Relative cost  A-Absolute cost
```

Table 7-90 Description of the **display isis cost interface** command output

Item	Description
Interface	Type and ID of an interface on which IS-IS is enabled
Link effective cost	Link cost
IP prefix effective cost	Cost of an IPv4 route
cost	Interface cost
enabled by circuit cost	Default cost or cost configured in the **isis cost** command
enabled by auto cost	Cost configured in the **auto-cost enable** command
enabled by global cost	Cost configured in the **circuit cost** command
enabled by igp ldp	The interface cost is configured by LDP
enabled by rui cost	Cost that inherits the cost of the RUI route
enabled by silent cost	Cost configured in the **isis silent** command in the interface view
enabled by tunnel cost	Cost generated after the TE Tunnel is configured
IPv6 prefix effective cost	Cost of an IPv6 route
Flags	Cost flag ● R-Relative cost: relative cost ● A-Absolute cost: absolute cost

7.6.17 display isis bfd interface

Function

The **display isis bfd interface** command displays information about BFD-enabled IS-IS interfaces.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display isis [*process-id*] **bfd interface**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

BFD can provide millisecond-level fault detection. It can work with IS-IS to fast detect faults on neighboring devices and instruct IS-IS to recalculate routes for correct packet forwarding. You can run the **display isis bfd interface** command to check information about BFD-enabled IS-IS interfaces.

Example

Display information about BFD-enabled IS-IS interfaces.

```
<HUAWEI> display isis 1 bfd interface

                    BFD information of interface for ISIS(1)
                   -----------------------------------------
 Interface                  BFD.State      Min-Tx       Min-Rx        Mul
 Vlanif101                   enable         1000         1000         3
 Total interfaces: 1                       Total bfd enabled interfaces: 1
```

Table 7-91 Description of the display isis bfd interface command output

Item	Description
Interface	BFD-enabled IS-IS interface. To enable BFD on an IS-IS interface, run the **bfd all-interfaces enable** or **isis bfd enable** command.
BFD.State	BFD status on the IS-IS interface: ● enable: BFD is enabled on the interface. ● disable: BFD is disabled on the interface. To enable BFD on an IS-IS interface, run the **bfd all-interfaces enable** or **isis bfd enable** command.
Min-Tx	Minimum interval for transmitting BFD packets. To set the minimum interval, run the **bfd all-interfaces** or **isis bfd** command.
Min-Rx	Minimum interval for receiving BFD packets. To set the minimum interval, run the **bfd all-interfaces** or **isis bfd** command.
Mul	Local detection multiplier. To set the local detection multiplier, run the **bfd all-interfaces** or **isis bfd** command.

7.6.18 display isis bfd session

Function

The **display isis bfd session** command displays information about dynamic BFD sessions.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display isis [*process-id* | **vpn-instance** *vpn-instance-name*] **bfd session** { **all** | **peer** *ip-address* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.
all	Specifies all IS-IS interfaces in the IS-IS process.	-
peer *ip-address*	Specifies the IP address of a neighbor.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the interface on which BFD session statistics need to be collected.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

BFD can provide millisecond-level fault detection. It can work with IS-IS to fast detect faults on neighboring devices and instruct IS-IS to recalculate routes for correct packet forwarding. You can run the **display isis bfd session** command to check information about dynamic BFD sessions.

Example

Display information about dynamic BFD sessions.

```
<HUAWEI> display isis bfd session all
                    BFD session information for ISIS(1)
                    -----------------------------------
Peer System ID : 0000.0000.0002          Interface : Vlanif10
TX : 1000          BFD State : up        Peer IP Address : 10.1.1.2
RX : 1000          LocDis : 8194         Local IP Address: 10.1.1.1
Multiplier : 3     RemDis : 8197          Type : L1
Diag : No diagnostic information
Total BFD session(s) : 1
```

Table 7-92 Description of the display isis bfd session all command output

Item	Description
Peer System ID	System ID of the neighbor.

Item	Description
Interface	Local IS-IS interface connected to the neighbor.
TX	Negotiated minimum interval for transmitting BFD packets.
BFD State	BFD session status: Up or Down.
Peer IP Address	IP address of the remote IS-IS interface.
RX	Negotiated minimum interval for receiving BFD packets.
LocDis	Local discriminator dynamically assigned by BFD.
Local IP Address	IP address of the local IS-IS interface.
Multiplier	Remote detection multiplier.
RemDis	Remote identifier dynamically assigned by BFD.
Type	Level of the neighbor: ● L1: Level-1 ● L2: Level-2 ● L1L2: Level-1-2
Diag	Diagnostic information. "No diagnostic information" indicates that BFD runs properly and no diagnostic information is displayed.
Total BFD session (s)	Total number of BFD sessions.

7.6.19 display isis brief

Function

The **display isis brief** command displays brief information about IS-IS.

Format

display isis brief [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis [*process-id*] **brief**

Parameters

Parameter	Description	Value
process-id	Display brief information about a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Display brief information about the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis brief** command to check brief information about IS-IS.

Example

Display brief information about IS-IS.

```
<HUAWEI> display isis brief

                   ISIS Protocol Information for ISIS(1)
                   ------------------------------------
SystemId: 0000.0000.0001      System Level: L1
Area-Authentication-mode: NULL
Domain-Authentication-mode: NULL
Ipv6 is not enabled
ISIS is in starting status
ISIS is in protocol hot standby state: Real-Time Backup
Flush Protect Mode: False

Interface: (Vlanif10)
Cost: L1 10        L2 10               Ipv6 Cost: L1 10   L2 10
State: IPV4 Down                        IPV6 Down
Type: BROADCAST                           MTU: 1497
Priority: L1 64   L2 64
Timers:     Csnp: L1 10    L2 10    ,Retransmit: L12 5   , Hello: L1 10 L2 10  ,

Hello Multiplier: L1 3    L2 3     , LSP-Throttle Timer: L12 50
```

Table 7-93 Description of the display isis brief command output

Item	Description
ISIS Protocol Information for ISIS(1)	Information about IS-IS process 1. To create an IS-IS process, run the **isis** command.

Item	Description
SystemId	System ID of the current IS-IS device. To set the system ID, run the **network-entity** command.
System Level	Level of an IS-IS device: - L1: Level-1 - L2: Level-2 - L12: Level-1-2 To set the level of an IS-IS device, run the **is-level** command.
Area-Authentication-mode	IS-IS area authentication mode. To set the IS-IS area authentication mode and password, run the **area-authentication-mode** command.
Domain-Authentication-mode	IS-IS routing domain authentication mode. To set the IS-IS domain authentication mode and password, run the **domain-authentication-mode** command.
Ipv6 is not enabled	IPv6 is not enabled in the IS-IS process.
ISIS is in starting status	IS-IS is running.
ISIS is in protocol hot standby state: Real-Time Backup	IS-IS hot standby is real-time backup.
Flush Protect Mode	Indicates whether the process works in purge LSP protection mode.
Interface	Interface on which IS-IS is enabled. To enable IS-IS on an interface, run the **isis enable** command.
Cost	Cost of IS-IS IPv4 interfaces. To set the cost of IS-IS IPv4 interfaces, run the **circuit-cost** or **isis cost** command.
Ipv6 Cost	Cost of IS-IS IPv6 interfaces. To set the cost of IS-IS IPv6 interfaces, run the **ipv6 circuit-cost** or **isis ipv6 cost** command.
State	Status of the IS-IS interface.
Type	Network type of the IS-IS interface: P2P or broadcast. To set the network type of an IS-IS interface, run the **isis circuit-type** command.
MTU	MTU of the IS-IS interface.

Item	Description
Priority	Priority of the IS-IS interface. **NOTE** When the current interface is a virtual link interface, the priority field is not displayed.
Timers	IS-IS timer.
Csnp	Interval for sending CSNPs. To set the interval for sending CSNPs, run the **isis timer csnp** command.
Retransmit	Interval for retransmitting LSPs on a P2P link. To set the retransmit interval, run the **isis timer lsp-retransmit** command.
Hello	Interval for sending Hello packets. To set the interval for sending Hello packets, run the **isis timer hello** command.
Hello Multiplier	Number of consecutive Hello packets that are not received before the neighbor is declared Down. To set this value, run the **isis timer holding-multiplier** command.
LSP-Throttle Timer	Interval for sending LSPs or CSNPs and number of LSPs or CSNPs that are sent each time. To set the two values, run the **isis timer lsp-throttle** command.

7.6.20 display isis debug-switches

Function

The **display isis debug-switches** command displays the current IS-IS debugging status.

Format

display isis debug-switches [*process-id*]

display isis [*process-id*] **debug-switches**

Parameters

Parameter	Description	Value
process-id	Displays the current status of IS-IS debugging of specified IS-IS process ID. If *process-id* is not specified, display the current status of IS-IS debugging of all IS-IS process.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no IS-IS process is enabled or IS-IS debugging is not enabled, the **display isis debug-switches** command output is empty.

Example

Display the IS-IS debugging status.

```
<HUAWEI> display isis debug-switches 1
ISIS-1 SPF events related debugging switch is on
```

7.6.21 display isis error

Function

The **display isis error** command displays statistics about error LSPs and Hello packets that are received by IS-IS interfaces or processes.

Format

display isis error [{ *process-id* | **vpn-instance** *vpn-instance-name* } [**interface**]]

display isis error interface *interface-type interface-number*

Parameters

Parameter	Description	Value
process-id	Displays statistics about error packets received by a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about error packets received by the IS-IS process in a specified VPN instance.	The value must be an existing VPN instance name.
interface	Displays statistics about error packets received on all interfaces in a specified IS-IS process or VPN instance.	-
interface-type interface-number	Displays statistics about error packets received by a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis error** command to check statistics about error LSPs and Hello packets that are received by IS-IS interfaces or processes.

Example

Display statistics about error LSPs and Hello packets received on all interfaces in IS-IS process 1.

```
<HUAWEI> display isis error 1
                   Statistics of error packets for ISIS(1)
                   ---------------------------------------
LSP packet errors:
Longer LSP              : 0          Smaller LSP             : 0
Mismatched Level        : 0          Invalid Sysid           : 0
Zero Sequence Number    : 0          Illegal IS Type         : 0
Zero Checksum           : 0          Incorrect Checksum      : 0
Bad Authentication      : 0          Bad Auth Count          : 0
More Protocol TLV       : 0          Bad Nbr TLV             : 0
Bad Extended IS TLV     : 0          Bad IF Addr TLV         : 0
Bad Reach TLV           : 0          Bad Inter Domain TLV    : 0
Mismatched Area Id(L1)  : 0          Bad TLV Length          : 0
Bad Alias TLV           : 0          Bad Area TLV            : 0
Bad SRLG TLV            : 0          Unknown Adjacency       : 0
Bad Protocol ID         : 0          Bad Version             : 0
Zero Lifetime           : 0          Bad Ext Reach TLV       : 0
Bad TE Router ID TLV    : 0          Bad TE Sub TLV          : 0

Hello packet errors:
Bad Packet Length       : 0          Reserved CircType       : 0
Repeated System ID      : 0          Bad Circuit Type        : 0
Longer packet           : 0          More Area Addr          : 0
Longer Area Addr        : 0          Bad Area Addr TLV       : 0
More IF Addr            : 0          Bad Formatted IF TLV    : 0
More Nbr SNPA(LAN)      : 0          Invalid Sysid           : 0
Bad TLV Length          : 0          Zero HoldingTime        : 0
```

```
Unusable IP Addr        : 0           Repeated IPv4 Addr      : 0
Mismatched Area Addr(L1): 0           Mismatched Proto        : 0
SNPA Conflicted(LAN)    : 0           Mismatched Level        : 0
Mismatched Max Area Addr: 0           Bad Authentication      : 0
More Auth TLV           : 0           3-Way Option Error(P2P) : 0
No Area Addr TLV        : 0           Bad Protocol ID         : 0
Bad Version             : 0           Invalid IPv6 Addr       : 0
More IPv6 IF Addr       : 0           Duplicate IPv6 Addr     : 0
More Optional Checksum  : 0           Bad Optional Checksum   : 0
-------------------------------------------------------------------
```

Table 7-94 Description of the display isis error command output

Item	Description
LSP packet errors	LSP errors.
Longer LSP	The LSP length is greater than the value set using the **lsp-length receive** command.
Smaller LSP	The LSP header length is smaller than the fixed length.
Mismatched Level	The level of received LSPs mismatches the local IS-IS level.
Invalid Sysid	The system ID in an LSP is invalid.
Zero Sequence Number	The sequence number of an LSP is 0.
Illegal IS Type	The IS type is invalid.
Zero Checksum	The checksum of an LSP is 0.
Incorrect Checksum	The checksum of an LSP is incorrect.
Bad Authentication	The authentication field of an LSP is incorrect.
Bad Auth Count	The number of authentication fields carried in an LSP is incorrect, that is, it is greater than 1.
More Protocol TLV	The number of protocol TLVs in an LSP is greater than 1.
Bad Nbr TLV	The neighbor TLV is incorrect.
Bad Extended IS TLV	The extended IS TLV is incorrect.
Bad IF Addr TLV	The interface address TLV is incorrect.
Bad Reach TLV	The reachability TLV is incorrect.
Bad Inter Domain TLV	The inter-domain TLV is incorrect. The correct TLV is 0x83.
Mismatched Area Id(L1)	Mismatched Level-1 area ID.
Bad TLV Length	The TLV length is incorrect.
Bad Alias TLV	The Alias TLV is incorrect.

Item	Description
Bad Area TLV	The area TLV is incorrect.
Bad SRLG TLV	The SRLG TLV is incorrect.
Unknown Adjacency	LSPs are received from unknown adjacency.
Bad Protocol ID	The protocol ID is incorrect.
Bad Version	The version is incorrect.
Zero Lifetime	The remaining lifetime of an LSP is 0.
Bad Ext Reach TLV	The Ext Reach TLV is incorrect.
Bad TE Router ID TLV	The TE Router ID TLV is incorrect.
Bad TE Sub TLV	The TE sub-TLV is incorrect.
Hello packet errors	Hello packet errors.
Bad Packet Length	The Hello packet length is incorrect.
Reserved CircType	The reserved link type is incorrect.
Repeated System ID	The system ID is repeated.
Bad Circuit Type	The link type is incorrect.
Longer packet	The Hello packet length is greater than the larger value between the interface MTU and the value set using the **lsp-length originate** command.
More Area Addr	Area addresses are superfluous.
Longer Area Addr	The area address is too long.
Bad Area Addr TLV	The area address TLV is incorrect.
More IF Addr	Interface addresses are superfluous.
Bad Formatted IF TLV	The format of the interface TLV is incorrect.
More Nbr SNPA(LAN)	Sub-network Points of Attachment (SNPAs) of a neighbor on a broadcast network are superfluous.
Invalid Sysid	The system ID length field is not 0 or 6.
Bad TLV Length	The TLV length is incorrect.
Zero HoldingTime	The neighbor holdtime is 0.
Unusable IP Addr	The IP address is on a different network segment than the peer end.
Repeated IPv4 Addr	The IPv4 address is repeated.
Mismatched Area Addr(L1)	Mismatched Level-1 area address.
Mismatched Proto	Mismatched protocol.

Item	Description
SNPA Conflicted(LAN)	Conflicting SNPA on a broadcast network.
Mismatched Level	The level of received Hello packets mismatches the local IS-IS level.
Mismatched Max Area Addr	The maximum area address is incorrect.
Bad Authentication	The authentication field of a Hello packet is incorrect.
More Auth TLV	Authentication TLVs are superfluous.
3-Way Option Error(P2P)	3-way information is incorrect.
No Area Addr TLV	The received Hello packet has no area address TLV.
Bad Protocol ID	The protocol ID is incorrect.
Bad Version	The version is incorrect.
Invalid IPv6 Addr	An IPv6 address is invalid.
More IPv6 IF Addr	A Hello packet carries more than 11 IPv6 addresses.
Duplicate IPv6 Addr	The IPv6 address is repeated.
More Optional Checksum	More than one optional checksum TLV is contained in a packet.
Bad Optional Checksum	Error optional checksum TLV.

7.6.22 display isis graceful-restart status

Function

The **display isis graceful-restart status** command displays the IS-IS GR status.

Format

display isis *process-id* **graceful-restart status** [**level-1** | **level-2**]

display isis graceful-restart status [**level-1** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
level-1	Displays the Level-1 IS-IS GR status.	-
level-2	Displays the Level-2 IS-IS GR status.	-

Parameter	Description	Value
process-id	Displays the IS-IS GR status of a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the IS-IS GR status of the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis graceful-restart status** command to check the IS-IS GR status.

Example

Display the IS-IS GR status.

```
<HUAWEI> display isis graceful-restart status
                      Restart information for ISIS(1)
                        -------------------------------
IS-IS(1) Level-1 Restart Status
Restart Interval: 300
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTART COMPLETE
IS-IS(1) Level-2 Restart Status
Restart Interval: 300
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTART COMPLETE
```

Table 7-95 Description of the display isis graceful-restart status command output

Item	Description
Restart Interval	Expected restart time of the device. This parameter is configured using the **graceful-restart interval** command.
SA Bit Supported	Whether the device supports SA.
Total Number of Interfaces = 1	Number of interfaces on which IS-IS is enabled. IS-IS is enabled using the **isis enable** command on an interface.

Item	Description
Restart Status:	Restart status of the current device. RESTART COMPLETE indicates that the restart is complete.

7.6.23 display isis interface

Function

The **display isis interface** command displays information about IS-IS interfaces.

Format

display isis interface [[**verbose** | **traffic-eng**] * | **te-tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*] (supported only by the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display isis *process-id* **interface** [**te-tunnel** | [**traffic-eng** | **verbose**] *] (supported only by the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display isis interface *interface-type interface-number* [**verbose**]

display isis interface *interface-type interface-number* [**verbose**]

display isis interface

display isis interface *process-id*

display isis *process-id* **interface**

display isis interface vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
verbose	Displays detailed information about IS-IS interfaces.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
traffic-eng	Displays Traffic Engineering information of IS-IS.	-

Parameter	Description	Value
te-tunnel	Displays information on the MPLS TE tunnel of IS-IS.	-
vpn-instance *vpn-instance-name*	Display IS-IS interface information in the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IS-IS interface information, including the interface name, IP address, link status of the interface. If **verbose** is specified, the command output also includes the configuration of IS-IS parameters for the interface, such as the CSNP broadcast interval, Hello packet broadcast interval, and number of IS-IS Hello packets that fail to be received before IS-IS declares the neighbor Down.

Example

Display information about IS-IS interfaces.

```
<HUAWEI> display isis interface

                       Interface information for ISIS(1)
                       ---------------------------------
 Interface       Id      IPV4.State          IPV6.State      MTU  Type  DIS
 Vlanif10        001        Up                  Down         1497 L1/L2 No/No
```

Display detailed information about IS-IS interfaces.

```
<HUAWEI> display isis interface verbose
                       Interface information for ISIS(1)
                       ---------------------------------
 Interface       Id      IPV4.State          IPV6.State      MTU  Type  DIS
 Vlanif10       001         Up                Down         1497 L1/L2 No/No
  Circuit MT State            : Standard
  Description                 :
  SNPA Address                : 0000-1382-4569
  IP Address                  : 10.1.1.5
  IPV6 Link Local Address     :
  IPV6 Global Address (es)    :
  Csnp Timer Value            :  L1    10  L2    10
  Hello Timer Value           :  L1    10  L2    10
  DIS Hello Timer Value       :  L1     3  L2     3
  Hello Multiplier Value      :  L1     3  L2     3
```

```
LSP-Throttle Timer          :  L12    50
Cost                        :  L1    10  L2    10
Ipv6 Cost                   :  L1    10  L2    10
Priority                    :  L1    64  L2    64
Retransmit Timer Value      :  L12    5
Bandwidth-Value             :  Low 1000000000  High          0
Static Bfd                  :  NO
Dynamic Bfd                 :  NO
Dynamic IPv6 Bfd            :  NO
Fast-Sense Rpr              :  NO
Suppress flapping peer      :  enable (flapping-count: 0, threshold: 10)
```

Table 7-96 Description of the display isis interface command output

Item	Description
Interface	IS-IS interface type and number.
Id	Link ID.
IPV4.State	IPv4 link status.
MTU	Interface MTU. An IS-IS neighbor relationship can be established only when two interfaces on both ends of a link have the same MTU.
Type	Interface type: - L1: Level-1 interface - L2: Level-2 interface - L1/L2: Level-1-2 interface
DIS	Whether the interface is a DIS. **NOTE** Only an interface with network type broadcast can be selected as the DIS. If an interface is a P2P interface, "--" is displayed in this field.

Item	Description
Circuit MT State	Topology status on the interface: ● Standard: – IPv4 is enabled on the interface, but IPv6 is not. – IPv6 is enabled on the interface, but IPv4 is not. In addition, the topology type is standard. – Both IPv4 and IPv6 are enabled on the interface. In addition, the topology type is standard. ● IPv6: IPv6 is enabled on the interface, but IPv4 is not. In addition, the topology type is IPv6. ● Standard IPv6: – IPv6 is enabled on the interface, but IPv4 is not. In addition, the topology type is compatible. – Both IPv4 and IPv6 are enabled on the interface. In addition, the topology type is compatible or IPv6. To configure the IPv6 topology type, run the **ipv6 enable** command in the IS-IS view.
SNPA Address	MAC address.
IP Address	IPv4 address of the interface.
IPV6 Link Local Address	IPv6 link-local address.
IPV6 Global Address(es)	IPv6 global address.
Csnp Timer Value	Interval for sending CSNPs. To set the interval for sending CSNPs, run the **isis timer csnp** command.
Hello Timer Value	Interval for sending Hello packets. To set the interval for sending Hello packets, run the **isis timer hello** command.
DIS Hello Timer Value	Interval at which the DIS sends Hello packets, which is one third of **Hello Timer Value**. The field takes effect only when the interface functions as the DIS.
Hello Multiplier Value	Number of consecutive Hello packets that are not received before the neighbor is declared Down. To set this value, run the **isis timer holding-multiplier** command.

Item	Description
LSP-Throttle Timer	Interval for sending LSPs or CSNPs and number of LSPs or CSNPs that are sent each time. To set the two values, run the **isis timer lsp-throttle** command.
Cost	Cost of an IPv4 interface. This field value affects route selection.
Ipv6 Cost	Cost of an IPv6 interface. This field value affects route selection in IPv6 topologies.
Priority	Priority for DIS election. To set the priority for DIS election, run the **isis dis-priority** command.
Retransmit Timer Value	Interval for retransmitting LSPs on a P2P link. To set the retransmit interval, run the **isis timer lsp-retransmit** command.
Bandwidth-Value	Physical bandwidth of an interface. The value can be calculated using the following formula: **Bandwidth-Value** = 4294967296 x **high** + **low**. For example, if the value of **high** is 1 and the value of **low** is 705032704, Bandwidth-Value = 1 x 4294967296 + 705032704 = 5000000000. ● low: low bandwidth with the maximum value of 4294967295 ● high: high bandwidth with the maximum value of 4294967295
Static Bfd	Static BFD status: ● NO: Static BFD is not enabled. ● YES: Static BFD is enabled. To enable BFD on an interface, run the **isis bfd static** command.
Dynamic Bfd	Dynamic BFD status: ● NO: Dynamic BFD is not enabled. ● YES: Dynamic BFD is enabled. To enable dynamic BFD on an interface, run the **bfd all-interfaces enable** or **isis bfd enable** command.

Item	Description
Dynamic IPv6 Bfd	Status of dynamic IPv6 BFD: ● NO: Dynamic BFD is not enabled on the interface. ● YES: Dynamic BFD is enabled on the interface. To enable dynamic IPv6 BFD on an interface, run the **ipv6 bfd all-interfaces enable** or **isis ipv6 bfd enable** command.
Fast-Sense Rpr	Whether the fast sense RPR function is enabled.
Suppress flapping peer	Status of IS-IS neighbor relationship flapping suppression: ● NO: IS-IS neighbor relationship flapping suppression is disabled. ● YES (flapping-count: 3, threshold: 10): IS-IS neighbor relationship flapping suppression is enabled and IS-IS neighbor relationship is not suppressed. The flapping-count and threshold value. ● Hold-down(start: UTC 10:20:30, remain-interval: 7): IS-IS neighbor relationship flapping suppression works in Hold-down mode. The starting and remaining time of the flapping suppression. ● Hold-max-cost(start: UTC 10:20:30, remain-interval: 7): IS-IS neighbor relationship flapping suppression works in Hold-max-cost mode. The starting and remaining time of the flapping suppression. **NOTE** In the flapping suppression state, *remain-interval* is reset each time when the device detects a valid neighbor flapping event.

7.6.24 display isis last-peer-change

Function

The **display isis last-peer-change** command displays changes in IS-IS neighbor relationships.

Format

display isis *process-id* **last-peer-change**

display isis last-peer-change [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display isis last-peer-change** command to view a maximum of 100 latest records in each IS-IS process.

Example

Display changes in IS-IS neighbor relationships.

```
<HUAWEI> display isis last-peer-change
                      Peer change information for ISIS(1)
                      -----------------------------------

Time      : 2011-03-28 09:30:34
System Id : 0000.0000.0002
Type      : L1 LAN
Interface : vlanif10
State     : IPv4 -> IPv4/IPv6
Details   : Protocol change
```

Table 7-97 Description of the display isis last-peer-change command output

Item	Description
Time	Time a neighbor relationship changes.
System Id	System ID of a neighbor.
Type	Neighbor type: • L1 LAN • L2 LAN • P2P
Interface	Interface connected to the neighbor.

Item	Description
State	Changes in the IS-IS neighbor relationship status: ● Init -> Up ● Up -> Down ● Up -> Init ● Down -> Up ● IPv4/IPv6 -> IPv4 ● IPv4/IPv6 -> IPv6 ● IPv4 -> IPv4/IPv6 ● IPv6 -> IPv4/IPv6 ● IPv4 -> IPv6 ● IPv6 -> IPv4 ● L12 -> L2 ● L2 -> L12
Details	Causes for IS-IS neighbor relationship changes: ● Circuit down ● BFD down ● Hold timer expired ● New adjacency created ● Clear neighbor ● Multiple P2P adjacency ● Adjacency usage mismatch ● Internal error ● Memory low ● P2P circuit ID conflict ● Area mismatch ● Three way down ● Three way init ● Three way up ● Protocol change ● Mt usage mismatch ● Peer state change ● Peer level change

7.6.25 display isis lsdb

Function

The **display isis lsdb** command displays information about IS-IS LSDBs.

Format

display isis *process-id* **lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] *

display isis lsdb [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
level-1	Displays Level-1 LSDBs. If no level is specified, Level-1 and Level-2 LSDBs are displayed.	-
level-2	Displays Level-2 LSDBs. If no level is specified, Level-1 and Level-2 LSDBs are displayed.	-
verbose	Displays detailed information about IS-IS LSDBs.	-
local	Displays information about the local LSDB.	-
lsp-id	Specifies an LSP ID.	The value is in dotted decimal notation. The value ranges from 16 to 20 in ####.####.####.##-## format, such as 0050.0500.5004.00-00.
is-name *symbolic-name*	Specifies the dynamic host name in is-name or is-name.##-## format. ##-## indicates the pseudonode ID-LSP fragment ID.	The value is a string of 1 to 70 characters.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the LSDB of the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis lsdb** command to check information about IS-IS LSDBs.

Example

Display IS-IS LSDB information.

```
<HUAWEI> display isis lsdb
                        Database information for ISIS(1)
                        --------------------------------
                          Level-2 Link State Database
LSPID                 Seq Num       Checksum       Holdtime       Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x0000017a   0xa21c        846           84      0/0/0
2222.2222.2222.00-00* 0x000001ce   0xbdcc        845           111     0/0/0
3333.3333.3333.00-00  0x00000013   0x8847        1004          84      0/0/0
3333.3333.3333.01-00  0x0000000b   0x95bc        1004          55      0/0/0
Total LSP(s): 4
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload
```

Table 7-98 Description of the display isis lsdb command output

Item	Description
LSPID	LSP ID.
Seq Num	LSP sequence number.
Checksum	LSP checksum.
Holdtime	LSP holdtime.
Length	LSP length.
ATT/P/OL	• ATT: Attach bit • P: partition bit • OL: overload bit
Total LSP(s)	Number of LSPs.

Item	Description
*/+	- *(In TLV): Leaking route. - *(By LSPID): Locally generated LSP. - +: Locally generated extended LSP.

Display detailed information about IS-IS LSDB.

```
<HUAWEI> display isis lsdb verbose

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000010   0xc776        0 (724)       36      0/0/0
 SOURCE       0000.0000.0001.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    10.22.21.1
 NBR  ID      0000.0000.0002.02  COST: 10
 IP-Internal  10.22.21.0      255.255.255.0    COST: 10

0000.0000.0003.00-00* 0x00000026   0x6fb4        1145          350     0/0/0
 SOURCE       0000.0000.0003.00
 HOST NAME    RouterA
 NLPID        IPV4
 NLPID        IPV6
 AREA ADDR    10
 INTF ADDR    10.1.1.2
 INTF ADDR    10.1.2.2
 INTF ADDR V6 FC00:1::1
 Topology     Standard
 NBR  ID      0000.0000.0001.00  COST: 10
+NBR  ID      0000.0000.0001.00  COST: 10
 IP-Internal  10.1.1.0       255.255.255.0    COST: 10
 IP-Internal  10.1.2.0       255.255.255.0    COST: 10
+IP-Extended  10.1.1.0       255.255.255.0    COST: 10 +IP-Extended  10.1.2.0       255.255.255.0    COST: 10
 IPV6         FC00:1::/64                      COST: 10
Total LSP(s): 2
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload


                          Level-2 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0003.00-00* 0x0000001c   0x9b0d        1131          233     0/0/0
 SOURCE       RouterA.00 ORG ID: RouterA.00 ORG ID: 0000.0000.0003.00
 HOST NAME    RouterA
 NLPID        IPV4
 NLPID        IPV6
 AREA ADDR    10
 INTF ADDR    10.1.1.2
 INTF ADDR    10.1.2.2
 INTF ADDR V6 FC00:1::1
 Topology     Standard
 NBR  ID      0000.0000.0004.00  COST: 10
+NBR  ID      0000.0000.0004.00  COST: 10 +MT NBR ID    0000.0000.0004.00  COST: 10
 IP-Internal  10.1.1.0       255.255.255.0    COST: 10
 IP-Internal  10.1.2.0       255.255.255.0    COST: 10
+IP-Extended  10.1.1.0       255.255.255.0    COST: 10 +IP-Extended  10.1.2.0       255.255.255.0    COST: 10
```

```
 IPV6         FC00:1::/64                     COST: 10

0000.0000.0003.00-01* 0x00000005   0x5ec1        1129          70      0/0/0
 SOURCE       RouterA.00
Auth: *****      Len: --      Type: MD5
 IP-External  10.1.3.0       255.255.255.0    COST: 0
+IP-Extended  10.1.3.0       255.255.255.0    COST: 0 Total LSP(s): 2
    *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
           ATT-Attached, P-Partition, OL-Overload
```

Table 7-99 Description of the display isis lsdb verbose command output

Item	Description
SOURCE	System ID of the source node.
ORG ID	Source system ID of the virtual system.
HOST NAME	Dynamic host name.
Auth	Authentication password.
Len	Authentication password length.
Type	Authentication type: ● Plain Text: indicates that the password is sent in plain text. ● MD5: indicates that the password is encrypted using the MD5 algorithm. ● CRYPTO_AUTH: The password is encrypted with the HMAC-SHA256 encryption algorithm.
NLPID	Supported network protocol. ● IPV4: supported the IPv4 network protocol. ● IPV6: supported the IPv6 network protocol.
AREA ADDR	Area address.
INTF ADDR	Interface IPv4 address.
INTF ADDR V6	Interface IPv6 address.
Topology	Topology type.
NBR ID	System ID of a neighbor.
+NBR ID	System ID of a neighbor, which can carry TE information.
+MT NBR ID	Neighbor ID in the MT topology.
COST	Route cost.
IP-Internal	Internal IPv4 routing information.
IP-External	External IPv4 routing information.

Item	Description
+IP-Extended	Extended IP routing information, which can carry TE information.
IPV6	Internal IPv6 routing information.

7.6.26 display isis mesh-group

Function

The **display isis mesh-group** command displays the configuration of the IS-IS mesh-group.

Format

display isis mesh-group [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **mesh-group**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis mesh-group** command to check the configuration of the IS-IS mesh-group.

Example

Display information about the configured IS-IS mesh-group.

```
<HUAWEI> display isis mesh-group
              Mesh Group information for ISIS(1)
----------------------------------------------------------------------
Interface         Status
```

```
Vlanif10         100
Vlanif20         100
```

Table 7-100 Description of the display isis mesh group command output

Item	Description
Interface	Type and number of the interface in the mesh-group.
Status	Mesh-group number.

7.6.27 display isis name-table

Function

The **display isis name-table** command displays the mapping between the dynamic hostnames of IS-IS routers and the system IDs.

Format

display isis name-table [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **name-table**

Parameters

Parameter	Description	Value
process-id	Displays the mapping between dynamic hostnames of IS-IS routers and system IDs in a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the mapping between dynamic hostnames of IS-IS routers and system IDs in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After dynamic hostnames are configured, you can run the **display isis name-table** command to check the mapping between the dynamic hostnames and system IDs.

Example

Configure a name for the local IS-IS system.

```
[Switch] isis
[Switch-isis-1] is-name RUTA
```

Configure a static name mapping for the remote IS-IS system (0000.0000.0041).

```
[Switch-isis-1] is-name map 0000.0000.0041 RUTB
```

Display the IS-IS system name table.

```
<Switch> display isis name-table
            Name table information for ISIS(1)
System ID               Hostname       Type
-------------------------------------------------------------------
6789.0000.0001          RUTA           DYNAMIC
0000.0000.0041          RUTB           STATIC
```

Table 7-101 Description of the display isis name-table command output

Item	Description
System ID	System ID of the current IS-IS device. To set the system ID, run the **network-entity** command.
Hostname	Host name of the device. To set a host name for the local or remote device, run the **is-name** or **is-name map** command.
Type	Type of the mapping between the host name and system ID: static or dynamic.

7.6.28 display isis peer

Function

The **display isis peer** command displays IS-IS neighbor information.

Format

display isis *process-id* **peer** [**verbose**]

display isis peer [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis peer interface *interface-type interface-number* [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed IS-IS neighbor information, including the area address, period during which the neighbor remains Up, and IP address of its directly connected interface.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an IS-IS area, if you need to check whether two devices can communicate properly, run the **display isis peer** command to view information about the neighbor, including the neighbor status, period during which the neighbor remains Up, and neighbor type.

Example

Display information about IS-IS neighbors.

```
<HUAWEI> display isis peer
                          Peer information for ISIS(1)

  System Id     Interface          Circuit Id       State HoldTime Type     PRI
-------------------------------------------------------------------------------
0000.0000.0001   Vlanif10         0000.0000.0001.01   Up    24s   L1(L1L2)  64
0000.0000.0001   Vlanif10         0000.0000.0001.01   Up    24s   L2(L1L2)  64

Total Peer(s): 2
```

Table 7-102 Description of the display isis peer command output

Item	Description
System Id	System ID of the neighbor.
Interface	Type and number of the interface.
Circuit Id	Circuit ID.
State	Neighbor status: ● Up: indicates that the neighbor is Up and the two ends can communicate. ● Init: indicates that the local end can receive packets from the remote end but the remote end cannot receive packets from the local end. This status is displayed when authentication is configured on the remote end. ● Down: indicates that the neighbor is Down. This is the initial status, indicating that no message is received from the neighbor. In most cases, this status is not displayed.
HoldTime	Neighbor holdtime.
Type	Neighbor type: ● L1: indicates that the neighbor type is Level-1 and interfaces on both ends are Level-1 interfaces. ● L2: indicates that the neighbor type is Level-2 and interfaces on both ends are Level-2 interfaces. ● L1(L1L2): indicates that the neighbor type is Level-1 and interfaces on both ends are Level-1-2 interfaces. ● L2(L1L2): indicates that the neighbor type is Level-2 and interfaces on both ends are Level-1-2 interfaces.
PRI	Priority of the neighbor in DIS election.

Display detailed information about IS-IS neighbor.

```
<HUAWEI> display isis peer verbose
                          Peer information for ISIS(1)

  System Id     Interface          Circuit Id         State  HoldTime   Type     PRI
------------------------------------------------------------------------------
0000.0000.0001  Vlanif10          0000.0000.0001.01      Up     26s     L1(L1L2)   64
  MT IDs supported     : 0(UP)    Local MT IDs         : 0
  Area Address(es)     : 10
  Peer IP Address(es)  : 10.10.10.1
```

```
  Peer IPv6 Address(es): FE80:2000:57::7
  Uptime               : 00:00:19
  Adj Protocol         : IPV4  IPv6
  Restart Capable      : YES
  Suppressed Adj       : NO
  Peer System Id     : 0000.0000.0001

0000.0000.0001  Vlanif10          0000.0000.0001.01      Up     27s     L2(L1L2)   64
  MT IDs supported     : 0(UP)    Local MT IDs         : 0
  Area Address(es)     : 10
  Peer IP Address(es)  : 10.10.10.1
  Peer IPv6 Address(es): FE80:2000:56::6
  Uptime               : 00:00:19
  Adj Protocol         : IPV4  IPv6
  Restart Capable      : YES
  Suppressed Adj       : NO
  Peer System Id     : 0000.0000.0001

Total Peer(s): 2
```

Table 7-103 Description of the **display isis peer verbose** command output

Item	Description
MT IDs supported	IDs of topology instances supported by the remote interface.
Local MT IDs	IDs of topology instances supported by the local interface.
Area Address(es)	Area addresses of the neighbor.
Peer IP Address(es)	IP address of the remote interface.
Peer IPv6 Address(es)	IPv6 address of the remote interface.
Uptime	Period during which the neighbor remains Up.
Adj Protocol	Protocol used for establishing the adjacency.
Restart Capable	Whether GR is supported: ● YES: indicates that GR is supported. ● NO: indicates that GR is not supported.
Suppressed Adj	Whether neighbor suppression is supported: ● YES: indicates that neighbor suppression is supported. ● NO: indicates that neighbor suppression is not supported.
Peer System Id	The System ID of the IS-IS peer.
Total Peer(s)	Number of neighbors.

7.6.29 display isis purge packet

Function

The **display isis purge packet** command displays statistics about received IS-IS purge LSPs carrying the POI TLV.

Format

display isis *process-id* **purge packet** [*packet-number*]

display isis purge packet *process-id* [*packet-number*]

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer ranging from 1 to 65535.
packet-number	Specifies the number of purge LSPs whose statistics are to be displayed.	The value is an integer ranging from 1 to 20.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check statistics about received IS-IS purge LSPs carrying the POI TLV, run the **display isis purge packet** command. You can specify *packet-number* in the command to check statistics about a specified number of purge LSPs, and the maximum value of *packet-number* is 20. If its value is set to 20:

- The first two displayed purge LSPs are sent by the local source system, with fragment number 0, one of which is Level-1, and the other is Level-2.
- The first 10 displayed purge LSPs are generated locally, and the next 10 purge LSPs are from neighbors. The purge LSPs are displayed in reverse order of the time when they were received. If the LSP ID is followed by an asterisk (*), the purge LSP is generated locally.

Example

Display statistics about received IS-IS purge LSPs carrying the POI TLV.

```
<HUAWEI> display isis purge packet 1 10

                  Purge LSP packet for ISIS(1)
--------------------------------------------------------------
Packet information(Index 1):
```

```
----------------------------------------------------
Received LSPID      :  0000.0000.0027.00-00*
Source Interface    :  Vlanif100
Time                :  2015-1-22 13:55:06
Level               :  Level-2
PDU Type            :  20(Level-2 LSP)
PDU Length          :  55
Sequence Number     :  0x00000015
Checksum            :  0xc891
POI NAME            :  0000.0000.0004
POI NAME(Neighbor)  :  0000.0000.0005
HOST NAME           :  RT4-Pro1
Auth Type           :  **
0010: 83 1b 01 06 12 01 00 03 00 43 00 00 00 00 00 00
0020: 00 27 00 00 00 01 6a 6c bd ed 01 0d 07 01 00 00
0030: 00 00 00 01 89 0a 52 54 31 2d 50 72 6f 2d 30 31
0040: ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
0050: ** ** **
----------------------------------------------------
   **-Authentication TLV, *(By LSPID)-Self LSP
```

Table 7-104 Description of the **display isis purge packet** command output

Item	Description
Received LSPID	ID of a received purge LSP
Source Interface	Source interface of a received purge LSP
Time	Time when a purge LSP was received
Level	Level of a received purge LSP
PDU Type	Type of received purge LSP
PDU Length	Length of a received purge LSP
Sequence Number	Sequence number (LSN) of a received purge LSP
Checksum	Checksum of a received purge LSP
POI NAME	POI TLV carried in a received purge LSP
POI NAME(Neighbor)	Neighbor system ID in the POI TLV carried in a received purge LSP
HOST NAME	Dynamic hostname carried in a received purge LSP
Auth Type	Authentication information carried in a received purge LSP

7.6.30 display isis route

Function

The **display isis route** command displays IS-IS routing information.

Format

display isis route [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] *

display isis route [*process-id* | **vpn-instance** *vpn-instance-name*] **ipv6** [**verbose** | [**level-1** | **level-2**] | *ipv6-address* [*prefix-length*]] *

display isis *process-id* **route** [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] *

display isis *process-id* **route ipv6** [**verbose** | [**level-1** | **level-2**] | *ipv6-address* [*prefix-length*]] *

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.
ipv4	Displays IPv4 routes. If this parameter is not specified, both IPv4 and IPv6 IS-IS routes are displayed.	-
verbose	Displays detailed routing information.	-
level-1	Displays Level-1 IS-IS routes.	-
level-2	Displays Level-2 IS-IS routes.	-
ip-address	Displays the routes with the specified IPv4 destination address.	The value is in dotted decimal notation.
mask	Specifies the mask of an IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 0 or 32.
ipv6	Displays IPv6 routes. If this parameter is not specified, both IPv4 and IPv6 IS-IS routes are displayed.	-
ipv6-address	Displays the routes with the specified IPv6 destination address.	The value is a 32-digit hexadecimal number, in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis route** command to check IS-IS routing information.

Example

Display all IS-IS routes.

```
<HUAWEI> display isis route

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.2.1.0/24          10         NULL    Vlanif10        Direct          D/-/L/-
172.18.0.0/16        20         NULL    Vlanif10        10.2.1.1        A/-/L/-

 IPV6 Dest.          ExitInterface   NextHop                     Cost      Flags
-------------------------------------------------------------------------------
 FC00:0:0:200::/64    Vlanif10        Direct                      10        D/L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                           U-Up/Down Bit Set


                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.2.1.0/24          10         NULL    Vlanif10        Direct          D/-/L/-
172.18.0.0/16        20         NULL    Vlanif10        10.2.1.1        A/-/L/-

 IPV6 Dest.          ExitInterface   NextHop                     Cost      Flags
-------------------------------------------------------------------------------
 FC00:0:0:200::/64    Vlanif10        Direct                      10        D/L/-

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                           U-Up/Down Bit Set
```

Table 7-105 Description of the display isis route command output

Item	Description
IPV4 Destination	IPv4 destination address and mask.
IPV6 Dest.	IPv6 destination address and mask.

Item	Description
IntCost	IPv4 internal cost or IS-IS route cost. To change the IS-IS IPv4 route cost, run the **circuit-cost** or **isis cost** command to set the link cost of an IS-IS IPv4 interface.
ExtCost	IPv4 external cost or cost of routes imported from other routing protocols. To set the cost of imported routes, run the **import-route** command. **NOTE** The costs of external routes imported using the **import-route cost-type external** command are displayed in this field to differentiate the costs of IS-IS routes.
Cost	IPv6 route cost. To change the IS-IS IPv6 route cost, run the **ipv6 circuit-cost** or **isis ipv6 cost** command to set the link cost of an IS-IS IPv6 interface.
ExitInterface	Outbound interface of a route.
NextHop	Next hop address of a route. This field displays Direct if the destination network segment is the direct network segment.
Flags	Route flag: ● D-Direct: indicates a direct route. ● A-Added to URT: indicates that a route is added to the unicast routing table. ● L-Advertised in LSPs: indicates that a route is advertised through an LSP. ● S-IGP Shortcut: indicates that the interface on which IGP-Shortcut is enabled exists on the path to the destination. ● U-Up/Down Bit Set: indicates the Up/ Down bit.

Display IS-IS IPv4 routes.

```
<HUAWEI> display isis route ipv4

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24          10         NULL    Loop1           Direct          D/-/L/-
10.2.2.0/24          10         NULL    Loop2           Direct          D/-/L/-
```

```
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                           U-Up/Down Bit Set


                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
10.1.1.0/24          10         NULL    Loop1           Direct          D/-/L/-
10.2.2.0/24          10         NULL    Loop2           Direct          D/-/L/-
     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                           U-Up/Down Bit Set
```

Display detailed IS-IS routing information.

```
<HUAWEI> display isis route verbose

                         Route information for ISIS(1)
                         -----------------------------

                        ISIS(1) Level-1 Forwarding Table
                        --------------------------------

 IPV4 Dest  : 10.0.0.0/24        Int. Cost : 10            Ext. Cost : NULL
 Admin Tag  : -                Src Count : 2             Flags     : D/L/-
 Priority   : -
 NextHop    :                  Interface :               ExitIndex :
    Direct                        Vlanif10                  0x00000000

 IPV4 Dest  : 10.1.0.0/24        Int. Cost : 10            Ext. Cost : NULL
 Admin Tag  : -                Src Count : 2             Flags     : D/L/-
 Priority   : -
 NextHop    :                  Interface :               ExitIndex :
    Direct                        Vlanif20                  0x00000000

 IPV4 Dest  : 10.2.0.0/24        Int. Cost : 20            Ext. Cost : NULL
 Admin Tag  : -                Src Count : 2             Flags     : A/L/-
 Priority   : Low
 NextHop    :                  Interface :               ExitIndex :
    10.2.0.2                      Vlanif20                  0x00000003
    10.0.0.2                      Vlanif10                  0x00000005

 IPV4 Dest  : 10.4.1.1/32        Int. Cost : 10            Ext. Cost : NULL
 Admin Tag  : -                Src Count : 1             Flags     : A/L/-
 Priority   : Medium
 NextHop    :                  Interface :               ExitIndex :
    10.0.0.2                      Vlanif10                  0x00000005
 (B)10.2.0.2                      Vlanif20                  0x00000003

     Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                           U-Up/Down Bit Set



                        ISIS(1) Level-2 Forwarding Table
                        --------------------------------

 IPV4 Dest  : 10.0.0.0/24        Int. Cost : 10            Ext. Cost : NULL
 Admin Tag  : -                Src Count : 3             Flags     : D/L/-
 Priority   : -
 NextHop    :                  Interface :               ExitIndex :
    Direct                        Vlanif10                  0x00000000

 IPV4 Dest  : 10.1.0.0/24        Int. Cost : 10            Ext. Cost : NULL
 Admin Tag  : -                Src Count : 3             Flags     : D/L/-
 Priority   : -
 NextHop    :                  Interface :               ExitIndex :
    Direct                        Vlanif20                  0x00000000
```

```
IPV4 Dest  : 10.2.0.0/24      Int. Cost : 20          Ext. Cost : NULL
Admin Tag  : -                Src Count : 2           Flags     : -/-/-
Priority   : Low

IPV4 Dest  : 10.3.1.1/32      Int. Cost : 10          Ext. Cost : NULL
Admin Tag  : -                Src Count : 2           Flags     : -/-/-
Priority   : Medium

   Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                           U-Up/Down Bit Set
```

Table 7-106 Description of the display isis route verbose command output

Item	Description
IPV4 Dest	IPv4 destination address and mask.
Int.Cost	IPv4 internal cost, the cost of an IS-IS route.
Ext.Cost	IPv4 external cost, the cost of other protocol route imported by IS-IS. **NOTE** The costs of non-IS-IS routes imported by the **import-route cost-type external** command are displayed in this field so that the costs of non-IS-IS routes are kept independently from the costs of IS-IS routes.
Admin Tag	Administrative tag.
Src Count	Number of source addresses to the same destination.
Priority	Convergence priority of IS-IS routes: ● Critical ● High ● Medium ● Low To set the convergence priority of IS-IS routes, run the **prefix-priority** command.
NextHop	Next hop of a route. The next hop (B) tag of a route is a backup route tag.
Interface	Outbound interface of a route.
ExitIndex	Index of the outbound interface.
Flags	Flags of routing information

7.6.31 display isis spf-log

Function

The **display isis spf-log** command displays IS-IS SPF logs.

Format

display isis spf-log [*process-id* | **vpn-instance** *vpn-instance-name*] [[**level-1** | **level-2**] | **ipv6** | **verbose**]*

display isis *process-id* **spf-log** [[**level-1** | **level-2**] | **ipv6** | **verbose**]*

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.
ipv6	Displays SPF logs in IPv6 topologies.	-
level-1	Displays Level-1 SPF logs.	-
level-2	Displays Level-2 SPF logs.	-
verbose	Displays detailed information about SPF logs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the SPT calculated by IS-IS is incorrect, you can run the **display isis spf-log** command to diagnose the fault. The command displays information about SPF calculation, such as the start time and duration of the SPF calculation, number of nodes, and events that trigger the SPF calculation. You can determine whether the events are the cause of the SPF calculation fault based on the start time of the SPF calculation.

Example

Display IS-IS SPF logs.

```
<HUAWEI> display isis spf-log

                        SPF Log information for ISIS(10)
                        --------------------------------

                            ISIS(10) Level-1 SPF Log
                            ------------------------

 StartTime  Duration  Nodes  Count  Last Trigger LSP      Trigger Event
-----------------------------------------------------------------------------
 2013-09-05 10:14:48+00:00
            0         1      1      NULL                  ISPF_CIRC_DR_CHANGE
 2013-09-05 10:13:23+00:00
            1         1      2      NULL                  FULL_SPF

                            ISIS(10) Level-2 SPF Log
                            ------------------------

 StartTime  Duration  Nodes  Count  Last Trigger LSP      Trigger Event
-----------------------------------------------------------------------------
 2013-09-05 10:14:48+00:00
            1         1      1      NULL                  ISPF_CIRC_DR_CHANGE
 2013-09-05 10:13:23+00:00
            1         1      2      NULL                  FULL_SPF
```

Table 7-107 Description of the display isis spf-log command output

Item	Description
StartTime	Start time of SPF calculation.
Duration	Duration of SPF calculation.
Nodes	Number of nodes in SPF calculation.
Count	Number of times SPF calculated is triggered.
Last Trigger LSP	LSP that triggers the last SPF calculation: ● NULL indicates that the LSP is local. ● LSP ID (specific ID) indicates that the LSP is not local.

Item	Description
Trigger Event	Event that triggers the last SPF calculation: ● NEWAREA indicates that a new NET is configured. ● TUNNEL_ADJ indicates that a tunnel neighbor relationship is established. ● ADJDOWN indicates that a tunnel neighbor goes Down. ● NEWLSP indicates that the router receives an LSP of a new process. ● LSPCHANGE indicates that the received LSP is different from local LSPs. ● RST_T2_CANCEL indicates that the GR T2 Timer is disabled. ● RST_T3_EXPIRE indicates that the GR T3 Timer expires. ● RESTART_COMPLETE indicates that the GR is over. ● CIRC_VLINK_CHANGE indicates that the status of the VLink interface changes. ● PRC_IPV4_PREFIX_ADD indicates that an IPv4 route is added. ● PRC_IPV4_PREFIX_DEL indicates that an IPv4 route is deleted. ● PRC_IPV4_PREFIX_MODIFY indicates that an IPv4 route is modified. ● PRC_IPV4_PREFIX_MIGP_ADD indicates that an MIGP IPv4 route is added. ● PRC_IPV4_PREFIX_MIGP_DEL indicates that an MIGP IPv4 route is deleted. ● PRC_IPV4_PREFIX_MIGP_MODIFY indicates that an MIGP IPv4 route is modified. ● PRC_IPV6_PREFIX_ADD indicates that an IPv6 route is added. ● PRC_IPV6_PREFIX_DEL indicates that an IPv6 route is deleted. ● PRC_IPV6_PREFIX_MODIFY indicates that an IPv6 route is modified. ● ISPF_ADJ_STATE_CHANGE indicates that the IS-IS neighbor status changes. ● ISPF_ADJ_USAGE_CHANGE indicates that the IS-IS neighbor level changes.

Item	Description
	• ISPF_ADJ_PROT_USAGE_CHANGE indicates that the protocol used by the IS-IS neighbor changes. • ISPF_ADJ_NEXTHOP_CHANGE indicates that the next hop of the IS-IS neighbor changes. • ISPF_CIRC_METRIC_CHANGE indicates that the cost on the interface changes. • ISPF_CIRC_DR_CHANGE indicates that the DIS changes. • ISPF_NODE_DEL indicates that the nodes in the SPT change. • ISPF_NODE_OLOAD_CHANGE indicates that the overload bit of the system changes. • ISPF_LINK_ADD indicates that a new link is added to the SPT. • ISPF_LINK_DEL indicates that a link is deleted from the SPT. • ISPF_LINK_METRIC_CHANGE indicates that the cost of a link changes. • FULL_SPF indicates that a full SPF calculation is triggered. • AREA_CFG_CHANGE indicates that the area of the process changes. • AREA_LEARNT_CHANGE indicates that the area of the IS-IS neighbor changes. • ISPF_TUNNEL_TYPE_CHANGE indicates that the tunnel type changes. • PRC_LEAVE_MAN_OVERLOAD indicates that the system exits the **set-overload** state that is set manually. • PRC_IPV4_SELFLSP_CHANGE indicates that the IPv4 route in the local LSP changes. • PRC_IPV6_SELFLSP_CHANGE indicates that the IPv6 route in the local LSP changes. • PRC_ALIAS_TLV_CHANGE indicates that the **ALIAS TLV** in the LSP changes. • LFA_LINK_ADD indicates that a link is added to the routes for FRR. • LFA_LINK_DEL indicates that a link is deleted from the routes for FRR.

Item	Description
	- LFA_LINK_CHANGE indicates that the links of the routes for FRR change. - LFA_NODE_ADD indicates that a node is added along the links of the routes for FRR. - LFA_NODE_DEL indicates that a node is deleted from the links of the routes for FRR. - LFA_NODE_CHANGE indicates that the nodes along the links of the routes for FRR change. - KEY_RESRORE indicates that the local device receives an indirect next hop key.

7.6.32 display isis spf-tree

Function

The **display isis spf-tree** command displays the topology of the SPF tree that is generated by IS-IS.

Format

display isis spf-tree [**systemid** *systemid* | **dname** *dname*] [[**level-1** | **level-2**] | **ipv6** | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **spf-tree** [**systemid** *systemid* | **dname** *dname*] [[**level-1** | **level-2**] | **ipv6** | **verbose**] *

display isis *process-id* **spf-tree statistics** [[**level-1** | **level-2**] | **ipv6**] *

display isis spf-tree statistics [[**level-1** | **level-2**] | **ipv6**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
systemid *systemid*	Displays the SPF tree of the switch with a specified system ID or pseudonode ID.	The value is in XXXX.XXXX.XXXX[.XX] format.

Parameter	Description	Value
dname *dname*	Displays the SPF tree of the switch with a specified dynamic name.	The value is a string of 1 to 64 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
level-1	Displays Level-1 SPF tree.	-
level-2	Displays Level-2 SPF tree.	-
ipv6	Displays SPF tree in IPv6 topologies.	-
verbose	Displays detailed information about SPF tree.	-
process-id	Display SPF tree in a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays SPF tree of the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.
statistics	Displays SPF tree statistics, including information about links and nodes on the SPF tree.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify **statistics** to view the current status of the SPF tree. The generated SPF tree can be used to calculate routes only when the SPF calculation status is Completed, that is, incremental SPF (ISPF) calculation is complete.

Example

Display information about the SPF tree.

```
<HUAWEI> display isis spf-tree
                    Shortest Path Tree for ISIS(1)
                    ------------------------------
```

```
        Flags:   T-System is on SPF TREE  R-System is directly reachable
                 O-System is Overload     D-System or Link is to be deleted
                 C-Neighbor is child      P-Neighbor is parent
                 G-Cost gets greater      L-Cost gets lower
                 H-Nexthop is changed     U-Protocol usage is changed
                 V-Link is involved       N-Link is a new path
                 S-Link is IGP Shortcut   *-Relative cost
                      ISIS(1) Level-1 Shortest Path Tree
                      ----------------------------------

 SpfNode           NodeFlags  NeighbourNode     LinkCost   LinkFlags
----------------------------------------------------------------------
----------------------------------------------------------------------
 0000.0000.0001.00 T/-/-/-   >0000.0000.0002.01       10   P/-/-/-/-/-/-
>0000.0000.0002.00 T/-/-/-    0000.0000.0003.01       10   C/-/-/-/-/-/-
                             >0000.0000.0002.01       10   C/-/-/-/-/-/-
                              0000.0000.0004.00      -10*  C/-/-/-/S/-/-
>0000.0000.0002.01 T/R/-/-    0000.0000.0001.00        0   C/-/-/-/-/-/-
                             >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0003.00 T/-/-/-    0000.0000.0004.02       10   C/-/-/-/-/-/-
                              0000.0000.0003.01       10   P/-/-/-/-/-/-
 0000.0000.0003.01 T/R/-/-    0000.0000.0003.00        0   C/-/-/-/-/-/-
                             >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0004.00 T/-/-/-    0000.0000.0004.02       10   P/-/-/-/-/-/-
                              0000.0000.0004.01       10   C/-/-/-/-/-/-
 0000.0000.0004.01 T/-/-/-    0000.0000.0004.00        0   P/-/-/-/-/-/-
                              0000.0000.0005.00        0   C/-/-/-/-/-/-
 0000.0000.0004.02 T/-/-/-    0000.0000.0004.00        0   C/-/-/-/-/-/-
                              0000.0000.0003.00        0   P/-/-/-/-/-/-
 0000.0000.0005.00 T/-/-/-    0000.0000.0004.01       10   P/-/-/-/-/-/-
                      ISIS(1) Level-2 Shortest Path Tree
                      ----------------------------------

 SpfNode           NodeFlags  NeighbourNode     LinkCost   LinkFlags
----------------------------------------------------------------------
----------------------------------------------------------------------
 0000.0000.0001.00 T/-/-/-   >0000.0000.0002.01       10   P/-/-/-/-/-/-
>0000.0000.0002.00 T/-/-/-    0000.0000.0003.01       10   C/-/-/-/-/-/-
                             >0000.0000.0002.01       10   C/-/-/-/-/-/-
                              0000.0000.0004.00      -10*  C/-/-/-/S/-/-
>0000.0000.0002.01 T/R/-/-    0000.0000.0001.00        0   C/-/-/-/-/-/-
                             >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0003.00 T/-/-/-    0000.0000.0004.02       10   C/-/-/-/-/-/-
                              0000.0000.0003.01       10   P/-/-/-/-/-/-
 0000.0000.0003.01 T/R/-/-    0000.0000.0003.00        0   C/-/-/-/-/-/-
                             >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0004.00 T/-/-/-    0000.0000.0004.02       10   P/-/-/-/-/-/-
                              0000.0000.0004.01       10   C/-/-/-/-/-/-
 0000.0000.0004.01 T/-/-/-    0000.0000.0004.00        0   P/-/-/-/-/-/-
                              0000.0000.0005.00        0   C/-/-/-/-/-/-
 0000.0000.0004.02 T/-/-/-    0000.0000.0004.00        0   C/-/-/-/-/-/-
                              0000.0000.0003.00        0   P/-/-/-/-/-/-
 0000.0000.0005.00 T/-/-/-    0000.0000.0004.01       10   P/-/-/-/-/-/-
```

Table 7-108 Description of the display isis spf-tree command output

Item	Description
SpfNode	Node ID in the network topology.

Item	Description
NodeFlags	Node flag: ● T: The node is on the SPF tree. ● R: The node is directly reachable. ● O: The node is overloaded. ● D: The node is to be deleted.
NeighbourNode	ID of the neighboring node.
LinkCost	Link cost.
LinkFlags	Link flag: ● C: Neighbor is child ● P: Neighbor is parent ● G: Cost gets greater ● L: Cost gets lower ● H: Nexthop is changed ● U: Protocol usage is changed ● V: Link is involved ● N: Link is a new path ● S: Link is IGP Shortcut ● *: Relative cost
>	Mark of the local node.

Display detailed information about SPF tree.

```
<HUAWEI> display isis spf-tree verbose
                          Shortest Path Tree for ISIS(1)
                          ------------------------------

                        ISIS(1) Level-1 Shortest Path Tree
                        ----------------------------------
>0000.0000.0001.00
   Distance            : 0
   Distance-URT        : 0
   Flags               : SPT
   IPv4 Nexthops-URT   : 0
   IPv4 Nexthops-MIGP  : 0
   IPv6 Nexthops       : 0
   Neighbors: 2 (Children:2 Parents:0 Others:0)
             (1)   0000.0000.0002.01
                    Cost  : 10
                    Flags : Child

             (2)  >0000.0000.0001.01
                    Cost  : 10
                    Flags : Child

>0000.0000.0001.01
   Distance            : 10
   Distance-URT        : 10
   Flags               : SPT/Direct/Isolate/V6_Islt
   IPv4 Nexthops-URT   : 0
```

```
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
           (1)   0000.0000.0003.00
                 Cost  : 0
                         C:0 I:vlanif 10
                 Flags : Adj/Child

           (2)  >0000.0000.0001.00
                 Cost  : 0
                 Flags : Parent

0000.0000.0002.00
  Distance           : 10
  Distance-URT       : 10
  Flags              : SPT/V6_Islt
  IPv4 Nexthops-URT   : 1
           (1) 10.1.0.2         IF:vlanif 10  NBR:0000.0000.0002.00
           (B) 10.0.0.2         IF:vlanif 20  NBR:0000.0000.0003.00
                                TYPE:LOOP-FREE  PROTECT:LINK
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
           (1)   0000.0000.0002.02
                 Cost  : 10
                 Flags : Child

           (2)   0000.0000.0002.01
                 Cost  : 10
                 Flags : Parent

0000.0000.0002.01
  Distance           : 10
  Distance-URT       : 10
  Flags              : SPT/Direct/Isolate/V6_Islt
  IPv4 Nexthops-URT   : 0
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
           (1)   0000.0000.0002.00
                 Cost  : 0
                         C:0 I:vlanif 10
                 Flags : Adj/Child

           (2)  >0000.0000.0001.00
                 Cost  : 0
                 Flags : Parent

0000.0000.0002.02
  Distance           : 20
  Distance-URT       : 20
  Flags              : SPT/V6_Islt
  IPv4 Nexthops-URT   : 2
           (1) 10.1.0.2         IF:vlanif 10  NBR:0000.0000.0002.00
           (2) 10.0.0.2         IF:vlanif 20  NBR:0000.0000.0003.00
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:0 Parents:2 Others:0)
           (1)   0000.0000.0002.00
                 Cost  : 0
                 Flags : Parent

           (2)   0000.0000.0003.00
                 Cost  : 0
                 Flags : Parent

0000.0000.0003.00
  Distance           : 10
  Distance-URT       : 10
```

```
   Flags              : SPT/V6_Islt
   IPv4 Nexthops-URT   : 1
             (1) 10.0.0.2         IF:vlanif 10  NBR:0000.0000.0003.00
             (B) 10.1.0.2         IF:vlanif 20  NBR:0000.0000.0002.00
                                 TYPE:LOOP-FREE  PROTECT:LINK
   IPv4 Nexthops-MIGP  : 0
   IPv6 Nexthops       : 0
   Neighbors: 2 (Children:1 Parents:1 Others:0)
             (1)   0000.0000.0002.02
                    Cost  : 10
                    Flags : Child

             (2)  >0000.0000.0001.01
                    Cost  : 10
                    Flags : Parent


                      ISIS(1) Level-2 Shortest Path Tree
                      ----------------------------------
>0000.0000.0001.00
   Distance           : 0
   Distance-URT        : 0
   Flags              : SPT
   IPv4 Nexthops-URT   : 0
   IPv4 Nexthops-MIGP  : 0
   IPv6 Nexthops       : 0
   Neighbors: 2 (Children:2 Parents:0 Others:0)
             (1)   0000.0000.0002.01
                    Cost  : 10
                    Flags : Child

             (2)  >0000.0000.0001.01
                    Cost  : 10
                    Flags : Child

>0000.0000.0001.01
   Distance           : 10
   Distance-URT        : 10
   Flags              : SPT/Direct/Isolate/V6_Islt
   IPv4 Nexthops-URT   : 0
   IPv4 Nexthops-MIGP  : 0
   IPv6 Nexthops       : 0
   Neighbors: 2 (Children:1 Parents:1 Others:0)
             (1)   0000.0000.0003.00
                    Cost  : 0
                            C:0 I:vlanif 10
                    Flags : Adj/Child

             (2)  >0000.0000.0001.00
                    Cost  : 0
                    Flags : Parent

 0000.0000.0002.00
   Distance           : 10
   Distance-URT        : 10
   Flags              : SPT/V6_Islt
   IPv4 Nexthops-URT   : 1
             (1) 10.1.0.2         IF:Meth0/0/1  NBR:0000.0000.0002.00
             (B) 10.0.0.2         IF:vlanif 20  NBR:0000.0000.0003.00
                                 TYPE:LOOP-FREE  PROTECT:LINK
   IPv4 Nexthops-MIGP  : 0
   IPv6 Nexthops       : 0
   Neighbors: 2 (Children:1 Parents:1 Others:0)
             (1)   0000.0000.0002.02
                    Cost  : 10
                    Flags : Child

             (2)   0000.0000.0002.01
                    Cost  : 10
```

```
                   Flags : Parent

0000.0000.0002.01
  Distance            : 10
  Distance-URT        : 10
  Flags               : SPT/Direct/Isolate/V6_Islt
  IPv4 Nexthops-URT   : 0
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
           (1)   0000.0000.0002.00
                   Cost  : 0
                          C:0 I:vlanif 10
                   Flags : Adj/Child

           (2)  >0000.0000.0001.00
                   Cost  : 0
                   Flags : Parent

0000.0000.0002.02
  Distance            : 20
  Distance-URT        : 20
  Flags               : SPT/V6_Islt
  IPv4 Nexthops-URT   : 2
           (1) 10.1.0.2         IF:vlanif 10  NBR:0000.0000.0002.00
           (2) 10.0.0.2         IF:vlanif 20  NBR:0000.0000.0003.00
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:0 Parents:2 Others:0)
           (1)   0000.0000.0002.00
                   Cost  : 0
                   Flags : Parent

           (2)   0000.0000.0003.00
                   Cost  : 0
                   Flags : Parent

0000.0000.0003.00
  Distance            : 10
  Distance-URT        : 10
  Flags               : SPT/V6_Islt
  IPv4 Nexthops-URT   : 1
           (1) 10.0.0.2         IF:vlanif 10  NBR:0000.0000.0003.00
           (B) 10.1.0.2         IF:vlanif 20  NBR:0000.0000.0002.00
                             TYPE:LOOP-FREE   PROTECT:LINK
  IPv4 Nexthops-MIGP  : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
           (1)   0000.0000.0002.02
                   Cost  : 10
                   Flags : Child

           (2)  >0000.0000.0001.01
                   Cost  : 10
                   Flags : Parent
```

Table 7-109 Description of the display isis spf-tree verbose command output

Item	Description
Distance	Cost of the shortest path from the root node to the destination node, excluding the TE tunnel link.
Distance-URT	Cost of the shortest path from the root node to the destination node, including the TE tunnel link.

Item	Description
Flags	Flag: - SPT: The node is in the tree. - Direct: The node is a direct node. - Shortcut: The node is on a shortcut link. - Oload: The node is in Overload state. - Isolate: The node is not in the tree. - MIGP_Islt: The node is not in the MIGP tree. - V6_Islt: The node is not in the IPv6 tree. - Del: The node will be deleted. - Remote: The node is on a tunnel.
IPv4 Nexthops-URT	IPv4 next hop of the node in the unicast routing table.
IPv6 Nexthops	IPv6 next hop of the node in the unicast routing table.
Neighbors	Information about all the neighbors of this node.
Cost	Cost of the link from the root node to this node.
Flags	Relationship with the neighbor: - Parent: The neighbor is a parent node. - Child: The neighbor is a child node.
IF	Name of the outbound interface.
NBR	System ID of the next hop.
TYPE	Traffic protection type: - LOOP-FREE: loop-free protection for the backup next hop
PROTECT	Traffic protection type of IS-IS Auto FRR: - NONE: indicates no protection. - LINK: indicates link protection. - NODE: indicates node protection. - LINK-NODE: indicates link and node protection.

Display the current status statistics of the SPF tree.

```
<HUAWEI> display isis spf-tree statistics
                   Statistics information of SPT for ISIS(100)
                  ------------------------------------------


                              Level-1 Statistics
                              ------------------
Nodes information:
         Total:                          1
         Count of nodes in SPT:                1
         Count of isolate nodes in SPT:       0
         Count of IPv6 isolate nodes in SPT:  0
```

```
        Max Distance of nodes in SPT:        0
Links information:
        Total:                          0
        Count of links from Parent to Son:   0
        Count of links from Son to Parent:   0
        Count of links that just changed:    0
Status of SPF:                          Completed
```

Table 7-110 Description of the display isis spf-tree statistics command output

Item	Description
Total (Nodes information)	Total number of nodes.
Count of nodes in SPT	Number of nodes in the SPF tree.
Count of isolate nodes in SPT	Number of isolated nodes in the network topology.
Count of IPv6 isolate nodes in SPT	Number of isolated IPv6 nodes in the network topology.
Max Distance of nodes in SPT	Maximum distance from the root node to the leaf node.
Total (Links information)	Total number of links.
Count of links from Parent to Son	Number of links from the parent node to the child node.
Count of links from Son to Parent	Number of links from the child node to the parent node.
Count of links that just changed	Number of links that just changed.
Status of SPF	Status of SPF calculation: ● Completed: indicates that SPF calculation is complete. ● Scheduled: indicates that SPF calculation is triggered but does not start. ● Running: indicates that SPF calculation is being performed.

7.6.33 display isis statistics

Function

The **display isis statistics** command displays IS-IS process statistics.

Format

display isis statistics packet [**interface** [*interface-type interface-number*]]

display isis statistics [**updated-lsp** [**history**]] [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **statistics** [[[**updated-lsp** [**history**]] [**level-1** | **level-2** | **level-1-2**]] | **packet**]

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **updated-lsp** and **history** parameters.

Parameters

Parameter	Description	Value
packet	Displays IS-IS packet statistics.	-
interface *interface-type interface-number*	Displays IS-IS packet statistics on a specified interface.	-
updated-lsp	Displays real-time data of received LSPs. By default, statistics about the LSPs received within the last 1 hour are displayed.	-
history	Displays historical data of received LSPs. By default, statistics about the LSPs received within the last 24 hours are displayed.	-
level-1	Displays IS-IS Level-1 statistics.	-
level-2	Displays IS-IS Level-2 statistics.	-
level-1-2	Displays IS-IS Level-1-2 statistics.	-
process-id	Displays statistics in a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays statistics about the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display isis statistics** command to view IS-IS process statistics, including the number of routes learned from other IS-IS devices, number of routes imported from other routing protocols, number of locally generated LSPs, and convergence priorities of IS-IS routes.

Example

Display IS-IS process statistics.

```
<HUAWEI> display isis statistics
                       Statistics information for ISIS(1)
                       ----------------------------------
                               Level-1 Statistics
                               ------------------

Forwarding routes information:
         Total IPV4 Learnt Routes: 0
                         Critical: 0
                         High    : 0
                         Medium  : 0
                         Low     : 0
         Total IPv4 Forwarding Routes: 1
Total IPv6 Learnt Routes: 0
                        Critical: 0
                        High    : 0
                        Medium  : 0
                        Low     : 0
         Total IPv6 Forwarding Routes: 1

Imported routes information:
         IPv4 Imported Routes:
                         Static: 0       Direct: 0
                         ISIS:   0       BGP:    0
                         RIP:    0       OSPF:   0
         IPv6 Imported Routes:
                         Static: 0       Direct: 0
                         ISIS:   0       BGP:    0
                         RIPng:  0       OSPFv3: 0
Number of advertised imported routes:
        IPv4 Imported Routes:   0
        IPv6 Imported Routes:   0

Lsp information:
                  LSP Source ID:          No. of used LSPs
                  0000.0000.0022                  002

                               Level-2 Statistics
                               ------------------

Forwarding routes information:
         Total IPV4 Learnt Routes: 0
                         Critical: 0
                         High    : 0
                         Medium  : 0
                         Low     : 0
         Total IPv4 Forwarding Routes: 1
Total IPv6 Learnt Routes: 0
                        Critical: 0
                        High    : 0
```

```
                   Medium  : 0
                   Low     : 0
        Total IPv6 Forwarding Routes: 1

Imported routes information:
        IPv4 Imported Routes:
                   Static: 0       Direct: 0
                   ISIS:   0       BGP:    0
                   RIP:    0       OSPF:   0
        IPv6 Imported Routes:
                   Static: 0       Direct: 0
                   ISIS:   0       BGP:    0
                   RIPng:  0       OSPFv3: 0
Number of advertised imported routes:
       IPv4 Imported Routes:   0
       IPv6 Imported Routes:   0

Lsp information:
               LSP Source ID:          No. of used LSPs
               0000.0000.0002                001
```

Table 7-111 Description of the display isis statistics command output

Item	Description
Total IPV4 Learnt Routes ● Critical ● High ● Medium ● Low	Number of IPv4 routes learned by IS-IS: ● Critical: indicates the number of IPv4 routes with convergence priority critical. ● High: indicates the number of IPv4 routes with convergence priority high. ● Medium: indicates the number of IPv4 routes with convergence priority medium. ● Low: indicates the number of IPv4 routes with convergence priority low.
Total IPv4 Forwarding Routes	Number of IPv4 routes counted based on the destination address. If there are multiple routes to the same destination, these routes are counted as one route.
Total IPv6 Learnt Routes ● Critical ● High ● Medium ● Low	Number of IPv6 routes learned by IS-IS: ● Critical: indicates the number of IPv6 routes with convergence priority critical. ● High: indicates the number of IPv6 routes with convergence priority high. ● Medium: indicates the number of IPv6 routes with convergence priority medium. ● Low: indicates the number of IPv6 routes with convergence priority low.
Total IPv6 Forwarding Routes	Number of IPv6 routes counted based on the destination address. If there are multiple routes to the same destination, these routes are counted as one route.
IPv4 Imported Routes	Imported IPv4 routes.

Item	Description
Static	Number of imported static routes.
Direct	Number of imported direct routes.
ISIS	Number of imported IS-IS routes.
BGP	Number of imported BGP routes.
RIP	Number of imported RIP routes.
OSPF	Number of imported OSPF routes.
IPv6 Imported Routes	Imported IPv6 routes.
RIPng	Number of imported RIPng routes.
OSPFv3	Number of imported OSPFv3 routes.
LSP Source ID	System ID of the switch that generates the LSP.
No. of used LSPs	Number of used LSPs.
Number of advertised imported routes	Number of imported external routes that are advertised.

Display IS-IS packet statistics.

```
<HUAWEI> display isis statistics packet

                  PDUs information for ISIS(1)
                  ----------------------------
       Sent packets:
       PDU type              Total(packets)
       L1 IIH                2516
       L1 LSP                  84
       L1 CSNP                   8
       L1 PSNP                  44
       L2 IIH                5028
       L2 LSP                  80
       L2 CSNP                   8
       L2 PSNP                  46

       Received packets:
       PDU type              Total(packets)
       L1 IIH               12943
       L1 LSP                 216
       L1 CSNP                 3911
       L1 PSNP                  40
       L2 IIH               14907
       L2 LSP                 206
       L2 CSNP                 3900
       L2 PSNP                  41
```

Table 7-112 Description of the display isis statistics packet command output

Item	Description
PDU type	Packet type.

Item	Description
Total(packets)	Total number of packets.
L1 IIH	Level-1 Hello packets.
L1 LSP	Level-1 LSPs.
L1 CSNP	Level-1 CSNPs.
L1 PSNP	Level-1 PSNPs.
L2 IIH	Level-2 Hello packets.
L2 LSP	Level-2 LSPs.
L2 CSNP	Level-2 CSNPs.
L2 PSNP	Level-2 PSNPs.

7.6.34 display isis traffic-eng advertisements

Function

The **display isis traffic-eng advertisements** command displays latest advertised traffic engineering (TE) information.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display isis traffic-eng advertisements [{ **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** }] * [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng advertisements** [{ **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** }] *

Parameters

Parameter	Description	Value
level-1	Displays TE information in a Level-1 LSDB.	-
level-2	Displays TE information in a Level-2 LSDB.	-

Parameter	Description	Value
level-1-2	Displays TE information in a Level-1 or Level-2 LSDB based on the local node type. That is, if the local node is a Level-1 or Level-2 node, TE information in a Level-1 or Level-2 LSDB is displayed. If the local node is a Level-1-2 node, TE information in Level-1 and Level-2 LSDBs is displayed.	-
lsp-id	Displays TE information in the specified LSP.	The value is in dotted decimal notation. The value ranges from 16 to 20 in ####.####.####.##-## format, such as 0050.0500.5004.00-00.
local	Displays locally advertised TE information.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis traffic-eng advertisements** command to check latest advertised TE information.

Example

Display advertised TE information.

```
<HUAWEI> display isis traffic-eng advertisements
                          TE information for ISIS(1)
                          --------------------------
Level-1 Link State Database
---------------------------
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.0001.00-00* 0x00000001   0x3f57        534           0/0/0
 NLPID      : IPV4
 AREA ADDR  : 00.0005
Level-2 Link State Database
```

```
---------------------------
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.0001.00-00* 0x0000001c   0xf1ec        687           0/0/0
 NLPID      : IPV4
 AREA ADDR  : 00.0005
 Router ID  : 10.1.1.9
+NBR        : 0000.0000.0002.02  COST: 10
    Affinity: 0x00000000
    Interface IP Address:  10.1.1.1
    Physical BW  :      12500 Bytes/sec
    Reservable BW:       6250 Bytes/sec
    Unreserved BW:
    BW Unresrv[0] :       6250 Bytes/sec BW Unresrv[1] :       6250 Bytes/sec
    BW Unresrv[2] :       6250 Bytes/sec BW Unresrv[3] :       6250 Bytes/sec
    BW Unresrv[4] :       6250 Bytes/sec BW Unresrv[5] :       6250 Bytes/sec
    BW Unresrv[6] :       6250 Bytes/sec BW Unresrv[7] :       6250 Bytes/sec
    TE Cost      :         10
    Sub Unreserved BW for Class Type 1:
    BW Unresrv[0] :          0 Bytes/sec BW Unresrv[1] :          0 Bytes/sec
    BW Unresrv[2] :          0 Bytes/sec BW Unresrv[3] :          0 Bytes/sec
    BW Unresrv[4] :          0 Bytes/sec BW Unresrv[5] :          0 Bytes/sec
    BW Unresrv[6] :          0 Bytes/sec BW Unresrv[7] :          0 Bytes/sec
    Bandwidth Constraint Model: Russian Doll
    Bandwidth Constraints:
    BC[0] :       6250 Bytes/sec BC[1] :          0 Bytes/sec
    Local Overbooking Multiplier:
    LOM[0] :        100 %         LOM[1] :        100 %
+NBR        : 0000.0000.0004.00  COST: 10
    Affinity: 0x00000000
    Interface IP Address:  10.3.1.1
    Peer IP Address     :  10.3.1.2
    Physical BW  :      12500 Bytes/sec
    Reservable BW:       6250 Bytes/sec
    Unreserved BW:
    BW Unresrv[0] :       6250 Bytes/sec BW Unresrv[1] :       6250 Bytes/sec
    BW Unresrv[2] :       6250 Bytes/sec BW Unresrv[3] :       6250 Bytes/sec
    BW Unresrv[4] :       6250 Bytes/sec BW Unresrv[5] :       6250 Bytes/sec
    BW Unresrv[6] :       6250 Bytes/sec BW Unresrv[7] :       6250 Bytes/sec
    TE Cost      :         10
    Sub Unreserved BW for Class Type 1:
    BW Unresrv[0] :          0 Bytes/sec BW Unresrv[1] :          0 Bytes/sec
    BW Unresrv[2] :          0 Bytes/sec BW Unresrv[3] :          0 Bytes/sec
    BW Unresrv[4] :          0 Bytes/sec BW Unresrv[5] :          0 Bytes/sec
    BW Unresrv[6] :          0 Bytes/sec BW Unresrv[7] :          0 Bytes/sec
    Bandwidth Constraint Model: Russian Doll
    Bandwidth Constraints:
    BC[0] :       6250 Bytes/sec BC[1] :          0 Bytes/sec
    Local Overbooking Multiplier:
    LOM[0] :        100 %         LOM[1] :        100 %
+SRLG NBR ID: 0000.0000.0004.00
    Interface IP Address: 10.3.1.1
    Neighbor IP Address : 10.3.1.2
    Shared Risk Link Group: 10,20
```

Table 7-113 Description of the display isis traffic-eng advertisements command output

Item	Description
LSPID	LSP ID.
LSP Seq Num	LSP sequence number.
LSP Checksum	LSP checksum.
LSP Holdtime	LSP holdtime.

Item	Description
ATT/P/OL	● ATT: Attach bit ● P: partition bit ● OL: overload bit
NLPID	Network protocol.
AREA ADDR	Area address.
Router ID	Router ID of the switch.
+NBR	System ID of the neighbor with the cost style wide, wide-compatible, or compatible.
COST	Cost.
Affinity:	Affinity attribute of a link.
Interface IP Address	IP address of an interface.
Peer IP Address	Peer IP address of an interface.
Physical BW	Physical bandwidth of a link.
Reservable BW	Reservable bandwidth of a link.
Unreserved BW	Unreserved bandwidth.
Sub Unreserved BW for Class Type 1	Unreserved bandwidth for CT1.
BW Unresrv [x]	Unreserved bandwidth for the link with priority x.
TE Cost	TE cost of a link.
Bandwidth Constraint Model	Bandwidth constraint model used by a link.
Bandwidth Constraints	Bandwidth constraint.
BC[x]	Bandwidth constraint of BCx.
Local Overbooking Multiplier	Local overbooking multiplier.
LOM[x]	Local overbooking multiplier of BCx.
+SRLG NBR ID	System ID of a neighbor in a shared risk link group (SRLG).
Neighbor IP Address	IP address of the neighbor.
Shared Risk Link Group	Shared risk link group. **NOTE** When SRLG is enabled on an interface, TE information contains SRLG information.

7.6.35 display isis traffic-eng link

Function

The **display isis traffic-eng link** command displays IS-IS TE link information.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display isis traffic-eng link [{ **level-1** | **level-2** | **level-1-2** } | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng link** [{ **level-1** | **level-2** | **level-1-2** } | **verbose**] *

Parameters

Parameter	Description	Value
level-1	Displays TE link information on a Level-1 switch.	-
level-2	Displays TE link information on a Level-2 switch.	-
level-1-2	Displays TE link information on a Level-1-2switch.	-
verbose	Displays detailed TE link information.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the IS level is not specified, Level-1-2 TE link information is displayed.

Example

Display IS-IS TE link information.

```
<HUAWEI> display isis traffic-eng link
                         TE information for ISIS(1)
                         --------------------------
Level-2 Link Information
------------------------
 0000.0000.0001.00--> 0000.0000.0001.01    Type: MULACC  LinkID: 10.1.1.1
 0000.0000.0002.00--> 0000.0000.0003.00    Type: P2P     LinkID: 10.3.3.9
 0000.0000.0002.00--> 0000.0000.0001.01    Type: MULACC  LinkID: 10.1.1.1
 0000.0000.0003.00--> 0000.0000.0002.00    Type: P2P     LinkID: 10.2.2.9
 0000.0000.0003.00--> 0000.0000.0004.01    Type: MULACC  LinkID: 10.1.1.2
 0000.0000.0004.00--> 0000.0000.0004.01    Type: MULACC  LinkID: 10.1.1.2
 Total Number of TE Links in Level-2 Area: 6, Num Active: 6
```

Table 7-114 Description of the display isis traffic-eng link command output

Item	Description
Type	Link type: ● MULACC: multi-point access link ● P2P: point-to-point link
LinkID	TE link ID.
Total Number of TE Links in Level-2 Area	Total number of TE links in a Level-2 area.
Num Active	Number of active TE links.

Display detailed IS-IS TE link information.

```
<HUAWEI> display isis traffic-eng link verbose
                         TE information for ISIS(1)
                         --------------------------

Level-2 Link Information
------------------------
 Link Status In CSPF : INACTIVE
 0000.0000.0001.00-->0000.0000.0002.00        Type: P2P     LinkID: 10.2.2.2
         Process ID       :  1          Router ID        :  10.2.2.1
         Area ID          :  2          Admin Group      :  0
         Te Cost          :  10         Igp Cost         :  10
         Max Bandwidth    :  0          Max Res Bandwidth:  0
         Shared Risk Link Group: 20
         BC Model         :  RDM
         DS-TE Mode       :  Non-standard IETF DS-TE Mode

 Link Status In CSPF : INACTIVE
 0000.0000.0002.00-->0000.0000.0001.00        Type: P2P     LinkID: 10.2.2.1
         Process ID       :  1          Router ID        :  10.2.2.2
         Area ID          :  2          Admin Group      :  0
         Te Cost          :  10         Igp Cost         :  10
         Max Bandwidth    :  0          Max Res Bandwidth:  0
         BC Model         :  RDM
         DS-TE Mode       :  Non-standard IETF DS-TE Mode

 Total Number of TE Links in Level-2 Area: 2, Num Active: 0
```

Table 7-115 Description of the display isis traffic-eng link verbose command output

Item	Description
Link Status In CSPF	Link status in CSPF calculation.
Process ID	IS-IS process ID.
Router ID	Router ID.
Area ID	Area ID.
Admin Group	Administrative group.
Te Cost	TE cost.
Igp Cost	IGP cost.
Max Bandwidth	Maximum bandwidth.
Max Res Bandwidth	Maximum reservable bandwidth.
Shared Risk Link Group	Shared risk link group.
BC Model	Bandwidth constraint model.
DS-TE Mode	DS-TE mode, including standard and non-standard DS-TE modes.

7.6.36 display isis traffic-eng network

Function

The **display isis traffic-eng network** command displays IS-IS TE network information.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display isis traffic-eng network [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng network** [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Displays TE network information on a Level-1 router.	-
level-2	Displays TE network information on a Level-2 router.	-
level-1-2	Displays TE network information on a Level-1-2 router.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command does not take effect on P2P networks.

If the IS level is not specified, Level-1-2 TE network information is displayed.

Example

Display IS-IS TE network information.

```
<HUAWEI> display isis traffic-eng network
                          TE information for ISIS(1)
                          --------------------------
Level-2 Network Information
---------------------------
    DIS Router ID   : 10.1.1.9     DIS''s Ip Address          : 10.1.1.1
    Status In CSPF : ACTIVE      Attached Router Count    : 2
    List of Attached Routers
 RouterId : 10.1.1.9   Nbr : 0000.0000.0001.00  Link State : 1
 RouterId : 10.2.2.9   Nbr : 0000.0000.0002.00  Link State : 1
    DIS Router ID   : 10.4.4.9     DIS''s Ip Address          : 10.1.1.2
    Status In CSPF : ACTIVE      Attached Router Count    : 2
    List of Attached Routers
 RouterId : 10.4.4.9   Nbr : 0000.0000.0004.00  Link State : 1
 RouterId : 10.3.3.9   Nbr : 0000.0000.0003.00  Link State : 1
 Total Number of TE Networks in Level-2 Area: 2, Num Active: 2
```

Table 7-116 Description of the display isis traffic-eng network command output

Item	Description
DIS Router ID	Router ID of the DIS.
DIS's Ip Address	IP address of the DIS.
Status In CSPF	Whether CSPF is enabled on the switch.
Attached Router Count	Number of connected switches, including the local switch.
List of Attached Routers	List of connected switches.
RouterId	Router ID of the local switch.
Nbr	IP address of the neighbor.
Link State	Link status.
Total Number of TE Networks in Level-2 Area	Total number of networks on which TE is enabled in a Level-2 area.

7.6.37 display isis traffic-eng statistics

Function

The **display isis traffic-eng statistics** command displays IS-IS TE statistics.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display isis traffic-eng statistics [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng statistics**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID. If no process ID is specified, TE statistics about all IS-IS processes are displayed.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IS-IS TE statistics on the switch, including the IS level, cost style, IS-IS TE level, and IS-IS router ID.

Example

Display IS-IS TE statistics.

```
<HUAWEI> display isis traffic-eng statistics
                          TE information for ISIS(1)
                          --------------------------
TE Statistics Information
-------------------------
 IS-IS System Type                          : Level-1-2
 IS-IS Cost Style Status                    : Wide
 IS-IS Level-1 Traffic Engineering Status   : Disabled
 IS-IS Level-2 Traffic Engineering Status   : Enabled
 IS-IS Router ID                            : 10.1.1.9
```

Table 7-117 Description of the display isis traffic-eng statistics command output

Item	Description
IS-IS System Type	IS level.
IS-IS Cost Style Status	Cost style of the switch.
IS-IS Level-1 Traffic Engineering Status	TE status of a Level-1 router.
IS-IS Level-2 Traffic Engineering Status	TE status of a Level-2 router.
IS-IS Router ID	Router ID of an IS-IS router.

7.6.38 display isis traffic-eng sub-tlvs

Function

The **display isis traffic-eng sub-tlvs** command displays the types of sub-TLVs carrying DS-TE parameters.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

display isis traffic-eng sub-tlvs [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng sub-tlvs**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display isis traffic-eng sub-tlvs** command to check the types of sub-TLVs carrying DS-TE parameters.

Example

Display the types of sub-TLVs carrying DS-TE parameters.

```
<HUAWEI> display isis traffic-eng sub-tlvs
IS-IS(1) SubTlv Information
---------------------------------
 Unreserved sub-pool bandwidth sub-tlv value : 251
 Bandwidth constraint sub-tlv value          : 252
 LO multiplier sub-tlv value                 : 253
```

Table 7-118 Description of the display isis traffic-eng sub-tlvs command output

Item	Description
IS-IS(1) SubTlv Information	Sub-TLV information about IS-IS process 1.
Unreserved sub-pool bandwidth sub-tlv value	Sub-TLV of the unreserved sub-pool bandwidth.
Bandwidth constraint sub-tlv value	Sub-TLV of the bandwidth constraint.
LO multiplier sub-tlv value	Sub-TLV of the local overbooking multiplier.

7.6.39 domain-authentication-mode

Function

The **domain-authentication-mode** command configures an IS-IS routing domain to authenticate received Level-2 packets using the specified authentication mode and password and adds authentication information to Level-2 packets to be sent.

The **undo domain-authentication-mode** command cancels authenticating Level-2 packets and deletes the added authentication information from Level-2 packets.

By default, the system neither encapsulates generated Level-2 packets with authentication information nor authenticates received Level-2 packets.

Format

domain-authentication-mode { **simple** { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } | **md5** { [**cipher**] *plain-cipher-text* | **plain** *plain-text* } } [**ip** | **osi**] [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

domain-authentication-mode keychain *keychain-name* [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

domain-authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

undo domain-authentication-mode

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
simple	Transmits the password in plain text. **NOTICE** Simple authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-

Parameter	Description	Value
plain *plain-text*	Specifies the authentication password in plain text. You can enter only the password in plain text. When you view the configuration file, the password is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters.
cipher *plain-cipher-text*	Specifies the authentication password in cipher text. You can enter the password in plain or cipher text. When you view the configuration file, the password is displayed in cipher text. By default, the password is in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters in plain text or a string of 32 or 48 characters in cipher text. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters in plain text or a string of 20 to 392 characters in cipher text.
md5	Transmits the password that is encrypted using MD5. **NOTICE** MD5 authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
keychain *keychain-name*	Specifies the keychain that changes with time. Currently, IS-IS supports only HMAC-MD5 and HMAC-SHA256 algorithms.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ip	Indicates the IP authentication password. When neither **ip** nor **osi** is specified, the default parameter **osi** is used.	-
osi	Indicates the OSI authentication password. When neither **ip** nor **osi** is specified, the default parameter **osi** is used.	-
snp-packet	Authenticates SNPs.	-
authentication-avoid	Encapsulates generated LSPs but not SNPs with authentication information and authenticates received LSPs but not SNPs.	-
send-only	Encapsulates generated LSPs and SNPs with authentication information, and authenticates received LSPs but not SNPs.	-
all-send-only	Encapsulates generated LSPs and SNPs with authentication information, but does not authenticate received LSPs and SNPs.	-
hmac-sha256	Encapsulates generated packets with the HMAC-SHA256 authentication and a password encrypted by the HMAC-SHA256 algorithm and authenticates received packets.	-
key-id *key-id*	Indicates key ID of the HMAC-SHA256 algorithm.	It is an integer ranging from 0 to 65535.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IS-IS packets to be sent are not encapsulated with authentication information, and the received packets are not authenticated. If a user sends malicious packets to attack a network, information on the entire network may be stolen. Therefore, you can configure IS-IS authentication to improve the network security.

The domain authentication password is encapsulated into Level-2 IS-IS packets. Only the packets that pass the domain authentication can be accepted. Therefore, you can configure IS-IS domain authentication to authenticate Level-2 area.

Precautions

This command is valid in all the topologies in the specified IS-IS process and is only valid for Level-2 or Level-1-2 routers.

By using this command, you can discard all the Level-2 packets whose domain authentication password does not contain the one set through this command. At the same time, IS-IS adds the configured domain authentication password in all the Level-2 packets carrying routing information sent from the local node.

The authentication takes effect on the interface with the password. The port without the password can still receive the LSP and SNP with password.

Example

Set the domain authentication mode to HMAC-SHA256, authentication password to **YsHsjx_202206**, and key ID to **33** to authenticate Level-2 packets.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] domain-authentication-mode hmac-sha256 key-id 33 cipher YsHsjx_202206
```

7.6.40 filter-policy export (IS-IS)

Function

The **filter-policy export** command configures a filtering policy to allow IS-IS to filter the imported routes to be advertised.

The **undo filter-policy export** command cancels the filtering function.

By default, IS-IS does not filter the imported routes to be advertised.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix-list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the imported routes that need to be filtered when the routes are advertised. If this parameter is not specified, all the imported routes to be advertised are filtered.	The value can be **direct**, **static**, **unr**, **rip**, **bgp, ospf**, or another **isis** process.
process-id	Specifies the process ID if *protocol* is **rip**, **ospf**, or another **isis** process.	The value is an integer that ranges from 1 to 65535.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IS-IS and other routing protocols are running on the network, and a boundary router in the IS-IS routing domain has imported routes of other routing protocols, the boundary router will advertise all the imported routes to its IS-IS neighbors by default. To advertise some of the imported routes to neighbors, use the **filter-policy export** command.

Precautions

Running the **filter-policy export** command does not affect the routes on the local device, but only advertises specific imported routes to IS-IS neighbors.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all external routes of the specified routing domain that are imported by IS-IS are advertised to the specified neighbor.

Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all external routes of the specified routing domain that are imported by IS-IS are advertised to the specified neighbor.

Example

Configure IS-IS to filter the imported routes using ACL 2000 before advertising the routes to other switches.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] filter-policy 2000 export
```

7.6.41 filter-policy import (IS-IS)

Function

The **filter-policy import** command configures a filtering policy to allow IS-IS to filter the received routes to be added to the IP routing table.

The **undo filter-policy import** command cancels the filtering function.

By default, IS-IS does not filter the received routes to be added to the IP routing table.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS routing entries need to be added to an IP routing table to guide IP packet forwarding. If an IS-IS routing table has routes destined for a specific network segment, but these routes are not expected to be added to an IP routing table, run the **filter-policy import** command with specified parameters to allow only the needed IS-IS routes to be added to the IP routing table.

Precautions

Running the **filter-policy import** command on a router does not affect LSP flooding and LSDB synchronization on the router, but affects the local IP routing table.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes received by IS-IS are delivered to the IP routing table.

Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all routes received by IS-IS are delivered to the IP routing table.

Example

Configure IS-IS to filter the received routes using ACL 2000 and add the routes matching the filtering conditions to the IP routing table.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] filter-policy 2000 import
```

7.6.42 flash-flood

Function

The **flash-flood** command enables LSP fast flooding to speed up IS-IS network convergence.

The **undo flash-flood** command disables LSP fast flooding.

By default, LSP fast flooding is disabled.

Format

flash-flood [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]] *

undo flash-flood [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]] *

Parameters

Parameter	Description	Value
lsp-count	Specifies the maximum number of LSPs to be flooded at a time on an interface.	The value is an integer that ranges from 1 to 15. The default value is 5.
max-timer-interval *interval*	Specifies the maximum interval for LSP flooding.	The value is an integer that ranges from 10 to 50000, in milliseconds. The default value is 10 ms.
level-1	Enables LSP fast flooding in Level-1. If no level is specified, by default, LSP fast flooding is enabled in both Level-1 and Level-2.	-

Parameter	Description	Value
level-2	Enables LSP fast flooding in Level-2. If no level is specified, by default, LSP fast flooding is enabled in both Level-1 and Level-2.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, when an IS-IS router receives new LSPs from other routers, it updates the LSPs in its LSDB and periodically floods the updated LSPs according to a timer.

LSP fast flooding speeds up LSDB synchronization because it allows a device to flood fewer LSPs than the specified number before route calculation when the device receives one or more new LSPs. This mechanism also speeds up network convergence.

Precautions

You can specify the number of LSPs to be flooded each time. The number is valid for all IS-IS interfaces. If the number of LSPs to be flooded is greater than the specified value, the *lsp-count* number of the LSPs are sent. If the timer is configured and does not time out before route calculation, LSPs are flooded immediately; otherwise, LSPs are flooded when the timer times out.

Example

Enable LSP fast flooding, configure each interface to send a maximum of six LSPs at a time, and set the maximum interval for sending LSPs to 100 ms.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] flash-flood 6 max-timer-interval 100
```

7.6.43 frr (IS-IS)

Function

The **frr** command enables the IS-IS Auto FRR function and displays the IS-IS Auto FRR view.

The **undo frr** command disables the IS-IS Auto FRR function.

By default, the IS-IS Auto FRR function is disabled.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

frr

undo frr

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

With the development of networks, the Voice over IP (VoIP) and on-line video services require high-quality real-time transmission. Nevertheless, if an IS-IS fault occurs, multiple processes, including fault detection, LSP update, LSP flooding, route calculation, and FIB entry delivery, must be performed to switch traffic to a new link. This results in a lengthy traffic interruption, which cannot meet the requirement for real-time services.

IS-IS Auto FRR can fast switch traffic to a backup link, ensuring millisecond-level traffic interruption. This protects traffic and improves IS-IS network reliability.

Precautions

After running this command, run the **loop-free-alternate** command to calculate a loop-free backup route.

Example

Enter the IS-IS FRR view.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] frr
[HUAWEI-isis-1-frr] loop-free-alternate
```

7.6.44 frr-policy route

Function

The **frr-policy route** command configures a filtering policy to allow IS-IS to filter the IS-IS backup routes to be added in the IP routing table.

The **undo frr-policy route** command cancels the filtering function.

By default, IS-IS does not filter the IS-IS backup routes to be added in the IP routing table.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

frr-policy route route-policy *route-policy-name*

undo frr-policy route

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy to filter IS-IS backup routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The filtering policy can be configured as required. In this case, the IS-IS backup route that satisfies specified rules can be added to the IP routing table and delivered to the forwarding table. When a fault occurs on the route, the system can fast switch the forwarded traffic to the IS-IS backup route to protect traffic.

You can use IP prefix lists or ACLs to filter IS-IS backup routes.

Precautions

If you run the **frr-policy route** command multiple times, only the latest configuration takes effect.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, IS-IS adds all backup routes to the IP routing table.

Example

Configure IS-IS to filter IS-IS backup routes using route-policy and add the routes matching the route-policy **abc** to the IP routing table.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] frr
[HUAWEI-isis-1-frr] frr-policy route route-policy abc
```

7.6.45 graceful-restart (IS-IS)

Function

The **graceful-restart** command enables the graceful restart (GR) function for an IS-IS process.

The **undo graceful-restart** command disables the GR function for an IS-IS process.

By default, the GR function is disabled for an IS-IS process.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is valid for all topologies in an IS-IS process.

When an IS-IS process on a device is restarted, neighbors delete neighbor relationships with the device and delete LSPs from the device. As a result, routes of neighbors are calculated incorrectly and packets are lost. Consequently, the network is temporarily interrupted.

To solve this problem, you can enable GR of the IS-IS process by running the **graceful-restart** command.

After the **graceful-restart** command is run, the device can notify its restart status to neighbors and permit neighbors to maintain neighbor relationships. In this manner, nonstop packet forwarding is implemented.

Configuration Impact

If IS-IS GR is enabled on a router, the holdtimes of this router's neighbors are automatically changed to 60s if they are smaller than 60s, and the holdtimes of this router's neighbors are kept unchanged if they are equal to or greater than 60s. If a router is faulty in non-GR scenarios, its neighbors need to take 60 seconds to detect the fault. A large number of packets may be discarded within the 60 seconds.

To resolve this problem, run the **graceful-restart no-impact-holdtime** command to configure the holdtimes of the neighbors to remain unchanged after IS-IS GR is enabled.

Example

Enable the GR function for IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] graceful-restart
```

7.6.46 graceful-restart no-impact-holdtime

Function

The **graceful-restart no-impact-holdtime** command configures the holdtime of an IS-IS neighbor to remain unchanged after IS-IS GR is enabled.

The **undo graceful-restart no-impact-holdtime** command cancels the configuration.

By default, after IS-IS GR is enabled, the holdtime of an IS-IS neighbor is automatically changed to 60s if it is smaller than 60s, and the holdtime of an IS-IS neighbor is kept unchanged if it is equal to or greater than 60s.

Format

graceful-restart no-impact-holdtime

undo graceful-restart no-impact-holdtime

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If IS-IS GR is enabled on a router, the holdtimes of this router's neighbors are automatically changed to 60s if they are smaller than 60s, and the holdtimes of this router's neighbors are kept unchanged if they are equal to or greater than 60s. If a router is faulty in non-GR scenarios, its neighbors need to take 60 seconds to detect the fault. A large number of packets may be discarded within the 60 seconds.

To resolve this problem, run the **graceful-restart no-impact-holdtime** command to configure the holdtimes of the neighbors to remain unchanged after IS-IS GR is enabled. After you run this command, the router can still fast detect neighbor status, implementing rapid network convergence.

Prerequisites

You have run the **graceful-restart (IS-IS)** command in the IS-IS view.

Example

Configure the holdtime of an IS-IS neighbor to remain unchanged after IS-IS GR is enabled.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] graceful-restart
[HUAWEI-isis-1] graceful-restart no-impact-holdtime
```

7.6.47 graceful-restart interval

Function

The **graceful-restart interval** command sets the GR T3 timer.

The **undo graceful-restart interval** command restores the default T3 timer.

By default, the GR T3 timer is 300 seconds.

Format

graceful-restart interval *interval-value*

undo graceful-restart interval

Parameters

Parameter	Description	Value
interval-value	Specifies the GR T3 timer.	The value is an integer that ranges from 30 to 1800, in seconds. Setting a value greater than that of the GR T2 timer specified using the **graceful-restart t2-interval** command is recommended. If the value is smaller than that of the GR T2 timer, the GR may fail.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS GR can be classified into restarting GR and starting GR based on the restart type. The restarting GR is triggered by a master/slave main control board switchover or an IS-IS process restart, while the starting GR is triggered by a restart of the IS-IS-enabled router.

During a restarting GR, the restarter restarts the protocol and starts the T1, T2, and T3 timers at the same time. The value of the T1 timer indicates the longest time during which the GR restarter waits for the LSP from the GR helper. The value of the T2 timer indicates the longest time during which the system waits for the LSDB synchronization. The value of the T3 timer indicates the longest time that a GR lasts. A router disables the T3 timer after the LSDB synchronization ends in all areas. If LSDBs are not synchronized yet when the T3 timer expires, the GR fails.

You can run the **graceful-restart interval** command to adjust the value of the T3 timer so that the LSDB synchronization can end before the T3 timer expires, which prevents the GR failure.

Prerequisites

The GR of the IS-IS process has been enabled using the **graceful-restart** command.

Configuration Impact

If the **graceful-restart interval** command is run on an IS-IS-enabled router, *interval-value* is used as the holdtime of its neighbor during the GR.

Precautions

The **graceful-restart interval** command is applicable only to restarting GRs.

Example

Set the GR interval for IS-IS process 1 to 120 seconds (2 minutes).

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] graceful-restart
[HUAWEI-isis-1] graceful-restart interval 120
```

7.6.48 graceful-restart suppress-sa

Function

The **graceful-restart suppress-sa** command suppresses the suppress-advertisement (SA) bit of the restart TLV.

The **undo graceful-restart suppress-sa** command restores the default setting.

By default, the SA bit of the restart TLV is not suppressed.

Format

graceful-restart suppress-sa

undo graceful-restart suppress-sa

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch that starts for the first time (not including GR) does not maintain the forwarding status. If the switch does not start for the first time, the LSPs generated when the switch run last time may exist in the LSP database of other switches in the network.

The sequence number of the LSP fragment is reinitialized when the switch starts, so the LSPs stored in the LSP database of other switches seem to be newer than the LSPs generated after the switch starts. This leads to the black hole in the network, and the black hole lasts until the switch regenerates its LSPs and advertises the LSPs with the highest sequence number.

If the neighbor suppresses the advertisement of the adjacency relationship to this switch during the switch starting until the switch advertises the updated LSPs, the preceding case can be avoided.

Prerequisites

GR has been enabled for the IS-IS process using the **graceful-restart** command.

Example

Suppress the SA bit in the restart TLV of IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] graceful-restart
[HUAWEI-isis-1] graceful-restart suppress-sa
```

7.6.49 graceful-restart t2-interval

Function

The **graceful-restart t2-interval** command configures a value for the T2 timer during an IS-IS GR.

The **undo graceful-restart t2-interval** command restores the default value of the T2 timer.

By default, the GR T2 timer is 60 seconds.

Format

graceful-restart t2-interval *interval-value*

undo graceful-restart t2-interval

Parameters

Parameter	Description	Value
interval-value	Specifies the value of the T2 timer during the IS-IS GR.	The value is an integer that ranges from 30 to 1800, in seconds. Setting a value smaller than that of the GR T3 timer specified using the **graceful-restart interval** command is recommended.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS GR can be classified into restarting GR and starting GR based on the restart type. The restarting GR is triggered by a master/slave main control board switchover or an IS-IS process restart, while the starting GR is triggered by a restart of the IS-IS-enabled router.

A GR restarter starts the T1 and T2 timers during all GRs. The value of the T1 timer indicates the longest time during which the GR restarter waits for the LSP from the GR helper. The value of the T2 timer indicates the longest time during which the system waits for the LSDB synchronization. The T2 timer is disabled after the LSDB synchronization among Level-1 or Level-2 routers ends. If LSDBs are not synchronized yet when the T2 timer expires, the GR fails.

You can run the **graceful-restart t2-interval** command to adjust the value of the T2 timer so that the LSDB synchronization can end before the T2 timer expires, which prevents the GR failure.

Prerequisites

The GR of the IS-IS process has been enabled using the **graceful-restart** command.

Precautions

If the value of the T2 timer is too small, a GR may fail. Keeping the default value is recommended. If you want to adjust it, configure a value to meet the conditions on the live network.

Example

Set the GR T2 timer of IS-IS process 1 to 120 seconds (2 minutes).

```
<HUAWEI> system-view
```

```
[HUAWEI] isis 1
[HUAWEI-isis-1] graceful-restart
[HUAWEI-isis-1] graceful-restart t2-interval 120
```

7.6.50 import-route (IS-IS)

Function

The **import-route** command configures IS-IS to import routes from other routing protocols.

The **undo import-route** command restores the default setting.

By default, IS-IS does not import routes from other routing protocols.

Format

import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **static** | **direct** | **unr** | **bgp** [**permit-ibgp**] } [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **unr** | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

import-route limit *limit-number* [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

undo import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **static** | **direct** | **unr** | **bgp** [**permit-ibgp**] } [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **unr** | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo import-route limit [*limit-number*] [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

Parameters

Parameter	Description	Value
rip	Indicates that the routing protocol from which routes are imported is RIP.	-
isis	Indicates that the routing protocol from which routes are imported is IS-IS.	-
ospf	Indicates that the routing protocol from which routes are imported is OSPF.	-
process-id	Specifies a process ID. When *protocol* is **rip**, **ospf**, or **isis**, a process ID needs to be specified. The default process ID is 1.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
static	Indicates that the imported routes are active static routes.	-
direct	Indicates that the imported routes are direct routes.	-
unr	Specifies the imported source routing protocol as **unr**. User Network Route (UNR) is allocated if dynamic routing protocols cannot be used when users are getting online.	-
bgp	Indicates that the routing protocol from which routes are imported is BGP.	-
permit-ibgp	Specifies the imported source route as an IBGP route. If you do not configure this parameter, only the EBGP routes are imported.	-
cost-type { **external** | **internal** }	Indicates the cost type of the imported routes. By default, the cost type is **external**. The configuration of this parameter will affect the costs of imported routes. ● If the cost type of an imported route is configured as **external**, the cost of the imported route equals the cost of the original route plus 64. ● If the cost type of an imported route is configured as **internal**, the imported route inherits the cost of the original route. **NOTE** If the cost style of the switch is wide, compatible, or wide-compatible, the cost types of imported routes are not differentiated between **external** and **internal**.	-
cost *cost*	Specifies the cost value of imported routes.	If the cost style of the switch is wide or wide-compatible, the cost value of imported routes ranges from 0 to 4261412864. Otherwise, the value ranges from 0 to 63. The default value is 0.

Parameter	Description	Value
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
level-1	Indicates that routes are imported into Level-1 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-2	Indicates that routes are imported into Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-1-2	Indicates that routes are imported into Level-1 and Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
inherit-cost	Indicates that the original cost value of imported external routes is retained. When IS-IS is configured to retain the original cost value of imported routes, the cost style and cost value cannot be set for the imported routes.	-
limit *limit-number*	Specifies the maximum number of external routes allowed to be imported to the IS-IS area.	The value is an integer ranging from 1 to 10000000.
threshold-alarm	Specifies the alarm threshold for imported routes.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 80.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 70.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IS-IS and other routing protocols are deployed on a network, you can enable the traffic within an IS-IS routing domain to reach a destination outside the IS-IS routing domain using either of the following methods:

- Configure boundary devices in the IS-IS routing domain to advertise default routes to the IS-IS routing domain.
- Configure boundary devices in the IS-IS routing domain to import routes from other routing domains into the IS-IS routing domain.

If there are multiple boundary devices in the IS-IS routing domain, optimal routes destined for another routing domain need to be selected. This requires all devices in the IS-IS routing domain learn all or some external routes. Configure boundary devices in the IS-IS routing domain to import routes from other routing domains into the IS-IS routing domain. Alternatively, run the **route-policy** *route-policy-name* command to import some external routes from other routing domains.

Precautions

When the routes of the other protocols are imported, you can set the cost value and cost style for the imported route. You can also configure IS-IS to retain the original cost value of the imported external route. During route advertisement and route calculation, the original cost values of these routes are used. In this case, the cost style and cost value of the imported routes cannot be set, and static routes cannot be imported.

After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the ISIS routing table. Therefore, use this command with caution.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all routes of the specified routing domain are imported to the IS-IS routing table.

Example

Configure IS-IS to import static routes and set the cost value of the routes to 15.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] import-route static cost 15
```

Configure IS-IS to import OSPF routes and retain the original cost value of the routes.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] import-route ospf inherit-cost
```

7.6.51 import-route isis level-1 into level-2

Function

The **import-route isis level-1 into level-2** command configures route leaking from Level-1 areas to Level-2 areas.

The **undo import-route isis level-1 into level-2** command prohibits route leaking from Level-1 areas to Level-2 areas.

By default, all Level-1 routing information, excluding information about default routes, is leaked to Level-2 areas.

Format

import-route isis level-1 into level-2 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

undo import-route isis level-1 into level-2 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy.	-
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list. Only the routes that match the IP prefix can be leaked to Level-2 areas.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
tag *tag*	Specifies the administrative tag value of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Specifies the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can be shared with the Level-2 area with this parameter, and all Level-1 area direct routing information will be shared with the Level-2 area without this parameter.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS is designed for a hierarchical network. This means that routes of Level-1 areas are leaked to Level-2 areas, whereas routes of Level-2 areas are not leaked to Level-1 areas.

The import-route isis level-1 into level-2 command can be run only on Level-1-2 routers to allow some or no Level-1 routes to be leaked to Level-2 areas. For example, there are two Level-1-2 routers in a Level-1 area. You can run the import-route isis level-1 into level-2 command on one Level-1-2 router to allow some Level-1 routes to be leaked to the Level-2 area, and run the import-route isis level-1 into level-2 command on the other Level-1-2 router to allow the remaining Level-1 routes to be leaked to the Level-2 area. Then, traffic that is sent from the Level-2 area and destined for different network segments in Level-1 area will be forwarded to different Level-1-2 routers. This allows route selection to be controlled.

Precautions

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes in the Level-1 area leak to the Level-2 area.

Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all routes in the Level-1 area leak to the Level-2 area.

Example

Control route leaking from Level-1 areas to Level-2 areas on Level-1-2 routers using filtering policy 2000.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] import-route isis level-1 into level-2 filter-policy 2000
```

7.6.52 import-route isis level-2 into level-1

Function

The **import-route isis level-2 into level-1** command configures route leaking from Level-2 areas to Level-1 areas.

The **undo import-route isis level-2 into level-1** command prohibits route leaking from Level-2 areas to Level-1 areas.

By default, Level-2 routing information is not leaked to Level-1 areas.

Format

import-route isis level-2 into level-1 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

undo import-route isis level-2 into level-1 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy.	-
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list. Only the routes that match the specified IP prefix can be imported.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag value of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Indicates the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can leak to the Level-2 area with this parameter, and all Level-1 area direct routing information is available to the Level-2 area without this parameter.	-
direct allow-up-down-bit	Indicates that the Up or Down bit is used during the leak of directs routes. If **direct allow-up-down-bit** is specified, the direct routes that have already leaked to the Level-1 area have the lowest priority and cannot leak back.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Level-1-2 switches in a Level-1 area are connected to a Level-2 area, Level-1 switches are unable to know the network topology of the Level-2 area, but forward traffic to the nearest Level-1-2 switch (based on the route with the smallest cost). For Level-2 switches, however, this route may not be the optimal one. Therefore, you need to allow some Level-2 routes to be leaked to the Level-1 area to help Level-1 switches select the optimal route for forwarding traffic to the Level 2 area.

To solve the preceding problem, IS-IS provides the route leaking function to enable Level-1 devices to choose the best path for traffic forwarding.

The **import-route isis level-2 into level-1** command can be run only on Level-1-2 routers to allow all or some Level-2 routes to be leaked to the Level-1 area.

Precautions

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes in the Level-2 area leak to the Level-1 area.

Creating an IP prefix list or route-policy before it is referenced is recommended. By default, nonexistent IP prefix lists or route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list or route-policy is referenced using the current command, all routes in the Level-1 area leak to the Level-2 area.

Example

Configure IS-IS to perform route leaking from a Level-2 area to a Level-1 area using filtering policy 2000.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] import-route isis level-2 into level-1 filter-policy 2000
```

7.6.53 isis

Function

The **isis** command starts an IS-IS process and a specified VPN instance, and displays the IS-IS view.

The **undo isis** command deletes a specified IS-IS process.

By default, no IS-IS instance exists on the network.

Format

isis [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo isis *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you configure IS-IS functions and interface-related features, run the **isis** command to create an IS-IS process and enable IS-IS on the interface.

On a large-scale network, if a large number of switches run IS-IS, there will be a huge number of routes, increasing maintenance costs, slowing down route convergence, and affecting network stability. To resolve the problem, you can run the **isis** *process-id* command to start multi-processes to reduce the number of routes to be maintained.

In addition, to ensure that different services are forwarded properly on the network, you can run the **isis vpn-instance** *vpn-instance-name* command to start multiple IS-IS processes on one device to isolate these services.

Follow-up Procedure

After the **isis** command is used to enable an IS-IS process, run the **network-entity** command to set a NET for the switch, and run the **isis enable** command to enable IS-IS on each interface that needs to run IS-IS. You can start IS-IS only when these configurations are completed.

Precautions

One IS-IS process can be bound to only one VPN instance. Multiple IS-IS interfaces can be bound to one VPN instance.

If a VPN instance is deleted, the IS-IS process bound to the VPN instance is deleted.

When creating an IS-IS process, bind it to a VPN instance. An existing IS-IS process cannot be bound to any VPN instance.

Example

Bind IS-IS process 2 to VPN instance **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] isis 2 vpn-instance vpn1
```

7.6.54 isis authentication-mode

Function

The **isis authentication-mode** command configures an IS-IS interface to authenticate Hello packets using the specified mode and password.

The **undo isis authentication-mode** command cancels the authentication and deletes the authentication information in Hello packets.

By default, no authentication information is added to Hello packets and no authentication is performed on received Hello packets.

Format

isis authentication-mode { **simple** | **md5** } { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]

isis authentication-mode keychain *keychain-name* [**level-1** | **level-2**] [**send-only**]

isis authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**send-only**]

undo isis authentication-mode [**level-1** | **level-2**]

undo isis authentication-mode keychain *keychain-name* [**level-1** | **level-2**] [**send-only**]

undo isis authentication-mode { **simple** { **plain** *plain-text* | **cipher** *plain-cipher-text* } | **md5** { **cipher** *plain-cipher-text* | **plain** *plain-text* } } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]

undo isis authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | **cipher** *plain-cipher-text* } [**level-1** | **level-2**] [**send-only**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **keychain** *keychain-name* parameter.

Parameters

Parameter	Description	Value
simple	Indicates that the password is transmitted in plain text. **NOTICE** Simple authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
plain *plain-text*	Indicates that the password is in plain text. Only a plain-text password can be entered. The password in the configuration file is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. In **simple** authentication mode, the value is a string of 1 to 16 characters. In **md5** or **hmac-sha256** authentication mode, the value is a string of 1 to 255 characters.
cipher *plain-cipher-text*	Indicates that the password is in cipher text. A plain-text or cipher-text password can be entered. The password in the configuration file is displayed in cipher text. By default, the password is in cipher text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. In **simple** authentication mode, the value is a string of 1 to 16 characters in plain text or a string of 32 characters in cipher text. In **md5** or **hmac-sha256** authentication mode, the value is a string of 1 to 255 characters in plain text or a string of 20 to 392 characters in cipher text.
md5	Indicates that the password to be transmitted is encrypted using MD5. **NOTICE** MD5 authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-

Parameter	Description	Value
level-1	Indicates Level-1 authentication. When the link type of an IS-IS interface is Level-1-2, if **level-1** and **level-2** are not specified, both Level-1 and Level-2 Hello packets are configured with the authentication mode and password.	-
level-2	Indicates Level-2 authentication. When the link type of an IS-IS interface is Level-1-2, if **level-1** and **level-2** are not specified, both Level-1 and Level-2 Hello packets are configured with the authentication mode and password.	-
ip	Indicates the IP authentication password. This parameter cannot be configured in keychain authentication mode. If parameters **ip** and **osi** are not specified, the parameter **osi** is used by default.	-
osi	Indicates the OSI authentication password. This parameter cannot be configured in **keychain** authentication mode. If parameters **ip** and **osi** are not specified, the parameter **osi** is used by default.	-
send-only	Encapsulates sent Hello packets with authentication information but does not authenticate received Hello packets.	-
keychain *keychain-name*	Indicates that the password is a keychain that changes with time. This parameter takes effect only when *keychain-name* is set using the **keychain** command. Currently, IS-IS supports only HMAC-MD5 and HMAC-SHA256 algorithms.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Parameter	Description	Value
hmac-sha256	Encapsulates generated packets with the HMAC-SHA256 authentication and a password encrypted by the HMAC-SHA256 algorithm and authenticates received packets.	-
key-id *key-id*	Indicates key ID of the HMAC-SHA256 algorithm.	It is an integer ranging from 0 to 65535.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve network security, authenticate received packets or encapsulate sent packets with authentication information. Only the packets that pass the authentication can be transmitted on the network.

You can use the **isis authentication-mode** command to discard the Hello packets whose authentication passwords are different from the authentication password configured using this command. At the same time, IS-IS adds the configured interface authentication password into all the Hello packets sent from the local node.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If a broadcast interface is emulated as a P2P interface using the **isis circuit-type** command and then restored to the broadcast interface using the **undo isis circuit-type** command, the authentication configuration of the IS-IS area is restored to the default setting.

Example

Set HMAC-SHA256 authentication password **YsHsjx_202206** key id **33** on VLANIF100

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis authentication-mode hmac-sha256 key-id  33 cipher YsHsjx_202206
```

Set HMAC-SHA256 authentication password **YsHsjx_202206** key id **33** GE0/0/1

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis authentication-mode hmac-sha256 key-id  33 cipher YsHsjx_202206
```

7.6.55 isis bfd

Function

The **isis bfd** command sets values of BFD session parameters on a specified IS-IS interface.

The **undo isis bfd** command restores the default values of BFD session parameters on a specified IS-IS interface.

By default, BFD session parameters use default values.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis bfd { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } *

undo isis bfd { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } *

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Specifies the minimum interval for receiving BFD packets from the peer end.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
min-tx-interval *transmit-interval*	Specifies the minimum interval for transmitting BFD packets to the peer end.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Specifies the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.
frr-binding	Binds the BFD session status to IS-IS Auto FRR. When BFD detects the link fault on an interface, the BFD session goes Down, triggering FRR on the interface. After that, the traffic is switched from the faulty link to the backup link, which protects the traffic.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can quickly detect faults on links. Configure proper parameters based on the actual network situation to improve the IS-IS convergence speed when network faults occur. You can use the **isis bfd** command to change BFD session parameters such as the minimum interval for sending BFD packets, minimum interval for receiving BFD packets, and local detection multiplier.

In an IS-IS process, after IS-IS establishes a BFD session, the value of *receive-interval* is obtained after the negotiation of the local **min-rx-interval** value and the remote **min-tx-interval** value. If no BFD packet is received from the peer end within the specified period (*receive-interval* x *multiplier-value*), the neighbor is considered Down.

Negotiation principle: Actual interval for the local device to receive BFD packets = MAX {local **min-rx-interval** value, remote **min-tx-interval** value}

Prerequisites

BFD has been enabled globally. In the interface view, IS-IS has been enabled and BFD has been enabled on the interface using the **isis bfd enable** command.

Precautions

The BFD priority of the interface is higher than that of the process. If BFD of the interface is enabled, the BFD session is set up based on the BFD parameters on the interface.

Example

Enable BFD on VLANIF100 and set the minimum receive interval to 600 ms and local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis bfd enable
[HUAWEI-Vlanif100] isis bfd min-rx-interval 600 detect-multiplier 4
```

Enable BFD on GE0/0/1 and set the minimum receive interval to 600 ms and local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis bfd enable
[HUAWEI-GigabitEthernet0/0/1] isis bfd min-rx-interval 600 detect-multiplier 4
```

7.6.56 isis bfd block

Function

The **isis bfd block** command prevents an IS-IS interface from dynamically establishing a BFD session.

The **undo isis bfd block** command restores the default setting.

By default, an interface can dynamically establish a BFD session.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis bfd block

undo isis bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can provide millisecond-level fault detection, help IS-IS rapidly detect the faults that occur on neighboring devices or links, and instruct IS-IS to recalculate routes for correct packet forwarding. If the network contains unstable links that do not require high reliability and BFD has been enabled, a link cannot transmit data normally when it flaps. You can use the **isis bfd block** command to prevent specified interfaces from dynamically establishing BFD sessions.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If the **isis bfd block**, **isis bfd enable**, and **isis bfd static** commands are executed, only the last command takes effect.

Example

Prevent VLANIF100 from dynamically establishing a BFD session.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis bfd block
```

Prevent GE0/0/1 from dynamically establishing a BFD session.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis bfd block
```

7.6.57 isis bfd enable

Function

The **isis bfd enable** command enables BFD on a specified IS-IS interface.

The **undo isis bfd enable** command disables BFD on a specified IS-IS interface.

By default, BFD is not enabled on an IS-IS interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis bfd enable

undo isis bfd enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can provide millisecond-level fault detection, help IS-IS to detect the faults that occur on neighboring devices or links more rapidly, and instruct IS-IS to recalculate routes for correct packet forwarding. The **isis bfd enable** command can be used to enable BFD on a specified IS-IS interface and establish BFD sessions by using default parameters.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If global BFD is not enabled, you can configure BFD parameters on an interface but cannot establish a BFD session.

The BFD priority of the interface is higher than the BFD priority of the process. If BFD of the interface is enabled, the BFD session is set up based on the BFD parameters on the interface.

If the **isis bfd block**, **isis bfd enable**, and **isis bfd static** commands are run, only the last command takes effect.

Example

Enable BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis bfd enable
```

Enable BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis bfd enable
```

7.6.58 isis bfd static

Function

The **isis bfd static** command enables static BFD on a specified IS-IS interface.

The **undo isis bfd static** command disables static BFD on a specified IS-IS interface.

By default, static BFD is disabled on an IS-IS interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis bfd static

undo isis bfd static

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In static BFD, BFD session parameters are set manually and BFD session establishment requests are delivered manually. Then static BFD can quickly detect faults on links. You can run the **isis bfd static** command to enable static BFD on a specified interface to establish static BFD sessions on specified links.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If the **isis bfd block**, **isis bfd enable**, and **isis bfd static** commands are run, only the last command takes effect.

Example

Enable static BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis bfd static
```

Enable static BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis bfd static
```

7.6.59 isis circuit-level

Function

The **isis circuit-level** command sets the link type of an interface on a Level-1-2 router.

The **undo isis circuit-level** command restores the default link type of an interface on a Level-1-2 router.

By default, the link type of an interface on a Level-1-2 router is Level-1-2, and both Level-1 and Level-2 neighbor relationships can be established on the interface.

Format

isis circuit-level [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

Parameters

Parameter	Description	Value
level-1	Specifies the Level-1 link type. That is, only Level-1 neighbor relationship can be established on the interface.	-
level-1-2	Specifies the Level-2 link type. That is, both Level-1 and Level-2 neighbor relationships can be established on the interface.	-
level-2	Specifies the Level-2 link type. That is, only Level-2 neighbor relationship can be established on the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an adjacency is established between a Level-1-2 router and a remote device, the Level-1-2 router sends and receives both Level-1 and Level-2 Hello packets, wasting bandwidth and memory resources. To solve this problem, run the **isis circuit-level** command to set a specified link type for an interface.

Prerequisites

IS-IS has been enabled using the **isis enable** command in the interface view.

Precautions

Network flapping may occur if the link type of an IS-IS interface is changed during network operation. Therefore, setting a link type for an IS-IS interface on the switch when configuring IS-IS is recommended.

The configuration of the **isis circuit-level** command takes effect only when the IS-IS system type is Level-1-2. Otherwise, the level configured using the **is-level** command is used as the link type.

Example

If VLANIF100 is connected to a non-backbone router in the same area, set this interface to Level-1, and prohibit the interface from sending and receiving Level-2 Hello packets.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis circuit-level level-1
```

If GE0/0/1 is connected to a non-backbone router in the same area, set this interface to Level-1, and prohibit the interface from sending and receiving Level-2 Hello packets.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis circuit-level level-1
```

7.6.60 isis circuit-type

Function

The **isis circuit-type** command simulates the network type of an IS-IS broadcast interface to a P2P interface.

The **undo isis circuit-type** command restores the default network type of an IS-IS interface.

By default, the network type of an interface is determined by the physical type of the interface.

Format

isis circuit-type p2p [**strict-snpa-check**]

undo isis circuit-type

Parameters

Parameter	Description	Value
p2p	Sets the network type of an IS-IS interface to P2P.	-
strict-snpa-check	Enables IS-IS to check the SNPA address of each received LSP or SNP.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network type of IS-IS interfaces at the ends of the link must be identical. Otherwise, the two interfaces cannot set up the neighbor relationship. In most cases, the network types of interfaces on a broadcast network and a P2P network are Ethernet and P2P respectively.

The **isis circuit-type** command sets the network type of an interface to simulate a P2P interface so that the network type of IS-IS interfaces at the ends of the link is identical and the neighbor relationship can be established between them.

When an IS-IS neighbor relationship is established between a P2P interface and a simulated P2P interface and the simulated P2P interface has direct neighbors, the P2P interface may receive unneeded packets from these direct neighbors. To prevent the P2P interface from accepting these unneeded packets, specify **strict-snpa-check** in the **isis circuit-type** command to enable IS-IS to check the SNPA address of each received LSP or SNP. After the command is run, the P2P interface accepts only the packets whose SNPA addresses are included in the local neighbor address list, which improves network security.

Precautions

For an interface enabled with IS-IS using the **isis enable** command, when the network type of an interface changes, the corresponding configurations change. Details are as follows:

- After a broadcast interface is simulated as a P2P interface using the **isis circuit-type** command, the interval for sending Hello packets, the number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down, interval for resending LSP packets on a P2P link, and various IS-IS authentication modes are restored to the default settings; other configurations such as the DIS priority, DIS name, and interval for sending CSNP packets on a broadcast network become invalid.
- After the **undo isis circuit-type** command is run to restore the network type of an IS-IS interface, the interval for sending Hello packets, the number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down, interval for resending LSP packets on a P2P link, various IS-IS authentication modes, DIS priority, and interval for sending CSNP packets on a broadcast network are restored to the default settings.

Example

Set the network type of VLANIF100 to P2P.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis circuit-type p2p
```

Set the network type of GE0/0/1 to P2P.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis circuit-type p2p
```

7.6.61 isis cost

Function

The **isis cost** command sets the link cost value of an IS-IS interface.

The **undo isis cost** command restores the default link cost value of an IS-IS interface.

By default, the link cost value of an IS-IS interface is 10.

Format

isis cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo isis cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the link cost value of an interface.	The value is an integer that varies according to the cost style. - When the cost style is **narrow**, **narrow-compatible**, or **compatible**, the value ranges from 1 to 63. - When the cost style is **wide** or **wide-compatible**, the value ranges from 1 to 16777214. The default value is 10.
maximum	Sets the link cost of IS-IS interfaces to 16777215. **NOTE** You can configure this parameter only when the IS-IS cost style is wide or wide-compatible. After the interface cost is set to 16777215, the neighbor TLV generated on the link can only be used to transmit TE information but cannot be used for route calculation.	-
level-1	Specifies the link cost value of a Level-1 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-

Parameter	Description	Value
level-2	Specifies the link cost value of a Level-2 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On large networks, there may be multiple valid routes to the same destination. IS-IS uses the SPF algorithm to calculate an optimal route and transmits traffic over it, which brings the following problems:

- All traffic is transmitted over the optimal route, causing load imbalance.
- If the optimal route is faulty, traffic will get lost.

To solve the preceding problems, run the **isis cost** command to set a link cost for interfaces so that traffic can be transmitted over different physical links.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Configuration Impact

If the link cost of an interface is changed, routes will be re-calculated on the whole network, causing the changes in traffic forwarding paths.

Precautions

The priority of the **circuit-cost** command is lower than that of the **isis cost** command.

Example

Set the Level-2 link cost of VLANIF100 to 5.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis cost 5 level-2
```

Set the Level-2 link cost of GE0/0/1 to 5.

```
<HUAWEI> system-view
[HUAWEI] isis
```

```
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis cost 5 level-2
```

7.6.62 isis delay-peer

Function

The **isis delay-peer** command configures a delay for an interface so that the interface delays establishing neighbor relationships after the neighbor relationship with the last neighbor goes Down due to packet timeout.

The **undo isis delay-peer** command deletes the configured delay and restores the default configurations.

By default, if the neighbor relationship goes Down due to packet timeout, the interface re-establishes the neighbor relationship after it receives a new Hello packet.

Format

isis delay-peer track last-peer-expired [**delay-time** *delay-interval*]

undo isis delay-peer [**track last-peer-expired** [**delay-time** *delay-interval*]]

Parameters

Parameter	Description	Value
track	Tracks the mode of the neighbor relationship establishment delay.	-
last-peer-expired	Indicates that neighbor relationship establishment is delayed after the neighbor relationship with the last neighbor goes Down due to packet timeout.	-
delay-time *delay-interval*	Specifies the neighbor relationship establishment delay.	The value is an integer ranging from 1 to 3600, in seconds. The default value is 60 seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On IS-IS networks, devices at both ends of a link establish a neighbor relationship by exchanging Hello packets. After the neighbor relationship is established, both devices need to send Hello packets at a specified interval to maintain the neighbor relationship. If an IS-IS device does not receive any Hello packets from the neighbor at the other end within the specified period (Holddown time), the local device considers the neighbor Down and re-establishes the neighbor relationship after it receives a new Hello packet. If links are unstable or some Hello packets are lost or incorrect due to network transmission delay or poor transmission, neighbor relationships may alternate between Up and Down frequently, which causes a route flapping.

To address this issue, run the **isis delay-peer** command to configure a neighbor relationship establishment delay after the neighbor relationship goes Down.

Pre-configuration Tasks

IS-IS has been enabled using the **isis enable** command in the interface view.

Precautions

If a new *delay-interval* is configured and it is less than the remaining time of the ongoing delay, the new *delay-interval* takes effect immediately; if the new *delay-interval* is greater than the remaining time of the ongoing delay, the ongoing delay continues until the new *delay-interval* takes effect at the next delay.

Example

Set the delay to 100s on VLANIF100 so that the neighbor relationship establishment is delayed after the neighbor relationship with the last neighbor goes Down due to packet timeout.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis delay-peer track last-peer-expired delay-time 100
```

Set the delay to 100s on GE0/0/1 so that the neighbor relationship establishment is delayed after the neighbor relationship with the last neighbor goes Down due to packet timeout.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis delay-peer track last-peer-expired delay-time 100
```

7.6.63 isis dis-name

Function

The **isis dis-name** command configures a host name for the DIS.

The **undo isis dis-name** command deletes the host name configured for the DIS.

By default, no host name is configured for the DIS.

Format

isis dis-name *symbolic-name*

undo isis dis-name

Parameters

Parameter	Description	Value
symbolic-name	Specifies a host name for the DIS.	The value is a string of 1 to 64 characters without spaces. It is case sensitive. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can configure the name for the DIS on an interface only after you run the **isis enable** command to enable IS-IS on the interface. The DIS name is advertised in a pseudo-node LSP. In this manner, the configured DIS name is associated with the system ID of the DIS.

NOTE

This command takes effect only on the DIS in the broadcast network.

If the **isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis dis-name** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the **isis dis-name** command becomes valid on the interface.

Example

Configure a host name for the DIS on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
```

```
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis dis-name LOCALAREA
```

Configure a host name for the DIS on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis dis-name LOCALAREA
```

7.6.64 isis dis-priority

Function

The **isis dis-priority** command sets the priority of the IS-IS interface that is a candidate for the DIS at a specified level.

The **undo isis dis-priority** command restores the default priority.

By default, the DIS priority of broadcast IS-IS interfaces at Level-1 and Level-2 is 64.

Format

isis dis-priority *priority* [**level-1** | **level-2**]

undo isis dis-priority [*priority*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
priority	Specifies the priority for DIS election.	The value is an integer that ranges from 0 to 127. The default value is 64. A larger value indicates a higher DIS priority.
level-1	Indicates the DIS priority of interfaces at Level 1. If the level is not specified, the same priority is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the DIS priority of interfaces at Level 2. If the level is not specified, the same priority is set for Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The configuration is useful only for the broadcast network.

The DIS priority is advertised through Hello packets. The switch with the highest priority is elected as the DIS. In the case of the same priority, the switch with the largest MAC address is elected as the DIS.

NOTE

IS-IS has been enabled on the interface using the **isis enable** command.

If the **isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis dis-priority** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the **isis dis-priority** command becomes valid on the interface.

Example

Set the Level-2 priority for electing the DIS to 127 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis dis-priority 127 level-2
```

Set the Level-2 priority for electing the DIS to 127 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis dis-priority 127 level-2
```

7.6.65 isis enable

Function

The **isis enable** command enables IS-IS on an interface and specifies the ID of the IS-IS process to be associated with the interface.

The **undo isis enable** command disables IS-IS on an interface and cancels the ID of the IS-IS process associated with the interface.

By default, IS-IS is disabled on an interface.

Format

isis enable [*process-id*]

undo isis enable

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an IS-IS process is configured in the system view, to make the IS-IS protocol function normally, enable IS-IS on an interface to associate the interface with the IS-IS process.

Prerequisites

An IS-IS process has been enabled using the **isis** command in the system view.

Precautions

An interface can be associated with only one IS-IS process.

Example

Create IS-IS process 1 and activate the process on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] network-entity 10.0001.1010.1020.1030.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
```

Create IS-IS process 1 and activate the process on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] network-entity 10.0001.1010.1020.1030.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
```

7.6.66 isis lfa-backup

Function

The **isis lfa-backup** command enables an IS-IS interface to participate in loop-free alternate (LFA) calculation so that the interface can be a candidate for a backup interface.

The **undo isis lfa-backup** command disables an IS-IS interface from participating in LFA calculation.

By default, an IS-IS interface can participate in LFA calculation.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

isis lfa-backup [**level-1** | **level-2** | **level-1-2**]

undo isis lfa-backup [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Indicates that an interface can be a backup interface in Level-1 areas.	-
level-2	Indicates that an interface can be a backup interface in Level-2 areas.	-
level-1-2	Indicates that an interface can be a backup interface in both Level-1 and Level-2 areas.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

To facilitate traffic management and avoid the uncertainty in the traffic forwarding path in the case the primary link fails, run the **undo isis lfa-backup** command on some interfaces to disable them from participating in LFA calculation.

IS-IS has been enabled on the interface using the **isis enable** command.

Example

Disable VLANIF100 from becoming a backup interface for IS-IS Auto FRR.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] undo isis lfa-backup
```

Disable GE0/0/1 from becoming a backup interface for IS-IS Auto FRR.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] undo isis lfa-backup
```

7.6.67 isis lsp seq-overflow auto-recover disable

Function

The **isis lsp seq-overflow auto-recover disable** command prevents an IS-IS system from changing its system ID when it receives a locally generated LSP with the maximum sequence number (0xFFFFFFFF).

The **undo isis lsp seq-overflow auto-recover disable** command restores the default configuration.

By default, an IS-IS system changes its system ID when it receives a locally generated LSP with the maximum sequence number.

Format

isis lsp seq-overflow auto-recover disable

undo isis lsp seq-overflow auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, if a device receives a locally generated LSP with the sequence number greater than that of the corresponding LSP stored locally, the device adds 1 to the sequence number of the received LSP and floods it. An attacker may send an IS-IS LSP with the maximum sequence number (0xFFFFFFFF) and the system ID of a target device. Upon receipt of the LSP, the target device considers it a locally generated LSP because it carries the local system ID and adds 1 to the sequence number because the sequence number is greater than that of the corresponding LSP stored locally. Consequently, the sequence number exceeds the maximum number, causing the target device to enter the hibernation state. The state can last 18 hours and 1 minute, affecting network operation. To prevent this problem, an IS-IS system changes its system ID when it receives a locally generated LSP with the sequence number of 0xFFFFFFFF. However, if the IS-IS system has changed its system ID for three times within 24 hours when it receives one more such an LSP, it directly enters the hibernation state.

The preceding function also applies to CSNPs and PSNPs.

By default, an IS-IS system changes its system ID when it receives a locally generated LSP with the maximum sequence number. To disable this function, run the **isis lsp seq-overflow auto-recover disable** command.

Example

Prevent an IS-IS system from changing its system ID when it receives a locally generated LSP with the maximum sequence number (0xFFFFFFFF).

```
<HUAWEI> system-view
[HUAWEI] isis lsp seq-overflow auto-recover disable
```

7.6.68 isis mesh-group

Function

The **isis mesh-group** command adds an IS-IS interface to a specified mesh group.

The **undo isis mesh-group** command deletes an IS-IS interface from a specified mesh group.

By default, an IS-IS interface does not belong to any mesh group and floods LSPs normally.

Format

isis mesh-group { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

Parameters

Parameter	Description	Value
mesh-group-number	Specifies the mesh group number.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
mesh-blocked	Blocks an interface to prevent it from flooding received LSPs to other interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving LSPs, the interface, not in the mesh group, floods the LSPs to other interfaces following the normal procedure. For the NBMA network that is with higher connectivity and several P2P links, this process causes repeated LSP flooding and wastes bandwidth.

After receiving LSPs, the interface that joins a mesh group only floods the LSPs to the interfaces that are not in the local mesh group.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

When adding interfaces to mesh groups or blocking interfaces, keep certain interfaces from being configured with the isis mesh-group command. This can prevent link faults from affecting the normal spreading of LSPs.

Example

Add VLANIF100 to mesh group 3.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis mesh-group 3
```

Add GE0/0/1 to mesh group 3.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis mesh-group 3
```

7.6.69 isis padding-hello

Function

The **isis padding-hello** command configures an IS-IS interface to send Hello packets with the padding field.

The **undo isis padding-hello** command restores the default setting.

By default, an IS-IS interface is not configured to send Hello packets with the padding field.

Format

isis padding-hello

undo isis padding-hello

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **isis padding-hello** and **isis small-hello** commands are mutually exclusive and cannot be configured on the same interface simultaneously.

If an interface that is not configured with the two commands, it sends Hello packets based on the following rules:

- For a P2P interface
  - Before the P2P neighbor relationship is established, the P2P interface sends Hello packets with the padding field.
  - After the P2P neighbor relationship is established, the P2P interface sends Hello packets without the padding field.

  NOTE

  For a P2P interface, the length of the padding field is equal to the length of LSP packets generated by the local IS.
- For a broadcast interface

  It sends Hello packets with the padding field.

  NOTE

  For a broadcast interface, the length of padding field is equal to the length of MTU.

IS-IS has been enabled on the interface using the **isis enable** command.

Example

Configure VLANIF100 to send Hello packets with the padding field.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis padding-hello
```

Configure GE0/0/1 to send Hello packets with the padding field.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis padding-hello
```

7.6.70 isis peer-ip-ignore

Function

The **isis peer-ip-ignore** command configures IS-IS not to check the IP address of Hello packets received by an interface.

The **undo isis peer-ip-ignore** command restores the default setting.

By default, IS-IS checks the IP address of received Hello packets.

Format

isis peer-ip-ignore

undo isis peer-ip-ignore

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IS-IS checks the IP address carried in the Hello packet. The neighbor relationship can be set up only when the local interface address and the interface address carried in the received packets belong to the same network segment. When the two interface IP addresses are not in the same network segment, if the **isis peer-ip-ignore** command is used, the check on the peer IP address is ignored, and the two IS-IS interfaces can set up normal neighbor relationship. Routes of this two network segments exist in the routing table, but cannot ping through each other.

Precautions

This command is valid for P2P interfaces, NBMA interfaces and the interface with the network type configured to P2P by using the **isis circuit-type p2p** command. The command takes effect only when the command is used on the two ends of the link.

NOTE

- For the broadcast interface, you can run the **isis peer-ip-ignore** command only after you run the **isis circuit-type p2p** command. The **isis circuit-type p2p** command is valid only for the broadcast interface.
- For the P2P and NBMA interfaces, you can run the **isis peer-ip-ignore** command without running the **isis circuit-type p2p** command.

Example

Configure VLANIF100 not to check the IP address of the Hello packets sent by the peer.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis circuit-type p2p
[HUAWEI-Vlanif100] isis peer-ip-ignore
```

Configure GE0/0/1 not to check the IP address of the Hello packets sent by the peer.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis circuit-type p2p
[HUAWEI-GigabitEthernet0/0/1] isis peer-ip-ignore
```

7.6.71 isis ppp-negotiation

Function

The **isis ppp-negotiation** command specifies the PPP negotiation mode for establishing neighbor relationships.

The **undo isis ppp-negotiation** command restores the default negotiation mode.

By default, the 3-way handshake mode is used.

Format

isis ppp-negotiation { **2-way** | **3-way** [**only**] }

undo isis ppp-negotiation

Parameters

Parameter	Description	Value
2-way	Establishes the neighbor relationship using the 2-way handshake negotiation mode.	-
3-way	Establishes the neighbor relationship using the 3-way handshake negotiation mode.	-
only	Establishes the neighbor relationship using the 3-way handshake negotiation mode that is not backward compatible.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The 3-way handshake negotiation mode is backward compatible. If the neighbor only supports 2-way handshake, use the 2-way handshake negotiation mode to establish a neighbor relationship.

The command is applicable only for P2P interfaces. It can be used on the broadcast interfaces only after the circuit type is set to P2P.

Example

Establish the neighbor relationship on VLANIF100 using the 2-way handshake negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis circuit-type p2p
[HUAWEI-Vlanif100] isis ppp-negotiation 2-way
```

Establish the neighbor relationship on GE0/0/1 using the 2-way handshake negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] isis
```

```
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis circuit-type p2p
[HUAWEI-GigabitEthernet0/0/1] isis ppp-negotiation 2-way
```

7.6.72 isis ppp-osicp-check

Function

The **isis ppp-osicp-check** command enables OSICP negotiation check on a PPP interface. The negotiation status can affect IS-IS interface status.

The **undo isis ppp-osicp-check** command restores the default setting.

By default, IS-IS does not check OSICP status of PPP.

Format

isis ppp-osicp-check

undo isis ppp-osicp-check

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, OSCIP status of PPP does not affect IS-IS interface status.

After this command is configured, OSI network negotiation status of PPP can affect IS-IS interface status. When PPP senses that the OSI network fails, the link status of the IS-IS interface turns Down and the route to the network segment where the interface resides is not advertised through LSP.

Precautions

This command applies to only PPP interfaces. For other point-to-point interfaces, this command is invalid.

Example

Configure VLANIF100 to check OSICP status of PPP.

```
<HUAWEI> system-view
[HUAWEI] isis
```

```
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis circuit-type p2p
[HUAWEI-Vlanif100] isis ppp-osicp-check
```

Configure GE0/0/1 to check OSICP status of PPP.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis circuit-type p2p
[HUAWEI-GigabitEthernet0/0/1] isis ppp-osicp-check
```

7.6.73 isis purge-lsp auto-protect disable

Function

The **isis purge-lsp auto-protect disable** command disables IS-IS purge LSPs from triggering master/slave main control board switchovers.

The **undo isis purge-lsp auto-protect disable** command restores the default configuration.

By default, IS-IS purge LSPs trigger master/slave main control board switchovers.

Format

isis purge-lsp auto-protect disable

undo isis purge-lsp auto-protect disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an IS-IS process on a device proactively sends a purge LSP, the device deletes the corresponding LSP and floods it to the network. In most cases, before the device sends a purge LSP, the end that generated the corresponding LSP sends an updated LSP. If the clock on the device runs fast, the device frequently floods purge LSPs to devices on the entire network, causing network flapping. If the device generates more than five purge LSPs for 80% or more non-pseudonode LSPs with a non-zero fragment number in the local LSDB within 6500s, a master/

slave main control board switchover is performed if the device has two main control boards, or the device is restarted if it has only one main control board. The switchover or restart prevents network flapping.

By default, IS-IS purge LSPs trigger master/slave main control board switchovers. To disable IS-IS purge LSPs from triggering master/slave main control board switchovers, run the **isis purge-lsp auto-protect disable** command.

Example

Disable IS-IS purge LSPs from triggering master/slave main control board switchovers.

```
<HUAWEI> system-view
[HUAWEI] isis purge-lsp auto-protect disable
```

7.6.74 isis silent

Function

The **isis silent** command configures an IS-IS interface as a silent interface. That is, the interface is suppressed from sending and receiving IS-IS packets, but routes of the network segment on which the interface resides can be advertised.

The **undo isis silent** command restores the default setting.

By default, no IS-IS interface is configured as a silent interface.

Format

isis silent [**advertise-zero-cost**]

undo isis silent

Parameters

Parameter	Description	Value
advertise-zero-cost	Specifies the route cost as 0. The default cost of IS-IS routes is 10.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IS-IS network is connected to other ASs, it is required to enable IS-IS on the interfaces that connect the IS-IS network to other ASs so that the switch on the IS-IS network can learn the routes to other ASs. This interface, however, unnecessarily advertises IS-IS Hello packets on its network segment. In this case, you can run the **isis silent** command to suppress the IS-IS interface.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Example

Configure VLANIF100 as a silent interface.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis silent
```

Configure GE0/0/1 as a silent interface.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis silent
```

7.6.75 isis small-hello

Function

The **isis small-hello** command configures an IS-IS interface to send Hello packets without the padding field.

The **undo isis small-hello** command restores the default setting.

By default, an IS-IS interface is not configured to send Hello packets without the padding field.

Format

isis small-hello

undo isis small-hello

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The command can simplify the operations of sending and receiving Hello packets.

The **isis small-hello** and **isis padding-hello** commands are mutually exclusive and cannot be configured on the same interface simultaneously.

If an interface is not configured with the two commands, it sends Hello packets based on the following rules:

- P2P interface
  - Before the P2P neighbor relationship is established, the P2P interface sends Hello packets with the padding field.
  - After the P2P neighbor relationship is established, the P2P interface sends Hello packets without the padding field.

  NOTE

  For a P2P interface, the length of the padding field is equal to the length of LSP packets generated by the local IS.
- Broadcast interface

  The interface sends Hello packets with the padding field.

  NOTE

  For a broadcast interface, the length of padding field is equal to the length of MTU.

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Example

Configure VLANIF100 to send Hello packets without the padding field.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis small-hello
```

Configure GE0/0/1 to send Hello packets without the padding field.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis small-hello
```

7.6.76 isis suppress-flapping peer

Function

The **isis suppress-flapping peer** command configures detection parameters for IS-IS neighbor relationship flapping suppression.

The **undo isis suppress-flapping peer** command restores the default detection parameters.

By default, the detection interval of IS-IS neighbor relationship flapping suppression is 60s, the suppression threshold is 10, and the interval for exiting from suppression is 120s.

Format

isis suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

undo isis suppress-flapping peer { **detecting-interval** [*detecting-interval*] | **threshold** [*threshold*] | **resume-interval** [*resume-interval*] } *

Parameters

Parameter	Description	Value
detecting-interval *detecting-interval*	Specifies the detection interval of IS-IS neighbor relationship flapping suppression. Each IS-IS interface on which IS-IS neighbor relationship flapping suppression is enabled starts a flapping counter. If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count is incremented by 1.	The value is an integer ranging from 1 to 300, in seconds. The default value is 60s.
threshold *threshold*	Specifies the threshold of IS-IS neighbor relationship flapping suppression. When the flapping-count reaches or exceeds *threshold*, flapping suppression takes effect.	The value is an integer ranging from 1 to 1000. The default value is 10.

Parameter	Description	Value
resume-interval *resume-interval*	- Specifies the interval for exiting from IS-IS neighbor relationship flapping suppression. If the interval between two successive neighbor status changes from Full to a non-Full state is longer than *resume-interval*, the flapping-count is reset. - If IS-IS neighbor relationship flapping suppression works in hold-max-cost mode, *resume-interval* indicates the duration of this mode. **NOTE** The value of *resume-interval* must be greater than that of *detecting-interval*.	The value is an integer ranging from 2 to 1000, in seconds. The default value is 120s.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure detection parameters for IS-IS neighbor relationship flapping suppression on an interface, run the **isis suppress-flapping peer** command. However, keeping the default configurations is recommended.

Prerequisites

IS-IS neighbor relationship flapping suppression must have been enabled globally before you configure detection parameters for it. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the detection parameters.

Example

Set the detection interval of IS-IS neighbor relationship flapping suppression to 5s, the suppression threshold to 40, and the interval for exiting from suppression to 20s on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis suppress-flapping peer detecting-interval 5 threshold 40 resume-interval 20
```

7.6.77 isis suppress-flapping peer disable

Function

The **isis suppress-flapping peer disable** command disables IS-IS neighbor relationship flapping suppression from an interface.

The **undo isis suppress-flapping peer disable** command enables IS-IS neighbor relationship flapping suppression on an interface.

By default, IS-IS neighbor relationship flapping suppression is enabled on all interfaces.

Format

isis suppress-flapping peer disable

undo isis suppress-flapping peer disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IS-IS neighbor relationship flapping suppression is enabled on all interfaces in the same IS-IS process. To disable the function from one of the interfaces, run the **isis suppress-flapping peer disable** command.

NOTE

When an interface enters the flapping suppression state, all neighbor relationships on the interface enter the state accordingly.

Prerequisites

IS-IS neighbor relationship flapping suppression must have been enabled globally before you enable the function on an interface using the **undo isis suppress-flapping peer disable** command. By default, the function is enabled globally. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it first.

Example

Disable IS-IS neighbor relationship flapping suppression from VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis suppress-flapping peer disable
```

7.6.78 isis suppress-flapping peer hold-down

Function

The **isis suppress-flapping peer hold-down** command configures the Hold-down mode and sets duration for this mode.

The **undo isis suppress-flapping peer hold-down** command cancels the Hold-down mode.

By default, the Hold-down mode is disabled.

Format

isis suppress-flapping peer hold-down *interval*

undo isis suppress-flapping peer hold-down [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the duration of the Hold-down mode.	The value is an integer ranging from 1 to 600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use the maximum value (16777214 for the wide mode and 63 for the narrow mode) as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **isis suppress-flapping peer hold-down** *interval* command.

Prerequisites

IS-IS neighbor relationship flapping suppression must have been enabled globally before you configure the Hold-down mode and set duration for this mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the Hold-down mode and set duration for this mode.

Example

Configure the Hold-down mode and set its duration to 200s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis suppress-flapping peer hold-down 200
```

7.6.79 isis suppress-flapping peer hold-max-cost disable

Function

The **isis suppress-flapping peer hold-max-cost disable** command disables the Hold-max-cost mode.

The **undo isis suppress-flapping peer hold-max-cost disable** command enables the Hold-max-cost mode.

By default, the Hold-max-cost mode is enabled.

Format

isis suppress-flapping peer hold-max-cost disable

undo isis suppress-flapping peer hold-max-cost disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use the maximum value (16777214 for the wide mode and 63 for the narrow mode) as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link. If a device on a key path is isolated from the network due to IS-IS neighbor relationship flapping, the network is separated into two isolated parts. To prevent this problem, use the Hold-max-cost mode on the key path.

If the neighbor relationship does not go Down within successive **resume-interval**s, or the interval between two successive neighbor Down events is greater than or equal to **resume-interval**, the suppression in Hold-max-cost mode exits.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **isis suppress-flapping peer hold-down** *interval* command.

Precautions

The Hold-max-cost mode takes effect only unidirectionally. If a remote device does not support IS-IS neighbor relationship flapping suppression, bidirectional traffic between the local and remote devices may travel along different paths.

Example

Disable the Hold-max-cost mode on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis suppress-flapping peer hold-max-cost disable
```

7.6.80 isis suppress-reachability

Function

The **isis suppress-reachability** command suppresses the advertisement of direct routes on an IS-IS interface in a specified topology.

The **undo isis suppress-reachability** command restores the default setting.

By default, direct routes on an IS-IS interface are advertised.

Format

isis suppress-reachability [**level-1** | **level-1-2** | **level-2**]

undo isis suppress-reachability

Parameters

Parameter	Description	Value
level-1	Indicates that the advertisement of IPv4 addresses is suppressed on Level-1 interfaces. If the level is not specified, the advertisement of IPv6 addresses on Level-1 and Level-2 interfaces is suppressed.	-
level-1-2	Indicates that the advertisement of IPv4 addresses is suppressed on Level-1 and Level-2 interfaces.	-
level-2	Indicates that the advertisement of IPv4 addresses is suppressed on Level-2 interfaces. If the level is not specified, the advertisement of IPv4 addresses is suppressed on Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Example

Suppress the advertisement of IPv4 addresses on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis suppress-reachability
```

Suppress the advertisement of IPv4 addresses on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis suppress-reachability
```

7.6.81 isis system-id auto-recover disable

Function

The **isis system-id auto-recover disable** command disables the system from automatically resolving IS-IS system ID conflicts.

The **undo isis system-id auto-recover disable** command enables the system to automatically resolve IS-IS system ID conflicts.

By default, if the system detects an IS-IS system ID conflict, it automatically changes the local system ID to resolve the conflict.

Format

isis system-id auto-recover disable

undo isis system-id auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A system ID uniquely identifies an IS-IS device. If the same system ID is configured for more than one device on the network, a routing loop may occur. By default, if the system detects an IS-IS system ID conflict, it automatically changes the local system ID to resolve the conflict.

To disable the system from automatically resolving IS-IS system ID conflicts, run the **isis system-id auto-recover disable** command. After the command is run, IS-IS system ID conflicts need to be manually resolved.

NOTE

The first two bytes of the system ID automatically changed by the system are Fs, and the last four bytes are randomly generated. For example, FFFF:1234:5678 is such a system ID.

Precautions

If an IS-IS system ID conflict occurs between two directly connected devices, a neighbor relationship fails to be established only between the two devices, without affecting the entire network. As a result, the conflict is not automatically resolved in this case.

On broadcast networks, the system ID generated automatically is not recorded in the configuration file. If the device is restarted, the system restores this system ID to the originally configured one and then generates another one, which may be different from the one last generated automatically. If the conflict persists after the system automatically generates three system IDs, the system no longer resolves this conflict.

Example

Disable the system to automatically resolve IS-IS system ID conflicts.

```
<HUAWEI> system-view
[HUAWEI] isis system-id auto-recover disable
```

7.6.82 isis tag-value

Function

The **isis tag-value** command sets the administrative tag value of an IS-IS interface.

The **undo isis tag-value** command deletes the administrative tag value on an IS-IS interface.

By default, an IS-IS interface has no administrative tag value.

Format

isis tag-value *tag* [**level-1** | **level-2**]

undo isis tag-value [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag of an IS-IS interface.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates the administrative tag value of a Level-1 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the administrative tag value of a Level-2 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrative tag carries administrative information about IP address prefixes. The tag can be used to import routes of different levels and different areas. Administrative tags can advertise IP address prefixes in an IS-IS routing domain to control routes and simplify management.

Using the **isis tag-value** command, you can set the administrative tag value for all routes of a specified IS-IS process. The tag can be used as a filtering condition of a route-policy to filter routes.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

The advertised LSPs contain the administrative tag value only when the IS-IS cost style is wide, wide-compatible, or compatible.

The administrative tag value set using the **isis tag-value** command has a higher priority than the administrative tag value set using the **circuit default-tag** command.

Example

Set the administrative tag value of VLANIF100 to 77.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis tag-value 77
```

Set the administrative tag value of GE0/0/1 to 77.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis tag-value 77
```

7.6.83 isis timer csnp

Function

The **isis timer csnp** command sets the interval for sending CSNPs on a broadcast network.

The **undo isis timer csnp** command restores the default setting.

By default, the interval for sending CSNPs on a broadcast network is 10 seconds.

Format

isis timer csnp *csnp-interval* [**level-1** | **level-2**]

undo isis timer csnp [*csnp-interval*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
csnp-interval	Specifies the interval for sending CSNPs on a broadcast network.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 10 seconds.
level-1	Indicates the interval for sending Level-1 CSNPs. If no level is specified, the interval for the IS-IS process of the current level to send CSNP packets is set by default.	-
level-2	Indicates the interval for sending Level-2 CSNPs. If no level is specified, the interval for the IS-IS process of the current level to send CSNP packets is set by default.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a broadcast network, a DIS sends CSNPs periodically to enable all devices to synchronize LSDBs with one another. If a device finds that the local LSDB does not have a specific LSP or an existing LSPs is not the latest one after the device has received a CSNP, the device will send a PSNP to request the corresponding LSP. Only a DIS sends CSNPs periodically. Therefore, the **isis timer csnp** command will take effect only on a broadcast interface of the DIS. This command can be used to set an interval for sending CSNPs in an area at a specified level. A router may be elected as a DIS in both Level-1 and Level-2 areas. Therefore, you can set different intervals at which the DIS sends CSNPs in Level-1 and Level-2 areas.

Precautions

The IS-IS route convergence speed depends on the LSDB synchronization speed. Therefore, reducing the interval for sending CSNPs can speed up LSDB synchronization and IS-IS route convergence. If the interval is set too small, however, the DIS will send CSNPs frequently. This causes high CPU, memory, and network bandwidth usage and affects services.

NOTE

If the **isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis timer csnp** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the interval for sending CSNPs is restored to the default setting.

Example

Set the interval for sending Level-2 CSNPs to 15 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer csnp 15 level-2
```

Set the interval for sending Level-2 CSNPs to 15 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer csnp 15 level-2
```

7.6.84 isis timer hello

Function

The **isis timer hello** command sets the interval for sending Hello packets on an IS-IS interface.

The **undo isis timer hello** command restores the default setting.

By default, the interval for sending Hello packets 10 seconds on an interface.

Format

isis timer hello *hello-interval* [**level-1** | **level-2**] [**conservative**]

undo isis timer hello [*hello-interval*] [**level-1** | **level-2**] [**conservative**]

Parameters

Parameter	Description	Value
hello-interval	Specifies the interval for sending Hello packets.	The value is an integer that ranges from 3 to 255, in seconds. The default value is 10 seconds.
level-1	Indicates the interval for sending Level-1 Hello packets. If the level is not specified, the interval for sending Level-1 and Level-2 Hello packets is set by default.	-
level-2	Indicates the interval for sending Level-2 Hello packets. If the level is not specified, the interval for sending Level-1 and Level-2 Hello packets is set by default. **NOTE** Parameters **level-1** and **level-2** are configured only on a broadcast interface that is enabled with IS-IS. Level-1 and Level-2 Hello packets are sent separately and their intervals must be set respectively. There is only one Hello packet on a point-to-point link. Therefore, level-1 and level-2 parameters are not used.	-
conservative	Indicates the conservative mode of the dead timer. If the conservative mode is configured, the value configured for the dead timer takes effect even when the value is less than 10s.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS maintains neighbor relationships between neighbors by sending and receiving Hello packets. If the local device does not receive Hello packets from its neighbor within a specified period, the device considers the neighbor Down.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

The shorter the interval, the more system resources used to send Hello packets. The interval should therefore be set according to the actual conditions.

If a broadcast interface is emulated as a P2P interface through the **isis circuit-type** command or then restored to the broadcast interface through the **undo isis circuit-type** command, the interval for sending IS-IS Hello packets is restored to the default value.

Example

Set the interval for sending Level-2 Hello packets to 20 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer hello 20 level-2
```

Set the interval for sending Level-2 Hello packets to 20 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer hello 20 level-2
```

7.6.85 isis timer holding-multiplier

Function

The **isis timer holding-multiplier** command sets the multiplier of the interval for sending Hello packets to change the holdtime of IS-IS neighbor relationship.

The **undo isis timer holding-multiplier** command restores the default setting.

By default, the multiplier of the interval for sending Hello packets is 3, that is, the neighbor holdtime is three times the interval for sending Hello packets.

Format

isis timer holding-multiplier *number* [**level-1** | **level-2**]

undo isis timer holding-multiplier [*number*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
number	Indicates that the neighbor holdtime is a multiplier of the interval for sending Hello packets.	The value is an integer that ranges from 3 to 1000. The default value is 3.
level-1	Indicates the holdtime of Level-1 neighbors. If the level is not specified, the holdtime is set for both Level-1 and Level-2 neighbors.	-
level-2	Indicates the holdtime of Level-2 neighbors. If the level is not specified, the holdtime is set for both Level-1 and Level-2 neighbors. **NOTE** Parameters **level-1** and **level-2** are configured only on a broadcast interface that is enabled with IS-IS. Level-1 and Level-2 Hello packets are sent separately and their intervals must be set respectively. There is only one Hello packet on a point-to-point link. Therefore, level-1 and level-2 parameters are not used.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Devices at both ends of a link establish a neighbor relationship by sending Hello packets to each other. After the neighbor relationship is established, both devices need to send Hello packets at a specified interval to maintain the neighbor relationship. If a device does not receive any Hello packet from its neighbor within a specified period of time, the device considers the neighbor to be Down. The specified time period is known as the neighbor holdtime.

For example, run the **isis timer hello** command on a local device to set the interval for sending Hello packets to 20s. Then, run the **isis timer holding-multiplier** 4 command. The holdtime is 80s (four times the interval for sending Hello packets). If the interval for sending Hello packets is changed using the **isis timer hello** 20 command, the holdtime will be changed accordingly.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If the *number* value is set too large, the local device needs to wait a long time before detecting that the remote device has gone Down. This slows down IS-IS route convergence. If the value of *number* is set too small, the neighbor relationship will alternate between **Up** and **Down** when some Hello packets are lost due to transmission delays and errors on the network. This causes route flapping on the IS-IS network. Therefore, exercise caution when setting the value of *number*. Set the same interval for sending Hello packets and the same neighbor holdtime for all devices on the IS-IS network is recommended. This is to ensure that all devices detect link failures at the same time and guarantee timely IS-IS route convergence.

If a broadcast interface is emulated as a P2P interface through the **isis circuit-type** command or then restored to the broadcast interface through the **undo isis circuit-type** command, the number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down is restored to the default value.

Example

Set the number of Level-2 Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down to 6 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer holding-multiplier 6 level-2
```

Set the number of Level-2 Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down to 6 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer holding-multiplier 6 level-2
```

7.6.86 isis timer lsp-retransmit

Function

The **isis timer lsp-retransmit** command sets the interval for retransmitting LSPs over a P2P link.

The **undo isis timer lsp-retransmit** command restores the default value.

By default, the interval for retransmitting LSPs over a P2P link is 5 seconds.

Format

isis timer lsp-retransmit *retransmit-interval*

undo isis timer lsp-retransmit

Parameters

Parameter	Description	Value
retransmit-interval	Specifies the interval for retransmitting LSPs.	The value is an integer that ranges from 1 to 300.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a point-to-point network, devices at both ends of a link synchronize LSDBs with each other by flooding LSPs. The device at one end of the link sends an LSP. If the device at the other end receives this LSP, it replies with a PSNP. If the device that has sent an LSP does not receive a PSNP from the other end in a period of time, the device will retransmit the LSP.

The **isis timer lsp-retransmit** command is used to set an interval for retransmitting LSPs. Only the devices on a point-to-point network send PSNPs. Therefore, the **isis timer lsp-retransmit** command will take effect only when it is run on point-to-point interfaces.

Precautions

After the **isis timer lsp-retransmit** command is run on a device, the device will wait *retransmit-interval* after having sent an LSP. If the device receives a PSNP from the other end, the device will not retransmit the LSP. Otherwise, the device will retransmit the LSP.

If the value of *retransmit-interval* is set too small, an LSP will be retransmitted even though it is not necessary, causing high CPU, memory, and network bandwidth usage.

NOTE

If a broadcast interface is emulated as a P2P interface through the **isis circuit-type** command or restored a P2P interface to the broadcast interface through the **undo isis circuit-type** command, the interval for retransmitting LSP packets on a P2P link is restored to the default value.

Example

Set the interval for retransmitting LSPs on VLANIF100 to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis circuit-type p2p
[HUAWEI-Vlanif100] isis timer lsp-retransmit 10
```

Set the interval for retransmitting LSPs on GE0/0/1 to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis circuit-type p2p
[HUAWEI-GigabitEthernet0/0/1] isis timer lsp-retransmit 10
```

7.6.87 isis timer lsp-throttle

Function

The **isis timer lsp-throttle** command sets the minimum interval for sending LSPs on an IS-IS interface and the maximum number of LSPs sent within the interval.

The **undo isis timer lsp-throttle** command restores the default setting.

By default, the minimum interval for sending LSPs on an IS-IS interface is 50 milliseconds and the maximum number of LSPs sent within the interval is 10.

Format

isis timer lsp-throttle *throttle-interval* [**count** *count*]

undo isis timer lsp-throttle

Parameters

Parameter	Description	Value
throttle-interval	Specifies the minimum interval for sending LSPs.	The value is an integer that ranges from 1 to 10000, in milliseconds.
count *count*	Specifies the maximum number of LSPs that are sent within the interval specified by *throttle-interval*.	The value is an integer that ranges from 1 to 1000.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The value specified by *throttle-interval* is the interval between two consecutive LSPs and is also the interval for sending multiple fragments of a CSNP.

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Example

Set the interval for retransmitting LSPs on VLANIF100 to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer lsp-throttle 500
```

Set the interval for retransmitting LSPs on GE0/0/1 to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer lsp-throttle 500
```

7.6.88 is-level

Function

The **is-level** command sets the level of an IS-IS switch.

The **undo is-level** command restores the default setting.

By default, the level of an IS-IS switch is Level-1-2.

Format

is-level { **level-1** | **level-1-2** | **level-2** }

undo is-level

Parameters

Parameter	Description	Value
level-1	Indicates that the level of the switch is Level-1. The switch calculates only intra-area routes and maintains the Level-1 LSDB.	-

Parameter	Description	Value
level-1-2	Indicates that the level of the switch is Level-1-2. The switch calculates Level-1 and Level-2 routes and maintains Level-1 and Level-2 LSDBs.	-
level-2	Indicates that the level of the switch is Level-2. The switch calculates only Level-2 routes, and maintains the Level-2 LSDB.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To support a network with a large number of routes, IS-IS uses a two-level structure in an IS-IS routing domain. IS-IS switches are classified into the following levels:

- Level-1 switch: A Level-1 switch manages intra-area routing. It establishes neighbor relationships with only Level-1 and Level-1-2 switches in the same area. Level-1 switches can be connected to other areas through Level-1-2 switches only.
- Level-2 switch: A Level-2 switch manages intra-area routing. It establishes neighbor relationships with Level-2 switches in the same area and Level-1-2 switches in other areas only. All Level-2 switches form the backbone network of the routing domain. They are responsible for communications between areas. The Level-2 switches in the routing domain must be reachable, and no switch of other levels is deployed between every two Level-2 switches.
- Level-1-2 switch: A Level-1-2 switch can establish Level-1 neighbor relationships with Level-1 switches and Level-1-2 switches in the same area. It can also establish Level-2 neighbor relationships with Level-2 switches and Level-1-2 switches in other areas.

In most cases, Level-1 switches are located within an area, Level-2 switches are located between areas, and Level-1-2 switches are located between Level-1 switches and Level-2 switches.

The level of an IS-IS switch and of an interface determine the level of a neighbor relationship. By default, neighbor relationships between two Level-1-2 switches are Level-1 and Level-2. To establish a Level-1 or Level-2 neighbor relationship, run the **isis circuit-level** command to modify the level of interfaces.

If only one area exists, setting the level of switches to Level-1 or Level-2 is recommended to prevent devices from maintaining two LSDBs that are the same. On an IP network, setting the level of all switches to Level-2 for future extension is recommended.

Precautions

- If the levels of IS-IS switches are changed during network operation, the IS-IS process will be restarted and IS-IS neighbor relationships will be disconnected. Setting the levels of switches when configuring IS-IS is recommended.
- If the **is-level** command is not configured for a switch, the switch works at Level-1-2. That is, the switch calculates Level-1 and Level-2 routes and maintains Level-1 and Level-2 LSDBs simultaneously.
- When both Level-1 and Level-2 switches have routes destined for the same destination address, the route on the Level-1 switch is preferred.

Example

Set the level of the current switch to Level-1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] is-level level-1
```

7.6.89 is-name

Function

The **is-name** command enables the capability of identifying the host name in an LSP and configures the dynamic host name for the IS-IS system of the local switch. The dynamic hostname is advertised in an LSP packet.

The **undo is-name** command deletes the dynamic host name configured for the IS-IS system of the local switch.

By default, the IS-IS system of the local switch has no dynamic host name.

Format

is-name *symbolic-name*

undo is-name [*symbolic-name*]

Parameters

Parameter	Description	Value
symbolic-name	Specifies a dynamic host name.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

In most cases, to check information about IS-IS neighbors and LSDBs on an IS-IS switch, you need to use a system ID of a 12-digit hexadecimal number, for example, aaaa.eeee.1234. This representation, however, is complicated and not easy to use. The dynamic host name mapping mechanism is introduced to facilitate maintenance and management of IS-IS networks. The **is-name** command is used to configure a simple host name for a local switch and enables the switch to advertise it in an LSP.

After the configuration is completed, you can run the **display isis name-table** command to check the configured hostname.

Example

Configure host name **RUTA** for the local IS-IS system.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] is-name RUTA
```

7.6.90 is-name map

Function

The **is-name map** command enables the local switch to identify the host name in LSPs, and sets a static host name for a remote IS-IS system on the local switch.

The **undo is-name map** command disables the local switch from identifying the host name in LSPs, and deletes the static host name for a remote IS-IS system set by the local switch.

By default, the local switch does not identify the host name in LSPs, and has no static host name of a remote IS-IS system.

Format

is-name map *system-id symbolic-name*

undo is-name map *system-id* [*symbolic-name*]

Parameters

Parameter	Description	Value
system-id	Specifies the ID of the remote mapped IS-IS system or pseudonode ID.	The format is XXXX.XXXX.XXXX[.XX].

Parameter	Description	Value
symbolic-name	Specifies the static host name of the remote mapped IS-IS system.	The value is a string of 1 to 64 characters without spaces. It is case sensitive. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When checking information about IS-IS neighbors and LSDBs on the switch that runs IS-IS, each switch in the IS-IS routing domain is represented by a system ID with a 12-bit hexadecimal number, for example, aaaa.eeee.1234. This representation is complicated and not easy to use. To manage and maintain IS-IS networks conveniently, IS-IS uses the dynamic host name exchange mechanism. The **is-name map** command can configure a host name for the remote switch and does not advertise the host name through an LSP.

After running the **is-name map** command to map the remote switch to the host name, you can find that the system ID of the remote switch is replaced by the host name configured using the **display isis name-table** command.

Precautions

This configuration is static configuration and takes effect only on the local device. Therefore, the configured host name *symbolic-name* is not advertised through an LSP. If dynamic host name mapping is configured on an IS-IS device, dynamic host name mapping takes precedence over static host name mapping.

Example

Configure static host name mapping for the IS-IS system on the remote switch as 0000.0000.0041.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] is-name map 0000.0000.0041 RUTB
```

7.6.91 log-peer-change

Function

The **log-peer-change** command enables the output of IS-IS adjacency changes.

The **undo log-peer-change** command disables the output of IS-IS adjacency changes.

By default, the output of IS-IS adjacency changes is disabled.

Format

log-peer-change [**topology**]

undo log-peer-change

Parameters

Parameter	Description	Value
topology	Enables the output of the IS-IS adjacency changes in an IPv6 topology.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, IS-IS adjacency changes pose a threat to network stability, causing frequent route convergence which consumes a lot of memory resources and possible traffic loss. Therefore, diagnose the fault immediately when the IS-IS adjacency changes.

To locate the fault, run the **log-peer-change** command to enable the output of IS-IS adjacency changes and record the changes in the log.

Precautions

IS-IS adjacency changes are recorded only when the **terminal monitor** and **log-peer-change** commands are run.

Example

Enable the output of IS-IS adjacency changes on the current switch.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] log-peer-change
```

7.6.92 loop-free-alternate

Function

The **loop-free-alternate** command enables IS-IS Auto FRR to calculate loop-free backup routes using the loop-free alternate (LFA) algorithm.

The **undo loop-free-alternate** command disables IS-IS Auto FRR from calculating loop-free backup routes using the LFA algorithm.

By default, IS-IS Auto FRR is disabled from calculating loop-free backup routes using the LFA algorithm.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

loop-free-alternate [**level-1** | **level-2** | **level-1-2**]

undo loop-free-alternate [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables Level-1 IS-IS Auto FRR to generate loop-free backup routes. If the IS level is not specified, Level-1 and Level-2 IS-IS Auto FRR is enabled to generate backup routes.	-
level-2	Enables Level-2 IS-IS Auto FRR to generate loop-free backup routes. If the IS level is not specified, Level-1 and Level-2 IS-IS Auto FRR is enabled to generate backup routes.	-
level-1-2	Enables Level-1 and Level-2 IS-IS Auto FRR to generate loop-free backup routes.	-

Views

IS-IS FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS Auto FRR pre-computes a backup link by using the Loop-Free Alternate (LFA) algorithm, and then adds the backup link and the primary link to the forwarding table. In the case of an IS-IS network failure, IS-IS Auto FRR can fast switch traffic to the backup link before routes on the control plane converge.

Precautions

To make IS-IS Auto FRR to take effect, enter the IS-IS FRR view and then run the **loop-free-alternate** command.

IS-IS can generate loop-free backup routes only when the IS-IS Auto FRR traffic protection inequality is met.

Example

Enable Level-2 IS-IS Auto FRR to generate loop-free backup routes.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] frr
[HUAWEI-isis-1-frr] loop-free-alternate level-2
```

7.6.93 lsp-fragments-extend

Function

The **lsp-fragments-extend** command enables LSP fragment extension on the IS-IS switch.

The **undo lsp-fragments-extend** command disables LSP fragment extension on the IS-IS switch.

By default, LSP fragment extension is disabled on the IS-IS switch.

Format

lsp-fragments-extend [[**level-1** | **level-2** | **level-1-2**] | [**mode-1** | **mode-2**]] *

undo lsp-fragments-extend [**mode-1** | **mode-2**] [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables LSP fragment extension on a Level-1 switch.	-
level-2	Enables LSP fragment extension on a Level-2 switch.	-

Parameter	Description	Value
level-1-2	Enables LSP fragment extension on a Level-1-2 switch.	-
mode-1	Indicates that the switch supporting LSP fragment extension is compatible with the switch with an earlier version that does not support LSP fragment extension.	-
mode-2	Requires that all the switches support LSP fragment extension. **NOTE** By default, **mode-1** and **level-1-2** are used.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

To enable the IS-IS switch to generate extended LSP fragments, run the **virtual-system** command to configure at least one virtual system ID.

After the **lsp-fragments-extend** command is run, run the **reset isis all** command to restart the IS-IS process to make LSP fragment extension take effect.

Example

Enable Level-2 LSP fragment extension in mode 1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] lsp-fragments-extend mode-1 level-2
```

7.6.94 lsp-length

Function

The **lsp-length** command sets the length of the LSP that is generated and received by the current IS-IS switch.

The **undo lsp-length** command restores the default setting.

By default, the IS-IS switch generates and receives 1497-byte LSPs.

Format

lsp-length { **originate** | **receive** } *max-size*

undo lsp-length { **originate** | **receive** }

Parameters

Parameter	Description	Value
originate	Indicates the maximum length of generated LSPs.	-
receive	Indicates the maximum length of received LSPs.	-
max-size	Specifies the maximum length of LSPs. The *max-size* of a generated LSP must be smaller than or equal to the *max-size* of a received LSP.	The value is an integer that ranges from 512 to 16384, in bytes. The default value is 1497. **NOTE** Because the maximum MTU supported by interfaces is 9600 bytes and the LSP header length is 3 bytes, the allowed maximum LSP length is 9597 (9600 – 3) bytes to ensure that two devices on both ends communicate properly.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By controlling the length of LSPs generated and received by IS-IS switches, you can adjust the LSDB synchronization speed and change the network convergence speed.

Precautions

The *max-size* set using the **lsp-length** command must meet the following requirements:

- The MTU of an Ethernet interface must be greater than or equal to the sum of the value of *max-size* and 3.
- The MTU of a P2P interface must be greater than or equal to the value of *max-size*.

Example

Set the maximum length of an LSP generated by the IS-IS switch to 1024 bytes.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] lsp-length originate 1024
```

7.6.95 maximum load-balancing (IS-IS)

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for load balancing. You need to set the maximum value according to memory capacity.

The **undo maximum load-balancing** command restores the default maximum number of equal-cost routes for load balancing.

By default, the maximum number of equal-cost routes on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S6720S-S, and S5736-S is 8, and the maximum number of equal-cost routes on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S is 16.

Format

maximum load-balancing *number*

undo maximum load-balancing [*number*]

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes for load balancing.	The value is an integer that ranges from 1 to 8 on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S and S6720S-S. The value ranges from 1 to 16 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple routes are available on an IS-IS network, multiple equal-cost routes may exist. Use the load balancing method to allocate traffic evenly to each link. This method improves link efficiency on the network and reduces the congestion possibility caused by overloaded links.

Specify the *number* parameter to limit the number of equal-cost routes for load balancing.

Precautions

To cancel load balancing, set the *number* parameter to 1 or run the **nexthop** command to set the preferences of equal-cost routes.

Example

Set the maximum number of equal-cost routes for load balancing to 2.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] maximum load-balancing 2
```

Restore the default value.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] undo maximum load-balancing
```

7.6.96 network-entity

Function

The **network-entity** command configures a network entity title (NET) for an IS-IS process.

The **undo network-entity** command deletes the NET of an IS-IS process.

By default, no NET is configured for an IS-IS process.

Format

network-entity *net*

undo network-entity *net*

Parameters

Parameter	Description	Value
net	Specifies a NET.	The format is X...X.XXXX.XXXX.XXXX.00, in which X...X indicates an area address, the 12 Xs in the middle indicate the system ID of the switch, and the last 00 indicates the selector (SEL).

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NET is the special form of the network service access point (NSAP). After the IS-IS view is displayed, IS-IS can start only when a NET is configured for an IS-IS process.

A NET consists of the following parts:

- Area ID: is 1 to 13 bytes in length.
- System ID: is 6 bytes in length.
- SEL: is 1 byte in length and fixed as 00.

Generally, you only need to configure one NET for an IS-IS process. When an area needs to be redefined, for example, the area needs to be merged with other areas or divided into sub-areas, configure multiple NETs to ensure route correctness.

Precautions

An area address uniquely identifies an area in a routing domain. All the switches in the same Level-1 area must have the same area address. The switches in a Level-2 area can have different area addresses.

The switches in an area or a backbone area must have the same system ID.

A maximum of three area addresses can be configured for an IS-IS process. Therefore, a maximum of three NETs can be configured for an IS-IS process. When configuring multiple NETs, ensure that their system IDs are the same.

Example

Set the NET to 10.0001.1010.1020.1030.00, in which the system ID is 1010.1020.1030 and the area ID is 10.0001.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] network-entity 10.0001.1010.1020.1030.00
```

7.6.97 nexthop (IS-IS)

Function

The **nexthop** command sets the preference of equal-cost routes.

The **undo nexthop** command cancels the preference of equal-cost routes.

By default, no preference is set for equal-cost routes.

Format

nexthop *ip-address* **weight** *value*

undo nexthop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies a next-hop IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
weight *value*	Specifies the next-hop weight.	The value is an integer that ranges from 1 to 254.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When there are multiple redundant links on an IS-IS network, there may be multiple equal-cost routes to the same destination network segment.

You can use this command to set the next-hop preference to determine the next hop when the interface cost remains unchanged. A smaller preference value indicates a higher preference.

Precautions

After this command is used, an IS-IS device does not load balance traffic when forwarding the traffic. Instead, the device forwards the traffic to the next hop with the highest preference.

Example

Set the preference of IS-IS equal-cost routes.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] nexthop 10.0.0.3 weight 1
```

7.6.98 optional-checksum enable

Function

The **optional-checksum enable** command enables IS-IS to configure Hello packets and SNP packets to carry optional checksum TLVs and to check received IS-IS packets and SNP packets.

The **undo optional-checksum enable** command restores IS-IS packets to default settings.

By default, Hello packets and SNPs do not carry checksum TLVs and the receiver does not check received packets.

Format

optional-checksum enable

undo optional-checksum enable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of malicious packets and to ensure packets are correctly received on an IS-IS network, you can configure the **optional-checksum enable** command to enable IS-IS routers to send SNP packets and Hello packets carrying optional checksum TLVs. After the peer device receives the packets, it checks whether the carried optional checksum TLVs are correct. If the TLVs are not correct, the peer device rejects the packets.

Prerequisites

You have run the **isis** command to create an IS-IS process and entered the IS-IS view.

Precautions

If MD5 authentication or Keychain authentication with valid MD5 authentication is configured on an IS-IS interface or area, IS-IS routers send Hello packets and SNP packets carrying no checksum TLVs and verify the checksum of the received packets.

Example

Configure IS-IS to add optional checksum TLVs to Hello packets and SNPs.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] optional-checksum enable
```

7.6.99 preference (IS-IS)

Function

The **preference** command sets the IS-IS preference.

The **undo preference** command restores the default IS-IS preference.

The default IS-IS preference is 15.

Format

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Parameters

Parameter	Description	Value
preference	Specifies the IS-IS preference. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device may run multiple dynamic routing protocols and there may be multiple routes of different routing protocols to the same destination. Therefore, routing protocols may share and select routing information. To solve this problem, the system sets a preference for each routing protocol. If different protocols discover routes to the same destination, the system selects the route with a higher protocol preference to forward traffic.

The **preference** command can set the preference of IS-IS routes to affect routing information sharing and selection:

- The **preference** *preference* command can set the preference for all IS-IS routes.
- The **preference** *preference* **route-policy** *route-policy-name* command can set different preferences for matched and unmatched routes.
- The **preference route-policy** *route-policy-name preference* command can set the preference for matched routes without affecting the preference of other IS-IS routes.

Precautions

You can use route-policies to set the preference for specified routes. If the **apply preference** clause is configured in the **route-policy** command, the route preference is as follows:

- The preference of matched routes is set using the **apply** clause.
- The preference of unmatched routes is set using the **preference** command.

As shown in the following example, the preference of the routes that pass route-policy **abc** is set to 50 and the preference of the routes that do not pass the route-policy is set to 30.

```
#
route-policy abc permit node 1
 if-match cost 20
 apply preference 50
#
isis 1
 preference 30 route-policy abc
```

If the **apply preference 50** clause is not configured in route-policy **abc**, the preference of all routes is set to 30.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured priority applies to all IS-IS routes.

Example

Set the IPv4 IS-IS preference to 25.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] preference 25
```

7.6.100 prefix-priority (IS-IS)

Function

The **prefix-priority** command sets the convergence priority of IS-IS routes.

The **undo prefix-priority** command restores the default convergence priority of IS-IS routes.

By default, the convergence priority of IS-IS host routes and default routes is medium, and the convergence priority of other IS-IS routes is low.

Format

prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** } { **ip-prefix** *prefix-name* | **tag** *tag-value* }

undo prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** }

Parameters

Parameter	Description	Value
level-1	Specifies the convergence priority of Level-1 IS-IS routes.	-

Parameter	Description	Value
level-2	Specifies the convergence priority of Level-2 IS-IS routes.	-
critical	Sets the convergence priority of IS-IS routes to critical.	-
high	Sets the convergence priority of IS-IS routes to high.	-
medium	Sets the convergence priority of IS-IS routes to medium.	-
ip-prefix *prefix-name*	Sets the convergence priority of the IS-IS routes matching the specified IP prefix.	The value is a string of 1 to 169 case-sensitive characters without spaces.
tag *tag-value*	Sets the convergence priority of the IS-IS routes with the specified tag value. To use the tag value to filter the IPv4 routes for which convergence priorities need to be set, ensure that the IS-IS cost style of sent packets is not narrow and the routes carry the tag value.	The value is an integer that ranges from 1 to 4294967295.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a routing table has a large number of routing entries on an IS-IS device, the device needs to spend much time performing SPF calculation. To enable some key routes to be calculated first, run the **prefix-priority** command to set the convergence priority for these routes.

The convergence priorities of IS-IS routes are classified as critical, high, medium, and low in descending order.

The rules for applying convergence priorities to IS-IS routes are as follows:

- Existing IS-IS routes are converged based on the priorities set using the **prefix-priority** command.
- New IS-IS routes are converged based on the priorities set using the **prefix-priority** command.
- If an IS-IS route conforms to the matching rules of multiple convergence priorities, the highest convergence priority is used.
- If the route level is not specified, the **prefix-priority** command configuration takes effect for both Level-1 and Level-2 IS-IS routes.

Precautions

The **prefix-priority** command applies only to the public network.

After the **prefix-priority** command is run to set the convergence priority for IS-IS routes (including IS-IS host routes and default routes), the convergence priority of all the IS-IS routes that meet the matching rules is changed according to the command configuration, and the convergence priority of the IS-IS routes that do not meet the matching rules is changed to low.

Example

Set the convergence priority of Level-1 routes with tag value 3 to critical.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] prefix-priority level-1 critical tag 3
```

Set the convergence priority of the routes matching IP prefix **p1** to medium.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix p1 permit 192.168.0.1 24
[HUAWEI] isis 1
[HUAWEI-isis-1] prefix-priority medium ip-prefix p1
```

7.6.101 purge-originator-identification enable

Function

The **purge-originator-identification enable** command configures IS-IS to add purge-originator-identification (POI) TLV to Purge packets. If a dynamic hostname has been configured for the local device, the hostname TLV is also added to the Purge packets.

The **undo purge-originator-identification enable** command deletes POI TLV and hostname TLV from Purge packets.

By default, Purge packets do not carry POI TLV or hostname TLV.

Format

purge-originator-identification enable [**always**]

undo purge-originator-identification enable [**always**]

Parameters

Parameter	Description
always	

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When **Remaining Lifetime** of an LSP is 0, the LSP is invalid, and this invalid packet is a Purge packet. In most cases, a Purge packet does not carry any information about the router that generated the Purge packet. Without such information, troubleshooting is difficult if a network problem occurs.

To address this issue, you can run the **purge-originator-identification enable** command to configure IS-IS to add POI TLV to Purge packets. If a dynamic hostname has been configured for the local device, the hostname TLV is also added to the Purge packets, which facilitates troubleshooting.

- If the **purge-originator-identification enable** command is run and an authentication mode is configured, generated Purge LSPs do not carry the POI TLV or hostname TLV.
- If the **purge-originator-identification enable** command is run and no authentication is configured, generated Purge LSPs will carry the POI TLV or hostname TLV.
- If the **purge-originator-identification enable always** command is run, generated Purge LSPs carry the POI TLV and hostname TLV, regardless of whether authentication is configured.

Example

Configure IS-IS to add POI TLV to Purge packets.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] purge-originator-identification enable
```

7.6.102 reset isis all

Function

The **reset isis all** command restarts IS-IS processes.

Format

reset isis all [[*process-id* | **vpn-instance** *vpn-instance-name*] | **graceful-restart**] *

reset isis *process-id* **all** [**graceful-restart**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process to be restarted.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance. *vpn-instance-name* specifies the name of a VPN instance.	The value must be an existing VPN instance name.
graceful-restart	Restarts an IS-IS process in GR mode.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset isis all** command is used when LSPs need to be updated immediately. For example, after the **area-authentication-mode** and **domain-authentication-mode** commands are used, you can run the **reset isis all** command to clear old LSPs.

Precautions

NOTICE

Restarting IS-IS processes may interrupt services. Therefore, confirm the action before running the **reset isis all** command.

Example

Restart IS-IS processes.

```
<HUAWEI> reset isis all
Warning: The ISIS process(es) will be reset. Continue?[Y/N]y
```

7.6.103 reset isis peer

Function

The **reset isis peer** command resets a specified IS-IS neighbor relationship.

Format

reset isis peer *system-id* [*process-id* | **vpn-instance** *vpn-instance-name*]

reset isis *process-id* **peer** *system-id*

Parameters

Parameter	Description	Value
system-id	Specifies the system ID of an IS-IS neighbor.	The value is 6 bytes in length and in XXXX.XXXX.XXXX format.
process-id	Specifies the IS-IS process ID for which the neighbor relationship needs to be reset.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance. This parameter is optional for a default VPN instance.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset isis peer** command is used when a device needs to re-establish the neighbor relationship with a specified neighbor.

NOTICE

Exercise caution when using the **reset isis peer** command. This command will re-establish neighbor relationships with a specified neighbor, which may result in route flapping.

Example

Reset the IS-IS neighbor with system ID 0000.0c11.1111.

```
<HUAWEI> reset isis peer 0000.0c11.1111
```

7.6.104 reset isis suppress-flapping peer

Function

The **reset isis suppress-flapping peer** command forces an interface to exit from IS-IS neighbor relationship flapping suppression.

Format

reset isis *process-id* **suppress-flapping peer** [**interface** *interface-type interface-number*] [**notify-peer**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process.	The value is an integer ranging from 1 to 65535.
interface *interface-type interface-number*	Specifies an interface type and number.	-
notify-peer	Instructs neighbors to exit from IS-IS neighbor relationship flapping suppression too.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Interfaces exit from flapping suppression in the following scenarios:

- The suppression timer expires.
- The corresponding IS-IS process is reset.
- An IS-IS neighbor is reset using the **reset isis peer** command.
- IS-IS neighbor relationship flapping suppression is disabled globally using the **suppress-flapping peer disable (IS-IS)** command in the IS-IS view.
- The **reset isis suppress-flapping peer** command is run.
- Suppression is aborted forcibly using the **reset isis** *process-id* **suppress-flapping peer** [**interface** *interface-type interface-number*] **notify-peer** command on the remote device.

Example

Force interfaces to exit from IS-IS neighbor relationship flapping suppression.

```
<HUAWEI> reset isis 1 suppress-flapping peer
```

7.6.105 set-overload

Function

The **set-overload** command sets the overload bit for non-pseudonode LSPs.

The **undo set-overload** command removes the overload bit of non-pseudonode LSPs.

By default, no overload bit is set for non-pseudonode LSPs.

Format

set-overload [**on-startup** [*timeout1* | **start-from-nbr** *system-id* [*timeout1* [*timeout2*]] | **wait-for-bgp** [*timeout1*]] [**send-sa-bit** [*timeout3*]]] [**allow** { **interlevel** | **external** }*]

undo set-overload

Parameters

Parameter	Description	Value
on-startup	Indicates that the overload bit remains set within the specified period when the switch restarts or is faulty.	-
timeout1	Specifies the duration of the overload bit after the system starts.	The value is an integer that ranges from 5 to 86400, in seconds. The default value is 600 seconds.
start-from-nbr *system-id*	Specifies the duration of the system overload bit according to the status of a specified neighbor.	The value is in XXXX.XXXX.XXXX format.

Parameter	Description	Value
timeout1 [*timeout2*]	Specifies the period during which the overload bit remains set, which is related to the neighbor status.	- If the specified neighbor does not go Up before *timeout2* expires, the duration of the system overload bit is *timeout2*. *timeout2* ranges from 5 to 86400, in seconds. The default value is 1200 seconds (20 minutes). - If the specified neighbor goes Up before *timeout2* expires, the duration of the system overload bit is *timeout1*. *timeout1* ranges from 5 to 86400, in seconds. The default value is 600 seconds (10 minutes).
wait-for-bgp	Specifies the period during which the overload bit of the system remains set according to the BGP convergence status.	-
send-sa-bit	Specifies the overload bit remains in Hello packets after the device is started.	-
timeout3	Specifies the period during which the overload bit remains in Hello packets after the device is started.	The value is an integer ranging from 5 to 120, in seconds. The default value is 30 seconds.
allow	Allows advertising IP prefixes. By default, the system is prohibited from advertising IP prefixes when the system enters the overload state.	-
interlevel	Allows advertising the IP prefixes learned from IS-IS of different levels when **allow** is specified.	-
external	Allows advertising the IP prefixes learned from other protocols when **allow** is specified.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Although LSPs with the overload bit are flooded on the network, the LSPs are ignored in the calculation of the routes that pass through the switch in overload state. That is, after the overload bit is set on the switch, other switches ignore the switch when performing SPF calculation. Direct routes of the switch are not ignored during SPF calculation.

To prevent the local switch from being used by other switches to perform SPF calculation, run the **set-overload** command on the local switch without specifying the **on-startup** keyword. Then the system immediately sets the overload bit in the LSP to be sent. To remove the overload bit, run the **undo set-overload** command.

When the local switch restarts or is faulty, to prevent the local switch from being used by other switches to perform SPF calculation, run the **set-overload** command on the local switch and specify the **on-startup** keyword.

When the switch is experiencing memory shortage, the system automatically sets the overload bit in the sent LSPs regardless of whether the **set-overload** command is run.

You can set the overload bit to solve the problem of network traffic loss caused by the difference between the BGP convergence speed and IGP convergence speed.

Precautions

If a TE LSP uses the local device as a transit node before the **set-overload** command is run, the TE LSP is not torn down and re-established and still uses the local device as a transit node after the **set-overload** command is run; if the local device is restarted after the command is run and fast convergence is not configured on the ingress of the RSVP-LSP, TE LSP forwarding fails, and services are affected. Therefore, the **mpls te path-selection overload** command needs to be run on the ingress of the RSVP-LSP before the device is restarted.

Example

Set the overload bit for IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] set-overload
Warning: The IS-IS process overload state will be set. Continue?[Y/N]
```

7.6.106 spf-priority

Function

The **spf-priority** command sets the priority of SPF calculation.

The **undo spf-priority** command restores the default priority of SPF calculation.

By default, the priority of SPF calculation in a base topology is 64.

Format

spf-priority *priority-value*

undo spf-priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of SPF calculation. A larger value indicates a higher priority.	The value is an integer that ranges from 1 to 127.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

When multiple IS-IS topology instances are deployed on a network, the **spf-priority** command can be used to set a priority for the SPF calculation in each IS-IS topology instance.

If a higher priority is set for a topology, routes of the topology instance are converged first, ensuring that important services are running properly.

Example

Set the priority of SPF calculation in an IPv4 base topology to 30.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] spf-priority 30
```

7.6.107 spf-slice-size

Function

The **spf-slice-size** command sets the maximum duration for IS-IS route calculation.

The **undo spf-slice-size** command restores the default setting.

By default, IS-IS route calculation lasts for a maximum of 2 ms at a time.

Format

spf-slice-size *duration-time*

undo spf-slice-size

Parameters

Parameter	Description	Value
duration-time	Specifies the maximum duration for IS-IS route calculation.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 2.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

When a routing table contains a large number of routes, run the **spf-slice-size** command to specify the maximum duration of SPF calculation to prevent route calculation from using system resources for a long period.

Example

Set the maximum duration of IS-IS route calculation to 50 ms.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] spf-slice-size 50
```

7.6.108 summary (IS-IS)

Function

The **summary** command configures IS-IS to generate summarized routes.

The **undo summary** command disables IS-IS from generating summarized routes.

By default, IS-IS does not generate summarized routes.

Format

summary *ip-address mask* [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] *

undo summary *ip-address mask* [**level-1** | **level-1-2** | **level-2**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a summarized route.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address of a summarized route.	The value is in dotted decimal notation.
avoid-feedback	Prevents summarized routes from being learned through SPF calculation.	-
generate_null0_route	Generates null0 routes to prevent routing loops.	-
tag *tag*	Assigns administrative tags to advertised routes.	The value is an integer that ranges from 1 to 4294967295.
level-1	Summarizes only the routes imported into Level-1 areas. If no level is specified, Level-2 is used by default.	-
level-1-2	Summarizes the routes imported into Level-1 areas and the backbone network. If no level is specified, Level-2 is used by default.	-
level-2	Summarizes only the routes imported into the backbone network. If no level is specified, Level-2 is used by default.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Route summarization on a large-scale IS-IS network efficiently reduces routing entries. This minimizes system resource consumption and maintains system performance.

If a link frequently alternates between Up and Down, the links not involved in the route summarization will not be affected. Therefore, route summarization prevents route flapping on the network and improves network stability.

Precautions

Configuring route summarization does not affect the routing table of the local device because each specific route is still displayed in the routing table. Route summarization reduces the flooding of LSPs. Routing tables of other devices that receive the LSP from the local device contain only one summarized routes but not specific routes. Specific routes are still displayed in the routing table of the device directly connected to the summarized network segment.

Both IS-IS routes and routes imported from other protocols can be summarized. The lowest cost among that of the routes that are summarized is used as the cost of the summarized route.

Example

Generate a summarized route with destination subnet 202.0.0.0/8.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] summary 10.0.0.0 255.0.0.0
```

7.6.109 suppress-flapping peer disable (IS-IS)

Function

The **suppress-flapping peer disable** command disables IS-IS neighbor relationship flapping suppression globally.

The **undo suppress-flapping peer disable** command enables IS-IS neighbor relationship flapping suppression globally.

By default, IS-IS neighbor relationship flapping suppression is enabled globally.

Format

suppress-flapping peer disable

undo suppress-flapping peer disable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

If an interface carrying IS-IS services alternates between Up and Down, IS-IS neighbor relationship flapping occurs on the interface. During the flapping, IS-IS reestablishes the neighbor relationship and recalculates routes. In this process, a large number of packets are exchanged, adversely affecting neighbor relationship stability, IS-IS services, and other IS-IS-dependent services, such as LDP and BGP. IS-IS neighbor relationship flapping suppression can address this problem by delaying IS-IS neighbor relationship reestablishment or preventing service traffic from passing through flapping links.

By default, IS-IS neighbor relationship flapping suppression is enabled globally. To disable this function globally, run the **suppress-flapping peer disable** command.

Example

Disable neighbor relationship flapping suppression globally.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] suppress-flapping peer disable
```

7.6.110 timer lsp-generation

Function

The **timer lsp-generation** command configures an intelligent timer for generating LSPs.

The **undo timer lsp-generation** command cancels the intelligent timer for generating LSPs.

By default, no intelligent timer is configured to generate LSPs.

Format

timer lsp-generation *max-interval* [*init-interval* [*incr-interval*]] [**level-1** | **level-2**]

undo timer lsp-generation [*max-interval* [*init-interval* [*incr-interval*]]] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
max-interval	Specifies the maximum delay in generating LSPs with the same LSP ID.	The value is an integer that ranges from 1 to 120, in seconds. The default value is 2.
init-interval	Specifies the initial delay in generating LSPs.	The value is an integer that ranges from 1 to 60000, in milliseconds. By default, this delay is not used.
incr-interval	Specifies the incremental delay in generating two LSPs with the same LSP ID.	The value is an integer that ranges from 1 to 60000, in milliseconds. By default, this delay is not used.
level-1	Specifies the delay in generating Level-1 LSPs. If no level is specified, the delay in generating Level-1 and Level-2 LSPs is set.	-
level-2	Specifies the delay in generating Level-2 LSPs. If no level is specified, the delay in generating Level-1 and Level-2 LSPs is set.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, if the local routing information changes, a device needs to generate a new LSP to notify this change. If the local routing information changes frequently, a large number of new LSPs are generated, which occupies a lot of system resources and decreases system performance.

To speed up network convergence and prevent the system from being affected, run the **timer lsp-generation** command to configure an intelligent timer for generating LSPs. This timer can adjust the delay in generating LSPs based on the routing information change frequency. This command can implement different functions when different parameters are specified:

- When only *max-interval* is specified, the intelligent timer functions as an ordinary one-time triggering timer.

- When both *init-interval* and *incr-interval* are specified, the delay in generating an LSP for the first time is determined by *init-interval*, and the delay in generating an LSP with the same LSP ID for the second time is determined by *incr-interval*. Subsequently, each time routes change, the delay in generating an LSP doubles the last delay until the delay reaches the value specified by *max-interval*. After the delay remains at the value specified by *max-interval* for three times or the IS-IS process is restarted, the delay decreases to the value specified by *init-interval*.
- When *init-interval* is specified but *incr-interval* is not, the delay in generating an LSP for the first time is determined by *init-interval*, and the delay in generating subsequent LSPs is determined by *max-interval*. After the delay remains at the value specified by *max-interval* for three times or the IS-IS process is restarted, the delay decreases to the value specified by *init-interval*.
- The initial delay for generating an LSP is *init-interval*; the delay for generating the LSP with the same LSP ID is *incr-interval*. From the third time on, the delay for generating the LSP doubles each time until the delay reaches *max-interval*. After *max-interval* expires without flapping or the IS-IS process is restarted, the delay decreases to *init-interval*.

Precautions

If the delay in generating an LSP is too long, a device cannot advertise routing information changes to neighbors in time. This slows down network convergence.

Example

Set the delay in generating LSPs to 5s.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] timer lsp-generation 5
```

Set the maximum delay in generating LSPs to 20s, initial delay to 50 ms, and incremental delay to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] timer lsp-generation 20 50 2000
```

7.6.111 timer lsp-max-age

Function

The **timer lsp-max-age** command sets the maximum lifetime for the LSPs generated by an IS-IS process.

The **undo timer lsp-max-age** command restores the default setting.

By default, the maximum lifetime of LSPs is 1200 seconds.

Format

timer lsp-max-age *age-time*

undo timer lsp-max-age

Parameters

Parameter	Description	Value
age-time	Specifies the maximum lifetime for LSPs.	The value is an integer that ranges from 2 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch generates the system LSP, the system fills in the LSP with its maximum lifetime. After other switches receive this LSP, the lifetime of the LSP is reduced accordingly. If the switch does not receive an updated LSP, the lifetime of the LSP is reduced to 0, and the switch retains the LSP for another 60 seconds. If the switch still does not receive any updated LSP within 60 seconds, the switch deletes the LSP.

You can run the **timer lsp-max-age** command to adjust the maximum lifetime of LSPs to ensure the validity of existing LSPs before new LSPs are received.

Precautions

The maximum lifetime of LSPs must be longer than the interval for updating LSPs to ensure that LSPs can be updated before being deleted.

Example

Set the maximum lifetime of the LSPs generated by the current IS-IS process to 25 minutes (1500 seconds).

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] timer lsp-max-age 1500
```

7.6.112 timer lsp-refresh

Function

The **timer lsp-refresh** command sets the interval for updating LSPs.

The **undo timer lsp-refresh** command restores the default setting.

By default, the interval for updating LSPs is 900 seconds.

Format

timer lsp-refresh *refresh-time*

undo timer lsp-refresh

Parameters

Parameter	Description	Value
refresh-time	Specifies the interval for updating LSPs.	The value is an integer that ranges from 1 to 65534, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, LSDB synchronization is implemented through LSP flooding. During LSP flooding, a device sends an LSP to its neighbors and then the neighbors send the received LSP to their respective neighbors except the device that first sends the LSP. In this manner, the LSP is flooded among the devices of the same level. LSP flooding allows each device of the same level to have the same LSP information and synchronize its LSDB with each other.

LSPs need to be periodically flooded. When the system generates the system LSP, the system fills in the LSP with its maximum lifetime. After other devices receive this LSP, the lifetime of the LSP is reduced accordingly. If the device does not receive an updated LSP, the lifetime of the LSP is reduced to 0, and the device retains the LSP for another 60 seconds. If the device still does not receive any updated LSP within 60 seconds, the device deletes the LSP.

You can run the **timer lsp-refresh** command to set the interval for updating LSPs to control network convergence speed.

Precautions

If the interval for updating LSPs is small, LSPs may be updated frequently, which occupies a lot of bandwidth resources. If the interval is long, routing information changes cannot be notified in a timely manner.

Example

Set the interval for updating LSPs to 1200 seconds.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] timer lsp-refresh 1200
```

7.6.113 timer spf

Function

The **timer spf** command sets the delay in SPF calculation.

The **undo timer spf** command restores the default setting.

By default, the maximum delay in SPF calculation is 5 seconds.

Format

timer spf *max-interval* [*init-interval* [*incr-interval*]]

undo timer spf

Parameters

Parameter	Description	Value
max-interval	Specifies the maximum delay in SPF calculation.	The value is an integer that ranges from 1 to 120, in seconds. The default value is 5s.
init-interval	Specifies the initial delay in SPF calculation. If the *init-interval* parameter is not specified, the intelligent timer functions as an ordinary one-time triggering timer.	The value is an integer that ranges from 1 to 60000, in milliseconds. By default, it is 50 milliseconds.
incr-interval	Specifies the incremental delay in two SPF calculations. If the *incr-interval* parameter is not specified, the delay in SPF calculation for the first time is determined by *init-interval*. From the second time on, the delay in SPF calculation is determined by *max-interval*.	The value is an integer that ranges from 1 to 60000, in milliseconds. The default value is 200 milliseconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IS-IS, route calculation is required when an LSDB changes. Frequent route calculations, however, consume lots of system resources and decrease system performance. Delaying SPF calculation can improve route calculation efficiency. However, a long delay in SPF calculation slows down route convergence.

To speed up route convergence without affecting the efficiency of switches, configure an intelligent timer for SPF calculation. This timer automatically adjusts the delay in SPF calculation based on the LSDB change frequency.

When SPF calculation is performed for the first time, the interval is *init-interval*. Each time a route changes, the interval is added by *incr-interval* until the interval reaches *max-interval*. After *max-interval* expires without flapping or the IS-IS process is restarted, the delay decreases to *init-interval*.

When only *max-interval* is used, the intelligent timer becomes a one-short triggered timer.

Example

Set the delay in SPF calculation to 5s.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] timer spf 5
```

Set the maximum delay in SPF calculation to 15s, initial delay to 10 ms, and incremental delay to 5000 ms.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] timer spf 15 10 5000
```

7.6.114 virtual-system

Function

The **virtual-system** command sets the virtual system ID for an IS-IS process. If no virtual system ID is set, no extended LSP can be generated. A maximum of 50 virtual system IDs can be configured for an IS-IS process.

The **undo virtual-system** command deletes the virtual system ID of an IS-IS process.

By default, no virtual system ID is configured for an IS-IS process.

Format

virtual-system *virtual-system-id*

undo virtual-system *virtual-system-id*

Parameters

Parameter	Description	Value
virtual-system-id	Specifies a virtual system ID for an IS-IS process.	The value is 6 bytes in length and in XXXX.XXXX.XXXX format.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Like a common system ID, a virtual system ID must be unique in a routing domain.

The **virtual-system** command is used together with the **lsp-fragments-extend** command. The configured virtual system ID takes effect only when LSP fragment extension is enabled and the IS-IS process is restarted using the **reset isis all** command.

If LSP fragment extension is not enabled and the IS-IS process is not restarted, you can configure the virtual system ID but the configured virtual system ID does not take effect.

Before running this command, run the **network-entity** command in the IS-IS view to configure a network entity title for the IS-IS process.

Example

Set the virtual system ID of IS-IS process 1 to 2222.2222.2222.

```
<HUAWEI> system-view
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 10.0000.0000.0001.00
[HUAWEI-isis-1] virtual-system 2222.2222.2222
```

7.7 IPv6 IS-IS Configuration Commands

7.7.1 Command Support

Only the following switch models support IPv6 IS-IS:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

7.7.2 display isis ipv6 bfd interface

Function

The **display isis ipv6 bfd interface** command displays information about the interface enabled with IPv6 BFD for IS-IS.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display isis [*process-id*] **ipv6 bfd interface**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

BFD can provide millisecond-level fault detection. It can work with IS-IS to fast detect faults on neighboring devices and instruct IS-IS to recalculate routes for correct packet forwarding. You can run the **display isis ipv6 bfd interface** command to check information about the interface enabled with IPv6 BFD for IS-IS.

Example

Display information about the interface enabled with IPv6 BFD.

```
<HUAWEI> display isis 1 ipv6 bfd interface
                 IPV6 BFD information of interface for ISIS(1)
                ----------------------------------------------
 Interface                   BFD6.State     Min-Tx        Min-Rx        Mul
 GE0/0/1                      enable         150           150           3
 GE0/0/2                      enable         150           150           3
 Total interfaces: 2                   Total IPv6 bfd enabled interfaces: 2
```

Table 7-119 Description of the **display isis ipv6 bfd interface** command output

Item	Description
Interface	Interface enabled with IPv6 BFD for IS-IS
BFD6.State	IPv6 BFD status on the interface: ● enable ● disable To enable IPv6 BFD for IS-IS, run the **ipv6 bfd all-interfaces enable (IS-IS)** or **isis ipv6 bfd enable** command.

Item	Description
Min-Tx	Configured minimum interval for sending IPv6 BFD packets. To the parameters of IPv6 BFD sessions, run the **ipv6 bfd all-interfaces (IS-IS)** or **isis ipv6 bfd** command.
Min-Rx	Configured minimum interval for receiving IPv6 BFD packets. To the parameters of IPv6 BFD sessions, run the **ipv6 bfd all-interfaces (IS-IS)** or **isis ipv6 bfd** command.
Mul	Local detection multipliers of IPv6 BFD packets. To the parameters of IPv6 BFD sessions, run the **ipv6 bfd all-interfaces (IS-IS)** or **isis ipv6 bfd** command.
Total interfaces	Number of interfaces enabled with the IS-IS process
Total IPv6 bfd enabled interfaces	Number of interfaces enabled with IPv6 BFD for IS-IS

7.7.3 display isis ipv6 bfd session

Function

The **display isis ipv6 bfd session** command displays information about the IPv6 BFD session for IS-IS.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display isis [*process-id* | **vpn-instance** *vpn-instance-name*] **ipv6 bfd session** { **all** | **peer** *ipv6-address* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance, which is case sensitive.	The value must be an existing VPN instance name.
all	Indicates all the interfaces that run the IS-IS process.	-

Parameter	Description	Value
peer *ipv6-address*	Specifies the IPv6 link-local address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the interface whose IPv6 BFD session statistics need to be collected.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

BFD can provide millisecond-level fault detection. It can work with IS-IS to fast detect faults on neighboring devices and instruct IS-IS to recalculate routes for correct packet forwarding. You can run the **display isis ipv6 bfd session** command to check information about the IPv6 BFD session for IS-IS.

Example

Display information about the IPv6 BFD session for IS-IS.

```
<HUAWEI> display isis 1 ipv6 bfd session all

                      IPv6 BFD session information for ISIS(1)
                      ----------------------------------------

Peer System ID : 0000.0000.0002   Type : L2
Interface : GE0/0/1
IPv6 BFD State : up       TX : 150    RX : 150    Multiplier : 3
LocDis : 8195          Local IPv6 Address : FE80::200:13FF:FE82:4569
RemDis : 8194          Peer  IPv6 Address : FE80::225:9EFF:FEFB:BFF1
Diag : No diagnostic information

Peer System ID : 0000.0000.0003   Type : L2
Interface : GE0/0/2
IPv6 BFD State : up       TX : 150    RX : 150    Multiplier : 3
LocDis : 8196          Local IPv6 Address : FE80::200:13FF:FE82:4569
RemDis : 8205          Peer  IPv6 Address : FE80::201:FF:FE01:1
Diag : No diagnostic information

Total IPv6 BFD session(s): 2
```

Display information about the IPv6 BFD session for IS-IS of the peer with the specified IPv6 address.

```
<HUAWEI> display isis 1 ipv6 bfd session peer FE80::225:9EFF:FEFB:BFF1

                      IPv6 BFD session information for ISIS(1)
                      ----------------------------------------

Peer System ID : 0000.0000.0002   Type : L2
```

```
Interface : GE0/0/2
IPv6 BFD State : up       TX : 150   RX : 150   Multiplier : 3
LocDis : 8195         Local IPv6 Address : FE80::200:13FF:FE82:4569
RemDis : 8194         Peer  IPv6 Address : FE80::225:9EFF:FEFB:BFF1
Diag : No diagnostic information

Total IPv6 BFD session(s): 1
```

Display information about the IPv6 BFD session for IS-IS of the specified interface.

```
<HUAWEI> display isis 1 ipv6 bfd session interface GigabitEthernet 0/0/2

                IPv6 BFD session information for ISIS(10)
                -----------------------------------------

Peer System ID : 0000.0000.0002   Type : L2
Interface : GE0/0/2
IPv6 BFD State : up       TX : 150   RX : 150   Multiplier : 3
LocDis : 8195         Local IPv6 Address : FE80::200:13FF:FE82:4569
RemDis : 8194         Peer  IPv6 Address : FE80::225:9EFF:FEFB:BFF1
Diag : No diagnostic information

Total IPv6 BFD session(s): 1
```

Table 7-120 Description of the **display isis ipv6 bfd session** command output

Item	Description
Peer system ID	System ID of the peer
Interface	Local interface name
Type	Level of the peer: - L1: Level-1 - L2: Level-2 - L12: Level-1-2
IPv6 BFD State	IPv6 BFD status: - up: indicates that the IPv6 BFD session is established successfully. - down: indicates that the IPv6 BFD fails to be established.
TX	Negotiated minimum interval for sending IPv6 BFD packets
RX	Negotiated minimum interval for receiving IPv6 BFD packets
Multiplier	Remote detection multiplier
LocDis	Local identifier dynamically assigned by IPv6 BFD
Local IPv6 Address	IPv6 link-local address
RemDis	Remote identifier dynamically assigned by IPv6 BFD
Peer IPv6 Address	IPv6 link-local address of the peer

Item	Description
Diag	Diagnostic information: ● No diagnostic information: IPv6 BFD runs properly, and no diagnostic information is displayed. ● Administrator down: The session is set Down by the network administrator. ● Global IPv6 BFD is not enabled: Global IPv6 BFD is disabled. ● IPv6 BFD session number reaches the MAX BFD: The number of IPv6 BFD sessions reaches the upper limit. ● No IPv6 BFD packets were received: The device does not receive any IPv6 BFD packet. ● Neighbour is down: The neighbor goes Down. ● Administrator down event received: The device receives an event indicating that the IPv6 BFD session is set Down by the network administrator.
Total IPv6 BFD session(s)	Total number of IPv6 BFD sessions

7.7.4 ipv6 auto-cost enable

Function

The **ipv6 auto-cost enable** command enables IS-IS to automatically calculate the interface cost on an IPv6 network according to the interface bandwidth.

The **undo ipv6 auto-cost enable** command disables IS-IS from automatically calculating the interface cost on an IPv6 network according to the interface bandwidth.

By default, the automatic interface cost calculation function is disabled on an IPv6 network.

Format

ipv6 auto-cost enable [**compatible**]

undo ipv6 auto-cost enable

Parameters

Parameter	Description	Value
compatible	Specifies the IS-IS to calculate the cost of an interface on an IPv6 network based on the bandwidth of the interface automatically in compatible.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function is enabled, for a certain IS-IS interface, if the cost of the interface is not configured in the interface view, and the global cost is not configured in the IS-IS view, the system calculates the cost for the interface automatically.

If the cost style of the system is wide or wide-compatible:

When **auto-cost enable** command is configured, Interface cost = (Bandwidth-reference/Link-bandwidth) x 10.

The cost style is set by the **cost-style** command. The Bandwidth-reference is set by the **ipv6 bandwidth-reference** command. The Link-bandwidth is the interface bandwidth.

If the cost-style of the system is narrow, narrow-compatible, or compatible, the cost of each interface is determined according to the following table.

Table 7-121 Relationship of the IS-IS interface cost and the bandwidth

Cost	Range of Interface Bandwidth
60	Interface bandwidth ≤ 10 Mbit/s
50	10 Mbit/s < Interface bandwidth ≤ 100 Mbit/s
40	100 Mbit/s < Interface bandwidth ≤ 155 Mbit/s
30	155 Mbit/s < Interface bandwidth ≤ 622 Mbit/s
20	622 Mbit/s < Interface bandwidth ≤ 2.5 Gbit/s
10	2.5 Gbit/s < Interface bandwidth

Precautions

The priority of the cost value of the global IPv6 configured by the **ipv6 circuit-cost** command is higher than the auto cost value.

This command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

The **ipv6 auto-cost enable** command cannot change the cost of the loopback interface.

Example

Enable IS-IS to automatically calculate the interface cost on an IPv6 network according to the interface bandwidth.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 auto-cost enable
```

7.7.5 ipv6 bandwidth-reference

Function

The **ipv6 bandwidth-reference** command sets the bandwidth reference value used in automatic interface cost calculation on an IPv6 network.

The **undo ipv6 bandwidth-reference** command restores the default setting.

By default, the bandwidth reference value is 100 Mbit/s.

Format

ipv6 bandwidth-reference *bandwidth-reference-value*

undo ipv6 bandwidth-reference

Parameters

Parameter	Description	Value
bandwidth-reference-value	Specifies the bandwidth reference value used in automatic interface cost calculation.	The value is an integer that ranges from 1 to 2147483648, in Mbit/s.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the link cost of IS-IS routes reflect the actual link cost, configure a proper link cost for all interfaces or enable the automatic interface cost calculation function. To enable automatic interface cost calculation, set a proper bandwidth reference value.

You can run the **ipv6 bandwidth-reference** command to set a proper reference bandwidth value. After the automatic interface cost calculation function is enabled, the system automatically calculates the interface cost according to the bandwidth reference value set using the command.

The **bandwidth** *bandwidth* command can only set an interface bandwidth obtained by the NMS from the MIB. It cannot change an interface actual bandwidth and interface cost.

Precautions

The **ipv6 bandwidth-reference** command takes effect only after IPv6 is enabled for the IS-IS process using the **ipv6 enable** command.

Example

Set the IPv6 reference bandwidth value used in automatic interface cost calculation to 200 Mbit/s.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 bandwidth-reference 200
```

7.7.6 ipv6 bfd all-interfaces enable (IS-IS)

Function

The **ipv6 bfd all-interfaces enable** command enables IPv6 BFD for IS-IS globally in the IS-IS process.

The **undo ipv6 bfd all-interfaces enable** command disables IPv6 BFD for IS-IS globally in the IS-IS process.

By default, IPv6 BFD for IS-IS is disabled in the IS-IS process.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv6 bfd all-interfaces enable

undo ipv6 bfd all-interfaces enable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPv6 BFD for IS-IS can provide millisecond level fault detection, help IS-IS to detect faults on neighboring devices or links rapidly, and instruct IS-IS to recalculate routes for correct packet forwarding.

Prerequisites

The **ipv6 bfd all-interfaces enable** command can take effect only after global BFD is enabled by the **bfd** and IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Configuration Impact

After the **ipv6 bfd all-interfaces enable** command is run, all the interfaces in the IS-IS process are automatically enabled with IPv6 BFD for IS-IS. IS-IS establishes IPv6 BFD sessions on the interfaces whose IS-IS IPv6 neighbor status is Up (the DIS is Up on the broadcast network) by using the default IPv6 BFD parameters.

After the **ipv6 bfd all-interfaces enable** command is run, if you start the IS-IS process on the IS-IS interface that is not enabled with the IS-IS process, the interface is also automatically enabled with IPv6 BFD for IS-IS.

After the **ipv6 bfd all-interfaces enable** command is run, check whether all the interfaces need to be enabled with IPv6 BFD for IS-IS according to network planning. If some interfaces do not need to be enabled with IPv6 BFD for IS-IS, run the **isis ipv6 bfd block** command on these interfaces to block IPv6 BFD for IS-IS.

Precautions

If IPv6 BFD for IS-IS is neither enabled globally nor enabled on interfaces, you can configure IPv6 BFD parameters of IS-IS; however, IPv6 BFD sessions cannot be established.

Example

Configure IPv6 BFD for an IS-IS process.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 bfd all-interfaces enable
```

7.7.7 ipv6 bfd all-interfaces(IS-IS)

Function

The **ipv6 bfd all-interfaces** command configures the parameters of IPv6 BFD sessions.

The **undo ipv6 bfd all-interfaces** command restores the default parameters of IPv6 BFD sessions.

By default, the minimum interval for sending or receiving IPv6 BFD packets is 1000 milliseconds, and the local IPv6 BFD detection multiplier is 3.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ipv6 bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* } *

undo ipv6 bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* } *

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Specifies the minimum interval for receiving BFD packets from the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *transmit-interval*	Specifies the minimum interval for sending BFD packets to the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Indicates the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPv6 BFD for IS-IS can provide millisecond level fault detection, help IS-IS to detect faults on neighboring devices or links rapidly, and instruct IS-IS to recalculate routes for correct packet forwarding. The **isis ipv6 bfd** command can be used to configure IPv6 BFD detection parameters on a specified interface.

Prerequisites

The **ipv6 bfd all-interfaces** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Precautions

If only IPv6 BFD session parameters are configured but the **ipv6 bfd all-interfaces enable** command is not run, no IPv6 BFD sessions can be established.

After the local *min-rx-interval* is compared with the remote *min-tx-interval*, the larger value is chosen as the actual local receiving interval.

NOTE

> To ensure that the actual local receiving interval is the same as the local configured value, you are recommended to configure the same value for the local *min-rx-interval* and the remote *min-tx-interval*.
>
> Similarly, to ensure that the actual local IPv6 BFD detection multiplier is the same as the local configured value, you are recommended to configure the same value for the local *multiplier-value* and the remote *multiplier-value*.

If no IPv6 BFD packets are received from the peer within the actual local detection time, the IPv6 BFD session status is set to Down. The actual local detection time is calculated with the following formula: Actual local detection time = Actual local receiving interval x Local detection multiplier.

If IPv6 BFD parameters are configured in both an IS-IS process and an IS-IS interface, IPv6 BFD parameters configured on the interface take effect.

Example

Configure IPv6 BFD for an IS-IS process, and specify the minimum interval for sending IPv6 BFD packets to 300 ms.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 bfd all-interfaces enable
[HUAWEI-isis-1] ipv6 bfd all-interface min-tx-interval 300
```

7.7.8 ipv6 circuit-cost

Function

The **ipv6 circuit-cost** command sets the cost value of all IPv6 interfaces in IS-IS SPF calculation, that is, the global IPv6 cost value.

The **undo ipv6 circuit-cost** command deletes the configured global IPv6 cost value.

By default, the global IPv6 cost value is not set.

Format

ipv6 circuit-cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo ipv6 circuit-cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the cost value of IPv6 interfaces in IS-IS SPF calculation.	IF the IS-IS cost style is **wide** or **wide-compatible**, the cost value of imported routes ranges from 1 to 16777214. Otherwise, the value ranges from 1 to 63.
maximum	Sets the link cost value of an interface to 16777215. **NOTE** This parameter can be configured only when the IS-IS cost style is **wide** or **wide-compatible**. When the link cost value of an interface is set to 16777215, the neighbor TLV generated on the link cannot be used for route calculation and can only be used to transmit TE information.	-
level-1	Indicates the cost value of a Level-1 interface. If the interface level is not specified, the cost value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the cost value of a Level-2 interface. If the interface level is not specified, the cost value is set for Level-1 and Level-2 interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, multiple valid routes to the same destination are available on large IPv6 networks. IS-IS calculates the optimal routes using SPF calculation and chooses the optimal routes for traffic forwarding. This process often causes the following two problems:

- All the traffic is forwarded through the optimal route, which may cause unbalanced load.
- If the optimal route on a network is disconnected intermittently, traffic is still forwarded through the optimal route, which causes traffic loss.

To solve the preceding problems, run the **ipv6 circuit-cost** command to change the cost value of all interfaces at a time and traffic can be forwarded through different physical links.

Precautions

The priority of the IPv6 cost value on the interface is higher than the priority of the global IPv6 cost value.

The **ipv6 circuit-cost** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set the global IPv6 cost value in SPF calculation to 20.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 circuit-cost 20
```

7.7.9 ipv6 circuit default-tag

Function

The **ipv6 circuit default-tag** command sets the administrative tag value of all interfaces in IS-IS processes on an IPv6 network.

The **undo ipv6 circuit default-tag** command restores the default tag value.

By default, the administrative tag value of all interfaces in IS-IS processes on an IPv6 network is 0.

Format

ipv6 circuit default-tag *tag* [**level-1** | **level-2**]

undo ipv6 circuit default-tag [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag value of an interface in an IS-IS process on an IPv6 network.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates the administrative tag value of all Level-1 interfaces in IS-IS processes on an IPv6 network. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the administrative tag value of all Level-2 interfaces in IS-IS processes on an IPv6 network. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **ipv6 circuit default-tag** command, you can set the administrative tag value for all routes of a specified IS-IS process and use the tag to filter routes.

The administrative tag value is advertised together with the routing information.

- When the cost style of IS-IS is narrow or narrow-compatible, the administrative tag value is not advertised in the LSP and does not takes effect.
- When the cost style of IS-IS is wide, wide-compatible, or compatible, the administrative tag value is advertised in the LSP.

Precautions

The **ipv6 circuit default-tag** command takes effect only after IPv6 is enabled for the IS-IS process using the **ipv6 enable** command.

Example

Set the administrative tag value for a Level-1 IPv6 interface to 30.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 circuit default-tag 30 level-1
```

7.7.10 ipv6 default-route-advertise

Function

The **ipv6 default-route-advertise** command configures the switch to advertise default IPv6 routes.

The **undo ipv6 default-route-advertise** disables the switch from advertising default IPv6 routes.

By default, the switch does not advertise default IPv6 routes.

Format

ipv6 default-route-advertise [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost* | **tag** *tag* | [**level-1** | **level-2** | **level-1-2**]] * [**avoid-learning**]

undo ipv6 default-route-advertise

Parameters

Parameter	Description	Value
always	Indicates that the switch always advertises default IPv6 routes.	-
match default	Indicates that if the routing table contains a default IPv6 route generated by other routing protocols but not IS-IS, the default route is advertised through an LSP.	-
route-policy *route-policy-name*	Specifies the name of a route-policy. A Level-1-2 device advertises default routes to the IS-IS routing domain only when there are external routes matching the route-policy in the routing table of the device. This prevents routing blackhole when link faults make some important external routes unavailable but default routes are still advertised. This route-policy does not affect external route import in IS-IS.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cost *cost*	Specifies the cost value of an advertised default route.	The value is an integer that ranges from 0 to 4261412864.
tag *tag*	Specifies the tag value of an advertised default route.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
level-1	Sets the level of advertised default IPv6 routes to Level-1. If the level is not specified, Level-2 default routes are generated by default.	-
level-2	Sets the level of advertised default IPv6 routes to Level-2. If the level is not specified, Level-2 default routes are generated by default.	-
level-1-2	Sets the level of advertised default IPv6 routes to Level-1-2. If the level is not specified, Level-2 default routes are generated by default.	-
avoid-learning	Prevents an IS-IS process from learning default routes and adding them to the routing table. If there has been an active default IPv6 route in the routing table, the default IPv6 route becomes inactive after this parameter is specified.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, if other routing protocols are configured on an IS-IS network, to forward traffic in the IS-IS routing domain outside the domain, use the following two methods:

- Configure IS-IS on a Level-1-2 device to advertise default routes into the IS-IS routing domain.
- Configure IS-IS on a Level-1-2 device to import routes of other routing domains into the IS-IS routing domain.

Advertising default routes is easy to configure and does not require an IS-IS process to learn external routes. You can run the **ipv6 default-route-advertise** command to configure IS-IS devices to advertise default routes into the IS-IS routing domain.

Precautions

Using the route-policy, you can force IS-IS to generate default routes only when there are matched routes in the routing table.

- If the **apply isis level-1** command is used in the route-policy view, IS-ISv6 can generate default routes in Level-1 LSPs. If the **apply isis level-1** command is used in the route-policy view, IS-IS can generate default routes in Level-1 LSPs.

- If the **apply isis level-2** command is used in the route-policy view, IS-ISv6 can generate default routes in Level-2 LSPs.
- If the **apply isis level-1-2** command is used in the route-policy view, IS-ISv6 can generate default routes in Level-1 and Level-2 LSPs.

The **ipv6 default-route-advertise** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, an ABR advertises the default IPv6 route to the IS-IS domain as long as the local routing table contains external routes.

Example

Configure the current switch to generate default IPv6 routes in Level-1-2 LSPs.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 default-route-advertise level-1-2
```

7.7.11 ipv6 enable(IS-IS)

Function

The **ipv6 enable** command enables the IPv6 capability of an IS-IS process.

The **undo ipv6 enable** command disables the IPv6 capability of an IS-IS process.

By default, the IPv6 capability of an IS-IS process is disabled.

Format

ipv6 enable [**topology** { **compatible** [**enable-mt-spf**] | **ipv6** | **standard** }]

undo ipv6 enable

Parameters

Parameter	Description	Value
topology	Specifies the network topology type.	-

Parameter	Description	Value
compatible	Sets the topology type to compatible. That is, the standard topology and the IPv6 topology are compatible. After IS-IS IPv6 adjacency relationship is established, IS-IS advertises IPv6 topology links and standard topology links. SPF, however, runs only in a standard topology. The compatible mode is helpful in a transition from the standard topology to the IPv6 topology.	-
enable-mt-spf	Indicates that SPF runs in the IPv6 topology in compatible mode.	-
ipv6	Sets the topology type to IPv6. That is, the IPv6 capability of an IS-IS process can be enabled in an IPv6 topology. Links on the network can be configured as IPv4 or IPv6 links. SPF calculation is performed separately in IPv4 and IPv6 topologies.	-
standard	Sets the topology type to standard. That is, the IPv6 capability of an IS-IS process can be enabled in the integrated topology. Network administrators must ensure that all links on the network support the same topology mode. If the IPv6 capability of an IS-IS process is enabled, **standard** is used by default.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

To enable the IPv6 capability of an IS-IS process, perform the following operations:

1. Run the **ipv6** command in the system view to enable IPv6 globally.
2. Run the **isis** command to enable an IS-IS process.
3. Run the **network-entity** command to set a NET for IS-IS.
4. Run the **ipv6 enable** command in the IS-IS view to enable the IPv6 capability of an IS-IS process.
5. On each interface that needs to run an IS-IS process, run the **ipv6 enable** command to enable the IPv6 capability and configure an IPv6 address.
6. Run the **isis ipv6 enable** command to enable IS-IS for IPv6 on each interface.

Example

Enable the IPv6 capability in the IPv6 topology in IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
```

```
[HUAWEI-isis-1] network-entity 10.0001.1010.1020.1030.00
[HUAWEI-isis-1] ipv6 enable topology ipv6
```

7.7.12 ipv6 filter-policy export

Function

The **ipv6 filter-policy export** command configures a filtering policy to allow IS-IS to filter the imported IPv6 routes to be advertised.

The **undo ipv6 filter-policy export** command cancels the filtering function.

By default, IS-IS does not filter imported IPv6 routes to be advertised.

Format

ipv6 filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*] | **unr**]

undo ipv6 filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*] | **unr**]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value of *acl6-name* is a string of 1 to 64 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
protocol	Specifies the imported routes that need to be filtered when the routes are advertised. Currently, the *protocol* can be **direct**, **static**, **ripng**, **bgp**, **unr**, **ospfv3**, or another **isis** process. If the *protocol* parameter is not specified, all imported routes are filtered.	-
process-id	Specifies the process ID if *protocol* is **ripng**, **ospfv3**, or another **isis** process.	The value is an integer that ranges from 1 to 65535.
unr	Indicates the imported UNR routes that need to be filtered when the routes are advertised.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ipv6 filter-policy export** command together with the **ipv6 import-route** command can be used to filter only the imported routes that are advertised to other switches. If *protocol* is not specified, the routes that are imported from all other protocols are filtered. If *protocol* is specified, the routes that are imported from the specific protocol are filtered.

The **ipv6 filter-policy export** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all external IPv6 routes of the specified routing domain that are imported by IS-IS are advertised to the specified neighbor.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all external IPv6 routes of the specified routing domain that are imported by IS-IS are advertised to the specified neighbor.

Example

Configure IS-IS to filter the imported IPv6 routes using ACL6 2002 before advertising the IPv6 routes to other switches.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 filter-policy 2002 export
```

7.7.13 ipv6 filter-policy import

Function

The **ipv6 filter-policy import** command configures a filtering policy to allow IS-IS to filter the received routes to be added to the IPv6 routing table.

The **undo ipv6 filter-policy import** command cancels the filtering function.

By default, IS-IS does not filter the received routes to be added to the IPv6 routing table.

Format

ipv6 filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo ipv6 filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value of *acl6-name* is a string of 1 to 64 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS routing entries need to be added to an IPv6 routing table to guide IPv6 packet forwarding. If an IS-IS routing table has routes destined for a specified network segment, but these routes do not need to be sent to the IPv6 routing table, run the **ipv6 filter-policy import** command and specify an IPv6 prefix list or a route-policy to allow only the required IS-IS routes to be added to the IPv6 routing table.

Precautions

The **ipv6 filter-policy import** command can take effect only after IPv6 is enabled for the IS-IS process by the ipv6 enable command.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes received by IS-IS are delivered to the IPv6 routing table.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes received by IS-IS are delivered to the IPv6 routing table.

Example

Filter received IPv6 routes using a route-policy.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 filter-policy route-policy test import
```

7.7.14 ipv6 import-route

Function

The **ipv6 import-route** command configures IS-IS to import IPv6 routes from other routing protocols.

The **undo ipv6 import-route** command disables IS-IS form importing IPv6 routes from other routing protocols.

By default, IS-IS does not import IPv6 routes from other routing protocols.

Format

ipv6 import-route { **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

ipv6 import-route { **static** | **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } [**cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

ipv6 import-route limit *limit-number* [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

undo ipv6 import-route { **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo ipv6 import-route { **static** | **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } [**cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo ipv6 import-route limit [*limit-number*] [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

Parameters

Parameter	Description	Value
direct	Indicates that the imported routes are direct routes.	-
static	Indicates that the imported routes are activated static routes.	-

Parameter	Description	Value
unr	Indicates that the routing protocol from which routes are imported is UNR. The user network route (UNR) is used to allocate routes to user traffic when users cannot use dynamic routing protocols during logins.	-
ospfv3	Indicates that the routing protocol from which routes are imported is OSPFv3.	-
ripng	Indicates that the routing protocol from which routes are imported is RIPng.	-
isis	Indicates that the routing protocol from which routes are imported is IS-IS.	-
process-id	When the protocol is **ospfv3**, **ripng**, or **isis**, a process ID needs to be specified.	The value is an integer that ranges from 1 to 65535.
bgp	Indicates that the routing protocol from which routes are imported is BGP.	-
permit-ibgp	Indicates that the imported routes are IBGP routes. If this parameter is not set, only EBGP routes can be imported.	-
inherit-cost	Indicates that the original cost value of imported external routes is retained.	-
cost *cost*	Specifies the cost value of imported routes.	The value is an integer that ranges from 0 to 4261412864. The default value is 0.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
level-1	Indicates that routes are imported into Level-1 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-2	Indicates that routes are imported into Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-1-2	Indicates that routes are imported into Level-1 and Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
limit *limit-number*	Specifies the maximum number of external IPv6 routes allowed to be imported to the IS-IS area.	The value is an integer ranging from 1 to 10000000.
threshold-alarm	Specifies the alarm threshold for imported routes.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 80.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 70.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If other routing protocols are configured on an IS-IS network, to forward traffic in the IS-IS routing domain outside the domain, use either of the following methods:

- Configure IS-IS on a Level-1-2 device to advertise default routes into the IS-IS routing domain.
- Configure IS-IS on a Level-1-2 device to import routes of other routing domains into the IS-IS routing domain.

If there are multiple Level-1-2 devices in the IS-IS routing domain, optimal routes destined for another routing domain need to be selected. This requires all devices in the IS-IS routing domain learn all or some external routes.

Configure IS-IS on a Level-1-2 device to import routes of other routing domains into the IS-IS routing domain. Alternatively, run the **route-policy** *route-policy-name* command to import some external routes from other routing domains.

Prerequisites

IS-IS has been enabled using the **isis** command and the IS-IS view has been displayed. IPv6 has been enabled for the IS-IS process using the **ipv6 enable** command.

Precautions

When routes of other routing protocols are imported, you can set the cost value and cost style of the imported routes. You can also configure IS-IS to retain the original cost value of the imported external routes. During route advertisement and route calculation, the original cost values of these routes are used. In this case, the cost style and cost value of the imported routes cannot be set, and static routes cannot be imported.

After the **ipv6 import-route direct** command is executed, routes to the network segment where the IPv6 address of the management interface belongs are also imported in the IS-IS routing table. Therefore, use this command with caution.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes of the specified routing domain are imported to the IS-IS routing table.

Example

Configure IS-IS to import static IPv6 routes and set the cost value of the routes to 15.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 import-route static cost 15
```

Configure IS-IS to import OSPFv3 routes and retain the original cost value of the routes.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 import-route ospfv3 1 inherit-cost
```

7.7.15 ipv6 import-route isis level-1 into level-2

Function

The **ipv6 import-route isis level-1 into level-2** command configures IPv6 route leaking from Level-1 areas to Level-2 areas.

The **undo ipv6 import-route isis level-1 into level-2** command prohibits IPv6 route leaking from Level-1 areas to Level-2 areas.

By default, all Level-1 routing information, excluding information about default routes, is leaked to Level-2 areas.

Format

ipv6 import-route isis level-1 into level-2 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

undo ipv6 import-route isis level-1 into level-2 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy for IPv6 routes.	-
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value of *acl6-name* is a string of 1 to 64 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list. Only the routes that match the IPv6 prefix can be imported to Level-2 areas.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Specifies the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can be shared with the Level-2 area with this parameter, and all Level-1 area direct routing information will be shared with the Level-2 area without this parameter.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ipv6 import-route isis level-1 into level-2** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes in the Level-1 area leak to the Level-2 area.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes in the Level-1 area leak to the Level-2 area.

Example

Control IPv6 route leaking from Level-1 areas to Level-2 areas on Level-1-2 routers using IPv6 prefix list **list**.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 import-route isis level-1 into level-2 filter-policy ipv6-prefix list
```

7.7.16 ipv6 import-route isis level-2 into level-1

Function

The **ipv6 import-route isis level-2 into level-1** command configures IPv6 route leaking from Level-2 areas to Level-1 areas.

The **undo ipv6 import-route isis level-2 into level-1** command prohibits IPv6 route leaking from Level-2 areas to Level-1 areas.

By default, Level-2 routing information is not leaked to Level-1 areas.

Format

ipv6 import-route isis level-2 into level-1 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

undo ipv6 import-route isis level-2 into level-1 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy for IPv6 routes.	-
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL. The value is a string of case-sensitive characters.	The value of *acl6-name* is a string of 1 to 64 case-sensitive characters without spaces.

Parameter	Description	Value
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Specifies the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can be shared with the Level-2 area with this parameter, and all Level-1 area direct routing information will be shared with the Level-2 area without this parameter.	-
direct allow-up-down-bit	Indicates that the Up or Down bit is used during the leak of directs routes. If **direct allow-up-down-bit** is specified, the direct routes that have already leaked to the Level-1 area have the lowest priority and cannot leak back.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ipv6 import-route isis level-2 into level-1** command must be configured on Level-1-2 routers at the area border.

The **ipv6 import-route isis level-2 into level-1** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes in the Level-2 area leak to the Level-1 area.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes in the Level-2 area leak to the Level-1 area.

Example

Configure the switch to perform IPv6 route leaking from a Level-2 area to a Level-1 area using filtering policy 2002.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 import-route isis level-2 into level-1 filter-policy 2002
```

7.7.17 ipv6 maximum load-balancing

Function

The **ipv6 maximum load-balancing** command sets the maximum number of IS-IS IPv6 equal-cost routes for load balancing.

The **undo ipv6 maximum load-balancing** command restores the default number of equal-cost routes for load balancing.

By default, IS-IS supports IPv6 load balancing and the maximum number of IS-IS IPv6 equal-cost routes is 8.

Format

ipv6 maximum load-balancing *number*

undo ipv6 maximum load-balancing [*number*]

Parameters

Parameter	Description	Value
number	Specifies the number of IPv6 equal-cost routes for load balancing.	The value is an integer that ranges from 1 to 8.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The **ipv6 maximum load-balancing** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set the maximum number of IS-IS IPv6 equal-cost routes for load balancing to 2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 100
[HUAWEI-isis-100] ipv6 enable
[HUAWEI-isis-100] ipv6 maximum load-balancing 2
```

7.7.18 ipv6 preference

Function

The **ipv6 preference** command configures the preference of IPv6 routes generated by the IS-IS protocol.

The **undo ipv6 preference** command restores the default reference of IPv6 routes generated by the IS-IS protocol.

By default, the preference of IPv6 routes generated by the IS-IS protocol is 15.

Format

ipv6 preference { **route-policy** *route-policy-name* | *preference* } *

undo ipv6 preference

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
preference	Specifies the preference of IPv6 routes generated by the IS-IS. A smaller value indicates a higher priority.	The value is an integer that ranges from 1 to 255.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The routing policy can be used to set the preference for the filtered routes. If the preference is set, only the routes that pass the route-policy can apply the preference specified by this command; otherwise, routes apply the default value of the preference.

Multiple dynamic routing protocols can be run on a switch at the same time. To properly select routes, the system sets a default preference for each routing protocol. If different protocols find routes to the same destination, the route of the protocol with a higher priority is preferred.

The **ipv6 preference** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Precautions

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured priority applies to all IS-IS IPv6 routes.

Example

Set the IS-IS protocol preference to 20.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
```

```
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 preference 20
```

7.7.19 ipv6 prefix-priority (IS-IS)

Function

The **ipv6 prefix-priority** command configures the convergence priority of IS-IS IPv6 routes.

The **undo ipv6 prefix-priority** command restores the default convergence priority of IS-IS IPv6 routes.

By default, the convergence priority of IS-IS IPv6 host routes and default routes is medium, and the convergence priority of other IS-IS IPv6 routes is low.

Format

ipv6 prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** } { **ipv6-prefix** *prefix-name* | **tag** *tag-value* }

undo ipv6 prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** }

Parameters

Parameter	Description	Value
level-1	Specifies the convergence priority of Level-1 IS-IS IPv6 routes.	-
level-2	Specifies the convergence priority of Level-2 IS-IS IPv6 routes.	-
critical	Sets the convergence priority of IS-IS IPv6 routes to critical.	-
high	Sets the convergence priority of IS-IS IPv6 routes to high.	-
medium	Sets the convergence priority of IS-IS IPv6 routes to medium.	-
ipv6-prefix *prefix-name*	Specifies the prefix name of IPv6 addresses for filtering routes to set the convergence priority for IS-IS IPv6 routes that match the specified IPv6 address prefix.	The value of *prefix-name* is a string of 1 to 169 case-sensitive characters without spaces.

Parameter	Description	Value
tag *tag-value*	Specifies the tag value used for filtering routes to set the convergence priority for IS-IS IPv6 routes that carry the specified tag value. To specify the tag value to filter the IPv6 routes that need to be set with the convergence priority, ensure that IS-IS IPv6 routes carry the tag value.	The value is an integer that ranges from 1 to 4294967295.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

This command takes effect only in IPv6 base topologies but not in VPNs.

The convergence priorities of IS-IS IPv6 routes are classified as critical, high, medium, and low in descending order.

After the **ipv6 prefix-priority** command is run to set the convergence priority for IS-IS IPv6 routes, the following situations occur:

- The convergence priority of existing IS-IS IPv6 routes is re-set according to the configuration of the **ipv6 prefix-priority** command.
- The convergence priority of new IS-IS IPv6 routes is set according to the filtering result of the **ipv6 prefix-priority** command.
- If an IS-IS IPv6 route meets the matching rules specified in multiple commands that are used to configure convergence priorities, this IS-IS IPv6 route is of top convergence priority among the set convergence priorities.
- no level is specified, the convergence priority is set for both Level-1 routes and Level-2 routes according to the configuration of the **ipv6 prefix-priority** command.

NOTE

The **ipv6 prefix-priority** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

After the **ipv6 prefix-priority** command is run to set the convergence priority for IS-IS IPv6 routes (including IS-IS IPv6 host routes and default routes), the convergence priority of all the IS-IS IPv6 routes that meet the matching rules is changed according to the configuration of the **ipv6 prefix-priority** command, and the convergence priority of the IS-IS IPv6 routes that do not meet the matching rules is changed to low.

Example

In an IPv6 base topology, set the convergence priority of IS-IS Level-1 routes with tag value 3 to critical.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 prefix-priority level-1 critical tag 3
```

7.7.20 ipv6 spf-priority

Function

The **ipv6 spf-priority** command configures a priority for SPF calculation in an IPv6 base topology.

The **undo ipv6 spf-priority** command restores the default priority for SPF calculation in an IPv6 base topology.

By default, the priority of SPF calculation in an IPv6 base topology is 64.

Format

ipv6 spf-priority *priority-value*

undo ipv6 spf-priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority for SPF calculation in an IPv6 base topology. A larger value indicates a higher priority.	The value is an integer that ranges from 1 to 127.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

A higher priority of SPF calculation in an IPv6 base topology means that the routes in the IPv6 base topology are converged preferentially, which ensures the proper operation of important services.

The **ipv6 spf-priority** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set the priority of SPF calculation in an IPv6 base topology to 30.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
```

```
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 spf-priority 30
```

7.7.21 ipv6 summary

Function

The **ipv6 summary** command configures IS-IS to generate IPv6 summarized routes.

The **undo ipv6 summary** command disables IS-IS from generating IPv6 summarized routes.

By default, IS-IS does not generate IPv6 summarized routes.

Format

ipv6 summary *ipv6-address prefix-length* [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] *

undo ipv6 summary *ipv6-address prefix-length* [**level-1** | **level-1-2** | **level-2**]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the address range of IPv6 routes to be summarized.	-
prefix-length	Specifies the prefix length of an IPv6 route.	The value is an integer that ranges from 0 to 128.
avoid-feedback	Avoids learning summarized routes through SPF calculation.	-
generate_null0_route	Generates NULL0 routes to avoid routing loop.	-
tag *tag*	Specifies the administrative tag value.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates that only routes in Level-1 areas are summarized. If the level is not specified, **level-2** is used by default.	-
level-1-2	Indicates that routes in Level-1 and Level-2 areas are summarized. If the level is not specified, **level-2** is used by default.	-

Parameter	Description	Value
level-2	Indicates that only routes in Level-2 areas are summarized. If the level is not specified, **level-2** is used by default.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The routes with the same prefix can be aggregated into one route. This can reduce the scale of the routing table, the size of the LSPs generated by the local switch, and the scale of the LSDB. The aggregated routes can be the routes discovered by IS-IS or the imported IPv6 routes. After the aggregation, the smallest cost among those of the routes that are aggregated is used as the cost of the aggregated IPv6 route.

The **ipv6 summary** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set a summarized route fc00::/32.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] ipv6 summary fc00:: 32
```

7.7.22 isis ipv6 bfd

Function

The **isis ipv6 bfd** command configures IPv6 BFD detection parameters on a specified interface.

The **undo isis ipv6 bfd** command restores the default values of IPv6 BFD detection parameters on a specified interface.

By default, the minimum interval for sending or receiving IPv6 BFD packets is 1000 milliseconds, and the local IPv6 BFD detection multiplier is 3.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis ipv6 bfd { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* } *

undo isis ipv6 bfd { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] } *

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Specifies the minimum interval for receiving BFD packets from the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-tx-interval *transmit-interval*	Specifies the minimum interval for sending BFD packets to the peer.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Indicates the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPv6 BFD for IS-IS can provide millisecond level fault detection, help IS-IS to detect faults on neighboring devices or links rapidly, and instruct IS-IS to recalculate routes for correct packet forwarding. The **isis ipv6 bfd** command can be used to configure IPv6 BFD detection parameters on a specified interface.

Prerequisites

Before running the **isis ipv6 bfd** command, you need to run the **ipv6 enable** command in the IS-IS process and configure IS-IS on the interface.

The configured IPv6 BFD detection parameters take effect on an interface only when the **isis ipv6 bfd enable** command is configured on the interface.

Precautions

After the local *receive-interval* is compared with the remote *transmit-interval*, the larger value is chosen as the actual local receiving interval. If no IPv6 BFD packets are received from the peer within the actual local detection time, the IPv6 BFD session status is set to Down. The actual local detection time is calculated with the following formula: Actual local detection time = Actual local receiving interval x Local detection multiplier.

NOTE

To ensure that the actual local receiving interval is the same as the local configured value, you are recommended to configure the same value for the local *min-rx-interval* and the remote *min-tx-interval*.

Similarly, to ensure that the actual local IPv6 BFD detection multiplier is the same as the local configured value, you are recommended to configure the same value for the local *multiplier-value* and the remote *multiplier-value*.

The **isis ipv6 bfd** command takes priority over the **ipv6 bfd all-interfaces** command.

Example

Enable IPv6 BFD for IS-IS on Vlanif10, and specify the minimum interval for receiving IPv6 BFD packets to 400 ms and the local detection multiplier to 4.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] isis ipv6 bfd enable
[HUAWEI-Vlanif10] isis ipv6 bfd min-rx-interval 400 detect-multiplier 4
```

7.7.23 isis ipv6 bfd block

Function

The **isis ipv6 bfd block** command disables an interface from dynamically establishing an IPv6 BFD session.

The **undo isis ipv6 bfd block** command cancels the configuration.

By default, no interface is disabled from dynamically establishing a BFD session.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis ipv6 bfd block

undo isis ipv6 bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the **ipv6 bfd all-interfaces enable** command is run in an IS-IS process, IPv6 BFD for IS-IS is enabled on all IS-IS interfaces that are associated with this IS-IS process. You can run the **isis ipv6 bfd block** command to disable an interface from dynamically establishing an IPv6 BFD session.

Prerequisites

To make the **isis ipv6 bfd block** command take effect, do as follows first:

1. Enable IPv6 globally in the system view by using the **ipv6** command.
2. Enable an IS-IS process by using the **isis** command.
3. Enable IPv6 capability of the IS-IS process by using the **ipv6 enable** command in the IS-IS view.
4. On each interface that runs an IS-IS process, enable IPv6 capability by using the **ipv6 enable** command.
5. Enable IS-IS on each interface by using the **isis ipv6 enable** command.

Precautions

The **isis ipv6 bfd block** command and the **isis ipv6 bfd enable** command are mutually exclusive and cannot be run on the same interface.

The function of the **isis ipv6 bfd block** command is similar to the function of the **undo isis ipv6 bfd enable** command, except that:

- After the **undo isis ipv6 bfd enable** command is configured on an IS-IS interface, if the **ipv6 bfd all-interfaces enable** command is reconfigured in the IS-IS view, the interface still has IPv6 BFD for IS-IS capabilities.

- After the **isis ipv6 bfd block** command is configured on an IS-IS interface, the interface does not have IPv6 BFD for IS-IS capabilities, even if the **ipv6 bfd all-interfaces enable** command is reconfigured in the IS-IS view.

NOTE

- To enable IPv6 BFD for IS-IS on most IS-IS interfaces, you need to configure the **isis ipv6 bfd block** command on the IS-IS interfaces that do not need to be enabled with IPv6 BFD for IS-IS, and then configure the **ipv6 bfd all-interfaces enable** command in the IS-IS view.
- To enable IPv6 BFD for IS-IS only on a few IS-IS interfaces, configure the **isis ipv6 bfd enable** command on these interfaces. In this situation, you can configure the **undo isis ipv6 bfd enable** or **isis ipv6 bfd block** command to disable IPv6 BFD for IS-IS on these interfaces.

Example

Disable Vlanif10 from dynamically establishing an IPv6 BFD session.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 bfd block
```

7.7.24 isis ipv6 bfd enable

Function

The **isis ipv6 bfd enable** command enables IPv6 BFD for IS-IS on the IS-IS interface and uses the default parameters to establish an IPv6 BFD session.

The **undo isis ipv6 bfd enable** command disables IPv6 BFD for IS-IS on the IS-IS interface.

By default, if IPv6 BFD for IS-IS is enabled in the IS-IS view, the IS-IS interface is also enabled with IPv6 BFD for IS-IS. If IPv6 BFD for IS-IS is not enabled in the IS-IS view, the IS-IS interface is not enabled with IPv6 BFD for IS-IS either.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

isis ipv6 bfd enable

undo isis ipv6 bfd enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPv6 BFD for IS-IS can provide millisecond level fault detection, help IS-IS to detect faults on neighboring devices or links rapidly, and instruct IS-IS to recalculate routes for correct packet forwarding. The **isis ipv6 bfd enable** command can be used to enable IPv6 BFD for IS-IS on a specified IS-IS interface.

If IPv6 BFD for IS-IS is not enabled globally, you can run the **isis ipv6 bfd enable** command on an interface to enable IPv6 BFD for IS-IS on this interface.

Prerequisites

To make the **isis ipv6 bfd enable** command take effect, do as follows:

1. Enable IPv6 globally in the system view by using the **ipv6** command.
2. Enable an IS-IS process by using the **isis** command.
3. Enable IPv6 capability of the IS-IS process by using the **ipv6 enable** command in the IS-IS view.
4. On each interface that runs an IS-IS process, enable IPv6 capability by using the **ipv6 enable** command.
5. Enable IS-IS on each interface by using the **isis ipv6 enable** command.

Example

Enable IPv6 BFD on Vlanif10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 bfd enable
```

7.7.25 isis ipv6 cost

Function

The **isis ipv6 cost** command sets the link cost value of an IS-IS interface in an IPv6 topology.

The **undo isis ipv6 cost** command restores the default link cost value of an IS-IS interface in an IPv6 topology.

By default, the link cost value of an IS-IS interface in an IPv6 topology is 10.

Format

isis ipv6 cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo isis ipv6 cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the IPv6 link cost value of an interface.	The value is an integer that varies according to the cost style. ● When the cost style is **narrow**, **narrow-compatible** or **compatible**, the value ranges from 1 to 63. ● When the cost style is **wide** or **wide-compatible**, the value ranges from 1 to 16777214. The default value is 10. To set the cost style, use the **cost-style** command.
maximum	Sets the link cost value of an interface to 16777215. **NOTE** This parameter can be configured only when the IS-IS cost style is **wide** or **wide-compatible**. When the link cost value of an interface is set to 16777215, the neighbor TLV generated on the link cannot be used for route calculation and can only be used to transmit TE information.	-
level-1	Specifies the link cost value of a Level-1 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-
level-2	Specifies the link cost value of a Level-2 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale IPv6 network, there may be multiple valid routes to the same destination. IS-IS uses the SPF algorithm to calculate an optimal route and transmits traffic over it, which brings the following problems:

- All traffic is transmitted over the optimal route, causing load imbalance.
- If the optimal route is faulty, traffic will get lost.

To solve the preceding problems, run the **isis ipv6 cost** command to set IPv6 link costs for interfaces so that traffic can be transmitted over different physical links.

Prerequisites

IS-IS has been enabled on a specified interface using the **isis ipv6 enable** [*process-id*] command in the interface view.

Configuration Impact

If the link cost of an interface is changed, routes will be re-calculated on the whole network, causing the changes in traffic forwarding paths.

The priority of the **ipv6 circuit-cost** command is lower than that of the **isis ipv6 cost** command.

If the IPv6 topology type is **compatible** or **standard**, the IPv6 and IPv4 link costs are the same on an interface even though the IPv6 link cost set using the **isis ipv6 cost** command is different from the IPv4 link cost. The IPv6 link cost set using the **isis ipv6 cost** command takes effect only when the IPv6 topology type is **compatible enable-mt-spf** or **ipv6**.

NOTE

The IPv6 topology type can be set for an IS-IS process using the **ipv6 enable(IS-IS)** command.

Example

Set the IPv6 link cost of VLANIF 10 to 50.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 cost 50
```

Set the IPv6 link cost of GE0/0/1 to 50.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 cost 50
```

7.7.26 isis ipv6 enable

Function

The **isis ipv6 enable** command enables the IS-IS IPv6 capability for an interface and specifies the ID of the IS-IS process to be associated with the interface.

The **undo isis ipv6 enable** command disables the IS-IS IPv6 capability of an interface and disassociates an IS-IS process from the interface.

By default, the IS-IS IPv6 capability is disabled on an interface.

Format

isis ipv6 enable [*process-id*]

undo isis ipv6 enable

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After completing the configuration of an IS-IS process in the system view, enable IS-IS IPv6 on the interface that runs IS-IS and associate the interface with the IS-IS process using the **isis ipv6 enable** command.

Prerequisites

The following steps have been performed:

1. Enable IPv6 globally using the **ipv6** command in the system view.
2. Enable an IS-IS process using the **isis** command and configure a network entity title (NET) for the device running IS-IS using the **network-entity** command.
3. Enable IPv6 for the IS-IS process using the **ipv6 enable (IS-IS)** command in the IS-IS view.
4. Enable IPv6 and configure an IPv6 address using the **ipv6 enable** command on each interface that runs the IS-IS process.

Precautions

An interface can be associated with only one IS-IS process.

NOTE

To perform IPv6-related IS-IS configurations, you must enable IPv6 first.

Example

Create IS-IS process 1, enable the IPv6 capability, and activate the IPv6 capability on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] network-entity 10.0001.1010.1020.1030.00
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ipv6 address fc00:0:0:2::1/64
[HUAWEI-Vlanif10] isis ipv6 enable 1
```

Create IS-IS process 1, enable the IPv6 capability, and activate the IPv6 capability on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] network-entity 10.0001.1010.1020.1030.00
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00:0:0:2::1/64
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 enable 1
```

7.7.27 isis ipv6 suppress-reachability

Function

The **isis ipv6 suppress-reachability** command suppresses the advertisement of direct routes on an IPv6 interface in a specified topology.

The **undo isis ipv6 suppress-reachability** command restores the default configuration of an IPv6 interface.

By default, the advertisement of IPv6 addresses on an interface is not suppressed.

Format

isis ipv6 suppress-reachability [**level-1** | **level-1-2** | **level-2**]

undo isis ipv6 suppress-reachability

Parameters

Parameter	Description	Value
level-1	Suppresses the advertisement of IPv6 addresses is suppressed on Level-1 interfaces. If the level is not specified, Level-1-2 is used by default.	-
level-1-2	Indicates that the advertisement of IPv6 addresses is suppressed on Level-1 and Level-2 interfaces. If the level is not specified, Level-1-2 is used by default.	-
level-2	Indicates that the advertisement of IPv6 addresses is suppressed on Level-2 interfaces. If the level is not specified, Level-1-2 is used by default.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You must enable the IPv6 capability for an IS-IS process before running this command. For details, see the **isis ipv6 enable** command.

Example

Suppress the advertisement of IPv6 addresses on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 enable
[HUAWEI-Vlanif10] isis ipv6 suppress-reachability
```

Suppress the advertisement of IPv6 addresses on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
```

```
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 suppress-reachability
```

7.7.28 isis ipv6 tag-value

Function

The **isis ipv6 tag-value** command configures the IPv6 administrative tag value on an IS-IS interface.

The **undo ipv6 isis tag-value** command deletes the IPv6 administrative tag value on an IS-IS interface.

By default, an IS-IS interface has no IPv6 administrative tag value.

Format

isis ipv6 tag-value *tag* [**level-1** | **level-2**]

undo isis ipv6 tag-value [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag value.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates the administrative tag value of a Level-1 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the administrative tag value of a Level-2 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **isis ipv6 tag-value** command, you can set the administrative tag value for all routes of a specified IS-IS process. The tag can be used as a filtering condition of a route-policy to filter routes.

Precautions

You must enable the IPv6 capability for an IS-IS process before running this command.

If the IS-IS cost style is wide, wide-compatible, or compatible, the administrative tag for an interface is advertised using an LSP.

Example

Set the IPv6 administrative tag value of VLANIF100 to 77.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] isis ipv6 enable
[HUAWEI-Vlanif100] isis ipv6 tag-value 77
```

Set the IPv6 administrative tag value of GE0/0/1 tp 77.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] isis 1
[HUAWEI-isis-1] ipv6 enable
[HUAWEI-isis-1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] isis ipv6 tag-value 77
```

7.8 BGP Configuration Commands

7.8.1 Command Support

Only the following switch models support BGP:

S5720I-SI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

NOTE

The S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support only the BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, and BGP-IPv6 unicast address family view.

The S5731-S, S5731S-S, S6730-S, and S6730S-S support only the BGP-IPv4 multicast address family view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

7.8.2 active-route-advertise

Function

The **active-route-advertise** command enables BGP to advertise only the preferred routes in the IP routing table.

The **undo active-route-advertise** command restores the default setting.

By default, BGP advertises all preferred routes in the BGP routing table to neighbors.

Format

active-route-advertise

undo active-route-advertise

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, BGP advertises all preferred routes in the BGP routing table to neighbors. After the **active-route-advertise** is configured, only the routes preferred by BGP and also active at the routing management layer are advertised to neighbors.

Precautions

The **active-route-advertise** command and the **routing-table rib-only** command are mutually exclusive.

Example

Enable BGP to advertise only the preferred routes in the IP routing table to neighbors.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] active-route-advertise
```

7.8.3 aggregate (BGP)

Function

The **aggregate** command creates a summary route in the BGP routing table.

The **undo aggregate** command deletes a summary route from the BGP routing table.

By default, no summary route is created in the BGP routing table.

Format

aggregate *ipv4-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*] *

aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*] *

undo aggregate *ipv4-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*] *

undo aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*] *

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a summary route.	The address is in dotted decimal notation.
mask	Specifies the network mask of a summary route.	The mask is in dotted decimal notation.
mask-length	Specifies the network mask length of a summary route.	The value is an integer that ranges from 0 to 32.
ipv6-address	Specifies the IPv6 address of a summary route.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of the prefix of an IPv6 summary route.	The value is an integer that ranges from 0 to 128.

Parameter	Description	Value
as-set	Generates a route with the AS-SET.	-
attribute-policy *route-policy-name1*	Specifies the name of an attribute policy for summary routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
detail-suppressed	Advertises only the summary route.	-
origin-policy *route-policy-name2*	Specifies the name of a policy that allows route summarization.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
suppress-policy *route-policy-name3*	Specifies the name of a policy for suppressing the advertisement of specific routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP route summarization is classified into manual summarization and automatic summarization. The **aggregate** command can be used to configure manual summarization. This command can summarize routes in the local BGP routing table. Manually-summarized routes take precedence over automatically-summarized routes. The outbound interface of the summary route on the local switch is NULL0. When receiving the summary route, other switches automatically add the outbound interface.

The generated summary route inherits the Origin attribute from the specific routes if they have the same Origin attribute. If the specific routes have different Origin attributes, the summary route selects one as its own from these Origin attributes in descending order of preference: incomplete > egp > igp. If specific routes are not suppressed, the summary route carries the community attribute of every specific route.

The **aggregate** command adds a summary route to the BGP routing table.

- The parameter **as-set** is used to create a summary route whose AS_Path attribute contains AS_Path information of specific routes. Exercise caution when using this parameter if many AS_Path attributes need to be summarized because frequent changes in routes may cause route flapping.
- The parameter **detail-suppressed** is used to suppress the advertisement of specific routes. After **detail-suppressed** is configured, only summary routes are advertised. Summary routes carry the atomic-aggregate attribute, not the community attributes of specific routes.
- The parameter **suppress-policy** is used to suppress the advertisement of specific routes. The **if-match** clause of **route-policy** can be used to filter the routes to be suppressed. This means that only the routes matching the policy will be suppressed, and the other routes will still be advertised. The **peer route-policy** command can also be used to filter out the routes not to be advertised to peers.
- After the parameter **origin-policy** is used, only the routes matching **route-policy** are summarized.
- The parameter **attribute-policy** is used to set attributes for a summary route. If the AS_Path attribute is set in the policy using the **apply as-path** command and **as-set** is set in the **aggregate** command, the AS_Path attribute in the policy does not take effect. The **peer route-policy** command can also be used to set attributes for a summary route.

Prerequisites

Before the **aggregate** command is run, BGP must be enabled.

Configuration Impact

Summary routes are generated after you run the **aggregate** command. If **detail-suppressed** is configured in the command, the advertisement of specific routes will be suppressed. If **suppress-policy** is configured in the command, the advertisement of specific routes that match the policy will be suppressed.

Precautions

When the **undo aggregate** command is run, the system matches routes based on the configured parameter **attribute-policy**, **origin-policy**, **suppress-policy**, **as-set**, or **detail-suppressed**. If none of these parameters is configured, the **undo aggregate** command will fail to be executed.

Example

Create a summary route. The path that is used to advertise this route is an AS-SET consisting of all summarized paths.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] aggregate 172.16.0.0 255.255.0.0 as-set
```

7.8.4 as-notation plain

Function

The **as-notation plain** command configures a BGP 4-byte AS number to be displayed as an integer.

The **undo as-notation plain** command configures a BGP 4-byte AS number to be displayed in dotted notation.

By default, a BGP 4-byte AS number is displayed in dotted notation (that is, in the format of x.y).

Format

as-notation plain

undo as-notation plain

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, display commands such as the **display bgp peer** command display 4-byte AS numbers in dotted notation.

To display a 4-byte AS number as an integer, run the **as-notation plain** command. After the **as-notation plain** command is run, display commands display all 4-byte AS numbers as integers. These 4-byte AS numbers include:

- Independent 4-byte AS number
- 4-byte AS number in an extended community attribute
- 4-byte AS number in a route distinguisher (RD)

- 4-byte AS number in a VPN target (also called a route target)
- 4-byte AS number in the Site-of-Origin attribute

Assume that a 4-byte AS number in dotted notation is *x.y*. Following is the conversion relationship between an integral 4-byte AS number and a 4-byte AS number in dotted notation:

Integral 4-byte AS number = *x* x 65536 + *y*

For example, if a 4-byte AS number in dotted notation is 2.3, the corresponding integral 4-byte AS number is 131075 (2 x 65536 + 3).

Precautions

After the **as-notation plain** command is run, the formats of 4-byte AS numbers in configuration information generated by the system do not change.

- If integral 4-byte AS numbers are configured, 4-byte AS numbers in configuration information generated by the system are also displayed as integers.
- If 4-byte AS numbers in dotted notation are configured, 4-byte AS numbers in configuration information generated by the system are also displayed in dotted notation.

Changing the format of 4-byte AS numbers will affect matching results of AS_Path regular expressions and extended community attribute filters. Therefore, if the system is using an AS_Path regular expression or an extended community attribute filter as an import or export policy, you must reconfigure an AS_Path regular expression using the **ip as-path-filter** command or an extended community attribute filter using the **ip extcommunity-filter** command after changing the format of 4-byte AS numbers. This reconfiguration ensures that routes match the import or export policy.

- If integral 4-byte AS numbers are configured, you must change 4-byte AS numbers in AS_Path regular expressions and extended community attribute filters to integral 4-byte AS numbers.
- If 4-byte AS numbers in dotted notation are configured, you must change 4-byte AS numbers in AS_Path regular expressions and extended community attribute filters to 4-byte AS numbers in dotted notation.

Example

Configure a BGP 4-byte AS number to be displayed as an integer.

```
<HUAWEI> system-view
[HUAWEI] as-notation plain
Warning: If the configuration takes effect, the regular expression of the filter for 4-byte AS path should be
changed to the asplain format, otherwise match will fail. Continue? [Y/N]y
```

Configure a BGP 4-byte AS number to be displayed in dotted notation.

```
<HUAWEI> system-view
[HUAWEI] undo as-notation plain
Warning: If the configuration takes effect, the regular expression of the filter for 4-byte AS path should be
changed to the asdot format, otherwise match will fail. Continue? [Y/N]y
```

7.8.5 as-path-limit

Function

The **as-path-limit** command sets the maximum number of AS numbers in the AS_Path attribute.

The **undo as-path-limit** command restores the default setting.

By default, no limit is configured on the maximum number of AS numbers in the AS_Path attribute, but the maximum number of AS numbers carried in the AS_Path attribute is limited by the BGP message length.

Format

as-path-limit [*as-path-limit-num*]

undo as-path-limit

Parameters

Parameter	Description	Value
as-path-limit-num	Specifies the maximum number of AS numbers in the AS-Path attribute.	The value is an integer that ranges from 1 to 2000. **NOTE** ● The maximum value of *as-path-limit-num* for the 2-byte and 4-byte AS numbers is the same. ● If *as-path-limit-num* is not specified, the maximum number of AS numbers in the AS_Path attribute is 255.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to restrict the maximum number of AS numbers in the AS_Path attribute only when the AS_Path attribute is reconstructed or the aggregated routes are generated.

Precautions

After the **as-path-limit** command is configured, a switch checks whether the number of AS numbers in the AS-Path attribute of each received or advertised route exceeds the maximum value. If the number of AS numbers exceeds the maximum value, the local switch discards the route. Therefore, if the maximum number of AS numbers in the AS-Path attribute is set too small, routes are lost.

Example

Set the maximum number of AS numbers in the AS-Path attribute to 200.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] as-path-limit 200
```

7.8.6 auto-frr

Function

The **auto-frr** command enables BGP Auto FRR.

The **undo auto-frr** command disables BGP Auto FRR.

By default, BGP Auto FRR is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

auto-frr

undo auto-frr

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This function is applicable to networks that require a low packet loss rate and a short delay.

Using BGP Auto FRR together with BFD is recommended. They can rapidly detect a link fault and switch traffic to a standby link if a fault occurs.

Precautions

If both the **ip frr** command and the **auto-frr** command are configured, the **ip frr** command takes precedence over the **auto-frr** command. If a route fails to match the routing policy specified in the **ip frr** command, the **auto-frr** command takes effect.

NOTE

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the **auto-frr** command can implement fast active/standby link switchovers of the forwarding plane and fast route convergence of the control plane. On other switch models, this command can only implement fast route convergence of the control plane.

Example

Enable BGP Auto FRR for unicast routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] auto-frr
```

7.8.7 bestroute as-path-ignore

Function

The **bestroute as-path-ignore** command configures BGP to ignore the AS_Path attribute when it selects the optimal route.

The **undo bestroute as-path-ignore** command restores the default configuration.

By default, BGP uses the AS_Path attribute as one of route selection rules.

Format

bestroute as-path-ignore

undo bestroute as-path-ignore

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **bestroute as-path-ignore** command is used, BGP does not compare the AS path lengths of routes. By default, the route with the shortest AS path is preferred.

Precautions

After the **bestroute as-path-ignore** command is run, the AS_Path attribute is not used as one of the BGP route selection rules.

Example

Configure BGP to ignore the AS_Path attribute when selecting the optimal route.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] bestroute as-path-ignore
```

7.8.8 bestroute igp-metric-ignore

Function

The **bestroute igp-metric-ignore** command configures BGP to ignore the metric value of the next-hop IGP route when selecting the optimal route.

The **undo bestroute igp-metric-ignore** command restores the default setting.

By default, BGP selects a route with the smallest metric value of the next-hop IGP route as the optimal route.

Format

bestroute igp-metric-ignore

undo bestroute igp-metric-ignore

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a BGP network, the BGP device always receives multiple routes with the same prefix but to different paths from neighbors. BGP must select the optimal route to the prefix to guide packet forwarding. By default, BGP compares the next-hop IGP route metric values of these routes and selects the route with the smallest metric value as the optimal route.

To customize route selection policies, you can run the **bestroute igp-metric-ignore** command to configure BGP to ignore the metric value of the next-hop IGP route when selecting the optimal route.

Example

Configure BGP to ignore the IGP metric when selecting the optimal route.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] bestroute igp-metric-ignore
```

7.8.9 bestroute l2vpn-preference vpls

Function

The **bestroute l2vpn-preference vpls** command configures BGP to compare the L2VPN preferences of routes when selecting the optimal route.

The **undo bestroute l2vpn-preference vpls** command restores the default setting.

By default, BGP does not compare the L2VPN preferences when selecting the optimal route.

Format

bestroute l2vpn-preference vpls

undo bestroute l2vpn-preference vpls

Parameters

None

Views

BGP-L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP often receives routes with the same prefix but different next hops from multiple peers. In this case, BGP needs to select the optimal route and deliver it to the routing table to guide packet forwarding.

To configure BGP to compare the L2VPN preferences of routes when selecting the optimal route, run the **bestroute l2vpn-preference vpls** command.

Precautions

This command is valid only for Kompella VPLS.

After this command is configured, routes with the same prefix are preferentially selected.

When you run the **multi-homing-preference** command to configure multi-homing preferences for VSIs, ensure that the preference configured on the local device and that configured on the remote device are different. Otherwise, the **bestroute l2vpn-preference vpls** configuration does not take effect.

Example

Configure BGP to compare the L2VPN preferences of routes when selecting the optimal route.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
[HUAWEI-bgp-af-l2vpn-ad] bestroute l2vpn-preference vpls
```

7.8.10 bestroute med-confederation (BGP)

Function

The **bestroute med-confederation** command enables BGP to compare the Multi Exit Discriminator (MED) values of routes in a confederation when BGP selects the optimal route.

The **undo bestroute med-confederation** command restores the default settings.

By default, BGP compares the MED values of the routes that are from the same AS only.

Format

bestroute med-confederation

undo bestroute med-confederation

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, BGP compares only MED values of routes from the same AS, not including sub-ASs in a confederation. To enable BGP to compare MED values of routes in a confederation when selecting the optimal route, run the **bestroute med-confederation** command.

After the **bestroute med-confederation** command is configured, BGP compares MED values only when AS_Path does not contain the external AS (AS that is not in the confederation) number. Otherwise, BGP does not compare MED values.

For example, ASs 65000, 65001, 65002, and 65004 belong the same confederation. Routes to the same destination are listed as follows:

- path1: AS_Path=65000 65004, med=2
- path2: AS_Path=65001 65004, med=3
- path3: AS_Path=65002 65004, med=4
- path4: AS_Path=65003 65004, med=1

After the **bestroute med-confederation** command is run, the AS_Path attributes of paths 1, 2, and 3 does not contain the numbers of ASs that belong to other confederations. Therefore, when selecting routes based on MED values, BGP compares the MED values of paths 1, 2, and 3 only. This is because the AS_Path attribute of path 4 contains the number of an AS that does not belong to this confederation.

Example

Configure BGP to compare the MED values of routes only in the confederation when selecting the optimal route.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] bestroute med-confederation
```

7.8.11 bestroute med-none-as-maximum

Function

The **bestroute med-none-as-maximum** command configures BGP to assign the maximum Multi Exit Discriminator (MED), 4294967295, to a route without an MED in route selection.

The **undo bestroute med-none-as-maximum** command restores the default configuration.

By default, BGP assigns 0 to a route without an MED in route selection.

Format

bestroute med-none-as-maximum

undo bestroute med-none-as-maximum

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **bestroute med-none-as-maximum** command takes effect in BGP route selection and is used only when the MED is null in the route attributes. If the MED is null and the **bestroute med-none-as-maximum** command is not run, the system probably cannot select an optimal route.

Configuration Impact

During BGP route selection, if the **bestroute med-none-as-maximum** command is run, a route without any MED is assigned the maximum MED of 4294967295.

Example

Configure BGP to assign the maximum MED of 4294967295 to a route without an MED in route selection.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] bestroute med-none-as-maximum
```

7.8.12 bestroute nexthop-resolved

Function

The **bestroute nexthop-resolved** command configures the condition of the route selection of labeled BGP IPv4 routes, VPNv4 routes, or VPNv6 routes for next hop recursion.

The **undo bestroute nexthop-resolved** command restores the default configuration.

By default, labeled BGP IPv4 routes, VPNv4 routes, or VPNv6 routes participate in route selection only when their next hops recurse to IP addresses.

Product	Support
S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

bestroute nexthop-resolved { **ip** | **tunnel** }

undo bestroute nexthop-resolved

Parameters

Parameter	Description	Value
ip	Allows labeled routes that recurse to IP addresses to participate in route selection.	-
tunnel	Allows labeled routes that recurse to MPLS tunnels to participate in route selection.	-

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Route Reflector (RR) networking where the next hop of a labeled BGP IPv4 route is changed or non-RR networking, BGP needs to check whether there is an LSP destined for the next hop. If the LSP is not found, BGP needs to establish an LSP in advance. If the default setting is adopted, a labeled BGP IPv4 unicast route may be selected prior to LSP establishment. As a result, services are incorrectly switched before LSP establishment and service stability is affected. The **bestroute nexthop-resolved tunnel** command can be run to allow route selection only after the labeled BGP IPv4 route recurses to an LSP. This ensures service stability.

By default, a VPNv4 route or VPNv6 routes can participate in route selection if its next hop recurses to an IP address. The system adds the optimal VPNv4 route or VPNv6 route to the forwarding table for traffic forwarding. However, traffic cannot be forwarded over the route if the route does not recurse to an LSP. In this situation, run the **bestroute nexthop-resolved tunnel** command to enable VPNv4 routes or VPNv6 routes to be available in route selection only when their next hops recurse to LSPs to ensure uninterrupted traffic forwarding.

Precautions

The **bestroute nexthop-resolved ip** and **bestroute nexthop-resolved tunnel** commands are mutually exclusive.

Example

In the BGP VPNv4 view, configure BGP VPNv4 routes that recurse to LSP tunnels to participate in route selection.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] bestroute nexthop-resolved tunnel
```

In the BGP VPNv6 view, configure BGP VPNv6 routes that recurse to LSP tunnels to participate in route selection.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv6-family vpnv6
[HUAWEI-bgp-af-vpnv6] bestroute nexthop-resolved tunnel
```

7.8.13 bestroute routerid-prior-clusterlist

Function

The **bestroute routerid-prior-clusterlist** command enables Originator_ID to take precedence over Cluster_List during BGP route selection.

The **undo bestroute routerid-prior-clusterlist** command restores the default configurations.

By default, Cluster_List takes precedence over Originator_ID during BGP route selection.

Format

bestroute routerid-prior-clusterlist

undo bestroute routerid-prior-clusterlist

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP-IPv4 multicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-L2VPN address family view

Default Level

2: Configuration level

Usage Guidelines

On a BGP network, after a device receives multiple routes with the same prefix but different paths from different peers, the device needs to select an optimal route from these routes to forward packets. By default, Cluster_List takes precedence over Originator_ID during BGP route selection. To enable Originator_ID to take precedence over Cluster_List during BGP route selection, run the **bestroute routerid-prior-clusterlist** command.

Example

Enable Router ID to take precedence over Cluster_List during BGP route selection.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] bestroute routerid-prior-clusterlist
```

7.8.14 bgp

Function

The **bgp** command enables BGP and displays the BGP view.

The **undo bgp** command disables BGP.

By default, BGP is disabled.

Format

bgp { *as-number-plain* | *as-number-dot* }

undo bgp [*as-number-plain* | *as-number-dot*]

Parameters

Parameter	Description	Value
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP is an inter-AS dynamic routing protocol. BGP running within an AS is called Internal BGP (IBGP), and BGP running between ASs is called External BGP (EBGP).

Whether to apply BGP to routing information transmission between ASs depends on the following conditions:

- If at least one of the following conditions is met, BGP can be used:
  - An AS allows data packets to pass through on their way to another AS.
  - Multiple connections to external ISPs and the Internet exist in ASs.
  - Data flows entering or leaving ASs must be controlled.
- If one of the following conditions is met, BGP does not need to be used:
  - Users are connected to only one ISP network.
  - The ISP does not need to provide Internet access services for users.
  - ASs adopt default routes between each other.

Precautions

- After the **bgp** command is run, BGP is enabled.
- Each device runs in only one AS; therefore, each device can be specified with only one local AS number.
- If the BGP AS number is changed, the route calculation result of the local or remote OSPF VPN process may be affected. Because the tag value of the LSAs of the OSPF VPN process is calculated based on the BGP AS number, the local tag value of the OSPF VPN process and the tag value carried in the LSA advertised by the OSPF VPN process change. After receiving an LSA, the local or remote OSPF process checks the tag of the LSA. If the local tag of the OSPF process is the same as the tag of the received LSA, the LSA is not used for OSPF route calculation.

NOTICE

After the **undo bgp** [*as-number-plain* | *as-number-dot*] command is run, BGP services may be interrupted, and all BGP configurations on the device are cleared. Therefore, exercise caution when you run this command.

Example

Enable BGP and enter the BGP view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp]
```

7.8.15 bgp dynamic-session-limit

Function

The **bgp dynamic-session-limit** command configures a maximum number for dynamic BGP peer sessions.

The **undo bgp dynamic-session-limit** command restores the default configuration.

By default, a maximum of 100 dynamic BGP peer sessions can be established after the dynamic BGP peer function is enabled.

Format

bgp dynamic-session-limit *limit-value*

undo bgp dynamic-session-limit [*limit-value*]

Parameters

Parameter	Description	Value
limit-value	Specifies the maximum number of dynamic BGP peer sessions allowed.	The value is an integer that ranges from 1 to 256.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the dynamic BGP peer function is enabled using the **peer listen-net** command, BGP listens to BGP connection requests from the network segment specified in the command and establish BGP peer relationships dynamically. If a large number of dynamic BGP peer sessions are established, excessive system resources will be consumed. To prevent this problem, run the **bgp dynamic-session-limit** command to configure a maximum number for dynamic BGP peer sessions as required.

Precautions

This command does not apply to static BGP peer sessions.

Example

Configure the maximum number of dynamic BGP peer sessions to 128.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] bgp dynamic-session-limit 128
```

7.8.16 bgp fast-refresh enable

Function

The **bgp fast-refresh enable** command enables the BGP Prefix Independent Convergence (PIC) function.

The **undo bgp fast-refresh enable** command disables the BGP PIC function.

By default, the BGP PIC function is enabled on the switch.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

bgp fast-refresh enable

undo bgp fast-refresh enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When there are primary and backup paths for a BGP route, and a fault occurs on the primary path, the route must be updated and traffic must be switched to the backup path as soon as possible. This process is called BGP route convergence. As the network expands in scale and route prefixes, the BGP route convergence speed is affected by the number of route prefixes. More route prefixes indicate slower route convergence speed. If a network fault occurs, many packets are lost due to the slow route convergence speed. This can have a large impact on some services that are sensitive to packet loss. BGP PIC is also called BGP fast refresh. It indicates that the BGP route convergence speed is independent of the number of route prefixes. After this function is enabled, the BGP route convergence speed becomes faster without being affected by the number of route prefixes. This function reduces data loss during route convergence. When this function becomes unavailable, you can run the **undo bgp fast-refresh enable** command to disable it. BGP routes are then converged as usual; however, the route convergence speed is slow.

Precautions

- Only IBGP routes support the BGP PIC function, and VPN routes do not support this function.
- If the BGP load balancing (ECMP) or BGP Auto FRR function has been configured on the device or the next hop of a BGP route recurses to a tunnel interface, the BGP PIC function does not take effect.
- Disabling the BGP PIC function requires the device to be restarted after the configuration is saved or requires all BGP ASs to be **reset**. Otherwise, disabling the BGP PIC function takes effect only for the subsequently generated routing tables.

  Enabling the BGP PIC function requires the device to be restarted.

Example

Disable the BGP PIC function on the switch.

```
<HUAWEI> system-view
[HUAWEI] undo bgp fast-refresh enable
Warning: The operation will take effect only on routing tables generated later.
Please save configuration and reboot this device or reset all BGP ASs after this
 operation.
```

7.8.17 check-first-as

Function

The **check-first-as** command enables the function to check the first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer.

The **undo check-first-as** command disables the function.

By default, the function is enabled.

Format

check-first-as

undo check-first-as

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, BGP checks the first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer. If only the first AS number indicates the AS where the EBGP peer locates, the Update message is accepted. Otherwise, the Update message is denied, and the EBGP connection goes Down.

Precautions

The **check-first-as** command is not listed in the configuration file.

After the **undo check-first-as** command is configured, loops have a greater chance to occur. Therefore, use the command with caution.

Follow-up Procedure

After the configuration is complete, run the **refresh bgp** command if you want to check the received routes again.

Example

Check the first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] check-first-as
```

7.8.18 compare-different-as-med

Function

The **compare-different-as-med** command enables BGP to compare the MEDs in the routes of peers in different ASs.

The **undo compare-different-as-med** command restores the default configuration.

By default, BGP does not compare the MEDs in the routes of peers in different ASs.

Format

compare-different-as-med

undo compare-different-as-med

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command is used to control the MEDs to change the policy of BGP route selection. If the **compare-different-as-med** command is run, BGP will compare the MEDs of the routes from different ASs. If there are multiple reachable paths to the same destination, BGP prefers the route with the smallest MED.

Precautions

Do not use this command unless different ASs use the same IGP and route selection mode.

Example

Enable BGP to compare the MEDs in the routes of peers in different ASs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] compare-different-as-med
```

7.8.19 confederation id

Function

The **confederation id** command configures a BGP confederation and specifies a confederation ID for the BGP confederation.

The **undo confederation id** command removes the specified BGP confederation.

By default, no BGP confederation is configured.

Format

confederation id { *as-number-plain* | *as-number-dot* }

undo confederation id

Parameters

Parameter	Description	Value
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large AS may contain a huge number of fully meshed IBGP peer relationships. In this situation, configure a confederation.

Divide the AS into multiple small sub-ASs and group them into a confederation. Then establish EBGP connections between sub-ASs and establish fully meshed IBGP connections within the same sub-AS. Some key attributes of routes, such as the next hop, MED, and local preference are not discarded when these routes pass through sub-ASs. This can reduce the number of fully meshed IBGP peer relationships in an AS and keep the integrity of the original AS.

Precautions

The confederation ID is equal to the AS number. An external AS must specify the confederation ID when specifying the AS number of the peer. All the sub-ASs in the same confederation must be configured with the same confederation ID that must be different from the number of any sub-AS.

Example

Configure a confederation ID. An AS is divided into sub-ASs 65001, 65002, 65003, and 65004, and their confederation ID is 9. Peer 10.2.3.4 is a member of the AS confederation. Peer 10.4.5.6 is a member outside the AS confederation. For the external members, confederation 9 is a complete AS.

```
<HUAWEI> system-view
[HUAWEI] bgp 65001
[HUAWEI-bgp] confederation id 9
[HUAWEI-bgp] confederation peer-as 65002 65003 65004
[HUAWEI-bgp] peer 10.2.3.4 as-number 65002
```

```
[HUAWEI-bgp] peer 10.4.5.6 as-number 65005
```

7.8.20 confederation nonstandard

Function

The **confederation nonstandard** command configures standard devices (in RFC 3065) in a confederation to communicate with nonstandard devices.

The **undo confederation nonstandard** command configures standard devices in a confederation to communicate only with standard devices.

By default, only standard devices in a confederation can communicate with each other.

Format

confederation nonstandard

undo confederation nonstandard

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To communicate with nonstandard devices, configure this command on all switches in a confederation.

Precautions

After the confederation ID is configured, running the **confederation nonstandard** command will disconnect the sessions between a router and its IBGP peers as well as its confederation EBGP peers. Then, new connections are reestablished.

Example

Enable the switch to communicate with nonstandard routers. AS 100 contains two sub-ASs, 64000 and 65000.

```
<HUAWEI> system-view
[HUAWEI] bgp 64000
[HUAWEI-bgp] confederation id 100
[HUAWEI-bgp] confederation peer-as 65000
[HUAWEI-bgp] confederation nonstandard
```

7.8.21 confederation peer-as

Function

The **confederation peer-as** command configures the number of each sub-AS of the same confederation.

The **undo confederation peer-as** command removes the specified sub-AS from the confederation.

By default, no sub-AS number of a confederation is configured.

Format

confederation peer-as { *as-number-plain* | *as-number-dot* } &<1-32>

undo confederation peer-as { *as-number-plain* | *as-number-dot* } &<1-32>

Parameters

Parameter	Description	Value
as-number-plain	Specifies the number of an AS, which is an integer.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of an AS, which is in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large AS may contain a huge number of fully meshed IBGP peer relationships. In this situation, configure a confederation.

Prerequisites

The **confederation id** command specifies the confederation ID of each sub-AS. If the confederation ID is not configured, this configuration is invalid.

Precautions

The sub-ASs configured in this command belong to the same confederation, and each sub-AS uses fully meshed network.

Example

Configure sub-ASs for a confederation.

```
<HUAWEI> system-view
[HUAWEI] bgp 1090
[HUAWEI-bgp] confederation id 100
[HUAWEI-bgp] confederation peer-as 1091 1092 1093
```

7.8.22 confederation route unicast-to-label disable

Function

The **confederation route unicast-to-label disable** command prevents non-RRs from advertising the IPv6 non-labeled routes learned from peers in the local confederation as labeled routes carrying a label of all Fs to the BGP peers in another confederation.

The **undo confederation route unicast-to-label disable** command restores the default configuration.

By default, non-RRs can advertise the IPv6 non-labeled routes learned from peers in the local confederation as labeled routes carrying a label of all Fs to the BGP peers in another confederation.

Product	Support
S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5731-S, S5731S-S, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

confederation route unicast-to-label disable

undo confederation route unicast-to-label disable

Parameters

None

Views

BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

If two PEs that are not RRs reside in two confederations, the PEs can advertise labeled routes carrying a label of all Fs to each other by default. However, non-Huawei devices may consider the label of all Fs invalid, and if these non-Huawei devices receive such labeled routes, BGP peer relationships may be disconnected. To prevent this problem, run the **confederation route unicast-to-label disable** command to prevent the PEs from advertising labeled routes carrying a label of all Fs.

Example

Prevent non-RRs from advertising the IPv6 non-labeled routes learned from peers in the local confederation as labeled routes carrying a label of all Fs to the BGP peers in another confederation.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] confederation id 100
[HUAWEI-bgp] confederation peer-as 38 39
[HUAWEI-bgp] peer 192.168.1.1 as-number 38
[HUAWEI-bgp] peer fc00:0:0:191::1 as-number 39
[HUAWEI-bgp] ipv6-family unicast
[HUAWEI-bgp-af-ipv6] peer 192.168.1.1 enable
[HUAWEI-bgp-af-ipv6] peer 192.168.1.1 label-route-capability
[HUAWEI-bgp-af-ipv6] peer fc00:0:0:191::1 enable
[HUAWEI-bgp-af-ipv6] confederation route unicast-to-label disable
```

7.8.23 dampening

Function

The **dampening** command enables BGP route flap suppression and modifies BGP route flap suppression parameters.

The **undo dampening** command restores the default configuration.

By default, BGP route flap suppression is disabled.

Format

dampening [ibgp] [*half-life-reach reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening [ibgp]

Parameters

Parameter	Description	Value
half-life-reach	Specifies the half life of a reachable route.	The value is an integer that ranges from 1 to 45, in minutes. The default value is 15.
reuse	Specifies the threshold for the route to be unsuppressed. If the penalty of the route falls below the threshold, the route is reused.	The value is an integer that ranges from 1 to 20000. The default value is 750.
suppress	Specifies the threshold for the route to be suppressed. If the penalty value of the route exceeds the threshold, the route is not used.	The value is an integer that ranges from 1 to 20000, which must be greater than the value of *reuse*. The default value is 2000.
ceiling	Specifies the penalty ceiling.	The value is an integer that ranges from 1001 to 20000. The configured value must be greater than that of *suppress*. The default value is 16000.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ibgp	Specifies the route type as IBGP route. If this parameter is not specified, the route type is EBGP route. **NOTE** This parameter takes effect only in the BGP-VPNv4 address family view.	-

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP-IPv4 multicast address family view, BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP route flap dampening measures the stability of a route by using a penalty value. The greater the penalty value, the less stable the route. Each time route flapping occurs, that is, when the switch receives a Withdraw packet or an Update packet for a route, BGP adds a certain penalty value (1000) for the route.

When the penalty value of the route exceeds the suppression threshold, the route is suppressed. The switch does not add the route to the IP routing table or advertise any Update packet to other BGP peers. If the route is marked with the d flag, the last packet received by the switch is an Update packet; if the route is marked with the h flag, the last packet received by the switch is a Withdraw packet. After the penalty value reaches a certain limit, it does not increase any more. The limit is called the penalty ceiling.

After the route is suppressed for a certain period, the penalty value is reduced by half. If the penalty value of a route marked with the d flag decreases to the reuse threshold, the d flag is removed, and the route becomes available and is selected preferentially. After that, the route can be added to the IP routing table and used to send Update packets to other BGP peers. If the penalty value of a route marked with the h flag decreases to 0, the route is deleted from the BGP routing table.

You can run the **display bgp routing-table label** command to check the d flag and h flag indicating the routes that have been dampened and were dampened respectively.

Precautions

If the **dampening** command is run multiple times, the latest configuration overrides the previous one.

After the **dampening** command is run, the system suppresses unstable routes. This means that the system does not add unstable routes to the BGP routing table or advertise them to other BGP peers.

Note the following items when configuring BGP route flap dampening:

- The value of *suppress* must be greater than that of *reuse* and smaller than that of *ceiling*.
- If MaxSuppressTime obtained by using the formula of MaxSuppressTime = *half-life-reach* x 60 x (ln(*ceiling*/*reuse*)/ln(2)) is smaller than 1, suppression cannot be performed. You need to ensure that the value of MaxSuppressTime is equal to or greater than 1. This means that the value of *ceiling*/*reuse* must be great enough.

NOTE

The **dampening** command is valid only for EBGP routes.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-**

policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured dampening parameters apply to all routes; if no dampening parameters are configured, the default dampening parameters apply to the routes.

Example

Enable EBGP route dampening and modify EBGP route damping parameters.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] dampening 10 1000 2000 5000
```

7.8.24 default ipv4-unicast

Function

The **default ipv4-unicast** command enables the IPv4 unicast address family for BGP peers by default.

The **undo default ipv4-unicast** command disables the IPv4 unicast address family for BGP peers by default.

By default, the IPv4 unicast address family is enabled for BGP peers.

Format

default ipv4-unicast

undo default ipv4-unicast

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the IPv4 unicast address family needs to be enabled by default for created BGP peers, the **default ipv4-unicast** command can be used to configure the default address family of BGP to the IPv4 unicast address family.

If the IPv4 unicast address family does not need to be enabled by default for created BGP peers, the **undo default ipv4-unicast** command can be used to disable the IPv4 unicast address family for all peers.

Precautions

After the **undo default ipv4-unicast** command is run, the **peer enable** command needs to be run if the created BGP peer needs to be enabled with the IPv4 unicast address family.

Example

Enable the IPv4 unicast address family for all peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] default ipv4-unicast
```

7.8.25 default local-preference

Function

The **default local-preference** command sets the default local preference for BGP routes.

The **undo default local-preference** command restores the default configuration.

By default, the local preference for BGP routes is 100.

Format

default local-preference *local-preference*

undo default local-preference

Parameters

Parameter	Description	Value
local-preference	Specifies the local preference for BGP routes. The greater the value, the higher the preference.	The value is an integer that ranges from 0 to 4294967295.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Local_Pref attribute is used to determine an optimal route for traffic before traffic leaves an AS. When the switch that runs BGP has multiple routes to the same destination, the switch selects the route with the highest local preference as the optimal route.

Precautions

If the switch is already configured with a default local preference for BGP routes, the configuration of a new default local preference will override the previous configuration.

The local preference is exchanged only between IBGP peers and is not advertised to other ASs.

Example

Set the default local preference for BGP routes to 200.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] default local-preference 200
```

7.8.26 default med

Function

The **default med** command sets the default multi-exit-discriminator (MED) for BGP routes.

The **undo default med** command restores the default configuration.

By default, the MED is 0.

Format

default med *med*

undo default med

Parameters

Parameter	Description	Value
med	Specifies the MED for BGP routes.	The value is an integer that ranges from 0 to 4294967295.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **default med** command is valid only for the routes imported by using the **import-route (BGP)** command and the routes summarized by BGP on the local device.

The **default med** command sets the default MED and controls route selection for the traffic entering an AS. If the other attributes of routes to the same destination are the same, BGP will select the route with the smallest MED as the optimal route.

Precautions

If a default MED is configured on a device, configuring a new default MED will override the previous configuration and the new default MED will overwrite the previous one.

The MED is transmitted between two neighboring ASs only. Devices in an AS do not advertise the received MED to peers in other ASs.

Example

Set the default MED of a BGP route to 10.

```
<HUAWEI> system-view
[HUAWEI] bgp 1
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] default med 10
```

7.8.27 default-route imported

Function

The **default-route imported** command enables the import of default routes in the local IP routing table to the BGP routing table.

The **undo default-route imported** command disables the import of the default routes in the local IP routing table to the BGP routing table.

By default, BGP does not add the default route to the BGP routing table.

Format

default-route imported

undo default-route imported

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This configuration reduces the number of routes on the network and minimizes the routing table size. If a default route exists in the local IP routing table and the **default-route imported** command is run, the system imports the default route to the BGP routing table. After the default route is imported, the packets can be transmitted over the default route when no matched routing entry is found in the routing table, preventing packet loss.

Precautions

To import default routes, you need to run both the **default-route imported** command and the **import-route (BGP)** command. If only the **import-route (BGP)** command is used, default routes cannot be imported. In addition, the **default-route imported** command is used to import only the default routes that exist in the local routing table.

When a device needs to advertise default routes to a peer (group) and no default route exists in the local routing table, the **peer default-route-advertise** command needs to be used.

Example

Import default routes to the BGP routing table.

```
<HUAWEI> system-view
[HUAWEI] bgp 1
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] default-route imported
[HUAWEI-bgp-af-ipv4] import-route ospf 1
```

7.8.28 deterministic-med (BGP)

Function

The **deterministic-med** command enables the BGP deterministic-MED function so that routes with the same leftmost AS number are first compared during route selection.

The **undo deterministic-med** command disables the BGP deterministic-MED function so that routes are compared against each other according to the sequence in which they are received.

By default, the BGP deterministic-MED function is disabled.

Format

deterministic-med

undo deterministic-med

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

After the BGP deterministic-MED function is enabled, when an optimal route is to be selected from routes that are received from different ASs and carry the same prefix, routes are first grouped based on the leftmost AS number in the AS_Path attribute. Routes with the same leftmost AS number are grouped together, and after comparison, an optimal route is selected for the group. The group optimal route is then compared with optimal routes from other groups to determine the final optimal route. This mode of route selection ensures that the sequence in which routes are received is irrelevant to the route selection result.

If the BGP deterministic-MED function is disabled, routes are compared against each other according to the sequence in which they are received. In this manner, the sequence in which routes are received is relevant to the result of route selection.

For example: Assume that the following BGP routes are available on the switch.

- Route A1: AS(PATH) 12, med 100, igp metric 13, internal, rid 4.4.4.4
- Route A2: AS(PATH) 12, med 150, igp metric 11, internal, rid 5.5.5.5
- Route B: AS(PATH) 3, med 0, igp metric 12, internal, rid 6.6.6.6

If Route A1, Route A2, and Route B are received in turn, Route A1 and Route A2 are first compared. The leftmost AS number of Route A1 is the same as the leftmost AS number of Route A2, and therefore Route A1 is selected because its MED is smaller. After that, Route A1 and Route B are compared. Because the leftmost AS numbers of the two routes are different, the optimal route cannot be selected by comparing the MEDs of the two routes unless the **compare-different-as-med** command is configured. As a result, Route B is selected because its IGP metric is smaller.

If Route A2, Route B, and Route A1 are received in turn, Route A2 and Route B are first compared. Because leftmost AS number of Route A2 is different from the leftmost AS number of Route B, the optimal route cannot be selected by comparing the MEDs of the two routes unless the **compare-different-as-med** command is configured. As a result, Route A2 is selected because its IGP metric is smaller. After that, Route A2 and Route A1 are compared. The leftmost AS number of Route A1 is the same as the leftmost AS number of Route A2, and therefore Route A1 is selected because its MED is smaller.

Judging from the preceding route selection procedure, when the BGP deterministic-MED function is disabled, the sequence in which routes are received is relevant to the result of route selection. After the BGP deterministic-MED function is enabled, the sequence in which routes are received is no longer relevant to the result of route selection. Route A1 and Route A2 have the same leftmost AS number, Route A1 and Route A2 are compared first regardless of the sequence in which routes are received.

Example

Enable the deterministic-MED function in the BGP view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] deterministic-med
```

7.8.29 display bgp bfd session

Function

The **display bgp bfd session** command displays information about BFD sessions between BGP peers.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp bfd session { [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** *ipv4-address* | **all** }

Parameters

Parameter	Description	Value
vpnv4 vpn-instance *vpn-instance-name*	Displays information about the BFD session between BGP peers with the specified IPv4 VPN instance name.	The value must be an existing VPN instance name.
peer *ipv4-address*	Displays information about the BFD session of the BGP peer with the specified IPv4 address.	The value is in dotted decimal notation.
all	Displays all BFD sessions between BGP peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The BFD session set up by BGP helps BGP quickly discover faults between BGP peers and informs BGP to recalculate routes for packet forwarding.

Run the **display bgp bfd session** command to display information about the BFD session set up by BGP in the following situations:

- Check whether the BFD session is successfully set up or view detailed information about the BFD session that is successfully configured.
- Check whether the BFD session set up by BGP is successfully deleted after running the **undo peer bfd enable** command.
- Verify the configuration after running the **undo peer bfd block** command to prevent a peer from inheriting the BFD function of the peer group.
- Verify the configuration after running the **peer bfd** command to set BFD parameters.

The information about the BFD session of a specified BGP peer can be displayed by specifying different parameters.

- Run the **display bgp bfd session vpnv4 vpn-instance** *vpn-instance-name* **peer** *ipv4-address* command to display information about the BFD session of a specified BGP peer in a specified VRF.
- Run the **display bgp bfd session peer** *ipv4-address* command to display information about the BFD session of a specified BGP peer on the public network.
- Run the **display bgp bfd session all** command to display information about the BFD sessions of all BGP peers.

Prerequisites

The BFD session has been set up using the **peer bfd enable** command. If the BFD session has not been set up by BGP, no information is displayed after running the **display bgp bfd session** command.

Example

Display all BFD sessions between BGP peers.

```
<HUAWEI> display bgp bfd session all
  Local_Address      Peer_Address       LD/RD       Interface
  10.1.1.2           10.1.1.1           8192/8193   Unknown
  Tx-interval(ms)    Rx-interval(ms)    Multiplier  Session-State
  1000               1000               3           Up
  Wtr-interval(m)
0
```

Table 7-122 Description of the display bgp bfd session command output

Item	Description
Local_Address	Local address
Peer_Address	Peer address

Item	Description
LD/RD	Local/remote discriminator
Interface	Interface on which the BFD session is set up **NOTE** Information about the interface on which the BFD session is set up only when the directly connected interface is used to set up the EBGP neighbor relationship. In other cases, information about the interface is displayed as Unknown.
Tx-interval (ms)	Interval for sending BFD packets, in milliseconds
Rx-interval (ms)	Interval for receiving BFD packets, in milliseconds
Multiplier	Local detection multiple
Session-State	BFD status ● Admin down: The BFD session is closed on the local end. ● BFD global disable: BFD is disabled globally. ● BFD session number exceed: The number of BFD sessions exceeds the maximum limit. ● Detect down: BFD detects a link status fault and interrupts the connection. ● Init: The BFD session is in the initialized state. ● Neighbor down: The peer end detects that the BFD session goes Down and informs the local end of the change, and the local end then sets the neighbor status to Down. ● Receive admin down: The BFD session is closed on the peer end (for example, the BFD session is disabled on the peer end). ● Up: The BFD session is set up.
Wtr-interval(m)	Interval for flap dampening, in minutes

7.8.30 display bgp error

Function

The **display bgp error** command displays BGP errors.

Format

display bgp error

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a BGP fault occurs, run the **display bgp error** command to display BGP error information. BGP error information includes peer error information, route error information, and resource threshold-crossing error information.

Precautions

If no BGP fault occurs, no information is displayed after running the **display bgp error** command.

Example

Display BGP errors.

```
<HUAWEI> display bgp error
 Error Type    : Peer Error
 Date/Time     : 2010/03/22 11:40:39 UTC-08:00
 Peer Address  : 10.1.1.2
 VRF Name      : Public
 Error Info    : Router-ID conflict

 Error Type    : Peer Error
 Date/Time     : 2010/03/22 11:40:39 UTC-08:00
 Peer Address  : 10.1.1.2
 VRF Name      : Public
 Error Info    : Incorrect remote AS

 Error Type    : Route Error
 AddressFamily : IPv4-UNC
 InstanceID    : 0
 Discard count : 20

 Error Type    : Resource exceed limit
 Date/Time     : 2010/03/22 11:40:39 UTC-08:00
 Limit info    : Route number limit

 Error Type    : Resource exceed limit
 Date/Time     : 2010/03/22 11:40:39 UTC-08:00
 Limit info    : Label number limit
```

Table 7-123 Description of the display bgp error command output

Item	Description
Error Type	Error type: ● Peer Error: indicates neighbor errors. ● Route Error: indicates route errors. ● Resource exceed limit: indicates that resources exceed the limit.
Date/Time	Date and Time when an error occurs
Peer Address	Address of a peer
VRF Name	VPN Instance name
Error Info	Error information: ● Router-ID conflict: indicates that router IDs conflict. ● Incorrect remote AS: indicates an incorrect remote AS number.
AddressFamily	Address family
Discard count	Number of discarded routes
Limit info	Information indicating that resources exceed the limit: ● Memory shortage: indicates that memory exceeds the limit. ● Route number limit: indicates that the number of routes exceeds the limit. ● Label number limit: indicates that the number of labels exceeds the limit.

7.8.31 display bgp error discard

Function

The **display bgp error discard** command displays the information about the discarded error BGP packets.

Format

display bgp error discard [**peer** { *ipv4-address* | *ipv6-address* }]

Parameters

Parameter	Description	Value
peer	Displays errors on a specified peer.	-
ipv4-address	Displays errors on a peer with the specified IPv4 address.	It is in dotted decimal notation.
ipv6-address	Displays errors on a peer with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a BGP fault occurs, the **display bgp error discard** command can be run to check the information about discarded error packets. The errors include cluster ID conflicts and the threshold overflow of AS-Path attributes.

By specifying the **peer** parameter, you can check the information about the error packets discarded by a specified BGP peer.

Precautions

The **display bgp error discard** command can be used to check only the error routing. To check the error routing among BGP peers, run the **display bgp error** command.

Example

Display information about discarded BGP error packets.

```
<HUAWEI> display bgp error discard
BGP Discard Info Counts:
Routes received with cluster ID loop           : 0
Routes received with as path count over limit  : 0
Routes advertised with as path count over limit: 0

 No discard record.
```

Table 7-124 Description of the display bgp error discard command output

Item	Description
BGP Discard Info Counts	Number of discarded BGP routes

Item	Description
Routes received with cluster ID loop	Number of discarded BGP routes with a duplicate cluster ID
Routes received with as path count over limit	Number of received BGP routes discarded due to the number of AS-Paths exceeding the upper threshold
Routes advertised with as path count over limit	Number of sent BGP routes discarded due to the number of AS-Paths exceeding the upper threshold
No discard record	No record about packet discarding

7.8.32 display bgp group

Function

The **display bgp group** command displays information about BGP peer groups.

Format

display bgp group [*group-name*]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*]

display bgp vpls group [*group-name*]

display bgp ipv6 group [*group-name*]

display bgp vpnv6 all group [*group-name*]

display bgp vpnv6 vpn-instance *vpn-instance-name* **group** [*group-name*]

display bgp l2vpn-ad group [*group-name*]

display bgp { **mdt** | **mvpn** } **all group** [*group-name*]

NOTE

The **mdt,mvpn** parameter is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpnv4	Displays information about BGP VPNv4 peer groups.	-
all	Displays information about all BGP VPNv4 or VPNv6 peer groups.	-
vpn-instance *vpn-instance-name*	Displays information about BGP peer groups in a specified VPN instance.	The value must be an existing VPN instance name.
vpls	Displays information about BGP peer groups of VPLS.	- **NOTE** The **vpls** parameter is supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H.
ipv6	Displays information about IPv6 peer groups.	-
vpnv6	Displays information about BGP VPNv6 peer groups.	- **NOTE** The **vpnv6** parameter is supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H.
l2vpn-ad	Displays information about BGP peer groups of L2VPN-AD.	- **NOTE** The **l2vpn-ad** parameter is supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Configuring BGP peer groups simplifies BGP network configuration and improves the route advertisement efficiency.

The **display bgp group** command displays information about the peer group, including peers in the peer group and configuration information about the peer group. This command is used in the following scenarios:

- Verify the configuration after running the **group** command to configure the peer group.
- Verify the configuration after running the **peer group** command to add a peer to the peer group.
- Verify the configuration after running the **undo peer group** command to delete a peer from the peer group.
- Verify the configuration after modifying the configuration of the peer group.

Precautions

BGP has multiple address families, each of which is configured independently. Information about peer groups in address families can be displayed by specifying different parameters.

If no parameter is specified, the **display bgp group** command displays default information about peer groups in the IPv4 unicast address family.

Example

Display information about a peer group named **my-peer**.

```
<HUAWEI> display bgp group my-peer

 BGP peer-group: my-peer
 Remote AS: 200
 listen-net: 10.1.1.0 24
 Authentication type configured: None
 Group's BFD has been enabled
 Type : internal
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum route advertisement interval is 15 seconds
 listen-only has been configured
 PeerSession Members:
   10.2.2.2

 Maximum allowed route limit: 8000  Threshold: 75%, Parameter:  always connect-retry(default)
 Status codes: * - Dynamic
 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
  10.1.1.2        4   200        0        0     0 00:00:47      Active       0
```

Table 7-125 Description of the **display bgp group** command output

Item	Description
BGP peer-group	Name of a BGP peer group.
Remote AS	Number of the AS where a peer group resides.
listen-net	Network segment from which BGP listens to BGP connection requests.
Authentication type configured	Configured BGP authentication type. The value can be: ● MD5 ● None: indicates that no BGP authentication is configured.
Group's BFD has been enabled	BFD has been enabled for a peer group.
Type	Type of a peer group: ● internal: indicates that the peer group is an IBGP peer group. ● external: indicates that the peer group is an EBGP peer group.
Configured hold timer value	Value of the Hold timer.
Keepalive timer value	Value of the Keepalive timer.
Minimum route advertisement interval	Minimum interval between route advertisements.
listen-only has been configured	The peer or peer group only detects connection requests, and does not initiate any connection.
PeerSession Members	Peers that set up sessions.
Maximum allowed route limit	Maximum number of allowed BGP routes.
Threshold	Threshold for the quantity of received BGP routes (in percentage) out of the maximum number of routes that can be received.

Item	Description
Parameter	If **peer route-limit** command is configured, this parameter will be displayed: ● always connect-retry(default): By default, BGP always attempts to re-establish a connection after the BGP session is terminated due to the number of routes exceeding the threshold. ● alert-only: When the number of routes reaches the threshold, the switch generates only log information without terminating the BGP session. ● idle-forever: After the BGP session is terminated due to the number of routes exceeding the threshold, BGP does not re-establish a connection if the **reset bgp** command is not executed. ● idle-timeout: After the BGP session is terminated due to the number of routes exceeding the threshold, BGP automatically attempts to re-establish a connection if the timer expires.
Status codes: * - Dynamic	Status code. If the value starts with an asterisk (*), the peer is a dynamic peer. Currently, the value can only be *** - Dynamic**.
Peer Preferred Value	Preferred value of a peer.
Peer Members	Information about peers.
Peer	IP address of a peer.
V	BGP version.
AS	Number of the AS where a member of a peer group resides.
MsgRcvd	Number of received messages.
MsgSent	Number of sent messages.
OutQ	Number of messages to be sent to peers.
Up/Down	Period of time during which a BGP session keeps the current state.

Item	Description
State	BGP state mechanism: - Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. - Idle(Admin): indicates that the peer relationship is shut down initiatively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. - Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. - Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer

Item	Description
	with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for an Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established.

Item	Description
	- Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PrefRcv	Indicates the number of route prefixes received by the local peer from the remote peer.

Display information about all BGP VPNv4 peer groups.

```
<HUAWEI> display bgp vpnv4 all group
Group in VPNV4:

 BGP peer-group: aa
 Remote AS number isn't specified
 Type : external
 PeerSession Members:
   10.3.3.3

 Peer Members:
   10.3.3.3
 **************************

 BGP peer-group: bb
 Remote AS 100
 Type : internal
 PeerSession Members:
  NONE

 Peer Members:
   10.4.4.4

Group in VPN-Instance:

 BGP peer-group: cc
 Remote AS number isn't specified
 VPN-Instance(IPv4-family): vpn1

 Type : external
 PeerSession Members:
   10.2.2.1

 Peer Members:
   10.2.2.1
```

Table 7-126 Description of the **display bgp vpnv4 all group** command output

Item	Description
Group in VPNV4	Information about all BGP peer groups in the VPNv4 address family view.

Item	Description
Remote AS number isn't specified	This item is displayed when the peer group is a mixed EBGP peer group.
Group in VPN-Instance	Information about peer groups in a VPN instance.
VPN-Instance	Name of a VPN instance.

Display information about a BGP VPNv4 peer group named **rr1**.

```
<HUAWEI> display bgp vpnv4 all group rr1
Group in VPNV4:
 No such a peer-group

Group in VPN-Instance:

 BGP peer-group: rr1
 Remote AS number isn't specified
 VPN-Instance: 1

 Type : external
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum route advertisement interval is 30 seconds
 PeerSession Members:
  NONE

 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  No Peer Exists
```

Display information about all BGP IPv6 peer groups.

```
<HUAWEI> display bgp vpnv6 all group
Group in VPNV6:

 BGP peer-group: 123
 Remote AS number isn't specified
 Type : external
 PeerSession Members:
   FC00:0:0:1::1

 Peer Members:
  No Peer Exists
 **********************

 BGP peer-group: 222
 Remote AS 200
 Type : internal
 PeerSession Members:
   FC00:0:0:2::2

 Peer Members:
  No Peer Exists
 **********************

 BGP peer-group: 333
 Remote AS 400
 Type : external
 PeerSession Members:
   FC00:0:0:3::3
```

```
 Peer Members:
  No Peer Exists


Group in VPN-Instance:

 BGP peer-group: 55
 Remote AS number isn't specified
 VPN-Instance(IPv6-family): vpn1

 Type : external
 PeerSession Members:
   FC00:0:0:4::4

 Peer Members:
   FC00:0:0:4::4
```

Table 7-127 Description of the **display bgp vpnv6 all group** command output

Item	Description
Group in VPNV6	Information about all BGP peer groups in a VPNv6 address family.
Group in VPN-Instance	Information about peer groups in an IPv6 VPN instance.
VPN-Instance	Name of an IPv6 VPN instance.

Display information about all BGP IPv6 peer groups.

```
<HUAWEI> display bgp ipv6 group
BGP peer-group is in
 Remote AS 100
 Type : internal
 PeerSession Members:
   FC00:0:0:2::1

 Peer Members:
   FC00:0:0:1::1              FC00:0:0:2::1
 ***********************


 BGP peer-group is ex
 Remote AS number not specified
 Type : external
 PeerSession Members:
   FC00:0:0:20::1
 Peer Members:
   FC00:0:0:10::1              FC00:0:0:20::1
```

Display information about a BGP VPNv6 peer group named **rr1**.

```
<HUAWEI> display bgp vpnv6 all group rr1
Group in VPNV6:
 No such a peer-group

Group in VPN-Instance:
 BGP peer-group: rr1
 Remote AS number isn't specified
 VPN-Instance: 1
 Type : external
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum route advertisement interval is 30 seconds
```

```
PeerSession Members:
  NONE
 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  No Peer Exists
```

Display information about all peer groups in an IPv6 VPN instance named **vpn6** on the local device.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn6 group
BGP peer-group: g1
 Remote AS 65410
 Type : external
 PeerSession Members:
   FC00:0:0:2000::2

 Peer Members:
   FC00:0:0:2000::2
```

Display information about a peer group named **g1** in an IPv6 VPN instance named **vpn6** on the local device.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn6 group g1
BGP peer-group: g1
 Remote AS 65410
 Type : external
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 PeerSession Members:
   FC00:0:0:2000::2

 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  FC00:0:0:2000::2 4 65410      103       90     0 01:20:55 Established       0
```

7.8.33 display bgp ipv6 bfd session

Function

The **display bgp ipv6 bfd session** command displays information about the BFD session set up by BGP.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp ipv6 bfd session { [**vpnv6 vpn-instance** *vpn-instance-name*] **peer** *ipv6-address* | **all** }

Parameters

Parameter	Description	Value
vpnv6	Displays the BFD session of VPNv6.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance.	The value must be an existing VPN instance name.
peer *ipv6-address*	Specifies the IPv6 address of the peer.	-
all	Displays all BFD sessions set up by BGP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The BFD session set up by BGP4+ helps BGP4+ quickly discover faults between BGP4+ peers and inform BGP4+ to recalculate routes for packet forwarding.

Run the **display bgp ipv6 bfd session** command to display information about the BFD session set up by BGP4+ in the following situations:

- Check whether the BFD session is successfully set up or view detailed information about the BFD session that is successfully configured.
- Check whether the BFD session set up by BGP4+ is successfully deleted after running the **undo peer bfd enable** command.
- Verify the configuration after running the **undo peer bfd block** command to restore a peer inheriting the BFD function of the peer group.
- Verify the configuration after running the **peer bfd** command to set BFD parameters.

The information about the BFD session of a specified peer can be displayed by specifying different parameters.

- Run the **display bgp ipv6 bfd session vpnv6 vpn-instance** *vpn-instance-name* **peer** *ipv6-address* command to display information about the BFD session of a specified peer in a VPN instance.
- Run the **display bgp ipv6 bfd session peer** *ipv6-address* command to display information about the BFD session of a specified peer on the public network.

- Run the **display bgp ipv6 bfd session all** command to display information about the BFD sessions of all BGP4+ peers.

Prerequisites

The BFD session has been set up using the **peer bfd enable** command. If the BFD session has not been set up by BGP4+, no information is displayed after running the **display bgp ipv6 bfd session** command.

Example

Display all BFD sessions set up by BGP.

```
<HUAWEI> display bgp ipv6 bfd session all
  Local_Address  : FC00:3::1
  Peer_Address   : FC00:3::2
  Tx-interval(ms): 100         Rx-interval(ms): 100
  Multiplier     : 4           Interface      : GigabitEthernet0/0/1
  LD/RD          : 8193/8207   Session-State  : Up
  Wtr-interval(m): 0
```

Table 7-128 Description of the **display bgp ipv6 bfd session** command output

Item	Description
Local_Address	Local address
Peer_Address	Peer address
Tx-interval (ms)	Interval for sending BFD packets, in milliseconds
Rx-interval (ms)	Interval for receiving BFD packets, in milliseconds
Multiplier	Local detection multiple
Interface	Interface on which the BFD session is set up **NOTE** Information about the interface on which the BFD session is set up only when the directly connected interface is used to set up the EBGP neighbor relationship. In other cases, information about the interface is displayed as Unknown.
LD/RD	Local/remote discriminator

Item	Description
Session-State	BFD status ● Admin down: The BFD session is closed on the local end. ● BFD global disable: BFD is disabled globally. ● BFD session number exceed: The number of BFD sessions exceeds the maximum limit. ● Detect down: BFD detects a link status fault and interrupts the connection. ● Init: The BFD session is in the initialized state. ● Neighbor down: The peer end detects that the BFD session goes Down and informs the local end of the change, and the local end then sets the neighbor status to Down. ● Receive admin down: The BFD session is closed on the peer end (for example, the BFD session is disabled on the peer end). ● Up: The BFD session is set up.
Wtr-interval(m)	Interval for flap dampening, in minutes

7.8.34 display bgp ipv6 routing-table

Function

The **display bgp ipv6 routing-table** command displays BGP IPv6 routes.

Format

display bgp ipv6 routing-table [**verbose**]

display bgp ipv6 routing-table *ipv6-address* [*prefix-length*]

display bgp ipv6 routing-table as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

display bgp ipv6 routing-table community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp ipv6 routing-table community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp ipv6 routing-table different-origin-as

display bgp ipv6 routing-table regular-expression *as-regular-expression*

display bgp ipv6 routing-table peer *ipv6-address* { **accepted-routes** | **advertised-routes** [*dest-ipv6-address* [*prefix-length*]] | **received-routes** [**active**] }

display bgp ipv6 routing-table peer *ipv6-address* **received-routes** *dest-ipv6-address* [*prefix-length* [**original-attributes**]]

display bgp ipv6 routing-table peer *ipv4-address* **received-routes** *dest-ipv6-address* [*prefix-length* [**original-attributes**]]

display bgp ipv6 routing-table time-range *start-time end-time*

Parameters

Parameter	Description	Value
verbose	Displays detailed information about BGP4+ public network routes.	-
ipv6-address	Specifies the IPv6 address of the peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of the prefix.	The value is an integer that ranges from 0 to 128.
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
community	Displays the routing information of the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.

Parameter	Description	Value
aa:nn	Specifies the community attribute number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
whole-match	Indicates the exact matching.	-
community-filter	Displays the routes that match the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
different-origin-as	Displays routes that have the same destination address but different source ASs.	-

Parameter	Description	Value
peer	Displays the routing information for the specified BGP peer.	-
ipv4-address	Specifies the IPv4 address of the peer. **NOTE** The parameter is not supported on S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S.	The value is in dotted decimal notation.
advertised-routes	Displays the routes advertised to the specified peer.	-
dest-ipv6-address	Specifies the destination IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
received-routes	Displays the routes received from the specified peer.	-
active	Displays the active routes received from the specified peer.	-
original-attributes	Displays the original attributes of a public route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.

Parameter	Description	Value
accepted-routes	Displays the routes that are received from the peer and filtered through a routing policy.	-
time-range *start-time end-time*	Displays IPv6 BGP routes that flap within the specified time period. For example, the value 0d0h5m0s of *start-time* indicates 5 minutes before the current time. The value 0d0h10m0s of *end-time* indicates 10 minutes before the current time. All IPv6 BGP routes with the Keepalive time in the range of 5 to 10 minutes are displayed.	The value ranges of *start-time* and *end-time* both are 0d0h0m0s-10000d23h59m59s.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

You can run the **display bgp ipv6 routing-table time-range** *start-time end-time* command to view BGP4+ routes that flap within the specified time period. For example, if service traffic is abnormal or CPU usage of the device remains high within a certain time period, you can run this command to check whether route flapping occurs within the specified time period. The faulty route can be viewed in the command output, facilitating fault location.

Example

Display BGP IPv6 routes.

```
<HUAWEI> display bgp ipv6 routing-table

 BGP Local router ID is 10.1.1.1
 Status codes: * - valid, > - best, d - damped, x - best external,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
 Total Number of Routes: 1
 *>  Network  : FC00:0:0:2000::                      PrefixLen : 64
     NextHop  : FC00:0:0:2000::1                     LocPrf    :
     MED      : 0                            PrefVal   : 0
     Label    :
     Path/Ogn : i
```

Displays BGP IPv6 routes that flap within the specified time period.

```
<HUAWEI> display bgp ipv6 routing-table time-range 0d5h0m0s 1d5h0m0s
BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>i Network  : FC00:0:0:100::100                     PrefixLen : 128
     NextHop  : FC00:0:0:12::1                       Duration  : 05h46m16s
     Peer     : FC00:0:0:12::1
     Path/Ogn : ?
 * i
     NextHop  : FC00:0:0:112::1                       Duration  : 05h46m16s
     Peer     : FC00:0:0:112::1
     Path/Ogn : ?
 *>i Network  : FC00:0:0:111::111                     PrefixLen : 128
     NextHop  : FC00:0:0:12::1                       Duration  : 05h46m16s
     Peer     : FC00:0:0:12::1
     Path/Ogn : ?
 * i
     NextHop  : FC00:0:0:112::1                       Duration  : 05h46m16s
     Peer     : FC00:0:0:112::1
     Path/Ogn : ?
```

Table 7-129 Description of the display bgp ipv6 routing-table command output

Item	Description
BGP Local router ID	Indicates the router ID of the local BGP device.
Network	Indicates the network address in the BGP routing table.
PrefixLen	Indicates the prefix length.
NextHop	Indicates the next-hop address of the packet.
LocPrf	Indicates the local preference.
MED	Indicates the MED of the route.
PrefVal	Indicates the preferred value.
Label	Indicates the label value.
Duration	Route duration
Peer	Peer IP address
Path/Ogn	Indicates the AS_Path number and the Origin attribute.

Display detailed information about the specified invalid BGP4+ routes.

```
<HUAWEI> display bgp ipv6 routing-table FC00::1
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   1 available, 0 best, 0 select
 BGP routing table entry information of FC00::1/128
 From: 10::2 (10.1.1.2)
 Route Duration: 00h17m46s
 Relay IP Nexthop: ::
 Relay IP Out-Interface:
 Original nexthop: FC00::2
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet
```

Table 7-130 Description of the display bgp ipv6 routing-table command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Paths	Information about paths of BGP routes
BGP routing table entry information of FC00::1/128	The following information is about FC00::1/128 routing entries.
From	IP address of the router that sends the route. 10.1.1.2 is the source interface IP address of the peer with which the BGP connection is established, and 10::2 is the router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.
AS-path 200	AS_Path attribute.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
pre 255	The priority of the BGP route is 255.
invalid for IP unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to recurse to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to recurse to a tunnel.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

7.8.35 display bgp ipv6 routing-table statistics

Function

The **display bgp ipv6 routing-table statistics** command displays statistics about BGP IPv6 routes.

Format

display bgp ipv6 routing-table statistics

display bgp ipv6 routing-table statistics as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

display bgp ipv6 routing-table statistics community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp ipv6 routing-table statistics community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp ipv6 routing-table peer *ipv6-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

display bgp ipv6 routing-table statistics regular-expression *as-regular-expression*

display bgp ipv6 routing-table statistics different-origin-as

Parameters

Parameter	Description	Value
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
community	Displays the routing information of the specified BGP community attribute in the routing table.	-

Parameter	Description	Value
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
aa:nn	Specifies the community attribute number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with the No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays the routing information that matches the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
peer	Displays the routing information for the specified BGP peer.	-
ipv6-address	Specifies the IPv6 address of the peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
advertised-routes	Displays the routes advertised to the specified peer.	-
received-routes	Displays the routes received from the specified peer.	-
active	Displays the active routes received from the specified peer.	-

Parameter	Description	Value
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.
different-origin-as	Displays routes that have the same destination address but different source ASs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp ipv6 routing-table statistics** command to check statistics about BGP IPv6 routes.

Example

Display statistics of BGP IPv6 routes.

```
<HUAWEI> display bgp ipv6 routing-table statistics

 Total Number of Routes: 4
```

Table 7-131 Description of the **display bgp ipv6 routing-table statistics** command output

Item	Description
Total Number of Routes	Total number of routes in the routing table.

7.8.36 display bgp mdt brief

Function

The **display bgp mdt brief** command displays brief information about VPN instances in BGP MDT address family.

Format

display bgp mdt { **all** | **vpn-instance** *vpn-instance-name* } **brief**

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Displays information about MDT and all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bgp mdt brief** command is used to display brief information about VPN instances in BGP MDT address family.

Example

Display brief information about MDT and all VPN instances.

```
<HUAWEI> display bgp mdt all brief

MDT:
  Rd Num              Peer Num           Route Num
  0                 1                  0

VPN-Instance(IPv4-MDT-family):
  VPN-Instance Name   Peer Num            Route Num
  vrf0                  0                 0
  vrf1                  0                 0
  vrf11                 0                 0
  vrf12                 0                 0
  vrf13                 0                 0
  vrf14                 0                 0
  vrf2                  0                 20
  vrf3                  0                 20
  vrf4                  0                 24
  vrf5                  0                 24
  vrf6                  0                 0
  vrf7                  0                 0
  vrf8                  0                 20
```

Table 7-132 Description of the **display bgp mdt all brief** command output

Item	Description
Rd Num	Number of Route Distinguishers (RDs).
Peer Num	Number of peers.
Route Num	Number of routes.
VPN-Instance Name	Name of a VPN instance.

7.8.37 display bgp mdt routing-table

Function

The **display bgp mdt routing-table** command displays the information of BGP MDT routes.

Format

display bgp mdt { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

display bgp mdt route-distinguisher *route-distinguisher* **routing-table** [*network* [*mask* | *mask-length*]]

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table regular-expression** *as-regular-expression*

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community** [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp mdt all routing-table peer *ipv4-address* [**advertised-routes** [**statistics** | *ipv4-address*] | **received-routes** [**active**] [**statistics**]]

display bgp mdt all routing-table peer *ipv4-address* **received-routes** *network*

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Display all the BGP MDT routing information.	-
route-distinguisher *route-distinguisher*	Displays the BGP MDT routing information of the specified Route Distinguisher (RD).	-
vpn-instance *vpn-instance-name*	Displays the BGP MDT routing information of the specified VPN instance.	The value must be an existing VPN instance name.
network	Specifies the IPv4 network address.	It is in dotted decimal notation.
mask | *mask-length*	Specifies mask in dotted decimal notation or mask-length.	The value of mask-length is an integer that ranges from 0 to 32.
longer-prefixes	Matches according to the mask longer than the specified length.	-
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals.
cidr	Displays the BGP MDT routing information about the Classless Inter-Domain Routing (CIDR).	-
different-origin-as	Displays routes that have the same destination address but different source ASs.	-

Parameter	Description	Value
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.
community-filter	Displays the BGP MDT routing information that matches the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community	Displays the BGP MDT routing information of the specified BGP community attribute in the routing table.	-
aa:nn	Specifies the community attribute number.	Both aa and nn are integers ranging from 0 to 65535. You can set a maximum of 29 community numbers.
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-

Parameter	Description	Value
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
whole-match	Indicates the exact matching.	-
peer *ipv4-address*	Displays the BGP MDT routing information for the specified BGP peer.	-
advertised-routes	Displays the BGP MDT routing information advertised to the specified peer.	-
statistics	Display the statistics of the BGP MDT routes.	-
ipv4-address	Specifies the IPv4 network address.	It is in dotted decimal notation.
received-routes	Displays the BGP MDT routing information received from the specified peer.	-
active	Displays the BGP MDT routing information received from the specified peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information of BGP MDT routes. If the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed.

Example

Display all the BGP MDT routing information.

```
<HUAWEI> display bgp mdt all routing-table
```

```
 BGP Local router ID is 192.168.7.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 3
 Route Distinguisher: 100:1

      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                     0      ?

 Route Distinguisher: 200:1

      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  1.1.1.1/32         192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?

 Total number of routes of IPv4-MDT-family for vpn-instance vrf1: 3
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                     0      ?
 * i                    192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?
```

Display all the BGP MDT routing information of the VPN instance named vpna.

```
<HUAWEI> display bgp mdt vpn-instance vpna routing-table

Total Number of Routes: 2

 BGP Local router ID is 2.2.2.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network          NextHop        MED       LocPrf    PrefVal Path/Ogn

 *>i  10.1.1.0/24      1.1.1.9         0         100        0      ?
 *>i  10.2.1.0/24      3.3.3.9         0         100        0      ?
```

Display the BGP MDT routing information of the specified RD.

```
<HUAWEI> display bgp mdt route-distinguisher 100:1 routing-table

 BGP Local router ID is 192.168.7.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1

 Total Number of Routes: 1

      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                     0      ?

 Total number of routes of IPv4-MDT-family for vpn-instance vrf1: 3
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                     0      ?
 * i                    192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?
```

Display all BGP MDT routes of community 1000:100.

```
<HUAWEI> display bgp mdt all routing-table community 1000:100

 BGP Local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 1

 Route Distinguisher: 100:1

      Network            NextHop        MED        LocPrf    PrefVal Community

 *>i  10.1.1.0/24        1.1.1.1        0          100        0      <1000:100>

 Total number of routes of IPv4-MDT-family for vpn-instance vpna: 1
      Network            NextHop        MED        LocPrf    PrefVal Community

 *>i  10.1.1.0/24        1.1.1.1        0          100        0      <1000:100>
```

Table 7-133 Description of the **display bgp mdt routing-table** command output

Item	Description
Network	Network address in the BGP routing table.
Next Hop	Next Hop address through which the packet has to be sent.
MED	Multi-Exit discriminator.
LocPrf	Local priority.
PrefVal	Value preferred by the protocol.
Path/Ogn	AS_Path number and the attributes of Origin.
Community	Community attributes.

Display all BGP MDT routes of community 1000:100 with the Internet community attribute.

```
<HUAWEI> display bgp mdt all routing-table community 1000:100 internet

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 1

 Route Distinguisher: 100:1


      Network            NextHop        MED        LocPrf    PrefVal Community

 *>i  10.1.1.0/24        1.1.1.1        0          100        0      <1000:100>

 Total number of routes of IPv4-MDT-family for vpn-instance vpna: 4
      Network            NextHop        MED        LocPrf    PrefVal Community

 *>i  10.1.1.0/24        1.1.1.1        0          100        0      <1000:100>
 *>   10.2.1.0/24        0.0.0.0        0                     0
 *                    10.2.1.1        0                     0
 *>   10.2.1.2/32        0.0.0.0
```

Display routes sent by 2.2.2.2.

```
<HUAWEI> display bgp mdt all routing-table peer 2.2.2.2 received-routes

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1

 Route Distinguisher: 2:2


      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  2.2.2.2/32         2.2.2.2         0          100        0      ?
```

Display detailed information about the route with prefix 2.2.2.2 sent by 2.2.2.2.

```
<HUAWEI> display bgp mdt all routing-table peer 2.2.2.2 received-routes 2.2.2.2

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Route Distinguisher: 2:2

 BGP routing table entry information of 2.2.2.2/32:
 From: 2.2.2.2 (2.2.2.9)
 Route Duration: 00h03m42s
 Relay IP Nexthop: 10.1.1.2
 Relay IP Out-Interface: Ethernet0/0/1
 Original nexthop: 2.2.2.2
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, pre 255, IGP
cost 1
 MDT group address: 232.1.1.1
 Not advertised to any peer yet
```

Table 7-134 Description of the **display bgp mdt all routing-table peer received-routes** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Route Distinguisher	Route distinguisher.
BGP routing table entry information of 2.2.2.2/32	The following information is about 2.2.2.2/32 routing entries.
From	IP address of the router that sends the route. 2.2.2.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 2.2.2.9 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.

Item	Description
Original nexthop	Original next hop.
Qos information	QoS information.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
localpref	Local priority.
pref-val	Value preferred by the protocol.
valid	The BGP route is a valid route.
internal	The BGP route is an internal route.
best	The BGP route is an optimal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.
IGP cost	Cost of the relied next hop route of BGP route.
MDT group address	Group address of MDT.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

7.8.38 display bgp mdt routing-table statistics

Function

The **display bgp mdt routing-table statistics** command displays the statistics of the BGP MDT routes.

Format

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics**

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics regular-expression** *as-regular-expression*

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community** [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Displays all the statistics of the BGP MDT routes.	-
route-distinguisher *route-distinguisher*	Displays the BGP MDT routing statistics of the specified Route Distinguisher (RD).	-
vpn-instance *vpn-instance-name*	Displays the BGP MDT routing statistics of the specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matched AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals.
cidr	Displays the BGP MDT routing statistics about the Classless Inter-Domain Routing (CIDR).	-
different-origin-as	Displays the routes that have the same destination address but different source AS number.	-
regular-expression *as-regular-expression*	Indicates the matched AS regular expression.	The value is a string of 1 to 80 characters.
community-filter	Displays the BGP MDT routing statistics that matches the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
whole-match	Indicates exact matching.	-
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.

Parameter	Description	Value
community	Displays the BGP MDT routing statistics of the specified BGP community attribute in the routing table.	-
aa:nn	Specifies the community number.	Both aa and nn are integers ranging from 0 to 65535. You can set a maximum of 29 community numbers.
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with the No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Displays all the statistics of the BGP MDT routes.

```
<HUAWEI> display bgp mdt all routing-table statistics

 Total number of routes from all PE: 20
```

```
Total number of routes of IPv4-MDT-family for vpn-instance vpn1: 12
```

Table 7-135 Description of the **display bgp mdt routing-table statistics** command output

Item	Description
Total number of routes from all PE	The number of the routes received from PEs in the BGP MDT routing table.
Total number of routes of IPv4-MDT-family for vpn-instance	The number of the routes of the specified VPN instance in the BGP MDT routing table.

7.8.39 display bgp multicast group

Function

The **display bgp multicast group** command displays the information about an MBGP peer group.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the peer group is specified, the detailed information on the specified peer group is displayed.

If the peer group is not specified, the information on all MBGP peer groups is displayed.

Example

Display the information about peer group **my-peer**.

```
<HUAWEI> display bgp multicast group my-peer
BGP peer-group: my-peer
 Remote AS: 1
 Authentication type configured: None
 Type : external
 Configured hold timer value: 180
 Keepalive timer value: 60
 Connect-retry timer value: 32
 Minimum route advertisement interval is 30 seconds
 PeerSession Members:
   172.16.14.1
 It's route-reflector-client
 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  Peer         V  AS  MsgRcvd  MsgSent  OutQ   Up/Down    State   PrefRcv
  172.16.14.1  4   1      43       29      0    00:03:03   Established   21
```

Table 7-136 Description of the display bgp multicast group command output

Item	Description
BGP peer-group: my-peer	Peer group: name of the group
Remote AS	The number of the AS where the peer resides
Authentication type configured	Indicates the configured BGP authentication type: ● MD5 ● Keychain (kk), in which kk indicates the name of the configured keychain authentication ● None, which indicates no BGP authentication is configured
Type	Indicates the types of peers: ● internal: The type of the peer group is IBGP ● external: The type of the peer group is EBGP
Configured hold timer value	Value of the holdtime timer
Keepalive timer value	Value of the Keepalive timer

Item	Description
Connect-retry timer value	Value of the Connect-retry timer
Minimum route advertisement interval	Shortest interval for advertising routes
PeerSession Members	Indicates peers that set up session connections
It's route-reflector-client	The local device is a route reflector client
Peer Preferred Value	Preferred value of peers
Peer	IP address of the peer
V	MBGP version
AS	The number of the AS where the peer resides
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent to the peer
Up/Down	Time during which the MBGP session is in the current state
State	Indicates the MBGP state mechanism: ● Idle: indicates that MBGP denies the connection request. This is the initiate status of MBGP. ● Active: indicates that MBGP tries to set up TCP connection. This is the intermediate status of MBGP. ● Established: In the status, MBGP peers can exchange Update, Notification and Keepalive packets. ● Connect: indicates that MBGP performs other actions after the TCP connection is set up. ● OpenSent: indicates that MBGP waits for an Open message from the peer. ● OpenConfirm: indicates that MBGP waits for a Notification message or a Keepalive message.
PrefRcv	The number of prefixes received by the local peer from the remote peer

7.8.40 display bgp multicast network

Function

The **display bgp multicast network** command displays the routes to be advertised by MBGP through the **network** command.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast network

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to display all the configurations of the **network (BGP)** command in the IPv4 multicast address family view. Routes can be imported and then advertised by MBGP only when the route prefix satisfies the following conditions:

- It is specified in the **network** command.
- It already exists in the IP routing table.
- It is active.

Example

Display the routing information of a network segment advertised by MBGP.

```
<HUAWEI> display bgp multicast network
 BGP Local Router ID is 10.2.2.9
 Local AS Number is 100(Multicast)
 Network         Mask           Route-policy

 10.1.1.1       255.255.255.0
 10.2.2.2       255.255.255.0
```

Table 7-137 Description of the display bgp multicast network command output

Item	Description
BGP Local Router ID	ID of the local MBGP router
Local AS Number	Number of the local AS
Network	Network address locally advertised
Mask	Mask of the network address
Route-policy	Used routing policy

7.8.41 display bgp multicast paths

Function

The **display bgp multicast paths** command displays AS_Path information of MBGP.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast paths [*as-regular-expression*]

Parameters

Parameter	Description	Value
as-regular-expression	Displays the AS_Path regular expression.	The value is a string of 1 to 80 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast paths** command to check AS_Path information of MBGP.

Example

Display information about MBGP paths.

```
<HUAWEI> display bgp multicast paths 1

Total Number of Routes: 17
Total Number of Paths: 1


   Address         Refcount   MED        Path/Origin
   0x54169A4        17         0          1?
```

Table 7-138 Description of the display bgp multicast paths command output

Item	Description
Total Number of Routes	Total number of routes
Total Number of Paths	Total number of AS paths
Address	Address of the path attribute node in the local database in the hexadecimal format
Refcount	Number of times that the route is referenced
MED	Multi-Exit discriminator
Path	AS_Path list of the route
Origin	Origin of the route

7.8.42 display bgp multicast peer

Function

The **display bgp multicast peer** command displays information about a specified MBGP peer. If *peer-address* is not specified, information about all MBGP peers is displayed.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast peer [[*peer-address*] **verbose**]

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MBGP peer.	The value is in dotted decimal notation.
verbose	Specifies detailed information about an MBGP peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast peer** command to check information about a specified MBGP peer. If *peer-address* is not specified, information about all MBGP peers is displayed.

Example

Display information about all MBGP peers.

```
<HUAWEI> display bgp multicast peer

 BGP local router ID : 10.13.13.9
 Local AS number : 1
 Total number of peers : 1                Peers in established state : 1

  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  10.2.1.2        4     2       36       37     0 00:15:35 Established      24
```

Table 7-139 Description of the display bgp multicast peer command output

Item	Description
BGP local router ID	ID of the local MBGP router
Local AS number	Local AS number
Total number of peers	Total number of peers
Peers in established state	Number of peers in established state
Peer	IP address of peers
V	MBGP version of peers
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Messages to be sent to the specified peers
Up/Down	Period during which the MBGP session is in the current state
State	Status of the peers
PrefRcv	Number of prefixes received by the local peer from the remote peer

7.8.43 display bgp multicast routing-table

Function

The **display bgp multicast routing-table** command displays the MBGP routing information of a specified network in the MBGP routing table.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table [*ip-address* [*mask-length* [**longer-prefixes**] | *mask* [**longer-prefixes**]]]

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address.	The address is in dotted decimal notation.
mask-length	Specifies the mask length of the IPv4 address.	The value is an integer that ranges from 0 to 32.
mask	Specifies the mask of the IPv4 address.	The value is in dotted decimal notation.
longer-prefixes	Matches routes whose masks are shorter than the specified mask length.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *ip-address* is not specified, this command will display all the information in the MBGP routing table.

Example

Display MBGP routing information.

```
<HUAWEI> display bgp multicast routing-table

 BGP local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 14
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   10.1.2.0/24        10.2.1.2                             0      2?
 *>   10.1.13.0/24        0.0.0.0         0                    0      ?
 *>   10.1.13.2/32        0.0.0.0         0                    0      ?
 *>   10.2.1.0/24        0.0.0.0         0                    0      ?
 *>   10.2.1.0/24        10.2.1.2         0                    0      2?
 *>   10.2.1.1/32        0.0.0.0         0                    0      ?
 *>   10.2.13.0/24        0.0.0.0         0                    0      ?
 *>   10.2.13.1/32        0.0.0.0         0                    0      ?
 *>   10.2.13.2/32        0.0.0.0         0                    0      ?
```

Table 7-140 Description of the display bgp multicast routing-table command output

Item	Description
BGP local router ID	BGP local router ID.
Status codes	Status of a routing entry.
Total Number of Routes	Total number of routes in the routing table.
Network	Indicates the network address in the MBGP routing table.
NextHop	Indicates the next-hop address for the packet.
MED	Indicates the MED of the route.
LocPrf	Indicates the local preference.
PrefVal	Indicates the preferred value.
Path/Ogn	Indicates the AS_Path number and the Origin attribute.

Display detailed information about the specified invalid MBGP routes.

```
<HUAWEI> display bgp multicast routing-table 192.168.1.1
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   2 available, 0 best, 0 select
 BGP routing table entry information of 192.168.1.1/32:
 From: 10.2.2.2 (10.1.1.2)
 Route Duration: 00h01m15s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 172.16.1.2
```

```
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP 
unreachable
 Not advertised to any peer yet

 BGP routing table entry information of 192.168.1.1/32:
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h01m15s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 172.16.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP 
unreachable
 Not advertised to any peer yet
Not advertised to any peers yet
```

Table 7-141 Description of the display bgp multicast routing-table command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Paths	Information about paths of BGP routes
BGP routing table entry information of 192.168.1.1/32	The following information is about 192.168.1.1/32 routing entries.
From	IP address of the router that sends the route. 10.1.1.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 10.2.2.2 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.

Item	Description
Qos information	QoS information. - 0x20000000: indicates that the **apply behavior** command has been run. - 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. - 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. - 0x0: indicates that the preceding QoS configurations are not performed.
AS-path 200	AS_Path attribute.
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: - IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. - EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. - Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
pre 255	The BGP route preference is 255.

Item	Description
invalid for IP unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to recurse to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to recurse to a tunnel.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

7.8.44 display bgp multicast routing-table as-path-filter

Function

The **display bgp multicast routing-table as-path-filter** command displays information about the routes that match the AS_Path filter.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

Parameters

Parameter	Description	Value
as-path-filter-number	Specifies the number of the matching AS_Path filter.	The value is an integer that ranges from 1 to 256.

Parameter	Description	Value
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The value is a string of 1 to 51 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table as-path-filter** command to check information about the routes that match the AS_Path filter.

Example

Display information about the routes that match the AS_Path filter 1.

```
<HUAWEI> display bgp multicast routing-table as-path-filter 1
BGP local router ID is 10.14.14.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 15
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>i  10.1.13.0/24       10.2.1.1        0          100        0      1?
 *>i  10.2.1.0/24        10.2.1.1        0          100        0      1?
 *>i  10.2.13.0/24       10.2.1.1        0          100        0      1?
 *>i  10.2.13.1/32       10.2.1.1        0          100        0      1?
```

Table 7-142 Description of the display bgp multicast routing-table as-path-filter command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packets
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	AS path and Origin attribute

7.8.45 display bgp multicast routing-table cidr

Function

The **display bgp multicast routing-table cidr** command displays routing information of classless inter-domain routing (CIDR).

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table cidr

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table cidr** command to check routing information of CIDR.

Example

Display routing information about CIDR.

```
<HUAWEI> display bgp multicast routing-table cidr
 BGP Local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 9
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>   10.1.2.0/24        10.2.1.2                             0      2?
 *>   10.2.1.0/24        10.2.1.2       0                      0      2?
 *>   10.7.1.0/24        10.2.1.2                             0      2?
 *>   10.7.1.1/32        10.2.1.2                             0      2?
 *>   10.7.1.2/32        10.2.1.2       0                      0      2?
 *>   10.11.12.0/24       10.2.1.2       0                      0      2?
 *>   10.11.12.1/32       10.2.1.2       0                      0      2?
```

Table 7-143 Description of the display bgp multicast routing-table cidr command output

Item	Description
BGP local router ID	BGP local router ID
Status codes	Status of a routing entry
Total Number of Routes	Total number of routes in the routing table
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packets
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	AS path and Origin attribute

7.8.46 display bgp multicast routing-table community

Function

The **display bgp multicast routing-table community** command displays routing information of a specified MBGP community.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table community [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

Parameters

Parameter	Description	Value
aa:nn	Specifies the MBGP community number. You can specify a maximum of 29 MBGP communities.	Both aa and nn are integers ranging from 0 to 65535.
community-number	Specifies the MBGP community number. You can specify a maximum of 29 community numbers.	The value is an integer that ranges from 0 to 4294967295.

Parameter	Description	Value
internet	Displays the MBGP routes with the Internet community attribute. The Internet community attribute indicates the matching routes sent to all remote peers.	-
no-advertise	Displays MBGP routes with the no-advertise community attribute. The no-advertise community attribute indicates that the matching routes are not sent to any peer.	-
no-export	Indicates MBGP routes with the no-export community attribute. The no-expert community attribute indicates that the matching routes are not advertised to other ASs but to other sub-ASs in the confederation.	-
no-export-subconfed	Displays MBGP routes with the no-export-subconfed community attribute. The no-export-subconfed community attribute indicates that the matching routes are not advertised outside the local AS.	-
whole-match	Indicates precise matching.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table community** command to check routing information of a specified MBGP community.

Example

Display MBGP routing information of Community 100:100.

```
<HUAWEI> display bgp multicast routing-table community 100:100
 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 1
      Network          NextHop      MED    LocPrf    PrefVal    Community
 *>   10.1.1.0/24     10.2.1.1      0                 0         <100:100>
```

Display MBGP routing information with the internet community attribute or that of Community 100:100.

```
<HUAWEI> display bgp multicast routing-table community 100:100 internet
```

```
BGP local router ID is 10.12.12.9
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 5
     Network          NextHop       MED       LocPrf     PrefVal   Community

*>   10.1.1.1/32      10.1.1.2      0                    0         <100:100>,internet
*>   10.3.3.3/32      10.2.1.1      0                    0         <100:100>,internet
*>   10.1.1.0/24      10.2.1.1      0                    0         <100:100>,internet
*>   10.2.13.0/24     10.2.1.1      0                    0         <100:100>,internet
```

Table 7-144 Description of the display bgp multicast routing-table community command output

Item	Description
BGP local router ID	BGP local router ID
Status codes	Status of a routing entry.
Total Number of Routes	Total number of routes in the routing table.
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packets
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Community	Community attribute

7.8.47 display bgp multicast routing-table community-filter

Function

The **display bgp multicast routing-table community-filter** command displays the multicast routing information that matches a specified MBGP community list.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

Parameters

Parameter	Description	Value
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community-filter-name	Specifies the name of the community filter.	The value is a string of 1 to 51 case-sensitive characters without spaces.
whole-match	Indicates exact matching.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table community-filter** command to check the multicast routing information that matches a specified MBGP community list.

Example

Display the multicast routing information that matches a specified MBGP community list.

```
<HUAWEI> display bgp multicast routing-table community-filter 1
BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal    Community
 *>   10.10.10.0/24      10.2.1.1       0                    0          <100:100>
```

Table 7-145 Description of the display bgp multicast routing-table community-filter command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
NextHop	Next hop address of packets

Item	Description
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value
Community	Community attribute

7.8.48 display bgp multicast routing-table dampened

Function

The **display bgp multicast routing-table dampened** command displays dampened MBGP routes.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table [**statistics**] **dampened**

Parameters

Parameter	Description	Value
statistics	Displays statistics of dampened routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table dampened** command to check dampened MBGP routes.

Example

Display dampened MBGP routes.

```
<HUAWEI> display bgp multicast routing-table dampened
 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
```

```
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 1
    Network            From             Reuse     Path/Ogn
d   10.1.0.0/16        10.2.1.1          00:45:05  1?
```

Table 7-146 Description of the display bgp multicast routing-table dampened command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
From	IP address of MBGP peer from which the route is received
Reuse	Reuse value
Path/Ogn	AS_Path number and Origin attribute

7.8.49 display bgp multicast routing-table dampening parameter

Function

The **display bgp multicast routing-table dampening parameter** command displays information about MBGP dampening parameters.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table dampening parameter

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table dampening parameter** command to check information about MBGP dampening parameters.

Example

Display MBGP dampening parameters.

```
<HUAWEI> display bgp multicast routing-table dampening parameter
 Maximum Suppress Time(in second) : 3973
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in second)         : 900
 Suppress-Limit                   : 2000
```

Table 7-147 Description of the display bgp multicast routing-table dampening parameter command output

Item	Description
Maximum Suppress Time (in second)	Maximum suppression time (in seconds)
Ceiling Value	Ceiling value of the penalty
Reuse Value	Threshold for routes leaving the suppression state
HalfLife Time (in second)	Half life time of the reachable route
Suppress-Limit	Threshold for routes entering the suppression state

7.8.50 display bgp multicast routing-table different-origin-as

Function

The **display bgp multicast routing-table different-origin-as** command displays the routes with the same destination but different source AS numbers.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table different-origin-as

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table different-origin-as** command to check the routes with the same destination but different source AS numbers.

Example

Display the routes with the same destination but different source AS numbers.

```
<HUAWEI> display bgp multicast routing-table different-origin-as
BGP local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 8
      Network            NextHop        MED      LocPrf    PrefVal Path/Ogn
 *>   10.2.1.0/24        10.2.1.2        0                  0        2?
 *>                      0.0.0.0         0                  0        ?
 *>   10.2.0.0/16        10.2.1.2                           0        2?
 *>                      0.0.0.0         0                  0        ?
 *>   192.168.14.0       10.2.1.2                           0        2?
 *>                      0.0.0.0         0                  0        ?
 *>   192.168.14.1/32    10.2.1.2                           0        2?
 *>                      0.0.0.0         0                  0        ?
```

Table 7-148 Description of the display bgp multicast routing-table different-origin-as command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packets
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	AS path and Origin attribute

7.8.51 display bgp multicast routing-table flap-info

Function

The **display bgp multicast routing-table flap-info** command displays information about MBGP route flapping.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table flap-info [*ip-address* [*mask* [**longer-match**] | *mask-length* [**longer-match**]] | **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }]

display bgp multicast routing-table flap-info regular-expression *as-regular-expression*

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 network address.	The address is in dotted decimal notation.
mask	Specifies the mask of an IPv4 network address.	The address is in dotted decimal notation.
mask-length	Specifies the mask length of the IPv4 network address.	The value is an integer that ranges from 0 to 32.
longer-match	Indicates the longest prefix matching rules.	-
regular-expression *as-regular-expression*	Displays the statistics of route flapping that matches the AS_Path regular expression. *as-regular-expression* specifies the AS path regular expression.	The value is a string of 1 to 80 characters.
as-path-filter *as-path-filter-number*	Displays the statistics of the route flapping for the specified AS path list. *as-path-filter-number* indicates the matched AS path list number.	The value is an integer that ranges from 1 to 256.

Parameter	Description	Value
as-path-filter *as-path-filter-name*	Displays the statistics of the route flapping for the specified AS path list. *as-path-filter-name* indicates the matched AS path list name.	The value is a string of 1 to 51 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table flap-info** command to check information about MBGP route flapping.

Example

Display information about MBGP route flapping.

```
<HUAWEI> display bgp multicast routing-table flap-info
BGP Local router ID is 10.12.12.9
 Status codes: * - valid, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network            From            Flaps  Duration     Reuse  Path/Ogn
 *>   10.1.1.0/24         10.2.1.1        1      00:00:29           1?
```

Table 7-149 Description of the display bgp multicast routing-table flap-info command output

Item	Description
BGP Local router ID	BGP local router ID
Network	Network address in the MBGP routing table
From	IP address of MBGP peer from which the route is received
Flaps	Count of route flapping
Duration	Duration of route flapping
Reuse	Reuse value
Path/Ogn	AS_Path number and Origin attribute

7.8.52 display bgp multicast routing-table peer

Function

The **display bgp multicast routing-table peer** command displays the routes received from or sent to a specified MBGP peer.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table peer *peer-address* { **advertised-routes** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] | **accepted-routes** }

display bgp multicast routing-table peer *peer-address* **received-routes** *network* [{ *mask* | *mask-length* } [**longer-prefixes** | **original-attributes**]]

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MBGP peer.	The value is in dotted decimal notation.
advertised-routes	Indicates the routes sent to a specified peer.	-
network	Specifies the IPv4 network address.	The value is in dotted decimal notation.
mask	Specifies the address mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
longer-prefixes	Uses the longest match rule to select routes.	-
received-routes	Indicates the routes received from a specified peer.	-
active	Displays the active routes received from the specified peer.	-
accepted-routes	Displays routing information that is received from neighbors and matches the filter policy.	-

Parameter	Description	Value
original-attributes	Displays the original attributes of a public route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table peer** command to check routes received of a specified MBGP peer.

Example

Display the routes sent to multicast peer 10.10.1.11.

```
<HUAWEI> display bgp multicast routing-table peer 10.10.1.11 advertised-routes
 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 9
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>i  10.1.2.0/24        10.7.1.2        0          100        0      ?
 *>   10.2.1.0/24        0.0.0.0        0                     0      ?
 *>   10.7.1.0/24        0.0.0.0        0                     0      ?
 *>i  10.7.1.0/24        10.7.1.2        0          100        0      ?
 *>i  10.7.1.1/32        10.7.1.2        0          100        0      ?
 *>   10.7.1.2/32        0.0.0.0        0                     0      ?
 *>   10.10.1.0/24        0.0.0.0        0                     0      ?
```

Table 7-150 Description of the display bgp multicast routing-table peer command output

Item	Description
BGP local router ID	BGP local router ID
Total Number of Routes	Total number of routes
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packets
MED	Multi-Exit discriminator
LocPrf	Local preference

Item	Description
PrefVal	Preferred value of protocols
Path/Ogn	AS path and Origin attribute

7.8.53 display bgp multicast routing-table regular-expression

Function

The **display bgp multicast routing-table regular-expression** command displays the routes that match the specified AS_Path regular expression.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table regular-expression *as-regular-expression*

Parameters

Parameter	Description	Value
as-regular-expression	Specifies the AS_Path regular expression.	The value is a string of 1 to 80 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table regular-expression** command to check the routes that match the specified AS_Path regular expression.

Example

Display the routes that match the AS_Path regular expression 2.

```
<HUAWEI> display bgp multicast routing-table regular-expression 2
BGP local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
```

```
            Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 13
     Network            NextHop        MED      LocPrf     PrefVal Path/Ogn
*>   10.1.2.0/24        10.2.1.2                          0      2?
*>   10.2.1.0/24        10.2.1.2       0                   0      2?
*>   10.7.1.0/24        10.2.1.2                          0      2?
*>   10.7.1.1/32        10.2.1.2                          0      2?
*>   10.7.1.2/32        10.2.1.2       0                   0      2?
*>   10.11.12.0/24       10.2.1.2       0                   0      2?
*>   10.11.12.1/32       10.2.1.2       0                   0      2?
```

Table 7-151 Description of the display bgp multicast routing-table regular-expression command output

Item	Description
BGP local router ID	BGP local router ID.
Network	Network address in the MBGP routing table.
NextHop	Next-hop address for packets.
MED	MED of the route.
LocPrf	Local preference.
PrefVal	Preferred value.
Path/Ogn	AS_Path number and Origin attribute.

7.8.54 display bgp multicast routing-table statistics

Function

The **display bgp multicast routing-table statistics** command displays statistics about routes in the MBGP routing table.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast routing-table statistics

display bgp multicast routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
peer *ipv4-address*	Displays the number of routes with a specified peer address.	The value is in dotted decimal notation.
advertised-routes	Displays the number of routes advertised to a specified peer.	-
received-routes	Displays the number of routes received from a specified peer.	-
active	Displays the number of active routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp multicast routing-table statistics** command to check statistics about routes in the MBGP routing table.

Example

Display statistics about routes in the MBGP routing table.

```
<HUAWEI> display bgp multicast routing-table statistics
Total Number of Routes: 50
```

Table 7-152 Description of the display bgp multicast routing-table statistics command output

Item	Description
Total Number of Routes	Total number of routes in the MBGP routing table

7.8.55 display bgp multicast update-peer-group

Function

The **display bgp multicast update-peer-group** command displays information about MBGP update-groups.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display bgp multicast update-peer-group [**index** *update-group-index*]

Parameters

Parameter	Description	Value
index *update-group-index*	Specifies the index of an update-group.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the index of an update-group is specified, the command will display detailed information about the specified update-group.

Example

Display information about MBGP update-groups.

```
<HUAWEI> display bgp multicast update-peer-group
 The Multicast instance's update peer group number : 1
 Keep buffer update peer group number : 0
 BGP Version : 4

 Group ID : 0
 Group Type : external
 Addr Family : IPv4-MLC
 AdvMinTimeVal : 30
 Total Peers : 1
 Leader Peer : 192.168.1.2
 Peers List : 192.168.1.2
```

Table 7-153 Description of the display bgp multicast update-peer-group command output

Item	Description
The Multicast instance's update peer group number	Indicates the number of update-groups in the instance.
Keep buffer update peer group number	Number of packets in update-groups saved in the batch buffer.

Item	Description
BGP Version	Indicates the BGP version.
Group ID	Indicates the ID of the update-group.
Group Type	Indicates the type of the update-group, which can be one of the following: ● external: indicates an EBGP update-group. ● internal: indicates an IBGP update-group. ● external-confed: indicates an EBGP update-group in the confederation. ● internal-confed: indicates an IBGP update-group in the confederation. ● unknown: indicates an update-group of an unknown type.
Addr Family	Indicates the address family.
AdvMinTimeVal	Indicates the minimum interval for sending Update packets with the same route prefix.
Total Peers	Indicates the total number of peers in an update-group.
Leader Peer	Indicates the representative of an update-group.
Peers List	Indicates a list of peers.

7.8.56 display bgp mvpn brief

Function

The **display bgp mvpn brief** command displays brief information about VPN instances in BGP MVPN address family.

Format

display bgp mvpn { **all** | **vpn-instance** *vpn-instance-name* } **brief**

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Displays brief information about MVPN and all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bgp mvpn brief** command is used to display brief information about VPN instances in BGP MVPN address family.

Example

Display brief information about MVPN and all VPN instances.

```
<HUAWEI> display bgp mvpn all brief

MVPN:
  Rd Num            Peer Num          Route Num
  0                1                 0

VPN-Instance(IPv4-MVPN-family):
  VPN-Instance Name   Peer Num           Route Num
  vrf0              0                0
  vrf1              0                0
  vrf11              0                0
  vrf12              0                0
  vrf13              0                0
  vrf14              0                0
  vrf2              0                20
  vrf3              0                20
  vrf4              0                24
  vrf5              0                24
  vrf6              0                0
  vrf7              0                0
  vrf8              0                20
```

Table 7-154 Description of the **display bgp mvpn all brief** command output

Item	Description
Rd Num	Number of Route Distinguishers (RDs).
Peer Num	Number of peers.

Item	Description
Route Num	Number of routes.
VPN-Instance Name	Name of a VPN instance.

7.8.57 display bgp mvpn routing-table

Function

The **display bgp mvpn routing-table** command displays the information of BGP MVPN routes.

Format

display bgp mvpn { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

display bgp mvpn route-distinguisher *route-distinguisher* **routing-table** [*network* [*mask* | *mask-length*]]

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table regular-expression** *as-regular-expression*

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community** [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp mvpn all routing-table peer *ipv4-address* { **advertised-routes** [*network*] | **received-routes** [**active**] }

display bgp mvpn all routing-table peer *ipv4-address* **received-routes** *network*

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Display all the BGP MVPN routing information.	-
vpn-instance *vpn-instance-name*	Displays the BGP MVPN routing information of the specified VPN instance.	The value must be an existing VPN instance name.
network	Specifies the IPv4 network address.	It is in dotted decimal notation.
mask | *mask-length*	Specifies mask in dotted decimal notation or mask-length.	The value of mask-length is an integer that ranges from 0 to 32.
longer-prefixes	Matches according to the mask longer than the specified length.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays BGP routing information of the specified Route Distinguisher (RD).	The RD formats are divided into the following types: ● 2-byte AS number:32-bit user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● 32-bit IP address:16-bit user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

Parameter	Description	Value
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals.
cidr	Displays the BGP MVPN routing information about the Classless Inter-Domain Routing (CIDR).	-
different-origin-as	Displays routes that have the same destination address but different source ASs.	-
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.
community-filter	Displays the BGP MVPN routing information that matches the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
whole-match	Indicates the exact matching.	-
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.

Parameter	Description	Value
community	Displays the BGP MVPN routing information of the specified BGP community attribute in the routing table.	-
aa:nn	Specifies the community attribute number.	Both aa and nn are integers ranging from 0 to 65535. You can set a maximum of 29 community numbers.
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
peer *ipv4-address*	Displays the BGP MVPN routing information for the specified BGP peer.	It is in dotted decimal notation.
advertised-routes	Displays the BGP MVPN routing information advertised to the specified peer.	-
received-routes	Displays the BGP MVPN routing information received from the specified peer.	-

Parameter	Description	Value
active	Displays the active BGP MVPN routing information received from the specified peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information of BGP MVPN routes. If the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed.

Example

Display all the BGP MVPN routing information.

```
<HUAWEI> display bgp mvpn all routing-table

 BGP Local router ID is 192.168.7.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 3
 Route Distinguisher: 100:1

      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                     0      ?

 Route Distinguisher: 200:1

      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  1.1.1.1/32         192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?

 Total number of routes of IPv4-MVPN-family for vpn-instance vrf1: 3
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                     0      ?
 * i                   192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?
```

Display all the BGP MVPN routing information of the VPN instance named vpna.

```
<HUAWEI> display bgp mvpn vpn-instance vpna routing-table

Total Number of Routes: 2

 BGP Local router ID is 2.2.2.9
 Status codes: * - valid, > - best, d - damped,
```

```
            h - history,  i - internal, s - suppressed, S - Stale
            Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop        MED      LocPrf    PrefVal Path/Ogn

*>i  10.1.1.0/24      1.1.1.9         0        100       0      ?
*>i  10.2.1.0/24      3.3.3.9         0        100       0      ?
```

Display the BGP MVPN routing information of the specified RD.

```
<HUAWEI> display bgp mvpn route-distinguisher 100:1 routing-table

 BGP Local router ID is 192.168.7.1
 Status codes: * - valid, > - best, d - damped,
            h - history,  i - internal, s - suppressed, S - Stale
            Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1

 Total Number of Routes: 1

     Network           NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   1.1.1.1/32        0.0.0.0         0                    0      ?

 Total number of routes of IPv4-MVPN-family for vpn-instance vrf1: 3
     Network           NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   1.1.1.1/32        0.0.0.0         0                    0      ?
* i                 192.168.100.10  0          100        0      33 55?
*>i  2.2.2.2/32        192.168.100.10  0          100        0      33 55?
```

Display all BGP MVPN routes of community 1000:100.

```
<HUAWEI> display bgp mvpn all routing-table community 1000:100

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
            h - history,  i - internal, s - suppressed, S - Stale
            Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 1

 Route Distinguisher: 100:1

     Network           NextHop        MED        LocPrf    PrefVal Community

*>i  10.1.1.0/24       1.1.1.1         0          100        0      <1000:100>

 Total number of routes of IPv4-MVPN-family for vpn-instance vpna: 1
     Network           NextHop        MED        LocPrf    PrefVal Community

*>i  10.1.1.0/24       1.1.1.1         0          100        0      <1000:100>
```

Table 7-155 Description of the **display bgp mvpn routing-table** command output

Item	Description
Network	Network address in the BGP routing table.
Next Hop	Next Hop address through which the packet has to be sent.
MED	Multi_Exit discriminator.
LocPrf	Local preference.

Item	Description
PrefVal	Value preferred by the protocol.
Path/Ogn	AS_Path number and the attributes of Origin.
Community	Community attributes.

Display all BGP MVPN routes of community 1000:100 with the Internet community attribute.

```
<HUAWEI> display bgp mvpn all routing-table community 1000:100 internet

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 1

 Route Distinguisher: 100:1


      Network            NextHop        MED        LocPrf    PrefVal Community

 *>i  10.1.1.0/24        1.1.1.1         0          100        0      <1000:100>

 Total number of routes of IPv4-MVPN-family for vpn-instance vpna: 4
      Network            NextHop        MED        LocPrf    PrefVal Community

 *>i  10.1.1.0/24        1.1.1.1         0          100        0      <1000:100>
 *>   10.2.1.0/24        0.0.0.0         0                     0
 *                       10.2.1.1        0                     0
 *>   10.2.1.2/32        0.0.0.0
```

Display routes sent by 2.2.2.2.

```
<HUAWEI> display bgp mvpn all routing-table peer 2.2.2.2 received-routes

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1

 Route Distinguisher: 2:2


      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  2.2.2.2/32         2.2.2.2         0          100        0      ?
```

Display detailed information about the BGP MVPN route with prefix 3.3.3.3.

```
<HUAWEI> display bgp mvpn all routing-table 3.3.3.3


 BGP local router ID : 192.168.1.108
 Local AS number : 100

 Total routes of Route Distinguisher(1:1): 2
 BGP routing table entry information of 3.3.3.3/32:
 From: 1.1.1.1 (192.168.1.104)
```

```
 Route Duration: 00h00m10s
 Relay IP Nexthop: 10.1.1.4
 Relay IP Out-Interface: Ethernet0/0/1
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 Ext-Community:RT <111 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, pre 255, IGP cost 10,
 PMSI: Flags 0, PIM-SM, label 0:0:0(0), Sender address: 3.3.3.3, Group address: 232.1.1.1
 Not advertised to any peer yet

 BGP routing table entry information of 3.3.3.3/32:
 From: 10.1.1.4 (192.168.1.104)
 Route Duration: 00h05m44s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface: Ethernet0/0/1
 Original nexthop: 10.1.1.4
 Qos information : 0x0
 Ext-Community:RT <111 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, pre 255, IGP cost 0, not preferred for peer address,
 PMSI: Flags 0, PIM-SM, Label 0:0:0(0), Sender address: 3.3.3.3, Group address: 232.1.1.1
 Not advertised to any peer yet


 Total number of routes of IPv4-MVPN-family for vpn-instance 1: 2
 BGP routing table entry information of 3.3.3.3/32:
 From: 1.1.1.1 (192.168.1.104)
 Route Duration: 00h00m10s
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 Ext-Community:RT <111 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, pre 255,
 PMSI: Flags 0, PIM-SM, Label 0:0:0(0), Sender address: 3.3.3.3, Group address: 232.1.1.1
 Not advertised to any peer yet

 BGP routing table entry information of 3.3.3.3/32:
 From: 10.1.1.4 (192.168.1.104)
 Route Duration: 00h05m45s
 Original nexthop: 10.1.1.4
 Qos information : 0x0
 Ext-Community:RT <111 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, pre 255, not preferred for peer address,
 PMSI: Flags 0, PIM-SM, Label 0:0:0(0), Sender address: 3.3.3.3, Group address: 232.1.1.1
 Not advertised to any peer yet
```

Display detailed information about the route with prefix 2.2.2.2 sent by 2.2.2.2.

```
<HUAWEI> display bgp mvpn all routing-table peer 2.2.2.2 received-routes 2.2.2.2

 BGP local router ID : 1.1.1.1
 Local AS number : 100
 Route Distinguisher: 2:2

 BGP routing table entry information of 2.2.2.2/32:
 From: 2.2.2.2 (2.2.2.9)
 Route Duration: 18h27m03s
 Relay IP Nexthop: 10.1.1.2
 Relay IP Out-Interface: Ethernet0/0/1
 Original nexthop: 2.2.2.2
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, pre 255, IGP cost 1
 PMSI: Flags 0, PIM-SM, label 0:0:0, Sender address: 2.2.2.2, Group address: 232.1.1.1
 Not advertised to any peer yet
```

Table 7-156 Description of the display bgp mvpn all routing-table peer received-routes command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Route Distinguisher	Route distinguisher.
BGP routing table entry information of 2.2.2.2/32	The following information is about 2.2.2.2/32 routing entries.
From	IP address of the router that sends the route. 2.2.2.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 2.2.2.9 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *ip-precedence* command has been run and the *ip-precedence* varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
localpref	Local priority.
pref-val	Value preferred by the protocol.
valid	The BGP route is a valid route.
internal	The BGP route is an internal route.
best	The BGP route is an optimal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.
IGP cost	Cost of the relied route.
PMSI: Flags 0, PIM-SM, label 0:0:0, Sender address: 2.2.2.2, Group address: 232.1.1.1	In NG MVPNs, P-Multicast Service Interfaces (PMSIs) are logical channels that transmit multicast VPN services over the public network. ● Flags: Point-to-Multipoint (P2MP) tunnel flags. ● PIM-SM: The PIM-SM protocol. ● label: Label information about the PMSI. ● Sender address: IP address of the sender PE. ● Group address: IP address of the multicast group.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

7.8.58 display bgp mvpn routing-table statistics

Function

The **display bgp mvpn routing-table statistics** command displays the statistics of the BGP MVPN routes.

Format

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics**

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics regular-expression** *as-regular-expression*

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp mvpn { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community** [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp mvpn all routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Displays all the statistics of the BGP MVPN routes.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the BGP MVPN routing statistics of the specified Route Distinguisher (RD).	-
vpn-instance *vpn-instance-name*	Displays the BGP MVPN routing statistics of the specified VPN instance.	The value must be an existing VPN instance name.
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matched AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals.
cidr	Displays the BGP MVPN routing statistics about the Classless Inter-Domain Routing (CIDR).	-
different-origin-as	Displays the routes that have the same destination address but different source AS number.	-
regular-expression *as-regular-expression*	Indicates the matched AS regular expression.	The value is a string of 1 to 80 characters.
community-filter	Displays the BGP MVPN routing statistics that matches the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
whole-match	Indicates exact matching.	-

Parameter	Description	Value
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community	Displays the BGP MVPN routing statistics of the specified BGP community attribute in the routing table.	-
aa:nn	Specifies the community number.	Both aa and nn are integers ranging from 0 to 65535. You can set a maximum of 29 community numbers.
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with the No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
peer *ipv4-address*	Displays the BGP MVPN routing statistics for the specified BGP peer.	It is in dotted decimal notation.
advertised-routes	Displays the BGP MVPN routing statistics advertised to the specified peer.	-
received-routes	Displays the BGP MVPN routing statistics from the specified peer.	-

Parameter	Description	Value
active	Displays the active BGP MVPN routing statistics received from the specified peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display all the statistics of the BGP MVPN routing table.

```
<HUAWEI> display bgp mvpn all routing-table statistics

 Total number of routes from all PE: 20

 Total number of routes of IPv4-MVPN-family for vpn-instance vpn1: 12
```

Table 7-157 Description of the **display bgp mvpn routing-table statistics** command output

Item	Description
Total number of routes from all PE	The number of the routes received from PEs in the BGP MVPN routing table
Total number of routes of IPv4-MVPN-family for vpn-instance	The number of the routes of the specified VPN instance in the BGP MVPN routing table

7.8.59 display bgp network

Function

The **display bgp network** command displays the routes imported into the BGP routing table by using the **network** command.

Format

display bgp network

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **network**

display bgp ipv6 network

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **network** (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
vpnv4	Displays the VPNv4 routes that are advertised by using the **network** command.	-
vpnv6	Displays the VPNv6 routes that are advertised by using the **network** command.	-
all	Displays all the VPNv4 routes that are advertised by using the **network** command.	-
vpn-instance *vpn-instance-name*	Displays the routes of a specified VPN instance that are advertised by using the **network** command.	The value must be an existing VPN instance name.
ipv6	Displays the IPv6 routes advertised by BGP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

BGP cannot discover routes by itself. Run the **network (BGP)** command and the **import-route (BGP)** command to import routes from other protocols, such as IGP routes or static routes, to the BGP routing table.

The **display bgp network** command displays the routing information advertised by BGP through the **network (BGP)** command.

Precautions

BGP has multiple address families and the routing information about each address family is isolated from each other. The routing information about address families advertised by BGP through the **network (BGP)** command can be displayed by specifying different parameters.

If no parameter is specified, the **display bgp network** command displays the routing information about the IPv4 unicast address family advertised by BGP through the **network (BGP)** command.

Example

Display information about routes that are imported using the **network** command.

```
<HUAWEI> display bgp network
  BGP Local Router ID is 10.1.1.9
  Local AS Number is 10(Public)
  Network          Mask            Route-policy

  10.2.0.0         255.255.0.0
  10.0.0.0         255.0.0.0       Policy1
  10.4.4.0         255.255.255.0
```

Table 7-158 Description of the display bgp network command output

Item	Description
Local AS Number	Indicates the local AS number.
Network	Indicates the locally-advertised network address.
Mask	Indicates the mask of the network address.
Route-policy	Indicates the used routing policy.

Display information about BGP VPNv4 routes that are imported using the **network** command.

```
<HUAWEI> display bgp vpnv4 all network
  BGP Local Router ID is 10.2.2.9
  Local AS Number is 100
 VPN-Instance vrf1, Router ID 10.2.2.9:
  Network          Mask            Route-policy
  10.4.4.4         255.255.255.255
 VPN-Instance vrf2, Router ID 2.2.2.9:
  Network          Mask            Route-policy
  10.5.5.5         255.255.255.255
```

Table 7-159 Description of the display bgp vpnv4 all network command output

Item	Description
VPN-Instance	Name of the VPN instance
Router ID	Router ID of the local BGP router.

Display IPv6 routes advertised by BGP.

```
<HUAWEI> display bgp ipv6 network
  BGP Local Router ID is 10.5.5.5
  Local AS Number is 100(PublicV6)
  Network          Prefix           Route-policy
  FC00:0:0:100::   64
  FC00:0:0:200::   64
```

Display VPNv6 routes locally advertised by BGP (by using the **network** command) for a specified VPN instance.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 network
  BGP Local Router ID is 10.1.1.1
  Local AS Number is 100
  Route Distinguisher: 100:1
  (vpn1)
  Network          Prefix           Route-policy
  FC00:0:0:2000::  100               policy1
```

Table 7-160 Description of the display bgp vpnv6 network command output

Item	Description
BGP Local Router ID	Indicates the ID of the local BGP device. The ID is in the same format as an IPv4 address.
Local AS Number	Indicates the local AS number.
Route Distinguisher	Indicates the route distinguisher for the VPN instance.
Prefix	Indicates the network address mask advertised by the local BGP device.

Display the VPNv6 routes locally advertised by BGP (by using the **network** command).

```
<HUAWEI> display bgp vpnv6 all network
  BGP Local Router ID is 10.2.2.9
  Local AS Number is 100
  Route Distinguisher: 100:4
  (vpn1)
  Network          Prefix           Route-policy
  FC00:0:0:1::1    128
  FC00:0:0:2::2    128
  Route Distinguisher: 100:5
  (vrf1)
  Network          Prefix           Route-policy
  FC00:0:0:3::3    128
  Route Distinguisher: 100:9
  (vrf2)
  Network          Prefix           Route-policy
  FC00:0:0:8::9    128
```

7.8.60 display bgp paths

Function

The **display bgp paths** command displays the AS_Path information of BGP routes.

Format

display bgp paths [*as-regular-expression*]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

display bgp ipv6 paths [*as-regular-expression*]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*] (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp { **mdt** | **mvpn** } { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

NOTE

The **mdt,mvpn** parameter is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
as-regular-expression	Specifies the regular expression used to match the AS_Path information.	The name is a string of 1 to 80 characters.
vpnv4	Displays the AS_Path information of the routes of a VPNv4 instance.	-
vpnv6	Displays the AS_Path information of the routes of a VPNv6 instance.	-
all	Displays the AS_Path information of all VPNv4 routes.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ipv6	Displays the path attributes of IPv6-BGP routes in the local BGP database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bgp paths** command displays the path attributes of BGP stored in the system.

BGP usually has a large number of path attributes. The **display bgp paths** command displays a lot of BGP path information for viewing. After configuring *as-regular-expression*, the **display bgp paths** command displays only the path attributes of BGP that match *as-regular-expression*. For details on a regular expression, see Filtering Output Information Based on the Regular Expression in "CLI Overview" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Basic Configuration*.

Precautions

BGP has a number of address families and the path attributes of BGP in each address family is stored independently. By default, the **display bgp paths** command displays only the path attributes of BGP in the IPv4 unicast address family. The path attributes of BGP in other address families can be displayed by specifying address family parameters.

Example

Display the AS_Path information.

```
<HUAWEI> display bgp paths

 Total number of routes of IPv4-family for vpn-instance _public_: 6
 Total Number of Paths: 1

 Address          Refcount        MED  Path/Origin
 1282430404              6          0  N?
```

Table 7-161 Description of the display bgp paths command output

Item	Description
Address	Indicates the address of the route in the local database, in hexadecimal notation.
Refcount	Indicates the number of times that the route is referenced.
MED	Indicates the MED of the route.
Path	Indicates the list of ASs through which the packet has to pass through.
Origin	Indicates the origin of the route.

7.8.61 display bgp peer

Function

The **display bgp peer** command displays information about BGP peers.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** [{ *group-name* | *ipv4-address* } **log-info** | [*ipv4-address*] **verbose**]

display bgp vpnv4 all peer [[*ipv4-address*] **verbose**]

display bgp vpls peer [[*ipv4-address*] **verbose**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp ipv6 peer [**verbose**]

display bgp ipv6 peer *ipv6-address* { **log-info** | **verbose** }

display bgp ipv6 peer *ipv4-address* **verbose**

display bgp vpnv6 all peer [[*ipv4-address*] **verbose**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv6 vpn-instance *vpn-instance-name* **peer** [{ *group-name* | *ipv6-address* } **log-info** | [*ipv6-address*] **verbose**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp l2vpn-ad peer [[*ipv4-address*] **verbose**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp l2vpn peer [[*ipv4-address*] **verbose**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp { **mdt** | **mvpn** } **all peer** [[*ipv4-address*] **verbose**](supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ipv4-address	Specifies the IPv4 address of a peer to be displayed.	It is in dotted decimal notation.

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
log-info	Indicates to display log information of the specified peer.	-
verbose	Indicates to display detailed peer information.	-
vpnv4	Indicates to display information about peers in a VPNv4 instance.	-
all	Indicates to display information about peers in all VPNv4 or VPNv6 instances.	-
vpls	Displays information about peers in the BGP-VPLS view.	-
ipv6-address	Specifies the IPv6 address of a peer to be displayed.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vpnv6	Indicates to display BGP VPNv6 peer information.	-
l2vpn-ad	Displays information about peers in the BGP L2VPN-AD view.	-
l2vpn	Displays information about peers in the BGP L2VPN view.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bgp peer** command displays information about a BGP peer. You can implement the following operations based on the command output:

- To check the status of BGP connections
- To check information about a BGP peer
- To check whether a BGP peer is successfully configured using the **peer as-number** command
- To check whether a BGP peer is successfully deleted using the **undo peer as-number** command

Precautions

BGP has multiple address families. By default, the **display bgp peer** command displays information about BGP peers in IPv4 unicast address family only. If you want to view information about BGP peers in another address family, you need to specify its address family parameter.

To view detailed information about a BGP peer, such as information about BGP timers, the number of sent and received routes, capacities supported, the number of sent and received BGP messages, and enabled functions, specify **verbose** in the command.

If **log-info** is specified in the command, log information about a BGP peer is displayed, including information about BGP peer flapping.

Example

Display peer information.

```
<HUAWEI> display bgp peer

 Status codes: * - Dynamic

 BGP Local router ID : 10.2.3.4
 local AS number : 10
 Total number of peers : 2                 Peers in established state : 1
 Total number of dynamic peers : 0

  Peer        V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  10.1.1.1    4   100        0        0     0 00:00:07        Idle       0
  10.2.5.6    4   200       32       35     0 00:17:49 Established       0
```

Table 7-162 Description of the display bgp peer command output

Item	Description
Status codes: * - Dynamic	Status code. If the value starts with an asterisk (*), the peer is a dynamic peer. Currently, the value can only be *** - Dynamic**.

Item	Description
BGP Local router ID	Indicates the ID of the BGP local router. **NOTE** If two ends have the same BGP local router ID, no BGP peer relationship can be established between them. In this situation, run the **router id** command in the BGP view on either end to change the BGP local router ID. Changing it to the IP address of a loopback interface is recommended.
local AS number	Indicates the local AS number.
Total number of peers	Indicates the number of peers.
Peers in established state	Indicates the number of peers in established state.
Total number of dynamic peers	Total number of dynamic BGP peers.
Peer	Indicates the IP address of the peer.
V	Indicates the BGP version used on the peer.
AS	Indicates the AS number.
MsgRcvd	Indicates the number of received messages.
MsgSent	Indicates the number of sent messages.
OutQ	Indicates the message to be sent to the specified peer.
Up/Down	Indicates the period of time during which a BGP session keeps the current state.

Item	Description
State	Status of the peer: - Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. - Idle(Admin): indicates that the peer relationship is shut down initiatively and no attempt is made to establish the peer relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. - No neg: The capabilities of the BGP peer's address family have not been negotiated. - Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. - Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer

Item	Description
	with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for an Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues

Item	Description
	to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. ● Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PrefRcv	Indicates the number of route prefixes sent from the peer.

Display detailed information about the peer 10.2.2.9.

```
<HUAWEI> display bgp peer 10.2.2.9 verbose

         BGP Peer is 10.2.2.9,  remote AS 100
         Type: IBGP link
         BGP version 4, Remote router ID 10.1.1.1
         Update-group ID: 1
         BGP current state: Established, Up for 00h57m53s
         BGP current event: RecvKeepalive
         BGP last state: Established
         BGP Peer Up count: 1
         Received total routes: 0
         Received active routes total: 0
         Received mac routes: 0
         Advertised total routes: 2
         Port: Local - 42796        Remote - 179
         Configured: Connect-retry Time: 32 sec
         Configured: Min Hold Time: 0 sec
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Peer optional capabilities:
         Peer supports bgp multi-protocol extension
         Peer supports bgp route refresh capability
         Peer supports bgp 4-byte-as capability
         Address family IPv4 Unicast: advertised and received
         Address family IPv6 Unicast: received
```

```
 Received: Total 60 messages
                 Update messages               1
                 Open messages                1
                 KeepAlive messages            58
                 Notification messages         0
                 Refresh messages             0
 Sent: Total 61 messages
                 Update messages               2
                 Open messages                1
                 KeepAlive messages            58
                 Notification messages         0
                 Refresh messages             0
 Authentication type configured: None
 Last keepalive received: 2012/03/06 19:17:37  Last keepalive sent    : 2012/03/06 19:17:37  Last update
received: 2012/03/06 19:17:43  Last update    sent    : 2012/03/06 19:17:37

 Minimum route advertisement interval is 15 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 Listen-only has been configured
 Peer's BFD has been enabled
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

Table 7-163 Description of the display bgp peer verbose command output

Item	Description
Type	Indicates the BGP link type, which can be IBGP or EBGP.
BGP version	Indicates the BGP version.
remote router ID	Indicates the router ID of the peer.
Update-group ID	Indicates the ID of the update-group to which the peer belongs.

Item	Description
BGP current state	Current state of BGP: ● Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. ● Idle(Admin): indicates that the peer relationship is shut down initiatively and no attempt is made to establish the peer relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. ● No neg: The capabilities of the BGP peer's address family have not been negotiated. ● Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. ● Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer

Item	Description
	with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for an Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues

Item	Description
	to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. ● Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
BGP current event	Indicates the current BGP event.
BGP last state	Indicates the last BGP status, which may be Idle, Connect, Active, OpenSent, OpenConfirm, or Established.
BGP Peer Up count	Indicates the flapping count of a BGP peer in a specified period of time.
Received total routes	Indicates the number of received route prefixes.
Received active routes total	Indicates the number of received active route prefixes.
Received mac routes	Number of MAC routes received.
Advertised total routes	Indicates the number of sent route prefixes.
Port	Indicates the port number. ● Local: indicates the local port number, which is always 179. BGP uses TCP at the transport layer. ● Remote: indicates the port number used on the peer.

Item	Description
Configured	Indicates locally configured timers. ● Connect-retry Time: indicates the ConnectRetry interval for a BGP peer or peer group, in seconds. When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. ● Min Hold Time: indicates the minimum Holdtime configured on the local device, in seconds. ● Active Hold Time: indicates the hold time. If BGP does not receive any Keepalive message from the peer in the hold time, BGP considers that the peer is Down and then instructs other peers to remove the routes that are sent from the peer. ● Keep Alive Time: indicates the interval for sending Keepalive messages to the peer. BGP peers send Keepalive messages to each other periodically to maintain their relationships.
Received : Active Hold Time	Indicates the hold time on the peer.
Negotiated : Active Hold Time	Indicates the hold time agreed between the BGP peers after capability negotiation.
Address family IPv4 Unicast	Indicates the IPv4 unicast address family.
Address family IPv6 Unicast	Indicates the IPv6 unicast address family.

Item	Description
Received	Indicates the number of packets received from a peer. - Total: indicates the total number of messages received from a peer. - Update messages: indicates the number of Update messages received from a peer. - Open messages: indicates the number of Open messages received from a peer. - KeepAlive messages: indicates the number of Keepalive messages received from a peer. - Notification messages: indicates the number of Notification messages received from a peer. - Refresh messages: indicates the number of route-refresh messages received from a peer.
Sent	Indicates the number of messages sent to a peer. - Total: indicates the total number of messages sent to a peer. - Update messages: indicates the number of Update messages sent to a peer. - Open messages: indicates the number of Open messages sent to a peer. - KeepAlive messages: indicates the number of Keepalive messages sent to a peer. - Notification messages: indicates the number of Notification messages sent to a peer. - Refresh messages: indicates the number of route-refresh messages sent to a peer.
Authentication type configured	Indicates the authentication type configured.

Item	Description
Last keepalive received	Indicates the time when the Keepalive packet is received last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
Last keepalive sent	Indicates the time when the Keepalive packet is sent last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.

Item	Description
Last update received	Indicates the time when the Update packet is received last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
Last update sent	Indicates the time when the Update packet is sent last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
Minimum route advertisement interval is 15 seconds	Indicates the minimum interval between route advertisements. ● The minimum interval for advertising EBGP routes is 30 seconds. ● The minimum interval for advertising IBGP routes is 15 seconds.
Optional capabilities	(Optional) Indicates the peer-supported capabilities.
Route refresh capability has been enabled	Indicates that route refreshing has been enabled.

Item	Description
4-byte-as capability has been enabled	Indicates that the 4-byte AS number capability is enabled.
Listen-only has been configured	Indicates that only connection requests are snooped and no connections will be initiated proactively.
Peer Preferred Value	Indicates the preferred value of the peer.
Routing policy configured	Indicates the configured routing policy.
Peer's BFD has been enabled	Indicates that BFD has been enabled on the peer.

Display log information on BGP peer 10.1.1.2.

```
<HUAWEI> display bgp peer 10.1.1.2 log-info
Peer : 10.1.1.2
 Date/Time     : 2011/13/06 11:53:21
 State         : Up
 Date/Time     : 2011/13/06 11:53:09
 State         : Down
 Error Code    : 6(CEASE)
 Error Subcode : 4(Administrative Reset)
 Notification  : Receive Notification
 Date/Time     : 2011/13/06 10:34:05
 State         : Up
```

Table 7-164 Description of the display bgp peer 1.1.1.2 log-info command output

Item	Description
Error Code	Error code.
Error Subcode	Error subcode.
Notification	Notification packet sent or received by a peer.

Display information about the BGP peer of the VPN instance vrf1.

```
<HUAWEI> display bgp vpnv4 vpn-instance vrf1 peer

 Status codes: * - Dynamic

 BGP local router ID : 10.1.1.9
 Local AS number : 100
 VPN-Instance vrf1, router ID 10.1.1.1:
 Total number of peers : 1                 Peers in established state : 1
 Total number of dynamic peers : 0

  Peer        V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  10.1.1.1    4 65410      207      192     0 02:59:49 Established       1
```

Display detailed information about the BGP peer of the VPN instance vpna.

```
<HUAWEI> display bgp vpnv4 vpn-instance vpna peer verbose

         BGP Peer is 10.1.1.1,  remote AS 200
         Type: EBGP link
         BGP version 4, remote router ID 10.1.1.1

         Update-group ID: 1
         BGP current state: Established, Up for   03h01m22s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         BGP Peer Up count: 1              Received total routes: 0             Received active routes total: 0
Received mac routes: 0             Advertised total routes: 3
         Port:  Local - 3722     Remote - 179
         Configured: Connect-retry Time: 32 sec
         Configured: Min Hold Time: 0 sec
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer supports bgp multi-protocol extension
         Peer supports bgp route refresh capability
         Peer supports bgp 4-byte-as capability
         Address family IPv4 Unicast: advertised and received

 Received: Total 76 messages
                  Update messages               0
                  Open messages                 5
                  KeepAlive messages            71
                  Notification messages         0
                  Refresh messages              0

 Sent: Total 91 messages
                  Update messages               0
                  Open messages                 10
                  KeepAlive messages            77
                  Notification messages         4
                  Refresh messages              0
 Authentication type configured: None
 Last keepalive received: 2012/03/06 19:17:37
 Last keepalive sent    : 2012/03/06 19:17:37
 Last update    received: 2012/03/06 19:17:43
 Last update    sent    : 2012/03/06 19:17:37
 Maximum allowed prefix number: 150000  Threshold: 75%
 Minimum route advertisement interval is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

Display information about IPv6 peers.

```
<HUAWEI> display bgp ipv6 peer

 BGP Local router ID : 10.0.0.1
 local AS number : 100
  Total number of peers : 1                 Peers in established state : 1

  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  FC00:0:0:20::21 4   200       17       19     0 00:09:59 Established       3
```

Display information about IPv6 peers.

```
<HUAWEI> display bgp ipv6 peer fc00:0:0:2001::1 verbose
         BGP Peer is FC00:0:0:2001::1,  remote AS 1
         Type: EBGP link
         BGP version 4, remote router ID 10.1.1.1
```

```
        Update-group ID: 1
        BGP current state: Established, Up for 00h00m59s
        BGP current event: RecvKeepalive
        BGP last state: OpenConfirm
        BGP Peer Up count: 2
        Received total routes: 0
        Received active routes total: 0
        Received mac routes: 0
        Advertised total routes: 0
        Port:  Local - 179      Remote - 49153
        Configured: Connect-retry Time: 32 sec
        Configured: Min Hold Time: 0 sec
        Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
        Received  : Active Hold Time: 180 sec
        Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
        Peer optional capabilities:
        Peer supports bgp multi-protocol extension
        Peer supports bgp route refresh capability
        Peer supports bgp 4-byte-as capability
        Address family IPv6 Unicast: advertised and received

 Received: Total 76 messages
                Update messages                0
                Open messages                  5
                KeepAlive messages             71
                Notification messages          0
                Refresh messages               0

 Sent: Total 91 messages
                Update messages                0
                Open messages                  10
                KeepAlive messages             77
                Notification messages          4
                Refresh messages               0
 Authentication type configured: None
 Last keepalive received: 2012/03/06 19:17:37
 Last keepalive sent    : 2012/03/06 19:17:37
 Last update    received: 2012/03/06 19:17:43
 Last update    sent    : 2012/03/06 19:17:37
 Minimum route advertisement interval is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 listen-only has been configured
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

Display brief information about a VPNv6 peer.

```
<HUAWEI> display bgp vpnv6 all peer

 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Total number of peers : 2                 Peers in established state : 2

  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  10.2.2.2        4   100      210      220     0   02:42:55    Established    1

  Peer of IPv6-family for vpn instance :

  VPN-Instance vpn1, Router ID 10.4.4.4 :
  FC00:0:0:200::2 4 65410      205      178     0 02:42:53     Established    0
```

Display detailed information about the VPNv6 peer whose IPv4 address is 10.2.2.2.

```
<HUAWEI> display bgp vpnv6 all peer 10.2.2.2 verbose
        BGP Peer is 10.2.2.2,  remote AS 200,
```

```
         Type: IBGP link
         BGP version 4, remote router ID 10.2.2.2

Group ID : 0
Peer Local Interface Name: Vlanif10
Local Ifnet Tunnel: 0xb0010000
         BGP current state: Established, Up for 02h43m52s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         BGP Peer Up count: 2
         Received total routes: 0
         Received active routes total: 0
         Received mac routes: 0
         Advertised total routes: 0
         Port:  Local - 53308    Remote - 179
         Configured: Connect-retry Time: 32 sec
         Configured: Min Hold Time: 0 sec
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Peer optional capabilities:
         Peer supports bgp multi-protocol extension
         Peer supports bgp route refresh capability
         Peer supports bgp 4-byte-as capability
         Address family IPv4 Unicast: advertised and received
         Address family VPNv6: advertised and received

 Received: Total 76 messages
                  Update messages               0
                  Open messages                 5
                  KeepAlive messages            71
                  Notification messages         0
                  Refresh messages              0

 Sent: Total 91 messages
                  Update messages               0
                  Open messages                 10
                  KeepAlive messages            77
                  Notification messages         4
                  Refresh messages              0
 Last keepalive received: 2009-09-30 09:52:41
 Minimum route advertisement interval is 15 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 Connect-interface has been configured
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

Display detailed information about the BGP peer of an IPv6 address family-enabled VPN instance whose IPv6 address is FC00:0:0:2000::2.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 peer fc00:0:0:2000::2 verbose

         BGP Peer is FC00:0:0:2000::2,  remote AS 65410,
         Type: EBGP link
         BGP version 4, remote router ID 10.1.1.1

Group ID : 0
Peer Local Interface Name: Vlanif10
Local Ifnet Tunnel: 0xb0010000
         BGP current state: Established, Up for 02h39m36s
         BGP current event: KATimerExpired
         BGP last state: OpenConfirm
         BGP Peer Up count: 2
         Received total routes: 0
         Received active routes total: 0
         Received mac routes: 0
         Advertised total routes: 0
```

```
        Port:  Local - 49177    Remote - 179
        Configured: Connect-retry Time: 32 sec
        Configured: Min Hold Time: 0 sec
        Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
        Received  : Active Hold Time: 180 sec
        Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
        Peer optional capabilities:
        Peer supports bgp multi-protocol extension
        Peer supports bgp route refresh capability
        Peer supports bgp 4-byte-as capability
        Address family IPv6 Unicast: advertised and received

Received: Total 76 messages
                Update messages               0
                Open messages                 5
                KeepAlive messages            71
                Notification messages         0
                Refresh messages              0

Sent: Total 91 messages
                Update messages               0
                Open messages                 10
                KeepAlive messages            77
                Notification messages         4
                Refresh messages              0
Last keepalive received: 2009-09-30 09:51:52
Minimum route advertisement interval is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
```

7.8.62 display bgp resource

Function

The **display bgp resource** command displays statistics about BGP specification information.

Format

display bgp resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check statistics about BGP specification information, run the **display bgp resource** command. This command displays only the total number of supported BGP peer sessions, including the numbers of various configured sessions.

Example

Display statistics about BGP specification information.

```
<HUAWEI> display bgp resource

 BGP Peer session support total number : 64

  Capacity Statistics     Used Number

  BGP Peer Session          3
  IBGP Peer Session         3
  EBGP Peer Session          0
```

Table 7-165 Description of the **display bgp resource** command output

Item	Description
BGP Peer session support total number	Maximum number of BGP peer sessions that are supported.
Capacity Statistics	BGP peer session type.
Used Number	Number of currently configured peer sessions.
BGP Peer Session	Total number of currently configured BGP peer sessions.
IBGP Peer Session	Number of IBGP peer sessions, including confederation IBGP and common IBGP peer sessions.
EBGP Peer Session	Number of EBGP peer sessions, including confederation EBGP and common EBGP peer sessions.

7.8.63 display bgp routing-table

Function

The **display bgp routing-table** command displays information about BGP routes. Information about specified routes can be displayed by specifying different parameters.

Format

display bgp routing-table [**verbose** | *ipv4-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

display bgp routing-table [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp routing-table regular-expression *as-regular-expression*

display bgp routing-table community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp routing-table community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp routing-table peer *ipv4-address* **received-routes** *ipv4-address* [{ *mask* | *mask-length* } [**longer-prefixes** | **original-attributes**]]

display bgp routing-table peer *ipv4-address* { **advertised-routes** [*ipv4-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] }

display bgp routing-table peer *ipv4-address* **accepted-routes**

display bgp routing-table time-range *start-time end-time*

Parameters

Parameter	Description	Value
verbose	Displays detailed information about BGP public network routes.	-
ipv4-address	Specifies an IPv4 network address.	The value is in dotted decimal notation.
mask | *mask-length*	Specifies a mask in dotted decimal notation or the mask length.	-
longer-prefixes	Matches any route whose prefix mask is longer than the specified length.	-
as-path-filter	Displays the routes that match a specified filter.	-
as-path-filter-number	Specifies the number of the matching AS_Path filter.	The value is an integer in the range from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The value is a string of 1 to 51 case-sensitive characters. It cannot contain spaces.

Parameter	Description	Value
cidr	Displays Classless InterDomain Routing (CIDR) information.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
different-origin-as	Displays routes that have the same destination address but different source AS numbers.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 characters. The string cannot contain only digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer in the range from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer in the range from 100 to 199.
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies a community number.	The value is an integer in the range from 0 to 4294967295.
aa:*nn*	Specifies a community number. A maximum of 29 community numbers can be set.	The values of *aa* and *nn* are both an integer in the range from 0 to 65535.
internet	Displays the BGP routes carrying the Internet community attribute.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-

Parameter	Description	Value
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
peer *ipv4-address*	Displays routes of a specified peer.	-
advertised-routes	Displays the routes advertised to a specified peer.	-
received-routes	Displays the routes received from a specified peer.	-
active	Displays the active routes received from a specified peer.	-
original-attributes	Displays the original attributes of a public route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
accepted-routes	Displays the routes that are received from the peer and filtered through a routing policy.	-

Parameter	Description	Value
time-range *start-time end-time*	Displays BGP routes that flap within the specified time period. For example, the value **0d0h5m0s** of *start-time* indicates 5 minutes before the current time. The value **0d0h10m0s** of *end-time* indicates 10 minutes before the current time. All BGP routes with the keepalive time in the range of 5 minutes to 10 minutes are displayed.	The value ranges of *start-time* and *end-time* are both **0d0h0m0s** to **10000d23h59m59s**.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can check information about specified routes by specifying different parameters.

The **display bgp routing-table** command is used to display active and inactive BGP routes on the public network.

Example

Display information about all BGP routes.

```
<HUAWEI> display bgp routing-table
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped, h - history,
               i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 4
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *     10.1.1.0/24        10.1.1.1        0                    0      100?
 *     10.1.1.2/32        10.1.1.1        0                    0      100?
 *>    10.1.1.0/24        10.1.1.1        0                    0      100?
 *>    10.1.1.0/24        10.1.1.1        0                    0      100?
```

Display routes with the community attribute.

```
<HUAWEI> display bgp routing-table community
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped, h - history,
               i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 4
      Network            NextHop        MED        LocPrf    PrefVal Community
```

```
*    10.1.1.0/24        10.1.1.1        0                  0      no-export
*    10.1.1.2/32        10.1.1.1        0                  0      no-export
*>   10.1.1.0/24        10.1.1.1        0                  0      no-export
*>   10.1.1.0/24        10.1.1.1        0                  0      no-export
```

Table 7-166 Description of the **display bgp routing-table** command output

Item	Description
BGP Local router ID	Router ID of the local BGP device.
Network	Network address in the BGP routing table.
NextHop	Next-hop address for packets.
MED	MED of a route.
LocPrf	Local preference.
PrefVal	Preferred value (PrefVal).
Path/Ogn	AS_Path number and Origin attribute.
Community	Community attribute information.

Display detailed information about a specified route.

```
<HUAWEI> display bgp routing-table 10.1.1.1
 BGP local router ID : 10.2.3.107
 Local AS number : 100
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 10.1.1.1/32:
 Imported route.
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 0d00h01m33s
 Direct Out-interface: Vlanif10
 Original nexthop: 10.1.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, pref-val 0, valid, external, best, select, pre 255
 Advertised to such 1 peers:
    10.1.1.2
```

Table 7-167 Description of the **display bgp routing-table** command output

Item	Description
Local AS number	Local AS number.
Paths	Route selection result.
BGP routing table entry information of	Routing entry information.
Imported route	Route imported into the BGP routing table using the **import-route** command.
From	IP address of the device that advertises the route.

Item	Description
Route Duration	Route duration.
Direct Out-interface	Directly connected outbound interface.
Original nexthop	Original next hop. **NOTE** If no routes to the BGP original next hop are available in the IP routing table, BGP routes cannot be advertised. In this case, find out why there is no route to the original next hop (this fault is generally associated with IGP or static routes).
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* value varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* value varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
AS-path	AS_Path attribute, with **Nil** indicating that the attribute value is null.
origin	Origin attribute of a BGP route. The value can be: ● IGP: If a route is added to the BGP routing table using the **network** command, its origin is IGP. ● EGP: indicates that the route is obtained through EGP. ● Incomplete: indicates that the origin of the route is unknown. For example, the origin attribute of the routes imported using the **import-route** command is Incomplete.
valid	Valid route.
external	External route.
best	Optimal route.
select	Preferred route.
pre	BGP route preference.

Display detailed information about a specified invalid BGP route.

```
<HUAWEI> display bgp routing-table 192.168.1.1
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   2 available, 0 best, 0 select
 BGP routing table entry information of 192.168.1.1/32:
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h01m31s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 172.16.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet
```

Table 7-168 Description of the **display bgp routing-table** command output

Item	Description
BGP local router ID	ID of the local BGP router. The format is the same as an IPv4 address.
Local AS number	Local AS number.
Paths	Information about paths of BGP routes.
BGP routing table entry information of 192.168.1.1/32	The following information is about the route to 192.168.1.1/32.
From	IP address of the device that advertises the route.
Route Duration	Route duration.
Relay IP Nexthop	IP address of the recursive next hop.
Relay IP Out-Interface	Outbound interface obtained when the route recurses to another route.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* value varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* value varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.

Item	Description
AS-path 200	AS_Path attribute.
origin incomplete	Origin attribute of a route. The value can be: - IGP: If a route is added to the BGP routing table using the **network (BGP)** command, its origin is IGP. - EGP: indicates that the route is obtained through EGP. - Incomplete: indicates that the origin of the route is unknown. For example, the origin of the routes that are added to the BGP routing table using the **import-route (BGP)** command is Incomplete.
MED	MED of a route.
localpref	Local preference.
pref-val	Preferred value (PrefVal).
internal	Internal route.
pre 255	The BGP route preference is 255.
invalid for IP unreachable	Reason why a route is invalid: - invalid for route-policy not pass: The route does not match the route-policy. - invalid for supernet route: The route is a supernet route. - invalid for IP unreachable: The route fails to recurse to another route. - invalid for supernet route not advertise: No supernet routes are advertised. - invalid for supernet label route not advertise: No supernet labeled routes are advertised. - invalid for next-hop unreachable: The next-hop IP address is unreachable. - invalid for tunnel unreachable: The route fails to recurse to a tunnel.
Not advertised to any peer yet	Flag indicating that the BGP route has not been advertised to any peer yet.

7.8.64 display bgp routing-table dampened

Function

The **display bgp routing-table dampened** command displays BGP dampened routes.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table** [**statistics**] **dampened**

display bgp ipv6 routing-table [**statistics**] **dampened**

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table** [**statistics**] **dampened** (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table** [**statistics**] **dampened** (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
vpnv4	Displays the BGP routes of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
statistics	Displays the statistics of dampened routes.	-
ipv6	Displays all dampened IPv6 routes.	-
vpnv6	Displays the BGP routes of a VPNv6 instance.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the Route Distinguisher dampened BGP routes.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed after the command is run.

Example

Display BGP dampened routes.

```
<HUAWEI> display bgp routing-table dampened

 BGP Local router ID is 10.1.41.102
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 8
     Network            From              Reuse     Path/Origin
  d  10.6.244.0/23      10.10.41.247      01:06:25  65534 4837 174 11096 6356i
  d  10.17.79.0/24      10.10.41.247      01:06:25  65534 837 3356 23504 29777i
  d  10.17.110.0/24     10.10.41.247      01:06:25  65534 837 3356 23504 29777i
  d  10.57.144.0/20     10.10.41.247      01:06:25  65534 4837 10026 9924 18429,18429i
  d  10.76.216.0/24     10.10.41.247      01:06:25  65534 4837 701 26959i
  d  10.78.142.0/24     10.10.41.247      01:06:25  65534 4837 701 26959i
  d  10.115.136.0/23    10.10.41.247      01:06:25  65534 4837 701 26956i
  d  10.243.170.0/24    10.10.41.247      01:06:25  65534 4837 701 26959i
```

Table 7-169 Description of the display bgp routing-table dampened command output

Item	Description
Network	Indicates the network address in the BGP routing table.
From	Indicates the IP address of the peer that receives the routes.
Reuse	Indicates the reuse value (in seconds).
Path/Origin	Indicates the AS_Path number and the Origin attribute.

Display IPv6 dampened routes in the BGP routing table.

```
<HUAWEI> display bgp ipv6 routing-table dampened



 BGP Local router ID is 10.0.0.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale,
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 4
  d  Network : FC00:0:0:1:1::                          PrefixLen : 48
     From    : FC00:0:0:1::2:2                        Reuse     : 01:06:26
     Path/Ogn: 65001?

  d  Network : FC00:0:0:1:2::                          PrefixLen : 48
     From    : FC00:0:0:1::2:2                        Reuse     : 01:06:26
     Path/Ogn: 65001?

  d  Network : FC00:0:0:1:3::                          PrefixLen : 48
     From    : FC00:0:0:1::2:2                        Reuse     : 01:06:26
     Path/Ogn: 65001?

  d  Network : FC00:0:0:1:4::                          PrefixLen : 48
```

```
    From    : FC00:0:0:1::2:2                    Reuse      : 01:06:26
    Path/Ogn: 65001?
```

Table 7-170 Description of the **display bgp ipv6 routing-table dampened** command output

Item	Description
PrefixLen	Prefix length

7.8.65 display bgp routing-table dampening parameter

Function

The **display bgp routing-table dampening parameter** command displays configured BGP route dampening parameters.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table dampening parameter**

display bgp ipv6 routing-table dampening parameter

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table dampening parameter** (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 all routing-table dampening parameter (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
vpnv4	Displays the BGP route dampening parameters of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ipv6	Displays configured BGP4+ route dampening parameters.	-
vpnv6	Displays the BGP route dampening parameters of a VPNv6 instance.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp routing-table dampening parameter** command to check configured BGP route dampening parameters.

Example

Display BGP route dampening parameters.

```
<HUAWEI> display bgp routing-table dampening parameter
 Maximum Suppress Time(in second) : 3973
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in  second)        : 900
 Suppress-Limit                   : 2000
```

Table 7-171 Description of the display bgp routing-table dampening parameter command output

Item	Description
Maximum Suppress Time (in second)	Maximum time taken for route suppression, in seconds.
Ceiling Value	Penalty ceiling.
Reuse Value	Threshold for a route to be unsuppressed.
HalfLife Time(in second)	Half life of a reachable route, in seconds.
Suppress-Limit	Threshold for a route to be suppressed.

Display BGP4+ route dampening parameters.

```
<HUAWEI> display bgp ipv6 routing-table dampening parameter
 Maximum Suppress Time(in second) : 3069
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in  second)        : 900
 Suppress-Limit                   : 2000
```

7.8.66 display bgp routing-table flap-info

Function

The **display bgp routing-table flap-info** command displays statistics about BGP route flapping.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table flap-info** [**regular-expression** *as-regular-expression*]

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table flap-info** { **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [{ *mask* | *mask-length* } [**longer-match**]] }

display bgp ipv6 routing-table flap-info [**regular-expression** *as-regular-expression*]

display bgp ipv6 routing-table flap-info { **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*prefix-length* [**longer-match**]] }

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table flap-info** [**regular-expression** *as-regular-expression*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table flap-info** { **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*prefix-length* [**longer-match**]] } (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table flap-info** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *ipv4-address* [{ *mask* | *mask-length* } [**longer-match**]]] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table flap-info** [**regular-expression** *as-regular-expression*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
vpnv4	Displays statistics about route flapping of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
regular-expression *as-regular-expression*	Displays statistics about the flapping routes that match the AS_Path regular expression.	The value is a string of 1 to 80 characters.
as-path-filter *as-path-filter-number*	Specifies the number of an AS_Path filter.	It is an integer that ranges from 1 to 256.

Parameter	Description	Value
as-path-filter *as-path-filter-name*	Specifies the name of an AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
network-address	Specifies the network address related to dampened routes.	-
mask	Specifies the network mask.	It is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
longer-match	Matches a route with a longer prefix.	-
prefix-length	Specifies the prefix length.	The value is an integer that ranges from 0 to 128.
vpnv6	Displays statistics about route flapping of a VPNv6 instance.	-
ipv4-address	Displays statistics about the flapping routes that match the IPv4 prefix.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the Route Distinguisher dampened BGP routes.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp routing-table flap-info** command to check statistics about BGP route flapping.

Example

Display statistics about BGP route flapping.

```
<HUAWEI> display bgp routing-table flap-info


 BGP Local router ID is 10.20.200.201
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed,
               Origin codes: i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
     Network          From             Flaps  Duration      Reuse  Path/Ogn

 d  10.1.1.0         10.20.200.200    5      00:00:36  00:40:47  600i
 *>  10.1.1.0         10.20.200.202   1      00:04:07             100?
 d  10.1.2.0         10.20.200.200    5      00:00:36  00:40:47  600i
 *>  10.1.2.0         10.20.200.202   1      00:04:07             100?
 d  10.1.3.0         10.20.200.200    5      00:00:36  00:40:47  600i
 d  10.1.4.0         10.20.200.200    5      00:00:36  00:40:47  600i
 d  10.1.5.0         10.20.200.200    5      00:00:36  00:40:47  600i
```

Table 7-172 Description of the display bgp routing-table flap command output

Item	Description
Network	Network address in the BGP routing table.
From	IP address of the peer that receives the routes.
Flaps	Total number of times of route flapping.
Duration	Total time length of flapping.
Reuse	Reuse value.
Path/Ogn	AS_Path number and Origin attribute.

Display statistics about BGP4+ route flapping.

```
<HUAWEI> display bgp ipv6 routing-table flap-info


 BGP Local router ID is 10.53.53.53
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 3
  d  Network : FC00:0:0:1::                          PrefixLen : 96
     From    : FC00:0:0:1::1                       Flaps     : 8
     Duration: 00:02:11                            Reuse     : 00:49:21
     Path/Ogn: 100?

  d  Network : FC00:0:0:2::2                          PrefixLen : 128
```

```
   From    : FC00:0:0:1::1                    Flaps     : 5
   Duration: 00:00:18                          Reuse     : 00:41:06
   Path/Ogn: 100?

d  Network : FC00:0:0:2::3                     PrefixLen : 128
   From    : FC00:0:0:1::1                    Flaps     : 5
   Duration: 00:00:18                          Reuse     : 00:41:06
   Path/Ogn: 100?
```

7.8.67 display bgp routing-table label

Function

The **display bgp routing-table label** command displays labeled routes in the BGP routing table.

Product	Support
S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5731-S, S5731S-S, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table label include-mask**

display bgp routing-table label [**statistics** | **include-mask**]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [**statistics**] **label**

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [**statistics**] **label**

display bgp ipv6 routing-table [**statistics**] **label**

Parameters

Parameter	Description	Value
include-mask	Displays labeled routes carrying masks.	-

Parameter	Description	Value
statistics	Indicates statistics about labeled routes.	-
vpnv4	Displays VPNv4 labeled routes.	-
all	Displays the labeled routes of all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ipv6	Displays BGP4+ labeled routes.	-
vpnv6	Displays VPNv6 labeled routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp routing-table label** command to check labeled routes in the BGP routing table.

Example

Display BGP labeled routes of all VPN instances.

```
<HUAWEI> display bgp vpnv4 all routing-table label
 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 3
 Route Distinguisher: 100:1

        Network           NextHop           In/Out Label
 *>i    10.22.22.22       10.3.3.9          NULL/1036

 Route Distinguisher: 100:4

        Network           NextHop           In/Out Label
 *>     10.1.2.0          10.1.2.1          1037/NULL
 *>     10.11.11.11       127.0.0.1         1038/NULL

 VPN-Instance vpn1, router ID 1.1.1.9:
 Total Number of Routes: 1
```

```
      Network          NextHop          In/Out Label
*>i    10.22.22.22       10.3.3.9         NULL/1036

 VPN-Instance vpn2, router ID 10.1.1.9:
 Total Number of Routes: 0
```

Table 7-173 Description of the display bgp vpnv4 all routing-table label command output

Item	Description
Network	Network address in the BGP routing table.
NextHop	IP address of the reachable next hop.
In/Out Label	Incoming label and outgoing label.

Display BGP4+ labeled routes.

```
<HUAWEI> display bgp ipv6 routing-table label
Total Number of Routes: 3

  Network        Prefix     NextHop          Label
  FC00:0:0:1::4  128        FC00:0:0:2::2     1024
  FC00:0:0:1::5  128        FC00:0:0:2::2     1025
  FC00:0:0:1::6  128        FC00:0:0:2::2     1026
```

Table 7-174 Description of the display bgp ipv6 routing-table label command output

Item	Description
Prefix	IP prefix.

7.8.68 display bgp routing-table peer no-advertise

Function

The **display bgp routing-table peer no-advertise** command displays the routes that a device is prevented from advertising to a specified peer in different address families.

Format

display bgp routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp ipv6 routing-table peer *ipv6-address* **no-advertise** *ipv6–network* [*prefix-length*]

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp vpnv4 all routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*] (supported only by the S5731-H, S5731S-H, S5731-S,

S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp ipv6 routing-table peer *ipv4-address* **no-advertise** *ipv6–network* [*prefix-length*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp multicast routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv6 all routing-table peer *ipv4-address* **no-advertise** *ipv6–network* [*prefix-length*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* **no-advertise** *ipv6–network* [*prefix-length*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp l2vpn-ad routing-table peer *ipv4-address* **no-advertise** *network* (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
peer *ipv4-address*	Displays the routes that a device is prevented from advertising to the specified IPv4 peer.	The value is in dotted decimal notation.
network	Displays the routes with the specified destination IPv4 address that are prevented from being advertised.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the specified IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the subnet mask length of the specified IPv4 address.	The value is an integer that ranges from 0 to 32.
vpnv4	Displays the routes that a device is prevented from advertising to a specified peer in the VPNv4 address family.	-

Parameter	Description	Value
all	Displays the routes that a device is prevented from advertising to a specified peer in all VPN instances of the current address family.	-
vpn-instance *vpn-instance-name*	Displays the routes that a device is prevented from advertising to a specified peer in the specified VPN instance of the current address family.	The value must be an existing VPN instance name.
multicast	Displays the routes that a device is prevented from advertising to a specified peer in the IPv4 multicast address family.	-
ipv6	Displays the routes that a device is prevented from advertising to a specified peer in the IPv6 unicast address family.	-
peer *ipv6-address*	Displays the routes that a device is prevented from advertising to the specified IPv6 peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv6–network	Displays the routes with the specified destination IPv6 address that are prevented from being advertised.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
vpnv6	Displays the routes that a device is prevented from advertising to a specified peer in the VPNv6 address family.	-
l2vpn-ad	Displays the routes that a device is prevented from advertising to a specified peer in the L2VPN-AD address family.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the routes that a device is prevented from advertising to a specified peer in different address families, run the **display bgp routing-table peer no-advertise** command. The command output also includes the reasons why the routes are not advertised.

You can specify an address family to check the routes that a device is prevented from advertising to a specified peer in the address family. If you do not specify any address family, the command output shows the routes that a device is prevented from advertising to a specified peer in the IPv4 unicast address family.

Example

Display the route 10.3.3.4/32 that a device is prevented from advertising to peer with IP address 192.168.1.1 in the IPv4 unicast address family.

```
<HUAWEI> display bgp routing-table peer 192.168.1.1 no-advertise 10.3.3.4 32
 BGP routing table entry information of 10.3.3.4/32:
 From: 192.168.1.1 (10.1.1.1)
 Route Duration: 22h36m17s
 Relay IP Nexthop: 10.1.1.1
 Relay IP Out-Interface: Vlanif100
 Original nexthop: 192.168.1.1
 Qos information : 0x0
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, active, pre 255,
IGP cost 1
 No advertise without config reflect-client
```

Table 7-175 Description of the **display bgp routing-table peer no-advertise** command output

Item	Description
From	Peer from which the route was received.
Route Duration	Duration of the route.
Relay IP Nexthop	Next-hop IP address to which the route recurses.
Relay IP Out-Interface	Outbound interface to which the route recurses.
Original nexthop	Original next-hop IP address of the route.

Item	Description
Qos information	QoS information. - 0x20000000: indicates that the **apply behavior** command has been run. - 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. - 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. - 0x0: indicates that the preceding QoS configurations are not performed.
AS-path	AS_Path attribute. **Nil** indicates that the attribute value is null.
origin	Origin attribute: - IGP: indicates that the route is added to the BGP routing table using the **network (BGP)** command. - EGP: indicates that the route is learned through the EGP protocol. - Incomplete: indicates that the origin of the route cannot be identified. For example, if a route is imported using the **import-route (BGP)** command, its origin is **Incomplete**.
MED	MED of the route.
localpref	Local_Pref of the BGP route.
pref-val	PrefVal of the route.
valid	Valid route.
internal	Internal route.
best	Optimal route.
select	Selected route.
active	Active route.
pre 255	Priority of the route (255 in this example).
IGP cost 1	IGP cost of the route (1 in this example).

Item	Description
No advertise without config reflect-client	Reason why the route is not advertised: - No advertise with no-adv flag: The route carries the No-Advertise flag. - No advertise with peer default-route-advertise in vt family: The local device is configured to advertise only default routes to the peer in the VT address family. - No advertise with no-adv flag in community attr: The route carries the No-Advertise community attribute. - No advertise with no-export flag in community attr: The route carries the No-Export community attribute. - No advertise with no-export-subconfed flag in community attr: The route carries the No_Export_Subconfed community attribute. - No advertise by detail route with config aggregate: Specific routes for summarization are not advertised. - No advertise with config active-route-advertise: Only the active routes in the IP routing table are advertised. - No advertise with config peer upe and no export policy: The specified peer is a UPE, and the route fails to match the export policy. - No advertise without config reflect-client: No RR is configured. - No advertise with config reflect-client but without config reflect between-clients: Route reflection among RR clients is disabled. - No advertise for other reason: Other reasons prevent the route from being advertised.

7.8.69 display bgp routing-table peer statistics

Function

The **display bgp routing-table peer statistics** command displays statistics about received and advertised BGP routes.

Format

display bgp [**multicast** | **ipv6**] **routing-table peer statistics**

display bgp [**l2vpn** | **vpls** | **l2vpn-ad**] **routing-table peer statistics**

display bgp { **vpnv4** | **vpnv6** } { **all** | **vpn-instance** *vpn-instance-name* } **routing-table peer statistics**

display bgp l2vpn-ad routing-table [**all** | **vpls-ad** | **vpws** | **vpls**] **peer statistics**

NOTE

The **l2vpn**, **l2vpn-ad**, **vpls**, **vpls-ad**, **vpnv4**, and **vpnv6** parameters are supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H.

Parameters

Parameter	Description	Value
multicast	Displays statistics about routes in the IP multicast routing table.	-
l2vpn	Displays statistics about routes in the BGP-L2VPN address family.	-
vpls	Displays statistics about routes in the BGP VPLS address family.	-
ipv6	Displays statistics about routes in the BGP IPv6 unicast address family.	-
l2vpn-ad	Displays statistics about routes in the BGP L2VPN-AD address family.	-
vpnv4	Displays statistics about routes in the BGP-VPNv4 address family.	-
vpnv6	Displays statistics about routes in the BGP-VPNv6 address family.	-
all	Displays statistics about all types of routes.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.
vpls-ad	Displays statistics about VPLS-AD routes.	-

Parameter	Description	Value
vpws	Displays statistics about virtual private wire service (VPWS) routes.	-
vpls	Displays statistics about virtual private LAN service (VPLS) routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check statistics of received and advertised BGP routes, run the **display bgp routing-table peer statistics** command. You can specify parameters as needed. If no parameter is specified in the command, statistics about BGP IPv4 unicast routes are displayed.

Example

Display statistics about received and advertised BGP IPv4 unicast routes.

```
<HUAWEI> display bgp routing-table peer statistics
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Total number of peers : 3              Number of Peers in established state : 3

  Peer                  Received routes           Advertised routes

  10.2.2.2                1                      1
  10.2.2.3                1                      1
  10.3.3.3                2                      0
```

Table 7-176 Description of the **display bgp routing-table peer statistics** command output

Item	Description
BGP local router ID	Local router ID
Local AS number	AS number
Total number of peers	Total number of peers
Number of Peers in established state	Number of peers in the established state
Peer	IP address of a peer

Item	Description
Received routes	Total number of routes received from the peer
Advertised routes	Total number of routes advertised to the peer

7.8.70 display bgp routing-table statistics

Function

The **display bgp routing-table statistics** command displays statistics about BGP routes.

Format

display bgp routing-table statistics

display bgp routing-table statistics as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

display bgp routing-table statistics cidr

display bgp routing-table statistics community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp routing-table statistics community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp routing-table statistics dampened

display bgp routing-table statistics different-origin-as

display bgp routing-table statistics regular-expression *as-regular-expression*

display bgp routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
as-path-filter *as-path-filter-number*	Displays the routes that match an AS-Path filter with the specified number.	It is an integer that ranges from 1 to 256.

Parameter	Description	Value
as-path-filter *as-path-filter-name*	Displays the routes that match an AS-Path filter with the specified name.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
cidr	Displays CIDR information.	-
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
aa:*nn*	Specifies the community attribute number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the matching routes that can be sent to any peer.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.

Parameter	Description	Value
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.
dampened	Displays the statistics of BGP dampened roues.	-
different-origin-as	Displays routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
peer *ipv4-address*	Displays the routing information for the specified BGP peer.	It is in dotted decimal notation.
advertised-routes	Displays the routes advertised to the specified peer.	-
received-routes	Displays the routes received from the specified peer.	-
active	Specifies the number of active routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bgp routing-table statistics** command is used to display statistics about BGP routes on the public network.

The **display bgp routing-table statistics as-path-filter** command is used to display statistics about the BGP routes that match the specified AS_Path filter on the public network.

The **display bgp routing-table statistics cidr** command is used to display statistics about the BGP CIDR information of the public network.

The **display bgp routing-table statistics community** command is used to display statistics about the BGP routes carrying the specified community attribute on the public network.

The **display bgp routing-table statistics community-filter** command is used to display statistics about the BGP routes that match the specified community filter on the public network.

The **display bgp routing-table statistics dampened** command is used to display statistics about BGP dampened routes on the public network.

The **display bgp routing-table statistics different-origin-as** command is used to display statistics about the BGP routes with the same destination address but different source AS numbers on the public network.

The **display bgp routing-table statistics regular-expression** command is used to display statistics about the BGP routes whose AS_Path information matches the AS_Path regular expression on the public network.

Example

Display route statistics.

```
<HUAWEI> display bgp routing-table statistics
 Total Number of Routes: 4
```

Table 7-177 Description of the display bgp routing-table statistics command output

Item	Description
Total Number of Routes	Total number of routes in the routing table

7.8.71 display bgp update-peer-group

Function

The **display bgp update-group** command displays information about update-groups. By setting **index** in the command displays detailed information about a specified update-group. If no address family is specified, information about the update-group of the IPv4 unicast address family is displayed by default.

Format

display bgp update-peer-group [**index** *update-group-index*]

display bgp ipv6 update-peer-group [**index** *update-group-index*]

display bgp vpnv4 all update-peer-group [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **update-peer-group** [**index** *update-group-index*]

display bgp vpnv6 all update-peer-group [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv6 vpn-instance *vpn-instance-name* **update-peer-group** [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp l2vpn all update-peer-group [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpls all update-peer-group [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp l2vpn-ad update-peer-group [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp { **mdt** | **mvpn** } **all update-peer-group** [**index** *update-group-index*] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
index *update-group-index*	Specifies the index of an update-group.	The value is an integer that ranges from 0 to 65535.
ipv6	Displays information about the BGP update-groups of IPv6 routes.	-
vpnv4	Displays information about the BGP update-groups of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
vpnv6	Displays information about the BGP update-groups of a VPNv6 instance.	-

Parameter	Description	Value
all	Displays information about all the update-groups in a VPNv6 address family.	-
l2vpn	Displays information about L2VPN BGP update-groups.	-
vpls	Displays information about VPLS BGP update-groups.	-
l2vpn-ad	Displays information about L2VPN-AD BGP update-groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify the index of an update-group to view detailed information about the specified update-group. If no address family is specified, information about the update peer-groups in the IPv4 unicast address family is displayed by default.

Example

Display information about the update peer-groups in the IPv4 unicast address family.

```
<HUAWEI> display bgp update-peer-group
 The Public instance's update peer group number : 1
 Keep buffer update peer group number : 0
 BGP Version : 4
 Group ID : 0
 Group Type : external
 Addr Family : IPv4-UNC
 AdvMinTimeVal : 30
 Total Peers : 1
 Leader Peer : 192.168.1.2
 Peers List : 192.168.1.2
```

Table 7-178 Description of the display bgp update-peer-group command output

Item	Description
The Public instance's update peer group number	Number of update-groups in the instance

Item	Description
Keep buffer update peer group number	Number of packets in update-groups saved in the batch buffer
BGP Version	Indicates the BGP version.
Group ID	Indicates the ID of the update-group.
Group Type	Indicates the type of the update-group, which can be one of the following: ● external: indicates that this is an EBGP peer group. ● internal: indicates that this is an IBGP peer group. ● unknown: indicates that the type is unknown.
Addr Family	Indicates the address family.
AdvMinTimeVal	Indicates the minimum interval for sending Update packets with the same route prefix.
Total Peers	Indicates the total number of peers in an update-group.
Leader Peer	Indicates the representative of an update-group.
Peers List	Indicates a list of peers.

Display information about the update-group with a specified index.

```
<HUAWEI> display bgp update-peer-group index 0
 Group ID : 0
 BGP Version : 4
 Group Type : external
 Addr Family : IPv4-UNC
 AdvMinTimeVal : 30
 Total Peers : 1
  Leader Peer : 192.168.1.2

 Total format packet number : 3
 Total send packet number : 3
 Total replicate packet number : 0
 The replication percentages(%) : 0

 Peers List : 192.168.1.2
```

Table 7-179 Description of the display bgp update-peer-group index command output

Item	Description
Total format packet number	Indicates the total number of formatted packets.
Total send packet number	Indicates the total number of sent packets.

Item	Description
Total replicate packet number	Indicates the total number of replicate packets, which equals the total number of sent packets minus the total number of formatted packets.
The replication percentages(%)	Indicates the replication percentage, which is obtained with the formula: (Total number of sent packets - Total number of formatted packets) x 100/Total number of formatted packets.

7.8.72 display bgp vpnv4 brief

Function

The **display bgp vpnv4 brief** command displays brief information about VPNv4 and VPN instances (IPv4 address family).

Format

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **brief**

Parameters

Parameter	Description	Value
all	Displays information about all VPNv4 and VPN instances (IPv4 address family).	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **display bgp vpnv4 brief** command is used to display information about VPNv4 and VPN instances (IPv4 address family), the VPN instances are displayed and arranged alphabetically by name.

Example

Display brief information about VPNv4 instances and all VPN instances (IPv4 address family).

```
<HUAWEI> display bgp vpnv4 all brief

VPNV4 :
 Rd Num            Peer Num           Route Num
 0              1              0

VPN-Instance(IPv4-family):
 VPN-Instance Name   Peer Num            Route Num
 vrf0              0              0
 vrf1              0              0
 vrf11              0              0
 vrf12              0              0
 vrf13              0              0
 vrf14              0              0
 vrf2              0              20
 vrf3              0              20
 vrf4              0              24
 vrf5              0              24
 vrf6              0              0
 vrf7              0              0
 vrf8              0              20
```

Table 7-180 Description of the display bgp vpnv4 brief command output

Item	Description
Rd Num	Indicates the number of RDs.
Peer Num	Indicates the number of peers.
Route Num	Indicates the number of routes.
VPN-Instance Name	Indicates the name of a VPN instance.

7.8.73 display bgp vpnv4 routing-table

Function

The **display bgp vpnv4 routing-table** command displays BGP routes of VPNv4 address family and the private networks.

Format

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table regular-expression** *as-regular-expression* (supported only by the S5731-H,

S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table regular-expression** *as-regular-expression*

display bgp vpnv4 route-distinguisher *route-distinguisher* **routing-table** [**verbose** | *ipv4-address* [*mask* | *mask-length*]] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [**verbose** | *ipv4-address* [*mask* [**longer-prefixes**] | *mask-length* [**longer-prefixes**]]]

display bgp vpnv4 all routing-table peer *ipv4-address* { **advertised-routes** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] } (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* { **advertised-routes** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] }

display bgp vpnv4 all routing-table peer *ipv4-address* **received-routes** *network* [{ *mask* | *mask-length* } [**longer-prefixes**]] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* **received-routes** *network* [{ *mask* | *mask-length* } [**longer-prefixes** | **original-attributes**]]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* } (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* **accepted-routes**

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time* (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table time-range** *start-time end-time*

Parameters

Parameter	Description	Value
all	Displays all BGP VPNv4 routes.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the BGP routes with the specified RD.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Displays the BGP routes of a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
cidr	Displays CIDR information.	-
different-origin-as	Displays the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
verbose	Displays detailed information about BGP VPNv4 routes.	-
ipv4-address	Specifies the destination address.	-
mask	Specifies a mask in dotted decimal notation.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
peer *ipv4-address*	Displays routes of a specified peer.	-
advertised-routes	Displays the routes advertised to a specified peer.	-

Parameter	Description	Value
network	Specifies the IPv4 network address.	The value is in dotted decimal notation.
longer-prefixes	Matches any route whose prefix mask is longer than the specified length.	-
received-routes	Displays the routes received from a specified peer.	-
active	Displays the active routes received from a specified peer.	-
original-attributes	Displays the original attributes of a BGP route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
whole-match	Indicates exact matching.	-
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-

Parameter	Description	Value
community-number	Specifies the number of a community.	-
aa:*nn*	Specifies the community number. A maximum of 29 community numbers can be set.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the matching routes that can be sent to any peer.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
accepted-routes	Displays the routes that are received from a neighbor and accepted by a routing policy.	-
time-range *start-time end-time*	Displays information about BGP VPNv4 routes that have undergone status flapping during the specified period. For example, when *start-time* is set to 0d0h5m0s and *end-time* is set to 0d0h10m0s, information about all BGP VPNv4 routes whose lifetime ranges from 5 to 10 minutes is displayed.	In the values of *start-time* and *end-time*, d ranges from 0 to 10000, h ranges from 0 to 23, m ranges from 0 to 59, and s ranges from 0 to 59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

When BGP routing table is displayed, if the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed.

You can run the **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time* command to view BGP VPNv4 routes that flap within the specified time period. For example, if service traffic is abnormal or CPU usage of the device remains high within a certain time period, you can run this command to check whether route flapping occurs within the specified time period. The faulty route can be viewed in the command output, facilitating fault location.

Example

Display all the BGP routing information of the VPN instance named vpn1.

```
<HUAWEI> display bgp vpnv4 vpn-instance vpn1 routing-table

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1, Router ID 10.1.1.9:

 Total Number of Routes: 4
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   10.1.2.0/24        0.0.0.0         0                     0      ?
 *>   10.1.2.1/32        0.0.0.0         0                     0      ?
 *>   10.11.11.11/32     0.0.0.0         0                     0      ?
 *>i  10.22.22.22/32     10.3.3.9        0          100        0      ?
```

Display all the BGP VPNv4 routing information.

```
<HUAWEI> display bgp vpnv4 all routing-table


 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete



 Total number of routes from all PE: 4
 Route Distinguisher: 100:1


      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  10.22.22.22/32     10.3.3.9        0          100        0      ?

 Route Distinguisher: 100:4

```

```
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.2.0/24        0.0.0.0         0                    0      ?
*>   10.1.2.1/32        0.0.0.0         0                    0      ?
*>   10.11.11.11/32     0.0.0.0         0                    0      ?

 VPN-Instance vpn1, Router ID 10.1.1.9:

 Total Number of Routes: 4
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.2.0/24        0.0.0.0         0                    0      ?
*>   10.1.2.1/32        0.0.0.0         0                    0      ?
*>   10.11.11.11/32     0.0.0.0         0                    0      ?
*>i  10.22.22.22/32     10.3.3.9        0          100       0      ?
```

Display the VPNv4 routing information of the specified RD.

```
<HUAWEI> display bgp vpnv4 route-distinguisher 100:1 routing-table

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1


 Total Number of Routes: 3
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.1.0/24        0.0.0.0         0                    0      ?
*                       10.1.1.1        0                    0      65410?
*>   10.1.1.2/32        0.0.0.0         0                    0      ?

 VPN-Instance vpna, Router ID 10.1.1.9:

 Total Number of Routes: 7
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.1.0/24        0.0.0.0         0                    0      ?
                        10.1.1.1        0                    0      65410?
*>   10.1.1.2/32        0.0.0.0         0                    0      ?
*>   10.2.1.0/24        10.2.1.2        0                    0      ?
* i                     10.3.3.9        0          100       0      ?
*>   10.2.1.2/32        127.0.0.1       0                    0      ?
*>i  10.4.1.0/24        10.4.4.9        0          100       0      ?
```

Display all BGP VPNv4 routes of community 1000:100.

```
<HUAWEI> display bgp vpnv4 all routing-table community 1000:100

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total number of routes from all PE: 1

 Route Distinguisher: 100:1


     Network            NextHop        MED        LocPrf    PrefVal Community

*>i  10.22.22.22/32     10.3.3.9        0          100       0      <1000:100>

 VPN-Instance vpn1, Router ID 10.1.1.9:

 Total Number of Routes: 1
```

```
     Network            NextHop        MED        LocPrf    PrefVal Community

*>i  10.22.22.22/32     10.3.3.9       0          100       0      <1000:100>

VPN-Instance vpn2, Router ID 10.1.1.9:

Total Number of Routes: 0
```

Displays BGP VPNv4 routes that flap within the specified time period.

```
<HUAWEI> display bgp vpnv4 all routing-table time-range 0d5h0m0s 1d5h0m0s

 BGP Local router ID is 192.168.1.250
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Route Distinguisher: 2:2

     Network            NextHop         Peer            Duration        Path/Ogn

 *>i  0.0.0.0           10.2.2.2        10.2.2.2        05h30m11s       i
 *>   10.2.3.4/32        0.0.0.0         0.0.0.0         05h30m42s       ?

 VPN-Instance 1, Router ID 192.168.1.250:
     Network            NextHop         Peer            Duration        Path/Ogn

 *>   10.2.3.4/32        0.0.0.0         0.0.0.0         05h30m42s       ?

 VPN-Instance 2, Router ID 192.168.1.250:
     Network            NextHop         Peer            Duration        Path/Ogn

 *>i  0.0.0.0           10.2.2.2        10.2.2.2        05h30m11s       i
 *>   10.2.3.4/32        0.0.0.0         0.0.0.0         05h30m42s       ?
```

Table 7-181 Description of the display bgp vpnv4 routing-table command output

Item	Description
BGP Local router ID	ID of the local BGP device.
Network	Network address in the BGP routing table.
NextHop	Next Hop address through which the packet has to be sent
MED	MED of the route.
LocPrf	Local preference.
PrefVal	Preferred value.
Peer	Peer IP address
Duration	Route duration
Path/Ogn	AS_Path number and the origin attribute.
Community	Community attribute information.

Display information about a specified VPNv4 route.

```
<HUAWEI> display bgp vpnv4 all routing-table 192.168.2.0


 BGP local router ID : 10.2.2.9
 Local AS number : 100

 Total routes of Route Distinguisher(100:10): 2
 BGP routing table entry information of 192.168.2.0/24:
 Imported route.
 Label information (Received/Applied): NULL/1025
 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 00h50m09s
 Direct Out-interface: Vlanif30
 Original nexthop: 192.168.2.1
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select,
pre 255
 Advertised to such 1 peers:
    10.3.3.3
 BGP routing table entry information of 192.168.2.0/24:
 From: 192.168.2.2 (1.1.1.1)
 Route Duration: 00h48m50s
 Direct Out-interface: Vlanif30
 Original nexthop: 192.168.2.2
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path 10, origin incomplete, MED 0, pref-val 0, valid, external, pre 255, not
 preferred for route type
 Not advertised to any peer yet


 VPN-Instance vpna, Router ID 10.2.2.9:

 Total Number of Routes: 2
 BGP routing table entry information of 192.168.2.0/24:
 Imported route.
 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 00h50m09s
 Direct Out-interface: Vlanif30
 Original nexthop: 192.168.2.1
 Qos information : 0x0
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select,
pre 0
 Advertised to such 1 peers:
    192.168.2.2
 BGP routing table entry information of 192.168.2.0/24:
 From: 192.168.2.2 (1.1.1.1)
 Route Duration: 00h48m51s
 Direct Out-interface: Vlanif30
 Original nexthop: 192.168.2.2
 Qos information : 0x0
 AS-path 10, origin incomplete, MED 0, pref-val 0, external, pre 255
 Not advertised to any peer yet
```

Table 7-182 Description of the display bgp vpnv4 routing-table command output

Item	Description
Local AS number	Local AS number.
Total routes of Route Distinguisher	Total number of VPNv4 routes with a specified RD.

Item	Description
BGP routing table entry information of x.x.x.x/x	The following information is about a specified BGP routing entry.
Imported route	Routes imported to BGP using the **import-route** command.
Label information (Received/ Applied)	Information about labels, including received and sent labels.
From	IP address of the route originator.
Route Duration	Route duration.
Direct Out-interface	Direct outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute of BGP.
AS-path	AS_Path attribute.
origin	Origin attribute of the BGP route. ● IGP: indicates that the origin attribute of a route added to the BGP routing table by using the **network** command is IGP. ● EGP: indicates that the origin attribute of a route obtained by using EGP is EGP. ● Incomplete: indicates that the origin attribute of a route whose source is unknown is Incomplete. For example, the origin attribute of the routes imported by using the **import-route** command is Incomplete.
pref-val	Preferred value.
valid	Valid BGP route.

Item	Description
external	The BGP route is learned from the EBGP peer.
best	The BGP route is the optimal route.
select	The BGP route is a preferred route.
pre 255	The preference of the BGP route is 255.
Advertised to such 1 peers	The BGP route has been advertised to one peer.
Not advertised to any peer yet	The BGP route has not been advertised to any peer.
VPN-Instance vpna, Router ID 10.2.2.9	The VPN instance is vpna, the Route ID is 10.2.2.9
Total Number of Routes	Number of routes in VPN instance vpna.

Display detailed information about the specified invalid BGP VPNv4 routes.

```
<HUAWEI> display bgp vpnv4 all routing-table 192.168.4.4
 BGP local router ID : 10.1.1.1
 Local AS number : 100

 Total routes of Route Distinguisher(10:10): 1
 BGP routing table entry information of 192.168.4.4/32:
 Label information (Received/Applied): 1025/NULL
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h12m26s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface: GigabitEthernet0/0/0
 Relay Tunnel Out-Interface:
 Relay token: 0x0
 Original nexthop: 10.1.1.2
 Qos information : 0x0
 Ext-Community:RT <10 : 10>, RT <20 : 20>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, pre 255
 Not advertised to any peer yet

 VPN-Instance vrf1, Router ID 10.1.1.1:

 Total Number of Routes: 1
 BGP routing table entry information of 192.168.4.4/32:
 Label information (Received/Applied): 1025/NULL
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h12m26s
 Relay Tunnel Out-Interface:
 Relay token: 0x0
 Original nexthop: 10.1.1.2
 Qos information : 0x0
 Ext-Community:RT <10 : 10>, RT <20 : 20>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for tunnel
unreachable
 Not advertised to any peer yet
```

Table 7-183 Description of the display bgp vpnv4 routing-table command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher(10:10)	Total number of BGP VPNv4 routes of the specified RD.
BGP routing table entry information of 192.168.4.4/32	The following information is about 192.168.4.4/32 routing entries.
Label information (Received/ Applied)	Label information (received or sent).
From	IP address of the device that sends the route. 10.1.1.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 10.1.1.2 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.
Relay Tunnel Out-Interface	Tunnel recursed outbound interface.
Relay token	Recursive token value used for MPLS forwarding, which is a part of tunnel ID and is assigned by the system.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
valid	The BGP route is a valid route.
internal	The BGP route is an internal route.
best	The BGP route is an optimal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.

Item	Description
invalid for tunnel unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to recurse to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to recurse to a tunnel.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.
VPN-Instance vrf1, Router ID 10.1.1.1	The local VPN instance is vrf1, and its router ID is 10.1.1.1.
Total Number of Routes	Total number of BGP VPNv4 routes that match 192.168.4.4/32 in VPN instance vrf1.

7.8.74 display bgp vpnv4 routing-table statistics

Function

The **display bgp vpnv4 routing-table statistics** command displays statistics about BGP VPNv4 routes.

Format

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table statistics**

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table statistics regular-expression** *as-regular-expression* (supported only by the S5731-

H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table statistics regular-expression** *as-regular-expression*

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table statistics community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table statistics community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* } (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table statistics dampened**

display bgp vpnv4 all routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics** (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
all	Displays all the statistics of BGP VPNv4 routes.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays statistics about the BGP routes with a specified RD.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Displays statistics about the BGP routes of a specified VPN instance.	The value must be an existing VPN instance name.
as-path-filter	Displays the routes that match the specified filter.	-

Parameter	Description	Value
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
cidr	Displays CIDR statistics.	-
different-origin-as	Displays statistics about the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
community	Displays statistics about the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
aa:*nn*	Specifies a community attribute value.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays statistics about the matching routes that can be sent to any peer.	-
no-advertise	Displays statistics about the BGP routes carrying the No-Advertise community attribute.	-

Parameter	Description	Value
no-export	Displays statistics about the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays statistics about the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays statistics about the routes that match a specified BGP community filter.	-
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community-filter-name	Specifies the name of a community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
dampened	Displays the statistics of BGP dampened routes.	-
active	Displays statistics about the routes that have the same destination address but different source AS numbers.	-
peer *ipv4-address*	Displays statistics about routes of a specified peer.	It is in dotted decimal notation.
advertised-routes	Displays statistics about the routes advertised to a specified peer.	-

Parameter	Description	Value
received-routes	Displays statistics about the routes received from a specified peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp vpnv4 routing-table statistics** command to check statistics about BGP VPNv4 routes.

Example

Display statistics about BGP VPNv4 routes.

```
<HUAWEI> display bgp vpnv4 all routing-table statistics

 Total number of routes from all PE: 2

 VPN-Instance vpn1, Router ID 10.1.1.9:

 Total Number of Routes: 2
```

Table 7-184 Description of the display bgp vpnv4 routing-table statistics command output

Item	Description
Total number of routes from all PE	Total number of VPNv4 routes
VPN-Instance vpn1	Indicating the name of VPN instance is vpn1.
Router ID 10.1.1.9	Indicating the router ID is 10.1.1.9.
Total Number of Routes	Total number of routes of the VPN instance.
Route Distinguisher	RD of the VPN instance IPv4 address family.

7.8.75 display bgp vpnv6 brief

Function

The **display bgp vpnv6 brief** command displays brief information about VPNv6 and VPN instances (IPv6 address family).

Product	Support
S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5731-S, S5731S-S, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **brief**

Parameters

Parameter	Description	Value
all	Displays information about all VPNv6 and VPN instances (IPv6 address family).	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPNv6 instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **display bgp vpnv6 brief** command is used to display information about VPNv6 and VPN instances (IPv6 address family), the VPN instances are displayed and arranged alphabetically by name.

Example

Display brief information about VPNv6 and VPN instances (IPv6 address family).

```
<HUAWEI> display bgp vpnv6 all brief
VPNV6:
  Rd Num              Peer Num            Route Num
    2                   1                   2

VPN-Instance(IPv6-family):
  VPN-Instance Name   Peer Num            Route Num
    vrf0                1                   2
    vrf1                0                   0
    vrf11               0                   0
    vrf12               0                   0
    vrf13               0                   0
    vrf14               0                   0
    vrf2                0                   20
    vrf3                0                   20
    vrf4                0                   24
    vrf5                0                   24
    vrf6                0                   0
```

Table 7-185 Description of the display bgp vpnv6 all brief command output

Item	Description
Rd Num	Number of RDs.
Peer Num	Number of peers.
Route Num	Number of routes.
VPN-Instance Name	Name of a VPN instance.

7.8.76 display bgp vpnv6 routing-table

Function

The **display bgp vpnv6 routing-table** command displays BGP VPNv6 routes.

Product	Support
S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5731-S, S5731S-S, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table** [**verbose** | *ipv6-address* [*prefix-length*]]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [**verbose** | *ipv6-address* [*prefix-length*]]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* | **route-distinguisher** *route-distinguisher* } **routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table different-origin-as**

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table different-origin-as**

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table regular-expression** *as-regular-expression*

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table regular-expression** *as-regular-expression*

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* { **advertised-routes** [*dest-ipv6-address* [*prefix-length*]] | **received-routes** [**active**] }

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* **received-routes** *dest-ipv6-address* [*prefix-length* [**original-attributes**]]

display bgp vpnv6 all routing-table peer *ipv4-address* **received-routes** *dest-ipv6-address* [*prefix-length*]

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* **accepted-routes**

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time*

display bgp vpnv6 all routing-table peer *ipv4-address* { **advertised-routes** [*dest-ipv6-address* [*prefix-length*]] | **received-routes** [**active**] }

Parameters

Parameter	Description	Value
all	Displays statistics about all BGP VPNv6 routes.	-
vpn-instance *vpn-instance-name*	Displays the BGP routes of a specified an IPv6 address family-enabled VPN instance on the local end.	The value must be an existing VPN instance name.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the BGP routes with the specified RD.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer to be displayed.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
verbose	Displays detailed information about BGP VPNv6 routes.	-
prefix-length	Specifies the prefix length of an IPv6 address.	-
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
aa:nn	Specifies the community number. A maximum of 29 community numbers can be set.	-
internet	Displays the BGP routes carrying the Internet community attribute.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-

Parameter	Description	Value
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	-
basic-community-filter-number	Specifies the number of a basic community filter.	-
advanced-community-filter-number	Specifies the number of an advanced community filter.	-
different-origin-as	Displays the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
peer *ipv6-address*	Displays the BGP routes of a specified peer.	-
ipv4-address	Specifies the IPv4 address of the peer.	The value is in dotted decimal notation.
advertised-routes	Displays the routes advertised to a specified peer.	-

Parameter	Description	Value
dest-ipv6–address	Specifies the destination IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
received-routes	Displays the routes received from a specified peer.	-
active	Displays the active routes received from a specified peer.	-
original-attributes	Displays the original attributes of a BGP route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
accepted-routes	Displays the routes that are received from a neighbor and accepted by a routing policy.	-
time-range *start-time end-time*	Displays information about BGP VPNv6 routes that have undergone status flapping during the specified period. For example, when *start-time* is set to 0d0h5m0s and *end-time* is set to 0d0h10m0s, information about all BGP VPNv6 routes whose lifetime ranges from 5 to 10 minutes is displayed.	In the values of *start-time* and *end-time*, d ranges from 0 to 10000, h ranges from 0 to 23, m ranges from 0 to 59, and s ranges from 0 to 59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about specified routes can be displayed by specifying different parameters.

To view information about BGP VPNv6 route flapping during a specified period, you can run the **display bgp vpnv6** { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time* command. When service traffic is abnormal during a period of time, you can run this command to check whether route flapping occurs. When the CPU usage is high during a period of time, you can run this command to check whether a large number of routes have undergone status flapping. This command allows you to find the flapping routes, which facilitates fault location.

Example

Display all BGP VPNv6 routes.

```
<HUAWEI> display bgp vpnv6 all routing-table


 BGP Local router ID is 10.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total number of routes from all PE: 3
 Route Distinguisher: 100:1


 *>i Network  : FC00:0:0:2001::                          PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                         LocPrf    :
     MED      : 0                                 PrefVal   : 0
     Label    : NULL
     Path/Ogn :  ?
 *>  Network  : FC00:0:0:2001::2                         PrefixLen : 128
     NextHop  : ::                                 LocPrf    :
     MED      : 0                                 PrefVal   : 0
     Label    : NULL
     Path/Ogn :  ?
 *>  Network  : FE80::                                   PrefixLen : 10
     NextHop  : ::                                 LocPrf    :
     MED      : 0                                 PrefVal   : 0
     Label    : NULL
     Path/Ogn :  ?

 VPN-Instance whm1, Router ID 10.4.4.4 :

 Total Number of Routes: 3
 *>  Network  : FC00:0:0:2001::                          PrefixLen : 64
     NextHop  : ::                                 LocPrf    :
     MED      : 0                                 PrefVal   : 0
     Label    : NULL
     Path/Ogn :  ?
 *>  Network  : FC00:0:0:2001::2                         PrefixLen : 128
     NextHop  : ::                                 LocPrf    :
     MED      : 0                                 PrefVal   : 0
     Label    : NULL
     Path/Ogn :  ?
 *>  Network  : FE80::                                   PrefixLen : 10
     NextHop  : ::                                 LocPrf    :
     MED      : 0                                 PrefVal   : 0
     Label    : NULL
     Path/Ogn :  ?
```

Display information about BGP VPNv6 route flapping of a specified VPN instance during the specified period.

```
<HUAWEI> display bgp vpnv6 vpn-instance 1 routing-table time-range 0d5h0m0s 1d5h0m0s
BGP Local router ID is 10.1.1.1
 Status codes: * - valid, > - best, d - damped,
```

```
          h - history,  i - internal, s - suppressed, S - Stale
          Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 300:1

 *>  Network  : FC00:0:0:1991::                         PrefixLen : 64
     NextHop  : ::                                 Duration  : 16h32m17s
     Peer     : ::
     Path/Ogn : ?
 *>  Network  : FC00:0:0:2004::                         PrefixLen : 64
     NextHop  : ::                                 Duration  : 16h34m02s
     Peer     : ::
     Path/Ogn : ?

 Route Distinguisher: 10011:1

 *>i Network  : FC00:0:0:1998::                         PrefixLen : 32
     NextHop  : FC00:0:0:1::9                      Duration  : 16h38m16s
     Peer     : 10.1.1.9
     Path/Ogn : 65410  ?
 *>i Network  : FC00:0:0:1998::                         PrefixLen : 64
     NextHop  : FC00:0:0:1::9                      Duration  : 16h37m01s
     Peer     : 10.1.1.9
     Path/Ogn : ?
 *>i Network  : FC00:0:0:2001::                         PrefixLen : 64
     NextHop  : FC00:0:0:1::9                      Duration  : 16h47m31s
     Peer     : 10.1.1.9
     Path/Ogn : ?
 *>i Network  : FC00:0:0:3001::                         PrefixLen : 64
     NextHop  : FC00:0:0:1::9                      Duration  : 16h45m40s
     Peer     : 10.1.1.9
     Path/Ogn : 65410  ?

 VPN-Instance vpna, Router ID 10.4.4.4 :
 *>  Network  : FC00:0:0:1991::                         PrefixLen : 64
     NextHop  : ::                                 Duration  : 16h32m17s
     Peer     : ::
     Path/Ogn : ?
 *>i Network  : FC00:0:0:1998::                         PrefixLen : 32
     NextHop  : FC00:0:0:1::9                      Duration  : 16h38m16s
     Peer     : 10.1.1.9
     Path/Ogn : 65410  ?
 *>i Network  : FC00:0:0:1998::                         PrefixLen : 64
     NextHop  : FC00:0:0:1::9                      Duration  : 16h37m01s
     Peer     : 10.1.1.9
     Path/Ogn : ?
 *>i Network  : FC00:0:0:2001::                         PrefixLen : 64
     NextHop  : FC00:0:0:1::9                      Duration  : 16h47m31s
     Peer     : 10.1.1.9
     Path/Ogn : ?
 *>  Network  : FC00:0:0:2004::                         PrefixLen : 64
     NextHop  : ::                                 Duration  : 16h34m02s
     Peer     : ::
     Path/Ogn : ?
 *>i Network  : FC00:0:0:3001::                         PrefixLen : 64
     NextHop  : FC00:0:0:1::9                      Duration  : 16h45m40s
     Peer     : 10.1.1.9
     Path/Ogn : 65410  ?
```

Table 7-186 Description of the display bgp vpnv6 all routing-table command output

Item	Description
BGP Local router ID	ID of the local BGP router. The ID is in the same format as an IPv4 address.

Item	Description
Total number of routes from all PE	Total number of BGP VPNv6 routes received by the switch from its peer PEs.
Network	Destination network or host address of the route.
PrefixLen	Prefix length of the destination network or host address of the route.
NextHop	IPv6 address of the next hop.
LocPrf	Local preference of the BGP route. The default value is 100.
MED	MED of the route. The default value is 0.
PrefVal	Preferred value of the route.
Label	Label carried by the data packet destined for the destination network or host address of the route.
Duration	Route duration.
Peer	IP addresses of the peer.
Path/Ogn	AS_Path number and Origin attribute of the route.

Display the routes of an IPv6 address family-enabled VPN instance named vpn1 on the local device.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 2
 *>i Network  : FC00:0:0:1::                          PrefixLen : 64
     NextHop  : FC00:0:0:3::1                         LocPrf    :
     MED      : 0                               PrefVal   : 0
     Label    :
     Path/Ogn : 65410  ?
 *>i Network  : FC00:0:0:1::                          PrefixLen : 64
     NextHop  : FC00:0:0:2::1                         LocPrf    : 100
     MED      : 0                               PrefVal   : 0
     Label    : 1037/NULL
     Path/Ogn : ?
```

Display the BGP routes with a specified destination address of an IPv6 address family-enabled VPN instance.

```
<HUAWEI> display bgp vpnv6 vpn-instance vrf1 routing-table fc00:0:0:1::

 BGP local router ID : 10.1.1.1
 Local AS number : 100
```

```
 Paths:   2 available, 1 best, 1 select
 BGP routing table entry information of FC00:0:0:1::/64:
 Imported route.
 From: :: (0.0.0.0)
 Route Duration: 1d03h46m24s
 Direct Out-interface: Vlanif100
 Original nexthop: ::
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select,
pre 0
 Advertised to such 1 peers:
    FC00:0:0:2::2
 BGP routing table entry information of 2001::/64:
 From: FC00:0:0:1::1 (10.10.10.10)
 Route Duration: 02h39m43s
 Direct Out-interface: Vlanif100
 Original nexthop: FC00:0:0:1::1
 AS-path 65410, origin incomplete, MED 0, pref-val 0, external, pre 255
 Not advertised to any peer yet
```

Display BGP VPNv6 routes of the VPN instance named **vpn1** whose AS_Path attribute contains 65420.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table as-path-filter 1

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 1
     Network  : FC00:0:0:1::2001::                    PrefixLen : 64
     NextHop  : FC00:0:0:1::2001::1                   LocPrf    :
     MED      : 0                              PrefVal   : 0
     Label    :
     Path/Ogn : 65420  ?
```

Display BGP VPNv6 routes that the local switch advertises to the peer at 10.3.3.3.

```
<HUAWEI> display bgp vpnv6 all routing-table peer 10.3.3.3 advertised-routes

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1

 Route Distinguisher: 100:1


 *>  Network  : FC00:0:0:1::                          PrefixLen : 64
     NextHop  : FC00:0:0:2::2                         LocPrf    :
     MED      : 0                              PrefVal   : 0
     Label    : NULL
     Path/Ogn : 65410 ?
```

Display BGP VPNv6 routes that the local switch receives from the peer at 10.3.3.3.

```
<HUAWEI> display bgp vpnv6 all routing-table peer 10.3.3.3 received-routes


 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
```

```
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1

 Route Distinguisher: 100:2


 *>i Network  : FC00:0:0:1::2002::                      PrefixLen : 64
     NextHop  : FC00:0:0:1::2001::1                     LocPrf    : 100
     MED      : 0                               PrefVal   : 0
     Label    : 1037
     Path/Ogn : ?
```

Display all BGP VPNv6 routes that match the BGP community filter 1.

```
<HUAWEI> display bgp vpnv6 all routing-table community-filter 1 whole-match

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


 Total number of routes from all PE: 2

 Route Distinguisher: 100:1


 *>  Network  : FC00:0:0:2001::                         PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                        LocPrf    :
     MED      : 0                               PrefVal   : 0
     Label    : NULL

 Route Distinguisher: 100:2


 *>i Network  : FC00:0:0:2002::                         PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                        LocPrf    : 100
     MED      : 0                               PrefVal   : 0
     Label    : 1037

 VPN-Instance vpn1, Router ID 10.4.4.4, Router ID 10.4.4.4 :

 Total Number of Routes: 2
     Network  : FC00:0:0:2001::                         PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                        LocPrf    :
     MED      : 0                               PrefVal   : 0
     Label    :
 *>i Network  : FC00:0:0:2002::                         PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                        LocPrf    : 100
     MED      : 0                               PrefVal   : 0
     Label    : 1037/NULL
```

Display BGP4+ routes of the VPN instance named **vpn1** and matching the BGP community filter 1.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table community-filter 1 whole-match

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1 :

 Total Number of Routes: 2
     Network  : FC00:0:0:2001::                         PrefixLen : 64
```

```
    NextHop  : FC00:0:0:2001::1                    LocPrf    :
    MED      : 0                               PrefVal   : 0
    Label    :
 *>i Network  : FC00:0:0:2002::                    PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    : 100
    MED      : 0                               PrefVal   : 0
    Label    : 1037/NULL
```

Display all BGP4+ routes of the VPN instance named **vpn1** and matching the AS regular expression.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table regular-expression ^65420


 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1, Router ID 10.4.4.4, Router ID 10.4.4.4 :
    Network  : FC00:0:0:2001::                     PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    :
    MED      : 0                               PrefVal   : 0
    Label    :
    Path/Ogn : 65420  ?
```

Display all BGP4+ routes of the VPN instance named **vpn1** that are received from the peer at FC00:0:0:2001::1.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table peer fc00:0:0:2001::1 received-routes

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
    Network  : FC00:0:0:2001::                     PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    :
    MED      : 0                               PrefVal   : 0
    Label    :
    Path/Ogn : 65410  ?
```

Display BGP4+ routes sent to the peer at FC00:0:0:2001::1.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table peer fc00:0:0:2001::1 advertised-routes

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
 *>i Network  : FC00:0:0:2002::                    PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    : 100
    MED      : 0                               PrefVal   : 0
    Label    : 1037/NULL
    Path/Ogn : ?
```

Display detailed information about the specified invalid BGP VPNv6 routes.

```
<HUAWEI> display bgp vpnv6 vpn-instance vrf1 routing-table fc00:0:0:2001::5
 BGP local router ID : 10.1.1.1
 Local AS number : 100

 VPN-Instance vrf1, Router ID 10.1.1.1:
 Paths:   1 available, 0 best, 0 select
```

```
 BGP routing table entry information of fc00:0:0:2001::5/128:
 Label information (Received/Applied): 1027/NULL
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h01m22s
 Relay Tunnel Out-Interface:
 Relay token: 0x0
 Original nexthop: ::FFFF:10.1.1.2
 Ext-Community:RT <100 : 100>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for tunnel
unreachable
 Not advertised to any peer yet
```

Table 7-187 Description of the display bgp vpnv6 routing-table command output

Item	Description
BGP local router ID	Router ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
VPN-Instance vrf1, Router ID 10.1.1.1	The local VPN instance is vrf1, and its router ID is 10.1.1.1.
Paths	Information about paths of BGP routes
BGP routing table entry information of fc00:0:0:2001::5/128	The following information is about fc00:0:0:2001::5/128 routing entries.
Label information (Received/ Applied)	Label information (received or sent).
From	IP address of the router that sends the route. 10.1.1.2 is the source interface IP address of the peer with which the BGP connection is established, and 10.1.1.2 is the router ID of the peer.
Route Duration	Duration of routes.
Relay Tunnel Out-Interface	Tunnel recursed outbound interface.
Relay token	Recursive token value used for MPLS forwarding, which is a part of tunnel ID and is assigned by the system.
Original nexthop	Original next hop.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Preferred value of the protocol.
internal	The BGP route is an internal route.
pre 255	The priority of the BGP route is 255.
invalid for tunnel unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to recurse to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to recurse to a tunnel.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

7.8.77 display bgp vpnv6 routing-table statistics

Function

The **display bgp vpnv6 routing-table statistics** command displays statistics about BGP VPNv6 routes.

Product	Support
S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5731-S, S5731S-S, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **different-origin-as**]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **different-origin-as**]

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table statistics regular-expression** *as-regular-expression*

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table statistics regular-expression** *as-regular-expression*

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table statistics community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name*} **routing-table statistics community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 all routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
all	Displays statistics about all BGP VPNv6 routes.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays BGP routes with the specified RD.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Displays statistics about the BGP routes of a specified VPN instance.	The value must be an existing VPN instance name.
as-path-filter	Displays the routes that match the specified filter.	-

Parameter	Description	Value
as-path-filter-number	Specifies the number of the matching AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
different-origin-as	Displays statistics about the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 case-sensitive characters. It cannot contain spaces.
community	Displays statistics about the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	The value is an integer that ranges from 0 to 4294967295.
aa:nn	Specifies the community number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays statistics about the BGP routes carrying the Internet community attribute.	-
no-advertise	Displays statistics about the BGP routes carrying the No-Advertise community attribute.	-

Parameter	Description	Value
no-export	Displays statistics about the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays statistics about the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays statistics about the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
peer *ipv6-address*	Displays statistics about the BGP routes of a specified peer.	-
advertised-routes	Displays statistics about the routes advertised to a specified peer.	-
received-routes	Displays statistics about the routes received from a specified peer.	-
active	Specifies the number of active routes.	-
peer *ipv4-address*	Displays the routing information for the specified BGP peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bgp vpnv6 routing-table statistics** command to check statistics about BGP VPNv6 routes.

Example

Display statistics about BGP VPNv6 routes on the local device.

```
<HUAWEI> display bgp vpnv6 all routing-table statistics

 Total number of routes from all PE: 2

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics about the BGP4+ routes of an IPv6 address family-enabled VPN instance named **vpn1** on the local device.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table statistics

 Total Number of Routes: 5
```

Display statistics about the BGP VPNv6 routes received from peer 10.1.1.1.

```
<HUAWEI> display bgp vpnv6 all routing-table peer 10.1.1.1 received-routes statistics
  Received routes total: 1
```

Display statistics about the VPNv6 routes that have the Internet community attribute and specified RD on the local device.

```
<HUAWEI> display bgp vpnv6 route-distinguisher 100:1 routing-table statistics community internet

 Total number of routes from all PE: 1

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics about the BGP VPNv6 routes that match a specified community filter on the local device.

```
<HUAWEI> display bgp vpnv6 all routing-table statistics community-filter 1

 Total number of routes from all PE: 1

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics about the BGP VPNv6 routes that match a specified AS_Path regular expression.

```
<HUAWEI> display bgp vpnv6 all routing-table statistics regular-expression 65420*

 Total number of routes from all PE: 1
```

```
 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 1
```

Display statistics of BGP routes sent by the local device to peer 2001:db8:1::1 of the IPv6 VPN instance named **vpn1**.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table peer 2001:db8:1::1 received-routes
statistics
  Received routes total: 2
```

Display statistics about the IPv6 routes sent by the local device to peer 2001:db8:1::1 in a VPN instance named **vpn1**.

```
<HUAWEI> display bgp vpnv6 vpn-instance vpn1 routing-table peer 2001:db8:1::1 advertised-routes
statistics
  Advertised routes total: 2

  Default originated : 0
```

7.8.78 display default-parameter bgp

Function

The **display default-parameter bgp** command displays default configurations in BGP initialization.

Format

display default-parameter bgp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display default-parameter bgp** command to check default configurations in BGP initialization.

Example

Display default configurations in BGP initialization.

```
<HUAWEI> display default-parameter bgp
BGP version                  : 4
EBGP preference              : 255
IBGP preference              : 255
Local preference             : 255
BGP connect-retry            : 32s
```

```
BGP holdtime                 : 180s
BGP keepAlive                : 60s
EBGP route-update-interval  : 30s
IBGP route-update-interval  : 15s
Default local-preference    : 100
Default MED                  : 0
Default TRACKING TIMER      : 9
IPv4-family unicast         : enable
EBGP-interface-sensitive    : enable
Reflect between-clients     : enable
Check-first-as              : enable
Synchronization             : disable
Nexthop-resolved rules      :
    IPv4-family             : unicast(ip)
                              label-route(ip)
                              multicast(ip)
                              vpn-instance(tunnel)
                              vpnv4(ip)
    IPv6-family             : unicast(ip)
                              vpn-instance(tunnel)
                              vpnv6(ip)
                              6PE(tunnel)
    L2VPN-AD-family         : ip
 Routing-table limit max-alarm upper limit : 100
 Routing-table limit max-alarm lower limit : 95
 Routing-table limit threshold-alarm upper limit : 80
 Routing-table limit threshold-alarm lower limit : 70
```

Table 7-188 Description of the **display default-parameter bgp** command output

Item	Description
BGP version	BGP version number.
EBGP preference	EBGP route preference.
IBGP preference	IBGP route preference.
Local preference	Local route preference.
BGP connect-retry	BGP ConnectRetry interval.
BGP holdtime	BGP holdtime interval.
BGP keepAlive	BGP keepalive interval.
EBGP route-update-interval	Minimum interval for sending EBGP Update messages.
IBGP route-update-interval	Minimum interval for sending IBGP Update messages.
Default local-preference	Local preference of a BGP route.
Default MED	MED of a BGP route.
Default TRACKING TIMER	The interval between peer unreachability discovery and connection interruption.
IPv4-family unicast	BGP-IPv4 unicast address family view.

Item	Description
EBGP-interface-sensitive	The BGP session between the directly connected peer and an interface is deleted immediately when the interface becomes Down.
Reflect between-clients	Route reflection between clients.
Check-first-as	The first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer is checked.
Synchronization	Synchronization between IBGP and IGP.
Nexthop-resolved rules	Default recursion mode of preferred routes.
Routing-table limit max-alarm upper limit	Upper alarm threshold for the number of BGP routes.
Routing-table limit max-alarm lower limit	Lower alarm threshold for the number of BGP routes.
Routing-table limit threshold-alarm upper limit	Default upper alarm threshold for the number of BGP routes.
Routing-table limit threshold-alarm lower limit	Default lower alarm threshold for the number of BGP routes.

7.8.79 display mbgp routing-table

Function

The **display mbgp routing-table** command displays MBGP routes.

Format

display mbgp routing-table [*ipv4-address* [*mask* | *mask-length*]] [**verbose**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the destination IP address in dotted decimal notation.	-
mask | *mask-length*	Specifies mask in dotted decimal notation or mask-length.	-

Parameter	Description	Value
verbose	Displays detailed information about active and inactive routes. If the parameter **verbose** is not specified, detailed information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

Example

Display information about all MBGP routes.

```
<HUAWEI> display mbgp routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: MBGP
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags  NextHop  Interface

  10.5.5.1/32     MBGP   255     0     R   10.1.1.1  Vlanif10
```

Table 7-189 Description of the display mbgp routing-table command output

Item	Description
Route Flags	Flag of a route: - R: indicates that the route is a recursive route. - D: indicates that the route is delivered to the FIB table. - T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: MBGP	Indicates an MBGP routing table.
Destinations	Indicates the total number of destination networks or hosts.
Routes	Indicates the total number of routes.
Destination/Mask	Indicates the address and mask length of the destination network or host.

Item	Description
Proto	Indicates the protocol through which routes are learned.
Pre	Indicates the preference.
Cost	Indicates the route cost.
Flags	Indicates the route flag, that is, Route Flags in the header of the routing table.
NextHop	Indicates the next hop.
Interface	Indicates the outbound interface through which the next hop is reachable.

Display the detailed information of the specified routes.

```
<HUAWEI> display mbgp routing-table 5.5.5.1 verbose
Routing Table : MBGP
Summary Count : 1

 Destination: 10.5.5.1/32
    Protocol: MBGP           Process ID: 0
  Preference: 255                  Cost: 0
     NextHop: 10.1.1.1        Neighbour: 0.0.0.0
       State: Active Adv GotQ       Age: 00h43m25s
         Tag: 0              Priority: 0
       Label: NULL            QoSInfo: 0x0
RelayNextHop: 0.0.0.0       Interface: Vlanif 10
    TunnelID: 0x0               Flags: R
```

Table 7-190 Description of the display mbgp routing-table verbose command output

Item	Description
Destination	Indicates the address and mask length of the destination network or host.
Protocol	Indicates the routing protocol.
Process ID	Indicates the process ID of the routing protocol.
Preference	Indicates the preference of the route.
Cost	Indicates the route cost.
NextHop	Indicates the next hop.
Neighbour	Indicates the neighbor.

Item	Description
State	Indicates the status of routes: - Active: indicates active routes. - Invalid: indicates invalid routes. - Inactive: indicates inactive routes. - NoAdv: indicates the routes that cannot be advertised. - Adv: indicates the routes that can be advertised. - Del: indicates the routes to be deleted. - GotQ: indicates the route that finds the next hop and outbound interface or the route that finds the tunnel. - WaitQ: indicates the route that does not find the next hop or outbound interface or the route that does not find the tunnel. - Stale: indicates the routes with the stale flag. The routes are used in GR.
Age	Indicates the lifetime of the route.
Tag	Indicates the administrative tag for routes.
Priority	Indicates the priority.
Label	Indicates the allocated MPLS label.
QoSInfo	Indicates QoS information.
RelayNextHop	Indicates the relay next hop.
Interface	Indicates the outbound interface through which the next hop is reachable.
Tunnel ID	Indicates the tunnel ID.
Flags	Indicates the route flag, that is, Route Flags in the header of the routing table.

7.8.80 display mbgp routing-table statistics

Function

The **display mbgp routing-table statistics** command displays the statistics of the MBGP routes.

Format

display mbgp routing-table statistics

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted by the protocol
- Number of active routes or inactive routes that are labeled for deletion but are not actually deleted

Example

Display statistics of the MBGP routing table.

```
<HUAWEI> display mbgp routing-table statistics
Proto     total      active      added        deleted      freed
          routes     routes      routes       routes       routes
MBGP      6          4           10           0            0
```

Table 7-191 Description of the display mbgp routing-table statistics command output

Item	Description
Proto	Routing protocol
total routes	Total number of routes in the routing table
active routes	Number of active routes in the routing table
added routes	Number of active and inactive routes added in the routing table
deleted routes	Number of routes to be deleted from the routing table
freed routes	Number of routes that are permanently deleted from the routing table

7.8.81 ebgp-interface-sensitive

Function

The **ebgp-interface-sensitive** command immediately resets a BGP session on an interface that is directly connected to an external peer when the interface goes Down.

The **undo ebgp-interface-sensitive** command disables the function.

By default, this function is enabled.

Format

ebgp-interface-sensitive

undo ebgp-interface-sensitive

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the **ebgp-interface-sensitive** command is not configured, the system does not immediately select the sub-optimal route for packet transmission when an interface goes Down. Instead, the system waits for a period of time (defaulting to 180 seconds) before checking whether another interface can be used to send packets to the same destination address. This will interrupt services for a period of time. If the **ebgp-interface-sensitive** command is run, BGP can quickly detect EBGP link faults and use another interface to establish a BGP peer relationship with the remote peer.

When the interface used for a BGP connection alternates between Up and Down states, running the **undo ebgp-interface-sensitive** command can prevent the repeated reestablishment and deletion of the BGP session in the event of route flapping. This reduces the use of network bandwidth.

Precautions

If the interface used for a BGP connection alternates between Up and Down states, it would be better not to run the **ebgp-interface-sensitive** command to prevent route flapping.

Example

Enable the function that automatically resets a BGP session.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ebgp-interface-sensitive
```

7.8.82 ext-community-change enable

Function

The **ext-community-change enable** command enables a device to change extended community attributes based on a Route-Policy.

The **undo ext-community-change enable** command disables a device from changing extended community attributes based on a Route-Policy.

By default, extended community attributes cannot be changed based on a Route-Policy.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

ext-community-change enable

undo ext-community-change enable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, BGP prevents a device from changing extended community attributes from a peer or peer group based on an import policy or changing extended community attributes to be advertised to a peer or peer group based on an export policy. To enable a device to change extended community attributes from a peer or peer group based on an import policy and change extended community attributes to be advertised to a peer or peer group based on an export policy before advertising them, run the **ext-community-change enable** command.

Precautions

- The **ext-community-change enable** and **peer route-policy import** commands must both be run so that the device can change extended community attributes from a peer or peer group based on an import policy.
- The **ext-community-change enable** command must be run with either of the following commands so that the extended community attributes changed based on an export policy can be advertised to a peer or peer group.
  - **peer advertise-ext-community**
  - **peer route-policy export**

Example

Enable the device to change extended community attributes of the BGP routes received from peer 10.1.1.1 based on a Route-Policy named **policy1**.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy1 permit node 10
[HUAWEI-route-policy] if-match as-path-filter 2
[HUAWEI-route-policy] apply extcommunity rt 10.1.1.1:1 additive
[HUAWEI-route-policy] quit
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] ext-community-change enable
[HUAWEI-bgp-af-ipv4] peer 10.1.1.1 route-policy policy1 import
```

7.8.83 filter-policy export (BGP)

Function

The **filter-policy export** command configures a device to filter the routes to be advertised. BGP advertises only the routes that pass filtering.

The **undo filter-policy export** command restores the default configuration.

By default, the routes to be advertised are not filtered.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

undo filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IPv4 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the name of a routing protocol.	The BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view support **direct**, **isis**, **ospf**, **rip**, **static**, and **unr**. The BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view support **direct**, **isis**, **ospfv3**, **ripng**, **static**, and **unr**.
process-id	Specifies the number of a process that needs to perform matching. If *protocol* is **direct**, **static**, or **unr**, no process ID is required.	The value is an integer that ranges from 1 to 65535.
acl6-number	Specifies the number of a basic ACL6.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6.	The value is a string of 1 to 64 case-sensitive characters without spaces. The name should start with a letter and can contain numbers, hyphens (-), or underscores (_).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *protocol* [*process-id*] is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.
- **acl-name** *acl-name*, *acl-number*, and **ip-prefix** *ip-prefix-name* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- **acl6-name** *acl6-name*, *acl6-number*, and **ipv6-prefix** *ipv6-prefix-name* are valid only in the BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, and BGP-VPNv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-MDT address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

The **filter-policy export** command affects the routes advertised by BGP. After the command is run, BGP filters the routes that are imported by using the **import-route** command. Only the routes that pass the filtering can be added to the local BGP routing table and advertised by BGP.

If *protocol* is specified, only the routes imported from the specified protocol will be filtered. If *protocol* is not specified, the routes imported from all protocols will be filtered.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes are advertised to the specified peer.

Example

Use ACL 2000 to filter all the routes to be advertised by BGP.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] filter-policy 2000 export
```

7.8.84 filter-policy import (BGP)

Function

The **filter-policy import** command configures a device to filter received routes.

The **undo filter-policy import** command restores the default configuration.

By default, received routes are not filtered.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

undo filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IPv4 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl6-number	Specifies the number of a basic ACL6.	-
acl6-name *acl6-name*	Specifies the name of a named ACL6.	The value is a string of 1 to 64 case-sensitive characters without spaces. The name should start with a letter and can contain numbers, hyphens (-), or underscores (_).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- **acl-name** *acl-name*, *acl-number*, and **ip-prefix** *ip-prefix-name* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- **acl6-name** *acl6-name*, *acl6-number*, and **ipv6-prefix** *ipv6-prefix-name* are valid only in the BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, and BGP-VPNv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **filter-policy import** command is used to filter the routes received by BGP to determine whether to add them to the BGP routing table.

When the **rule** command is run to configure rules for an ACL, only the source address range specified by **source** and the time period specified by **time-range** are valid as the rules.

When the **rule (basic ACL6 view)** or **rule (advanced ACL6 view)** command is run to configure rules for an ACL6, only the source address range specified by **source** and the time period specified by **time-range** are valid as the rules.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes advertised by the specified peer are accepted.

Example

Use ACL 2000 to filter the routes received by BGP.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] filter-policy 2000 import
```

7.8.85 graceful-restart (BGP)

Function

The **graceful-restart** command enables GR for the BGP speaker.

The **undo graceful-restart** command restores the default configuration.

By default, GR is disabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **graceful-restart** command is configured to enable GR for the switch, to prevent traffic interruption, another GR-capable device can assist the switch to perform GR when BGP on the switch restarts due to an active/standby switchover, and the switch can assist other GR-capable devices to perform GR when BGP on other devices restarts.

Follow-up Procedure

After running the **graceful-restart** command, run the **graceful-restart timer wait-for-rib** command to set the time for waiting for the End-Of-RIB flag.

Precautions

Enabling or disabling GR may delete and reestablish all BGP sessions and instances.

If the **graceful-restart timer wait-for-rib** command has been configured, using the **undo graceful-restart** command will delete the **graceful-restart timer wait-for-rib** command configuration.

Example

Enable GR for the speaker in BGP process 100.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] graceful-restart
```

7.8.86 graceful-restart peer-reset

Function

The **graceful-restart peer-reset** command enables a device to reset a BGP connection in GR mode.

The **undo graceful-restart peer-reset** command restores the default configuration.

By default, a device is not enabled to reset a BGP connection in GR mode.

Format

graceful-restart peer-reset

undo graceful-restart peer-reset

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, BGP does not support dynamic capability negotiation. Therefore, each time a new BGP capability is enabled on a BGP speaker, the BGP speaker tears down existing sessions with its peer and renegotiates BGP capabilities.

With the GR reset function configured, when you enable a new BGP capability on the BGP speaker, the BGP speaker enters the GR state, resets the BGP session, and renegotiates BGP capabilities with the peer. In the whole process, the BGP speaker re-establishes the existing sessions but does not delete the routing entries for the existing sessions, so that the existing services are not interrupted.

Prerequisites

GR has been enabled by running the **graceful-restart** command. If this prerequisite is not met, the system does not allow you to configure the **graceful-restart peer-reset** command.

Precautions

After you run the **undo graceful-restart** command to disable GR, the **graceful-restart peer-reset** command configuration will be deleted automatically.

Example

Enable the switch to reset a BGP connection in GR mode.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] graceful-restart
[HUAWEI-bgp] graceful-restart peer-reset
```

7.8.87 graceful-restart timer restart

Function

The **graceful-restart timer restart** command sets the maximum period from the time when the peer finds that the local peer restarts to the time when the BGP session is reestablished.

The **undo graceful-restart timer restart** command deletes the setting.

By default, the maximum period from the time when the peer finds that the local peer restarts to the time when the BGP session is reestablished is 150 seconds.

Format

graceful-restart timer restart *time*

undo graceful-restart timer restart

Parameters

Parameter	Description	Value
time	Specifies the maximum period from the time when the peer finds that the local peer restarts to the time when the BGP session is reestablished.	The value ranges from 3 to 4095, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Modifying the maximum period for reestablishing the BGP session leads to the reestablishment of the BGP peer relationship.

NOTE

The **graceful-restart timer restart** command can be run only after the **graceful-restart** command is run.

Example

Set the maximum period for reestablishing the BGP session to 250 seconds.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] graceful-restart
[HUAWEI-bgp] graceful-restart timer restart 250
```

7.8.88 graceful-restart timer wait-for-rib

Function

The **graceful-restart timer wait-for-rib** command sets the length of time that the BGP restarter waits for the End-Of-RIB flag.

The **undo graceful-restart timer wait-for-rib** command deletes the configured length of time that the BGP restarter waits for the End-Of-RIB flag.

By default, the time that the BGP restarter waits for the End-Of-RIB flag is 600 seconds.

Format

graceful-restart timer wait-for-rib *time*

undo graceful-restart timer wait-for-rib

Parameters

Parameter	Description	Value
time	Specifies the length of time that the BGP restarter waits for the End-Of-RIB flag.	The value is an integer that ranges from 3 to 3000, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the BGP session is set up or reestablished, the BGP restarter must receive the End-Of-RIB flag in the period set by using this command. If the BGP restarter does not receive the End-Of-RIB flag, ensure that the switch can exit from the GR process.

Prerequisites

The **graceful-restart timer wait-for-rib** command can be run only after the **graceful-restart** command is run.

Configuration Impact

The latest configuration overrides the previous one.

Precautions

If there are a large number of routes, set a larger value for the *time* parameter to ensure that all routes will be updated.

Example

Set the time that the BGP restarter waits for the End-Of-RIB flag to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] graceful-restart timer wait-for-rib 100
```

7.8.89 group

Function

The **group** command creates a peer group.

The **undo group** command deletes a peer group.

By default, no peer group is created.

Format

group *group-name* [**external** | **internal**]

undo group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Creates an EBGP peer group.	-
internal	Creates an IBGP peer group.	-

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A peer group is a group of peers with the same configurations. After a peer is added to a peer group, it inherits the configurations of this peer group. Peers in a peer group inherit the configurations of the peer group. When the configurations of the peer group are changed, the configurations of these peers are changed accordingly.

On a large-scale BGP network, there are a large number of peers and many of them have the same configurations. To configure these peers, you have to repeatedly use some commands. In such a case, configuring peer groups can simplify configurations. If the configurations for several peers are the same, these peers can be added to a created and configured peer group. The peers in the peer group then inherit the configurations of the peer group.

Precautions

If the **group** command is run multiple times, the latest configuration does not override the previous one.

If the type (IBGP or EBGP) of a peer group is not specified, an IBGP peer group is created by default.

The configuration of a peer takes precedence over that of the peer group to which the peer belongs.

If an attribute configuration of a BGP peer in a peer group differs from that of the peer group, you can disable the attribute configuration of the peer by using an **undo** command; then the peer inherits the attribute configuration of the peer group.

NOTICE

Deleting a peer group closes the connections on the peers that have no AS numbers in the peer group. Before deleting a peer group, you are recommended to delete these peers or configure AS numbers for these peers.

Example

Create an IBGP peer group named in.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group in internal
```

Create an EBGP peer group named ex, and set its AS number to 500.1.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group ex external
[HUAWEI-bgp] peer ex as-number 500.1
```

7.8.90 import-route (BGP)

Function

The **import-route** command configures BGP to import routes of other routing protocols and types.

The **undo import-route** command restores the default setting.

By default, BGP does not import routes.

Format

import-route *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

Parameters

Parameter	Description	Value
protocol	Specifies the routing protocol type and route type.	The BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view support **direct**, **isis**, **ospf**, **rip**, **static**, and **unr**. The BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view support **direct**, **isis**, **ospfv3**, **ripng**, **static**, and **unr**.
process-id	Specifies a process ID if BGP is configured to import routes. If *protocol* is **direct**, **static**, or **unr**, no process ID is required.	The value is an integer that ranges from 1 to 65535.
med *med*	Specifies the MED.	The value is an integer that ranges from 0 to 4294967295.
route-policy *route-policy-name*	Indicates that routes are filtered and route attributes are modified by using the Route-Policy specified by the parameter when these routes are imported from other protocols.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP can import routes by using the **import-route** command or **network** command:

- In import mode, BGP imports IGP routes, including RIP, OSPF, and IS-IS routes, into the BGP routing table based on protocol type. To ensure the validity of imported IGP routes, BGP can also import static routes and direct routes in import mode.

- In network mode, BGP imports the routes in the IP routing table one by one into the BGP routing table. The network mode is more accurate than the import mode.

Precautions

If the **default-route imported** command has not been used, BGP cannot import default routes when you run the **import-route** command to import routes from other protocols.

After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the BGP routing table. Therefore, use this command with caution.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all routes of the specified protocol are imported to the BGP routing table.

Example

Import routes from RIP process 1.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] import-route rip 1
```

7.8.91 ipv4-family

Function

The **ipv4-family** command enables the IPv4 address family of BGP, and then displays the address family view.

The **undo ipv4-family** command deletes the configurations in the IPv4 address family.

By default, the BGP-IPv4 unicast address family view is displayed.

Format

ipv4-family unicast

ipv4-family multicast

ipv4-family vpnv4 [**unicast**] (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

ipv4-family vpn-instance *vpn-instance-name*

ipv4-family { **mdt** | **mvpn** }

undo ipv4-family vpnv4 [**unicast**](supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

undo ipv4-family { **multicast** | **vpn-instance** *vpn-instance-name* }

undo ipv4-family { **mdt** | **mvpn** }

NOTE

The **mdt, mvpn, multicast** parameter is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
unicast	Displays the unicast address family view.	-
multicast	Displays the multicast address family view.	-
vpnv4	Displays the BGP-VPNv4 address family view.	-
vpn-instance *vpn-instance-name*	Associates a specified VPN instance with the IPv4 address family. You can enter the BGP-VPN instance IPv4 address family view by using the parameter.	The value must be an existing VPN instance name.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing BGP configurations in an IPv4 address family, you need to run the **ipv4-family** command in the BGP view to enable the IPv4 address family, and then enter the address family view. By default, BGP uses the IPv4 unicast address family.

Precautions

To disable the IPv4 unicast address family from being the default BGP route, run the **undo default ipv4-unicast** command.

Example

Enter the BGP-IPv4 unicast address family view.

```
<HUAWEI> system-view
```

```
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4]
```

7.8.92 ipv6-family

Function

The **ipv6-family** command enters the IPv6 address family view of BGP.

The **undo ipv6-family** command quits the IPv6 address family view and deletes the configurations in the view.

Format

ipv6-family [**vpnv6**](supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

ipv6-family [**unicast** | **vpn-instance** *vpn-instance-name*]

undo ipv6-family [**vpnv6**] (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

undo ipv6-family [**unicast** | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
unicast	Displays the unicast address family view.	-
vpnv6	Displays the BGP-VPNv6 address family view.	-
vpn-instance *vpn-instance-name*	Associates a specified VPN instance with the IPv6 address family. You can enter the BGP-VPN instance IPv6 address family view by using the parameter. **NOTE** The parameter is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.	The value must be an existing VPN instance name.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If no parameter is specified, the IPv6 address family view is displayed by default. The **undo ipv6-family** command without any parameter is used to delete configurations in the BGP-IPv6 unicast address family view.

Precautions

The **undo ipv6-family** command without any parameters deletes all IPv6 unicast address family configurations.

Example

Enter the BGP-IPv6 unicast address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv6-family
[HUAWEI-bgp-af-ipv6]
```

7.8.93 load-balancing as-path-ignore

Function

The **load-balancing as-path-ignore** command configures a router not to compare the AS_Path attributes of routes that are to be used for load balancing.

The **undo load-balancing as-path-ignore** command configures a router to compare the AS_Path attributes of routes that are to be used for load balancing.

By default, a router compares the AS-Path attributes of routes that are to be used for load balancing.

Format

load-balancing as-path-ignore

undo load-balancing as-path-ignore

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **load-balancing as-path-ignore** command is run, a router does not compare the AS_Path attributes of the routes (including the AS_Path length and content) that are to be used for load balancing. This command applies to the scenarios where EBGP and IBGP routes carry out load balancing. Exercise caution when using the command because the execution of this command will change the conditions of load balancing.

Precautions

The **load-balancing as-path-ignore** command and the **bestroute as-path-ignore** command are mutually exclusive. This means that if the **bestroute as-path-ignore** command is configured, the **load-balancing as-path-ignore** command cannot be configured.

Example

Configure a router not to compare the AS-Path attributes of the routes that are to be used for load balancing.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] load-balancing as-path-ignore
```

7.8.94 maximum load-balancing (BGP)

Function

The **maximum load-balancing** command configures the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default value.

By default, the maximum number of equal-cost routes is 1, indicating that load balancing is not implemented.

Format

maximum load-balancing [**ebgp** | **ibgp**] *number* [**ecmp-nexthop-changed**]

undo maximum load-balancing [**ebgp** | **ibgp**]

Parameters

Parameter	Description	Value
ebgp	Indicates that only EBGP routes implement load balancing.	-

Parameter	Description	Value
ibgp	Indicates that only IBGP routes implement load balancing.	-
number	Specifies the maximum number of equal-cost routes in the BGP routing table.	BGP: The value is an integer that ranges from 1 to 8 on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S and S6720S-S. The value ranges from 1 to 16 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S BGP4+: The value is an integer that ranges from 1 to 8.
ecmp-nexthop-changed	Configures a BGP device to change the next-hop addresses of only the routes that participate in load balancing to its address.	-

NOTE

ecmp-nexthop-changed is valid only in the BGP view, BGP IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After BGP load balancing is configured, BGP routes that meet the following conditions and have the same AS_Path attribute will become equal-cost routes and implement load balancing:

- PrefVal values are the same.
- Local_Pref attributes are the same.

- All BGP routes are aggregated or non-aggregated routes.
- Accumulated Interior Gateway Protocol metric (AIGP) values are the same.
- Lengths of the AS_path attributes are the same.
- Origin types (IGP, EGP, or Incomplete) are the same.
- Multi_Exit Discriminator (MED) values are the same.
- All BGP routes are EBGP or IBGP routes.
- The IGP metric values within an AS are the same.

Configuring BGP load balancing better utilizes network resources.

After the **maximum load-balancing ebgp** *number* command is run, only EBGP routes take part in load balancing. After the **maximum load-balancing ibgp** *number* command is run, only IBGP routes take part in load balancing. If [**ebgp** | **ibgp**] is not set, both EBGP routes and IBGP routes take part in load balancing, and the number of EBGP routes involved in load balancing is the same as that of IBGP routes involved in load balancing.

If you run the **maximum load-balancing** *number* command, the device changes the next-hop addresses of the routes to be advertised to a local address no matter whether the routes are used for load balancing. However, in RR or BGP confederation scenarios, the device does not change the next-hop addresses of non-local routes to be advertised to a local address.

If you run the **maximum load-balancing** { **ebgp** | **ibgp** } *number* command, the device does not change the next-hop addresses of the routes to be advertised to a local address no matter whether the routes are used for load balancing.

If you run the **maximum load-balancing** [**ebgp** | **ibgp**] *number* **ecmp-nexthop-changed** command, the device changes the next-hop addresses of the routes to be advertised to a local address only when the routes are used for load balancing.

Configuration Impact

If the **maximum load-balancing** command is run for multiple times, the latest configuration overrides the previous one.

Precautions

The **maximum load-balancing** *number* command cannot be configured together with the **maximum load-balancing ebgp** *number* or **maximum load-balancing ibgp** *number* command.

Example

Set two equal-cost routes to a specified destination.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] maximum load-balancing 2
```

7.8.95 maximum load-balancing eibgp

Function

The **maximum load-balancing eibgp** command configures the maximum number of EBGP and IBGP routes for load balancing.

The **undo maximum load-balancing eibgp** command deletes the configured maximum number of EBGP and IBGP routes for load balancing.

By default, the maximum number of EBGP and IBGP routes for load balancing is not configured.

Format

maximum load-balancing eibgp *number* [**ecmp-nexthop-changed**]

undo maximum load-balancing eibgp

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost EBGP and IBGP routes.	The value is an integer that ranges from 1 to 8 on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S and S6720S-S. The value ranges from 1 to 16 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S
ecmp-nexthop-changed	Configures a BGP device to change the next-hop addresses of only the routes that participate in load balancing to its address.	-

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **maximum load-balancing eibgp** command is used in a VPN where a CE is dual-homed to two PEs. When the CE and one PE belong to an AS and the CE and the other PE belong to a different AS, you can set the number of EBGP and IBGP routes to be used for load balancing. This allows VPN traffic to be balanced among EBGP and IBGP routes.

After BGP load balancing is configured, BGP routes that meet the following conditions and have the same AS_Path attribute will become equal-cost routes and implement load balancing:

- PrefVal values are the same.
- Local_Pref attributes are the same.
- All BGP routes are summarized or non-summarized routes.
- Accumulated Interior Gateway Protocol metric (AIGP) values are the same.
- Lengths of the AS_path attributes are the same.
- Origin types (IGP, EGP, or Incomplete) are the same.
- Multi_Exit Discriminator (MED) values are the same.
- Protocol priorities are the same. By default, EBGP and IBGP routes have the same protocol priority (255). If the EBGP or IBGP route protocol priority is changed using a route-policy, load balancing cannot be implemented.
- Load balancing cannot be implemented between black-hole routes and non-black-hole routes.
- Load balancing cannot be implemented between labeled routes and non-labeled routes.
- Load balancing cannot be implemented between local routes and non-local routes.

Configuring BGP load balancing better utilizes network resources.

If you run the **maximum load-balancing eibgp** *number* command, the device changes the next-hop addresses of the routes to be advertised to a local address no matter whether the routes are used for load balancing. However, in RR or BGP confederation scenarios, the device does not change the next-hop addresses of non-local routes to be advertised to a local address.

If you run the **maximum load-balancing eibgp** *number* **ecmp-nexthop-changed** command, the device changes the next-hop addresses of the routes to be advertised to a local address only when the routes are used for load balancing.

Configuration Impact

If the **maximum load-balancing eibgp** command is run for multiple times, the latest configuration overrides the previous one.

Load balancing cannot be implemented between crossed and non-crossed routes.

Example

Set the maximum number of EBGP and IBGP routes for load balancing to 3.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpna
[HUAWEI-vpn-instance-vpna] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpna-af-ipv4] quit
[HUAWEI-vpn-instance-vpna] quit
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] maximum load-balancing eibgp 3
```

7.8.96 network (BGP)

Function

The **network** command configures BGP to statically add routes in the IP routing table to the BGP routing table and advertise these routes to peers.

The **undo network** command deletes the routes statically added to the BGP routing table.

By default, BGP does not statically add routes in the IP routing table to the BGP routing table.

Format

network { *ipv4-address* [*mask* | *mask-length*] | *ipv6-address prefix-length* } [**route-policy** *route-policy-name*]

undo network { *ipv4-address* [*mask* | *mask-length*] | *ipv6-address prefix-length* }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the route to be imported by BGP.	It is in dotted decimal notation.
mask	Specifies the IP address mask. If no mask is specified, the IP address is considered as a classful address.	It is in dotted decimal notation.
mask-length	Specifies the mask length of the IP address. If no mask length is specified, the IP address is considered as a classful address.	The value is an integer that ranges from 0 to 32.
ipv6-address	Specifies the IPv6 address of the route to be imported by BGP.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of the IPv6 network address advertised by BGP.	The value is an integer that ranges from 0 to 128.
route-policy *route-policy-name*	Specifies the name of the route-policy that is used for route import.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP itself cannot discover routes. Instead, it imports routes discovered by other protocols such as IGP or static routes into the BGP routing table. These imported routes then are transmitted within an AS or between ASs. Before adding routes to the BGP routing table, BGP filters these routes by the routing protocol. If routes in the local IP routing table need to be statically added to the BGP routing table and then advertised, you can use the **network** command.

The Origin attribute of the routes imported into the BGP routing table by using the **network** command is IGP.

If a route with a specific prefix or mask is added to the BGP routing table by using the **network** command, this route is the optimal route selected from all types of protocol routes. Unlike the **network** command, the **import-route (BGP)** command is used to add all routes of a particular protocol such as RIP, OSPF, IS-IS, static route, or direct route to the BGP routing table.

Precautions

The **network** command is used to import exactly-matching routes. This means that only the routes in the local IP routing table that exactly match the specified destination address and prefix length can be added to the BGP routing table. If *mask* is not specified, routes are exactly matched against the natural network mask.

When using the **undo network** command to delete the existing configuration, specify a correct mask.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, routes in the local routing table are added to the BGP routing table.

Example

Configure BGP to import the local route 10.0.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] network 10.0.0.0 255.255.0.0
```

7.8.97 nexthop recursive-lookup (BGP)

Function

The **nexthop recursive-lookup** command configures BGP to recurse the next hop based on a routing policy.

The **undo nexthop recursive-lookup** command restores the default setting.

By default, BGP does not recurse the next hop based on a routing policy.

Format

nexthop recursive-lookup route-policy *route-policy-name*

undo nexthop recursive-lookup route-policy

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Indicates the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP needs route recursion in case of indirect next hops. If an indirect next hop is not recursed based on a routing policy, a BGP route may recurse to an incorrect forwarding path, causing traffic loss. Therefore, next hop recursion should be performed according to certain conditions.

The **nexthop recursive-lookup route-policy** *route-policy-name* command can be run to control next hop recursion based on a routing policy. If a recursive route is filtered out by the routing policy, the route is considered unreachable. This prevents BGP routes from recursing to incorrect forwarding paths.

Prerequisites

The next hop to which a BGP route recurses has been determined and a routing policy has been configured.

NOTICE

Before configuring a routing policy, ensure that all desired recursive routes will not be filtered out by the routing policy.

Precautions

The command does not apply to the routes received from directly connected EBGP peers or LinkLocal peers and default routes.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, route recursion is not restricted.

Example

Configure next hop recursion based on the routing policy **rp_nexthop**.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] nexthop recursive-lookup route-policy rp_nexthop
```

7.8.98 nexthop recursive-lookup delay

Function

The **nexthop recursive-lookup delay** command configures the delay in responding to changes of the next hop.

The **undo nexthop recursive-lookup delay** command restores the default setting.

By default, the delay in responding to changes of the next hop is not configured.

Format

nexthop recursive-lookup delay [*delay-time*]

undo nexthop recursive-lookup delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in responding to changes of the next hop.	The value is an integer that ranges from 1 to 100, in seconds. The default value is 5 seconds.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the route path on the upstream of a PE connected to an RR changes, if the PE detects that the recursive next hop becomes unreachable before the RR instructs the PE to switch the route, the PE withdraws the original optimal route advertised to its connected CE. After the RR re-advertises the switched route to the PE, the PE re-advertises an optimal route to the CE after route selection. During the route switchover, a huge volume of traffic will be dropped. If the **nexthop recursive-lookup delay** command is run on the PE to delay responding to the next hop unreachable event and to respond to this event only after the RR advertises the switched route, the volume of lost traffic will be reduced during route switchover.

Example

Set the delay in responding to changes of the next hop to 10s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] nexthop recursive-lookup delay 10
```

7.8.99 nexthop recursive-lookup non-critical-event delay

Function

The **nexthop recursive-lookup non-critical-event delay** command enables a device to respond to non-urgent BGP next-hop recursion changes after a specified delay time.

The **undo nexthop recursive-lookup non-critical-event delay** command enables a device to immediately respond to non-urgent BGP next-hop recursion changes.

By default, a device immediately responds to non-urgent BGP next-hop recursion changes.

Format

nexthop recursive-lookup non-critical-event delay [*delay-time*]

undo nexthop recursive-lookup non-critical-event delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay time.	The value is an integer that ranges from 1 to 100, in seconds. The default value is 5.

Views

BGP view, BGP-IPv4 unicast address family view, or BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If repeated recursion causes the BGP next hop to frequently change on a device, the device frequently selects and advertises routes. To prevent unwanted re-routing and route advertisement, run the **nexthop recursive-lookup delay** command to enable the device to respond to BGP next-hop recursion changes after a specified delay time. The recursion results are as follows:

- Urgent recursion result change: The recursive next hop is changed, and BGP route reachability is also changed. For example, if a fault occurs on a network, a device finds no next-hop route or tunnel to which a BGP route recurses. As a result, traffic is interrupted.
- Non-urgent recursion result change: The recursive next hop is changed, and BGP route reachability is not affected. For example, after the interface or type of a tunnel to which the next hop of a BGP route recurses is changed, traffic keeps traveling over the BGP route.

To delay a response to the non-urgent recursion change, run the **nexthop recursive-lookup non-critical-event delay** command, not the **nexthop recursive-lookup delay** command.

Configuration Impact

After the **nexthop recursive-lookup delay** command is run, the device delays responses to all next-hop recursion changes. After the **nexthop recursive-lookup non-critical-event delay** command is run, the device delays responses only to non-urgent BGP next-hop recursion changes. If both commands are run, the

nexthop recursive-lookup non-critical-event delay command takes precedence over the **nexthop recursive-lookup non-critical-event delay** command. **Table 7-192** provides examples of the two commands.

Table 7-192 Functions and their descriptions

Example	Description
[HUAWEI-bgp] **nexthop recursive-lookup delay**	The device responds to all BGP next-hop recursion changes after a 5-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup non-critical-event delay**	The device immediately responds to urgent BGP next-hop recursion changes and responds to non-urgent BGP next-hop recursion changes after a 5-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup delay 3**	The device responds to all BGP next-hop recursion changes after a 3-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup non-critical-event delay 6**	The device immediately responds to urgent BGP next-hop recursion changes and responds to non-urgent BGP next-hop recursion changes after a 6-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup delay** [HUAWEI-bgp] **nexthop recursive-lookup non-critical-event delay**	The device responds to all BGP next-hop recursion changes after a 5-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup delay 3** [HUAWEI-bgp] **nexthop recursive-lookup non-critical-event delay**	The device responds to urgent BGP next-hop recursion changes after a 3-second delay and responds to non-urgent BGP next-hop recursion changes after a 5-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup delay 3** [HUAWEI-bgp] **nexthop recursive-lookup non-critical-event delay 6**	The device responds to urgent BGP next-hop recursion changes after a 3-second delay and responds to non-urgent BGP next-hop recursion changes after a 6-second delay.
[HUAWEI-bgp] **nexthop recursive-lookup delay** [HUAWEI-bgp] **nexthop recursive-lookup non-critical-event delay 6**	The device responds to urgent BGP next-hop recursion changes after a 5-second delay and responds to non-urgent BGP next-hop recursion changes after a 6-second delay.

Precautions

The delay time specified in the **nexthop recursive-lookup non-critical-event delay** command must be greater than or equal to that specified in the **nexthop recursive-lookup delay** command if both commands are run.

Example

Enable the device to respond to non-urgent BGP next-hop recursion changes after a **10**-second delay.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] nexthop recursive-lookup non-critical-event delay 10
```

7.8.100 out-delay

Function

The **out-delay** command configures a delay for sending Update packets to all BGP peers.

The **undo out-delay** command deletes the configured delay value.

The default delay value is 0, indicating that the intermediate device on the primary path sends Update packets without a delay.

Format

out-delay *delay-value*

undo out-delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay for sending Update packets.	The value is an integer that ranges from 0 to 3600, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario with both primary and backup routes, traffic may be lost after it switches back to the primary path. Use a VPN FRR scenario as an example. PE3 and CE2 connect both to PE1 and PE2. The primary path is PE3 -> PE1 -> CE2, and the backup path is PE3 -> PE2 -> CE2. CE2 uses BGP to communicate with PE1 and PE2. FRR is configured on PE3. If PE1 restarts or the link between PE3 and PE1 fails, traffic switches from the primary path to the backup path. After the primary path recovers, traffic switches back to the primary path. If PE3 completes refreshing forwarding entries before PE1 does, PE1 may temporarily fail to forward traffic from PE3, and packet loss may occur. The severity of packet loss is proportional to the number of routes stored on PE1.

To solve this problem, run the **out-delay** command on PE1 to configure a delay for sending Update packets. An appropriate delay ensures that traffic switches back to the primary path after PE1 completes refreshing forwarding entries.

To configure a delay for sending Update packets to all BGP peers, run the **out-delay** command. To configure a delay for sending Update packets to a specified BGP peer or peer group, run the **peer out-delay** command.

Precautions

If you run the **peer out-delay** command more than once, the latest configuration overrides the previous one.

If the **out-delay** and **peer route-update-interval** commands are both configured, only the **out-delay** command takes effect.

If a network has high route convergence requirements, do no use the **out-delay** command.

Example

Set the delay for sending Update packets to all BGP peers to 300s in the BGP view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] out-delay 300
```

7.8.101 peer advertise-community

Function

The **peer advertise-community** command configures a device to advertise a community attribute to its peer or peer group.

The **undo peer advertise-community** command restores the default setting.

By default, a device advertises no community attribute to its peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP L2VPN-AD address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer advertise-community** command is used to configure a device to advertise a community attribute to its peer or peer group. If a device advertises a community attribute to its peer group, all the members of the peer group will inherit the configuration. This simplifies the application of routing policies and facilitates route maintenance and management.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A specific community attribute has been defined in a routing policy.

Example

Configure a device to advertise a community attribute to its peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 advertise-community
```

7.8.102 peer advertise-ext-community

Function

The **peer advertise-ext-community** command enables a device to advertise an extended community attribute to its peer or peer group.

The **undo peer advertise-ext-community** command restores the default setting.

By default, a device advertises no extended community attribute to its peer or peer group.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

peer { *group-name* | *ipv6-address* } **advertise-ext-community**

undo peer { *group-name* | *ipv6-address* } **advertise-ext-community**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer advertise-ext-community** command is used to enable a device to advertise an extended community attribute to a specified peer or peer group. If a device advertises an extended community attribute to a specified peer group, all the members of the peer group will inherit the configuration. This simplifies the application of routing policies and facilitates route maintenance and management.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A specific extended community attribute has been defined in a routing policy.

Example

Configure a device to advertise an extended community attribute to its peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 2:3::4:5 as-number 200
[HUAWEI-bgp] ipv6-family vpn-instance abc
[HUAWEI-bgp6-abc] peer 2:3::4:5 as-number 200
[HUAWEI-bgp6-abc] peer 2:3::4:5 advertise-ext-community
```

7.8.103 peer allow-as-loop

Function

The **peer allow-as-loop** command sets the number of local AS number repetitions.

The **undo peer allow-as-loop** command restores the default setting.

By default, the local AS number cannot be repeated.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop** [*number*] [**global-as** [**vpn-as**]]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop** [*number*] [**global-as** [**vpn-as**]]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
number	Specifies the number of local AS number repetitions.	The value is an integer in the range from 1 to 10. The default value is 1.
global-as	Specifies a global AS number of BGP.	-
vpn-as	Specifies the AS number of a VPN instance.	-

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, and BGP L2VPN-AD address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.
- The **global-as** and **vpn-as** parameters apply only to BGP VPN instance IPv4 and BGP VPN instance IPv6 address family views.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view , BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP uses AS numbers to detect routing loops. The AS numbers in the AS_Path of each received route are matched against the local AS number configured using the **bgp** command, the fake AS number configured using the **peer fake-as** command, and the VPN instance AS number configured using the **as-number** command. The largest number of times any of the configured AS numbers is repeated is considered as the maximum number. In the Hub and Spoke networking, if EBGP runs between a Hub-PE and a Hub-CE on a Hub site, the route sent from the Hub-PE to the Hub-CE carries the AS number of the Hub-PE. If the Hub-CE sends a routing update to the Hub-PE, the Hub-PE will deny it because the routing update contains the AS number of the Hub-PE.

To ensure proper route transmission in the Hub and Spoke networking, configure all the BGP peers on the path, along which the Hub-CE advertises private network routes to the Spoke-CE, to accept the routes in which the AS number repeats once.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer allow-as-loop** command is run for a peer or peer group multiple times, the latest configuration overrides the previous one.

Example

Set the number of local AS number repetitions to 2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 allow-as-loop 2
```

7.8.104 peer as-number

Function

The **peer as-number** command creates a peer or configures an AS number for a specified peer group.

The **undo peer as-number** command deletes a specified peer or the AS number of a specified peer group.

By default, no BGP peer is configured, and no AS number is specified for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-number** { *as-number-plain* | *as-number-dot* }

peer *group-name* **as-number** { *as-number-plain* | *as-number-dot* } [**optional-as** { *optional-as-number-plain* | *optional-as-number-dot* } &<1-5>]

undo peer { *group-name* **as-number** | *ipv4-address* | *ipv6-address* }

undo peer *group-name* **as-number** { *as-number-plain* | *as-number-dot* } [**optional-as** { *optional-as-number-plain* | *optional-as-number-dot* } &<1-5>]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer. The IPv4 address can be the IP address of an interface that is directly connected to the peer or the IP address of a loopback interface of the reachable peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
optional-as	Specifies an optional AS number.	-
optional-as-number-plain	Specifies an integral optional AS number.	The value is an integer that ranges from 1 to 4294967295.
optional-as-number-dot	Specifies an optional AS number in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer** { *ipv4-address* | *ipv6-address* } **as-number** { *as-number-plain* | *as-number-dot* } command is used to create a BGP peer.

The **peer** *group-name* **as-number** { *as-number-plain* | *as-number-dot* } command is used to configure an AS number for a specified peer group.

Dynamic peers on the same network segment must be added to the same peer group. If the dynamic peers reside in different ASs, run the **peer** *group-name* **as-number** { *as-number-plain* | *as-number-dot* } **optional-as** { *optional-as-number-plain* | *optional-as-number-dot* } &<1-5> command to configure an optional AS number for the peer group.

Precautions

If a peer does not join any peer group or the peer group to which a peer belongs is not configured with an AS number, deleting the AS number of the peer will reset the peer relationship.

If a peer in a peer group is not configured with an AS number, deleting the AS number of the peer group will interrupt the connection on the peer.

The AS number of an external peer group must be different from the local AS number.

Example

Set the AS number to 100 for IPv4 peer 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.1 as-number 100
```

Set the AS number to 100 for a peer group named test.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group test
[HUAWEI-bgp] peer test as-number 100
```

Set the peer AS number and optional AS number for the peer group named **dynamic-group** to 65546 and 65547, respectively.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group dynamic-group external
[HUAWEI-bgp] peer dynamic-group as-number 65546 optional-as 65547
```

7.8.105 peer as-path-filter

Function

The **peer as-path-filter** command configures a BGP route filtering policy based on an AS_Path list for a peer or peer group.

The **undo peer as-path-filter** command cancels the existing configuration.

By default, no route filtering policy based on an AS_Path list is configured for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
as-path-filter-number	Specifies the number of an AS_Path filter.	The value is an integer that ranges from 1 to 256.

Parameter	Description	Value
as-path-filter-name	Specifies the name of an AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters. It cannot be all numbers. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a route filtering policy to received routes.	-
export	Applies a route filtering policy to routes to be advertised.	-

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer as-path-filter** command is used to apply a route filtering policy based on an AS_Path list to BGP routes, the routes that do not match the policy are filtered out.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

The **ip as-path-filter** command has been run to define an AS-Path filter.

Precautions

Only one AS_Path filter can be used to filter the routes received from the same peer. Similarly, only one AS_Path filter can be used to filter routes to be advertised to the same peer.

Creating an AS_Path filter before it is referenced is recommended. By default, the command in an IPv4 address family cannot reference a non-existent AS_Path filter, but the command in an IPv6 address family can reference a non-existent AS_Path filter. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent AS_Path filter is referenced using the current command, all routes are advertised to the specified peer, or all routes advertised by the specified peer are accepted.

Example

Configure an AS_Path filter for a peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 as-path-filter 3 export
```

7.8.106 peer bfd

Function

The **peer bfd** command sets BFD detection parameters for a peer or peer group.

The **undo peer bfd** command restores default BFD detection parameter values.

By default, the interval for sending BFD packets is 1000 ms, the interval for receiving BFD packets is 1000 ms, and the local detection multiplier is 3.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* } *

peer { *group-name* | *ipv6-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* } *

undo peer { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo peer { *group-name* | *ipv6-address* } **bfd** { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo peer { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* } *

undo peer { *group-name* | *ipv6-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
min-tx-interval *min-tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-rx-interval *min-rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection time multiplier.	The value is an integer that ranges from 3 to 50. By default, the value is 3.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD provides millisecond-level fault detection. It helps BGP to detect faults in neighboring devices or links more quickly, and instructs BGP to recalculate routes for correct packet forwarding. The **peer bfd** command can be used to set the values of BFD session parameters on a specified interface.

The BFD configuration of a peer takes precedence over that of the peer group to which the peer belongs. If BFD is not configured on a peer and the peer group to which the peer belongs is enabled with BFD, the peer will inherit the BFD configurations of the peer group.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A BFD session can be established only when the corresponding BGP session is in the Established state.

Precautions

If the **peer bfd** command is run multiple times, the latest configuration overwrites the previous one. The BFD session uses the latest parameters as the detection parameters.

Assume that BFD is configured on a peer group. If the **peer bfd block** command is not run on members of the peer group, the members will establish BFD sessions.

If BFD parameters are set on a peer, a BFD session will be established by using the BFD parameters on the peer.

Example

Configure BFD and set detection parameters on peer 10.2.2.9.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.2.2.9 as-number 200
[HUAWEI-bgp] peer 10.2.2.9 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 5
```

7.8.107 peer bfd block

Function

The **peer bfd block** command prevents a peer from inheriting the BFD function of its peer group.

The **undo peer bfd block** command restores the default configuration.

By default, a peer inherits the BFD function from its peer group.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer { *ipv4-address* | *ipv6-address* } **bfd block**

undo peer { *ipv4-address* | *ipv6-address* } **bfd block**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD provides millisecond-level fault detection. It helps BGP to detect faults in neighboring devices or links more quickly, and instructs BGP to recalculate routes for correct packet forwarding. If a peer group is configured with BFD, all members of the peer group will establish BFD sessions. The **peer bfd block** command can be used to prevent a peer from inheriting the BFD function from its peer group.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A BFD session has been established.

Precautions

After the **peer bfd block** command is run on a peer, the corresponding BFD session on the peer is deleted. As a result, fast link fault detection cannot be implemented.

The **peer bfd block** command and the **peer bfd enable** command are mutually exclusive. After the **peer bfd block** command is run, related BFD sessions are automatically deleted.

Example

Prevent peer 10.2.2.9 from inheriting the BFD function of its peer group.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.2.2.9 as-number 200
[HUAWEI-bgp] peer 10.2.2.9 bfd block
```

7.8.108 peer bfd enable

Function

The **peer bfd enable** command enables BFD for peers or a peer group.

The **undo peer bfd enable** command disables BFD for peers or a peer group.

By default, BFD is disabled for peers or a peer group.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **bfd enable** [**single-hop-prefer**]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **bfd enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
single-hop-prefer	Indicates that single-hop BFD sessions are preferentially established. **single-hop-prefer** takes effect only on IBGP peers. By default, **single-hop-prefer** is not specified, and multi-hop sessions are established between direct IBGP peers (Huawei devices). To interconnect a Huawei device and a non-Huawei device that defaults the sessions between IBGP peers to single-hop, configure **single-hop-prefer** in the command.	-

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP uses BFD to quickly detect faults in links between BGP4 peers. This accelerates network convergence. The **peer bfd enable** command is used to configure a device to establish a BFD session with its peer or peer group by using default detection parameter values.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A BFD session can be established only when the corresponding BGP peer relationship is in the Established state.

Precautions

The BFD configuration of a peer takes precedence over that of the peer group to which the peer belongs. If BFD is not configured on a peer and the peer group to which the peer belongs is enabled with BFD, the peer inherits the BFD configurations from the peer group.

Before enabling BFD on a BGP peer, enable BFD in the system view. If no BFD detection parameter is specified, a BFD session is established by using default parameter values.

NOTE

The **peer bfd block** command and the **peer bfd enable** command are mutually exclusive.

Example

Configure BFD for peer 10.2.2.9.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.2.2.9 as-number 200
[HUAWEI-bgp] peer 10.2.2.9 bfd enable
```

7.8.109 peer capability-advertise

Function

The **peer capability-advertise** command enables a BGP device to advertise optional BGP capabilities to its peer.

The **undo peer capability-advertise** command restores the default setting.

By default, a BGP device advertises route-refresh and 4-byte AS number capabilities to its peer.

Format

peer { *group-name* | *ipv4-address* } **capability-advertise** { **4-byte-as** | **route-refresh** | **conventional** }

peer *ipv6-address* **capability-advertise** { **4-byte-as** | **route-refresh** }

undo peer { *group-name* | *ipv4-address* } **capability-advertise** { **4-byte-as** | **route-refresh** | **conventional** }

undo peer *ipv6-address* **capability-advertise** { **4-byte-as** | **route-refresh** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
4-byte-as	Indicates the 4-byte AS number capability.	-
route-refresh	Indicates the route-refresh capability.	-

Parameter	Description	Value
conventional	Indicates the regular router capability.	-

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer capability-advertise route-refresh** command is used to configure a device to advertise the route-refresh capability to its peer.

The **peer capability-advertise conventional** command is used to configure a device to advertise the regular router capability to its peer. If **conventional** is specified in the command, the router does not have all extension functions such as route-refresh capability, GR capability, and multi-address family negotiation. This allows the router to be compatible with routers of earlier versions.

The **peer capability-advertise 4-byte-as** command is used to configure a device to advertise the 4-byte AS number capability to its peer. If AS number resources are used up, this command can be used to configure devices to use 4-byte AS numbers.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

The corresponding BGP session must be in the Established state.

Precautions

If you enable or disable the route-refresh, general router, or 4-byte AS number function, the BGP peer relationship will be re-established, which can lead to a temporary network interruption. Therefore, exercise caution when running the related commands.

Example

Configure a BGP device to advertise the route-refresh capability to its peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.89.2.33 as-number 100
[HUAWEI-bgp] peer 10.89.2.33 capability-advertise route-refresh
```

7.8.110 peer connect-interface

Function

The **peer connect-interface** command specifies a source interface from which BGP packets are sent, and a source address used for initiating a connection.

The **undo peer connect-interface** command restores the default setting.

By default, the outbound interface of a BGP packet serves as the source interface of the BGP packet.

Format

peer { *group-name* | *ipv4-address* } **connect-interface** *interface-type interface-number* [*ipv4-source-address*]

peer { *group-name* | *ipv6-address* } **connect-interface** *interface-type interface-number* [*ipv6-source-address*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **connect-interface**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of an interface.	-
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv4-source-address	Specifies an IPv4 source address used for establishing a connection.	It is in dotted decimal notation.
ipv6-source-address	Specifies an IPv6 source address used for establishing a connection.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command is used in the following scenarios:

- To establish a BGP peer connection between two indirectly connected physical interfaces, the **peer connect-interface** command must be run on both sides.

  To establish a BGP peer connection between a local loopback interface and a remote interface, the loopback interface must be specified as the source interface in the command. To establish a BGP peer connection between a local physical interface and a remote interface, the physical interface must be specified as the source interface in the command.
- If multiple IP addresses are configured for the physical interface that needs a BGP peer connection established with a remote interface, the **peer connect-interface** command must be run, with *ipv4-source-address* or *ipv6-source-address* set to the source IP address.
- If two devices need multiple BGP peer connections established through different interfaces, the **peer connect-interface** command must be run for each BGP peer connection, with the source interface specified.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

Running the **peer connect-interface** command causes the teardown and re-establishment of peer relationships.

NOTE

Because the BGP peer relationships in various address families on the same device share one TCP connection, **connect-interface** configured in the BGP view can be inherited in the IPv4 unicast address family.

To enable a device to send BGP packets even if its physical interface fails, you can configure the device to use a loopback interface as the source interface of the BGP packets. When configuring a device to use a loopback interface as the source interface of BGP packets, note the following points:

- The loopback interface of the device's BGP peer must be reachable.
- In the case of an EBGP connection, the **peer ebgp-max-hop** command needs to be run to enable the two devices to establish an indirect peer relationship.

NOTE

If the specified interface borrows the IP address of another interface and then the IP address of the specified interface is changed, BGP still uses the borrowed IP address to keep the connection if no connection reestablishment is triggered, and data receiving and sending is not affected; if connection reestablishment is triggered, BGP uses the new IP address to reestablish the connection.

Example

Specify a source interface for sending BGP packets and a source address for initiating a connection.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.16.2.3 as-number 100
[HUAWEI-bgp] peer 10.16.2.3 connect-interface vlanif 100
```

7.8.111 peer connected-check-ignore

Function

The **peer connected-check-ignore** command configures a device not to check the hop count when establishing a one-hop EBGP peer relationship using loopback interface addresses.

The **undo peer connected-check-ignore** command cancels the configuration.

By default, a device checks the hop count when establishing a one-hop EBGP peer relationship using loopback interface addresses.

Format

peer{ *group-name* | *ipv4-address* | *ipv6-address* } **connected-check-ignore**

undo peer{ *group-name* | *ipv4-address* | *ipv6-address* } **connected-check-ignore**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The value is a string of 1 to 47 case-sensitive characters, spaces not supported.
ipv4-address	Specifies the IPv4 address of a peer.	-
ipv6-address	Specifies the IPv6 address of a peer.	-

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow one-hop EBGP peer relationships to be established using loopback interface addresses, run the **peer connected-check-ignore** command or the **peer ebgp-max-hop** command (in which *hop-count* is greater than or equal to 2).

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer connected-check-ignore** command is used on one end of an EBGP connection, it must also be used on the other end.

Example

Configure the device not to check the hop count when establishing a one-hop EBGP peer relationship using loopback interface addresses.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 connected-check-ignore
```

7.8.112 peer default-route-advertise

Function

The **peer default-route-advertise** command configures a BGP device to advertise a default route to its peer or peer group.

The **undo peer default-route-advertise** command restores the default setting.

By default, a BGP device does not advertise default routes to its peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*] [**conditional-route-match-all** { *ipv4-address1* { *mask1* | *mask-length1* } } &<1-4> | **conditional-route-match-any** { *ipv4-address2* { *mask2* | *mask-length2* } } &<1-4>]

peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*] [**conditional-route-match-all** { *ipv6-address1* *prefix-length1* } &<1-4> | **conditional-route-match-any** { *ipv6-address2* *prefix-length2* } &<1-4>]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
prefix-length1	Specifies the IPv6 prefix range using the mask length.	The value is an integer that ranges from 0 to 128. If ::0 less-equal 128 is used, all IPv6 addresses will be matched.
prefix-length2	Specifies the IPv6 prefix range using the mask length.	The value is an integer that ranges from 0 to 128. If ::0 less-equal 128 is used, all IPv6 addresses will be matched.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
conditional-route-match-all	Configures the BGP device to send default routes to a peer or peer group when the routing table contains all conditional routes.	-

Parameter	Description	Value
ipv4-address1	Specifies the IPv4 address of conditional routes.	The value is in dotted decimal notation.
ipv6-address1	Specifies the IPv6 address of conditional routes.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
mask1	Specifies the mask of conditional routes.	The value is in dotted decimal notation.
mask-length1	Specifies the mask length of conditional routes.	The value is an integer that ranges from 0 to 32.
conditional-route-match-any	Configures the BGP device to send default routes to a peer or peer group when the routing table contains any conditional route.	-
ipv4-address2	Specifies the IPv4 address of conditional routes.	The value is in dotted decimal notation.
ipv6-address2	Specifies the IPv6 address of conditional routes.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
mask2	Specifies the mask of conditional routes.	The value is in dotted decimal notation.
mask-length2	Specifies the mask length of conditional routes.	The value is an integer that ranges from 0 to 32.

NOTE

- *ipv4-address* is only valid in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is only valid in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.
- **conditional-route-match-all** and **conditional-route-match-any** are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv4 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Default routes are commonly used on a network that meets the following conditions:

- Each device has multiple EBGP peers and receives all routes on the network from each EBGP peer.
- There are multiple route reflectors (RRs), and each RR receives all routes on the network.

If load balancing is not implemented on the network, a BGP peer receives at most one copy of active routes on the network. If load balancing is implemented on the network, the number of active routes received by a BGP peer will be increased by multiple times, causing the number of routes on the network to sharply increase. To greatly reduce the number of routes on such a network, configure a BGP device to advertise only default routes to its BGP peer and use default routes for traffic load balancing.

Prerequisites

BGP peer relationships have been established using the **peer as-number** command.

Precautions

After this command is run, a BGP device sends a default route with the next hop as itself to its peer or peer group regardless of whether default routes exist in the routing table.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the attributes of the default route to be advertised to the specified peer or peer group are not changed.

Example

Configure a BGP device to advertise a default route to its peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 default-route-advertise
```

7.8.113 peer description (BGP)

Function

The **peer description** command configures a description for a peer or peer group.

The **undo peer description** command deletes the description of a peer or peer group.

By default, no description is configured for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **description** *description-text*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **description**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
description-text	Specifies a description, which can be letters and digits.	The value is a string of 1 to 80 characters, with spaces supported.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer description** can be used to configure a description for a peer or peer group, which facilitates management of peers or peer groups. The description records information about the peer or peer group, such as the VPN instance to which the peer or peer group belongs, and devices that establish peer relationships with the peer or peer group.

Precautions

The description configured by using the **peer description** command for a peer is displayed from the first non-space character, and a maximum of 80 characters can be displayed.

Follow-up Procedure

You can run **display bgp peer** *ipv4-address* **verbose** command can be used to view the description of a peer.

Example

Configure a description for a peer group named group1.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group group1
[HUAWEI-bgp] peer group1 description ISP1
```

7.8.114 peer ebgp-max-hop

Function

The **peer ebgp-max-hop** command configures a BGP device to establish an EBGP peer relationship with a peer on an indirectly-connected network and set the maximum number of hops between the two devices.

The **undo peer ebgp-max-hop** command restores the default setting.

By default, an EBGP connection can be set up only on a directly-connected physical link.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ebgp-max-hop**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
hop-count	Specifies the maximum number of hops.	The value is an integer that ranges from 1 to 255. The default value is 255. If the maximum number of hops is 1, a device cannot establish an EBGP connection with a peer on an indirectly-connected network.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A directly-connected physical link must be available between EBGP peers. Otherwise, the **peer ebgp-max-hop** command must be used to allow EBGP peers to establish a TCP connection over multiple hops.

If loopback interfaces are used to establish an EBGP peer relationship, the **peer ebgp-max-hop** command (*hop-count* ≥ 2) must be run; otherwise, the peer relationship cannot be established. If a one-hop EBGP peer relationship is established using loopback interface addresses, you can also run the **peer connected-check-ignore** command to establish an EBGP peer relationship.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer ebgp-max-hop** command is used on one end of an EBGP connection, it must also be used on the other end.

The configurations of GTSM and EBGP-MAX-HOP affect the TTL values of sent BGP packets, and the configurations of the two functions are mutually exclusive.

Example

Allow an indirectly connected EBGP peer with the IP address of 10.1.1.2 to establish a connection with the local device.

```
<HUAWEI> system-view
```

```
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 ebgp-max-hop
```

7.8.115 peer enable (BGP)

Function

The **peer enable** command enables a BGP device to exchange routes with a specified peer or peer group in the address family view.

The **undo peer enable** command disables a BGP device from exchanging routes with a specified peer or peer group.

By default, only the peer in the BGP IPv4 unicast address family view is automatically enabled.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **enable**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view,BGP-MDT address family view, BGP-MVPN address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, and BGP L2VPN-AD address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, only the peer in the BGP IPv4 unicast address family view is automatically enabled. After the **peer as-number** command is used in the BGP view, the system automatically runs the **peer enable** command to enable a peer. In other address family views, however, a peer must be enabled manually.

After the **undo default ipv4-unicast** command is run, the **peer enable** command needs to be run in the BGP view or the BGP-IPv4 unicast address family view to enable the IPv4 unicast address family for the created BGP peer.

Precautions

Enabling or disabling a BGP peer in an address family, for example, running the **peer enable** command or the **undo peer enable** command in a VPNv4 address family, causes teardown and re-establishment of the BGP connection of the peer in other address families.

Example

Disable a BGP device from exchanging IPv4 routes with a specified peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] undo peer 10.1.1.2 enable
```

7.8.116 peer fake-as

Function

The **peer fake-as** command specifies a fake AS number for a local peer.

The **undo peer fake-as** command restores the default setting.

By default, a peer uses the actual local AS number.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **fake-as** { *as-number-plain* | *as-number-dot* } [**prepend-global-as**]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **fake-as**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.
prepend-global-as	Indicates that the actual AS number is added to packets to be sent.	-

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer fake-as** command is often used for network deployment changing of carriers' networks. For example, if carrier A purchases the network of carrier B and the networks of the two carriers belong to different ASs, the ASs of the two carriers need to be combined and the AS number of carrier B needs to be changed to the AS number of carrier A. BGP peers (in another AS) of devices on carrier B's network may not be willing to have their BGP configurations changed or changed immediately during network combination. As a result, the connections with these BGP peers will be interrupted.

To ensure that the ASs are combined properly, you can run the **peer fake-as** command on the ASBR on carrier's B network to set the AS number of carrier B to the fake AS number of carrier A. This setting enables the BGP peers of devices in carrier B's network to use the fake AS number to set up connections.

NOTE

If **prepend-global-as** is specified in the command and the local end establishes an EBGP peer relationship with the remote end using the fake AS number, the local end adds the actual AS number to the packets to be sent to the remote end.

Prerequisites

Peers have been created by using the **peer as-number** command.

Precautions

If the **peer fake-as** command is run several times for a peer or a peer group, the latest configuration will overwrite the previous one.

The **peer fake-as** command takes effect only for EBGP peers, and the configured fake AS number cannot be the same as the peer AS number.

After the 4-byte AS number capability is disabled on a peer, configuring a 4-byte fake AS number for the peer may cause a failure to establish a BGP session.

Example

Set a 2-byte fake AS number for a peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 fake-as 99
```

Set a 4-byte fake AS number for a peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 fake-as 100.200
```

7.8.117 peer filter-policy

Function

The **peer filter-policy** command configures a filtering policy to advertise routes to or receive routes from peers or peer group.

The **undo peer filter-policy** command deletes the filtering policy used to advertise routes to or receive routes from peers or peer group.

By default, no filtering policy is configured to advertise routes to or receive routes from peers or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** { *acl-number* | **acl-name** *acl-name* | *acl6-number* | **acl6-name** *acl6-name* } { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** { *acl-number* | **acl-name** *acl-name* | *acl6-number* | **acl6-name** *acl6-name* } { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The name should start with a letter and can contain numbers, hyphens (-), or underscores (_).
import	Filters received routes.	-
export	Filters routes to be advertised.	-

NOTE

- *ipv4-address*, **acl-name** *acl-name*, and *acl-number* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address*, **acl6-name** *acl6-name*, and *acl6-number* are valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer filter-policy** command is used to configure an ACL-based policy for filtering routes received from peers or routes to be advertised to peers.

A proper basic ACL needs to be selected based on the address family of a peer or peer group.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A basic ACL needs to be configured.

Precautions

If the **peer filter-policy** command is run multiple times, the latest configuration overwrites the previous one. For example, if the **peer 10.1.1.2 filter-policy 2600 import** command is run and then the **peer 10.1.1.2 filter-policy 2400 import** command is run, the configuration of the **peer 10.1.1.2 filter-policy 2400 import** command overwrites that of the **peer 10.1.1.2 filter-policy 2600 import** command.

When the **rule** command is run to configure rules for an ACL, only the source address range specified by **source** and the time period specified by **time-range** take effect.

Example

Set the IPv4 filtering policy for peers.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit
[HUAWEI-acl-basic-2000] quit
[HUAWEI] bgp 100
```

```
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 filter-policy 2000 import
```

Set the IPv6 filtering policy for peers.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2001
[HUAWEI-acl6-basic-2001] rule permit
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] bgp 100
[HUAWEI-bgp] peer fc00:0:0:2::3 as-number 200
[HUAWEI-bgp] ipv6-family unicast
[HUAWEI-bgp-af-ipv6] peer fc00:0:0:2::3 filter-policy 2000 import
```

7.8.118 peer group

Function

The **peer group** command adds a peer to a peer group.

The **undo peer group** command deletes a peer from a peer group and all configurations of the peer.

By default, no peer is in peer group.

Format

peer { *ipv4-address* | *ipv6-address* } **group** *group-name*

undo peer { *ipv4-address* | *ipv6-address* } **group** *group-name*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view, and BGP-EVPN address family view.
- *ipv6-address* is valid only in the BGP view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view, BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale BGP network, there are a large number of peers and many of them have the same routing policies. To configure these peers, you have to repeatedly use some commands. In such a case, configuring peer groups can simplify configurations. If you intend to perform the same configuration on several peers, create and configure a peer group. Then, add the peers to the peer group. The peers will inherit the configurations of the peer group.

Precautions

- Peers with different AS numbers can be added to the same peer group. If a peer has an AS number, the peer keeps its own AS number after being added to a peer group. If a peer has no AS number but the peer group to which the peer will be added has an AS number, the peer inherits the AS number of the peer group after being added to the peer group.
- The members of a peer group can be configured with different route receiving and advertising policies.
- The **undo peer group** command has the same function with the **undo peer** command and the **undo peer enable** command.
- By default, only the IPv4 peers configured in the BGP-IPv4 unicast address family view are automatically added to a peer group. That is, after the **peer** *ipv4-address* **group** *group-name* command is configured in the BGP view, the system configures the **peer** *ipv4-address* **group** *group-name* command in the BGP-IPv4 unicast address family view. In other address family views, peers must be manually added to a peer group.

Example

Create an IBGP peer group named test, and then add a peer to it.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group test internal
[HUAWEI-bgp] peer 10.1.1.1 group test
```

Create an EBGP peer group named **test** and add an IPv6 peer to this peer group.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group test external
```

```
[HUAWEI-bgp] peer 2001:db8:1::1 as-number 200
[HUAWEI-bgp] peer 2001:db8:1::1 group test
[HUAWEI-bgp] ipv6-family unicast
[HUAWEI-bgp-af-ipv6] peer test enable
[HUAWEI-bgp-af-ipv6] peer 2001:db8:1::1 group test
```

7.8.119 peer ignore

Function

The **peer ignore** command prevents a BGP device from establishing a session with a peer or peer group.

The **undo peer ignore** command permits a BGP device from establishing a session with a peer or peer group.

By default, the device is permitted to set up the session with the BGP peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **ignore**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ignore**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-VPN instance IPv4 address family view, and BGP-VPN instance IPv6 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a BGP device needs to transitorily close the session with a peer and reconfiguring the peer requires too much workload, the **peer ignore** command can be used to avoid the reconfiguration of the peer. For example, if the peer relationship frequently alternates between Up and Down because of the upgrade of a peer or the adjustment of the link, the BGP peer relationship needs to be interrupted temporarily. In this case, the **peer ignore** command can be used on the stabler end to prevent frequent flapping of the route or peer relationship.

The **peer ignore** command is used to tear down sessions between a BGP device and its peer or peer group and delete all related routing information. In the case of a peer group, a large number of sessions are suddenly torn down.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

After the **peer ignore** command is run on a device, the session between the device and its peer is closed and all the related routing information is cleared.

After a BGP session is successfully established, running the **peer ignore** command interrupts the BGP session. The interrupted BGP session cannot be established again, and the status of the corresponding BGP peer relationship is displayed as Idle.

Running the **peer ignore** command together with the **peer enable** command equals running of the **reset bgp** command. Both methods can be used to configure a device to re-establish a session.

Example

Prohibit a device from establishing any session with peer 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 ignore
```

7.8.120 peer ip-prefix

Function

The **peer ip-prefix** command configures a route filtering policy based on an IP address prefix list for a peer or peer group.

The **undo peer ip-prefix** command cancels the route filtering policy based on an IP address prefix list of a peer or peer group.

By default, no route filtering policy based on an IP address prefix list is configured for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* } **ip-prefix** *ip-prefix-name* { **import** | **export** }

peer { *group-name* | *ipv4-address* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* } **ip-prefix** [*ip-prefix-name*] { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ipv6-prefix** [*ipv6-prefix-name*] { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ip-prefix *ip-prefix-name*	Indicates the filtering policy that is based on the IPv4 prefix list of the peer or peer group.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a filtering policy to the routes received from a peer or peer group.	-
export	Applies a filtering policy to the routes to be advertised to a peer or peer group.	-
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
ipv6-prefix *ipv6-prefix-name*	Indicates the filtering policy that is based on the IPv6 prefix list of the peer or peer group.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer ip-prefix** command can be used to configure a route filtering policy that is based on an IP prefix list to filter routes received or routes to be advertised, implementing route control.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

If the **peer ip-prefix** command specifies an IP prefix list that does not exist for a peer or peer group, use the **ip ip-prefix** or **ip ipv6-prefix** command to create an IP prefix list.

Precautions

If an IP prefix list is specified for a peer group, all the members of the peer group inherit the configuration.

After an IP prefix list is specified for a peer or peer group, the peer or peers in the peer group filter the routes to be advertised to or received from other peers based on the IP prefix list. Only the routes that pass the filtering of the IP prefix list can be advertised or received.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes are advertised to the specified peer, or all routes advertised by the specified peer are accepted.

Example

Configure a route filtering policy based on an IP prefix list.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 ip-prefix list1 import
```

7.8.121 peer keychain (BGP)

Function

The **peer keychain** command configures the keychain authentication for establishing the TCP connection between BGP peers.

The **undo peer keychain** command restores the default setting.

By default, the keychain authentication is not configured for BGP peers.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

peer { *group-name* | *ipv4-address* } **keychain** *keychain-name*

undo peer { *group-name* | *ipv4-address* } **keychain**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
keychain-name	Specifies the name of the keychain authentication.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring keychain authentication improves the security of the TCP connection. You must configure keychain authentication specified for TCP-based applications on both BGP peers. Note that encryption algorithms and passwords configured for the keychain authentication on both peers must be the same; otherwise, the TCP connection cannot be set up between BGP peers and BGP messages cannot be transmitted.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Before configuring the BGP keychain authentication, a keychain in accordance with the configured *keychain-name* must be configured first. For keychain configuration details, see Keychain Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Security*.

Precautions

The **peer keychain** command and the **peer password** command are mutually exclusive. SHA256 and HMAC-SHA256 encryption algorithm are recommended in keychain authentication.

Example

Configure the keychain authentication named test for BGP peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 keychain test
```

7.8.122 peer keep-all-routes

Function

The **peer keep-all-routes** command saves all the BGP routing updates from the specified peer or the peer group after the BGP connection is set up, even though those routes do not pass the configured ingress policy.

The **undo peer keep-all-routes** command restores the default setting.

By default, only the BGP routing updates received from the peers and passing the configured ingress policy are saved.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-IPv6 unicast address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After changing a BGP import policy, you can reset BGP connections for the new import policy to take effect immediately, interrupting these BGP connections temporarily. If a device's peer does not support route-refresh, the **peer keep-all-routes** command can be used on the device to remain all routing updates received from the peer so that the device can refresh its routing table without closing the connection with the peer.

Precautions

If the switch does not support the route-refresh capability, the **peer keep-all-routes** command needs to be run on the switch and its peer. If the **peer keep-all-routes** command is run on a device for the first time, the sessions between the device and its peers will be reestablished.

If the switch supports the route-refresh capability, running this command does not result in re-establishment of the sessions between the switch and its peers. After the **refresh bgp** command is run on the switch, however, the switch does not refresh its routing table.

NOTE

If the switch supports the route-refresh capability, the **peer keep-all-routes** command does not need to be run on it.

Example

Configure a device to store all BGP routing updates received from its IPv4 peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 keep-all-routes
```

7.8.123 peer label-route-capability (BGP)

Function

The **peer label-route-capability** command enables a BGP device to send labeled routes to a specified peer or peer group.

The **undo peer label-route-capability** command disables this function.

By default, this function is disabled.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

BGP view and BGP-IPv4 unicast address family view:

peer { *group-name* | *ipv4-address* } **label-route-capability** [**check-tunnel-reachable**]

undo peer { *group-name* | *ipv4-address* } **label-route-capability**

BGP-IPv6 unicast address family view:

peer *ipv4-address* **label-route-capability**

undo peer *ipv4-address* **label-route-capability**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
check-tunnel-reachable	Checks tunnel reachability when imported routes are sent as labeled routes.	-

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

When the capability of sending labeled routes is enabled or disabled, BGP connection is automatically closed and the capability of the neighbor is re-negotiated.

To configure IPv6 provider edge (6PE), specify the peer as an IPv4 unicast address in the IPv6 unicast address family view.

Tunnel reachability checking can only be used to check tunnels on IPv4 public networks.

- If tunnel reachability checking is enabled, BGP advertises IPv4 unicast routes to peers when routed tunnels are unreachable or advertises labeled routes to peers when routed tunnels are reachable. This eliminates the risk of establishing an MP-EBGP peer relationship between PEs over a faulty label switched path (LSP) because this will cause data forwarding failures.
- If tunnel reachability checking is disabled, BGP advertises labeled routes to peers whether the tunnels for imported routes are reachable or not.

NOTE

To disable tunnel reachability checking, run the **peer** { *group-name* | *ipv4-address* } **label-route-capability** command, not the **undo peer label-route-capability** command.

Before you run the **peer label-route-capability** command, the **peer as-number** command should be used to create a peer or peer group.

Example

Enable BGP to send the labeled routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 200
[HUAWEI-bgp] peer 10.2.3.4 as-number 200
[HUAWEI-bgp] ipv6-family
[HUAWEI-bgp-af-ipv6] peer 10.2.3.4 enable
[HUAWEI-bgp-af-ipv6] peer 10.2.3.4 label-route-capability
```

7.8.124 peer listen-net

Function

The **peer listen-net** command configures BGP to listen to BGP connection requests from a specified network segment and establish BGP peer relationships dynamically.

The **undo peer listen-net** command restores the default configuration.

By default, BGP does not listen to BGP connection requests from any network segment.

Format

peer *group-name* **listen-net** *network* { *mask* | *mask-length* }

undo peer *group-name* **listen-net** *network* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
network	Specifies the address of the network segment from which BGP listens to BGP connection requests.	The value is in dotted decimal notation.
mask	Specifies the mask of the network segment from which BGP listens to BGP connection requests.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the network segment from which BGP listens to BGP connection requests.	The value is an integer ranging from 0 to 32.

Views

BGP or BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple BGP peers reside on the same network segment, and the number of the peers may change, you can run the **peer listen-net** command to configure BGP to listen to BGP connection requests from the network segment, establish BGP peer relationships dynamically, and add the peers to a peer group. This spares the local device from adding or deleting BGP peer configurations in response to each change in the peer number, which reduces the maintenance workload.

Prerequisites

A peer group has been configured using the **group** *group-name* [**external** | **internal**] command.

Precautions

If you run the command multiple times, BGP listens to BGP connection requests from multiple network segments.

Example

Configure BGP to listen to BGP connection requests from network segment 10.1.1.0/24 and establish BGP peer relationships dynamically.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group test internal
[HUAWEI-bgp] peer test listen-net 10.1.1.0 24
```

7.8.125 peer listen-only

Function

The **peer listen-only** command configures a peer or peer group to only detect connection requests and not to initiatively send connection requests.

The **undo peer listen-only** command restores the default setting.

By default, a peer or peer group detects and sends connection requests.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **listen-only**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **listen-only**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer listen-only** command is used to configure a peer or peer group to only detect connection requests and not to initiatively send connection requests.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer listen-only** command is run multiple times, the latest configuration overwrites the previous one.

After the **peer listen-only** command is executed, the local end does not initiate any connection request to a specified peer.

NOTICE

The **peer listen-only** command can be run at only one end of a peer relationship. If this command is run at both ends of a peer relationship, the ends fail to establish a connection.

Example

Configure peer 10.1.1.1 to only detect connection requests from the remote peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.1 as-number 200
[HUAWEI-bgp] peer 10.1.1.1 listen-only
```

7.8.126 peer log-change

Function

The **peer log-change** command enables a BGP device to log the session status and events of a specified peer or a peer group.

The **undo peer log-change** command disables a BGP device to log the session status and events of a specified peer or a peer group.

By default, a BGP device is enabled to log the session status and events of a specified peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **log-change**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **log-change**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

The **peer log-change** command can be used to enable a device to log the session status and events of a specified peer or peer group, facilitating service management.

Peer relationships have been established using the **peer as-number** command.

Example

Configure a BGP device to log the session status and events of peer 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 log-change
```

7.8.127 peer next-hop-invariable

Function

The **peer next-hop-invariable** command configures PEs in different ASs not to change next hops of routes when the PEs advertise them to their EBGP peers, and configures the PEs to use the next hops of imported IGP routes when the PEs advertise them to their IBGP peers.

The **undo peer next-hop-invariable** command restores the default setting.

By default, when advertising routes to its EBGP peers and imported IGP routes to IBGP peers, a BGP speaker changes the next hop to its interface address.

Format

peer { *ipv4-address* | *group-name* } **next-hop-invariable**

undo peer { *ipv4-address* | *group-name* } **next-hop-invariable**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-L2VPN address family view, BGP-VPLS address family view, BGP L2VPN-AD address family view, BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer next-hop-invariable** command is used on a device, the device does not change the next hop of an imported IGP route when advertising the route to its IBGP peers, and does not change the next hop of a route when advertising it to its EBGP peers.

In the inter-AS VPN option C networking where an RR is used, the **peer next-hop-invariable** command needs to be run to configure the RR not to change the next-hop address of a route when advertising the route to an EBGP peer. This ensures that the remote PE recurses a route to the BGP LSP destined for the local PE during traffic transmission.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Configuration Impact

After the **peer next-hop-invariable** command is used on a device, the device does not change the next hop of an imported IGP route when advertising the route to its IBGP peers, and does not change the next hop of a route when advertising it to its EBGP peers.

Precautions

The **peer next-hop-invariable** command configured on EBGP peers takes effect only for VPNv4 and VPNv6 routes.

If a device needs to advertise routes to its IBGP peer or peer group, the **peer next-hop-invariable** and **peer next-hop-local** commands are mutually exclusive on the device.

Example

Configure a BGP device not to change the next hop of a route when the BGP device advertises it to its EBGP peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] peer 10.1.1.2 enable
[HUAWEI-bgp-af-vpnv4] peer 10.1.1.2 next-hop-invariable
```

Use the next hop of an IGP route when advertising the IGP route to IBGP peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 next-hop-invariable
```

7.8.128 peer next-hop-local

Function

The **peer next-hop-local** command configures a BGP device to set its IP address as the next hop of routes when the BGP device advertises routes to an IBGP peer or peer group.

The **undo peer next-hop-local** command restores the default setting.

By default:

- A BGP router sets its interface IP address as the next-hop address of routes when advertising these routes to an EBGP peer.

- A BGP router does not change the next-hop address of non-labeled routes if the routes are from an EBGP peer and are to be sent to an IBGP peer. The router sets its interface IP address as the next-hop address of labeled routes if the routes are from an EBGP peer and are to be sent to an IBGP peer.
- A BGP router does not change the next-hop address of routes if the routes are from an IBGP peer and are to be sent to an IBGP peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **next-hop-local**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **next-hop-local**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, BGP-L2VPN address family view, and BGP L2VPN-AD address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer next-hop-local** command is usually run on an autonomous system boundary router (ASBR). By default, when an ASBR forwards a route learned from an EBGP peer to its IBGP peers, the ASBR does not change the next hop of the route. The next-hop address of a route advertised by an EBGP peer is the address of the EBGP peer. After being forwarded to the IBGP peers, the route cannot become an active route because of the unreachable next hop. The **peer next-hop-local** command needs to be run to configure the ASBR to change the next hop of the route to its IP address when the ASBR advertises the route to an IBGP peer. As an IGP runs within the AS, the next hop of the route is reachable. As such, the route received by the IBGP peer is active.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Precautions

The **peer next-hop-local** command is applicable to IBGP peers.

Regarding non-labeled BGP routes on a public network, running the **peer next-hop-local** command on a route reflector to change the next hop of BGP routes does not take effect.

Regarding labeled BGP routes, running this command on a route reflector to change the next hop of BGP routes takes effect.

Running this command on a local device to change the next hop of routes imported or aggregated by the local device does not take effect.

If a device needs to advertise routes to its IBGP peer or peer group, the **peer next-hop-local** and **peer next-hop-invariable** commands are mutually exclusive on the device.

The **peer next-hop-local** command can be configured in the L2VPN-AD address family view, but the configuration does not take effect.

This command is not supported on RRs in BGP VPNv6 scenarios. If it is incorrectly configured on an RR in a BGP VPNv6 scenario, traffic will be interrupted.

Example

Configure a BGP device to set its IP address as the next hop of routes when advertising the routes to peer 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 next-hop-local
```

7.8.129 peer out-delay

Function

The **peer out-delay** command configures a delay for sending Update packets.

The **undo peer out-delay** command deletes the delay for sending Update packets.

The default delay is 0, indicating that Update packets are sent without a delay.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **out-delay** *delay-value*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **out-delay**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
delay-value	Specifies the delay for sending Update packets.	The value is an integer that ranges from 0 to 3600, in seconds.

NOTE

- The *ipv4-address* parameter applies to the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-VPN instance IPv4 address family view, BGP L2VPN-AD address family view and BGP-EVPN address family view.
- The *ipv6-address* parameter applies to the BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view, BGP L2VPN-AD address family view, BGP-EVPN address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario in which primary and backup routes exist, packets may get lost after traffic switches back to the primary path from the backup path. Use a VPN FRR scenario as an example. PE3 and CE2 connect both to PE1 and PE2. The primary path is PE3 -> PE1 -> CE2, and the backup path is PE3 -> PE2 -> CE2. CE2 uses BGP to communicate with PE1 and PE2. FRR is configured on PE3. If PE1 restarts or the link between PE3 and PE1 is disconnected, traffic switches from the primary path to the backup path. After the primary path recovers, traffic switches back to the primary path. If PE3 completes refreshing forwarding entries before PE1 does so, PE1 may temporarily fail to forward traffic received from PE3, and packet loss may occur. The severity of packet loss is proportional to the number of routes stored on PE1.

To solve this problem, run the **peer out-delay** command on the PE1 to configure a delay for sending Update packets. An appropriate delay ensures that traffic switches back to the primary path after PE1 completes refreshing forwarding entries.

Precautions

If you run the **peer out-delay** command repeatedly, the latest configuration overrides the previous configurations.

If the **peer out-delay** and **peer route-update-interval** commands are both configured, only the **peer out-delay** command takes effect.

If a network has high route convergence requirements, do no use the **peer out-delay** command.

Example

In the BGP view, configure the delay for sending Update packets to 10.1.1.1 as 300s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.1 out-delay 300
```

7.8.130 peer password

Function

The **peer password** command enables a BGP device to implement MD5 authentication for BGP messages exchanged during the establishment of a TCP connection with a peer.

The **undo peer password** command restores the default setting.

By default, a BGP device does not perform MD5 authentication for BGP messages exchanged during the establishment of a TCP connection with a peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **password** { **cipher** *cipher-password* | **simple** *simple-password* }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **password**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
cipher *cipher-password*	Specifies a cipher text password.	The value is a string of case-sensitive characters without spaces. When the value is displayed in plaintext, its length ranges from 1 to 255. When the value is displayed in ciphertext, its length ranges from 20 to 392.
simple *simple-password*	Specifies a plain text password. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of 1 to 255 case-sensitive characters, without spaces.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-VPN instance IPv4 address family view, and BGP-VPN instance IPv6 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP uses TCP as the transport layer protocol. To enhance BGP security, MD5 authentication can be implemented for BGP packets exchanged during the establishment of a TCP connection. MD5 authentication sets the MD5 authentication password for the TCP connection, and the authentication is performed by TCP.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

After the **peer password** command is run, if the MD5 authentication fails, no TCP connection is established.

MD5 authentication and keychain authentication are mutually exclusive on a peer.

After the **peer password** command is run on a device to enable MD5 authentication, the device will re-establish the peer relationship with its peer.

Example

Configure authentication for the TCP connection between a device and peer 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 password cipher test
```

7.8.131 peer preferred-value

Function

The **peer preferred-value** command sets a preferred value for the routes that a BGP device learns from its peer.

The **undo peer preferred-value** command restores the default preferred value for the routes that a BGP device learns from its peer.

By default, the preferred value of a route learned from a BGP peer is 0.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **preferred-value** *value*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **preferred-value**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
value	Specifies the preferred value of the routes that a BGP device learns from its peer.	The value is an integer that ranges from 0 to 65535.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP L2VPN-AD address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer preferred-value** command is run, all the routes learned from the specified peer have the preferred value. If there are multiple routes to the same address prefix, the route with the highest preferred value is preferred.

Prerequisites

A BGP peer has been configured. If the **peer preferred-value** command is used but no BGP peer exists, a message is displayed, indicating that the peer does not exist.

Precautions

If a preferred value is set for the routes that a BGP device learns from a peer group, all members of the peer group inherit the configuration.

Example

Set the preferred value to 50 for the routes that a BGP device learns from a specified peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 preferred-value 50
```

7.8.132 peer public-as-only

Function

The **peer public-as-only** command configures the AS-Path attribute in a BGP Update packet not to carry the private AS number. Only the public AS number is contained in the update packets.

The **undo peer public-as-only** command restores the default setting.

By default, the AS-Path attribute in a BGP Update packet is allowed to carry private AS numbers.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **public-as-only** [**force**]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **public-as-only**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
force	In the following two cases, BGP does not delete the private AS number after the command is used: ● The AS_Path of a route contains the AS number of the peer. In this case, deleting the private AS numbers may lead to a routing loop. ● The AS_Path list contains both public network AS numbers and private AS numbers, indicating that the route has passed through the public network. Deleting the private AS numbers may lead to a forwarding error. To enable the device to delete the private AS numbers from the AS_Path attribute before sending update packets even in the preceding scenarios, specify **force** in the command.	-

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP L2VPN-AD address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In general, an AS number ranges from 1 to 4294967295. The public AS number ranges from 1 to 64511, and 65536 (1.0 in the format of x.y) to 4294967295 (65535.65535 in the format of x.y), and the private AS number ranges from 64512 to 65534. 65535 is used as the reserved AS number in certain circumstances.

Public AS numbers can be used on the Internet. Private AS numbers cannot be advertised to the Internet, and they are used only within ASs. If private AS numbers are advertised to the Internet, a routing loop may occur. After this command is configured, if the AS path attribute contains only private AS numbers, BGP deletes the private AS numbers and then advertises these update routes.

BGP does not delete private AS numbers in either of the following scenarios if the **peer public-as-only** command is run, without any parameter following **public-as-only** specified:

- The AS_Path attribute of a route carries the AS number of the remote peer. In this case, deleting private AS numbers may lead to a routing loop.
- The AS_Path attribute carries both public and private AS numbers, which indicates that the route has passed through the public network. In this case, deleting private AS numbers may lead to a traffic forwarding error.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Example

Configure a device to remove all private AS numbers from the AS_Path attribute when sending a BGP Update packet to its peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 public-as-only
```

7.8.133 peer reflect-client

Function

The **peer reflect-client** command configures the local device as the route reflector and the peer or peer group as the client of the route reflector.

The **undo peer reflect-client** command restores the default setting.

By default, the route reflector and its client are not configured.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view and BGP-EVPN address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view, BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Full-meshed connections need to be established between IBGP peers to ensure the connectivity between the IBGP peers. If there are n switches in an AS, n*(n-1)/2 IBGP connections need to be established. A large number of IBGP peer use a lot of network and CPU resources. An RR can be used to solve the problem.

In an AS, one switch functions as an RR and other switches function as clients. The clients establish IBGP connections with the RR. The RR and its clients form a cluster. The RR reflects routes among the clients, and therefore the clients do not need to establish any IBGP connection. Assume that an AS has n devices. If one of the devices functions as a RR, and other devices function as clients, the number of IBGP connections to be established is n-1. This means that network and CPU resources are greatly reduced.

An RR is easy to configure, because it needs to be configured only on the device that functions as a reflector and clients do not need to know that they are clients.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

The device where the **peer reflect-client** command is run serves as the RR and a specified peer or peer group serves as the client of the RR.

The **peer reflect-client** command can be only used between IBGP peers or IBGP peer groups.

reflect-client configured in an address family is valid in this family address and cannot be inherited by other address families. Configuring **reflect-client** in a specified address family is recommended.

Example

Configure a peer as a client of an RR.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 reflect-client
```

7.8.134 peer route-limit

Function

The **peer route-limit** command sets the maximum number of routes that can be received from a peer.

The **undo peer route-limit** command restores the default setting.

By default, there is no limit on the number of routes that can be received from a peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit** *limit* [*percentage*] [**alert-only** | **idle-forever** | **idle-timeout** *minutes*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
limit	Specifies the maximum number of routes that can be received from a peer.	-
percentage	Specifies the percentage of received routes when the switch starts to generate alarms.	The value is an integer that ranges from 1 to 100. The default value is 75.
alert-only	Indicates that if the number of received routes exceeds the limit, an alarm will be generated and no additional routes will be accepted.	-
idle-forever	Indicates that after the number of routes exceeds the limit, no connection is established automatically until the **reset bgp** command is run.	-
idle-timeout *minutes*	Specifies the value of the timeout timer. The connection, which is closed because the number of routes exceeds the threshold, is automatically reestablished after the timeout timer expires. Before the timer expires, the **reset bgp** command can be used to re-establish a connection.	The value is an integer that ranges from 1 to 1200, in minutes.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view,BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP L2VPN-AD address family, BGP-L2VPN address family view, BGP-VPLS address family view, BGP-IPv6 unicast address family view, and BGP-VPNv6 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP L2VPN-AD address family view, BGP-L2VPN address family view, BGP-VPLS address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer route-limit** command is used to set the maximum number of routes that a BGP switch is allowed to receive from its peer. This provides a mechanism for controlling the routes received from peers in addition to distribution lists, filtering lists, and route mappings.

If a peer relationship between two devices is in the Established state, the following situations occur:

- If the number of routes received by the switch exceeds the upper limit and the **peer route-limit** command is used for the first time, the switch and its peer re-establish the peer relationship, regardless of whether **alert-only** is set.
- If the upper limit set on the switch is increased to be greater than the number of received routes, the switch sends Refresh packets to receive routes again. If the switch does not support the route-refresh capability, the switch needs to re-establish the connection with its peer.
- If the upper limit set on the switch is reduced but is still greater than the number of received routes, only configuration parameters need to be modified.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer route-limit** command is run for a peer group, the peers of the peer group inherit the configuration.

If the peer relationship is in the Idle state because the number of received routes exceeds the upper limit and **idle-forever** or **idle-timeout** is set, the **reset bgp** command can be used to re-establish the peer relationship.

Assume that none of **alert-only**, **idle-forever**, and **idle-timeout** is configured. If the number of routes exceeds the upper limit, an alarm is generated and recorded in the log. Then, the peer relationship is disconnected. The devices try to re-establish the peer relationship after 30 seconds.

Example

Set the maximum number of routes that can be received from a peer to 5000.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 route-limit 5000
```

7.8.135 peer route-policy

Function

The **peer route-policy** command specifies a route-policy for filtering routes received from a peer or peer group or routes to be advertised to a peer or peer group.

The **undo peer route-policy** command restores the default setting.

By default, no route-policy is configured for filtering routes received from a peer or peer group or routes to be advertised to a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
route-policy-name	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a route-policy to routes to be imported from a peer or peer group.	-
export	Applies a route-policy to routes to be advertised to a peer or peer group.	-

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, and BGP L2VPN-AD address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a route-policy is created, the **peer route-policy** command is used to apply a Route-Policy to a peer or a peer group so that the routes advertised to or received from the peer or peer group can be controlled. To be specific, only the necessary routes are received from or advertised to the peer or peer group. In this manner, route management is implemented, the scale of the routing table is reduced, and fewer network resources are consumed.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

If the **peer route-policy** command specifies a route-policy that does not exist, use the **route-policy** command to create the route-policy.

Precautions

Currently, the **peer route-policy** command cannot be used to apply a route-policy to set preferences for BGP routes.

The **preference** command cannot configure the preference for routes imported using the **network** command or the **import-route** command. The preference for these routes is 0.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured priority is set for all routes; if no priority is configured, the default priority is set for the routes.

Example

Apply a route-policy named test-policy to the routes received from a peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer 10.1.1.2 route-policy test-policy import
```

7.8.136 peer route-update-interval

Function

The **peer route-update-interval** command sets the interval at which a device sends routing updates carrying the same prefix to a peer or peer group.

The **undo peer route-update-interval** command restores the default setting.

By default, the interval at which routing updates are sent to IBGP peers is 15s, and the interval at which routing updates are sent to EBGP peers is 30s.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-update-interval** *interval*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-update-interval**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
interval	Specifies the minimum interval at which routing updates are sent.	The value is an integer that ranges from 0 to 600, in seconds.

NOTE

- *group-name* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPN instance IPv6 address family view.
- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When routes change, the switch sends routing updates to notify its peers. If a route changes frequently, the **peer route-update-interval** command can be used to adjust the interval at which Update packets are sent for changes of this route. This frees the switch from sending Update packets for every route change.

Prerequisites

If the **peer route-update-interval** command is used but no peer exists, a message is displayed, indicating that the peer does not exist.

Precautions

If a route is withdrawn, the switch immediately sends an Update message to its peers, regardless of the **peer route-update-interval** configuration. If a route is added and the interval between the last route addition time and the current route addition time is greater than the interval configured using the **peer route-update-interval** command, the switch immediately sends an Update message to its peers. If a route is added and the interval between the last route addition time and the current route addition time is less than the interval configured using the **peer route-update-interval** command, the switch sends an Update message to its peers only after the configured interval expires.

Example

Set the interval at which routing updates are sent to a peer to 10s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 route-update-interval 10
```

7.8.137 peer timer

Function

The **peer timer** command sets the Keepalive timer and Hold timer for a peer or peer group.

The **undo peer timer** command restores the default values of the Keepalive timer and Hold timer.

By default, the value of a Keepalive timer is 60s and the value of a Hold timer is 180s.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive hold** [**min-holdtime**]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
keepalive-time	Specifies the Keepalive period.	The value is an integer that ranges from 0 to 21845, in seconds.
hold-time	Specifies the holdtime.	The value is an integer that can be 0, or ranges from 3 to 65535, in seconds. **NOTE** Setting the hold interval of a BGP peer or peer group to be longer than 20s is recommended. If the hold interval of a BGP peer or peer group is shorter than 20s, the session may be closed.
min-holdtime *min-holdtime*	Specifies the minimum Holdtime configured on the local device. **NOTE** The value of *min-holdtime* configured cannot exceed the value of *hold-time*.	The value is an integer that ranges from 20 to 65535, in seconds.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After establishing a BGP connection, two peers send Keepalive messages periodically to each other to detect the status of the BGP connection. If a device receives no Keepalive message or any other types of packets from its peer within the holdtime, the device considers the BGP connection closed, and it closes the BGP connection.

When the peers set up a connection, the values of *keepalive-time* and *hold-time* are determined by negotiations between the peers. Each of the two peers sends the other an Open packet containing *hold-time*. The smaller of the *hold-time* values contained in the Open packets from both peers is used. The smaller of the locally configured *keepalive-time* value and one third of the negotiated *hold-time* value is used as the actual *keepalive-time* value.

The **peer timer** command is used to set the Keepalive period and holdtime.

- If short Keepalive period and holdtime are set, BGP can detect a link fault quickly and implement link switching. The number of Keepalive messages on the network, however, is increased. This increases device loads and consumption of network bandwidth resources.
- If long Keepalive period and holdtime are set, the number of Keepalive messages on the network is reduced. This reduces device loads. If, however, the Keepalive period is too long, BGP is unable to detect link status changes in a timely manner, causing many packets to be lost.

If the local device establishes BGP peer relationships with many devices, it needs to process huge BGP messages. If *hold-time* negotiated among BGP peers is small, the timer may expire before the local device processes the Keepalive messages sent from other BGP peers. The peer relationships are then interrupted, and routes flap. To solve the preceding problem, you can configure an appropriate value for **min-holdtime** *min-holdtime* based on the CPU processing capability of the local device.

If the value of *min-holdtime* is changed, but the values of *keepalive-time* and *hold-time* negotiated between two BGP peers remain unchanged, the established peer relationship is not affected. Only when the local device attempts to re-establish a relationship with a remote device, the value of *min-holdtime* configured on the local device takes effect. The local device compares *min-holdtime* with *hold-time* sent from the remote device. If the value of *min-holdtime* exceeds that of *hold-time*, *hold-time* negotiation fails, and the peer relationship fails to be established.

NOTE

If *min-holdtime* is configured on the local device, and the value of *hold-time* sent from the remote device is 0, *hold-time* negotiation between the two devices succeeds. The negotiated value of *hold-time* is 0, and the peer relationship is established. The value 0 of *hold-time* indicates that the peer relationship never expires.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

NOTICE

If the value of a timer changes, the BGP peer relationship between devices will be disconnected. This is because the devices need to re-negotiate the values of *keepalive-time* and *hold-time*. Therefore, exercise caution before changing the value of a timer.

The Keepalive period must be at least three times of the holdtime.

When setting the values of *keepalive-time* and *hold-time*, note the following points:

- The values of *keepalive-time* and *hold-time* cannot both be set to 0. This renders the BGP timers invalid. BGP is unable to detect link faults using the timers.
- The *hold-time* value cannot be significantly greater than the *keepalive-time* value. A setting of **timer keepalive 1 hold 65535**, for example, would be improper. If the holdtime is too long, link faults cannot be detected in a timely manner.

The Keepalive period and Holdtime can be configured globally, or on a particular peer or peer group. The Keepalive period and Holdtime configured on a specific peer or peer group take precedence over the global Keepalive period and Holdtime. Using this command can still change the Keepalive period and Holdtime configured on a peer or peer group, although they were globally configured through the **timer** command.

Example

Set the Keepalive timer and Hold timer for peer 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 timer keepalive 10 hold 30
```

7.8.138 peer tnl-policy

Function

The **peer tnl-policy** command applies the tunnel policy to the specified IPv4 peer.

The **undo peer tnl-policy** command removes the tunnel policy applied to the peer.

By default, no tunnel policy is applied to the peer.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support this command.

Format

peer *ipv4-address* **tnl-policy** *tnl-policy-name*

undo peer *ipv4-address* **tnl-policy**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the peer.	-
tnl-policy-name	Specifies the name of the tunnel policy.	The name is a string of 1 to 39 characters. It is case-sensitive.

Views

BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

When you configure the 6PE to support the tunnel, you need to configure the tunnel policy and apply the tunnel policy by using the command.

Before you configure the **peer tnl-policy** command, the **peer as-number** command should be used to create a peer or peer group.

Example

Apply the tunnel policy to the specified peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 100
[HUAWEI-bgp] ipv6-family unicast
[HUAWEI-bgp-af-ipv6] peer 10.1.1.2 enable
[HUAWEI-bgp-af-ipv6] peer 10.1.1.2 tnl-policy policy-a
```

7.8.139 peer timer connect-retry

Function

The **peer timer connect-retry** command sets a ConnectRetry interval for a peer or peer group.

The **undo peer timer connect-retry** command restores the default setting.

By default, the ConnectRetry interval is 32s.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies an IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
connect-retry-time	Specifies a ConnectRetry interval.	The value ranges from 1 to 65535, in seconds.

NOTE

- *ipv4-address* can be set only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view.

Views

BGP view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. The ConnectRetry interval can be adjusted as needed.

- The ConnectRetry interval can be reduced in order to lessen the time BGP waits to retry establishing a TCP connection after the first attempt fails.
- To suppress route flapping caused by constant peer flapping, the ConnectRetry interval can be increased to accelerate route convergence.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Precautions

A ConnectRetry interval can be configured globally, or on a particular peer or peer group. A ConnectRetry interval configured on a specific peer or peer group takes precedence over a global ConnectRetry interval.

- If both the **peer** { *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command and the **peer** *group-name* **timer connect-retry** *connect-retry-time* command are run on a device, the configuration of the **peer** { *ipv4-address* | *ipv6-address* }**timer connect-retry** *connect-retry-time* command takes effect, but the configuration of the **peer** *group-name* **timer connect-retry** *connect-retry-time* command does not.
- If both the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command and the **timer connect-retry** *connect-retry-time* command are run on a device, the configuration of the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command takes effect, but the configuration of the **timer connect-retry** *connect-retry-time* command does not.

Example

Set the ConnectRetry interval to 60s for peer 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 timer connect-retry 60
```

7.8.140 peer tracking

Function

The **peer tracking** command enables BGP peer tracking.

The **undo peer tracking** The command restores the interval between peer unreachability discovery and connection interruption to the default value (9s).

The **peer tracking disable** command disables BGP peer tracking.

The **undo peer tracking disable** command enables BGP peer tracking. The default interval between peer unreachability discovery and connection interruption is 9s.

By default, BGP peer tracking is enabled, and the interval between peer unreachability discovery and connection interruption is 9s.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **tracking** [**delay** *delay-time*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **tracking**

peer { *group-name* | *ipv4-address* | *ipv6-address* } **tracking disable**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **tracking disable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The address is a 32-digit hexadecimal number in the X:X:X:X:X:X:X:X format.
delay *delay-time*	Indicates the interval between when BGP detects the peer unreachable and when BGP tears down the corresponding connection.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 9 seconds.

NOTE

- *ipv4-address* can be set only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* can be set only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a network where BFD is unsuitable to be deployed, you can configure BGP peer tracking on the local device to implement fast network convergence by rapidly detecting the unreachable state of the peer.

A proper value of *delay-time* can ensure network stability when a peer is detected unreachable.

- If *delay-time* is set to 0, BGP immediately tears down the connection between the local device and its peer after the peer is detected unreachable.

- If IGP route flapping occurs and *delay-time* for an IBGP peer is set to 0, the peer relationship between the local device and the peer alternates between Up and Down. Therefore, *delay-time* for an IBGP peer should be set to a value greater than the actual IGP route convergence time.
- When BGP neighbors successfully perform the GR negotiation, the active/standby switchover occurs on the BGP neighbors, to prevent the failure of GR, *delay-time* should be set to a value greater than GR convergence time. If *delay-time* is set to be smaller than the GR convergence time, the connection between the local device and the BGP peer will be torn down, which leads to the failure of GR.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Precautions

IGP is configured with GR, and the BGP neighbor relationship is established based on IGP routes. In such a situation, when a node fails on the network and the master/slave switchover occurs on the node, IGP does not delete the routes from the node, and BGP neighbors cannot sense the fault on the node. Therefore, the BGP peer tracking function does not take effect.

Example

Configure BGP peer tracking.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 tracking delay 20
```

7.8.141 peer valid-ttl-hops

Function

The **peer valid-ttl-hops** command applies the GTSM function on the peer or peer group.

The **undo peer valid-ttl-hops** command cancels the application of the GTSM function on the peer or peer group.

By default, the GTSM function on the peer or peer group is not configured.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **valid-ttl-hops** [*hops*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **valid-ttl-hops**

Parameters

Parameter	Description	Value
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
hops	Specifies the number of TTL hops to be checked.	The value is an integer that ranges from 1 to 255. The default value is 255. If the value is configured as *hops*, the valid TTL range of the detected packet is [255 - *hops* + 1, 255].

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device against the attacks of forged BGP packets, you can configure GTSM to check whether the TTL value in the IP packet header is within the specified range.

Prerequisites

Before configuring GTSM for a peer group, run the **peer group** command to add peers to the peer group.

Precautions

When the **undo peer valid-ttl-hops** command is run and no parameter is specified, all the GTSM configurations on a peer or a peer group are deleted.

The configuration in the BGP view is also valid for the extension of MP-BGP. This is because they use the same TCP connection.

The GTSM configurations are symmetrical, that is, GTSM must be enabled on both ends of the BGP connection at the same time.

NOTE

- GTSM and EBGP-MAX-HOP are mutually exclusive because both of them affect the TTL of the sent BGP packet. Therefore, the two functions cannot be enabled on a peer or peer group simultaneously.
- If GTSM is enabled on two directly connected EBGP peers, the fast sensing function is invalid on the interfaces directly connecting the two EBGP peers. This is because BGP considers the EBGP peers indirectly connected when GTSM is enabled on the EBGP peers.

Example

Configure the GTSM function for the peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.2 as-number 200
[HUAWEI-bgp] peer 10.1.1.2 valid-ttl-hops 1
```

Configure the GTSM function for the peer group.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group gtsm-group external
[HUAWEI-bgp] peer gtsm-group valid-ttl-hops 1
```

7.8.142 preference (BGP)

Function

The **preference** command configures the protocol preferences for external routes, internal routes, aggregated routes, and crossed routes.

The **undo preference** command restores the default protocol preferences.

By default, the protocol preferences of external routes, internal routes, aggregated routes, and crossed routes are all 255.

Format

preference { *external internal local* | **route-policy** *route-policy-name* }

preference *external internal local* **route-policy** *route-policy-name*

undo preference

Parameters

Parameter	Description	Value
external	Specifies the protocol preference for external routes. An external route is the optimal route learned from an EBGP peer outside the local AS.	The value is an integer that ranges from 1 to 255. The smaller the value is, the higher the preference is.

Parameter	Description	Value
internal	Specifies the protocol preference for internal routes. An internal route is a route learned from an IBGP peer inside the local AS.	The value is an integer that ranges from 1 to 255. The smaller the value is, the higher the preference is.
local	Specifies the protocol preference for aggregated and crossed routes. This parameter takes effect for the following routes: ● Manually summarized routes generated using the **aggregate (BGP)** command ● Automatically summarized routes generated using the **summary automatic** command ● Routes generated through remote route cross ● Routes generated through local route cross For details about these routes, see **Precautions**.	The value is an integer that ranges from 1 to 255. The smaller the value is, the higher the preference is.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **preference** command to set protocol preferences for BGP routes affects route selection among BGP routes and routes of other routing protocols.

After a route-policy is configured on a device, the device sets preferences only for the routes received from peers, which meet the matching rules. The routes that do not meet the rules use the default preference.

The smaller the preference value, the higher the preference.

Different protocol preferences can be configured for BGP routes in different address family views.

If both *external internal local* and **route-policy** *route-policy-name* are specified in the command, the priority of the routes that match the route-policy is set based on the route-policy, and the priorities of other routes are set based on the *external internal local* configuration.

Prerequisites

Create the route-policy first if the **preference** command uses the **route-policy** to set preferences.

Perform the following steps when the route-policy is used to set preferences:

- Use the **route-policy** command to create the route-policy, and enter the route-policy view.
- Configure the **if-match** clause to set the matching rules for routes. The relationship between the **if-match** clauses in a node of a route-policy is "AND". A route must match all the rules before the action defined by the **apply** clause is taken. If no **if-match** clause is specified, all routes will match the node in the route-policy.
- Use the **apply preference** command to set preferences for routes that pass the filtering.

Precautions

- Currently, the **peer route-policy** command cannot be used to apply a route-policy to set preferences for BGP routes.
- The **preference** command cannot configure the preference for routes imported using the **network** command or the **import-route** command. The preference for these routes is 0.
- Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured priority is set for all routes; if no priority is configured, the default priority is set for the routes.
- In this command, the *local* parameter specifies the protocol preference for aggregated routes and crossed routes. This parameter takes effect for the following routes:
  - Manually aggregated routes generated using the **aggregate (BGP)** command. The **Route type** field for this type of route displays **Aggregated route**. For example:

```
<HUAWEI> display bgp routing-table 10.0.0.0
 BGP local router ID : 192.168.2.4
 Local AS number : 200
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 10.0.0.0/8:
 Aggregated route
 Route Duration: 04h50m46s
 Direct Out-interface: NULL0
 Original nexthop: 127.0.0.1
 Qos information : 0x0
 AS-path {65001 10 100}, origin incomplete, pref-val 0, valid, local, best, select, active, pre 255
```

```
 Aggregator: AS 200, Aggregator ID 192.168.2.4, Atomic-aggregate
 Advertised to such 3 peers:
    10.1.7.2
    172.16.1.2
    192.168.1.2
...
```

- Automatically aggregated routes generated using the **summary automatic** command. The route type for these routes displays **Summary automatic route**. For example:

```
<HUAWEI> display bgp routing-table 10.0.0.0
 BGP local router ID : 192.168.2.4
 Local AS number : 200
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 10.0.0.0/8:
 Summary automatic route
 Route Duration: 04h50m46s
 Direct Out-interface: NULL0
 Original nexthop: 127.0.0.1
 Qos information : 0x0
 AS-path {65001 10 100}, origin incomplete, pref-val 0, valid, local, best, select, active, pre 255
 Aggregator: AS 200, Aggregator ID 192.168.2.4, Atomic-aggregate
 Advertised to such 3 peers:
    10.1.7.2
    172.16.1.2
    192.168.1.2
...
```

- Routes generated through remote route cross. The route type for these routes displays **Remote-Cross route**. For example:

```
[HUAWEI-diagnose] display bgp vpnv4 vpn-instance vrf routing-table 172.16.17.161

BGP local router ID : 10.17.0.17
Local AS number : 100

VPN-Instance vrf, Router ID 10.17.0.17:
Paths:   1 available, 1 best, 1 select
BGP routing table entry information of 172.16.17.161/32:
Remote-Cross route
Label information (Received/Applied): 155665/NULL
From: 10.216.0.1 (10.17.0.9)
Route Duration: 3d04h26m28s
 Relay Tunnel Out-Interface: Vlanif100
Relay token: 0x24e7
Relay Tunnel Key: 7
Original nexthop: 10.216.0.1
Qos information : 0x0
Ext-Community:RT <10 : 10>
AS-path 100, origin incomplete, localpref 150, pref-val 1, valid, internal, best, select, active, pre
255, IGP cost 1
...
```

- Routes generated through local route cross. The route type for these routes displays **Local-Cross route**. For example:

```
[HUAWEI-diagnose] display bgp vpnv4 vpn-instance vrf1 routing-table 10.2.2.0

 BGP local router ID :
10.1.1.1
 Local AS number :
100

 VPN-Instance vrf1, Router ID
10.1.1.1:
 Paths:   1 available, 1 best, 1
select
 BGP routing table entry information of
10.2.2.0/24:
 Local-Cross route(via VPN-Instance
vrf2)
```

```
 Route Duration:
00h26m00s
 Direct Out-interface:
Vlanif40
 Original nexthop:
10.2.2.2
 Qos information :
0x0
 Ext-Community:RT <100 :
1>
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select, active, pre 255
...
```

Example

Set the protocol preference to 2 for external routes, 2 for internal routes, and 20 for aggregated routes and crossed routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] preference 2 2 20
```

7.8.143 reflect between-clients

Function

The **reflect between-clients** command enables route reflection among clients.

The **undo reflect between-clients** command disables route reflection among clients.

By default, route reflection among clients is enabled.

Format

reflect between-clients

undo reflect between-clients

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view, BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On some networks, if the clients of an RR establish full-mesh connections with each other, they can directly exchange routing information. Route reflection among clients is unnecessary. The **undo reflect between-clients** command can be used to prohibit the clients from reflecting routes to each other to reduce costs.

Prerequisites

An RR has been configured.

Precautions

The **reflect between-clients** command is run only on RRs.

Example

Disable route reflection among fully-meshed clients.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] group rr-client internal
[HUAWEI-bgp] peer 10.1.2.1 group rr-client
[HUAWEI-bgp] peer 10.1.3.1 group rr-client
[HUAWEI-bgp] peer 10.1.4.1 group rr-client
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] peer rr-client reflect-client
[HUAWEI-bgp-af-ipv4] undo reflect between-clients
```

7.8.144 reflect change-path-attribute

Function

The **reflect change-path-attribute** command enables a route-reflector (RR) to modify the route attributes of BGP routes using the export policy.

The **undo reflect change-path-attribute** command disables an RR from modifying the route attributes of BGP routes using the export policy.

By default, an RR is disabled from modifying route attributes of BGP routes using the export policy.

Format

reflect change-path-attribute

undo reflect change-path-attribute

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using an RR to modify route attributes may cause route loops. According to RFC 4456, you cannot enable an RR to modify the route attributes using the export policy. So an RR is disabled from modifying route attributes using the export policy by default.

To re-plan the network traffic, run the **reflect change-path-attribute** command to enable the RR to modify the route attributes using the export policy. After the command is run, the following configurations take effect.

- Run the **apply as-path** command to modify the AS-Path attributes of BGP routes.
- Run the **apply comm-filter delete** command to delete all community attributes from BGP routes.
- Run the **apply community** command to modify the community attributes of BGP routes.
- Run the **apply cost** command to modify the cost of BGP routes, that is to modify its MED.
- Run the **apply ip-address next-hop** command to modify the next hop of BGP routes.
- Run the **apply ipv6 next-hop** command to modify the next hop of BGP4+ routes.
- Run the **apply local-preference** command to modify the local preference of BGP routes.
- Run the **apply origin** command to modify the Origin attributes of BGP routes.
- Run the **apply extcommunity** command to modify the extended community attributes of BGP routes.

After the **undo reflect change-path-attribute** command is used, the previous configurations on the RR do not take effect.

Precautions

Export policies on the RR do not take effect before the **reflect change-path-attribute** command is run. After the **reflect change-path-attribute** command is run, these configurations may take effect and affect BGP route selection. Exercise caution when using this command.

For example, peer relationships are established between Switch A(10.1.1.1) and Switch B(10.1.1.2), and Switch A functions as an RR. If two configurations are on SwitchA:

1.
```
[HUAWEI] bgp 65001
```

```
[HUAWEI-bgp] peer 10.1.1.2 next-hop-local
```

2.
```
[HUAWEI] route-policy aa permit node 10
[HUAWEI-route-policy] apply ip-address next-hop 10.3.3.3
[HUAWEI-route-policy] quit
[HUAWEI] bgp 65001
[HUAWEI-bgp] peer 10.1.1.2 route-policy aa export
```

Then:

- Before the **reflect change-path-attribute** command is run, the former configuration takes effect but the latter does not. After A receives routes information from its IBGP peers, it reflects the information to Switch B, and changes the next hop to 10.1.1.1.
- After the **reflect change-path-attribute** command is run, the latter configuration takes effect but the former does not. After A receives routes information from its IBGP peers, it reflects the information to Switch B, and changes the next hop to 10.3.3.3.

NOTE

After you enable the **reflect change-path-attribute** command on the RR, the **peer route-policy export** command takes precedence over the **peer next-hop-invariable** and **peer next-hop-local**.

Example

Enable the RR to modify the route attributes of the BGP routes by using the export policy.

```
<HUAWEI> system-view
[HUAWEI] bgp 65001
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] reflect change-path-attribute
```

7.8.145 reflector cluster-id

Function

The **reflector cluster-id** command sets a cluster ID for an RR.

The **undo reflector cluster-id** command restores the default setting.

By default, each RR uses its router ID as the cluster ID.

Format

reflector cluster-id *cluster-id*

undo reflector cluster-id

Parameters

Parameter	Description	Value
cluster-id	Specifies the cluster ID of an RR.	The value can be an integer that ranges from 1 to 4294967295 or in the format of an IPv4 address.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view, BGP-VPLS address family view, BGP-L2VPN address family view, BGP L2VPN-AD address family view, BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sometimes, more than one RR needs to be configured in a cluster to improve network reliability and prevent single-point failures. If a cluster has more than one RR, the **reflector cluster-id** command needs to be used to set the same cluster ID for the RRs. This helps to identify the cluster and avoid routing loops.

Configuring an RR allows IBGP peers to advertise routes learned in the local AS to each other. The Cluster_List attribute is introduced to avoid loops within an AS. The Cluster_List is composed of a series of Cluster_IDs. It records all the RRs through which a route passes.

Precautions

If the **reflector cluster-id** command is run several times, the latest configuration overrides the previous one.

The **reflector cluster-id** command is run only on RRs.

To enable clients to receive routes reflected by RRs, ensure that the cluster ID of the RRs is different from the router ID of any client. If the cluster ID of the RRs is the same as the router ID of a client, the client will discard received routes.

Example

Configure the cluster ID to 50 for the switch, which is an RR in a cluster.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] reflector cluster-id 50
```

7.8.146 refresh bgp

Function

The **refresh bgp** command softly resets a BGP connection.

Format

refresh bgp [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

refresh bgp ipv6 { **all** | **group** *group-name* | *ipv4-address* | *ipv6-address* | **external** | **internal** } { **export** | **import** } (The *ipv4-address* is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

refresh bgp vpnv6 { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

refresh bgp vpn-instance *vpn-instance-name* **ipv6-family** { **all** | *ipv6-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** } (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

refresh bgp l2vpn-ad { *ipv4-address* | **all** | **group** *group-name* | **internal** | **external** } { **import** | **export** }

refresh bgp { **mdt** | **mvpn** } { *ipv4-address* | **all** | **group** *group-name* | **internal** | **external** } { **import** | **export** }

NOTE

The **mdt, mvpn, l2vpn-ad**, **vpnv4**, and **vpnv6** parameter are only supported by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Softly resets the connection of a specified VPN instance enabled with an IPv4 address family.	The value must be an existing VPN instance name.
vpnv4	Softly resets the BGP connections in a VPNv4 address family.	-
all	Softly resets all the BGP IPv4 connections.	-
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.

Parameter	Description	Value
group *group-name*	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Softly resets EBGP connections.	-
internal	Softly resets IBGP connections.	-
export	Triggers outbound soft resetting.	-
import	Triggers inbound soft resetting.	-
ipv6	Softly resets BGP4+ connections.	-
ipv6-address	Specifies the IPv6 address of a BGP4+ peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vpnv6	Softly resets the BGP connections in a VPNv6 address family.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Resets the connection of a specified VPN instance enabled with an IPv6 address family.	The value must be an existing VPN instance name.
l2vpn-ad	Softly resets the BGP connections related to L2VPN-AD.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device's peer supports route-refresh, the **refresh bgp** command can be used on the device to softly reset the BGP connection with the peer. BGP soft resetting can be used to refresh the BGP routing table and apply new routing policies, without closing any BGP connection.

Prerequisites

Configuring BGP soft resetting requires that the peers support the route-refresh capability.

Precautions

After the **refresh bgp** command is run on a device configured with the **peer keep-all-routes** command, the device does not refresh its routing table.

Example

Perform inbound soft resetting for all BGP connections to make new configurations take effect.

```
<HUAWEI> refresh bgp all import
```

7.8.147 refresh bgp multicast

Function

The **refresh bgp multicast** command softly resets an MBGP connection. MBGP soft resetting can be used to refresh the MBGP routing table and apply new routing policies, without closing any MBGP connection.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

refresh bgp multicast { *peer-address* | **all** | **group** *group-name* } { **import** | **export** }

Parameters

Parameter	Description	Value
peer-address	Softly resets the MBGP connections with a specified peer.	The peer address is in dotted decimal notation.
all	Softly resets all MBGP connections.	-

Parameter	Description	Value
group-name	Specifies the name of an MBGP peer group. If the parameter is set, the MBGP connections between a device and the members of the specified MBGP peer group are softly reset.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Triggers inbound soft resetting.	-
export	Triggers outbound soft resetting.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

MBGP soft resetting requires that all MBGP devices on a network support the route-refresh capability. The **reset bgp** command can be used on a device that does not support the route-refresh capability to reset the connections between the device and its peer and enable the device to refresh its routing table.

Example

Perform inbound soft resetting for all the MBGP connections to make new configurations take effect.

```
<HUAWEI> refresh bgp multicast all import
```

7.8.148 refresh bgp multicast external

Function

The **refresh bgp multicast external** command softly resets the connections between multicast EBGP peers.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

refresh bgp multicast external { **import** | **export** }

Parameters

Parameter	Description	Value
import	Triggers inbound soft resetting.	-
export	Triggers outbound soft resetting.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **refresh bgp multicast external** command to softly reset the connections between multicast EBGP peers.

Example

Trigger inbound soft resetting for all multicast EBGP connections.

```
<HUAWEI> refresh bgp multicast external import
```

7.8.149 refresh bgp multicast internal

Function

The **refresh bgp multicast internal** command softly resets the connections between multicast IBGP peers.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

refresh bgp multicast internal { **import** | **export** }

Parameters

Parameter	Description	Value
import	Triggers inbound soft resetting.	-
export	Triggers outbound soft resetting.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **refresh bgp multicast internal** command to softly reset the connections between multicast IBGP peers.

Example

Trigger inbound soft resetting for all multicast IBGP connections.

```
<HUAWEI> refresh bgp multicast internal import
```

7.8.150 reset bgp

Function

The **reset bgp** command resets specified BGP connections.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** } [**graceful**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

reset bgp ipv4 all [**graceful**]

reset bgp ipv6 { **all** | *as-number-plain* | *as-number-dot* | **group** *group-name* | *ipv6-address* | *ipv4-address* | **external** | **internal** } [**graceful**] (The *ipv4-address* is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.)

reset bgp vpls { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **external** | **internal** } (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

reset bgp vpnv6 { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** } [**graceful**] (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

reset bgp vpn-instance *vpn-instance-name* **ipv6-family** { **all** | *as-number-plain* | *as-number-dot* | *ipv6-address* | **group** *group-name* | **external** } [**graceful**] (supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Resets the connection of a specified VPN instance enabled with an IPv4 address family.	The value must be an existing VPN instance name.
vpnv4	Resets BGP connections associated with VPNv4.	-
all	Resets all BGP connections.	-
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the BGP connection with a specified peer.	It is in dotted decimal notation.
group *group-name*	Resets the BGP connection with a specified peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Resets all EBGP connections.	-
internal	Resets all IBGP connections.	-
ipv4	Resets BGP IPv4 connections.	-
ipv6	Resets BGP IPv6 connections.	-
ipv6-address	Resets the TCP connection with a specified BGP4+ peer (all the routes learned by using the connection are deleted).	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
vpls	Resets BGP connections associated with VPLS.	-
vpnv6	Resets BGP connections associated with VPNv6.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Resets the connection of a specified VPN instance enabled with an IPv6 address family.	The value must be an existing VPN instance name.
graceful	Resets BGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **reset bgp** command is used to make new BGP configurations take effect.

If a BGP routing policy is configured on the device that does not support Route-Refresh, the **reset bgp** command can be used to make the new routing policy to take effect.

To reset a BGP connection in GR mode, run the **reset bgp** command with the **graceful** parameter specified and run the **graceful-restart peer-reset** command. If the **graceful** parameter is not specified in the **reset bgp** command or if the **graceful-restart peer-reset** command is not run, the GR reset mode does not take effect, so that routing entries will be deleted for existing sessions, interrupting services. The services will be restored after the BGP peer relationship is reestablished.

The **reset bgp ipv4 all** command resets all public-network BGP IPv4 connections.

Precautions

After the **reset bgp** command is run on a device, the TCP connection established by the BGP device and the corresponding peer is reestablished. Exercise caution when running this command.

Example

Reset all BGP connections.

```
<HUAWEI> reset bgp all
```

Reset BGP connections with the peer 2001:DB8:1::1.

```
<HUAWEI> reset bgp ipv6 2001:DB8:1::1
```

Reset all BGP connections with VPNv6.

```
<HUAWEI> reset bgp vpnv6 all
```

Reset BGP sessions with BGP peers within a specified 2-byte AS number.

```
<HUAWEI> reset bgp vpnv6 100
```

Reset BGP sessions with BGP peers within a specified 4-byte AS number.

```
<HUAWEI> reset bgp vpnv4 200.300
```

7.8.151 reset bgp dampening

Function

The **reset bgp dampening** command clears BGP route dampening information and releases the suppressed routes.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] **dampening** [*ipv4-address* [*mask* | *mask-length*]]

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } **dampening** [*ipv6-address prefix-length*]

reset bgp vpnv4 dampening [*ipv4-address* [*mask* | *mask-length*]] (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

NOTE

The **vpn-instance** *vpn-instance-name* **ipv6-family** is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears the route dampening information of the specified VPN instance.	The value must be an existing VPN instance name.
ipv4-family	Indicates an IPv4 unicast address family.	-
ipv4-address	Specifies an IPv4 network address.	It is in dotted decimal notation.

Parameter	Description	Value
mask	Specifies the network mask in dotted decimal notation. If neither of the mask and mask length is specified, the address is considered as a classful address.	It is in dotted decimal notation.
mask-length	Specifies the network mask length. If neither of the mask and mask length is specified, the address is considered as a classful address.	The value is an integer that ranges from 0 to 32.
ipv6	Clears IPv6 route dampening information and releases the suppressed routes.	-
ipv6-family	Indicates an IPv6 unicast address family.	-
ipv6-address	Specifies the IPv6 network address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of an IPv6 prefix in decimal notation. It specifies the number of bits in the network address.	The value is an integer that ranges from 0 to 128.
vpnv4	Clears the route dampening information of the BGP VPNv4 routes and releases the suppressed routes.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Route dampening is enabled to solve the problem of route instability. In most situations, BGP is applied to complex networks where routes change frequently. Route dampening is then used to suppress instable routes.

The **reset bgp dampening** command is used to clear the dampening information about specified routes on the public network and release specified suppressed routes. If no IP address is specified in the command, the dampening information about all the routes on the public network is cleared and all suppressed routes are released.

Prerequisites

You can use **display bgp routing-table dampened** command to view the information about suppressed routes.

Precautions

After the **reset bgp dampening** command is run, the suppressed routes are released. If the status of some routes still changes frequently, route flapping may occur. Routing flapping consumes a large number of bandwidth and CPU resources.

When *ipv6-address prefix-length* is not specified, after you run the **reset bgp ipv6 dampening** command, IPv6 route dampening information in the whole BGP routing table is cleared.

Example

Clear the dampening information about routes to network segment 10.1.0.0 and release suppressed routes.

```
<HUAWEI> reset bgp dampening 10.1.0.0 255.255.0.0
```

Clear the dampening information about the IPv6 routes to network segment FC00:0:0:1:: and release suppressed routes.

```
<HUAWEI> reset bgp ipv6 dampening fc00:0:0:1:: 64
```

Clear the dampening information about the routes of IPv6 VPN instance named vpn1.

```
<HUAWEI> reset bgp vpn-instance vpn1 ipv6-family dampening
```

7.8.152 reset bgp flap-info

Function

The **reset bgp flap-info** command clears route flapping statistics.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] **flap-info** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*mask* | *mask-length*] | **regexp** *as-path-regexp*]

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } **flap-info** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-ipv6-address prefix-length* | **regexp** *as-path-regexp*]

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] *ipv4-address* **flap-info**

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } *ipv6-address* **flap-info**

reset bgp vpnv4 flap-info [**regexp** *as-path-regexp* | **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *ipv4-address* [*mask* | *mask-length*]] (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

reset bgp vpnv4 *ipv4-address* **flap-info** (supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H)

NOTE

The **vpn-instance** *vpn-instance-name* **ipv6-family** is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Clears the route flapping information of a specified VPN instance enabled with an IPv4 address family.	The value must be an existing VPN instance name.
as-path-filter *as-path-filter-number*	Clears route flapping statistics based on the number of a specified AS_Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter *as-path-filter-name*	Clears route flapping statistics based on the name of a specified AS_Path filter.	The value of *as-path-filter-name* is a string of 1 to 51 case-sensitive characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
network-address	Specifies the IPv4 prefix address that is used to filter the BGP IPv4 routes.	It is in dotted decimal notation.
mask	Specifies the network mask that is used to filter the BGP IPv4 routes. If neither the mask nor the mask length is specified, the address is processed as a classful address.	It is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the network mask length that is used to filter the BGP IPv4 routes. If neither the mask nor the mask length is specified, the address is processed as a classful address.	The value is an integer that ranges from 0 to 32.
regexp *as-path-regexp*	Clears statistics about the flapping routes that match the AS_Path regular expression.	-
ipv6	Clears the route flapping statistics on all IPv6 peers.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Clears the route flapping information of a specified VPN instance enabled with an IPv6 address family.	The value must be an existing VPN instance name.
network-ipv6-address	Specifies the IPv6 prefix address that is used to filter the BGP IPv6 routes.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the network mask length that is used to filter the BGP IPv6 routes.	The value is an integer that ranges from 0 to 128.
ipv4-address	Specifies the network address of an IPv4 peer.	It is in dotted decimal notation.
ipv6-address	Specifies the network address of an IPv6 peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vpnv4	Resets route flapping statistics of BGP VPNv4 routes.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The process of adding a route to and then deleting the route from a routing table is called route flapping.

When route flapping occurs, the routing protocol sends Update packets to neighbors. The neighbors that receive the Update packets need to recalculate routes and modify the routing table. Therefore, frequent route flapping consumes great bandwidth and CPU resources and even seriously affects network operations.

The **reset bgp flap-info** command is used to clear the flapping information about routes. This allows the switch to re-collect statistics about flapping routes and helps to monitor route changes and locate network problems.

Prerequisites

You can use **display bgp routing-table flap-info** command to view the information about BGP route flapping.

If there are a large number of flapping routes, define an AS_Path filter or an AS_Path regular expression to be referenced in the **reset bgp flap-info** command. The flapping statistics of the routes matching the AS_Path filter or the AS_Path regular expression are then cleared.

Precautions

After the **reset bgp flap-info** command is run, the flapping statistics of routes are reset and cannot be displayed.

Follow-up Procedure

After the flapping statistics of routes are cleared, run the **display bgp routing-table flap-info** command again to display the flapping statistics about BGP routes in order to locate problems.

Example

Clear the flapping statistics about the routes that match AS_Path filter 10.

```
<HUAWEI> reset bgp flap-info as-path-filter 10
```

Clear the flapping statistics about the BGP4+ routes of the VPN instance named vpn1.

```
<HUAWEI> reset bgp vpn-instance vpn1 ipv6-family flap-info
```

7.8.153 reset bgp flapping-count

Function

The **reset bgp flapping-count** command resets the flapping count of a specified BGP peer.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] *ipv4-address* **flapping-count**

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } *ipv6-address* **flapping-count**

NOTE

The **vpn-instance** *vpn-instance-name* **ipv6-family** is only supported on S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Specifies the name of VPN instance enabled with an IPv4 address family.	The value must be an existing VPN instance name.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6	Clears the flapping count of a specified BGP IPv6 peer.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Specifies the name of VPN instance enabled with an IPv6 address family.	The value must be an existing VPN instance name.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP peer flapping affects the stability of a BGP network and BGP route convergence.

The **reset bgp flapping-count** command can be used to clear the flapping account of a BGP peer. This allows the switch to re-collect the flapping statistics of a peer to locate BGP network problems.

Precautions

After the **reset bgp flapping-count** command is run, the flapping statistics of BGP peers are reset and cannot be displayed.

Follow-up Procedure

After the reset bgp flapping-count command is used to clear the statistics count of a specified BGP peer, run the **display bgp peer** command to display the flapping count of BGP peers and locate BGP network problems.

Example

Clear the flapping count of a specified BGP peer.

```
<HUAWEI> reset bgp 10.116.10.2 flapping-count
```

7.8.154 reset bgp mdt

Function

The **reset bgp mdt** command resets the BGP connections of a BGP MDT address family.

Format

reset bgp mdt { **all** | *ipv4-address* | **group** *group-name* | *as-number-plain* | *as-number-dot* } [**graceful**]

reset bgp mdt { **internal** | **external** } [**graceful**]

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Resets all BGP connections of a BGP MDT address family.	-
as-number-plain	Specifies an integral AS number.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies an AS number in dotted notation.	The value is in the format of x.y, where x and y are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the connection with a specified BGP peer.	The value is in dotted decimal notation.

Parameter	Description	Value
group *group-name*	Resets the connection with a specified BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
internal	Resets all IBGP connections.	-
external	Resets all EBGP connections.	-
graceful	Resets BGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

When the BGP MDT configuration is changed, you can run the **reset bgp mdt** command to make the new configuration take effect immediately.

NOTICE

After the command is run, the TCP connection established by the BGP device is reset and the corresponding peer relationship is re-established. Therefore, exercise caution before you run this command.

Example

Reset all BGP connections of a BGP MDT address family.

```
<HUAWEI> reset bgp mdt all
```

7.8.155 reset bgp multicast

Function

The **reset bgp multicast** command resets the connections between a device and specified MBGP peers.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset bgp multicast { **all** | *peer-address* | **group** *group-name* | *as-number-plain* | *as-number-dot* | **external** | **internal** } [**graceful**]

Parameters

Parameter	Description	Value
all	Resets all MBGP connections.	-
peer-address	Resets the MBGP connection with a specified peer.	The peer address is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.
external	Reset all EBGP connections.	-
internal	Reset all IBGP connections.	-
graceful	Specifies to reset MBGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

NOTE

After the **reset bgp multicast** command is run on a device, the TCP connection established by the device and the corresponding peer is reset and then reestablished. Exercise caution when running this command.

Example

Reset the MBGP connections of all address families.

```
<HUAWEI> reset bgp multicast all
```

7.8.156 reset bgp multicast dampening

Function

The **reset bgp multicast dampening** command clears dampening information about routes in the MBGP routing table.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset bgp multicast dampening [*ip-address* [*mask* | *mask-length*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a network address.	The value is in dotted decimal notation.
mask	Specifies the mask of a network address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a network address.	The value is an integer that ranges from 0 to 32.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

If a network address is specified in the **reset bgp multicast dampening** command, running this command clears the dampening information about a specific route and releases the suppressed route.

Example

Clear the dampening information about routes to network segment 10.1.0.0 and release suppressed routes.

```
<HUAWEI> reset bgp multicast dampening 10.1.0.0 255.255.0.0
```

7.8.157 reset bgp multicast external

Function

The **reset bgp multicast external** command resets all multicast EBGP connections.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset bgp multicast external [**graceful**]

Parameters

Parameter	Description	Value
graceful	Resets MBGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **reset bgp multicast external** command to reset all multicast EBGP connections.

Example

Reset all multicast EBGP connections.

```
<HUAWEI> reset bgp multicast external
```

7.8.158 reset bgp multicast flap-info

Function

The **reset bgp multicast flap-info** command clears route flapping statistics.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset bgp multicast flap-info [*ip-address* [*mask* | *mask-length*] | **as-path-filter** { *as-path-list-number* | *as-path-list-name* } | **regexp** *regexp*]

reset bgp multicast *ip-address* **flap-info**

Parameters

Parameter	Description	Value
ip-address	Specifies a network address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a network address.	The value is an integer that ranges from 0 to 32.
mask	Specifies the mask of a network address.	The value is in dotted decimal notation.
as-path-filter *as-path-list-number*	Clears route flapping statistics based on the number of a specified AS_Path filter.	The value is an integer that ranges from 1 to 256.
as-path-filter *as-path-list-name*	Clears route flapping statistics based on the name of a specified AS_Path filter.	The value is a string of 1 to 51 case-sensitive characters without spaces.
regexp *regexp*	Clears flapping statistics about the routes that match the AS_Path regular expression.	The value is a string of 1 to 80 characters.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **reset bgp multicast flap-info** command to clear route flapping statistics.

Example

Clear the flapping statistics about the routes that match AS_Path filter 10.

```
<HUAWEI> reset bgp multicast flap-info as-path-filter 10
```

7.8.159 reset bgp multicast internal

Function

The **reset bgp multicast internal** command resets the multicast IBGP connections in an AS.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset bgp multicast internal [**graceful**]

Parameters

Parameter	Description	Value
graceful	Specifies to reset MBGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **reset bgp multicast internal** command to reset the multicast IBGP connections in an AS.

Example

Reset all multicast IBGP connections.

```
<HUAWEI> reset bgp multicast internal
```

7.8.160 reset bgp mvpn

Function

The **reset bgp mvpn** command resets the BGP connections of a BGP MVPN address family.

Format

reset bgp mvpn { **all** | *ipv4-address* | **group** *group-name* | *as-number-plain* | *as-number-dot* } [**graceful**]

reset bgp mvpn { **internal** | **external** } [**graceful**]

NOTE

Only the following switch models support this command:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Parameters

Parameter	Description	Value
all	Resets all BGP connections of a BGP MVPN address family.	-
as-number-plain	Specifies an integral AS number.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies an AS number in dotted notation.	The value is in the format of x.y, where x and y are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the connection with a specified BGP peer.	The value is in dotted decimal notation.
group *group-name*	Resets the connection with a specified BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
internal	Resets all IBGP connections.	-
external	Resets all EBGP connections.	-
graceful	Resets BGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

When the BGP MVPN configuration is changed, you can run the **reset bgp mvpn** command to make the new configuration take effect immediately.

NOTICE

After the command is run, the TCP connection established by the BGP device is reset and the corresponding peer relationship is re-established. Therefore, exercise caution before you run this command.

Example

Reset all BGP connections of a BGP MVPN address family.

```
<HUAWEI> reset bgp mvpn all
```

7.8.161 router-id (BGP)

Function

The **router-id** command configures a Router ID for the switch.

The **undo router-id** command deletes the Router ID configured for the switch.

By default, no BGP Router ID is configured, and the global Router ID configured through the **router id** command is used.

Format

router-id { *ipv4-address* | **vpn-instance auto-select** }

undo router-id [**vpn-instance auto-select**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies a Router ID.	It is in dotted decimal notation.
vpn-instance auto-select	Configures automatic Router ID selection for all BGP-VPN instance IPv4 or IPv6 address families. If a Router ID is manually specified for a BGP-VPN instance IPv4 or IPv6 address family, the manually specified Router ID takes precedence over the automatically selected Router ID.	-

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **router-id** command is used to configure a Router ID for the switch. Each Router ID uniquely identifies one BGP switch in an AS.

By configuring automatic Router ID selection for a BGP-VPN instanceIPv4 or IPv6 address family, you can differentiate the configured Router ID of the BGP-VPN instance IPv4 or IPv6 address family from the BGP Router ID. For more information about the Router ID of a BGP-VPN instance IPv4 or IPv6 address family, see the **router-id (BGP-VPN Instance View)** command.

Prerequisites

The **bgp** command is run to enable BGP.

Precautions

Changing or deleting a configured Router ID in the BGP view resets a BGP session. If a BGP session has been established in a BGP-VPN instance IPv4 address family, deleting the configured Router ID resets the BGP session. Exercise caution when changing or deleting a Router ID.

By default, the switch that is not configured with any interface uses the Router ID of 0.0.0.0 assigned by routing management.

Example

Configure a Router ID for the switch.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] router-id 10.1.1.1
```

Configure automatic Router ID selection for all BGP-VPN instance IPv4 address families.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] router-id vpn-instance auto-select
```

7.8.162 router-id (BGP-VPN Instance View)

Function

The **router-id** command configures router ID for BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view.

The **undo router-id** command deletes the router ID configured for BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view.

By default, no router ID is configured for BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view, and the BGP router ID is used as the router ID.

Format

router-id { *ipv4-address* | **auto-select** }

undo router-id

Parameters

Parameter	Description	Value
ipv4-address	Specifies the router ID of a BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view. The router ID is expressed in the IPv4 address format.	It is in dotted decimal notation.
auto-select	Configures automatic route ID selection for the current BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view.	-

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring router ID for BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view, you can differentiate the configured router ID of BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view from the BGP router ID.

For example, if two VPN instances named **vrf1** and **vrf2** are configured on a PE, and a BGP session needs to be established between the interfaces bound to the two VPN instances, you need to configure different router IDs for the two VPN instance IPv4 address families. If no router ID is configured for the two VPN instance IPv4 address families, no BGP session can be established because the two VPN instance IPv4 address families have the same router ID, which is consistent with the BGP router ID.

Rules for automatically selecting a router ID for a BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view are as follows:

- If loopback interfaces configured with IP addresses are bound to the VPN instance, the largest IP address among the IP addresses of the loopback interfaces is selected as the router ID.
- If no loopback interfaces configured with IP addresses are bound to the VPN instance, the largest IP address among the IP addresses of other interfaces bound to the VPN instance is selected as the router ID, regardless of whether the interface is Up or Down.

Precautions

If a BGP session has been established in a BGP VPN instance IPv4 address family or BGP-VPN instance IPv6 address family view, changing or deleting the configured router ID resets the BGP session. So, confirm the action before you use the **router-id** command.

Example

Configure a router ID for a BGP VPN instance IPv4 address family.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vrf1
[HUAWEI-bgp-vrf1] router-id 192.168.100.1
```

7.8.163 route-select delay

Function

The **route-select delay** command configures a delay for selecting routes.

The **undo route-select delay** command deletes the delay for selecting routes.

The default delay is 0, indicating that routes are selected without a delay.

Format

route-select delay *delay-value*

undo route-select delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay for selecting routes.	The value is an integer that ranges from 0 to 3600, in seconds.

Views

BGP view, BGP-IPv4 unicast address family view, ,BGP-MDT address family view, BGP-MVPN address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view, BGP L2VPN-AD address family view

Default Level

2: Configuration level

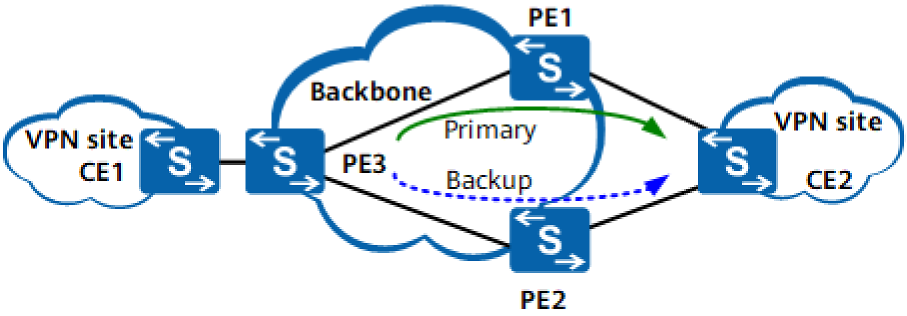
Usage Guidelines

Usage Scenario

In a scenario in which primary and backup routes exist, packets may get lost after traffic switches back to the primary path from the backup path. **Figure 7-3** illustrates a VPN FRR scenario. PE3 and CE2 connect both to PE1 and PE2. The primary path is PE3 -> PE1 -> CE2, and the backup path is PE3 -> PE2 -> CE2. CE2 uses BGP to communicate with PE1 and PE2. FRR is configured on PE3. If PE1 restarts or the link between CE2 and PE1 is disconnected, traffic switches from the primary path to the backup path. After the primary path recovers, traffic switches back to the primary path. If PE3 completes refreshing forwarding entries before PE1 does so, PE1 may temporarily fail to forward traffic after a switchback. As a result, packet loss may occur. The severity of packet loss is proportional to the number of routes stored on PE1.

To solve this problem, run the **route-select delay** command on PE3 to configure a delay for selecting a route to PE1. An appropriate delay ensures that traffic switches back to the primary path after PE1 completes refreshing forwarding entries.

Figure 7-3 VPN FRR networking



Precautions

If you run the **route-select delay** command repeatedly, the latest configuration overrides the previous configurations. If a route selection delay timer has started when you configure a new route select delay, the new route selection delay takes effect since the next route selection.

Example

Configure the delay for selecting routes as 300s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] route-select delay 300
```

7.8.164 routing-table limit threshold-alarm

Function

The **routing-table limit threshold-alarm** command configures alarm and alarm clear thresholds for the number of BGP routes.

The **undo routing-table limit threshold-alarm** command restores the default settings.

By default, the alarm threshold is 80%, and the alarm clear threshold is 70%.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

routing-table limit threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo routing-table limit threshold-alarm [**upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*]

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies an alarm threshold for the number of BGP routes.	The value is an integer that ranges from 1 to 100, in percentage. The default value is 80.
lower-limit *lower-limit-value*	Specifies an alarm clear threshold for the number of BGP routes.	The value is an integer that ranges from 1 to 100, in percentage. The default value is 70. *lower-limit-value* must be smaller than *upper-limit-value*; otherwise, alarms are generated and cleared repeatedly if route flapping occurs.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of BGP routes that can be added to a routing table is limited. If the value exceeds the limit, new routes cannot be added to the routing table, causing service interruptions. To address this problem, run the **routing-table limit threshold-alarm** command to configure alarm and alarm clear thresholds for the number of BGP routes. Alarms are then generated and cleared as expected. The alarms act as a prompt for checking whether an exception occurs and to take preventive measures.

- When the ratio of BGP routes to the maximum value exceeds *upper-limit-value*, an alarm is generated. New routes can still be accepted until the number of BGP routes reaches the maximum value.
- When the ratio falls below *lower-limit-value*, the alarm is cleared.

Configuration Impact

If the **routing-table limit threshold-alarm** command is run multiple times, the latest configuration takes effect.

Precautions

In addition to the **routing-table limit threshold-alarm** command, the **snmp-agent trap enable feature-name bgp trap-name** { **hwBgpRouteThresholdExceed** | **hwBgpRouteThresholdClear** } command must be run to enable the alarm and alarm clear functions; otherwise, alarms cannot be generated and cleared as expected.

Example

Configure alarm and alarm clear thresholds for the number of BGP routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] routing-table limit threshold-alarm upper-limit 70 lower-limit 60
```

7.8.165 routing-table rib-only

Function

The **routing-table rib-only** command prevents BGP routes from being added into the IP routing table.

The **undo routing-table rib-only** command restores the default setting.

By default, the preferred BGP routes are added to the IP routing table.

Format

routing-table rib-only [**route-policy** *route-policy-name*]

undo routing-table rib-only

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a Route-Policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, if the BGP routing table has large numbers of VPN routes, these routes will consume large numbers of memory resources after being delivered to the IP VPN routing table. If these routes are not used in traffic forwarding, you can run the **routing-table rib-only** command to prevent these routes from being added to the IP VPN routing table. If some of these routes are not used in traffic forwarding, you can run the **routing-table rib-only route-policy** command to prevent this part of routes from being added to the IP VPN routing table.

If a route reflector (RR) is used and preferred BGP routes do not need to be used during the forwarding, the **routing-table rib-only** command can be used to make BGP routes unable to be added to the IP routing table or the forwarding layer. This improves forwarding efficiency and the system capacity.

When **route-policy** *route-policy-name* is specified in the command, the routes matching the policy are not added to the IP routing table, and the routes not matching the policy are added to the IP routing table with the route attributes unchanged.

Configuration Impact

After the **routing-table rib-only** command is run, the routes preferred by BGP are not added to the IP routing table.

The **routing-table rib-only** command does not take effect on the labeled routes.

Precautions

The **routing-table rib-only** command and the **active-route-advertise** command are mutually exclusive.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all routes are not delivered to the IP routing table.

Example

Configure the routing policy named **ribonly** to prevent certain BGP routes from being added into the IP routing table.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] routing-table rib-only route-policy ribonly
```

7.8.166 shutdown (BGP)

Function

The **shutdown** command terminates all sessions between a device and its BGP peers.

The **undo shutdown** command restores the default setting.

By default, the function of closing all sessions between a device and its BGP peers is disabled.

Format

shutdown

undo shutdown

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

NOTICE

Running the **shutdown** command closes all sessions between a device and its peers. Exercise caution when using this command.

During system upgrade or maintenance, the sessions between a device and its BGP peers need to be closed to minimize the impact of BGP route flapping on the network. If a large number of BGP peers exist, the **shutdown** command can be run in the BGP view to close all sessions with BGP peers. This frees you from running the **peer ignore** command repeatedly to close the sessions one by one.

Example

Close all sessions between a device and its BGP peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] shutdown
Warning: All BGP peer sessions will be interrupted. Continue? [Y/N]:y
```

7.8.167 slow-peer detection disable

Function

The **slow-peer detection disable** command disables slow peer detection.

The **undo slow-peer detection disable** command restores the default configuration.

By default, slow peer detection is enabled.

Format

slow-peer detection disable

undo slow-peer detection disable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An update peer-group may consist of multiple BGP peers. If a network problem (congestion for example) occurs and slows down the speed at which the local device advertises routes to a BGP peer in the update peer-group, the speed at which the local device advertises routes to other BGP peers in the update peer-group is affected. To address this problem, slow peer detection is enabled by default.

When slow peer detection is enabled, the local device identifies the BGP peer to which routes are sent the slowest based on the time taken to send 100 packets to each BGP peer. If this time is greater than the period threshold for slow peer detection plus the average time taken to send 100 packets to BGP peers (excluding the longest and shortest times), the local device considers the peer a slow peer and removes it from the update peer-group. Slow peer detection prevents this slow peer from affecting route advertisement to other peers in the update peer-group.

To disable slow peer detection, run this command.

Example

Disable slow peer detection.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] slow-peer detection disable
```

7.8.168 slow-peer detection threshold

Function

The **slow-peer detection threshold** command sets a period threshold for slow peer detection.

The **undo slow-peer detection** command restores the default configuration.

By default, the period threshold for slow peer detection is 300s.

Format

slow-peer detection threshold *threshold-value*

undo slow-peer detection [**threshold** *threshold-value*]

Parameters

Parameter	Description	Value
threshold *threshold-value*	Specifies a period threshold for slow peer detection.	The value is an integer that ranges from 120 to 3600, in seconds.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When slow peer detection is enabled, the local device identifies the BGP peer to which routes are sent the slowest based on the time taken to send 100 packets to each BGP peer. If this time is greater than the period threshold for slow peer detection plus the average time taken to send 100 packets to BGP peers (excluding the longest and shortest times), the local device considers the peer a slow peer and removes it from the update peer-group. Slow peer detection prevents this slow peer from affecting route advertisement to other peers in the update peer-group.

By default, slow peer detection is enabled and the period threshold for slow peer detection is 300s. To adjust the period threshold for slow peer detection, run this command.

Configuration Impact

If the command is run more than once, the latest configuration overrides the previous one.

Precautions

After a slow peer is removed from the update peer-group, the peer relationship between the local device and the slow peer is reestablished.

Example

Set the period threshold for slow peer detection to 200s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] slow-peer detection threshold 200
```

7.8.169 summary automatic

Function

The **summary automatic** command enables automatic aggregation for the locally imported routes.

The **undo summary automatic** command disables automatic aggregation for the locally imported routes.

By default, automatic aggregation is disabled for the locally imported routes.

Format

summary automatic

undo summary automatic

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the BGP-IPv4 unicast address family view, the **summary automatic** command is used to configure a BGP device to automatically aggregate locally imported routes on the public network.

In the BGP-VPN instance IPv4 address family view, the **summary automatic** command is used to configure a BGP device to automatically aggregate locally imported routes on a private network.

The **summary automatic** command is used to aggregate the routes imported by BGP. These routes can be direct routes, static routes, RIP routes, OSPF routes, or IS-IS routes. After this command is run on a BGP device, the BGP device aggregates routes based on the natural network segment (for example, 10.1.1.0/24 and 10.2.1.0/24 are aggregated to 10.0.0.0/8, a Class A address), and sends only the aggregated route to its peers. This reduces the number of routes.

Precautions

BGP route aggregation is classified into manual aggregation and automatic aggregation. The command is used to implement automatic aggregation. Manual aggregation takes precedence over automatic aggregation.

The **summary automatic** command is invalid for the routes imported by using the **network** command.

Example

Enable automatic aggregation for imported routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] summary automatic
```

7.8.170 supernet unicast advertise

Function

The **supernet unicast advertise enable** command configures a BGP device to advertise BGP supernet unicast routes to its peers.

The **undo supernet unicast advertise enable** or **supernet unicast advertise disable** command restores the default configuration.

By default, BGP supernet unicast routes are considered invalid and cannot be advertised to BGP peers or delivered to the IP routing table.

Format

supernet unicast advertise enable

supernet unicast advertise disable

undo supernet unicast advertise enable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP supernet route has the same destination address and next-hop address or has a more detailed destination address than the next-hop address. Any route that meets one of the following conditions is a BGP supernet route.

- If you perform bitwise AND operations on the destination address mask with the destination address and next-hop address, respectively, the calculated network addresses are the same, and the destination address mask is greater than or equal to the next-hop address mask.
- If you perform bitwise AND operations on the destination address mask with the destination address and next-hop address, respectively, the calculated network addresses are different. However, if you perform bitwise AND operations on the next-hop address mask with the destination address and next-hop address, respectively, the calculated network addresses are the same.

For example, the route destined for 10.6.6.6 in the following command output is a BGP supernet route.

```
<HUAWEI> display bgp routing-table
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 1
       Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
   *>i  10.6.6.6/32        10.6.6.6       0          100       0      ?
```

BGP supernet routes include BGP supernet labeled routes and BGP supernet unicast routes. To allow a Huawei device to advertise BGP supernet unicast routes that it receives from a connected non-Huawei device to its BGP peers, run the **supernet unicast advertise enable** command on the Huawei device.

Example

Configure a BGP device to advertise BGP supernet unicast routes to its peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] supernet unicast advertise enable
```

7.8.171 timer (BGP)

Function

The **timer** command sets the values for the Keepalive timer and Hold timer.

The **undo timer** command restores the default values of the Keepalive timer and Hold timer.

By default, the value of a Keepalive timer is 60s and the value of a Hold timer is 180s.

Format

timer keepalive *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo timer keepalive *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo timer keepalive hold [**min-holdtime**]

Parameters

Parameter	Description	Value
keepalive *keepalive-time*	Specifies the Keepalive period.	The value is an integer that ranges from 0 to 21845, in seconds.
hold *hold-time*	Specifies the holdtime.	The value is an integer that can be 0, or ranges from 3 to 65535, in seconds.
min-holdtime *min-holdtime*	Specifies the minimum holdtime configured on the local device. **NOTE** The value of *min-holdtime* configured cannot exceed the value of *hold-time*.	The value is an integer that ranges from 20 to 65535, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a connection is established between peers, the values of *keepalive-time* and *hold-time* are negotiated by the peers.

- The smaller of the *hold-time* values carried by Open messages of both peers is taken as the *hold-time* value.
- The smaller of one third of the *hold-time* value and the locally configured *keepalive-time* value is taken as the *keepalive-time* value.

If the local device establishes BGP peer relationships with many devices, it needs to process huge BGP messages. If *hold-time* negotiated among BGP peers is small, the timer may expire before the local device processes the Keepalive messages sent from other BGP peers. The peer relationships are then interrupted, and routes flap. To solve the preceding problem, you can configure an appropriate value for **min-holdtime** *min-holdtime* based on the CPU processing capability of the local device.

If the value of *min-holdtime* is changed, but the values of *keepalive-time* and *hold-time* negotiated between two BGP peers remain unchanged, the established peer relationship is not affected. Only when the local device attempts to re-establish a relationship with a remote device, the value of *min-holdtime* configured on the local device takes effect. The local device compares *min-holdtime* with *hold-time* sent from the remote device. If the value of *min-holdtime* exceeds that of *hold-time*, *hold-time* negotiation fails, and the peer relationship fails to be established.

NOTE

If *min-holdtime* is configured on the local device, and the value of *hold-time* sent from the remote device is 0, *hold-time* negotiation between the two devices succeeds. The negotiated value of *hold-time* is 0, and the peer relationship is established. The value 0 of *hold-time* indicates that the peer relationship never expires.

Precautions

The timers configured for a specific peer or peer group by using the **peer timer** command override the timers configured for all BGP peers by using the **timer** command.

If the value of a timer changes, the BGP peer relationship between devices is disconnected. This is because the devices need to re-negotiate the values of *keepalive-time* and *hold-time*. Therefore, exercise caution before changing the value of a timer.

Setting the Hold timer value to at least three times the Keepalive timer value is recommended. When setting the values of *keepalive-time* and *hold-time*, note the following points:

- The values of *keepalive-time* and *hold-time* cannot both be set to 0. This renders the BGP timers become invalid. This means that BGP is unable to detect link faults using the timers.
- The *hold-time* value cannot be significantly greater than the *keepalive-time* value. A setting of **timer keepalive 1 hold 65535**, for example, would be improper. If the holdtime is too long, link faults cannot be detected in a timely manner.

Example

On a BGP device, set the value of the Keepalive timer to 30s and the value of the Hold timer to 90s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] timer keepalive 30 hold 90
```

7.8.172 timer connect-retry

Function

The **timer connect-retry** command sets a global ConnectRetry interval.

The **undo timer connect-retry** command restores the default setting.

By default, the ConnectRetry interval is 32s.

Format

timer connect-retry *connect-retry-time*

undo timer connect-retry

Parameters

Parameter	Description	Value
connect-retry-time	Specifies a ConnectRetry interval.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. The ConnectRetry interval can be adjusted as needed.

- The ConnectRetry interval can be reduced in order to lessen the time BGP waits to retry establishing a TCP connection after the first attempt fails.
- To suppress route flapping caused by constant peer flapping, the ConnectRetry interval can be increased to accelerate route convergence.

Precautions

A ConnectRetry interval can be configured globally, or on a particular peer or peer group. A ConnectRetry interval configured on a specific peer or peer group takes precedence over a global ConnectRetry interval.

If both the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command and the **timer connect-retry** *connect-retry-time* command are run on a device, the configuration of the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command takes effect, but the configuration of the **timer connect-retry** *connect-retry-time* command does not.

Example

Set a global BGP ConnectRetry interval to 60s.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] timer connect-retry 60
```

7.8.173 undo synchronization (BGP)

Function

The **undo synchronization** command disables synchronization between BGP and an IGP.

By default, synchronization between BGP and an IGP is disabled.

Format

undo synchronization

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo synchronization** command to disable synchronization between BGP and an IGP.

Example

Disable synchronization between BGP and an IGP.

```
<HUAWEI> system-view
```

```
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] undo synchronization
```

7.9 Routing Policy Configuration Commands

7.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.9.2 apply as-path

Function

The **apply as-path** command sets the action for changing the AS_Path attribute of BGP routes in a routing policy.

The **undo apply as-path** command restores the default setting.

By default, the action for changing the AS_Path attribute of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply as-path { { *as-number-plain* | *as-number-dot* } &<1-10> { **additive** | **overwrite** } | **none overwrite** }

undo apply as-path

Parameters

Parameter	Description	Value
as-number-dot	Specifies an AS number in dotted notation to be added to the AS_Path list or to replace the existing AS_Path list. A maximum of 10 AS numbers can be specified in one command.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
additive	Adds the specified AS number to the original AS_Path attribute.	-
overwrite	Replaces the original AS_Path with the specified AS number.	-
none	Clears the original AS_Path list.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the AS_Path attribute of BGP routes BGP for selecting the optimal route, you can apply a routing policy containing the **apply as-path** command.

AS_Path is a private attribute of BGP and records all ASs that a route passes through from the local end to the destination address. Using the AS_Path attribute controls route selection and prevents routing loops. If multiple routes are destined for the same destination address, BGP compares the AS_Path lists of these routes and considers the route with the shortest AS_Path list as the optimal route.

After this command is configured, the AS_Path list for matched BGP routes will change. Assume that the original AS-Path is (30, 40, 50) and the BGP route matching condition is met. In this case:

- If the **apply as-path 60 70 80 additive** command is run, the AS-Path list is changed to (60, 70, 80, 30, 40, 50). This configuration change is generally used to make the BGP route not preferentially selected.
- If the **apply as-path 60 70 80 overwrite** command is run, the AS-Path list is changed to (60, 70, 80). There are many application scenarios for changing the AS-Path list, and the major application scenarios are as follows:
  - Hide the real path information of routes. For example, after the AS-Path list is changed to (60, 70, 80), the AS-Path information of the route (30, 40, 50) is lost.

  - Implement load balancing. For example, a router receives two routes with the same destination IP address 10.1.0.0/16. The AS_Path list of one route is (60, 70, 80) and that of the other route is (30, 40, 50). In this case, you can change the AS_Path list (30, 40, 50) to (60, 70, 80), and load balancing then may be implemented on the two routes.
  - Shorten the AS-Path list to prevent the route from being discarded. If the **as-path-limit** command is configured, whether the number of AS numbers in the AS-Path list of the incoming route exceeds the maximum value needs to be checked. If the number exceeds the maximum value, the route is discarded. Therefore, before receiving a route with a long AS-Path list, replace the AS-Path list with a shorter AS-Path list. For example, if the original AS-Path list is (60, 70, 80, 65001, 65002, 65003), run the **apply as-path 60 70 80 overwrite** command to change the AS-Path list to (60, 70, 80). In this manner, the length of the AS-Path is shortened, preventing the route from being discarded.
  - Shorten the AS-Path list to make the route to be preferentially selected and traffic to be directed to the local AS.
- If the **apply as-path none overwrite** command is run, the AS-Path list is changed to be vacant. In BGP route selection, if the AS-Path list is vacant, the length of the AS-Path list is considered as 0. Therefore, clearing the AS-Path list cannot only hide the real path information, but also make the route to be preferentially selected and traffic to be directed to the local AS because the AS-Path list is shortened.

Prerequisites

The **apply as-path** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

Running the apply as-path command changes the path through which network traffic passes. Use this command only when you are familiar with the network topology and impact of the command on services.

Example

Change the AS number in the original AS_Path attribute to 200, 10.10.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply as-path 200 10.10 additive
```

7.9.3 apply backup-interface

Function

The **apply backup-interface** command configures a backup outbound interface in a routing policy.

The **undo apply backup-interface** command restores the default setting.

By default, the backup outbound interface is not configured in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply backup-interface *interface-type interface-number*

undo apply backup-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the backup outbound interface.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply backup-interface** command is used in IP FRR scenarios to configure a backup outbound interface for a route. After IP FRR is enabled, data traffic can be quickly switched to the backup outbound interface if the primary link fails.

Prerequisites

if-match clauses can be used to configure matching rules such as IP prefix lists, and ACLs before a backup outbound interface is configured.

Follow-up Procedure

Reference a configured route-policy in the **ip frr (system view)** command or the **ip frr (VPN instance view)** command to configure IP FRR on a public network or VPN.

The **apply backup-interface** command is usually used together with the **apply backup-nexthop** command.

Precautions

For P2P links, a backup next hop is not necessary. For non-P2P links, a backup next hop is necessary.

Example

Configure the backup outbound interface and the backup next hop in the route-policy named **ip_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-interface vlanif10
[HUAWEI-route-policy] apply backup-nexthop 192.168.20.2
```

Delete the configured backup outbound interface from the route-policy named **ip_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] undo apply backup-interface
```

7.9.4 apply backup-nexthop

Function

The **apply backup-nexthop** command configures a backup next hop in a routing policy.

The **undo apply backup-nexthop** command deletes the configured backup next hop.

By default, the backup next hop is not configured in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply backup-nexthop { *ipv4-address* | **auto** }

undo apply backup-nexthop

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IP address of a backup next hop.	It is in dotted decimal notation.
auto	Automatically searches for the backup next hop.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply backup-nexthop** command is used to configure a backup next hop for a route in IP FRR and VPN FRR scenarios. After IP FRR is enabled, data traffic can be quickly switched to the backup next hop if the primary link fails.

Prerequisites

if-match clauses can be used to set matching rules such as interfaces, IP prefix lists, and ACLs before a backup next hop is configured.

Follow-up Procedure

The configured route-policy can be used in the **ip frr (system view)** command or the **ip frr (VPN instance view)** command that is run to configure IP FRR for a public or private network. It can also be used in the **vpn frr** command that is run to enable VPN FRR.

In a VPN FRR scenario, you only need to run the **apply backup-nexthop** command to configure a backup next hop.

In an IP FRR scenario, you need to run both the **apply backup-nexthop** and **apply backup-interface** commands.

Precautions

For P2P links, a backup next hop is not necessary. For non-P2P links, a backup next hop is necessary.

NOTE

Example

Configure the backup interface and the backup next hop 192.168.20.2 in the route-policy named **ip_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-interface vlanif10
[HUAWEI-route-policy] apply backup-nexthop 192.168.20.2
```

Delete the configured backup next hop from the route-policy named **ip_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] undo apply backup-nexthop
```

7.9.5 apply behavior

Function

The **apply behavior** command configures a QoS traffic behavior for routes.

The **undo apply behavior** command restores the default setting.

By default, no QoS traffic behavior is configured.

Format

apply behavior *behavior-name*

undo apply behavior

Parameters

Parameter	Description	Value
behavior-name	Specifies the name of a QoS traffic behavior.	The value is a string of 1 to 31 case-sensitive characters without spaces, and must start with a letter.

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large and complex network is deployed, traffic flows of different types, such as voice, video, and data, need to be managed separately, with different bandwidth and delays assigned to these traffic flows. In this case, class-based QoS needs to be configured and complex traffic classification needs to be performed. The **apply behavior** command is used to associate filtered route with a specific traffic behavior.

Prerequisites

Before running the **apply behavior** *behavior-name* command, you need to create a traffic behavior.

Meanwhile, certain matching conditions need to be configured to classify routes, such as the AS-Path lost, community attribute list, address prefix list, and route cost.

Precautions

The **apply behavior** command is mutually exclusive with the **apply ip-precedence** command and the **apply qos-local-id** command, and only one of these commands can be configured on a node of a routing policy. For example, if the **apply behavior** command is configured in the view created by the **route-policy test permit node 10** command, configuring the **apply qos-local-id** command replaces **apply behavior** command.

Example

Configure the behavior named **example** in the system view, and then apply this QoS traffic behavior in the route-policy view.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior example
[HUAWEI-behavior-example] quit
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] apply behavior example
```

7.9.6 apply comm-filter delete

Function

The **apply comm-filter delete** command sets the action for deleting community attributes of a specified community filter in a routing policy.

The **undo apply comm-filter** command restores the default setting.

By default, the action for deleting community attributes of a specified community filter is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply comm-filter { *basic-comm-filter-number* | *adv-comm-filter-number* | *comm-filter-name* } **delete**

undo apply comm-filter

Parameters

Parameter	Description	Value
basic-comm-filter-number	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
adv-comm-filter-number	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
comm-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete the community attributes, you can run the **ip community-filter** command several times to configure community attributes one by one, and apply the routing policy containing the **apply comm-filter delete** command to delete these community attributes.

The community attribute is a private attribute of BGP. The **apply comm-filter delete** command takes effect only for BGP routes.

Prerequisites

The **apply comm-filter delete** command can be used only after the **route-policy** command is used.

Precautions

After routes meet the filtering conditions, the specified community attributes of these routes are deleted.

1. When the delete operation is configured on a specified community attribute list, only one community attribute can be configured for the specified community attribute list. To delete multiple community attributes, you need to configure multiple community attribute lists. For example, if community attribute list 1 is used to delete 100:100 200:200 from the community attribute 100:100 200:200 carried in a route, you need to perform the following configurations on community attribute list 1:

   ```
   [HUAWEI] ip community-filter 1 permit 100:100
   [HUAWEI] ip community-filter 1 permit 200:200
   [HUAWEI] display ip community-filter
   Community filter Number: 1
   permit 100:100
   permit 200:200
   [HUAWEI] route-policy RP1 permit node 10
   [HUAWEI-route-policy] apply comm-filter 1 delete
   ```

   If multiple community attributes are configured in the same community filter, the **apply comm-filter delete** command cannot delete these community attributes. To delete the community attributes, you can run the **ip community-filter** command several times to configure community attributes one by one, and apply the routing policy containing the **apply comm-filter delete** command to delete these community attributes. For example, the following command cannot delete the community attribute 100:100 200:200 of the route:

   ```
   [HUAWEI] ip community-filter 1 permit 100:100 200:200
   [HUAWEI] display ip community-filter
   Community filter Number: 1
   permit 100:100 200:200
   [HUAWEI] route-policy RP1 permit node 10
   [HUAWEI-route-policy] apply comm-filter 1 delete
   ```

2. When the **apply community** and **apply comm-filter delete** commands are run on the same node in a routing policy, the system performs the delete operation before the set operation regardless of the sequence in which the two commands are run.

   ```
   [HUAWEI] display route-policy
   Route-policy : 123a
     permit : 10
   Match clauses:
   Apply clauses: a
   apply community 999:9 additive
   apply comm-filter 1 delete
   ```

   The following command output shows that community attribute 111:1 of the corresponding BGP route is deleted and community attribute 999:9 is added.

   ```
   [HUAWEI] display ip community-filter
   Community filter Number: 1
   permit 111:1
   permit 999:9
   ```

Example

Delete the specified BGP route community attributes 1:200, 2:200, and 3:200 from the community filter.

```
<HUAWEI> system-view
[HUAWEI] ip community-filter 1 permit 1:200
[HUAWEI] ip community-filter 1 permit 2:200
[HUAWEI] ip community-filter 1 permit 3:200
```

```
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] apply comm-filter 1 delete
```

7.9.7 apply community

Function

The **apply community** command sets the action for changing the community attribute of BGP routes in a routing policy.

The **undo apply community** command restores the default setting.

By default, the action for changing the community attribute of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply community none

apply community { *community-number* | *aa:nn* | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } &<1-32> [**additive**]

undo apply community

Parameters

Parameter	Description	Value
none	Indicates that all the community attributes of routes are deleted.	-

Parameter	Description	Value
community-number | *aa:nn*	Specifies the community number. A maximum of 32 community numbers can be configured in the **apply community** command. - If you do not configure any one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 32 *community-number* and *aa:nn* together. - If you configure one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 31 *community-number* and *aa:nn* together. - If you configure two of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 30*community-number* and *aa:nn* together. - If you configure three of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 29 *community-number* and *aa:nn* together. - If you configure all of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 28 *community-number* and *aa:nn* together.	The value of *community-number* is an integer ranging from 0 to 4294967295. The value of *aa* or *nn* ranges from 0 to 65535.
internet	Indicates that matching routes are sent to any peer. By default, all routes belong to the Internet community.	-
no-advertise	Indicates that matching routes are not sent to any peer. That is, after a router receives a route with this attribute, it does not advertise the route to other BGP peers.	-
no-export	Indicates that matching routes are sent to other sub-ASs but not to other ASs. That is, after a router receives a route with this attribute, it does not advertise the route outside the local AS.	-
no-export-subconfed	Indicates that matching routes are neither sent to other sub-ASs nor to other ASs. That is, after a router receives a route with this attribute, it does not advertise the route to other sub-ASs.	-
additive	Indicates that community attributes are added to matching routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify the BGP routes, you can apply a routing policy containing the **apply community** command to configure the community attribute of matched BGP routes.

The community attribute is a private attribute of BGP. It simplifies the application of routing policies and facilitates route maintenance and management. A community is a set of destination addresses with the same characteristics. These addresses have no physical boundary and are independent of their ASs. They share one or multiple community attributes, which can be changed or set by running the **apply community** command.

Prerequisites

The **apply community** command can be used only after the **route-policy** command is used.

Precautions

If the **apply community** command is configured in a routing policy, the community attributes of the BGP routes that match the routing policy are changed according to the configurations in the routing policy.

Assume that the original community attribute of a BGP route is 30. If this BGP route matches a certain routing policy, the AS number is replaced or added on the basis of the routing policy. For example:

- If the **apply community 100** command is run, the community attribute is changed to 100.
- If the **apply community 100 150** command is run, the community attribute is changed to 100, 150.
- If the **apply community 100 150 additive** command is run, the community attribute is changed to 30, 100, 150.
- If the **apply community none** command is run, the community attribute of the BGP route is deleted.

Example

Configure a routing policy named **setcommunity**, match the route with the AS_Path filter being 8, and change its community attribute to **no-export**.

```
<HUAWEI> system-view
[HUAWEI] route-policy setcommunity permit node 16
[HUAWEI-route-policy] if-match as-path-filter 8
[HUAWEI-route-policy] apply community no-export
```

7.9.8 apply cost

Function

The **apply cost** command sets the action for changing the cost of routes in a routing policy.

The **undo apply cost** command restores the default setting.

By default, the action for changing the cost of routes is not set in a routing policy.

Format

apply cost [**+** | **-**] *cost*

undo apply cost

Parameters

Parameter	Description	Value
+	Increases the route cost.	If the MED of BGP routes or cost of non-BGP routes is greater than the maximum value (4294967295) after the adjustment, 4294967295 takes effect.
-	Reduces the route cost.	If the MED of BGP routes or cost of non-BGP routes is less than the minimum value (0) after the adjustment, 0 takes effect.
cost	Specifies the route cost. To control route selection, you can adjust the route cost to prevent routing loops.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the filtering conditions specified by **if-match** clauses are met, you can run the **apply cost** command to change the route MED or cost to control route selection. After setting the MED or cost, the MED or cost of the routes that are imported using the route-policy is changed accordingly.

Prerequisites

A route-policy has been configured by **route-policy**.

Configuration Impact

The costs of routes that match the route-policy are changed. BGP routes do not have costs, and instead, they have MEDs. If the **apply cost** command is run to configure an **apply** clause for a route-policy that is designed for BGP routes, the MEDs of BGP routes that match the route-policy are changed.

Precautions

The MEDs or costs of imported routes are independent of the route-policy after the **undo apply cost** command is used to cancel the route MED or cost.

Example

Define an **apply** clause to set the route cost to 120.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply cost 120
```

7.9.9 apply cost-type

Function

The **apply cost-type** command sets the action for changing the cost type of routes in a routing policy.

The **undo apply cost-type** command restores the default setting.

By default, the action for changing the cost type of routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply cost-type { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

Parameters

Parameter	Description	Value
external	Sets the cost type of IS-IS external routes.	-
internal	Sets the cost type of IS-IS internal routes or sets the MED value of BGP routes as the IGP cost of the next hop.	-
type-1	Sets Type 1 external routes of OSPF.	-
type-2	Sets Type 2 external routes of OSPF.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply cost-type** { **external** | **internal** } command sets the cost type of IS-IS routes. The cost of an internal route imported to IS-IS remains unchanged and the cost of an external route imported to IS-IS is increased by 64.

NOTE

When the cost-style of an IS-IS device is wide, compatible, or wide-compatible, the cost types of external or internal are classified. When the cost-style of an IS-IS device is narrow or narrow-compatible, the imported route classifies the cost type of external or internal. In other words, the **apply cost-type** command is valid on IS-IS devices only in the narrow or narrow-compatible modes.

The **apply cost-type** { **type-1** | **type-2** } command modifies the type of OSPF routes. During route import, OSPF modifies the type but not the cost value of the original route. When OSPF advertises the imported route with the cost and type information to a peer, the peer device will recalculate the cost value of the imported route based on the received information.

When the filtering conditions specified by **if-match** clauses are met, you can change the cost type of routes to set the imported external routes all to Type-1 or all to Type-2 by using the **apply cost-type** command. After the cost type of the routes that match the route-policy is set, the cost type of the routes that are imported by using the route-policy is the set cost type.

Prerequisites

Before running the **apply cost-type** command, you need to configure a route-policy by **route-policy**.

Configuration Impact

After routes match the route-policy, the cost type of the routes is changed.

Precautions

Different operations are performed when the **apply cost-type internal** command is applied to IS-IS routes and BGP routes:

- When the **apply cost-type internal** command is applied to IS-IS routes:

  Routes are configured as IS-IS internal routes.

- When the **apply cost-type internal** command is applied to BGP routes:

  When a switch advertises a route learned from an IBGP peer to an EBGP peer, if the **apply cost-type internal** command is run, the switch sets the MED value of the route to be advertised to the EBGP peer as the IGP cost of the next hop of the route.

Example

Set the cost type to OSPF external Type-1.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply cost-type type-1
```

7.9.10 apply dampening

Function

The **apply dampening** command sets the action for changing the dampening parameters of EBGP routes in a routing policy.

The **undo apply dampening** command restores the default setting.

By default, the action for changing the dampening parameters of EBGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply dampening *half-life-reach reuse suppress ceiling*

undo apply dampening

Parameters

Parameter	Description	Value
half-life-reach	Specifies the half-life of a reachable route.	The value is an integer ranging from 1 to 45, in minutes.
reuse	Specifies the threshold for routes to be released from the dampening state. When the penalty value falls below the threshold, routes are reused.	The value is an integer ranging from 1 to 20000.
suppress	Specifies the threshold for routes to enter the dampening state. When the penalty value exceeds the threshold, routes are suppressed.	The value is an integer ranging from 1 to 20000. The configured value of *suppress* must be greater than the value of *reuse*.
ceiling	Specifies the upper limit of the penalty value of routes.	The value is an integer ranging from 1001 to 20000. The configured value of *ceiling* must be greater than the value of *suppress*.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply dampening** command, which is mostly used in BGP, is used to prevent frequent route dampening from affecting routers on the network.

You can configure different route dampening parameters for different nodes in the same routing policy. When route flapping occurs, BGP can use different route dampening parameters to suppress the routes that match the routing policy.

Procedure

If the **apply dampening** command is run multiple times, the latest configuration overwrites the previous one.

Prerequisites

The **route-policy** command has been configured.

Precautions

The parameters in this command do not have default values and must be set. The values of *reuse*, *suppress*, and *ceiling* are listed in ascending order: *reuse* < *suppress* <*ceiling*. According to the formula, MaxSuppressTime = *half-life-reach* x 60 x (ln (*ceiling*/*reuse*)/ln (2)), routes are unsuppressed if the value of MaxSuppressTime is less than 1. Therefore, the value of the *ceiling*/*reuse* must be great enough so that the value of MaxSuppressTime can be equal to or greater than 1.

Example

Set dampening parameters for EBGP routes.

```
<HUAWEI> system-view
[HUAWEI] route-policy aa permit node 10
[HUAWEI-route-policy] apply dampening 20 2000 10000 16000
```

7.9.11 apply extcommunity

Function

The **apply extcommunity** command sets the action for changing the extended community attribute of BGP routes in a routing policy.

The **undo apply extcommunity** command restores the default setting.

By default, the action for changing the extended community attribute of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply extcommunity { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address:nn* } } &<1-16> [**additive**]

undo apply extcommunity

Parameters

Parameter	Description	Value
rt	Indicates the route-target extended community. A maximum of 16 route targets can be configured.	-
as-number	Specifies the AS number.	The value is an integer ranging from 0 to 65535.
4as-number	Specifies a 4-byte AS number.	A 4-byte AS number is divided into the following types: ● It is an integer ranging from 65536 to 4294967295. ● It is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 respectively
ipv4-address	Specifies the IPv4 address.	It is in dotted decimal notation.
nn	Specifies an integer.	● When the value of *as-number* is a 2-byte AS number, the value of *nn* ranges from 0 to 4294967295. ● When the value of *4as-number* is a 4-byte AS number, the value of *nn* ranges from 0 to 65535. ● For *ipv4-address*, the value of *nn* ranges from 0 to 65535.
additive	Indicates that existing community attributes can be added to routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When controlling inter-AS VPN route receiving and advertising, apply the routing policy that contains the **apply extcommunity** command to change the RT extended community attribute of matched routes. Currently, only the RT extended community attribute is supported. This command cannot specify an extended community attribute for public routes.

Prerequisites

The **apply extcommunity** command can be used only after the **route-policy** command is used.

Precautions

When the routing policy that contains the action is used in the BGP view, BGP IPv4 unicast address view, or BGP IPv6 unicast address view, the action does not take effect.

When a routing policy takes effect, it affects inter-AS VPN route receiving and advertising.

If the keyword **additive** is not set in the **apply extcommunity** command, the original extended community attribute is replaced.

Example

Add 100:2, 10.1.1.1:22, 100.100:100 to the VPN route-target extended community attribute of BGP.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply extcommunity rt 100:2 rt 10.1.1.1:22 rt 100.100:100 additive
```

7.9.12 apply ip-address next-hop (Route-Policy view)

Function

The **apply ip-address next-hop** command sets the action for changing the next hop address of BGP routes in a routing policy.

The **undo apply ip-address next-hop** command restores the default setting.

By default, the action for changing the next hop address of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply ip-address next-hop { *ipv4-address* | **peer-address** }

undo apply ip-address next-hop { *ipv4-address* | **peer-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the next hop address.	It is in dotted decimal notation.
peer-address	Sets the next hop address to the local address when the **apply** clause is used by an export policy. Sets the next hop address to the peer address when the **apply** clause is used by an import policy.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the next hop address of BGP routes for selecting the optimal route, you can apply a routing policy containing the **apply ip-address next-hop** command.

The next hop address of a BGP route is set using the policy in the following situations:

- IBGP: Configure the import or export policy for the IBGP peer. If the next hop address configured in the routing policy is unreachable, the IBGP peer adds the corresponding route to the BGP routing table. However, this route is invalid.
- EBGP: Configure the import policy for the EBGP peer. If an export policy is configured, the route destined for the EBGP peer is discarded because the next hop address is unreachable.

Prerequisites

The **apply ip-address next-hop** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

When a routing policy is specified in the **import-route** and **network** commands, the **apply ip-address next-hop** clause in the routing policy does not take effect.

The command sets a next hop IP address for the routes that match the relevant route-policy, which may change the service forwarding path. Therefore, exercise caution when running this command.

Example

Define an **apply** clause to set the next hop address as 192.168.1.8.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply ip-address next-hop 192.168.1.8
```

7.9.13 apply ip-precedence

Function

The **apply ip-precedence** command sets the QoS parameter *ip-precedence* for routes.

The **undo apply ip-precedence** command restores the configuration.

By default, no IP preference is set.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply ip-precedence *ip-precedence*

undo apply ip-precedence

Parameters

Parameter	Description	Value
ip-precedence	IP precedence	The value can be a preference value or a keyword: - The value is an integer ranging from 0 to 7. - The preference keyword can be Routine, Priority, Immediate, Flash, Flash-override, Critical, Internet, or Network. Table 7-193 shows the relationship between preference values and keywords.

Table 7-193 Relationship between preference values and keywords

Value	Keyword
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash-override
5	Critical
6	Internet
7	Network

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving routes, a BGP route receiver matches the attributes of the BGP routes based on the import route-policy, sets the IP precedence, delivers the BGP routes together with the associated QoS parameters, and applies QoS traffic policies to the classified data. In this case, the BGP route receiver can apply QoS policies to the data sent to the destination network segment based on the IP precedence. This applies QoS policies in BGP.

Prerequisites

The **apply ip-precedence** command can be used only after the **route-policy** command is used.

Configuration Impact

If a route matches a route-policy, you can change the value of the Precedence field in the IP header. The Precedence field is the first three bits of the Type of Service (ToS) field in the IP header.

Precautions

If an integer is used to specify *ip-precedence*, the preference is saved as an integer in the configuration file. If a keyword is used to specify *ip-precedence*, the preference is saved as a keyword in the configuration file.

Example

Set the IP precedence in the route-policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] apply ip-precedence internet
```

7.9.14 apply ipv6 backup-interface

Function

The **apply ipv6 backup-interface** command configures a backup outbound interface in a routing policy.

The **undo apply ipv6 backup-interface** command restores the default setting.

By default, the backup outbound interface is not configured in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply ipv6 backup-interface *interface-type interface-number*

undo apply ipv6 backup-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the backup outbound interface.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply ipv6 backup-interface** command is used in IPv6 FRR scenarios to configure a backup outbound interface for a route. After IPv6 FRR is enabled, data traffic can be quickly switched to the backup outbound interface if the primary link fails.

Prerequisites

if-match clauses can be used to configure matching rules such as IPv6 prefix lists, and ACLs before a backup outbound interface is configured.

Follow-up Procedure

Reference a configured route-policy in the **ipv6 frr (system view)** command or the **ipv6 frr (VPN instance view)** command to configure IPv6 FRR on a public network or VPN.

The **apply ipv6 backup-interface** command is usually used together with the **apply ipv6 backup-nexthop** command.

Precautions

For P2P links, a backup next hop is not necessary. For non-P2P links, a backup next hop is necessary.

Example

Configure the backup outbound interface and the backup next hop in the route-policy named **ipv6_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ipv6_frr_rp permit node 10
[HUAWEI-route-policy] apply ipv6 backup-interface vlanif10
[HUAWEI-route-policy] apply ipv6 backup-nexthop 2001:db8:1::1
```

Delete the configured backup outbound interface from the route-policy named **ipv6_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ipv6_frr_rp permit node 10
[HUAWEI-route-policy] undo apply ipv6 backup-interface
```

7.9.15 apply ipv6 backup-nexthop

Function

The **apply ipv6 backup-nexthop** command configures a backup next hop in a routing policy.

The **undo apply ipv6 backup-nexthop** command deletes the configured backup next hop.

By default, the backup next hop is not configured in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply ipv6 backup-nexthop { *ipv6-address* | **auto** }

undo ipv6 apply backup-nexthop

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a backup next hop.	The address is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
auto	Automatically searches for the backup next hop.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply ipv6 backup-nexthop** command is used to configure a backup next hop for a route in IPv6 FRR and VPN FRR scenarios. After IPv6 FRR is enabled, data traffic can be quickly switched to the backup next hop if the primary link fails.

Prerequisites

if-match clauses can be used to set matching rules such as interfaces, IPv6 prefix lists, and ACLs before a backup next hop is configured.

Follow-up Procedure

The configured route-policy can be used in the **ipv6 frr (system view)** command or the **ipv6 frr (VPN instance view)** command that is run to configure IPv6 FRR for a public or private network. It can also be used in the **vpn frr** command that is run to enable VPN FRR.

In a VPN FRR scenario, you only need to run the **apply ipv6 backup-nexthop** command to configure a backup next hop.

In an IPv6 FRR scenario, you need to run both the **apply ipv6 backup-nexthop** and **apply ipv6 backup-interface** commands.

Precautions

For P2P links, a backup next hop is not necessary. For non-P2P links, a backup next hop is necessary.

Example

Configure the backup interface and the backup next hop in the route-policy named **ipv6_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] apply ipv6 backup-interface vlanif10
[HUAWEI-route-policy] apply ipv6 backup-nexthop 2001:db8:1::1
```

Delete the configured backup next hop from the route-policy named **ipv6_frr_rp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy ipv6_frr_rp permit node 10
[HUAWEI-route-policy] undo apply ipv6 backup-nexthop
```

7.9.16 apply ipv6 next-hop

Function

The **apply ipv6 next-hop** command sets the action for changing an IPv6 next hop address of a BGP route in a route-policy.

The **undo apply ipv6 next-hop** command restores the default setting.

By default, the action for changing the IPv6 next hop addresses of BGP routes are not configured in a route-policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply ipv6 next-hop { **peer-address** | *ipv6-address* }

undo apply ipv6 next-hop { **peer-address** | *ipv6-address* }

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 next hop address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
peer-address	Specifies the peer address as the next hop.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply ipv6 next-hop** command configures an IPv6 next hop address for a BGP route.

In BGP, the next hop address of a route can be set through the route-policy in the following situations:

- IBGP

  For an IBGP peer, the configured inbound and outbound policies can take effect. If the next hop address configured in the policy is unreachable, the IBGP peer still adds the route to the BGP routing table, but the route is not valid.

- EBGP

  For an EBGP peer, when the policy is used to modify the next hop address of a route, the inbound policy is configured. If the outbound policy is configured, the route is discarded because its next hop is unreachable.

Prerequisites

The **apply ipv6 next-hop** command can be used only after the **route-policy** command is used.

Configuration Impact

After a BGP route matches a route-policy, you can change the IPv6 next hop address of the BGP route.

Precautions

When a route-policy is being applied in the **import-route** and **network** commands, the **apply ipv6 next-hop** clause in the route-policy does not take effect.

Example

Set FC00:0:0:6::1 as the next hop address.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply ipv6 next-hop fc00:0:0:6::1
```

7.9.17 apply isis

Function

The **apply isis** command sets the action for changing the level of routes imported to IS-IS in a routing policy.

The **undo apply isis** command restores the default setting.

By default, the action for changing the level of routes imported to IS-IS is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply isis { **level-1** \| **level-1-2** \| **level-2** }

undo apply isis

Parameters

Parameter	Description	Value
level-1	Indicates IS-IS Level-1 routes.	-
level-1-2	Indicates IS-IS Level-1 and Level-2 routes.	-
level-2	Indicates IS-IS Level-2 routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of external routes can be imported to IS-IS, which causes extra burdens on IS-IS-enabled devices. To solve this problem, run the **apply isis** command to set the level of the routes to be imported to IS-IS.

Prerequisites

The **apply isis** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects route receiving and advertising in IS-IS.

Example

Set the level of the routes imported to IS-IS.

```
<HUAWEI> system-view
```

```
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply isis level-1
```

7.9.18 apply local-preference

Function

The **apply local-preference** command sets the action for changing the local preference of BGP routes in a routing policy.

The **undo apply local-preference** command restores the default setting.

By default, the action for changing the local preference of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply local-preference *preference*

undo apply local-preference

Parameters

Parameter	Description	Value
preference	Specifies the local preference of BGP routes.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Local-Pref attribute is a private attribute of BGP. The **apply local-preference** command sets only the local preference for BGP routes. The Local_Pref attribute is used to determine the optimal route when traffic leaves an AS, and its default value is 100. When a BGP router obtains multiple routes to the same destination address but with different next hops through IBGP peers, the route with the largest Local_Pref value is selected.

Prerequisites

After a BGP route matches a routing policy, you can change the local preference of the BGP route.

Precautions

- When a routing policy takes effect, it affects BGP route selection.
- The Local_Pref attribute applies to the routing within an AS rather than be advertised to the outside of the AS. In this case, the **apply local-preference** command does not take effect when EBGP neighbor relationships are set up.
- After the **apply local-preference** command is run in a route-policy or its configuration is changed, route updates are triggered.

Example

Set the local preference of BGP routes to 130.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply local-preference 130
```

7.9.19 apply mpls-label

Function

The **apply mpls-label** command sets the action for allocating MPLS labels to public routes in a routing policy.

The **undo apply mpls-label** command restores the default setting.

By default, the action for allocating MPLS labels to public routes is not set in a routing policy.

NOTE

Only the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H support this command.

Format

apply mpls-label

undo apply mpls-label

Parameters

None

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where inter-AS VPN Option C or Carrier Support Carrier (CSC) is deployed, you can use the **apply mpls-label** command to allocate labels to public routes.

Prerequisites

The **apply mpls-label** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it allocates MPLS labels to public routes.

Example

Assign MPLS labels to the routes that match the routing policy.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply mpls-label
```

7.9.20 apply origin

Function

The **apply origin** command sets the action for changing the Origin attribute of BGP routes in a routing policy.

The **undo apply origin** command restores the default setting.

By default, the action for changing the Origin attribute of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply origin { **egp** { *as-number-plain* | *as-number-dot* } | **igp** | **incomplete** }

undo apply origin

Parameters

Parameter	Description	Value
egp *as-number-plain*	Sets the origin of BGP routes as EGP. The parameter *as-number-plain* specifies the Integral AS number of an external route. An AS number uniquely identifies an AS. *as-number-plain* is required when you need to change the origin of BGP routes as EGP. EGP has the secondary highest priority. The Origin attribute of the routes obtained through EGP is EGP.	The value is an integer ranging from 1 to 4294967295.
egp *as-number-dot*	Sets the origin of BGP routes as EGP. The parameter *as-number-dot* specifies the AS number in dotted notation of an external route. An AS number uniquely identifies an AS. *as-number-dot* is required when you need to change the origin of BGP routes as EGP. EGP has the secondary highest priority. The Origin attribute of the routes obtained through EGP is EGP.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
igp	Sets the origin of BGP routes as IGP. IGP has the highest priority. The Origin attribute of the routes obtained through an IGP of the AS that originates the routes, such as the routes imported to the BGP routing table through the **network** command, is IGP.	-

Parameter	Description	Value
incomplete	Sets the origin code of BGP routes as unknown. Incomplete has the lowest priority. The Origin attribute of the routes learned through other methods, such as the routes imported by BGP through the **import-route** command, is Incomplete.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the Origin attribute of routes for selecting the optimal route, you can apply a routing policy containing the **apply origin** command. The Origin attribute is a private attribute of BGP and defines the origin of a route.

Prerequisites

The **apply origin** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

Example

Set the origin of BGP routes to IGP.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply origin igp
```

7.9.21 apply ospf

Function

The **apply ospf** command sets the action performed for configuring an OSPF area to which the route is imported in a routing policy.

The **undo apply ospf** command restores the default setting.

By default, the action performed for configuring an OSPF area to which the route is imported is not set in a routing policy.

Format

apply ospf { **backbone** | **stub-area** }

undo apply ospf

Parameters

Parameter	Description	Value
backbone	Imports routes to the OSPF backbone area.	-
stub-area	Imports routes to an OSPF NSSA.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply ospf** command can be used to specify the OSPF backbone area or NSSA area to which routes are imported. This can prevent OSPF from importing too many external routes, which brings heavy burden on OSPF devices.

Prerequisites

The **apply ospf** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, routes are imported to the specified OSPF area.

Example

Import routes to the OSPF backbone area.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply ospf backbone
```

7.9.22 apply preference

Function

The **apply preference** command sets the action for changing the preference of routes in a routing policy.

The **undo apply preference** command restores the default setting.

By default, the action for changing the preference of routes is not set in a routing policy.

Format

apply preference *preference*

undo apply preference

Parameters

Parameter	Description	Value
preference	Specifies the route precedence. Route sharing and route selection are difficult because multiple routing protocols can run on the device at the same time; therefore, a default preference needs to be specified for each routing protocol. When different protocols discover multiple routes to the same destination, the route discovered by the protocol with a higher preference is selected to forward IP packets. The smaller the preference value, the higher the preference.	The value is an integer ranging from 1 to 255.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the preference of routes for selecting the optimal route, you can apply a routing policy containing the **apply preference** command.

Prerequisites

The **apply preference** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects route selection.

Example

Set the preference for routes.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply preference 90
```

7.9.23 apply preferred-value

Function

The **apply preferred-value** command sets the action for changing the preferred value of BGP routes in a routing policy.

The **undo apply preferred-value** command restores the default setting.

By default, the action for changing the preferred value of BGP routes is not set in a routing policy.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply preferred-value *preferred-value*

undo apply preferred-value

Parameters

Parameter	Description	Value
preferred-value	Specifies the preferred value of BGP routes. In route selection, the BGP route with the largest preferred value is preferred.	The value is an integer ranging from 0 to 65535.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the preferred value of BGP routes for selecting the optimal route, you can apply a routing policy containing the **apply preferred-value** command.

Prerequisites

The **apply preferred-value** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

The preferred value of a route indicates the weight of the route in BGP routing. The preferred value is not a standard RFC-defined attribute and is valid only on local devices. The preferred value is inapplicable to export policies of BGP.

Example

Set the preferred value for BGP routes.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply preferred-value 66
```

7.9.24 apply qos-local-id

Function

The **apply qos-local-id** command sets the QoS local ID.

The **undo apply qos-local-id** command cancels the configuration.

By default, no QoS local ID is set.

Format

apply qos-local-id *qos-local-id*

undo apply qos-local-id

Parameters

Parameter	Description	Value
qos-local-id	Specifies the QoS local ID.	The value is an integer ranging from 1 to 4095.

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The QoS local ID is a local identifier of QoS. In actual applications, you can set the QoS local ID in the route-policy, and add the command that matches the QoS local ID in the QoS policy. The QoS local ID set in the route-policy is delivered to the FIB table. During packet forwarding, the system obtains the QoS local ID from the FIB table and applies the related QoS policy according to the QoS local ID.

Configuration Impact

The **apply qos-local-id** command is mutually exclusive with the **apply behavior** and **apply ip-precedence** commands, and only one of these commands can be configured on a node of a routing policy. For example, if the **apply qos-local-id** command is configured in the view created by the **route-policy test permit node 10** command, configuring the **apply ip-precedence** command replaces **apply qos-local-id** command.

Example

Set the QoS local ID in the route-policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] apply qos-local-id 10
```

7.9.25 apply tag

Function

The **apply tag** command sets the action for changing the tag of routes in a routing policy.

The **undo apply tag** command restores the default setting.

By default, the action for changing the tag of routes is not set in a routing policy.

Format

apply tag *tag*

undo apply tag

Parameters

Parameter	Description	Value
tag	Specifies the tag of routes. Routes can be tagged as required. You can set the same tag for the same type of route. Routes can be flexibly controlled and managed through tags in the routing policy.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify the routes, you can apply a routing policy containing the **apply tag** command to add the same tag to the matched routes.

Prerequisites

The **apply tag** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effects, routes will be matched by routing policies related to the tag.

BGP routes do not support tags. The **apply tag** command sets the tag for only IGP routes.

Example

Set the tag of routes to 100.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] apply tag 100
```

7.9.26 apply traffic-index

Function

The **apply traffic-index** command sets the BGP traffic index.

The **undo apply traffic-index** command cancels the configuration.

By default, no BGP traffic index is set.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.

Product	Support
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

apply traffic-index *traffic-index*

undo apply traffic-index

Parameters

Parameter	Description	Value
traffic-index	Specifies the index of BGP traffic.	The value is an integer ranging from 1 to 64.

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP accounting uses different BGP traffic indexes in BGP community attributes to identify routes and charge the traffic accordingly.

The sending end of BGP routes can set attributes for BGP routes by using the route-policy. The receiving end of BGP routes can set the BGP traffic index for BGP routes according to the BGP community filter, BGP AS_Path filter, ACL, and IP prefix list. The BGP traffic index together with routing information is delivered to the FIB table. After BGP accounting is enabled on an interface, the traffic-index-based traffic collection table can be generated for the interface.

During packet forwarding, traffic statistics can be collected according to the traffic index on each interface. Traffic statistics can be collected according to either the destination address in the inbound direction or the source address in the outbound direction.

Prerequisites

The **route-policy** command has been run.

Example

Configure the BGP traffic index.

```
<HUAWEI> system-view
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] apply traffic-index 10
```

7.9.27 description (Route-Policy view)

Function

The **description** command configures the description of a route-policy.

The **undo description** command deletes the description of a route-policy.

By default, no description is configured for the route-policy.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a route-policy.	The description is a string of 1 to 80 case-sensitive characters that can contain spaces.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command can be used to configure a description for a created route-policy. If many route-policies have been configured, configuring descriptions for the policies will facilitate policy management.

Prerequisites

A route-policy has been created by using **route-policy** command.

Example

Configure the description of the route-policy named **temp**.

```
<HUAWEI> system-view
[HUAWEI] route-policy temp permit node 10
[HUAWEI-route-policy] description This policy-name is temp
```

7.9.28 display ip as-path-filter

Function

display ip as-path-filter command displays the configuration of the AS_Path filter.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

display ip as-path-filter [*as-path-filter-number* | *as-path-filter-name*]

Parameters

Parameter	Description	Value
as-path-filter-number	Displays the configuration of an AS_Path filter with a specified number.	It is an integer that ranges from 1 to 256.
as-path-filter-name	Displays the configuration of an AS_Path filter with a specified name.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The AS-Path attribute is a BGP-specific attribute. An AS-Path filter is used to filter BGP routes.

You can run the **display ip as-path-filter** command to:

- View detailed information about a configured AS path filter.
- Check whether an AS-Path filter is deleted successfully after running the **undo ip as-path-filter** command.

Precautions

The **display ip as-path-filter** command:

- Displays the configuration information about a specified AS-Path filter, if the number or name of the AS-Path filter is specified.
- Displays the configuration information about all AS-Path filters, if neither the number nor name of the AS-Path filter is specified.
- Does not display any information, if the AS-Path filter does not exist in the system or the AS-Path filter that is queried does not exist.

Example

Display the configured AS_Path filter.

```
<HUAWEI> display ip as-path-filter
As path filter number: 1
         permit    1.1 100,200
As path filter name: abc
         deny      2.2 200,400
```

Table 7-194 Description of the display ip as-path-filter command output

Item	Description
As path filter number	AS-Path filter number.
As path filter name	AS-Path filter name.
permit	Matching mode is permit.
1.1 100,200	Content of the regular expression.
deny	Matching mode is deny.

7.9.29 display ip community-filter

Function

The **display ip community-filter** command displays the configuration of the community filter.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

display ip community-filter [*basic-comm-filter-num* | *adv-comm-filter-num* | *comm-filter-name*]

Parameters

Parameter	Description	Value
basic-comm-filter-num	Displays the configuration of a basic community filter with a specified number.	The value is an integer ranging from 1 to 99.
adv-comm-filter-num	Displays the configuration of an advanced community filter with a specified number.	The value is an integer ranging from 100 to 199.
comm-filter-name	Displays the configuration of a community filter with a specified name.	The name is a string of 1 to 51 characters. The string cannot be all numerals.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The community attribute is a BGP-specific attribute. A community filter is used to filter BGP routes.

You can run the **display ip community-filter** command to:

- View detailed information about a configured community filter.
- Check whether a community filter is successfully deleted after running the **undo ip community-filter** command.

Precautions

The **display ip community-filter** command:

- Displays the configuration information about a specified community filter, if the number or name of the community filter is specified.
- Displays the configuration information about all community filters, if neither the number nor name of the community filter is specified.
- Does not display any information, if the community filter does not exist in the system or the community filter that is queried does not exist.

Example

Display all community filters.

```
<HUAWEI> display ip community-filter
Community filter Number: 10
         deny  no-export
Community filter Number: 110
         permit 110:110
Named Community basic filter: aa (ListID = 200)
         permit  1 internet
Named Community advanced filter: bb (ListID = 700)
         permit ^20
```

Table 7-195 Description of the display ip community-filter command output

Item	Description
Community filter Number	Indicates the number of a community filter.
permit	Indicates that the matching mode is permit.
deny	Indicates that the matching mode is deny.
Named Community basic filter	Indicates the name of a basic community filter.
Named Community advanced filter	Indicates the name of an advanced community filter.

7.9.30 display ip extcommunity-filter

Function

display ip extcommunity-filter command displays the configuration of the extended community filter.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

display ip extcommunity-filter [*basic-extcomm-filter-num* | *advanced-extcomm-filter-num* | *extcomm-filter-name*]

Parameters

Parameter	Description	Value
basic-extcomm-filter-num	Specifies the basic extended community filter number.	It is an integer that ranges from 1 to 199.
advanced-extcomm-filter-num	Specifies the advanced extended community filter number.	It is an integer that ranges from 200 to 399.
extcomm-filter-name	Displays the configuration of an extended community filter with a specified name.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The extended community attribute is a BGP-specific attribute. An extended community filter is used to filter VPN routes.

You can run the **display ip extcommunity-filter** command to:

- View detailed information about a configured extended community filter.

- Check whether an extended community filter is successfully deleted after running the **undo ip excommunity-filter** command.

Precautions

The **display ip extcommunity-filter** command:

- Displays the configuration information about a specified extended community filter, if the number or name of the extended community filter is specified.
- Displays the configuration information about all extended community filters, if neither the number nor name of the extended community filter is specified.
- Does not display any information, if the extended community filter does not exist in the system or the extended community filter that is queried does not exist.

Example

Display information about the extended community filter.

```
<HUAWEI> display ip extcommunity-filter
Extended Community filter Number 10
         permit rt : 100:10
Extended Community filter Number 280
         permit rt 100:65
Extended Community filter basic filter: bas-abc
         permit rt : 200:10
Extended Community filter advanced filter: adv-abc
         deny 1.1.1.1:10
```

Table 7-196 Description of the display ip extcommunity-filter command output

Item	Description
Extended Community filter Number	Indicates the number of an extended community filter.
Extended Community filter basic filter	Basic extended community filter name.
Extended Community filter advanced filter	Advanced extended community filter name.
permit	Indicates that the matching mode is permit.
deny	Indicates that the matching mode is deny.
rt	Indicates the extended community attribute of the specified RT.

7.9.31 display ip ip-prefix

Function

The **display ip ip-prefix** command displays the configuration of IPv4 prefix lists.

Format

display ip ip-prefix [*ip-prefix-name*]

Parameters

Parameter	Description	Value
ip-prefix-name	Displays the configuration of an IP prefix list with a specified name.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An IPv4 prefix list is used to filter IPv4 addresses. To achieve the following purposes, run the **display ip ip-prefix** command:

- View detailed configuration of a configured IPv4 prefix list.
- Check whether an IPv4 prefix list is deleted after running the **undo ip ip-prefix** command.
- View the number of routes that do or do not match the route-policy in an IPv4 prefix list.

Precautions

The **display ip ip-prefix** command:

- Displays the configuration of a specified IPv4 prefix list if the name of the IPv4 prefix list is specified.
- Displays the configuration of all IPv4 prefix lists if no IPv4 prefix list name is specified.
- Does not display information if no IPv4 prefix list exists in the system or the queried IPv4 prefix list does not exist.

Before collecting the number of routes that do or do not match the route-policy in an IPv4 prefix list within a certain period, run the **reset ip ip-prefix** command to clear existing statistics.

NOTE

If **The specified filter list does not exist** is displayed in the command output, the specified IPv4 prefix list failed to be configured. To re-configure it, run the **ip ip-prefix** command in the system view.

Example

Display the configuration of the IP prefix list named **p1**.

```
<HUAWEI> display ip ip-prefix p1
Prefix-list pl
Permitted 0
  Description prefixok
Denied 0
        index: 10      permit  192.168.0.0/16          ge  17  le  18
```

Table 7-197 Description of the display ip ip-prefix command output

Item	Description
Prefix-list	Name of an IPv4 prefix list.
Permitted	Number of routes that match a route-policy.
Description	Description of an IPv4 prefix list. This field is displayed only after a description is configured using the **ip ip-prefix** *ip-prefix-name* **description** *text* command.
Denied	Number of routes that do not match the route-policy.
index	Index of the entry in the IPv4 prefix list.
permit	Contents of the entry in the IPv4 prefix list.
ge 17	The mask is greater than or equal to 17.
le 18	The mask is less than or equal to 18.

7.9.32 display ip ipv6-prefix

Function

display ip ipv6-prefix displays the configuration of IPv6 prefix lists.

Format

display ip ipv6-prefix [*ipv6-prefix-name*]

Parameters

Parameter	Description	Value
ipv6-prefix-name	Displays the configuration of an IP prefix list with a specified name. If *ipv6-prefix-name* is not specified, the configuration of all the configured IPv6 prefix lists is displayed.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An IPv6 prefix list is used to filter IPv6 addresses. To achieve the following purposes, run the **display ip ipv6-prefix** command:

- View detailed configuration of a configured IPv6 prefix list.
- Check whether an IPv6 prefix list is deleted after running the **undo ip ipv6-prefix** command.
- View the number of routes that do or do not match the route-policy in an IPv6 prefix list.

Precautions

The **display ip ipv6-prefix** command:

- Displays the configuration of a specified IPv6 prefix list if the name of the IPv6 prefix list is specified.
- Displays the configuration of all IPv6 prefix lists if no IPv6 prefix list name is specified.
- Does not display information if no IPv6 prefix list exists in the system or the queried IPv6 prefix list does not exist.

Before collecting the number of routes that do or do not match the route-policy in an IPv6 prefix list within a certain period, run the **reset ip ipv6-prefix** command to clear existing statistics.

Example

Display the configuration of all the IPv6 prefix lists.

```
<HUAWEI> display ip ipv6-prefix
 Prefix-list6 abc
 Description prefixok
 Permitted 0
 Denied 0
 index:   10          permit  ::/0
 index:   20          permit  ::/1           ge  1   le  128
```

Table 7-198 Description of the display ip ipv6-prefix command output

Item	Description
Prefix-list6	Name of an IPv6 prefix list.
Description	Description of an IPv6 prefix list. This field is displayed only after a description is configured using the **ip ipv6-prefix** *ipv6-prefix-name* **description** *text* command.

Item	Description
Permitted	Number of routes that match a route-policy.
Denied	Number of routes that do not match a route-policy.
index	Index of the entry in the IPv6 prefix list.
permit	Contents of the entry in the IPv6 prefix list.
ge	Greater than or equal to.
le	Less than or equal to.

7.9.33 display ip rd-filter

Function

The **display ip rd-filter** command displays the configuration of the route distinguisher (RD) filter.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

display ip rd-filter [*rd-filter-number*]

Parameters

Parameter	Description	Value
rd-filter-number	Displays the configuration of an RD filter with a specified number.	The value is an integer ranging from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The RD attribute is carried in VPN routes. An RD filter is used to filter VPN routes.

You can run the **display ip rd-filter** command to:

- View detailed information about a configured RD filter.
- Check whether an RD filter is successfully deleted after running the **undo ip rd-filter** command.

Precautions

The **display ip rd-filter** command:

- Displays the configuration information about a specified RD filter, if the number of an RD filter is specified.
- Displays the configuration information about all RD filters, if the number of no RD filter is specified.
- Does not display any information, if the RD filter does not exist in the system or the RD filter that is queried does not exist.

Example

Display the configured RD filter.

```
<HUAWEI> display ip rd-filter
Route Distinguisher Filter 1
       permit 10.1.1.1:1 10.2.2.2:* 100:1 200:*
Route Distinguisher Filter 2
       deny 1:1 2:2
       permit 1:* 2:*
```

Table 7-199 Description of the display ip rd-filter command output

Item	Description
Route Distinguisher Filter	Number of the RD filter
permit	Matching mode: permit
deny	Matching mode: deny

7.9.34 display route-policy

Function

The **display route-policy** command displays the configuration of the route-policy.

Format

display route-policy [*route-policy-name*]

Parameters

Parameter	Description	Value
route-policy-name	Displays the configuration of a route-policy with a specified name.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display route-policy** command to check detailed configuration of a route-policy.

Example

Display the configuration of the route-policy named **policy1**.

```
<HUAWEI> display route-policy policy1
Route-policy : policy1
  permit : 10 (matched counts: 2)
    Match clauses :
       if-match acl 2000
    Apply clauses :
       apply cost 100
       apply tag 100
```

Table 7-200 Description of the display route-policy command output

Item	Description
Route-policy	Name of the routing policy
permit	Matching mode and node index of the routing policy
matched counts: 2	Number of nodes that routes are matched in a routing policy
Match clauses	Matching condition list
Apply clauses	Apply clause list

7.9.35 goto next-node

Function

The **goto next-node** command further matches routes against a specified node after the routes match the current node.

The **undo goto next-node** command restores the default configuration.

By default, if a route matches the current node, it matches the route-policy and is no longer matched against other nodes.

Product	Support
S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, S6730-S, and S6730S-S	Not supported

Format

goto next-node [*node*]

undo goto next-node

Parameters

Parameter	Description	Value
node	Specifies the index of a node against which routes are further matched.	The value is an integer ranging from 1 to 65535 and must be greater than the index of the current node.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The relationship among the matching rules of nodes in the same route-policy is OR. Specifically, if a route matches a node, it matches the route-policy and is no longer matched against other nodes. If you want the route to be matched against two or more nodes, run the **goto next-node** command so that the route is further matched against a specified node after the route matches the current node.

- If *node* is not specified in the command, the route will be further matched against the next node of the current node by default.
- If the node specified in the command does not exist, the route will be further matched against the next node of the specified node by default. If the next node of the specified node does not exist either, the route fails to match the route-policy, and no **apply** clause will be applied to the route.

Precautions

- If the **goto next-node** command is run in the route-policy view and a route matches all the specified nodes, the **apply** clauses of these nodes will be applied to the route.
- If the route fails to match one node, the route is matched against the next node until it succeeds in matching a node, and then the **apply** clauses of the nodes that the route matches will be applied to the route. If the route fails to match all nodes, no **apply** clauses will be applied to the route.
- In the same route-policy, a maximum of 50 nodes can be specified using the command.
- In the same route-policy, if this command is configured to match routes against multiple nodes, a maximum of 10 AS numbers, 16 RT extended community attributes, 16 color extended community attributes, and 36 community attributes can be added to the routes that match the nodes; if multiple community filters are used in the same route-policy to delete community attributes from the routes that match filtering conditions, only the first community filter takes effect.

Example

Configure a route-policy named **test** to further match routes against node 20 after the routes match node 10.

```
<HUAWEI> system-view
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] if-match tag 123
[HUAWEI-route-policy] apply cost 10
[HUAWEI-route-policy] goto next-node 20
```

7.9.36 if-match acl (Route-Policy view)

Function

The **if-match acl** command sets a matching rule that is based on the Access Control List (ACL).

The **undo if-match acl** command deletes the matching rule based on the specified ACL.

By default, no matching rule based on the ACL is configured.

Format

if-match acl { *acl-number* | *acl-name* }

undo if-match acl { *acl-number* | *acl-name* }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match acl** command to set a matching rule based on the ACL to match IPv4 prefixes.

Prerequisites

The **if-match acl** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes using the ACL. Routes that match the ACL will be checked by other **if-match** clauses of this node. Routes that do not match the ACL will be checked by the next node.

An ACL name is a character string that starts with a letter. For example, **2a** is an invalid ACL name.

The **if-match acl** command and the **if-match ip-prefix** command are mutually exclusive. If you run the **if-match ip-prefix** command after running the **if-match acl** command, the configuration of the **if-match ip-prefix** command overrides the configuration of the **if-match acl** command.

For an ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Set a matching rule that is based on ACL 2000.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match acl 2000
```

7.9.37 if-match as-path-filter

Function

The **if-match as-path-filter** command creates a matching rule based on the AS_Path filter.

The **undo if-match as-path-filter** command deletes a matching rule based on the specified AS_Path filter.

By default, no matching rule based on the AS_Path filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

if-match as-path-filter { *as-path-filter-number* &<1-16> | *as-path-filter-name* }

undo if-match as-path-filter [*as-path-filter-number* &<1-16> | *as-path-filter-name*]

Parameters

Parameter	Description	Value
as-path-filter-number	Specifies the number of an AS_Path filter. A maximum of 16 AS_Path filters can be specified.	The value is an integer ranging from 1 to 256.

Parameter	Description	Value
as-path-filter-name	Specifies the name of the AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The value cannot contain only numerals. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AS_Path attribute is the private attribute of BGP. The **if-match as-path-filter** command is applicable to only BGP routes. The **ip as-path-filter** command must be used to define an AS_Path filter so that the matching rule based on this AS_Path filter can take effect. For example:

- If the **if-match as-path-filter 1** command is used but AS_Path filter 1 is not configured, all routes are permitted, that is, all routes match the matching rule.
- If the **if-match as-path-filter 1** command after the **ip as-path-filter 1 permit *20** command is used, the BGP routes with the AS_Path attribute being 20 are permitted.

Multiple **if-match as-path-filter** clauses can be specified. The relationship between **if-match as-path-filter** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

Before running the **if-match as-path-filter** command, run the **ip as-path-filter** command to configure an AS_Path filter.

Precautions

The routing policy matches routes using the AS-Path filter. Routes that match the AS-Path filter will be checked by other **if-match** clauses of this node. Routes that do not match the AS-Path filter will be checked by the next node.

A maximum of 16 AS_Path filters can be specified. The relationship between these AS_Path filters is OR. Specifically, if a route matches one of these AS_Path filters, it matches the matching rules of the command.

Creating an AS_Path filter before it is referenced is recommended. By default, nonexistent AS_Path filters cannot be referenced using the command. If the **route-**

policy nonexistent-config-check disable command is run in the system view and a nonexistent AS_Path filter is referenced using the current command, all routes match the AS_Path filter.

Example

Configure AS_Path filter 2 to permit AS200 and AS300. Create a routing policy named **test**, and define AS_Path filter 2 in an **if-match** clause for node 10 of the routing policy.

```
<HUAWEI> system-view
[HUAWEI] ip as-path-filter 2 permit _200_300
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] if-match as-path-filter 2
```

7.9.38 if-match community-filter

Function

The **if-match community-filter** command creates a matching rule based on the community filter.

The **undo if-match community-filter** command deletes the matching rule based on the specified community filter.

By default, no matching rule based on the community filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

if-match community-filter { *basic-comm-filter-num* [**whole-match**] | *adv-comm-filter-num* } &<1-16>

if-match community-filter *comm-filter-name* [**whole-match**]

undo if-match community-filter [*basic-comm-filter-num* | *adv-comm-filter-num*] &<1-16>

undo if-match community-filter *comm-filter-name*

Parameters

Parameter	Description	Value
basic-comm-filter-num	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
adv-comm-filter-num	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
comm-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
whole-match	Indicates complete matching. That is, all the communities in the command must be matched. Complete matching is valid only for the basic community filter.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The community attribute is a private attribute of BGP. The **if-match community-filter** command is applicable to only BGP routes. The **ip community-filter** command must be used to define a community filter so that the matching rule based on this community filter can take effect. For example:

- If the **if-match community-filter 1** command is used but community filter 1 is not configured, all routes are permitted, that is, all routes can match the matching rule.
- If the **if-match community-filter 1** command is used after the **ip community-filter 1 permit 1:1** command is used, the BGP routes with the community attribute being 1:1 are permitted.

Multiple **if-match community-filter** clauses can be specified. The relationship between **if-match community-filter** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

Before using the **if-match community-filter** command, you must use the **ip community-filter** command to configure a community filter.

The **if-match community-filter** command can be used only after a routing policy is configured.

Precautions

The routing policy matches routes using the community filter. Routes that match the community filter will be checked by other **if-match** clauses of this node. Routes that do not match the community filter will be checked by the next node.

A maximum of 16 community filters can be configured in the **if-match community-filter** command. The relationship between these community-filters is OR. Specifically, if a route matches one of these community-filters, it matches the matching rules of the command.

The parameter **whole-match** is valid only for its front community filter number. If multiple community filters are specified in the **if-match community-filter** command and packets are required to completely match each filter, you need to specify the parameter **whole-match** behind each community filter and it is valid to only the basic community filter.

The name of a community filter cannot be all numerals.

Creating a community attribute filter before it is referenced is recommended. By default, nonexistent community attribute filters cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent community attribute filter is referenced using the current command, all routes match the community filter.

Example

Set a matching rule that is based on the community filter 1.

```
<HUAWEI> system-view
[HUAWEI] ip community-filter 1 permit 100:200
[HUAWEI] route-policy test permit node 10
[HUAWEI-route-policy] if-match community-filter 1
```

Set the complete matching rule for community attribute filters 1 and 2.

```
<HUAWEI> system-view
[HUAWEI] route-policy test permit node 11
[HUAWEI-route-policy] if-match community-filter 1 whole-match 2 whole-match
```

Set a matching rule that is based on the community filter named **aa**.

```
<HUAWEI> system-view
[HUAWEI] route-policy test permit node 12
[HUAWEI-route-policy] if-match community-filter aa
```

7.9.39 if-match cost

Function

The **if-match cost** command creates a matching rule based on the route cost.

The **undo if-match cost** command deletes the matching rule based on the specified route cost.

By default, no matching rule based on the route cost is configured.

Format

if-match cost { *cost* | **greater-equal** *greater-equal-value* [**less-equal** *less-equal-value*] | **less-equal** *less-equal-value* }

undo if-match cost

Parameters

Parameter	Description	Value
cost	Specifies the route cost. Route costs can be changed to prevent routing loops.	The value is an integer ranging from 0 to 4294967295.
greater-equal *greater-equal-value*	Specifies the minimum value of route cost.	The value is an integer ranging from 0 to 4294967294.
less-equal *less-equal-value*	Specifies the maximum value of route cost. *less-equal-value* is demanded to be greater than *greater-equal-value*.	The value is an integer ranging from 1 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **if-match cost** command to configure a node to filter routes based on the route costs. After such a matching rule is configured, you can apply the **apply** clauses to change the attributes of the routes that match the matching rule.

Prerequisites

The **if-match cost** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the route cost. Routes that match the route cost will be checked by other **if-match** clauses of this node. Routes that do not match the route cost will be checked by the next node.

Example

Match the route with the cost 8.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match cost 8
```

7.9.40 if-match extcommunity-filter

Function

The **if-match extcommunity-filter** command sets a matching rule that is based on the extended community filter.

The **undo if-match extcommunity-filter** command deletes the matching rule based on the specified extended community filter.

By default, no matching rule based on the extended community filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

if-match extcommunity-filter { { *basic-extcomm-filter-num* | *adv-extcomm-filter-num* } &<1-16> | *extcomm-filter-name* }

undo if-match extcommunity-filter [[*basic-extcomm-filter-num* | *adv-extcomm-filter-num*] &<1-16> | *extcomm-filter-name*]

Parameters

Parameter	Description	Value
basic-extcomm-filter-num	Specifies the number of a basic extended community filter.	It is an integer ranging from 1 to 199.
adv-extcomm-filter-num	Specifies the number of an advanced extended community filter.	It is an integer ranging from 200 to 399.

Parameter	Description	Value
extcomm-filter-name	Specifies the name of an extended community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The extended community attributes help flexibly control the routing policy. You can use the **if-match extcommunity-filter** command to configure a node to filter routes based on the extended community filter.

The **if-match extcommunity-filter** command is applicable to only BGP routes and must work in conjunction with the **ip extcommunity-filter** command. For example:

- If the **if-match extcommunity-filter 1** command is used but the extended community filter 1 is not configured, all routes are permitted, that is, all routes can match the matching rule.
- If the **if-match extcommunity-filter 1** command is used after the **ip extcommunity-filter 1 permit rt 1:1** command is used, the BGP routes with the extended community attribute being 1:1 are permitted.

Multiple **if-match extcommunity-filter** clauses can be specified. The relationship between **if-match extcommunity-filter** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

Before using the **if-match extcommunity-filter** command, you must use the **ip extcommunity-filter** command to configure an extended community filter.

Precautions

The routing policy matches routes using the extended community filter. Routes that match the extended community filter will be checked by other **if-match** clauses of this node. Routes that do not match the extended community filter will be checked by the next node.

A maximum of 16 extended community filters can be configured in the **if-match extcommunity-filter** command. The relationship between these extended community filters is OR. Specifically, if a route matches one of these extended community filters, it matches the matching rules of the command.

Example

Define a rule to match the routes of the specified extended community filter.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match extcommunity-filter 100
```

7.9.41 if-match interface

Function

The **if-match interface** command creates a matching rule based on the outbound interface.

The **undo if-match interface** command deletes the matching rule based on the specified outbound interface.

By default, no matching rule based on the outbound interface is configured.

Format

if-match interface { *interface-type interface-number* } &<1-16>

undo if-match interface [*interface-type interface-number*] &<1-16>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the outbound interface. A maximum of 16 outbound interfaces can be specified in the **if-match interface** command.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **if-match interface** command is used to filter routes based on the outbound interfaces.

A maximum of 16 outbound interfaces can be configured in this command.

If a node contains multiple **if-match interface** clauses, the relationship between the **if-match interface** clauses is OR. If a node contains both **if-match interface** clauses and other **if-match** clauses with different matching rules, the relationship between the **if-match interface** clauses and other **if-match** clauses is AND. For example, if a node contains **if-match interface GE0/0/1**, **if-match interface GE0/0/2**, and **if-match acl 2000** clauses, **if-match interface GE0/0/1** and **if-match interface GE0/0/2** are ORed, whereas **if-match interface GE0/0/1** and **if-match acl 2000** are ANDed.

Prerequisites

The **if-match interface** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on outbound interface information. Routes that match the outbound interface information will be checked by other **if-match** clauses of this node. Routes that do not match the outbound interface information will be checked by the next node.

Example

Define a rule to match the routes with the outbound interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match interface vlanif 100
```

7.9.42 if-match ip

Function

The **if-match ip** command creates a matching rule based on IP information.

The **undo if-match ip** command deletes the matching rule based on specified IP information.

By default, no matching rule based on IP information is configured.

Format

if-match ip { **next-hop** | **route-source** | **group-address** } { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }

undo if-match ip { **next-hop** | **route-source** | **group-address** } [**acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name*]

Parameters

Parameter	Description	Value
next-hop	Specifies the next hop address.	-
route-source	Specifies the source address of routes.	-
group-address	Indicates the IP address of the multicast group.	The value is in dotted decimal notation.

Parameter	Description	Value
acl	Indicates route filtering using the ACL.	-
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name	Specifies the name of a basic ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list that is used to filter routes.	The value is a string of case-sensitive characters without space and ranges from 1 to 169.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL or IP prefix must be configured before running the **if-match ip** command so that the matching rule can take effect. For example:

- If the **if-match ip next-hop ip-prefix aa** command is used but the IP prefix **aa** is not configured, all routes are permitted, that is, all routes match the matching rule. This rule also applies to ACL.
- If the **if-match ip next-hop ip-prefix aa** and **ip ip-prefix aa permit 10.1.1.1 32** commands are used, the routes with the next hop being 10.1.1.1 is permitted. This rule also applies to ACL.

Prerequisites

The **if-match ip** command can be used only after the **route-policy** command is used.

Before running the **if-match ip** command, configure an **ACL** or an **IP prefix**.

Precautions

- The routing policy matches routes based on the next hop address or source address. Routes that match the next hop address or source address will be checked by other **if-match** clauses of this node. Routes that do not match the next hop address or source address will be checked by the next node.
- If the next hop address or source address of a route to be filtered is 0.0.0.0, by default, the system considers the mask length as 0 and matches the route.

If the next hop address or source address of a route to be filtered is not 0.0.0.0, by default, the system considers the mask length as 32 and matches the route.

- When you run the **rule** command to configure a filtering rule in an ACL, only the **source** and **time-range** parameters are valid for the filtering rule.
- Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes match the ACL.
- Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

Set an IP prefix list named **p1** to filter routes.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match ip next-hop ip-prefix p1
```

Set a rule that source addresses of routes match ACL 2000 to filter routes.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match ip route-source acl 2000
```

7.9.43 if-match ip-prefix

Function

The **if-match ip-prefix** command creates a matching rule based on the IP prefix list.

The **undo if-match ip-prefix** command deletes the matching rule based on the specified IP prefix list.

By default, no matching rule based on the IP prefix list is configured in the routing policy.

Format

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix *ip-prefix-name*

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The routing policy matches routes using the IP prefix list. Routes are either permitted or denied.

The **ip ip-prefix** command must be used so that the matching rule can take effect. For example:

- If the **if-match ip-prefix aa** command is used but the IP prefix **aa** is not configured, all routes are permitted, that is, all routes match the matching rule.
- If the **if-match ip-prefix aa** and **ip ip-prefix aa permit 10.1.1.1 32** commands are used, the routes with the IP prefix being 10.1.1.1 and mask being 32 are permitted.

Prerequisites

The **if-match ip-prefix** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on IP prefix information. Routes that match the IP prefix information will be checked by other **if-match** clauses of this node. Routes that do not match the IP prefix information will be checked by the next node.

The **if-match acl** and **if-match ip-prefix** commands cannot be used together in the same node of a routing policy, because the latest configuration will override the previous one.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

Set an IP prefix list named **p1** to filter routes.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match ip-prefix p1
```

7.9.44 if-match ipv6

Function

The **if-match ipv6** command creates a matching rule based on IPv6 information.

The **undo if-match ipv6** command deletes a specified matching rule based on IPv6 information.

By default, no matching rule based on IPv6 information is configured in a routing policy.

Format

if-match ipv6 { **address** | **next-hop** | **route-source** } **prefix-list** *ipv6-prefix-name*

undo if-match ipv6 { **address** | **next-hop** | **route-source** } **prefix-list** *ipv6-prefix-name*

Parameters

Parameter	Description	Value
address	Matches the destination addresses of IPv6 routes.	-
next-hop	Matches the next hops of IPv6 routes. **NOTE** The S500 series switches do not support this parameter.	-
route-source	Matches the source addresses of the advertised IPv6 routes.	-
prefix-list	Indicates the IP prefix list.	-
ipv6-prefix-name	Specifies the name of the IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip ipv6-prefix** command must be used to configure an IPv6 prefix so that the matching rule (based on the destination addresses, next hop addresses, or source addresses of IPv6 routes) configured using the **if-match ipv6** command can take effect. If the **ip ipv6-prefix** command is not configured, all routes are permitted.

Prerequisites

The **if-match ipv6** command can be configured only after the **route-policy** command is configured.

Before running the **if-match ipv6** command, you must run the **ip ipv6-prefix** command to configure an IPv6 prefix.

Precautions

- When you filter routes based on the destination addresses, next hop addresses, or source addresses of IPv6 routes, the routes that match the matching rule are permitted and the routes that do not match the matching rule are denied.
- If the next hop address or source address of a route to be filtered is 0::0, by default, the system matches the route and considers that its mask length is 0.

  If the next hop address or source address of a route to be filtered is not 0::0, by default, the system matches the route and considers that its mask length is 128.
- Creating an IPv6 prefix list before it is referenced is recommended. If a nonexistent IPv6 prefix list is referenced using the command, all routes match the IPv6 prefix list.

Example

Define an if-match clause to match the related IPv6 routing information.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match ipv6 address prefix-list p1
[HUAWEI-route-policy] if-match ipv6 next-hop prefix-list p1
[HUAWEI-route-policy] if-match ipv6 route-source prefix-list p1
```

7.9.45 if-match mpls-label

Function

The **if-match mpls-label** command creates a matching rule based on the MPLS label.

The **undo if-match mpls-label** command deletes the matching rule based on the specified MPLS label.

By default, no matching rule based on the MPLS label is configured.

NOTE

Only the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H support this command.

Format

if-match mpls-label

undo if-match mpls-label

Parameters

None

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where inter-AS VPN Option C or Carrier Support Carrier (CSC) is deployed, you can use the **if-match mpls-label** command to allocate labels to public routes.

Prerequisites

The **if-match mpls-label** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the MPLS label. Routes that match the MPLS label will be checked by other **if-match** clauses of this node. Routes that do not match the MPLS label will be checked by the next node.

Example

Assign MPLS labels to the routes that match the routing policy.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match mpls-label
```

7.9.46 if-match rd-filter

Function

The **if-match rd-filter** command creates a matching rule based on the RD filter.

The **undo if-match rd-filter** command deletes the matching rule based on the specified RD filter.

By default, no matching rule based on the RD filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

if-match rd-filter *rd-filter-number*

undo if-match rd-filter

Parameters

Parameter	Description	Value
rd-filter-number	Specifies the number of an RD filter.	The value is an integer ranging from 1 to 255.

Views

Route-policy view, Tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **if-match rd-filter** command and the **ip rd-filter** command work together to filter routes based on RD attributes. For example:

- If **if-match rd-filter 1** is configured, but **rd-filter 1** is not configured, then all current routes will be permitted.
- If **if-match rd-filter 1** is configured, and **ip rd-filter 1 permit 1:1** has been configured, then routes with RD 1:1 will be permitted.

Prerequisites

The **if-match rd-filter** command must be run after the **route-policy** command is run.

Precautions

The routing policy matches routes using the RD filter. Routes that match the RD filter will be checked by other **if-match** clauses of this node. Routes that do not match the RD filter will be checked by the next node.

Example

Define a matching rule to match an RD filter.

```
<HUAWEI> system-view
[HUAWEI] route-policy abc permit node 10
[HUAWEI-route-policy] if-match rd-filter 1
```

7.9.47 if-match route-type

Function

The **if-match route-type** command sets a matching rule that is based on the route type.

The **undo if-match route-type** command deletes the matching rule based on the specified route type.

By default, no matching rule based on the route type is configured.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** }

undo if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** }

Parameters

Parameter	Description	Value
external-type1	Indicates OSPF external Type 1 routes.	-
external-type1or2	Indicates OSPF external routes.	-
external-type2	Indicates OSPF external Type 2 routes.	-
internal	Indicates internal routes, including OSPF inter-area routes and intra-area routes.	-
is-is-level-1	Indicates IS-IS Level-1 routes.	-
is-is-level-2	Indicates IS-IS Level-2 routes.	-
nssa-external-type1	Indicates NSSA external Type 1 routes.	-
nssa-external-type1or2	Indicates NSSA external routes.	-
nssa-external-type2	Indicates NSSA external Type 2 routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match route-type** command to filter OSPF or IS-IS routes based on the route type.

Multiple **if-match route-type** clauses can be specified. The relationship between **if-match route-type** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

The **if-match route-type** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the route type. Routes that match the route type will be checked by other **if-match** clauses of this node. Routes that do not match the route type will be checked by the next node.

For the same node in a routing policy, if two **if-match route-type** clauses are the same, the latter **if-match route-type** will not override the previous **if-match route-type**. After the latter clause is configured, both clauses take effect simultaneously. The relationship between **if-match route-type** clauses is "OR". That is, the actions defined by **apply** clauses can be performed on a route as long as the route meets one of the matching rules. For example, if both the **if-match route-type is-is-level-1** and **if-match route-type external-type1or2** commands are configured on the same node of a route policy, both IS-IS Level-1 routes and OSPF external routes can match the route policy.

NOTE

external-type1or2 refers to **external-type1** or **external-type2**. For the same node in a route policy, configuring both the **if-match route-type external-type1** and **if-match route-type external-type2** is equivalent to configuring the **if-match route-type external-type1or2** command. The two operations generate the same configuration file.

Similarly, **nssa-external-type1or2** refers to **nssa-external-type1** or **nssa-external-type2**. For the same node in a route policy, configuring both the **if-match route-type nssa-external-type1** and **if-match route-type nssa-external-type2** commands is equivalent to configuring the **if-match route-type nssa-external-type1or2** command. The two operations generate the same configuration file.

Example

Define a rule to match the routes of the specified type.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match route-type nssa-external-type1
```

7.9.48 if-match tag

Function

The **if-match tag** command sets a matching rule that is based on the route tag.

The **undo if-match tag** command deletes the matching rule based on the specified route tag.

By default, no matching rule based on the route tag is configured.

Format

if-match tag *tag*

undo if-match tag

Parameters

Parameter	Description	Value
tag	Indicates the tag value. Route tags classify routes as required. The same type of routes has the same tags. Routes are managed and controlled based on the tag by using the routing policy.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match tag** command to filter routes based on the tags.

Prerequisites

The **if-match tag** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the route tag. Routes that match the route tag will be checked by other **if-match** clauses of this node. Routes that do not match the route tag will be checked by the next node.

Example

Define a rule to match the OSPF routes with the tag value 8.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy permit node 10
[HUAWEI-route-policy] if-match tag 8
```

7.9.49 ip as-path-filter

Function

The **ip as-path-filter** command creates an AS_Path filter.

The **undo ip as-path-filter** command deletes a specified AS_Path filter.

By default, no AS_Path filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

ip as-path-filter { *as-path-filter-number* | *as-path-filter-name* } { **deny** | **permit** } *regular-expression*

undo ip as-path-filter { *as-path-filter-number* | *as-path-filter-name* } [{ **deny** | **permit** } *regular-expression*]

Parameters

Parameter	Description	Value
as-path-filter-number	Specifies the number of an AS_Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter-name	Specifies the name of an AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
deny	Sets the matching mode of the AS_Path filter to deny.	-
permit	Sets the matching mode of the AS_Path filter to permit.	-
regular-expression	Specifies the AS_Path regular expression.	The value is a string of 1 to 255 characters, with spaces supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AS_Path filter uses the regular expression to define matching rules. After an AS_Path filter is set, the RM module immediately instructs each protocol to apply the filter by default.

The AS_Path attribute is a private attribute of BGP, and is used to filter BGP routes.

- The filter can be directly applied by using a command such as **peer as-path-filter**.
- The filter can be used as a matching condition of a routing policy by using a command such as **if-match as-path-filter zz**.

Configuration Impact

Multiple rules (permit or deny) can be specified in a filter.

By default, AS_Path filters work in **deny** mode. If all matching rules in a filter are configured to work in **deny** mode, all routes are denied by the filter; to prevent this problem, configure one matching rule in **permit** mode after one or multiple matching rules in **deny** mode so that the routes except for those denied by preceding matching rules are permitted by the filter.

Before you run the **undo ip as-path-filter** command to delete an AS_Path filter that is referenced by another command, delete the reference configuration.

Follow-up Procedure

To view detailed configurations of the AS_Path filter, run the **display ip as-path-filter** command.

Example

Create the AS_Path filter with the sequence number being 1, and permit routes that begin with 10 in the AS_Path to pass.

```
<HUAWEI> system-view
[HUAWEI] ip as-path-filter 1 permit ^10_
```

Create the AS_Path filter 2, and permit routes that contain 20 in the AS_Path to pass through.

```
<HUAWEI> system-view
[HUAWEI] ip as-path-filter 2 permit _20_
```

Create the AS_Path filter 3, and prohibit routes that contain 30 in the AS_Path from passing through.

```
<HUAWEI> system-view
```

```
[HUAWEI] ip as-path-filter 3 deny _30_
[HUAWEI] ip as-path-filter 3 permit .*
```

7.9.50 ip community-filter

Function

The **ip community-filter** command creates a community filter.

The **undo ip community-filter** command deletes a community filter.

By default, no community filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

ip community-filter { **basic** *comm-filter-name* | *basic-comm-filter-num* } { **permit** | **deny** } [*community-number* | *aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] &<1-20>

ip community-filter { **advanced** *comm-filter-name* | *adv-comm-filter-num* } { **permit** | **deny** } *regular-expression*

undo ip community-filter { **basic** *comm-filter-name* | *basic-comm-filter-num* } [**permit** | **deny**] [*community-number* | *aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] &<1-20>

undo ip community-filter { **advanced** *comm-filter-name* | *adv-comm-filter-num* } [**permit** | **deny**] [*regular-expression*]

Parameters

Parameter	Description	Value
basic *comm-filter-name*	Specifies the name of a basic community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
basic-comm-filter-num	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
deny	Sets the matching mode of the community filter to deny.	-
permit	Sets the matching mode of the community filter to permit.	-
community-number	Specifies the community number.	The value is an integer ranging from 0 to 4294967295.

Parameter	Description	Value
aa:nn	Specifies the community number. You can configure a maximum of 20 community numbers once. ● If you do not configure any one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 20 *community-number* and *aa:nn* together. ● If you configure one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 19 *community-number* and *aa:nn* together. ● If you configure two of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 18 *community-number* and *aa:nn* together. ● If you configure three of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 17 *community-number* and *aa:nn* together. ● If you configure all of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 16 *community-number* and *aa:nn* together.	*aa* and *nn* are integers ranging from 0 to 65535.
internet	Indicates that the matching routes can be sent to any peer.	-
no-export-subconfed	Indicates that routes are not advertised outside an AS. If an AS confederation is used, routes are not advertised to any other sub-ASs in the AS confederation.	-
no-advertise	Indicates that routes are not advertised to other peers.	-
no-export	Indicates that routes are not advertised outside an AS. If an AS confederation is used, routes are not advertised outside the AS confederation, but to other sub-ASs.	-

Parameter	Description	Value
advanced *comm-filter-name*	Specifies the name of an advanced community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
adv-comm-filter-num	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
regular-expression	Specifies the regular expression used to match the community information.	The value is a string of 1 to 255 case-sensitive characters, with spaces supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The community attribute is a private attribute of BGP, and can be used only to filter BGP routes. The community attribute can be used as a matching rule of a routing policy by using the **ip community-filter** and **if-match community-filter** commands together.

Precautions

Only the community number or known community attribute can be specified for a basic community filter. The regular expression can be used as a matching rule in an advanced community filter.

- The **ip community-filter basic** *comm-filter-name* command or the **ip community-filter** *basic-comm-filter-num* command can be used to configure a basic community filter. **basic** *comm-filter-name* specifies the name of a basic community filter, and the name cannot be all digits. A maximum of 20 community numbers can be configured in one command. *basic-comm-filter-num* specifies only the basic community filter with the number ranging from 1 to 99. A maximum of 20 community numbers can be configured in one command.

- The **ip community-filter advanced** *comm-filter-name* command or the **ip community-filter** *adv-comm-filter-num* command can be used to configure an advanced community filter. **advanced** *comm-filter-name* specifies the name of an advanced community filter, and the name cannot be all digits. *adv-comm-filter-num* specifies only the advanced community filter with the number ranging from 100 to 199.

The relationship between the rules of the community filter is "AND". This is different from the route distinguisher (RD) filter. This is because each route has only one RD but can have multiple communities.

For example, the community filters in the following formats have different matching results:

Format 1:

```
ip community-filter 1 permit 100:1 200:1 300:1
```

Format 2:

```
ip community-filter 1 permit 100:1
ip community-filter 1 permit 200:1 300:1
```

In the preceding configuration of the community filter, the community defined in each rule must be a sub-set of route communities so that the rule can be matched.

The RD filters in the following formats have the same matching results:

Format 1:

```
ip rd-filter 100 permit 100:1 200:1 2.2.2.2:1 3.3.3.3:1
```

Format 2:

```
ip rd-filter 100 permit 100:1 200:1
ip rd-filter 100 permit 2.2.2.2:1
ip rd-filter 100 permit 3.3.3.3:1
```

The **apply comm-filter delete** command run in the Route-Policy view deletes the specified community attribute from routes. An **ip community-filter** command can be used to specify community attributes but one such command specifies only one community attribute each time. To delete more than one community attribute, run the **ip community-filter** command multiple times. If multiple community attributes are specified in one filter, none of them can be deleted. For information about examples, see **apply comm-filter delete**.

By default, Community filters work in **deny** mode. If all matching rules in a filter are configured to work in **deny** mode, all routes are denied by the filter; to prevent this problem, configure one matching rule in **permit** mode after one or multiple matching rules in **deny** mode so that the routes except for those denied by preceding matching rules are permitted by the filter.

Before you run the **undo ip community-filter** command to delete a community attribute filter that is referenced by another command, delete the reference configuration.

Follow-up Procedure

By default, the Route Management (RM) module will instruct all protocols to apply this community filter. To delay the effective time, run the **route-policy-change notify-delay** command.

Run the **display ip community-filter** command to view detailed configuration for the community filter.

Example

Configure a basic community filter of which the sequence number is 1 to prevent matching routes from being advertised to any peer.

```
<HUAWEI> system-view
[HUAWEI] ip community-filter 1 deny internet
```

Configure an advanced community filter of which the sequence number is 100 to permit all the routes that match the AS 65001.

```
<HUAWEI> system-view
[HUAWEI] ip community-filter advanced 100 permit 65001:[0-9]+
```

7.9.51 ip extcommunity-filter

Function

The **ip extcommunity-filter** command creates an extended community filter.

The **undo ip extcommunity-filter** command deletes an extended community filter.

By default, no extended community filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

ip extcommunity-filter { *basic-extcomm-filter-num* | **basic** *basic-extcomm-filter-name* } { **deny** | **permit** } { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address.nn* } } &<1-16>

ip extcommunity-filter { *advanced-extcomm-filter-num* | **advanced** *advanced-extcomm-filter-name* } { **deny** | **permit** } *regular-expression*

undo ip extcommunity-filter { *basic-extcomm-filter-num* | **basic** *basic-extcomm-filter-name* } [{ **deny** | **permit** } { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address.nn* } } &<1-16>]

undo ip extcommunity-filter { *advanced-extcomm-filter-num* | **advanced** *advanced-extcomm-filter-name* } [*regular-expression*]

Parameters

Parameter	Description	Value
deny	Sets the matching mode of the extended community filter to deny.	-
permit	Sets the matching mode of the extended community filter to permit.	-
rt	Sets the extended community filter type to RT.	-
as-number	Specifies the AS number.	The value is an integer ranging from 0 to 65535.
4as-number	Specifies a 4-byte AS number.	A 4-byte AS number is divided into the following types: ● It is an integer ranging from 65536 to 4294967295. ● It is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535.
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
nn	Specifies an integer.	● When the value of *as-number* is a 2-byte AS number, the value of *nn* ranges from 0 to 4294967295. ● When the value of *4as-number* is a 4-byte AS number, the value of *nn* ranges from 0 to 65535. ● For *ipv4-address*, the value of *nn* ranges from 0 to 65535.
basic-extcomm-filter-num	Specifies the number of a basic extended community filter.	The value is an integer ranging from 1 to 199.

Parameter	Description	Value
basic *basic-extcomm-filter-name*	Specifies the name of a basic extended community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The value cannot contain only numerals. When double quotation marks are used around the string, spaces are allowed in the string.
advanced-extcomm-filter-num	Specifies the number of an advanced extended community filter.	The value is an integer ranging from 200 to 399.
advanced *advanced-extcomm-filter-name*	Specifies the name of an advanced extended community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The value cannot contain only numerals. When double quotation marks are used around the string, spaces are allowed in the string.
regular-expression	Specifies the regular expression used to match the extended community information.	It is a string of 1 to 255 space-tolerant characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An extended community filter can be used as a matching condition of a route-policy by using a command such as **if-match extcommunity-filter zz**.

Only the extended community number can be specified for a basic extended community filter. The regular expression can be used as a matching rule in an advanced extended community filter.

- The **ip extcommunity-filter basic** *extcomm-filter-name* command or the **ip extcommunity-filter** *basic-extcomm-filter-num* command can be used to configure a basic extended community filter. **basic** *extcomm-filter-name* specifies the name of a basic extended community filter, and the name cannot be all digits. *basic-extcomm-filter-num* specifies only the basic extended community filter with the number ranging from 1 to 199. A maximum of 16 extended community numbers can be configured using one command.

- The **ip extcommunity-filter advanced** *extcomm-filter-name* command or the **ip extcommunity-filter** *adv-extcomm-filter-num* command can be used to configure an advanced extended community filter. **advanced** *extcomm-filter-name* specifies the name of an advanced extended community filter, and the name cannot be all digits. *adv-extcomm-filter-num* specifies only the advanced extended community filter with the number ranging from 200 to 399.

The relationship between the rules of the extended community filter is "OR".

For example, the extended community filters in the following formats have the same matching results:

Format 1:

```
ip extcommunity-filter 1 permit rt 100:1 200:1 300:1
```

Format 2:

```
ip extcommunity-filter 1 permit rt 100:1
ip extcommunity-filter 1 permit rt 200:1 300:1
```

After the extended community filter is configured, if the policy application delay is set by using the **route-policy-change notify-delay** command, the Route Management (RM) module will instruct each protocol to apply this filter after the delay expires. By default, the RM module instructs each protocol to immediately apply this filter.

The **undo ip extcommunity-filter** command is used to delete a specified extended community filter.

The **display ip extcommunity-filter** command is used to display the detailed configurations of the extended community filter.

Configuration Impact

The **ip extcommunity-filter** command is used to filter routes based on the RT attributes of the routes. The routes that pass the filtering are permitted to pass through and the routes that fail to pass the filtering are denied.

Precautions

The extended community attributes of a route include VPN-target and Site-of-Origin (SoO). Only VPN-target, however, is supported by the policy.

By default, extended community filters work in **deny** mode. If all matching rules in a filter are configured to work in **deny** mode, all routes are denied by the filter; to prevent this problem, configure one matching rule in **permit** mode after one or multiple matching rules in **deny** mode so that the routes except for those denied by preceding matching rules are permitted by the filter.

Example

Configure an RT extended community filter of which the sequence number is 1.

```
<HUAWEI> system-view
[HUAWEI] ip extcommunity-filter 1 deny rt 200:200
```

7.9.52 ip ip-prefix

Function

The **ip ip-prefix** command creates an IPv4 prefix list or an entry in an IPv4 prefix list.

The **undo ip ip-prefix** command deletes an IPv4 prefix list or an entry from an IPv4 prefix list.

By default, no IPv4 prefix list is created.

Format

ip ip-prefix *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ipv4-address mask-length* [**match-network**] [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

ip ip-prefix *ip-prefix-name* **description** *text*

undo ip ip-prefix *ip-prefix-name* **description** [*text*]

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IPv4 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
index *index-number*	Specifies the sequence number of an entry in the IPv4 prefix list.	The value is an integer that ranges from 1 to 4294967295. By default, the sequence number increases by 10 according to the configuration order, and the first sequence number is 10. **NOTE** A maximum of 65535 entries can be configured in an IP prefix list.

Parameter	Description	Value
permit	Specifies the matching mode of the IP prefix list as permit. In permit mode, if the IP address to be filtered is within the defined prefix range, the IP address matches the routing policy and does not continue to match the next entry. Otherwise, the IP address continues to match the next entry.	-
deny	Specifies the matching mode of the IP prefix list as deny. In deny mode, if the IP address to be filtered is within the defined prefix range, the IP address fails to match the routing policy and cannot match the next entry. Otherwise, the IP address continues to match the next entry.	-
ipv4-address	Specifies an IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
match-network	Matches the network address. The **match-network** parameter can be configured only when the IP address generated after *ipv4-address* is ANDed with *mask-length* is 0.0.0.0. This parameter is mainly used to match routes with a specified network address. For example, the **ip ip-prefix prefix1 permit 0.0.0.0 8** command filters all routes with mask length 8, while the **ip ip-prefix prefix1 permit 0.0.0.0 8 match-network** command filters all routes to the IP address range from 0.0.0.1 to 0.255.255.255.	-
greater-equal *greater-equal-value*	Specifies the lower threshold of the mask length. If **greater-equal** *greater-equal-value* and **less-equal** *less-equal-value* are not specified, the value of *mask-length* is the mask length.	*greater-equal-value* must meet the following requirement: *mask-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. If **greater-equal** is configured, the mask ranges from *greater-equal-value* to 32.

Parameter	Description	Value
less-equal *less-equal-value*	Specifies the upper threshold of the mask length. If **greater-equal** *greater-equal-value* and **less-equal** *less-equal-value* are not specified, the value of *mask-length* is the mask length.	*less-equal-value* must meet the following requirement: *mask-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. If **less-equal** is configured, the mask ranges from *mask-length* to *less-equal-value*.
description *text*	Specifies the description of the IP prefix list.	The value is a string of 1 to 80 case-sensitive characters without spaces. If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP prefix list can be used as a filter or as matching conditions of a routing policy when it is used together with the **if-match** command.

Each entry in an IP prefix list can be used as a filtering rule. When a route to be filtered matches an entry, whether the route matches the IP prefix list is determined by the matching mode. A route to be filtered matches an entry or entries based on the following rules:

- Sequential matching: The route has to match the entries in the IP prefix list in ascending order of their *index-number* values. Therefore, specifying *index-number* in a required sequence is recommended.
- One-time matching: If a route matches one entry, the route matches the IP prefix list and will not be matched against the next entry.
- Matching failure by default: If a route fails to match any of the entries, it fails to match the IP prefix list.

The following example shows how different IP prefix lists take effect on the routes 1.1.1.1/24, 1.1.1.1/32, 1.1.1.1/26, 2.2.2.2/24, and 1.1.1.2/16.

Table 7-201 Matching results of IP prefix lists

Case	Commands	Matching result	Note
1	`ip ip-prefix aa index 10 permit 1.1.1.1 24`	Only the route 1.1.1.1/24 is permitted, and the other routes are denied.	This is a single-node accurate matching case, which indicates that only the route whose destination IP address and mask are the same as those specified by the entry meets the matching conditions. In addition, **permit** is configured as the matching mode. Therefore, the route 1.1.1.1/24 is permitted, and other routes are denied because they fail to meet the matching conditions.
2	`ip ip-prefix aa index 10 deny 1.1.1.1 24`	All routes are denied.	This is also a single-node accurate matching case. **deny** is configured as the matching mode. Therefore, the route 1.1.1.1/24 is denied, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.
3	`ip ip-prefix aa index 10 permit 1.1.1.1 24 less-equal 32`	The routes 1.1.1.1/24, 1.1.1.1/32, and 1.1.1.1/26 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, and **less-equal** is set to 32. Therefore, the routes with 1.1.1.0 as the prefix and the mask ranging from 24 to 32 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.
4	`ip ip-prefix aa index 10 permit 1.1.1.0 24 greater-equal 24 less-equal 32`	The routes 1.1.1.1/24, 1.1.1.1/32, and 1.1.1.1/26 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, **greater-equal** is set to 24, and **less-equal** is set to 32. Therefore, the routes with 1.1.1.0 as the prefix and the mask ranging from 24 to 32 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions. This case is similar to case 3 in terms of the matching result.

Case	Commands	Matching result	Note
5	`ip ip-prefix aa index 10 permit 1.1.1.1 24 greater-equal 26`	The routes 1.1.1.1/32 and 1.1.1.1/26 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, and **greater-equal** is set to 26. Therefore, the routes with 1.1.1.0 as the prefix and the mask ranging from 26 to 32 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.
6	`ip ip-prefix aa index 10 permit 1.1.1.1 24 greater-equal 26 less-equal 32`	The routes 1.1.1.1/32 and 1.1.1.1/26 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, **greater-equal** is set to 26, and **less-equal** is set to 32. Therefore, the routes with 1.1.1.0 as the prefix and the mask ranging from 26 to 32 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions. This case is similar to case 5 in terms of the matching result.
7	`ip ip-prefix aa index 10 deny 1.1.1.1 24` `ip ip-prefix aa index 20 permit 1.1.1.1 32`	The route 1.1.1.1/32 is permitted, and the other routes are denied.	This is a multi-node accurate matching case. **deny** is configured as the matching mode of the matching entry indexed 10, and therefore the route 1.1.1.1/24 is denied by the matching entry indexed 10 based on the rule of one-time matching. The route 1.1.1.1/32 fails to match the matching conditions, and it is then matched against the entry indexed 20 for which **permit** is configured as the matching mode. Consequently, the route 1.1.1.1/32 matches the matching conditions of the entry indexed 20. The other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.

Case	Commands	Matching result	Note
8	`ip ip-prefix aa index 10 permit 0.0.0.0 8 less-equal 32`	The routes 1.1.1.1/24, 1.1.1.1/32, 1.1.1.1/26, 2.2.2.2/24, and 1.1.1.2/16 are all permitted.	If the IP prefix is 0.0.0.0 and you specify a mask and a mask length range after this IP prefix, all routes with the mask length within the specified mask length range are denied or permitted, regardless of the mask. The mask length range is from 8 to 32, 0.0.0.0 is specified as the IP address, and **permit** is configured as the matching mode. Therefore, all routes with the mask length within the range are permitted.
9	`ip ip-prefix aa index 10 deny 0.0.0.0 24 less-equal 32` `ip ip-prefix aa index 20 permit 0.0.0.0 0 less-equal 32`	The route 1.1.1.2/16 is permitted, and the other routes are denied.	Note: For the entry indexed 10, the mask length range is from 24 to 32, 0.0.0.0 is specified as the IP address, and **deny** is configured as the matching mode. Therefore, all routes with the mask length within the range are denied, and the route 1.1.1.2/16 that fails to match its matching conditions is then matched against the entry indexed 20. For the entry indexed 20, the mask length range is from 0 to 32, 0.0.0.0 is specified as the IP address, and **permit** is configured as the matching mode. Therefore, the route 1.1.1.2/16 is permitted by the entry indexed 20.
9	`ip ip-prefix aa index 10 deny 2.2.2.2 24` `ip ip-prefix aa index 20 permit 0.0.0.0 0 less-equal 32`	All routes except the route 2.2.2.2/24 are permitted.	For the entry indexed 10, **deny** is configured as the matching mode. Therefore, the route 2.2.2.2/24 that matches its matching conditions is denied, and the other routes that fail to match the matching conditions are then matched against the entry indexed 20. For the entry indexed 20, the mask length range is from 0 to 32, 0.0.0.0 is specified as the IP address, and **permit** is configured as the matching mode. Therefore, all routes except the route 2.2.2.2/24 are permitted by the entry indexed 20.

Configuration Impact

If you create an entry whose *index-number* has existed in the same IP prefix list but has different filtering rules, the new entry overwrites the existing one.

Precautions

- Because of the matching failure by default, if one or more than one entry with **deny** as the matching mode is created, create an entry using the **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] **permit 0.0.0.0 0 less-equal 32** command so that all IPv4 routes may match the IP prefix list.
- If *ipv4-address mask-length* is specified as **0.0.0.0 0**, only default routes are matched.
- If *ipv4-address mask-length* is set to **0.0.0.0 0 less-equal 32**, all routes are matched.
- Before you run the **undo ip ip-prefix** command to delete an IP prefix list that is referenced by another command, delete the reference configuration.
- After a configuration is delivered, the device checks the validity of the parameters in the configuration and processes these parameters. After the processing, the generated configuration is the result of the AND calculation between the specified *ipv4-address* and *mask-length*. For example, if the specified *ipv4-address* and *mask-length* are 1.1.1.1 and 24, respectively, the generated configuration is 1.1.1.0 24.

  If the *ipv4-address* in the generated configuration is 0.0.0.0, the configuration matches all IPv4 addresses. In this case, routes are filtered based on the following rules.

  NOTE

  If the specified *ipv4-address* is not 0.0.0.0, the *mask-length* must not be 0.

Table 7-202 Route filtering rules

Whether *greater-equal* and *less-equal* Exist in the Post-Processing Configuration	**Condition**	**Matching Result**	**Example**

Neither *greater-equal* nor *less-equal* exists.	The post-processing *ipv4-address* and *mask-length* are 0.0.0.0 and X (non-0 value), respectively.	Matches all routes with the mask length of X.	Pre-processing:
			`ip ip-prefix aa index 10 permit 0.0.1.1 16`
			Post-processing:
			`ip ip-prefix aa index 10 permit 0.0.0.0 16`
			Matching result: The routes with the mask length of 16 are permitted.

greater-equal exists, but *less-equal* does not.	The post-processing *ipv4-address* and *mask-length* are 0.0.0.0 and X (non-0 value), respectively.	Matches all the routes whose mask length is within the range from *greater-equal* to 32.	Pre-processing:
			`ip ip-prefix aa index 10 permit 0.0.1.1 16 greater-equal 20`
			Post-processing:
			`ip ip-prefix aa index 10 permit 0.0.0.0 16 greater-equal 20 less-equal 32`
			Matching result: The routes whose mask length is within the range from 20 to 32 are permitted.

greater-equal does not exist, but *less-equal* does.	The post-processing *ipv4-address* and *mask-length* are 0.0.0.0 and X (non-0 value), respectively.	Matches all the routes whose mask length is within the range from X to *less-equal*.	Pre-processing:
			`ip ip-prefix aa index 10 permit 0.0.1.1 16 less-equal 30`
			Post-processing:
			`ip ip-prefix aa index 10 permit 0.0.0.0 16 greater-equal 16 less-equal 30`
			Matching result: The routes whose mask length is within the range from 16 to 30 are permitted.

Whether *greater-equal* and *less-equal* Exist in the Post-Processing Configuration	Condition	Matching Result	Example

Both *greater-equal* and *less-equal* exist.	The post-processing *ipv4-address* and *mask-length* are 0.0.0.0 and X (non-0 value), respectively.	Matches all the routes whose mask length is within the range from *greater-equal* to *less-equal*.	Pre-processing:
			`ip ip-prefix aa index 10 permit 0.0.1.1 16 greater-equal 20 less-equal 30`
			Post-processing:
			`ip ip-prefix aa index 10 permit 0.0.0.0 16 greater-equal 20 less-equal 30`
			Matching result: The routes whose mask length is within the range from 20 to 30 are permitted.

Follow-up Procedure

In a scenario in which a routing policy is being modified, after an IP prefix is configured, the RM module notifies protocols of applying the changed routing policy immediately by default. However, in some cases, multiple commands need to be run to modify a routing policy. If other commands need to be run after an IP prefix is configured, protocols may apply the routing policy whose modification is not complete yet. To solve this problem, run the **route-policy-change notify-delay** command to configure a delay for protocols to apply the changed routing policy.

Example

Configure the IP prefix list named **p1** to permit only the routes with the mask length ranging from 17 to 18 on the network segment 10.0.0.0/8.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

Configure the IP prefix list named **p3** to deny the routes to the IP address ranging from 0.0.0.1 to 0.255.255.255.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix p3 index 10 deny 0.0.0.0 8 match-network
[HUAWEI] ip ip-prefix p3 index 20 permit 0.0.0.0 0 less-equal 32
```

7.9.53 ip ipv6-prefix

Function

The **ip ipv6-prefix** command configures an IPv6 prefix list or an entry in an IPv6 prefix list.

The **undo ip ipv6-prefix** command deletes an IPv6 prefix list or an entry from an IPv6 prefix list.

By default, no IPv6 prefix list is created.

Format

ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address prefix-length* [**match-network**] [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]

undo ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*]

ip ipv6-prefix *ipv6-prefix-name* **description** *text*

undo ip ipv6-prefix *ipv6-prefix-name* **description** [*text*]

Parameters

Parameter	Description	Value
ipv6-prefix-name	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
index *index-number*	Specifies the sequence number of an entry in the IPv6 prefix list.	The value is an integer that ranges from 1 to 4294967295. By default, the sequence number increases by 10 according to the configuration order, and the first sequence number is 10. **NOTE** A maximum of 65535 entries can be configured in an IPv6 prefix list.

Parameter	Description	Value
permit	Specifies the matching mode of the IPv6 prefix list as permit. In permit mode, if the IPv6 address to be filtered is within the defined prefix range, the IPv6 address matches the routing policy and does not continue to match the next entry. Otherwise, the IPv6 address continues to match the next entry.	-
deny	Specifies the matching mode of the IPv6 prefix list as deny. In deny mode, if the IPv6 address to be filtered is within the defined prefix range, the IPv6 address fails to match the routing policy and cannot match the next entry. Otherwise, the IPv6 address continues to match the next entry.	-
ipv6-address	Specifies the IPv6 prefix range in the form of an IPv6 address. If :: is specified, the address 0::0 is matched.	-
prefix-length	Specifies the IPv6 prefix range using the mask length.	The value is an integer that ranges from 0 to 128. If ::0 less-equal 128 is used, all IPv6 addresses are matched.
match-network	Matches the network address. The **match-network** parameter can be configured only when the IP address generated after *ipv6-address* is ANDed with *prefix-length* is ::. For example, the **ip ipv6-prefix prefix1 permit :: 96** command filters all IPv6 routes with mask length 96, while the **ip ipv6-prefix prefix1 permit :: 96 match-network** command filters all routes to the IPv6 address range from ::1 to ::FFFF:FFFF.	-
greater-equal *greater-equal-value*	Specifies the lower threshold of the mask length.	*greater-equal-value* must meet the following requirement: *prefix-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128.

Parameter	Description	Value
less-equal *less-equal-value*	Specifies the upper threshold of the mask length.	*less-equal-value* must meet the following requirement: *prefix-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128.
description *text*	Specifies the description of the IPv6 prefix list.	The value is a string of 1 to 80 case-sensitive characters without spaces. If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv6 prefix list can be used by the protocols as a prefix filter, or used with the **if-match ipv6** command as a matching condition of routing policies.

Each entry in the IPv6 prefix list can be considered as a filter rule. When a route to be filtered matches one of the entries, the route can be determined whether it is permitted the IPv6 prefix list based on the matching mode. Entries in the IPv6 prefix list can be matched with routes to be filtered based on the following rules:

- Sequence match: Each entry in the IP prefix list is matched in ascending order of the index number. When setting index numbers for entries, you can arrange your expected matching order.
- Unique match: When the route to be filtered matches one entry, the route stops to match the other entries.
- Default deny: By default, if routes to be filtered do not match any entry in the IP prefix list, the routes are denied by IP prefix list.

The following example shows how different IPv6 prefix lists take effect on the routes 1::1/96, 1::1/128, 1::1/100, 2::2/96, and 1::2/64.

Table 7-203 Matching results of IPv6 prefix lists

Case	Commands	Matching result	Note
1	`ip ipv6-prefix aa index 10 permit 1::1 96`	Only the route 1::1/96 is permitted, and the other routes are denied.	This is a single-node accurate matching case, which indicates that only the route whose destination IPv6 address and mask are the same as those specified by the entry meets the matching conditions. In addition, **permit** is configured as the matching mode. Therefore, the route 1::1/96 is permitted, and other routes are denied because they fail to meet the matching conditions.
2	`ip ipv6-prefix aa index 10 deny 1::1 96`	All routes are denied.	This is also a single-node accurate matching case. **deny** is configured as the matching mode. Therefore, the route 1::1/96 is denied, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.
3	`ip ipv6-prefix aa index 10 permit 1::1 96 less-equal 128`	The routes 1::1/96, 1::1/128, and 1::1/100 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, and **less-equal** is set to 128. Therefore, the routes with 1::1 as the prefix and the mask ranging from 96 to 128 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.
4	`ip ipv6-prefix aa index 10 permit 1::1 96 greater-equal 96 less-equal 128`	The routes 1::1/96, 1::1/128, and 1::1/100 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, **greater-equal** is set to 96, and **less-equal** is set to 128. Therefore, the routes with 1::1 as the prefix and the mask ranging from 96 to 128 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions. This case is similar to case 3 in terms of the matching result.

Case	Commands	Matching result	Note
5	ip ipv6-prefix aa index 10 permit 1::1 96 greater-equal 100	The routes 1::1/128 and 1::1/100 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, and **greater-equal** is set to 100. Therefore, the routes with 1::1 as the prefix and the mask ranging from 100 to 128 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.
6	ip ipv6-prefix aa index 10 permit 1::1 96 greater-equal 100 less-equal 128	The routes 1::1/128 and 1::1/100 are permitted, and the other routes are denied.	This is also a single-node accurate matching case. **permit** is configured as the matching mode, **greater-equal** is set to 100, and **less-equal** is set to 128. Therefore, the routes with 1::1 as the prefix and the mask ranging from 100 to 128 can be permitted, and the other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions. This case is similar to case 5 in terms of the matching result.
7	ip ipv6-prefix aa index 10 deny 1::1 96 ip ipv6-prefix aa index 20 permit 1::1 128	The route 1::1/128 is permitted, and the other routes are denied.	This is a multi-node accurate matching case. **deny** is configured as the matching mode of the matching entry indexed 10, and therefore the route 1::1/96 is denied by the matching entry indexed 10 based on the rule of one-time matching. The route 1::1/128 fails to match the matching conditions, and it is then matched against the entry indexed 20 for which **permit** is configured as the matching mode. Consequently, the route 1::1/128 matches the matching conditions of the entry indexed 20. The other routes are denied based on the rule of matching failure by default because they fail to meet the matching conditions.

Case	Commands	Matching result	Note
8	`ip ipv6-prefix aa index 10 permit :: 64 less-equal 128`	The routes 1::1/96, 1::1/128, 1::1/100, 2::2/96, and 1::2/64 are all permitted.	If the IPv6 prefix is :: and you specify a mask and a mask length range after this IPv6 prefix, all routes with the mask length within the specified mask length range are denied or permitted, regardless of the mask. The mask length range is from 64 to 128, :: is specified as the IPv6 address, and **permit** is configured as the matching mode. Therefore, all routes with the mask length within the range are permitted.
9	`ip ipv6-prefix aa index 10 deny :: 96 less-equal 128` `ip ipv6-prefix aa index 20 permit :: 0 less-equal 128`	The route 1::2/64 is permitted, and the other routes are denied.	For the entry indexed 10, the mask length range is from 96 to 128, :: is specified as the IPv6 address, and **deny** is configured as the matching mode. Therefore, all routes with the mask length within the range are denied, and the route 1::2/64 that fails to match its matching conditions is then matched against the entry indexed 20. For the entry indexed 20, the mask length range is from 0 to 128, :: is specified as the IPv6 address, and **permit** is configured as the matching mode. Therefore, the route 1::2/64 is permitted by the entry indexed 20.
10	`ip ipv6-prefix aa index 10 deny 2::2 96` `ip ipv6-prefix aa index 20 permit :: 0 less-equal 128`	All routes except the route 2::2/96 are permitted.	Note: For the entry indexed 10, **deny** is configured as the matching mode. Therefore, the route 2::2/96 that matches its matching conditions is denied, and the other routes that fail to match the matching conditions are then matched against the entry indexed 20. For the entry indexed 20, the mask length range is from 0 to 128, :: is specified as the IPv6 address, and **permit** is configured as the matching mode. Therefore, all routes except the route 2::2/96 are permitted by the entry indexed 20.

Configuration Impact

If you create an entry whose index number is the same as an existing entry in the IPv6 prefix list, the created entry will replace the existing entry.

Precautions

- The IPv6 prefix list adopts default deny as the matching mode. If you have created one or multiple entries in **deny** mode, but no entry in the **permit** mode, you must create an entry **permit :: 0 less-equal 128** to permit IPv6 routes which do not match the entries in **deny** mode.
- If you specify *ipv6-address prefix-length* to be :: 0, only IPv6 default routes are matched.
- If *ipv6-address prefix-length* is set to **:: 0 less-equal 128**, all routes will be matched.
- Before you run the **undo ip ipv6-prefix** command to delete an IPv6 prefix list that is referenced by another command, delete the reference configuration.
- After a configuration is delivered, the device checks the validity of the parameters in the configuration and processes these parameters. After the processing, the generated configuration is the result of the AND calculation between the specified *ipv6-address* and *prefix-length*. For example, if the specified *ipv6-address* and *prefix-length* are 1::1 and 64, respectively, the generated configuration is 1:: 64.

  If the *ipv6-address* in the generated configuration is ::, the configuration matches all IPv6 addresses. In this case, routes are filtered based on the following rules.

  NOTE

  If the specified *ipv6-address* is not ::, the *prefix-length* must not be 0.

Table 7-204 Route filtering rules

Whether *greater-equal* and *less-equal* Exist in the Post-Processing Configuration	**Condition**	**Matching Result**	**Example**

Neither *greater-equal* nor *less-equal* exists.	The post-processing *ipv6-address* and *prefix-length* are :: and X (non-0 value), respectively.	Matches all IPv6 routes with the prefix length of X.	Pre-processing:
			`ip ipv6-prefix aa index 10 permit ::1:1 96`
			Post-processing:
			`ip ipv6-prefix aa index 10 permit :: 96`
			Matching result: The IPv6 routes with the prefix length of 96 are permitted.

greater-equal exists, but *less-equal* does not.	The post-processing *ipv6-address* and *prefix-length* are :: and X (non-0 value), respectively.	Matches all the IPv6 routes whose prefix length is within the range from *greater-equal* to 128.	Pre-processing:
			`ip ipv6-prefix aa index 10 permit ::1:1 96 greater-equal 120`
			Post-processing:
			`ip ipv6-prefix aa index 10 permit :: 96 greater-equal 120 less-equal 128`
			Matching result: The IPv6 routes whose prefix length is within the range from 120 to 128 are permitted.

greater-equal does not exist, but *less-equal* does.	The post-processing *ipv6-address* and *prefix-length* are :: and X (non-0 value), respectively.	Matches all the IPv6 routes whose prefix length is within the range from X to *less-equal*.	Pre-processing:
			`ip ipv6-prefix aa index 10 permit ::1:1 96 less-equal 120`
			Post-processing:
			`ip ipv6-prefix aa index 10 permit :: 96 greater-equal 96 less-equal 120`
			Matching result: The IPv6 routes whose prefix length is within the range from 96 to 120 are permitted.

Whether *greater-equal* and *less-equal* Exist in the Post-Processing Configuration	Condition	Matching Result	Example

Both *greater-equal* and *less-equal* exist.	The post-processing *ipv6-address* and *prefix-length* are :: and X (non-0 value), respectively.	Matches all the IPv6 routes whose prefix length is within the range from *greater-equal* to *less-equal*.	Pre-processing:
			`ip ipv6-prefix aa index 10 permit ::1:1 96 greater-equal 120 less-equal 124`
			Post-processing:
			`ip ipv6-prefix aa index 10 permit :: 96 greater-equal 120 less-equal 124`
			Matching result: The IPv6 routes whose prefix length is within the range from 120 to 124 are permitted.

Follow-up Procedure

In a scenario in which a used routing policy is being modified, after you configure the IPv6 prefix list, RM immediately notifies the protocols of re-applying the routing policy. However, you must run several commands to modify the routing policy. To prevent the protocols from repeatedly re-applying the routing policy which is being modified, you can run the **route-policy-change notify-delay** command to configure delay time for re-applying the routing policy, after you configure the IPv6 prefix list.

Example

Permit the routes with the mask length ranging from 32 to 64 bits.

```
<HUAWEI> system-view
[HUAWEI] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

Deny the routes with the IP prefix FC00:0:0:D00::/32 and with the prefix longer than 32 bits, and permit the other IPv6 routes.

```
<HUAWEI> system-view
[HUAWEI] ip ipv6-prefix abc deny fc00:0:0:d00:: 32 less-equal 128
[HUAWEI] ip ipv6-prefix abc permit :: 0 less-equal 128
```

Configure the IPv6 prefix list named **p3** to deny the routes to the IPv6 address ranging from ::1 to ::FFFF:FFFF.

```
<HUAWEI> system-view
[HUAWEI] ip ipv6-prefix p3 index 10 deny :: 96 match-network
```

```
[HUAWEI] ip ipv6-prefix p3 index 20 permit :: 0 less-equal 128
```

7.9.54 ip rd-filter

Function

The **ip rd-filter** command creates an RD filter.

The **undo ip rd-filter** command deletes an RD filter.

By default, no RD filter is configured.

Product	Support
S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported.
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported.

Format

ip rd-filter *rd-filter-number* { **deny** | **permit** } *route-distinguisher* &<1-10>

undo ip rd-filter *rd-filter-number* [{ **deny** | **permit** } *route-distinguisher* &<1-10>]

Parameters

Parameter	Description	Value
rd-filter-number	Specifies the number of an RD filter.	The value is an integer ranging from 1 to 255.
permit	Permits a route to match the rules if its RD matches the rules.	-
deny	Denied a route if its RD matches the rules.	-

Parameter	Description	Value
route-distinguisher	Specifies the RD to aa:nn or ipv4-address:nn. You can set a maximum of 10 RDs. The switch support RDs in the following formats: ● ipv4-address:nn, such as 10.1.1.1:200 ● aa:nn, such as 100:1 ● aa.aa:nn, such as 100.100:1 ● ipv4-address:* in the wildcard format, such as 10.1.1.1:*, indicating that the RD begins with 10.1.1.1 ● aa:* in the wildcard format, such as 100:*, indicating that the RD begins with 100 ● aa.aa:* in the wildcard format, such as 100.100:*, indicating that the RD begins with 100.100	● The IPv4 address is in dotted decimal notation. ● The *nn* in ipv4-address:nn is an integer ranging from 0 to 65535. ● In aa:nn, the *aa* is an integer ranging from 0 to 65535, and *nn* is an integer ranging from 0 to 4294967295. ● The *aa* and *nn* in aa:*, aa.aa:*, and aa.aa:nn are both integers ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ip rd-filter** command is used together with the **if-match rd-filter** command. First use the **ip rd-filter** command to configure an RD filter, and use the **if-match rd-filter** command to configure a matching rule based on the RD filter in a routing policy. The routing policy is used to filter routes that are received and advertised.

The RD filter has the following rules:

- If the RD filter is not configured but is used to filter routes, the matching result is **permit**.

  For example, the RD filter 100 is not configured but is used by the routing policy:

  ```
  route-policy test permit node 10
  if-match rd-filter 100
  ```

  When the routing policy is used to filter routes, the routes match this **if-match** clause, and the routes match the node 10 in the routing policy named **test**.

- If the RD filter is configured but the RD of routes does not match any RD defined in the RD filter, the default matching result is **deny**.

  For example, the RD of routes is 100:1, and the configuration of the RD filter is as follows:

  ```
  ip rd-filter 100 permit 10.1.1.1:100
  ```

  When the RD filter is used to filter routes, the matching result is **deny**.
- The relationship between the rules of the RD filter is "OR". This is different from the community filter. This is because each route has only one RD but can have multiple communities.

  For example, the RD filters in the following formats have the same matching results:

  Format 1:

  ```
  ip rd-filter 100 permit 100:1 200:1 10.2.2.2:1 10.3.3.3:1
  ```

  Format 2:

  ```
  ip rd-filter 100 permit 100:1 200:1
  ip rd-filter 100 permit 10.2.2.2:1
  ip rd-filter 100 permit 10.3.3.3:1
  ```

  The community filters in the following formats have different matching results:

  Format 1:

  ```
  ip community-filter 1 permit 100:1 200:1 300:1
  ```

  Format 2:

  ```
  ip community-filter 1 permit 100:1
  ip community-filter 1 permit 200:1 300:1
  ```

  In the preceding configuration of the community filter, the community defined in each rule must be a sub-set of route communities so that the rule can be matched.
- Routes are filtered according to the configuration order of multiple rules. For example:

  ```
  ip rd-filter 100 deny 200:1 10.5.5.5:1
  ip rd-filter 100 permit 200:* 10.5.5.5:*
  ```

  In this situation, the route with the RD 200:1 or 5.5.5.5:1 is denied. If the configuration order of multiple rules is reversed as follows:

  ```
  ip rd-filter 100 permit 200:* 10.5.5.5:*
  ip rd-filter 100 deny 200:1 10.5.5.5:1
  ```

  In this situation, the route with the RD 200:1 or 10.5.5.5:1 is permitted.
- Each RD filter can be configured with a maximum of 255 rules.

Example

Configure an RD filter.

```
<HUAWEI> system-view
[HUAWEI] ip rd-filter 1 permit 100:1
```

7.9.55 reset ip ip-prefix

Function

The **reset ip ip-prefix** command resets the statistics of the specified IPv4 prefix list.

Format

reset ip ip-prefix [*ip-prefix-name*]

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IPv4 prefix list. If *ip-prefix-name* is not specified, you can reset the statistics of all the IPv4 prefix lists.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv4 prefix list can be used to filter IPv4 addresses. When filtering IPv4 addresses, the system records the numbers of prefixes that are permitted and denied by the IPv4 prefix list. You can run the **display ip ip-prefix** command to view the numbers.

To view the number of IPv4 prefixes that are permitted and denied by the IPv4 prefix list, run the **reset ip ip-prefix** command to clear statistics about permitted and denied routes in the IPv4 prefix list, and then run the **display ip ip-prefix** command to display the number of IPv4 prefixes since the previous operation.

Configuration Impact

The **reset ip ip-prefix** command clears statistics about the IPv4 prefix list. After that, the previous statistics cannot be shown.

Precautions

The **reset ip ip-prefix** command:

- Clears statistics in a specified IPv4 prefix list, if the name of the IPv4 prefix list is specified using *ip-prefix-name*.
- Clears statistics in all IPv4 prefix lists, if the name of the IPv4 prefix list is not specified using *ip-prefix-name*.

Example

Reset the statistics of the specified IPv4 prefix list.

```
<HUAWEI> reset ip ip-prefix abc
```

7.9.56 reset ip ipv6-prefix

Function

The **reset ip ipv6-prefix** command resets the timer of a specified IPv6 prefix list.

Format

reset ip ipv6-prefix [*ipv6-prefix-name*]

Parameters

Parameter	Description	Value
ipv6-prefix-name	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv6 prefix list can be used to filter IPv6 addresses. When filtering IPv6 addresses, the system records the numbers of prefixes that are permitted and denied by the IPv6 prefix list. You can run the **display ip ipv6-prefix** command to view the numbers.

To view the number of IPv6 prefixes that are permitted and denied by the IPv6 prefix list, run the **reset ip ipv6-prefix** command to clear statistics about permitted and denied routes in the IPv6 prefix list, and then run the **display ip ipv6-prefix** command to display the number of IPv6 prefixes since the previous operation.

Configuration Impact

The **reset ip ipv6-prefix** command clears statistics about the IPv6 prefix list. After that, the previous statistics cannot be shown.

Precautions

The **reset ip ipv6-prefix** command:

- Clears statistics in a specified IPv6 prefix list, if the name of the IPv6 prefix list is specified using *ipv6-prefix-name*.
- Clears statistics in all IPv6 prefix lists, if the name of the IPv6 prefix list is not specified using *ipv6-prefix-name*.

Example

Resets the timer of the IPv6 prefix list named **abc**.

```
<HUAWEI> reset ip ipv6-prefix abc
```

7.9.57 reset route-policy counters

Function

The **reset route-policy counters** command resets route-policy counters.

Format

reset route-policy *route-policy-name* **counters**

Parameters

Parameter	Description	Value
route-policy-name	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The route-policy is used to filter routes and set the attributes of a route that matches a route-policy. When a route-policy filters routes, the system records the number of routes that match the route-policy nodes. You can run the **display route-policy** to view the numbers.

The **reset route-policy counters** command clears the number of routes which match or do not match the route-policy. You can run both the **reset route-policy counters** command and the **display route-policy** command to instruct whether to record the number of routes matching a specified route-policy.

Configuration Impact

The **reset route-policy counters** command clears the number of routes which match or do not match the route-policy. After that, the number cannot be restored.

Example

Reset the counters of a route-policy named **policy1**.

```
<HUAWEI> reset route-policy policy1 counters
```

7.9.58 route-policy

Function

The **route-policy** command creates a routing policy and displays the Route-Policy view.

The **undo route-policy** command deletes a specified routing policy.

By default, no routing policy is configured.

Format

route-policy *route-policy-name* { **permit** | **deny** } **node** *node*

undo route-policy *route-policy-name* [**node** *node*]

Parameters

Parameter	Description	Value
route-policy-name	Specifies the name of a routing policy. If the routing policy does no exist, create a routing policy and enter its Route-Policy view. If the routing policy exists, enter its Route-Policy view.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
permit	Specifies the matching mode of the routing policy as permit. In permit mode, a route matches all the **if-match** clauses, the route matches the routing policy and the actions defined by the **apply** clause are performed on the route. Otherwise, the route continues to match the next entry.	-
deny	Specifies the matching mode of the routing policy as deny. In deny mode, if a route matches all the **if-match** clauses, the route fails to match the routing policy and cannot match the next node.	-
node *node*	Specifies the index of the node in the routing policy. When the routing policy is used to filter routes, the node with the smaller value of *node* is matched first.	The value is an integer ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A routing policy is used to filter routes and set route attributes for the routes that match the routing policy. A routing policy consists of multiple nodes. One node can be configured with multiple **if-match** and **apply** clauses.

The **if-match** clauses define matching rules for this node, and the **apply** clauses define behaviors for the routes that match the rules. The relationship between **if-match** clauses is "AND". That is, a route must match all the **if-match** clauses. The relationship between the nodes of a routing policy is "OR". That is, if a route matches one node, the route matches the routing policy. If the route does not match any node, the route fails to match the routing policy.

Procedure

After a routing policy is created, the system prompts "Info: New Sequence of this List !" and displays the Route-Policy view. The system displays no prompt when a routing policy is deleted.

Precautions

After a route-policy is configured, by default, the RM immediately notifies each protocol to apply the route-policy to filter routes. To delay applying a route-policy, you need to run the **route-policy-change notify-delay** command to set the delay for applying the route-policy.

You can run the **display route-policy** command to view the number of routes that match and do not match the route-policy.

A *route-policy-name* must have been configured using the **route-policy** command before the *route-policy-name* is referenced by another command.

Before you run the **undo route-policy** command to delete a route-policy that is referenced by another command, delete the reference configuration.

If an **if-match** clause of a route-policy defines an **ip-prefix**-based filtering rule, the filtering rule applies to IPv4 prefixes, not to IPv6 prefixes, and IPv6 prefixes match the filtering rule by default. If IPv6 prefixes also need to be filtered, add an **ipv6-prefix**-based **if-match** clause. Similarly, if an **if-match** clause of a route-policy defines an **ipv6-prefix**-based filtering rule, the filtering rule applies to IPv6 prefixes, not to IPv4 prefixes, and IPv4 prefixes match the filtering rule by default. If IPv4 prefixes also need to be filtered, add an **ip-prefix**-based **if-match** clause.

The configuration of a peer takes precedence over that of the peer group to which the peer belongs. That is, when a routing policy is used to control BGP route advertisement or receiving, the priority of this configuration on a BGP peer is higher than that of the configuration on the peer group.

Example

Configure the routing policy named **policy1** whose node number is 10 and the matching mode is **permit**.

```
<HUAWEI> system-view
[HUAWEI] route-policy policy1 permit node 10
[HUAWEI-route-policy]
```

7.9.59 route-policy-change notify-delay

Function

The **route-policy-change notify-delay** command sets the delay before the RM to notify each protocol of applying a new policy after the original route-policy changes.

The **undo route-policy-change notify-delay** command restores the default setting.

By default, this command is not configured, and the delay time is 0s.

Format

route-policy-change notify-delay *delay-time*

undo route-policy-change notify-delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay for applying a new policy after the original route-policy changes.	The value is an integer ranging from 1 to 180, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The switch process the changes of a route-policy according to the following rules.

After the configuration of a route-policy changes, by default, the RM immediately notifies the protocol of performing related operations. To delay processing the changes of the route-policy, you can run the **route-policy-change notify-delay** command to set the delay for change processing. The new policy is applied after the timer expires:

- If the configuration of the route-policy changes again within the delay, the RM resets the timer.
- If the new policy is configured for BGP, the **refresh bgp all** command can be used within the delay set by the **route-policy-change notify-delay** command to trigger BGP to immediately use the new policy.

The following commands are related to the timer:

- **route-policy**
- **ip ip-prefix**
- **ip ipv6-prefix**
- **ip as-path-filter**
- **ip community-filter**
- **ip extcommunity-filter**
- **ip rd-filter**
- **acl**

Example

Set the delay before the RM to notify each protocol of applying a new policy after the original route-policy changes.

```
<HUAWEI> system-view
[HUAWEI] route-policy-change notify-delay 20
```

7.9.60 route-policy nonexistent-config-check

Function

The **route-policy nonexistent-config-check** command controls whether the system allows a nonexistent route-policy to be specified in a command.

The **undo route-policy nonexistent-config-check disable** command forbids a nonexistent route-policy to be specified in a command.

By default, the system does not allow a nonexistent route-policy to be specified in a command.

Format

route-policy nonexistent-config-check { **disable** | **enable** }

undo route-policy nonexistent-config-check disable

Parameters

Parameter	Description	Value
disable	Indicates that the system allows a nonexistent route-policy to be specified in a command.	-
enable	Indicates that the system does not allow a nonexistent route-policy to be specified in a command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if you specify a nonexistent route-policy in a command, the command does not take effect. To enable the system to allow a nonexistent route-policy to be specified in a command, run the **route-policy nonexistent-config-check disable** command.

Example

Enable the system to allow a nonexistent route-policy to be specified in a command.

```
<HUAWEI> system-view
[HUAWEI] route-policy nonexistent-config-check disable
```

7.10 IP Routing Table Management Commands

7.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.10.2 arp vlink-direct-route advertise

Function

The **arp vlink-direct-route advertise** command configures the advertisement of IPv4 ARP Vlink direct routes.

The **undo arp vlink-direct-route advertise** command cancels advertising IPv4 ARP Vlink direct routes.

By default, a device does not advertise IPv4 ARP Vlink direct routes.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

arp vlink-direct-route advertise [**route-policy** *route-policy-name*]

undo arp vlink-direct-route advertise

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the route-policy used to filter IPv4 ARP Vlink direct routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view, VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, IPv4 ARP Vlink direct routes are only used to guide local traffic forwarding. To control the routing table size and maintain routing table stability, devices are prohibited from importing these direct routes into dynamic routing protocols for advertisement. In some situations, however, devices need to perform operations based on specific routes. For example, a device needs to direct remote traffic for different users using different export policies. Subsequently, the device needs to import IPv4 ARP Vlink direct routes into dynamic routing protocols and advertises them to the remote end.

If you only need to visit several users, you can specify the **route-policy** *route-policy-name* parameter to filter IPv4 ARP Vlink direct routes to be advertised. This operation can control the routing table size and implement precise control over data traffic.

Configuration Impact

After you specify the **route-policy** *route-policy-name* parameter to filter the IPv4 ARP Vlink direct routes to be advertised, only the routes that match the specified route-policy are advertised.

Follow-up Procedure

IPv4 ARP Vlink direct routes need to be imported into the routing tables of dynamic routing protocols on the device running dynamic routing protocols before being advertised by dynamic routing protocols.

Precautions

You need to run the **route-policy** command to configure a route-policy. If the specified route-policy does not exist, IPv4 ARP Vlink direct routes cannot be filtered.

Example

Configure the advertisement of IPv4 ARP Vlink direct routes and configure a route-policy **policy1** to allow route 10.1.1.4/32 to be advertised.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix prefix1 permit 10.1.1.4 32
[HUAWEI] route-policy policy1 permit node 10
[HUAWEI-route-policy] if-match ip-prefix prefix1
[HUAWEI-route-policy] quit
[HUAWEI] arp vlink-direct-route advertise route-policy policy1
```

7.10.3 display fib

Function

The **display fib** command displays information about the FIB table.

Format

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] [**verbose**]

Parameters

Parameter	Description	Value
slot-id	Displays information about the FIB table with a specified slot ID.	The value is an integer and the value range depends on the device configuration.
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value must be an existing VPN instance name.
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display fib** command displays information about the FIB table. Each row represents a route.

NOTE

If there are lots of routes, using wildcard (|, **begin**, **exclude**, **include**, *regular-expression*) to display information or details lasts a long time. You can press Ctrl+C to terminate information display.

Example

Display brief information about the FIB table.

```
<HUAWEI> display fib
Route Flags: G - Gateway Route, H - Host Route,    U - Up Route
           S - Static Route,  D - Dynamic Route, B - Black Hole Route
           L - Vlink Route
------------------------------------------------------------------------------
 FIB Table:
 Total number of Routes : 5

Destination/Mask   Nexthop         Flag  TimeStamp     Interface      TunnelID
192.168.150.111/32 127.0.0.1       HU    t[117]        InLoop0        0x0
127.0.0.1/32       127.0.0.1       HU    t[54]         InLoop0        0x0
127.0.0.0/8        127.0.0.1       U     t[54]         InLoop0        0x0
192.168.150.0/24   192.168.150.111 U     t[117]        MEth0/0/1      0x0
0.0.0.0/0          192.168.150.1   GSU   t[117]        MEth0/0/1      0x0
```

Display information starting from the line that contains 169.254.0.0

```
<HUAWEI> display fib | begin 10.254.0.0
Destination/Mask  Nexthop   Flag  TimeStamp  Interface   TunnelID
10.254.0.0/16    10.2.1.1   U     t[0]       Vlanif10     0x0
10.12.0.0/16     10.2.1.1   U     t[0]       Vlanif10     0x0
127.0.0.0/8      127.0.0.1  U     t[0]       InLoop0      0x0
```

Display all lines that contain Vlanif10.

```
<HUAWEI> display fib | include Vlanif10
Destination/Mask  Nexthop   Flag  TimeStamp  Interface  TunnelID
10.254.0.0/16    10.2.1.1   U     t[0]       Vlanif10    0x0
10.12.0.0/16     10.2.1.1   U     t[0]       Vlanif10    0x0
```

Display all lines that do not include 192.168.150.0.

```
<HUAWEI> display fib | exclude 192.168.150.0

Destination/Mask   Nexthop         Flag  TimeStamp     Interface      TunnelID
192.168.150.111/32 127.0.0.1       HU    t[117]        InLoop0        0x0
127.0.0.1/32       127.0.0.1       HU    t[54]         InLoop0        0x0
127.0.0.0/8        127.0.0.1       U     t[54]         InLoop0        0x0
0.0.0.0/0          192.168.150.1   GSU   t[117]        MEth0/0/1      0x0
```

Table 7-205 Description of the display fib command output

Item	Description
Route Flags	Flag of a route.
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.

Item	Description
Flag	Current flag, which is the combination of G, H, U, S, D, B and L. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S (static route): indicates that the route is manually configured. ● D (dynamic route): indicates that the route is generated based on the routing algorithm. ● B (blackhole route): indicates that the next hop is a null interface. ● L: indicates a Vlink route.
TimeStamp	Timestamp, which indicates the time equal to FIB entry generation time minus system startup time.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0x0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0x0, packets matching the entry are not forwarded through the MPLS tunnel.

Display detailed information about the FIB table.

```
<HUAWEI> display fib verbose
Route Flags: G - Gateway Route, H - Host Route,    U - Up Route
             S - Static Route,  D - Dynamic Route, B - Black Hole Route
             L - Vlink Route
------------------------------------------------------------------------------
 FIB Table:
 Total number of Routes : 3

 Destination: 127.0.0.1          Mask     : 255.255.255.255
 Nexthop    : 127.0.0.1          OutIf    : InLoopBack0
 LocalAddr  : 127.0.0.1          LocalMask: 0.0.0.0
 Flags      : HU                 Age      : 354280sec
 ATIndex    : 0                  Slot     : 0
 LspFwdFlag : 0                  LspToken : 0x0
 InLabel    : NULL               OriginAs : 0
 BGPNextHop : 0.0.0.0            PeerAs   : 0
 QosInfo    : 0x0                OriginQos: 0x0
 NexthopBak : 0.0.0.0            OutIfBak : [No Intf]
```

```
LspTokenBak: 0x0               InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
VlanId : 0x0
BgpKey : 0
BgpKeyBak : 0
LspType          : 0           Label_ForLspTokenBak   : 0
MplsMtu          : 0           Gateway_ForLspTokenBak : 0.0.0.0
NextToken        : 0x0         IfIndex_ForLspTokenBak : 0
Label_NextToken : 0            Label : 0
LspBfdState      : 0

Destination: 127.255.255.255    Mask      : 255.255.255.255
Nexthop    : 127.0.0.1          OutIf     : InLoopBack0
LocalAddr  : 127.0.0.1          LocalMask: 0.0.0.0
Flags      : HU                 Age       : 354280sec
ATIndex    : 0                  Slot      : 0
LspFwdFlag : 0                  LspToken : 0x0
InLabel    : NULL               OriginAs : 0
BGPNextHop : 0.0.0.0            PeerAs   : 0
QosInfo    : 0x0                OriginQos: 0x0
NexthopBak : 0.0.0.0            OutIfBak : [No Intf]
LspTokenBak: 0x0                InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
VlanId : 0x0
BgpKey : 0
BgpKeyBak : 0
LspType          : 0           Label_ForLspTokenBak   : 0
MplsMtu          : 0           Gateway_ForLspTokenBak : 0.0.0.0
NextToken        : 0x0         IfIndex_ForLspTokenBak : 0
Label_NextToken : 0            Label : 0
LspBfdState      : 0

Destination: 255.255.255.255    Mask      : 255.255.255.255
Nexthop    : 127.0.0.1          OutIf     : InLoopBack0
LocalAddr  : 127.0.0.1          LocalMask: 0.0.0.0
Flags      : HU                 Age       : 354280sec
ATIndex    : 0                  Slot      : 0
LspFwdFlag : 0                  LspToken : 0x0
InLabel    : NULL               OriginAs : 0
BGPNextHop : 0.0.0.0            PeerAs   : 0
QosInfo    : 0x0                OriginQos: 0x0
NexthopBak : 0.0.0.0            OutIfBak : [No Intf]
LspTokenBak: 0x0                InLabelBak : NULL
LspToken_ForInLabelBak : 0x0
EntryRefCount : 0
VlanId : 0x0
BgpKey : 0
BgpKeyBak : 0
LspType          : 0           Label_ForLspTokenBak   : 0
MplsMtu          : 0           Gateway_ForLspTokenBak : 0.0.0.0
NextToken        : 0x0         IfIndex_ForLspTokenBak : 0
Label_NextToken : 0            Label : 0
LspBfdState      : 0
```

Table 7-206 Description of the display fib verbose command output

Item	Description
Destination	Destination address.
Mask	Mask.
Nexthop	Next hop.
OutIf	Outbound interface.

Item	Description
LocalAddr	Local IP address.
LocalMask	Mask of the local IP address.
Flags	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S (static route): indicates that the route is manually configured. ● D (dynamic route): indicates that the route is generated based on the routing algorithm. ● B (blackhole route): indicates that the next hop is a null interface. ● L: indicates a Vlink route.
Age	Lifetime of a route, in seconds.
ATIndex	Index of the virtual link connecting the local end and the gateway.
Slot	Slot ID of the outbound interface.
LspFwdFlag	Forwarding flag of an LSP.
LspToken	Forwarding ID of an LSP.
InLabel	Inner tag of a VPN LSP.
OriginAs	Original AS number.
BGPNextHop	Address of the BGP next hop.
PeerAs	Neighbor AS number.
QosInfo	QoS information.
OriginQos	Original QoS information.
NexthopBak	Backup of the next hop.
OutIfBak	Backup of the outbound interface.
VlanId	VLAN ID.
BgpKey	Key value of the BGP route.
BgpKeyBak	Backup key value of the BGP route.

7.10.4 display fib acl

Function

The **display fib acl** command displays information about FIB entries that match a specified ACL rule.

Format

display fib [**vpn-instance** *vpn-instance-name*] **acl** *acl-number* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value must be an existing VPN instance name.
acl-number	Displays information about the FIB table with a specified ACL rule.	The value is an integer that ranges from 2000 to 2999.
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display fib acl** command to check information about FIB entries that match a specified ACL rule.

Example

Display FIB entries that match an ACL rule.

```
<HUAWEI> display fib acl 2010
Route Entry matched by access-list 2010
 Summary Counts: 1
Destination/Mask Nexthop  Flag TimeStamp Interface     TunnelID
127.0.0.0/8      127.0.0.1 U    t[0]      InLoop0       0x0
```

Table 7-207 Description of the display fib acl command output

Item	Description
Route Entry matched by access-list	FIB entries that match an ACL rule.
Summary Counts	Total number of the FIB entries.
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, B and T. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface. ● T: indicates ingress TOKEN_SETBYLSPM nodes.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

7.10.5 display fib interface

Function

The **display fib interface** command displays information about FIB entries with a specified outbound interface.

Format

display fib [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value must be an existing VPN instance name.
interface-type interface-number	Specifies the type and number of the outbound interface to a specified destination address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display fib interface** command to check information about FIB entries with a specified outbound interface.

Example

Display FIB entries with a specified outbound interface.

```
<HUAWEI> display fib interface vlanif10
Destination/Mask   Nexthop    Flag TimeStamp   Interface       TunnelID
10.1.1.0/24        10.1.1.2    U    t[115]     Vlanif10           0x0
```

Table 7-208 Description of the display fib interface command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.

Item	Description
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

7.10.6 display fib ip-prefix

Function

The **display fib ip-prefix** command displays information about the FIB table.

Format

display fib [**vpn-instance** *vpn-instance-name*] **ip-prefix** *prefix-name* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the FIB table of a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
prefix-name	Specifies the name of an IP prefix list.	The value is a string of 1 to 169 characters.
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays FIB entries that match a specified IP prefix list.

If 0 FIB entries match, the command output displays that zero FIB entries match.

If the name of an IP prefix list is not found, all FIB entries are displayed.

Example

Display FIB entries matching the IP prefix list **abc0**.

```
<HUAWEI> display fib ip-prefix abc0
Route Entry matched by prefix-list abc0
 Summary Counts: 4
Destination/Mask  Nexthop  Flag  TimeStamp  Interface   TunnelID
127.0.0.0/8       127.0.0.1 U     t[0]       InLoop0       0x0
127.0.0.1/32      127.0.0.1 U      t[0]       InLoop0       0x0
172.16.0.0/8      10.1.1.1  SU     t[0]       Vlanif10      0x0
172.16.0.0/15     10.1.1.1  SU     t[0]       Vlanif10      0x0
```

Table 7-209 Description of the display fib ip-prefix command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.

Item	Description
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the tunnel. If the value is 0, packets matching the entry are not forwarded through the tunnel.

7.10.7 display fib longer

Function

The **display fib longer** command displays FIB entries that match a specified parameter.

The **display fib** [*slot-id*] *destination-address* command displays FIB entries that match a specified destination IP address. If the specified destination IP address matches an FIB entry in the natural mask range, all the subnets are displayed. Otherwise, FIB entries are displayed based on the longest matching principle.

The **display fib** [*slot-id*] *destination-address destination-mask* command displays FIB entries that accurately match the destination address and mask.

The **display fib** [*slot-id*] *destination-address* **longer** command displays all FIB entries that match destination IP addresses in the natural mask range.

The **display fib** [*slot-id*] *destination-address* destination-mask **longer** command displays all FIB entries that match destination IP addresses in a specified mask range.

The **display fib** [*slot-id*] *destination-address1 destination-mask1 destination-address2 destination-mask2* command displays FIB entries that match destination

IP addresses in the range of *destination-address1 destination-mask1* to *destination-address2 destination-mask2*.

If *slot-id* is specified, FIB entries on the device are displayed.

Format

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] *destination-address1* [*destination-mask1*] [**longer**] [**verbose**]

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] *destination-address1* *destination-mask1* *destination-address2* *destination-mask2* [**verbose**]

Parameters

Parameter	Description	Value
slot-id	Displays information about the FIB table with a specified slot ID.	The value is an integer and the value range depends on the device configuration.
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value must be an existing VPN instance name.
destination-address1	Indicates destination IP address 1.	The value is in dotted decimal notation.
destination-mask1	Indicates subnet mask 1.	The value is in dotted decimal notation or an integer that ranges from 0 to 32.
destination-address2	Indicates destination IP address 2.	The value is in dotted decimal notation.
destination-mask2	Indicates subnet mask 2.	The value is in dotted decimal notation or an integer that ranges from 0 to 32.
longer	Displays FIB entries matching a specified network segment or mask.	-
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display fib longer** command to check FIB entries that match a specified condition.

Example

Display FIB entries that match destination address 172.16.0.0 in the natural mask range or based on the longest match principle.

```
<HUAWEI> display fib 172.16.0.0
  Route Entry Count: 1
Destination/Mask  Nexthop  Flag  TimeStamp  Interface  TunnelID
172.16.0.0/16     10.1.1.1 U     t[0]       Vlanif10     0x0
```

Display the FIB entries with the destination addresses in the range of 172.16.0.0/16 to 172.16.0.6/16.

```
<HUAWEI> display fib 172.16.0.0 255.255.0.0 172.16.0.6 255.255.0.0
  Route Entry Count: 1
Destination/Mask  Nexthop  Flag  TimeStamp  Interface  TunnelID
172.16.0.1/8      10.1.1.1  U     t[0]       Vlanif10     0x0
```

Table 7-210 Description of the display fib longer command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, and B. • G (gateway route): indicates that the next hop is a gateway. • H (host route): indicates that the route is a host route. • U (available route): indicates that the route status is Up. • S: indicates a static route. • D: indicates a dynamic route. • B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.

Item	Description
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the tunnel. If the value is 0, packets matching the entry are not forwarded through the tunnel.

7.10.8 display fib next-hop

Function

The **display fib next-hop** command displays FIB entries that match a specified next-hop IP address.

Format

display fib [**vpn-instance** *vpn-instance-name*] **next-hop** *ip-address*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies the next-hop IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display fib next-hop** command to check FIB entries that match a specified next-hop IP address.

Example

Display FIB entries that match a specified next-hop IP address.

```
<HUAWEI> display fib next-hop 10.1.1.1
Destination/Mask   Nexthop         Flag TimeStamp     Interface      TunnelID
```

```
10.1.1.1/32        10.1.1.1        HU   t[115]       Vlanif10         0x0
```

Table 7-211 Description of the display fib next-hop command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

7.10.9 display fib statistics

Function

The **display fib statistics** command displays the total number of IPv4 FIB entries.

Format

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] **statistics**

Parameters

Parameter	Description	Value
slot-id	Displays status information about a specified IPv4 FIB module.	The value is an integer and the value range depends on the device configuration.
vpn-instance *vpn-instance-name*	Specifies the name of an IPv4 VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display fib statistics** command to check the total number of IPv4 FIB entries.

Example

Display the total number of IPv4 FIB entries.

```
<HUAWEI> display fib statistics
Route Entry Count : 30
Route Prefix Count : 30
```

Table 7-212 Description of the display fib statistics command output

Item	Description
Route Entry Count	Total number of FIB entries.
Route Prefix Count	Total number of route prefix entries.

7.10.10 display fib statistics all

Function

The **display fib statistics all** command displays IPv4 FIB entry statistics.

Format

display fib [*slot-id*] **statistics all**

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of the switch on which IPv4 FIB entry statistics are displayed.	The value is an integer and the value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When running the **display fib statistics all** command, you can view the IPv4 FIB route prefix capacity and the number of IPv4 FIB forwarding entries on the device.

Example

Display statistics about IPv4 FIB entries on the switch in slot 0.

```
<HUAWEI> display fib 0 statistics all
IPv4 FIB Route Prefix Capacity : 320000
IPv4 FIB Total Route Prefix Count :2 ; Entry Count : 2
IPv4 FIB Public Route Prefix Count :2 ; Entry Count : 2
IPv4 FIB VPN-instance vpna Route Prefix Count :0 ; Entry Count : 0
```

Table 7-213 Description of the display fib statistics all command output

Item	Description
IPv4 FIB Route Prefix Capacity:	IPv4 FIB route prefix capacity on the local switch.
IPv4 FIB Total Route Prefix Count: Entry Count:	Total number of IPv4 FIB route prefixes and forwarding entries on the local switch.
IPv4 FIB Public Route Prefix Count: Entry Count:	Total number of IPv4 route prefixes and forwarding entries on a public network.
IPv4 FIB VPN-instance vpna Route Prefix Count: Entry Count:	Total number of route prefixes and forwarding entries of IPv4 VPN instance **vpna**.

7.10.11 display ip routing-table

Function

The **display ip routing-table** command displays information about an IPv4 routing table.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* { *mask* | *mask-length* } **nexthop** *nexthop-address* [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address1* { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] **acl** { *acl-number* | *acl-name* } [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] **ip-prefix** *ip-prefix-name* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance of an enabled IPv4 address family.	The value must be an existing VPN instance name.
verbose	Displays detailed information about active routes and inactive routes. If this keyword is not specified, only brief information about active routes is displayed.	-
ip-address	Displays the routes with the specified destination address.	The value is in dotted decimal notation.
nexthop *nexthop-address*	Displays the routes with the specified next-hop address.	The value is in dotted decimal notation.
longer-match	Displays the routes with the specified destination address and mask.	-

Parameter	Description	Value
mask	Specifies the mask of the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	The value is an integer that ranges from 0 to 32.
ip-address1	Specifies the start IP address in an IP address range. *ip-address1* and *ip-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is in dotted decimal notation.
ip-address2	Specifies the end IP address in an IP address range. *ip-address1* and *ip-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is in dotted decimal notation.
mask1	Specifies the subnet mask of the start IP address.	The value is in dotted decimal notation.
mask-length1	Specifies the mask length of the start IP address.	The value is an integer that ranges from 0 to 32.
mask2	Specifies the subnet mask of the end IP address.	The value is in dotted decimal notation.
mask-length2	Specifies the mask length of the end IP address.	The value is an integer that ranges from 0 to 32.
acl *acl-number*	Displays the routes that match the ACL with the specified ACL number. If the specified ACL does not exist, information about all active routes is displayed.	The value is an integer that ranges from 2000 to 2999.
acl *acl-name*	Displays the routes that match the ACL with the specified ACL name. If the specified ACL does not exist, information about all active routes is displayed.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Displays the routes that match the specified IP prefix list. If the specified IP prefix list does not exist, information about all active routes is displayed.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the **verbose** keyword is not specified in the **display ip routing-table** command, each line in the command output indicates a route, including the destination address, mask length, protocol, preference, cost, flag, next hop, and outbound interface of the route.

NOTE

A recursive route is counted as one route regardless of how many outbound interfaces and next hops the route finds.

Matching rules vary with parameters in the command:

- If the **display ip routing-table** *ip-address* command is used, the routes that longest match the destination address are displayed.
- If the **display ip routing-table** *ip-address mask* command is used, the routes that accurately match the destination address and mask are displayed.
- If the **display ip routing-table** *ip-address* **longer-match** command is used, all the routes that match the IP address specified by the destination address and the natural mask are displayed.
- If the **display ip routing-table** *ip-address mask* **longer-match** command is used, all the routes that match the IP address specified by the destination address and the input mask are displayed.
- If the **display ip routing-table** *ip-address1 mask1 ip-address2 mask2* command is used, the routes whose destination address ranges from *ip-address1 mask1* to *ip-address2 mask2* are displayed.

Example

Display brief information about the current IPv4 routing table. The command output shows that there are two static routes with the same destination address 10.1.1.1/32 but different next hops.

```
<HUAWEI> display ip routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 5        Routes : 5

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.1.1/32   Static  60   0           D   0.0.0.0         NULL0
                    Static  60   0           D   192.168.0.2     Vlanif100
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
     127.0.0.1/32   Direct  0    0           D   127.0.0.1       InLoopBack0
  192.168.150.0/24  Direct  0    0           D   192.168.150.22  Vlanif4094
 192.168.150.22/32  Direct  0    0           D   127.0.0.1       Vlanif4094
```

Table 7-214 Description of the display ip routing-table command output

Item	Description
Route Flags	Flag of a route: ● R: indicates that the route is a recursive route. ● D: indicates that the route is delivered to the FIB table. ● T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: Public	The routing table is a public routing table. If the routing table is a private routing table, a private network name is displayed, for example, Routing Tables: ABC.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol that learns a route.
Pre	Preference of a route.
Cost	Cost of a route.
Flags	Route flags in the heading of the routing table.
NextHop	Next-hop address of a route.
Interface	Outbound interface through which the next hop of a route is reachable.

Display the summary of the routing table of the IPv4 VPN instance named **vpn1**.

```
<HUAWEI> display ip routing-table vpn-instance vpn1
Route Flags: R - relay, D - download to fib, T - to vpn-instance
```

```
------------------------------------------------------------------------------
Routing Table: vpn1
         Destinations : 3        Routes : 3

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

       10.1.1.0/24  Direct 0    0           D  10.1.1.1        Vlanif10
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       Vlanif10
       10.5.5.0/24  Static 60   0          RD  10.1.1.2        Vlanif10
```

Table 7-215 Description of the display ip routing-table vpn-instance command output

Item	Description
Route Flags	Route flag: ● R: indicates a recursive route. ● D: indicates that the route is downloaded to the FIB table. ● T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: vpn1	VPN routing table named vpn1.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol.
Pre	Preference.
Cost	Route cost.
Flags	Route flag, that is, Route Flags in the heading of the routing table.
NextHop	Next hop.
Interface	Outbound interface through which the next hop is reachable.

Display brief information about the current routing table. Route 10.2.2.2/32 is a static route with next hop 10.1.1.1. This route is a recursive route and has two outbound interfaces because 10.1.1.1 has two outbound interfaces.

```
<HUAWEI> display ip routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 7

   Destination/Mask  Proto   Pre  Cost Flags  NextHop     Interface

       10.1.1.1/32   Static  60   0      D    0.0.0.0     NULL0
                     Static  60   0      D    10.10.0.2  Vlanif100
```

```
      10.2.2.2/32   Static  60   0     RD   10.1.1.1     NULL0
                    Static  60   0     RD   10.1.1.1     Vlanif100
     10.10.0.0/24   Direct   0   0      D    10.10.0.1  Vlanif100
     10.10.0.1/32   Direct   0   0      D    127.0.0.1  Vlanif100
     127.0.0.0/8    Direct   0   0      D    127.0.0.1  InLoopBack0
     127.0.0.1/32   Direct   0   0      D    127.0.0.1  InLoopBack0
```

Display detailed information about the IPv4 routing table.

```
<HUAWEI> display ip routing-table verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------ Routing Tables: Public
         Destinations : 5        Routes : 5


Destination: 10.0.0.36/32
     Protocol: Direct           Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1         Neighbour: 0.0.0.0
        State: Active Adv              Age: 01h03m56s
          Tag: 0                  Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: InLoopBack0
     TunnelID: 0x0                   Flags:  D

Destination: 10.10.36.0/24
     Protocol: Direct           Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.10.36.2        Neighbour: 0.0.0.0
        State: Active Adv              Age: 00h26m36s
          Tag: 0                  Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: Vlanif10
     TunnelID: 0x0                   Flags:  D

Destination: 10.10.36.2/32
     Protocol: Direct           Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1         Neighbour: 0.0.0.0
        State: Active Adv              Age: 00h26m46s
          Tag: 0                  Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: Vlanif10
     TunnelID: 0x0                   Flags:  D

Destination: 127.0.0.0/8
     Protocol: Direct           Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1         Neighbour: 0.0.0.0
        State: Active NoAdv            Age: 3d01h20m39s
          Tag: 0                  Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: InLoopBack0
     TunnelID: 0x0                   Flags:  D

Destination: 127.0.0.1/32
     Protocol: Direct           Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1         Neighbour: 0.0.0.0
        State: Active NoAdv            Age: 3d01h20m39s
          Tag: 0                  Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: InLoopBack0
     TunnelID: 0x0                   Flags:  D
```

Table 7-216 Description of the display ip routing-table verbose command output

Item	Description
Route Flags	Flag of a route: - R: indicates that the route is a recursive route. - D: indicates that the route is delivered to the FIB table. - T: indicates a route whose next hop belongs to a VPN instance.
Destinations	Total number of destination networks or hosts.
Routes	Total number of active routes and inactive routes.
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol of a route.
Process ID	Routing protocol process ID of a route.
Preference	Preference of a route.
Cost	Cost of a route.
NextHop	Next-hop address of a route.
Neighbour	Neighbor address of a route.
State	Status of a route: - Active: active route - Invalid: invalid route - Inactive: inactive route - NoAdv: route that cannot be advertised - Adv: route that can be advertised - Del: route to be deleted - Relied: route that recurses to an outbound interface and a next hop or that recurses to a tunnel - Stale: route that is marked Stale and used in GR
Age	Lifetime of a route.
Tag	Routing management tag. The value is an integer that ranges from 0 to 4294967295.

Item	Description
Priority	Convergence priority of route: ● low ● medium ● high ● critical
Label	Label allocated by MPLS.
QoSInfo	QoS information. The value 0x0 indicates that QoS information is empty.
IndirectID	ID of indirect next hop.
RelayNextHop	Recursive next-hop address.
Interface	Outbound interface.
TunnelID	Tunnel ID.
Flags	Route flags in the heading of the routing table.

7.10.12 display ip routing-table limit

Function

The **display ip routing-table limit** command displays the maximum number of routes and prefixes.

Format

display ip routing-table limit [**all-vpn-instance** | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv4 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a IPv4 VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays limits on the number of IPv4 routes and prefixes.

- The **display ip routing-table limit** command displays limits on the number of IPv4 public routes and prefixes.
- The **display ip routing-table limit all-vpn-instance** command displays the limit on the number of routes and prefixes of all IPv4 VPN instances.
- The **display ip routing-table limit vpn-instance** *vpn-instance-name* command displays the limit on the number of routes and prefixes of a specified IPv4 VPN instance.

Example

Display the limits on the number of IPv4 public routes and prefixes.

```
<HUAWEI> display ip routing-table limit
Public Instance:
Limit-Object Limit-Type     Upper-Limit  Warning    Current    Log-Interval
Route         Default        -            -          9          5
Prefix        Default        -            -          9          5
```

Display limits on the numbers of routes and prefixes of all IPv4 VPN instances.

```
<HUAWEI> display ip routing-table limit all-vpn-instance
Limit-Object     Limit-Type    Upper-Limit     Warning     Current    Log-Interval
--------------------------------------------------------------------------------
VPN Instance Name: vpn1
Route            Simply-Alert   5000          -           4223      5
Prefix           Alert-Percent  1000          800         760       5
---------------------------------------------------------------------------------
VPN Instance Name: vpn2
Route            Alert-Percent  2000          1000        823       5
Prefix           Default        -             -           760       5
```

Display limits on the numbers of routes and prefixes of the IPv4 VPN instance named **vpn1**.

```
<HUAWEI> display ip routing-table limit vpn-instance vpn1
VPN Instance Name: vpn1
Limit-Object     Limit-Type     Upper-Limit    Warning    Current    Log-Interval
Route            Simply-Alert    5000          -          4223       5
Prefix           Alert-Percent   1000          800        760        5
```

Table 7-217 Description of the display ip routing-table limit command output

Item	Description
Limit-Object	Object whose total number is limited: ● Prefix ● Route

Item	Description
Limit-Type	Limit type for the routes and prefixes in the routing table: ● Simply-Alert: indicates that only alarms are generated when the number of routes or prefixes exceeds the upper limit. ● Alert-Percent: indicates the percentage of the alarm threshold of routes. ● Default: indicates that the number of routes or prefixes is not limited by default.
Upper-Limit	Upper limit of routes or prefixes in the current routing table.
Warning	Alarm threshold of routes or prefixes in the current routing table.
Current	Number of routes or prefixes in the current routing table.
Log-Interval	Frequency of displaying logs when the number of routes or prefixes in the current routing table exceeds the upper limit, in seconds. The default value is 5s.

7.10.13 display ip routing-table protocol

Function

The **display ip routing-table protocol** command displays routing information about a specified routing protocol.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance of an enabled IPv4 address family.	The value must be an existing VPN instance name.

Parameter	Description	Value
protocol	Displays routing information of a specified routing protocol.	The value may be **bgp, direct**, **isis, ospf, rip**, **static**, or **unr**. The specific value varies depending on the routing protocol supported by the device.
inactive	Displays brief information about inactive routes only.	-
verbose	Displays detailed information about active routes and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If neither **verbose** nor **inactive** is specified, brief information about all the routes of each routing protocol is displayed.

Example

Display brief information about all direct routes.

```
<HUAWEI> display ip routing-table protocol direct
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Public routing table : Direct
        Destinations : 4        Routes : 4

Direct routing table status : <Active>
        Destinations : 4        Routes : 4

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

   10.137.216.0/23  Direct  0    0           D   10.137.217.210  Vlanif100
 10.137.217.210/32  Direct  0    0           D   127.0.0.1       Vlanif100
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0

Direct routing table status : <Inactive>
        Destinations : 0        Routes : 0
```

Table 7-218 Description of the display ip routing-table protocol command output

Item	Description
Route Flags	Flag of a route: - R: indicates that the route is a recursive route. - D: indicates that the route is delivered to the FIB table. - T: indicates a route whose next hop belongs to a VPN instance.
Public routing table	Contents of a public routing table.
Direct routing table status	Status of direct routes: - **Inactive**: inactive routes in the routing table - **Active**: active routes in the routing table
Destinations	Total number of destination addresses.
Routes	Total number of routes in the routing table.
Destination/Mask	Destination address or mask length.
Proto	Routing protocol of a route.
Pre	Routing protocol preference of a route.
Cost	Cost of a route.
Flags	Route flags in the heading of the routing table.
Nexthop	Next-hop address of a route.
Interface	Outbound interface of a route.

Display all the direct routes of the VPN instance named **vpn1**.

```
<HUAWEI> display ip routing-table vpn-instance vpn1 protocol direct
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
vpn4 routing table : Direct
         Destinations : 2          Routes : 2

Direct routing table status : <Active>
         Destinations : 2          Routes : 2

Destination/Mask    Proto  Pre  Cost     Flags NextHop         Interface

       10.1.1.0/24  Direct 0    0          D  10.1.1.1        Vlanif30
       10.1.1.1/32  Direct 0    0           D  127.0.0.1       Vlanif30

Direct routing table status : <Inactive>
         Destinations : 0          Routes : 0
```

Table 7-219 Description of the display ip routing-table vpn-instance protocol command output

Item	Description
Active	Active routes.
Inactive	Inactive routes.

7.10.14 display ip routing-table statistics

Function

The **display ip routing-table statistics** command displays statistics about routes in an IPv4 routing table.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name* | **all-vpn-instance**] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about routes in the routing table of a specified VPN instance. If neither **vpn-instance** *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	The value must be an existing VPN instance name.
all-vpn-instance	Displays statistics about routes in the routing tables of all VPN instances. If neither **vpn-instance** *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted through routing protocols
- Number of active or inactive routes that are labeled for deletion but are not deleted

Example

Display statistics about routes in an IPv4 routing table.

```
<HUAWEI> display ip routing-table statistics
Summary Prefixes: 9
Proto   total   active  added     deleted     freed
        routes  routes  routes     routes      routes
DIRECT   6        6      42          36         36
STATIC   3        3      21          18         18
RIP      0        0      0           0          0
OSPF     0        0      0           0          0
IS-IS    0        0      0           0          0
BGP      0        0      0           0          0
UNR      0        0      0           0          0
Total    9        9      63          54         54
```

Table 7-220 Description of the display ip routing-table statistics command output

Item	Description
Summary Prefixes	Total number of prefixes in the current routing table.
Proto	Routing protocol type
total routes	Total number of routes that a routing protocol learns in the routing table, including active and inactive routes.
active routes	Number of active routes that a routing protocol learns in the routing table.
added routes	Number of active and inactive routes that are added to the routing table through a routing protocol.
deleted routes	Number of routes to be deleted from the routing table.
freed routes	Number of routes that are permanently deleted from the routing table.

7.10.15 display ip routing-table time-range

Function

The **display ip routing-table time-range** command displays information about routes generated in a specified time range in an IP routing table.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] **time-range** *min-age max-age* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about routes generated in a specified time range in the IP routing table of the specified VPN instance. If you do not specify this parameter, the **display ip routing-table time-range** command displays information about routes generated in a specified time range in the public IP routing table.	The value must be an existing VPN instance name.
min-age	Specifies the end time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. ● d indicates days. The value is an integer that ranges from 0 to 10000. ● h indicates hours. The value is an integer that ranges from 0 to 23. ● m indicates minutes. The value is an integer that ranges from 0 to 59. ● s indicates seconds. The value is an integer that ranges from 0 to 59. For example, you can enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.

Parameter	Description	Value
max-age	Specifies the start time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. ● d indicates days. The value is an integer that ranges from 0 to 10000. ● h indicates hours. The value is an integer that ranges from 0 to 23. ● m indicates minutes. The value is an integer that ranges from 0 to 59. ● s indicates seconds. The value is an integer that ranges from 0 to 59. For example, you can enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.
verbose	Displays detailed information about active and inactive routes. If you do not specify this parameter, the **display ip routing-table time-range** command displays only brief information about active routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If route flapping occurs on a network, you can run the **display ip routing-table time-range** command and specify a small time range for the command. You can then find the flapping route rapidly and accelerate fault location.

Precautions

max-age must be larger than *min-age*. Otherwise, the **display ip routing-table time-range** command does not display any information.

If *max-age* is larger than *min-age* but no route was generated within this time range, the **display ip routing-table time-range** command displays only the table heading.

Example

Display information about public network routes generated in the last 20 minutes.

```
<HUAWEI> display ip routing-table time-range 0 20m
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: Public
        Destinations : 2        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.3.3.3/32  Direct  0    0           D   127.0.0.1       LoopBack1
      10.4.4.0/24  Static  60   0           D   0.0.0.0         NULL0
```

Table 7-221 Description of the display ip routing-table time-range command output

Item	Description
Route Flags	Route flags: ● R: The route is a recursive route. ● D: The route is sent to the FIB table. ● T: Indicates a route whose next hop belongs to a VPN instance.
Routing Tables: Public	The routing table is a public routing table.
Destinations	Number of destination networks and hosts.
Routes	Number of routes.
Destination/Mask	Address and mask length of the destination network and host.
Proto	Protocol used to learn routes.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the heading of the routing table.
NextHop	Next hop.
Interface	Outbound interface in a route with a reachable next hop.

Display detailed information about public network routes generated in the last 20 minutes.

```
<HUAWEI> display ip routing-table time-range 0 20m verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: Public
```

```
         Destinations : 3        Routes : 3


Destination: 10.3.3.3/32
     Protocol: Direct           Process ID: 0
   Preference: 0                      Cost: 0
      NextHop: 127.0.0.1         Neighbour: 0.0.0.0
        State: Active Adv              Age: 00h14m06s
          Tag: 0                  Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: LoopBack1
     TunnelID: 0x0                   Flags:  D

Destination: 10.4.4.0/24
     Protocol: Static           Process ID: 0
   Preference: 60                     Cost: 0
      NextHop: 0.0.0.0           Neighbour: 0.0.0.0
        State: Active Adv              Age: 00h01m38s
          Tag: 0                  Priority: medium
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: NULL0
     TunnelID: 0x0                   Flags:  D

Destination: 10.4.4.4/32
     Protocol: Static           Process ID: 0
   Preference: 60                     Cost: 0
      NextHop: 10.4.4.0          Neighbour: 0.0.0.0
        State: Invalid Adv Relied      Age: 00h01m38s
          Tag: 0                  Priority: medium
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x80000002
 RelayNextHop: 0.0.0.0           Interface: NULL0
     TunnelID: 0x0                   Flags: R
```

Table 7-222 Description of the display ip routing-table time-range verbose command output

Item	Description
Process ID	Process ID of the routing protocol.
Preference	Route preference.
Cost	Route cost.
NextHop	Next hop.
Neighbour	IP address of a neighbor. 0.0.0.0 indicates that the route is generated by a local device.

Item	Description
State	Route status: - Active: an active route - Invalid: an invalid route - Inactive: an inactive route - NoAdv: a route that cannot be advertised - Adv: a route that can be advertised - Del: a route to be deleted - Relied: a route that recurses to the next hop and outbound interface or that recurses to a tunnel - Stale: a route with the Stale flag and used in GR
Age	Time after the route is generated.
Tag	Administrative tag of the route. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of the route: - low: The convergence priority of a route is low. - medium: The convergence priority of a route is medium. - high: The convergence priority of a route is high. - critical: The convergence priority of a route is critical.
Label	Label allocated by MPLS.
QoSInfo	QoS information. 0x0 indicates QoS information is empty.
IndirectID	ID of the indirect next hop.
RelayNextHop	Recursive next hop.
Interface	Recursive outbound interface.
Tunnel ID	Tunnel ID: - The value 0x0 indicates that the route does not use a tunnel or the tunnel fails to be set up. - If the value is not 0x0, the route recurses to a tunnel.

Item	Description
Flags	Route flags in the heading of the routing table.

7.10.16 display ipv6 fib

Function

The **display ipv6 fib** command displays FIB entries on the device.

Format

display ipv6 fib [*slot-id*] **statistics** [**all**]

display ipv6 fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] **statistics**

display ipv6 fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] [*ipv6-address* [*prefix-length*]] [**verbose**]

display ipv6 fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] **verbose statistics**

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID.	-
ipv6-address	Specifies the prefix of an IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
statistics	Displays the statistics of FIB entries.	-
all	Displays all FIB entries.	-
vpn-instance *vpn-instance-name*	Displays FIB entries of the specified VPN instance.	The value must be an existing VPN instance name.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.
verbose	Displays detailed information about FIB entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 fib** command to check IPv6 FIB entries on the device.

Example

Display all FIB entries on the device.

```
<HUAWEI> display ipv6 fib
 IPv6 FIB Table:
 Total number of Routes : 1

Destination:  ::1                               PrefixLength : 128
Nexthop    :  ::1                               Flag         : HU
Interface  :  InLoopBack0                           Tunnel ID    : 0x0
TimeStamp  :  2008-11-03 13:47:52
```

Table 7-223 Description of the display ipv6 fib command output

Item	Description
Total number of Routes	Number of IPv6 routes.
Destination	Destination IPv6 address of a route.
PrefixLength	Prefix length of the destination IPv6 address.
Nexthop	Next-hop router that forwards packets to the destination address.
Flag	Description of route characteristics using S/U/G/H/B/D: ● S: static ● U: Up ● G: gateway ● H: host ● B. blackhole ● D: dynamic
Tunnel ID	ID of the tunnel. If packets are forwarded to the next hop using MPLS forwarding, the tunnel ID of the packets cannot be 0. If packets are forwarded using IP forwarding, the tunnel ID of the packets is 0.
TimeStamp	Time taken to generate a route in the FIB table.
Interface	Outbound interface through which packets are forwarded.

7.10.17 display ipv6 routing-table

Function

The **display ipv6 routing-table** command displays information about an IPv6 routing table.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address1* [*prefix-length1*] *ipv6-address2 prefix-length2* [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **acl** { *acl6-number* | *acl6-name* } [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **ipv6-prefix** *ipv6-prefix-name* [**verbose** | **brief**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance of an enabled IPv6 address family.	The value must be an existing VPN instance name.
verbose	Displays detailed information about all the routes in the current routing table, including active and inactive routes.	-
brief	Displays brief information about active routes in the current routing table.	-
ipv6-address	Displays the routes with the specified IPv6 destination address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 destination address.	The value is an integer that ranges from 0 to 128.
longer-match	Displays the routes with the specified destination address and mask.	-

Parameter	Description	Value
ipv6-address1	Specifies the start IPv6 address in an IP address range. *ipv6-address1* and *ipv6-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv6-address2	Specifies the end IPv6 address in an IP address range. *ipv6-address1* and *ipv6-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length1	Specifies the mask length of the start IPv6 address.	The value is an integer that ranges from 0 to 128.
prefix-length2	Specifies the mask length of the end IPv6 address.	The value is an integer that ranges from 0 to 128.
acl *acl6-number*	Displays the routes that match the ACL6 with the specified ACL number. If the specified ACL6 does not exist, information about all active routes is displayed.	The value is an integer that ranges from 2000 to 2999.
acl *acl6-name*	Displays the routes that match the ACL6 with the specified ACL name. If the specified ACL6 does not exist, information about all active routes is displayed.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ipv6-prefix *ipv6-prefix-name*	Displays the routes that match the specified IPv6 prefix list. If the specified IPv6 prefix list does not exist, information about all active routes is displayed.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the **verbose** keyword is not specified, the command output includes the destination address, prefix length, protocol type, preference, cost, next hop, outbound interface, tunnel ID, flag, and status of a route.

NOTE

A recursive route is counted as one route regardless of how many outbound interfaces and next hops the route finds.

Example

Display brief information about the current IPv6 routing table.

```
<HUAWEI> display ipv6 routing-table
Routing Table : Public
         Destinations : 4        Routes : 4

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:112::               PrefixLength : 64
 NextHop      : FC00:0:0:112::2              Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : Vlanif10                     Flags        : D

 Destination  : FC00:0:0:112::2              PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : Vlanif10                     Flags        : D

 Destination  : FE80::                       PrefixLength : 10
 NextHop      : ::                           Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : D
```

Table 7-224 Description of the display ipv6 routing-table command output

Item	Description
Routing Tables : Public	The routing table is a public routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination	IP address of the destination network or host of a route.
PrefixLength	Prefix length of a route.
NextHop	Next-hop IPv6 address of a route.
Preference	Preference of a route.

Item	Description
Cost	Cost of a route.
Protocol	Routing protocol of a route.
RelayNextHop	Recursive next-hop address.
TunnelID	Tunnel ID. The value 0x0 indicates that no tunnel is used or the tunnel fails to be established.
Interface	Outbound interface through which the next hop of a route can be reached.
Flags	Flag of a route: ● R: The route is a recursive route. ● D: The route is delivered to the FIB table.

Display detailed information about the IPv6 routing table.

```
<HUAWEI> display ipv6 routing-table verbose
Routing Table : Public
         Destinations : 2        Routes : 2

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Direct
 State        : Active NoAdv                 Cost         : 0
 Entry ID     : 1                            EntryFlags   : 0x80010050
 Reference Cnt: 1                            Tag          : 0
 Priority     : high                         Age          : 84410sec
 IndirectID   : 0x0
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : FC00:0:0:2::2                Preference   : 60
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Static
 State        : Active Adv Relied            Cost         : 0
 Entry ID     : 2                            EntryFlags   : 0x80020140
 Reference Cnt: 1                            Tag          : 0
 Priority     : high                         Age          : 79036sec
 IndirectID   : 0x80000001
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : RD
```

Table 7-225 Description of the display ipv6 routing-table verbose command output

Item	Description
Neighbour	IPv6 address of a neighbor interface.
ProcessID	Routing protocol process ID of a route.
Label	Label carried in a route.

Item	Description
State	Status of a route: - Active: active route - Invalid: invalid route - Inactive: inactive route - NoAdv: route that cannot be advertised - Adv: route that can be advertised - Del: route to be deleted - Relied: route that recurses to an outbound interface and a next hop or that recurses to a tunnel - Stale: route that is marked Stale and used in GR
Entry ID	ID of a routing entry in the routing table.
EntryFlags	Flag of a routing entry.
Reference Cnt	Number of times a route is referenced.
Tag	Routing management tag. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of a route: - low - medium - high - critical
IndirectID	ID of indirect next hop.
Age	Time a route is generated.

Display brief information about the active routes that match ACL6 2000.

```
<HUAWEI> display ipv6 routing-table acl 2000
Routes Matched by Access list  2000  :
Summary Count : 2

 Destination  : ::1                              PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : InLoopBack0                      Flags        : D

 Destination  : FC00:0:0:111::                   PrefixLength : 64
 NextHop      : FC00:0:0:111::2                  Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : Vlanif10                         Flags        : D
```

Display brief information about the routes with the specified IPv6 destination address.

```
<HUAWEI> display ipv6 routing-table fc00:0:0:111::1 64
Routing Table :Public
Summary Count : 1

 Destination  : FC00:0:0:111::                 PrefixLength : 64
 NextHop      : FC00:0:0:111::2                 Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Vlanif10                       Flags        : D
```

Display the routes within the specified IPv6 address range.

```
<HUAWEI> display ipv6 routing-table fc00:0:0:111::1 64 fc00:0:0:111::2 128
Routing Table :
Summary Count : 2

 Destination  : FC00:0:0:111::                 PrefixLength : 64
 NextHop      : FC00:0:0:111::2                 Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Vlanif10                       Flags        : D

 Destination  : FC00:0:0:111::2                 PrefixLength : 128
 NextHop      : ::1                         Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Vlanif10                       Flags        : D
```

Display brief information about the active routes that match IPv6 prefix list **abc2**.

```
<HUAWEI> display ipv6 routing-table ipv6-prefix abc2
Routes Matched by Prefix-list abc2 :
Summary Count: 3

 Destination  : ::1                         PrefixLength : 128
 NextHop      : ::1                         Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : InLoopBack0                       Flags        : D

 Destination  : FC00:0:0:112::                 PrefixLength : 64
 NextHop      : FC00:0:0:112::1                 Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Vlanif20                       Flags        : D

 Destination  : FC00:0:0:112::1                 PrefixLength : 128
 NextHop      : ::1                         Preference   : 0
 Cost         : 0                         Protocol     : Direct
 RelayNextHop : ::                             TunnelID     : 0x0
 Interface    : Vlanif20                       Flags        : D
```

7.10.18 display ipv6 routing-table limit

Function

The **display ipv6 routing-table limit** command displays limits on the numbers of routes and prefixes.

Format

display ipv6 routing-table limit [**all-vpn-instance** | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv6 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays limits on the number of IPv6 routes and prefixes.

- The **display ipv6 routing-table limit** command displays limits on the number of IPv6 public routes and prefixes.
- The **display ipv6 routing-table limit all-vpn-instance** command displays the limit on the number of routes and prefixes of all IPv6 VPN instances.
- The **display ipv6 routing-table limit vpn-instance** *vpn-instance-name* command displays the limit on the number of routes and prefixes of a specified IPv6 VPN instance.

Example

Display the limits on the number of IPv6 public routes and prefixes.

```
<HUAWEI> display ipv6 routing-table limit
Public Instance:
Limit-Object Limit-Type     Upper-Limit  Warning    Current    Log-Interval
Route         Default        -            -          1          5
Prefix        Default        -            -          1          5
```

Table 7-226 Description of the **display ipv6 routing-table limit** command output

Item	Description
Limit-Object	Indicates the object whose total number is limited: ● Prefix ● Route

Item	Description
Limit-Type	Indicates the limit mode for the routes and prefixes in the current routing table: ● Simply-Alert: indicates that only alarms are generated after the number of routes or prefixes exceeds the upper limit. ● Alert-Percent: indicates the percentage of the alarm threshold of routes. ● Default: indicates that the number of routes or prefixes is not limited by default.
Upper-Limit	Indicates the upper limit of routes or prefixes in the current routing table.
Warning	Indicates the alarm threshold of routes or prefixes in the current routing table.
Current	Indicates the number of routes or prefixes in the current routing table.
Log-Interval	Indicates the frequency of displaying logs when the number of routes or prefixes in the current routing table exceeds the upper limit, in seconds.

7.10.19 display ipv6 routing-table protocol

Function

The **display ipv6 routing-table protocol** command displays routing information about a specified IPv6 routing protocol.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose** | **brief**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance of an enabled IPv6 address family.	The value must be an existing VPN instance name.

Parameter	Description	Value
protocol	Displays routing information of a specified routing protocol.	The value may be **bgp, direct**, **isis, ospfv3, ripng**, **static**, or **unr**. The specific value varies depending on the routing protocol supported by the device.
inactive	Displays information about inactive routes. If this parameter is not specified, information about all active and inactive routes is displayed.	-
verbose	Displays detailed information about active and inactive routes. If this keyword is not specified, only brief information about active routes is displayed.	-
brief	Displays brief information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 routing-table protocol** command to check routing information about a specified IPv6 routing protocol.

Example

Display brief information about all IPv6 direct routes.

```
<HUAWEI> display ipv6 routing-table protocol direct
Public Routing Table : Direct
Summary Count : 2

Direct Routing Table's Status : < Active >
Summary Count : 2

 Destination  : ::1                              PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : InLoopBack0                      Flags        : D
```

```
 Destination  : FE80::                          PrefixLength : 10
 NextHop      : ::                              Preference   : 0
 Cost         : 0                               Protocol     : Direct
 RelayNextHop : ::                              TunnelID     : 0x0
 Interface    : NULL0                           Flags        : D

Direct Routing Table's Status : < Inactive >
Summary Count : 0
```

Table 7-227 Description of the display ipv6 routing-table protocol command output

Item	Description
Public Routing Table	Contents of a public routing table: ● Direct: direct IPv6 route ● Static: static IPv6 route ● bgp: BGP4+ route ● ripng: RIPng route ● isis: IS-IS IPv6 route ● ospfv3: OSPFv3 route ● unr: user network route
Summary Count	Number of prefixes of routes.
Direct Routing Table's Status	Status of direct routes: ● active: information about active routes ● inactive: information about inactive routes
Destination	IP address of the destination network or host of a route.
PrefixLength	Prefix length of a route.
NextHop	Next-hop address of a route.
Preference	Routing protocol preference of a route.
Cost	Cost of a route.
Protocol	Routing protocol that learns a route.
RelayNextHop	Recursive next-hop address.
TunnelID	Tunnel ID. The value 0x0 indicates that no tunnel is used or the tunnel fails to be established.
Interface	Outbound interface through which the next hop of a route can be reached.
Flags	Flag of a route: ● R: The route is a recursive route. ● D: The route is delivered to the FIB table.

7.10.20 display ipv6 routing-table statistics

Function

The **display ipv6 routing-table statistics** command displays statistics about routes in an IPv6 routing table.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name* | **all-vpn-instance**] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about routes in the routing table of a specified VPN instance. If neither *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	The value must be an existing VPN instance name.
all-vpn-instance	Displays statistics about routes in the routing tables of all VPN instances. If neither *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include the total number of routes, number of added routes, and number of deleted routes.

Example

Display statistics about routes in an IPv6 routing table.

```
<HUAWEI> display ipv6 routing-table statistics
Summary Prefixes : 0
Protocol   route      active     added      deleted    freed
DIRECT     0          0          0          0          0
STATIC     0          0          0          0          0
RIPng      0          0          0          0          0
OSPFv3     0          0          0          0          0
```

```
IS-IS     0          0          0          0          0
BGP       0          0          0          0          0
UNR       0          0          0          0          0
Total     0          0          0          0          0
```

Table 7-228 Description of the display ipv6 routing-table statistics command output

Item	Description
Summary Prefixes	Total number of prefixes in the current routing table.
Protocol	Routing protocol type:
route	Total number of routes that a routing protocol learns in the routing table, including active and inactive routes.
active	Number of active routes of a routing protocol in the routing table.
added	Number of active and inactive routes that are added to the routing table through a routing protocol.
deleted	Number of routes that are deleted from the routing table.
freed	Number of routes that are permanently deleted from the routing table.

7.10.21 display ipv6 routing-table time-range

Function

The **display ipv6 routing-table time-range** command displays information about routes generated in a specified time range in an IPv6 routing table.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **time-range** *min-age max-age* [**verbose** | **brief**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about routes generated in a specified time range in the IPv6 routing table of the specified VPN instance. If this parameter is not specified, the **display ipv6 routing-table time-range** command displays information about routes generated in a specified time range in the public IPv6 routing table.	The value must be an existing VPN instance name.
min-age	Specifies the end time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. - d indicates days. The value is an integer that ranges from 0 to 10000. - h indicates hours. The value is an integer that ranges from 0 to 23. - m indicates minutes. The value is an integer that ranges from 0 to 59. - s indicates seconds. The value is an integer that ranges from 0 to 59. For example, enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.

Parameter	Description	Value
max-age	Specifies the start time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. - d indicates days. The value is an integer that ranges from 0 to 10000. - h indicates hours. The value is an integer that ranges from 0 to 23. - m indicates minutes. The value is an integer that ranges from 0 to 59. - s indicates seconds. The value is an integer that ranges from 0 to 59. For example, enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.
verbose	Displays detailed information about active and inactive routes. If this parameter is not specified, the **display ipv6 routing-table time-range** command displays only brief information about active routes.	-
brief	Displays brief information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If route flapping occurs on a network, to find the flapping route rapidly and accelerate fault location, run the **display ipv6 routing-table time-range** command and specify a small time range.

Precautions

max-age must be larger than *min-age*. Otherwise, the **display ipv6 routing-table time-range** command does not display any information.

If *max-age* is larger than *min-age* but no route is generated within this time range, the **display ipv6 routing-table time-range** command displays only the table heading.

Example

Display information about public network IPv6 routes generated in the last 2 hours, 20 minutes, and 10 seconds.

```
<Switch> display ipv6 routing-table time-range 0 2h20m10s
Routing Table : Public
         Destinations : 4        Routes : 4

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : LoopBack2                    Flags        : D

 Destination  : FC00:0:0:1::2                PrefixLength : 128
 NextHop      : ::                           Preference   : 60
 Cost         : 0                            Protocol     : Static
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : D

 Destination  : FE80::                       PrefixLength : 10
 NextHop      : ::                           Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : D
```

Table 7-229 Description of the display ipv6 routing-table time-range command output

Item	Description
Routing Tables: Public	The routing table is a public routing table.
Destinations	Number of destination networks or hosts.
Routes	Number of routes.
Destination	IP addresses of the destination network or host.
PrefixLength	Prefix length of a route.
NextHop	Next-hop IPv6 address.
Preference	Route preference.
Cost	Route cost.

Item	Description
Protocol	Name of the routing protocol.
RelayNextHop	Recursive next hop.
TunnelID	Tunnel ID: ● The value 0x0 indicates that the route does not use a tunnel or the tunnel fails to be set up. ● If the value is not 0x0, the route recurses to a tunnel.
Interface	Outbound interface through which the next hop of a route can be reached.
Flags	Route flag: ● R: The route is a recursive route. ● D: The route is delivered to the FIB table.

Display detailed information about public network routes generated in the last 20 minutes.

```
<Switch> display ipv6 routing-table time-range 0 20m verbose
Routing Table : Public
        Destinations : 4        Routes : 5

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Direct
 State        : Active NoAdv                 Cost         : 0
 Entry ID     : 262551588                    EntryFlags   : 0x80010050
 Reference Cnt: 2                            Tag          : 0
 Priority     : high                         Age          : 7694sec
 IndirectID   : 0x0
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Direct
 State        : Active Adv                   Cost         : 0
 Entry ID     : 262552100                    EntryFlags   : 0x80010040
 Reference Cnt: 2                            Tag          : 0
 Priority     : high                         Age          : 101sec
 IndirectID   : 0x0
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : LoopBack2                    Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : FC00:0:0:1::2                Preference   : 60
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Static
 State        : Inactive Adv Relied          Cost         : 0
 Entry ID     : 262551716                    EntryFlags   : 0x20140
 Reference Cnt: 2                            Tag          : 0
 Priority     : medium                       Age          : 7668sec
 IndirectID   : 0x80000001
 RelayNextHop : ::                           TunnelID     : 0x0
```

```
Interface    : NULL0                       Flags        : R

Destination  : FC00:0:0:1::2                PrefixLength : 128
NextHop      : ::                         Preference   : 60
Neighbour    : ::                         ProcessID    : 0
Label        : NULL                        Protocol     : Static
State        : Active Adv                   Cost         : 0
Entry ID     : 262551844                    EntryFlags   : 0x80000040
Reference Cnt: 2                           Tag          : 0
Priority     : medium                       Age          : 7670sec
IndirectID   : 0x0
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : NULL0                       Flags        : D

Destination  : FE80::                       PrefixLength : 10
NextHop      : ::                         Preference   : 0
Neighbour    : ::                         ProcessID    : 0
Label        : NULL                        Protocol     : Direct
State        : Active NoAdv                   Cost         : 0
Entry ID     : 262551972                    EntryFlags   : 0x80010010
Reference Cnt: 2                           Tag          : 0
Priority     : high                       Age          : 104sec
IndirectID   : 0x0
RelayNextHop : ::                          TunnelID     : 0x0
Interface    : NULL0                       Flags        : D
```

Table 7-230 Description of the display ipv6 routing-table time-range verbose command output

Item	Description
Neighbour	IP address of a neighboring interface. :: indicates that the route is generated by a local device.
ProcessID	Process ID of the routing protocol.
Label	Label carried in a route.
State	Status of the route: • Active: an active route • Invalid: an invalid route • Inactive: an inactive route • NoAdv: a route that cannot be advertised • Adv: a route that can be advertised • Del: a route to be deleted • Relied: a route that recurses to the next hop and outbound interface or that recurses to a tunnel • Stale: a route with the Stale flag and used in GR
Entry ID	ID of a route in the routing table.
EntryFlags	Flag of a route.

Item	Description
Reference Cnt	Number of times the route is referenced.
Tag	Administrative tag of the route. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of the route: ● low ● medium ● high ● critical
IndirectID	ID of the indirect next hop.
Age	Time when the route is generated.

7.10.22 display rm bfd-session

Function

The **display rm bfd-session** command displays the BFD session configuration in routing management (RM).

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

display rm bfd-session [**vpn-instance** *vpn-instance-name*] [**destination** *destination-address*] [**source** *source-address*] [**interface** *interface-type interface-number*] [**protocol** { **bgp** | **isis-l1** | **isis-l2** | **isis-l1l2** | **ospf** | **rip** | **pim** }]

display rm bfd-session all

Parameters

Parameter	Description	Value
all	Displays all the BFD session configurations in RM, including the BFD session configurations of the public and private networks. If **all** is not specified, only the BFD session configuration on the public network is displayed.	-
vpn-instance *vpn-instance-name*	Displays the configurations of BFD sessions of the specified VPN instance in RM.	The value must be an existing VPN instance name.
destination *destination-address*	Displays the configurations of BFD sessions with the specified destination address in RM.	The value is in dotted decimal notation.
source *source-address*	Displays the configurations of BFD sessions with the specified source address in RM.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Displays the configurations of BFD sessions with the specified outbound interface type and number in RM.	-
protocol	Displays the configurations of BFD sessions of the specified routing protocol in RM: ● **bgp**: BGP ● **isis-l1**: IS-IS Level-1 ● **isis-l2**: IS-IS Level-2 ● **isis-l1l2**: IS-IS Level-1-2 ● **ospf**: OSPF ● **rip**: RIP ● **pim**: PIM	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view the configuration of BFD sessions dynamically created by routing protocols. The command output includes the global BFD status, number of BFD sessions, and BFD session configuration, such as VPN instance, destination address, source address, interface, and status.

Example

Display the BFD configuration in RM.

```
<HUAWEI> display rm bfd-session vpn-instance vrf1 destination 10.8.1.2 source 10.8.1.1 interface
Vlanif10
BFD Global Status: ON
BFD Session Total Number: 1

BFD Session: 1
  Interface: Vlanif10    VRF Name: vrf1
  Destination     Source          Session-State Create-State
  10.8.1.2        10.8.1.1        Up            Established
  Route-Protocol  Rx-Interval(ms) Tx-Interval(ms) Multiplier
  BGP             1000            1000            5
```

Table 7-231 Description of the display rm bfd-session command output

Item	Description
BFD Global Status	Global BFD status: ● ON: BFD is enabled globally. ● OFF: BFD is disabled globally. To set the global BFD status, run the **bfd** command.
BFD Session Total Number	Total number of BFD sessions.
BFD Session	Number of the BFD session.
Interface	Local physical interface bound to the BFD session.
VRF Name	Name of a VPN instance to which the BFD session is bound to.
Destination	Peer IP address bound to the BFD session.
Source	Source IP address bound to the BFD session.
Session-State	Status of the BFD session: ● AdminDown: indicates that the BFD session is in AdminDown state when the **shutdown** command is run. ● Down: indicates that the BFD session in Down state. ● Init: indicates that the BFD session is in Init state. ● Up: indicates that the BFD session is in Up state.

Item	Description
Create-State	BFD session setup status in RM: - Creating: indicates that the routing protocol notifies RM of the session, but RM does not instruct BFD to set up a session. - Established: indicates that RM notifies BFD to set up a BFD session. You can view the Session-State field to check whether a BFD session is set up.
Route-Protocol	Routing protocol enabled with BFD: - BGP - IS-IS Level-1 - IS-IS Level-2 - IS-IS Level-1-2 - OSPF - RIP - PIM
Rx-Interval(ms)	Configured receiving interval, in milliseconds.
Tx-Interval(ms)	Configured sending interval, in milliseconds.
Multiplier	Configured local detection multiplier.

7.10.23 display rm interface

Function

The **display rm interface** command displays routing management (RM) information on an interface.

Format

display rm interface [*interface-type interface-number*]

display rm interface [**vpn-instance** *vpn-instance-name*] [**ip-address** *ip-address*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RM information on the specified interface.	-
vpn-instance *vpn-instance-name*	Displays RM information on the interface of the specified VPN instance.	The value must be an existing VPN instance name.
ip-address *ip-address*	Displays RM information on the interface with the specified destination address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IPv4 RM information on an interface, including information about physical and logical interfaces of the interface. This information helps locate routing problems.

Example

Display RM information on interfaces.

```
<HUAWEI> display rm interface

Name: InLoopBack0
Physical IF Info:
 IfnetIndex: 0x1
 State: UP LOOP MULT
 Slot: 0(Logic Slot: 9)
 IntType: 26, PriLog: 1, MTU: 1500, Reference Count: 7
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0, Quality: 0

 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 75455sec
Logical IF Info:
 IfnetIndex: 0x1, PhyIndex: 1 Logical Index : 1,
 Dest: 127.0.0.1, Mask: 255.0.0.0
 State: UP LOOP PRM MULT , Reference Count 6
 Age: 75455sec

Name: NULL0
Physical IF Info:
```

```
 IfnetIndex: 0x2
 State: UP NBMA MULT
 Slot: 0(Logic Slot: 9)
 IntType: 27, PriLog: 2, MTU: 1500, Reference Count 1
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0, Quality: 0

 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 75455sec
Logical IF Info:
 IfnetIndex: 0x2, PhyIndex: 2 Logical Index : 2,
 Dest: 0.0.0.0, Mask: 255.255.255.255
 State: UP PRM NBMA MULT , Reference Count: 0
 Age: 75456sec

Name: MEth0/0/1                                          Physical IF
Info:
 IfnetIndex: 0x4
 State: UP BCA MULT OSI
 Hardware Address: 000e0-fc1-2123
 Slot: 0(Logic Slot: 9)
 IntType: 1, PriLog: 6, MTU: 1500, Reference Count: 4
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0, Quality: 0

 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 75423sec
Logical IF Info:
 IfnetIndex: 0x4, PhyIndex: 3 Logical Index : 6,
 Dest: 10.137.217.207, Mask: 255.255.254.0
 State: UP PRM BCA MULT , Reference Count: 3
 Age: 75447sec
```

Display RM information on VLANIF100.

```
<HUAWEI> display rm interface vlanif 100
Name: vlanif100
Physical IF Info:
 IfnetIndex: 0x23
 State: DOWN BCA MULT
 Hardware Address: 00E0-FCCB-7543
 Slot: 0(Logic Slot: 9)
 IntType: 38, PriLog: 3, MTU: 1500, Reference Count: 1
 Bandwidth: 0, 1000000000
 Baudrate: 0, 1000000000
 Delay: 0, Reliability: 0, Load: 0, Quality: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 2152167sec
Logical IF Info:
 IfnetIndex: 0x23, PhyIndex: 6, Logical Index: 3
 Dest: 10.20.10.2, Mask: 255.255.0.0
 State: DOWN PRM BCA MULT , Reference Count:
0
 Age: 2152166sec
```

Table 7-232 Description of the display rm interface command output

Item	Description
Name	Name of the interface.
Physical IF Info	Physical interface information.
IfnetIndex	Network segment index of the interface.
State	Current interface status.
Hardware Address	MAC address of the interface.
Slot	Slot ID of the interface.
IntType	Type of the interface.
PriLog	Index of the primary logical interface.
MTU	Maximum transmission unit (MTU) of the interface.
Reference Count	Number of times the interface is referenced.
Bandwidth	Bandwidth of the interface.
Baudrate	Baud rate of the interface.
Delay	Link delay.
Reliability	Link reliability.
Load	Link load.
Quality	Link quality. Currently: ● 0: indicates the link quality is "GOOD". ● 4: indicates the link quality is "LOW".
LDP-ISIS sync capability	Whether synchronization between LDP and IS-IS is enabled: ● enabled: indicates that synchronization is enabled. ● disabled: indicates that synchronization is disabled.
LDP-OSPF sync capability	Whether synchronization between LDP and OSPF is enabled: ● enabled: indicates that synchronization is enabled. ● disabled: indicates that synchronization is disabled.
InstanceID	Instance ID.
Instance Name	Instance name.

Item	Description
Logical IF Info	Logical interface information.
PhyIndex	Physical interface index.
Logical Index	Logical interface index.
Dest	Destination address.
Mask	Mask of the destination address.
Age	Lifetime of the displayed information.

7.10.24 display rm ipv6 bfd-session

Function

The **display rm ipv6 bfd-session** command displays the configurations of BFD sessions in Route Management (RM).

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

display rm ipv6 bfd-session [**all** | [[**vpn-instance** *vpn-instance-name*] [**destination** *destination-address*] [**source** *source-address*] [**interface** *interface-type interface-number*] [**protocol** { **bgp** | **isis-l1** | **isis-l2** | **isis-l1l2** | **ospfv3** | **pim** }]]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
destination *destination-address*	Specifies the remote destination address.	-
source *source-address*	Specifies the local source address.	-
interface *interface-type interface-number*	Specifies the type and number of an outbound interface.	-
protocol	Indicates a routing protocol. ● **bgp**: indicates the Border Gateway Protocol (BGP). ● **isis-l1**: indicates IS-IS Level-1. ● **isis-l2**: indicates IS-IS Level-2. ● **Isis-l1l2**: indicates IS-IS Level-1-2. ● **ospfv3**: indicates the Open Shortest Path First (OSPF) version 3 protocol. ● **pim**: indicates the Protocol Independent Multicast (PIM) protocol.	-
all	Displays all the configurations of BFD sessions in RM, including the BFD sessions of the public network and VPN. If **all** is not specified, only the configurations of BFD sessions in the public network are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the command to view the BFD sessions that are dynamically created by the routing protocol. The configurations include the global status of BFD, number of BFD sessions, and VPN instance, destination address, source address, interface, and session status of each BFD session. To modify the parameters of a BFD session, refer to the **bfd all-interfaces**, **ospfv3 bfd**, **isis ipv6 bfd**, and **peer bfd**.

Example

Display the configurations of BFD sessions in RM.

```
<HUAWEI> display rm ipv6 bfd-session vpn-instance a destination fc00:0:0::1 source fc00:0:0::2
interface GigabitEthernet0/0/1


BFD Global Status: ON
RM IPv6 BFD Session Total Number: 1
Destination: fc00:0:0::1
Source     : fc00:0:0::2
  Session-State      Local-Discr      Interface             VPN-Name
  Up                 8192             GigabitEthernet0/0/1  a
  Route-Protocol     Rx-Interval(ms)  Tx-Interval(ms)       Multiplier
  BGP                1000             1000                  7
```

Table 7-233 Description of the **display rm ipv6 bfd-session** command output

Item	Description
BFD Global Status	Global status of BFD: ● On: indicates that BFD is enabled globally. ● Off: indicates that BFD is disabled globally.
RM IPv6 BFD Session Total Number	Total number of BFD sessions.
Destination	Destination IP address bound to the BFD session.
Source	Source IP address bound to the BFD session.
Session-State	Current status of a BFD session: ● AdmDown: If the **shutdown (BFD session view)** command is used, the BFD session enters the AdmDown state. ● Down: the BFD session is in the Down state. ● Init: the BFD session is in the Init state. ● Up: the BFD session is in the Up state.
Local-Discr	Local discriminator of the BFD session. ● If the value is 0, it indicates that the RM is notified of the need to set up of a BFD session, but the RM has not instructed BFD to set up the session. ● If the value is not 0, it indicates that RM has instructed BFD to set up a BFD session. If you need to learn the establishment of the BFD session, you can view the Session-State.
Interface	Local physical interface bound to the BFD session.

Item	Description
Route-Protocol	Routing protocol enabled with BFD: ● BGP ● IS-IS Level-1 ● IS-IS Level-2 ● IS-IS Level-1-2 ● OSPFv3 ● PIM
Rx-Interval (ms)	Configured receiving interval in milliseconds.
Tx-Interval (ms)	Configured sending interval in milliseconds.
Multiplier	Configured local detection multiplier.
VPN-Name	Name of the VPN instance.

7.10.25 display rm ipv6 interface

Function

The **display rm ipv6 interface** command displays IPv6 routing management (RM) information on an interface.

Format

display rm ipv6 interface [*interface-type interface-number*]

display rm ipv6 interface [**vpn-instance** *vpn-instance-name*] [**ipv6-address** *ipv6-address*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays IPv6 RM information on the specified interface.	-
vpn-instance *vpn-instance-name*	Displays IPv6 RM information in a specified VPN instance.	The value must be an existing VPN instance name.
ipv6-address *ipv6-address*	Displays IPv6 RM information with the specified destination IPv6 address.	The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IPv6 RM information on an interface, including information about physical and logical interfaces of the interface. This information helps locate routing problems.

Example

Display IPv6 RM information on all interfaces.

```
<HUAWEI> display rm ipv6 interface

Name: InLoopBack0
Physical IF Info:
 IfnetIndex: 0x1
 State: UP LOOP MULT
 Slot: 0(Logic Slot: 0)
 IntType: 26, PriLog: 1, MTU: 1500, Ref: 1
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 Age: 1635sec

Logical IF Info:
 IfnetIndex: 0x1, PhyIndex: 1, LogiIndex: 1
 Dest: ::1, Mask: 128
 State: UP LOOP PRM MULT , Ref 1
 Age: 1635sec

Name: NULL0
Physical IF Info:
 IfnetIndex: 0x2
 State: UP NBMA MULT
 Slot: 0(Logic Slot: 0)
 IntType: 27, PriLog: 2, MTU: 1500, Ref: 0
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 Age: 1635sec

Logical IF Info:
 IfnetIndex: 0x2, PhyIndex: 2, LogiIndex: 2
 Dest: ::, Mask: 128
 State: UP PRM NBMA MULT , Ref: 0
 Age: 1635sec
```

Table 7-234 Description of the display rm ipv6 interface command output

Item	Description
Name	Name of an interface.
Physical IF Info	Physical interface information.

Item	Description
IfnetIndex	Network segment index of the interface.
State	Interface status.
IntType	Interface type.
Slot	Slot ID.
PriLog	Index of the primary logical interface.
MTU	Maximum transmission unit (MTU) of the interface.
Ref	Number of times the interface is referenced.
Bandwidth	Bandwidth of the interface.
Baudrate	Baud rate of the interface.
Delay	Link delay.
Reliability	Link reliability.
Load	Link load.
Age	Lifetime of the displayed information.
Logical IF Info	Logical interface information.
PhyIndex	Physical index.
LogiIndex	Logical index.
Dest	Destination IPv6 address.
Mask	Prefix length of the destination IPv6 address.

7.10.26 display router id

Function

The **display router id** command displays the configured router ID.

Format

display router id [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the configured router ID of the specified VPN instance. If this parameter is not specified, the configured router ID of the public network is displayed.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Some dynamic routing protocols require a router ID to uniquely identify a device. If no router ID is specified when these routing protocols are enabled, the global router ID is used by default. You can run the **display router id** command to check the global router ID.

Example

Display the configured router ID.

```
<HUAWEI> display router id
RouterID:10.1.1.1
```

7.10.27 display route resource

Function

The **display route resource** command displays the total number of IPv4 and IPv6 route prefixes in the IP routing table on the device.

Format

display route resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display route resource** command displays the total number of IPv4 and IPv6 route prefixes in the IP routing table on the device.

Example

Display the total number of IPv4 and IPv6 route prefixes in the IP routing table on the device.

```
<HUAWEI> display route resource
 Total number of IPv4 Prefixes: 16
 Total number of IPv6 Prefixes: 13
```

Table 7-235 Description of the **display route resource** command output

Item	Description
Total number of IPv4 Prefixes	Current number of IPv4 route prefixes.
Total number of IPv6 Prefixes	Current number of IPv6 route prefixes.

7.10.28 ecmp load-balance

Function

The **ecmp load-balance** command sets the ECMP load balancing mode.

The **undo ecmp load-balance** command deletes the configured ECMP load balancing mode.

By default, ECMP load balancing is performed on packets based on the source IP address, destination IP address, transport-layer source port number and destination port number.

Product	Support
S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730S-H, S6730-H, S6730-S, and S6730S-S	Supported
SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735S-H, S5736-S and S6720S-S	Not supported

Format

ecmp load-balance sip [**dip**] [**port**]

undo ecmp load-balance sip [**dip**] [**port**]

Parameters

Parameter	Description	Value
sip	Configures ECMP load balancing based on the source IP address.	-
dip	Configures ECMP load balancing based on the destination IP address.	-
port	Configures ECMP load balancing based on the transport-layer source port number and destination port number.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you run the **ecmp load-balance** command in the system view multiple times, only the latest configuration takes effect.

Example

Configure ECMP load balancing based on the source IP address.

```
<HUAWEI> system-view
[HUAWEI] ecmp load-balance sip
```

7.10.29 ecmp load-balance diffluence

Function

The **ecmp load-balance diffluence** command configures ECMP-based distribution of packets with the same source address and destination address.

The **undo ecmp load-balance diffluence** command cancels ECMP-based distribution of packets with the same source address and destination address.

By default, ECMP-based distribution of packets with the same source address and destination address is not configured.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ecmp load-balance diffluence

undo ecmp load-balance diffluence

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to analyzing the unidirectional traffic of the two communication parties, a packet analysis device needs to analyze traffic between the two communication parties so that the traffic information can be fully analyzed. In this case, the packets of the two communication parties need to be distributed to the same traffic distribution server. The traffic distribution device is required to support the algorithm based on the same source and destination in the specific forwarding procedure. Identical source and destination indicates that bidirectional data packets of a network connection must be sent out from the same outbound interface. To configure ECMP-based traffic distribution of packets with the same source addresses and destination addresses, run the **ecmp load-balance diffluence** command.

Precautions

This function may cause uneven load balancing among IPv4 and IPv6 routes.

In a VXLAN scenario, ECMP-based distribution of packets with the same source address and destination address does not take effect; instead, the configured ECMP load balancing mode takes effect..

Example

Configure ECMP-based distribution of packets with the same source addresses and destination addresses.

```
<HUAWEI> system-view
[HUAWEI] ecmp load-balance diffluence
```

7.10.30 ecmp local-preference disable

Function

The **ecmp local-preference disable** command disables ECMP local preferential forwarding.

The **undo ecmp local-preference disable** command enables ECMP local preferential forwarding.

By default, ECMP local preferential forwarding is enabled.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ecmp local-preference disable

undo ecmp local-preference disable

Parameters

None

Views

System view

Default Level

2: Configuration level

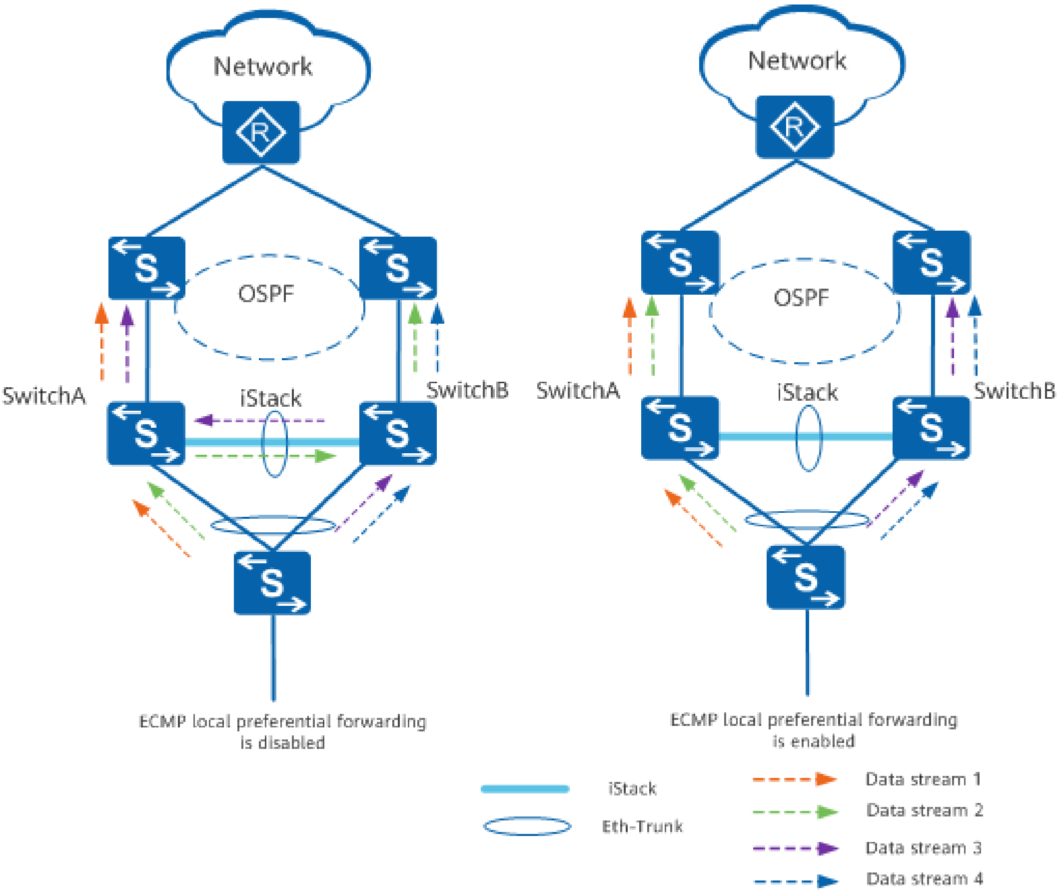
Usage Guidelines

Usage Scenario

Generally, you can use an Eth-Trunk or equal-cost routes to implement traffic load balancing. In a stack, when an inter-chassis Eth-Trunk is unavailable, you can use equal-cost routes for traffic load balancing. Because traffic will be forwarded between member switches, during a stack switchover, traffic switching depends on route convergence, causing some traffic to be lost. In this case, use ECMP local preferential forwarding to improve route convergence performance during a stack switchover and reduce traffic loss. In ECMP local preferential forwarding, traffic reaching the local switch is preferentially forwarded through a local interface. If the local outbound interface fails, traffic is forwarded through an interface on another member switch.

In **Figure 7-4**, SwitchA and SwitchB set up a stack and implement ECMP load balancing with upstream devices. If local preferential forwarding is not configured, traffic reaching SwitchA is load balanced based on ECMP, and some traffic is forwarded through stack cables and sent out from a physical interface on SwitchB. After local preferential forwarding is configured, traffic reaching SwitchA is forwarded through a local physical interface instead of a physical interface on SwitchB.

Figure 7-4 ECMP local preferential forwarding



Configuration Impact

After ECMP local preferential forwarding is enabled in a stack, traffic entering from the local device is preferentially forwarded through a local interface. Therefore, even load balancing of the traffic cannot be guaranteed. To address this issue, you can run the **ecmp local-preference disable** command to disable ECMP local preferential forwarding.

Precautions

- Only a stack supports ECMP local preferential forwarding.
- After the system software of a switch is upgraded to V200R010C00 or later, the **ecmp local-preference disable** configuration is automatically generated.
- Enabling or disabling ECMP local preferential forwarding takes effect immediately for newly added routes and takes effect for existing routes only after these routes are re-advertised.
- ECMP local preferential forwarding does not take effect in the following scenarios:
  - No ARP or ND entry for the next hop of a route is found.
  - The next hop of a route is a blackhole.
  - The next-hop outbound interface of a route is an Eth-Trunk interface.

Example

Disable ECMP local preferential forwarding.

```
<HUAWEI> system-view
[HUAWEI] ecmp local-preference disable
Warning: The operation will take effect only on routing tables generated later.
```

7.10.31 fib regularly-refresh

Function

The **fib regularly-refresh** command configures the entire FIB entry update interval, FIB entry update interval per cycle, and the number of FIB entries updated per cycle.

The **undo fib regularly-refresh** command restores the default entire FIB entry update interval, FIB entry update interval per cycle, and the number of FIB entries updated per cycle.

By default, the FIB entry update interval per cycle is 1 second, and the number of FIB entries updated per cycle is 50. The entire FIB entry update interval is 1 minute on the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H, and is fixed to 1440 minutes on other devices.

Format

fib regularly-refresh { **interval** *interval* [**entry-number** *entry-number*] | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* }

undo fib regularly-refresh { **interval** *interval* [**entry-number** *entry-number*] | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* }

Parameters

Parameter	Description	Value
interval *interval*	Specifies an interval at which FIB entries are refreshed.	The value is an integer ranging from 1 to 300, in seconds.

Parameter	Description	Value
entry-number *entry-number*	Specifies the number of FIB entries refreshed per circle.	The value is an integer ranging from 20 to 2000.
cycle-interval *cycle-interval*	Specifies the entire interval at which FIB entries are updated.	The value is an integer ranging from 1 to 1440, in minutes. **NOTE** This parameter is supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Regular FIB entry updating occupies system resources, including CPU and memory resources. A longer update interval and a smaller number of updated entries result in less impact on other services. You can flexibly configure the update interval and the number of entries to be updated based on system resources.

To allow underlying data to be forwarded in real-time and effective ways, you can configure a device to update FIB entries in cycles. The *cycle-interval* parameter specifies the interval for FIB entry update per cycle. Note that the *cycle-interval*, *interval*, and *entry-number* parameters together determine the FIB entry update process. As an example, assume that a device has 500 FIB entries.

- If *interval* is set to 1 second, *entry-number* is set to 50, and *cycle-interval* is set to 1 minute, the 500 FIB entries are updated in 10 cycles (with 50 FIB entries updated in each cycle), and the entry update can be completed within 10s (1s for each cycle). The device stays idle from 10s to 1 minute (entire FIB entry update interval).
- If *interval* is set to 10 seconds, *entry-number* is set to 50, and *cycle-interval* is set to 1 minute, the 500 FIB entries are still updated in 10 cycles, taking a total of 100 seconds. In this case, the update period exceeds 1 minute, and the device cycles update from the next minute (a total of 2 minutes at this point). That is, the device updates FIB entries at an interval of 2 minutes.

Prerequisites

Regular FIB entry updating has been enabled using the **undo fib regularly-refresh disable** command in the system view. This function is enabled by default.

Example

Set an interval at which FIB entries are updated to 5 seconds and the number of FIB entries updated per circle to 200.

```
<HUAWEI> system-view
[HUAWEI] fib regularly-refresh interval 5 entry-number 200
```

7.10.32 fib regularly-refresh disable

Function

The **fib regularly-refresh disable** command disables the FIB entry update function.

The **undo fib regularly-refresh disable** command enables the FIB entry update function.

By default, the FIB entry update function is enabled.

Format

fib regularly-refresh disable

undo fib regularly-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a device starts FIB entry update 30 minutes after a device is powered on, and the update is performed regularly at an interval of 1 minute. Updating FIB entries occupy system resources. To avoid a high CPU usage within a short period, run the **fib regularly-refresh** { **interval** *interval* [**entry-number** *entry-number*] | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* } command to set the entire FIB entry update interval or the FIB entry update interval per cycle to a larger value or reduce the number of FIB entries updated per cycle. If the CPU usage problem still persists, run the **fib regularly-refresh disable** command to disable the FIB entry update function.

Precautions

Disabling the FIB entry update function may cause a failure to rectify certain hardware faults in time. Exercise caution when running the **fib regularly-refresh disable** command.

Example

Disable the FIB from being refreshed.

```
<HUAWEI> system-view
[HUAWEI] fib regularly-refresh disable
```

7.10.33 fib threshold-alarm

Function

The **fib threshold-alarm** command enables the alarm function for IPv4 route prefix usage and sets the alarm threshold.

The **undo fib threshold-alarm** command restores the default alarm threshold.

By default, the alarm function for IPv4 route prefix usage is enabled. The upper alarm threshold is 85% and the lower alarm threshold is 75%.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

fib threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo fib threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for IPv4 route prefix usage.	The value is an integer that ranges from 1 to 100, in percentage.

Parameter	Description	Value
lower-limit *lower-limit-value*	Sets the lower alarm threshold for IPv4 route prefix usage.	The value is an integer that ranges from 1 to 100, in percentage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Overload of the IPv4 route prefix usage will cause entries unable to be delivered and result in a forwarding failure.

- When the upper alarm threshold for IPv4 route prefix usage is smaller than 100%, an alarm is generated when the resource usage exceeds the upper alarm threshold or reaches 100%.
- When the upper alarm threshold for IPv4 route prefix usage is set to 100%, an alarm is generated when the resource usage reaches 100%.

Precautions

In versions earlier than V200R019C00SPC300, the upper alarm threshold for the IPv4 route prefix usage can be greater than or equal to the lower alarm threshold. In V200R019C00SPC300 and later versions, the upper alarm threshold for the IPv4 route prefix usage must be greater than the lower alarm threshold. If the upper alarm threshold for the IPv4 route prefix usage is configured to be equal to the lower alarm threshold on a switch running a version earlier than V200R019C00SPC300, the configuration will be lost after the switch is upgraded to V200R019C00SPC300 or a later version, and the upper and lower alarm thresholds will be restored to the default settings.

Example

Enable the alarm function for IPv4 route prefix usage and set the upper and lower alarm thresholds to 85% and 60% respectively.

```
<HUAWEI> system-view
[HUAWEI] fib threshold-alarm upper-limit 85 lower-limit 60
```

7.10.34 fib trap lpm-fail enable

Function

The **fib trap lpm-fail enable** command enables the trap function for the event that FIB entries fail to be delivered.

The **undo fib trap lpm-fail enable** command disables the trap function for the event that FIB entries fail to be delivered.

By default, the trap function is enabled for the event that FIB entries fail to be delivered.

NOTE

Only the S5735S-H, S5736-S and S6720S-S support this command.

Format

fib trap lpm-fail enable

undo fib trap lpm-fail enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FIB entries may fail to be delivered because of an LPM algorithm error. For fault location, you can run the **fib trap lpm-fail enable** command to enable the trap function for the event that FIB entries fail to be delivered and check trap function. After this trap function is disabled, no trap is generated when FIB entries fail to be delivered because of an LPM algorithm error.

Precautions

Traps are generated for the event that FIB entries fail to be delivered only when this trap function is enabled. To set the trap interval, run the **fib trap lpm-fail interval** command. To set the maximum number of traps generated in a trap interval, run the **fib trap lpm-fail history** command.

Example

Enable the trap function for the event that FIB entries fail to be delivered because of an LPM algorithm error.

```
<HUAWEI> system-view
[HUAWEI] fib trap lpm-fail enable
```

7.10.35 fib trap lpm-fail history

Function

The **fib trap lpm-fail history** command sets the maximum number of traps generated when FIB entries fail to be delivered.

The **undo fib trap lpm-fail history** command restores the default maximum number of traps generated when FIB entries fail to be delivered.

By default, a maximum of 10 traps are generated each time FIB entries fail to be delivered.

NOTE

Only the S5735S-H, S5736-S and S6720S-S support this command.

Format

fib trap lpm-fail history *history-number*

undo fib trap lpm-fail history

Parameters

Parameter	Description	Value
history-number	Sets the maximum number of traps generated each time FIB entries fail to be delivered.	The value is an integer that ranges from 10 to 30.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FIB entries may fail to be delivered because of an LPM algorithm error. By default, a maximum of 10 traps are generated each time FIB entries fail to be delivered. To change the maximum number of traps generated each time FIB entries fail to be delivered, run the **fib trap lpm-fail history** *history-number* command.

Example

Set the maximum number of traps generated each time FIB entries fail to be delivered to 30.

```
<HUAWEI> system-view
```

```
[HUAWEI] fib trap lpm-fail history 30
```

7.10.36 fib trap lpm-fail interval

Function

The **fib trap lpm-fail interval** command sets the interval for generating traps when FIB entries fail to be delivered.

The **undo fib trap lpm-fail interval** command restores the default interval for generating traps when FIB entries fail to be delivered.

By default, traps are generated at an interval of 60s when FIB entries fail to be delivered.

NOTE

Only the S5735S-H, S5736-S and S6720S-S support this command.

Format

fib trap lpm-fail interval *interval-number*

undo fib trap lpm-fail interval

Parameters

Parameter	Description	Value
interval-number	Sets the interval for generating traps.	The value is an integer that ranges from 30 to 3600, in seconds. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FIB entries may fail to be delivered because of an LPM algorithm error. By default, traps are generated at an interval of 60s when FIB entries fail to be delivered because of an LPM algorithm error. To change the interval, run the **fib trap lpm-fail interval** *interval-number* command.

Example

Set the interval for generating traps when FIB entries fail to be delivered to 90s.

```
<HUAWEI> system-view
[HUAWEI] fib trap lpm-fail interval 90
```

7.10.37 ip frr (system view)

Function

The **ip frr** command enables IP FRR for public routes.

The **undo ip frr** command disables IP FRR for public routes.

By default, IP FRR is disabled for public routes.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ip frr route-policy *route-policy-name*

undo ip frr [**all**]

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Enables IP FRR for public routes matching the specified route-policy.	The value must be an existing route-policy.
all	Disables IP FRR for all public and private routes. If this parameter is not specified, IP FRR is disabled for all public routes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the development of the network, services such as audio, online video, and finance have more requirements for real time. Generally, active/standby links are deployed on the network to ensure service stability.

However, under traditional forwarding modes, when multiple routes to the same destination exist, switch selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, switch waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ip frr** command, you can enable IP FRR of the public network. IP FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv4 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

The **ip frr** command should be used with the **apply backup-interface** command and the **apply backup-nexthop** command. It is required to use the **route-policy** command to create route-policy at first, in which the **apply backup-interface** command and the **apply backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv4 route of the public network.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance IPv4 address family view will not interfere each other.

Using the **undo ip frr all** command, IP FRR of all the public network and the private networks is disabled. Use it with caution.

Example

Specify a backup outbound interface and a backup next hop in route-policy **ip_frr_rp** and enable IP FRR for public routes in the system view.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-interface vlanif 100
[HUAWEI-route-policy] apply backup-nexthop 192.168.20.2
[HUAWEI-route-policy] quit
[HUAWEI] ip frr route-policy ip_frr_rp
```

7.10.38 ip prefix-limit

Function

The **ip prefix-limit** command configures a limit on the number of IPv4 public route prefixes.

The **undo ip prefix-limit** command restores the default configuration.

By default, the maximum number of IPv4 public route prefixes is not limited.

Format

ip prefix-limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo ip prefix-limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IPv4 public route prefixes.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of IPv4 public route prefixes. If you specify *alert-percent* in the command, when the number of IPv4 public route prefixes exceeds the value calculated by (*number* x *alert-percent*) / 100, an alarm is generated. Additional IPv4 public route prefixes can still be added to the routing table until the number of IPv4 public route prefixes reaches *number*. Subsequent route prefixes are discarded.	The value is an integer ranging from 1 to 100.
route-unchanged	Indicates that the routing table remains unchanged. If you decrease *alert-percent* after the number of IPv4 public route prefixes exceeds *number*, whether the routing table remains unchanged is determined by **route-unchanged**. • If you specify **route-unchanged** in the command, the routing table remains unchanged. • If you do not specify **route-unchanged** in the command, the system deletes the routes from the routing table and re-adds routes. By default, the system deletes the routes from the routing table and re-adds routes.	-

Parameter	Description	Value
simply-alert	Indicates the following function: If you specify *simply-alert* in the command, new IPv4 public route prefixes can still be added to the routing table and only an alarm is generated after the number of IPv4 public route prefixes exceeds *number*. However, when the total number of private and public route prefixes reaches the limit on the number of unicast route prefixes specified in the PAF file, subsequent IPv4 public route prefixes are discarded.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the switch imports a large number of routes, system performance may be affected when processing services because the routes consume a lot of system resources. To improve system security and reliability, you can run the **ip prefix-limit** command to configure a limit on the number of IPv4 public route prefixes. When the number of IPv4 public route prefixes exceeds the limit, an alarm is generated, prompting you to check whether unneeded IPv4 public route prefixes exist.

Configuration Impact

After the **ip prefix-limit** command is run, the switch may discard unneeded IPv4 public route prefixes.

- If the number of IPv4 public route prefixes exceeds the value calculated from *number* x *alert-percent*/100, an alarm (RM_1.3.6.1.4.1.2011.5.25.145.19.1.3 hwPublicIpv4PrefixThresholdExceed) is generated.
- If the number of IPv4 public route prefixes exceeds *number*, an alarm (RM_1.3.6.1.4.1.2011.5.25.145.19.1.1 hwPublicIpv4PrefixExceed) is generated.
- If the number of IPv4 public route prefixes falls below the value calculated from (*number* x (*alert-percent* – 5))/100, a clear alarm (RM_1.3.6.1.4.1.2011.5.25.145.19.1.4 hwPublicIpv4PrefixThresholdExceedClear) is generated.
- If the number of IPv4 public route prefixes exceeds *number*, a clear alarm (RM_1.3.6.1.4.1.2011.5.25.145.19.1.2 hwPublicIpv4PrefixExceedClear) is generated.

Precautions

If you run the **ip prefix-limit** command for several times, the last configuration overrides previous configurations.

After the number of IPv4 public route prefixes exceeds the limit, note the following rules:

- If you run the **ip prefix-limit** command to increase *number* or the **undo ip prefix-limit** command to delete the limit, the switch relearns IPv4 public route prefixes.
- Direct and static routes can still be added to the IP routing table.

Example

Configure **simply-alert** so that only an alarm is generated when the switch imports more than 10000 IPv4 public route prefixes.

```
<HUAWEI> system-view
[HUAWEI] ip prefix-limit 10000 simply-alert
```

7.10.39 ip prefix-limit log-interval

Function

The **ip prefix-limit log-interval** command configures an interval at which logs are generated after the number of IPv4 public route prefixes exceeds the limit.

The **undo ip prefix-limit log-interval** command restores the default configuration.

By default, the system generates logs at an interval of 5s after the number of IPv4 public route prefixes exceeds the limit.

Format

ip prefix-limit log-interval *interval*

undo ip prefix-limit log-interval

Parameters

Parameter	Description	Value
interval	Specifies an interval at which logs are generated after the number of IPv4 public route prefixes exceeds the limit.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system generates logs at an interval of 5s after the number of IPv4 public route prefixes exceeds the limit. You can run the **ip prefix-limit log-interval** command to set a larger value for the interval to decrease the frequency at which these logs are generated.

The maximum number of IPv4 public route prefixes supported by the routing table can be adjusted using the **ip prefix-limit** command.

Precautions

If a log is generated to record the event that the number of IPv4 public route prefixes reaches the limit, no more routes can be added to the routing table, and subsequent routes are discarded.

Example

Set the interval at which logs are generated after the number of IPv4 public route prefixes exceeds the limit to 30s.

```
<HUAWEI> system-view
[HUAWEI] ip prefix-limit log-interval 30
```

7.10.40 ip route recursive-lookup default-route protocol

Function

The **ip route recursive-lookup default-route protocol** command sets specified routes to recurse to the default route.

The **undo ip route prefix-priority-scheduler protocol** command cancels specified routes from recursing to the default route.

By default, routes cannot recurse to the default route.

Format

ip route recursive-lookup default-route protocol { **static** | **bgp** | **msr** }

undo ip route recursive-lookup default-route protocol { **static** | **bgp** | **msr** }

NOTE

- Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **bgp** parameter.
- Only the S5720-LI, S5720S-LI, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **msr** parameter.

Parameters

Parameter	Description	Value
static	Static route	-
bgp	BGP Route	-
msr	Multicast Static Route	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic cannot be transmitted along static, BGP, or multicast static routes with an unreachable next hop. In this situation, route recursion is required. Run the **ip route recursive-lookup default-route protocol** command to recurse these routes to the default route.

Precautions

After route recursion, the actual forwarding route may change.

Example

Set static routes to recurse to the default route.

```
<HUAWEI> system-view
[HUAWEI] ip route recursive-lookup default-route protocol static
```

7.10.41 ip route trace unicast-route-change disable

Function

The **ip route trace unicast-route-change disable** command disables recording of unicast route changes.

The **undo ip route trace unicast-route-change disable** command enables recording of unicast route changes.

By default, recording of unicast route changes is enabled.

Format

ip route trace unicast-route-change disable

undo ip route trace unicast-route-change disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If recording of unicast route changes is enabled, information about changes in direct, static, OSPF, IS-IS, and BGP routes that are delivered to the routing table is recorded.

Example

Disable recording of unicast route changes.

```
<HUAWEI> system-view
[HUAWEI] ip route trace unicast-route-change disable
```

7.10.42 ipv6 fib-loadbalance-type hash-based

Function

The **ipv6 fib-loadbalance-type hash-based** command configures packets sent from a specified source to a specified destination to be forwarded using the same route.

The **undo ipv6 fib-loadbalance-type hash-based** command restores the default configuration.

By default, flow-based load balancing is used.

Format

ipv6 fib-loadbalance-type hash-based

undo ipv6 fib-loadbalance-type hash-based

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command configures packets sent from a specified source to a specified destination to be forwarded using the same route. This command takes effect only when the FIB cache fails.

Example

Configure packets sent from a specified source to a specified destination to be forwarded using the same route.

```
<HUAWEI> system-view
[HUAWEI] ipv6 fib-loadbalance-type hash-based
```

7.10.43 ipv6 fib regularly-refresh

Function

The **ipv6 fib regularly-refresh** command configures the entire IPv6 FIB entry update interval, IPv6 FIB entry update interval per cycle, and the number of IPv6 FIB entries updated per cycle.

The **undo ipv6 fib regularly-refresh** command restores the default entire IPv6 FIB entry update interval, IPv6 FIB entry update interval per cycle, and the number of IPv6 FIB entries updated per cycle.

By default, the IPv6 FIB entry update interval per cycle is 1 second, and the number of IPv6 FIB entries updated per cycle is 50. The entire IPv6 FIB entry update interval is 1 minute on the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H, and is fixed to 1440 minutes on other devices.

Format

ipv6 fib regularly-refresh { **interval** *interval* | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* }

undo ipv6 fib regularly-refresh { **interval** *interval* | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* }

Parameters

Parameter	Description	Value
interval *interval*	Specifies an interval at which IPv6 FIB entries are refreshed.	The value is an integer ranging from 1 to 300, in seconds.

Parameter	Description	Value
entry-number *entry-number*	Specifies the number of IPv6 FIB entries refreshed per circle.	The value is an integer ranging from 20 to 2000.
cycle-interval *cycle-interval*	Specifies the entire interval at which IPv6 FIB entries are updated.	The value is an integer ranging from 1 to 1440, in minutes. **NOTE** This parameter is supported only by the S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Regular IPv6 FIB entry updating occupies system resources, including CPU and memory resources. A longer update interval and a smaller number of updated entries result in less impact on other services. You can flexibly configure the update interval and the number of entries to be updated based on system resources.

To allow underlying data to be forwarded in real-time and effective ways, you can configure a device to update IPv6 FIB entries in cycles. The *cycle-interval* parameter specifies the interval for IPv6 FIB entry update per cycle. Note that the *cycle-interval*, *interval*, and *entry-number* parameters together determine the IPv6 FIB entry update process. As an example, assume that a device has 500 IPv6 FIB entries.

- If *interval* is set to 1 second, *entry-number* is set to 50, and *cycle-interval* is set to 1 minute, the 500 FIB entries are updated in 10 cycles (with 50 FIB entries updated in each cycle), and the entry update can be completed within 10s (1s for each cycle). The device stays idle from 10s to 1 minute (entire FIB entry update interval).
- If *interval* is set to 10 seconds, *entry-number* is set to 50, and *cycle-interval* is set to 1 minute, the 500 FIB entries are still updated in 10 cycles, taking a total of 100 seconds. In this case, the update period exceeds 1 minute, and the device cycles update from the next minute (a total of 2 minutes at this point). That is, the device updates FIB entries at an interval of 2 minutes.

Prerequisites

Regular IPv6 FIB entry updating has been enabled using the **undo ipv6 fib regularly-refresh disable** command in the system view. This function is enabled by default.

Example

Set an interval at which IPv6 FIB entries are updated to 5 seconds and the number of FIB entries updated per circle to 200.

```
<HUAWEI> system-view
[HUAWEI] ipv6 fib regularly-refresh interval 5 entry-number 200
```

7.10.44 ipv6 fib regularly-refresh disable

Function

The **ipv6 fib regularly-refresh disable** command disables IPv6 FIB regularly-refresh.

The **undo ipv6 fib regularly-refresh disable** command enables IPv6 FIB regularly-refresh.

By default, IPv6 FIB regularly-refresh is enabled.

Format

ipv6 fib regularly-refresh disable

undo ipv6 fib regularly-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During peak hours, refreshing the IPv6 FIB can cause over-high CPU usage and affect service reliability. To resolve this problem, run the **ipv6 fib regularly-refresh disable** command to disable IPv6 FIB regularly-refresh. After the CPU usage restores to a normal state, run the **undo ipv6 fib regularly-refresh disable** command to restore IPv6 FIB regularly-refresh.

Precautions

Disabling IPv6 FIB regularly-refresh may prevent the rectification of certain hardware forwarding entry faults. Exercise caution when running the **ipv6 fib regularly-refresh disable** command.

Example

Disable IPv6 FIB regularly-refresh.

```
<HUAWEI> system-view
[HUAWEI] ipv6 fib regularly-refresh disable
Warning: This operation will disable the function of the FIB regularly refresh,Confirm?[Y/N]:y
Info: The function of the FIB regularly refresh is disabled.
```

7.10.45 ipv6 prefix-limit

Function

The **ipv6 prefix-limit** command configures a limit on the number of IPv6 public route prefixes.

The **undo ipv6 prefix-limit** command restores the default configuration.

By default, the maximum number of IPv6 public route prefixes is not limited.

Format

ipv6 prefix-limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo ipv6 prefix-limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IPv6 public route prefixes.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of IPv6 public route prefixes. If you specify *alert-percent* in the command, when the number of IPv6 public route prefixes exceeds the value calculated by (*number* x *alert-percent*) / 100, an alarm is generated. Additional IPv6 public route prefixes can still be added to the routing table until the number of IPv6 public route prefixes reaches *number*. Subsequent route prefixes are discarded.	The value is an integer ranging from 1 to 100.

Parameter	Description	Value
route-unchanged	Indicates that the routing table remains unchanged. If you decrease *alert-percent* after the number of IPv6 public route prefixes exceeds *number*, whether the routing table remains unchanged is determined by **route-unchanged**. ● If you specify **route-unchanged** in the command, the routing table remains unchanged. ● If you do not specify **route-unchanged** in the command, the system deletes the routes from the routing table and re-adds routes. By default, the system deletes the routes from the routing table and re-adds routes.	-
simply-alert	Indicates the following function: If you specify *simply-alert* in the command, new IPv6 public route prefixes can still be added to the routing table and only an alarm is generated after the number of IPv6 public route prefixes exceeds *number*. However, when the total number of private and public route prefixes reaches the limit on the number of unicast route prefixes specified in the PAF file, subsequent IPv6 public route prefixes are discarded.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the switch imports a large number of routes, system performance may be affected when processing services because the routes consume a lot of system resources. To improve system security and reliability, you can run the **ipv6 prefix-limit** command to configure a limit on the number of IPv6 public route prefixes. When the number of IPv6 public route prefixes exceeds the limit, an alarm is generated, prompting you to check whether unneeded IPv6 public route prefixes exist.

Configuration Impact

After the **ipv6 prefix-limit** command is run, the switch may discard unneeded IPv6 public route prefixes.

Precautions

If you run the **ipv6 prefix-limit** command for several times, the last configuration overrides previous configurations.

After the number of IPv6 public route prefixes exceeds the limit, note the following rules:

- If you run the **ipv6 prefix-limit** command to increase *number* or the **undo ipv6 prefix-limit** command to delete the limit, the switch relearns IPv6 public route prefixes.
- Direct and static routes can still be added to the IPv6 routing table.

Example

Configure **simply-alert** so that only an alarm is generated when the switch imports more than 10000 IPv6 public route prefixes.

```
<HUAWEI> system-view
[HUAWEI] ipv6 prefix-limit 10000 simply-alert
```

7.10.46 ipv6 prefix-limit log-interval

Function

The **ipv6 prefix-limit log-interval** command configures an interval at which logs are generated after the number of IPv6 public route prefixes exceeds the limit.

The **undo ipv6 prefix-limit log-interval** command restores the default configuration.

By default, the system generates logs at an interval of 5s after the number of IPv6 public route prefixes exceeds the limit.

Format

ipv6 prefix-limit log-interval *interval*

undo ipv6 prefix-limit log-interval

Parameters

Parameter	Description	Value
interval	Specifies an interval at which logs are generated after the number of IPv6 public route prefixes exceeds the limit.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system generates logs at an interval of 5s after the number of IPv6 public route prefixes exceeds the limit. You can run the **ip prefix-limit log-interval** command to set a larger value for the interval to decrease the frequency at which these logs are generated.

The maximum number of IPv6 public route prefixes supported by the routing table can be adjusted using the **ipv6 prefix-limit** command.

Precautions

If a log is generated to record the event that the number of IPv6 public route prefixes reaches the limit, no more routes can be added to the routing table, and subsequent routes are discarded.

Example

Set the interval at which logs are generated after the number of IPv6 public route prefixes exceeds the limit to 30s.

```
<HUAWEI> system-view
[HUAWEI] ipv6 prefix-limit log-interval 30
```

7.10.47 ipv6 frr (system view)

Function

The **ipv6 frr** command enables IPv6 FRR for public routes.

The **undo ipv6 frr** command disables IPv6 FRR for public routes.

By default, IPv6 FRR is disabled for public routes.

Product	Support
S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI	Not supported

Format

ipv6 frr route-policy *route-policy-name*

undo ipv6 frr [**all**]

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Enables IPv6 FRR for public routes matching the specified route-policy.	The value must be an existing route-policy.
all	Disables IPv6 FRR for all public and private routes. If this parameter is not specified, IPv6 FRR is disabled for all public routes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the development of the network, services such as audio, online video, and finance have more requirements for real time. Generally, active/standby links are deployed on the network to ensure service stability.

However, under traditional forwarding modes, when multiple routes to the same destination exist, switch selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, switch waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ipv6 frr** command, you can enable IPv6 FRR of the public network. IPv6 FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv6 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

The **ipv6 frr** command should be used with the **apply ipv6 backup-interface** command and the **apply ipv6 backup-nexthop** command. It is required to use the **route-policy** command to create route-policy at first, in which the **apply ipv6 backup-interface** command and the **apply ipv6 backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv6 route of the public network.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance IPv6 address family view will not interfere each other.

Using the **undo ipv6 frr all** command, IPv6 FRR of all the public network and the private networks is disabled. Use it with caution.

Example

Specify a backup outbound interface and a backup next hop in route-policy **ipv6_frr_rp** and enable IPv6 FRR for public routes in the system view.

```
<HUAWEI> system-view
[HUAWEI] route-policy ipv6_frr_rp permit node 10
[HUAWEI-route-policy] apply ipv6 backup-interface vlanif 100
[HUAWEI-route-policy] apply ipv6 backup-nexthop 2001:db8:1::1
[HUAWEI-route-policy] quit
[HUAWEI] ipv6 frr route-policy ipv6_frr_rp
```

7.10.48 l3-forward-entry aging

Function

The **l3-forward-entry aging enable** command enables the l3-forward-entry aging function.

The **undo l3-forward-entry aging enable** command disables the l3-forward-entry aging function.

By default, the l3-forward-entry aging function is disabled.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

l3-forward-entry aging enable

undo l3-forward-entry aging enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **l3-forward-entry aging enable** command must be used together with the **l3-forward-entry regularly-check** command. After the l3-forward-entry aging function is enabled, the system reads the periodic l3-forward-entry check result everyday between 2 am and 5 am. When residual Layer 3 forwarding entries exist for more than 48 hours, the system triggers resource recycling and entry deletion.

Example

Enable the l3-forward-entry aging function.

```
<HUAWEI> system-view
[HUAWEI] l3-forward-entry aging enable
```

Disable the l3-forward-entry aging function.

```
<HUAWEI> system-view
[HUAWEI] undo l3-forward-entry aging enable
```

7.10.49 l3-forward-entry regularly-check

Function

The **l3-forward-entry regularly-check** command enables periodic l3-forward-entry check and sets the periodic l3-forward-entry check interval, scanning time for each round of check, and number of entries checked in each round of check.

The **undo l3-forward-entry regularly-check** command restores the default settings of periodic l3-forward-entry check.

By default, periodic l3-forward-entry check is enabled, the periodic l3-forward-entry check interval is 1 minute, the scanning time for each round of check is 1 second, and the number of entries checked in each round of check is 200.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

l3-forward-entry regularly-check { **enable** | **cycle-interval** *cycle-interval-value* | **interval** *interval-value* | **entry-number** *number* }

undo l3-forward-entry regularly-check { **enable** | **cycle-interval** | **interval** | **entry-number** }

Parameters

Parameter	Description	Value
enable	Enables periodic l3-forward-entry check	-
cycle-interval *cycle-interval-value*	Sets the periodic l3-forward-entry check interval.	The value is an integer that ranges from 1 to 1440, in minutes.
interval *interval-value*	Sets the scanning time for each round of l3-forward-entry check.	The value is an integer that ranges from 1 to 300, in seconds.
entry-number *number*	Sets the number of entries checked in each round of check.	The value is an integer that ranges from 20 to 2000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After periodic l3-forward-entry check is configured, the device periodically checks l3-forward-entries to ensure realtime and valid bottom-layer forwarded data and records the check result. The check result can help locate problems of Layer 3 forwarding software resource leak and residual Layer 3 forwarding hardware entries.

The three parameters, *cycle-interval*, *interval*, and *entry-number*, together determine the periodic l3-forward-entry check process. For example, the device has a total of 2,000 l3-forward-entries:

- If the three parameters use their default values, that is, 2,000 entries need to be checked in 10 rounds of check and can be checked within 10 seconds (with the scanning time of each round of check as 1 second), the system is idle during the period between 10 seconds to 1 minutes (periodic check interval).
- If *cycle-interval* is set to 1 minute, *interval* is set to 10 seconds, and *entry-number* uses the default value, 2,000 entries still need to be updated for 10 rounds of check, and a total of 100 seconds is required to finish updating these entries. Then the update time will exceed 1 minute, so the device needs to start periodic update within the next 1 minute. In this situation, periodic update is performed at an interval of 2 minutes.

Precautions

Periodic l3-forward-entry check occupies system resources, including CPU and memory resources. A longer check interval and fewer entries indicate a smaller impact on other services. You can flexibly configure the l3-forward-entry check interval and number of checked entries based on system resources.

Example

Enable periodic l3-forward-entry check.

```
<HUAWEI> system-view
[HUAWEI] l3-forward-entry regularly-check enable
```

Set the periodic l3-forward-entry check interval to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] l3-forward-entry regularly-check cycle-interval 10
```

Set the scanning time for each round of l3-forward-entry check to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] l3-forward-entry regularly-check interval 5
```

Set the number of entries checked in each round of check to 500.

```
<HUAWEI> system-view
[HUAWEI] l3-forward-entry regularly-check entry-number 500
```

Disable periodic l3-forward-entry check.

```
<HUAWEI> system-view
[HUAWEI] undo l3-forward-entry regularly-check enable
```

7.10.50 l3-forward-entry self-healing enable

Function

The **l3-forward-entry self-healing enable** command enables l3-forward-entry self-healing.

The **undo l3-forward-entry self-healing enable** command disables l3-forward-entry self-healing.

By default, the l3-forward-entry self-healing function is disabled.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

l3-forward-entry self-healing enable

undo l3-forward-entry self-healing enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **l3-forward-entry regularly-check** command is configured on a switch, the switch periodically checks l3-forward-entries to ensure real-time and effective forwarding of data at the bottom layer. In this situation, if the **l3-forward-entry self-healing enable** command is configured to enable l3-forward-entry self-healing, the switch can repair l3-forward-entries for self-healing based on the check result to ensure correct packet forwarding.

Example

Enable l3-forward-entry self-healing.

```
<HUAWEI> system-view
[HUAWEI] l3-forward-entry self-healing enable
```

7.10.51 l3-interface regularly-refresh

Function

The **l3-interface regularly-refresh** command enables periodic l3-interface entry update and configures the periodic l3-interface entry update interval, scanning time for each round of update, and number of entries updated in each round of update.

The **undo l3-interface regularly-refresh** command restores the default configuration.

By default, periodic l3-interface entry update is enabled, the periodic l3-interface entry update interval is 1 minute, the scanning time for each round of update is 1 second, and the number of entries updated in each round of update is 50.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

l3-interface regularly-refresh { **enable** | **cycle-interval** *cycle-interval-value* | **scan-interval** *scan-interval-value* | **entry-number** *entry-number* }

undo l3-interface regularly-refresh { **enable** | **cycle-interval** | **scan-interval** | **entry-number** }

Parameters

Parameter	Description	Value
enable	Enables periodic l3-interface entry update.	-
cycle-interval *cycle-interval-value*	Sets the periodic l3-interface entry update interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Parameter	Description	Value
scan-interval *scan-interval-value*	Sets the scanning time for each round of l3-interface entry update.	The value is an integer that ranges from 1 to 300, in seconds.
entry-number *entry-number*	Sets the number of entries updated in each round of l3-interface entry update.	The value is an integer that ranges from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the periodic l3-interface entry update function is configured on a switch, the switch periodically updates l3-interface entries to ensure real-time and effective forwarding of data at the bottom layer and records revision information.

The three parameters, *cycle-interval*, *scan-interval*, and *entry-number*, together determine the periodic l3-interface entry update process. For example, the switch has a total of 500 l3-interface entries:

- If the three parameters retain their default values, that is, 500 entries need to be updated in 10 rounds and can be checked within 10 second (with the scanning time of each round of update as 1 second), the system is idle during the period between 10 seconds to 1 minute (periodic update interval).
- If *cycle-interval* is set to 1 minute, *scan-interval* is set to 10 seconds, and *entry-number* retains the default value, 500 entries still need to be updated for 10 rounds, and a total of 100 seconds is required to finish updating these entries. Then the update time will exceed 1 minute, so the switch needs to start periodic update within the next 1 minute. In this situation, periodic update is performed at an interval of 2 minutes.

Precautions

Periodic l3-interface entry update occupies system resources, including CPU and memory resources. A longer check interval and fewer entries indicate a smaller impact on other services. Flexibly configure the l3-interface entry update interval and number of l3-interface entries updated each time based on system resources.

Example

Enable periodic l3-interface entry update.

```
<HUAWEI> system-view
[HUAWEI] l3-interface regularly-refresh enable
```

Set the periodic l3-interface entry update interval to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] l3-interface regularly-refresh cycle-interval 10
```

Set the scanning time for each round of l3-interface entry update to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] l3-interface regularly-refresh scan-interval 5
```

Set the number of entries checked in each round of update to 100.

```
<HUAWEI> system-view
[HUAWEI] l3-interface regularly-refresh entry-number 100
```

Disable periodic l3-interface entry update.

```
<HUAWEI> system-view
[HUAWEI] undo l3-interface regularly-refresh enable
```

7.10.52 l3-interface periodic-refresh disable

Function

The **l3-interface periodic-refresh disable** command disables the function of updating l3-interface entries every 10 hours.

The **undo l3-interface periodic-refresh disable** command enables the function of updating l3-interface entries every 10 hours.

By default, l3-interface entries are updated every 10 hours.

Format

l3-interface periodic-refresh disable

undo l3-interface periodic-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a device updates l3-interface entries every 10 hours. To reduce the load on the device, you can run this command to disable the device from updating l3-interface entries every 10 hours.

Precautions

To disable all functions of periodically updating l3-interface entries on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, you need to run both the **l3-interface periodic-refresh disable** and **undo l3-interface regularly-refresh** commands.

Example

Disable the function of updating l3-interface entries every 10 hours.

```
<HUAWEI> system-view
[HUAWEI] l3-interface periodic-refresh disable
```

7.10.53 refresh fib

Function

The **refresh fib** command delivers IPv4 FIB policies and forwarding entries.

Format

refresh fib slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a switch that needs to update IPv4 FIB policies.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IPv4 FIB policy changes, you must run the **refresh fib** command to update the switch to make the configuration take effect.

After the **refresh fib** command is executed, you can view the FIB table to check whether the update succeeds.

Precautions

If the FIB module is in overload state and the switch works in overload suspension mode, the IPv4 and IPv6 modules need to be updated.

Example

Refresh IPv4 FIB module on the switch in slot 2.

```
<HUAWEI> system-view
[HUAWEI] refresh fib slot 2
```

7.10.54 refresh ipv6 fib

Function

The **refresh ipv6 fib** command delivers IPv6 FIB policies and forwarding entries.

Format

refresh ipv6 fib slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a switch that needs to update IPv6 FIB policies.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the IPv6 FIB policy changes, you must run the **refresh ipv6 fib** command to update the switch to make the configuration take effect.

After the **refresh ipv6 fib** command is executed, you can view the FIB table to check whether the update succeeds.

NOTE

If the FIB module is in overload state and the switch works in overload suspension mode, the IPv4 and IPv6 modules need to be updated.

Example

Update the IPv6 FIB module on the switch in slot 2.

```
<HUAWEI> system-view
[HUAWEI] refresh ipv6 fib slot 2
```

7.10.55 reset ip routing-table statistics protocol

Function

The **reset ip routing-table statistics protocol** command clears route statistics in an IPv4 routing table.

Format

reset ip routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { **all** | *protocol* }

reset ip routing-table all-vpn-instance statistics protocol { **all** | *protocol* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears route statistics in an IPv4 routing table of the specified VPN instance. If this parameter is not specified, route statistics in an IPv4 routing table of the public network are cleared.	The value must be an existing VPN instance name.
all	Clear route statistics of all routing protocols in an IPv4 routing table.	-
protocol	Clears route statistics of the specified routing protocol in an IPv4 routing table. This parameter can be the following keywords. For details, see the routing protocols supported by the device: **direct**, **bgp**, **isis**, **ospf**, **rip**, **static**, and **unr**.	-
all-vpn-instance	Clears the statistics in the IPv4 routing tables of all VPN instances.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to clear route statistics in an IPv4 routing table, including statistics about the routes added, deleted, and released by each routing protocol. Subsequently, the system can re-collect route statistics of each routing protocol again to monitor route changes and locate network faults.

Precautions

IPv4 route statistics cannot be restored after being cleared. Exercise caution when you use this command.

Example

Clear route statistics of all routing protocols in an IPv4 routing table.

```
<HUAWEI> reset ip routing-table statistics protocol all
```

7.10.56 reset ipv6 routing-table statistics protocol

Function

The **reset ipv6 routing-table statistics protocol** command clears route statistics in an IPv6 routing table.

Format

reset ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **statistics protocol** { **all** | *protocol* }

reset ipv6 routing-table all-vpn-instance statistics protocol { **all** | *protocol* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value must be an existing VPN instance name.
all	Clear route statistics of all routing protocols in an IPv6 routing table.	-
protocol	Clears route statistics of the specified routing protocol in an IPv6 routing table.	The value may be **bgp, direct**, **isis, ospfv3, ripng**, **static**, or **unr**. The specific value varies depending on the routing protocol supported by the device.
all-vpn-instance	Clears the statistics in the IPv6 routing tables of all VPN instances.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to clear route statistics of each routing protocol in an IPv6 routing table. Subsequently, the switch can re-collect route statistics of each routing protocol to monitor route changes and locate network faults.

Precautions

IPv6 route statistics cannot be restored after being cleared. Exercise caution when you use this command.

Example

Clear route statistics of all routing protocols in an IPv6 routing table.

```
<HUAWEI> reset ipv6 routing-table statistics protocol all
```

7.10.57 router id

Function

The **router id** command sets the global router ID.

The **undo router id** command deletes the configured global router ID.

By default, the global router ID is 0.0.0.0 when no IPv4 interface address is configured.

Format

router id *router-id*

undo router id

Parameters

Parameter	Description	Value
router-id	Sets a router ID in the IPv4 address format.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router ID is a 32-bit integer used to uniquely identify a device that uses a specific dynamic routing protocol for route exchange. A router ID uses the same format as an IP address. Router IDs are classified into global router IDs of devices and router IDs of dynamic routing protocols.

The rules for selecting a global router ID are as follows:

1. If you set the global router ID using the **router id** command, the configured router ID is used.
2. If no global router ID is set, the router selects a router ID based on IP addresses of current interfaces:
   - If there are loopback interfaces that have IP addresses configured, the device selects the largest IP address among loopback interface addresses as the global router ID.
   - If no loopback interface is configured or loopback interfaces do not have IP addresses configured, the device selects the largest IP address among interface addresses as the global router ID without considering the Up/Down state of interfaces.

   NOTE

   The global router ID is reselected only when the interface address that is selected as the global router ID is deleted or changed. The global router ID is not reselected in any of the following situations:

   - The interface is Down.
   - A loopback interface is configured when the IP address of a non-loopback interface is selected as the router ID.
   - A larger interface address is configured later.

   You can run the **display router id** command to view the global router ID.
3. Each VPN instance selects the router ID from the IP addresses of the interfaces in the VPN instance based on rules 1 and 2.

After the global router ID is changed, manually run the **reset** command for each routing protocol to make the new global router ID take effect.

Precautions

When a device is being initialized and there is no interface address on the device, the first configured IP address on the device, which may be a loopback interface address or another interface address, will become the global router ID of the device. This global router ID remains unchanged even if there is a larger interface IP address on the device.

The IP address of the interface whose configuration is restored the first is used as the global router ID after the restart.

NOTE

To enhance network reliability, configure the address of a loopback interface as the global router ID.

Example

Set the global router ID to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] router id 10.10.10.1
```

7.10.58 route low-priority enable

Function

The **route low-priority enable** command sets the priority of routes on the forwarding plane to be lower than the ARP/ND priority.

The **undo route low-priority enable** command sets the priority of routes on the forwarding plane to be higher than the ARP/ND priority.

By default, on a device running a version earlier than V200R019C00SPC210, the priority of routes (excluding BGP routes and blackhole routes) on the forwarding plane is lower than the ARP/ND priority. On a device running V200R019C00SPC210 or later, the priority of routes on the forwarding plane is higher than the ARP/ND priority.

Format

route low-priority enable

undo route low-priority enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The control plane and forwarding plane of the routing system are separated and cooperate with each other to forward data. The control plane learns and exchanges routing protocols, calculates routes, generates routing entries, and delivers the entries to the forwarding plane for packet forwarding. The forwarding plane receives and sends packets, encapsulates and decapsulates packets, queries routing entries, and forwards packets.

If the control plane has host routes and ARP entries with the same destination IP address as the host routes, the forwarding plane forwards packets based on the routes because the route priority on the control plane is higher than the ARP/ND priority. On the forwarding plane, packets are forwarded based on routes or ARP/ND entries, depending on which ones have higher priority. For example, if the route priority on the forwarding plane is lower than the ARP/ND priority, packets are forwarded based on ARP/ND entries. In this case, if the outbound interface of an ARP/ND entry is different from that of a route, for example, the outbound interface is manually specified in a static ARP entry, different forwarding behaviors will be performed.

Therefore, you need to run the **route low-priority enable** command to adjust the route priority on the forwarding plane to control whether packets are forwarded based on routes or ARP/ND entries.

Precautions

- In actual deployment, if there is no special requirement, to ensure consistent forwarding behaviors on the forwarding plane and control plane, it is recommended that the route priority on the forwarding plane be higher than the ARP/ND priority.
- This command takes effect only for newly generated routes. For existing routes, you need to run the **refresh fib** and **refresh ipv6 fib** commands to manually refresh routes after running this command. During route refresh, path switching may cause temporary traffic interruptions.
- In an upgrade scenario, after a device running V200R019C00SPC200 or an earlier version is upgraded to V200R019C00SPC210 or a later version, the route priority on the forwarding plane remains unchanged. That is, the route priority on the forwarding plane is lower than the ARP/ND priority. This conflicts with the default setting on switches running V200R019C00SPC210 or a later version. This is because the route priority on the forwarding plane is higher than the ARP/ND priority on these switches by default. To resolve the conflict, the **route low-priority enable** command is automatically generated in the configuration file of a switch.

Example

Set the route priority on the forwarding plane to be higher than the ARP/ND priority.

```
<HUAWEI> system-view
[HUAWEI] undo route low-priority enable
```

7.11 PBR Configuration Commands

7.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.11.2 redirect ip-multihop

Function

The **redirect ip-multihop** command configures an action of redirecting packets to multiple next hop IP addresses in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to multiple next hop IP addresses is not configured in a traffic behavior.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

redirect [**vpn-instance** *vpn-instance-name*] **ip-multihop** { **nexthop** *ip-address* } &<2-4>

redirect [**vpn-instance** *vpn-instance-name*] **ip-multihop** *acl-ip-pool-name*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
nexthop *ip-address*	Specifies the IP address of the next hop.	The value is in dotted decimal notation and in X.X.X.X format.
acl-ip-pool-name	Specifies the name of an ACL IP address pool.	The ACL IP address pool name must exist.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple next hop IP addresses are specified, the device redirects packets through equal-cost routes in load balancing mode.

If the outbound interface corresponding to a next hop IP address becomes Down or a route changes, the device switches traffic to the outbound interface corresponding to an available next hop. If the specified next hops are unavailable, the device forwards the packets to the original destination.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to multiple next hop IP addresses.

Precautions

- In a traffic behavior, the **redirect ip-multihop** command cannot be used together with any of the following commands: **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id** and **remark vlan-id**.
- A traffic policy containing the redirection action can be only used globally, on an interface, or in a VLAN in the inbound direction.
- If you configure only two identical IP addresses when executing the **redirect ip-multihop** command, the system displays the following error message:
  ```
  Error: Redirect ip-multihop should configure at least two address.
  ```
- If the device has no ARP entry matching the specified next hop IP address, the **redirect ip-multihop** command can be used but redirection does not take effect. The device still forwards packets to the original destination until the device has the corresponding ARP entry.

Example

Configure three next hop IP addresses in the traffic behavior **b1**: 10.1.42.1, 10.2.12.3, and 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect ip-multihop nexthop 10.1.42.1 nexthop 10.2.12.3 nexthop 10.1.1.2
```

In the traffic behavior **b2**, configure the action of redirecting packets to five next hop IP addresses in the ACL IP address pool **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl ip-pool abc
[HUAWEI-acl-ip-pool-abc] ip address 192.168.10.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.20.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.30.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.40.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.50.1 32
[HUAWEI-acl-ip-pool-abc] quit
[HUAWEI] traffic behavior b2
[HUAWEI-behavior-b2] redirect ip-multihop abc
```

7.11.3 redirect ip-nexthop

Function

The **redirect ip-nexthop** command configures the action of redirecting packets to a next-hop IP address in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, the action of redirecting packets to a next-hop IP address is not configured in a traffic behavior.

Format

redirect [**remote**] [**vpn-instance** *vpn-instance-name*] **ip-nexthop** { *ip-address* [**track-nqa** *admin-name test-name*] } &<1-4> [**forced** | **low-precedence**] *

undo redirect

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vpn-instance** *vpn-instance-name* and **low-precedence**.

Parameters

Parameter	Description	Value
remote	Redirects packets to a remote next hop.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a next-hop IP address.	The value is in dotted decimal notation and in X.X.X.X format.
track-nqa	Specifies an NQA test instance.	-
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), hyphens (-), and a single or consecutive quotation marks (").

Parameter	Description	Value
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), hyphens (-), and a single or consecutive quotation marks (").
forced	Specifies that packets are discarded if the next hop is unavailable.	-
low-precedence	Specifies a low-priority next hop. **NOTE** If this parameter is specified, redirection-based PBR has a lower priority than routes generated through dynamic routing protocols or statically configured routes. If this parameter is not specified, the former has a higher priority than the latter. In enhanced-ipv4 or ipv4-ipv6 6:1 resource assignment mode, the S6720-EI does not support redirection to low-priority next hops. You can run the **display resource-mode configuration** command to view the resource assignment mode on the device, and run the **assign resource-mode** { **enhanced-mac** | **enhanced-arp** | **enhanced-ipv4** | **ipv4-ipv6 6:1** } [**slot** *slot-id* | **all**] command to change the resource assignment mode.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple next-hop IP addresses are configured, the device redirects packets in active/standby mode. A maximum of four next-hop IP addresses can be configured in a traffic behavior. The device determines the primary and backup paths according to the sequence in which next-hop IP addresses are configured. The next-hop IP address that is configured first has the highest priority and this next hop is used as the primary path. Other next hops are used as backup paths. When the primary link becomes Down, a next hop with a higher priority is used as the primary link.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to a next-hop IP address.

Precautions

- In a traffic behavior, the **redirect ip-nexthop** command cannot be used together with any of the following commands: **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id** and **remark vlan-id**.
- A traffic policy containing the redirection action can be applied globally, as well as on an interface and in a VLAN in the inbound direction.
- If no ARP entry matches the next-hop address on the device, the device triggers ARP learning. If the ARP entry cannot be learned, redirection does not take effect and packets are forwarded along the original path.
- In V200R021C00SPC600 and later versions, when the action of redirecting packets to a remote next hop, the configuration does not take effect if the next-hop address is reachable only through tunnel forwarding.

Example

Configure the action of redirecting packets to next hop 10.0.0.1 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect ip-nexthop 10.0.0.1
```

7.11.4 redirect ipv6-multihop

Function

The **redirect ipv6-multihop** command configures an action of redirecting packets to multiple next hop IPv6 addresses in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to multiple next hop IPv6 addresses is not configured in a traffic behavior.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

redirect [**vpn-instance** *vpn-instance-name*] **ipv6-multihop** { *ipv6-address* \| **link-local** *link-local-address* **interface** *interface-type interface-number* } & <2-4>

redirect [**vpn-instance** *vpn-instance-name*] **ipv6-multihop** *acl6-ip-pool-name*

undo redirect

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ipv6-address	Specifies a next hop IPv6 address.	The address is a 32-digit hexadecimal number, in X:X:X:X:X:X:X:X format.
link-local *link-local-address*	Specifies a link-local address. The prefix of the specified IPv6 address must match FE80::/10.	The address is a 32-digit hexadecimal number, in X:X:X:X:X:X:X:X format.
interface *interface-type interface-number*	Specifies the interface corresponding to the link-local address. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
acl6-ip-pool-name	Specifies the name of the ACL IPv6 address pool to be created.	The value is a string of 1 to 32 case-sensitive characters without spaces and starting with a letter.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple next hop IPv6 addresses are specified, the device redirects packets through equal-cost routes in load balancing mode.

If the outbound interface corresponding to a next hop IPv6 address becomes Down or a route changes, the device switches traffic to the outbound interface corresponding to an available next hop. If the specified next hops are unavailable, the device forwards the packets to the original destination.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to multihop IPv6 addresses.

Precautions

- In a traffic behavior, the **redirect ipv6-multithop** command cannot be used together with any of the following commands: **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id** and **remark vlan-id**.
- When the next hop IPv6 address is a local-link address, you must configure a VLANIF interface. The address is only valid in the VLAN corresponding to the VLANIF interface.
- The traffic policy that contains the redirection action can only be applied to the system, an interface, or a VLAN.
- When running the **redirect ipv6-multithop** command to configure multiple next hop IPv6 addresses, you can specify 2 to 4 next hop IPv6 addresses. When configuring multiple next hop IPv6 addresses through an ACL IPv6-POOL, you can specify a maximum of 64 next hop IPv6 addresses. To create and configure an ACL IPv6-POOL, run the **acl ipv6 ip-pool** and **ipv6 address (ACL IPv6-POOL view)** commands.
- If the device does not match the neighbor entry corresponding to the next hop IPv6 address, the device sends NS packets to check whether the neighbor

is reachable. If the neighbor is unreachable, packets are forwarded based on the original path and redirection does not take effect.

- If you run the **redirect ipv6-multithop** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure two next hop IPv6 addresses in the traffic behavior **b1**: FC00:0:0:2000::1 and FC00:0:0:3000::1.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect ipv6-multihop fc00:0:0:2000::1 fc00:0:0:3000::1
```

In the traffic behavior **b2**, configure an action of redirecting packets to five next hop IPv6 addresses in the ACL IPv6-POOL **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 ip-pool abc
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::1 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::2 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::3 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::4 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::5 128
[HUAWEI-acl6-ip-pool-abc] quit
[HUAWEI] traffic behavior b2
[HUAWEI-behavior-b2] redirect ipv6-multihop abc
```

7.11.5 redirect ipv6-nexthop

Function

The **redirect ipv6-nexthop** command configures the action of redirecting packets to a next-hop IPv6 address in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, the action of redirecting packets to a next-hop IPv6 address is not configured in a traffic behavior.

Format

redirect [**remote**] [**vpn-instance** *vpn-instance-name*] **ipv6-nexthop** { *ipv6-address* | **link-local** *link-local-address* **interface** *interface-type interface-number* } & <1-4> [**forced**]

undo redirect

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **vpn-instance** *vpn-instance-name* parameter.

Parameters

Parameter	Description	Value
remote	Redirects packets to a remote next hop.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ipv6-address	Specifies a next-hop IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
link-local *link-local-address*	Specifies a link-local IPv6 address. The prefix of the specified IPv6 address must match FE80::/10.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the interface corresponding to the link-local address. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
forced	Indicates that packets are discarded if the next hop is unavailable.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the action of redirecting packets to a specified next-hop IPv6 address in a traffic behavior to implement PBR.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the action of redirecting packets to a next-hop IPv6 address.

Precautions

- In a traffic behavior, the **redirect ipv6-nexthop** command cannot be used together with any of the following commands: **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id** and **remark vlan-id**.
- If no neighbor entry matches the next-hop IPv6 address, the device sends NS packets to check whether the neighbor is reachable. If the neighbor is unreachable, redirection does not take effect and packets are forwarded along the original path.
- If multiple next-hop IPv6 addresses are configured, the device redirects packets in active/standby mode. A maximum of four next-hop IPv6 addresses can be configured in a traffic behavior. The device determines the primary and backup paths according to the sequence in which next-hop IPv6 addresses are configured. The next-hop IPv6 address that is configured first has the highest priority and this next hop is used as the primary path. Other next hops are used as backup paths. When the primary link becomes Down, a next hop with a higher priority is used as the primary link.
- When the next-hop IPv6 address is a local-link address, you must configure a VLANIF interface. The address is valid only in the VLAN corresponding to the VLANIF interface.
- If you run the **redirect ipv6-nexthop** command in the same traffic classifier view multiple times, only the latest configuration takes effect.
- In V200R021C00SPC600 and later versions, when the action of redirecting packets to a remote next hop, the configuration does not take effect if the next-hop address is reachable only through tunnel forwarding.

Example

Configure the action of redirecting packets to the next-hop IPv6 address FC00:0:0:2001::1 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect ipv6-nexthop fc00:0:0:2001::1
```

7.12 Route Monitoring Group Configuration Commands

7.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

7.12.2 display ip route-monitor-group

Function

The **display ip route-monitor-group** command displays information about a route monitoring group or all route monitoring groups.

Format

display ip route-monitor-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays information about a specified route monitoring group. If *group-name* is specified, detailed information about the specified route monitoring group is displayed. If *group-name* is not specified, a summary of all route monitoring groups is displayed.	The value is a string of 1 to 31 case-sensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a route monitoring group is configured, you can run the **display ip route-monitor-group** command to check information about the route monitoring group, such as the status and information about routes in the route monitoring group.

Example

Display brief information about all route monitoring groups.

```
<HUAWEI> display ip route-monitor-group
 Route monitor group number : 1
 Route monitor group              State
 uplink                           Enable
```

Display detailed information about the route monitoring group **uplink**.

```
<HUAWEI> display ip route-monitor-group uplink
route monitor group uplink
 State         : Enabled
-------------------------------------------------------
 route monitor group tracking route number : 1
-------------------------------------------------------
```

```
VPN name      : Public
Destination  : 10.2.2.2
Mask          : 255.255.255.255
State         : Inactive
```

Table 7-236 Description of the **display ip route-monitor-group** command output

Item	Description
Route monitor group number	Number of route monitor groups.
Route monitor group	Name of a route monitoring group.
State	Status of a route monitoring group: ● Enabled: The route monitoring group is enabled. ● Disabled: The route monitoring group is disabled. ● Up: The route monitoring group is Up. ● Down: The route monitoring group is Down. You can run the **monitor enable** command to enable a route monitoring group.
route monitor group tracking route number	Number of routes in a route monitoring group.
VPN name	VPN instance to which routes belongs. The value **Public** indicates a public network.
Destination	Destination IP address of a route.
Mask	Mask of the destination IP address of a route.
State	Status of a route: ● Active ● Inactive

7.12.3 display ip route-monitor-group track-route

Function

The **display ip route-monitor-group track-route** command displays information about all route monitoring groups to which a specified route is added.

Format

display ip route-monitor-group track-route [**vpn-instance** *vpn-instance-name*] *dest-address* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which a route belongs. If this parameter is specified, information about all route monitoring groups to which a VPN route in the VPN instance is added is displayed. If this parameter is not specified, information about all route monitoring groups to which a public network route is added is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
dest-address	Specifies the destination IP address of a route.	The value is in dotted decimal notation.
mask	Specifies the mask of the destination IP address of a route.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address of a route.	The value is an integer in the range from 0 to 32.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A route can be added to multiple route monitoring groups to monitor the route status change. You can run the **display ip route-monitor-group track-route** command to display information about all route monitoring groups to which a specified route is added.

Example

Display information about all route monitoring groups to which the route to 192.168.1.0/24 is added.

```
<HUAWEI> display ip route-monitor-group track-route 192.168.1.0 24
 Route monitor group              State
 uplink                           Enabled
```

Table 7-237 Description of the **display ip route-monitor-group track-route** command output

Item	Description
Route monitor group	Name of a route monitoring group.
State	Status of a route monitoring group: - Enabled: The route monitoring group is enabled. - Disabled: The route monitoring group is disabled. - Up: The route monitoring group is Up. - Down: The route monitoring group is Down. You can run the **monitor enable** command to enable a route monitoring group.

7.12.4 ip route-monitor-group

Function

The **ip route-monitor-group** command creates a route monitoring group and displays the view of this route monitoring group, or displays the view of an existing route monitoring group.

The **undo ip route-monitor-group** command deletes a route monitoring group.

By default, no route monitoring group is created on a switch.

Format

ip route-monitor-group *group-name*

undo ip route-monitor-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a route monitoring group.	The value is a string of 1 to 31 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All network-side routes of the same type can be added to the same route monitoring group, which monitors a certain number of routes. In a hot standby scenario, you can add network-side routes to a route monitoring group and associate access-side service modules with it so that the service modules can perform active/standby link switchovers upon route changes in the group. This mechanism prevents network congestion and packet loss.

Follow-up Procedure

Run the **track ip route** command to add a route to the route monitoring group.

Example

Create a route monitoring group named **uplink**.

```
<HUAWEI> system-view
[HUAWEI] ip route-monitor-group uplink
[HUAWEI-route-monitor-group-uplink]
```

7.12.5 monitor enable

Function

The **monitor enable** command enables a route monitoring group.

The **undo monitor enable** command disables a route monitoring group.

By default, a route monitoring group is disabled.

Format

monitor enable

undo monitor enable

Parameters

None

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A route monitoring group can monitor status changes of network-side routes. After the routes to be monitored are added to a route monitoring group, run the

monitor enable command to enable the route monitoring group so that it can take effect immediately.

When a large number of routes are being added to or deleted from a route monitoring group, the status of the route monitoring group changes frequently, which in turn leads to service flapping of the service modules associated with the route monitoring group. To prevent such service flapping, run the **undo monitor enable** command to disable the route monitoring group so that it is dissociated from all service modules. After the routes are added or deleted, run the **monitor enable** command to re-associate the route monitoring group with all service modules.

Prerequisites

A route has been added to the route monitoring group using the **track ip route** command.

Example

Enable the route monitoring group **uplink**.

```
<HUAWEI> system-view
[HUAWEI] ip route-monitor-group uplink
[HUAWEI-route-monitor-group-uplink] track ip route 10.1.1.0 24
[HUAWEI-route-monitor-group-uplink] monitor enable
```

7.12.6 operator and

Function

The **operator and** command sets the status of routes in a route monitoring group to be of the AND relationship.

The **undo operator and** command restores the default configuration.

By default, the status of routes in a route monitoring group is of the OR relationship.

Format

operator and

undo operator and

Parameters

None

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

You can run the **operator and** command to set the status of routes in a route monitoring group to be of the AND relationship. That is, the status of the route monitoring group is Up only when all routes in the route monitoring group are Up. The status of the monitoring group is Down as long as one route in the group is Down. By default, the status of routes in a route monitoring group is of the OR relationship. That is, the status of the route monitoring group is Up as long as one route in the group is Up. The status of the monitoring group is Down only when all routes in the group are Down.

Example

Set the status of routes in a route monitoring group to be of the AND relationship.

```
<HUAWEI> system-view
[HUAWEI] ip route-monitor-group uplink
[HUAWEI-route-monitor-group-uplink] operator and
```

7.12.7 trigger-down-delay

Function

The **trigger-down-delay** command configures a delay after which the route management (RM) module instructs the associated service modules to perform link switchovers.

The **undo trigger-down-delay** command restores the default configuration.

By default, the delay is 0s.

Format

trigger-down-delay *delay-value*

undo trigger-down-delay [*delay-value*]

Parameters

Parameter	Description	Value
delay-value	Specifies a delay after which the RM module instructs the associated service modules to perform link switchovers.	The value is an integer in the range from 0 to 1000, in seconds.

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

In a hot standby scenario, service modules can be associated with a route monitoring group to trigger link switchovers. When the status of the route monitoring group goes Down, the RM module instructs the associated service modules to perform link switchovers. In addition, the RM module re-delivers routes to the forwarding table and establishes forwarding entries for the routes, which takes some time. Packet loss may occur if the RM module instructs the associated service modules to perform link switchovers immediately. To resolve this problem, run the **trigger-down-delay** command to configure a delay after which the RM module instructs the associated service modules to perform link switchovers.

Example

Set the delay to 10s after which the RM module instructs the associated service modules to perform link switchovers.

```
<HUAWEI> system-view
[HUAWEI] ip route-monitor-group uplink
[HUAWEI-route-monitor-group-uplink] trigger-down-delay 10
```

7.12.8 trigger-up-delay

Function

The **trigger-up-delay** command configures a delay after which the RM module instructs the associated service modules to perform link switchbacks.

The **undo trigger-up-delay** command restores the default configuration.

By default, the delay is 5s.

Format

trigger-up-delay *delay-value*

undo trigger-up-delay

Parameters

Parameter	Description	Value
delay-value	Specifies a delay after which the RM module instructs the associated service modules to perform link switchbacks.	The value is an integer in the range from 0 to 1000, in seconds.

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

In a hot standby scenario, service modules can be associated with a route monitoring group to trigger link switchovers. When the status of the route monitoring group goes Up, the RM module instructs the associated service modules to perform link switchbacks. In addition, the RM module re-delivers routes to the forwarding table and establishes forwarding entries for the routes, which takes some time. Packet loss may occur if the RM module instructs the associated service modules to perform link switchovers immediately. To resolve this problem, run the **trigger-up-delay** command to configure a delay after which the RM module instructs the associated service modules to perform link switchbacks.

Example

Set the delay to 10s after which the RM module instructs the associated service modules to perform link switchbacks.

```
<HUAWEI> system-view
[HUAWEI] ip route-monitor-group uplink
[HUAWEI-route-monitor-group-uplink] trigger-up-delay 10
```

7.12.9 track ip route

Function

The **track ip route** command adds a route to a route monitoring group.

The **undo track ip route** command deletes a route from a route monitoring group.

By default, no route is added to a route monitoring group.

Format

track ip route [**vpn-instance** *vpn-instance-name*] *dest-address* { *mask* | *mask-length* }

undo track ip route [**vpn-instance** *vpn-instance-name*] *dest-address* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which a route belongs. If this parameter is specified, a VPN route in the VPN instance is added to the route monitoring group. If this parameter is not specified, a public network route is added to the route monitoring group.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
dest-address	Specifies the destination IP address of a route.	The value is in dotted decimal notation.
mask	Specifies the mask of the destination IP address of a route.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address of a route.	The value is an integer in the range from 0 to 32.

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A route monitoring group can monitor the status of its member routes to prevent network congestion and packet loss. You can run the **track ip route** command to add a route to be monitored to a route monitoring group. All network-side routes of the same type can be added to the same route monitoring group.

Follow-up Procedure

Run the **monitor enable** command to enable the route monitoring group.

Precautions

A maximum of 16 routes can be added to a route monitoring group. A route can be added to multiple route monitoring groups.

Example

Add the route to 10.1.1.0/24 to the route monitoring group **uplink**.

```
<HUAWEI> system-view
[HUAWEI] ip route-monitor-group uplink
[HUAWEI-route-monitor-group-uplink] track ip route 10.1.1.0 24
```

8 IP Multicast Commands

8.1 IGMP Configuration Commands

8.1.1 Command Support

Product	Support
S1700	Not supported.

Product	Support
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the IGMP multi-instance feature.

8.1.2 display default-parameter igmp

Function

The **display default-parameter igmp** command displays default IGMP configurations.

Format

display default-parameter igmp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays default IGMP parameter settings even if IGMP parameters have been modified. Therefore, you can use this command to check which parameters have been modified.

Example

Display default IGMP configurations.

```
<HUAWEI> display default-parameter igmp
  IGMP View Default Configurations:
```

```
---------------------------------
Lastmember-queryinterval: 1 s
Max-response-time: 10 s
Require-router-alert: disabled
Robust-count: 2
Send-router-alert: enabled
Ssm-mapping: disabled
Timer other-querier-present: 125 s
Timer query: 60 s

Interface View Default Configurations:
--------------------------------------
Group-policy: disabled
Lastmember-queryinterval: 1 s
Lastmember-query time: 2 s
Max-response-time: 10 s
Other-querier-present-timer-expiry: off
Prompt-leave: disabled
Require-router-alert: disabled
Robust-count: 2
Send-router-alert: enabled
Ssm-mapping: disabled
Startup-query-timer-expiry: off
Static-group: disabled
Timer other-querier-present: 125 s
Timer query: 60 s
Version: 2
Ip-source-policy: disabled
```

Table 8-1 Description of the **display default-parameter igmp** command output

Item	Description
IGMP View Default Configurations	Default configurations in the IGMP view. The default configurations take effect globally.
Lastmember-queryinterval	Interval for sending IGMP Group-Specific Query messages. This parameter is configured using the **lastmember-queryinterval (IGMP view)** command in the IGMP view or the **igmp lastmember-queryinterval** command in the interface view.
Max-response-time	Maximum response time for IGMP Query messages. This parameter is configured using the **max-response-time (IGMP view)** command in the IGMP view or the **igmp max-response-time** command in the interface view.
Require-router-alert	Whether the device checks for the Router-Alert option in the received IGMP message. This parameter is configured using the **require-router-alert (IGMP view)** command in the IGMP view or the **igmp require-router-alert** command in the interface view.
Robust-count	Robustness variable of an IGMP querier. This parameter is configured using the **robust-count (IGMP view)** command in the IGMP view or the **igmp robust-count** command in the interface view.

Item	Description
Send-router-alert	Whether the IGMP messages sent from the device carry the Router-Alert option. This parameter is configured using the **send-router-alert (IGMP view)** command in the IGMP view or the **igmp send-router-alert** command.
Ssm-mapping	Status of the SSM mapping function. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. SSM mapping can be configured using the **igmp ssm-mapping enable** command.
Timer other-querier-present	Length of the other querier present timer. This parameter is configured using the **timer other-querier-present (IGMP view)** command in the IGMP view or the **igmp timer other-querier-present** command in the interface view.
Timer query	Interval for sending IGMP General Query messages. This parameter is configured using the **timer query (IGMP view)** command in the IGMP view or the **igmp timer query** command in the interface view.
Interface View Default Configurations	Default configurations in the interface view. The configurations take effect only for IGMP-enabled interfaces.
Group-policy	Whether a multicast group policy is configured. The value can be: ● enabled: A multicast group policy is configured. ● disabled: No multicast group policy is configured. A multicast group policy is configured using the **igmp group-policy** command.
Lastmember-query time	Last member query time, calculated using the following formula: Last member query time = Last member query interval x Robustness variable The last member query time is not defined in IGMPv1.

Item	Description
Other-querier-present-timer-expiry	Status of the other querier present timer: ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
Prompt-leave	Status of the fast leave function. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. This function is configured using the **igmp prompt-leave** command.
Startup-query-timer-expiry	Startup query interval of the querier. The interface sends Query messages at this interval when it starts to function as a querier. The value is expressed in seconds and is 1/4 of the query interval (Timer query). The value **off** indicates that the interface has not started to send Query messages as a querier. The startup query timer is enabled only when the interface starts as a querier.
Static-group	Whether static multicast groups are configured. The value can be: ● enabled: Static multicast groups are configured. ● disabled: No static multicast groups are configured. A static multicast group is configured using the **igmp static-group** command.
Version	IGMP version number. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3, which is configured using the **igmp version** command.
Ip-source-policy	Status of IGMP Report/Leave message filtering based on host addresses. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. This function is configured using the **igmp ip-source-policy** command.

8.1.3 display igmp control-message counters

Function

The **display igmp control-message counters** command displays statistics about IGMP control messages.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IGMP message statistics in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays IGMP message statistics in all instances.	-
interface *interface-type interface-number*	Displays IGMP message statistics on a specified interface. If this parameter is not specified, the command displays IGMP message statistics on all interfaces.	-
message-type	Indicates the IGMP message type. If this parameter is not specified, the command displays statistics about all types of IGMP messages.	-
query	Displays statistics about Query messages received by the interface. Query messages are sent from a querier.	-
report	Displays statistics about Report messages received by the interface. Report messages are sent by hosts to join a multicast group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the number of IGMP control messages sent and received on the device.

Example

Display statistics about the IGMP messages sent and received by VLANIF100.

```
<HUAWEI> display igmp control-message counters interface vlanif 100
Interface message counter information
 Vlanif100(192.168.2.1):
 Message Type              Sent       Valid      Invalid    Ignore
 -----------------------------------------------------------------
 General Query             1144       638186     0          0
 Group Query               0          0          0          0
 Source Group Query          0          0          0          0
 -----------------------------------------------------------------
 IGMPV1V2
 Report ASM                0          0          0          0
 Report SSM                0          0          0          0
 -----------------------------------------------------------------
 LEAVE ASM                 0          0          0          0
 LEAVE SSM                 0          0          0          0
 -----------------------------------------------------------------
 IGMPV3
 ISIN Report               0          0          0          0
 ISEX Report               0          0          0          0
 TOIN Report               0          0          0          0
 TOEX Report               0          0          0          0
 ALLOW Report              0          0          0          0
 BLOCK Report              0          0          0          0
 Source Records Total      0          0          0          0
 -----------------------------------------------------------------
 Others                    -          -          0          0
 -----------------------------------------------------------------
```

Table 8-2 Description of the **display igmp control-message counters interface vlanif 100** command output

Item	Description
Interface message counter information	IGMP packet information on an interface.
Vlanif100(192.168.2.1)	Type, number, and IP address of the interface.
Message Type	Type of IGMP messages.
Sent	Number of IGMP messages sent from the interface.
Valid	Number of valid IGMP messages received by the interface.
Invalid	Number of wrong IGMP messages received by the interface.
Ignore	Number of received IGMP messages ignored by the interface.
General Query	Number of IGMP General Query messages.

Item	Description
Group Query	Number of IGMP Group-Specific Query messages.
Source Group Query	Number of IGMP Group-and-Source-Specific Query messages.
Report ASM	Number of IGMPv1 and IGMPv2 Report messages with multicast group addresses in the ASM group address range.
Report SSM	Number of IGMPv1 and IGMPv2 Report messages with multicast group addresses in the SSM group address range.
LEAVE ASM	Number of IGMPv2 Leave messages with multicast group addresses in the ASM group address range.
LEAVE SSM	Number of IGMPv2 Leave messages with multicast group addresses in the SSM group address range.
ISIN Report	Number of IGMPv3 IS_IN Report messages.
ISEX Report	Number of IGMPv3 IS_EX Report messages.
TOIN Report	Number of IGMPv3 TO_IN Report messages.
TOEX Report	Number of IGMPv3 TO_EX Report messages.
ALLOW Report	Number of IGMPv3 ALLOW Report messages.
BLOCK Report	Number of IGMPv3 BLOCK Report messages.
Source Records Total	Number of multicast sources carried in IGMPv3 messages.
Others	Number of invalid and ignored IGMP messages of unknown types.

8.1.4 display igmp explicit-tracking

Function

The **display igmp explicit-tracking** command displays explicit (S, G) entries of IGMPv3 hosts, that is, (S, G) entries that IGMPv3 hosts have joined in Include mode.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **explicit-tracking** [**interface** *interface-type interface-number* [**host-address** *host-address* | **group** *group-address* **source** *source-address*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode in all instances.	-
interface *interface-type interface-number*	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode on a specified interface.	-
host-address *host-address*	Specifies the address of an IGMP host.	The address is in dotted decimal notation.
group *group-address*	Specifies the address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source *source-address*	Specifies the address of a multicast source.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view information about IGMPv3 hosts that have dynamically joined specified sources/groups in Include mode.

Example

Display information about the IGMPv3 hosts that have joined specified source/group in Include mode.

```
<HUAWEI> display igmp explicit-tracking
Explicit-tracking information
 Total 1 host, 2 entries

 Vlanif100(192.168.0.12)
  0001.Host: 192.168.0.28
       Uptime: 00:02:47
```

```
    Expires: 00:01:33
    (S, G) List:
      Group: 232.1.1.1
          Source: 10.12.12.12
            Uptime: 00:02:47
            Time since last refresh: 00:02:47
          Source: 10.13.13.13
            Uptime: 00:02:47
            Time since last refresh: 00:02:47
```

Table 8-3 Description of the **display igmp explicit-tracking** command output

Item	Description
Explicit-tracking information	IGMP host information.
Total 1 host, 2 entries	There is one IGMP host and two (S, G) entries.
Vlanif100(192.168.0.12)	Interface connected to IGMPv3 hosts that have joined a group with source addresses specified in Include mode.
Host	IGMP host address.
Uptime	Running time since an IGMP host joins a multicast group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Amount of time left before an IGMP host times out. After the IGMP host expires, it is deleted from the IGMP member host list. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
(S, G) List	List of multicast sources and groups an IGMP host has joined.
Group	Multicast group address.
Source	Multicast source address.

Item	Description
Time since last refresh	Amount of time since an IGMP host last joins a group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.

8.1.5 display igmp group

Function

The **display igmp group** command displays information about IGMP groups that hosts have dynamically joined by sending IGMP Report messages.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP groups in a VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP groups in all instances.	-
group-address	Displays information about the IGMP group with a specified group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about the IGMP group on the specified interface.	-

Parameter	Description	Value
verbose	Displays detailed information about IGMP groups. If the parameter is not specified, the command displays only the summary of IGMP groups.	-
entry-number	Displays statistics about IGMP multicast groups that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a host wants to receive multicast data for a multicast group, the host must join the multicast group in either of the following modes:

- Dynamic mode: After you run the **igmp enable** command to enable IGMP on the interface connected to the network segment on which the host resides, the host can dynamically join the multicast group.
- Static mode: After you run the **igmp static-group** command to enable IGMP on the interface connected to the network segment on which the host resides, the host can statically join the multicast group.

To monitor the status of the multicast group or locate a fault in a dynamically joined multicast group, run the **display igmp group** command. This command displays information about the multicast group that hosts have dynamically joined.

Example

Display information about dynamic IGMP groups.

```
<HUAWEI> display igmp group
Interface group report information of VPN-Instance: public net
 Vlanif100(10.1.6.2):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.2       10.1.6.10       00:02:04    00:01:17
```

Display detailed information about dynamic IGMP groups.

```
<HUAWEI> display igmp group verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(10.1.6.2):
  Total entry on this interface: 1
  Limited entry on this interface: -
```

```
 Total 1 IGMP Group reported
  Group: 225.1.1.2
    Uptime: 00:03:59
    Expires: off
    Last reporter: 10.1.6.10
    Last-member-query-counter: 0
    Last-member-query-timer-expiry: off
    Group mode: include
    Version1-host-present-timer-expiry: off
    Version2-host-present-timer-expiry: off
    Source list:
      Source: 192.168.232.1
         Uptime: 00:51:07
         Expires: 00:02:05
         Last-member-query-counter: 0
         Last-member-query-timer-expiry: off
```

Display statistics about IGMP multicast groups that hosts dynamically join.

```
<HUAWEI> display igmp group entry-number
Interface group report information of VPN-Instance: public net
  Total 4 IGMP Groups reported
 Vlanif200(10.36.1.10):
  Total 2 IGMP Groups reported
 Vlanif100(10.0.0.4):
  Total 2 IGMP Groups reported
```

Table 8-4 Description of the **display igmp group command** output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong. **public net** indicates the public network instance.
Group Address	Address of a multicast group.
Last Reporter	Link-local address of the last host that sends a Multicast Listener Report message. **NOTE** When a host joins a multicast group through a sub-interface for QinQ or Dot1q VLAN tag termination, the Last Reporter field displays the address of the multicast proxy. By default, the address of the multicast proxy is 192.168.0.1.
Limited entry of this VPN-Instance	Maximum number of IGMP entries that can be created for this instance.
Vlanif100(10.1.6.2)	Interface type and interface number (IP address).
Total entry on this interface	Total number of IGMP entries on the current interface.
Limited entry on this interface	Maximum number of IGMP entries that the current interface can create.
Total 1 IGMP Group reported	Number of IGMP groups that the current interface has dynamically joined.

Item	Description
Group	Address of a multicast group.
Uptime	Amount of time since a multicast group is created. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Time left before a group will be deleted from the IGMP group table. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days. "off" indicates that the group will never be aged out.
Last-member-query-counter	Number of times the querier will send Group-Specific Query messages after receiving a Leave message. The counter value decreases by 1 every time the querier sends a Group-Specific Query message. This parameter is configured using the **igmp robust-count** command. The value 0 indicates that the querier does not send Group-Specific Query messages after receiving a Leave message.
Last-member-query-timer-expiry	Length of the last member query timer. The timer starts only when a Leave message is received from a group member. The timer value is configured using the **igmp lastmember-queryinterval** command. The value **off** indicates that the last member query timer has not started.

Item	Description
Group mode	Multicast group record type, which can be Include or Exclude. It is displayed only when the interface is running IGMPv3.
Version1-host-present-timer-expiry	Timeout interval of IGMPv1 hosts. IGMPv1 does not define the Leave message; therefore, memberships of IGMPv1 hosts are aged using a timer. The device starts the timer when receiving a Report message from an IGMPv1 host. The timer value is calculated using the following formula: IGMPv1 timeout interval = General group query interval x Robustness variable + Maximum response time for Query messages The general group query interval is configured using the **igmp timer query** command. The robustness variable is configured using the **igmp robust-count** command. The maximum response time for Query messages is configured using the **igmp max-response-time** command. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.
Version2-host-present-timer-expiry	Timeout interval of IGMPv2 hosts. It is displayed only when the interface is running IGMPv3. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.
Source list	List of multicast sources. It is displayed only when the interface has IGMPv3 receiver hosts attached.
Source	IP address of a multicast source.

8.1.6 display igmp group ssm-mapping

Function

The **display igmp group ssm-mapping** command displays information about multicast group entries established with SSM mapping.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays group entries established with SSM mapping in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays group entries established with SSM mapping in all instances.	-
group-address	Displays information about the specified multicast group entries established with SSM mapping. If this parameter is not specified, the command displays information about all multicast group entries established with SSM mapping.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about multicast group entries established with SSM mapping on the specified interface. If this parameter is not specified, the command displays information about multicast group entries established with SSM mapping on all interfaces.	-
verbose	Displays detailed information about group membership established with SSM mapping. If the parameter is not specified, the command displays only the summary of group membership established with SSM mapping.	-
entry-number	Displays statistics about IGMP multicast groups established with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display igmp group ssm-mapping** command to view information about multicast group entries that are established with SSM mapping. SSM mapping entries are configured using the **ssm-mapping** command.

Example

Display summary of all multicast group entries established with SSM mapping.

```
<HUAWEI> display igmp group ssm-mapping

IGMP SSM mapping interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(192.168.101.1):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.0.0.1       192.168.101.2   00:00:02    00:02:08
```

Display detailed information about all multicast group entries established with SSM mapping.

```
<HUAWEI> display igmp group ssm-mapping verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(192.168.101.1):
  Total entry on this interface: 1
  Limited entries on this interface: -
  Total 1 IGMP SSM-Mapping Group reported
   Group: 232.0.0.1
     Uptime: 00:00:15
     Expires: 00:01:55
     Last reporter: 192.168.101.2
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: off
     Version2-host-present-timer-expiry: 00:01:55
```

Display detailed information about IGMP multicast groups established with SSM mapping.

```
<HUAWEI> display igmp group ssm-mapping entry-number
Interface group report information of VPN-Instance: public net
  Total 4 IGMP SSM-Mapping Groups reported
 Vlanif200(10.36.1.10):
  Total 2 IGMP SSM-Mapping Groups reported
 Vlanif100(10.0.0.4):
  Total 2 IGMP SSM-Mapping Groups reported
```

Table 8-5 Description of the **display igmp group ssm-mapping** command output

Item	Description
IGMP SSM mapping interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong. **public net** indicates the public network instance.

Item	Description
Group Address	Group address.
Last Reporter	Link-local address of the last host that sends a Multicast Listener Report message.
Limited entry of this VPN-Instance	Maximum number of entries that can be generated in the VPN instance.
Vlanif100(192.168.101.1)	Interface type and interface number (IP address).
Interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong.
Total entry on this interface	Total number of entries generated on the interface.
Limited entries on this interface	Maximum number of entries that can be generated on the interface.
Total 1 IGMP SSM-Mapping Group reported	Number of IGMP Report messages with SSM group addresses received on the interface.
Group	Group address.
Uptime	Amount of time since the last Report message is received. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Timeout period of a group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Last-member-query-counter	Number of times Group-Specific Query messages are sent.

Item	Description
Last-member-query-timer-expiry	Length of the last member query timer. The timer starts only when a Leave message is received from a group member. The timer value is configured using the **igmp lastmember-queryinterval** command. The value **off** indicates that the last member query timer has not started.
Group mode	Filter mode of a group, which can be Include or Exclude. It is displayed only when the interface is running IGMPv3.
Version1-host-present-timer-expiry	Timeout interval of IGMPv1 hosts. IGMPv1 does not define the Leave message; therefore, memberships of IGMPv1 hosts are aged using a timer. The device starts the timer when receiving a Report message from an IGMPv1 host. The timer value is calculated using the following formula: IGMPv1 timeout interval = General group query interval x Robustness variable + Maximum response time for Query messages The general group query interval is configured using the **igmp timer query** command. The robustness variable is configured using the **igmp robust-count** command. The maximum response time for Query messages is configured using the **igmp max-response-time** command. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.
Version2-host-present-timer-expiry	Timeout interval of IGMPv2 hosts. It is displayed only when the interface is running IGMPv3. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.

8.1.7 display igmp group static

Function

The **display igmp group static** command displays information about static IGMP entries.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static** [**up** | **down**] [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **static** [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static interface-number**

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group static interface** *interface-type interface-number* **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about static IGMP entries in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about static IGMP entries in all instances.	-
group-address	Displays information about static IGMP entries of a specified group. If this parameter is not specified, the command displays static IGMP entries of all groups.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
up | **down**	Displays information about interfaces in Up or Down state. If this parameter is not specified, the command displays all interfaces in IGMP entries.	-
verbose	Displays detailed interface list in a static IGMP group. If the parameter is not specified, the command displays only summary of static IGMP entries.	-
interface-number	Displays the number of interfaces in a static IGMP group.	-
interface *interface-type interface-number*	Displays information about the static IGMP groups on a specified interface. *interface-type interface-number* specifies the type and number of an interface.	-

Parameter	Description	Value
entry-number	Displays the number of static IGMP groups on an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about static IGMP entries configured using the **igmp static-group** command.

Example

Display information about all static IGMP entries.

```
<HUAWEI> display igmp group static
Static join group information
 Total 2 entries, Total 2 active entries
  Group Address   Source Address  Interface         State     Expires
  225.1.1.1       10.1.1.1        Vlanif10          UP        never
  225.1.1.2       10.1.1.1        Vlanif20          UP        never
```

Table 8-6 Description of the **display igmp group static** command output

Item	Description
Static join group information	information about static IGMP groups.
Total 2 entries, Total 2 active entries	Number of static IGMP entries and active IGMP entries on the interface.
Group Address	Multicast group address.
Source Address	Multicast source address.
Interface	Interface type and number.
State	Status of an interface, which can be: ● UP: The interface is operating normally. ● DOWN: An error occurs on the physical link of the interface.
Expires	Amount of time left before a group entry times out. If this field displays **never**, the corresponding multicast group is a static group and will never age out.

Display detailed information about static IGMP entries.

```
<HUAWEI> display igmp group static verbose
Static join group information
 Total 2 entries
  00001.(*, 225.1.1.1)
      Total List of 1 joined interface
      1.Vlanif10
          State:            UP
          Reference Count:   1
          Multicast Boundary:NO
          Outgoing Interface:YES
  00002.(*, 225.1.1.2)
      Total List of 1 joined interface
      1.Vlanif20
          State:            UP
          Reference Count:   1
          Multicast Boundary:NO
          Outgoing Interface:YES
```

Table 8-7 Description of the display igmp group static verbose command output

Item	Description
Static join group information	information about static IGMP groups.
Total 2 entries	Number of static IGMP entries on the interface.
00001.(*, 225.1.1.1)	(*, G) entry ID.
Total List of 1 joined interface	Downstream interface list of the (*, G) entry.
1.Vlanif10	Interface type and interface number.
State	Status of an interface, which can be: ● UP: The interface is operating normally. ● DOWN: An error occurs on the physical link of the interface.
Reference Count	Number of the IGMP entry on the current interface is referenced.
Multicast Boundary	Whether the multicast forwarding boundary is configured: ● YES ● NO This function is configured using the **multicast boundary** *group-address* { *mask* | *mask-length* } command.
Outgoing Interface	Whether downstream interfaces exist: ● YES ● NO

Display lists of Up interfaces in static IGMP entries.

```
<HUAWEI> display igmp group static up
Static join group information
 Total 4 entries
  00001.(*,225.1.1.1)
      Total List of 2 joined interfaces
      Total Matched 2 interfaces
      1.Vlanif10
      2.Vlanif20
  00002.(*,225.1.1.2)
      Total List of 2 joined interfaces
      Total Matched 2 interfaces
      1.Vlanif10
      2.Vlanif20
```

Table 8-8 Description of the display igmp group static up command output

Item	Description
Total List of 2 joined interfaces	Number of interfaces in a static group.
Total Matched 2 interfaces	List of Up interfaces in a static group.

Display information about IGMP groups statically configured on VLANIF100.

```
<HUAWEI> display igmp group interface vlanif 100 static
Static join group information
 Total 2 entries
 Specified interface state:UP
 Total 2 entries matched
   Group Address   Source Address  Expires
   226.0.0.1       10.0.5.120      never
   226.0.0.2       0.0.0.0         never
```

Table 8-9 Description of the display igmp group interface vlanif 100 static command output

Item	Description
Static join group information	information about static IGMP groups.
Total 2 entries	Number of static IGMP entries on the interface.
Specified interface state	Status of an interface, which can be: ● UP: The interface is operating normally. ● DOWN: An error occurs on the physical link of the interface.
Total 2 entries matched	Number of IGMP groups that meet the query conditions.
Group Address	Multicast group address.
Source Address	Multicast source address.

Item	Description
Expires	Amount of time left before a group entry times out. If this field displays **never**, the corresponding multicast group is a static group and will never age out.

8.1.8 display igmp interface

Function

The **display igmp interface** command displays information about IGMP interfaces.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**]**interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP interfaces in a VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP interfaces in all instances.	-
interface-type interface-number	Displays information about a specified IGMP interface. If this parameter is not specified, the command displays information about all IGMP interfaces.	-
up	Displays information about the IGMP interfaces with the IP protocol in Up state and the IGMP protocol in Active state.	-
down	Displays information about the IGMP interfaces with the IP protocol in Down state and the IGMP protocol in Inactive state.	-
verbose	Displays detailed information about IGMP interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the IGMP configuration and running information on an interface, run the **display igmp interface** command. This command displays IGMP information only when IGMP is enabled on the interface.

Example

Display the IGMP configuration and running information on VLANIF100.

```
<HUAWEI> display igmp interface vlanif 100
Interface information of VPN-Instance: public net
 Vlanif100(192.168.1.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.2 (this router)
  Total 1 IGMP Group reported
```

Display IGMP parameters on all interfaces.

```
<HUAWEI> display igmp interface verbose
Interface information of VPN-Instance: public net
 Vlanif100(192.168.1.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Value of last member query time: 2 s
   Value of last member query interval: 1 s
   Value of startup query interval: 15 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:44
   Querier for IGMP: 192.168.1.2 (this router)
   IGMP activity: 1 joins, 0 leaves
   Robustness (negotiated): -
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled
   Prompt-leave: disabled
   SSM-Mapping: enabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
```

```
 TTL-check: disabled
Total 1 IGMP Group reported
```

Table 8-10 Description of the **display igmp interface** command output

Item	Description
Interface information of VPN-Instance	VPN instance to which IGMP interface information belongs. **public net** indicates the public network instance.
Vlanif100(192.168.1.2)	Interface type and interface number (IP address).
IGMP is enabled	IGMP has been enabled on an interface. IGMP can be enabled on an interface using the **igmp enable** command.
Current IGMP version is 2	IGMP version running on an interface. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. This parameter is configured using the **igmp version** command.
IGMP state	Status of an IGMP interface, which can be up or down.
IGMP group policy	Number of the ACL used in an IGMP group policy, which is used to control the number of groups that an interface can join. The ACL is specified by using the **igmp group-policy** command. The value **none** indicates that no ACL is applied to the interface.
IGMP limit	Maximum number of IGMP group memberships that the current interface can maintain. This parameter is configured using the **igmp limit** command.
Value of query interval for IGMP (negotiated)	Interval negotiated by non-queriers for sending Query messages. The negotiated value is only supported by IGMPv3.
Value of query interval for IGMP (configured)	Configured interval for sending IGMP Query messages. This parameter is configured using the **igmp timer query** command.
Value of other querier timeout for IGMP	Length of the other querier present timer. This parameter is configured using the **igmp timer other-querier-present** command. The value is 0 on the interface that functions as the querier.

Item	Description
Value of maximum query response time for IGMP	Maximum response time carried by an IGMP Query message. This parameter is configured using the **igmp max-response-time** command.
Value of last member query time	Last member query time, calculated using the following formula: Last member query time = Last member query interval x Robustness variable The last member query time is not defined in IGMPv1.
Value of last member query interval	Interval for sending Group-Specific Query messages. The value is configured using the **igmp lastmember-queryinterval** command. This interval is not defined in IGMPv1.
Value of startup query interval	Startup query interval of the querier. The interface sends Query messages at this interval when it starts to function as a querier. The value is 1/4 of the query interval configured using the **igmp timer query** command. The startup query interval is not defined in IGMPv1.
Value of startup query count	Number of query messages the querier interface sends at startup. The value is configured using the **igmp robust-count** command. The startup query count is not defined in IGMPv1.
General query timer expiry (hours:minutes:seconds)	Timeout interval of a general query timer.
Querier for IGMP	Link-local address of the IGMP querier. In IGMPv1, the querier is selected based on the multicast routing protocol. In IGMPv2, the multicast switch with the smallest IP address functions as the querier on the shared network segment.
IGMP activity: 1 joins, 0 leaves	Active group memberships on an interface. ● joins: indicates the number of IGMP groups that the interface has joined. When the interface joins a new group, the value increases by 1. When the interface leaves a group, the value remains unchanged. ● leaves: indicates the number of groups that the interface has left. When the interface leaves a group, the value increases by 1.

Item	Description
Robustness (negotiated)	Robustness variable negotiated by non-queriers. The negotiated value is only supported by IGMPv3.
Robustness (configured)	Robustness variable configured on an interface. This parameter is configured using the **igmp robust-count** command.
Require-router-alert	Whether the switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● enable: The switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● disable: The switch does not discard IGMP packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **igmp require-router-alert** command.
Send-router-alert	Whether the switch sends IGMP packets with the Router-Alert option. ● enabled: The switch sends IGMP packets with the Router-Alert option. ● disabled: The switch sends IGMP packets without the Router-Alert option. This function is configured using the **igmp send-router-alert** command.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses. ● enabled: The switch filters IGMP Report/ Leave messages based on host addresses. ● disabled: The switch does not filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.
Query Ip-source-policy	Whether to filter IGMP Query messages based on source addresses. ● enabled: The switch filters IGMP Query messages based on source addresses. ● disabled: The switch does not filter IGMP Query messages based on source addresses. This function is configured using the **igmp query ip-source-policy** command.

Item	Description
Prompt-leave	Whether fast leave is enabled. - enabled: Fast leave is enabled. - disabled: Fast leave is disabled. This function is configured using the **igmp prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. - enabled: SSM mapping is enabled. - disabled: SSM mapping is disabled. This function is enabled using the **igmp ssm-mapping enable** command.
Startup-query-timer-expiry	Interval at which the interface sends Query messages when it starts to function as a querier. The value is 1/4 of Timer query. The value **off** indicates that the interface has not started to send Query messages. The startup query timer is enabled only when the interface starts as a querier.
Other-querier-present-timer-expiry	Status of the other querier present timer: - off: The interface considers itself a querier and no other queriers exist. - on: The interface no longer considers itself a querier and another querier exists.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: - enabled - disabled This function is configured using the **igmp ttl-check** command.
Total 1 IGMP Group reported	Indicates the number of IGMP groups that the interface dynamically joins.

8.1.9 display igmp invalid-packet

Function

The **display igmp invalid-packet** command displays statistics and details about invalid IGMP packets received by the switch.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **leave** | **query** | **report** }] *

display igmp invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid IGMP messages received in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid IGMP messages received in all VPN instances.	-
interface *interface-type interface-number*	Displays statistics about invalid IGMP messages received on a specified interface. If this parameter is not specified, the command displays statistics about IGMP messages received on all interfaces.	-
message-type	Displays statistics about invalid IGMP messages of a specific type.	-
leave	Displays statistics about invalid Leave messages.	-
query	Displays statistics about invalid Query messages.	-
report	Displays statistics about invalid Report messages.	-
packet-number	Displays details about a specified number of invalid, recently received IGMP messages.	The value is an integer that ranges from 1 to 100. By default, details about all invalid, currently stored IGMP messages are displayed.
verbose	Displays details about invalid IGMP messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display igmp invalid-packet** command to view statistics and details about invalid IGMP messages for fault location and rectification.

If IGMP entries fail to be generated on a multicast network, you can run the **display igmp invalid-packet** command to check whether devices have received invalid IGMP messages. If the command output contains statistics about invalid IGMP messages, run the **display igmp invalid-packet** [*packet-number*] **verbose** command to view details about invalid IGMP messages to locate faults.

You can run the following commands to view information about specific invalid IGMP messages:

- Run the **display igmp invalid-packet interface** *interface-type interface-number* command to view statistics about invalid IGMP messages received by a specified interface.
- Run the **display igmp invalid-packet** *packet-number* **verbose** command to view details about invalid, recently received IGMP messages. Currently, the command output can contain details about a maximum of 100 invalid IGMP messages.

Example

Display statistics about invalid IGMP messages received by the switch.

```
<HUAWEI> display igmp invalid-packet

         Statistics of invalid packets for public net:
-------------------------------------------------------------------
IGMP Query invalid packet:
Unwanted Source List    : 1000        Zero Max Resp Code      : 0
Fault Length            : 1000        Invalid Multicast Group : 0
Bad Checksum            : 0

IGMP Report invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Checksum            : 0
Illegal Report Type     : 0

IGMP Leave invalid packet:
Invalid Multicast Group : 0           Bad Checksum            : 0
-------------------------------------------------------------------
```

Table 8-11 Description of the **display igmp invalid-packet** command output

Item	Description
Statistics of invalid packets for public net	Statistics of invalid IGMP messages in public network.
IGMP Query invalid packet	Number of invalid IGMP Query messages.
Unwanted Source List	Number of messages with unwanted source lists.

Item	Description
Zero Max Resp Code	Number of messages whose Max Resp Code field is 0.
Fault Length	Number of messages with invalid lengths.
Invalid Multicast Group	Number of messages with invalid group addresses.
Bad Checksum	Number of messages with checksum errors.
IGMP Report invalid packet	Number of invalid IGMP Report messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Illegal Report Type	Number of IGMP Report messages of invalid types.
IGMP Leave invalid packet	Number of invalid IGMP Leave messages.

Display details of one invalid recently received IGMP message.

```
<HUAWEI> display igmp invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 6):
-----------------------------------------------------
Interface           :  Vlanif100
Time                :  2010-06-09 11:03:51 UTC-08:00
Message Length      :  24
Invalid Type        :  Invalid Multicast Group
0000: 16 3c 00 00 01 34 04 04
-----------------------------------------------------
```

Table 8-12 Description of the **display igmp invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details about the invalid IGMP message.
Packet information (Index 6)	Sequence number of the invalid IGMP message, which is numbered in the opposite order in which the message is received.
Interface	Interface receiving invalid IGMP messages.

Item	Description
Time	Time when the invalid IGMP message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid IGMP message.
Invalid Type	Type of the invalid IGMP message.
0000: 16 3c 00 00 01 34 04 04	Contents of the invalid IGMP message.

8.1.10 display igmp proxy group

Function

The **display igmp proxy group** command displays information about IGMP proxy groups.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] [**interface** *interface-type interface-number*] [**verbose**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy groups in a specific VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP proxy groups in all VPN instances.	-

Parameter	Description	Value
group-address	Specifies a multicast group address. If you specify *group-address* in this command, the command displays information about a specified multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about IGMP proxy groups in the specified instances.	-
verbose	Displays detailed information about IGMP proxy groups. If you specify **verbose** in this command, the command displays status parameters of IGMP groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of an IGMP proxy group or find out the cause of a fault in an IGMP proxy group, run the **display igmp proxy group** command.

Example

Display information about IGMP proxy groups.

```
<HUAWEI> display igmp proxy group
Interface group report information
    Vlanif100(10.1.6.2):
     Total 2 IGMP proxy Groups
      Group Address   Filter mode
      225.1.1.1       exclude
      225.1.1.2       include
```

Display details of IGMP proxy groups.

```
<HUAWEI> display igmp proxy group verbose
Interface group report information
       Vlanif100(10.1.6.2):
        Total 2 IGMP proxy Groups
        Group: 225.1.1.1
          Filter mode: exclude
          Query Response Expiry: 00:00:02
          Source list (total 1 source)
             Source: 2.1.1.1
        Group: 225.1.1.2
          Filter mode: include
          Query Response Expiry: off
          Source list (total 1 source)
             Source: 2.1.1.2
```

Table 8-13 Description of the **display igmp proxy group** command output

Item	Description
Interface group report information	-
Vlanif100(10.1.6.2)	Interface type and interface number (IP address).
Total 2 IGMP proxy Groups	Total two IGMP proxy groups on an interface.
Group Address	Multicast group address.
Filter mode	Filter mode of a group, which can be exclude or include.
Query Response Expiry	Amount of time before the query response time expires.
Source list (total 1 source)	Multicast source list (number of sources in the source list).
Source	Multicast source address.
Group	Multicast group address.

8.1.11 display igmp proxy interface

Function

The **display igmp proxy interface** command displays information about IGMP proxy interfaces.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy interfaces in a specific VPN instance. If neither **vpn-instance** nor **all-instance** is specified, the command displays only IGMP proxy interfaces in the public network instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP proxy interfaces in all VPN instances.	-
interface-type interface-number	Displays information about IGMP proxy interfaces in a specific interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of an IGMP proxy interface or find out the cause of a fault in an IGMP proxy interface, run the **display igmp proxy interface** command.

Example

Display information about IGMP proxy interfaces.

```
<HUAWEI> display igmp proxy interface
Interface information of VPN-Instance: public net
 Vlanif100(192.168.1.2):
   IGMP proxy is enabled
   Current IGMP proxy version (negotiated) is 2
   Current IGMP proxy version (configured) is 2
   IGMP proxy state: up
   Value of query interval for IGMP (negotiated): 60 s
   Value of query interval for IGMP (configured): 60 s
   Value of querier present timeout for IGMPv1: off
   Value of querier present timeout for IGMPv2: 168 s
   Value of querier present timeout for IGMPv3: 124 s
   General query response expiry: off
   Querier for IGMP: 192.168.1.1
   Robustness (negotiated): 3
   Robustness (configured): 3
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query ip-source-policy: 2000
   TTL-check: disabled
```

Table 8-14 Description of the **display igmp proxy interface** command output

Item	Description
Interface information of VPN-Instance: public net	VPN instance to which IGMP proxy interface information belongs. **public net** indicates the public network instance.
Vlanif100(192.168.1.2)	Interface type and interface number (IP address).
IGMP proxy is enabled	IGMP proxy is enabled on the interface.
Current IGMP proxy version (negotiated) is	Negotiated IGMP version on the IGMP proxy interface .
Current IGMP proxy version (configured) is	Configured IGMP version on the IGMP proxy interface.
IGMP proxy state	Status of the IGMP proxy interface, which can be Up or Down.
Value of query interval for IGMP (negotiated)	Query interval negotiated between the query interval configured on the IGMP proxy interface and the query interval carried in a Query message, in seconds. Only IGMPv3 Query messages carry this field. This field takes effect only in IGMPv3.
Value of query interval for IGMP (configured)	Interval at which the IGMP proxy interface sends IGMP Query messages, in seconds.
Value of querier present timeout for IGMPv1	Timeout period of an IGMPv1 querier.
Value of querier present timeout for IGMPv2	Timeout period of an IGMPv2 querier.
Value of querier present timeout for IGMPv3	Timeout period of an IGMPv3 querier.
General query response expiry	Timeout period of a general group query timer.
Querier for IGMP	Address of an IGMP querier. In IGMPv1, a querier is selected based on a multicast routing protocol; in IGMPv2 and IGMPv3, the switch with the lowest IP address acts as the querier on the shared network segment. If no querier exists, this field is displayed as "-".
Robustness (negotiated)	Robustness variable negotiated between the robustness variable configured on an IGMP proxy interface and the robustness variable carried in a Query message. This field takes effect only in IGMPv3.

Item	Description
Robustness (configured)	Robustness variable configured on the IGMP proxy interface.
Require-router-alert	Whether the switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● enable: The switch discards IGMP packets that do not contain the Router-Alert option in IP packet headers. ● disable: The switch does not discard IGMP packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **igmp require-router-alert** command.
Send-router-alert	Whether the switch sends IGMP packets with the Router-Alert option. ● enabled: The switch sends IGMP packets with the Router-Alert option. ● disabled: The switch sends IGMP packets without the Router-Alert option. This function is configured using the **igmp send-router-alert** command.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses. ● enabled: The switch filters IGMP Report/Leave messages based on host addresses. ● disabled: The switch does not filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.
Query ip-source-policy	Whether to filter IGMP Query messages based on source addresses. ● enabled: The switch filters IGMP Query messages based on source addresses. ● disabled: The switch does not filter IGMP Query messages based on source addresses. This function is configured using the **igmp query ip-source-policy** command.

Item	Description
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: - enabled - disabled This function is configured using the **igmp ttl-check** command.

8.1.12 display igmp proxy routing-table

Function

The **display igmp proxy routing-table** command displays information about an IGMP proxy routing table.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **none** } | **incoming-interface** *interface-type interface-number* | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about an IGMP proxy routing table in a specific VPN instance. If you specify neither **vpn-instance** nor **all-instance** in this command, the command displays only the IGMP proxy routing table in the public network instance.	The value must be an existing VPN instance name.
all-instance	Displays information about IGMP proxy routing tables in all VPN instances.	-

Parameter	Description	Value
group-address	Displays information about the routing entry of a specified group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask	Indicates the mask of a multicast group address or a source address.	-
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of a multicast group address.	The value is in dotted decimal notation.
source-address	Displays the routing entry for a multicast source.	The value is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of a multicast source address.	The value is in dotted decimal notation.
outgoing-interface	Displays the routing entries with a specific interface as the outbound interface.	-
include	Displays the routing entries of which the downstream interface list has a specific interface.	-
exclude	Displays the routing entries of which the downstream interface list does not have a specific interface.	-
match	Displays the routing entries of which the downstream interface list has only a specific interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-

Parameter	Description	Value
none	Displays the routing entries with an empty downstream interface list.	-
incoming-interface	Displays the routing entries with a specific interface as the inbound interface.	-
flags *flag-value*	Indicates an IGMP proxy routing entry with a specific type. *flag-value* specifies the flag of a routing entry. If you specify **flags** *flag-value* in this command, the command displays IGMP proxy routing entries with the flag.	*flag-value* can be act, del, join, none, niif, sgjoin, wcjoin, upchg, or wc. For information about each value, see the flag-value field description in the **display pim routing-table** command output.
fsm	Displays detailed information about a finite state machine (FSM).	-
outgoing-interface-number	Displays the number of downstream interfaces in an IGMP proxy routing entry.	-
number	Specifies the number of downstream interfaces in an entry to be queried.	The value is an integer that ranges from 0 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To find information about an IGMP proxy routing table, run the **display igmp proxy routing-table** command. You can specify different parameters in this command to view specific routing information. This command helps you find specific routes and locate faults.

Example

Display details of an FSM in an IGMP proxy routing table.

```
<HUAWEI> display igmp proxy routing-table fsm
Routing table
```

```
Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Flag: WC, UpTime: 6d:10h
     Upstream interface: Vlanif100
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif200
             Protocol: igmp, UpTime: 17:27:13
             IGMP querier: 10.1.1.1(this router)
             IGMP state: EXCLUDE

     FSM information for non-downstream interfaces: None

 (10.3.3.100, 225.1.1.1)
     Flag: JOIN ACT, UpTime: 6d:17h
     Upstream interface: GigabitEthernetVlanif100
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif200
             Protocol: igmp, UpTime: 17:27:13
             IGMP querier: 10.1.1.1(this router)
             IGMP state: NI

     FSM information for non-downstream interfaces: None
```

Table 8-15 Description of the **display igmp proxy routing-table fsm** command output

Item	Description
Routing table	-
Total 1 (*, G) entry; 1 (S, G) entry	Total number of (*, G) and (S, G) entries in the IGMP proxy routing table.
(*, 225.1.1.1)	(*, G) or (S, G) entry in the IGMP proxy routing table.
Flag	Flag of a (*, G) or an (S, G) entry in the IGMP proxy routing table.
UpTime	Amount of time since a (*, G) or an (S, G) entry is created.
Upstream interface	Upstream interface of a (*, G) or an (S, G) entry.
Downstream interface(s) information	Information about downstream interfaces.
Total number of downstreams	Total number of downstream interfaces.
Vlanif200	Name of a downstream interface.
Protocol	Protocol of a downstream interface.

Item	Description
UpTime	Amount of time a downstream interface has been in Up state, expressed in hh:mm:ss format. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
IGMP querier	Address of an IGMP querier
IGMP state	IGMP status on a downstream interface: ● NI: indicates that an (S, G) entry inherits the downstream interfaces of a (*, G) entry. ● BLOCK: indicates that the interface does not forward traffic based on an (S, G) entry. ● INCLUDE: indicates that the interface needs to join the specified group and source. ● EXCLUDE: indicates that the interface does not join the specified group and source.
FSM information for non-downstream interfaces	Interfaces that do not forward multicast data packets matching (*, G) or (S, G) entries.

8.1.13 display igmp routing-table

Function

The **display igmp routing-table** command displays the IGMP routing table.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]] * [**static**] [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IGMP routing information in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays IGMP routing information in all instances.	-
group-address	Displays IGMP routing information of a specified multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the mask of a multicast group address or a multicast source address.	-
group-mask	Specifies the mask of a multicast group address.	It is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Displays IGMP routing information of a specified multicast source.	It is in dotted decimal notation.
source-mask	Specifies the mask of a multicast source address.	It is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.
static	Displays static IGMP routing entries.	-
outgoing-interface-number	Displays the number of the outbound interfaces in IGMP routing entries.	-
number	Specifies the number of outbound interfaces. If this parameter is specified, the command displays the specified number of outbound interfaces.	The value is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display igmp routing-table** command provides IGMP routing information. You can specify different parameters to view specific IGMP routing information and locate faults.

NOTE

This command provides output information only when PIM is not enabled on the IGMP-capable interface.

Example

Display the IGMP routing table.

```
<HUAWEI> display igmp routing-table
Routing table
 Total 2 entries

 00001. (10.10.10.10, 232.1.1.3)
       List of 1 downstream interface in include mode
        Vlanif100 (10.20.20.1),
                   Protocol: SSM-MAP

 00002. (*, 225.1.1.1)
       List of 1 downstream interface
        Vlanif100 (10.20.20.1),
                   Protocol: IGMP
```

Table 8-16 Description of the **display igmp routing-table** command output

Item	Description
Routing table	IGMP routing table.
Total 2 entries	Total number of IGMP routing entries.
00001. (10.10.10.10, 232.1.1.3)	Entry 00001. (S, G) indicates that data is transmitted from S to G. (*, G) indicates that data is transmitted from any source to G.
List of 1 downstream interface in include mode	List of the downstream interfaces that join the multicast group in INCLUDE mode.
Vlanif100 (10.20.20.1)	Interface type and interface number (IP address).
Protocol	Protocol type, including: ● SSM-MAP: Entries are generated using SSM mapping. ● IGMP: Entries are generated using IGMP. ● STATIC: Entries are generated by configuring static IGMP groups.

8.1.14 display igmp ssm-mapping

Function

The **display igmp ssm-mapping** command displays configuration of IGMP SSM mapping.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays SSM mapping entries in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays SSM mapping entries in all instances.	-
group [*group-address*]	Displays the SSM mapping entries of a specified group. If *group-address* is not specified, the command displays SSM mapping entries of all groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface [*interface-type interface-number*]	Displays whether SSM mapping is enabled on a specified interface. If *interface-type interface-number* is not specified, the command displays all the interfaces that are in Up state and have SSM mapping enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays mapping between multicast groups and multicast sources configured using the **ssm-mapping** command. You can also use this command to check the SSM mapping configuration on an interface. To enable SSM mapping on an interface, run the **igmp ssm-mapping enable** command in the interface view.

Example

Display SSM mapping entries of all the multicast sources and multicast groups.

```
<HUAWEI> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table
 Total 2 entries    2 entries matched

 00001. (10.1.0.2, 225.1.1.0/24)

 00002. (10.1.0.2, 239.255.255.0/24)

 Total 2 entries matched
```

Table 8-17 Description of the **display igmp ssm-mapping group** command output

Item	Description
IGMP SSM-Mapping conversion table	IGMP SSM mapping table.
Total 2 entries 2 entries matched	Total number of SSM mapping entries and total number of entries matching the query conditions.
00001. (10.1.0.2, 225.1.1.0/24) 00002. (10.1.0.2, 239.255.255.0/24)	Number of an (S, G) entry.
Total 2 entries matched	Number of SSM mapping entries matching the query conditions.

Display whether IGMP SSM mapping is enabled on VLANIF100.

```
<HUAWEI> display igmp ssm-mapping interface vlanif 100
IGMP SSM-Mapping is enabled
```

Table 8-18 Description of the display igmp ssm-mapping interface vlanif 100 command output

Item	Description
IGMP SSM-Mapping is enabled	SSM mapping is enabled on the interface.

8.1.15 igmp

Function

The **igmp** command displays the IGMP view.

The **undo igmp** command deletes all configurations in the IGMP view.

Format

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Global IGMP parameters must be configured in the IGMP view.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTE

Running the **undo igmp** command in the system view may interrupt IGMP services and deletes all global IGMP configurations of the public network instance. To restore the IGMP function, you have to re-run the deleted commands.

Example

Enter the IGMP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp]
```

8.1.16 igmp enable

Function

The **igmp enable** command enables IGMP on an interface.

The **undo igmp enable** command disables IGMP on an interface.

By default, IGMP is disabled on an interface.

Format

igmp enable

undo igmp enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User hosts and Layer 3 multicast devices directly connected to user network segments must run IGMP. A multicast device can process IGMP messages sent from user hosts only after IGMP is enabled on the interfaces connected to user network segments.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

If IGMPv1 is run on an interface, you must enable **pim dm** or **pim sm**. This is because IGMPv1 does not the querier election. In IGMPv1, the querier is specified by Protocol Independent Multicast (PIM).

If IGMPv2/v3 is run on an interface, **pim dm** or **pim sm** is recommended. Although IGMPv2/v3 supports the querier election, enabling PIM improves the system stability.

Precautions

- If PIM and IGMP need to be enabled on the same interface, enable PIM, and then IGMP.
- If IGMP parameters are configured on an interface, the parameter settings take effect only after IGMP is enabled.
- Running the **igmp enable** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

- When Layer 2 and Layer 3 multicast are both deployed, pay attention to the following points:
  - If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable IGMP on the corresponding VLANIF interface first, and then enable IGMP snooping in the VLAN. If IGMP snooping is enabled in the VLAN first, IGMP cannot be enabled on the VLANIF interface.
  - If Layer 2 and Layer 3 multicast are both configured in a VLAN, you must delete the Layer 2 multicast configuration before you can modify or delete the Layer 3 multicast configuration. This means that you must disable IGMP snooping in the VLAN first, then modify or disable the IGMP and PIM (IPv4) configuration in the VLANIF interface view, and finally enable IGMP snooping in the VLAN. Otherwise, the Layer 3 multicast configuration cannot be modified or deleted on the corresponding VLANIF interface.
  - If a VLANIF interface is shut down in the VLANIF interface view, Layer 2 multicast in the corresponding VLAN becomes ineffective accordingly. To make Layer 2 multicast effective, you must disable IGMP snooping in the VLAN first, then disable IGMP and PIM (IPv4) in the VLANIF interface view, and finally enable IGMP snooping in the VLAN.
  - When both Layer 2 and Layer 3 multicast services are configured, traffic is forwarded based on Layer 3 multicast forwarding entries instead of Layer 2 multicast forwarding entries. This means that Layer 2 multicast provides physical outbound interfaces for Layer 3 multicast, implementing accurate forwarding of multicast data. In addition, the maximum number of Layer 3 multicast forwarding entries depends on the maximum number of Layer 2 multicast forwarding entries.

Example

Enable IGMP on VLANIF100 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp enable
```

Enable IGMP on GE0/0/1 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp enable
```

8.1.17 igmp global limit

Function

The **igmp global limit** command sets the maximum number of IGMP entries that can be created on the switch.

The **undo igmp global limit** command deletes the configured maximum number of IGMP entries.

The following lists the maximum number of IGMP entries allowed on each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S6730-S, S6730S-S: 4096
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H: 8192

Format

igmp global limit *number*

undo igmp global limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created on the switch.	The value is an integer that ranges from 1 to *The maximum number of IGMP entries allowed by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of IGMP entries reaches the limit, the system does not create any new IGMP entries. To enable the switch to create new IGMP entries, delete unnecessary entries or increase the limit. Alternatively, you can configure static IGMP entries or source-groups.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.

- Each (*, G) entry established with SSM mapping is counted as one entry.

Precautions

You can also run the **limit (IGMP view)** command in the IGMP view to set the maximum number of IGMP group memberships in the system. If both the **igmp global limit** and **limit (IGMP view)** commands are run, the smaller value takes effect.

Example

Set the maximum number of IGMP entries that can be created on the switch to 248.

```
<HUAWEI> system-view
[HUAWEI] igmp global limit 248
```

8.1.18 igmp group-policy

Function

The **igmp group-policy** command configures an IGMP group policy on an interface to limit the range of multicast groups that the hosts can join.

The **undo igmp group-policy** command deletes the IGMP group policy.

By default, no IGMP group policy is configured on an interface, and the hosts can join any multicast groups.

Format

igmp group-policy *acl-number* [**1** | **2** | **3**]

undo igmp group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL or an advanced ACL. The ACL defines a multicast group range.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
1	Sets the range of multicast groups that IGMPv1 hosts can join.	-
2	Sets the range of multicast groups that IGMPv2 hosts can join.	-
3	Sets the range of multicast groups that IGMPv3 hosts can join.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control the multicast groups that hosts on the network attached to an interface can join, specify an ACL in the **igmp group-policy** command on the interface. This configuration improves security of the IGMP application. You can also use this command to prevent the switch from receiving Join messages for specified groups.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- Before running the **igmp group-policy** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the interface can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that an interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.
- After the **igmp group-policy** command is executed on an interface:
  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

Example

Create ACL 2005, and configure a rule that allows hosts to receive data of multicast group 225.1.1.1. Configure an IGMP group policy on VLANIF100 and

reference ACL 2005 to allow hosts connected to the interface to join only multicast group 225.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.1.1 0
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp group-policy 2005
```

Create ACL 2005, and configure a rule that allows hosts to receive data of multicast group 225.1.1.1. Configure an IGMP group policy on GE0/0/1 and reference ACL 2005 to allow hosts connected to the interface to join only multicast group 225.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.1.1 0
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp group-policy 2005
```

8.1.19 igmp ip-source-policy

Function

The **igmp ip-source-policy** command enables filtering of IGMP Report/Leave messages based on source addresses.

The **undo igmp ip-source-policy** command disables filtering of IGMP Report/Leave messages based on source addresses.

By default, the switch does not filter IGMP Report/Leave messages based on source addresses.

Format

igmp ip-source-policy [*basic-acl-number*]

undo igmp ip-source-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP runs on member hosts and their directly connected multicast devices. A multicast device processes all received Report/Leave messages. For security purposes, you can configure the multicast device to filter Report/Leave messages received on an interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

IGMP Report/Leave messages are encapsulated in IP packets. The **igmp ip-source-policy** command configures the switch to check the source address in the IP header of each received Report/Leave message. The switch filters Report/Leave messages based on the following rules (if ACL rules are not configured):

- If the source IP address of a Report/Leave message is 0.0.0.0 or on the same network segment as the IP address of the inbound interface, the switch processes the Report/Leave message.
- If the source IP address of a Report/Leave message is on a different network segment than the IP address of the inbound interface, the switch discards the Report/Leave message.

If you have specified an ACL rule, the interface filters out the IGMP Report/Leave messages whose source addresses do not match the ACL rule.

The **igmp ip-source-policy** command works with the **acl** command. For a numbered ACL, you can configure the source address of IGMP messages by specifying the **source** parameter in the **rule** command in the basic ACL view.

Example

Enable filtering of IGMP Report/Leave messages based on source addresses on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp ip-source-policy
```

Configure VLANIF100 to accept the IGMP Report/Leave messages with the source address 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp ip-source-policy 2001
```

Enable filtering of IGMP Report/Leave messages based on source addresses on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp ip-source-policy
```

8.1.20 igmp lastmember-queryinterval

Function

The **igmp lastmember-queryinterval** command configures interval at which an IGMP querier interface sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages after receiving IGMP Leave messages from hosts.

The **undo igmp lastmember-queryinterval** command restores the default value.

By default, the interval at which an IGMP querier interface sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages is 1s.

Format

igmp lastmember-queryinterval *interval*

undo igmp lastmember-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a querier receives a Leave message for a group, the querier periodically sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to check for other members in the group. The **igmp lastmember-queryinterval** command sets the interval at which the querier sends Last Member Query messages. The querier stops forwarding multicast data to the group if it receives no Report message from the group within the period specified by *interval* x *robust-value*. Here, *robust-value* is the robustness variable configured using the **igmp robust-count** or **robust-count** command.

If the querier receives at least one more Report message from the group within the specified period, the querier continues maintaining memberships of the group. Otherwise, the querier considers that the last member has left the group and no longer maintains memberships of the group.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 or IGMPv3.
- The **igmp lastmember-queryinterval** command has the same function as the **lastmember-queryinterval** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp lastmember-queryinterval 3
```

Set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp lastmember-queryinterval 3
```

8.1.21 igmp limit

Function

The **igmp limit** command sets the maximum number of IGMP group memberships allowed on an interface.

The **undo igmp limit** command restores the maximum number of IGMP group memberships allowed on an interface to the default value.

The following lists the maximum number of IGMP group memberships allowed on an interface of each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S6730-S, S6730S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H: 2048
- S6720S-EI, S6735-S, S6720-EI: 4096

Format

igmp limit *number* [**except** *acl-number*]

undo igmp limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP group memberships allowed on an interface.	The value is an integer that ranges from 1 to *The maximum number of IGMP group memberships allowed on an interface by default.* **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.
except	Specifies the range of multicast groups whose IGMP entries are not limited by the IGMP limit.	-

Parameter	Description	Value
acl-number	Specifies a basic ACL or an advanced ACL.	The value is an integer. The basic ACL number ranges from 2000 to 2999. A basic ACL filters group addresses only. The advanced ACL number ranges from 3000 to 3999. An advanced ACL filters (S, G) entries as well as group addresses.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To allow the switch to create more IGMP entries, delete useless entries or increase the limit. Alternatively, you can configure static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

If **except** is not specified in the command, the maximum number of all dynamic IGMP (*, G) or (S, G) entries is the configured IGMP limit. Before setting **except**, configure the associated ACL. The interface then uses the ACL to filter the received IGMP Report messages. The number of entries corresponding to the multicast groups that match the ACL is not limited.

The **igmp limit** command must be used with ACL configuration commands. When configuring ACL rules, note that:

- In the basic ACL view, specify the **source** parameter in the **rule** command to set the range of multicast groups whose IGMP entries are not limited.

- In the advanced ACL view, specify the **source** parameter in the **rule** command to set the range of sources that send multicast data to the multicast groups. Specify the **destination** parameter to set the range of multicast groups whose IGMP entries are not limited.

Example

Set the maximum number of IGMP entries that can be created on the VLANIF100 to 220.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp limit 220
```

Set the maximum number of IGMP entries that can be created on the GE0/0/1 to 220.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp limit 220
```

8.1.22 igmp max-response-time

Function

The **igmp max-response-time** command sets the maximum response time for IGMP General Query messages on an interface.

The **undo igmp max-response-time** command restores the default maximum response time for General IGMP Query messages.

By default, the maximum response time for IGMP General Query messages is 10s on an interface.

Format

igmp max-response-time *interval*

undo igmp max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. This may cause congestion on the network.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- This command is valid only for IGMPv2 and IGMPv3.
- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The **igmp max-response-time** command has the same function as the **max-response-time** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Set the maximum response time for IGMP General Query messages to 8 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp max-response-time 8
```

Set the maximum response time for IGMP General Query messages to 8 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp max-response-time 8
```

8.1.23 igmp on-demand

Function

The **igmp on-demand** command enables the IGMP on-demand function. This function enables a querier to maintain group memberships according to requirements of group members, without sending Query messages. After IGMP on-demand is enabled on an interface, dynamic IGMP entries on the interface will never age out.

The **undo igmp on-demand** command restores the default configuration.

By default, a querier does not maintain group memberships according to requirements of group members, and dynamic entries are aged out when the aging time expires.

Format

igmp on-demand

undo igmp on-demand

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a standard IGMP working process, a querier sends General Query messages periodically and collects group membership information based on received Report and Leave messages. Multicast group members respond to every Query message they receive. After IGMP on-demand is configured on the querier, the querier does not send Query messages, reducing IGMP packets exchanged between the querier and member hosts.

The IGMP on-demand function enables a querier to maintain group memberships based on requirements of members, without sending Query messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- IGMP on-demand applies only to IGMPv2 and IGMPv3.
- This command cannot be configured on a VLANIF interface if IGMP snooping is enabled in the VLAN corresponding to the VLANIF interface.
- If dynamic IGMP entries have been generated on the querier, run the **reset igmp group** command to clear these dynamic IGMP entries before running the **igmp on-demand** command.
- After the **igmp on-demand** command is executed on an interface (IGMP querier):
  - The interface does not send IGMP Query messages
  - IGMP group entries are generated after the interface receives IGMP Report messages and will never age out.
  - When the interface receives an IGMP Leave message, it deletes the corresponding IGMP entry.

Example

Enable the IGMP on-demand function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp on-demand
```

Enable the IGMP on-demand function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp on-demand
```

8.1.24 igmp prompt-leave

Function

The **igmp prompt-leave** command enables the fast leave function on an interface. This function enables an IGMP querier to delete IGMP entries immediately after receiving Leave messages from group members, without sending Group-Specific Query messages.

The **undo igmp prompt-leave** command disables fast leave on an interface.

By default, an IGMP querier sends a Group-Specific Query message after receiving a Leave message for a specific multicast group.

Format

igmp prompt-leave [**group-policy** *acl-number*]

undo igmp prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies an IGMP group policy. If this parameter is specified, the fast leave function takes effect only for multicast groups specified in the policy. When specifying this parameter, ensure that the referenced ACL has been configured. The device filters Leave messages on the interface based on the ACL. ● If a host leaves a multicast group in the range permitted by the ACL, the device immediately deletes the multicast group entry without sending a Group-Specific Query message. ● If a host leaves a multicast group out of the range permitted by the ACL, the device sends a Group-Specific Query message. If this parameter is not specified, the fast leave function takes effect for all multicast groups.	-
acl-number	Specifies the number of a basic ACL or an advanced ACL. This ACL defines a range of multicast groups. The specified ACL is configured using the **acl** command.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, a querier interface connects to only one receiver host. If the host frequently switches between multiple multicast groups, you can configure the fast leave function on the interface so that the interface can quickly respond to Leave messages sent from the host. After the fast leave function is configured, the querier does not send a Group-Specific Query message after receiving a Leave message. Instead, the querier directly notifies the upstream multicast device that the host has left the multicast group. The fast leave function reduces delay in response to Leave messages and saves network bandwidth.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- IGMP fast leave applies only to IGMPv2 and IGMPv3.
- When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.
- This command functions in the same way as the **prompt-leave** command used in the IGMP view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specific interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Create ACL 2005 and configure a rule that allows hosts to fast leave multicast groups in the range of 225.1.0.0/16. Configure fast leave on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp prompt-leave group-policy 2005
```

Create ACL 2005 and configure a rule that allows hosts to fast leave multicast groups in the range of 225.1.0.0/16. Configure fast leave on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2005
[HUAWEI-acl-basic-2005] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2005] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp prompt-leave group-policy 2005
```

8.1.25 igmp proxy

Function

The **igmp proxy** command enables IGMP proxy on an interface.

The **undo igmp proxy** command disables IGMP proxy on an interface.

By default, IGMP proxy is disabled on an interface.

Format

igmp proxy [**track nqa** *admin-name test-name*]

undo igmp proxy

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the administrator name and test name of an NQA test instance.	The value of either *admin-name* or *test-name* is a string of 1 to 32 case-sensitive characters, and spaces are not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a simple tree topology, multicast switches directly connected to user network segments do not need to run any complicated multicast routing protocol (such as PIM). However, the upstream access devices have to manage many users because the multicast switches transparently transmit all IGMP messages from hosts. To reduce the load on the upstream device, configure IGMP proxy on the multicast switches. The multicast switches then collect and summarize Report/Leave messages received from downstream hosts before sending them to the upstream device. The multicast switches also maintain group memberships and forward multicast packets based on the group memberships. The upstream device considers the multicast switches as hosts.

IGMP proxy lacks a fault detection mechanism to trigger link switchover quickly. Therefore, multicast services will be interrupted for a long time when a link failure occurs. You can solve this problem by associating IGMP proxy with a network quality analysis (NQA) test instance. If you specify **track nqa** *admin-name test-name* in the command, IGMP proxy will be associated with the specified NQA test instance for end-to-end link status monitoring. When the NQA test instance detects a link failure on the active IGMP proxy interface, the switch with the IGMP proxy interface protection mode configured can trigger a switchover between the active/standby or active/active links quickly to minimize the communication interruption time.

- If an NQA test instance detects a primary link Down event, the IGMP proxy-capable device switches traffic from the primary link to the backup link or to the other primary link.
- If an NQA test instance detects a primary link Up event or if the NQA test instance is ineffective or deleted, the IGMP proxy-capable device switches traffic back from the backup link to the primary link or balances traffic between the primary links based on the computing result of the group hash algorithm.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

Only one active IGMP proxy interface and one backup IGMP proxy interface or two active IGMP proxy interfaces can be configured. Only the primary IGMP proxy interface can be associated with an NQA

IGMP proxy conflicts with the following features:

- PIM: If the **pim sm** or **pim dm** command has been configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command is configured first, the **pim sm** or **pim dm** command cannot be used on the interface.
- IGMP: If the **igmp enable** command has been configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command is configured first, the **igmp enable** command cannot be used on the interface.
- Static group: After a static group is configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command has been configured, no static group can be configured on the interface.
- If two or more IGMP proxy interfaces have been configured on a device, the device's other interfaces cannot be configured as backup IGMP proxy interfaces.

Example

Enable IGMP proxy on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp proxy
```

Enable IGMP proxy on VLANIF100, and associate VLANIF100 with an NQA test instance named user test.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] destination-address ipv4 1.1.1.1
[HUAWEI-nqa-user-test] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp proxy track nqa user test
```

8.1.26 igmp proxy backup

Function

The **igmp proxy backup** command configures a backup IGMP proxy interface.

The **undo igmp proxy backup** command cancels the configuration.

By default, no backup IGMP proxy interface is configured.

Format

igmp proxy backup

undo igmp proxy backup

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IGMP proxy function becomes unavailable if the upstream interface with IGMP proxy configured fails. To enhance reliability of the IGMP service, configure a backup IGMP proxy interface after configuring IGMP proxy on the upstream interface. If the upstream interface fails, the backup interface takes over the IGMP proxy service to resume multicast services.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

An instance allows only one IGMP proxy interface and one backup IGMP proxy interface. Only one backup IGMP proxy interface can be configured on a device.

IGMP proxy conflicts with the following features:

- PIM: If the **pim sm** or **pim dm** command has been configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command is configured first, the **pim sm** or **pim dm** command cannot be used on the interface.
- IGMP: If the **igmp enable** command has been configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command is configured first, the **igmp enable** command cannot be used on the interface.
- Static group: After a static group is configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command has been configured, no static group can be configured on the interface.
- If two or more IGMP proxy interfaces have been configured on a device, the device's other interfaces cannot be configured as backup IGMP proxy interfaces.

Example

Configure VLANIF100 as a backup IGMP proxy interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp proxy backup
```

8.1.27 igmp proxy interface reroute

Function

The **igmp proxy interface reroute** command deletes switchback delay configurations of IGMP proxy interfaces, so that the interfaces enter the switchback state immediately after the switchback trigger conditions are met.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

igmp proxy [**vpn-instance** *vpn-instance* | **all-instance**] **interface** [*interface-type interface-number*] **reroute**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies a VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all VPN instances.	-
interface [*interface-type interface-number*]	Specifies an IGMP proxy interface. If *interface-type interface-number* is not specified, the command deletes switchback delay configuration of all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To delete switchback delay configurations of IGMP proxy interfaces, run the **igmp proxy interface reroute** command, after which the IGMP proxy interfaces enter the switchback state immediately after the switchback trigger conditions are met.

If neither **vpn-instance** *vpn-instance* nor **all-instance** is specified, the command deletes switchback delay configurations of IGMP proxy interfaces in the public network instance only.

Example

Delete switchback delay configurations of IGMP proxy interfaces in the public network instance.

```
<HUAWEI> igmp proxy interface reroute
Warning: This operation will lead to reroute IGMP proxy in the instance to which the interface belongs.
Continue? [Y/N]:Y
```

8.1.28 igmp proxy reroute delay

Function

The **igmp proxy reroute delay** command sets a switchback delay for an IGMP proxy interface.

The **undo igmp proxy reroute delay** command restores the default configuration.

By default, an IGMP proxy interface never enters the switchback state.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

igmp proxy reroute delay { *delay-time* | **never** }

undo igmp proxy reroute delay [*delay-time* | **never**]

Parameters

Parameter	Description	Value
delay-time	Sets a switchback delay for an IGMP proxy interface.	The value is an integer ranging from 10 to 86400, in seconds.
never	Indicates that an IGMP proxy interface never enters the switchback state.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

After a primary IGMP proxy interface recovers, multicast routing entries are updated. If the primary IGMP proxy interface fails again during an entry update, multicast traffic may be lost. To resolve such issues in primary IGMP proxy interface flapping scenarios, run the **igmp proxy reroute delay** command to set a switchback delay for the IGMP proxy interface. The multicast routing entry update process then starts only after the specified switchback delay expires.

Example

Set the switchback delay to 100s for an IGMP proxy interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp proxy reroute delay 100
```

8.1.29 igmp query ip-source-policy

Function

The **igmp query ip-source-policy** command configures IGMP Query message filtering based on source addresses.

The **undo igmp query ip-source-policy** command restores the default configuration.

By default, no source address-based IGMP Query message filtering is configured.

Format

igmp query ip-source-policy *basic-acl-number*

undo igmp query ip-source-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged IGMP Query messages with an IP address smaller than the querier IP address, the querier will be replaced by the attacker. As a result, the real querier cannot respond to Report messages from group members and bandwidth is wasted. Source address-based IGMP Query message filtering can protect the querier from such attacks. After this function is configured on a switch, the switch accepts only the IGMP Query messages with source addresses permitted by the specified ACL. This function controls querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

IGMP Query messages are encapsulated into IP messages. This command configures a policy to filter IGMP Query messages based on source addresses in IP headers, allowing only the source addresses that are in the ACL referenced in the policy.

The **igmp query ip-source-policy** command works with the **acl** command. For a numbered ACL, you can configure the source address of IGMP Query messages by specifying the **source** parameter in the **rule** command in the basic ACL view.

Example

Configure VLANIF100 to accept only the IGMP Query messages with the source address 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp query ip-source-policy 2001
```

Configure GE0/0/1 to accept only the IGMP Query messages with the source address 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp query ip-source-policy 2001
```

8.1.30 igmp require-router-alert

Function

The **igmp require-router-alert** command configures an interface to discard IGMP messages without the Router-Alert Option.

The **undo igmp require-router-alert** command disables an interface from checking for the Router-Alert Option in IGMP messages.

By default, the device does not check for the Router-Alert Option in IGMP messages and processes all the IGMP messages received on an interface.

Format

igmp require-router-alert

undo igmp require-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a packet to the corresponding protocol module for processing only when the destination address of the packet is a local interface address. Destination addresses of IGMP packets are multicast addresses but not interface addresses of multicast devices. Therefore, multicast devices do not send IGMP packets to the IGMP module, and the IGMP module cannot maintain group memberships.

The Router-Alert option in the IP header of an IGMP message solves this problem. If an IGMP message contains the Router-Alert option, the device sends the message to the routing protocol module.

You can configure the device to accept only IGMP messages with the Router-Alert option to improve IGMP security.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command has the same function as the **require-router-alert** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to discard IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp require-router-alert
```

Configure GE0/0/1 to discard IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp require-router-alert
```

8.1.31 igmp robust-count

Function

The **igmp robust-count** command sets an IGMP querier robustness variable on an interface.

The **undo igmp robust-count** command restores the default IGMP querier robustness variable on an interface.

By default, the IGMP querier robustness variable is 2.

Format

igmp robust-count *robust-value*

undo igmp robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the IGMP querier robustness variable.	The value is an integer that ranges from 2 to 5.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize the impact of packet loss on the network.

On a shared network segment, a querier maintains IGMP-attached group memberships. The robustness variable affects the timeout interval of group memberships. The timeout interval of group memberships is calculated using the formula:

Timeout interval of group memberships = Interval for sending IGMP General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the query interval configured using the **igmp timer query** or **timer query** command.

- Number of times the querier sends IGMPv2 Group-Specific Query messages or IGMPv3 Source-and-Group-Specific Query messages when the querier receives a Leave message

  When receiving an IGMP Leave message of a multicast group, the querier sends Group-Specific Query messages certain times specified by the robustness variable to check whether the group has members. When the querier receives a Report message indicating that source-group mapping changes, the querier sends Source-and-Group-Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Group-Specific Query messages and Source-and-Group-Specific Query messages can set using the **igmp lastmember-queryinterval** or **lastmember-queryinterval** command.

- Number of times for a querier to send IGMPv3 group/source-specific query messages after receiving the Report message about the change of the relationship between the multicast group and its source list.

  When receiving a Report message, the querier sends group/source-specific query messages for the "robustness variable" times. The interval for sending group/source-specific query messages can be set using the **igmp lastmember-queryinterval** command or the **lastmember-queryinterval** command.

A larger robustness variable makes an IGMP querier more robust, but increases the timeout interval of group memberships.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **igmp robust-count** command has the same function as the **robust-count** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Set the querier robustness variable on VLANIF100 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp robust-count 3
```

Set the querier robustness variable on GE0/0/1 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp robust-count 3
```

8.1.32 igmp send-router-alert

Function

The **igmp send-router-alert** command configures an interface to send IGMP messages containing the Router-Alert option in IP headers.

The **undo igmp send-router-alert** command disables an interface from sending IGMP messages containing the Router-Alert option in IP headers.

By default, the IP headers of IGMP messages sent by an interface contain the Router-Alert option.

Format

igmp send-router-alert

undo igmp send-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch sends IGMP messages that contain the Router-Alert option in IP headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo igmp send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option. The **igmp send-router-alert** command is usually used together with the **igmp require-router-alert** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **igmp send-router-alert** command has the same function as the **send-router-alert** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to send IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo igmp send-router-alert
```

Configure GE0/0/1 to send IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] undo igmp send-router-alert
```

8.1.33 igmp ssm-mapping enable

Function

The **igmp ssm-mapping enable** command enables SSM mapping on an interface.

The **undo igmp ssm-mapping enable** command disables SSM mapping on an interface.

By default, SSM mapping is disabled on an interface.

Format

igmp ssm-mapping enable

undo igmp ssm-mapping enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM model allows only IGMPv3 hosts to specify the multicast sources which they want to receive data from. However, some hosts can only run IGMPv1 or IGMPv2. To enable these hosts to use the SSM service, configure IGMP SSM mapping on the switch. IGMP SSM mapping is implemented based on static SSM mapping entries on the switch. The switch converts (*, G) information in IGMPv1 and IGMPv2 Report messages to (S, G) information according to static SSM mapping entries to provide the SSM service for IGMPv1 and IGMPv2 hosts.

The **igmp ssm-mapping enable** command enables SSM mapping on an interface. The mappings between multicast source addresses and group addresses take effect only when SSM mapping is enabled on an interface. SSM mappings are configured using the **ssm-mapping** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The SSM mapping function takes effect on an interface only when the interface runs IGMPv3.

Example

Enable SSM mapping on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp ssm-mapping enable
```

Enable SSM mapping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp ssm-mapping enable
```

8.1.34 igmp static-group

Function

The **igmp static-group** command configures a static multicast group on an interface.

The **undo igmp static-group** command deletes a static multicast group from an interface.

By default, no static multicast group is configured on an interface.

Format

igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] }

igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] { **qinq pe-vid** *pe-vid* **ce-vid** *low-ce-vid* [**to** *high-ce-vid*] | **dot1q vid** *low-pe-vid* [**to** *high-pe-vid*] } (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

undo igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] { **qinq pe-vid** *pe-vid* **ce-vid** *low-ce-vid* [**to** *high-ce-vid*] | **dot1q vid** *low-pe-vid* [**to** *high-pe-vid*] } (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address. In batch configuration mode, this parameter specifies the start address of the multicast group range.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
inc-step-mask	Sets the step mask of group addresses in batch configuration mode.	-

Parameter	Description	Value
group-mask	Specifies the step mask of a group address in batch configuration mode, that is, the gap between two consecutive group addresses.	The value is a wildcard mask format that ranges from 0.0.0.1 to 15.255.255.255, in dotted decimal notation.
group-mask-length	Specifies the step mask length in batch configuration mode.	The value is an integer that ranges from 4 to 32. If *group-mask-length* is used to configure the step mask and the **display current-configuration** command is used to display related configurations, the step mask of group addresses is displayed in *group-mask* format.
number *group-number*	Specifies the number of group addresses in batch configuration mode.	The value is an integer that ranges from 2 to 512.
source *source-address*	Specifies a multicast source address. If the specified static group address is an SSM group address, you must specify a multicast source address for the group.	The address is in dotted decimal notation.
all	Indicates all multicast groups that an interface statically joins.	-
qinq	Statically adds a sub-interface for QinQ Virtual Local Area Network (VLAN) tag termination to a multicast group.	-
pe-vid *pe-vid*	Specifies the ID of the outer VLAN tag.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid	Indicates the ID of the inner VLAN tag.	-
low-ce-vid	Specifies the lower limit of the CE-VLAN ID (inner VLAN tag).	The value is a decimal integer that ranges from 1 to 4094.

Parameter	Description	Value
to	Indicates a value range.	-
high-ce-vid	Specifies the upper limit of the CE-VLAN ID (inner VLAN tag).	The value is a decimal integer that ranges from 1 to 4094. The value of *high-ce-vid* cannot be smaller than that of *low-ce-vid*. By default, the values of *high-ce-vid* and *low-ce-vid* are the same.
dot1q	Statically adds a sub-interface for dot1q VLAN tag termination to a multicast group.	-
vid	Indicates the VLAN ID.	-
low-pe-vid	Specifies the lower limit of PE-VLAN ID (outer VLAN tag).	The value is a decimal integer that ranges from 1 to 4094.
high-pe-vid	Specifies the upper limit of PE-VLAN ID (outer VLAN tag).	The value is a decimal integer that ranges from 1 to 4094. The value of *high-pe-vid* cannot be smaller than that of *low-pe-vid*. By default, the values of *high-pe-vid* and *low-pe-vid* are the same.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following are two scenarios in which you can configure static multicast groups on user-side interfaces of the switch:

- There are long-term group members on a shared network segment, and the switch needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the switch considers that the multicast group always has members on the network segment of the interface. Therefore, the switch always forwards multicast data of the multicast group.

The **igmp static-group** command is used on an interface connected to user hosts. The command can configure a single group or source-group binding on an interface or configure multiple groups or source-group bindings in a batch.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Follow-up Procedure

If a user host no longer needs to receive multicast data of a static group, delete the static group configuration.

Precautions

- The IGMP entries of static groups configured on an interface never time out. The switch considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment of the interface.
- After you run the **igmp static-group** command without specifying the **qinq** or **dot1q** keyword to configure batch multicast static groups for the first time and when you run this command again, the new configuration overwrites the previous one if only the value of **group-number** is changed but the values of *group-address* and *group-mask* | *group-mask-length* are the same.

  After you run the **igmp static-group** command with specifying the **qinq** or **dot1q** keyword to configure batch multicast static groups for the first time and when you run this command again, the new configuration overwrites the previous one if only the value of **group-number** is changed but the values of *group-address* and *group-mask* | *group-mask-length* and the values of tag parameters the same. If the values of tag parameters are different, the device considers that the later command is different from the first one and the new configuration does not overwrite the previous configuration.
- You can specify the **qinq** keyword for only the sub-interface for QinQ VLAN tag termination and **dot1q** keyword for only the sub-interface for dot1q VLAN tag termination. The static group with tag parameters can be configured only on the sub-interface for QinQ VLAN tag termination or the sub-interface for dot1q VLAN tag termination.
- When the interface is configured with multiple VLAN tags, you must specify the **qinq** or **dot1q** keyword. The multicast source address cannot be specified in such a case. That is, source address and the **qinq** or **dot1q** keyword cannot be specified at the same time.

- The specified range of VLAN IDs must be consistent with that specified in the **dot1q termination vid** command or the **qinq termination pe-vid ce-vid** command. If they are inconsistent, only the intersected tag values take effect.
- When the interface that connects a multicast device to the user network segment joins a multicast group in both dynamic and static modes, the interface preferentially joins the multicast group in static mode if a conflict occurs.
- You can configure overlapping multicast group addresses in different batch configurations. When you configure multiple static multicast groups in a batch on an interface, do not delete any static group configuration before the system completes the batch static group configuration.
- Do not statically add an interface to multicast groups if the interface is in the PIM NDR or assert loser state, because such an interface will not be added to the PIM outbound interface list.

Example

Configure static multicast group 224.1.1.1 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 224.1.1.1
```

Configure the switch to forward multicast packets from multicast source 192.168.11.1 to multicast group 232.1.1.1 through VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 232.1.1.1 source 192.168.11.1
```

Configure 10 static multicast groups on VLANIF100 in a batch. Set the start multicast group address to 225.1.1.1 and the step mask length to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 225.1.1.1 inc-step-mask 32 number 10
```

Configure 10 source-group bindings on VLANIF100 in a batch. Set the start multicast group address to 232.1.1.1, the source address to 192.168.11.1, and the step mask length to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp static-group 232.1.1.1 inc-step-mask 32 number 10 source 192.168.11.1
```

Configure static multicast group 224.1.1.1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp static-group 224.1.1.1
```

Configure the sub-interface for QinQ VLAN tag termination GE 0/0/1.1 to statically join multicast groups in batches, with the start group address of 225.0.0.0, the incremental mask length of 32, and the number of group addresses of 2. The outer VLAN tag is 1 and the inner VLAN tag ranges from 1 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] igmp static-group 225.0.0.0 inc-step-mask 32 number 2 qinq pe-vid 1
ce-vid 1 to 3
```

8.1.35 igmp timer other-querier-present

Function

The **igmp timer other-querier-present** command sets the other querier present timer on an interface.

The **undo igmp timer other-querier-present** command restores the default value of the other querier present timer on an interface.

The formula used to calculate the other querier present timer value is:

Other querier present timer = Robustness variable x Interval for sending IGMP General Query messages + 1/2 x Maximum response time for IGMP query messages

If the default values of the robustness variable, the interval for sending IGMP General Query messages, and the maximum response time for IGMP query messages are used, the other querier present timer value is 125s.

Format

igmp timer other-querier-present *interval*

undo igmp timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the IGMP querier to send Query messages to hosts on the network segment. If the querier fails to send Query messages, group memberships cannot be created or maintained. Non-queriers running IGMPv2 or IGMPv3 start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **igmp timer other-querier-present** command applies only to IGMPv2 and IGMPv3.
- The **igmp timer other-querier-present** command has the same function as the **timer other-querier-present** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer value is shorter than the interval for sending IGMP General Query messages, the querier election is triggered frequently.

Example

On VLANIF100, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp timer other-querier-present 200
```

On GE0/0/1, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp timer other-querier-present 200
```

8.1.36 igmp timer query

Function

The **igmp timer query** command sets the interval at which an interface sends IGMP General Query messages.

The **undo igmp timer query** command restores the default interval at which an interface sends IGMP General Query messages.

By default, an interface sends IGMP General Query messages at an interval of 60s.

Format

igmp timer query *interval*

undo igmp timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an interface sends IGMP General Query messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier checks whether a local network segment has group members by sending IGMP General Query messages at an interval, known as the general query interval. You can set the general query interval based on the needs of your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the general query interval. The robustness variable can be set using the **igmp robust-count** command or the **robust-count** command.

- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval, but more bandwidth and resources are consumed.
- The function of the **igmp timer query** command is the same as that of the **timer query** command used in the IGMP view. The configuration in the IGMP view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

NOTE

The default *interval* value in this command is 60 seconds, which is different than the default value 125 seconds defined by the RFC standard. A Huawei querier and a non-Huawei querier must send IGMP general query messages at the same interval.

Example

Set the interval at which VLANIF100 sends General Query messages to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp timer query 50
```

Set the interval at which GE0/0/1 sends General Query messages to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp timer query 50
```

8.1.37 igmp ttl-check

Function

The **igmp ttl-check** command enables the device to check the TTL values in received IGMP Report, Leave, and Query messages on a specific interface.

The **undo igmp ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received IGMP Report, Leave, and Query messages on an interface.

Format

igmp ttl-check

undo igmp ttl-check

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables TTL check for IGMP Report, Leave, and Query messages on an interface. This function protects the system against attacking IGMP messages by dropping the messages of which the TTL value is not 1. By default, TTL values of IGMP messages are not checked on an interface.

You can also configure TTL check for IGMP Report, Leave, and Query messages by using the **ttl-check** command in the IGMP view. This command takes effect for all IGMP-enabled interfaces.

Precautions

If both the **igmp ttl-check** and **ttl-check** commands are run, the **igmp ttl-check** configuration in the interface view takes precedence over the **ttl-check** configuration in the IGMP view.

Example

Enable TTL check for IGMP Report, Leave, and Query messages on a physical interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp ttl-check
```

Enable TTL check for IGMP Report, Leave, and Query messages on a VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] igmp ttl-check
```

8.1.38 igmp version

Function

The **igmp version** command specifies an IGMP version on an interface.

The **undo igmp version** command restores the default IGMP version on an interface.

By default, an interface runs IGMPv2.

Format

igmp version *version*

undo igmp version

Parameters

Parameter	Description	Value
version	Specifies the IGMP version running on the interface.	The value is integer that ranges from 1 to 3.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can only identify IGMP messages of a version earlier than its own IGMP version. To ensure normal IGMP operation, set on the switch an IGMP version the same as or alter than that running on member hosts.

If multiple switches exist on a shared network segment, configure the same IGMP version on all switch interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command functions in the same way as the **version** command used in the IGMP view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Configure IGMPv1 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] igmp version 1
```

Configure IGMPv1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] igmp version 1
```

8.1.39 lastmember-queryinterval (IGMP)

Function

The **lastmember-queryinterval** command configures interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages after receiving IGMP Leave messages from hosts.

The **undo lastmember-queryinterval** command restores the default value.

By default, the interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages is 1 second.

Format

lastmember-queryinterval *interval*

undo lastmember-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the querier receives a Leave message that a host sends to leave a multicast group, the querier periodically sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to check for other members in the multicast group. The **lastmember-queryinterval** command sets the interval at which the querier sends Last Member Query messages. The querier stops forwarding multicast data to the group if it receives no Report message from the group within the period specified by *interval* x *robust-value*. Here, *robust-value* is the robustness variable configured using the **igmp robust-count** or **robust-count** command.

If the querier does not receive any Report message within the specified period, it considers that the last member has left the group and no longer maintains the membership of this group.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 or IGMPv3.
- This command has the same function as the **igmp lastmember-queryinterval** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] lastmember-queryinterval 3
```

8.1.40 limit (IGMP)

Function

The **limit** command sets the maximum number of IGMP entries that can be created globally or in an instance.

The **undo limit** command restores the maximum number of IGMP entries that can be created globally or in an instance to the default value.

The following lists the maximum number of IGMP entries that can be created globally or in an instance on each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S6730-S, S6730S-S: 4096
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H: 8192

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created globally or in the current instance.	The value is an integer that ranges from 1 to *The maximum number of IGMP entries that can be created globally or in an instance by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the maximum number of IGMP entries supported globally or in an instance.

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To enable the switch to create more IGMP entries, delete useless entries or increase the limit. Alternatively, create static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry established with SSM mapping is counted as one entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can also run the **igmp global limit** *number* command in the system view to set the maximum number of global IGMP group memberships. If both the **limit** and **igmp global limit** *number* commands are executed, the smaller value takes effect.

Example

Set the maximum number of IGMP entries that can be created globally to 248.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] limit 248
```

8.1.41 max-response-time (IGMP)

Function

The **max-response-time** command sets a global maximum response time for IGMP General Query messages.

The **undo max-response-time** command restores the global maximum response time for IGMP General Query messages to the default value.

By default, the global maximum response time for IGMP General Query messages is 10 seconds.

Format

max-response-time *interval*

undo max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. This may cause congestion on the network.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- A smaller response time allows the switch to learn multicast memberships more quickly but occupies more bandwidth and system resources.
- This command has the same function as the **igmp max-response-time** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the maximum response time for IGMP General Query messages to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] max-response-time 8
```

8.1.42 prompt-leave (IGMP)

Function

The **prompt-leave** command enables the fast leave function globally. After receiving a Leave message for a group, the device immediately deletes the group entry, without sending an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message.

The **undo prompt-leave** command restores the default configuration.

By default, a multicast device sends an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message after receiving a Leave message from a host.

Format

prompt-leave [**group-policy** *acl-number*]

undo prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a group policy that controls the range of groups to which the fast leave takes effect.	-
acl-number	Specifies the number of a basic or advanced ACL. This list specifies the range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, after receiving a Leave message of a group or source-specific group, a multicast device sends an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message to check whether this group has other members. To minimize the response delay and save network bandwidth, configure fast leave on multicast devices. This function enables a multicast device to delete a group or source/group entry immediately after receiving a Leave message, without sending an IGMP Group-Specific Query message or IGMP Group-and-Source-Specific Query message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

IGMP fast leave applies only to IGMPv2 and IGMPv3.

This command functions in the same way as the **igmp prompt-leave** command used in the interface view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Enable IGMP fast leave in the IGMP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] prompt-leave
```

In the IGMP view, create ACL 2000, configure an ACL rule that permits group 225.1.0.0/16, and enable IGMP fast leave for the group.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp
[HUAWEI-igmp] prompt-leave group-policy 2000
```

8.1.43 proxy reroute delay

Function

The **proxy reroute delay** command sets a switchback delay for IGMP proxy interfaces in the IGMP view.

The **undo proxy reroute delay** command restores the default configuration.

By default, IGMP proxy interfaces never enter the switchback state.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

proxy reroute delay { *delay-time* | **never** }

undo proxy reroute delay [*delay-time* | **never**]

Parameters

Parameter	Description	Value
delay-time	Sets a switchback delay for IGMP proxy interfaces.	The value is an integer ranging from 10 to 86400, in seconds.
never	Indicates that IGMP proxy interfaces never enter the switchback state.	-

Views

IGMP view of the public network instance or IGMP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

After a primary IGMP proxy interface recovers, multicast routing entries are updated. If the primary IGMP proxy interface fails again during an entry update, multicast traffic may be lost. To resolve such issues in primary IGMP proxy interface flapping scenarios, run the **proxy reroute delay** command to set a switchback delay for IGMP proxy interfaces in the IGMP view. The multicast routing entry update process then starts only after the specified switchback delay expires.

The **proxy reroute delay** command configuration applies to all IGMP proxy interfaces in the public network instance or a VPN instance. If the **igmp proxy reroute delay** command is also run for a specific IGMP proxy interface, the **igmp proxy reroute delay** command takes precedence over the **proxy reroute delay** command configuration.

Example

Set the switchback delay to 100s for IGMP proxy interfaces in the public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] igmp
[HUAWEI-igmp] proxy reroute delay 100
```

8.1.44 proxy source-lifetime

Function

The **proxy source-lifetime** command sets the timeout period for an (S, G) entry that an IGMP proxy-capable switch generates.

The **undo proxy source-lifetime** command restores the default configuration.

By default, the timeout period of an (S, G) entry that an IGMP proxy-capable switch generates is 210 seconds.

Format

proxy source-lifetime *interval*

undo proxy source-lifetime

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of an (S, G) entry.	The value is an integer that ranges from 60 to 65535, in seconds. The default value is recommended for general use.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP proxy-capable switch starts a timer for each (S, G) entry and records the time when a multicast source S sends multicast packets. The **proxy source-lifetime** command sets the timeout period for (S, G) entries on an IGMP proxy-capable switch. An IGMP proxy interface starts a timer when it receives the first multicast packet from a multicast source and resets the timer every time it receives a multicast packet from the multicast source. If the interface does not receive any multicast packet from the multicast source within the timeout period, it considers the (S, G) entry invalid.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

#Set the timeout period for (S, G) entries to 200s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] proxy source-lifetime 200
```

In VPN instance mvpn, set the timeout period for (S, G) entries to 200s.

8.1.45 proxy source-policy

Function

The **proxy source-policy** command configures an IGMP proxy-capable router to filter received multicast data packets based on source addresses or source and group addresses.

The **undo proxy source-policy** command restores the default configuration.

By default, an IGMP proxy-capable router does not filter received multicast data packets.

Format

proxy source-policy *acl-number*

undo proxy source-policy

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL or an advanced ACL. The ACL defines a multicast group range.	The number of a basic ACL is an integer in the range 2000 to 2999. The number of an advanced ACL is an integer in the range 3000 to 3999.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an IGMP proxy-capable device needs to restrict multicast data packets sent from some multicast sources, run the **proxy source-policy** command to configure the device to filter multicast data packets based on source addresses or source and group addresses. This command can also be used to filter the multicast data encapsulated in Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **proxy source-policy** command takes effect only when IGMP proxy is enabled.

To reference a numbered ACL to a proxy source policy, run the **proxy source-policy** and **acl** commands together.

- In the basic ACL view, specify the **source** parameter in the **rule** command to set a multicast group range.
- In the advanced ACL view, specify **source** in the **rule** command to set a source address range and specify **destination** to set a group address range.

Named ACLs are classified into basic and advanced ACLs. The configuration rules of a named ACL are the same as that of a numbered ACL.

Example

Configure an IGMP proxy-capable router to accept the multicast data packets from multicast source 10.10.1.2 and to discard the multicast data packets from the multicast source 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.2 0
[HUAWEI-acl-basic-2001] rule deny source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] igmp
[HUAWEI-igmp] proxy source-policy 2001
```

Configure an IGMP proxy-capable router to accept the multicast data packets sent from multicast source 10.10.1.2 to multicast group 232.1.0.0.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl name myacl
[HUAWEI-acl-adv-myacl] rule permit ip source 10.10.1.2 0 destination 232.1.0.0 0.0.255.255
[HUAWEI-acl-adv-myacl] quit
[HUAWEI] igmp
[HUAWEI-igmp] proxy source-policy acl-name myacl
```

8.1.46 proxy ssm-policy

Function

The **proxy ssm-policy** command configures an SSM group address range for IGMP proxy.

The **undo proxy ssm-policy** command restores the default configuration.

The default SSM group address range for IGMP proxy is 232.0.0.0/8.

Format

proxy ssm-policy *basic-acl-number*

undo proxy ssm-policy

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL. This ACL defines a range of multicast groups.	The sequence number is an integer that ranges from 2000 to 2999.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default SSM group address range is 232.0.0.0 to 232.255.255.255. Generally, an IGMP proxy device provides the SSM service for hosts only when it receives Report messages with a group address in this range. If the SSM group address range needs to be narrowed to ensure security of a multicast network or be expanded to increase the number of SSM group addresses, configure a new SSM group address range on the IGMP proxy device. Ensure that all the multicast devices on the network are configured with the same SSM group address range.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The SSM model can be used in the following situations:

- Multicast group addresses are in an SSM address range, IGMPv3 is running on the user network segment, and multicast source addresses are specified in Report messages.

- Multicast group addresses are in an SSM address range, IGMPv1 or IGMPv2 is running on the user network segment, and SSM mapping is configured.

The **proxy ssm-policy** command works with the **acl** command. If a basic ACL is configured, you can specify **source** in the **rule** command to configure an SSM address range.

Example

Set the SSM group address range for IGMP proxy to 232.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp
[HUAWEI-igmp] proxy ssm-policy 2000
```

8.1.47 require-router-alert (IGMP)

Function

The **require-router-alert** command configures the switch to discard IGMP messages without the Router-Alert option.

The **undo require-router-alert** command disables the switch from checking for the Router-Alert option in IGMP messages.

By default, the switch does not check whether the received IGMP messages contain the Router-Alert option in IP headers, and it accepts all the received IGMP messages.

Format

require-router-alert

undo require-router-alert

Parameters

None

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a packet to the corresponding protocol module for processing only when the destination address of the packet is a local interface address. Destination addresses of IGMP packets are multicast addresses but not interface addresses of multicast devices. Therefore, multicast devices do not send IGMP packets to the IGMP module, and the IGMP module cannot maintain group memberships.

The Router-Alert option in IP packet headers solves this problem. This option indicates that a packet needs to be sent to the protocol module.

You can configure the switch to accept only IGMP messages with the Router-Alert option. This configuration improves security of the IGMP service.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command has the same function as the **igmp require-router-alert** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, configure the switch to discard IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] require-router-alert
```

8.1.48 reset igmp control-message counters

Function

The **reset igmp control-message counters** command clears statistics about IGMP messages.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears IGMP message statistics in a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all-instance	Clears IGMP message statistics in all instances.	-
interface *interface-type interface-number*	Clears IGMP message statistics on a specified interface. If this parameter is not specified, the command clears IGMP statistics on all interfaces.	-
message-type	Clears statistics about IGMP messages of a specified type. If this parameter is not specified, the command clears statistics about all IGMP messages.	-
query	Clears statistics about Query messages received by an interface.	-
report	Clears statistics about Report messages received by an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

IGMP still operates normally after IGMP message statistics are deleted.

Example

Clear statistics about IGMP messages on all interfaces.

```
<HUAWEI> reset igmp control-message counters
```

Clear statistics about IGMP messages on VLANIF100.

```
<HUAWEI> reset igmp control-message counters interface vlanif 100
```

8.1.49 reset igmp explicit-tracking

Function

The **reset igmp explicit-tracking** command deletes information about the hosts with dynamic group memberships established through IGMP on an interface.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **explicit-tracking** { **all** | **interface** *interface-type interface-number* [**host** *host-address* [**group** *group-address* [**source** *source-address*]]] }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes information about the hosts with IGMP-attached group memberships on interfaces in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Deletes information about the hosts with IGMP-attached group memberships on interfaces in all instances.	-
all	Deletes information about all the hosts.	-
interface *interface-type interface-number*	Deletes information about the hosts with IGMP-attached group memberships on a specified interface. If this parameter is not specified, the command deletes information about the hosts with IGMP-attached group memberships on all interfaces.	-
host *host-address*	Specifies the IP address of a host.	The address is in dotted decimal notation.
group *group-address*	Specifies the address of a multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
source *source-address*	Specifies the address of a multicast source.	The address is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete information about the hosts with dynamic group memberships established on interfaces using IGMP.

Example

Delete information about IGMP host 192.168.0.12 in group 232.1.1.1 on VLANIF10.

```
<HUAWEI> reset igmp explicit-tracking interface vlanif 10 host 192.168.0.12 group 232.1.1.1
```

Delete information about IGMP host 192.168.0.12 in (10.12.12.12, 232.1.1.1) on VLANIF10.

```
<HUAWEI> reset igmp explicit-tracking interface vlanif 10 host 192.168.0.12 group 232.1.1.1 source
10.12.12.12
```

8.1.50 reset igmp group

Function

The **reset igmp group** command deletes dynamic IGMP entries on interfaces.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes dynamic IGMP entries in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Deletes dynamic IGMP entries in all instances.	-
all	The first **all** deletes dynamic IGMP entries on all interfaces. The second **all** deletes all dynamic IGMP entries on a specified interface.	-
interface *interface-type interface-number*	Deletes dynamic IGMP entries on a specified interface.	-
group-address	Deletes dynamic IGMP entries of a specified group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask	Sets the mask of a multicast source address or group address.	-
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.

Parameter	Description	Value
source-mask	Specifies the mask of a multicast source address.	The mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command does not delete static group memberships configured on interfaces.

Deleting IGMP entries on an interface does not prevent the interface from joining the involved groups again.

NOTICE

After IGMP group memberships are deleted, group members may fail to receive multicast data. Therefore, exercise caution when using this command.

Example

Delete dynamic IGMP entries on all interfaces.

```
<HUAWEI> reset igmp group all
```

Delete all dynamic IGMP entries on VLANIF100.

```
<HUAWEI> reset igmp group interface vlanif 100 all
```

Delete the IGMP entries of group 225.0.0.1 on VLANIF100.

```
<HUAWEI> reset igmp group interface vlanif 100 225.0.0.1
```

Delete IGMP entries of groups 225.1.1.0 to 225.1.1.255 on VLANIF100.

```
<HUAWEI> reset igmp group interface vlanif 100 225.1.1.0 mask 255.255.255.0
```

8.1.51 reset igmp group ssm-mapping

Function

The **reset igmp group ssm-mapping** command deletes group memberships established with SSM mapping.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes group memberships established with SSM mapping in a specified VPN instance.	The value must be an existing VPN instance name.
all-instance	Deletes group memberships established with SSM mapping in all instances.	-
all	First **all**: deletes group memberships established with SSM mapping on all interfaces. Second **all**: deletes all group membership established with SSM mapping on the specified interface.	-
interface *interface-type interface-number*	Deletes group memberships established with SSM mapping on a specified interface.	-
group-address	Deletes the group membership established with SSM mapping for a specified group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Sets the mask of a multicast group address.	-
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete group memberships established with SSM mapping.

NOTICE

After IGMP group memberships are cleared, group members may fail to receive multicast data. Therefore, confirm your operation before clearing IGMP group information.

Example

Delete group memberships established with SSM mapping on all the interfaces.

```
<HUAWEI> reset igmp group ssm-mapping all
```

8.1.52 robust-count (IGMP)

Function

The **robust-count** command sets a global robustness variable for an IGMP querier.

The **undo robust-count** command restores the default robustness variable.

By default, the robustness variable of an IGMP querier is 2.

Format

robust-count *robust-value*

undo robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an IGMP querier.	The value is an integer that ranges from 2 to 5.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize the impact of packet loss on the network.

On a shared network, a querier maintains IGMP-attached group memberships on an interface. The robustness variable determines the timeout interval of group memberships. The timeout interval of group memberships is calculated using the following formula:

Timeout interval of group memberships = Interval for sending IGMP General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages at startup

  When the querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query members of multicast groups. The interval for sending General Query messages during this process is 1/4 of the interval configured using the **igmp timer query** or **timer query** command.
- In IGMPv2 and IGMPv3, the robustness variable determines the number of times the querier sends Group-Specific Query or Source-and-Group-Specific Query messages.

  When receiving an IGMP Leave message of a multicast group, the querier sends Group-Specific Query messages a certain number of times specified by the robustness variable to check whether the group has members. When the querier receives a Report message indicating that source-group mapping changes, the querier sends Source-and-Group-Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Group-Specific Query messages and Source-and-Group-Specific Query messages can be set using the **igmp lastmember-queryinterval** or **lastmember-queryinterval** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- A larger robustness variable makes an IGMP querier more robust, but increases the timeout interval of group memberships.
- This command has the same function as the **igmp robust-count** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the current interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the robustness variable of an IGMP querier to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] robust-count 3
```

8.1.53 send-router-alert (IGMP)

Function

The **send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in IP headers.

The **undo send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option.

By default, IGMP messages sent by the switch contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP messages sent by the switch contain the Router-Alert option in their IP headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option. The **send-router-alert** command is usually used together with the **require-router-alert** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command has the same function as the **igmp send-router-alert** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, configure the switch to send IGMP messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] undo send-router-alert
```

8.1.54 ssm-mapping (IGMP)

Function

The **ssm-mapping** command configures an SSM mapping rule to map a multicast source to a group address.

The **undo ssm-mapping** command deletes an SSM mapping rule.

By default, no SSM mapping rule is configured.

Format

ssm-mapping *group-address* { *group-mask* | *group-mask-length* } *source-address*

undo ssm-mapping { *group-address* { *group-mask* | *group-mask-length* } [*source-address*] | **static all** }

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
static all	Deletes all the configured static SSM mapping entries.	-

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts that support only IGMPv1 and IGMPv2 cannot join SSM groups. To enable multicast devices to provide the SSM service for these hosts, configure SSM mapping on the multicast devices. An SSM mapping entry maps a multicast source to a multicast group. After SSM mapping entries are configured on a multicast device, the device can convert (*, G) information in Report messages of IGMPv1 and IGMPv2 to (S, G) information.

The default range of SSM group addresses is 232.0.0.0 to 232.255.255.255. You can use the **ssm-policy** command to change the address range. All multicast groups out of this range are ASM groups.

The configured SSM mapping entries take effect only after the **igmp ssm-mapping enable** command is run on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- You can configure multiple static SSM mapping entries by running this command several times.
- To delete an SSM mapping entry, run the **undo ssm-mapping** *group-address* { *group-mask* | *group-mask-length* } *source-address* command. The **undo ssm-mapping static all** command deletes all the SSM mapping entries. Do not use this command unless necessary.

Example

In the public network instance, configure an SSM mapping entry to map multicast source address 10.8.8.8 to group address 225.5.5.5/32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] ssm-mapping 225.5.5.5 32 10.8.8.8
```

8.1.55 timer other-querier-present (IGMP)

Function

The **timer other-querier-present** command sets the other querier present timer.

The **undo timer other-querier-present** command restores the default value of the other querier present timer.

The formula used to calculate the other querier present timer value is:

Other querier present timer = Robustness variable x Interval for sending IGMP General Query messages + 1/2 x Maximum response time for IGMP query messages

If the robustness variable, the interval for sending IGMP General Query messages, and the maximum response time for IGMP Query messages all use default values, the other querier present timer value is 125 seconds.

Format

timer other-querier-present *interval*

undo timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer value.	The value is an integer that ranges from 60 to 300, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the IGMP querier to send Query messages to hosts on the network segment. If the querier fails to send Query messages, group memberships cannot be created or maintained. Non-queriers running IGMPv2 or IGMPv3 start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- This command has the same function as the **igmp timer other-querier-present** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

NOTICE

If the other querier present timer value is shorter than the interval for sending IGMP General Query messages, the querier election is triggered frequently.

Example

In the IGMP view, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] timer other-querier-present 200
```

8.1.56 timer query (IGMP)

Function

The **timer query** command sets a global interval for sending IGMP General Query messages.

The **undo timer query** command restores the default interval for sending IGMP General Query messages.

By default, the interval for sending IGMP General Query messages is 60 seconds.

Format

timer query *interval*

undo timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending IGMP General Query messages	The value is an integer that ranges from 1 to 18000, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier checks whether a local network segment has group members by sending IGMP General Query messages at an interval, known as the general query interval. You can set the general query interval based on needs of your network. The general query interval affects the following processes:

- When the querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query members of multicast groups. The message sending interval during this process is 1/4 of the interval for sending General Query messages. The robustness variable is configured using the **igmp robust-count** or **robust-count** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval. However, more bandwidth and switch resources are consumed in this case.
- This command has the same function as the **igmp timer query** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the global interval for sending IGMP General Query messages to 125 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] timer query 125
```

8.1.57 ttl-check (IGMP)

Function

The **ttl-check** command enables the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces.

The **undo ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received IGMP Report, Leave, and Query messages.

Format

ttl-check

undo ttl-check

Parameters

None

Views

IGMP view of the public network instance or IGMP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

To protect a device against IGMP message attacks, run the **ttl-check** command to enable the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces and discard such a message if its TTL value is not 1.

Example

Enable TTL check for IGMP Report, Leave, and Query messages in the IGMP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] ttl-check
```

8.1.58 version (IGMP)

Function

The **version** command configures a global IGMP version.

The **undo version** command restores the default configuration.

By default, the IGMP version is IGMPv2.

Format

version *version*

undo version

Parameters

Parameter	Description	Value
version	Specifies the IGMP version running on the interface.	The value is integer that ranges from 1 to 3.

Views

IGMP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can identify IGMP messages of a version earlier than its own IGMP version. To ensure normal IGMP operation, set on the switch an IGMP version the same as or later than that running on user hosts.

If multiple switches exist on a shared network segment, configure the same IGMP version on all switch interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command functions in the same way as the **igmp version** command used in the interface view, except that the configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the IGMP version to IGMPv3 globally.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] igmp
[HUAWEI-igmp] version 3
```

8.2 MLD Configuration Commands

8.2.1 MLD Configuration Commands

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.

Product	Support
S6700	Supported.

8.2.2 display default-parameter mld

Function

The **display default-parameter mld** command displays default MLD configurations.

Format

display default-parameter mld

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check default MLD parameter settings even after MLD parameters are modified. This command helps you determine which MLD parameters have been modified.

Example

Display default MLD configurations.

```
<HUAWEI> display default-parameter mld
 MLD View Default Configurations:
 --------------------------------
 Lastmember-queryinterval: 1 s
 Lastmember-query time: 2 s
 Max-response-time: 10 s
 Require-router-alert: disabled
 Robust-count: 2
 Send-router-alert: enabled
 Ssm-mapping: disabled
 Timer query: 125 s

 Interface View Default Configurations:
 -------------------------------------
 Group-policy: disabled
 Last listener query time: 2 s
 Lastlistener-query-interval: 1 s
 Max-response-time: 10 s
```

```
Other-querier-present-timer-expiry: off
Prompt-leave: disabled
Require-router-alert: disabled
Robust-count: 2
Send-router-alert: enabled
Ssm-mapping: disabled
Startup-query-timer-expiry: off
Static-group:  disabled
Timer query: 125 s
Version: 2
Ipsec sa: disabled
```

Table 8-19 Description of the **display default-parameter mld** command output

Item	Description
MLD View Default Configurations	Default configurations in the MLD view.
Lastmember-queryinterval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. This parameter is configured using the **lastlistener-queryinterval (MLD view)** command in the MLD view or the **mld lastlistener-queryinterval** command in the interface view.
Lastmember-query time	Last listener query time, equaling Lastmember-query-interval x Robust-count.
Max-response-time	Maximum response time for MLD Query messages. This parameter is configured using the **max-response-time (MLD view)** command in the MLD view or the **mld max-response-time** command in the interface view.
Require-router-alert	Whether the switch checks the Router-Alert option in received MLD messages. This function is configured using the **require-router-alert (MLD view)** command in the MLD view or the **mld require-router-alert** command in the interface view.
Robust-count	Robustness variable of the MLD querier. This parameter is configured using the **robust-count (MLD view)** command in the MLD view or the **mld robust-count** command in the interface view.
Send-router-alert	Whether the MLD messages sent from the switch carry the Router-Alert option. This function is configured using the **send-router-alert (MLD view)** command in the MLD view or the **mld send-router-alert** command in the interface view.

Item	Description
Ssm-mapping	Status of the MLD SSM mapping function. The value can be: ● enabled: This function is enabled. ● disabled: This function is disabled. This function is configured using the **mld ssm-mapping enable** command in the interface view.
Timer query	Interval for sending MLD General Query messages. This parameter is configured using the **timer query (MLD view)** command in the MLD view or the **mld timer query** command in the interface view.
Interface View Default Configurations	Default configurations in the interface view.
Group-policy	Whether a multicast group policy is configured. ● enabled: A multicast group policy is configured. ● disabled: No multicast group policy is configured. A multicast group policy is configured using the **mld group-policy** command.
Last listener query time	Last listener query time, equaling Lastlistener-query-interval x Robust-count.
Lastlistener-query-interval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Other-querier-present-timer-expiry	Status of the other querier present timer. ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
Prompt-leave	Whether the fast leave function is configured. This function is configured using the **mld prompt-leave** command.
Startup-query-timer-expiry	Status of the query timer on the interface that functions as the querier. ● off: The interface has sent Query messages. ● on: The interface has not finished sending Query messages.

Item	Description
Static-group	Whether static multicast groups are configured. ● enabled: Static multicast groups are configured. ● disabled: No static multicast groups are configured. A static multicast group is configured on an interface using the **mld static-group** command.
Version	MLD version number. MLD has two versions: MLDv1 and MLDv2. This parameter is configured using the **mld version** command.
Ipsec sa	Whether IPSec is enabled on the interface. The switch does not support this function.

8.2.3 display mld control-message counters

Function

The **display mld control-message counters** command displays statistics about MLD control messages.

Format

display mld control-message counters [**interface** *interface-type interface-number*] [**message-type** { **query** \| **report** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about MLD messages on a specified interface. If this parameter is not specified, the command displays statistics about MLD messages on all interfaces.	-
message-type	Displays statistics about MLD messages of a specified type. If this parameter is not specified, the command displays statistics about all types of MLD messages.	-
query	Displays statistics about Query messages received by the interface. Query messages are sent from a querier.	-
report	Displays statistics about Report messages received by the interface. Report messages are sent by hosts to join a multicast group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the number of MLD control messages sent and received on an interface.

Example

Display statistics about the MLD messages sent and received by VLANIF100.

```
<HUAWEI> display mld control-message counters interface vlanif 100
Interface message counter information
 Vlanif100(FE80::219:74FF:FE59:3302):
 Message Type                 Sent        Valid       Invalid     Ignore
 -----------------------------------------------------------------
 General Query               45          0           0           0
 Group Query                 0           0           0           0
 Source Group Query            0           0           0           0
 -----------------------------------------------------------------
 MLDV1
 Report ASM                  0           35679       0           0
 Report SSM                  0           0           0           0
 -----------------------------------------------------------------
 DONE  ASM                    0           0           0           0
 DONE  SSM                    0           0           0           0
 -----------------------------------------------------------------
 MLDV2
 ISIN Report                0           0           0           0
 ISEX Report                0           0           0           0
 TOIN Report                 0           0           0           0
 TOEX Report                 0           0           0           0
 ALLOW Report                 0           0           0           0
 BLOCK Report                0           0           0           0
 Source Records Total         0           0           0           0
 -----------------------------------------------------------------
 Others                     -           -           0           0
 -----------------------------------------------------------------
```

Table 8-20 Description of the **display mld control-message counters interface vlanif 100** command output

Item	Description
Interface message counter information	Statistics about MLD messages on an interface.
Vlanif100(FE80::219:74FF:FE59:3302)	Interface type and interface number (IPv6 link-local address).
Message Type	Type of the MLD messages.
Sent	Number of MLD messages sent from the interface.

Item	Description
Valid	Number of valid MLD messages received by the interface.
Invalid	Number of invalid MLD messages received by the interface.
Ignore	Number of received MLD messages ignored by the interface.
General Query	Number of MLD General Query messages.
Group Query	Number of MLD Multicast Address Specific Query messages.
Source Group Query	Number of MLD Multicast Address and Source Specific Query messages.
Report ASM	Number of MLDv1 Multicast Listener Report messages with multicast group addresses in the ASM group address range.
Report SSM	Number of MLDv1 Multicast Listener Report messages with multicast group addresses in the SSM group address range.
DONE ASM	Number of MLDv1 Multicast Listener Done messages with multicast group addresses in the ASM group address range.
DONE SSM	Number of MLDv1 Multicast Listener Done messages with multicast group addresses in the SSM group address range.
ISIN Report	Number of MLDv2 Multicast Listener ISIN Report messages.
ISEX Report	Number of MLDv2 Multicast Listener ISEX Report messages.
TOIN Report	Number of MLDv2 Multicast Listener TOIN Report messages.
TOEX Report	Number of MLDv2 Multicast Listener TOEX Report messages.
ALLOW Report	Number of MLDv2 Multicast Listener ALLOW Report messages.
BLOCK Report	Number of MLDv2 Multicast Listener BLOCK Report messages.
Source Records Total	Number of multicast sources carried in MLDv2 messages.

Item	Description
Others	Total number of ignored MLD messages and invalid MLD messages whose types cannot be identified.

8.2.4 display mld explicit-tracking

Function

The **display mld explicit-tracking** command displays information about the MLDv2 hosts that have joined the specific source/group in Include mode.

Format

display mld explicit-tracking [**interface** *interface-type interface-number* [**host-address** *ipv6-host-address* | **group** *ipv6-group-address* **source** *ipv6-source-address*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about MLDv2 hosts that join a specified multicast source in Include mode on a specified interface. If this parameter is not specified, the command displays information about MLDv2 hosts that join a specified multicast source in Include mode on all interfaces.	-
host-address *ipv6-host-address*	Specifies the link-local address of a host.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
group *ipv6-group-address*	Specifies the IPv6 address of a multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Parameter	Description	Value
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view information about MLDv2 hosts that have dynamically joined specified sources/groups in Include mode.

Example

Display information about the MLDv2 hosts that have joined the specific source/group in Include mode.

```
<HUAWEI> display mld explicit-tracking
Explicit-tracking information
 Total 2 hosts, 4 entries

 Vlanif100(FE80::2:4)
  0001.Host: FE80::224
       Uptime: 00:02:47
       Expires: 00:01:33
       (S, G) List:
         Group: FF44::1
             Source: FC00:0:0:1::1
               Uptime: 00:02:47
               Time since last refresh: 00:02:47
             Source: FC00:0:0:2222::3
               Uptime: 00:02:47
               Time since last refresh: 00:02:47
  0002.Host: FE80::225
       Uptime: 00:01:59
       Expires: 00:02:21
       (S, G) List:
         Group: FF44::1
             Source: FC00:0:0:1::1
               Uptime: 00:01:59
               Time since last refresh: 00:01:59
             Source: FC00:0:0:1::3
               Uptime: 00:01:59
               Time since last refresh: 00:01:59
```

Table 8-21 Description of the **display mld explicit-tracking** command output

Item	Description
Explicit-tracking information	Host information.

Item	Description
Total 2 hosts, 4 entries	Two hosts and four (S, G) entries in total.
Vlanif100(FE80::2:4)	Interface type and interface number (IPv6 link-local address).
Host	IPv6 host address.
Uptime	Running time after a host joins a multicast group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Predicted timeout period of a host. After the host times out, the host is deleted from the MLD member list. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
(S, G) List	List of (S, G) entries.
Group	IPv6 multicast group address.
Source	IPv6 unicast address of a multicast source.
Time since last refresh	Time since the host joins a multicast group last time. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.

8.2.5 display mld group

Function

The **display mld group** command displays information about MLD groups that hosts have dynamically joined by sending Report messages.

Format

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* [**verbose**]

display mld group [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command displays MLD group membership information on all interfaces.	-
verbose	Displays detailed information about a multicast group. If this parameter is not specified, the command displays only the summary of the MLD group.	-
entry-number	Displays statistics about MLD multicast groups that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check information about multicast groups that have established memberships.

Example

Display detailed information about all multicast groups that the interface dynamically joins.

```
<HUAWEI> display mld group verbose
Total entry on this router: 1
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(FE80::2E0:49FF:FE29:1103):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 MLD Group reported
   Group: FF05::2
     Uptime: 00:01:07
     Expires: 00:03:45
     Last reporter: FE80::215:E9FF:FEAC:7666
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: 00:03:45
```

Display statistics about MLD multicast groups that hosts dynamically join.

```
<HUAWEI> display mld group entry-number
Interface group report information of VPN-Instance: public net
  Total 100 MLD Groups reported
 Vlanif100(FE80:2300::4):
  Total 100 MLD Groups reported
```

Table 8-22 Description of the **display mld group** command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which MLD groups on an interface belong. **public net** indicates the public network instance.
Total entry on this router	Total number of dynamic MLD multicast groups on the switch.
Limited entry of this VPN-Instance	Maximum number of MLD entries that can be created for this instance.
Vlanif100(FE80::2E0:49FF:FE29:1103)	Interface type and interface number (IPv6 link-local address).
Total entry on this interface	Total number of dynamic MLD multicast groups on the interface.

Item	Description
Limited entry on this interface	Maximum number of MLD entries that the current interface can create.
Total 1 MLD Group reported	One MLD Report message is received on the interface.
Group	IPv6 address of an IPv6 multicast group.
Uptime	Time since a multicast group is discovered. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Time left before a group will be deleted from the MLD group table. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days. "off" indicates that the group will never be aged out.
Last reporter	Link-local address of the last host that sends a Multicast Listener Report message.

Item	Description
Last-listener-query-counter	Number of Multicast Address and Source Specific Query messages sent by the querier. After the querier receives an MLD done message sent from a host leaving a group, it sends the specified number of Multicast Address and Source Specific Query messages to check whether this group has other members on the network segment. The Last-listener-query-counter value reduces by 1 every time the querier sends a Multicast Address and Source Specific Query message. The number of times is configured using the **mld robust-count** command.
Last-listener-query-timer-expiry	The timeout time of the Multicast Address and Source Specific Query timer. The timer starts when the querier receives an MLD done message sent from a host leaving a group. The timer value is configured using the **mld lastlistener-queryinterval** command.
Group mode	Filter mode of multicast groups, that is, exclude or include.
Version1-host-present-timer-expiry	Timeout time of MLDv1 hosts. The timer value is calculated using the following formula: Timer value = General query interval x Robustness variable + Maximum response time for Query messages. The three parameters used in the formula are configured using the **mld timer query**, **mld robust-count**, and **mld max-response-time** commands respectively.

8.2.6 display mld group ssm-mapping

Function

The **display mld group ssm-mapping** command displays information about multicast group entries established with MLD SSM mapping.

Format

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]

display mld group ssm-mapping [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address. If this parameter is not specified, the command displays information about all multicast group entries established with SSM mapping.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Displays information about the multicast group entries established with SSM mapping on a specified interface. If this parameter is not specified, the command displays information about multicast group entries established with SSM mapping on all interfaces.	-
verbose	Displays detailed information about multicast group entries established with SSM mapping. If this parameter is not specified, the command displays only the summary of multicast groups mapped by SSM mapping.	-
entry-number	Displays statistics about MLD multicast groups established with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display mld group ssm-mapping** command to view information about multicast group entries that are established with SSM mapping. SSM mapping entries can be configured using the **ssm-mapping (MLD view)** command.

Example

Display detailed information about all multicast group entries established with SSM mapping.

```
<HUAWEI> display mld group ssm-mapping verbose
Total entry on this router: 1
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 Vlanif100(FE80::DD:84):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 MLD SSM-Mapping Group reported
   Group: FF36::1
     Uptime: 00:00:13
     Expires: 00:04:07
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: 00:04:07
```

Display detailed information about MLD multicast groups established with SSM mapping.

```
<HUAWEI> display mld group ssm-mapping entry-number
Interface group report information of VPN-Instance: public net
  Total 100 MLD SSM-Mapping Groups reported
 Vlanif100(FE80:2300::4):
  Total 100 MLD SSM-Mapping Groups reported
```

Table 8-23 Description of the **display mld group ssm-mapping** command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which MLD groups on an interface belong. **public net** indicates the public network instance.
Total entry on this router	Number of multicast group entries established with SSM mapping on the switch.
Limited entry of this VPN-Instance	Maximum number of multicast group entries that can be generated in the VPN instance.
Vlanif100(FE80::DD:84)	Interface type and interface number (IPv6 link-local address).

Item	Description
Total entry on this interface	Number of multicast group entries established with SSM mapping on the interface.
Limited entry on this interface	Maximum number of multicast group entries that can be generated on the interface.
Total 1 MLD SSM-Mapping Group reported	Total number of SSM mapping groups is 1.
Group	Multicast group address.
Uptime	Time since a multicast group is discovered. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Timeout period of a group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Last reporter	Link-local address of the last host that sends a Multicast Listener Report message.
Last-listener-query-counter	Number of times for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Last-listener-query-timer-expiry	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Group mode	Filter mode of the multicast group, that is, include or exclude.
Version1-host-present-timer-expiry	Timeout period of an MLDv1 host.

8.2.7 display mld group static

Function

The **display mld group static** command displays information about static MLD multicast groups on interfaces.

Format

display mld group [*ipv6-group-address*] **static** [**up** | **down**] [**verbose**]

display mld group [*ipv6-group-address*] **static interface-number**

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* **static** [**verbose**]

display mld group static interface *interface-type interface-number* **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address. If this parameter is not specified, the command displays information about all multicast groups with memberships.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
up | **down**	Displays information about an Up or Down interface. If this parameter is not specified, the command displays information about all interfaces.	-
verbose	Displays detailed information about the interfaces that statically join MLD multicast groups or source-specific multicast groups. If this parameter is not specified, the command displays only the summary of the MLD group.	-

Parameter	Description	Value
interface-number	Displays the number of the interfaces that statically join MLD multicast groups.	-
interface *interface-type interface-number*	Displays information about the MLD multicast groups that the specified interface statically joins.	-
entry-number	Displays the number of the MLD multicast groups that the interface statically joins.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mld group static** command to view information about the multicast groups and the interfaces that statically join MLD multicast groups or source-specific multicast groups. To configure a static multicast group on an interface, run the **mld static-group** command.

Example

Display information about statically joined MLD groups.

```
<HUAWEI> display mld group static
Static join group information
 Total 2 entries, Total 2 active entries
  (*, FF25::1)
  Interface:Vlanif10
  State:UP
  Expires:Never

  (*, FF25:100::1)
  Interface:Vlanif10
  State:UP
  Expires:Never
```

Table 8-24 Description of the **display mld group static** command output

Item	Description
Static join group information	Information about the MLD multicast groups that a switch statically joins.
Total 2 entries, Total 2 active entries	Total number of static multicast groups and active entries set on the switch.
(*, FF25::1)	(*, G) entry.
Interface:Vlanif10	Interface where the multicast group exists.
State	Status of an entry.
Expires	Timeout period of a multicast group.

Display detailed information about all static MLD multicast groups on an interface.

```
<HUAWEI> display mld group static verbose
Static join group information
 Total 1 entry
  00001.(*, FF25::1)
      Total List of 2 joined interfaces
      1.Vlanif10
          State:              UP
          Reference Count:    1
          Multicast Boundary:YES
          Outgoing Interface:YES
      2.Vlanif20
          State:              UP
          Reference Count:    1
          Multicast Boundary:YES
          Outgoing Interface:YES
```

Table 8-25 Description of the **display mld group static verbose** command output

Item	Description
Static join group information	Information about the multicast groups that an interface statically joins.
Total 1 entry	Number of static MLD group memberships on the device.
00001.(*, FF25::1)	(*, G) entry.
Total List of 2 joined interfaces	List of the interfaces that statically join multicast groups.
1.Vlanif10	Type and number of the interface.

Item	Description
State	Status of an interface, including: - UP: The interface is working properly. - DOWN: An error occurs on the physical link of the interface.
Reference Count	Number of times when a multicast group on the current interface is referenced.
Multicast Boundary	Whether the multicast forwarding boundary is configured. - YES - NO This function is configured using the **multicast boundary** *ipv6-group-address ipv6-group-mask-length* command.
Outgoing Interface	Whether downstream interfaces are available. - YES - NO

Display information about all the interfaces that statically join multicast groups and are in Up state.

```
<HUAWEI> display mld group static up
Static join group information
 Total 4 entries
  00001.(*,FF25::1)
      Total List of 2 joined interfaces
      Total Matched 2 interfaces
      1.Vlanif10
      2.Vlanif20
  00002.(FC00:0:0:1::1,FF25::1)
      Total List of 2 joined interfaces
      Total Matched 2 interfaces
      1.Vlanif10
      2.Vlanif20
```

Table 8-26 Description of the **display mld group static up** command output

Item	Description
Total List of 2 joined interfaces	Number of the interfaces that statically join multicast groups.
Total Matched 2 interfaces	List of the interfaces that statically join multicast groups and are in Up state.

Display the number of interfaces that statically join all multicast groups.

```
<HUAWEI> display mld group static interface-number
Static join group information
 Total 2 entries
  (*, FF25::1)
  Interface-Number:24

  (*, FF25::2)
  Interface-Number:24
```

Table 8-27 Description of the **display mld group static interface-number** command output

Item	Description
Interface-Number	Number of the interfaces that statically join multicast groups.

8.2.8 display mld interface

Function

The **display mld interface** command displays MLD information on an interface.

Format

display mld interface [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays MLD information on a specified interface. If this parameter is not specified, the command displays MLD information on all interfaces.	-
up	Indicates that the status of the IPv6 protocol on the MLD interface is Up, that is, MLD is in Active state.	-
down	Indicates that the status of the IPv6 protocol on the MLD interface is Down, that is, MLD is in Inactive state.	-
verbose	Displays detailed information about MLD interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the MLD configuration and running status on an interface, run the **display mld interface** command. This command displays MLD information only when MLD-enabled interfaces exist on the device.

Example

Display the MLD configuration and running status on VLANIF100.

```
<HUAWEI> display mld interface vlanif 100 verbose
Interface information
 Vlanif100(FE80::2E0:B4FF:FE35:FF01):
   MLD is enabled
   Current MLD version is 2
   MLD state: up
   MLD group policy: none
   MLD limit: -
   Value of query interval for MLD (negotiated): 125 s
   Value of query interval for MLD (configured): 125 s
   Value of other querier timeout for MLD: 0 s
   Value of maximum query response time for MLD: 10 s
   Value of last listener query time: 2 s
   Value of last listener query interval: 1 s
   Value of startup query interval: 31 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:28
   Querier for MLD: FE80::2E0:B4FF:FE35:FF01 (this router)
   MLD activity: 2 joins, 0 dones
   Robustness (negotiated): 2
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled
   Prompt-leave: disabled
   SSM-Mapping: enabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
    TTL-check: disabled
  Total 2 MLD Groups reported
```

Table 8-28 Description of the **display mld interface** command output

Item	Description
Vlanif100(FE80::2E0:B4FF:FE35:FF01)	Interface type and interface number (IPv6 link-local address).
MLD is enabled	MLD is enabled. To enable MLD, run the **mld enable** command.
Current MLD version is 2	MLD version is set to 2 on the interface. To set the MLD version, run the **mld version** command.
MLD state	Status of the MLD interface, that is, up or down.

Item	Description
MLD group policy	ACL6 number of the MLD group policy. To set ACL6 number of the MLD group policy, run the **mld group-policy** command.
MLD limit	Maximum number of MLD group members that the current interface can maintain. To set the maximum number of MLD group members that the current interface can maintain, run the **mld limit** command.
Value of query interval for MLD (negotiated)	Actual interval for sending MLD Query messages after negotiation, in seconds.
Value of query interval for MLD (configured)	Configured interval for sending MLD Query messages, in seconds. To set the interval for sending MLD Query messages, run the **mld timer query** command.
Value of other querier timeout for MLD	Timeout period of other MLD queriers, in seconds. To set the timeout period of an MLD querier, run the **mld timer other-querier-present** command.
Value of maximum query response time for MLD	Maximum response time for MLD Query messages, in seconds. To set the maximum response time for MLD Query messages, run the **mld max-response-time** command.
Value of last listener query time	Last listener query time, in seconds. The last listener query time is calculated by multiplying the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages by the robustness variable.
Value of last listener query interval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages (Last listener query), in seconds. To set the interval for sending Last listener query, run the **mld lastlistener-queryinterval** command.

Item	Description
Value of startup query interval	Interval for sending Query messages when a querier starts, in seconds. The interval is 1/4 the query interval configured using the **mld timer query** command.
Value of startup query count	Number of times the querier sends Query messages when a querier starts. To set the number of times for sending Query messages when the querier starts, run the **mld robust-count** command.
General query timer expiry (hours:minutes:seconds)	Timeout period of the general query timer.
Querier for MLD	Link-local address of the MLD querier.
MLD activity	Statistics about MLD activities (join or leave).
Robustness (negotiated)	Robustness variable after negotiation by the non-querier device.
Robustness (configured)	Robustness variable set on the interface. To set the robustness variable on an interface, run the **mld robust-count** command.
Require-router-alert	Whether the switch discards MLD packets that do not contain the Router-Alert option in IP packet headers. ● enable: The switch discards MLD packets that do not contain the Router-Alert option in IP packet headers. ● disable: The switch does not discard MLD packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **mld require-router-alert** command.

Item	Description
Send-router-alert	Whether the sent MLD packet carries the Router-Alert option. To configure whether the sent MLD packet carries the Router-Alert option, run the **mld send-router-alert** command.
Ip-source-policy	Whether to filter Multicast Listener Report/Done messages based on host addresses. ● enabled: The switch filters MLD Report/Leave messages based on host addresses. ● disabled: The switch does not filter MLD Report/Leave messages based on host addresses. This function is configured using the **mld ip-source-policy** command.
Query Ip-source-policy	Whether to filter MLD Query messages based on host addresses. To configure whether to filter MLD Query messages based on host addresses, run the **mld query ip-source-policy** command.
Prompt-leave	Whether fast leave is enabled. ● enabled: Fast leave is enabled. ● disabled: Fast leave is disabled. This function is configured using the **mld prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. ● enabled: SSM mapping is enabled. ● disabled: SSM mapping is disabled. This function is configured using the **mld ssm-mapping enable** command.

Item	Description
Startup-query-timer-expiry	Status of the timer for the interface functioning as the querier after startup to send Query messages. ● off: The interface sends Query messages immediately after startup. ● on: The interface delays sending Query messages after startup.
Other-querier-present-timer-expiry	Status of the timer identifying whether another querier is present. ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
TTL-check	Whether the function to check the TTL values in received MLD Report, Leave, and Query messages is enabled: ● enabled ● disabled
Total 2 MLD Groups reported	Two Multicast Listener Report messages are received on the interface.

8.2.9 display mld invalid-packet

Function

The **display mld invalid-packet** command displays statistics and details about invalid MLD packets received by a device.

Format

display mld invalid-packet [**interface** *interface-type interface-number* | **message-type** { **done** | **query** | **report** }]*

display mld invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about invalid MLD messages received by a specified interface. If this parameter is not specified, the command displays statistics about invalid MLD messages on all interfaces.	-
message-type	Displays statistics about invalid MLD messages of a specified type.	-
done	Displays statistics about invalid Multicast Listener Done messages.	-
query	Displays statistics about invalid Query messages.	-
report	Displays statistics about invalid Multicast Listener Report messages.	-
packet-number	Displays details of a specified number of invalid MLD messages recently received.	The value is an integer that ranges from 1 to 100.
verbose	Displays details of invalid MLD messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mld invalid-packet** command to view statistics and details of invalid MLD messages for fault location and rectification.

If MLD entries fail to be generated on a multicast network, you can run the **display mld invalid-packet** command first to check whether devices have received invalid MLD messages. If the command output contains statistics about invalid MLD messages, you need to run the **display mld invalid-packet** [*packet-number*] **verbose** command to view details of invalid MLD messages to locate the fault.

You can run the following related commands to view information about specific invalid MLD messages:

- Run the **display mld invalid-packet** command to view statistics about invalid MLD messages received by a device.
- Run the **display mld invalid-packet interface** *interface-type interface-number* command to view statistics about invalid MLD messages received by a specified interface.

- Run the **display mld invalid-packet** *packet-number* **verbose** command to view details of invalid MLD messages recently received. Currently, details of a maximum of 100 invalid MLD messages can be displayed.

Example

Display statistics about invalid MLD messages received by the device.

```
<HUAWEI> display mld invalid-packet
        Statistics of invalid packets for public net:
-------------------------------------------------------------------
MLD Query invalid packet:
Unwanted Source List    : 1000        Zero Max Resp Code      : 0
Fault Length            : 1000        Invalid Multicast Group : 0
Bad Checksum            : 0

MLD Report invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Checksum            : 0
Illegal Report Type     : 0

MLD Done invalid packet:
Invalid Multicast Group : 0           Bad Checksum            : 0
-------------------------------------------------------------------
```

Table 8-29 Description of the **display mld invalid-packet** command output

Item	Description
Statistics of invalid packets for public net	Invalid packets received in the public net.
MLD Query invalid packet	Invalid MLD Query messages.
Unwanted Source List	Messages with unwanted source lists.
Zero Max Resp Code	Messages with the Max Resp Code fields being 0.
Fault Length	Messages with invalid lengths.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Bad Checksum	Messages with checksum errors.
MLD Report invalid packet	Invalid MLD Report messages.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Illegal Report Type	Messages with the illegal Report message type.
MLD Done invalid packet	Invalid Multicast Listener Done messages.

Display details of one invalid MLD message recently received by the device.

```
<HUAWEI> display mld invalid-packet 1 verbose
      Detailed information of invalid packets
```

```
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Interface           :  Vlanif100
Time                :  2012-06-09 11:03:51 UTC-08:00
Message Length      :  24
Invalid Type        :  Invalid Multicast Group
0000: 84 00 4c d7 00 00 00 00 11 17 00 00 00 00 00 00
0010: 00 00 00 00 00 01 00 01
-----------------------------------------------------
```

Table 8-30 Description of the **display mld invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of the invalid MLD message.
Packet information (Index 1)	Sequence number of the invalid MLD message (numbered in the opposite order that the message is received).
Interface	Interface receiving the invalid MLD message.
Time	Time when the invalid MLD message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid MLD message.
Invalid Type	Type of the invalid MLD message: ● Unwanted Source List ● Zero Max Resp Code ● Fault Length ● Invalid Multicast Group ● Bad Checksum ● Invalid Multicast Source ● Illegal Report Type
0000: 84 00 4c d7 00 00 00 00 11 17 00 00 00 00 00 00 0010: 00 00 00 00 00 01 00 01	Contents of the invalid MLD message.

8.2.10 display mld routing-table

Function

The **display mld routing-table** command displays information about the MLD routing table.

Format

display mld routing-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*]] * [**static**] [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
ipv6-source-mask-length	Specifies the mask length of the IPv6 address of a multicast source.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
static	Displays the MLD routing table of the static multicast group.	-
outgoing-interface-number	Displays the number of the outbound interfaces in MLD routing entries.	-

Parameter	Description	Value
number	Specifies the number of outbound interfaces. After this parameter is specified, the command displays information about the specified number of outbound interfaces.	The value is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view MLD routing entries, run the **display mld routing-table** command. You can specify parameters to view specified routing information, which facilitates fault location.

NOTE

This command provides output information only when PIM (IPv6) is not enabled on the MLD-capable interface.

Example

Display the MLD routing entry of the specified multicast group.

```
<HUAWEI> display mld routing-table
Routing table
 Total 2 entries

 00001. (FC00:0:0:1::3, FF44::)
       List of 1 downstream interface in include mode
        Vlanif100 (FE80::EE:53),
                    Protocol: STATIC

 00002. (*, FF55::)
       List of 1 downstream interface
        Vlanif100 (FE80::EE:53),
                    Protocol: MLD
```

Table 8-31 Description of the **display mld routing-table** command output

Item	Description
Routing table	MLD routing table.
Total 2 entries	Total number of MLD routing entries.
00001. (FC00:0:0:1::3, FF44::)	Entry 00001. (S, G) indicates that data is transmitted from S to G. (*, G) indicates that data is transmitted from any source to G.
List of 1 downstream interface in include mode	List of the downstream interfaces that join the multicast group in INCLUDE mode.
Vlanif100(FE80::EE:53)	Interface type and interface number (IPv6 link-local address).
Protocol	Protocol type. ● SSM-MAP: Entries are generated using MLD SSM mapping. ● MLD: Entries are generated using MLD. ● STATIC: Entries are generated by the MLD static multicast group.
List of 1 downstream interface	Downstream interface list.

8.2.11 display mld ssm-mapping

Function

The **display mld ssm-mapping** command displays the configuration of MLD SSM mapping.

Format

display mld ssm-mapping { **group** [*ipv6-group-address*] | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
group *ipv6-group-address*	Specifies the source IPv6 address of a specified multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Parameter	Description	Value
interface *interface-type interface-number*	Displays whether a specified interface is enabled with SSM mapping. If this parameter is not specified, the command displays information about all Up interfaces enabled with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view multicast sources mapped to a multicast group. SSM mapping entries can be configured using the **ssm-mapping (MLD view)** command. The **display mld ssm-mapping** command also allows you to view the SSM mapping status on an interface, which can be configured using the **mld ssm-mapping enable** command.

Example

Display information about the interface configured with SSM mapping.

```
<HUAWEI> display mld ssm-mapping interface
Interface information
Vlanif100(FE80::1)
```

Table 8-32 Description of the **display mld ssm-mapping interface** command output

Item	Description
Vlanif100(FE80::1)	Interface type and interface number (IPv6 address).

Display information about SSM mapping of all multicast sources and groups.

```
<HUAWEI> display mld ssm-mapping group
MLD SSM-Mapping conversion table
 Group: FF3E::/64
  Number of Source(s): 3
     FC00:0:0:1::1
```

```
    FC00:0:0:1::2
    FC00:0:0:1::3
```

Table 8-33 Description of the **display mld ssm-mapping group** command output

Item	Description
MLD SSM-Mapping conversion table	MLD SSM mapping entries.
Group	Address of a multicast group.
Number of Source(s)	Number of multicast sources configured with SSM mapping.
FC00:0:0:1::1	Multicast source address.

Check whether MLD SSM mapping is enabled on VLANIF100.

```
<HUAWEI> display mld ssm-mapping interface Vlanif 100
MLD SSM-Mapping is enabled
```

Table 8-34 Description of the **display mld ssm-mapping interface Vlanif 100** command output

Item	Description
MLD SSM-Mapping is enabled	SSM mapping is enabled on the interface.

8.2.12 display mld ssm-mapping interface

Function

The **display mld ssm-mapping interface** command displays information about interfaces enabled with SSM mapping.

Format

display mld ssm-mapping interface [*interface-type interface-number* [**group** *ipv6-group-address*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies an interface.	-

Parameter	Description	Value
group *ipv6-group-address*	Displays the source address list associated with a specified group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display mld ssm-mapping interface** command to view information about an interface enabled with SSM mapping.

Example

Display information about the interface configured with SSM mapping.

```
<HUAWEI> display mld ssm-mapping interface
Interface information
 Vlanif100(FE80::1)
```

Table 8-35 Description of the **display mld ssm-mapping interface** command output

Item	Description
Vlanif100(FE80::1)	Interface type and interface number (IPv6 link-local address).

8.2.13 lastlistener-queryinterval (MLD view)

Function

The **lastlistener-queryinterval** command globally sets the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after the MLD querier receives an MLD Done message from a host.

The **undo lastlistener-queryinterval** command restores the default value.

By default, the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is 1 second.

Format

lastlistener-queryinterval *interval*

undo lastlistener-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after the MLD querier receives a Multicast Listener Done message.	The value is an integer that ranges from 1 to 5, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MLD querier receives a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages continuously to check for other members in the multicast group. The **lastlistener-queryinterval** command sets the interval at which the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If the querier receives no Multicast Listener Report message for a specified period, the querier stops forwarding data to the multicast group. The period is calculated by multiplying *interval* by *robust-value*. To set *robust-value*, run the **mld robust-count** or **robust-count (MLD view)** command.

If the querier receives a Multicast Listener Report message from a host within the maximum response time, the querier maintains the membership of the multicast group. Otherwise, the querier considers that the last member has left the group and does not maintain the membership of the multicast group.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld lastlistener-queryinterval** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] lastlistener-queryinterval 3
```

8.2.14 limit (MLD view)

Function

The **limit** command sets the maximum number of MLD entries that can be created globally.

The **undo limit** command restores the maximum number of MLD entries that can be created globally to the default value.

The following lists the maximum number of MLD entries allowed on each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S: 512
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S: 4096

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created globally.	The value is an integer that ranges from 1 to *The maximum number of MLD entries allowed by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the maximum number of MLD entries globally.

When the number of MLD entries reaches the limit, the system no longer creates MLD entries. To enable the switch to allow new join requests, you can either delete useless entries or increase the limit. Alternatively, configure static multicast groups or source-group bindings on interfaces.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **mld global limit** *number* command in the system view to set the maximum number of global MLD group memberships. If both the **limit** and **mld global limit** *number* commands are run, the smaller value takes effect.

Example

Set the maximum number of MLD entries to 1000 globally.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] limit 1000
```

8.2.15 max-response-time (MLD view)

Function

The **max-response-time** command sets a global maximum response time for MLD General Query messages.

The **undo max-response-time** command restores the default global maximum response time for MLD General Query messages.

By default, the global maximum response time for MLD General Query messages is 10 seconds.

Format

max-response-time *interval*

undo max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for MLD General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send Multicast Listener Report messages immediately after receiving MLD General Query messages, the querier on the local network segment may receive a large number of Multicast Listener Report messages from the hosts at the same time. This may cause congestion on the network.

To avoid such situations, MLD messages specify the maximum response time for MLD General Query messages. When a host receives an MLD Query message, the host starts a timer for the multicast group that it joins. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Multicast Listener Report message to the querier.

The maximum response time specifies the deadline for the host to send a Multicast Listener Report message. A proper maximum response time allows hosts to respond to MLD Query messages and prevents hosts from sending Report messages at the same time.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The function of this command is the same as that of the **mld max-response-time** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the maximum response time for MLD General Query messages to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] max-response-time 8
```

8.2.16 mld

Function

The **mld** command displays the MLD view.

The **undo mld** command clears all configurations in the MLD view.

Format

mld

undo mld

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Global MLD parameters must be configured in the MLD view.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In using the **undo mld** command, you need to enter Y or N to confirm the action. This command will clear global MLD configurations. So, use this command with caution.

Example

Enter the MLD view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld]
```

8.2.17 mld enable

Function

The **mld enable** command enables MLD on an interface.

The **undo mld enable** command disables MLD on an interface.

By default, MLD is disabled on an interface.

Format

mld enable

undo mld enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a shared IPv6 network segment, hosts and multicast devices must run MLD. A multicast device can process MLD messages sent from hosts only after MLD is enabled on the interfaces connected to user network segments.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- If MLD parameters are configured on an interface, the parameter settings take effect only after MLD is enabled.
- If PIM (IPv6) and MLD need to be enabled on the same interface, enable PIM (IPv6) and MLD in sequence.
- Running the **mld enable** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.
- When Layer 2 and Layer 3 multicast are both deployed, pay attention to the following points:
  - If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable MLD on the corresponding VLANIF interface first, and then enable MLD snooping in the VLAN. If MLD snooping is enabled in the VLAN first, MLD cannot be enabled on the VLANIF interface.
  - If Layer 2 and Layer 3 multicast are both configured in a VLAN, you must delete the Layer 2 multicast configuration before you can modify or delete the Layer 3 multicast configuration. This means that you must disable MLD snooping in the VLAN first, then modify or disable the MLD and PIM (IPv6) configuration in the VLANIF interface view, and finally enable MLD snooping in the VLAN. Otherwise, the Layer 3 multicast configuration cannot be modified or deleted on the corresponding VLANIF interface.
  - If a VLANIF interface is shut down in the VLANIF interface view, Layer 2 multicast in the corresponding VLAN becomes ineffective accordingly. To make Layer 2 multicast effective, you must disable MLD snooping in the VLAN first, then disable MLD and PIM (IPv6) in the VLANIF interface view, and finally enable MLD snooping in the VLAN.
  - When both Layer 2 and Layer 3 multicast services are configured, traffic is forwarded based on Layer 3 multicast forwarding entries instead of Layer 2 multicast forwarding entries. This means that Layer 2 multicast provides physical outbound interfaces for Layer 3 multicast, implementing accurate forwarding of multicast data. In addition, the maximum number of Layer 3 multicast forwarding entries depends on the maximum number of Layer 2 multicast forwarding entries.
  - The default MLD version of the switch is MLDv2 (configured using the **mld version** *version* command); the default MLD snooping version of the

switch is MLDv1 (configured using the **mld-snooping version** *version* command). When Layer 2 and Layer 3 multicast services are both configured, MLD and MLD snooping must have the same version number.

Example

Enable MLD on VLANIF100 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld enable
```

Enable MLD on GE0/0/1 connected to a user network segment.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld enable
```

8.2.18 mld global limit

Function

The **mld global limit** command sets the maximum number of MLD entries that can be created on the entire switch.

The **undo mld global limit** command deletes the configured maximum number of MLD entries.

The following lists the maximum number of MLD entries allowed on each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S: 512
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S: 4096

Format

mld global limit *number*

undo mld global limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created on the entire switch.	The value is an integer that ranges from 1 to *The maximum number of MLD entries allowed by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of MLD entries reaches the limit, the system no longer creates MLD entries. To enable the switch to allow new join requests, you can either delete useless entries or modify the limit. Alternatively, you can enable static addition on a multicast group or source group.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **limit (MLD view)** command in the MLD view to set the maximum number of global MLD group entries. If both the **mld global limit** and **limit (MLD view)** commands are run, the smaller value takes effect.

Example

Set the maximum number of MLD entries that can be created on the switch to 500.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld global limit 500
```

8.2.19 mld group-policy

Function

The **mld group-policy** command configures an MLD group policy on an interface to limit the range of multicast groups that the hosts can join.

The **undo mld group-policy** command deletes the MLD group policy.

By default, no MLD group policy is configured on an interface, and the hosts can join any multicast groups.

Format

mld group-policy *acl6-number* [**1** | **2**]

undo mld group-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic or advanced IPv6 ACL6. This ACL6 defines the range of multicast groups.	The number of a basic ACL6 is an integer that ranges from 2000 to 2999. The number of an advanced ACL6 is an integer that ranges from 3000 to 3999.
1	Limits the range of multicast groups that MLDv1 hosts can join.	-
2	Limits the range of multicast groups that MLDv2 hosts can join.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control the range of multicast groups that hosts on the network attached to an interface can join, specify an ACL6 in the **mld group-policy** command. This configuration improves security of the MLD application. You can also run this command to prevent the switch from receiving Multicast Listener Report messages for specified groups.

If the MLD version is not specified, ACL6 rule is applicable to the two versions by default.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

An ACL6 defining the range of multicast groups has been created.

The **mld group-policy** command is used with the **acl ipv6** command. To use a numbered ACL6 in the MLD group policy:

- In the basic ACL6 view, set **source** in the **rule (basic ACL6 view)** command to the range of multicast groups that an interface can join.
- In the advanced ACL6 view, set **source** in the **rule (advanced ACL6 view)** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.

The configurations of the Named ACL6 and the advanced ACL6 are the same, and can implement filtering of both source addresses and multicast group addresses. The Named ACL6 can also be configured with the **time-range** parameter.

After the **mld group-policy** command is executed on an interface:

- The interface filters the received Report messages based on the ACL6 and maintains memberships only for the multicast groups permitted by the ACL6.
- The interface discards the Report messages that are denied by the ACL6. If the entries of the multicast groups denied by the ACL6 exist on the switch, the switch deletes these entries when the aging time of the entries expires.

Example

Create ACL6 2005, and configure a rule that allows hosts to receive data of multicast group FF13::101. Configure an MLD group policy on VLANIF100 and reference ACL6 2005 to allow hosts connected to the interface to join only multicast group FF13::101.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2005
[HUAWEI-acl6-basic-2005] rule permit source ff13::101 128
[HUAWEI-acl6-basic-2005] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld group-policy 2005
```

Create ACL6 2005, and configure a rule that allows hosts to receive data of multicast group FF13::101. Configure an MLD group policy on GE0/0/1 and reference ACL6 2005 to allow hosts connected to the interface to join only multicast group FF13::101.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2005
[HUAWEI-acl6-basic-2005] rule permit source ff13::101 128
[HUAWEI-acl6-basic-2005] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld group-policy 2005
```

8.2.20 mld ip-source-policy

Function

The **mld ip-source-policy** command enables filtering of Multicast Listener Report/ Done messages based on source addresses.

The **undo mld ip-source-policy** command disables filtering of MLD messages based on source addresses.

By default, a multicast device does not filter MLD messages based on source addresses.

Format

mld ip-source-policy *basic-acl6-number*

undo mld ip-source-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic ACL6, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD runs on receiver hosts and their directly connected multicast devices. A multicast device processes all received Multicast Listener Report/Done messages. For security purposes, you can configure the multicast device to filter Multicast Listener Report/Done messages received on an interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

For a numbered ACL, the **mld ip-source-policy** command works with the **acl ipv6** command. You can configure the source address of MLD messages by specifying the **source** parameter in the **rule** command in the basic ACL view.

Example

Configure VLANIF100 to accept only the Multicast Listener Report/Done messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld ip-source-policy 2001
```

Configure GE0/0/1 to accept only the Multicast Listener Report/Done messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld ip-source-policy 2001
```

8.2.21 mld lastlistener-queryinterval

Function

The **mld lastlistener-queryinterval** command sets the interval at which the MLD querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after receiving Multicast Listener Done messages from a host.

The **undo mld lastlistener-queryinterval** command restores the default value.

By default, the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is 1 second.

Format

mld lastlistener-queryinterval *interval*

undo mld lastlistener-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MLD querier receives a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages continuously to check for other members in the multicast group. The **mld lastlistener-queryinterval** command sets the interval at which the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If the querier receives no Multicast Listener Report message for a specified period, the querier stops forwarding data to the multicast group. The period is calculated by multiplying *interval* by *robust-value*. To set *robust-value*, run the **mld robust-count** or **robust-count (MLD view)** command.

If the querier receives a Multicast Listener Report message from a host within the maximum response time, the querier maintains the membership of the multicast group. Otherwise, the querier considers that the last member has left the group and does not maintain the membership of the multicast group.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld lastlistener-queryinterval** command is the same as that of the **lastlistener-queryinterval** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query message to 3 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld lastlistener-queryinterval 3
```

Set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query message to 3 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld lastlistener-queryinterval 3
```

8.2.22 mld limit

Function

The **mld limit** command sets the maximum number of MLD group memberships that the current interface can maintain.

The **undo mld limit** command restores the maximum number of MLD group memberships that the current interface can maintain to the default value.

The following lists the maximum number of MLD group memberships that can be maintained on the current interface of each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S 512
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S: 2048
- S6720S-EI, S6735-S, S6720-EI: 4096

Format

mld limit *number* [**except** *acl6-number*]

undo mld limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD group memberships that can be maintained on the current interface.	The value is an integer that ranges from 1 to *The maximum number of MLD group memberships that can be maintained on the current interface by default*. **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.
except	Specifies the range of multicast groups that are not limited by the specified maximum number.	-
acl6-number	Specifies the basic or advanced ACL6.	The value is an integer. The number of the basic ACL6 ranges from 2000 to 2999. The basic ACL6 filters group addresses only, without distinguishing (*, G) entries and (S, G) entries. The number of the advanced ACL6 ranges from 3000 to 3999. The advanced ACL6 filters (S, G) entries of the interface only.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of MLD entries reaches the limit, the system does not create any MLD entries. To allow more new join requests, delete unnecessary entries or increase the limit. Alternatively, configure static multicast groups or source-group bindings on interfaces.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If **except** is not set in the command, the maximum number of MLD entries corresponding to all the groups or source/groups is limited.

Before setting **except**, configure the associated ACL6. The interface then filters the received MLD Join messages according to the ACL6. The maximum number of entries corresponding to the multicast groups that match the ACL6 is not limited.

The **mld limit** command must be used with ACL6 configuration commands. When configuring ACL6 rules, note that:

- In the basic ACL6 view, specify the **source** parameter in the **rule (basic ACL6 view)** command for setting the range of multicast groups whose MLD entries do not need to be limited.
- In the advanced ACL6 view, specify the **source** parameter in the **rule (advanced ACL6 view)** command for setting the range of sources that are allowed to send multicast data to the multicast groups. Specify the **destination** parameter in the **rule (advanced ACL6 view)** command for setting the range of multicast groups whose MLD entries do not need to be limited.

The Named ACL and the advanced ACL can be configured based on the same rules, and can implement filtering of both source addresses and multicast group addresses. The **time-range** parameter takes effect in the **rule** command only for the Named ACL.

Example

Set the maximum number of MLD entries that can be created on the VLANIF100 to 500.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld limit 500
```

Create the advanced ACL6 with the number being 3100; set the maximum number of MLD entries that can be created on VLANIF100 to 500; allow the hosts to receive messages from the specific-source multicast group (FC00:0:0:2001::1, FF3E::1). That is, the specific-source multicast group (FC00:0:0:2001::1, FF3E::1) is not limited by the maximum number of MLD entries.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] acl ipv6 3100
[HUAWEI-acl6-adv-3100] rule permit ipv6 source fc00:0:0:2001::1 64 destination ff3e::1 64
[HUAWEI-acl6-adv-3100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld limit 500 except 3100
```

Set the maximum number of MLD entries that can be created on the GE0/0/1 to 500.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld limit 500
```

8.2.23 mld max-response-time

Function

The **mld max-response-time** command sets the maximum response time for MLD General Query messages on an interface.

The **undo mld max-response-time** command restores the default maximum response time for General MLD Query messages.

By default, the maximum response time for MLD General Query messages is 10s on an interface.

Format

mld max-response-time *interval*

undo mld max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for MLD General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send Multicast Listener Report messages immediately after receiving MLD General Query messages, the querier on the local network segment may receive a large number of Multicast Listener Report messages from the hosts at the same time. This may cause congestion on the network.

To avoid such situations, MLD messages specify the maximum response time for MLD General Query messages. When a host receives an MLD Query message, the host starts a timer for the multicast group that it joins. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Multicast Listener Report message to the querier.

The maximum response time specifies the deadline for the host to send a Multicast Listener Report message. A proper maximum response time allows hosts to respond to MLD Query messages and prevents hosts from sending Report messages at the same time.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The function of the **mld max-response-time** command is the same as that of the **max-response-time (MLD view)** command used in the MLD view. The configuration in the MLD view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the maximum response time for MLD General Query messages to 8 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld max-response-time 8
```

Set the maximum response time for MLD General Query messages to 8 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld max-response-time 8
```

8.2.24 mld on-demand

Function

The **mld on-demand** command enables the MLD on-demand function. This function enables a querier to maintain group memberships according to requirements of group members, without sending Query messages. After MLD on-demand is enabled on an interface, dynamic MLD entries on the interface will never age out.

The **undo mld on-demand** command restores the default configuration.

By default, a querier does not maintain group memberships according to requirements of group members, and dynamic entries are aged out when the aging time expires.

Format

mld on-demand

undo mld on-demand

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a standard MLD working process, a querier sends General Query messages periodically and collects group membership information based on received Multicast Listener Report and Done messages. Group members respond to every Query message they receive. The querier stops sending Query messages after MLD on-demand is configured, reducing MLD packets exchanged between the querier and receiver hosts.

The MLD on-demand function enables a querier to maintain group memberships based on Report messages sent from hosts, reducing traffic transmitted between the querier and receiver hosts.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The **mld on-demand** command can be used on the querier only.
- If dynamic MLD entries have been generated on the querier, run the **reset mld group** command to clear these dynamic MLD entries before running the **mld on-demand** command.
- After the **mld on-demand** command is executed on an interface:
  - The interface no longer sends MLD Query messages.

  - MLD group entries are generated after the interface receives Multicast Listener Report messages and will never age out.
  - When the interface receives a Multicast Listener Done message, it deletes the corresponding MLD group entry.
- The **mld on-demand** configuration of the VLANIF interface and the **mld-snooping enable** command in a VLAN are mutually exclusive.

Example

Enable the MLD on-demand function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld on-demand
```

Enable the MLD on-demand function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld on-demand
```

8.2.25 mld prompt-leave

Function

The **mld prompt-leave** command enables the fast leave function on an interface. This function enables an MLD querier to delete MLD entries immediately after receiving Multicast Listener Done messages from group members, without sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.

The **undo mld prompt-leave** command disables fast leave on an interface.

By default, an MLD querier sends a Multicast Address Specific Query message or Multicast Address and Source Specific Query message after receiving a Multicast Listener Done message for a specific multicast group.

Format

mld prompt-leave [**group-policy** *acl6-number*]

undo mld prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies an MLD multicast group policy. If this parameter is specified, the fast leave function takes effect only for multicast groups specified in the policy. When specifying this parameter, ensure that the referenced ACL6 has been configured. The interface filters Multicast Listener Done messages on the interface based on the ACL6. ● If a host leaves a multicast group in the range permitted by the ACL6, the device immediately deletes the multicast group entry without sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. ● If a host leaves a multicast group out of the range permitted by the ACL6, the device sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If this parameter is not specified, the fast leave function takes effect for all multicast groups.	-
acl6-number	Specifies the number of a basic ACL6 or an advanced ACL6. This ACL6 defines the range of multicast groups.	The number of a basic ACL6 is an integer that ranges from 2000 to 2999. The number of an advanced ACL6 is an integer that ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, an interface on the MLD querier connects to only one receiver host. If the host frequently switches between multiple multicast groups, you can configure fast leave on the interface of the querier so that the interface can quickly respond to Multicast Listener Done messages sent from the host. After fast leave is configured, the querier does not send a Multicast Address Specific Query message or Multicast Address and Source Specific Query message after receiving a Multicast Listener Done message. Instead, the querier directly notifies the upstream multicast device that the host has left the multicast group. The fast leave function reduces delay in response to Multicast Listener Done messages and saves network bandwidth.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- When an interface has more than one receiver connected, enabling fast leave interrupts multicast traffic of the other receivers in the multicast group. You are advised to enable this function on interfaces with only one receiver.
- When configuring an ACL6 to specify the range of multicast groups, pay attention to the following points:
  - When you run the **rule** command in the view of a basic ACL6, set **source** to the address range of multicast groups that hosts can fast leave.
  - When you run the **rule** command in the view of an advanced ACL6, set **source** to the multicast source address and **destination** to the range of multicast groups that hosts can fast leave.

Example

Configure fast leave on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld prompt-leave
```

Configure fast leave on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld prompt-leave
```

8.2.26 mld query ip-source-policy

Function

The **mld query ip-source-policy** command configures MLD Query message filtering based on source addresses.

The **undo mld query ip-source-policy** command restores the default configuration.

By default, no source address-based MLD Query message filtering is configured.

Format

mld query ip-source-policy *basic-acl6-number*

undo mld query ip-source-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic ACL6, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged MLD Query messages with an IPv6 address smaller than the querier IPv6 address, the querier is replaced by the attacker. As a result, the real querier cannot respond to Multicast Listener Report messages from group members and bandwidth is wasted. Source address-based MLD Query message filtering can protect the querier from such attacks. With this function configured, the switch accepts only the MLD Query messages with source addresses permitted by the specified ACL6. This function controls querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- MLD Query messages are encapsulated into IPv6 messages. This command is used to filter the source addresses in IPv6 headers.
- After you configure source address-based MLD Query message filtering on an interface, the interface filters out the MLD Query messages whose source addresses do not match a specified ACL6 rule.

Example

Configure VLANIF100 to receive the MLD Query messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld query ip-source-policy 2001
```

Configure GE0/0/1 to receive the MLD Query messages with the source address FC00::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld query ip-source-policy 2001
```

8.2.27 mld require-router-alert

Function

The **mld require-router-alert** command configures an interface to discard MLD messages without the Router-Alert option.

The **undo mld require-router-alert** command disables an interface from checking for the Router-Alert option in MLD messages.

By default, all received MLD messages are processed, including the MLD messages without the Router-Alert option.

Format

mld require-router-alert

undo mld require-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a message to the routing protocol module for processing only when the destination address of the message is a local interface address. Destination addresses of MLD messages are multicast addresses but not addresses of interfaces on multicast devices. Therefore, multicast devices do not send MLD messages to the MLD module for processing, and the MLD module cannot maintain group memberships.

The Router-Alert option in the IPv6 header of an MLD message solves this problem. If an MLD message contains the Router-Alert option, the device sends the message to the MLD module.

You can configure the device to accept only MLD messages with the Router-Alert option to improve MLD security.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld require-router-alert** command is the same as that of the **require-router-alert (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The system prefers the configuration in the interface view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to discard MLD messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld require-router-alert
```

Configure GE0/0/1 to discard MLD messages without the Router-Alert option.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld require-router-alert
```

8.2.28 mld robust-count

Function

The **mld robust-count** command sets a robustness variable of an MLD querier on an interface.

The **undo mld robust-count** command restores the default robustness variable of an MLD querier.

By default, the robustness variable of an MLD querier is 2.

Format

mld robust-count *robust-value*

undo mld robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an MLD querier.	The value is an integer that ranges from 2 to 5.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD querier robustness variable specifies the retransmission count of MLD packets to minimize the impact of packet loss on the network.

On a shared network segment, a querier maintains MLD group memberships. The robustness variable affects the timeout period of group memberships. The timeout period of the group membership is calculated using the formula:

Timeout period of the group memberships = Interval for sending MLD General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The interval for sending General Query messages is configured using the **mld timer query** or **timer query (MLD view)** command.
- Number of times the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages

  When receiving a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages a certain number of times specified by the robustness variable to check whether the group has members. When the querier receives a Multicast Listener Report message indicating that source-group mapping changes, the querier sends Multicast

Address and Source Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is set using the **mld lastlistener-queryinterval** or **lastlistener-queryinterval (MLD view)** command.

A larger robustness variable makes an MLD querier more robust but increases the timeout period of group memberships.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld robust-count** command is the same as that of the **robust-count (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the robustness variable of the querier on VLANIF100 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld robust-count 3
```

Set the robustness variable of the querier on GE0/0/1 to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld robust-count 3
```

8.2.29 mld send-router-alert

Function

The **mld send-router-alert** command configures an interface to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo mld send-router-alert** command disables an interface from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, the IPv6 headers of MLD messages sent by an interface contain the Router-Alert option.

Format

mld send-router-alert

undo mld send-router-alert

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch sends MLD messages that contain the Router-Alert option in IPv6 headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo mld send-router-alert** command to configure the switch to send MLD messages without the Router-Alert option. The **mld send-router-alert** command is usually used together with the **mld require-router-alert** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld send-router-alert** command is the same as that of the **send-router-alert (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Configure VLANIF100 to send MLD messages with the Router-Alert option in their IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld send-router-alert
```

Configure GE0/0/1 to send MLD messages with the Router-Alert option in their IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld send-router-alert
```

8.2.30 mld ssm-mapping enable

Function

The **mld ssm-mapping enable** command enables MLD SSM mapping on an interface.

The **undo mld ssm-mapping enable** command disables MLD SSM mapping on an interface.

By default, MLD SSM mapping is disabled on an interface.

Format

mld ssm-mapping enable

undo mld ssm-mapping enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM model allows MLDv2 hosts to specify the multicast sources from which they want to receive data. However, some hosts can only run MLDv1. To allow these hosts to use SSM, configure MLD SSM mapping on the switch. MLD SSM mapping is implemented based on static SSM mapping entries on the switch. The switch converts (*, G) information in MLDv1 Multicast Listener Report messages to (S, G) information according to static SSM mapping entries to provide the SSM service for MLDv1 hosts.

The **mld ssm-mapping enable** command enables MLD SSM mapping on an interface. The mappings between SSM sources and multicast group addresses take effect only when MLD SSM mapping is enabled on an interface. SSM mapping entries are configured using the **ssm-mapping (MLD view)** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

SSM mapping enabled on an interface is irrelevant to the version number of MLD.

Example

Enable MLD SSM mapping on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld ssm-mapping enable
```

Enable MLD SSM mapping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld ssm-mapping enable
```

8.2.31 mld static-group

Function

The **mld static-group** command configures a static multicast group on an interface.

The **undo mld static-group** command deletes a static multicast group from an interface.

By default, no static multicast group is configured on an interface.

Format

mld static-group *ipv6-group-address* [**inc-step-mask** *ipv6-group-mask-length* **number** *group-number*] [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**inc-step-mask** *ipv6-group-mask-length* **number** *group-number*] [**source** *ipv6-source-address*] }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies the IPv6 address of the multicast group that an interface statically joins. In batch configuration mode, this parameter specifies the initial address of the multicast group addresses.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Parameter	Description	Value
inc-step-mask *ipv6-group-mask-length*	Specifies the incremental length of the step mask in batch configuration mode.	The value is an integer that ranges from 8 to 128.
number *group-number*	Specifies the number of group addresses in batch configuration mode.	The value is an integer that ranges from 2 to 512.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
all	Specifies all the multicast groups that the interface statically joins.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following are two scenarios in which you can configure static multicast groups on user-side interfaces of the switch:

- There are long-term group members on a shared network segment, and the switch needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the switch considers that the multicast group always has members on the network segment of the interface. Therefore, the switch always forwards multicast data of the multicast group.

The **mld static-group** command is used on an interface connected to user hosts. The command can configure a single group or source-group binding on an interface or configure multiple groups or source-group bindings in a batch.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- After multicast groups are configured in batches for the first time, if you only modify the value of *group-number* but not the value of *ipv6-group-address* or *ipv6-group-mask-length* to configure multicast groups in batches again, the new configurations overwrite the corresponding original configurations.
- After you run the **mld static-group** command on an interface connected to user hosts, the entries matching the MLD groups that the interface statically joins never time out. The switch considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment where the interface resides.
- You can configure overlapping multicast group addresses in different batch configurations. When you configure multiple static multicast groups in a batch on an interface, do not delete any static group configuration before the system completes the batch static group configuration.
- If a user host no longer needs to receive multicast data of a static group, delete the static group configuration.
- When the interface that connects a multicast device to the user network segment joins a multicast group in both dynamic and static modes, the interface preferentially joins the multicast group in static mode if a conflict occurs.
- Running the **mld static-group** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

Example

Configure static multicast group FF13::101 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff13::101
```

Configure the switch to forward multicast packets from multicast source FC00::101 to multicast group FF14::202 through VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff14::202 source fc00::101
```

Add VLANIF100 statically to two multicast groups in a batch. Set the start multicast group address to FF25::1 and the step mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff25::1 inc-step-mask 24 number 2
```

Add VLANIF100 statically to two multicast source/groups in a batch. Set the start multicast group address to FF33::1, the source address to FC00::101, and the step mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld static-group ff33::1 inc-step-mask 24 number 2 source fc00::101
```

Configure static multicast group FF13::101 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld static-group ff13::101
```

8.2.32 mld timer other-querier-present

Function

The **mld timer other-querier-present** command sets the other querier present timer on an interface.

The **undo mld timer other-querier-present** command restores the default value of the other querier present timer on an interface.

By default, the Keepalive period of the other queriers is calculated as follows:

Other querier present timer = Robustness variable x Interval for sending MLD General Query messages + 1/2 x Maximum response time

If the default values of the robustness variable, interval for sending MLD General Query messages, and maximum response time are used, the other querier present timer value is 255 seconds.

Format

mld timer other-querier-present *interval*

undo mld timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the MLD querier to send Query messages to hosts on the network segment. To create and maintain normal group memberships, non-queriers running MLD start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld timer other-querier-present** command is the same as that of the **timer other-querier-present (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer is shorter than the interval for sending General Query messages, the querier election is triggered frequently.

Example

On VLANIF100, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld timer other-querier-present 200
```

On GE0/0/1, set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld timer other-querier-present 200
```

8.2.33 mld timer query

Function

The **mld timer query** command sets the interval at which an interface sends MLD General Query messages.

The **undo mld timer query** command restores the default interval at which an interface sends MLD General Query messages.

By default, an interface sends MLD General Query messages at an interval of 125s.

Format

mld timer query *interval*

undo mld timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an interface sends MLD General Query messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier checks whether a local network segment has multicast group members by sending MLD General Query messages at an interval, known as the general query interval. You can set the general query interval based on needs of your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the interval for sending General Query messages.

The robustness variable can be set using the **mld robust-count** or **robust-count (MLD view)** command.

- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and switch resources are consumed in this case.
- The function of the **MLD timer query** command is the same as that of the **timer query (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The system prefers the configuration in the interface view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the interval at which VLANIF100 sends General Query messages to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld timer query 200
```

Set the interval at which GE0/0/1 sends General Query messages to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld timer query 200
```

8.2.34 mld ttl-check

Function

The **mld ttl-check** command enables the device to check the TTL values in received MLD Report, Done, and Query messages on a specific interface.

The **undo mld ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received MLD Report, Done, and Query messages on an interface.

Format

mld ttl-check

undo mld ttl-check

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables TTL check for MLD Report, Leave, and Query messages on an interface. This function protects the system against attacking MLD messages by dropping the messages of which the TTL value is not 1. By default, TTL values of MLD messages are not checked on an interface.

You can also configure TTL check for MLD Report, Leave, and Query messages by using the **ttl-check** command in the MLD view. This command takes effect for all MLD-enabled interfaces.

Precautions

If both the **mld ttl-check** and **ttl-check** commands are run, the **mld ttl-check** configuration in the interface view takes precedence over the **ttl-check** configuration in the MLD view.

Example

Enable TTL check for MLD Report, Leave, and Query messages on a physical interface.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mld ttl-check
```

Enable TTL check for MLD Report, Leave, and Query messages on a VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] quit
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] mld ttl-check
```

8.2.35 mld version

Function

The **mld version** command specifies an MLD version on an interface.

The **undo mld version** command restores the default MLD version on an interface.

By default, an interface runs MLDv2.

Format

mld version *version*

undo mld version

Parameters

Parameter	Description	Value
version	Specifies the MLD version running on the interface.	The value is integer that ranges from 1 to 2.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast switch can only identify MLD messages of a version earlier than its own MLD version. To ensure normal MLD operation, set on the switch an MLD version the same as or later than that running on user hosts.

If many switches exist on a shared network segment, configure the same MLD version on all switch interfaces connected to hosts. If multicast devices run MLD of different versions, errors may occur in MLD operation because interfaces running different MLD versions send messages in different formats.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Configure MLDv2 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] mld version 2
```

Configure MLDv2 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] mld version 2
```

8.2.36 require-router-alert (MLD view)

Function

The **require-router-alert** command configures the switch to discard MLD messages without the Router-Alert option.

The **undo require-router-alert** command disables the switch from checking the Router-Alert option in MLD messages.

By default, the switch does not check whether the received MLD messages contain Router-Alert options in IPv6 headers, and it accepts all the received MLD messages.

Format

require-router-alert

undo require-router-alert

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a message to the routing protocol module for processing only when the destination address of the message is a local interface address. Destination addresses of MLD messages are multicast addresses but not addresses of interfaces on multicast devices. Therefore, multicast devices do not send MLD messages to the MLD module for processing, and the MLD module cannot maintain group memberships.

The Router-Alert option in the IPv6 header of an MLD message solves this problem. If an MLD message contains the Router-Alert option, the device sends the message to the MLD module.

You can configure the device to accept only MLD messages with the Router-Alert option to improve MLD security.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld require-router-alert** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, configure the switch to discard the MLD messages that do not contain Router-Alert options in IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] require-router-alert
```

8.2.37 reset mld control-message counters

Function

The **reset mld control-message counters** command deletes statistics of MLD messages.

Format

reset mld control-message counters [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears MLD packet statistics on a specified interface. If this parameter is not specified, MLD packets on all interfaces are deleted.	-

Parameter	Description	Value
message-type	Clears statistics about MLD messages of a specified type. If this parameter is not specified, the command clears statistics about MLD messages of all types.	-
query	Clears the number of received Query messages.	-
report	Clears the number of received Multicast Listener Report messages.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After statistics about MLD messages are deleted, MLD still operates properly.

Example

Delete statistics about MLD messages from all interfaces.

```
<HUAWEI> reset mld control-message counters
```

Delete statistics about MLD messages from VLANIF100.

```
<HUAWEI> reset mld control-message counters interface vlanif 100
```

8.2.38 reset mld explicit-tracking

Function

The **reset mld explicit-tracking** command deletes hosts that dynamically join a multicast group using MLD from an interface.

Format

reset mld explicit-tracking { **all** | **interface** *interface-type interface-number* [**host** *ipv6-host-address* [**group** *ipv6-group-address* [**source** *ipv6-source-address*]]] }

Parameters

Parameter	Description	Value
all	Indicates information about all MLD hosts.	-
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command deletes hosts that dynamically join the host group using MLD from all interfaces.	-
host *ipv6-host-address*	Specifies the link-local address of a host.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
group *ipv6-group-address*	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete hosts that dynamically join a multicast group using MLD from an interface. A host can rejoin the multicast group after being deleted from this group.

Example

Delete the host FE80::101 that joins multicast group FF23::101 through MLD on VLANIF100.

```
<HUAWEI> reset mld explicit-tracking interface vlanif 100 host fe80::101 group ff23::101
```

Delete the host FE80::101 that joins the (FC00:0:0:1::12, FF23::101) forwarding entry from VLANIF100.

```
<HUAWEI> reset mld explicit-tracking interface vlanif 100 host fe80::101 group ff23::101 source
fc00:0:0:1::12
```

8.2.39 reset mld group

Function

The **reset mld group** command deletes dynamic MLD entries on interfaces.

Format

reset mld group all

reset mld group interface *interface-type interface-number* { **all** | *ipv6-group-address* [*ipv6-group-mask-length*] [*ipv6-source-address* [*ipv6-source-mask-length*]] }

Parameters

Parameter	Description	Value
all	The first **all** deletes dynamic MLD entries on all interfaces. The second **all** deletes all MLD entries on a specified interface.	-
interface *interface-type interface-number*	Deletes dynamic MLD entries on a specified interface.	-
ipv6-group-address	Deletes dynamic MLD entries of a specified multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 8 to 128.

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
ipv6-source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 128.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command deletes all the dynamic MLD group memberships on an interface, including common group memberships and group memberships established with SSM mapping. This command cannot delete statically configured MLD group memberships.

A host can rejoin the multicast group after being deleted from this group.

NOTICE

After dynamic MLD entries on an interface are deleted, the interface cannot receive multicast data. Exercise caution before running this command.

Example

Delete dynamic MLD entries within the range of FF03::101:0 to FF03::101:FFFF on VLANIF100.

```
<HUAWEI> reset mld group interface vlanif 100 ff03::101:0 112
```

8.2.40 reset mld group ssm-mapping

Function

The **reset mld group ssm-mapping** command deletes multicast group entries established with MLD SSM mapping.

Format

reset mld group ssm-mapping all

reset mld group ssm-mapping interface *interface-type interface-number* { **all** | *ipv6-group-address* [*ipv6-group-mask-length*] }

Parameters

Parameter	Description	Value
all	The first **all** deletes multicast group entries established with MLD SSM mapping on all interfaces. The second **all** deletes all multicast group entries established with MLD SSM mapping on a specified interface.	-
interface *interface-type interface-number*	Deletes the multicast group entries established with MLD SSM mapping on a specified interface.	-
ipv6-group-address	Specifies an IPv6 multicast group address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 8 to 128.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command is valid only on the multicast groups that an interface has dynamically joined, and deletes only the MLDv1 multicast group entries within the range of SSM group addresses.

SSM mapping can be re-configured after being deleted.

NOTICE

After the multicast group entries established with MLD SSM mapping on an interface are deleted, the interface cannot receive multicast data. Exercise caution before running this command.

Example

Delete multicast group entries established with MLD SSM mapping within the range of FF13::101:0 to FF13::101:FFFF on VLANIF100.

```
<HUAWEI> reset mld group ssm-mapping interface vlanif 100 ff13::101:0 112
```

8.2.41 robust-count (MLD view)

Function

The **robust-count** command sets a global robustness variable for an MLD querier.

The **undo robust-count** command restores the default robustness variable.

By default, the robustness variable of an MLD querier is 2.

Format

robust-count *robust-value*

undo robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an MLD querier.	The value is an integer that ranges from 2 to 5.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD querier robustness variable specifies the retransmission count of MLD packets to minimize the impact of packet loss on the network.

On a shared network segment, a querier maintains MLD group memberships. The robustness variable affects the timeout period of group memberships. The timeout period of the group membership is calculated using the formula:

Timeout period of the group memberships = Interval for sending MLD General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The interval for sending General Query messages is configured using the **mld timer query** or **timer query (MLD view)** command.

- Number of times the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages

  When receiving a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages a certain number of times specified by the robustness variable to check whether the group has members. When the querier receives a Multicast Listener Report message indicating that source-group mapping changes, the querier sends Multicast Address and Source Specific Query messages a certain number of times specified by the robustness variable. The interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is set using the **mld lastlistener-queryinterval** or **lastlistener-queryinterval (MLD view)** command.

A larger robustness variable makes an MLD querier more robust but increases the timeout period of group memberships.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld robust-count** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the current interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the robustness variable of an MLD querier to 3 in the MLD view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] robust-count 3
```

8.2.42 send-router-alert (MLD view)

Function

The **send-router-alert** command configures the switch to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo send-router-alert** command disables the switch from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, the MLD messages sent by the switch contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the MLD messages sent by the switch contain the Router-Alert option in their IPv6 headers. If the switch needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the switch to send MLD messages without the Router-Alert option. The **send-router-alert** command is usually used together with the **require-router-alert (MLD view)** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld send-router-alert** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, configure the switch to send MLD packets with the Router-Alert option in IPv6 headers.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] send-router-alert
```

8.2.43 ssm-mapping (MLD view)

Function

The **ssm-mapping** command configures an SSM mapping entry to map a multicast source to a group address.

The **undo ssm-mapping** command deletes an SSM mapping entry.

By default, no SSM mapping entry is configured.

Format

ssm-mapping *ipv6-group-address ipv6-group-mask-length ipv6-source-address*

undo ssm-mapping { **all** | *ipv6-group-address ipv6-group-mask-length* [*ipv6-source-address*] }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies the IPv6 address of a multicast group configured with SSM mapping.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer, which can be 16, 32, 64, or 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
all	Deletes all the configured static SSM mapping entries.	-

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts that support only MLDv1 cannot join SSM groups. To enable multicast devices to provide the SSM service for these hosts, configure SSM mapping on the multicast devices. An SSM mapping entry maps a multicast source to a multicast group. After SSM mapping entries are configured on a multicast device, the device can convert (*, G) information in Report messages of MLDv1 to (S, G) information.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- You can configure multiple static SSM mapping entries by running the **ssm-mapping** command several times.
- To delete an SSM mapping entry, run the **undo ssm-mapping** *ipv6-group-address ipv6-group-mask-length* [*ipv6-source-address*] command. The **undo ssm-mapping all** command deletes all the SSM mapping entries. Exercise caution before running this command.

Example

Configure an SSM mapping entry mapping the source address FC00::1 to group address FF35::1/128.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] ssm-mapping ff35::1 128 fc00::1
```

8.2.44 timer other-querier-present (MLD view)

Function

The **timer other-querier-present** command sets a global other querier present timer.

The **undo timer other-querier-present** command restores the default value of the other querier present timer.

By default, the Keepalive period of the other queriers is calculated as follows:

Other querier present timer = Robustness variable x Interval for sending MLD General Query messages + 1/2 x Maximum response time

If the default values of the robustness variable, interval for sending MLD General Query messages, and maximum response time are used, the other querier present timer value is 255 seconds.

Format

timer other-querier-present *interval*

undo timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the MLD querier to send Query messages to hosts on the network segment. To create and maintain normal group memberships, non-queriers running MLD start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld timer other-querier-present** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer is shorter than the interval for sending General Query messages, the querier election is triggered frequently.

Example

Set the other querier present timer to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] timer other-querier-present 200
```

8.2.45 timer query (MLD view)

Function

The **timer query** command sets a global interval for sending MLD General Query messages.

The **undo timer query** command restores the default interval for sending MLD General Query messages.

By default, the interval for sending MLD General Query messages is 125 seconds.

Format

timer query *interval*

undo timer query

Parameters

Parameter	Description	Value
interval	Interval for sending MLD General Query messages	The value is an integer that ranges from 1 to 18000, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier checks whether a local network segment has multicast group members by sending MLD General Query messages at an interval, known as the general query interval. You can set the general query interval based on needs of your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages a certain number of times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the interval for sending General Query messages. The robustness variable can be set using the **mld robust-count** or **robust-count (MLD view)** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and switch resources are consumed in this case.
- The function of this command is the same as that of the **mld timer query** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the interval for sending MLD General Query messages to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] timer query 200
```

8.2.46 ttl-check (MLD view)

Function

The **ttl-check** command enables the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces.

The **undo ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received MLD Report, Done, and Query messages.

Format

ttl-check

undo ttl-check

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

To protect a device against MLD message attacks, run the **ttl-check** command to enable the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces and discard such a message if its TTL value is not 1.

Example

Enable the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] mld
[HUAWEI-mld] ttl-check
```

8.3 IPv4 PIM Configuration Commands

8.3.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the PIM multi-instance feature.

8.3.2 bsm semantic fragmentation (IPv4)

Function

The **bsm semantic fragmentation** command enables BSR message fragmentation.

The **undo bsm semantic fragmentation** command disables BSR message fragmentation.

By default, BSR message fragmentation is not enabled.

Format

bsm semantic fragmentation

undo bsm semantic fragmentation

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BSR message carries information about all C-RPs on the network. Therefore, if there is a large number of C-RPs on the network, the length of a BSR message exceeds the MTU of the outgoing interface. As a result, the BSR message cannot be processed and RP election fails. Consequently, multicast services cannot be transmitted normally. In this case, you can enable BSR message fragmentation to ensure that the devices on the network can learn consistent RP information and MDTs can be successfully established.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

You can also configure IP fragmentation to solve the preceding problem. The difference between IP fragmentation and BSR message fragmentation is as follows:

- If IP fragmentation is enabled, the protocol layer transmits the entire BSR message up to the IP layer regardless of the length of the BSR message. The BSR message is then fragmented at the IP layer. During the transmission of BSR message fragments to the destination, if one fragment is lost, the destination cannot parse the entire BSR message. As a result, the destination cannot learn RP information and MDTs cannot be established, which causes a multicast data forwarding failure.
- If BSR message fragmentation is enabled, the protocol layer directly fragments a long BSR message. During the transmission of BSR message fragments to the destination, if one fragment is lost, only the information carried in this fragment is lost. As a result, only MDTs corresponding to the information carried in the lost fragments cannot be established. Since the other BSR message fragments can still reach the destination, the corresponding MDTs can be correctly established.

BSR message fragmentation is recommended because IP fragmentation causes all fragments to become unavailable when fragment information is lost.

Precautions

Enable BSR message fragmentation on all devices on the network. If BSR message fragmentation is not enabled on some devices, RP information on these devices is inconsistent with that on other devices and MDTs cannot be established on these devices.

Example

Enable BSR message fragmentation in the public network instance PIM view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] bsm semantic fragmentation
```

8.3.3 bsr-policy (IPv4)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses. Then the switch drops the BSR messages sent from the addresses out of this range to defend against BSR spoofing.

The **undo bsr-policy** command restores the default configuration.

By default, the range of BSR addresses is not limited, and all BSR packets are considered valid.

Format

bsr-policy *basic-acl-number*

undo bsr-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the basic ACL number. The ACL defines the filtering policy for the range of source addresses of BSR packets. This parameter corresponds to *basic-acl-number* in the **acl** command.	The value is an integer that ranges from 2000 to 2999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any switch as a C-BSR to take part in BSR election. Once a switch is elected as the BSR, the switch is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, take the following measures:

- Certain hosts try changing the RP mapping to spoof the switch by forging BSR packets.

  Solution: The attack often occurs on edge switches because the BSR packet is a multicast packet with the TTL value of 1. As the BSR is inside the network and hosts are outside the network, the switches can perform neighbor checks and RPF checks on the received BSR packets to prevent the attack.
- Certain attackers control the switch on the network, or the switch accesses the network. The attackers configure the switch as a C-BSR, and help the switch win the BSR election. The attackers obtain the right of advertising RP information in the network.

  Solution: After the switch is configured as a C-BSR, the switch spreads multicast BSR packets in the network. The BSR packets have a TTL value of 1 and are forwarded hop by hop. As long as the neighboring switch cannot receive the packets, the packets are not spread in the entire network. The solution is to use the **bsr-policy** command on every switch in the network to limit the valid BSR range. For example, only switches 10.1.1.1/32 and 10.1.1.2/32 are elected as BSRs; therefore, the switches do not receive or forward other BSR packets.

The two countermeasures mentioned above can partially protect BSRs in the network. However, if attackers control a valid BSR, problems can still be caused on the network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

After the **bsr-policy** command is run, the switch accepts only BSR messages matching the configured policy.

Precautions

The **bsr-policy** command and the **acl** command are used together. In the ACL view, you can set the source address range for BSR packets by specifying the **source** parameter in the **rule** command.

Example

In the public network instance PIM view, configure address 10.1.1.0/24 as the valid BSR address range.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.1.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] quit
```

```
[HUAWEI] pim
[HUAWEI-pim] bsr-policy 2001
```

8.3.4 c-bsr (IPv4)

Function

The **c-bsr** command configures a C-BSR.

The **undo c-bsr** command restores the default configuration.

By default, the C-BSR is not configured.

Format

c-bsr *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface. C-BSR is configured on this interface. PIM-SM must be enabled on this interface to make the configuration effective. **NOTE** To avoid frequent protocol changes caused by interface flapping, using loopback interfaces is recommended.	-
hash-length	Specifies the hash mask length of the C-BSR. The mask is used in a hash function to calculate the RP.	The value is an integer that ranges from 0 to 32. By default, the value is 30.
priority	Specifies a priority of the C-BSR. The greater the value, the higher the priority of the C-BSR.	The value is an integer ranging from 0 to 255. By default, the value is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more C-BSRs need to be configured in a PIM-SM domain. A BSR is elected from C-BSRs and is responsible for collecting C-RP information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM domain.

The process of BSR election is as follows:

1. Each C-BSR considers itself as the BSR of the local PIM-SM domain and uses IP address of this interface as the address of the BSR to send Bootstrap messages.
2. When a C-BSR receives a Bootstrap message from other devices, it compares the BSR in the received Bootstrap message with the current BSR. The BSR with the highest priority is preferred. If BSRs have the same priority, the BSR with a larger IP address is preferred. If the BSR carried in the received Bootstrap message is superior to the current BSR, the C-BSR replaces its BSR address with the address of the BSR carried in the received Bootstrap message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Before configuring an interface as a C-BSR, enable PIM-SM on the interface.

For the multicast BSR messages learned through the GRE tunnel, you need to configure a static multicast route to ensure that the next hop to the BSR is a GRE interface. You need to configure static multicast routes properly to avoid routing loops.

Example

In the PIM view of public network instance, configure a C-BSR on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim sm
[HUAWEI-Vlanif100] quit
[HUAWEI] pim
[HUAWEI-pim] c-bsr vlanif 100
```

In the PIM view, configure a C-BSR on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] pim
[HUAWEI-pim] c-bsr gigabitethernet 0/0/1
```

8.3.5 c-bsr admin-scope

Function

The **c-bsr admin-scope** command configures a BSR administrative scope in a PIM-SM domain.

The **undo c-bsr admin-scope** command restores the default configuration.

By default, no BSR administrative scope is configured.

Format

c-bsr admin-scope

undo c-bsr admin-scope

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BSR that serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative domains and a global domain. This can reduce the workload of a single BSR and designate a private-network group address for users in a specific domain.

Each BSR administrative domain maintains one BSR that serves multicast groups on network segment 239.0.0.0/8. Multicast packets for groups on this network segment cannot pass through the border of the BSR administrative domain. Multicast groups that do not belong to any BSR administrative domain belong to a global domain. The global domain maintains a BSR that serves all the remaining multicast groups, namely, multicast groups beyond the range 239.0.0.0/8.

A BSR administrative domain is similar to a VPN in unicast, and multicast address segment 239.0.0.0/8 is equivalent to unicast address segment 10.0.0.0/8. Other multicast group addresses can be used on the public network and address conflicts need be avoided. If a PIM-SM domain is divided into different BSR administrative domains, each BSR administrative domain is equivalent to a VPN, serving the multicast groups on the network segment 239.0.0.0/8. You can use the same multicast group address in different BSR administration domains. If you configure the BSR in a BSR administration domain to serve multicast groups beyond 239.0.0.0/8, a message indicating a configuration error will be displayed.

The **c-bsr admin-scope** command configures a BSR administrative scope on the switch.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

After the **undo pim** command or the **undo multicast routing-enable** command is run in the system view, the BSR administrative domain is automatically disabled.

Precautions

The **c-bsr admin-scope** command needs to be run on all the devices in a PIM-SM domain.

Example

In the public network instance PIM view, configure a BSR administrative scope in a PIM-SM domain.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr admin-scope
```

8.3.6 c-bsr global

Function

The **c-bsr global** command configures the switch as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

By default, no C-BSR is configured in the global domain.

Format

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

Parameters

Parameter	Description	Value
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in the global domain.	The value is an integer that ranging from 0 to 32. By default, the value is 30.
priority *priority*	Specifies the priority of the C-BSR in the global domain. The greater the value, the higher the priority of the C-BSR.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BootStrap router (BSR) and the BSR serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative domains and a global domain.

Each BSR administrative domain maintains one BSR that serves the multicast groups in a specific group address range. Multicast packets for groups in the range cannot pass through the border of the BSR administrative domain. Addresses of multicast groups that BSRs in different BSR administrative domains serve can overlap. Overlapped multicast groups, however, similar to private group addresses, take effect only in local BSR administrative domains. Multicast groups that do not belong to any BSR administrative domain belong to a global domain. A global domain maintains a BSR that serves all the remained multicast groups.

The **c-bsr global** command configures the switch as a C-BSR in the global domain. The BSR in the global domain is generated through election.

C-BSRs compare the priorities and IP addresses to elect the BSR in the global area. The conditions for the election are as follows:

- The C-BSR with the highest priority is elected as the BSR.
- In the case of the same priority, the C-BSR with the largest IP address is elected as the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If the **c-bsr global** command is run several times, the latest configuration overrides the previous one.

After the **undo pim** command or the **undo multicast routing-enable** command is run in the system view, the C-BSRs in the global domain are automatically disabled.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain and can enable a device in a BSR administrative domain to receive multicast data of groups beyond 239.0.0.0/8.

The **c-bsr global** command needs to be used together with the **c-bsr admin-scope** command.

Example

In the public network instance PIM view, configure the switch as a C-BSR in the global domain, and then set the priority of the C-BSR to 1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr global priority 1
```

8.3.7 c-bsr group

Function

The **c-bsr group** command specifies the range of multicast groups that an administrative domain can serve on a C-BSR.

The **undo c-bsr group** command restores the default configuration.

By default, range of multicast groups that an administrative domain can serve is not configured.

Format

c-bsr group *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr group *group-address*

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address.	The address is in dotted decimal notation. The value ranges from 239.0.0.0 to 239.255.255.255.
mask	Specifies the mask of a multicast group address.	The address is in dotted decimal notation.
mask-length	Indicates the mask length of a multicast address.	The value is an integer ranging from 8 to 32.
hash-length *hash-length*	Specifies the hash mask length for the C-BSR in a BSR administrative domain.	The value is an integer ranging from 0 to 32. By default, it is 30.
priority *priority*	Specifies the priority of the C-BSR in the BSR administrative domain. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PIM-SM domain is divided into different BSR administrative domains, configure a multicast group address for each BSR administrative domain on the C-BSR. The group addresses must be in the range of 239.0.0.0/8. The group address ranges served by different BSR administrative domains can overlap. The address of a multicast group that a BSR administrative domain serves is used as a private group address.

By running this command on the C-BSR of each administrative domain, you can specify the group address of the administrative domain served by each C-BSR and the priority of each C-BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If the **c-bsr group** command is run several times, the latest configuration overrides the previous one.

After the **undo pim** command or the **undo multicast routing-enable** command is run in the system view or the VPN instance view, the C-BSRs in the BSR administrative domain are automatically disabled.

Example

In the public network instance PIM view, configure a C-BSR in the BSR administrative domain to serve groups 239.0.0.0/8, and set the priority of the C-BSR to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

8.3.8 c-bsr hash-length (IPv4)

Function

The **c-bsr hash-length** command configures the global hash mask length of a C-BSR.

The **undo c-bsr hash-length** command restores the default configuration.

By default, the global hash mask length of a C-BSR is 30.

Format

c-bsr hash-length *hash-length*

undo c-bsr hash-length

Parameters

Parameter	Description	Value
hash-length	Specifies the global hash mask length of a C-BSR.	The value is an integer that ranges from 0 to 32.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic RP election, if C-RPs have the same interface address mask and priority for a specified multicast group, a hash function needs to be executed to select the RP for the multicast group. The switch performs hash calculation for the group address of G, C-RP address, and hash mask length of the C-RPs with the same priority and compares the hash values. The C-RP with the greatest hash value acts as the RP for G.

The hash mask length is used to adjust the hash calculation result.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can run the **c-bsr** *interface-type interface-number hash-length* command in the PIM view to configure the C-BSR interface and specify the hash mask length. The **c-bsr hash-length** *hash-length* command specifies the global hash mask length. If both **c-bsr** *interface-type interface-number hash-length* and **c-bsr hash-length** *hash-length* are used, the **c-bsr** *interface-type interface-number hash-length* command takes effect.

Example

In the public network instance PIM view, set the global hash mask length of a C-BSR to 16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr hash-length 16
```

8.3.9 c-bsr holdtime (IPv4)

Function

The **c-bsr holdtime** command configures the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR.

The **undo c-bsr holdtime** command restores the default configuration.

By default, the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR is 130s.

Format

c-bsr holdtime *interval*

undo c-bsr holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which C-BSR waits for the Bootstrap message to be sent by BSR.	The value is an integer that ranges from 1 to 214748364, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IP address and the RP-set information. The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the elected BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command.

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer. The C-BSRs that fail in the election also refresh the timeout period of the BSR according to the holdtime. After the BSR times out, the C-BSRs receive new BSR messages.
- If the timer times out, the elected BSR is considered faulty. The C-BSRs that failed in the election triggers a new BSR election, preventing service interruption.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime; otherwise, the BSR will become unstable. This may result in multicast faults. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If BS_interval or holdtime is configured, use the following formula to calculate the other one: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither BS_interval nor holdtime is configured, the default values are used. The default BS_interval is 60s and the default holdtime is 130s.

Example

In the PIM view of public network instance, set the timeout interval during which the C-BSR waits for the Bootstrap message to be sent by BSR to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr holdtime 150
```

8.3.10 c-bsr interval (IPv4)

Function

The **c-bsr interval** command configures the interval for the BSR to continuously send Bootstrap messages.

The **undo c-bsr interval** command restores the default configuration.

By default, the interval for the BSR to continuously send Bootstrap messages is 60s.

Format

c-bsr interval *interval*

undo c-bsr interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for the BSR to continuously send the Bootstrap messages.	The value is an integer that ranges from 1 to 107374177, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IP address and the RP-set information to the network.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command. The following applies to the timer:

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer.
- If the timer times out, the BSR is considered to be faulty. The C-BSRs that failed in the election triggers a new BSR election, preventing service interruption.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime values; otherwise, the BSR will become unstable. This may result in a multicast fault. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If only one of the BS_interval and holdtime is configured, use the following formula to calculate the other parameter: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.

- If neither the BS_interval nor the holdtime is configured, default values are used. The default value of BS_interval is 60s, and the default value of holdtime is 130s.

Example

In the PIM view of public network instance, set the interval for the C-BSR to continuously send Bootstrap messages to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr interval 30
```

8.3.11 c-bsr priority (IPv4)

Function

The **c-bsr priority** command configures the global priority for a C-BSR.

The **undo c-bsr priority** command restores the default configuration.

By default, the global priority of the C-BSR is 0.

Format

c-bsr priority *priority*

undo c-bsr priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of the C-BSR. The greater the value, the higher the priority of the C-BSR.	The value is an integer that ranges from 0 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple C-BSRs take part in the BSR election in the PIM-SM domain, the following situations occur:

- The switch with the highest priority wins in the BSR election.

- If they have the same priority, the switch with the largest IP address wins in the BSR election.

To enable a C-BSR to function as the BSR, you can run the **c-bsr priority** command to increase the priority value of the C-BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can run the **c-bsr** *interface-type interface-number priority* command in the PIM view to configure the C-BSR interface and specify the C-BSR priority. The **c-bsr priority** *priority* command specifies the global C-BSR priority. If both **c-bsr** *interface-type interface-number priority* and **c-bsr priority** *priority* are used, the **c-bsr** *interface-type interface-number priority* command takes effect.

Example

In the PIM view of public network instance, configure the global priority of the C-BSR to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-bsr priority 5
```

8.3.12 c-rp (IPv4)

Function

The **c-rp** command configures the switch to advertise itself as a C-RP to the BSR.

The **undo c-rp** command restores the default configuration.

By default, no C-RP is configured.

Format

c-rp *interface-type interface-number* [**group-policy** *basic-acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface. The IP address of the specified interface is advertised as a C-RP address. **NOTE** To avoid frequent protocol changes caused by interface flapping, using loopback interfaces is recommended.	-
group-policy *basic-acl-number*	Specifies the range of the multicast groups served by a C-RP. The range is restricted to the multicast group range permitted by the specified ACL. The *basic-acl-number* parameter specifies the number of the basic ACL to identify the service range of the advertised RP.	The value is an integer ranging from 2000 to 2999.
priority *priority*	Specifies the priority of a C-RP. The greater the value, the lower the priority.	The value is an integer ranging from 0 to 255. The default value is 0.
holdtime *hold-interval*	Specifies the timeout period during which the BSR waits to receive an Advertisement message from a C-RP.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 150.
advertisement-interval *adv-interval*	Specifies the interval for a C-RP to send Advertisement messages.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 60.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM domain. You are advised to configure a C-RP on the core switch and reserve enough bandwidth between the switch and each of the other devices in the PIM-SM domain.

An RP is elected from multiple C-RPs following these rules, in descending order of precedence:

1. The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.
2. The C-RP with highest priority wins.
3. The C-RP with the largest hash value wins.
4. The C-RP with the largest address wins.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- PIM-SM has been enabled on the interface that acts as the C-RP.

Configuration Impact

An interface is specified in the command; therefore, the settings of **group-policy** *basic-acl-number*, **priority** *priority*, **holdtime** *hold-interval* and **advertisement-interval** *adv-interval* configured using this command override the global parameter settings that the interface obtains from the PIM view. If you run this command multiple times and specify the same interface, only the latest configuration takes effect.

NOTE

If IP address unnumbered is configured, it is not recommended to configure C-RP on the interfaces that use the same addresses. If the interfaces have different priorities, the BSR considers that the C-RP configuration has been repeatedly modified.

Precautions

- *basic-acl-number* specifies a group range. All permitted group ranges will be advertised as the ranges of groups that the RP serves. If no group range is specified, the C-RP serves all multicast groups.
- To enable a C-RP to serve multiple PIM-SM domains, configure multiple **rule**s in the ACL to specify multicast group ranges for the domains.
- The **c-rp** command needs to be used together with the **acl** command. In the ACL view, **source** can be specified in the **rule** command to specify the range of groups that a C-RP serves.

Example

In the PIM view of public network instance, use basic ACL 2069 to specify Loopback 0 as the C-RP for PIM-SM domains 225.1.0.0/16 and 226.2.0.0/16, and set the C-RP priority to 10.

```
<HUAWEI> system-view
[HUAWEI] acl number 2069
[HUAWEI-acl-basic-2069] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2069] rule permit source 226.2.0.0 0.0.255.255
[HUAWEI-acl-basic-2069] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface loopback 0
```

```
[HUAWEI-LoopBack0] pim sm
[HUAWEI-LoopBack0] quit
[HUAWEI] pim
[HUAWEI-pim] c-rp loopback 0 group-policy 2069 priority 10
```

8.3.13 c-rp advertisement-interval (IPv4)

Function

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **undo c-rp advertisement-interval** command restores the default interval.

By default, a C-RP sends Advertisement messages at an interval of 60 seconds.

Format

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a C-RP sends Advertisement messages.	The value ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All C-RPs in a PIM-SM domain periodically send Advertisement messages to the same BSR. The BSR can collect the integrated RP-Set.

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages to the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can also set the advertisement interval when you run the **c-rp** *interface-type interface-number* **advertisement-interval** *adv-interval* command in the PIM view to configure the C-RP interface. The **c-rp advertisement-interval** *interval* command specifies the global advertisement interval. If both the commands are configured, the interval configured by the **c-rp** *interface-type interface-number* **advertisement-interval** *adv-interval* command takes effect.

Example

In the PIM view of public network instance, set the interval at which a C-RP sends Advertisement messages to 30s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-rp advertisement-interval 30
```

8.3.14 c-rp holdtime (IPv4)

Function

The **c-rp holdtime** command configures the holdtime for a received Advertisement message on a BSR.

The **undo c-rp holdtime** command restores the default holdtime.

By default, the holdtime for a received Advertisement message is 150 seconds.

Format

c-rp holdtime *interval*

undo c-rp holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period for a BSR to wait the Advertisement message from a C-RP.	The value ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When *interval* is set on a C-RP, the C-RP encapsulates *interval* in an Advertisement message and sends it to the BSR. The BSR obtains this *interval* from the message and starts the timer. If the BSR receives no Advertisement message from the C-RP within the timeout period, the BSR regards the C-RP invalid or unreachable.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can also set the holdtime for a received Advertisement message when you run the **c-rp** *interface-type interface-number* **holdtime** *hold-interval* in the PIM view to configure a C-PR interface. The **c-rp holdtime** *hold-interval* configures the global holdtime for Advertisement messages. If both the two commands are configured, the holdtime configured by the **c-rp** *interface-type interface-number* **holdtime** *hold-interval* command takes effect.

Example

In the PIM view of public network instance, set the holdtime for a received Advertisement message to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-rp holdtime 100
```

8.3.15 c-rp priority (IPv4)

Function

The **c-rp priority** command configures the global priority of a C-RP.

The **undo c-rp priority** command restores the default configuration.

By default, the global priority of a C-RP is 0.

Format

c-rp priority *priority*

undo c-rp priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of a C-RP. The greater the value, the lower the priority.	The value is an integer that ranges from 0 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs, in descending order of precedence:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- The C-RP with the largest hash value wins.
- The C-RP with the largest address wins.

To enable a C-RP to function as an RP, you can run the **c-rp priority** command to increase the priority of the C-RP.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

You can run the **c-rp** *interface-type interface-number* **priority** *priority* command in the PIM view to configure the C-RP interface and specify the C-RP priority. The **c-rp priority** *priority* command specifies the global C-RP priority. If both **c-rp** *interface-type interface-number* **priority** *priority* and **c-rp priority** *priority* are used, the **c-rp** *interface-type interface-number* **priority** *priority* command takes effect.

Example

In the PIM view of public network instance, set the global priority of a C-RP to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] c-rp priority 5
```

8.3.16 crp-policy (IPv4)

Function

The **crp-policy** limits the range of valid C-RP addresses and the range of the multicast addresses served by a C-RP. The BSR drops the C-RP messages with addresses out of the specified range to protect valid C-RPs.

The **undo crp-policy** command restores the default configuration.

By default, the BSR does not limit the range of valid C-RP addresses and the range of the multicast groups served by a C-RP. The BSR considers all the received C-RP messages valid.

Format

crp-policy *advanced-acl-number*

undo crp-policy

Parameters

Parameter	Description	Value
advanced-acl-number	Specifies the number of an advanced ACL. The ACL defines the range of the C-RP addresses and the range of the group addresses served by a C-RP.	The value is an integer that ranges from 3000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any switch can be configured as a C-RP to serve the multicast groups in a specified range. Each C-RP sends its information to the BSR in unicast mode. The BSR summarizes all received C-RP information into am RP-set and floods it on the entire network using BSR messages. The local switch then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RPs from spoofing, configure **crp-policy** on BSR switches to limit the range of valid C-RP addresses and the range of multicast group addresses served by a C-RP. Configure the same filtering rule on each C-BSR because any C-BSR can become the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If an ACL rule is specified but no C-RP address range is set, all C-RP messages are denied.

Precautions

The **crp-policy** command and the **acl** command are used together. In the ACL view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule** command. You can set the address range of multicast groups that are served by specifying the **destination** parameter in the **rule** command.

A received C-RP message matches the configured filtering policy only when the C-RP address carried by the message matches **source** and the group address range carried by the message is a subset of the group address range defined in the ACL.

Example

Configure a C-RP policy on the C-BSR, which allows only the C-RP with the address 10.1.1.1/32 and allows the C-RP to serve only the multicast groups 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100
[HUAWEI-acl-adv-3100] rule permit ip source 10.1.1.1 0 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3100] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] crp-policy 3100
```

8.3.17 display default-parameter pim-dm

Function

The **display default-parameter pim-dm** command displays default configurations about PIM-DM.

Format

display default-parameter pim-dm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-dm** command displays default configurations about PIM-DM. Even if PIM-DM parameters are modified, the **display default-parameter pim-dm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configurations about PIM-DM.

```
<HUAWEI> display default-parameter pim-dm
 PIM View Default Configurations:
 --------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
```

```
Holdtime assert: 180 s
Holdtime join-prune: 210 s
Source-lifetime: 210 s
State-refresh-interval: 60 s
State-refresh-rate-limit: 30 s
State-refresh-ttl: 255
Hello periodic interval: 30 s
Join-prune periodic interval: 60 s

Interface View Default Configurations:
-------------------------------------
Pim bfd: disabled
Pim hello-option dr-priority: 1
Pim hello-option holdtime: 105 s
Pim hello-option lan-delay: 500 ms
Pim hello-option neighbor-tracking: disabled
Pim hello-option override-interval: 2500 ms
Pim holdtime assert: 180 s
Pim holdtime join-prune: 210 s
Pim require-genid: disabled
Pim silent: disabled
Pim state-refresh-capable: enabled
Pim timer dr-switch-delay: disabled
Pim timer graft-retry: 3 s
Pim hello periodic interval: 30 s
Pim join-prune periodic interval: 60 s
Pim triggered-hello-delay: 5 s
Pim version: 2
Pim ipsec sa: disabled
Pim neighbor-policy: disabled
```

Table 8-36 Description of the **display default-parameter pim-dm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled This function is configured using the **hello-option neighbor-tracking (IPv4)** command.

Item	Description
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv4)** command.
State-refresh-interval	Interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv4)** command.
State-refresh-rate-limit	Minimum interval from when the last State-Refresh message is received to when the next State-Refresh message is received. This parameter is configured by the **state-refresh-rate-limit (IPv4)** command.
State-refresh-ttl	TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.

Item	Description
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at the shared network segment where the interface resides. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. - enabled: Neighbor tracking is enabled. - disabled: Neighbor tracking is disabled This function is configured using the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. - enabled: The received Hello message is required to carry the Generation ID. - disabled: The received Hello message is not required to carry the Generation ID. This parameter is configured using the **pim require-genid** command.

Item	Description
Pim silent	Whether the interface is set to PIM silent state. ● enabled: The interface is in PIM silent state. ● disabled: The interface is not in PIM silent state. This function is configured using the **pim silent** command.
Pim state-refresh-capable	Whether State-Refresh is enabled on the interface. ● enabled: State-Refresh is enabled on the interface. ● disabled: State-Refresh is disabled on the interface. This function is configured using the **pim state-refresh-capable** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. ● enabled: The DR switch delay is set on the interface. ● disabled: The DR switch delay is not set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim timer graft-retry	Interval for the interface to retransmit Graft messages. This parameter is configured by the **pim timer graft-retry** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.

Item	Description
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. This parameter is configured by the **pim ipsec sa** command.
Pim neighbor-policy	Whether a neighbor policy is configured on the interface. - enabled: A neighbor policy is configured on the interface. - disabled: No neighbor policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

8.3.18 display default-parameter pim-sm

Function

The **display default-parameter pim-sm** command displays default configurations about PIM-SM.

Format

display default-parameter pim-sm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-sm** command displays default configurations about PIM-SM. Even if PIM-SM parameters are modified, the **display default-parameter pim-sm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configurations about PIM-SM.

```
<HUAWEI> display default-parameter pim-sm
 PIM View Default Configurations:
 ---------------------------------
 Auto-rp listening enable: disabled
 Bsr-policy: disabled
 C-bsr admin-scope: disabled
 C-bsr global: disabled
 C-bsr group: none
 C-bsr hash-length: 30
 C-bsr holdtime: 130 s
 C-bsr interval: 60 s
 C-bsr priority: 0
 C-rp advertisement-interval: 60 s
 C-rp holdtime: 150 s
 C-rp priority: 0
 Crp-policy: disabled
 Bsm semantic fragmentation: disabled
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Probe-interval: 5 s
 Register-header-checksum: disabled
 Register-policy: disabled
 Register-suppression-timeout: 60 s
 Source-lifetime: 210 s
 Source-policy: disabled
 Spt-switch-threshold: disabled
 Ssm-policy: disabled
 Static-rp:  disabled
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s
 Timer spt-switch: 15 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim bsr-boundary: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim timer dr-switch-delay: disabled
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim join-policy: disabled
 Pim neighbor-policy: disabled
```

Table 8-37 Description of the **display default-parameter pim-sm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.

Item	Description
Auto-rp listening enable	Whether the auto-RP listening function is enabled. The switch does not support this function.
Bsr-policy	Whether the valid address range of the BSR is set. This parameter is configured by the **bsr-policy (IPv4)** command.
C-bsr admin-scope	Whether the BSR administrative domain is configured. This parameter is configured by the **c-bsr admin-scope** command.
C-bsr global	Whether the C-BSR in the global domain is configured. This parameter is configured by the **c-bsr global** command.
C-bsr group	Whether the C-BSR in the BSR administrative domain is configured. This parameter is configured by the **c-bsr group** command.
C-bsr hash-length	Global hash mask length of the C-BSR. This parameter is configured by the **c-bsr hash-length (IPv4)** command.
C-bsr holdtime	Waiting time for the BSR to receive the Bootstrap message. This parameter is configured by the **c-bsr holdtime (IPv4)** command.
C-bsr interval	Interval for the BSR to send Bootstrap messages. This parameter is configured by the **c-bsr interval (IPv4)** command.
C-bsr priority	Global priority of the C-BSR. This parameter is configured by the **c-bsr priority (IPv4)** command.
C-rp advertisement-interval	Interval for the C-RP to send Advertisement messages. This parameter is configured by the **c-rp advertisement-interval (IPv4)** command.
C-rp holdtime	Waiting time for the BSR to receive the Advertisement message. This parameter is configured by the **c-rp holdtime (IPv4)** command.
C-rp priority	Global priority of the C-RP. This parameter is configured by the **c-rp priority (IPv4)** command.

Item	Description
Crp-policy	Whether the valid address range of the C-RP and the range of multicast groups that the C-RP serves are set. This parameter is configured by the **crp-policy (IPv4)** command.
Bsm semantic fragmentation	Whether the BSR fragmentation is enabled. This parameter is configured by the **bsm semantic fragmentation (IPv4)** command.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state, in seconds. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment, in milliseconds. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Interval for sending Prune Override messages, in milliseconds. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state, in seconds. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state, in seconds. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP, in seconds. This parameter is configured by the **probe-interval (IPv4)** command.
Register-header-checksum	Whether calculating the checksum based on information in Register message header is required. This parameter is configured by the **register-header-checksum** command.

Item	Description
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv4)** command.
Register-suppression-timeout	Time period for holding the register-suppression state, in seconds. This parameter is configured by the **register-suppression-timeout (IPv4)** command.
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv4)** command.
Spt-switch-threshold	Whether the threshold of the multicast packet rate that triggers the switch from the RPT to the SPT is configured. This parameter is configured by the **spt-switch-threshold (IPv4)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv4)** command.
Static-rp	Whether the static RP is configured. This parameter is configured by the **static-rp (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages, in seconds. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages, in seconds. This parameter is configured by the **timer join-prune (IPv4)** command.
Timer spt-switch	Whether the interval for checking whether the multicast packet rate exceeds the threshold before the switchover from RPT to SPT is configured, in seconds. This parameter is configured by the **timer spt-switch (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.

Item	Description
Pim bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim bsr-boundary** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state, in seconds. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface, in milliseconds. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages, in milliseconds. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state, in seconds. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state, in seconds. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.

Item	Description
Pim hello periodic interval	Interval for the interface to send Hello messages, in seconds. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages, in seconds. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages, in seconds. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. This parameter is configured by the **pim ipsec sa** command.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

8.3.19 display default-parameter pim-ssm

Function

The **display default-parameter pim-ssm** command displays default configurations of PIM-SM for SSM.

Format

display default-parameter pim-ssm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-ssm** command displays default configuration of PIM-SM for SSM. Even if the configuration of PIM-SM for SSM is modified, the **display default-parameter pim-ssm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configuration of PIM-SM for SSM.

```
<HUAWEI> display default-parameter pim-ssm
 PIM View Default Configurations:
 ---------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Probe-interval: 5 s
 Register-header-checksum: disabled
 Register-policy: disabled
 Register-suppression-timeout: 60 s
 Source-lifetime: 210 s
 Source-policy: disabled
 Ssm-policy: disabled
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim timer dr-switch-delay: disabled
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim join-policy: disabled
 Pim neighbor-policy: disabled
```

Table 8-38 Description of the **display default-parameter pim-ssm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.

Item	Description
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state, in seconds. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment, in milliseconds. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Interval for sending Prune Override messages, in milliseconds. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state, in seconds. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state, in seconds. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP, in seconds. This parameter is configured by the **probe-interval (IPv4)** command.
Register-header-checksum	Whether calculating the checksum based on information in Register message header is required. This parameter is configured by the **register-header-checksum** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv4)** command.
Register-suppression-timeout	Time period for holding the register-suppression state, in seconds. This parameter is configured by the **register-suppression-timeout (IPv4)** command.

Item	Description
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv4)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages, in seconds. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages, in seconds. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state, in seconds. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface, in milliseconds. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages, in milliseconds. This parameter is configured by the **pim hello-option override-interval** command.

Item	Description
Pim holdtime assert	Time period for the interface to hold the Assert state, in seconds. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state, in seconds. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages, in seconds. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages, in seconds. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages, in seconds. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. This parameter is configured by the **pim ipsec sa** command.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

8.3.20 display pim bfd session

Function

The **display pim bfd session** command displays the information about PIM BFD sessions.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bfd session statistics**

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bfd session** [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. The *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
statistics	Displays PIM BFD statistics.	-
interface *interface-type interface-number*	Specifies an interface to be displayed. *interface-type interface-number* specifies the type and number of the interface.	-
neighbor *neighbor-address*	Specifies the IP address of a PIM neighbor to be displayed.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim bfd session** command output helps you locate communication faults between neighbors.

Example

Display PIM BFD sessions on VLANIF 10.

```
<HUAWEI> display pim bfd session interface vlanif 10
 VPN-Instance: public net

 Vlanif10 (10.1.2.2): Total 2 BFD sessions Created

 Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
 10.1.2.3     20            20            5            8756/8652        Up
 10.1.2.4     30            10            3            8754/8423        Up
```

Display PIM BFD sessions on VLANIF 10 when the switch is not enabled with global BFD.

```
<HUAWEI> display pim bfd session interface vlanif 10
 VPN-Instance: public net

 Vlanif10 (10.1.2.2): Total 1 BFD session Created

 Neighbor    ActTx(ms)    ActRx(ms)    ActMulti    Local/Remote          State
 10.1.2.1    --           --           --          0/0                   BFD global disable
```

Display the statistics of a PIM BFD session.

```
<HUAWEI> display pim bfd session statistics
 VPN-Instance: public net
  Total 1 PIM BFD session in this instance.

   Total 1 PIM BFD session up.
   Total 0 PIM BFD session down.
```

Display information about PIM BFD sessions of the neighbor 10.1.2.3.

```
<HUAWEI> display pim bfd session neighbor 10.1.2.3
VPN-Instance: public net
  Vlanif10 (10.1.2.2)
 Neighbor     ActTx(ms)     ActRx(ms)     ActMulti     Local/Remote     State
 10.1.2.3     20            20            5            8756/8652        Up
```

Table 8-39 Description of the **display pim bfd session** command output

Item	Description
Vlanif10 (10.1.2.2)	PIM interface name (the IP address).
Neighbor	IP address of a PIM neighbor.
ActTx (ms)	Actual minimum transmission interval, in milliseconds.
ActRx (ms)	Actual minimum receiving interval, in milliseconds.
ActMulti	Actual local detection multiple.
Local/Remote	Local and remote discriminators.

Item	Description
State	Status of the PIM BFD session. ● Up: indicates that the BFD session is set up successfully and detection packets are periodically exchanged. ● Init: indicates that the local end can communicate with the remote end and wants the session status to be Up. ● BFD global disable: indicates that BFD is globally disabled. ● Detect down: indicates that no BFD packets are not received when the detection time expires. ● Neighbour down: indicates that the packets with the State field being Down are received from neighbors.
Total 1 PIM BFD session in this instance	Total number of PIM BFD sessions in a public network instance or a VPN instance.
Total 1 PIM BFD session up	Number of PIM BFD sessions in the Up state in a public network instance or a VPN instance.
Total 0 PIM BFD session down	Number of PIM BFD sessions in the Down state in a public network instance or a VPN instance, that is, all PIM BFD sessions except the PIM BFD sessions in the Up state.

8.3.21 display pim bsr-info

Function

The **display pim bsr-info** command displays the BSRs in a PIM-SM domain.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bsr-info**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command applies to the PIM-SM domain where the RP is dynamically elected among BSRs. You can run this command on any switch in the domain to view the BSR information.

- If the current switch is configured with the C-BSR, the command output includes information about the elected BSR and locally configured C-BSR.
- If the current switch is not configured with the C-BSR, the command output includes information about the elected BSR only.

Precautions

When the **display pim bsr-info** command is used, only information about the public network instance is displayed if the **vpn-instance** or **all-instance** is not specified.

This command has output only after C-BSRs have been configured in a PIM-SM domain.

Example

Display information about the BSR in the PIM-SM domain. If the switch is not configured with C-BSR, only information about the elected BSR is displayed.

```
<HUAWEI> display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.1.2.2
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 00:01:46
     Expires: 00:02:02
     C-RP Count: 1
```

Display information about BSR in the current PIM-SM.

If the switch is configured with C-BSR, information about the elected BSR and C-BSR is displayed.

```
<HUAWEI> display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.1.2.2
     Priority: 0
     Hash mask length: 30
     State: Elected
     Scope: Not scoped
     Uptime: 00:10:42
     Next BSR message scheduled at: 00:00:31
     C-RP Count: 1
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: 10.1.2.2
     Priority: 0
```

```
    Hash mask length: 30
    State: Elected
    Scope: Not scoped
    Wait to be BSR: 0
```

Table 8-40 Description of the **display pim bsr-info** command output

Item	Description
Elected AdminScoped BSR Count	Number of elected AdminScoped BSRs.
Elected BSR Address	Address of the elected BSR.
Priority	Priority of the BSR. By default, the value is 0.
Hash mask length	Mask length in the RP hash calculation.
State	Status of the BSR.
Scope	Range of multicast addresses in the administrative scope when the BSR is an AdminScoped BSR. Not scoped indicates that the BSR is not an AdminScoped BSR.
Uptime	Period during which the BSR exists. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Remaining time of the BSR. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
C-RP Count	Number of RPs learned through the BSR.
Next BSR message scheduled at	Period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.

Item	Description
Candidate AdminScoped BSR Count	Number of AdminScoped C-BSRs.
Candidate BSR Address	Address of the C-BSR.
Wait to be BSR	Whether the current C-BSR is valid. The values are as follows: ● 0: indicates that the current C-BSR is valid. The current C-BSR takes part in the BSR election. ● 1: indicates that the current C-BSR is invalid. The current C-BSR does not take part in the BSR election. When the number of C-BSRs configured on the switch exceeds the threshold, the value is 1.

8.3.22 display pim claimed-route

Function

The **display pim claimed-route** command displays the unicast routing information used by PIM.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **claimed-route** [*source-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
source-address	Specifies the multicast source address.	The address is in decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pim claimed-route** command is used to view information about unicast routes used by PIM, including RPF neighbors, interfaces, route types, and route selection policies.

Configuration Impact

Differences between the **display pim claimed-route** and **display multicast rpf-info** commands are as follows:

- The **display multicast rpf-info** command is used to check information about RPF neighbors, RPF interfaces, or whether there is a route to a specified source address.
- The **display pim claimed-route** command is used to check information about unicast routes used by multicast routing and entries of these routes.

Example

Display the unicast routing information used by PIM.

```
<HUAWEI> display pim claimed-route
 VPN-Instance: public net
 multicast load-splitting rule: source-group
 RPF information about: 10.1.0.0 in PIM-SM routing table
     RPF interface: Vlanif10, RPF neighbor: 10.1.2.2
     Referenced route/mask: 10.1.0.0/24
     Referenced route type: igp
     RPF-route selecting rule: preference-preferred
     The (S, G) or (*, G) list dependent on this route entry
     (10.1.0.1, 225.0.0.1)
```

Table 8-41 Description of the **display pim claimed-route** command output

Item	Description
multicast load-splitting rule	How multi-cast loads are split. The following policies apply: • group: multicast group-based load splitting • source: multicast source-based load splitting • source-group: multicast source and group-based load splitting • stable-preferred: stable-preferred load splitting • balance-preferred: balance-preferred load splitting This parameter is configured by the **multicast load-splitting** command.

Item	Description
RPF information about: 10.1.0.0 in PIM-SM routing table	RPF routing information with the source address of 10.1.0.0 in the PIM-SM routing table
RPF interface	RPF interface on the switch.
RPF neighbor	RPF neighbor of the switch.
Referenced route/mask	Destination address/mask of the referenced route.
Referenced route type	Type of the route.
RPF-route selecting rule	Preferred rule for selecting the RPF-route.
The (S,G) or (*,G) list dependent on this route entry	List of multicast entries based on RPF routes.

8.3.23 display pim control-message counters

Function

The **display pim control-message counters** command displays the number of sent, received, and invalid PIM control messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters message-type** { **probe** | **register** | **register-stop** | **crp** }

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
message-type	Indicates a PIM control message type.	-
probe	Indicates the Probe message.	-
register	Indicates the Register message.	-

Parameter	Description	Value
register-stop	Indicates the Register-stop message.	-
crp	Indicates the C-RP message.	-
assert	Indicates the Assert message.	-
graft	Indicates the Graft message.	-
graft-ack	Indicates the Graft-ack message.	-
hello	Indicates the Hello message.	-
join-prune	Indicates the Join/Prune message.	-
state-refresh	Indicates the State-Refresh message.	-
bsr	Indicates the BSR message.	-
interface *interface-type interface-number*	Indicates the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When multicast data messages cannot be forwarded on a PIM network, run the **display pim control-message counters** command to view statistics on protocol messages. The command output helps you locate faults.

When you run the **display pim control-message counters** command:

- If you specify **interface** *interface-type interface-number*, you can view the number of various PIM control messages that were sent and received on the specified interface only.
- If you specify **message-type**, you can view the number of PIM control messages of this type sent and received on all interfaces of the switch.

Example

Display the statistics about sent, received, and invalid PIM control messages on the device.

```
<HUAWEI> display pim control-message counters
 VPN-Instance: public net
 PIM global control-message counters:
 Message Type      Received        Sent           Invalid          Filtered
 Register          51              0              0                0
 Register-Stop     0               48             0                0
 Probe             44              0              0                0
 C-RP              0               0              0                0

 PIM control-message counters for interface: Vlanif10
```

```
 Message Type     Received        Sent           Invalid         Filtered
 Assert          0              6              0              0
 Graft           0              0              0              0
 Graft-Ack       0              0              0              0
 Hello           34496          34495          0              0
 Join-prune      26171          90             0              0
 State-Refresh   0              0              0              0
 BSR             0              0              0              0

 PIM control-message counters for interface: Vlanif20
 Message Type     Received        Sent           Invalid         Filtered
 Assert          0              0              0              0
 Graft           0              0              0              0
 Graft-Ack       0              0              0              0
 Hello           34491          34495          0              0
 Join-prune      0              41             0              0
 State-Refresh   0              0              0              0
 BSR             0              0              0              0
```

Display the statistics about sent, received, invalid PIM control messages on VLANIF 10.

```
<HUAWEI> display pim control-message counters interface Vlanif 10
 VPN-Instance: public net
 PIM control-message counters for interface: Vlanif 10
 Message Type     Received        Sent           Invalid     Filtered
 Assert          0              0              0          0
 Graft           0              0              0              0
 Graft-Ack       0              0              0              0
 Hello           328            331            0          0
 Join-prune      2              0              0          0
 State-Refresh   0              0              0              0
 BSR             0              0              0          0
```

Table 8-42 Description of the **display pim control-message counters** command output

Item	Description
PIM global control-message counters	Number of PIM control messages in the public network.
PIM control-message counters for interface	Name of the interface where statistics about PIM control messages are collected.
Message Type	Type of the control messages.
Received	Number of control messages received by the interface.
Sent	Number of control messages sent by the interface.
Invalid	Number of invalid control messages.
Filtered	Number of control messages filtered out by the interface.
Register	Number of Register messages.
Register-Stop	Number of Register-Stop messages.
Probe	Number of Probe messages.

Item	Description
C-RP	Number of CRP messages.
Assert	Number of Assert messages.
Graft	Number of Graft messages.
Graft-Ack	Number of Graft-Ack messages.
Hello	Number of Hello messages.
Join-prune	Number of Join/Prune messages.
State-Refresh	Number of State-Refresh messages.
BSR	Number of Bootstrap messages.

8.3.24 display pim grafts

Function

The **display pim grafts** command displays the information about unacknowledged PIM-DM Graft messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **grafts**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM, after sending the Graft message, the switch needs to wait to receive the Graft-Ack message from the upstream device. You can run the **display pim grafts** command to view the information about the PIM-DM Graft messages sent but unacknowledged.

Example

Display the unacknowledged PIM-DM graft messages on the switch.

```
<HUAWEI> display pim grafts
VPN-Instance: public net
Source                  Group                 Expire   RetransmitIn
10.0.5.200               226.3.3.3             00:02:52 00:00:02
```

Table 8-43 Description of the **display pim grafts** command output

Item	Description
Source	Multicast source address.
Group	Multicast group address.
Expire	Timeout period of an (S, G) entry.
RetransmitIn	Amount of time before the next retransmission of the Graft message.

8.3.25 display pim interface

Function

The **display pim interface** command displays PIM information on an interface.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
interface-type interface-number	Specifies the type and number of an interface.	-
up	Displays PIM information on interfaces in Up state.	-
down	Displays PIM information on interfaces in Down state.	-

Parameter	Description	Value
verbose	Displays detailed information about a PIM interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An interface with PIM enabled is called a PIM interface. The **display pim interface** command is used to display information about PIM interfaces, including the PIM state, number of PIM neighbors, interval at which Hello messages are sent, DR priority, and DR address.

When the **display pim interface** command is used:

- If *interface-type interface-number* is specified, the command displays various PIM state parameters on the specified interface.
- If *interface-type interface-number* is not specified, the command displays state parameters of all the PIM interfaces.
- If **up** is specified in the command, the command displays parameters of the PIM interfaces in the Up stated.
- If **down** is specified in the command, the command displays parameters of the PIM interfaces in the Down state.

Example

Display information about all the PIM interfaces.

```
<HUAWEI> display pim interface
 VPN-Instance: public net
 Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
 Loop0          up      0        30         1          10.1.0.2    (local)
 Vlanif10       up      1        30         1          10.1.1.2
 Vlanif20       up      0        30         1          10.1.2.2    (local)
 Vlanif30       up      1        30         1          10.1.3.2
```

Table 8-44 Description of the **display pim interface** command output

Item	Description
Interface	Name of the PIM interface.
State	Status of the PIM interface, Up or Down.
NbrCnt	Number of PIM neighbors on the interface.

Item	Description
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

Display detailed information about PIM on VLANIF10.

```
<HUAWEI> display pim interface vlanif 10 verbose
 VPN-Instance: public net
 Interface: Vlanif10, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0XF5712241
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: enabled
     PIM dr-switch-delay timer : 20 s
     Number of routers on link not using DR priority: 0
     Number of routers on link not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 2
     ACL of PIM neighbor policy: myacl
     ACL of PIM ASM join policy: 2000
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
     PIM ipsec: disabled
```

Table 8-45 Description of the **display pim interface verbose** command output

Item	Description
Interface	Name and IP address of the PIM interface.
PIM version	PIM version enabled on the interface.
PIM mode	PIM mode used on the interface.
PIM state	Status of the PIM interface, Up or Down.
PIM DR	DR address on the interface.

Item	Description
PIM DR Priority (configured)	DR priority configured on the interface.
PIM neighbor count	Number of PIM neighbors on the interface.
PIM hello interval	Interval for sending PIM Hello messages, in seconds.
PIM LAN delay (negotiated)	Negotiated delay for transmitting packets on the interface, in milliseconds.
PIM LAN delay (configured)	Configured delay for transmitting packets on the interface, in milliseconds.
PIM hello override interval (negotiated)	Negotiated override interval on the interface, in milliseconds.
PIM hello override interval (configured)	Configured override interval on the interface, in milliseconds.
PIM Silent	Whether the interface is set to PIM silent state. - enabled: The interface is in the PIM silent state. - disabled: The interface is not in the PIM silent state. This function is configured using the **pim silent** command.
PIM neighbor tracking (negotiated)	Whether PIM neighbor tracking is enabled on the interface after negotiation. - enabled: PIM neighbor tracking is enabled on the interface. - disabled: PIM neighbor tracking is disabled on the interface.
PIM neighbor tracking (configured)	Whether PIM neighbor tracking is configured on the interface. - enabled: PIM neighbor tracking is configured on the interface. - disabled: PIM neighbor tracking is not configured on the interface. This function is configured using the **pim hello-option neighbor-tracking** command.
PIM generation ID	Generation ID option on the interface.

Item	Description
PIM require-GenID	Whether the switch is enabled to reject Hello messages not carrying the Generation ID. - enabled: The switch is enabled to reject Hello messages not carrying the Generation ID. - disabled: The switch is disabled from rejecting Hello messages not carrying the Generation ID. This function is configured using the **pim require-genid** command.
PIM hello hold interval	Interval during which the receiver of the Hello message to keep its neighbor reachable, in seconds.
PIM assert hold interval	Interval for sending Assert messages, in seconds.
PIM triggered hello delay	Maximum random delay for triggering Hello messages, in seconds.
PIM J/P interval	Interval at which the interface sends Join/Prune messages, in seconds.
PIM J/P hold interval	Period for holding the Join/Prune status on the interface, in seconds.
PIM BSR domain border	Whether the BSR boundary is configured on the interface. - enabled: The BSR boundary is configured on the interface. - disabled: The BSR boundary is not configured on the interface. This function is configured using the **multicast boundary** command.
PIM BFD	Whether PIM BFD is enabled. - enabled: PIM BFD is enabled. - disabled: PIM BFD is disabled. This function is configured using the **pim bfd enable** command.
PIM BFD min-tx-interval	Minimum interval for sending PIM BFD packets. This parameter is configured using the **pim bfd min-tx-interval** *tx-value* command.

Item	Description
PIM BFD min-rx-interval	Minimum interval for receiving PIM BFD packets. This parameter is configured using the **pim bfd min-rx-interval** *rx-value* command.
PIM BFD detect-multiplier	PIM BFD detection multiplier. This parameter is configured using the **pim bfd detect-multiplier** *multiplier-value* command.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of switches that do not use DR priority in all the network segments connected to the interface.
Number of routers on link not using LAN delay	Number of switches that do not use LAN delay in all the network segments connected to the interface.
Number of routers on link not using neighbor tracking	Indicates the number of switches that are not enabled with the neighbor tracing function in the network segment where the interface resides.
ACL of PIM neighbor policy	Neighbor filtering policy configured on the interface.
ACL of PIM ASM join policy	ASM Join information filtering policy configured on the interface.
ACL of PIM SSM join policy	SSM Join information filtering policy configured on the interface.
ACL of PIM join policy	Join information filtering policy configured on the interface.

Item	Description
PIM ipsec	Whether PIM IPSec is configured in the PIM view or interface view, and the SA policy name if PIM IPSec is configured. The value can be: ● PIM ipsec: enabled(sa-name: sa1) Security association sa1 has been configured to authenticate all PIM protocol packets using the **ipsec sa (IPv4)** command in the PIM view or the **pim ipsec sa** command in the interface view. If the SA is configured in the interface view, the configuration on the interface is displayed. Otherwise, the configuration in the PIM view is displayed. ● PIM hello ipsec: enabled(sa-name: sa1) Security association sa1 has been configured to authenticate only PIM Hello packets using the **hello ipsec sa (IPv4)** command in the PIM view or the **pim hello ipsec sa** command in the interface view. If the SA is configured in the interface view, the configuration on the interface is displayed. Otherwise, the configuration in the PIM view is displayed. ● PIM ipsec: disabled PIM IPSec is not configured in the PIM view or interface view.

8.3.26 display pim invalid-packet

Function

The **display pim invalid-packet** command displays statistics about invalid PIM messages received by a device and details of these messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** }] *

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet message-type** { **crp** | **register** | **register-stop** }

display pim invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid PIM messages received in a specified VPN instance. The *vpn-instance-name* parameter specifies the VPN instance name.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid PIM messages received in all VPN instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface on the switch.	-
message-type	Displays statistics about invalid PIM messages of a specific type.	-
assert	Displays statistics about invalid Assert messages.	-
bsr	Displays statistics about invalid BSR messages.	-
hello	Displays statistics about invalid Hello messages.	-
join-prune	Displays statistics about invalid Join/Prune messages.	-
graft	Displays statistics about invalid Graft messages.	-
graft-ack	Displays statistics about invalid Graft-Ack messages.	-
state-refresh	Displays statistics about invalid State-Refresh messages.	-
crp	Displays statistics about invalid C-RP messages.	-
register	Displays statistics about invalid Register messages.	-

Parameter	Description	Value
register-stop	Displays statistics about invalid Register-Stop messages.	-
packet-number	Displays details about a specified number of invalid PIM messages recently received.	The value is an integer that ranges from 1 to 100. By default, details of all the invalid PIM messages currently stored are displayed.
verbose	Displays details of invalid PIM messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a switch fails to create PIM entries, you can run the **display pim invalid-packet** command first to check whether the switch has received invalid PIM messages. If the command output displays counters of invalid PIM messages, run the **display pim invalid-packet** [*packet-number*] **verbose** command to view details of invalid PIM messages for fault location.

You can run the following commands to view information about specific invalid PIM messages:

- Run the **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** command to view statistics about invalid PIM messages received in a specified VPN instance or in all VPN instances.
- Run the **display pim invalid-packet interface** *interface-type interface-number* command to view statistics about invalid PIM messages received by a specified interface.
- Run the **display pim invalid-packet** *packet-number* **verbose** command to view details of invalid PIM messages recently received. Currently, details of a maximum of 100 invalid PIM messages can be displayed.

Example

Display statistics about invalid PIM messages received on the switch.

```
<HUAWEI> display pim invalid-packet
          Statistics of invalid packets for public net:
```

```
-------------------------------------------------------------------
PIM General invalid packet:
Invalid PIM Version      : 0          Invalid PIM Type         : 0
Fault Length             : 0          Bad Checksum             : 0

PIM Register invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
Invalid Dest Addr        : 0

PIM Register-Stop invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
Invalid Dest Addr        : 0          IP Source not RP         : 0

PIM CRP invalid packet:
Invalid Dest Addr        : 0          Invalid CRP Addr         : 0
Fault Length             : 0          CRP Adv Fault Length     : 0
Invalid Multicast Group : 0

PIM Assert invalid packet:
Invalid Dest Addr        : 0          Invalid IP Source Addr  : 0
Invalid Multicast Source: 0           Invalid Multicast Group : 0

PIM BSR invalid packet:
Bad Payload              : 0          Fault Length             : 0
Bad Scope Mask           : 0          Invalid Multicast Group : 0
Not CBSR But BSR         : 0          Invalid BSR Addr         : 0
Fault Hash Length        : 0          Invalid IP Source Addr  : 0

PIM Hello invalid packet:
Invalid Addr List        : 0          Fault Length             : 0
Bad Holdtime Length      : 0          Bad LanPruneDelay Length: 0
Bad DrPriority Length    : 0          Bad GenID Length         : 0
Invalid Dest Addr        : 0          Invalid IP Source Addr  : 0

PIM Join/Prune invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
Invalid Up Neighbor      : 0          Invalid IP Source Addr  : 0
Invalid Dest Addr        : 0          Fault Length             : 0

PIM Graft invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
Invalid Up Neighbor      : 0          Invalid IP Source Addr  : 0
Fault Length             : 0

PIM Graft-Ack invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
Invalid Up Neighbor      : 0          Invalid IP Source Addr  : 0
Fault Length             : 0

PIM State Refresh invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0
Invalid Originator Addr : 0           Fault Length             : 0
-------------------------------------------------------------------
```

Table 8-46 Description of the **display pim invalid-packet** command output

Item	Description
PIM General invalid packet	General invalid PIM messages.
Invalid PIM Version	Number of messages with invalid PIM versions.
Invalid PIM Type	Number of messages with invalid PIM message types.

Item	Description
Fault Length	Number of messages of invalid lengths.
Bad Checksum	Number of messages with invalid checksum.
PIM Register invalid packet	Number of invalid PIM Register messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Invalid Multicast Group	Number of messages with invalid multicast group addresses.
Invalid Dest Addr	Number of messages with invalid destination addresses.
PIM Register-Stop invalid packet	Number of invalid PIM Register-Stop messages.
IP Source not RP	Number of messages whose source addresses are not the RP address.
PIM CRP invalid packet	Number of invalid PIM C-RP messages.
Invalid CRP Addr	Number of messages with invalid C-RP addresses.
CRP Adv Fault Length	Number of messages whose CRP Adv fields are of invalid lengths.
PIM Assert invalid packet	Number of invalid PIM Assert messages.
Invalid IP Source Addr	Number of messages with invalid multicast source addresses.
PIM BSR invalid packet	Number of invalid PIM BSR messages.
Bad Payload	Number of messages with invalid payloads.
Bad Scope Mask	Number of messages with invalid scope masks.
Not CBSR But BSR	Number of BSR messages received on interfaces that do not act as a C-BSR.
Invalid BSR Addr	Number of messages with invalid BSR addresses.
Fault Hash Length	Number of messages with hash mask fields of invalid lengths.
PIM Hello invalid packet	Number of invalid PIM Hello messages.
Invalid Addr List	Number of messages with invalid address lists.
Bad Holdtime Length	Number of messages with Holdtime fields of invalid lengths.

Item	Description
Bad LanPruneDelay Length	Number of messages with LanPruneDelay fields of invalid lengths.
Bad DrPriority Length	Number of messages with DrPriority fields of invalid lengths.
Bad GenID Length	Number of messages with Generation ID fields of invalid lengths.
PIM Join/Prune invalid packet	Number of invalid PIM Join/Prune messages.
Invalid Up Neighbor	Number of messages with invalid upstream neighbors.
PIM Graft invalid packet	Number of invalid PIM Graft messages.
PIM Graft-Ack invalid packet	Number of invalid PIM Graft-Ack messages.
PIM State Refresh invalid packet	Number of invalid PIM State-Refresh messages.
Invalid Originator Addr	Number of messages with invalid Originator address.

Display details of one invalid PIM message recently received on the switch.

```
<HUAWEI> display pim invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Interface           :  Vlanif10
Time                :  2010-6-1 20:04:35 UTC-08:00
Message Length      :  26
Invalid Type        :  Invalid Multicast Source
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00
0010: 00 00 80 00 00 64 00 00 00 00
-----------------------------------------------------
```

Table 8-47 Description of the **display pim invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of an invalid PIM message.
Packet information (Index 1)	Sequence number of the invalid PIM message (numbered in the opposite order the message is received. For example, the index of the last received message is 1, the index of the penultimate message is 2, and so on).
Interface	Interface that received the invalid PIM message.

Item	Description
Time	Time when the invalid SPT switch message was received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST The format UTC±HH:MM indicates that a time zone has been configured using the **clock timezone** command; DST indicates that the daylight saving time has been configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid PIM message.
Invalid Type	Type of the invalid PIM message.
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00 0010: 00 00 80 00 00 64 00 00 00 00	Contents of the invalid PIM message.

8.3.27 display pim neighbor

Function

The **display pim neighbor** command displays information about PIM neighbors.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Parameter	Description	Value
neighbor-address	Specifies the IP address of a PIM neighbor.	The address is in dotted decimal notation.
verbose	Displays detailed information about PIM neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim neighbor** command displays information about PIM neighbors, including the number of neighbors, DR priority, and BFD session status. You can adjust PIM neighbor relationships based on the command output.

When you run the **display pim neighbor** command:

- If you specify **interface** *interface-type interface-number*, the command displays information about PIM neighbors connected to the specified interface.
- If you do not specify **interface** *interface-type interface-number*, the command displays information about all PIM neighbors attached to the switch.

Example

Display information about all PIM neighbors.

```
<HUAWEI> display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 2

 Neighbor        Interface     Uptime       Expires      Dr-Priority  BFD-Session
 10.1.1.2        Vlanif10      02:50:49     00:01:31     1            Y
 10.1.2.2        Vlanif20      02:49:39     00:01:42     1            Y
```

Table 8-48 Description of the **display pim neighbor** command output

Item	Description
Total Number of Neighbors	Total number of PIM neighbors on an interface.
Neighbor	IP Address of a PIM neighbor.
Interface	Interface connected to a PIM neighbor.
Uptime	Time elapsed since a PIM neighbor relationship is set up.

Item	Description
Expires	Amount of time left before a PIM relationship times out.
Dr-Priority	DR priority of a PIM neighbor.
BFD-Session	Whether the BFD session has been set up with a neighbor. ● Y: The BFD session has been set up. ● N: The BFD session has not been set up.

Display detailed information about the PIM neighbor with IP address 10.1.1.2 in the public network instance.

```
<HUAWEI> display pim neighbor 10.1.1.2 verbose
 VPN-Instance: public net
 Neighbor: 10.1.1.2
     Interface: Vlanif 10
     Uptime: 02:53:50
     Expiry time: 00:01:30
     DR Priority: 1
     Generation ID: 0X90B0360B
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     Neighbor tracking: Disabled
     PIM BFD-Session: Y
     PIM BFD-Session min-tx-interval: 1000 ms
     PIM BFD-Session min-rx-interval: 1000 ms
     PIM BFD-Session detect-multiplier: 3
```

Table 8-49 Description of the **display pim neighbor verbose** command output

Item	Description
Expiry time	Amount of time left before a PIM relationship times out.
Generation ID	PIM neighbor status random value.
Holdtime	Keepalive period of the PIM neighbor.
LAN delay	Delay in transmitting Prune messages.
Override interval	Override interval for a prune action.
State refresh interval	Interval at which State-Refresh messages are sent.
Neighbor tracking	Whether the neighbor tracking function is enabled. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled.

Item	Description
PIM BFD-Session	Whether the BFD session is set up. ● Y: The BFD session has been set up. ● N: The BFD session has not been set up.
PIM BFD-Session min-tx-interval	Minimum interval at which PIM BFD packets are sent.
PIM BFD-Session min-rx-interval	Minimum interval at which PIM BFD packets are received.
PIM BFD-Session detect-multiplier	PIM BFD detection multiplier.

8.3.28 display pim routing-table

Function

The **display pim routing-table** command displays the PIM routing table.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table brief** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** }] *

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

display pim routing-table [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **register** | **none** } | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays PIM routing entries in a specified VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all-instance	Displays PIM routing entries in all the instances.	-
group-address	Displays the PIM routing entry of a specified group.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast source address or group address.	-
group-mask	Specifies the group address mask.	The address is in dotted decimal notation.
group-mask-length	Specifies the length of the group address mask.	The value is an integer that ranges from 4 to 32.
source-address	Displays the PIM routing entry of a specified multicast source.	The source address is in dotted decimal notation.
source-mask	Specifies the multicast source IP address mask.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the length of the source address mask.	The value is an integer that ranges from 0 to 32.
incoming-interface	Displays the PIM routing entries with a specified interface as the upstream interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface.	-
outgoing-interface	Displays the PIM routing entries with a specified interface as the downstream interface.	-
include	Displays the PIM routing entries with the downstream interface list containing a specified interface.	-

Parameter	Description	Value
exclude	Displays the PIM routing entries with the downstream interface list not containing a specified interface.	-
match	Displays the PIM routing entries with the downstream interface list containing only the specified interface.	-
none	Displays the PIM routing entries with an empty downstream interface list.	-
mode	Specifies the PIM operation mode.	-
dm	Displays PIM-DM routing entries.	-
sm	Displays PIM-SM routing entries.	-
ssm	Displays PIM-SSM routing entries.	-
flags *flag-value*	Displays PIM-SSM routing entries with the specified flag. The *flag-value* parameter is the type flag of entries.	-
fsm	Displays the details of FSM states.	-
outgoing-interface-number	Displays the number of downstream interfaces of PIM routing entries.	-
number	Specifies the number of the downstream interfaces to be displayed.	The value is an integer that ranges from 0 to 2048.
brief	Displays only the upstream interface names and the number of downstream interfaces in PIM routing entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to:

- Check whether PIM has been configured successfully on the network.
- Check the inbound interfaces, outbound interfaces, flags, and other information in the routing entries to identify failure points when forwarding errors occur on the PIM network.

The PIM routing table includes both (*, G) and (S, G) entries. (*, G) entries are used to set up a rendezvous point tree (RPT), and (S, G) entries are used to set up a shortest path tree (SPT).

Table 8-50 lists the values of the **flags** *flag-value* parameter.

Table 8-50 Values of the flag-value parameter

Item	Description
2msdp	The RP received a Register message recently and learned the (S, G) entry. The RP will notify MSDP of the (S, G) entry in the next SA message.
act	Multicast routing entries that have matched received data.
del	Multicast routing entries to be deleted.
exprune	Multicast routing entries pruned from the RPT, with no receiver interested in the data from the source.
ext	Multicast routing entries that contain downstream interfaces provided by other multicast routing protocols.
loc	Multicast routing entries on the switch directly connected to the network segment of the multicast source.
msdp	Multicast routing entries learned from recently received MSDP SA messages.
niif	Multicast routing entries with unknown upstream interfaces.
nonbr	Multicast routing entries in which the upstream neighbor address (link-local address) towards the RP or the source is not found.
none	Multicast routing entries without any flag.
rpt	Multicast routing entries that are on the RPT but do not use the RPT data.
sg_rcvr	The switch has receivers of the source specified in the (S, G) entry, and PIM is the owner of the downstream interfaces.
sgjoin	The switch has receivers of the source specified in the (S, G) entry, but PIM is not the owner of the downstream interfaces.

Item	Description
spt	Multicast routing entries on the shortest path tree (SPT).
swt	Multicast routing entries during the SPT switchover.
upchg	A route change has occurred. The current entry is using the original upstream interface to forward data and is waiting for data received from a new interface.
wc	(*, G) entry.

Example

Display the PIM routing table of the switch.

```
<HUAWEI> display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (172.16.0.12, 227.0.0.1)
     RP: 10.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Vlanif10
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlanif20
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 8-51 Description of the **display pim routing-table** command output

Item	Description
Total 0 (*, G) entry; 1 (S, G) entry	Total number of (S, G) and (*, G) entries in the PIM routing table.
(172.16.0.12, 227.0.0.1)	(S, G) entry in the PIM routing table.
RP	RP address.
Protocol	PIM protocol type, which can be PIM-DM, PIM-SM or PIM-SSM.
Flag	Flag of PIM (S, G) or (*, G) entry. Refer to the table of *Values of the flag-value parameter*.
UpTime	Amount of time an interface has been Up.
Upstream interface	Upstream interface in an (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of an (S, G) or (*, G) entry.

Item	Description
RPF prime neighbor	RPF neighbor of an (S, G) or (*, G) entry. ● For a (*, G) entry, when the local device is an RP, the RPF neighbor in the (*, G) entry is null. ● For an (S, G) entry, when the local device is directly connected to the source, the RPF neighbor in the (S, G) entry is null.
Downstream interface(s) information	Information about the downstream interface, including the following: ● Total number of downstream interfaces ● Name of each downstream interface ● PIM protocol type configured for the downstream interface ● Keepalive period and timeout period of the downstream interface
Total number of downstreams	Number of downstream interfaces.
Expires	Timeout period of an interface.

Display the number of the downstream interfaces of PIM routing entries on the switch.

```
<HUAWEI> display pim routing-table outgoing-interface-number
 VPN-Instance: public net
 Total 2 (*, G) entries; 0 (S, G) entry

 (*, 226.1.1.1)
     RP: 10.2.2.2 (local)
     Protocol: pim-sm, Flag: WC EXT
     UpTime: 21:37:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 50

 (*, 226.1.2.1)
     RP: 10.2.2.2 (local)
     Protocol: pim-sm, Flag: WC EXT
     UpTime: 21:37:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 50
```

Table 8-52 Description of the **display pim routing-table outgoing-interface-number** command output

Item	Description
Total 2 (*, G) entries; 0 (S, G) entry	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
Total number of downstreams	Total number of the downstream interfaces of the (*, G) entries or (S, G) entries.

8.3.29 display pim rp-info

Function

The **display pim rp-info** command displays information about the RP for a multicast group.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **rp-info** [*group-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
group-address	Displays the information about the RP for a specified multicast group.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view information about the RP for a multicast group.

Configuration Impact

The command output includes information about the RP discovered through the BSR mechanism and static RP.

If *group-address* is not specified, the command displays RP information for all the multicast groups.

Example

Display RP information for all the multicast groups in the public network instance.

```
<HUAWEI> display pim rp-info
 VPN-Instance: public net
 PIM-SM BSR RP Number:1
 Group/MaskLen: 224.0.0.0/4
     RP: 10.2.2.2 (local)
     Priority: 0
     Uptime: 03:01:36
     Expires: 00:02:29
 PIM SM static RP Number:1
     Static RP: 10.1.1.1
```

Table 8-53 Description of the **display pim rp-info** command output

Item	Description
PIM-SM BSR RP Number	Number of PIM-SM RPs elected dynamically using the BSR mechanism.
Group/MaskLen	Multicast group address and mask length.
RP	RP address.
Priority	Priority of the RP.
Uptime	Time elapsed since presence of the RP.
Expires	Amount of time left before the RP times out.
PIM SM static RP Number	Number of static RPs.
Static RP	IP address of a static RP.

8.3.30 graceful-restart (IPv4)

Function

The **graceful-restart** command enables PIM GR.

The **undo graceful-restart** command disables PIM GR.

By default, PIM GR is not enabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a stack is used on the PIM-SM network, after an active/standby switchover occurs in the stack system, multicast data transmission is interrupted because the new master device does not have PIM forwarding entries.

PIM GR enables the system to back up join and prune information in PIM routing entries to the new master device when an active/standby switchover is performed in the system. This ensures normal multicast data forwarding during restoration of the multicast distribution tree. For details about stack configuration, see Stack Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

At least one switch interface must have PIM-SM enabled for the **graceful-restart** command to take effect.

Example

Enable PIM GR in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] graceful-restart
```

8.3.31 graceful-restart period (IPv4)

Function

The **graceful-restart period** command configures the minimum PIM GR period.

The **undo graceful-restart period** command restores the default minimum PIM GR period.

By default, the minimum PIM GR period is 120 seconds.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	The value is an integer that ranges from 90 to 3600 in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimum time for maintaining forwarding entries.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If you run the **graceful-restart period** command multiple times, only the latest configuration takes effect.

Precautions

Unicast protocol GR form the basis of PIM GR; therefore, the minimum PIM GR period must be longer than the unicast protocol GR period.

The PIM GR period also depends on the complexity of the network topology and increases with the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the PIM view of public network instance to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
```

```
[HUAWEI-pim] graceful-restart
[HUAWEI-pim] graceful-restart period 150
```

8.3.32 hello ipsec sa (IPv4)

Function

The **hello ipsec sa** command specifies an IPSec SA globally used for encrypting and authenticating PIM Hello (IPv4) messages sent and received by the device.

The **undo hello ipsec sa** command deletes the IPSec SA globally used for encrypting and authenticating PIM Hello (IPv4) messages sent and received by the device.

By default, no IPSec SA is specified for encrypting and authenticating PIM Hello (IPv4) messages.

Format

hello ipsec sa *sa-name*

undo hello ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of the globally used SA.	The value is an existing SA name.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Huawei device connects to a non-Huawei device that can only encrypt and authenticate PIM Hello messages, run this command to configure the Huawei device to encrypt and authenticate only PIM Hello messages, so that the devices can interwork.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- Basic IPSec functions have been configured.

Precautions

If you run both this command and the **ipsec sa (IPv4)** command in the PIM view, the last configured one takes effect.

This command has the same function as the **pim hello ipsec sa** command used in the interface view except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM Hello messages using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello ipsec sa sa1
```

8.3.33 hello-option dr-priority (IPv4)

Function

The **hello-option dr-priority** command configures the priority of the switch that candidates for the Designated Router (DR).

The **undo hello-option dr-priority** command restores the default priority.

By default, the priority of the switch that candidates for the DR is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the switch that candidates for the DR. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 4294967295.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, switches on a shared network segment are candidates for the DR. The DR is responsible for registration of local multicast sources and the joining of receivers.

The DR is elected based on the priority and the IP address. Candidates send Hello messages with their priorities, and the switch with the highest priority becomes the DR. If multiple switches have the same priority, the switch with the largest IP address becomes the DR.

If at least one switch in the network does not support Hello packets that contain the priority, the switch with the largest IP address becomes the DR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **hello-option dr-priority** command has the same function as the **pim hello-option dr-priority** command in the interface view. By default, if the **pim hello-option dr-priority** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM view of public network instance, configure the DR priority of a switch to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option dr-priority 3
```

8.3.34 hello-option holdtime (IPv4)

Function

The **hello-option holdtime** command sets the timeout period for a switch to wait to receive Hello messages from its PIM neighbor.

The **undo hello-option holdtime** command restores the default configuration.

By default, the timeout period for a switch to wait to receive Hello messages from its PIM neighbor is 105 seconds.

Format

hello-option holdtime *interval*

undo hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which a switch waits to receive a Hello message from its PIM neighbor.	The value is an integer ranging from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, after the switch receives a Hello message from its PIM neighbor, it starts a timer. The timer length is the value of Holdtime in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, it considers the neighbor invalid or unreachable.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- The **hello-option holdtime** command is valid for PIM-SM and PIM-DM.
- The timeout period must be greater than the interval for sending Hello messages. You can run the **timer hello** command to set the interval for sending Hello messages.
- The **hello-option holdtime** command has the same function as the **pim hello-option holdtime** command in the interface view. By default, if the **pim hello-option holdtime** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM view of public network instance, set the timeout interval to 120 seconds. The timeout interval is the period during which a switch waits to receive the Hello message from its PIM neighbor.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option holdtime 120
```

8.3.35 hello-option lan-delay (IPv4)

Function

The **hello-option lan-delay** command sets the delay in transmitting Prune message on the shared network segment.

The **undo hello-option lan-delay** command restores the default delay.

By default, the delay in transmitting Prune message on the shared network segment is 500 milliseconds.

Format

hello-option lan-delay *interval*

undo hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting Prune message on the shared network segment.	The value is an integer that ranges from 1 to 32767, in milliseconds (ms).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If switches on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of the **lan-delay** and **override-interval** values, and refers to the delay from the switch receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface in PPT, the switch cancels the prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the delay in transmitting Prune message is too short, the upstream switch will stop forwarding multicast packets before the downstream switch determines whether to override the Prune action or not. Exercise caution when you run the **hello-option lan-delay** command.

The **hello-option lan-delay** command has the same function as the **pim hello-option lan-delay** command in the interface view. By default, if the **pim hello-option lan-delay** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting Prune message on the shared network segment to 200 ms in PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option lan-delay 200
```

8.3.36 hello-option neighbor-tracking (IPv4)

Function

The **hello-option neighbor-tracking** command enables the neighbor tracking function.

The **undo hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the status of the switch changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the switch to update the neighbor relationship. If multiple devices on the shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when this function is enabled on all devices on the shared network segment.

The **hello-option neighbor-tracking** command has the same function as the **pim hello-option neighbor-tracking** command in the interface view. By default, if neighbor tracking is not used on an interface, the neighbor tracking configuration in the PIM view takes effect.

Example

In the PIM view of public network instance, enable the downstream neighbor tracking function.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option neighbor-tracking
```

8.3.37 hello-option override-interval (IPv4)

Function

The **hello-option override-interval** command sets the interval for overriding the prune action in a Hello message.

The **undo hello-option override-interval** command restores the default interval.

By default, the interval for overriding the prune action in a Hello message is 2500 ms.

Format

hello-option override-interval *interval*

undo hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** parameters. The **override-interval** parameter indicates the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

When a device has only one PIM neighbor on a link and receives a Prune message from the neighbor, the device immediately deletes the downstream interface of the multicast routing entry. If a device has two or more PIM neighbors on a link and the **override-interval** values in the messages sent from the two neighbors are different, the largest **override-interval** value takes effect.

The value of Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT times out. If the switch receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

The **hello-option override-interval** command has the same function as the **pim hello-option override-interval** command in the interface view. By default, if the **pim hello-option override-interval** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM view of public network instance, set the interval for denying the prune action in a Hello message to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] hello-option override-interval 2000
```

8.3.38 holdtime assert (IPv4)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local switch.

The **undo holdtime assert** command restores the default timeout.

By default, the timeout period for all PIM interfaces to keep the Assert state on the local switch is 180 seconds.

Format

holdtime assert *interval*

undo holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the time during which the PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **holdtime assert** command is valid for PIM-SM and PIM-DM.

The **holdtime assert** command has the same function as the **pim holdtime assert** command in the interface view. By default, if the timeout period is not used on an interface, the timeout period configured in the PIM view is used.

Example

In the PIM view of public network instance, set the interval during which a switch keeps the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] holdtime assert 100
```

8.3.39 holdtime join-prune (IPv4)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. The devices that receive Join/Prune messages set the time during which the downstream interface keeps the Join or Prune state according to holdtime.

The **undo holdtime join-prune** command restores the default value.

By default, the holdtime value in Join/Prune messages sent by all PIM interfaces is 210 seconds.

Format

holdtime join-prune *interval*

undo holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime carried in Join/Prune messages sent by the local switch.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the hold timer. If this message carries group-join information and the switch does not receive subsequent Join/Prune messages from the downstream device when the timer expires, it suppresses multicast data forwarding to downstream interfaces of the specified group. If Join/Prune message carries group-prune information, the switch resumes multicast data forwarding to downstream interfaces when the hold timer expires.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages and is generally 3.5 times the interval for sending Join/Prune messages.

The **holdtime join-prune** command has the same function as the **pim holdtime join-prune** command in the interface view. By default, if the holdtime value is not used on an interface, the holdtime value configured in the PIM view is used.

Example

In the PIM view of public network instance, set the time during which the downstream interface of a switch keeps the Join or Prune state to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] holdtime join-prune 280
```

8.3.40 ipsec sa (IPv4)

Function

The **ipsec sa** command specifies an IPSec SA globally used for encrypting and authenticating PIM messages sent and received by the device.

The **undo ipsec sa** command deletes the IPSec SA globally used for encrypting and authenticating PIM messages sent and received by the device.

By default, no IPSec SA is specified for encrypting and authenticating PIM messages.

Format

ipsec [**unicast-message**] **sa** *sa-name*

undo ipsec [**unicast-message**] **sa**

Parameters

Parameter	Description	Value
unicast-message	Authenticates only PIM unicast messages. If you do not specify this keyword, the device authenticates only PIM multicast messages.	-
sa-name	Specifies the name of the globally used SA.	The value is an existing SA name.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IPv4 multicast network, if multicast devices are attacked by forged PIM messages, multicast data forwarding between multicast devices will be interrupted. To protect multicast devices against such attacks, configure PIM IPSec on the multicast devices to authenticate PIM messages they send and receive.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.

- Basic IPSec functions have been configured.

Precautions

If you run both the **ipsec sa** *sa-name* command and the **hello ipsec sa (IPv4)** command in the PIM view, the last configured one takes effect.

This command has the same function as the **pim ipsec sa** command used in the interface view, except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM multicast messages using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] ipsec sa sa1
```

8.3.41 join-prune max-packet-length (IPv4)

Function

The **join-prune max-packet-length** command sets the maximum size of each PIM-SM Join/Prune message to be sent.

The **undo join-prune max-packet-length** command restores the default maximum size of each PIM-SM Join/Prune message to be sent.

By default, the maximum length of Join/Prune message sent by PIM-SM is 8100 bytes.

Format

join-prune max-packet-length *packet-length*

undo join-prune max-packet-length

Parameters

Parameter	Description	Value
packet-length	Specifies the maximum size of each PIM-SM Join/Prune message to be sent.	The value is an integer ranging from 100 to 8100, in bytes.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has low performance and takes a long time to process a large Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be reduced to relieve the burden on the peer device.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the maximum size specified in the **join-prune max-packet-length** command is greater than the interface MTU, the maximum size of each message to be sent is equal to the interface MTU.

Example

Set the maximum size of each Join/Prune message to be sent to 2100 bytes.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] join-prune max-packet-length 2100
```

8.3.42 join-prune periodic-messages queue-size (IPv4)

Function

The **join-prune periodic-messages queue-size** command sets the maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.

The **undo join-prune periodic-messages queue-size** command restores the default maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.

By default, a PIM-SM Join/Prune message that is sent every second contains 1020 entries.

Format

join-prune periodic-messages queue-size *queue-size*

undo join-prune periodic-messages queue-size

Parameters

Parameter	Description	Value
queue-size	Specifies the maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.	The value is an integer ranging from 16 to 4096.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has a low throughput, reduce the length of a queue for periodically sending messages to control the number of (S, G) entries. This setting allows the local device to send Join/Prune messages with a small number of (S, G) entries multiple times, preventing packet loss or route flapping.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

Example

Allow each PIM-SM Join/Prune message that is sent every second to carry a maximum of 2000 (S, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] join-prune periodic-messages queue-size 2000
```

8.3.43 join-prune triggered-message-cache disable (IPv4)

Function

The **join-prune triggered-message-cache disable** command disables the Join/Prune message package function.

The **undo join-prune triggered-message-cache disable** command enables the Join/Prune message package function.

By default, the Join/Prune message package function is enabled.

Format

join-prune triggered-message-cache disable

undo join-prune triggered-message-cache disable

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system performs more efficiently when sending package of PIM Join/Prune messages than when sending a large number of individual PIM Join/Prune messages. A switch sends PIM Join/Prune messages in packages. To disable the package function, run the **join-prune triggered-message-cache disable** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

Example

Disable the Join/Prune message package function.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] join-prune triggered-message-cache disable
```

8.3.44 neighbor-check (IPv4)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

By default, the PIM neighbor check function is not enabled.

Format

neighbor-check { **receive** | **send** }

undo neighbor-check { **receive** | **send** }

Parameters

Parameter	Description	Value
receive	Checks whether the Join/Prune and Assert messages are received from a PIM neighbor. If not, these messages are discarded.	-
send	Checks whether the Join/Prune and Assert messages are sent to a PIM neighbor. If not, these messages are not sent.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices send Join/Prune messages to the upstream PIM neighbor to perform join, and prune actions and PIM neighbors often exchange Assert messages. To save system resources and protect security of Join/Prune messages and Assert messages, run the **neighbor-check** command to enable the PIM neighbor check function.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

You can specify both **receive** and **send** to enable the PIM neighbor check function for the received and sent Join/Prune and Assert messages.

Precautions

This command is valid only for PIM-SM.

Example

In the PIM view of public network instance, enable the PIM neighbor check function for the received Join/Prune and Assert messages.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] neighbor-check receive
```

8.3.45 pim

Function

The **pim** command displays the PIM view.

The **undo pim** command clears the configuration in the PIM view.

Format

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing PIM configurations, run the **pim** command to enter the PIM view.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTE

Running the **undo pim** command in the system view may interrupt IPv4 PIM services and deletes all global IPv4 PIM configurations of the public network instance. To restore the IPv4 PIM services, you have to re-run the deleted commands.

Example

Enter the PIM view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] pim
[HUAWEI-pim]
```

8.3.46 pim bfd

Function

The **pim bfd** command adjusts the PIM BFD parameters on an interface.

The **undo pim bfd** command restores the default values of PIM BFD parameters.

By default, the minimum interval for transmitting BFD packets and minimum interval for receiving BFD packets are 1000 ms, and the BFD detection multiplier is 3.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *

undo pim bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo pim bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-value*	Specifies the minimum interval for transmitting BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
min-rx-interval *rx-value*	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
detect-multiplier *multiplier-value*	Specifies the BFD detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view, 100GE interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM BFD is enabled, you may need to run the **pim bfd** command to adjust PIM BFD parameters to adapt to the state of the link. This command can set the minimum interval for sending BFD packets, minimum interval for receiving PIM BFD packets, and local detection multiplier.

In application, you can continuously configure one or more parameters. If some parameters are configured, other parameters that are not configured reserve the existing configurations.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid only for PIM-SM.

Before setting PIM BFD parameters, run the **pim bfd enable** command to enable PIM BFD. Otherwise, the configured parameters do not take effect.

The minimum values of *tx-value* and *rx-value* vary with products.

Example

Adjust the minimum interval for transmitting BFD packets on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] pim sm
[HUAWEI-Vlanif10] pim bfd enable
[HUAWEI-Vlanif10] pim bfd min-tx-interval 100
```

Adjust the minimum interval for transmitting BFD packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
[HUAWEI-GigabitEthernet0/0/1] pim bfd enable
[HUAWEI-GigabitEthernet0/0/1] pim bfd min-tx-interval 100
```

8.3.47 pim bfd enable

Function

The **pim bfd enable** command enables PIM BFD on an interface.

The **undo pim bfd enable** command disables PIM BFD on an interface.

By default, PIM BFD is not enabled on an interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim bfd enable

undo pim bfd enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view, 100GE interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables PIM BFD on an interface to quickly detect link failures on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Run the **pim sm** command on the interface to enable PIM-SM. You can run the **undo pim sm** command to disable PIM BFD on the interface.

Precautions

This command is valid for only PIM-SM.

PIM BFD depends on the BFD protocol. If global BFD is not enabled using the **bfd** command, PIM BFD sessions can still be set up but the session state is **BFD global disable**.

Example

Enable PIM BFD on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim sm
[HUAWEI-Vlanif100] pim bfd enable
```

Enable PIM BFD on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
[HUAWEI-GigabitEthernet0/0/1] pim bfd enable
```

8.3.48 pim bsr-boundary

Function

The **pim bsr-boundary** command configures the BSR boundary of a PIM-SM domain on an interface.

The **undo pim bsr-boundary** command restores the default configuration.

By default, the BSR boundary of a PIM-SM domain is not set.

Format

pim bsr-boundary

undo pim bsr-boundary

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the management core of the PIM-SM network, the BSR is responsible for sending collected RP-set information to PIM neighbors through Bootstrap messages.

You can divide a large PIM-SM network into multiple PIM-SM domains by configuring the bsr boundary on an interface. Each BSR then serves the local PIM-SM domain.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

The Bootstrap messages cannot traverse the BSR boundary but other multicast packets can.

Example

Configure the BSR boundary of a PIM-SM domain on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim bsr-boundary
```

Configure the BSR boundary of a PIM-SM domain on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim bsr-boundary
```

8.3.49 pim dm

Function

The **pim dm** command enables PIM-DM on an interface.

The **undo pim dm** command restores the default configuration.

By default, PIM-DM is disabled on an interface.

Format

pim dm

undo pim dm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-DM network, after PIM-DM is enabled on an interface, the switch can set up the PIM neighbor relationship with the neighboring device. The switch can then process protocol packets received from the PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- PIM-DM and PIM-SM cannot be enabled simultaneously on interfaces bound to the same VPN instance or public network instance.
- If PIM-DM and IGMP need to be enabled on the same interface, enable PIM-DM, and then enable IGMP.

- If Layer 2 multicast querier or Layer 2 multicast packet suppression is enabled in a VLAN, running the **pim dm** command on the corresponding VLANIF interface will fail.
- If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable IPv4 PIM on the corresponding VLANIF interface first, and then enable IGMP snooping in the VLAN. If IGMP snooping is enabled in the VLAN first, IPv4 PIM cannot be enabled on the corresponding VLANIF interface.
- PIM-DM cannot be deployed on the public network of the MVPN.
- Since V200R010, the S5720-HI, S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S support IPv4 PIM configuration on dot1q and QinQ termination sub-interfaces only when the VLAN tag to be terminated (or both inner and outer VLAN tags on the QinQ termination sub-interface) is a single VLAN ID, but not a range of VLAN IDs. Sub-interfaces running PIM can only be used as inbound interfaces of multicast streams and cannot be used as outbound interfaces. The S5720-EI, S6720-EI, S6735-S, and S6720S-EI also support IPv4 PIM command configuration on dot1q and QinQ termination sub-interfaces, but they do not support multicast traffic forwarding on these sub-interfaces.
- PIM-DM and PIM-SM cannot be configured simultaneously in a VPN instance or the public network instance. IPv4 PIM can be configured in a VPN instance, but the VPN instance cannot be bound to a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command. Only the following products and versions support the IPv4 PIM multi-instance feature:
  - S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S: all versions
  - S6700-EI and S5700-HI: V200R005C01
  - S6700-EI, S5700-HI, and S5710-HI: V200R005C02
  - S5710-HI: V200R005C03
  - S5720-EI, S5720-HI, S6720-EI, S6735-S, and S6720S-EI: V200R010 and later versions
- Secondary IP addresses does not support PIM, and the direct routes generated based on secondary IP addresses are not involved during multicast RPF check. Therefore, if the source IP address of multicast packets is on the same network segment as the secondary IP address of a Layer 3 interface, these multicast packets received on the Layer 3 interface cannot pass the RPF check.

Example

Enable PIM-DM on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim dm
```

Enable PIM-DM on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim dm
```

8.3.50 pim dr-election dr-priority

Function

The **pim dr-election dr-priority** command configures an IP address and a priority for PIM DR election.

The **undo dr-election dr-priority** command restores the default IP address and priority for PIM DR election.

By default, no IP address or priority is configured for PIM DR election.

NOTE

This command is supported only on the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, and S5731-H.

Format

pim dr-election *ip-address* **dr-priority** *priority-value*

undo pim dr-election *ip-address* **dr-priority** *priority-value*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address used for PIM DR election.	The value is in dotted decimal notation.
dr-priority *priority-value*	Specifies the DR priority of a PIM interface. A larger value indicates a higher priority.	The value is an integer in the range from 0 to 4294967295.

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a VXLAN multi-border distributed gateway scenario, the same primary IP address is configured for VBDIF interfaces on multiple border nodes. These VBDIF interfaces use the primary IP address to send PIM protocol packets. During PIM negotiation, the local device considers itself as a PIM DR and forwards multicast traffic. As a result, excessive multicast traffic instead of only one copy of multicast traffic is forwarded. In this case, you can run this command to specify the IP address used to send PIM protocol packets.

During PIM DR election, the IP address and DR priority configured using the **pim dr-election dr-priority** command take precedence over the interface IP address and the DR priority configured using the **pim hello-option dr-priority** command.

During PIM Assert election, the IP address configured using the **pim dr-election dr-priority** command takes precedence over the interface IP address.

Precautions

- PIM can be configured on a VBDIF interface, which supports only DR election.
- In the multi-border distributed gateway scenario, to solve the problem of multiple copies of multicast traffic on the network segment where the VBDIF interface resides, configure different IP addresses for PIM DR election.
- If a fault occurs in the multi-border scenario, PIM needs to be associated with BFD to implement fast route switchover. In this case, you need to configure a secondary IP address that is the same as the IP address for PIM DR election on the VBDIF interface to send BFD packets.
- After the **pim dr-election dr-priority** command is run on a VBDIF interface, the **pim hello-option dr-priority** command no longer takes effect.

Example

Set the IP address and priority for DR election on VBDIF 10 to 10.0.0.1 and 20 respectively.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] quit
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] pim dr-election 10.1.1.2 dr-priority 20
```

8.3.51 pim hello ipsec sa

Function

The **pim hello ipsec sa** command specifies an IPSec SA used for encrypting and authenticating PIM Hello messages sent and received on an interface.

The **undo pim hello ipsec sa** command deletes the IPSec SA used for encrypting and authenticating PIM Hello messages sent and received on an interface.

By default, no IPSec SA is specified for encrypting and authenticating PIM Hello messages on an interface.

Format

pim hello ipsec sa *sa-name*

undo pim hello ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of the SA used on an interface.	The value is an existing SA name.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Huawei device connects to a non-Huawei device that can only encrypt and authenticate PIM Hello messages, run this command to configure the Huawei device to encrypt and authenticate only PIM Hello messages.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- Basic IPSec functions have been configured.

Precautions

If you run both this command and the **pim ipsec sa** command on an interface, the last configured one takes effect.

This command has the same function as the **hello ipsec sa (IPv4)** command used in the PIM view, except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM Hello messages sent and received on VLANIF100 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello ipsec sa sa1
```

Configure the device to encrypt and authenticate PIM Hello messages sent and received on GE0/0/1 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello ipsec sa sa1
```

8.3.52 pim hello-option dr-priority

Function

The **pim hello-option dr-priority** command sets the priority for the PIM interface that is elected as DR.

The **undo pim hello-option dr-priority** command restores the default value of the priority.

By default, the priority for the PIM interface that is elected as DR is 1.

Format

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the PIM interface that is elected as DR. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 4294967295.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, switches on a shared network segment are candidates for the DR. The DR is responsible for registration of local multicast sources and the joining of receivers.

The DR is elected based on the priority and the IP address. Candidates send Hello messages with their priorities, and the switch with the highest priority becomes the DR. If multiple switches have the same priority, the switch with the largest IP address becomes the DR.

If at least one switch in the network does not support Hello packets that contain the priority, the switch with the largest IP address becomes the DR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **pim hello-option dr-priority** command has the same function as the **hello-option dr-priority (IPv4)** command in the PIM view. By default, if the **pim hello-option dr-priority** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the priority of VLANIF100 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option dr-priority 3
```

Set the priority of GE0/0/1 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option dr-priority 3
```

8.3.53 pim hello-option holdtime

Function

The **pim hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

The **undo pim hello-option holdtime** command restores the default value of the timeout.

By default, the timeout period during which the PIM interface waits to receive the Hello message from its neighbor is 105 seconds.

Format

pim hello-option holdtime *interval*

undo pim hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the PIM interface waits to receive Hello messages from its neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM network, after the switch receives a Hello message from its PIM neighbor, it starts a timer. The timer length is the value of Holdtime in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, it considers the neighbor invalid or unreachable.

The **pim hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The timeout period must be greater than the interval for sending Hello messages, which is set using the **pim timer hello** command.

The **pim hello-option holdtime** command has the same function as the **hello-option holdtime (IPv4)** command in the PIM view. By default, if the **pim hello-option holdtime** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period during which VLANIF100 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option holdtime 120
```

Set the timeout period during which GE0/0/1 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option holdtime 120
```

8.3.54 pim hello-option lan-delay

Function

The **pim hello-option lan-delay** command sets the delay in transmitting messages in a shared network in the interface view.

The **undo pim hello-option lan-delay** command restores the default value of the delay.

By default, the delay in transmitting messages in the shared network is 500 ms.

Format

pim hello-option lan-delay *interval*

undo pim hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If switches on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of the **lan-delay** and **override-interval** values, and refers to the delay from the switch receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface in PPT, the switch cancels the prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the prune delay is set too short, the upstream switch stops forwarding multicast packets before the downstream switch overrides Prune messages of neighbors. Exercise caution when you run this command.

The function of this command in the interface view is the same as that of the **hello-option lan-delay (IPv4)** command in the PIM view. By default, if the configuration on the interface is not performed, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting messages to 200 ms in VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option lan-delay 200
```

Set the delay in transmitting messages to 200 ms in GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option lan-delay 200
```

8.3.55 pim hello-option neighbor-tracking

Function

The **pim hello-option neighbor-tracking** command enables the neighbor tracking function in the interface view.

The **undo pim hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

pim hello-option neighbor-tracking

undo pim hello-option neighbor-tracking

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the status of the switch changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the switch to update the neighbor relationship. If multiple devices on the shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when all devices on the shared network segment have this function enabled.

The **pim hello-option neighbor-tracking** command has the same function as the **hello-option neighbor-tracking (IPv4)** command in the PIM view. By default, if the **pim hello-option neighbor-tracking** command is not used, the configuration in the PIM view takes effect; otherwise, the configuration in the interface view takes effect.

Example

Enable the neighbor tracking function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option neighbor-tracking
```

Enable the neighbor tracking function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option neighbor-tracking
```

8.3.56 pim hello-option override-interval

Function

The **pim hello-option override-interval** command sets the interval carried in Hello messages for overriding the prune action on the interface.

The **undo pim hello-option override-interval** command, restores the default configuration.

By default, the interval carried in Hello messages for overriding the prune action on the interface is 2500 milliseconds.

Format

pim hello-option override-interval *interval*

undo pim hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval of overriding the prune action.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** parameters. The **override-interval** parameter indicates the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, other switches that still request multicast data need to send a Join message to the upstream device within the override-interval period.

When a device has only one PIM neighbor on a link and receives a Prune message from the neighbor, the device immediately deletes the downstream interface of the multicast routing entry. If a device has two or more PIM neighbors on a link and the **override-interval** values in the messages sent from the two neighbors are different, the largest **override-interval** value takes effect.

The value of Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT times out. If the switch receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If you run the **pim hello-option override-interval** command multiple times, only the latest configuration takes effect.

Precautions

This command is valid for PIM-SM and PIM-DM.

The **pim hello-option override-interval** command has the same function as the **hello-option override-interval (IPv4)** command in the PIM view. By default, if the **pim hello-option override-interval** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval for overriding the prune action in Hello messages to 2000 ms in VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim hello-option override-interval 2000
```

Set the interval for overriding the prune action in Hello messages to 2000 ms in GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim hello-option override-interval 2000
```

8.3.57 pim holdtime assert

Function

The **pim holdtime assert** command sets the timeout period during which a PIM interface keeps the Assert state.

The **undo pim holdtime assert** command restores the default value of the timeout.

By default, the timeout period during which a PIM interface keeps the Assert state is 180 seconds.

Format

pim holdtime assert *interval*

undo pim holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which a PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, devices that failed the previous election triggers a new round of election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

The **pim holdtime assert** command has the same function as the **holdtime assert (IPv4)** command in the PIM view. By default, if the **pim holdtime assert** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period for the interface VLANIF100 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim holdtime assert 100
```

Set the timeout period for the interface GE0/0/1 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim holdtime assert 100
```

8.3.58 pim holdtime join-prune

Function

The **pim holdtime join-prune** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **undo pim holdtime join-prune** command restores the default value of the holdtime.

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210 seconds.

Format

pim holdtime join-prune *interval*

undo pim holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the holdtime timer. If the switch does not receive subsequent Join/Prune messages from the downstream device within the holdtime interval, the switch suppresses forwarding of Join/Prune messages carrying group join information on the downstream interface in the group. If Join/Prune messages carry group prune information, the downstream interface is restored.

The **pim holdtime join-prune** command sets the holdtime interval for Join/Prune messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for PIM-SM and PIM-DM.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages and is generally 3.5 times the interval for sending Join/Prune messages.

The **pim holdtime join-prune** command has the same function as the **holdtime join-prune (IPv4)** command in the PIM view. By default, if the **pim holdtime join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the holdtime in a Join/Prune message sent by the interface VLANIF100 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim holdtime join-prune 280
```

Set the holdtime in a Join/Prune message sent by the interface GE0/0/1 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim holdtime join-prune 280
```

8.3.59 pim ipsec sa

Function

The **pim ipsec sa** command specifies an IPSec SA used for encrypting and authenticating PIM messages sent and received on an interface.

The **undo pim ipsec sa** command deletes the IPSec SA used for encrypting and authenticating PIM messages sent and received on an interface.

By default, no IPSec SA is specified for encrypting and authenticating PIM messages on an interface.

Format

pim ipsec sa *sa-name*

undo pim ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of the SA used on an interface.	The value is an existing SA name.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IPv4 multicast network, if multicast devices are attacked by forged PIM messages, multicast data forwarding between multicast devices will be interrupted. To protect multicast devices against such attacks, configure PIM IPSec on some interfaces to authenticate PIM messages sent and received on these interfaces.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command.
- Basic IPSec functions have been configured.

Precautions

If you run both this command and the **pim hello ipsec sa** command on an interface, the last configured one takes effect.

This command has the same function as the **ipsec sa (IPv4)** command used in the PIM view, except for the effective scope. The configuration in the interface view takes precedence over the configuration in the PIM view. If SAs are specified in both the interface view and PIM view, the specified interface uses the SA configured in the interface view. If no SA is specified on an interface, the interface uses the SA specified in the PIM view.

Example

Configure the device to encrypt and authenticate PIM messages sent and received on VLANIF100 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim ipsec sa sa1
```

Configure the device to encrypt and authenticate PIM messages sent and received on GE0/0/1 using the PIM IPSec SA named **sa1**. (This SA has been created.)

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim ipsec sa sa1
```

8.3.60 pim join-policy

Function

The **pim join-policy** command enables the system to filter join information in Join/Prune messages.

The **undo pim join-policy** command restores the default setting.

By default, join information in Join/Prune message is not filtered.

Format

pim join-policy { **asm** { *basic-acl-number* } | **ssm** { *advanced-acl-number* } | *advanced-acl-number* }

undo pim join-policy [**asm** | **ssm**]

Parameters

Parameter	Description	Value
asm	Filters join information, with the group address in the ASM group address range.	-
basic-acl-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
ssm	Filters join messages, with the group addresses within the SSM group address range and specified source address.	-
advanced-acl-number	Specifies the advanced ACL number.	The value is an integer that ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on a PIM-SM network by filtering join information in Join/Prune messages, run the **pim join-policy** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

The **pim join-policy** command is valid for only PIM-SM.

The **pim join-policy** command and the **acl** command are used together.

- If **asm** is specified, you can set the multicast group address range of join information in the basic ACL view by specifying the **source** parameter in the **rule** command.
- If **ssm** is specified, you can set the source address range and multicast group address range of join information in the advanced ACL view by specifying the **source** parameter and **destination** parameter in the **rule** command.

Example

Configure VLANIF100 to accept the join information with the group address in the range of 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim join-policy asm 2001
```

Configure GE0/0/1 to accept the join information with the group address in the range of 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim join-policy asm 2001
```

8.3.61 pim neighbor-policy

Function

The **pim neighbor-policy** command configures a policy for filtering PIM neighbors on an interface.

The **undo pim neighbor-policy** command restores the default setting.

By default, PIM neighbors on the interface are not filtered.

Format

pim neighbor-policy *basic-acl-number*

undo pim neighbor-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized neighbors from being involved in the PIM protocol, run the **pim neighbor-policy** command to configure a policy for filtering PIM neighbors and set the address range of PIM neighbors. The switch sets up neighbor relationships with the addresses matching the filtering rules and deletes the neighbors that do not match the filtering rules.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

The **pim neighbor-policy** command and the **acl** command are used together. In the ACL view, set the address range of PIM neighbors by specifying **source** in the **rule** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

When configuring the neighbor filtering function on the interface, you must also configure the neighbor filtering function correspondingly on the PIM neighbor of the interface.

If a PIM device has established a neighbor relationship with the switch but its IP address is not in the configured range of valid neighbor addresses, the switch will no longer receive Hello messages from this PIM neighbor. When the holdtime of Hello messages expires, the neighbor relationship between the PIM device and the switch is terminated.

Example

Allow VLANIF100 to set up a PIM neighbor relationship with a PIM device at 10.4.4.4.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.4.4.4 0.0.0.0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim neighbor-policy 2001
```

Allow GE0/0/1 to set up a PIM neighbor relationship with a PIM device at 10.4.4.4.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.4.4.4 0.0.0.0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim neighbor-policy 2001
```

8.3.62 pim require-genid

Function

The **pim require-genid** command configures a PIM interface to reject the Hello messages without the Generation ID.

The **undo pim require-genid** command restores the default configuration.

By default, a PIM interface receives the Hello messages without the Generation ID.

Format

pim require-genid

undo pim require-genid

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface on the switch is enabled with PIM, the switch generates a random number as the Generation ID of the Hello message. If the status of the switch is updated, the switch generates a new Generation ID. When the switch finds that the Hello message received from a PIM neighbor contains a different Generation ID, it considers that the status of the PIM neighbor has changed.

To ensure that PIM neighbors work properly, run the **pim require-genid** command to configure a PIM interface to reject the Hello messages without the Generation ID.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

Configure VLANIF100 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim require-genid
```

Configure GE0/0/1 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim require-genid
```

8.3.63 pim silent

Function

The **pim silent** command enables the PIM silent function on an interface.

The **undo pim silent** command cancels the PIM silent function on an interface.

By default, the PIM silent function is disabled on an interface.

Format

pim silent

undo pim silent

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the switch against pseudo PIM Hello messages sent from malicious hosts, configure the **pim silent** command on the interface directly connected to the host network segment to set the interface to PIM silent mode. Then the interface cannot receive or forward any PIM packet, and all PIM neighbors and PIM state machines on this interface are deleted. This interface becomes the DR, but the IGMP function on the interface is not affected.

The PIM silent function applies only to the interface directly connected to a host network segment, and only one PIM switch can be connected to this network segment.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

Running the **pim silent** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If PIM BFD function is enabled on the interface, this command cannot be configured.

This command and **pim timer dr-switch-delay** command are mutually exclusive.

NOTICE

After you run this command on an interface, the interface no longer receives or sends any PIM packets and other PIM functions on the interface become invalid. Confirm your action before using this command.

If a host network segment is connected to multiple switches and PIM silent is enabled on multiple interfaces, all these interfaces become static DRs. This causes multicast forwarding failures.

Example

Configure the PIM silent function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim silent
```

Configure the PIM silent function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim silent
```

8.3.64 pim sm

Function

The **pim sm** command enables PIM-SM on an interface.

The **undo pim sm** command restores the default configuration.

By default, PIM-SM is disabled on an interface.

Format

pim sm

undo pim sm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With PIM-SM enabled on interfaces, switches can set up PIM neighbor relationships and process protocol packets received from PIM neighbors.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

- PIM-DM and PIM-SM cannot be enabled simultaneously on interfaces bound to the same VPN instance or public network instance.
- If PIM-SM and IGMP need to be enabled on the same interface, enable PIM-SM, and then enable IGMP.
- Running the **pim sm** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.
- If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable PIM on the corresponding VLANIF interface first, and then enable IGMP snooping in the VLAN. If IGMP snooping is enabled in the VLAN first, PIM cannot be enabled on the VLANIF interface.
- In versions earlier than V200R022C10, VBDIF interfaces cannot be configured as inbound or outbound interfaces of multicast entries. In V200R022C10, VBDIF interfaces can only be configured as outbound interfaces of multicast entries, and cannot be configured as inbound interfaces. In V200R023C00 and later versions, VBDIF interfaces can be configured as both inbound and outbound interfaces of multicast entries.
- After super VXLAN resource mode is configured using the **set vxlan resource super-mode** command, a maximum of 12,288 VBDIF interfaces can be configured as inbound interfaces of multicast entries. If the number of VBDIF interfaces to be configured as inbound interfaces exceeds the upper limit, the configuration takes effect only for the first 12,288 VBDIF interfaces.
- PIM can be configured on VBDIF interfaces. A VBDIF interface that has PIM configured can only connect the multicast source and receives, and it cannot function as a PIM interconnection interface.
- Since V200R010, the S5720-HI, S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S support IPv4 PIM configuration on dot1q and QinQ termination sub-interfaces only when the VLAN tag to be terminated (or both inner and outer VLAN tags on the QinQ termination sub-interface) is a single VLAN ID, but not a range of VLAN IDs. Sub-interfaces running PIM can only be used as inbound interfaces of multicast streams and cannot be used as outbound interfaces. The S5720-EI, S6720-EI, S6735-S, and S6720S-EI also support IPv4 PIM command configuration on dot1q and QinQ termination sub-interfaces, but they do not support multicast traffic forwarding on these sub-interfaces.
- PIM-DM and PIM-SM cannot be configured simultaneously in a VPN instance or the public network instance. IPv4 PIM can be configured in a VPN instance, but the VPN instance cannot be bound to a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command. Only the following products and versions support the IPv4 PIM multi-instance feature:
  - S5730-HI, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-HI, S6730-H, S6730S-H, S6730-S, and S6730S-S: all versions
  - S6700-EI and S5700-HI: V200R005C01
  - S6700-EI, S5700-HI, and S5710-HI: V200R005C02
  - S5710-HI: V200R005C03
  - S5720-EI, S5720-HI, S6720-EI, S6735-S, and S6720S-EI: V200R010 and later versions
- Secondary IP addresses does not support PIM, and the direct routes generated based on secondary IP addresses are not involved during multicast RPF check. Therefore, if the source IP address of multicast packets is on the same

network segment as the secondary IP address of a Layer 3 interface, these multicast packets received on the Layer 3 interface cannot pass the RPF check.

Example

Enable PIM-SM on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim sm
```

Enable PIM-SM on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim sm
```

8.3.65 pim state-refresh-capable

Function

The **pim state-refresh-capable** command enables PIM-DM state refresh on an interface.

The **undo pim state-refresh-capable** command disables PIM-DM state refresh.

By default, PIM-DM state refresh is enabled.

Format

pim state-refresh-capable

undo pim state-refresh-capable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM state refresh is implemented by periodically sending State-Refresh messages in the network. After receiving a State-Refresh message, the switch in the pruned state resets the prune-status timer, preventing the downstream interface from forwarding packets.

After PIM-DM state refresh is disabled on an interface, the interface starts to forward multicast data when the prune timer expires. The downstream routers that do not want to receive the data send Prune messages. The process repeats, wasting a lot of network resources. Enabling PIM-DM state refresh can reduce traffic on the network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Disable PIM-DM state refresh on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo pim state-refresh-capable
```

Disable PIM-DM state refresh on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] undo pim state-refresh-capable
```

8.3.66 pim timer dr-switch-delay

Function

The **pim timer dr-switch-delay** command enables PIM DR switching delay and configures the delay on an interface. When the interface changed from a DR to a non-DR, the interface continues to forward data before the delay expires.

The **undo pim timer dr-switch-delay** command disables PIM DR switching delay on the interface.

By default, when the interface changes from a DR to a non-DR, the interface stops forwarding data immediately.

Format

pim timer dr-switch-delay *interval*

undo pim timer dr-switch-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DR on a shared network segment becomes the non-DR, original multicast forwarding entries will be deleted immediately, causing multicast data interruption in a short time. To solve the problem, set the DR switching delay. Original multicast forwarding entries still take effect until the delay is reached.

After a new PIM neighbor joins, the outbound interface may not function as a DR any more; however, within the switching delay or before the new DR takes effect to forward multicast traffic, the original outbound interface still has the DR function and continues to forward multicast data. In this manner, non-stop multicast traffic forwarding is ensured during DR switchover.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

This command and **pim silent** command are mutually exclusive.

Example

Enable PIM DR switching delay on VLANIF100 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer dr-switch-delay 20
```

Enable PIM DR switching delay on GE0/0/1 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer dr-switch-delay 20
```

8.3.67 pim timer graft-retry

Function

The **pim timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

The **undo pim timer graft-retry** command restores the default value of the interval.

By default, the interval for retransmitting Graft messages on an interface is 3 seconds.

Format

pim timer graft-retry *interval*

undo pim timer graft-retry

Parameters

Parameter	Description	Value
interval	Specifies the interval of retransmitting Graft messages.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM mode, when a member joins a pruned group, the switch sends a Graft message and waits to receive an ACK message from the upstream switch. If the downstream switch does not receive the ACK message in the period configured through the command, the switch resends the Graft message until the switch receives the ACK message from the upstream switch.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Set the interval for retransmitting Graft messages to 80s on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer graft-retry 80
```

Set the interval for retransmitting Graft messages to 80s on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer graft-retry 80
```

8.3.68 pim timer hello

Function

The **pim timer hello** command sets the interval for sending Hello messages on an interface.

The **undo pim timer hello** command restores the default value of the interval.

By default, the interval for sending Hello messages on an interface is 30 seconds.

Format

pim timer hello *interval*

undo pim timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim timer hello** command to set the interval for sending Hello messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors, which is set using the **hello-option holdtime (IPv4)** command.

The configuration is the same as the **timer hello (IPv4)** command in the PIM view but takes precedence over the command used in the PIM view. The value configured in the PIM view is used if no value is configured on the interface.

Example

Set the interval for sending Hello messages to 40 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer hello 40
```

Set the interval for sending Hello messages to 40 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer hello 40
```

8.3.69 pim timer join-prune

Function

The **pim timer join-prune** command sets the interval for periodically sending Join/Prune messages to the upstream device.

The **undo pim timer join-prune** command restores the default interval.

By default, the interval for periodically sending Join/Prune messages to the upstream device is 60 seconds.

Format

pim timer join-prune *interval*

undo pim timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Join/Prune messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends join information to the upstream device, requesting the upstream device to forward multicast data. The device sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The device periodically sends Join/Prune messages to the upstream device to update the forwarding status.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid only for PIM-SM.

The interval configured through this command must be shorter than the interval configured through the **pim holdtime join-prune** command. The interval at which Join or Prune messages are sent must be shorter than the holdtime carried in Join/Prune messages.

The configuration is the same as that of the **timer join-prune (IPv4)** command in the PIM view. The system prefers the configuration in the interface view. The value configured in the PIM view is used if no value is configured on the interface.

Example

Set the interval for sending Join or Prune messages to 80 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim timer join-prune 80
```

Set the interval for sending Join or Prune messages to 80 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim timer join-prune 80
```

8.3.70 pim triggered-hello-delay

Function

The **pim triggered-hello-delay** command sets the maximum delay for triggering Hello messages.

The **undo pim triggered-hello-delay** command restores the default maximum delay.

By default, the maximum delay for triggering Hello messages is 5 seconds.

Format

pim triggered-hello-delay *interval*

undo pim triggered-hello-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum delay for triggering Hello messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Conflicts will occur if multiple PIM devices send Hello message at the same time. To avoid such conflicts, when a PIM device detects Hello messages on the network, it waits for a random delay that is smaller than the value configured using this command before sending a Hello message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Set the maximum delay for triggering the Hello message to 3 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] pim triggered-hello-delay 3
```

Set the maximum delay for triggering the Hello message to 3 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] pim triggered-hello-delay 3
```

8.3.71 probe-interval (IPv4)

Function

The **probe-interval** command sets the interval for a switch to send Probe messages (null Register message) to the RP.

The **undo probe-interval** command restores the default value of the interval.

By default, the interval for a switch to send Probe messages to the RP is 5 seconds.

Format

probe-interval *interval*

undo probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Probe messages to RP.	The value is an integer that ranges from 1 to 1799, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving a Register-Stop message sent by the RP, the DR at the source side stops sending Register messages and enters the register suppression state.

During the register suppression, the DR at the source side sends Probe messages to notify the RP that the multicast source is still in the Active state. After the register suppression times out, the DR at the source side starts to send Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

The interval set using the **probe-interval** command must be less than half the interval set using the **register-suppression-timeout (IPv4)** command.

Example

In the PIM view of public network instance, set the interval for sending Probe messages to RP to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] probe-interval 6
```

8.3.72 register-header-checksum

Function

The **register-header-checksum** command configures devices to calculate the checksum based on the header of a Register message only.

The **undo register-header-checksum** command restores the default configuration.

By default, the checksum is calculated according to all the contents of a Register message.

Format

register-header-checksum

undo register-header-checksum

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the source's DR calculates the checksum based on all fields in a Register message. After the **register-header-checksum** command is executed, the source's DR calculates the checksum based on the Register message header. This shortens the checksum calculation time and improves efficiency of encapsulating multicast data in Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Example

Calculate the checksum based only on the header of a Register message PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-header-checksum
```

8.3.73 register-policy (IPv4)

Function

The **register-policy** command sets the rules used by an RP to filter Register messages.

The **undo register-policy** command restores the default setting.

By default, the rules for filtering Register messages are not configured.

Format

register-policy *advanced-acl-number*

undo register-policy

Parameters

Parameter	Description	Value
advanced-acl-number	Specifies the number of the advanced ACL that defines the rules for filtering packets based on source addresses or group addresses.	The value is an integer that ranges from 3000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of invalid Register messages, you can configure devices to receive or deny Register messages according to the packet filtering rules.

If the (S, G) entry contained in a Register message does not pass the filtering of the ACL or the ACL does not filter the entry, RP discards the Register message. The multicast source cannot register with the RP.

If *advanced-acl-number* is set in the **register-policy** command but the corresponding ACL is not defined, the RP discards all Register messages. The RP cannot register with any multicast source.

The **register-policy** command and the **acl** command are used together. In the ACL view, you can set the multicast source address range by specifying the **source** parameter in the **rule** command, and set the multicast group address range by specifying the **destination** parameter in the **rule** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTICE

When the **register-policy** command is used on the RP, only Register messages matching the rule of the ACL are received by the RP. If an undefined ACL is specified, the RP denies all Register messages.

This command is valid for only PIM-SM.

The **register-policy** command takes effect for only subsequently received Register messages. The multicast entries that have been registered successfully are not deleted and can still be used for multicast data forwarding.

Example

Configure the RP to receive Register packets sent by the source on network segment 10.10.0.0/16 to group 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 3000
[HUAWEI-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3000] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-policy 3000
```

8.3.74 register-source

Function

The **register-source** command specifies the source address used by the source's DR to send Register messages.

The **undo register-source** command restores the default setting.

By default, the source address used by the source's DR to send Register messages is not specified.

Format

register-source *interface-type interface-number*

undo register-source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source's DR.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the source IP address for sending Register messages is no longer the only IP address in the network for the RP router or the source IP address is filtered out, errors occur in the registration process and extra traffic occupies bandwidth on the network. In this case, use the **register-source** command to specify an appropriate interface as the source IP address for sending Register messages. Using the loopback address of the source's DR as the source IP address is recommended.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Before specifying the source IP address for sending Register messages, enable PIM-SM.

Precautions

The command is effective only when the specified interface is in Up state.

Example

In the PIM view of public network instance, specify the IP address of loopback 0 as the source IP address for source's DR to send Register messages.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-source loopback 0
```

8.3.75 register-suppression-timeout (IPv4)

Function

The **register-suppression-timeout** command sets the timeout period during which a switch keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a switch keeps the register suppression state for 60 seconds.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the switch keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the switch immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the switch keeps the register suppression state. When the timeout period expires, the switch (source DR) starts to send Register messages to the RP.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If the timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, there will be a long delay for new receivers to join a group after an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv4)** command to configure the switch to send null Register messages before the suppression timer times out. This configuration reduces burst Register messages and shortens the timeout period to reduce the delay for a new receiver to join a group.

Precautions

This command is valid only for PIM-SM.

The interval set by the **register-suppression-timeout** command must be larger than two times the interval set by the **probe-interval (IPv4)** command.

Example

In the PIM view of public network instance, set the timeout period during which the switch keeps the register suppression state to 70 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] register-suppression-timeout 70
```

8.3.76 reset pim control-message counters

Function

The **reset pim control-message counters** command resets the statistics about PIM Control messages.

Format

reset pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the name and the number of an interface. It is used to reset the statistics about PIM control messages on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a PIM-enabled interface on the switch has been forwarding multicast packets for a long period of time, the switch stores statistics on a large number of control messages. You can run this command to reset statistics on control messages.

Example

Reset the statistics about PIM control messages on all interfaces in the public network instance.

```
<HUAWEI> reset pim control-message counters
```

Reset the statistics about PIM control messages on VLANIF100 in the public network instance.

```
<HUAWEI> reset pim control-message counters interface vlanif 100
```

8.3.77 reset pim routing-table

Function

The **reset pim routing-table** command resets PIM status of a specified downstream interface in a specified PIM routing entry.

Format

reset pim [**vpn-instance** *vpn-instance-name*] **routing-table group** *group-address* **mask** { *group-mask-length* | *group-mask* } **source** *source-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
group *group-address*	Specifies the multicast group address of a PIM routing entry.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask *group-mask-length*	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
mask *group-mask*	Specifies the mask of a multicast group address.	It is in dotted decimal notation.
source *source-address*	Specifies the source address of a PIM routing entry.	The value is in dotted decimal notation. If a (*, G) entry is specified, the source address is 0.0.0.0.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset pim routing-table** command resets PIM status of a specified downstream interface in a specified PIM routing entry.

Configuration Impact

This command can reset the PIM status of the specified interface in a specified PIM routing entry. It cannot reset the IGMP state and static group memberships on a specified interface.

Precautions

This command is valid only for PIM-SM.

NOTICE

Resetting PIM status of downstream interfaces can trigger transmission of Join/Prune messages, which causes multicast service interruption.

Example

In the public network instance, reset PIM status of downstream interface VLANIF100 of (10.1.1.1, 225.0.0.1).

```
<HUAWEI> reset pim routing-table group 225.0.0.1 mask 255.255.255.0 source 10.1.1.1 interface vlanif 100
```

8.3.78 source-lifetime (IPv4)

Function

The **source-lifetime** command specifies the timeout period of (S, G) or (*, G) entries on the switch.

The **undo source-lifetime** command restores the default value of the timeout period.

By default, the timeout period is 210 seconds.

Format

source-lifetime { *interval* | **infinity** } [**group-policy** *acl-number*]

undo source-lifetime

undo source-lifetime { *interval* | **infinity** } [**group-policy** *acl-number*]

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of (S, G) or (*, G) entries on the switch.	The value is an integer that ranges from 60 to 65535, in seconds.
infinity	Indicates that (S, G) entries on the switch will never age out.	-
group-policy	Specifies a group policy to determine to which the configured timeout period takes effect.	-
acl-number	Specifies the number of a basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch starts a timer for each (S, G) or (*, G) entry. The **source-lifetime** command sets the timer value. After receiving a multicast packet from S, the interface resets the timer. If the timer times out, the (S, G) or (*, G) entry is considered invalid.

- If you configure **source-lifetime** *interval*, the configured timeout period applies to all (S, G) entries.
- If you configure **source-lifetime** *interval* { **group-policy** *acl-number* }:
  - If you specify a basic ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source addresses are permitted by the specified ACL.
  - If you specify an advanced ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
  - If you specify an advanced ACL name in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
- If you configure **source-lifetime infinity**, all (S, G) entries will never age out.
- If you configure **source-lifetime infinity** { **group-policy** *acl-number* }:
  - If you specify a basic ACL number in the command, the (S, G) entries in which the source addresses are permitted by the specified ACL will never age out.
  - If you specify an advanced ACL number in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.
  - If you specify an advanced ACL name in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.

If you run this command multiple times for the same range of multicast forwarding entries and specify *interval* and **infinity** respectively in the commands, **infinity** takes precedence over *interval*.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

In the PIM view of public network instance, set the timeout period of an (S, G) or (*, G) entry of the switch to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] source-lifetime 200
```

8.3.79 source-policy (IPv4)

Function

The **source-policy** command configures a policy to filter received multicast data packets based on source addresses or source-group addresses.

The **undo source-policy** command deletes the configuration.

By default, a switch does not filter received multicast data packets based on source addresses or source-group addresses.

Format

source-policy *acl-number*

undo source-policy

Parameters

Parameter	Description	Value
acl-number	Specifies number of the basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the switch to filter received multicast data packets based on source addresses or source/group addresses.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If a basic ACL is referenced in the policy, multicast data packets that do not match the specified source addresses are discarded.

If an advanced AC is referenced in the policy, multicast data packets that do not match the specified group-source addresses are discarded.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

In the PIM view of public network instance, configure the switch to receive multicast data packets with the source address of 10.10.1.2 and to discard those with the source address of 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.10.1.2 0
[HUAWEI-acl-basic-2001] rule deny source 10.10.1.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] source-policy 2001
```

8.3.80 spt-switch-threshold (IPv4)

Function

The **spt-switch-threshold** command sets the rate threshold of the multicast packets when the DR at the member side joins the SPT.

The **undo spt-switch-threshold** command restores the default value.

By default, the system performs SPT switchover on receiving the first multicast data packet through the RPT.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** *basic-acl-number* [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy***basic-acl-number*]

Parameters

Parameter	Description	Value
traffic-rate	Specifies the threshold rate for the switchover from the RPT to the SPT. **NOTE** Setting this parameter may affect operation of multicast services. You are advised to use the default triggering condition. That is, an SPT switchover is triggered immediately after the first multicast data packet is received from the RPT. The default triggering condition can reduce the number of multicast packets forwarded on the RPT.	The value is an integer that ranges from 1 to 4194304, in kbit/s.
infinity	Indicates that the SPT switchover is never triggered.	-
basic-acl-number	Specifies an entry of the group-policy list. It works with the multicast group that matches **group-policy** *basic-acl-number* to enable the threshold. *basic-acl-number* specifies the number of the basic ACL that defines the range of multicast groups.	If the parameter is not set, the threshold is applied to all multicast groups. The value ranges from 2000 to 2999.
order *order-value*	Adjusts the order of the ACLs in the group-policy list.	If a group matches multiple ACLs, the threshold is selected in the order specified by *order-value*. *order-value* specifies the updated number. It is an integer. The value is any value other than original one in the current group-policy list. If the parameter is not set, the order of the ACLs in the group-policy list does not change.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source's DR encapsulates multicast packets in a Register message, and then transmits the unicast Register message to the RP. Then, the RP decapsulates the Register message and forwards the multicast packets to the receivers along the RPT. By default, when the RP or receiver's DR receives the first multicast packet, it initiates an SPT switchover to the source.

After the **spt-switch-threshold** command is executed on the receiver's DR, the receiver's DR periodically checks the forwarding rate of multicast packets. When the forwarding rate exceeds the threshold, the receiver's DR sends a Join messages to the source, triggering the SPT switchover.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid to all devices that may function as the DR at the member side, but is invalid to RPs.

This command is valid for only PIM-SM.

If this command is used several times for the same group, the first matching command takes effect.

Example

In the PIM view of public network instance, set the traffic rate threshold to 4 kbit/s. If the transmission rate of packets from the source to the multicast group exceeds the threshold, the switch triggers an SPT switchover so that packets are forwarded along the SPT towards the source.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] spt-switch-threshold 4
```

In the public network instance, create a group-policy that uses ACL 2010, specify the **infinity** keyword in the command to ensure that an SPT switchover will never be triggered, and set the order of ACL 2010 in the group-policy to 1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2010
[HUAWEI-acl-basic-2010] rule permit source 225.1.1.1 0
[HUAWEI-acl-basic-2010] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] spt-switch-threshold infinity group-policy 2010 order 1
```

8.3.81 ssm-policy (IPv4)

Function

The **ssm-policy** command sets the range of SSM group addresses.

The **undo ssm-policy** command restores the default configuration.

By default, the range of SSM group addresses is 232.0.0.0/8.

Format

ssm-policy *basic-acl-number*

undo ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL that defines the range of SSM group addresses.	The value is an integer that ranges from 2000 to 2999.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the address of an SSM group ranges from 232.0.0.0 to 232.255.255.255. You can run the **ssm-policy** command to specify the range of PIM SSM group addresses. All the PIM-SM interfaces consider that PIM SSM is enabled on all the multicast groups in the specified address range. The specified SSM group address range can be beyond 232.0.0.0/8.

You can enable SSM mode under the following conditions:

- The address of the multicast group is in the range of SSM group addresses, the network segment where the host resides runs IGMPv3, and the source address is specified in the Report message.
- The address of the multicast group is in the range of SSM group addresses, the network segment where the host resides runs IGMPv1 or IGMPv2, and the switch is configured with SSM mapping.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

The **ssm-policy** command and the **acl** command are used together.

- For the numbered ACL, in the ACL view, you can set the address range of SSM multicast groups by specifying the **source** parameter in the **rule** command.

- For the Named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the multicast group address range specified by the **destination** parameter and the period specified by the **time-range** parameter.

Example

In the PIM view of public network instance, set the range of PIM SSM multicast addresses to 232.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2000] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] ssm-policy 2000
```

8.3.82 state-refresh-interval (IPv4)

Function

The **state-refresh-interval** command sets the interval for sending PIM State-Refresh messages.

The **undo state-refresh-interval** command restores the default value of the interval.

By default, the interval for sending PIM State-Refresh messages is 60 seconds.

Format

state-refresh-interval *interval*

undo state-refresh-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending PIM State-Refresh messages.	The value is an integer that ranges from 1 to 255, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-DM network, the device periodically sends State-Refresh messages to update the timeout interval of the prune timer on the downstream device. By doing this, the interface that has no multicast requirements retains in prune state. You can use the **state-refresh-interval** command to set the interval at which State-Refresh messages are sent.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

To prevent a pruned interface from forwarding packets when the Prune status times out, the interval for sending State-Refresh messages is shorter than the period for keeping the Prune status.

You can run the **holdtime join-prune (IPv4)** command to set the period during which the device keeps the Prune status.

This command is valid for only PIM-DM.

This command takes effect only on the switch directly connected to a source.

Example

Set the interval for sending PIM State-Refresh messages to 70s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] state-refresh-interval 70
```

8.3.83 state-refresh-rate-limit (IPv4)

Function

The **state-refresh-rate-limit** command sets the minimum period to wait before receiving the next PIM State-Refresh message.

The **undo state-refresh-rate-limit** command restores the default value.

By default, the minimum period to wait to receive the next PIM State-Refresh message is 30 seconds.

Format

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

Parameters

Parameter	Description	Value
interval	Specifies the minimum period for waiting to receive the next PIM State-Refresh message.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch can receive multiple PIM State-Refresh messages in a short period. Some of the messages are the same. To avoid duplicate messages, you can run the **state-refresh-rate-limit** command to set the period to wait to receive the next State-Refresh message.

- Before the State-Refresh timer times out, the switch discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the switch can receive the next State-Refresh message.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Set the minimum period to wait to receive the next PIM State-Refresh message to 45s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] state-refresh-rate-limit 45
```

8.3.84 state-refresh-ttl (IPv4)

Function

The **state-refresh-ttl** command sets the TTL value for sending PIM State-Refresh messages.

The **undo state-refresh-ttl** command restores the default value of the TTL.

By default, the TTL value for sending PIM State-Refresh messages is 255.

Format

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Parameters

Parameter	Description	Value
ttl-value	Specifies the TTL value of the PIM State-Refresh message sent by an interface.	The value is an integer that ranges from 1 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a State-Refresh message, a switch decreases the TTL value in the message by 1, and then sends the message to the downstream device until the value of the TTL becomes 0. If the network is small, the message is delivered in a loop. You can use the **state-refresh-ttl** command to set an appropriate TTL value depending on the scale of your network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

This command takes effect only on the switch directly connected to a source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45 in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] state-refresh-ttl 45
```

8.3.85 static-rp (IPv4)

Function

The **static-rp** command configures a static RP.

The **undo static-rp** command restores the default configuration.

By default, no static RP is configured.

Format

static-rp *rp-address* [*basic-acl-number*] [**preferred**]

undo static-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Specifies address of a static RP.	The address is in dotted decimal notation. It must be a valid unicast IP address and cannot be configured as an address of network segment 127.0.0.0/8.
basic-acl-number	Specifies the basic ACL that is used to control the range of multicast groups served by a static RP.	The value is an integer that ranges from 2000 to 2999.
preferred	Indicates that the static RP is preferred.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one RP exists on a network, you can manually specify the static RP address and do not need to configure dynamic RP. This saves the bandwidth used for information exchange between the C-RPs and the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

If the static RP address is the address of an Up interface on the local device, the local device works as the static RP. PIM does not need to be enabled on the interface where the static RP address is located.

If no ACL is specified, the static RP serves all the multicast groups of 224.0.0.0/4. If an ACL is specified but no rule is configured in the ACL, the static RP serves all the groups of 224.0.0.0/4. If ACL rules are configured, the static RP serves only the multicast groups permitted by the ACL.

If the **static-rp** command does not contain **preferred**, devices apply the BSR mechanism to elect a dynamic RP. If dynamic RP is not configured or the dynamic RP is invalid, the static RP becomes valid. If the **static-rp** command contains **preferred**, the static RP is preferred over the dynamic RP.

If you run this command multiple times, multiple static RPs are configured. If multiple static RPs serve the same group, the RP with the largest IP address is selected to serve the group. If you specify the same RP address when running the **static-rp** command multiple times, the latest RP takes effect.

Precautions

NOTE

Up to 50 static RPs can be configured by using this command, but an ACL cannot be applied to multiple static RPs. If no ACL is referenced, only one static RP can be configured.

To ensure normal operating of a static RP, run the **static-rp** command to configure the same RP information on all devices in the PIM-SM domain.

The **static-rp** and **acl** commands are used together. In the ACL view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command. The filtering rule is effective only with the **source** parameter and the time period specified by the **time-range** parameter.

This command is valid only for PIM-SM.

Example

In the PIM view of public network instance, configure the switch with address 10.110.0.6 as a static RP serving the groups permitted by ACL 2001, and configure the static RP to be preferred.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] static-rp 10.110.0.6 2001 preferred
```

8.3.86 timer hello (IPv4)

Function

The **timer hello** command sets the interval at which the PIM switch sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM switch sends Hello messages is 30 seconds.

Format

timer hello *interval*

undo timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer ranging from 1 to 18000, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM routers periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim timer hello** command to set the interval for sending Hello messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Configuration Impact

This command is valid for both PIM-DM and PIM-SM.

The interval at which the PIM switch sends Hello messages should be less than the timeout period of the PIM neighbor. You can run the **hello-option holdtime (IPv4)** command to set the timeout period of PIM neighbors.

The **timer hello** command has the same function as the **pim timer hello** command in the interface view. By default, if the **pim timer hello** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which PIM Hello messages are sent to 40s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] pim
[HUAWEI-pim] timer hello 40
```

8.3.87 timer join-prune (IPv4)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream device.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream device is 60 seconds.

Format

timer join-prune *interval*

undo timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Join/Prune messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch sends join information to the upstream device, requesting the upstream device to forward multicast data. The switch sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The PIM router periodically sends Join/Prune messages to the upstream router to update the forwarding status.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid only for PIM-SM.

The interval configured using the **timer join-prune** command must be shorter than the interval configured using the **holdtime join-prune (IPv4)** command.

The **timer join-prune** command has the same function as the **pim timer join-prune** command in the interface view. By default, if the **pim timer join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which Join/Prune messages are sent to 80s in the PIM view of public network instance.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] timer join-prune 80
```

8.3.88 timer spt-switch (IPv4)

Function

The **timer spt-switch** command sets the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT.

The **undo timer spt-switch** command restores the default value of the interval.

By default, the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT is 15 seconds.

Format

timer spt-switch *interval*

undo timer spt-switch

Parameters

Parameter	Description	Value
interval	Specifies the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from RPT to SPT.	The value is an integer that ranges from 15 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **timer spt-switch** command to set the interval for checking whether the rate for transmitting multicast data exceeds the threshold.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is valid for only PIM-SM.

Before running this command, you must set the threshold for SPT switchover by using the **spt-switch-threshold (IPv4)** command; otherwise, the **timer spt-switch** command takes no effect.

Example

In the PIM view of public network instance, set the interval for checking the rate for transmitting the multicast data before the switchover from RPT to SPT to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] pim
[HUAWEI-pim] spt-switch-threshold 100
[HUAWEI-pim] timer spt-switch 30
```

8.4 IPv6 PIM Configuration Commands

8.4.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

8.4.2 bsm semantic fragmentation (IPv6)

Function

The **bsm semantic fragmentation** command enables BSR message fragmentation.

The **undo bsm semantic fragmentation** command disables BSR message fragmentation.

By default, BSR message fragmentation is not enabled.

Format

bsm semantic fragmentation

undo bsm semantic fragmentation

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BSR message carries information about all C-RPs on the network. Therefore, if there is a large number of C-RPs on the network, the length of a BSR message exceeds the MTU of the outgoing interface. As a result, the BSR message cannot be processed and RP election fails. Consequently, multicast services cannot be transmitted normally. In this case, you can enable BSR message fragmentation to ensure that the devices on the network can learn consistent RP information and MDTs can be successfully established.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

You can also configure IP fragmentation to solve the preceding problem. The difference between IP fragmentation and BSR message fragmentation is as follows:

- If IP fragmentation is enabled, the protocol layer transmits the entire BSR message up to the IP layer regardless of the length of the BSR message. The BSR message is then fragmented at the IP layer. If one fragment is lost during transmission, the destination cannot parse the entire BSR message. As a result, the destination cannot learn RP information and MDTs cannot be established, which causes a multicast data forwarding failure.

- If BSR message fragmentation is enabled, the protocol layer directly fragments a long BSR message. If one fragment is lost during transmission, only the information carried in this fragment is lost. As a result, only MDTs corresponding to the information carried in the lost fragments cannot be established. Since the other BSR message fragments can still reach the destination, the corresponding MDTs can be correctly established.

BSR message fragmentation is recommended because IP fragmentation causes all fragments to become unavailable when fragment information is lost.

Precautions

Enable BSR message fragmentation on all devices on the network. If BSR message fragmentation is not enabled on some devices, RP information on these devices is inconsistent with that on other devices and an MDT cannot be established correctly.

Example

Enable BSR message fragmentation in the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] bsm semantic fragmentation
```

8.4.3 bsr-policy (IPv6)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses so that the device discards BSR messages sent from addresses out of this range. This prevents BSR spoofing.

The **undo bsr-policy** command restores the default configuration.

By default, the range of BSR addresses is not limited, and all BSR packets are considered valid.

Format

bsr-policy *basic-acl6-number*

undo bsr-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the basic ACL number. The ACL defines the filtering policy for the range of source addresses of BSR packets.	The value is an integer that ranges from 2000 to 2999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any switch as a C-BSR to take part in the BSR election. Once a switch is elected as the BSR, it is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, take the following measures:

- Attacking hosts change the RP mapping to spoof the switch by forging BSR packets.

  Solution: Such attacks often occur on edge devices because a BSR packet is a multicast packet with TTL value of 1. As the BSR is inside the network and hosts are outside the network, the switches can perform neighbor check and RPF check on the received BSR packets to prevent the attacks.
- A switch is controlled by an attacker or an authorized switch is connected to the network. The attacker configures the switch as a C-BSR and makes the switch win the BSR election, so as to obtain the right of advertising RP information in the network.

  Solution: After the switch is configured as a C-BSR, it spreads multicast BSR packets in the network. The BSR packets have a TTL value of 1 and are forwarded hop by hop. As long as the neighboring device does not accept the BSR packets, the packets will not spread in the entire network. The solution is to use the **bsr-policy** command on every device in the network to specify the valid BSR range. For example, you can configure a policy to allow only switches with addresses FC00:0:0:2001::1/62 and FC00:0:0:2001::2/64 to function as BSRs. Then switches will not accept or forward BSR packets with addresses out of this range.

The two countermeasures mentioned above can partially protect BSRs in the network. If attackers control a valid BSR, it also brings problems to the network.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

After the **bsr-policy** command is run, the switch accepts only BSR messages matching the configured policy.

Precautions

The **bsr-policy** command and the **acl ipv6 (system view)** command are used together. In the ACL view, you can set the source address range for BSR packets by specifying the **source** parameter in the **rule (basic ACL6 view)** command.

Example

In the PIM-IPv6 view, configure address FC00:0:0:2001::/64 as the valid BSR address range.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:2001:: 64
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] bsr-policy 2001
```

8.4.4 c-bsr (IPv6)

Function

The **c-bsr** command configures a C-BSR.

The **undo c-bsr** command restores the default configuration.

By default, the C-BSR is not configured.

Format

c-bsr *ipv6-address* [*hash-length* [*priority*]]

undo c-bsr

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of a C-BSR. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the global IPv6 unicast address of the C-BSR.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
hash-length	Specifies the hash mask length of the C-BSR. The mask is used in a hash function to calculate the RP.	The value is an integer that ranges from 0 to 128. By default, the value is 126.

Parameter	Description	Value
priority	Specifies a priority of the C-BSR. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255. By default, the value is 0.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more C-BSRs need to be configured in a PIM-SM domain. A BSR is elected from multiple C-BSRs and is responsible for collecting C-RP information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM domain.

The process of BSR election is as follows:

- Each C-BSR considers itself as the BSR of the local PIM-SM domain and uses the IPv6 address of this interface as the address of the BSR to send Bootstrap messages.
- When a C-BSR receives a Bootstrap message from other devices, it compares the BSR in the received Bootstrap message with the current BSR. The BSR with the highest priority is preferred. If BSRs have the same priority, the BSR with a larger IPv6 address is preferred. If the BSR carried in the received Bootstrap message is superior to the current BSR, the C-BSR replaces its BSR address with the BSR address carried in the received Bootstrap message.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If PIM-SM (IPv6) is disabled on an interface, the interface can be configured as a C-BSR but the configuration does not take effect.

For the multicast BSR messages learned through the GRE tunnel, you need to configure a static multicast route to ensure that the next hop to the BSR is a GRE interface. You need to configure static multicast routes properly to avoid routing loops.

Example

In the PIM-IPv6 view, set the IPv6 address of the C-BSR to FC00:0:0:3001::1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```

```
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr fc00:0:0:3001::1
```

8.4.5 c-bsr admin-scope (IPv6)

Function

The **c-bsr admin-scope** command configures a BSR administrative scope in a PIM-SM domain.

The **undo c-bsr admin-scope** command restores the default configuration.

By default, no BSR administrative scope is configured.

Format

c-bsr admin-scope

undo c-bsr admin-scope

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BSR that serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative scopes and a global domain. This can reduce the workload of a single BSR and designate a private-network group address for users in a specific domain.

Each BSR administrative scope maintains a BSR that serves the multicast groups in a specified range. The multicast packets for the groups in a BSR administrative domain cannot travel across the boundary of the domain. The global domain maintains a BSR that serves all multicast groups that do not belong to any BSR administrative domains.

The relationship between the BSR administrative domain and the global domain is described as follows from the aspects of the region, group address range, and multicast function.

- Region

  Though different BSR administrative domains may serve the same group, devices in each BSR administrative domain differ. One device cannot belong to multiple BSR administrative domains. Each BSR administrative domain is independent of and isolated from each other geographically. A BSR administrative domain manages the multicast groups in a specific group address range. The multicast packets for the group in the range can be transmitted only in this administrative domain and cannot pass through the border of the BSR administrative domain.

A global domain contains all the switches on the PIM-SM network. The multicast packet that does not belong to any BSR administrative domain can be transmitted on the entire PIM network.

- Group address range

  Each BSR administrative domain serves the multicast groups in a specific group address range. The multicast groups that different BSR administrative domains serve can overlap. The address of the multicast group that the BSR administrative domain serves is valid only in its BSR administrative domain. That is, the multicast address is used as a private group address.

  The multicast group that does not belong to any BSR administrative domain belongs to a global domain.

- Multicast function

  The global domain and each BSR administrative domain have their respective Candidate-Rendezvous Point (C-RP) and BSR devices. Functions enabled on these devices take effect only in the local domain. That is, the BSR mechanism and the RP election are independent of each other among administrative domains.

  Each BSR administrative domain has its border. Multicast information of this domain, such as the C-RP Advertisement message and BSR BootStrap message, can be transmitted only within the domain. Multicast information of a global domain can be transmitted in the entire global domain and traverse any BSR administrative domain.

NOTE

Each BSR administrative domain corresponds to a scope ID defining the range of multicast groups.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **c-bsr admin-scope** command needs to be run on all the devices in a PIM-SM domain.

Example

Configure a BSR administrative scope in a PIM-SM domain.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr admin-scope
```

8.4.6 c-bsr global (IPv6)

Function

The **c-bsr global** command configures the switch as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

By default, no C-BSR is configured in the global domain.

Format

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

Parameters

Parameter	Description	Value
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in the global domain.	The value is an integer that ranging from 0 to 128. By default, the value is 126.
priority *priority*	Specifies the priority of the C-BSR in the global domain.	The value is an integer that ranges from 0 to 255. By default, it is 0. The greater the value, the higher the priority of the C-BSR.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PIM-SM network is divided into multiple BSR administrative domains and a global domain. The global domain maintains a BSR that serves the remaining multicast groups.

The **c-bsr global** command configures the switch as a C-BSR in the global domain. The BSR in the global domain is generated through election.

The rules of electing a BSR from C-BSRs in the global domain are as follows:

1. The C-BSR with the highest priority is elected as the BSR.
2. In the case of the same priority, the C-BSR with the highest IP address is elected as the BSR.

NOTE

A global domain contains all the switches on the PIM-SM network. The multicast packet that does not belong to any BSR administrative domain can be transmitted on the entire PIM network.

The multicast group that does not belong to any BSR administrative domain belongs to a global domain.

Multicast information of a global domain can be transmitted in the entire global domain and traverse any BSR administrative domain.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain and can enable a device in this BSR administrative domain to accept multicast data for groups beyond the address range of the administrative domain.

Example

In the PIM-IPv6 view, configure the switch as a C-BSR in the global domain, and then set the priority of the C-BSR to 1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr global priority 1
```

8.4.7 c-bsr hash-length (IPv6)

Function

The **c-bsr hash-length** command configures the global hash mask length of a C-BSR.

The **undo c-bsr hash-length** command restores the default configuration.

By default, the global hash mask length of a C-BSR is 126.

Format

c-bsr hash-length *hash-length*

undo c-bsr hash-length

Parameters

Parameter	Description	Value
hash-length	Specifies the global hash mask length of a C-BSR.	The value is an integer that ranges from 0 to 128.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic RP election, if C-RPs have the same interface address mask and priority for a specified multicast group, a hash function needs to be executed to select the RP for the multicast group. The switch performs hash calculation for the group address of G, C-RP address, and hash mask length of the C-RPs with the same priority and compares the hash values. The C-RP with the greatest hash value acts as the RP for G.

The hash mask length is used to adjust the hash calculation result.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-bsr** *ipv6-address hash-length* command in the PIM-IPv6 view configure the hash mask length while configuring a C-BSR address. The **c-bsr hash-length** *hash-length* command specifies the global hash mask length. If both the two commands are configured, the hash mask length configured by the **c-bsr** *ipv6-address hash-length* command takes effect.

Example

In the PIM-IPv6 view, set the global hash mask length of a C-BSR to 16.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr hash-length 16
```

8.4.8 c-bsr holdtime (IPv6)

Function

The **c-bsr holdtime** command configures the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR.

The **undo c-bsr holdtime** command restores the default configuration.

By default, the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR is 130s.

Format

c-bsr holdtime *interval*

undo c-bsr holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which C-BSR waits for the Bootstrap message to be sent by BSR.	The value is an integer that ranges from 1 to 214748364, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IPv6 address and the RP-set information. The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the elected BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command.

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer. The C-BSRs that fail in the election also refresh the timeout period of the BSR according to the holdtime.
- If the timer times out, the elected BSR is considered faulty. The C-BSRs that fail the previous election elect a new BSR. Services are not interrupted.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime. If the configured values are different, the BSR may become unstable. This may result in multicast faults. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If BS_interval or holdtime is configured, use the following formula to calculate the other one: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.

  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither BS_interval nor holdtime is configured, the default values are used. The default BS_interval is 60s and the default holdtime is 130s.

Example

In the PIM-IPv6 view, set the timeout interval during which the C-BSR waits for the Bootstrap message to be sent by BSR to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr holdtime 150
```

8.4.9 c-bsr interval (IPv6)

Function

The **c-bsr interval** command configures the interval at which the BSR continuously sends Bootstrap messages.

The **undo c-bsr interval** command restores the default interval.

By default, the BSR sends Bootstrap messages at a 60-second interval.

Format

c-bsr interval *interval*

undo c-bsr interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a BSR continuously sends Bootstrap messages.	The value is an integer that ranges from 1 to 107374177, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, it periodically sends Bootstrap messages carrying its own IPv6 address and the RP-set information.

The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command. The following applies to the timer:

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer.
- If the timer times out, the BSR is considered to be faulty. The C-BSRs that failed in the election triggers a new BSR election to prevent service interruption.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime values. If C-BSRs use different BS_interval or holdtime values, the BSR changes frequently, causing multicast forwarding errors. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If only one of the BS_interval and holdtime is configured, use the following formula to calculate the other parameter: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither the BS_interval nor the holdtime is configured, default values are used. The default value of BS_interval is 60s, and the default value of holdtime is 130s.

Example

In the PIM-IPv6 view, set the interval for the C-BSR to continuously send Bootstrap messages to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr interval 30
```

8.4.10 c-bsr priority (IPv6)

Function

The **c-bsr priority** command configures the global C-BSR priority.

The **undo c-bsr priority** command restores the default configuration.

By default, the global C-BSR priority is 0.

Format

c-bsr priority *priority*

undo c-bsr priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of the C-BSR.	The value is an integer that ranges from 0 to 255. A larger value indicates a higher priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple C-BSRs participate in the BSR election in the PIM-SM domain:

- The switch with the highest priority wins in the BSR election.
- If they have the same priority, the switch with the largest IPv6 address wins in the BSR election.

To enable a C-BSR to function as the BSR, you can run the **c-bsr priority** command to increase the priority value of the C-BSR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-bsr** *ipv6-address hash-length priority* command in the PIM-IPv6 view to set the C-BSR priority while configuring a C-BSR. The **c-bsr priority** *priority* command sets the global priority. When both the two commands are configured, the priority configured by the **c-bsr** *ipv6-address hash-length priority* command takes effect.

Example

In the PIM-IPv6 view, set the global C-BSR priority to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```

```
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr priority 5
```

8.4.11 c-bsr scope

Function

The **c-bsr scope** command specifies the scope ID of the BSR administrative domain served by a C-BSR.

The **undo c-bsr scope** command restores the default configuration.

By default, no scope ID is specified for a C-BSR. That is, the C-BSR does not belong to any BSR administrative domain.

Format

c-bsr scope *scope-id* [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr scope *scope-id*

Parameters

Parameter	Description	Value
scope-id	Specifies the scope ID of the administrative domain served by a C-BSR.	The value is an integer that ranges from 3 to 15.
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in a BSR administrative domain.	The value is an integer that ranges from 0 to 128. The default value is 126.
priority *priority*	Specifies the priority of a C-BSR in a BSR administrative domain.	The value is an integer that ranges from 0 to 255. The default value is 0. The greater the value, the higher the priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each BSR administrative domain is assigned a scope ID. To configure a C-BSR to serve a BSR administrative domain, use the **c-bsr scope** command to specify the scope ID of the BSR administrative domain. Packets forwarded by the C-BSR cannot travel across the boundary of the BSR administrative domain.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

A BSR administrative domain has been configured using the **c-bsr admin-scope (IPv6)** command in the PIM-IPv6 view.

Precautions

The multicast group that does not belong to any BSR administrative domain belongs to a global domain.

Example

In the PIM-IPv6 view, configure the switch as a C-BSR in the BSR administrative domain to serve groups of Scope 5, and set the priority of the C-BSR to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-bsr scope 5 priority 10
```

8.4.12 c-rp (IPv6)

Function

The **c-rp** command configures the switch to advertise itself as a C-RP to the BSR.

The **undo c-rp** command restores the default configuration.

By default, no C-RP is configured.

Format

c-rp *ipv6-address* [**advertisement-interval** *adv-interval* | [**group-policy** *basic-acl6-number* | **scope** *scope-id*] | **holdtime** *hold-interval* | **priority** *priority*] *

undo c-rp *ipv6-address* [**scope** *scope-id*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of a C-RP. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the global IPv6 unicast address of the C-RP.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
advertisement-interval *adv-interval*	Specifies the interval at which the C-RP sends Advertisement messages.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the value is 60 seconds.
group-policy *basic-acl6-number*	Specifies the range of multicast groups that the C-RP serves. The range is limited through the ACL6. *basic-acl6-number* specifies the number of the basic ACL6 used to limit the range of multicast groups that the C-RP serves.	The value is an integer that ranges from 2000 to 2999.
scope *scope-id*	Specifies the scope ID of the BSR administrative domain that a C-RP serves.	The value is an integer that ranges from 3 to 15.
holdtime *hold-interval*	Specifies the holdtime period during which the C-RP sends Advertisement messages. *hold-interval* specifies the time remaining before the C-RP sends Advertisement messages.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the value is 150 seconds.
priority *priority*	Specifies the priority of a C-RP. The value of *priority* indicates the priority of a C-RP.	The value is an integer that ranges from 0 to 255. By default, the value is 192. The greater the value is, the lower the priority is.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM (IPv6) domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM (IPv6) domain. It is recommended that you configure a C-RP on the device that aggregates multicast traffic and reserve enough bandwidth between this device and each of the other devices in the PIM-SM (IPv6) domain.

The rules used to elect an RP from multiple C-RPs are as follows, in descending order of precedence:

1. The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.
2. The C-RP with highest priority wins.
3. The C-RP with the largest hash value wins.
4. The C-RP with the largest IPv6 address wins.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **group-policy** *basic-acl6-number*, **priority** *priority*, **holdtime** *hold-interval* and **advertisement-interval** *adv-interval* set by using the command take precedence over the values of the global parameters configured in the PIM-IPv6 view because this command specifies an interface address. If this command is run several times on the same interface, only the latest configuration is valid.

Precautions

- If PIM-SM (IPv6) is disabled on an interface, the interface can be configured as a C-RP but the configuration does not take effect.
- **group-policy** *basic-acl6-number* specifies a group range. All permitted group ranges will be advertised as the ranges of groups that the RP serves. If no group range is specified for a C-RP or a C-RP is configured to serve all addresses, the C-RP serves all multicast groups.

The **c-rp** command and the **acl** command are used together.

- For the IPv6 numbered ACL, in the ACL6 view, you can set the address range of multicast groups that are serviced by the candidate RP by specifying the **source** parameter in the **rule** command.
- For the IPv6 Named ACL, in the ACL6 view, you can set the address range of multicast groups that are serviced by the candidate RP by specifying the **destination** parameter in the **rule** command.

If you want the switch to function as C-RPs in multiple BSR administrative domains, you need to specify the scope ID of each BSR administrative domain. For each scope ID, the settings of **advertisement-interval** *interval*, **priority** *priority-value*, and **holdtime** *interval* will overwrite the global settings in the PIM view.

Example

In the PIM-IPv6 view, configure an interface with the IPv6 address FC00:0:0:2001::1 as a C-RP of the PIM-SM (IPv6) domain.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp fc00:0:0:2001::1
```

8.4.13 c-rp advertisement-interval (IPv6)

Function

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **undo c-rp advertisement-interval** command restores the default interval.

By default, a C-RP sends Advertisement messages at an interval of 60 seconds.

Format

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a C-RP sends Advertisement messages.	The value ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All C-RPs in a PIM-SM domain periodically send Advertisement messages to the same BSR. The BSR can collect the integrated RP-Set.

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages to the BSR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **advertisement-interval** *interval* command in the PIM-IPv6 view to configure the advertisement interval while configuring a C-RP. The **c-rp advertisement-interval** *interval* command specifies the global interval. If both the commands are configured, the interval configured by the **c-rp** *ipv6-address* **advertisement-interval** *interval* command takes effect.

Example

In the PIM-IPv6 view, set the interval at which a C-RP sends Advertisement messages to 30s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp advertisement-interval 30
```

8.4.14 c-rp holdtime (IPv6)

Function

The **c-rp holdtime** command configures the holdtime for a received Advertisement message on a BSR.

The **undo c-rp holdtime** command restores the default holdtime.

By default, the holdtime for a received Advertisement message is 150 seconds.

Format

c-rp holdtime *hold-interval*

undo c-rp holdtime

Parameters

Parameter	Description	Value
hold-interval	Specifies the timeout period for a BSR to wait the Advertisement message from a C-RP.	The value ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When *hold-interval* is set on a C-RP, the C-RP encapsulates *hold-interval* in an Advertisement message and sends it to the BSR. The BSR obtains this *hold-interval* from the message and starts the timer. If the BSR receives no Advertisement message from the C-RP within the timeout period, the BSR regards the C-RP invalid or unreachable.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **holdtime** *hold-interval* command in the PIM-IPv6 view to configure the advertisement message holdtime while configuring a C-RP. The **c-rp holdtime** *hold-interval* configures the global holdtime for Advertisement messages. If both the two commands are configured, the holdtime configured by the **c-rp** *ipv6-address* **holdtime** *hold-interval* command takes effect.

Example

In the PIM-IPv6 view, set the holdtime for a received Advertisement message to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp holdtime 100
```

8.4.15 c-rp priority (IPv6)

Function

The **c-rp priority** command configures the global C-RP priority.

The **undo c-rp priority** command restores the default configuration.

By default, the global C-RP priority is 192.

Format

c-rp priority *priority*

undo c-rp priority

Parameters

Parameter	Description	Value
priority	Specifies the global C-RP priority.	The value is an integer that ranges from 0 to 255. A larger value indicates a lower priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs, in descending order of precedence:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- The C-RP with the largest hash value wins.
- The C-RP with the largest IPv6 address wins.

To enable a C-RP to function as an RP, you can run the **c-rp priority** command to increase the priority of the C-RP.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **priority** *priority* command in the PIM-IPv6 view to configure the C-RP priority while configuring a C-RP. The **c-rp priority** *priority* command specifies the global C-RP priority. If both the two commands are configured, the priority configured by the **c-rp** *ipv6-address* **priority** *priority* command takes effect.

Example

In the PIM-IPv6 view, set the global C-RP priority to 5.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] c-rp priority 5
```

8.4.16 crp-policy (IPv6)

Function

The **crp-policy** command limits the range of valid C-RP addresses and the range of the multicast addresses served by a C-RP. The BSR drops the C-RP messages with addresses out of the specified range to protect valid C-RPs.

The **undo crp-policy** command restores the default configuration.

By default, the BSR does not limit the range of valid C-RP addresses and the range of the multicast groups served by a C-RP. The BSR considers all the received C-RP messages valid.

Format

crp-policy *advanced-acl6-number*

undo crp-policy

Parameters

Parameter	Description	Value
advanced-acl6-number	Specifies the number of an advanced ACL. The ACL defines the range of the C-RP addresses and the range of the group addresses served by a C-RP.	The value is an integer that ranges from 3000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any switch can be configured as a C-RP to serve the multicast groups in a specified range. Each C-RP sends its information to the BSR in unicast mode. The BSR summarizes all received C-RP information into an RP-set, and floods it to the entire network using BSR messaged. The local switch then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RPs from being spoofed, configure **crp-policy** on the BSR to limit the range of valid C-RP addresses and the range of multicast group addresses served by a C-RP. Configure the same filtering rule on each C-BSR because any C-BSR can become the BSR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **crp-policy** command and the **acl ipv6 (system view)** command are used together. In the ACL6 view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule (advanced ACL6 view)** command. You can set the address range of multicast groups that are served by specifying the **destination** parameter in the **rule (advanced ACL6 view)** command.

If an ACL rule is specified but no C-RP address range is set, all C-RP messages are denied.

The **crp-policy** command and the **acl** command are used together. In the ACL6 view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule** command, and set the address range of multicast groups that are serviced by specifying the **destination** parameter in the **rule** command.

The matching of the received C-RP message succeeds only when the C-RP address carried in the message matches **source** and the address of the multicast groups carried in the message is a subset of the group address range in the ACL.

The configurations of the named ACL6 and the advanced ACL are the same, and can implement filtering of both source addresses and multicast group addresses. The named ACL can also be configured with the **time-range** parameter.

Example

Configure a C-RP policy on the C-BSR, which allows only the C-RP with the address FC00:0:0:2001::1/128 and allows the C-RP to serve only the multicast groups FF13::101/128.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3100
[HUAWEI-acl6-adv-3100] rule permit ipv6 source fc00:0:0:2001::1 128 destination ff13::101 128
[HUAWEI-acl6-adv-3100] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] crp-policy 3100
```

8.4.17 display default-parameter pim-dm6

Function

The **display default-parameter pim-dm6** command displays default PIM-DM (IPv6) configurations.

Format

display default-parameter pim-dm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-dm6** command displays default PIM-DM (IPv6) configurations. Even if PIM-DM (IPv6) parameters are modified, the **display default-parameter pim-dm6** command still displays default parameter settings. Therefore, you can use this command to check which parameters have been modified.

Example

Display default configurations about PIM-DM (IPv6).

```
<HUAWEI> display default-parameter pim-dm6
 PIM6 View Default Configurations:
 --------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Source-lifetime: 210 s
 State-refresh-interval: 60 s
 State-refresh-rate-limit: 30 s
 State-refresh-ttl: 255
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 -------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim state-refresh-capable: enabled
 Pim timer dr-switch-delay: disabled
 Pim timer graft-retry: 3 s
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim neighbor-policy: disabled
```

Table 8-54 Description of the **display default-parameter pim-dm6** command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.

Item	Description
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled This function is configured using the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
State-refresh-interval	Interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv6)** command.
State-refresh-rate-limit	Minimum interval from when the last State-Refresh message is received to when the next State-Refresh message is received. This parameter is configured by the **state-refresh-rate-limit (IPv6)** command.
State-refresh-ttl	TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.

Item	Description
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether the PIM BFD is enabled on the interface. This parameter is configured by the **pim ipv6 bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at the shared network segment where the interface resides. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. ● enabled: Neighbor tracking is enabled. ● disabled: Neighbor tracking is disabled This function is configured using the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.

Item	Description
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. - enabled: The received Hello message is required to carry the Generation ID. - disabled: The received Hello message is not required to carry the Generation ID. This parameter is configured using the **pim ipv6 require-genid** command.
Pim silent	Whether the interface is in PIM silent state. - enabled: The interface is in PIM silent state. - disabled: The interface is not in PIM silent state. This parameter is configured using the **pim ipv6 silent** command.
Pim state-refresh-capable	Whether State-Refresh is enabled on the interface. - enabled: State-Refresh is enabled on the interface. - disabled: State-Refresh is disabled on the interface. This function is configured using the **pim ipv6 state-refresh-capable** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. - enabled: The DR switch delay is set on the interface. - disabled: The DR switch delay is not set on the interface. This function is configured using the **pim ipv6 timer dr-switch-delay** command.
Pim timer graft-retry	Interval for the interface to retransmit Graft messages. This parameter is configured by the **pim ipv6 timer graft-retry** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.

Item	Description
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. The switch does not support this function.
Pim neighbor-policy	Whether the neighbor-policy is set on the interface. ● enabled: A neighbor policy is configured on the interface. ● disabled: No neighbor policy is configured on the interface. This function is configured using the **pim ipv6 neighbor-policy** command.

8.4.18 display default-parameter pim-sm6

Function

The **display default-parameter pim-sm6** command displays default PIM-SM (IPv6) configurations.

Format

display default-parameter pim-sm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-sm6** command displays default configurations about PIM-SM (IPv6) for both ASM and SSM. Even if PIM-SM (IPv6) parameters are modified, the **display default-parameter pim-sm6** command still displays default parameter settings. This command helps you determine which parameters have been modified.

Example

Display default PIM-SM (IPv6) configurations.

```
<HUAWEI> display default-parameter pim-sm6
 PIM6 View Default Configurations:
  ---------------------------------
  Bsr-policy: disabled
  C-bsr admin-scope: disabled
  C-bsr global: disabled
  C-bsr group: none
  C-bsr hash-length: 126
  C-bsr holdtime: 130 s
  C-bsr interval: 60 s
  C-bsr priority: 0
  C-rp advertisement-interval: 60 s
  C-rp holdtime: 150 s
  C-rp priority: 192
  Crp-policy: disabled
  Bsm semantic fragmentation: disabled
  Embedded-rp: enabled
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
  Holdtime join-prune: 210 s
  Probe-interval: 5 s
  Register-policy: disabled
  Register-suppression-timeout: 60 s
  Source-lifetime: 210 s
  Source-policy: disabled
  Spt-switch-threshold: disabled
  Ssm-policy: disabled
  Static-rp:  disabled
  Hello periodic interval: 30 s
  Join-prune periodic interval: 60 s
  Timer spt-switch: 15 s

  Interface View Default Configurations:
  --------------------------------------
  Pim bfd: disabled
  Pim bsr-boundary: disabled
  Pim hello-option dr-priority: 1
  Pim hello-option holdtime: 105 s
  Pim hello-option lan-delay: 500 ms
  Pim hello-option neighbor-tracking: disabled
  Pim hello-option override-interval: 2500 ms
  Pim holdtime assert: 180 s
  Pim holdtime join-prune: 210 s
  Pim require-genid: disabled
  Pim silent: disabled
  Pim timer dr-switch-delay: disabled
  Pim hello periodic interval: 30 s
  Pim join-prune periodic interval: 60 s
  Pim triggered-hello-delay: 5 s
  Pim version: 2
  Pim ipsec sa: disabled
```

```
Pim join-policy: disabled
Pim neighbor-policy: disabled
```

Table 8-55 Description of the **display default-parameter pim-sm6** command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Bsr-policy	Whether the valid address range of the BSR is set. This parameter is configured by the **bsr-policy (IPv6)** command.
C-bsr admin-scope	Whether the BSR administrative domain is configured. This parameter is configured by the **c-bsr admin-scope (IPv6)** command.
C-bsr global	Whether the C-BSR in the global domain is configured. This parameter is configured by the **c-bsr global (IPv6)** command.
C-bsr group	Whether the C-BSR in the BSR administrative domain is configured. This parameter is configured by the **c-bsr scope** command.
C-bsr hash-length	Global hash mask length of the C-BSR. This parameter is configured by the **c-bsr hash-length (IPv6)** command.
C-bsr holdtime	Waiting time for the BSR to receive the Bootstrap message. This parameter is configured by the **c-bsr holdtime (IPv6)** command.
C-bsr interval	Interval for the BSR to send Bootstrap messages. This parameter is configured by the **c-bsr interval (IPv6)** command.
C-bsr priority	Global priority of the C-BSR. This parameter is configured by the **c-bsr priority (IPv6)** command.
C-rp advertisement-interval	Interval for the C-RP to send Advertisement messages. This parameter is configured by the **c-rp advertisement-interval (IPv6)** command.
C-rp holdtime	Waiting time for the BSR to receive the Advertisement message. This parameter is configured by the **c-rp holdtime (IPv6)** command.
C-rp priority	Global priority of the C-RP. This parameter is configured by the **c-rp priority (IPv6)** command.

Item	Description
Crp-policy	Whether the valid address range of the C-RP and the range of multicast groups that the C-RP serves are set. This parameter is configured by the **crp-policy (IPv6)** command.
Bsm semantic fragmentation	Whether the BSR fragmentation is enabled. This parameter is configured by the **bsm semantic fragmentation (IPv6)** command.
Embedded-rp	Whether the embedded RP is enabled. This parameter is configured by the **embedded-rp** command.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP. This parameter is configured by the **probe-interval (IPv6)** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv6)** command.

Item	Description
Register-suppression-timeout	Time period for holding the register-suppression state. This parameter is configured by the **register-suppression-timeout (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv6)** command.
Spt-switch-threshold	Whether the threshold of the multicast packet rate that triggers the switch from the RPT to the SPT is configured. This parameter is configured by the **spt-switch-threshold (IPv6)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv6)** command.
Static-rp	Whether the static RP is configured. This parameter is configured by the **static-rp (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Timer spt-switch	Whether the interval for checking whether the multicast packet rate exceeds the threshold before the switchover from RPT to SPT is configured. This parameter is configured by the **timer spt-switch (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether the PIM BFD is enabled on the interface. This parameter is configured by the **pim ipv6 bfd enable** command.
Pim bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim ipv6 bsr-boundary** command.

Item	Description
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.

Item	Description
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. The switch does not support this function.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim ipv6 join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

8.4.19 display default-parameter pim-ssm6

Function

The **display default-parameter pim-ssm6** command displays default configurations of PIM-SM (IPv6) for SSM.

Format

display default-parameter pim-ssm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-ssm6** command displays default configuration of PIM-SM (IPv6) for SSM. Even if the configuration of PIM-SM (IPv6) for SSM is modified, the **display default-parameter pim-ssm6** command still displays default parameter settings. This command helps you determine which parameters have been modified.

Example

Display default configuration of PIM-SM (IPv6) for SSM.

```
<HUAWEI> display default-parameter pim-ssm6
 PIM6 View Default Configurations:
 --------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Probe-interval: 5 s
 Register-policy: disabled
 Register-suppression-timeout: 60 s
 Source-lifetime: 210 s
 Source-policy: disabled
 Ssm-policy: disabled
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 -------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim timer dr-switch-delay: disabled
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim ipsec sa: disabled
 Pim join-policy: disabled
 Pim neighbor-policy: disabled
```

Table 8-56 Description of the **display default-parameter pim-ssm6** command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.

Item	Description
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP. This parameter is configured by the **probe-interval (IPv6)** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv6)** command.
Register-suppression-timeout	Time period for holding the register-suppression state. This parameter is configured by the **register-suppression-timeout (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv6)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.

Item	Description
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether the PIM BFD is enabled on the interface. This parameter is configured by the **pim ipv6 bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.

Item	Description
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim ipsec sa	Whether PIM IPSec is enabled on the interface. The switch does not support this function.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim ipv6 join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

8.4.20 display pim ipv6 bsr-info

Function

The **display pim ipv6 bsr-info** command displays the BSRs in a PIM-SM (IPv6) domain.

Format

display pim ipv6 bsr-info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check BSR configuration on a PIM-SM (IPv6) network.

Example

Display information about BSR in the current PIM-SM (IPv6) domain. If the switch is configured with C-BSR, information about the elected BSR and C-BSR is displayed.

```
<HUAWEI> display pim ipv6 bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: FC00:0:0:2004::2
     Priority: 0
     Hash mask length: 128
     State: Elected
     Scope: 5
     Uptime: 00:00:07
     Next BSR message scheduled at: 00:00:53
     C-RP Count: 0
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: FC00:0:0:2004::2
     Priority: 0
     Hash mask length: 128
     State: Elected
     Scope: 5
     Wait to be BSR: 0
```

Table 8-57 Description of the **display pim ipv6 bsr-info** command output

Item	Description
Elected AdminScoped BSR Count	number of elected AdminScoped BSRs.
Elected BSR Address	IPv6 address of the elected BSR.
Priority	Priority of the BSR.
Hash mask length	Mask length in the RP hash calculation.

Item	Description
State	Status of the BSR. - Accept Preferred: No C-BSR is configured on the device and another device functions as a BSR and does not time out. - Accept Any: No C-BSR is configured on the device and the current BSR times out (applicable to the situation that a BSR administrative domain is set) - Candidate: A C-BSR is configured on a device and another device functions as a BSR. - Pending: The device changes from the non-BSR state to the BSR state or a C-BSR is configured on the device and the current BSR times out. - Elected: The device is elected as the BSR.
Scope	Scope ID of the BSR administrative domain served by a BSR. Not scoped indicates that the BSR is not an AdminScoped BSR.
Uptime	Period during which the BSR exists.
Next BSR message scheduled at	Period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.
C-RP Count	Number of RPs learned through the BSR.
Candidate AdminScoped BSR Count	Number of AdminScoped C-BSRs.
Candidate BSR Address	IPv6 Address of the C-BSR.
Wait to be BSR	Whether the current C-BSR is valid. The values are as follows: - 0: The current C-BSR is valid. The current C-BSR takes part in the BSR election. - 1: The current C-BSR is invalid. The current C-BSR does not take part in the BSR election. When the number of C-BSRs configured on the switch exceeds the threshold, the value is 1.

8.4.21 display pim ipv6 bfd session

Function

The **display pim ipv6 bfd session** command displays information about PIM IPv6 BFD sessions.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display pim ipv6 bfd session statistics

display pim ipv6 bfd session [**interface** *interface-type interface-number* | **neighbor** *ipv6-link-local-address*]*

Parameters

Parameter	Description	Value
statistics	Displays statistics about PIM IPv6 BFD sessions.	-
interface *interface-type interface-number*	Displays information about PIM IPv6 BFD sessions on a specified interface. *interface-type interface-number* specifies the type and number of an interface.	-
neighbor *ipv6-link-local-address*	Displays information about PIM IPv6 BFD sessions on a specified neighbor. *ipv6-link-local-address* specifies the link-local address of a PIM neighbor.	The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After PIM BFD (IPv6) is configured to detect the status of PIM neighbors, a PIM IPv6 BFD session needs to be established. The **display pim ipv6 bfd session** command can be used to view statistics about and configurations of PIM IPv6 BFD sessions.

Precautions

The two ends of a BFD session negotiate the actual interval at which PIM IPv6 BFD packets are sent, the interval at which PIM IPv6 BFD packets are received, and the detection period based on the following negotiation mechanisms:

- The formula used to calculate the interval for sending PIM IPv6 BFD packets and the formula used to calculate the interval for receiving PIM IPv6 BFD packets are as follows:
  - Interval for sending PIM IPv6 BFD packets = Max (Local **min-tx-interval**, Remote **min-rx-interval**)
  - Interval for receiving PIM IPv6 BFD packets = Max (Remote **min-tx-interval**, Local **min-rx-interval**)
- The formula used to calculate the detection period is as follows:
  - Detection period = Remote **detect-multiplier** x Max (Remote **min-tx-interval**, Local **min-rx-interval**)

Example

Display information about PIM IPv6 BFD sessions on all interfaces.

```
<HUAWEI> display pim ipv6 bfd session
 VPN-Instance: public net
 Total 1 BFD session Created

 Vlanif100 (FE80::7): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 FE80::6         200       300       4        8211/8214    Up
```

Display information about the PIM IPv6 BFD session on VLANIF 100.

```
<HUAWEI> display pim ipv6 bfd session interface vlanif 100
 VPN-Instance: public net

 Vlanif100 (FE80::7): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 FE80::6         200       300       4        8211/8214    Up
```

Table 8-58 Description of the **display pim ipv6 bfd session** command output

Item	Description
Total 1 BFD session Created	Total number of established PIM IPv6 BFD sessions.
Vlanif100 (FE80::7)	PIM interface name (Link-local address).
Neighbor	IPv6 link-local address of a PIM neighbor.
ActTx(ms)	Actual interval for sending PIM IPv6 BFD packets.
ActRx(ms)	Actual interval for receiving PIM IPv6 BFD packets.
ActMulti	Actual detection multiplier of PIM IPv6 BFD packets.
Local/Remote	Local/remote discriminator of a PIM IPv6 BFD session.
State	Status of a PIM IPv6 BFD session: ● Up: indicates that the BFD session is set up successfully and detection packets are periodically exchanged. ● Init: indicates that the local end can communicate with the remote end and wants the session status to be Up. ● Admin down: indicates that the session is in the administratively Down state (The **shutdown** command is run in the BFD session view). ● Down: indicates that the BFD session is down.

Display statistics about PIM IPv6 BFD sessions.

```
<HUAWEI> display pim ipv6 bfd session statistics
 VPN-Instance: public net
  Total 1 PIM BFD session in this instance.

   Total 1 PIM BFD session up.
   Total 0 PIM BFD session down.
```

Table 8-59 Description of the display pim ipv6 bfd session statistics command output

Item	Description
Total 1 PIM BFD session in this instance	Total number of PIM IPv6 BFD sessions.
Total 1 PIM BFD session up	Total number of PIM IPv6 BFD sessions in the Up state.

Item	Description
Total 0 PIM BFD session down	Total number of PIM IPv6 BFD sessions in the Down state, that is, the total number of PIM IPv6 BFD sessions minus the number of PIM IPv6 BFD sessions in the Up state.

8.4.22 display pim ipv6 claimed-route

Function

The **display pim ipv6 claimed-route** command displays the unicast routing information used by PIM (IPv6).

Format

display pim ipv6 claimed-route [*ipv6-source-address*]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is in hexadecimal format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim ipv6 claimed-route** command displays the unicast routes used by PIM (IPv6), such as the RPF neighbors, detailed information about interfaces, route types, and route selection policy.

Example

Display the unicast route of multicast source FC00:0:0:2001::2.

```
<HUAWEI> display pim ipv6 claimed-route fc00:0:0:2001::2
VPN-Instance: public net
multicast load-splitting rule: source-group
RPF information about: FC00:0:0:2001::2 in PIM-SM routing table
    RPF interface: Vlanif100, RPF neighbor: FE80::A01:100:1
    Referenced route/mask: FC00:0:0:2001::/64
    Referenced route type: igp
    RPF-route selecting rule: preference-preferred
    The (S, G) or (*, G) list dependent on this route entry
    (FC00:0:0:2001::2, FF03::1)
```

Table 8-60 Description of the **display pim ipv6 claimed-route** command output

Item	Description
multicast load-splitting rule	Mode in which multi-cast loads are split. The following policies apply: ● group: multicast group-based load splitting ● source: multicast source-based load splitting ● source-group: multicast source and group-based load splitting ● stable-preferred: stable-preferred load splitting ● balance-preferred: balance-preferred load splitting
RPF information about: FC00:0:0:2001::2 in PIM-SM routing table	RPF routing information with the source address of FC00:0:0:2001::2 in the PIM-SM (IPv6) routing table
RPF interface	RPF interface in a routing entry.
RPF neighbor	RPF neighbor in a routing entry.
Referenced route/mask	Route/mask used by PIM.
Referenced route type	Type of a route.
RPF-route selecting rule	Preferred rule for selecting the RPF-route.
The (S, G) or (*, G) list dependent on this route entry	List of multicast entries based on RPF routes.

8.4.23 display pim ipv6 control-message counters

Function

The **display pim ipv6 control-message counters** command displays the number of sent and received PIM (IPv6) control messages.

Format

display pim ipv6 control-message counters message-type { **probe** | **register** | **register-stop** | **crp** }

display pim ipv6 control-message counters [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
message-type	Indicates the types of PIM control message.	-
probe	Indicates the Probe message.	-
register	Indicates the Register message.	-
register-stop	Indicates the Register-stop message.	-
crp	Indicates the C-RP message.	-
assert	Indicates the Assert message.	-
graft	Indicates the Graft message.	-
graft-ack	Indicates the Graft-ack message.	-
hello	Indicates the Hello message.	-
join-prune	Indicates the Join-prune message.	-
state-refresh	Indicates the State-Refresh message.	-
bsr	Indicates the BSR message.	-
interface *interface-type interface-number*	Indicates the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When multicast forwarding fails on a PIM (IPv6) network, run the **display pim control-message counters** command to view statistics about protocol packets. The command output helps you locate faults.

Example

Display the number of PIM (IPv6) control messages that were sent and received on VLANIF100.

```
<HUAWEI> display pim ipv6 control-message counters interface vlanif 100
VPN-Instance: public net
 PIM control-message counters for interface: Vlanif100
 Message Type     Received         Sent            Invalid      Filtered
 Assert           0                0               0            0
 Graft            0                0               0            0
 Graft-Ack        0                0               0            0
 Hello            328              331             0            0
 Join-prune       2                0               0            0
 State-Refresh    0                0               0            0
 BSR              9778             0               0            0
```

Table 8-61 Description of the **display pim ipv6 control-message counters** command output

Item	Description
PIM control-message counters for interface	Name of the interface for collecting statistics on PIM control messages
Message Type	Type of the control messages.
Received	Number of control messages received by the current interface.
Sent	Number of control messages sent by the current interface.
Invalid	Number of invalid control packets.
Filtered	Number of control messages filtered out by the current interface.
Assert	Number of Assert messages.
Graft	Number of Graft messages.
Graft-Ack	Number of Graft-Ack messages.
Hello	Number of Hello messages.
Join-prune	Number of Join/Prune messages.
State-Refresh	Number of State-Refresh messages.
BSR	Number of Bootstrap messages.

8.4.24 display pim ipv6 grafts

Function

The **display pim ipv6 grafts** command displays the information about unacknowledged PIM-DM (IPv6) Graft messages.

Format

display pim ipv6 grafts

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM (IPv6), after sending the Graft message, the switch needs to wait to receive the Graft-Ack message from the upstream device.

You can run the **display pim ipv6 grafts** command to view the information about the PIM-DM (IPv6) Graft messages sent but unacknowledged.

Example

Display the unacknowledged PIM-DM (IPv6) graft messages.

```
<HUAWEI> display pim ipv6 grafts
Source                   Group                  Expire    RetransmitIn
fc00:0:0:2001::2           ff03::101              00:02:52  00:00:02
```

Table 8-62 Description of the **display pim ipv6 grafts** command output

Item	Description
Source	Multicast source address.
Group	Multicast group address.
Expire	Timeout period of an (S, G) entry.
RetransmitIn	Amount of time before the next Graft message is transmitted.

8.4.25 display pim ipv6 interface

Function

The **display pim ipv6 interface** command displays information about PIM (IPv6) on an interface.

Format

display pim ipv6 interface [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Indicates the type and number of an interface.	-

Parameter	Description	Value
up	Indicates that the IPv6 status is Up on the PIM interface.	-
down	Indicates that the IPv6 status is Down on the PIM interface.	-
verbose	Indicates detailed information about a PIM (IPv6) interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An interface enabled with PIM (IPv6) is called a PIM (IPv6) interface. The **display pim ipv6 interface** command is used to display information about PIM (IPv6) interfaces, including status of the PIM (IPv6) interface, the number of PIM (IPv6) neighbors, interval at which Hello messages are sent, DR priority, and DR address.

Example

Display PIM (IPv6) information on VLANIF100.

```
<HUAWEI> display pim ipv6 interface vlanif 100
 VPN-Instance: public net
 Interface           State NbrCnt HelloInt   DR-Pri     DR-Address
 Vlanif100             up    0      30         1          FE80::2E0:3FFF:FE27:AE01(local)
```

Table 8-63 Description of the display pim ipv6 interface command output

Item	Description
Interface	Name of the PIM (IPv6) interface.
State	Status of the PIM (IPv6) interface, up or down.
NbrCnt	Number of PIM (IPv6) neighbors on the interface.
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

Display detailed information about PIM (IPv6) on VLANIF100.

```
<HUAWEI> display pim ipv6 interface vlanif 100 verbose
 VPN-Instance: public net
 Interface: Vlanif100, FE80::2E0:3FFF:FE27:AE01
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: FE80::2E0:3FFF:FE27:AE01 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 0
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0x18FF94EC
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: disabled
     PIM dr-switch-delay timer : not configured
     Number of routers on link not using DR priority: 0
     Number of routers on link not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 1
     ACL of PIM neighbor policy: myacl6
     ACL of PIM ASM join policy: 2000
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
```

Table 8-64 Description of the **display pim ipv6 interface verbose** command output

Item	Description
PIM version	Version number of PIM (IPv6) enabled on the interface.
PIM mode	PIM mode.
PIM state	Status of the PIM (IPv6) interface, up or down.
PIM DR	DR address on the interface.
PIM DR Priority (configured)	Configured DR priority on the interface.
PIM neighbor count	Number of PIM (IPv6) neighbors on the interface.
PIM hello interval	Interval for sending Hello messages.
PIM LAN delay (negotiated)	Negotiated delay for transmitting packets on the interface.
PIM LAN delay (configured)	Configured delay for transmitting packets on the interface.

Item	Description
PIM hello override interval (negotiated)	Negotiated override interval on the interface.
PIM hello override interval (configured)	Configured override interval on the interface.
PIM Silent	Whether the PIM Silent (IPv6) function is enabled on the interface.
PIM neighbor tracking (negotiated)	Whether the PIM (IPv6) neighbor tracking function is enabled on the interface after negotiation.
PIM neighbor tracking (configured)	Whether the PIM (IPv6) neighbor tracking function is configured on the interface.
PIM generation ID	Generation ID option on the interface.
PIM require-GenID	Whether the function of rejecting the Hello messages without the Generation ID option is enabled.
PIM hello hold interval	Interval for the receiver of the Hello message to keep its neighbor reachable.
PIM assert hold interval	Interval for sending Assert messages.
PIM triggered hello delay	Maximum random delay for triggering Hello messages.
PIM J/P interval	Interval for the interface to send Join/Prune messages.
PIM J/P hold interval	Period for holding the Join/Prune status on the interface.
PIM BSR domain border	Whether the BSR domain boundary is configured on the interface.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of switches that do not use DR priority in all the network segments connected to the interface.
Number of routers on link not using LAN delay	Number of switches that do not use LAN delay in all the network segments connected to the interface.
Number of routers on link not using neighbor tracking	Number of switches that are not enabled with the neighbor tracing function in the network segment where the interface resides.
ACL of PIM neighbor policy	Neighbor filtering policy configured on the interface.

Item	Description
ACL of PIM ASM join policy	ASM Join information filtering policy configured on the interface.
ACL of PIM SSM join policy	SSM Join information filtering policy configured on the interface.
ACL of PIM join policy	Join information filtering policy configured on the interface.

8.4.26 display pim ipv6 invalid-packet

Function

The **display pim ipv6 invalid-packet** command displays statistics about invalid PIM (IPv6) messages received by a device and details of these messages.

Format

display pim ipv6 invalid-packet [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** }] *

display pim ipv6 invalid-packet message-type { **crp** | **register** | **register-stop** }

display pim ipv6 invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about invalid PIM (IPv6) messages received by a specified interface. *interface-type interface-number* specifies the interface type and interface number.	-
message-type	Displays statistics about invalid PIM (IPv6) messages of a specific type.	-
assert	Displays statistics about invalid Assert messages.	-
bsr	Displays statistics about invalid BSR messages.	-
hello	Displays statistics about invalid Hello messages.	-

Parameter	Description	Value
join-prune	Displays statistics about invalid Join/ Prune messages.	-
graft	Displays statistics about invalid Graft messages.	-
graft-ack	Displays statistics about invalid Graft-Ack messages.	-
state-refresh	Displays statistics about invalid State-Refresh messages.	-
crp	Displays statistics about invalid C-RP messages.	-
register	Displays statistics about invalid Register messages.	-
register-stop	Displays statistics about invalid Register-Stop messages.	-
packet-number	Displays details of a specified number of invalid PIM (IPv6) messages recently received.	The value is an integer that ranges from 1 to 100. By default, details of all the invalid PIM (IPv6) messages currently stored are displayed.
verbose	Displays details of invalid PIM (IPv6) messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on a PIM (IPv6) network, use the **display pim ipv6 invalid-packet** command to check statistics and details about invalid PIM (IPv6) packets. The command output can help you locate the fault.

If PIM (IPv6) entries fail to be generated on a multicast network, you can run the **display pim ipv6 invalid-packet** command first to check whether devices have received invalid PIM (IPv6) messages. If the command output contains statistics about invalid PIM (IPv6) messages, run the **display pim ipv6 invalid-packet** [*packet-number*] **verbose** command to view details of invalid PIM (IPv6) messages to locate the fault.

You can run the following related commands to view information about specific invalid IPv6 PIM messages:

- Run the **display pim ipv6 invalid-packet** command to view statistics about invalid IPv6 PIM messages received by a device in the public network instance.
- Run the **display pim ipv6 invalid-packet interface** *interface-type interface-number* command to view statistics about invalid IPv6 PIM messages received by a specified interface.
- Run the **display pim ipv6 invalid-packet** *packet-number* **verbose** command to view details of invalid IPv6 PIM messages recently received. Currently, details of a maximum of 100 invalid IPv6 PIM messages can be displayed.

Example

Display statistics about invalid PIM (IPv6) messages received by a device.

```
<HUAWEI> display pim ipv6 invalid-packet

          Statistics of invalid packets for public net:
-------------------------------------------------------------------
PIM General invalid packet: Invalid PIM Version     : 0          Invalid PIM Type        : 0 Fault Length            :
0          Bad Checksum           : 0
PIM Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0

PIM Register-Stop invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0          IP Source not RP        : 0

PIM CRP invalid packet:
Invalid Dest Addr       : 0          Invalid CRP Addr        : 0
Fault Length            : 0          CRP Adv Fault Length    : 0
Invalid Multicast Group : 0

PIM Assert invalid packet:
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0
Invalid Multicast Source: 0          Invalid Multicast Group : 0

PIM BSR invalid packet:
Bad Payload             : 0          Fault Length            : 0
Bad Scope Mask          : 0          Invalid Multicast Group : 0
Not CBSR But BSR        : 0          Invalid BSR Addr        : 0
Fault Hash Length       : 0          Invalid IP Source Addr  : 0

PIM Hello invalid packet:
Invalid Addr List       : 0          Fault Length            : 0
Bad Holdtime Length     : 0          Bad LanPruneDelay Length: 0
Bad DrPriority Length   : 0          Bad GenID Length        : 0
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0

PIM Join/Prune invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Invalid Dest Addr       : 0          Fault Length            : 0
 PIM Graft invalid packet: Invalid Multicast Source: 0          Invalid Multicast Group : 0 Invalid Up
```

```
Neighbor     : 0           Invalid IP Source Addr  : 0 Fault Length            : 0  PIM Graft-Ack invalid packet:
Invalid Multicast Source: 0           Invalid Multicast Group : 0 Invalid Up Neighbor     : 0           Invalid IP
Source Addr  : 0 Fault Length            : 0  PIM State Refresh invalid packet: Invalid Multicast Source: 0
Invalid Multicast Group : 0 Invalid Originator Addr : 0           Fault Length            : 0
----------------------------------------------------------------------
```

Table 8-65 Description of the **display pim ipv6 invalid-packet** command output

Item	Description
PIM General invalid packet	Number of general invalid PIM (IPv6) messages.
Invalid PIM Version	Number of messages with invalid PIM (IPv6) version.
Invalid PIM Type	Number of messages with invalid PIM (IPv6) message type.
Fault Length	Number of messages with invalid lengths.
Bad Checksum	Number of messages with invalid checksum.
PIM Register invalid packet	Number of PIM Register messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Invalid Multicast Group	Number of messages with invalid multicast group addresses.
Invalid Dest Addr	Number of messages with invalid destination addresses.
PIM Register-Stop invalid packet	Number of invalid Register-Stop messages.
IP Source not RP	Number of messages whose source addresses are not the RP address.
PIM CRP invalid packet	Number of invalid C-RP messages.
Invalid CRP Addr	Number of messages with invalid C-RP addresses.
CRP Adv Fault Length	Number of messages with CRP Adv fields of invalid lengths.
PIM Assert invalid packet	Number of invalid Assert messages.
Invalid IP Source Addr	Number of messages with invalid source addresses.
PIM BSR invalid packet	Number of invalid BSR messages.
Bad Payload	Number of messages with invalid payloads.
Bad Scope Mask	Number of messages with invalid scope masks.

Item	Description
Not CBSR But BSR	Number of messages received from non-C-BSRs.
Invalid BSR Addr	Number of messages with invalid BSR addresses.
Fault Hash Length	Number of messages whose hash mask fields of invalid lengths.
PIM Hello invalid packet	Number of invalid Hello messages.
Invalid Addr List	Number of messages with invalid address lists.
Bad Holdtime Length	Number of messages whose Holdtime fields are of invalid lengths.
Bad LanPruneDelay Length	Number of messages whose LanPruneDelay fields are of invalid lengths.
Bad DrPriority Length	Number of messages with DrPriority fields of invalid lengths.
Bad GenID Length	Number of messages with GenerationID fields of invalid lengths.
PIM Join/Prune invalid packet	Number of invalid Join/Prune messages.
Invalid Up Neighbor	Number of messages with invalid upstream neighbors.
PIM Graft invalid packet	Number of invalid Graft messages.
PIM Graft-Ack invalid packet	Number of invalid Graft-Ack messages.
PIM State Refresh invalid packet	Number of invalid State-Refresh messages.
Invalid Originator Addr	Number of messages with invalid Originator address.

Display details of one invalid PIM (IPv6) message recently received lately.

```
<HUAWEI> display pim ipv6 invalid-packet 1 verbose
      Detailed information of invalid packets
-------------------------------------------------------
Packet information (Index 1):
-------------------------------------------------------
Interface           :  Vlanif100
Time                :  2012-06-01 20:04:35 UTC-08:00
Message Length      :  26
Invalid Type        :  Invalid Multicast Source
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00
0010: 00 00 80 00 00 64 00 00 00 00
-------------------------------------------------------
```

Table 8-66 Description of the display pim ipv6 invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details about invalid PIM (IPv6) messages.
Packet information (Index 1)	Sequence number of an invalid PIM (IPv6) message (numbered in the opposite order).
Interface	Number of interfaces that receive the invalid PIM (IPv6) message.
Time	Time when the invalid SPT switch message was received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST The format UTC±HH:MM indicates that a time zone was configured with the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid PIM (IPv6) message.
Invalid Type	Type of the invalid PIM (IPv6) message.
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00 0010: 00 00 80 00 00 64 00 00 00 00	Contents of the invalid PIM (IPv6) message.

8.4.27 display pim ipv6 neighbor

Function

The **display pim ipv6 neighbor** command displays information about PIM (IPv6) neighbors.

Format

display pim ipv6 neighbor [*ipv6-link-local-address* | **interface** *interface-type interface-number* | **verbose**] *

Parameters

Parameter	Description	Value
ipv6-link-local-address	Specifies the IPv6 link-local address of a neighbor.	The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
verbose	Indicates the details of PIM neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim ipv6 neighbor** command displays PIM (IPv6) neighbor information, including the number of PIM (IPv6) neighbors and DR priorities of neighbors. You can adjust PIM (IPv6) neighbor relationships according to the command output.

Example

Display detailed information about PIM (IPv6) neighbors on VLANIF100.

```
<HUAWEI> display pim ipv6 neighbor interface vlanif 100 verbose
 VPN-Instance: public net

 Total Number of Neighbors on this interface  = 1

Neighbor: FE80::FFE0:FFFF:FE4A:8E04
     Interface: Vlanif100
     Uptime: 00:01:18
     Expiry time: 00:01:31
     DR Priority: 1
     Generation ID: 0x7751638D
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     Neighbor tracking: disabled
     PIM BFD-session: N
     Neighbor Secondary Address(es):
     FC00:0:0:2004::2
```

Table 8-67 Description of the **display pim ipv6 neighbor** command output

Item	Description
Total Number of Neighbors on this interface	Total number of PIM (IPv6) neighbors on an interface.
Neighbor	Address of a PIM (IPv6) neighbor.
Interface	Interface where the PIM (IPv6) neighbor resides.
Uptime	How long has the PIM (IPv6) neighbor been in Up state.
Expiry time	How soon the PIM (IPv6) neighbor will time out.
DR Priority	DR priority of the PIM (IPv6) neighbor.
Generation ID	Indicates the randomly generated 32-bit value of PIM (IPv6) neighbor.
Holdtime	Keepalive period of the PIM (IPv6) neighbor.
LAN delay	Delay in transmitting Prune messages.
Override interval	Interval for overriding the Prune action.
Neighbor tracking	Whether the neighbor tracking neighbor function is enabled.
PIM BFD-session	Whether a BFD session is set up.
Neighbor Secondary Address (es)	IPv6 address of the neighbor.

8.4.28 display pim ipv6 routing-table

Function

The **display pim ipv6 routing-table** command displays the PIM (IPv6) multicast routing table.

Format

display pim ipv6 routing-table [*ipv6-source-address* [**mask** *mask-length*] | *ipv6-group-address* [**mask** *mask-length*] | **flags** *flag-value* | **fsm** | **incoming-interface** { *interface-type interface-number* | **register** } | **mode** { **dm** | **sm** | **ssm** } | **outgoing-interface** { **exclude** | **include** | **match** } { *interface-type interface-number* | **none** | **register** }] * [**outgoing-interface-number** [*number*]]

display pim ipv6 routing-table brief [*ipv6-source-address* [**mask** *mask-length*] | *ipv6-group-address* [**mask** *mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** }] *

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-group-address	Specifies the IPv6 address of a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
mask *mask-length*	Specifies the mask length of a multicast source or group.	The value is an integer. The mask length of a multicast source ranges from 0 to 128. The mask length of a multicast group ranges from 8 to 128.
flags *flag-value*	Displays of routing entries of a specified type. *flag-value* specifies the flag of a routing entry.	-
fsm	Displays detailed information about the finite state machine (FSM).	-
incoming-interface	Displays the routing entry with the specified upstream interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Displays the register interface.	-
dm	Displays PIM-DM (IPv6) routing entries.	-
sm	Displays PIM-SM (IPv6) routing entries.	-
ssm	Displays PIM-SSM (IPv6) routing entries.	-

Parameter	Description	Value
outgoing-interface { **exclude** | **include** | **match** }	Displays the routing entries with or without a specified outbound interface. - exclude: displays the entries that do not contain the specified interface. - include: displays the entries that contain the specified interface. - match: displays the entries match the specified interface.	-
none	Displays the routing entry without the downstream interface.	-
outgoing-interface-number	Displays the number of the outbound interfaces of routing entries.	-
number	Specifies the number of the outbound interfaces to be queried.	-
brief	Displays only the name of upstream interface and the number of downstream interfaces of routing entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to:

- Check whether PIM (IPv6) has been configured successfully on the network.
- Check the inbound interfaces, outbound interfaces, flags, and other information in the routing entries to identify failure points when forwarding errors occur on the PIM (IPv6) network.

The PIM (IPv6) routing table includes both (*, G) and (S, G) entries. (*, G) entries are used to set up a rendezvous point tree (RPT), and (S, G) entries are used to set up a shortest path tree (SPT).

Table 8-68 lists the values of the **flags** *flag-value* parameter.

Table 8-68 Values of the *flag-value* parameter

Item	Description
act	Indicates that the multicast routing entry at which actual data arrives exists.
del	Indicates the multicast routing entry to be deleted.
exprune	Indicates that the entry on the RPT is pruned and no receiver on the RPT requests the information sent by the source.
ext	Indicates routing entries that contain downstream interfaces provided by other multicast routing protocols.
loc	Indicates routing entries on the switch directly connected to the network segment where the source resides.
niif	Indicates routing entries with unknown upstream interfaces.
nonbr	Indicates that the routing entry of the upstream neighbor address (link-local address) towards the RP or the source is not found.
none	Indicates routing entries without any flag.
rpt	Indicates the routing entries that are on the RPT but do not use the RPT data.
sg_rcvr	Indicates that the (S, G) receiver of S exists on the local switch and PIM (IPv6) is the owner of the downstream interface.
sgjoin	Indicates that the (S, G) receiver of S exists on the local switch and PIM (IPv6) is not the owner of the downstream interface.
spt	Indicates routing entries on the shortest path tree (SPT).
swt	Indicates routing entries during the SPT switchover.
upchg	Indicates a route change has occurred. The current entry uses the original upstream interface to forward data and waits for data received from a new interface.
wc	Indicates a (*, G) entry.

Example

Display the PIM (IPv6) multicast routing table.

```
<HUAWEI> display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FFE3::1)
     RP: FC00:0:0:1::1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:57:31
     Upstream interface: NULL
         Upstream neighbor: NULL
```

```
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlanif10
            Protocol: static, UpTime: 00:57:31, Expires: never

(FC00:0:0:2001::2, FFE3::1)
    RP: FC00:0:0:1::1
    Protocol: pim-sm, Flag: ACT WC
    UpTime: 00:04:24
        1: Vlanif20
        Upstream neighbor: FE80::A01:100:1
        RPF prime neighbor: FE80::A01:100:1
    Downstream interface(s) information:
    Upstream interface: Vlanif10
            Protocol: pim-dm, UpTime: 00:04:24, Expires:  -
```

Table 8-69 Description of the **display pim ipv6 routing-table** command output

Item	Description
Total 1 (*, G) entry; 1 (S, G) entry	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
(*, FFE3::1)	(*, G) entry in the PIM routing table.
RP	RP address.
Protocol	Type of PIM (IPv6) protocols, PIM-DM (IPv6), PIM-SM (IPv6), or PIM-SSM (IPv6).
Flag	Flag of a (S, G) entry or (*, G) entry in the PIM (IPv6) routing table.
UpTime	Lifetime of an interface.
Upstream interface	Upstream interface of a (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of a (S, G) entry or (*, G) entry.
RPF prime neighbor	RPF neighbor of a (S, G) entry or (*, G) entry. ● For a (*, G) entry, when the local device is an RP, the RPF neighbor is Null. ● For a (S, G) entry, when the local device is directly connected to the multicast source, the RPF neighbor is Null.

Item	Description
Downstream interface(s) information	Information about downstream interfaces, including: - Number of downstream interfaces - Names of downstream interfaces - Type of the PIM (IPv6) protocol configured on the downstream interfaces - Existing period and timeout period of downstream interfaces
Total number of downstreams	Number of downstream interfaces.
Vlanif10	Interface name.
Expires	Timeout period of an entry.

Display the brief information about PIM (IPv6) routing entries.

```
<HUAWEI> display pim ipv6 routing-table brief FF25::1
 VPN-Instance: public net
 Total 3 (*, G) entries; 3 (S, G) entries

 Total matched 1 (*, G) entry; 1 (S, G) entry

  00001. (FC00:0:0:2008::55, FF25::1)
       Upstream interface: Vlanif10
       Number of downstreams: 2
  00002. (*, FF25::1)
       Upstream interface: Vlanif10
       Number of downstreams: 2
```

Table 8-70 Description of the display pim ipv6 routing-table brief command output

Item	Description
Total 3 (*, G) entries; 3 (S, G) entries	Total number of the (S, G) entries and (*, G) entries in the PIM (IPv6) routing table.
Total matched 1 (*, G) entry; 1 (S, G) entry	Total number of the (S, G) entries and (*, G) entries that meet the query conditions in the PIM routing table.
00001. (FC00:0:0:2008::55, FF25::1)	(S, G) entry.
Number of downstreams	Number of downstream interfaces in (S, G) entries or (*, G) entries.

Display the number of the outbound interfaces of PIM (IPv6) routing entries.

```
<HUAWEI> display pim ipv6 routing-table outgoing-interface-number
 VPN-Instance: public net
```

```
Total 2 (*, G) entries; 0 (S, G) entry

(*, FF25::1)
    RP: FC00:0:0:2008::5:3:2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:04
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2

(*, FF25::2)
    RP: FC00:0:0:2008::5:3:2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:00:05
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 2
```

8.4.29 display pim ipv6 rp-info

Function

The **display pim ipv6 rp-info** command displays information about the RP corresponding to a multicast group.

Format

display pim ipv6 rp-info [*ipv6-group-address*]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pim ipv6 rp-info** command displays information about the RP to which a multicast group corresponds. This command can help determine whether multicast forwarding errors are caused by faults of an RP.

Precautions

The RP information contains the information about the RP discovered through the BSR mechanism and static RP.

If the group address is not specified in this command, the corresponding RP information of all the multicast groups is displayed.

Example

Display the RP of multicast group FF1E::1.

```
<HUAWEI> display pim ipv6 rp-info ff1e::1
 VPN-Instance: public net
 BSR RP Address is: FE1E::1
     Priority: 192
     Uptime: 00:00:52
     Expires: 00:01:38
 RP mapping for this group is: FC00:0:0:2001::1 (local host)
```

Table 8-71 Description of the **display pim ipv6 rp-info** command output

Item	Description
VPN-Instance	VPN instance to which RP information belongs. **public net** indicates the public network instance.
BSR RP Address is	IP address of a dynamical RP
Priority	RP priority
Uptime	Period during which the RP exists
Expires	Time before an RP times out
RP mapping for this group is	Address of the RP to which multicast group corresponds

8.4.30 embedded-rp

Function

The **embedded-rp** command enables the embedded RP function.

The **undo embedded-rp** command disables the embedded RP function.

By default, the embedded RP function is enabled.

Format

embedded-rp [*basic-acl6-number*]

undo embedded-rp [*basic-acl6-number*]

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The embedded RP function is enabled by default after PIM-SM (IPv6) is enabled. This function enables the switch to obtain the RP address from the IPv6 multicast address of a received multicast packet, so that the switch does not need to know the RP information beforehand.

By default, the switch can parse group addresses in the range of FF7x::/12. The value of x can be 0 or any integer in the range of 3 to F. When the switch receives a multicast packet with an IPv6 group address in this range, the switch can obtain the RP address from the IPv6 group address. This RP will replace the static RP or dynamically elected RP. If you do not want the switch to use RP information obtained from IPv6 multicast addresses of multicast packets, run the **undo embedded-rp** command to disable the embedded RP function.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If an IPv6 ACL is specified in the command, the final group address range for embedded RP is the intersection of the group address range specified by the IPv6 ACL and the default group address range. All the devices in the PIM (IPv6) domain must be configured with the same group address range.

The **embedded-rp** command and the **acl** command are used together.

- For the IPv6 numbered ACL, in the ACL6 view, you can set the source address range of multicast groups that is enabled with the embedded RP by specifying the **source** parameter in the **rule** command.
- For the IPv6 Named ACL, in the ACL6 view, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the address range of multicast groups that is specified by the **destination** parameter and with the time period that is specified by the **time-range** parameter.

This command is cyclical in nature. That is, the latest command overwrites the previous one, and takes effect.

Example

Enable the embedded RP function on multicast group ff73::.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule permit source ff73:: 12
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] embedded-rp 2000
```

8.4.31 graceful-restart (IPv6)

Function

The **graceful-restart** command enables PIM GR.

The **undo graceful-restart** command disables PIM GR.

By default, PIM GR is not enabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a stack is used on the PIM-SM (IPv6) network, multicast data transmission is interrupted after an active/standby switchover occurs in the stack, because the slave switch on the new master device does not have PIM (IPv6) forwarding entries.

PIM GR enables the system to back up join and prune information in PIM (IPv6) routing entries to the new master device when an active/standby switchover is performed in the system. This ensures normal multicast data forwarding during restoration of the multicast distribution tree. For details about stack configuration, see Stack Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

At least one interface must have PIM-SM (IPv6) enabled for the **graceful-restart** command to take effect.

Example

Enable PIM GR in the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] graceful-restart
```

8.4.32 graceful-restart period (IPv6)

Function

The **graceful-restart period** command configures the minimum PIM GR period.

The **undo graceful-restart period** command restores the default minimum PIM GR period.

By default, the minimum PIM GR period is 120 seconds.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	The value is an integer that ranges from 90 to 3600 in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimum time for maintaining forwarding entries.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

Unicast protocol GR forms the basis of PIM GR; therefore, the minimum PIM GR period should be longer than the corresponding unicast protocol GR period.

The PIM GR period also depends on the complexity of the network topology and increases with the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the PIM-IPv6 view to 150 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] graceful-restart
[HUAWEI-pim6] graceful-restart period 150
```

8.4.33 hello-option dr-priority (IPv6)

Function

The **hello-option dr-priority** command configures the designated router (DR) priority for the switch.

The **undo hello-option dr-priority** command restores the default DR priority.

By default, the DR priority for the switch is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the DR priority of the switch.	The value is an integer that ranges from 0 to 4294967295. The greater the value, the higher the priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IPv6 PIM-SM network, switches on a shared network segment are candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR is elected based on the priority and the IPv6 address. The switches send Hello messages carrying the priority for DR election. The switch with the highest priority becomes the DR. If the switches have the same priority, the switch with the largest IPv6 address becomes the DR.

If at least one switch in the network does not support Hello packets that contain the priority, the switch with the largest IPv6 address functions as the DR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **hello-option dr-priority** command has the same function as the **pim ipv6 hello-option dr-priority** command in the interface view. By default, if the **pim ipv6 hello-option dr-priority** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, configure the DR priority of a switch to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option dr-priority 3
```

8.4.34 hello-option holdtime (IPv6)

Function

The **hello-option holdtime** command sets the timeout period for a switch to wait to receive Hello messages from its PIM neighbor.

The **undo hello-option holdtime** command restores the default configuration.

By default, the timeout period for a switch to wait to receive Hello messages from its PIM neighbor is 105 seconds.

Format

hello-option holdtime *interval*

undo hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which a switch waits to receive a Hello message from its PIM neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM (IPv6) network, after a switch receives a Hello message from its PIM neighbor, the switch starts a timer based on the Holdtime value in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, it considers the neighbor invalid or unreachable.

The **hello-option holdtime (IPv6)** command sets the timeout period during which a PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The timeout period must be greater than the interval for sending Hello messages. You can run the **timer hello (IPv6)** command to set the interval for sending Hello messages.

The **hello-option holdtime** command has the same function as the **pim ipv6 hello-option holdtime** command in the interface view. By default, if the **pim ipv6 hello-option holdtime** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, set the timeout interval to 120 seconds. The timeout interval is the period during which a switch waits to receive the Hello message from its PIM neighbor.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option holdtime 120
```

8.4.35 hello-option lan-delay (IPv6)

Function

The **hello-option lan-delay** command sets the delay in transmitting Prune message on the shared network segment.

The **undo hello-option lan-delay** command restores the default delay.

By default, the delay in transmitting Prune message on the shared network segment is 500 milliseconds.

Format

hello-option lan-delay *interval*

undo hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting Prune message on the shared network segment.	The value is an integer that ranges from 1 to 32767, in milliseconds (ms).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If devices on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values and refer to the delay from the current device receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface before the PPT timer expires, it cancels the prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If the delay in transmitting Prune message is too short, the upstream device will stop forwarding multicast packets before the downstream device determines whether to override the Prune action or not. Exercise caution when you run the **hello-option lan-delay** command.

The **hello-option lan-delay** command has the same function as the **pim ipv6 hello-option lan-delay** command in the interface view. By default, if the **pim ipv6 hello-option lan-delay** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting Prune message on the shared network segment to 200 ms in the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option lan-delay 200
```

8.4.36 hello-option neighbor-tracking (IPv6)

Function

The **hello-option neighbor-tracking** command enables the neighbor tracking function.

The **undo hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on a shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

When the switch with neighbor tracking enabled detects Join messages from other devices, the switch still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Neighbor tracking can be implemented only when this function is enabled on all devices on the shared network segment.

The **hello-option neighbor-tracking** command has the same function as the **pim ipv6 hello-option neighbor-tracking** command in the interface view. By default, if neighbor tracking is not used on an interface, the neighbor tracking configuration in the PIM-IPv6 view takes effect.

Example

In the PIM-IPv6 view, enable the downstream neighbor tracking function.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option neighbor-tracking
```

8.4.37 hello-option override-interval (IPv6)

Function

The **hello-option override-interval** command sets the interval for overriding the prune action in a Hello message.

The **undo hello-option override-interval** command restores the default interval.

By default, the interval for overriding the prune action in a Hello message is 2500 ms.

Format

hello-option override-interval *interval*

undo hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **override-interval** parameter refers to the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

If switches on the same link have different values, the maximum value is used.

The value of PPT is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT expires. If the switch receives a Join message from the downstream interface before the PPT expires, it cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **hello-option override-interval** command has the same function as the **pim ipv6 hello-option override-interval** command in the interface view. By default, if the **pim ipv6 hello-option override-interval** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, set the interval for denying the prune action in a Hello message to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] hello-option override-interval 2000
```

8.4.38 holdtime assert (IPv6)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local switch.

The **undo holdtime assert** command restores the default timeout.

By default, the timeout period for all PIM interfaces to keep the Assert state on the local switch is 180 seconds.

Format

holdtime assert *interval*

undo holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the time during which the PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **holdtime assert** command has the same function as the **pim ipv6 holdtime assert** command in the interface view. By default, if the timeout period is not used on an interface, the timeout period configured in the PIM-IPv6 view is used.

Example

In the PIM-IPv6 view, set the interval during which a switch keeps the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] holdtime assert 100
```

8.4.39 holdtime join-prune (IPv6)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. Devices that receive Join/Prune messages set the time during which the downstream interface keeps the Join or Prune state according to holdtime.

The **undo holdtime join-prune** command restores the default value.

By default, the holdtime value in Join/Prune messages sent by all PIM interfaces is 210 seconds.

Format

holdtime join-prune *interval*

undo holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime carried in Join/Prune messages sent by the local device.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the hold timer. If this message carries group-join information and the switch does not receive subsequent Join/Prune messages from the downstream device when the timer expires, it suppresses multicast data forwarding to downstream interfaces of the specified group. If Join/Prune message carries group-prune information, the switch resumes multicast data forwarding to downstream interfaces when the hold timer expires.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **holdtime join-prune** command has the same function as the **pim ipv6 holdtime join-prune** command in the interface view. By default, if the holdtime value is not used on an interface, the holdtime value configured in the PIM-IPv6 view is used.

Example

In the PIM-IPv6 view, set the time during which the downstream interface of a switch keeps the Join or Prune state to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] holdtime join-prune 280
```

8.4.40 join-prune max-packet-length (IPv6)

Function

The **join-prune max-packet-length** command sets the maximum size of each Join/Prune message to be sent.

The **undo join-prune max-packet-length** command restores the default maximum size of each Join/Prune message to be sent.

By default, the maximum length of Join/Prune message sent by is 8100 bytes.

Format

join-prune max-packet-length *packet-length*

undo join-prune max-packet-length

Parameters

Parameter	Description	Value
packet-length	Specifies the maximum size of each PIM-SM Join/Prune message to be sent.	The value is an integer that ranges from 100 to 64000, in bytes.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has low performance and takes a long time to process a large Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be reduced to relieve the burden on the peer device.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

If the maximum size specified in the **join-prune max-packet-length** command is greater than the interface MTU, the maximum size of each message to be sent is equal to the interface MTU.

Example

Set the maximum size of each Join/Prune message to be sent to 2100 bytes.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] join-prune max-packet-length 2100
```

8.4.41 join-prune periodic-messages queue-size (IPv6)

Function

The **join-prune periodic-messages queue-size** command sets the maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.

The **undo join-prune periodic-messages queue-size** command restores the default maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.

By default, a Join/Prune message that is sent every second contains 1020 entries.

Format

join-prune periodic-messages queue-size *queue-size*

undo join-prune periodic-messages queue-size

Parameters

Parameter	Description	Value
queue-size	Specifies the maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.	The value is an integer that ranges from 16 to 4096.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has a low throughput, reduce the length of a queue for periodically sending messages to control the number of (S, G) entries. This setting allows the local device to send Join/Prune messages with a small number of (S, G) entries multiple times, preventing packet loss or route flapping.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

Allow each Join/Prune message that is sent every second to carry a maximum of 2000 (S, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] join-prune periodic-messages queue-size 2000
```

8.4.42 join-prune triggered-message-cache disable (IPv6)

Function

The **join-prune triggered-message-cache disable** command disables the Join/Prune message package function.

The **undo join-prune triggered-message-cache disable** command enables the Join/Prune message package function.

By default, the Join/Prune message package function is enabled.

Format

join-prune triggered-message-cache disable

undo join-prune triggered-message-cache disable

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system performs more efficiently when sending a package of Join/Prune messages than sending a large number of individual Join/Prune messages. A device sends Join/Prune messages in packages. To disable the package function, run the **join-prune triggered-message-cache disable** command.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

Disable the Join/Prune message package function.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] join-prune triggered-message-cache disable
```

8.4.43 neighbor-check (IPv6)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

By default, the PIM neighbor check function is not enabled.

Format

neighbor-check { **receive** | **send** }

undo neighbor-check { **receive** | **send** }

Parameters

Parameter	Description	Value
receive	Checks whether the Join/Prune and Assert messages are received from a PIM neighbor. If not, these messages are discarded.	-
send	Checks whether the Join/Prune and Assert messages are sent to a PIM neighbor. If not, these messages are not sent.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices send Join/Prune messages to the upstream PIM neighbor to perform join and prune actions and PIM neighbors often exchange Assert messages. To save system resources and protect security of Join/Prune messages and Assert messages, run the **neighbor-check** command to enable the PIM neighbor check function.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can specify both **receive** and **send** to enable the PIM neighbor check function for the received and sent Join/Prune and Assert messages.

This command is valid for only PIM-SM (IPv6).

Example

In the PIM-IPv6 view, enable the PIM neighbor check function for the received Join/Prune and Assert messages.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] neighbor-check receive
```

8.4.44 pim-ipv6

Function

The **pim-ipv6** command displays the PIM-IPv6 view.

The **undo pim-ipv6** command clears the configuration in the PIM-IPv6 view.

Format

pim-ipv6

undo pim-ipv6

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing PIM (IPv6) configurations, run the **pim-ipv6** command to enter the PIM-IPv6 view.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

In using the **undo pim-ipv6** command, enter Y or N to confirm the action. This command clears global PIM (IPv6) configurations in the current instance. Use this command with caution.

Example

Enter the PIM-IPv6 view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6]
```

8.4.45 pim ipv6 bfd

Function

The **pim ipv6 bfd** command configures PIM BFD (IPv6) parameters on an interface.

The **undo pim ipv6 bfd** command restores default PIM BFD (IPv6) parameters on an interface.

By default, the interval for transmitting BFD packets and interval for receiving BFD packets are 1000 ms, and the BFD detection multiplier is 3.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim ipv6 bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* }*

undo pim ipv6 bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** }*

undo pim ipv6 bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* }*

Parameters

Parameter	Description	Value
min-tx-interval *tx-value*	Specifies the interval for sending BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.
min-rx-interval *rx-value*	Specifies the interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Parameter	Description	Value
detect-multiplier *multiplier-value*	Specifies the local detection multiplier of BFD packets. - For a stable link, you can set the detection multiplier to a large value to avoid frequent link detection. - For an unstable link, a small detection multiplier may cause BFD session flapping. Therefore, it is recommended that you set the detection multiplier to a large value.	The value is an integer ranging from 3 to 50. The default value is 3.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to control detection parameters of BFD packets, run the **pim ipv6 bfd** command to configure the sending interval, receiving interval, and local detection multiplier for PIM BFD (IPv6) packets.

The **min-tx-interval**, **min-rx-interval**, and **detect-multiplier** parameters can be configured separately at two ends of a link so that the two ends can send or receive BFD packets at different rates. If there is no special requirement for the detection period and the link is stable, you are advised to configure the same parameter settings for the routing devices that have the same performance and are on the shared network segment.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

After BFD parameters are configured, PIM (IPv6) provides the address to be detected, the minimum sending interval and receiving interval of PIM BFD (IPv6) packets, and the local detection multiplier for BFD. The two ends enabled with BFD then negotiate the actual sending interval and receiving interval, and the detection period based on these configured parameters. During the detection phase, BFD notifies the route management (RM) module of the BFD session status and the RM module then notifies PIM (IPv6) of the session status.

If a link fault occurs, BFD quickly notifies the RM of the session status and the RM then notifies PIM (IPv6) of the session status. The PIM (IPv6) protocol deletes the status of the faulty interface, triggers a new DR or Assert election, and restores the forwarding of multicast data to the downstream interface. This shortens the period of multicast traffic interruption caused by the interface fault.

Precautions

To validate PIM BFD (IPv6), ensure that a BFD session has been set up and the session is in the Up state.

The two ends negotiate the actual sending interval and receiving interval, and detection period of BFD packets based on the following negotiation mechanism:

- The formula used to calculate the interval for sending PIM IPv6 BFD packets and the formula used to calculate the interval for receiving PIM IPv6 BFD packets are as follows:
  - Interval for sending PIM IPv6 BFD packets = Max (Local **min-tx-interval**, Remote **min-rx-interval**)
  - Interval for receiving PIM IPv6 BFD packets = Max (Remote **min-tx-interval**, Local **min-rx-interval**)
- The formula used to calculate the detection period is as follows:
  - Detection period = Remote **detect-multiplier** x Max (Remote **min-tx-interval**, Local **min-rx-interval**)

If a large parameter value is set, BFD will take a long time to detect a fault on a link. This may cause packet loss.

Example

Enable PIM BFD (IPv6) on VLANIF 100, and set both the minimum interval for sending BFD packets and the minimum interval for receiving BFD packets to 200 ms and the local detection multiplier to 5.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 sm
[HUAWEI-Vlanif100] pim ipv6 bfd enable
[HUAWEI-Vlanif100] pim ipv6 bfd min-tx-interval 200 min-rx-interval 200 detect-multiplier 5
```

Enable PIM BFD (IPv6) on GE0/0/1, and set both the minimum interval for sending BFD packets and the minimum interval for receiving BFD packets to 200 ms and the local detection multiplier to 5.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 sm
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bfd enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bfd min-tx-interval 200 min-rx-interval 200 detect-multiplier
5
```

8.4.46 pim ipv6 bfd enable

Function

The **pim ipv6 bfd enable** command enables PIM BFD (IPv6) on an interface.

The **undo pim ipv6 bfd enable** command disables PIM BFD (IPv6) on an interface.

By default, PIM BFD (IPv6) is disabled on an interface.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

pim ipv6 bfd enable

undo pim ipv6 bfd enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To minimize the impact of a fault on services and improve network availability, a network device is required to quickly detect a communications fault between adjacent devices so that the upper layer protocol can rectify the fault to ensure normal services.

On a PIM network, changes of link status between PIM neighbors will restart some PIM mechanisms, such as DR election or Assert winner election. For example, when the DR or Assert winner on a shared network segment fails, PIM neighbors on the network segment trigger DR or Assert winner re-election only when the PIM neighbor relationships time out. Multicast data transmission is interrupted before a new DR or Assert winner is elected. The multicast service interruption time is longer than or equal to the neighbor relationship timeout interval or Assert timer value, and is usually several seconds.

PIM BFD (IPv6) can detect link status changes on a shared network segment in milliseconds, enabling PIM devices to rapidly respond to failures of PIM neighbors. If a PIM BFD (IPv6)-capable interface does not receive any BFD packets from the DR or Assert winner within the detection interval, it considers that the DR or Assert winner has failed. Then BFD rapidly reports the session status to the route management (RM) module, which then reports the link status change to the PIM module. After receiving the notification, the PIM module triggers DR or Assert winner re-election immediately, without waiting for timeout of the neighbor relationship. This mechanism reduces the multicast service interruption time and improves reliability of multicast data transmission.

Pre-configuration Tasks

PIM BFD (IPv6) depends on the BFD protocol. Therefore, you need first to enable BFD globally to validate the PIM BFD (IPv6) function.

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Before configuring PIM BFD (IPv6), enable PIM-SM (IPv6) in the interface view. If the **undo pim ipv6 sm** command is run, IPv6 PIM-SM is disabled and the PIM BFD (IPv6) function is removed from the interface at the same time.

Example

Enable PIM BFD (IPv6) on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 sm
[HUAWEI-Vlanif100] pim ipv6 bfd enable
```

Enable PIM BFD (IPv6) on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 sm
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bfd enable
```

8.4.47 pim ipv6 bsr-boundary

Function

The **pim ipv6 bsr-boundary** command configures the BSR boundary of a PIM-SM (IPv6) domain on an interface.

The **undo pim ipv6 bsr-boundary** command restores the default configuration.

By default, the BSR boundary of a PIM-SM (IPv6) domain is not set.

Format

pim ipv6 bsr-boundary

undo pim ipv6 bsr-boundary

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the management core of the PIM-SM (IPv6) network, the BSR is responsible for sending collected RP-set information to PIM neighbors through Bootstrap messages.

You can divide a large PIM-SM (IPv6) network into multiple PIM-SM (IPv6) domains by configuring the bsr boundary on an interface. Each BSR then serves the local PIM-SM (IPv6) domain.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The Bootstrap messages cannot traverse the BSR boundary but other multicast packets can.

Example

Configure the BSR boundary of a PIM-SM (IPv6) domain on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 bsr-boundary
```

Configure the BSR boundary of a PIM-SM (IPv6) domain on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 bsr-boundary
```

8.4.48 pim ipv6 dm

Function

The **pim ipv6 dm** command enables PIM-DM (IPv6) on an interface.

The **undo pim ipv6 dm** command restores the default configuration.

By default, PIM-DM (IPv6) is disabled on an interface.

Format

pim ipv6 dm

undo pim ipv6 dm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM (IPv6) is a multicast routing protocol in dense mode and applies to small-scale networks with densely-distributed group members.

After PIM-DM (IPv6) is enabled on an interface, the switch can set up the PIM neighbor relationship with the neighboring device. The switch then can process protocol packets received from PIM neighbors.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM-DM (IPv6) and PIM-SM (IPv6) cannot be enabled simultaneously on the device.

If PIM-DM (IPv6) and MLD need to be enabled on the same interface, enable PIM-DM (IPv6), and then enable MLD.

Running the **pim ipv6 dm** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable PIM (IPv6) on the corresponding VLANIF interface first, and then enable MLD snooping in the VLAN. If MLD snooping is enabled in the VLAN first, PIM (IPv6) cannot be enabled on the VLANIF interface.

Example

Enable PIM-DM (IPv6) on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 dm
```

Enable PIM-DM (IPv6) on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 dm
```

8.4.49 pim ipv6 hello-option dr-priority

Function

The **pim ipv6 hello-option dr-priority** command sets the priority for the PIM interface that is elected as DR.

The **undo pim ipv6 hello-option dr-priority** command restores the default value of the priority.

By default, the priority for the PIM interface that is elected as DR is 1.

Format

pim ipv6 hello-option dr-priority *priority*

undo pim ipv6 hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the PIM interface that is elected as DR.	The value is an integer that ranges from 0 to 4294967295. The greater the value, the higher the priority.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM (IPv6) network, devices on a shared network segment are candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR is elected based on the priority and the IPv6 address. Switches send Hello messages carrying their priorities to each other, and the one with the highest priority becomes the DR. If the switches have the same priority, the switch with the largest IPv6 address becomes the DR.

If at least one device in the network does not support Hello packets that contain the priority, the device with the largest IPv6 address functions as the DR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 hello-option dr-priority** command has the same function as the **hello-option dr-priority (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option dr-priority** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the priority of VLANIF100 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option dr-priority 3
```

Set the priority of GE0/0/1 that is elected as DR to 3.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option dr-priority 3
```

8.4.50 pim ipv6 hello-option holdtime

Function

The **pim ipv6 hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

The **undo pim ipv6 hello-option holdtime** command restores the default value of the timeout.

By default, the timeout period during which the PIM interface waits to receive the Hello message from its neighbor is 105 seconds.

Format

pim ipv6 hello-option holdtime *interval*

undo pim ipv6 hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the PIM interface waits to receive Hello messages from its neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM (IPv6) network, after a switch receives a Hello message from its PIM neighbor, it starts a timer based on Holdtime value in the Hello message. If the switch does not receive any Hello message from its PIM neighbor when the timer expires, the switch considers the neighbor invalid or unreachable.

The **pim ipv6 hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The timeout period must be greater than the interval for sending Hello messages, which is set using the **pim ipv6 time hello** command.

The **pim ipv6 hello-option holdtime** command has the same function as the **hello option holdtime (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option holdtime** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period during which VLANIF100 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option holdtime 120
```

Set the timeout period during which GE0/0/1 waits to receive Hello messages from its neighbor to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option holdtime 120
```

8.4.51 pim ipv6 hello-option lan-delay

Function

The **pim ipv6 hello-option lan-delay** command sets the delay in transmitting messages in a shared network in the interface view.

The **undo pim ipv6 hello-option lan-delay** command restores the default value of the delay.

By default, the delay in transmitting messages in the shared network is 500 ms.

Format

pim ipv6 hello-option lan-delay *interval*

undo pim ipv6 hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent switches carry **lan-delay** and **override-interval** values. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. If devices on the same link have different **lan-delay** values, the maximum value is used.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

The value of the Prune-Pending Timer (PPT) is the sum of **lan-delay** and **override-interval** values and refer to the delay from the current device receiving a Prune message from the downstream interface to performing the prune action. If the switch receives a Join message from the downstream interface before the PPT timer expires, it cancels the prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

If the prune delay is set too short, the upstream device stops forwarding multicast packets before the downstream device overrides Prune messages of neighbors. Exercise caution when you run this command.

The function of this command in the interface view is the same as that of the **hello-option lan-delay (IPv6)** command in the PIM-IPv6 view. By default, if the configuration on the interface is not performed, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting messages to 200 ms on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option lan-delay 200
```

Set the delay in transmitting messages to 200 ms on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option lan-delay 200
```

8.4.52 pim ipv6 hello-option neighbor-tracking

Function

The **pim ipv6 hello-option neighbor-tracking** command enables the neighbor tracking function in the interface view.

The **undo pim ipv6 hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

pim ipv6 hello-option neighbor-tracking

undo pim ipv6 hello-option neighbor-tracking

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, a switch generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. In this case, the neighboring device detects the Generation ID change after receiving the Hello message and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment prepare to send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. This means that the upstream neighbor cannot update neighbor relationships with downstream devices after a Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

The neighbor tracking function can be implemented on a shared network segment only when this function is enabled on all devices on the network segment.

The **pim ipv6 hello-option neighbor-tracking** command has the same function as the **hello-option neighbor-tracking (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option neighbor-tracking** command is not used, the configuration in the PIM-IPv6 view takes effect; otherwise, the configuration in the interface view takes effect.

Example

Enable the neighbor tracking function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option neighbor-tracking
```

Enable the neighbor tracking function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option neighbor-tracking
```

8.4.53 pim ipv6 hello-option override-interval

Function

The **pim ipv6 hello-option override-interval** command sets the interval carried in Hello messages for overriding the prune action on the interface.

The **undo pim ipv6 hello-option override-interval** command, restores the default configuration.

By default, the interval carried in Hello messages for overriding the prune action on the interface is 2500 milliseconds.

Format

pim ipv6 hello-option override-interval *interval*

undo pim ipv6 hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval of overriding the prune action.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent from switches carry **lan-delay** and **override-interval** values. The **override-interval** parameter refers to the period during which a downstream switch can override the prune action.

When a switch sends a Prune message to the upstream device in the same network segment, the other devices that still request multicast data need to send a Join message to the upstream device within the override-interval period.

If switches on the same link have different values, the maximum value is used.

The value of PPT is the sum of **lan-delay** and **override-interval** values. When receiving a Prune message from a downstream interface, the switch does not perform the prune action until the PPT expires. If the switch receives a Join message from the downstream interface before the PPT expires, it cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 hello-option override-interval** command has the same function as the **hello-option override-interval (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option override-interval** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval for overriding the prune action in Hello messages to 2000 ms on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 hello-option override-interval 2000
```

Set the interval for overriding the prune action in Hello messages to 2000 ms on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 hello-option override-interval 2000
```

8.4.54 pim ipv6 holdtime assert

Function

The **pim ipv6 holdtime assert** command sets the timeout period during which a PIM interface keeps the Assert state.

The **undo pim ipv6 holdtime assert** command restores the default value of the timeout.

By default, the timeout period during which a PIM interface keeps the Assert state is 180 seconds.

Format

pim ipv6 holdtime assert *interval*

undo pim ipv6 holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which a PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM routers need to initiate the assert mechanism. The router that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **pim ipv6 holdtime assert** command has the same function as the **holdtime assert (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 holdtime assert** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period for VLANIF100 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 holdtime assert 100
```

Set the timeout period for GE0/0/1 to keep the Assert state to 100s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 holdtime assert 100
```

8.4.55 pim ipv6 holdtime join-prune

Function

The **pim ipv6 holdtime join-prune** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **undo pim ipv6 holdtime join-prune** command restores the default value of the holdtime.

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210 seconds.

Format

pim ipv6 holdtime join-prune *interval*

undo pim ipv6 holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the switch starts the hold timer. If this message carries group-join information and the switch does not receive subsequent Join/Prune messages from the downstream device when the timer expires, it suppresses multicast data forwarding to downstream interfaces of the specified group. If Join/Prune message carries group-prune information, the switch resumes multicast data forwarding to downstream interfaces when the hold timer expires.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 holdtime join-prune** command has the same function as the **holdtime join-prune (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 holdtime join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the holdtime in a Join/Prune message sent by VLANIF100 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 holdtime join-prune 280
```

Set the holdtime in a Join/Prune message sent by GE0/0/1 to 280 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 holdtime join-prune 280
```

8.4.56 pim ipv6 join-policy

Function

The **pim ipv6 join-policy** command enables the system to filter join information in Join/Prune messages.

The **undo pim ipv6 join-policy** command restores the default setting.

By default, join information in Join/Prune message is not filtered.

Format

pim ipv6 join-policy { **asm** *basic-acl6-number* | **ssm** *advanced-acl6-number* | *advanced-acl6-number* }

undo pim ipv6 join-policy [**asm** | **ssm**]

Parameters

Parameter	Description	Value
asm	Filters join information, with the group address in the ASM group address range.	-
basic-acl6-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
ssm	Filters join messages, with the group addresses within the SSM group address range and specified source address.	-
advanced-acl6-number	Specifies the advanced ACL number.	The value is an integer that ranges from 3000 to 3999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on the PIM-SM (IPv6) network by filtering join information in Join/Prune messages, run the **pim ipv6 join-policy** command.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

This command is valid for only IPv6 PIM-SM.

The **pim ipv6 join-policy** command and the **acl ipv6 (system view)** command are used together.

- If **asm** is specified, you can set the multicast group address range of join information in the basic ACL6 view by specifying the **source** parameter in the **rule (basic ACL6 view)** command.
- If **ssm** is specified, you can set the source address range and multicast group address range of join information in the advanced ACL6 view by respectively specifying the **source** parameter and **destination** parameter in the **rule (advanced ACL6 view)** command.

You must run the **multicast ipv6 routing-enable** command to enable the multicast function before using the command.

Example

Configure VLANIF100 to accept the join information with the group address FF25::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source ff25::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 join-policy asm 2001
```

Configure GE0/0/1 to accept the join information with the group address FF25::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source ff25::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 join-policy asm 2001
```

8.4.57 pim ipv6 neighbor-policy

Function

The **pim ipv6 neighbor-policy** command configures a policy for filtering PIM neighbors on an interface.

The **undo pim ipv6 neighbor-policy** command restores the default setting.

By default, PIM neighbors on the interface are not filtered.

Format

pim ipv6 neighbor-policy *basic-acl6-number*

undo pim ipv6 neighbor-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized neighbors from being involved in the PIM protocol, run the **pim ipv6 neighbor-policy** command to configure a policy for filtering PIM neighbors and set the address range of PIM neighbors. The switch sets up neighbor relationships with the addresses matching the filtering rules and deletes the neighbors that do not match the filtering rules.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **pim ipv6 neighbor-policy** command and the **acl ipv6** command are used together. In the ACL view, set the address range of PIM neighbors by specifying **source** in the **rule** command.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

When configuring the neighbor filtering function on the interface, you must also configure the neighbor filtering function correspondingly on the PIM neighbor of the interface.

If the IPv6 address of a PIM neighbor that has established a neighbor relationship with the device is not in the configured range of valid neighbor IPv6 addresses, the device will no longer receive Hello messages from this PIM neighbor. When the holdtime of Hello messages expires, the neighbor relationship between the PIM device and the device is terminated.

Example

Configure VLANIF100 to set up the PIM neighbor relationship with the switch of the address FC00:0:0:2000::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:2000::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 neighbor-policy 2001
```

Configure GE0/0/1 to set up the PIM neighbor relationship with the switch of the address FC00:0:0:2000::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:2000::1 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 neighbor-policy 2001
```

8.4.58 pim ipv6 require-genid

Function

The **pim ipv6 require-genid** command configures a PIM interface to reject the Hello messages without the Generation ID.

The **undo pim ipv6 require-genid** command restores the default configuration.

By default, a PIM interface is allowed to receive the Hello messages without the Generation ID.

Format

pim ipv6 require-genid

undo pim ipv6 require-genid

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface is enabled with PIM, the switch generates a random number as the Generation ID of the Hello message. If the device status is updated, the switch generates a new Generation ID. When the switch finds that the Hello message received from a PIM neighbor contains a different Generation ID, it considers that the status of the PIM neighbor has changed.

To ensure that connected PIM neighbors work properly, run the **pim ipv6 require-genid** command to configure a PIM interface to reject the Hello messages without the Generation ID.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Configure VLANIF100 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 require-genid
```

Configure GE0/0/1 to reject the Hello messages without the Generation ID.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 require-genid
```

8.4.59 pim ipv6 silent

Function

The **pim ipv6 silent** command enables the PIM silent (IPv6) function on an interface.

The **undo pim ipv6 silent** command cancels the PIM silent (IPv6) function on an interface.

By default, the PIM silent (IPv6) function is disabled on an interface.

Format

pim ipv6 silent

undo pim ipv6 silent

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the switch against pseudo PIM Hello (IPv6) messages sent from malicious hosts, configure the **pim ipv6 silent** command on the interface directly connected to the host network segment to set the interface to PIM silent (IPv6) mode. Then the interface cannot receive or forward any PIM (IPv6) packet, and all PIM (IPv6) neighbors and PIM (IPv6) state machines on this interface are deleted. This interface becomes the DR, but the MLD function on the interface is not affected.

The PIM silent (IPv6) function applies only to the interface directly connected to a host network segment, and only one PIM switch can be connected to this network segment.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

Running the **pim ipv6 silent** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If PIM BFD (IPv6) function is enabled on the interface, this command cannot be configured.

This command and **pim ipv6 timer dr-switch-delay** command are mutually exclusive.

NOTICE

After you run this command on an interface, the interface no longer receives or sends any PIM (IPv6) packets and other PIM (IPv6) functions on the interface become invalid. Confirm your action before using this command.

If a host network segment is connected to multiple switches and PIM silent (IPv6) is enabled on multiple interfaces, all these interfaces become static DRs. This causes multicast forwarding failures.

Example

Configure the PIM silent (IPv6) function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 silent
```

Configure the PIM silent (IPv6) function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 silent
```

8.4.60 pim ipv6 sm

Function

The **pim ipv6 sm** command enables PIM-SM (IPv6) on an interface.

The **undo pim ipv6 sm** command disables PIM-SM (IPv6).

By default, PIM-SM (IPv6) is disabled on an interface.

Format

pim ipv6 sm

undo pim ipv6 sm

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM-SM (IPv6) is enabled on interfaces, devices can set up PIM neighbor relationships with each other and process protocol packets received from PIM neighbors.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM-DM (IPv6) and PIM-SM (IPv6) cannot be enabled simultaneously on the device.

If PIM-SM (IPv6) and MLD need to be enabled on the same interface, enable PIM-SM (IPv6), and then enable MLD.

Running the **pim ipv6 sm** command failed on the VLANIF interface because Layer 2 multicast querier or report-suppress is enabled for this VLAN.

If both Layer 2 and Layer 3 multicast services are required in a VLAN, enable PIM (IPv6) on the corresponding VLANIF interface first, and then enable MLD snooping in the VLAN. If MLD snooping is enabled in the VLAN first, PIM (IPv6) cannot be enabled on the VLANIF interface.

Example

Enable PIM-SM (IPv6) on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 sm
```

Enable PIM-SM (IPv6) on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 sm
```

8.4.61 pim ipv6 state-refresh-capable

Function

The **pim ipv6 state-refresh-capable** command enables PIM-DM (IPv6) State-Refresh on an interface.

The **undo pim ipv6 state-refresh-capable** command disables PIM-DM (IPv6) State-Refresh.

By default, PIM-DM (IPv6) State-Refresh is enabled.

Format

pim ipv6 state-refresh-capable

undo pim ipv6 state-refresh-capable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM (IPv6) State-Refresh is implemented by periodically sending State-Refresh messages in the network. After receiving a State-Refresh message, the switch in the pruned state resets the prune-status timer, preventing the downstream interface from forwarding packets.

After PIM-DM (IPv6) state-refresh is disabled, the interface starts to forward multicast data when the prune timer expires. The downstream routers that do not require the data send Prune messages. The process repeats and wastes a lot of network resources. Enabling PIM-DM (IPv6) State-Refresh can reduce traffic on the network.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Disable PIM-DM (IPv6) State-Refresh on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo pim ipv6 state-refresh-capable
```

Disable PIM-DM (IPv6) State-Refresh on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo pim ipv6 state-refresh-capable
```

8.4.62 pim ipv6 timer dr-switch-delay

Function

The **pim ipv6 timer dr-switch-delay** command enables PIM DR switching delay and configures the delay on an interface. When the interface changed from a DR to a non-DR, the interface continues to forward data before the delay expires.

The **undo pim ipv6 timer dr-switch-delay** command disables PIM DR switching delay on the interface.

By default, when the interface changes from a DR to a non-DR, the interface stops forwarding data immediately.

Format

pim ipv6 timer dr-switch-delay *interval*

undo pim ipv6 timer dr-switch-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DR on a shared network segment becomes the non-DR, original multicast forwarding entries will be deleted immediately, causing multicast data interruption in a short time. To solve the problem, set the DR switching delay. Original multicast forwarding entries still take effect until the delay is reached.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

This command and **pim ipv6 silent** command are mutually exclusive.

Example

Enable PIM DR switching delay on VLANIF100 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
```

```
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer dr-switch-delay 20
```

Enable PIM DR switching delay on GE0/0/1 and set the delay to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer dr-switch-delay 20
```

8.4.63 pim ipv6 timer graft-retry

Function

The **pim ipv6 timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

The **undo pim ipv6 timer graft-retry** command restores the default value of the interval.

By default, the interval for retransmitting Graft messages on an interface is 3 seconds.

Format

pim ipv6 timer graft-retry *interval*

undo pim ipv6 timer graft-retry

Parameters

Parameter	Description	Value
interval	Specifies the interval of retransmitting Graft messages.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM (IPv6) mode, when a member joins a pruned group, the switch sends a Graft message and waits to receive an ACK message from the upstream switch. If the downstream switch does not receive the ACK message in the period configured through the command, the switch resends the Graft message until the switch receives the ACK message from the upstream switch.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Set the interval for retransmitting Graft messages to 80s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer graft-retry 80
```

Set the interval for retransmitting Graft messages to 80s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer graft-retry 80
```

8.4.64 pim ipv6 timer hello

Function

The **pim ipv6 timer hello** command sets the interval for sending Hello messages on an interface.

The **undo pim ipv6 timer hello** command restores the default value of the interval.

By default, the interval for sending Hello messages on an interface is 30 seconds.

Format

pim ipv6 timer hello *interval*

undo pim ipv6 timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim ipv6 timer hello** command to set the interval for sending Hello messages.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors. You can run the **pim ipv6 hello-option holdtime** command to set the timeout period of PIM neighbors.

The configuration is the same as the **timer hello (IPv6)** command in the PIM-IPv6 view. The configuration in the interface view takes precedence over the configuration in the PIM-IPv6 view. The value configured in the PIM-IPv6 view is used if no value is configured on the interface.

Example

Set the interval for sending Hello messages to 40 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer hello 40
```

Set the interval for sending Hello messages to 40 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer hello 40
```

8.4.65 pim ipv6 timer join-prune

Function

The **pim ipv6 timer join-prune** command sets the interval for periodically sending Join/Prune messages to the upstream device.

The **undo pim ipv6 timer join-prune** command restores the default interval.

By default, the interval for periodically sending Join/Prune messages to the upstream device is 60 seconds.

Format

pim ipv6 timer join-prune *interval*

undo pim ipv6 timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Join/Prune messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends join information to the upstream device, requesting the upstream device to forward multicast data. The device sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The device periodically sends Join/Prune messages to the upstream device to update the forwarding status.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval configured through this command must be shorter than the interval configured through the **pim ipv6 holdtime join-prune** command. The interval at which Join or Prune messages are sent must be shorter than the holdtime carried in Join/Prune messages.

The configuration is the same as that of the **timer join-prune (IPv6)** command in the PIM-IPv6 view. The system prefers the configuration in the interface view. The value configured in the PIM-IPv6 view is used if no value is configured on the interface.

Example

Set the interval for sending Join or Prune messages to 80 seconds on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 timer join-prune 80
```

Set the interval for sending Join or Prune messages to 80 seconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 timer join-prune 80
```

8.4.66 pim ipv6 triggered-hello-delay

Function

The **pim ipv6 triggered-hello-delay** command sets the maximum delay for triggering Hello messages.

The **undo pim ipv6 triggered-hello-delay** command restores the default maximum delay.

By default, the maximum delay for triggering Hello messages is 5 seconds.

Format

pim ipv6 triggered-hello-delay *interval*

undo pim ipv6 triggered-hello-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum delay for triggering Hello messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Conflicts will occur if multiple PIM devices sending Hello message at the same time. To avoid such conflicts, when a PIM device detects Hello messages on the network, it waits for a random delay that is smaller than the value configured using this command before sending a Hello message.

To avoid the conflict caused by multiple PIM devices sending Hello message at the same time, the PIM device automatically selects a random number smaller than the configured value as the delay. When detecting Hello messages in the network, the PIM device sends Hello message after the delay.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Example

Set the maximum delay for triggering the Hello message to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] pim ipv6 triggered-hello-delay 3
```

Set the maximum delay for triggering the Hello message to 3 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] pim ipv6 triggered-hello-delay 3
```

8.4.67 probe-interval (IPv6)

Function

The **probe-interval** command sets the interval for a switch to send Probe messages (null Register message) to the RP.

The **undo probe-interval** command restores the default value of the interval.

By default, the interval for a switch to send Probe messages to the RP is 5 seconds.

Format

probe-interval *interval*

undo probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Probe messages to RP.	The value is an integer that ranges from 1 to 1799, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving a Register-Stop message sent by the RP, the DR at the source side stops sending Register messages and enters the register suppression state.

During the register suppression, the DR at the source side sends Probe messages to notify the RP that the multicast source is still in the Active state. After the register suppression times out, the DR at the source side starts to send Register messages.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

The interval set using the **probe-interval** command must be less than half the interval set using the **register-suppression-timeout (IPv6)** command.

Example

In the PIM-IPv6 view, set the interval for sending Probe messages to RP to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] probe-interval 6
```

8.4.68 register-policy (IPv6)

Function

The **register-policy** command sets the rules used by an RP to filter Register messages.

The **undo register-policy** command restores the default setting.

By default, the rules for filtering Register messages are not configured.

Format

register-policy *advanced-acl6-number*

undo register-policy

Parameters

Parameter	Description	Value
advanced-acl6-number	Specifies the number of the advanced ACL that defines the rules for filtering packets based on source addresses or group addresses.	The value is an integer that ranges from 3000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of invalid Register messages, you can configure devices to receive or deny Register messages according to the packet filtering rules.

If the ACL rejects an (S, G) entry contained in a Register message or the ACL does not filter this entry, the RP sends a Register-Stop message to the DR on the source side to stop the registration of this multicast data stream.

The **register-policy** command and the **acl ipv6** command are used together. In the ACL6 view, you can set the multicast source address range by specifying the **source** parameter in the **rule** command, and set the multicast group address range by specifying the **destination** parameter in the **rule** command.

The configurations of the IPv6 Named ACL and the advanced ACL are the same, and can implement filtering of both source addresses and multicast group addresses. The Named ACL can also be configured with the **time-range** parameter.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

When the **register-policy** command is used on the RP, only Register messages matching the rule of the ACL are received by the RP. If an undefined ACL is specified, the RP denies all Register messages.

This command is valid for only PIM-SM (IPv6).

The **register-policy** command takes effect for only subsequently received Register messages. The multicast entries that have been registered successfully are not deleted and can still be used for multicast data forwarding.

Example

Configure the RP to receive Register packets sent by the multicast source on the network segment FC00:0:0:2001::2/64 to the multicast group FF02:13::/64.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 3000
[HUAWEI-acl6-adv-3000] rule permit ipv6 source fc00:0:0:2001::2 64 destination ff02:13:: 64
[HUAWEI-acl6-adv-3000] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] register-policy 3000
```

8.4.69 register-source (IPv6)

Function

The **register-source** command specifies the source IPv6 address used by the source's DR to send Register messages.

The **undo register-source** command restores the default setting.

By default, the source IPv6 address used by the source's DR to send Register messages is not specified.

Format

register-source *ipv6-address*

undo register-source

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of the registered source.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the source IPv6 address for sending Register messages is no longer the only IPv6 address in the network for the RP device or the source IPv6 address is filtered out, errors occur in the registration process and extra traffic occupies bandwidth on the network. In this case, use the **register-source** command to specify an appropriate interface as the source IPv6 address for sending Register messages. Using the loopback address of the source's DR as the source IPv6 address is recommended.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Before specifying the source IPv6 unicast address for sending Register messages, enable PIM-SM.

Precautions

The command is effective only when the specified interface is in Up state.

Example

Specify the source IPv6 address used by the source's DR to send Register message as FC00:0:0:1101::1.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] register-source fc00:0:0:1101::1
```

8.4.70 register-suppression-timeout (IPv6)

Function

The **register-suppression-timeout** command sets the timeout period during which a switch keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a switch keeps the register suppression state for 60 seconds.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the switch keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the switch immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the switch keeps the register suppression state. When the timeout period expires, the switch (source DR) starts to send Register messages to the RP.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid only for PIM-SM (IPv6).

If the timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, there will be a long delay for a new receiver to join a group when an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv6)** command to configure the switch to send null Register messages before the suppression timer times out. This configuration reduces burst Register messages and shortens the timeout period to reduce the delay for a new receiver to join a group.

Example

In the PIM-IPv6 view, set the timeout period during which the switch keeps the register suppression state to 70 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] register-suppression-timeout 70
```

8.4.71 reset pim ipv6 control-message counters

Function

The **reset pim ipv6 control-message counters** command resets the statistics about PIM (IPv6) control messages.

Format

reset pim ipv6 control-message counters [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the name and the number of an interface. It is used to reset the statistics about PIM (IPv6) control messages on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If an interface with PIM (IPv6) enabled has been forwarding multicast packets for a long time, the switch stores statistics on a large number of control messages. You can run this command to reset statistics on control messages.

Example

Reset the statistics about PIM (IPv6) control messages on all interfaces.

```
<HUAWEI> reset pim ipv6 control-message counters
```

8.4.72 reset pim ipv6 routing-table

Function

The **reset pim ipv6 routing-table** command clears PIM status of the specified downstream interface of a specified PIM (IPv6) entry.

Format

reset pim ipv6 routing-table group *ipv6-group-address* **mask** *ipv6-group-mask-length* **source** *ipv6-source-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
group *ipv6-group-address*	Specifies the group address of an IPv6 PIM entry.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Parameter	Description	Value
mask *ipv6-group-mask-length*	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 0 to 128.
source *ipv6-source-address*	Specifies the source address of an IPv6 PIM entry.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset pim ipv6 routing-table** command clears PIM status of the specified downstream interface of a specified PIM entry.

Configuration Impact

Using this command can clear the PIM status of the specified interface in a specified PIM entry. The command cannot be used to clear the MLD and static group join status on a specified interface.

Precautions

This command is valid for only PIM-SM (IPv6).

NOTICE

Clearing PIM status of the downstream interfaces can trigger sending of Join/Prune messages, which causes multicast service interruption.

Example

Clear PIM status of the downstream interface VLANIF100 of the (S, G) entry (FC00:0:0:2001::4,FF25::1).

```
<HUAWEI> reset pim ipv6 routing-table group ff25::1 mask 128 source fc00:0:0:2001::4 interface vlanif
100
```

8.4.73 source-lifetime (IPv6)

Function

The **source-lifetime** command specifies the timeout period of (S, G) entries on the switch.

The **undo source-lifetime** command restores the default value of the timeout period.

By default, the timeout period is 210 seconds.

Format

source-lifetime { *interval* | **infinity** } [**group-policy** *acl6-number*]

undo source-lifetime

undo source-lifetime { *interval* | **infinity** } [**group-policy** *acl6-number*]

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of (S, G) entries on the switch.	The value is an integer that ranges from 60 to 65535, in seconds.
infinity	Indicates that (S, G) entries on the switch will never age out.	-
group-policy	Specifies a group policy to determine to which the configured timeout period takes effect.	-
acl6-number	Specifies the number of a basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch creates a timer for each (S, G) entry. The **source-lifetime** command is used to set the value of the timer. After receiving a multicast packet from S, the interface resets the timer. If the timer times out, the (S, G) entry is considered invalid.

- If you configure **source-lifetime** *interval*, the configured timeout period applies to all (S, G) entries.
- If you configure **source-lifetime** *interval* { **group-policy** *acl6-number* }:
  - If you specify an advanced ACL name in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
  - If you specify a basic ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source addresses are permitted by the specified ACL.
  - If you specify an advanced ACL number in the command, the configured timeout period applies to the (S, G) entries in which the source and group addresses are permitted by the specified ACL.
- If you configure **source-lifetime infinity**, all (S, G) entries will never age out.
- If you configure **source-lifetime infinity** { **group-policy** *acl6-number* }:
  - If you specify an advanced ACL name in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.
  - If you specify a basic ACL number in the command, the (S, G) entries in which the source addresses are permitted by the specified ACL will never age out.
  - If you specify an advanced ACL number in the command, the (S, G) entries in which the source and group addresses are permitted by the specified ACL will never age out.

If you run this command multiple times for the same range of multicast forwarding entries and specify *interval* and **infinity** respectively in the commands, **infinity** takes precedence over *interval*.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Set the timeout period of (S, G) entries on the switch to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] source-lifetime 200
```

8.4.74 source-policy (IPv6)

Function

The **source-policy** command configures the switch to filter received multicast data packets based on source addresses or source/group addresses.

The **undo source-policy** command deletes the configuration.

By default, a switch does not filter received multicast data packets based on source addresses or source/group addresses.

Format

source-policy *acl6-number*

undo source-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies number of the basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the switch to filter received multicast data packets based on source addresses or source/group addresses.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

For the numbered ACL, the **source-policy** command and the **acl ipv6acl ipv6** command are used together.

- In the basic ACL6 view, you can set the source address range of multicast packets by specifying the **source** parameter in the **rule** command.
- In the advanced ACL6 view, you can set the source address range of multicast packets by specifying the **source** parameter in the **rule** command, and set the multicast group IPv6 address range by specifying the **destination** parameter in the **rule** command.

The configurations of the named ACL and advanced ACL are the same, and can filter both source addresses and group addresses. A named ACL can also be configured with the **time-range** parameter.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

In the public network instance, configure the switch to receive multicast data packets with the source address of FC00:0:0:3121::1 and to discard those with the source address of FC00:0:0:3121::2.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source fc00:0:0:3121::1 128
[HUAWEI-acl6-basic-2001] rule deny source fc00:0:0:3121::2 128
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] source-policy 2001
```

8.4.75 spt-switch-threshold (IPv6)

Function

The **spt-switch-threshold** command sets the rate threshold of the multicast packets when the DR at the member side joins the SPT.

The **undo spt-switch-threshold** command restores the default value.

By default, the system performs SPT switchover on receiving the first multicast data packet through the RPT.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** { *basic-acl6-number* } [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy** { *basic-acl6-number* }]

Parameters

Parameter	Description	Value
traffic-rate	Specifies the threshold rate for the switchover from the RPT to the SPT. **NOTE** Setting this parameter may affect operation of multicast services. You are advised to use the default triggering condition. That is, an SPT switchover is triggered immediately after the first multicast data packet is received from the RPT. The default triggering condition can reduce the number of multicast packets forwarded on the RPT.	The value is an integer that ranges from 1 to 4194304, in kbit/s.
infinity	Indicates that the SPT switchover is never enabled.	-

Parameter	Description	Value
basic-acl6-number	Specifies an entry of the group-policy list. It works with the multicast group that matches *basic-acl6-number* to enable the threshold. *basic-acl6-number* specifies the number of the basic ACL that defines the range of multicast groups.	If the parameter is not set, the threshold is applied to all multicast groups. The value ranges from 2000 to 2999.
order *order-value*	Adjusts the order of the ACLs in the group-policy list. If a group matches multiple ACLs, the threshold is selected in the order specified by *order-value*. *order-value* specifies the updated number.	The value is an integer. The value is any value other than original one in the current group-policy list. If the parameter is not set, the order of the ACLs in the group-policy list does not change.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source's DR encapsulates multicast packets in a Register message, and then transmits the unicast Register message to the RP. Then, the RP decapsulates the Register message and forwards the multicast packets to the receivers along the RPT. By default, when the RP or receiver's DR receives the first multicast packet, it initiates an SPT switchover to the source.

After the **spt-switch-threshold** command is executed on the receiver's DR, the receiver's DR periodically checks the forwarding rate of multicast packets. When the forwarding rate exceeds the threshold, the receiver's DR sends a Join messages to the source, triggering the SPT switchover.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If this command is used several times for the same group, the first matched command takes effect.

This command is valid to all devices that may function as the DR at the member side, but is invalid to RPs.

Precautions

This command is valid for only PIM-SM (IPv6).

Example

Set the threshold to 4 kbit/s. If the transmission rate of packets from the source to the multicast group is higher than the threshold, the switch switches packets to the SPT towards the source.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] spt-switch-threshold 4
```

Add a group-policy: the ACL number, rate threshold, and order of the group-policy are 2010, 100 kbit/s, and 1 respectively.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2010
[HUAWEI-acl6-basic-2010] rule permit source ff02:: 96
[HUAWEI-acl6-basic-2010] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] spt-switch-threshold 100 group-policy 2010 order 1
```

8.4.76 ssm-policy (IPv6)

Function

The **ssm-policy** command sets the range of SSM group addresses.

The **undo ssm-policy** command restores the default configuration.

By default, the range of IPv6 SSM group addresses is FF3x::/32. (The value of x ranges from 0 to F.)

Format

ssm-policy *basic-acl6-number*

undo ssm-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of the basic ACL that defines the range of SSM group addresses.	The value is an integer that ranges from 2000 to 2999.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the SSM group address range is FF3x::/32. The value of x ranges from 0 to F. You can run the **ssm-policy** command to specify the range of PIM SSM group addresses. All the PIM-SM (IPv6) interfaces consider that PIM SSM is enabled on all the multicast groups in the specified address range. The specified SSM group address range can exceed the default group address range.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If Multicast Listener Discovery version 2 (MLDv2) is used to add an (S, G) entry, this command does not take effect.

The **ssm-policy** command and the **acl ipv6acl ipv6** command are used together.

- For the numbered ACL6, in the ACL6 view, you can set the IPv6 address range of SSM multicast groups by specifying the **source** parameter in the **rule (basic ACL6 view)** command.
- For the named ACL6, in the ACL6 view, when the **rule (basic ACL6 view)** command is used to configure a filtering rule, the filtering rule is effective only with the multicast group address range that is specified by the **destination** parameter and with the time period that is specified by the **time-range** parameter.

This command is valid for only PIM-SM (IPv6).

Example

Set the range of PIM SSM multicast addresses to FF31:0:8192::/96.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule permit source ff31:0:8192:: 96
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] ssm-policy 2000
```

8.4.77 state-refresh-interval (IPv6)

Function

The **state-refresh-interval** command sets the interval for sending PIM State-Refresh messages.

The **undo state-refresh-interval** command restores the default value of the interval.

By default, the interval for sending PIM State-Refresh messages is 60 seconds.

Format

state-refresh-interval *interval*

undo state-refresh-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending PIM State-Refresh messages.	The value is an integer that ranges from 1 to 255, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-DM (IPv6) network, the device periodically sends State-Refresh messages to update the timeout interval of the prune timer on the downstream device. By doing this, the interface that has no multicast requirements retains in prune state.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

To prevent a pruned interface from forwarding packets when the Prune status times out, the interval for sending State-Refresh messages is shorter than the period for keeping the Prune status.

You can run the **holdtime join-prune (IPv6)** command to set the period during which the device keeps the Prune status.

This command takes effect only when it is run on the routers directly connected to the source.

Example

Set the interval for sending PIM State-Refresh messages to 70s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] state-refresh-interval 70
```

8.4.78 state-refresh-rate-limit (IPv6)

Function

The **state-refresh-rate-limit** command sets the minimum period to wait before receiving the next PIM State-Refresh message.

The **undo state-refresh-rate-limit** command restores the default value.

By default, the minimum period to wait to receive the next PIM State-Refresh message is 30 seconds.

Format

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

Parameters

Parameter	Description	Value
interval	Specifies the minimum period for waiting to receive the next PIM State-Refresh message.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch can receive multiple PIM State-Refresh messages in a short period. Some of the messages are the same. To avoid duplicate messages, you can run the **state-refresh-rate-limit** command to set the period to wait to receive the next State-Refresh message.

- Before the State-Refresh timer times out, the switch discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the switch can receive the next State-Refresh message.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Set the minimum period to wait to receive the next PIM State-Refresh message to 45s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] state-refresh-rate-limit 45
```

8.4.79 state-refresh-ttl (IPv6)

Function

The **state-refresh-ttl** command sets the TTL value for sending PIM State-Refresh messages.

The **undo state-refresh-ttl** command restores the default value of the TTL.

By default, the TTL value for sending PIM State-Refresh messages is 255.

Format

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Parameters

Parameter	Description	Value
ttl-value	Specifies the minimum TTL value of the PIM state refresh message sent by an interface.	The value is an integer that ranges from 1 to 255.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a State-Refresh message, the switch decreases the value of the TTL in the message by 1, and then sends the message to the downstream switch until the value of the TTL becomes 0. If the scale of the network is small, the message is delivered in a loop.

You can use the **state-refresh-ttl** command to set the value of the TTL according to the scale of the network.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

This command takes effect only when it is run on the routers directly connected to the source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] state-refresh-ttl 45
```

8.4.80 static-rp (IPv6)

Function

The **static-rp** command configures a static RP.

The **undo static-rp** command restores the default configuration.

By default, no static RP is configured.

Format

static-rp *rp-address* [*basic-acl6-number*] [**preferred**]

undo static-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Specifies address of a static RP.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
basic-acl6-number	Specifies the basic ACL that is used to control the range of multicast groups served by a static RP.	The value is an integer that ranges from 2000 to 2999.
preferred	Indicates that the static RP is preferred.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one RP exists in the network, you can manually configure a static RP rather than a dynamic RP. This can reduce bandwidth used to exchange information between the C-RP and the BSR.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If the address of the static RP is the address of an interface in the Up state on the local host, the local host acts as the static RP. PIM (IPv6) does not need to be enabled on the interface of the static RP.

If no ACL number is specified in the command, the static RP serves all the multicast groups. If an ACL is specified but the ACL does not contain any rules, the static RP serves all the multicast groups. If the specified ACL has rules configured, the static RP serves only the multicast groups permitted by the ACL.

If the command used to configure the static RP does not contain **preferred**, devices apply BSR mechanism to elect a dynamic RP. If the dynamic RP is not configured in the network or the dynamic RP is invalid, the static RP becomes valid. If the command used to configure static RP contains **preferred**, the static RP is preferred.

If this command is used many times, multiple static RPs are configured. In the case that multiple static RPs serve a group, the RP with the largest IPv6 address is selected to serve the group. If *rp-address* of the RPs is identical, the latest RP replaces the previous one.

Precautions

The **static-rp** command and the **acl ipv6** command are used together. In the ACL6 view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command. The filtering rule is effective only with the **source** parameter and the time period specified by the **time-range** parameter.

NOTE

Up to 50 static RPs can be configured by using this command repeatedly, but the same ACL cannot correspond to multiple static RPs. If the ACL is not referenced, only one static RP can be configured.

To make the static RP work normally, run the **static-rp** command on all devices in the PIM-SM (IPv6) domain.

Example

Configure the switch with the address of FC00:0:0:1111::1111 as the static RP in the PIM-SM (IPv6) domain.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] static-rp fc00:0:0:1111::1111
```

8.4.81 timer hello (IPv6)

Function

The **timer hello** command sets the interval at which the PIM switch sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM switch sends Hello messages is 30 seconds.

Format

timer hello *interval*

undo timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim ipv6 timer hello** command to set the interval for sending Hello messages.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval at which the PIM device sends Hello messages should be less than the timeout period of the PIM neighbor. You can run the **hello-option holdtime (IPv6)** command to set the timeout period of PIM neighbors.

The **timer hello** command has the same function as the **pim ipv6 timer hello** command in the interface view. By default, if the **pim ipv6 timer hello** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which PIM Hello messages are sent to 40s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] timer hello 40
```

8.4.82 timer join-prune (IPv6)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream device.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream device is 60 seconds.

Format

timer join-prune *interval*

undo timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Join/Prune messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch sends join information to the upstream device, requesting the upstream device to forward multicast data. The switch sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The PIM switch periodically sends Join/Prune messages to the upstream switch to update the forwarding status.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval configured using the **timer join-prune** command must be shorter than the interval configured using the **holdtime join-prune (IPv6)** command.

The **timer join-prune** command has the same function as the **pim ipv6 timer join-prune** command in the interface view. By default, if the **pim ipv6 timer join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which Join/Prune messages are sent to 80s.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] timer join-prune 80
```

8.4.83 timer spt-switch (IPv6)

Function

The **timer spt-switch** command sets the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT.

The **undo timer spt-switch** command restores the default value of the interval.

By default, the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT is 15 seconds.

Format

timer spt-switch *interval*

undo timer spt-switch

Parameters

Parameter	Description	Value
interval	Specifies the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from RPT to SPT.	The value is an integer that ranges from 15 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **timer spt-switch** command to set the interval for checking whether the rate for transmitting multicast data exceeds the threshold.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Before running this command, you must set the threshold for SPT switchover by using the **spt-switch-threshold (IPv6)** command; otherwise, the **timer spt-switch** command takes no effect.

Example

Set the interval for checking the rate for transmitting the multicast data before the switchover from RPT to SPT to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] pim-ipv6
[HUAWEI-pim6] timer spt-switch 30
```

8.5 MSDP Configuration Commands

8.5.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the MSDP multi-instance feature.

8.5.2 cache-sa-enable

Function

The **cache-sa-enable** command enables the SA cache function on a switch. After receiving an SA message, the switch caches (S, G) information carried in the SA message.

The **cache-sa-disable** command disables the SA cache function.

The **undo cache-sa-enable** command disables the SA cache function.

By default, the SA cache function is enabled on a switch.

Format

cache-sa-enable

cache-sa-disable

undo cache-sa-enable

Parameters

None

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch enabled with the SA cache function locally saves (S, G) information carried in the received SA messages. When the switch receives requests for receiving multicast data, it directly obtains (S, G) information from the SA cache.

A switch no longer saves (S, G) information carried in the received SA messages locally after the **undo cache-sa-enable** or the **cache-sa-disable** command is run to disable the SA cache function. When the switch receives requests for receiving multicast data, it must wait for the SA messages sent by the MSDP peer in the next sending period. This may result in a delay in receiving multicast data.

Prerequisites

MSDP has been enabled using the **msdp** command.

Configuration Impact

When an RP receives a new (*, G) Join message,

- If the SA cache function is enabled, the RP searches the SA cache for the (S, G) information.
  - If the SA cache contains related (S, G) information, the RP directly joins the SPT with the root being S.
  - If the SA cache does not contain related (S, G) information, the RP does not process the received Join message.
- If the SA cache function is disabled, the RP processes the message in one of the following ways:
  - If the sending of SA Request messages is enabled, the RP sends an SA Request message to the specified MSDP peer and waits for the response.
  - If the sending of SA Request messages is disabled, the RP must wait for the SA message sent by the MSDP peer in the next sending period.

Precautions

The **cache-sa-disable** and **undo cache-sa-enable** commands' configurations are both **undo cache-sa-enable** in the configuration file.

Example

Disable the SA cache function on the switch.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] undo cache-sa-enable
```

8.5.3 display default-parameter msdp

Function

The **display default-parameter msdp** command displays default configurations about MSDP.

Format

display default-parameter msdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command still displays the default configurations even after the MSDP parameters are changed. You can use this command to check the consistency of default configurations about MSDP parameters on MSDP peers.

Example

Display default configurations about MSDP.

```
<HUAWEI> display default-parameter msdp
  MSDP View Default Configurations:
  ---------------------------------
  Cache-sa-enable: enabled
  Msdp description:
  Encap-data-enable: disabled
  Request-sa-enable: disabled
  Sa-request-policy: disabled
  Sa-policy: disabled
  Connect-retry-period: 30 s
  Minimum TTL: 0
```

Table 8-72 Description of the **display default-parameter msdp** command output

Item	Description
MSDP View Default Configurations	Default configurations in the MSDP view.

Item	Description
Cache-sa-enable	Whether SA cache is enabled. By default, SA cache is enabled. This parameter is configured using the **cache-sa-enable** command.
Msdp description	Whether MSDP peer description is configured. By default, no description is configured for an MSDP peer. This parameter is configured using the **peer description (MSDP)** command.
Encap-data-enable	Whether encapsulating multicast data packets into the SA message is enabled. By default, an SA message does not encapsulate any multicast packet. This parameter is configured using the **encap-data-enable** command.
Request-sa-enable	Whether sending an SA Request message immediately when a Join message is received. By default, when receiving a Join message, the switch waits for the SA message in the next period instead of sending an SA Request message to its MSDP peer. This parameter is configured using the **peer request-sa-enable** command.
Sa-request-policy	Whether the filtering rule for responding to the SA Request message is configured. By default, the switch is not configured with any filtering rule for responding to the SA Request message and responds to all SA Request messages from all MSDP peers. This parameter is configured using the **peer sa-request-policy** command.
Sa-policy	Whether the filtering rule for receiving or forwarding the SA message is configured. By default, the switch does not filter the received or forwarded SA messages. This parameter is configured using the **peer sa-policy** command.

Item	Description
Connect-retry-period	Interval for retrying to set up a TCP connection between MSDP peers. By default, the interval for retrying to set up an MSDP peer relationship is 30 seconds. This parameter is configured using the **timer retry** command.
Minimum TTL	TTL value of SA messages that are encapsulated with multicast data. By default, the TTL value of SA messages that are encapsulated with multicast data is 0. This parameter is configured using the **peer minimum-ttl** command.

8.5.4 display msdp brief

Function

The **display msdp brief** command displays summary information about the status of MSDP peers.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
state	Displays summary information about the MSDP peers in specified status.	-
connect	Indicates the MSDP peers in Connect state.	-

Parameter	Description	Value
down	Indicates the MSDP peers in Down state.	-
listen	Indicates the MSDP peers in Listen state.	-
shutdown	Indicates the MSDP peers in Shutdown state.	-
up	Indicates the MSDP peers in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MSDP peers establish a TCP connection, the **display msdp brief** command can be used to display the brief information about the remote MSDP peer, such as the address, AS number, the number of (S, G) entries, and the status of the TCP connection.

Precautions

This command displays summary information about the status of MSDP peers only when the MSDP peer has been configured.

MSDP specifies that the peer with the higher IP address acts as the server and listens at port 639. The peer with the lower IP address acts as client and enables the connection. If the connection fails, the client enables the connection again.

Example

Display summary information about MSDP peers.

```
<HUAWEI> display msdp brief
MSDP Peer Brief Information
  Configured   Up          Listen      Connect     Shutdown     Down
  2            2           0           0           0            0

  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.3.2        Up        01:07:08        ?      8          0
  192.168.5.1        Up        00:16:39        ?      13         0
```

Table 8-73 Description of the **display msdp brief** command output

Item	Description
MSDP Peer Brief Information	summary information about MSDP peers.
Configured	Total number of configured MSDP peers.
Up	Number of MSDP peers in Up state.
Listen	Number of MSDP peers in Listen state.
Connect	Number of MSDP peers in Connect state.
Shutdown	Number of MSDP peers in Shutdown state.
Down	Number of MSDP peers in Down state.
Peer's Address	Address of the peer. This parameter is configured using the **peer connect-interface (MSDP)** command.
State	Status of the MSDP session. ● Up: The connection is set up and is in Up state. ● Listen: The local device acts as the server and is in Listen state. The connection is not set up. ● Connect: The local device acts as the client and is in Connect state. The connection is not set up. ● Shutdown: The MSDP peer is in Shutdown state. ● Down: The connection fails.
Up/Down time	Time when the session becomes Up or Down. The time format is as follows: ● Time that is shorter than or equal to 24 hours: hour: minute: second. ● Time that is longer than 24 hours but shorter than or equal to one week: day: hour. ● Time that is longer than one week: week: day.
AS	The AS number of the MSDP peer. A question mark (?) indicates that the AS number cannot be obtained.
SA Count	Number of (S, G) entries in the SA cache.
Reset Count	Resetting times, including the resetting because the Notification message is received or Holdtimer times out.

8.5.5 display msdp control-message counters

Function

The **display msdp control-message counters** command displays statistics about MSDP messages.

Format

display msdp control-message counters [**peer** *peer-address* | **message-type** { **source-active** | **sa-request** | **sa-response** | **keepalive** | **notification** | **traceroute-request** | **traceroute-reply** | **data-packets** | **unknown-type** }] *

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies IP address of MSDP peer. If **peer** *peer-address* is specified, only statistics about the MSDP messages received, sent, and discarded on a specified MSDP peer are displayed.	The value is in dotted decimal notation.
message-type	Specifies MSDP message types. If **message-type** is specified, only statistics about the MSDP messages received, sent, and discarded of a specified type are displayed.	-
source-active	Displays the statistics about Source-Active messages on the interface.	-
sa-request	Displays the statistics about Source-Active Request messages on the interface.	-
sa-response	Displays the statistics about Source-Active Response messages on the interface.	-
keepalive	Displays the statistics about KeepAlive messages on the interface.	-
notification	Displays the statistics about Notification messages on the interface.	-
traceroute-request	Displays the statistics about Traceroute Request messages on the interface.	-
traceroute-reply	Displays the statistics about Traceroute Reply messages on the interface.	-
data-packets	Displays the statistics about data packets on the interface.	-

Parameter	Description	Value
unknown-type	Displays the statistics about unknown type messages on the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command helps you learn MSDP running status by displaying statistics about received, sent, and discarded MSDP messages.

Precautions

This command displays statistics about MSDP messages only when the MSDP peer has been configured.

Example

Display statistics about the MSDP messages that are received, sent, and discarded by the peer 192.168.3.3.

```
<HUAWEI> display msdp control-message counters peer 192.168.3.3
 MSDP message counters for peer: 192.168.3.3
                         Received        Sent            Invalid
 Source-Active              0              0               0
 Source-Active Request      0              0               0
 Source-Active Response     0              0               0
 KeepAlive                 48             49               0
 Notification               0              1               0
 Traceroute Request         0              -               -
 Traceroute Reply           0              -               -
 Data Packets               0              0               0
 Unknown Type               1              -               1
```

Table 8-74 Description of the **display msdp control-message counters peer 192.168.3.3** command output

Item	Description
MSDP message counters for peer	IP addresses of MSDP peers.
Received	Number of received messages.
Sent	Number of sent messages.
Invalid	Number of invalid messages.

Item	Description
Source-Active	Source-Active message: carries multiple (S, G) entries and is transmitted among several RPs; encapsulates PIM-SM multicast data.
Source-Active Request	Source-Active Request message: requests (S, G) list of a specified group G to reduce the delay in joining the group.
Source-Active Response	Source-Active Response message: responds to SA request messages.
KeepAlive	Keepalive message: maintains MSDP peer connections. Keepalive packets are sent only when no other protocol packets are exchanged between MSDP peers.
Notification	Notification message.
Traceroute Request	Traceroute Request message: traces and detects the RPF path along which SA messages are transmitted.
Traceroute Reply	Traceroute Reply message: traces and detects the RPF path along which SA messages are transmitted.
Data Packets	Data packets.
Unknown Type	Unknown type message.

8.5.6 display msdp invalid-packet

Function

The **display msdp invalid-packet** command displays statistics about invalid MSDP messages received by a device and details of these messages.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**peer** *peer-address* | **message-type** { **keepalive** | **notification** | **sa-request** | **sa-response** | **source-active** }] *

display msdp invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid MSDP messages received in all VPN instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
peer *peer-address*	Displays statistics about invalid MSDP messages received from a specified peer. *peer-address* specifies an MSDP peer address.	The address is in dotted decimal notation.
message-type	Displays statistics about invalid MSDP messages of a specific type.	-
keepalive	Displays statistics about invalid Keepalive messages.	-
notification	Displays statistics about invalid Notification messages.	-
sa-request	Displays statistics about invalid Source-Active Request messages.	-
sa-response	Displays statistics about invalid Source-Active Response messages.	-
source-active	Displays statistics about invalid Source-Active messages.	-
packet-number	Displays details about a specified number of invalid MSDP messages recently received. If this parameter is not specified, details about all invalid MSDP messages.	The value is an integer that ranges from 1 to 100.
verbose	Displays details about invalid MSDP messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display msdp invalid-packet** command to view statistics and details of invalid MSDP messages for fault location and rectification.

If MSDP peer relationships fail to be set up on a multicast network, you can run the **display msdp invalid-packet** command first to check whether devices have received invalid MSDP messages. If the command output contains statistics about invalid MSDP messages, run the **display msdp invalid-packet** [*packet-number*] **verbose** command to view details of invalid MSDP messages to locate the fault.

You can run the following related commands to view information about specific invalid MSDP messages:

- Run the **display msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** command to view statistics about invalid MSDP messages received in a specified VPN instance or in all VPN instances.
- Run the **display msdp invalid-packet peer** *peer-address* command to view statistics about invalid MSDP messages received from a specified peer.
- Run the **display msdp invalid-packet** *packet-number* **verbose** command to view details of invalid MSDP messages recently received. Currently, details of a maximum of 100 invalid MSDP messages can be displayed.

Example

Display statistics about invalid MSDP messages received by a device.

```
<HUAWEI> display msdp invalid-packet peer 192.168.1.1

            Statistics of invalid packets for public net:
-------------------------------------------------------------------
MSDP SA invalid packet:
Fault Length            : 0           Bad Length-x            : 0
Bad Sprefix             : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Encap Data          : 0
Illegal RP Addr         : 0           RP Loop                 : 0

MSDP SA Response invalid packet:
Fault Length            : 0           Bad Length-x            : 0
Bad Sprefix             : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Illegal RP Addr         : 0
RP Loop                 : 0

MSDP SA Request invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0

MSDP Keep Alive invalid packet:
Fault Length            : 0

MSDP Notification invalid packet:
Fault Length            : 0
-------------------------------------------------------------------
```

Table 8-75 Description of the **display msdp invalid-packet peer 192.168.1.1** command output

Item	Description
Statistics of invalid packets for public net	Statistics about invalid MSDP messages in the public network instance.

Item	Description
MSDP SA invalid packet	Invalid Source-Active messages.
Fault Length	Messages with invalid lengths.
Bad Length-x	Messages with invalid Length-x fields.
Bad Sprefix	Messages with invalid Sprefix fields.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Bad Encap Data	Messages with invalid data encapsulated.
Illegal RP Addr	Messages with illegal Rendezvous Point addresses.
RP Loop	Messages whose Rendezvous Point addresses are local addresses.
MSDP SA Response invalid packet	Invalid Source-Active Response messages.
MSDP SA Request invalid packet	Invalid Source-Active Request messages.
MSDP Keep Alive invalid packet	Invalid Keepalive messages.
MSDP Notification invalid packet	Invalid Notification messages.

Display details of a specific invalid MSDP message recently received.

```
<HUAWEI> display msdp invalid-packet 1 verbose
       Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Peer                :  10.2.2.2
Time                :  2010-6-9 11:25:46 UTC-08:00
Message Length      :  22
Invalid Type        :  Invalid Addr List
0000: 00 01 00 02 00 69 00 13 00 04 00 00 00 64 00 02
0010: 00 04 81 f4 09 c4
-----------------------------------------------------
```

Table 8-76 Description of the **display msdp invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details about invalid MSDP messages.

Item	Description
Packet information (Index 1)	Sequence number of the invalid MSDP message (numbered in the opposite order that the message is received, for example, the index of the last received message is 1, the index of the last but one message is 2, and so on).
Peer	IP address of the peer that sends the invalid MSDP message.
Time	Time when the invalid MSDP message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid MSDP message.
Invalid Type	Type of the invalid MSDP message.
0000: 00 01 00 02 00 69 00 13 00 04 00 00 00 64 00 02 0010: 00 04 81 f4 09 c4	Contents of the invalid MSDP message.

8.5.7 display msdp peer-status

Function

The **display msdp peer-status** command displays the detailed information about MSDP peers.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer-status** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
peer-address	Specifies the address of a remote MSDP peer. If this parameter is not specified, information about all the MSDP peers in the instance is displayed.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MSDP peers establish a TCP connection, the **display msdp peer-status** command can be used to display the detailed information about a specified MSDP peer, such as the interface status, interface configuration, policy for filtering messages, and number of messages.

Precautions

This command displays the detailed information about a specified MSDP peer only when the MSDP peer has been configured.

Example

Display the detailed information about the MSDP peer 10.110.11.11.

```
<HUAWEI> display msdp peer-status 10.110.11.11
 MSDP Peer 10.110.11.11, AS 100
 Description:
 Information about connection status:
   State: Up
   Up/down time: 14:41:08
   Resets: 0
   Connection interface: LoopBack0 (10.110.11.22)
   Number of sent/received messages: 867/947
   Number of discarded output messages: 0
   Elapsed time since last connection or counters clear: 14:42:40
```

```
Information about (Source, Group)-based SA filtering policy:
  Import policy: none
  Export policy: none
  Local Export policy: none
Information about SA-Requests:
  Policy to accept SA-Request messages: none
  Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA-cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 0/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
Peer authentication: unconfigured
Peer authentication type: none
```

Table 8-77 Description of the **display msdp peer-status** command output

Item	Description
MSDP Peer	Address of the peer. This parameter is configured using the **peer connect-interface (MSDP)** command.
AS	AS number of the MSDP peer. A question mark (?) indicates that the AS number cannot be obtained.
Description	Description of the verbose information.
Information about connection status	Information of connection status.
State	Status of the MSDP session. ● Up: The connection is set up and is in the Up state. ● Listen: The local device acts as the server. The connection is not set up. ● Connect: The local device acts as the client. The connection is not set up. ● Shutdown: The MSDP peer is in Shutdown state. ● Down: The connection fails.
Up/down time	Time when the session becomes Up or Down. The time format is as follows: ● Time that is shorter than or equal to 24 hours: hour: minute: second. ● Time that is longer than 24 hours but shorter than or equal to one week: day: hour. ● Time that is longer than one week: week: day.
Resets	Resetting times.

Item	Description
Connection interface	Address of a connect-interface that is used to set up the TCP connection with the peer address. This parameter is configured using the **peer connect-interface (MSDP)** command.
Number of sent/ received messages	Number of MSDP messages received or sent through the connection.
Number of discarded output messages	Number of discarded messages.
Elapsed time since last connection or counters clear	Time that elapsed since the MSDP peer resetting count and control packet statistics were reset.
Information about (Source, Group)-based SA filtering policy	- Import policy: is used to receive the filtering list of the SA messages of a specified MSDP peer. You can configure the policy using the **peer sa-policy import** command. - Export policy: is used to forward the filtering list of the SA messages of a specified MSDP peer. You can configure the policy using the **peer sa-policy export** command. - Local Export policy: is used to send the policy of locally created SA messages tof a specified MSDP peer. You can configure the policy using the **peer sa-policy local-export** command. By default, a device accepts all SA messages from MSDP peers, sends all locally created SA messages to MSDP peers, and forwards all SA messages to MSDP peers.
Information about SA-Requests	- Policy to accept SA-Request messages: restricts the SA request messages received from an MSDP peer by the switch. By default, the switch receives all the SA Request messages sent by the MSDP peer. The item is expressed by none. You can set the policy using the **peer sa-request-policy** command. - Sending SA-Requests status: enables or disables the switch to send SA request messages to a specified MSDP peer when the switch receives a Join message. By default, when receiving a Join message, the switch does not send the SA Request message to its MSDP peers, but waits for the next SA message. You can configure the switch to send SA Request messages using the **peer request-sa-enable** command.

Item	Description
Minimum TTL to forward SA with encapsulated data	If the SA message received is encapsulated with the multicast data packet, the switch forwards the SA message to other peers only when the TTL of the packet is not smaller than the minimum TTL. You can configure the function using the **peer minimum-ttl** command.
SAs learned from this peer	SA messages that pass through the MSDP peer and the number of SA entries in the cache.
SA-cache maximum for the peer	Maximum number of (S, G) entries in the cache when the switch receives the SA message from an MSDP peer. You can configure the maximum number of (S, G) entries in the cache using the **peer sa-cache-maximum** command.
Input queue size	Length of the data in the input cache.
Output queue size	Length of the data in the output cache.
Counters for MSDP message	Number of MSDP messages. ● Count of RPF check failure: indicates the number of SA messages discarded because of the RPF check failure. ● Incoming/outgoing SA messages: indicates the number of sent or received SA messages. ● Incoming/outgoing SA requests: indicates the number of sent or received SA-Request messages. ● Incoming/outgoing SA responses: indicates the number of sent or received SA-Response messages. ● Incoming/outgoing data packets: indicates the number of sent or received SA messages that are encapsulated with multicast data packets.
Peer authentication	Whether MSDP authentication is configured.
Peer authentication type	MSDP authentication modes, including: ● none: indicates authentication is not configured. ● MD5: indicates MD5 authentication. This parameter is configured using the **peer password (MSDP)** command. ● Keychain: indicates Keychain authentication. This parameter is configured using the **peer keychain (MSDP)** command.

8.5.8 display msdp rpf-peer

Function

The **display msdp rpf-peer** command displays information about all RPF peers of a specific source RP address, including RPF peer selection rules and RPF route types.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-peer original-rp** *original-rp-address*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Displays information about all the RPF peers of a specific source's RP address in all instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
original-rp *original-rp-address*	Displays information about all the RPF peers of a specific source's RP address. *original-rp-address* specifies the source's RP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To prevent looping of SA messages between MSDP peers, MSDP peers perform RPF checks on received SA messages and drop the SA messages that do not comply with RPF rules.

The **display msdp rpf-peer** command is used to check whether the forwarding path of SA messages works properly. Based on the RPF peer information in the command output, you can check every hop in the forwarding path. If the forwarding path is not working properly, this command helps you locate the faulty node.

Precautions

A device does not perform RPF checks on the SA messages received from an MSDP peer in the following situations:

- The address of the MSDP peer is the RP address of the source.
- The MSDP peer is a static RPF peer of the device.
- The MSDP peer is a unique MSDP peer of the device.
- The MSDP peer has joined a full-mesh group.

Before configuring this command, ensure that MSDP peers are configured. Only the MSDP peers with Up TCP connection can become RPF peers.

Example

Display information about RPF peers of the source RP 192.168.4.5.

```
<HUAWEI> display msdp rpf-peer original-rp 192.168.4.5
MSDP RPF peer information
 MSDP RPF peer information for Original RP: 192.168.4.5
 01. RPF peer: 10.6.6.6
  RPF selection rule: Peer is IGP next hop of best route
  RPF used topology: default
  RPF route type: multicast(static)
```

Table 8-78 Description of the **display msdp rpf-peer original-rp** command output

Item	Description
MSDP RPF peer information	information about the MSDP RPF peer.
MSDP RPF peer information for Original RP	Information about the MSDP RPF peer of a specific source's RP address.
01. RPF peer	RPF peer address.

Item	Description
RPF selection rule	RPF peer selection rule: ● Peer is IGP next hop of best route: RPF peer is a next hop of an IGP route. ● Peer is IGP advertiser of best route: RPF peer is a forwarder of an IGP route. ● Peer is in the AS-path to original RP: RPF peer is on an AS-path to the RP address of the source. ● Peer is BGP/MBGP next hop of best route: RPF peer is a next hop of a/an BGP/MBGP route. ● Peer is BGP/MBGP advertiser of best route: RPF peer is a forwarder of a/an BGP/MBGP route.
RPF used topology	RPF used topology: ● default: default topology. ● multicast: multicast topology. ● topology name (user-defined): unicast topology.
RPF route type	RPF route type: ● mbgp: MBGP route. ● unicast(bgp): BGP route ● multicast(static): static multicast route. ● unicast: IGP route (unicast route).

8.5.9 display msdp sa-cache

Function

The **display msdp sa-cache** command displays (S, G) entries in the SA cache.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address* | *source-address* | [*as-number-plain* | *as-number-dot*]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
group-address	Specifies the group address of an (S, G) entry. It is used to display the corresponding (S, G) of the group in SA Cache.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
source-address	Specifies the source address of an (S, G) entry. It is used to display the corresponding the (S, G) of the source.	The value is in dotted decimal notation.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the SA cache function is enabled, the **display msdp sa-cache** command can be used to display the information about (S, G) entries learned from other MSDP peers in the SA cache. The information includes the source address, group address, address of the source's RP, routing protocol, AS number, and timeout period of entries.

Precautions

This command displays (S, G) entries in the SA cache only when SA cache is enabled (default setting).

Example

Display (S, G) entries in the SA cache.

```
<HUAWEI> display msdp sa-cache
MSDP Source-Active Cache Information
 MSDP Total Source-Active Cache - 2 entries
 MSDP matched 2 entries

(10.0.5.120, 225.0.0.1)
 Origin RP: 3.3.3.3
 Pro: ?, AS: ?
 Uptime: 00:01:01, Expires: 00:05:59

(10.0.5.120, 225.0.0.2)
 Origin RP: 3.3.3.3
 Pro: ?, AS: ?
 Uptime: 00:00:01, Expires: 00:05:59
```

Table 8-79 Description of the **display msdp sa-cache** command output

Item	Description
MSDP Source-Active Cache Information	MSDP SA cache.
MSDP Total Source-Active Cache - 2 entries	Two entries are cached by MSDP SA.
MSDP matched 2 entries	Two entries are matched by MSDP, such as the filtering policy and specified source/group address.
(10.0.5.120, 225.0.0.1)	(source address, group address) entry in the SA cache.
Origin RP	Source RP address that advertises the (S, G) entry.
Pro	Type of the protocol from which the AS number of the source RP is obtained. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.
AS	AS number of the source RP. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.
Uptime	Time when the (S, G) entry is created in the cache.

Item	Description
Expires	Time when the (S, G) entry in the cache times out.

8.5.10 display msdp sa-count

Function

The **display msdp sa-count** command displays statistics about the (S, G) entries in the SA cache.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-count** [*as-number-plain* | *as-number-dot*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the SA cache function is enabled, the **display msdp sa-count** command can be used to display the statistics about the (S, G) entries in the SA cache, including the addresses of the peers that send SA messages and the (S, G) entry statistics collected according to the AS numbers of sources' RPs.

Precautions

This command displays the number of (S, G) entries in the SA cache only when the MSDP peer has been enabled with SA cache (default setting).

Example

Display the number of (S, G) entries in the SA cache.

```
<HUAWEI> display msdp sa-count
MSDP Source-Active Count Information
  Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5

  Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                   3

  Total 5 Source-Active entries matched
```

Table 8-80 Description of the **display msdp sa-count** command output

Item	Description
MSDP Source-Active Count Information	Number of MSDP SA messages.
Number of cached Source-Active entries, counted by Peer	Number of the (S, G) entries that are cached according to peers.
Peer's Address	Address of the peer that sends the SA message.
Number of SA	Number of the (S, G) entries received from the peer.
Number of source and group, counted by AS	Number of the (S, G) entries that is counted according to the AS to which the source RP belongs.
AS	AS number of the source RP. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.

Item	Description
Number of source	Number of sources in the AS. **NOTE** If **0** is displayed in the **Number of source** and **Number of group** fields, the local device does not receive SA messages from its MSDP peer. Contact technical support personnel to troubleshoot faults.
Number of group	Number of groups in the AS.
Total 5 Source-Active entries matched	Number of (S, G) entries matching specified conditions in the cache.

8.5.11 encap-data-enable

Function

The **encap-data-enable** command enables the device to encapsulate a multicast data packet into an SA message.

The **undo encap-data-enable** command disables the device from encapsulating a multicast data packet into an SA message.

By default, no multicast data packet is encapsulated into an SA message.

Format

encap-data-enable

undo encap-data-enable

Parameters

None

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source RP encapsulates information about all active sources into multiple SA messages to advertise it. Each SA message contains multiple (S, G) entries.

After the **encap-data-enable** command is configured on the source's RP, the RP encapsulates the multicast data carried in the Register message into an SA message, and then sends the SA message to the MSDP peer. Only one multicast data packet can be encapsulated into an SA message.

After the **encap-data-enable** command is configured on the MSDP peer, the switch can transmit the SA messages carrying a multicast data packet between PIM-SM domains.

Prerequisites

MSDP has been enabled using the **msdp** command.

Example

Encapsulate a multicast data packet into an SA message

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] encap-data-enable
```

8.5.12 import-source

Function

The **import-source** command prevents the information about active sources in a domain from being advertised when an SA message is created.

The **undo import-source** command restores the default configuration.

By default, the information about all active sources is advertised in a domain through SA messages.

Format

import-source [**acl** *acl-number*]

undo import-source

Parameters

Parameter	Description	Value
acl	Indicates the ACL that controls which source is to be advertised to a domain through an SA message and to which groups the SA message is to be advertised. If this parameter is not specified, multicast sources are not advertised.	-
acl-number	Specifies the number of the basic ACL or advanced ACL. ● Basic ACL: filters source addresses. ● Advanced ACL: filters source addresses and multicast group addresses.	The value is an integer that ranges from 2000 to 3999.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **import-source** command is used to filter (S, G) forwarding entries to be advertised in SA messages based on source addresses. This configuration controls transmission of information about multicast sources.

You can also run the **peer sa-policy** command to filter the SA messages to be forwarded.

The **import-source** command takes effect for all peers. If both the **import-source** and **peer** *peer-address* **sa-policy local-export** commands are run, the parameters configured in the **peer** *peer-address* **sa-policy local-export** command take effect preferentially.

Prerequisites

MSDP has been enabled using the **msdp** command.

Precautions

The **import-source** and **acl** commands are used together.

- In the basic ACL view, set the source address range of advertised multicast packets using SA messages by specifying the **source** parameter in the **rule** command.
- In the advanced ACL view, set the source address range of advertised multicast packets using SA messages by specifying the **source** parameter in the **rule** command, and set the address range of advertised multicast groups using SA messages by specifying the **destination** parameter in the **rule** command.

Example

Configure an MSDP peer to advertise the information about a specified active source when creating SA messages. The multicast source is on 10.10.0.0/16 network segment, and the multicast group address is 225.1.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] acl number 3101
[HUAWEI-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3101] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] import-source acl 3101
```

8.5.13 msdp

Function

The **msdp** command enables MSDP and displays the MSDP view in the public network instance or the VPN instance.

The **undo msdp** command clears all configurations in the MSDP view, releases the resources occupied by MSDP, and restores the initial state.

By default, MSDP is disabled.

Format

msdp [**vpn-instance** *vpn-instance-name*]

undo msdp [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MSDP, you can run the **msdp** command to enable MSDP and display the MSDP view. All the configurations related to MSDP peers must be done in the MSDP view.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command.

Configuration Impact

Running the **undo msdp** command interrupts MSDP services. Therefore, use this command with caution.

Example

Enable MSDP and enter the MSDP view.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp]
```

8.5.14 originating-rp

Function

The **originating-rp** command configures an RP to replace the source RP address in the SA message with an IP address of a specified interface when the RP constructs an SA message. This interface is also called a logical RP.

The **undo originating-rp** command restores the default configuration.

By default, the source RP address in an SA message is the address of the RP that actually sends the SA message.

Format

originating-rp *interface-type interface-number*

undo originating-rp

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface that functions as a logical RP.	-

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You must run this command when configuring anycast RP in a PIM-SM domain.

An MSDP peer performs the RPF check on a received SA message and then discards the message if the addresses of the local RP and the remote RP are the same. In anycast RP, however, you need to configure RPs on two or more devices in a PIM-SM domain, assign the same IP address to these RPs, and set up MSDP peer relationships between these devices. You must configure an address that is different from the actual RP address for the logical RP so that the SA message can pass the RPF check.

Prerequisites

MSDP has been enabled using the **msdp** command.

Precautions

The interface functioning as a logical RP cannot be an actual RP interface. Commonly, the interfaces setting up an MSDP peer relationship can be specified as logical RP addresses.

Example

Configure VLANIF100 as the logical RP for the SA message.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] originating-rp vlanif 100
```

8.5.15 peer connect-interface (MSDP)

Function

The **peer connect-interface** command configures an MSDP peer.

The **undo peer** command removes the configured MSDP peer.

By default, no MSDP peer is configured.

Format

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a remote MSDP peer.	The address is in dotted decimal notation.
interface-type interface-number	Specifies the type and the number of the interface. The local switch uses the primary address of the interface as the source IP address to set up the TCP connection with the remote MSDP peer.	-

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP peers are identified by addresses. You can run the **peer connect-interface** command on two devices to specify the peer addresses for each other and specify interfaces for establishing the TCP connection. In this way, an MSDP peer connection is established.

Prerequisites

MSDP has been enabled using the **msdp** command.

Configuration Impact

You can run the **peer** *peer-address* **connect-interface** *interface-type interface-number* command repeatedly to configure multiple MSDP peers for the local switch.

- You can specify the same *interface-type interface-number* for different *peer-address*. That is, you can specify the same local interface for different remote peers.
- You can specify different *interface-type interface-number* for different *peer-address*. That is, you can specify different local interfaces for different remote peers.

Precautions

Run the **peer connect-interface** command before running other peer commands. Otherwise, the system displays a message indicating that the peer does not exist.

When configuring a static RPF peer, you need to first run the **peer connect-interface** command to set the remote end as an MSDP peer and then the **static-rpf-peer** command to set the MSDP peer as a static RPF peer.

Example

Configure IP address 10.10.7.6 for the remote MSDP peer and specify VLANIF100 as the local interface.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
```

8.5.16 peer description (MSDP)

Function

The **peer description** command adds the description text for an MSDP peer.

The **undo peer description** command restores the default configuration.

By default, an MSDP peer does not have the description text.

Format

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
text	Specifies the description text.	The description text is a string of 1 to 80 case-sensitive characters.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple MSDP peers are configured on the network, the MSDP peers cannot be easily distinguished only by IP addresses. The administrator can distinguish the MSDP peers by setting the descriptions for them.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Add a description **ClientA** for the MSDP peer with the IP address being 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 description ClientA
```

8.5.17 peer keychain (MSDP)

Function

The **peer keychain** command configures keychain authentication for establishing a TCP connection between MSDP peers and transmitting MSDP message.

The **undo peer keychain** command removes keychain authentication between MSDP peers.

By default, MSDP keychain authentication is not configured.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

peer *peer-address* **keychain** *keychain-name*

undo peer *peer-address* **keychain**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The value is in dotted decimal notation.
keychain-name	Specifies the name of the keychain. This parameter is set using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP supports MD5 authentication and keychain authentication that improve security on TCP connections between MSDP peers. Keychain authentication supports multiple algorithms and is more suitable than MD5 authentication for networks that require high security.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

A keychain in accordance with the configured *keychain-name* has been enabled using the **keychain** command; otherwise, the TCP connection cannot be set up.

Precautions

You must configure keychain authentication on both MSDP peers. Note that encryption algorithms and passwords configured for keychain authentication on both peers must be the same; otherwise, the TCP connection cannot be set up between MSDP peers and MSDP messages cannot be transmitted.

MSDP MD5 authentication and MSDP keychain authentication are mutually exclusive.

Example

Configure MSDP keychain authentication between the local switch and the peer 10.1.1.2 and configure a keychain named **test**.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] key-id 1
[HUAWEI-keychain-test-keyid-1] algorithm sha-256
[HUAWEI-keychain-test-keyid-1] key-string cipher Test@1234
[HUAWEI-keychain-test-keyid-1] quit
[HUAWEI-keychain-test] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.1.1.2 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.1.1.2 keychain test
```

8.5.18 peer mesh-group

Function

The **peer mesh-group** command adds an MSDP peer to a mesh group.

The **undo peer mesh-group** command restores the default configuration.

By default, an MSDP peer does not belong to any mesh group.

Format

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer that is to be a member of a mesh group.	The address is in dotted decimal notation.
name	Specifies the name of a mesh group.	The name is a string of 1 to 32 case-sensitive characters.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple MSDP peers exist on a network, SA messages may be flooded between peers. Especially when many MSDP peers are configured in the same PIM-SM domain, RPF rules cannot filter out useless SA messages effectively. The MSDP peer needs to perform an RPF check on each SA message received, which brings a heavy load to the system.

Configuring multiple MSDP peers to join the same mesh group can reduce the number of SA messages transmitted between these MSDP peers and reduce the load on the system.

Prerequisites

The device has established MSDP peer relationships with current mesh group members using the **peer connect-interface** command.

Configuration Impact

One MSDP peer can join only one mesh group. If an MSDP peer is added to different mesh groups several times, the latest configuration takes effect.

When a member of the mesh group receives an SA message, it checks the source of the SA message:

- If the SA message is sent by a certain MSDP peer outside the mesh group, the member performs the RPF check on the SA message. If the SA message passes the check, the member forwards it to other members of the mesh group.
- If the SA message is sent by a member of the mesh group, the member directly accepts the message without performing the RPF check. In addition, it does not forward the message to other members in the mesh group.

Precautions

The MSDP peer relationships must be established between the peers in a mesh group.

Commonly, the MSDP peers in the same AS join the same mesh group and EBGP routes need be configured between inter-AS MSDP peers.

Example

Add the MSDP peer with the address of 10.10.7.6 to the mesh group **Group1**

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 mesh-group Group1
```

8.5.19 peer minimum-ttl

Function

The **peer minimum-ttl** command sets a TTL threshold for the multicast data packet that can be encapsulated in an SA message and forwarded to a specified MSDP peer.

The **undo peer minimum-ttl** command restores the default value.

By default, the TTL threshold is 0.

Format

peer *peer-address* **minimum-ttl** *ttl*

undo peer *peer-address* **minimum-ttl**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
ttl	Specifies the TTL threshold.	The value is an integer that ranges from 0 to 255.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP peers transmit SA messages to each other over an established TCP connection. The **peer minimum-ttl** command limits the forwarding of SA messages with multicast data packets encapsulated.

After the TTL threshold is set for a specified peer, the switch checks the TTL values of multicast data packets before encapsulating them in SA messages. Only the multicast data packets with a TTL value greater than the threshold are encapsulated in an SA message and sent to the peer.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Set the TTL threshold to 10. Only the multicast data packet with the TTL value being greater than 10 is encapsulated in the SA message and forwarded to MSDP peer 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.10.1 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.10.1 minimum-ttl 10
```

8.5.20 peer password (MSDP)

Function

The **peer password** command configures MD5 authentication for establishing a TCP connection between MSDP peers.

The **undo peer password** command removes the MD5 authentication between MSDP peers.

By default, the MSDP MD5 authentication is not configured.

Format

peer *peer-address* **password** { **cipher** *cipher-password* | **simple** *simple-password* }

undo peer *peer-address* **password**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
cipher *cipher-password*	Specifies the password in the cipher text.	The value is a string of case sensitive characters without any space. A cipher password may contain 1 to 255 plain characters or 20 to 392 encrypted characters. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
simple *simple-password*	Specifies the password in the plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings high security risks. It is recommended that you select **cipher** to save the password in cipher text. To improve the device security, change the password periodically.	The value is a string of 1 to 255 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP supports MD5 authentication and keychain authentication that improves security on TCP connections between MSDP peers.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

MD5 is not a secure authentication algorithm. For security purposes, you are advised to use the more secure Keychain algorithm for MSDP authentication.

MSDP peers must be configured with the same authentication password; otherwise, the TCP connections cannot be set up between MSDP peers and MSDP messages cannot be transmitted. The authentication password on peers can be in different formats, for example, the password on one end can be in the cipher text while the password on the peer can be in the plain text.

MSDP MD5 authentication and MSDP keychain authentication are mutually exclusive.

Example

Configure MSDP MD5 authentication between the local switch and the peer 10.1.1.1 and set the authentication password to **Test@1234** in the cipher text.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

```
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.1.1.1 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.1.1.1 password cipher Test@1234
```

8.5.21 peer request-sa-enable

Function

The **peer request-sa-enable** command enables the function of immediately sending the SA Request message to a specified MSDP peer.

The **undo peer request-sa-enable** command restores the default configuration.

By default, when receiving a new Join message for a group, the switch does not send an SA Request message to MSDP peer but waits to receive the next SA message.

Format

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a new user joins multicast group G in a PIM-SM domain, a (*, G) entry is created on the RP. If no corresponding (S, G) information exists on the RP and SA cache is not enabled on the RP, multicast routes cannot be generated for this user. The RP then must wait for the next SA message from the remote MSDP peer to obtain valid (S, G) information.

Generally, the interval for an MSDP peer to send SA messages is set to a large value to reduce traffic load in the PIM-SM domain. This, however, will cause a delay in joining the source's SPT. To minimize the delay, enable the function of immediately sending SA Request messages on the local RP and enable the SA cache function on the remote MSDP peer. If a new Join message is received but the local entries and SA cache do not contain corresponding (S, G) information, the local RP immediately sends an SA Request message to the remote MSDP peer instead of waiting to receive the next SA message.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

Before configuring the **peer request-sa-enable** command on the local switch, disable SA cache on the local switch and enable SA cache on the peer of the specified *peer-address*. Therefore, when the local switch has new receiving requests, it can actively send SA Request messages to the peer and receive responses from the peer.

Example

Configure the switch to send SA Request messages to the MSDP peer 10.10.7.6 when receiving a new Join message.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 request-sa-enable
```

8.5.22 peer sa-cache-maximum

Function

The **peer sa-cache-maximum** command limits the maximum number of (S, G) entries that are learnt from MSDP peers and cached by the SA cache.

The **undo peer sa-cache-maximum** command restores the maximum number of (S, G) entries that are learnt from MSDP peers and cached by the SA cache to the default configuration.

By default, the maximum number of (S, G) entries in the SA cache is 8192.

Format

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Parameter	Description	Value
sa-limit	Specifies the maximum number of (S, G) entries that are allowed to cache.	The number is an integer that ranges from 1 to 4294967295.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You are recommended to perform this configuration on all MSDP peers on the network vulnerable to DoS attacks.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Configuration Impact

The total number of (S, G) entries that can be stored in SA-Cache is limited by the specification of the SA-Cache. At present, for an entire switch, the maximum number of (S, G) entries in SA-Cache is 8192.

For the (S, G) entries of a single peer:

- If the number of (S, G) entries is not set or exceeds 8192, the maximum number of (S, G) entries in the SA cache can be set to 8192.
- If the number of (S, G) entries is smaller than 8192, the maximum number of (S, G) entries in the SA cache is the configured value. The redundant (S, G) entries are not cached or advertised to PIM-SM but can be forwarded through SA messages.

Example

Set the maximum number of (S, G) entries that are learnt from MSDP peers and cached by the SA cache to 100 when the switch receives an SA message from MSDP peer 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] cache-sa-enable
[HUAWEI-msdp] peer 10.10.7.6 sa-cache-maximum 100
```

8.5.23 peer sa-policy

Function

The **peer sa-policy** command sets a filtering policy for SA messages received or forwarded.

The **undo peer sa-policy** command restores the default configuration.

By default, a device accepts all SA messages from MSDP peers, sends all locally created SA messages to MSDP peers, and forwards all SA messages to MSDP peers.

Format

peer *peer-address* **sa-policy** { **import** | **export** | **local-export** } [**acl** *advanced-acl-number*]

undo peer *peer-address* **sa-policy** { **import** | **export** | **local-export** }

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a remote MSDP peer.	The address is in dotted decimal notation.
import	Receives the SA messages from a specified MSDP peer.	-
export	Forwards the SA messages to a specified MSDP peer.	-
local-export	Indicates that the locally created SA messages to be sent to the specified peer are filtered.	-
acl	Indicates the ACL that defines the import or export policy.	-
advanced-acl-number	Specifies the number of the advanced ACL.	The number is an integer that ranges from 3000 to 3999.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer sa-policy** command is configured, MSDP can filter (S, G) forwarding entries carried in the SA message received from or forwarded to specified MSDP peers based on multicast source addresses, to control transmission of multicast source information.

- After the **peer** *peer-address* **sa-policy import** command is run, when an SA message reaches the local device from the specified peer, the local device filters the message using the import policy to determine whether to process the SA message.
  - If **acl** parameter is not configured, the device does not receive SA messages from any MSDP peer.
  - If **acl** parameter is configured, the device receives SA messages that carry the (S, G) entry only from a specified MSDP peer.
- After the **peer** *peer-address* **sa-policy export** command is run, the device filters an SA message using the export policy to determine whether to forward the SA message.
  - If **acl** parameter is not configured, the device does not forward SA messages from any MSDP peer.
  - If **acl** parameter is configured, the device forwards SA messages that carry the (S, G) entry only to a specified MSDP peer.
- After the **peer** *peer-address* **sa-policy local-export** command is run, the device filters the locally created SA messages to be sent to the peer specified by *peer-address*.
  - If **acl** parameter is not configured, no locally created SA messages that match the specified ACL to the specified MSDP peer.
  - If **acl** parameter is configured, the device sends only the locally created SA messages that match the specified ACL to the specified MSDP peer.

You can also run the **import-source** command on the peer nearest to a source to control the creation of SA messages.

The **import-source** command takes effect for all peers. If both the **import-source** and **peer** *peer-address* **sa-policy local-export** commands are run, the parameters configured in the **peer** *peer-address* **sa-policy local-export** command take effect preferentially.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Configure the switch to forward only the SA messages that pass the ACL3100 filtering to peer 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100
[HUAWEI-acl-adv-3100] rule permit ip source 10.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[HUAWEI-acl-adv-3100] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.10.7.6 sa-policy export acl 3100
```

8.5.24 peer sa-request-policy

Function

The **peer sa-request-policy** command configures the filtering policy to respond to the SA Request messages sent by a specified MSDP peer. Once the SA Request message passes the filtering, the switch responds to the SA message immediately.

The **undo peer sa-request-policy** command restores the default configuration.

By default, the switch responds to all SA request messages sent by all MSDP peers.

Format

peer *peer-address* **sa-request-policy** [**acl** *basic-acl-number*]

undo peer *peer-address* **sa-request-policy**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of MSDP peer that sends the SA Request message.	The address is in dotted decimal notation.
acl	Indicates an ACL. If the ACL is not specified, all SA Requests messages of the MSDP peer are ignored. If the ACL is specified, only the SA Request messages of the group that meets the requirements of the ACL are processed.	-
basic-acl-number	Indicates the number of the basic ACL.	The number is an integer that ranges from 2000 to 2999.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a local MSDP peer receives SA Request messages, the MSDP peer responds to all SA Request messages by default. To configure the switch to respond only to certain SA Request messages, configure the **peer sa-request-policy** command.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

The **peer sa-request-policy** and **acl** commands are used together.

- In the basic ACL view, you can set the multicast group address range of SA messages that are forwarded by the MSDP peer by specifying the **source** parameter in the **rule** command.

Example

Configure the ACL for filtering SA request messages sent by the MSDP peer 10.58.6.5: only SA request messages bound for the group whose address is 225.1.1.0/24 are received.

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.58.6.5 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.58.6.5 sa-request-policy acl 2001
```

8.5.25 reset msdp control-message counters

Function

The **reset msdp control-message counters** command clears statistics about MSDP messages.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**peer** *peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
all-instance	Indicates all instances, including the public network instance and all VPN instances. If **vpn-instance** or **all-instance** is not specified, only information about the public network instance is cleared.	-
peer *peer-address*	Specifies IP address of MSDP peer. If **peer** *peer-address* is specified, only statistics about the MSDP messages exchanged with a specified MSDP peer are cleared.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics about the received, sent, and discarded MSDP messages.

Example

Clear statistics about the MSDP messages received, sent, and discarded on the peer 10.3.3.3.

```
<HUAWEI> reset msdp control-message counters peer 10.3.3.3
```

8.5.26 reset msdp peer

Function

The **reset msdp peer** command resets the TCP connection with a specified MSDP peer, and clears statistics about the specified MSDP peer.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, the TCP connections set up between MSDP peers in the public network instance are reset and statistics about MSDP peers in the public network instance are cleared.	-
peer-address	Specifies the address of an MSDP peer. If the *peer-address* is not specified, all peers are reset.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-configure the TCP connection between MSDP peers and clear statistics about the specified MSDP peer, run the **reset msdp peer** command.

Use the **reset msdp statistics** command to clear the statistics about an MSDP peer without resetting the MSDP peer.

Configuration Impact

NOTICE

After you run this command, the TCP connection with the specified MSDP peer is torn down and a new TCP is set up again. During this process, MSDP services are interrupted, which may affect multicast services; for example, multicast data transmission may fail. Therefore, use this command with caution.

Example

Reset the TCP connection with MSDP peer 10.10.7.6 and clear the statistics about MSDP peer 10.10.7.6.

```
<HUAWEI> reset msdp peer 10.10.7.6
```

8.5.27 reset msdp sa-cache

Function

The **reset msdp sa-cache** command clears (S, G) entries in the SA cache.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the entries in the SA cache of the public network instance are cleared.	-
group-address	Specifies the group address carried in (S, G) information. If this parameter is not specified, all (S, G) information in the SA cache is cleared.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear (S, G) information from an SA cache, run the **reset msdp sa-cache** command.

Configuration Impact

NOTICE

(S, G) information in the SA cache cannot be restored after you clear it. Therefore, confirm the action before you use this command.

Example

Clear the (S, G) entries with the group address of 225.5.4.3 in the SA cache.

```
<HUAWEI> reset msdp sa-cache 225.5.4.3
```

8.5.28 reset msdp statistics

Function

The **reset msdp statistics** command clears statistics about one or more MSDP peers without resetting the MSDP peer (s).

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **statistics** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only information about the public network instance is cleared.	-
peer-address	Specifies the address of an MSDP peer. If the *peer-address* is not specified, the statistics about all MSDP peers are cleared.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **reset msdp statistics** command is used, the statistics about the MSDP peer are cleared automatically. However, the TCP connections among peers are not closed, and MSDP services are not affected.

To clear the statistics about an MSDP peer and to rebuild the TCP connections among MSDP peers at the same time, use the **reset msdp peer** command.

Example

Clear the statistics of MSDP peer 10.10.7.6.

```
<HUAWEI> reset msdp statistics 10.10.7.6
```

8.5.29 shutdown (MSDP)

Function

The **shutdown** command terminates a specified MSDP peer.

The **undo shutdown** command restores the default configuration.

By default, the MSDP peers are not closed after the peer relationship is established.

Format

shutdown *peer-address*

undo shutdown *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shutdown** command can be used to close the TCP connection between two MSDP peers while keeping the MSDP peer relationship.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Configuration Impact

After the **shutdown** command is run on MSDP peers, the MSDP peers do not transmit SA messages or attempt to establish a connection. When the **display msdp brief** command or the **display msdp peer-status** command is used to check the status of MSDP peers, **State** in the command output is displayed as **Shutdown**.

Precautions

You only need to run the **undo shutdown** command to restore the configuration, and do not need to re-configure the MSDP peer using the **peer connect-interface (MSDP)** command.

Example

Close MSDP peer 10.10.7.6.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.10.7.6 connect-interface vlanif 100
[HUAWEI-msdp] shutdown 10.10.7.6
```

8.5.30 static-rpf-peer

Function

The **static-rpf-peer** command configures an MSDP peer as a static RPF peer. The SA messages sent by the static RPF peer do not require RPF checks.

The **undo static-rpf-peer** command restores the default configuration.

By default, no MSDP peer is configured as a static RPF peer.

Format

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a static RPF peer.	The value is in dotted decimal notation.

Parameter	Description	Value
rp-policy *ip-prefix-name*	Specifies the filtering policy that is used to filter SA messages based on RP addresses. **ip ip-prefix** specifies the name of the filtering policy.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent SA messages from being circularly forwarded between MSDP peers, MSDP performs the RPF check on the received SA message. MSDP strictly controls the incoming SA messages. The SA messages that do not comply with the RPF rules are discarded.

To protect the SA messages transmitted between MSDP peers from being discarded in RPF checks and reduce redundant traffic, you can specify MSDP peers as static RPF peers. The SA messages received from a static RPF peer do not need to be checked according to RPF rules.

Prerequisites

The MSDP peer relationship has been established between the switch and a specified RPF peer using the **peer connect-interface (MSDP)** command.

Configuration Impact

You can specify multiple remote static RPF peers for the switch using the **static-rpf-peer** *peer-address* command repeatedly.

Precautions

When you specify multiple static RPF peers for the switch, pay attention to the following points:

- All the peers are configured with **rp-policy**

  When SA messages sent by a static RPF peer in the active state reaches the local switch, the local switch filters the SA messages according to specified **rp-policy** on the peers, and receives only the SA messages that pass the filter.
- None of the peers is configured with **rp-policy**

  The local switch receives all the SA messages from the static RPF peers in the active state.

Example

Configure 192.168.3.2 as a static RPF peer, with the source RP address range of 192.168.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 192.168.3.2 connect-interface vlanif 100
[HUAWEI-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
```

8.5.31 timer retry

Function

The **timer retry** command sets the interval for retrying to set up an MSDP peer relationship.

The **undo timer retry** command restores the default value.

By default, the interval for retrying to set up an MSDP peer relationship is 30 seconds.

Format

timer retry *interval*

undo timer retry

Parameters

Parameter	Description	Value
interval	Specifies the interval for retrying to set up an MSDP peer relationship.	The value is an integer that ranges from 1 to 60, in seconds.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A TCP connection needs to be set up between two MSDP peers. The peer with a larger IP address listens to port 639, and the peer with a smaller IP address initiates a connection. If the connection setup fails, the peer retries connection setup after a specified interval.

A TCP connection needs to be established between MSDP peers in one of the following situations:

- An MSDP peer is created.
- A disconnected MSDP peer needs to be reconnected
- A faulty MSDP peer attempts to restore work.

You can run the **timer retry** command to adjust the interval for retrying to set up an MSDP peer relationship.

Prerequisites

MSDP has been enabled using the **msdp** command.

Example

Set the interval for retrying to set up an MSDP peer relationship to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] timer retry 60
```

8.6 Multicast VPN Configuration Commands

8.6.1 Command Support

Only the following switch models support Multicast VPN:

S5731-S, S5731-H, S5731S-H, S5732-H,, S6720-EI, S6720S-EI, S6730-S, S6730-H, and S6730S-H

8.6.2 auto-discovery

Function

The **auto-discovery** command configures the auto-discovery (A-D) mode for the multicast VPN, and associates an inbound multicast routing policy with the IPv4 address family of the current VPN instance.

The **undo auto-discovery** command deletes the A-D mode configuration for the multicast VPN and removes the association between the inbound multicast routing policy and the IPv4 address family of the current VPN instance.

By default, the A-D mode is not configured for the multicast VPN and the IPv4 address family of the current VPN instance is not associated with an inbound multicast routing policy.

Format

auto-discovery { **mdt** | **mvpn** } [**import route-policy** *route-policy-name*]

undo auto-discovery

Parameters

Parameter	Description	Value
mdt	Specifies the MDT-Subsequent Address Family Identifier (SAFI) A-D mode for the multicast VPN.	-
mvpn	Specifies the MCAST-VPN SAFI A-D mode for the multicast VPN.	-
route-policy *route-policy-name*	Specifies the inbound multicast routing policy that is to be associated with the IPv4 address family of the VPN instance.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, the multicast VPN is implemented by establishing the PIM-SSM MDT on the public network to transmit multicast VPN services as all Provider Edges (PEs) on the network know information about the Rendezvous Point (RP). This mechanism, however, does not support the Share-Group address within the SSM address range. This is because PEs in the same VPN do not know the peer information of each other, therefore knowing nothing about the multicast source information. As a result, these PEs cannot directly send Join messages to the multicast source and establish the PIM-SSM MDT.

To solve this problem, in an autonomous system (AS), you can configure the BGP A-D mode to enable automatic discovery of the peer information about PEs in the same VPN. In this manner, multicast VPN services can be transmitted over the public network tunnel which is based on the PIM-SSM MDT.

At present, the multicast VPN supports two A-D modes:

- MDT-SAFI A-D mode: In this mode, a new address family is defined in the MDT-SAFI message advertised through BGP. After the multicast VPN is configured on a PE, the multicast VPN configurations, including the Route Distinguisher (RD) and the Share-Group address, can be advertised to all BGP peers. After a remote PE (a BGP peer) receives the MDT-SAFI message advertised through BGP, the remote PE compares the RD carried in the message with its local RD. If the RDs are the same, the remote PE is in the same VPN as the local PE. The remote PE then uses the MDT-SAFI message to establish the PIM-SSM MDT for transmitting multicast VPN services.

- MCAST-VPN SAFI A-D mode: In this mode, a new address family is defined in the MCAST-VPN-SAFI message advertised through BGP. Similar to the MDT-SAFI A-D mode, the MCAST-VPN SAFI A-D mode uses the MCAST-VPN-SAFI message advertised between BGP peers to transmit multicast VPN configurations, including the RD and Share-Group address. The difference is that the MCAST-VPN SAFI A-D mode has a broader definition, supports more extensions, and carries more multicast VPN attributes and information for establishing the public network tunnel. Therefore, the MCAST-VPN SAFI A-D mode applies to the next-generation multicast VPN.

Prerequisites

The **multicast routing-enable** command is configured in the public network instance view or the VPN instance view.

Precautions

- When configuring the A-D mode for the multicast VPN, you need to configure a matching A-D address family in the BGP view so that the BGP A-D mode can be used to implement the multicast VPN function. If the configured A-D mode is inconsistent with the A-D address family enabled in the BGP view, the A-D mode will not take effect.
- This command applies to the single-AS scenario, with no RP configured on the public network.
- In a VPN enabled with the IPv4 address family, only one A-D mode can be used. Different VPNs enabled with the IPv4 address family on a PE can use different A-D modes. Therefore, you need to enable two types of A-D address families in the BGP view, so that the VPNs can use different A-D modes to forward multicast data.
- The PEs enabled with the BGP A-D function must support the same PIM protocol and use the Share-Group address within the SSM address range.
- Running this command does not affect the original multicast VPN service flow. If the Share-Group address is in the Any-Source Multicast (ASM) address range, or if the PIM-DM protocol is used on the public network, multicast VPN traffic can still be transmitted over the public network tunnel for which PIM-SM or PIM-DM is configured.

Example

Configure the MDT-SAFI A-D mode for vpn1 enabled with the IPv4 address family, so that the multicast VPN services are transmitted over the public network tunnel based on the PIM-SSM MDT.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family mdt
[HUAWEI-bgp-af-mdt] peer 3.3.3.3 enable
[HUAWEI-bgp-af-mdt] quit
[HUAWEI-bgp] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] vpn-target 100:1 both
[HUAWEI-vpn-instance-vpn1-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-vpn1-af-ipv4] multicast-domain share-group 232.2.2.0 binding mtunnel 0
[HUAWEI-vpn-instance-vpn1-af-ipv4] auto-discovery mdt
```

8.6.3 display default-parameter mvpn

Function

The **display default-parameter mvpn** command displays default configurations about the multicast VPN (MVPN).

Format

display default-parameter mvpn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using this command displays only default configurations, regardless of whether the configurations about MVPN parameters are changed.

Example

Display default configurations about the MVPN.

```
<HUAWEI> display default-parameter mvpn
  MVPN Instance View Default Configurations:
  ------------------------------------------
  Multicast-domain switch-delay: 5 s
  Multicast-domain switch threshold: 0 kbps-preferred
  Multicast-domain holddown-time: 60 s
  Multicast-domain log switch-group-reuse: disabled
  Multicast-domain share-group: disabled
  Multicast-domain switch-group-pool: disabled
  Multicast-domain auto-discovery: disabled
  Multicast-domain switch-without-register: disabled
  Multicast extranet select-rpf rule: disabled
```

Table 8-81 Description of the **display default-parameter mvpn** command output

Item	Description
MVPN Instance View Default Configurations	Default configurations in the MVPN instance view.

Item	Description
Multicast-domain switch-delay	Delay in switching from the share-MDT to the switch-MDT. This parameter can be configured using the **multicast-domain switch-delay** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain switch threshold	Threshold of the multicast packet rate that can trigger the switch to the switch-MDT. This parameter can be configured using the **multicast-domain switch-group-pool** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain holddown-time	Delay in switching from the switch-MDT to the share-MDT. This parameter can be configured using the **multicast-domain holddown-time** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain log switch-group-reuse	Whether recording logs about switch-group address reuse is configured. This parameter can be configured using the **multicast-domain log switch-group-reuse** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain share-group	Whether the Share-Group address is configured and whether the MTI is bound to a VPN instance. This parameter can be configured using the **multicast-domain share-group binding** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain switch-group-pool	Whether the range of the switch-MDT switch-group-pool is configured. This parameter can be configured using the **multicast-domain switch-group-pool** command in the VPN instance view or VPN IPv4 address family view.
Multicast-domain auto-discovery	Whether the A-D mode is configured for the VPN. The switch does not support the A-D mode currently.

Item	Description
Multicast-domain switch-without-register	Whether the source PE sends the null Register message to the RP to establish the SPT on the public network before the Switch-Group address is used to encapsulate VPN data. This parameter can be configured using the **multicast-domain switch-without-register** command in the VPN instance view or VPN IPv4 address family view.
Multicast extranet select-rpf rule	Whether the multicast routing policy configured for a VPN is configured. The switch does not support the configuration of a multicast routing policy for a VPN currently.

8.6.4 display multicast-domain control-message counters

Function

The **display multicast-domain control-message counters** command displays statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances.

Format

display multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **control-message counters**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about sent and received MDT switch messages in a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
all-instance	Displays statistics about sent and received MDT switch messages in all VPN instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a Switch-MDT, you can run the **display multicast-domain control-message counters** command to view statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances and check whether packets are normally sent and received on the current device.

You can run the **reset multicast-domain control-message counters** command to clear the statistics.

Example

Display statistics about sent and received MDT switch messages in VPN instance **red**.

```
<HUAWEI> display multicast-domain vpn-instance red control-message counters
VPN-Instance red:
 Message Type     Received         Sent            Invalid
 Switch           5000             0               5000
```

Table 8-82 Description of the **display multicast-domain vpn-instance red control-message counters** command output

Item	Description
VPN-Instance red	VPN instance in which statistics about sent and received MDT switch messages need to be displayed.
Message Type	Message type, that is MDT switch messages.
Received	Number of received messages.
Sent	Number of sent messages.
Invalid	Number of received invalid messages.

8.6.5 display multicast-domain invalid-packet

Function

The **display multicast-domain invalid-packet** command displays statistics about invalid MDT switch messages received by a device and details of these messages.

Format

display multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **invalid-packet**

display multicast-domain invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid MDT switch messages received in a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
all-instance	Displays statistics about invalid MDT switch messages received in all VPN instances.	-
packet-number	Displays details of a specified number of invalid MDT switch messages recently received.	The value is an integer ranging from 1 to 100. By default, details of all the invalid MDT switch messages currently stored are displayed.
verbose	Displays details of invalid MDT switch messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast-domain invalid-packet** command to view statistics and details of invalid MDT switch messages for fault location and rectification.

If an SPT fails to be set up in a VPN instance on a multicast network, you can run the **display multicast-domain invalid-packet** command first to check whether devices have received invalid MDT switch messages. If the command output contains statistics about invalid MDT switch messages, you need to run the **display multicast-domain invalid-packet** [*packet-number*] **verbose** command to view details of invalid MDT switch messages to locate the fault.

Example

Displays statistics about invalid MDT switch messages received in **vpn1**.

```
<HUAWEI> display multicast-domain vpn-instance vpn1 invalid-packet

             Statistics of invalid packets for vpn1:
-------------------------------------------------------------------
MDT Switch invalid packet:
Fault Length            : 0           Invalid Message Type    : 0
```

```
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Switch Group    : 0
------------------------------------------------------------------
```

Table 8-83 Description of the **display multicast-domain vpn-instance vpn1 invalid-packet** command output

Item	Description
Statistics of invalid packets for vpn1	VPN instance in which statistics about MDT switch messages need to be displayed.
MDT Switch invalid packet	Invalid MDT switch messages.
Fault Length	Messages with invalid lengths.
Invalid Message Type	Messages with invalid message types.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Switch Group	Messages with invalid switch group addresses.

Display details of one invalid MDT switch message recently received in the public network instance.

```
<HUAWEI> display multicast-domain invalid-packet 1 verbose
      Detailed information of invalid packets
----------------------------------------------------
Packet information (Index 1):
----------------------------------------------------
Interface           :  10.44.44.44
Time                :  2010-6-9 10:50:08 UTC-08:00
Message Length      :  16
Invalid Type        :  Invalid Switch Group
0000: 01 00 10 00 64 64 64 64 e8 00 00 00 0a 00 00 00
----------------------------------------------------
```

Table 8-84 Description of the **display multicast-domain invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of the invalid MDT switch message.
Packet information (Index 1)	Sequence number of the invalid MDT switch message (numbered in the opposite order that the message is received, for example, the index of the last received message is 1, the index of the last but one message is 2, and so on).

Item	Description
Interface	IP address of interface receiving the invalid MDT switch message
Time	Time when the invalid MDT switch message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid MDT switch message.
Invalid Type	Type of the invalid MDT switch message.
0000: 01 00 10 00 64 64 64 64 e8 00 00 00 0a 00 00 00	Contents of the invalid MDT switch message.

8.6.6 display multicast-domain vpn-instance share-group

Function

The **display multicast-domain vpn-instance share-group** command displays information about the Share-Group address configured for a specified VPN instance.

Format

display multicast-domain vpn-instance *vpn-instance-name* **share-group** [**local** | **remote**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the Share-Group of a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.

Parameter	Description	Value
local	Indicates the locally configured Share-Group address.	-
remote	Indicates the Share-Group address configured on remote PE and learned through BGP Update packets.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast-domain vpn-instance share-group** command displays information about the Share-Group, peer IP address, and tunnel type, which allows you to determine whether the multicast tunnel is correctly established to forward multicast services.

Example

Display the Share-Group information of VPN instance **BLUE** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance BLUE share-group
MD local share-group information for VPN-Instance: BLUE
  Share-group: 239.2.2.0
  MTunnel address: 3.3.3.3
```

Table 8-85 Description of the **display multicast-domain vpn-instance share-group** command output

Item	Description
MD local share-group information for VPN-Instance	VPN instance to which local Share-Group information in the multicast domain belongs.
Share-group	Share-MDT group address configured on the local switch. This parameter can be configured using the **multicast-domain share-group binding** command in the VPN instance view or VPN IPv4 address family view.

Item	Description
MTunnel address	Configured IP address of the MTI bound to the Share-Group on the local switch. The source interface whose IP address is referenced by the MTI can be configured using the **multicast-domain source-interface** command in the VPN IPv4 address family view. In this way, the IP address of the MTI is obtained. You can also directly configure an IP address for an MTI in the MTI interface view.

8.6.7 display multicast-domain vpn-instance switch-group receive

Function

The **display multicast-domain vpn-instance switch-group receive** command displays the Switch-Group information received by a specified VPN instance.

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive brief**

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive** [**active** | **sender** *source-address* | **group** *group-address* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the Switch-Group information received by a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
active	Displays the received Switch-Group that joins the Switch-MDT.	-
brief	Displays brief information about the received Switch-Group.	-

Parameter	Description	Value
group *group-address*	Displays the Switch-Group related to a multicast group specified by *group-address* of the public network. *group-address* specifies the address of the multicast group.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
sender *source-address*	Displays the Switch-Group information related to the specified multicast source *source-address* of the public network. The *source-address* indicates the multicast.	The value is in dotted decimal notation.
vpn-source-address	Displays the Switch-Group information related to a VPN multicast source specified by *vpn-source-address*.	The value is in dotted decimal notation.
mask	Indicates the mask of the VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of the VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of the VPN multicast source address.	The value is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to a VPN multicast group specified by *vpn-group-address*.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of the VPN multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of the VPN multicast group address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast-domain vpn-instance switch-group receive** command to display the Switch-Group information received by the local router:

- Each VPN instance corresponds to an MD. *vpn-instance-name* specifies a VPN instance. Use the command to display the information about the Switch-Group of a specified MD.

- If **brief** is specified, brief information about all Switch-Groups is displayed in ascending order of the Switch-Group address.
- If **active** is specified, only information about the Switch-Groups that have joined the Switch-MDT is displayed, in ascending order of the VPN (S, G).

Example

Display Switch-Group information received by VPN instance **VPN1** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group receive
MD switch-group information received by VPN-Instance: VPN1
Switch group:  226.1.1.0 ref count: 8, active count: 8
  Sender:  172.16.1.1 active count: 8
    (192.168.1.5, 239.1.1.1)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.1.158)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.2.12)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.2.197)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.5, 239.1.3.62)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.2, 225.1.1.109)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.2, 225.1.4.80)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.168.1.2, 225.1.4.173)
    Up time: 01:20:20  expire time: 00:03:10  active
```

Display brief Switch-Group information received by VPN instance **VPN1** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group receive brief
MD switch-group information received by VPN-Instance: VPN1
switch group:  226.1.1.0 ref count: 8, active count: 0
switch group:  226.1.1.1 ref count: 4, active count: 0
switch group:  226.1.1.2 ref count: 8, active count: 0
switch group:  226.1.1.3 ref count: 4, active count: 0
switch group:  226.1.1.4 ref count: 8, active count: 0
```

Table 8-86 Description of the **display multicast-domain vpn-instance switch-group receive** command output

Item	Description
MD switch-group information received by VPN-Instance	VPN instance to which MD Switch-Group information belongs.
switch group	Address of the received Switch-Group.
ref count	Number of VPN multicast groups referenced by the Switch-Group.
active count	Number of active VPN multicast groups (where receivers exist) referenced by the Switch-Group.
sender	BGP peer IP address of the PE that sends Switch-Group information.

Item	Description
Up time	Creation time of switching messages in which the VPN multicast (S, G) entry is referenced by the Switch-group
expire time	Timeout period of the VPN multicast (S, G) entry referenced by the Switch-Group.

8.6.8 display multicast-domain vpn-instance switch-group send

Function

The **display multicast-domain vpn-instance switch-group send** command displays the Switch-Group information sent by the specified VPN instance in an MD.

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group send** [**reuse** *interval* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }] | **group** *group-address*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the Switch-Group information sent by a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
group *group-address*	Displays the Switch-Group information related to a multicast group G. The parameter *group-address* indicates multicast group address.	The value is in dotted decimal notation format. The address ranges from 224.0.1.0 to 239.255.255.255.
reuse *interval*	Displays Switch-Group information that is reused by an MD in the specified period. The parameter *interval* indicates the specified period.	The value of the interval is an integer that ranges from 1 to 2147483647 seconds.

Parameter	Description	Value
vpn-source-address	Displays the Switch-Group information related to the specified VPN multicast source.	The value is in dotted decimal notation format.
mask	Indicates the mask of the VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of the VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of the VPN multicast source address.	The value is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to the specified VPN multicast group G.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of the VPN multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of the VPN multicast group address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use the **display multicast-domain vpn-instance switch-group send** command to display the Switch-Group information sent by the local switch:

- Each VPN instance corresponds to an MD. *vpn-instance-name* specifies a VPN instance. The command is only used to display the Switch-Group information related to the specified MD.
- The Switch-Group information is displayed in ascending order of VPN (S, G) entry.
- If **reuse** *interval* is specified, the group information that is reused in a specified interval is displayed in ascending order of Switch-Group address.

Example

Display the Switch-Group information sent by VPN instance **VPN1** in an MD.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group send
MD switch-group information sent by VPN-Instance: VPN1
  226.1.1.0 reference_count: 3
    (1.1.1.1, 239.1.1.1)                switch time: 00:00:21
    (1.1.1.1, 239.1.1.158)              switch time: 00:00:21
```

```
   (1.1.1.1, 239.1.2.50)              switch time: 00:00:05
 226.1.1.1 reference_count: 3
   (1.1.1.1, 225.1.1.1)               switch time: 00:00:21
   (1.1.1.1, 225.1.2.50)              switch time: 00:00:05
   (1.1.1.1, 239.1.1.159)             switch time: 00:00:21
```

Display information about the Switch-Group reuse sent by VPN instance **VPN1** in an MD within the latest 30s.

```
<HUAWEI> display multicast-domain vpn-instance VPN1 switch-group send reuse 30
MD switch-group information sent by VPN-Instance: VPN1
  226.1.1.0 reuse_count: 1
  226.1.1.1 reuse_count: 1
  226.1.1.2 reuse_count: 1
```

Table 8-87 Description of the **display multicast-domain vpn-instance switch-group send** command output

Item	Description
MD switch-group information sent by VPN-Instance	VPN instance to which MD Switch-Group information belongs.
226.1.1.0 reference_count	Number of VPN multicast groups referenced by the Switch-Group.
switch time	Switching time of the VPN multicast (S, G) entry referenced by the Switch-Group.
226.1.1.0 reuse_count	Number of times of reusing the Switch-Group sent in the specified period.

8.6.9 interface mtunnel

Function

The **interface mtunnel** command displays the MTI view.

Format

interface mtunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies an MTI number.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MTI is the inbound/outbound interface of a multicast tunnel and also functions as the inbound/outbound interfaces of the MD. A local PE sends VPN data through the MTI, and the remote PE receives data from the MTI. The MTI is the tunnel for data exchange between the public network instance and the VPN instance on the PE. A PE connects to the MT through the MTI. The VPN instances on PEs in the MD establish PIM neighbor relationships with each other on the MTI.

When you run the **multicast-domain share-group binding** command, the MTI is automatically created. You can run the **interface mtunnel** command to enter the MTI view and configure MTI parameters

Prerequisites

The MIT has been automatically created after the **multicast-domain share-group binding** command is executed to configure a Share-Group for a VPN instance and bind the Share-Group to the MTI.

Example

Enter the view of MTunnel interface 10, which has been automatically created.

```
<HUAWEI> system-view
[HUAWEI] interface mtunnel 10
[HUAWEI-MTunnel10]
```

8.6.10 mtu (MTI view)

Function

The **mtu** command sets the MTU for a multicast tunnel interface (MTI).

The **undo mtu** command restores the default MTU of an MTI.

By default, the MTU of an MTI is 1472 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU value of an MTI.	The value is an integer that ranges from 46 to 1500, in bytes.

Views

MTI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the length of a VPN multicast packet is equal or close to the MTU of the outbound interface of the public network instance, the length of the GRE-encapsulated public network multicast data packet is larger than the MTU of the outbound interface of the public network instance. In this case, the local PE must fragment the encapsulated packet and sends it through the outbound interface of the public network instance. Upon receiving the packet, the remote PE reassembles the packet.

You can set the MTU of the MTI to a smaller value so that VPN multicast packets can be fragmented before being encapsulated using the GRE. The remote PE does not need to reassemble the packets, improving efficiency.

Precautions

If the MTU is set too small and the size of packets is large, packets are broken into a great number of fragments, and may be discarded by QoS queues.

Example

Set the MTU of MTunnel 10 to 1400.

```
<HUAWEI> system-view
[HUAWEI] interface mtunnel 10
[HUAWEI-MTunnel10] mtu 1400
```

8.6.11 multicast-domain holddown-time

Function

The **multicast-domain holddown-time** command sets the delay for the switching from the Switch-MDT to the Share-MDT.

The **undo multicast-domain holddown-time** command restores the default value of the interval.

By default, the delay for the switching from the Switch-MDT to the Share-MDT is 60 seconds.

Format

multicast-domain holddown-time *interval*

undo multicast-domain holddown-time

Parameters

Parameter	Description	Value
interval	Specifies the delay for the switching from the Switch-MDT to the Share-MDT.	The value of the delay ranges from 0 to 512, in seconds.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the Switch-MDT configuration, the forwarding rate of VPN multicast data may fluctuate above and below the switchover threshold due to network instability. To prevent multicast data traffic from being frequently switched between the Switch-MDT and Share-MDT, the system does not perform the switchover immediately after it finds that the forwarding rate is smaller than the switching threshold. Instead, the system starts the hold-down timer and performs the switchover after the hold-down timer expires.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Precautions

During a switchover, there is a delay about 1 to 30 seconds from the time when the forwarding rate ranges to the time when the system starts the Switch-Delay timer. The delay is not included in the hold-down time. Consequently, the total delay from the time when the forwarding rate changes to the time when the system completes the switchover is 1-30 seconds longer than the hold-down time.

When *interval* is set to 0, the system triggers a switchover from the Switch-MDT to the Share-MDT immediately after it finds that the forwarding rate is below the threshold.

If a VPN instance has many multicast forwarding entries, the time taken to collect multicast traffic statistics will exceed the default hold-down time. In this case, increase the hold-down time to prevent frequent switchovers between the Switch-MDT and Share-MDT. Table 8-88 lists the recommended hold-down time values in various conditions.

Table 8-88 Recommended hold-down time values

Number of Multicast Forwarding Entries in a VPN Instance	Recommended Hold-down Time Value (Seconds)
1024	60
2048	128
4094	256

Example

Set the delay for the switching from the Switch-MDT to the Share-MDT to 80 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain holddown-time 80
```

8.6.12 multicast-domain log switch-group-reuse

Function

The **multicast-domain log switch-group-reuse** command enables the output of log information about reusing group address in Switch-Group-Pool.

The **undo multicast-domain log** command disables the output of log information about reusing group address in Switch-Group-Pool.

By default, the output of log information about reusing Switch-Group is disabled.

Format

multicast-domain log switch-group-reuse

undo multicast-domain log

Parameters

None

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the VPN instance that the source PE is bound to, if the Switch-Group-Pool cannot provide enough addresses for VPN multicast data packets whose transmission path needs to be switched to the Switch-MDT, the multicast group addresses can be reused. To record information about reusing Switch-Group, enable the output of log information about reusing Switch-Group addresses.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Example

Enable the output of log information about reusing Switch-Group addresses in VPN **mytest**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain log switch-group-reuse
```

8.6.13 multicast-domain share-group binding

Function

The **multicast-domain share-group binding** command specifies the Share-MDT group and binds the Multicast Tunnel Interface (MTI) to a VPN instance.

The **undo multicast-domain share-group** command restores the default configuration.

By default, the group address of Share-MDT is not specified.

Format

multicast-domain share-group *group-address* **binding mtunnel** *number*

undo multicast-domain share-group

Parameters

Parameter	Description	Value
group-address	Specifies the multicast group address. **NOTE** Do not enter an IP address in the SSM address range (232.*.*.*); otherwise, the multicast VPN cannot be established.	The value is in the dotted decimal notation. The address ranges from 224.0.1.0 to 239.255.255.255.
mtunnel *number*	Specifies the MTI number.	The value is an integer that ranges from 0 to 1023.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you run the **multicast-domain share-group binding** command, the device automatically creates the MTI and establishes a Share-MDT with the *group-address* value as the multicast group address for forwarding VPN multicast packets.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command in the VPN instance.

Follow-up Procedure

Manually configure an IP address for the MTI in the MTI view or run the **multicast-domain source-interface** command in the VPN IPv4 address family view to configure the MTI to automatically obtain an IP address.

Precautions

You cannot configure the same Share-Group address for different VPN instances on a PE. The Share-Group address cannot be the same as the Switch-Group address. The *number* value must be set different from the MTI number.

You cannot repeatedly run the **multicast-domain share-group binding** command in the same VPN instance view. You can configure a new Share-MDT group address and MTI only after deleting the existing ones.

After the **undo multicast-domain share-group** command is executed, configurations about the MTI and Switch-MDT are deleted.

Some multicast protocol packets (such as Register and Graft packets) are sent in unicast mode. These packets are transmitted over unicast VPN tunnels but not multicast VPN tunnels (Mtunnels) on the public network.

Example

Specify the Share-Group of VPN instance **mytest** as 224.1.1.1 and bind MTI0.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
```

8.6.14 multicast-domain source-interface

Function

The **multicast-domain source-interface** command allows an MTI to use an IP address of a default interface.

The **undo multicast-domain source-interface** command restores the default setting.

By default, an MTI does not use an IP address of a default interface.

Format

multicast-domain source-interface *interface-type interface-number*

undo multicast-domain source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the MTI address.	-

Views

System view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PE encapsulates VPN multicast packets, the MTI address is used as the multicast source address of the encapsulated public network multicast data packets. You can run the **multicast-domain source-interface** command to configure the source interface whose address is referenced by the MTI. This keeps the MTI address consistent with the IP address of the interface on which IBGP neighbor relationships are established, which ensures that VPN multicast packets pass the RPF check.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command in the VPN instance.

Precautions

If the **multicast-domain source-interface** command is run in the system view, the setting takes effect globally. The command run in the VPN IPv4 address family view takes precedence over that run in the system view. If the command is configured in the system view rather than the VPN IPv4 address family view, the setting in the system view takes effect.

A manually configured IP address on an MTI takes precedence over a default interface address specified using the **multicast-domain source-interface** command.

The source interface whose address is referenced by the MTI must be the interface on which public network IBGP neighbor relationships are established on the PE; otherwise, VPN multicast packets cannot pass the RPF check.

Example

Configure the MTI to use the IP address of the default interface named **loopback 1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain source-interface loopback 1
```

8.6.15 multicast-domain switch-delay

Function

The **multicast-domain switch-delay** command specifies the delay for the switchover from the Share-MDT to Switch-MDT in a specified VPN instance.

The **undo multicast-domain switch-delay** command restores the default value of the delay.

By default, the delay for the switchover from the Share-MDT to Switch-MDT is 5 seconds.

Format

multicast-domain switch-delay *switch-delay*

undo multicast-domain switch-delay

Parameters

Parameter	Description	Value
switch-delay	Specifies the delay for the switchover from the Share-MDT to Switch-MDT.	The value of the delay is an integer that ranges from 3 to 60, in seconds.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some cases, the forwarding rate of VPN multicast data packets fluctuates above and below the switchover threshold. To prevent frequent switchovers between the Share-MDT and Switch-MDT, configure a delay for the switchover from the Share-MDT to Switch-MDT. When detecting that the forwarding rate is higher than the switchover threshold, the system does not immediately perform the switchover but starts the Switch-Delay timer. Before the Switch-Delay timer expires, the system continues to detect the data forwarding rate. If the rate remains higher than the switchover threshold throughout the duration of the Switch-Delay timer, the transmission path of data packets is switched to the Switch-MDT; otherwise, the packets are still forwarded along the Share-MDT.

Prerequisites

The Share-Group has been configured using the **multicast-domain share-group binding** command in the VPN instance.

Precautions

During a switchover, there is a delay about 1 to 30 seconds from the time when the forwarding rate ranges to the time when the system starts the Switch-Delay timer. The delay is not included in the value of the Switch-Delay. Consequently, the total delay from the time when the forwarding rate of the data changes to the time when the system completes the switchover is 1-30 seconds longer than the Switch-Delay.

Example

Specify the delay for the switching to Switch-MDT to 20 seconds in VPN instance **mytest**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain switch-delay 20
```

8.6.16 multicast-domain switch-group-pool

Function

The **multicast-domain switch-group-pool** command specifies the conditions for the switchover from the Share-MDT to Switch-MDT and configures the Switch-Group-Pool in a specified VPN instance.

The **undo multicast-domain switch-group-pool** command restores the default configuration.

By default, the Switch-Group-Pool is not specified, and the switchover to the Switch-MDT is not performed.

Format

multicast-domain switch-group-pool *switch-group-pool* { *network-mask* | *network-mask-length* } [**threshold** *threshold-value* | **acl** *advanced-acl-number*] *

undo multicast-domain switch-group-pool

Parameters

Parameter	Description	Value
switch-group-pool	Specifies the start address of the Switch-Group-Pool.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
network-mask	Specifies the mask of a Switch-Group-Pool address.	The value is in dotted decimal notation and ranges from 255.255.255.0 to 255.255.255.255.
network-mask-length	Specifies the mask length of a Switch-Group-Pool address.	The value is an integer that ranges from 24 to 32; that is, the range of the group address in the Switch-MDT Switch-Group-Pool is from 0 to 255.
threshold *threshold-value*	Specifies the switchover threshold.	The value is an integer that ranges from 0 to 4194304, in kbit/s. By default, it is 0.
acl *advanced-acl-number*	Specifies the (S, G) entry which the Switch-Group-Pool takes effect on. *advanced-acl-number* indicates the advanced ACL number. If the ACL is not specified, the Switch-Group-Pool takes effect on all (S, G) entries.	The value is an integer that ranges from 3000 to 3999.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Between the PE connected to the VPN receivers and the PE connected to the VPN multicast source, a special Switch-MDT is set up for the high-speed VPN multicast data packets flowing into the public network. The multicast data flow can be switched from the Share-MDT to the Switch-MDT. Therefore, on-demand multicast can be realized. This prevents data from be flooded in the public network when the Share-MDT is used to transmit VPN multicast data packets.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Follow-up Procedure

In some cases, the forwarding rate of VPN multicast data packets fluctuates above and below the switchover threshold. Configure a delay for the switchover from the Share-MDT to Switch-MDT using the **multicast-domain switch-delay** command. If the rate remains higher than the switchover threshold throughout the duration of the Switch-Delay timer, the transmission path of data packets is switched to the Switch-MDT; otherwise, the packets are still forwarded along the Share-MDT.

Precautions

On a PE, the address ranges defined by the Switch-Group-Pool cannot overlap for VPN instances.

From the time when data forwarding rate changes to the time when the system starts the switch-delay timer, there is a delay of 1 to 30 seconds because of necessary traffic calculation and protocol processing. In actual switchover, the delay is longer than the switch-delay period by 1 to 30 seconds.

Example

Configure the Switch-Group-Pool of VPN instance named **mytest** to range from 225.2.2.1 to 225.2.2.15.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28
```

8.6.17 multicast-domain switch-without-register

Function

The **multicast-domain switch-without-register** command disables the source PE from sending null Register messages to the RP to establish the SPT on the public network before the Switch-Group address is used to encapsulate VPN data.

The **undo multicast-domain switch-without-register** command restores the default setting.

By default, before the Switch-Group address is used to encapsulate VPN data, the source PE sends null Register messages to the RP and establishes the SPT on the public network.

Format

multicast-domain switch-without-register

undo multicast-domain switch-without-register

Parameters

None

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In previous implementation, if the Switch-Group address is in the ASM address range, when the SPT switchover occurs on the multicast tunnel of the public network, the source PE sends the switchover message to all receiver PEs. After receiving the switchover message, these receiver PEs send the (*, G) Join messages to the RP of the public network to establish the RPT. When the Switch-Group address is used in the VPN to encapsulate multicast data, the public network side of the source PE receives the data forwarded from the VPN based on the Switch-Group address. Then the forwarding entries are created on the source PE, and the source PE encapsulates the data in the Register messages which are sent to the RP of the public network. Then, the RP decapsulates the Register messages, and sends the data to the receiver PEs. Finally, the receiver PEs trigger the SPT switchover towards the source PE. In this manner, the SPT is established on the public network.

When there are many entries involved in SPT switchovers, the speed of sending Register messages is reduced. As a result, sending the first Register message to the RP takes a long time for certain entries, and establishing the SPT on the public network is delayed. In addition, in the process of establishing the SPT on the public network, multicast services are interrupted and certain VPN data may also be discarded, leading to the service interruption on the user end.

To address the preceding problems, disable the source PE from sending the null Register message to the RP and establishing a public network SPT before the Switch-Group address is used to encapsulate VPN data.

Prerequisites

A Share-Group has been configured using the **multicast-domain share-group binding** command.

Configuration Impact

After the VPN data traffic exceeds the upper limit, the source PE uses the Switch-Group address to encapsulate data and sends the switchover message to the receiver PEs. If the Switch-Group address is allocated for the first time, when sending the switchover message, the source PE sends the Register message that is encapsulated with the VPN Hello message to the RP, and the RP forwards the Register message to the receiver PEs. Based on the received messages, the receiver PEs and the RP directly send the (S, G) Join messages to the source PE and establish the SPT on the public network in advance. In this manner, when the public network tunnel is switched from the RPT to the SPT, the number of discarded multicast messages is reduced and the impact on multicast services is minimized.

Example

When the Switch-Group address is not used to encapsulate VPN data for mytest, configure the source PE to send the null Register message to the RP to establish the SPT on the public network.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance mytest
[HUAWEI-vpn-instance-mytest] route-distinguisher 11:11
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast routing-enable
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
[HUAWEI-vpn-instance-mytest-af-ipv4] multicast-domain switch-without-register
```

8.6.18 reset multicast-domain control-message counters

Function

The **reset multicast-domain control-message counters** command clears statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances.

Format

reset multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **control-message counters**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears statistics about sent and received MDT switch messages in a specified VPN instance. The parameter *vpn-instance-name* specifies the name of an existing VPN instance on the device.	The value must be an existing VPN instance name.
all-instance	Clears statistics about sent and received MDT switch messages in all VPN instances.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a fault occurs on a multicast VPN network, you need to check whether MDT switch messages are properly sent and received. If the current device already records a large number of statistics about MDT switch messages, you can run the **reset multicast-domain control-message counters** command to clear statistics about sent and received messages in a specified VPN instance or all VPN instances and then run the **display multicast-domain control-message counters** command to check whether the count of MDT switch messages increases, which helps fault location.

Precautions

Running the **reset multicast-domain control-message counters** command will clear all statistics about MDT switch messages. Therefore, exercise caution before using this command.

Example

Clear statistics about sent and received MDT switch messages in VPN instance **red**.

```
<HUAWEI> reset multicast-domain vpn-instance red control-message counters
```

8.6.19 service type (Eth-trunk interface view)

Function

The **service type multicast-tunnel** command configures an Eth-trunk interface as a multicast loopback interface.

The **undo service type multicast-tunnel** command cancels the configuration.

By default, an Eth-trunk interface is not configured as a multicast loopback interface.

Format

service type multicast-tunnel

undo service type multicast-tunnel

Parameters

None

Views

Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can receive the VPN multicast packets and use GRE to encapsulate them only after a multicast loopback interface has been configured.

Follow-up Procedure

Configure member interfaces of the multicast loopback interface using the **trunkport** command.

Precautions

- After you configure an interface as a multicast loopback interface, the switch automatically disables STP on this interface. The interface then does not support STP configuration commands. After the multicast loopback interface configuration is cancelled, the switch automatically enables STP on the interface.
- On the switch, only one Eth-Trunk interface can function as the multicast loopback interface. All VPN multicast packets are encapsulated on this interface into public network multicast data packets.
- The configurations allowed on an Eth-Trunk to be configured as a loopback interface include **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **traffic-policy (interface view)**, and **trust**. If other configurations exist on the Eth-Trunk, the Eth-Trunk cannot be configured as a loopback interface.
- After an Eth-Trunk is configured as a loopback interface, the Eth-Trunk supports only the following configurations: **authentication open ucl-policy enable**, **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **statistic enable (interface view)**, **traffic-policy (interface view)**, **vcmp disable**, and **trust**.

- Before disabling an Eth-Trunk interface from working as the multicast loopback interface, delete all member interfaces of the Eth-Trunk interface.
- If "Warning: ACL resources are insufficient when the physical interface is added to the multicast loopback interface, so the multicast VPN function may be abnormal." is displayed when you add a physical interface to a multicast loopback interface, resources on the multicast loopback interface are occupied by other services. To ensure normal running of services, delete this physical interface from the multicast loopback interface or delete unnecessary configurations, for example, unnecessary traffic policies.
- If an Eth-Trunk has been configured as a multicast VPN loopback interface, do not use the MIB to perform other service configuration on the Eth-Trunk. Otherwise, the multicast VPN loopback interface will become invalid or the service configuration issued by the MIB may not take effect.

Example

Configure Eth-Trunk 1 as a multicast loopback interface.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] service type multicast-tunnel
```

8.6.20 set multicast tunnel enhanced

Function

The **set multicast tunnel enhanced** command allows an Eth-Trunk that works as a multicast VPN loopback interface to have member interfaces from different cards.

The **undo set multicast tunnel enhanced** command forbids an Eth-Trunk that works as a multicast VPN loopback interface to have member interfaces from different cards.

By default, an Eth-Trunk that works as a multicast VPN loopback interface cannot have member interfaces from different cards.

Format

set multicast tunnel enhanced

undo set multicast tunnel enhanced

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an Eth-Trunk that works as a multicast VPN loopback interface have member interfaces from different member switches in a stack system, multicast VPN services can function properly if the switch where a member interface is located fails. This improves device reliability.

Follow-up Procedure

Run the **service type multicast-tunnel** command to configure an Eth-Trunk as a multicast VPN loopback interface.

Configuration Impact

After the **set multicast tunnel enhanced** command is executed, the number of ACLs for multicast VPN will increase if the Eth-Trunk that functions as a multicast VPN loopback interface contains more than one member interface from a device. The number of ACLs equals to the number of interfaces on a device configured as the member interfaces of an Eth-Trunk functioning as a multicast VPN loopback interface multiplied by the number of Mtunnel outbound interfaces for accessing the public network. For example, if two interfaces on a device are configured as member interfaces of the Eth-Trunk functioning as a multicast VPN loopback interface, and if the device is configured with four Mtunnel outbound interfaces for accessing the public network, a total of eight (2*4) ACLs will be used by multicast VPN services. If there are insufficient ACL resources, multicast VPN services cannot run properly.

Precautions

A multicast VPN loopback interface cannot be configured together with the **set multicast tunnel enhanced** and **undo set multicast tunnel enhanced** commands.

Example

Configure the Eth-Trunk that works as a multicast VPN loopback interface to allow member ports from different cards.

```
<HUAWEI> system-view
[HUAWEI] set multicast tunnel enhanced
```

8.7 IPv4 Multicast Route Management Commands

8.7.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.

Product	Support
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the multicast multi-instance feature.

8.7.2 display default-parameter mrm

Function

The **display default-parameter mrm** command displays the default configurations for multicast routing management (MRM).

Format

display default-parameter mrm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the default configurations, regardless of whether MRM parameters are changed. Therefore, you can use this command to check which parameters have been modified.

Example

Display default configurations for MRM.

```
<HUAWEI> display default-parameter mrm
 System View Default Configurations:
 ----------------------------------
 Load splitting rule: disabled
 Load-splitting-timer: 1800 s
 Route selection rule: preference-preferred
```

```
Multi-topology: disabled

Interface View Default Configurations:
--------------------------------------
Minimum TTL: 1
Reject inbound data: disabled
Reject outbound data: disabled
Multicast load-splitting weight: 1
```

Table 8-89 Description of the **display default-parameter mrm** command output

Item	Description
System View Default Configurations	Default configurations for multicast routing management (MRM) in the system view.
Load splitting rule	Whether multicast load splitting is configured. By default, multicast load splitting is not configured. To configure multicast load splitting, run the **multicast load-splitting** command.
Load-splitting-timer	Default value of the multicast load splitting balancing timer. By default, the value is 1800s. You can run the **multicast load-splitting-timer** command to set the value of the multicast load splitting balancing timer.
Route selection rule	RPF route selection rule. By default, RPF route selection is based on the preference of the routing protocol.
Interface View Default Configurations	Default configurations for multicast routing management (MRM) in the interface view.
Minimum TTL	Minimum TTL value for multicast packet forwarding.
Reject inbound data	Whether the interface is disabled from receiving multicast packets.
Reject outbound data	Whether the interface is disabled from forwarding multicast packets.
Multicast load-splitting weight	Multicast load splitting weight of the interface. By default, the multicast load splitting weight of an interface is 1. You can run the **multicast load-splitting weight** command to set the value of the multicast load splitting weight.

8.7.3 display migp routing-table

Function

The **display migp routing-table** command displays brief information about the MIGP routing table.

Format

display migp routing-table [*ip-address* [*mask-length* | *mask*]] [**verbose**]

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Indicates a mask.	The mask is in dotted decimal notation.
mask-length	Specifies the length of the mask.	The value is a decimal integer ranging from 0 to 32.
verbose	Displays detailed information about active routes and inactive routes. If the parameter is not specified, only brief information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the MIGP routing table. You can specify parameters in the command to view specified routes.

Example

Display brief information about the MIGP routing table.

```
<HUAWEI> display migp routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
```

```
Routing Tables: MIGP
         Destinations : 4        Routes : 4

Destination/Mask    Proto  Pre  Cost     Flags NextHop         Interface

10.4.4.4/32        OSPF   10   3             10.0.1.1        Vlanif100
10.5.5.5/32        OSPF   10   4             10.0.1.1        Vlanif100
10.0.3.0/24        OSPF   10   3             10.0.1.1        Vlanif100
192.168.3.0/24      OSPF   10   4             10.0.1.1        Vlanif100
```

Table 8-90 Description of the **display migp routing-table** command output

Item	Description
Route Flags	Flag of a route: ● R: indicates that the route is a recursive route. ● D: indicates that the route is delivered to the FIB table. ● T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: MIGP	MIGP routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol that learns a route.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

Display detailed information about the MIGP routing table.

```
<HUAWEI> display migp routing-table verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Table : MIGP
         Destinations : 5        Routes : 5


Destination: 10.4.4.4/32
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 20
      NextHop: 10.0.1.1          Interface: Vlanif100
```

```
        State: Active Adv             Age: 00h34m26s

Destination: 10.5.5.5/32
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 30
      NextHop: 10.0.1.1         Interface: Vlanif100
        State: Active Adv             Age: 00h34m26s

Destination: 10.0.2.0/24
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 20
      NextHop: 10.0.1.1         Interface: Vlanif100
        State: Active Adv             Age: 00h34m26s

Destination: 10.0.3.0/24
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 30
      NextHop: 10.0.1.1         Interface: Vlanif100
        State: Active Adv             Age: 00h34m27s

Destination: 192.168.3.0/24
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 40
      NextHop: 10.0.1.1         Interface: Vlanif100
        State: Active Adv             Age: 00h34m28s
```

Table 8-91 Description of the **display migp routing-table** verbose command output

Item	Description
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol that learns a route.
Process ID	Process ID of the routing protocol.
Preference	Preference of a route.
Cost	Indicates the route cost.
NextHop	Next hop of a route.
Interface	Outbound interface of a route.

Item	Description
State:	Status of routes, which can be: ● Active: indicates routes in the Active state. ● Invalid: indicates invalid routes. ● Inactive: indicates routes in the Inactive state. ● NoAdv: indicates routes that cannot be advertised. ● Adv: indicates routes that can be advertised. ● Del: indicates routes to be deleted. ● GotQ: indicates routes that are relayed successfully. ● WaitQ: indicates routes that are not relayed successfully yet. ● Stale: indicates routes with the Stale flag. The routes are used in GR.
Age	Time that elapsed since a route is generated.

8.7.4 display migp routing-table statistics

Function

The **display migp routing-table statistics** command displays the statistics about the MIGP routing table.

Format

display migp routing-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Integrated route statistics contain the total number of routes added or deleted through protocols and the total number of active or inactive routes with deletion flags but are not deleted.

Example

Display the statistics about routes in the MIGP routing table.

```
<HUAWEI> display migp routing-table statistics
Proto     total      active      added        deleted      freed
         routes     routes      routes       routes       routes
OSPF      0           0           0            0            0
IS-IS     5           5           45           40           40
Total     5           5           45           40           40
```

Table 8-92 Description of the **display migp routing-table statistics** command output

Item	Description
Proto	Routing protocol.
total routes	Total number of routes in the current routing table.
active routes	Number of active routes in the routing table.
added routes	Number of routes (active and inactive) added to the routing table.
deleted routes	Number of routes deleted from the routing table.
freed routes	Number of released routes that are deleted permanently from the routing table.

8.7.5 display mrt routing-table

Function

The **display mrt routing-table** command displays MRT routes.

Format

display mrt routing-table [**vpn-instance** *vpn-instance-name*] [*ip-address* [*mask* | *mask-length*]] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Specifies mask.	The mask is in dotted decimal notation.
mask-length	Specifies mask length.	It is an integer ranging from 0 to 32.
verbose	Displays detailed information about active and inactive routes. If the parameter **verbose** is not specified, detailed information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view specific routing information.

Example

Display information about all MRT routes.

```
<HUAWEI> display mrt routing-table
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Tables: MRT
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags  NextHop  Interface

  10.5.5.1/32     MSR    255     0     R   10.1.1.1  Vlanif100
```

Table 8-93 Description of the **display mrt routing-table** command output

Item	Description
Route Flags	Flag of a route: - R: indicates that the route is a recursive route. - D: indicates that the route is delivered to the FIB table. - T: indicates a route whose next hop belongs to a VPN instance.
Routing Tables: MRT	IMRT routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Protocol that learns a route.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

Display the detailed information of the specified routes.

```
<HUAWEI> display mrt routing-table 10.12.12.12 verbose
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Routing Table : MRT
Summary Count : 1

Destination: 10.12.12.12/32
     Protocol: MSR            Process ID: 0
   Preference: 1                    Cost: 0
      NextHop: 10.11.11.12     Neighbour: 0.0.0.0
        State: Active Adv Relied     Age: 00h04m49s
          Tag: 0                Priority: low
        Label: NULL              QoSInfo: 0x0
   IndirectID: 0x80000002
 RelayNextHop: 0.0.0.0         Interface: Vlanif100
     TunnelID: 0x0                 Flags: R
```

Table 8-94 Description of the **display mrt routing-table verbose** command output

Item	Description
Routing Table: MRT	MRT routing table.

Item	Description
Summary Count	Number of the destination network and host.
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol that learns a route.
Process ID	Process ID of the routing protocol.
Preference	Route preference.
Cost	Route cost.
NextHop	Next hop of a route.
Neighbour	Address of the neighbor.
State	Status of routes: ● Active: indicates active routes. ● Invalid: indicates invalid routes. ● Inactive: indicates inactive routes. ● NoAdv: indicates the routes that cannot be advertised. ● Adv: indicates the routes that can be advertised. ● Del: indicates the routes to be deleted. ● Relied: indicates the route that finds the next hop and outbound interface or the route that finds the tunnel during packet forwarding. ● WaitQ: indicates the route that does not find the next hop or outbound interface or the route that does not find the tunnel. ● Stale: indicates the routes with the stale flag. The routes are used in GR.
Age	Time that elapsed since a route is generated.
Tag	Administrative tag for routes.
Priority	Priority of a route.
Label	MPLS label allocated to a route.
QoSInfo	QoS information.
IndirectID	ID of the indirect next hop.
RelayNextHop	Relay next hop.
Interface	Outbound interface through which the next hop is reachable.
TunnelID	Tunnel ID.

Item	Description
Flags	Route flags in the header of the routing table.

8.7.6 display mrt routing-table statistics

Function

The **display mrt routing-table statistics** command displays statistics about the MRT routes.

Format

display mrt routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted by the protocol
- Number of active or inactive routes that are tagged for deletion but not deleted

Example

Display statistics about routes in the MRT routing table.

```
<HUAWEI> display mrt routing-table statistics
Proto     total      active      added       deleted      freed
          routes     routes      routes      routes       routes
MSTATIC   1          0           1           0            0
```

Table 8-95 Description of the **display mrt routing-table statistics** command output

Item	Description
Proto	Routing protocol.
total routes	Total number of routes in the routing table.
active routes	Number of active routes in the routing table.
added routes	Number of active and inactive routes added in the routing table.
deleted routes	Number of routes to be deleted from the routing table.
freed routes	Number of routes that are permanently deleted from the routing table.

8.7.7 display mrt routing-table vpn-instance

Function

The **display mrt routing-table vpn-instance** command displays the MRT routing table of a VPN instance.

Format

display mrt routing-table vpn-instance *vpn-instance-name* [*ip-address* [*mask* | *mask-length*] [**longer-match**]] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Specifies mask.	The mask is in dotted decimal notation.
mask-length	Specifies mask length.	The value is a decimal integer that ranges from 0 to 32.
longer-match	Displays only routes that match the specified network or mask.	-
verbose	Displays detailed information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

Example

Display the MRT routing table of the IPv4 VPN instance named vpn1.

```
<HUAWEI> display mrt routing-table vpn-instance vpn1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: MSR
        Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags  NextHop  Interface

  10.5.5.1/32     MSR    255    0     R    10.1.1.1    Vlanif100
```

Table 8-96 Description of the **display mrt routing-table vpn-instance** command output

Item	Description
Route Flags	Route flag that identifies the attribute of a route. ● R: indicates an iterated route. ● D: indicates that the route is downloaded to the FIB table.
Routing Tables: MSR	MRT routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Protocol through which routes are learned.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

8.7.8 display mtrace statistics

Function

The **display mtrace statistics** command displays statistics about multicast trace (Mtrace) packets.

Format

display mtrace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To collect statistics about Mtrace traffic generated in a certain period, clear the original statistics.

Example

Display statistics about the current Mtrace traffic.

```
<HUAWEI> display mtrace statistics
Mtrace statistics:
 Type         Send        Receive        Invalid
 Query         10          5              0
 Request        20          4              0
 Response      3           7              1
```

Table 8-97 Description of the **display mtrace statistics** command output

Item	Description
Type	Indicates the types of Mtrace packets. The types are as follows: ● Query: IGMP-Tracert-Query packets. ● Request: IGMP-Tracert-Request packets. ● Response: IGMP-Tracert-Response packets.
Send	Indicates the number of sent packets.
Receive	Indicates the number of received packets.
Invalid	Indicates the number of invalid packets.

8.7.9 display multicast boundary

Function

The **display multicast boundary** command displays the multicast boundary configured on an interface.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
group-address	Specifies a multicast group address.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of the multicast group address.	The mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast group address.	The value is a decimal integer that ranges from 4 to 32.
interface *interface-type interface-number*	Specifies the type and the number of an interface. The parameter is used to specify an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to check the boundary of a PIM-SM network. When some hosts cannot receive multicast data, you can use this command to check whether the problem is caused by multicast boundary configuration.

Example

Display the boundaries configured on all the interfaces.

```
<HUAWEI> display multicast boundary
Multicast boundary information
Total 1 Multicast IPv4 boundary
 Interface           Boundary
 Vlanif100            225.1.1.0/24
```

Table 8-98 Description of the **display multicast boundary** command output

Item	Description
Multicast boundary information of	multicast boundary information.
Total 1 Multicast IPv4 boundary	Total number of multicast boundaries configured on a switch.
Interface	Interface configured with a multicast boundary.
Boundary	Information about the multicast boundary address.

8.7.10 display multicast forwarding-table

Function

The **display multicast forwarding-table** command displays the multicast forwarding table.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | { **statistics** | **verbose** }] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
group-address	Specifies a multicast group address.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast address or source address.	-
group-mask	Specifies the mask of the multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of the multicast group address.	The value is a decimal integer that ranges from 4 to 32.
source-address	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
source-mask	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is a decimal integer that ranges from 0 to 32.
incoming-interface	Indicates the inbound interface of a multicast forwarding entry.	-
interface-type interface-number	Specifies the type and the number of an interface.	-
register	Indicates the register interface of PIM-SM.	-
outgoing-interface	Indicates the outbound interface of a multicast forwarding entry.	-

Parameter	Description	Value
include	Displays the (S, G) entry list that contains the specified downstream interface.	-
exclude	Displays the (S, G) entry list that does not contain the specified downstream interface.	-
match	Displays the (S, G) entry list that matches the specified interface and the (S, G) entries have only one specified interface.	-
none	Indicates that the downstream interface list is null.	-
verbose	Displays the detailed information about the multicast forwarding table.	-
statistics	Displays the statistics about the multicast forwarding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During multicast routing and forwarding, routing information generated by multicast routing protocols is saved in a multicast routing table. The switch selects the optimal multicast routes from the routing table according to multicast routing and forwarding policies, and then delivers the selected multicast routes to the multicast forwarding table to guide multicast data forwarding.

You can use the **display multicast forwarding-table** command to check whether multicast forwarding entries have been generated and whether multicast data can be forwarded normally.

Example

Display the multicast forwarding table.

```
<HUAWEI> display multicast forwarding-table
Multicast Forwarding Table of VPN-Instance: public net
```

```
Total 1 entry, 1 matched

00001. (10.10.10.2, 225.0.0.1)
     MID: 0, Flags: ACT
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Vlanif10
     List of 1 outgoing interfaces:
       1:  Vlanif20
           Activetime: 00:23:15
     Matched 154 packets(15378 bytes), Wrong If 0 packets
     Forwarded 154 packets(15378 bytes)
```

Table 8-99 Description of the **display multicast forwarding-table** command output

Item	Description
Multicast Forwarding Table of VPN-Instance: public net	VPN instance to which the multicast forwarding table corresponds. **public net** indicates the public network instance.
Total 1 entry, 1 matched	Total number of forwarding entries and number of eligible forwarding entries.
00001	Sequence number of the (S, G) entry.
(10.10.10.2, 225.0.0.1)	(S, G) entry in the multicast forwarding table.
MID	Uniquely identifies the multicast forwarding entry in the MFIB table. MID is used to rapidly search the multicast forwarding table.

Item	Description
Flags	Indicates the status flag of the (S, G) entry. ● ACT: indicates that an active event is triggered. ● DUM: indicates a dummy entry. ● MISS: indicates that the nocache time needs to be reported. ● DROP: indicates packet dropping. ● LTH: indicates that the traffic volume is below the threshold. ● DEL: indicates a deleted entry. ● RST: indicates that registration of the known timer is started. ● 2SYNC: indicates that the entry is contained in the MFIB table but it does not exist on the device. ● 2ADD: indicates that the entry existing on the device has not been added to the MFIB table. ● CLR: indicates that the MFIB table is resetting. ● L2FWD: indicates that the device forwards Layer 2 traffic in multicast mode. ● 2ACK: indicates that the VPN instance is waiting for the ACK message from the slave main control board. ● 2RSED: indicates that the entry is waiting for retransmission. ● BKCLR: indicates that the MFIB table on the slave main control board is resetting. ● 2DEL: indicates that the entry deleted from the device has not been removed from the MFIB table. ● PDEL: indicates that the entry does not exist on the device. ● A denotes addition; D denotes deletion; I denotes upstream update; R denotes RP update; P denotes PMBR; F denotes flag. ● S denotes SPT; E denotes encapsulation group update; US denotes status update; CS denotes status clearing.
Uptime	Period duration of the (S, G) entry.
Timeout in	Remaining time of the (S, G) entry.
Incoming interface	Upstream interface of the (S, G) entry.
List of 1 outgoing interfaces	Downstream interface list. The contents of the downstream interface list are as follows: ● Name and number of the outbound interface ● The existing time of outbound interface

Item	Description
Matched 154 packets(15378 bytes)	Number of multicast packets and bytes matching the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.
Wrong If 0 packets	Number of multicast packets matching the (S, G) entry but are not forwarded. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.
Forwarded 154 packets(15378 bytes)	Number of packets and bytes forwarded by the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.

8.7.11 display multicast forwarding-table optimization-mode configuration

Function

The **display multicast forwarding-table optimization-mode configuration** command displays the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

display multicast forwarding-table optimization-mode configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, configurations of all slots are displayed.	The value is an integer and must be the slot ID of a running slot.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to display the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored. The configuration helps you select a slot based on your storage requirement.

Example

Display the configuration of the optimization modes.

```
<HUAWEI> display multicast forwarding-table optimization-mode configuration
Multicast forwarding-table optimization mode :
Slot      Mode
-------------------------
2         Normal mode
4         Normal mode
5         Rich MCast mode
```

Table 8-100 Description of the **display multicast forwarding-table optimization-mode configuration** command output

Item	Description
Multicast forwarding-table optimization mode	When the multicast optimization mode is enabled.
slot	Slot ID.
mode	Storage Mode. The following storage modes are available: ● Normal: The ARP cache table or ND cache table and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table. ● Rich MCast mode: also known as multicast optimization mode. The system allocates hardware resources preferentially to the multicast forwarding table. The ARP/ND cache table and routing table share hardware resources.

8.7.12 display multicast routing-table

Function

The **display multicast routing-table** command displays information about a multicast routing table.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

display multicast routing-table [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **vpn-instance** *vpn-instance-name* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Specifies all the instances.	-
group-address	Indicates the multicast group address.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask { *group-mask* | *group-mask-length* }	Indicates the mask of the multicast group address.	● *group-mask*: The address is in dotted decimal notation. The value ranges from 240.0.0.0 to 255.255.255.255. ● *group-mask-length*: The value is an integer that ranges from 4 to 32
source-address	Indicates the multicast source address.	The address is in dotted decimal notation.

Parameter	Description	Value
mask { *source-mask* | *source-mask-length* }	Indicates the mask of the specified source address.	● *source-mask*: The address is in dotted decimal notation. The value ranges from 0.0.0.0 to 255.255.255.255. ● *source-mask-length*: The value is an integer that ranges from 0 to 32
incoming-interface	Indicates the upstream interface of a multicast routing entry.	-
interface-type interface-number	Indicates the type and the number of an interface.	-
register	Indicates the register interface of a multicast routing entry.	-
outgoing-interface	Indicates the downstream interface of a multicast routing entry.	-
include	Indicates the (S, G) entries whose downstream interface list contains specified downstream interfaces.	-
exclude	Indicates the (S, G) entries whose downstream interface list does not contain specified downstream interfaces.	-
match	Indicates (S, G) entries whose the downstream interface list contains only one interface that is the same as a specified downstream interface.	-
none	Indicates that the downstream interface list is null.	-

Parameter	Description	Value
outgoing-interface-number	Indicates the number of downstream interfaces of multicast routing entries.	-
number	Specifies the number of downstream interfaces.	The value is an integer that ranges from 0 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast routing-table** command is used to display the information of a multicast routing table.

Example

Display the corresponding routing entry of a multicast group in the multicast routing table.

```
<HUAWEI> display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry
 00001. (192.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: Vlanif10
       List of 2 downstream interfaces
           1:  Vlanif20
           2:  Vlanif30
```

Table 8-101 Description of the **display multicast routing-table** command output

Item	Description
Multicast routing table of VPN-Instance	VPN instance to which the multicast routing information corresponds. **public net** indicates the public network instance.
Total 1 entry	Number of eligible routing entries.
00001	Sequence number of the (S, G) entry.
(192.168.0.2, 227.0.0.1)	(S, G) entry in the multicast routing table.
Uptime	Time that elapsed since the (S, G) entry was generated.

Item	Description
Upstream Interface	Upstream interface of the (S, G) entry.
List of 2 downstream interfaces	Downstream interface list.

Display the number of downstream interfaces of the multicast routing entries.

```
<HUAWEI> display multicast routing-table outgoing-interface-number
Multicast routing table
 Total 2 entries

 00001. (10.1.1.22, 232.1.1.1)
       Uptime: 00:00:07
       Upstream Interface: Vlanif10
       List of 20 downstream interfaces

 00002. (10.1.1.22, 232.1.2.1)
       Uptime: 00:00:07
       Upstream Interface: Vlanif20
       List of 20 downstream interfaces
```

Table 8-102 Description of the display multicast routing-table outgoing-interface-number command output

Item	Description
List of 20 downstream interfaces	Number of downstream interfaces in multicast routing entries.

8.7.13 display multicast routing-table static

Function

The **display multicast routing-table static** command displays the multicast static routes.

Format

display multicast routing-table [**vpn-instance** *vpn-instance-name*] **static** [**config**] [*source-address* { *mask* | *mask-length* }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
config	Displays the configuration of the multicast static routes.	-

Parameter	Description	Value
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
mask	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether multicast RPF static routes are configured successfully, run the **display multicast routing-table static** command.

If the multicast static route configured on the local switch cannot be displayed, use the **ip rpf-route-static** command to configure multicast static routes.

Example

Display all multicast static routes on the switch.

```
<HUAWEI> display multicast routing-table static
Multicast Routing Table
Routes : 1

 Mroute 10.1.0.0/24
         Interface = Vlanif100       RPF Neighbor = 10.1.2.2
         Matched routing protocol = ospf, process-id = 100, Route-policy = none
         Preference = 1, Order = 1
 Running Configuration = ip rpf-route-static 10.1.0.0 24 ospf 100 10.1.2.2 order 1
```

Table 8-103 Description of the **display multicast routing-table static** command output

Item	Description
Multicast Routing Table	Multicast routing table.
Routes	Number of routes.
Mroute	Source address and mask length of a multicast route.
Interface	Outbound interface of the reachable multicast source.
RPF Neighbor	Neighbor IP address through which the source address is reachable.

Item	Description
Matched routing protocol	Matching unicast route type, which can be: ● IS-IS ● RIP ● OSPF ● BGP ● Unicast static route
process-id	Process ID of a routing protocol.
Route-policy	Routing policy. The source address of a route must match the routing policy.
Preference	Preference of a route.
Order	Order of a route.
Running Configuration	Command line for configuring a static route.

8.7.14 display multicast rpf-info

Function

The **display multicast rpf-info** command displays the Reverse Path Forwarding (RPF) routes of a specified IPv4 multicast source or source/group.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
source-address	Specifies the address of a multicast source, used to display the information of RPF routing corresponding to the source.	The address is in dotted decimal notation.

Parameter	Description	Value
group-address	Specifies the multicast group address, used to display the information of RPF routing corresponding to the source/group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
rpt	Displays the RPF routing information corresponding to a specified source or source/group on the shared RP-tree.	-
spt	Displays the RPF routing information corresponding to a specified source or source/group on the shortest path tree.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The RPF route with the *source-address* as the destination address is an optimal route selected from unicast routes, multicast static routes, MBGP routes, and MIGP routes. You can use the **display multicast rpf-info** command to check the RPF route to the specified source or source-group.

Example

Display all RPF routes to the source address 192.168.0.1.

```
<HUAWEI> display multicast rpf-info 192.168.0.1
 VPN-Instance: public net
 RPF information about source: 192.168.0.1
     RPF interface: Vlanif100, RPF neighbor: 10.1.5.2
     Referenced route/mask: 192.168.0.0/24
     Referenced route type: unicast
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 8-104 Description of the **display multicast rpf-info** command output

Item	Description
RPF information about source	Multicast source to which the multicast RPF path belongs.
RPF interface	RPF interface.
RPF neighbor	RPF neighbor.
Referenced route/mask	Referenced route and its mask.

Item	Description
Referenced route type	Referenced route types: - unicast: unicast routes - MBGP: MBGP routes - mstatic: multicast static routes - MIGP: MIGP routes
Route selection rule	RPF route selection rules: - preference-preferred: selecting routes based on the preference of the routing protocols - longest-match: selecting routes based on the longest matching rule
Load splitting rule	Load splitting rules: - disable: load splitting disabled. - balance-preferred: load balancing preferred. - stable-preferred: stable-preferred load splitting. - source: load splitting based on source addresses. - group: load splitting based on group addresses. - source-group: load splitting based source and group addresses.

8.7.15 ip rpf-route-static

Function

The **ip rpf-route-static** command configures a multicast static route.

The **undo ip rpf-route-static** command deletes a multicast static route.

By default, no multicast static route is configured.

Format

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] { *interface-type interface-number* | *gateway-address* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] { *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value must be an existing VPN instance name.
source-address	Specifies the address of a multicast source.	The address is in dotted decimal notation.
mask	Indicates the address mask of the multicast source.	The address mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast source address.	The value is a decimal integer that ranges from 0 to 32.
isis *process-id*	Specifies that matched routes must be generated by the IS-IS protocol. *process-id* indicates the IS-IS process ID.	The value is a decimal integer that ranges from 1 to 65535.
ospf *process-id*	Specifies that matched routes must be generated by the OSPF protocol. *process-id* indicates the OSPF process ID.	The value is a decimal integer that ranges from 1 to 65535.
rip *process-id*	Specifies that matched routes must be generated by the RIP protocol. *process-id* indicates the RIP process ID.	The value is a decimal integer that ranges from 1 to 65535.
bgp	Specifies that matched routes must be generated by the BGP protocol.	-
static	Specifies that matched routes must be static routes.	-
route-policy *route-policy-name*	Indicates the matching rule of multicast static routes. *route-policy-name* specifies the name of a route matching rule.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
gateway-address	Specifies the address of the gateway.	-
order *order-number*	Indicates the configuration order of routes in the same network segment.	The value is a decimal integer that ranges from 1 to 100.
preference *preference*	Indicates the preference of routes. The greater the value is, the lower the preference is.	The value is a decimal integer that ranges from 1 to 255. By default, it is 1.
all	Indicates all multicast static routes in the multicast static routing table.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast static route specifies an RPF interface or RPF neighbor for multicast packets from a specified multicast source. You can configure a multicast static route to:

- Change an RPF route.

  If you want an interface to receive multicast data packets from a specified multicast source but the interface is not the RPF interface for the multicast source, configure a multicast static route to specify this interface as the RPF interface for the multicast source. When the switch receives multicast data packets from the multicast source, it performs an RPF check using the configured RPF route. Packets sent from the source to the switch through other interfaces fail the RPF check.

- Connect RPF routes.

  If the unicast route on a network segment is incomplete, multicast packets cannot be forwarded due to the lack of an RPF route. For example, when two adjacent devices run different routing protocols and the routing protocols do not import routes from each other, packets cannot be forwarded between the two devices. In this case, you can configure RPF static routes on the devices. The devices can perform RPF checks using the specified RPF interfaces so that multicast packets can be forwarded successfully.

Precautions

- If you specify a protocol type in the **ip rpf-route-static** command, the switch compares the configured multicast static route with the unicast routes of the specified protocol. If protocol types of the optimal unicast route and the multicast static route are different, the switch selects the optimal unicast route as the RPF route.
- A multicast static route is identified by three elements: *source-address* { *mask* | *mask-length* }, protocol type, and *route-policy-name*. Two multicast static routes are considered different as long as one element has different values in the two routes. A maximum of eight multicast static routes can be configured on a network segment.
- If the next-hop interface of a multicast static route is a P2P interface, you can specify the next-hop interface in the command. If the next-hop interface is not a P2P interface, you must specify the next-hop address.
- A multicast static route may not take effect after you configure it using the **ip rpf-route-static**, because the specified interface is Down. After configuring a multicast static route, you are advised to run the **display multicast routing-table static** command to check whether the route is configured successfully and takes effect.

Example

Configure a multicast static route.

```
<HUAWEI> system-view
[HUAWEI] ip rpf-route-static 10.0.0.0 255.0.0.0 rip 1 route-policy map1 10.10.0.1
```

8.7.16 mtrace

Function

The **mtrace** command detects the multicast path or RPF path from a multicast source to the querier or to a destination host. The querier indicates the switch on which the **mtrace** command is executed.

Format

mtrace -gw *last-hop-router* **-r** *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-a** *source-ip-address* | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace -b -r *receiver* **-g** *group* [[**-mr** | **-ur** *resp-dest*] | **-a** *source-ip-address* | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace -d -r *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-a** *source-ip-address* | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace -r *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

mtrace [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-l** [[*stat-times*] [**-st** *stat-int*]] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

Parameters

Parameter	Description	Value
-l	Performs Mtrace tracking for multiple times, collects traffic statistics and rate, uses detailed display mode, and ignores the configuration of **-v**.	If **-l** is not specified, Mtrace tracking is performed once.
stat-times	Indicates the number of times for Mtrace tracking.	The value is an integer that ranges from 2 to 65535. If **-l** is specified while *stat-times* is not specified, Mtrace tracking stops after it is performed 65535 times.
-st *stat-int*	Sets the interval at which the rate is calculated during cyclic query.	The value is an integer that ranges from 10 to 60, in seconds. The default value is 10. To configure **-st**, configure **-l** first. In addition, the cyclic count must be greater than or equal to 2.
-m *max-ttl*	Specifies the maximum number of hops to be traced.	The value is an integer that ranges from 1 to 255. The default value is 255.
-mr	Indicates that the response address is specified as the traced multicast group address.	The **-mr** is applicable only when the querier resides in a multicast distribution tree.
-q *nqueries*	Sets the number of retry times of mtrace.	The value is an integer that ranges from 1 to 65535. The default value is 3.

Parameter	Description	Value
-tr *ttl*	Specifies the TTL value of the IGMP Tracert Response messages sent in multicast mode.	The value is an integer that ranges from 1 to 255. The default value is 30.
-ts *ttl*	Sets the maximum number of hops to be traced in hop-by-hop mode.	The value is an integer that ranges from 1 to 255. The default value is 30. When Mtrace in max-hop mode fails, Mtrace automatically enters the hop-by-hop mode. The number of hops increases by one each time a new hop is traced.
-ur *resp-dest*	Specifies the response address as a unicast address. The value of *resp-dest* must be a local interface address. **NOTE** If neither **-mr** nor **-ur** *resp-dest* is specified, multicast address 224.0.1.32 is used as the response address.	-
-v	Sets the detailed mode and exports time and statistics.	-
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
-w *timeout*	Specifies the timeout period to wait for an IGMP Tracert Response message.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 3.
-g *group*	Specifies the multicast group address to be traced.	The address cannot be a reserved group address.
-gw *last-hop-router*	Specifies the last-hop switch address, which ensures that unicast packets can be transmitted between the querier and the last-hop switch. After this parameter is specified, the initiating mode of Mtrace is specified as last-hop.	-

Parameter	Description	Value
-d	Indicates that unicast packets can be transmitted between the querier and the destination host. After this parameter is specified, the initiating mode of Mtrace is specified as destination.	-
-r *receiver*	Specifies the destination host address.	The value is in dotted decimal notation.
-a *source-ip-address*	Specifies the source address of an IGMP Tracert Query message. The value of *source-ip-address* must be a local interface address. **NOTE** When you need to detect the multicast path or the RPF path from the multicast source to the querier, **-a** is not supported.	The value is in dotted decimal notation.
-b	Indicates that the querier is directly connected to the destination host, but whether the querier is the last-hop switch is unknown. After this parameter is specified, the initiating mode of Mtrace is specified as all-router. **NOTE** After a VPN or RPF is specified, the initiating mode of Mtrace cannot be specified as all-router.	-
source *source-address*	Specifies the multicast source address.	The value is in dotted decimal notation.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

During multicast troubleshooting and routine maintenance, you can run the **mtrace** command to collect traffic information for locating faulty nodes, which helps reduce configuration errors, perform cyclic tracert, and collect statistics on multicast flow rates.

The **mtrace** command format varies according to the types of paths.

- **mtrace source** *source-address*: detects the RPF path from the multicast source to the querier.
- **mtrace -g** *group* **source** *source-address*: detects the multicast path from the multicast source to the querier.

  The corresponding (S, G) entry must exist on the querier.
- **mtrace** [**-gw** *last-hop-router* | **-d**] **-r** *receiver* **source** *source-address*: detects the RPF path from the multicast source to the destination host.
  - The querier is directly connected to the destination host, or the querier can ping the last-hop switch or detonation host in unicast mode.
  - When multiple switches are connected to the specified host, RPF paths from different switches can be different. You can specify the last-hop switch using **-gw** *last-hop-router* to uniquely define an RPF path.
- **mtrace** [**-b** | **-gw** *last-hop-router* | **-d**] **-r** *receiver* **-g** *group* **source** *source-address*: detects the multicast path from the multicast source to the destination host.

  The corresponding (S, G) entry must exist on the querier. In addition, one of the following conditions must be met:
  - The querier is directly connected to the destination host.
  - The querier can ping the last-hop switch or the destination host in unicast mode.
  - The querier resides in the multicast path from the multicast source to the destination host. For example, the querier is the first hop switch.

When running the **mtrace** [**-b** | **-gw** *last-hop-router* | **-d**] **-r** *receiver* **-g** *group* **source** *source-address* command to detect the multicast path from a multicast source to a destination host, specify **-gw** *last-hop-router*, **-b** or **-d**, which helps implement tracking quickly and accurately.

- **-b**: indicates that the querier is directly connected to the destination host.
- **-gw** *last-hop-router*: specifies the last-hop switch address. Unicast packets can be transmitted between the querier and the last-hop switch.
- **-d**: indicates that unicast packets can be transmitted between the querier and the destination host.
- If none of the preceding three parameters are specified, Mtrace fails unless the querier resides in the multicast path from the multicast source to the destination host.

Precautions

- According to draft-fenner-traceroute-ipm-01, the Router Alert option needs to be carried in the IGMP Tracert Query messages that are sent to the destination address in unicast mode and in the IGMP Tracert Response messages that sent in response in multicast mode. However, manufacturers have not reached an agreement on this issue. Packets sent from a Huawei switch carry the Router Alert option. If Huawei switches need to communicate with devices that do not support the Router Alert option, use **-gw** to specify the last-hop address and **-ur** to specify the unicast response address.

- The parameter **vpn-instance** is used on the PE to initiate a multicast VPN probe.
- If the destination address of an IGMP Tracert Response message is a multicast address, the device sends the message to all PIM-enabled interfaces (except the interface that receives the message). The message is then looped back on the ring network until the TTL value becomes 0, upon which time the message is discarded.

Example

- Detect the RPF path from a multicast source to the querier.

Detect the RPF path from the multicast source 10.1.0.1 to the querier 10.1.5.1.

```
<HUAWEI> mtrace source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace reverse path to source (10.1.0.1) according to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute finished.
```

Detect the RPF path from the multicast source 10.1.0.1 to the querier 10.1.5.1. The unicast response address is 10.1.5.1, and the maximum number of hops to be traced in hop-by-hop mode is 2.

```
<HUAWEI>mtrace -ur 10.1.5.1 -ts 2 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace reverse path to source (10.1.0.1) accordin
g to RPF rules *  *  *
 Switch from max hop mode to hop-by-hop mode
 In hop-by-hop mode, current probe hops is: 1
 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 In hop-by-hop mode, current probe hops is: 2
 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
  In hop-by-hop mode, the current trace hops is equal to the specified max hops,
 hops is 2,and multicast traceroute finished.
```

- Detect the multicast path from a multicast source to the querier.

Detect the multicast path from the multicast source 10.1.0.1 to the querier 10.1.5.1. The group address is 225.0.0.1, the cyclic count is 2, and the interval at which the rate is calculated is 10s.

```
<HUAWEI> mtrace -g 225.0.0.1 -l 2 -st 10 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table
 In calculating-rate mode, current statistic times is: 1

 -1 10.1.5.1
   Incoming Interface Address: 10.1.5.1 Input packets rate: 0
   Outgoing Interface Address: 0.0.0.0 Output packets rate: 0xffffffff
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -2 10.1.2.1
   Incoming Interface Address: 10.1.2.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.5.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
```

```
-3 10.1.0.1
  Incoming Interface Address: 10.1.0.1 Input packets rate: 0
  Outgoing Interface Address: 10.1.2.2 Output packets rate: 0
  Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
*******************************************************
 In calculating-rate mode, reach the demanded number of statistic,and multicast
 traceroute finished.
```

- Detect the RPF path from the multicast source to the destination host.

Detect the RPF path from the multicast source 10.1.0.1 to the destination host 10.1.6.4. The last hop address is 10.1.6.3, unicast packets can be transmitted, and the time and statistics are displayed in detail.

```
<HUAWEI> mtrace -gw 10.1.6.3 -r 10.1.6.4 -v source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace reverse path to source (10.1.0.1) according to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.6.4
 -1   10.1.5.1        1      PIM
   Incoming Interface Address: 10.1.5.1
   Outgoing Interface Address: 10.1.6.3
   Previous-Hop Router Address: 10.1.5.2
   Input packet count on incoming interface: 0
   Output packet count on outgoing interface: 0
   Total number of packets for this source-group pair: 0xffffffff
   Forwarding TTL: 1
   Forwarding Code: NO_ERROR
 -2   10.1.2.1        1      PIM
   Incoming Interface Address: 10.1.2.1
   Outgoing Interface Address: 10.1.5.2
   Previous-Hop Router Address: 10.1.2.2
   Input packet count on incoming interface: 0
   Output packet count on outgoing interface: 0
   Total number of packets for this source-group pair: 0xffffffff
   Forwarding TTL: 1
   Forwarding Code: NO_ERROR
 -3   10.1.0.1        1      PIM
   Incoming Interface Address: 10.1.0.1
   Outgoing Interface Address: 10.1.2.2
   Previous-Hop Router Address: 0.0.0.0
   Input packet count on incoming interface: 0
   Output packet count on outgoing interface: 0
   Total number of packets for this source-group pair: 0xffffffff
   Forwarding TTL: 1
   Forwarding Code: NO_ERROR
  In maximum-hop mode, received the response message, and multicast traceroute finished.
```

- Detect the multicast path from the multicast source to the destination host.

Detect the multicast path from the multicast source 10.1.0.1 to the destination 225.0.0.1. The destination host address is 10.1.6.4, the querier is directly connected to the destination host, the response address is the default value 224.0.1.32, and the TTL value of a Response packet is 5.

```
<HUAWEI> mtrace -b -r 10.1.6.4 -g 225.0.0.1 -tr 5 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.6.4
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
 -3   10.1.0.1        1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute finished.
```

Detect the multicast path from the multicast source 10.1.0.1 to the destination 225.0.0.1. The destination host address is 10.1.6.4, the last hop address is 10.1.6.3,

unicast packets are reachable, the number of cyclic times is 2, and the interval at which the rate is calculated is 12s.

```
<HUAWEI> mtrace -gw 10.1.6.3 -r 10.1.6.4 -g 225.0.0.1 -l 2 -st 12 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table
 In calculating-rate mode, current statistic times is: 1

 -1 10.1.5.1
   Incoming Interface Address: 10.1.5.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.6.3 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -2 10.1.2.1
   Incoming Interface Address: 10.1.2.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.5.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -3 10.1.0.1
   Incoming Interface Address: 10.1.0.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.2.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
 ********************************************************
  In calculating-rate mode, reach the demanded number of statistic, and multicast
 traceroute finished.
```

Table 8-105 Description of the **mtrace** command output

Item	Description
Press Ctrl+C to break multicast traceroute facility	The ongoing Mtrace test is terminated after you press **Ctrl+C**.
From the receiver (10.1.6.4), trace reverse path to source (10.1.0.1) according to RPF rules	The RPF path from destination host 10.1.6.4 to multicast source 10.1.0.1 is detected.
From the receiver (10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table	The transmission path of multicast data (10.1.0.1, 225.0.0.1) from the destination host 10.1.6.4 to the source is tested.
Num	Number of traced hops.
Reverse-Path	Reverse path of multicast traffic.
FwdTTL	Minimum TTL value for multicast packet forwarding.
Protocol	Multicast routing protocol used on the switch.
-1 10.1.5.1 1 PIM	The address of the last hop is 10.1.5.1, the minimum TTL value for multicast forwarding is 1, and the multicast routing protocol used on the switch is PIM.
In calculating-rate mode, current statistic times is: 1	The rate is calculated for the first time in the calculating rate mode.

Item	Description
-1 10.1.5.1	Last hop with the address as 10.1.5.1 in calculating rate mode.
Incoming Interface Address: 10.1.5.1 Input packets rate: 0	Multicast inbound interface address and the inbound packet rate on the inbound interface in calculating rate mode.
Outgoing Interface Address: 0.0.0.0 Output packets rate: 0xffffffff	Multicast outbound interface address and the outbound packet rate on the outbound interface in calculating rate mode.
Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0	Rate for a switch to forward multicast packets of the (S, G) entry in calculating rate mode.
In maximum-hop mode, received the response message, and multicast traceroute finished.	IGMP Tracert Response messages are received in maximum hop tracking mode.
In calculating-rate mode, reach the demanded number of statistic, and multicast traceroute finished.	Mtrace is complete in calculating rate mode when the required number of calculating times is reached.

8.7.17 mtrace query-policy

Function

The **mtrace query-policy** command enables a device to filter IGMP-Tracert-Query packets in unicast mode based on the source address of these packets.

The **undo mtrace query-policy** command cancels the filtering of IGMP-Tracert-Query packets.

By default, the switch does not filter IGMP-Tracert-Query packets.

Format

mtrace query-policy [*basic-acl-number*]

undo mtrace query-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL. This ACL defines the address range of a trusted querier. According to this ACL, the last hop switch rejects the IGMP-Tracert-Query packets sent by an invalid querier.	The value is an integer ranging from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The source address of IGMP-Tracert-Query packets in unicast mode is the local interface address. Before you create an ACL rule, create an ACL.

Run this command on the switch that is connected to the host.

- This command takes effect only on the last hop switch, which is not the querier.
- This command filters only the IGMP-Tracert-Query packets encapsulated in unicast IP packets.
- This command is not applicable to the tracking initiated from the querier.

When you run the **mtrace query-policy** command on the last hop switch, note the following points:

- If *basic-acl-number* is not specified, the last hop switch does not reject IGMP-Tracert-Query packets in unicast mode.
- If *basic-acl-number* is specified but the ACL is not defined on the switch, the last hop switch rejects any IGMP-Tracert-Query packet in unicast mode.
- If *basic-acl-number* is specified and this ACL is defined on the switch, only the IGMP-Tracert-Query packets allowed by the ACL can be received.

Example

Apply the querier filtering rules to the last hop switch.

```
<HUAWEI> system-view
[HUAWEI] mtrace query-policy 2000
```

8.7.18 multicast boundary

Function

The **multicast boundary** command configures a multicast boundary for a single administrative range.

The **undo multicast boundary** command deletes the configured multicast boundary.

By default, no multicast boundary is configured on an interface.

Format

multicast boundary *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

Parameters

Parameter	Description	Value
group-address	Specifies the address of a multicast group, used to specify a multicast group and configure the forwarding range of the multicast packets for the group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the mask of a specified group address.	The mask is in dotted decimal notation.
mask-length	Indicates the mask length of a specified group address.	The value is an integer that ranges from 4 to 32.
all	Deletes all the multicast boundaries configured on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view, tunnel interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Data of some multicast groups needs to be forwarded within a specified range. For example, each BSR administrative domain serves a specific group address range, and data packets sent from multicast sources to these groups need to be forwarded within the matching administrative domain. After a multicast boundary is configured for specified multicast groups on an interface, multicast packets sent to these groups cannot be forwarded through the interface. This restricts multicast forwarding within a range.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

To configure the boundary for different multicast groups, you can repeat the command on the same interface.

A and B are the forwarding boundary sets of the multicast group range to be configured, and B is a subset of A. If A is first configured on an interface, B cannot be configured. If you configure A on the interface that has been configured with B, B is replaced by A.

Example

Configure VLANIF100 as the boundary of group 239.2.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] multicast boundary 239.2.0.0 16
```

Configure GE0/0/1 as the boundary of group 239.2.0.0/16.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] multicast boundary 239.2.0.0 16
```

8.7.19 multicast cpu-forward disable

Function

The **multicast cpu-forward disable** command disables software forwarding for multicast packets.

The **undo multicast cpu-forward disable** command restores the default configuration.

By default, software forwarding for multicast packets is enabled.

Format

multicast cpu-forward disable

undo multicast cpu-forward disable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, the switch forwards packets based on software before the hardware forwarding is completed. Then, the switch forwards packets based on hardware. Soft forwarding for multicast packets must be disabled on the switch to prevent packet loss and disorder caused by the low forwarding speed and first packet cache mechanism of soft forwarding.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Disable software forwarding for multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast cpu-forward disable
```

8.7.20 multicast forwarding-table downstream-limit

Function

The **multicast forwarding-table downstream-limit** command sets the maximum number of downstream nodes of an entry in the multicast forwarding table.

The **undo multicast forwarding-table downstream-limit** command restores the default setting.

By default, the maximum number of downstream nodes of an entry is 128.

Format

multicast forwarding-table downstream-limit *limit*

undo multicast forwarding-table downstream-limit

Parameters

Parameter	Description	Value
limit	Indicates the maximum number of downstream nodes of an entry in the forwarding table.	The value of ranges from 0 to 128.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch receives a multicast packet, it copies the packet for each downstream node in the matching multicast forwarding entry. If the switch has a large number of multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the load on the switch, limit the maximum number of downstream nodes in each multicast forwarding entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

If the configured number is smaller than the current number, the excessive downstream nodes are not deleted immediately, and must be deleted by the multicast routing protocol. In addition, no new downstream node can be added to the entry in the forwarding table.

Example

Set the maximum number of downstream nodes of an entry in the forwarding table to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast forwarding-table downstream-limit 32
```

8.7.21 multicast forwarding-table route-limit

Function

The **multicast forwarding-table route-limit** command sets the limit on the number of entries in the multicast forwarding table.

The **undo multicast forwarding-table route-limit** command restores the default value of the limit.

The following lists the maximum number of entries allowed in the multicast forwarding table of each model by default:

- S5720-LI, S5720S-LI: 1022
- S5731-S, S5731S-S, S5720I-SI: 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5735S-H, S5736-S, S6720S-S: 1536
- S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S: 4096

Format

multicast forwarding-table route-limit *limit*

undo multicast forwarding-table route-limit

Parameters

Parameter	Description	Value
limit	Specifies the limit on the number of entries in the multicast forwarding table.	The value is an integer that ranges from 0 to *The maximum number of entries allowed in the multicast forwarding table by default.* **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive multicast forwarding entries will exhaust the memory of the switch. To prevent this problem, use the **multicast forwarding-table route-limit** command to limit the number of entries in the multicast forwarding table.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

NOTICE

If you set the limit on the number of entries in the multicast forwarding table after multicast services are deployed on a switch, ensure that the limit is greater than or equal to the number of current forwarding entries. Otherwise, faults may occur.

It is recommended that you set this limit based on the actual network environment before deploying multicast services on the switch.

If the configured limit is smaller than the number of existing entries, the excessive entries are not deleted immediately. The configured limit takes effect in the following cases:

- Entries are added to the multicast forwarding table after the existing entries age out.
- The **reset multicast forwarding-table all** command is run.

Example

Set the limit on the number of the entries in the forwarding table to 60.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast forwarding-table route-limit 60
```

8.7.22 multicast invalid-packet

Function

The **multicast invalid-packet** command sets the maximum number of invalid multicast protocol packets that can be stored on the switch.

The **undo multicast invalid-packet** command deletes the set maximum number of invalid multicast protocol packets that can be stored on the switch.

By default, the switch can save a maximum of 10 invalid packets for each specific multicast protocol.

Format

multicast invalid-packet { **igmp** | **mdt** | **msdp** | **pim** } **max-count** *max-number*

undo multicast invalid-packet { **igmp** | **mdt** | **msdp** | **pim** }

Parameters

Parameter	Description	Value
igmp	Sets the maximum number of invalid IGMP messages.	-
mdt	Sets the maximum number of invalid multicast VPN messages.	-
msdp	Sets the maximum number of invalid MSDP messages.	-
pim	Sets the maximum number of invalid PIM messages.	-
max-count *max-number*	Sets the maximum number of invalid multicast protocol packets that can be stored on a device.	The value is an integer ranging from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If multicast entries fail to be generated or peer relationships fail to be set up, you can enable the switch to store invalid multicast protocol packets and view statistics and details of the invalid multicast protocol packets. Based on the command output, you can locate and rectify faults.

Example

Set the maximum number of invalid IGMP messages that can be stored on the switch to 20.

```
<HUAWEI> system-view
[HUAWEI] multicast invalid-packet igmp max-count 20
```

8.7.23 multicast load-splitting

Function

The **multicast load-splitting** command enables load splitting among multicast routes.

The **undo multicast load-splitting** command restores the default configuration.

By default, load splitting among multicast routes is disabled.

Format

multicast load-splitting { **balance-preferred** | **stable-preferred** | **group** | **source** | **source-group** }

undo multicast load-splitting

Parameters

Parameter	Description	Value
balance-preferred	Indicates balance-preferred load splitting. This policy is applicable to the scenario where hosts frequently join or leave groups, which requires automatic load adjustment.	-
stable-preferred	Indicates stable-preferred load splitting. This policy is applicable to stable multicast networking.	-

Parameter	Description	Value
group	Indicates group address-based load splitting. This policy is applicable to the scenario of one source to multiple groups.	-
source	Indicates source address-based load splitting. This policy is applicable to the scenario of multiple sources to one group.	-
source-group	Indicates source and group addresses-based load splitting. This policy is applicable to the scenario of multiple sources to multiple groups.	-

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the switch applies the following route selection rules during RPF check:

- If the equal-cost routes are in the same routing table, for example, a unicast routing table, multicast static routing table, or MBGP routing table, the switch selects the route with the largest next-hop address as the RPF route.
- If the equal-cost routes are in different routing tables, the switch selects the route with the highest preference. If the routes have the same preference, the switch selects the route with the longest mask length. If the routes have the same preference and mask length, the switch uses certain algorithm to select a route as the RPF route.

No matter which rule is used, the switch selects only one route as the RPF route. To enable multicast data to be forwarded through multiple paths, run the **multicast load-splitting** command to configure multicast load splitting. After multicast load splitting is configured, the switch uses the specified load splitting policy to distribute multicast data among multiple paths. This function improves quality of multicast forwarding.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Follow-up Procedure

Because the forwarding capabilities of equal-cost routes are different from the actual load distribution situation on the equal-cost routes, even load splitting cannot meet network requirements in some scenarios. Then, you can run the

multicast load-splitting weight command to configure the multicast load splitting weight on the interface to realize unbalanced load splitting.

Precautions

The five load splitting policies are mutually exclusive. It is recommended that you use a fixed load splitting policy based on the actual situation on your network. The **balance-preferred** or **stable-preferred** policy is preferred.

If PIM-DM is enabled in the current public network instance, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure group address-based load splitting.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast load-splitting group
```

8.7.24 multicast load-splitting weight

Function

The **multicast load-splitting weight** command sets the multicast load splitting weight for an interface.

The **undo multicast load-splitting weight** command restores the default setting.

By default, the multicast load splitting weight of an interface is 1.

Format

multicast load-splitting weight *weight-value*

undo multicast load-splitting weight

Parameters

Parameter	Description	Value
weight-value	Specifies the multicast load splitting weight of an interface.	The value is an integer that ranges from 0 to 32.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stable-preferred or balance-preferred multicast splitting policy is configured, you can run this command to set load splitting weights for interfaces to realize unbalanced load splitting. The larger weight value an interface has, the more multicast routing entries have it as the upstream interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Precautions

This command is applicable only when the multicast load splitting policy is set to stable-preferred or balance-preferred.

When the multicast load splitting weight on an interface is 0, the routes that have this interface as the upstream interface do not take part in load splitting.

Example

Set the multicast load splitting weight on VLANIF100 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] multicast load-splitting weight 10
```

Set the multicast load splitting weight on GE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] multicast load-splitting weight 10
```

8.7.25 multicast load-splitting-timer

Function

The **multicast load-splitting-timer** command sets a load splitting timer.

The **undo multicast load-splitting-timer** command restores the default setting.

By default, the value of a load splitting timer is 1800 seconds.

Format

multicast load-splitting-timer *interval*

undo multicast load-splitting-timer

Parameters

Parameter	Description	Value
interval	Specifies the value of the load splitting timer.	The value is an integer ranging from 10 to 1800, in seconds.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In stable-preferred load splitting or balance-preferred load splitting mode, entries may not be well-balanced among paths because of the addition or deletion of entries, change of load splitting weights of the paths, or change of equal-cost routes. In such a case, the device will balance entries after a certain waiting time to reduce the impact of frequent changes on the system.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is stable, for example, when entries are not deleted or added frequently or equal-cost routes are not changed frequently, set the load splitting timer value to a smaller value so that entries can be balanced rapidly. The recommended value is 300 to 600 seconds.
- If the network is not stable, for example, when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a larger value to reduce the impact of frequent entry changes on the system and network stability. The recommended value is 1200 to 1800 seconds.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Set a load splitting timer to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast load-splitting-timer 100
```

8.7.26 multicast longest-match

Function

The **multicast longest-match** command configures the switch to select the RPF route based on the longest matching rule.

The **undo multicast longest-match** command restores the default configuration.

By default, the switch selects the route with the highest preference as the RPF route.

Format

multicast longest-match

undo multicast longest-match

Parameters

None

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch selects the RPF route based on route preference. This command changes the route selection policy used by the switch during RPF check. After you run this command, the switch selects the RPF route with the longest mask. If multiple routes have the same mask length, the switch selects the route with the highest preference.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command.

Example

Select routes according to the longest match on the switch.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
[HUAWEI] multicast longest-match
```

8.7.27 multicast routing-enable

Function

The **multicast routing-enable** command enables the multicast routing function.

The **undo multicast routing-enable** command restores the default configuration.

By default, the multicast routing function is disabled.

Format

multicast routing-enable

undo multicast routing-enable

Parameters

None

Views

System view, VPN instance view, VPN IPv4 address family view

NOTE

Only the following models support the VPN instance view and VPN IPv4 address family view: S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, S6720-EI, S6735-S and S6720S-EI

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring Layer 3 multicast, you must enable the multicast routing function globally. Layer 3 multicast protocols (such as PIM and IGMP) and other Layer 3 multicast functions can be configured only after multicast routing is enabled.

Precautions

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

NOTICE

The **undo multicast routing-enable** command deletes all multicast configurations of the public network instance or VPN instance. After this command is run, multicast services that are running on the instance will be interrupted. To restore the multicast services, you must run the deleted multicast commands again.

Example

Enable multicast routing globally.

```
<HUAWEI> system-view
[HUAWEI] multicast routing-enable
```

8.7.28 multicast ttl-check disable

Function

The **multicast ttl-check disable** command disables a switch from checking the TTL value of multicast packets.

The **undo multicast ttl-check disable** command enables a switch to check the TTL value of multicast packets again.

By default, a switch checks the TTL value of multicast packets.

NOTE

This command is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

multicast ttl-check disable

undo multicast ttl-check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In V200R019C10 and later versions, when multicast packets between a multicast source and receiver are forwarded across VLANs, the multicast packets with a TTL value less than or equal to 1 will be discarded by default.

In versions earlier than V200R019C10, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not discard multicast packets whose TTL value is less than or equal to 1. After the switch software version is upgraded to V200R019C10 or later, however, if you want a switch not to discard multicast packets whose TTL value is less than or equal to 1, run the **multicast ttl-check disable** command to disable the switch from checking the TTL value of multicast packets.

The **multicast ttl-check disable** command does not apply to the following scenarios:

- This command is not applicable to multicast packets on a VPN. A switch always discards multicast packets on a VPN if their TTL value is less than or equal to 1.
- This command does not apply when a multicast source and receiver are in the same VLAN, in which case, the switch does not check the TTL value of multicast packets between them.
- When the forwarding mode of multicast packets is changed to MAC address-based forwarding, the switch does not check the TTL value of multicast packets.

Example

Disable a switch from checking the TTL value of multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast ttl-check disable
```

8.7.29 ping multicast

Function

The **ping multicast** command enables a device to detect the reserved members in the network segment, simulates the common group traffic, triggers the establishment of a distribution tree, and checks whether the network can normally bear multicast services.

Format

ping multicast [**-c** *count* | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host*

Parameters

Parameter	Description	Value
-c *count*	Specifies the number of times for sending ICMP Echo Request messages.	The value is an integer that ranges from 1 to 65535. The default value is 5.
-h *ttl-value*	Sets the TTL value of an ICMP Echo Request message.	The value is an integer that ranges from 1 to 255. The default value is 255.
-i *interface-type interface-number*	Sets the outgoing interface that sends ICMP Echo Request messages. • When the MPing destination group address is a reserved multicast group address, **-i** must be specified. • When the MPing destination group address is a common multicast group address, **-i** cannot be specified.	-
-m *time*	Specifies the time to wait before sending the next ICMP Echo Request message. Each time the source sends an ICMP Echo Request message using the **ping multicast** command, the source waits a period of time (2000 ms by default) before sending the next ICMP Echo Request message. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-p *pattern*	Specifies the padding byte of ICMP Echo Request messages. After the padding byte of the ICMP Echo Request message is set, the destination host can identify a certain ICMP Echo Reply message.	The value ranges from 0 to FFFFFFFF, in the hexadecimal format. By default, the padding starts from 0x01, and continues in ascending order.

Parameter	Description	Value
-q	Indicates that only statistics are displayed. When **-q** is specified in the **ping multicast** command, only the number of sent and received packets, packet loss rate, and the minimum, average, and maximum RTTs are displayed.	By default, all information is displayed.
-s *packetsize*	Sets the length of an ICMP Echo Request message, excluding the IP or ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56.
-t *timeout*	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent. After the **ping multicast** command is run, the source sends an ICMP Echo Request message to a destination and waits for an ICMP Echo Reply message. If the destination, after receiving the ICMP Echo Request message, returns an ICMP Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMP Echo Reply message within the specified period, the source displays a message indicating that the message times out. Normally, the source receives an ICMP Echo Reply message within 1 to 10 seconds after sending an ICMP Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tos *tos-value*	Specifies the ToS value of the sent ICMP Echo Request messages.	The value is an integer that ranges from 0 to 255. The default value is 196.

Parameter	Description	Value
-v	Displays all received ICMP Echo Reply messages. - If **-v** is not specified, the system displays the received ICMP Echo Reply messages of the user. - If **-v** is specified, the system displays all received ICMP Echo Reply messages.	By default, only ICMP Echo Reply messages of the user are displayed.
host	Specifies the destination address of an ICMP Echo Request message, also called the MPing destination group address.	It includes reserved group addresses and common group addresses.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping multicast** command is used to check a multicast network in the following scenarios:

Scenario 1: When configuring the destination group address *host* as a reserved group address, you can run the **ping multicast** command to check which reserved multicast members reside on the network segment of the outbound interface. In this scenario, the TTL of an ICMP Echo Request message cannot be set.

The reserved multicast group identifies a group of network devices (reserved multicast members) that match certain conditions. When the reserved multicast members receive ICMP Echo Request messages with the destination addresses as the reserved group addresses, they return ICMP Echo Reply messages. Common reserved group addresses are as follows:

- 224.0.0.1: indicates all systems in the subnet.
- 224.0.0.2: indicates all routers in the subnet.
- 224.0.0.5: indicates OSPF IGP routers.
- 224.0.0.13: indicates PIM routers.

NOTE

In this scenario, **-i** must be specified in the **ping multicast** command.

Scenario 2: When setting the destination group address *host* as a common group address, you can run the **ping multicast** command to implement the following functions:

- Simulates the multicast traffic and triggers a series of protocol processes. By viewing the multicast routing information on the switch, check whether the protocol running status is normal and whether the multicast distribution tree is correctly established.
- Check multicast members in the network and calculate the TTL value and the RTT from the MPing initiator to multicast members. This function requires that the host support MPing and is implemented by calculating the number of ICMP Echo Reply messages sent by the destination host. MPing is performed continuously at a certain interval to calculate the network delay and route jitter.

NOTE

In this scenario, **-i** cannot be specified in the **ping multicast** command.

You can specify different parameters in **ping multicast** command for different scenarios:

- On an unstable network, you can run the **ping multicast -c** *count* **-t** *timeout host* command to check the quality of the multicast network. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.
- You can run the **ping multicast -s** *packetsize host* to set the size of a multicast probe packet. In this way, you can check the quality of the multicast network by simulating real service datagrams. The path MTU is then obtained through multiple probes.

Prerequisites

Before running the **ping multicast** command, ensure that the ICMP module is working properly.

Configuration Impact

If an intermediate device is disabled from responding to ICMP messages, detection on this node fails.

Precautions

If a fault occurs in the MPing process, you can press **Ctrl+C** to terminate the MPing operation.

Example

Perform MPing, specify the reserved multicast group address as 224.0.0.5 and the outbound interface as VLANIF 100, and detect the OSPF IGP router in the network segment.

```
<HUAWEI> ping multicast -i vlanif 100 224.0.0.5
MULTICAST PING 224.0.0.5 : 56 data bytes, press Ctrl+C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 TTL =255 time=30ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 TTL =255 time=20ms
```

```
Reply from 10.1.1.5 : bytes=56 Sequence=5 TTL =255 time=10ms
Destination multicast address 224.0.0.5
--- Multicast ping statistics ---
5 Request packet(s) transmitted
5 Reply packet(s) received
0.00% packet loss
Round-trip min/avg/max = 10/16/40 ms
```

Specify the padding field of **-p**.

```
<HUAWEI> ping multicast -i vlanif 100 -p 12345678 224.0.0.5
MULTICAST PING 224.0.0.5 : 56 data bytes, press Ctrl+C to break
The padding string: 12345678
Reply from 10.1.1.5 : bytes=56 Sequence=1 TTL =255 time=30ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 TTL =255 time=20ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 TTL =255 time=10ms
Destination multicast address 224.0.0.5
--- Multicast ping statistics ---
5 Request packet(s) transmitted
5 Reply packet(s) received
0.00% packet loss
Round-trip min/avg/max = 10/16/40 ms
```

Table 8-106 Description of the ping multicast command output

Item	Description
MULTICAST PING 224.0.0.5	The destination group address of MPing is 224.0.0.5.
56 data bytes	The length of the sent ICMP Echo Request message is 56 bytes.
press Ctrl+C to break	The ongoing MPing test can be terminated by pressing **Ctrl+C**.
The padding string: 12345678	The padding string is 12345678. If **-p** is not specified, the padding character string is not displayed.
Reply from 10.1.1.5: bytes=56 Sequence=1 TTL=255 time=30ms	The ICMP Echo Reply message sent from 10.1.1.5 is received. The message carries the following information: ● bytes=56: indicates the length of the ICMP Echo Reply message. ● Sequence=1: indicates the sequence number of the ICMP Echo Reply message. ● TTL=255: indicates the TTL value of the ICMP Echo Reply message. ● time=30ms: indicates the RTT, in milliseconds. If no ICMP Echo Reply message is received after the timeout period, "Request time out" is displayed.
Destination multicast address 224.0.0.5	The destination group address is 224.0.0.5.

Item	Description
--- Multicast ping statistics --- 5 Request packet(s) transmitted 5 Reply packet(s) received 0.00% packet loss Round-trip min/avg/max = 10/16/40 ms	Statistics collected after the Ping test on the destination host. The statistics are as follows: ● Number of sent ICMP Echo Request messages: 5 ● Number of received ICMP Echo Reply messages: 5 ● Percentage of non-Reply messages against total sent messages: 0.00% ● The minimum RTT is 10 ms, the average RTT is 16 ms, and the maximum RTT is 40 ms.

8.7.30 reset mtrace statistics

Function

The **reset mtrace statistics** command clears statistics about Mtrace packets.

Format

reset mtrace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect statistics about Mtrace traffic generated in a certain period, reset the original statistics.

Example

Clear statistics about the current Mtrace traffic.

```
<HUAWEI> reset mtrace statistics
```

8.7.31 reset multicast forwarding-table

Function

The **reset multicast forwarding-table** command clears the entries of the multicast forwarding table.

Format

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table all**

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* indicates the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
all	Indicates all forwarding entries of multicast forwarding tables.	-
group-address	Specifies the address of a multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast group address or source address.	-
group-mask	Specifies the address mask of a multicast group.	The address mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the address of a multicast source.	The address is in dotted decimal notation.
source-mask	Specifies the address mask of a multicast source.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.
incoming-interface	Indicates the upstream interface of the forwarding entry.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
register	Indicates the register interface in PIM-SM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the multicast forwarding table, multicast data will be interrupted for a period. Confirm the action before you use the command.

The time interval before you run the **reset multicast forwarding-table** command again must be longer than 30 seconds.

Example

Delete the multicast forwarding entries of the group 225.5.4.3 from the forwarding table.

```
<HUAWEI> reset multicast forwarding-table 225.5.4.3
```

8.7.32 reset multicast routing-table

Function

The **reset multicast routing-table** command clears the entries in the multicast routing table. The corresponding forwarding entries in the forwarding table are deleted at the same time.

Format

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table all**

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* indicates the name of the VPN instance.	The value must be an existing VPN instance name.
all-instance	Indicates all the instances.	-
all	Indicates all entries in the multicast routing table.	-
group-address	Specifies the address of the specified group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the address mask of a multicast group or source.	-
group-mask	Specifies the address mask of a multicast group.	The address mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the address of a specified source.	The address is in dotted decimal notation.
source-mask	Specifies the address mask of a multicast source, in dotted decimal notation.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.
incoming-interface	Specifies the incoming interface of a multicast entry.	-
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
register	Indicates the register interface of PIM-SM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the multicast routing table, the matching entries in the multicast forwarding table are also deleted. As a result, multicast forwarding will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the entries of the group 225.5.4.3 from the multicast routing table.

```
<HUAWEI> reset multicast routing-table 225.5.4.3
```

8.7.33 set multicast forwarding-table enhance-mode

Function

The **set multicast forwarding-table enhance-mode** command sets the multicast forwarding mode to enhanced forwarding. In this forwarding mode, the device generates dummy entries (Layer 3 multicast dummy forwarding entries) for multicast packets that fail RPF check, even if Layer 2 multicast is disabled on the device.

The **undo set multicast forwarding-table enhance-mode** command disables enhanced forwarding for multicast traffic on the device. After this command is run, the device no longer generates dummy entries (Layer 3 multicast dummy forwarding entries) for multicast packets that fail RPF check, if Layer 2 multicast is disabled on the device.

By default, a device forwards multicast traffic in enhanced mode.

Format

set multicast forwarding-table enhance-mode

undo set multicast forwarding-table enhance-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Layer 2 multicast is not enabled on a device using the **igmp-snooping enable (VLAN view)** command, the device cannot generate dummy entries for multicast packets that fail the RPF check, so such packets cannot match any multicast entries. As a result, a large number of unknown multicast packets will be continuously sent to the CPU, causing high CPU usage. To prevent such a problem, you can run the **set multicast forwarding-table enhance-mode** command to set the multicast forwarding mode to enhanced forwarding. In this forwarding mode, the device generates dummy entries for multicast packets that fail RPF check, even if Layer 2 multicast is disabled on the device. The dummy entries guide Layer 3 multicast traffic forwarding, preventing high CPU usage caused by continuous sending of unknown multicast traffic.

Precautions

This command takes effect only for multicast packets in a VLAN.

Example

Set multicast forwarding mode to enhanced forwarding.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table enhance-mode
```

8.7.34 set multicast forwarding-table optimization-mode

Function

The **set multicast forwarding-table optimization-mode** command configures the multicast optimization mode in which the Layer 3 forwarding entries are stored on a switch.

The **undo set multicast forwarding-table optimization-mode** command restores the default storage mode.

By default, a switch uses the normal storage mode.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

set multicast forwarding-table optimization-mode [**slot** *slot-id*]

undo set multicast forwarding-table optimization-mode [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, storage modes of all slots are configured to be the multicast optimization mode.	The value is an integer and must be the slot ID of a running slot.

Views

System view

Default Level

3: Management level

Usage Guidelines

Applicable Environment

In most cases, the Layer 3 forwarding entries are stored in normal mode. The ARP cache table, ND cache table, and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table.

This command optimizes storage resources of Layer 3 forwarding entries through preferential allocation of hardware resources preferentially to the multicast forwarding table. The ARP cache table, ND cache table, and routing table share hardware resources. Run this command if either of the following situations occurs:

- A large number of ARP prefix entries and multicast forwarding entries exist in the system at the same time.
- A large number of ND prefix entries and multicast forwarding entries exist in the system at the same time.

Precautions

Note the following points when running this command:

- If the multicast optimization modes on a switch are configured or deleted, the system prompts the user to save the configurations and then restart the device. If the device configuration is not saved, the new storage mode does not take effect after the restart.
- This function can be implemented on an IPv6 network only when a switch with an extended entry register is available. In addition, the storage mode of the register must be set to IPv6 mode. For details on how to configure the extended entry register, see **assign resource-mode** in "Device Management Commands > Hardware Configuration Commands".

NOTICE

When the user configures this mode or restores the default mode, the system will prompt the user to restart the device or a specified slot. If the system receives no response, the configuration times out, and the system view is displayed. The system does not restart. The restart can cause the network to crash for a short period. In most cases, this command is not recommended.

Example

Configure the storage mode to be the multicast optimization mode for a switch.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table optimization-mode
```

8.7.35 set multicast forwarding-table super-mode

Function

The **set multicast forwarding-table super-mode** command configures the high specification mode for multicast forwarding. In the high specification mode, the number of multicast entries can reach the maximum value supported by the switch, which is much more than the default limit.

The **undo set multicast forwarding-table super-mode** command restores the default configuration.

By default, the common specification mode is used for multicast forwarding after Layer 3 multicast is configured. In this mode, the number of multicast entries cannot exceed the default limit defined on the switch.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Format

set multicast forwarding-table super-mode

undo set multicast forwarding-table super-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 3 multicast is enabled, the common specification mode is used for multicast forwarding by default. This mode can meet requirements of most multicast service scenarios. In some large-scale multicast applications, a network has a large number of multicast sources to provide many channels for multicast users. In these applications, the number of multicast entries may exceed the default limit defined on a multicast device. When this occurs, some multicast entries cannot be generated. As a result, some users cannot receive the multicast data they request.

The **set multicast forwarding-table super-mode** command configures the high specification mode to increase the number of entries used for multicast forwarding. In high specification mode, the number of multicast entries supported by the switch is much larger than the default limit on the number of multicast entries. This mode maximizes a device's capability to support large-scale multicast applications.

Precautions

After you run this command:

- This command can only increase the number of Layer 3 multicast forwarding entries, but cannot increase the number of Layer 2 multicast forwarding entries. In scenarios when both Layer 2 and Layer 3 multicast services are configured, the number of Layer 3 multicast forwarding entries is limited by the number of Layer 2 multicast forwarding entries. Therefore, this command cannot increase the number of multicast forwarding entries if both Layer 2 and Layer 3 multicast services are configured.
- Restart the switch for the configuration to take effect.
- The default value of the IGMP general query interval changes from 60s to 120s. You can set the IGMP general query interval using the **igmp timer query** or **timer query (IGMP view)** command.
- The default value of the IGMP robustness variable changes from 2 to 3. You can set the robustness variable using the **igmp robust-count** or **robust-count (IGMP view)** command.
- The default value of the other querier present interval changes from 125s to 245s. You can set the other querier present interval using the **igmp timer other-querier-present** or **timer other-querier-present (IGMP view)** command.
- The default value of the MLD robustness variable changes from 2 to 3. You can set the robustness variable using the **mld robust-count** or **robust-count (MLD view)** command.
- The default interval for sending PIM-DM State-Refresh messages changes from 60s to 255s. On an IPv4 multicast network, run the **state-refresh-interval (IPv4)** command to set the interval for sending PIM-DM State-Refresh messages. On an IPv6 network, run the **state-refresh-interval (IPv6)** command to set the interval for sending PIM-DM State-Refresh messages.
- The default interval for sending PIM Join-Prune messages changes from 210s to 300s. On an IPv4 multicast network, run the **holdtime join-prune (IPv4)** or **pim holdtime join-prune** command to set the interval for sending PIM

Join-Prune messages. On an IPv6 network, run the **holdtime join-prune (IPv6)** or **pim ipv6 holdtime join-prune** command to set the interval for sending PIM Join-Prune messages.

- Run the **car** command to change the rate limit for IGMP/MLD messages sent to the CPU according to the actual situations of multicast services.
- More system resources are consumed in the high specification mode. If the number of multicast protocol packets sent to the switch increases sharply in a short time, the CPU usage of the switch becomes high.
- It is recommended that you set the same general query interval on all the IGMP/MLD-enabled interfaces of a switch. For an IGMP-enabled interface, run the **igmp timer query** command in the interface view to set the general query interval. For an MLD-enabled interface, run the **mld timer query** command in the interface view to set the general query interval. This configuration prevents IGMP/MLD-enabled interfaces from sending Query messages at the same time, so that the switch does not have to process a large number of Report messages in a short time, which could cause a high CPU usage.
- In a stack, if member interfaces of an Eth-trunk interface are located on member switches that support different numbers of multicast forwarding entries, the maximum number of multicast forwarding entries supported by the Eth-Trunk interface depends on the member switch that supports the fewest multicast forwarding entries. Multicast forwarding entries supported by an Eth-Trunk interface meet either of the following conditions:
  - The outbound interface of the multicast forwarding entries is the Eth-Trunk interface that has been switched to the Layer 3 mode using the **undo portswitch** command.
  - The Eth-Trunk interface belongs to the VLANs corresponding to the VLANIF interfaces of the multicast forwarding entries.

Example

Configure the high specification mode for multicast forwarding.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table super-mode
Warning: This command will modify some default multicast settings and has limitations
in a few special scenarios. Use the command according to product manual.Continue? [Y/N]:y
```

8.7.36 set multicast-hash-mode

Function

The **set multicast-hash-mode** command specifies a hash algorithm for multicast forwarding.

The **undo multicast-hash-mode** command restores the default hash algorithm for multicast forwarding.

By default, the crc-32-lower algorithm is used.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support support this command.

Format

set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

undo set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

Parameters

Parameter	Description
crc-32-upper	
crc-32-lower	
lsb	
crc-16-upper	
crc-16-lower	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve multicast forwarding performance, the switch uses a hash algorithm to learn multicast addresses. If multiple addresses match a key value, a hash conflict occurs. A large number of hash conflicts will cause failures to learn some multicast addresses. When such a problem occurs, use an appropriate hash algorithm to reduce hash conflicts.

Precautions

- An appropriate hash algorithm can reduce but not eliminate hash conflicts.
- MAC addresses are distributed on a network randomly, so the system cannot determine the best hash algorithm. The default hash algorithm is the best algorithm in most cases, so changing the hash algorithm is not recommended.
- After changing the hash algorithm, restart the switch for the configuration to take effect.

Example

Set the hash algorithm for multicast forwarding to crc-32-upper.

```
<HUAWEI> system-view
[HUAWEI] set multicast-hash-mode crc-32-upper
```

8.8 IPv6 Multicast Route Management Commands

8.8.1 Command Support

Product	Support
S1700	Not supported.
S300	Supported.
S500	Supported.
S2700	Supported.
S5700	Supported except S5731-L and S5731S-L.
S6700	Supported.

8.8.2 display multicast ipv6 boundary

Function

The **display multicast ipv6 boundary** command displays the multicast boundary configured on an interface.

Format

display multicast ipv6 boundary [*ipv6-group-address ipv6-group-mask-length* | **scope** *scope-id*] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address to display the corresponding multicast routing table.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.

Parameter	Description	Value
scope *scope-id*	Specifies a scope ID.	The value is an integer that ranges from 3 to 15.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to check the boundary of a PIM-SM (IPv6) network. When some hosts cannot receive multicast data, you can use this command to check whether the problem is caused by multicast boundary configuration.

Example

Display the boundaries configured on all the interfaces.

```
<HUAWEI> display multicast ipv6 boundary
IPv6 multicast boundary information
Total 1 Multicast IPv6 boundary
 Interface           Boundary
 Vlanif100            FF02::/64
```

Table 8-107 Description of the display multicast ipv6 boundary command output

Item	Description
IPv6 multicast boundary information	IPv6 multicast boundary.
Total 1 Multicast IPv6 boundary	Total number of IPv6 multicast boundaries.
Interface	Name of the interface configured with multicast boundary.
Boundary	Multicast group with the interface as the boundary.

8.8.3 display multicast ipv6 forwarding-table

Function

The **display multicast ipv6 forwarding-table** command displays the IPv6 multicast forwarding table.

Format

display multicast ipv6 forwarding-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** | **none** } } | { **statistics** | **verbose** }] *

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 8 to 128.
incoming-interface	Indicates the incoming interface of an IPv6 multicast forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of PIM-SM.	-
outgoing-interface	Indicates the outgoing interface of an IPv6 multicast forwarding entry.	-
exclude	Indicates that the downstream interface list does not contain the route forwarding entries of a specified interface.	-

Parameter	Description	Value
include	Indicates that the downstream interface list contains the route forwarding entries of a specified interface.	-
match	Indicates that the downstream interface list matches the route forwarding entries of a specified interface.	The downstream interface list contains only one eligible interface. After **match** is configured, the route forwarding entries of a null downstream interface list are displayed if the outgoing interface is not specified.
none	Displays the (S, G) entry without a downstream interface.	-
statistics	Displays the statistics of the multicast forwarding table.	-
verbose	Displays the detailed information about the multicast forwarding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During IPv6 multicast routing and forwarding, routing information generated by IPv6 multicast routing protocols is saved in an IPv6 multicast routing table. The switch selects the optimal multicast routes from the routing table according to multicast routing and forwarding policies, and then delivers the selected multicast routes to the IPv6 multicast forwarding table to guide multicast data forwarding.

You can use the **display multicast ipv6 forwarding-table** command to check whether IPv6 multicast forwarding entries have been generated and whether multicast data can be forwarded normally.

Example

Display the IPv6 multicast forwarding table.

```
<HUAWEI> display multicast ipv6 forwarding-table
IPv6 Multicast Forwarding Table
Total 2 entries, 2 matched

00001. (FC00:AA::123, FF33::)
     MID: 0, Flags: ACT
     Uptime: 00:01:03, Timeout in: 00:02:27
     Incoming interface: Vlanif10
     List of 1 outgoing interfaces:
       1: LoopBack0
         Activetime: 00:23:15
     Matched 0 packets(0 bytes), Wrong If 0 packets
     Forwarded 0 packets(0 bytes)

00002. (FC00:AA::123, FF34::)
     MID: 1, Flags: ACT
     Uptime: 00:00:03, Timeout in: 00:03:27
     Incoming interface: Vlanif20
     List of 1 outgoing interfaces:
       1: LoopBack0
         Activetime: 00:23:15
     Matched 0 packets(0 bytes), Wrong If 0 packets
     Forwarded 0 packets(0 bytes)
```

Table 8-108 Description of the **display multicast ipv6 forwarding-table** command output

Item	Description
IPv6 Multicast Forwarding Table	IPv6 multicast forwarding table.
Total 2 entries, 2 matched	Total forwarding entries and total eligible forwarding entries.
00001	Number of the (S, G) entry.
(FC00:AA::123, FF33::)	(S, G) entry in the multicast routing table.
MID	Unique multicast forwarding entry in the MFIB table. MID is used to rapidly search the multicast forwarding table.

Item	Description
Flags	Status flag of the (S, G) entry. - ACT: indicates that an active event is triggered. - DUM: indicates a dummy entry. - MISS: indicates that the nocache time needs to be reported. - DROP: indicates packet dropping. - LTH: indicates that the traffic volume is below the threshold. - DEL: indicates a deleted entry. - RST: indicates that registration of the known timer is started. - 2IODEL: indicates that an entry is deleted from the MFIB table, and the update needs to be synchronized to the IO board. - 2PDEL: indicates that an entry is deleted from the device, and the update needs to be synchronized to the IO board. - 2SYNC: indicates that the entry is contained in the MFIB table but it does not exist on the device. - 2ADD: indicates that the entry existing on the device has not been added to the MFIB table. - CLR: indicates that the MFIB table is resetting. - L2FWD: indicates that the device forwards Layer 2 traffic in multicast mode. - NORPF: indicates that the device does not perform RPF check. - 2ACK: indicates that the VPN instance is waiting for the ACK message from the slave main control board. - 2RSED: indicates that the entry is waiting for retransmission. - IOACK: indicates that the VPN instance has received the ACK message from the device. - SACK: indicates that the VPN instance has received the ACK message forwarded by software.

Item	Description
	- BKCLR: indicates that the MFIB table on the slave main control board is resetting. - EXTR: indicates an extranet entry. - 2DEL: indicates that the entry deleted from the device has not been removed from the MFIB table. - PDEL: indicates that the entry does not exist on the device. - A denotes addition; D denotes deletion; I denotes upstream update; R denotes RP update; P denotes PMBR; F denotes flag. - S denotes SPT; E denotes encapsulation group update; US denotes status update; CS denotes status clearing.
Uptime	Period during which the (S, G) entry exists.
Timeout in	Remaining time of the (S, G) entry.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces: 1: LoopBack0	Outgoing interface list, including the outgoing interface number and name.
Activetime	Existing time of the outgoing interface of the (S, G) entry.
Matched 0 packets(0 bytes)	Bytes of multicast packets matching the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.
Wrong If 0 packets	Number of multicast packets matching the (S, G) entry but are not forwarded. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.

Item	Description
Forwarded 0 packets(0 bytes)	Number of packets and bytes forwarded by the (S, G) entry. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can provide the accurate counter values.

8.8.4 display multicast forwarding-table optimization-mode configuration

Function

The **display multicast forwarding-table optimization-mode configuration** command displays the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

display multicast forwarding-table optimization-mode configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, configurations of all slots are displayed.	The value is an integer and must be the slot ID of a running slot.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to display the configuration of the optimization mode in which Layer 3 multicast forwarding entries are stored. The configuration helps you select a slot based on your storage requirement.

Example

Display the configuration of the optimization modes.

```
<HUAWEI> display multicast forwarding-table optimization-mode configuration
Multicast forwarding-table optimization mode :
Slot      Mode
-------------------------
2         Normal mode
4         Normal mode
5         Rich MCast mode
```

Table 8-109 Description of the **display multicast forwarding-table optimization-mode configuration** command output

Item	Description
Multicast forwarding-table optimization mode	When the multicast optimization mode is enabled.
slot	Slot ID.
mode	Storage Mode. The following storage modes are available: ● Normal: The ARP cache table or ND cache table and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table. ● Rich MCast mode: also known as multicast optimization mode. The system allocates hardware resources preferentially to the multicast forwarding table. The ARP/ND cache table and routing table share hardware resources.

8.8.5 display multicast ipv6 routing-table

Function

The **display multicast ipv6 routing-table** command displays information about an IPv6 multicast routing table.

Format

display multicast ipv6 routing-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
incoming-interface	Indicates the incoming interface of a multicast forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of IPv6 PIM-SM.	-
outgoing-interface	Indicates the outgoing interface of a multicast forwarding entry.	-
include	Displays the (S, G) entries whose downstream interface list contains specified outgoing interfaces.	-
exclude	Displays the (S, G) entries whose downstream interface list does not contain specified outgoing interfaces.	-
match	Displays (S, G) entries whose the downstream interface list contains only one interface that is the same as a specified outgoing interface.	If no interface is specified, the (S, G) entry with the null downstream interface list is displayed.
none	Displays the routing entry without a downstream interface.	-
outgoing-interface-number	Displays the number of the outgoing interfaces of multicast routing entries.	-
number	Specifies the number of outgoing interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast ipv6 routing-table** command to view the IPv6 multicast routing table, including the multicast source address, multicast group address, upstream interface, and downstream interface list.

Example

Display the corresponding routing entry of a multicast group in the IPv6 multicast routing table.

```
<HUAWEI> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (FC00::2, FFE3::1)
       Uptime: 00:00:14
       Upstream Interface: Vlanif10
       List of 1 downstream interface
           1:  Vlanif20
```

Table 8-110 Description of the display multicast ipv6 routing-table command output

Item	Description
IPv6 multicast routing table	IPv6 multicast routing table.
Total 1 entry	Number of routing entries that meet the query condition.
00001	Sequence number of the (S, G) entry.
(FC00::2, FFE3::1)	(S, G) entry in the IPv6 multicast routing table.
Uptime	Period during which the (S, G) entry exists.
Upstream Interface	Upstream interface of the (S, G) entry.
List of 1 downstream interface	Downstream interface list.

Display the number of downstream interfaces of the IPv6 multicast routing entries.

```
<HUAWEI> display multicast ipv6 routing-table outgoing-interface-number
IPv6 multicast routing table
 Total 2 entries

 00001. (FC00::55, FF33::1)
       Uptime: 00:00:05
```

```
     Upstream Interface: Vlanif10
     List of 2 downstream interfaces

00002. (FC00::55, FF33::2)
     Uptime: 00:00:05
     Upstream Interface: Vlanif20
     List of 2 downstream interfaces
```

Table 8-111 Description of the display multicast ipv6 routing-table outgoing-interface-number command output

Item	Description
List of 2 downstream interfaces	Number of the outgoing interfaces of IPv6 multicast routing entries.

8.8.6 display multicast ipv6 rpf-info

Function

The **display multicast ipv6 rpf-info** command displays the Reverse Path Forwarding (RPF) routes of a specified IPv6 multicast source or source/group.

Format

display multicast ipv6 rpf-info *ipv6-source-address* [*ipv6-group-address*] [**rpt** | **spt**]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source, used to display the information of RPF routing corresponding to the source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-group-address	Specifies the IPv6 address of a multicast group, used to display the information of RPF routing corresponding to the group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
rpt	Displays the RPF routing information corresponding to a specified source or group on the RPT.	-
spt	Displays the RPF routing information corresponding to a specified source or group on the SPT.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The RPF route with the *ipv6-source-address* as the destination address is an optimal route selected from IPv6 unicast routes. You can use the **display multicast ipv6 rpf-info** command to check the RPF route to the specified source or source-group.

Example

Display all RPF routes to the source address FC00::101.

```
<HUAWEI> display multicast ipv6 rpf-info fc00::101
 VPN-Instance: public net
 RPF information about source: FC00::101
     RPF interface: Vlanif100
     Referenced route/mask: FC00::/64
     Referenced route type: unicast
     Load splitting rule: disabled
```

Table 8-112 Description of the display multicast ipv6 rpf-info command output

Item	Description
RPF information about source	Indicates the multicast source to which RPF information belongs.
RPF interface	Indicates the RPF interface.
Referenced route/mask	Indicates the referenced route and its mask.
Referenced route type	Indicates the referenced route type.
Load splitting rule	Load splitting rules: ● disable: load splitting disabled. ● balance-preferred: load balancing preferred. ● stable-preferred: stable-preferred load splitting. ● source: source address-based load splitting. ● group: group address-based load splitting. ● source-group: source and group addresses-based load splitting.

8.8.7 multicast ipv6 boundary

Function

The **multicast ipv6 boundary** command configures a multicast boundary on an interface.

The **undo multicast ipv6 boundary** command deletes the configured multicast boundary.

By default, no multicast boundary is configured on an interface.

Format

multicast ipv6 boundary { *ipv6-group-address ipv6-group-mask-length* | **scope** *scope-id* }

undo multicast ipv6 boundary { *ipv6-group-address ipv6-group-mask-length* | **all** | **scope** }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
scope *scope-id*	Specifies a scope ID.	The value is an integer that ranges from 3 to 15.
all	Deletes all the multicast boundaries configured on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Data of some multicast groups needs to be forwarded within a specified range. For example, each BSR administrative domain serves a specific group address range, and data packets sent from multicast sources to these groups need to be forwarded within the matching administrative domain. After a multicast boundary is configured for specified multicast groups on an interface, multicast packets sent to these groups cannot be forwarded through the interface. This restricts multicast forwarding within a range.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

To configure the boundary for different multicast groups, you can repeat the command on the same interface.

A and B are the forwarding boundary sets of the multicast group range to be configured, and B is a subset of A. If A is first configured on an interface, B cannot be configured. If you configure A on the interface that has been configured with B, B is replaced by A.

Example

Configure VLANIF100 as the boundary of group FF02::101/16.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] multicast ipv6 boundary FF02::101 16
```

Configure GE0/0/1 as the boundary of group FF02::101/16.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] multicast ipv6 boundary FF02::101 16
```

8.8.8 multicast ipv6 cpu-forward disable

Function

The **multicast ipv6 cpu-forward disable** command disables software forwarding for IPv6 multicast packets.

The **undo multicast ipv6 cpu-forward disable** command restores the default configuration.

By default, software forwarding for IPv6 multicast packets is enabled.

Format

multicast ipv6 cpu-forward disable

undo multicast ipv6 cpu-forward disable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, the switch forwards packets based on software before the hardware forwarding is completed. Then, the switch forwards packets based on hardware. Soft forwarding for multicast packets must be disabled on the switch to prevent packet loss and disorder caused by the low forwarding speed and first packet cache mechanism of soft forwarding.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Disable software forwarding for IPv6 multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 cpu-forward disable
```

8.8.9 multicast ipv6 forwarding-table downstream-limit

Function

The **multicast ipv6 forwarding-table downstream-limit** command sets the maximum number of downstream nodes of an entry in the IPv6 multicast forwarding table.

The **undo multicast ipv6 forwarding-table downstream-limit** command restores the default setting.

By default, the maximum number of downstream nodes of an entry is 128.

Format

multicast ipv6 forwarding-table downstream-limit *limit*

undo multicast ipv6 forwarding-table downstream-limit

Parameters

Parameter	Description	Value
limit	Indicates the maximum number of downstream nodes of an entry in the forwarding table.	The value is an integer that ranges from 0 to 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch receives a multicast packet, it copies the packet for each downstream node in the matching IPv6 multicast forwarding entry. If the switch has a large number of IPv6 multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the load on the switch, limit the maximum number of downstream nodes in each IPv6 multicast forwarding entry.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If the configured number is smaller than the current number, the excessive downstream nodes are not deleted immediately, and must be deleted by the IPv6 multicast routing protocol. In addition, no new downstream node can be added to the entry in the forwarding table.

Example

In the system view, set the maximum number of downstream nodes of an entry in the IPv6 multicast forwarding table to 32.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 forwarding-table downstream-limit 32
```

8.8.10 multicast ipv6 forwarding-table route-limit

Function

The **multicast ipv6 forwarding-table route-limit** command sets the limits on the number of entries in the IPv6 multicast forwarding table.

The **undo multicast ipv6 forwarding-table route-limit** command restores the default value of the limit.

The following lists the maximum number of entries allowed in the IPv6 multicast forwarding table of each model by default:

- S5720-LI, S5720S-LI: 496
- S5735S-H, S5736-S, S6720S-S: 512
- S5731-S, S5731S-S, S5720I-SI 1024
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: 1500
- S5732-H, S6730-H, S6730S-H: 2048
- S6730-S, S6730S-S, S5731-H, S5731S-H, S6735-S, S6720-EI, S6720S-EI: 4096

Format

multicast ipv6 forwarding-table route-limit *limit*

undo multicast ipv6 forwarding-table route-limit

Parameters

Parameter	Description	Value
limit	Specifies the limit on the number of entries in the IPv6 multicast forwarding table.	The value is an integer that ranges from 0 to *The maximum number of entries allowed in the multicast forwarding table by default.* **NOTE** The value range of S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H are expanded after the high specification mode is configured for multicast forwarding using the **set multicast forwarding-table super-mode** command. The actual value range depends on the specification of the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive IPv6 multicast forwarding entries will exhaust the memory of the switch. To prevent this problem, use the **multicast ipv6 forwarding-table route-limit** command to limit the number of entries in the IPv6 multicast forwarding table.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

If the limit on the number of entries in the IPv6 multicast forwarding table is set after multicast services are deployed on a switch, ensure that this limit is greater than or equal to the number of existing forwarding entries. Otherwise, faults may occur.

It is recommended that you set the limit based on the actual network environment before deploying multicast services on the switch.

If the newly-configured limit on the number of entries is smaller than the number of existing entries, the excessive entries are not deleted immediately. The configured limit takes effect in the following cases:

- Entries are added to the IPv6 multicast forwarding table after the existing entries age out.
- The **reset multicast ipv6 forwarding-table all** command is executed.

Example

Set the limit on the number of the entries in the IPv6 forwarding table to 1024.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 forwarding-table route-limit 1024
```

8.8.11 multicast ipv6 invalid-packet

Function

The **multicast ipv6 invalid-packet** command sets the maximum number of invalid IPv6 multicast protocol packets that can be stored on the switch.

The **undo multicast ipv6 invalid-packet** command deletes the set maximum number of invalid IPv6 multicast protocol packets that can be stored on the switch.

By default, the switch can save a maximum of 10 invalid packets for each specific IPv6 multicast protocol.

Format

multicast ipv6 invalid-packet { **mld** | **pim** } **max-count** *max-number*

undo multicast ipv6 invalid-packet { **mld** | **pim** }

Parameters

Parameter	Description	Value
mld	Sets the maximum number of invalid MLD messages.	-
pim	Sets the maximum number of invalid PIM (IPv6) messages.	-
max-count *max-number*	Sets the maximum number of invalid IPv6 multicast protocol packets that can be stored on a device.	The value is an integer that ranges from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If IPv6 multicast entries fail to be generated or peer relationships fail to be set up, you can enable the switch to store invalid IPv6 multicast protocol packets and view statistics and details of the invalid IPv6 multicast protocol packets. Based on the command output, you can locate and rectify faults.

Example

Set the maximum number of invalid MLD messages that can be stored on the switch to 20.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 invalid-packet mld max-count 20
```

8.8.12 multicast ipv6 load-splitting

Function

The **multicast ipv6 load-splitting** command enables load splitting among IPv6 multicast routes.

The **undo multicast ipv6 load-splitting** command restores the default configuration.

By default, load splitting among IPv6 multicast routes is disabled.

Format

multicast ipv6 load-splitting { **balance-preferred** | **stable-preferred** | **group** | **source** | **source-group** }

undo multicast ipv6 load-splitting

Parameters

Parameter	Description	Value
balance-preferred	Indicates balance-preferred load splitting. This policy is applicable to the scenario where hosts frequently join or leave groups, which requires automatic load adjustment.	-
group	Indicates group address-based load splitting. This policy is applicable to the scenario of one source to multiple groups.	-
source	Indicates source address-based load splitting. This policy is applicable to the scenario of multiple sources to one group.	-
source-group	Indicates source and group addresses-based load splitting. This policy is applicable to the scenario of multiple sources to multiple groups.	-
stable-preferred	Indicates stable-preferred load splitting. This policy is applicable to stable multicast networking.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the device selects the route with the largest next-hop address as the RPF route. To enable multicast data to be forwarded through multiple paths, run this command to configure multicast load splitting. After multicast load splitting is configured, the device uses the specified load splitting policy to distribute multicast data among multiple paths. This function improves quality of multicast forwarding.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Follow-up Procedure

Because the forwarding capabilities of equal-cost routes are different from the actual load distribution situation on the equal-cost routes, even load splitting cannot meet network requirements in some scenarios. In this case, you can run the **multicast ipv6 load-splitting weight** command to configure the IPv6 multicast load splitting weight on the interface to realize unbalanced load splitting.

Precautions

The five load splitting policies are mutually exclusive. It is recommended that you use a fixed load splitting policy based on the actual situation on your network. The **balance-preferred** or **stable-preferred** policy is preferred.

If PIM-DM (IPv6) is enabled on the switch, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure stable-preferred load splitting in the system view.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 load-splitting stable-preferred
```

8.8.13 multicast ipv6 load-splitting weight

Function

The **multicast ipv6 load-splitting weight** command sets the IPv6 multicast load splitting weight for an interface.

The **undo multicast ipv6 load-splitting weight** command restores the default setting.

By default, the IPv6 multicast load splitting weight of an interface is 1.

Format

multicast ipv6 load-splitting weight *weight-value*

undo multicast ipv6 load-splitting weight

Parameters

Parameter	Description	Value
weight-value	Specifies the IPv6 multicast load splitting weight of an interface.	The value is an integer that ranges from 0 to 32.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view, loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stable-preferred or balance-preferred multicast splitting policy is configured, you can run this command to set load splitting weights for interfaces to realize unbalanced load splitting. The larger weight value an interface has, the more IPv6 multicast routing entries have it as the upstream interface.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is applicable only when the IPv6 multicast load splitting policy is set to stable-preferred or balance-preferred.

When the IPv6 multicast load splitting weight on an interface is 0, the routes with this interface as the upstream interface do not take part in load splitting.

Example

Set the IPv6 multicast load splitting weight on VLANIF100 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] multicast ipv6 load-splitting weight 10
```

Set the IPv6 multicast load splitting weight on GE0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] multicast ipv6 load-splitting weight 10
```

8.8.14 multicast ipv6 load-splitting-timer

Function

The **multicast ipv6 load-splitting-timer** command sets an IPv6 multicast load splitting timer.

The **undo multicast ipv6 load-splitting-timer** command restores the default setting.

By default, the value of the IPv6 multicast load splitting timer is 1800 seconds.

Format

multicast ipv6 load-splitting-timer *interval*

undo multicast ipv6 load-splitting-timer

Parameters

Parameter	Description	Value
interval	Specifies the value of the IPv6 multicast load splitting timer.	The value is an integer that ranges from 10 to 1800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In stable-preferred load splitting or balance-preferred load splitting mode, entries may not be well-balanced among paths because of the addition or deletion of entries, change of load splitting weights of the paths, or change of equal-cost routes. In such a case, the device will balance entries after a certain waiting time to reduce the impact of frequent changes on the system.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is stable, for example, when entries are not deleted or added frequently or equal-cost routes are not changed frequently, set the load splitting timer value to a smaller value so that entries can be balanced rapidly. The recommended value is 300 to 600 seconds.
- If the network is not stable, for example, when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a larger value to reduce the impact of frequent entry changes on the system and network stability. The recommended value is 1200 to 1800 seconds.

Prerequisites

IPv6 multicast routing has been enabled globally using the **multicast ipv6 routing-enable** command in the system view.

Example

Set the IPv6 multicast load splitting timer to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
[HUAWEI] multicast ipv6 load-splitting-timer 100
```

8.8.15 multicast ipv6 routing-enable

Function

The **multicast ipv6 routing-enable** command enables the IPv6 multicast routing function.

The **undo multicast ipv6 routing-enable** command restores the default configuration.

By default, the IPv6 multicast routing function is disabled.

Format

multicast ipv6 routing-enable

undo multicast ipv6 routing-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring Layer 3 IPv6 multicast, you must enable the IPv6 multicast routing function globally. Layer 3 IPv6 multicast protocols (such as PIM (IPv6) and MLD) and other Layer 3 IPv6 multicast functions can be configured only after IPv6 multicast routing is enabled.

Precautions

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

NOTICE

The **undo multicast ipv6 routing-enable** command deletes all IPv6 multicast configurations of the device. If IPv6 multicast services are running on the device, the IPv6 multicast services are interrupted when this command is executed. To restore IPv6 multicast services on the instance, you must re-configure the corresponding commands.

Example

Enable IPv6 multicast routing globally.

```
<HUAWEI> system-view
[HUAWEI] multicast ipv6 routing-enable
```

8.8.16 multicast ttl-check disable

Function

The **multicast ttl-check disable** command disables a switch from checking the TTL value of multicast packets.

The **undo multicast ttl-check disable** command enables a switch to check the TTL value of multicast packets again.

By default, a switch checks the TTL value of multicast packets.

NOTE

This command is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

multicast ttl-check disable

undo multicast ttl-check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In V200R019C10 and later versions, when multicast packets between a multicast source and receiver are forwarded across VLANs, the multicast packets with a TTL value less than or equal to 1 will be discarded by default.

In versions earlier than V200R019C10, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not discard multicast packets whose TTL value is less than or equal to 1. After the switch software version is upgraded to V200R019C10 or later, however, if you want a switch not to discard multicast packets whose TTL value is less than or equal to 1, run the **multicast ttl-check disable** command to disable the switch from checking the TTL value of multicast packets.

The **multicast ttl-check disable** command does not apply to the following scenarios:

- This command is not applicable to multicast packets on a VPN. A switch always discards multicast packets on a VPN if their TTL value is less than or equal to 1.
- This command does not apply when a multicast source and receiver are in the same VLAN, in which case, the switch does not check the TTL value of multicast packets between them.
- When the forwarding mode of multicast packets is changed to MAC address-based forwarding, the switch does not check the TTL value of multicast packets.

Example

Disable a switch from checking the TTL value of multicast packets.

```
<HUAWEI> system-view
[HUAWEI] multicast ttl-check disable
```

8.8.17 reset multicast ipv6 forwarding-table

Function

The **reset multicast ipv6 forwarding-table** command clears the entries of the IPv6 multicast forwarding table.

Format

reset multicast ipv6 forwarding-table all

reset multicast ipv6 forwarding-table { *ipv6-group-address* [*ipv6-group-mask-length*] | *ipv6-source-address* [*ipv6-source-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
all	Resets all the multicast forwarding caches (MFCs) in the multicast forwarding table.	-
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 8 to 128.

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
incoming-interface	Indicates the incoming interface of a forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of IPv6 PIM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the IPv6 multicast forwarding table, multicast data will be interrupted for a period. Confirm the action before you use the command.

Example

Delete all the IPv6 multicast forwarding entries.

```
<HUAWEI> reset multicast ipv6 forwarding-table all
```

8.8.18 reset multicast ipv6 routing-table

Function

The **reset multicast ipv6 routing-table** command clears the entries in the IPv6 multicast routing table. The corresponding forwarding entries in the forwarding table are deleted at the same time.

Format

reset multicast ipv6 routing-table all

reset multicast ipv6 routing-table { *ipv6-group-address* [*ipv6-group-mask-length*] | *ipv6-source-address* [*ipv6-source-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
all	Resets all routing entries in the multicast core routing table.	-
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
incoming-interface	Indicates the incoming interface of a routing entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicate the register interface of IPv6 PIM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the IPv6 multicast routing table, the matching entries in the IPv6 multicast forwarding table are also deleted. As a result, multicast forwarding will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the entries of the group FF02::101 from the IPv6 multicast routing table.

```
<HUAWEI> reset multicast ipv6 routing-table FF02::101
```

8.8.19 set multicast forwarding-table optimization-mode

Function

The **set multicast forwarding-table optimization-mode** command configures the multicast optimization mode in which the Layer 3 forwarding entries are stored on a switch.

The **undo set multicast forwarding-table optimization-mode** command restores the default storage mode.

By default, a switch uses the normal storage mode.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support this command.

Format

set multicast forwarding-table optimization-mode [**slot** *slot-id*]

undo set multicast forwarding-table optimization-mode [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	*slot-id* specifies the slot that uses the multicast optimization mode. If no slot ID is specified, storage modes of all slots are configured to be the multicast optimization mode.	The value is an integer and must be the slot ID of a running slot.

Views

System view

Default Level

3: Management level

Usage Guidelines

Applicable Environment

In most cases, the Layer 3 forwarding entries are stored in normal mode. The ARP cache table, ND cache table, and multicast forwarding table share hardware resources, without affecting hardware resources allocated to the routing table.

This command optimizes storage resources of Layer 3 forwarding entries through preferential allocation of hardware resources preferentially to the multicast forwarding table. The ARP cache table, ND cache table, and routing table share hardware resources. Run this command if either of the following situations occurs:

- A large number of ARP prefix entries and multicast forwarding entries exist in the system at the same time.
- A large number of ND prefix entries and multicast forwarding entries exist in the system at the same time.

Precautions

Note the following points when running this command:

- If the multicast optimization modes on a switch are configured or deleted, the system prompts the user to save the configurations and then restart the device. If the device configuration is not saved, the new storage mode does not take effect after the restart.
- This function can be implemented on an IPv6 network only when a switch with an extended entry register is available. In addition, the storage mode of the register must be set to IPv6 mode. For details on how to configure the extended entry register, see **assign resource-mode** in "Device Management Commands > Hardware Configuration Commands".

NOTICE

When the user configures this mode or restores the default mode, the system will prompt the user to restart the device or a specified slot. If the system receives no response, the configuration times out, and the system view is displayed. The system does not restart. The restart can cause the network to crash for a short period. In most cases, this command is not recommended.

Example

Configure the storage mode to be the multicast optimization mode for a switch.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table optimization-mode
```

8.8.20 set multicast forwarding-table super-mode

Function

The **set multicast forwarding-table super-mode** command configures the high specification mode for multicast forwarding. In the high specification mode, the number of multicast entries can reach the maximum value supported by the switch, which is much more than the default limit.

The **undo set multicast forwarding-table super-mode** command restores the default configuration.

By default, the common specification mode is used for multicast forwarding after Layer 3 multicast is configured. In this mode, the number of multicast entries cannot exceed the default limit defined on the switch.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Format

set multicast forwarding-table super-mode

undo set multicast forwarding-table super-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 3 multicast is enabled, the common specification mode is used for multicast forwarding by default. This mode can meet requirements of most multicast service scenarios. In some large-scale multicast applications, a network has a large number of multicast sources to provide many channels for multicast users. In these applications, the number of multicast entries may exceed the default limit defined on a multicast device. When this occurs, some multicast entries cannot be generated. As a result, some users cannot receive the multicast data they request.

The **set multicast forwarding-table super-mode** command configures the high specification mode to increase the number of entries used for multicast forwarding. In high specification mode, the number of multicast entries supported by the switch is much larger than the default limit on the number of multicast entries. This mode maximizes a device's capability to support large-scale multicast applications.

Precautions

After you run this command:

- This command can only increase the number of Layer 3 multicast forwarding entries, but cannot increase the number of Layer 2 multicast forwarding entries. In scenarios when both Layer 2 and Layer 3 multicast services are configured, the number of Layer 3 multicast forwarding entries is limited by the number of Layer 2 multicast forwarding entries. Therefore, this command cannot increase the number of multicast forwarding entries if both Layer 2 and Layer 3 multicast services are configured.
- Restart the switch for the configuration to take effect.

- The default value of the IGMP general query interval changes from 60s to 120s. You can set the IGMP general query interval using the **igmp timer query** or **timer query (IGMP view)** command.
- The default value of the IGMP robustness variable changes from 2 to 3. You can set the robustness variable using the **igmp robust-count** or **robust-count (IGMP view)** command.
- The default value of the other querier present interval changes from 125s to 245s. You can set the other querier present interval using the **igmp timer other-querier-present** or **timer other-querier-present (IGMP view)** command.
- The default value of the MLD robustness variable changes from 2 to 3. You can set the robustness variable using the **mld robust-count** or **robust-count (MLD view)** command.
- The default interval for sending PIM-DM State-Refresh messages changes from 60s to 255s. On an IPv4 multicast network, run the **state-refresh-interval (IPv4)** command to set the interval for sending PIM-DM State-Refresh messages. On an IPv6 network, run the **state-refresh-interval (IPv6)** command to set the interval for sending PIM-DM State-Refresh messages.
- The default interval for sending PIM Join-Prune messages changes from 210s to 300s. On an IPv4 multicast network, run the **holdtime join-prune (IPv4)** or **pim holdtime join-prune** command to set the interval for sending PIM Join-Prune messages. On an IPv6 network, run the **holdtime join-prune (IPv6)** or **pim ipv6 holdtime join-prune** command to set the interval for sending PIM Join-Prune messages.
- Run the **car** command to change the rate limit for IGMP/MLD messages sent to the CPU according to the actual situations of multicast services.
- More system resources are consumed in the high specification mode. If the number of multicast protocol packets sent to the switch increases sharply in a short time, the CPU usage of the switch becomes high.
- It is recommended that you set the same general query interval on all the IGMP/MLD-enabled interfaces of a switch. For an IGMP-enabled interface, run the **igmp timer query** command in the interface view to set the general query interval. For an MLD-enabled interface, run the **mld timer query** command in the interface view to set the general query interval. This configuration prevents IGMP/MLD-enabled interfaces from sending Query messages at the same time, so that the switch does not have to process a large number of Report messages in a short time, which could cause a high CPU usage.
- In a stack, if member interfaces of an Eth-trunk interface are located on member switches that support different numbers of multicast forwarding entries, the maximum number of multicast forwarding entries supported by the Eth-Trunk interface depends on the member switch that supports the fewest multicast forwarding entries. Multicast forwarding entries supported by an Eth-Trunk interface meet either of the following conditions:
  - The outbound interface of the multicast forwarding entries is the Eth-Trunk interface that has been switched to the Layer 3 mode using the **undo portswitch** command.
  - The Eth-Trunk interface belongs to the VLANs corresponding to the VLANIF interfaces of the multicast forwarding entries.

Example

Configure the high specification mode for multicast forwarding.

```
<HUAWEI> system-view
[HUAWEI] set multicast forwarding-table super-mode
Warning: This command will modify some default multicast settings and has limitations
in a few special scenarios. Use the command according to product manual.Continue? [Y/N]:y
```

8.8.21 set multicast-hash-mode

Function

The **set multicast-hash-mode** command specifies a hash algorithm for multicast forwarding.

The **undo multicast-hash-mode** command restores the default hash algorithm for multicast forwarding.

By default, the crc-32-lower algorithm is used.

NOTE

Only the S6720-EI, S6735-S and S6720S-EI support support this command.

Format

set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

undo set multicast-hash-mode { **crc-32-upper** | **crc-32-lower** | **lsb** | **crc-16-upper** | **crc-16-lower** }

Parameters

Parameter	Description
crc-32-upper	
crc-32-lower	
lsb	
crc-16-upper	
crc-16-lower	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve multicast forwarding performance, the switch uses a hash algorithm to learn multicast addresses. If multiple addresses match a key value, a hash conflict occurs. A large number of hash conflicts will cause failures to learn some multicast addresses. When such a problem occurs, use an appropriate hash algorithm to reduce hash conflicts.

Precautions

- An appropriate hash algorithm can reduce but not eliminate hash conflicts.
- MAC addresses are distributed on a network randomly, so the system cannot determine the best hash algorithm. The default hash algorithm is the best algorithm in most cases, so changing the hash algorithm is not recommended.
- After changing the hash algorithm, restart the switch for the configuration to take effect.

Example

Set the hash algorithm for multicast forwarding to crc-32-upper.

```
<HUAWEI> system-view
[HUAWEI] set multicast-hash-mode crc-32-upper
```

8.9 VLAN-based IGMP Snooping Configuration Commands

8.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.9.2 dhcp-snooping user-offline remove igmp-snooping

Function

The **dhcp-snooping user-offline remove igmp-snooping** command enables the switch to delete the IGMP snooping entries of DHCP snooping users immediately after the users go offline.

The **undo dhcp-snooping user-offline remove igmp-snooping** command restores the default configuration.

By default, the switch does not delete the IGMP snooping entries of DHCP snooping users immediately after the users go offline.

Format

dhcp-snooping user-offline remove igmp-snooping

undo dhcp-snooping user-offline remove igmp-snooping

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, when IGMP snooping is enabled for DHCP snooping users, the switch does not delete the IGMP snooping entry of a user immediately after the user goes offline. The multicast flow requested by the user is still transmitted until the IGMP snooping entry of the user is aged out.

The **dhcp-snooping user-offline remove igmp-snooping** command enables the switch to delete the IGMP snooping entry of a DHCP snooping user immediately after the user goes offline, terminating the multicast flow requested by the user.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Example

Enable the system to delete IGMP snooping entries of DHCP snooping users immediately after the users go offline.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] dhcp-snooping user-offline remove igmp-snooping
```

8.9.3 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters.

Format

display igmp-snooping [**vlan** [*vlan-id*]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the IGMP snooping running parameters in a specified VLAN. If this parameter is not specified, the system displays the IGMP running parameters in all VLANs with IGMP snooping configured.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view the IGMP snooping running parameters.

To view the IGMP snooping configuration, run the **display igmp-snooping configuration** command.

Precautions

This command can display the IGMP snooping running parameters in a VLAN only when at least one interface in the VLAN is in Up state and IGMP snooping enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Display the IGMP snooping running parameters.

```
<HUAWEI> display igmp-snooping
 IGMP Snooping Information for VLAN 3
    IGMP Snooping is Enabled
    IGMP Version is Set to default 2
    IGMP Query Interval is Set to default 125s
    IGMP Max Response Interval is Set to default 10s
    IGMP Robustness is Set to default 2
    IGMP Last Member Query Interval is Set to default 1s
    IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
    IGMP Filter Group-Policy is not set
    IGMP Prompt Leave Disable
    IGMP Host-based Prompt Leave Disable
    IGMP Router Alert is Not Required
    IGMP Send Router Alert Enable
```

```
  IGMP Proxy Disable
  IGMP Report Suppress Disable
  IGMP Suppress Time is set to default 10 seconds
  IGMP Querier Disable
  IGMP Router Port Learning Enable
  IGMP SSM-Mapping Disable
  IGMP Limit Action Disable
  IGMP Suppress-dynamic-join Disable
IGMP Snooping Information for VLAN 4
  IGMP Snooping is Enabled
  IGMP Version is 3
  IGMP snooping version 3 uses ASM-SSM mode
  IGMP Query Interval is Set to default 125s
  IGMP Max Response Interval is Set to default 10s
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1s
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is not set
  IGMP Prompt Leave Disable
  IGMP Host-based Prompt Leave Disable
  IGMP Router Alert is Not Required
  IGMP Send Router Alert Enable
  IGMP Proxy Disable
  IGMP Report Suppress Disable
  IGMP Suppress Time is set to default 10 seconds
  IGMP Querier Disable
  IGMP Router Port Learning Enable
  IGMP SSM-Mapping Disable
  IGMP Limit Action Disable
  IGMP Suppress-dynamic-join Disable
```

Table 8-113 Description of the **display igmp-snooping** command output

Item	Description
IGMP Snooping Information for VLAN 3	The following information displayed is the IGMP snooping running parameters in VLAN 3.
IGMP Snooping is Enabled	IGMP snooping is enabled in the VLAN. By default, IGMP snooping is disabled in a VLAN. IGMP snooping can be enabled in a VLAN using the **igmp-snooping enable (VLAN view)** command.
IGMP Version is Set to default 2 IGMP Version is 3	Version of IGMP messages that can be processed in the VLAN. The default version is 2, indicating that both IGMPv1 and IGMPv2 messages can be processed. This parameter is configured using the **igmp-snooping version** command.
IGMP snooping version 3 uses ASM-SSM mode	The ASM-SSM model is used for IGMPv3. This parameter is configured using the **igmp-snooping version** command.
IGMP Query Interval is Set to default 125s	Interval at which IGMP General Query messages are sent. In this example, the default value (125 seconds) is displayed. This parameter is configured using the **igmp-snooping query-interval** command.

Item	Description
IGMP Max Response Interval is Set to default 10s	Maximum response time for IGMP General Query messages. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **igmp-snooping max-response-time** command.
IGMP Robustness is Set to default 2	IGMP robustness variable. In this example, the default value 2 is displayed. This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1s	Interval at which IGMP Group-Specific Query messages are sent. In this example, the default value (1 second) is displayed. This parameter is configured using the **igmp-snooping lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s or holdtime in hello	Aging time of a router port. In this example, the default value (180 seconds or the holdtime value contained in PIM Hello messages) is displayed. This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is not set	Multicast group policy. In this example, the default configuration is displayed. That is, no policy is configured. A multicast group policy is configured using the **igmp-snooping group-policy** command.
IGMP Prompt Leave Disable	The fast leave function is disabled for interfaces in the VLAN (default configuration). The fast leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Host-based Prompt Leave Disable	The host-based fast leave function is disabled (default configuration). The host-based fast leave function can be enabled using the **igmp-snooping host-based prompt-leave** command.
IGMP Router Alert is Not Required	The switch does not require that the IGMP messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The switch can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.

Item	Description
IGMP Send Router Alert Enable	The switch sends the IGMP messages with the Router-Alert option to the VLAN (default configuration). The switch can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Router Port Learning Enable	Router port learning is enabled (default configuration). Router port learning can be enabled using the **igmp-snooping router-learning** command.
IGMP Proxy Disable	IGMP snooping proxy is disabled (default configuration). IGMP snooping proxy can be enabled using the **igmp-snooping proxy** command.
IGMP Report Suppress Disable	IGMP message suppression is disabled (default configuration). IGMP message suppression can be enabled using the **igmp-snooping report-suppress** command.
IGMP Suppress Time is set to default 10 seconds	IGMP message suppression time. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **igmp-snooping suppress-time** command.
IGMP Querier Disable	IGMP snooping querier is disabled (default configuration). IGMP snooping querier can be enabled using the **igmp-snooping querier enable** command.
IGMP SSM-Mapping Disable	IGMP snooping SSM mapping is disabled (default configuration). IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.
IGMP Limit Action Disable	Layer 2 multicast entry overwriting is disabled (default configuration). Layer 2 multicast entry overwriting can be enabled using the **igmp-snooping limit-action** command.
IGMP Suppress-dynamic-join Disable	Report and Leave messages received in the VLAN can be forwarded to the upstream multicast device with static multicast groups configured (default configuration). This function can be disabled using the **igmp-snooping static-group suppress-dynamic-join** command.

8.9.4 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration.

Format

display igmp-snooping [**vlan** [*vlan-id*]] **configuration**

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the IGMP snooping configuration in a specified VLAN. If this parameter is not specified, the system displays the IGMP snooping configuration in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the IGMP snooping configuration so that you can check whether the IGMP snooping configuration made in the system is proper.

To check all IGMP snooping running parameters, run the **display igmp-snooping** command.

Prerequisites

The IGMP snooping configuration in a VLAN can be displayed as long as IGMP snooping parameters have been configured in the VLAN, no matter whether the VLAN contains interfaces in Up state.

Global IGMP snooping must be enabled using the **igmp-snooping enable (system view)** command before any IGMP snooping configuration is performed.

Example

Display the IGMP snooping configuration in all VLANs.

```
<HUAWEI> display igmp-snooping configuration
 IGMP Snooping Configuration for VLAN 7
    igmp-snooping enable
    igmp-snooping version 3
    igmp-snooping ssm-mapping enable
    igmp-snooping ssm-policy 2000
    igmp-snooping ssm-mapping 232.1.1.0 255.255.255.0 10.1.2.1
```

8.9.5 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about multicast group member ports.

Format

display igmp-snooping port-info [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays information about multicast group member ports in a specified VLAN. If this parameter is not specified, the system displays multicast group member ports in all VLANs.	The value is an integer ranging from 1 to 4094.
group-address *group-address*	Displays information about member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When the switch with IGMP snooping enabled receives IGMP messages exchanged between hosts and a Layer 3 device, the switch maintains a Layer 2 multicast forwarding table based on information in the messages. The **display igmp-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink ports of the switch have multicast users connected, and control multicast services conveniently.

Precautions

This command can display information about multicast group member ports in a VLAN only when IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command, and at least one interface in the VLAN is in Up state. If interfaces in the VLAN are dynamic group member ports, the command can display information about these member ports only after they receive IGMP Report messages and before their aging time expires.

Example

Display information about multicast group member ports in VLAN 7.

```
<HUAWEI> display igmp-snooping port-info vlan 7
-------------------------------------------------------------------------------
                       (Source, Group)  Port                      Flag
             Flag: S:Static    D:Dynamic    M: Ssm-mapping
-------------------------------------------------------------------------------
 VLAN 7, 2 Entry(s)
                        (*, 225.0.0.1)  GE0/0/1                   -D-
                                               1 port(s) include
                  (1.1.1.1, 225.0.0.1)  GE0/0/1                   -D-
                                               1 port(s) exclude
-------------------------------------------------------------------------------
```

Table 8-114 Description of the **display igmp-snooping port-info** command output

Item	Description
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. Multicast data is sent from multicast source S to group G. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.
Port	Member port. **include** and **exclude** indicate the multicast source filtering mode.
Flag	Type of a member port, which can be: ● S: static member port, which is configured using the **l2-multicast static-group** command ● D: dynamic member port learned through IGMP snooping ● M: member port established through SSM mapping
VLAN *x*, *x* Entry(s)	VLAN ID and the number of entries in the VLAN.

Display detailed information about all multicast group member ports.

```
<HUAWEI> display igmp-snooping port-info verbose

The port information of Group 225.0.0.1 on VLAN
100:
   Time of this group has been up : 00:00:55

  The port information of (0.0.0.0, 225.0.0.1):
   Time of this source has been up : 00:00:55
   Port Table on this source(0.0.0.0):
   List of ports in include mode:
     No.1
       Port name : GE0/0/1
       Time of this port has been up as a host-port : 00:00:55
       Remain time of port expire as dynamic host-port :
00:03:33
       Host-port flags : Dynamic
   There are 1 port(s) in include mode.

  The port information of (1.1.1.1, 225.0.0.1):
   Time of this source has been up : 00:00:55
   Port Table on this source(1.1.1.1):
   List of ports in exclude mode:
     No.1
       Port name : GE0/0/1
       Time of this port has been up as a host-port : 00:00:55
       Remain time of port expire as dynamic host-port :
00:03:33
       Host-port flags : Dynamic
   There are 1 port(s) in exclude mode.
```

Table 8-115 Description of the display igmp-snooping port-info verbose command output

Item	Description
The port information of Group *xxx*	Information about member ports of multicast group in VLAN.
Time of this group has been up	Time that elapsed since the multicast group was set up.
The port information of *xxx*	Information about member ports of a specified (S, G).
Time of this source has been up	Time that elapsed since the multicast source was set up.
Port Table on this source	List of member ports of the specified multicast source.
List of ports in include mode	Information about member ports that join a multicast group in INCLUDE mode.
List of ports in exclude mode	Information about member ports that join a multicast group in EXCLUDE mode.
No.1	First member port.
Port name	Type and number of the first member port.
Time of this port has been up as a host-port	Time that elapsed since the first member port was bound to a source or (S, G).
Remain time of port expire as dynamic host-port	Remaining aging time of the first member port. This field displays "NA" for a static member port. The aging time of a dynamic member port is calculated using the following formula: Aging time = Robustness variable x General query interval + Maximum response time for General Query messages. The robustness variable is configured using the **igmp-snooping robust-count** command. The general query interval is configured using the **igmp-snooping query-interval** command. The maximum response time for General Query messages is configured using the **igmp-snooping max-response-time** command.
Version2-host-present-timer-expiry	Aging time of the IGMPv2 host.
Version1-host-present-timer-expiry	Aging time of the IGMPv1 host.

Item	Description
Host-port flags	Type of a member port, which can be: - Static: static member - Dynamic: dynamic member port learned through IGMP snooping - Mapping: member port established through SSM mapping
There are *x* port(s) in include mode	Number of member ports that join a multicast group in INCLUDE mode.
There are *x* port(s) in exclude mode	Number of member ports that join a multicast group in EXCLUDE mode.

8.9.6 display igmp-snooping host-tracking

Function

The **display igmp-snooping host-tracking** command displays information about group member hosts.

Format

display igmp-snooping host-tracking [**vlan** *vlan-id* [**group-address** *group-address*]] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays information about group member hosts in a specified VLAN. If this parameter is not specified, the command displays information about group member hosts in all VLANs.	The value is an integer that ranges from 1 to 4094.
group-address *group-address*	Displays information about member hosts of a specified multicast group. If this parameter is not specified, the command displays information about member hosts of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about group member hosts on a specified interface. If this parameter is not specified, the command displays information about group member hosts on all interfaces. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

IGMP snooping creates and maintains a Layer 2 multicast forwarding table by listening to IGMP messages exchanged between hosts and an upstream Layer 3 device. You can use this command to view information about member hosts in the Layer 2 multicast forwarding table. The command output shows which hosts under group member ports are using multicast services, helping you manage multicast services.

Precautions

If no forwarding entry is available for a member host, the command does not display information about this host.

Example

Display information about group member hosts.

```
<HUAWEI> display igmp-snooping host-tracking
-------------------------------------------------------------------------------------------------
VLAN                    (Source, Group)       Interface         Reporter         Mode
-------------------------------------------------------------------------------------------------
100                    (*, 225.0.0.2)       GE0/0/1          192.51.100.1      Include
100               (192.1.1.1,225.0.0.1)       GE0/0/1          10.10.5.2        Exclude
-------------------------------------------------------------------------------------------------
```

Table 8-116 Description of the **display igmp-snooping host-tracking** command output

Item	Description
VLAN	VLAN ID.
(Source, Group)	(S, G) entry, indicating that data is sent from multicast source S to group G. If Source is displayed as *, multicast data may be sent from any multicast source. If Source is displayed as an IP address, multicast data is sent from this IP address.
Interface	Group member interface.
Reporter	Host IP address.
Mode	Mode in which an interface filters multicast traffic specified by (S,G) entries. ● Include: The interface receives multicast traffic specified by (S,G) entries. ● Exclude: The interface does not receive multicast traffic specified by (S,G) entries.

8.9.7 display igmp-snooping qinq-port-info

Function

The **display igmp-snooping qinq-port-info** command displays multicast group membership on a QinQ or dot1q termination sub-interface.

Format

display igmp-snooping qinq-port-info interface *interface-type interface-number* [**group-address** *group-address*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays multicast group membership of a specified interface.	-

Parameter	Description	Value
group-address *group-address*	Displays group membership of a specified multicast group. If this parameter is not specified, the command displays group membership of all multicast groups on the specified interface.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command is used to check group membership on a QinQ or dot1q termination sub-interface.

Example

Display group membership of all multicast groups on QinQ termination sub-interface GE0/0/18.1.

```
<HUAWEI> display igmp-snooping qinq-port-info interface GigabitEthernet 0/0/18.1
Interface GigabitEthernet0/0/18.1, 1 Group(s)
 (Source,Group)                    PE-VID/CE-VID LiveTime          Flag
 -------------------------------------------------------------------------------
 (*,225.0.0.1)                    1001/0        --                S-
 (*,225.0.0.2)                    1001/0        00:00:23          -D-
```

Table 8-117 Description of the **display igmp-snooping qinq-port-info** command output

Item	Description
Interface GigabitEthernet0/0/18.1, 1 Group(s)	Group membership on a termination sub-interface.
(Source, Group)	(S, G) entry. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.

Item	Description
PE-VID/CE-VID	Outer VLAN ID and inner VLAN ID.
LiveTime	Time elapsed since the group is discovered, in any of the following formats: ● If the time is shorter than or equal to 24 hours, the format is hh:mm:ss. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is day:hour. ● If the time is longer than one week, the format is week:day. -- indicates that the group Up time is not obtained.
Flag	Type of a member port, which can be: ● S: static member port, which is configured using the **igmp static-group** command ● D: dynamic member port learned through IGMP snooping ● M: member port established through SSM mapping

8.9.8 display igmp-snooping querier

Function

The **display igmp-snooping querier** command displays whether the IGMP snooping querier function is enabled in a VLAN.

Format

display igmp-snooping querier vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays whether the IGMP snooping querier function is enabled in a specified VLAN. If *vlan-id* is not specified, the system displays status of the IGMP snooping querier function in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can configure an IGMP snooping querier on the switch to send IGMP Query messages in place of the upstream Layer 3 device in the following situations:

- The Layer 3 device cannot send IGMP messages for some reasons, for example, IGMP is not enabled on the Layer 3 device.
- The Layer 3 device uses static multicast forwarding entries and does not need to learn multicast forwarding entries.

You can use the **display igmp-snooping querier** command to check in which VLANs the IGMP snooping querier function is enabled.

Precautions

The querier function is disabled in a VLAN by default after IGMP snooping is enabled in the VLAN. To enable the querier function, run the **igmp-snooping querier enable** command.

Example

Display the status of the IGMP snooping querier function in all VLANs.

```
<HUAWEI> display igmp-snooping querier vlan
 VLAN              Querier-state
------------------------------------------------
 10                Enable
 20                Disable
 30                Disable
------------------------------------------------
 total entry 3
```

Table 8-118 Description of the **display igmp-snooping querier vlan** command output

Item	Description
VLAN	VLAN ID.
Querier-state	Querier status in a VLAN. ● Disable: The IGMP snooping querier function is disabled in the VLAN. ● Enable: The IGMP snooping querier function is enabled in the VLAN.
total entry 3	Number of VLANs in which the querier status is displayed.

8.9.9 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified VLAN, including static and dynamic router ports.

Format

display igmp-snooping router-port vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays information about the router ports in a specified VLAN. If *vlan-id* is not specified, the command displays router ports in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects the switch to an upstream Layer 3 multicast device. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message or a PIM Hello message.

You can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and aging time of a router port.

Precautions

This command can display information about router ports in a VLAN only when IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command, and at least one interface in the VLAN is in Up state.

Example

Display information about router ports in VLAN 2.

```
<HUAWEI> display igmp-snooping router-port vlan 2
Port Name              UpTime      Expires     Flags
```

```
-------------------------------------------------------------
VLAN 2, 2 router-port(s)
GE0/0/1                03:28:16    00:01:20    DYNAMIC
GE0/0/2                2d:10h      --          STATIC
```

Table 8-119 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Type and number of a router port.
UpTime	Time that elapsed since the interface became a router port.
Expires	Aging time of the router port. ● The aging time is displayed for a dynamic router port. This parameter is configured using the **igmp-snooping router-aging-time** command. ● For a static router port, "--" is displayed, indicating that the static router does not age.
Flags	Type of the router port, which can be: ● STATIC: static router port configured using the **igmp-snooping static-router-port** command. ● DYNAMIC: dynamic router port

8.9.10 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays IGMP snooping statistics in a specified VLAN. - If *vlan-id* is not specified, the system displays IGMP snooping statistics in all VLANs. - If *vlan-id* is specified, the system displays statistics about IGMP messages in the specified VLAN, but does not display the counts of IGMP snooping events that occur in the VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration, you can use the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent, number of IGMP messages received, number of PIM Hello messages received in each VLAN, and number of Layer 2 events that have occurred in all VLANs. Layer 2 events include changes in interface status, changes in VLAN status, changes in VLAN member interfaces (interfaces join or leave VLANs), and MSTP events. When a multicast fault occurs, the IGMP snooping statistics help you identify the cause of the fault.

Precautions

This command displays IGMP snooping statistics only when IGMP snooping has been enabled globally using the **igmp-snooping enable (VLAN view)** command.

Example

Display IGMP snooping statistics in all VLANs.

```
<HUAWEI> display igmp-snooping statistics vlan
 IGMP Snooping Events Counter
```

```
    Recv VLAN Up Event Times      3
    Recv VLAN Down Event Times    0
    Recv VLAN Del Event Times     0
    Recv Port Up Event Times      2
    Recv Port Down Event Times    0
    Recv Port Del Event Times     0
    Recv Port Inc Event Times     0
    Recv Port Exc Event Times     0
    Recv MSTP Block Event Times   0
    Recv MSTP Forward Event Times 0
    Recv LINK Change Event Times  0
 IGMP Snooping Packets Counter
  Statistics for VLAN 10
    Recv V1 Report          0
    Recv V2 Report          0
    Recv V3 Report          0
    Recv V1 Query           0
    Recv V2 Query           0
    Recv V3 Query           0
    Recv General Query      0
    Recv Leave              0
    Recv Pim Hello          0
    Send Query(S=0)         0
    Send Query(S!=0)        0
    Suppress Report         0
    Suppress Leave          0
    Proxy Send General Query              0
    Proxy Send Group-Specific Query       0
    Proxy Send Group-Source-Specific Query 0
```

Display IGMP snooping statistics in VLAN 10.

```
<HUAWEI> display igmp-snooping statistics vlan 10
 IGMP Snooping Packets Counter
  Statistics for VLAN 10
    Recv V1 Report  16
    Recv V2 Report  8768
    Recv V3 Report  0
    Recv V1 Query   0
    Recv V2 Query   2243
    Recv V3 Query   0
    Recv Leave      215
    Recv Pim Hello  0
    Send Query(S=0) 0
    Send Query(S!=0)529
    Suppress Report         0
    Suppress Leave          0
    Proxy Send General Query              0
    Proxy Send Group-Specific Query       0
    Proxy Send Group-Source-Specific Query 0
```

Table 8-120 Description of the display igmp-snooping statistics command output

Item	Description
IGMP Snooping Events Counter	Statistics on IGMP snooping events, including changes in interface status, changes in VLAN status, interfaces joining or leaving VLANs, and MSTP events.
Recv VLAN Up Event Times	Number of VLAN Up events.
Recv VLAN Down Event Times	Number of VLAN Down events.
Recv VLAN Del Event Times	Number of VLAN deletion events.

Item	Description
Recv Port Up Event Times	Number of interface Up events.
Recv Port Down Event Times	Number of interface Down events.
Recv Port Del Event Times	Number of interface deletion events.
Recv Port Inc Event Times	Number of times interfaces join VLANs.
Recv Port Exc Event Times	Number of times interfaces leave VLANs.
Recv MSTP Block Event Times	Number of times static groups fail to be created on interfaces that are blocked by MSTP and cannot forward multicast packets.
Recv MSTP Forward Event Times	Number of times static groups are successfully created on interfaces that are in MSTP forwarding state and can forward multicast packets normally.
Recv LINK Change Event Times	Number of link status change events.
IGMP Snooping Packets Counter	Statistics on IGMP Snooping packets.
Statistics for VLAN 10	Packet statistics in VLAN 10.
Recv V1 Report	Number of IGMPv1 Report messages received.
Recv V2 Report	Number of IGMPv2 Report messages received.
Recv V3 Report	Number of IGMPv3 Report messages received.
Recv V1 Query	Number of IGMPv1 Query messages received.
Recv V2 Query	Number of IGMPv2 Query messages received.
Recv V3 Query	Number of IGMPv3 Query messages received.
Recv General Query	Interval for sending IGMP General Query messages.
Recv Leave	Number of IGMP Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.
Send Query(S=0)	Number of IGMP Query messages sent with the source address 0.0.0.0.
Send Query(S!=0)	Number of IGMP Query messages sent with source addresses other than 0.0.0.0.
Suppress Report	Number of duplicate IGMP Report messages dropped.
Suppress Leave	Number of duplicate IGMP Leave messages dropped.

Item	Description
Proxy Send General Query	Number of General Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Specific Query	Number of Group-Specific Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent by the IGMP snooping proxy.

8.9.11 display l2-multicast forwarding-mode

Function

The **display l2-multicast forwarding-mode** command displays the Layer 2 multicast forwarding mode in VLANs.

Format

display l2-multicast forwarding-mode vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the Layer 2 multicast forwarding mode in a specified VLAN. If *vlan-id* is not specified, the system displays the Layer 2 multicast forwarding mode in all VLANs.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on the switch, the switch maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the switch searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The switch determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

To check which Layer 2 multicast forwarding mode is used, run the **display l2-multicast forwarding-mode** command.

Precautions

You can change the forwarding mode using the **l2-multicast forwarding-mode** command.

Example

Display the Layer 2 multicast forwarding mode in all VLANs.

```
<HUAWEI> display l2-multicast forwarding-mode vlan
VLAN                 Forwarding-mode        Router-discard
-------------------------------------------------------------
1                    IP                     disable
2                    IP                     disable
3                    MAC                       disable
```

Table 8-121 Description of the **display l2-multicast forwarding-mode vlan** command output

Item	Description
VLAN	VLAN ID.
Forwarding-mode	Forwarding mode used in a VLAN, which can be: ● MAC address-based forwarding ● IP address-based forwarding This parameter can be configured using the **l2-multicast forwarding-mode** { **ip** | **mac** } command.
Router-discard	Whether the switch is configured not to forward multicast data packets to router ports in a VLAN. ● enable: The switch does not forward multicast data packets to router ports in the VLAN. ● disable: The switch forwards multicast data packets to router ports in the VLAN. This function is configured using the **l2-multicast router-port-discard** command.

8.9.12 display l2-multicast forwarding-table vlan

Function

The **display l2-multicast forwarding-table vlan** command displays the Layer 2 multicast forwarding table in VLANs.

Format

display l2-multicast forwarding-table vlan [*vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]]

Parameters

Parameter	Description	Value
vlan-id	Displays Layer 2 multicast forwarding entries in a specified VLAN. If *vlan-id* is not specified, the command displays Layer 2 multicast forwarding entries in all VLANs.	The value is an integer that ranges from 1 to 4094.
source-address *source-address*	Displays the forwarding entries of a specified Layer 2 multicast source.	The value is in dotted decimal notation.
group-address *group-address*	Displays multicast forwarding entries of a specified Layer 2 multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
router-group	Displays Layer 2 multicast forwarding entries of all router ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table. This command displays statically configured and dynamically learned multicast forwarding entries.

Each entry contains the multicast source, multicast group, list of outbound interfaces, and VLAN ID of multicast data packets. When the IGMP snooping version is set to v3 in a VLAN or when the IGMP snooping version is set to v2 or v1 but SSM mapping is configured, the **display l2-multicast forwarding-table** command displays (S, G) entries.

Precautions

This command displays Layer multicast forwarding entries in a VLAN only when the VLAN is in Up state (At least one interface in the VLAN is in Up state. If interfaces in the VLAN are dynamic group member ports, the interfaces must have received IGMP Report messages and have not been aged out.)

Example

Display multicast forwarding entries in VLAN 10.

```
<HUAWEI> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
Total Group(s): 2
-------------------------------------------------------------------------------
             (Source, Group)     Interface                Out-Vlan
-------------------------------------------------------------------------------
                 Router-port    GigabitEthernet0/0/1           10
               (*, 225.1.1.6)    GigabitEthernet0/0/1           10
                                GigabitEthernet0/0/2           10
            (*, 235.80.68.83)    GigabitEthernet0/0/1           10
                                GigabitEthernet0/0/2           10
-------------------------------------------------------------------------------
```

Table 8-122 Description of the **display l2-multicast forwarding-table** command output

Item	Description
VLAN ID	VLAN ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode in the VLAN, which can be: ● IP ● MAC The multicast forwarding mode is configured using the **l2-multicast forwarding-mode** command.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. The Router-port field indicates a router port.
Interface	Outbound interface. The value **Stream** indicates an unknown flow entry.
Out-Vlan	VLAN ID of packets.
Total Group(s)	Total number of multicast forwarding entries.

8.9.13 display l2-multicast forwarding-table statistics

Function

The **display l2-multicast forwarding-table statistics** command displays statistics about Layer 2 multicast forwarding entries.

Format

display l2-multicast forwarding-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring IGMP snooping, you can use this command to view statistics about Layer 2 multicast forwarding entries.

Example

Display statistics about Layer 2 multicast forwarding entries. (The actual output information may differ from the following information.)

```
<HUAWEI> display l2-multicast forwarding-table statistics
---------------------------------------------------------------------
0 Stream entries are calculated in statistics
1 IP entries are calculated in statistics
0 MAC entries are calculated in statistics
1 VLAN entries are calculated in statistics
0 VPLS entries are calculated in statistics
0 VXLAN entries are calculated in statistics
---------------------------------------------------------------------
```

Table 8-123 Description of the **display l2-multicast forwarding-table statistics** command output

Item	Description
Stream entries are calculated in statistics	Number of unknown stream entries in a VLAN.
IP entries are calculated in statistics	Number of entries for IP address-based forwarding in a VLAN.
MAC entries are calculated in statistics	Number of entries for MAC address-based forwarding in a VLAN.
VLAN entries are calculated in statistics	Number of entries for IP address-based and MAC address-based forwarding in a VLAN.
VPLS entries are calculated in statistics	Number of entries for MAC address-based forwarding on a VPLS network.

Item	Description
VXLAN entries are calculated in statistics	Number of entries for MAC address-based forwarding on a VXLAN network.

8.9.14 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally or in specified VLANs.

The **undo igmp-snooping enable** command disables IGMP snooping globally or in specified VLANs.

By default, IGMP snooping is disabled globally and in a VLAN.

Format

igmp-snooping enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo igmp-snooping enable [**vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }]

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Enables IGMP snooping in a VLAN or in multiple VLANs. *vlan-id1* and *vlan-id2* identify a range of VLAN IDs. If VLAN IDs are specified, IGMP snooping is enabled in the specified VLANs. If no VLAN ID is specified, IGMP snooping is enabled globally.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Disables IGMP snooping in all VLANs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping runs on a Layer 2 device between a Layer 3 multicast device and hosts. By listening on the multicast protocol packets exchanged between the Layer 3 device and hosts, IGMP snooping maintains a multicast forwarding table to control Layer 2 multicast forwarding.

Before configuring IGMP snooping parameters, run the **igmp-snooping enable** command in the system view to enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after IGMP snooping is enabled globally.

You can enable IGMP snooping in multiple VLANs by using the **igmp-snooping enable** command in the system view.

Prerequisites

To enable IGMP snooping in multiple VLANs, ensure that IGMP snooping has been enabled globally.

Precautions

If you run the **igmp-snooping enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command multiple times, all the configurations take effect.

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configurations are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the switch uses the default IGMP snooping configuration.

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

The **igmp snooping enable** command in a VLAN and the **igmp on-demand** configuration of the VLANIF interface are mutually exclusive.

After global IGMP snooping is enabled on a switch, the switch sends all the IGMP messages received from a VLAN to the CPU for processing. If the multicast service is not configured in a VLAN and you want the switch to directly forward the IGMP messages of this VLAN without sending them to the CPU, run the **protocol-transparent** command in the VLAN view to enable transparent transmission of protocol packets.

Example

Enable IGMP snooping globally.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

Enable IGMP snooping in multiple VLANs.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan batch 2 to 10
[HUAWEI] igmp-snooping enable vlan 2 to 10
```

8.9.15 igmp-snooping enable (VLAN view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a VLAN.

The **undo igmp-snooping enable** command disables IGMP snooping in a VLAN.

By default, IGMP snooping is disabled in a VLAN.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP snooping is not enabled in a VLAN after being enabled in the system view. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable** command in the VLAN view.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

After IGMP snooping is enabled in a VLAN, this function takes effect only on interfaces in this VLAN.

After IGMP snooping is enabled globally, it is recommended that you enable IGMP snooping in all other VLANs. This prevents IGMP messages in this VLAN from being broadcast to access switches in the other VLANs.

Precautions

The **igmp snooping enable** command in a VLAN and the **igmp on-demand** configuration of the VLANIF interface are mutually exclusive.

If Layer 2 and Layer 3 multicast are both configured in a VLAN, you must delete the Layer 2 multicast configuration before you can modify or delete the Layer 3 multicast configuration. This means that you must disable IGMP snooping in the VLAN first, then modify or disable the IGMP and PIM (IPv4) configuration in the VLANIF interface view, and finally enable IGMP snooping in the VLAN. Otherwise, the Layer 3 multicast configuration cannot be modified or deleted on the corresponding VLANIF interface.

Example

Enable IGMP snooping in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
```

8.9.16 igmp-snooping fast-switch enable

Function

The **igmp-snooping fast-switch enable** command enables fast multicast forwarding path switching upon STP topology changes.

The **undo igmp-snooping fast-switch enable** command disables fast multicast forwarding path switching upon STP topology changes.

By default, fast multicast forwarding path switching upon STP topology changes is disabled.

Format

igmp-snooping fast-switch enable

undo igmp-snooping fast-switch enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the Layer 2 network topology changes, multicast forwarding paths may change. You can configure the switch to send Query messages upon topology changes using the **igmp-snooping send-query enable** command. In this way, multicast data flows can be switched to new forwarding paths quickly after the Layer 2 network topology changes. However, the downstream device may not receive the Query message immediately after convergence of the Layer 2 network, because the Query message is sent after a certain interval (60s by default). As a result, multicast traffic cannot be quickly switched to the new forwarding paths.

If the Layer 2 network is running the Spanning Tree Protocol (STP), you can enable fast multicast forwarding path switching upon STP topology changes. When the STP topology changes, this function quickly changes the ports in Forwarding state into router ports to direct multicast data flows to the new forwarding paths.

Prerequisite

Global IGMP snooping has been enabled using the **igmp-snooping enable (system view)** command.

Precautions

- This function takes effect only when STP is used as the loop prevention protocol on a Layer 2 network and the STP operation mode is MSTP, RSTP, or STP.
- With this function configured, the switch sets all ports in Forwarding state as router ports when the STP topology changes. In this case, multicast data flows are forwarded to all the router ports before the router ports are aged. This will cause increase in multicast traffic on the network.

Example

Enable fast multicast forwarding path switching upon STP topology changes.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping fast-switch enable
```

8.9.17 igmp-snooping fast-send report enable

Function

The **igmp-snooping fast-send report enable** command configures a device to send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

The **undo igmp-snooping fast-send report enable** command disables a device from proactively sending IGMP Report messages to the upstream device when a member interface in a Smart Link group experiences a change of state.

By default, a device does not proactively send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

Format

igmp-snooping fast-send report enable

undo igmp-snooping fast-send report enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the status of a Smart Link member interface on a device changes, the active interface in the Smart Link group can forward IGMP Report messages to the upstream device only after receiving the next IGMP General Query message. In this way, multicast data can be switched to the new forwarding path. To enable a device to proactively send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the status of the other Smart Link member interface changes, run the **igmp-snooping fast-send report enable** command. In this way, multicast data can be quickly switched to the new forwarding path.

Prerequisites

IGMP snooping has been enabled globally by running the **igmp-snooping enable** command in the system view.

Precautions

Use this command only on networks configured with Smart Link.

Example

Configure a device to send IGMP Report messages when a member interface of a Smart Link group experiences a change of state.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping fast-send report enable
```

8.9.18 igmp-snooping fast-send robust-count interval

Function

The **igmp-snooping fast-send robust-count interval** command configures the robustness variable and interval for sending Report messages through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

The **undo igmp-snooping fast-send robust-count interval** command restores the default robustness variable and interval for sending Report messages through the active interface in a Smart Link group when the other Smart Link member interface experiences a change of state.

By default, the robustness variable is 3 and the interval is 10s.

Format

igmp-snooping fast-send robust-count *robust-count* **interval** *interval*

undo igmp-snooping fast-send robust-count *robust-count* **interval** *interval*

Parameters

Parameter	Description	Value
robust-count *robust-count*	Specifies the robustness variable for sending Report messages.	The value is an integer in the range from 1 to 10.
interval *interval*	Specifies the interval for sending Report messages.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to proactively send IGMP Report messages to the upstream device through the active interface in a Smart Link group when the status of the other Smart Link member interface changes, run the **igmp-snooping fast-send report enable** command. In this way, multicast data can be quickly switched to the new forwarding path. Then, you can run the **igmp-snooping fast-send robust-count interval** command to adjust IGMP parameters to optimize multicast services.

- The robustness variable for sending Report messages refers to the number of times Report messages are sent through the active interface of a Smart Link group when the status of the other Smart Link member interface changes. The robustness variable helps prevent packet loss.
- The interval parameter configures a device to periodically send IGMP Report messages to the upstream device through the active interface of the Smart Link group when the status of the other Smart Link member interface changes. On a network with a small number of multicast receivers, a smaller interval enables multicast data to be switched to the new forwarding path more rapidly.

Maximum total time for sending Report messages = Robustness variable for sending Report messages x Interval for sending Report messages

Prerequisites

IGMP snooping has been enabled globally by running the **igmp-snooping enable** command in the system view.

Precautions

Use this command only after the **igmp-snooping fast-send report enable** command is run.

When receiving a Query message, a device stops sending IGMP Report messages to the upstream device through the active interface of a Smart Link group.

When a device sends IGMP Report messages, the transmitting interval is the maximum response time. It is recommended that you set the interval to a value greater than the suppression time, thereby preventing messages from being suppressed.

Example

Set the robustness variable and interval for sending Report messages through the active interface in a Smart Link group to 5 and 20s, respectively.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping fast-send robust-count 5 interval 20
```

8.9.19 igmp-snooping group-limit

Function

The **igmp-snooping group-limit** command sets the maximum number of multicast entries that an interface can learn.

The **undo igmp-snooping group-limit** command cancels the limit on the number of multicast entries that an interface can learn.

By default, the number of multicast entries that an interface can learn is not limited.

Format

igmp-snooping group-limit *group-limit* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping group-limit *group-limit* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping group-limit vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
group-limit	Specifies the maximum number of multicast groups that an interface can learn.	The value is an integer and the value range depends on the product model: - SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5731-S, S5731S-S, and S5720I-SI: 1 to 1024 - S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S: 1 to 1500 - S5735S-H, S5736-S, and S6720S-S: 1 to 1536 - S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1 to 4096
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN. *vlan-id1* and *vlan-id2* identify a range of VLAN IDs.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Cancels the limit on the number of multicast groups that interfaces in all VLANs can learn.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **igmp-snooping group-limit** command to limit the number of multicast programs that a user can request. This configuration limits the multicast data traffic volume on the interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

During the configuration, if the number of multicast entries on the interface already exceeds the configured threshold, the number of multicast entries on the interface does not change and the interface cannot learn new multicast entries.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Configure GE0/0/1 to learn a maximum of 10 IGMP snooping entries in VLAN 10, and IGMP snooping is enabled globally and in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-limit 10 vlan 10
```

Configure GE0/0/1 to learn a maximum of 50 IGMP snooping entries in VLANs 20 to 30, and IGMP snooping is enabled globally and in these VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-limit 50 vlan 20 to 30
```

8.9.20 igmp-snooping group-policy (interface view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy on an interface.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from an interface.

By default, no multicast group policy is available on an interface, and hosts connected to the interface can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*] **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy *acl-number* **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy *acl-number* **version** *version-number* **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VLAN can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer ranging from 1 to 3. ● 1: IGMPv1 ● 2: IGMPv2 ● 3: IGMPv3
vlan *vlan-id1* [**to** *vlan-id2*]	Applies the multicast group policy to the specified VLANs on the interface.	*vlan-id1* and *vlan-id2* are integers that range 1 from 4094.
all	Deletes multicast groups policies in all VLANs from the interface.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message to the device, requesting to join the multicast group. The device checks whether the multicast group matches the ACL in the multicast group policy applied to the interface. If so, the device allows the user to join the multicast group. If not, the device drops the message and prohibits the user from joining the multicast group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect when IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)** command.
- Before running the **igmp-snooping group-policy (interface view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the interface can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that an interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.

  After the **igmp-snooping group-policy (interface view)** command is executed on an interface:
  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- A multicast group policy can also be configured in the VLAN view to control the multicast groups that users in the VLAN can join. A multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent users in VLANs 20 to 30 from joining multicast group 225.1.1.123 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan batch 20 to 30
[HUAWEI] igmp-snooping enable vlan 20 to 30
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
```

```
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 to 30
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-policy 2000 vlan 20 to 30
```

Allow hosts belonging to VLANs 20 to 30 on GE0/0/1 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan batch 20 to 30
[HUAWEI] igmp-snooping enable vlan 20 to 30
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 to 30
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-policy 2000 vlan 20 to 30
```

8.9.21 igmp-snooping group-policy (VLAN view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a VLAN.

The **undo igmp-snooping group-policy** command deletes the multicast group policy from a VLAN.

By default, no multicast group policy is available in a VLAN, and hosts in the VLAN can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL used to restrict the range of groups users can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer that ranges from 1 to 3. ● 1: IGMPv1 ● 2: IGMPv2 ● 3: IGMPv3

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a switch with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. After the switch receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If the messages match the ACL, the switch allows user hosts in the VLAN to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the VLAN from joining the group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect when IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)** command.
- Before running the **igmp-snooping group-policy (VLAN view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the VLAN can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that a VLAN can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that a VLAN can join.

  After the **igmp-snooping group-policy (VLAN view)** command is executed on an interface:
  - The VLAN filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VLAN discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- A multicast group policy can also be configured in the interface view to control the multicast groups that users in one or more VLANs on the interface

can join. A multicast group policy configured in the VLAN view controls the multicast groups that users in the VLAN can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 2 from joining group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping group-policy 2000
```

Allow hosts in VLAN 2 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping group-policy 2000
```

8.9.22 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a VLAN, that is, the interval at which Group-Specific Query messages are sent in the VLAN.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a VLAN.

By default, Group-Specific Query messages are sent in a VLAN at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the last member query interval, you can:

- Configure the switch to send IGMP Group-Specific Query messages at intervals when the querier function is enabled.
- Change the aging time of multicast group member ports.

  When the switch receives an IGMP Leave message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

  If the switch (querier) receives Report messages from other hosts within the aging time, it continues to maintain memberships of the multicast group. If the switch does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The switch sets the maximum response time field in the Group-Specific Query message to the configured last member query interval. Therefore, the maximum response time for Group-Specific Query messages is the same as the interval at which Group-Specific Query messages are sent.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The IGMP message version is set to v2 or v3 messages in the VLAN. (Hosts running IGMPv1 do not send Leave messages when they leave a multicast group.)

Example

Set the last member query interval in VLAN 3 to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping lastmember-queryinterval 4
```

8.9.23 igmp-snooping learning

Function

The **igmp-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo igmp-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. ● *vlan-id1*: specifies the first VLAN ID. ● **to** *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member port is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. After IGMP snooping is enabled in a VLAN, all interfaces in the VLAN are enabled to learn forwarding entries from multicast packets. An interface is identified as a dynamic group member port when it receives an IGMP Report message.

If users connected to an interface need to receive data of a fixed multicast group, the interface can be statically bound to the multicast group. In this case, run the **undo igmp-snooping learning** command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The interface belongs to the specified VLANs.

If you run the **undo igmp-snooping learning** command multiple times, all the configurations take effect.

Example

Disable learning of group memberships in VLAN 3 and VLAN 4 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] quit
[HUAWEI] vlan 4
[HUAWEI-vlan4] igmp-snooping enable
[HUAWEI-vlan4] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 3 to 4
[HUAWEI-GigabitEthernet0/0/1] undo igmp-snooping learning vlan 3 to 4
```

8.9.24 igmp-snooping limit-action

Function

The **igmp-snooping limit-action** command enables multicast entry overwriting on interfaces in a VLAN.

The **undo igmp-snooping limit-action** command disables multicast entry overwriting on interfaces in a VLAN.

By default, multicast entry overwriting is disabled on an interface. When the number of multicast entries on an interface reaches the limit, the switch does not process subsequent Report messages or replace the existing entries on the interface.

Format

igmp-snooping limit-action

undo igmp-snooping limit-action

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of multicast groups on an interface or the switch reaches the limit, users connected to the interface or switch cannot join new multicast groups. To allow users to join new multicast groups in this case, enable multicast entry overwriting on interfaces in a VLAN.

After the configuration is complete, the switch records information about multicast users. When a user requests to join a new multicast group but the number of multicast groups on the interface or switch has reached the limit, the switch checks all the programs that the user has ordered. If a program is watched only by this user, the switch replaces the entry of this program with the entry of the new program.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

To make the multicast entry overwriting configuration take effect, perform the following operations:

- Run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- Run the **igmp-snooping group-limit** command to set the maximum number of multicast entries that an interface can learn.

The multicast entry overwriting function has the following limitations:

- When an interface is statically bound to a multicast group, the Layer 2 multicast entry overwriting function becomes invalid on the interface.
- The new multicast entry cannot replace the old one when the old multicast group has multiple multicast users or is a static multicast group.
- A new (S, G) entry can replace only an old (S, G), and a new (*, G) entry can replace only an old (*, G) entry.

Example

Enable multicast entry overwriting on interfaces in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping limit-action
```

8.9.25 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a VLAN.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a VLAN.

By default, the maximum response time for IGMP General messages in a VLAN is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the maximum response time for IGMP General Query messages, you can:

- Control the deadline for a host to send an IGMP Report message. When hosts are required to respond to IGMP General Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of IGMP messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the switch receives a Report message, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **igmp-snooping max-response-time** command sets the maximum response time. The General query count is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

The switch sets the maximum response time field in General Query messages to the value set by the **igmp-snooping max-response-time** command.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

The maximum response time for General Query messages must be shorter than the interval at which General Query messages are sent. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the maximum response time for IGMP Query messages in VLAN 3 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping max-response-time 20
```

8.9.26 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a VLAN so that member ports in the VLAN can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a VLAN.

By default, the fast leave function is disabled in a VLAN.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a multicast group policy that allows member ports to fast leave some multicast groups. Before using this parameter, create an ACL and configure filter rules in the ACL.	-
acl-number	Specifies the number of an ACL that defines a range of multicast groups. A basic or advanced ACL can be used.	The value is an integer that ranges from 2000 to 3999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the switch to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP Leave message for the group. This function saves bandwidth and system resources because the switch does not need to wait until the aging timer of the interface expires.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- IGMPv2 or IGMPv3 messages can be processed in the VLAN.
- If you do not specify **group-policy** when configuring the fast leave function, this function takes effect for all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command.

Example

Allow member ports in VLAN 2 to fast leave all groups.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping prompt-leave
```

Allow member ports in VLAN 3 to fast leave group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping prompt-leave group-policy 2000
```

Prevent member ports in VLAN 3 from fast leaving group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
```

```
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping prompt-leave group-policy 2000
```

8.9.27 igmp-snooping host-based prompt-leave

Function

The **igmp-snooping host-based prompt-leave** command enables host-based fast leave in a VLAN.

The **undo igmp-snooping host-based prompt-leave** command disables host-based fast leave in a VLAN.

By default, host-based fast leave is disabled.

Format

igmp-snooping host-based prompt-leave

undo igmp-snooping host-based prompt-leave

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The host-based fast leave function enables a switch to delete a host from the host list of a group immediately after receiving an IGMP Leave message from the host. If the deleted host is the last receiver host connected to the member port, the switch deletes the forwarding entry of the group from the port, without waiting the aging timer of the port to expire. This conserves bandwidth and system resources.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command, then IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.

Precautions

If a group member port is connected to multiple receiver hosts, the forwarding entry of the multicast group will be deleted without waiting for aging of the port only when the last receiver host leaves the group.

The configuration takes effect only when the switch can process IGMPv2 or IGMPv3 packets in the VLAN.

Example

Enable host-based fast leave in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping host-based prompt-leave
```

8.9.28 igmp-snooping proxy

Function

The **igmp-snooping proxy** command enables IGMP snooping proxy in a VLAN.

The **undo igmp-snooping proxy** command disables IGMP snooping proxy in a VLAN.

By default, IGMP snooping proxy is disabled in a VLAN.

Format

igmp-snooping proxy

undo igmp-snooping proxy

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IGMP snooping is enabled on a switch, the switch forwards Query messages from the upstream IGMP querier and Report/Leave messages from downstream hosts without changing the messages. When there are a large number of hosts on a network, redundant IGMP messages overload the upstream device. Enabling the IGMP snooping proxy function on the switch can solve this problem. This function allows the switch to send IGMP Query messages in place of the upstream Layer 3 device and send Report/Leave messages in place of downstream hosts, conserving link bandwidth between the Layer 3 device and switch. The switch sends IGMP Report/Leave messages to the upstream Layer 3 device only in the following situations:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

An upstream Layer 3 device does not send Query messages as a querier when IGMP is not enabled, for example, the Layer 3 device has only static multicast groups. In this case, the switch cannot create or maintain group memberships even though IGMP snooping is enabled. The IGMP snooping proxy function enables the switch to send Query messages to downstream hosts. For the hosts, the switch is a querier.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

If IGMP is enabled on the upstream Layer 3 device, enabling the IGMP snooping proxy function on the switch may affect the querier election result, because the General Query messages sent by the switch have a smaller source IP address than the General Query messages sent by the Layer 3 device. To solve this problem, run the **igmp-snooping proxy-uplink-port** command to prevent the switch from sending Query messages to the uplink interface connected to the upstream device. Alternatively, run the **igmp-snooping send-query source-address** command to set a large source IP address for Query messages.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- IGMP snooping proxy cannot be enabled in a VLAN if the corresponding VLANIF interface has Layer 3 multicast function (such as IGMP and PIM) enabled.
- After enabling IGMP snooping proxy in a VLAN, do not enable IGMP snooping querier or IGMP message suppression in the VLAN because these functions conflict.
- If multicast VLAN replication is configured on the switch, the IGMP snooping proxy function cannot be enabled in user VLANs.

Example

Enable IGMP snooping proxy in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] igmp-snooping enable
[HUAWEI-vlan100] igmp-snooping proxy
```

8.9.29 igmp-snooping proxy-uplink-port

Function

The **igmp-snooping proxy-uplink-port** command configures an IGMP snooping proxy uplink interface. No IGMP Query message can be sent to this interface.

The **undo igmp-snooping proxy-uplink-port** command deletes an IGMP snooping proxy uplink interface.

By default, no IGMP snooping proxy uplink interface exists in a VLAN.

Format

igmp-snooping proxy-uplink-port vlan *vlan-id*

undo igmp-snooping proxy-uplink-port vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IGMP snooping proxy or IGMP snooping querier is enabled in a VLAN, the switch periodically broadcasts IGMP Query messages to all interfaces in the VLAN, including router ports in the VLAN. This may result in IGMP querier reelection. To prevent IGMP querier reelection, run the **igmp-snooping proxy-uplink-port** command on the router port to disable the switch from sending IGMP Query messages to the router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

Only one IGMP snooping proxy uplink interface can be configured in a VLAN.

The **igmp-snooping proxy-uplink-port** command is used only on an uplink interface. Therefore, the specified VLAN cannot be a user VLAN mapping the multicast VLAN.

Example

Configure GE0/0/1 in VLAN 10 as an IGMP snooping proxy uplink interface.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping proxy-uplink-port vlan 10
```

8.9.30 igmp-snooping querier enable

Function

The **igmp-snooping querier enable** command enables the IGMP snooping querier function in a VLAN.

The **undo igmp-snooping querier enable** command disables the IGMP snooping querier function in a VLAN.

By default, the IGMP snooping querier function is disabled in a VLAN.

Format

igmp-snooping querier enable

undo igmp-snooping querier enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IGMP-capable network, a Layer 3 multicast device functions as a querier to send IGMP Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run IGMP or it uses only static multicast forwarding entries, it cannot function as a querier. In this case, you can enable IGMP snooping querier on the downstream Layer 2 device so that it acts as a querier to send IGMP Query messages.

On a Layer 2 network that has no Layer 3 devices, multicast sources are connected to Layer 2 devices. IGMP snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations as required on your network:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.
- Run the **igmp-snooping robust-count** command to set the number of times Query messages are sent.

Configuration Impact

The IGMP snooping querier does not participate in IGMP querier election. However, the IGMP snooping querier on an IGMP-capable multicast network may affect the election result, because the Query messages sent by the IGMP snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the IGMP snooping querier function is not recommended on an IGMP-capable multicast network.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- The IGMP snooping querier function cannot be enabled in a VLAN if the corresponding Layer 3 VLANIF interface has Layer 3 multicast functions (such as IGMP and PIM) enabled.
- The IGMP snooping proxy and IGMP snooping querier functions cannot be enabled in the same VLAN.
- If multicast VLAN replication is configured on the switch, the IGMP snooping querier function cannot be enabled in user VLANs.

Example

Enable the querier function in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping querier enable
Warning: Please confirm that no other querier is configured on the network, otherwise this command may
cause querier re-election, continue? [Y/N]:y
```

8.9.31 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a VLAN, that is, the interval at which IGMP General Query messages are sent in the VLAN.

The **undo igmp-snooping query-interval** command restores the default general query interval in a VLAN.

By default, the general query interval is 125 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the general query interval, you can:

- Configure the switch to send IGMP General Query messages at intervals to maintain memberships of interfaces. When a shorter interval is configured, the switch is more sensitive to multicast membership changes, but more bandwidth and system resources are consumed.
- Change the aging time of multicast member ports.

  When receiving an IGMP Report message from a host, the switch starts the aging timer for the multicast member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The general query count is set by the **igmp-snooping robust-count** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

The general query interval affects the aging time of group member ports. A shorter general query interval results in a shorter aging time of group member ports and therefore a faster update speed of Layer 2 multicast entries. However, when there are many downstream users connected to a device, a short general query interval can cause flapping of multicast entries, leading to a high CPU usage on the device. Therefore, the default general query interval is recommended. If you need to change the interval to suit service deployment, set the value according to the following table.

Number of IGMP Messages Sent from Downstream Users Within Maximum Response Time	Minimum General Query Interval Reference Value (Seconds)
1 to 1024	10
1024 to 2048	20
2048 to 5120	40

NOTE

The default general query interval defined in RFC documents is 125 seconds, but some vendors define their own default general query intervals. It is recommended that all devices on a multicast network use the same general query intervals (including IGMP and IGMP snooping general query intervals). On Huawei fixed switches, the default value of the IGMP general query interval is 60 seconds, and the default value of the IGMP snooping general query interval is 125 seconds.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the general query interval in VLAN 3 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping query-interval 100
```

8.9.32 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave messages in a VLAN.

The **undo igmp-snooping report-suppress** command disables suppression of IGMP Report and Leave messages in a VLAN.

By default, IGMP Report and Leave message suppression is disabled in a VLAN.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Leave messages from the member hosts.

After Report message suppression is enabled on a Layer 2 device, the device forwards only one IGMP Membership Report message to the upstream device in the following scenarios:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- When receiving a Leave message from a group member, the device sends Group-Specific Query messages to check whether the group has other members on the network segment.
- IGMP message suppression cannot be configured in a VLAN if the corresponding VLANIF interface has Layer 3 multicast function (such as IGMP and PIM) enabled.
- The functions of IGMP snooping proxy and IGMP message suppression cannot be configured in the same VLAN.
- If multicast VLAN replication is configured on the switch, the IGMP message suppression function cannot be enabled in user VLANs.
- The device can suppress duplicate Report messages even when IGMP message suppression is disabled. The default suppression time is 10 seconds. To change the suppression time, run the **igmp-snooping suppress-time** *suppress-time* command. If the *suppress-time* is set to 0, all the membership packets are forwarded immediately.
- This function cannot suppress IGMPv3 packets.

Example

Enable suppression of Report and Leave messages in VLAN 2.

```
<HUAWEI> system view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping report-suppress
```

8.9.33 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the switch to drop the IGMP messages without the Router-Alert option in the IP header received from a VLAN.

The **undo igmp-snooping require-router-alert** command restores the default configuration.

By default, the switch does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the switch checks each IGMP message for the Router-Alert option and discards those IGMP messages without this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Configure the switch to forward only the IGMP messages with the Router-Alert option in the IP header received from VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
```

```
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping require-router-alert
```

8.9.34 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a VLAN, which specifies how many times IGMP Query messages are sent.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a VLAN.

By default, the robustness variable in a VLAN is 2.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a VLAN.	The value is an integer that ranges from 2 to 5.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the IGMP robustness variable, you can:

- Specify the number of times the querier sends a Group-Specific Query message, which prevents packet loss on the network.

  When receiving an IGMP Leave message for a multicast group, the switch sends a Group-Specific Query message a certain number of times (specified by the IGMP robustness variable) to check whether this group has any other members. If the quality of transmission links is low, increase the IGMP robustness variable.
- Change the aging time of multicast group member ports.

When receiving an IGMP Report message from a host, the switch starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Set the IGMP robustness variable to 5 in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping robust-count 5
```

8.9.35 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a VLAN.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VLAN.

By default, the aging time of dynamic router ports in a VLAN is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a VLAN.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the switch. If a router port on the switch ages in this period, the switch does not send Report or Leave messages to router ports. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for the router port if the network is unstable.

When a dynamic router port on the switch receives an IGMP Query message or a PIM Hello message, the switch resets the aging time of the router port.

- If the router port receives an IGMP Query message, the switch sets the remaining aging time of the interface to the configured value.
- If the router port receives a PIM Hello message, the switch sets the aging time of the interface to the holdtime value.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in VLAN 3 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
```

```
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping router-aging-time 300
```

8.9.36 igmp-snooping router-learning (interface view)

Function

The **igmp-snooping router-learning** command enables router port learning on an interface.

The **undo igmp-snooping router-learning** command disables router port learning on an interface.

By default, router port learning is enabled on an interface.

Format

igmp-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Enables an interface to function as a router port in the specified VLANs.	*vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Enables an interface to function as a router port in all the VLANs.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the switch does not need to receive Query messages or PIM

Hello messages from a VLAN, disable router port learning in the VLAN. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a VLAN are forwarded only to router ports in the VLAN.

By default, router port learning is enabled on an interface. To prevent an interface from becoming a router port, disable router port learning on the interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

After router port learning is disabled on an interface, the interface no longer listens on IGMP Query or PIM Hello messages. Run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

- This command takes effect only when the interface has been added to the specified VLANs and IGMP snooping has been enabled in these VLANs using the **igmp-snooping enable (VLAN view)** command.
- You can also disable router port learning by running the **undo igmp-snooping router-learning (VLAN view)** command. The **undo igmp-snooping router-learning (VLAN view)** command is the same as the **undo igmp-snooping router-learning (interface view)** command only except for the scopes they take effect. The command used in the VLAN view disables router port learning on all interfaces in a VLAN, whereas the command used in the interface view disables router port learning on a specific interface in a VLAN.
- If the specified VLAN is bound to a BD, this command takes effect only in the VLAN, but not in the BD bound to the VLAN.

Example

Disable router port learning on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo igmp-snooping router-learning vlan 10
```

8.9.37 igmp-snooping router-learning (VLAN view)

Function

The **igmp-snooping router-learning** command enables router port learning in a VLAN.

The **undo igmp-snooping router-learning** command disables router port learning in a VLAN.

By default, router port learning is enabled in a VLAN.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the switch does not need to receive Query messages or PIM Hello messages from a VLAN, disable router port learning in the VLAN. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a VLAN are forwarded only to router ports in the VLAN.

By default, router port learning is enabled on an interface. To prevent interfaces in a VLAN from becoming a router port, disable router port learning in the VLAN.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

The switch does not listen on IGMP Query or PIM Hello messages in a VLAN after router port learning is disabled in the VLAN. To ensure normal multicast forwarding in the VLAN, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

You can also disable router port learning by running the **undo igmp-snooping router-learning (interface view)** command. The **undo igmp-snooping router-learning (interface view)** command is the same as the **undo igmp-snooping router-learning (VLAN view)** command only except for the scope they take effect. The command used in the VLAN view disables router port learning on all interfaces in a VLAN, whereas the command used in the interface view disables router port learning on a specific interface in a VLAN.

When inter-VLAN multicast replication is enabled on the switch, enable router port learning in user VLANs.

Example

Disable router port learning in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] undo igmp-snooping router-learning
```

8.9.38 igmp-snooping send-query enable

Function

The **igmp-snooping send-query enable** command enables the switch to send IGMP General Query messages to non-router ports when receiving topology change events.

The **undo igmp-snooping send-query enable** command disables the switch from sending IGMP General Query messages to non-router ports.

By default, the switch does not send IGMP General Query messages to non-router ports when receiving topology change events.

Format

igmp-snooping send-query enable

undo igmp-snooping send-query enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network topology changes, the switch receives a topology change event. By default, the switch does not send IGMP General Query messages in this case. A network topology change triggers recalculation of the ring network protocol used (such as STP, MSTP, RRPP, SEP, and Smart Link), but multicast data packets cannot be switched to the new path immediately. To enable multicast data flows to be switched to the new forwarding path immediately after a network topology change, configure the switch to send IGMP General Query messages upon topology changes.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

This command is used on a ring network. When the ring network topology changes, the switch sends IGMP General Query messages with source IP address 192.168.0.1. When this address has been occupied by another device on the network, run the **igmp-snooping send-query source-address** command to change the source IP address.

Precautions

Use this command only when a ring network protocol is enabled on the switch.

Example

Configure the switch to send IGMP General Query messages upon topology changes.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping send-query enable
```

8.9.39 igmp-snooping send-query source-address

Function

The **igmp-snooping send-query source-address** command sets the source IP address of IGMP Query messages.

The **undo igmp-snooping send-query source-address** command restores the default source IP address of IGMP Query messages.

By default, the source IP address of IGMP Query messages is 192.168.0.1.

Format

igmp-snooping send-query source-address *ip-address*

undo igmp-snooping send-query source-address

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address of IGMP Query messages.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP Query messages include General Query messages, Group-Specific Query messages, and Group-and-Source-Specific Query messages. A Layer 2 device sends two types of IGMP General Query messages:

- IGMP General Query messages sent by the querier when the querier function is enabled using the **igmp-snooping proxy** or **igmp-snooping querier enable** command.
- IGMP General Query messages that the Layer 2 device sends after receiving Layer 2 topology change events (configured using the **igmp-snooping send-query enable** command).

By default, IGMP Query messages sent from a Layer 2 device use the source IP address 192.168.0.1. When this IP address is used by another device on the network, run the **igmp-snooping send-query source-address** command to change the source IP address of IGMP Query messages.

When multiple Layer 2 devices exist on a shared network, you can set source IP addresses of IGMP Query messages to identify the devices. For example, when multiple devices with different performance need to participate in querier election, you must configure a different source IP address of IGMP Query messages for each device.

When the IGMP proxy function is enabled on a device using the **igmp-snooping proxy** command or the function of suppressing Report and Leave messages is enabled in a VLAN using the **igmp-snooping report-suppress** command, the device sends IGMP Report and IGMP Leave messages on behalf of downstream users, with the default source IP address of the IGMP Report and IGMP Leave messages being 192.168.0.1. You can run this command to change the source IP address of IGMP Report and IGMP Leave messages.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Example

Set the source IP address of IGMP Query messages sent by the switch to 192.168.0.2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping send-query source-address 192.168.0.2
```

8.9.40 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in the IP header to a VLAN.

The **undo igmp-snooping send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option in the IP header to a VLAN.

By default, the switch sends IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch sends IGMP messages with the Router-Alert option. If some devices in the same VLAN as the switch can process only the IGMP messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option.

The switch adds the Router-Alert option only to locally originated IGMP messages and does not add this option to IGMP messages received from other devices.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Configure the switch to send IGMP messages that do not contain the Router-Alert option in the IP header to VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] undo igmp-snooping send-router-alert
```

8.9.41 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a VLAN.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a VLAN.

By default, no mappings between multicast groups and multicast sources exist in a VLAN.

Format

igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

undo igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

Parameters

Parameter	Description	Value
group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the IP address of the multicast source mapped to a multicast group.	The value is in dotted decimal notation.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such as S1, S2 on the Layer 2 device connected to user hosts. When the Layer 2 device receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the Layer 2 device converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

- IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

Before configuring the mapping between a multicast group and a multicast source:

- IGMP snooping has been enabled in the specified VLAN using the **igmp-snooping enable (VLAN view)** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VLAN.
- SSM mapping has been enabled using the **igmp-snooping ssm-mapping enable** command.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the VLAN to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.

Example

Map multicast groups 238.1.1.1 through 238.1.1.255 to multicast source 10.1.1.1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping version 3
[HUAWEI-vlan10] igmp-snooping ssm-mapping enable
[HUAWEI-vlan10] igmp-snooping ssm-mapping 238.1.1.0 24 10.1.1.1
```

8.9.42 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables Source-Specific Multicast (SSM) mapping in a VLAN.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a VLAN.

By default, SSM mapping is disabled in a VLAN.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the Layer 2 devices connected to the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Run the **igmp-snooping ssm-mapping** command to configure group-source mappings.

Precautions

- If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.
- SSM mapping is applicable only to the VLANs where IGMP snooping can process IGMPv3 messages. To set the IGMP message version to v3, use the **igmp-snooping version** command in the VLAN.
- If the multicast group address is an Any-Source Multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the VLAN view.
- If the inter-VLAN multicast replication function is configured, you only need to configure SSM mapping in the multicast VLAN.

Example

Enable SSM mapping in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping version 3
[HUAWEI-vlan10] igmp-snooping ssm-mapping enable
```

8.9.43 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a VLAN to specify the range of SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a VLAN.

By default, no SSM group policy is available in a VLAN.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts need to join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The **igmp-snooping ssm-policy** command takes effect only when the following configurations are complete:

- IGMP snooping has been enabled in the specified VLAN using the **igmp-snooping enable (VLAN view)** command.
- SSM mapping has been enabled in the specified VLAN using the **igmp-snooping ssm-mapping enable** command.
- If IGMPv1 or IGMPv2 packets are sent by user hosts, the IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VLAN.
- The ACL has been created and configured rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **14.1 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] igmp-snooping enable
[HUAWEI-vlan3] igmp-snooping ssm-mapping enable
[HUAWEI-vlan3] igmp-snooping ssm-policy 2000
```

8.9.44 igmp-snooping static-group suppress-dynamic-join

Function

The **igmp-snooping static-group suppress-dynamic-join** command disables a device from forwarding IGMP Report and Leave messages that are received from a VLAN and contain a static group address to upstream Layer 3 devices configured with the static group address.

The **undo igmp-snooping static-group suppress-dynamic-join** command enables a device to forward IGMP Report and Leave messages that are received from a VLAN and contain a static group address to upstream Layer 3 devices configured with the static group address.

By default, a device forwards IGMP Report and Leave messages that are received from a VLAN and contain a static group address to upstream Layer 3 devices configured with the static group address.

Format

igmp-snooping static-group suppress-dynamic-join

undo igmp-snooping static-group suppress-dynamic-join

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the upstream Layer 3 multicast device is a non-Huawei device and a static group is configured on its interface connected to the device, users cannot dynamically join or leave the multicast group. You must disable the device from sending Report and Leave messages that contain static group addresses to the Layer 3 multicast device.

This function takes effect only for IGMPv1 and IGMPv2 message and is invalid for IGMPv3 messages.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Disable a device from forwarding IGMP Report and Leave messages that are received from VLAN 10 and contain a static group address to upstream Layer 3 devices configured with the static group address.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping static-group suppress-dynamic-join
```

8.9.45 igmp-snooping static-router-port

Function

The **igmp-snooping static-router-port** command configures an interface as a static router port in specified VLANs.

The **undo igmp-snooping static-router-port** command cancels the router port configuration in specified VLANs.

By default, an interface is not a static router port.

Format

igmp-snooping static-router-port vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping static-router-port vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies VLAN IDs. This parameter specifies in which VLANs the current interface functions as a router port. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface functions as a router port only in the VLAN specified by *vlan-id1*.	The value is an integer that ranges from 1 to 4094. The value of vlan-id2 must be greater than the value of vlan-id1. The vlan-id1 and vlan-id2 parameters identify a range of VLANs.

Parameter	Description	Value
all	Cancels the static router port configuration in all VLANs on the interface.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to keep forwarding IGMP Report/Leave messages for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

This command takes effect only when the interface is added to the specified VLANs.

If you run the **igmp-snooping static-router-port** command multiple times, all the configurations take effect.

Example

Configure GE0/0/1 as a static router port in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping static-router-port vlan 2
```

8.9.46 igmp-snooping suppress-time

Function

The **igmp-snooping suppress-time** command sets the IGMP message suppression time in a VLAN.

The **undo igmp-snooping suppress-time** command restores the default IGMP message suppression time in a VLAN.

By default, the IGMP message suppression time is 10 seconds.

Format

igmp-snooping suppress-time *suppress-time*

undo igmp-snooping suppress-time

Parameters

Parameter	Description	Value
suppress-time	Specifies the IGMP message suppression time in a VLAN.	The value is an integer that ranges from 0 to 300, in seconds. The value 0 indicates that IGMP messages are not suppressed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce the IGMP messages sent from a Layer 2 device to the upstream Layer 3 device and protect the Layer 3 device from attacks, enable the Layer 2 device to suppress IGMP Report and IGMP Leave messages sent by hosts in a VLAN. After this function is enabled, the Layer 2 device processes IGMP Report and IGMP Leave messages as follows:

- After receiving an IGMP Report/Leave message and forwarding the message, the Layer 2 device does not forward the same type of messages to the router port within the suppression time.
- If the Layer 2 device receives an IGMP General Query message or Group-Specific message, it does not suppress the first IGMP Report message that responds to the General Query message. In addition, the Layer 2 device resets the suppression timer when it receives the first IGMP Report message.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages. It is recommended that the suppression time be the same as the maximum response time for IGMP Query messages in a VLAN.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

The configured suppression time is invalid for IGMPv3 messages.

Example

Set the IGMP message suppression time in VLAN 2 to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping suppress-time 15
```

8.9.47 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that IGMP snooping can process in a VLAN.

The **undo igmp-snooping version** command restores the default IGMP message version.

By default, the IGMP snooping version is 2, indicating that IGMP snooping can process IGMPv1 and IGMPv2 messages.

Format

igmp-snooping version { **1** | **2** | **3** [**mode asm-ssm**] }

undo igmp-snooping version

Parameters

Parameter	Description	Value
1	Indicates that IGMP snooping only processes IGMPv1 messages.	-
2	Indicates that IGMP snooping processes both IGMPv1 and IGMPv2 messages.	-
3	Indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.	-

Parameter	Description	Value
mode asm-ssm	Indicates that when IGMPv3 is configured, the ASM-SSM model is used.	If this parameter is not specified, the SSM model is used when IGMPv3 is configured.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP protocol maintains group memberships between Layer 3 multicast devices and hosts. IGMP has three versions: v1, v2, and v3. This command specifies the version of IGMP messages that IGMP snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If IGMP is not enabled on the Layer 3 multicast device, configure the IGMP message version on the Layer 2 device to be later than or equal to the version running on downstream hosts.

When hosts in a VLAN run different IGMP versions, run the **igmp-snooping version** command to enable the Layer 2 device to process IGMP messages sent from all the hosts.

Table 8-124 compares how Report messages are processed in the ASM and ASM-SSM models when IGMPv3 is configured.

Table 8-124 Difference in Report message processing in SSM and ASM-SSM models

Multicast Address in a Report Message	Filtering Action	Processing Mode in the SSM Model	Processing Mode in the ASM-SSM Model
SSM group address, for example, 232.1.1.1	INCLUDE	The message is processed normally and the (S, G) entry is generated.	The message is processed normally and the (S, G) entry is generated.
SSM group address, for example, 232.1.1.1	EXCLUDE	The message is considered invalid and discarded.	The message is considered invalid and discarded.

Multicast Address in a Report Message	Filtering Action	Processing Mode in the SSM Model	Processing Mode in the ASM-SSM Model
ASM group address, for example, 225.1.1.1	INCLUDE	The message is considered invalid and discarded.	The message is processed normally and the (S, G) entry is generated.
ASM group address, for example, 225.1.1.1	EXCLUDE (None)	The message is processed normally and the (*, G) entry is generated.	The message is processed normally and the (*, G) entry is generated.
ASM group address, for example, 225.1.1.1	EXCLUDE (Source)	The message is processed, and the (*, G) entry is generated. However, the expected result cannot be achieved.	The message is processed normally, and the INCLUDE (*, G) and EXCLUDE (S, G) entries are generated, which are consistent with the expected result.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.
- When the IGMP snooping version is set to IGMPv3:
  - The switch can use only the default Layer 2 multicast forwarding mode.
  - The S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S forward multicast data by looking up the forwarding table according to the VLAN ID and group address.
- This command cannot be used in user VLANs of a multicast VLAN.
- If the IGMP message version is changed from IGMPv3 to IGMPv2, the system deletes all the dynamic IGMP snooping entries when the aging time expires and processes static IGMP snooping entries as follows:
  - Does not delete static entries that have only multicast groups and no multicast sources.
  - Deletes the static entries that have both multicast groups and multicast sources. When the IGMP message version is restored to IGMPv3, the system restores these entries.

- Before modifying the service model used when IGMP snooping v3 is configured, run the **undo igmp-snooping enable** command in the VLAN view to disable IGMP snooping in the VLAN.
- After the **igmp-snooping version 3 mode asm-ssm** command is configured in a VLAN, no (S, G) entry can be generated if the **l2-multicast static-group** command is run to add an interface to a specified multicast group with a non-SSM multicast address to receive multicast packets from a multicast source. For example, when the **igmp-snooping version 3 mode asm-ssm** command is configured in VLAN 10 and the **l2-multicast static-group source-address 2.1.1.1 group-address 225.0.0.1 vlan 10** command is configured on an interface, the (2.1.1.1, 225.0.0.1) entry cannot be generated.

Example

Set the version of the IGMP messages that can be processed by IGMP snooping to IGMPv1 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] igmp-snooping version 1
```

8.9.48 l2-multicast forwarding-mode

Function

The **l2-multicast forwarding-mode** command configures the forwarding mode of multicast data in a VLAN.

The **undo l2-multicast forwarding-mode** command restores the default forwarding mode of multicast data.

By default, multicast data is forwarded in a VLAN based on IP addresses.

Format

l2-multicast forwarding-mode { **ip** | **mac** }

undo l2-multicast forwarding-mode mac

Parameters

Parameter	Description	Value
ip	Forwards multicast data based on IP addresses.	-
mac	Forwards multicast data based on MAC addresses.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on a Layer 2 device, the Layer 2 device maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the Layer 2 device searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The Layer 2 device determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

Multiple multicast IP addresses may be mapped to one MAC address. If multicast data is forwarded based on MAC addresses, multicast data may be sent to the users who do not require the multicast data. To prevent this problem, use the IP address-based forwarding mode on devices with Layer 3 functions.

Configuration Impact

To set the IGMP snooping version to IGMPv3 or the MLD snooping version to MLDv2, do not change the default forwarding mode using this command.

After the multicast data forwarding mode is set to MAC address-based forwarding in a VLAN using this command, the VLAN cannot be configured as a multicast VLAN.

Precautions

- This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.
  - On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
  - On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

After IGMP snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] igmp-snooping enable
```

After MLD snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] mld-snooping enable
```

8.9.49 l2-multicast router-port-discard

Function

The **l2-multicast router-port-discard** command disables the switch from sending multicast data to routed ports in a VLAN.

The **undo l2-multicast router-port-discard** command restores the default configuration.

By default, multicast data can be forwarded to routed ports in a VLAN.

Format

l2-multicast router-port-discard

undo l2-multicast router-port-discard

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, multicast data does not need to be forwarded to routed ports in a VLAN. For example, when all interfaces on a switch are configured as static router ports in a VLAN, you can use this command to conserve bandwidth by preventing multicast data from being sent to these interfaces.

Precautions

This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.

- On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv4 network.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] igmp-snooping enable
```

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv6 network.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] mld-snooping enable
```

8.9.50 l2-multicast static-group

Function

The **l2-multicast static-group** command configures static group memberships on an interface.

The **undo l2-multicast static-group** command deletes static group memberships from an interface.

By default, no static group membership is configured on an interface.

Format

Configure a single static multicast group:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Configure a series of static multicast groups:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address all vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
source-address *source-ip-address*	Specifies the IP address of a multicast source.	The value of *source-ip-address* can be any Class A, Class B, or Class C address, in dotted decimal notation.

Parameter	Description	Value
group-address *group-ip-address*	Specifies the IP address of a multicast group.	The value of *group-ip-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the VLANs that the interface belongs to. *vlan-id1* [**to** *vlan-id2*] specifies a range of VLAN IDs. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface is bound only to the multicast group in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.
all	Deletes all group memberships from the interface. ● In **group-address all**, **all** indicates that the interface is removed from all multicast groups. ● In **vlan** { **all** | {*vlan-id1* [**to** *vlan-id2*] } &<1-10> }, **all** indicates that the interface is removed from multicast groups in all VLANs.	-
group-ip-address1 **to** *group-ip-address2*	Configures multiple static group memberships on the interface. *group-ip-address1* and *group-ip-address2* identify a range of multicast group addresses.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation. The values of *group-ip-address1* and *group-ip-address2* must be in the same network segment (with a 24-bit mask).

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocols, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can receive multicast data of the multicast group over a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when both the following conditions are met:
  - IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)**.
  - The specified VLANs have been created and the interface has been added to these VLANs.
  - The specified group address is not a reserved group address.
- If a device is configured to forward Layer 2 multicast traffic on a network configured with MUX VLAN using the **multicast-snooping mux-vlan enable** command, the VLAN specified in the **l2-multicast static-group** command must not be a MUX VLAN (include principal VLAN and subordinate VLAN).
- After the **igmp-snooping version 3 mode asm-ssm** command is configured in a VLAN, no (S, G) entry can be generated if the **l2-multicast static-group** command is run to add an interface to a specified multicast group with a non-SSM multicast address to receive multicast packets from a multicast source. For example, when the **igmp-snooping version 3 mode asm-ssm** command is configured in VLAN 10 and the **l2-multicast static-group**

source-address 2.1.1.1 group-address 225.0.0.1 vlan 10 command is configured on an interface, the (2.1.1.1, 225.0.0.1) entry cannot be generated.

Example

Configure a static multicast group 224.1.1.1 on GE0/0/1 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 vlan 2
```

Configure static multicast groups 224.1.1.1 to 224.1.1.3 on GE0/0/1 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 to 224.1.1.3 vlan 2
```

Delete static multicast group 224.1.1.1 from GE0/0/1 in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo l2-multicast static-group group-address 224.1.1.1 vlan all
```

8.9.51 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the switch to drop unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

The default method that a switch uses to process unknown multicast flows depends on whether Layer 2 multicast is enabled and which Layer 2 multicast forwarding mode is used.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are those that do not match any entry in the multicast forwarding table or match multicast forwarding entries with an empty outbound interface list. These flows are not requested by users. The default method that a switch uses to process unknown IPv4 multicast flows depends on whether Layer 2 multicast is enabled and which Layer 2 multicast forwarding mode is used:

- If Layer 2 multicast is not enabled on the switch, the switch broadcasts unknown multicast flows in the corresponding VLAN.
- If Layer 2 multicast is enabled on the S1720GW-E and S1720GWR-E, they broadcast unknown multicast flows in the corresponding VLAN.
- If Layer 2 multicast is enabled on other switch models, they broadcast unknown multicast flows in the corresponding VLAN in MAC address-based forwarding mode and drop unknown multicast flows in IP address-based forwarding mode.

If a switch broadcasts unknown multicast flows in a VLAN, you can configure the switch to drop unknown multicast flows, reducing instant bandwidth usage.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown IPv4 and IPv6 multicast packets are dropped, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

After the **multicast drop-unknown** command is run on the following models, protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address will not be discarded: S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H S6730S-H, S6730-S, and S6730S-S

After the **multicast drop-unknown** command is run on the following models, protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address 224.0.0.9 will not be discarded: S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if MAC address-based forwarding is configured as the Layer 2 multicast forwarding mode and the **multicast drop-unknown** command is executed, unknown multicast packets destined for the following reserved network segments and IP address cannot be dropped: 239.0.0.0/8, 224.0.0.0/24, 224.0.1.0/24, FF0X:0:0:0:0:0:0:0/96, FF0X::DB8:0:0/96, and the IPv6 address with the last 32 bits being 0000:00XX. To drop such unknown multicast packets, configure a traffic policy.

Example

Drop unknown multicast packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] multicast drop-unknown
```

8.9.52 multicast-snooping mux-vlan enable

Function

The **multicast-snooping mux-vlan enable** command enables a device to transmit Layer 2 multicast traffic on a network configured with MUX VLAN.

The **undo multicast-snooping mux-vlan enable** command disables a device from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

By default, a device is disabled from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

Format

multicast-snooping mux-vlan enable

undo multicast-snooping mux-vlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, on a network configured with MUX VLAN, Layer 2 multicast traffic cannot be transmitted between the principal VLAN and subordinate VLANs. You can run the **multicast-snooping mux-vlan enable** command to enable Layer 2 multicast traffic to be transmitted on the network configured with MUX VLAN.

Precautions

If a MUX VLAN is bound to a static multicast group using the **l2-multicast static-group** or **mld-snooping static-group** command, the **multicast-snooping mux-vlan enable** command cannot be executed. You must delete the association between the MUX VLAN and static multicast group before running the **multicast-snooping mux-vlan enable** command.

After the **multicast-snooping mux-vlan enable** command is configured, you cannot run the **l2-multicast static-group** or **mld-snooping static-group** command to bind a MUX VLAN to a static multicast group.

Example

Enable a device to forward Layer 2 multicast traffic on a network configured with MUX VLAN.

```
<HUAWEI> system-view
[HUAWEI] multicast-snooping mux-vlan enable
```

8.9.53 multicast-source-deny

Function

The **multicast-source-deny** command discards multicast data packets sent from specified VLANs on an interface.

The **undo multicast-source-deny** command restores multicast forwarding in specified VLANs on an interface.

By default, multicast data packets from all VLANs are forwarded on an interface.

Format

multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies a VLAN ID. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If you do not specify **to** *vlan-id2*, only one VLAN is specified.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **multicast-source-deny** command on an interface, multicast packets received from specified VLANs are discarded on the interface. You may need to use this command in the following scenarios:

- A user-side interface receives multicast packets, but the switch does not need to receive multicast data packets from user-side interfaces. Discarding multicast data packets received on a user-side interface protects the system against forged multicast flows sent from malicious users.
- Multiple multicast sources in different VLANs are connected to the switch through a Layer 2 network, but the switch only needs to receive multicast data from some of the multicast sources.
- In some situations, for example, multicast services for users connected to an interface have expired and need to be stopped, the network administrator can use this command on this interface. Then multicast data packets from specified VLANs cannot be sent to the users.

Precautions

If you run the **multicast-source-deny** command multiple times, all the configurations take effect.

When using the **multicast-source-deny** command on an interface, ensure that the interface has been added to the specified VLANs. Otherwise, the configuration does not take effect.

This command can discard only multicast data packets that meet both of the following conditions:

- The destination MAC address is an IP multicast MAC address (IPv4 MAC address starting with 0x01-00-5e or IPv6 multicast MAC address starting with 0x3333).
- The packet encapsulation protocol is UDP.

Example

Discard multicast data packets sent from VLANs 100 to 105 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-source-deny vlan 100 to 105
```

8.9.54 reset igmp-snooping group

Function

The **reset igmp-snooping group** command deletes dynamic group memberships learned by IGMP snooping.

Format

reset igmp-snooping group { **all** | **vlan** { **all** | *vlan-id* [[**source-address** *source-address*] **group-address** *group-address*] } }

Parameters

Parameter	Description	Value
all	Deletes all dynamic group memberships learned by IGMP snooping.	-
vlan { **all** | *vlan-id* }	Deletes the dynamic group memberships of a specified VLAN. If **all** is specified, the system deletes IGMP dynamic group memberships of all VLANs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
source-address *source-address*	Deletes the dynamic group memberships of a specified source address.	The multicast source address is a Class A, Class B, or Class C IP address on a nature network segment. The value is in dotted decimal notation.
group-address *group-address*	Deletes the dynamic group memberships of a specified group address.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups on a network change, the switch generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the switch to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to delete existing group memberships.

Precautions

NOTICE

Deleting group memberships in a VLAN temporarily interrupts multicast forwarding in the VLAN. The switch generates new forwarding entries only when receiving IGMP Report messages from hosts in the VLAN. The hosts can then receive multicast data.

This command cannot delete static group memberships.

This command is valid only for VLANs with IGMP snooping enabled and is invalid for a VLAN if IGMP is enabled on the corresponding VLANIF interface.

Example

Delete all dynamic group memberships learned by IGMP snooping.

```
<HUAWEI> reset igmp-snooping group all
```

Delete dynamic group memberships in VLAN 3.

```
<HUAWEI> reset igmp-snooping group vlan 3
```

8.9.55 reset igmp-snooping qinq-port-info

Function

The **reset igmp-snooping qinq-port-info** command clears multicast group membership on a QinQ or Dot1q termination sub-interface.

Format

reset igmp-snooping qinq-port-info interface *interface-type interface-number*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears multicast group membership on a specified interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast users access a multicast group through a sub-interface, multicast group members change, and the switch generates new Layer 3 multicast forwarding entries until the aging time of multicast member interfaces expires. To enable the switch to generate new multicast forwarding entries immediately, use the **reset igmp-snooping qinq-port-info** command to clear old Layer 3 multicast forwarding entries.

Configuration Impact

During the execution of the **reset igmp-snooping qinq-port-info** command on a sub-interface, multicast traffic to hosts connected to this sub-interface will be interrupted.

Precautions

This command cannot delete static group membership.

Example

Clear group membership of all multicast groups on QinQ termination sub-interface GE0/0/18.1.

```
<HUAWEI> reset igmp-snooping qinq-port-info interface GigabitEthernet 0/0/18.1
```

8.9.56 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics { **all** | **vlan** { **all** | *vlan-id* } }

Parameters

Parameter	Description	Value
all	Clears all the IGMP snooping statistics.	-
vlan { **all** | *vlan-id* }	Clears IGMP snooping statistics of a specified VLAN. If **all** is specified, the system clears IGMP snooping statistics of all VLANs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of VLAN 2.

```
<HUAWEI> reset igmp-snooping statistics vlan 2
```

8.10 VSI-based IGMP Snooping Configuration Commands

8.10.1 Command Support

Only the S5731-H, S5731S-H, S5731-S, S6730-S, S5732-H, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support VSI-based IGMP Snooping.

VSI-based IGMP snooping depends on the MPLS feature.

8.10.2 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters in a VSI.

Format

display igmp-snooping [**vsi** [*vsi-name*]]

Parameters

Parameter	Description	Value
vsi [*vsi-name*]	Displays the IGMP snooping running parameters in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration in a VSI, you can use this command to check IGMP snooping parameter settings. When a fault occurs in the multicast service, use this command to identify the cause of the fault.

Precautions

The IGMP snooping configuration of a VSI is displayed only when the VSI is in Up state.

Example

Display IGMP snooping running parameters in VSI company1.

```
<HUAWEI> display igmp-snooping vsi company1
  IGMP Snooping Information for VSI company1
     IGMP Snooping is Enabled
     IGMP Version is Set to default 2
     IGMP Query Interval is Set to default 125s
     IGMP Max Response Interval is Set to default 10s
     IGMP Robustness is Set to default 2
     IGMP Last Member Query Interval is Set to default 1s
     IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
     IGMP Filter Group-Policy is not set
     IGMP Prompt Leave Disable
     IGMP Router Alert is Not Required
     IGMP Send Router Alert Enable
     IGMP Router Port Learning Enable
     IGMP SSM-Mapping Disable
```

Table 8-125 Description of the **display igmp-snooping** command output

Item	Description
IGMP Snooping Information for VSI company1	IGMP snooping running parameters are displayed in VSI company1.
IGMP Snooping is Enabled	IGMP snooping is enabled in the VSI. By default, IGMP snooping is disabled in a VSI. IGMP snooping can be enabled in a VSI using the **igmp-snooping enable (VSI view)** command.
IGMP Version is Set to default 2	Both IGMPv1 and IGMPv2 messages can be processed in the VSI (default configuration). This parameter is configured using the **igmp-snooping version** command.
IGMP Query Interval is Set to default 125s	The interval at which IGMP General Query messages are sent in the VSI is 125 seconds (default configuration). This parameter is configured using the **igmp-snooping query-interval** command.
IGMP Max Response Interval is Set to default 10s	The maximum response time for IGMP General Query messages in the VSI is 10 seconds (default configuration). This parameter is configured using the **igmp-snooping max-response-time** command.
IGMP Robustness is Set to default 2	The IGMP robustness variable is 2 (default configuration). This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1s	The interval at which IGMP Group-Specific Query messages are sent in the VSI 1 second (default configuration). This parameter is configured using the **igmp-snooping lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s or holdtime in hello	The aging time of router ports in the VSI is 180 seconds or the holdtime in PIM Hello messages (default configuration). This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is not set	The default multicast group policy is used in the VSI. A multicast group policy is configured using the **igmp-snooping group-policy** command.

Item	Description
IGMP Prompt Leave Disable	Prompt leave is disabled in the VSI (default configuration). The prompt leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Router Alert is Not Required	The device does not require that the IGMP messages received in the VSI contain the Router-Alert option in the IP header (default configuration). The switch can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.
IGMP Send Router Alert Enable	The device sends the IGMP messages that contain the Router-Alert option in the IP headers to the hosts in the VSI (default configuration). The switch can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Router Port Learning Enable	Learning of IGMP router ports is enabled in the VSI. Router port learning can be enabled using the **igmp-snooping router-learning** command.
IGMP SSM-Mapping Disable	IGMP SSM mapping is disabled in the VSI. IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.

8.10.3 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration in a VSI.

Format

display igmp-snooping [**vsi** [*vsi-name*]] **configuration**

Parameters

Parameter	Description	Value
vsi [*vsi-name*]	Displays the non-default IGMP snooping configuration in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration in a VSI, use this command to verify the configuration. This command displays only the IGMP snooping configuration.

Prerequisites

This command does not display information about static multicast groups and static router ports. To view information about static multicast groups and static router ports, run the **display igmp-snooping port-info** and **display igmp-snooping router-port** command.

Example

Display the IGMP snooping configuration in VSI company1.

```
<HUAWEI> display igmp-snooping vsi company1 configuration
 IGMP Snooping Configuration for VSI company1
    igmp-snooping enable
    igmp-snooping version 3
```

8.10.4 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about group member ports.

Format

display igmp-snooping port-info [**vsi** *vsi-name* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Displays group memberships in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
group-address *group-address*	Displays member ports of a specified multicast group in a VSI. *group-address* specifies the IP address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After IGMP snooping is configured in a VSI on a switch, the IGMP snooping module maintains a Layer 2 multicast forwarding table by snooping the IGMP messages exchanged between the upstream router and downstream hosts. The **display igmp-snooping port-info** command shows member interfaces in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink interfaces have multicast users connected, and control multicast services conveniently.

Precautions

Only multicast member ports in Up state are displayed in the command output.

Example

Display information about group member ports in the VSI **company1**.

```
<HUAWEI> display igmp-snooping port-info vsi company1
-----------------------------------------------------------------------
                (Source, Group)  Port                      Flag
 Flag: S:Static     D:Dynamic     M: Ssm-mapping
 ------------------------------------------------------------------------
 VSI company1, 3 Entry(s)
                 (*, 225.0.0.1)  GE0/0/11(VID:1001)             -D-
                                       1 port(s) include
                 (*, 225.0.0.2)  PW(10.1.1.1/100)              -D-
                                       1 port(s) include
                 (*, 225.0.0.3)  GE0/0/13                      -D-
                                       1 port(s) include
 ------------------------------------------------------------------------
```

Table 8-126 Description of the **display igmp-snooping port-info** command output

Item	Description
(Source, Group)	(S, G) entry, specifying a multicast source and multicast group.
Port	Outbound port name. **include** and **exclude** indicate the multicast source filtering mode. Different ports in the command output are described as follows: ● GE0/0/11 (VID:1001) indicates that the AC-side interface is VLANIF 1001, and the group member port is GE0/0/11 in VLAN 1001. ● PW (10.1.1.1/100) indicates that the member port is a PW-side interface. 10.1.1.1 is the IP address of the remote peer, and 100 is the VC ID of the remote peer. ● GE0/0/13 indicates that the AC-side interface is GE0/0/13 working in Layer 3 mode, and the group member port is GE0/0/13.
Flag	Type of an outbound port. ● S: static member port ● D: dynamic member port ● M: member port established through SSM mapping
VSI company1, 3 Entry(s)	Number of multicast entries in VSI company 1.

8.10.5 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified VSI, including static and dynamic router ports.

Format

display igmp-snooping router-port vsi [*vsi-name*]

Parameters

Parameter	Description	Value
vsi [*vsi-name*]	Displays information about router ports in a specified VSI. If *vsi-name* is not specified, the command displays router ports in all VSIs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects to an upstream multicast router. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message.

After completing basic IGMP snooping configuration in a VSI, you can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and remaining aging time of a router port in the VSI.

Precautions

Information about a router port is displayed only when the interface is in Up state.

Example

Display information about router ports in VSI company1.

```
<HUAWEI> display igmp-snooping router-port vsi company1
 Port Name                   UpTime        Expires       Flags
 ---------------------------------------------------------------------
 VSI company1, 3 router-port(s)
 GE0/0/21(VID:100)              18:02:13      00:02:35      DYNAMIC
 PW(1.1.1.1/2)                 03:28:16      00:01:20      DYNAMIC
 GE0/0/15                     18:02:13      00:02:35      DYNAMIC
```

Table 8-127 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Router port name. Different ports in the command output are described as follows: ● GE0/0/21(VID:100) indicates that the AC-side interface is VLANIF 100, and the router port is GE0/0/21 in VLAN 100. ● PW(1.1.1.1/2) indicates that the member port is a PW-side interface. 1.1.1.1 is the IP address of the remote peer, and 2 is the VC ID of the remote peer. ● GE0/0/15 indicates that the AC-side interface is GE0/0/15 working in Layer 3 mode, and the router port is GE0/0/15.
UpTime	Time elapsed since the interface became a router port.
Expires	Remaining aging time of the router port. ● The remaining aging time is displayed for a dynamic router port. ● For a static router port, "--" is displayed, indicating that the interface does not age.
Flags	Type of the router port. ● STATIC: static router port ● DYNAMIC: dynamic router port
VSI company1, 3 router-port(s)	Number of router ports in VSI company 1.

8.10.6 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics vsi [*vsi-name*]

Parameters

Parameter	Description	Value
vsi-name	Displays IGMP snooping statistics on a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing basic IGMP snooping configuration in a VSI, you can use the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent and received, and the number of PIM hello messages received in each VSI. When a multicast fault occurs, the IGMP snooping statistics help you identify the cause of the fault.

Configuration Impact

When *vsi-name* is specified, this command displays IGMP snooping statistics in the specified VSI, but does not display IGMP snooping events that occur in the VSI.

Example

Display IGMP snooping statistics in VSI company1.

```
<HUAWEI> display igmp-snooping statistics vsi company1
 IGMP Snooping Packets Counter
   Statistics for VSI company1
     Recv V1 Report          0
     Recv V2 Report          304
     Recv V3 Report          0
     Recv V1 Query           0
     Recv V2 Query           523
     Recv V3 Query           0
     Recv Leave            0
     Recv Pim Hello         0
     Send Query(S=0)         0
     Send Query(S!=0)        0
```

Table 8-128 Description of the **display igmp-snooping statistics** command output

Item	Description
IGMP Snooping Packets Counter	Statistics on IGMP and PIM packets.
Statistics for VSI company1	Packet statistics in VSI company1.
Recv V1 Report	Number of received IGMPv1 Membership Report messages.
Recv V2 Report	Number of received IGMPv2 Membership Report messages.
Recv V3 Report	Number of received IGMPv3 Membership Report messages.
Recv V1 Query	Number of received IGMPv1 Query messages.
Recv V2 Query	Number of received IGMPv2 Query messages.
Recv V3 Query	Number of received IGMPv3 Query messages.
Recv Leave	Number of received IGMP Leave messages.
Recv Pim Hello	Number of received PIM Hello messages.
Send Query(S=0)	Number of sent IGMP Query messages with the source address 0.0.0.0.
Send Query(S!=0)	Number of sent IGMP Query messages with source addresses other than 0.0.0.0.

8.10.7 display l2-multicast forwarding-table vsi

Function

The **display l2-multicast forwarding-table vsi** command displays the VSI-based Layer 2 multicast forwarding table.

Format

display l2-multicast forwarding-table vsi [*vsi-name* [**group-address** { *group-address* | **router-group** }]]

Parameters

Parameter	Description	Value
vsi-name	Displays Layer 2 multicast forwarding entries in a specified VSI. If *vsi-name* is not specified, the command displays Layer 2 multicast forwarding entries in all VSIs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
group-address { *group-address* | **router-group** }	Displays Layer 2 multicast forwarding entries of a specified multicast group or all router ports. ● If you specify *group-address*, the command displays forwarding entries of the specified multicast group. ● If you specify **router-group**, the command displays forwarding entries of all router ports.	The value of *group-address* is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing configuration of IGMP snooping over VPLS, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table.

Precautions

This command displays multicast forwarding entries in a VSI only when the VSI is in Up state.

Example

Display the multicast forwarding entries of the VSI **company1**.

```
<HUAWEI> display l2-multicast forwarding-table vsi company1
VSI Name : company1, Forwarding Mode : MAC
Total Group(s) : 2
----------------------------------------------------------------------
Group(Mac)                  Interface     Out-Vlan/InLabel
----------------------------------------------------------------------
               Router-port   5.5.5.9/28            1036
0100-5e00-0001                  5.5.5.9/28             1036
                       GigabitEthernet0/0/21    1000
0100-5e00-0002                  5.5.5.9/28             1036
                       GigabitEthernet0/0/21    1000
                       GigabitEthernet0/0/22    0
----------------------------------------------------------------------
```

Table 8-129 Description of the **display l2-multicast forwarding-table** command output

Item	Description
VSI Name	Name of the VSI of which the multicast forwarding entries are displayed.
Forwarding Mode	Multicast forwarding mode used in the VSI. Only the MAC address-based forwarding mode is supported.
Group(Mac)	Group MAC address.
Interface	Group member ports and router ports. In this example, 5.5.5.9/28 indicates a PW-side interface, of which the remote peer IP address is 5.5.5.9 and remote peer VSI ID is 28. GigabitEthernet0/0/21 indicates an AC-side interface.
Out-Vlan/InLabel	VLAN ID or inner MPLS label of packets. The value 0 indicates that the router port or member port is an AC-side interface, which is a physical interface working in Layer 3 mode.
Router-port	Router port in the VSI.

8.10.8 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally.

The **undo igmp-snooping enable** command disables IGMP snooping globally.

By default, IGMP snooping is disabled globally.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IGMP snooping is enabled in a VSI, IGMP snooping runs on PE devices in the VSI and maintains a multicast forwarding table by snooping IGMP messages forwarded between the PE devices. The PE devices can manage and control Layer 2 multicast forwarding based on the multicast forwarding table.

Before configuring IGMP snooping in a VSI, enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after you run the **igmp-snooping enable** command in the system view.

Precautions

NOTICE

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configurations are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the device uses the default IGMP snooping configuration.

Example

Enable IGMP snooping globally.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

8.10.9 igmp-snooping enable (VSI view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a VSI.

The **undo igmp-snooping enable** command disables IGMP snooping in a VSI.

By default, IGMP snooping is disabled in a VSI.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP snooping not enabled in a VSI after being enabled in the system view. To enable IGMP snooping in a VSI, run the **igmp-snooping enable** command in the VSI view.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Example

Enable IGMP snooping in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
```

8.10.10 igmp-snooping group-limit

Function

The **igmp-snooping group-limit** command sets the maximum number of Layer 2 multicast entries that an AC-side interface can learn.

The **undo igmp-snooping group-limit** command cancels the limit on the number of Layer 2 multicast entries that an AC-side interface can learn.

By default, the number of Layer 2 multicast entries that an AC-side interface can learn is not limited.

Format

igmp-snooping group-limit *group-limit* **vsi** *vsi-name*

undo igmp-snooping group-limit [*group-limit*] **vsi** *vsi-name*

Parameters

Parameter	Description	Value
group-limit	Specifies the maximum number of Layer 2 multicast entries that an AC-side interface can learn.	The value is an integer ranging from 1 to 4096.
vsi *vsi-name*	Limits the number of Layer 2 multicast entries that can be learned in a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By limiting the number of Layer 2 multicast entries learned on an interface, you can control the number of programs users connected to the interface can order. This configuration limits the multicast data traffic volume on the interface.

On a VPLS network, the maximum number of Layer 2 multicast entries can only be configured on an AC-side interface. The configuration method varies according to the type of the AC-side interface:

- If the AC-side interface bound to a VSI is a VLANIF interface, configure the maximum number of Layer 2 multicast entries on the Layer 2 interface in the corresponding VLAN. For details, see the **igmp-snooping group-limit** command in "VLAN-based IGMP Snooping Configuration Commands."
- If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping group-limit** *group-limit* **vsi** *vsi-name* command on this interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

If the number of Layer 2 multicast entries on the interface already exceeds the configured limit, the number of Layer 2 multicast entries on the interface does not change and the interface cannot learn new Layer 2 multicast entries.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VSI view)** command to enable IGMP snooping in the VSI.

Example

Set the maximum number of Layer 2 multicast entries on the AC-side interface GE0/0/1 bound to the VSI **company1** to 10. (IGMP snooping has been enabled globally and in the VSI.)

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-limit 10 vsi company1
```

8.10.11 igmp-snooping group-policy (interface view)

Function

The **igmp-snooping group-policy** command applies a multicast group policy on an AC-side interface.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from an AC-side interface.

By default, no multicast group policy is available on an AC-side interface bound to a VSI, and hosts in sites connected to the interface can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*] **vsi** *vsi-name*

undo igmp-snooping group-policy [*acl-number* [**version** *version-number*]] **vsi** *vsi-name*

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VSI can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Parameter	Description	Value
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version.	The value is an integer that ranges from 1 to 3. - 1: IGMPv1 - 2: IGMPv2 - 3: IGMPv3
vsi *vsi-name*	Specifies the VSI to which the multicast group policy is applied.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. In multicast applications, user hosts send IGMP Report messages to join a group when they order programs of this group. When the upstream Layer 2 device receives the Report messages, the switch matches the Report messages with the ACL referenced in the group policy configured on the interface. If the messages match the ACL, the switch allows user hosts in the VSI to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the VSI from joining the group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- Before running the **igmp-snooping group-policy (interface view)** command, run the **acl** command to configure the ACL that you want to apply to the

group policy to limit the range of multicast groups that hosts connected to the VLAN can join.

  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the VLAN can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the VLAN can join.

  After the **igmp-snooping group-policy (interface view)** command is executed on an interface:

  - The VLAN filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VLAN discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- The **igmp-snooping group-policy (interface view)** applies a multicast group policy to the sites connected to an AC-side interface. You can also apply a multicast group policy to a VSI using the **igmp-snooping group-policy (VSI view)** command. If multicast group policies are configured for the same VSI in the VSI view and interface view, the system first uses the policy configured in the interface to filter the groups that hosts in the VSI can join, and then use the group configured in the VSI view.
- On a VPLS network, ACs can be set up on different types of interfaces. The method to apply a multicast group policy to an AC-side interface various according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping group-policy** command on this interface.
  - If the AC-side interface bound to a VSI instance is a VLANIF interface, configure a multicast group policy on the Layer 2 interface in the corresponding VLAN. For details, see the **igmp-snooping group-policy (interface view)** commands in "VLAN-based IGMP Snooping Configuration Commands."

Example

Apply a multicast group policy to AC-side interface GE0/0/1 bound to the VSI **company1**, which allows hosts in the sites connected to GE0/0/1 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
```

```
[HUAWEI-vsi-company1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping group-policy 2000 vsi company1
```

8.10.12 igmp-snooping group-policy (VSI view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a VSI.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from a VSI.

By default, no multicast group policy is available in a VSI, and hosts in the VSI can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VSI can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version.	The value is an integer that ranges from 1 to 3. ● 1: IGMPv1 ● 2: IGMPv2 ● 3: IGMPv3

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. In multicast applications, user hosts send IGMP Report messages to join a group when they order programs of this group. When the upstream Layer 2 device receives the Report messages, the switch matches the Report messages with the ACL referenced in the group policy configured in the VSI. If the messages match the ACL, the switch allows user hosts in the VSI to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the VSI from joining the group.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- Before running the **igmp-snooping group-policy (VSI view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the VSI can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that a VSI can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that a VSI can join.

  After the **igmp-snooping group-policy (VSI view)** command is executed on a VSI:
  - The VSI filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VSI discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.
- The **igmp-snooping group-policy (VSI view)** command applies a multicast group policy to a VSI. You can also apply a multicast group to the sites connected to an AC-side interface by using either of the following methods:
  - If the AC-side interface bound to a VSI instance is a VLANIF interface, configure a multicast group policy on the Layer 2 interface in the corresponding VLAN. For details, see the **igmp-snooping group-policy (interface view)** commands in "VLAN-based IGMP Snooping Configuration Commands."
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping group-policy** *acl-number* [**version** *version-number*] **vsi** *vsi-name* command on this interface.

If multicast group policies are configured for the same VSI in the VSI view and interface view, the system first uses the policy configured in the interface to filter the groups that hosts in the VSI can join, and then use the group configured in the VSI view.

Example

Allow hosts in the VSI **company1** to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping group-policy 2000
```

8.10.13 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a VSI, that is, the interval at which Group-Specific Query messages are sent in the VSI.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a VSI.

By default, Group-Specific Query messages are sent in a VSI at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a member interface receives an IGMP Leave message from a downstream host, the switch starts the aging timer for the interface. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

If the member interface receives Report messages from downstream hosts within the aging time, the switch retains the member interface in the outbound interface list of the corresponding Layer 2 multicast forwarding entry. If the member interface does not receive any Report messages within the aging time, the switch considers that no group member is connected to the interface, and therefore deletes the interface from the Layer 2 multicast forwarding entry.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Hosts running IGMPv1 do not send Leave messages when they leave a multicast group. Therefore, the **igmp-snooping lastmember-queryinterval** command is valid only when the IGMP message version is set to v2 or v3 in the VSI.

Example

Set the last member query interval in VSI company1 to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping lastmember-queryinterval 4
```

8.10.14 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a VSI.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a VSI.

By default, the maximum response time for IGMP General messages in a VSI is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum response time for General Query messages is used to calculate the aging time of group member interfaces. When a member port receives a Report message from a downstream host, the switch starts the aging timer for the interface. The aging time is calculated using the following formula: Aging time = Query count x General query interval + Maximum response time for General Query messages. This command sets the maximum response time in the formula. The general query interval is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

If the member port receives Report messages from downstream hosts within the aging time, the switch retains the member port in the outbound interface list of the corresponding Layer 2 multicast forwarding entry. If the member port does not receive any Report messages within the aging time, the switch considers that no group member is connected to the interface, and therefore deletes the interface from the Layer 2 multicast forwarding entry.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the maximum response time for IGMP General Query messages in VSI company1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping max-response-time 20
```

8.10.15 igmp-snooping over-vpls enable

Function

The **igmp-snooping over-vpls enable** command enables IGMP snooping for VPLS.

The **undo igmp-snooping over-vpls enable** command disables IGMP snooping for VPLS.

By default, IGMP snooping for VPLS is disabled.

Format

igmp-snooping over-vpls enable

undo igmp-snooping over-vpls enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring IGMP snooping in a VSI, enable IGMP snooping globally and for VPLS in the system view.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command in the system view.

Precautions

When you run the **undo igmp-snooping over-vpls enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping for VPLS. If any IGMP snooping for VPLS configuration has been made in the system, the device prompts you to delete all the IGMP snooping for VPLS configuration.

Example

Enable IGMP snooping for VPLS.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
```

8.10.16 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a VSI so that member ports in the VSI can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a VSI.

By default, the fast leave function is disabled in a VSI.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy *acl-number*	Allows member ports to fast leave the multicast group specified by an ACL.	The value of *acl-number* is an integer that ranges from 2000 to 3999.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function allows the switch to delete an interface from a group immediately after the interface receives an IGMP Leave message for the multicast group.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- The configuration is valid only when IGMPv2 or IGMPv3 messages can be processed in the VSI.
- If you do not specify **group-policy** when configuring the fast leave function, this function applies to all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command. The default ACL rule denies all multicast groups. If you do not want to apply the fast leave to a group, use the **rule permit source any** command.

Example

Allow member ports in the VSI **company1** to fast leave group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping prompt-leave group-policy 2000
```

Prevent member ports in the VSI **company1** from fast leaving group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping prompt-leave group-policy 2000
```

8.10.17 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a VSI, that is, the interval at which IGMP General Query messages are sent in the VSI.

The **undo igmp-snooping query-interval** command restores the default general query interval in a VSI.

By default, Group-Specific Query messages are sent in a VSI at an interval of 125 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 125.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The general query interval is used to calculate the aging time of group member ports. When a member port receives an IGMP Report message from a host, the switch starts the aging timer for the interface. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The general query count is set by the **igmp-snooping robust-count** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

If the member port receives Report messages from downstream hosts within the aging time, the switch retains the member port in the outbound interface list of the corresponding Layer 2 multicast forwarding entry. If the member port does not receive any Report messages within the aging time, the switch considers that no group member is connected to the interface, and therefore deletes the interface from the Layer 2 multicast forwarding entry.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the general query interval in VSI company1 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
```

```
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping query-interval 100
```

8.10.18 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the switch to drop the IGMP messages without the Router-Alert option in the IP header received from a VSI.

The **undo igmp-snooping require-router-alert** command restores the default setting.

By default, the switch does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol packets that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the switch checks each IGMP message for the Router-Alert option and discards those IGMP messages with this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to discard the IGMP messages without the Router-Alert option in the IP header received from VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping require-router-alert
```

8.10.19 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a VSI, which specifies the query count.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a VSI.

By default, the robustness variable in a VSI is 2.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a VSI.	The value is an integer that ranges from 2 to 5. The default value is 2.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP robustness variable is used to adjust the aging time of group member interfaces.

- When a member port receives an IGMP Report message from a downstream host, the switch sets the aging time of the interface to: General query count x General query interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count. The general query interval is set by the **igmp-snooping query-interval** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.
- When the member port receives a Leave message from a downstream host, the switch starts the aging timer of the interface to: Last member query interval x Last member query count. The **igmp-snooping robust-count** command sets the general query count. The last member query interval is set by the **igmp-snooping lastmember-queryinterval** command.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the IGMP robustness variable to 5 in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping robust-count 5
```

8.10.20 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a VSI.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VSI.

By default, the aging time of dynamic router ports in a VSI is 180 seconds.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a VSI.	The value is an integer that ranges from 1 to 1000, in seconds. The default value is 180 seconds.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the switch. If a router port on the switch ages in this period, the switch does not send Report or Leave messages to the router port. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for router ports if the network is unstable.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Configuration Impact

If a router port receives an IGMP Query message, the switch sets the remaining aging time of the router port to the configured value.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

A too short aging time causes frequent aging of router ports and degrades system performance.

Example

Set the aging time of router ports in VSI company1 to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping router-aging-time 500
```

8.10.21 igmp-snooping router-learning

Function

The **igmp-snooping router-learning** command enables router port learning in a VSI.

The **undo igmp-snooping router-learning** command disables router port learning in a VSI.

By default, router port learning is enabled in a VSI.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0. Router ports are configured to guide forwarding of IGMP Report/Leave messages. To prevent interfaces in a VSI from becoming a router port, disable router port learning in the VSI.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Follow-up Procedure

The switch does not listen on IGMP Query messages in a VSI after router port learning is disabled in the VSI. Therefore, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Disable router port learning in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] undo igmp-snooping router-learning
```

8.10.22 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in the IP header to a VSI.

The **undo igmp-snooping send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option in the IP header to a VSI.

By default, the switch sends the IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol packets that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. Sending IGMP messages without the Router-Alert option improves device performance, reduces cost, and enhances security of the upper-layer routing protocol.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to send IGMP messages without the Router-Alert option in the IP header to VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] undo igmp-snooping send-router-alert
```

8.10.23 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a VSI.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a VSI.

By default, no mappings between multicast groups and multicast sources exist in a VSI.

Format

igmp-snooping ssm-mapping *ip-group-address* { *ip-group-mask* | *mask-length* } *ip-source-address*

undo igmp-snooping ssm-mapping *ip-group-address* { *ip-group-mask* | *mask-length* } *ip-source-address*

Parameters

Parameter	Description	Value
ip-group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
ip-group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
ip-source-address	Specifies the IP address of a multicast source.	The value is in dotted decimal notation.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such as S1, S2 on the switch connected to user hosts. When the switch receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the switch converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

- IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VSI.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the VSI to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.
- SSM mapping is enabled using the **igmp-snooping ssm-mapping enable** command.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Map multicast group 238.0.0.1 to multicast source 10.1.1.1 in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping version 3
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping enable
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping 238.0.0.1 32 10.1.1.1
```

8.10.24 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables source-specific multicast (SSM) mapping in a VSI.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a VSI.

By default, SSM mapping is disabled in a VSI.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the switch.

Prerequisites

- IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command.
- The IGMP message version is set to v3 using the **igmp-snooping version** command in the VSI.

Follow-up Procedure

If the multicast group address is an any-source multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the VSI view.

Run the **igmp-snooping ssm-mapping** command to configure mapping between multicast groups and multicast sources.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Enable SSM mapping in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping version 3
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping enable
```

8.10.25 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a VSI. All the multicast groups permitted by the SSM group policy are SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a VSI.

By default, no SSM group policy is available in a VSI.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts need to join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The **igmp-snooping ssm-policy** command takes effect only when the following configurations are complete:

- IGMP snooping has been enabled in the specified VSI using the **igmp-snooping enable (VSI view)** command.
- SSM mapping has been enabled in the specified VSI using the **igmp-snooping ssm-mapping enable** command.
- If IGMPv1 or IGMPv2 packets are sent by user hosts, the IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VSI.
- The ACL has been created and configured rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **14.1 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping ssm-mapping enable
[HUAWEI-vsi-company1] igmp-snooping ssm-policy 2000
```

8.10.26 igmp-snooping static-router-port (interface view)

Function

The **igmp-snooping static-router-port** command configures an AC-side interface in a VSI as a static router port.

The **undo igmp-snooping static-router-port** command deletes the static router port configuration.

By default, no AC-side interface in a VSI is configured as a static router port.

Format

igmp-snooping static-router-port vsi *vsi-name*

undo igmp-snooping static-router-port vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the VSI to which a static router port belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the interface connected to an upstream router to keep receiving or forwarding IGMP Report/Leave packets for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command configures an AC-side interface as a static router port. To configure a PW-side interface as a static router port, run the **igmp-snooping static-router-port (VSI view)** command.

- On a VPLS network, ACs can be set up on different types of interfaces. The method to configure an AC-side interface as a static router port varies according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping static-router-port** command on this interface.
  - If the AC-side interface bound to a VSI is a VLANIF interface, configure the Layer 2 interface in the corresponding VLAN as a static router port. For details, see the **igmp-snooping static-router-port vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command in "VLAN-based IGMP Snooping Configuration Commands."

Example

Configure GE0/0/1 as a static router port in the VSI **company1**. (GE0/0/1 has been bound to the VSI **company1**. IGMP snooping has been enabled globally and in the VSI **company1**.)

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping static-router-port vsi company1
```

8.10.27 igmp-snooping static-router-port (VSI view)

Function

The **igmp-snooping static-router-port** command configures a PW-side interface in a VSI as a static router port.

The **undo igmp-snooping static-router-port** command deletes the static router port configuration.

By default, no PW-side interface in a VSI is configured as a static router port.

Format

igmp-snooping static-router-port remote-peer *ip-address* [**negotiation-vc-id** *vc-id*]

undo igmp-snooping static-router-port remote-peer *ip-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
remote-peer *ip-address*	Specifies the IP address of the remote peer.	The value is in dotted decimal notation.

Parameter	Description	Value
negotiation-vc-id *vc-id*	Specifies a virtual circuit ID. Generally, this parameter is specified when two ends of a PW have different VSI names. The *vc-id* parameter must specify an unused VC ID. That is, the specified VC ID cannot be the same as the VSI ID configured for any other VSI or the VC ID specified by **negotiation-vc-id** *vc-id* in another VSI.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the interface connected to an upstream router to keep receiving or forwarding IGMP Report/Leave packets for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command configures a PW-side interface as a static router port. The method to configure an AC-side interface as a static router port varies according to the type of the AC-side interface:

- If the AC-side interface bound to a VSI is a VLANIF interface, configure the Layer 2 interface in the corresponding VLAN as a static router port. For details, see the **igmp-snooping static-router-port vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command in "VLAN-based IGMP Snooping Configuration Commands."

- If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **igmp-snooping static-router-port vsi** *vsi-name* command on this interface.

Example

Configure the PW-side interface (with remote peer 1.1.1.1) as a static router port.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping static-router-port remote-peer 1.1.1.1
```

8.10.28 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that can be processed by IGMP snooping in a VSI.

The **undo igmp-snooping version** command restores the default IGMP snooping version.

By default, the IGMP snooping version is 2, indicating that IGMP snooping can process IGMPv1 and IGMPv2 messages.

Format

igmp-snooping version *version*

undo igmp-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of IGMP messages that can be processed in a VSI.	The value is an integer that ranges from 1 to 3. • 1: indicates that IGMP snooping processes only IGMPv1 messages. • 2: indicates that IGMP snooping processes IGMPv1 and IGMPv2 messages. • 3: indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When hosts in a VSI run different IGMP versions, run the **igmp-snooping version** command to enable the switch to process IGMP message from all the hosts.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Set the IGMP snooping version to IGMPv1 in VSI company1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] igmp-snooping version 1
```

8.10.29 l2-multicast backup-query forward

Function

The **l2-multicast backup-query forward** command configures the switch to forward IGMP Query messages to the backup PW.

The **undo l2-multicast backup-query forward** command disables the switch from forwarding IGMP Query messages to the backup PW.

By default, the switch does not forward IGMP Query messages to the backup PW.

Format

l2-multicast backup-query forward [**source-mac-replace**]

undo l2-multicast backup-query forward

Parameters

Parameter	Description	Value
source-mac-replace	Replaces the source MAC addresses in Query messages to the device MAC address before forwarding the Query messages.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, two PWs are deployed on a VPLS network to ensure reliable service traffic transmission. The two PWs provide redundancy protection for service transmission. If IGMP snooping over VPLS is configured on the switch, the switch does not forward IGMP protocol packets to the backup PW by default. In this case, devices on the backup PW cannot create Layer 2 multicast forwarding entries because they cannot receive IGMP protocol packets. When the primary PW is Down and the backup PW becomes the new primary PW, multicast data traffic will be interrupted for a short time because devices on the new primary PW have not learned Layer 2 multicast forwarding entries. To solve this problem, configure the switch to forward IGMP protocol packets to the backup PW so that multicast data traffic can be quickly switched to the new primary PW.

This command configures the switch to forward IGMP Query messages to the backup PW.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to forward IGMP Query messages to the backup PW.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] l2-multicast backup-query forward
```

8.10.30 l2-multicast backup-report forward

Function

The **l2-multicast backup-report forward** command configures the switch to forward IGMP Report/Leave messages to the backup PW.

The **undo l2-multicast backup-report forward** command disables the switch from forwarding IGMP Report/Leave messages to the backup PW.

By default, the switch does not forward IGMP Report/Leave messages to the backup PW.

Format

l2-multicast backup-report forward [**source-mac-replace**]

undo l2-multicast backup-report forward

Parameters

Parameter	Description	Value
source-mac-replace	Replaces the source MAC addresses in Report/Leave messages to the device MAC address before forwarding the Report/Leave messages.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, two PWs are deployed on a VPLS network to ensure reliable service traffic transmission. The two PWs provide redundancy protection for service transmission. If IGMP snooping over VPLS is configured on the switch, the switch does not forward IGMP protocol packets to the backup PW by default. In this case, devices on the backup PW cannot create Layer 2 multicast forwarding entries because they cannot receive IGMP protocol packets. When the primary PW is Down and the backup PW becomes the new primary PW, multicast data traffic will be interrupted for a short time because devices on the new primary PW have not learned Layer 2 multicast forwarding entries. To solve this problem, configure the switch to forward IGMP protocol packets to the backup PW so that multicast data traffic can be quickly switched to the new primary PW.

This command configures the switch to forward IGMP Report/Leave messages to the backup PW.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.

Example

Configure the switch to forward IGMP Report/Leave messages to the backup PW.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] l2-multicast backup-report forward
```

8.10.31 l2-multicast static-group (interface view)

Function

The **l2-multicast static-group** command statically binds a multicast group to an AC-side interface in a VSI.

The **undo l2-multicast static-group** command deletes a static multicast from an AC-side interface.

By default, no multicast group is statically bound to an AC-side interface in a VSI.

Format

l2-multicast static-group [**source-address** *source-address*] **group-address** *group-address1* [**to** *group-address2*] **vsi** *vsi-name*

undo l2-multicast static-group [**source-address** *source-address*] **group-address** { *group-address1* [**to** *group-address2*] | **all** } **vsi** *vsi-name*

Parameters

Parameter	Description	Value
source-address *source-address*	Specifies the IP address of a multicast source.	The value is in dotted decimal notation.
group-address *group-address1* [**to** *group-address2*]	Specifies the IP address of a static multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Deletes all static multicast groups.	-

Views

GE interface view, 100GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 protocol protocols, you can configure static Layer 2 multicast forwarding entries by binding groups to interfaces. After a group is statically bound to an interface, users connected to this interface can keep receiving multicast data of the group over a long time.

Static Layer 2 multicast has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- A static multicast member port does not respond to Query messages sent from an IGMP querier. When a group or (S, G) is statically bound to or

unbound from an interface, the interface does not send an IGMP Membership Report message or Leave message.

- Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command statically binds a group to an AC-side interface. To statically bind a group to a PW-side interface, run the **l2-multicast static-group (VSI view)** command.
- On a VPLS network, ACs can be set up on different types of interfaces. The method to statically bind a group to an AC-side interface varies according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **l2-multicast static-group** command on this interface.
  - If the AC-side interface bound to a VSI is a VLANIF interface, bind a group to the Layer 2 interface in the corresponding VLAN. For details, see the **l2-multicast static-group** command in "VLAN-based IGMP Snooping Configuration Commands."

Example

Statically bind group 225.0.0.1 to GE0/0/1. (GE0/0/1 has been bound to the VSI **company1**. IGMP snooping has been enabled globally and in the VSI **company1**.)

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 225.0.0.1 vsi company1
```

8.10.32 l2-multicast static-group (VSI view)

Function

The **l2-multicast static-group** command statically binds a multicast group to a PW-side interface in a VSI.

The **undo l2-multicast static-group** command deletes a static multicast from a PW-side interface.

By default, no multicast group is statically bound to a PW-side interface in a VSI.

Format

l2-multicast static-group [**source-address** *source-address*] **group-address** *group-address* **remote-peer** *ip-address* [**negotiation-vc-id** *vc-id*]

undo l2-multicast static-group [**source-address** *source-address*] **group-address** { *group-address* | **all** } **remote-peer** *ip-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
source-address *source-address*	Specifies the IP address of a multicast source.	The value is in dotted decimal notation.

Parameter	Description	Value
group-address *group-address*	Specifies the IP address of a static multicast group.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
remote-peer *ip-address*	Indicates the IP address of the remote peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies a virtual circuit ID. Generally, this parameter is specified when two ends of a PW have different VSI names.	The *vc-id* parameter must specify an unused VC ID. That is, the specified VC ID cannot be the same as the VSI ID configured for any other VSI or the VC ID specified by **negotiation-vc-id** *vc-id* in another VSI. The value is an integer that ranges from 1 to 4294967295.
all	Deletes all static multicast groups.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 protocol protocols, you can configure static Layer 2 multicast forwarding entries by binding entries to interfaces. After a multicast group is statically bound to an interface, users connected to this interface can keep receiving multicast data of the multicast group for a long time.

Static Layer 2 multicast has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled for VPLS using the **igmp-snooping over-vpls enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the VSI using the **igmp-snooping enable (VSI view)** command.
- A static multicast member port does not respond to Query messages sent from an IGMP querier. When an interface is statically bound to or unbound from a multicast group or (S, G), the interface does not send an IGMP Membership Report message or Leave message.
- Interfaces on a VPLS network include PW-side interfaces and AC-side interfaces. This command statically binds a group to a PW-side interface. The method to statically bind a group to an AC-side interface varies according to the type of the AC-side interface:
  - If the AC-side interface bound to a VSI is a VLANIF interface, bind a group to the Layer 2 interface in the corresponding VLAN. For details, see the **l2-multicast static-group** command in "VLAN-based IGMP Snooping Configuration Commands."
  - If the AC-side interface bound to a VSI is a physical interface that has been switched to Layer 3 mode using the **undo portswitch** command, run the **l2-multicast static-group** [**source-address** *source-address*] **group-address** *group-address1* [**to** *group-address2*] **vsi** *vsi-name* command on this interface.

Example

Statically bind group 224.1.1.1 to the PW (with the remote IP address as 1.1.1.1) in the VSI **company1**.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vpls enable
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] igmp-snooping enable
[HUAWEI-vsi-company1] l2-multicast static-group group-address 224.1.1.1 remote-peer 1.1.1.1
```

8.10.33 reset igmp-snooping group

Function

The **reset igmp-snooping group** command clears dynamic multicast forwarding entries.

Format

reset igmp-snooping group { **vsi** { **name** *vsi-name* [[**source-address** *source-address*] **group-address** *group-address*] | **all** } | **all** }

Parameters

Parameter	Description	Value
name *vsi-name*	Clears the dynamic multicast forwarding entries of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Clears the dynamic multicast forwarding entries of all VSIs.	-
source-address *source-address*	Deletes the dynamic group memberships of a specified source address.	The value is in dotted decimal notation.
group-address *group-address*	Deletes the dynamic group memberships of a specified group address.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups on interfaces change, the system generates new Layer 2 multicast forwarding entries until the aging time of multicast member interfaces expire. To enable the system to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to clear old multicast forwarding entries.

Precautions

NOTICE

If the command clears the dynamic forwarding entries of a VSI, the hosts in the VSI cannot receive multicast packets.

This command cannot clear static multicast forwarding entries.

Example

Delete all dynamic forwarding entries of VSI **company1**.

```
<HUAWEI> reset igmp-snooping group vsi name company1
```

8.10.34 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics { **vsi** { **name** *vsi-name* | **all** } | **all** }

Parameters

Parameter	Description	Value
name *vsi-name*	Clears IGMP snooping statistics in a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Clears all the IGMP snooping statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of VSI company1.

```
<HUAWEI> reset igmp-snooping statistics vsi name company1
```

8.11 BD-based IGMP Snooping Configuration Commands

8.11.1 Command Support

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI support BD-based IGMP snooping.

8.11.2 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters.

Format

display igmp-snooping [**bridge-domain** [*bd-id*]]

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays the IGMP snooping running parameters in a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After IGMP snooping is configured for a VXLAN network, you can use this command to view the IGMP snooping running parameters.

To view the IGMP snooping configuration, run the **display igmp-snooping configuration** command.

Example

Display the IGMP snooping running parameters.

```
<HUAWEI> display igmp-snooping bridge-domain 123
  IGMP Snooping Information for BDID 123
     IGMP Snooping is Enabled
     IGMP Version is Set to default 2
     IGMP Query Interval is 1s
     IGMP Max Response Interval is Set to default 10s
     IGMP Robustness is Set to default 2
     IGMP Last Member Query Interval is Set to default 1s
     IGMP Router Port Aging Interval is Set to 180s
     IGMP Filter Group-Policy is not set
     IGMP Prompt Leave Disable
     IGMP Router Alert is Not Required
     IGMP Send Router Alert Enable
     IGMP Report Suppress Disable
     IGMP Suppress Time is set to default 10 seconds
     IGMP Querier Enable
     IGMP Router Port Learning Enable
     IGMP SSM-Mapping Enable
     IGMP SSM-policy acl number is 2008
```

Table 8-130 Description of the **display igmp-snooping** command output

Item	Description
IGMP Snooping Information for BDID 123	The following information displayed is the IGMP snooping running parameters in BD 123.
IGMP Snooping is Enabled	IGMP snooping is enabled in the BD. By default, IGMP snooping is disabled in a BD. IGMP snooping can be enabled in a BD using the **igmp-snooping enable (BD view)** command.
IGMP Version is Set to default 2	Version of IGMP messages that can be processed in the BD. In this example, the default version 2 is displayed, indicating that both IGMPv1 and IGMPv2 messages can be processed. This parameter is configured using the **igmp-snooping version** command.
IGMP Query Interval is 1s	Interval at which IGMP General Query messages are sent. This parameter is configured using the **igmp-snooping query-interval** command.
IGMP Max Response Interval is Set to default 10s	Maximum response time for IGMP General Query messages. This parameter is configured using the **igmp-snooping max-response-time** command.

Item	Description
IGMP Robustness is Set to default 2	IGMP robustness variable. This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1s	Interval at which IGMP Group-Specific Query messages are sent. This parameter is configured using the **igmp-snooping lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s	Aging time of a router port. This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is not set	Multicast group policy. In this example, that is, no policy is configured. A multicast group policy is configured using the **igmp-snooping group-policy** command.
IGMP Prompt Leave Disable	The fast leave function is disabled for interfaces in the BD. The fast leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Router Alert is Not Required	The switch does not require that the IGMP messages received from the BD contain the Router-Alert option in the IP header. The switch can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.
IGMP Send Router Alert Enable	The switch sends the IGMP messages with the Router-Alert option to the BD. The switch can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Report Suppress Disable	IGMP message suppression is disabled. IGMP message suppression can be enabled using the **igmp-snooping report-suppress** command.
IGMP Suppress Time is set to default 10 seconds	IGMP message suppression time. This parameter is configured using the **igmp-snooping suppress-time** command.
IGMP Querier Enable	IGMP snooping querier is enabled. IGMP snooping querier can be enabled using the **igmp-snooping querier enable** command.
IGMP Router Port Learning Enable	Router port learning is enabled. Router port learning can be enabled using the **igmp-snooping router-learning** command.

Item	Description
IGMP SSM-Mapping Disable	IGMP snooping SSM mapping is disabled. IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.
IGMP SSM-policy acl number is 2008	SSM group policy for IGMP snooping. The SSM group policy for IGMP snooping can be configured using the **igmp-snooping ssm-policy** command.

8.11.3 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration.

Format

display igmp-snooping [**bridge-domain** [*bd-id*]] **configuration**

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays IGMP snooping configurations in a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether the IGMP snooping configurations for a VXLAN network are correct.

To check all IGMP snooping running parameters, run the **display igmp-snooping** command.

Example

Display the IGMP snooping configuration in BD 123.

```
<HUAWEI> display igmp-snooping bridge-domain 123 configuration
 IGMP Snooping Configuration for BDID 123
    igmp-snooping enable
    igmp-snooping query-interval 1s
    igmp-snooping querier enable
    igmp-snooping ssm-mapping enable
    igmp-snooping ssm-policy 2008
    igmp-snooping ssm-mapping 225.0.0.1 255.255.255.255 10.0.0.1
```

8.11.4 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about multicast group member ports.

Format

display igmp-snooping port-info [**bridge-domain** *bd-id* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
bridge-domain *bd-id*	Displays multicast group member ports in a specified BD.	The value is an integer that ranges from 1 to 16777215.
group-address *group-address*	Displays information about member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When the switch with IGMP snooping enabled receives IGMP messages exchanged between hosts and a Layer 3 device, the switch maintains a Layer 2 multicast forwarding table based on information in the messages. The **display igmp-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink ports of the switch have multicast users connected, and control multicast services conveniently.

Precautions

Information about multicast group member ports can be displayed only after IGMP snooping is enabled in the BD using the **igmp-snooping enable** command.

Example

Display information about multicast group member ports in BD 123.

```
<HUAWEI> display igmp-snooping port-info bridge-domain 123
-------------------------------------------------------------------------------
                      (Source, Group)   Port                       Flag
            Flag: S:Static     D:Dynamic     M: Ssm-mapping
-------------------------------------------------------------------------------
 BDID 123, 1 Entry(s)
                       (*, 225.0.0.2)  XGE0/0/4(VID:101)            S--
                                          1 port(s) include
-------------------------------------------------------------------------------
```

Table 8-131 Description of the **display igmp-snooping port-info** command output

Item	Description
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. Multicast data is sent from multicast source S to group G. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.
Port	Member port. TNL indicates VXLAN tunnel information. **include** and **exclude** indicate the multicast source filtering mode.
Flag	Type of a member port, which can be: - S: static member port, which is configured using the **l2-multicast static-group** command - D: dynamic member port learned through IGMP snooping - M: member port established through SSM mapping
BDID 123, 1 Entry(s)	BD ID and the number of entries in the BD.

Display detailed information about all multicast group member ports.

```
<HUAWEI> display igmp-snooping port-info verbose
The port information of Group 225.0.0.2 on BDID 123:
    Time of this group has been up : 05:05:07

  The port information of (0.0.0.0, 225.0.0.2):
    Time of this source has been up : 05:05:07
    Port Table on this source(0.0.0.0):
    List of ports in include mode:
      No.1
        Port name : XGE0/0/4(VID:101)
        Time of this port has been up as a host-port : NA
        Remain time of port expire as dynamic host-port : NA
        Host-port flags : Static
    There are 1 port(s) in include mode.
    List of ports in exclude mode:
      No.1
        Port name : XGE0/0/5(VID:101)
        Time of this port has been up as a host-port : NA
        Remain time of port expire as dynamic host-port : NA
        Host-port flags : Static
    There are 1 port(s) in exclude mode.
```

Table 8-132 Description of the display igmp-snooping port-info verbose command output

Item	Description
The port information of Group 225.0.0.2 on BDID 123	Information about member ports of multicast group 225.0.0.2 in BD 123.
Time of this group has been up	Time that elapsed since the multicast group was set up.
The port information of (0.0.0.0, 225.0.0.2)	Information about member ports of a specified (S, G).
Time of this source has been up	Time that elapsed since the multicast source was set up.
Port Table on this source	List of member ports of the specified multicast source.
List of ports in include mode	Information about member ports that join a multicast group in INCLUDE mode.
List of ports in exclude mode	Information about member ports that join a multicast group in EXCLUDE mode.
No.1	First member port.
Port name	Type and number of the first member port.
Time of this port has been up as a host-port	Time that elapsed since the first member port was bound to a source or (S, G).

Item	Description
Remain time of port expire as dynamic host-port	Aging time of the first member port. This field displays "NA" for a static member port. The aging time of a dynamic member port is calculated using the following formula: Aging time = Robustness variable x General query interval + Maximum response time for General Query messages. The robustness variable is configured using the **igmp-snooping robust-count** command. The general query interval is configured using the **igmp-snooping query-interval** command. The maximum response time for General Query messages is configured using the **igmp-snooping max-response-time** command.
Host-port flags	Type of a member port, which can be: ● Static: static member ● Dynamic: dynamic member port learned through IGMP snooping ● Mapping: member port established through SSM mapping
There are *x* port(s) in include mode	Number of member ports that join a multicast group in INCLUDE mode.
There are *x* port(s) in exclude mode	Number of member ports that join a multicast group in EXCLUDE mode.

8.11.5 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified BD, including static and dynamic router ports.

Format

display igmp-snooping router-port bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays information about the router ports in a specified BD. If *bd-id* is not specified, the command displays router ports in all BDs.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects the switch to an upstream Layer 3 multicast device. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message or a PIM Hello message.

You can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and aging time of a router port.

Precautions

This command can display information about router ports in a BD only when IGMP snooping has been enabled in the BD using the **igmp-snooping enable (BD view)** command, and at least one interface in the BD is in Up state.

Example

Display information about router ports in BD 123.

```
<HUAWEI> display igmp-snooping router-port bridge-domain 123
Port Name                    UpTime        Expires       Flags
 ---------------------------------------------------------------------
 BDID 123, 2 router-port(s)
 XGE0/0/36(VID:101)             07:24:05      --            STATIC
 XGE0/0/4(VID:102)              05:15:50      --            STATIC
```

Table 8-133 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Type and number of a router port. TNL indicates VXLAN tunnel information.
UpTime	Time that elapsed since the interface became a router port.
Expires	Aging time of the router port. - The aging time is displayed for a dynamic router port. This parameter is configured using the **igmp-snooping router-aging-time** command. - For a static router port, "--" is displayed, indicating that the static router does not age.

Item	Description
Flags	Type of the router port, which can be: ● STATIC: static router port configured using the **igmp-snooping static-router-port** command. ● DYNAMIC: dynamic router port

8.11.6 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bridge-domain [*bd-id*]	Displays IGMP snooping statistics in a specified BD. If *bd-id* is not specified, the system displays IGMP snooping statistics in all BDs.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After IGMP snooping is configured, you can run the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent and received in each BD.

Precautions

This command displays IGMP snooping statistics only when IGMP snooping has been enabled globally using the **igmp-snooping enable (BD view)** command.

Example

Display IGMP snooping statistics in BD 123.

```
<HUAWEI> display igmp-snooping statistics bridge-domain 123
 IGMP Snooping Packets Counter
   Statistics for BDID 123
     Recv V1 Report         0
     Recv V2 Report         6621
     Recv V3 Report         0
     Recv V1 Query          0
     Recv V2 Query          335516
     Recv V3 Query          0
     Recv General Query     0
     Recv Leave             26
     Recv Pim Hello         0
     Send Query(S=0)        33
     Send Query(S!=0)       0
     Suppress Report        0
     Suppress Leave         0
     Proxy Send General Query              0
     Proxy Send Group-Specific Query       0
     Proxy Send Group-Source-Specific Query 0
```

Table 8-134 Description of the display igmp-snooping statistics command output

Item	Description
IGMP Snooping Packets Counter	Statistics on IGMP Snooping packets.
Statistics for BDID 123	Packet statistics in BD 123.
Recv V1 Report	Number of IGMPv1 Report messages received.
Recv V2 Report	Number of IGMPv2 Report messages received.
Recv V3 Report	Number of IGMPv3 Report messages received.
Recv V1 Query	Number of IGMPv1 Query messages received.
Recv V2 Query	Number of IGMPv2 Query messages received.
Recv V3 Query	Number of IGMPv3 Query messages received.
Recv General Query	Interval for sending IGMP General Query messages.
Recv Leave	Number of IGMP Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.
Send Query(S=0)	Number of IGMP Query messages sent with the source address 0.0.0.0.
Send Query(S!=0)	Number of IGMP Query messages sent with source addresses other than 0.0.0.0.

Item	Description
Suppress Report	Number of duplicate IGMP Report messages dropped.
Suppress Leave	Number of duplicate IGMP Leave messages dropped.
Proxy Send General Query	Number of General Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Specific Query	Number of Group-Specific Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent by the IGMP snooping proxy.

8.11.7 display l2-multicast forwarding-table bridge-domain

Function

The **display l2-multicast forwarding-table bridge-domain** command displays the Layer 2 multicast forwarding table in BDs.

Format

display l2-multicast forwarding-table bridge-domain [*bd-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]]

Parameters

Parameter	Description	Value
bd-id	Displays Layer 2 multicast forwarding entries in a specified BD. If *bd-id* is not specified, the command displays Layer 2 multicast forwarding entries in all BDs.	The value is an integer that ranges from 1 to 16777215.
source-address *source-address*	Displays the forwarding entries of a specified Layer 2 multicast source.	The value is in dotted decimal notation.
group-address *group-address*	Displays multicast forwarding entries of a specified Layer 2 multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Parameter	Description	Value
router-group	Displays Layer 2 multicast forwarding entries of all router ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After completing IGMP snooping configuration, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table. This command displays statically configured and dynamically learned multicast forwarding entries.

Example

Display the Layer 2 multicast forwarding table in BD 123.

```
<HUAWEI> display l2-multicast forwarding-table bridge-domain 123
Bridge domain  : 123, Forwarding Mode : MAC
Total Group(s) : 1
--------------------------------------------------------------------------------
Group(Mac)                                Interface      Out-Vlan/InLabel
--------------------------------------------------------------------------------
                        Router-port     XGigabitEthernet0/0/36          101
                        Router-port     XGigabitEthernet0/0/4           102
0100-5e00-0002                             XGigabitEthernet0/0/4           101
                                   XGigabitEthernet0/0/36           101
                                   XGigabitEthernet0/0/4            102
--------------------------------------------------------------------------------
```

Table 8-135 Description of the **display l2-multicast forwarding-table bridge-domain** command output

Item	Description
Bridge domain	BD ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode used in the BD. Only the MAC address-based forwarding mode is supported.
Total Group(s)	Total number of multicast forwarding entries.
Group(Mac)	Group MAC address.
Interface	Outbound interface. The Router-port field indicates a router port.

Item	Description
Out-Vlan/InLabel	VLAN ID. When the **Interface** value is a VTEP IP address, this parameter is left blank.

8.11.8 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally.

The **undo igmp-snooping enable** command disables IGMP snooping globally.

By default, IGMP snooping is disabled globally.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BD-based IGMP snooping runs on multiple VTEPs on a VXLAN network. A device sets up a Layer 2 multicast forwarding table by snooping IGMP messages exchanged between multicast users in a BD and the upstream device, and forwards multicast packets on the VXLAN network according to the Layer 2 multicast forwarding table.

Before configuring IGMP snooping for a VXLAN network, enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after you run the **igmp-snooping enable** command in the system view.

Precautions

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configurations are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the device uses the default IGMP snooping configuration.

Example

Enable IGMP snooping globally.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

8.11.9 igmp-snooping enable (BD view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a BD.

The **undo igmp-snooping enable** command disables IGMP snooping in a BD.

By default, IGMP snooping is disabled in a BD.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

To implement IGMP snooping on a VXLAN network, a device needs to set up Layer 2 multicast forwarding entries by snooping IGMP messages exchanged between multicast users in a BD and the upstream router. To achieve this, IGMP snooping needs to be enabled in the BD view.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Example

Enable IGMP snooping in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

```
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
```

8.11.10 igmp-snooping fast-switch enable

Function

The **igmp-snooping fast-switch enable** command enables fast multicast forwarding path switching upon STP topology changes.

The **undo igmp-snooping fast-switch enable** command disables fast multicast forwarding path switching upon STP topology changes.

By default, fast multicast forwarding path switching upon STP topology changes is disabled.

Format

igmp-snooping fast-switch enable

undo igmp-snooping fast-switch enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the Layer 2 network topology changes, multicast forwarding paths may change. When this occurs, the upstream querier sends a Query message to switch the multicast forwarding path. However, there is a delay (60s by default) between the time when network topology change occurs and the time when the Query message is sent. As a result, the downstream device cannot receive the Query message immediately, so the multicast forwarding path cannot be quickly switched.

If the Layer 2 network is running the Spanning Tree Protocol (STP), you can enable fast multicast forwarding path switching upon STP topology changes. When the STP topology changes, this function quickly changes the ports in Forwarding state into router ports to direct multicast data flows to the new forwarding paths.

Prerequisite

Global IGMP snooping has been enabled using the **igmp-snooping enable (system view)** command.

Precautions

- This function takes effect only when STP is used as the loop prevention protocol on a Layer 2 network and the STP operation mode is MSTP, RSTP, or STP.
- With this function configured, the switch sets all ports in Forwarding state as router ports when the STP topology changes. In this case, multicast data flows are forwarded to all the router ports before the router ports are aged. This will cause increase in multicast traffic on the network.

Example

Enable fast multicast forwarding path switching upon STP topology changes.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] igmp-snooping fast-switch enable
```

8.11.11 igmp-snooping group-policy(BD view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a BD.

The **undo igmp-snooping group-policy** command deletes the multicast group policy from a BD.

By default, no multicast group policy is available in a BD, and hosts in the BD can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL used to restrict the range of groups users can join.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.

Parameter	Description	Value
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer that ranges from 1 to 3. ● 1: IGMPv1 ● 2: IGMPv2 ● 3: IGMPv3

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a switch with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. After the switch receives the message, it checks whether the multicast group matches the multicast group policy applied to the BD. If the messages match the ACL, the switch allows user hosts in the BD to join the group and accepts the Report messages. If the messages do not match the ACL, the switch prevents the user hosts in the BD from joining the group.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

- The configuration takes effect only when IGMP snooping is enabled in the BD using the **igmp-snooping enable (BD view)** command..
- Before running the **igmp-snooping group-policy (BD view)** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the BD can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the BD can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the BD can join.

After the **igmp-snooping group-policy (BD view)** command is executed on the BD:

- The BD filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
- The BD discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
- If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

Example

Prevent hosts in BD 123 from joining group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping group-policy 2000
```

Allow hosts in BD 123 to join group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping group-policy 2000
```

8.11.12 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a BD, that is, the interval at which Group-Specific Query messages are sent in the BD.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a BD.

By default, Group-Specific Query messages are sent in a BD at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the last member query interval, you can:

- Configure the switch to send IGMP Group-Specific Query messages at intervals when the querier function is enabled.
- Change the aging time of multicast group member ports.

  When the switch receives an IGMP Leave message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

  If the switch (querier) receives Report messages from other hosts within the aging time, it continues to maintain memberships of the multicast group. If the switch does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The switch sets the maximum response time field in the Group-Specific Query message to the configured last member query interval. Therefore, the maximum response time for Group-Specific Query messages is the same as the interval at which Group-Specific Query messages are sent.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the BD using the **igmp-snooping enable (BD view)** command.

- The IGMP message version is set to v2 or v3 messages in the BD. (Hosts running IGMPv1 do not send Leave messages when they leave a multicast group.)

Example

Set the last member query interval in BD 123 to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping lastmember-queryinterval 4
```

8.11.13 igmp-snooping learning

Function

The **igmp-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo igmp-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. ● *vlan-id1*: specifies the first VLAN ID. ● **to** *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member port is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. An interface is identified as a dynamic group member port when it receives an IGMP Report message.

If users connected to an interface need to receive data of a fixed multicast group, the interface can be statically bound to the multicast group. In this case, run the

undo igmp-snooping learning command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The configuration takes effect only when all the following conditions are met:

- The VLAN specified in this command has been bound to a BD, and IGMP snooping has been enabled in the BD using the **igmp-snooping enable (BD view)** command.
- The interface belongs to the specified VLANs.

If you run the **undo igmp-snooping learning** command multiple times, all the configurations take effect.

Example

Disable learning of group memberships on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 100
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] undo igmp-snooping learning vlan 100
```

8.11.14 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a BD.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a BD.

By default, the maximum response time for IGMP General messages in a BD is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the maximum response time for IGMP General Query messages, you can:

- Control the deadline for a host to send an IGMP Report message. When hosts are required to respond to IGMP General Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of IGMP messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the switch receives a Report message, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **igmp-snooping max-response-time** command sets the maximum response time. The General query count is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

The switch sets the maximum response time field in General Query messages to the value set by the **igmp-snooping max-response-time** command.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

The maximum response time for General Query messages must be shorter than the interval at which General Query messages are sent. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the maximum response time for IGMP Query messages in BD 123 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping max-response-time 20
```

8.11.15 igmp-snooping over-vxlan enable

Function

The **igmp-snooping over-vxlan enable** command enables IGMP snooping for VXLAN.

The **undo igmp-snooping over-vxlan enable** command disables IGMP snooping for VXLAN.

By default, IGMP snooping for VXLAN is disabled.

Format

igmp-snooping over-vxlan enable

undo igmp-snooping over-vxlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring IGMP snooping in a VXLAN, enable IGMP snooping globally and for VXLAN in the system view.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

When you run the **undo igmp-snooping over-vxlan enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping for VXLAN. If any IGMP snooping for VXLAN configuration has been made in the system, the device prompts you to delete all the IGMP snooping for VXLAN configuration.

Example

Enable IGMP snooping for VXLAN.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
```

8.11.16 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a BD so that member ports in the BD can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a BD.

By default, the fast leave function is disabled in a BD.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a multicast group policy that allows member ports to fast leave some multicast groups. Before using this parameter, create an ACL and configure filter rules in the ACL.	-

Parameter	Description	Value
acl-number	Specifies the number of an ACL that defines a range of multicast groups. A basic or advanced ACL can be used.	The value is an integer that ranges from 2000 to 3999.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the switch to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP Leave message for the group. This function saves bandwidth and system resources because the switch does not need to wait until the aging timer of the interface expires.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the BD using the **igmp-snooping enable (BD view)** command.
- IGMPv2 or IGMPv3 messages can be processed in the BD.
- If you do not specify **group-policy** when configuring the fast leave function, this function takes effect for all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command.

Example

Allow member ports in BD 123 to fast leave all groups.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
```

```
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping prompt-leave
```

Allow member ports in BD 123 to fast leave group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping prompt-leave group-policy 2000
```

Prevent member ports in BD 123 from fast leaving group 225.1.1.123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule deny source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping prompt-leave group-policy 2000
```

8.11.17 igmp-snooping querier enable

Function

The **igmp-snooping querier enable** command enables the IGMP snooping querier function in a BD.

The **undo igmp-snooping querier enable** command disables the IGMP snooping querier function in a BD.

By default, the IGMP snooping querier function is disabled in a BD.

Format

igmp-snooping querier enable

undo igmp-snooping querier enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IGMP-capable network, a Layer 3 multicast device functions as a querier to send IGMP Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run IGMP or it uses only static multicast forwarding entries, it cannot function as a querier. In this case, you can enable IGMP snooping querier on the downstream Layer 2 device so that it acts as a querier to send IGMP Query messages.

On a Layer 2 network that has no Layer 3 devices, multicast sources are connected to Layer 2 devices. IGMP snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Perform the following operations as required on your network:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.
- Run the **igmp-snooping robust-count** command to set the number of times Query messages are sent.

Configuration Impact

The IGMP snooping querier does not participate in IGMP querier election. However, the IGMP snooping querier on an IGMP-capable multicast network may affect the election result, because the Query messages sent by the IGMP snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the IGMP snooping querier function is not recommended on an IGMP-capable multicast network.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

Example

Enable the querier function in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping querier enable
Warning: Please confirm that no other querier is configured on the network, otherwise this command may
cause querier re-election, continue?[Y/N]:y
```

8.11.18 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a BD, that is, the interval at which IGMP General Query messages are sent in the BD.

The **undo igmp-snooping query-interval** command restores the default general query interval in a BD.

By default, the general query interval is 125 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the general query interval, you can:

- Configure the switch to send IGMP General Query messages at intervals to maintain memberships of interfaces. When a shorter interval is configured, the switch is more sensitive to multicast membership changes, but more bandwidth and system resources are consumed.
- Change the aging time of multicast member ports.

  When receiving an IGMP Report message from a host, the switch starts the aging timer for the multicast member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The general query count is set by the **igmp-snooping robust-count** command,

and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

The general query interval affects the aging time of group member ports. A shorter general query interval results in a shorter aging time of group member ports and therefore a faster update speed of Layer 2 multicast entries. However, when there are many downstream users connected to a device, a short general query interval can cause flapping of multicast entries, leading to a high CPU usage on the device. Therefore, the default general query interval is recommended. If you need to change the interval to suit service deployment, set the value according to the following table.

Number of IGMP Messages Sent from Downstream Users Within Maximum Response Time	Minimum General Query Interval Reference Value (Seconds)
1 to 1024	10
1024 to 2048	20
2048 to 5120	40

NOTE

The default general query interval defined in RFC documents is 125 seconds, but some vendors define their own default general query intervals. It is recommended that all devices on a multicast network use the same general query intervals (including IGMP and IGMP snooping general query intervals). On Huawei fixed switches, the default value of the IGMP general query interval is 60 seconds, and the default value of the IGMP snooping general query interval is 125 seconds.On Huawei modular switches, the default values of the IGMP general query interval and IGMP snooping general query interval are both 60 seconds.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.
- The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the general query interval in BD 123 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping query-interval 100
```

8.11.19 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave messages in a BD.

The **undo igmp-snooping report-suppress** command disables suppression of IGMP Report and Leave messages in a BD.

By default, IGMP Report and Leave message suppression is disabled in a BD.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a BD, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a BD, the Layer 3 device receives duplicate Leave messages from the member hosts.

After Report message suppression is enabled on a Layer 2 device, the device forwards only one IGMP Membership Report message to the upstream device in the following scenarios:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Configuration Impact

- The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.
- When receiving a Leave message from a group member, the device sends Group-Specific Query messages to check whether the group has other members on the network segment.
- The device can suppress duplicate Report messages even when IGMP message suppression is disabled. The default suppression time is 10 seconds. To change the suppression time, run the **igmp-snooping suppress-time** *suppress-time* command. If the *suppress-time* is set to 0, all the membership packets are forwarded immediately.
- This function cannot suppress IGMPv3 packets.

Example

Enable suppression of Report and Leave messages in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping report-suppress
```

8.11.20 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the switch to drop the IGMP messages without the Router-Alert option in the IP header received from a BD.

The **undo igmp-snooping require-router-alert** command restores the default configuration.

By default, the switch does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the switch checks each IGMP message for the Router-Alert option and discards those IGMP messages without this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

Example

Configure the switch to forward only the IGMP messages with the Router-Alert option in the IP header received from BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping require-router-alert
```

8.11.21 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a BD, which specifies how many times IGMP Query messages are sent.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a BD.

By default, the robustness variable in a BD is 2.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a BD.	The value is an integer that ranges from 2 to 5.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve the multicast forwarding performance. By setting the IGMP robustness variable, you can:

- Specify the number of times the querier sends a Group-Specific Query message, which prevents packet loss on the network.

  When receiving an IGMP Leave message for a multicast group, the switch sends a Group-Specific Query message a certain number of times (specified by the IGMP robustness variable) to check whether this group has any other members. If the quality of transmission links is low, increase the IGMP robustness variable.
- Change the aging time of multicast group member ports.

  When receiving an IGMP Report message from a host, the switch starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

Example

Set the IGMP robustness variable to 5 in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping robust-count 5
```

8.11.22 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a BD.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a BD.

By default, the aging time of dynamic router ports in a BD is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a BD.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the switch. If a router port on the switch ages in this period, the switch does not send Report or Leave messages to router ports. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for the router port if the network is unstable.

When a dynamic router port on the switch receives an IGMP Query message or a PIM Hello message, the switch resets the aging time of the router port.

- If the router port receives an IGMP Query message, the switch sets the remaining aging time of the interface to the configured value.
- If the router port receives a PIM Hello message, the switch sets the aging time of the interface to the holdtime value.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in BD 123 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
```

```
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping router-aging-time 300
```

8.11.23 igmp-snooping router-learning (BD view)

Function

The **igmp-snooping router-learning** command enables router port learning in a BD.

The **undo igmp-snooping router-learning** command disables router port learning in a BD.

By default, router port learning is enabled in a BD.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the switch does not need to receive Query messages or PIM Hello messages from a BD, disable router port learning in the BD. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a BD are forwarded only to router ports in the BD.

By default, router port learning is enabled on an interface. To prevent interfaces in a BD from becoming a router port, disable router port learning in the BD.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

The switch does not listen on IGMP Query messages in a BD after router port learning is disabled in the BD. To ensure normal multicast forwarding in the BD, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

Example

Disable router port learning in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] undo igmp-snooping router-learning
```

8.11.24 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the switch to send IGMP messages with the Router-Alert option in the IP header to a BD.

The **undo igmp-snooping send-router-alert** command configures the switch to send IGMP messages without the Router-Alert option in the IP header to a BD.

By default, the switch sends IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch sends IGMP messages with the Router-Alert option. If some devices in the same BD as the switch can process only the IGMP messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the switch to send IGMP messages without the Router-Alert option.

The switch adds the Router-Alert option only to locally originated IGMP messages and does not add this option to IGMP messages received from other devices.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

Example

Configure the switch to send IGMP messages that do not contain the Router-Alert option in the IP header to BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] undo igmp-snooping send-router-alert
```

8.11.25 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a BD.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a BD.

By default, no mappings between multicast groups and multicast sources exist in a BD.

Format

igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

undo igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

Parameters

Parameter	Description	Value
group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the IP address of the multicast source mapped to a multicast group.	The value is in dotted decimal notation.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such as S1, S2 on the Layer 2 device connected to user hosts. When the Layer 2 device receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the Layer 2 device converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

Before configuring the mapping between a multicast group and a multicast source:

- IGMP snooping has been enabled in the specified BD using the **igmp-snooping enable (BD view)** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the BD.
- SSM mapping has been enabled using the **igmp-snooping ssm-mapping enable** command.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the BD to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.

Example

Map multicast groups 238.1.1.1 through 238.1.1.255 to multicast source 10.1.1.1 in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping version 3
[HUAWEI-bd123] igmp-snooping ssm-mapping enable
[HUAWEI-bd123] igmp-snooping ssm-mapping 238.1.1.0 24 10.1.1.1
```

8.11.26 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables Source-Specific Multicast (SSM) mapping in a BD.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a BD.

By default, SSM mapping is disabled in a BD.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the Layer 2 devices connected to the hosts.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Run the **igmp-snooping ssm-mapping** command to configure group-source mappings.

Precautions

- If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.
- SSM mapping is applicable only to the BDs where IGMP snooping can process IGMPv3 messages. To set the IGMP message version to v3, use the **igmp-snooping version** command in the BD.
- If the multicast group address is an Any-Source Multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the BD view.

Example

Enable SSM mapping in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping version 3
[HUAWEI-bd123] igmp-snooping ssm-mapping enable
```

8.11.27 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a BD to specify the range of SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a BD.

By default, no SSM group policy is available in a BD.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts need to join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

The **igmp-snooping ssm-policy** command takes effect only when the following configurations are complete:

- IGMP snooping has been enabled in the specified BD using the **igmp-snooping enable (BD view)** command.
- SSM mapping has been enabled in the specified BD using the **igmp-snooping ssm-mapping enable** command.
- If IGMPv1 or IGMPv2 packets are sent by user hosts, the IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the BD.
- The ACL has been created and configured rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **14.1 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in BD 123.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
[HUAWEI-acl-basic-2000] rule permit source 225.1.1.123 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping ssm-mapping enable
[HUAWEI-bd123] igmp-snooping ssm-policy 2000
```

8.11.28 igmp-snooping static-group suppress-dynamic-join

Function

The **igmp-snooping static-group suppress-dynamic-join** command disables a device from forwarding IGMP Report and Leave messages that are received from a BD and contain a static group address to upstream Layer 3 devices configured with the static group address.

The **undo igmp-snooping static-group suppress-dynamic-join** command enables a device to forward IGMP Report and Leave messages that are received from a BD and contain a static group address to upstream Layer 3 devices configured with the static group address.

By default, a device forwards IGMP Report and Leave messages that are received from a BD and contain a static group address to upstream Layer 3 devices configured with the static group address.

Format

igmp-snooping static-group suppress-dynamic-join

undo igmp-snooping static-group suppress-dynamic-join

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the upstream Layer 3 multicast device is a non-Huawei device and a static group is configured on its interface connected to the device, users cannot dynamically join or leave the multicast group. You must disable the device from sending Report and Leave messages that contain static group addresses to the Layer 3 multicast device.

This function takes effect only for IGMPv1 and IGMPv2 message and is invalid for IGMPv3 messages.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

Example

Disable a device from forwarding IGMP Report and Leave messages that are received from BD 123 and contain a static group address to upstream Layer 3 devices configured with the static group address.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping static-group suppress-dynamic-join
```

8.11.29 igmp-snooping static-router-port

Function

The **igmp-snooping static-router-port** command configures an interface as a static router port in specified BDs.

The **undo igmp-snooping static-router-port** command cancels the router port configuration in specified BDs.

By default, an interface is not a static router port.

Format

igmp-snooping static-router-port vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping static-router-port vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies VLAN IDs. This parameter specifies in which VLANs the current interface functions as a router port. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface functions as a router port only in the VLAN specified by *vlan-id1*.	The value is an integer that ranges from 1 to 4094. The value of vlan-id2 must be greater than the value of vlan-id1. The vlan-id1 and vlan-id2 parameters identify a range of VLANs.
all	Cancels the static router port configuration in all VLANs on the interface.	-

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to keep forwarding IGMP Report/Leave messages for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

- This command can be configured only on access-side interfaces of a VXLAN network, but not on tunnel-side interfaces of a VXLAN network.
- The VLAN specified in this command has been created, and the interface on which the command needs to be executed has been added to the VLAN.

- The VLAN specified in this command has been bound to a BD, and IGMP snooping has been enabled in the BD.
- If you run the **igmp-snooping static-router-port** command multiple times, all the configurations take effect.

Example

Configure GE0/0/1 as a static router port.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 100
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] igmp-snooping static-router-port vlan 100
```

8.11.30 igmp-snooping suppress-time

Function

The **igmp-snooping suppress-time** command sets the IGMP message suppression time in a BD.

The **undo igmp-snooping suppress-time** command restores the default IGMP message suppression time in a BD.

By default, the IGMP message suppression time is 10 seconds.

Format

igmp-snooping suppress-time *suppress-time*

undo igmp-snooping suppress-time

Parameters

Parameter	Description	Value
suppress-time	Specifies the IGMP message suppression time in a BD.	The value is an integer that ranges from 0 to 300, in seconds. The value 0 indicates that IGMP messages are not suppressed.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce the IGMP messages sent from a Layer 2 device to the upstream Layer 3 device and protect the Layer 3 device from attacks, enable the Layer 2 device to suppress IGMP Report and IGMP Leave messages sent by hosts in a BD. After this function is enabled, the Layer 2 device processes IGMP Report and IGMP Leave messages as follows:

- After receiving an IGMP Report/Leave message and forwarding the message, the Layer 2 device does not forward the same type of messages to the router port within the suppression time.
- If the Layer 2 device receives an IGMP General Query message or Group-Specific message, it does not suppress the first IGMP Report message that responds to the General Query message. In addition, the Layer 2 device resets the suppression timer when it receives the first IGMP Report message.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Follow-up Procedure

Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages. It is recommended that the suppression time be the same as the maximum response time for IGMP Query messages in a BD.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (BD view)** command to enable IGMP snooping in the BD.

The configured suppression time is invalid for IGMPv3 messages.

Example

Set the IGMP message suppression time in BD 123 to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping suppress-time 15
```

8.11.31 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that IGMP snooping can process in a BD.

The **undo igmp-snooping version** command restores the default IGMP message version.

By default, the IGMP snooping version is 2, indicating that IGMP snooping can process IGMPv1 and IGMPv2 messages.

Format

igmp-snooping version *version*

undo igmp-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of IGMP messages that can be processed in a BD.	The value is an integer ranging from 1 to 3. ● 1: indicates that IGMP snooping processes only IGMPv1 messages. ● 2: indicates that IGMP snooping processes IGMPv1 and IGMPv2 messages. ● 3: indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP protocol maintains group memberships between Layer 3 multicast devices and hosts. IGMP has three versions: v1, v2, and v3. This command specifies the version of IGMP messages that IGMP snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If IGMP is not enabled on the Layer 3 multicast device, configure the IGMP message version on the Layer 2 device to be later than or equal to the version running on downstream hosts.

When hosts in a BD run different IGMP versions, run the **igmp-snooping version** command to enable the Layer 2 device to process IGMP messages sent from all the hosts.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

If IGMP snooping is disabled in the specified BD, the configuration succeeds but does not take effect until IGMP snooping is enabled in the BD. To enable IGMP snooping in a BD, run the **igmp-snooping enable (BD view)** command.

If the IGMP message version is changed from IGMPv3 to IGMPv2, the system deletes all the dynamic IGMP snooping entries when the aging time expires and processes static IGMP snooping entries as follows:

- Does not delete static entries that have only multicast groups and no multicast sources.
- Deletes the static entries that have both multicast groups and multicast sources. When the IGMP message version is restored to IGMPv3, the system restores these entries.

Example

Set the version of the IGMP messages that can be processed by IGMP snooping to IGMPv1 in BD 123.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] igmp-snooping version 1
```

8.11.32 l2-multicast static-group

Function

The **l2-multicast static-group** command configures static group memberships on an interface.

The **undo l2-multicast static-group** command deletes static group memberships from an interface.

By default, no static group membership is configured on an interface.

Format

Configure a single static multicast group:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Configure a series of static multicast groups:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address all vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
source-address *source-ip-address*	Specifies the IP address of a multicast source.	The value of *source-ip-address* can be any Class A, Class B, or Class C address, in dotted decimal notation.
group-address *group-ip-address*	Specifies the IP address of a multicast group.	The value of *group-ip-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the VLANs that the interface belongs to. *vlan-id1* [**to** *vlan-id2*] specifies a range of VLAN IDs. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface is bound only to the multicast group in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.
all	Deletes all group memberships from the interface. ● In **group-address all**, **all** indicates that the interface is removed from all multicast groups. ● In **vlan** { **all** | {*vlan-id1* [**to** *vlan-id2*] } &<1-10> }, **all** indicates that the interface is removed from multicast groups in all VLANs.	-

Parameter	Description	Value
group-ip-address1 **to** *group-ip-address2*	Configures multiple static group memberships on the interface. *group-ip-address1* and *group-ip-address2* identify a range of multicast group addresses.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation. The values of *group-ip-address1* and *group-ip-address2* must be in the same network segment (with a 24-bit mask).

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocols, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can receive multicast data of the multicast group over a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled for the VXLAN network using the **igmp-snooping over-vxlan enable** command in the system view.

Precautions

This command can be configured only on access-side interfaces of a VXLAN network, but not on tunnel-side interfaces of a VXLAN network.

The configuration takes effect only when both the following conditions are met:

- The specified VLANs have been created and the interface has been added to these VLANs.
- The VLAN specified in this command has been bound to a BD, and IGMP snooping has been enabled in the BD using the **igmp-snooping enable (BD view)** command.
- The specified group address is not a reserved group address.

Example

Configure a static multicast group 224.1.1.1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 2
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 vlan 2
```

Configure static multicast groups 224.1.1.1 to 224.1.1.3 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping over-vxlan enable
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] l2 binding vlan 2
[HUAWEI-bd123] igmp-snooping enable
[HUAWEI-bd123] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] l2-multicast static-group group-address 224.1.1.1 to 224.1.1.3 vlan 2
```

Delete static multicast group 224.1.1.1 from GE0/0/1 in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo l2-multicast static-group group-address 224.1.1.1 vlan all
```

8.11.33 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the switch to drop unknown multicast flows in a BD.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

By default, a switch broadcasts unknown multicast packets in a BD.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are those that do not match any entry in the multicast forwarding table or match multicast forwarding entries with an empty outbound interface list. These flows are not requested by users. By default, a switch broadcasts unknown multicast flows. To reduce bandwidth usage, you can configure the **multicast drop-unknown** command to discard unknown multicast flows.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown IPv4 multicast packets in a BD are dropped.

Example

Drop unknown multicast flows in BD 123.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 123
[HUAWEI-bd123] multicast drop-unknown
```

8.11.34 reset igmp-snooping group

Function

The **reset igmp-snooping group** command deletes dynamic group memberships learned by IGMP snooping.

Format

reset igmp-snooping group bridge-domain { *bd-id* [[**source-address** *source-address*] **group-address** *group-address*] | **all** }

Parameters

Parameter	Description	Value
all	Deletes IGMP dynamic group memberships of all BDs.	-

Parameter	Description	Value
bd-id	Deletes the dynamic group memberships of a specified BD.	The value is an integer that ranges from 1 to 16777215.
source-address *source-address*	Deletes the dynamic group memberships of a specified source address.	The multicast source address is a Class A, Class B, or Class C IP address on a nature network segment. The value is in dotted decimal notation.
group-address *group-address*	Deletes the dynamic group memberships of a specified group address.	The value of *group-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups on a network change, the switch generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the switch to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to delete existing group memberships.

Precautions

This command cannot delete static group memberships.

NOTICE

Deleting group memberships in a BD temporarily interrupts multicast forwarding in the BD. The switch generates new forwarding entries only when receiving IGMP Report messages from hosts in the BD. The hosts can then receive multicast data.

Example

Delete dynamic group memberships in BD 123.

```
<HUAWEI> reset igmp-snooping group bridge-domain 123
```

8.11.35 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics bridge-domain { *bd-id* | **all** }

Parameters

Parameter	Description	Value
all	Clears IGMP snooping statistics of all BDs.	-
bd-id	Clears IGMP snooping statistics of a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of BD 123.

```
<HUAWEI> reset igmp-snooping statistics bridge-domain 123
Warning: If reset statistical information, the information will be unrecoverable, continue?[Y/N]:y
```

8.12 MLD Snooping Configuration Commands

8.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.12.2 display l2-multicast forwarding-mode

Function

The **display l2-multicast forwarding-mode** command displays the Layer 2 multicast forwarding mode in VLANs.

Format

display l2-multicast forwarding-mode vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the Layer 2 multicast forwarding mode in a specified VLAN. If *vlan-id* is not specified, the system displays the Layer 2 multicast forwarding mode in all VLANs.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on the switch, the switch maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the switch searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The switch determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

To check which Layer 2 multicast forwarding mode is used, run the **display l2-multicast forwarding-mode** command.

Precautions

You can change the forwarding mode using the **l2-multicast forwarding-mode** command.

Example

Display the Layer 2 multicast forwarding mode in all VLANs.

```
<HUAWEI> display l2-multicast forwarding-mode vlan
VLAN                Forwarding-mode        Router-discard
------------------------------------------------------------
1                   IP                     disable
2                   IP                     disable
3                   MAC                       disable
```

Table 8-136 Description of the **display l2-multicast forwarding-mode vlan** command output

Item	Description
VLAN	VLAN ID.
Forwarding-mode	Forwarding mode used in a VLAN, which can be: - MAC address-based forwarding - IP address-based forwarding This parameter can be configured using the **l2-multicast forwarding-mode** { **ip** | **mac** } command.
Router-discard	Whether the switch is configured not to forward multicast data packets to router ports in a VLAN. - enable: The switch does not forward multicast data packets to router ports in the VLAN. - disable: The switch forwards multicast data packets to router ports in the VLAN. This function is configured using the **l2-multicast router-port-discard** command.

8.12.3 display mld-snooping

Function

The **display mld-snooping** command displays the MLD snooping running parameters in a VLAN.

Format

display mld-snooping [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the MLD snooping running parameters in a specified VLAN. If this parameter is not specified, the system displays the MLD running parameters in all VLANs with MLD snooping configured.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view the MLD snooping running parameters. If you run this command after configuring MLD snooping parameters, the command displays the configured parameter values.

To view the MLD snooping configuration, run the **display mld-snooping configuration** command.

Precautions

This command can display the MLD snooping configuration in a VLAN only when at least one interface in the VLAN is in Up state and MLD snooping is enabled in the VLAN.

Example

Display the MLD snooping running parameters in VLAN 3.

```
<HUAWEI> display mld-snooping vlan 3
MLD Snooping Vlan Information for VLAN 3
   MLD Snooping is Enabled
   MLD Version is Set to default 1
   MLD Query Interval is Set to default 125s
   MLD Max Response Interval is Set to default 10s
   MLD Robustness is Set to default 2
   MLD Last Member Query Interval is Set to default 1s
```

```
MLD Router Port Aging Interval is Set to 180s or holdtime in hello
MLD Filter Group-Policy is not set
MLD Prompt Leave Disable
MLD Router Alert is Not Required
MLD Send Router Alert Enable
MLD Snooping proxy is disabled
MLD Snooping report-suppress is disabled
MLD Snooping Querier is disabled
```

Table 8-137 Description of the **display mld-snooping vlan 3** command output

Item	Description
MLD Snooping Vlan Information for VLAN 3	The following information displayed is the MLD snooping running parameters in VLAN 3.
MLD Snooping is Enabled	MLD snooping is enabled in the VLAN. By default, MLD snooping is disabled in a VLAN. MLD snooping can be enabled using the **mld-snooping enable** command.
MLD Version is Set to default 1	Version of MLD messages that can be processed in the VLAN. In this example, the default version 1 is displayed. This parameter is configured using the **mld-snooping version** command.
MLD Query Interval is Set to default 125s	Interval at which MLD General Query messages are sent. In this example, the default value (125 seconds) is displayed. This parameter is configured using the **mld-snooping query-interval** command.
MLD Max Response Interval is Set to default 10s	Maximum response time for MLD General Query messages. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **mld-snooping max-response-time** command.
MLD Robustness is Set to default 2	MLD robustness variable. In this example, the default value 2 is displayed. This parameter is configured using the **mld-snooping robust-count** command.
MLD Last Member Query Interval is Set to default 1s	Interval at which MLD Group-Specific Query messages are sent. In this example, the default value (1 second) is displayed. This parameter is configured using the **mld-snooping last-listener-query-interval** command.

Item	Description
MLD Router Port Aging Interval is Set to 180s or holdtime in hello	Aging time of a router port. In this example, the default value (180 seconds or the holdtime value contained in PIM Hello messages) is displayed. This parameter is configured using the **mld-snooping router-aging-time** command.
MLD Filter Group-Policy is not set	Multicast group policy. In this example, the default configuration is displayed. That is, no policy is configured. A multicast group policy is configured using the **mld-snooping group-policy (VLAN view)** command.
MLD Prompt Leave Disable	The fast leave function is disabled for interfaces in the VLAN (default configuration). The fast leave function can be enabled using the **mld-snooping prompt-leave** command.
MLD Router Alert is Not Required	The switch does not require that MLD messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The switch can be configured to discard MLD messages without the Router-Alert option using the **mld-snooping require-router-alert** command.
MLD Send Router Alert Enable	The switch sends MLD messages with the Router-Alert option to the VLAN (default configuration). The switch can be configured to send MLD messages with the Router-Alert option using the **mld-snooping send-router-alert** command.
MLD Snooping proxy is disabled	MLD snooping proxy is disabled (default configuration). MLD snooping proxy can be enabled using the **mld-snooping proxy** command.
MLD Snooping report-suppress is disabled	MLD snooping report suppression is disabled (default configuration). MLD snooping report suppression can be enabled using the **mld-snooping report-suppress** command.
MLD Snooping Querier is disabled	MLD snooping querier is disabled (default configuration). MLD snooping querier can be enabled using the **mld-snooping querier enable** command.

8.12.4 display mld-snooping configuration

Function

The **display mld-snooping configuration** command displays the MLD snooping configuration.

Format

display mld-snooping [**vlan** *vlan-id*] **configuration**

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the MLD snooping configuration in a specified VLAN. If this parameter is not specified, the system displays the MLD snooping configuration in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the MLD snooping configuration so that you can check whether the MLD snooping configuration made in the system is proper.

To check all MLD snooping running parameters, run the **display mld-snooping** command.

Precautions

Before running the **display mld-snooping configuration** command, run the **mld-snooping enable** commands to enable IGMP snooping globally and in the VLAN. Otherwise, no information is displayed.

Example

Display the MLD snooping configuration in all VLANs.

```
<HUAWEI> display mld-snooping configuration
 MLD Snooping Configuration for VLAN 20
```

```
  mld-snooping enable
  mld-snooping version 2
MLD Snooping Configuration for VLAN 90
  mld-snooping enable
```

Table 8-138 Description of the **display mld-snooping configuration** command output

Item	Description
MLD Snooping Configuration for VLAN	The following information displayed is the MLD snooping configuration in a specific VLAN.
mld-snooping enable	MLD snooping is enabled in the VLAN. By default, MLD snooping is disabled in a VLAN. MLD snooping can be enabled using the **mld-snooping enable** command.
mld-snooping version 2	MLDv1 and MLDv2 messages can be processed in the VLAN. By default, only MLDv1 messages can be processed in a VLAN. This parameter is configured using the **mld-snooping version** command.

8.12.5 display mld-snooping forwarding-table

Function

The **display mld-snooping forwarding-table** command displays the Layer 2 multicast forwarding table.

Format

display mld-snooping forwarding-table vlan [*vlan-id* [[**source-address** *source-ipv6-address*] **group-address** { *group-ipv6-address* | **router-group** }]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays Layer 2 multicast forwarding entries in a specified VLAN. If *vlan-id* is not specified, information about the MLD snooping forwarding table of all VLANs.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
source-address *source-ipv6-address*	Displays the forwarding entries of a specified Layer 2 multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
group-address *group-ipv6-address*	Displays multicast forwarding entries of a specified Layer 2 multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
router-group	Displays Layer 2 multicast forwarding entries of all router ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing MLD snooping configuration, you can use the **display mld-snooping forwarding-table** command to view the MLD snooping forwarding table. This command displays statically configured and dynamically learned multicast forwarding entries.

Each entry contains the multicast source, multicast group, list of outbound interfaces, and VLAN ID of multicast data packets. When the MLD snooping version is set to v2 in a VLAN or when the MLD snooping version is set to v2, the **display mld-snooping forwarding-table** command displays (S, G) entries.

Precautions

This command displays Layer 2 multicast forwarding entries in a VLAN only when at least one interface in the VLAN is in Up state.

Example

Display multicast forwarding entries in VLAN 10.

```
<HUAWEI> display mld-snooping forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
Total Group(s): 2
--------------------------------------------------------------------------------
                    (Source, Group)     Interface                Out-Vlan
--------------------------------------------------------------------------------
```

```
                  Router-port    GigabitEthernet0/0/1             10
         (*, ff1e:0:0:0:0:0:0:1)   GigabitEthernet0/0/1             10
                                   GigabitEthernet0/0/2             10
         (*, ff1e:0:0:0:0:0:0:2)   GigabitEthernet0/0/1             10
                                   GigabitEthernet0/0/2             10
-------------------------------------------------------------------------------
```

Table 8-139 Description of the **display mld-snooping forwarding-table** command output

Item	Description
VLAN ID	VLAN ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode in the VLAN, which can be: ● IP ● MAC The multicast forwarding mode is configured using the **l2-multicast forwarding-mode** command.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. The Router-port field indicates a router port.
Interface	Outbound interface. The value **Stream** indicates an unknown flow entry.
Out-Vlan	VLAN ID of packets.
Router-port	Router port in the VLAN.
Total Group(s)	Total number of multicast forwarding entries.

8.12.6 display mld-snooping port-info

Function

The **display mld-snooping port-info** command displays information about multicast group member ports.

Format

display mld-snooping port-info [**vlan** *vlan-id* [**group-address** *ipv6-group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays multicast group member ports in a specified VLAN. If this parameter is not specified, the system displays multicast group member ports in all VLANs.	The value is an integer that ranges from 1 to 4094.
group-address *ipv6-group-address*	Displays member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value is an IPv6 multicast address, which is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The first two digits are FF.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

MLD snooping creates and maintains a Layer 2 multicast forwarding table by listening on MLD messages exchanged between hosts and a Layer 3 device. The **display mld-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink interfaces have multicast users connected, and control multicast services conveniently.

Precautions

This command can display member port information only when MLD snooping is enabled globally and in a VLAN using the **mld-snooping enable** command and the VLAN is in Up state. If interfaces in the VLAN are dynamic group member ports, the command can display information about these member port information only after they receive MLD Report messages and before their aging time expires.

Example

Display information about multicast group member ports.

```
<HUAWEI> display mld-snooping port-info
-------------------------------------------------------------------------------
                    (Source, Group)   Port                         Flag
                    Flag: S:Static    D:Dynamic
-------------------------------------------------------------------------------
VLAN 10, 1 Entry(s)
              (*, ff1e:0:0:0:0:0:0:1)  GE0/0/1                     S--
                                            1 port(s) include
-------------------------------------------------------------------------------
```

Table 8-140 Description of the **display mld-snooping port-info** command output

Item	Description
(Source, Group)	An (S, G) entry, specifying the multicast source and multicast group.
Port	Multicast group member port. **include** and **exclude** indicate the multicast source filtering mode.
Flag	Type of a member port, which can be: ● **S**: static member port, which is configured using the **mld-snooping static-group** command ● **D**: dynamic member port learned through MLD

8.12.7 display mld-snooping router-port

Function

The **display mld-snooping router-port** command displays information about router ports, including static and dynamic router ports.

Format

display mld-snooping router-port [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the router interfaces in a specified VLAN. If this parameter is not specified, the system displays router ports in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port is a switch port connected to an upstream Layer 3 multicast device. Router ports can be statically configured or dynamically created after receiving an MLD Query message or a PIM Hello message. A router port receives multicast data packets from the upstream multicast device and forwards the packets to group member ports.

The **display mld-snooping router-port** command displays information about router ports, including the type, name, age, and aging time of each router port.

Precautions

This command can display router port information only when MLD snooping is enabled globally and in a VLAN using the **mld-snooping enable** command and the VLAN is in Up state.

Example

Display information about router ports.

```
<HUAWEI> display mld-snooping router-port
 Total Number of Router Port on VLAN 2 is 1
   Port Name              UpTime          Expires          Flags
   GE0/0/1                00:00:06        --               STATIC
```

Table 8-141 Description of the **display mld-snooping router-port** command output

Item	Description
Total Number of Router Port on VLAN 2 is 1	Number of router ports in VLAN 2.
Port Name	Type and number of a router port.
UpTime	Age of a router port, that is, time that elapsed since the interface became a router port.
Expires	Aging time of the router port. ● The aging time is displayed for a dynamic router port. ● For a static router interface, "--" is displayed, indicating that the interface will never age out.
Flags	Type of the router port, which can be: ● **STATIC**: static router port, which is configured using the **mld-snooping static-router-port** command ● **DYNAMIC**: dynamic router port

8.12.8 display mld-snooping forwarding-table statistics

Function

The **display mld-snooping forwarding-table statistics** command displays statistics about Layer 2 multicast forwarding entries.

Format

display mld-snooping forwarding-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring MLD snooping, you can use this command to view statistics about Layer 2 multicast forwarding entries.

Example

Display statistics about Layer 2 multicast forwarding entries.

```
<HUAWEI> display mld-snooping forwarding-table statistics
-------------------------------------------------------------------
0 Stream entries are calculated in statistics
1 IP entries are calculated in statistics
0 MAC entries are calculated in statistics
1 VLAN entries are calculated in statistics
-------------------------------------------------------------------
```

Table 8-142 Description of the **display mld-snooping forwarding-table statistics** command output

Item	Description
Stream entries are calculated in statistics	Number of unknown stream entries in a VLAN.
IP entries are calculated in statistics	Number of entries for IP address-based forwarding in a VLAN.
MAC entries are calculated in statistics	Number of entries for MAC address-based forwarding in a VLAN.
VLAN entries are calculated in statistics	Number of entries for IP address-based and MAC address-based forwarding in a VLAN.

8.12.9 display mld-snooping statistics

Function

The **display mld-snooping statistics** command displays MLD snooping statistics.

Format

display mld-snooping statistics [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MLD snooping statistics in a specified VLAN. If this parameter is not specified, the system displays MLD snooping statistics in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing MLD snooping configuration, you can use the **display mld-snooping statistics** command to view MLD snooping statistics, including the number of MLD messages sent, number of MLD messages received, number of PIM Hello messages received in each VLAN, and number of Layer 2 events that have occurred in all VLANs. Layer 2 events include changes in interface status, changes in VLAN status, changes in VLAN member interfaces (interfaces join or leave VLANs), and MSTP events. When a multicast fault occurs, the MLD snooping statistics help you identify the cause of the fault.

Precautions

This command displays information only when global MLD snooping is enabled using the **mld-snooping enable** command.

Example

Display MLD snooping statistics in all VLANs.

```
<HUAWEI> display mld-snooping statistics
MLD Snooping Events Counter
    Recv VLAN Up Event Times      1027
    Recv VLAN Down Event Times    5
    Recv VLAN Del Event Times     0
    Recv Port Up Event Times      12
    Recv Port Down Event Times    12
    Recv Port Del Event Times     0
    Recv Port Inc Event Times     3069
    Recv Port Exc Event Times     1023
    Recv MSTP Block Event Times   7
    Recv MSTP Forward Event Times 7
    Recv LINK Change Event Times  0
 MLD Snooping Packets Counter
   Statistics for VLAN 10
    Recv V1 Report 16
    Recv V2 Report 8768
    Recv V1 Query  0
    Recv V2 Query  2243
    Recv Done      215
    Recv Pim Hello 0
    Send Query(S=0) 0
    Send Query(S!=0)0
    Send General Query              0
    Send Group-Specific Query       0
    Send Group-Source-Specific Query 0
```

Display MLD snooping in VLAN 20.

```
<HUAWEI> display mld-snooping statistics vlan 20
 MLD Snooping Packets Counter
   Statistics for VLAN 20
```

```
  Recv V1 Report  0
  Recv V2 Report  0
  Recv V1 Query   0
  Recv V2 Query   0
  Recv Done       0
  Recv Pim Hello  0
  Send Query(S=0) 0
  Send Query(S!=0)0
  Send General Query              0
  Send Group-Specific Query        0
  Send Group-Source-Specific Query 0
```

Table 8-143 Description of the **display mld-snooping statistics** command output

Item	Description
MLD Snooping Events Counter	Statistics about MLD snooping events.
Recv VLAN Up Event Times	Number of VLAN Up events.
Recv VLAN Down Event Times	Number of VLAN Down events.
Recv VLAN Del Event Times	Number of VLAN deletion events.
Recv Port Up Event Times	Number of interface Up events.
Recv Port Down Event Times	Number of interface Down events.
Recv Port Del Event Times	Number of interface deletion events.
Recv Port Inc Event Times	Number of times interfaces join VLANs.
Recv Port Exc Event Times	Number of times interfaces leave VLANs.
Recv MSTP Block Event Times	Number of times static groups fail to be created on interfaces that are blocked by MSTP and cannot forward multicast packets.
Recv MSTP Forward Event Times	Number of times static groups are successfully created on interfaces that are in MSTP forwarding state and can forward multicast packets normally.
Recv LINK Change Event Times	Number of link change events.
MLD Snooping Packets Counter	Statistics about MLD snooping packets.
Statistics for VLAN 10	Packet statistics in VLAN 10.
Recv V1 Report	Number of MLDv1 Report messages received.
Recv V2 Report	Number of MLDv2 Report messages received.
Recv V1 Query	Number of MLDv1 Query messages received.
Recv V2 Query	Number of MLDv2 Query messages received.
Recv Done	Number of MLD Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.

Item	Description
Send Query(S=0)	Number of MLD Query messages sent with the source address of ::.
Send Query(S!=0)	Number of MLD Query messages with sent source addresses other than ::.
Send General Query	Number of General Query messages sent.
Send Group-Specific Query	Number of Group-Specific Query messages sent.
Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent.

8.12.10 l2-multicast forwarding-mode

Function

The **l2-multicast forwarding-mode** command configures the forwarding mode of multicast data in a VLAN.

The **undo l2-multicast forwarding-mode** command restores the default forwarding mode of multicast data.

By default, multicast data is forwarded in a VLAN based on IP addresses.

Format

l2-multicast forwarding-mode { **ip** | **mac** }

undo l2-multicast forwarding-mode mac

Parameters

Parameter	Description	Value
ip	Forwards multicast data based on IP addresses.	-
mac	Forwards multicast data based on MAC addresses.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After Layer 2 multicast is enabled on a Layer 2 device, the Layer 2 device maintains a Layer 2 multicast forwarding table. When receiving a multicast packet, the Layer 2 device searches the Layer 2 multicast forwarding table for the outbound interface based on the multicast address of the packet. The Layer 2 device determines the outbound interface based on the IP multicast address or IP multicast MAC address, depending on the configured Layer 2 multicast forwarding mode.

Multiple multicast IP addresses may be mapped to one MAC address. If multicast data is forwarded based on MAC addresses, multicast data may be sent to the users who do not require the multicast data. To prevent this problem, use the IP address-based forwarding mode on devices with Layer 3 functions.

Configuration Impact

To set the IGMP snooping version to IGMPv3 or the MLD snooping version to MLDv2, do not change the default forwarding mode using this command.

After the multicast data forwarding mode is set to MAC address-based forwarding in a VLAN using this command, the VLAN cannot be configured as a multicast VLAN.

Precautions

- This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.
  - On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
  - On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

After IGMP snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] igmp-snooping enable
```

After MLD snooping is enabled globally, configure the switch to forward multicast data in VLAN 100 based on MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] l2-multicast forwarding-mode mac
[HUAWEI-vlan100] mld-snooping enable
```

8.12.11 l2-multicast router-port-discard

Function

The **l2-multicast router-port-discard** command disables the switch from sending multicast data to routed ports in a VLAN.

The **undo l2-multicast router-port-discard** command restores the default configuration.

By default, multicast data can be forwarded to routed ports in a VLAN.

Format

l2-multicast router-port-discard

undo l2-multicast router-port-discard

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, multicast data does not need to be forwarded to routed ports in a VLAN. For example, when all interfaces on a switch are configured as static router ports in a VLAN, you can use this command to conserve bandwidth by preventing multicast data from being sent to these interfaces.

Precautions

This command can only be used in VLANs with Layer 2 multicast snooping disabled. After running this command in a VLAN, enable Layer 2 multicast snooping in the VLAN for the configuration to take effect.

- On an IPv4 network, run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- On an IPv6 network, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv4 network.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] igmp-snooping enable
```

Disable the switch from forwarding multicast data to routed ports in VLAN 10 on an IPv6 network.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] l2-multicast router-port-discard
[HUAWEI-vlan10] mld-snooping enable
```

8.12.12 mld-snooping enable

Function

The **mld-snooping enable** command enables MLD snooping globally or in a VLAN.

The **undo mld-snooping enable** command disables MLD snooping globally or in a VLAN.

By default, MLD snooping is disabled.

Format

System view

mld-snooping enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo mld-snooping enable [**vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }]

VLAN view

mld-snooping enable

undo mld-snooping enable

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Disables MLD snooping on the specified VLANs. *vlan-id1* and *vlan-id2* identify a range of VLANs. If VLAN IDs are specified, MLD snooping is enabled in the specified VLANs. If no VLAN ID is specified, MLD snooping is enabled globally.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.

Parameter	Description	Value
all	Disables MLD snooping on all VLANs.	-

Views

System view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD snooping runs on a Layer 2 device between a Layer 3 multicast device and hosts, and listens on multicast protocol packets exchanged between the Layer 3 device and hosts to maintain a Layer 2 multicast forwarding table. The Layer 2 device manages and controls Layer 2 multicast forwarding based on this forwarding table.

Before configuring MLD snooping, enable global MLD snooping using the **mld-snooping enable** command in the system view. Other MLD snooping configuration commands can be used only after global MLD snooping is enabled.

You can enable MLD snooping in multiple VLANs by using the **mld-snooping enable** command in the system view.

Precautions

After MLD snooping is enabled in a VLAN, IPv6 Layer 3 multicast cannot be configured on the corresponding VLANIF interface. To use the two functions simultaneously, configure IPv6 Layer 3 multicast on the VLANIF interface before enabling MLD snooping in the VLAN.

After you run the **undo mld-snooping enable** command to disable global MLD snooping, all MLD snooping configurations on the switch are deleted. After you run the **mld-snooping enable** command to enable global MLD snooping again, the switch uses the default MLD snooping configuration.

Multicast functions (Layer 2 and Layer 3 multicast) and the flow control function (configured using the **flow-control** command) are mutually exclusive on the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I

Example

Enable global MLD snooping.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
```

Enable MLD snooping in multiple VLANs in the system view.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping enable vlan 2 to 10
```

Enable MLD snooping in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
```

8.12.13 mld-snooping group-policy (interface view)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy on an interface.

The **undo mld-snooping group-policy** command deletes an IPv6 multicast group policy from an interface.

By default, no IPv6 multicast group policy is available on an interface, and hosts connected to the interface can join any IPv6 multicast group.

Format

mld-snooping group-policy *acl6-number* **vlan** *vlan-id* [**version** *mld-version*]

undo mld-snooping group-policy [*acl6-number*] **vlan** *vlan-id*

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
vlan *vlan-id*	Applies the IPv6 multicast group policy to a specified VLAN on an interface.	The value is an integer that ranges from 1 to 4094.
version *mld-version*	Specifies an MLD version. The multicast group policy is applied only to the MLD messages of this version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. ● 1: MLDv1 ● 2: MLDv2

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPv6 multicast group policy controls the multicast programs that users can order on a Layer 2 device with MLD snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. When the Layer 2 device receives the message, it checks whether the multicast group matches the multicast group policy applied to the interface. If the Report messages match the filter rule, the Layer 2 device allows the hosts in the VLAN to join the group and forwards the Report messages. If the Report messages do not match the filter rule, the Layer 2 device prevents the hosts from joining the group and drops the Report messages.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configured multicast group policy takes effect only when all the following conditions are met:

- The interface has been added to the specified VLAN.
- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The ACL specified in the command has been created and had filtering rules configured.
- Run the **acl** command to configure the ACL.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the interface can join.

  After the **mld-snooping group-policy (interface view)** command is executed on the interface:

  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch,

the switch deletes these entries when the aging time of the entries expires.

- If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

An IPv6 multicast group policy can also be configured in the VLAN view (using the **mld-snooping group-policy (VLAN view)** command) to control the multicast groups that users in the VLAN can join. An IPv6 multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 10 on GE0/0/1 from joining IPv6 multicast group ff1c::3/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule deny source ff1c::3/32
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mld-snooping group-policy 2000 vlan 10
```

Allow hosts in VLAN 10 connected to GE0/0/1 to join IPv6 multicast group ff1c::3/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule permit source ff1c::3/32
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mld-snooping group-policy 2000 vlan 10
```

8.12.14 mld-snooping group-policy (VLAN view)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy in a VLAN.

The **undo mld-snooping group-policy** command deletes an IPv6 multicast group policy from a VLAN.

By default, no IPv6 multicast group policy is available in a VLAN, and hosts in the VLAN can join any IPv6 multicast group.

Format

mld-snooping group-policy *acl6-number* [**version** *mld-version*]

undo mld-snooping group-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
mld-version	Applies the multicast group policy only to the MLD messages of the specified version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. ● 1: MLDv1 ● 2: MLDv2

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPv6 multicast group policy controls the multicast programs that users can order on a Layer 2 device with MLD snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. When the Layer 2 device receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If the Report messages match the filter rule, the Layer 2 device allows the hosts in the VLAN to join the group and forwards the Report messages. If the Report messages do not match the filter rule, the Layer 2 device prevents the hosts from joining the group and drops the Report messages.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configured multicast group policy takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- Run the **acl** command to configure the ACL.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that the VLAN can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that the VLAN can join.

  After the **mld-snooping group-policy (VLAN view)** command is executed on the interface:

  - The VLAN filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The VLAN discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the switch, the switch deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

An IPv6 multicast group policy can also be configured in the interface view using the **mld-snooping group-policy (interface view)** command to control the multicast groups that users in one or more VLANs on the interface can join. An IPv6 multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 4 from joining IPv6 multicast group ff1e::1/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule deny source ff1e::1/32
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping group-policy 2001
```

Allow hosts in VLAN 4 to join IPv6 multicast group ff1e::1/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule permit source ff1e::1/32
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping group-policy 2001
```

8.12.15 mld-snooping last-listener-query-interval

Function

The **mld-snooping last-listener-query-interval** command sets the last listener query interval, that is, the interval at which Multicast-Address-Specific Query messages are sent in MLD snooping.

The **undo mld-snooping last-listener-query-interval** command restores the default interval.

By default, the last listener query interval is 1 second.

Format

mld-snooping last-listener-query-interval *query-interval*

undo mld-snooping last-listener-query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies interval at which Multicast-Address-Specific Query messages are sent.	The value ranges from 1 to 5, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring the last listener query interval, you can:

- Adjust the interval at which the querier sends Multicast-Address-Specific Query messages.

  When MLD snooping querier is enabled, you can use the **mld-snooping last-listener-query-interval** command to set the interval at which the querier sends Multicast-Address-Specific Query messages.
- Change the aging time of member ports.

  When a Layer 2 device receives an MLD Done message from a host, it starts an aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last listener query interval x Last listener query count. This command sets the last listener query interval in the formula. The last listener query count is set by the **mld-snooping robust-count** command.

If the querier receives Report messages from other hosts within the aging time, it continues to maintain the memberships of the multicast group. If the querier does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The querier sets the maximum response time field in the Multicast-Address-Specific Query messages to the configured last listener query interval. Therefore, the maximum response time for Multicast-Address-Specific Query messages is the same as the interval at which Multicast-Address-Specific Query messages are sent.

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The local device is enabled to send Query messages using the **mld-snooping querier enable** or **mld-snooping proxy** command.

Example

Set the last listener query interval to 2 seconds in VLAN 4.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping last-listener-query-interval 2
```

8.12.16 mld-snooping learning

Function

The **mld-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo mld-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

mld-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo mld-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. ● *vlan-id1*: specifies the first VLAN ID. ● *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member interface is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. After MLD snooping is enabled in a VLAN, all interfaces in the VLAN are enabled to learn forwarding entries from multicast packets. An interface is identified as a dynamic group member interface when it receives an MLD Report message.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only when all the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The interface belongs to the specified VLANs.

An interface can be statically bound to a multicast group using the **mld-snooping static-group** command. Then you can run the **undo mld-snooping learning** command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Example

Disable learning of group memberships in VLAN 3 and VLAN 4 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] quit
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 3 to 4
[HUAWEI-GigabitEthernet0/0/1] undo mld-snooping learning vlan 3 to 4
```

8.12.17 mld-snooping max-response-time

Function

The **mld-snooping max-response-time** command sets the maximum response time for MLD General Query messages in a VLAN.

The **undo mld-snooping max-response-time** command restores the maximum response time for MLD General Query messages in a VLAN to the default value.

By default, the maximum response time for MLD Listener Query messages is 10 seconds.

Format

mld-snooping max-response-time *max-response-time*

undo mld-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve the multicast forwarding performance on the switch. By setting the maximum response time for MLD General messages, you can:

- Control the deadline for a host to send a Report message. When hosts are required to respond to Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of Report messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the switch receives a Report message from a host, it starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. This command sets the maximum response time in the formula. The number of times General Query messages are sent is set by the **mld-snooping robust-count** command, and the general query interval is set by the **mld-snooping query-interval** command.

The switch sets the maximum response time field in General Query messages to the value configured by the **mld-snooping max-response-time** command.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **mld-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **mld-snooping last-listener-query-interval** command to set the interval at which Multicast-Address-Specific Query messages are sent.

Precautions

To make the configured maximum response time effective in a VLAN, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the maximum response time for General Query messages in VLAN 3 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping max-response-time 20
```

8.12.18 mld-snooping prompt-leave

Function

The **mld-snooping prompt-leave** command enables the fast leave function in a VLAN so that member ports in the VLAN can fast leave multicast groups.

The **undo mld-snooping prompt-leave** command disables the fast leave function in a VLAN.

By default, the fast leave function is disabled in a VLAN.

Format

mld-snooping prompt-leave [**group-policy** *acl6-number*]

undo mld-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy *acl6-number*	Allows member ports to fast leave the multicast groups matching an ACL6. *acl6-number* specifies the number of an ACL6. A basic or advanced ACL6 can be used.	The value is an integer that ranges from 2000 to 3999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the switch to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives a Done message for the group. This function saves bandwidth and system resources because the switch does not need to wait until the aging timer of the interface expires.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- If you do not specify **group-policy** when configuring the fast leave function, this function takes effect for all groups. To specify a group policy in the command, create an ACL and configure rules for the ACL before running the command. For details about ACL configuration commands, see **14.1 ACL Configuration Commands** in "Security Commands."

Example

Allow member ports in VLAN 2 to fast leave all multicast groups.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] mld-snooping enable
[HUAWEI-vlan2] mld-snooping prompt-leave
```

Allow member ports in VLAN 3 to fast leave multicast group 0xff13::0001:0002.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule permit source ff13::0001:0002 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping prompt-leave group-policy 2000
```

Prevent member ports in VLAN 3 from fast leaving multicast group 0xff13::0001:0002.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] acl ipv6 number 2000
```

```
[HUAWEI-acl6-basic-2000] rule deny source ff13::0001:0002 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping prompt-leave group-policy 2000
```

8.12.19 mld-snooping proxy

Function

The **mld-snooping proxy** command enables Multicast Listener Discovery (MLD) snooping proxy in a VLAN.

The **undo mld-snooping proxy** command disables MLD snooping proxy in a VLAN.

By default, MLD snooping proxy is disabled in a VLAN.

Format

mld-snooping proxy

undo mld-snooping proxy

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MLD snooping is enabled, the switch forwards Report messages to router ports and broadcasts Query messages in a VLAN. The MLD snooping proxy function allows the switch to send Query messages in place of the upstream Layer 3 device and send Report/Done messages in place of downstream hosts. This saves the bandwidth on the link between the Layer 3 device and switch. The switch sends a Report/Done message to the upstream Layer 3 device only in the following situations:

- When the first member joins a multicast group or a host sends a Report message in response to an MLD Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Done message to the upstream device. The upstream device then deletes the matching forwarding entry.

An upstream Layer 3 device does not send Query messages as a querier when MLD is not enabled for some reasons, for example, the Layer 3 device has only static multicast groups. In this case, the switch cannot create or maintain group memberships even though MLD snooping is enabled. The MLD snooping proxy function enables the switch to send Query messages to downstream hosts. For the hosts, the switch is a querier.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Configuration Impact

If MLD is enabled on the upstream Layer 3 device, enabling the MLD snooping proxy function on the switch may affect the querier election result. This is because the General Query messages sent by the switch may have a smaller source IP address than the General Query messages sent by the Layer 3 device. Therefore, MLD snooping proxy is not recommended on an MLD-capable multicast network.

Precautions

- The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.
- MLD snooping proxy cannot be enabled in a VLAN if the corresponding VLANIF interface has IPv6 Layer 3 multicast function (such as MLD and IPv6 PIM) enabled.
- After MLD snooping proxy is enabled in a VLAN, MLD snooping querier and MLD message suppression cannot be enabled in the VLAN.
- If multicast VLAN replication is configured on the switch, the MLD snooping proxy function cannot be enabled in user VLANs.

Example

Enable MLD snooping proxy in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] mld-snooping enable
[HUAWEI-vlan100] mld-snooping proxy
```

8.12.20 mld-snooping querier enable

Function

The **mld-snooping querier enable** command enables the MLD snooping querier in a VLAN.

The **undo mld-snooping querier enable** command disables the MLD snooping querier in a VLAN.

By default, the MLD snooping querier is disabled in a VLAN.

Format

mld-snooping querier enable

undo mld-snooping querier enable

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MLD-capable network, a Layer 3 multicast device functions as the querier to send MLD Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run MLD or it uses only static multicast forwarding entries, it cannot function as a querier. You can enable MLD snooping querier on the downstream Layer 2 device so that the device can act as a querier to send MLD Query messages.

On a Layer 2 network that has no Layer 3 devices, multicast sources are connected to Layer 2 devices. MLD snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations as required on your network:

- Set the interval at which the MLD snooping querier sends General Query messages using the **mld-snooping query-interval** command.
- Set the interval at which the MLD snooping querier sends Multicast-Address-Specific Query messages using the **mld-snooping last-listener-query-interval** command.
- Set the query count using the **mld-snooping robust-count** command.

Configuration Impact

The MLD snooping querier does not participate in MLD querier election. However, the MLD snooping querier on an MLD-capable multicast network may affect the election result, because the Query messages sent by the MLD snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the MLD snooping querier function is not recommended on an MLD-enabled multicast network.

Precautions

- The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.
- The MLD snooping querier function cannot be enabled in a VLAN if the corresponding VLANIF interface has IPv6 Layer 3 multicast function (such as MLD and IPv6 PIM) enabled.
- The MLD snooping querier function and MLD snooping proxy cannot be enabled in the same VLAN.
- If multicast VLAN replication is configured, the MLD snooping querier function cannot be enabled in user VLANs.

Example

Enable the MLD snooping querier in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping querier enable
```

8.12.21 mld-snooping query-interval

Function

The **mld-snooping query-interval** command sets the general query interval in a VLAN, that is, the interval at which MLD General Query messages are sent in the VLAN.

The **undo mld-snooping query-interval** command restores the default general query interval in a VLAN.

By default, MLD General Query messages are sent at an interval of 125 seconds.

Format

mld-snooping query-interval *query-interval*

undo mld-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which General Query messages are sent.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the MLD general query interval, you can:

- Specify the interval at which the querier sends MLD General Query messages.

  When the querier function is enabled in a VLAN, you can use this command to set the general query interval. Then the querier sends General Query messages at the configured interval to maintain group memberships. The querier is more sensitive when it sends General Query messages at a smaller interval, but more bandwidth and resources are consumed.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **mld-snooping query-interval** command sets the general query interval. The general query count is set by the **mld-snooping robust-count** command, and the maximum response time for General Query messages is set by the **mld-snooping max-response-time** command.

NOTE

The default general query interval defined in RFC documents is 125 seconds, but some vendors define their own default general query intervals. It is recommended that all devices on a multicast network use the same general query intervals (including MLD and MLD snooping general query intervals). On Huawei fixed switches, the default values of the MLD general query interval and MLD snooping general query interval are both 125 seconds.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Use this command only when the switch can send MLD Query message. The switch can send MLD Query messages only when MLD snooping proxy is enabled using the **mld-snooping proxy** command, or MLD snooping querier is enabled using the **mld-snooping querier enable** command.

The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the switch will delete multicast memberships that should not be deleted.

Example

Set the general MLD query interval in VLAN 3 to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping query-interval 100
```

8.12.22 mld-snooping report-suppress

Function

The **mld-snooping report-suppress** command enables suppression of MLD Report and Done messages in a VLAN.

The **undo mld-snooping report-suppress** command disables suppression of MLD Report and Done messages in a VLAN.

By default, MLD Report and Done message suppression is disabled in a VLAN.

Format

mld-snooping report-suppress

undo mld-snooping report-suppress

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an MLD Membership Report message (Report or Done message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an MLD General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- When leaving a multicast group, a host sends a Done message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Done messages from the member hosts.

When MLD Report suppression is configured on the Layer 2 device, the Layer 2 device sends only one copy of MLD Report message when members join or leave a group. When the first member joins a multicast group or a host sends a Report message in response to a Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device can create or maintain the matching forwarding entry based on the Report message. When the last member of a multicast group leaves the group, the Layer 2 device forwards a Done message to the upstream device. The upstream device then deletes the matching forwarding entry. This reduces the number of MLD messages on the network.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping_enable** command.

Precautions

- The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.
- When receiving a Done message from a group member, the device sends Group-Specific Query messages to check whether the group has other members on the network segment.
- MLD Report message suppression cannot be configured in a VLAN if the corresponding VLANIF interface has IPv6 Layer 3 multicast function (such as MLD and IPv6 PIM) enabled.
- MLD snooping proxy and MLD Report message suppression cannot be configured in the same VLAN.
- If multicast VLAN replication is configured, the MLD message suppression function cannot be enabled in user VLANs.
- The switch can suppress duplicate Report messages even when MLD message suppression is disabled. The default suppression time is 10 seconds. To change the suppression time, run the **mld-snooping suppression-time** *suppression-time* command. If *suppression-time* is set to 0, all membership packets are forwarded immediately.
- This function cannot suppress MLDv2 packets.

Example

Enable suppression of Report and Done messages in VLAN 2.

```
<HUAWEI>system view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] mld-snooping enable
[HUAWEI-vlan2] mld-snooping report-suppress
```

8.12.23 mld-snooping require-router-alert

Function

The **mld-snooping require-router-alert** command configures the switch to check the received MLD messages for the Router-Alert option and discard the MLD messages without the Router-Alert option.

The **undo mld-snooping require-router-alert** command restores the default configuration.

By default, the switch processes the received MLD messages regardless of whether the messages contain the Router-Alert option.

Format

mld-snooping require-router-alert

undo mld-snooping require-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch does not check whether MLD messages contain the Router-Alert option and sends all the MLD messages to the upper-layer routing protocol. After the **mld-snooping require-router-alert** command is executed, the switch checks each MLD message for the Router-Alert option and discards those MLD messages without this option. This improves device performance, reduces cost, and enhances security of the upper-layer routing protocol.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

If MLD snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until MLD snooping is enabled in the VLAN. To enable MLD snooping in a VLAN, run the **mld-snooping enable** command in the VLAN view.

Example

Configure the switch to accept only MLD messages with the Router-Alert option in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
```

```
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping require-router-alert
```

8.12.24 mld-snooping robust-count

Function

The **mld-snooping robust-count** command sets the MLD robustness variable in a VLAN.

The **undo mld-snooping robust-count** command restores the default MLD robustness variable in a VLAN.

By default, the MLD robustness variable in a VLAN is 2.

Format

mld-snooping robust-count *robust-count*

undo mld-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the MLD robustness variable.	The value is an integer that ranges from 2 to 5.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve the multicast forwarding performance. By setting the MLD robustness variable, you can:

- Set the last listener query count for the querier to prevent packet loss.

  When receiving an MLD Done message of a multicast group, the querier sends Multicast-Address-Specific Query messages a certain number of times specified by the robustness variable to check whether the multicast has members. If the quality of transmission links is low, increase the MLD robustness variable.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the switch starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = MLD robustness variable x General query interval + Maximum response time for General Query messages. The **mld-snooping robust-count** command sets the MLD robustness variable.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **mld-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **mld-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **mld-snooping last-listener-query-interval** command to set the interval at which Multicast-Address-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Example

Set the robustness variable to 5 in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping robust-count 5
```

8.12.25 mld-snooping router-aging-time

Function

The **mld-snooping router-aging-time** command sets the aging time of dynamic router ports in a VLAN.

The **undo mld-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VLAN.

By default, the aging time of dynamic router ports in a VLAN is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

mld-snooping router-aging-time *router-aging-time*

undo mld-snooping router-aging-time

Parameters

Parameter	Description	Value
router-aging-time	Indicates the aging time of a router port.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on a network, it takes a longer time to transmit Query messages from the MLD querier to a Layer 2 device. If a router port on the Layer 2 device ages out within this period, the Layer 2 device does not send Report or Done messages to the router port. As a result, multicast data forwarding may be interrupted. To solve this problem, set a longer aging time for router ports if the network is unstable.

When a dynamic router port receives an MLD Query message or PIM Hello message, the Layer 2 device sets the aging time of the router port as follows:

- If the router port receives an MLD Query message, the Layer 2 device sets the aging time of the router port to the configured value.
- If the router port receives a PIM Hello packet, the Layer 2 device sets the aging time of the router port to the Holdtime value contained in the PIM Hello packet.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in VLAN 3 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
```

```
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] mld-snooping router-aging-time 300
```

8.12.26 mld-snooping router-learning

Function

The **mld-snooping router-learning** command enables router port learning in a VLAN.

The **undo mld-snooping router-learning** command disables router port learning in a VLAN.

By default, router port learning is enabled in a VLAN.

Format

mld-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo mld-snooping router-learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Enables an interface to function as a router port in the specified VLANs.	*vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.
all	Enables an interface to function as a router port in all the VLANs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A switch running MLD snooping considers an interface as a router port when the interface receives an MLD General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. A router port provides the following functions:

- Receives multicast data from the upstream device.
- Forwards MLD Report/Done messages. MLD Report/Done messages received in a VLAN are forwarded only to router ports in the VLAN.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

The switch does not listen on MLD Query or PIM Hello messages in a VLAN after router port learning is disabled in the VLAN. To ensure normal multicast forwarding in the VLAN, run the **mld-snooping static-router-port** command to configure a static router port.

Precautions

This command takes effect only when the interface has been added to the specified VLANs and MLD snooping has been enabled in these VLANs using the **mld-snooping enable** command.

Example

Disable router port learning on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo mld-snooping router-learning vlan 10
```

8.12.27 mld-snooping send-query enable

Function

The **mld-snooping send-query enable** command enables the switch to send MLD General Query messages to non-router ports when receiving Layer 2 topology change events.

The **undo mld-snooping send-query enable** command disables the switch from sending MLD General Query messages when receiving Layer 2 topology change events.

By default, the switch does not send MLD General Query messages when receiving Layer 2 topology change events.

Format

mld-snooping send-query enable

undo mld-snooping send-query enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network topology changes, the switch receives a topology change event. By default, the switch does not send MLD General Query messages in this case. The network topology change triggers recalculation of the ring network protocol used (such as STP, MSTP, RRPP, SEP, and Smart Link). If the switch cannot respond to the topology change immediately, multicast data traffic cannot be switched to the new path in a timely manner. The **mld-snooping send-query enable** command enables the switch to send MLD General Query messages to update group memberships when the network topology changes. This ensures that multicast data traffic can be switched to the new transmission path.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

This command is used on a ring network. When the ring network topology changes, the switch sends MLD General Query messages with source IPv6 address FE80::. When this address has been occupied by another device on the network, run the **mld-snooping send-query source-address** command to set the source IPv6 address to FE80::.

Precautions

Use this command only when a ring network protocol is enabled on the switch.

Example

Enable the switch to send MLD General Query messages to non-router ports when receiving Layer 2 topology change events.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping send-query enable
```

8.12.28 mld-snooping send-query source-address

Function

The **mld-snooping send-query source-address** command sets the source IPv6 address of MLD General Query.

The **undo mld-snooping send-query source-address** command restores source IPv6 address of MLD General Query messages.

By default, the source IPv6 address of MLD General Query messages is FE80::.

Format

mld-snooping send-query source-address *ipv6-address*

undo mld-snooping send-query source-address

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address of MLD General Query messages.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, and the network prefix must be FE80::/64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 device sends two types of MLD General Query messages:

- MLD General Query messages sent by the querier when the querier function is enabled using the **mld-snooping proxy** or **mld-snooping querier enable** command.
- MLD General Query messages that the Layer 2 device sends after receiving Layer 2 topology change events (configured using the **mld-snooping send-query enable** command).

By default, MLD General Query messages sent from a Layer 2 device use the source IPv6 address FE80::. When this IPv6 address is used by another device on the network, run the **mld-snooping send-query source-address** command to change the source IPv6 address of MLD General Query messages.

When multiple Layer 2 devices exist on a shared network, you can set source IPv6 addresses of MLD Query messages to identify the devices. For example, when multiple devices with different performance need to participate in querier election, you must configure a different source IPv6 address of MLD Query messages for each device.

When the MLD proxy function is enabled on a device using the **mld-snooping proxy** command or the function of suppressing Report and Leave messages is enabled in a VLAN using the **mld-snooping report-suppress** command, the device sends MLD Report and MLD Done messages on behalf of downstream users, with the default source IP address of the MLD Report and MLD Done messages being FE80::. You can run this command to change the source IP address of MLD Report and MLD Done messages.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Example

Set the source IPv6 address of MLD General Query messages to FE80::1.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping send-query source-address fe80::1
```

8.12.29 mld-snooping send-router-alert

Function

The **mld-snooping send-router-alert** command configures the switch to send MLD messages with the Router-Alert option in the IPv6 header to a VLAN.

The **undo mld-snooping send-router-alert** command configures the switch to send MLD messages without the Router-Alert option to a VLAN.

By default, the MLD messages sent by the switch contain the Router-Alert option.

Format

mld-snooping send-router-alert

undo mld-snooping send-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the switch sends MLD messages with the Router-Alert option. If some devices in the same VLAN as the switch can process only the MLD messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the switch to send MLD messages without the Router-Alert option.

The switch adds the Router-Alert option only to locally originated MLD messages and does not add this option to MLD messages received from other devices.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Example

Configure the switch to send MLD messages that do not contain the Router-Alert option in the IPv6 header to VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 3
[HUAWEI-vlan3] mld-snooping enable
[HUAWEI-vlan3] undo mld-snooping send-router-alert
```

8.12.30 mld-snooping static-group

Function

The **mld-snooping static-group** command configures static IPv6 group memberships on an interface.

The **undo mld-snooping static-group** command deletes the static IPv6 group memberships on an interface.

By default, no static IPv6 group membership is configured on an interface.

Format

mld-snooping static-group *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id*

undo mld-snooping static-group { *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id* | **all** }

Parameters

Parameter	Description	Value
group-ipv6-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
source *source-ipv6-address*	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Deletes all static group memberships from an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocol, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can keep receiving multicast data of the multicast group for a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the specified VLAN using the **mld-snooping enable** command.
- The specified VLAN has been created and the interface has been added to the VLAN.

Multicast group addresses starting with FFx1 or FFx2 (x is any value) cannot be configured as static multicast group addresses.

If a device is configured to forward Layer 2 multicast traffic on a network configured with MUX VLAN using the **multicast-snooping mux-vlan enable** command, the VLAN specified in the **mld-snooping static-group** command must not be a MUX VLAN (include principal VLAN and subordinate VLAN).

Example

Statically bind GE0/0/1 in VLAN 2 to multicast group ff1a::1.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[HUAWEI-GigabitEthernet0/0/1] mld-snooping static-group ff1a::1 vlan 2
```

8.12.31 mld-snooping static-router-port

Function

The **mld-snooping static-router-port** command configures a static router port in a VLAN.

The **undo mld-snooping static-router-port** command deletes a static router port in a VLAN.

By default, no static router port is configured in a VLAN.

Format

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. This parameter specifies in which VLAN the current interface functions as a router port.	The value is an integer that ranges from 1 to 4094.
all	Disables the interface from functioning as a router port in all VLANs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to keep receiving or forwarding multicast data packets for a long time, configure the interface as a static router port.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

This command takes effect only when the interface is added to the specified VLAN.

Example

Configure GE0/0/1 as a router port in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mld-snooping static-router-port vlan 2
```

8.12.32 mld-snooping suppression-time

Function

The **mld-snooping suppression-time** command sets the MLD message suppression time.

The **undo mld-snooping suppression-time** command restores the default MLD message suppression time.

By default, the MLD message suppression time is 10 seconds.

Format

mld-snooping suppression-time *suppression-time*

undo mld-snooping suppression-time

Parameters

Parameter	Description	Value
suppression-time	Specifies the MLD message suppression time.	The value is an integer ranging from 0 to 300, in seconds. The value 0 indicates that MLD messages are not suppressed.

Views

system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect an upstream Layer 3 device from attacks and reduce the load on the Layer 3 device, a Layer 2 device can suppress duplicate MLD Report messages. The default MLD message suppression time is 10 seconds. You can change the MLD message suppression time using the **mld-snooping suppression-time** command.

After you set the MLD message suppression time on a Layer 2 multicast device, the device acts as follows:

- After the Layer 2 device receives an MLD Report message, it does not forward identical MLD Report messages to the router port within the suppression time.

- If the Layer 2 device receives an MLD General Query message or Multicast-Address-Specific Query message within the suppression time, it does not suppress the first MLD Report message sent in response to the Query message. In addition, the Layer 2 device resets the suppression timer when it receives the first MLD Report message.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

You can run this command for MLDv1 Done and MLDv2 packets, but the command does not take effect.

Example

Set the MLD message suppression time to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] mld-snooping suppression-time 15
```

8.12.33 mld-snooping table limit

Function

The **mld-snooping table limit** command sets the maximum number of MLD snooping entries that can be learned on an interface.

The **undo mld-snooping table limit** command cancels the limit on the number of MLD snooping entries that can be learned on an interface.

By default, the number of multicast entries that an interface can learn is not limited.

Format

mld-snooping table limit *limit* **vlan** *vlan-id*

undo mld-snooping table limit [*limit*] **vlan** *vlan-id*

Parameters

Parameter	Description	Value
limit	Specifies the maximum number of MLD snooping entries that can be learned on an interface.	The value is an integer and the value range depends on the product model: - SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5731-S, S5731S-S, and S5720I-SI: 1 to 1024 - S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S: 1 to 1500 - S5735S-H, S5736-S, and S6720S-S: 1 to 1536 - S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1 to 4096
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum number of MLD snooping entries on an interface limits the number of programs that users on the interface can order. You can set this limit to control the multicast data traffic on an interface.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Configuration Impact

If the number of multicast entries on the interface already exceeds the configured threshold, the number of multicast entries on the interface does not change and the interface cannot learn new multicast entries.

Precautions

The configuration takes effect only after you run the **mld-snooping_enable** command to enable MLD snooping in the VLAN.

Example

Set the maximum number of MLD snooping entries that can be learned on GE0/0/1 in VLAN 5 to 100. (GE0/0/1 has been added to VLAN 5, and MLD snooping has been enabled globally and in VLAN 5.)

```
<HUAWEI> system view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 5
[HUAWEI-vlan5] mld-snooping enable
[HUAWEI-vlan5] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mld-snooping table limit 100 vlan 5
```

8.12.34 mld-snooping version

Function

The **mld-snooping version** command sets the version of MLD messages that MLD snooping can process in a VLAN.

The **undo mld-snooping version** command restores the default MLD message version.

By default, MLD snooping can process only MLDv1 messages.

Format

mld-snooping version *version*

undo mld-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of MLD messages that MLD snooping can process.	The value is 1 or 2. ● 1: Only MLDv1 messages can be processed. ● 2: Both MLDv1 and MLDv2 messages can be processed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD protocol maintains group memberships between Layer 3 multicast devices and hosts. MLD has two versions: v1 and v2. This command specifies the version of MLD messages that MLD snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If MLD is not enabled on the Layer 3 multicast device, configure the MLD message version on the Layer 2 device to be later than or equal to the MLD version running on downstream hosts.

When hosts in a VLAN run different MLD versions, run the **mld-snooping version** command to enable the Layer 2 device to process MLD messages sent from all the hosts.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

This command cannot be used in user VLANs of a multicast VLAN.

When the MLD snooping version is set to MLDv2:

- The switch can use only the default Layer 2 multicast forwarding mode.
- The S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S forward multicast data by looking up the forwarding table according to the VLAN ID and group address.

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Set the MLD message version to 2 in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] mld-snooping enable
[HUAWEI-vlan2] mld-snooping version 2
```

8.12.35 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the switch to discard unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

The default method that a switch uses to process unknown multicast flows depends on whether Layer 2 multicast is enabled and which Layer 2 multicast forwarding mode is used.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are those that do not match any entry in the multicast forwarding table or match multicast forwarding entries with an empty outbound interface list. These flows are not requested by users. When MLD snooping is disabled, the switch broadcasts unknown IPv6 multicast flows in the corresponding VLAN. After MLD snooping is enabled, the switch broadcasts unknown IPv6 multicast flows in the corresponding VLAN in MAC address-based forwarding mode. If IP address-based forwarding is used, the following switch models broadcast unknown IPv6 multicast flows in the corresponding VLAN and other switch models discard unknown IPv6 multicast flows: S5735S-H, S5736-S (except S5736-S48S4X-A, S5736-S48S4X-D, and S5736-S24UM4XC).. If a switch broadcasts unknown multicast flows in a VLAN, you can configure the switch to drop unknown multicast flows, reducing instant bandwidth usage.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown IPv4 and IPv6 multicast packets are discarded, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if MAC address-based forwarding is configured as the Layer 2 multicast forwarding mode and the **multicast drop-unknown** command is executed, unknown multicast packets destined for the following reserved network segments and IP address cannot be dropped: 239.0.0.0/8, 224.0.0.0/24, 224.0.1.0/24, FF0X:0:0:0:0:0:0:0/96, FF0X::DB8:0:0/96, and the IPv6 address with the last 32 bits being 0000:00XX. To drop such unknown multicast packets, configure a traffic policy.

Example

Discard unknown multicast packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] multicast drop-unknown
```

8.12.36 multicast-snooping mux-vlan enable

Function

The **multicast-snooping mux-vlan enable** command enables a device to transmit Layer 2 multicast traffic on a network configured with MUX VLAN.

The **undo multicast-snooping mux-vlan enable** command disables a device from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

By default, a device is disabled from transmitting Layer 2 multicast traffic on a network configured with MUX VLAN.

Format

multicast-snooping mux-vlan enable

undo multicast-snooping mux-vlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, on a network configured with MUX VLAN, Layer 2 multicast traffic cannot be transmitted between the principal VLAN and subordinate VLANs. You can run the **multicast-snooping mux-vlan enable** command to enable Layer 2 multicast traffic to be transmitted on the network configured with MUX VLAN.

Precautions

If a MUX VLAN is bound to a static multicast group using the **l2-multicast static-group** or **mld-snooping static-group** command, the **multicast-snooping mux-vlan enable** command cannot be executed. You must delete the association between the MUX VLAN and static multicast group before running the **multicast-snooping mux-vlan enable** command.

After the **multicast-snooping mux-vlan enable** command is configured, you cannot run the **l2-multicast static-group** or **mld-snooping static-group** command to bind a MUX VLAN to a static multicast group.

Example

Enable a device to forward Layer 2 multicast traffic on a network configured with MUX VLAN.

```
<HUAWEI> system-view
[HUAWEI] multicast-snooping mux-vlan enable
```

8.12.37 multicast-source-deny

Function

The **multicast-source-deny** command discards multicast data packets sent from specified VLANs on an interface.

The **undo multicast-source-deny** command restores multicast forwarding in specified VLANs on an interface.

By default, multicast data packets from all VLANs are forwarded on an interface.

Format

multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo multicast-source-deny [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies a VLAN ID. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If you do not specify **to** *vlan-id2*, only one VLAN is specified.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **multicast-source-deny** command on an interface, multicast packets received from specified VLANs are discarded on the interface. You may need to use this command in the following scenarios:

- A user-side interface receives multicast packets, but the switch does not need to receive multicast data packets from user-side interfaces. Discarding multicast data packets received on a user-side interface protects the system against forged multicast flows sent from malicious users.
- Multiple multicast sources in different VLANs are connected to the switch through a Layer 2 network, but the switch only needs to receive multicast data from some of the multicast sources.
- In some situations, for example, multicast services for users connected to an interface have expired and need to be stopped, the network administrator can use this command on this interface. Then multicast data packets from specified VLANs cannot be sent to the users.

Precautions

If you run the **multicast-source-deny** command multiple times, all the configurations take effect.

When using the **multicast-source-deny** command on an interface, ensure that the interface has been added to the specified VLANs. Otherwise, the configuration does not take effect.

This command can discard only multicast data packets that meet both of the following conditions:

- The destination MAC address is an IP multicast MAC address (IPv4 MAC address starting with 0x01-00-5e or IPv6 multicast MAC address starting with 0x3333).
- The packet encapsulation protocol is UDP.

Example

Discard multicast data packets sent from VLANs 100 to 105 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-source-deny vlan 100 to 105
```

8.12.38 reset mld-snooping group

Function

The **reset mld-snooping group** command deletes dynamic group memberships learned by MLD snooping.

Format

reset mld-snooping group { **all** | **vlan** *vlan-id* [[**source-address** *source-ipv6-address*] **group-address** *group-ipv6-address*] }

Parameters

Parameter	Description	Value
all	Deletes dynamic group memberships learned by MLD snooping.	-
vlan *vlan-id*	Deletes dynamic group memberships in a specified VLAN.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
group-ipv6-address	Deletes the dynamic group memberships of a specified source address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Parameter	Description	Value
source-address *source-ipv6-address*	Deletes the dynamic group memberships of a specified source address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast groups change on a network, the switch generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the switch to generate new multicast forwarding entries immediately, use the **reset mld-snooping group** command to delete old memberships.

Precautions

NOTICE

Deleting group memberships in a VLAN temporarily interrupts multicast forwarding in the VLAN. The switch generates new forwarding entries only when receiving MLD Report messages from hosts in the VLAN. The hosts can then receive multicast data.

This command cannot delete static group memberships.

This command is valid only for VLANs with MLD snooping enabled and is invalid for a VLAN if MLD is enabled on the corresponding VLANIF interface.

Example

Delete dynamic group memberships in VLAN 2.

```
<HUAWEI> reset mld-snooping group vlan 2
```

8.12.39 reset mld-snooping statistics

Function

The **reset mld-snooping statistics** command clears MLD snooping statistics.

Format

reset mld-snooping statistics [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears the MLD snooping statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To analyze the MLD snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display mld-snooping statistics** command to view the MLD snooping statistics.

Precautions

NOTICE

The cleared MLD snooping statistics cannot be restored.

Example

Clear MLD snooping statistics in VLAN 2.

```
<HUAWEI> reset mld-snooping statistics vlan 2
```

8.13 Static Multicast MAC Address Configuration Commands

8.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.13.2 display mac-address multicast

Function

The **display mac-address multicast** command displays the static multicast MAC address entries.

Format

display mac-address multicast [[*mac-address*] **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
mac-address	Specifies a multicast MAC address. If this parameter is not specified, the system displays all the configured multicast MAC address entries.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Displays multicast MAC address entries in a specified VLAN. If this parameter is not specified, the system displays multicast MAC address entries in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays static multicast MAC address entries. To configure a static multicast MAC address on the device, use the **mac-address multicast interface** or **mac-address multicast** command.

Example

Display static multicast MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address multicast vlan 10
-------------------------------------------------------------------------------
```

```
MAC Address         VLANID        Out-Interface              Status
---------------------------------------------------------------------------
0111-1111-2222      10            GigabitEthernet0/0/1       InActive
                                  GigabitEthernet0/0/2       InActive
                                  2 port(s)
---------------------------------------------------------------------------
Total Group(s) : 1
```

Table 8-144 Description of the **display mac-address multicast vlan 10** command output

Item	Description
MAC Address	Static multicast MAC address.
VLANID	VLAN that the interface bound to the multicast MAC address belongs to.
Out-Interface	Interface bound to the multicast MAC address.
Status	Status of a VLAN. InActive indicates that the VLAN has not been created or no physical interface is added to the VLAN after it is created. Active indicates that the VLAN has been created and has physical interfaces in it.
Total Group(s)	Total number of multicast groups.

8.13.3 display mac-address multicast total-number

Function

The **display mac-address multicast total-number** command displays the number of static multicast MAC address entries.

Format

display mac-address multicast [**vlan** *vlan-id*] **total-number**

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the number of static multicast MAC address entries in a specified VLAN. If this parameter is not specified, the system displays the total number of static multicast MAC address entries in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenarios

The **display mac-address multicast total-number** displays the number of static multicast MAC address entries.

Precautions

If no static MAC address entry is configured, the total number of MAC address entries is displayed as 0. You can use the **mac-address multicast** command to statically bind a multicast MAC address to an interface or use the **mac-address multicast interface** command to statically bind a MAC address to multiple interfaces.

Example

Display the number of static multicast MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address multicast vlan 10 total-number
Total number of mac-address : 3
```

Table 8-145 Description of the **display mac-address multicast vlan 10 total-number** command output

Item	Description
Total number of mac-address	Number of static multicast MAC address entries.

8.13.4 mac-address multicast

Function

The **mac-address multicast** command configures a static multicast MAC address on an interface.

The **undo mac-address multicast** command deletes the static MAC address from an interface.

By default, no static multicast MAC address is configured on an interface.

Format

mac-address multicast *mac-address* **vlan** *vlan-id*

undo mac-address multicast *mac-address* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a multicast MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Specifies the VLAN that the interface belongs to.	The value is an integer that ranges from 1 to 4094.

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch broadcasts received multicast packets in a VLAN, wasting network bandwidth and threatens network security. To reduce broadcasting of multicast packets, configure IGMP snooping or MLD snooping on the switch so that the switch can generate Layer 2 multicast forwarding entries. Alternatively, configure static multicast MAC address entries by binding multicast MAC addresses to interfaces.

After a static multicast MAC address is configured on an interface, multicast packets destined for this multicast MAC address are forwarded only to the interface in the specified VLAN.

Prerequisites

- The specified VLAN exists and the interfaces have been added to the VLAN.
- The switch has been configured to forward multicast data based on MAC addresses using the **l2-multicast forwarding-mode mac** command.

Precautions

- The MAC address specified in the command must be a multicast MAC address with the rightmost bit as 1 (xxxx xxx1).
- The VLAN specified in the command cannot be a super-VLAN, control VLAN of an Ethernet Ring Protection Switching (ERPS) ring, control VLAN of a Smart Ethernet Protocol (SEP) segment, or control VLAN of a Rapid Ring Protection Protocol (RRPP) ring.

- When the static multicast MAC address configured on an interface is an IPv4 multicast MAC address starting with 0x01-00-5e or an IPv6 multicast MAC address starting with 0x3333, Layer 2 multicast snooping cannot be enabled in the VLANs on the interface.
- Before configuring static multicast MAC addresses on an interface of the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, set the multicast data forwarding mode to MAC address-based mode in the VLAN to which the interface belongs.

Example

Configure static MAC address 0100-2100-2200 on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mac-address multicast 0100-2100-2200 vlan 10
```

8.13.5 mac-address multicast interface

Function

Using the **mac-address multicast interface** command, you can bind a multicast MAC address to multiple interfaces. Multicast packets destined for the specified multicast MAC address are forwarded by these interfaces.

Using the **undo mac-address multicast interface** command, you can delete a MAC address from multiple interfaces.

Format

mac-address multicast *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **vlan** *vlan-id*

undo mac-address multicast *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10> **vlan** *vlan-id*

undo mac-address multicast { **all** | [*mac-address*] **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
mac-address	Specifies a multicast MAC address.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.
interface-type interface-number1	Specifies the start interface to which the MAC address is bound.	-

Parameter	Description	Value
to *interface-type interface-number2*	Specifies the end interface to which the MAC address is bound. The specified interfaces and *interface-number2* must be greater than *interface-number1*.	-
all	Deletes the multicast MAC address from all interfaces.	-
vlan *vlan-id*	Specifies the VLAN that the interfaces belong to.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

If Layer 2 multicast snooping is disabled on a switch, the switch broadcasts all the received multicast data packets in corresponding VLANs. This wastes network bandwidth and threatens network security.

Configuring static multicast MAC addresses on interfaces can solve this problem. This configuration ensures that multicast packets destined for a multicast MAC address are forwarded only to interfaces configured with this multicast MAC address in the VLAN.

Precautions

- If you run the **mac-address multicast** command multiple times, all the configurations take effect.
- Before running this command, ensure that the VLAN has been created, and the interface where the multicast MAC address is configured has been added to this VLAN. Otherwise, configuration of this command does not take effect.
- The MAC address specified in the command must be a multicast MAC address with the rightmost bit as 1 (xxxx xxx1).
- The VLAN specified in the command cannot be a super-VLAN, control VLAN of an Ethernet Ring Protection Switching (ERPS) ring, control VLAN of a Smart Ethernet Protocol (SEP) segment, or control VLAN of a Rapid Ring Protection Protocol (RRPP) ring.

- When the static multicast MAC address configured on an interface is an IPv4 multicast MAC address starting with 0x01-00-5e or an IPv6 multicast MAC address starting with 0x3333, Layer 2 multicast snooping cannot be enabled in the VLANs on the interface.
- Before configuring static multicast MAC addresses on an interface of the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, set the multicast data forwarding mode to MAC address-based mode in the VLAN to which the interface belongs.

Example

Bind multicast MAC address 0100-2100-2200 to interfaces GE0/0/1 to GE0/0/4 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] mac-address multicast 0100-2100-2200 interface gigabitethernet 0/0/1 to gigabitethernet
0/0/4 vlan 10
```

8.13.6 multicast mac-ip check enable

Function

The **multicast mac-ip check enable** command enables the function of checking the mapping between multicast IP and MAC addresses.

The **undo multicast mac-ip check enable** command disables the function of checking the mapping between multicast IP and MAC addresses.

By default, the function of checking the mapping between multicast IP and MAC addresses is disabled.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported

Product	Support
SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S	Not supported The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S check the mapping between multicast IP and MAC addresses for received packets by default. On these models, Layer 2 multicast packets with incorrect mappings cannot be forwarded based on IP addresses but can be forwarded based on MAC addresses; Layer 3 multicast packets with incorrect mappings are discarded. Other switch models do not perform this check on multicast packets. They simply forward Layer 2 multicast packets and discard Layer 3 multicast packets.

Format

multicast mac-ip check enable

undo multicast mac-ip check enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable multicast sources and group members to communicate, network-layer multicast services must be provided using multicast IP addresses. To enable multicast data to be correctly transmitted on the local physical network, link-layer multicast services must be provided using multicast MAC addresses. The destination address of a multicast data packet is a group with unknown members but not a specific receiver. Therefore, multicast IP addresses must be mapped to multicast MAC addresses. For the detailed mapping between multicast IP and MAC addresses, see Multicast Addresses under **IP Multicast Configuration Guide** > **Understanding IP Multicast** in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide*.

By default, the function of checking the mapping between multicast IP and MAC addresses is disabled. Therefore, packets with incorrect mapping will be processed normally. After the mapping between multicast IP and MAC addresses is enabled, different products process multicast packets in different modes. The following table provides the details.

Table 8-146 Methods used by different products to process multicast packets

Product	How Multicast Packets Are Processed
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S	Packets with incorrect IP and MAC address mapping are discarded.
S6720-EI, S6735-S, and S6720S-EI	If no MAC address entries are available for the packets with incorrect IP and MAC address mapping, the packets are forwarded as unknown multicast packets. For the forwarding process of unknown multicast packets, see **multicast drop-unknown**.

Example

Enable the function of checking the mapping between multicast IP and MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] multicast mac-ip check enable
```

8.14 Multicast VLAN Configuration Commands

8.14.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.14.2 display l2-multicast-bind

Function

The **display l2-multicast-bind** command displays bindings between multicast VLANs and user VLANs.

Format

display l2-multicast-bind [**mvlan** *vlan-id*]

Parameters

Parameter	Description	Value
mvlan *vlan-id*	Displays the binding between user VLANs and a specified multicast VLAN. *vlan-id* specifies a multicast VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring multicast VLAN replication on an interface, you can run the **display l2-multicast-bind** command to view the configuration. This command can be used for fault location when multicast VLAN replication fails.

Precautions

If there is no binding between any multicast VLAN and user VLAN, the **display l2-multicast-bind** command does not display any information.

Example

Display bindings between user VLANs and multicast VLAN 400.

```
<HUAWEI> display l2-multicast-bind mvlan 400
 ------------------------------------------------------------------
 Port                         Startvlan        Endvlan        Mvlan
 ------------------------------------------------------------------
 GigabitEthernet0/0/1               222             --          400
 ------------------------------------------------------------------
 Total Table(s) : 1
```

Table 8-147 Description of the **display l2-multicast-bind** command output

Item	Description
Port	Interface where user VLANs are bound to the multicast VLAN.
Startvlan	First user VLAN ID.
Endvlan	Last user VLAN ID. If "--" is displayed, only one user VLAN is bound to the multicast VLAN.

Item	Description
Mvlan	Multicast VLAN ID.
Total Table(s)	Total number of multicast VLAN binding entries.

8.14.3 display multicast static-flow

Function

The **display multicast static-flow** command displays the configuration of the static flow in a multicast VLAN.

Format

display multicast static-flow [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays static multicast flows in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a static flow is configured in a multicast VLAN, you can run the **display multicast static-flow** command to view the mapping between the multicast VLAN and (S, G) entry.

Example

Display the static flow configured in multicast VLAN 10.

```
<HUAWEI> display multicast static-flow vlan 10
---------------------------------------------------------
   Vlan           (Source, Group)
---------------------------------------------------------
    10            (*,  225.0.0.1)
---------------------------------------------------------
Total Table(s): 1
```

Table 8-148 Description of the **display multicast static-flow** command output

Item	Description
Vlan	VLAN where the static flow is configured.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group.
Total Table(s)	Total number of static multicast flows.

8.14.4 display multicast-vlan

Function

The **display multicast-vlan** command displays information about multicast VLANs.

Format

display multicast-vlan vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Specifies the ID of a multicast VLAN. - If *vlan-id* is specified, detailed information about the specified multicast VLAN and its user VLANs is displayed. - If *vlan-id* is not specified, brief information about all the multicast VLANs is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast-vlan** command displays configuration of multicast VLANs. You can run the **display multicast-vlan** command to check whether any user VLAN is bound to the multicast VLAN and whether IGMP snooping or MLD snooping is enabled in the multicast VLAN and user VLAN. This command can be used to locate faults when the multicast service fails.

Example

Display information about all multicast VLANs and user VLANs.

```
<HUAWEI> display multicast-vlan vlan
 Total multicast vlan   2
 multicast-vlan     user-vlan number     snooping-state
 ----------------------------------------------------------------
 5                1                    IGMP Enable /MLD Disable
 7                2                    IGMP Enable /MLD Disable
```

Table 8-149 Description of the **display multicast-vlan vlan** command output

Item	Description
Total multicast vlan	Number of multicast VLANs.
multicast-vlan	ID of a multicast VLAN.
user-vlan number	Number of user VLANs bound to a multicast VLAN.
snooping-state	Whether IGMP snooping and MLD snooping is enabled in a multicast VLAN.

Display information about multicast VLAN 7 and its user VLANs.

```
<HUAWEI> display multicast-vlan vlan 7
 Multicast-vlan         : 7
 User-vlan Number       : 2
 IGMP snooping state    : Enable
 MLD  snooping state    : Disable
 User-vlan              Snooping-state
 Prune-source-port state: Disable
 -------------------------------------
 8                      IGMP Enable /MLD Disable
 9                      IGMP Enable /MLD Disable
```

Table 8-150 Description of the **display multicast-vlan vlan** *vlan-id* command output

Item	Description
Multicast-vlan	ID of a multicast VLAN.
User-vlan Number	Number of user VLANs bound to a multicast VLAN.
IGMP snooping state	Whether IGMP snooping is enabled in a multicast VLAN.

Item	Description
MLD snooping state	Whether MLD snooping is enabled in a multicast VLAN.
User-vlan	ID of a user VLAN.
Prune-source-port state	Whether permits Query messages received in a multicast VLAN to be sent back to from the upstream interface through user VLANs.
Snooping-state	Whether IGMP snooping and MLD snooping are enabled in a user VLAN.

8.14.5 display user-vlan

Function

Using the **display user-vlan** command, you can view information about a user VLAN.

Format

display user-vlan vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Specifies the ID of a user VLAN. If *vlan-id* is specified, information about the specified user VLAN is displayed. If *vlan-id* is not specified, information about all user VLANs is displayed.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After binding a user VLAN to a multicast VLAN, you can run the **display user-vlan** command to verify the configuration and check whether IGMP snooping or MLD

Snooping is enabled. This command can be used to locate faults when the multicast service fails.

Example

Display information about all user VLANs.

```
<HUAWEI> display user-vlan vlan
 Total user vlan   3
 user-vlan  snooping-state            multicast-vlan  snooping-state
 ------------------------------------------------------------------------------
 8          IGMP Disable/MLD Disable  7               IGMP Enable /MLD Disable
 9          IGMP Disable/MLD Disable  7               IGMP Enable /MLD Disable
 11         IGMP Disable/MLD Disable  7               IGMP Enable /MLD Disable
```

Display information about user VLAN 8.

```
<HUAWEI> display user-vlan vlan 8
 user-vlan  snooping-state            multicast-vlan
 --------------------------------------------------
 8         IGMP Disable/MLD Disable   7
```

Table 8-151 Description of the **display user-vlan** command output

Item	Description
Total user vlan	Number of user VLANs.
user-vlan	ID of a user VLAN.
multicast-vlan	ID of the multicast VLAN that a user VLAN belongs to.
snooping-state	Whether IGMP snooping and MLD snooping are enabled in a multicast VLAN or a user VLAN.

8.14.6 l2-multicast-bind vlan

Function

The **l2-multicast-bind vlan** command binds user VLANs to a multicast VLAN on an interface.

The **undo l2-multicast-bind vlan** command restores the default setting.

By default, no user VLAN is bound to a multicast VLAN on an interface.

Format

l2-multicast-bind vlan *vlan-id1* [**to** *vlan-id2*] **mvlan** *mvlan-id*

undo l2-multicast-bind vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a user VLAN.	The value is an integer that ranges from 1 to 4094.
mvlan *mvlan-id*	Specifies the ID of a multicast VLAN.	The value is an integer that ranges from 1 to 4094.
all	Unbinds all user VLANs from the multicast VLAN on an interface.	-

Views

MultiGE interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A carrier provides the multicast service for multiple Internet service providers (ISPs), and each ISP is assigned a multicast VLAN to isolate multicast data and routes of different ISPs. Users connected to different user-side interfaces of the switch may order multicast services of different ISPs but belong to the same user VLAN. If multicast replication based on user VLANs is used in this case, users may receive multicast data they do not require. This affects the income of the ISPs.

To solve this problem, bind the user VLAN to multicast VLANs of the ISPs whose services are ordered on user-side interfaces. Then the user-side interfaces accept only the data from multicast VLANs of the specified ISPs.

Prerequisites

IGMP snooping has been enabled using the **igmp-snooping enable (VLAN view)** command on the multicast VLAN.

Precautions

Before running this command, run the **vlan** command to create the corresponding user VLAN and multicast VLAN. Otherwise, configuration of this command does not take effect.

On an interface, a user VLAN can be bound to only one multicast VLAN.

Currently, the binding of user VLANs to a multicast VLAN on an interface is only supported on IPv4 networks.

Example

Bind user VLAN100 to multicast VLAN20 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] igmp-snooping enable
[HUAWEI-vlan100] quit
[HUAWEI] vlan 20
[HUAWEI-vlan20] igmp-snooping enable
[HUAWEI-vlan20] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] l2-multicast-bind vlan 100 mvlan 20
```

8.14.7 l2-multicast user-vlan limit

Function

The **l2-multicast user-vlan limit** command sets the number of user VLANs that are allowed.

The **undo l2-multicast user-vlan limit** command restores the default configuration.

By default, 512 user VLANs can be configured.

Format

l2-multicast user-vlan limit *number*

undo l2-multicast user-vlan limit

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S.

Parameters

Parameter	Description	Value
number	Specifies the number of user VLANs that can be configured.	The value is an integer in the range from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

User VLANs and the Layer 3 VLANIF service share resources. Too large a number of user VLANs will affect the specification of VLANIF interfaces. You can run the **l2-multicast user-vlan limit** command to adjust the number of user VLANs that can be configured based on your service requirements.

Example

Set the number of user VLANs that can be configured to 300.

```
<HUAWEI> system-view
[HUAWEI] l2-multicast user-vlan limit 300
```

8.14.8 multicast flow-trigger enable

Function

The **multicast flow-trigger enable** command enables the triggering of multicast flows in a VLAN.

The **undo multicast flow-trigger enable** command disables the triggering of multicast flows in a VLAN.

By default, the triggering of multicast flows is disabled in VLANs.

Format

multicast flow-trigger enable

undo multicast flow-trigger enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user VLAN (for example, UVLAN) needs to join multiple multicast VLANs (for example, MVLAN1 to MVLAN*n*), you need to perform the following operations to ensure that N-to-N mappings based on {UVLAN, Source, Group} can be created between UVLANs and MVLANs and multicast entries can be generated when UVLANs send VOD requests to the MVLANs:

1. Run the **multicast flow-trigger enable** command in the UVLAN to enable triggering of multicast flows.

2. Run the **multicast-vlan user-vlan** command in each MVLAN to configure mappings between the UVLAN and MVLANs.
3. Run the **multicast static-flow** command in each MVLAN to configure a static flow.

Precautions

The **multicast flow-trigger enable** and **multicast-vlan enable** commands cannot be configured in the same VLAN.

Example

Enable the triggering of multicast flows in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] multicast flow-trigger enable
```

8.14.9 multicast static-flow

Function

The **multicast static-flow** command configures static flows in a multicast VLAN.

The **undo multicast static-flow** command deletes static flows from a multicast VLAN.

By default, no static flow is configured in multicast VLANs.

Format

multicast static-flow { *ipv4-group-address1* [**to** *ipv4-group-address2*] [**source** *ipv4-source-address*] | **ipv6** *ipv6-group-address1* [**to** *ipv6-group-address2*] [**source** *ipv6-source-address*] }

undo multicast static-flow { *ipv4-group-address1* [**to** *ipv4-group-address2*] [**source** *ipv4-source-address*] | **ipv6** *ipv6-group-address1* [**to** *ipv6-group-address2*] [**source** *ipv6-source-address*] | **all** }

Parameters

Parameter	Description	Value
ipv4-group-address1 [**to** *ipv4-group-address2*]	Specifies the IPv4 address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source *ipv4-source-address*	Specifies the source IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
ipv6 *ipv6-group-address1* [**to** *ipv6-group-address2*]	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
source *ipv6-source-address*	Specifies the source IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all static multicast flows in a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user VLAN (for example, UVLAN) needs to join multiple multicast VLANs (for example, MVLAN1 to MVLANn), you need to run the **multicast flow-trigger enable** command in the view of user VLAN to enable the triggering of multicast flows, and then configure static flows in each multicast VLAN. In this manner, the many-to-many mapping based on {UVLAN, Source, Group} is set up between user VLANs and multicast VLANs.

Precautions

Any two static flows in a multicast VLAN cannot be the same. Note that flows of the same multicast group with different source IP addresses are considered as different flows.

When you use the **multicast static-flow** { *ipv4-group-address1* **to** *ipv4-group-address2* | *ipv6-group-address1* **to** *ipv6-group-address2* } command to configure static multicast flows in batches, a maximum of 256 flows can be configured each time. When configuring an IPv4 multicast address segment, ensure that the consecutive addresses are in a multicast address segment with a 24-bit mask. When configuring an IPv6 multicast address segment, ensure that the consecutive addresses are in a multicast address segment with a 120-bit prefix. For example, the **multicast static-flow 225.0.0.255 to 225.0.1.1** command will not take effect because the addresses belong to two different segments: 225.0.0.0/24 and 225.0.1.0/24.

Example

Configure a static flow with the source address being 10.0.0.1 and group address being 232.0.0.1 in multicast VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] igmp-snooping version 3
[HUAWEI-vlan10] multicast-vlan enable
[HUAWEI-vlan10] multicast static-flow 232.0.0.1 source 10.0.0.1
```

Configure a static flow with the source address being FE80::1 and group address being FF23::123 in multicast VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan 20
[HUAWEI-vlan20] mld-snooping enable
[HUAWEI-vlan20] mld-snooping version 2
[HUAWEI-vlan20] multicast-vlan enable
[HUAWEI-vlan20] multicast static-flow ipv6 ff23::123 source fe80::1
```

8.14.10 multicast-vlan enable

Function

The **multicast-vlan enable** command configures a VLAN as a multicast VLAN.

The **undo multicast-vlan enable** command restores the default configuration.

By default, a VLAN is a common VLAN.

Format

multicast-vlan enable

undo multicast-vlan enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a switch needs to replicate multicast packets for each VLAN when users in different VLANs need to receive multicast data from the same multicast source. If a multicast VLAN is configured and the VLANs that users belong to are configured as the user VLANs of the multicast VLAN, the switch only needs to replicate the multicast data for the multicast VLAN. Multicast data is then replicated to the user VLANs by the multicast VLAN. This reduces load on the upstream router and separates the multicast source from the users.

Prerequisites

IGMP snooping or MLD snooping has been enabled in a VLAN using the **igmp-snooping enable (VLAN view)** or **mld-snooping enable** command.

Follow-up Procedure

Run the **multicast-vlan user-vlan** command to bind user VLANs to the multicast VLAN.

Precautions

- A multicast VLAN cannot be configured as a user VLAN. A user VLAN cannot be configured as a multicast VLAN.
- If MAC address-based forwarding is configured using the **l2-multicast forwarding-mode** command in a VLAN, the VLAN cannot be configured as a multicast VLAN.
- Before running the **undo multicast-vlan enable** command in a multicast VLAN, delete all the user VLANs from the multicast VLAN. If OAM is bound to the multicast VLAN, unbind OAM from the multicast VLAN first.
- The **multicast flow-trigger enable** and **multicast-vlan enable** commands cannot be configured in the same VLAN.

Example

Configure VLAN 2 as a multicast VLAN.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] multicast-vlan enable
```

8.14.11 multicast-vlan send-query prune-source-port

Function

The **multicast-vlan send-query prune-source-port** command prevents the upstream interface from sending Query messages received in a multicast VLAN back to upstream devices through user VLANs.

The **undo multicast-vlan send-query prune-source-port** command restores the default configuration.

By default, an upstream interface can send Query messages received in a multicast VLAN back to upstream devices through user VLANs.

Format

multicast-vlan send-query prune-source-port

undo multicast-vlan send-query prune-source-port

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In multicast VLAN application, an upstream interface usually belongs to a multicast VLAN and user VLANs bound to the multicast VLAN. By default, an upstream interface can send Query messages received in a multicast VLAN back to upstream devices through user VLANs.

To prevent Query messages from being sent back to upstream devices, run this command in the multicast VLAN.

Prerequisites

The multicast VLAN function has been enabled using the **multicast-vlan enable** command in the VLAN view.

Example

Prevent the upstream interface from sending Query messages received in multicast VLAN 10 back to upstream devices through user VLANs.

```
<HUAWEI> system-view
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] multicast-vlan enable
[HUAWEI-vlan10] multicast-vlan send-query prune-source-port
```

8.14.12 multicast-vlan user-vlan

Function

The **multicast-vlan user-vlan** command binds user VLANs to a multicast VLAN.

The **undo multicast-vlan user-vlan** command unbinds user VLANs from a multicast VLAN.

By default, a multicast VLAN does not have any user VLAN.

Format

multicast-vlan user-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo multicast-vlan user-vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies IDs of the user VLANs. - *vlan-id1* specifies the start VLAN ID. - *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs. If **to** *vlan-id2* is not specified, only one user VLAN is bound to the multicast VLAN.	The settings of the parameters are as follows: - The value of *vlan-id1* is an integer that ranges from 1 to 4094. - The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all the user VLANs from a multicast VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring a multicast VLAN, you can use the **multicast-vlan user-vlan** command to bind user VLANs to the multicast VLAN. The Layer 3 device replicates multicast data only in the multicast VLAN and sends the multicast data to the Layer 2 device. This saves bandwidth and reduces load on the Layer 3 device because it does not need to replicate multicast data in every user VLAN.

Prerequisites

- Before running this command, run the **igmp-snooping enable** or **mld-snooping enable** command to enable IGMP snooping or MLD snooping globally, in the user VLANs, and in the multicast VLAN.
- Before running this command, run the **multicast-vlan enable** command to enable the multicast VLAN function in the multicast VLAN.

Precautions

- A user VLAN cannot be configured as a multicast VLAN.
- The user VLANs must exist.
- For the S6720-EI, S6735-S, and S6720S-EI, if the received multicast packets carry double VLAN tags, the inner VLAN tag will be removed and the double VLAN tags will be replaced with a single user VLAN tag when the multicast-vlan user-vlan command is run to bind user VLANs to the multicast VLAN.

Example

Bind user VLAN 10 to multicast VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 2 10
[HUAWEI] igmp-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] vlan 2
[HUAWEI-vlan2] igmp-snooping enable
[HUAWEI-vlan2] multicast-vlan enable
[HUAWEI-vlan2] multicast-vlan user-vlan 10
```

Bind user VLANs 3 to 10 to multicast VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 2 to 10
[HUAWEI] igmp-snooping enable
[HUAWEI] igmp-snooping enable vlan 2 to 10
[HUAWEI] vlan 2
[HUAWEI-vlan2] multicast-vlan enable
[HUAWEI-vlan2] multicast-vlan user-vlan 3 to 10
```

8.15 Controllable Multicast Configuration Commands

8.15.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.15.2 add multicast-group

Function

The **add multicast-group** command adds multicast groups to a multicast group list.

The **undo add multicast-group** command removes multicast groups from a multicast group list.

By default, no multicast group is contained in a multicast group list.

Format

add multicast-group { **name** *group-name* | **index** *start-index* **to** *end-index* }

undo add multicast-group { **name** *group-name* | **index** *start-index* **to** *end-index* }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a multicast group.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast group. *start-index* specifies the start index of a multicast group, and *end-index* specifies the end index of a multicast group.	The value is an integer that ranges from 1 to 1024.

Views

Multicast group list view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group is at the lowest level of the three-level control mechanism for controllable multicast. A multicast group corresponds to a multicast address such as 224.1.1.1. A multicast group can be regarded as a channel or program of IPTV. When configuring controllable multicast, you must create a multicast group and add the group to a multicast group list.

Prerequisites

The specified multicast group has been created.

Example

Add the multicast group named **test** to the multicast group list **list1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group test ip-address 225.1.1.1
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1] add multicast-group name test
```

Add the multicast groups whose indexes range from 2 to 4 to the multicast group list **list1**.

```
<HUAWEI> system-view
[HUAWEI] btv
```

```
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1] add multicast-group index 2 to 4
```

8.15.3 add multicast-list

Function

The **add multicast-list** command adds multicast group lists in a multicast profile.

The **undo add multicast-list** command removes multicast group lists from a multicast profile.

By default, no multicast group list is referenced in a multicast profile.

Format

add multicast-list { **name** *list-name* | **index** *start-index* **to** *end-index* } { **preview** | **watch** }

undo add multicast-list { **name** *list-name* | **index** *start-index* **to** *end-index* }

Parameters

Parameter	Description	Value
name *list-name*	Indicates the name of a multicast group list.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast group list. *start-index* specifies the start index of a multicast group list, and *end-index* specifies the end index of a multicast group list.	The value is an integer that ranges from 1 to 128.
preview	Indicates that multicast group lists are added to a multicast profile in preview mode. Users applying this profile can preview all programs in the multicast group lists.	-
watch	Indicates that multicast group lists are added to a multicast profile in watch mode. Users applying this profile can watch all programs in the multicast group lists.	-

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group list is in the middle of the three-level control mechanism for controllable multicast, and is a set of multicast groups. A multicast group list can contain multiple multicast groups. For example, multicast group list l1 contains g1, g2, g3, and g4. A multicast group can be contained in multiple multicast group lists. For example, g3 is contained in l1 and l2. When you configure controllable multicast, you must add the multicast group list to a multicast profile.

Prerequisites

The specified multicast group list has been created.

Example

Reference the multicast group list named **list1** in the multicast profile **profile1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1] quit
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] add multicast-list name list1 watch
```

Reference the multicast group lists with indexes 1 to 10 in the multicast profile **profile1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] add multicast-list index 1 to 10 watch
```

8.15.4 attach multicast-profile

Function

The **attach multicast-profile** command binds a multicast profile to a user.

The **undo attach multicast-profile** command cancels the binding between a multicast profile and a user.

By default, no multicast profile is bound to a user.

Format

attach multicast-profile *profile-name* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *

undo attach multicast-profile [*profile-name* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a multicast profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.
interface *interface-type interface-number*	Specifies a user interface. *interface-type* specifies the type of the user interface. *interface-number* specifies the number of the user interface.	-
mac-address *mac-address*	Specifies the MAC address of a user host.	The MAC address is in the format of H-H-H. Each H stands for four hexadecimal numbers.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traditional multicast services are uncontrollable. User hosts send IGMP/MLD Report packets to join a specified multicast group. Then they can receive multicast packets of the group. With the development of IPTV services, uncontrollable multicast services cannot meet carriers' requirements. You can configure controllable multicast to authenticate user rights in the VLAN that join a multicast group. The controllable multicast function authenticates users in a VLAN that need to join a multicast group using the multicast group, multicast group list, and multicast profile. After a multicast profile is configured, bind this profile to a VLAN. When a user host sends a request to join a channel, the request is snooped if the channel requested by the user host is not in the multicast profile.

Prerequisites

The specified multicast profile has been created.

Precautions

The switch supports the port+VLAN multicast control mode. To configure the multicast service for multiple user interfaces in the same VLAN, you need to specify a multicast profile for each interface individually by specifying the **interface** *interface-type interface-number* parameter.

Example

Bind **profile1** to the user with the MAC address being 1-2-3 on GE0/0/1 in VLAN 4.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] quit
[HUAWEI-btv] quit
[HUAWEI] vlan 4
[HUAWEI-vlan4] attach multicast-profile profile1 interface gigabitethernet 0/0/1 mac-address 1-2-3
```

8.15.5 btv

Function

The **btv** command enables controllable multicast and displays the BTV view.

The **undo btv** command disables controllable multicast and deletes all configurations in the BTV view.

By default, controllable multicast is disabled.

Format

btv

undo btv

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **btv** command allows you to configure controllable multicast in the BTV view.

NOTICE

The **undo btv** deletes all the controllable multicast configurations. Exercise caution when you run this command.

Example

Enter the BTV view.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv]
```

8.15.6 display multicast-group

Function

The **display multicast-group** command displays the configuration of a multicast group.

Format

display multicast-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a multicast group.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display multicast-group** command, you can view details about a specified multicast group, if *group-name* is specified. Otherwise, you can view brief information about all multicast groups.

Example

Display brief information about all multicast groups.

```
<HUAWEI> display multicast-group
--------------------------------------------------------------------------
 Index       Multicast-group-name             Address
 --------------------------------------------------------------------------
  1          g1                               232.0.0.1[10.1.1.1]
  2          g2                               232.0.0.2[10.2.1.1]

 Total: 2
```

Display details about the multicast group named **g1**.

```
<HUAWEI> display multicast-group g1
 Multicast-group-name        : g1
 Address                     : 232.0.0.1[10.1.1.1]
 Referenced list :
        l1

 Total: 1
```

Table 8-152 Description of the **display multicast-group** command output

Item	Description
Index	Index of a multicast group
Multicast-group-name	Name of a multicast group
Address	Multicast group and source address
Referenced list	Multicast group list that a multicast group is added to
Total	Total number of multicast groups

8.15.7 display multicast-list

Function

The **display multicast-list** command displays the configuration of a multicast group list.

Format

display multicast-list [*list-name*]

Parameters

Parameter	Description	Value
list-name	Specifies the name of a multicast group list.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify the name of a multicast group list in the **display multicast-list** command, detailed information about the specified multicast group list is displayed. If you do not specify a multicast group list in the command, the summary information about all multicast group lists is displayed.

Example

Display brief information about all multicast group lists.

```
<HUAWEI> display multicast-list
 -------------------------------------------------------------------------
 Index        Multicast-list-name             Multicast-group
 -------------------------------------------------------------------------
  1            l1                                    2

 Total: 1
```

Display details about the multicast group list named **l1**.

```
<HUAWEI> display multicast-list l1
 Multicast-list-name : l1

 Referenced multicast-group  (Total: 2)
        g1                           232.0.0.1[10.1.1.1]
        g2                           232.0.0.2[10.2.1.1]

 Referenced multicast-profile  (Total: 2)
        p1                           [w]
        p2                           [w]
```

Table 8-153 Description of the **display multicast-list** command output

Item	Description
Index	Index of a multicast group list.
Multicast-list-name	Name of a multicast group list.
Multicast-group	Number of multicast groups contained in a multicast group list.
Referenced multicast-group	Multicast groups contained in a multicast group list. For example, g1 and 232.0.0.1 are the name and address of the multicast group, while 10.1.1.1 is a multicast source address.
Referenced multicast-profile	Profile that a multicast group list is added to. p1 is the name of the multicast profile. [w] means that the profile is in watching state, and [p] indicates that the profile is in preview state.

Item	Description
Total	- The first **Total** field indicates the total number of multicast group lists. - The second **Total** field indicates the number of multicast groups in the specified multicast group list. - The third **Total** field indicates the number of multicast profiles that references the multicast group list.

8.15.8 display multicast-profile

Function

The **display multicast-profile** command displays information about multicast profile.

Format

display multicast-profile [*profile-name* [**verbose**]]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a multicast profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.
verbose	Indicates detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify *profile-name*, this command displays information about a specified multicast profile. If you do not specify *profile-name*, this command displays brief information about all multicast profiles.

Example

Display brief information about all multicast profiles.

```
<HUAWEI> display multicast-profile
 ---------------------------------------------------------------------------
 Index       Profile-Name                      Multicast-list  Attach-User
 ---------------------------------------------------------------------------
  1          p1                                1             2
  2          p2                                2             2

 Total: 2
```

Display detailed information about the multicast profile **p1**.

```
<HUAWEI> display multicast-profile p1 verbose
 Profile-name : p1
 Referenced multicast-group  (Total: 2)
       g1                              225.0.0.1        [w]
       g2                              225.0.0.2        [w]
```

Table 8-154 Description of the **display multicast-profile** command output

Item	Description
Index	Index of a multicast profile.
Profile-Name	Name of the multicast profile.
Multicast-list	Number of multicast group lists contained in the multicast profile.
Attach-User	Number of user VLANs that the multicast profile is bound to.
Referenced multicast-group	Number of multicast groups in the multicast profile. In this example, g1 is the multicast group name, 225.0.0.1 is the group address. [w] means that the profile is in watching state, and [p] indicates that the profile is in preview state.
Total	● The first **Total** field indicates the total number of multicast profiles. ● The second **Total** field indicates the number of multicast groups in the specified multicast profile.

8.15.9 display multicast-profile-apply

Function

The **display multicast-profile-apply** command displays bindings between multicast profiles and VLANs.

Format

display multicast-profile-apply

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the multicast profiles applied to different VLANs.

Example

Display bindings between multicast profiles and VLANs on the switch.

```
<HUAWEI> display multicast-profile-apply
-----------------------------------------------------------------------------
 Vlan-id  Port                   SMAC                          Max-Users
                Index              Profile-name
 -----------------------------------------------------------------------------
 Vlan1    --                    --                            8
                 1                 p1
 Vlan2    --                    --                            8
                 1                 p1
 Vlan3    --                    --                            8
                 2                 p2
 Vlan4    --                    --                            8
                 2                 p2

 Total: 4
```

Table 8-155 Description of the **display multicast-profile-apply** command output

Item	Description
Vlan-id	ID of a VLAN bound to a multicast profile.
Port	Interface in the VLAN. -- indicates that no interfaces are bound to the multicast profile in this VLAN.
Index	Index of a multicast profile.
SMAC	MAC address of a user. -- indicates that no user hosts are bound to the multicast profile in this VLAN.
Profile-name	Name of a multicast profile.

Item	Description
Max-Users	Maximum number of programs that users can watch and preview at the same time. If the value is set in a VLAN and the multicast profile bound to the VLAN, only the configuration in the VLAN takes effect. If the value is not set in a VLAN: ● The configuration in the multicast profile takes effect if the VLAN is bound to only one multicast profile. ● The default value 8 is used if the VLAN is bound to multiple multicast profiles.
Total	Total number of binding entries between VLANs and multicast profiles.

8.15.10 max-program-num (multicast profile view)

Function

The **max-program-num** command sets the maximum number of programs that users can receive simultaneously.

The **undo max-program-num** command restores the maximum number of programs for a user to the default value.

By default, users can receive a maximum of 8 programs simultaneously.

Format

max-program-num *max-value*

undo max-program-num [*max-value*]

Parameters

Item	Description	Value
max-value	Indicates the maximum number of programs that users can receive simultaneously.	The value ranges from 1 to 8.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Run the **max-program-num (VLAN view)** command in the VLAN view to set the maximum number of multicast groups that users can simultaneously join. If the value is set in a VLAN and the multicast profile bound to the VLAN, only the configuration in the VLAN takes effect. If the value is not set in a VLAN:

- The configuration in the multicast profile takes effect if the VLAN is bound to only one multicast profile.
- The default value 8 is used if the VLAN is bound to multiple multicast profiles.

Example

Set the maximum number of programs that multicast profile **p1** allows users to receive simultaneously to 4.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile p1
[HUAWEI-btv-profile-p1] max-program-num 4
```

8.15.11 max-program-num (VLAN view)

Function

The **max-program-num** command sets the maximum number of programs that users can receive simultaneously.

The **undo max-program-num** command restores the maximum number of programs for a user to the default value.

By default, users can receive a maximum of 8 programs simultaneously.

Format

max-program-num *max-value* [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *

undo max-program-num [**interface** *interface-type interface-number* | **mac-address** *mac-address*] *

Parameters

Item	Description	Value
max-value	Indicates the maximum number of programs that users can receive simultaneously.	The value ranges from 1 to 8.

Item	Description	Value
interface *interface-type interface-number*	Indicates the maximum number of programs that users on a specified interface can watch simultaneously.	-
mac-address *mac-address*	Indicates the maximum number of programs that users with specified MAC addresses can watch simultaneously.	The value is in H-H-H format, in which H is a 4-digit hexadecimal number.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Run the **max-program-num (multicast profile view)** command in the multicast profile view to set the maximum number of multicast groups that users can simultaneously join. If the value is set in a VLAN and the multicast profile bound to the VLAN, only the configuration in the VLAN takes effect. If the value is not set in a VLAN:

- The configuration in the multicast profile takes effect if the VLAN is bound to only one multicast profile.
- The default value 8 is used if the VLAN is bound to multiple multicast profiles.

The **interface** *interface-type interface-number* and **mac-address** *mac-address* parameters specified in the command must be the same as those specified in the **attach multicast-profile** command.

Example

Allow users in VLAN 10 to watch four programs simultaneously.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] max-program-num 4
```

8.15.12 multicast-group

Function

The **multicast-group** command creates a controllable multicast group.

The **undo multicast-group** command deletes a controllable multicast group.

By default, no multicast group is created.

Format

multicast-group *group-name* { **ip-address** *ipv4-group-address* [**source** *ipv4-source-address*] | **ipv6-address** *ipv6-group-address* [**source** *ipv6-source-address*] }

undo multicast-group { **all** | *group-name* | **index** *start-index* **to** *end-index* }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a multicast group.	The value is a string of 1 to 31 case-insensitive characters without spaces.
ip-address *ipv4-group-address*	Specifies the address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
source *ipv4-source-address*	Specifies an IPv4 source address.	It is in dotted decimal notation.
ipv6-address *ipv6-group-address*	Specifies an IPv6 multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, excluding the multicast addresses reserved for protocols.
source *ipv6-source-address*	Specifies an IPv6 source address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all multicast groups.	-
index *start-index* **to** *end-index*	Specifies the index of a multicast group. *start-index* specifies the start index of a multicast group, and *end-index* specifies the end index of a multicast group.	The value is an integer that ranges from 1 to 1024.

Views

Broadband TV (BTV) view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group is at the lowest level of the three-level control mechanism for controllable multicast. A multicast group corresponds to a multicast address such as 224.1.1.1. A multicast group can be regarded as a channel or program of IPTV.

Precautions

If two programs have the same multicast IP address but different source addresses, the two programs are considered different.

Example

Configure the IP address of a multicast group to 225.0.0.1 and name the multicast program **tv-1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group tv-1 ip-address 225.0.0.1
```

Configure the IP address of a multicast group to ff1e::1234 and name the multicast program **tv-2**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group tv-2 ipv6-address ff1e::1234
```

Configure the IP address of a multicast group to 232.0.0.1, specify the source IP address to 192.168.1.1, and name the multicast program **tv-3**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-group tv-3 ip-address 232.0.0.1 source 192.168.1.1
```

8.15.13 multicast-list

Function

The **multicast-list** command creates a multicast group list.

The **undo multicast-list** command deletes a multicast group list.

By default, no multicast group list is configured.

Format

multicast-list *list-name*

undo multicast-list { *list-name* | **index** *start-index* **to** *end-index* | **all** }

Parameters

Parameter	Description	Value
list-name	Specifies the name of a multicast group list.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast group list. *start-index* specifies the start index of a multicast group, and *end-index* specifies the end index of a multicast group.	The value is an integer that ranges from 1 to 128.
all	Deletes all multicast group lists.	-

Views

BTV view

Default Level

2: Configuration level

Usage Guidelines

A multicast group list is in the middle of the three-level control mechanism for controllable multicast, and is a set of multicast groups. A multicast group list can contain multiple multicast groups. For example, multicast group list L1 contains G1, G2, G3, and G4. A multicast group can be contained in multiple multicast group lists. For example, G3 is contained in L1 and L2. When you configure controllable multicast, you must add the multicast group list to a multicast profile.

Using the **multicast-list** command, you can create a multicast group list and enter the multicast group list view. If a multicast group list is already created, you can directly enter the multicast group list view.

Example

Create the multicast group list named **list1**.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-list list1
[HUAWEI-btv-list-list1]
```

8.15.14 multicast-preview interval

Function

The **multicast-preview interval** command sets the interval between the first and second previews on a multicast group.

The **undo multicast-preview interval** command restores the default interval between the first and second previews on a multicast group.

By default, the interval between the first and second previews on a multicast group is 5 minutes.

Format

multicast-preview interval *interval*

undo multicast-preview interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval between the first and second previews on a multicast group.	The value is an integer that ranges from 1 to 30, in minutes.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Controllable multicast allows users to preview programs. The **multicast-preview interval** command sets the interval between the first and second previews. Users can preview the same program after this interval.

Example

Set the interval between the first and second previews on a multicast profile named **profile1** to 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] multicast-preview interval 15
```

8.15.15 multicast-preview minutes

Function

The **multicast-preview minutes** command sets the period for a user to preview a multicast group each time.

The **undo multicast-preview minutes** command restores the default preview period.

By default, the period for a user to preview a multicast group each time is 5 minutes.

Format

multicast-preview minutes *minutes*

undo multicast-preview minutes [*minutes*]

Parameters

Parameter	Description	Value
minutes	Specifies the period for a user to preview a multicast group each time.	The value is an integer that ranges from 1 to 10, in minutes.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Controllable multicast allows users to preview programs. The **multicast-preview minutes** command sets the period for a user to preview a multicast group. Users are not allowed to preview the program after the configured period is reached.

Example

Set the period for previewing the multicast profile named **profile1** each day to 9 minutes.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] multicast-preview minutes 9
```

8.15.16 multicast-preview times

Function

The **multicast-preview times** command sets the number of times for a user to preview a multicast group each day.

The **undo multicast-preview times** command restores the default number of previews each day.

By default, the number of times a user can preview a multicast group each day is 10.

Format

multicast-preview times *times*

undo multicast-preview times [*times*]

Parameters

Parameter	Description	Value
times	Specifies the number of times for a user to preview a multicast group each day.	The value is an integer that ranges from 1 to 10.

Views

Multicast profile view

Default Level

2: Configuration level

Usage Guidelines

Controllable multicast allows users to preview programs. The **multicast-preview times** command sets the number of times for a user to preview a multicast group each day.

Example

Set the number of times for a user to preview the multicast profile named **profile1** each day to 8.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1] multicast-preview times 8
```

8.15.17 multicast-profile

Function

The **multicast-profile** command creates a multicast profile and enters the multicast profile view. If a multicast profile is already created, you can directly enter the multicast profile view.

The **undo multicast-profile** command deletes a multicast profile.

By default, no multicast profile is configured.

Format

multicast-profile *profile-name*

undo multicast-profile { *profile-name* | **index** *start-index* **to** *end-index* | **all** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a multicast profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.
index *start-index* **to** *end-index*	Specifies the index of a multicast profile. *start-index* specifies the start index of a multicast profile, and *end-index* specifies the end index of a multicast profile.	The value is an integer that ranges from 1 to 64.
all	Deletes all multicast profiles.	-

Views

BTV view

Default Level

2: Configuration level

Usage Guidelines

A multicast profile is a set of multicast group lists, and it defines user rights to join related multicast groups. A multicast profile can contain multiple multicast group lists. For example, multicast profile P1 contains L1, L2, and L3. A multicast group list can be contained in several multicast profiles. For example, L2 is contained in

P1 and P2. Multicast group lists that are added to a profile have their attributes, that is, preview or watch. If a multicast group list is added to a multicast profile in watch mode, users bound to the multicast profile can watch all multicast groups in the list. If a multicast group list is added to a multicast profile in preview mode, users bound to the multicast profile can only preview all multicast groups in the list.

Example

Create the multicast profile named **profile1** and enter the multicast profile view.

```
<HUAWEI> system-view
[HUAWEI] btv
[HUAWEI-btv] multicast-profile profile1
[HUAWEI-btv-profile-profile1]
```

8.16 Multicast Network Management Commands

8.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

8.16.2 display multicast threshold-alarm

Function

The **display multicast threshold-alarm** command displays the alarm thresholds for multicast entry resource usage.

Format

display multicast threshold-alarm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the alarm thresholds for multicast entry resource usage.

Example

Display the alarm thresholds for multicast entry resource usage.

```
<HUAWEI> display multicast threshold-alarm
Multicast table trap threshold value
Upperlimit value: 86%
Lowerlimit value: 78%
```

Table 8-156 Description of the **display multicast threshold-alarm** command output

Item	Description
Multicast table trap threshold value	Alarm thresholds for multicast entry resource usage.
Upperlimit value	Upper threshold value. This parameter is configured using the **multicast threshold-alarm upper-limit** *upper-limit* **lower-limit** *lower-limit* command.
Lowerlimit value	Lower threshold value. This parameter is configured using the **multicast threshold-alarm upper-limit** *upper-limit* **lower-limit** *lower-limit* command.

8.16.3 display pim mib-control-message

Function

The **display pim mib-control-message** command displays PIM-related statistics and counts of various messages received the last time.

Format

display pim mib-control-message { **counters** | **join-prune** | **assert** | **register** }

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
counters	Indicates related PIM counters.	-

Parameter	Description	Value
join-prune	Indicates the number of invalid Join/Prune messages that are received at the last time.	-
assert	Indicates the number of Assert messages that are received or sent at the last time.	-
register	Indicates the number of invalid Register messages that are received at the last time.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim mib-control-message counters** command displays the number of neighbor loss events, the number of DR elections, the number of invalid Join/Prune messages, the number of invalid Register messages, the number of RP-mapping changes, and the number of received and sent Assert messages.

The **display pim mib-control-message join-prune** command displays the source address, group address, and RP address carried in the last received invalid Join/Prune message.

The **display pim mib-control-message assert** command displays the source address and group address carried in the last received or sent Assert message.

The **display pim mib-control-message register** command displays the source address, group address, and RP address carried in the last received invalid Register message.

Example

Display the number of neighbor loss events, the number of times for DR election, the number of invalid Join/Prune messages, the number of invalid Register messages, the number of RP-Mapping, the number of received and sent Assert messages.

```
<HUAWEI> display pim mib-control-message counters
 pim mib-control-message counters
 Neighbor-loss (times)        : 0
 DR-Election(times)          : 0
 Invalid-join-prune (times)   : 0
 RP-Mapping (times)           : 0
 Invalid-register (times)     : 0
 Assert-received(times)      : 0
 Assert-send(times)          : 0
```

Display the invalid Join/Prune message that is received at the last time.

```
<HUAWEI> display pim mib-control-message join-prune
The last invalid join-prune message received information:
Group address  : 225.1.1.1
Source address : 0.0.0.0
RP address     : 10.0.5.5
```

Display the Assert message that is sent or received at the last time. If the interface that receives or sends the Assert message is pulled out when this command is used, the prompt that "The last assert message was received or sent on lost interface" is displayed.

```
<HUAWEI> display pim mib-control-message assert
The last assert message received or sent on Vlanif100
Group address   : 226.3.3.3
Source address  : 10.0.5.55
```

Display the invalid Register message that is received at the last time.

```
<HUAWEI> display pim mib-control-message register
The last invalid register message received information:
Group address  : 225.1.1.1
Source address : 10.0.5.100
RP address     : 10.0.3.1
```

Table 8-157 Description of the **display pim mib-control-message** command output

Item	Description
pim mib-control-message counters	Numbers of neighbor loss events, DR election events, invalid Join/Prune messages, invalid Register messages, RP-mapping changes, and received and sent Assert messages.
The last invalid join-prune message received information	Invalid Join/Prune message received the last time.
The last assert message received or sent on Vlanif100	Assert message sent or received the last time.
The last invalid register message received information	Invalid Register message received the last time.
Neighbor-loss(times)	Number of neighbor loss events.
DR-Election (times)	Number of DR election events.
Invalid-join-prune(times)	Number of invalid Join/Prune messages.
RP-Mapping(times)	Number of RP-Mapping changes.
Invalid-register(times)	Number of invalid Register messages.
Assert-received(times)	Number of received Assert messages.
Assert-send(times)	Number of sent Assert messages.
Group address	Multicast group address.
Source address	Multicast source address

Item	Description
RP address	IP address of the RP.

8.16.4 display pim mib-notification interval

Function

The **display pim mib-notification interval** command displays the interval for sending PIM notification messages.

Format

display pim mib-notification interval

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the interval for sending PIM notification messages is set or modified by using the **pim mib-notification interval** command, you can run the **display pim mib-notification interval** command to view the configured interval.

Example

Display the interval for sending PIM notification messages.

```
<HUAWEI> display pim mib-notification interval
Neighbor-loss notification interval      : 0 s
Invalid-join-prune notification interval : 50 s
RP-mapping-change notification interval  : 100 s
Interface-election notification interval : 2000 s
Invalid-register notification interval   : 60000 s
New-neighbor notification interval       : 0 s
Mrt-limit notification interval          : never
```

Table 8-158 Description of the **display pim mib-notification interval** command output

Item	Description
Neighbor-loss notification interval	Interval for sending the notification messages about the neighbor loss
Invalid-join-prune notification interval	Interval for sending the notification messages about invalid Join/Prune messages
RP-mapping-change notification interval	Interval for sending the notification messages about RP-mapping changes
Interface-election notification interval	Interval for sending the notification messages about interface election
Invalid-register notification interval	Interval for sending the notification messages about invalid Register messages
New-neighbor notification interval	Interval for sending trap messages about neighbor addition.
Mrt-limit notification interval	Interval for sending trap messages about the failure in joining multicast groups because the number of PIM entries reaches the upper limit.

8.16.5 igmp trap-interval limit

Function

The **igmp trap-interval limit** command configures the interval for sending trap messages on failures to join IGMP groups because the number of the IGMP entries exceeds the limit.

The **undo igmp trap-interval limit** command deletes the interval for sending trap messages on failures to join IGMP groups because the number of the IGMP entries exceeds the limit. When a group joining failure occurs, a trap message is sent immediately.

By default, a trap message is sent immediately when an IGMP group joining failure occurs because the number of the IGMP entries exceeds the limit.

Format

igmp trap-interval limit *min-interval*

undo igmp trap-interval limit

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
min-interval	Specifies the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

If the interval is set to 0, a trap message will be sent immediately when an IGMP group joining failure occurs because the number of the IGMP entries exceeds the limit; otherwise, the interval for sending such trap messages should be equal to or longer than the configured one.

Example

Set the interval for sending trap messages on failures to join IGMP groups because the number of the IGMP entries exceeds the limit to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] igmp trap-interval limit 50
```

8.16.6 mgmd total-number threshold-alarm

Function

The **mgmd total-number threshold-alarm** command sets the upper and lower alarm thresholds for IGMP/MLD entries.

The **undo mgmd total-number threshold-alarm** command restores the default alarm thresholds for IGMP/MLD entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

mgmd total-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mgmd total-number threshold-alarm

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for IGMP/MLD entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for IGMP/MLD entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of IGMP/MLD entries. After the number of IGMP/MLD entries reaches the maximum value, no more IGMP/MLD entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operation and maintenance, configure the upper and lower alarm thresholds for IGMP/MLD entries. IGMP/MLD entry alarms and clear alarms quickly notify you of IGMP/MLD entry usage. The **mgmd total-number threshold-alarm** command allows you to flexibly adjust the alarm thresholds for IGMP/MLD entries based on service requirements. Note that:

- If the proportion of existing IGMP/MLD entries to the maximum number reaches *upper-limit-value*, an IGMP/MLD entry alarm is reported for all VPN instances. This alarm is informational only and does not affect creation of new IGMP/MLD entries.

- If the proportion of existing IGMP/MLD entries to the maximum number falls below *lower-limit-value*, an IGMP/MLD entry clear alarm is reported for all VPN instances.

Prerequisites

This command only configures the alarm thresholds for IGMP/MLD entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name igmp trap-name** { **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** } command twice to enable the device to report IGMP/MLD entry alarms and clear alarms.

Precautions

If the **mgmd total-number threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for IGMP/MLD entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] mgmd total-number threshold-alarm upper-limit 88 lower-limit 77
```

8.16.7 mgmd host threshold-alarm

Function

The **mgmd host threshold-alarm** command configures the upper and lower alarm thresholds for the multicast entry usage of all instances on a user-side IGMP/MLD device.

The **undo mgmd host threshold-alarm** command restores the default upper and lower alarm thresholds.

By default, the upper and lower alarm thresholds are 80% and 75%, respectively.

Format

mgmd host { **star-group-number** | **source-group-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mgmd host { **star-group-number** | **source-group-number** } **threshold-alarm**

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
star-group-number	Enables you to configure the upper and lower alarm thresholds for the (*, G) entry usage of all instances.	-
source-group-number	Enables you to configure the upper and lower alarm thresholds for the (S, G) entry usage of all instances.	-
upper-limit *upper-limit-value*	Configures an upper alarm threshold for the multicast entry usage of all instances, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Configures a lower alarm threshold for the multicast entry usage of all instances, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user-side IGMP/MLD device has an upper limit for the number of multicast entries. When this upper limit is reached, the device cannot create new entries, so it will reject new multicast service requests. To resolve this issue and improve device maintenance, run the **mgmd host threshold-alarm** command to configure the upper and lower alarm thresholds for the multicast entry usage on a user-side IGMP/MLD device, enabling you to learn the multicast entry usage status. After the **mgmd host threshold-alarm** command is executed:

- When the value of *upper-limit-value* is reached, the device triggers a multicast entry usage alarm. Such an alarm is a notification only, and the device can still create new multicast entries before the multicast entry usage reaches 100%.
- When the multicast entry usage falls below the value specified by *lower-limit-value*, the device triggers a clear alarm for the multicast entry usage alarm.

Prerequisites

The **mgmd host threshold-alarm** command works with the **snmp-agent trap enable feature-name igmp trap-name** { **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhostsgthresholdexceed** | **hwmgmdhostsgthresholdexceedclear** } command. The former configures the upper and lower alarm thresholds, while the latter enables or disables the function to report alarms.

Precautions

If the **mgmd host threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

Example

Configure the upper and lower alarm thresholds for the (*, G) entry usage of all instances.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] mgmd host star-group-number threshold-alarm upper-limit 88 lower-limit 77
```

Configure the upper and lower alarm thresholds for the (S, G) entry usage of all instances.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] mgmd host source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

8.16.8 multicast forwarding-table source-group-number threshold-alarm

Function

The **multicast forwarding-table source-group-number threshold-alarm** command configures the upper and lower alarm thresholds for multicast forwarding entries.

The **undo multicast forwarding-table source-group-number threshold-alarm** command restores the default alarm thresholds for multicast forwarding entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

multicast forwarding-table source-group-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo multicast forwarding-table source-group-number threshold-alarm

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for multicast forwarding entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for multicast forwarding entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of multicast forwarding entries. After the number of multicast forwarding entries reaches the maximum value, no more multicast forwarding entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operations and maintenance, configure the upper and lower alarm thresholds for multicast forwarding entries. Multicast forwarding entry alarms and clear alarms quickly notify you of IGMP/MLD entry usage. The **multicast forwarding-table source-group-number threshold-alarm** command allows you to flexibly adjust the alarm thresholds for multicast forwarding entries based on service requirements. Note that:

- If the proportion of existing multicast forwarding entries to the maximum number reaches *upper-limit-value*, a multicast forwarding entry alarm is reported. This alarm is informational only and does not affect creation of new multicast forwarding entries.
- If the proportion of existing multicast forwarding entries to the maximum number falls below *lower-limit-value*, a multicast forwarding entry clear alarm is reported.

Prerequisites

This command only configures the alarm thresholds for multicast forwarding entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name mrm trap-name** { **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** } command twice to enable the device to report multicast forwarding entry alarms and clear alarms.

Precautions

If the **multicast forwarding-table source-group-number threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for multicast forwarding entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] multicast forwarding-table source-group-number threshold-alarm upper-limit
88 lower-limit 77
```

8.16.9 multicast mib-notification join-leave frequency

Function

The **multicast mib-notification join-leave frequency** command sets the maximum number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.

The **undo multicast mib-notification join-leave frequency** command restores the default number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.

By default, the system does not send any trap message when IGMP/MLD joining or leaving events occur.

Format

multicast mib-notification join-leave frequency *count*

undo multicast mib-notification join-leave frequency

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
count	Specifies the maximum number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.	The value is an integer that ranges from 0 to 240. The unit is in packets per second. The default value is 0.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

If network administrators need to know which receivers join or leave multicast groups in real time, run this command. The switch will send trap messages after receivers join or leave multicast groups.

Example

Set the maximum number of trap messages sent by the system per second to 30 when IGMP/MLD joining or leaving events occur.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] multicast mib-notification join-leave frequency 30
```

8.16.10 multicast-mib

Function

The **multicast-mib** command enables the multicast MIB and displays the multicast MIB view.

The **undo multicast-mib** command deletes all configurations in the multicast MIB view.

By default, the multicast MIB is not enabled.

Format

multicast-mib

undo multicast-mib

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **undo multicast-mib** command to delete all configurations in the multicast MIB view.

NOTICE

When using the **undo multicast-mib** command, you need to enter Y or N to confirm the action. This command will clear global multicast MIB configurations. So, use this command with caution.

Example

Enable multicast MIB and enter the multicast MIB view.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib]
```

8.16.11 multicast threshold-alarm

Function

The **multicast threshold-alarm** command configures an alarm threshold for the usage of multicast entry resources.

The **undo multicast threshold-alarm** command restores the default alarm threshold for the usage of multicast entry resources.

By default, the upper and lower alarm thresholds are 85% and 75% respectively.

Format

multicast threshold-alarm upper-limit *upper-limit* **lower-limit** *lower-limit*

undo multicast threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit*	Indicates the upper threshold for the usage of multicast entry resources.	The value is an integer that ranges from 2 to 100, in percentage.
lower-limit *lower-limit*	Indicates the lower threshold for the usage of multicast entry resources.	The value is an integer that ranges from (*upper-limit* - 10) to (*upper-limit* - 1), in percentage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Multicast packets are forwarded based on multicast forwarding entries no matter whether the Layer 2 or Layer 3 multicast mode is used. A high entries resource usage indicates that the switch has forwarded too many multicast packets and there is a heavy load on it. If the resources for multicast forwarding entries are used up, multicast packets cannot be forwarded.

After the alarm threshold is set, the switch sends a trap when entries resource usage reaches the threshold. You can monitor multicast entries resource usage. When entries resource usage reaches the upper threshold, the alarm 1.3.6.1.4.1.2011.5.25.227.2.1.8, 1.3.6.1.4.1.2011.5.25.227.2.1.10, or 1.3.6.1.4.1.2011.5.25.227.2.1.62 is generated, indicating that the entries resources will be used up. When entries resource usage falls below the lower threshold, the alarm 1.3.6.1.4.1.2011.5.25.227.2.1.9, 1.3.6.1.4.1.2011.5.25.227.2.1.11, or 1.3.6.1.4.1.2011.5.25.227.2.1.63 is generated, indicating that entries resource usage is restored to an acceptable range.

Example

Set the upper threshold to 80% and lower threshold to 70%.

```
<HUAWEI> system-view
[HUAWEI] multicast threshold-alarm upper-limit 80 lower-limit 70
```

8.16.12 pim mib-notification interval

Function

The **pim mib-notification interval** command sets the interval for sending trap messages about various PIM events.

The **undo pim mib-notification interval** command restores the default interval for sending trap messages about various PIM events.

By default, an alarm is generated only when a neighbor loss event or a neighbor addition event occurs. No alarm is generated when the other events occur.

Format

pim mib-notification interval { **interface-election-dr** *election-value* | **invalid-join-prune** *jp-value* | **invalid-register** *register-value* | **neighbor-loss** *loss-value* | **new-neighbor** *new-value* | **rp-mapping-change** *change-value* | **mrt-limit** *mrt-value* }

undo pim mib-notification interval { **all** | **interface-election-dr** | **invalid-join-prune** | **invalid-register** | **neighbor-loss** | **new-neighbor** | **rp-mapping-change** | **mrt-limit** }

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface-election-dr *election-value*	Specifies the minimum interval for sending trap messages about DR election.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 65535 seconds.
invalid-join-prune *jp-value*	Specifies the minimum interval for sending trap messages about invalid Join/Prune messages.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 65535 seconds.
invalid-register *register-value*	Specifies the minimum interval for sending trap messages about invalid Register messages.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 65535 seconds.
neighbor-loss *loss-value*	Specifies the minimum interval for sending trap messages about neighbor loss.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.
new-neighbor *new-value*	Specifies the minimum interval for sending trap messages about neighbor addition.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.
rp-mapping-change *change-value*	Specifies the minimum interval for sending trap messages about the RP-mapping change.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 65535 seconds.
mrt-limit *mrt-value*	Specifies the minimum interval for sending trap messages about the failure in joining multicast groups because the number of PIM entries reaches the upper limit.	The value is an integer that ranges from 10 to 65535, in seconds. By default, the value is 65535 seconds.

Parameter	Description	Value
all	Restore the default interval for PIM to send all trap messages.	-

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

The **pim mib-notification interval** command sets the interval for sending trap messages. When an event occurs but the period from when the last trap message was sent to the current time is shorter than the configured interval, the system does not send any trap message.

- If the default interval is 0, a trap message is sent immediately after an event occurs.
- If the default interval is 65535, no trap message is sent after an event occurs. In this case, run this command to adjust the interval to a smaller value so that a trap message can be sent after an event occurs.

Example

Set the interval for PIM to send trap messages about invalid Join/Prune messages.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] pim mib-notification interval invalid-join-prune 50
```

8.16.13 pim threshold-alarm

Function

The **pim threshold-alarm** command configures the upper and lower alarm thresholds for PIM entries.

The **undo pim threshold-alarm** command restores the default alarm thresholds for PIM entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

pim { **star-group-number** | **source-group-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo pim { **star-group-number** | **source-group-number** } **threshold-alarm**

NOTE

Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
star-group-number	Sets the alarm thresholds for PIM (*, G) entries.	-
source-group-number	Sets the alarm thresholds for PIM (S, G) entries.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold value for PIM entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold value for PIM entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of PIM entries. After the number of PIM entries reaches the maximum value, no more PIM entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operations and maintenance, configure the upper and lower alarm thresholds for PIM entries. PIM entry alarms and clear alarms quickly notify you of PIM entry usage. The **pim threshold-alarm** command allows you to adjust the alarm thresholds for PIM entries based on service requirements. Note that:

- If the proportion of existing PIM entries to the maximum number reaches *upper-limit-value*, a PIM entry alarm is reported. This alarm is informational only and does not affect creation of new PIM entries.
- If the proportion of existing PIM entries to the maximum number falls below *lower-limit-value*, a PIM entry clear alarm is reported.

Prerequisites

This command only configures the alarm thresholds for PIM entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name pim trap-name** { **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** } command twice to enable the device to report PIM entry alarms and clear alarms.

Precautions

If the **pim threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for PIM (*, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] pim star-group-number threshold-alarm upper-limit 88 lower-limit 77
```

Configure the upper and lower alarm thresholds for PIM (S, G) entries.

```
<HUAWEI> system-view
[HUAWEI] multicast-mib
[HUAWEI-mcast-mib] pim source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

9 MPLS Configuration Commands

9.1 Basic MPLS Configuration Commands

9.1.1 Command Support

Only the following switch models support MPLS:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

9.1.2 authentication exclude

Function

The **authentication exclude** command configures LDP peers in a batch that a local device does not authenticate after LDP keychain or LDP MD5 is configured to authenticate all LDP peers or LDP peers in a specified group.

The **undo authentication exclude** command enables a local device to authenticate all LDP peers using LDP keychain or LDP MD5.

By default, a local device is enabled to authenticate all LDP peers using LDP keychain or LDP MD5.

Format

authentication exclude peer *peer-id*

undo authentication exclude peer *peer-id*

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the ID of an LDP peer.	This value is in dotted decimal notation.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a local device is enabled to authenticate all LDP peers using LDP keychain or LDP MD5 after LDP keychain or LDP MD5 is configured for a peer group or all LDP peers. To disable the local device from authenticating some LDP peers, run the **authentication exclude** command.

Precautions

The following commands are mutually exclusive for a specified LDP peer:

- **authentication key-chain peer** *peer-id* **name** *keychain-name*
- **md5-password** { **plain** | **cipher** } *peer-lsr-id password*

Example

Disable a local device from authenticating an LDP peer with IP address **10.1.1.1** after LDP keychain or MD5 is configured for all LDP peers or LDP peers in a specified group.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication exclude peer 10.1.1.1
```

9.1.3 authentication key-chain

Function

The **authentication key-chain** command enables Label Distribution Protocol (LDP) keychain authentication.

The **undo authentication key-chain** command disables Label Distribution Protocol (LDP) keychain authentication.

By default, LDP keychain authentication is disabled.

Format

authentication key-chain peer *peer-id* **name** *keychain-name*

undo authentication key-chain peer *peer-id*

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the ID of an LDP peer enabled with LDP keychain. The parameter is specified in the **mpls lsr-id** command.	The value is in dotted decimal notation.
name *keychain-name*	Specifies the keychain name. The keychain name is specified in the **keychain** command.	The value is an existing keychain name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Information spoofing may occur during an LDP session. To enhance security of an LDP session, configure keychain authentication for a TCP connection over which an LDP session is created.

During keychain authentication, a group of passwords are defined to form a password string, and each password is specified with the encryption and decryption algorithms such as MD5 and SHA-1, and is configured with a validity period. When sending or receiving a packet, the system selects a valid password based on the user's configuration. Within the password validity period, the system either uses the encryption algorithm matching the password to encrypt the packet before sending it or uses the decryption algorithm matching the password to decrypt the packet before receiving it. In addition, the system automatically uses a new password after the previous one expires, preventing the password from being decrypted.

The keychain authentication password, the encryption and decryption algorithms, and password validity period that construct a keychain configuration node are configured using different commands. A keychain configuration node requires at least one password along with encryption and decryption algorithms.

To reference a keychain configuration node, specify the required peer and the node name in the MPLS-LDP view. In this manner, an LDP session is encrypted. Different peers can reference the same keychain configuration node.

Keychain authentication involves a set of passwords. It uses a new password when the previous one expires. Keychain authentication is complex to configure and is therefore recommended only for networks requiring high security.

Prerequisites

You have performed the following operations:

- Enable MPLS LDP globally using the **mpls ldp (system view)** command.
- Configure keychain authentication globally using the **keychain** command.

Precautions

- MD5 authentication and keychain authentication cannot be configured together on one peer.
- Configuring LDP keychain authentication leads to reestablishment of an LDP session and deletes the Label Switched Path (LSP) associated with the LDP session.

Example

Configure LDP keychain authentication for the peer with an LSR ID of **10.1.1.1**. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain peer 10.1.1.1 name kc1
```

9.1.4 authentication key-chain all

Function

The **authentication key-chain all** command enables keychain authentication in a batch for all LDP peers.

The **undo authentication key-chain all** command disables keychain authentication in a batch for all LDP peers.

By default, keychain authentication in a batch is disabled for all LDP peers. LDP keychain authentication is recommended to ensure security.

Format

authentication key-chain all name *keychain-name*

undo authentication key-chain all

Parameters

Parameter	Description	Value
name *keychain-name*	Specifies a keychain name. The keychain name is configured using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. The string does not contain question marks or spaces. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve LDP session security, keychain authentication can be configured for a TCP connection over which an LDP session has been established. If a great number of LDP peers are configured, run the **authentication key-chain all** command to enable keychain authentication in a batch for all LDP peers.

Prerequisites

A keychain has been configured using the **keychain** command.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1. Keychain authentication takes effect on other peers.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.
- After the **authentication key-chain all** command is run, the referenced keychain is applied to all LDP peers. If keychain authentication fails, an LDP session fails to be established.

Example

Configure LDP keychain authentication for all LDP peers and use the keychain named **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] key-id 1
[HUAWEI-keychain-kc1-keyid-1] algorithm sha-256
[HUAWEI-keychain-kc1-keyid-1] key-string YsHsjx_202206
[HUAWEI-keychain-kc1-keyid-1] send-time 14:30 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] receive-time 14:40 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] default send-key-id
[HUAWEI-keychain-kc1-keyid-1] quit
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain all name kc1
```

9.1.5 authentication key-chain peer-group

Function

The **authentication key-chain peer-group** command enables keychain authentication in a batch for a specified LDP peer group.

The **undo authentication key-chain peer-group** command disables keychain authentication in a batch for a specified LDP peer group.

By default, keychain authentication in a batch is disabled for all peer groups. LDP keychain authentication is recommended to ensure security.

Format

authentication key-chain peer-group *ip-prefix-name* **name** *keychain-name*

undo authentication key-chain peer-group

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP prefix list. The IP prefix list name is configured using the **ip ip-prefix** command.	The value is a string of 1 to 169 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks (").
name *keychain-name*	Specifies a keychain name. The keychain name is configured using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. The string does not contain question marks or spaces. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help improve LDP session security, keychain authentication can be configured for a TCP connection over which an LDP session has been established. If a great number of LDP peers are configured, run the **authentication key-chain peer-group** command to enable keychain authentication in a batch for LDP peers in a specified peer group. An IP prefix list can be specified to define the range of IP addresses in a group.

Prerequisites

The following steps have been performed:

- An IP prefix list has been configured using the **ip ip-prefix** command.
- A keychain has been configured using the **keychain** command.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.
- After the **authentication key-chain peer-group** command is run, the referenced Keychain authentication is applied to a specified peer. If keychain authentication fails, an LDP session fails to be established.
- Before a peer group is referenced, create it. By default, a nonexistent peer group cannot be specified in this command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is specified in this command, a local device performs keychain authentication for each LDP session connected to each LDP peer.

Example

Enable LDP keychain authentication for LDP peers with IP addresses matching the IP prefix list named **list1** in a specified peer group and use a keychain named **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] key-id 1
[HUAWEI-keychain-kc1-keyid-1] algorithm sha-256
[HUAWEI-keychain-kc1-keyid-1] key-string YsHsjx_202206
[HUAWEI-keychain-kc1-keyid-1] send-time 14:30 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] receive-time 14:40 2016-10-10 to 14:50 2016-10-10
[HUAWEI-keychain-kc1-keyid-1] default send-key-id
[HUAWEI-keychain-kc1-keyid-1] quit
[HUAWEI-keychain-kc1] quit
[HUAWEI] ip ip-prefix list1 permit 10.1.1.1 32
```

```
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain peer-group list1 name kc1
```

9.1.6 auto-frr lsp-trigger

Function

The **auto-frr lsp-trigger** command configures a policy for triggering LDP to establish backup LSPs based on backup routes.

The **undo auto-frr lsp-trigger** command restores the default setting.

By default, LDP uses backup routes with 32-bit addresses to establish backup LSPs.

Format

auto-frr lsp-trigger { **all** | **host** | **ip-prefix** *ip-prefix-name* | **none** }

undo auto-frr lsp-trigger

Parameters

Parameter	Description	Value
all	Specifies all backup routes to trigger LDP to establish backup LSPs.	-
host	Specifies backup routes with 32-bit addresses to trigger LDP to establish backup LSPs.	-
ip-prefix *ip-prefix-name*	Specifies IP prefix list to trigger LDP to establish backup LSPs.	The value is an existing IP prefix list name.
none	Specifies no backup routes to trigger LDP to establish backup LSPs.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network with a backup link, if a link fault occurs, Interior Gateway Protocol (IGP) routes converge and routes related to the backup link become available. After IGP route convergence is complete, an LDP LSP over the backup link becomes available. During this process, traffic is interrupted. To prevent traffic interruption, you can configure LDP fast reroute (FRR). On the network enabled with LDP FRR, if an interface failure (detected by the interface itself or by an associated BFD session) or a primary LSP failure (detected by an associated BFD session) occurs, LDP FRR is notified of the failure and rapidly forwards traffic to a backup LSP, protecting traffic on the primary LSP. The traffic switchover is performed within 50 milliseconds, avoiding traffic interruption.

LDP FRR is classified into the following types:

- LDP manual FRR: A backup LSP is configured manually by specifying an outbound interface or a next hop. The configuration is complex but flexible because a backup LSP can be configured manually. LDP manual FRR applies to simple networks.
- Auto LDP FRR: A backup LSP is automatically created based on a specified policy. The configuration is simple and loop-free. Auto LDP FRR applies to complex and large networks.

Auto LDP FRR depends on the automatic reroute function of IGP. Auto LDP FRR is automatically enabled after IGP automatic reroute is enabled using the **frr (IS-IS)** command. To change the policy for triggering LDP to establish backup LSPs, run the **auto-frr lsp-trigger** command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp(system view)** command in the system view.

Precautions

During LDP GR, changing the policy for triggering the setup of backup LSPs is not allowed.

If both the **auto-frr lsp-trigger** command and the **lsp-trigger** command are run, the established backup LSPs are controlled by both the policy for triggering LDP LSP establishment and the policy for triggering backup LDP LSP establishment. For example, if the policy for triggering LDP LSP establishment is **none** and that for triggering backup LDP LSP establishment is **all**, the backup LDP LSP is established using the **none** policy.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all backup routes trigger backup LDP LSP establishment.

Example

#Configure the policy for specifying no backup routes to trigger LDP to establish backup LSPs.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] auto-frr lsp-trigger none
```

9.1.7 backoff timer

Function

The **backoff timer** command sets the initial and maximum values for an Exponential backoff timer.

The **undo backoff timer** command restores the default settings.

By default, the initial value is 15 and the maximum value is 120, in seconds.

Format

backoff timer *init max*

undo backoff timer

Parameters

Parameter	Description	Value
init	Specifies the initial value of an Exponential backoff timer.	The value is an integer ranging from 5 to 2147483, in seconds.
max	Specifies the maximum value of an Exponential backoff timer.	The value is an integer ranging from 5 to 2147483, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an LSR fails to process an LDP Initialization message or is informed that the peer LSR rejects the received LDP Initialization message, the LSR starts the Exponential backoff timer and periodically resends an LDP Initialization message to initiate an LDP session before the Exponential backoff timer expires.

When the Exponential backoff timer starts, the active role waits a period of time equal to the initial value of the Exponential backoff timer to attempt to set up an LDP session for the first time. Subsequently, the active role waits a period of time twice as long as the previous one to attempt to set up an LDP session. When the waiting period reaches the maximum value of the Exponential backoff timer, the active role waits a period of time equal to the maximum value of the Exponential backoff timer to attempt to set up an LDP session.

Run the **backoff timer** command to change the interval at which the active role attempts to set up a session.

By setting the initial value and maximum value for the Exponential backoff timer, you can flexibly control the reestablishment of sessions in different network environments.

- When a device is being upgraded, increase the initial and maximum values to set a large interval at which the active role attempts to set up a session.
- When a device that is transmitting services is prone to intermittent disconnections, reduce the initial and maximum values to set a small interval at which the active role attempts to set up a session.

NOTE

The initial value for the Exponential backoff timer cannot be smaller than 15, and the maximum value cannot be smaller than 120.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

If a session is disconnected after the **backoff timer** command is run, the device attempts to set up a session based on the set initial and maximum values of the Exponential backoff timer.

Example

Set the initial value to 20s and the maximum value to 160s for the Exponential backoff timer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] backoff timer 20 160
```

9.1.8 bfd bind ldp-lsp

Function

The **bfd bind ldp-lsp** command creates a bidirectional forwarding detection (BFD) session for detecting LDP LSPs.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is created for detecting LDP LSPs.

Format

bfd *cfg-name* **bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	The value is in dotted decimal notation.
nexthop*ip-address*	Specifies the next hop IP address of the detected LSP.	The value is in dotted decimal notation.
interface*interface-type interface-number*	Specifies the outbound interface that is bound to a BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A dynamic LSP is established using LDP on an MPLS network. It takes an interface a long period of time to detect a link fault. After a static BFD session is bound to the LDP LSP, the interface can quickly detect faults on LDP LSPs. This method applies to small networks.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

- When the IP address of the outbound interface of the detected LSP is lent or borrowed, an outbound interface must be specified.

- When the LDP LSP is deleted but the LDP session exists, the BFD session is in Down state, but the configuration of the BFD session bound to the LDP session is not deleted.
- When configuring static BFD for LDP LSP on a network deployed with LDP over TE, specify **interface** *interface-type interface-number* as the tunnel interface.

Example

Create a BFD session to detect the LDP LSP with the egress IP address being 10.2.1.1, the next hop IP address being 10.1.1.1, and the outbound interface being VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd 1to4 bind ldp-lsp peer-ip 10.2.1.1 nexthop 10.1.1.1 interface vlanif 100
[HUAWEI-bfd-lsp-session-1to4]
```

9.1.9 bfd bind static-lsp

Function

The **bfd bind static-lsp** command creates a BFD session to detect static LSPs.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is created to detect static LSPs.

Format

bfd *cfg-name* **bind static-lsp** *lsp-name*

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the BFD configuration name.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
lsp-name	Specifies the name of the static LSP bound to the BFD session.	The value is an existing static LSP name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can deploy MPLS services by manually configuring static LSPs on small networks with simple topology and stable performance. It takes an interface a long period of time to detect a link fault. After a static BFD session is bound to the LDP LSP, the interface can quickly detect faults on LDP LSPs.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

- If the specified static LSP does not exist or the BFD configuration name exists, the BFD session cannot be created.
- The **commit** command must be run to make the configured BFD parameters take effect before a BFD session is created.
- When the status of the static LSP is Down, a BFD session cannot be created.

Example

Create a BFD session to detect the static LSP named **1to4**.

```
<HUAWEI> system-view
[HUAWEI] bfd bfd1to4 bind static-lsp 1to4
[HUAWEI-bfd-lsp-session-bfd1to4]
```

9.1.10 display default-parameter mpls ldp

Function

The **display default-parameter mpls ldp** command displays the default configurations of MPLS LDP.

Format

display default-parameter mpls ldp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS LDP, run the **display default-parameter mpls ldp** command.

Example

Display the default configurations of MPLS LDP.

```
<HUAWEI> display default-parameter mpls ldp

 LDP Default Values:
 ----------------------------------------------------------
          Protocol version               : V1
          Graceful restart              : Off
            Neighbor liveness(sec)       : 600
            FT reconnect timer(sec)      : 300
            Recovery timer(sec)          : 300
          MTU signaling                  : On
          Label retention mode           : Liberal
          Label distribution mode        : Ordered
          Label advertisement            : DU
          Local hello-hold timer(sec)    : 15
          Remote hello-hold timer(sec)   : 45
          Keepalive-hold timer(sec)      : 45
          Backoff timer init(sec)        : 15
          Backoff timer max(sec)         : 120
          IGP-Sync delay timer(sec)      : 10
          Graceful delete                : Off
            Graceful delete timer(sec)   : 5
          Capability-announcement        : Off
          mLDP MBB Capability            : Off
            Wait-ack timer(sec)          : 10
            Switch-delay timer(ms)       : 100
          mLDP P2MP Capability           : Off
          mLDP MP2MP Capability          : Off
          Label withdraw-delay           : Off
            Withdraw-delay timer(sec)    : 5
          Send LSP down reason           : Off
          Ingress LSP Load-balance Num   : 16
          Transit LSP Load-balance Num   : 16
          Smart-policy Ingress           : Off
          Smart-policy Auto-dod-request  : Off
          Label default-route            : Off
 ----------------------------------------------------------
```

Table 9-1 Description of the **display default-parameter mpls ldp** command output

Item	Description
Protocol version	LDP version number.
Graceful restart	LDP GR capability status. - On: LDP GR is enabled. - Off: LDP GR is disabled. By default, LDP GR is disabled. You can configure the LDP GR capability status using the **graceful-restart** command.

Item	Description
Neighbor liveness(sec)	Value of the neighbor-liveness timer, in seconds. The default value is 600s. You can set this value using the **graceful-restart timer neighbor-liveness** command.
FT reconnect timer(sec)	Value of the reconnect timer of an LDP session, in seconds. The default value is 300s. You can set this value using the **graceful-restart timer reconnect** command.
Recovery timer(sec)	Value of the recovery timer of an LDP LSP, in seconds. The default value is 300s. You can set this value using the **graceful-restart timer recovery** command.
MTU signaling	MTU TLV status. ● On: MTU TLV is enabled. ● Off: MTU TLV is disabled. By default, MTU TLV is enabled.
Label retention mode	LDP label retention modes include: ● Liberal: free mode. ● Conservative: conservative mode. The default label retention mode is liberal.
Label distribution mode	LDP label distribution mode. Currently, only the ordered mode is supported.
Label advertisement	LDP label advertisement modes include: ● DU: downstream unsolicited mode. ● DOD: downstream on demand mode. The default label advertisement mode is DU. You can set the LDP label advertisement mode using the **mpls ldp advertisement** command.
Local hello-hold timer(sec)	Value of the local Hello hold timer, in seconds. The default value is 15s. You can set this value using the **mpls ldp timer hello-hold** command.
Remote hello-hold timer(sec)	Value of the remote Hello hold timer, in seconds. The default value is 45s. You can set this value using the **mpls ldp timer hello-hold** command.
Keepalive-hold timer(sec)	Value of the keepalive hold timer for the local and remote LDP sessions, in seconds. The default value is 45s. You can set this value using the **mpls ldp timer keepalive-hold** command.
Backoff timer init(sec)	Initial value of the Exponential backoff timer, in seconds. The default value is 15s. You can set this value using the **backoff timer** command.

Item	Description
Backoff timer max(sec)	Maximum value of the Exponential backoff timer, in seconds. The default value is 120s. You can set this value using the **backoff timer** command.
IGP-Sync delay timer(sec)	Value of the LDP-IGP association timer, in seconds. The default value is 10s. You can set this value using the **mpls ldp timer igp-sync-delay** command.
Graceful delete	Graceful deletion. This function is disabled and not supported currently.
Graceful delete timer(sec)	Value of the graceful deletion timer, in seconds. The default value is 5s.
Capability-announcement	Dynamic capability announcement function. This function is disabled and not supported currently.
mLDP MBB Capability	Whether the mLDP make-before-break capability is enabled. The default value is "Off", indicating that mLDP make-before-break is disabled.
Wait-ack timer(sec)	Time (in seconds) elapses before a local device receives a Make-before-break (MBB) ACK Notification message
Switch-delay timer(ms)	Delay time (in seconds) for switching traffic to an MBB LSP
mLDP P2MP Capability	Whether mLDP P2MP is enabled globally. The default value is "Off", indicating that mLDP P2MP is disabled globally.
mLDP MP2MP Capability	Whether mLDP multipoint-to-multipoint (MP2MP) is enabled globally. The default value is "Off", indicating that mLDP MP2MP is disabled globally.
Label withdraw-delay	Whether the label withdraw delay function is enabled. The default value is "Off", indicating that this function is disabled.
Withdraw-delay timer(sec)	Default value of the label withdraw delay timer (in seconds).
Send LSP down reason	Whether a node is enabled to report the fault cause to the ingress. The default value is "Off", indicating that the faulty node is disabled from reporting the fault cause to the ingress.
Ingress LSP Load-balance Num	Default maximum number of equal-cost LDP LSPs that can be established on the ingress.
Transit LSP Load-balance Num	Default maximum number of equal-cost LDP LSPs that can be established on a transit node.

Item	Description
Smart-policy Ingress	Whether the smart LDP ingress policy is enabled.
Smart-policy Auto-dod-request	Whether on-demand LDP request trigger is enabled.
Label default-route	Whether the device is enabled to assign a label to a default IGP route. You can set this value using the **label distribution default-route** command.

9.1.11 display default-parameter mpls management

Function

The **display default-parameter mpls management** command displays default configurations of the MPLS management module.

Format

display default-parameter mpls management

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS management module, run the **display default-parameter mpls management** command.

Example

Display the default configurations of the MPLS management module.

```
<HUAWEI> display default-parameter mpls management

 Global Information:
 ------------------------------------------------------------
         BFD detect-multiplier        : 3
         BFD min-tx-interval(ms)      : 1000
         BFD min-rx-interval(ms)      : 1000
         Label advertisement mode     : Implicit null
         LSP trigger mode             : Host
         LDP LSP number threshold-alarm upper limit  : 80
         LDP LSP number threshold-alarm lower limit  : 75
```

```
         BGP LSP number threshold-alarm upper limit  : 80
         BGP LSP number threshold-alarm lower limit  : 75
         BGP V6 LSP number threshold-alarm upper limit  : 80
         BGP V6 LSP number threshold-alarm lower limit  : 75
         Dynamic Label number threshold-alarm upper limit  : 80
         Dynamic Label number threshold-alarm lower limit  : 70
         RSVP LSP number threshold-alarm upper limit  : 80
         RSVP LSP number threshold-alarm lower limit  : 75
         Total LSP number threshold-alarm upper limit  : 80
         Total LSP number threshold-alarm lower limit  : 75
         Total CR LSP number threshold-alarm upper limit  : 80
         Total CR LSP number threshold-alarm lower limit  : 75
         Ingress LDP LSP number threshold-alarm upper limit  : 80
         Ingress LDP LSP number threshold-alarm lower limit  : 75
         Transit LDP LSP number threshold-alarm upper limit  : 80
         Transit LDP LSP number threshold-alarm lower limit  : 75
         Egress LDP LSP number threshold-alarm upper limit  : 80
         Egress LDP LSP number threshold-alarm lower limit  : 75
         Ingress BGP LSP number threshold-alarm upper limit  : 80
         Ingress BGP LSP number threshold-alarm lower limit  : 75
         Egress BGP LSP number threshold-alarm upper limit  : 80
         Egress BGP LSP number threshold-alarm lower limit  : 75
         Egress BGP V6 LSP number threshold-alarm upper limit  : 80
         Egress BGP V6 LSP number threshold-alarm lower limit  : 75
         Ingress RSVP LSP number threshold-alarm upper limit  : 80
         Ingress RSVP LSP number threshold-alarm lower limit  : 75
         Transit RSVP LSP number threshold-alarm upper limit  : 80
         Transit RSVP LSP number threshold-alarm lower limit  : 75
         Egress RSVP LSP number threshold-alarm upper limit  : 80
         Egress RSVP LSP number threshold-alarm lower limit  : 75
         Total ingress LSP number threshold-alarm upper limit  : 80
         Total ingress LSP number threshold-alarm lower limit  : 75
         Total transit LSP number threshold-alarm upper limit  : 80
         Total transit LSP number threshold-alarm lower limit  : 75
         Total egress LSP number threshold-alarm upper limit  : 80
         Total egress LSP number threshold-alarm lower limit  : 75
         Total ingress CR LSP number threshold-alarm upper limit  : 80
         Total ingress CR LSP number threshold-alarm lower limit  : 75
         Total transit CR LSP number threshold-alarm upper limit  : 80
         Total transit CR LSP number threshold-alarm lower limit  : 75
         Total egress CR LSP number threshold-alarm upper limit  : 80
         Total egress CR LSP number threshold-alarm lower limit  : 75
         Auto bypass tunnel interface number threshold-alarm upper limit  : 80
         Auto bypass tunnel interface number threshold-alarm lower limit  : 75
         P2MP auto tunnel interface number threshold-alarm upper limit  : 80
         P2MP auto tunnel interface number threshold-alarm lower limit  : 75
         TE dynamic bfd number threshold-alarm upper limit  : 80
         TE dynamic bfd number threshold-alarm lower limit  : 75
         LDP dynamic bfd number threshold-alarm upper limit  : 80
         LDP dynamic bfd number threshold-alarm lower limit  : 75
         Total MLDP tree number threshold-alarm upper limit  : 80
         Total MLDP tree number threshold-alarm lower limit  : 75
         Total MLDP branch number threshold-alarm upper limit  : 80
         Total MLDP branch number threshold-alarm lower limit  : 75
         Total LDP remote adjacency number threshold-alarm upper limit  : 80
         Total LDP remote adjacency number threshold-alarm lower limit  : 75
         Total LDP local adjacency number threshold-alarm upper limit  : 80
         Total LDP local adjacency number threshold-alarm lower limit  : 75
         Total CSPF node number threshold-alarm upper limit  : 80
         Total CSPF node number threshold-alarm lower limit  : 75
         Total CSPF link number threshold-alarm upper limit  : 80
         Total CSPF link number threshold-alarm lower limit  : 75
         Total CSPF network-lsa number threshold-alarm upper limit  : 80
         Total CSPF network-lsa number threshold-alarm lower limit  : 75
         Total CSPF SRLG number threshold-alarm upper limit  : 80
         Total CSPF SRLG number threshold-alarm lower limit  : 75
         RSVP peer number threshold-alarm upper limit  : 80
         RSVP peer number threshold-alarm lower limit  : 75
-------------------------------------------------------------
```

Table 9-2 Description of the display default-parameter mpls management command output

Item	Description
BFD detect-multiplier	BFD detection multiplier. The default value is 3. You can set this value using the **mpls bfd** command.
BFD min-tx-interval(ms)	Interval for sending BFD packets. You can set this value using the **mpls bfd** command.
BFD min-rx-interval(ms)	Interval for receiving BFD packets. You can set this value using the **mpls bfd** command.
Label advertisement mode	Mode in which the egress node assigns labels to the penultimate hop. ● Implicit null: The egress node assigns an implicit empty label to the penultimate hop. The value of the label is 3. ● Explicit null: The egress node assigns an explicit empty label to the penultimate hop. The value of the label is 0. ● Non null: The egress node assigns a label to the penultimate hop properly. The value of the label is not smaller than 16. By default, the implicit null mode is used. You can set the label advertisement mode using the **label advertise** command.
LSP trigger mode	Policy for triggering LSP setup. ● All: All static routes and IGP routing entries trigger the setup of LSPs. ● Host: The IP route of the 32-bit address host triggers the setup of LSPs. ● Ip-prefix: Only FECs that match entries in the IP address prefix list trigger the setup of LSPs. ● None: The setup of LSPs is not triggered. The default trigger policy is **Host**. You can set the LSP trigger mode using the **lsp-trigger** command.
LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for LDP LSPs. You can set the LSP trigger mode using the **mpls ldp-lsp-number threshold-alarm** command.
LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for LDP LSPs. You can set the LSP trigger mode using the **mpls ldp-lsp-number threshold-alarm** command.
BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for BGP LSPs. You can set the LSP trigger mode using the **mpls bgp-lsp-number threshold-alarm** command.

Item	Description
BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for BGP LSPs. You can set the LSP trigger mode using the **mpls bgp-lsp-number threshold-alarm** command.
BGP V6 LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for BGP IPv6 LSPs. You can set the LSP trigger mode using the **mpls bgpv6-lsp-number threshold-alarm** command.
BGP V6 LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for BGP IPv6 LSPs. You can set the LSP trigger mode using the **mpls bgpv6-lsp-number threshold-alarm** command.
Dynamic Label number threshold-alarm upper limit	Upper limit of the alarm threshold for dynamic label usage. You can set the LSP trigger mode using the **mpls dynamic-label-number threshold-alarm** command.
Dynamic Label number threshold-alarm lower limit	Lower limit of the alarm threshold for dynamic label usage. You can set the LSP trigger mode using the **mpls dynamic-label-number threshold-alarm** command.
RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for RSVP LSPs. You can set the LSP trigger mode using the **mpls rsvp-lsp-number threshold-alarm** command.
RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for RSVP LSPs. You can set the LSP trigger mode using the **mpls rsvp-lsp-number threshold-alarm** command.
Total LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total LSPs. You can set the LSP trigger mode using the **mpls total-lsp-number threshold-alarm** command.
Total LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total LSPs. You can set the LSP trigger mode using the **mpls total-lsp-number threshold-alarm** command.
Total CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total CR-LSPs. You can set the LSP trigger mode using the **mpls total-crlsp-number threshold-alarm** command.
Total CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total CR-LSPs. You can set the LSP trigger mode using the **mpls total-crlsp-number threshold-alarm** command.
Ingress LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress LDP LSP

Item	Description
Ingress LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress LDP LSP
Transit LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for transit LDP LSP
Transit LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for transit LDP LSP
Egress LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress LDP LSP
Egress LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress LDP LSP
Ingress BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress BGP LSP
Ingress BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress BGP LSP
Egress BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress BGP LSP
Egress BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress BGP LSP
Egress BGP V6 LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress BGP V6 LSP
Egress BGP V6 LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress BGP V6 LSP
Ingress RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress RSVP LSP
Ingress RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress RSVP LSP

Item	Description
Transit RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for transit RSVP LSP
Transit RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for transit RSVP LSP
Egress RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress RSVP LSP
Egress RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress RSVP LSP
Total ingress LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total ingress LSP
Total ingress LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total ingress LSP
Total transit LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total transit LSP
Total transit LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total transit LSP
Total egress LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total egress LSP
Total egress LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total egress LSP
Total ingress CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total ingress CR-LSP
Total ingress CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total ingress CR-LSP
Total transit CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total transit CR-LSP

Item	Description
Total transit CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total transit CR-LSP
Total egress CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total egress CR-LSP
Total egress CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total egress CR-LSP
Auto bypass tunnel interface number threshold-alarm upper limit	Upper limit of the alarm threshold for auto bypass tunnel interface
Auto bypass tunnel interface number threshold-alarm lower limit	Lower limit of the alarm threshold for auto bypass tunnel interface
P2MP auto tunnel interface number threshold-alarm upper limit	Upper limit of the alarm threshold for P2MP auto tunnel interface
P2MP auto tunnel interface number threshold-alarm lower limit	Lower limit of the alarm threshold for P2MP auto tunnel interface
TE dynamic bfd number threshold-alarm upper limit	Upper limit of the alarm threshold for TE dynamic bfd
TE dynamic bfd number threshold-alarm lower limit	Lower limit of the alarm threshold for TE dynamic bfd
LDP dynamic bfd number threshold-alarm upper limit	Upper limit of the alarm threshold for LDP dynamic bfd
LDP dynamic bfd number threshold-alarm lower limit	Lower limit of the alarm threshold for LDP dynamic bfd
Total MLDP tree number threshold-alarm upper limit	Upper limit of the alarm threshold for total MLDP tree

Item	Description
Total MLDP tree number threshold-alarm lower limit	Lower limit of the alarm threshold for total MLDP tree
Total MLDP branch number threshold-alarm upper limit	Upper limit of the alarm threshold for total MLDP branch
Total MLDP branch number threshold-alarm lower limit	Lower limit of the alarm threshold for total MLDP branch
Total LDP remote adjacency number threshold-alarm upper limit	Upper limit of the alarm threshold for total LDP remote adjacency
Total LDP remote adjacency number threshold-alarm lower limit	Lower limit of the alarm threshold for total LDP remote adjacency
Total LDP local adjacency number threshold-alarm upper limit	Upper limit of the alarm threshold for total LDP local adjacency
Total LDP local adjacency number threshold-alarm lower limit	Lower limit of the alarm threshold for total LDP local adjacency
Total CSPF node number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF node
Total CSPF node number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF node
Total CSPF link number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF link
Total CSPF link number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF link
Total CSPF network-lsa number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF network-lsa
Total CSPF network-lsa number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF network-lsa

Item	Description
Total CSPF SRLG number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF SRLG
Total CSPF SRLG number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF SRLG
RSVP peer number threshold-alarm upper limit	Upper limit of the alarm threshold for RSVP peer
RSVP peer number threshold-alarm lower limit	Lower limit of the alarm threshold for RSVP peer

9.1.12 display isis ldp-sync interface

Function

The **display isis ldp-sync interface** command displays information about LDP and IS-IS synchronization on an interface.

Format

display isis [*process-id* | **vpn-instance** *vpn-instance-name*] **ldp-sync interface**

Parameters

Parameter	Description	Value
process-id	Specifies the IS-IS process ID.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

For all the interfaces that are enabled with LDP and IS-IS synchronization, run the **display isis ldp-sync** command to view information about LDP and IS-IS synchronization.

Example

Display information about LDP and IS-IS synchronization on an interface.

```
<HUAWEI> display isis ldp-sync interface

               Ldp Sync interface information for ISIS(1)
               ------------------------------------------
Interface    HoldDownTimer    HoldMaxCostTimer   LDP State   Sync State
Vlanif100     10               10                Down        Init
```

Table 9-3 Description of the display isis ldp-sync interface command output

Item	Description
Interface	Interface connected to neighbors.
HoldDownTimer	Interval during which the interface waits for the LDP session establishment and does not create the IS-IS neighbor relationship. The default value is 10 seconds. You can set this value using the **isis timer ldp-sync hold-down** command.
HoldMaxCostTimer	Interval for IS-IS to notify the local device of the maximum metric in the link state PDU (LSP). The default value is 10 seconds. You can set this value using the **isis timer ldp-sync hold-max-cost** command. **NOTE** If the value of this field is **infinite**, IS-IS permanently notifies the local device of the maximum metric in the LSP before an LDP session is established.
LDP State	LDP session status, which can be: - Up: The LDP session is normal. - Down: The LDP session is disconnected. - GR: The LDP session is in GR state. If the interface is maintaining the session before GR, the LDP status is displayed as GR state during GR.

Item	Description
Sync State	Status of synchronization between LDP and IS-IS: ● Sync-Achieved: The creation of an LDP session and establishment of the IS-IS neighbor relationship are synchronized. ● HoldDown: indicates the state in which the interface waits to create an LDP session without creating the IS-IS neighbor relationship. ● HoldMaxCost: indicates the state in which IS-IS advertises the maximum metric in LSPs sent by the local device. ● Init: indicates the initial state.

9.1.13 display lspv configuration

Function

The **display lspv configuration** command displays the current configuration of LSPV tracert.

Format

display lspv configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display lspv configuration** command to check the current LSPV configurations.

Example

Display the current configuration of LSPV tracert.

```
<HUAWEI> display lspv configuration
lspv packet filter 2100
undo lspv mpls-lsp-ping echo enable
```

Table 9-4 Description of the **display lspv configuration** command output

Item	Description
lspv packet filter 2100	Filters the LSPV tracert packet with the specific source address according to ACL 2100. To configure the filtering of the LSPV tracert packet with the specific source address, run the **lspv packet-filter** command.
undo lspv mpls-lsp-ping echo enable	Disables the response to MPLS Ping packets. To configure a device to respond to MPLS Echo Request packets, run the **lspv mpls-lsp-ping echo enable** command.

9.1.14 display lspv statistics

Function

The **display lspv statistics** command displays LSPV statistics.

Format

display lspv statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In MPLS network management, the **ping lsp** or **tracert lsp** command can be used for LSP detection.

If the LSP detection fails, you can run the **display lspv statistics** command to view statistics about MPLS packets sent and received on the local device. If the number of MPLS packets that the local device sends is the same as the number of MPLS packets that the local device receives, but the ping or trace operation fails, the detection failure is caused by the fault of the local device, not the LSP.

Precautions

Before running the **display lspv statistics** command to collect LSPV statistics, run the **reset lspv statistics** command to clear the existing statistics.

Example

Display LSPV statistics on the device.

```
<HUAWEI> display lspv statistics
Total sent: 0 packet(s)
Total received: 0 packet(s)
MPLS echo request sent: 0 packet(s), received: 0 packet(s)
MPLS echo reply sent: 0 packet(s), received: 0 packet(s)
-------------------------------------------------------------------
Statistics base on ReturnCode:
0 - No return code,1 - Malformed echo request received,2 - One or more
of the TLVs was not understood,3 - Replying router is an egress for
the FEC at stack-depth, 4 - Replying router has no mapping for the FEC
at stack-depth,5 - Downstream Mapping Mismatch, 6 - Upstream Interface
Index Unknown, 7 - Reserved, 8 - Label switched at stack-depth,9 -
Label switched but no MPLS forwarding at stack-depth,10 - Mapping for
this FEC is not the given label at stack-depth,11 - No label entry at
stack-depth,12 - Protocol not associated with interface at FEC
stack-epth,13 - Premature termination of ping due to label stack
shrinking to a single label.:
-------------------------------------------------------------------
Value     SendNum     RecvNum     Value     SendNum     RecvNum
   0          0           0          1          0          0
   2          0           0          3          0          0
   4          0           0          5          0          0
   6          0           0          7          0          0
   8          0           0          9          0          0
  10          0           0         11          0          0
  12          0           0         13          0          0
-------------------------------------------------------------------
```

Table 9-5 Description of the **display lspv statistics** command output

Item	Description
Total sent	Total number of sent MPLS Echo Request and MPLS Echo Reply packets
Total received	Total number of received MPLS Echo Request and MPLS Echo Reply packets
MPLS echo request sent, received	Number of sent and received MPLS Echo Request packets
MPLS echo reply sent, received	Number of sent and received MPLS Echo Reply packets

Item	Description
Statistics base on ReturnCode	Statistics base on ReturnCode: - 0: No return code - 1: Malformed echo request received - 2: One or more of the TLVs was not understood - 3: Replying router is an egress for the FEC at stack-depth - 4: Replying router has no mapping for the FEC at stack-depth - 5: Downstream Mapping Mismatch - 6: Upstream Interface Index Unknown - 7: Reserved - 8: Label switched at stack-depth - 9: Label switched but no MPLS forwarding at stack-depth - 10: Mapping for this FEC is not the given label at stack-depth - 11: No label entry at stack-depth - 12: Protocol not associated with interface at FEC stack-epth - 13: Premature termination of ping due to label stack shrinking to a single label
Value	The value of ReturnCode in sent or received LSP verification packets.
SendNum	Number of sent packets with this ReturnCode.
RecvNum	Number of received packets with this ReturnCode.

9.1.15 display mpls bfd session

Function

The **display mpls bfd session** command displays information about BFD sessions for MPLS.

Format

display mpls bfd session [**fec** *fec-address* | **monitor** | **nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number* | **statistics** | **verbose**]

display mpls bfd session protocol ldp [**fec** *fec-address* [**verbose**]]

display mpls bfd session protocol { **cr-static** | **rsvp-te** } [**lsp-id** *ingress-lsr-id session-id lsp-id* [**verbose**]]

display mpls bfd session protocol bgp [**fec** *fec-address* [**verbose**]]

Parameters

Parameter	Description	Value
fec *fec-address*	Displays information about the BFD session of a specified FEC.	The value is in dotted decimal notation.
monitor	Displays monitoring information of BFD sessions.	-
nexthop *ip-address*	Displays information about the BFD session of a specified next hop.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Displays information about the BFD session of the LSP with a specified outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
protocol	Indicates the type of the protocol.	-
cr-static	Displays information about the BFD session for static CR-LSP.	-
ldp	Displays information about the BFD session for LDP.	-
rsvp-te	Displays information about the BFD session for RSVP-TE.	-
statistics	Displays statistics about BFD sessions such as the total number of BFD sessions.	-
verbose	Displays detailed information about BFD sessions.	-
lsp-id *ingress-lsr-id*	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer ranging from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer ranging from 0 to 65535.
bgp	Displays information about BFD sessions for BGP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls bfd session** command to view information about a BFD session and the LSP detected by BFD, including the destination address and outbound interface of the LSP, the local discriminator of the BFD session, and the status of an MPLS BFD session.

Example

Display information about the BFD session.

```
<HUAWEI> display mpls bfd session
--------------------------------------------------------------------------------
              BFD Information: LDP  LSP
--------------------------------------------------------------------------------
FEC            DISC  OUT-IF      NEXTHOP        TUNNEL         STATE
3.3.3.3        8     VLANIF100   10.1.1.2       Tunnel1        Up
```

Table 9-6 Description of the display mpls bfd session command output

Item	Description
FEC	Forwarding equivalence class.
DISC	Local discriminator of a BFD session.
OUT-IF	Outbound interface.
NEXTHOP	IP address of the next hop.
TUNNEL	Name of a tunnel.
STATE	Status of an MPLS BFD session. ● Up ● Down

Display detailed information about a BFD session with the specified protocol type and LSP ID.

```
<HUAWEI> display mpls bfd session protocol rsvp-te lsp-id 3.3.3.3 3 1 verbose
----------------------------------------------------------------------
              BFD Information: TE TUNNEL
----------------------------------------------------------------------
 No                    :  1
 LspIndex              :  6157
 Protocol              :  RSVP-TE
 Tunnel-Interface      :  Tunnel1
 Fec                   :  2.2.2.2
 Nexthop               :  10.2.3.2
```

```
Out-Interface            :  Vlanif100
Bfd-Discriminator        :  8195
TEMIB Tunn Table Index   :  3
SessionTunnelID          :  3
LocalLspId               :  1
PrevSessionTunnelID      :  -
NextSessionTunnelID      :  12
ActTx                    :  2200
ActRx                    :  2200
ActMulti                 :  -
Bfd-State                :  Down
Time                     :  2559 sec
```

Table 9-7 Description of the display mpls bfd session protocol rsvp-te lsp-id 3.3.3.3 3 1 verbose command output

Item	Description
No	Serial number.
LspIndex	Index number of an LSP.
Protocol	Protocol type.
Tunnel-Interface	Name of a tunnel interface.
Fec	Forwarding equivalence class.
Nexthop	IP address of the next hop.
Out-Interface	Name of an outbound interface.
Bfd-Discriminator	Local discriminator of a BFD session.
TEMIB Tunn Table Index	Index of the tunnel entry to which an LSP corresponds.
SessionTunnelID	BFD session ID.
LocalLspId	ID of a local LSP.
PrevSessionTunnelID	Tunnel ID mapping the previous LSP to which a BFD session is bound.
NextSessionTunnelID	Tunnel ID mapping the next LSP to which a BFD session is bound.
ActTx	Actual interval for sending BFD packets, in milliseconds.
ActRx	Actual interval for receiving BFD packets, in milliseconds.
ActMulti	Actual local detection multiple of a BFD session.
Bfd-State	Status of the BFD session. ● Up ● Down

Item	Description
Time	Period from the time when the BFD session is created or updated till now, in seconds.

Display BFD session statistics.

```
<HUAWEI> display mpls bfd session statistics
Lsp Type       sess num   Tx        Rx        Mult      Trig-type
LDP LSP        0          1000      1000      3         NONE
BGP LSP        0          1000      1000      3         NONE
STATIC CRLSP   0          1000      1000      3         -
RSVP           0          1000      1000      3         -
TOTAL          0
```

Table 9-8 Description of the **display mpls bfd session statistics** command output

Item	Description
Lsp Type	LSP type.
sess num	Number of BFD sessions monitoring the LSP.
Tx	Effective minimum interval (in ms) at which BFD packets are sent.
Rx	Effective minimum interval (in ms) at which BFD packets are received.
Mult	Effective BFD detection multiplier.
Trig-type	BFD session establishment policy: ● HOST: BFD sessions are established using host addresses. ● IP-PREFIX: BFD sessions are established using an IP address prefix list. ● FEC-LIST: BFD sessions are established using a FEC list. ● NONE: No policy for establishing BFD sessions is configured. ● -: N/A

Display BFD session monitoring information.

```
<HUAWEI> display mpls bfd session monitor

LDP BFD TRIGGER INFO:
  Trig-Type  : None
  OutIfIndex : Invalid
  NextHop    : Invalid

LDP BFD SCAN INFO:
  Cur BackGround Oper  : Off
  Cur Scan Index       : Invalid
```

```
  First Bfd Scan Index : Invalid
  Scan Again           : No
  License Lim Reached  : No
  License Lim Scn Agn  : No
  BackGround Status    : Suspended/Off
  Current Scan Node    : -

BGP BFD SCAN INFO:
  Cur BackGround Oper  : Off
  Cur Scan Index       : Invalid
  Scan Again           : No
  License Lim Reached  : No
  BackGround Status    : Suspended/Off

TE BFD SCAN INFO:
  Cur BackGround Oper  : Off
  Cur Scan Index       : 0
  First Bfd Scan Index : 0
  Scan Again           : No
  License Lim Reached  : No
  License Lim Scn Agn  : No
  BackGround Status    : Suspended/Off

CAPABILITY :
  Bfd Capability     : Disable
  Ldp Bfd Capability : Disable
  Bgp Bfd Capability : Disable
  Te Bfd Capability  : Disable
  Bfd Session Full   : Not-full
  Bfd Clearing       : No


BFD FOR LSP PAF LICENSE INFORMATION:
Lsp Type  Min-Val   Max-Val   Avail-Val Created
LDP LSP   0         1024      1024      0
BGP LSP   0         1024      1024      0
TE LSP    0         2048      256       0 + 0 (RSVP + CRSTATIC)
```

Table 9-9 Description of the **display mpls bfd session monitor** command output

Item	Description
Trig-Type	BFD session establishment policy: ● HOST: BFD sessions are established using host addresses. ● IP-PREFIX: BFD sessions are established using an IP address prefix list. ● FEC-LIST: BFD sessions are established using a FEC list. ● NONE: No policy for establishing BFD sessions is configured. ● -: N/A
OutIfIndex	Index of a BFD session outbound interface.
NextHop	Next-hop IP address of a BFD session.

Item	Description
Cur BackGround Oper	Background operation: ● Create ● Delete ● Update ● Off
Cur Scan Index	Scanned BFD session index. "Invalid" indicates that no BFD session is established.
First Bfd Scan Index	First scanned BFD session index. "Invalid" indicates that no BFD session is established.
Scan Again	Whether a device scans BFD sessions again: ● Yes ● No
License Lim Reached	Whether the number of established BFD sessions reaches the upper limit specified in the license file: ● Yes ● No
License Lim Scn Agn	Whether the switch needs to check the threshold-crossing event about establishment BFD sessions: ● Yes ● No
BackGround Status	Background status: ● Running ● Suspended/Off
Current Scan Node	Name of a node that is being scanned.
Bfd Capability	Whether MPLS BFD is enabled: ● Enable ● Disable
Ldp Bfd Capability	Whether BFD for LDP is enabled: ● Enable ● Disable
Bgp Bfd Capability	Whether BFD for BGP tunnel is enabled: ● Enable ● Disable
Te Bfd Capability	Whether BFD for Traffic Engineering (TE) is enabled: ● Enable ● Disable

Item	Description
Bfd Session Full	Whether the number of created BFD sessions reaches the upper limit: - Full: The number of created BFD sessions reached the upper limit. - Not-full: The number of created BFD sessions is lower than the upper limit.
Bfd Clearing	Whether BFD is disabled globally: - Yes - No
Lsp Type	LSP type
Min-Val	Minimum number of supported LSPs specified in the license file.
Max-Val	Maximum number of supported LSPs specified in the license file.
Avail-Val	Average number of supported LSPs specified in the license file.
Created	Number of established LSPs.

9.1.16 display mpls graceful-restart

Function

The **display mpls graceful-restart** command displays graceful restart (GR) information about all protocols related to MPLS.

Format

display mpls graceful-restart

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When MPLS is used together with other protocols, run the **display mpls graceful-restart** command to view GR information about protocols related to MPLS, including the GR status, GR start time, and GR type.

Example

Display GR information related to all protocols.

```
<HUAWEI> display mpls graceful-restart
Protocol       GR state       GR start time            GR type
LDP            Normal         -                        -
CRLDP          Normal         -                        -
RSVP           Normal         -                        -
BGP            Normal         -                        -
L3VPN          Normal         -                        -
STATIC         Normal         -                        -
CRSTATIC       Normal         -                        -
BGP IPV6       Normal         -                        -
STATIC HA      Normal         -                        -
L3VPN IPV6     Normal         -                        -
STATIC TP      Normal         -                        -
```

Table 9-10 Description of the display mpls graceful-restart command output

Item	Description
Protocol	Protocol type: LDP, CRLDP, RSVP, BGP, L3VPN, STATIC, CRSTATIC, BGP IPV6, STATIC HA, L3VPN IPV6, and STATIC TP.
GR state	GR status of a protocol: ● Restarting: The protocol is in the GR process. ● Normal: The protocol is not in the GR process.
GR start time	Time when the GR process starts When the GR process does not start, a hyphen (-) is displayed.
GR type	GR type: ● System restart: indicates the system GR. ● Protocol restart: indicates the protocol GR. When the GR process does not start, a hyphen (-) is displayed.

9.1.17 display mpls interface

Function

The **display mpls interface** command displays information about all MPLS-enabled interfaces.

Format

display mpls interface [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
verbose	Displays detailed information about the interface enabled with MPLS.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After enabling MPLS functions, run the **display mpls interface** command to view information about the interface enabled with MPLS.

Example

Display information about all MPLS-enabled interfaces.

```
<HUAWEI> display mpls interface
Interface            Status    TE Attr    LSP Count   CRLSP Count Effective MTU
Vlanif100              Up        Dis        2           0           1500
```

Table 9-11 Description of the display mpls interface command output

Item	Description
Interface	The interface enabled with MPLS.
Status	Interface status: ● Up ● Down
TE Attr	Status of the TE attributes on an interface: ● Dis: MPLS TE is disabled on the interface. ● En: MPLS TE is enabled on the interface.
LSP Count	Number of LSPs established on an interface.
CRLSP Count	Number of CR-LSPs established on an interface.

Item	Description
Effective MTU	MPLS MTU used during data forwarding: ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect. To set the MPLS MTU, run the **mpls mtu** command. To set the interface MTU, run the **mtu** command.

Display detailed information about a specified MPLS-enabled interface.

```
<HUAWEI> display mpls interface vlanif 100 verbose
No                    :  1
Interface             :  Vlanif100
Status                :  Up
TE Attribute          :  Disable
Static LSPCount       :  0
Static CR-LSPCount    :  0
LDP LSPCount          :  0
RSVP LSPCount         :  0
MPLS MTU              :  -
Interface MTU         :  1500
Effective MTU         :  1500
TE FRR                :  Disable
Interface Index       :  0xd1
```

Table 9-12 Description of the display mpls interface verbose command output

Item	Description
No	Serial number.
Interface	The interface enabled with MPLS.
Status	Interface status: ● Up ● Down
TE Attribute	Status of the TE attributes on the interface: ● Disable: MPLS TE is disabled on the interface. ● Enable: MPLS TE is enabled on the interface.
Static LSPCount	Number of static LSPs established on the interface.
Static CR-LSPCount	Number of static CR-LSPs established on the interface.
LDP LSPCount	Number of LDP LSPs created on the interface.
RSVP LSPCount	Number of RSVP-TE LSPs established on the interface.
MPLS MTU	MPLS MTU value configured using the **mpls mtu** command. When no MPLS MTU is set, a hyphen (-) is displayed.

Item	Description
Interface MTU	MTU value configured on an interface. To set the interface MTU, run the **mtu** command.
Effective MTU	MPLS MTU used during data forwarding: ● If no MPLS MTU is set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect. To set the MPLS MTU, run the **mpls mtu** command. To set the interface MTU, run the **mtu** command.
TE FRR	Whether the TE FRR is enabled or disabled on the interface: ● Disable: No bypass tunnel is set up in manual FRR mode to protect the interface. ● Enable: A bypass tunnel is set up in manual FRR mode to protect the interface.
Interface Index	Interface index value.

9.1.18 display mpls label static available

Function

The **display mpls label static available** command displays information about labels available for transmitting static services.

Format

display mpls label static available [[**label-from** *label-index*] **label-number** *label-number*]

Parameters

Parameter	Description	Value
label-from *label-index*	Specifies the start label value.	The value is an integer ranging from 16 to 1023.
label-number *label-number*	Specifies the number of the required labels.	The value is an integer ranging from 1 to 1008.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

By default, the system reserves separate label spaces for dynamic and static services, allowing labels for dynamic and static services to be stored in separate spaces.

Before specifying a label for static services, ensure that the specified label is available. You can run the **display mpls label static available** command to view labels for static services.

In the command output, a hyphen is used to specify a range. For example, labels 1000, 1001, and 1002 are displayed as 1000-1002.

Follow-up Procedure

Labels displayed in the command output can be allocated for static services.

Example

Display information about labels available for transmitting static services.

```
<HUAWEI> display mpls label static available
16-1023
```

9.1.19 display mpls label-stack ilm inlabel

Function

The **display mpls label-stack ilm inlabel** command displays information about the label stack for packets with a specified incoming label.

Format

display mpls label-stack ilm inlabel *in-label*

Parameters

Parameter	Description	Value
in-label	Specifies the incoming label for the packets about which label-stack information is to be displayed.	The value is an integer ranging from 16 to 1048575.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to query information about the outgoing label stack for packets based on the incoming label. The supported public network tunnels include static LSP tunnels, LDP LSPs, dynamic TE tunnels, and static TE tunnels. This command cannot be used in the following situations:

- Tunnels overlap.
- Tunnels load-balance traffic.
- The primary and secondary SPE egresses are used.
- Routes recurse to a ring network.
- Layer 3 labels are used.

Example

Display the outgoing label, outbound interface, and tunnel type in the packets with the incoming label value of 1028.

```
<HUAWEI> display mpls label-stack ilm inlabel 1028
Label-stack  : 1
Level        : 1
Type         : LDP
Label        : 1025
OutInterface : Vlanif111
```

Table 9-13 Description of the **display mpls label-stack ilm inlabel** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

9.1.20 display mpls last-info lsp-down

Function

The **display mpls last-info lsp-down** command displays information about LSPs in Down state.

Format

display mpls last-info lsp-down [**protocol ldp**] [**verbose**]

Parameters

Parameter	Description	Value
protocol ldp	Displays information about LSPs in Down state.	-
verbose	Displays detailed information about LDP LSPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If LSPs fail and enter the Down state, run the **display mpls last-info lsp-down** command to view the faults that cause the latest 64 LSPs to go Down.

Example

Display brief information about LDP LSPs that just enter the Down state.

```
<HUAWEI> display mpls last-info lsp-down
-------------------------------------------------------------------------------
                 LDP LSP Information: Host Address
-------------------------------------------------------------------------------
FEC                In/Out Label  Out Interface       Down Reason
10.12.12.12/32     1029/3        vlanif10            route changed
10.12.12.12/32     NULL/3         vlanif10            route changed
10.11.11.11/32     1034/3        vlanif10            cannot recovery from GR
10.11.11.11/32     NULL/3         vlanif10            cannot recovery from GR
10.11.11.11/32     1033/3        vlanif10            DS lost
10.11.11.11/32     NULL/3         vlanif10            DS lost
```

Table 9-14 Description of the display mpls last-info lsp-down command output

Item	Description
FEC	Forwarding equivalence class.
In/Out Label	Values of the incoming and outgoing labels.
Out Interface	Outbound interface.

Item	Description
Down Reason	LSPs go Down due to the following causes: - route changed: A route was changed. - adjacency changed: An adjacency was changed. - cannot recovery from GR: The LDP LSP failed to be reestablished during GR. - recv release msg: A Release message was received. - recv withdraw msg: A Withdraw message was received. - US lost: The session with the upstream node went Down. - DS lost: The session with the downstream node went Down. - policy changed: The policy to establish LSPs was changed (Generally, configurations of the policy was changed). - reach paf limit: PAF resources are insufficient. - GR aging: The LSP aged after GR. - others

Display detailed information about LDP LSPs that just enter the Down state.

```
<HUAWEI> display mpls last-info lsp-down protocol ldp verbose
-------------------------------------------------------------------------------
                 LDP LSP Information: Host Address
-------------------------------------------------------------------------------
 No                 :  1
 VrfIndex           :
 Fec                :  10.1.1.1/32
 Nexthop            :  127.0.0.1
 In-Label           :  3
 Out-Label          :  NULL
 Out-Interface      :  vlanif13
 LspIndex           :  6144
 Token              :  0x0
 LsrType            :  Egress
 Outgoing token     :  0x0
 Label Operation    :  POP
 Down Time          :  2011/11/08 16:39:59+00:00
 Exist time         :  14sec
 Down Reason        :  policy changed

 No                 :  2
 VrfIndex           :
 Fec                :  10.2.2.2/32
 Nexthop            :  10.1.2.2
 In-Label           :  NULL
 Out-Label          :  3
 Out-Interface      :  vlanif13
 LspIndex           :  6146
 Token              :  0x1
 LsrType            :  Ingress
 Outgoing token     :  0x0
 Label Operation    :  PUSH
```

```
Down Time          :  2011/11/08 16:51:26+00:00
Exist time         :  5sec
Down Reason        :  route changed
```

Table 9-15 Description of the display mpls last-info lsp-down protocol ldp verbose command output

Item	Description
No	Record No.
VrfIndex	Index of a VRF instance.
Fec	Forwarding equivalence class.
Nexthop	Next hop IP address.
In-Label	Value of the incoming label.
Out-Label	Value of the outgoing label.
Out-Interface	Outbound interface.
LspIndex	Index of an LSP.
Token	Token value, in the hexadecimal format.
LsrType	Type of an LSR on an LSP, which can be ingress, transit, or egress.
Outgoing token	Outgoing token value, in the hexadecimal format.
Label Operation	Label operation, which can be PUSH, POP, SWAP, or SWAPPUSH.
Down Time	Time when an LSP goes Down.
Exist time	Existing period of an LDP LSP, in seconds.

Item	Description
Down Reason	LSPs go Down due to the following causes: ● route changed: A route was changed. ● adjacency changed: An adjacency was changed. ● cannot recovery from GR: The LDP LSP failed to be reestablished during GR. ● recv release msg: A Release message was received. ● recv withdraw msg: A Withdraw message was received. ● US lost: The session with the upstream node went Down. ● DS lost: The session with the downstream node went Down. ● policy changed: The policy to establish LSPs was changed (Generally, configurations of the policy was changed). ● reach paf limit: PAF resources are insufficient. ● GR aging: The LSP aged after GR. ● others

9.1.21 display mpls ldp

Function

The **display mpls ldp** command displays global LDP configurations.

Format

display mpls ldp [**all**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all LDP information.	-
verbose	Displays detailed information about the LDP protocol and the LSR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After global MPLS is enabled, run the **display mpls ldp** command to view LDP configurations, including configurations of the GR timer, label distribution, and label management.

Prerequisites

MPLS has been enabled globally using the **mpls** command, and MPLS LDP has been enabled globally using the **mpls ldp** command.

Example

Display global LDP configurations.

```
<HUAWEI> display mpls ldp

                         LDP Global Information
 ------------------------------------------------------------------------------
 Protocol Version        : V1            Neighbor Liveness    : 600 Sec
 Graceful Restart        : Off           FT Reconnect Timer   : 300 Sec
 MTU Signaling           : On            Recovery Timer       : 300 Sec
 Capability-Announcement : On            Longest-match        : Off
 mLDP P2MP Capability    : Off           mLDP MBB Capability  : Off
 mLDP MP2MP Capability   : Off

                         LDP Instance Information
 ------------------------------------------------------------------------------
 Instance ID             : 0             VPN-Instance         :
 Instance Status         : Active        LSR ID               : 10.1.1.1
 Loop Detection          : Off           Path Vector Limit    : 32
 Label Distribution Mode : Ordered
 Label Retention Mode    : Liberal(DU)/Conservative(DOD)
 Instance Deleting State : No            Instance Resetting State : No
 Graceful-Delete         : Off           Graceful-Delete Timer : 5 Sec
 ------------------------------------------------------------------------------
```

Table 9-16 Description of the display mpls ldp command output

Item	Description
LDP Global Information	Global LDP information.
Protocol Version	LDP protocol version.
Neighbor Liveness	Timeout period of the GR Neighbor-liveness timer. To set the timeout period of the GR Neighbor-liveness timer, run the **graceful-restart timer neighbor-liveness** command.

Item	Description
Graceful Restart	Whether LDP is enabled with GR: - On: GR is enabled. - Off: GR is disabled. To enable LDP GR, run the **graceful-restart** command.
FT Reconnect Timer	Timeout period of the GR reconnect timer. To set the timeout period of the GR reconnect timer, run the **graceful-restart timer reconnect** command.
MTU Signaling	Whether the MTU signaling is enabled: - On: The private MTU TLV is sent. - Off: The MTU TLV is not supported. - On(apply-tlv): The MTU TLV is sent according to RFC 3988. To set the MTU signaling, run the **mtu-signalling** command.
Recovery Timer	Timeout period of the GR Recovery timer. To set the timeout period of the GR Recovery timer, run the **graceful-restart timer recovery** command.
Capability-Announcement	Status of the LDP dynamic capability announcement function: - On: LDP dynamic capability announcement is enabled. - Off: LDP dynamic capability announcement is disabled. **NOTE** The switch does not support this parameter.
Longest-match	Status of LDP extension for inter-area LSP: - On: LDP extension for inter-area LSP is enabled. - Off: LDP extension for inter-area LSP is disabled. To set the status of LDP extension for inter-area LSP, run the **longest-match** command.
mLDP P2MP Capability	Whether mLDP P2MP is globally enabled: - On: mLDP P2MP is enabled globally. - Off: mLDP P2MP is disabled globally. **NOTE** The switch does not support this parameter.

Item	Description
mLDP MBB Capability	Whether the mLDP make-before-break capability is enabled: - On: mLDP make-before-break is enabled. - Off: mLDP make-before-break is disabled. **NOTE** The switch does not support this parameter.
mLDP MP2MP Capability	Whether multipoint extensions for LDP (mLDP) multipoint-to-multipoint (MP2MP) is globally enabled: - On: mLDP MP2MP is enabled globally. - Off: mLDP MP2MP is disabled globally. **NOTE** The switch does not support this parameter.
LDP Instance Information	Information about the LDP multi-instance.
Instance ID	ID of a VPN instance in the integer format.
VPN-Instance	Name of a VPN instance. The default name is **null**. **NOTE** The switch does not support this parameter.
Instance Status	Status of an instance: - Active: The instance is in the Active state. - NotInService: The instance is in the NotInService state temporarily due to certain operations. For example, after the **reset mpls ldp** or **graceful-restart** command is used, the instance is unavailable temporarily. - Destroy: The instance is in the Destroy state. For example, after the **undo mpls ldp** command is used, the instance is in the Destroy state.
LSR ID	LSR ID of an LDP instance.
Loop Detection	Loop detection status: - On: Loop detection is enabled. - Off: Loop detection is disabled. To set the status of the loop detection, run the **loop-detect** command.
Path Vector Limit	Path vector limit for loop detection. To set the path vector limit for loop detection, run the **path-vectors** command.

Item	Description
Label Distribution Mode	Label distribution mode: ● Ordered ● Independent Currently, the switch supports only the ordered mode.
Label Retention Mode	● If label advertisement mode is DU, label retention mode will be Liberal. ● If label advertisement mode is DOD, label retention mode will be Conservative.
Instance Deleting State	Deletion status of an instance: ● Yes: The instance is being deleted. ● No: The instance is not being deleted.
Instance Resetting State	Resetting status of an instance: ● Yes: The instance is being reset. ● No: The instance is not being reset.
Graceful-Delete	Whether graceful deletion is enabled: ● On: enables graceful deletion. ● Off: disables graceful deletion. **NOTE** The switch does not support this parameter.
Graceful-Delete Timer	Value of the Graceful-delete Timer, in seconds.

9.1.22 display mpls ldp adjacency

Function

The **display mpls ldp adjacency** command displays information about LDP adjacencies.

Format

display mpls ldp adjacency [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**]

display mpls ldp adjacency all [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays information about the LDP adjacency of a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
remote	Displays information about the LDP adjacency of a specified remote end.	-
peer *peer-id*	Displays information about the LDP adjacency of a specified peer.	The value is in dotted decimal notation.
verbose	Displays detailed information about LDP adjacencies.	-
all	Displays information about all the LDP adjacencies.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an LDP session is established, run the **display mpls ldp adjacency** command to view real-time information about LDP adjacencies, for example, the number of received Hello messages.

Example

Display information about LDP adjacencies.

```
<HUAWEI> display mpls ldp adjacency

 LDP Adjacency Information in Public Network
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 -------------------------------------------------------------------------
 SN   SourceAddr      PeerID          VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 -------------------------------------------------------------------------
  1   10.1.2.2        2.2.2.2         0      0000:00:22        527       L
  2   10.2.3.3        3.3.3.3         0      0000:00:20        254       L
  3   3.3.3.3         3.3.3.3         0      0000:00:18        79        R
 -------------------------------------------------------------------------
 TOTAL: 3 Record(s) found.
```

Table 9-17 Description of the display mpls ldp adjacency command output

Item	Description
SN	Serial number.
SourceAddr	Source address of the Hello message received by an LDP adjacency.
PeerID	LSR ID of an LDP peer.
VrfID	ID of a VPN instance.
AdjAge(DDDD:HH:MM)	Time elapsed since the LDP adjacency was created, in DDDD:HH:MM format.
RcvdHello	Number of Hello messages received by an LDP adjacency.
Type	Type of an LDP adjacency: ● L: local LDP adjacency. ● R: remote LDP adjacency.

Display detailed information about the LDP adjacency of the remote peer with the LSR ID of 3.3.3.3/32.

```
<HUAWEI> display mpls ldp adjacency remote peer 3.3.3.3 verbose

 LDP Adjacency Information in Public Network
 -------------------------------------------------------------------------------
                          LDP Peer ID : 3.3.3.3
                     VPNInstance name : -
                           CreateDate : 2005-07-27
                           CreateTime : 11:15:41+00:00
                        Adjacency Age : 0000:03:44
                        AdjacencyType : Remote Adjacency
                     Discovery-Source : -
                   UDP Source Address : 3.3.3.3
                        UDP Socket ID : 33
                         Sequence No. : 0
  Configuration Hello Hold Timer(sec) : 45
                   Hello Message Rcvd : 899
            Adjacency Deletion Status : No
 -------------------------------------------------------------------------------
 TOTAL: 1 Adjacency(s) found.
```

Table 9-18 Description of the display mpls ldp adjacency remote peer command output

Item	Description
LDP Peer ID	LSR ID of an LDP peer.
VPNInstance name	Name of a VPN instance. **NOTE** The switch does not support this parameter.
CreateDate	Creation date of an LDP adjacency.

Item	Description
CreateTime	Creation time of an LDP adjacency.
Adjacency Age	Time elapsed since the LDP adjacency was created, in DDDD:HH:MM format.
AdjacencyType	Type of an LDP adjacency: ● Local Adjacency. ● Remote Adjacency.
Discovery-Source	Discovery source of an LDP adjacency: ● Interface: a discovery source of the local LDP adjacency. ● Null: a discovery source of the remote LDP adjacency.
UDP Source Address	Source address of the UDP packet contained in the Hello message received by an LDP adjacency.
UDP Socket ID	Socket ID of the LDP adjacency to receive Hello message.
Sequence No	Serial number carried in the received Hello message. The default value is 0.
Configuration Hello Hold Timer(sec)	Hello hold timer configured on the peer, in seconds: ● Link Hello hold timer: maintains the local LDP adjacency. The default value is 15. ● Target Hello hold timer: maintains the remote LDP adjacency. The default value is 45.
Hello Message Rcvd	Number of Hello messages received by an LDP adjacency.
Adjacency Deletion Status	Deletion status of an LDP adjacency: ● Yes: The LDP adjacency is being deleted. ● No: The LDP adjacency is not being deleted.

9.1.23 display mpls ldp adjacency statistics

Function

The **display mpls ldp adjacency statistics** command displays statistics about LDP adjacencies.

Format

display mpls ldp adjacency statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls ldp adjacency statistics** command to view the number of LDP adjacencies that are classified into local and remote LDP adjacencies.

Example

Display statistics about LDP adjacencies.

```
<HUAWEI> display mpls ldp adjacency statistics

 LDP Adjacency Statistics Information
 -------------------------------------------------
 AdjacencyType          Local   Remote   Total
 -------------------------------------------------
 AdjacencyNumber          1       2        3
 -------------------------------------------------
```

Table 9-19 Description of the display mpls ldp adjacency statistics command output

Item	Description
AdjacencyType	Type of LDP adjacencies.
AdjacencyNumber	Number of LDP adjacencies.
Local	Number of local LDP adjacencies.
Remote	Number of remote LDP adjacencies.
Total	Total number of LDP adjacencies.

9.1.24 display mpls ldp error packet

Function

The **display mpls ldp error packet** command displays information about LDP-related error messages.

Format

display mpls ldp error packet { **tcp** | **udp** | **l2vpn** } [*number*]

Parameters

Parameter	Description	Value
tcp	Displays information about TCP error messages related to LDP sessions.	-
udp	Displays information about UDP error messages related to LDP sessions.	-
l2vpn	Displays information about L2VPN error messages related to LDP sessions.	-
number	Specifies the number of LDP-related error messages to be displayed.	The value is an integer ranging from 1 to 100.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an exception occurs on an MPLS network, run the **display mpls ldp error packet** command to view information about LDP-related error messages such as the number of received error messages.

Example

Displays information about error UDP packets related to LDP.

```
<HUAWEI> display mpls ldp error packet udp

 LDP Error UDP Packet
 Total received error packet number: 58
 Record error packet number         : 10
 Max Record error packet number     : 10
------------------- Number 1 ----------------------
 Date&Time          : 2011-11-08 16:39:59+08:00
 Error Reason       : unknown
 Interface          : Vlanif100
 Instance ID        : 0
 Message Type       : Hello
 Length             : 34
 Packet content     :
 01 64 00 14 00 00 00 32 04 00 00 04 00 0f 00 00
 04 01 00 04 01 01 01 01 00 00 00 00 00 00 00 00
 00 00
```

Table 9-20 Description of the **display mpls ldp error packet** command output

Item	Description
Total received error packet number	Number of received error messages related to LDP sessions.
Record error packet number	Number of recorded error messages related to LDP sessions.
Max Record error packet number	Maximum number of error messages that can be recorded.
Date&Time	Date and time when an error message was received.
Error Reason	Cause for an error.
Interface	An interface that receives the message.
Instance ID	ID of an LDP instance to which the error message belongs.
Message Type	Message type, which includes but is not limited to the following: ● Address ● Address Withdraw ● Capability ● Hello ● Initialization ● KeepAlive ● Label Request ● Label Mapping ● Label Withdraw ● Label Release ● Label Abort Request ● Notification ● Unknown
Length	Length of the error message
Packet content	Contents of the error message in the binary format.

9.1.25 display mpls ldp error packet state

Function

The **display mpls ldp error packet state** command displays the record status of LDP-related error messages.

Format

display mpls ldp error packet state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an exception occurs on an MPLS network, run the **display mpls ldp error packet state** command to view the record status of UDP, TCP, and L2VPN error messages related to LDP sessions.

Example

Display the record status of LDP-related error messages.

```
<HUAWEI> display mpls ldp error packet state
-------------------------------------------
 Error UDP packet state            : ON
 Max UDP error packet number       : 100
 Current UDP error packet number   : 0
 Error TCP packet state            : ON
 Max TCP error packet number       : 100
 Current TCP error packet number   : 0
 Error L2VPN packet state          : ON
 Max L2VPN error packet number     : 100
 Current L2VPN error packet number : 0
-------------------------------------------
```

Table 9-21 Description of the display mpls ldp error packet state command output

Item	Description
Error UDP packet state	Whether UDP error messages can be detected and recorded: ● ON: UDP error message detection is enabled. ● OFF: UDP error message detection is disabled.
Max UDP error packet number	Maximum number of UDP error messages that can be recorded.
Current UDP error packet number	Number of recorded UDP error messages.

Item	Description
Error TCP packet state	Whether TCP error messages can be detected and recorded: - ON: TCP error message detection is enabled. - OFF: TCP error message detection is disabled.
Max TCP error packet number	Maximum number of TCP error messages that can be recorded.
Current TCP error packet number	Number of recorded TCP error messages.
Error L2VPN packet state	Whether L2VPN error messages can be detected and recorded: - ON: L2VPN error message detection is enabled. - OFF: L2VPN error message detection is disabled.
Max L2VPN error packet number	Maximum number of L2VPN error messages that can be recorded.
Current L2VPN error packet number	Number of recorded L2VPN error messages.

9.1.26 display mpls ldp event adjacency-down

Function

The **display mpls ldp event adjacency-down** command displays events that LDP adjacencies go Down.

Format

display mpls ldp event adjacency-down [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays events that LDP adjacencies on a specified interface go Down. - *interface-type* specifies the type of the interface. - *interface-number* specifies the number of the interface.	-

Parameter	Description	Value
remote	Indicates the remote LDP peer.	-
peer *peer-id*	Specifies the LSR ID of an LDP peer.	The value is in dotted decimal notation.
verbose	Displays details about events that LDP adjacencies go Down.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Run the **display mpls ldp event adjacency-down** command to view the event that an LDP adjacency went Down. The information includes the time, reason, and the duration of the LDP adjacency.

Precautions

A maximum of 1024 events can be displayed.

Example

Display the events that LDP adjacencies go Down.

```
<HUAWEI> display mpls ldp event adjacency-down

 LDP Adjacency Down Information
 ------------------------------------------------------------------------
 PeerID           Down       Down                  Duration      Reason
                 Date       Time                  Time
 ------------------------------------------------------------------------
 2.2.2.2:0        2012-04-24 17:08:59+00:00        0h44m54s      C
 2.2.2.2:0        2012-04-26 15:43:54+00:00        46h34m54s     A
 ----------------------------------------------------------------------------
 TOTAL: 2 Record(s) Found.
 A : The Adjacency is down because Hello Timer Expired.
 C : The administrator configuration to trigger.
 D : The Adjacency is down because delay-deleting timer expired.
 P : The Adjacency is down because the peer is being deleted.
 O : Other reason.
```

Table 9-22 Description of the display mpls ldp event adjacency-down command output

Item	Description
PeerID	LSR ID of an LDP peer.

Item	Description
Down Date	Date when an LDP adjacency went Down.
Down Time	Time when an LDP adjacency went Down.
Duration Time	Time elapsed since an LDP adjacency established.
Reason	Causes for the LDP adjacency Down event: ● A: The Hello timer expires. ● C: The configuration is changed. ● D: The delay deleting timer expires. ● P: The peer is deleted. ● O: other causes.

Display detailed information that LDP adjacencies go Down.

```
<HUAWEI> display mpls ldp event adjacency-down verbose

 LDP Adjacency-Down Information
 ------------------------------------------------------------------------
 SN                               : 1
 PeerID                            : 2.2.2.2
 VrfID                            : 0
 DownDate                              : 2012-04-24
 DownTime                              : 17:08:59+00:00
 DurationTime                          : 0h44m54s
 MaxInterval(sec)                      : 5
 Reason                             : configuration to trigger
 Type                             : Local Adjacency
 DiscoverySource                       : Vlanif60
 -------------------------------------------------------------------------------
 SN                               : 2
 PeerID                            : 2.2.2.2
 VrfID                            : 0
 DownDate                              : 2012-04-26
 DownTime                              : 15:43:54+00:00
 DurationTime                          : 46h34m54s
 MaxInterval(sec)                      : 6
 Reason                             : Hello Timer Expired
 Type                             : Local Adjacency
 DiscoverySource                       : Vlanif60
 -------------------------------------------------------------------------------
  TOTAL: 2 Record(s) Found.
```

Table 9-23 Description of the display mpls ldp event adjacency-down verbose command output

Item	Description
SN	Serial number.
PeerID	LSR ID of an LDP peer.

Item	Description
VrfID	ID of a VPN instance.
DownDate	Date when an LDP adjacency went Down.
DownTime	Time when an LDP adjacency went Down.
DurationTime	Time elapsed since an LDP adjacency established.
MaxInterval (sec)	Maximum interval for sending a Hello message.
Reason	Reason for the LDP adjacency Down event: ● A: The Hello timer expires. ● C: The configuration is changed. ● D: The delay deleting timer expires. ● P: The peer is deleted. ● O: other causes.
Type	Adjacency type: ● Local Adjacency: Directly connected adjacency. ● Remote Adjacency: Indirectly connected adjacency.
DiscoverySource	Interface where an LDP peer is discovered.

9.1.27 display mpls ldp event gr-helper

Function

The **display mpls ldp event gr-helper** command displays GR Helper information.

Format

display mpls ldp event gr-helper [**all** | *peer-id*]

Parameters

Parameter	Description	Value
all	Displays information about all GR Helpers.	-

Parameter	Description	Value
peer-id	Displays information about a GR Helper on a specified LDP peer.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If GR Helpers are configured, run the **display mpls ldp event gr-helper** command to view GR Helper information.

Example

Display GR Helper information.

```
<HUAWEI> display mpls ldp event gr-helper
 LDP GR-Helper Peer Info
 ------------------------------------------------------------------
 LDP InstanceId              : 0          Vpn Instance Name:
 Peer ID                     : 1.1.1.1
 Label Advertisement Mode   : Downstream Unsolicited
 Timer State                 :
 Recovery Timer Left         : 229(s)
 Peer Gr Timer Configuration:
 Reconnect Timer             : 300(s)     Recovery Timer   : 300(s)
 Stale Lsp State             :
 USCB Counter                : 3          DSCB Counter     : 3
 ------------------------------------------------------------------
 Total GR Peer Counter: 1
```

Table 9-24 Description of the display mpls ldp event gr-helper command output

Item	Description
LDP InstanceId	LDP instance name.
Vpn Instance Name	VPN instance name. **NOTE** The device does not support this parameter.
Peer ID	LSR ID of an LDP peer.
Label Advertisement Mode	Mode used by LDP to advertise labels. To set the mode used by LDP to advertise labels, run the **mpls ldp advertisement** command.
Timer State	Status of the timer.

Item	Description
Recovery Timer Left	Remaining time before an LSP starts to be reestablished.
Peer Gr Timer Configuration	Configuration of the GR timers.
Reconnect Timer	Value of the LDP session reconnection timer. To set the value of the LDP session reconnection timer, run the **graceful-restart timer reconnect** command.
Recovery Timer	Value of the LSP recovery timer. To set the value of the LSP recovery timer, run the **graceful-restart timer recovery** command.
Stale Lsp state	Status of the primary LSP.
USCB Counter	Number of upstream control blocks (USCBs).
DSCB Counter	Number of downstream control blocks (DSCBs).
Total GR Peer Counter	Number of GR Helper.

9.1.28 display mpls ldp event session-down

Function

The **display mpls ldp event session-down** command displays events that LDP sessions go Down.

Format

display mpls ldp event session-down

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp event session-down** command to view events that LDP sessions go Down, including the cause and time.

Example

Display events that LDP sessions go Down.

```
<HUAWEI> display mpls ldp event session-down

LDP Session Down Information
------------------------------------------------------------------------------
PeerID       Down        Down              Duration   Flag Reason
             Date        Time              Time
------------------------------------------------------------------------------
10.1.2.9:0  2011-12-15 10:14:11+00:00   0h6m15s    L    Recv Noti(0x000a)

10.1.2.9:0  2011-12-15 10:14:26+00:00   0h6m34s    L    Recv Noti(0x000a)

------------------------------------------------------------------------------
TOTAL: 2 Record(s) Found.
R: Remote peer.
L: Local peer.
B: Both of local and remote peer.
G: Graceful Restart Session.
Important notification message error code:
  0x0003: Bad PDU Length.
  0x0005: Bad Message Length.
  0x0007: Bad TLV Length.
  0x0009: Hello Hold Timer Expired.
  0x000a: Shutdown.
  0x0014: KeepAlive Timer Expired.
```

Table 9-25 Description of the display mpls ldp event session-down command output

Item	Description
PeerID	LSR ID of an LDP peer.
Down Date	Date when an LDP session went down.
Down Time	Time when an LDP session went down.
Duration Time	Time elapsed since an LDP adjacency established.
Flag	Peer type. ● R: Remote peer, indicating that a remote session has been established. ● L: Local peer, indicating that a local session has been established. ● B: Both of local and remote peer, indicating that both local and remote sessions have been established. ● G: Graceful Restart Session.
Reason	Description of the cause.

Item	Description
Important notification message error code	Important notification message error code.
Bad PDU Length	Incorrect PDU length.
Bad Message Length	Incorrect message length.
Bad TLV Length	Incorrect TLV length.
Hello Hold Timer Expired	Hello Hold timer expired.
Shutdown	The peer actively shuts down the session.
KeepAlive Timer Expired	Keepalive timer expired.

9.1.29 display mpls ldp interface

Function

The **display mpls ldp interface** command displays information about LDP-enabled interfaces.

Format

display mpls ldp interface [*interface-type interface-number* | [**all**] [**verbose**]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If the parameter is specified, the configurations of a specified LDP-enabled interface are displayed.	-
all	Displays information about all LDP-enabled interfaces.	-
verbose	Displays detailed information about LDP-enabled interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp interface** command to view configurations of LDP-enabled interfaces and some real-time information, such as the number of sent and received Hello messages.

Example

Display information about LDP-enabled interfaces.

```
<HUAWEI> display mpls ldp interface

 LDP Interface Information in Public Network
 Codes:LAM(Label Advertisement Mode), IFName(Interface name)
 A '*' before an interface means the entity is being deleted.
 ------------------------------------------------------------------------------
 IFName         Status       LAM   TransportAddress    HelloSent/Rcv
 ------------------------------------------------------------------------------
Vlanif100       Active       DU    10.1.1.1            29574/29539
 ------------------------------------------------------------------------------
```

Table 9-26 Description of the display mpls ldp interface command output

Item	Description
IFName	Name of an LDP-enabled interface.
Status	Status of the local LSR: ● Active ● Inactive
LAM	Label advertisement mode: ● DU: downstream unsolicited mode. ● DoD: downstream on demand mode. To set the label advertisement mode, run the **mpls ldp advertisement** command.
TransportAddress	IP address of a node that initiates a TCP connection for an LDP session.
HelloSent/Rcv	Number of sent and received Hello messages.

Display detailed information about LDP-enabled interfaces.

```
<HUAWEI> display mpls ldp interface verbose

 LDP Interface Information in Public Network
 ------------------------------------------------------------------------------
 Interface Name :Vlanif100
 LDP ID         : 10.1.1.1:0            Transport Address : 10.1.1.1
 Entity Status  : Active                Effective MTU : 1500

 Configured Hello Hold Timer      : 15 Sec
 Negotiated Hello Hold Timer      : 15 Sec
 Configured Hello Send Timer      : 2 Sec
 Configured Keepalive Hold Timer : 45 Sec
```

```
Configured Keepalive Send Timer : 3 Sec
Configured Delay Timer          : 10 Sec
Label Advertisement Mode        : Downstream Unsolicited
Hello Message Sent/Rcvd         : 29913/29878 (Message Count)
Entity Deletion Status          : No
mLDP P2MP Capability            : Disable
mLDP MP2MP Capability           : Disable
------------------------------------------------------------------------------
```

Table 9-27 Description of the display mpls ldp interface verbose command output

Item	Description
Interface Name	Name of an LDP-enabled interface.
LDP ID	LDP identifier.
Transport Address	IP addresses used in the TCP connection of a session.
Entity Status	Status of this entity: - Active - Inactive
Effective MTU	MTU value used for creating an LSP.
Configured Hello Hold Timer	Timeout period of the configured Hello hold timer. To set the timeout period of the Hello hold timer, run the **mpls ldp timer hello-hold** command.
Negotiated Hello Hold Timer	Negotiated value of the Hello hold timer, which is the smaller value of the Hello hold timers configured on the local and remote LDP peers.
Configured Hello Send Timer	Timeout period of the configured Hello send timer. To set the timeout period of the Hello send timer, run the **mpls ldp timer hello-send** command.
Configured Keepalive Hold Timer	Timeout period of the configured Keepalive hold timer. To set the timeout period of the Keepalive hold timer, run the **mpls ldp timer keepalive-hold** command.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer. To set the timeout period of the Keepalive send timer, run the **mpls ldp timer keepalive-send** command.

Item	Description
Configured Delay Timer	Timeout period of the Delay timer, which, in LDP and IGP synchronization, is the time that an interface waits to establish an LSP after an LDP session is established.
Label Advertisement Mode	Label advertisement mode: ● Downstream Unsolicited ● Downstream on Demand To set the label advertisement mode, run the **mpls ldp advertisement** command.
Hello Message Sent/Rcvd	Number of sent and received Hello messages.
Entity Deletion Status	Deletion status of an instance: ● Yes: The instance is being deleted. ● No: The instance is not being deleted.
mLDP P2MP Capability	Whether mLDP P2MP is enabled: ● Enable ● Disable **NOTE** The switch does not support this function.
mLDP MP2MP Capability	Whether mLDP MP2MP is enabled: ● Enable ● Disable **NOTE** The switch does not support this function.

9.1.30 display mpls label all summary

Function

The **display mpls label all summary** displays allocation information about all MPLS labels.

Format

display mpls label all summary

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a session is established, the system collects statistics on label usage, including the allocation range and protocol type. You can use the **display mpls label all summary** command to view the allocation of label space and the corresponding protocol type.

Example

Display allocation information about MPLS labels.

```
<HUAWEI> display mpls label all summary
TableType      MinValue    MaxValue    AvailableNum
Reserved             0          15             16
Static              16        1023           1008
Dynamic           1024      163840         162815
Block           163841      180244          16404
```

NOTE

The preceding information is an example. The allocation ranges of labels depend on the actual situation.

Table 9-28 Description of the **display mpls label all summary** command output

Item	Description
TableType	Label type. - Reserved: indicates reserved labels. - Static: indicates static labels, mainly for MPLS TE and BGP. - Dynamic: indicates dynamic labels, mainly for LDP, MPLS TE, and BGP. - Block: indicates block labels, mainly for BGP.
MinValue	Minimum label value.
MaxValue	Maximum label value.
AvailableNum	Number of labels that can be allocated.

9.1.31 display mpls ldp lsp

Function

The **display mpls ldp lsp** command displays information about an LDP LSP.

Format

display mpls ldp lsp [**all** | *destination-address mask-length*] [**peer** *peer-id*]

display mpls ldp lsp inbound-policy

Parameters

Parameter	Description	Value
all	Displays information about all LDP LSPs.	-
destination-address	Specifies the destination IPv4 address of an LDP LSP.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the specified IPv4 address.	The value is an integer ranging from 0 to 32.
peer *peer-id*	Specifies the peer ID.	The value is in dotted decimal notation.
inbound-policy	Displays information about the LSPs that have passed an inbound policy, in addition to information about the LSPs that are established without applying the inbound policy.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After LDP LSPs are set up, run the **display mpls ldp lsp** command to view detailed information about LSPs such as the outbound interfaces, next hop addresses, total number, and types.

Example

Display information about LSPs.

```
<HUAWEI> display mpls ldp lsp

 LDP LSP Information
 -------------------------------------------------------------------------------
 Flag after Out IF: (I) - LSP Is Only Iterated by RLFA
 -------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop        OutInterface
 -------------------------------------------------------------------------------
 10.3.3.3/32        3/NULL         10.4.4.9        127.0.0.1      InLoop0
 10.3.3.9/32        3/NULL         10.4.4.9        127.0.0.1      InLoop0
*10.3.3.9/32        Liberal/1024                   DS/10.4.4.9
 10.4.4.9/32        NULL/3         -               172.16.1.2     Vlanif100
 10.4.4.9/32        1029/3         10.4.4.9        172.16.1.2     Vlanif100
 -------------------------------------------------------------------------------
 TOTAL: 4 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is stale
 A '*' before a DS means the session is stale
 A '*' before a NextHop means the LSP is FRR LSP
```

Table 9-29 Description of the display mpls ldp lsp command output

Item	Description
DestAddress/ Mask	Destination address and mask of an LSP.
In/OutLabel	Values of the incoming and outgoing labels. An asterisk (*) before In/OutLabel indicates that the LSP is in the Stale state and needs to be restored.
UpstreamPeer	Upstream peer of an LSP. An asterisk (*) before UpstreamPeer indicates that the session is in the GR state.
NextHop	Next hop IP address. An asterisk (*) before NextHop indicates that the LSP is an FRR LSP. DS is short for DownStream. The address next to DS/ is the LSR ID of a downstream peer.
OutInterface	Name of an outbound interface.
TOTAL: 4 Normal LSP(s) Found.	Total number of normal LSPs.
TOTAL: 1 Liberal LSP(s) Found.	Total number of liberal LSPs.
TOTAL: 0 Frr LSP(s) Found.	Total number of FRR LSPs.

9.1.32 display mpls ldp lsp statistics

Function

The **display mpls ldp lsp statistics** command displays statistics about LDP LSPs.

Format

display mpls ldp lsp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls ldp lsp statistics** command displays the statistics about an LDP LSP, whereas the **display mpls lsp statistics** command displays the statistics about all types of LSPs.

Example

Display statistics about LDP LSPs.

```
<HUAWEI> display mpls ldp lsp statistics

 LDP LSP Statistics Information
 A '*' before a number means the LSP is for longest-match
 -------------------------------------------------------------------------------
 VPNInstanceName   Total   Ingress   Transit   Egress   Liberal  FRR
 -------------------------------------------------------------------------------
 -                   14      4         4         3        3        0
                     *0     *0        *0        *0       *-       *0
 -------------------------------------------------------------------------------
```

Table 9-30 Description of the display mpls ldp lsp statistics command output

Item	Description
VPNInstanceName	Name of a VPN instance: • A hyphen (-) indicates a public network instance. • If LDP multi-instance is configured, the name of the created VPN instance is displayed. **NOTE** The switch does not support this parameter.

Item	Description
Total	Number of LDP LSPs in an instance.
Ingress	Number of ingress LSPs in an instance.
Transit	Number of transit LSPs in an instance.
Egress	Number of egress LSPs in an instance.
Liberal	Number of liberal LSPs in an instance.
FRR	Number of FRR LSPs in an instance. **NOTE** The switch does not support this parameter.

9.1.33 display mpls ldp peer

Function

The **display mpls ldp peer** command displays information about LDP peers.

Format

display mpls ldp peer [[**all**] [**verbose**] | *peer-id*]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about LDP peers.	-
peer-id	Displays information about a specified LDP peer.	The value is in dotted decimal notation.
all	Displays information about all LDP peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If an LDP LSP fails to be established, run the **display mpls ldp peer** command to view the **DiscoverySource** field and check the interface through which the peer relationship is established.

The system supports the coexistent local and remote LDP peers. When you run the **display mpls ldp peer** command, information about both local and remote LDP peers is displayed.

You can set the *peer-id* parameter to specify a peer.

Precautions

You can view information about LDP peers only after the peers have been established using the **mpls ldp (interface view)** or **remote-ip** command.

Example

Display information about LDP peers.

```
<HUAWEI> display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                 TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0              2.2.2.2            Remote Peer : rtb
 3.3.3.3:0              3.3.3.3            Vlanif100
 ------------------------------------------------------------------------------
 TOTAL: 2 Peer(s) Found.
```

Table 9-31 Description of the display mpls ldp peer command output

Item	Description
PeerID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● Non-0: per-interface label space.
TransportAddress	Transport address of an LDP peer. The transport address is used to set up TCP connections.
DiscoverySource	Discovery source of an LDP peer: ● Interface name: indicates the source that discovers the local LDP peer. ● Remote LDP peer name: indicates the source that discovers the remote LDP peer.

Display detailed information about LDP peers.

```
<HUAWEI> display mpls ldp peer verbose

 LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 Peer LDP ID          : 2.2.2.2:0
 Peer Max PDU Length : 4096          Peer Transport Address   : 2.2.2.2
 Peer Loop Detection : Off           Peer Path Vector Limit   : ----
 Peer FT Flag         : Off          Peer Keepalive Timer     : 45 Sec
```

```
Recovery Timer      : ----         Reconnect Timer          : ----
Peer Type           :Remote
Peer Label Advertisement Mode : Downstream Unsolicited
Peer Discovery Source         : remote peer: rtb
Peer Deletion Status          : No
Capability-Announcement       : Off
Peer mLDP P2MP Capability     : Off
Peer mLDP MBB Capability      : Off
------------------------------------------------------------------------------
Peer LDP ID         : 3.3.3.3:0
Peer Max PDU Length : 4096         Peer Transport Address   : 3.3.3.3
Peer Loop Detection : Off          Peer Path Vector Limit   : ----
Peer FT Flag        : Off          Peer Keepalive Timer     : 45 Sec
Recovery Timer      : ----         Reconnect Timer          : ----
Peer Type           : Local
Peer Label Advertisement Mode : Downstream Unsolicited
Peer Discovery Source         : Vlanif100
Peer Deletion Status          : No
Capability-Announcement       : Off
Peer mLDP P2MP Capability     : Off
Peer mLDP MBB Capability      : Off
------------------------------------------------------------------------------
```

Table 9-32 Description of the display mpls ldp peer verbose command output

Item	Description
Peer LDP ID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: - 0: per-platform label space. - Non-0: per-interface label space.
Peer Max PDU Length	Maximum size of a PDU sent by an LDP peer.
Peer Transport Address	Transport address of an LDP peer. The transport address is used to set up TCP connections.
Peer Loop Detection	Whether loop detection of an LDP peer is enabled: - On: Loop detection is enabled. - Off: Loop detection is disabled. To configure the loop detection function, run the **loop-detect** command.
Peer Path Vector Limit	Indicates the upper limit of the Path Vector for an LDP peer. To set the upper limit of the Path Vector for an LDP peer, run the **path-vectors** command.
Peer FT Flag	GR FT flag of an LDP peer: - On: LDP GR is enabled. - Off: LDP GR is disabled. The flag can only be set after an Initialization message containing an FT TLV is received.

Item	Description
Peer Keepalive Timer	Configured value of the Keepalive timer on an LDP peer. To set the value of the Keepalive timer, run the **mpls ldp timer keepalive-hold** command.
Recovery Timer	Timeout period of the Recovery timer of an LDP peer. The value of the Recovery Timer field is not null only when the Peer FT Flag field is On. To set the timeout period of the Recovery timer, run the **graceful-restart timer recovery** command.
Reconnect Timer	Timeout period of the Reconnect timer of an LDP peer. The value of the Recovery Timer field is not null only when the Peer FT Flag field is On. To set the timeout period of the Reconnect timer, run the **graceful-restart timer reconnect** command.
Peer Type	Type of an LDP peer: ● Local ● Remote ● Local&Remote
Peer Label Advertisement Mode	Indicates the label advertisement mode of an LDP peer: ● Downstream Unsolicited ● Downstream on Demand The switch supports the Downstream Unsolicited (DU) mode.
Peer Discovery Source	Discovery source of an LDP peer: ● If the interface is displayed, the source of the local LDP peer is the local interface. ● If the configuration name of the remote peer is displayed, the source end of the remote LDP peer is the remote peer.
Peer Deletion Status	Deletion status of an LDP peer: ● Yes: LDP peer is being deleted. ● No: LDP peer is not being deleted.

Item	Description
Capability-Announcement	Status of the LDP dynamic capability announcement function: - On: LDP dynamic capability announcement is enabled. - Off: LDP dynamic capability announcement is disabled. **NOTE** The switch does not support this parameter.
Peer mLDP P2MP Capability	Whether the LDP peer supports mLDP P2MP: - On: The LDP peer supports mLDP P2MP. - Off: The LDP peer does not support mLDP P2MP.
Peer mLDP MBB Capability	Whether the LDP peer supports make-before-break: - On: The LDP peer supports mLDP make-before-break. - Off: The LDP peer does not support mLDP make-before-break.

9.1.34 display mpls ldp peer statistics

Function

The **display mpls ldp peer statistics** command displays statistics about LDP peers.

Format

display mpls ldp peer statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp peer statistics** command to view the number of local LDP peers, remote LDP peers, and coexistent local and remote LDP peers.

Example

Display statistics about LDP peers.

```
<HUAWEI> display mpls ldp peer statistics

 LDP Peer Statistics Information
 ------------------------------------------------------------
 PeerType        Local   Remote   Local&Remote   Total
 ------------------------------------------------------------
 PeerNumber      0       1        1              2
 ------------------------------------------------------------
```

Table 9-33 Description of the display mpls ldp peer statistics command output

Item	Description
PeerType	Type of LDP peers.
PeerNumber	Number of LDP peers.
Local	Number of local LDP peers.
Remote	Number of remote LDP peers.
Local&Remote	Number of coexistent local and remote LDP peers.
Total	Total number of all types of LDP peers.

9.1.35 display mpls ldp remote-peer

Function

The **display mpls ldp remote-peer** command displays information about a remote LDP peer.

Format

display mpls ldp remote-peer [*remote-peer-name* | **peer-id** *lsr-id*]

Parameters

Parameter	Description	Value
remote-peer-name	Specifies the name of a remote LDP peer.	The value is an existing remote LDP peer.
peer-id *lsr-id*	Specifies the LSR ID of a remote LDP peer.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Remote LDP peers are used to set up remote LDP sessions to transmit VPN services.

To view information about the configured remote LDP peers, run the **display mpls ldp remote-peer** command.

Run the **display mpls ldp remote-peer** command to view information about the configured remote LDP peer. Different from the **display mpls ldp peer** command, the **display mpls ldp remote-peer** command is used to view the remote LDP peer that is configured on the local device if the configuration takes effect. The **display mpls ldp peer** command is used to view the LDP peer discovered by the local device only when the LDP peers are configured on local and peer devices and the LDP peer relationship is set up.

Example

Display information about remote LDP peers.

```
<HUAWEI> display mpls ldp remote-peer

                         LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name  : lsrc
 Remote Peer IP    : 3.3.3.9           LDP ID        : 1.1.1.9:0
 Transport Address : 1.1.1.9           Entity Status : Active

 Configured Keepalive Hold Timer : 45 Sec
 Configured Keepalive Send Timer : ---
 Configured Hello Hold Timer     : 45 Sec
 Negotiated Hello Hold Timer     : 45 Sec
 Configured Hello Send Timer     : ---
 Configured Delay Timer          : 10 Sec
 Hello Packet sent/received      : 61/59
 Label Advertisement Mode        : Downstream Unsolicited
 Remote Peer Deletion Status     : No
 Auto-config                     : ---
------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.
```

Table 9-34 Description of the **display mpls ldp remote-peer** command output

Item	Description
Remote Peer Name	Name of a remote LDP peer.
Remote Peer IP	IP address of a remote LDP peer.
LDP ID	Local LDP ID.
Transport Address	Transport address, which is used to set up the LDP session between the local and remote peers.

Item	Description
Entity Status	Status of a remote LDP peer: - Active - Inactive
Configured Keepalive Hold Timer	Timeout period of the configured Keepalive hold timer.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Configured Hello Hold Timer	Timeout period of the configured Hello hold timer.
Negotiated Hello Hold Timer	Timeout period of the negotiated Hello hold timer.
Configured Hello Send Timer	Timeout period of the configured Hello send timer.
Configured Delay Timer	Timeout period of the Delay timer, which, in LDP and IGP synchronization, is the time that an interface waits to establish an LSP after an LDP session is established.
Hello Packet sent/received	Number of sent and received Hello packets.
Label Advertisement Mode	Label advertisement mode in an LDP session. The default mode is DU. To set the label advertisement mode, run the **mpls ldp advertisement** command.
Remote Peer Deletion Status	Deletion status of an LDP peer: - Yes: The LDP peer is being deleted. - No: The LDP peer is not being deleted.
Auto-config	Source that triggers the creation of a remote peer: - ---: created using LDP configurations. - L2VPN: After an L2VPN is configured, the remote LDP peer is automatically configured. LDP configurations can also be involved. - RLFA: created using remote LFA. - Auto Accept: The remote LDP session is automatically established after a local device receives Targeted Hello messages.

9.1.36 display mpls ldp session

Function

The **display mpls ldp session** command displays information about LDP sessions.

Format

display mpls ldp session [*peer-id* | [**all**] [**verbose**]]

Parameters

Parameter	Description	Value
peer-id	Displays information about LDP sessions of a specified LSR ID.	The value is in dotted decimal notation.
all	Displays information about all LDP sessions.	-
verbose	Displays detailed information about LDP sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After creating an LDP session, run the **display mpls ldp session** command to verify that the LDP session is created successfully and view information about the LDP session, such as the number of sent or received Keepalive messages.

Prerequisites

MPLS has been enabled globally using the **mpls** command, and MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If you run the **display mpls ldp session** command without specifying any parameter, information about all LDP sessions is displayed.

Example

Display information about all LDP sessions.

```
<HUAWEI> display mpls ldp session
 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID             Status      LAM  SsnRole  SsnAge      KASent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0          Operational DU   Passive  0000:01:36  387/386
 3.3.3.3:0          Operational DU   Passive  0000:01:30  361/361
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.
```

Table 9-35 Description of the display mpls ldp session command output

Item	Description
PeerID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.
Status	Status of an LDP session: ● NonExistent: LDP peers at both ends of the LDP session exchange Hello messages to negotiate a TCP connection. After the TCP connection is established, the LDP session enters the Initialized state. The Non-Existent state is the initial state in the LDP session state machine. ● Initialized: The LDP session is in the initialization state. ● Open Sent: The LSR playing the active role in the LDP session sends an Initialization message to the LSR playing the passive role and waits for a reply during initialization. ● Open Recv: LDP peers at both ends of the LDP session wait for receiving a Keepalive message from each other during initialization. If they receive a Keepalive message from each other, the LDP session enters the Operational state. ● Operational: An LDP session is established successfully.
LAM	Label advertisement mode of an LDP peer. The default mode is DU. To set the label advertisement mode, run the **mpls ldp advertisement** command.

Item	Description
SsnRole	Role that an LSR plays in an LDP session: - Active: an LSR with a larger LSR ID between two LSRs. - Passive: an LSR with a smaller LSR ID between two LSRs.
SsnAge	Time elapsed since an LDP session was set up in DDDD:HH:MM format.
KASent/Rcv	Number of Keepalive messages sent and received by an LDP session.

Display detailed information about all LDP sessions.

```
<HUAWEI> display mpls ldp session verbose

 LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer LDP ID      : 2.2.2.2:0           Local LDP ID    : 1.1.1.1:0
 TCP Connection   : 1.1.1.1 <- 2.2.2.2
 Session State    : Operational          Session Role    : Passive
 Session FT Flag  : Off                  MD5 Flag        : Off
 Reconnect Timer  : ---                  Recovery Timer  : ---
 Keychain Name    : kc1
 Authentication applied:---

 Negotiated Keepalive Hold Timer   : 45 Sec
 Configured Keepalive Send Timer   : 3 Sec
 Keepalive Message Sent/Rcvd       : 438/438 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 0000:01:49 (DDDD:HH:MM)
 Session Deletion Status           : No

 Capability:
  Capability-Announcement           : On
  mLDP P2MP Capability              : Off
  mLDP MP2MP Capability             : Off
  mLDP MBB Capability               : Off

 Outbound&Inbound Policies applied : NULL

 Addresses received from peer: (Count: 3)
 10.1.1.2           2.2.2.2            10.1.2.1
 ------------------------------------------------------------------------------
```

Table 9-36 Description of the display mpls ldp session verbose command output

Item	Description
Peer LDP ID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: - 0: per-platform label space. - 1: per-interface label space.

Item	Description
Local LDP ID	Local LDP identifier in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.
TCP Connection	TCP connection of an LDP session: ● The LSR with a larger LSR ID value plays an active role in establishing the TCP connection. ● The LSR with a smaller LSR ID value plays a passive role in establishing the TCP connection.
Session State	Status of an LDP session: ● NonExistent: LDP peers at both ends of the LDP session exchange Hello messages to negotiate a TCP connection. After the TCP connection is established, the LDP session enters the Initialized state. The Non-Existent state is the initial state in the LDP session state machine. ● Initialized: The LDP session is in the initialization state. ● Open Sent: The LSR playing the active role in the LDP session sends an Initialization message to the LSR playing the passive role and waits for a reply during initialization. ● Open Recv: LDP peers at both ends of the LDP session wait for receiving a Keepalive message from each other during initialization. If they receive a Keepalive message from each other, the LDP session enters the Operational state. ● Operational: An LDP session is established successfully.
Session Role	Role that an LSR plays in an LDP session: ● Active: an LSR with a larger LSR ID between two LSRs. ● Passive: an LSR with a smaller LSR ID between two LSRs.

Item	Description
Session FT Flag	Negotiated LDP GR capability: - On: Negotiated LDP GR capability is enabled. - Off: Negotiated LDP GR capability is disabled.
MD5 Flag	MD5 authentication flag: - On: MD5 authentication is enabled during the TCP connection establishment. - Off: MD5 authentication is disabled during the TCP connection establishment.
Reconnect Timer	Negotiated timeout period of the Reconnect timer. The value of the Recovery Timer field is not null only when the Session FT Flag field is On.
Recovery Timer	Negotiated timeout period of the Recovery timer. The value of the Recovery Timer field is not null only when the Session FT Flag field is On.
Keychain Name	Referenced keychain authentication name.
Authentication applied	Existing authentication mode: - Peer: single peer authentication - Peer-group PeerGroupName: peer-group authentication. PeerGroupName indicates a peer group name. - ALl: All authentication
Negotiated Keepalive Hold Timer	Negotiated value of the Keepalive hold timer, which is the smallest value of the Keepalive hold timers configured on the local and remote LDP peers.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Keepalive Message Sent/Rcvd	Number of Keepalive messages sent and received by an LDP session.

Item	Description
Label Advertisement Mode	Label advertisement mode: ● Downstream Unsolicited ● Downstream on Demand The default mode is Downstream Unsolicited (DU). To set the label advertisement mode, run the **mpls ldp advertisement** command.
Label Resource Status(Peer/ Local)	Label resource status of the remote and local peers.
Session Age	Time elapsed since an LDP session was set up.
Session Deletion Status	Deletion status of an LDP session: ● Yes: The LDP session is being deleted. ● No: The LDP session is not being deleted.
Capability	LDP capability.
Capability-Announcement	LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled. **NOTE** The switch does not support this parameter.
mLDP P2MP Capability	Whether mLDP P2MP is supported after a session is negotiated: ● On: mLDP P2MP is supported. ● Off: mLDP P2MP is not supported. **NOTE** The switch does not support this parameter.
mLDP MP2MP Capability	Whether mLDP MP2MP is supported after a session is negotiated: ● On: mLDP MP2MP is supported. ● Off: mLDP MP2MP is not supported. **NOTE** The switch does not support this parameter.

Item	Description
mLDP MBB Capability	Whether mLDP make-before-break is supported after a session is negotiated: ● On: mLDP make-before-break is supported. ● Off: mLDP make-before-break is not supported. **NOTE** The switch does not support this parameter.
Outbound&Inbound Policies applied	Outbound and inbound policies on the local node.
Addresses received from peer	Contents of an Address message sent by an LDP peer. The contents include the LSR ID of the peer and the IP address of the LDP-enabled interface.

9.1.37 display mpls ldp session statistics

Function

The **display mpls ldp session statistics** command displays statistics about sessions between LDP peers.

Format

display mpls ldp session statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp session statistics** command to view the number of sessions between LDP peers. Statistics are collected based on the session type and status. The session type can be local, remote, or coexistent local and remote. The session status can be Not Operational or Operational.

Example

Display statistics about LDP sessions.

```
<HUAWEI> display mpls ldp session statistics

 LDP Session Statistics Information
 ------------------------------------------------------------
 SessionType        Local   Remote   Local&Remote   Total
 ------------------------------------------------------------
 Not Operational     0       0        0              0
 Operational         0       1        1              2
 ------------------------------------------------------------
 SessionStatistics   0       1        1              2
 ------------------------------------------------------------
```

Table 9-37 Description of the display mpls ldp session statistics command output

Item	Description
SessionType	Type of LDP sessions.
Local	Number of local LDP sessions.
Remote	Number of remote LDP sessions.
Local&Remote	Number of coexistent local and remote LDP sessions.
Total	Total number of sessions.
Not Operational	Number of sessions in the Not Operational state.
Operational	Number of sessions in the Operational state.
SessionStatistics	Total number of local sessions, remote sessions, and coexistent local and remote sessions.

9.1.38 display mpls lsp

Function

The **display mpls lsp** command displays information about LSPs.

The **display mpls lsp lsp-id** command displays information about CR-LSPs only.

Format

display mpls lsp lsp-id *ingress-lsr-id session-id lsp-id* [**verbose**]

display mpls lsp [[**vpn-instance** *vpn-instance-name* [**ipv4-family** | **ipv6-family**]] [**protocol** { **bgp** | **bgp-ipv6** | **rsvp-te** | **static** | **static-cr** }] | **asbr**] [{ **exclude** | **include** } *ip-address mask-length*] [**incoming-interface** *interface-type interface-number*] [**outgoing-interface** *interface-type interface-number*]

[**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp [**vpn-instance** *vpn-instance-name* [**ipv4-family** | **ipv6-family**]] **protocol ldp** [{ **exclude** | **include** } *ip-address mask-length*] [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp stale-incoming-interface *interface-index* [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp stale-outgoing-interface *interface-index* [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

Parameters

Parameter	Description	Value
lsp-id	Specifies the LSP ID.	The value is an integer ranging from 0 to 65535.
ingress-lsr-id	Specifies the ID of the ingress LSR.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer ranging from 0 to 65535.
vpn-instance *vpn-instance-name*	Displays detailed configurations of LSPs of a specified VPN instance.	The value must be an existing VPN instance name.
ipv4-family	Indicates the IPv4 unicast address-family.	-
ipv6-family	Indicates the IPv6 unicast address-family.	-
protocol	Displays information about LSPs of a specified type.	-
ldp	Indicates LDP.	-
bgp	Indicates BGP.	-
bgp-ipv6	Indicates BGP IPv6.	-

Parameter	Description	Value
rsvp-te	Indicates RSVP-TE.	-
static	Indicates Static.	-
static-cr	Indicates Static-CR.	-
asbr	Displays information about LSPs of a specified ASBR.	-
exclude	Displays information about LSPs, excluding information about the specific FEC.	-
include	Displays information about LSPs, including information about the specific FEC.	-
ip-address	Displays information about LSPs of a specified IPv4 address or a specified IPv6 address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the specified IPv4 address or a specified IPv6 address.	The value is an integer ranging from 0 to 32. Alternatively, it specifies the mask length of the specified IPv6 address. The value is an integer ranging from 0 to 128.
incoming-interface *interface-type interface-number*	Specifies the type and number of an inbound interface. You can view the configuration of an LSP on a specified interface.	-
outgoing-interface *interface-type interface-number*	Indicates the type and number of an outbound interface. You can view the configuration of an LSP on a specified interface.	-
in-label *in-label-value*	Displays information about LSPs of a specified incoming label.	The value is an integer ranging from 0 to 1048575.
out-label *out-label-value*	Displays information about LSPs of a specified outgoing label.	The value is an integer ranging from 0 to 1048575.

Parameter	Description	Value
nexthop *ip-address*	Displays information about LSPs of a specified IPv4 or IPv6 next hop address.	The value is in dotted decimal notation.
lsr-role	Displays information about all LSPs on the current LSR that plays a specified role.	-
egress	Displays information about LSPs of an egress LSR.	-
ingress	Displays information about LSPs of an ingress LSR.	-
transit	Displays information about LSPs of a transit LSR.	-
verbose	Displays detailed information about LSPs.	-
stale-incoming-interface	Displays information about the stale inbound interface of an LSP.	-
stale-outgoing-interface	Displays information about the stale outbound interface of an LSP.	-
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer ranging from 1 to FFFFFFFE.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify a parameter, information about all LSPs is displayed.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

Display information about all types of LSPs.

```
<HUAWEI> display mpls lsp
-------------------------------------------------------------------------------
               LSP Information: RSVP LSP
-------------------------------------------------------------------------------
 FEC                In/Out Label  In/Out IF                    Vrf Name
 10.2.2.9/32        NULL/11264    -/Vlanif10

Flag after Out IF: (I) - LSP Is Only Iterated by RLFA
-------------------------------------------------------------------------------
               LSP Information: LDP LSP
-------------------------------------------------------------------------------
 FEC                In/Out Label  In/Out IF                    Vrf Name

 10.2.2.9/32        NULL/3         -/Vlanif10
 10.2.2.9/32        1024/3        -/Vlanif10
 10.3.3.9/32        NULL/3         -/Vlanif20
 10.3.3.9/32        1025/3        -/Vlanif20
```

Display information about all LSPs with the next hop of 192.168.1.1.

```
<HUAWEI> display mpls lsp nexthop 192.168.1.1

Flag after Out IF: (I) - LSP Is Only Iterated by RLFA
-------------------------------------------------------------------------------
           LSP Information: L3VPN Label-Per-Nexthop LSP
-------------------------------------------------------------------------------
IndirectID  NextHop           In/Out Label  In/Out IF      Vrf Name
0x1         192.168.1.1       13312/13312   -/-            ASBR LSP
```

Display detailed information about all types of LSPs.

```
<HUAWEI> display mpls lsp verbose
-------------------------------------------------------------------------------
               LSP Information: RSVP LSP
-------------------------------------------------------------------------------

 No                  :  1
 SessionID           :  300
 IngressLsrID        :  10.1.1.9
 LocalLspID          :  1
 Tunnel-Interface    :  Tunnel1
 Fec                 :  10.2.2.9/32
 TunnelTableIndex    :  0x1
 Nexthop             :  10.5.1.2
 In-Label            :  NULL
 Out-Label           :  11264
 In-Interface        :  ----------
 Out-Interface       :  Vlanif10
 LspIndex            :  3072
 Token               :  0x8002008
 LsrType             :  Ingress
 Mpls-Mtu            :  1500
 TimeStamp           :  1171sec
 Bfd-State           :  ---
 CBfd-Event          :  0x0
 Bed-State           :  ---
 Bed-LastNotifyValue :  ---
 Bed-LastNotifyLspId :  ---
 Flag after FEC: (I) - LSP Is Only Iterated by RLFA
-------------------------------------------------------------------------------
               LSP Information: LDP LSP
-------------------------------------------------------------------------------
 No                  :  2
 VrfName             :
 Fec                 :  10.2.2.2/32
```

```
Nexthop            :  10.1.1.2
In-Label           :  NULL
Out-Label          :  3
In-Interface       :  ----------
Out-Interface      :  Vlanif10
LspIndex           :  9217
Token              :  0x802009
FrrToken           :  0x0
LsrType            :  Ingress
Outgoing token     :  0x0
Label Operation    :  PUSH
Mpls-Mtu           :  ------
TimeStamp          :  21086sec
Bfd-State          :  ---
BGPKey             :  -----

No                 :  3
VrfName            :
Fec                :  10.2.2.2/32
Nexthop            :  10.2.1.2
In-Label           :  NULL
Out-Label          :  3
In-Interface       :  ----------
Out-Interface      :  Vlanif20
LspIndex           :  9218
Token              :  0x80200a
FrrToken           :  0x0
LsrType            :  Ingress
Outgoing token     :  0x0
Label Operation    :  PUSH
Mpls-Mtu           :  ------
TimeStamp          :  19569sec
Bfd-State          :  ---
BGPKey             :  -----
```

Table 9-38 Description of the display mpls lsp command output

Item	Description
LSP Information	LSP information: • STATIC LSP: manually created. • LDP LSP: created using LDP. • STATIC CR-LSP: a static MPLS TE tunnel created manually. • RSVP LSP: an MPLS TE tunnel created using RSVP-TE. • BGP LSP: an LSP created using BGP based on private or public IPv4 BGP routes. • L3VPN LSP: an LSP based on IPv4 VPN routes received by means of BGP. • BGP IPV6 LSP: an LSP based on private-network IPv6 routes received by means of BGP. • L3VPN IPV6 LSP: an LSP based on IPv6 VPN routes received by means of BGP.
FEC/Fec	Forwarding equivalence class. Usually, the value is the destination address of an LSP.
In/Out Label	Values of the incoming and outgoing labels.

Item	Description
In/Out IF	Names of the incoming and outbound interfaces.
Vrf Name	Name of a VPN instance.
IndirectID	Index of the next hop of a BGP route.
No	Serial number of an LSP.
SessionID	Session ID of a CR-LSP.
IngressLsrID	Ingress LSR ID of a CR-LSP.
LocalLspID	Local LSP ID of a CR-LSP.
Tunnel-Interface	Tunnel interface.
VrfName	Name of a VPN instance. This value is available for only non-CR-LSPs.
Nexthop	IP address of the next hop of an LSP.
TunnelTableIndex	Index of a tunnel table.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Name of an inbound interface.
Out-Interface	Name of an outbound interface.
LspIndex	Index number of an LSP, which uniquely identifies an LSP that is established using a specific protocol.
Token	LSP token. It guides the packet forwarding.
FrrToken	Token of a standby LDP LSP. This value is available for only non-CR-LSPs.
LsrType	Role of an LSR on an LSP: ● Ingress ● Transit ● Egress
Outgoing token	Token that guides the packet forwarding, which is available for only non-CR-LSPs.
Label Operation	Type of a label operation, which is available for only non-CR-LSPs: ● PUSH ● SWAP ● POP ● SWAPPUSH

Item	Description
Mpls-Mtu	Maximum transmission unit (MTU) of an interface of an LSP.
TimeStamp	Time elapsed since an LSP was set up.
Bfd-State	BFD status.
CBfd-Event	Error code event that BFD reports to the RSVP LSP on the ingress node.
Bed-State	Error code status of an RSVP LSP on the ingress node.
Bed-LastNotifyValue	Error code association of which the RSVP LSP notifies BFD on the egress node.
Bed-LastNotifyLspId	ID of the reversed LSP that corresponds to the error code association event on the egress node. The association event is notified of BFD by the RSVP LSP.
BGPKey	Index of BGP.

9.1.39 display mpls lsp statistics

Function

The **display mpls lsp statistics** command displays statistics about the LSPs that are in the Up state and the number of the LSPs that are activated on the ingress, transit, and egress nodes.

Format

display mpls lsp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls lsp statistics** command to view statistics about the LSPs and CR-LSPs that are in the Up state.

To view detailed information about the LSPs and CR-LSPs, run the **display mpls lsp** command.

Example

Display statistics about LSPs.

```
<HUAWEI> display mpls lsp statistics
Lsp Type       Total     Ingress   Transit   Egress
STATIC LSP     0         0         0         0
STATIC CRLSP   0         0         0         0
LDP LSP        4         3         0         1
RSVP CRLSP     0         0         0         0
BGP LSP        1         0         0         1
ASBR LSP       0         0         0         0
BGP IPV6 LSP   0         0         0         0
L3VPN IPV6 LSP 0         0         0         0
-------------------------------------------------------------------------
LSP            5         3         0         2
CRLSP          0         0         0         0
-------------------------------------------------------------------------
Lsp Type       IngressLspBypassState         TransitLspBypassState
               ExistNotUsed   InUse          ExistNotUsed   InUse
RSVP CRLSP     0              0              0              0
-------------------------------------------------------------------------
```

Table 9-39 Description of the display mpls lsp statistics command output

Item	Description
Lsp Type	Type of an LSP: - STATIC LSP: a static LSP. - STATIC CRLSP: a static CR-LSP. - LDP LSP: created using LDP. - RSVP CRLSP: an MPLS TE tunnel created using RSVP-TE. - BGP LSP: an LSP created using BGP based on private or public IPv4 BGP routes. - ASBR LSP: created using BGP based on received IPv4 VPN route. - BGP IPV6 LSP: an LSP created using BGP based on private IPv6 routes. - L3VPN IPV6 LSP: created using BGP based on received IPv6 VPN routes. - LSP: Label Switched Path. - CRLSP: Constraint-based Routed Label Switched Path.
Total	Number of LSPs of a specific type.
Ingress	Number of LSPs on the local ingress LSR.

Item	Description
Transit	Number of LSPs on the local transit LSR.
Egress	Number of LSPs on the local egress LSR.
IngressLspBypassState	State of the ingress LSP enabled with FRR: - ExistNotUsed: Bypass LSP that is bound to the primary LSP but has no traffic. - InUse: Traffic switched to the bypass LSP.
TransitLspBypassState	State of the Transit LSP enabled with FRR: - ExistNotUsed: Bypass LSP that is bound to the primary LSP but has no traffic. - InUse: Traffic switched to the bypass LSP.

9.1.40 display mpls route-state

Function

The **display mpls route-state** command displays routing information about a dynamic LSP.

Format

display mpls route-state [**vpn-instance** *vpn-instance-name*] [{ **exclude** | **include** } { **idle** | **ready** | **settingup** } * | *destination-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
exclude	Displays routing information excluding the specified route.	-

Parameter	Description	Value
include	Displays information about a specified route.	-
idle	Indicates that a route is not used to establish an LSP.	-
ready	Indicates that a route has been used to establish an LSP.	-
settingup	Indicates that a signaling protocol is creating an LSP.	-
destination-address	Specifies the destination address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a specified destination address.	The value is an integer ranging from 0 to 32.
verbose	Displays detailed routing information about an LSP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing LDP LSP configurations, run the **display mpls ldp lsp** command to view information about an LDP LSP. If the command output displays no information about the LDP LSP, run the **display mpls route-state** command to view LDP LSP routing information.

Precautions

Only routing states of the LSPs that are set up based on dynamic signaling protocols can be changed. Therefore, the **display mpls route-state** command displays only routing states of dynamic LSPs, but not routing information about static LSPs.

Example

Display detailed information about routes of dynamic LSPs.

```
<HUAWEI> display mpls route-state verbose

Codes: B(BGP), I(IGP), L(Public Label BGP), O(Original BGP), U(Unknown)
-------------------------------------------------------------------------------
Dest/Mask         Next-Hop       Out-Interface        State    LSP   VRF Type
-------------------------------------------------------------------------------
10.21.21.21/32    10.22.22.21    Vlanif100            READY    2     0   I
     LspIndex: 30720     InLabel: NULL      OutLabel: 3
     LspIndex: 32728     InLabel: 1024      OutLabel: 3
10.0.0.6/32       10.21.22.21    Vlanif100            READY    1     0   I
     LspIndex: 33053     InLabel: NULL      OutLabel: 3338
```

Table 9-40 Description of the display mpls route-state verbose command output

Item	Description
Dest/Mask	Destination IP address and mask length.
Next-Hop	Next hop IP address.
Out-Interface	Outbound interface.
State	Routing state of the MPLS control plane: ● IDLE: The route is not used to establish an LSP. ● SETTINGUP: A signaling protocol is creating an LSP. ● READY: The route has been used to establish an LSP. Static LSPs are only in READY state.
LSP	Number of LSPs reachable to the destination address. If the displayed value is not 0, there are LSPs reachable to the destination address and LSP information about these LSPs is also displayed.
VRF	Index of a VPN instance. The value 0 indicates the public network.
Type	Route type: ● B: BGP routes ● I: IGP routes ● L: labeled BGP routes of a public network ● O: original BGP routes ● U: unidentified routes (such as multicast routes)
LspIndex	Index of an LSP established using the route.
InLabel	Incoming label of an LSP established using the route. If NULL is displayed, the current node is the ingress node of the LSP; if a number is displayed, the current node is the transit or egress node of the LSP.
OutLabel	Outgoing label of an LSP established using the route.

9.1.41 display mpls static-lsp

Function

The **display mpls static-lsp** command displays information about static LSPs.

Format

display mpls static-lsp [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is an existing static LSP name.
include	Displays information about LSPs, including information about the specific FEC.	-
exclude	Displays information about LSPs, excluding information about the specific FEC.	-
ip-address	Specifies the destination IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the length of an IPv4 mask.	The value is an integer ranging from 0 to 32.
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Static LSPs are configured locally, so you need to run the **ping lsp** command to check whether the static LSP can work normally. If the static LSP cannot work normally, run the **display mpls static-lsp** command to view information about static LSPs.

Example

Display brief information about static LSPs.

```
<HUAWEI> display mpls static-lsp
TOTAL          : 1       STATIC LSP(S)
```

```
UP              : 1       STATIC LSP(S)
DOWN            : 0       STATIC LSP(S)
Name       FEC              I/O Label  I/O If               Status
lsp1       3.3.3.9/32       NULL/100   -/Vlanif100          Up
```

Table 9-41 Description of the display mpls static-lsp command output

Item	Description
TOTAL	Total number of static LSPs.
UP	Number of static LSPs that are in the Up state.
DOWN	Number of static LSPs that are in the Down state.
Name	Name of an LSP.
FEC	Destination IP address and mask length of an LSP.
I/O Label	Incoming and outgoing labels.
I/O If	Incoming and outbound interfaces.
Status	Current status of an LSP: ● Up ● Down

Display detailed information about static LSPs.

```
<HUAWEI> display mpls static-lsp verbose
No              : 1
LSP-Name        : lsp1
LSR-Type        : Ingress
FEC             : 3.3.3.9/32
In-Label        : NULL
Out-Label       : 100
In-Interface    : -
Out-Interface   : Vlanif100
NextHop         : 10.1.1.2
Static-Lsp Type: Normal
Lsp Status      : Up
```

Table 9-42 Description of the display mpls static-lsp verbose command output

Item	Description
No	Serial number.
LSP-Name	Name of an LSP.
LSR-Type	Role of the current LSR on a static LSP: ● Ingress ● Transit ● Egress
FEC	Destination IP address and mask length of an LSP.

Item	Description
In-Label	Incoming label.
Out-Label	Outgoing label.
In-Interface	Inbound interface.
Out-Interface	Outbound interface.
NextHop	Next hop IP address.
Static-Lsp Type	Type of a static LSP.
Lsp Status	LSP status: ● Up ● Down

9.1.42 display ospf ldp-sync interface

Function

The **display ospf ldp-sync interface** command displays the status of LDP and OSPF synchronization on an interface.

Format

display ospf ldp-sync interface { **all** \| *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays information about the synchronization status on all interfaces enabled with LDP and OSPF synchronization.	-
interface-type interface-number	Displays information about the synchronization status on a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

For all interfaces that are enabled with LDP and OSPF synchronization, run the **display ospf ldp-sync interface** command to view information about the status of LDP and OSPF synchronization.

Example

Display information about the status of LDP and OSPF synchronization on a specified interface.

```
<HUAWEI> display ospf ldp-sync interface vlanif 100
 Interface Vlanif100   HoldDown Timer: 9         HoldMaxCost Timer: 50
 LDP State: Up             OSPF Sync State: Sync-Achieved
```

Table 9-43 Description of the display ospf ldp-sync interface command output

Item	Description
Interface	Interface connected to neighbors.
HoldDown Timer	Interval at which the interface waits to create an LDP session without creating the OSPF neighbor relationship. The default interval is 10 seconds. To set the interval at which the interface waits to create an LDP session without creating the OSPF neighbor relationship, run the **ospf timer ldp-sync hold-down** command.
HoldMaxCost Timer	Interval at which OSPF advertises the maximum metric in LSAs sent by the local device. The default interval is 10 seconds. To set the interval at which OSPF advertises the maximum metric in LSAs sent by the local device, run the **ospf timer ldp-sync hold-max-cost** command. **NOTE** If the value of this field is **infinite**, OSPF keeps advertising the maximum metric value in LSAs sent by the local device before the LDP session is reestablished.
LDP State	Status of an LDP session: ● Up ● Down

Item	Description
OSPF Sync State	Status of LDP and OSPF synchronization: ● Sync-Achieved: The creation of an LDP session and establishment of the OSPF neighbor relationship are synchronized. ● HoldDown: The interface is waiting to create an LDP session without creating the OSPF neighbor relationship. ● HoldMaxCost: OSPF advertises the maximum metric in LSAs or LSPs sent by the local device. ● Init: the initial state.

9.1.43 display static-route ldp-sync

Function

The **display static-route ldp-sync** command displays information about the outbound interface of a static route configured with synchronization between LDP and static routes.

Format

display static-route ldp-sync [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display static-route ldp-sync** command to view synchronization between LDP and static routes to diagnose faults in static routes.

- If no outbound interface is specified, information about all outbound interfaces of the static routes configured with synchronization between LDP and static routes is displayed.

- If an outbound interface is specified, information about the specified outbound interface of the static routes configured with synchronization between LDP and static routes is displayed.

Example

Display information about the outbound interface of the static route configured with synchronization between LDP and static routes.

```
<HUAWEI> display static-route ldp-sync
Total number of routes enable Ldp-Sync: 2
-----------------------------------------------------
Interface GigabitEthernet0/0/1
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 20s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 10.1.1.1.
-----------------------------------------------------
Interface GigabitEthernet0/0/2
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 10s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 20.1.1.1.
-----------------------------------------------------
```

Table 9-44 Description of the display static-route ldp-sync command output

Item	Description
Total number of routes enable Ldp-Sync	Number of static routes configured with synchronization between LDP and static routes.
Interface GigabitEthernet0/0/1	Outbound interface of the static route configured with synchronization between LDP and static routes.
Enable ldp-sync static routes number	Number of static routes enabled with synchronization between LDP and static routes, with an outbound interface of GE1/0/0.
Static-route ldp-sync holddown timer	Time during which the static route remains inactive and waits for an LDP session to be established.
Sync state	Status of synchronization between LDP and static routes: ● Normal ● HoldDown
Dest	Destination address of the static route.
Mask	Mask length of the destination address of the static route.
NextHop	Next hop address of the static route.

9.1.44 fec-list

Function

The **fec-list** command creates a FEC list used in dynamic BFD for LDP LSP.

The **undo fec-list** command deletes a FEC list.

By default, no FEC list is created.

Format

fec-list *list-name*

undo fec-list *list-name*

Parameters

Parameter	Description	Value
list-name	Specifies the name of a FEC list.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a BFD session is established based on the FEC list, run the **fec-list** command to create a FEC list. Run the **fec-node** command to specify a host route to trigger the establishment of BFD sessions.

Only a single FEC list can be configured globally.

Example

Create FEC list 1.

```
<HUAWEI> system-view
[HUAWEI] fec-list 1
```

9.1.45 fec-node

Function

The **fec-node** command adds an FEC node.

The **undo fec-node** command deletes an FEC node.

By default, no FEC node is created.

Format

fec-node *ip-address* [**nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number*]*

undo fec-node *ip-address* [**nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number*]*

Parameters

Parameter	Description	Value
ip-address	Specifies the FEC address.	The value is in dotted decimal notation.
nexthop *ip-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

FEC-list view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the establishment of BFD sessions is triggered in FEC list mode, the system sets up BFD sessions for the added FEC nodes.

Prerequisites

An FEC list has been created by running the **fec-list** command.

Example

Create FEC nodes in the FEC list.

```
<HUAWEI> system-view
[HUAWEI] fec-list 1
[HUAWEI-fec-list-1] fec-node 10.1.1.1 nexthop 10.2.1.1 outgoing-interface vlanif 100
```

9.1.46 graceful-restart (MPLS-LDP view)

Function

The **graceful-restart** command enables LDP GR.

The **undo graceful-restart** command disables LDP GR.

By default, LDP GR is disabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LDP GR mode, when AMB/SMB switchover or protocol restart occurs on the neighboring device of the local device, the local device (GR helper) helps the device (restarter) to restart without interrupting packet forwarding.

If LDP GR is not enabled, during the AMB/SMB switchover or upgrade, the neighboring device deletes the LSP because the session is in the Down state. As a result, the traffic is interrupted in a short time. If LDP GR is enabled, the labels before and after unexpected AMB/SMB switchover or protocol restart can be consistent, and uninterrupted MPLS forwarding is ensured.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp(system view)** command in the system view.

Precautions

Enabling or disabling GR causes the reestablishment of all LDP sessions.

LDP GR must be enabled on both the GR Restarter and Helper.

Example

Enable LDP GR.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.47 graceful-restart timer neighbor-liveness

Function

The **graceful-restart timer neighbor-liveness** command sets the value of the Neighbor-liveness timer.

The **undo graceful-restart timer neighbor-liveness** command restores the default setting.

By default, the value of the Neighbor-liveness timer is 600 seconds.

Format

graceful-restart timer neighbor-liveness *time*

undo graceful-restart timer neighbor-liveness

Parameters

Parameter	Description	Value
time	Specifies the value of the Neighbor-liveness timer.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The value of the neighbor-liveness timer defines the LDP GR period.

During LDP GR, the reestablishment time of the LDP session is negotiated as the smaller value between the value of the neighbor-liveness timer on the GR helper and the value of the Reconnect timer on the GR restarter.

In general, the default value of the timer is recommended. When the number of LSPs on a network is small, you can set a smaller value for the neighbor-liveness timer to shorten the GR period.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the neighbor-liveness timer causes the reestablishment of all the LDP sessions.

Example

Set the value of the Neighbor-liveness timer to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[HUAWEI-mpls-ldp] graceful-restart timer neighbor-liveness 500
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.48 graceful-restart timer reconnect

Function

The **graceful-restart timer reconnect** command sets the value of the Reconnect timer of an LDP session.

The **undo graceful-restart timer reconnect** command restores the default setting.

By default, the Reconnect timer is set to 300 seconds.

Format

graceful-restart timer reconnect *time*

undo graceful-restart timer reconnect

Parameters

Parameter	Description	Value
time	Specifies the value of a Reconnect timer of an LDP session.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the GR restarter performs the active/standby switchover, the GR helper detects that the LDP session with the GR restarter fails, and then starts the Reconnect timer and waits for the reestablishment of the LDP session.

- If no LDP session between the GR helper and the GR restarter has been established after the Reconnect timer times out, the GR helper immediately deletes the MPLS forwarding entries associated with the GR restarter and exits from the GR help process.
- If the LDP session between the GR helper and the GR restarter is established before the Reconnect timer times out, the GR helper deletes the timer and starts the Recovery timer.

During LDP GR, when the reestablishment time of the LDP session is negotiated, the value of the Reconnect timer that actually takes effect on the local end is the smaller value between the value of the neighbor-liveness timer on the GR helper and the value of the Reconnect timer on the GR restarter.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the Reconnect timer causes the reestablishment of all the LDP sessions.

Example

Set the time of the Reconnect timer of an LDP session to 270 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[HUAWEI-mpls-ldp] graceful-restart timer reconnect 270
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.49 graceful-restart timer recovery

Function

The **graceful-restart timer recovery** command sets the value of the LSP Recovery timer.

The **undo graceful-restart timer recovery** command restores the default setting.

By default, the LSP Recovery timer is set to 300 seconds.

Format

graceful-restart timer recovery *time*

undo graceful-restart timer recovery

Parameters

Parameter	Description	Value
time	Specifies the value of an LSP Recovery timer.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the LDP session is reestablished, the GR helper starts the Recovery timer and waits for the recovery of the LSP.

- If the Recovery timer times out, the GR helper considers that the GR process is complete on the GR restarter and deletes the unrecovered LSPs.
- If all the LSPs recover before the Recovery timer times out, the GR helper considers that the GR process is complete on the GR restarter only after the Recovery timer times out.

When a network with a large number of routes is faulty, run the **graceful-restart timer recovery** command to increase the value of the Recovery timer to ensure that all the LSPs recover within the timeout period of the timer.

During the LDP GR process, the value of the LSP Recovery timer that actually takes effect on the local end is negotiated as the smaller one of the values of the LSP Recovery timers configured on both ends of an LDP session.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the LSP Recovery timer causes the reestablishment of all the LDP sessions.

Example

Set the value of the LSP Recovery timer to 330 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[HUAWEI-mpls-ldp] graceful-restart timer recovery 330
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.50 gtsm peer valid-ttl-hops

Function

The **gtsm peer valid-ttl-hops** command configures the generalized TTL security mechanism (GTSM) on a specified LDP peer.

The **undo gtsm** command deletes the GTSM on all LDP peers or a specified LDP peer.

By default, no LDP peer is configured with the GTSM.

Format

gtsm peer *ip-address* **valid-ttl-hops** *hops*

undo gtsm { **all** | **peer** *ip-address* }

Parameters

Parameter	Description	Value
peer *ip-address*	Specifies the transport address of an LDP peer.	The value is in dotted decimal notation.
valid-ttl-hops *hops*	Specifies the maximum number of valid hops permitted by the GTSM.	The value is an integer ranging from 1 to 255.
all	Indicates all LDP peers.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The GTSM checks TTL values to verify packets and protect devices against attacks. LDP peers are configured with the GTSM and a valid TTL range to check TTLs in LDP packets exchanged between them. If the TTL in an LDP packet is out of the valid range, this LDP packet is considered invalid and discarded. The GTSM defends against CPU-based attacks initiated using a large number of forged packets and protects upper-layer protocols.

If the value of *hops* is set to the maximum number of valid hops permitted by GTSM, when the TTL values carried in the packets sent by an LDP peer are within the range [255 - Number of hops +1, 255], the packets are received; otherwise, the packets are discarded.

NOTE

Configuring the GTSM on both ends of an LDP session is recommended.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

The valid TTL range is from 1 to 255 or from 1 to 64, depending on the specific vendor. If a Huawei device is connected to a non-Huawei device, set *hops* to a value in a valid range that both devices support; otherwise, the Huawei device will discard packets sent by the non-Huawei device, resulting in LDP session interruption.

Example

On the LSR, set valid TTL values carried in LDP packets sent by the peer with transport address 10.1.1.1 to 254 and 255.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] gtsm peer 10.1.1.1 valid-ttl-hops 2
```

9.1.51 inbound peer fec

Function

The **inbound peer fec** command configures an inbound policy, which allows the LSR to receive Label Mapping messages for IGP routes only from a specified peer.

The **undo inbound peer fec** command restores the default setting.

By default, no inbound policy is configured.

Format

inbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec** { **none** | **host** | **ip-prefix** *prefix-name* }

undo inbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec**

undo inbound peer all

Parameters

Parameter	Description	Value
peer-id	Specifies the ID of an LDP peer.	The value is in dotted decimal notation.

Parameter	Description	Value
peer-group *peer-group-name*	Specifies the name of a peer group.	The value is an existing peer group name.
all	Indicates all LDP peers.	-
none	Forbids all Label Mapping messages. After the parameter **none** is configured, the specified LSR does not receive Label Mapping messages for IGP routes from its peers.	-
host	Allows only Label Mapping messages for host routes. After the parameter **host** is configured, the specified LSR receives only Label Mapping messages for host routes from its peers.	-
ip-prefix *prefix-name*	Allows only Label Mapping messages for IGP routes that are defined in the IP prefix list. After the parameter **ip-prefix** is configured, the specified LSR receives Label Mapping messages only for IGP routes that are defined in the IP prefix list by its peers.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an LSR receives Label Mapping messages from all LDP peers to speed up LDP LSP convergence. This leads to establishment of a great number of unwanted LSPs, which wastes resources. To reduce the number of LSPs and save memory resources, configure an inbound policy to filter out LDP LSPs not matching the policy.

When running the **inbound peer fec** command to specify the peer ID and FEC of the IGP route, configure the peer to receive only Label Mapping messages for specified IGP routes.

To apply a policy associated with the same FEC range to an LDP peer group or all LDP peers receiving Label Mapping messages, configure either **peer-group** *peer-group-name* or **all** in the command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If multiple inbound policies are configured for a specified LDP peer, the earliest configuration takes effect. For example, the following two inbound policies are configured:

```
inbound peer 2.2.2.2 fec host
inbound peer peer-group group1 fec none
```

As group1 also contains an LDP peer with *peer-id* of 2.2.2.2, the following inbound policy takes effect:

```
inbound peer 2.2.2.2 fec host
```

If two inbound policies are configured in sequence and the **peer** parameters in the two commands are the same, the second command overrides the first one. For example, the following two outbound policies are configured:

```
inbound peer 2.2.2.2 fec host
inbound peer 2.2.2.2 fec none
```

The second configuration overrides the first one. This means that the following inbound policy takes effect on the LDP peer with *peer-id* of 2.2.2.2:

```
inbound peer 2.2.2.2 fec none
```

Creating a peer group before it is referenced is recommended. By default, nonexistent peer groups cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is referenced using the current command, the current command applies to all LDP peers.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device receives Label Mapping messages of all LDP FECs from the specified peer.

Example

Configure all LSRs to receive Label Mapping messages only for host routes from peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] inbound peer all fec host
```

9.1.52 ip route-static ldp-sync

Function

The **ip route-static ldp-sync** command configures unicast static routes for synchronization with LDP.

The **undo ip route-static ldp-sync** command deletes unicast static routes for synchronization with LDP.

By default, unicast static routes for synchronization with LDP are not configured.

Format

ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync** [**description** *text*]

undo ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync**

ip route-static vpn-instance *vpn-source-name ip-address* { *mask* | *mask-length* } { *nexthop-address* [**public**] | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-destination-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * **ldp-sync** [**description** *text*]

undo ip route-static vpn-instance *vpn-source-name ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] * **ldp-sync**

Parameters

Parameter	Description	Value
vpn-instance *vpn-source-name*	Specifies the name of the source VPN instance. Each VPN instance has its own routing table. The configured static routes are added to the routing table of the specified VPN instance.	The value must be an existing VPN instance name.
vpn-instance *vpn-destination-name*	Specifies the name of the destination VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation.
mask	Specifies the subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length. As 1s in a 32-bit mask must be consecutive, the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer that ranges from 0 to 32.
interface-type interface-number	Specifies the type and number of the interface that forwards packets.	-
nexthop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
public	Specifies the next-hop address as a public network address but not an address in the source VPN instance.	-
preference *preference*	Specifies the preference of a static route. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255. The default value is 60.

Parameter	Description	Value
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.
description *text*	Configures the description of a static route.	The value is a string of 1 to 80 characters that can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On an MPLS network with primary and backup links, LSRs establish LSPs based on static routes. When the LDP session of the primary link becomes faulty (the fault is not caused by a link failure) or the primary link recovers, configuring synchronization between LDP and static routes minimizes traffic loss during traffic switchover and switchback.

After synchronization between LDP and static routes is enabled, the recovered static route becomes temporarily inactive. It waits for the establishment of an LDP session before the Hold-down timer expires, which synchronizes LDP and the static route.

Example

Configure static routes for synchronization with LDP.

```
<HUAWEI> system-view
[HUAWEI] ip route-static 10.1.1.0 255.255.255.0 vlanif 100 ldp-sync
```

9.1.53 isis ldp-sync

Function

The **isis ldp-sync** command enables synchronization between LDP and IS-IS on an interface.

The **undo isis ldp-sync** command disables synchronization between LDP and IS-IS on an interface.

By default, synchronization between LDP and IS-IS is disabled on an interface.

Format

isis ldp-sync

undo isis ldp-sync

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LDP convergence speed depends on the convergence speed of IS-IS routes. To enable MPLS LDP on a network with the primary and backup links, the following problems may occur:

- Upon a fault on the primary link, IS-IS routes and ISP are both switched to the backup link using LDP FRR. When the primary link recovers, IS-IS routes are switched back to the primary link earlier than LDP traffic because IGP route convergence is faster than LDP convergence. As a result, LSP traffic is lost.
- If a fault occurs on the LDP session between nodes on the primary link where the IS-IS routes are working properly, the IS-IS routes still use the primary link and the LSP on the primary link is deleted. No IS-IS route exists on the backup link; therefore, no LSP can be established on the backup link. LSP traffic is lost.

Run the **isis ldp-sync** command to enable synchronization between LDP and IS-IS to prevent traffic loss in the preceding problems. Run this command on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Example

Enable synchronization between LDP and IS-IS on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis ldp-sync
```

Enable synchronization between LDP and IS-IS on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis ldp-sync
```

9.1.54 isis ldp-sync block

Function

The **isis ldp-sync block** command blocks synchronization between LDP and IS-IS on an interface.

The **undo isis ldp-sync block** command restores the default setting.

By default, synchronization between LDP and IS-IS is not blocked on an interface.

Format

isis ldp-sync block

undo isis ldp-sync block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ldp-sync enable** command run in the IS-IS view on a device enables synchronization between LDP and IS-IS on all local IS-IS interfaces. On an IS-IS interface transmits importance services, LDP and IS-IS synchronization may affect service transmission. If the link is working properly and an LDP session over the link fails, IS-IS sends link state PDUs (LSPs) to advertise the maximum cost of the link. As a result, IS-IS does not select the route for the link, which affects important service transmission.

To prevent the preceding problem, run the **isis ldp-sync block** command to block synchronization between LDP and IS-IS on the IS-IS interface that transmits important services.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Example

Block synchronization between LDP and IS-IS on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis ldp-sync block
```

Block synchronization between LDP and IS-IS on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis ldp-sync block
```

9.1.55 isis timer ldp-sync hold-down

Function

The **isis timer ldp-sync hold-down** command sets the interval during which an interface waits for creating an LDP session before setting up the IS-IS neighbor relationship.

The **undo isis timer ldp-sync hold-down** command restores the default setting.

By default, the interval is 10 seconds.

Format

isis timer ldp-sync hold-down *value*

undo isis timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the interval during which an interface waits for creating an LDP session before setting up the IS-IS neighbor relationship.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network with both active and standby links, if the active link fails, traffic switches to a standby link. Therefore, the standby IS-IS route and backup LDP label switched path (LSP) along the standby link become reachable. After the active link recovers, its IS-IS route converges more rapidly than the LDP LSP. As a result, the IS-IS neighbor relationship is established earlier than the LDP session on the active link. Although traffic is directed over the IS-IS route to the active link, traffic fails to be forwarded because no LDP LSP is established.

To prevent the traffic forwarding failure, LDP and IS-IS synchronization can be configured. After the active link recovers from a physical fault, the IS-IS route for the active link is set to the Hold-down state, and the Hold-down timer starts. After an LDP session is established over the active link or the Hold-down timer expires, the IS-IS neighbor relationship starts to be established. This allows the LDP LSP and IS-IS route to go Up simultaneously. To set the Hold-down timer, run the **isis timer ldp-sync hold-down** command.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

Set the value of the Hold-down timer for VLANIF100 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the IS-IS neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer ldp-sync hold-down 15
```

Set the value of the Hold-down timer for GE0/0/1 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the IS-IS neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer ldp-sync hold-down 15
```

9.1.56 isis timer ldp-sync hold-max-cost

Function

The **isis timer ldp-sync hold-max-cost** command sets the interval during which IS-IS sends LSPs to advertise the maximum metric on the local device.

The **undo isis timer ldp-sync hold-max-cost** command restores the default setting.

By default, the interval is 10 seconds.

Format

isis timer ldp-sync hold-max-cost { *value* | **infinite** }

undo isis timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
value	Specifies the interval during which IS-IS sends LSPs to advertise the maximum metric on the local device.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that IS-IS keeps advertising the maximum metric in LSPs on the local device before an LDP session is reestablished.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network with active and standby links, when the IS-IS route of the active link is reachable and an LDP session between two nodes on the active link fails, traffic is transmitted over the IS-IS route of the active link, whereas the label switched path (LSP) on the active link fails. Although LSP traffic attempts to be switched to the backup LSP, the active IS-IS route is selected to direct traffic. As a result, traffic on the primary LSP is lost.

To prevent the traffic forwarding failure, LDP and IS-IS synchronization can be configured. If the LDP session over the active link fails, IS-IS advertises the maximum cost of the active link route. The IS-IS route for the standby link is selected, and the Hold-max-cost timer starts. After the LDP LSP over the standby link is established, and the IS-IS route for the standby link is reachable, traffic switches to the standby link. After the LDP session on the active link recovers or the Hold-max-cost timer expires, IS-IS advertises the actual cost of the active link route. To set the Hold-max-cost timer, run the **isis timer ldp-sync hold-max-cost** command.

Select one of the following parameters as required:

- When IS-IS carries LDP services only, configure **infinite** to keep the IS-IS route and LSP over the same link.
- If IS-IS carries multiple types of services including LDP services in the networking, configure *value* to ensure that interruption of an LDP session over the active link does not affect IS-IS routing and other services. The default is 10, in seconds, which is a recommended value.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

Set the interval to 8 seconds, during which IS-IS sends LSPs to advertise the maximum metric on the local device.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] isis enable 1
[HUAWEI-Vlanif100] isis timer ldp-sync hold-max-cost 8
```

Set the interval to 8 seconds, during which IS-IS sends LSPs to advertise the maximum metric on the local device.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] isis enable 1
[HUAWEI-GigabitEthernet0/0/1] isis timer ldp-sync hold-max-cost 8
```

9.1.57 label advertise

Function

The **label advertise** command enables the egress node to advertise labels of a specified type to the penultimate hop.

The **undo label advertise** command restores the default setting.

By default, the egress node assigns implicit null labels to the penultimate hop.

Format

label advertise { **explicit-null** | **implicit-null** | **non-null** }

undo label advertise

Parameters

Parameter	Description	Value
explicit-null	Disables Penultimate Hop Popping (PHP) and enables the egress node to assign explicit null labels to the penultimate hop.	The value of the explicit null label is 0.
implicit-null	Enables PHP and enables the egress node to assign implicit null labels to the penultimate hop.	The value of the implicit null label is 3.

Parameter	Description	Value
non-null	Disables PHP and enable the egress node to assign normal labels to the penultimate hop.	The value is equal to or greater than 16.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS transmits packets along label switched paths (LSPs). The egress at the last hop on the LSP removes MPLS labels from packets before forwarding the packets over IP links or using next layer labels. MPLS labels are useless at the last hop on an LSP. Therefore, penultimate hop popping (PHP) can be configured to enable the penultimate hop to remove labels, which improves forwarding efficiency.

By default, PHP is enabled, and the egress assigns implicit-null labels to the penultimate hop. To specify the type of label that the egress assigns to the penultimate hop, run the following commands:

- In a bidirectional association LSP scenario, run the **label advertise non-null** command to enable the egress to assign a normal label to the penultimate hop.
- In an MPLS QoS scenario, run the **label advertise explicit-null** command to enable the egress to assign an explicit null label to the penultimate hop.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command in the system view.

Precautions

After the **label advertise** command is run to specify a label, the egress on a newly established LDP LSP or constraint-based routed label switched path (CR-LSP) assigns the specified label to the penultimate hop. The **label advertise** command can take effect on existing LDP LSPs or CR-LSPs when one of the following conditions is met:

- A master/slave main control board switchover is performed.
- The **reset mpls ldp** command is run to reset an LDP public instance for an LDP LSP.
- If a CR-LSP is established, the **reset mpls rsvp-te** command is run to reset Resource Reservation Protocol-Traffic Engineering (RSVP-TE), or the **reset mpls te tunnel-interface tunnel** command is run to restart a specified TE tunnel.

If the **label advertise** command is run more than once, the latest configuration overrides the previous one.

Example

Configure the egress node to assign explicit null labels to the penultimate hop.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] label advertise explicit-null
```

9.1.58 label distribution default-route

Function

The **label distribution default-route** command enables a device to assign a label to a default IGP route.

The **undo label distribution default-route** command restores the default configuration.

By default, the device is disabled from assigning a label to a default IGP route.

Format

label distribution default-route

undo label distribution default-route

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

To enable a device to use MPLS assign a label to a default IGP route in independent mode, run the **label distribution default-route** command. An LSP can be established using the default route.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Example

Enable a device to assign a label to a default IGP route.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] label distribution default-route
```

9.1.59 label-withdraw-delay

Function

The **label-withdraw-delay** command enables a node to delay sending Label Withdraw messages.

The **undo label-withdraw-delay** command disables a node from delaying sending Label Withdraw messages.

By default, the label withdraw delay function is disabled.

Format

label-withdraw-delay

undo label-withdraw-delay

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The label withdraw delay function prevents downstream LSP flapping from spreading to upstream nodes. For example, an LSP on a local node flaps because an LDP session between the node and its downstream peer flaps, a route flaps, or an LDP policy is modified. The local node repeatedly sends Label Withdraw and Label Mapping messages in sequence to upstream nodes. This causes the upstream nodes to repeatedly tear down and reestablish LSPs. As a result, the entire LDP LSP flaps. The label withdraw delay function can be enabled on each node of the LDP LSP to suppress the spread of LSP flapping.

Follow-up Procedure

Use the default delay time of 5s or run the **label-withdraw-delay timer** command to set the delay time.

Example

Enable the label withdraw delay function.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] label-withdraw-delay
```

9.1.60 label-withdraw-delay timer

Function

The **label-withdraw-delay timer** command sets the delay time before a node sends a Label Withdraw message.

The **undo label-withdraw-delay timer** command restores the default delay time.

The default delay time is 5 seconds.

Format

label-withdraw-delay timer *time*

undo label-withdraw-delay timer

Parameters

Parameter	Description	Value
time	Specifies the delay time before a Label Withdraw message can be sent.	The value is an integer ranging from 1 to 65535, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The label withdraw delay function prevents downstream LSP flapping from spreading to upstream nodes. For example, an LSP on a local node flaps because an LDP session between the node and its downstream peer flaps, a route flaps, or an LDP policy is modified. The local node repeatedly sends Label Withdraw and Label Mapping messages in sequence to upstream nodes. This causes the upstream nodes to repeatedly tear down and reestablish LSPs. As a result, the entire LDP LSP flaps. To suppress the spread of LSP flapping, run the **label-withdraw-delay** command to enable the label withdraw delay function on each node and the **label-withdraw-delay timer** command to set the delay time before a node sends a Label Withdraw message to its upstream node.

Prerequisites

The label withdraw delay function has been enabled using the **label-withdraw-delay** command.

Example

Enable the label withdraw delay function on the node and set the delay time to 10s.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] label-withdraw-delay
[HUAWEI-mpls-ldp] label-withdraw-delay timer 10
```

9.1.61 ldp-over-te enable

Function

The **ldp-over-te enable** command enables LDP over Traffic Engineering (TE).

The **undo ldp-over-te enable** command disables LDP over TE.

By default, LDP over TE is not enabled.

Format

ldp-over-te enable

undo ldp-over-te enable

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TE supports strong traffic engineering capabilities and provides various QoS guarantees. Due to live network limitations, such as application types and costs, deploying MPLS TE on the entire network is difficult. Therefore, LDP over TE can be used to deploy MPLS TE on a core area and LDP on non-core areas.

To enable LDP over TE on the ingress of a TE tunnel, run the **ldp-over-te enable** command.

Precautions

In LDP over TE networking, load balancing is supported when the ingress node of a TE tunnel is an S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, or S6730-H. When there are multiple TE tunnels or there are both TE tunnels and LDP tunnels in the MPLS TE domain, LDP LSP service traffic can be load balanced among multiple tunnels. To adjust the load balancing mode, run the **mpls ecmp load-balance** command in the system-view.

Example

Enable LDP over TE.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] ldp-over-te enable
```

9.1.62 ldp-sync enable

Function

The **ldp-sync enable** command enables synchronization between LDP and IS-IS on all interfaces in an IS-IS process.

The **undo ldp-sync enable** command disables synchronization between LDP and IS-IS on all interfaces in an IS-IS process.

By default, synchronization between LDP and IS-IS is disabled on all interfaces in an IS-IS process.

Format

ldp-sync enable [**mpls-binding-only**]

undo ldp-sync enable

Parameters

Parameter	Description	Value
mpls-binding-only	Synchronization between LDP and IS-IS can only be enabled on MPLS LDP-enabled interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Synchronization between LDP and IGP reduces LSP traffic loss on a network with both primary and backup LSPs. Traffic loss occurs in either of the following situations:

- The primary LSP works properly and an LDP session between two nodes on the primary LSP fails. IGP guides traffic still through the primary LSP even though a primary/backup LSP switchover is performed.
- If a link on the primary LSP or the primary LSP recovers, IGP routes converge. IGP routes associated with the primary LSP become reachable earlier than the primary LSP because IGP routes converge faster than LDP routes. IGP routes guide traffic through the primary LSP before the primary LSP recovers.

Synchronization between LDP and IGP delays IGP route advertisement so that the LDP session and IGP route can converge simultaneously.

The **ldp-sync enable** command run in the IS-IS view can enable synchronization between LDP and IS-IS on all interfaces within a specified IS-IS process.

Follow-up Procedure

Run the **isis ldp-sync block** command to disable synchronization between LDP and IGP on desired IS-IS interfaces.

Precautions

Although the **undo ldp-sync enable** command has been run, synchronization between LDP and IS-IS configured using the **isis ldp-sync** command still takes effect on an IS-IS interface.

Example

Enable synchronization between LDP and IS-IS on all interfaces in an IS-IS instance.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] ldp-sync enable
```

9.1.63 longest-match

Function

The **longest-match** command configures inter-domain LDP extension capability and enables LDP to search for routes to establish LSPs based on the longest match rule.

The **undo longest-match** command restores the default setting.

By default, LDP searches for routes to establish LSPs based on the exact matching rule.

Format

longest-match

undo longest-match

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large network, multiple IGP areas need to be configured for flexible network deployment and fast route convergence. In this situation, when advertising routes between IGP areas, to prevent a large number of routes from consuming too many resources, an Area Border Router (ABR) needs to aggregate the routes in an area and then advertise the aggregated route to neighbor IGP areas. By default, when establishing LSPs, LDP searches the routing table for the route that exactly matches the forwarding equivalence class (FEC) carried in the received Label Mapping message. For aggregated routes, only liberal LDP LSPs, not inter-area LDP LSPs, can be set up.

In this case, run the **longest-match** command to enable LDP to search for routes or establishing inter-area LDP LSPs based on the longest match rule.

Precautions

Configuring this command is not allowed during LDP GR.

Example

Enable LDP to search for routes for establishing LDP LSPs based on the longest match rule.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] longest-match
```

9.1.64 loop-detect

Function

The **loop-detect** command enables a device to advertise the capability of loop detection during the initialization of an LDP session.

The **undo loop-detect** command disables a device from advertising the capability of loop detection during the initialization of an LDP session.

By default, a device cannot advertise the capability of loop detection during the initialization of an LDP session.

Format

loop-detect

undo loop-detect

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

The switch does not support the loop detection function. In the scenario where its neighbor supports the loop detection function and requires that the notification about whether the loop detection function is enabled be consistent on the two ends, run the **loop-detect** command to ensure that the switch sets up an LDP session with this neighbor.

Though the **loop-detect** command is run, the switch still does not support the LDP loop detection function but only has the loop detection negotiation capability.

Example

Enable the device to advertise the capability of loop detection during the initialization of an LDP session.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] loop-detect
```

9.1.65 lsp-trigger bgp-label-route

Function

The **lsp-trigger bgp-label-route** command enables LDP to allocate labels to labeled BGP routes on the public network.

The **undo lsp-trigger bgp-label-route** command restores the default setting.

By default, LDP does not allocate labels to labeled BGP routes on the public network.

Format

lsp-trigger bgp-label-route [**ip-prefix** *ip-prefix-name*] [**not-only-host**]

undo lsp-trigger bgp-label-route

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the labeled BGP routes on the public network to set up LDP LSPs.	The value is an existing IP prefix list name.
not-only-host	Uses labeled public network BGP routes with 0-bit to 32-bit masks based on the IP prefix list to establish LDP LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Both the **lsp-trigger bgp-label-route** command and the **lsp-trigger** command can be used to configure policies to trigger the establishment of LDP LSPs. The former command is used for labeled public network BGP routes with 0-bit to 32-bit masks, and the latter command is used for static routes and IGP routes.

If **not-only-host** is not configured, LDP distributes labels only for labeled public network BGP routes with 32-bit masks. If **not-only-host** is configured, LDP distributes labels for labeled public network BGP routes with 0-bit to 32-bit masks.

Precautions

Modifying the LSP-triggering policy during the LDP GR period is invalid.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all public-network labeled BGP routes trigger LDP LSP establishment.

Example

Trigger the establishment of LDP LSPs according to labeled public network BGP routes with 32-bit masks.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] lsp-trigger bgp-label-route
```

9.1.66 lsp-trigger

Function

The **lsp-trigger** command sets a policy for establishing LDP LSPs.

The **undo lsp-trigger** command restores the default setting.

By default, LDP uses IP host routes with 32-bit addresses (excluding host routes with 32-bit interface addresses) to establish LSPs.

Format

lsp-trigger { **all** | **host** | **ip-prefix** *ip-prefix-name* | **none** }

undo lsp-trigger

Parameters

Parameter	Description	Value
all	Indicates that all static and IGP routes trigger the establishment of LSPs.	-
host	Indicates that IP host routes with 32-bit addresses (excluding host routes with 32-bit interface addresses) trigger the establishment of LSPs.	-
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the establishment of LSPs.	The value is an existing IP prefix list name.
none	Indicates that the establishment of an LSP is not triggered.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MPLS LDP is enabled, LSPs are automatically established. If no policy is configured, an increasing number of LSPs are established, wasting resources.

The **lsp-trigger** command configures a policy to allow LDP to use specified routes to establish LSPs. This setting prevents unwanted LSPs from being established and helps reduce resource wastes.

NOTE

The **lsp-trigger all** command is not recommended. If this command is run, LDP uses all IGP routes to establish LSPs, causing a large number of unwanted LSPs to be established and wasting system resources. Before using this command, configure a policy for filtering out routes unnecessary for the LSP establishment. The policy helps reduce the number of LSPs to be established and save system resources.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

- Modifying the LSP-triggering policy during the LDP GR period is invalid.
- The **lsp-trigger** command can be used to configure policies only for ingress and egress LSPs on the public network and ingress and egress LSPs on the private network that are established using IGP routes. To configure a policy for triggering the transit LSP establishment, run the **propagate mapping** command.
- The **lsp-trigger host** command can be run on either of the following nodes to provide a specific function:
  - Ingress: This command enables the ingress to use all routes with a 32-bit mask to establish LDP LSPs.
  - Egress: This command enables the egress to use local routes with a 32-bit mask to establish LDP LSPs.

  The **lsp-trigger** { **all** | **ip-prefix** *ip-prefix-name* } command can be used to establish proxy egress LSPs. The **lsp-trigger host** command, however, cannot be used to establish proxy egress LSPs.
- Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all static and IGP routes trigger LDP LSP establishment.

Example

Trigger the establishment of LSPs based on all static and IGP routes.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] lsp-trigger all
```

9.1.67 lspv mpls-lsp-ping echo enable

Function

The **lspv mpls-lsp-ping echo enable** command enables a device to respond to MPLS Echo Request packets.

The **undo lspv mpls-lsp-ping echo enable** command disables a device from responding to MPLS Echo Request packets.

By default, a device is enabled to respond to MPLS Echo Request packets.

Format

lspv mpls-lsp-ping echo enable

undo lspv mpls-lsp-ping echo enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ping and trace tests use ICMP packets to locate faulty nodes on a forwarding path. When an LSP fails, IP forwarding-based ICMP packets cannot be used to detect the faulty node.

In this case, the **ping lsp** and **tracert lsp** command can be used to locate the faulty node on the LSP. These commands use MPLS Echo Request and MPLS Echo Reply packets to detect the connectivity of an LSP. Both MPLS Echo Request and MPLS Echo Reply packets are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes MPLS Echo Request and MPLS Echo Reply packets based on the port number. An MPLS Echo Request packet carries FEC information to be detected, and is sent along the same LSP as other packets with the same FEC information. In this manner, the connectivity of the LSP is checked. MPLS Echo Request packets are transmitted to the destination through MPLS, whereas MPLS Echo Reply packets are transmitted to the source through IP.

For network security or management, you can run the **lspv mpls-lsp-ping echo enable** command to enable a device to respond to MPLS Echo Request packets or run the **undo lspv mpls-lsp-ping echo enable** command to disable the device from responding to MPLS Echo Request packets. This function is implemented by enabling or disabling port 3503. By default, port 3503 is enabled.

After you run the **ping lsp** and **tracert lsp** command to detect the connectivity of an LSP, you are advised to run the **undo lspv mpls-lsp-ping echo enable** command to disable the device from responding to MPLS Echo Request packets to avoid occupation of system resources.

Precautions

If you run the **undo lspv mpls-lsp-ping echo enable** command to disable a device from responding to MPLS Echo Request packets, this device does not respond to the **ping lsp** and **tracert lsp** command. As a result, the ping or trace test with the address of the device as the destination address times out.

Example

Disable a device to respond to MPLS Echo Request packets.

```
<HUAWEI> system-view
[HUAWEI] undo lspv mpls-lsp-ping echo enable
```

9.1.68 lspv packet-filter

Function

The **lspv packet-filter** command enables the filtering of MPLS Echo Request packets based on source addresses. Filtering rules are defined in ACL configurations.

The **undo lspv packet-filter** command disables the filtering of MPLS Echo Request packets based on source addresses.

By default, the filtering of MPLS Echo Request packets based on source addresses is disabled.

Format

lspv packet-filter *acl-number*

undo lspv packet-filter

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The ACL number is a decimal integer that ranges from 2000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **lspv packet-filter** command often runs on the destination device of the LSPV check. In the case that the filtering of MPLS Echo Request packets based on source addresses is enabled, upon receiving MPLS Echo Request packets, the device matches the source addresses of the packets with a specified ACL. The packets permitted by the ACL are processed; those denied by the ACL are discarded.

Example

Enable the filtering of the MPLS Echo Request packets based on source addresses based on ACL 2100.

```
<HUAWEI> system-view
[HUAWEI] lspv packet-filter 2100
```

9.1.69 lsr-id

Function

The **lsr-id** command sets the LSR ID of an LDP instance.

The **undo lsr-id** command restores the default setting.

By default, the LSR ID of an LDP instance is the LSR ID of the LSR where the LDP instance is configured

Format

lsr-id *lsr-id*

undo lsr-id

Parameters

Parameter	Description	Value
lsr-id	Specifies the LSR ID of an LDP instance.	The value is in dotted decimal notation.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the LSR ID of an LDP instance is the same as the MPLS LSR ID configured using the **mpls lsr-id** command. On some networks such as the BGP/MPLS VPNs to which VPN instances apply, if the VPN address space and the public network address space overlap, configure LSR IDs for LDP instances to ensure the correct establishment of TCP connections.

Prerequisites

- MPLS has been enabled globally using the **mpls (system view)** command.
- MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

Modifying or deleting the LSR ID of an LDP instance causes the reestablishment of all sessions in the LDP instance.

Example

Set the LSR ID of an LDP instance to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] lsr-id 10.1.1.1
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.70 maintain-session received-error-message

Function

The **maintain-session received-error-message** command enables LDP to maintain a session after receiving error TCP packets.

The **undo maintain-session received-error-message** command restores the default configuration.

By default, LDP tears down a session after receiving error TCP packets.

Format

maintain-session received-error-message

undo maintain-session received-error-message

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

According to RFC5036, LDP tears down a session after receiving error TCP packets. When a device from another vendor fails or a link fails, the LDP session alternates between Up and Down after processing in this way. If the LDP transmits L2VPN services, the L2VPN services will be interrupted. To prevent this problem, run the **maintain-session received-error-message** command to enable LDP to maintain a session after receiving error TCP packets. This prevents LDP session flapping and helps maintain upper-layer L2VPN services.

Example

Enable LDP to maintain a session after receiving error TCP packets.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] maintain-session received-error-message
```

9.1.71 md5-password

Function

The **md5-password** command sets the password that is used by a TCP connection during the creation of an LDP session.

The **undo md5-password** command disables MD5 authentication.

By default, MD5 authentication is disabled during the creation of an LDP session.

Format

md5-password { **plain** | **cipher** } *peer-lsr-id password*

undo md5-password [**plain** | **cipher**] *peer-lsr-id*

Parameters

Parameter	Description	Value
plain	Displays the password in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. In this case, users at a lower level can easily obtain the password by viewing the configuration file. This brings security risks. Therefore, it is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Displays the password in cipher text.	-
peer-lsr-id	Specifies the LSR ID of the peer, which identifies the peer LSR.	The value is in dotted decimal notation.

Parameter	Description	Value
password	Specifies the password.	The value is a string of characters, spaces not supported. For a plain password, the string is 1 to 255 characters. For an encrypted password, the string is 20 to 392 characters. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. Note that the peers of an LDP session can be configured with different encryption modes (plain or cipher text mode), but must be configured with a single password.

LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

A password can be set either in cipher text or plain text. A plain text password is a character string that is pre-configured and directly recorded in a configuration file. A cipher text password is a character string that is recorded in a configuration file after being encrypted using a specified algorithm.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

- MD5 authentication and keychain authentication cannot be configured together on one peer. Note that MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.
- If the password on a peer changes, the LDP session is reestablished and the LSP associated with the original LDP session is deleted.

Example

Configure the local node to perform MD5 authentication when it establishes an LDP session with its peer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] md5-password cipher 2.2.2.2 YsHsjx_202206
```

9.1.72 md5-password all

Function

The **md5-password all** command enables LDP MD5 authentication in a batch for all LDP peers.

The **undo md5-password all** command disables LDP MD5 authentication in a batch for all LDP peers.

By default, MD5 authentication in a batch is disabled for all LDP peers.

Format

md5-password { **plain** | **cipher** } **all** *password*

undo md5-password all

Parameters

Parameter	Description	Value
plain	Indicates a simple text password. A simple text password is saved in simple text in a configuration file. This format poses risks. A ciphertext password is recommended. To improve device security, periodically modify the password.	-
cipher	Indicates a ciphertext password.	-
password	Specifies an authentication password.	A password must not contain spaces. A simple text password is a string of 1 to 255 characters. A ciphertext password is a string of 1 to 255 characters. An MD5 ciphertext password is 20 bits to 392 bits long. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

If a great number of LDP peers are configured, run the **md5-password all** command to enable MD5 authentication in a batch for all LDP peers.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- The session is not re-established if the passwords on both ends are the same. If the interval between password settings on both ends exceeds the session Keepalive time and the passwords become different, the session is disconnected due to a timeout, causing an LSP to be deleted.
- Note that the peers of an LDP session can be configured with different authentication modes (simple text or ciphertext), but must be configured with a single password.
- After the **md5-password all** command is run, MD5 authentication takes effect on all LDP peers. If MD5 authentication fails, an LDP session fails to be established.
- MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.

Example

Enable LDP MD5 authentication for all LDP peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] md5-password cipher all YsHsjx_202206
```

9.1.73 md5-password peer-group

Function

The **md5-password peer-group** command enables LDP MD5 authentication in a batch for a specified LDP peer group.

The **undo md5-password peer-group** command disables LDP MD5 authentication in a batch for a specified LDP peer group.

By default, MD5 authentication in a batch is disabled for all peer groups.

Format

md5-password { **plain** | **cipher** } **peer-group** *ip-prefix-name password*

undo md5-password peer-group

Parameters

Parameter	Description	Value
plain	Indicates a simple text password. A simple text password is saved in simple text in a configuration file. This format poses risks. A ciphertext password is recommended. To improve device security, periodically modify the password.	-
cipher	Indicates a ciphertext password.	-
ip-prefix-name	Specifies the name of an IP prefix list. The IP prefix list name is configured using the **ip ip-prefix** command.	The value is a string of 1 to 169 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks (").

Parameter	Description	Value
password	Specifies an authentication password.	A password must not contain spaces. A simple text password is a string of 1 to 255 characters. A ciphertext password is a string of 1 to 255 characters. An MD5 ciphertext password is 20 bits to 392 bits long. The string can contain spaces if it is enclosed with double quotation marks (").

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

If a great number of LDP peers are configured, run the **md5-password peer-group** command to enable MD5 authentication in a batch for LDP peers in a specified peer group. An IP prefix list can be specified to define the range of IP addresses in a group.

Prerequisites

An IP prefix list has been configured using the **ip ip-prefix** command.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.

- The session is not re-established if the passwords on both ends are the same. If the interval between password settings on both ends exceeds the session Keepalive time and the passwords become different, the session is disconnected due to a timeout, causing an LSP to be deleted.
- Note that the peers of an LDP session can be configured with different authentication modes (simple text or ciphertext), but must be configured with a single password.
- After the **md5-password peer-group** command is run, MD5 authentication takes effect on a specified LDP peer group. If MD5 authentication fails, an LDP session fails to be established.
- MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.
- Before a peer group is referenced, create it. By default, a nonexistent peer group cannot be specified in this command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is specified in this command, a local device performs MD5 authentication for each LDP session connected to each LDP peer.

Example

Enable LDP MD5 authentication for LDP peers with IP addresses matching the IP prefix list named **list1**.

```
<HUAWEI>system-view
[HUAWEI] ip ip-prefix list1 permit 4.4.4.4 32
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] md5-password cipher peer-group list1 YsHsjx_202206
```

9.1.74 mpls (system view)

Function

The **mpls** command enables MPLS on the local node and displays the MPLS view.

The **undo mpls** command deletes all MPLS configurations.

By default, no node is enabled with MPLS.

Format

mpls

undo mpls

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **mpls** command on a network where MPLS services are to be deployed.

You can run MPLS-related commands only after running the **mpls** command.

Prerequisites

The LSR ID has been configured using the **mpls lsr-id** command.

Precautions

NOTICE

After the **undo mpls** command is run in the system view, MPLS services may be interrupted and all MPLS configurations in the system and interface views are deleted. To restore the MPLS services, reconfigure these commands.

Example

Enable MPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
Info: Mpls starting, please wait... OK!
```

9.1.75 mpls (interface view)

Function

The **mpls** command enables MPLS on an interface.

The **undo mpls** command disables MPLS on an interface.

By default, no interface is enabled with MPLS.

Format

mpls

undo mpls

Parameters

None

Views

Interface view

NOTE

The **mpls** command does not take effect in the sub-interface view or tunnel interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS services are deployed, after enabling MPLS on a node, enable MPLS on the interfaces of the node before performing other MPLS configurations.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

Running the **undo mpls** command in the interface view deletes all MPLS configurations on the interface.

Example

Enable MPLS on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
```

Enable MPLS on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
```

9.1.76 mpls bfd enable

Function

The **mpls bfd enable** command enables dynamic creation of BFD sessions on the ingress node of an LDP LSP.

The **undo mpls bfd enable** command disables the dynamic creation of BFD sessions on the ingress node of an LDP LSP.

By default, an ingress cannot dynamically create BFD sessions for monitoring LDP LSPs.

Format

mpls bfd enable

undo mpls bfd enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network, use LDP to dynamically create LSP tunnels. Upon a fault on the link, the convergence is slow. Configure BFD to detect LDP LSP connectivity to speed up convergence.

To dynamically establish a BFD session, run the **mpls bfd enable** command on the source end of the LDP LSP.

NOTE

After the **mpls bfd enable** command is used, no BFD session is set up.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Example

Enable the dynamic creation of BFD sessions on the ingress node of an LDP LSP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd enable
```

9.1.77 mpls bfd

Function

The **mpls bfd** command sets the parameters of BFD sessions.

The **undo mpls bfd** command deletes the parameters of BFD sessions.

By default, no parameter of BFD sessions is set.

Format

mpls bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

On an MPLS network, use BFD to detect LSP connectivity to increase the link fault detection speed. Users can change the values of BFD parameters based on actual networking. On an unstable link, if the BFD parameters are set small, the BFD session may flap. You can increase the values of BFD parameters.

Actual interval for the local device to send BFD packets = max { interval for sending BFD packets on the local end, interval for receiving BFD packets on the peer end }; actual interval for the local device to receive BFD packets = max { interval for sending BFD packets on the peer end, interval for receiving BFD packets on the local end }; and local BFD detection time = actual interval for receiving BFD packets on the local end x BFD detection multiplier on the peer end.

If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Example

Set the interval at which BFD packets are sent to 200 ms.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd min-tx-interval 200
```

9.1.78 mpls bfd-trigger

Function

The **mpls bfd-trigger** command configures a trigger policy for an LDP BFD session.

The **undo mpls bfd-trigger** command deletes a trigger policy for an LDP BFD session.

By default, no trigger policy for an LDP BFD session is configured.

Format

mpls bfd-trigger [**host** [**nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number*] * | **fec-list** *list-name*]

undo mpls bfd-trigger [**host** [**nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number*] * | **fec-list** *list-name*]

Parameters

Parameter	Description	Value
host	Indicates that all host addresses are used to create LDP BFD sessions.	-
nexthop *next-hop-address*	Specifies the next hop address on an LSP.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
fec-list *list-name*	Specifies the name of a FEC list, by which the creation of an LDP BFD session is triggered.	The value is an existing FEC list name.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The trigger policy for LDP BFD has two types: the host address and FEC list.

If you want all host addresses to trigger the establishment of BFD sessions, use the host trigger mode. Specify the LSPs that can set up BFD sessions by specifying the next hop address and the outbound interface.

If you only want part of hosts to trigger the establishment of BFD sessions, use the FEC list trigger mode to specify the corresponding host addresses. Before specifying the FEC list triggering mode, run the **fec-list** and **fec-node** commands to configure a FEC list.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Example

Configure the host trigger policy of BFD sessions in the MPLS view.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd enable
[HUAWEI-mpls] mpls bfd-trigger host
```

9.1.79 mpls bfd-ldp-number threshold-alarm

Function

The **mpls bfd-ldp-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for LDP. The conditions include the upper and lower alarm thresholds (percent) for the proportion of established dynamic BFD sessions for LDP to all supported ones.

The **undo mpls bfd-ldp-number threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%.

Format

mpls bfd-ldp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bfd-ldp-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established dynamic BFD sessions for LDP to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established dynamic BFD sessions for LDP to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of dynamic BFD sessions for LDP reaches a specified upper limit, new dynamic BFD sessions for LDP cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established dynamic BFD sessions for LDP to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls bfd-ldp-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established dynamic BFD sessions for LDP to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established dynamic BFD sessions for LDP to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls bfd-ldp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls bfd-ldp-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for LDP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd-ldp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.80 mpls bgp bfd

Function

The **mpls bgp bfd** command sets time parameters for BGP BFD sessions.

The **undo mpls bgp bfd** command restores default time parameters for BGP BFD sessions.

By default, the minimum interval for sending BFD packets is 1000 ms, the minimum interval for receiving BFD packets is 1000 ms, and the local detection multiplier is 3.

Format

mpls bgp bfd { **min-tx-interval** *interval* | **min-rx-interval** *interval* | **detect-multiplier** *multiplier* } *

undo mpls bgp bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls bgp bfd { **min-tx-interval** *interval* | **min-rx-interval** *interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *interval*	Specifies the minimum interval at which BGP BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *interval*	Specifies the minimum interval at which BGP BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local BGP BFD detection multiplier.	The value is an integer ranging from 3 to 50. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

A BGP BFD session working in asynchronous mode monitor BGP label switched paths (LSPs) over BGP tunnels. The ingress and egress of E2E BGP LSPs exchange BFD packets periodically. If a node receives no BFD packet after the detection period elapses, the node considers the BGP LSP faulty.

Effective BFD time parameters are calculated using the following formulas:

- Effective local interval at which BFD packets are sent = MAX { Locally configured minimum interval at which BFD packets are sent, Remotely configured minimum interval at which BFD packets are received }
- Effective local interval at which BFD packets are received = MAX { Remotely configured minimum interval at which BFD packets are sent, Locally configured minimum interval at which BFD packets are received }
- Local BFD detection period = Effective local interval at which BFD packets are received x Remotely configured BFD detection multiplier

Example

Set the minimum interval at which BGP BFD packets are sent to **200** ms.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp bfd min-tx-interval 200
```

9.1.81 mpls bgp bfd enable

Function

The **mpls bgp bfd enable** command enables the MPLS ability to dynamically create BGP BFD sessions.

The **undo mpls bgp bfd enable** command disables the MPLS ability to dynamically create BGP BFD sessions.

By default, the MPLS ability to dynamically create BGP BFD sessions is disabled.

Format

mpls bgp bfd enable

undo mpls bgp bfd enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD for BGP tunnel rapidly detects faults in E2E BGP tunnels. Before a BGP BFD session is established, run the **mpls bgp bfd enable** command on the ingress of a BGP tunnel to enable the MPLS ability to dynamically create a BGP BFD session.

Prerequisites

BFD has been globally enabled using the **bfd** command.

Follow-up Procedure

Run the **mpls bgp bfd-trigger-tunnel** command to establish a BGP BFD session.

Example

Enable the MPLS ability to dynamically create a BGP BFD session on the ingress of a BGP tunnel.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp bfd enable
```

9.1.82 mpls bgp bfd-trigger-tunnel

Function

The **mpls bgp bfd-trigger-tunnel** command specifies a policy to establish BGP BFD sessions.

The **undo mpls bgp bfd-trigger-tunnel** command deletes a policy to establish BGP BFD sessions.

By default, no trigger policy is configured.

Format

mpls bgp bfd-trigger-tunnel { **host** | **ip-prefix** *ip-prefix-name* }

undo mpls bgp bfd-trigger-tunnel

Parameters

Parameter	Description	Value
host	Allows a device to use host addresses to establish BGP BFD sessions.	-

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Allows a device to use an IP address prefix list with a specified name to establish BGP BFD sessions.	The value is an existing IP address prefix list.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD for BGP tunnel rapidly detects faults in E2E BGP tunnels. Before a BGP BFD session is established, the **mpls bgp bfd enable** command must be run to enable the MPLS ability to dynamically establish BGP BFD sessions on the ingress of a BGP tunnel. Then to specify the policy for dynamically establish BGP BFD sessions, run the **mpls bgp bfd-trigger-tunnel** command.

Either of the following trigger policies can be used:

- Host address-based policy: used when all host addresses are available to trigger the creation of BGP BFD sessions.
- IP address prefix list-based policy: used when only some host addresses can be used to establish BFD sessions.

Prerequisites

BFD has been globally enabled using the **bfd** command.

Precautions

If the **mpls bgp bfd-trigger-tunnel** command is run more than once, the latest configuration overrides the previous one.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all host addresses trigger BGP BFD session establishment.

Example

Allow a device to use host addresses to dynamically establish BGP BFD sessions.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp bfd enable
[HUAWEI-mpls] mpls bgp bfd-trigger-tunnel host
```

9.1.83 mpls bgp-lsp-number threshold-alarm

Function

The **mpls bgp-lsp-number threshold-alarm** command configures the alarm threshold for BGP LSP usage.

The **undo mpls bgp-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for BGP LSP usage is 80%. The default lower limit of the clear alarm threshold for BGP LSP usage is 75%.

Format

mpls bgp-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls bgp-lsp-number { **ingress** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bgp-lsp-number threshold-alarm

undo mpls bgp-lsp-number { **ingress** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for BGP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for BGP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	Specifies the alarm threshold for ingress BGP LSPs.	-
egress	Specifies the alarm threshold for egress BGP LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of BGP LSPs in the system reaches a specific limit, establishing additional BGP LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of BGP LSPs reaches the specific limit. To configure the alarm threshold for BGP LSP usage, run the **mpls bgp-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of BGP LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of BGP LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for ingress BGP LSPs or egress BGP LSPs, run **mpls bgp-lsp-number** { **ingress** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls bgp-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for BGP LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual BGP LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual BGP LSP usage falls below the lower limit of the clear alarm threshold.

Example

Configure the upper limit and the lower limit of the alarm threshold for BGP LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgp-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.84 mpls bgpv6-lsp-number threshold-alarm

Function

The **mpls bgpv6-lsp-number threshold-alarm** command configures the alarm threshold for BGP IPv6 LSP usage.

The **undo mpls bgpv6-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for BGP IPv6 LSP usage is 80%. The default lower limit of the clear alarm threshold for BGP IPv6 LSP usage is 75%.

Format

mpls bgpv6-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls bgpv6-lsp-number egress threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bgpv6-lsp-number threshold-alarm

undo mpls bgpv6-lsp-number egress threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for BGP IPv6 LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for BGP IPv6 LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
egress	Specifies the alarm threshold for egress BGP IPv6 LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of BGP IPv6 LSPs in the system reaches a specific limit, establishing additional BGP IPv6 LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of BGP IPv6 LSPs reaches the specific limit. To configure the alarm threshold for BGP IPv6 LSP usage, run the **mpls bgpv6-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of BGP IPv6 LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of BGP IPv6 LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for egress BGP IPv6 LSPs, run **mpls bgpv6-lsp-number egress threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls bgpv6-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for BGP IPv6 LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual BGP IPv6 LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual BGP IPv6 LSP usage falls below the lower limit of the clear alarm threshold.

Example

Configure the upper limit and the lower limit of the alarm threshold for BGP IPv6 LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bgpv6-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.85 mpls dynamic-label-number threshold-alarm

Function

The **mpls dynamic-label-number threshold-alarm** command sets alarm thresholds of dynamic label usage.

The **undo mpls dynamic-label-number threshold-alarm** command restores the default settings.

By default, the upper limit is 80%, and the lower limit is 70%.

Format

mpls dynamic-label-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls dynamic-label-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of dynamic label usage.	The value is a percent integer ranging from 1 to 100. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of dynamic label usage.	The value is a percent integer ranging from 1 to 100. The lower limit must be less than the upper limit. Using the default value 70 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If dynamic labels run out but the system receives new dynamic label requests, the system fails to satisfy the requests because the dynamic labels are insufficient. As a result, the module that fails to be assigned labels works abnormally. The modules that apply for labels including MPLS TE, MPLS LDP, BGP, L3VPN and L2VPN. To facilitate operation and maintenance, run **mpls dynamic-label-number threshold-alarm** command to set alarm thresholds of dynamic label usage. The system can alert users to the issue that dynamic labels will exhaust.

This command enables the system to generate an alarm in either of the following situations:

- *upper-limit-value*: a percent indicating the upper limit of dynamic labels. If dynamic label usage reaches the upper limit, an alarm is generated.
- *lower-limit-value*: a percent indicating the lower limit of dynamic labels. If dynamic label usage falls below the lower limit, a clear alarm can be generated.

Precautions

If the **mpls dynamic-label-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

The **mpls dynamic-label-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsdynamiclabelthresholdexceed** | **hwmplsdynamiclabelthresholdexceedclear** } command is run to enable the device to generate a dynamic label insufficiency alarm and its clear alarm.

Example

Set the thresholds for triggering dynamic label alarms.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls dynamic-label-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.86 mpls ecmp load-balance

Function

The **mpls ecmp load-balance** command configures the load balancing mode when packets are forwarded through LSPs established by MPLS LDP.

The **undo mpls ecmp load-balance** command restores the default load balancing mode when packets are forwarded through LSPs established by MPLS LDP.

By default, the load balancing mode is **label** when packets are forwarded through LSPs established by MPLS LDP.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

mpls ecmp load-balance { **sip** | **dip** | **label** | **l4-sport** | **l4-dport** } *

undo mpls ecmp load-balance

Parameters

Parameter	Description	Value
sip	Indicates that load balancing is performed based on source IP addresses in MPLS packets.	-
dip	Indicates that load balancing is performed based on destination IP addresses in MPLS packets.	-
label	Indicates that load balancing is performed based on labels in MPLS packets.	-
l4-sport	Indicates that load balancing is performed based on the transport-layer source port in MPLS packets.	-
l4-dport	Indicates that load balancing is performed based on the transport-layer destination port in MPLS packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In real-world scenarios, you need to configure a proper load balancing mode based on MPLS service traffic characteristics on a transit node. If a service traffic parameter changes frequently, it is easier to load balance the traffic if you use the load balancing mode based on this parameter. For example, if the IP addresses of MPLS packets change frequently, it is easier to load balance traffic among LSPs if you use the load balancing mode based on **dip** or **sip**.

Precautions

This command takes effect only on newly established LSPs. If you want this command to take effect on previously created LSPs, run the **reset mpls ldp** command to re-establish the LSPs.

Example

Set the load balancing mode to **sip** when packets are forwarded through LSPs established by MPLS LDP.

```
<HUAWEI> system-view
[HUAWEI] mpls ecmp load-balance sip
```

9.1.87 mpls forward-resource threshold-alarm

Function

The **mpls forward-resource threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for MPLS forwarding resources.

The **undo mpls forward-resource threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 85%, and the lower alarm threshold is 75%.

Format

mpls forward-resource threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls forward-resource threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold.	The value is an integer ranging from 2 to 100, represented in percentage.
lower-limit *lower-limit-value*	Sets the lower alarm threshold.	The value is an integer ranging from 1 to (*upper-limit-value*-1), represented in percentage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of MPLS forwarding resources reaches a specified upper limit, new MPLS forwarding entries cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of MPLS forwarding resources reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls forward-resource threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of MPLS forwarding resources reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of MPLS forwarding resources falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls forward-resource threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls forward-resource threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls trap-name** { **hwboardmplsfwdreslack** | **hwboardmplsfwdreslackresume** } command is run to enable the device to generate MPLS forwarding resources insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for MPLS forwarding resources.

```
<HUAWEI> system-view
[HUAWEI] mpls forward-resource threshold-alarm upper-limit 90 lower-limit 60
```

9.1.88 mpls remote-adjacency-number threshold-alarm

Function

The **mpls remote-adjacency-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for remote LDP adjacencies.

The **undo mpls remote-adjacency-number threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%.

Format

mpls remote-adjacency-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls remote-adjacency-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established remote LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established remote LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of remote LDP adjacencies reaches a specified upper limit, new remote LDP adjacencies cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established remote LDP adjacencies to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls remote-adjacency-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established remote LDP adjacencies to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established remote LDP adjacencies to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls remote-adjacency-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls remote-adjacency-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for remote LDP adjacencies.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls remote-adjacency-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.89 mpls ldp advertisement

Function

The **mpls ldp advertisement** command configures the label advertisement mode.

The **undo mpls ldp advertisement** command restores the default setting.

By default, the label advertisement mode is downstream unsolicited (DU).

Format

mpls ldp advertisement { **dod** | **du** }

undo mpls ldp advertisement

Parameters

Parameter	Description	Value
dod	Indicates the downstream on demand (DoD) mode. After the upstream requests the downstream for a label, the downstream sends a Label Mapping message to the upstream.	-
du	Indicates the DU mode. Without a request, the downstream voluntarily sends a Label Mapping message to the upstream.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, downstream LSRs unsolicitedly send Label Mapping messages to upstream LSRs. Establishing a large number of LSPs burdens an LSR such as a DSLAM (a low-performance access device) deployed on an MPLS network. On a large network, run the **mpls ldp advertisement dod** command. This setting allows a DSLAM to send Label Mapping messages to upstream LSRs only after receiving requests for labels. This setting helps minimize the number of unwanted MPLS forwarding entries forwarded by the DSLAM.

Prerequisites

MPLS LDP has been enabled on the interface using the **mpls ldp (interface view)** command.

Precautions

- When multiple links exist between neighbors, all interfaces must use the same label advertisement mode.
- Modifying the label advertisement mode causes reestablishment of LDP sessions.

Example

Set the label advertisement mode to DoD.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp advertisement dod
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Set the label advertisement mode to DoD.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp advertisement dod
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.90 mpls ldp (system view)

Function

The **mpls ldp** command enables LDP on the local node and displays the MPLS-LDP view.

The **undo mpls ldp** command deletes all LDP configurations.

By default, LDP is not enabled on a node.

Format

mpls ldp

undo mpls ldp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS LDP needs to be deployed, run the **mpls ldp** command to enable MPLS LDP globally and create a public network instance running LDP.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Follow-up Procedure

You can perform other LDP configurations.

Precautions

NOTICE

After the **undo mpls ldp** command is run in the system view, MPLS LDP services may be interrupted and all MPLS LDP configurations in the system and interface views are deleted. To restore the MPLS LDP services, reconfigure these commands.

Example

Enable LDP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp]
```

9.1.91 mpls ldp (interface view)

Function

The **mpls ldp** command enables MPLS LDP function on an interface.

The **undo mpls ldp** command disables MPLS LDP function on an interface.

By default, no interface is enabled with MPLS LDP function.

Format

mpls ldp

undo mpls ldp

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS LDP needs to be deployed, enable MPLS LDP function on an interface before configuring other LDP configurations.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

MPLS has been enabled on the interface using the **mpls** command in the interface view.

Follow-up Procedure

You can perform other MPLS LDP configurations.

Precautions

Running the **undo mpls ldp** command in the interface view deletes all MPLS LDP configurations on the interface.

Example

Enable MPLS LDP function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls ldp
```

Enable MPLS LDP function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
```

9.1.92 mpls ldp frr nexthop

Function

The **mpls ldp frr nexthop** command enables LDP FRR on an interface.

The **undo mpls ldp frr** command disables LDP FRR on an interface.

By default, no interface is enabled with LDP FRR.

Format

mpls ldp frr nexthop *nexthop-address* [**ip-prefix** *ip-prefix-name*] [**priority** *priority*]

undo mpls ldp frr [**nexthop** *nexthop-address*] [**ip-prefix** *ip-prefix-name*] [**priority** *priority*]

Parameters

Parameter	Description	Value
nexthop-address	Specifies the next hop address on a backup LSP.	The value is in dotted decimal notation.

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the IP prefix name. Only the FEC that matches the specified IP prefix can trigger the generation of a backup LSP.	The value is an existing IP prefix name.
priority *priority*	Specifies the priority of a backup LSP. The greater the value is, the lower priority the backup LSP has.	The value is an integer ranging from 1 to 65535. By default, the value is 50.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traditional IP FRR technology cannot effectively protect the traffic on an MPLS network. The device provides the LDP FRR function and the solution to port protection.

In the manual LDP FRR mode, you need to configure a backup LSP by specifying the outbound interfaces or the next hops. This mode applies to simple-structured networks.

When running the **mpls ldp frr nexthop** command to configure the next hop IP address, note that:

- You can configure multiple next hops on one interface. This allows you to configure multiple backup LSPs with different outbound interfaces for the primary LSP.
- You can configure different prefix lists for the same next hop on one interface.
  - If no prefix list is specified, LDP FRR tries to establish backup LSPs along the path specified by *nexthop-address* for all primary LSPs on the interface.
  - If only the DENY item is in a specified prefix list, no backup LSP is allowed to set up along the path specified by *nexthop-address* for the primary LSP mapping to the FEC denied by the interface.
  - If only PERMIT item is in the specified prefix list, backup LSPs are allowed to set up along the path specified by *nexthop-address* only for the primary LSPs mapping to the FEC permitted by the interface.
  - If both PERMIT and DENY items are in the prefix list, only the PERMIT item is effective. That is, backup LSPs are allowed to set up along the

path specified by *nexthop-address* only for the primary LSPs mapping to the FEC permitted by the interface.

- A single interface supports LDP FRR with a maximum of 10 priorities. Only a single backup LSP is generated.

Prerequisites

MPLS has been enabled in the interface view using the **mpls** command.

Precautions

- If the **undo mpls ldp** command is run in the system view or the **undo mpls ldp** command is run in the interface view to disable LDP functions, the LDP FRR configuration in the interface remains but does not take effect. During the LDP FRR configuration, the LSP that functions as the backup LSP must be in the liberal state. For a backup LSP, the routing status of the backup LSP from the ingress node to the egress node must be Inactive Adv.
- LDP FRR cannot be enabled or disabled during LDP GR.
- When both LDP FRR and IP FRR are enabled, IP FRR takes effect.
- Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, backup LSPs are established for all LDP LSPs on the local interface along the path to the specified next-hop IP address.

Example

Enable LDP FRR on VLANIF100, and set the next hop IP address of the backup LSP to 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls ldp frr nexthop 10.1.1.2
```

Enable LDP FRR on GE0/0/1, and set the next hop IP address of the backup LSP to 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls ldp frr nexthop 10.1.1.2
```

9.1.93 mpls ldp remote-peer

Function

The **mpls ldp remote-peer** command creates a remote peer and displays the remote peer view.

The **undo mpls ldp remote-peer** command deletes a remote peer.

By default, no remote peer is created.

Format

mpls ldp remote-peer *remote-peer-name*

undo mpls ldp remote-peer *remote-peer-name*

Parameters

Parameter	Description	Value
remote-peer-name	Specifies the name of a remote LDP peer.	A string of 1 to 32 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A remote LDP session applies to the following scenarios:

- Allocate inner L2VPN labels.

  If a Martini VLL or VPLS connection is to be established between two LSRs, the remote LDP session must be established between the LSRs to allocate inner labels.

- Configure LDP over TE.

  If the core devices on an MPLS network support TE while edge devices use LDP, you need to configure a remote LDP session between the two edge LSRs on the TE network. After LDP over TE is configured, the TE tunnel is regarded as a hop of the entire LDP LSP.

A remote LDP session can be established between two indirectly connected LSRs or two directly connected LSRs.

A local and a remote LDP session can be established together between two LSRs.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Follow-up Procedure

An IP address can be assigned to the LDP remote peer.

Precautions

When configuring a remote LDP peer, run the **mpls ldp remote-peer** command on the local LDP and remote LDP peers.

Example

Create a remote peer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] quit
[HUAWEI] mpls ldp remote-peer BJI
[HUAWEI-mpls-ldp-remote-bji]
```

9.1.94 mpls ldp timer hello-hold

Function

The **mpls ldp timer hello-hold** command sets the value of a Hello Hold timer.

The **undo mpls ldp timer hello-hold** command restores the default value.

By default, the link Hello Hold timer is 15 seconds and the target Hello Hold timer is 45 seconds.

Format

mpls ldp timer hello-hold *interval*

undo mpls ldp timer hello-hold

Parameters

Parameter	Description	Value
interval	Specifies the value of a Hello Hold timer.	The value is an integer ranging from 3 to 65535, in seconds. Value 65535 indicates that the timer never expires.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two LDP peers periodically exchange Hello messages to maintain the Hello adjacency. If no Hello message is received after the target Hello hold timer expires, the Hello adjacency is deleted.

The default value of the timer is recommended. On a network where the link status is unstable or a large number of packets are sent, increase the value of the timer to prevent the session flapping.

Hello hold timers are classified into the following types:

- Link-Hello hold timer: maintains the local adjacency. The **mpls ldp timer hello-hold** command in the interface view sets a value of the timer.
- Target-Hello hold timer: maintains the remote adjacency. The **mpls ldp timer hello-hold** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the timer that actually takes effect is the smaller one between the two Hello holder timers configured on both ends of an LDP session. If the value is smaller than 9, the Hello hold timer is 9.

Example

Set the value of the link Hello hold timer to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer hello-hold 30
```

Set the value of the link Hello hold timer to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer hello-hold 30
```

Set the value of the target Hello hold timer to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer hello-hold 60
```

9.1.95 mpls ldp timer hello-send

Function

The **mpls ldp timer hello-send** command sets the value of a Hello send timer.

The **undo mpls ldp timer hello-send** command restores the default setting.

By default, the value of a Hello send timer is one third the value of a Hello hold timer.

Format

mpls ldp timer hello-send *interval*

undo mpls ldp timer hello-send

Parameters

Parameter	Description	Value
interval	Specifies the value of a Hello send timer.	The value is an integer ranging from 1 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Hello messages to the neighboring LSR to advertise its presence on the network and sets up the Hello adjacency. The Hello messages are sent at an interval specified by the Hello send timer.

The default value of the Hello send timer is recommended. On a network with poor performance, you can reduce the value of the Hello send timer, enabling the network to recover from faults as soon as possible.

Hello send timers are classified into the following types:

- Link-Hello send timer: maintains the local adjacency. The **mpls ldp timer hello-send** command in the interface view sets a value of the timer.
- Target-Hello send timer: maintains the remote adjacency. The **mpls ldp timer hello-send** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the Hello send timer that takes effect is not necessarily the same as the set value. If the value of the Hello send timer is greater than one third of the value of the Hello hold timer, the value of the Hello send timer that takes effect is equal to one third of the value of the link-Hello hold timer. Run the **mpls ldp timer hello-hold** command to set the value for the Hello hold timer.

Example

Set the value of the link Hello send timer to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer hello-send 10
```

Set the value of the link Hello send timer to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer hello-send 10
```

Set the value of the target Hello send timer to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer hello-send 20
```

9.1.96 mpls ldp timer igp-sync-delay

Function

The **mpls ldp timer igp-sync-delay** command sets the interval during which an LSP is being set up after an LDP session is created.

The **undo mpls ldp timer igp-sync-delay** command restores the default setting.

By default, the interval is 10 seconds.

Format

mpls ldp timer igp-sync-delay *value*

undo mpls ldp timer igp-sync-delay

Parameters

Parameter	Description	Value
value	Specifies the interval, during which an LSP is being set up after an LDP session is created.	The value is an integer ranging from 0 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

LDP-Interior Gateway Protocol (IGP) synchronization-enabled devices complete to establish an LDP session earlier than an LSP. The **mpls ldp timer igp-sync-delay** command can be used to switch traffic to the established LSP after a specified period of time. This setting prevents traffic loss that occurs if the LDP session in the Up state attempts to switch traffic to the LSP that has not been established. Using the default delay value is recommended.

Example

After the LDP session is established on VLANIF100, the interval is set to 15 seconds, during which the LSP is being set up.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer igp-sync-delay 15
```

After the LDP session is established on GE0/0/1, the interval is set to 15 seconds, during which the LSP is being set up.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1]  mpls ldp
[HUAWEI-GigabitEthernet0/0/1]  mpls ldp timer igp-sync-delay 15
```

After the LDP session is established in the remote MPLS LDP peer view, the interval is set to 15 seconds, during which the LSP is being set up.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer rta
[HUAWEI-mpls-ldp-remote-rta] mpls ldp timer igp-sync-delay 15
```

9.1.97 mpls ldp timer keepalive-hold

Function

The **mpls ldp timer keepalive-hold** command sets the value of a Keepalive hold timer.

The **undo mpls ldp timer keepalive-hold** command restores the default setting.

By default, the value of the Keepalive-hold timers of both local and remote sessions is 45 seconds.

Format

mpls ldp timer keepalive-hold *interval*

undo mpls ldp timer keepalive-hold

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a Keepalive hold timer.	The value is an integer ranging from 30 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LDP peers exchange LDP PDUs over session connections to maintain LDP sessions. If a node does not receive any LDP PDU after the Keepalive hold timer expires, the node closes the connection to terminate the session.

The default value of the Keepalive hold timer is recommended. On a network with unstable links, increase the value of a Keepalive hold timer, preventing the session flapping.

Keepalive hold timers are classified into the following types:

- Keepalive hold timer of the local session: maintains the local LDP session. The **mpls ldp timer keepalive-hold** command in the interface view sets a value of the timer.
- Keepalive hold timer of the remote session: maintains the remote LDP session. The **mpls ldp timer keepalive-hold** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

- The value of the Keepalive hold timer that takes effect is the smaller one between the two Keepalive hold timers configured on both ends of an LDP session.
- If more than one LDP link exists between two LSRs, the values of the Keepalive hold timers set for the links must be the same; otherwise, the LDP sessions may be unstable.
- Changing the value of a Keepalive hold timer causes the reestablishment of related LDP sessions.

Example

Set the value of the Keepalive hold timer for a local session to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer keepalive-hold 60
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Set the value of the Keepalive hold timer for a local session to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer keepalive-hold 60
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Set the value of the Keepalive hold timer for a remote session to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer keepalive-hold 50
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.98 mpls ldp timer keepalive-send

Function

The **mpls ldp timer keepalive-send** command sets the value of a Keepalive send timer.

The **undo mpls ldp timer keepalive-send** command restores the default setting.

By default, the value of a Keepalive send timer is one third the value of a Keepalive hold timer.

Format

mpls ldp timer keepalive-send *interval*

undo mpls ldp timer keepalive-send

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a Keepalive send timer.	The value is an integer ranging from 1 to 65535, in seconds.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an LDP session is set up, LSRs on the two ends of the session periodically exchange Keepalive messages to maintain the LDP session.

The default value of the Keepalive send timer is recommended. On a network with poor performance, reduce the value of the Keepalive send timer, enabling the network to recover as soon as possible.

Keepalive send timers are classified into the following types:

- Keepalive send timer of the local LDP session: controls the interval at which Keepalive messages are sent to the peer end of the local session. The **mpls ldp timer keepalive-send** command in the interface view sets a value of this timer.
- Keepalive send timer of the remote LDP session: controls the interval at which Keepalive messages are sent to the peer end of the remote session. The **mpls**

ldp timer keepalive-send command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the Keepalive send timer that actually takes effect may be different from the configured one. If the value of the Keepalive send timer is greater than one third of the value of the Keepalive hold timer, the value of the Keepalive send timer that actually takes effect is equal to one third of the value of the Keepalive hold timer.

Example

Set the value of the Keepalive send timer for setting up a local LDP session to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp timer keepalive-send 10
```

Set the value of the Keepalive send timer for setting up a local LDP session to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp timer keepalive-send 10
```

Set the value of the Keepalive send timer for setting up a remote LDP session to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] mpls ldp timer keepalive-send 20
```

9.1.99 mpls ldp transport-address

Function

The **mpls ldp transport-address** command configures an LDP transport address.

The **undo mpls ldp transport-address** command restores the default setting.

By default, the transport address for a node on a public network is the LSR ID of the node, and the transport address for a node on a private network is the primary IP address of an interface on the node.

Format

mpls ldp transport-address { *interface-type interface-number* | **interface** }

undo mpls ldp transport-address

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. LDP uses the address of the interface as the TCP transport address.	-
interface	Indicates that LDP uses the IP address of the current interface as the TCP transport address.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before two LSRs establish an LDP session, the two LSRs need to establish a TCP connection to exchange label messages. Run the **mpls ldp transport-address** command to set the address (the LDP transport address) for the TCP connection.

The transport address is used to establish a TCP connection between the local node and its peer. The peer must have a reachable route to this transport address. The default transport address is the loopback interface address (an LSR ID). When the address of the loopback interface is a public network address, configure different transport addresses for LSRs so that LSRs can set up connections with private network addresses.

You can run the **mpls ldp transport-address** command in the interface view to set the transport address for a TCP connection. When more than one link exists between two LSRs, and the links are bound to VPN instances, the default transport address is the IP address of an interface rather than the LSR ID of an LSR.

NOTE

- If LDP sessions are to be established over multiple links connecting two LSRs, LDP-enabled interfaces of either LSR must use the default transport address or the same transport address. If interfaces on either of the LSRs are assigned different transport addresses, a single transport address can be used and a single LDP session can be established.
- When the LDP transport address changes, the session is not interrupted immediately. The session is interrupted after the Hello hold timer times out.

Prerequisites

MPLS LDP has been enabled on the interface using the **mpls ldp (interface view)** command.

An IP address must be assigned to the specified interface. If no IP address is assigned, 0.0.0.0 is used as a transport address, causing a failure to establish an LDP session.

Precautions

Changing an LDP transport address interrupts an LDP session. Exercise caution when running the **mpls ldp transport-address** command.

Example

Set the transport address for link Hello messages to the current interface address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls ldp
[HUAWEI-Vlanif100] mpls ldp transport-address interface
```

Set the transport address for link Hello messages to the current interface address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls ldp
[HUAWEI-GigabitEthernet0/0/1] mpls ldp transport-address interface
```

9.1.100 mpls ldp-lsp-number threshold-alarm

Function

The **mpls ldp-lsp-number threshold-alarm** command configures the alarm threshold for LDP LSP usage.

The **undo mpls ldp-lsp-number threshold-alarm** command restores the default settings.

By default, the upper limit of the alarm threshold for LDP LSP usage is 80%, the lower limit of the clear alarm threshold for LDP LSP usage is 75%.

Format

mpls ldp-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls ldp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls ldp-lsp-number threshold-alarm

undo mpls ldp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for LDP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for LDP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	Specifies the alarm threshold for ingress LDP LSPs.	-
transit	Specifies the alarm threshold for transit LDP LSPs.	-
egress	Specifies the alarm threshold for egress LDP LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of LDP LSPs in the system reaches a specific limit, establishing additional LDP LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of LDP LSPs reaches the specific limit. To configure the alarm threshold for LDP LSP usage, run the **mpls ldp-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of LDP LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.

- *lower-limit-value*: lower alarm threshold. If the proportion of LDP LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for ingress LDP LSPs, transit LDP LSPs or egress LDP LSPs, run **mpls ldp-lsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls ldp-lsp-number threshold-alarm** command is run several times, the latest configuration overrides the previous one.
- This command configures the alarm threshold for LDP LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual LDP LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual LDP LSP usage fells to the lower limit of the clear alarm threshold.

Example

Configure the upper limit and the lower limit of the alarm threshold for LDP LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls ldp-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.101 mpls local-adjacency-number threshold-alarm

Function

The **mpls local-adjacency-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for local LDP adjacencies. The conditions include the upper and lower alarm thresholds (percent) for the proportion of established local LDP adjacencies to all supported ones.

The **undo mpls local-adjacency-number threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%.

Format

mpls local-adjacency-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls local-adjacency-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established local LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established local LDP adjacencies to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of local LDP adjacencies reaches a specified upper limit, new local LDP adjacencies cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established local LDP adjacencies to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls local-adjacency-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established local LDP adjacencies to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established local LDP adjacencies to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls local-adjacency-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls local-adjacency-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for local LDP adjacencies.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls local-adjacency-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.102 mpls lsr-id

Function

The **mpls lsr-id** command sets an LSR ID.

The **undo mpls lsr-id** command deletes an LSR ID.

By default, no LSR ID is set.

Format

mpls lsr-id *lsr-id*

undo mpls lsr-id

Parameters

Parameter	Description	Value
lsr-id	Specifies the LSR ID of a device, which identifies the LSR.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR ID identifies an LSR on a network. On a network where MPLS services are deployed, you must configure the LSR IDs for devices.

An LSR does not have the default LSR ID, and you must configure an LSR ID for it. To enhance network reliability, you are advised to use the IP address of a loopback interface on the LSR as the LSR ID.

Follow-up Procedure

You can configure MPLS and associated services.

Precautions

Before changing or deleting a configured LSR ID, you must run the **undo mpls** command in the system view to delete all MPLS configurations. Exercise caution when you run the **undo mpls** command.

NOTICE

Running the **undo mpls** command deletes all MPLS configurations (including established LDP sessions and LSPs).

Example

Set the LSR ID to 1.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
```

9.1.103 mpls mtu

Function

The **mpls mtu** command configures the MTU of MPLS packets on an interface.

The **undo mpls mtu** command restores the default setting.

By default, the MTU of MPLS packets is equal to the interface MTU.

Format

mpls mtu *mtu*

undo mpls mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MPLS MTU of an interface.	The value range varies according to the interface type.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, Tunnel interface view

NOTE

The **mpls mtu** command does not take effect in the tunnel interface view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MTU value determines the maximum number of bytes that can be sent each time. If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, increasing the network transmission load. MTU values must be correctly negotiated between LSRs to enable packets to successfully reach the receiver.

To calculate the MPLS MTU, an LSR on the path to a specified FEC compares all MTUs advertised by downstream devices with the interface MTU of its own, and adds the smaller MTU (the MPLS MTU) to the MTU TLV field in the Label Mapping message, and send the Label Mapping message upstream.

If an MTU value changes (for example when the local outbound interface or its configuration changes), an LSR recalculates the MTU value and sends a Label Mapping message carrying the new MTU value to all upstream devices.

The relationships between the MPLS MTU and the interface MTU are as follows:

- If no MPLS MTU is configured on an interface, the interface MTU is used to control forwarding of MPLS packets.
- If both an MPLS MTU and an interface MTU are configured on an interface, the smaller value between the two MTUs is used to control forwarding of MPLS packets.

Prerequisites

MPLS has been enabled on the interface using the **mpls (interface view)** command.

Precautions

After changing the MTU using the **mpls mtu** or **mtu** command on an interface, you need to restart the interface to make the new MTU take effect. To restart the interface, run the **shutdown** command and then the **undo shutdown** command, or run the **restart** command in the interface view.

After the **mpls mtu** command is run, LDP compares the MPLS MTU and the interface MTU, and uses the smaller value between the two MTUs.

After the **mpls mtu** command is run:

- The device checks the MTU of packets on the control plane.
- On the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H, the MTU of packets on the forwarding plane is checked only when the following conditions are met:
  - IP packet fragmentation has been enabled using the **ipv4 fragment enable** command.
  - In an MPLS LDP, MPLS TE, static LSP, or L3VPN scenario, IP packets on a PE enter an MPLS network for MPLS encapsulation and forwarding.

Example

Set the MPLS MTU to 1500 bytes on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls mtu 1500
```

Set the MPLS MTU to 1500 bytes on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls mtu 1500
```

9.1.104 mpls total-lsp-number threshold-alarm

Function

The **mpls total-lsp-number threshold-alarm** command configures the alarm threshold for total LSP usage.

The **undo mpls total-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for total LSP usage is 80%. The default lower limit of the clear alarm threshold for total LSP usage is 75%.

Format

mpls total-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls total-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls total-lsp-number threshold-alarm

undo mpls total-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for total LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for total LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Parameter	Description	Value
ingress	Specifies the alarm threshold for total ingress LSPs.	-
transit	Specifies the alarm threshold for total transit LSPs.	-
egress	Specifies the alarm threshold for total egress LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of total LSPs (including static LSPs, LDP LSPs, BGP LSPs, BGP IPv6 LSPs) in the system reaches a specific limit, establishing subsequent LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of total LSPs reaches the specific limit. To configure the alarm threshold for total LSP usage, run the **mpls total-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- *upper-limit-value*: upper alarm threshold. If the proportion of total LSP usage to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of total LSP usage to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

If you want to set the alarm threshold for total ingress LSPs, total transit LSPs or total egress LSPs, run **mpls total-lsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls total-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for total LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm**

trap-name hwmplslspthresholdexceed is configured, and the actual total LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the lower threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual total LSP usage falls below the lower limit of the clear alarm threshold.

Example

Configure the upper limit and the lower limit of the alarm threshold for total LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls total-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.1.105 mpls-passive

Function

The **mpls-passive** command enables the egress node of an LSP to passively create a BFD session.

The **undo mpls-passive** command disables the egress node of an LSP from passively creating a BFD session.

By default, the egress node of an LSP cannot passively create a BFD session.

Format

mpls-passive

undo mpls-passive

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a unidirectional LSP, the ingress node creates a BFD session, which triggers the sending of an LSP ping packet. After the egress node receives the ping packet, a BFD session can be automatically created on the egress node. Run the **mpls-passive** command to enable the BFD session to be created passively on the egress node of an LSP. If the feature is disabled, the egress node cannot automatically create a BFD session.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

You need to run the **mpls-passive** command on the egress node. Then, the egress node can create a BFD session in an opposite direction after receiving an LSP ping request packet carrying a BFD TLV.

Example

Enable the egress node of an LSP to automatically and passively create a BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] mpls-passive
```

9.1.106 mpls ping interval

Function

The **mpls ping interval** command sets the interval at which LSP ping packets are sent in a dynamic BFD session.

The **undo mpls ping interval** command restores the default setting.

By default, the interval at which LSP ping packets are sent in a dynamic BFD session is 60 seconds.

Format

mpls ping interval *interval*

undo mpls ping interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending LSP ping packets.	The value is an integer ranging from 30 to 600, in seconds. The default value is 60.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an LSP, when the active role (the ingress node) creates a dynamic BFD session, an LSP ping request packet carrying a BFD TLV is sent. After receiving the LSP ping request packet, the passive role (the egress node) replies with an LSP ping response packet carrying the BFD TLV. Then, a BFD session is established. To set the interval for sending the LSP ping packet by dynamic BFD, run the **mpls ping interval** command.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

A small interval for sending LSP ping packets imposes a heady burden on links.

Set the interval for sending the LSP ping packet according to the actual networking because the egress node can establish a BFD session only after receiving an LSP ping packet.

Example

Set the interval to 80 seconds for sending LSP ping packets in a dynamic BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] mpls ping interval 80
```

9.1.107 mtu-signalling

Function

The **mtu-signalling** command enables the switch to send Label Mapping messages carrying the MTU TLV and determines the MTU TLV type.

The **undo mtu-signalling** command disables the switch to send Label Mapping messages carrying the MTU TLV

By default, the switch with MPLS LDP globally enabled sends Label Mapping messages carrying the MTU TLV, in compliance with draft-ietf-mpls-ldp-mtu-extensions.

Format

mtu-signalling [**apply-tlv**]

undo mtu-signalling [**apply-tlv**]

Parameters

Parameter	Description	Value
apply-tlv	Indicates the type of MTU TLV carried in Label Mapping messages to be sent. After this parameter is configured, the implementation is in compliance with RFC 3988. If this parameter is not configured, the implementation is in compliance with draft-ietf-mpls-ldp-mtu-extensions.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If different types of links on an MPLS network support different MTU values, this function enables devices to negotiate MTU values, prevents packets from being discarded if the packet size exceeds an MTU.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

By default, after MPLS LDP is globally enabled, a device sends Label Mapping messages carrying an MTU TLV in compliance with draft-ietf-mpls-ldp-mtu-extensions. If an LDP peer does not identify the MTU TLV carried in a received message, the peer must process the TLV as an unknown TLV defined in RFC 5036.

Changing the configuration disconnects an existing LDP session and causes the LDP session to be reestablished.

Example

Enable LDP to send Label Mapping messages carrying the MTU TLV, as defined in RFC3988.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] mtu-signalling apply-tlv
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

9.1.108 no-renegotiate session-parameter-change graceful-restart

Function

The **no-renegotiate session-parameter-change graceful-restart** command disables a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed.

The **undo no-renegotiate session-parameter-change graceful-restart** command restores the default configuration.

By default, a device re-establishes LDP sessions when LDP GR status or a GR parameter is changed.

Format

no-renegotiate session-parameter-change graceful-restart

undo no-renegotiate session-parameter-change graceful-restart

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

After the **no-renegotiate session-parameter-change graceful-restart** command is run, running the following commands does not affect the existing LDP sessions.

- **graceful-restart (MPLS-LDP view)**
- **graceful-restart timer neighbor-liveness**
- **graceful-restart timer reconnect**
- **graceful-restart timer recovery**

Example

Disable a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] no-renegotiate session-parameter-change graceful-restart
```

9.1.109 ospf ldp-sync

Function

The **ospf ldp-sync** command enables synchronization between LDP and OSPF on an interface.

The **undo ospf ldp-sync** command disables synchronization between LDP and OSPF on an interface.

By default, synchronization between LDP and OSPF is disabled on an interface.

Format

ospf ldp-sync

undo ospf ldp-sync

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The LDP convergence speed depends on the convergence speed of OSPF routes. To enable MPLS LDP on a network with the primary and backup links, the following problems may occur:

- Upon a fault on the active link, OSPF routes and ISP are switched to the backup link using LDP FRR. When the primary link recovers, OSPF routes are switched back to the primary link earlier than LDP traffic because IGP route convergence is faster than LDP convergence. As a result, LSP traffic is lost.
- If a fault occurs on the LDP session between nodes on the primary link where the OSPF routes are working properly, the OSPF routes still use the primary link and the LSP on the primary link is deleted. No OSPF route exists on the backup link; therefore, no LSP can be established on the backup link. LSP traffic is lost.

Run the **ospf ldp-sync** command to enable synchronization between LDP and OSPF to prevent traffic loss in the preceding problems. Run this command on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.

Example

Enable synchronization between LDP and OSPF on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf ldp-sync
```

Enable synchronization between LDP and OSPF on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf ldp-sync
```

9.1.110 ospf timer ldp-sync hold-down

Function

The **ospf timer ldp-sync hold-down** command sets the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship.

The **undo ospf timer ldp-sync hold-down** command restores the default setting.

By default, the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship is 10 seconds.

Format

ospf timer ldp-sync hold-down *value*

undo ospf timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is configured, OSPF routes are not immediately switched to the primary link after the primary link is restored and before the LDP session is established. LSP traffic is transmitted through the backup link in a period of time specified by this command.

Prerequisites

LDP and OSPF synchronization has been enabled using the **ospf ldp-sync** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

Set the value of the Hold-down timer for VLANIF100 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the OSPF neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf timer ldp-sync hold-down 15
```

Set the value of the Hold-down timer for GE0/0/1 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the OSPF neighbor relationship.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf timer ldp-sync hold-down 15
```

9.1.111 ospf timer ldp-sync hold-max-cost

Function

The **ospf timer ldp-sync hold-max-cost** command sets the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device.

The **undo ospf timer ldp-sync hold-max-cost** command restores the default setting.

By default, the interval is 10 seconds.

Format

ospf timer ldp-sync hold-max-cost { *value* | **infinite** }

undo ospf timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
value	Specifies the interval for sending OSPF LSAs to advertise the maximum metric on the local device.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that OSPF always advertises the maximum metric in LSAs on the local device before an LDP session is reestablished.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the primary LSP recovers from a fault, run the **ospf timer ldp-sync hold-max-cost** command to set the interval during which traffic is still transmitted along the backup LSP before the LDP session of the primary LSP is reestablished.

You can choose different parameters as required.

- When OSPF carries only LDP services, to ensure that OSPF routing is always consistent with the LDP LSP, specify **infinite**.
- When OSPF carries multiple services including LDP services, to ensure that OSPF route selection and other services still run properly in case the LDP session of the primary LSP fails, specify *value*.

Prerequisites

LDP and OSPF synchronization has been enabled using the **ospf ldp-sync** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

Example

Set the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf ldp-sync
[HUAWEI-Vlanif100] ospf timer ldp-sync hold-max-cost 8
```

Set the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device to 8 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ospf ldp-sync
[HUAWEI-GigabitEthernet0/0/1] ospf timer ldp-sync hold-max-cost 8
```

9.1.112 outbound peer split-horizon

Function

The **outbound peer split-horizon** command enables split horizon on an LSR to allow the LSR to distribute labels only to its upstream LDP peers.

The **undo outbound peer split-horizon** command restores the default setting.

By default, split horizon is not enabled, which means that an LSR distributes labels to both upstream and downstream LDP peers.

Format

outbound peer { *peer-id* | **all** } **split-horizon**

undo outbound peer { *peer-id* | **all** } **split-horizon**

Parameters

Parameter	Description	Value
peer-id	Specifies the LSR ID of an LDP peer.	The value is in dotted decimal notation.
all	Indicates all LDP peers.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Label Mapping messages to both upstream and downstream LDP peers by default, speeding up LDP LSP convergence. This leads to the establishment of a great number of unwanted LSPs, wasting resources. To reduce the number of LSPs and saving memory resources, run the **outbound peer** { *peer-id* | **all** } **split-horizon** command to configure an LDP split horizon policy, enabling the LSR to send Label Mapping messages only to upstream LDP peers.

In the **outbound peer split-horizon** command, configure either of the following parameters to prevent an LSR from distributing labels to specified downstream peers:

- *peer-id*: prevents the LSR from distributing labels to a specified downstream peer.
- **all**: prevents the LSR from distributing labels to all downstream peers.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

The **all** parameter takes preference over the *peer-id* parameter. For example, the **outbound peer all split-horizon** and then **outbound peer 2.2.2.2 split-horizon** commands are run, the **outbound peer all split-horizon** command can be saved in the configuration file and take effect, not the **outbound peer 2.2.2.2 split-horizon** command.

Example

Enable split horizon for all LDP peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] outbound peer all split-horizon
```

9.1.113 path-vectors

Function

The **path-vectors** command sets the maximum number of hops of the path vector that is used for LDP loop detection.

The **undo path-vectors** command restores the default setting.

By default, a maximum of 32 hops of the path vector are used for LDP loop detection.

Format

path-vectors *integer*

undo path-vectors

Parameters

Parameter	Description	Value
integer	Specifies the path vector.	The value is an integer ranging from 1 to 32.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A scenario assumes that LDP loop detection is configured using the path vector, and the maximum number of hops of the path vector is n. The egress LSP triggered by local routes detects loop after n + 1 hops, whereas the egress LSP triggered by non-local routes (proxy egress) detects loops after n hops.

Prerequisites

The **path-vectors** command has been configured before LDP is enabled on all interfaces. The **path-vectors** command takes effect only after **MPLS LDP** is enabled in the related view.

Example

Set the maximum value of the path vector to 3.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] path-vectors 3
```

9.1.114 ping lsp

Function

The **ping lsp** command checks the LSP connectivity and LSP forwarding status.

Format

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **ip** *destination-address mask-length* [*ip-address*] [**nexthop** *nexthop-address* | **draft6**]

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **te tunnel** *interface-number* [**hot-standby** | **primary**] [**draft6**]

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **vpn-instance** *vpn-name* **remote** *remote-address mask-length* [**vpn-frr-path**]

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **bgp** *destination-address mask-length* [*ip-address*]

Parameters

Parameter	Description	Value
-a *source-ip*	Specifies the source IP address of MPLS Echo Request packets to be sent. If the source IP address is not specified, the IP address of the outbound interface from which MPLS Echo Request packets are sent is used as the source IP address. **NOTE** If an E2E BGP LSP has been established between two devices and the LSR ID is not used on the ingress, to run the **ping lsp** command with **bgp** specified on the ingress, you must specify **-a** *source-ip* as the IP address used for establishing the E2E BGP LSP.	-
-c *count*	Specifies the number of MPLS Echo Request packets to be sent. In the case of poor network quality, you can set this parameter to a comparatively large value to check the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-exp *exp-value*	Specifies the EXP value of MPLS Echo Request packets to be sent. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
-h *ttl-value*	Specifies the value of the TTL. Each time the **ping lsp** command is run, an MPLS Echo Request packet carrying a sequence number is sent. The sequence number of the MPLS Echo Request packet starts from 1 and is increased by 1. By default, a maximum of five MPLS Echo Request packets are sent. You can set the number of MPLS Echo Request packets to be sent through the parameter *ttl-value*. If the destination is reachable, the source can receive five MPLS Echo Reply packets from the destination, with sequence numbers corresponding to those of MPLS Echo Request packets. If the TTL field is decreased to 0 during packet forwarding, the switch that the packet reaches sends an MPLS timeout packet to the source, indicating that the destination is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 64.
-m *interval*	Specifies the time to wait before sending the next MPLS Echo Request packet. Each time the source sends an MPLS Echo Request packet using the **ping lsp** command, the source waits a period of time (2000 ms by default) before sending the next MPLS Echo Request packet. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *interval*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets.	The value is an integer that ranges from 1 to 4. The default value is 2. ● 1: The peer does not return MPLS Echo Reply packets. ● 2: The peer end responds to MPLS Echo Reply packets with IPv4 or IPv6 User Datagram Protocol (UDP) packets. ● 3: The peer end responds to MPLS Echo Reply packets with IPv4 or IPv6 UDP packets containing the Router alert option. ● 4: The peer end responds to MPLS Echo Reply packets through the control channel on the application plane.
-s *packet-size*	Indicates the length of the payload in a packet, excluding the IP header and UDP header.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100. The configured value must be smaller than the MTU of the interface.
-t *time-out*	Indicates the timeout period to wait for an MPLS Echo Reply packet after an MPLS Echo Request packet is sent.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.

Parameter	Description	Value
-v	Displays MPLS Echo Reply packets not for the local user. By default, only MPLS Echo Reply packets for the local user are displayed. - If **-v** is not specified, the system displays only the MPLS Echo Reply packets received by the local user. - If **-v** is specified, the system displays all received MPLS Echo Reply packets.	By default, the system displays only the MPLS Echo Reply packets received by the local user.
ip *destination-address mask-length*	Specifies the IPv4 address and mask length of the destination.	The destination IPv4 address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
ip-address	Specifies the destination IP address carried in the IP header of an MPLS Echo Request packet.	The value is in dotted decimal notation. By default, the destination IP address carried in the IP header of an MPLS Echo Request packet is 127.0.0.1.
nexthop *nexthop-address*	Specifies the IP address of the next hop.	The value is in dotted decimal notation.
draft6	Specifies the version of the **ping lsp** command. If this parameter is specified, the ping operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the ping operation is performed according to RFC 4379.	-
te tunnel *interface-number*	Specifies the number of a tunnel interface.	-
hot-standby	Indicates that the hot-standby CR-LSP is to be detected.	-

Parameter	Description	Value
primary	Indicates that the primary CR-LSP is to be monitored.	-
vpn-instance *vpn-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
remote *remote-address mask-length*	Specifies the destination IP address and mask of the VPN LSP to be monitored.	The IP address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
bgp *destination-address mask-length*	Specifies the IP address and mask length of the BGP destination.	-
vpn-frr-path	Specifies that the connectivity of the backup VPN FRR LSP will be checked. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

On an MPLS network, you can run the **ping lsp** command to check LSP connectivity after an LSP is established.

The LSP ping uses Echo Request messages and MPLS Echo Reply messages to monitor the connectivity of LSPs. Both Echo Request and Echo Reply messages are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes Echo Request and MPLS Echo Reply messages based on the port number. An Echo Request message carries FEC information to be monitored and travels along the same LSP as other packets with the same Forwarding Equivalence Class (FEC) to monitor the connectivity of the LSP. Echo Request messages are transmitted to the destination using MPLS, whereas MPLS Echo Reply messages are transmitted to the source using IP.

The LSP ping can be used to monitor the following types of links:

- LDP LSP Ping: Run the **ping lsp ip** *destination-address mask-length* command on the ingress node to ping the egress node to monitor the connectivity of the LSP.
- TE Tunnel Ping: If a tunnel exists, run the **ping lsp te tunnel** *interface-number* command on the ingress node to ping the egress node to monitor the connectivity of the tunnel.
- L3VPN LSP Ping: After a VPN is correctly configured, run the **ping lsp vpn-instance** *vpn-name* **remote** *remote-address mask-length* command on the ingress node to ping the egress node to monitor the connectivity of the VPN LSP established using BGP.

If the **ping lsp** command detects a fault on an LSP that packets transmitted along this LSP cannot reach the egress node, you can run the **tracert lsp** command to locate the fault.

Prerequisites

Before running the **ping lsp** command, ensure that the MPLS module is working properly.

Precautions

To prevent the egress node from forwarding the received MPLS Echo Request packet to other nodes, the destination address in the IP header of the Echo Request packet is set to 127.0.0.1/8 (the local loopback address), and the TTL value contained in the IP header is set to 1.

Example

Ping 10.1.1.1/32 by sending ten 200-byte MPLS Echo Request packets.

```
<HUAWEI> ping lsp -c 10 -s 200 ip 10.1.1.1 32
  LSP PING FEC: IPV4 PREFIX 10.1.1.1/32/ : 200 data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=200 Sequence=1 time = 11 ms
    Reply from 10.1.1.1: bytes=200 Sequence=2 time = 6 ms
    Reply from 10.1.1.1: bytes=200 Sequence=3 time = 6 ms
    Reply from 10.1.1.1: bytes=200 Sequence=4 time = 6 ms
    Reply from 10.1.1.1: bytes=200 Sequence=5 time = 12 ms
    Reply from 10.1.1.1: bytes=200 Sequence=6 time = 9 ms
    Reply from 10.1.1.1: bytes=200 Sequence=7 time = 12 ms
    Reply from 10.1.1.1: bytes=200 Sequence=8 time = 9 ms
    Reply from 10.1.1.1: bytes=200 Sequence=9 time = 12 ms
    Reply from 10.1.1.1: bytes=200 Sequence=10 time = 12 ms

  --- FEC: IPV4 PREFIX 10.1.1.1/32 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/10/12 ms
```

Ping an MPLS TE tunnel.

```
<HUAWEI> ping lsp te tunnel 1
  LSP PING FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 : 100 data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=100 Sequence=1 time = 50 ms
    Reply from 10.1.1.2: bytes=100 Sequence=2 time = 28 ms
    Reply from 10.1.1.2: bytes=100 Sequence=3 time = 33 ms
    Reply from 10.1.1.2: bytes=100 Sequence=4 time = 52 ms
```

```
  Reply from 10.1.1.2: bytes=100 Sequence=5 time = 8 ms
--- FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 8/34/52 ms
```

Ping 10.2.1.1/32 and output detailed information.

```
<HUAWEI> ping lsp -v ip 10.2.1.1 32
 LSP PING FEC: IPV4 PREFIX 10.2.1.1/32 : 100 data bytes, press CTRL_C to break
  Reply from 10.2.1.1: bytes=100 Sequence=1 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=2 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=3 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=4 time = 4 ms Return Code 3, Subcode 1
  Reply from 10.2.1.1: bytes=100 Sequence=5 time = 5 ms Return Code 3, Subcode 1
 --- FEC: IPV4 PREFIX 10.2.1.1/32 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/5 ms
```

Table 9-45 Description of the **ping lsp** command output

Item	Description
Reply from	IP address in an Echo Reply packet.
bytes	Length of an Echo Reply packet.
Sequence	Serial number of an Echo Reply packet.
time	RTT of an Echo Reply packet.

Item	Description
Return Code	Return code. The meaning of each value is as follows: ● 0: No return code is received. ● 1: Incorrect request is received. ● 2: An unknown TLV is received. ● 3: There is the outbound interface of one LSP. ● 4: No mapping between the request device and the replying device exists. ● 5: The mapping does not match that on the downstream device. ● 6: An unknown upstream interface exists. ● 7: The return code is reserved. ● 8: indicates label switching. ● 9: indicates label switching without MPLS forwarding. ● 10: indicates mapping without labels. ● 11: indicates the entity without labels. ● 12: No protocol is loaded on the interface. ● 13: The ping operation is ended ahead of schedule because of shortened labels.
Subcode	Number of labels. Usually, the value is 1.

Item	Description
xxx ping statistics	Statistics collected after the ping test. The statistics include the following information: - packet(s) transmitted: indicates the number of sent ICMP Echo Request messages. - packet(s) received: indicates the number of received ICMP Echo Reply messages. - % packet loss: indicates the percentage of unresponded messages to total sent messages. - round-trip min/avg/max: indicates the minimum, average, and maximum RTTs. The unit is ms.

9.1.115 propagate mapping

Function

The **propagate mapping for ip-prefix** command allows the system to filter out the received routes using an IP prefix list. LDP uses routes that match the addresses in the prefix list to establish an LSP.

The **undo propagate mapping** command restores the default setting.

By default, when LDP establishes an LSP, LDP does not filter out received routes.

Format

propagate mapping for ip-prefix *ip-prefix-name*

undo propagate mapping

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list used to filter out routes.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MPLS LDP is enabled, LDP LSPs are automatically established, leading to a large number of LSPs and wasting resources. Run the **propagate mapping** command to configure a policy for establishing an LSP, allowing LDP to use routes that match the specified conditions to establish LSPs.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device does not filter received routes.

Example

Allow routes that match the IP prefix list named **policy1** to set up an LSP.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] propagate mapping for ip-prefix policy1
```

9.1.116 proxy-egress disable

Function

The **proxy-egress disable** command disables a device from establishing proxy egress LSPs.

The **undo proxy-egress disable** command enables a device to establish proxy egress LSPs.

By default, a device is enabled to establish proxy egress LSPs.

Format

proxy-egress disable

undo proxy-egress disable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a policy allows a device to use all static and IGP routes to establish LSPs or use an IP address prefix list to establish LSPs, the policy also triggers proxy egress LSP establishment. However, the proxy egress LSPs may be unavailable, which wastes system resources. To prevent this problem, run the **proxy-egress disable** command to disable a device from establishing such proxy egress LSPs.

Prerequisites

MPLS has been enabled using the **mpls** command.

Precautions

During the LDP GR, the **proxy-egress disable** command cannot be run.

Example

Disable a device from establishing proxy egress LSPs in the MPLS view.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] proxy-egress disable
```

9.1.117 remote-ip

Function

The **remote-ip** command allows you to assign an IP address to a remote LDP peer.

The **undo remote-ip** command deletes the configuration.

By default, the IP address of the remote LDP peer is not configured.

Format

remote-ip *ip-address* [**pwe3**]

undo remote-ip [**pwe3**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a remote peer.	The value is in decimal notation. The IPv4 address of a local interface is not supported.
pwe3	Prohibits labels from being distributed to a specified remote peer.	-

Views

Remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a remote LDP peer is configured, to assign an IP address to the remote LDP peer, run the **remote-ip** command in the remote MPLS LDP peer view.

The IP address must be the LSR ID of the remote LDP peer. When the LDP LSR ID and the MPLS LSR ID are different, the LDP LSR ID takes effect.

The remote peer uses the LSR ID as the transport address to create a TCP connection.

PEs on both ends of an MPLS L2VPN that runs LDP signaling can establish a remote LDP session. The MPLS L2VPN can be a Martini VLL, PWE3, or Martini VPLS network. The remote LDP session is expected to transmit Label Mapping messages carrying VC labels, not LDP labels. By default, the PE distributes LDP labels to its peer. To disable the PE from distributing LDP labels to its peer, run either of the following commands, which helps prevent LDP label wastes and minimize memory usage.

- **remote-ip** *ip-address* **pwe3** command: prevents the LSR from distributing labels to a specified remote peer.
- **remote-peer pwe3** command: prevents the LSR from distributing labels to all remote peers.

NOTE

When a backbone network is transmitting TE services in the LDP over TE scenario, do not disable a device from distributing labels to remote peers.

Prerequisites

Remote LDP peers have been configured.

Precautions

- Modifying or deleting the configured IP address of a remote peer leads to the deletion of a remote LDP session.
- After a remote peer IP address is specified using the **remote-ip** *ip-address* command, *ip-address* cannot be used as a local interface IP address. If it is used as a local interface IP address, the remote LDP session is interrupted.

Example

Configure the address for a remote peer.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer bji
[HUAWEI-mpls-ldp-remote-bji] remote-ip 10.3.3.3
```

Prohibit labels from being distributed to the remote peer at 10.1.1.1/32.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer rtc
[HUAWEI-mpls-ldp-remote-rtc] remote-ip 10.1.1.1 pwe3
```

9.1.118 remote-ip auto-dod-request

Function

The **remote-ip auto-dod-request** command configures automatic triggering of a request to a specified downstream remote LDP peer for a Label Mapping message in DoD mode.

The **undo remote-ip auto-dod-request** command restores the default setting.

By default, the configuration of the **remote-peer auto-dod-request** command is inherited.

Format

remote-ip auto-dod-request [**block**]

undo remote-ip auto-dod-request [**block**]

Parameters

Parameter	Description	Value
block	Disables the automatic triggering of a request to a downstream node for a Label Mapping message associated with a remote LDP peer of a specified LSR ID in DoD mode.	-

Views

Remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale network, to reduce the burden on edge devices, use the DoD mode. Because edge devices cannot learn the accurate route to the remote peer, an LDP LSP cannot be set up even if LDP extensions for inter-area LSPs are configured. You can configure the DoD mode in which the local LSR requests a Label Mapping message from a specified downstream LSR or all LSRs to set up an LDP LSP.

To block this function, run the **remote-ip auto-dod-request block** command.

Precautions

Before running the **remote-ip auto-dod-request** command, ensure that the following operations has been performed:

- Configure a remote LDP session.
- Run the **longest-match** command to configure LDP extensions for inter-area LSPs.
- Run the **mpls ldp advertisement dod** command to set the DoD mode.

Example

Enable automatic triggering of a request to a downstream specified remote LDP peer for a Label Mapping message in DoD mode.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp remote-peer lsrc
[HUAWEI-mpls-ldp-remote-lsrc] remote-ip 4.4.4.4
[HUAWEI-mpls-ldp-remote-lsrc] remote-ip auto-dod-request
```

9.1.119 remote-peer auto-dod-request

Function

The **remote-peer auto-dod-request** command configures automatically trigger requests for Label Mapping messages in DoD mode from all downstream remote LDP peers.

The **undo remote-peer auto-dod-request** command restores the default setting.

By default, the device does not automatically trigger requests for Label Mapping messages in DoD mode from all downstream remote LDP peers.

Format

remote-peer auto-dod-request

undo remote-peer auto-dod-request

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale network, to reduce the burden on edge devices, use the DoD mode. Because edge devices cannot learn the accurate route to the remote peer, an LDP LSP cannot be set up even if LDP extensions for inter-area LSPs are configured. You can configure the DoD mode in which the local LSR requests a Label Mapping message from a specified downstream LSR or all LSRs to set up an LDP LSP.

Precautions

Before running the **remote-peer auto-dod-request** command, ensure that the following operations have been performed:

- Configure a remote LDP session.
- Run the **longest-match** command to configure LDP extensions for inter-area LSPs.
- Run the **mpls ldp advertisement dod** command to set the DoD mode.

Example

Enable automatically trigger requests for Label Mapping messages in DoD mode from all downstream remote LDP peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] remote-peer auto-dod-request
Warning: The operation will affect all the remote peers on which the attribute is not manually configured.
Continue?[Y/N]:y
```

9.1.120 remote-peer pwe3

Function

The **remote-peer pwe3** command prevents LSP transport labels from being distributed to all remote peers.

The **undo remote-peer pwe3** command restores the default setting.

By default, an LSR is permitted to distribute LSP transport labels to all remote peers.

Format

remote-peer pwe3

undo remote-peer pwe3

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PEs on both ends of an MPLS L2VPN that runs LDP signaling can establish a remote LDP session. The MPLS L2VPN can be a Martini VLL, PWE3, or Martini VPLS network. The remote LDP session is expected to transmit Label Mapping messages carrying VC labels, not LDP labels.

By default, the PE distributes LDP labels to its peer. To disable the PE from distributing LDP labels to its peer, run either of the following commands, which helps prevent LDP label wastes and minimize memory usage.

- The **remote-peer pwe3** command prohibits an LSR from distributing labels to all remote peers.
- The **remote-ip** *ip-address* **pwe3** command in the remote MPLS LDP peer view prohibits an LSR from distributing labels to a specified remote peer.

When you create a remote LDP session, run the **remote-peer pwe3** or **remote-ip** *ip-address* **pwe3** command to prevent LSP transport labels from being distributed to remote peers. If you do not run either of the preceding commands, the command configuration may affect system performance.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

The configuration will take effect on all remote LDP peers, including existing remote peers.

Example

Prevent LSP transport labels from being distributed to all remote peers.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
```

```
[HUAWEI-mpls-ldp] remote-peer pwe3
Warning: The modification has impact on all remote peers including the existing ones. Continue? [Y/N]: y
```

9.1.121 reset lspv statistics

Function

The **reset lspv statistics** command clears LSPV statistics.

Format

reset lspv statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display lspv statistics** command can be used to display LSPV statistics of an LSP ping or trace test instance. LSPV statistics of multiple test instances are accumulated, which obsesses the analysis. The **reset lspv statistics** command can be used to clear LSPV statistics.

If the **reset lspv statistics** command is run before an LSP ping or trace test instance starts, the **display lspv statistics** command displays LSPV statistics of the current test instance.

Precautions

Statistics cannot be restored after being cleared. Therefore, exercise caution before running the **reset lspv statistics** command.

Example

Clear LSPV statistics collected on the device.

```
<HUAWEI> reset lspv statistics
```

9.1.122 reset mpls ldp

Function

The **reset mpls ldp** command resets LDP instances of the public network.

The **reset mpls ldp all** command resets all LDP instances.

Format

reset mpls ldp [**peer** *peer-id*]

reset mpls ldp all

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the LSR ID of a peer.	Expressed in dotted decimal notation.
all	Specifies all LDP instances.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When there is a new LDP configuration, to validate the configuration, you can run the **reset mpls ldp** command.

Run the **reset mpls ldp peer** command to reset sessions, and LSPs, and CR-LSPs of a specified peer.

Precautions

The **reset mpls ldp** command cannot be run during GR.

If this command is run in an attempt to restart LDP and the interval at which LDP is restarted is small, the attempt fails. The interval varies according to the number of LSPs. The more the LSPs are established, the longer the interval is. The interval can be set to 30, 60, 90, or 120, in seconds.

Example

Reset the global LDP function.

```
<HUAWEI> reset mpls ldp
Warning: The MPLS LDP services will be reset. Continue? [Y/N]:y
```

Reset all LDP instances.

```
<HUAWEI> reset mpls ldp all
Warning: The MPLS LDP services will be reset. Continue? [Y/N]:y
```

Reset the peer.

```
<HUAWEI> reset mpls ldp peer 10.2.2.9
```

9.1.123 reset mpls ldp error packet

Function

The **reset mpls ldp error packet** command deletes information about LDP-related error messages.

Format

reset mpls ldp error packet { **tcp** | **udp** | **l2vpn** | **all** }

Parameters

Parameter	Description	Value
tcp	Deletes information about TCP error messages.	-
udp	Deletes information about UDP error messages.	-
l2vpn	Deletes information about L2VPN error messages.	-
all	Deletes information about all LDP-related error messages.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records information about LDP-related error messages. To delete the information, run the **reset mpls ldp error packet** command.

Example

Delete information about LDP-related TCP error messages.

```
<HUAWEI> reset mpls ldp error packet tcp
```

9.1.124 reset mpls ldp event adjacency-down

Function

The **reset mpls ldp event adjacency-down** command deletes the recorded events that LDP adjacencies go Down.

Format

reset mpls ldp event adjacency-down

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records the events that LDP adjacencies go Down. To delete the recorded events, run the **reset mpls ldp event adjacency-down** command.

Example

Delete the recorded events that LDP adjacencies go Down.

```
<HUAWEI> reset mpls ldp event adjacency-down
```

9.1.125 reset mpls ldp event session-down

Function

The **reset mpls ldp event session-down** command deletes the recorded events that LDP sessions go Down.

Format

reset mpls ldp event session-down

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records events that LDP sessions go Down. To delete the recorded events, run the **reset mpls ldp event session-down** command.

Example

Delete the recorded events that LDP sessions go Down.

```
<HUAWEI> reset mpls ldp event session-down
```

9.1.126 route recursive-lookup tunnel

Function

The **route recursive-lookup tunnel** command enables tunnel recursion.

The **undo route recursive-lookup tunnel** command disables tunnel recursion.

By default, tunnel recursion is disabled.

Format

route recursive-lookup tunnel [**only**] [**ip-prefix** *ip-prefix-name*]

undo route recursive-lookup tunnel

Parameters

Parameter	Description	Value
only	Recurses unlabeled public routes only to LSPs.	-
ip-prefix *ip-prefix-name*	Specifies the name of an IP-prefix list.	The value is an existing IP-prefix list name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an unlabeled BGP public network route or a static route can only recurse to the outbound interface and next hop, but not a tunnel. After tunnel recursion is enabled, this route preferentially recurses to an LSP. If no LSP exists, the route can also recurse to the outbound interface and next hop.

After **ip-prefix** *ip-prefix-name* is set, only the unlabeled BGP routes or static routes that match the specified IP prefix list recurse to LSPs.

If the **ip-prefix** *ip-prefix-name* parameter is not set, all static routes and non-labeled public BGP routes will preferentially recurse to LSP tunnels.

Precautions

If the **route recursive-lookup tunnel** command is run for several times, the latest configuration overrides the previous one.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

Recurse the unlabeled public routes to the LSP tunnel.

```
<HUAWEI> system-view
[HUAWEI] route recursive-lookup tunnel
```

Recurse unlabeled public routes only to LSPs.

```
<HUAWEI> system-view
[HUAWEI] route recursive-lookup only
```

9.1.127 snmp-agent trap suppress feature-name lsp

Function

The **snmp-agent trap suppress feature-name lsp** command configures the interval for suppressing the display of excessive LSP traps.

The **undo snmp-agent trap suppress feature-name lsp** command restores the default configuration.

By default, the interval for suppressing the display of excessive LSP traps is 300 seconds, and a maximum of three LSP traps can be sent in the suppression interval.

Format

snmp-agent trap suppress feature-name lsp trap-name { **mplsxcup** | **mplsxcdown** } **trap-interval** *trap-interval* [**max-trap-number** *max-trap-number*]

undo snmp-agent trap suppress feature-name lsp trap-name { **mplsxcup** | **mplsxcdown** } **trap-interval**

Parameters

Parameter	Description	Value
mplsxcup	Indicates the excessive traps generated when an LSP goes Up.	-
mplsxcdown	Indicates the excessive traps generated when an LSP goes Down.	-

Parameter	Description	Value
trap-interval *trap-interval*	Specifies the interval for suppressing the display of excessive LSP traps.	The value is an integer ranging from 0 to 65535, in seconds. By default, the value is 300.
max-trap-number *max-trap-number*	Sets the maximum number of traps to be sent during the suppression interval.	The value is an integer ranging from 1 to 65535. By default, the value is 3. If only *trap-interval* is specified, but *max-trap-number* is not, at most one trap can be sent during the suppression interval.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To prevent excessive traps from being displayed because of frequent LSP status changes, run the **snmp-agent trap suppress feature-name lsp** command to set the interval for suppressing the display of excessive LSP traps. During a specified suppression interval, a trap of a specified type is displayed only once. This setting reduces traps to be displayed.

For example, when the interval for suppressing the display of excessive traps when the LSP goes Down is set to 60s, only one trap indicating that the LSP goes Down is displayed every 60s. Within this interval, no other trap of the same type is displayed, but the number of the same traps generated is logged. During the next 60s, another trap indicating that an LSP goes Down can be displayed.

Example

Set the interval for suppressing the display of excessive traps when an LSP goes Up to 80s.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap suppress feature-name lsp trap-name mplsxcup trap-interval 80
```

9.1.128 static-lsp egress

Function

The **static-lsp egress** command configures the egress node for a static LSP.

The **undo static-lsp egress** command deletes the configuration.

By default, no static LSP is configured for the egress node.

Format

static-lsp egress *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*]

undo static-lsp egress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the inbound interface of an LSP. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
in-label	Specifies the value of an incoming label.	The value is an integer ranging from 16 to 1023.
lsrid *ingress-lsr-id*	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id *tunnel-id*	Specifies the ID of a tunnel.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp egress** command on the egress node to configure a static LSP.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify **incoming-interface** *interface-type interface-number* or **in-label** *in-label*, run the **static-lsp egress** command to set a new value. You do not need to run the **undo static-lsp egress** command before changing a configured value.

Example

Configure the local LSR as the egress node of the static LSP **bj-sh**, with the inbound interface of VLANIF100 and incoming label of 233.

```
<HUAWEI> system-view
[HUAWEI] static-lsp egress bj-sh incoming-interface vlanif 100 in-label 233
```

9.1.129 static-lsp ingress

Function

The **static-lsp ingress** command configures the ingress node for a static LSP.

The **undo static-lsp ingress** command deletes the configuration.

By default, no static LSP is configured for the ingress node.

Format

static-lsp ingress *lsp-name* **destination** *ip-address* { *mask-length* | *mask* } { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label*

static-lsp ingress tunnel-interface tunnel *interface-number* **destination** *ip-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label*

undo static-lsp ingress { *lsp-name* | **tunnel-interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tunnel-interface tunnel *interface-number*	Specifies the index of a tunnel interface.	Numeral type. Range: varies with the configuration.
destination *ip-address*	Specifies the destination IP address.	It is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	An integer ranging from 0 to 32.

Parameter	Description	Value
mask	Specifies the mask of the IP address.	It is in dotted decimal notation.
nexthop *next-hop-address*	Specifies the next-hop address.	It is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
out-label *out-label*	Specifies the value of an outgoing label.	An integer ranging from 16 to 1048575.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp ingress** command on the ingress node to configure a static LSP.

NOTE

The local IP address cannot be designated as the next hop address.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify the parameter **destination** *destination-address*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, or **out-label** *out-label*, run the **static-lsp ingress** command to set a new value. You do not need to run the **undo static-lsp ingress** command before changing a configured value.

When configuring a static LSP, ensure that the route of the static LSP exactly matches the routing information. For example:

- If you specify a next hop when configuring a static LSP, specify a next hop when configuring a static IP route. If you do not specify a next hop, the static LSP cannot be set up. For example:

```
[HUAWEI] ip route-static 10.1.0.0 16 10.1.1.2
[HUAWEI] static-lsp ingress staticlsp1 destination 10.1.0.0 16 nexthop 10.1.1.2 out-label 100
```

- If a dynamic routing protocol applies to the link between LSRs, the next-hop IP address along the LSP must be the same as the IP address of the next hop in the routing table.

If **outgoing-interface** is configured and *next-hop-address* is not configured, Ethernet forwarding failures occur.

Example

Configure the local LSR as the ingress node of the static LSP whose destination address is 10.25.38.1, next hop IP address is 10.55.25.33, and outgoing label is 237.

```
<HUAWEI> system-view
[HUAWEI] static-lsp ingress bj-sh destination 10.25.38.1 24 nexthop 10.55.25.33 out-label 237
```

9.1.130 static-lsp transit

Function

The **static-lsp transit** command configures the transit node for the static LSP.

The **undo static-lsp transit** command deletes the configuration.

By default, the transit node for the static LSP is not configured.

Format

static-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* }* **out-label** *out-label*

undo static-lsp transit *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface	Specifies the inbound interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
next-hop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface	Specifies the outbound interface.	-

Parameter	Description	Value
in-label	Specifies the value of an incoming label.	The value is an integer ranging from 16 to 1023.
out-label	Specifies the value of an outgoing label.	The value is an integer ranging from 16 to 1048575.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp transit** command on the transit node to configure a static LSP.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify the parameter **incoming-interface** *interface-type interface-number*, **in-label** *in-label*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, or **out-label** *out-label*, run the **static-lsp transit** command to set a new value. You do not need to run the **undo static-lsp transit** command before changing a configured value.

If **outgoing-interface** is configured and *next-hop-address* is not configured, Ethernet forwarding failures occur.

Example

Configure the LSR, with the inbound interface of VLANIF100, the incoming label of 123, and the outgoing label of 253, as the transit node of a static LSP named **bj-sh**.

```
<HUAWEI> system-view
[HUAWEI] static-lsp transit bj-sh incoming-interface vlanif 100 in-label 123 nexthop 10.1.1.1 out-label
253
```

9.1.131 static-route timer ldp-sync hold-down

Function

The **static-route timer ldp-sync hold-down** command sets the time during which a static route remains inactive and waits for the establishment of an LDP session.

The **undo static-route timer ldp-sync hold-down** command restores the default setting.

By default, the time during which a static route remains inactive and waits for the establishment of an LDP session is 10 seconds.

Format

static-route timer ldp-sync hold-down { *timer* | **infinite** }

undo static-route timer ldp-sync hold-down

Parameters

Parameter	Description	Value
timer	Specifies the time during which a static route remains inactive and waits for an LDP session to be established.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that the Hold-down timer never expires. A static route becomes active only after an LDP session is established.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network with primary and backup links, LSRs establish LSPs based on static routes. When the LDP session of the primary link becomes faulty (the fault is not caused by a link failure) or the primary link recovers, configuring synchronization between LDP and static routes minimizes traffic loss during traffic switchover and switchback. After synchronization between LDP and static routes is enabled, and the **static-route timer ldp-sync hold-down** command is run, the recovered static route becomes temporarily inactive. It waits for the establishment of an LDP session before the Hold-down timer expires, which synchronizes LDP and the static route.

If the Hold-down timer expires, the static route becomes active regardless of whether an LDP session has been established.

- If the Hold-down timer is set to 0 seconds, synchronization between LDP and static routes is disabled on an interface.
- If the Hold-down timer is set to **infinite**, the timer never expires. In this case, the static route becomes active and MPLS traffic is switched only after an LDP session is established.

Precautions

The Hold-down timer cannot be set on loopback interfaces, Layer 2 Ethernet interfaces, or null interfaces.

Example

Set the time during which a static route remains inactive and waits for the establishment of an LDP session to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] static-route timer ldp-sync hold-down 20
```

9.1.132 timer ldp-sync hold-down

Function

The **timer ldp-sync hold-down** command sets the Hold-down time for all IS-IS interfaces within an IS-IS process so that these interfaces remain in the Hold-down state before LDP sessions are established.

The **undo timer ldp-sync hold-down** command restores the default Hold-down time.

The default Hold-down time is 10 seconds.

Format

timer ldp-sync hold-down *value*

undo timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the period of time during which all IS-IS interfaces within an IS-IS process remain in the Hold-down state before LDP sessions are established.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an active link between two devices enabled with synchronization between LDP and IS-IS recovers from a fault, the IS-IS module enters the Hold-down state and starts a Hold-down timer. This timer allows the devices to create an LDP session and set up an IS-IS neighbor relationship at the same time. Traffic can be switched back to the active link over a reachable IS-IS route for an established LDP LSP.

To set the Hold-down time for all interfaces within an IS-IS process, run the **timer ldp-sync hold-down** command.

Precautions

If both the **timer ldp-sync hold-down** command and the **isis timer ldp-sync hold-down** command in the interface view are executed, the **isis timer ldp-sync hold-down** command takes effect.

Example

Set the Hold-down time for all interfaces within an IS-IS process 100 to **15** seconds.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] timer ldp-sync hold-down 15
```

9.1.133 timer ldp-sync hold-max-cost

Function

The **timer ldp-sync hold-max-cost** command sets the Hold-max-cost time during which all interfaces enabled with synchronization between LDP and IS-IS advertise link state PDUs (LSPs) carrying the maximum route cost.

The **undo timer ldp-sync hold-max-cost** command restores the default setting.

The default Hold-max-cost time is 10 seconds.

Format

timer ldp-sync hold-max-cost { **infinite** | *interval* }

undo timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
infinite	Enables IS-IS to advertise LSPs carrying the maximum route cost before LDP sessions are reestablished.	-
interval	Specifies the Hold-max-cost time during which IS-IS advertises LSPs carrying the maximum route cost on a local device.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After synchronization between LDP and IS-IS is enabled, if the LDP session over the active link fails but the IS-IS route for the active link is reachable, IS-IS advertises the LSPs carrying the maximum route cost so that the IS-IS route and LDP session over a standby link can become reachable at the same time.

To set the Hold-max-cost time, run the **timer ldp-sync hold-max-cost** command.

Select parameters based on networking requirements:

- If an IGP carries only LDP services, configure the parameter **infinite** to ensure that a selected IGP route is kept consistent with the LDP LSP.
- If an IGP carries multiple types of services including LDP services, set the value of the parameter *interval* to ensure that a teardown of LDP sessions does not affect IGP route selection or other services.

Precautions

- If the **timer ldp-sync hold-max-cost infinite** command is executed and the LDP session is Down, interfaces enabled with LDP and IS-IS synchronization keep advertising LSPs carrying the maximum route cost, which affects IS-IS routing.
- If both the **timer ldp-sync hold-max-cost** command and the **isis timer ldp-sync hold-max-cost** command in the interface view are executed, the **isis timer ldp-sync hold-max-cost** command takes effect.

Example

Configure IS-IS to keep advertising the maximum cost by sending Link State PDUs until the LSP is established.

```
<HUAWEI> system-view
[HUAWEI] isis 100
[HUAWEI-isis-100] timer ldp-sync hold-max-cost infinite
```

9.1.134 tracert lsp

Function

The **tracert lsp** command detects the gateways along the LSP from the source to the destination.

Format

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out* | **-v**] * **ip** *destination-address mask-length* [*ip-address*] [**nexthop** *nexthop-address* | **draft6**]

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **te tunnel** *interface-number* [**hot-standby** | **primary**] [**draft6**]

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **bgp** *destination-address mask-length* [*ip-address*]

Parameters

Parameter	Description	Value
-a *source-ip*	Specifies the source IP address of Echo Request packets to be sent. If no source IP address is specified, the IP address of the outbound interface through which Echo Request packets are sent is used as a source IP address. **NOTE** If an E2E BGP LSP has been established between two devices and the LSR ID is not used on the ingress, to run the **tracert lsp** command with **bgp** specified on the ingress, you must specify **-a** *source-ip* as the IP address used for establishing the E2E BGP LSP.	-
-exp *exp-value*	Specifies the EXP value of Echo Request packets to be sent. The EXP value represents the priority of Echo Request packets. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	An integer that ranges from 0 to 7. The default value is 0.
-h *ttl-value*	Specifies the TTL value of MPLS Echo Request packets to be sent. The TTL field indicates the lifetime of the MPLS Echo Request packet and specifies the maximum number of hops that the packet can pass through. The TTL value is set on the source and reduced by 1 each time the packet passes through a hop. When the TTL value is reduced to 0, the packet is discarded. At the same time, an ICMP Timeout message is sent to notify the source host.	An integer that ranges from 1 to 255. The default value is 30.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets.	An integer that ranges from 1 to 4. The default value is 2. The meaning of each value is as follows: ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are responded using the control channels on the application plane. If the value of *reply-mode* is 1, the initiator starts a unidirectional test. If the test succeeds, the initiator prompts that the test times out; if the test fails, the initiator prompts that the LSP does not exist.
-t *time-out*	Specifies the period of time for waiting for an MPLS Echo Reply packet.	An integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet. This parameter is used when LSP transport labels need to be displayed after tracert is initiated on the PE.	-
ip *destination-address mask-length*	Specifies the destination IPv4 address and the mask length.	The destination IPv4 address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.

Parameter	Description	Value
ip-address	Specifies the destination IP address carried in the IP header of an MPLS Echo Request packet.	The value is in dotted decimal notation. By default, the destination IP address carried in the IP header of an MPLS Echo Request packet is 127.0.0.1.
nexthop *nexthop-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
draft6	Specifies the version of the **tracert lsp** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379.	-
te tunnel *interface-number*	Specifies the number of the TE tunnel interface.	-
hot-standby	Indicates that the hot-standby CR-LSP is to be monitored.	-
primary	Indicates that the primary CR-LSP is to be monitored.	-
bgp *destination-address mask-length*	Specifies the destination IP address and mask length of BGP.	*destination-address* is in dotted decimal notation. *mask-length* is an integer that ranges from 0 to 32.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When a fault occurs on the LSPs of an MPLS network, you can run the **ping lsp** command to check the LSP connectivity based on the reply packet, and then run the **tracert lsp** command to locate the fault.

The **tracert lsp** command uses MPLS Echo Request messages and MPLS Echo Reply messages to monitor the connectivity of the LSP. Both MPLS Echo Request and MPLS Echo Reply messages are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes MPLS Echo Request and MPLS Echo Reply messages based on the port number. An MPLS Echo Request message carries FEC information to be monitored, and is sent along the same LSP as other packets with the same FEC. In this manner, the connectivity of the LSP is checked. Echo Request messages are transmitted to the destination using MPLS, whereas MPLS Echo Reply messages are transmitted to the source using IP.

The LSP tracert can be used to monitor the following types of links:

- LDP LSP Tracert: Run the **tracert lsp ip** *destination-address mask-length* command on the ingress node to trace the egress node to detect the fault on the LSP.
- TE Tunnel Tracert: You can run the **tracert lsp te tunnel** *interface-number* command on the ingress node to trace the egress node to check the connectivity of a tunnel.
  - To check the connectivity of a hot-standby tunnel, run the **tracert lsp te tunnel** *interface-number* **hot-standby** command.
  - To check the connectivity of a primary tunnel, run the **tracert lsp te tunnel** *interface-number* **primary** command.

Prerequisites

- The UDP module of each node is working properly; otherwise, the tracert operation fails.
- The MPLS module of each node is enabled and is working properly.
- The ICMP module of each node is working properly; otherwise, three asterisks (* * *) are displayed.

Procedure

The execution process of the **tracert lsp** command is as follows:

- The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
- The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
- The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
- The preceding process proceeds until the MPLS Echo Request packet reaches the destination.

When the device on the destination hop receives the MPLS Echo Request packet, it returns an MPLS Echo Reply packet, indicating the end of the tracert. The purpose behind this is to record the source of each ICMP Timeout packet to provide a trace of the path the packet took to reach the destination.

Precautions

When you run the **tracert lsp te tunnel** *interface-number* command to detect a tunnel, if a transit node is not enabled with LDP, a packet is returned, indicating that the destination is unreachable.

To prevent the egress node from forwarding the received MPLS Echo Request packet to other nodes, you can set the destination address in the IP header of the Echo Request packet to a loopback address with the prefix being 127.0.0.1/8.

Example

Tracert the LSP to 10.4.4.9/32.

```
<HUAWEI> tracert lsp ip 10.4.4.9 32
  LSP Trace Route FEC: IPV4 PREFIX 10.4.4.9/32 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.1.2.2/[1028 ]
  1     10.1.2.2          94 ms   Transit   10.4.4.9/[3 ]
  2     10.4.4.9          94 ms   Egress
```

Tracert the LSP to 10.3.3.9/32 with the MTU value.

```
<HUAWEI> tracert lsp -v ip 10.3.3.9 32
  LSP Trace Route FEC: IPV4 PREFIX 10.3.3.9/32 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream/Label/MTU
  0                                Ingress   172.16.1.1/[3 ]/1500
  1     10.3.3.9          20 ms   Egress
```

Tracert a TE tunnel.

```
<HUAWEI> tracert lsp te tunnel 1
  LSP Trace Route FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel1 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.1.2.2/[13312 ]
  1     10.1.2.2          63 ms   Transit   10.4.4.9/[3 ]
  2     10.6.6.6          93 ms   Egress
```

Table 9-46 Description of the tracert lsp command output

Item	Description
TTL	Indicates the TTL value in an Echo Request packet. It represents the number of hops of the tunnel an Echo Request packet passes.
Replier	IP address of a switching node that returns an MPLS Echo Reply packet.
Time	RTT, in milliseconds.
Type	Type of a node. Available node types: ● Ingress node ● Transit node ● Egress node
Downstream	Address of a downstream device.
Label	Label of a downstream device.
MTU	Link Maximum Transmission Unit.

9.1.135 ttl expiration pop

Function

The **ttl expiration pop** command enables a device to use the local IP route to forward ICMP response packets after the MPLS TTL expires.

The **undo ttl expiration pop** command disables this function. Therefore, ICMP response packets are sent along LSPs.

By default, the LSR returns an ICMP packet using the local IP route if the received MPLS TTL-expired packet contains one label.

Format

ttl expiration pop

undo ttl expiration pop

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network, when an LSR receives MPLS packets with the TTL value of 1, the LSR generates an ICMP TTL-expired message.

The LSR returns the TTL-expired message to the sender in the following ways:

- If the LSR has a reachable route to the sender, it directly sends the TTL-expired message to the sender through the IP route.
- If the LSR has no reachable route to the sender, it forwards the TTL-expired message along the LSP. The egress node forwards the TTL-expired message to the sender.

In most cases, the received MPLS packet contains only one label and the LSR responds to the sender with the TTL-expired message using the first method. If the MPLS packet contains multiple labels, the LSR uses the second method.

The MPLS VPN packets may contain only one label when they arrive at an autonomous system boundary router (ASBR) on the MPLS VPN. These devices have no IP routes to the sender, so they use the second method to reply to the TTL-expired messages.

Precautions

The **undo mpls (system view)** command deletes all configurations of the **ttl expiration pop** command.

Example

Forward ICMP packets through an LSP after the MPLS TTL expires.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] undo ttl expiration pop
```

9.1.136 ttl propagate

Function

The **ttl propagate** command sets the TTL propagate mode of MPLS packets to uniform.

The **undo ttl propagate** command sets the TTL propagate mode of MPLS packets to pipe.

By default, the TTL propagate function is enabled and the MPLS TTL processing mode is uniform.

Format

ttl propagate

undo ttl propagate

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TTL processing modes include uniform and pipe:

- Uniform

  When IP packets reach the ingress node of an MPLS network, the IP TTL decreases by one and is mapped to the MPLS TTL field. In this manner, packets are processed in the standard mode used on the MPLS network. On the egress node, the MPLS TTL decreases by one and is mapped to the IP TTL field. The traceroute output shows the path that the packets pass by.

- Pipe

  On an MPLS network, the IP TTL does not decrease by one at each hop. The traceroute output hides all the hops on the MPLS backbone network, as if the ingress node is directly connected to the egress node.

In MPLS VPN applications, the MPLS backbone network needs to be hidden to ensure network security. The pipe mode is recommended for private network packets.

Precautions

The **ttl propagate** command only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Example

Set the TTL propagate mode of MPLS packets to uniform.

```
<HUAWEI> system-view
[HUAWEI] ttl propagate
```

9.1.137 ttl propagate public

Function

The **ttl propagate public** command enables IP TTL propagation for MPLS packets of the public network.

The **undo ttl propagate public** command disables IP TTL propagation for MPLS packets of the public network.

By default, IP TTL propagation for MPLS packets of the public network is enabled.

Format

ttl propagate public

undo ttl propagate public

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **ttl propagate public** and **undo ttl propagate public** commands only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Example

Enable the IP TTL propagation for MPLS packets of the public network.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] ttl propagate public
```

9.1.138 ttl propagate vpn

Function

The **ttl propagate vpn** command enables IP TTL propagation for MPLS packets of the VPN.

The **undo ttl propagate vpn** command disables IP TTL propagation for MPLS packets of the VPN.

By default, IP TTL propagation is disabled for VPN packets.

Format

ttl propagate vpn

undo ttl propagate vpn

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **ttl propagate vpn** and **undo ttl propagate vpn** commands only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Configure the IP TTL propagation consistently on all PEs. If you enable the IP TTL propagation only on some PEs, the traceroute output cannot reflect the real network situation.

Example

Enable the IP TTL propagation for MPLS packets of the VPN.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] ttl propagate vpn
```

9.1.139 undo outbound peer all

Function

The **undo outbound peer all** command deletes all outbound policies.

Format

undo outbound peer all

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before MPLS LDP is used, the **outbound peer split-horizon** command needs to be executed to configure an outbound policy to control LDP LSP establishments. If multiple outbound policies have been configured, run the **undo outbound peer all** command to simultaneously delete all the outbound policies.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

Running the **undo outbound peer all** command deletes all outbound policies. Therefore, exercise caution when running this command.

Example

Delete all outbound policies.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] undo outbound peer all
```

9.1.140 undo inbound peer all

Function

The **undo inbound peer all** command deletes all inbound policies.

Format

undo inbound peer all

Parameters

None.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete all inbound policies in batches, run the **undo inbound peer all** command.

Before MPLS LDP is used, the **inbound peer fec** command needs to be executed to configure an inbound policy to control LDP LSP establishments. If multiple inbound policies have been configured, run the **undo inbound peer all** command to simultaneously delete all the inbound policies.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

Running the **undo inbound peer all** command deletes all inbound policies. Therefore, exercise caution when running this command.

Example

Delete all inbound policies.

```
<HUAWEI> system-view
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] undo inbound peer all
```

9.2 MPLS QoS Configuration Commands

9.2.1 Command Support

Only the following switch models support MPLS QoS:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

9.2.2 diffserv-mode

Function

The **diffserv-mode** command configures a DiffServ mode for MPLS L2VPN or MPLS L3VPN labels to implement end-to-end QoS.

The **undo diffserv-mode** command restores the default DiffServ mode of an MPLS network.

By default, the uniform mode is used for MPLS L2VPN or MPLS L3VPN labels.

Format

diffserv-mode { **pipe** { **mpls-exp** *mpls-exp* | **domain** *ds-name* } | **short-pipe** [**mpls-exp** *mpls-exp*] **domain** *ds-name* | **uniform** [**domain** *ds-name*] }

undo diffserv-mode

Parameters

Parameter	Description	Value
pipe	Indicates that the DiffServ mode of an MPLS network is pipe.	-
short-pipe	Indicates that the DiffServ mode of an MPLS network is short pipe.	-
uniform	Indicates that the DiffServ mode of an MPLS network is uniform.	-
mpls-exp *mpls-exp*	Specifies the EXP priority in the private label. This parameter is valid only when the DiffServ mode on the ingress PE is set to pipe or short pipe. It is invalid on the egress PE. If a DiffServ domain is configured, the inner label specified by *mpls-exp* is preferred for the mapping. When the *mpls-exp* parameter is set to a large value, the packets have high priority and packet forwarding quality is high.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
domain *ds-name*	Indicates the name of the DiffServ domain. The default DiffServ domain name is **default**. This parameter is specified in the **diffserv domain** command.	The value is an existing DiffServ domain name.

Views

Interface view, VSI view, VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for VPN traffic on an MPLS VPN network, set the DiffServ mode based on actual needs.

- If you want to differentiate priorities of different services in a VPN, set the DiffServ mode to uniform. You can also set the DiffServ mode to pipe or short pipe, but you need to specify the DiffServ domain in which the mode applies.
- If you want to differentiate priorities of services in different VPNs but not priorities of services in a VPN, set the DiffServ mode to pipe or short pipe and specify EXP values in private labels.

If you do not want to change priorities carried in original packets, you are advised to set the DiffServ mode to pipe or short pipe. In uniform and pipe modes, the egress node determines the per-hop behavior (PHB) based on EXP priorities of packets. In short pipe mode, the egress node determines the PHB based on DSCP or 802.1p priorities of packets.

Precautions

Before configuring the MPLS Diff-Serv mode for IPv4 services, ensure that an IPv4 address family is configured in the VPN instance view using the **ipv4-family** command.

Before configuring the MPLS Diff-Serv mode for IPv6 services, ensure that an IPv6 address family is configured in the VPN instance view using the **ipv6-family** command.

On the ingress, all the three modes can be set. On the egress, only the short pipe mode can be set.

- If you specify the DiffServ domain in the **diffserv-mode** command, ensure that the specified DiffServ domain is already created using the **diffserv domain** command in the system view.
- Before running this command, use the **undo portswitch** command to set the working mode of the Ethernet interfaces to Layer 3 mode.

- The **diffserv-mode** command takes effect only for the new LSPs. To make the command take effect for the existing LSPs, run the **reset mpls ldp** command to reestablish LSPs.

Example

On VLANIF100, set the MPLS DiffServ mode to pipe and the value of *mpls-exp* to 3.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] diffserv-mode pipe mpls-exp 3
```

On GE0/0/1, set the MPLS DiffServ mode to pipe and the value of *mpls-exp* to 3.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] diffserv-mode pipe mpls-exp 3
```

9.2.3 mpls-exp-inbound

Function

The **mpls-exp-inbound** command maps EXP priorities of MPLS packets to PHBs and colors in a DiffServ domain on an inbound interface.

The **undo mpls-exp-inbound** command restores the default mapping.

The following table shows the default mappings from EXP priorities to PHBs and colors of MPLS packets in a DiffServ domain on an inbound interface.

Table 9-47 Default mappings from EXP priorities to PHBs and colors of MPLS packets in a DiffServ domain on an inbound interface

EXP Priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

Format

mpls-exp-inbound *exp-value* **phb** *service-class* [*color*]

undo mpls-exp-inbound [*exp-value*]

Parameters

Parameter	Description	Value
exp-value	Specifies the EXP priority of an MPLS packet.	The value is an integer ranging from 0 to 7. A larger value indicates a higher EXP priority of MPLS packets.
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7.
color	Specifies the color of a packet.	The value can be green, yellow, or red.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

To implement QoS scheduling on the MPLS packets that come from the upstream device, run the **mpls-exp-inbound** command to map EXP priorities of MPLS packets to PHBs and colors. After a DiffServ domain is bound to the inbound interface of packets, the QoS mechanism performs congestion management and congestion avoidance according to PHBs and colors of the packets.

Example

In the DiffServ domain **ds1**, map EXP priority 2 of MPLS packets to PHB AF1 and color incoming MPLS packets as yellow.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] mpls-exp-inbound 2 phb af1 yellow
```

9.2.4 mpls-exp-outbound

Function

The **mpls-exp-outbound** command maps PHBs and colors of MPLS packets to EXP priorities in a DiffServ domain on an outbound interface.

The **undo mpls-exp-outbound** command restores the default mapping.

The following table shows the default mappings from PHBs and colors to EXP priorities of MPLS packets in a DiffServ domain on an outbound interface.

Table 9-48 Default mappings from PHBs and colors to EXP priorities of MPLS packets in a DiffServ domain on an outbound interface

PHB	Color	EXP Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

Format

mpls-exp-outbound *service-class color* **map** *exp-value*

undo mpls-exp-outbound [*service-class color*]

Parameters

Parameter	Description	Value
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7.
color	Specifies the color of a packet.	The value can be green, yellow, or red.
exp-value	Specifies the EXP priority of an MPLS packet.	The value is an integer ranging from 0 to 7. A larger value indicates a higher EXP priority of the MPLS packet.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

After QoS scheduling is performed on the MPLS packets, run the **mpls-exp-outbound** command to map the PHB and color of the MPLS packets in a DiffServ domain to the EXP priority. After the DiffServ domain is bound to the outbound interface of MPLS packets, the downstream device implements QoS scheduling according to EXP priority.

The switch can map PHBs and colors in MPLS packets to EXP priorities and 802.1p priorities on an outbound interface.

Example

In the DiffServ domain **ds1**, map the PHB AF1 of outgoing MPLS packets marked yellow to EXP priority 2.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] mpls-exp-outbound af1 yellow map 2
```

9.2.5 mpls-qos egress

Function

The **mpls-qos egress** command maps the mapping from the EXP priority of the public tunnel to the PHB/color on the egress node.

The **undo mpls-qos egress** command restores the default settings.

By default, mapping of the EXP priority of the public tunnel is performed according to the settings in the default domain.

Format

mpls-qos egress trust upstream { *ds-name* | **default** }

undo mpls-qos egress trust upstream

mpls-qos egress trust upstream none

undo mpls-qos egress trust upstream none

Parameters

Parameter	Description	Value
trust upstream	Trusts the specified DiffServ domain.	-
ds-name	Specifies the name of a DiffServ domain.	The value is an existing DiffServ domain name.
default	Specifies the DiffServ domain as a default domain.	-
none	Indicates that the system does not perform EXP priority mapping in the public network tunnel, and sets the EXP field to 0 in the public network tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement certain QoS functions on an MPLS network, the device needs to determine the packet precedence according to the tunnel label of the MPLS public network. Therefore, you need to map the tunnel label to the EXP field.

Prerequisites

The specified DiffServ domain has been created using the **diffserv domain** command in the system view.

Precautions

Run the **mpls-qos egress** command before setting up the public tunnel; otherwise, you must reestablish the MPLS LDP session to make the command take effect.

If you modify the settings of the global DiffServ domain or change the DiffServ mode of the interface, VSI, or VPN instance, you must reestablish the MPLS LDP session; otherwise, the modification cannot take effect.

Example

Map the mapping from the EXP priority of the public tunnel to the PHB/color on the egress node.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] quit
[HUAWEI] mpls-qos egress trust upstream ds1
```

9.2.6 mpls-qos ingress

Function

The **mpls-qos ingress** command maps the PHB/color of packets to the EXP priority of the public tunnel on the ingress node.

The **undo mpls-qos ingress** command restores the default settings.

By default, mapping of the EXP priority of the public tunnel is performed according to the settings in the default domain.

Format

mpls-qos ingress { **use vpn-label-exp** | **trust upstream** { *ds-name* | **default** } }

undo mpls-qos ingress { **use vpn-label-exp** | **trust upstream** }

mpls-qos ingress trust upstream none

undo mpls-qos ingress trust upstream none

Parameters

Parameter	Description	Value
use vpn-label-exp	Indicates the EXP value in the inner label of a packet.	-
trust upstream	Trusts the specified DiffServ domain.	-
ds-name	Specifies the name of a DiffServ domain.	The value is an existing DiffServ domain name.

Parameter	Description	Value
default	Specifies the DiffServ domain as a default domain.	-
none	Indicates that the system does not perform EXP priority mapping in the public network tunnel, and sets the EXP field to 0 in the public network tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement certain QoS functions on an MPLS network, the device needs to determine the packet precedence according to the tunnel label of the MPLS public network. Therefore, you need to map the tunnel label to the EXP field. You can specify **use vpn-label-exp**.

Prerequisites

The specified DiffServ domain has been created using the **diffserv domain** command in the system view.

Precautions

Run the **mpls-qos ingress** command before setting up the public tunnel; otherwise, you must reestablish the MPLS LDP session to make the command take effect.

Example

Map the PHB/color of packets to the EXP priority of the public tunnel on the ingress node.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] quit
[HUAWEI] mpls-qos ingress trust upstream ds1
```

System Response

None

9.2.7 mpls-qos transit

Function

The **mpls-qos transit** command performs the priority mapping based on the EXP priority of the public tunnel on the transit node.

The **undo mpls-qos transit** command restores the default settings.

By default, mapping of the EXP priority of the public tunnel is performed according to the settings in the default domain.

Format

mpls-qos transit trust upstream { *ds-name* | **default** }

undo mpls-qos transit trust upstream

mpls-qos transit trust upstream none

undo mpls-qos transit trust upstream none

Parameters

Parameter	Description	Value
trust upstream	Trusts the specified DiffServ domain.	-
ds-name	Specifies the name of a DiffServ domain.	The value is an existing DiffServ domain name.
default	Specifies the DiffServ domain as a default domain.	-
none	Indicates that the system does not perform EXP priority mapping in the public network tunnel, and sets the EXP field to 0 in the public network tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement certain QoS functions on an MPLS network, the device needs to determine the packet precedence according to the tunnel label of the MPLS public network. Therefore, you need to map the tunnel label to the EXP field.

Prerequisites

The specified DiffServ domain has been created using the **diffserv domain** command in the system view.

Precautions

Run before setting up the public tunnel; otherwise, you must reestablish the MPLS LDP session to make the command take effect.

If you modify the settings of the global DiffServ domain or change the DiffServ mode of the interface, VSI, or VPN instance, you must reestablish the MPLS LDP session; otherwise, the modification cannot take effect.

Example

Perform the priority mapping based on the EXP priority of the public tunnel on the transit node.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] quit
[HUAWEI] mpls-qos transit trust upstream ds1
```

9.3 MPLS TE Configuration Commands

9.3.1 Command Support

Only the following switch models support MPLS TE:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

9.3.2 add hop

Function

The **add hop** command adds a specified node on an MPLS TE explicit path.

Format

add hop *ip-address1* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**] { **after** | **before** } *ip-address2*

Parameters

Parameter	Description	Value
ip-address1	Specifies the IP address of the added node.	The value is in dotted decimal notation.

Parameter	Description	Value
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Specifies the node with an IP address *ip-address1* on the explicit path. - **strict**: indicates that the node is added in **strict** mode. The node of *ip-address1* is directly connected to the node of *ip-address2*. - **loose**: indicates that the node is added in **loose** mode. The node of *ip-address1* may not be directly connected to the node of *ip-address2*. - **incoming**: indicates that the *ip-address1* is the IP address of an inbound interface of a new-added node. - **outgoing**: indicates that the *ip-address1* is the IP address of an outbound interface of a new-added node.	By default, an explicit path is added in **include strict** mode.
exclude	Excludes the node of *ip-address1* from the explicit path.	-
after	Indicates that the node of *ip-address1* is added after the node of *ip-address2*.	-
before	Indicates that the node of *ip-address1* is added before the node of *ip-address2*.	-
ip-address2	Specifies the IP address of an interface or the Router ID of a node on the explicit path.	The value is in dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Prerequisites

The **next hop** command must have been run to specify a next-hop IP address before the **add hop** command is run.

Follow-up Procedure

Run the **display explicit-path** command to view information about the explicit path.

Precautions

A node can be added to an explicit path using the **add hop** command only when the following conditions are met:

- *ip-address2* is the IP address of a node that exists on the explicit path.
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

Exclude the next hop of 10.2.2.2 after 10.1.1.1 from the explicit path named **p1**.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] next hop 10.1.1.1
[HUAWEI-explicit-path-p1] add hop 10.2.2.2 exclude after 10.1.1.1
```

9.3.3 affinity property

Function

The **affinity property** command configures the affinity property for a CR-LSP attribute template.

The **undo affinity property** command deletes the affinity property from a CR-LSP attribute template.

By default, no affinity property for a CR-LSP attribute template is configured.

Format

affinity property *affinity-value* [**mask** *mask-value*]

undo affinity property

Parameters

Parameter	Description	Value
affinity-value	Specifies the value of the affinity property.	The value ranges from 0x0 to 0xFFFFFFFF, in hexadecimal format. By default, the affinity value is 0.

Parameter	Description	Value
mask *mask-value*	Specifies the mask value of an affinity property. Then an operation is performed between the mask value and the affinity property value, and the result indicates the bits of the affinity property to be checked.	The value ranges from 0x0 to 0xFFFFFFFF, in hexadecimal format. By default, the value is 0.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Affinity property and masks determine the link properties that should be checked by a device.

Example

Set the affinity property to 123 and the mask to fff in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] affinity property 123 mask fff
```

9.3.4 bandwidth (LSP attribute view)

Function

The **bandwidth** command configures the bandwidth in the CR-LSP attribute template.

The **undo bandwidth** command deletes the bandwidth in the CR-LSP attribute template.

By default, no bandwidth in the CR-LSP attribute template is configured.

Format

bandwidth { **ct0** *ct0-bandwidth* | **ct1** *ct1-bandwidth* }

undo bandwidth { **all** | **ct0** | **ct1** }

Parameters

Parameter	Description	Value
ct0 *ct0-bandwidth*	Specifies the bandwidth of an LSP of CT0.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. By default, the bandwidth is 0 kbit/s.
ct1 *ct1-bandwidth*	Specifies the bandwidth of an LSP of CT1.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. By default, the bandwidth is 0 kbit/s.
all	Deletes the bandwidth configured for the LSP of each CT.	-

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **undo bandwidth** command can be used to delete the bandwidth of all CTs or a specified CT:

- **undo bandwidth all**: deletes all configured bandwidth.
- **undo bandwidth** { **ct0** | **ct1** }: deletes the bandwidth of the specified CT configured on the current TE tunnel.

Example

Configure the bandwidth of an LSP of CT0 as 20 kbit/s in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] bandwidth ct0 20
```

9.3.5 bfd bind mpls-te

Function

The **bfd bind mpls-te** command configures BFD to monitor TE tunnels, or the primary or backup LSP bound to a TE tunnel.

The **undo bfd** command deletes a specified BFD session.

By default, no TE tunnel applies BFD.

Format

bfd *cfg-name* **bind mpls-te interface tunnel** *interface-number* [**te-lsp** [**backup**]]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the BFD configuration name.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface tunnel *interface-number*	Specifies the interface number of the TE tunnel bound to a BFD session.	-
te-lsp [**backup**]	Indicates that BFD monitors the LSP bound to the TE tunnel. ● If **backup** is not selected, BFD monitors the primary LSP bound to the TE tunnel. ● If **backup** is selected, BFD monitors the backup LSP bound to the TE tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **bfd bind mpls-te** command to configure BFD to monitor TE tunnels, or the primary or backup LSP bound to a TE tunnel.

Prerequisites

Before configuring BFD to monitor TE tunnels, the following tasks must have been completed:

- BFD has been enabled globally using the **bfd** command.
- An MPLS TE tunnel interface has been configured.

Precautions

BFD can monitor a TE tunnel and the primary or backup LSP bound to the TE tunnel.

- If BFD is configured to monitor the primary or backup LSP bound to a TE tunnel, a BFD session cannot be created if the LSP status is Down.
- If the tunnel status is Down when BFD is configured to monitor a TE tunnel, the BFD session can still be created, but its status is Down.

  Multiple LSPs can be bound to a TE tunnel. When BFD detects the tunnel, the BFD session will go Down only if all LSPs bound to the TE tunnel fail.

Example

Configure BFD to detect the primary LSP bound to the TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] bfd 1to4rsvp bind mpls-te interface Tunnel 1 te-lsp
[HUAWEI-bfd-lsp-session-1to4rsvp]
```

Configure BFD to detect the backup LSP bound to the TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] bfd 1to4backup bind mpls-te interface Tunnel 1 te-lsp backup
[HUAWEI-bfd-lsp-session-1to4backup]
```

9.3.6 bypass-attributes

Function

The **bypass-attributes** command configures bypass CR-LSP attributes in a CR-LSP attribute template.

The **undo bypass-attributes** command deletes bypass CR-LSP attributes from a CR-LSP attribute template.

By default, no bypass CR-LSP attributes are configured.

Format

bypass-attributes { **bandwidth** *bandwidth* | **priority** *setup_priority_value* [*hold_priority_value*] }*

undo bypass-attributes

Parameters

Parameter	Description	Value
bandwidth *bandwidth*	Specifies the bandwidth value assigned to a bypass CR-LSP. **NOTE** The function of bandwidth value assigned to a bypass CR-LSP does not take effect on the devices.	An integer ranging from 1 to 4000000000, in kbit/s. By default, the bandwidth is 0 kbit/s.
priority *setup_priority_value*	Specifies the setup priority of a bypass CR-LSP.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. By default, the setup priority is 7.
hold_priority_value	Specifies the holding priority of the bypass CR-LSP.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. By default, the holding priority is 7.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

To configure the **bypass-attributes** command in the CR-LSP attribute template, note the following preconditions:

- The **fast-reroute bandwidth** command must be configured in the CR-LSP attribute template, and the bandwidth of the bypass CR-LSP must be less than or equal to that of the primary CR-LSP.
- The bandwidth of the bypass CR-LSP must be less than or equal to that of the CR-LSP attribute template.
- The values of the setup and holding priority of the CR-LSP attribute template must be less than or equal to those of the bypass CR-LSP.

Example

Configure the bypass CR-LSP attributes in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] fast-reroute bandwidth
[HUAWEI-lsp-attribute-lsp-attribute-name] bypass-attributes bandwidth 30 priority 5 5
```

9.3.7 commit (LSP attribute view)

Function

The **commit** command commits the configurations of the CR-LSP attribute template.

Format

commit

Parameters

None

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

When the CR-LSP attribute template is modified, if the commands that conflict with the CR-LSP attribute template are configured on a tunnel interface, the configurations of the CR-LSP attribute template cannot be committed.

When the CR-LSP attribute template is applied by a tunnel, you can modify the tunnel attributes by modifying the configurations of the CR-LSP attribute template. Different modifications in the CR-LSP attribute template have different impacts on the setup of the tunnel. If the priorities of the CR-LSP attribute template are modified, Break-Before-Make (BBM) is performed on the tunnel. If the Make-Before-Break (MBB) attribute of the CR-LSP attribute template is modified, MBB may be performed on the tunnel.

Example

Configure the CR-LSP attribute template and commit relevant configurations.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] hop-limit 15
[HUAWEI-lsp-attribute-lsp-attribute-name] commit
```

9.3.8 delete hop

Function

The **delete hop** command deletes a specified node from an MPLS TE explicit path.

Format

delete hop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an interface on a node.	In dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Follow-up Procedure

Run the **display explicit-path** command to view information about the explicit path.

Precautions

A node can be deleted from an explicit path using the **delete hop** command only when the following conditions are met:

- The node must exist on the explicit path
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

Delete the node of 10.10.10.10 from the MPLS TE explicit path.

```
<HUAWEI> system-view
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] list hop
 Path Name : p1         Path Status : Enabled
 1       2.2.2.2            Strict       Include
 2       10.10.10.10        Strict       Include
 3       10.20.20.20        Strict       Include
[HUAWEI-explicit-path-p1] delete hop 10.10.10.10
```

```
[HUAWEI-explicit-path-p1] list hop
 Path Name : p1         Path Status : Enabled
 1       2.2.2.2           Strict       Include
 2       10.20.20.20        Strict       Include
```

9.3.9 display default-parameter mpls rsvp-te

Function

The **display default-parameter mpls rsvp-te** command displays the default parameters of MPLS RSVP-TE.

Format

display default-parameter mpls rsvp-te

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS RSVP-TE, run the **display default-parameter mpls rsvp-te** command.

Example

Display default MPLS RSVP-TE parameters.

```
<HUAWEI> display default-parameter mpls rsvp-te
  RSVP-TE View Default Configurations:
  ------------------------------------------
  Resv Confirmation Request  : Disabled
  RSVP Hello Extension       : Disabled
  GR Capability              : Disabled
  GR Basic-Restart-Time      : 90000 ms
  Hello Interval             : 3000 ms
  Max Times Of Hello Misses  : 3
  Path/Resv Message Refresh Interval    : 30000 ms
  Path/Resv Message Refresh Retry Times : 3
  Challenge Retransmission Interval     : 1000 ms
  Max Times Of Challenge Lost           : 3
  Soft Preemption Timeout               : 30 s

  Interface View Default Configurations:
  ------------------------------------------
  SRefresh Feature           : Disabled
  Authentication Feature     : Disabled
  BFD Feature                : Disabled
  Hello Feature              : Disabled
  BFD Min-Tx                 : 1000
  BFD Min-Rx                  : 1000
```

```
BFD Detect-Multi          : 3
MPLS MTU                  : 1500
SRefresh Interval         : 30000 ms
SRefresh Retransmission Interval        : 5000 ms
SRefresh Retransmission Increment Value : 1
Authentication Life Time                : 1800000 ms
```

Table 9-49 Description of the display default-parameter mpls rsvp-te command output

Item	Description
Resv Confirmation Request	Whether the request for reservation confirmation is enabled.
RSVP Hello Extension	Whether the Hello extension is enabled.
GR Capability	RSVP GR capability.
GR Basic-Restart-Time	Basic RSVP GR time.
Hello Interval	Interval of Hello message.
Max Times Of Hello Misses	Maximum number of Hello messages that consecutively fail to be received.
Path/Resv Message Refresh Interval	Interval for refreshing Path or Resv messages.
Path/Resv Message Refresh Retry Times	Interval for retrying refreshing Path or Resv messages.
Challenge Retransmission Interval	Interval for resending Challenge messages.
Max Times Of Challenge Lost	Maximum number of Challenge messages that consecutively fail to be received.
Soft Preemption Timeout	The timeout of soft preemption
SRefresh Feature	Whether Srefresh is enabled.
Authentication Feature	Whether authentication is enabled.
BFD Feature	Whether BFD is enabled.
Hello Feature	Whether the Hello feature is enabled.
BFD Min-Tx	Actual interval for sending BFD packets.
BFD Min-Rx	Actual interval for receiving BFD packets.
BFD Detect-Multi	Actual local BFD detection multiplier.
MPLS MTU	Actual MTU value used for MPLS forwarding.
SRefresh Interval	Srefresh interval.
SRefresh Retransmission Interval	Srefresh retransmission interval.

Item	Description
SRefresh Retransmission Increment Value	Increment value of Srefresh retransmission.
Authentication Life Time	Authentication lifetime.

9.3.10 display default-parameter mpls te cspf

Function

The **display default-parameter mpls te cspf** command displays the default CSPF configurations.

Format

display default-parameter mpls te cspf

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of CSPF, run the **display default-parameter mpls te cspf** command.

Example

Display the default CSPF configurations.

```
<HUAWEI> display default-parameter mpls te cspf
----------------------------------------------
        CSPF Default Configuration
----------------------------------------------
        Preferred-IGP : OSPF
        Failed-link Interval(Sec): 10
```

Table 9-50 Description of the display default-parameter mpls te cspf command output

Item	Description
Preferred-IGP	The IGP type whose database is in CSPF TEDB and that will be preferred for path calculation.
Failed-link Interval(Sec)	The default value of the failed link timer.

9.3.11 display default-parameter mpls te management

Function

The **display default-parameter mpls te management** command displays the default configurations of the MPLS TE management module.

Format

display default-parameter mpls te management

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of the MPLS TE management module, run the **display default-parameter mpls te management** command.

Example

Display the default configurations of the MPLS TE management module.

```
<HUAWEI> display default-parameter mpls te management

  Global Information
  ----------------------------------------------------------
  DS-TE MODE                      : NON-IETF
  Bandwidth constraint model          : RDM
  Switch-delay time(ms)             : 5000
  Delete-delay time(ms)             : 7000
  Auto-bandwidth timer(sec)           : 300
  FRR timer(sec)                 : 300
  Path metric-type                : TE
  Tie-breaking                   : Random
```

```
------------------------------------------------------------

Interface Information
------------------------------------------------------------
Administrative group value              : 0
TE metric value                         : 0
Bandwidth change thresholds up          : 10
Bandwidth change thresholds down        : 10
------------------------------------------------------------

Tunnel Interface Information
------------------------------------------------------------
Retry timer(sec)                        : 30
Set priority                            : 7
Hold priority                           : 7
Default signal protocol                 : Rsvp
Default resv-style                      : SE
Default classtype                       : CT0
Reoptimization frequency(sec)           : 3600
Auto-bandwidth adjustment frequency(sec) : 86400
Auto-bandwidth max-bw                   : 4294901760
Auto-bandwidth min-bw                   : 0
Auto-bandwidth threshold                : 0
Hop-limit                               : 32
Diffserv-mode                           : Uniform
------------------------------------------------------------

Explicit-path Information
------------------------------------------------------------
Default type                            : include strict
------------------------------------------------------------

Default TEClass Mapping
------------------------------------------------------------
TE-Class    ID    Class Type    Priority
TE-Class    0     0             0
TE-Class    1     1             0
TE-Class    2     2             0
TE-Class    3     3             0
TE-Class    4     0             7
TE-Class    5     1             7
TE-Class    6     2             7
TE-Class    7     3             7
------------------------------------------------------------
```

Table 9-51 Description of the display default-parameter mpls te management command output

Item	Description
DS-TE MODE	DS-TE mode: • IETF: indicates DS-TE in IETF mode. • NON-IETF: indicates DS-TE in non-IETF mode.
Bandwidth constraint model	Bandwidth Constraints model: • RDM: indicates the Russian Dolls Model. • MAM: indicates the Maximum Allocation Model. • Extended MAM: indicates the extended Maximum Allocation Model.

Item	Description
Switch-delay time(ms)	Delay time before switching TE traffic from the primary CR-LSP to the modified CR-LSP in milliseconds.
Delete-delay time(ms)	Delay before deleting the primary CR-LSP after TE traffic is switched to the modified CR-LSP, in milliseconds.
Auto-bandwidth timer(sec)	Time interval at which the output rate of each tunnel configured with automatic bandwidth adjustment is sampled, in seconds.
FRR timer(sec)	FRR switching time, in seconds.
Path metric-type	Link metric type for path selection for tunnels.
Tie-breaking	Rule for selecting a route to the destination if multiple routes of equal cost are available.
Administrative group value	Administrative-group attribute.
TE metric value	TE metric of a link.
Bandwidth change thresholds up	Upper threshold of the bandwidth of an MPLS TE tunnel to be flooded.
Bandwidth change thresholds down	Lower threshold of the bandwidth of an MPLS TE tunnel to be flooded.
Retry timer(sec)	Time interval between attempts to establish a tunnel, in seconds.
Set priority	Setup priority.
Hold priority	Holding priority.
Default signal protocol	Signaling protocol used to set up an LSP.
Default resv-style	Resource reservation style.
Default classtype	Class type.
Reoptimization frequency(sec)	Time interval between attempts of re-optimization, in seconds.
Auto-bandwidth adjustment frequency(sec)	Time interval between attempts of automatic bandwidth adjustment, in seconds.
Auto-bandwidth max-bw	Maximum bandwidth allowed by automatic bandwidth adjustment.
Auto-bandwidth min-bw	Minimum bandwidth allowed by automatic bandwidth adjustment.
Auto-bandwidth threshold	Indicates the threshold of the difference between the new and existing bandwidth. The value is expressed in percentage.

Item	Description
Hop-limit	Maximum number of hops.
Diffserv-mode	DiffServ mode.
Default type	Default type.
TE-Class ID	TE-class ID. The value is an integer that ranges from 0 to 7.
Class Type	Service type. When the TE-class is not configured, "--" is displayed.
Priority	Preemption priority of a tunnel. The value is an integer that ranges from 0 to 7. The smaller the value, the higher tunnel preemption priority.

9.3.12 display explicit-path

Function

The **display explicit-path** command displays information about an explicit path and the tunnels using it.

Format

display explicit-path [[**name**] *path-name*] [**tunnel-interface** | **lsp-attribute** | **verbose**]

Parameters

Parameter	Description	Value
name	Displays information about the specified explicit path.	-
path-name	Specifies the explicit path name.	The value is an existing explicit path name.
tunnel-interface	Displays information about the interface of the tunnel that uses the explicit path.	-
lsp-attribute	Displays information about the LSP attribute template that uses the explicit path.	-
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no path name is specified, information about all explicit paths is displayed.

Example

Display detailed information about the explicit path named p1.

```
<HUAWEI> display explicit-path p1 verbose
Path Name : p1          Path Status : Enabled
 1      1.1.1.1          Strict      Include
 2      2.2.2.2          Strict      Exclude
 3      3.3.3.3          Loose        Include            Outgoing
 4      4.4.4.4          Strict      Include            Incoming
 List of p2p tunnels using this path:
     Tunnel1
 Number of p2p tunnels using this path: 1
 List of lsp-attributes referring this path:
     a1
 Number of lsp-attributes referring this path: 1
```

Table 9-52 Description of the display explicit-path verbose command output

Item	Description
Path Name	Name of an explicit path.
Path Status	Status of an explicit path. ● Enabled ● Disabled
Strict	The address is a strict next hop. The address is the ingress address or the address of the node that is connected directly to the previous node.
Loose	The address is a loose next hop.
Include	The explicit path contains the node of this IP address.
Exclude	The explicit path does not contain the node of this IP address.

Item	Description
Incoming or Outgoing	Type of an interface to which the IP address belongs: ● Incoming ● Outgoing If this field is not displayed, the IP address belongs to either an outbound interface or an inbound interface.
List of p2p tunnels using this path	List of tunnels using the path.
Number of p2p tunnels using this path	Number of tunnels using the path.
List of lsp-attributes referring this path	List of CR-LSP attribute templates using the path.
Number of lsp-attributes referring this path	Number of CR-LSP attribute templates using the path.

9.3.13 display lsp-attribute

Function

The **display lsp-attribute** command displays the configurations of the CR-LSP attribute template and the tunnels using it.

Format

display lsp-attribute [**name** *lsp-attribute-name*] [**tunnel-interface** | **verbose**]

Parameters

Parameter	Description	Value
name *lsp-attribute-name*	Specifies the name of the CR-LSP attribute template.	The value is an existing CR-LSP attribute template name.
tunnel-interface	Displays information about the interface of the tunnel that uses the explicit path.	-
verbose	Displays detailed information about the CR-LSP attribute template, including information about the tunnels using it.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the name of the CR-LSP attribute template is not specified, information about all CR-LSP attribute templates is displayed in the command output.

Example

Display information about the tunnel-interface using the attribute templates of lspattr1.

```
<HUAWEI> display lsp-attribute name lspattr1 tunnel-interface
lsp-attribute Name : lspattr1
explicit-path 2
commit
List of tunnels using this lsp-attribute:
    Tunnel1                        Tunnel2
Number of tunnels using this lsp-attribute: 2
```

Display detailed information about all CR-LSP attribute templates.

```
<HUAWEI> display lsp-attribute verbose

lsp-attribute Name : lsp-attribute-name11
bandwidth ct0 100
explicit-path path-name
affinity property 2 mask 2
priority 4
hop-limit 20
record-route label
fast-reroute bandwidth
bypass-attributes bandwidth 10 priority 4
commit
List of tunnels using this lsp-attribute:
    Tunnel1                      Tunnel2
Number of tunnels using this lsp-attribute: 2
```

Table 9-53 Description of the display lsp-attribute verbose command output

Item	Description
lsp-attribute Name	Name of a CR-LSP attribute template. To set the name of a CR-LSP attribute template, run the **lsp-attribute** command.
bandwidth ct0 100	Bandwidth of the LSP of each CT configured in the CR-LSP attribute template. To set the bandwidth of the LSP of each CT configured in the CR-LSP attribute template, run the **bandwidth** command.

Item	Description
explicit-path path-name	Explicit path in the CR-LSP attribute template. To set the explicit path in the CR-LSP attribute template, run the **explicit-path** command.
affinity property 2 mask 2	Affinity property and affinity mask in a CR-LSP attribute template. To set the affinity property and affinity mask in a CR-LSP attribute template, run the **affinity property** command.
priority 4	Setup and holding priorities in a CR-LSP attribute template. To set the setup and holding priorities in a CR-LSP attribute template, run the **priority** command.
hop-limit 20	Hop limit in a CR-LSP attribute template. To set the hop limit in a CR-LSP attribute template, run the **hop-limit** command.
record-route label	Route and label storing function that is enabled in the CR-LSP attribute template. To set the route and label storing function, run the **record-route** command.
fast-reroute bandwidth	FRR enabled and bandwidth protection configured in a CR-LSP attribute template. To set the FRR and bandwidth protection in a CR-LSP attribute template, run the **fast-reroute** command.
bypass-attributes bandwidth 10 priority 4	Bypass tunnel attributes in a CR-LSP attribute template. To set the bypass tunnel attributes in a CR-LSP attribute template, run the **bypass-attributes** command.
commit	Committing configurations of a CR-LSP attribute template. To set the committing configurations of a CR-LSP attribute template, run the **commit** command.

Item	Description
List of tunnels using this lsp-attribute	List of tunnels that use a CR-LSP attribute template.
Number of tunnels using this lsp-attribute	Number of tunnels that use a CR-LSP attribute template.

9.3.14 display mpls aps statistics global

Function

The **display mpls aps statistics global** command displays statistics about MPLS TE tunnel protection group.

Format

display mpls aps statistics global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After MPLS TE tunnel protection groups are configured, this command can be used to view statistics about these MPLS TE tunnel protection groups.

Example

Display statistics about MPLS TE tunnel protection groups.

```
<HUAWEI> display mpls aps statistics global
  Max APS Instance Num                   :  10240
  Created APS Instance Num               :  2
```

Table 9-54 Description of the **display mpls aps statistics global** command output

Item	Description
Max APS Instance Num	Maximum number of supported APS instances

Item	Description
Created APS Instance Num	Number of created MPLS TE tunnel protection groups

9.3.15 display mpls lsp attribute

Function

The **display mpls lsp attribute** command displays information about the local bypass LSP attributes.

Format

display mpls lsp attribute { **bypass-inuse** { **exists-not-used** | **inuse** | **not-exists** } | **bypass-tunnel** *tunnel-name* }

Parameters

Parameter	Description	Value
bypass-inuse	Displays the attribute of the bypass LSPs in use.	-
exists-not-used	Displays the attributes of the existing bypass LSPs that are not in use.	-
inuse	Displays the attribute of the bypass LSPs in use.	-
not-exists	Displays the attributes of the bypass LSPs that are not in use.	-
bypass-tunnel	Displays the attribute of the specified bypass tunnel.	-
tunnel-name	Specifies the name of the bypass tunnel.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls lsp attribute** command to view information about attributes of local bypass LSPs in the TE FRR scenarios.

Example

Display information about attributes of the existing bypass LSPs that are not in use.

```
<HUAWEI> display mpls lsp attribute bypass-inuse exists-not-used
-------------------------------------------------------------------------------
                 LSP Information: RSVP LSP
-------------------------------------------------------------------------------

 No                  :  1
 SessionID           :  300
 IngressLsrID        :  3.3.3.9
 LocalLspID          :  5
 Tunnel-Interface    :  Tunnel1
 Fec                 :  1.1.1.9/32
 TunnelTableIndex    :  0x1
 Nexthop             :  -------
 In-Label            :  3
 Out-Label           :  NULL
 In-Interface        :  Vlanif100
 Out-Interface       :  ----------
 LspIndex            :  2049
 Token               :  0x0
 LsrType             :  Egress
 Mpls-Mtu            :  ------
 TimeStamp           :  333sec
 Bfd-State           :  ---
 CBfd-Event          :  ---
 Bed-State           :  ---
 Bed-LastNotifyValue :  ---
 Bed-LastNotifyLspId :  ---
```

Table 9-55 Description of the display mpls lsp attribute command output

Item	Description
No	Sequence number of an LSP.
SessionID	Session ID of a CR-LSP.
IngressLsrID	Ingress LSR ID of a CR-LSP.
LocalLspID	Local LSP ID of a CR-LSP.
Tunnel-Interface	Tunnel interface.
Fec	Forwarding Equivalence Class, which is destination address of an LSP.
TunnelTableIndex	Index of a tunnel table.
Nexthop	IP address of the next hop of an LSP.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Name of an incoming interface.
Out-Interface	Name of an outgoing interface.

Item	Description
LspIndex	Index number of an LSP, which uniquely identifies an LSP that is established using a specified protocol.
Token	LSP token, which guides the packet forwarding.
LsrType	Role of an LSR on an LSP: ● Ingress ● Transit ● Egress
Mpls-Mtu	Maximum transmission unit (MTU) of an interface of an LSP.
TimeStamp	Time elapsed since an LSP was set up.
Bfd-State	BFD status.
CBfd-Event	BFD-reported error code event received on the ingress of an RSVP LSP.
Bed-State	Error code status received on the ingress of an RSVP LSP.
Bed-LastNotifyValue	Event of association relationship related to error codes informed on the egress of an RSVP LSP.
Bed-LastNotifyLspId	ID of a reverse LSP when an event of association relationship related to error codes is informed on the egress of an RSVP LSP.

9.3.16 display mpls rsvp-te

Function

The **display mpls rsvp-te** command displays the RSVP-TE configurations.

Format

display mpls rsvp-te

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When configuring a dynamic MPLS TE tunnel, you can run the **display mpls rsvp-te** command to view RSVP-TE configurations.

Example

Display information about RSVP-TE.

```
<HUAWEI> display mpls rsvp-te
 LSR ID: 1.1.1.9
 RSVP-TE Function Capability: Enable
 Resv Confirmation Request: DISABLE
 RSVP Hello Extension: ENABLE
 Hello interval: 3 sec         Max Hello misses: 3
 Path and Resv message refresh interval: 30 sec
 Path and Resv message refresh retries count: 3
 Blockade Multiplier: 4
 Graceful-Restart Capability: GR-Support GR-Self
 Restart Time:  90000 Millisecond
 Recovery Time: 0 Millisecond
 Bfd Enabled: DISABLE                  Bfd Min-Tx: 1000
 Bfd Min-Rx: 1000                      Bfd Detect-Multi: 3
 Soft Preemption Timeout: 30 sec
```

Table 9-56 Description of the display mpls rsvp-te command output

Item	Description
LSR ID	LSR ID in the format X.X.X.X.
RSVP-TE Function Capability	Whether RSVP-TE is enabled. To enable the RSVP-TE function, run the **mpls rsvp-te** command.
Resv Confirmation Request	Whether reservation confirmation is requested. To enable the reservation confirmation mechanism, run the **mpls rsvp-te resvconfirm** command.
RSVP Hello Extension	Whether the RSVP Hello extension is enabled. To enable the RSVP Hello extension, run the **mpls rsvp-te hello** command.
Hello interval	The interval at which Hello messages are sent, in seconds. To specify the interval, run the **mpls rsvp-te timer hello** command.
Max Hello misses	Maximum number of times for the consecutively lost Hello messages. To specify the maximum number, run the **mpls rsvp-te hello-lost** command.
Path and Resv message refresh interval	Time interval at which the Path and Resv messages are refreshed, in seconds. To specify the interval, run the **mpls rsvp-te timer refresh** command.

Item	Description
Path and Resv message refresh retries count	Number of retry times allowed for refreshing the Path and Resv messages. To specify the number, run the **mpls rsvp-te keep-multiplier** command.
Blockade Multiplier	Multiplier for keeping the blocked state.
Graceful-Restart Capability	RSVP GR capability of a device: ● GR-Support GR-Self: indicates that the RSVP GR on the local node is enabled and the RSVP GR of the neighbor is supported. ● GR-Self: indicates that the RSVP GR is enabled only on the local node. ● GR-Support: indicates that the RSVP GR of the neighbor is supported. ● DISABLE: indicates that the RSVP GR is disabled. To enable the RSVP GR capability, run the **mpls rsvp-te hello support-peer-gr** command or**mpls rsvp-te hello full-gr** command.
Restart Time	Start time of the GR process, in milliseconds. It is displayed only after the command **mpls rsvp-te hello basic-restart-time** is run.
Recovery Time	Time spent on recovering all LSPs, in milliseconds. It is displayed only after the command **mpls rsvp-te hello basic-restart-time** is run.
Bfd Enabled	Whether the BFD for RSVP is enabled globally in the MPLS view: ● ENABLE: indicates that BFD for RSVP is globally enabled in the MPLS view. ● DISABLE: indicates that BFD for RSVP is globally disabled in the MPLS view. To enable the BFD for RSVP function, run the **mpls rsvp-te bfd all-interfaces enable** command.
Bfd Min-Tx	Local interval at which BFD packets are sent, in milliseconds. To specify the interval, run the **mpls rsvp-te bfd all-interfaces** command.

Item	Description
Bfd Min-Rx	Local interval at which BFD packets are received, in milliseconds. To specify the interval, run the **mpls rsvp-te bfd all-interfaces** command.
Bfd Detect-Multi	Local BFD detection multiplier. To specify the multiplier, run the **mpls rsvp-te bfd all-interfaces** command.
Soft Preemption Timeout	Timeout period of soft preemption.

9.3.17 display mpls rsvp-te bfd session

Function

The **display mpls rsvp-te bfd session** command displays information about the BFD session for RSVP.

Format

display mpls rsvp-te bfd session { **all** | **interface** *interface-type interface-number* | **peer** *ip-address* } [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all the BFD sessions for RSVP.	-
interface *interface-type interface-number*	Displays information about the BFD session for RSVP on the specified interface.	-
peer *ip-address*	Displays information about the BFD session for RSVP of the specified peer.	The value is in dotted decimal notation.
verbose	Displays detailed information about a BFD session for RSVP.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about the BFD session for RSVP, run the **display mpls rsvp-te bfd session** command.

Example

Display information about a BFD session for RSVP.

```
<HUAWEI> display mpls rsvp-te bfd session all
Total Nbrs/Rsvp triggered sessions : 1/1
--------------------------------------------------------------------
Local    Remote   Local       Peer        Interface    Session
Discr    Discr    Addr        Addr        Name         State
--------------------------------------------------------------------
8192     8192     10.1.1.1    10.1.1.2    VLANIF100    UP
```

Display detailed information about a BFD session for RSVP.

```
<HUAWEI> display mpls rsvp-te bfd session all verbose
Total Nbrs/Rsvp triggered sessions : 1/1
--------------------------------------------------------------------
  Local Discriminator     :  8192
  Remote Discriminator    :  8192
  Local Address           :  10.1.1.1
  Peer Address            :  10.1.1.2
  Interface Name          :  VLANIF100
  ActTx                   :  1000
  ActRx                   :  1000
  ActMulti                :  3
  Session State           :  UP
```

Table 9-57 Description of the display mpls rsvp-te bfd session command output

Item	Description
Total Nbrs/Rsvp triggered sessions	Number of BFD neighbors or RSVP-triggered sessions in the system or interface view.
Local Discr/Local Discriminator	Local discriminator of a BFD session. The value 0 indicates an invalid discriminator. To specify a local discriminator of a BFD session, run the **discriminator** command.
Remote Discr/ Remote Discriminator	Remote discriminator of a BFD session. The value 0 indicates an invalid discriminator. To specify a remote discriminator of a BFD session, run the **discriminator** command.
Local Addr/Local Address	IP address of the local node in a BFD session.
Peer Addr/Peer Address	IP address of the peer in a BFD session.
Interface Name	Outgoing interface of a BFD session.

Item	Description
ActTx/ActRx/ActMulti	Parameters of a BFD session: To specify parameters of a BFD session, run the **mpls rsvp-te bfd all-interfaces** command. ● ActTx: indicates the actual interval at which BFD packets are sent, in milliseconds. ● ActRx: indicates the actual interval at which BFD packets are received, in milliseconds. ● ActMulti: indicates the actual local detection multiplier. The default value is 3.
Session State	Status of a BFD session: ● UP: indicates that the BFD session is Up. ● DOWN: indicates that the BFD session is Down. ● NONE: indicates that no BFD session is created. ● ADMIN DOWN: indicates that the administrator manually closes the BFD session. ● INITIAL: indicates the BFD session is in the Initial state.

9.3.18 display mpls rsvp-te established

Function

The **display mpls rsvp-te established** command displays information about RSVP resource reservation based on an interface, and about the RSVP-TE LSPs that pass through the interface.

Format

display mpls rsvp-te established [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
peer-ip-address	Specifies the IP address of an interface on the RSVP peer connected to the local device.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an interface is specified, information about the establishment of the RSVP-TE LSP on this interface is displayed.

Example

Display information about the establishment of the RSVP-TE LSPs of all interfaces.

```
<HUAWEI> display mpls rsvp-te established
Interface: Outgoing-Interface at the Egress
 Token Bucket Rate: 0.00            Peak Data Rate: 0.00
 Tunnel Addr: 10.1.1.9              Ingress LSR ID: 10.3.3.9
 Local LSP ID: 4                    Session Tunnel ID: 301
 Next Hop Addr:  -----
 Upstream Label: 3

 Token Bucket Rate: 0.00            Peak Data Rate: 0.00
 Tunnel Addr: 10.1.1.9              Ingress LSR ID: 10.3.3.9
 Local LSP ID: 4                    Session Tunnel ID: 300
 Next Hop Addr:  -----
 Upstream Label: 3

 Token Bucket Rate: 0.00            Peak Data Rate: 0.00
 Tunnel Addr: 10.3.3.9              Ingress LSR ID: 10.1.1.9
 Local LSP ID: 3                    Session Tunnel ID: 300
 Next Hop Addr: 172.16.1.2
 Upstream Label: NULL               Downstream Label: 1040

 Token Bucket Rate: 0.00            Peak Data Rate: 0.00
 Tunnel Addr: 10.3.3.9              Ingress LSR ID: 10.1.1.9
 Local LSP ID: 2                    Session Tunnel ID: 301
 Next Hop Addr: 172.16.1.2
 Upstream Label: NULL               Downstream Label: 1038
```

Table 9-58 Description of the display mpls rsvp-te established command output

Item	Description
Interface: Outgoing-Interface at the Egress	Information about RSVP resource reservation based on the outgoing interface on the egress node and about the RSVP LSPs that pass through the interface.
Token Bucket Rate	Token bucket rate, in byte/s.
Peak Data Rate	Peak data rate, in byte/s.
Tunnel Addr	Tunnel address in the format X.X.X.X.
Ingress LSR ID	LSR ID on the ingress in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Session Tunnel ID	Tunnel ID.
Next Hop Addr	Next-hop address in the format X.X.X.X.
Upstream Label	Value of an incoming label.
Downstream Label	Value of an outgoing label.

9.3.19 display mpls rsvp-te graceful-restart

Function

The **display mpls rsvp-te graceful-restart** command displays the status of RSVP GR.

Format

display mpls rsvp-te graceful-restart

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After completing the RSVP GR configuration, you can run the **display mpls rsvp-te graceful-restart** command to view the RSVP-TE GR status.

Example

Display the status of RSVP-TE GR.

```
<HUAWEI> display mpls rsvp-te graceful-restart
Display Mpls Rsvp te graceful restart information
 LSR ID: 1.1.1.9
 Graceful-Restart Capability:   GR-Self GR-Support
 Restart Time:  90000 Milli Second
 Recovery Time: 0 Milli Second
 GR Status:  Gracefully Restart Not going on
 Number of Restarting neighbors: 0
 Number of LSPs recovered: 0
 Received Gr Path message count: 0
 Send Gr Path message count: 0
 Received RecoveryPath message count: 0
 Send RecoveryPath message count: 0
```

Table 9-59 Description of the display mpls rsvp-te graceful-restart command output

Item	Description
LSR ID	LSR ID.
Graceful-Restart Capability	RSVP GR capability of a device.
Restart Time	Restart time for a device, in milliseconds. To set the restart time, run the **mpls rsvp-te hello basic-restart-time** command.
Recovery Time	Time spent on recovering all LSPs, in milliseconds. To set the recovery time, run the **mpls rsvp-te hello basic-restart-time** command.
GR Status	RSVP GR status of the local device: ● Gracefully Restart Not going on: indicates that the protocol is not entering the GR process. ● Gracefully Restart on going restarting: indicates that the protocol has entered the GR process. ● Gracefully Restart on going recovery: indicates that the configurations are being restored.
Number of Restarting neighbors	Number of supporting nodes.
Number of LSPs recovered	Number of recovered LSPs.
Received Gr Path message count	Number of Path messages received by restarting nodes.

Item	Description
Send Gr Path message count	Number of Path messages sent by supporting nodes.
Received RecoveryPath message count	Number of Recovery Path messages received by restarting nodes.
Send RecoveryPath message count	Number of Recovery Path messages sent by supporting nodes.

9.3.20 display mpls rsvp-te graceful-restart peer

Function

The **display mpls rsvp-te graceful-restart peer** command displays the status of RSVP GR on a neighbor.

Format

display mpls rsvp-te graceful-restart peer [{ **interface** *interface-type interface-number* | **node-id** } [*ip-address*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the RSVP GR status of a neighbor on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
node-id	Displays the RSVP GR status of a manually-configured neighbor.	-
ip-address	Specifies the IP addresses of a neighbor.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the RSVP-TE GR status of a specified RSVP neighbor, run the **display mpls rsvp-te graceful-restart peer** command.

Example

Display the RSVP-TE GR status of the neighbor.

```
<HUAWEI> display mpls rsvp-te graceful-restart peer
 Neighbor on Interface Vlanif100
 Neighbor Addr: 172.16.1.2             Last Attribute: Added Usually
 SrcInstance: 0x7C832B3D               NbrSrcInstance: 0x6A48E0F5
 Neighbor Capability:
                  Can Do Self GR
                  Can Support GR
 GR Status:          Normal
 Restart Time:  90000 Millisecond
 Recovery Time: 0 Millisecond
 Stored GR message number: 0
 PSB Count: 0                          RSB Count: 1
 Total to be Recover PSB Count: 0      Recovered PSB Count: 0
 Total to be Recover RSB Count: 0      Recovered RSB Count: 0
 P2MP PSB Count: 0                     P2MP RSB Count: 0
 Total to be Recover P2MP PSB Count: 0      Recovered P2MP PSB Count: 0
 Total to be Recover P2MP RSB Count: 0      Recovered P2MP RSB Count: 0
```

Table 9-60 Description of the display mpls rsvp-te graceful-restart peer command output

Item	Description
Neighbor Addr	IP address of a neighbor.
Last Attribute	Neighbor attribute: ● Added Usually: indicates the neighbor is discovered based on an interface. ● Added by Node-Id: indicates the neighbor is discovered based on the configured node ID. ● To be deleted: indicates the neighbor that is to be deleted because of the Hello timeout. ● Add by Frr: indicates an FRR neighbor.
SrcInstance	Source instance.
NbrSrcInstance	Source instance of a neighbor.

Item	Description
Neighbor Capability	GR capability of a neighbor: - Can Do Self GR: indicates that the neighbor can perform GR. - Can Support GR: indicates that the neighbor has the capability of supporting GR. - Can Transmit Recovery Path Messages: indicates that the neighbor can send Recovery Path messages. - No Gr capabilities: indicates that the neighbor does not have the capability of supporting GR.
GR Status	GR status of a neighbor: - Normal: indicates that the neighbor does not perform GR. - Supporting: indicates that the neighbor is supporting the local node of performing GR. - Restarting: indicates that the neighbor is supporting the local node of the restart.
Restart Time	Restart time of a neighbor, in milliseconds.
Recovery Time	Recovery time of a neighbor, in milliseconds.
Stored GR message number	Number of GR messages stored on the supporting node.
PSB Count	Number of PSBs.
RSB Count	Number of RSBs.
Total to be Recover PSB Count	Total number of the PSBs to be recovered.
Recovered PSB Count	Number of the recovered PSBs.
Total to be Recover RSB Count	Total number of the RSBs to be recovered.
Recovered RSB Count	Number of recovered RSBs.
P2MP PSB Count	Number of P2MP PSBs
P2MP RSB Count	Number of P2MP RSBs
Total to be Recover P2MP PSB Count	Number of P2MP PSBs to be restored after the GR process is complete
Recovered P2MP PSB Count	Number of P2MP PSBs that have been restored after the GR process is complete
Total to be Recover P2MP RSB Count	Number of P2MP RSBs to be restored after the GR process is complete

Item	Description
Recovered P2MP RSB Count	Number of P2MP RSBs that have been restored after the GR process is complete

9.3.21 display mpls rsvp-te interface

Function

The **display mpls rsvp-te interface** command displays the RSVP-TE configurations on an interface.

Format

display mpls rsvp-te interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the type and number of an interface is not specified, the **display mpls rsvp-te interface** command displays the RSVP-TE information of all RSVP TE-enabled interfaces.

Example

Display information about RSVP-TE of a specified interface.

```
<HUAWEI> display mpls rsvp-te interface vlanif 100
Interface: Vlanif100
 Interface Address: 11.11.11.11
 Interface state: UP                  Interface Index: 0x4
 Total-BW: 0                        Used-BW: 0
 Hello configured: NO                 Num of Neighbors: 0
 SRefresh feature: DISABLE             SRefresh Interval: 30 sec
 Mpls Mtu: 1500                      Retransmit Interval: 5000 msec
```

```
Increment Value: 1
Authentication: DISABLE
Bfd Enabled: DISABLE              Bfd Min-Tx: 400
Bfd Min-Rx: 300                 Bfd Detect-Multi: 4
```

Table 9-61 Description of the display mpls rsvp-te interface command output

Item	Description
Interface	Name of a tunnel interface.
Interface Address	IP address of an interface.
Interface state	Interface status: - UP - DOWN
Interface Index	Index of an interface.
Total-BW	Total available bandwidth of an interface, in kbit/s.
Used-BW	Total bandwidth of an interface in use, in kbit/s.
Hello configured	Whether the Hello feature is configured on an interface: - YES: indicates that the Hello feature is configured. - NO: indicates that the Hello feature is not configured.
Num of Neighbors	Number of neighbor devices of the local node.
SRefresh feature	Whether the Srefresh feature is enabled. To enable the Srefresh feature, run the **mpls rsvp-te srefresh** command in the interface view.
SRefresh Interval	Value of the Srefresh timer, in seconds. To specify the value of the Srefresh timer, run the **mpls rsvp-te timer refresh** command.
Mpls Mtu	MTU value used in MPLS forwarding.
Retransmit Interval	Value of the Retransmit timer, in milliseconds. To specify the value of the Retransmit timer, run the **mpls rsvp-te timer retransmission** command.
Increment Value	Retransmission increment. To specify the retransmission increment, run the **mpls rsvp-te timer retransmission** command.

Item	Description
Authentication	Whether the authentication function is enabled: ● ENABLE: indicates that the authentication function is enabled. ● DISABLE: indicates that the authentication function is disabled. To enable the authentication function, run the **mpls rsvp-te authentication** command.
Bfd Enabled	Whether BFD for RSVP is enabled on the interface: ● ENABLE: indicates that BFD for RSVP is enabled on the interface. ● DISABLE: indicates that BFD for RSVP is not enabled on the interface. To enable BFD for RSVP, run the **mpls rsvp-te bfd enable** command.
Bfd Min-Tx	Local interval at which BFD packets are sent, in milliseconds. To specify the local minimum interval at which BFD packets are sent, run the **mpls rsvp-te bfd** command.
Bfd Min-Rx	Local interval at which BFD packets are received, in milliseconds. To specify the local minimum interval at which BFD packets are received, run the **mpls rsvp-te bfd** command.
Bfd Detect-Multi	Local BFD detection multiplier. To specify the local BFD detection multiplier, run the **mpls rsvp-te bfd** command.

9.3.22 display mpls rsvp-te peer

Function

The **display mpls rsvp-te peer** command displays information about RSVP-TE neighbor devices on an RSVP-TE-enabled interface.

Format

display mpls rsvp-te peer [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about RSVP-TE of a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface is specified, information about RSVP-TE neighbors of all interfaces is displayed.

Example

Display information about RSVP-TE neighbors of all interfaces.

```
<HUAWEI> display mpls rsvp-te peer
 Remote Node id Neighbor
 Neighbor Addr:  -----
 SrcInstance: 0x3A76A0FA              NbrSrcInstance: 0x0
 PSB Count: 2                    RSB Count: 2
 Hello Type Sent: REQ
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL

Interface: Vlanif10
 Neighbor Addr: 172.16.1.2
 SrcInstance: 0x3A76A0FA              NbrSrcInstance: 0x22A6B5C2
 PSB Count: 2                    RSB Count: 2
 Hello Type Sent: REQ              Neighbor Hello Extension: ENABLE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL
```

Table 9-62 Description of the display mpls rsvp-te peer command output

Item	Description
Neighbor Addr	Neighboring device address.
SrcInstance	Source instance.
NbrSrcInstance	Source instance of a neighbor device.
PSB Count	Number of Path State Blocks (PSBs).
RSB Count	Number of Reservation State Blocks (RSBs).

Item	Description
Hello Type Sent	Type of Hello message sent to the neighbor device: - REQ - ACK - NONE
Neighbor Hello Extension	Whether the Hello extension feature of the neighboring device is enabled.
SRefresh Enable	Whether the Srefresh mechanism is enabled: - YES - NO
Last valid seq # rcvd	Serial number of the valid RSVP message last received.

9.3.23 display mpls rsvp-te psb-content

Function

The **display mpls rsvp-te psb-content** command displays information about an RSVP TE Path State Block (PSB).

Format

display mpls rsvp-te psb-content [*ingress-lsr-id tunnel-id lsp-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all RSVP-TE PSBs is displayed.

Example

Display information about the PSB.

```
<HUAWEI> display mpls rsvp-te psb-content 10.1.1.9 100 7
===============================================================
                 The PSB Content
===============================================================
 Tunnel Addr: 10.4.4.9                  Exist time: 17h 12m 57s
 Tunnel ExtID: 10.1.1.9                 Session ID: 100
 Ingress LSR ID: 10.1.1.9               Local LSP ID: 7
 Previous Hop : 172.16.1.1/0x2d    Next Hop : 172.20.1.2
 Incoming / Outgoing Interface: Vlanif100  / Vlanif20
 InLabel : 1028                         OutLabel : 1028
 Send Message ID : 30                   Recv Message ID : 0
 Refresh Timer : 510224684              Cleanup Timer : 408260940
 Session Attribute-
  SetupPrio: 7         HoldPrio: 7
  SessionAttrib: Local Protect desired. Node Protect desired. Label Recording de
sired. SE Style desired.
 LSP Type: -
 FRR Flag : Will be MP                  Local RRO Flag : 0x1
 ERO Information-
    L-Type         ERO-IPAddr       ERO-PrefixLen
  ERHOP_STRICT    172.20.1.2           32
  ERHOP_STRICT    172.30.1.1           32
  ERHOP_STRICT    172.30.1.2           32
 Bypass ERO Information-
    L-Type         ERO-IPAddr       ERO-PrefixLen
  ERHOP_STRICT    10.3.3.9             32
  ERHOP_STRICT    172.30.1.1           32
  ERHOP_STRICT    172.30.1.2           32
 RRO Information-
  RRO-CType: IPV4   IPAddress: 172.16.1.1        PrefixLen: 32  Flag: 0x9
  RRO-CType: IPV4   IPAddress: 10.1.1.9          PrefixLen: 32  Flag: 0x20
 SenderTspec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 1500
 Path Message arrive on Vlanif100 from PHOP 172.16.1.1
 Path Message sent to NHOP 172.20.1.2  on Vlanif20
 Resource Reservation OK

 LSP Statistics Information:
  SendPacketCounter: 3623        RecvPacketCounter: 3648
  SendPathCounter: 1794          RecvPathCounter: 1791
  SendResvCounter: 1829          RecvResvCounter: 1857
```

Table 9-63 Description of the display mpls rsvp-te psb-content command output

Item	Description
Tunnel Addr	Tunnel address in the format X.X.X.X.
Exist time	Duration that an LSP has been established.
Tunnel ExtID	Tunnel extended ID.
Session ID	RSVP session ID

Item	Description
Ingress LSR ID	Ingress address in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Previous Hop	Previous-hop address in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Incoming / Outgoing Interface	Incoming or outgoing interface through which a tunnel passes on the local device.
InLabel	Value of an incoming label.
OutLabel	Value of an outgoing label.
Send Message ID	ID of the sent refresh reduction message.
Recv Message ID	ID of the received refresh reduction message.
Refresh Timer	Refresh timer.
Cleanup Timer	Timeout timer.
Session Attribute	Attribute of an RSVP session.
SetupPrio	Setup priority of an RSVP session.
HoldPrio	Holding priority of an RSVP session.
SessionAttrib	RSVP session attributes, such as resource reservation style.
LSP Type	Type of LSP.
FRR Flag	State of MPLS TE FRR
Local RRO Flag	Flag bit of the local RRO.
ERO Information	Information about the Explicit Route Object (ERO).
L-Type	Types of the explicit route.
ERO-IPAddr	Explicit route address.
ERO-PrefixLen	Explicit route prefix length.
RRO Information	Information about the Record Route Object (RRO).
RRO-CType	RRO of the C type, IPv4 or label.
IPAddress	IP address of a record route.
PrefixLen	Prefix length of a recorded route.
Flag	Flag bit of a recorded route.

Item	Description
SenderTspec Information	Information about the traffic specification of the sender.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size.
Path Message arrive on	Incoming interfaces and previous-hop addresses of messages.
Path Message sent to NHOP	Next-hop addresses and outgoing interfaces of messages.
Resource Reservation OK	Ready state of resource reservation that is displayed only when the resource reserved flag is set.
LSP Statistics Information	Statistics of LSPs.
SendPacketCounter	Number of sent packets.
RecvPacketCounter	Number of received packets.
SendPathCounter	Number of sent Path messages.
RecvPathCounter	Number of received Path messages.
SendResvCounter	Number of sent Resv messages.
RecvResvCounter	Number of received Resv messages.

9.3.24 display mpls rsvp-te request

Function

The **display mpls rsvp-te request** command displays information about the RSVP-TE request messages on interfaces.

Format

display mpls rsvp-te request [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about RSVP TE request messages on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of a neighbor device.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays information about the RSVP-TE request information of all RSVP-TE-enabled interfaces.

Example

Display information about RSVP-TE of a specified interface.

```
<HUAWEI> display mpls rsvp-te request interface vlanif 10 172.16.1.1
Interface: Vlanif10
 Tunnel Addr: 10.2.2.9              Ingress LSR ID: 10.1.1.9
 Local LSP ID: 0                   Session Tunnel ID: 100
 NextHopAddr:  -----
 SessionAttrib: Label Recording desired. SE Style desired.
 Token bucket rate: 0.00             Token bucket size: 1000.00
 Out Interface:  -----
```

Table 9-64 Description of the display mpls rsvp-te request command output

Item	Description
Interface	Name of the interface that is enabled with RSVP-TE.
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.

Item	Description
Local LSP ID	Local identifier of an LSP.
Session Tunnel ID	Tunnel ID
NextHopAddr	Next-hop address in the format X.X.X.X.
SessionAttrib	Session attribute: ● Local protection desired ● Label record desired ● Resource reservation style
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.
Out Interface	Outgoing interface of an LSP.

9.3.25 display mpls rsvp-te reservation

Function

The **display mpls rsvp-te reservation** command displays RSVP-TE resource reservation information of an interface enabled with RSVP-TE.

Format

display mpls rsvp-te reservation [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the RSVP-TE reservation information of the interface that is not in stale state. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of an RSVP-TE neighbor device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays the resource reservation information of all RSVP-TE-enabled interfaces.

Example

Display information about the RSVP-TE resource reservation information of all interfaces.

```
<HUAWEI> display mpls rsvp-te reservation
Interface: Outgoing-Interface at the Egress
 Tunnel Addr: 1.1.1.9              Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4                   Session Tunnel ID: 301
 Upstream Label: 3
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 1.1.1.9              Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4                   Session Tunnel ID: 300
 Upstream Label: 3
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 3.3.3.9              Ingress LSR ID: 1.1.1.9
 Local LSP ID: 3                   Session Tunnel ID: 300
 Upstream Label: NULL
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 3.3.3.9              Ingress LSR ID: 1.1.1.9
 Local LSP ID: 2                   Session Tunnel ID: 301
 Upstream Label: NULL
 Token bucket rate: 0.00           Token bucket size: 1000.00
```

Table 9-65 Description of the display mpls rsvp-te reservation command output

Item	Description
Interface	Name of the interface that is enabled with RSVP-TE
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local identifier of an LSP.
Session Tunnel ID	Tunnel ID.
Upstream Label	Incoming label.
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.

9.3.26 display mpls rsvp-te rsb-content

Function

The **display mpls rsvp-te rsb-content** command displays information about the RSVP TE Reserve State Block (RSB).

Format

display mpls rsvp-te rsb-content [*ingress-lsr-id tunnel-id lsp-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all RSVP TE RSBs is displayed.

Example

Display information about the RSVP TE Reserve State Block.

```
<HUAWEI> display mpls rsvp-te rsb-content 10.1.1.9 300 3
===============================================================
                   The RSB Content
===============================================================
 Tunnel Addr: 10.3.3.9              Session Tunnel ID: 300
 Tunnel ExtID: 10.1.1.9
 Next Hop: 172.16.1.2               Reservation Style: SE Style
 Reservation Incoming Interface: Vlanif100
 Reservation Interface: Vlanif100
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 10.1.1.9       Local LSP ID: 3       OutLabel: 1040
   Cleanup Timer : 504613260
   RRO Information-
```

```
    RRO-CType: IPV4   RRO-IPAddress: 172.16.1.2       RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 1040
    RRO-CType: IPV4   RRO-IPAddress: 10.2.2.9        RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 1040
    RRO-CType: IPV4   RRO-IPAddress: 172.20.1.1       RRO-IPPrefixLen: 32
    RRO-CType: IPV4   RRO-IPAddress: 172.20.1.2       RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 3
    RRO-CType: IPV4   RRO-IPAddress: 10.3.3.9        RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 3
  Message ID : 0
FlowSpec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 1500
  Bandwidth guarantees: 0.00
  Delay guarantees: 0
  Qos Service is Controlled
Resv Message arrive on Vlanif100 from NHOP 172.16.1.2
```

Table 9-66 Description of the display mpls rsvp-te rsb-content command output

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Session Tunnel ID	Tunnel ID.
Tunnel ExtID	Tunnel extension ID (ingress LSR ID) in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Reservation Style	Reservation style: ● SE ● FF
Reservation Incoming Interface	Incoming interface for the reservation message.
Reservation Interface	Name of the interface on which bandwidth is reserved.
Message ID	ID of the Refresh Reduction message.
Filter Spec Information	Filtering conditions.
The filter number	Total number of filters.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local identifier of an LSP.
OutLabel	Outgoing label.
Cleanup Timer	Timeout timer.
RRO Information	Information about the RRO.

Item	Description
RRO-CType	Class type in the RRO: - IPv4 - Label
RRO-IPAddress	IP address in the RRO, in the format X.X.X.X.
RRO-IPPrefixLen	Length of the route prefix in the RRO.
RRO-Label	Label information in the RRO
FlowSpec Information	Traffic information including flow specifications.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size.
Bandwidth guarantees	Bandwidth guarantee.
Delay guarantees	Delay guarantee.
Qos Service	QoS guarantee/control.
Resv Message	Reservation message received on an interface.

9.3.27 display mpls rsvp-te sender

Function

The **display mpls rsvp-te sender** command displays information about an RSVP-TE enabled interface as an RSVP-TE sender.

Format

display mpls rsvp-te sender [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface receiving Path messages. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of the outgoing interface on the previous hop sending Path messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays the information about all RSVP-TE enabled interfaces as RSVP-TE senders.

Example

Display information about all RSVP-TE enabled interfaces as RSVP-TE senders.

```
<HUAWEI> display mpls rsvp-te sender
Interface: Incoming-Interface at the Ingress
 Tunnel Addr: 10.3.3.9              Ingress LSR ID: 10.1.1.9
 Local LSP ID: 3                  Session Tunnel ID: 300
 Session Name: Tunnel1
 Previous Hop Address:  -----
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 10.1.1.9              Ingress LSR ID: 10.3.3.9
 Local LSP ID: 4                  Session Tunnel ID: 300
 Session Name: Tunnel1
 Previous Hop Address: 172.16.1.2
 Token bucket rate: 0.00           Token bucket size: 1000.00
```

Table 9-67 Description of the display mpls rsvp-te sender command output

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local LSP ID.

Item	Description
Session Tunnel ID	Tunnel ID.
Session Name	Name of a session.
Previous Hop Address	Previous-hop address in the format X.X.X.X.
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.
Interface: Incoming-Interface at the Ingress	Information about the RSB functioning as the ingress on the local node.

9.3.28 display mpls rsvp-te session

Function

The **display mpls rsvp-te session** command displays all information about any specified RSVP session.

Format

display mpls rsvp-te session *ingress-lsr-id tunnel-id egress-lsr-id*

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
egress-lsr-id	Specifies the egress LSR ID.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about the RSVP session includes information about the Path State Block (PSB), Reservation State Block (RSB), and ReFresh State Block (RFSB).

Example

Display all information about the RSVP session between nodes 10.1.1.9 and 10.3.3.9 (Tunnel ID is 300).

```
<HUAWEI> display mpls rsvp-te session 10.1.1.9 300 10.3.3.9
===============================================================
  Display PSB, RSB and RFSB information in session table
===============================================================
===============================================================
                     The PSB Content
===============================================================
 Tunnel Addr: 10.3.3.9                    Exist time: 1h 1m 4s
 Tunnel ExtID: 10.1.1.9                   Session ID: 300
 Ingress LSR ID: 10.1.1.9                 Local LSP ID: 4
 Previous Hop :  ----- /0x0      Next Hop : 172.16.1.2
 Incoming / Outgoing Interface: -----  / Vlanif100
 InLabel : NULL                           OutLabel : 1042
 Send Message ID : 29                     Recv Message ID : 0
 Refresh Timer : 504613692                Cleanup Timer : ---
 Session Attribute-
  SetupPrio: 0         HoldPrio: 0
  SessionAttrib: Local Protect desired. Node Protect desired. Label Recording de
sired. SE Style desired.
 LSP Type: -
 FRR Flag : No protection                 Local RRO Flag : 0x0
 ERO Information-
     L-Type         ERO-IPAddr       ERO-PrefixLen
   ERHOP_STRICT    172.16.1.2           32
   ERHOP_STRICT    172.20.1.1           32
   ERHOP_STRICT    172.20.1.2           32
 RRO Information-
    -----
 SenderTspec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 4294967295
 Path Message arrive on ----- from PHOP  -----
 Path Message sent to NHOP 172.16.1.2  on Vlanif100
 Resource Reservation OK

 LSP Statistics Information:
   SendPacketCounter: 106         RecvPacketCounter: 115
   SendPathCounter: 106           RecvPathCounter: 0
   SendResvCounter: 0             RecvResvCounter: 115

===============================================================
                     The RSB Content
===============================================================
 Tunnel Addr: 10.3.3.9               Session Tunnel ID: 300
 Tunnel ExtID: 10.1.1.9
 Next Hop: 172.16.1.2                Reservation Style: SE Style
 Reservation Incoming Interface: Vlanif100
 Reservation Interface: Vlanif100
 Message ID : 0
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 10.1.1.9        Local LSP ID: 4       OutLabel: 1042
   Cleanup Timer : 504613800
   RRO Information-
     RRO-CType: IPV4   RRO-IPAddress: 172.16.1.2       RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1042
     RRO-CType: IPV4   RRO-IPAddress: 10.2.2.9         RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1042
     RRO-CType: IPV4   RRO-IPAddress: 172.20.1.1       RRO-IPPrefixLen: 32
     RRO-CType: IPV4   RRO-IPAddress: 172.20.1.2       RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
```

```
    RRO-CType: IPV4   RRO-IPAddress: 10.3.3.9         RRO-IPPrefixLen: 32
    RRO-CType: Label    RRO-Label: 3
FlowSpec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 1500
  Bandwidth guarantees: 0.00
  Delay guarantees: 0
  Qos Service is Controlled
Resv Message arrive on Vlanif100 from NHOP 172.16.1.2
```

Table 9-68 Description of the display mpls rsvp-te session command output

Item	Description
The PSB Content	Contents of the PSB.
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Exist time	Time elapsed since the PSB is created.
Tunnel ExtID	Tunnel extension ID (ingress LSR ID) in the format X.X.X.X.
Session ID/ Session Tunnel ID	Tunnel ID.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Previous Hop	Previous-hop address in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Incoming / Outgoing Interface	Name of the incoming or outgoing interface.
InLabel	Value of an incoming label.
OutLabel	Value of an outgoing label.
Send Message ID	ID of the sent refresh reduction message.
Recv Message ID	ID of the received refresh reduction message.
Refresh Timer	ID of the Refresh timer.
Cleanup Timer	ID of the Cleanup timer.
Session Attribute	Attribute of a session.
SetupPrio	Setup priority of a session.

Item	Description
HoldPrio	Holding priority of a session.
SessionAttrib	Session attributes, including required local protection, bandwidth protection, node protection, label record, and reservation style.
LSP Type	Type of an LSP.
FRR Flag	Flag bit of FRR: - No protection: indicates no FRR protection. - PLR in use: provides protection on the Point of Local Repair. - MP in use: provides protection on the Merge Point. - Under protecting: provides FRR protection.
Local RRO Flag	Flag bit of the local RRO.
ERO Information	Information about the Explicit Route Object (ERO).
L-Type	Types of the explicit route: - ERHOP_STRICT - ERHOP_LOOSE
ERO-IPAddr	Explicit route address.
ERO-PrefixLen	Explicit route prefix length.
RRO Information	Information about the Record Route Object (RRO).
RRO-CType	Class C routes, including IPv4 or IPv6 addresses and labels recorded.
RRO-IPAddress	IPv4 or IPv6 address of the recorded route.
RRO-IPPrefixLen	Prefix length of a recorded route.
RRO-Label	Label information in the RRO.
SenderTspec Information	Information about the traffic specification of the sender.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.

Item	Description
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size, in bytes.
Path Message arrive on	Pre-hop addresses and incoming interfaces of messages.
Path Message sent to	Next-hop addresses and outgoing interfaces of messages.
Resource Reservation OK	Displayed only when the resource reservation flag is set.
LSP Statistics Information	Statistics of LSPs.
SendPacketCounter	Number of sent packets.
RecvPacketCounter	Number of received packets.
SendPathCounter	Number of sent Path messages.
RecvPathCounter	Number of received Path messages.
SendResvCounter	Number of sent Resv messages.
RecvResvCounter	Number of received Resv messages.
The RSB Content	Number of Reservation State Blocks (RSBs).
Reservation Style	Reservation style: ● SE: Shared Explicit Style ● FF: Fixed-Filter Style
Reservation Incoming Interface	Incoming interface for the reservation message.
Reservation Interface	Name of the interface on which bandwidth is reserved.
Message ID	Message ID locally allocated, used in the Srefresh feature and reliability.
Filter Spec Information	Filtering conditions.
The filter number	Total number of filters.
FlowSpec Information	Information about flow specifications.
Bandwidth guarantees	Bandwidth guarantee.
Delay guarantees	Delay guarantee.
Qos Service is Controlled	QoS guarantee.
Resv Message arrive on	Incoming interfaces and previous-hop addresses of messages.

9.3.29 display mpls rsvp-te statistics

Function

The **display mpls rsvp-te statistics** command displays statistics on RSVP-TE.

Format

display mpls rsvp-te statistics { **global** | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Displays the global statistics on RSVP-TE.	-
interface	Displays statistics on RSVP-TE on all interface that enabled RSVP-TE function.	-
interface-type interface-number	Displays statistics on RSVP-TE on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the statistics on RSVP-TE, run the **display mpls rsvp-te statistics** command.

Example

Display the global RSVP-TE statistics.

```
<HUAWEI> display mpls rsvp-te statistics global
 LSR ID: 10.1.1.1                    LSP Count: 0
 PSB Count: 0                        RSB Count: 0
 RFSB Count: 0

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0         RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 0                RecPacketCounter: 0
 SendCreatePathCounter: 0            RecCreatePathCounter: 0
 SendRefreshPathCounter: 0           RecRefreshPathCounter: 0
```

```
SendCreateResvCounter: 0             RecCreateResvCounter: 0
SendRefreshResvCounter: 0            RecRefreshResvCounter: 0
SendResvConfCounter: 0               RecResvConfCounter: 0
SendHelloCounter: 0                  RecHelloCounter: 0
SendAckCounter: 0                    RecAckCounter: 0
SendPathErrCounter: 0                RecPathErrCounter: 0
SendResvErrCounter: 0                RecResvErrCounter: 0
SendPathTearCounter: 0               RecPathTearCounter: 0
SendResvTearCounter: 0               RecResvTearCounter: 0
SendSrefreshCounter: 0               RecSrefreshCounter: 0
SendAckMsgCounter: 0                 RecAckMsgCounter: 0
SendChallengeMsgCounter: 0           RecChallengeMsgCounter: 0
SendResponseMsgCounter: 0            RecResponseMsgCounter: 0
SendErrMsgCounter: 0                 RecErrMsgCounter: 0
SendRecoveryPathMsgCounter: 0        RecRecoveryPathMsgCounter: 0
SendGRPathMsgCounter: 0              RecGRPathMsgCounter: 0
ResourceReqFaultCounter: 0           RecGRPathMsgFromLSPMCounter: 0
Bfd neighbor count: 0                Bfd session count: 0
```

Table 9-69 Description of the display mpls rsvp-te statistics command output

Item	Description
LSR ID	Local LSR ID.
PSB Count	Number of PSBs.
RSB Count	Number of RSBs.
RFSB Count	Number of RFSBs.
LSP Count	Number of LSPs established through RSVP TE.
Total Statistics Information	Total statistics information.
PSB CleanupTimeOutCounter	Number of times that the PSB is reset after the timer expires.
RSB CleanupTimeOutCounter	Number of times that the RSB is reset after the timer expires.
SendPacketCounter	Number of sent packets.
RecPacketCounter	Number of received packets.
SendCreatePathCounter	Number of sent CreatePath messages.
RecCreatePathCounter	Number of received CreatePath messages.
SendRefreshPathCounter	Number of sent RefreshPath messages.
RecRefreshPathCounter	Number of received RefreshPath messages.
SendCreateResvCounter	Number of sent CreateResv messages.
RecCreateResvCounter	Number of received CreateResv messages.
SendRefreshResvCounter	Number of sent RefreshResv messages.
RecRefreshResvCounter	Number of received RefreshResv messages.
SendResvConfCounter	Number of sent ResvConf messages.

Item	Description
RecResvConfCounter	Number of received ResvConf messages.
SendHelloCounter	Number of sent Hello messages.
RecHelloCounter	Number of received Hello messages.
SendAckCounter	Number of sent Ack messages.
RecAckCounter	Number of received Ack messages.
SendPathErrCounter	Number of sent PathErr messages.
RecPathErrCounter	Number of received PathErr messages.
SendResvErrCounter	Number of sent ResvErr messages.
RecResvErrCounter	Number of received ResvErr messages.
SendPathTearCounter	Number of sent PathTear messages.
RecPathTearCounter	Number of received PathTear messages.
SendResvTearCounter	Number of sent ResvTear messages.
RecResvTearCounter	Number of received ResvTear messages.
SendSrefreshCounter	Number of sent Srefresh messages.
RecSrefreshCounter	Number of received Srefresh messages.
SendAckMsgCounter	Number of sent Msg_ID_ACK messages.
RecAckMsgCounter	Number of received Msg_ID_ACK messages.
SendChallengeMsgCounter	Number of sent Challenge messages.
RecChallengeMsgCounter	Number of received Challenge messages.
SendResponseMsgCounter	Number of sent Response messages.
RecResponseMsgCounter	Number of received Response messages.
SendErrMsgCounter	Number of sent Msg_ID_NACK messages.
RecErrMsgCounter	Number of received Msg_ID_NACK messages.
SendRecoveryPathMsgCounter	Number of sent Recovery Path messages.
RecRecoveryPathMsgCounter	Number of received Recovery Path messages.
SendGRPathMsgCounter	Number of sent GR Path messages.
RecGRPathMsgCounter	Number of received GR Path messages.
ResourceReqFaultCounter	Number of failed attempts to request resources.

Item	Description
RecGRPathMsgFromLSPM-Counter	Number of GR Path messages received from the LSPM module.
Bfd neighbor count	Number of upstream or downstream BFD peers through which at least one LSP in the Up state passes.
Bfd session count	Number of BFD sessions.

9.3.30 display mpls rsvp-te statistics fast-reroute

Function

The **display mpls rsvp-te statistics fast-reroute** command displays the CR-LSP statistics on the local node serving as a Point of Local Repair (PLR) or Merge Point (MP).

Format

display mpls rsvp-te statistics fast-reroute

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be used to check the following information:

- Number of CR-LSPs in the PLR Available state
- Number of CR-LSPs in the PLR Inuse state
- Number of CR-LSPs in the MP Available state
- Number of CR-LSPs in the MP Inuse state

Example

Display CR-LSP statistics information on the local node serving as PLR or MP.

```
<HUAWEI> display mpls rsvp-te statistics fast-reroute
FRR statistics information:
 PLR AvailLsps: 0                 PLR InuseLsps: 0
 MP AvailLsps: 0                  MP InuseLsps: 0
```

Table 9-70 Description of the display mpls rsvp-te statistics fast-reroute command output

Item	Description
PLR AvailLsps	Number of CR-LSPs whose local node is the PLR in the PLR Available state (the CR-LSPs are bound to the bypass tunnel but FRR does not occur on the PLR).
PLR InuseLsps	Number of CR-LSPs whose local node is the PLR in the PLR Inuse state.
MP AvailLsps	Number of CR-LSPs whose local node is the MP in the MP Available state (the CR-LSPs are bound to the bypass tunnel but FRR does not occur on the MP).
MP InuseLsps	Number of CR-LSPs whose local node is the MP in the MP Inuse state.

9.3.31 display mpls static-cr-lsp

Function

The **display mpls static-cr-lsp** command displays information about a static CR-LSP.

Format

display mpls static-cr-lsp [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is an existing LSP name.
exclude	Displays information about the CR-LSPs without specified destination IP addresses.	-
include	Displays information about the CR-LSPs of specified destination IP addresses.	-
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a destination address.	The value is an integer that ranges from 0 to 32.

Parameter	Description	Value
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about static CR-LSPs, run the **display mpls static-cr-lsp** command.

Example

Display brief information about static CR-LSPs.

```
<HUAWEI> display mpls static-cr-lsp
TOTAL         : 2     STATIC CRLSP(S)
UP            : 2     STATIC CRLSP(S)
DOWN          : 0     STATIC CRLSP(S)
Name            FEC               I/O Label    I/O If           Status
Tunnel1       3.3.3.3/32        NULL/20      -/Vlanif10         Up
Tunnel2       -/-               130/NULL     Vlanif10/-         Up
```

Table 9-71 Description of the display mpls static-cr-lsp command output

Item	Description
TOTAL	Total number of static CR-LSPs.
UP	Number of the static CR-LSPs in the Up state.
DOWN	Number of the static CR-LSPs in the DOWN state.
Name	Name of a static CR-LSP.
FEC	Destination IP address and mask length.
I/O Label	Incoming and outgoing labels.
I/O If	Incoming and outgoing interfaces.
Status	Current status of a CR-LSP.

Display detailed information about static CR-LSPs.

```
<HUAWEI> display mpls static-cr-lsp verbose
No             : 1
LSP-Name       : tunnel1
```

```
LSR-Type       : Transit
FEC            : -/-
In-Label       : 20
Out-Label      : 30
In-Interface   : Vlanif10
Out-Interface  : Vlanif20
NextHop        : 10.1.3.2
Lsp Status     : Up
```

Table 9-72 Description of the display mpls static-cr-lsp verbose command output

Item	Description
No	Sequence number of a static CR-LSP.
LSP-Name	Name of a static CR-LSP.
LSR-Type	Type of a static CR-LSP: ● Ingress ● Transit ● Egress
FEC	Destination address and mask length. "-/-" is displayed for the transit node and egress node.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Incoming interface.
Out-Interface	Outgoing interface.
NextHop	Next-hop address in the format X.X.X.X.
Lsp Status	Status of a static CR-LSP: ● Up: indicates that the static CR-LSP is successfully established. ● Down: indicates that the static CR-LSP fails to be established.

9.3.32 display mpls stale-interface

Function

The **display mpls stale-interface** command displays information about MPLS interfaces in the Stale state.

Format

display mpls stale-interface [*interface-index*] [**verbose**]

Parameters

Parameter	Description	Value
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer ranging from 1 to FFFFFFFE.
verbose	Displays detailed information about an interface, for example, whether FRR is configured. If FRR is configured, information about the bound tunnels is also displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The outbound interface of the primary tunnel protected by TE FRR becomes a stale interface in one of the following situations:

MPLS is disabled on the interface when the primary tunnel is in the FRR In-used state.

The **display mpls stale-interface** command displays information about the stale interfaces.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

Display information about all MPLS interfaces in the Stale state.

```
<HUAWEI> display mpls stale-interface
Stale-Interface       Status    TE Attr   LSP Count  CRLSP Count Effective MTU
0x81a                 Up        Dis       0          1           1500
```

Table 9-73 Description of the display mpls stale-interface command output

Item	Description
Stale-Interface	Index of an MPLS interface in the Stale state.
Status	Status of the stale interface. ● Up ● Down

Item	Description
TE Attr	Whether MPLS TE is enabled on an interface: ● Dis: MPLS TE is not enabled on the interface. ● En: MPLS TE is enabled on the interface.
LSP Count	Number of LSPs on an interface.
CRLSP Count	Number of CR-LSPs on an interface.
Effective MTU	MTU value used in the MPLS forwarding. ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.

Display detailed information about all MPLS interfaces in the Stale state.

```
<HUAWEI> display mpls stale-interface verbose
No                    :  1
Interface             :  0x81a
Status                :  Up
TE Attribute          :  Disable
Static LSPCount       :  0
Static CR-LSPCount    :  0
LDP LSPCount          :  0
RSVP LSPCount         :  1
MPLS MTU              :  -
Interface MTU         :  -
Effective MTU         :  1500
TE FRR                :  Enable
Manual Bypass         :  Tun1
Interface State       :  Stale
```

Table 9-74 Description of the display mpls stale-interface verbose command output

Item	Description
No	Serial number.
Interface	Index of an MPLS interface in the Stale state.
Status	Status of the stale interface, which is the Up state in this example.
TE Attribute	Whether MPLS TE is enabled on the interface: ● Disable: MPLS TE is disabled. ● Enable: MPLS TE is enabled.
Static LSPCount	Number of static LSPs created on the interface.
Static CR-LSPCount	Number of static CR-LSPs created on the interface.
LDP LSPCount	Number of LDP LSPs created on the interface.

Item	Description
RSVP LSPCount	Number of RSVP-TE LSPs created on the interface.
MPLS MTU	MPLS MTU set using the **mpls mtu** command. When the interface is in the Stale state, a hyphen (-) is displayed.
Interface MTU	MTU configured on the interface. To set the MTU, run the **mtu** command.
Effective MTU	MTU value used in the MPLS forwarding. ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.
TE FRR	Whether MPLS TE is enabled on the interface: ● Disable: No bypass tunnel is set up in manual FRR mode to protect the interface. ● Enable: A bypass tunnel is set up in manual FRR mode to protect the interface.
Manual Bypass	Name of a bypass tunnel set up in manual FRR mode.
Interface State	Interface status. Stale indicates that the interface is to be deleted.

9.3.33 display mpls te cspf destination

Function

The **display mpls te cspf destination** command helps you check whether the specified path is available or not. You can specify relevant parameters in the command to set constraint conditions.

Format

display mpls te cspf destination *ip-address* [**affinity** *properties* [**mask** *mask-value*] | **bandwidth** { **ct0** *ct0-bandwidth* | **ct1** *ct1-bandwidth* } * | **explicit-path** *path-name* | **hop-limit** *hop-limit-number* | **metric-type** { **igp** | **te** } | **priority** *setup-priority* | **srlg-strict** *exclude-path-name* | **tie-breaking** { **random** | **most-fill** | **least-fill** }] * [**hot-standby** [**explicit-path** *path-name* | **overlap-path** | **affinity** *properties* [**mask** *mask-value*] | **hop-limit** *hop-limit-number* | **srlg** { **preferred** | **strict** }] *]

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the destination IP address of an MPLS TE tunnel.	The value is in dotted decimal notation.
affinity *properties*	Specifies the affinity property of an MPLS TE tunnel.	The value is a hexadecimal number that ranges from 0 to FFFFFFFF.
mask *mask-value*	Specifies the value of the affinity property mask.	The value is a hexadecimal number that ranges from 0 to FFFFFFFF.
bandwidth	Specifies the required bandwidth of an MPLS TE tunnel.	-
ct0 *ct0-bandwidth* | **ct1** *ct1-bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT1.	The value is an integer that ranges from 1 to 4000000000.
explicit-path *path-name*	Specifies the explicit path of an MPLS TE tunnel.	The value is an existing explicit path name.
hop-limit *hop-limit-number*	Specifies the maximum number of hops on an MPLS TE tunnel.	The value is an integer that ranges from 1 to 32. By default, the maximum number of hops is 32.
metric-type	Specifies the metric type for the CSPF calculation.	-
igp	Specifies the metric type as IGP.	-
te	Specifies the metric type as TE.	-
priority *setup-priority*	Specifies the setup priority of an MPLS TE tunnel.	The value is an integer that ranges from 0 to 7.
srlg-strict *exclude-path-name*	Specifies the path of a specified SRLG.	The value is an existing explicit path name.

Parameter	Description	Value
tie-breaking	Configures a tie-breaking mode for CSPF.	-
random	Configures the random mode.	-
most-fill	Configures the most-fill mode, meaning the path with the highest ratio of used bandwidth to maximum reservable bandwidth is selected.	-
least-fill	Configures the least-fill mode, meaning the path with the lowest ratio of used bandwidth to the maximum capacity of reservable bandwidth is selected.	-
hot-standby	Configures hot-standby path excluding primary path.	-
overlap-path	Specifies that if a completely disjoint path is not available, a maximally disjoint path should be computed for the Hot-standby.	-
srlg preferred	Specifies that the SRLG attribute is an optional constraint used by CSPF to calculate the path for the hot-standby CR-LSP. If CSPF fails to calculate the path for the hot-standby CR-LSP based on the SRLG attribute, CSPF recalculates the path, regardless of the SRLG attribute.	-
srlg strict	Specifies that the SRLG attribute is a required constraint used by CSPF to calculate the path for the hot-standby CR-LSP. The links of the hot-standby CR-LSP and the primary CR-LSP cannot be in the same SRLG.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Prerequisites

Before running this command, the CSPF function must have been enabled by using the **mpls te cspf** command.

Precautions

When this command is run, the device uses CSPF to check whether there is a path satisfying the specified constraints. If such a path exists, its information is displayed; otherwise, the display is empty.

Example

Display the path with the destination address being 10.3.3.9 by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.3.3.9
Path for the given constraints is:
10.1.1.9            Include      LSR-ID
172.16.1.1           Include
172.16.1.2           Include
10.2.2.9            Include      LSR-ID
172.17.1.1           Include
172.17.1.2           Include
10.3.3.9            Include      LSR-ID
The total metrics of the calculated path is :   2
```

Display the explicit path named path1 with the destination address being 10.3.3.9 by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.3.3.9 explicit-path path1
Path for the given constraints is:
10.1.1.9            Include      LSR-ID
172.16.1.1           Include
172.16.1.2           Include
10.2.2.9            Include      LSR-ID
172.17.1.1           Include
172.17.1.2           Include
10.3.3.9            Include      LSR-ID
The total metrics of the calculated path is :   2
```

Display the hot standby path with the destination address being 10.3.3.9 by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.3.3.9 hot-standby
Path for the given constraints is:
10.1.1.9            Include      LSR-ID
172.16.1.1           Include
172.16.1.2           Include
10.2.2.9            Include      LSR-ID
172.17.1.1           Include
172.17.1.2           Include
10.3.3.9            Include      LSR-ID
The total metrics of the calculated path is :   2

Hot-standby path for the given constraints is:
10.1.1.9            Include      LSR-ID
172.19.1.1           Include
```

```
172.19.1.2                Include
10.6.6.9                Include        LSR-ID
172.20.1.1                Include
172.20.1.2                Include
10.3.3.9                Include        LSR-ID
Complete disjoint path computed and the total metrics of the calculated path is :    2
```

Display the hot standby path with the destination address being 10.4.4.9 and partial overlapping by performing the CSPF calculation.

```
<HUAWEI> display mpls te cspf destination 10.4.4.9 hot-standby overlap-path
Main path for the given constraints is:
10.1.1.9                Include        LSR-ID
172.16.1.1                Include
172.16.1.2                Include
10.2.2.9                Include        LSR-ID
172.17.1.1                Include
172.17.1.2                Include
10.3.3.9                Include        LSR-ID
172.18.1.1                Include
172.18.1.2                Include
10.4.4.9                Include        LSR-ID
The total metrics of the calculated path is :   3

Hot-standby path for the given constraints is:
10.1.1.9                Include        LSR-ID
172.21.1.1                Include
172.21.1.2                Include
10.6.6.9                Include        LSR-ID
172.22.1.1                Include
172.22.1.2                Include
10.3.3.9                Include        LSR-ID
172.18.1.1                Include
172.18.1.2                Include
10.4.4.9                Include        LSR-ID
Partial Overlap path computed and the total metrics of the calculated path is :
   3
```

Table 9-75 Description of the display mpls te cspf destination command output

Item	Description
Path for the given constraints is	Path calculated by CSPF. If * is displayed, it indicates the node does not exist on the explicit path calculated by CSPF. If * is not displayed, it indicates that the node exists on the path calculated by CSPF.
10.1.1.9 Include LSR-ID	Path information. 10.1.1.9 is the next hop address, Include is the node name, and LSR-ID indicates that the LSR ID is used as the address.
The total metrics of the calculated path is	Calculated metric value of a path.
Main path for the given constraints is	Path for the main request, when both main and hot-standby are requested.
Hot-standby path for the given constraints is	Path calculated by CSPF for the hot-standby.

Item	Description
Complete disjoint path computed and the total metrics of the calculated path is	CSPF has calculated complete disjoint path from main path for hot-standby.
Partial Overlap path computed and the total metrics of the calculated path is	CSPF has calculated partial overlap path from main path for hot-standby.

9.3.34 display mpls te cspf tedb

Function

The **display mpls te cspf tedb** command displays the CSPF TEBD information based on specified conditions.

Format

display mpls te cspf tedb { **all** | **area** { *area-id* | *area-id-ip* } | **interface** *ip-address* | **network-lsa** | **node** [*router-id*] | **srlg** *srlg-number* | **overload-node** }

Parameters

Parameter	Description	Value
all	Displays information about all TEDB nodes.	-
area *area-id*	Specifies the ID of an area.	For an OSPF area, the value is an integer that ranges from 0 to 4294967295. For an IS-IS area, the value is 1 or 2.
area *area-id-ip*	Specifies the ID of an area in IP address format.	For an OSPF area, the value is in dotted decimal notation.
interface *ip-address*	Specifies the IP address of an interface	The value is in dotted decimal notation.
network-lsa	Displays information about all network LSAs.	-
node	Displays information about a node.	-
router-id	Specifies the router ID.	The value is in dotted decimal notation.
srlg *srlg-number*	Specifies the SRLG number.	The value is an integer that ranges from 0 to 4294967295.
overload-node	Displays information of all the overload-nodes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the CSPF TEBD information, run the **display mpls te cspf tedb** command.

Example

Display information about network LSAs in a TEDB.

```
<HUAWEI> display mpls te cspf tedb network-lsa
Maximum Network LSA Supported    : 512
Current Total Network LSA Number : 6

ID : 1
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.16.1.2
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID      NBR-OSPF-Router-ID
     10.2.2.9           10.2.2.9
     10.1.1.9           10.1.1.9

ID : 2
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.20.1.1
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID      NBR-OSPF-Router-ID
     10.2.2.9           10.2.2.9
     10.3.3.9           10.3.3.9

ID : 3
   IGP-Type: ISIS
   Process-ID: 1
   DR-Router-ID : 10.1.1.9
   DR-Address : 172.16.1.1
   Area : Level-2
   DR-ISIS-System-ID : 0000.0000.0001.01
     NBR-Router-ID      NBR-ISIS-System-ID
     10.1.1.9           0000.0000.0001.00
     10.2.2.9           0000.0000.0002.00

ID : 4
   IGP-Type: ISIS
   Process-ID: 1
   DR-Router-ID : 10.1.1.9
   DR-Address : 172.16.1.1
   Area : Level-1
   DR-ISIS-System-ID : 0000.0000.0001.01
     NBR-Router-ID      NBR-ISIS-System-ID
     10.1.1.9           0000.0000.0001.00
     10.2.2.9           0000.0000.0002.00

ID : 5
```

```
   IGP-Type: ISIS
   Process-ID: 1
   DR-Router-ID : 10.3.3.9
   DR-Address : 172.20.1.2
   Area : Level-1
   DR-ISIS-System-ID : 0000.0000.0003.01
     NBR-Router-ID       NBR-ISIS-System-ID
     10.3.3.9            0000.0000.0003.00
     10.2.2.9            0000.0000.0002.00

ID : 6
   IGP-Type: ISIS
   Process-ID: 1
   DR-Router-ID : 10.3.3.9
   DR-Address : 172.20.1.2
   Area : Level-2
   DR-ISIS-System-ID : 0000.0000.0003.01
     NBR-Router-ID       NBR-ISIS-System-ID
     10.3.3.9            0000.0000.0003.00
     10.2.2.9            0000.0000.0002.00
```

Table 9-76 Description of the display mpls te cspf tedb network-lsa command output

Item	Description
Maximum Network LSA Supported	Maximum network LSAs supported.
Current Total Network LSA Number	Current total number of network LSAs.
IGP-Type	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
ID	Sequence number.
DR-Router-ID	DR Router ID.
DR-Address	Interface address of the DR.
Area	Area to which the device belongs.
DR-OSPF-Router-ID	OSPF router ID of a DR.
DR-ISIS-System-ID	IS-IS system ID of a DR.
NBR-Router-ID	Neighbor Router ID.
NBR-OSPF-Router-ID	Neighbor OSPF router ID.
NBR-ISIS-System-ID	Neighbor IS-IS system ID.

Display information about all TEDBs.

```
<HUAWEI> display mpls te cspf tedb all
Maximum Nodes Supported: 512   Current Total Node Number: 6
```

```
Maximum Links Supported: 2048   Current Total Link Number: 12
Maximum SRLGs supported: 5120   Current Total SRLG Number: 0
ID     Router-ID        IGP      Process-ID     Area           Link-Count
1      10.1.1.9         OSPF     1              0              1
2      10.2.2.9         OSPF     1              0              2
3      10.3.3.9         OSPF     1              0              1
4      10.1.1.9         ISIS     1              Level-1,2      2
5      10.2.2.9         ISIS     1              Level-1,2      4
6      10.3.3.9         ISIS     1              Level-1,2      2
```

Table 9-77 Description of the **display mpls te cspf tedb all** command output

Item	Description
Maximum Nodes Supported	Maximum number of nodes supported.
Maximum Links Supported	Maximum number of links supported.
Maximum SRLGs supported	Maximum SRLGs supported.
Current Total Node Number	Current total number of nodes.
Current Total Link Number	Current total number of links.
Current Total SRLG Number	Current total number of SRLGs.
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
Area	Area to which the device belongs.
Link-Count	Total number of connected links with a specified IGP and process ID.

Display TEDB information of a specified area.

```
<HUAWEI> display mpls te cspf tedb area 0
 Router Node Information for Area 0:
ID     Router-ID        IGP      Process-ID     Area           Link-Count
1      10.1.1.9         OSPF     1              0              1
2      10.2.2.9         OSPF     1              0              2
3      10.3.3.9         OSPF     1              0              1

Network LSA Information for Area 0:

ID : 1
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.16.1.2
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
     NBR-Router-ID       NBR-OSPF-Router-ID
     10.2.2.9            10.2.2.9
```

```
    10.1.1.9           10.1.1.9

ID : 2
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 10.2.2.9
   DR-Address : 172.20.1.1
   Area : 0
   DR-OSPF-Router-ID : 10.2.2.9
    NBR-Router-ID      NBR-OSPF-Router-ID
    10.2.2.9           10.2.2.9
    10.3.3.9           10.3.3.9
```

Table 9-78 Description of the display mpls te cspf tedb area command output

Item	Description
Router Node Information for Area 0	Router node information for area 0.
Network LSA Information for Area 0	Network LSA information for area 0.
Link-Count	Total number of connected links with a specified IGP and process ID.
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
IGP-Type	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
DR-Router-ID	Router ID of the DR.
DR-Address	Interface address of the DR.
Area	Area to which the device belongs.
DR-OSPF-Router-ID	OSPF router ID of the designated router.
NBR-Router-ID	Router ID of a neighbor router.
NBR-OSPF-Router-ID	OSPF router ID of a neighbor device.

Display TEDB information of a specified node.

```
<HUAWEI> display mpls te cspf tedb node 10.1.1.9
 Router ID: 10.1.1.9
 IGP Type: OSPF      Process ID: 1
  MPLS-TE Link Count: 1
  Link[1]:
```

```
  OSPF Router ID: 10.1.1.9           Opaque LSA ID: 10.0.0.1
  Interface IP Address: 172.16.1.1
  DR Address: 172.16.1.2
  IGP Area: 0
  Link  Type: Multi-access  Link Status: Active
  IGP Metric: 1             TE Metric: 1         Color: 0x0
  Bandwidth Allocation Model : Russian Dolls Model
  Maximum Link Bandwidth: 40000 (kbps)
  Maximum Reservable Bandwidth: 40000 (kbps)
  Bandwidth Constraints:       Local Overbooking Multiplier:
      BC[0]:      40000 (kbps)         LOM[0]:        1
      BC[1]:      30000 (kbps)         LOM[1]:        1
      BC[2]:      20000 (kbps)         LOM[2]:        1
      BC[3]:          0 (kbps)         LOM[3]:        1
      BC[4]:          0 (kbps)         LOM[4]:        1
      BC[5]:          0 (kbps)         LOM[5]:        1
      BC[6]:          0 (kbps)         LOM[6]:        1
      BC[7]:          0 (kbps)         LOM[7]:        1
  BW Unreserved:
      Class  ID:
      [0]:          0 (kbps),          [1]:          0 (kbps)
      [2]:          0 (kbps),          [3]:          0 (kbps)
      [4]:          0 (kbps),          [5]:          0 (kbps)
      [6]:          0 (kbps),          [7]:          0 (kbps)
Router ID: 10.1.1.9
IGP Type: ISIS      Process ID: 1
 MPLS-TE Link Count: 2
 Link[1]:
  ISIS System ID: 0000.0000.0001.00     Opaque LSA ID: 0.0.0.0
  Interface IP Address: 172.16.1.1
  DR Address: 172.16.1.1
  DR ISIS System ID: 0000.0000.0001.01
  IGP Area: Level-2
  Link  Type: Multi-access  Link Status: Active
  IGP Metric: 10            TE Metric: 10        Color: 0x0
  Bandwidth Allocation Model : Russian Dolls Model
  Maximum Link Bandwidth: 40000 (kbps)
  Maximum Reservable Bandwidth: 40000 (kbps)
  Bandwidth Constraints:       Local Overbooking Multiplier:
      BC[0]:      40000 (kbps)         LOM[0]:        1
      BC[1]:      30000 (kbps)         LOM[1]:        1
      BC[2]:      20000 (kbps)         LOM[2]:        1
      BC[3]:          0 (kbps)         LOM[3]:        1
      BC[4]:          0 (kbps)         LOM[4]:        1
      BC[5]:          0 (kbps)         LOM[5]:        1
      BC[6]:          0 (kbps)         LOM[6]:        1
      BC[7]:          0 (kbps)         LOM[7]:        1
  BW Unreserved:
      Class  ID:
      [0]:          0 (kbps),          [1]:          0 (kbps)
      [2]:          0 (kbps),          [3]:          0 (kbps)
      [4]:          0 (kbps),          [5]:          0 (kbps)
      [6]:          0 (kbps),          [7]:          0 (kbps)
```

Table 9-79 Description of the display mpls te cspf tedb node command output

Item	Description
Router ID	Router ID in the format X.X.X.X.
IGP Type	IGP type: - OSPF - IS-IS
Process ID	IGP Process ID.

Item	Description
MPLS-TE Link Count	Number of MPLS TE link.
OSPF Router ID	OSPF Route ID.
ISIS System ID	IS-IS system ID.
Interface IP Address	Interface IP address.
DR Address	DR address.
DR ISIS System ID	IS-IS system ID of the DR.
IGP Area	IGP area.
Link Type	Link type.
Link Status	Link status.
Link [x]	Link information, with "x" being the link number.
IGP Metric	IGP metric of a link.
TE Metric	TE metric of a link.
Color	Color of a link.
Maximum Link Bandwidth	Maximum bandwidth of a link.
Maximum Reservable Bandwidth	Maximum capacity of reserved bandwidth for a link.
Bandwidth Allocation Model	Bandwidth allocation model.
Bandwidth Constraints	Bandwidth constraints.
Local Overbooking Multiplier	Local overbooking multiplier.
BC	Bandwidth constraints.
LOM	Local overbooking multiplier.
BW Unreserved	Unreserved bandwidth for LSPs.
Class ID: [x]:	Class 0 to Class 7.

Display information about overloaded nodes in a TEDB.

```
<HUAWEI> display mpls te cspf tedb overload-node
Current Total Overload Node Number : 4
ID     Router-ID      IGP    Process-ID   Area       IGP_ID
1      10.3.3.3       ISIS   1            Level-1    3333.3333.3333.00
2      10.1.1.1       ISIS   1            Level-1    1111.1111.1111.00
3      10.1.1.1       ISIS   2            Level-1    1111.1111.1112.00
4      10.2.2.2       ISIS   1            Level-1    2222.2222.2222.00
```

Table 9-80 Description of the display mpls te cspf tedb overload-node command output

Item	Description
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
Process-ID	IGP Process ID.
Area	Area to which a device belongs.
IGP_ID	● OSPF router ID of a neighbor device. ● IS-IS system ID of a neighbor device.

9.3.35 display mpls te hot-standby state

Function

The **display mpls te hot-standby state** command displays the hot-standby status of all tunnels or a specified tunnel.

Format

display mpls te hot-standby state { **all** [**verbose**] | **interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
all	Displays the status of all hot-standby tunnels.	-
verbose	Displays detailed information about hot-standby tunnels.	-
interface tunnel *interface-number*	Displays the status of a specified hot-standby tunnel.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When running the **display mpls te hot-standby state** command, note the following issues:

- The command displays the status of only hot-standby TE tunnels.
- If a tunnel interface is deleted or traffic switches from the tunnel to an ordinary backup tunnel, no command output is displayed.

Example

Display the hot-standby status of Tunnel 1.

```
<HUAWEI> display mpls te hot-standby state interface tunnel 1
(s): same path
----------------------------------------------------------------------
Verbose information about the Tunnel1 hot-standby state
----------------------------------------------------------------------
session id                  : 300
main LSP token              : 0x9
hot-standby LSP token       : 0x0
HSB switch result           : Primary LSP
HSB switch reason           : -
WTR config time             : 10s
WTR remain time             : -
using overlapped path       : -
```

Table 9-81 Description of the display mpls te hot-standby state command output

Item	Description
session id	Session ID, which is the configured tunnel ID.
main LSP token	Index of the primary CR-LSP.
hot-standby LSP token	Index of the hot-standby CR-LSP.
HSB switch result	Result of a switchover: - Primary LSP: indicates that data is switched to the primary CR-LSP. - Hot-standby LSP: indicates that data is switched to the hot-standby CR-LSP. - Ordinary LSP: indicates that data is switched to the ordinary CR-LSP. - Best-Effort LSP: indicates that data is switched to the best-effort path.
HSB switch reason	Reason why traffic is switched to the hot-standby LSP.

Item	Description
WTR config time	WTR time. If a primary CR-LSP recovers from a fault, the system waits for a period of time, or the WTR time, to switch data from the hot-standby CR-LSP or best-effort path to the primary LSP.
WTR remain time	WTR remain time.
using overlapped path	Whether the path of the primary tunnel and the path of the backup tunnel overlap: ● yes: indicates that they overlap. ● no: indicates that they do not overlap. ● -: indicates that the system does not check whether they overlap.

Display the hot-standby status of all hot-standby tunnels.

```
<HUAWEI> display mpls te hot-standby state all
(s): same path
------------------------------------------------------------------------------
No.        tunnel name         session id      switch result        overlap
------------------------------------------------------------------------------
1          Tunnel1             3               Best-Effort LSP      -
2          Tunnel2             9               Primary LSP          -
```

Table 9-82 Description of the display mpls te hot-standby state all command output

Item	Description
No.	Sequence number.
tunnel name	Name of a tunnel.
session id	Session ID, which is the configured tunnel ID.
switch result	Result of a switchover: ● Primary LSP: indicates that data is switched to the primary CR-LSP. ● Hot-standby LSP: indicates that data is switched to the hot-standby CR-LSP. ● Ordinary LSP: indicates that data is switched to the ordinary CR-LSP. ● Best-Effort LSP: indicates that data is switched to the best-effort path.

Item	Description
overlap	Whether the primary path overlaps the hot-standby path: - yes: They share one or multiple links. - no: They do not share links. - -: Their paths cannot be compared. - yse(s): They overlap each other.

9.3.36 display mpls te link-administration admission-control

Function

The **display mpls te link-administration admission-control** command displays CR-LSP information received by all links, including bandwidth and priority.

Format

display mpls te link-administration admission-control [**interface** *interface-type interface-number* | **stale-interface** *interface-index*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about admission control of a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
stale-interface *interface-index*	Displays information about admission control of a stale interface. *interface-index* specifies the index of the stale interface.	The value is a hexadecimal integer that ranges from 1 to FFFFFFFE.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls stale-interface** command without specifying any parameter to view the index of a stale interface.

Example

Display information about the admission control of all MPLS TE links.

```
<HUAWEI> display mpls te link-administration admission-control
LspID                    In/Out IF                    S/H Prio CT BW(kbps)
10.3.3.9:300:4             Vlanif10 / ---                 7 /7     -  -
```

Display information about admission control of a stale interface.

```
<HUAWEI> display mpls te link-administration admission-control stale-interface 18000106
LspID                    In/Out IF              S/H Prio  CT        BW (kbps)
10.1.1.1:600:1          --- / 0x18000106           0 /0      0         0
```

Table 9-83 Description of the display mpls te link-administration admission-control command output

Item	Description
LspID	LSP ID, uniquely identified in the form of <Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID>.
In/Out IF	Incoming and outgoing interfaces.
S/H Prio	Setup and holding priorities. Setup priority: An integer ranging from 0 to 7. The smaller the value, the higher the priority. Holding priority: An integer ranging from 0 to 7. The smaller the value, the higher the priority.
CT	Class type.
BW	Bandwidth.

9.3.37 display mpls te link-administration bandwidth-allocation

Function

The **display mpls te link-administration bandwidth-allocation** command displays information about bandwidth allocation of a specified MPLS TE interface or all MPLS TE interfaces.

Format

display mpls te link-administration bandwidth-allocation [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about bandwidth allocation of a specified interface. - *interface-type*: indicates the interface type. - *interface-number*: indicates the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about bandwidth allocation of the MPLS TE interfaces, run the **display mpls te link-administration bandwidth-allocation** command.

Example

Display information about the bandwidth allocation of all MPLS TE interfaces.

```
<HUAWEI> display mpls te link-administration bandwidth-allocation
 Link ID:  Vlanif10
 Bandwidth Constraint Model   :  Russian Dolls Model (RDM)
 Physical Link Bandwidth(Kbits/sec)          :  1000000
 Maximum Link Reservable Bandwidth(Kbits/sec):  1000000
 Reservable Bandwidth BC0(Kbits/sec)         :  500000
 Reservable Bandwidth BC1(Kbits/sec)         :  4000
 Downstream Bandwidth (Kbits/sec)            :  0
 IPUpdown Link Status                        :  UP
 PhysicalUpdown Link Status                  :  UP
 GracefulUpdown Link Status                  :  DOWN
 ----------------------------------------------------------------------
 TE-CLASS  CT    PRIORITY   BW RESERVED    BW AVAILABLE   DOWNSTREAM
                            (Kbit/sec)     (Kbit/sec) RSVPLSPNODE COUNT
 ----------------------------------------------------------------------
    0      0       0           0            500000         0
    1      0       1           0            500000         0
    2      0       2           0            500000         0
    3      0       3           0            500000         0
    4      0       4           0            500000         0
    5      0       5           0            500000         0
    6      0       6           0            500000         0
    7      0       7           0            500000         0
    8      1       0           0            4000           0
    9      1       1           0            4000           0
   10      1       2           0            4000           0
   11      1       3           0            4000           0
```

```
   12     1        4          0           4000            0
   13     1        5          0           4000            0
   14     1        6          0           4000            0
   15     1        7          0           4000            0

----------------------------------------------------------------------


 Link ID:  GigabitEthernet0/0/1
 Bandwidth Constraint Model   :  Russian Dolls Model (RDM)
 Physical Link Bandwidth(Kbits/sec)          :  1000000
 Maximum Link Reservable Bandwidth(Kbits/sec):  1000000
 Reservable Bandwidth BC0(Kbits/sec)         :  500000
 Reservable Bandwidth BC1(Kbits/sec)         :  4000
 Downstream Bandwidth (Kbits/sec)            :  0
 IPUpdown Link Status                        :  UP
 PhysicalUpdown Link Status                  :  UP
 GracefulUpdown Link Status                  :  DOWN
 ----------------------------------------------------------------------
 TE-CLASS  CT    PRIORITY   BW RESERVED    BW AVAILABLE   DOWNSTREAM
                       (Kbit/sec)      (Kbit/sec)  RSVPLSPNODE COUNT
 ----------------------------------------------------------------------
    0      0       0          0           500000          0
    1      0       1          0           500000          0
    2      0       2          0           500000          0
    3      0       3          0           500000          0
    4      0       4          0           500000          0
    5      0       5          0           500000          0
    6      0       6          0           500000          0
    7      0       7          0           500000          0
    8      1       0          0           4000            0
    9      1       1          0           4000            0
    10     1       2          0           4000            0
    11     1       3          0           4000            0
    12     1       4          0           4000            0
    13     1       5          0           4000            0
    14     1       6          0           4000            0
    15     1       7          0           4000            0
 ----------------------------------------------------------------------
```

Table 9-84 Description of the display mpls te link-administration bandwidth-allocation command output

Item	Description
Link ID	MPLS TE interface number.
Bandwidth Constraint Model	Bandwidth Constraints Model used by a TE tunnel: ● RDM: Russian Dolls Model ● MAM: Maximum Allocation Model ● Extended MAM: Extended Maximum Allocation Model
Physical Link Bandwidth(Kbits/sec)	Indicates the capacity of bandwidth for a physical link.

Item	Description
Maximum Link Reservable Bandwidth(Kbits/sec)	Maximum capacity of reserved bandwidth for a link. To set the maximum capacity of reserved bandwidth for a link, run the **mpls te bandwidth max-reservable-bandwidth** command.
Reservable Bandwidth BCi(0≤i≤7) (Kbits/sec)	Bandwidth that is reserved for BCi. To set the bandwidth that is reserved for BCi, run the **mpls te bandwidth** command.
Downstream Bandwidth (Kbits/ sec)	Bandwidth of an outgoing interface.
IPUpdown Link Status	IP link status of an interface: ● UP: IP link is available. ● DOWN: IP link is unavailable.
PhysicalUpdown Link Status	Physical link status of an interface: ● UP: The physical link is available. ● DOWN: The physical link is unavailable.
GracefulUpdown Link Status	Graceful link status of an interface: ● UP: The graceful link is available. ● DOWN: The graceful link is unavailable.
TE-CLASS	TE class.
CT	Class type.
PRIORITY	Preemption priority of an MPLS TE tunnel. To set the preemption priority of an MPLS TE tunnel, run the **mpls te priority** command.
BW RESERVED (Kbit/sec)	Reserved bandwidth for LSPs of the CT.
BW AVAILABLE (Kbit/sec)	Available bandwidth for LSPs of the CT.
DOWNSTREAM RSVPLSPNODE COUNT	Number of downstream RSVP LSP nodes.

9.3.38 display mpls te link-administration srlg-information

Function

The **display mpls te link-administration srlg-information** command displays SRLG(s) to which the interface belongs.

Format

display mpls te link-administration srlg-information [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the SRLG in the interface view, you can run the **display mpls te link-administration srlg-information** command to check the configuration.

Example

Display the SLRG(s) to which VLANIF100 belongs to.

```
<HUAWEI> display mpls te link-administration srlg-information interface vlanif100

 SRLGs on Vlanif100 :
            2             3             9
```

Table 9-85 Description of the display mpls te link-administration srlg-information command output

Item	Description
SRLGs on Vlanif100	SRLG number to which an interface belongs.

9.3.39 display mpls te protection binding protect-tunnel

Function

The **display mpls te protection binding protect-tunnel** command displays the tunnel protection relationship.

Format

display mpls te protection binding protect-tunnel { *tunnel-id* | **interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
tunnel-id	Displays information about the protection relationship related to a protection tunnel (that is, a backup tunnel) with a specified ID.	The value is an integer that ranges from 1 to 10000.
tunnel *interface-number*	Displays information about the protection relationship related to the specified tunnel interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the tunnel protection relationship, run the **display mpls te protection binding protect-tunnel** command.

Example

Display the protection relationship related to the protection tunnel with the ID of 10.

```
<HUAWEI> display mpls te protection binding protect-tunnel 10
------------------------------------------------------------------------
Binding information of( tunnel id:  10 )
------------------------------------------------------------------------
    Protect-tunnel id                    :10
    Protect-tunnel name                  :Tunnel1
    Maximum number of bound work-tunnels :16
    Currently bound work-tunnels         :Total( 1 )
                                         :Tunnel2
```

Table 9-86 Description of the display mpls te protection binding protect-tunnel command output

Item	Description
Protect-tunnel id	ID of a protection tunnel (the backup tunnel).
Protect-tunnel name	Name of a protection tunnel (the interface name).

Item	Description
Maximum number of bound work-tunnels	Maximum number of tunnels that a protection tunnel can protect.
Currently bound work-tunnels	Information about the working tunnel to which a protection tunnel is currently bound, including the quantity and list.

9.3.40 display mpls te protection tunnel

Function

The **display mpls te protection tunnel** command displays information about a specified tunnel and its tunnel protection group.

Format

display mpls te protection tunnel { **all** | *tunnel-id* | **interface tunnel** *interface-number* } [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all tunnel protection groups.	-
tunnel-id	Specifies the ID of a working tunnel or its protection tunnel.	The value is an integer that ranges from 1 to 10000.
interface	Displays information about tunnel protection groups on an interface.	-
tunnel *interface-number*	Specifies the name of a working tunnel or its protection tunnel.	-
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls te protection tunnel** command can be used to display information about a specified tunnel protection group. The following parameters can be specified to display various types of information:

- If the ID or tunnel interface of the working tunnel is specified, information about the working tunnel and its protection tunnel is displayed.
- If the ID or tunnel interface of a protection tunnel is specified, information about the protection tunnel and all its protected working tunnels is displayed.

Example

Display information about a working tunnel with the tunnel ID of 100 and its protection tunnel.

```
<HUAWEI> display mpls te protection tunnel 100
------------------------------------------------------------------------
No. Work-tunnel status  /id  Protect-tunnel status /id    Switch-Result
------------------------------------------------------------------------
1          in defect   /100       non-defect     /300  protect-tunnel
```

Table 9-87 Description of the display mpls te protection tunnel command output

Item	Description
No.	Sequence number of a tunnel protection group.
Work-tunnel status /id	Status and ID of a working tunnel. The tunnel status can be: ● non-defect: The tunnel functions properly. ● in defect: The tunnel fails.
Protect-tunnel status /id	Status and ID of a protection tunnel. The tunnel status can be: ● non-defect: The tunnel functions properly. ● in defect: The tunnel fails.
Switch-Result	Switching result: ● work-tunnel: Traffic switches to the working tunnel. ● protect-tunnel: Traffic switches to the protection tunnel.

Display detailed information about working tunnels and their protection tunnels.

```
<HUAWEI> display mpls te protection tunnel all verbose
----------------------------------------------------------------
Verbose information about the No.1 protection-group
----------------------------------------------------------------
Work-tunnel id                    : 1
Protect-tunnel id                 : 2
```

```
Work-tunnel name                         : Tunnel1
Protect-tunnel name                      : Tunnel2
Work-tunnel reverse-lsp                  : -
Protect-tunnel reverse-lsp               : -
Bridge type                              : 1:1
Switch type                              : unidirectional
Switch result                            : work-tunnel
Tunnel using Best-Effort                 : none
Tunnel using Ordinary                    : none
Work-tunnel frr in use                   : none
Work-tunnel defect state                 : non-defect
Protect-tunnel defect state              : non-defect
Work-tunnel forward-lsp defect state     : non-defect
Protect-tunnel forward-lsp defect state  : non-defect
Work-tunnel reverse-lsp defect state     : non-defect
Protect-tunnel reverse-lsp defect state  : non-defect
HoldOff config time                      : 0ms
HoldOff remain time                      : -
WTR config time                          : 30s
WTR remain time                          : -
Mode                                     : revertive
Using same path                          : -
Local state                              : no request
Far end request                          : no request
```

Table 9-88 Description of the display mpls te protection tunnel all verbose command output

Item	Description
Work-tunnel id	ID of the working tunnel.
Protect-tunnel id	ID of the protection tunnel.
Work-tunnel name	Tunnel interface name of the working tunnel.
Protect-tunnel name	Tunnel interface name of the protection tunnel.
Work-tunnel reverse-lsp	Name of the reverse CR-LSP in the working tunnel.
Protect-tunnel reverse-lsp	Name of the reverse CR-LSP in the protection tunnel.
Bridge type	Bridge mode.
Switch type	Switch mode.
Switch result	Switching result: ● work-tunnel: Traffic switches to the working tunnel. ● protect-tunnel: Traffic switches to the protection tunnel.
Tunnel using Best-Effort	Whether a best-effort path is used as a protection tunnel.
Tunnel using Ordinary	Whether an ordinary backup tunnel is used as a protection tunnel.

Item	Description
Work-tunnel frr in use	Whether the working tunnel is in the FRR in-use state.
Work-tunnel defect state	Working tunnel status: - non-defect: The working tunnel functions properly. - in defect: The working tunnel fails.
Protect-tunnel defect state	Protection tunnel status: - non-defect: The protection tunnel functions properly. - in defect: The protection tunnel fails.
Work-tunnel forward-lsp defect state	Status of the forward CR-LSP in the working tunnel: - non-defect: The forward CR-LSP functions properly. - in defect: The forward CR-LSP fails.
Protect-tunnel forward-lsp defect state	Status of the forward CR-LSP in the protection tunnel: - non-defect: The forward CR-LSP functions properly. - in defect: The forward CR-LSP fails.
Work-tunnel reverse-lsp defect state	Status of the reverse CR-LSP in the working tunnel: - non-defect: The reverse CR-LSP functions properly. - in defect: The reverse CR-LSP fails.
Protect-tunnel reverse-lsp defect state	Status of the reverse CR-LSP in the protection tunnel: - non-defect: The reverse CR-LSP functions properly. - in defect: The reverse CR-LSP fails.
HoldOff config time	Switching delay time. To set the switching delay time, run the **mpls te protection tunnel** command.
HoldOff remain time	Remain time of switching delay time.
WTR config time	Wait-to-restore time. To set the wait-to-restore time, run the **mpls te protection tunnel** command.
WTR remain time	Remain time of wait-to-restore time.

Item	Description
Mode	Switchback mode: ● revertive: supports a switchback. ● non-revertive: does not support a switchback. To set the switchback mode, run the **mpls te protection tunnel** command.
Using same path	Whether a path of the working tunnel and a path of the protection tunnel overlap: ● yes: The two tunnels have an overlapped path. ● no: The two tunnels do not have an overlapped path. ● -: Undetected.
Local state	Switching mode on the local end: ● signal fail for protection ● no request
Far end request	Switching mode on the remote end.

9.3.41 display mpls te session-entry

Function

The **display mpls te session-entry** command displays detailed information about LSP sessions of tunnels.

Format

display mpls te session-entry [*ingress-lsr-id tunnel-id egress-lsr-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the LSR ID of the ingress.	In dotted decimal notation.
tunnel-id	Specifies the ID of a tunnel.	The value is an integer that ranges from 0 to 65535.
egress-lsr-id	Specifies the LSR ID of the egress.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view detailed information about LSP sessions of tunnels, run the **display mpls te session-entry** command.

Example

Display detailed information about LSP sessions of a tunnel.

```
<HUAWEI> display mpls te session-entry

 Ingress-ID               :  1.1.1.9
 Tunnel-ID                :  300
 Egress-ID                :  3.3.3.9
 Crlsp num                :  1
 First TunnelTable index  :  4
 LSP No.     :  1
 LSP ID      :  1.1.1.9:300:6
 In/Out IF   :  -/Vlanif10
 Bandwidth(Kbit/sec):
   CT0 : 500        CT1 : 0
```

Table 9-89 Description of the display mpls te session-entry command output

Item	Description
Ingress-ID	LSR ID of the ingress.
Tunnel-ID	Tunnel ID, which is the session ID.
Egress-ID	LSR ID of the egress.
Crlsp num	Number of CR-LSPs of the session entry.
First TunnelTable index	Index of the first CR-LSP of the session entry.
LSP No.	Sequence number of a CR-LSP.
LSP ID	LSP ID, uniquely identified in the form of <Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID>.
In/Out IF	Incoming and outgoing interface through which the CR-LSP passes on the local node.
Bandwidth(Kbit/sec)	Bandwidth, in kbit/s.
CT0	Bandwidth value of CR-LSPs of CT0.
CT1	Bandwidth value of CR-LSPs of CT1.

9.3.42 display mpls te srlg

Function

The **display mpls te srlg** command displays the Shared Risk Link Group (SRLG) configurations and the interfaces that belong to it.

Format

display mpls te srlg { *srlg-number* | **all** }

Parameters

Parameter	Description	Value
srlg-number	Specifies the number of the SRLG to which an interface belongs.	The value is an integer that ranges from 0 to 4294967295.
all	Displays information about all SRLGs on the node and the interfaces that belong to the SRLG groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the configuring the SRLG on an interface, you can run the **display mpls te srlg** command to check the configuration.

The **display mpls te srlg** command displays the following information:

- Maximum of SRLGs that a node can support
- Number of SRLGs that are configured on the node
- Member interfaces of each SRLG

Example

Display information about all SRLGs on the node.

```
<HUAWEI> display mpls te srlg all
Total SRLG supported : 1024
Total SRLG configured : 1
SRLG  239:            Vlanif30
```

Table 9-90 Description of the display mpls te srlg all command output

Item	Description
Total SRLG supported	Total SRLGs supported.
Total SRLG configured	Total SRLGs configured.
SRLG	Shared risk link group. To set the shared risk link group, run the **mpls te srlg** command.

9.3.43 display mpls te tunnel-interface

Function

The **display mpls te tunnel-interface** command displays information about tunnel interfaces on the local LSR.

Format

display mpls te tunnel-interface [**tunnel** *interface-number* | **auto-bypass-tunnel** [*tunnel-name*]]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the number of a tunnel interface on the local LSR.	-
auto-bypass-tunnel *tunnel-name*	Specifies the name of an MPLS TE tunnel. If the *tunnel-name* parameter is configured, information about the specified Auto bypass tunnel is displayed. If this parameter is not configured, information about all Auto bypass tunnels is displayed.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify any parameters, information about all tunnel interfaces is displayed.

Example

Display information about Tunnel 1.

```
<HUAWEI> display mpls te tunnel-interface tunnel 1
    ----------------------------------------------------------------
                            Tunnel1
    ----------------------------------------------------------------
    Tunnel State Desc   :  GRACEFUL SWITCH
    Active LSP          :  Best-Effort LSP
    Traffic Switch      :  Best-Effort LSP -> Ordinary LSP
    Session ID          :  50
    Ingress LSR ID      :  1.1.1.1          Egress LSR ID:  2.2.2.2
    Admin State         :  UP               Oper State   :  UP
    Primary LSP State      : DOWN
      Main LSP State       : SETTING UP
    Hot-Standby LSP State  : UP
      Main LSP State       : READY              LSP ID  : 32799
      Modify LSP State     : SETTING UP
    Ordinary LSP State     : UP
      Main LSP State       : READY              LSP ID  : 32782
    Best-Effort LSP State  : UP
      Main LSP State       : READY              LSP ID  : 32780
```

Table 9-91 Description of the display mpls te tunnel-interface command output

Item	Description
Tunnel State Desc	Tunnel status: - UP: indicates that the tunnel is successfully set up. - DOWN: indicates that the tunnel fails to be set up. - GRACEFUL SWITCH: indicates that the tunnels are switched through GR. - GRACEFUL DELETE: indicates that during the GR process a type of LSP is deleted.
Active LSP	Type of CR-LSP in use: - Primary LSP: indicates the primary CR-LSP. - Hot-Standby LSP: indicates the hot-standby CR-LSP. - Ordinary LSP: indicates the ordinary backup CR-LSP. - Best-Effort LSP: indicates the best-effort path.
Traffic Switch	Traffic switching status.
Session ID	Session ID of a CR-LSP.
Ingress LSR ID	LSR ID of the ingress.
Egress LSR ID	LSR ID of the egress.
Admin State	Administrative status.
Oper State	Operating status.

Item	Description
Primary LSP State	Status of a primary CR-LSP: - UP: indicates that the primary CR-LSP is successfully set up. - DOWN: indicates that no primary CR-LSP is set up. - GRACEFUL SWITCH: indicates that the primary CR-LSP is being switched to the Modified CR-LSP. - GRACEFUL DELETE: indicates that during the GR process, the primary CR-LSP is deleted.
Main LSP State	Status of the primary CR-LSP: - READY: indicates that the primary CR-LSP is successfully set up. - SETTING UP: indicates that the primary CR-LSP is being set up.
Hot-Standby LSP State	Status of a hot-standby CR-LSP: - UP: indicates that a hot-standby CR-LSP is successfully set up. - DOWN: indicates that no hot-standby CR-LSP is set up. - GRACEFUL SWITCH: indicates that the primary CR-LSP is being switched to the Modified CR-LSP. - GRACEFUL DELETE: indicates that during the GR process, the primary CR-LSP is deleted.
Modify LSP State	Status of a modified CR-LSP: - READY: indicates that the Modified CR-LSP is successfully set up. - SETTING UP: indicates that the Modified CR-LSP is being set up.
Ordinary LSP State	Status of an ordinary backup CR-LSP: - UP: indicates that the ordinary backup CR-LSP is successfully set up. - DOWN: indicates that no ordinary backup CR-LSP is set up. - GRACEFUL SWITCH: indicates that the main CR-LSP is being switched to the modified CR-LSP. - GRACEFUL DELETE: indicates that during the GR process, the main CR-LSP is deleted.

Item	Description
Best-Effort LSP State	Status of a best-effort path: - UP: indicates that the best-effort path is successfully set up. - DOWN: indicates that no best-effort path is set up. - GRACEFUL SWITCH: indicates that the main CR-LSP is being switched to the Modified CR-LSP. - GRACEFUL DELETE: indicates that during the GR process, the main CR-LSP is deleted.
LSP ID	LSP ID.

9.3.44 display mpls te tunnel-interface failed

Function

The **display mpls te tunnel-interface failed** command displays the MPLS TE tunnels that fail to be set up or that are being set up.

Format

display mpls te tunnel-interface failed

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring multiple MPLS TE tunnels, you can use the **display mpls te tunnel-interface failed** command to check whether there are any tunnels that fail to be set up or are still being set up.

Example

Display the MPLS TE tunnels that fail to be set up or that are being set up.

```
<HUAWEI> display mpls te tunnel-interface failed
  Tunnel name       SessionId       State Desc
  ----------------------------------------------------------
  Tunnel1          39              DOWN
```

Table 9-92 Description of the display mpls te tunnel-interface failed command output

Item	Description
Tunnel name	Name of a tunnel interface.
SessionId	Session ID, which is the tunnel ID.
State Desc	Description of the tunnel status: ● UP: The tunnel is in Up state. ● DOWN: The tunnel is in Down state.

9.3.45 display mpls te tunnel-interface last-error

Function

The **display mpls te tunnel-interface last-error** command displays the last errors of a tunnel interface on the local node.

Format

display mpls te tunnel-interface last-error [*tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-name	Displays the last errors of a specified tunnel interface.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mpls te tunnel-interface last-error** command on the ingress to view the error of a local node or the error carried in an RSVP PathErr message sent by a downstream node. The errors can be as follows:

- CSPF computation fails.
- RSVP times out.

- One or more LSPs are deleted during RSVP GR smooth.
- One or more LSPs are deleted during RSVP aging.
- RSVP GR fails to be triggered.

Precautions

The **display mpls te tunnel-interface last-error** command shows the last 20 recorded errors of each TE tunnel and LSP on which the errors occur, including errors about the primary CR-LSP, modified LSP, and backup CR-LSP.

If an RSVP PathErr message sent by a downstream node carries the error information, the ErroInfo field in the command output shows the IP address of the faulty downstream node and the cause of the error. If an error occurs on the ingress, the command output only shows the cause of the error.

Example

Display information about the last errors of Tunnel1.

```
<HUAWEI> display mpls te tunnel-interface last-error Tunnel1
  Tunnel name: Tunnel1


    Error No.  : 1
    LSP Type   : Hot-Standby LSP             LSP ID     : 10.1.1.9:300:32776
    Error Code : 0x3e8                   Occur Time : 2013/01/07 14:42:23+00:00
    Error Info : Link 172.20.1.2 is excluded, IGP: ISIS Process-ID: 1 Area: Level
-1.

    Error No.  : 2
    LSP Type   : Primary LSP                LSP ID     : 10.1.1.9:300:1
    Error Code : 0x5080007                 Occur Time : 2013/01/07 11:13:45+00:00
    Error Info : error node = 172.16.1.1    error lsrid = 10.1.1.9
                 BKGD error SHUTDOWN IF

    Error No.  : 3
    LSP Type   : Primary LSP                LSP ID     : 10.1.1.9:300:1
    Error Code : 0x3e8                   Occur Time : 2013/01/07 09:55:06+00:00
    Error Info : Cannot find the same IGP type and process ID for 10.1.1.9 and 17
10.1.1.2 (inter area scenario).

    Error No.  : 4
    LSP Type   : Primary LSP                LSP ID     : 10.1.1.9:300:1
    Error Code : 0x3e8                   Occur Time : 2013/01/07 09:43:06+00:00
    Error Info : Cspf failed to calculate a path for Tunnel.

    Error No.  : 5
    LSP Type   : Primary LSP                LSP ID     : 10.1.1.9:300:1
    Error Code : 0x3e8                   Occur Time : 2013/01/07 08:43:06+00:00
    Error Info:  error node = 172.16.1.1    error lsrid = 10.1.1.9
    Routing Problem: No route available toward destination.

    Error No.  : 6
    LSP Type   : Primary LSP                LSP ID     : 10.1.1.9:300:1
    Error Code : 0x180001                 Occur Time : 2013/01/07 07:47:19+00:00
    Error Info : error node = 172.16.1.2    error lsrid = 0.0.0.0
                 Routing Problem Bad EXPLICIT_ROUTE object

    Error No.  : 7
    LSP Type   : Primary LSP                LSP ID     : 10.1.1.9:300:1
    Error Code : 0x5080002                 Occur Time : 2013/01/6 20:03:05+00:00
    Error Info : error node = 0.0.0.0     error lsrid = 10.1.1.9
                 BKGD error TEAR ALL LSP
```

Table 9-93 Description of the display mpls te tunnel-interface last-error command output

Item	Description
Tunnel name	Name of an MPLS TE tunnel.
Error No	Number of errors.
LSP Type	Type of LSP: ● Modified LSP: indicates the LSP which is in modified state. ● Primary LSP: indicates the primary LSP. ● Backup LSP: indicates the backup LSP. ● Hot-Standby LSP: indicates the hot-standby LSP.
LSP ID	LSP ID, uniquely identified in the form of Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID.
Error Code	Returned code, which specifies a unique type of error. The value is an integer in hexadecimal notation. For specific error information, see the **Error Info** field.
Occur Time	Time when an error occurred.
Error Info	Error description.
error node	Node on which an error occurs.
error lsrid	LSR ID of the node on which an error occurred.
Routing Problem	Error information carried in a received RSVP PathErr message: No route available toward destination: indicates that no route to the destination address of the tunnel is available. Bad EXPLICIT_ROUTE object: indicates that an unknown EXPLICIT_ROUTE object is received. bad strict node: indicates that a certain node cannot be found on the strict explicit path.
Cspf failed to calculate a path for Tunnel	CSPF computation failure.

9.3.46 display mpls te tunnel-interface lsp-constraint

Function

The **display mpls te tunnel-interface lsp-constraint** command displays information about the CR-LSP attribute template on an MPLS TE tunnel interface.

Format

display mpls te tunnel-interface lsp-constraint [**tunnel** *interface-number*]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies information about the CR-LSP attribute template on a specified MPLS TE tunnel interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information about the CR-LSP attribute template on an MPLS TE tunnel interface, run the **display mpls te tunnel-interface lsp-constraint** command.

Example

Display information about the CR-LSP attribute template on all MPLS TE tunnel interfaces.

```
<HUAWEI> display mpls te tunnel-interface lsp-constraint
    Tunnel Name                      :  Tunnel1
    Primary-lsp-constraint Name      :  p1
    Hotstandby-lsp-constraint Number:  2
    Hotstandby-lsp-constraint Name  :  p1
    Ordinary-lsp-constraint Number  :  2
    Ordinary-lsp-constraint Name     :  p1
```

Table 9-94 Description of the display mpls te tunnel-interface lsp-constraint command output

Item	Description
Tunnel Name	Name of a tunnel.

Item	Description
Primary-lsp-constraint Name	Name of a CR-LSP attribute template.
Hotstandby-lsp-constraint Number	Number of the hot-standby CR-LSP attribute template, which indicates the sequence in which the template is used. To set the number of the hot-standby CR-LSP attribute template, run the **mpls te hotstandby-lsp-constraint** command.
Hotstandby-lsp-constraint Name	Name of a hot-standby CR-LSP attribute template. To set the name of a hot-standby CR-LSP attribute template, run the **mpls te hotstandby-lsp-constraint** command.
Ordinary-lsp-constraint Number	Number of the ordinary CR-LSP attribute template, which indicates the sequence in which the template is used. To set the number of the ordinary CR-LSP attribute template, run the **mpls te ordinary-lsp-constraint** command.
Ordinary-lsp-constraint Name	Name of an ordinary CR-LSP attribute template. To set the name of an ordinary CR-LSP attribute template, run the **mpls te ordinary-lsp-constraint** command.

9.3.47 display mpls te tunnel-interface traffic-state

Function

The **display mpls te tunnel-interface traffic-state** command displays information about the traffic on the tunnel interface of the local LSR.

Format

display mpls te tunnel-interface traffic-state [*tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-name	Specifies a tunnel name.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the traffic protection mode, traffic state, and traffic switchover reasons of a tunnel interface on a local LSR, run the **display mpls te tunnel-interface traffic-state** command.

Example

Display information about the traffic on the tunnel interface of the local LSR.

```
<HUAWEI> display mpls te tunnel-interface traffic-state
 Protect Config: HSB - Hot-Standby,       OBK - Ordinary Backup
                 FRR - Fast Reroute,      BBK - Best-Effort Backup
                 PS  - Protection Switch

 -------------------------------------------------------------------------------
 Tunnel Interface    Protect Config   Traffic State          Switch Reason
 -------------------------------------------------------------------------------
 Tunnel1           OBK             Primary LSP           --
 Tunnel2           HSB             Primary LSP           Signal Fail
```

Table 9-95 Description of the display mpls te tunnel-interface traffic-state command output

Item	Description
Tunnel Interface	Tunnel interface name.
Protect Config	Protection modes. The protection modes are displayed using short names. If two protection modes are performed, both the two protection modes are displayed. ● HSB: indicates the hot standby. ● OBK: indicates ordinary backup. ● BBK: indicates the best-effort path. ● FRR: indicates FRR. ● PS: indicates the tunnel protection group.

Item	Description
Traffic State	Traffic protection state, including the following types: - Hot-Standby LSP: Traffic is switched to the hot-standby LSP. - Primary LSP FRR In Use: Traffic is on the primary LSP that is in the FRR in use state. - Best-Effort LSP: Traffic is on the best-effort LSP. - Ordinary LSP: Traffic is on the ordinary backup LSP. - Protection Tunnel: Traffic is on the protection tunnel. - Primary LSP: Traffic is on the primary LSP, and no switchover is performed.
Switch Reason	Reason why traffic is not on the primary LSP. If the traffic is on the primary LSP, or the traffic is on the primary LSP which is in the FRR in use state, this field is not displayed. If multiple reasons exist, only one reason with the highest priority is displayed. Following are the reasons listed in descending order of priorities: - Manual Command: The user uses a command to enable a switchover. - Signal Fail: The signaling protocol or detection protocol is Down. - Signal Degrade: The detection protocol signal degrades. This field is also displayed when bit errors occur. - Wait To Restore (WTR): The system waits for the WTR period to elapse and then switches traffic back to the primary LSP. - Do Not Revertive: Traffic is not switched back to the primary LSP even if the primary LSP recovers.

9.3.48 display mpls te tunnel

Function

The **display mpls te tunnel** command displays information about an MPLS TE tunnel.

Format

display mpls te tunnel [**destination** *ip-address*] [**lsp-id** *ingress-lsr-id session-id local-lsp-id*] [**lsr-role** { **all** | **egress** | **ingress** | **remote** | **transit** }] [**name** *tunnel-*

name] [{ **incoming-interface** | **interface** | **outgoing-interface** } *interface-type interface-number*] [**verbose**]

display mpls te tunnel { **stale-incoming-interface** | **stale-interface** | **stale-outgoing-interface** } *interface-index* [**verbose**]

Parameters

Parameter	Description	Value
destination *ip-address*	Displays information about an MPLS TE tunnel with a specified destination address.	-
lsp-id	Displays information about an MPLS TE tunnel with a specified LSP ID.	-
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer that ranges from 0 to 65535.
local-lsp-id	Specifies the local LSP ID.	The value is an integer that ranges from 0 to 65535.
lsr-role	Displays information about an MPLS TE tunnel according to the specified role of the local LSR.	-
all	Displays information of all MPLS TE tunnels.	-
egress	Displays information about an MPLS TE tunnel with the local LSR as the egress.	-
ingress	Displays information about an MPLS TE tunnel with the local LSR as the ingress.	-
remote	Displays information about an MPLS TE tunnel with the local LSR as the egress or the transit node.	-

Parameter	Description	Value
transit	Displays information about an MPLS TE tunnel with the local LSR as a transit node.	-
name *tunnel-name*	Displays the MPLS TE tunnel whose name is specified.	*tunnel-name* must be the name of an existing tunnel and its format, including the upper and lower casing, and blank spaces, must be consistent with that of the configuration file. For example, when the tunnel interface in a configuration file is named "interface Tunnel1", the tunnel name to be specified must also be Tunnel1. "tunnel1" or "Tunnel 1" is incorrect.
incoming-interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with a specified incoming interface.	-
interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with an outgoing or incoming interface of the specified type and number.	-
outgoing-interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with a specified outgoing interface.	-
verbose	Displays detailed information.	-
stale-incoming-interface	Displays information about MPLS TE tunnels with a specified incoming interface in the stale state.	-
stale-interface	Displays information about MPLS TE tunnels on an interface in the stale state.	-

Parameter	Description	Value
stale-outgoing-interface	Displays information about MPLS TE tunnels with a specified outgoing interface in the stale state.	-
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer that ranges from 1 to FFFFFFFE.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When **verbose** is configured, the command output varies with the signaling protocol used by the MPLS TE tunnel.

Example

Display information about an MPLS TE tunnel.

```
<HUAWEI> display mpls te tunnel
-------------------------------------------------------------------------------
Ingress LsrId    Destination      LSPID   In/Out Label     R  Tunnel-name
-------------------------------------------------------------------------------
10.1.1.9         10.3.3.9         6       --/1027          I  Tunnel1
```

Table 9-96 Description of the display mpls te tunnel command output

Item	Description
Ingress LsrId	Ingress LSR ID.
Destination	Destination IP address.
LSPID	LSP ID of the ingress.
In/Out Label	Incoming and outgoing labels.
R	LSR role: • I: Ingress • T: Transit • E: Egress
Tunnel-name	Tunnel name.

Display information about the MPLS TE tunnel with the ingress IP address being 10.1.1.9 and the LSP ID being 1.

```
<HUAWEI> display mpls te tunnel lsp-id 10.1.1.9 1 1
------------------------------------------------------------------------------
Ingress LsrId    Destination      LSPID  In/Out Label     R  Tunnel-name
------------------------------------------------------------------------------
10.1.1.9         10.2.2.9         1      --/3             I  Tunnel1
```

Display detailed information about an MPLS TE tunnel.

```
<HUAWEI> display mpls te tunnel verbose
  No                       :  1
  Tunnel-Name              :  LSRAtoLSRC
  Tunnel Interface Name    :  Tunnel1
  TunnelIndex              :  0            LSP Index          :  1024
  Session ID               :  100          LSP ID             :  1
  LSR Role                 :  Ingress      LSP Type           :  Primary
  Ingress LSR ID           :  10.1.1.1
  Egress LSR ID            :  10.2.2.2
  In-Interface             :  -
  Out-Interface            :  Vlanif10
  Sign-Protocol            :  Static CR    Resv Style         :
  IncludeAnyAff            :  0x0          ExcludeAnyAff      :  0x0
  IncludeAllAff            :  0x0
  LspConstraint            :  1
  ER-Hop Table Index       :  -            AR-Hop Table Index:  -
  C-Hop Table Index        :  -
  PrevTunnelIndexInSession:  -            NextTunnelIndexInSession:  -
  PSB Handle               :  0
  Created Time             :  2013/01/29 18:21:36+00:00
  RSVP LSP Type            :  -
  --------------------------------
          DS-TE Information
  --------------------------------
  Bandwidth Reserved Flag :  Unreserved
  CT0 Bandwidth(Kbit/sec) :  0           CT1 Bandwidth(Kbit/sec):  0
  CT2 Bandwidth(Kbit/sec) :  0           CT3 Bandwidth(Kbit/sec):  0
  CT4 Bandwidth(Kbit/sec) :  0           CT5 Bandwidth(Kbit/sec):  0
  CT6 Bandwidth(Kbit/sec) :  0           CT7 Bandwidth(Kbit/sec):  0
  Setup-Priority           :  7          Hold-Priority          :  7
  --------------------------------
           FRR Information
  --------------------------------
  Primary LSP Info
  TE Attribute Flag        :  0x63       Protected Flag     : 0x0
  Bypass In Use            :  Not Exists
  Bypass Tunnel Id         :  -
  BypassTunnel             :  -
  Bypass LSP ID            :  -          FrrNextHop         :  -
  ReferAutoBypassHandle    :  -
  FrrPrevTunnelTableIndex :  -           FrrNextTunnelTableIndex:  -
  Bypass Attribute(Not configured)
  Setup Priority           :  -          Hold Priority      :  -
  HopLimit                 :  -          Bandwidth          :  -
  IncludeAnyGroup          :  -          ExcludeAnyGroup    :  -
  IncludeAllGroup          :  -
  Bypass Unbound Bandwidth Info(Kbit/sec)
  CT0 Unbound Bandwidth    :  -          CT1 Unbound Bandwidth:  -
  CT2 Unbound Bandwidth    :  -          CT3 Unbound Bandwidth:  -
  CT4 Unbound Bandwidth    :  -          CT5 Unbound Bandwidth:  -
  CT6 Unbound Bandwidth    :  -          CT7 Unbound Bandwidth:  -
  --------------------------------
           BFD Information
  --------------------------------
  NextSessionTunnelIndex  :  -           PrevSessionTunnelIndex:  -
  NextLspId                :  -          PrevLspId          :  -
```

Table 9-97 Description of the display mpls te tunnel verbose command output

Item	Description
No	Number of an MPLS TE tunnel.
Tunnel-Name	Name of an MPLS TE tunnel.
Tunnel Interface Name	Interface name of an MPLS TE tunnel.
TunnelIndex	Index of an MPLS TE tunnel.
LSP Index	Index of an LSP.
Session ID	Session ID, which is the tunnel ID.
LSP ID	LSP ID.
LSR Role	Role of the LSR: ● Ingress: indicates the node is the ingress of the tunnel. ● Egress: indicates the node is the egress of the tunnel. ● Transit: indicates the node is the transit of the tunnel.
LSP Type	Type of an LSP: ● Primary: indicates the primary CR-LSP. ● Hot-Standby: indicates the hot-standby CR-LSP. ● Ordinary: indicates the ordinary backup CR-LSP. ● Best-Effort: indicates the best-effort path.
Ingress LSR ID	LSR ID of the ingress.
Egress LSR ID	LSR ID of the egress.
In-Interface	Incoming interface of the LSP on the local node.
Out-Interface	Outgoing interface of the LSP on the local node.
Sign-Protocol	Tunnel protocol: ● Static: indicates Static LSP. ● Static CR: indicates Static CR-LSP. ● RSVP TE: uses RSVP TE signaling.

Item	Description
Resv Style	Style of resource reservation. For a static CR-LSP, no resource reservation style is displayed. For an RSVP-TE tunnel, shared explicit (SE) or fixed filter (FF) is displayed.
IncludeAnyAff	Valid affinity property. The default value is 0x0.
ExcludeAnyAff	Invalid affinity property. The default value is 0x0.
IncludeAllAff	The affinity property needs to be included. The default value is 0x0.
LspConstraint	Sequence number of the constraint used by an LSP.
ER-Hop Table Index	Index of an explicit routing table.
AR-Hop Table Index	Index of the actual explicit routing table.
C-Hop Table Index	Routing table index that is calculated by CSPF.
PrevTunnelIndexInSession	Index of the previous tunnel entry in the same session.
NextTunnelIndexInSession	Index of the next tunnel entry in the same session.
PSB Handle	Handle of the PSB.
Created Time	Amount of time an MPLS TE tunnel is created for.
RSVP LSP Type	LSP type. ● Primary: indicates that the LSP is a primary LSP. ● Hot-Standby: indicates that the LSP is a hot-standby LSP. **NOTE** This field is displayed as "-" because the device does not support the error code switching function.
Bandwidth Reserved Flag	Bandwidth reservation flag: ● Unreserved: indicates that no bandwidth is reserved for CTs. ● Reserved: indicates that the bandwidth is reserved for one or multiple CTs.
CT0 Bandwidth(Kbit/sec) - CT7 Bandwidth(Kbit/sec)	Value of the bandwidth that is reserved for CT0 to CT7.

Item	Description
Setup-Priority	Setup priority of an MPLS TE tunnel.
Hold-Priority	Holding priority of an MPLS TE tunnel.
Primary LSP Info	Information about the primary LSP.
TE Attribute Flag	Flag of the TE tunnel attribute.
Protected Flag	Flag of the primary tunnel of the protection group.
Bypass In Use	LSP ID of the bypass tunnel. "Not Exists" indicates that the primary tunnel is not bound to a bypass tunnel.
Bypass Tunnel Id	Tunnel ID of the bypass tunnel.
BypassTunnel	Name of the bypass tunnel.
Bypass LSP ID	LSP ID of the bypass tunnel.
FrrNextHop	Next hop of the redirect route.
ReferAutoBypassHandle	Handle of the automatic bypass tunnel.
FrrPrevTunnelTableIndex	Index value of the previous tunnel entry in FRR.
FrrNextTunnelTableIndex	Index value of the next tunnel entry in FRR.
Bypass Attribute	Attributes of a bypass tunnel. "(Not configured)" indicates that no such attribute is configured and the bypass tunnel inherits the attributes of the primary tunnel.
Setup Priority	Setup priority of a bypass tunnel.
Hold Priority	Holding priority of a bypass tunnel.
HopLimit	Maximum number of hops along a bypass tunnel.
Bandwidth	Bandwidth of a bypass tunnel.
IncludeAnyGroup	Valid affinity property of a bypass tunnel.
ExcludeAnyGroup	Invalid affinity property of a bypass tunnel.
IncludeAllGroup	The affinity property of a bypass tunnel needs to be included.
Bypass Unbound Bandwidth Info	Information about the bandwidth that is not bound to a bypass tunnel.

Item	Description
CT0 Unbound Bandwidth - CT7 Unbound Bandwidth	Bandwidth that is able to be reserved, but not for CT0 to CT7.
NextSessionTunnelIndex	Next index of a bypass tunnel entry.
PrevSessionTunnelIndex	Previous index of a bypass tunnel entry.
NextLspId	Value of the next bypass LSP ID.
PrevLspId	Value of the previous bypass LSP ID.

9.3.49 display mpls te tunnel c-hop

Function

The **display mpls te tunnel c-hop** command displays the path computation results of tunnels.

Format

display mpls te tunnel c-hop [*tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*]

Parameters

Parameter	Description	Value
tunnel-name	Displays the path computation result of the specified tunnel.	The value is an existing tunnel name.
lsp-id	Displays the path computation result of the specified tunnel based on the LSP ID.	-
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
session-id	Specifies the session ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Tunnels are established based on path computation results. When a tunnel cannot be established successfully, run the **display mpls te tunnel c-hop** command to view the path computation results for locating causes on a per-hop basis.

Example

Display the path computation result of a tunnel.

```
<HUAWEI> display mpls te tunnel c-hop
 Tunnel Interface Name : Tunnel1
 Lsp ID : 10.2.2.2 :1 :10958
 CHop Information:
  Hop 0   10.3.0.2
  Hop 1   10.3.0.3
```

Display the path computation result of the specified tunnel based on the LSP ID.

```
<HUAWEI> display mpls te tunnel c-hop lsp-id 10.2.2.2 1 10958
 Tunnel Interface Name : Tunnel1
 Lsp ID : 10.2.2.2 :1 :10958
 CHop Information:
  Hop 0   10.3.0.2
  Hop 1   10.3.0.3
```

Table 9-98 Description of the display mpls te tunnel c-hop command output

Item	Description
Tunnel Interface Name	Interface name of a tunnel.
Lsp ID	LSP ID of a tunnel, in the Ingress-Lsr-Id:Tunnel-Id:LSP-Id format.
CHop Information	Information about CSPF path computation. **Hop** specifies the IPv4 address of each hop in the path computation result.

9.3.50 display mpls te tunnel path

Function

The **display mpls te tunnel path** command displays the path of an MPLS TE tunnel.

Format

display mpls te tunnel path [[[**tunnel-name**] *tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*] | **fast-reroute** { **local-protection-available** | **local-protection-inuse** } | **lsr-role** { **ingress** | **transit** | **egress** }]

display mpls te tunnel path expanded tunnel-name *tunnel-name* [**lsp-id** *ingress-lsr-id session-id lsp-id*]

display mpls te tunnel path expanded lsp-id *ingress-lsr-id session-id lsp-id*

Parameters

Parameter	Description	Value
tunnel-name *tunnel-name*	Specifies the name of an MPLS TE tunnel. If the **mpls te signalled tunnel-name** command has been used to configure a tunnel name, this specified name is used.	The value is an existing tunnel name.
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.
fast-reroute local-protection-available	Specifies the available path for local protection of FRR.	-
fast-reroute local-protection-inuse	Specifies the path in use for local protection of FRR.	-
lsr-role { **ingress** | **transit** | **egress** }	Indicates the role of an LSR. ● **ingress**: indicates the ingress LSR. ● **transit**: indicates the transit LSR. ● **egress**: indicates the egress LSR.	-
expanded	Displays the expanded LSP path information by completing the RRO information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display mpls te tunnel path** command displays information about the path of an MPLS TE tunnel.

If no tunnel name is specified, information about all MPLS TE tunnels' path attributes is displayed.

When a Huawei device is interconnected with a non-Huawei device and the RRO information carried in the packet sent by the non-Huawei device is incomplete, the RRO information can be complemented using the **display mpls te tunnel path expanded** command on the Huawei device to display the information about the entire LSP path.

Precautions

The system can record and display the paths only after the **mpls te record-route** command is configured.

Example

Display information about path attributes of all MPLS TE tunnels.

```
<HUAWEI> display mpls te tunnel path
Tunnel Interface Name : Tunnel1
 Lsp ID : 10.1.1.9 :100 :34
 Hop Information
  Hop 0   172.16.1.1 Local-Protection available | node
  Hop 1   172.16.1.2  Label 1055
  Hop 2   10.2.2.9  Label 1055
  Hop 3   172.20.1.1 Local-Protection available
  Hop 4   172.20.1.2  Label 1063
  Hop 5   10.3.3.9  Label 1063
  Hop 6   172.30.1.1
  Hop 7   172.30.1.2  Label 3
  Hop 8   10.4.4.9  Label 3
```

Display path attributes of the MPLS TE tunnel with the ingress IP address being 10.1.1.9, the session ID being 300, and the LSP ID being 4.

```
<HUAWEI> display mpls te tunnel path lsp-id 10.1.1.9 300 4
 Tunnel Interface Name : Tunnel1
 Lsp ID : 10.1.1.9 :300 :4
 Hop Information
  Hop 0   172.16.1.1
  Hop 1   172.16.1.2  Label 1043
  Hop 2   10.2.2.9  Label 1043
  Hop 3   172.20.1.1
  Hop 4   172.20.1.2  Label 4
  Hop 5   10.3.3.9  Label 4
```

Display path attributes of a tunnel named **LSRAtoLSRC**.

```
<HUAWEI> display mpls te tunnel path tunnel-name LSRAtoLSRC
 Tunnel Interface Name : LSRAtoLSRC
 Lsp ID : 10.1.1.9 :1 :2
 Hop Information
  Hop 0   10.11.1.1  Local-Protection in use
  Hop 1   10.11.1.2  Label 3
  Hop 2   10.2.2.9
```

Display path attributes of a tunnel named **A2** using the command which expanded the information about the path.

```
<HUAWEI> display mpls te tunnel path expanded tunnel-name A2
 Tunnel Interface Name : A2
 Lsp ID : 10.1.1.9 :300 :4
```

```
Hop Information
 Hop 0   10.1.1.9   Local-Protection available | bandwidth
 Hop 1   172.16.1.1
 Hop 2   172.16.1.2  Label 1042
 Hop 3   10.2.2.9  Label 1042
 Hop 4   172.20.1.1
 Hop 5   172.20.1.2  Label 3
 Hop 6   10.3.3.9  Label 3
```

Table 9-99 Description of the display mpls te tunnel path command output

Item	Description
Tunnel Interface Name	Name of a tunnel interface.
Lsp ID	LSP ID on the ingress.
Hop Information	Number, IP address, and label of each hop.
Local-Protection available	Link protection provided by the bypass tunnel.
Local-Protection available | bandwidth	Bandwidth protection provided by the bypass tunnel.
Local-Protection available | node	Node protection provided by the bypass tunnel.
Local-Protection in use	The bypass tunnel in use.

9.3.51 display mpls te tunnel statistics

Function

The **display mpls te tunnel statistics** command displays the number and status of MPLS TE tunnels.

Format

display mpls te tunnel statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the number and status of MPLS TE tunnels, run the **display mpls te tunnel statistics** command.

Example

Display the number and status of MPLS TE tunnels.

```
<HUAWEI> display mpls te tunnel statistics
Ingress:    84 Tunnels     83 Up,     83 CRLSPs Up
            0 Modified,    0 In-Progress,    1 Failed
Transit:     2 Up
Egress :     3 Up
```

Table 9-100 Description of the display mpls te tunnel statistics command output

Item	Description
Ingress	Number and status of MPLS TE tunnels on the local LSR functioning as the ingress node: ● Tunnel: indicates the number of primary tunnels. ● Up: indicates the number of MPLS TE tunnels in the Up state. ● CRLSPs Up: indicates the number of CR-LSPs in the Up state. ● Modified: indicates the number of tunnels in the reestablishing state. **NOTE** The possible causes that an MPLS TE tunnel is in the Modified state are as follows: Configurations of the MPLS TE tunnel are manually modified. The MPLS TE tunnel is being re-optimized. The MPLS TE tunnel is in the FRR inuse state. The MPLS TE tunnel is in the Backup state. ● In-Progress: indicates the number of MPLS TE tunnels in the establishing process. At the moment, these tunnels do not go Up. ● Failed: indicates the number of MPLS TE tunnels in the Down state.
Transit	Number of MPLS TE tunnels, which are in the Up state, on the local LSR functioning as a transit node.
Egress	Number of MPLS TE tunnels, which are in the Up state, on the local LSR functioning as the egress node.

9.3.52 display ospf mpls-te

Function

The **display ospf mpls-te** command displays information about TE LSAs in an LSDB.

Format

display ospf [*process-id*] **mpls-te** [**area** *area-id*] [**self-originated**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID.	The value ranges from 1 to 65535.
area *area-id*	Displays information about the area with a specified ID. The value can be a decimal integer or in the IP address format.	The integer value ranges from 0 to 4294967295.
self-originated	Displays information about the self originated TE LSAs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view information about LSAs of a specific process or area by specifying parameters.

Example

Display information about all TE LSAs in the LSDB.

```
<HUAWEI> display ospf mpls-te
        OSPF Process 1 with Router ID 172.16.1.2

 Area ID                  : 0.0.0.0

 Traffic Engineering LSAs of the database

 ------------------------------------------------

 LSA [ 1 ]

 ------------------------------------------------
   Lsa  Type               : Opq-Area
```

```
  Opaque Type             : 1
  Opaque Id               : 2
  Advertising Router Id    : 172.16.1.2
  Lsa  age                : 36
  Length                  : 200
  Lsa  Options            : E
  LS Seq Number           : 80000001
  CheckSum                : 7130

  Link Type               : MultiAccess
  Link ID                 : 172.20.1.1
  Local Interface Address  : 172.20.1.1
  Remote Interface Address : 0.0.0.0
  TE Metric               : 1
  Maximum Bandwidth       : 0 bytes/sec
  Maximum Reservable BW    : 0 bytes/sec
  Admin Group             : 0X0

 Global Pool              :
  Unreserved BW [ 0] =   0  bytes/sec
  Unreserved BW [ 1] =   0  bytes/sec
  Unreserved BW [ 2] =   0  bytes/sec
  Unreserved BW [ 3] =   0  bytes/sec
  Unreserved BW [ 4] =   0  bytes/sec
  Unreserved BW [ 5] =   0  bytes/sec
  Unreserved BW [ 6] =   0  bytes/sec
  Unreserved BW [ 7] =   0  bytes/sec
  Sub Pool                :
  Unreserved BW [ 8] =   0  bytes/sec
  Unreserved BW [ 9] =   0  bytes/sec
  Unreserved BW [10] =   0  bytes/sec
  Unreserved BW [11] =   0  bytes/sec
  Unreserved BW [12] =   0  bytes/sec
  Unreserved BW [13] =   0  bytes/sec
  Unreserved BW [14] =   0  bytes/sec
  Unreserved BW [15] =   0  bytes/sec

  DS-TE Mode: Non-Standard IETF Mode

  Bandwidth Constraint Model: RDM

 Bandwidth Constraints

          BC [ 0] =   0  bytes/sec           BC [ 1] =   0  bytes/sec

 Local OverBooking Multipliers

          LOM [ 0] =   1              LOM [ 1] =   1


------------------------------------------------

 LSA [ 2 ]

 ------------------------------------------------
  Lsa  Type               : Opq-Area
  Opaque Type             : 1
  Opaque Id               : 1
  Advertising Router Id    : 172.16.1.2
  Lsa  age                : 1681
  Length                  : 200
  Lsa  Options            : E
  LS Seq Number           : 80000033
  CheckSum                : 77F4

  Link Type               : MultiAccess
  Link ID                 : 172.17.1.1
  Local Interface Address  : 172.17.1.1
  Remote Interface Address : 0.0.0.0
```

```
  TE Metric                : 1
  Maximum Bandwidth        : 0 bytes/sec
  Maximum Reservable BW    : 0 bytes/sec
  Admin Group              : 0X0

Global Pool                :
  Unreserved BW [ 0] =   0  bytes/sec
  Unreserved BW [ 1] =   0  bytes/sec
  Unreserved BW [ 2] =   0  bytes/sec
  Unreserved BW [ 3] =   0  bytes/sec
  Unreserved BW [ 4] =   0  bytes/sec
  Unreserved BW [ 5] =   0  bytes/sec
  Unreserved BW [ 6] =   0  bytes/sec
  Unreserved BW [ 7] =   0  bytes/sec
  Sub Pool                 :
  Unreserved BW [ 8] =   0  bytes/sec
  Unreserved BW [ 9] =   0  bytes/sec
  Unreserved BW [10] =   0  bytes/sec
  Unreserved BW [11] =   0  bytes/sec
  Unreserved BW [12] =   0  bytes/sec
  Unreserved BW [13] =   0  bytes/sec
  Unreserved BW [14] =   0  bytes/sec
  Unreserved BW [15] =   0  bytes/sec

  DS-TE Mode: Non-Standard IETF Mode

  Bandwidth Constraint Model: RDM

 Bandwidth Constraints

            BC [ 0] =   0  bytes/sec             BC [ 1] =   0  bytes/sec

 Local OverBooking Multipliers

           LOM [ 0] =   1                  LOM [ 1] =   1
...
```

Table 9-101 Description of the display ospf mpls-te command output

Item	Description
OSPF Process 1 with Router ID 172.16.1.2	OSPF process 1 with Router ID being 172.16.1.2.
Area ID	ID of the OSPF area enabled with TE.
Traffic Engineering LSAs of the database	TE LSAs in an LSDB.
Lsa Type	LSA type: - Opq-Link: indicates Type 9 LSAs that can only be spread on a specified interface. - Opq-Area: indicates Type 10 LSAs that can only be spread within a specified area. - Opq-As: indicates Type 11 LSAs that can be spread the same as Type 5 LSAs in the entire AS, except for the stub and NSSA areas.

Item	Description
Opaque Type	Application type of LSAs. For example, when LSAs are applied to traffic engineering, the value of the LSA type is 1. When LSAs are applied to the OSPF graceful restart, the value of the LSA type is 3.
Opaque Id	LSAs that are applied to the same application type. Opaque type and Opaque ID in an LSA header together specify the link status ID.
Advertising Router Id	Device that generates the LSA.
Lsa age	Aging time of the LSA. It is in the header of Opaque LSA, in seconds.
Length	Length of the Opaque LSA, including the LSA header, in bytes.
Lsa Options	LSA options: ● E: floods AS-external-LSAs. ● MC: forwards IP multicast packets. ● N/P: processes Type 7 LSAs. ● DC: processes required links.
LS Seq Number	LSA sequence, according to which other devices can identify the latest LSAs.
CheckSum	Checksum of LSA fields except for the LS age field.
Link Type	Link type: ● Point-to-point ● Point-to-multi-point (P2MP) ● Broadcast
Link ID	Link ID in the IP address format: ● Point-to-point: indicates the router ID of an OSPF neighbor. ● P2MP or broadcast: indicates the IP address of the DR interface.
Local Interface Address	IP address of the local interface.
Remote Interface Address	IP address of the peer interface: ● Point-to-point: indicates that the IP address of the peer is used. ● P2MP or broadcast: indicates that 0.0.0.0 is used or the IP address is omitted.
TE Metric	TE metric.

Item	Description
Maximum Bandwidth	Maximum bandwidth.
Maximum Reservable BW	Maximum capacity of reserved bandwidth.
Admin Group	Administration group.
Global Pool	Global address pool.
Unreserved BW [0] to [7]	Available bandwidth of eight levels.
Sub Pool	Sub-address pool. It is only applied to DS-TE LSAs.
Unreserved BW [8] to [15]	Available bandwidth of eight levels in the sub-address pool.
DS-TE Mode	DS-TE mode: ● Standard IETF mode ● Non-standard IETF mode
Bandwidth Constraint Model	Bandwidth Constraints model of LSAs: ● RDM ● MAM ● Extended-MAM
Bandwidth Constraints	Bandwidth constraints, which are only applied to DS-TE LSAs.
BC [0] - [7]	Eight bandwidth constraints, which are only applied to DS-TE LSAs.
Local OverBooking Multipliers	Local overbooking multiplier.
LOM [0] LOM [1]	Local overbooking multipliers for BC0 or BC1. It is applied only to DS-TE LSAs.

9.3.53 display ospf traffic-adjustment

Function

The **display ospf traffic-adjustment** command displays OSPF process-specific tunnel information relevant to traffic adjustment (through IGP shortcut and forwarding adjacency).

Format

display ospf [*process-id*] **traffic-adjustment**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID. If you do not specify a process ID, information about all OSPF processes is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you want to look up the OSPF process-specific tunnel information relevant to traffic adjustment, you can run this command.

Example

Display tunnel information, which is relevant to traffic adjustment, of OSPF process 100.

```
<HUAWEI> display ospf 100 traffic-adjustment

         OSPF Process 100 with Router ID 1.1.1.9
                 Traffic adjustment

 Interface: 1.1.1.9 (Tunnel1)
 Type: Forwarding Adjacency
 Neighbor ID: 3.3.3.9           Cost: 1
 Configuration:
  Neighbor ip address: 3.3.3.9
  Cost     :1
  Cost Type: Absolute
  Hold Time: 0
```

Table 9-102 Description of the display ospf traffic-adjustment command output

Item	Description
Interface	Name and IP address of a tunnel interface
Type	Whether a tunnel is applied to IGP shortcut or forwarding adjacency
Neighbor ID	Router ID of a neighbor device
Cost	Actual cost
Neighbor ip address	IP address of a neighbor device
Cost	Configured cost

Item	Description
Cost Type	Cost type: ● Relative: Relative cost ● Absolute: Absolute cost
Hold Time	Time elapsed since the tunnel has been created

9.3.54 enable traffic-adjustment

Function

The **enable traffic-adjustment** command enables the IGP shortcut function.

The **enable traffic-adjustment advertise** command enables the forwarding adjacency function.

The **undo enable traffic-adjustment** command disables the IGP shortcut function.

The **undo enable traffic-adjustment advertise** command disables the forwarding adjacency function.

By default, the IGP shortcut function and the forwarding adjacency function are disabled.

Format

enable traffic-adjustment [**advertise**]

undo enable traffic-adjustment [**advertise**]

Parameters

None.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

After the configuration of a command, all TE tunnels are involved in the SPF calculation and flooding.

Example

Enable the forwarding adjacency function of the OSPF process.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] enable traffic-adjustment advertise
```

9.3.55 explicit-path

Function

The **explicit-path** command configures an explicit path of a tunnel.

The **undo explicit-path** command deletes a configured explicit path.

By default, no explicit path of a tunnel is configured.

Format

explicit-path *path-name*

undo explicit-path *path-name*

Parameters

Parameter	Description	Value
path-name	Indicates the name of an explicit path.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You must enable MPLS TE before running the **explicit-path** command.

The addresses of the hops along the explicit path must be different, without loops. If a loop exists, CSPF detects the loop and fails to compute a path.

If the explicit path is in use, the **undo explicit-path** command cannot be run to delete the explicit path.

Example

Create an explicit path named path1.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] explicit-path path1
[HUAWEI-explicit-path-path1] quit
```

9.3.56 explicit-path (LSP attribute view)

Function

The **explicit-path** command configures an explicit path in a CR-LSP attribute template.

The **undo explicit-path** command deletes an explicit path from a CR-LSP attribute template.

No explicit path is configured in a CR-LSP attribute template by default.

Format

explicit-path *path-name*

undo explicit-path

Parameters

Parameter	Description	Value
path-name	Specifies the name of an explicit path.	The value is an existing explicit path name.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

To specify an explicit path in a CR-LSP attribute template, you must configure the explicit path in the system view and ensure that its hop list is not null.

Example

Configure an explicit path in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] explicit-path path-name
```

9.3.57 fast-reroute

Function

The **fast-reroute** command enables the Fast Reroute (FRR) function in a CR-LSP attribute template.

The **undo fast-reroute** command disables the FRR function in the CR-LSP attribute template.

The FRR function is disabled in the CR-LSP attribute template by default.

Format

fast-reroute [**bandwidth**]

undo fast-reroute

Parameters

Parameter	Description	Value
bandwidth	Indicates that bandwidth protection is needed during fast rerouting.	-

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

After the FRR function is enabled, the route storing function is automatically enabled. After the FRR function is disabled, the bypass tunnel configurations are automatically deleted.

Example

Enable the FRR function in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] fast-reroute
```

9.3.58 hop-limit

Function

The **hop-limit** command sets the hop limit in a CR-LSP attribute template.

The **undo hop-limit** command restores the default hop limit from a CR-LSP attribute template.

By default, the hop limit in a CR-LSP attribute template is 32.

Format

hop-limit *hop-limit*

undo hop-limit

Parameters

Parameter	Description	Value
hop-limit	Specifies the value of the hop limit.	The value is an integer that ranges from 1 to 32. The hop limit is 32 by default.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the maximum number of hops supported by each CR-LSP established using the CR-LSP attribute template, run the **hop-limit** command in the LSP attribute view. This hop limit restricts CR-LSP path selection.

Prerequisites

A CR-LSP attribute template has been created and the LSP attribute view has been entered using the **lsp-attribute** command.

Example

Set the maximum number of hops in the CR-LSP attribute template to 20.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] hop-limit 20
```

9.3.59 hotstandby-switch

Function

The **hotstandby-switch force** command forcibly switches traffic from a primary CR-LSP to a hot-standby CR-LSP.

The **hotstandby-switch clear** command disables the forcible switchover function and switches traffic from a hot-standby CR-LSP to the primary CR-LSP.

Format

hotstandby-switch { **force** | **clear** }

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a hot-standby CR-LSP is established and a primary CR-LSP needs to be adjusted, run the **hotstandby-switch force** command to switch traffic forcibly to the hot-standby CR-LSP. After the primary CR-LSP has been adjusted, run the **hotstandby-switch clear** command to disable the forcible switchover function and switch traffic back to the primary CR-LSP.

Precautions

A hot-standby CR-LSP must have been established before the **hotstandby-switch force** command is used. If this command is run but no hot-standby CR-LSP is established, traffic will be dropped.

Example

Forcibly switch traffic from a primary CR-LSP to a hot-standby CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] hotstandby-switch force
```

9.3.60 list hop

Function

The **list hop** command displays information about nodes along an explicit path of an MPLS TE tunnel.

Format

list hop [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a node.	The value is in dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

To view the information about nodes along an explicit path of an MPLS TE tunnel, run the **list hop** command.

Example

Display information about nodes along an explicit path of an MPLS TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] explicit-path path1
[HUAWEI-explicit-path-path1] list hop
 Path Name : path1      Path Status : Enabled
 1      10.1.1.1          Strict      Include
 2      10.2.2.2          Strict      Exclude
 3      10.3.3.3          Loose       Include             Outgoing
 4      10.4.4.4          Strict      Include             Incoming
```

9.3.61 lsp-attribute

Function

The **lsp-attribute** command creates a CR-LSP attribute template and displays the LSP attribute view.

The **undo lsp-attribute** command deletes a specified CR-LSP attribute template.

By default, no CR-LSP attribute template is created.

Format

lsp-attribute *lsp-attribute-name*

undo lsp-attribute *lsp-attribute-name*

Parameters

Parameter	Description	Value
lsp-attribute-name	Specifies the name of the CR-LSP attribute template.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To simplify configurations of TE tunnel interfaces and enhance their flexibility, you can reference CR-LSP attribute templates to set up TE tunnels. The CR-LSP attribute template contains the attributes relevant to a TE tunnel, including the bandwidth, affinity property, explicit path, hop limit, route storing, setup priority, holding priority, FRR, and bypass tunnel attribute.

Prerequisites

Before configuring a CR-LSP attribute template, you must enable the MPLS TE function in the system view.

Precautions

When deleting a CR-LSP attribute template, ensure that the CR-LSP attribute template is not referenced by any tunnel interface.

Example

Create the CR-LSP attribute template named **lsp-attribute-name**.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name]
```

9.3.62 modify hop

Function

The **modify hop** command modifies the IP address of a hop on an explicit path.

Format

modify hop *ip-address1 ip-address2* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**]

Parameters

Parameter	Description	Value
ip-address1 ip-address2	Changes *ip-address1* to *ip-address2* on an explicit path.	The value is in dotted decimal notation.

Parameter	Description	Value
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Indicates that the explicit path must pass through the modified node on the explicit path. ● **strict**: indicates the strict explicit path. The modified node must be directly connected to the previous node. ● **loose**: indicates the loose explicit path. The modified node can be not directly connected to the previous node. ● **incoming**: indicates that the *ip-address2* is the IP address of an inbound interface of the modified node. ● **outgoing**: indicates that the *ip-address2* is the IP address of an outbound interface of the modified node.	By default, a node is added to an explicit path in **include strict** mode.
exclude	Indicates that the LSP set up along an explicit path excludes the modified link or node.	-

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Prerequisites

A next-hop IP address has been configured using the **next hop** command.

Follow-up Procedure

Run the **display explicit-path** command to view information about the explicit path.

Precautions

A node can be modified on an explicit path using the **modify hop** command only when the following conditions are met:

- *ip-address2* must not be a next-hop IP address of an existing node on the explicit path.
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

Modify IP address of a node along the explicit path from 10.1.1.9 to 10.2.2.9.

```
<HUAWEI> system-view
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] next hop 10.1.1.9
[HUAWEI-explicit-path-p1] modify hop 10.1.1.9 10.2.2.9
```

9.3.63 mpls-te enable

Function

The **mpls-te enable** command enables the MPLS TE feature in the current OSPF area.

The **undo mpls-te** command disables the MPLS TE feature in the current OSPF area.

OSPF area does not support MPLS TE by default.

Format

mpls-te enable [**standard-complying**]

undo mpls-te

Parameters

Parameter	Description	Value
standard-complying	Accepts only LSAs in the standard format. This means that an LSA is rejected if it has more than one Top level TLV.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

MPLS TE can only be enabled in an OSPF area after the OSPF process is enabled with the Opaque LSA function.

Example

Enable TE in OSPF area 1.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] opaque-capability enable
[HUAWEI-ospf-100] area 1
[HUAWEI-ospf-100-area-0.0.0.1] mpls-te enable
```

9.3.64 mpls autobypass-tunnel-number threshold-alarm

Function

The **mpls autobypass-tunnel-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for Auto bypass tunnel interfaces.

The **undo mpls autobypass-tunnel-number threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%.

Format

mpls autobypass-tunnel-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls autobypass-tunnel-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for the proportion of configured Auto bypass tunnel interfaces to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for the proportion of configured Auto bypass tunnel interfaces to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of Auto bypass tunnel interfaces reaches a specified upper limit, new Auto bypass tunnel interfaces cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of configured Auto bypass tunnel interfaces to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls autobypass-tunnel-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of configured Auto bypass tunnel interfaces to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of configured Auto bypass tunnel interfaces to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls autobypass-tunnel-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls autobypass-tunnel-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for Auto bypass tunnel interfaces.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls autobypass-tunnel-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.65 mpls bfd-te-number threshold-alarm

Function

The **mpls bfd-te-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for TE.

The **undo mpls bfd-te-number threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%.

Format

mpls bfd-te-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls bfd-te-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Sets the upper alarm threshold for the proportion of established dynamic BFD sessions for TE to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Sets the lower alarm threshold for the proportion of established dynamic BFD sessions for TE to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of dynamic BFD sessions for TE reaches a specified upper limit, new dynamic BFD sessions for TE cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of established dynamic BFD sessions for TE to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls bfd-te-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of established dynamic BFD sessions for TE to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of established dynamic BFD sessions for TE to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls bfd-te-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls bfd-te-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for dynamic BFD sessions for TE.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls bfd-te-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.66 mpls cspf threshold-alarm

Function

The **mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command sets the upper and lower alarm thresholds for the proportion of the number of existing CSPF resources of a specified type to the maximum number of CSPF resources that a device supports. The CSPF resources can be CSPF links, nodes, network LSAs, or SRLGs.

The **undo mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command restores the default the upper and lower alarm thresholds.

By default, the upper threshold for alarms is 80 (percent), and the lower threshold for clear alarms is 75 (percent).

Format

mpls { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm**

Parameters

Parameter	Description	Value
cspf-link-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF links to the maximum number of CSPF links that a device supports.	-
cspf-node-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF nodes to the maximum number of CSPF nodes that a device supports.	-
cspf-nlsa-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF network LSAs to the maximum number of CSPF network LSAs that a device supports.	-
cspf-srlg-number	Indicates the upper and lower alarm thresholds of the proportion of the existing CSPF SRLGs to the maximum number of CSPF SRLGs that a device supports.	-
upper-limit *upper-limit-value*	Specifies a percent for the upper alarm threshold.	The value is a percent integer ranging from 1 to 100. Set the value less than or equal to 95. Default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies a percent for the lower alarm threshold.	The value is a percent integer ranging from 1 to 100. *lower-limit-value* must be less than *upper-limit-value*. Default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the following example, the alarm thresholds for CSPF links are used. If the number of CSPF links reaches the maximum number of CSPF links that a device supports, new CSPF links fail to be established. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of configured CSPF links to all supported ones reaches a specified upper alarm threshold. To enable this function, run the **mpls cspf-link-number threshold-alarm** command to set the upper and lower alarm thresholds with the following parameters configured:

- *upper-limit-value*: An alarm is generated if the proportion of the number of existing CSPF links to the maximum number reaches *upper-limit-value*.
- *lower-limit-value*: The alarm is cleared if the proportion of the number of existing CSPF links to the maximum number falls to *lower-limit-value*.

Precautions

- If the **mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- The **mpls** { **cspf-link-number** | **cspf-node-number** | **cspf-nlsa-number** | **cspf-srlg-number** } **threshold-alarm** command only configures trigger conditions for alarms and clear alarms. Although trigger conditions are met, an alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsresourcethresholdexceed** | **hwmplsresourcethresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Set the upper and lower alarm thresholds to 90% and 60%, respectively, for the proportion of existing CSPF links to the maximum number of CSPF links that a device supports.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls cspf-link-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.67 mpls rsvp-lsp-number threshold-alarm

Function

The **mpls rsvp-lsp-number threshold-alarm** command configures the alarm threshold for Resource Reservation Protocol (RSVP) label switched path (LSP) usage.

The **undo mpls rsvp-lsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for RSVP LSP usage is 80%. The default lower limit of the clear alarm threshold for RSVP LSP usage is 75%.

Format

mpls rsvp-lsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls rsvp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls rsvp-lsp-number threshold-alarm

undo mpls rsvp-lsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for RSVP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for RSVP LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	The alarm that the number of ingress RSVP LSPs reached the upper threshold is generated.	-
transit	The alarm that the number of transit RSVP LSPs reached the upper threshold is generated.	-
egress	The alarm that the number of egress RSVP LSPs reached the upper threshold is generated.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of RSVP LSPs in the system reaches a specific limit, establishing subsequent RSVP LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of RSVP LSPs reaches the specific limit. To configure the alarm threshold for RSVP LSP usage, run the **mpls rsvp-lsp-number threshold-alarm** command. The parameters in this command are described as follows:

- When the RSVP LSP usage increases to the value of *upper-limit-value*, an alarm for RSVP LSPs is generated.
- When the RSVP LSP usage falls below the value of *lower-limit-value*, a clear alarm for RSVP LSPs is generated.

If you want to set the alarm threshold for ingress RSVP LSPs, transit RSVP LSPs or egress RSVP LSPs, run **mpls rsvp-lsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls rsvp-lsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for RSVP LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual RSVP LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the lower threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual RSVP LSP usage falls below the lower limit of the clear alarm threshold.

Example

Configure the upper limit and the lower limit of the alarm threshold for RSVP LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-lsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.68 mpls rsvp-peer-number threshold-alarm

Function

The **mpls rsvp-peer-number threshold-alarm** command configures the conditions that trigger the threshold-reaching alarm and its clear alarm for RSVP neighbors.

The **undo mpls rsvp-peer-number threshold-alarm** command restores the default settings.

By default, the upper alarm threshold is 80%, and the lower alarm threshold is 75%.

Format

mpls rsvp-peer-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls rsvp-peer-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for the proportion of configured RSVP neighbors to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for the proportion of configured RSVP neighbors to all supported ones.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of RSVP neighbors reaches a specified upper limit, new RSVP neighbors cannot be configured due to insufficient resources. To alert the administrator in operation and maintenance, enable a device to generate an alarm when the proportion of configured RSVP neighbors to all supported ones reaches a specified upper alarm threshold. The following parameters can be configured in the **mpls rsvp-peer-number threshold-alarm** command:

- *upper-limit-value*: upper alarm threshold. If the proportion of configured RSVP neighbors to all supported ones reaches the upper alarm threshold, an alarm can be generated.
- *lower-limit-value*: lower alarm threshold. If the proportion of configured RSVP neighbors to all supported ones falls below the lower alarm threshold, a clear alarm can be generated.

Precautions

- If the **mpls rsvp-peer-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

- The **mpls rsvp-peer-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_rsvp trap-name** { **hwrsvpteifnbrthresholdexceed** | **hwrsvpteifnbrthresholdexceedclear** } command is run to enable the device to generate an MPLS resource insufficiency alarm and its clear alarm.

Example

Configure conditions that trigger the threshold-reaching alarm and its clear alarm for RSVP neighbors.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-peer-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.69 mpls rsvp-te

Function

The **mpls rsvp-te** command enables the RSVP-TE function on an interface or globally.

The **undo mpls rsvp-te** command disables the RSVP-TE function.

RSVP-TE is disabled by default.

Format

mpls rsvp-te

undo mpls rsvp-te

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

You must run the **mpls (system view)** and **mpls te** commands to enable MPLS and MPLS TE before running the **mpls rsvp-te** command in the MPLS view.

You must run the **mpls (interface view)** and **mpls te** commands to enable MPLS and MPLS TE before running the **mpls rsvp-te** command in the interface view.

Precautions

Before enabling the RSVP-TE function on an interface, you need to run this command in the MPLS view to enable the RSVP-TE function globally.

NOTICE

After the **undo mpls rsvp-te** command is run in the MPLS view, MPLS RSVP-TE services may be interrupted and all MPLS RSVP-TE configurations are deleted. To restore the MPLS RSVP-TE services, reconfigure these commands.

Example

Enable RSVP-TE globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
```

Enable RSVP-TE on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
```

Enable RSVP-TE on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
```

9.3.70 mpls rsvp-te authentication

Function

The **mpls rsvp-te authentication** command run in the interface or neighbor view enables authentication and sets an authentication key.

The **undo mpls rsvp-te authentication** command run in the interface or neighbor view disables authentication.

Authentication is disabled by default.

Format

mpls rsvp-te authentication { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* [**sha256-compatible**] }

undo mpls rsvp-te authentication

Parameters

Parameter	Description	Value
cipher	Indicates that the key is displayed in cipher text.	-
plain	Indicates that the key is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. In this case, users at a lower level can easily obtain the password by viewing the configuration file. This brings security risks. Therefore, it is recommended that you select **cipher** to save the password in cipher text.	-
auth-key	Specifies the password.	A string of case-sensitive characters, spaces not supported. When the key is displayed in plaintext, its length ranges from 1 to 255; when the key is displayed in MD5 cipher text, its length ranges from 20 to 392. When double quotation marks are used around the string, spaces are allowed in the string.
keychain *keychain-name*	Specifies the keychain name, which is configured by running the **keychain** command.	The value is the name of an existing keychain.
sha256-compatible	Indicates that the calculated digest includes the authentication key when the SHA-256 algorithm is used for Keychain authentication. If this parameter is not specified, the calculated digest does not include the authentication key.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RSVP authentication can be configured to improve network reliability and security and prevent attacks initiated using messages modified or forged by unauthorized users.

RSVP authentication can prevent the setup of an illegal RSVP neighbor relationship using the following methods and protect the local node against attacks (such as malicious reservation of a larger number of bandwidth resources):

- An unauthorized node attempts to set up an RSVP neighbor relationship with the local node.
- A remote node generates and sends forged RSVP messages to set up a neighbor relationship with the local node.

Prerequisites

The **mpls rsvp-te** command is run to enable RSVP-TE in the MPLS view and interface view.

Precautions

The **mpls rsvp-te authentication** command run in either of the following views produces a specific result:

- If this command is run in the interface view, RSVP authentication takes effect on packets received by the interface. The interface sends RSVP-TE packets all carrying authentication information that is calculated using the key of the configured authentication mode, and authenticates all received RSVP-TE packets based on the configured key.
- If this command is run in the MPLS RSVP-TE neighbor view, RSVP authentication takes effect on packets received by the local RSVP-TE neighbor. The RSVP-TE packets sending by neighbor node all carry authentication information that is calculated using the key of the configured authentication mode, and authenticates all RSVP-TE packets sending to the neighbor node based on the configured key.

Parameters are optional for configuring HMAC-MD5 or keychain authentication:

- **cipher**: indicates HMAC-MD5 authentication with the key displayed in cipher text.
- **plain**: indicates HMAC-MD5 authentication with the key displayed in plain text.
- **keychain**: indicates keychain authentication with a globally configured keychain.
  - If the **sha256-compatible** parameter is specified and the SHA-256 algorithm is used for Keychain authentication, the calculated digest includes the authentication key.
  - If the **sha256-compatible** parameter is not specified and the SHA-256 algorithm is used for Keychain authentication, the digest is calculated using only original packets.

  – If the SHA-256 algorithm is not used for Keychain authentication, the **sha256-compatible** parameter does not need to be specified.

Note that HMAC-MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.

Example

Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication keychain kc1
```

Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication keychain kc1
```

Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication keychain kc1
```

9.3.71 mpls rsvp-te authentication handshake

Function

The **mpls rsvp-te authentication handshake** command configures the RSVP-TE handshake mechanism.

The **undo mpls rsvp-te authentication handshake** command deletes the RSVP-TE handshake mechanism configuration.

By default, no RSVP-TE handshake mechanism is configured.

Format

mpls rsvp-te authentication handshake

undo mpls rsvp-te authentication handshake

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication handshake** command can be used to configure the RSVP-TE handshake mechanism to prevent anti-replay and improve network security.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* [**sha256-compatible**] } command in the interface view or the MPLS RSVP-TE neighbor view.

Example

Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 172.16.1.1
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication handshake
```

Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
```

```
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication handshake
```

Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication handshake
```

9.3.72 mpls rsvp-te authentication lifetime

Function

The **mpls rsvp-te authentication lifetime** command sets the RSVP-TE authentication lifetime.

The **undo mpls rsvp-te authentication lifetime** command restores the default RSVP-TE authentication lifetime.

By default, the RSVP-TE authentication lifetime is 30 minutes.

Format

mpls rsvp-te authentication lifetime *lifetime*

undo mpls rsvp-te authentication lifetime

Parameters

Parameter	Description	Value
lifetime	Specifies the authentication lifetime.	The value ranges from 00:00:01 to 23:59:59 in the format of HH:MM:SS. The default value is 00:30:00.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSVP lifetime functions are as follows:

- When no CR-LSP exists between RSVP neighbors, the RSVP adjacency remains until the RSVP authentication lifetime expires. The configuration of the RSVP authentication time does not affect the status of existing CR-LSPs.
- This function can avoid continuous RSVP authentication. For example, when RSVP authentication is enabled between RTA and RTB, but the key is damaged because the RSVP messages sent from RTA to RTB are incorrect, RTB receives and discards the messages. This can cause RTA to continuously send RTB the faulty RSVP messages and RTB to continuously discard these RSVP messages. The authentication relationship between the neighbors, however, cannot be torn down. In this case, the authentication lifetime needs to be configured. When a neighbor is able to receive a valid RSVP message within the lifetime, the RSVP authentication lifetime resets. Otherwise, the authentication relationship between RSVP-TE neighbors is deleted after the authentication lifetime expires.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* [**sha256-compatible**] } command in the interface view or the MPLS RSVP-TE neighbor view.

Example

Set the authentication lifetime to 40 minutes.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication lifetime 00:40:00
```

Set the authentication lifetime to 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication lifetime 00:20:00
```

Set the authentication lifetime to 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication lifetime 00:20:00
```

9.3.73 mpls rsvp-te authentication window-size

Function

The **mpls rsvp-te authentication window-size** command specifies the maximum number of RSVP authentication messages that can be received out of sequence.

The **undo mpls rsvp-te authentication window-size** command restores the default configuration.

By default, the maximum number of RSVP authentication messages that can be received out of sequence is 1.

Format

mpls rsvp-te authentication window-size *window-size*

undo mpls rsvp-te authentication window-size

Parameters

Parameter	Description	Value
window-size	Specifies the size of a message window.	The value is an integer that ranges from 1 to 64. The default size is 1.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism and sets the local password.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication window-size** command can be used to set the maximum number of RSVP authentication messages that can be received. This setting prevents authentication termination due to RSVP message disorder.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name*

[**sha256-compatible**] } command in the interface view or the MPLS RSVP-TE neighbor view.

Precautions

Setting the window size to a value greater than 32 is recommended. If the size of a sliding window is small, the RSVP messages may be dropped and the RSVP neighbor relationship may be terminated. If the size of a sliding window is set to 1, all the RSVP authentication messages that are received out of sequence are dropped.

Example

Set the size of the message window to 64.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 172.16.1.1
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-mpls-rsvp-te-peer-172.16.1.1] mpls rsvp-te authentication window-size 64
```

Set the size of the message window to 1.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication window-size 1
```

Set the size of the message window to 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication window-size 1
```

9.3.74 mpls rsvp-te bfd

Function

The **mpls rsvp-te bfd** command sets parameters of a BFD session for RSVP on a specified interface.

The **undo mpls rsvp-te bfd** command restores the default configuration.

By default, no parameter of a BFD session for RSVP on a specified interface is set.

Format

mpls rsvp-te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls rsvp-te bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls rsvp-te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Actual local interval at which BFD packets are sent = MAX { Local interval at which BFD packets are sent, Remote interval at which BFD packets are received }; Actual local interval at which BFD packets are received = MAX { Remote interval at which BFD packets are sent, Local interval at which BFD packets are received }; Local detection period = Actual interval at which BFD packets are received x Remote BFD detection multiplier.

For example:

- The local sending interval is 200 ms, while the local receiving interval is 300 ms, and the detection multiplier is 4.
- The remote sending interval is 100 ms, while the remote receiving interval is 600 ms, and the detection multiplier is 5.

Then,

- The actual local sending interval is 600 ms (MAX { 200 ms, 600 ms }), while the local receiving interval is 300 ms (MAX { 100 ms, 300 ms }), and the detection period is 1500 ms (300 ms x 5).
- The actual remote sending interval is 300 ms (MAX { 100 ms, 300 ms }), while the receiving interval is 600 ms (MAX { 200 ms, 600 ms }), and the detection period is 2400 ms (600 ms x 4).

Example

Set the parameters for the BFD session on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te bfd min-tx-interval 50 detect-multiplier 5
```

Set the parameters for the BFD session on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te bfd min-tx-interval 50 detect-multiplier 5
```

9.3.75 mpls rsvp-te bfd all-interfaces

Function

The **mpls rsvp-te bfd all-interfaces** command sets session parameters on all RSVP-TE interfaces.

The **undo mpls rsvp-te bfd all-interfaces** command restores the default configuration.

By default, no session parameters on all RSVP-TE interfaces are set.

Format

mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls rsvp-te bfd all-interfaces { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.

Parameter	Description	Value
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Actual local interval at which BFD packets are sent = MAX { Local interval at which BFD packets are sent, Remote interval at which BFD packets are received }; Actual local interval at which BFD packets are received = MAX { Remote interval at which BFD packets are sent, Local interval at which BFD packets are received }; Local detection period = Actual interval at which BFD packets are received x Remote BFD detection multiplier.

For example:

- The local sending interval is 200 ms, while the local receiving interval is 300 ms, and the detection multiplier is 4.
- The remote sending interval is 100 ms, while the remote receiving interval is 600 ms, and the detection multiplier is 5.

Then,

- The actual local sending interval is 600 ms (MAX { 200 ms, 600 ms }), while the local receiving interval is 300 ms (MAX { 100 ms, 300 ms }), and the detection period is 1500 ms (300 ms x 5).
- The actual remote sending interval is 300 ms (MAX { 100 ms, 300 ms }), while the receiving interval is 600 ms (MAX { 200 ms, 600 ms }), and the detection period is 2400 ms (600 ms x 4).

Example

Set the session parameters of all RSVP-TE interfaces.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te bfd all-interfaces min-tx-interval 500 min-rx-interval 400
```

9.3.76 mpls rsvp-te bfd all-interfaces enable

Function

The **mpls rsvp-te bfd all-interfaces enable** command globally enables BFD for RSVP.

The **undo mpls rsvp-te bfd all-interfaces enable** command restores the default configuration.

By default, BFD for RSVP is disabled.

Format

mpls rsvp-te bfd all-interfaces enable

undo mpls rsvp-te bfd all-interfaces enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd all-interfaces enable** command enables the capability of creating BFD sessions on all interfaces that are not blocked from BFD for RSVP.

Example

Enable BFD for RSVP globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te bfd all-interfaces enable
```

9.3.77 mpls rsvp-te bfd block

Function

The **mpls rsvp-te bfd block** command blocks the BFD for RSVP capability on an interface.

The **undo mpls rsvp-te bfd block** command restores the default configuration.

By default, the BFD for RSVP capability on an interface is not blocked.

Format

mpls rsvp-te bfd block

undo mpls rsvp-te bfd block

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd block** command and the **mpls rsvp-te bfd enable** command are mutually exclusive.

The **mpls rsvp-te bfd block** command is similar to the **undo mpls rsvp-te bfd enable** command. Their differences are as follows:

- When the **undo mpls rsvp-te bfd enable** command is run to disable BFD for RSVP on an RSVP interface, the interface can obtain the BFD for RSVP capability after you configure the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view.
- When the **mpls rsvp-te bfd block** command is run on an interface, the interface cannot obtain the BFD for RSVP capability even if the **mpls rsvp-te bfd all-interfaces enable** command is run in the MPLS view.

NOTE

- To enable the BFD for RSVP capability on a majority of interfaces, you can run the **mpls rsvp-te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for RSVP. Then, you can run the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view to enable the BFD for RSVP capability for the desired majority.
- To enable BFD for RSVP capability on a few interfaces, you can run the **mpls rsvp-te bfd enable** command on these specific interfaces. In addition, you can run the **undo mpls rsvp-te bfd enable** command or the **mpls rsvp-te bfd block** command to disable BFD for RSVP on these interfaces.

Example

Disable BFD for RSVP on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te bfd block
```

Disable BFD for RSVP on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te bfd block
```

9.3.78 mpls rsvp-te bfd enable

Function

The **mpls rsvp-te bfd enable** command enables the BFD for RSVP capability on an interface.

The **undo mpls rsvp-te bfd enable** command restores the default configuration.

By default, the BFD for RSVP capability on an interface is disabled.

Format

mpls rsvp-te bfd enable

undo mpls rsvp-te bfd enable

Parameters

None

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd enable** command and the **mpls rsvp-te bfd block** command are mutually exclusive. When using these commands, note the following:

- If the **undo mpls rsvp-te bfd enable** command is run to disable BFD for RSVP on an RSVP interface, the interface can still obtain the BFD for RSVP capability after you configure the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view.
- If the **mpls rsvp-te bfd block** command is run on an interface, the interface cannot obtain the BFD for RSVP capability even if the **mpls rsvp-te bfd all-interfaces enable** command is run in the MPLS view.

NOTE

- To enable the BFD for RSVP capability on a majority of interfaces, you can run the **mpls rsvp-te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for RSVP. Then, you can run the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view to enable the BFD for RSVP capability for the desired majority.
- To enable BFD for RSVP capability on a few interfaces, you can run the **mpls rsvp-te bfd enable** command on these specific interfaces. In addition, you can run the **undo mpls rsvp-te bfd enable** command or the **mpls rsvp-te bfd block** command to disable BFD for RSVP on these interfaces.

Example

Enable the BFD for RSVP capability on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te bfd enable
```

Enable the BFD for RSVP capability on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te bfd enable
```

9.3.79 mpls rsvp-te challenge-lost

Function

The **mpls rsvp-te challenge-lost** command sets the maximum number of times that the authenticator allows itself to retransmit Challenge messages during RSVP authentication.

The **undo mpls rsvp-te challenge-lost** command restores the default setting.

By default, the number of times for retransmitting Challenge messages is 3.

Format

mpls rsvp-te challenge-lost *max-miss-times*

undo mpls rsvp-te challenge-lost

Parameters

Parameter	Description	Value
max-miss-times	Specifies the number of times for retransmitting Challenge messages.	The value is an integer that ranges from 1 to 10. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Assume node A and node B are RSVP neighbors and they need to authenticate each other. Node A authenticates node B as follows:

- Node A sends an RSVP message carrying an Integrity object to node B.
- When node B receives the message and detects that the key ID of node A is different from that in the Integrity object, node B sends a Challenge message to node A and starts a timer determining the time interval at which the Challenge message will be periodically retransmitted, and records the number of retries.
- When node A receives the Challenge message from node B, it directly copies the Challenge object in a message and adds its Integrity object to the message to generate a Response message to be sent to node B.
- When node B receives the Response message from node A, it checks whether the Challenge object in the Response message is consistent with the local Challenge object.
  - If the Challenge objects are consistent, node B stops and resets the timer for sending Challenge messages. Then, the authentication is successful.
  - If the Challenge message timer expires before node B receives the Response message, the authentication fails.

You can run the **mpls rsvp-te challenge-lost** command to change the maximum number of times for sending Challenge messages. In addition, you can use the **mpls rsvp-te retrans-timer challenge** command to change the interval for retransmitting Challenge messages.

Example

Set the number of times for retransmitting Challenge messages to 5.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te challenge-lost 5
```

9.3.80 mpls rsvp-te fast-reroute-bandwidth compatible

Function

The **mpls rsvp-te fast-reroute-bandwidth compatible** command configures the bandwidth of FRR objects to be saved in the integer mode.

The **undo mpls rsvp-te fast-reroute-bandwidth compatible** command restores the default configuration.

By default, the bandwidth of FRR objects is saved in the float point mode.

Format

mpls rsvp-te fast-reroute-bandwidth compatible

undo mpls rsvp-te fast-reroute-bandwidth compatible

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

When Huawei devices communicate with devices from other vendors whose saving mode of the bandwidth of FRR objects is set to the integer mode, you need to run this command to set the saving mode of the bandwidth of FRR objects to the integer mode.

Example

Configure the saving mode of the bandwidth of FRR objects as the integer mode.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te fast-reroute-bandwidth compatible
```

9.3.81 mpls rsvp-te hello-lost

Function

The **mpls rsvp-te hello-lost** command sets the maximum number of times for the consecutively lost Hello messages.

The **undo mpls rsvp-te hello-lost** command restores the default configuration.

By default, a maximum of three Hello messages can be lost consecutively.

Format

mpls rsvp-te hello-lost *times*

undo mpls rsvp-te hello-lost

Parameters

Parameter	Description	Value
times	Specifies the maximum number of times for the consecutively lost Hello messages.	The value is an integer that ranges from 3 to 10. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RSVP Hello extension function is enabled, you can run this command to set the maximum number of times for the consecutively lost Hello messages. If the number of times a node does not receive Hello messages consecutively exceeds the maximum value, it is considered that the link fails.

Prerequisites

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command in the MPLS view.

Example

Set the maximum number of times for the consecutively lost Hello messages to 5.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello-lost 5
```

9.3.82 mpls rsvp-te hello

Function

The **mpls rsvp-te hello** command enables the RSVP Hello extension function globally or on an interface.

The **undo mpls rsvp-te hello** command disables the RSVP Hello extension function globally or on an interface.

By default, the RSVP Hello extension function is disabled.

Format

mpls rsvp-te hello

undo mpls rsvp-te hello

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSVP Hello extension mechanism provides fast detection on the reachability between RSVP nodes. The function increases network costs. Therefore, you need to determine whether to enable this function based on network requirements.

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

Precautions

The **undo mpls rsvp-te hello** command in the MPLS view disables the Hello function from all interfaces and disables GR on the local node.

You can run the **mpls rsvp-te hello** command in the MPLS view to enable the Hello function globally. After that, you can run the **mpls rsvp-te hello** command in the interface view to enable the Hello function on an interface.

The **undo mpls rsvp-te hello** command in the interface view is used to disable the Hello function on the interface. The **undo mpls rsvp-te hello** command in the MPLS view is used to disable the Hello function globally.

Example

Enable the RSVP Hello extension function globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
```

Enable the RSVP Hello extension function on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te hello
```

Enable the RSVP Hello extension function on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te hello
```

9.3.83 mpls rsvp-te hello basic-restart-time

Function

The **mpls rsvp-te hello basic-restart-time** command changes the basic time of RSVP GR.

The **undo mpls rsvp-te hello basic-restart-time** command restores the default setting.

By default, the basic time of RSVP GR is 90 seconds.

Format

mpls rsvp-te hello basic-restart-time *basic-restart-time*

undo mpls rsvp-te hello basic-restart-time

Parameters

Parameter	Description	Value
basic-restart-time	Specifies the basic time of RSVP GR.	The value is an integer that ranges from 30 to 1200, in seconds.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

At the beginning of the AMB/SMB switchover, an RSVP-TE GR node enters a period during which the data plane can forward data but the control plane is not restored. A Restart timer starts following this phase. The restart time is relevant to the basic time, the number of ingress LSPs and the number of non-ingress LSPs. The default basic time is 90 seconds. You can use the **mpls rsvp-te hello basic-restart-time** command to change the value of the basic time.

After the Restart timer expires, the node starts a Recovery timer. The recovery time is relevant to the restart time and total number of LSPs.

Prerequisites

RSVP GR has been enabled by running the **mpls rsvp-te hello full-gr** command in the MPLS view.

Example

Set the basic time of RSVP GR to 39 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te hello basic-restart-time 39
```

9.3.84 mpls rsvp-te hello full-gr

Function

The **mpls rsvp-te hello full-gr** command enables RSVP GR and RSVP GR Helper.

The **undo mpls rsvp-te hello full-gr** command restores the default configurations.

By default, RSVP GR and RSVP GR Helper are disabled.

Format

mpls rsvp-te hello full-gr

undo mpls rsvp-te hello full-gr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command.

Example

Enable RSVP GR and RSVP GR Helper.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello full-gr
```

9.3.85 mpls rsvp-te hello nodeid-session

Function

The **mpls rsvp-te hello nodeid-session** command establishes a Hello session between a PLR node and an MP node and specifies the ID of a single-hop or multi-hop node.

The **undo mpls rsvp-te hello nodeid-session** command restores the default configuration.

By default, no Hello session is established between a PLR node and an MP node.

Format

mpls rsvp-te hello nodeid-session *ip-address*

undo mpls rsvp-te hello nodeid-session [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a neighbor.	The value is in dotted decimal notation.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

On a TE FRR network, to ensure the protection of the primary tunnel when FRR and RSVP GR simultaneously occur, run the **mpls rsvp-te hello nodeid-session** command to establish a Hello session between a PLR node and an MP node.

Example

Establish a Hello session between the PLR and MP along the bypass tunnel.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello nodeid-session 10.0.0.1
```

9.3.86 mpls rsvp-te hello support-peer-gr

Function

The **mpls rsvp-te hello support-peer-gr** command enables RSVP GR Helper.

The **undo mpls rsvp-te hello support-peer-gr** command restores the default configuration.

By default, RSVP GR Helper is disabled.

Format

mpls rsvp-te hello support-peer-gr

undo mpls rsvp-te hello support-peer-gr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command.

Precautions

If the **mpls rsvp-te hello full-gr** command is run on an RSVP node, this node has the capability of RSVP GR Helper. If a node is a GR supporter rather than a GR node, run the **mpls rsvp-te hello support-peer-gr** command.

To change a node from a GR node to a GR supporter, you must run the **undo mpls rsvp-te hello full-gr** command, then run the **mpls rsvp-te hello support-peer-gr** command.

Example

Enable RSVP GR Helper.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te hello support-peer-gr
```

9.3.87 mpls rsvp-te keep-multiplier

Function

The **mpls rsvp-te keep-multiplier** command sets the number of retry times allowed for RSVP Refresh messages.

The **undo mpls rsvp-te keep-multiplier** command restores the default settings.

The number of retry times allowed for RSVP Refresh messages is 3 by default.

Format

mpls rsvp-te keep-multiplier *keep-multiplier-number*

undo mpls rsvp-te keep-multiplier

Parameters

Parameter	Description	Value
keep-multiplier-number	Specifies the number of retry times allowed for RSVP Refresh messages.	The value is an integer that ranges from 3 to 255. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a node does not receive any Refresh message about PSB or RSB within a specified time period, the node deletes the state. You can run this command to modify the number of retry times for Refresh messages to change of the timeout period.

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

Precautions

The timeout period is calculated by using the following formula:

Timeout period = (*keep-multiplier-number* + 0.5) x 1.5 x *refresh-interval*.

In the formula, *keep-multiplier-number* specifies the number of retry times allowed for RSVP Refresh messages; *refresh-interval* specifies the interval at which RSVP Refresh messages are sent. To set these two parameters, run the **mpls rsvp-te timer refresh** command.

Example

Set the number of retry times for RSVP Refresh messages to 5.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te keep-multiplier 5
```

9.3.88 mpls rsvp-te peer

Function

The **mpls rsvp-te peer** command sets up an RSVP neighbor node and displays the MPLS RSVP-TE neighbor view.

The **undo mpls rsvp-te peer** command deletes an RSVP neighbor node.

No RSVP neighbor node is set up by default.

Format

mpls rsvp-te peer *ip-address*

undo mpls rsvp-te peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor interface or the LSR ID. The LSR ID is specified in the **mpls lsr-id** command.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command in the MPLS view.

Precautions

You can run this command on two neighboring devices to configure neighbor nodes. Then you can configure these neighbors with other functions such as authentication and handshake. The command functions differ according to the values of *ip-address*.

- When *ip-address* is the LSR-ID of a neighbor, the command takes effect on an entire device.
- When *ip-address* is the IP address of a neighbor interface, the command takes effect only on the single interface.

NOTE

If a neighbor node is identified by its LSR-ID, CSPF must be enabled on two neighboring devices where RSVP authentication is required.

Example

Set up an RSVP neighbor node and displays the MPLS RSVP-TE neighbor view.

```
<HUAWEI> system-view
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1]
```

9.3.89 mpls rsvp-te resv-rro

Function

The **mpls rsvp-te resv-rro** command configures record route objects (RROs) carried in Resv messages.

The **undo mpls rsvp-te resv-rro** command restores the default setting.

By default, the labels carried in the transit LSP RRO in turn are inbound interface address with upstream label, LSR ID with upstream label, and outbound interface address. The labels carried in the egress LSP RRO in turn are inbound interface address with upstream label, LSR ID with upstream label.

Format

mpls rsvp-te resv-rro transit { { **incoming** | **incoming-with-label** } | { **routerid** | **routerid-with-label** } | { **outgoing** | **outgoing-with-label** } } *

mpls rsvp-te resv-rro egress { { **incoming** | **incoming-with-label** } | { **routerid** | **routerid-with-label** } } *

undo mpls rsvp-te resv-rro transit

undo mpls rsvp-te resv-rro egress

Parameters

Parameter	Description	Value
transit	Indicates a transit node.	-
incoming	Indicates an inbound interface address.	-
incoming-with-label	Indicates an inbound interface address and upstream label.	-
routerid	Indicates an LSR ID.	-
routerid-with-label	Indicates an LSR ID and an upstream label.	-
outgoing	Indicates an outbound interface address.	-
outgoing-with-label	Indicates an outbound interface address and a downstream label.	-
egress	Indicates an egress.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two devices of different types must have the same RRO configuration to ensure that they can communicate with each other. You can run the **mpls rsvp-te resv-rro** command to configure RROs carried in Resv messages.

Precautions

The modification takes effect only for new LSPs.

Example

Configure the transit LSP RRO to carry the following labels: LSR ID with upstream label, inbound interface address, and outbound interface address with downstream label.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te resv-rro transit routerid-with-label incoming outgoing-with-label
```

Configure the egress LSP RRO to carry the following labels: LSR ID with upstream label, and inbound interface address.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te resv-rro egress routerid-with-label incoming
```

9.3.90 mpls rsvp-te resvconfirm

Function

The **mpls rsvp-te resvconfirm** command enables the reservation confirmation mechanism on a node.

The **undo mpls rsvp-te resvconfirm** command disables the reservation confirmation mechanism.

The mechanism is disabled on a node by default.

Format

mpls rsvp-te resvconfirm

undo mpls rsvp-te resvconfirm

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te resvconfirm** command is configured on the egress of the TE tunnel.

Example

Enable the reservation confirmation mechanism on the local node.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te resvconfirm
```

9.3.91 mpls rsvp-te retrans-timer challenge

Function

The **mpls rsvp-te retrans-timer challenge** command configures the interval at which a Challenge message is retransmitted.

The **undo mpls rsvp-te retrans-timer challenge** command restores the default value.

The interval at which a Challenge message is retransmitted is set to 1000 milliseconds by default.

Format

mpls rsvp-te retrans-timer challenge *retransmission-interval*

undo mpls rsvp-te retrans-timer challenge

Parameters

Parameter	Description	Value
retransmission-interval	Specifies the interval at which a Challenge message is retransmitted.	An integer ranging from 500 to 10000 in milliseconds. The value is 1000 milliseconds by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Assume node A and node B are RSVP neighbors and they need to authenticate each other. Node A authenticates node B as follows:

- Node A sends an RSVP message carrying an Integrity object to node B.
- When node B receives the message and detects that the key ID of node A is different from that in the Integrity object, node B sends a Challenge message to node A and starts a timer determining the time interval at which the Challenge message will be periodically retransmitted, and records the number of retries.
- When node A receives the Challenge message from node B, it directly copies the Challenge object in a message and adds its Integrity object to the message to generate a Response message to be sent to node B.
- When node B receives the Response message from node A, it checks whether the Challenge object in the Response message is consistent with the local Challenge object.
  - If the Challenge objects are consistent, node B stops and resets the timer for sending Challenge messages. Then, the authentication is successful.
  - If the Challenge message timer expires before node B receives the Response message, the authentication fails.

You can run the **mpls rsvp-te challenge-lost** command to change the maximum number of attempts to send Challenge messages. In addition, you can use the

mpls rsvp-te retrans-timer challenge command to change the interval at which a Challenge message is retransmitted.

Example

Set the interval for retransmitting a Challenge message to 800 ms.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te retrans-timer challenge 800
```

9.3.92 mpls rsvp-te send-message

Function

The **mpls rsvp-te send-message** command configures the formats of objects in a sent message.

The **undo mpls rsvp-te send-message** command restores the default configuration.

By default, the formats of objects in the sent message are not configured.

Format

mpls rsvp-te send-message { **suggest-label** | **extend-class-type value-length-type** | **session-attribute without-affinity** | **down-reason** }

undo mpls rsvp-te send-message { **suggest-label** | **extend-class-type value-length-type** | **session-attribute without-affinity** | **down-reason** }

Parameters

Parameter	Description	Value
suggest-label	Indicates that an RSVP message carries the suggest-label object.	-
extend-class-type value-length-type	Indicates that the encoding format of the extend-class-type object in an RSVP message is value-length-type.	-
session-attribute without-affinity	Indicates that the session-attribute in an RSVP message does not carry the affinity attribute.	-
down-reason	Indicates that RSVP messages carry the down-reason object.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls rsvp-te send-message** command controls the formats of objects in the messages sent by nodes. If required, you can use this command to adjust the transmission of messages so that downstream nodes can use the carried object format in processing.

When a Huawei device attempts to communicate with a non-Huawei device, RSVP messages sent by the non-Huawei device may not support the affinity attribute, causing a communication failure. To allow successful communication, run the **mpls rsvp-te send-message session-attribute without-affinity** command to allow the Huawei device to receive RSVP messages without the affinity attribute.

If you want an ingress to learn RSVP-TE tunnel Down causes of the transit and egress nodes, run the **mpls rsvp-te send-message down-reason** command on the transit and egress nodes, facilitating fault locating.

Precautions

The modification takes effect only for new LSPs.

Configurations of the four formats of objects in a sent message can take effect simultaneously.

Example

Include the suggest-label object from a message.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message suggest-label
```

Set the encoding format of the extend-class-type object in an RSVP message to value-length-type.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message extend-class-type value-length-type
```

Allow a message to carry the session-attribute object without the affinity attribute.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message session-attribute without-affinity
```

Configure RSVP messages to carry the down-reason object.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message down-reason
```

9.3.93 mpls rsvp-te srefresh

Function

The **mpls rsvp-te srefresh** command enables the summary refresh (Srefresh) function on an interface or globally.

The **undo mpls rsvp-te srefresh** command disables the Srefresh function.

The Srefresh function is disabled by default.

Format

mpls rsvp-te srefresh

undo mpls rsvp-te srefresh

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Each RSVP session needs to generate, send, receive, and process RSVP Path messages and Resv message within the refresh period. With an increasing number of RSVP sessions, a large number of Refresh messages are generated to maintain the RSVP soft state. When an RSVP message, not an RSVP Refresh message, is dropped, reliability is deteriorated and causes delay. The Srefresh extension can solve the preceding problems. The summary refresh mechanism reduces the required number of Refresh messages and improves reliability of RSVP messages and efficiency of resource usage.

After the Srefresh function is enabled in the MPLS view, the Srefresh function is enabled globally. In addition, the interface enabled with the Srefresh function can refresh the path status and the reservation status by sending Srefresh messages, rather than Path or Resv messages.

Example

Enable the Srefresh function globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te srefresh
```

Enable the Srefresh function on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te srefresh
```

Enable the Srefresh function on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te srefresh
```

9.3.94 mpls rsvp-te timer hello

Function

The **mpls rsvp-te timer hello** command sets an interval at which Hello messages are sent.

The **undo mpls rsvp-te timer hello** command restores the default setting.

The interval at which Hello messages are sent is 3 seconds by default.

Format

mpls rsvp-te timer hello *interval*

undo mpls rsvp-te timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 3s.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command in the MPLS view.

NOTE

If the interval at which Hello messages are sent is changed, the new interval can only take effect after the previous Hello timer expires.

Example

Set the interval at which Hello messages are sent to 5s.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te hello
[HUAWEI-mpls] mpls rsvp-te timer hello 5
```

9.3.95 mpls rsvp-te timer refresh

Function

The **mpls rsvp-te timer refresh** command sets an interval at which RSVP Refresh messages are sent.

The **undo mpls rsvp-te timer refresh** command restores the default setting.

The time interval is 30 seconds by default.

Format

mpls rsvp-te timer refresh *refresh-interval*

undo mpls rsvp-te timer refresh

Parameters

Parameter	Description	Value
refresh-interval	Specifies the interval at which RSVP Refresh messages are sent.	An integer ranging from 10 to 65535 in seconds.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

NOTE

If the interval at which RSVP Refresh messages are sent is changed, the new interval can only take effect after the previous refreshing timer expires. Therefore, you are not recommended to set an excessively long refreshing interval, or frequently change a refreshing interval.

Example

Set the interval at which RSVP Refresh messages are sent to 60s.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] mpls rsvp-te timer refresh 60
```

9.3.96 mpls rsvp-te timer retransmission

Function

The **mpls rsvp-te timer retransmission** command adjusts retransmission-related parameters on an interface.

The **undo mpls rsvp-te timer retransmission** command restores the default settings.

By default, the retransmission incremental is 1 and the timeout period of a retransmission timer is 5000 ms.

Format

mpls rsvp-te timer retransmission { **increment-value** *increment* | **retransmit-value** *interval* } *

undo mpls rsvp-te timer retransmission [**increment-value** [*increment*] | **retransmit-value** [*interval*]] *

Parameters

Parameter	Description	Value
increment-value *increment*	Specifies the retransmission incremental value.	The value is an integer that ranges from 1 to 10. The default value is 1.
retransmit-value *interval*	Specifies the timeout period of a retransmission timer.	The value is an integer that ranges from 500 to 5000, in milliseconds. The default value is 5000 ms.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The relationship between *increment* and *interval*: Next retransmission *interval* = Current retransmission *interval* x (1 + *increment*)

Prerequisites

The Srefresh function has been enabled by running the **mpls rsvp-te srefresh** command in the MPLS view.

Example

Set the timeout period of the retransmission timer to 500 ms and the increment to 2 on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te timer retransmission retransmit-value 500 increment-value 2
```

Set the timeout period of the retransmission timer to 500 ms and the increment to 2 on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te timer retransmission retransmit-value 500 increment-value 2
```

9.3.97 mpls te

Function

The **mpls te** command enables MPLS TE.

The **undo mpls te** command disables MPLS TE.

MPLS TE is disabled by default.

Format

mpls te

undo mpls te

Parameters

None

Views

MPLS view, VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When running the **mpls te** command in the MPLS view, you can globally enable MPLS TE. When running the **mpls te** command in the interface view, you can enable MPLS TE on a specified interface. MPLS TE can only be enabled on interfaces after the function is enabled globally.

Precautions

NOTICE

When the MPLS TE is disabled in the interface view, all the CR-LSPs on the current interface change to Down.

After the **undo mpls te** command is run in the MPLS view, MPLS TE services may be interrupted and all MPLS TE configurations are deleted. To restore the MPLS TE services, reconfigure these commands.

Example

Enable MPLS TE globally.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.9
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
```

Enable MPLS TE on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
```

Enable MPLS TE on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
```

9.3.98 mpls te affinity property

Function

The **mpls te affinity property** command configures the affinity property for an MPLS TE tunnel.

The **undo mpls te affinity property** command restores the default settings.

By default, both the affinity value and the affinity mask are 0x0 for an MPLS TE tunnel.

Format

mpls te affinity property *properties* [**mask** *mask-value*] [**secondary** | **best-effort**]

undo mpls te affinity property [**secondary** | **best-effort**]

undo mpls te affinity property *properties* [**mask** *mask-value*] { **secondary** | **best-effort** }

Parameters

Parameter	Description	Value
properties	Specifies the affinity property of links that carry a tunnel.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF. The default value is 0x0.
mask *mask-value*	Specifies the link property to be checked.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF. The default value is 0x0.
secondary	Indicates the affinity property of a backup CR-LSP.	-
best-effort	Indicates the affinity property of the best-effort path.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Affinity property masks determine the link properties that should be checked by a device.

To ensure that a link can be used by a tunnel, for the bits that are 1 in a mask, it is required that at least one bit in the administrative group and the corresponding bit in the affinity property be 1. In addition, if the bits in the affinity property are 0, the corresponding bits in the administrative group cannot be 1.

After an affinity property for the MPLS TE tunnel is changed and the new configuration is committed, the established LSPs can be affected, and the path of the TE tunnel is recalculated.

Example

Set the affinity property of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te affinity property a04 mask e0c
[HUAWEI-Tunnel1] mpls te commit
```

Set the affinity property of the backup CR-LSP and the best-effort path.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup hot-standby
[HUAWEI-Tunnel1] mpls te backup ordinary best-effort
[HUAWEI-Tunnel1] mpls te affinity property a04 mask e0c secondary
[HUAWEI-Tunnel1] mpls te affinity property a04 mask e0c best-effort
[HUAWEI-Tunnel1] mpls te commit
```

9.3.99 mpls te auto-bandwidth

Function

The **mpls te auto-bandwidth** command configures automatic bandwidth adjustment of a tunnel.

The **undo mpls te auto-bandwidth** command disables automatic bandwidth adjustment.

Automatic bandwidth adjustment is disabled by default.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, and S6730S-H support this command.

Format

mpls te auto-bandwidth { **adjustment** [**threshold** *percent*] | **collect-bw** } [**frequency** *interval*] [**max-bw** *max-bandwidth* **min-bw** *min-bandwidth*]

undo mpls te auto-bandwidth

Parameters

Parameter	Description	Value
adjustment	Enables automatic bandwidth adjustment.	-
threshold *percent*	Specifies the threshold of the difference between the new and existing bandwidth. The value is expressed in percentage.	An integer ranging from 0 to 100. The default value is 0.
collect-bw	Collects output rate information of a tunnel without adjusting the bandwidth.	-
frequency *interval*	Specifies the time interval for automatic bandwidth adjustment.	An integer ranging from 300 to 604800 in seconds. The default value is 86400. The recommended value is not less than the interval for sampling the output rate of a tunnel specified in the **mpls te timer auto-bandwidth** command.
max-bw *max-bandwidth*	Specifies the maximum allowable bandwidth.	An integer ranging from 0 to 4000000000 in kbit/s. The default value is 4294901760.
min-bw *min-bandwidth*	Specifies the minimum allowable bandwidth.	An integer ranging from 0 to 4000000000 in kbit/s. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The bandwidth of a tunnel can be set manually, but is not adaptable to changeable traffic on the tunnel. To ensure continuity of traffic, reserve enough bandwidth for the maximum volume of traffic. This provides enough bandwidth for traffic, but wastes bandwidth resources. To save bandwidth, configure automatic bandwidth adjustment by running the **mpls te auto-bandwidth** command.

After automatic bandwidth adjustment is enabled, run the **mpls te timer auto-bandwidth** command to configure periodic sampling and obtain the average bandwidth of the MPLS TE tunnel during a sampling interval. The system calculates the average bandwidth during the sampling interval and attempts to establish an MPLS TE tunnel based on the average bandwidth.

- After the MPLS TE tunnel is established, traffic switches to the new MPLS TE tunnel, and the original is deleted.
- If a new MPLS TE tunnel fails to be established, traffic is still transmitted along the original MPLS TE tunnel. The bandwidth will be adjusted after the next sampling period expires.

Configuring the parameter **threshold** controls whether the bandwidth of an MPLS TE tunnel should be adjusted. The system compares the average bandwidth D within a sampling period with the actual bandwidth C. If the percentage of the bandwidth change in comparison to the actual bandwidth is greater than the **threshold** value, that is, (|D-C|÷C)×100 > **threshold**, the system adjusts the bandwidth.

If traffic volume fluctuates on a network but the bandwidth does not need to be adjusted accordingly, set the value of **threshold** to a larger value.

Precautions

The **mpls te auto-bandwidth** command cannot be configured with the following commands on the same tunnel interface:

- **mpls te route-pinning**
- **mpls te resv-style ff**
- **mpls te bandwidth** (tunnel interface view) with the multi-CT specified

Example

Set the interval for automatic bandwidth adjustment to **1** hour.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te auto-bandwidth adjustment frequency 3600
```

9.3.100 mpls te auto-frr (MPLS view)

Function

The **mpls te auto-frr** command globally enables the TE Auto FRR function.

The **undo mpls te auto-frr** command globally disables the TE Auto FRR function.

TE Auto FRR is disabled by default.

Format

mpls te auto-frr

undo mpls te auto-frr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mpls te auto-frr** command to globally enable the TE Auto FRR function.

Precautions

After the TE Auto FRR function is enabled globally, all MPLS TE-enabled interfaces use node protection by default.

If TE Auto FRR is enabled globally, all interfaces that are enabled with MPLS TE on the device are automatically configured with the **mpls te auto-frr default** command by default. To disable TE Auto FRR on certain interfaces, run the **mpls te auto-frr block** command on these interfaces.

Example

Enable the TE Auto FRR function.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te auto-frr
```

Disable the TE Auto FRR function.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] undo mpls te auto-frr
```

9.3.101 mpls te auto-frr (interface view)

Function

The **mpls te auto-frr** command configures the TE Auto FRR function in the interface view.

The **undo mpls te auto-frr** command restores the default configuration.

The TE Auto FRR function is disabled on an interface by default.

Format

mpls te auto-frr { **default** | **link** | **node** | **block** }

undo mpls te auto-frr { **block** | **link** | **node** }

Parameters

Parameter	Description	Value
default	Indicates that the configuration of the TE Auto FRR function in the MPLS view is used by default. Only node protection is provided.	-
link	Indicates that only link protection is provided.	-
node	Indicates that node protection is provided. When the topology does not meet the requirement to set up a bypass CR-LSP for node protection, the penultimate hop (but not other hops) on the primary CR-LSP attempts to set up a bypass CR-LSP for link protection.	-
block	Disables the TE Auto FRR function in the interface view.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the TE Auto FRR function is enabled globally, all MPLS TE-enabled interfaces can use the TE Auto FRR configuration configured in the MPLS view.

To disable the TE Auto FRR function on a specified interface, you must run the **mpls te auto-frr block** command. To enable link protection on a specified interface, you must run the **mpls te auto-frr link** command.

Prerequisites

MPLS TE has been enabled by running the **mpls te** command in the interface view.

Precautions

After the **mpls te auto-frr block** command is run on an interface, the interface does not have the TE Auto FRR capability, regardless of whether TE Auto FRR is already enabled or reenabled globally.

After the command **mpls te auto-frr** is configured in the MPLS view, the device provides only node protection when you run the **mpls te auto-frr default** or **mpls te auto-frr node** command on an interface. When the topology does not meet the requirement to set up a bypass CR-LSP for node protection, the penultimate hop (but not other hops) on the primary CR-LSP attempts to set up a bypass CR-LSP for link protection.

Example

Enable TE Auto FRR that provides link protection on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te auto-frr link
```

Disable the TE Auto FRR function in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te auto-frr block
```

Enable TE Auto FRR that provides node protection on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te auto-frr node
```

9.3.102 mpls te auto-frr reoptimization

Function

The **mpls te auto-frr reoptimization** command enables auto bypass tunnel re-optimization.

The **undo mpls te auto-frr reoptimization** command disables auto bypass tunnel re-optimization.

By default, auto bypass tunnel re-optimization is disabled.

Format

mpls te auto-frr reoptimization [**frequency** *interval*]

undo mpls te auto-frr reoptimization

Parameters

Parameter	Description	Value
frequency *interval*	Indicates the re-optimization interval. Paths are recalculated at the *interval* based on auto bypass tunnel constraints. If an optimal path to the same destination is available, the system re-optimizes the auto bypass tunnel.	The value is an integer ranging from 60 to 604800, in seconds. The default value is 3600s (one hour).

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network changes often cause the changes in optimal paths. Run the **mpls te auto-frr reoptimization** to allow paths to be recalculated at certain intervals for an auto bypass tunnel. If an optimal path to the same destination is found due to some reasons, such as the changes in the cost, a new auto bypass tunnel will be set up over this optimal path. In this manner, network resources are optimized.

Auto bypass tunnel re-optimization can be classified into the following modes:

- Automatic re-optimization: Auto bypass tunnels are re-optimized at intervals, requiring no manual intervention. The **mpls te auto-frr reoptimization** command can be used to implement the function, and this command takes effect on the auto bypass tunnels that have been already set up successfully.
- Manual re-optimization: After the **mpls te auto-frr reoptimization** command is run, run the **mpls te reoptimization (user view)** command to re-optimize auto bypass tunnels manually.

Prerequisites

MPLS TE has been enabled using the **mpls te** command.

Example

Configure auto bypass tunnel re-optimization at 8939-second intervals.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te auto-frr reoptimization frequency 8939
```

9.3.103 mpls te backup

Function

The **mpls te backup** command specifies the backup mode of an existing tunnel.

The **undo mpls te backup** command restores the default configuration.

By default, no tunnel is backed up.

Format

mpls te backup ordinary [**best-effort**]

mpls te backup hot-standby [**mode** { **revertive** [**wtr** *interval*] | **non-revertive** } | **dynamic-bandwidth**] *

mpls te backup hot-standby wtr *interval* [**dynamic-bandwidth**]

mpls te backup hot-standby dynamic-bandwidth wtr *interval*

undo mpls te backup { **hot-standby** [**mode** { **revertive** [**wtr** [*interval*]] | **non-revertive** } | **dynamic-bandwidth**] * | **ordinary** }

Parameters

Parameter	Description	Value
ordinary	Enables the ordinary backup mode. In ordinary backup mode, an ordinary backup CR-LSP is created only after the primary CR-LSP fails.	-
hot-standby	Enables the hot-standby mode. In hot-standby mode, both the primary and backup CR-LSP are set up. If the primary CR-LSP fails, traffic is immediately switched to the hot-standby CR-LSP.	-
dynamic-bandwidth	Enables the dynamic bandwidth function for a hot-standby CR-LSP.	-
wtr *interval*	Specifies the wait-to-restore (WTR) time in hot standby.	The value is an integer that ranges from 0 to 2592000, in seconds. The default value is 10 seconds.
best-effort	Enables the best-effort path mode. When both the primary and backup CR-LSPs fail, the system triggers the establishment of a best-effort path.	-

Parameter	Description	Value
mode { **revertive** | **non-revertive** }	Specifies the revertive mode. - **revertive**: The current mode can be switched to the original mode. - **non-revertive**: The current mode cannot be switched to the original mode.	The default mode is **revertive**.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help enhance the reliability of a CR-LSP, you are recommended to set up a backup CR-LSP to protect traffic on the primary CR-LSP.

You can select the following CR-LSP backup modes as required:

- Hot-standby mode: A hot-standby backup CR-LSP is set up over a separate path immediately after the primary CR-LSP is set up. When the CR-LSP transmitting services fails, traffic can be immediately switched to the other CR-LSP. However, additional bandwidth is needed in hot-standby mode.
- Ordinary backup mode: The system attempts to set up an ordinary backup CR-LSP over a new explicit path, only when the primary CR-LSP fails. No additional bandwidth is needed in ordinary backup mode. In the case that the primary CR-LSP fails, this mode provides a traffic switchover slower than that of the hot-standby mode.
- Best-effort path mode: When both the primary and backup CR-LSP fail, the system establishes a best-effort path. There are few constraints on the establishment of best-effort path; therefore, it is easy to set up. In best-effort path mode, packet loss is decreased, and certain QoS requirements may not be guaranteed.

Prerequisites

A tunnel ID has been configured by running the **mpls te tunnel-id** command.

Precautions

After tunnel backup is enabled, the route storing function is automatically enabled, regardless of whether the **mpls te record-route** command is run.

Tunnel backup and the function configured by running the **mpls te resv-style ff** command are mutually exclusive.

The **mpls te backup ordinary** command and the **mpls te backup ordinary best-effort** command cannot be configured together; otherwise, the previous configuration overrides the later one.

After initiating the dynamic bandwidth function for a hot-standby CR-LSP, the hot-standby CR-LSP does not occupy any bandwidth when bearing no traffic. If the primary CR-LSP fails, the system re-establishes a hot-standby CR-LSP with the expected bandwidth according to the Make-Before-Break mechanism. The new hot-standby CR-LSP now transmits traffic. The system then deletes the hot-standby CR-LSP with the bandwidth being 0 bit/s.

Example

Enable hot standby for the current CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup hot-standby
[HUAWEI-Tunnel1] mpls te commit
```

9.3.104 mpls te backup frr-in-use

Function

The **mpls te backup frr-in-use** command allows a device to start a bypass CR-LSP if a primary CR-LSP becomes faulty (when the primary CR-LSP is in the FRR-in-use state), and to attempt to set up a backup CR-LSP while the system is restoring the primary CR-LSP.

The **undo mpls te backup frr-in-use** command restores the default configuration.

If the primary CR-LSP is faulty, the system starts the bypass CR-LSP and attempts to restore the primary CR-LSP, but does not set up a backup CR-LSP by default.

Format

mpls te backup frr-in-use

undo mpls te backup frr-in-use

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the primary CR-LSP is faulty, the system starts the bypass CR-LSP and tries to restore the primary CR-LSP the same time it sets up a backup CR-LSP.

Prerequisites

End-to-end protection in hot standby or ordinary backup mode has been enabled by running the **mpls te backup** { **hot-standby** | **ordinary** } command, and local protection of TE FRR has been enabled by running the **mpls te fast-reroute** command.

Precautions

If only the best-effort path is configured, rather than another end-to-end protection mode, the **mpls te backup frr-in-use** command cannot take effect.

After the **mpls te backup frr-in-use** command is run and if the primary CR-LSP is faulty:

- If ordinary backup is configured, the system tries to set up a backup CR-LSP when the traffic is switched to the bypass CR-LSP and also attempts to restore the primary CR-LSP. If the backup CR-LSP is set up successfully and the primary CR-LSP is not restored, traffic is switched to the backup CR-LSP.
- If hot standby is configured and the backup CR-LSP is in the Up state, the traffic is switched to the bypass CR-LSP and then immediately to the backup CR-LSP while the system attempts to restore the primary CR-LSP.

It is recommended that ordinary backup be configured together with the **mpls te backup frr-in-use** command. This saves bandwidth resources and improves tunnel security.

Example

Configure the system to set up a backup CR-LSP the same time it starts the bypass CR-LSP and tries to restore the primary CR-LSP after the primary CR-LSP is faulty.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup ordinary
[HUAWEI-Tunnel1] mpls te fast-reroute
[HUAWEI-Tunnel1] mpls te backup frr-in-use
[HUAWEI-Tunnel1] mpls te commit
```

9.3.105 mpls te backup hot-standby overlap-path

Function

The **mpls te backup hot-standby overlap-path** command enables the path partially overlapping function for hot-standby CR-LSPs.

The **undo mpls te backup hot-standby overlap-path** command disables the path overlapping function for hot-standby CR-LSPs.

By default, the path partially overlapping function is disabled for hot-standby CR-LSPs.

Format

mpls te backup hot-standby overlap-path

undo mpls te backup hot-standby overlap-path

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After the path overlapping function is configured, the path of a hot-standby CR-LSP can partially overlap the path of the primary CR-LSP when primary CR-LSP is not excluded by the system in path calculation.

Example

Enable the path overlapping function for hot-standby CR-LSPs.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te backup hot-standby
[HUAWEI-Tunnel1] mpls te backup hot-standby overlap-path
[HUAWEI-Tunnel1] mpls te commit
```

9.3.106 mpls te backup hotstandby-lsp-constraint

Function

The **mpls te backup hotstandby-lsp-constraint** command sets the WTR time for a switchback, locks an attribute template, and enables the dynamic bandwidth function for a hot-standby CR-LSP.

The **undo mpls te backup hotstandby-lsp-constraint** command restores default settings.

By default, the interval between switchbacks is 10 seconds; no attribute template is locked; the dynamic bandwidth function is disabled for a hot-standby CR-LSP.

Format

mpls te backup hotstandby-lsp-constraint { **wtr** *interval* | **lock** | **dynamic-bandwidth** | **overlap-path** }

mpls te backup hotstandby-lsp-constraint mode { **revertive** [**wtr** *interval*] | **non-revertive** }

undo mpls te backup hotstandby-lsp-constraint { **wtr** | **lock** | **dynamic-bandwidth** | **overlap-path** }

undo mpls te backup hotstandby-lsp-constraint mode { **non-revertive** | **revertive wtr** }

Parameters

Parameter	Description	Value
dynamic-bandwidth	Enables the dynamic bandwidth function for a hot-standby CR-LSP.	-
lock	Enables the function of locking a hot-standby CR-LSP attribute template.	-
wtr *interval*	Specifies the WTR time for a switchback from a hot-standby CR-LSP.	The value is an integer that ranges from 0 to 2592000, in seconds. The default value is 10 seconds.
overlap-path	Indicates that if no other path is available, the hot-standby LSP can overlap the primary LSP.	-
mode { **revertive** | **non-revertive** }	Specifies the revertive mode. ● **revertive**: The current mode can be switched to the original mode. ● **non-revertive**: The current mode cannot be switched to the original mode.	The default mode is **revertive**.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The function of locking a hot-standby CR-LSP attribute template allows the system to lock a lower-priority attribute template that has been used by an exiting hot-standby CR-LSP. The system will not attempt to use a higher-priority template to set up a new hot-standby CR-LSP.

Prerequisites

The following configurations must be completed before the **mpls te backup hotstandby-lsp-constraint** command is run:

- Run the **mpls te primary-lsp-constraint** command to use attribute templates to set up a primary CR-LSP.
- Run the **mpls te hotstandby-lsp-constraint** command to use attribute template to set up a hot-standby CR-LSP.

Precautions

This command is valid only for the hot-standby CR-LSP that is set up using a CR-LSP attribute template. If a hot-standby CR-LSP is set up without a CR-LSP attribute template, the following commands apply:

- The **mpls te backup hot-standby wtr** *interval* command is used to set the WTR time for a switchback.
- The **mpls te backup hot-standby dynamic-bandwidth** command is used to enable the dynamic bandwidth function for the hot-standby CR-LSP.
- The **mpls te backup hot-standby overlap-path** command is used to enable the path overlapping function for hot-standby CR-LSPs that are not established using attribute templates.

The dynamic bandwidth function for the hot-standby CR-LSP prevents a hot-standby CR-LSP transmitting no traffic from using bandwidth resources. If the primary CR-LSP fails, the system attempts to re-establish a new hot-standby CR-LSP with the required bandwidth determined by the Make-Before-Break mechanism. After the new hot-standby CR-LSP takes over traffic, the bandwidth of the failed hot-standby CR-LSP becomes 0 bit/s and is deleted by the system.

Example

Set the WTR time for a switchback from the hot-standby CR-LSP to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te hotstandby-lsp-constraint 1 lsp-attribute t2
[HUAWEI-Tunnel1] mpls te backup hotstandby-lsp-constraint wtr 20
[HUAWEI-Tunnel1] mpls te commit
```

9.3.107 mpls te backup ordinary-lsp-constraint

Function

The **mpls te backup ordinary-lsp-constraint** command globally locks an attribute template for ordinary backup CR-LSPs.

The **undo mpls te backup ordinary-lsp-constraint** command restores the default setting.

The attribute template for ordinary backup CR-LSPs is unlocked by default.

Format

mpls te backup ordinary-lsp-constraint lock

undo mpls te backup ordinary-lsp-constraint lock

Parameters

Parameter	Description	Value
lock	Locks an attribute template for ordinary backup CR-LSPs.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that an existing ordinary backup CR-LSP has been set up using a lower-priority attribute template. When the lower-priority attribute template is locked, the system does not attempt to use a higher-priority attribute template to set up a new ordinary backup CR-LSP, avoiding unnecessary traffic switchover.

Prerequisites

An ordinary backup CR-LSP has been set up using a CR-LSP attribute template by running the **mpls te ordinary-lsp-constraint** command.

Precautions

This command is valid only for an ordinary backup CR-LSP that is set up using a CR-LSP attribute template.

Example

Lock an attribute template for ordinary backup CR-LSPs.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te ordinary-lsp-constraint 2 lsp-attribute t2
[HUAWEI-Tunnel1] mpls te ordinary-lsp-constraint 3 lsp-attribute t3
[HUAWEI-Tunnel1] mpls te backup ordinary-lsp-constraint lock
[HUAWEI-Tunnel1] mpls te commit
```

9.3.108 mpls te bandwidth (interface view)

Function

The **mpls te bandwidth** command sets the BC bandwidth for a link.

The **undo mpls te bandwidth** command restores the default setting.

By default, no BC bandwidth is configured for a link.

Format

mpls te bandwidth { **bc0** *bc0-bw-value* | **bc1** *bc1-bw-value* } *

undo mpls te bandwidth

Parameters

Parameter	Description	Value
bc0 *bc0-bw-value*	Specifies the bandwidth of BC0.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc1 *bc1-bw-value*	Specifies the bandwidth of BC1.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In real-world situations, the bandwidth value is set on outbound interfaces along links of a TE tunnel that requires sufficient bandwidth.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Precautions

To change bandwidth BC values, reconfigure the **mpls te bandwidth** command. The last configured BC bandwidth value overrides the previous one.

One or more BC bandwidth values can be set in a single command in a random order.

A BC bandwidth value can be changed only to a value greater than or equal to the set one. For example, the BC0 bandwidth of 10 Mbit/s can be changed to 10 or a larger value.

Example

Set the maximum reservable bandwidth to 10000 kbit/s, the bandwidth of BC0 to 1000 kbit/s on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te bandwidth max-reservable-bandwidth 10000
[HUAWEI-Vlanif100] mpls te bandwidth bc0 1000
```

Set the maximum reservable bandwidth to 10000 kbit/s, the bandwidth of BC0 to 1000 kbit/s on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth max-reservable-bandwidth 10000
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth bc0 1000
```

9.3.109 mpls te bandwidth (tunnel interface view)

Function

The **mpls te bandwidth** command sets the bandwidth of an MPLS TE tunnel.

The **undo mpls te bandwidth** command restores the default settings.

By default, the bandwidth of an MPLS TE tunnel is not set.

Format

mpls te bandwidth { **ct0** *ct0-bw-value* | **ct1** *ct1-bw-value* }

undo mpls te bandwidth { **all** | **ct0** [*ct0-bw-value*] | **ct1** [*ct1-bw-value*] }

Parameters

Parameter	Description	Value
ct0 *ct0-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT0.	*ct0-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct1 *ct1-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT1.	*ct1-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
all	Deletes bandwidth for all CTs.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

The **undo mpls te bandwidth** command is used to restore the default settings of all CTs or specified CTs:

- **undo mpls te bandwidth all**: deletes all configured bandwidth.
- **undo mpls te bandwidth** { **ct0** | **ct1** }: deletes the bandwidth of the specified CT configured on the current TE tunnel.

Example

Set the bandwidth required by Tunnel1. The bandwidth of CT0 is 2000 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 10.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bandwidth ct0 2000
[HUAWEI-Tunnel1] mpls te commit
```

9.3.110 mpls te bandwidth change thresholds

Function

The **mpls te bandwidth change thresholds** command sets the percentage threshold of the physical link bandwidth used by an MPLS TE tunnel for flooding link information.

The **undo mpls te bandwidth change thresholds** command restores the default settings.

If the ratio of the reserved (or released) bandwidth for a tunnel to the remaining bandwidth in a Traffic Engineering Database (TEDB) is equal to or greater than 10%, an IGP floods link information and CSPF updates the TEDB by default.

Format

mpls te bandwidth change thresholds { **down** | **up** } *percent*

undo mpls te bandwidth change thresholds { **down** | **up** }

Parameters

Parameter	Description	Value
down	Indicates the flooding threshold of the bandwidth used by an MPLS TE tunnel. If the ratio of the bandwidth used by an MPLS TE tunnel to the remaining link bandwidth in a TEDB is equal to or greater than the threshold, an IGP floods link information and CSPF updates the TEDB.	-
up	Indicates the flooding threshold of the bandwidth released by an MPLS TE tunnel. If the ratio of the bandwidth released by an MPLS TE tunnel to the remaining link bandwidth in a TEDB is equal to or greater than the threshold, an IGP floods link information and CSPF updates the TEDB.	-
percent	Specifies the threshold as a percentage.	The value is an integer that ranges from 0 to 100. The default value is 10.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the bandwidth changes slightly, flooding the bandwidth wastes network resources. For example, the bandwidth of a link is 100 Mbit/s. During the creation of 100 TE tunnels each with the bandwidth being 1 Mbit/s, the bandwidth of all TE tunnels needs to be flooded 100 times. If the flooding threshold is set to 10%, the first nine tunnels are created without flooding. When the tenth tunnel is created, the 10 Mbit/s bandwidth that is used by the preceding 10 tunnels is flooded. The tunnels from the eleventh tunnel to the eighteenth are created without flooding. When the nineteenth tunnel is created, the bandwidth is flooded, and so on.

Example

On VLANIF100, when the link bandwidth reserved for the MPLS TE tunnel exceeds 10% of the overall bandwidth or the bandwidth released by the MPLS TE tunnel exceeds 25% of the overall bandwidth, the link information is flooded.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te bandwidth change thresholds up 25
[HUAWEI-Vlanif100] mpls te bandwidth change thresholds down 10
```

On GE0/0/1, when the link bandwidth released by the MPLS TE tunnel exceeds 25% of the overall bandwidth, the link information is flooded.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth change thresholds up 25
```

9.3.111 mpls te bandwidth max-reservable-bandwidth

Function

The **mpls te bandwidth max-reservable-bandwidth** command sets or modifies the maximum reservable bandwidth of a link.

The **undo mpls te bandwidth max-reservable-bandwidth** command restores the default configuration.

The maximum reservable bandwidth of a link is not configured by default.

Format

mpls te bandwidth max-reservable-bandwidth *bw-value*

undo mpls te bandwidth max-reservable-bandwidth

Parameters

Parameter	Description	Value
bw-value	Specifies the maximum reservable bandwidth of a link.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

In practical applications, the **mpls te bandwidth max-reservable-bandwidth** command can be configured for a TE tunnel on an outgoing interface of the link through which the tunnel passes.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Example

Set the maximum reservable bandwidth of the link to 10000 kbit/s on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te bandwidth max-reservable-bandwidth 10000
```

Set the maximum reservable bandwidth of the link to 10000 kbit/s on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te bandwidth max-reservable-bandwidth 10000
```

9.3.112 mpls te bfd

Function

The **mpls te bfd** command sets the parameters of a BFD session for TE.

The **undo mpls te bfd** command restores the default configuration.

By default, no parameters of a BFD session for TE are set.

Format

mpls te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls te bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If **min-tx-interval** *tx-interval* configured on the local end is different from **min-rx-interval** *rx-interval* configured on the peer, the larger value is used as the actual session parameter.

The used **detect-multiplier** *multiplier* is the value set on the peer.

If the **mpls te bfd** command is configured in the MPLS view, it takes effect globally. If the command is configured in the tunnel interface view, it only takes effect on the current tunnel interface, and the parameters of the BFD session for TE set in the MPLS view are overridden.

Example

Set the parameters of the BFD session.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bfd min-tx-interval 200 detect-multiplier 5
[HUAWEI-Tunnel1] mpls te commit
```

9.3.113 mpls te bfd block

Function

The **mpls te bfd block** command blocks the BFD capability on a specified tunnel interface of a CR-LSP.

The **undo mpls te bfd block** command restores the default configuration.

The BFD capability is not blocked on a tunnel interface by default.

Format

mpls te bfd block

undo mpls te bfd block

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te bfd block** command and the **mpls te bfd enable** command are mutually exclusive.

The differences between the **mpls te bfd block** command and the **undo mpls te bfd enable** command in the tunnel interface view are as follows:

- When the **undo mpls te bfd enable** command is run on a tunnel interface, the interface can still obtain the BFD for TE capability after you configure the **mpls te bfd enable** command in the MPLS view.
- When the **mpls te bfd block** command is run on a tunnel interface, the interface cannot obtain the BFD for TE capability even if the **mpls te bfd enable** command is run in the MPLS view.

NOTE

To enable the BFD for TE capability on a majority of interfaces, you can run the **mpls te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for TE. Then, you can run the **mpls te bfd enable** command in the MPLS view to enable the BFD for TE capability on the other interfaces.

To enable BFD for TE capability on a few interfaces, you can run the **mpls te bfd enable** command on these interfaces. After, you can run the **undo mpls te bfd enable** command or the **mpls te bfd block** command to disable BFD for TE from these interfaces.

Example

Block the BFD capability on Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bfd block
[HUAWEI-Tunnel1] mpls te commit
```

9.3.114 mpls te bfd enable

Function

The **mpls te bfd enable** command enables BFD for TE.

The **undo mpls te bfd enable** command restores the default configuration.

BFD for TE is disabled by default.

Format

mpls te bfd enable

undo mpls te bfd enable

Parameters

None.

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If the **mpls te bfd enable** command is configured in the MPLS view, all TE tunnel interfaces are enabled with BFD for TE, except those configured with the **mpls te bfd block** command, blocking BFD for TE.

If this command is configured in the tunnel interface view, it only takes effect on the single tunnel interface.

The differences between the **undo mpls te bfd enable** command and the **mpls te bfd block** command configured in the tunnel interface view are as follows:

- When the **undo mpls te bfd enable** command is run on a tunnel interface, the interface can still obtain the BFD for TE capability after you configure the **mpls te bfd enable** command in the MPLS view.
- When the **mpls te bfd block** command is run on a tunnel interface, the interface cannot obtain the BFD for TE capability even if the **mpls te bfd enable** command is run in the MPLS view.

NOTE

- To enable the BFD for TE capability on a majority of interfaces, you can run the **mpls te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for TE. Then, you can run the **mpls te bfd enable** command in the MPLS view to enable the BFD for TE capability for the other interfaces.
- To enable BFD for TE capability on a few interfaces, you can run the **mpls te bfd enable** command on these interfaces. After, you can run the **undo mpls te bfd enable** command or the **mpls te bfd block** command to disable BFD for TE from these interfaces.

Example

Enable BFD for TE globally.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te bfd enable
```

Enable BFD for TE on the tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bfd enable
[HUAWEI-Tunnel1] mpls te commit
```

9.3.115 mpls te bypass-attributes

Function

The **mpls te bypass-attributes** command configures the bypass tunnel attributes in the MPLS TE Auto FRR feature.

The **undo mpls te bypass-attributes** command restores the default settings.

By default, no bypass tunnel attributes in the MPLS TE Auto FRR feature are configured.

Format

mpls te bypass-attributes [**bandwidth** *bandwidth*] [**priority** *setup-priority* [*hold-priority*]]

undo mpls te bypass-attributes

Parameters

Parameter	Description	Value
bandwidth *bandwidth*	Specifies the bandwidth.	The value is an integer that ranges from 1 to 4000000000, in kbit/s.
setup-priority	Specifies the setup priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. The value is 7 by default.
hold-priority	Specifies the holding priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. The value is 7 by default.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

Before running the **mpls te bypass-attributes** command, you must run the **mpls te fast-reroute bandwidth** command to enable FRR function. The bandwidth of a bypass tunnel cannot be greater than that of the primary tunnel.

Precautions

The setup priority of a bypass tunnel cannot be higher than the holding priority. Both cannot be higher than the priorities of the primary tunnel.

On the same TE tunnel interface, the **mpls te bypass-attributes** command cannot be configured together with the **mpls te bandwidth (tunnel interface view)** command.

Example

Set the bandwidth of the bypass tunnel to 2048 kbit/s, the setup priority to 3, and the holding priority to 3.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bandwidth ct0 10000
[HUAWEI-Tunnel1] mpls te priority 3 3
[HUAWEI-Tunnel1] mpls te fast-reroute bandwidth
[HUAWEI-Tunnel1] mpls te bypass-attributes bandwidth 2048 priority 3 3
[HUAWEI-Tunnel1] mpls te commit
```

9.3.116 mpls te bypass-tunnel

Function

The **mpls te bypass-tunnel** command specifies the bypass tunnel for MPLS TE Auto FRR.

The **undo mpls te bypass-tunnel** command deletes the bypass tunnel configuration.

By default, no bypass tunnel for MPLS TE Auto FRR is specified.

Format

mpls te bypass-tunnel

undo mpls te bypass-tunnel

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The total bandwidth of LSPs protected by the bypass tunnel is not more than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system selects a single bypass tunnel through the best-fit algorithm.

If global Srefresh or RSVP GR needs to be enabled on the bypass PLR and MP node, configure the MPLS LSR ID of the destination peer FRR MP node as the destination address of the bypass tunnel.

NOTE

The **mpls te bypass-tunnel** command cannot be configured simultaneously with the following commands on the same tunnel interface:

- **mpls te fast-reroute**
- **mpls te backup**
- **mpls te protection tunnel**

Example

Configure the bypass tunnel on Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bypass-tunnel
[HUAWEI-Tunnel1] mpls te commit
```

9.3.117 mpls te commit

Function

The **mpls te commit** command commits the tunnel configurations to the system for processing.

Format

mpls te commit

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The configurations of an MPLS TE tunnel can only take effect after the **mpls te commit** command is run. The destination and tunnel ID must be configured;

otherwise, the commitment fails, and you need to configure both of them and then commit the configuration again. If the MPLS TE configuration changes, you must run the **mpls te commit** command to validate the modification.

NOTE

Each time the MPLS TE tunnel configuration is changed, the **mpls te commit** command must be run to make the modification take effect. If this command is not run, the changed configuration can be saved in the configuration file but cannot take effect.

Example

Configure an MPLS TE tunnel and then commit the configuration.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 10.2.2.9
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te commit
```

9.3.118 mpls te cspf

Function

The **mpls te cspf** command enables CSPF.

The **undo mpls te cspf** command disables CSPF.

CSPF is disabled by default.

Format

mpls te cspf

undo mpls te cspf

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

You must enable MPLS TE in the MPLS view before enabling CSPF.

CSPF provides a mechanism for selecting a path in an MPLS domain. You must enable CSPF before configuring CSPF functions.

Example

Enable CSPF.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te cspf
```

9.3.119 mpls te cspf disable

Function

The **mpls te cspf disable** command disables CSPF calculation when an LSP is being established in a TE tunnel.

The **undo mpls te cspf disable** command enables CSPF calculation when an LSP is being established in a TE tunnel.

By default, CSPF calculation is enabled when an LSP is being established in a TE tunnel.

Format

mpls te cspf disable

undo mpls te cspf disable

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After CSPF is enabled globally, CSPF calculation is triggered each time an LSP is being established in a TE tunnel. In the inter-AS VPN-OptionC scenario, no IGP is configured between two ASs, causing the TEDB to fail to be generated. As a result, CSPF calculation fails to be performed, and inter-area TE tunnels fail to be set up. Run the **mpls te cspf disable** command on the configured TE tunnel interface to disable CSPF calculation in the TE tunnel, and set up inter-area TE tunnels using direct routes or static routes.

Precautions

After the **mpls te cspf disable** command is run, CR-LSP selection functions, such as hop limit, CSPF tie-breaking, and SRLG, will become invalid.

Example

Disable CSPF calculation when an LSP is being established in a TE tunnel.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te cspf disable
[HUAWEI-Tunnel1] mpls te commit
```

9.3.120 mpls te cspf preferred-igp

Function

The **mpls te cspf preferred-igp** command specifies a preferred IGP for the CSPF calculation.

The **undo mpls te cspf preferred-igp** command restores the default settings.

The TEDB generated by OSPF is preferred by default.

Format

mpls te cspf preferred-igp { **isis** [*isis-process-id* [**level-1** | **level-2**]] | **ospf** [*ospf-process-id* [**area** { *area-id-1* | *area-id-2* }]] }

undo mpls te cspf preferred-igp

Parameters

Parameter	Description	Value
isis	Indicates that the TEDB generated by IS-IS is preferred.	-
isis-process-id	Specifies the process ID.	The value is an integer that ranges from 1 to 65535.
level-1	Indicates that the TEDB generated by a Level-1 IS-IS device is preferred.	-
level-2	Indicates that the TEDB generated by a Level-2 IS-IS device is preferred.	-
ospf	Indicates that the TEDB generated by OSPF is preferred.	-
ospf-process-id	Specifies the ID of an OSPF process.	The value is an integer that ranges from 1 to 65535.
area *area-id-1*	Specifies a preferred OSPF area configured in number format.	The value is an integer that ranges from 0 to 4294967295.
area *area-id-2*	Specifies a preferred OSPF area configured in IP address format.	The value is in dotted decimal notation.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When selecting a path, CSPF prefers the TEDB generated by OSPF to calculate a CR-LSP by default. When the OSPF TEDB can be used to calculate a path, the IS-IS TEDB is not used. If the calculation based on the OSPF TEDB fails, recalculation based on the IS-IS TEDB is performed.

You can run the **mpls te cspf preferred-igp** command to configure CSPF to prefer the TEDB generated by IS-IS when calculating a CR-LSR. In this case, the OSPF TEDB is only used to calculate a path when the path calculation based on the IS-IS TEDB fails.

Prerequisites

CSPF has been enabled using the **mpls te cspf** command.

Example

Configure CSPF to prefer the TEDB generated by OSPF when calculating a CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te cspf
[HUAWEI-mpls] mpls te cspf preferred-igp ospf
```

9.3.121 mpls te cspf timer failed-link

Function

The **mpls te cspf timer failed-link** command sets the timeout period of a failed-link timer.

The **undo mpls te cspf timer failed-link** command restores the default setting.

By default, the timeout period of the failed-link timer is 10 seconds.

Format

mpls te cspf timer failed-link *interval*

undo mpls te cspf timer failed-link

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a failed-link timer.	The value is an integer that ranges from 1 to 300, in seconds. The default value is 10.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A failed-link timer starts when a link goes Down.

- If an IGP deletes or modifies the link before the timer expires, CSPF is informed of the change. Then CSPF updates the link in the Traffic Engineering DataBase (TEDB) and terminates the timer.
- If IGP does not delete the link after the timer expires, the link goes Up.

Prerequisites

The CSPF function has been enabled by running the **mpls te cspf** command.

Example

Set the timeout period of the failed-link timer to 50 seconds.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te cspf
[HUAWEI-mpls] mpls te cspf timer failed-link 50
```

9.3.122 mpls te fast-reroute

Function

The **mpls te fast-reroute** command enables FRR.

The **undo mpls te fast-reroute** command disables FRR.

By default, FRR is disabled.

Format

mpls te fast-reroute [**bandwidth**]

undo mpls te fast-reroute

Parameters

Parameter	Description	Value
bandwidth	Indicates that bandwidth protection is needed.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

When FRR is enabled on a tunnel interface, the record route flag is automatically set as "record reroute with label", irrespective of the configuration of the **mpls te record-route label** command.

You must disable FRR If run the **mpls te record-route** or **undo mpls te record-route** command.

NOTE

- The **mpls te fast-reroute** command and the **mpls te resv-style ff** command cannot be configured together.
- The **mpls te fast-reroute** command and the **mpls te bypass-tunnel** command cannot be configured on the same tunnel interface.
- The **mpls te fast-reroute** command and the **mpls te protected-interface** command cannot be configured on the same tunnel interface.
- The **mpls te fast-reroute** command and the **mpls te protection tunnel** command cannot be configured for the protection tunnel in a tunnel protection group, whereas these two commands can be configured on the interface of the primary tunnel in the tunnel protection group.

Example

Enable FRR on Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te fast-reroute
[HUAWEI-Tunnel1] mpls te commit
```

9.3.123 mpls te hop-limit

Function

The **mpls te hop-limit** command limits the maximum number of hops of a CR-LSP.

The **undo mpls te hop-limit** command restores the default setting.

By default, the maximum number of hops of a CR-LSP is 32.

Format

mpls te hop-limit *hop-limit-value* [**best-effort** | **secondary**]

undo mpls te hop-limit [**best-effort** | **secondary**]

undo mpls te hop-limit *hop-limit-value* { **secondary** | **best-effort** }

Parameters

Parameter	Description	Value
hop-limit-value	Specifies the value of the hop limit.	The value is an integer that ranges from 1 to 32. The default value is 32.
best-effort	Indicates the hop limit of a best-effort path.	-
secondary	Indicates the hop limit of a backup CR-LSP.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After a CR-LSP is configured with a hop limit, the hop limit acts as one of routing conditions such as the link bandwidth and affinity property when the CR-LSP is created. After the hop limit is set, the number of hops of a CR-LSP cannot exceed this limit.

Example

Set the maximum number of hops of the primary CR-LSP, bypass CR-LSP, and best-effort path in hot-standby to 10.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te hop-limit 10
[HUAWEI-Tunnel1] mpls te hop-limit 10 secondary
[HUAWEI-Tunnel1] mpls te hop-limit 10 best-effort
[HUAWEI-Tunnel1] mpls te commit
```

9.3.124 mpls te hotstandby-lsp-constraint

Function

The **mpls te hotstandby-lsp-constraint** command allows you to use a CR-LSP attribute template to set up a hot-standby CR-LSP.

The **undo mpls te hotstandby-lsp-constraint** command deletes the used CR-LSP attribute template.

No CR-LSP attribute template is used to set up a hot-standby CR-LSP by default.

Format

mpls te hotstandby-lsp-constraint *number* { **dynamic** | **lsp-attribute** *lsp-attribute-name* }

undo mpls te hotstandby-lsp-constraint *number*

Parameters

Parameter	Description	Value
number	Specifies the number of a CR-LSP attribute template. It indicates the sequence of using each CR-LSP attribute template to set up a hot-standby CR-LSPs. The CR-LSP attribute templates are used in ascending order of their number.	The value is an integer ranging from 1 to 3.
dynamic	Indicates that when a hot-standby CR-LSP is being set up, it is assigned the same bandwidth and priority as the primary CR-LSP, but specified with a different path from the primary LSP.	-
lsp-attribute *lsp-attribute-name*	Specifies the name of a CR-LSP attribute template.	The value is an existing CR-LSP attribute template name.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

A maximum number of three CR-LSP attribute templates can be configured to set up hot-standby CR-LSPs. The hot-standby CR-LSPs must be consistent with the primary CR-LSP in the following attributes:

- Setup priority
- Holding priority
- Bandwidth type

In each of the three CR-LSP attribute template types corresponding to the primary CR-LSP, the hot-standby CR-LSP, and the ordinary backup CR-LSP respectively, only one attribute template can be specified with the **dynamic** parameter.

The parameter *number* is used to number each CR-LSP attribute template, which indicates the sequence of using each CR-LSP attribute template to set up a hot-standby CR-LSP. To set up a hot-standby CR-LSP, the system attempts to apply each CR-LSP attribute template by the template number in ascending order until a hot-standby CR-LSP is successfully up.

NOTE

- Before configuring the **mpls te hotstandby-lsp-constraint** command, you must run the **mpls te primary-lsp-constraint** command to use a CR-LSP attribute template to set up a primary CR-LSP.
- When the **mpls te hotstandby-lsp-constraint** command is configured to help set up a hot-standby CR-LSP, the **record-route** function is automatically enabled.

Example

Use the attribute template named t2 to set up a hot-standby CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te hotstandby-lsp-constraint 1 lsp-attribute t2
[HUAWEI-Tunnel1] mpls te commit
```

9.3.125 mpls te igp advertise

Function

The **mpls te igp advertise** command configures forwarding adjacency to take an MPLS TE tunnel as a virtual link and advertise the virtual link to an IGP network.

The **undo mpls te igp advertise** command restores the default configuration.

By default, forwarding adjacency to take an MPLS TE tunnel as a virtual link and advertise the virtual link to an IGP network is disabled.

Format

mpls te igp advertise [**hold-time** *interval*]

undo mpls te igp advertise

Parameters

Parameter	Description	Value
hold-time *interval*	Specifies the interval between the time when a TE tunnel goes Down and when the network is notified of the change.	The value is an integer that ranges from 0 to 4294967295 in milliseconds. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te igp advertise** command and the **mpls te igp shortcut** command cannot be configured simultaneously.

Example

Configure the forwarding adjacency and use the default hold time.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te igp advertise
[HUAWEI-Tunnel1] mpls te commit
```

9.3.126 mpls te igp metric

Function

The **mpls te igp metric** command specifies the MPLS TE tunnel metric for the SPF calculation in IGP shortcut or forwarding adjacency mode.

The **undo mpls te igp metric** command restores the default settings.

The TE tunnel metric is equal to the IGP metric of the TE tunnel by default.

Format

mpls te igp metric { **absolute** *absolute-value* | **relative** *relative-value* }

undo mpls te igp metric

Parameters

Parameter	Description	Value
absolute *absolute-value*	Specifies the absolute metric mode.	The value is an integer that ranges from 1 to 65535.
relative *relative-value*	Specifies the relative metric mode, indicating the offset value between the MPLS TE metric and the IGP metric.	The value is an integer that ranges from -10 to 10. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGP uses an auto route related to a CR-LSP in a TE tunnel that functions as a logical link to calculate a path. The tunnel interface is used as an outbound interface in the auto route. An auto route can work in IGP shortcut or forwarding adjacency mode. You can set a metric for a TE tunnel in either mode.

When specifying the metric for a TE tunnel in IGP shortcut mode, pay attention to the following points:

- If the **absolute** parameter is used, the metric of the TE tunnel is the set metric.
- If the **relative** parameter is used, the metric of the TE tunnel is the sum of the metric of the corresponding IGP path and relative metric.

A proper IGP metric for the TE tunnel in forwarding adjacency mode can ensure that the LSP be advertised and used correctly. For example, the metric of a TE tunnel should be less than the metric of an IGP route.

Precautions

When specifying an IGP metric for a TE tunnel in forwarding adjacency mode, select the **absolute** parameter if the IGP protocol is IS-IS.

Example

Set the MPLS TE tunnel metric to the IGP metric minus 1 in the SPF calculation.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te igp metric relative -1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.127 mpls te igp shortcut

Function

The **mpls te igp shortcut** command configures an IGP to use MPLS TE tunnels in the Up state for performing the enhanced SPF calculation.

The **undo mpls te igp shortcut** command restores the default configuration.

By default, an IGP does not use MPLS TE tunnels for performing the enhanced SPF calculation.

Format

mpls te igp shortcut [**isis** | **ospf**]

undo mpls te igp shortcut

Parameters

Parameter	Description	Value
isis	Indicates the IS-IS protocol.	-
ospf	Indicates the OSPF protocol.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te igp shortcut** command and the **mpls e igp advertise** command cannot be configured simultaneously.

Example

Configure OSPF or IS-IS to use Tunnel 1 in the enhanced SPF calculation if this tunnel is Up.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te igp shortcut
[HUAWEI-Tunnel1] mpls te commit
```

9.3.128 mpls te link administrative group

Function

The **mpls te link administrative group** command sets the value of the administrative-group attribute for an interface.

The **undo mpls te link administrative group** command restores the default setting.

The default administrative-group attribute is 0x0.

Format

mpls te link administrative group *value*

undo mpls te link administrative group

Parameters

Parameter	Description	Value
value	Specifies the link attributes compared with affinity bits during the selection of a path.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

After being advertised globally, interface attributes can work as a standard for the ingress of a tunnel to select a path.

The modification on the administrative-group attributes takes effect only on the LSPs created after the modification and does not affect the established LSPs.

The **mpls te link administrative group** command can be run on the outgoing interface of the link through which a TE tunnel passes.

Example

Set the administrative-group attribute to 0x0101 on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
```

```
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te link administrative group 101
```

Set the administrative-group attribute to 0x0101 on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te link administrative group 101
```

9.3.129 mpls te loop-detection

Function

The **mpls te loop-detection** command enables the loop detection function while a tunnel is being set up.

The **undo mpls te loop-detection** command disables this function.

The loop detection function is disabled by default.

Format

mpls te loop-detection

undo mpls te loop-detection

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

To prevent loops, you can run the **mpls te loop-detection** command on the ingress of the MPLS TE tunnel to enable the loop detection function.

Example

Enable the loop detection when an MPLS TE tunnel is being set up.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te loop-detection
[HUAWEI-Tunnel1] mpls te commit
```

9.3.130 mpls te metric

Function

The **mpls te metric** command configures the TE metric value of a link.

The **undo mpls te metric** command restores the default configuration.

The IGP metric value of a link is used as the TE metric value by default.

Format

mpls te metric *value*

undo mpls te metric

Parameters

Parameter	Description	Value
metric *value*	Specifies the TE metric of a link.	An integer ranging from 1 to 16777215.

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

If the IGP is OSPF and the current device is a stub router, the **mpls te metric** command does not take effect.

Example

Set the TE metric of the link to 20 on interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te metric 20
```

Set the TE metric of the link to 20 on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te metric 20
```

9.3.131 mpls te ordinary-lsp-constraint

Function

The **mpls te ordinary-lsp-constraint** command allows you to use a CR-LSP attribute template to set up an ordinary backup CR-LSP.

The **undo mpls te ordinary-lsp-constraint** command deletes a used CR-LSP attribute template.

No CR-LSP attribute template is used to set up an ordinary backup CR-LSP by default.

Format

mpls te ordinary-lsp-constraint *number* { **dynamic** | **lsp-attribute** *lsp-attribute-name* }

undo mpls te ordinary-lsp-constraint *number*

Parameters

Parameter	Description	Value
number	Specifies the number of a CR-LSP attribute template. The CR-LSP attribute templates are used to set up ordinary backup CR-LSPs in sequence of ascending number.	An integer ranging from 1 to 3.
dynamic	Indicates that when an ordinary backup CR-LSP is being set up, it is assigned the same bandwidth and priority as the primary CR-LSP.	-
lsp-attribute *lsp-attribute-name*	Specifies the name of a CR-LSP attribute template.	It is a string of 1 to 31 characters.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

A maximum number of three CR-LSP attribute templates can be configured to set up an ordinary backup CR-LSP. The ordinary backup CR-LSPs must be consistent with the primary CR-LSP in the following attributes:

- Setup priority

- Holding priority
- Bandwidth type

Among the three CR-LSP attribute templates corresponding to a primary CR-LSP and ordinary backup CR-LSP, only one CR-LSP attribute template can be specified with the **dynamic** parameter.

The parameter *number* is used to number each CR-LSP attribute template. The CR-LSP attribute templates are each applied by the system in sequence of ascending number until an ordinary backup CR-LSP is set up.

NOTE

- Before running the **mpls te ordinary-lsp-constraint** command, you must run the **mpls te primary-lsp-constraint** command to use a CR-LSP attribute template to set up a primary CR-LSP.
- When the **mpls te ordinary-lsp-constraint** command is run to help set up an ordinary backup CR-LSP, the **record route** function is automatically enabled.

Example

Use the attribute template named t3 to set up an ordinary backup CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te ordinary-lsp-constraint 1 lsp-attribute t3
[HUAWEI-Tunnel1] mpls te commit
```

9.3.132 mpls te path explicit-path

Function

The **mpls te path explicit-path** command configures an explicit path for a tunnel.

The **undo mpls te path** command deletes a configured explicit path.

By default, no explicit path for a tunnel is configured.

Format

mpls te path explicit-path *path-name* [**secondary**]

undo mpls te path [**secondary**]

undo mpls te path explicit-path *path-name* **secondary**

Parameters

Parameter	Description	Value
path-name	Specifies the name of the explicit path for a tunnel.	The value is an existing explicit path name.

Parameter	Description	Value
secondary	Indicates that the explicit path is configured for a backup tunnel. The parameter is applied only to configuring a backup CR-LSP using the **mpls te backup** command.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te path explicit-path** command can be run successfully only after an explicit path is set up by running the **explicit-path** command in the system view, and the nodes on the path are specified.

Example

Apply the explicit path named path1 to Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] explicit-path path1
[HUAWEI-explicit-path-path1] next hop 10.2.2.9
[HUAWEI-explicit-path-path1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te path explicit-path path1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.133 mpls te path metric-type

Function

The **mpls te path metric-type** command specifies a link metric type used to select a path for a tunnel without any metric type.

The **undo mpls te path metric-type** command restores the default settings.

The TE metric is used to select a path for a tunnel by default.

Format

mpls te path metric-type { **igp** | **te** }

undo mpls te path metric-type

Parameters

Parameter	Description	Value
igp	Indicates that the IGP metric is used.	-
te	Indicates that the TE metric is used.	-

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If the **mpls te path metric-type** command is not configured in the tunnel interface view, the metric type set in the MPLS view is used. Otherwise, the metric type set in the tunnel interface view will be used.

Example

Adopt the IGP metric that is used to select a path for the tunnel that is not configured with any metric type.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te path metric-type igp
```

Adopt the TE metric that is used to select a path for Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te path metric-type te
[HUAWEI-Tunnel1] mpls te commit
```

9.3.134 mpls te path-selection overload

Function

The **mpls te path-selection overload** command associates CR-LSP establishment with the IS-IS overload setting. This association allows CSPF to calculate paths excluding overloaded IS-IS nodes.

The **undo mpls te path-selection** command restores the default configuration.

By default, CR-LSP establishment is not associated with the IS-IS overload setting.

Format

mpls te path-selection overload

undo mpls te path-selection

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrator can run the **set-overload** command to mark a node overloaded if the node is transmitting a large number of services or its CPU is overburdened. If there are overloaded nodes on an MPLS TE network, associate CR-LSP establishment with the IS-IS overload setting to ensure that CR-LSPs are established over paths excluding overloaded nodes. This configuration prevents overloaded nodes from being further burdened and improves CR-LSP reliability.

Prerequisites

The route record has been enabled using the **mpls te record-route** command.

Precautions

The **mpls te path-selection overload** command has the following influences on the CR-LSP establishment:

- CSPF recalculates paths excluding overloaded nodes for established CR-LSPs.

  NOTE

  Traffic travels through an existing CR-LSP before a new CR-LSP is established. After the new CR-LSP is established, traffic is switched to the new CR-LSP and the original CR-LSP is deleted. This traffic switchover is performed based on the Make-Before-Break mechanism. Traffic is not dropped during the switchover.

- CSPF calculates paths excluding overloaded nodes for new CR-LSPs.

This command does not take effect on bypass tunnels.

If the ingress or egress is marked overloaded, the **mpls te path-selection overload** command does not take effect. The established CR-LSPs associated with the ingress or egress will not be reestablished and new CR-LSPs associated with the ingress or egress will also not be established.

If a TE LSP uses the local device as a transit node before the **set-overload** command is run, the TE LSP is not torn down and re-established and still uses the local device as a transit node after the **set-overload** command is run; if the local device is restarted after the command is run and fast convergence is not configured on the ingress of the RSVP-LSP, TE LSP forwarding fails, and services are affected. Therefore, the **mpls te path-selection overload** command needs to be run on the ingress of the RSVP-LSP before the device is restarted.

Example

Associate CR-LSP establishment with the IS-IS overload setting.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te path-selection overload
```

9.3.135 mpls te primary-lsp-constraint

Function

The **mpls te primary-lsp-constraint** command allows you to use a CR-LSP attribute template to set up a primary CR-LSP.

The **undo mpls te primary-lsp-constraint** command restores the default configuration.

No CR-LSP attribute template is used to set up a primary CR-LSP by default.

Format

mpls te primary-lsp-constraint { **dynamic** | **lsp-attribute** *lsp-attribute-name* }

undo mpls te primary-lsp-constraint

Parameters

Parameter	Description	Value
dynamic	Indicates that when a CR-LSP attribute template is used to set up a primary CR-LSP, all attributes in the attribute template use the default values.	-
lsp-attribute *lsp-attribute-name*	Specifies the name of a CR-LSP attribute template.	The value is an existing CR-LSP attribute template name.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

A CR-LSP attribute template already configured with the bandwidth and priority can be referenced to set up CR-LSPs in batches, greatly simplifying configurations of CR-LSPs.

If the TE attribute configured in the tunnel interface view and that configured through a CR-LSP attribute template coexist, the former takes precedence over the latter.

Example

Use the attribute template named **t1** to set up a primary CR-LSP.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te primary-lsp-constraint lsp-attribute t1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.136 mpls te priority

Function

The **mpls te priority** command configures the setup priority and holding priority for an MPLS TE tunnel.

The **undo mpls te priority** command restores the default settings.

The default setup and holding priority for an MPLS TE tunnel are both 7.

Format

mpls te priority *setup-priority* [*hold-priority*]

undo mpls te priority

Parameters

Parameter	Description	Value
setup-priority	Specifies the setup priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority.
hold-priority	Specifies the holding priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. Its value is the same as the setup priority by default.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bandwidth resources on a link cannot satisfy the requirements for establishing all CR-LSPs, you can specify the setup and holding priorities for certain CR-LSPs. In this manner, the CR-LSPs with higher priorities can be established by preempting bandwidth resources of CR-LSPs with lower priorities before transmitting certain user services.

Priorities of a CR-LSP consist of the setup priority and holding priority, representing the preemption relationship between a CR-LSP to be established and an established CR-LSP. If the setup priority of a CR-LSP to be established is higher than the holding priority of an established CR-LSP, the CR-LSP to be established can preempt the bandwidth resources of the established one.

The default setup and holding priorities of CR-LSPs are 7, the lowest priority value. Default priorities take effect on all CR-LSPs if no priorities are specified. These CR-LSPs with the default priorities are at the risk of being preempted by those with higher priorities.

Precautions

During the planning of a network, it is recommended that the setup and holding priorities of all CR-LSPs be strictly planned. To preferentially transmit services over a CR-LSP, you can set the higher setup and holding priorities for the CR-LSP, preventing unwanted bandwidth preemption. The same setup and holding priorities are set for CR-LSPs which are transmitting services with the same priority, also preventing bandwidth preemption.

In addition, on one TE tunnel, its setup priority must be less than or equal to its holding priority. This ensures that CR-LSPs in the tunnel can be successfully set up, and prevents CR-LSP flapping caused by bandwidth preemption between CR-LSPs.

NOTICE

After the priorities of an existing CR-LSP have been changed, the existing CR-LSP will be deleted and a new one will be established. Therefore, back up CR-LSPs with lower priorities before setting higher priorities for a certain CR-LSP.

Example

Set the setup priority and the holding priority to 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te priority 1
[HUAWEI-Tunnel1] mpls te commit
```

9.3.137 mpls te protected-interface

Function

The **mpls te protected-interface** command specifies an interface to be protected by a bypass tunnel.

The **undo mpls te protected-interface** command delete an interface protected by a bypass tunnel.

By default, no interface to be protected by a bypass tunnel is specified.

Format

mpls te protected-interface *interface-type interface-number*

undo mpls te protected-interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be protected. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te protected-interface** command must be configured together with the **mpls te bypass-tunnel** command on the same tunnel interface. Otherwise, the configured **mpls te protected-interface** command cannot take effect.

Currently, a bypass tunnel can protect up to six interfaces that must be enabled with MPLS TE.

NOTE

If a tunnel interface is configured with the **mpls te protected-interface** command, it cannot be configured with the **mpls te backup** or **mpls te fast-reroute** command.

Example

Use Tunnel 1 as a bypass tunnel of VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te protected-interface vlanif 100
[HUAWEI-Tunnel1] mpls te commit
```

9.3.138 mpls te protect-switch

Function

The **mpls te protect-switch** command configures the manual switching mode for a specified tunnel.

The **mpls te protect-switch clear** and **undo mpls te protect-switch** commands delete the manual switching mode for a specified tunnel.

By default, no manual switching mode for a specified tunnel is configured.

Format

mpls te protect-switch { **force** | **lock** | **manual** }

mpls te protect-switch clear

undo mpls te protect-switch

Parameters

Parameter	Description	Value
force	Forcibly directs traffic to a protection tunnel.	-
lock	Locks traffic in the working tunnel. Being locked, traffic cannot be switched to a protection tunnel even if the working tunnel fails.	-
manual	Enables manual switching.	-
clear	Deletes the switching request manually configured on the current tunnel.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an LSP fault is detected, traffic switching is automatically triggered in a tunnel protection group. Alternatively, run the **mpls te protect-switch** command to trigger traffic switching.

MPLS OAM supports multiple traffic switching modes. These switching modes are prioritized. A newly configured switching mode takes effect only if its priority is higher than that of the existing switching mode.

The traffic switching modes are prioritized in descending order when the protection tunnel is Up:

- Force switching mode: has the highest priority. If force switching is configured, traffic is forced to switch to a protection tunnel and does not switch back even if the working tunnel recovers. Both the **mpls te protect-switch force** command and the **mpls te protect-switch lock** command can trigger force switching, but force switching triggered by the latter command has a higher priority.

- Signal failure mode: automatically triggers traffic switching if an LSP fault is detected.
- Manual switching mode: manually switches traffic to a protection tunnel.
- WTR mode: switches traffic back to a working tunnel after the WTR time expires. Although the WTR time is set, if a command is run to manually switch traffic, traffic will be switched immediately before the WTR time expires.

If a new local or remote request has a higher priority than an existing request manually configured using the **mpls te protect-switch** command, the APS state machine is changed, and the manual switching command is deleted. In the **mpls te protect-switch** command, the **force** and **manual** parameters, except the **lock** parameter, configure lower priority requests. After the **mpls te protect-switch** command with **force** or **manual** configured is run, the command is lost after a device is restarted. This situation is normal, in compliance with Recommendation G.8131.

Prerequisites

A tunnel protection group has been created by running the **mpls te protection tunnel** command.

Follow-up Procedure

The **mpls te protect-switch clear** command can be used to cancel force or manual switching.

Example

Switch traffic to the protection tunnel manually on Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te protect-switch manual
```

Delete the traffic switching to the protection tunnel on Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] mpls te protect-switch clear
```

9.3.139 mpls te protection tunnel

Function

The **mpls te protection tunnel** command creates a tunnel protection group by binding a configured protection tunnel to a primary tunnel.

The **undo mpls te protection tunnel** command deletes the binding between the protection tunnel and the primary tunnel.

By default, no protection tunnel group is created.

Format

mpls te protection tunnel *tunnel-id* [**holdoff** *holdoff-time*] [**mode** { **non-revertive** | **revertive** [**wtr** *wtr-time*] }]

undo mpls te protection tunnel

Parameters

Parameter	Description	Value
tunnel-id	Specifies the ID of a protection tunnel.	The value is an integer that ranges from 1 to 10000.
holdoff *holdoff-time*	Specifies the delay time. When a fault on a primary tunnel is detected, the switchover is performed after the delay time expires.	The value is an integer that ranges from 0 to 100 with the step of 100 milliseconds. The maximum delay time is 10 seconds. By default, the value is 10, indicating that the switchover is performed immediately after a fault on the primary tunnel is detected.
mode	Specifies the revertive mode. ● **non-revertive**: The current mode cannot be switched to the original mode. ● **revertive**: The current mode can be switched to the original mode.	By default, the revertive mode is used.
wtr *wtr-time*	Specifies the WTR time for the switchback. When a primary tunnel recovers from a fault, the switchback is performed after the WRT time expires.	The value is an integer that ranges from 0 to 60, with the increment of 30 seconds. By default, the value is 24, that is, 12 minutes.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

In addition to configuring a tunnel protection group to protect a working tunnel, you can configure TE FRR on the working tunnel. In this manner, the working tunnel can work under dual protection. The protection tunnel, however, cannot function as the working tunnel that is protected by another tunnel. In addition, the protection tunnel cannot be enabled with TE FRR.

After creating a protection tunnel in the tunnel interface view, you must run the **mpls te commit** command to commit the configuration.

NOTE

Tunnel protection group and TE FRR cannot be configured simultaneously on the ingress of a primary tunnel.

Example

Configure a protection tunnel for Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te protection tunnel 239 holdoff 100 mode revertive wtr 30
[HUAWEI-Tunnel1] mpls te commit
```

9.3.140 mpls te record-route

Function

The **mpls te record-route** command enables the system to record routes and labels during tunnel establishment.

The **undo mpls te record-route** command configures the system not to record routes and labels during tunnel establishment.

By default, the system does not record routes and labels during tunnel establishment.

Format

mpls te record-route [**label**]

undo mpls te record-route

Parameters

Parameter	Description	Value
label	Indicates that a label is also recorded when the system records a route.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an MPLS TE tunnel is not established over an explicit path, the system does not record detailed path information. In this case, to view detailed path information about the tunnel, run this command on a tunnel interface. After the configuration, RROs are carried in Path and Resv messages and record the IP address of each hop along the tunnel. In addition, the keyword **label** can be configured to record the label of each hop along the tunnel.

Precautions

After the **mpls te record-route** command is configured and the MPLS TE tunnel is established, the **display mpls te tunnel path** command can be run to display detailed path information about the tunnel.

Do not run the **mpls te record-route** command on a large-scale network. On such a network, a large number of hops exist along a tunnel. Running this command allows the Path and Resv messages to carry RROs that record the IP address of each hop along the tunnel. As a result, the Path or Resv message will be oversized, lowering the system performance.

NOTE

After the **mpls te fast-reroute**, **mpls te backup**, or **mpls te bypass-tunnel** command has been configured on a tunnel interface, the route record function is automatically enabled.

Example

Enable the system to record routes and labels during tunnel establishment.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te record-route label
[HUAWEI-Tunnel1] mpls te commit
```

9.3.141 mpls te reoptimization (user view)

Function

The **mpls te reoptimization** command immediately triggers re-optimization for an MPLS TE tunnel.

Format

mpls te reoptimization [**tunnel** *interface-number*]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies a tunnel that needs immediate re-optimization.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The manual re-optimization function is used in either of the following situations:

- After the network topology is modified manually, a new optimal path will be calculated. The new optimal path needs to be immediately used by the TE tunnel.
- TE tunnels need to be immediately optimized in batches, optimizing resources of these TE tunnels in time.

If you run the **mpls te reoptimization** command without specifying the **tunnel** *interface-number* parameter, all TE tunnels are optimized. If you run the **mpls te reoptimization** command and specify the **tunnel** *interface-number* parameter, the specified TE tunnels are optimized.

Re-optimization of a TE tunnel can be performed in either of the following modes:

- Automatic re-optimization: means that the TE tunnel is periodically optimized, saving manpower. To enable automatic re-optimization, run the **mpls te reoptimization (tunnel interface view)** command in the tunnel interface view. In addition, this command takes effect only on an established TE tunnel.
- Manual re-optimization: means that the TE tunnel is immediately optimized. To immediately optimize the TE tunnel, run the **mpls te reoptimization** command in the user view.

Precautions

- If the re-optimization function is configured after an explicit path is configured and a new path fails to meet the explicit path constraints, the re-optimization function will not take effect.
- After a TE tunnel is configured with the re-optimization function, the tie-breaking in most-fill mode will not be supported.
- The **mpls te reoptimization** command cannot be run together with the following commands:
  - **mpls te route-pinning**
  - **mpls te resv-style ff**

Example

Immediately re-optimize all the TE tunnels on the local device.

```
<HUAWEI> mpls te reoptimization
```

9.3.142 mpls te reoptimization (tunnel interface view)

Function

The **mpls te reoptimization** command enables automatic re-optimization for a TE tunnel.

The **undo mpls te reoptimization** command restores the default setting.

By default, automatic re-optimization for a TE tunnel is disabled.

Format

mpls te reoptimization [**frequency** *interval*]

undo mpls te reoptimization

Parameters

Parameter	Description	Value
frequency *interval*	Specifies the interval for re-optimization. The system calculates the path for a TE tunnel based on constraints at the intervals of *interval*. If a better path to the same destination is calculated, the TE tunnel will be re-established over the better path.	The value is an integer that ranges from 60 to 604800, in seconds. By default, the interval is 3600 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a better path is calculated, to allow a TE tunnel to be automatically re-established over the better path, the **mpls te reoptimization** command needs to be run in the tunnel interface view. In this manner, after a better path to the same destination has been calculated for a certain reason such as the change of the cost, the TE tunnel can be automatically re-established, optimizing the resources on the network.

Re-optimization of a TE tunnel can be performed in either of the following modes:

- Automatic re-optimization: means that the TE tunnel is periodically optimized, saving manpower. To enable automatic re-optimization, run the **mpls te reoptimization** command in the tunnel interface view. In addition, this command takes effect only on an established TE tunnel.
- Manual re-optimization: means that the TE tunnel is immediately optimized. To immediately optimize the TE tunnel, run the **mpls te reoptimization** command in the user view.

Prerequisites

CSPF has been enabled by running the **mpls te cspf** command.

Precautions

- If the re-optimization function is configured after an explicit path is configured and a new path fails to meet the explicit path constraints, the re-optimization function will not take effect.
- After a TE tunnel is configured with the re-optimization function, the tie-breaking in most-fill mode will not be supported.
- The **mpls te reoptimization** command cannot be run together with the following commands:
  - **mpls te route-pinning**
  - **mpls te resv-style ff**

Example

Enable periodic re-optimization for a TE tunnel named Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te reoptimization frequency 43200
[HUAWEI-Tunnel1] mpls te commit
```

9.3.143 mpls te resv-style

Function

The **mpls te resv-style** command specifies a reservation style.

The **undo mpls te resv-style** command restores the default setting.

The default reservation style is SE.

Format

mpls te resv-style { **ff** | **se** }

undo mpls te resv-style

Parameters

Parameter	Description	Value
ff	Indicates the style of fixed filter.	-
se	Indicates the style of shared explicit.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

RSVP-TE only supports two resources reservation styles: FF and SE.

NOTE

The **mpls te resv-style ff** command cannot be configured simultaneously with the following commands: **mpls te fast-reroute**, **mpls te backup**, and **mpls te reoptimization (tunnel interface view)**.

Example

Set up a CR-LSP with the resource reservation style being FF.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te signal-protocol rsvp-te
[HUAWEI-Tunnel1] mpls te resv-style ff
[HUAWEI-Tunnel1] mpls te commit
```

9.3.144 mpls te route-pinning

Function

The **mpls te route-pinning** command enables the route pinning function.

The **undo mpls te route-pinning** command disables this function.

Route pinning is disabled by default.

Format

mpls te route-pinning

undo mpls te route-pinning

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te route-pinning** command cannot be configured simultaneously the **mpls te reoptimization (tunnel interface view)** command.

Example

Enable route pinning function.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te route-pinning
[HUAWEI-Tunnel1] mpls te commit
```

9.3.145 mpls te signal-protocol

Function

The **mpls te signal-protocol** command specifies a signaling protocol to set up an LSP.

The **undo mpls te signal-protocol** command deletes the signaling protocol to set up an LSP.

The default signaling protocol used to set up an LSP is RSVP-TE.

Format

mpls te signal-protocol { **cr-static** | **rsvp-te** | **static** }

undo mpls te signal-protocol { **cr-static** | **static** }

Parameters

Parameter	Description	Value
cr-static	Uses static CR-LSPs to establish TE tunnels.	-
rsvp-te	Uses RSVP-TE as the signaling protocol.	-
static	Uses static LSPs to establish TE tunnels.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

When configuring MPLS TE, you can run this command to specify a signaling protocol to set up a tunnel.

- When configuring a static MPLS TE tunnel, the signaling protocol used is **cr-static**.
- When configuring a dynamic MPLS TE tunnel, the signaling protocol used is **rsvp-te**.

Example

Use RSVP-TE as the signaling protocol for MPLS TE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te signal-protocol rsvp-te
[HUAWEI-Tunnel1] mpls te commit
```

9.3.146 mpls te signaling-delay-trigger enable

Function

The **mpls te signaling-delay-trigger enable** command enables the RSVP signaling delay-trigger function.

The **undo mpls te signaling-delay-trigger enable** command disables the RSVP signaling delay-trigger function.

The RSVP signaling delay-trigger function is disabled by default.

Format

mpls te signaling-delay-trigger enable

undo mpls te signaling-delay-trigger enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a fault occurs on an MPLS network and a large number of RSVP CR-LSPs need to be re-established, a large amount of system resources may be required. In this case, after the RSVP signaling delay-trigger function is configured, the interval between re-establishments of a CR-LSP is prolonged so that system resources are saved.

Prerequisites

Before running the **mpls te signaling-delay-trigger enable** command, the **mpls te** command must be run in the MPLS view.

Precautions

Use caution when configuring the RSVP signaling delay-trigger function because it causes the delay of CR-LSP convergence. The default settings are recommended.

Example

Enable the RSVP signaling delay-trigger function.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te signaling-delay-trigger enable
```

9.3.147 mpls te signalled tunnel-name

Function

The **mpls te signalled tunnel-name** command configures the name of a TE tunnel.

The **undo mpls te signalled tunnel-name** command deletes the configured name of the TE tunnel.

By default, the name of a TE tunnel is not configured.

Format

mpls te signalled tunnel-name *tunnel-name*

undo mpls te signalled tunnel-name

Parameters

Parameter	Description	Value
tunnel-name	Specifies the name of a TE tunnel.	A string of 1 to 63 case-sensitive characters, spaces or slashes (/) not supported. The initial character must be an underscore (_) or an English letter, not a digit.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A tunnel interface name is used as a tunnel name by default, for example, Tunnel1. Alternatively, if you want to customize a name for a TE tunnel, the **mpls te signalled tunnel-name** command can be used to configure a TE tunnel name. For example, a TE tunnel from LSR A to LSR C is named LSRAtoLSRC.

Prerequisites

MPLS TE has been enabled using the **mpls te** command.

Precautions

A TE tunnel name must be unique on an entire device.

If a TE tunnel name is specified, RSVP signaling messages will carry the specified name. If a configured TE tunnel name is deleted or no TE tunnel name is specified, RSVP signaling messages will carry the TE tunnel interface name as the TE tunnel name.

The **mpls te signalled tunnel-name** command or its undo form takes effect on a TE tunnel established using only RSVP signaling, not a static route.

Example

Name a TE tunnel **LSRAtoLSRC**.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te signalled tunnel-name LSRAtoLSRC
[HUAWEI-Tunnel1] mpls te commit
```

9.3.148 mpls te srlg

Function

The **mpls te srlg** command configures an interface as an SRLG member.

The **undo mpls te srlg** command deletes an interface from an SRLG.

No interface is added to any SRLG by default.

Format

mpls te srlg *srlg-number*

undo mpls te srlg { *srlg-number* | **all** }

Parameters

Parameter	Description	Value
srlg-number	Specifies the number of the SRLG to which an interface belongs.	The value is an integer that ranges from 0 to 4294967295.
all	Indicates that all SRLG configurations are deleted from an interface.	-

Views

VLANIF interface view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SRLG, like the bandwidth and affinity property, is a constraint in path calculation. If SRLG is configured for links, an IGP floods the TE link information along with the SRLG membership information to all devices in an IGP area. The SRLG membership information is also added into the TEDB.

Prerequisites

Before running the **mpls te srlg** command, the **mpls te** command must be run in the interface view.

Precautions

If SRLG is configured for links and the **mpls te srlg path-calculation** command is configured on the ingress of the primary tunnel, when calculating the path of a bypass tunnel or a hot-standby tunnel, CSPF determines whether the SRLG attribute is used as a constraint according to the configured SRLG calculation mode.

One interface can join multiple SRLGs.

Example

Add VLANIF100 to SRLG 1 and SRLG 2.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls te srlg 1
[HUAWEI-Vlanif100] mpls te srlg 2
```

Add GE0/0/1 to SRLG 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls te srlg 1
```

9.3.149 mpls te srlg path-calculation

Function

The **mpls te srlg path-calculation** command configures an SRLG-based path calculation mode.

The **undo mpls te srlg path-calculation** command deletes an SRLG-based path calculation mode.

By default, when calculating a path, CSPF does not consider an SRLG constraint or check whether the primary CR-LSP and a Bypass CR-LSP or a hot-standby CR-LSP are in the same SRLG.

Format

mpls te srlg path-calculation [**strict** | **preferred**]

undo mpls te srlg path-calculation

Parameters

Parameter	Description	Value
strict	Indicates that CSPF must calculate a bypass CR-LSP or a hot-standby CR-LSP according to the SRLG attribute. The link that the primary path uses and the link that the bypass CR-LSP or hot-standby CR-LSP uses cannot be in the same SRLG. **NOTE** After you specify this parameter, all the links on the primary CR-LSP regardless of whether the SRLG attribute is configured cannot be used for calculation of the bypass or hot-standby CR-LSP. However, nodes on the primary CR-LSP can be used in CSPF calculation.	-
preferred	Indicates that CSPF prefers the SRLG attribute the first time it calculates a Bypass CR-LSP or hot-standby CR-LSP. If the initial calculation fails, the CSPF does not use the SRLG attribute as a constraint. **NOTE** If no path calculation mode is specified in the **mpls te srlg path-calculation** command, SRLG-based path calculation is performed in preferred mode by default.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the TE FRR or hot standby scenario, to enable CSPF to calculate a path for a Bypass CR-LSP or a hot-standby CR-LSP based on the SRLG attribute, you must run the **mpls te srlg path-calculation** command on the ingress of the tunnel.

The SRLG, like the bandwidth and affinity property, is a constraint in path calculation. If SRLG is configured for links and the **mpls te srlg path-calculation** command is configured on the ingress of the primary CR-LSP, when calculating the path of a Bypass CR-LSP or a hot-standby tunnel, CSPF determines whether the SRLG attribute is used as a constraint according to the configured SRLG calculation mode.

Precautions

If **strict** is configured, CSPF always considers SRLG as a constraint.

If **preferred** is configured, the first time that CSPF calculates a path is according to the SRLG attribute. If the calculation fails, CSPF tries to calculate again without considering SRLG.

Example

Enable path calculation in **strict** mode.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te srlg path-calculation strict
```

9.3.150 mpls te switch-delay

Function

The **mpls te switch-delay** command sets the switching and deletion delays for a TE tunnel.

The **undo mpls te switch-delay** command restores the default settings.

By default, the switching delay is 5000 milliseconds and the deletion delay is 7000 milliseconds.

Format

mpls te switch-delay *switch-time* **delete-delay** *delete-time*

undo mpls te switch-delay *switch-time* **delete-delay** *delete-time*

Parameters

Parameter	Description	Value
switch-delay *switch-time*	Specifies the time period that the TE traffic is switched from the primary CR-LSP to the Modified CR-LSP.	The value is an integer that ranges from 0 to 600000, in milliseconds. The default value is 5000.
delete-delay *delete-time*	Specifies the delay for deleting the primary CR-LSP after the TE traffic is switched to a Modified CR-LSP.	The value is an integer that ranges from 0 to 600000, in milliseconds. The default value is 7000.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TE uses the Make-Before-Break mechanism. When the attributes of an MPLS TE tunnel such as bandwidth and path change, a new CR-LSP with new attributes, also called Modified CR-LSP, must be established.

On the same modified CR-LSP, when a downstream LSR is too busy but the upstream LSR is not as busy, the Modified CR-LSP may go Up earlier on the upstream LSR than on the downstream LSR. The upstream LSR switches traffic to the Modified CR-LSP but the Modified CR-LSP is not Up on the downstream LSR. This causes a momentary traffic interruption. You can set a suitable switching delay time to avoid the traffic interruption.

If a modified CR-LSP fails, the failed node sends PathErr messages to its upstream LSRs and deletes the Modified CR-LSP, and traffic should be switched back to the primary CR-LSP. In applications, when detecting the fault, the upstream LSRs of the failed node are too occupied to forward the PathErr messages. This causes a traffic interruption on the failed node because the primary CR-LSP is deleted on the failed node. You can set a suitable deletion delay time to prevent the traffic interruption.

NOTE

In a VPLS over MPLS TE scenario, you can configure TE FRR to improve network reliability. TE FRR protects links and nodes on an MPLS TE tunnel. If a link or node fails, TE FRR rapidly switches traffic to the protection path. However, traffic loss may occur during a traffic switchback if the delay for deleting the TE FRR protection path is too short. To prevent this situation, run the **delete-delay** *delete-time* command to configure an appropriate delay based on the number of VSIs on the MPLS TE tunnel:

- 30s if there are 2001 to 4000 VSIs
- 20s if there are 1001 to 2000 VSIs
- 10s if there are 501 to 1000 VSIs
- 7s if there are 1 to 500 VSIs

Prerequisites

MPLS TE has been enabled globally by running the **mpls te** command.

Example

Set the switching delay of the TE tunnel to 3000 milliseconds and the deletion delay of the TE tunnel to 8000 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te switch-delay 3000 delete-delay 8000
```

9.3.151 mpls te tie-breaking

Function

The **mpls te tie-breaking** command configures a rule for selecting a route among multiple available equal-cost routes to the destination.

The **undo mpls te tie-breaking** command restores the default settings.

By default, tie-breaking policy is random.

Format

mpls te tie-breaking { **least-fill** | **most-fill** | **random** }

undo mpls te tie-breaking

Parameters

Parameter	Description	Value
least-fill	Selects the route with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.	-
most-fill	Selects the route with the largest ratio of the occupied bandwidth to the maximum reservable bandwidth.	-
random	Selects a route randomly.	-

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The route is selected based on the ratio of the occupied available bandwidth to the maximum reservable bandwidth. If **least-fill** is configured, the route with the smallest ratio is selected; if **most-fill** is configured, the route with the largest ratio is selected.

Prerequisites

MPLS TE has been enabled by running the **mpls te** command.

Precautions

Note that the link is selected according to a ratio through the tie-breaking mechanism. In the case that the ratios are the same when the reservable bandwidth is not used or the same reservable bandwidth is used on the links, the first found link is used regardless of whether **least-fill** or **most-fill** is configured.

NOTE

A tunnel prefers the route-selecting rule configured in the local tunnel interface view. If no rule is configured in the tunnel interface view, the rule configured in the MPLS view is used.

Example

Select the path with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te tie-breaking least-fill
[HUAWEI-Tunnel1] mpls te commit
```

Select the path with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te tie-breaking least-fill
```

9.3.152 mpls te timer auto-bandwidth

Function

The **mpls te timer auto-bandwidth** command enables automatic bandwidth adjustment and samples the output rate for tunnels.

The **undo mpls te timer auto-bandwidth** command disables automatic bandwidth adjustment.

By default, automatic bandwidth adjustment is not enabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, and S6730S-H support this command.

Format

mpls te timer auto-bandwidth [*interval*]

undo mpls te timer auto-bandwidth

Parameters

Parameter	Description	Value
interval	Specifies the interval for sampling the output rate of each tunnel configured with automatic bandwidth adjustment.	The value is an integer that ranges from 1 to 604800 in seconds. The default value is 300 seconds, and is a recommended value.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Before a sampling interval is changed, the **undo mpls te timer auto-bandwidth** command must be run. Then the **mpls te timer auto-bandwidth** command is run to set an interval.

Example

Sample the output rate of the MPLS TE tunnel every 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls te timer auto-bandwidth 600
```

9.3.153 mpls te timer fast-reroute

Function

The **mpls te timer fast-reroute** command sets the interval at which the binding between a bypass CR-LSP and a primary CR-LSP is refreshed.

The **undo mpls te timer fast-reroute** command restores the default configuration.

By default, the time weight used to calculate the interval is 300. And the actual interval at which the binding between a bypass CR-LSP and a primary LSP is refreshed depends on device performance and the maximum number of LSPs that can be established on the device.

Format

mpls te timer fast-reroute [*weight*]

undo mpls te timer fast-reroute

Parameters

Parameter	Description	Value
weight	Specifies the weight value used to calculate the interval at which the binding between a bypass CR-LSP and a primary LSP is refreshed.	The value is an integer that ranges from 0 to 604800. **NOTE** If *weight* is not specified, the default weight value is 300.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After TE FRR is configured, a PLR refreshes the binding between a bypass CR-LSP and a primary CR-LSP at a specified interval. The PLR searches for the optimal bypass CR-LSP and binds it to a primary CR-LSP. To set the interval at which the binding between a bypass CR-LSP and a primary CR-LSP is refreshed, run the **mpls te timer fast-reroute** command.

The PLR calculates the interval using the value of *weight*. And the actual interval depends on device performance and the maximum number of LSPs that can be established on the device

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command in the MPLS view.

Example

Set the weight of the interval at which binding between a bypass CR-LSP and a primary LSP is refreshed to **120**.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te timer fast-reroute 120
```

9.3.154 mpls te timer retry

Function

The **mpls te timer retry** command sets the interval for re-establishing a tunnel.

The **undo mpls te timer retry** command restores the default setting.

The default interval is 30 seconds.

Format

mpls te timer retry *interval*

undo mpls te timer retry [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval for resetting up tunnels.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 30 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TE tunnel has been established, the TE tunnel is kept Up by periodically sending a Path message from the local node to its neighbor and receiving a Resv message from the neighbor. If no Resv message is received after the specified interval at which a tunnel is re-established, the local node considers the tunnel Down and reattempts to establish the tunnel. You can run this command to modify the interval for re-establishing a tunnel.

Precautions

A rather smaller interval imposes heavy burden of message processing on the system, causing network flapping; a rather large interval deteriorates the efficiency of RSVP CR-LSP convergence. Therefore, the default interval, 30 seconds, is recommended.

Example

Set the interval for setting up tunnels to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te timer retry 20
[HUAWEI-Tunnel1] mpls te commit
```

9.3.155 mpls te tunnel-id

Function

The **mpls te tunnel-id** command specifies the ID for a tunnel.

Format

mpls te tunnel-id *tunnel-id*

Parameters

Parameter	Description	Value
tunnel-id	Specifies the ID for a tunnel.	The value is an integer that ranges from 1 to 10000.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ID for a tunnel is a number that uniquely identifies an MPLS TE tunnel to facilitate tunnel planning and management.

Prerequisites

MPLS TE has been configured as the tunnel protocol using the **tunnel-protocol mpls te** command in the tunnel interface view.

Precautions

A tunnel ID must be set for a tunnel; otherwise, the tunnel fails to be established.

Example

Create a tunnel interface, configure MPLS TE as a tunnel protocol, set the tunnel ID to 100, and assign a tunnel destination address 2.2.2.2 to the interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te commit
```

9.3.156 mpls total-crlsp-number threshold-alarm

Function

The **mpls total-crlsp-number threshold-alarm** command configures the alarm threshold for total constraint-based routed label switched path (CR-LSP) usage.

The **undo mpls total-crlsp-number threshold-alarm** command restores the default settings.

The default upper limit of the alarm threshold for total CR-LSP usage is 80%. The default lower limit of the clear alarm threshold for total CR-LSP usage is 75%.

Format

mpls total-crlsp-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

mpls total-crlsp-number { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls total-crlsp-number threshold-alarm

undo mpls total-crlsp-number { **ingress** | **transit** | **egress** } **threshold-alarm**

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of the alarm threshold for total CR-LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of the clear alarm threshold for total CR-LSP usage.	The value is an integer ranging from 1 to 100, represented in percentage. The value must be smaller than the value of *upper-limit-value*. Using the default value 75 is recommended.
ingress	Specifies the alarm threshold for total ingress CR-LSPs.	-
transit	Specifies the alarm threshold for total transit CR-LSPs.	-
egress	Specifies the alarm threshold for total egress CR-LSPs.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of total CR-LSPs (including static CR-LSPs and Resource Reservation Protocol (RSVP) LSPs) in the system reaches a specific limit, establishing subsequent CR-LSPs may fail because of insufficient resources. To facilitate user operation and maintenance, enable an alarm to be generated when the number of total CR-LSPs reaches the specific limit. To configure the alarm threshold for total CR-LSP usage, run the **mpls total-crlsp-number threshold-alarm** command. The parameters in this command are described as follows:

- When the total CR-LSP usage increases to the value of *upper-limit-value*, an alarm for total CR-LSPs is generated.
- When the total CR-LSP usage falls below the value of *lower-limit-value*, a clear alarm for total CR-LSPs is generated.

If you want to set the alarm threshold for total ingress CR-LSPs, total transit CR-LSPs or total egress CR-LSPs, run **mpls total-crlsp-number** { **ingress** | **transit** | **egress** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*.

Precautions

- If the **mpls total-crlsp-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.
- This command configures the alarm threshold for total CR-LSP usage. The alarm that the number of LSPs exceeded the upper threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceed** is configured, and the actual total CR-LSP usage reaches the upper limit of the alarm threshold. The alarm that the number of LSPs fell below the lower threshold is generated only when the command **snmp-agent trap enable feature-name mpls_lspm trap-name hwmplslspthresholdexceedclear** is configured, and the actual total CR-LSP usage falls below the lower limit of the clear alarm threshold.

Example

Configure the upper limit and the lower limit of the alarm threshold for total CR-LSP usage.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls total-crlsp-number threshold-alarm upper-limit 90 lower-limit 60
```

9.3.157 next hop

Function

The **next hop** command specifies the next-hop address on an explicit path, and creates an MPLS TE tunnel through nodes in the order in which they are configured.

The **undo next hop** command restores the default configuration.

By default, no next-hop address on an explicit path is specified.

Format

next hop *ip-address* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**]

undo next hop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the next-hop IP address on an explicit path.	The value is in dotted decimal notation.
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Specifies the IP address of a node included on an explicit path. - **strict**: indicates that the node is added in **strict** mode. The node of *ip-address* is directly connected to the previous hop. - **loose**: indicates that the node is added in **loose** mode. The node of *ip-address* may not be directly connected to the previous hop. - **incoming**: indicates that the *ip-address1* is the IP address of an inbound interface of a next-hop node. - **outgoing**: indicates that the *ip-address1* is the IP address of an outbound interface of a next-hop node.	By default, a node is added to an explicit path in **include strict** mode.
exclude	Excludes the IP address from an explicit path.	-

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **next hop** command is used to plan nodes for an explicit path.

Precautions

The **include strict** parameter is used by default, meaning the tunnel must pass through a specified node.

Example

Exclude the IP address 10.0.0.125 from the MPLS TE explicit path.

```
<HUAWEI> system-view
[HUAWEI] explicit-path p1
[HUAWEI-explicit-path-p1] next hop 10.0.0.125 exclude
```

9.3.158 notify neighbor-down

Function

The **notify neighbor-down** command configures a BFD session to notify the upper layer protocol when the BFD session detects a neighbor Down event.

The **undo notify neighbor-down** command restores the default configuration.

By default, when the BFD detection time expires or a BFD session detects a neighbor Down event, the BFD session notifies the upper layer protocol.

Format

notify neighbor-down

undo notify neighbor-down

Parameters

None

Views

BFD-LSP session view

Default Level

2: Configuration level

Usage Guidelines

In most cases, when you use a BFD session to detect link faults, the BFD session notifies the upper layer protocol of a link fault in the following scenarios:

- When the BFD detection time expires, the BFD session notifies the upper layer protocol. BFD sessions must be configured on both ends. If the BFD session on the local end does not receive any BFD packets from the remote end within the detection time, the BFD session on the local end concludes that the link fails and notifies the upper layer protocol of the link fault.
- When a BFD session detects a neighbor Down event, the BFD session notifies the upper layer protocol. If the BFD session on the local end detects a neighbor Down event within the detection time, the BFD session on the local end directly notifies the upper layer protocol of the neighbor Down event.

When you use a BFD session to detect faults on an LSP, you need only be concerned about whether a fault occurs on the link from the local end to remote end. In this situation, run the **notify neighbor-down** command to configure the BFD session to notify the upper layer protocol only when the BFD session detects a neighbor Down event. This configuration prevents the BFD session from notifying the upper layer protocol when the BFD detection time expires and ensures that services are not interrupted.

Example

Configure the BFD session to notify the upper layer protocol when the BFD session detects a neighbor Down event.

```
<HUAWEI> system-view
[HUAWEI] bfd atob bind ldp-lsp peer-ip 10.1.2.1 nexthop 10.1.1.2 interface vlanif 100
[HUAWEI-bfd-lsp-session-atob] discriminator local 1
[HUAWEI-bfd-lsp-session-atob] discriminator remote 2
[HUAWEI-bfd-lsp-session-atob] notify neighbor-down
[HUAWEI-bfd-lsp-session-atob] commit
```

9.3.159 opaque-capability enable

Function

The **opaque-capability enable** command enables the Opaque-LSA capability so that an OSPF process can generate Opaque LSAs and receive Opaque LSAs from neighbors.

The **undo opaque-capability** command disables the Opaque-LSA capability.

By default, the Opaque-LSA capability is disabled.

Format

opaque-capability enable

undo opaque-capability

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Opaque LSAs provide a generic mechanism for OSPF extension:

- OSPF supports GR using Type 9 LSAs.
- OSPF supports TE using Type 10 LSAs.

Before configuring OSPF GR or OSPF TE, you must enable opaque LSA capability running the **opaque-capability enable** command.

Configuration Impact

Enabling or disabling the opaque LSA function may delete and re-establish all sessions and instances.

Example

Enable OSPF opaque-lsa.

```
<HUAWEI> system-view
[HUAWEI] ospf
[HUAWEI-ospf-1] opaque-capability enable
```

9.3.160 priority

Function

The **priority** command sets the setup priority and holding priority in a CR-LSP attribute template.

The **undo priority** command restores the default setup priority and holding priority in a CR-LSP attribute template.

The default setup and holding priority for a CR-LSP attribute template are both 7.

Format

priority *setup_priority_value* [*hold_priority_value*]

undo priority

Parameters

Parameter	Description	Value
setup_priority_value	Specifies the setup priority value in a CR-LSP attribute template.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. The default setup priority is 7.
hold_priority_value	Specifies the holding priority value in a CR-LSP attribute template.	An integer ranging from 0 to 7. The smaller the value, the higher the priority. The default holding priority is 7.

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

When configuring the **priority** command in the LSP attribute view, ensure that the setup priority is greater than or equal to the holding priority.

Example

Set both the setup priority and holding priority to 4 in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] priority 4 4
```

9.3.161 record-route

Function

The **record-route** command enables the system to record routes in a CR-LSP attribute template.

The **undo record-route** command configures the system not to record routes in a CR-LSP attribute template.

The system does not record routes in a CR-LSP attribute template.

Format

record-route [**label**]

undo record-route

Parameters

Parameter	Description	Value
label	Indicates that a label is also recorded when the system records a route.	-

Views

LSP attribute view

Default Level

2: Configuration level

Usage Guidelines

If the FRR function is enabled in a CR-LSP attribute template, the route storing function cannot be disabled.

Example

Enable the system to record routes in the CR-LSP attribute template.

```
<HUAWEI> system-view
[HUAWEI] lsp-attribute lsp-attribute-name
[HUAWEI-lsp-attribute-lsp-attribute-name] record-route
```

9.3.162 reset mpls rsvp-te

Function

The **reset mpls rsvp-te** command resets RSVP-TE process.

Format

reset mpls rsvp-te

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can delete and re-establish a CR-LSP by running the **reset mpls rsvp-te** command. This command is used to verify the working process of RSVP-TE in special cases. Generally, this command is not needed.

NOTE

If this command is run in an attempt to restart RSVP-TE and the interval at which RSVP-TE is restarted is small, the attempt fails. The interval varies according to the number of LSPs. The more the LSPs are established, the longer the interval is. The interval can be set to 30, 60, 90, or 120, in seconds.

Example

Reset RSVP-TE.

```
<HUAWEI> reset mpls rsvp-te
Warning: The MPLS RSVP-TE services will be reset. Continue? [Y/N]:y
```

9.3.163 reset mpls rsvp-te statistics

Function

The **reset mpls rsvp-te statistics** command clears the operational statistics on RSVP-TE.

Format

reset mpls rsvp-te statistics { **global** | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Clears the global operational statistics on RSVP-TE.	-
interface	Clears the operational statistics on RSVP-TE on the interface.	-
interface-type interface-number	Clears the operational statistics on RSVP-TE on the specifies interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	If no type or number of an interface is specified, statistics about all RSVP-TE interfaces are cleared.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When you run this command to clear the running information about RSVP-TE, the system displays the statistics from after the previous information is cleared.

Example

Clear the global operational statistics on RSVP-TE.

```
<HUAWEI> reset mpls rsvp-te statistics global
```

9.3.164 reset mpls stale-interface

Function

The **reset mpls stale-interface** command deletes information about MPLS interfaces in the Stale state.

Format

reset mpls stale-interface [*interface-index*]

Parameters

Parameter	Description	Value
interface-index	Specifies the index of a specified stale interface.	A hexadecimal integer ranging from 1 to FFFFFFFE.

Views

User view

Default Level

3: Management level

Usage Guidelines

If the configuration of an interface is deleted, or MPLS is disabled on an interface, the interface status becomes Stale. Run the **reset mpls stale-interface** command to delete information about a stale interface.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

Delete information about a specified stale interface.

```
<HUAWEI> reset mpls stale-interface 9d
```

Delete information about all stale interfaces.

```
<HUAWEI> reset mpls stale-interface
```

9.3.165 reset mpls te auto-bandwidth adjustment timers

Function

The **reset mpls te auto-bandwidth adjustment timers** command initializes automatic bandwidth adjustment.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730-H, and S6730S-H support this command.

Format

reset mpls te auto-bandwidth adjustment timers

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After the automatic bandwidth adjustment function runs for a certain period of time, to delete the running information and re-collect information, run the **reset mpls te auto-bandwidth adjustment timers** command in the user view. You do not need to delete this function or reconfigure it.

After the **reset mpls te auto-bandwidth adjustment timers** command is run, the device deletes information about the sampled traffic rate on the outbound interface and resets the automatic bandwidth adjustment timer.

Example

Initialize automatic bandwidth adjustment for MPLS TE tunnels.

```
<HUAWEI> reset mpls te auto-bandwidth adjustment timers
```

9.3.166 reset mpls te auto-frr

Function

The **reset mpls te auto-frr** command resets a specified auto bypass tunnel.

NOTE

After the Auto FRR function is enabled, you can use this command to recreate a bypass tunnel.

Format

reset mpls te auto-frr { **lsp-id** *ingress-lsr-id tunnel-id* | **name** *bypass-tunnel-name* }

Parameters

Parameter	Description	Value
lsp-id	Specifies the ID of an LSP.	-
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
tunnel-id	Specifies the ID of a tunnel.	The value is an integer and its ranges from 0 to 65535.

Parameter	Description	Value
name *bypass-tunnel-name*	Specifies the name of a bypass tunnel.	The value is a string of 1 to 63 characters.

Views

User view

Default Level

3: Management level

Usage Guidelines

To immediately recreate a specified auto bypass tunnel, run the **reset mpls te auto-frr** command.

Example

Reset the bypass tunnel with the ingress address being 1.1.1.1 and the tunnel ID being 10.

```
<HUAWEI> reset mpls te auto-frr lsp-id 1.1.1.1 10
```

9.3.167 reset mpls te tunnel-interface tunnel

Function

The **reset mpls te tunnel-interface tunnel** command resets a TE tunnel interface and re-establishes a TE tunnel.

Format

reset mpls te tunnel-interface tunnel *interface-number*

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the number of a TE tunnel.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

To validate the configurations of an MPLS TE tunnel, you can run the **mpls te commit** command in the tunnel interface view, and then run the **reset mpls te tunnel-interface tunnel** command in the user view.

If you do not run the **mpls te commit** command after modifying the configuration of a TE tunnel in the tunnel interface view, the system prompts a fault after the **reset mpls te tunnel-interface tunnel** command is run.

Example

Reset Tunnel 1.

```
<HUAWEI> reset mpls te tunnel-interface tunnel 1
```

9.3.168 static-cr-lsp egress

Function

The **static-cr-lsp egress** command configures a static CR-LSP on the egress LSR.

The **undo static-cr-lsp egress** command deletes a static CR-LSP from the egress LSR.

By default, no static CR-LSP on the egress LSR is configured.

Format

static-cr-lsp egress *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label*

undo static-cr-lsp egress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of a CR-LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the type and number of an inbound interface.	-
in-label *in-label*	Specifies the value of an incoming label.	The value is an integer that ranges from 16 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When configuring the egress of the CR-LSP, you can run the command **static-cr-lsp egress**. Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

To modify the value of **incoming-interface** *interface-type interface-number* and **in-label** *in-label*, run the **static-cr-lsp egress** command to set a new value. There is no need to run the **undo static-cr-lsp egress** command before changing a configured value.

Example

Configure the static CR-LSP named tunnel34 with the inbound interface being VLANIF100, and the incoming label being 233 on the egress LSR.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp egress tunnel34 incoming-interface vlanif 100 in-label 233
```

9.3.169 static-cr-lsp ingress

Function

The **static-cr-lsp ingress** command configures a static CR-LSP on the ingress LSR.

The **undo static-cr-lsp ingress** command deletes a static CR-LSP from the ingress LSR.

By default, no static CR-LSP on the ingress LSR is configured.

Format

static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* } **destination** *destination-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* [**bandwidth** [**ct0** | **ct1**] *bandwidth*]

undo static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* }

Parameters

Parameter	Description	Value
tunnel-interface tunnel *interface-number*	Specifies the tunnel interface of a static CR-LSP. *interface-number* indicates the tunnel interface number.	-
tunnel-name	Specifies the name of a CR-LSP.	The name is a string of 1 to 19 case-sensitive characters, spaces and abbreviation not supported. If you use the **interface Tunnel 1** command to create a tunnel interface for a static CR-LSP, the tunnel name in the **static-cr-lsp ingress** command must be formatted as "Tunnel1", otherwise, the tunnel cannot be created. There is no such a limit for the transit node and egress node.
destination *destination-address*	Specifies the destination IP address of a static CR-LSP.	The value is in dotted decimal notation.
nexthop *next-hop-address*	Specifies the next-hop IP address of a static CR-LSP.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outgoing interface. This parameter is only applicable to a P2P link.	-
out-label *out-label*	Specifies the value of an outgoing label.	The value is an integer that ranges from 16 to 1048575.
bandwidth [**ct0** | **ct1**] *bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT1.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command on the ingress node to configure a static CR-LSP.

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

Precautions

To modify parameters including **destination** *destination-address*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, and **out-label** *out-label*, run the **static-cr-lsp ingress** command to set a new value. There is no need to run the **undo static-cr-lsp ingress** command before changing a configured value.

When configuring a static CR-LSP ensure that the route of the static CR-LSP exactly matches the routing information. For example:

- If you specify a next hop when configuring a static CR-LSP, specify a next hop when configuring a static IP route. If you do not specify a next hop, the static LSP cannot be set up. For example:

```
[HUAWEI] ip route-static 10.1.3.0 24 10.1.1.2
[HUAWEI] static-cr-lsp ingress Tunnel1 destination 10.1.3.1 nexthop 10.1.1.2 out-label 237
```

- If a dynamic routing protocol applies to the link between LSRs, the next-hop IP address along the LSP must be the same as the IP address of the next hop in the routing table.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Example

Configure the static CR-LSP named Tunnel1, with the destination IP address being 10.1.3.1, the next-hop address being 10.1.1.2, the outgoing label being 237.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp ingress Tunnel1 destination 10.1.3.1 nexthop 10.1.1.2 out-label 237
```

9.3.170 static-cr-lsp transit

Function

The **static-cr-lsp transit** command configures a static CR-LSP on a transit LSR.

The **undo static-cr-lsp transit** command deletes a static CR-LSP from the transit LSR.

By default, no static CR-LSP on a transit LSR is configured.

Format

static-cr-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* [**bandwidth** [**ct0** | **ct1**] *bandwidth*] [**description** *description*]

undo static-cr-lsp transit *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the CR-LSP name.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the incoming interface of the CR-LSP. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
in-label *in-label*	Specifies the value of an incoming label.	The value is an integer that ranges from 16 to 1023.
nexthop *next-hop-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the name of an outgoing interface.	-
out-label *out-label*	Specifies the value of an outgoing label.	The value is an integer that ranges from 16 to 1048575.
bandwidth [**ct0** | **ct1**] *bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT1.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.
description *description*	Specifies the description information.	The value is a string of 1 to 63 case-sensitive characters with spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

To modify parameters including **incoming-interface** *interface-type interface-number*, **in-label** *in-label*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, and **out-label** *out-label*, run the **static-cr-lsp transit** command to set a new value for each parameter. There is no need to run the **undo static-cr-lsp transit** command before modifying a value.

NOTE

The configured bandwidth takes effect only during tunnel establishment and protocol negotiation, and does not limit the bandwidth for traffic forwarding.

Example

Configure the static CR-LSP named tunnel39 with the incoming interface being VLANIF100, the incoming label being 123, the outgoing interface being VLANIF200, the outgoing label as 253.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp transit tunnel39 incoming-interface vlanif 100 in-label 123 outgoing-interface
vlanif 200 out-label 253
```

9.3.171 statistic enable (MPLS TE tunnel interface view)

Function

The **statistic enable** command enables MPLS TE traffic statistics collection.

The **undo statistic enable** command disables MPLS TE traffic statistics collection.

By default, MPLS TE traffic statistics collection is disabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

statistic enable

undo statistic enable

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view MPLS TE traffic statistics collected in the outbound direction of an interface, run the **statistic enable** command in the tunnel interface view to enable MPLS TE traffic statistics collection first. After a period of time, run the **display interface tunnel** or **display counters interface** command to view the MPLS TE traffic statistics.

Prerequisites

The tunneling protocol of the tunnel interface has been set to MPLS TE using the **tunnel-protocol mpls te** command in the tunnel interface view.

Precautions

MPLS TE traffic statistics collection is supported only in the outbound direction of a tunnel interface.

Example

Enable MPLS TE traffic statistics collection on Tunnel1.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] statistic enable
```

9.3.172 traffic-eng

Function

The **traffic-eng** command enables TE features on a specified level for an IS-IS process.

The **undo traffic-eng** command restores the default settings.

By default, TE features are disabled for an IS-IS process.

Format

traffic-eng [**level-1** | **level-2** | **level-1-2**]

undo traffic-eng [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables IS-IS TE on Level-1.	-
level-2	Enables IS-IS TE on Level-2.	-
level-1-2	Enables IS-IS TE on Level-1-2. **NOTE** If no level is specified, TE is enabled on Level-1-2.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you deploy MPLS TE on the MPLS backbone network where IS-IS is used to advertise routes, run this command to enable TE features on a specified level for an IS-IS process.

Prerequisites

The **cost-style** command has been executed to set the cost type of IS-IS packets to wide, compatible, or wide-compatible.

Precautions

The IS-IS level in this command must be the same as that on the MPLS backbone network.

Example

Enable TE on level-2 for IS-IS process 1.

```
<HUAWEI> system-view
[HUAWEI] isis 1
[HUAWEI-isis-1] cost-style compatible
[HUAWEI-isis-1] traffic-eng level-2
```

9.3.173 undo mpls te srlg all-config

Function

The **undo mpls te srlg all-config** command deletes the member interfaces of all SRLGs on an MPLS TE node.

Format

undo mpls te srlg all-config

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

If an MPLS TE node is configured with the **undo mpls te srlg all-config** command, the **mpls te srlg** command is deleted from all the interfaces of an MPLS TE node, while the **mpls te srlg path-calculation** command configured in the MPLS view is not deleted.

Example

Delete the SRLG configuration from all the interfaces of the MPLS TE node.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls te srlg 1
[HUAWEI-Vlanif10] mpls te srlg 2
[HUAWEI-Vlanif10] quit
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] mpls te srlg 1
[HUAWEI-Vlanif20] mpls te srlg 2
[HUAWEI-Vlanif20] quit
[HUAWEI] mpls
[HUAWEI-mpls] undo mpls te srlg all-config
```

10 VPN Configuration Commands

10.1 GRE Configuration Commands

10.1.1 Command Support

Only the following switch models support GRE:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

10.1.2 description (tunnel interface view)

Function

The **description** command sets the description of the current tunnel interface.

The **undo description** command deletes the description of the current tunnel interface.

By default, a tunnel interface does not have a description.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a tunnel interface.	The value is a string of 1 to 242 case-sensitive characters, with spaces supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After using the **interface tunnel** command to create a tunnel interface, you can run the **description** command to configure a description of the tunnel interface to facilitate later query.

To check the description of a tunnel interface, run the **display this interface** command in the tunnel interface view or the **display interface tunnel** command.

Example

Configure the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

Delete the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo description
```

10.1.3 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Establish a manual IPv6 over IPv4 tunnel between VLANIF 10 at 10.1.1.1 on switch HUAWEI1 and VLANIF 20 at 10.2.1.1 on switch HUAWEI2.

```
<HUAWEI1> system-view
[HUAWEI1] interface tunnel 1
[HUAWEI1-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI1-Tunnel1] source 10.1.1.1
[HUAWEI1-Tunnel1] destination 10.2.1.1
<HUAWEI2> system-view
[HUAWEI2] interface tunnel 1
[HUAWEI2-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI2-Tunnel1] source 10.2.1.1
[HUAWEI2-Tunnel1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel1 to 10.1.1.1 that belongs to vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] destination vpn-instance vpn1 10.1.1.1
```

10.1.4 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.

Parameter	Description	Value
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command. You can run this command to obtain tunnel interface information when configuring tunnels or when locating the fault on these tunnels.

Prerequisites

Before run **display interface tunnel**, please ensure that tunnel interface has been created using the **interface tunnel** command.

Example

Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-11-16 19:16:33 UTC+08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.2.1.2 (Vlanif1234), destination 10.2.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2012-11-16 19:17:39+08:00
Last 300 seconds input rate 16 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  5 packets, 650 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 10-1 Description of the display interface tunnel command output

Item	Description
Tunnel1 current state	Physical layer status of the tunnel interface: - UP: The interface is in normal state. - Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status: - UP: The link layer protocol of the tunnel interface works normally. - Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time the link layer protocol of the tunnel interface goes UP. **NOTE** This field is displayed only when the link layer protocol status of the tunnel interface is UP.
Description	Description of the tunnel interface.
Route Port	Indicates the Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.3.1.2/24	IP address of the tunnel interface is 10.3.1.2. The mask is 24 bits, that is, 255.255.255.0.
Encapsulation is TUNNEL,	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.2.1.2 (Vlanif1234)	The source address of the tunnel is 10.2.1.2. That is, the IP address of the VLANIF 1234 interface sending packets at the source side is 10.2.1.2.
destination 10.2.1.1	Destination address of the tunnel.

Item	Description
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive enable period 5 retry-times 3	The keepalive function of GRE.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization : --	Input bandwidth usage.
Output bandwidth utilization : --	Output bandwidth usage.

10.1.5 display keepalive packets count

Function

The **display keepalive packets count** command displays the number of Keepalive packets and Keepalive response packets sent and received by the local GRE tunnel interface.

Format

display keepalive packets count

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a tunnel is a GRE tunnel, you can enable the Keepalive function to check the link connectivity. If the function is disabled, service packets are continuously forwarded through this tunnel interface when the link fails, resulting in a tunnel black hole and loss of service data.

The **display keepalive packets count** command allows you to view the number of Keepalive packets and Keepalive response packets sent and received through the GRE tunnel interface.

Prerequisites

1. The tunnel interface view has been displayed using the **interface tunnel** command.
2. The tunnel type has been set to GRE using the **tunnel-protocol gre** command.
3. The Keepalive function has been enabled for the GRE tunnel using the **keepalive** command.

Follow-up Procedure

Run the **reset keepalive packets count** command to reset the Keepalive packet statistics.

Example

View the Keepalive packet statistics of GRE tunnel interface 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] keepalive
[HUAWEI-Tunnel1] display keepalive packets count
Send 10 keepalive packets to peers, Receive 10 keepalive response packets from
peers
Receive 8 keepalive packets from peers, Send 8 keepalive response packets to
peers.
```

Table 10-2 Description of the display keepalive packets count command output

Item	Description
Send 10 keepalive packets to peers	Ten Keepalive packets are sent to the remote end.
Receive 10 keepalive response packets from peers	Ten Keepalive response packets are received from the remote end.
Receive 8 keepalive packets from peers	Eight Keepalive packets are received from the remote end.
Send 8 keepalive response packets to peers	Eight Keepalive response packets are sent to the remote end.

10.1.6 display tunnel-info

Function

The **display tunnel-info** command displays the tunnel information.

Format

display tunnel-info { **tunnel-id** *tunnel-id* | **all** | **statistics** [**slots**] }

Parameters

Parameter	Description	Value
tunnel-id *tunnel-id*	Specifies the tunnel ID. If the specified ID does not exist, the system prompts errors.	A hexadecimal integer ranging from 1 to FFFFFFFE.
all	Displays information about all the tunnels.	-
statistics	Displays statistics about all tunnels.	-
slots	Displays tunnel statistics in the order of slots.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display tunnel-info all** command displays existing tunnel IDs, tunnel types, destination IP addresses, and Token information about all tunnels.

The **display tunnel-info tunnel-id** *tunnel-id* command displays detailed information about a tunnel when you only know the tunnel ID.

The **display tunnel-info statistics** command displays the number of tunnels configured on the switch.

Example

View information about the tunnel.

```
<HUAWEI> display tunnel-info tunnel-id 2
Tunnel ID:                  0x2
Tunnel Token:                 2
Type:                      cr lsp
Destination:                 1.1.1.1
Out Slot:                   0
Instance ID:                 0
Interface:                  Tunnel1
Sub Tunnel ID:                0x0
<HUAWEI> display tunnel-info tunnel-id 3
Tunnel ID:                  0x3
Tunnel Token:                 3
Type:                      lsp
Destination:                 10.20.10.10
Out Slot:                   0
Instance ID:                 0
Out Interface:                Vlanif1024
Out Label:                   3
Next Hop:                   10.24.10.200
Lsp Index:                  2048
<HUAWEI> display tunnel-info tunnel-id 10006
Tunnel ID:                  0x10006
Tunnel Token:                 2
Type:                      lsp
Destination:                 6.6.6.6
Out Slot:                   0
Instance ID:                 0
Out Interface:                Vlanif15
Lsp Index:                  0
SubTunnel Type:                L2VPN QoS Token
```

Table 10-3 Description of the **display tunnel-info tunnel-id** command output

Item	Description
Tunnel ID	Tunnel ID in hexadecimal notation that is assigned by the system.
Tunnel Token	Token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.
Type	Type of a tunnel, such as GRE, MPLS LSP, or CR-LSP. The command output varies according to the tunnel type.
Destination	Destination IP address of the tunnel.

Item	Description
Out Slot	Number of the slot that is used when the switch sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.
Sub Tunnel ID	Sub-tunnel ID of VPN QoS in hexadecimal notation that is automatically assigned by the system.
Out Label	Out label value.
Next Hop	Next hop.
Lsp Index	LSP index, which is allocated by MPLS.
Out Interface	Local outbound interface of the tunnel.
SubTunnel Type	Types of tokens of sub-tunnels: ● LDP LSP over TE QoS Token ● LDP LSP QoS Token ● BGP LSP over TE QoS Token ● BGP LSP QoS Token ● Static LSP QoS Token ● CR-LSP over TE QoS Token ● L2VPN over TE QoS Token ● L2VPN QoS Token This field is displayed only for sub-tunnels.

Display all tunnel information.

```
<HUAWEI> display tunnel-info all
 * -> Allocated VC Token
Tunnel ID            Type                Destination          Token
----------------------------------------------------------------------
0x10006              lsp                 10.2.1.1             6
```

Display tunnel statistics.

```
<HUAWEI> display tunnel-info statistics
LSP/32bit LSP :                         0/0
GRE :                                   2
CRLSP :                                 0
LOCAL IFNET :                           0
MPLS LOCAL IFNET :                      0
VPN QOS LSP :                           0
Reserved :                              0
Vxlan :                                 0
```

Table 10-4 Description of the **display tunnel-info statistics** command output

Item	Description
LSP/32bit LSP	Number of LSP tunnels created in the system view/Number of LSP tunnels triggered by the route of host with the 32-bit mask address.
GRE	Number of tunnel IDs allocated to the GRE tunnels.
CRLSP	Number of tunnel IDs allocated to the CR-LSP tunnels.
LOCAL IFNET	Number of tunnels used by the VPN internal module.
MPLS LOCAL IFNET	Number of tunnels used by the MPLS internal module.
VPN QOS LSP	Number of the tunnel ID allocated to the LSP used in VPN QoS.
Reserved	Number of the tunnel ID allocated to the product.
Vxlan	Number of tunnel IDs allocated to the Vxlan tunnels.

Display tunnel statistics in the order of slots.

```
<HUAWEI> display tunnel-info statistics slots
------------------------------------------------------------------
Slot        LSP     CR      GRE     LCL     MPLS-L  VPN     VXLAN
Num                 LSP             IFNET   IFNET   QOS
------------------------------------------------------------------
0           0       0       0       0       0       0       0
Logic Slot: 0                      Total:  0
```

Table 10-5 Description of the display tunnel-info statistics slots command output

Item	Description
Slot Num	Slot number used by the device to send packets.
LSP	Total LSP tunnels set up by the device.
CR LSP	Number of CR-LSPs created on the device.
GRE	Number of GRE tunnels created on the device.
LCL IFNET	Number of tunnels used by the VPN module.
MPLS-L IFNET	Number of tunnels used by the MPLS module.
VPN QOS	Number of tunnels used for VPN QoS.
VXLAN	Number of VXLAN tunnels created on the device.

10.1.7 gre key

Function

The **gre key** command sets the key number of a GRE tunnel.

The **undo gre key** command deletes the key number of a GRE tunnel.

By default, the GRE key number is not configured.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

gre key { **plain** *key-number* | [**cipher**] *plain-cipher-text* }

undo gre key

Parameters

Parameter	Description	Value
plain *key-number*	Specifies a plaintext key. **NOTICE** If **plain** is selected, the key is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the key in cipher text.	The value is an integer that ranges from 0 to 4294967295.
[**cipher**] *plain-cipher-text*	Specifies that a ciphertext key is displayed.	You can specify a plaintext key (integer) ranging from 0 to 4294967295 or a ciphertext key of 32 or 48 characters.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure key numbers for both ends of a GRE tunnel to improve GRE tunnel security. This security mechanism ensures that a device accepts only packets sent from the valid tunnel interface and discards invalid packets.

Prerequisites

The tunnel interface view has been displayed using the **interface tunnel** command.

The tunnel type has been set to GRE using the **tunnel-protocol gre** command.

Precautions

Packets pass authentication only when the key numbers set on both ends of the tunnel are consistent. Otherwise, the packets are discarded.

When you run the **gre key** command several times, the latest configuration overrides the previous configurations.

Example

Configure the GRE key number for the ends of a tunnel is 123.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] gre key cipher 123
```

10.1.8 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is an integer that ranges from 0 to 2047 .

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

Follow-up Procedure

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Example

Create a tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1]
```

10.1.9 keepalive

Function

The **keepalive** command enables the Keepalive function of GRE tunnels.

The **undo keepalive** command disables the Keepalive function of GRE tunnels.

By default, the Keepalive function of a GRE tunnel is disabled.

Format

keepalive [**period** *period* [**retry-times** *retry-times*]]

undo keepalive

Parameters

Parameter	Description	Value
period *period*	Specifies the interval for sending Keepalive packets.	The value is an integer that ranges from 1 to 32767, in seconds. The default value is 5 seconds.
retry-times *retry-times*	Specifies the parameter of the unreachable counter.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you configure a tunnel policy and set the VPN tunnel type to GRE, you need to enable the Keepalive function. After Keepalive is enabled, the VPN cannot choose a tunnel with an unreachable remote end, preventing data loss.

When Keepalive is disabled on a local end, the tunnel interface status of the local end might be Up even if the remote end is unreachable. After Keepalive is enabled on the local end, the tunnel interface status of the local end changes to Down if the remote end is unreachable. Therefore, when the remote end is unreachable, the VPN cannot choose the GRE tunnel, preventing data loss.

The Keepalive function takes effect uni-directionally. To enable the Keepalive function on both ends of a tunnel, run the **keepalive** command on each end of the tunnel. The Keepalive configuration takes effect on one end even if the function is disabled on the other end. However, it is recommended that you enable the Keepalive function on both ends.

After the Keepalive function is enabled on a GRE tunnel, the tunnel periodically sends Keepalive packets. The unreachable counter increases by one each time a packet is sent. If no response packet is received when the value of the counter reaches the value of *retry-times*, the remote end is considered unreachable.

Prerequisites

The **keepalive** command can be used only when the encapsulation mode has been set to GRE on an interface.

Precautions

When you run the **keepalive** command several times, the latest configuration overrides the previous configurations.

When the VPN instance to which a GRE tunnel interface is bound is not the specified destination VPN instance, the **keepalive** command cannot be used to check GRE tunnel connectivity. If this command is used in this situation, the Keepalive function cannot be implemented.

Follow-up Procedure

Run the **display keepalive packets count** command to display the number of Keepalive packets and Keepalive response packets sent and received by the local GRE tunnel interface.

Example

Enable the Keepalive function for the GRE tunnel using default parameters.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] keepalive
```

Enable the Keepalive function for the GRE tunnel, and set the interval for sending Keepalive packets to 12 seconds and **retry-times** to 4.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] keepalive period 12 retry-times 4
```

10.1.10 map interface virtual-ethernet

Function

The **map interface virtual-ethernet** command binds an L2VE interface to a tunnel interface.

The **undo map interface virtual-ethernet** command deletes the binding relationship between a tunnel interface and a specified VE interface.

The **undo map** command deletes the binding relationship between a tunnel interface and all VE interfaces.

By default, no L2VE interface is bound to a tunnel interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.

Format

map interface virtual-ethernet *ve-number*

undo map interface virtual-ethernet *ve-number*

undo map

Parameters

Parameter	Description	Value
ve-number	Specifies the number of a VE interface.	The VE interface number must already exist.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customers want to use GRE to transparently transmit Ethernet packets over networks of a different network layer protocol, such as the IPv4 network. You can configure Ethernet over GRE to achieve this purpose. Run the **map interface virtual-ethernet** command in the tunnel interface view to bind a VE interface to a tunnel interface. After the binding, the tunnel interface can transparently transmit Ethernet packets over the GRE tunnel.

Prerequisites

- A VE interface has been created by using the **interface virtual-ethernet** *ve-number* command, and the VE interface has been changed from Layer 3 mode to Layer 2 mode by using the **portswitch** command.
- The tunnel protocol of a tunnel interface has been set to GRE by using the **tunnel-protocol gre** command in the tunnel interface view.

Precautions

NOTE

- If a VLANIF interface has been created for a VLAN, this VLAN cannot be specified for a VE interface. If a VLAN has been specified for a VE interface, no VLANIF interface can be created for this VLAN.
- One tunnel interface can be bound with two VE interfaces, but one VE interface can be bound to only one tunnel interface.
- Only VE interfaces of the Trunk type can be bound to a tunnel interface.
- A tunnel interface bound with a VE interface does not support the IPv6 protocol stack. A VE interface cannot be bound to a tunnel interface enabled with the IPv6 protocol stack.
- To prevent loops, packets transmitted through an Ethernet over GRE tunnel cannot be sent to a GRE tunnel again.
- Ensure that the VE interfaces at both ends of a GRE tunnel are added to the same VLAN. Otherwise, the VE interfaces will learn MAC addresses not in the VLANs to which the VE interfaces belong, and these MAC addresses cannot be deleted using the **undo mac-address** command. Run the **undo mac-address** [*mac-address*] [**vlan** *vlan-id*] command to delete a specific MAC address or delete MAC addresses by VLAN ID, or wait until the MAC addresses automatically age out.
- When configuring Ethernet over GRE, ensure that routes can recurse to GRE tunnels. Otherwise, packets cannot be encapsulated using Ethernet over GRE.

Example

Bind Virtual-Ethernet 0/0/1 to Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] portswitch
[HUAWEI-Virtual-Ethernet0/0/1] port link-type trunk
[HUAWEI-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[HUAWEI-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-Virtual-Ethernet0/0/1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] map interface virtual-ethernet 0/0/1
```

10.1.11 reset keepalive packets count

Function

The **reset keepalive packets count** command clears the statistics on Keepalive packets sent and received by a GRE tunnel interface.

Format

reset keepalive packets count

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Keepalive function is enabled on a GRE tunnel, the VPN cannot choose a tunnel with an unreachable remote end, preventing data loss. You can run the **display keepalive packets count** command to view the statistics on Keepalive packets and Keepalive response packets sent and received by the GRE tunnel interface, and the running status of the GRE tunnel.

The **reset keepalive packets count** command resets the statistics of Keepalive packets and Keepalive response packets sent and received by the GRE tunnel interface. You can monitor the running status of the GRE tunnel.

Precautions

The cleared packet statistics cannot be restored. Exercise caution when you run the command.

Example

Reset the Keepalive packet statistics of GRE tunnel interface 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] reset keepalive packets count
 Info: Succeeded in resetting tunnel keepalive packets count.
```

10.1.12 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel. The following types of interfaces are often used: VLANIF and loopback.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the source address of the local tunnel interface is the destination address of the remote tunnel interface, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Example

Set the tunnel type of Tunnel1 to IPv6 over IPv4 of manual mode and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI-Tunnel1] source 10.1.1.1
```

Configure Tunnel1 of GRE and use Loopback1 address as the interface address.

```
<HUAWEI> system-view
[HUAWEI] interface Loopback 1
[HUAWEI-LoopBack1] ip address 10.2.1.1 32
[HUAWEI-LoopBack1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] source loopback 1
```

10.1.13 statistic enable (Tunnel interface view)

Function

The **statistic enable** command enables traffic statistics collection on a Tunnel interface.

The **undo statistic enable** command disables traffic statistics collection on a Tunnel interface.

By default, traffic statistics collection is disabled on a Tunnel interface.

Format

statistic enable { **both** | **inbound** | **outbound** }

undo statistic enable { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
both	Enables traffic statistics collection for incoming and outgoing traffic.	-
inbound	Enables incoming traffic statistics collection.	-
outbound	Enables outgoing traffic statistics collection.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable traffic statistics collection on Tunnel interfaces. The device then collect traffic statistics on the Tunnel interfaces.

Prerequisites

The protocol type of the tunnel interface has been configured using the **tunnel-protocol** command.

Precautions

After running the **statistic enable** command on an interface, you can run the **display interface tunnel** command to view the traffic statistics on the interface. The traffic statistics help you diagnose the fault of a tunnel.

Example

Enable incoming traffic statistics collection on a Tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] statistic enable inbound
```

10.1.14 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** | **ipv6-ipv4** [**6to4** | **isatap**] | **ipv4-ipv6** | **mpls te** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicate that the GRE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameters.	-
ipv4-ipv6	Indicate that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameter.	-
ipv6-ipv4 [**6to4** | **isatap**]	Configure the tunnel protocol of the tunnel interface as ipv6-ipv4: ● **ipv6-ipv4**: use a manual IPv6 over IPv4 tunnel ● **ipv6-ipv4 6to4** : using 6to4 tunnel ● **ipv6-ipv4 isatap** : using isatap tunnel **NOTE** Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support these parameter.	-
mpls te	Indicate that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730-S, S6730S-S, and S6730S-H support the parameter.	-
none	Indicate that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface.

Example

Set the tunnel encapsulation mode of Tunnel2 to GRE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 2
[HUAWEI-Tunnel2] tunnel-protocol gre
```

10.2 IPSec Configuration Commands (IPSec Encryption)

10.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

10.2.2 ah authentication-algorithm

Function

The **ah authentication-algorithm** command configures the authentication algorithm for AH.

The **undo ah authentication-algorithm** command restores the default authentication algorithm for AH.

By default, AH uses the Secure Hash Algorithm-256 (SHA2-256) authentication algorithm.

Format

ah authentication-algorithm { **sha1** | **sha2-256** }

undo ah authentication-algorithm

Parameters

Parameter	Description	Value
sha1	Specifies Secure Hash Algorithm-1 (SHA-1) as the authentication algorithm. SHA-1 generates a 160-bit message summary based on a message of less than 2^{64} bits.	-
sha2-256	Specifies SHA2-256 as the authentication algorithm. SHA2-256 generates a 256-bit message summary based on a message of less than 2^{64} bits.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use AH to authenticate packets, preventing packets from being intercepted or modified, you can run the **ah authentication-algorithm** command to configure the authentication algorithm for AH.

Prerequisite

The protocol of this IPSec proposal has been configured to AH using the **transform** command.

Precautions

The authentication algorithms on both IPSec peers must be identical.

The system software does not support the **md5** parameter. To use the **md5** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2-256** parameter.

For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the IPSec proposal **prop1** to use the AH protocol, and specify SHA2-256 as the authentication algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform ah
[HUAWEI-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
```

10.2.3 display ipsec proposal

Function

The **display ipsec proposal** command displays IPSec proposal information.

Format

display ipsec proposal [**name** *proposal-name*]

Parameters

Parameter	Description	Value
name *proposal-name*	Specifies the name of an IPSec proposal.	The value is an existing name of an IPSec proposal.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

After IPSec is configured, when valid packets are dropped between IPSec peers, you can run the **display ipsec proposal** command to check whether the IPSec proposal configurations on both IPSec peers are identical.

IPSec ensures security using the IPSec proposal. You can run the **display ipsec proposal** command to view the following information:

- Name of the IPSec proposal

- Encapsulation mode defined in the IPSec proposal
- Security protocol defined in the IPSec proposal
- Authentication and encryption algorithms defined in the IPSec proposal

Example

Display information about all IPSec proposals.

```
<HUAWEI> display ipsec proposal
  Total IP security proposal number: 1

  IP security proposal name: proposal1
    encapsulation mode: transport
    transform: esp-new
    ESP protocol: authentication SHA2-HMAC-256, encryption AES-192
```

Table 10-6 Description of the **display ipsec proposal** command output

Item	Description
Total IP security proposal number	Number of IPSec proposals created.
IP security proposal name	Name of an IPSec proposal. To configure an IPSec proposal, run the **ipsec proposal** command.
encapsulation mode	IPSec encapsulation mode: - transport - tunnel To configure an encapsulation mode, run the **encapsulation-mode** command.
transform	Security protocol defined in the security proposal: - esp-new: ESP - ah-new: AH To configure a security protocol, run the **transform** command.
ESP protocol	The authentication algorithm and encryption algorithm used by the ESP protocol. To configure the authentication algorithm and encryption algorithm, run the **esp authentication-algorithm** and **esp encryption-algorithm** command separately.
AH protocol	To configure an authentication algorithm used by the AH protocol, run the **ah authentication-algorithm** command.

10.2.4 display ipsec sa

Function

The **display ipsec sa** command displays information about a Security Association (SA).

Format

display ipsec sa [**name** *sa-name*] [**brief**]

Parameters

Parameter	Description	Value
name *sa-name*	Specifies the SA name.	The value is an existing SA name.
brief	Displays brief information of the SA, such as the SA name and the Security Parameter Index (SPI) value.	-

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

You can run the **display ipsec sa** command to check whether the SA configurations for outgoing packets on the local end are identical with those for incoming packets on the peer end. The **display ipsec sa** command output displays the following information:

- SA name
- Security proposal applied to the SA
- Number of times the SA is applied
- SA configurations for incoming Authentication Header (AH) packets
- SA configurations for outgoing AH packets
- SA configurations for incoming Encapsulating Security Payload (ESP) packets
- SA configurations for outgoing ESP packets

Example

Display configurations of the SA.

```
<HUAWEI> display ipsec sa
  IP security association name: sa1
  Number of references: 0
    proposal name: prop1
    inbound AH setting:
      AH spi:
      AH string-key:
      AH authentication hex key: %^%#0D_@HS5002;U1AR{t$3W:H188Ghs~N'_r`Y&R<j70V5-,r-NF(z!
92N)oSNA%^%#
    inbound ESP setting:
      ESP spi:
      ESP string-key:
      ESP encryption hex key: %^%#A*v9(B!U3U%*HL%Rod;%|G}F;B3[5%q#VMTG#9EP%^%#
      ESP authentication hex key: %^%#w_eeVg;FD3ybX!(2&P2ecMN%'JMGWXm^bR#qcUNKj_3AGrb@#
\B4(Vn5cYC%^%#
    outbound AH setting:
      AH spi:
      AH string-key:
      AH authentication hex key: %^%#jp!o1aA7qD^qMN&yI4M8nG_(~~O.{8;tyqI3%o5M4&L@G]rJw/
au]r'm=j^9%^%#
    outbound ESP setting:
      ESP spi:
      ESP string-key:
      ESP encryption hex key: %^%#".dAYkLlqV_o-'SI0.":&<M';66l4UGMEjB9Cl\S%^%#
      ESP authentication hex key: %^%#Nkz8Z-sF*Pw3clT]@_F9B4:8>RIwc'r#sCJl0N[;{drLI|
%uU5lVUWQkY3p1%^%#
```

Table 10-7 Description of the **display ipsec sa** command output

Item	Description
IP security association name	SA name
Number of references	Number of times the SA is applied
proposal name	Security proposal applied to the SA
inbound AH setting	SA configurations for incoming AH packets
AH spi	SPI for AH
AH string-key	Authentication key for AH in the string format displayed in cipher text
AH authentication hex key	Authentication key for AH in cipher text
inbound ESP setting	SA configurations for incoming ESP packets
ESP spi	SPI for ESP
ESP string-key	Authentication key for ESP in the string format displayed in cipher text
ESP encryption hex key	Encryption key for ESP in cipher format

Item	Description
ESP authentication hex key	Authentication key for ESP in cipher text
outbound AH setting	SA configurations for outgoing AH packets
outbound ESP setting	SA configurations for outgoing ESP packets

10.2.5 display ipsec statistics

Function

The **display ipsec statistics** command displays the statistics about packets processed by IPSec.

Format

display ipsec statistics [**sa-name** *sa-name* **slot** *slot-number*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing SA name.
slot *slot-number*	Displays the IPSec SA statistics of the specified slot.	The value is an integer, and the value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

After IPSec protection is configured for a routing protocol, you can run the **display ipsec statistics** command to view information about transmitted packets and dropped packets. The details are as follows:

- Number of received and sent packets
- Number of received and sent bytes
- Number of dropped incoming and outgoing packets
- Detailed information about dropped packets

Example

Display statistics about packets processed by IPSec.

```
<HUAWEI> display ipsec statistics
 IPv6 security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   dropped security packet detail:
     memory process problem: 0
     can't find SA: 0
     queue is full: 0
     authentication is failed: 0
     wrong length: 0
     replay packet: 0
     too long packet: 0
     invalid SA: 0
     policy deny: 0
 the normal packet statistics:
   input/output dropped normal packets: 0/0
 IPv4 security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   dropped security packet detail:
     memory process problem: 0
     can't find SA: 0
     queue is full: 0
     authentication is failed: 0
     wrong length: 0
     replay packet: 0
     too long packet: 0
     invalid SA: 0
     policy deny: 0
 the normal packet statistics:
   input/output dropped normal packets: 0/0
```

Table 10-8 Description of the **display ipsec statistics** command output

Item	Description
IPv6 security packet statistics	Statistics on IPv6 security packets.
IPv4 security packet statistics	Statistics on IPv4 security packets.
input/output security packets	Indicates the number of received and sent packets.
input/output security bytes	Indicates the number of received and sent bytes.
input/output dropped security packets	Indicates the number of dropped incoming and outgoing packets.

Item	Description
dropped security packet detail	Detailed information about dropped packets.
memory process problem	Indicates the number of packets that are dropped due to a memory fault.
can't find SA	Indicates the number of packets that are dropped because no SA is found.
queue is full	Indicates the number of packets that are dropped because the queue is full.
authentication is failed	Indicates the number of packets that are dropped due to authentication failure.
wrong length	Indicates the number of packets that are dropped due to a packet length fault.
replay packet	Indicates the number of packets that are dropped due to repeated transmission.
too long packet	Indicates the number of packets that are dropped due to excess packet length.
invalid SA	Indicates the number of packets that are dropped due to an invalid SA.
policy deny	Indicates the number of packets that are dropped due to a deny action in the policy.
the normal packet statistics	Statistics about normal packets.
input/output dropped normal packets	Indicates the number of received/sent normal packets that are dropped.

10.2.6 encapsulation-mode

Function

The **encapsulation-mode** command sets the encapsulation mode for IP packets.

The **undo encapsulation-mode** command restores the default encapsulation mode for IP packets.

By default, the encapsulation mode is set to **tunnel**.

Format

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

Parameters

Parameter	Description	Value
transport	Sets the encapsulation mode to **transport**.	-
tunnel	Sets the encapsulation mode to **tunnel**.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Authentication Header (AH) or Encapsulating Security Payload (ESP) to ensure security based on data confidentiality. If AH is configured, an AH header is generated; if ESP is configured, an ESP header, an ESP tail, and an ESP authentication field are generated. Two encapsulation modes are available for IPSec: transport and tunnel.

- The transport mode is applicable to a scenario in which two hosts, or a host and a security gateway, are communicating with each other. In transport mode, the two devices encrypting and decrypting packets must be the original packet sender and the final receiver, respectively.
- The tunnel mode is generally applied to a scenario in which two security gateways are communicating with each other. The packets that are encrypted on the local security gateway can be decrypted only on the peer security gateway. Therefore, an IP packet must be encapsulated using the tunnel mode and an IP header embed. After arriving at the peer security gateway, the IP packet can be decrypted.

Precautions

The encapsulation modes on both IPSec peers must be identical.

Example

Set the encapsulation mode to **transport** in the security proposal named **prop2**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop2
[HUAWEI-ipsec-proposal-prop2] encapsulation-mode transport
```

10.2.7 esp authentication-algorithm

Function

The **esp authentication-algorithm** command configures the authentication algorithm for ESP.

The **undo esp authentication-algorithm** command cancels the authentication algorithm for ESP.

By default, ESP uses the Secure Hash Algorithm-256 (SHA2-256) authentication algorithm.

Format

esp authentication-algorithm { **sha1** | **sha2-256** }

undo esp authentication-algorithm

Parameters

Parameter	Description	Value
sha1	Specifies Secure Hash Algorithm-1 (SHA-1) as the authentication algorithm. SHA-1 generates a 160-bit message summary based on a message of less than 2^{64} bits.	-
sha2-256	Specifies SHA2-256 as the authentication algorithm. SHA2-256 generates a 256-bit message summary based on a message of less than 2^{64} bits.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use ESP protocol to authenticate and encrypt packets, preventing packets from being intercepted or modified, you can run the **esp authentication-algorithm** command to configure the authentication algorithm for ESP.

Prerequisite

The protocol of this IPSec proposal has been configured to ESP using the **transform** command.

Precautions

The authentication algorithms on both IPSec peers must be identical.

The authentication algorithm and encryption algorithm cannot be both set to **NULL** for ESP.

The system software does not support the **md5** parameter. To use the **md5** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2-256** parameter.

For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the IPSec proposal **prop1** to use the ESP protocol, and specify SHA2-256 as the authentication algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform esp
[HUAWEI-ipsec-proposal-prop1] esp authentication-algorithm sha2-256
```

10.2.8 esp encryption-algorithm

Function

The **esp encryption-algorithm** command configures the encryption algorithm for ESP protocol.

The **undo esp encryption-algorithm** command cancels the encryption algorithm for ESP protocol.

By default, ESP protocol uses the Advanced Encryption Standard-256 (AES-256) encryption algorithm.

Format

esp encryption-algorithm { **3des** | **aes** [**128** | **192** | **256**] }

undo esp encryption-algorithm

Parameters

Parameter	Description	Value
3des	Indicates that ESP uses 3DES algorithm to encrypt packets.	-

Parameter	Description	Value
aes	Indicates that ESP uses Advanced Encryption Standard (AES) algorithm in CBC mode to encrypt packets. By default, If 128, 192 and 256 are not configured, AES 128 bits algorithm is used for ESP to encrypt packets.	-
128	Indicates that ESP uses AES 128 bits algorithm to encrypt packets.	-
192	Indicates that ESP uses AES 192 bits algorithm to encrypt packets.	-
256	Indicates that ESP uses AES 256 bits algorithm to encrypt packets.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use ESP protocol to authenticate and encrypt packets, preventing packets from being intercepted or modified, you can run the **esp encryption-algorithm** command to configure the encryption algorithm for ESP protocol.

Prerequisite

The protocol of this IPSec proposal has been configured to ESP using the **transform** command.

Precautions

The encryption algorithms on both IPSec peers must be identical.

The authentication algorithm and encryption algorithm cannot be both set to **NULL** for ESP.

The system software does not support the **des** parameter. To use the **des** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **aes** [**128** | **192** | **256**] parameter.

For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the IPSec proposal **prop1** to use the ESP protocol, and specify AES-128 as the encryption algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform esp
[HUAWEI-ipsec-proposal-prop1] esp encryption-algorithm aes 128
```

10.2.9 ipsec proposal

Function

The **ipsec proposal** command creates an IPSec proposal and displays the IPSec proposal view.

The **undo ipsec proposal** command deletes an IPSec proposal.

By default, no IPSec proposal is configured.

Format

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of an IPSec proposal.	The value is a string of 1 to 15 case-insensitive characters without question marks (?) or spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec proposal, part of an IPSec SA, defines security parameters for IPSec SA negotiation, including the security protocol, encryption and authentication algorithms, and encapsulation mode.

Follow-up Procedure

Run the **proposal** command to reference the IPSec proposal in an IPSec SA.

Precautions

Both ends of an IPSec tunnel must be configured with the same parameters.

You cannot delete the security proposal applied on a Security Association (SA). However, you can apply the same proposal on different SA's. To delete a security proposal, run the **undo proposal** command to remove a security proposal from the SA.

Example

Create an IPSec proposal **newprop1**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal newprop1
[HUAWEI-ipsec-proposal-newprop1]
```

10.2.10 ipsec sa

Function

The **ipsec sa** command creates an SA and displays the SA view.

The **undo ipsec sa** command deletes an SA.

By default, no SA is created.

Format

ipsec sa *sa-name*

undo ipsec sa *sa-name*

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	The value is a string of 1 to 15 case-insensitive characters without question marks (?) or spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec uses an SA to ensure security during data transmission. When configuring IPSec, run the **ipsec sa** command to create an SA and configure SA parameters.

Follow-up Procedure

Run the **proposal** command to import a security proposal; run the **sa spi** command to configure the SPI; run the **sa string-key** or **sa authentication-hex** command to configure the authentication key.

Precautions

An SA is unidirectional. Incoming packets and outgoing packets are processed by different SAs.

An SA can be configured with only one security protocol.

Example

Create an SA.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1]
```

10.2.11 proposal

Function

The **proposal** command applies a security proposal to a Security Association (SA).

The **undo proposal** command removes a security proposal from an SA.

By default, no security proposal is created.

Format

proposal *proposal-name*

undo proposal

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of an IPSec proposal.	The value is an existing IPSec proposal name.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SA defines a protection policy, and a security proposal defines a protection method. Data protection can be implemented only after a security proposal is applied to an SA.

Prerequisite

The **ipsec proposal** command has been run to create a security proposal before the **proposal** command is run. If no security proposal has been created, an error message will be displayed when the **proposal** command is run.

Before running the **proposal** command, it needs to set the encapsulation mode to transport.

Precautions

After the **proposal** command is run, the security proposal is applied to an SA and cannot be deleted.

Example

Create an IPSec proposal **prop1** and configure it to use the default parameters. Then reference the IPSec proposal in IPSec SA **sa1**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform ah
[HUAWEI-ipsec-proposal-prop1] encapsulation-mode transport
[HUAWEI-ipsec-proposal-prop1] quit
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] proposal prop1
```

10.2.12 reset ipsec statistics

Function

The **reset ipsec statistics** command clears statistics about packets processed by IPSec.

Format

reset ipsec statistics [**sa-name** *sa-name* **slot** *slot-number*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing SA name.
slot *slot-number*	Displays the IPSec SA statistics of the specified slot.	The value is an integer, and the value range depends on the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting statistics about packets processed by IPSec in a specified length of time, you can run the **reset ipsec statistics** command to clear the original statistics.

Follow-up Procedure

Run the **display ipsec statistics** command to check statistics about packets processed by IPSec.

Precautions

The statistics cannot be restored after being cleared. Therefore, confirm the action before running this command.

Example

Clear statistics about packets processed by IPSec.

```
<HUAWEI> reset ipsec statistics
```

10.2.13 sa authentication-hex

Function

The **sa authentication-hex** command sets an authentication in hexadecimal format or cipher text for Security Associations (SAs).

The **undo sa authentication-hex** command deletes an authentication key from SAs.

By default, no authentication key is created.

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] { *hex-plain-key* | *hex-cipher-key* }

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa authentication-hex** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa authentication-hex** command.	-
cipher	Indicates the cipher text used for authentication.	-
hex-plain-key	Sets the authentication password to be in plaintext format.	The value is in hexadecimal notation. ● If authentication algorithm Message Digest 5 (MD5) is used, the length of the key is 16 bytes. ● If authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used, the length of the key is 20 bytes. ● If authentication algorithm SHA2-256 is used, the length of the key is 32 bytes.

Parameter	Description	Value
hex-cipher-key	Sets the authentication password to be in ciphertext format.	The value is a string of case-insensitive characters, spaces not supported. ● If authentication algorithm MD5 is used, the length of the key is 68. ● If authentication algorithm SHA-1 is used, the length of the key is 88. ● If authentication algorithm SHA2-256 is used, the length of the key is 108.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH and ESP can use either MD5, SHA-1, or SHA-256 that require an authentication key in the string or hexadecimal format. If an authentication key in the hexadecimal format is required, run the **sa authentication-hex** command. The MD5 and SHA-1 algorithms are not recommended because they cannot meet your security defense requirements.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

SA parameters on both IPSec peers must be identical. The authentication key for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

The authentication key can be in the hexadecimal or string format. To configure an authentication key in the string format, run the **sa string-key** command. If multiple authentication keys are configured, the latest one takes effect. The formats of authentication keys on both IPSec peers must be identical. If an authentication key in the string format is configured on one end and an authentication key in the hexadecimal format on another end, the two ends cannot communicate.

Example

In an IPSec SA, set the authentication key of the inbound SA to 112233445566778899aabbccddeeff00, and the authentication key of the

outbound SA to aabbccddeeff001100aabbccddeeff00. The authentication key is displayed in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa authentication-hex inbound ah cipher 112233445566778899aabbccddeeff00
[HUAWEI-ipsec-sa-sa1] sa authentication-hex outbound ah cipher aabbccddeeff001100aabbccddeeff00
```

10.2.14 sa encryption-hex

Function

The **sa encryption-hex** command configures an encryption key for manual Security Association (SA) in hexadecimal format.

The **undo sa encryption-hex** command deletes an encryption key for manual SA configured in hexadecimal format.

By default, no encryption key is created.

Format

sa encryption-hex { **inbound** | **outbound** } **esp** [**cipher**] { *hex-plain-key* | *hex-cipher-key* }

undo sa encryption-hex { **inbound** | **outbound** } **esp**

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa encryption-hex** command.	-
cipher	Indicates the ciphertext used for encryption.	-

Parameter	Description	Value
hex-plain-key	Sets the authentication password to be in plaintext format.	The value is in hexadecimal notation. ● If encryption algorithm Data Encryption Standard (DES) is used, the length of the key is 8 bytes. ● If encryption algorithm Triple Data Encryption Standard (3DES) is used, the length of the key is 24 bytes. ● If encryption algorithm Advanced Encryption Standard 128 (AES-128) is used, the length of the key is 16 bytes. ● If encryption algorithm AES-192 is used, the length of the key is 24 bytes. ● If encryption algorithm AES-256 is used, the length of the key is 32 bytes.
hex-cipher-key	Sets the authentication password to be in ciphertext format.	The value is a string of case-insensitive characters, spaces not supported. ● If encryption algorithm DES is used, the length of the key is 48. ● If encryption algorithm 3DES is used, the length of the key is 88. ● If encryption algorithm AES-128 is used, the length of the key is 68. ● If encryption algorithm AES-192 is used, the length of the key is 88. ● If encryption algorithm AES-256 is used, the length of the key is 108.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

ESP security protocol support encryption of IP packets. The algorithm used for encryption/decryption is either DES, 3DES or AES. These algorithms need a key either in hexadecimal format to operate. The hexadecimal key to be used for encryption is configured using the **sa encryption-hex** command.

NOTICE

- The DES and 3DES algorithms have security risks; therefore, you are advised to use AES algorithm preferentially.
- If **sa encryption-hex** command is configured, then the encryption key configured using **sa string-key** command is deleted automatically.

Example

In an IPSec SA, set the encryption key of the inbound SA to 0x1234567890abcdef, and the encryption key of the outbound SA to 0xabcdefabcdef1234. The encryption key is displayed in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa encryption-hex inbound esp cipher 1234567890abcdef
[HUAWEI-ipsec-sa-sa1] sa encryption-hex outbound esp cipher abcdefabcdef1234
```

10.2.15 sa spi

Function

The **sa spi** command configures the Security Parameter Index (SPI) for a Security Association (SA).

The **undo sa spi** command deletes the SPI from an SA.

By default, no SPI is configured.

Format

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa spi** command.	-

Parameter	Description	Value
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa spi** command.	-
spi-number	Specifies the SPI.	The value is an integer ranging from 256 to 4294967295.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SPI uniquely identifies an SA. When an SPI is configured for an SA, the SPI is carried in each sent packet. The receiver checks the packet authenticity based on the SPI. When the **ipsec sa** *sa-name* command is used to create an SA, run the **sa spi** command to configure the SPI.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

The SPI for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

Example

In an IPSec SA, set the SPI of the inbound SA to 10000 and the SPI of the outbound SA to 20000.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa spi inbound ah 10000
[HUAWEI-ipsec-sa-sa1] sa spi outbound ah 20000
```

10.2.16 sa string-key

Function

The **sa string-key** command configures an authentication key in the string format.

The **undo sa string-key** command deletes an authentication key from Security Associations (SAs).

By default, no authentication key is created.

Format

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] *string-cipher-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa string-key** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa string-key** command.	-
cipher	Indicates the cipher text used for authentication.	-
string-cipher-key	Specifies the cipher text key.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 127 characters in plain text or a string of 20 to 392 characters in encrypted text. Except the question mark (?) and space. However, when quotation marks (") are used around the string, spaces are allowed in the string.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH and ESP can use either Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1) or SHA-256, that require an authentication key in the string or hexadecimal format. If an authentication key in the string format is required, run the **sa string-key** command. The MD5 and SHA-1 algorithms are not recommended because they cannot meet your security defense requirements.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

SA parameters on both IPSec peers must be identical. The authentication key for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

The authentication key can be in the hexadecimal or string format. To configure an authentication key in the hexadecimal format, run the **sa authentication-hex** command. If multiple authentication keys are configured, the latest one takes effect. The formats of authentication keys on both IPSec peers must be identical. If an authentication key in the string format is configured on one end and an authentication key in the hexadecimal format on another end, the two ends cannot communicate.

Example

In an IPSec SA, set the authentication key of the inbound SA to abcdef, and the authentication key of the outbound SA to efcdab. The authentication key is displayed in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa sa1
[HUAWEI-ipsec-sa-sa1] sa string-key inbound ah cipher abcdef
[HUAWEI-ipsec-sa-sa1] sa string-key outbound ah cipher efcdab
```

10.2.17 transform

Function

The **transform** command configures the security protocol in a security proposal.

The **undo transform** command restores the default security protocol.

By default, the Encapsulating Security Payload (ESP) protocol is used, as defined in RFC.

Format

transform { **ah** | **esp** }

undo transform

Parameters

Parameter	Description	Value
ah	Configures Authentication Header (AH) as the security protocol.	-
esp	Configures ESP as the security protocol.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When AH is specified, AH only authenticates packets.

  When AH is specified, by default, AH uses the SHA-256 authentication algorithm.
- When ESP is specified, ESP can encrypt/authenticate, or encrypt and authenticate packets.

  When ESP is specified, ESP uses the SHA-256 authentication algorithm, the AES-256 encryption algorithm.

AH prevents data tampering but cannot prevent data interception, so it applies only to the transmission of non-confidential data. ESP provides authentication service inferior to that of AH, but it can encrypt packet payloads.

Follow-up Procedure

Configure the authentication algorithm for AH when AH is used.

Configure the authentication and encryption algorithms for ESP when ESP is used.

Precautions

When multiple security proposals are configured, the latest configuration takes effect, and the default authentication and encryption algorithms will be restored.

The IPSec proposals configured on both ends of an IPSec tunnel must use the same security tunnel.

Example

Configure AH for the security proposal named **prop**.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop
[HUAWEI-ipsec-proposal-prop] transform ah
```

10.3 IPSec Configuration Commands (IPSec Efficient VPN)

10.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

10.3.2 anti-replay window

Function

The **anti-replay window** command sets the anti-replay window size for an IPSec tunnel.

The **undo anti-replay window** command restores the default anti-replay window size of an IPSec tunnel.

By default, the anti-replay window size of a single IPSec tunnel is not set. The global value is used.

Format

anti-replay window *window-size*

undo anti-replay window

Parameters

Parameter	Description	Value
window-size	Specifies the anti-replay window size of an IPSec tunnel.	The value can be 32, 64, 128, 256, 512, or 1024, in bits.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Configuration Impact

You may need to change the anti-replay window size for an IPSec tunnel in some situations. For example, if QoS is performed for packets passing an IPSec tunnel, sequence numbers of service data packets may be different from those in common data packets. As a result, these service data packets are dropped as replay attack packets. To prevent such packets from being dropped incorrectly, you can disable the anti-replay function or increase the anti-replay window size for the IPSec tunnel.

Prerequisites

The anti-replay function is enabled for the IPSec tunnel. By default, the anti-replay function is enabled (through the **ipsec anti-reply enable** command).

Precautions

When both **anti-replay window** and **ipsec anti-replay window** are configured, the **anti-replay window** configuration takes effect. When **anti-replay window** is not configured, the **ipsec anti-replay window** configuration takes effect.

Example

Set the IPSec anti-replay window size to 128 bits.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] anti-replay window 128
```

10.3.3 dh

Function

The **dh** command specifies a Diffie-Hellman (DH) group used for IKE negotiation.

The **undo dh** command restores the default DH group for IKE negotiation.

By default, group14 is used for IKE negotiation.

Format

dh { **group14** | **group19** | **group20** | **group21** }

undo dh

Parameters

Parameter	Description	Value
group14	Uses the 2048-bit DH group in IKE negotiation phase 1.	-
group19	Uses the 256-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-
group20	Uses the 384-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-

Parameter	Description	Value
group21	Uses the 521-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DH algorithm is a public key algorithm. Two communicating parties calculate a shared key based on data exchanged between them, without transmitting the key. A third party (such as a hacker) cannot calculate the actual key even if it obtains all exchanged data for key calculation.

Precautions

- Both ends of an IPSec tunnel must be configured with the same DH group. Otherwise, the negotiation fails.
- The security level order of the DH groups is: **group21** > **group20** > **group19** > **group14**.
- The system software does not support the **group1**, **group2**, and **group5** parameters. To use these DH groups, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify other DH groups.

  For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Example

Specify the 2048-bit DH group for the IPSec Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dh group14
```

10.3.4 display ike error-info

Function

The **display ike error-info** command displays information about IPSec tunnel negotiation failures using IKE.

Format

display ike error-info [**verbose**] [**peer** *remote-address*]

Parameters

Parameter	Description	Value
verbose	Displays details about IPSec tunnel negotiation failures using IKE.	-
peer *remote-address*	Displays information about IPSec tunnel negotiation failures using IKE with a specified remote IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output contains information of the latest 200 IPSec tunnel negotiation failures using IKE.

Example

Display information about IPSec tunnel negotiation failures using IKE.

```
<HUAWEI> display ike error-info

  current info Num :2
  Ike error information:
  current ike Error-info number :2
  ---------------------------------------------------------------------------
  peer       port      error-reason               version     error-time
  ---------------------------------------------------------------------------
  10.1.1.1   500       phase1 proposal mismatch     v1         2013-08-26 13:42:37
  10.1.1.1   500       phase1 proposal mismatch     v1         2013-08-26 13:08:45
  ---------------------------------------------------------------------------
```

Display details about IPSec tunnel negotiation failures using IKE.

```
<HUAWEI> display ike error-info verbose

  current info Num :1
  Ike error information:
  current ike Error-info number :1
---------------------------------------------------------------------------
Peer       : 10.1.1.1
Port       : 500
version    : v1
Reason     : phase1 proposal mismatch
Detail     : phase1 proposal mismatch
Error-time : 2013-08-26 12:02:37
---------------------------------------------------------------------------
```

Table 10-9 Description of the **display ike error-info** command output

Item	Description
current info Num	Current information number.
Ike error information	Information about IPSec tunnel negotiation failures using IKE.
current ike Error-info number	Number of IPSec tunnel negotiation failures using IKE.
peer or Peer	Peer IP address.
port or Port	Peer UDP port number.

Item	Description
error-reason or Reason	Causes for IPSec tunnel negotiation failures using IKE: ● phase1 proposal mismatch: IKE proposal parameters of the two ends do not match. ● phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match. ● responder dh mismatch: The DH algorithm of the responder does not match. ● initiator dh mismatch: The DH algorithm of the initiator does not match. ● encapsulation mode mismatch: The encapsulation mode does not match. ● flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match. ● version mismatch: The IKE version number of the two ends does not match. ● peer address mismatch: The IKE peer address of the two ends does not match. ● config ID mismatch: The IKE peer of the specified ID is not found. ● exchange mode mismatch: The negotiation mode of the two ends does not match. ● authentication fail: Identity authentication fails. ● construct local ID fail: The local ID fails to be constructed. ● rekey no find old sa: The old SA is not found during re-negotiation. ● rekey fail: The old SA is going offline during re-negotiation. ● first packet limited: The rate of the first packet is limited. ● unsupported version: The IKE version number is not supported. ● malformed message: Malformed message. ● malformed payload: Malformed payload. ● critical drop: Unidentified critical payload. ● cookie mismatch: Cookie mismatch. ● invalid cookie: Invalid cookie. ● invalid length: Invalid packet length. ● unknown exchange type: Unknown negotiation mode. ● uncritical drop: Unidentified non-critical payload. ● local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.

Item	Description
	- dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit. - ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit. - no policy applied on interface: No policy is applied to an interface. - nat detection fail: NAT detailed failed. - fragment packet limit: Fragment packets exceed the limit. - fragment packet reassemble timeout: Fragment packet reassembly times out. - max transmit reached: Tunnel negotiation fails after the number of IKE packet retransmissions reaches the maximum value. - no valid local cert: No valid CA/local certificate exists.
version	IKE version.
Error-time/error-time	Time of IPSec tunnel negotiation failures using IKE.

Item	Description
Detail	Details about IPSec tunnel negotiation failures using IKE. ● phase1 proposal mismatch: IKE proposal parameters of the two ends do not match. ● phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match. ● responder dh mismatch: The DH algorithm of the responder does not match. ● initiator dh mismatch: The DH algorithm of the initiator does not match. ● encapsulation mode mismatch: The encapsulation mode does not match. ● flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match. ● version mismatch: The IKE version number of the two ends does not match. ● peer address mismatch: The IKE peer address of the two ends does not match. ● config ID mismatch: The IKE peer of the specified ID is not found. ● exchange mode mismatch: The negotiation mode of the two ends does not match. ● authentication fail: Identity authentication fails. ● construct local ID fail: The local ID fails to be constructed. ● rekey no find old sa: The old SA is not found during re-negotiation. ● rekey fail: The old SA is going offline during re-negotiation. ● first packet limited: The rate of the first packet is limited. ● unsupported version: The IKE version number is not supported. ● malformed message: Malformed message. ● malformed payload: Malformed payload. ● critical drop: Unidentified critical payload. ● cookie mismatch: Cookie mismatch. ● invalid cookie: Invalid cookie. ● invalid length: Invalid packet length. ● unknown exchange type: Unknown negotiation mode. ● uncritical drop: Unidentified non-critical payload. ● local address mismatch: The local IP address in IKE negotiation and interface IP address do not match.

Item	Description
	● dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit. ● ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit. ● no policy applied on interface: No policy is applied to an interface. ● nat detection fail: NAT detailed failed. ● fragment packet limit: Fragment packets exceed the limit. ● fragment packet reassemble timeout: Fragment packet reassembly times out. ● max transmit reached: Tunnel negotiation fails after the number of IKE packet retransmissions reaches the maximum value. ● no valid local cert: No valid CA/local certificate exists. ● receive phase1 proposal mismatch: The received IKE proposal parameters do not match the local parameters. ● receive phase2 proposal mismatch: The received IPSec proposal parameters do not match the local parameters. ● phase2 proposal mismatch: IPSec proposal parameters on both ends do not match. ● receive flow or peer mismatch: The received security ACL or IKE peer address does not match the local one. ● (peer local or tunnel local or interface) address mismatch: The peer's local IP address, local tunnel IP address or interface IP address does not match the local one. ● remote auth method mismatch: The peer authentication method does not match. ● proc auth payload fail(pre-share-key): Failed to process the authentication payload during pre-shared key authentication. ● recv peer auth fail notification: An authentication failure notification from the peer end is received. ● recv peer auth fail notification(pre-share-key): An authentication failure notification from the peer end is received during pre-shared key authentication. ● proc and auth ID payload fail(pre-share-key): The peer ID fails to be authenticated during pre-shared key authentication.

10.3.5 display ike global config

Function

The **display ike global config** command displays global IKE configurations.

Format

display ike global config

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view global IKE configurations, such as the local name used in IKE negotiation, interval for sending heartbeat packets, timeout interval of heartbeat packets, and interval for sending NAT keepalive packets.

Example

Display global IKE configurations.

```
<HUAWEI> display ike global config
IKE Global Config:
----------------------------------------------------------------
  IKE local-name                     : huawei
  IKE heartbeat-timer interval      : 30
  IKE heartbeat-timer timeout       : 100
  IKE nat-keepalive-timer interval : 52   IKEv1 phase1-phase2 sa dependent : enable   IKE
DSCP                          : -   IKEv2 initial-contact             : enable   IKEv2 delete old child-sa         : enable
----------------------------------------------------------------
```

Table 10-10 Description of the **display ike global config** command output

Item	Description
IKE Global Config	Global IKE configurations.
IKE local-name	Local peer name used in IKE negotiation. This parameter can be configured using the **ike local-name** command. If the **ike local-name** command is not run, the device name configured using the **sysname** command is used for IKE negotiation.

Item	Description
IKE heartbeat-timer interval	Interval (in seconds) at which a device sends heartbeat packets through an IKE SA. This parameter is configured using the **ike heartbeat-timer interval** command.
IKE heartbeat-timer timeout	Timeout period (in seconds) of sending heartbeat packets through an IKE SA. This parameter is configured using the **ike heartbeat-timer timeout** command.
IKE nat-keepalive-timer interval	Interval (in seconds) at which a device sends NAT keepalive packets through an IKE SA. This parameter is configured using the **ike nat-keepalive-timer interval** command.
IKEv1 phase1-phase2 sa dependent	Dependency between an IPSec SA and an IKE SA during IKEv1 negotiation is enabled. ● enable ● disable This function is configured using the **ikev1 phase1-phase2 sa dependent** command.
IKE DSCP	Global DSCP value of IKE packets. This parameter can be configured using the **ike dscp** command.
IKEv2 initial-contact	Whether the first IKE_AUTH request message carries the INITIAL_CONTACT notification payload. ● enable ● disable This function is configured using the **ikev2 initial-contact enable** command.
IKEv2 delete old child-sa	Whether to enable the function of instructing the peer device to delete the old child SA: ● enable ● disable This function is configured using the **ikev2 delete old child-sa enable** command.

10.3.6 display ike offline-info

Function

The **display ike offline-info** command displays information about deleted IPSec tunnels established through IKE negotiation.

Format

display ike offline-info [**peer** *remote-address*]

Parameters

Parameter	Description	Value
peer *remote-address*	Displays information about deleted IPSec tunnels with a specified remote IP address and established through IKE negotiation.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output contains the possible causes and time of the latest 200 IPSec tunnel deletions.

Example

Display information about deleted IPSec tunnels established through IKE negotiation.

```
<HUAWEI> display ike offline-info

  Current info Num :2
  Ike offline information:
---------------------------------------------------------------------------
  peer              offline-reason              version     offline-time
---------------------------------------------------------------------------
  2.1.1.2           dpd timeout                  v2         2017-02-18 02:12:39
  2.1.1.2           dpd timeout                  v2         2017-02-18 01:17:06
---------------------------------------------------------------------------
```

Table 10-11 Description of the **display ike offline-info** command output

Item	Description
Current info Num	Current number of information records.
Ike offline information	Information about IPSec tunnels established through IKE negotiation have been deleted.
peer	Peer IP address of a deleted IPSec tunnel.

Item	Description
offline-reason	Causes for deletion of IPSec tunnels established through IKE negotiation: ● dpd timeout: Dead peer detection (DPD) times out. ● peer request: The remote end has sent a message, asking the local end to tear down the tunnel. ● config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted. ● phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received). ● phase2 hard expiry: Hard lifetime expires in phase 2. ● heartbeat timeout: heartbeat detection times out. ● modecfg address soft expiry: The IP address lease applied by the remote end from the server expires. ● re-auth timeout: An SA is deleted due to reauthentication timeout. ● aaa cut user: The AAA module disconnects users. ● hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. ● spi conflict: An SPI conflict occurs. ● phase1 sa replace: The new IKE SA replaces the old IKE SA. ● phase2 sa replace: The new IPSec SA replaces the old IPsec SA. ● receive invalid spi notify: The device receives an invalid SPI notification. ● dns resolution status change: DNS resolution status changes. ● ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPSec SA when deleting an IKEv1 SA. ● exchange timeout: Packet interaction timeout.
version	IKE version.
offline-time	IPSec tunnel deletion time.

10.3.7 display ike sa

Function

The **display ike sa** command displays information about SAs established through IKE negotiation.

Format

display ike sa [**remote** *ipv4-address*]

display ike sa [**remote-id-type** *remote-id-type*] **remote-id** *remote-id*

display ike sa verbose [**remote** *ipv4-address* | **connection-id** *connection-id* | [**remote-id-type** *remote-id-type*] **remote-id** *remote-id*]

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote peer.	The value is in dotted decimal notation.
remote-id-type *remote-id-type*	Specifies a remote ID type.	The remote ID type can be ip, key-id, fqdn, or user-fqdn.
remote-id *remote-id*	Specifies the remote ID.	The remote ID must be an existing one.
verbose	Displays detailed information about SAs. **NOTE** If only this parameter is specified (other parameters are not specified), the command displays detailed information about all SAs.	-
connection-id *connection-id*	Specifies the connection ID of an SA.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ike sa** command to check the following SA information: connection ID, peer IP address, VPN instance name, SA phase, remote ID type, remote ID, and SA status.

NOTE

After an IPSec tunnel is established successfully, the **display ike sa** command does not display the latest local ID or remote ID until the IPSec tunnel is re-negotiated if the local ID or remote ID is modified.

Example

Display IKE SAs and IPSec SAs.

```
<HUAWEI> display ike sa
IKE SA information :
   Conn-ID       Peer            VPN    Flag(s)    Phase    RemoteType   RemoteID
 ----------------------------------------------------------------------------------
   117477244     10.100.1.1/4500 vrf1   RD|M       v2:2     IP           10.100.1.1
   117477242     10.100.1.1/4500 vrf1   RD|M       v2:1     IP           10.100.1.1

  Number of IKE SA : 2
 ----------------------------------------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Table 10-12 Description of the **display ike sa** command output

Item	Description
IKE SA information	Configuration of SAs.
Conn-ID	Connection ID of an SA.
Peer	IP address and UDP port number of the peer.
VPN	VPN instance bound to the interface where the IPSec policy was applied to.

Item	Description
Flag(s)	SA status: - RD--READY: The SA has been established successfully. - ST--STAYALIVE: This end is the initiator of tunnel negotiation. - RL--REPLACED: This SA has been replaced by a new one and will be deleted after a period of time. - FD--FADING: A soft timeout has occurred, but the SA is still in use. The SA will be deleted when the hard lifetime expires. - TO--TIMEOUT: This SA has not received any heartbeat packet after the last heartbeat timeout. The SA will be deleted if it still does not receive any heartbeat packet till the next heartbeat timeout. - HRT--HEARTBEAT: The local IKE SA sends heartbeat packets. - LKG--LAST KNOWN GOOD SEQ NO: It is the last known sequence number. - BCK--BACKED UP: The SA is backed up. - M--ACTIVE: The IPSec policy group is in active state. - S--STANDBY: The IPSec policy group is in standby state. - A--ALONE: The IPSec policy group is not backed up. - NEG--NEGOTIATING: The devices are negotiating an SA. - Empty: IKE SA negotiation is being performed because the settings at the two ends of the tunnel are inconsistent.
Phase	Phases of the SA: - v1:1 or v2:1: v1 and v2 are IKE versions. The digit 1 indicates the phase during which a security channel, that is IKE SA, is established. - v1:2 or v2:2: v1 and v2 are IKE versions. The digit 2 indicates the phase during which a security service, that is IPSec SA, is negotiated.
RemoteType	Remote ID type.
RemoteID	Remote ID.

Display detailed information about established IKE SAs and IPSec SAs when the peers use IKEv1 to negotiate IPSec SAs.

```
<HUAWEI> display ike sa verbose remote 10.100.1.1
------------------------------------------------
Ike Sa phase   : 2
Establish Time : 2017-02-08 13:10:29
```

```
PortCfg Index  : 0x448
IKE Peer Name  : _resv_ikev1__1
Connection Id  : 26
Version        : v1
Flow VPN       :
Peer VPN       :
------------------------------------------------
Initiator Cookie        : 0x33d7a5bbf8ad12bb
Responder Cookie        : 0xf311b3991d739d38
Local Address           : 10.1.1.1/500
Remote Address          : 10.100.1.1/500
PFS                     :
Flags                   : RD|ST|A
------------------------------------------------

------------------------------------------------
Ike Sa phase   : 1
Establish Time : 2017-02-07 20:57:48
PortCfg Index  : 0x448
IKE Peer Name  : _resv_ikev1__1
Connection Id  : 7
Version        : v1
Exchange Mode  : Aggressive
Flow VPN       :
Peer VPN       :
------------------------------------------------
Initiator Cookie               : 0x33d7a5bbf8ad12bb
Responder Cookie               : 0xf311b3991d739d38
Local Address                  : 10.1.1.1/500
Remote Address                 : 10.100.1.1/500
Encryption Algorithm           : 3DES-CBC
Authentication Algorithm       : SHA1
Authentication Method          : Pre-Shared key
DPD Capability                 : Yes
DPD Enable                     : Yes
DPD Message Learning Enable    : Yes
DPD Message Format             : Seq-Notify-Hash
Reference Counter              : 0
Flags                          : RD|ST|A
Local Id Type                  : IP
local Id                       : 10.1.1.1
Remote Id Type                 : IP
Remote Id                      : 10.1.1.2
DH Group                       : 2
NAT Traversal Version          : RFC3947
SA Remaining Soft Timeout (sec):100 SA Remaining Hard Timeout (sec):200
------------------------------------------------

  Number of IKE SA : 2
------------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Display detailed information about established IKE SAs and IPSec SAs when the peers use IKEv2 to negotiate IPSec SAs.

```
<HUAWEI> display ike sa verbose remote 10.100.1.1
------------------------------------------------
Ike Sa phase   : 2
Establish Time : 2017-02-20 22:07:57
PortCfg Index  : 0x98
IKE Peer Name  : _resv_ikev2__1
Connection Id  : 4
Version        : v2
Flow VPN       :
Peer VPN       :
------------------------------------------------
```

```
Initiator Cookie        : 0x039b87ea4e1e91b2
Responder Cookie        : 0xdedd86121d2038d7
Local Address           : 10.1.1.1/500
Remote Address          : 10.100.1.1/4500
PFS                     :
Flags                   : RD|ST|A
------------------------------------------------

------------------------------------------------
Ike Sa phase   : 1
Establish Time : 2017-02-20 22:07:57
PortCfg Index  : 0x98
IKE Peer Name  : _resv_ikev2__1
Connection Id  : 3
Version        : v2
Flow VPN       :
Peer VPN       :
------------------------------------------------
Initiator Cookie                     : 0x039b87ea4e1e91b2
Responder Cookie                     : 0xdedd86121d2038d7
Local Address                        : 10.1.1.1/500
Remote Address                       : 10.100.1.1/4500
Encryption Algorithm                 : 3DES-CBC
Authentication Method                : Pre-Shared key
Integrity Algorithm                  : hmac-sha1-96
Prf Algorithm                        : hmac-sha1
DPD Capability                       : Yes
DPD Enable                           : Yes
Reference Counter                    : 1
Flags                                : RD|ST|A
Local Id Type                        : IP
Local Id                             : huawei1Remote Id Type                        : IP
Remote Id                            : huawei
DH Group                             : 14
Re-authentication remaining time (sec) : -
SA Remaining Soft Timeout (sec)        :100
SA Remaining Hard Timeout (sec)        :200
------------------------------------------------

  Number of IKE SA : 2
------------------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
  M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Table 10-13 Description of the **display ike sa verbose** command output

Item	Description
Ike Sa phase	Phases of the SA: - 1: IKE peers establish an IPSec tunnel. An IKE SA is established in this phase. - 2: IKE peers negotiate security services. An IPSec SA is established in this phase.
Establish Time	Time when the SA was created.
PortCfg Index	Index of the interface where the IPSec policy was applied to.
IKE Peer Name	IKE peer name.

Item	Description
Connection Id	Connection ID of an SA.
Version	IKE version of the IKE peer: ● v1: IKEv1 is enabled. ● v2: IKEv2 is enabled. ● v1v2: Both IKEv1 and IKEv2 are enabled.
Exchange Mode	Negotiation mode of the IKEv1 phase 1. ● Main: main mode. ● Aggressive: aggressive mode.
Flow VPN	VPN to which the data flow belongs.
Peer VPN	VPN to which the peer belongs.
Initiator Cookie	Cookie of the initiator.
Responder Cookie	Cookie of the responder.
Local Address	Local IP address of an IPSec tunnel.
Remote Address	Remote IP address and UDP port number of an IPSec tunnel.
Encryption Algorithm	Encryption algorithm in the IKE proposal.
Authentication Algorithm	Authentication algorithm in the IKE proposal.
Authentication Method	Authentication method in the IKE proposal.
Integrity Algorithm	Integrity algorithm used in an IKEv2 proposal.
Prf Algorithm	Pseudo-random function (PRF) used in an IKEv2 proposal.
DPD Capability	Whether DPD capability is successfully negotiated. ● yes ● no
DPD Enable	Whether the DPD function is enabled. ● yes ● no
DPD Message Learning Enable	Whether automatic learning of the payload sequence of DPD packets is enabled. ● Yes ● No To configure the automatic learning function, run the **dpd msg notify-hash-sequence learning** command.

Item	Description
DPD Message Format	Sequence of the payload in DPD packets. ● Seq-Notify-Hash ● Seq-Hash-Notify
Reference Counter	Number of IPSec SAs negotiated by the IKE SA.
PFS	Perfect Forward Secrecy (PFS) when the local end initiates negotiation.
Flags	SA status: ● RD--READY: The SA has been established successfully. ● ST--STAYALIVE: This end is the initiator of tunnel negotiation. ● RL--REPLACED: This SA has been replaced by a new one and will be deleted after a period of time. ● FD--FADING: A soft timeout has occurred, but the SA is still in use. The SA will be deleted when the hard lifetime expires. ● TO--TIMEOUT: This SA has not received any heartbeat packet after the last heartbeat timeout. The SA will be deleted if it still does not receive any heartbeat packet till the next heartbeat timeout. ● HRT--HEARTBEAT: The local IKE SA sends heartbeat packets. ● LKG--LAST KNOWN GOOD SEQ NO: It is the last known sequence number. ● BCK--BACKED UP: The SA is backed up. ● M--ACTIVE: The IPSec policy group is in active state. ● S--STANDBY: The IPSec policy group is in standby state. ● A--ALONE: The IPSec policy group is not backed up. ● NEG--NEGOTIATING: The devices are negotiating an SA. ● Empty: IKE SA negotiation is being performed because the settings at the two ends of the tunnel are inconsistent.
Local Id Type	Local ID type.
Local Id	Local ID for IKE negotiation.
Remote Id Type	Remote ID type.
Remote Id	Remote ID for IKE negotiation.
DH Group	DH group in the IKE proposal.

Item	Description
NAT Traversal Version	Version of NAT traversal. - draft-ietf-ipsec-nat-t-ike-00 - draft-ietf-ipsec-nat-t-ike-02 - RFC3947
Re-authentication remaining time (sec)	Remaining time for IKEv2 to initiate re-authentication, in seconds.
SA Remaining Soft Timeout (sec)	Soft remaining lifetime of an IKE SA, in seconds.
SA Remaining Hard Timeout (sec)	Hard remaining lifetime of an IKE SA, in seconds.
Number of IKE SA	Total number of IKE SAs and IPSec SAs.

10.3.8 display ike statistics

Function

The **display ike statistics** command displays IKE statistics.

Format

display ike statistics { **v1** | **v2** }

Parameters

Parameter	Description	Value
v1	Displays IKEv1 statistics.	-
v2	Displays IKEv2 statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on the IPSec tunnel that is established through IKE negotiation, you can check statistics about IKE peers, IKE SAs, and DPD packets to diagnose and locate the fault.

Example

Display IKEv1 statistics.

```
<HUAWEI> display ike statistics v1
--------------------------------------------------------------------------------
 IKE V1 statistics information

 Number of total peers                         : 7
 Maximum of total peers in history             : 0
 Begin time of total peers                     : 2015-04-08 21:23:10
 Maximum time of total peers                   : 2015-04-08 21:23:10
 Number of proposals                           : 4
 Number of established V1 phase 1 SAs          : 0
 Number of established V1 phase 2 SAs          : 0
 Number of total V1 phase 1 SAs                : 0
 Number of total V1 phase 2 SAs                : 0
 Number of total SAs                           : 0
 Maximum of V1 phase 1 SAs in history          : 0
 Begin time of V1 phase 1 SAs                  : 2015-04-08 21:23:10
 Maximum time of V1 phase 1 SAs                : 2015-04-08 21:23:10
 Maximum of V1 phase 2 SAs in history          : 0
 Begin time of V1 phase 2 SAs                  : 2015-04-08 21:23:10
 Maximum time of V1 phase 2 SAs                : 2015-04-08 21:23:10
 Maximum of total SAs in history               : 0
 Begin time of total SAs                       : 2015-04-08 21:23:10
 Maximum time of total SAs                     : 2015-04-08 21:23:10
 Number of messages in V1 fast queue           : 0
 Number of messages in V1 slow queue           : 0
 Number of DPD request sent                    : 0
 Number of DPD ack received                    : 0
 Number of DPD request received                : 0
 Number of DPD ack sent                        : 0
 Number of DPD request receive dropped         : 0
 Number of DPD ack receive dropped             : 0
--------------------------------------------------------------------------------
```

Display IKEv2 statistics.

```
<HUAWEI> display ike statistics v2
--------------------------------------------------------------------------------
 IKE V2 statistics information

 Number of total peers                         : 0
 Maximum of total peers in history             : 0
 Begin time of total peers                     : 2015-04-08 21:23:10
 Maximum time of total peers                   : 2015-04-08 21:23:10
 Number of proposals                           : 4
 Number of established V2 phase 1 SAs          : 0
 Number of established V2 phase 2 SAs          : 0
 Number of total V2 phase 1 SAs                : 0
 Number of total V2 phase 2 SAs                : 0
 Number of total SAs                           : 0
 Maximum of V2 phase 1 SAs in history          : 0
 Begin time of V2 phase 1 SAs                  : 2015-04-08 21:23:10
 Maximum time of V2 phase 1 SAs                : 2015-04-08 21:23:10
 Maximum of V2 phase 2 SAs in history          : 0
 Begin time of V2 phase 2 SAs                  : 2015-04-08 21:23:10
 Maximum time of V2 phase 2 SAs                : 2015-04-08 21:23:10
 Maximum of total SAs in history               : 0
 Begin time of total SAs                       : 2015-04-08 21:23:10
```

```
Maximum time of total SAs                    : 2015-04-08 21:23:10
Number of messages in V2 fast queue          : 0
Number of messages in V2 slow queue          : 0
Number of DPD request sent                   : 0
Number of DPD ack received                   : 0
Number of DPD request received               : 0
Number of DPD ack sent                       : 0
Number of DPD request receive dropped        : 0
Number of DPD ack receive dropped            : 0
--------------------------------------------------------------------------------
```

Table 10-14 Description of the **display ike statistics** command output

Item	Description
IKE V1 statistics information	IKEv1 statistics.
IKE V2 statistics information	IKEv2 statistics.
Number of total peers	Total number of peers.
Maximum of total peers in history	Historical maximum number of IKE peers.
Begin time of total peers	Time when the system started to count the number of IKE peers.
Maximum time of total peers	Time when the total number of IKE peers reached the maximum value.
Number of proposals	Number of IKE proposals.
Number of established V1/V2 phase 1 SAs	Total number of IKE SAs that have been established successfully.
Number of established V1/V2 phase 2 SAs	Total number of IPSec SAs that have been established successfully.
Number of total V1/V2 phase 1 SAs	Total number of IKE SAs.
Number of total V1/V2 phase 2 SAs	Total number of IPSec SAs.
Number of total SAs	Total number of SAs.
Maximum of V1/V2 phase 1 SAs in history	Maximum number of IKE SAs in the history.
Begin time of V1/V2 phase 1 SAs	Time when the system started to count the number of IKE SAs.

Item	Description
Maximum time of V1/V2 phase 1 SAs	Time when the total number of IKE SAs reaches the maximum value.
Maximum of V1/V2 phase 2 SAs in history	Maximum number of IPSec SAs in the history.
Begin time of V1/V2 phase 2 SAs	Time when the system started to count the number of IPSec SAs.
Maximum time of V1/V2 phase 2 SAs	Time when the total number of IPSec SAs reached the maximum value.
Maximum of total SAs in history	Maximum number of total SAs in the history.
Begin time of total SAs	Time when the system started to count the total number of SAs.
Maximum time of total SAs	Time when the total number of SAs reached the maximum value.
Number of messages in V1/V2 fast queue	Number of IKE messages in high-priority queues.
Number of messages in V1/V2 slow queue	Number of IKE messages in low-priority queues.
Number of DPD request sent	Number of DPD request packets sent from the local end.
Number of DPD ack received	Number of DPD ack packets received by the local end.
Number of DPD request received	Number of DPD request packets received by the local end.
Number of DPD ack sent	Number of DPD ack packets sent from the local end.
Number of DPD request receive dropped	Number of received DPD request packets that are dropped.
Number of DPD ack receive dropped	Number of received DPD response packets that are dropped.

10.3.9 display ikev2 statistics

Function

The **display ikev2 statistics** command displays statistics on IPSec tunnels negotiated using IKEv2.

Format

display ikev2 statistics { **error** | **notify-info** | **packet** | **sa** }

Parameters

Parameter	Description	Value
error	Displays error statistics on IPSec tunnels negotiated using IKEv2.	-
notify-info	Displays notification message statistics on IPSec tunnels negotiated using IKEv2.	-
packet	Displays packet statistics on IPSec tunnels negotiated using IKEv2.	-
sa	Displays SA statistics on IPSec tunnels negotiated using IKEv2.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view error, packet, SA, and notification message statistics on IPSec tunnels negotiated using IKEv2.

Example

Display error statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics error

Error statistics:
--------------------------------------------------------------------------------
```

```
Config error:
Version error            :0
Peer address can not match with any ike peer config                  :0
Phase1 proposal mismatch :0           Phase2 proposal or pfs mismatch:0
Responder dh mismatch    :0           Initiator dh mismatch          :0
Flow mismatch            :1
ID can not match with any ike peer config                            :0
Construct local id fail                                              :0
Authentication fail (may be pre-shared-key error)                    :0
Peer's flow netmask range is too wide                                :0
-----------------------------------------------------------------------------
Packet or payload error:
Invalid length           :0
Message-id unordered     :0
Unknown exchange type    :0
Invalid cookie           :6
Shortpacket              :0
Malformed message        :4
Malformed payload        :0
Rekey, not find old child:0           Rekey, old child close         :14
Exchange-type or role(initiator or responder) mismatch               :0
Unexpected critical payload, drop                                    :0
Unexpected uncritical payload, ignore                                :0
-----------------------------------------------------------------------------
Maybe ddos attack:
Responder request IKEV2_COOKIE                                       :0
Responder receive invalid cookie for IKEV2_COOKIE request            :0
Responder receive no cookie for IKEV2_COOKIE request                 :0
-----------------------------------------------------------------------------
System abnormal:
Fail decrypt             :0           Fail encrypt                   :0
Fail integrity check     :0
No memory, fail send packet                                          :0
No memory, fail process packet                                       :0
-----------------------------------------------------------------------------
System limited:
First packet speed limited :0             License limited          :0
-----------------------------------------------------------------------------
```

Table 10-15 Description of the **display ikev2 statistics error** command output

Item	Description
Error statistics	Error statistics.
Config error	Configurations are incorrect.
Version error	The IKE version does not match.
Peer address can not match with any ike peer config	The corresponding IKE peer is not found based on the peer address.
Phase1 proposal mismatch	The phase 1 IPSec proposal does not match.
Phase2 proposal or pfs mismatch	The phase 2 IPSec proposal or PFS does not match.

Item	Description
Responder dh mismatch	DH group match on the responder failed. (If a matching DH group is available in the algorithm list of the initiator, the responder will send an information message to the initiator to instruct the initiator to start negotiation using the matching DH group. If the initiator accepts the information message, the negotiation succeeds.)
Initiator dh mismatch	DH group match on the initiator failed. (The initiator failed to process the message requesting a matching DH group.)
Flow mismatch	The data flow does not match.
ID can not match with any ike peer config	The peer ID does not match that configured in the IKE peer.
Construct local id fail	Local ID construction failed.
Authentication fail (may be pre-shared-key error)	Authentication failed. The possible cause is that the pre-shared key does not match.
Peer's flow netmask range is too wide	The mask length of the peer flow is too large.
Packet or payload error	Incorrect packet or payload.
Invalid length	Invalid length.
Message-id unordered	Message ID out of order.
Unknown exchange type	Unknown exchange type.
Invalid cookie	Invalid cookie: ● The corresponding SA does not exist in the received IKEv2 message that does not trigger negotiation. ● The cookie in the IKEv2 message that triggers negotiation is 0.
Shortpacket	The packet is too short.
Malformed message	Invalid message.
Malformed payload	Invalid payload.
Rekey, not find old child	The old IPSec SA is not found for re-negotiation.
Rekey, old child close	The old IPSec SA is offline for re-negotiation.

Item	Description
Exchange-type or role(initiator or responder) mismatch	The exchange type or role (initiator or responder) does not match.
Unexpected critical payload, drop	The unidentified key payload is dropped.
Unexpected uncritical payload, ignore	The unidentified key payload is ignored.
Maybe ddos attack	Maybe DDoS attacks occur.
Responder request IKEV2_COOKIE	The device requests a cookie when the SA in negotiation status exceeds the threshold.
Responder receive invalid cookie for IKEV2_COOKIE request	The received cookie is invalid.
Responder receive no cookie for IKEV2_COOKIE request	No cookie is received.
System abnormal	The system is abnormal.
Fail decrypt	Decryption failed.
Fail encrypt	Encryption failed.
Fail integrity check	Integrity check failed.
No memory, fail send packet	Packet sending failed due to insufficient memory.
No memory, fail process packet	Packet parsing failed due to insufficient memory.
System limited	System restriction.
First packet speed limited	The rate of the first packet is limited.
License limited	License restriction.

Display notification message statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics notify-info

Ikev2 notification statistics:
------------------------------------------------------------------------------
Notification:
INVALID_IKE_SPI notification              send:0          receive:0
```

```
INVALID_MAJOR_VERSION notification          send:0          receive:0
INVALID_SYNTAX notification                 send:0          receive:0
INVALID_IPSEC_SPI notification              send:0          receive:0
INVALID_KE_PAYLOAD notification             send:0          receive:0
SINGLE_PAIR_REQUIRED notification           send:0          receive:0
NO_ADDITIONAL_SA notification               send:0          receive:0
TS_UNACCEPTABLE notification                send:0          receive:0
INVALID_IPSEC_SELECTORS notification        send:0          receive:0
INITIAL_CONTACT payload                     send:0          receive:0
SET_WINDOW_SIZE payload                     send:0          receive:0
NAT_DETECTION_SOURCE_IP payload             send:0          receive:0
NAT_DETECTION_DESTINATION_IP payload        send:0          receive:0
USE_TRANSPORT_MODE notification             send:0          receive:0
REKEY_SA notification                       send:0          receive:0
ESP_TFC_PADDING_NOT_SUPPORTED payload       send:0          receive:0
AUTH_LIFETIME payload                       send:0          receive:0
REDIRECT payload                            send:0          receive:0
DELETE_OLD_CHILDSA notification             send:0          receive:0
DSCP payload                                send:0          receive:0
IKEV2_FRAGMENTATION_SUPPORTED payload       send:0          receive:0
------------------------------------------------------------------------------
```

Table 10-16 Description of the **display ikev2 statistics notify-info** command output

Item	Description
Ikev2 notification statistics	IKEv2 notification message statistics.
Notification	IKEv2 notification message.
INVALID_IKE_SPI notification	Invalid IKE SPI notification message.
INVALID_MAJOR_VERSION notification	Invalid Major version number notification message.
INVALID_SYNTAX notification	Invalid syntax notification message.
INVALID_IPSEC_SPI notification	Invalid IPSec SPI notification message.
INVALID_KE_PAYLOAD notification	Incorrect KE payload.
SINGLE_PAIR_REQUIRED notification	Single_Pair_Required notification message.
NO_ADDITIONAL_SA notification	No additional SA notification message.
TS_UNACCEPTABLE notification	Invalid TS payload.
INVALID_IPSEC_SELECTORS notification	Invalid IPSec Selectors notification message.
INITIAL_CONTACT payload	Initial_Contact notification message.

Item	Description
SET_WINDOW_SIZE payload	Set_Window_Size notification message.
NAT_DETECTION_SOURCE_IP payload	NAT source IP notification message.
NAT_DETECTION_DESTINATION_IP payload	NAT destination IP notification message.
USE_TRANSPORT_MODE notification	Transport mode notification message.
REKEY_SA notification	SA re-negotiation notification message.
ESP_TFC_PADDING_NOT_SUPPORTED payload	ESP_TFC_Padding_Not_Supported notification message.
AUTH_LIFETIME payload	Auth_Lifetime notification message.
REDIRECT payload	Redirection notification message.
DELETE_OLD_CHILDSA notification	Delete_Old_ChildSa notification message.
DSCP payload	DSCP notification message.
IKEV2_FRAGMENTATION_SUPPORTED payload	IKEV2_FRAGMENTATION_SUPPORTED notify payload message.
send	Number of sent messages.
receive	Number of received messages.

Display packet statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics packet

Packet statistics:
-----------------------------------------------------------------------------
Ike_init request  send   :0           Ike_init request   recv   :0
Ike_init response recv   :0           Ike_init response  send   :0
Ike_auth request  send   :0           Ike_auth request   recv   :0
Ike_auth response recv   :0           Ike_auth response  send   :0
Create_child req  send   :0           Create_child req   recv   :0
Create_child resp recv   :0           Create_child resp  send   :0
Ike_info request  send   :0           Ike_info request   recv   :0
Ike_info response recv   :0           Ike_info response  send   :0
Del_info request  send   :0           Del_info request   recv   :0
Del_info response recv   :0           Del_info response  send   :0
DPD_info request  send   :0           DPD_info request   recv   :0
DPD_info response recv   :0           DPD_info response  send   :0
DPD_info req recv drop   :0           DPD_info resp recv drop   :0
Fragment message  send   :0           Fragment message   recv   :0
```

```
Fragment packet   send   :0           Fragment packet    recv   :0

Ike_init request resend  :0
Ike_auth request resend  :0
Create_child req resend  :0
Ike_info request resend  :0
--------------------------------------------------------------------------------
```

Table 10-17 Description of the **display ikev2 statistics packet** command output

Item	Description
Packet statistics	IPSec packet statistics.
Ike_init request send	Number of sent IKE SA initialization exchange (ike_init) request packets.
Ike_init request recv	Number of received ike_init request packets.
Ike_init response recv	Number of received ike_init response packets.
Ike_init response send	Number of sent ike_init response packets.
Ike_auth request send	Number of sent IKE authentication exchange (ike_auth) request packets.
Ike_auth request recv	Number of received ike_auth request packets.
Ike_auth response recv	Number of received ike_auth response packets.
Ike_auth response send	Number of sent ike_auth response packets.
Create_child req send	Number of sent IPSec SA for sub-tunnel creation (create_child) request packets.
Create_child req recv	Number of received create_child request packets.
Create_child resp recv	Number of received create_child response packets.
Create_child resp send	Number of sent create_child response packets.
Ike_info request send	Number of sent IKE notification exchange (ike_info) request packets.
Ike_info request recv	Number of received ike_info request packets.
Ike_info response recv	Number of received ike_info response packets.
Ike_info response send	Number of sent ike_info response packets.

Item	Description
Del_info request send	Number of sent tunnel information deletion (del_info) request packets.
Del_info request recv	Number of received del_info request packets.
Del_info response recv	Number of received del_info response packets.
Del_info response send	Number of sent del_info response packets.
Dpd_info request send	Number of sent DPD information (dpd_info) request packets.
Dpd_info request recv	Number of received dpd_info request packets.
Dpd_info response recv	Number of received dpd_info response packets.
Dpd_info response send	Number of sent dpd_info response packets.
Dpd_info req recv drop	Number of received dpd_info request packets that are dropped.
Dpd_info resp recv drop	Number of received dpd_info response packets that are dropped.
Fragment message send	Number of sent fragment messages.
Fragment message recv	Number of received fragment messages.
Fragment packet send	Number of sent fragment packets.
Fragment packet recv	Number of received fragment packets.
Ike_init request resend	Number of retransmitted ike_init requests.
Ike_auth request resend	Number of retransmitted ike_auth requests.
Create_child req resend	Number of retransmitted create_child requests.
Ike_info request resend	Number of retransmitted ike_info requests.

Display SA statistics on IPSec tunnels negotiated using IKEv2.

```
<HUAWEI> display ikev2 statistics sa

Sa establish and offline statistic:
------------------------------------------------------------------------------
Establish:
Initiator request phase1 negotiation                         :33
Initiator request phase2 negotiation                         :16
Initiator request and success phase1 negotiation             :10
Initiator request and success phase2 negotiation             :41
Responder response phase1 negotiation                        :0
Responder response phase2 negotiation                        :0
Responder response and success phase1 negotiation            :0
Responder response and success phase2 negotiation            :0
Offline:
Receive delete info      :1          Config modify           :0
Manual reset             :1          Dpd timeout             :0
Phase1 hardware expire   :0          Phase2 hardware expire  :0
Phase1 replace           :0          Phase2 replace          :0
Aaa cut user             :0          Reauth timeout          :0
Flow overlap             :0          IP address syn failed   :0
Port mismatch            :0          Kick old SA             :0
CPU table updated        :0          SPI conflict            :0
EAP delete old sa        :0          Hash gene adjusted      :0
------------------------------------------------------------------------------
```

Table 10-18 Description of the **display ikev2 statistics sa** command output

Item	Description
Sa establish and offline statistic	SA establishment and deletion information.
Establish	Statistics on established IPSec tunnels.
Initiator request phase1 negotiation	Number of times that the initiator requests phase 1 negotiation.
Initiator request phase2 negotiation	Number of times that the initiator requests phase 2 negotiation.
Initiator request and success phase1 negotiation	Number of times that the initiator succeeds in requesting phase 1 negotiation.
Initiator request and success phase2 negotiation	Number of times that the initiator succeeds in requesting phase 2 negotiation.
Responder response phase1 negotiation	Number of times that the responder responds to phase 1 negotiation.
Responder response phase2 negotiation	Number of times that the responder responds to phase 2 negotiation.
Responder response and success phase1 negotiation	Number of times that the responder succeeds in responding to phase 1 negotiation.
Responder response and success phase2 negotiation	Number of times that the responder succeeds in responding to phase 2 negotiation.

Item	Description
Offline	Statistics on deleted IPSec tunnels.
Receive delete info	Number of times that the device receives tunnel deletion messages.
Config modify	Number of times that the tunnel is deleted by modifying the configuration.
Manual reset	Number of times that the tunnel is deleted manually.
Phase1 hardware expire	Number of times that the phase 1 tunnel is deleted due to hard timeout.
Phase2 hardware expire	Number of times that the phase 2 tunnel is deleted due to hard timeout.
Phase1 replace	Number of phase 1 tunnel re-negotiation times.
Phase2 replace	Number of phase 2 tunnel re-negotiation times.
Aaa cut user	Number of tunnel deletion times caused by forced user offline.
Dpd timeout	Number of tunnel deletion times caused by DPD timeout.
Reauth timeout	Number of tunnel deletion times caused by re-authentication timeout.
Flow overlap	Number of tunnel deletion times caused by the conflict between the IP address in the encrypted flow and remote IP address.
IP address syn failed	Number of tunnel deletion times caused by the failure to synchronize IP addresses.
Port mismatch	Number of tunnel deletion times caused by the UDP port mismatch.
Kick old SA	Number of tunnel deletion times caused by a flow conflict.
CPU table updated	Number of tunnel deletion times caused by a CPU table update.
SPI conflict	Number of tunnel deletion times caused by an SPI conflict.
EAP delete old sa	Number of times the device deletes the old SA during EAP authentication.
Hash gene adjusted	Number of tunnel deletion times caused by hash factor adjustment.

10.3.10 display ipsec efficient-vpn

Function

The **display ipsec efficient-vpn** command displays Efficient VPN policy information.

Format

display ipsec efficient-vpn [**brief** | **capability** | **name** *efficient-vpn-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about Efficient VPN policies.	-
capability	Displays the IPSec configuration supported by an Efficient VPN policy.	-
name *efficient-vpn-name*	Displays information about a specified Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Efficient VPN policy is configured, you can run this command to know the configuration information of the Efficient VPN policy, such as the name, interface, authentication method, IKE version, DH algorithm, and PFS algorithm of the Efficient VPN.

Example

Display brief information about Efficient VPN policies.

```
<HUAWEI> display ipsec efficient-vpn brief
 Total number of IPSec efficient-vpn: 1

 Efficient-vpn name       Efficient-vpn mode
 ------------------------------------------
 v1                       client
```

Display information about the Efficient VPN policy named **easyvpn_1**.

```
<HUAWEI> display ipsec efficient-vpn name easyvpn_1
===========================================IPSec efficient-vpn name: easyvpn_1
Using interface         : Vlanif27
===========================================
 IPSec Efficient-vpn Mode  : 1 (1:Client 2:Network 3:Network-plus)
 ACL Number                :
 Auth Method               : 8 (8:PSK)
 VPN name                  : wbh
 Local ID Type             : 11 (1:IP 2:Name 3:User-fqdn 11:Key-id)
 IKE Version               : 2 (1:IKEv1 2:IKEv2)
 Remote Address            : 10.10.10.1
 Pre Shared Key Cipher     : ******
 DH Group                  : DH group 14
 PFS Type                  : DH group 14 Remote Name               :
 Re-auth interval          : 400 seconds
 Anti-replay window size   : 0
 Service-scheme name       : ser
 DPD message  type         : seq-notify-hash
 DPD message  learning     : enable
 Interface loopback        : LoopBack0
 Interface loopback IP     : 1.1.1.1/32
```

Table 10-19 Description of the **display ipsec efficient-vpn** command output

Item	Description
Total number of IPSec efficient-vpn	Total number of the Efficient VPN policy.
Efficient-vpn name/IPSec Efficient-vpn Name	Name of the Efficient VPN policy. To configure an Efficient VPN policy, run the **ipsec efficient-vpn (system view)** command.
Using interface	Interface to which an Efficient VPN policy is applied.
Efficient-vpn mode/IPSec Efficient-vpn Mode	Mode used by the Efficient VPN policy. ● 1: client ● 2: network ● 3: network-plus To configure an Efficient VPN policy, run the **ipsec efficient-vpn (system view)** command.
ACL Number	ACL used by the Efficient VPN policy. To configure an ACL referenced by an Efficient VPN policy, run the **security acl** command.
Auth Method	Authentication method used by the Efficient VPN policy is pre-shared key authentication (8).
VPN name	Name of the VPN instance bound to the Efficient VPN policy. To bind a VPN instance to an Efficient VPN policy, run the **sa binding vpn-instance (Efficient VPN policy view)** command.

Item	Description
Local ID Type	Local ID type in IKE negotiation. ● 1: IP ● 2: Name ● 3: User-fqdn ● 11: Key-id To set the local ID type, run the **local-id-type** command.
IKE Version	Configured IKE version: ● 1: IKEv1 ● 2: IKEv2
Remote Address	IP address of the remote IKE peer. To configure the remote IP address, run the **remote-address** command.
Pre Shared Key Cipher	Pre-shared key. To configure a pre-shared key, run the **pre-shared-key** (Efficient VPN policy view) command.
DH Group	DH group used in IKE negotiation. To specify a DH group, run the **dh** command.
PFS Type	Perfect Forward Secrecy (PFS) used in IKE negotiation. To specify a PFS, run the **pfs** command.
Remote Name	Remote name used in IKE negotiation.
Re-auth interval	IKEv2 re-authentication interval. To configure an IKEv2 re-authentication interval, run the **re-authentication interval** command.
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **anti-replay window** command. When the value is 0, the IPSec anti-replay function is enabled in the system view. To enable this function, run the **ipsec anti-replay enable** command.
Service-scheme name	Name of the bound service scheme. To configure the name of the bound service scheme, run the **service-scheme** command.

Item	Description
DPD message type	Sequence of the payload in DPD packets. - seq-notify-hash - seq-hash-notify To configure the sequence of the payload, run the **dpd msg** command.
DPD message learning	Whether automatic learning of the payload sequence of DPD packets is enabled. - enable - disable To configure the automatic learning function, run the **dpd msg notify-hash-sequence learning** command.
Interface loopback	Number of the loopback interface. The loopback interface is dynamically created on the remote device and is used to establish an IPSec tunnel with the Efficient VPN server.
Interface loopback IP	IP address of the loopback interface, which is allocated by the Efficient VPN server to the remote device.

Display the IPSec configuration supported by an Efficient VPN policy.

```
<HUAWEI> display ipsec efficient-vpn capability

  IKEv1 Global Supported Algorithms
------------------------------------------------------
  Supported DH Groups:
    DH_GROUP1 | DH_GROUP2 | DH_GROUP5 | DH_GROUP14 | DH_GROUP19 | DH_GROUP20 |
DH_GROUP21
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256
  Supported Authentication Algorithms:
    MD5 | SHA1 | SHA2-256 | SHA2-384 | SHA2-512
  Supported Authentication Methods:
    Pre Shared Key

  IKEv2 Global Supported Algorithms
------------------------------------------------------
  Supported DH Groups:
    DH_GROUP1 | DH_GROUP2 | DH_GROUP5 | DH_GROUP14 | DH_GROUP19 | DH_GROUP20 |
DH_GROUP21
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256
  Supported Integrity Algorithms:
    MD5 | SHA1 | AES-XCBC-96 | SHA2-256 | SHA2-384 | SHA2-512
  Supported PRF:
    PRF-MD5 | PRF-SHA1 | PRF-AES-XCBC-128 | PRF-SHA2-256 | PRF-SHA2-384 |
    PRF-SHA2-512

  IPSEC Global Supported Algorithms
------------------------------------------------------
  Supported Security Protocols:
    ESP
```

```
Supported Encapsulation Modes:
  TUNNEL
Supported Authentication Algorithms:
  MD5 | SHA1 | SHA256 | SHA384 | SHA512
Supported Encryption Algorithms:
  DES | 3DES | AES128 | AES192 | AES256
```

NOTE

- The MD5 and SHA-1 authentication algorithms have security risks; therefore, you are advised to use SHA-2 preferentially.
- The DES and 3DES encryption algorithms have security risks; therefore, you are advised to use AES preferentially.
- The PRF-MD5 and PRF-SHA1 algorithms have security risks; therefore, you are advised to use PRF-AES-XCBC-128 or SHA-2 preferentially.

Table 10-20 Description of the **display ipsec efficient-vpn capability** command output

Item	Description
IKEv1 Global Supported Algorithms	Supported algorithms when IKEv1 is specified in the Efficient VPN policy. The server can use only the supported algorithms to negotiate with the remote device.
Supported DH Groups	Supported DH groups when IKEv1 or IKEv2 is used.
Supported Encryption Algorithms	Supported encryption algorithms when IKEv1 or IKEv2 is used.
Supported Authentication Algorithms	Supported authentication algorithms when IKEv1 is used. To configure an authentication algorithm on the server.
Supported Authentication Methods	Supported authentication algorithms when IKEv1 is used: Pre Shared Key (pre-shared key authentication).
IKEv2 Global Supported Algorithms	Supported algorithms when IKEv2 is specified in the Efficient VPN policy. The server can use only the supported algorithms to negotiate with the remote device.
Supported Integrity Algorithms	Supported integrity algorithms when IKEv2 is used. To configure an integrity algorithm on the server.
Supported PRF	Supported PRF algorithms when IKEv2 is used.
IPSEC Global Supported Algorithms	Algorithms supported by the system.
Supported Security Protocols	Security protocol supported by IPSec: ESP.

Item	Description
Supported Encapsulation Modes	Encapsulation mode supported by IPSec: tunnel mode.
Supported Authentication Algorithms	Authentication algorithm supported by IPSec.
Supported Encryption Algorithms	Encryption algorithm supported by IPSec.

10.3.11 display ipsec global config

Function

The **display ipsec global config** command displays IPSec global configurations.

Format

display ipsec global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view IPSec global configurations, run the **display ipsec global config** command. The global configurations include the global SA lifetime and whether the anti-replay function is enabled.

Example

Display IPSec global configurations.

```
<HUAWEI> display ipsec global config
IPSec Global Config:
-----------------------------------------------------------------
  IPSec sa global-duration time-based(seconds)        : 3600
  IPSec sa global-duration traffic-based(kbytes)      : 1843200
  IPSec anti-replay                                   : enable
-----------------------------------------------------------------
```

Table 10-21 Description of the **display ipsec global config** command output

Item	Description
IPSec Global Config	IPSec global configurations.
IPSec sa global-duration time-based(seconds)	Time-based global SA lifetime, in seconds. To set the time-based global SA lifetime, run the **ipsec sa global-duration time-based** command.
IPSec sa global-duration traffic-based(kbytes)	Traffic-based global SA lifetime, in kilobytes. To set the traffic-based global SA lifetime, run the **ipsec sa global-duration traffic-based** command.
IPSec anti-replay	Whether the anti-replay function is enabled. To configure the anti-replay function, run the **ipsec anti-replay enable** command.

10.3.12 display ipsec interface brief

Function

The **display ipsec interface brief** command displays IPSec policies bound to an interface.

Format

display ipsec interface brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an IPSec policy is bound to an interface, you can run this command to view information about the bound IPSec policy, such as the policy name and interface to which the policy is bound.

Example

Display IPSec policies bound to an interface.

```
<HUAWEI> display ipsec interface brief
------------------------------------------------
```

```
 IPSec policy        : evpn_client
 Using interface     : Vlanif100
 IPSec policy number : -
 IPSec policy Type   : efficient-vpn
------------------------------------------------
```

Table 10-22 Description of the **display ipsec interface brief** command output

Item	Description
IPSec policy	Sequence number of the IPSec policy bound to the interface. Name of the IPSec policy bound to an interface. To apply an IPSec policy to an interface, run the **ipsec efficient-vpn (interface view)** command.
Using interface	Interface to which an IPSec policy is applied.
IPSec policy number	Sequence number of the IPSec policy bound to the interface.
IPSec policy Type	Type of the IPSec policy bound to an interface.

10.3.13 display ipsec history record

Function

The **display ipsec history record** command displays history information about IPSec tunnels.

Format

display ipsec history record [**remote-address** *remote-address*]

Parameters

Parameter	Description	Value
remote-address *remote-address*	Displays history information about the IPSec tunnel with the specified remote IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipsec history record** command to view the reason and time of the last teardown of the IPSec tunnel.

Example

Display history information about IPSec tunnels.

```
<HUAWEI> display ipsec history record
IPSec history record:
Current record number: 1
===============================
Interface              : Vlanif100
remote-address         : 2.1.1.1
remote-port            : 500
VPN instance           : huawei
flow-source            : 10.1.1.1/255.255.255.255
flow-destination       : 10.2.2.2/255.255.255.255
last-offline-reason    : peer request
last-offline-time      : 2017-07-17 20:25:31
offline-times-in-24Hour: 1
```

Table 10-23 Description of the **display ipsec history record** command output

Item	Description
IPSec history record	Display history information about IPSec tunnels.
Current record number	Current record number of the teardown of the IPSec tunnel.
Interface	Interface to which an IPSec policy is applied.
remote-address	Remote IP address of an IPSec tunnel.
remote-port	Remote UDP port number.
VPN instance	Name of a VPN instance.
flow-source	Source address segment of data flows.
flow-destination	Destination address segment of data flows.

Item	Description
last-offline-reason	Reason of the last teardown of an IPSec tunnel. ● dpd timeout: Dead peer detection (DPD) times out. ● peer request: The remote end has sent a message, asking the local end to tear down the tunnel. ● config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted. ● phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received). ● phase2 hard expiry: Hard lifetime expires in phase 2. ● heartbeat timeout: heartbeat detection times out. ● modecfg address soft expiry: The IP address lease applied by the remote end from the server expires. ● re-auth timeout: An SA is deleted due to reauthentication timeout. ● aaa cut user: The AAA module disconnects users. ● hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. ● spi conflict: An SPI conflict occurs. ● phase1 sa replace: The new IKE SA replaces the old IKE SA. ● phase2 sa replace: The new IPSec SA replaces the old IPsec SA. ● receive invalid spi notify: The device receives an invalid SPI notification. ● dns resolution status change: DNS resolution status changes. ● ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPSec SA when deleting an IKEv1 SA. ● exchange timeout: Packet interaction timeout.
last-offline-time	Last time an IPSec tunnel was torn down.
offline-times-in-24Hour	Number of times an IPSec tunnel was torn down within 24 hours.

10.3.14 display ipsec sa efficient-vpn

Function

The **display ipsec sa efficient-vpn** command displays IPSec SA information.

Format

display ipsec sa efficient-vpn *efficient-vpn-name*

Parameters

Parameter	Description	Value
efficient-vpn-name	Displays SA information of an Efficient VPN policy with a specified name.	The value is an existing Efficient VPN policy name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check Efficient VPN SA information, such as the local and remote addresses of IPSec tunnels, source and destination addresses of data flows, and SA lifetime.

Example

Display information about the IPSec SA of Efficient VPN policy.

```
<HUAWEI> display ipsec sa efficient-vpn evpn

ipsec sa information:

===============================
Interface: Vlanif20
===============================


  -----------------------------
  IPSec efficient-vpn name: "evpn"
  Mode                 : EFFICIENTVPN-CLIENT MODE
  -----------------------------
    Connection ID     : 268435456
    Tunnel index      : 4026531842
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 10.10.10.1/500
    Tunnel remote     : 10.2.1.2/500
    Flow source       : 10.10.10.6/255.255.255.255 0/0
    Flow destination  : 0.0.0.0/0.0.0.0 0/0
    Flow dscp         : af11

    [Outbound ESP SAs]
      SPI: 2703436139 (0xa123296b)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-SHA1
      SA remaining key soft duration (kilobytes/sec): 4666163/2960
      SA remaining key hard duration (kilobytes/sec): 5242880/3355
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      SA encrypted packets (number/bytes): 0/0
```

```
[Inbound ESP SAs]
  SPI: 2303751342 (0x895074ae)
  Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-SHA1
  SA remaining key soft duration (kilobytes/sec): 4666163/2960
  SA remaining key hard duration (kilobytes/sec): 5242880/3355
  Max received sequence-number: 0
  UDP encapsulation used for NAT traversal: N
  SA decrypted packets (number/bytes): 0/0
  Anti-replay : Enable
  Anti-replay window size: 1024
```

Table 10-24 Description of the **display ipsec sa efficient-vpn** command output

Item	Description
ipsec sa information	Information about the IPSec SA.
Interface	Interface to which the Efficient VPN policy is applied.
IPSec efficient-vpn name	Name of the Efficient VPN policy. To configure the Efficient VPN policy name, run the **ipsec efficient-vpn** command in the system view.
Mode	Mode in which an Efficient VPN policy is created.
Connection ID	ID of the IPSec SA connection.
Tunnel index	Tunnel index.
Encapsulation mode	Encapsulation mode in an IPSec proposal.
Holding time	Time elapsed since an IPSec tunnel was created.
Tunnel local	IP address and NAT traversal port of the local interface. To configure the IP address of the local interface, run the **tunnel local** command.
Tunnel remote	IP address and NAT traversal port of the remote interface. To configure the IP address of the remote interface, run the **remote-address** command in the Efficient VPN policy view.
Flow source	Source IP address segment of the data flow sent from the local end and the protocol number and port number of the ACL.
Flow destination	Destination IP address segment of the data flow sent from the local end and the protocol number and port number of the ACL.
Flow dscp	DSCP value of the data flow sent from the local end.
Outbound ESP SAs	Outbound IPSec SA information using ESP.
SPI	SPI of an SA.
Proposal	IPSec proposal.

Item	Description
SA remaining key soft duration (kilobytes/sec)	Remaining soft lifetime of an IPSec SA, in kilobytes or seconds.
SA remaining key hard duration (kilobytes/sec)	Remaining hard lifetime of an IPSec SA, in kilobytes or seconds. To set the SA lifetime, run the **ipsec sa global-duration** command.
Max sent sequence-number	Maximum sequence number of sent packets. The sequence number increases during communication and is used for anti-replay.
UDP encapsulation used for NAT traversal	Whether NAT traversal is enabled: ● Y ● N
SA encrypted packets (number/bytes)	Number of packets that are successfully encrypted using the IPSec SA.
Inbound ESP SAs	Inbound IPSec SA information using ESP.
Max received sequence-number	Maximum sequence number of received packets.
SA decrypted packets (number/bytes)	Number of packets that are successfully decrypted using the IPSec SA.
Anti-replay	Whether the anti-replay function is enabled for an IPSec tunnel: ● Enable ● disable To configure the anti-replay function for an IPSec tunnel, run the **ipsec anti-replay enable** command.
Anti-replay window size	IPSec anti-replay window size. This field is valid only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **anti-replay window** or **ipsec anti-replay window** command.

10.3.15 display ipsec packet statistics

Function

The **display ipsec packet statistics** command displays IPSec packet statistics.

Format

display ipsec packet statistics

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipsec packet statistics** command to view IPSec packet statistics, including statistics about incoming or outgoing packets that are protected, statistics about encrypted and decrypted packets, detailed statistics about discarded packets that are protected, and statistics about IKE negotiation related packets. The IPSec packet statistics facilitate IPSec fault diagnosis and maintenance.

Precautions

The **display ipsec packet statistics** command only displays the number of plaintext bytes.

Example

Display statistics about all IPSec packets.

```
<HUAWEI> display ipsec packet statistics
 IPSec statistics information:
 Number of IPSec tunnels: 1
 Number of standby IPSec tunnels: 0
 the security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   the encrypt packet statistics:
     send chip: 0, recv chip: 0, send err: 0
     local cpu: 0, other cpu: 0, recv other cpu: 0
     intact packet: 0, first slice: 0, after slice: 0
   the decrypt packet statistics:
     send chip: 0, recv chip: 0, send err: 0
     local cpu: 0, other cpu: 0, recv other cpu: 0
     reass  first slice: 0, after slice: 0
   dropped security packet detail:
     can not find SA: 0, wrong SA: 0
     authentication: 0, replay: 0
     front recheck: 0, after recheck: 0
     change cpu enc: 0, dec change cpu: 0
     fib search: 0, output l3: 0
     flow err: 0, slice err: 0, byte limit: 0
  negotiate about packet statistics:
```

```
IKE fwd packet ok: 0, err: 0
IKE ctrl packet inbound ok: 0, outbound ok: 0
SoftExpr: 0, HardExpr: 0, DPDOper: 0
trigger ok: 0, switch sa: 0, sync sa: 0
recv IKE nat keepalive: 0, IKE input: 0
```

Table 10-25 Description of the **display ipsec packet statistics** command output

Item	Description
IPSec statistics information	Statistics about IPSec packets.
Number of IPSec tunnels	Number of the IPSec tunnels.
Number of standby IPSec tunnels	Number of the standby IPSec tunnels.
the security packet statistics	Statistics about packets that are protected.
input/output security packets	Number of incoming or outgoing packets that are protected.
input/output security bytes	Number of incoming or outgoing bytes that are protected.
input/output dropped security packets	Number of discarded incoming or outgoing packets that are protected.
the encrypt packet statistics	Statistics about encrypted packets.
send chip	Number of packets sent to the hardware for encryption and decryption.
recv chip	Number of packets encrypted and decrypted by hardware.
send err	Number of packets that fail to be sent to hardware for encryption and decryption.
local cpu	Number of packets encrypted and decrypted by the local CPU.
other cpu	Number of packets forwarded to another CPU for encryption and decryption.
recv other cpu	Number of packets received from another CPU for encryption and decryption.
intact packet	Number of non-fragmented encrypted packets.
first slice	Number of initial fragmented packets.
after slice	Number of non-initial fragmented packets.

Item	Description
the decrypt packet statistics	Statistics about decrypted packets.
reass first slice	Number of initial packets that are reassembled.
after slice	Number of non-initial packets that are reassembled.
dropped security packet detail	Detailed statistics about discarded packets that are protected.
can not find SA	Number of packets for which SAs are not found.
wrong SA	Number of packets with invalid SAs.
authentication	Number of packets that fail to be authenticated.
replay	Number of discarded packets due to replay check.
front recheck	Number of discarded packets due to IPSec pre-check.
after recheck	Number of discarded packets due to IPSec post-check.
change cpu enc	Number of encrypted packets that fail to be forwarded.
dec change cpu	Number of decrypted packets that fail to be forwarded.
fib search	Number of encrypted packets that are discarded due to route searching failure.
output l3	Number of encrypted packets that fail to be sent.
flow err	Number of packets discarded because negotiation is triggered.
slice err	Number of IPSec packets that fail to be fragmented.
byte limit	Number of discarded packets due to traffic limit.
negotiate about packet statistics	Statistics about IKE negotiation packets.
IKE fwd packet ok	Number of IKE packets sent to the IKE process.

Item	Description
err	Number of IKE packets that fail to be sent to the IKE process.
IKE ctrl packet inbound ok	Number of IKE packets received by the control plane.
outbound ok	Number of IKE packets sent by the control plane.
SoftExpr	Number of traffic soft timeouts.
HardExpr	Number of traffic hard timeouts.
DPDOper	Number of times DPD is performed in on-demand DPD mode.
trigger ok	Number of times that negotiation is triggered.
switch sa	Number of times the local device receives data encrypted with the new SA and instructs the IKE process to replace the SA.
sync sa	Number of times the active device notifies the IKE process that the SA 3-tuple (remote address, SPI, protocol ID) does not exist on the standby device.
recv IKE nat keepalive	Number of received IKE nat keepalive packets.
IKE input	Number of received IKE packets.

10.3.16 display ipsec statistics tunnel-number

Function

The **display ipsec statistics tunnel-number** command displays the number of IPSec tunnels.

Format

display ipsec statistics tunnel-number

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the number of IPSec tunnels.

Example

Display the number of IPSec tunnels.

```
<HUAWEI> display ipsec statistics tunnel-number
  IPSec tunnel totals: 0
  IPSec tunnel specifications: 4000
```

Table 10-26 Description of the **display ipsec statistics tunnel-number** command output

Item	Description
IPSec tunnel totals	Number of IPSec tunnels.
IPSec tunnel specifications	IPSec tunnel specifications.

10.3.17 dpd msg

Function

The **dpd msg** command configures the payload sequence of DPD packets on the specified IKE peer.

The **undo dpd msg** command restores the default payload sequence of DPD packets on the specified IKE peer.

By default, the payload sequence of DPD packets on an IKE peer is **seq-notify-hash**.

Format

dpd msg { **seq-hash-notify** | **seq-notify-hash** }

undo dpd msg

Parameters

Parameter	Description	Value
seq-hash-notify	Indicates that in a DPD packet, the hash payload is before the notify payload.	-
seq-notify-hash	Indicates that in a DPD packet, the notify payload is before the hash payload.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

DPD packets carrying the notify payload and hash payload are exchanged bidirectionally. The notify payload sent by the initiator carries an R-U-THERE message equivalent to a Hello packet, and the notify payload sent by the responder carries an R-U-THERE-ACK message equivalent to an ACK packet.

The payload sequence of DPD packets sent by different devices may be different. IKE peers on both ends must send DPD packets with the same payload sequence; otherwise, DPD does not take effect. In this case, run the **dpd msg** command to set the same payload sequence of DPD packets on both ends.

Precautions

This command applies only when an IKE peer uses IKEv1.

Example

Set the payload sequence of DPD packets to **hash-notify**.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dpd msg seq-hash-notify
```

10.3.18 dpd msg notify-hash-sequence learning

Function

The **dpd msg notify-hash-sequence learning** command enables automatic learning of the payload sequence of DPD packets.

The **undo dpd msg notify-hash-sequence learning** command disables automatic learning of the payload sequence of DPD packets.

By default, automatic learning of the payload sequence of DPD packets is enabled.

Format

dpd msg notify-hash-sequence learning

undo dpd msg notify-hash-sequence learning

Parameters

None

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

When DPD is used to detect the IKEv1 peer status, the payload sequence of DPD packets on both ends must be consistent. Otherwise, DPD does not take effect, and even the IPSec tunnel between both ends flaps.

If the local end does not know the payload sequence of DPD packets sent from the remote end, run the **dpd msg notify-hash-sequence learning** command on the local end to enable automatic learning of the payload sequence of DPD packets. When the local end receives a DPD packet from the remote end, the local end learns the payload sequence of the DPD packet and sends a DPD packet in the same payload sequence.

Example

Enable automatic learning of the payload sequence of DPD packets.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dpd msg notify-hash-sequence learning
```

10.3.19 ike dscp

Function

The **ike dscp** command sets a global DSCP priority of IKE packets.

The **undo ike dscp** command cancels the DSCP priority configuration.

By default, the global DSCP priority of IKE packets is 0.

Format

ike dscp *dscp-value*

undo ike dscp

Parameters

Parameter	Description	Value
dscp-value	Specifies the global DSCP priority of IKE packets.	The value can be an integer or a string of characters. That is, the value can be an integer that ranges from 0 to 63, or a string of AF11 to AF13, AF21 to AF23, AF31 to AF33, AF41 to AF43, CS1 to CS7, EF, or default.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IKE packets are used for IKE SA and IPSec SA negotiation or DPD. When IKE packets are lost during transmission, IPSec SAs may fail to be negotiated. As a result, packets that need to be protected by IPSec are not protected. The DSCP priority of IKE packets can be improved so that IKE packets are processed preferentially. IKE packet transmission reliability is therefore improved.

To configure the DSCP priority for IKE packets of all IKE peers, run this command.

Example

Set a global DSCP priority of IKE packets to CS2.

```
<HUAWEI> system-view
[HUAWEI] ike dscp cs2
```

10.3.20 ike heartbeat

Function

The **ike heartbeat** command sets heartbeat parameters.

The **undo ike heartbeat** command restores the default configuration.

By default, a heartbeat packet uses old type sequence number mechanism and does not carry the SPI list.

Format

ike heartbeat { **seq-num** { **new** | **old** } | **spi-list** }

undo ike heartbeat { **seq-num** | **spi-list** }

Parameters

Parameter	Description	Value
seq-num { **new** | **old** }	Configures the sequence number mechanism for heartbeat packets. ● **new**: The sequence number mechanism conforms to draft-ietf-ipsec-heartbeats-00.txt. ● **old**: The sequence number mechanism conforms to the standard that before draft-ietf-ipsec-heartbeats-00.txt emerges.	-
spi-list	Configures heartbeat packets to carry the SPI list.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IPSec communication, if the local end becomes faulty and the remote end does not detect the fault because of system failures, the remote end still sends IPSec packets to the local end, causing traffic loss. Heartbeat detection solves this problem. After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status.

Precautions

The two ends must use the same heartbeat parameters.

If you run the **ike heartbeat** { **seq-num** { **new** | **old** } | **spi-list** } command multiple times, only the latest configuration takes effect.

Example

Configure the sequence number mechanism for heartbeat packets to **new**.

```
<HUAWEI> system-view
[HUAWEI] ike heartbeat seq-num new
```

10.3.21 ike heartbeat-timer interval

Function

The **ike heartbeat-timer interval** command sets the interval for sending heartbeat packets through an IKE SA.

The **undo ike heartbeat-timer interval** command cancels the configuration.

By default, an IKE SA does not send heartbeat packets.

Format

ike heartbeat-timer interval *interval*

undo ike heartbeat-timer interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending heartbeat packets through an IKE SA.	The value is an integer that ranges from 20 to 28800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status. This command sets the interval for sending heartbeat packets through an IKE SA.

The interval at which heartbeat packets are sent (configured using the **ike heartbeat-timer timeout** command) at the local end must be used with the timeout interval of heartbeat packets (configured using the **ike heartbeat-timer timeout** command) at the remote end. If the remote end does not receive any heartbeat packet within the timeout interval, it deletes the IKE SA with a timeout tag along with its corresponding IPSec SA. If the IKE SA does not have a timeout tag, it is marked as timeout.

Precautions

When the **ike heartbeat-timer interval** command is configured at one end, the **ike heartbeat-timer timeout** command must be used at the other end.

The timeout interval of heartbeat packets must be longer than the interval at which heartbeat packets are sent. On a network, packet loss seldom occurs more than three consecutive times. Therefore, it is recommended that the timeout interval of heartbeat packets be three times the interval at which heartbeat packets are sent.

Example

Set the interval for sending heartbeat packets to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] ike heartbeat-timer interval 20
```

10.3.22 ike heartbeat-timer timeout

Function

The **ike heartbeat-timer timeout** command sets the timeout interval during which an IKE SA waits for a heartbeat packet.

The **undo ike heartbeat-timer timeout** command cancels the configuration.

By default, the timeout interval during which an IKE SA waits for a heartbeat packet is not configured.

Format

ike heartbeat-timer timeout *seconds*

undo ike heartbeat-timer timeout

Parameters

Parameter	Description	Value
seconds	Specifies the timeout interval during which an IKE SA waits for a heartbeat packet.	The value is an integer that ranges from 30 to 28800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status. This command sets the timeout interval during which an IKE SA waits for a heartbeat packet.

Precautions

When the **ike heartbeat-timer interval** command is configured at one end, the **ike heartbeat-timer timeout** command must be used at the other end.

The timeout interval of heartbeat packets must be longer than the interval at which heartbeat packets are sent. On a network, packet loss seldom occurs more than three consecutive times. Therefore, it is recommended that the timeout interval of heartbeat packets be three times the interval at which heartbeat packets are sent.

Example

Set the timeout interval during which an IKE SA waits for a heartbeat packet to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] ike heartbeat-timer timeout 60
```

10.3.23 ike local-name

Function

The **ike local-name** command configures the local name for IKE negotiation.

The **undo ike local-name** command deletes the local name for IKE negotiation.

By default, no local name is configured for IKE negotiation.

Format

ike local-name *local-name*

undo ike local-name

Parameters

Parameter	Description	Value
local-name	Specifies a local name for IKE negotiation.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When identity authentication, If the ID type of an IKE peer is fully qualified domain name (FQDN), or USER-FQDN, the IKE peer uses the name for identity authentication. In this case, you need to run the **ike local-name** command to configure the local name.

Example

Set the local ID for IKE negotiation to **Huawei**.

```
<HUAWEI> system-view
[HUAWEI] ike local-name Huawei
```

10.3.24 ike nat-keepalive-timer interval

Function

The **ike nat-keepalive-timer interval** command configures the interval for sending NAT Keepalive packets.

The **undo ike nat-keepalive-timer interval** command restores the default setting.

By default, the interval for sending NAT Keepalive packets is 20 seconds.

Format

ike nat-keepalive-timer interval *interval*

undo ike nat-keepalive-timer interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NAT Keepalive packets.	The value is an integer that ranges from 5 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an NAT gateway exists between two IKE peers, to prevent NAT entries from being aged, the device on the private network side of the NAT gateway sends NAT Keepalive packets to its peer at a certain interval to maintain the NAT session.

Example

Configure the interval for sending NAT Keepalive packets to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] ike nat-keepalive-timer interval 30
```

10.3.25 ikev1 phase1-phase2 sa dependent

Function

The **ikev1 phase1-phase2 sa dependent** command enables dependency between IPSec SA and IKE SA during IKEv1 negotiation.

The **undo ikev1 phase1-phase2 sa dependent** command cancels dependency between IPSec SA and IKE SA during IKEv1 negotiation.

By default, no dependency exists between IPSec SA and IKE SA during IKEv1 negotiation.

Format

ikev1 phase1-phase2 sa dependent

undo ikev1 phase1-phase2 sa dependent

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During IKEv1 negotiation, an IKE SA is established during phase 1, and an IPSec SA is established during phase 2. By default, no dependency exists between IPSec SA and IKE SA, that is, the two SAs can be deleted separately. If the IKE SA is deleted but the corresponding IPSec SA still exists, traffic forwarding will be effected. To prevent this problem, you can run this command to enable dependency between IPSec SA and IKE SA.

Prerequisites

Before running this command, you need to install the weak encryption algorithm plug-in and run the **version 1** command in the IKE peer view to enable IKEv1. Otherwise, the command configuration does not take effect. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Example

Enable dependency between IPSec SA and IKE SA during IKEv1 negotiation.

```
<HUAWEI> system-view
[HUAWEI] ikev1 phase1-phase2 sa dependent
```

10.3.26 ikev2 delete old child-sa enable

Function

The **ikev2 delete old child-sa enable** command enables the function of instructing the peer device to delete the old child SA.

The **undo ikev2 delete old child-sa enable** command disables the function of instructing the peer device to delete the old child SA.

By default, the function of instructing the peer device to delete the old child SA is enabled.

Format

ikev2 delete old child-sa enable

undo ikev2 delete old child-sa enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In an IKEv2 scenario, when the local device deletes the child SA and initiates IKEv2 negotiation to the peer device again, the default negotiation message carries the IKEV2_NOTIFY_DELETE_OLD_CHILDSA payload, instructing the peer device to delete the old child SA. If the peer device does not support the processing of this payload, IKEv2 negotiation between the two ends fails. To prevent this problem, run the **undo ikev2 delete old child-sa enable** command on the local device to disable it from instructing the peer device to delete the old child SA so that the IKEv2 negotiation message does not carry this payload.

Example

Enable the function of instructing the peer device to delete the old child SA.

```
<HUAWEI> system-view
[HUAWEI] ikev2 delete old child-sa enable
```

10.3.27 ikev2 initial-contact enable

Function

The **ikev2 initial-contact enable** command enables the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

The **undo ikev2 initial-contact enable** command disables the device from sending the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

By default, the device is disabled to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

Format

ikev2 initial-contact enable

undo ikev2 initial-contact enable

Parameters

None

Views

System View

Default Level

2: Configuration level

Usage Guidelines

The INITIAL_CONTACT notify payload asserts that an IKE SA is the only active IKE SA between a pair of IKE peers. By default, the device will delete the old IKE SA without the INITIAL_CONTACT notify payload after the new IKE SA is created. When the remote end requires the INITIAL_CONTACT notify payload to delete the old IKE SA, configure this command.

When the local device restarts or expects to use the current IKE SA for establishing an IPSec tunnel only, run this command to enable the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request so that the remote device deletes the old IKE SA.

Example

Enable the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

```
<HUAWEI> system-view
[HUAWEI] ikev2 initial-contact enable
```

10.3.28 ipsec anti-replay enable

Function

The **ipsec anti-replay enable** command enables the anti-replay function globally.

The **undo ipsec anti-replay enable** command disables the anti-replay function globally.

By default, the anti-replay function is enabled globally.

Format

ipsec anti-replay enable

undo ipsec anti-replay enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Replayed packets refer to the packets that have been processed by the device. IPSec uses the sliding window (anti-replay window) to detect replayed packets. AH and ESP packet headers carry 32-bit sequence numbers. The sequence numbers carried in the AH or ESP packet headers of the same SA are in ascending order. If the sequence number of an authenticated packet is the same as that of a decapsulated packet or the sequence number is outside the sliding window, the packet is considered a replayed packet.

Decapsulating replayed packets consumes many resources and makes system performance deteriorate. Therefore, attackers may use replayed packets to initiate a DoS attack. After the anti-replay function is enabled, the system discards replayed packets to save system resources.

Precautions

In some situations, for example, network congestion occurs or QoS is performed for packets, the sequence numbers of some service data packets may be different from those in common data packets. The device that has IPSec anti-replay enabled considers the packets replayed and discards them. You can disable global IPSec anti-replay to prevent packets from being discarded incorrectly or adjust the IPSec anti-replay window size to meet service requirements.

Example

Enable the anti-replay function globally.

```
<HUAWEI> system-view
[HUAWEI] ipsec anti-replay enable
```

10.3.29 ipsec anti-replay window

Function

The **ipsec anti-replay window** command sets the global IPSec anti-replay window size.

The **undo ipsec anti-replay window** command restores the default global IPSec anti-replay window size.

By default, the global IPSec anti-replay window size is 1024 bits.

Format

ipsec anti-replay window *window-size*

undo ipsec anti-replay window

Parameters

Parameter	Description	Value
window-size	Specifies the global IPSec anti-replay window size.	The value can be 32, 64, 128, 256, 512, or 1024, in bits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some situations, for example, network congestion occurs or QoS is performed for packets, the sequence numbers of some service data packets may be unusual. The device that has IPSec anti-replay enabled considers the packets replayed and discards them. To prevent packets from being discarded incorrectly, you can disable global IPSec anti-replay or adjust the IPSec anti-replay window size to meet service requirements.

Prerequisites

The anti-replay function has been enabled. By default, the anti-replay function is enabled (through **ipsec anti-reply enable** command).

Precautions

When both **anti-replay window** and **ipsec anti-replay window** are used, the **anti-replay window** command takes effect. When **anti-replay window** is not configured, the **ipsec anti-replay window** command takes effect.

Example

Set the global IPSec anti-replay window size to 128 bits.

```
<HUAWEI> system-view
[HUAWEI] ipsec anti-replay window 128
```

10.3.30 ipsec efficient-vpn (interface view)

Function

The **ipsec efficient-vpn** command binds an Efficient VPN policy to an interface.

The **undo ipsec efficient-vpn** command deletes the Efficient VPN policy from an interface.

By default, no Efficient VPN policy is applied to an interface.

Format

ipsec efficient-vpn *efficient-vpn-name*

undo ipsec efficient-vpn

Parameters

Parameter	Description	Value
efficient-vpn-name	Specifies the name of an Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many branches and traveling staff connect to the headquarters over IPSec tunnels, similar or duplicate IPSec configurations and other network resource configurations must be configured on the branch and headquarters gateways. The Efficient VPN solution uses centralized IPSec configurations on the headquarters gateway and simplified IPSec configuration on each branch gateway. This solution reduces the manual configuration workload, and facilitates IPSec VPN configuration and maintenance.

Prerequisites

An Efficient VPN policy has been created using the **ipsec efficient-vpn (system view)** command.

Precautions

If an Efficient VPN policy is used to establish an IPSec tunnel between the enterprise branch and headquarters, apply the Efficient VPN policy to the branch gateway and use an IPSec policy template on the headquarters gateway to create an IPSec policy.

Example

Apply the Efficient VPN policy named **evpn** to **VLANIF10**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipsec efficient-vpn evpn
```

10.3.31 ipsec efficient-vpn (system view)

Function

The **ipsec efficient-vpn** command creates an IPSec Efficient VPN policy and displays the IPSec Efficient VPN policy view.

The **undo ipsec efficient-vpn** command deletes an IPSec Efficient VPN policy.

By default, no IPSec Efficient VPN policy is created in the system.

Format

ipsec efficient-vpn *efficient-vpn-name* [**mode** { **client** | **network** | **network-plus** }]

undo ipsec efficient-vpn *efficient-vpn-name*

Parameters

Parameter	Description	Value
efficient-vpn-name	Specifies the name of an Efficient VPN policy.	The value is a string of 1 to 12 case-sensitive characters without question marks (?) or spaces.
mode	Specifies the mode of the Efficient VPN policy.	-
client	Indicates the client mode.	-
network	Indicates the network mode.	-
network-plus	Indicates the network-plus mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many branches and traveling staff connect to the headquarters over IPSec tunnels, similar or duplicate IPSec configurations and other network resource configurations must be configured on the branch and headquarters gateways. The Efficient VPN solution uses centralized IPSec configurations on the headquarters gateway and simplified IPSec configuration on each branch gateway. This solution reduces the manual configuration workload, and facilitates IPSec VPN configuration and maintenance.

The Efficient VPN policy has the following modes:

- Client mode

  When a remote device requests an IP address from the Efficient VPN server, a loopback interface is dynamically created on the remote device and the IP address obtained from the server is assigned to the loopback interface. The remote device uses this IP address to establish an IPSec tunnel with the headquarters.

  The client mode applies to scenarios where small-scale branches connect to the headquarters network through private networks. In client mode, devices connected to the Efficient VPN server or remote devices can use the same IP address. However, the number of devices allowed depends on the number of IP addresses assigned by the Efficient VPN server.
- Network mode

  In network mode, a remote device does not apply to the Efficient VPN server for an IP address. Instead, the remote device uses the original IP address to establish an IPSec tunnel with the headquarters.

  The network mode applies to scenarios where IP addresses of the headquarters and branches are planned uniformly. Ensure that IP addresses do not conflict.
- Network-plus mode

  Compared with the network mode, the remote device applies to the Efficient VPN server for an IP address in network-plus mode. IP addresses of branches and headquarters are configured beforehand. A remote device applies to the Efficient VPN server for an IP address. The Efficient VPN server uses the IP address to perform ping, Telnet, or other management and maintenance operations on the remote device.

Follow-up Procedure

Configure negotiation parameters of Efficient VPN in the Efficient VPN policy view, and use the **ipsec efficient-vpn (interface view)** command to bind the Efficient VPN policy to an interface.

Example

Create the Efficient VPN policy named **vpn1** in client mode.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn vpn1 mode client
[HUAWEI-ipsec-efficient-vpn-vpn1]
```

10.3.32 ipsec sa global-duration

Function

The **ipsec sa global-duration** command sets the global hard lifetime of IPSec SAs.

The **undo ipsec sa global-duration** command restores the default global hard lifetime of IPSec SAs.

By default, the global time-based SA hard lifetime is 3600 seconds and the global traffic-based SA hard lifetime is 1843200 Kbytes.

Format

ipsec sa global-duration { **time-based** *interval* | **traffic-based** *size* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Parameters

Parameter	Description	Value
time-based *interval*	Specifies the time-based global IPSec SA hard lifetime. When a large number of IPSec tunnels are established between two devices, you are advised to set the global IPSec SA hard lifetime to a value larger than or equivalent to 1800s.	It is an integer that ranges from 30 to 604800, in seconds.
traffic-based *size*	Specifies the traffic-based global IPSec SA hard lifetime. It is recommended that the traffic volume be equal to or larger than the size of IPSec traffic forwarded in 1 hour.	The value is 0 or an integer from 256 to 200000000, in Kbytes. ● IKEv1 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function. ● IKEv2 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, the local device disables the traffic timeout function.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a dynamic SA, configure the SA hard lifetime so that the SA can be updated in real time, reducing the crash risk and improving security.

There are two methods to measure the lifetime:

- Time-based lifetime

  The period from when an SA is set up to when the SA is expired.
- Traffic-based lifetime

  The maximum volume of traffic that this SA can process.

The lifetime is classified as follows:

- Hard lifetime: specifies the lifetime of an IPSec SA.

  When two devices negotiate an IPSec SA, the actual hard lifetime is the smaller of the two values configured on the two devices.
- Soft lifetime: specifies the time after which a new IPSec SA is negotiated so that the new IPSec SA will be ready before the hard lifetime of the original IPSec SA expires.

  Table 10-27 lists the default soft lifetime values.

Table 10-27 Soft lifetime values

Soft Lifetime Type	Description
Time-based soft lifetime (soft timeout period)	The value is 70% of the actual hard lifetime (hard timeout period).
Traffic-based soft lifetime (soft timeout traffic)	• For IKEv1, the value is 70% of the actual hard lifetime (hard timeout traffic). • For IKEv2, the value is 65% to 75% of the actual hard lifetime (hard timeout traffic) plus or minus a random value.

Before an IPSec SA becomes invalid, IKE negotiates a new IPSec SA for the remote end. The remote end uses the new IPSec SA to protect IPSec communication immediately after the new IPSec SA is negotiated. If service traffic is transmitted, the original IPSec SA is deleted immediately. If no service traffic is transmitted, the original IPSec SA will be deleted after 10s or the hard lifetime expires.

If the time-based lifetime and traffic-based lifetime are both set for an IPSec SA, the IPSec SA becomes invalid when either lifetime expires.

Precautions

During IKEv1 negotiation:

- The responder cannot initiate IPSec SA renegotiation after the IPSec SA soft lifetime expires.
- The initiator cannot initiate IPSec SA renegotiation when its IKE SA is deleted and the IPSec SA soft lifetime expires.

During IKEv2 negotiation, the initiator or responder cannot initiate IPSec SA renegotiation if the IKE SA is deleted and the IPSec SA soft lifetime expires.

Example

Set the time-based global SA hard lifetime to 7200s.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa global-duration time-based 7200
```

Set the traffic-based global SA hard lifetime to 10 MB.

```
<HUAWEI> system-view
[HUAWEI] ipsec sa global-duration traffic-based 10240
```

10.3.33 local-id-type

Function

The **local-id-type** command sets the type of the local ID used in IKE negotiation.

The **undo local-id-type** command restores the default type of the local ID used in IKE negotiation.

By default, the local ID type used by IKE negotiation is IP.

Format

local-id-type { **fqdn** | **ip** | **key-id** | **user-fqdn** }

undo local-id-type

Parameters

Parameter	Description	Value
fqdn	Specifies the name as the local ID.	-
ip	Specifies the IP address as the local ID.	-
key-id	Specifies the key-id as the local ID.	-
user-fqdn	Specifies the USER-FQDN as the local ID.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism for IKE negotiation. The device ensures security by confirming identities of communication parties. IKE peers can use different types. This command configures the type of the local ID of an IKE peer.

Precautions

- The local ID type can be different from the remote ID type. You can use commands to specify the local and remote ID types.
- For pre-shared key authentication, the local ID type on the local end must be the same as the remote ID type on the remote end, and the local ID on the local end must be the same as the remote ID on the remote end.

Different authentication methods support different ID types, as shown in **Table 10-28**.

Table 10-28 Relationship between local IKE ID types, local ID, and authentication methods

Authentication Method	IP	FQDN	USER-FQDN	key-id
pre-share	Supported The IP address is the local IP address used for IKE negotiation by default.	Supported The ID specified by the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication.	Supported The ID specified by the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication.	Supported This parameter is often used when the device using the Efficient VPN policy functions as a remote end to communicate with Cisco devices.

Example

Set the local ID type of Efficient VPN to FQDN.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] local-id-type fqdn
```

10.3.34 pfs

Function

The **pfs** command enables PFS when the local end initiates IPSec tunnel negotiation.

The **undo pfs** command disables PFS when the local end initiates IPSec tunnel negotiation.

By default, PFS is not used when the local end initiates IPSec tunnel negotiation.

Format

pfs { **dh-group14** | **dh-group19** | **dh-group20** | **dh-group21** }

undo pfs

Parameters

Parameter	Description	Value
dh-group14	Uses the 2048-bit DH group.	-
dh-group19	Uses the 256-bit Elliptic Curve Groups modulo a Prime (ECP) DH group.	-
dh-group20	Uses the 384-bit ECP DH group.	-
dh-group21	Uses the 521-bit ECP DH group.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the local end initiates negotiation, there is an additional DH exchange in IKEv1 phase 2 or IKEv2 CREATE_CHILD_SA exchange. The additional DH exchange ensures security of the IPSec SA key and improves communication security.

Precautions

The system software does not support the **dh-group1**, **dh-group2**, and **dh-group5** parameters. To use these DH groups, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify other DH groups.

For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Example

Enable the PFS feature in the IPSec Efficient VPN policy **evpn**.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] pfs dh-group14
```

10.3.35 pre-shared-key (Efficient VPN policy view)

Function

The **pre-shared-key** command configures the pre-shared key used by IKE peers to perform pre-shared key authentication.

The **undo pre-shared-key** command deletes the pre-shared key used by IKE peers to perform pre-shared key authentication.

By default, the pre-shared key used by IKE peers to perform pre-shared key authentication is not configured.

Format

pre-shared-key cipher *key*

undo pre-shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the pre-shared key in cipher text. You can enter a pre-shared key in plain text or cipher text, but the pre-shared key is displayed in cipher text in the configuration file.	-
key	Specifies the pre-shared key used by IKE peers to perform pre-shared key authentication.	The value is a string of case-sensitive characters without spaces. A plaintext key contains 1 to 128 characters, and a ciphertext key contains 48 to 188 characters. If the character string is enclosed in double quotation marks (" "), the character string can contain spaces. **NOTE** For security purposes, it is recommended that the pre-shared key contain at least three types of lowercase letters, uppercase letters, digits, and special characters and contain at least 8 characters.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During IKE negotiation, IPSec can use pre-shared key authentication to verify identities of communication parties. After pre-shared key authentication is configured, the initiator encrypts data using the pre-shared key before transmitting the data, and the receiver decrypts the data using the same pre-shared key. If the receiver succeeds in data decryption, the initiator passes the identity verification.

Precautions

Both ends of IKE negotiation must be configured with the same pre-shared key.

Example

Configure pre-shared key authentication in the Efficient VPN policy **evpn** and set the pre-shared key to YsHsjx_202206 in cipher text.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] pre-shared-key cipher YsHsjx_202206
```

10.3.36 re-authentication interval

Function

The **re-authentication interval** command sets the IKEv2 re-authentication interval.

The **undo re-authentication interval** command cancels the configuration.

By default, the device does not perform IKEv2 re-authentication.

Format

re-authentication interval *interval*

undo re-authentication interval

Parameters

Parameter	Description	Value
interval	Specifies the IKEv2 re-authentication interval. When about 70% of the time interval has elapsed, the device initiates IKEv2 re-authentication.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the remote access scenario, third-party attacks may occur during communications of peers. To improve IPSec network security, you can run this command to enable the peers to periodically re-authenticate each other.

Precautions

Only IKEv2 supports re-authentication.

Example

Set the re-authentication interval to 400 seconds in the IPSec Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] re-authentication interval 400
```

10.3.37 remote-address (Efficient VPN policy view)

Function

The **remote-address** command configures an IP address or domain name for the remote IKE peer during IKE negotiation.

The **undo remote-address** command deletes an IP address or domain name for the remote IKE peer during IKE negotiation.

By default, no IP address or domain name is configured for the remote IKE peer during IKE negotiation.

Format

remote-address { *ip-address* | **host-name** *host-name* } { **v1** | **v2** }

undo remote-address [*ip-address* | **host-name** *host-name*]

NOTE

The **v1** parameter is supported only when the WEAKEA plug-in is installed. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the remote IKE peer.	The value is in dotted decimal notation.
host-name *host-name*	Specifies the domain name of the remote IKE peer.	The value is an existing remote IKE peer domain name.
v1	Indicates that both ends use IKEv1.	-
v2	Indicates that both ends use IKEv2.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remote-address** command configures an IP address or domain name for the remote IKE peer in an Efficient VPN policy. If the domain name is configured for the remote IKE peer, the IP address of the remote IKE peer is obtained in either of the following modes:

- Static mode: The IP address of the remote IKE peer is obtained based on the mapping between the domain name and IP address.
- Dynamic mode: The IP address of the remote IKE peer is obtained from the DNS server.

To improve network reliability, two devices can be deployed at the headquarters to connect to the branch gateway. In an Efficient VPN solution, two IP addresses or domain names of the remote IKE peer can be configured on the branch gateway. The branch gateway first attempts to use the first configured IP address or domain name to establish an IKE connection with the headquarters gateway. If establishing an IKE connection fails, the branch gateway uses the second IP address or domain name to establish an IKE connection.

Precautions

When you configure IP addresses or domain names for two remote IKE peers, ensure that the value type of **remote-address** and the IKE version are respectively the same. Generally, only one device is deployed at the headquarters to connect to the branch gateway. Therefore, only one remote address is configured.

Example

Assign the IP addresses 10.1.1.1 and 10.1.2.1 to the remote peer in the Efficient VPN policy view.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] remote-address 10.1.1.1 v2
[HUAWEI-ipsec-efficient-vpn-evpn] remote-address 10.1.2.1 v2
```

Set the domain name of the remote peer to **mypeer** in the Efficient VPN policy view.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] remote-address host-name mypeer v2
```

10.3.38 remote-id

Function

The **remote-id** command specifies the remote ID for IKE negotiation.

The **undo remote-id** command deletes the remote ID for IKE negotiation.

By default, the remote ID for IKE negotiation is not configured.

Format

remote-id *id*

undo remote-id

Parameters

Parameter	Description	Value
id	Specifies the remote ID.	The value is a string of 1 to 255 case-sensitive characters including special characters, such as the exclamation point (!), at sign (@), number sign (#), dollar sign ($), and percent (%).

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the remote ID type of the IKE peer is FQDN or USER-FQDN, you can run this command to set a value for the remote ID.

If the remote ID type of the IKE peer is DN, FQDN, or USER-FQDN, you can run this command to set a value for the remote ID.

During IKE negotiation, you can run the **remote-id** commands to configure the remote ID for authentication.

Precautions

- In IKEv1, the configured remote ID is used to authenticate only the peer.
- In IKEv2, the configured remote ID can be sent to the peer to check whether the local name of the peer is the same as this remote ID.

Example

Set the remote peer name to **Huawei** in the Efficient VPN policy view.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn name mode client
[HUAWEI-ipsec-efficient-vpn-name] remote-id Huawei
```

10.3.39 reset ike error-info

Function

The **reset ike error-info** command clears information about IPSec tunnel negotiation failures using IKE.

Format

reset ike error-info

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

You can run the **display ike error-info** command to view information about IPSec tunnel negotiation failures using IKE.

Example

Clear information about IPSec tunnel negotiation failures using IKE.

```
<HUAWEI> reset ike error-info
```

10.3.40 reset ike offline-info

Function

The **reset ike offline-info** command clears information about deleted IPSec tunnels established through IKE negotiation.

Format

reset ike offline-info

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

You can run the **display ike offline-info** command to check the reasons why IPSec tunnels established through IKE negotiation have been deleted.

Example

Clear information about deleted IPSec tunnels established using IKE negotiation.

```
<HUAWEI> reset ike offline-info
```

10.3.41 reset ike sa

Function

The **reset ike sa** command clears information about SAs established through IKE negotiation.

Format

reset ike sa [**conn-id** *conn-id* | **remote** *ipv4-address*]

Parameters

Parameter	Description	Value
conn-id *conn-id*	Specifies the connection ID of an SA.	The value is an integer that ranges from 1 to 4294967295.
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear an IPSec tunnel established through IKE negotiation, run the **reset ike sa** command to clear the IKE SA that is used to negotiate the IPSec tunnel.

There are two types of SAs established by IKE negotiation: IKE SAs in phase 1 and IPSec SAs in phase 2. IKE SAs in phase 1 are used for IKE negotiation. Under the protection of these IKE SAs, IPSec SAs in phase 2 are used to protect data flows.

- If the specified *conn-id* parameter corresponds to an IKE SA in phase 1, IKE peers do not automatically negotiate an IKE SA after the IKE SA is cleared. The IKE peers re-negotiate an IKE SA in phase 1 only when data flows match ACL rules in the IPSec policy again.
- If the specified *conn-id* parameter corresponds to an IPSec SA in phase 2, either of the following will occur:

  - Automatic triggering mode: The IKE peers re-negotiate an IPSec SA in phase 2 under the protection of the IKE SA in phase 1 after the IPSec SA is cleared.
  - Traffic-based triggering mode: The IKE peers do not automatically negotiate an IPSec SA after the IPSec SA is cleared. They re-negotiate an IPSec SA in phase 2 under the protection of the IKE SA in phase 1 only when data flows match ACL rules in the IPSec policy again.
- If the *conn-id* parameter is not specified, all IKE SAs in phase 1 are cleared, and IKE negotiation process is similar to that described above.

Precautions

After dependency between IPSec SA and IKE SA during IKEv1 negotiation is disabled using the **undo ikev1 phase1-phase2 sa dependent** command, running the **reset ike sa** *conn-id* command to delete an IKE SA will also delete the corresponding IPSec SA.

Example

Clear IKE SAs in both phases.

```
<HUAWEI> reset ike sa
```

10.3.42 reset ike statistics

Function

The **reset ike statistics** command clears IKE statistics.

Format

reset ike statistics

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

To diagnose and locate faults of IPSec tunnels established using IKE, you can collect IKE statistics in a given period of time. You can run the **reset ike statistics** command to clear historical IKE statistics before starting statistics collection. You can then run the **display ike statistics** command to check IKE statistics.

Example

Clear IKE statistics.

```
<HUAWEI> reset ike statistics
```

10.3.43 reset ipsec history record

Function

The **reset ipsec history record** command clears history information about IPSec tunnels.

Format

reset ipsec history record

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored once being cleared.

You can run the **display ipsec history record** command to view history information about the current IPSec tunnel.

Example

Clear history information about IPSec tunnels.

```
<HUAWEI> reset ipsec history record
```

10.3.44 reset ipsec sa

Function

The **reset ipsec sa** command deletes IPSec SAs.

Format

reset ipsec sa [**remote** *ipv4-address* | **parameters** *ipv4-address* **esp** *spi* | **efficient-vpn** *efficient-vpn-name*]

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.
parameters *ipv4-address* **esp** *spi*	Specifies the three elements that uniquely identify an IPSec SA. The three elements are *ipv4-address* (destination address), *protocol* (ESP), and Security Parameter Index (SPI). To reset an SA, the three elements must be specified.	The three elements are described as follows: ● *ipv4-address*: IPv4 address. ● *protocol*: ESP. ● *spi*: an integer that ranges from 256 to 4294967295.
efficient-vpn *efficient-vpn-name*	Specifies the name of an Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

User view

Default Level

3: Management level

Usage Guidelines

When you run the **reset ipsec sa** command to delete IPSec SAs, note the following points:

- If no parameter is specified, all IPSec SAs are deleted.
- If **parameters** is specified, the IPSec SAs in two directions are deleted simultaneously.
- To delete IPSec SAs established through IKE negotiation, you must run the **reset ipsec sa** and **reset ike sa** commands in sequence. Otherwise, IPSec SAs established through IKE negotiation fail to be deleted. After the IPSec SAs are deleted, IKE peers re-negotiate IPSec SAs only when packets trigger IKE negotiation.

Example

Delete the IPSec SA created through Efficient VPN policy **evpn**.

```
<HUAWEI> reset ipsec sa efficient-vpn evpn
```

10.3.45 reset ipsec packet statistics

Function

The **reset ipsec packet statistics** command deletes statistics about IPSec packets.

Format

reset ipsec packet statistics

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics about IPSec packets within a given period of time, run this command to delete existing statistics.

Precautions

The deleted statistics about IPSec packets cannot be restored. Exercise caution when you run this command.

Example

Delete statistics about all IPSec packets.

```
<HUAWEI> reset ipsec packet statistics
```

10.3.46 sa binding vpn-instance (Efficient VPN policy view)

Function

The **sa binding vpn-instance** command binds a VPN instance to an IPSec tunnel.

The **undo sa binding vpn-instance** command unbinds a VPN instance from an IPSec tunnel.

By default, no VPN instance is bound to an IPSec tunnel.

Format

sa binding vpn-instance *vpn-instance-name*

undo sa binding vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance bound to an IPSec tunnel.	The value is an existing VPN instance name.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Applicable environment

On an VPN with small VPN sites, if CEs and PEs are connected through the Internet but not leased lines, hosts connected to a CE can access resources on another VPN site only through the insecure Internet. To enhance access security, these hosts can connect to the backbone network of the VPN through an IPSec tunnel.

This command specifies the VPN that the remote end of the IPSec tunnel belongs to. The tunnel initiator then can obtain the outbound interface and send packets through the outbound interface.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

A route distinguisher (RD) for the VPN instance has been configured using the **route-distinguisher** command.

Example

Bind the VPN instance **vpna** to the Efficient VPN policy **evpn**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpna
[HUAWEI-vpn-instance-vpna] ipv4-family
[HUAWEI-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpna-af-ipv4] vpn-target 100:100
[HUAWEI-vpn-instance-vpna-af-ipv4] quit
```

```
[HUAWEI-vpn-instance-vpna] quit
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] sa binding vpn-instance vpna
```

10.3.47 security acl

Function

The **security acl** command specifies an ACL to be referenced in an IPSec policy or IPSec policy template.

The **undo security acl** command cancels the configuration.

By default, an IPSec policy or IPSec policy template does not reference an ACL.

Format

security acl *acl-number*

undo security acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **security acl** command references an ACL that defines data flows to be protected by IPSec. In practice, you need to configure rules in an ACL to define data flows to be protected and apply the ACL to an IPSec policy to protect the data flows.

When an IPSec policy is created using an IPSec policy template, you can determine whether to define data flows to be protected by IPSec on the responder.

- If data flows to be protected by IPSec are not specified on the responder, the responder accepts the range of data flows to be protected by IPSec defined on the initiator.
- If data flows to be protected by IPSec are specified on the responder, the configuration on the responder must mirror that on the initiator or the range

of protected data flows on the responder must contain the range of protected data flows on the initiator.

Precautions

To reference an ACL in an IPSec policy, ensure that rules must be configured in this ACL view and the number of rules configured in this ACL view does not exceed 32. Otherwise, this ACL cannot be referenced in this IPSec policy.

Example

Reference ACL 3101 in an Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] acl number 3101
[HUAWEI-acl-adv-3101] rule permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.1.2 0.0.0.0
[HUAWEI-acl-adv-3101] quit
[HUAWEI] ipsec efficient-vpn name mode network
[HUAWEI-ipsec-efficient-vpn-name] security acl 3101
```

10.3.48 service-scheme (Efficient VPN policy view)

Function

The **service-scheme** command configures a server-end service scheme in an Efficient VPN policy.

The **undo service-scheme** command deletes a server-end service scheme from an Efficient VPN policy.

By default, no server-end service scheme is configured in an Efficient VPN policy.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme on the server end.	The service scheme name must already exist.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

In an Efficient VPN scenario, the customer wants to deploy network resources including the DNS domain name, DNS server address, WINS server address, and IP addresses on the server end (headquarters gateway). The server end pushes network resource information to remote ends (branch gateways) to simplify configuration and maintenance of network resources on them.

Remote ends are authorized based on network resource information pushed by the server end or the server-end AAA service scheme specified in an Efficient VPN policy. To use the AAA service scheme, run the **service-scheme** command to configure a server-end service scheme in an Efficient VPN policy and run the **local-id-type** command to specify the **key-id** parameter. Otherwise, the configuration does not take effect.

Example

Configure the server-end service scheme **service** in an Efficient VPN policy.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn name mode network
[HUAWEI-ipsec-efficient-vpn-name] service-scheme service
```

10.3.49 tunnel local

Function

The **tunnel local** command specifies the local address of an IPSec tunnel.

The **undo tunnel local** command cancels the configuration.

By default, no local IP address is configured for the IPSec tunnel.

Format

tunnel local { *ipv4-address* | **applied-interface** }

undo tunnel local

Parameters

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address for the local end of an IPSec tunnel.	The value is in dotted decimal notation.
applied-interface	Indicates the primary IP address of the IPSec-enabled interface is used as the local address of an IPSec tunnel.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to specify a start point for an IPSec tunnel.

You do not need to configure an IP address for the local end of an IPSec tunnel. During SA negotiation, the device will select a proper address based on route information. The local address needs to be configured in the following situations:

- If the IP address of the interface to which an IPSec policy is applied varies or is unknown, run the **tunnel local** *ipv4-address* command to specify the IP address of another interface (such as the loopback interface) on the device as the IP address for the local end of an IPSec tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface to which an IPSec policy is applied as the local address of an IPSec tunnel.
- If the interface to which an IPSec policy is applied has multiple IP addresses (one primary IP address and several secondary IP addresses), run the **tunnel local** *ipv4-address* command to specify one of these IP addresses as the IP address for the local end of an IPSec tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the primary IP address of the interface as the local address of an IPSec tunnel.
- If equal-cost routes exist between the local and remote ends, run the **tunnel local** command to specify a local IP address for an IPSec tunnel.

Example

Set the primary IP address of the interface to which the Efficient VPN policy in IKE negotiation mode is applied as the local IP address of the IPSec tunnel.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn name mode network
[HUAWEI-ipsec-efficient-vpn-name] tunnel local applied-interface
```

10.4 BGP/MPLS IP VPN Configuration Commands

10.4.1 Command Support

- Only the following switch models support working as a PE:

  S5731-H, S5731S-H, S5732-H, S5731-S, S6730-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H
- S1720GW-E and S1720GWR-E switches support working as an MCE. All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support working as an MCE.

10.4.2 apply tunnel-policy (tunnel-selector view)

Function

The **apply tunnel-policy** command applies a tunnel policy to routes filtered by the **if-match** clause.

The **undo apply tunnel-policy** command cancels the setting.

By default, no tunnel policy is configured for filtered routes.

Format

apply tunnel-policy *tunnel-policy-name*

undo apply tunnel-policy

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of a tunnel policy to be applied to the routes that match the **if-match** clause.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, by default, LSPs are selected for VPNv4 and BGP labeled routes without performing load balancing. If you want to select other types of tunnels or configure load balancing for VPNv4 or BGP labeled routes, run the **apply tunnel-policy** command to apply a tunnel policy. The **apply tunnel-policy** command can be used in the following situations:

- The RR on the backbone network of a VPN needs to apply a tunnel policy to VPNv4 routes learned from PEs.

If you want to apply a tunnel policy to only specific VPNv4 or BGP labeled routes in the situations mentioned above, first use the **if-match** clause to filter routes. The **if-match** commands that can be used are listed below:

- **if-match ip next-hop (tunnel-selector view)**

  The command filters IPv4 routes by next hop.
- **if-match ipv6 next-hop (tunnel-selector view)**

  The command filters IPv6 routes by next hop.
- **if-match rd-filter**

  The command filters routes by RD.

Prerequisite

The **tunnel-selector** command is run to create a tunnel selector; **if-match** clauses are configured as needed.

Follow-up Procedure

If the tunnel policy specified in the **apply tunnel-policy** command does not exist in the system, run the **tunnel-policy** command to create the tunnel policy.

Example

Select policy1 for the VPN routes that are filtered by RD in the tunnel selector view.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy policy1
[HUAWEI-tunnel-policy-policy1] tunnel select-seq cr-lsp lsp load-balance-number 1
[HUAWEI-tunnel-policy-policy1] quit
[HUAWEI] tunnel-selector tps permit node 10
[HUAWEI-tunnel-selector] if-match rd-filter 1
[HUAWEI-tunnel-selector] apply tunnel-policy policy1
```

10.4.3 apply-label per-instance

Function

The **apply-label per-instance** command sets the label allocation mode to one label per instance. In this mode, all the routes of the VPN instance address family destined for the remote PE are assigned the same label.

The **undo apply-label per-instance** command restores the default configuration.

By default, the VPN instance address family assigns the same label to all routes to be sent to the peer PE.

Format

apply-label per-instance

undo apply-label per-instance

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, if VPN routes on PE are numerous but MPLS label resources are insufficient, the **apply-label per-instance** command can be run to minimize MPLS label consumption on PE.

When a large number of routes of the VPN instance IPv4 address family need to apply for labels, the **apply-label per-instance** command saves label resources of PEs and lowers the requirements for PE capacities.

By default, the system applies for a label for each route in a VPN instance enabled with the IPv4 or IPv6 address family. After the **apply-label per-instance** command is run in the IPv4 or IPv6 address family view of the VPN instance, the routes of the VPN instance enabled with the corresponding address family will be allocated the same label. For example, a PE is configured with two VPN instances that have 20000 routes in total. By default, 20000 MPLS labels will be allocated to the routes. If the **apply-label per-instance** command is run, only two MPLS labels will be allocated to the routes.

You can run the **display fib statistics** command to check the number of VPN routes.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to enter the IPv4 or IPv6 VPN instance address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The change of the label allocation mode leads to the re-advertising of VPN routes. The services may be interrupted temporarily. Therefore, use the **apply-label per-instance** and **undo apply-label per-instance** commands with caution.

NOTE

If there are a large number of VPN routes in the system, frequently executing this command will cause flapping of many routes. Route flapping results in a high CPU usage but does not affect real-time services in the system.

Example

Assign one label to all routes of the IPv4 address family of the VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] apply-label per-instance
```

10.4.4 apply-label per-nexthop

Function

The **apply-label per-nexthop** command enables the ASBR to allocate labels for IPv4 VPN routes or IPv6 VPN routes based on the next hop.

The **undo apply-label per-nexthop** command disables the ASBR from allocating labels for IPv4 VPN routes or IPv6 VPN routes based on the next hop.

By default, next-hop-based label allocation for VPN routes is disabled on the ASBR, and a label is allocated to each VPN instance.

Format

apply-label per-nexthop

undo apply-label per-nexthop

Parameters

None

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In inter-AS VPN Option B or HoVPN networking, if MPLS label resources on the ASBR or SPE are insufficient for the advertised VPNv4 or VPNv6 routes to use, the **apply-label per-nexthop** command can be run to minimize MPLS label consumption on the ASBR or SPE.

By default, the ASBR or SPE allocates a label to each VPNv4 or VPNv6 route when advertising it to an MP-BGP peer. If the **apply-label per-nexthop** command is run, the ASBR or SPE will allocate one label to all the routes with the same next hop and outgoing label. To make the routes learned from the same next hop have the same outgoing label, run the **apply-label per-instance** command on the PE. Otherwise, the effect of the **apply-label per-nexthop** command will be affected.

Configuration Impact

After next-hop-based label allocation is enabled or disabled, the label allocated by the ASBR to a route changes, which leads to a transient loss of VPN packets.

Example

In the BGP-VPNv4 view, enable the ASBR to allocate labels to IPv4 VPN routes based on the next hop.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] apply-label per-nexthop
```

10.4.5 apply-label per-route

Function

The **apply-label per-route** command enables the one-label-per-route mode. The VPN instance address family assigns a unique label to each route to be sent to the peer PE.

The **undo apply-label per-route** command disables the one-label-per-route mode.

By default, the VPN instance address family assigns the same label to all routes to be sent to the peer PE.

Format

apply-label per-route

undo apply-label per-route

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to change the label allocation mode from one-label-per-instance to one-label-per-route, run the **apply-label per-route** command.

Prerequisite

The **route-distinguisher** command is run to configure an RD for the VPN instance enabled with the IPv4 or IPv6 address family.

Configuration Impact

The change of the label allocation mode leads to the re-advertising of VPN routes. The services may be interrupted temporarily. Exercise caution when running the **apply-label per-route** or **undo apply-label per-route** command.

The **apply-label per-instance** and **apply-label per-route** commands are mutually exclusive. If both commands are run, the latest configuration overrides the previous one.

Example

Enable the one-label-per-route mode for routes of **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] apply-label per-route
```

10.4.6 arp vpn-cross enable

Function

The **arp vpn-cross enable** command enables direct ARP entry delivery for mutual access between local VPNs.

The **undo arp vpn-cross enable** command disables direct ARP entry delivery for mutual access between local VPNs.

By default, direct ARP entry delivery is disabled for mutual access between local VPNs.

NOTE

Only the S5720I-SI, S5731-S, S5731S-S, S5731-H, S5732-H, S5735-S, S500, S5735S-S, S5735-S-I, S5736-S, S5735S-H, S6720S-S, S6720S-EI, S6735-S, S6720-EI, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

arp vpn-cross enable

undo arp vpn-cross enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The initial traffic between two local VPNs triggers ARP Miss messages and ARP learning. If a PE device fails to timely process the ARP Miss messages due to some reasons, mutual access traffic between the VPNs cannot be transmitted.

After direct ARP entry delivery is enabled on the PE device, the PE device delivers ARP entries before the mutual access traffic triggers ARP Miss messages and ARP learning. This ensures normal traffic transmission between local VPNs.

Precautions

ARP entry delivery before triggering of ARP Miss messages and ARP learning consumes ARP entries. Configure this command only when required.

Example

Enable direct ARP entry delivery for mutual access between local VPNs.

```
<HUAWEI> system-view
[HUAWEI] arp vpn-cross enable
Warning: After this function is enabled, a large number of ARP entries will be occupied.
```

10.4.7 as-number

Function

The **as-number** command configures an AS number for a VPN instance.

The **undo as-number** command restores the default setting.

By default, a VPN instance uses the AS number of BGP.

Format

as-number { *as-number-plain* | *as-number-dot* }

undo as-number

Parameters

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network transfer or service identification, a device needs to be simulated as multiple BGP devices logically. In this case, you can run the **as-number** command to configure an AS number for each VPN instance.

After the **as-number** command is used:

- BGP peer relationships in the VPN instance are established by using the configured AS number.
- The configured AS number is used to generate the aggregator attribute during route aggregation.
- When advertising routes to an EBGP peer, the local device carries the AS number configured in the VPN instance.

Prerequisites

If a BGP peer or a BGP peer group is configured in the VPN instance, you need to delete the configuration of the BGP peer or peer group before configuring or deleting an AS number.

Precautions

A VPN instance configured with an AS number cannot be configured with BGP confederation. Conversely, a VPN instance configured with BGP confederation cannot be configured with an AS number.

NOTE

The AS number configured in the BGP-VPN instance view cannot be the same as the AS number configured in the BGP view.

Example

Set the AS number of the VPN instance named **vpna** to 65001.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] as-number 65001
```

10.4.8 auto-frr

Function

The **auto-frr** command enables BGP Auto FRR.

The **undo auto-frr** command disables BGP Auto FRR.

By default, BGP Auto FRR is disabled.

Format

auto-frr

undo auto-frr

Parameters

None

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This function is applicable to networks that require a low packet loss ratio and a short delay.

Using BGP Auto FRR together with BFD is recommended. They can rapidly detect a link fault and switch traffic to a standby link if a fault occurs.

Example

Enable BGP Auto FRR for unicast routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] auto-frr
```

10.4.9 auto-frr (BGP-VPNv4 address family view)

Function

The **auto-frr** command enables VPNv4 FRR.

The **undo auto-frr** command restores the default configuration.

By default, VPNv4 FRR is disabled.

Format

auto-frr

undo auto-frr

Parameters

None.

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **auto-frr** command in the BGP-VPNv4 address family view enables VPNv4 FRR and improves network reliability. After VPNv4 FRR is configured, traffic can be switched to the backup LSP (Label Switched Path) immediately after the primary LSP to which a VPNv4 route recurses becomes faulty. VPNv4 FRR applies to HVPN scenarios.

- In an HVPN scenario, VPNv4 FRR is deployed on SPEs.

Prerequisites

BGP has been enabled.

Precautions

If used with BFD, VPNv4 FRR can rapidly detect link faults and switch services to the standby link for transmission.

Do not configure the **apply-label per-nexthop** command in the BGP-VPNv4 address family view if VPNv4 FRR is enabled, or VPNv4 FRR will fail to take effect.

If the **auto-frr** command is configured in the BGP-VPNv4 address family view, the **bestroute nexthop-resolved tunnel** command must also be configured, so that packets will not get lost during traffic switchback.

Example

Enable VPNv4 FRR.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] auto-frr
```

10.4.10 description (VPN instance view)

Function

The **description** command specifies the description of the current VPN instance.

The **undo description** command deletes the description of the current VPN instance.

By default, no description is specified for a VPN instance.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of a VPN instance.	The value is a string of 1 to 242 case-sensitive characters with spaces.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To record the purpose of creating a VPN instance and the CEs with which the VPN instance is associated, you can run the **description** command to specify the description of the VPN instance.

To check the description of a VPN instance, run the **display ip vpn-instance** command.

Precautions

If you run the **description** command several times, the latest configuration overrides the previous configurations.

Example

Specify the description of a VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] description OnlyForAB
```

10.4.11 description (tunnel interface view)

Function

The **description** command sets the description of the current tunnel interface.

The **undo description** command deletes the description of the current tunnel interface.

By default, a tunnel interface does not have a description.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a tunnel interface.	The value is a string of 1 to 242 case-sensitive characters, with spaces supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After using the **interface tunnel** command to create a tunnel interface, you can run the **description** command to configure a description of the tunnel interface to facilitate later query.

To check the description of a tunnel interface, run the **display this interface** command in the tunnel interface view or the **display interface tunnel** command.

Example

Configure the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

Delete the description of Tunnel 1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo description
```

10.4.12 description (tunnel-policy view)

Function

The **description** command configures the description of the current tunnel policy.

The **undo description** command cancels the setting.

By default, a tunnel policy does not have a description.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of the tunnel policy.	The value is a string of 1 to 80 case-sensitive characters with spaces.

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

After using the **tunnel-policy** command to create a tunnel policy, you can run the **description** command to configure a description of the tunnel policy to facilitate later query.

To check tunnel policy configurations, run the **display tunnel-policy-config** command.

Example

Configure the description of the tunnel policy named test1.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy test1
[HUAWEI-tunnel-policy-test1] description two TE tunnels are used
```

10.4.13 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Establish a manual IPv6 over IPv4 tunnel between VLANIF 10 at 10.1.1.1 on switch HUAWEI1 and VLANIF 20 at 10.2.1.1 on switch HUAWEI2.

```
<HUAWEI1> system-view
[HUAWEI1] interface tunnel 1
[HUAWEI1-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI1-Tunnel1] source 10.1.1.1
[HUAWEI1-Tunnel1] destination 10.2.1.1
<HUAWEI2> system-view
[HUAWEI2] interface tunnel 1
[HUAWEI2-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI2-Tunnel1] source 10.2.1.1
[HUAWEI2-Tunnel1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel1 to 10.1.1.1 that belongs to vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] destination vpn-instance vpn1 10.1.1.1
```

10.4.14 display default-parameter l3vpn

Function

The **display default-parameter l3vpn** command displays the default configuration of L3VPN during initialization.

Format

display default-parameter l3vpn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Scenario

You can run this command to check the default configuration of L3VPN during initialization, for example, default label allocation mode in a VPN instance.

Precautions

This command displays only the default configuration of L3VPN during initialization. The command output shows the default configuration of L3VPN during initialization even when the default configuration is changed.

Example

Display the default configuration of L3VPN during initialization.

```
<HUAWEI> display default-parameter l3vpn
 Apply label mode          :
    IPv4-family           : label per instance
    IPv6-family           : label per instance
```

Table 10-29 Description of the display default-parameter l3vpn command output

Item	Description
Apply label mode	Default label allocation mode.
IPv4-family	IPv4 address family.
IPv6-family	IPv6 address family.
label per instance	The default label allocation mode is label per instance.

10.4.15 display ip prefix-limit statistics

Function

The **display ip prefix-limit statistics** command displays the statistics of the prefix limits of VPN instances.

Format

display ip prefix-limit { **all-vpn-instance** | **vpn-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified VPN instance.

Example

Display the statistics of the prefix limits of all VPN instances.

```
<HUAWEI> display ip prefix-limit all-vpn-instance statistics
-------------------------------------------------------------------------------
VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0                0            0               0              0
STATIC         0                0            0               0              0
UNR            0                0            0               0              0
OSPF           0                0            0               0              0
IS-IS          0                0            0               0              0
RIP            0                0            0               0              0
BGP            0                0            0               0              0
MSR            0                0            0               0              0
-------------------------------------------------------------------------------
VPN instance name: vrf2
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0                0            0               0              0
STATIC         0                0            0               0              0
UNR            0                0            0               0              0
OSPF           0                0            0               0              0
IS-IS          0                0            0               0              0
RIP            0                0            0               0              0
BGP            0                0            0               0              0
MSR            0                0            0               0              0
```

Display the statistics of the prefix limit of the VPN instance named **vrf1**.

```
<HUAWEI> display ip prefix-limit vpn-instance vrf1 statistics
-------------------------------------------------------------------------------
VPN instance name: vrf2
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0                0            0               0              0
STATIC         0                0            0               0              0
UNR            0                0            0               0              0
OSPF           0                0            0               0              0
IS-IS          0                0            0               0              0
RIP            0                0            0               0              0
BGP            0                0            0               0              0
MSR            0                0            0               0              0
```

Table 10-30 Description of the display ip prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

10.4.16 display ipv6 prefix-limit statistics

Function

The **display ipv6 prefix-limit statistics** command displays the statistics of the prefix limits of IPv6 VPN instances.

Format

display ipv6 prefix-limit { **all-vpn-instance** | **vpn-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv6 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value is the name of an existing IPv6 VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified IPv6 VPN instance.

Example

Display the statistics of the prefix limits of all IPv6 VPN instances.

```
<HUAWEI> display ipv6 prefix-limit all-vpn-instance statistics
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT          0              0          0             0            0
STATIC          0              0          0             0            0
UNR             0              0          0             0            0
OSPFv3          0              0          0             0            0
IS-IS           0              0          0             0            0
RIPng           0              0          0             0            0
BGP             0              0          0             0            0
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf2
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT          0              0          0             0            0
STATIC          0              0          0             0            0
UNR             0              0          0             0            0
OSPFv3          0              0          0             0            0
IS-IS           0              0          0             0            0
RIPng           0              0          0             0            0
BGP             0              0          0             0            0
```

Display the statistics of the prefix limit of the IPv6 VPN instance named **vrf1**.

```
<HUAWEI> display ipv6 prefix-limit vpn-instance vrf1 statistics
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT          0              0          0             0            0
STATIC          0              0          0             0            0
UNR             0              0          0             0            0
OSPFv3          0              0          0             0            0
IS-IS           0              0          0             0            0
RIPng           0              0          0             0            0
BGP             0              0          0             0            0
```

Table 10-31 Description of the display ipv6 prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.

Item	Description
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

10.4.17 display ip vpn-instance

Function

The **display ip vpn-instance** command displays configurations of VPN instances.

Format

display ip vpn-instance [**verbose**] [*vpn-instance-name*]

display ip vpn-instance [*vpn-instance-name*] **interface**

display ip vpn-instance [*vpn-instance-name*] **tunnel-info**

Parameters

Parameter	Description	Value
verbose	Displays detailed information about VPN instances.	-
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
interface	Displays information about the interfaces bound to the VPN instance.	-
tunnel-info	Displays information about the LSP associated with the VPN instance.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you want to check the configurations of VPN instances, interfaces bound to them, and LSPs associated with them, run the **display ip vpn-instance** command.

Since VPN instances support both IPv4 and IPv6 address families, the **display ip vpn-instance** command displays the information of different address families separately.

If *vpn-instance-name* is not specified, the **display ip vpn-instance** command displays information about all configured VPN instances on the device.

If **interface** is specified, the display ip vpn-instance command displays all interfaces bound to the specified VPN instance.

If **tunnel-info** is specified, the **display ip vpn-instance** command displays information about the LSPs to which the routes of the VPN instance enabled with the IPv4 or IPv6 address family recurse (in other words, information about the LSPs between PEs). If the tunnels between PEs are not LSPs, the **display ip vpn-instance** command does not display tunnel information.

Precautions

If the VPN instance to be displayed is not created, the system prompts that the VPN instance does not exist.

Example

Display brief information about all VPN instances.

```
<HUAWEI> display ip vpn-instance
 Total VPN-Instances configured      : 2
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 0

  VPN-Instance Name              RD                  Address-family
  vpn1
  vpna                         100:1               IPv4
  vpnb                         100:2               IPv4
```

Table 10-32 Description of the display ip vpn-instance command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name	Name of the VPN instance.
RD	RD of the VPN instance IPv4 address family or IPv6 address family.

Item	Description
Address-family	Address family enabled for the VPN instance. The address family can be: ● Null, if no address family is enabled. ● IPv4, if only the IPv4 address family is enabled. ● IPv6, if only the IPv6 address family is enabled.

Display detailed information about all VPN instances.

```
<HUAWEI> display ip vpn-instance verbose
 Total VPN-Instances configured      : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 1

 VPN-Instance Name and ID : vpna, 6
  Description : vpna-1
  Service ID : 12
  Interfaces : Vlanif10
 Address family ipv4
  Create date : 2013-03-06 15:20:43+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Route Distinguisher : 100:1
  Export VPN Targets :  1:1
  Import VPN Targets :  1:1
  Label Policy : label per instance
  Per-Instance Label : 1024
  IP FRR Route Policy : 20
  VPN FRR Route Policy : 12
  Import Route Policy : 10
  Export Route Policy : 20
  Tunnel Policy : bindTE
  Maximum Routes Limit : 2000
  Threshold Routes Limit : 80%
  Maximum Prefixes Limit : 1024
  Threshold Prefixes Limit : 50%
  Install Mode : route-unchanged
  Log Interval : 10
 Address family ipv6
  Create date : 2013-03-06 15:20:43+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Log Interval : 5
```

Table 10-33 Description of the display ip vpn-instance verbose command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.

Item	Description
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name and ID	Name and ID of the VPN instance. The ID is assigned by the system, which facilitates indexing.
Description	Description of the VPN instance. This field is displayed in the command output only when the **description (VPN instance view)**command is used.
Service ID	Service ID of the VPN instance. This item is displayed only after the **service-id (VPN instance view)** command is run in the VPN instance view.
Interfaces	Interfaces bound to the VPN instance. This field is displayed only after the **ip binding vpn-instance** command is configured on these interfaces.
Address family ipv4	Information about the IPv4 address family enabled for the VPN instance.
Address family ipv6	Information about the IPv6 address family enabled for the VPN instance.
Create date	Time when the VPN instance is created.
Up time	Period during which the VPN instance maintains in the Up state.
Route Distinguisher	RD of the VPN instance IPv4 address family or IPv6 address family. To specify an RD, run the **route-distinguisher** command.
Export VPN Targets	Route Target list in the outbound direction. To set the VPN target, run the **vpn-target** command.
Import VPN Targets	Route Target list in the inbound direction. To set the VPN target, run the **vpn-target** command.

Item	Description
Label Policy	Label policy: ● label per instance: indicates that the same label is allocated to routes of a VPN instance. This field is displayed in the command output only when the **apply-label per-instance** command is run in the VPN instance view. ● label per route: indicates that each route of a VPN instance is assigned a label.
Per-Instance Label	Label value used when all VPN routes of the VPN instance address family share one label. This field is displayed only after the **apply-label per-instance** command is run in the VPN instance address family view.
IP FRR Route Policy	IP FRR route policy used for the address family. This item is displayed only after the **ip frr** command is run in the VPN instance IPv4 address family view.
VPN FRR Route Policy	VPN FRR route policy used for the address family. This item is displayed only after the **vpn frr** command is run in the VPN instance IPv4 address family view.
Import Route Policy	Import Route-Policy applied to the VPN instance. This field is displayed only after the **import route-policy** command is run in the VPN instance address family view.
Export Route Policy	Export Route-Policy applied to the VPN instance. This field is displayed only after the **export route-policy** command is run in the VPN instance address family view.
Tunnel Policy	Tunnel policy applied to the VPN instance. This field is displayed only after the **tnl-policy** command is run in the VPN instance address family view.

Item	Description
Maximum Routes Limit	Maximum number of routes supported by the current address family. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Threshold Routes Limit	Percentage of the maximum number of routes specified for the current address family. When the maximum number of routes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Maximum Prefixes Limit	Maximum number of prefixes supported by the current address family of the VPN instance. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Threshold Prefixes Limit	Percentage of the maximum number of prefixes specified for the current address family of the VPN instance. When the maximum number of prefixes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Install Mode	Method of processing routes. The **prefix limit** command can be used to specify the route processing method when the threshold is lowered due to the number of route prefixes exceeding the upper threshold. ● If **route-unchanged** is configured, routes in the routing information base (RIB) table remain unchanged. ● If **route-unchanged** is not configured, all routes in the RIB table are deleted and the routes are re-installed in the RIB table.

Item	Description
Log Interval	Interval for displaying log messages when the number of VPN instance routes exceeds the maximum value. The default interval is 5 seconds. The value can be set by the command **limit-log-interval**.

Display information about the interface bound to the VPN instance named **vrf1**.

```
<HUAWEI> display ip vpn-instance vrf1 interface
 VPN-Instance Name and ID : vrf1, 1
  Interface Number : 1
  Interface list : Vlanif40
```

Table 10-34 Description of the display ip vpn-instance interface command output

Item	Description
Interface Number	Number of interfaces bound to the VPN instance
Interface list	List of interfaces bound to the VPN instance

Display information about the LSP associated with the vrf1 VPN instance.

```
<HUAWEI> display ip vpn-instance vrf1 tunnel-info
 VPN-Instance Name and ID : vrf1, 1
 Address family ipv4
  Nexthop Address              Tunnel ID
  1.1.1.1                    0x3
 Address family ipv6
  Nexthop Address              Tunnel ID
  1.1.1.1                    0x3
```

Table 10-35 Description of the display ip vpn-instance tunnel-info command output

Item	Description
Nexthop Address	Indicates the next-hop address of the route learned by the VPN instance from the peer PE.
Tunnel ID	Indicates the ID of the LSP corresponding to the next-hop address of the route learned by the VPN instance from the peer PE.

10.4.18 display ip vpn-instance import-vt

Function

The **display ip vpn-instance import-vt** command displays all VPN instances with the specified import vpn-target attribute.

Format

display ip vpn-instance import-vt *ivt-value*

Parameters

Parameter	Description	Value
ivt-value	Specifies the value of the import VPN-target attribute. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a PE is configured with multiple VPN instances, the **display ip vpn-instance import-vt** command can be run on the PE to check into which VPN instances a VPNv4 route with a specified VPN target can be imported.

The VPN target controls route learning between VPN instances. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 route to be advertised to a remote MP-BGP peer. Receiving a VPNv4 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 route can be added to the routing table of the local VPN instance IPv4 address family.

Precautions

At present, this command cannot be used to view the VPN instance with multiple import VPN-target attributes specified.

Example

Display the VPN instance with the import VPN-target attribute being 1:1.

```
<HUAWEI> display ip vpn-instance import-vt 1:1
The number of ipv4-family matched the import-vt : 3
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf4, 5
 VPN-Instance Name and ID : vrf5, 4

The number of ipv6-family matched the import-vt : 2
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf5, 4
```

Table 10-36 Description of the display ip vpn-instance import-vt command output

Item	Description
The number of ipv4-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv4 address family view.
The number of ipv6-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv6 address family view.
VPN-Instance Name and ID	Name and ID of the VPN instance.

10.4.19 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command. You can run this command to obtain tunnel interface information when configuring tunnels or when locating the fault on these tunnels.

Prerequisites

Before run **display interface tunnel**, please ensure that tunnel interface has been created using the **interface tunnel** command.

Example

Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-11-16 19:16:33 UTC+08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.1.2/24
```

```
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.2.1.2 (Vlanif1234), destination 10.2.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2012-11-16 19:17:39+08:00
Last 300 seconds input rate 16 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  5 packets, 650 bytes
Output:  0 packets, 0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 10-37 Description of the display interface tunnel command output

Item	Description
Tunnel1 current state	Physical layer status of the tunnel interface: ● UP: The interface is in normal state. ● Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status: ● UP: The link layer protocol of the tunnel interface works normally. ● Down: The link layer protocol of the tunnel interface is abnormal.
Last line protocol up time	Last time the link layer protocol of the tunnel interface goes UP. **NOTE** This field is displayed only when the link layer protocol status of the tunnel interface is UP.
Description	Description of the tunnel interface.
Route Port	Indicates the Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is 10.3.1.2/24	IP address of the tunnel interface is 10.3.1.2. The mask is 24 bits, that is, 255.255.255.0.
Encapsulation is TUNNEL,	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.2.1.2 (Vlanif1234)	The source address of the tunnel is 10.2.1.2. That is, the IP address of the VLANIF 1234 interface sending packets at the source side is 10.2.1.2.

Item	Description
destination 10.2.1.1	Destination address of the tunnel.
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive enable period 5 retry-times 3	The keepalive function of GRE.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization : --	Input bandwidth usage.
Output bandwidth utilization : --	Output bandwidth usage.

10.4.20 display l3vpn vpn-list tunnel-policy

Function

The **display l3vpn vpn-list tunnel-policy** command displays all the VPN instances to which a specified tunnel policy is applied.

Format

display l3vpn vpn-list tunnel-policy *tunnel-policy-name*

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of a tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To have its routes recursing to tunnels, a VPN instance needs to apply a tunnel policy. If the tunnel policy used by a VPN instance is changed or the status of tunnels selected based on the tunnel policy changes, the recursive tunnels may change. The **display l3vpn vpn-list tunnel-policy** command displays all the VPN instances to which a specified tunnel policy is applied. The command output will show the VPN instances that will be affected by changes in the tunnel policy.

Example

Display the referential relationship between a tunnel policy and a VPN instance.

```
<HUAWEI> display l3vpn vpn-list tunnel-policy p1
Codes: *(Tunnel policy is not configured)
Tunnel Policy Name: p1
Total VPN Instance(s) number: 1
VPN(s) using the tunnel policy:
vrf1
```

Table 10-38 Description of the **display l3vpn vpn-list tunnel-policy** command output

Item	Description
Codes	Comments

Item	Description
Tunnel Policy Name	Name of a tunnel policy
Total VPN Instance(s) number	Number of VPN instances specified with tunnel policies
VPN(s) using the tunnel policy	Name of VPN instances specified with tunnel policies

10.4.21 display mpls label-stack vpn-instance

Function

The **display mpls label-stack vpn-instance** command displays information about L3VPN label stacks.

Format

display mpls label-stack vpn-instance *vpn-instance-name ip-address*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
ip-address	Specifies a private IPv4 address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In a non-inter-AS L3VPN scenario, this command allows you to query label stack information on PEs based on VPN instance names and private IP addresses.

Example

Display label stack information about the VPN instance named **vpna**.

```
<HUAWEI> display mpls label-stack vpn-instance vpna 10.12.12.1
Label-stack  : 1
Level        : 1
Type         : VPN
```

```
Label       : 1033
Level       : 2
Type        : LDP
Label       : 1041
OutInterface : Vlanif100
```

Table 10-39 Description of the **display mpls label-stack vpn-instance** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

10.4.22 display tunnel-info

Function

The **display tunnel-info** command displays the tunnel information.

Format

display tunnel-info { **tunnel-id** *tunnel-id* | **all** | **statistics** [**slots**] }

Parameters

Parameter	Description	Value
tunnel-id *tunnel-id*	Specifies the tunnel ID. If the specified ID does not exist, the system prompts errors.	A hexadecimal integer ranging from 1 to FFFFFFFE.
all	Displays information about all the tunnels.	-
statistics	Displays statistics about all tunnels.	-
slots	Displays tunnel statistics in the order of slots.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display tunnel-info all** command displays existing tunnel IDs, tunnel types, destination IP addresses, and Token information about all tunnels.

The **display tunnel-info tunnel-id** *tunnel-id* command displays detailed information about a tunnel when you only know the tunnel ID.

The **display tunnel-info statistics** command displays the number of tunnels configured on the switch.

Example

View information about the tunnel.

```
<HUAWEI> display tunnel-info tunnel-id 2
Tunnel ID:                    0x2
Tunnel Token:                 2
Type:                         cr lsp
Destination:                  1.1.1.1
Out Slot:                     0
Instance ID:                  0
Interface:                    Tunnel1
Sub Tunnel ID:                0x0
<HUAWEI> display tunnel-info tunnel-id 3
Tunnel ID:                    0x3
Tunnel Token:                 3
Type:                         lsp
Destination:                  10.20.10.10
Out Slot:                     0
Instance ID:                  0
Out Interface:                Vlanif1024
Out Label:                    3
Next Hop:                     10.24.10.200
Lsp Index:                    2048
<HUAWEI> display tunnel-info tunnel-id 10006
Tunnel ID:                    0x10006
Tunnel Token:                 2
Type:                         lsp
Destination:                  6.6.6.6
Out Slot:                     0
Instance ID:                  0
Out Interface:                Vlanif15
Lsp Index:                    0
SubTunnel Type:               L2VPN QoS Token
```

Table 10-40 Description of the **display tunnel-info tunnel-id** command output

Item	Description
Tunnel ID	Tunnel ID in hexadecimal notation that is assigned by the system.
Tunnel Token	Token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.

Item	Description
Type	Type of a tunnel, such as GRE, MPLS LSP, or CR-LSP. The command output varies according to the tunnel type.
Destination	Destination IP address of the tunnel.
Out Slot	Number of the slot that is used when the switch sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.
Sub Tunnel ID	Sub-tunnel ID of VPN QoS in hexadecimal notation that is automatically assigned by the system.
Out Label	Out label value.
Next Hop	Next hop.
Lsp Index	LSP index, which is allocated by MPLS.
Out Interface	Local outbound interface of the tunnel.
SubTunnel Type	Types of tokens of sub-tunnels: ● LDP LSP over TE QoS Token ● LDP LSP QoS Token ● BGP LSP over TE QoS Token ● BGP LSP QoS Token ● Static LSP QoS Token ● CR-LSP over TE QoS Token ● L2VPN over TE QoS Token ● L2VPN QoS Token This field is displayed only for sub-tunnels.

Display all tunnel information.

```
<HUAWEI> display tunnel-info all
 * -> Allocated VC Token
Tunnel ID           Type                Destination           Token
----------------------------------------------------------------------
0x10006             lsp                 10.2.1.1              6
```

Display tunnel statistics.

```
<HUAWEI> display tunnel-info statistics
LSP/32bit LSP :                     0/0
GRE :                               2
CRLSP :                             0
LOCAL IFNET :                       0
MPLS LOCAL IFNET :                  0
VPN QOS LSP :                       0
```

```
Reserved :                        0
Vxlan :                         0
```

Table 10-41 Description of the **display tunnel-info statistics** command output

Item	Description
LSP/32bit LSP	Number of LSP tunnels created in the system view/Number of LSP tunnels triggered by the route of host with the 32-bit mask address.
GRE	Number of tunnel IDs allocated to the GRE tunnels.
CRLSP	Number of tunnel IDs allocated to the CR-LSP tunnels.
LOCAL IFNET	Number of tunnels used by the VPN internal module.
MPLS LOCAL IFNET	Number of tunnels used by the MPLS internal module.
VPN QOS LSP	Number of the tunnel ID allocated to the LSP used in VPN QoS.
Reserved	Number of the tunnel ID allocated to the product.
Vxlan	Number of tunnel IDs allocated to the Vxlan tunnels.

Display tunnel statistics in the order of slots.

```
<HUAWEI> display tunnel-info statistics slots
--------------------------------------------------------------------
Slot      LSP     CR     GRE      LCL     MPLS-L  VPN     VXLAN
Num               LSP           IFNET    IFNET   QOS
--------------------------------------------------------------------
0         0     0      0      0      0      0      0
Logic Slot: 0                  Total:  0
```

Table 10-42 Description of the display tunnel-info statistics slots command output

Item	Description
Slot Num	Slot number used by the device to send packets.
LSP	Total LSP tunnels set up by the device.
CR LSP	Number of CR-LSPs created on the device.
GRE	Number of GRE tunnels created on the device.
LCL IFNET	Number of tunnels used by the VPN module.
MPLS-L IFNET	Number of tunnels used by the MPLS module.

Item	Description
VPN QOS	Number of tunnels used for VPN QoS.
VXLAN	Number of VXLAN tunnels created on the device.

10.4.23 display tunnel-policy

Function

The **display tunnel-policy** command displays the configurations of tunnel policies.

Format

display tunnel-policy [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of tunnel policy. If *tunnel-policy-name* is specified, information about the specified tunnel policy is displayed.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display tunnel-policy** command, you can check the configured tunnel policy and information about a tunnel policy before applying it.

Example

Display information about all the tunnel policies.

```
<HUAWEI> display tunnel-policy
Total   tunnel policy num:            3
Sel-Seq tunnel policy num:            1
Binding tunnel policy num:            1
Invalid tunnel policy num:            1

Tunnel Policy Name                    Select-Seq                    Load balance No
-------------------------------------------------------------------------------------------
po2                              CR-LSP LSP                    3
```

```
Tunnel Policy Name                    Destination      Tunnel Intf       Ignore-dest-check   Down switch
------------------------------------------------------------------------------------------------------------------
po2                            1.1.1.9         Tunnel2           Disable             Enable
```

Table 10-43 Description of the display tunnel-policy command output

Item	Description
Total tunnel policy num	Total number of tunnel policies.
Sel-Seq tunnel policy num	Total number of tunnel policies in select-sequence mode.
Binding tunnel policy num	Total number of tunnel policies in tunnel binding mode.
Invalid tunnel policy num	Total number of invalid tunnel policies.
Tunnel Policy Name	Name of tunnel policies.
Select-Seq	Priorities of tunnel types in descending order.
Load balance No	Number of tunnels for load balancing. The default value is 1.
Destination	Destination IP addresses of the bound tunnels, that is, IP addresses of the peer interfaces that receive packets.
Tunnel Intf	Local tunnel interface of the bound tunnel.
Ignore-dest-check	Check is disabled regardless of whether the destination IP address specified in a tunnel policy is consistent with the actual destination address of the tunnel to be bound to the tunnel policy.
Down switch	Tunnel switch over status: ● Enable indicates that the function is enabled ● Disable indicates that the function is disabled

Display information about the tunnel policy.

```
<HUAWEI> display tunnel-policy p1
The number of binding:1
Tunnel Policy Name                    Destination      Tunnel Intf       Ignore-dest-check   Down Switch
------------------------------------------------------------------------------------------------------------------
p1                             1.1.1.1         Tunnel2           Disable             Enable
```

Table 10-44 Description of the display tunnel-policy tunnel-policy-name command output

Item	Description
The number of binding	Number of the bound destination addresses.

10.4.24 display tunnel-policy-config

Function

The **display tunnel-policy-config** command displays the configuration of tunnel policies.

Format

display tunnel-policy-config [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Indicates the name of the tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After tunnel policies are configured, you can view the configuration of a tunnel policy by using the **display tunnel-policy-config** command. If you do not specify the tunnel policy to be displayed, the configurations of all tunnel policies are displayed.

Example

Display the configurations of all tunnel policies.

```
<HUAWEI> display tunnel-policy-config
#
tunnel-policy whm1
 description 1.1.1.1
#
tunnel-policy whm2
 description 1.1.1.1
```

```
 tunnel select-seq cr-lsp lsp load-balance-number 3
#
tunnel-policy whm3
 tunnel binding destination 1.1.1.1 te Tunnel2
#
return
```

Display the configuration of the tunnel policy named p1.

```
<HUAWEI> display tunnel-policy-config p1
#
tunnel-policy p1
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
return
```

10.4.25 display tunnel-policy subscriber statistics

Function

The **display tunnel-policy subscriber statistics** command displays the number of times a tunnel policy is used by external services.

Format

display tunnel-policy *tunnel-policy-name* **subscriber statistics**

Parameters

Parameter	Description	Value
tunnel-policy-name	Specify the name of a tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A system has many tunnel policies that can be used by different services. The **display tunnel-policy subscriber statistics** command can be used to view the number of times a tunnel policy is used by external services. This prevents the tunnel policy from being deleted mistakenly.

Example

View the number of times a tunnel policy is used by external services.

```
<HUAWEI> display tunnel-policy nms-vrf-vpna subscriber statistics
The specified tunnel policy does not exist.
Total 0 applications subscribed the tunnel policy.
```

View the number of times a tunnel policy is used by external services.

```
<HUAWEI> display tunnel-policy nms-vrf-vpna subscriber statistics
Total 200 applications subscribed the tunnel policy.
```

Table 10-45 Description of the **display tunnel-policy subscriber statistics** command output

Item	Description
The specified tunnel policy does not exist. Total 0 applications subscribed the tunnel policy.	The tunnel policy does not exist and is not used by applications.
Total 200 applications subscribed the tunnel policy.	The tunnel policy exists and is used by 200 applications.

10.4.26 display tunnel-selector

Function

The **display tunnel-selector** command displays the configurations of tunnel selectors of a system.

Format

display tunnel-selector [*tunnel-selector-name*]

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel selector.	The value is the name of an existing tunnel selector.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *tunnel-selector-name* is not specified in the command, the command displays the configurations of all the tunnel selectors of the system.

Example

Display information about a tunnel selector named tps.

```
<HUAWEI> display tunnel-selector tps
Tunnel-selector : tps
  permit : 10 (matched counts: 0)
    Match clauses :
      if-match ip next-hop ip-prefix ipv4prefix
    Apply clauses :
      apply tunnel-policy policy1
```

Table 10-46 Description of the **display tunnel-selector** command output

Item	Description
Tunnel-selector	Name of a tunnel selector
permit : 10	Matching mode and number of the node of the tunnel selector
Match clauses	**if-match** clauses
Apply clauses	**apply** causes

10.4.27 export route-policy

Function

The **export route-policy** command associates the current VPN instance address family with an export Route-Policy.

The **undo export route-policy** command disassociates the current VPN instance address family from the export Route-Policy.

By default, the current VPN instance address family is not associated with any export Route-Policy.

Format

export route-policy *policy-name*

undo export route-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the export Route-Policy to be associated with the VPN instance address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can implement a more accurate advertisement of the routes of the VPN instance address family based on the export Route-Policy than that based on the extended community attribute. The export Route-Policy is used to filter the routing information and to set the routing attributes of the routes that pass the filtering.

The **export route-policy** command advertises local routes of the VPN instance address family to other VPN instances address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

In local cross scenarios, you can run the **export route-policy** command to filter out locally crossed routes and set the attributes of these routes. Locally crossed routes include both locally imported routes and routes learned from VPN peers.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one export Route-Policy. If the **export route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy does not exist, you need to configure the route policy.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command in the VPN instance view or BGP-VPN instance IPv4 address family view, all routes in the VPN instance address family can be crossed to the VPNv4 address family. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command in the BGP-VPN instance IPv6 address family view, all routes in the BGP-VPN instance IPv6 address family can be crossed to the VPNv6 address family.

Example

Apply an export Route-Policy named poly-1 to the IPv4 address family of the VPN instance named vrf1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] export route-policy poly-1
```

10.4.28 if-match ip next-hop (tunnel-selector view)

Function

The **if-match ip next-hop** command configures route filtering based on the next hop.

The **undo if-match ip next-hop** command cancels the setting.

By default, route filtering based on the next hop is not configured.

Format

if-match ip next-hop { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }

undo if-match ip next-hop [**acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name*]

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be run in the tunnel selector view on the SPE in HVPN networking needs to apply a tunnel policy to VPNv4 routes to, for example, have the VPNv4 routes recursing to MPLS TE tunnels.

The **if-match ip next-hop** command is used to apply a tunnel policy to the VPNv4 or BGP-IPv4 labeled routes with a specified next hop, not all VPNv4 or BGP-IPv4 labeled routes.

Either an ACL or IP prefix list can be used to filter routes by next hop.

Prerequisite

The **tunnel-selector** command is run to create a tunnel selector.

An IP prefix list is configured using the **ip ip-prefix** command, or an ACL is configured using the **acl** command in the system view or the **acl name** command to specify the next hop.

Follow-up Procedure

Run the **apply tunnel-policy** command in the tunnel selector view to apply a tunnel policy to the routes that pass the filtering.

Precautions

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes match the ACL.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

Configure route filtering based on the next hop.

```
<HUAWEI> system-view
[HUAWEI] tunnel-selector abc permit node 10
[HUAWEI-tunnel-selector] if-match ip next-hop acl 2000
```

10.4.29 if-match ip-prefix (tunnel-selector view)

Function

The **if-match ip-prefix** command configures a tunnel selector to use an IP prefix list as a route filtering rule.

The **undo if-match ip-prefix** command restores the default configuration.

By default, a tunnel selector does not use any IP prefix list as a route filtering rule.

Format

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix *ip-prefix-name*

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel-selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to match routes against a specified IP prefix list and determine whether to permit or deny the routes based on matching results, run the **if-match ip-prefix** command to configure a tunnel selector to use the IP prefix list as a route filtering rule.

The **if-match ip-prefix** command must be used with the **ip ip-prefix** command. For example:

If the **if-match ip-prefix aa** and **ip ip-prefix aa permit 1.1.1.1 32** commands are both configured, BGP routes with IP prefix 1.1.1.1/32 will be permitted.

Prerequisites

A tunnel selector has been configured using the **tunnel-selector** command.

The IPv4 prefix list has been created by running the **ip ip-prefix** command.

Precautions

Routes are filtered by IP prefix. Only routes matching the specified IP prefix list are permitted.

Example

Configure a tunnel selector to use IP prefix list **p1** as a route filtering rule.

```
<HUAWEI> system-view
[HUAWEI] ip ip-prefix p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
[HUAWEI] tunnel-selector policy permit node 10
[HUAWEI-tunnel-selector] if-match ip-prefix p1
```

10.4.30 if-match ipv6 next-hop (tunnel-selector view)

Function

The **if-match ipv6 next-hop** command configures the filtering of IPv6 routes based on the next hop.

The **undo if-match ipv6 next-hop** command cancels the setting.

By default, the filtering of IPv6 routes based on the next hop is not configured.

Format

if-match ipv6 next-hop prefix-list *ipv6-prefix-name*

undo if-match ipv6 next-hop prefix-list *ipv6-prefix-name*

Parameters

Parameter	Description	Value
prefix-list *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

You can run the **if-match ipv6 next-hop** command if it is required to filter IPv6 routes based on the next hop. When you run the **if-match ipv6 next-hop** command in the tunnel selector view, you can use an **apply** clause to apply a tunnel policy to the IPv6 routes filtered based on the next hop.

The next hop can be specified by the IPv6 prefix list.

Example

Configure filtering of IPv6 routes based on the next hop.

```
<HUAWEI> system-view
[HUAWEI] tunnel-selector abc permit node 10
[HUAWEI-tunnel-selector] if-match ipv6 next-hop prefix-list ipv6prefix
```

10.4.31 import route-policy

Function

The **import route-policy** command associates the current VPN instance address family with an import Route-Policy.

The **undo import route-policy** command disassociates the current VPN instance address family from an import Route-Policy.

By default, the current VPN instance address family is not associated with any import Route-Policy.

Format

import route-policy *policy-name*

undo import route-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the import Route-Policy to be associated with the VPN instance address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no import Route-Policy is configured, routes that match the export VPN target attribute of the received routes and the import VPN target attribute of the local VPN instance address family are added to the VPN instance address family.

To control the import of the routes into the VPN instance address family more accurately, you can use the import Route-Policy. The import Route-Policy is used to filter the imported routing information and to set the routing attributes of the routes that pass the filtering.

The **import route-policy** command controls the VPN routes that are cross added to the VPN instance address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one import Route-Policy. If the **import route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy to be associated with the VPN instance address family does not exist, you need to configure the route policy.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command in the VPN instance view or BGP-VPN instance IPv4 address family view, all routes in the VPNv4 address family can be crossed to the VPN instance address family. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command in the BGP-VPN instance IPv6 address family view, all routes in the VPNv6 address family can be crossed to the VPN instance address family.

Example

Apply an import Route-Policy named poly-1 to the IPv4 address family of the VPN instance named vrf1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] import route-policy poly-1
```

10.4.32 ingress-lsp trigger

Function

The **ingress-lsp trigger** command specifies a routing policy to control the creation of ingress LSPs based on BGP labeled routes.

The **undo ingress-lsp trigger** command restores the default setting.

By default, ingress LSPs are created based on all received BGP labeled routes.

NOTE

This command is not supported by the S5731S-S, S6730S-S, and S6735-S.

Format

ingress-lsp trigger route-policy *route-policy-name*

undo ingress-lsp trigger

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a routing policy to be used to create ingress LSPs based on BGP labeled routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a MAN where the hybrid access mode is used, a large number of BGP labeled routes are used to establish end-to-end LSPs. On certain intermediate nodes where VPN services do not need to be supported, excessive ingress LSPs are created, causing the waste of network resources. In this case, you can run the **ingress-lsp trigger** command to create ingress LSPs based on a routing policy to save network resources.

Precautions

If the **ingress-lsp trigger** command is run more than once, the latest configuration overrides the previous ones.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, ingress LSPs are established for all labeled routes.

Example

Specify a routing policy named test-policy to control the creation of ingress LSPs based on labeled IPv4 routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] ingress-lsp trigger route-policy test-policy
```

10.4.33 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is an integer that ranges from 0 to 2047 .

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- GRE

- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

Follow-up Procedure

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Example

Create a tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1]
```

10.4.34 ip binding vpn-instance

Function

The **ip binding vpn-instance** command associates an interface on a PE with a VPN instance.

The **undo ip binding vpn-instance** command disables the association between a VPN instance and an interface.

By default, an interface is a public network interface and is not associated with any VPN instance.

Format

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance that is associated with the interface.	The value must be an existing VPN instance name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a VPN instance is created, you need to associate the PE interface connecting to the VPN with the VPN instance. Then, the interface is used as a private network interface on which a private network address and a private network routing protocol can be configured.

Prerequisites

The **ip vpn-instance** command has been executed to create a VPN instance.

Precautions

Binding an interface to a VPN instance or deleting the binding will result in the deletion of the IP address, Layer 3 features, and IP-related routing protocols of the interface as well as IGMP snooping and MLD snooping configurations of the VLAN to which the interface is added. These features must be re-configured if needed.

An interface cannot be bound to any VPN instance that is not enabled with any address family.

Using the **undo ipv4-family** or **undo ipv6-family** command to disable the IPv4 or IPv6 address family also deletes the IPv4 or IPv6 configurations of the interfaces bound to the VPN instance.

The binding relationship between an interface and a VPN instance with a BFD session bound is removable using the **undo ip binding vpn-instance** command only after the bound BFD session is removed.

Example

Associate the VLANIF 10 interface with the VPN instance named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
```

```
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip binding vpn-instance vrf1
```

Associate the GE0/0/1 interface with the VPN instance named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip binding vpn-instance vrf1
```

10.4.35 ip frr (VPN instance view)

Function

The **ip frr** command enables IP FRR of a private network in the VPN instance IPv4 address family view.

The **undo ip frr** command disables IP FRR of a private network in the VPN instance IPv4 address family view.

By default, IP FRR of a private network is disabled in the VPN instance IPv4 address family view.

Format

ip frr route-policy *route-policy-name*

undo ip frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Enables IP FRR for the private routes matching the specified route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the development of the network, services such as audio, online video, and finance have more requirements for real time. Generally, active/standby links are deployed on the network to ensure service stability.

However, under traditional forwarding modes, when multiple routes to the same destination exist, the system selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, the system waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ip frr** command, you can enable IP FRR of the private network. IP FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv4 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

You are advised to use the **route-policy** command to create Route-Policy at first, in which the **apply backup-interface** command and the **apply backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv4 route of the private network.

The **ip frr** command should be used with the **apply backup-interface** command and the **apply backup-nexthop** command.

- To configure IP FRR for a private network, you need to run the **route-policy** command to create Route-Policy first. Then set a backup outbound interface and next hop for IPv4 routes of the private network using the **apply backup-interface** and **apply backup-nexthop** commands.
- To configure IP+VPN hybrid FRR, you need to run the **route-policy** command to create Route-Policy first. Then set a backup next hop for IPv4 routes of the private network using the **apply backup-nexthop** command.

NOTE

The differences between the IP FRR configuration and IP+VPN hybrid FRR configuration is as follows:

- If the backup next hop and the backup outgoing interface are specified at the same time, the configurations are for IP FRR.
- If only the backup next hop is specified, the configurations are for IP+VPN hybrid FRR. Based on the backup next hop, a matched VPNv4 route from another PE is found. Then a hybrid FRR entry is formed according to the fields of Token, BackupToken, and Label in the route.
- It is invalid to only specify the backup outgoing interface.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance view will not interfere each other.

Example

Specify a backup outbound interface and a backup next hop in route-policy **ip_frr_rp** and enable IP FRR for private routes in the VPN instance view.

```
<HUAWEI> system-view
[HUAWEI] route-policy ip_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-interface vlanif 100
[HUAWEI-route-policy] apply backup-nexthop 192.168.20.2
[HUAWEI-route-policy] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ip frr route-policy ip_frr_rp
```

10.4.36 ipv6 frr (VPN instance IPv6 address family view)

Function

The **ipv6 frr** command enables IPv6 FRR of the private network in the VPN instance IPv6 address family view.

The **undo ipv6 frr** command disables IPv6 FRR of the private network.

By default, IPv6 FRR of the private network is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.

Format

ipv6 frr route-policy *route-policy-name*

undo ipv6 frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the Route-Policy used by IPv6 FRR.	The name must be unique. The value is a string of 1 to 40 case-sensitive characters.

Views

VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the development of the network, services such as audio, online video, and finance have more requirements for real time. Generally, active/standby links are deployed on the network to ensure service stability.

However, under traditional forwarding modes, when multiple routes to the same destination exist, the system selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, the system waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ipv6 frr** command enables IPv6 FRR of the private network. IPv6 FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv6 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

The **ipv6 frr** command should be used with the **apply ipv6 backup-interface** command and the **apply ipv6 backup-nexthop** command. You are advised to use the **route-policy** command to create Route-Policy at first, in which the **apply ipv6 backup-interface** command and the **apply ipv6 backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv6 route of the private network.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance IPv6 address family view will not interfere each other.

Example

Specify a backup next hop in the Route-Policy named ipv6_frr_rp. Enable IPv6 FRR of the private network in the VPN instance IPv6 address family view.

```
<HUAWEI> system-view
[HUAWEI] route-policy ipv6_frr_rp permit node 10
[HUAWEI-route-policy] apply ipv6 backup-interface GigabitEthernet1/0/0
[HUAWEI-route-policy] apply ipv6 backup-nexthop 2001:db8:1::1
[HUAWEI-route-policy] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv6-family
[HUAWEI-vpn-instance-vpn1-af-ipv6] route-distinguisher 100:100
[HUAWEI-vpn-instance-vpn1-af-ipv6] ipv6 frr route-policy ip_frr_rp
```

10.4.37 ip vpn-instance

Function

The **ip vpn-instance** command creates a VPN instance and displays the VPN instance view.

The **undo ip vpn-instance** command deletes a specified VPN instance.

By default, no VPN instance is configured.

Format

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When private network data needs to travel across a public network, you need to configure a VPN instance on the PE of the public network. The public network mentioned here is an MPLS backbone network.

A multi-VPN-instance CE (MCE) device can connect to multiple VPNs. The MCE solution isolates services of different VPNs while reducing cost of network devices. Before configuring an MCE device, configure a VPN instance on the MCE device.

VPN instances are required for all L3VPN configurations.

Precautions

After the ip vpn-instance command is run, a virtual routing table is created on the PE or MCE and consumes resources on the PE or MCE.

After the **undo ip vpn-instance** command is used to delete a VPN instance, all configurations of this VPN instance are deleted.

A VPN instance with a BFD session bound can be deleted using the **undo ip vpn-instance** command only after the bound BFD session is deleted.

When you run the **undo ip vpn-instance** command to delete the VPN instance, if this instance is specified by the **source ip** (NETCONF view) command, you need to delete the bound VPN instance using the **undo source ip** (NETCONF view) command, and then delete the VPN instance.

Follow-up Procedure

After creating a VPN instance, perform the following configurations in the VPN instance view:

- Enable the IPv4 or IPv6 address family for the VPN instance. A VPN instance supports both the IPv4 and IPv6 address families. You need to run the **ipv4-family (VPN instance view)** or **ipv6-family (VPN instance view)** command to enable the IPv4 or IPv6 address family based on the type of the protocol stack used to advertise VPN routes in the VPN instance.

- Configure an RD for the IPv4 address family of the VPN instance. You are allowed to perform VPN configurations in the address family view only after using the **route-distinguisher** command to configure an RD for the address family.
- Configure a VPN target for the VPN instance using the **vpn-target** command. The VPN target controls route learning between VPN instances.
- Bind the VPN instance to the PE or MCE interface connected to the VPN using the **ip binding vpn-instance** command. After an interface is bound to a VPN instance, the interface becomes a part of the VPN. Packets entering the interface will be forwarded based on the VRF table of the VPN.

Example

Create a VPN instance named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1]
```

10.4.38 ipv4-family (VPN instance view)

Function

The **ipv4-family** command enables the IPv4 address family for a VPN instance and displays the VPN instance IPv4 address family view.

The **undo ipv4-family** command disables the IPv4 address family for a VPN instance.

By default, VPN instances are disabled with the IPv4 address family.

Format

ipv4-family

undo ipv4-family

Parameters

None.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv4-family** command to enable the IPv4 address family for the VPN instance. You can then perform VPN configurations in the address family view to advertise IPv4 VPN routes and allow IPv4 VPN data to be forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv4 address family of the VPN instance. Before performing VPN configurations in the IPv4 address family view, configure an RD for the IPv4 address family of the VPN instance.

Precautions

Configurations of the commands run in the VPN instance view, except the **description** and **service id** command, are automatically synchronized to the VPN instance IPv4 address family view.

The IPv4 address family for a VPN instance with a BFD session bound can be disabled using the **undo ipv4-family** command only after the bound BFD session is deleted.

Example

Enable the IPv4 address family for a VPN instance.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4]
```

10.4.39 ipv6-family (VPN instance view)

Function

The **ipv6-family** command enables the IPv6 address family for a VPN instance and displays the VPN instance IPv6 address family view.

The **undo ipv6-family** command disables the IPv6 address family for a VPN instance.

By default, the IPv6 address family is disabled for a VPN instance.

Format

ipv6-family

undo ipv6-family

Parameters

None

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IPv6 VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv6-family** command to enable the IPv6 address family for the VPN instance and perform VPN configurations in the address family view if you want to have IPv6 VPN routes advertised and IPv6 VPN data forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv6 address family of the VPN instance. VPN configurations can be performed in the IPv6 address family view only after an RD is configured for the IPv6 address family of the VPN instance.

Precautions

The IPv6 address family for a VPN instance with a BFD session bound can be disabled using the **undo ipv6-family** command only after the bound BFD session is deleted.

Example

Enable the IPv6 address family for the VPN instance named vrf1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv6-family
[HUAWEI-vpn-instance-vrf1-af-ipv6]
```

10.4.40 limit-log-interval

Function

The **limit-log-interval** command configures the interval for displaying logs when the number of routes exceeds the threshold.

The **undo limit-log-interval** command restores the default setting.

By default, the interval for displaying logs when the number of routes exceeds the threshold is 5 seconds.

Format

limit-log-interval *interval*

undo limit-log-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for displaying logs when the number of routes exceeds the threshold.	An integer ranging from 1 to 60, in seconds.

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the routes or prefixes in the IPv4 or IPv6 address family of a VPN instance reach the maximum, the system will generate logs at intervals (defaulting to 5 seconds). To prevent logs from being displayed frequently, run the **limit-log-interval** command to prolong the interval of log generation.

The maximum number of routes or prefixes that the IPv4 or IPv6 address family of a VPN instance supports can be configured using the **routing-table limit** or **prefix limit** command.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to create a VPN instance and enter the VPN instance IPv4 or IPv6 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

If a log is generated to record the event that routes or prefixes in the IPv4 or IPv6 address family of a VPN instance reach the maximum, no more routes can be added to the routing table of the IPv4 or IPv6 address family of the VPN instance. Instead, the routes will be discarded.

Example

Set the interval for displaying logs to 8 seconds when the number of routes in the IPv4 address family of the VPN instance named vpn1 exceeds the threshold.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] limit-log-interval 8
```

10.4.41 mpls te reserved-for-binding

Function

The **mpls te reserved-for-binding** command reserves an MPLS TE tunnel for VPN binding.

The **undo mpls te reserved-for-binding** command removes the configuration.

By default, an MPLS TE tunnel can be selected based on any type of tunnel policy.

Format

mpls te reserved-for-binding

undo mpls te reserved-for-binding

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN has high requirements for bandwidth, you can apply a tunnel binding policy to the VPN to have the routes of the VPN recursing to MPLS TE tunnels. Before applying that tunnel binding policy to the VPN, you need to run the **mpls te reserved-for-binding** command to reserve MPLS TE tunnels for VPN binding.

Prerequisites

MPLS TE tunnels are available in the system.

Configuration Impact

After the **mpls te reserved-for-binding** command is configured on an MPLS TE tunnel, the tunnel can be selected based on a tunnel binding policy only. Even if no tunnel binding policy is configured, a tunnel type prioritizing policy created using the **tunnel select-seq** command will not select the MPLS TE tunnel for which the **mpls te reserved-for-binding** command has been configured.

Follow-up Procedure

Run the **tunnel-policy** command to create a tunnel policy and the **tunnel binding** command to bind the policy to the MPLS TE tunnel.

Example

Reserve Tunnel1 for VPN binding.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] mpls te reserved-for-binding
```

Delete the configuration of a tunnel that is reserved for VPN binding.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo mpls te reserved-for-binding
```

10.4.42 nd vpn-cross enable

Function

The **nd vpn-cross enable** command enables direct ND entry delivery for mutual access between IPv6 VPNs.

The **undo nd vpn-cross enable** command disables direct ND entry delivery for mutual access between IPv6 VPNs.

By default, direct ND entry delivery for mutual access between IPv6 VPNs is disabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6720S-EI, S6720-EI, S6730-S, S6730S-S, and S6730-H support this command.

Format

nd vpn-cross enable

undo nd vpn-cross enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario of mutual access between IPv6 VPNs, traffic initiated during mutual access for the first time will trigger ND Miss messages and ND entry learning. If a PE device fails to process the ND Miss messages in time (for example, when a new card is installed), mutual access traffic between the VPNs cannot be transmitted.

After direct ND entry delivery for mutual access between IPv6 VPNs is enabled on the PE device, the device delivers ND entries in advance when a new card is installed without the need to trigger mutual access traffic. This ensures proper transmission of mutual access traffic between local VPNs.

Precautions

After direct ND entry delivery for mutual access between IPv6 VPNs is enabled, the ND entries delivered by the device in advance will consume some ND entry resources. Therefore, configure this function only when required.

Example

Enable direct ND entry delivery for mutual access between IPv6 VPNs.

```
<HUAWEI> system-view
[HUAWEI] nd vpn-cross enable
Warning: After this function is enabled, a large number of ND entries will be occupied.
```

10.4.43 peer default-originate vpn-instance

Function

The **peer default-originate vpn-instance** command configures BGP to advertise all default routes related to the specified VPN instance to the specified VPNv4 peer or peer group.

The **undo peer default-originate vpn-instance** command removes the configuration.

By default, BGP does not advertise its default route to the VPNv4 peer or peer group.

Format

peer { *ipv4-address* | *group-name* } **default-originate vpn-instance** *vpn-instance-name*

undo peer { *ipv4-address* | *group-name* } **default-originate vpn-instance** *vpn-instance-name*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HoVPN refers to a hierarchical VPN, with multiple PEs functioning as different roles to form a hierarchical architecture and provide functions of a single PE. In this manner, the performance requirement on PEs is lowered. If the **peer default-originate vpn-instance** command is used, SPE sends the default route with the address of the next hop as the local address, regardless of whether there is a default route in the local routing table. The UPE then only needs to maintain the local VPN routes, whereas all remote routes are replaced by the default route. The workload of the UPE is reduced.

Precautions

If an SPE does not have an active default route, either of the following methods can be used to generate a default route on the SPE and allow the SPE to advertise the route to the UPE:

- Method 1: Run the **peer default-originate vpn-instance** command to enable the SPE to automatically generate a default route and advertise it to the UPE.
- Method 2: Run the **ip route-static vpn-instance** command to configure a default route on the SPE, run the **default-route imported** command to enable the SPE to import the default route to the BGP routing table, and then run the **import-route static** or **network** command in the BGP-VPN instance IPv4 address family view to import the default route to the BGP IPv4 VPN instance routing table.

Either of the preceding methods can be used to advertise a default route to the UPE. The priority of the default route generated through method 1 is higher than that generated through method 2. If method 1 is used, the default route generated through method 2 will be suppressed, and no Update messages will be sent for a route change or withdrawal. If the SPE has an active default route, the SPE can advertise the route to the UPE without the need for either of the preceding methods.

Example

Advertise default routes of vpn1 to VPNv4 peer 1.1.1.1.

```
<HUAWEI> system-view
```

```
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 1.1.1.1 as-number 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.1 enable
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.1 upe
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.1 default-originate vpn-instance vpn1
```

10.4.44 peer mpls-local-ifnet disable

Function

The **peer mpls-local-ifnet disable** command disables EBGP peers from establishing an MPLS local ifnet tunnel between them.

The **undo peer mpls-local-ifnet disable** command enables EBGP peers to establish an MPLS local ifnet tunnel between them.

By default, EBGP peers can automatically establish MPLS local ifnet tunnels between them if one of the following conditions is met:

- EBGP peers are enabled to exchange labeled routes.
- EBGP peers are configured in the BGP-VPLS address families.
- EBGP peers are configured in the BGP-VPNv4 or BGP-VPNv6 address family.

Format

peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

undo peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	The value is in dotted decimal notation.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS local ifnet tunnel: In inter-AS VPN Option B or Option C scenarios, the VPN routes with L2VPN label block information that ASBRs advertise to BGP peers must contain public-network tunnel information. However, no tunnels are configured between ASBRs. To allow EBGP routes to be advertised to IBGP peers, an MPLS local ifnet tunnel is generated between MPLS interfaces of ASBRs.

In the L3VPN over inter-as seamless MPLS or VPLS scenario, EBGP peer relationships are established between BGP peers. The BGP peers can be endpoint PEs in the VPLS scenario or the CSG and MASG in the inter-AS seamless MPLS scenario. These EBGP peers automatically establish MPLS local ifnet tunnels between them. The E2E MPLS local ifnet tunnel fails to transmit traffic if the two peers are indirectly connected.

If a fault occurs on a tunnel between the two EBGP peers, the route recurses to the MPLS local ifnet tunnel, not an FRR bypass tunnel. As the MPLS local ifnet tunnel cannot forward traffic, traffic is interrupted. To prevent the traffic interruption, run this command to disable the establishment of an MPLS local ifnet tunnel between the EBGP peers.

Prerequisites

The EBGP peer relationship must be in the Established between PEs.

Example

Disable EBGP peers from establishing an MPLS local ifnet tunnel.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 10.1.1.1 as-number 200
[HUAWEI-bgp] peer 10.1.1.1 mpls-local-ifnet disable
```

10.4.45 peer upe

Function

The **peer upe** command specifies a BGP peer or peer group as UPE of HoVPN.

The **undo peer upe** command cancels the configuration.

Format

peer { *group-name* | *ipv4-address* } **upe**

undo peer { *group-name* | *ipv4-address* } **upe**

Parameters

Parameter	Description	Value
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	-

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a UPE is specified on the SPE through the **peer upe** command, the SPE does not send a specific route to the UPE. If the **peer route-policy export** command is run on the SPE to configure routing policies for the UPE and certain specific routes can pass the filtration of routing policies, these specific routes can be sent to the UPE.

Prerequisites

Before you run the peer upe command, the **peer as-number** command should be used to create a peer or peer group.

Precautions

The BGP peer relationship is interrupted after you run the **peer upe** command. So, confirm the action before you use the command.

If an SPE does not have an active default route, either of the following methods can be used to generate a default route on the SPE and allow the SPE to advertise the route to the UPE:

- Method 1: Run the **peer default-originate vpn-instance** command to enable the SPE to automatically generate a default route and advertise it to the UPE.
- Method 2: Run the **ip route-static vpn-instance** command to configure a default route on the SPE, run the **default-route imported** command to enable the SPE to import the default route to the BGP routing table, and then run the **import-route static** or **network** command in the BGP-VPN instance IPv4 address family view to import the default route to the BGP IPv4 VPN instance routing table.

Either of the preceding methods can be used to advertise a default route to the UPE. The priority of the default route generated through method 1 is higher than that generated through method 2. If method 1 is used, the default route generated through method 2 will be suppressed, and no Update messages will be sent for a route change or withdrawal. If the SPE has an active default route, the SPE can advertise the route to the UPE without the need for either of the preceding methods.

Follow-up Procedure

After the **peer upe** command is configured, to send the default route 0.0.0.0 to the UPE, you need to run the **peer default-originate vpn-instance** command on the SPE.

Example

Specify the peer 1.1.1.2 as UPE.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 1.1.1.2 as-number 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.2 enable
[HUAWEI-bgp-af-vpnv4] peer 1.1.1.2 upe
```

10.4.46 peer soo

Function

The **peer soo** command configures the Site of Origin (SoO) attribute for an EBGP peer in a BGP VPN instance.

The **undo peer soo** command deletes the SoO.

By default, no SoO attribute is configured for an EBGP peer in a BGP VPN instance.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo** *site-of-origin*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The address is in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
Site-of-origin	Specifies the SoO attribute, which is a BGP extended community attribute and can be expressed in any of the following formats: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a SoO cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0.0:0.	-

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. As a result, different sites of the same VPN cannot communicate. The **peer substitute-**

as command can be used to enable AS number substitution on PEs to address this problem.

Enabling AS number substitution will cause another problem. Several CEs at a VPN site may establish EBGP connections with different PEs of a BGP/MPLS IP VPN backbone network, and a routing protocol has been configured on the CEs. If AS number substitution is enabled on PEs, the AS numbers carried by VPN routes of this site will be replaced on the PEs. As a result, routes advertised from a CE to a PE may be re-advertised to this VPN site after the routes traverse the backbone network, causing a routing loop. The **peer soo** command can be run on the PEs to address this problem.

After the **peer soo** command is run on a PE to configure the SoO attribute for a specified CE, the PE adds the attribute to a route sent from the CE and advertises the route to the remote PE. The remote PE checks the SoO attribute of the route before sending it to its attached CE. If the SoO attribute is the same as the local SoO attribute on the remote PE, the remote PE does not send the route to its attached CE, preventing a routing loop in a VPN site.

Precautions

The **peer soo** command is used only in the scenarios where PEs and CEs establish EBGP peer relationships.

Example

Configure the SoO attribute for EBGP peers in a BGP VPN instance.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] peer 192.168.15.2 soo 10.2.2.2:45
```

10.4.47 peer substitute-as

Function

The **peer substitute-as** command enables AS number substitution. This command enables a device to replace the AS number of the peer specified in the AS_Path attribute with the local AS number.

The **undo peer substitute-as** command disables AS number substitution.

By default, AS number substitution is disabled.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **substitute-as**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **substitute-as**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The address is in the format of X:X:X:X:X:X:X:X.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. If a CE in a VPN site sends a VPN route to the connected PE using EBGP and the PE then sends the route to the remote PE, the remote CE will discard the route because the AS number carried by the route is the same as the local AS number. As a result, different sites of the same VPN cannot communicate. The **peer substitute-as** command can be used on the PE to enable AS number substitution to address this problem. After that, the PE replaces the AS number carried in the VPN route with the local AS number. As a result, the remote CE will not discard the route due to identical AS numbers.

Pre-configuration Tasks

Run the **peer as-number** command to create a peer or configure an AS number for a specified peer group.

Example

Configure a device to replace the AS number of a specified peer in the AS_Path of a route with the local AS number.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpn1
```

```
[HUAWEI-bgp-vpn1] peer 10.1.1.2 as-number 200
[HUAWEI-bgp-vpn1] peer 10.1.1.2 substitute-as
```

10.4.48 policy vpn-target

Function

The **policy vpn-target** command configures a device to implement VPN target-based filtering for received routes.

The **undo policy vpn-target** command cancels VPN target-based filtering.

By default, the VPN-Target filtering is enabled.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-MDT address family view, BGP-MVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the networking of BGP/MPLS IP VPN, Kompella VLL, and Kompella VPLS, VPN target attributes are used to filter received VPN routes or label blocks. If VPN target attributes are not configured, received VPN routes or label blocks are discarded.

VPNs and VPN target attributes are not configured on the following devices in certain networking scenarios:

- RRs in BGP/MPLS IP VPN, Kompella VPLS, or Kompella VLL
- ASBRs (not functioning as PEs) in inter-AS BGP/MPLS IP VPN OptionB

In this case, VPN routes or label blocks are not saved on the RRs or ASBRs.

The RRs or ASBRs, however, need to save all VPN routes or label blocks sent from PEs. Therefore, the **undo policy vpn-target** command can be configured on the RRs or ASBRs to disable the filtering of VPN routes or label blocks.

Precautions

Running the **undo policy vpn-target** makes all VPN routes or label blocks from PEs received. Therefore, this command is configured only on devices of particular roles (RRs or ASBRs)

Example

Configure a device to implement VPN target-based filtering for received VPNv4 routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] policy vpn-target
```

10.4.49 prefix limit

Function

The **prefix limit** command sets a limit on the maximum number of prefixes supported in the existing VPN instance address family, preventing the PE from importing excessive VPN route prefixes.

The **undo prefix limit** command restores the default setting.

By default, the maximum number of VPN route prefixes is not limited.

Format

prefix limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo prefix limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of prefixes supported in the VPN instance address family.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.

Parameter	Description	Value
alert-percent	Specifies the proportion of the alarm threshold to the maximum number of prefixes. When the number of prefixes in the VPN instance address family exceeds *number* x *alert-percent*/100, alarms are displayed. The VPN route prefixes, however, can still join the VPN routing table. When the number of the prefixes exceeds the *number*, the subsequent prefixes are discarded.	The value is an integer ranging from 1 to 100.
route-unchanged	Indicates that the routing table remains unchanged. By default, **route-unchanged** is not configured. When the number of prefixes in the routing table is greater than the value of the parameter number, routes are processed as follows: ● If **route-unchanged** is configured, routes in the routing table remain unchanged. ● If **route-unchanged** is not configured, all routes in the routing table are deleted and then re-added.	-
simply-alert	Indicates that when the number of VPN route prefixes exceeds *number*, prefixes can still join the VPN routing table and alarms are displayed. On the device, however, the subsequent VPN route prefixes are discarded after the total number of the unicast prefixes of the private network and the public network reaches the upper limit.	-

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many useless route prefixes imported into a VPN instance constitute a large proportion of the route prefixes on a device, run the **prefix limit** command to set a limit on the maximum number of prefixes supported by the VPN instance. After the **prefix limit** command is run in the current VPN instance address family, if the number of route prefixes reaches the set limit, the system will generate an alarm to instruct the user to check the validity of route prefixes of the VPN instance.

The **prefix limit** command enables the system to display a message when the number of route prefixes added to the routing table of the VPN instance IPv6 address family exceeds the limit. If you run the **prefix limit** command to increase the maximum number of route prefixes in the VPN instance IPv6 address family or run the **undo prefix limit** command to cancel the limit, the system adds the excess route prefixes to the VPN IP routing table.

When the number of route prefixes exceeds the limit, direct routes and static routes can still be added to the routing table of the VPN instance IPv6 address family.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The **prefix limit** command can prevent the routing table of the current VPN instance address family on a PE from importing too many route prefixes, but cannot prevent the PE from importing excessive route prefixes from other PEs. Therefore, configuring both the **prefix limit** and **peer route-limit** commands is recommended.

Do not run both the **routing-table limit** (the command restricts the number of routes) and **prefix limit** (the command restricts the number of route prefixes) commands in the current VPN instance address family. Configure either one of them based on your need.

Example

Configure the system to only generate alarms when the number of prefixes exceeds the maximum number 1000 in the VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] prefix limit 1000 simply-alert
```

10.4.50 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.

By default, no RD is configured for the VPN instance address family.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD. The forms of RD are as follows: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view, EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a VPN instance and enabling the IPv4 or IPv6 address family for the VPN instance, you need to run the **route-distinguisher** command to configure an RD for the address family.

Different VPN instances may have the same route prefix. To allow a PE to determine to which VPN instance a route belongs, run the **route-distinguisher** command to configure an RD for an address family of a VPN instance on the PE. After the configuration, the PE will add an RD to the route received from the VPN instance, and then the route prefix becomes a globally unique VPNv4 or VPNv6 route.

Configuration Impact

An RD configured for the IPv4 or IPv6 address family of a VPN instance cannot be directly modified or deleted. Before modifying an RD, you need to disable the IPv4 or IPv6 address family of the VPN instance or delete the VPN instance and then reconfigure the address family or the VPN instance.

Precautions

Configuring a unique RD for the IPv4 or IPv6 address family of a VPN instance is recommended; otherwise, route overlap may occur.

When the **route-distinguisher** command is run in the VPN instance view, an **ipv4-family** command is created at the same time by default. The command results are equivalent to running the **ipv4-family** command in the VPN instance view and then running the **route-distinguisher** command in the VPN instance IPv4 address family view. For example:

```
[HUAWEI-vpn-instance-vpn1] route-distinguisher 200:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] display this
#
 ipv4-family
  route-distinguisher 200:1
#
return
```

Example

Configure an RD for the VPN instance named **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 22:1
```

10.4.51 routing-table limit

Function

The **routing-table limit** command sets the maximum number of routes that the current VPN instance address family supports.

The **undo routing-table limit** command restores the maximum number of routes that the current VPN instance address family can support to the default setting.

By default, there is no limit on the maximum number of routes that the current VPN instance address family can support, but the total number of private network and public network routes on a device cannot exceed the allowed maximum number of unicast routes.

Format

routing-table limit *number* { *alert-percent* | **simply-alert** }

undo routing-table limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of routes supported by a VPN instance.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of routes. When the maximum number of routes that join the VPN instance is up to the value (*number***alert-percent*)/100, the system prompts alarms. The VPN routes can be still added to the routing table, but after the number of routes reaches *number*, the subsequent routes are dropped.	An integer ranging from 1 to 100.
simply-alert	Indicates that when VPN routes exceed *number*, routes can still be added into the routing table, but the system prompts alarms. However, after the total number of VPN routes and network public routes reaches the unicast route limit specified in the License, the subsequent VPN routes are dropped.	-

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many useless routes imported into a VPN instance constitute a large proportion of the routes on a device, run the **routing-table limit** command to set a limit on the maximum number of routes supported by the VPN instance. After the **routing-table limit** command is run in the current VPN instance address family, if the number of routes of the VPN instance reaches the set limit, the system will generate an alarm to instruct the user to check the validity of routes of the VPN instance.

The **routing-table limit** command enables the system to display a message when the number of routes added to the routing table of the VPN instance IPv6 address family exceeds the limit. If you run the **routing-table limit** command to increase the maximum number of routes in the VPN instance IPv6 address family or run the **undo routing-table limit** command to cancel the limit, the system adds the excess routes to the VPN IP routing table.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to enter the IPv4 or IPv6 VPN instance address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

Using the **routing-table limit** command prevents the routing table of the current VPN instance address family on a PE from importing too many routes, but cannot prevent the PE from importing excessive routes from other PEs. Therefore, configuring both the **routing-table limit** and **peer route-limit** commands is recommended.

Do not run both the **routing-table limit** (the command restricts the number of routes) and **prefix limit** (the command restricts the number of route prefixes) commands in the current VPN instance address family. Configure either one of them based on your need.

If the remote cross routes learned using MP-IBGP and the BGP routes learned from CEs failed to be added to the routing table, the system automatically refreshes the routing table to add these routes.

Example

Configure the maximum number of routes for the IPv4 address family of the VPN instance named vpn1 to 1000, and when VPN routes exceed 1000, routes can still be added into the routing table, but the system prompts alarms.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] routing-table limit 1000 simply-alert
```

10.4.52 rr-filter

Function

The **rr-filter** command creates a reflection policy for the route reflectors.

The **undo rr-filter** command removes the configuration.

By default, no reflection policy for a route reflector is created.

Format

rr-filter { *extcomm-filter-number* | *extcomm-filter-name* }

undo rr-filter

Parameters

Parameter	Description	Value
extcomm-filter-number	specifies the number of the extended community filter supported by the route-reflector group. You can specify only one extended community filter each time.	It is an integer that ranges from 1 to 399.
extcomm-filter-name	specifies the name of the extended community filter supported by the route-reflector group. You can specify only one extended community filter each time.	The name is a string of 1 to 51 characters without any space. It is case-sensitive. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-MDT address family view, BGP-MVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Full-mesh connections need to be established between IBGP peers in an AS to ensure the connectivity between the IBGP peers. When there are many IBGP peers, it is costly to establish a fully-meshed network. An RR or a confederation can be used to solve the problem. Only the IBGP route of which route-target extended community attribute meets the matching rules can be reflected. This allows load balancing among RRs.

Example

Create a route-reflector group, and enable the automatic filtering for VPNv4 route updates on the outbound interface. The group should be created on the basis of the permitted route target extended community attributes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] rr-filter 10
```

10.4.53 service-id (VPN instance view)

Function

The **service-id** command sets a service ID for a VPN instance.

The **undo service-id** command deletes the service ID of a VPN instance.

By default, no service ID is set for a VPN instance.

Format

service-id *service-id*

undo service-id

Parameters

Parameter	Description	Value
service-id	Specifies the service ID of a VPN instance.	An integer ranging from 1 to 4294967295.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A service ID set in the view of a VPN instance identifies the service of the VPN instance, which facilitates later service query using the NMS.

A service ID is unique on a device. It distinguishes a VPN service from other VPN services on the network. A service ID used by a VPN instance cannot be allocated to other VPN instances.

Configuration Impact

If the **service-id** command is run repeatedly, the last configuration overrides the previous ones.

Example

Set a service ID for a VPN instance.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] service-id 123
```

10.4.54 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel. The following types of interfaces are often used: VLANIF and loopback.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, IPv4 over IPv6 or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the source address of the local tunnel interface is the destination address of the remote tunnel interface, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Example

Set the tunnel type of Tunnel1 to IPv6 over IPv4 of manual mode and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI-Tunnel1] source 10.1.1.1
```

Configure Tunnel1 of GRE and use Loopback1 address as the interface address.

```
<HUAWEI> system-view
[HUAWEI] interface Loopback 1
[HUAWEI-LoopBack1] ip address 10.2.1.1 32
[HUAWEI-LoopBack1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] source loopback 1
```

10.4.55 supernet label-route advertise

Function

The **supernet label-route advertise disable** command disables a BGP device from advertising BGP supernet labeled routes.

The **undo supernet label-route advertise disable** or **supernet label-route advertise enable** command restores the default configuration.

By default, BGP supernet labeled routes can be preferentially selected and advertised.

Format

supernet label-route advertise disable

supernet label-route advertise enable

undo supernet label-route advertise disable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP supernet route has the same destination address and next hop address or has a more detailed destination address than the next hop address. Any route that meets one of the following conditions is a BGP supernet route.

- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are the same, and the destination address mask is greater than or equal to the next hop address mask.
- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are different. However, if you perform bitwise AND operations on the next hop address mask with the destination address and next hop address, respectively, the calculated network addresses are the same.

For example, the route destined for 10.6.6.6 in the following command output is a BGP supernet route.

```
<HUAWEI> display bgp routing-table
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 1
       Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
   *>i  10.6.6.6/32        10.6.6.6       0          100       0      ?
```

Example

Disable a BGP device from advertising BGP supernet labeled routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] supernet label-route advertise disable
```

10.4.56 tunnel binding

Function

The **tunnel binding** command binds a specified tunnel to the destination IP address. Therefore, the tunnel can be used by a specified VPN.

The **undo tunnel binding** command cancels the binding.

By default, a tunnel is not bound to any IP address.

Format

tunnel binding destination *dest-ip-address* **te** { **tunnel** *interface-number* } &<1-6> [**ignore-destination-check**] [**down-switch**]

undo tunnel binding destination *dest-ip-address*

Parameters

Parameter	Description	Value
dest-ip-address	Specifies the destination address of the tunnel.	-
interface-number	Specifies the interface number of the bound tunnel interface.	-
ignore-destination-check	Specifies whether to ignore destination consistency check. If this parameter is enabled, a tunnel policy selects a TE tunnel for route recursion even if the destination address of that TE tunnel is different from the destination address specified in the tunnel policy.	-
down-switch	Indicates that the tunnel switchover is enabled. After this parameter is configured, an available tunnel, with the priority as LSP, CR-LSP, is adopted when the bound TE tunnel fails.	-

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A tunnel policy determines the selection of proper tunnels for VPN services. There are two types of tunnel policies. Only one policy type can be configured in the tunnel policy view.

- Tunnel type prioritizing policy: Such a policy specifies the sequence in which different types of tunnels are selected. The **tunnel select-seq** command is used to configure a tunnel type prioritizing policy.
- Tunnel binding policy: Such a policy binds a tunnel to a VPN for service transmission. The **tunnel binding** command is used to configure a tunnel binding policy.

Only MPLS TE tunnels can be bound to VPNs. The **tunnel binding** command can specify the MPLS TE tunnels that are used for VPN binding, facilitating QoS deployment. If some VPN services have high requirements for QoS, run the **tunnel binding** command to use specific MPLS TE tunnels to transmit these VPN services.

Prerequisites

The **tunnel-policy** command is run to create a tunnel policy.

The **mpls te reserved-for-binding** command is run in the view of the tunnel interface to be bound to an MPLS TE tunnel.

Precautions

The **tunnel binding** command can be run repeatedly in the tunnel policy view so long as the value of *dest-ip-address* varies.

Apply the tunnel binding policy to the VPN instance so that the VPN instance can have its routes recursing to the bound MPLS TE tunnel.

Example

Bind the IP address of the remote PE, 10.2.2.9, to the local tunnel interface Tunnel1 in the tunnel policy view.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy tnlpolicyname
[HUAWEI-tunnel-policy-tnlpolicyname] tunnel binding destination 10.2.2.9 te tunnel 1
```

10.4.57 tunnel-selector (system view)

Function

The **tunnel-selector** command creates a tunnel selector and displays the tunnel selector view.

The **undo tunnel-selector** command cancels the setting.

By default, no tunnel selector is created.

Format

tunnel-selector *tunnel-selector-name* { **permit** | **deny** } **node** *node*

undo tunnel-selector *tunnel-selector-name* [**node** *node*]

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel selector.	The value is a string of 1 to 40 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
permit	Specifies the matching mode of the tunnel selector to **permit**. If a route matches all the **if-match** clauses of a node, the route matches the node and all the actions defined by the **apply** clause are performed on the route. If a route does not match one **if-match** clause of a node, the route continues to match the next node.	-
deny	Specifies the matching mode of the tunnel selector to **deny**. If a route matches all the **if-match** clauses of a node, the route is denied and does not match the next node.	-
node *node*	Specifies the index of the node of the tunnel selector. The route first matches the node with a smaller index value.	The value is an integer ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **tunnel-selector** command is often used in BGP/MPLS IP VPN networking. A tunnel selector needs to be created in the following scenarios:

- The SPE in the HVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.

Follow-up Procedure

Configure the following clauses after creating a tunnel selector (each node of the tunnel selector consists of two parts):

- **if-match** clause: sets filtering conditions on a node. To filter routes by RD, run the **if-match rd-filter** command. To filter routes by next hop, run the **if-match ip next-hop** command.
- **apply** clause: applies a tunnel policy to the routes filtered by the **if-match** clause using the **apply tunnel-policy** command.

In addition, the system will have routes recursing to expected tunnels only after applying a tunnel selector. The **tunnel-selector** command can be run in the BGP view for the application of a tunnel selector.

Precautions

A change in the tunnel selector may cause VPN services to be interrupted because BGP-VPNv4 or BGP labeled routes may fail to recurse to tunnels.

Example

Create a tunnel selector named tps, and set the node number to 10 and the matching mode to **permit**.

```
<HUAWEI> system-view
[HUAWEI] tunnel-selector tps permit node 10
[HUAWEI-tunnel-selector]
```

10.4.58 tunnel-selector (BGP-VPNv4 address family view)

Function

The **tunnel-selector** command applies a tunnel selector to BGP-VPNv4 or BGP labeled routes.

The **undo tunnel-selector** command cancels the configuration.

By default, no tunnel selector is applied to BGP-VPNv4 or BGP labeled routes. BGP-VPNv4 or BGP labeled route recurse only to LSPs.

Format

tunnel-selector *tunnel-selector-name*

undo tunnel-selector

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel policy selector.	The value is a string of 1 to 40 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **tunnel-selector** command is often used in BGP/MPLS IP VPN networking. It can be used in the following scenarios to apply a tunnel selector to BGP-VPNv4 or BGP labeled routes:

- The SPE in the HVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.

Prerequisites

The **tunnel-selector** command is run to create a tunnel selector.

Precautions

Deleting the tunnel selector applied to BGP-VPNv4 or BGP labeled routes may cause VPN service interruption because the BGP-VPNv4 or BGP labeled routes may fail to recurse to tunnels.

Example

Apply a tunnel selector to BGP labeled routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpnv4
[HUAWEI-bgp-af-vpnv4] tunnel-selector tps
```

10.4.59 tunnel select-seq

Function

The **tunnel select-seq** command specifies the priority sequence of the tunnels taking part in load balancing.

The **undo tunnel select-seq load-balance-number** command restores the default setting.

By default, only LDP LSPs, BGP LSP or static LSPs are selected and no load balancing is performed.

Format

tunnel select-seq { **gre** | **lsp** | **cr-lsp** } * **load-balance-number** *load-balance-number*

undo tunnel select-seq

Parameters

Parameter	Description	Value
gre	Specifies a GRE tunnel. **NOTE** This parameter is not supported in this version.	-

Parameter	Description	Value
lsp	Specifies the LDP LSPs, BGP LSP or static LSPs. **NOTE** This parameter is not supported by the S5731S-S, S6730S-S, and S6735-S.	-
cr-lsp	Specifies the CR-LSP tunnel. **NOTE** This parameter is not supported by the S5731S-S, S6730S-S, and S6735-S.	-
load-balance-number	Specifies the number of tunnels taking part in load balancing.	The value is an integer that ranges from 1 to 6.

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

Precautions

A tunnel policy determines the selection of proper tunnels for VPN services. There are two types of tunnel policies.

- Tunnel type prioritizing policy: Such a policy specifies the sequence in which different types of tunnels are selected. The **tunnel select-seq** command is used to configure a tunnel type prioritizing policy.
- Tunnel binding policy: Such a policy binds a tunnel to a VPN for service transmission. The **tunnel binding** command is used to configure a tunnel binding policy.

If the **tunnel select-seq** command is run, the VPN instance preferably selects the tunnel type with the highest priority according to the specified sequence. For example, after the **tunnel select-seq cr-lsp lsp load-balance-number 2** command is run in the tunnel policy view, the VPN instance will select CR-LSPs to transmit services on the backbone network.

- If two or more CR-LSPs are available on the network, the VPN instance randomly selects two of them for service transmission.
- If no CR-LSP or only one CR-LSP is available on the network, the VPN instance selects LSPs as substitutes with the existing CR-LSP for service transmission.
- If the number of tunnels used by the VPN instance is reduced to 1, the VPN instance uses the tunnel policy to re-select tunnels.

If **lsp** is specified in the command, three types of LSPs can serve as candidate tunnels: LDP LSP, BGP LSP, and static LSP. The priority sequence of these LSPs taking part in load balancing is LDP LSP > BGP LSP > static LSP. For example, if the **tunnel select-seq lsp cr-lsp load-balance-number 3** command is configured for the tunnel policy:

- If three or more LDP LSPs are available on the network, the VPN instance randomly selects three of them for service transmission.
- If less than three LDP LSPs are available on the network, the VPN instance selects BGP LSPs as substitutes to ensure that three LSPs work in load balancing mode to transmit services.
- If the total number of LDP and BGP LSPs available on the network is less than 3, the VPN instance selects static LSPs as substitutes to ensure that three LSPs work in load balancing mode to transmit services.

After the **tunnel select-seq** command is executed, apply the configured tunnel policy to the VPN instance so that the VPN instance can select tunnels based on the tunnel policy and have its services load-balanced across tunnels.

The load balancing mode configured using the **tunnel select-seq** command in a tunnel policy takes effect only for L3VPN.

Example

Configure a tunnel policy that only LDP LSPs, BGP LSP or static LSPs can be used and no load balancing is performed.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy l2
[HUAWEI-tunnel-policy-l2] tunnel select-seq lsp load-balance-number 1
```

10.4.60 tunnel-policy nonexistent-config-check

Function

The **tunnel-policy nonexistent-config-check** command configures whether a nonexistent tunnel policy can be specified in a command.

The **undo tunnel-policy nonexistent-config-check disable** command configures only an existing tunnel policy can be specified in a command.

By default, only an existing tunnel policy can be specified in a command.

Format

tunnel-policy nonexistent-config-check { **disable** | **enable** }

undo tunnel-policy nonexistent-config-check disable

Parameters

Parameter	Description	Value
disable	Indicates that a nonexistent tunnel policy can be specified in a command.	-
enable	Indicates that only an existing tunnel policy can be specified in a command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if you specify a nonexistent tunnel policy in a command, the command does not take effect.

If you need the nonexistent tunnel policy can be specified in a command, run the **tunnel-policy nonexistent-config-check disable** command.

Example

# Indicates that a nonexistent tunnel policy can be specified in a command.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy nonexistent-config-check disable
```

10.4.61 tunnel-policy (system view)

Function

The **tunnel-policy** command creates a tunnel policy and displays the tunnel policy view.

The **undo tunnel-policy** command deletes the specified tunnel policy.

By default, no tunnel policy is created in the system.

Format

tunnel-policy *policy-name*

undo tunnel-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Displays the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance selects LSPs without performing load balancing based on the default tunnel policy. If you want to make a change, run the **tunnel-policy** command to create a tunnel policy.

There are two types of tunnel policies:

- Tunnel type prioritizing policy: It specifies the sequence in which different types of tunnels are selected and the number of tunnels taking part in load balancing.
- Tunnel binding policy: It binds a tunnel to a destination address. In this manner, the VPN traffic bound for the destination address enters the bound tunnel only, and as a result, QoS is guaranteed for the VPN traffic.

Precautions

If you change the tunnel policy in a VPN instance, VPN services may be interrupted due to a possibility of recursion failures.

Run one of the following commands to perform further configuration on the created tunnel policy:

- To configure the tunnel policy as a tunnel type prioritizing policy, run the **tunnel select-seq** command.
- To configure the tunnel policy as a tunnel binding policy, run the **tunnel binding** command.

The system can select tunnels for a VPN instance based on a tunnel policy only after the tunnel policy is applied to the VPN instance. The mode in which a tunnel policy is applied to a VPN instance varies according to the VPN type.

Example

Create a tunnel policy named policy1 and enter the tunnel policy view.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy policy1
[HUAWEI-tunnel-policy-policy1]
```

10.4.62 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** | **ipv6-ipv4** [**6to4** | **isatap**] | **ipv4-ipv6** | **mpls te** | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicate that the GRE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameters.	-
ipv4-ipv6	Indicate that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameter.	-
ipv6-ipv4 [**6to4** | **isatap**]	Configure the tunnel protocol of the tunnel interface as ipv6-ipv4: ● **ipv6-ipv4**: use a manual IPv6 over IPv4 tunnel ● **ipv6-ipv4 6to4** : using 6to4 tunnel ● **ipv6-ipv4 isatap** : using isatap tunnel **NOTE** Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support these parameter.	-

Parameter	Description	Value
mpls te	Indicate that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730-S, S6730S-S, and S6730S-H support the parameter.	-
none	Indicate that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface.

Example

Set the tunnel encapsulation mode of Tunnel2 to GRE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 2
[HUAWEI-Tunnel2] tunnel-protocol gre
```

10.4.63 tnl-policy

Function

The **tnl-policy** command associates a tunnel policy with the current VPN instance address family.

The **undo tnl-policy** command dissociates the current VPN instance address family from a tunnel policy.

By default, no tunnel policy is associated with the VPN instance address family. By default, a tunnel is selected for a VPN in the sequence of the LSP, CR-LSP, and Local_IfNet, and no load balancing is performed.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the tunnel policy to be associated with the VPN instance address family.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a device only uses an LSP tunnel to forward data on the backbone network and cannot implement multi-path load balancing at the same time. To ensure transmission quality of services and specify a TE tunnel to transmit VPN services, or to improve transmission efficiency and implement load balancing, run the **tunnel-policy** command to configure a tunnel policy and run the **tnl-policy** command to reference the tunnel policy in the VPN address family view.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** command has been executed to create a VPN instance and enter the VPN instance IPv4 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

If the tunnel policy associated with a VPN instance enabled with the address family cannot match an existing tunnel on the network, the routes in the VPN instance enabled with the address family will have routes recursing to tunnels based on the default tunnel policy. If the recursion fails, services will be interrupted.

If the address family of a VPN instance changes or the associated tunnel policy is deleted, VPN services will be interrupted for a short time even if tunnels matching the tunnel policy are available on the network. Therefore, use the **tnl-policy** command with caution.

Follow-up Procedure

If the associated tunnel policy does not exist, run the **tunnel-policy** command to create the tunnel policy.

Example

Associate a tunnel policy named **po1** with the VPN instance named *vpn2*.

```
<HUAWEI> system-view
[HUAWEI] tunnel-policy po1
[HUAWEI-tunnel-policy-po1] tunnel select-seq lsp load-balance-number 2
[HUAWEI-tunnel-policy-po1] quit
[HUAWEI] ip vpn-instance vpn2
[HUAWEI-vpn-instance-vpn2] ipv4-family
[HUAWEI-vpn-instance-vpn2-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn2-af-ipv4] tnl-policy po1
```

10.4.64 transit-vpn

Function

The **transit-vpn** command ensures that the status of a VRF (VPN Routing and Forwarding table) obtained from MIB is always Up, no matter whether this VRF is bound to interfaces.

The **undo transit-vpn** command restores the default setting.

By default, the status of a VRF obtained from MIB is Up only if it is bound to at least one interface in the Up state.

NOTE

Only the following switch models support this command:

S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H

Format

transit-vpn

undo transit-vpn

Parameters

None.

Views

VPN instance view or VPN instance IPv4 address family view

Level

2: Configuration level

Usage Guidelines

Usage Scenario

According to RFC, the status of a VRF obtained from MIB is Up only if it is bound to at least one interface in the Up state. In the HoVPN or H-VPN networking, however, a VRF does not need to be bound to any interface. If the VRF is not bound to an interface in this networking, the status of the VRF obtained from MIB is Down by default.

In this case, you can run the **transit-vpn** command to ensure that the status of a VRF obtained from MIB is always Up.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Example

Configure the status of the VRF vpna obtained from MIB to be always Up, no matter whether the VRF is bound to interfaces.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpna
[HUAWEI-vpn-instance-vpna] ipv4-family
[HUAWEI-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpna-af-ipv4] transit-vpn
```

10.4.65 undo vpn frr all

Function

Using the **undo vpn frr all** command, you can disable VPN FRR in all the VPN instances.

Format

undo vpn frr all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPN FRR function may be configured in multiple VPN instances on a device. The **undo vpn frr** command takes a long time to cancel the VPN FRR function of all VPN instances one by one.

In the system view, run the **undo vpn frr all** command to simultaneously cancel the VPN FRR function of IPv4 and IPv6 address families in all VPN instances.

Precautions

To cancel the VPN FRR function of a VPN instance, run the **undo vpn frr** command.

Example

Disable VPN FRR of all the VPN instances in the system view.

```
<HUAWEI> system-view
[HUAWEI] undo vpn frr all
```

10.4.66 vpn-route cross multipath

Function

The **vpn-route cross multipath** command adds multiple VPNv4 or VPNv6 routes to a VPN instance with a different RD from these routes' RDs.

The **undo vpn-route cross multipath** command restores the default configuration.

By default, if the RDs of multiple VPNv4 or VPNv6 routes are different from the RD of a VPN instance, only the optimal route is added to the VPN instance.

Format

vpn-route cross multipath

undo vpn-route cross multipath

Parameters

None

Views

BGP-VPN instance IPv4 address family view or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if the RD of the VPN instance on the local PE is different from the RDs of the VPN instances on multiple remote PEs, and the RDs of the VPN instances on remote PEs are the same, the local PE adds only the optimal route to the VPN instance after receiving VPNv4 or VPNv6 routes with the same destination address from the remote PEs. As a result, load balancing or VPN FRR does not take effect. To resolve this problem, run the **vpn-route cross multipath** command on the local PE.

Configuration Impact

After you run the **vpn-route cross multipath** command, the local PE adds multiple VPNv4 or VPNv6 routes to a VPN instance with a different RD from these routes' RDs. The number of VPNv4 or VPNv6 routes that can be added to the VPN instance depends on whether load balancing or VPN FRR is configured.

- If no load balancing is configured, a maximum of two VPNv4 or VPNv6 routes can be added to the VPN instance.
- If you set the maximum number of equal-cost routes for load balancing to *n* using the **maximum load-balancing** command, *n* VPNv4 or VPNv6 routes can be added to the VPN instance.
- If you configure VPN FRR and set the maximum number of equal-cost routes for load balancing to *n* using the **maximum load-balancing** and **auto-frr** command, *n* + 1 VPNv4 or VPNv6 routes can be added to the VPN instance.

Example

Add multiple VPNv4 routes to a VPN instance with a different RD from these routes' RDs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vrf1
[HUAWEI-bgp-vrf1] vpn-route cross multipath
```

Add multiple VPNv6 routes to a VPN instance with a different RD from these routes' RDs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv6-family vpn-instance vrf1
[HUAWEI-bgp6-vrf1] vpn-route cross multipath
```

10.4.67 vpn-target

Function

The **vpn-target** command configures the export or import VPN target extended community attribute for the VPN instance address family.

The **undo vpn-target** command deletes the setting.

By default, no export or import VPN target extended community list is configured for the VPN instance address family.

Format

vpn-target *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

NOTE

Only the following switch models support this command:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

The S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S only support the VPN instance view and VPN instance IPv4 address family view.

Parameters

Parameter	Description	Value
vpn-target	Specifies the VPN target extended community attribute to be added to the VPN target extended community list of the VPN instance address family. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-
both	Adds the VPN target extended community attribute to the export and import VPN target extended community lists of the VPN instance address family. If none of **both**, **export-extcommunity**, or **import-extcommunity** is specified, **both** is adopted by default.	-
export-extcommunity	Adds the VPN target extended community attribute to the export VPN target extended community lists of the VPN instance address family.	-
import-extcommunity	Adds the VPN target extended community attribute to the import VPN target extended community lists of the VPN instance address family.	-

Parameter	Description	Value
all	Delete all the VPN targets of the VPN instance IPv4 address family.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN instance is configured on a PE, the **vpn-target** command must be used to configure a VPN target for the IPv4 or IPv6 address family of the VPN instance.

The VPN target controls route learning between VPN sites. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 or IPv6 route to be advertised to a remote MP-BGP peer. After receiving a VPNv4 or IPv6 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 or IPv6 route can be added to the routing table of the local VPN instance enabled with the IPv4 or IPv6 address family.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

A VPN target configured using the **vpn-target** command will not overwrite any previously configured VPN target. If the number of configured VPN targets has reached the maximum limit, no VPN target can be added by using the **vpn-target** command.

After a VPN target is configured for the IPv4 or IPv6 address family of a VPN instance, only the routes that match the VPN target will be accepted by the IPv4 or IPv6 address family of the VPN instance.

If all the VPN targets of the IPv4 or IPv6 address family of a VPN instance are deleted using the **undo vpn-target** command, all routes learned by the IPv4 or IPv6 address family of the VPN instance from other VPN instances will be deleted.

Multiple VPN targets can be configured for the IPv4 or IPv6 address family of a VPN instance. One **vpn-target** command can configure a maximum of eight VPN targets at a time. If you want to configure more VPN targets in the VPN instance IPv4 or IPv6 address family view, run the **vpn-target** command multiple times. When VPN routes are advertised between VPN instances, if one of the VPN targets carried in the VPNv4 or IPv6 routes matches the import VPN target of the IPv4 or

IPv6 address family of a local VPN instance, the routes will be added to the routing table of the local VPN instance.

Example

Add 3:3 to the export VPN target extended community list and 4:4 to the import VPN target extended community list of the VPN instance named *vrf1*.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity
```

10.4.68 vpn frr

Function

Using the **vpn frr** command, you can enable VPN FRR.

Using the **undo vpn frr** command, you can disable VPN FRR.

By default, VPN FRR is disabled.

Format

vpn frr route-policy *route-policy-name*

undo vpn frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VPN FRR is applied on a VPN where a CE is dual-homed to two PEs. VPN FRR uses a secondary tunnel to back up the primary tunnel and detects the connectivity of the primary tunnel in combination with rapid detection technologies such as BFD. When a fault occurs on the primary tunnel, a PE configured with VPN FRR can switch VPN traffic to the secondary tunnel before the VPN routes are converged. This improves reliability of data forwarding on the public network.

VPN FRR has two modes: VPN static FRR and VPN auto FRR. The **vpn frr** command configures manual VPN FRR and the **auto-frr** command configures VPN Auto FRR.

Compared with VPN Auto FRR, manual VPN FRR specifies backup next hop more precisely. If manual VPN FRR and VPN Auto FRR are configured simultaneously, manual VPN FRR takes preference over VPN Auto FRR. If manual VPN FRR fails, VPN Auto FRR takes effect.

Prerequisites

Manual VPN FRR function takes effect after the backup next hop is manually specified. It is recommended that you run the **route-policy** command to specify the backup next hop for VPN routes before configuring Manual VPN FRR function.

Follow-up Procedure

After configuring Manual VPN FRR function, run the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* **verbose** command to check whether the route has a secondary tunnel and a backup label.

Precautions

NOTE

The **undo vpn frr** command cancels the VPN FRR function of only the specified VPN instance. In the system view, run the **undo vpn frr all** command to simultaneously cancel the VPN FRR function of IPv4 and IPv6 address families in all VPN instances.

Example

Specify the IP address of the backup next hop in the route-policy named **vpn_frr_rp**, and enable VPN FRR in the VPN instance view.

```
<HUAWEI> system-view
[HUAWEI] route-policy vpn_frr_rp permit node 10
[HUAWEI-route-policy] apply backup-nexthop 10.2.2.9
[HUAWEI-route-policy] quit
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] vpn frr route-policy vpn_frr_rp
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
```

10.5 VLL Configuration Commands

10.5.1 Command Support

Only the following switch models support VLL:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

Command support and parameter support on your switches may differ from those described in this section. For details, see the specific commands.

10.5.2 bfd bind pw

Function

The **bfd bind pw** command configures a BFD session to detect a PW.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is configured to detect a PW.

Format

bfd *cfg-name* **bind pw interface** *interface-type interface-number* [**secondary**]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of the BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of the interface where the PW to be detected resides, namely, the AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates that the BFD session detects the secondary PW.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link detection mechanism on an interface. On networks demanding fast fault detection, run the **bfd bind pw** command to configure a BFD session to detect a PW.

Prerequisites

- A PW has been configured on an AC interface by running the **mpls l2vc** command.
- BFD has been enabled globally by running the **bfd** command.
- A single-segment or multi-segment PW has been configured.

Precautions

- When detecting a PW, BFD sessions must be bound to the source and destination ends of a PW.
- You need to create a BFD session to detect primary and secondary PWs separately.

NOTE

When running the **bfd bind pw** command to detect a multi-segment PW, ensure that the first-segment PW is a VLL PW configured on a non-SPE node.

When running the **bfd bind pw** command to detect a single-segment PW, ensure that the single-segment PW is configured on a non-SPE node.

Example

Create a BFD session to detect a PW.

```
<HUAWEI> system-view
[HUAWEI] bfd pe2 bind pw interface vlanif 10
```

10.5.3 ccc interface in-label out-label

Function

The **ccc interface in-label out-label** command creates a remote CCC connection between CEs connected to different PEs. This command must be configured on two PEs.

The **undo ccc** command deletes the CCC connection.

By default, no remote CCC connection is created.

Format

ccc *ccc-connection-name* **interface** *interface-type1 interface-number1* [**raw** | **tagged**] **in-label** *in-label-value* **out-label** *out-label-value* **nexthop** *nexthop-address* [**control-word** | **no-control-word**]

undo ccc *ccc-connection-name*

Parameters

Parameter	Description	Value
ccc-connection-name	Specifies the CCC connection name, which uniquely identifies a CCC connection on a PE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type1 interface-number1*	Specifies the type and number of the incoming interface of data traffic. In the preceding information: ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
raw	Sets the inbound interface to raw mode. When packets arrive at the inbound interface in raw mode, the system deletes the Provider tags (P-Tags) of packets.	By default, the tagged mode is used.
tagged	Sets the inbound interface to tagged mode. When packets arrive at the inbound interface in tagged mode, the system retains the Provider tags (P-Tags) of packets.	By default, the tagged mode is used.
in-label *in-label-value*	Specifies the inbound label.	The value is a decimal integer that ranges from 16 to 1023.
out-label *out-label-value*	Specifies the outbound label.	The value is a decimal integer that ranges from 0 to 1048575.
nexthop *nexthop-address*	Specifies the IP address of the next hop.	The value is in dotted decimal notation.
control-word | **no-control-word**	Enables or disable the control word (CW).	By default, the control word is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two CEs connected to different PEs, use the **ccc interface in-label out-label** command to create a remote CCC connection between the CEs. This command must be executed on both PEs.

Precautions

An interface cannot serve as an L2VPN AC (Attachment Circuit) interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid.

NOTE

The device supports only VLANIF interfaces as AC interfaces of CCC connections.

A PE uses connection names to identify different CCC connections. On different PEs, the same CCC connection can use different names. When a P is connected to a PE, the static LSP must be configured between the P and PE. Do not configure the name of a CCC connection as **type**. Otherwise, you cannot view information about the CCC connection using the **display vll ccc** *ccc-name* command. Note that the outgoing label of the previous device is the inner label of the next device.

By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

Example

Create a remote CCC connection between CEs connected to different PE devices.

```
<HUAWEI> system-view
[HUAWEI] ccc ccc-connection interface vlanif 10 in-label 100 out-label 200 nexthop 10.1.1.2
```

10.5.4 ccc interface out-interface

Function

The **ccc interface out-interface** command creates a local CCC connection between two CEs connected to the same PE.

The **undo ccc** command deletes the CCC connection.

By default, no local CCC connection is created.

Format

ccc *ccc-connection-name* **interface** *interface-type1 interface-number1* [**raw** | **tagged**] **out-interface** *interface-type2 interface-number2* [**raw** | **tagged**]

undo ccc *ccc-connection-name*

Parameters

Parameter	Description	Value
ccc-connection-name	Specifies a CCC connection name, which uniquely identifies a CCC connection on a PE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type1 interface-number1*	Specifies the type and number of the interface connected to the first CE. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
out-interface *interface-type2 interface-number2*	Specifies the type and number of the interface connected to the second CE. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-
raw	Sets the inbound interface to raw mode. When packets arrive at the inbound interface in raw mode, the system deletes the provider tags (P-tags) of packets.	By default, the tagged mode is used.
tagged	Sets the inbound interface to tagged mode. When packets arrive at the inbound interface in tagged mode, the system retains the provider tags (P-tags) of packets.	By default, the tagged mode is used.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two CEs connect to the same PE, use the **ccc interface out-interface** command to create a local CCC connection between the CEs.

Precautions

An interface cannot serve as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid. After the interface is bound to a CCC connection, its sub-interfaces no longer transmit Layer 3 traffic.

NOTE

- The device supports only VLANIF interfaces as AC interfaces of CCC connections.

A CCC connection is bidirectional; therefore, only one connection is needed. Do not configure the name of a CCC connection as **type**; otherwise, you cannot view information about the CCC connection by running the **display vll ccc** command.

By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

Example

Create a local CCC connection between two CEs connected to the same PE device.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] ccc ccc-connect-1 interface vlanif 10 out-interface vlanif 11
```

10.5.5 ce

Function

The **ce** command creates a CE and displays the MPLS-L2VPN-CE view.

The **undo ce** command deletes a CE.

By default, no CE is created in a L2VPN instances.

Format

ce *ce-name* [**id** *ce-id* [**range** *ce-range*] [**default-offset** *ce-offset*]]

undo ce *ce-name*

Parameters

Parameter	Description	Value
ce-name	Specifies the name of a CE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported.
id *ce-id*	Specifies the ID of the CE.	The value is a decimal integer that ranges from 0 to 249. A CE ID uniquely identifies a CE in a L2VPN instances. For convenience, you are advised to set the CE IDs in the sequence of natural number that starts from 1.
range *ce-range*	Specifies the number of CEs in an L2VPN instance.	The value is a decimal integer that ranges from 1 to 250 and the default is 10.
default-offset *ce-offset*	Indicates the default CE offset. The CE offset refers to the ID of the other local CE or the remote CE that establishes the connection with the local CE.	It can be either 0 or 1. The default is 0.

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use the **ce** command to create a CE in a L2VPN instance and enter the MPLS-L2VPN-CE view.

Prerequisites

An RD has been configured for the L2VPN instance.

Precautions

ce-range can be increased but cannot be decreased. If multiple label blocks exist, the *ce-range* equals the total size of all label blocks. A device allocates labels to the ranges of Kompella L2VPN instances and VPLS VSIs from the same label block. Therefore, the ranges of Kompella L2VPN instances and VPLS VSIs cannot be larger than the size of the label block. Otherwise, the system displays a message indicating that the number of required labels exceeds the permitted maximum labels. As a result, the system fails to create a CE or fails to allocate a site ID to a VSI.

The constraints between **default-offset** and *ce-range* in this command and *ce-offset* in **connection** are as follows:

- If **default-offset** in this command is 0, *ce-offset* in the **connection** command must be less than *ce-range* in this command.
- If **default-offset** in this command is 1, *ce-offset* in the **connection** command must be not more than *ce-range* in this command and cannot be 0.

Example

Create a CE named ce1 inside the vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation ethernet
[HUAWEI-mpls-l2vpn-vpn1] route-distinguisher 100:1
[HUAWEI-mpls-l2vpn-vpn1] ce ce1 id 1 range 10
[HUAWEI-mpls-l2vpn-ce-vpn1-ce1]
```

10.5.6 connection

Function

The **connection** command creates a connection in Kompella mode between CEs.

The **undo connection ce-offset** command deletes a connection in Kompella mode between CEs.

By default, no connection in Kompella mode is created between CEs.

Format

connection [**ce-offset** *id*] **interface** *interface-type interface-number* [**tunnel-policy** *policy-name*] [**raw** | **tagged**] [**secondary**]

undo connection ce-offset *id*

Parameters

Parameter	Description	Value
ce-offset *id*	Specifies the ID of the peer CE connected to the L2VPN.	The value is a decimal integer that ranges from 0 to 249. *id* must be not more than *ce-range*. For the configuration about *ce-range*, see **ce**. For a remote connection, **ce-offset** and the ID of the remote CE must be the same; for a local connection between two CEs, **ce-offset** of a CE is the ID of the other CE.
interface *interface-type interface-number*	Specifies the type and number of the interface connected to the CE. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
tunnel-policy *policy-name*	Specifies the name of a tunnel policy applied to a VLL connection.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Sets the encapsulation mode to raw mode. In raw mode, the device deletes the Provider tag (P-Tag) in the packets. The P-Tag is inserted by an SP device to distinguish traffic from different users.	-
tagged	Sets the encapsulation mode to tagged mode. In tagged mode, the device retains the P-Tag in the packets.	-

Parameter	Description	Value
secondary	Specifies the secondary connection of the CE. If this parameter is not specified, the new connection becomes the primary connection. Specify this parameter only when a primary connection exists locally.	-

Views

MPLS-L2VPN-CE view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use the **connection** command to create a connection.

Precautions

An interface cannot serve as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid.

NOTE

- When the sub-interface is bound to a VLL, the encapsulation protocol type of the main interface cannot be changed.
- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- VLANIF interfaces, XGE interfaces, MultiGE interface, 25GE interface, 40GE interfaces, 100GE interfaces, GE interfaces, Eth-Trunk interfaces, XGE sub-interfaces, 25GE sub-interface, MultiGE sub-interfaces, 40GE sub-interfaces, 100GE sub-interfaces, GE sub-interfaces, or Eth-Trunk sub-interfaces can be used as AC interfaces connected to CEs.

  To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.
- The management interface cannot be configured as the AC interface connected to a CE.

When creating a connection in Kompella mode, you need to specify the peer CE ID and the local CE interface.

If you do not specify **ce-offset** *id*:

- For the first connection of the CE, by default, **ce-offset** *id* is the same as the **default-offset**. For the description about **default-offset**, see **ce**. If **ce-offset** equals the current CE ID, **ce-offset** increases by 1.

- For other connections, **ce-offset** *id* is the last CE ID plus 1. If the CE offset ID of the last connection plus 1 equals the current CE ID, the **ce-offset** *id* is the value obtained by CE offset of the last connection plus 2.

It is recommended that you number CE IDs from 1 in ascending order, and to configure connections in the order of CE IDs. To simplify configuration, you can use the default **ce-offset** directly in most connections.

After the command is configured, the default policy is adopted in the following situations:

- If you do not specify a policy name
- If the specified policy is not configured

In the default policy:

- Only LSP tunnels are selected.
- No load balancing is performed.

By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

Example

Create a connection in Kompella mode.

```
<HUAWEI1> system-view
[HUAWEI1] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI1-mpls-l2vpn-vpn1] route-distinguisher 100:1
[HUAWEI1-mpls-l2vpn-vpn1] vpn-target 1:1
[HUAWEI1-mpls-l2vpn-vpn1] ce ce1 id 1 range 10
[HUAWEI1-mpls-l2vpn-ce-vpn1-ce1] connection ce-offset 2 interface vlanif 10
<HUAWEI2> system-view
[HUAWEI2] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI2-mpls-l2vpn-vpn1] route-distinguisher 100:1
[HUAWEI2-mpls-l2vpn-vpn1] vpn-target 1:1
[HUAWEI2-mpls-l2vpn-vpn1] ce ce2 id 2 range 10
[HUAWEI2-mpls-l2vpn-ce-vpn1-ce2] connection ce-offset 1 interface vlanif 20
```

10.5.7 display bgp l2vpn

Function

The **display bgp l2vpn** command displays information about the Kompella L2VPN label block stored in BGP.

Format

display bgp l2vpn { **all** | **group** [*group-name*] | **peer** [[*peer-ip-address*] **verbose**] | **route-distinguisher** *route-distinguisher* [**ce-id** *ce-id* [**label-offset** *label-offset*]] }

Parameters

Parameter	Description	Value
all	Displays all information about the local label block of Kompella L2VPN stored in BGP.	-
group *group-name*	Displays information about the label block of Kompella L2VPN stored in a specified BGP peer group.	The value is an existing BGP peer group.
peer-ip-address	Displays information about the Kompella L2VPN label block of the specified peer stored in BGP.	The value is in dotted decimal notation.
verbose	Displays detailed information about the Kompella L2VPN label block stored in BGP.	-
route-distinguisher *route-distinguisher*	Specifies the specific route identification value. The RD format can be any of the following: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.	-
ce-id *ce-id*	Specifies the number of CE of the L2VPN instance.	The value ranges from 0 to 65535.

Parameter	Description	Value
label-offset *label-offset*	Specifies the offset value of the label.	It is a decimal integer ranging from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use the **display bgp l2vpn** command to check information about a label block, including the RD value, CE ID, label offset, start label in the label block, and BGP routing attributes of the label block.

Precautions

If **route-distinguisher**, **ce-id**, and **label-offset** all are specified, you can view the BGP extended community attribute, the value of each label in the label block, the status of the L2VPN connection status using this label as well as the BGP peers to which this label block is advertised.

Example

View the BGP L2VPN label block with the specified RD, CE ID, and label offset.

```
<HUAWEI> display bgp l2vpn route-distinguisher 1:1 ce-id 1 label-offset 0
 BGP Local router ID : 10.1.1.2, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 nexthop:6.6.6.6,  pref :100,     as-path :(null)
 label base: 35840, label range: 10, layer-2 mtu: 1500, encap type:Ethernet VLAN
 label          state
  35840           down
  35841           down
  35842           up
  35843           down
  35844           down
  35845           down
  35846           down
  35847           down
  35848           down
  35849           down
```

Table 10-47 Description of the **display bgp l2vpn** command output

Item	Description
BGP Local router ID	Local router ID of local BGP. Its format is the same as the IPv4 address.

Item	Description
Origin codes	The origin attributes of BGP route: ● i - IGP: Interior Gateway Protocol (IGP), It is of the highest priority. ● e - EGP: Exterior Gateway Protocol (EGP): It is of the second highest priority. ● ? - incomplete: It is of the lowest priority.
local AS number	Local autonomous system (AS) number.
nexthop	Next-hop address of MP-BGP.
pref	Local preference, which is one type of BGP routing attribute.
as-path	AS path attribute, which is one type of BGP routing attribute. It records the numbers of all ASs sequentially that a packet passes through from the local address to the destination address.
label base	Starting value of the label.
label range	Range of the labels.
layer-2 mtu	MTU value of the link layer.
encap type	Encapsulation mode of the link layer.
label	Allocated label.
state	Status of the allocated label.

10.5.8 display l2vpn ccc-interface vc-type

Function

The **display l2vpn ccc-interface vc-type** command displays information about the interface used by an L2VPN connection.

Format

display l2vpn ccc-interface vc-type { **all** | *vc-type* } [**down** | **up**]

Parameters

Parameter	Description	Value
all	Displays information about all interfaces of L2VPN connections.	-
vc-type	Specifies the type of the L2VPN connection.	The following types of the L2VPN connection are available: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection
down	Displays information about interfaces of L2VPN connection in the Down state.	-
up	Displays information about interfaces of L2VPN connection in the Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating L2VPN faults, you can use the **display l2vpn ccc-interface vc-type** command to view information about the AC interface of the current L2VPN connection, the total number of AC interfaces of various L2VPN connections, interface status, interface encapsulation type, and L2VPN connection types.

Example

Display information about all the interfaces of L2VPN.

```
<HUAWEI> display l2vpn ccc-interface vc-type all
Total ccc-interface of LDP VC: 1
up (1), down (0)
Interface               Encap Type             State    VC Type
Vlanif12                vlan                up       ldp-vc
```

Table 10-48 Description of the **display l2vpn ccc-interface vc-type** command output

Item	Description
Total ccc-interface of CCC : 2 up (2), down (0)	Total number of L2VPN connections is 2. Two connections is Up. No connection is Down.
Interface	Interface connected to the L2VPN connection on the switch.
Encap Type	Encapsulation type of the L2VPN connection. The encapsulation type can be VLAN encapsulation or Ethernet encapsulation.
State	Current status of the L2VPN connection. The status can be Up or Down.
VC Type	Type of the L2VPN connection: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection

10.5.9 display mpls l2vc

Function

The **display mpls l2vc** command displays information about virtual circuits (VCs) in LDP mode.

Format

display mpls l2vc [*vc-id* | **interface** *interface-type interface-number* | **remote-info** [*vc-id* | **verbose**] | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface connected to the CE. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
remote-info	Displays information about the VC on the remote end.	-
vc-id	Displays static PW information with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays the detailed information about the VC on the remote end.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc** command displays information about the VCs in LDP signaling mode, including the Martini VC and PWE3 VC.

- If the interface is specified, information about VCs on the specified AC interface is displayed.
- If **remote-info** is specified but *vc-id* is not specified, information about all VCs set up by the remote and local peers is displayed.

Example

Display information about all the LDP VCs configured on the switch.

```
<HUAWEI> display mpls l2vc
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 101
  VC type                : VLAN
  destination            : 10.3.3.9
  local VC label         : 1026         remote VC label      : 1026
```

```
control word           : disable
remote control word    : disable
forwarding entry       : exist
local group ID         : 0
remote group ID        : 0
local AC OAM State     : up
local PSN OAM State    : up
local forwarding state : forwarding
local status code      : 0x0
remote AC OAM state    : up
remote PSN OAM state   : up
remote forwarding state: forwarding
remote status code     : 0x0
ignore standby state   : no
BFD for PW             : unavailable
VCCV State             : up
manual fault           : not set
active state           : active
link state             : up
local VC MTU           : 1500         remote VC MTU         : 1500
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
tunnel policy name     : --
PW template name       : --
primary or secondary   : primary
load balance type      : flow
Access-port            : false
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x48000020
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 6 minutes, 50 seconds
up time                : 0 days, 0 hours, 6 minutes, 34 seconds
last change time       : 0 days, 0 hours, 6 minutes, 34 seconds
VC last up time        : 2013/09/24 18:23:35
VC total up time       : 0 days, 0 hours, 6 minutes, 34 seconds
CKey                   : 16
NKey                   : 15
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : be
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 10-49 Description of the **display mpls l2vc** command output

Item	Description
Total LDP VC	Total number of established LDP VCs, including the number of LDP VCs in Up and Down state.
client interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface. This field can be displayed as **yes** or **no**.
session state	Status of the LDP session established between both ends of the VC: ● up: The LDP session has been established. ● down: The LDP session is not established.

Item	Description
AC status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. ● enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. ● disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token state	Token status: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
VC ID	ID of the VC, which uniquely identifies a VC. **NOTE** If the VC IDs on both ends are different, run the **mpls l2vc** command in the interface view to change the VC ID on one end to be the same as that on the other end.
VC type	Encapsulation type of the VC: ● VLAN ● Ethernet The PW can go Up only when the local and remote encapsulation types are the same.
destination	LSR ID of the VC peer device.
local VC label	Local VC label.
remote VC label	Remote VC label.

Item	Description
control word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.
forwarding entry	Whether forwarding entries exist.
local group ID	Local group ID.
remote group ID	Remote group ID.
manual fault	Whether a PW fault is simulated.
active state	Whether the PW is in active state. A PW in active state can forward packets.
link state	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● Status of the mPW associated with service PWs ● Status of the BFD session associated with service PWs ● PW state code ● PW status detected by VCCV ● OAM status
local VC MTU	MTU of the local VC.
remote VC MTU	MTU of the remote VC.
tunnel policy name	Name of the tunnel policy.
PW template name	Name of the PW template.
primary or secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.

Item	Description
Switchover Flag	Whether a switchover has occurred.
create time	How long the VC has been created.
up time	How long the VC keeps the Up state. If the current PW status is Down, the value is 0.
last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
AdminPw interface	AC interface on which the mPW is bound to the PW. The AC interface must be a loopback interface. This field is displayed only when the PW is not an mPW: ● Name of the loopback interface. ● --: indicates that the PW is not bound to an mPW.
AdminPw link state	Status of the mPW bound to the PW. This field is displayed only when the PW is not an mPW. This field can be displayed as: ● Up ● Down ● --: indicates that the PW is not bound to an mPW.
Diffserv Mode	QoS DiffServ mode.
Service Class	QoS service class.
Color	QoS color.
DomainId	ID of a domain.
Domain Name	Name of a domain.

Display LDP VC information about the AC interface VLANIF 100.

```
<HUAWEI> display mpls l2vc interface vlanif 100
 *client interface       : Vlanif100  is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 1
```

```
VC type                : VLAN
destination            : 10.2.2.2
local group ID         : 0            remote group ID      : 0
local VC label         : 16400        remote VC label      : 16400
local AC OAM State     : up
local PSN OAM State    : up
local forwarding state : forwarding
local status code      : 0x0
remote AC OAM state    : up
remote PSN OAM state   : up
remote forwarding state: forwarding
remote status code     : 0x20
ignore standby state   : no
BFD for PW             : unavailable
VCCV State             : up
manual fault           : not set
active state           : active
forwarding entry       : exist
link state             : up
local VC MTU           : 1500         remote VC MTU        : 1500
local VCCV             : cw alert ttl lsp-ping bfd
remote VCCV            : cw alert ttl lsp-ping bfd
local control word     : enable       remote control word  : enable
tunnel policy name     : --
PW template name       : --
primary or secondary   : primary
load balance type      : flow
Access-port            : false
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x800802
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 0 minutes, 29 seconds
up time                : 0 days, 0 hours, 0 minutes, 6 seconds
last change time       : 0 days, 0 hours, 0 minutes, 6 seconds
VC last up time        : 2011/07/04 20:25:50
VC total up time       : 0 days, 0 hours, 0 minutes, 6 seconds
CKey                   : 2
NKey                   : 1
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : --
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 10-50 Description of the **display mpls l2vc interface** command output

Item	Description
local AC OAM State	OAM status of the local AC. - up - down
local PSN OAM State	Status of the local device on the Packet Switch Network (PSN) side. - up - down

Item	Description
local forwarding state	Status of the local forwarding table. ● forwarding ● down
local status code	Status code of the local PW: ● 0x0: indicates that the local PW functions as the master PW and is in Up state. ● 0x20: indicates that the local PW functions as the backup PW and is in Up state. ● 0x1: indicates that the local PW functions as the master PW and is in Down state. ● 0x21: indicates that the local PW functions as the backup PW and is in Down state.
remote AC OAM state	OAM status of the remote AC. ● up ● down
remote PSN OAM state	Status of the remote device on the PSN side. ● up ● down
remote forwarding state	Status of the remote forwarding table. ● forwarding ● down
remote status code	Status code of the remote PW: ● 0x0: indicates that the remote PW functions as the master PW and is in Up state. ● 0x20: indicates that the remote PW functions as the backup PW and is in Up state. ● 0x1: indicates that the remote PW function as the master PW and is in Down state. ● 0x21: indicates that the remote PW function as the backup PW and is in Down state.
BFD for PW	Whether BFD for PW is enabled: ● available ● unavailable
VCCV State	Whether Virtual Circuit Connectivity Verification (VCCV) is enabled.

Item	Description
local VCCV	Type of VCCV supported on the local device. - By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. - If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
remote VCCV	Type of VCCV supported on the remote device. - By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. - If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
local control word	Whether the control word is enabled on the local device: - Disable - Enable
remote control word	Whether the control word is enabled on the remote device: - Disable - Enable
ignore standby state	Whether the status of the secondary PW is ignored.
VC Tunnel/token info: 1 tunnels/tokens	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
TNL type	Type of the tunnel used by the PW.
TNL ID	ID of the tunnel used by the PW.
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.

Item	Description
PW redundancy mode	PW redundancy mode. By default, the mode is FRR. - Independent: indicates that the PW is in negotiation mode. - frr: indicates that the PW is in FRR mode. - --: indicates that the PW is in master/slave mode.

Display the LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info
Total remote ldp vc : 1

Transport  Group      Peer            Remote        Remote     C   MTU/  N   S
VC ID      ID         Addr            Encap         VC Label   Bit CELLS Bit Bit

101        0          10.3.3.9        ethernet       1024       0   1500  0   0
```

Display the detailed LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info verbose
Total remote LDP VC : 1

VC ID              : 1
VC Type            : vlan
VC Label           : 1025
Peer Address       : 10.5.5.5
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 1
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 10-51 Description of the **display mpls l2vc remote-info** command output

Item	Description
Total remote ldp vc	Total number of created remote LDP VCs.
Transport VC ID	VC ID, which uniquely identifies a VC.
Group ID	ID of the group to which the L2VPN belongs. The default value is 0.
Peer Addr and Peer Address	IP address of the remote peer.
Remote Encap	Encapsulation type of the remote VC. - vlan - ethernet

Item	Description
Remote VC Label	Remote VC label.
C Bit	Whether the control word is enabled: - 1: indicates that the control word is enabled. - 0: indicates that the control word is disabled.
MTU/CELLS	MTU of the L2VPN.
N Bit and Notification	Whether the Notification message is supported: - 1: indicates the message is supported. - 0: indicates the message is not supported.
S Bit and Status Code	Status code: - 0: indicates the forwarding state. - 1: indicates the non-forwarding state. - 32: indicates the backup state.
Match Local VC	Whether the local VC ID matches the remote VC ID: - MATCH - NOT-MATCH
Max ATM CELLS	Maximum number of ATM cells that can be transmitted. If ATM encapsulation is used, the value ranges from 1 to 28, and the default value is 28. If non-ATM encapsulation is used, double hyphens (--) are displayed.
TDM RTP Header	Whether the RTP-header option is enabled: - enable: The RTP header is added to TDM packets to be transparently transmitted. - disable: The RTP header is not added to TDM packets to be transparently transmitted. This is the default value. - --: Non-TDM encapsulation is used.
TDM Encap Num	Number of frames in a TDM packet. If TDM encapsulation is used, the value is 8, 16, 24, 32 or 40, and the default value is 32. If non-TDM encapsulation is used, double hyphens (--) are displayed.
TDM Bit Rate	Number of timeslots in a TDM packet. Number of timeslots in a TDM packet = Number of bytes in a TDM packet/Number of frames in a TDM packet

Display information about the VCs in Up state.

```
<HUAWEI> display mpls l2vc state up
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 100
  VC type                : VLAN
  destination            : 10.2.2.9
  local VC label         : 1024         remote VC label      : 1024
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : alert ttl lsp-ping bfd
  remote VCCV            : alert ttl lsp-ping bfd
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x12
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 1 hours, 0 minutes, 17 seconds
  up time                : 0 days, 0 hours, 24 minutes, 56 seconds
  last change time       : 0 days, 0 hours, 24 minutes, 56 seconds
  VC last up time        : 2013/10/10 14:29:39
  VC total up time       : 0 days, 0 hours, 24 minutes, 56 seconds
  CKey                   : 10
  NKey                   : 9
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : --
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

10.5.10 display mpls l2vc brief

Function

The **display mpls l2vc brief** command displays brief information about LDP Layer 2 virtual circuits (L2VCs) on the device.

Format

display mpls l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc brief** command is recommended when many L2VCs are configured on a device. The command output is more concise than that of the **display mpls l2vc** command.

Example

Display brief information about all LDP L2VCs on the device.

```
<HUAWEI> display mpls l2vc brief
 Total LDP VC : 1     1 up       0 down

 *Client Interface     : Vlanif1111
  Administrator PW     : no
  AC status            : up
  Ignore AC state      : disable
  VC state             : up
  Label state          : 0
  Token state          : 0
  VC ID                : 116119
  VC Type              : VLAN
  session state        : up
  Destination          : 10.6.6.6
  link state           : up
```

Table 10-52 Description of the **display mpls l2vc brief** command output

Item	Description
Total LDP VC	Total number of LDP VCs, including the number of LDP VCs in Up and Down state.

Item	Description
Client Interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface.
AC status	Status of the AC: - up - down
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. - enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. - disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: - up - down
Label state	Label status: - 0: The label can be used. - 1: Wait for the SMB to confirm the label status. - 2: The label is released. - 3: SMB confirming failed.
Token state	Token status: - 0: The label can be used. - 1: Wait for the SMB to confirm the label status. - 2: The label is released. - 3: SMB confirming failed.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
session state	Status of the session between peers: - up - down
Destination	Peer address.
link state	Status of the VC: - up - down

10.5.11 display mpls l2vpn

Function

The **display mpls l2vpn** command displays information about an L2VPN on a PE.

Format

display mpls l2vpn [*l2vpn-name* [**local-ce** | **remote-ce**]]

Parameters

Parameter	Description	Value
l2vpn-name	Specifies the VPN to be displayed.	The value is an existing VPN name.
local-ce	Displays information about all the local CEs of a specified L2VPN.	-
remote-ce	Displays information about remote CEs learned from other PEs of a specified L2VPN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify parameters, the **display mpls l2vpn** command displays information related to the parameters. If not, information about all the L2VPNs is displayed.

Example

Display information about all the VPNs configured on the PE.

```
<HUAWEI> display mpls l2vpn
VPN number: 1
vpn-name        encap-type   route-distinguisher     mtu   ce(L)  ce(R)
vpn1           ethernet     100:1                   1500   1      1
```

Table 10-53 Description of the display mpls l2vpn command output

Item	Description
vpn-name	Name of the created VPN instance.
encap-type	Encapsulation type of L2VPN.
route-distinguisher	RD of L2VPN.

Item	Description
mtu	MTU of L2VPN.
ce (L)	The number of local CE connections. "L" indicates "local".
ce (R)	Number of remote CE connections. "R" indicates "remote".

Display information about the L2VPN named vpn1.

```
<HUAWEI> display mpls l2vpn vpn1
VPN name: vpn1, encap type: vlan, local ce number(s): 1, remote ce number(s): 1
route distinguisher: 100:1, MTU: 128
import vpn target: 1:1
export vpn target: 1:1

remote vpn site(s) :
no.  remote-pe-id    route-distinguisher
1    3.3.3.9         100:1
```

Table 10-54 Description of the display mpls l2vpn vpn1 command output

Item	Description
VPN name	Name of the created VPN instance.
encap type	Encapsulation type of the L2VPN.
local ce number (s)	Number of local CE connections.
remote ce number (s)	Number of remote CE connections.
route distinguisher	RD of the local L2VPN.
MTU	MTU of the interface associated with the L2VPN.
import vpn target	Route attribute of the received VPN route.
export vpn target	Attributes configured for the target VPN route.
remote vpn site (s)	The following display is about the remote site.
no.	Remote peer number.
remote-pe-id	ID of remote PE peer. Usually, it is MPLS LSR-ID or the session address of the BGP peer.
route-distinguisher	RD of the remote L2VPN. For the related command, see **route-distinguisher (MPLS-L2VPN instance view)**.

Display information about the local CE on L2VPN named vpn1.

```
<HUAWEI> display mpls l2vpn vpn1 local-ce
ce-name            ce-id   range   conn-num  CEBase/LBBase/Offset/Range
ce1                1       10      1         0/21504/0/10
ce2                2       10      1         0/21514/0/10
```

Table 10-55 Description of the display mpls l2vpn vpn1 local-ce command output

Item	Description
ce-name	CE name.
ce-id	CE ID that uniquely identifies a CE.
range	Local CE range. Indicates how many CEs are connected to the local CEs.
conn-num	Number of local connections set for local CEs.
CEBase/LBBase/Offset/Range	Label block assigned by the CE with which the local port sets up a connection. 0/21504/0/10 indicates the offset base address of the label block/the initial value of the label block/initial CE offset/the number of remote labels.

Display information about the remote CE on the L2VPN named vpn1.

```
<HUAWEI> display mpls l2vpn vpn1 remote-ce
no.  ce-id peer-id         route-distinguisher      LB
1    2     3.3.3.9         100:1                    19456/0/10
```

Table 10-56 Description of the display mpls l2vpn vpn1 remote-ce command output

Item	Description
no.	Sequence number of the connection.
ce-id	ID of the remote CE.
peer-id	IP address of the remote peer.
route-distinguisher	RD of the remote peer.
LB	Remote Label block. 19456/0/10 indicates the initial value of the label block/remote initial CE offset/the number of remote labels.

10.5.12 display mpls l2vpn (route-target-list)

Function

The **display mpls l2vpn** command displays the VPN target list for Kompella VLL.

Format

display mpls l2vpn { **export-route-target-list** | **import-route-target-list** }

Parameters

Parameter	Description	Value
export-route-target-list	Displays the VPN target list for Kompella VLL in the outbound direction.	-
import-route-target-list	Displays the VPN target list for Kompella VLL in the inbound direction.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an L2VPN connection in Kompella mode is Up but packet forwarding between CE devices fails, you can run this command to view the VPN target list of a specified VPN instance and check whether the VPN targets of the two PE devices match each other.

- The VPN target in the outbound direction of the local PE device must be the same as the VPN target in the inbound direction of the remote PE device.
- The VPN target in the inbound direction of the local PE device must be the same as the VPN target in the outbound direction of the remote PE device.

Example

Display the VPN target list for Kompella VLL in the inbound direction.

```
<HUAWEI> display mpls l2vpn import-route-target-list
import vpn target list:
 744:7  745:7  746:7  888:8
```

Display the VPN target list for Kompella VLL in the outbound direction.

```
<HUAWEI> display mpls l2vpn export-route-target-list
export vpn target list:
 755:7  888:8
```

Table 10-57 Description of the **display mpls l2vpn** command output

Item	Description
import vpn target list	VPN target list in the inbound direction.
export vpn target list	VPN target list in the outbound direction.

10.5.13 display mpls l2vpn connection

Function

The **display mpls l2vpn connection** command displays information about L2VPN connections of the Kompella mode.

Format

display mpls l2vpn connection *vpn-name* [**remote-ce** *ce-id* | **down** | **up** | **verbose**]

display mpls l2vpn connection [**summary** | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-name	Displays information about the specified L2VPN.	The value is an existing VPN name. If you do not specify a VPN name, information about all the L2VPNs is displayed.
remote-ce *ce-id*	Displays information about the remote connections of the specified CE.	The value is a decimal integer ranging from 0 to 249.
down	Displays the information of the connections that are Down. If you do not specify this parameter, the detailed information about connections in both Up and Down state is displayed.	-
up	Displays the information of the connections that are Up. If you do not specify this parameter, the detailed information about connections in both Up and Down state is displayed.	-

Parameter	Description	Value
verbose	Shows detailed information of connections. It is valid only when information about all the connections is displayed.	-
summary	Displays the summary information of connections.	-
interface *interface-type interface-number*	Displays information about the connections on the interface of the specified type and number. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an L2VPN connection of the Kompella mode, you can use the **display mpls l2vpn connection** *vpn-name* command to check the status of the connection.

The **display mpls l2vpn connection** command displays information about all the L2VPN connections of the Kompella mode on the local device.

Example

Display information about all the L2VPN Kompella connections.

```
<HUAWEI> display mpls l2vpn connection
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown

VPN name: komcon1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown

  CE name: 116-119, id: 2,
  Rid type status peer-id         route-distinguisher interface
  primary or not
--------------------------------------------------------------------------
  1    rmt  up      6.6.6.6         1:1                 Vlanif222
  primary
```

Table 10-58 Description of the display mpls l2vpn connection command output

Item	Description
1 total connections,connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown	The first two lines indicate information about all the Kompella connections on the local device, including: ● Total number of connections ● Number of connections in the Up state ● Number of connections in the Down state ● Number of local connections ● Number of remote connections ● Number of unknown connections
VPN name	Name of the created VPN instance.
1 total connections,connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown	Information about the VPN connections, including: ● Total number of connections ● Number of connections in the Up state ● Number of connections in the Down state ● Number of local connections ● Number of remote connections ● Number of unknown connections
CE name:	Name of the CE.
id:	CE ID of the CE connection, which uniquely identifies a CE in a VPN.
Rid	ID of the remote CE that establishes the connection with the local CE.
type	Type of the CE connection: ● rmt: indicates a remote connection. ● loc: indicates a local connection. ● ---: indicates the destination CE does not exist or the signaling connection setup fails when you set up a remote connection.
status	Status of the CE connection: ● Up: indicates the connection is set up successfully. ● Down: indicates the connection setup fails because the configuration is incorrect or the associated interface is Down.

Item	Description
peer-id	IP address of the peer that sets up the session with the local end.
route-distinguisher	RD of the VPN to which the CE belongs.
interface	Interface (an AC interface) connected to the CE.
primary or not	Whether the VC is a primary VC or a secondary VC.

Display the Kompella L2VPN remote connection on GE0/0/1

```
<HUAWEI> display mpls l2vpn connection interface gigabitethernet 0/0/1
conn-type: remote
    local vc state:         up
    remote vc state:          up
    local ce-id:            1
    local ce name:            ce1
    remote ce-id:             2
    intf (state,encap):        GigabitEthernet0/0/1(up,ethernet)
    peer id:               2.2.2.2
    route-distinguisher:       100:2
    local vc label:         31745
    remote vc label:          35842
    tunnel policy:           default
    CKey:                  2
    NKey:                   1
    primary or secondary:        primary
    forward entry exist or not: true
    forward entry active or not:true
    manual fault set or not:     not set
    AC OAM state:              up
    BFD for PW session index:   --
    BFD for PW state:           invalid
    BFD for LSP state:         true
    Local C bit is not set
    Remote C bit is not set
    tunnel type:             lsp
    tunnel id:              0x1000c
    Slave tunnel type:         lsp
    Slave tunnel id:          0x0
```

Table 10-59 Description of the remote connection in the display mpls l2vpn connection interface command output

Item	Description
conn-type	Type of the L2VPN connection: - local: indicates the local L2VPN connection. - remote: indicates the remote L2VPN connection. - unknown: indicates the unknown L2VPN connection. The reason that the unknown connection appears may be that the destination CE does not exist, or the signaling connection fails to be set up during the configuration of a remote connection.
local vc state	Status of the local VC: - Up: indicates that the connection is successfully set up. - Down: indicates the setup of the connection fails because the configuration is incorrect or the status of related interfaces is Down.
remote vc state	Status of the destination VC: - Up: indicates that the connection is successfully set up. - Down: indicates the setup of the connection fails because the configuration is incorrect or the status of related interfaces is Down.
local ce-id	ID of the local CE.
local ce name	Name of the local CE.
remote ce-id	ID of the destination CE that sets up the connection with the local CE.
intf (state,encap)	Status and encapsulation type of the local interface.
peer id	IP address of the peer setting up a session with the CE.
route-distinguisher	RD of the VPN to which the CE interface belongs.
local vc label	Label generated by the local system.
remote vc label	Remote label that is assigned to the local end by the remote LDP.

Item	Description
tunnel policy	Tunnel policy applied to the CE connection.
CKey	Index of the public tunnel (for VPN QoS).
NKey	Index of the public tunnel.
primary or secondary	Whether the VC is a primary VC or a secondary VC.
forward entry exist or not	Whether forwarding entries exist.
forward entry active or not	Whether forwarding entries are in the active state. (If so, user packets can be forwarded.)
manual fault set or not	Whether the PW fault is configured manually.
AC OAM state	OAM status of the local AC.
BFD for PW session index	Index of the BFD for PW.
BFD for PW state	Status of BFD for PW.
BFD for LSP state	Status of BFD for LSP.
Local C bit is not set	L2VPN disabled with the control word. If the control word is enabled, the information is not displayed.
Remote C bit is not set	The remote site disabled with the control word. If the control word is enabled, the information is not displayed.
tunnel type	Tunnel type. The tunnel transmits data of the CE in the public network.
tunnel id	ID of the tunnel. The tunnel transmits data of the CE in the public network.
Slave tunnel type	Type of the backup tunnel when PW over LDP FRR is applied.
Slave tunnel id	ID of the backup tunnel when PW over LDP FRR is applied.

Display the summary of the Kompella L2VPN connections.

```
<HUAWEI> display mpls l2vpn connection summary
1 total connections,
connections: 1 up,  0 down , 0 local, 1 remote, 0 unknown
No.   vpn-name    local-num remote-num unknown-num up-num total-num
1     vpn1              0         1          0         1      1
```

Table 10-60 Description of the display mpls l2vpn connection summary command output

Item	Description
total connections	Number of all L2VPN connections on the device.
connections:	Number of L2VPN connections of the following status: ● Up ● Down ● remote ● local ● unknown
No.	Sequence number of the connection.
vpn-name	VPN instance name. Various types of connections are displayed in the order of L2VPN instances.
local-num	Number of local connections of the L2VPN instance.
remote-num	Number of all remote connections of the L2VPN instance.
unknown-num	Number of all unknown connections of the L2VPN instance.
up-num	Total number of successful connections of the L2VPN instance.
total-num	Total number of connections of the L2VPN instance.

10.5.14 display mpls l2vpn forwarding-info

Function

The **display mpls l2vpn forwarding-info** command displays MPLS L2VPN forwarding information.

Format

display mpls l2vpn forwarding-info [*vc-label*] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vc-label	Specifies L2VPN VC label.	The value is a decimal integer that ranges from 16 to 1048575.
interface *interface-type interface-number*	Specifies the type and number of the interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vpn forwarding-info** command displays:

- Private network data carrying the specified label is forwarded from which tunnel.
- Whether the data supports the connectivity verification.
- Whether the data carries the control word.

Example

Display MPLS L2VPN forwarding information.

```
<HUAWEI> display mpls l2vpn forwarding-info interface vlanif 10
 The Main PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
-------------------------------------------------------------------------------
35841   LSP            SEND      ACTIVE   UP       UP    FALSE   2  a  0x1
   1   Record(s) Found.

 The Second PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
-------------------------------------------------------------------------------
   0   Record(s) Found.
```

Table 10-61 Description of the display mpls l2vpn forwarding-info interface command output

Item	Description
The Main PW Forward Information :	Forwarding information about the primary PW.
VCLABEL	Label of the VC bound to the interface.
TNLTYPE	Types of public network tunnels used by the VC such as LSP and CR-LSP.
ENTRYTYPE	Type of forwarding entries: ● SEND: forwarding entries of L2VPN except CCC ● CCC_SEND: forwarding entries of the CCC remote connection ● LOCAL: forwarding entries of the local connection ● INVALID: invalid forwarding entries
PWSTATE	PW state used for guiding packet forwarding: active or inactive. The primary PW and the secondary PW are mutually exclusive and both cannot be in the active state simultaneously.
BFDSTATE	BFD state used for guiding packet forwarding. If BFD is not configured, this flag bit is Up by default. If BFD is configured and the BFD session is Down (not Admin Down), this flag bit is Down and packets cannot be forwarded.
ADMIN	Whether the primary or secondary PW fault is configured manually: ● Up: indicates that the primary or secondary PW fault is not configured manually. ● Down: indicates that the primary or secondary PW fault is configured manually.
CTLWORD	Whether the control word is enabled on the local end: ● FALSE: indicates that the control word is disabled. ● TRUE: indicates that the control word is enabled.
CC	Connection channel of the VCCV: Control word Label alert.
CV	Connectivity verification.

Item	Description
TNLID	ID of the public tunnel used by the VC, which is a hexadecimal integer.
Record (s) Found	Number of VC forwarding entries on the local interface.
The Second PW Forward Information :	Forwarding information about the secondary PW.

Display MPLS L2VPN forwarding information with VC label as 35842.

```
<HUAWEI> display mpls l2vpn forwarding-info 35842 interface vlanif 10
 The Main PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
--------------------------------------------------------------------------------
35842   LSP            SEND      ACTIVE   UP       UP    FALSE   0  0  0x1
   1   Record(s) Found.

 The Second PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
--------------------------------------------------------------------------------
   0   Record(s) Found.
```

10.5.15 display mpls l2vpn label-space

Function

The **display mpls l2vpn label-space** command displays information about label space distribution and different types of labels in the label cache.

Format

display mpls l2vpn label-space

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After L2VPN is enabled, run the **display mpls l2vpn label-space** command and you can view information about label space distribution and different types of labels in the label cache.

Example

Display information about label space distribution when L2VPN is enabled and the cache contains labels.

```
<HUAWEI> display mpls l2vpn label-space
 there are 0 labels or label blocks in label-space.
 ------------------------------------------------------------
 label(s) released in SVC connection:             0
 label(s) released in LDP connection:             1
 label block(s) released in BGP connection:        0
 label(s) released in VPLS LDP connection:         0
 label block(s) released in VPLS BGP connection:   0
 ------------------------------------------------------------
```

Table 10-62 Description of the **display mpls l2vpn label-space** command output

Item	Description
Label	Indicates the value of the label in the label cache.
Label (s) released in SVC connection	Indicates the total number of labels in the label cache for the VLL SVC connections.
Label (s) released in LDP connection	Indicates the total number of labels in the label cache for the VLL LDP connections.
Label block (s) released in BGP connection	Indicates the total number of label blocks in the label cache for the VLL BGP connections.
Label (s) released in VPLS LDP connection	Indicates the total number of labels in the label cache for the VPLS LDP connections.
Label (s) released in VPLS BGP connection	Indicates the total number of labels in the label cache for the VPLS BGP connections.

10.5.16 display mpls l2vpn vpws

Function

The **display mpls l2vpn vpws** command displays information about the VPWS service.

Format

display mpls l2vpn vpws [**interface** *interface-type interface-number* [**verbose**]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
verbose	Displays detailed VPWS service information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring or commissioning VPWS, you can run the **display mpls l2vpn vpws** command to check whether VPWS service configurations are correct.

Note the following points when using the **display mpls l2vpn vpws** command:

- If **interface** *interface-type interface-number* is specified, only VPWS service information on a specified AC interface is displayed.
- If **verbose** is also specified, detailed information about the VPWS service on a specified AC interface is displayed.

Prerequisites

VPWS configurations are complete on the local end.

Example

Display VPWS service information.

```
<HUAWEI> display mpls l2vpn vpws

Pri : Primary          Sec : Secondary          Byp : Bypass
PWb : PW-bypass            ACb : AC-bypass

Access Circuit            Virtual Circuit            States Active   Role
GE0/0/2                  10.3.3.9:200                 Up     Active   Pri
                      10.2.2.9:201                Up     Inactive Sec
```

Table 10-63 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.

Item	Description
Virtual Circuit	Virtual circuit.
States	VC status, which can be: ● Up ● Down
Active	Activation status of a VC, which can be: ● Active ● Inactive
Role	Role of a PW, which can be: ● Pri: Primary PW ● Sec: Secondary PW ● PWb: PW-bypass ● ACb: AC-bypass ● Byp: Bypass

Display the detailed information about the VPWS service on a specified AC interface.

```
<HUAWEI> display mpls l2vpn vpws interface gigabitethernet 0/0/2 verbose

Access circuit     : GigabitEthernet0/0/2
Interface state    : Up
Protect mode       : FRR

Members:
Virtual Circuit              States Active   Role
10.3.3.9:200                  Up     Active   Primary
10.2.2.9:201                  Up     Inactive Secondary

Primary:
 VC type                : LDP VC
 VC state               : up
 Peer IP                : 10.3.3.9
 VC ID                  : 200
 Encapsulation type     : Ethernet
 LDP session state      : up
 VC information (Local / Remote)
  Label                 : 1025 / 1024
  MTU                   : 1500 / 1500
  Control word          : enable / enable
  Status code           : 0x0 / 0x0
  Group ID              : 0 / 0
  VCCV status           : cw alert ttl lsp-ping bfd / cw alert ttl lsp-ping bfd
 VC last up time        : 2013/12/21 16:42:51
 VC total up time       : 0 days, 6 hours, 20 minutes, 0 seconds

Secondary:
 VC type                : LDP VC
 VC state               : up
 Peer IP                : 10.2.2.9
 VC ID                  : 201
 Encapsulation type     : Ethernet
 LDP session state      : up
 VC information (Local / Remote)
  Label                 : 1026 / 1025
```

```
  MTU                 : 1500 / 1500
  Control word          : enable / enable
  Status code           : 0x0 / 0x0
  Group ID              : 0 / 0
  VCCV status           : cw alert ttl lsp-ping bfd / cw alert ttl lsp-ping bfd
 VC last up time        : 2013/12/21 14:57:13
 VC total up time       : 0 days, 20 hours, 44 minutes, 40 seconds
```

Table 10-64 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.
Protect mode	Protection mode, which can be FRR, independent, or master.
Members	PW member.
Virtual Circuit	Virtual circuit.
States	VC status
Active	Activation status of a VC, which can be:
Role	Role of a PW, which can be: ● Pri: Primary PW ● Sec: Secondary PW ● PWb: PW-bypass ● ACb: AC-bypass ● Byp: Bypass
Primary	Information about the primary PW.
VC type	The type of a VC.
VC state	VC status.
Peer IP	IP address of a peer.
VC ID	ID of a VC. The value is an integer in decimal notation. The default value is 0.
Encapsulation type	Encapsulation type of a VC.
LDP session state	Status of an LDP session.
VC information (Local / Remote)	VC information (local/remote).
Label	VC label.
MTU	Maximum transmission unit of a VC interface.
Control word	Whether the control word is enabled.

Item	Description
Status code	Status code, which can be: - 0x0: indicates the forwarding state. - 0x1: indicates the non-forwarding state. - 0x06: indicates the ACOAM fault. - 0x18: indicates the public network fault. - 0x20: indicates the standby state.
Group ID	Group ID.
VCCV status	VCCV status.
VC last up time	Time when the VC last goes Up.
VC total up time	Total Up time of a VC.
Secondary	Information about the secondary PW.

10.5.17 display mpls label-stack vll interface

Function

The **display mpls label-stack vll interface** command displays information about label stacks in VLL networking.

Format

display mpls label-stack vll interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about label stacks in VLL networking, run the **display mpls label-stack vll interface** command.

Example

Display information about the label stack on VLANIF100 in VLL networking.

```
<HUAWEI> display mpls label-stack vll interface vlanif 100
Label-stack  : 1
Level        : 1
Type         : VLL primary
Label        : 1027
Level        : 2
Type         : LDP
Label        : --
OutInterface : Vlanif1024
```

Table 10-65 Description of the **display mpls label-stack vll interface** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

10.5.18 display mpls static-l2vc

Function

The **display mpls static-l2vc** command displays information about static VCs on the device.

Format

display mpls static-l2vc [*vc-id* | **interface** *interface-type interface-number* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
vc-id	Displays information about a static VC with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about all static PWs on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you run the **display mpls static-l2vc** command with the interface name specified, information about static VCs on the interface connected to a CE is displayed. If no interface is specified, information about static VCs on all interfaces is displayed.

Example

Display information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : active
  Link State           : down
  Tunnel Policy Name   : tun
  PW Template Name     : --
  Main or Secondary    : Main
```

```
load balance type    : flow
Access-port          : false
VC tunnel/token info : 1 tunnels/tokens
NO.0  TNL type       : lsp   , TNL ID : 0x800802
Backup TNL type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
VC last up time      : 2011/07/04 20:29:18
VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
CKey                 : 2
NKey                 : 1
BFD for PW           : unavailable
```

Table 10-66 Description of the **display mpls static-l2vc** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up ● down
VC State	Status of the VC: ● up ● down
VC ID	ID of the VC, which uniquely identifies a VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Label Status	Whether the label can be used: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.

Item	Description
Token Status	Whether the token can be used: - 0: The token can be used. - 1: Wait for the SMB to confirm the token status. - 2: The token is released. - 3: SMB confirmation failed.
Control Word	Whether the control word function is enabled: - enable - disable
VCCV Capability	Whether VCCV is enabled.
active state	Whether the PW is in active state. A PW in active state can forward packets. - active - inactive
Link State	Integrative PW status: - up - down If any of the following status is Down, the PW link state is Down: - Service PW status - OAM status
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: - flow: indicates flow-based load balancing. - packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: - true: indicates that the interface supports the access-port attribute. - false: indicates that the interface does not support the access-port attribute.
VC Tunnel/token info	Information about the VC tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
NO.0 TNL Type	Type of the tunnel used by the PW

Item	Description
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

Display information about static VCs on VLANIF 10.

```
<HUAWEI> display mpls static-l2vc interface vlanif 10
 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : active
  Link State           : down
  Tunnel Policy        : tun
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
  VC last up time      : 2011/07/04 20:29:18
  VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
  CKey                 : 2
  NKey                 : 1
  Diffserv Mode        : uniform
  Service Class        : be
  Color                : --
  DomainId             : --
```

```
Domain Name          : --
BFD for PW          : unavailable
```

Table 10-67 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the link between the PE and its directly connected CE.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	VC label sent by the local device.
Receive VC Label	VC label received by the local device.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy	Name of the tunnel policy. The value -- indicates that no tunnel policy is configured.
PW Template Name	Name of the PW template. The value -- indicates that no PW template is configured.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
VC tunnel/token info	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Diffserv Mode	QoS DiffServ mode for VLL services.
Service Class	QoS service class for VLL services.
Color	QoS color for VLL services.

Item	Description
DomainId	ID of a domain.
Domain Name	Name of a domain.
BFD for PW	Whether BFD is configured. - unavailable: indicates that BFD is not configured. - available: indicates that BFD is configured. - timeout: timeout period after which a BFD session fails to be established

Display information about SVCs in Up state between peers.

```
<HUAWEI> display mpls static-l2vc state up
 Total svc connections:  1,  1 up,  0 down
 *Client Interface     : Vlanif10 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 2.2.2.2
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 4 hours, 55 minutes, 41 seconds
  UP time              : 0 days, 4 hours, 55 minutes, 40 seconds
  Last change time     : 0 days, 4 hours, 55 minutes, 40 seconds
  VC last up time      : 2011/09/09 10:25:22
  VC total up time     : 0 days, 4 hours, 55 minutes, 40 seconds
  CKey                 : 19
  NKey                 : 1
  BFD for PW           : unavailable
```

Table 10-68 Description of the **display mpls static-l2vc state** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC.
VC State	Status of the VC.

Item	Description
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

10.5.19 display mpls static-l2vc brief

Function

The **display mpls static-l2vc brief** command displays brief information about static VCs on the device.

Format

display mpls static-l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls static-l2vc brief** command is recommended when a large number of static VCs are configured on the device.

Example

Display brief information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc brief
Total svc connections:  2,  1 up,  1 down

 *Client Interface            : Eth-Trunk2  is up
  AC Status                   : up
  VC State                    : up
  VC ID                       : 0
  VC Type                     : VLAN
  Destination                 : 10.1.1.1

 *Client Interface            : Eth-Trunk3  is down
  AC Status                   : down
  VC State                    : down
  VC ID                       : 100
  VC Type                     : Ethernet
  Destination                 : 10.1.1.2
```

Table 10-69 Description of the **display mpls static-l2vc brief** command output

Item	Description
Total SVC Connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.

Item	Description
VC ID	ID of the static VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	IPv4 address of the peer. Generally, the value is the loopback address of the peer.

10.5.20 display traffic-statistics l2vpn interface

Function

The **display traffic-statistics l2vpn interface** command displays VLL traffic statistics on a specified interface.

Format

display traffic-statistics l2vpn interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays VLL traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After enabling the function of collecting L2VPN traffic statistics by running the **mpls l2vpn traffic-statistics enable** command, you can run the **display traffic-statistics l2vpn interface** command to view traffic statistics on the created VLL. The VLL traffic sent and received through the interface are collected from the time when the VLL becomes Up to the time you run the **display traffic-statistics l2vpn interface** command.

Example

Display VLL traffic statistics on VLANIF10.

```
<HUAWEI> display traffic-statistics l2vpn interface vlanif 10
 Input: 1000 bytes, 10 packets
 Output: 2000 bytes, 20 packets
```

10.5.21 display vll ccc

Function

The **display vll ccc** command displays information about a CCC connection.

Format

display vll ccc [*ccc-name* | **type** { **local** | **remote** }]

Parameters

Parameter	Description	Value
ccc-name	Specifies the connection name.	The value is an existing connection name.
type	Specifies the CCC connection type.	-
local	Displays local CCC connections.	-
remote	Displays remote CCC connections.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a CCC connection is configured, you can use the **display vll ccc** command to see whether the configuration is successful.

If you do not specify a connection name or type, information about all the existing CCC connections is displayed.

Example

Display a specified CCC connection.

```
<HUAWEI> display vll ccc CE1-CE2
name: CE1-CE2, type: remote, state: up
intf: Vlanif11 (up ethernet), in-label: 116 ,
out-label: 119 , nexthop: 10.1.1.1
no control word
VC last up time : 2009/10/08 13:38:01
VC total up time: 0 days, 0 hours, 11 minutes, 2 seconds
```

Display information about all the CCC connections.

```
<HUAWEI> display vll ccc
total  ccc vc : 1
local  ccc vc : 0,  0 up
remote ccc vc : 1,  1 up

name: CE1-CE2, type: remote, state: up,
intf: Vlanif11 (up), in-label: 116 , out-label: 119 , nexthop: 10.1.1.1
VC last up time : 2009/10/08 13:38:01
VC total up time: 0 days, 0 hours, 10 minutes, 50 seconds
```

Table 10-70 Description of the display vll ccc command output

Item	Description
total ccc vc	Total number of CCC local connections and remote connections at the local end.
local ccc vc	The number of CCC local connections at the local end.
remote ccc vc	The number of CCC remote connections at the local end.
name	Name of CCC connection in a character string.
type	Types of CCC connections. ● local: connection between two CEs that are connected to the same PE. ● remote: connection between CEs that are connected to two different PEs.

Item	Description
state	Status of a CCC connection: - down: indicates that the CCC connection fails because the configuration is incorrect or the associated interface is Down. - up: indicates that the CCC connection is set up successfully.
intf	Interface connected to the CCC connection. The S300, S500, S2700, S5700, and S6700 supports only VLANIF interfaces to be connected to CCC connections. By default, the Ethernet encapsulation type is adopted.
in-label	Incoming label of the CCC connection that is specified manually. It is consistent with the outgoing label of the peer end.
out-label	Outgoing label of the CCC connection which is specified manually. It is consistent with the incoming label of the peer end.
nexthop	Next-hop address of the CCC connection.
VC last up time	Indicates the last time the VC was Up.
VC total up time	Indicates the total duration the VC is Up.

Display information about all the local CCC connections.

```
<HUAWEI> display vll ccc type local
total local  ccc vc : 1,  1 up
name: c2, type: local, state: up,
intf1: Vlanif10 (up),  access-port: false

intf2: Vlanif11 (up),  access-port: false
VC last up time : 2009/03/23 11:16:07
VC total up time: 0 days, 0 hours, 14 minutes, 14 seconds
```

Table 10-71 Description of the display vll ccc type local command output

Item	Description
total local ccc vc	Total number of local CCC connections and the number of local CCC connections whose status is Up.
name	Name of the CCC connection in a character string.
type: local	Information about the local CCC connection. Local indicates the connection between two CEs that are connected to a PE.

Item	Description
state	Status of a CCC connection: - down: indicates that the CCC connection fails to be set up. The cause may be that the configuration is incorrect or the associated interface is Down. - up: indicates that the CCC connection is successfully set up.
intf1: Vlanif10 (up), intf2: Vlanif11 (up)	Interfaces of the local connection on two CEs. One is Vlanif10(the status is Up), and the other is Vlanif11(the status is Up).
access-port	Whether the interface supports the access-port attribute. - true: indicates that the interface supports the access-port attribute. - false: indicates that the interface does not support the access-port attribute.

Display information about all the remote CCC connections.

```
<HUAWEI> display vll ccc type remote
total remote ccc vc : 1,  1 up
name: CE1-CE2, type: remote, state: up,
intf: Vlanif11 (up), in-label: 116 , out-label: 119 , nexthop: 10.1.1.1
VC last up time : 2007/10/08 13:38:01
VC total up time: 0 days, 0 hours, 18 minutes, 10 seconds
```

Table 10-72 Description of the display vll ccc type remote command output

Item	Description
total remote ccc vc	Total number of remote CCC connections and the number of remote CCC connections whose status is Up.
name	Name of CCC connection in a character string.
type: remote	Type of the displayed CCC connection. The word **remote** indicates that the connection is of the remote type.
state	Status of a CCC connection: - down: indicates that the CCC connection fails to be set up. The cause may be that the configuration is incorrect or the associated interface is Down. - up: indicates that the CCC connection is successfully set up.

Item	Description
intf: Vlanif11 (up)	Access interface on the CE for setting up CCC connection at the local end. The interface is Vlanif11, and its status is Up.
in-label	Incoming label of the CCC connection. The label is manually specified, and is consistent with the outgoing label of the peer.
out-label	Outgoing label of the CCC connection. The label is manually specified, and is consistent with the incoming label of the peer.
nexthop	Next-hop address of the CCC connection.

10.5.22 interface-parameter-type vccv (interface view)

Function

The **interface-parameter-type vccv** command configures Mapping packets to carry the VCCV byte.

The **undo interface-parameter-type vccv** command deletes the VCCV byte (an interface parameter) in the Mapping packet.

By default, a Mapping packet carries the VCCV byte.

Format

interface-parameter-type vccv [**secondary**]

undo interface-parameter-type vccv [**secondary**]

Parameters

Parameter	Description	Value
secondary	Indicates that the configuration applies to the secondary VC. If this keyword is not specified, the command applies to the primary VC. The command can be configured only when a local VC exists.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The command can be configured only when a local VC exists.

Example

When configuring the VLL in LDP mode on an interface, delete the VCCV byte in the Mapping packet.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] undo interface-parameter-type vccv
```

10.5.23 ignore-mtu-match (MPLS-L2VPN instance view)

Function

The **ignore-mtu-match** command disables the MTU matching check of the L2VPN on both ends.

The **undo ignore-mtu-match** command enables the check.

By default, the PE checks whether MTUs of the L2VPN instances on both ends are consistent.

Format

ignore-mtu-match

undo ignore-mtu-match

Parameters

None

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, if a Huawei device connects to a non-Huawei device that does not support MTU matching check, run the **ignore-mtu-match** command to configure the Huawei device to ignore the check.

Prerequisites

vpn-target is not configured for the L2VPN instance.

Precautions

By default, a PE checks whether MTUs of the L2VPN instances at both ends are consistent. If not, the VC cannot be in the Up state.

Example

Ignore the check of MTU of the L2VPN instance named vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] ignore-mtu-match
```

10.5.24 l2vpn-family

Function

The **l2vpn-family** command displays the BGP-L2VPN address family view.

The **undo l2vpn-family** command deletes all configurations in the BGP-L2VPN address family view.

NOTE

You can run this command on the S5731S-S or S6730S-S to enter the BGP-L2VPN address family view but cannot configure VLL configuration commands in this view.

Only MPLS-capable devices support the VLL configuration commands in the BGP-L2VPN address family view. For the S5731-S and S6730-S, when the MPLS function license is not obtained, you can run this command to enter the BGP-L2VPN address family view but cannot configure VLL configuration commands in this view.

Format

l2vpn-family

undo l2vpn-family

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

In Kompella VLL networking, you can run the **l2vpn-family** command to enter the BGP-L2VPN address family view.

Example

Display the BGP-L2VPN address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family
[HUAWEI-bgp-af-l2vpn]
```

10.5.25 manual-set pw-ac-fault

Function

The **manual-set pw-ac-fault** command simulates a fault on the primary or secondary PW.

The **undo manual-set pw-ac-fault** command cancels the fault that is simulated on a primary or secondary PW.

By default, no fault is simulated on a PW.

Format

manual-set pw-ac-fault [**secondary**]

undo manual-set pw-ac-fault [**secondary**]

Parameters

Parameter	Description	Value
secondary	Simulates a fault on the secondary PW. If this parameter is not specified, a fault is simulated on the primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where the primary and secondary PWs need to be configured, you can run the **manual-set pw-ac-fault** command to simulate a fault on the primary or secondary PW to check whether services can be switched between the primary and secondary PWs.

Prerequisites

A VC has been created.

Example

Simulate a fault on the PW.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] manual-set pw-ac-fault
```

10.5.26 mpls l2vc

Function

The **mpls l2vc** command creates a Martini VLL.

The **undo mpls l2vc** command deletes the Martini VLL from an interface.

By default, no Martini L2VPN connection is created.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**] *

undo mpls l2vc [**secondary** | **bypass**]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies a L2VC ID.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
group-id *group-id*	Specifies a VC group ID. With the VC group ID specified, the system can execute the same operation on a group of VCs; therefore, fewer packets are exchanged between PEs. Only the VCs with the same attribute can be configured with the same VC group ID; otherwise, the PW may be torn down by mistake. This parameter is valid only on sub-interfaces.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Removes the provider-tag (P-Tag) from a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-
tagged	Retains the P-Tag in a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-

Parameter	Description	Value
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
mtu *mtu-value*	Specifies the MTU value. **NOTE** This parameter can be configured only on VLANIF interfaces. The MTU of another type of interface or its sub-interface can be configured in the PW template.	The value is an integer that ranges from 46 to 9600. The default value is 1500.
secondary	Indicates a secondary VC. If this parameter is not specified, a primary VC is created. You can configure a secondary VC only when the primary VC exists on the local device.	-
bypass	Indicates that the VC is a bypass VC. The encapsulation type of the bypass VC must be the same as that of the primary VC.	-
ignore-standby-state	Indicates that the PW ignores standby state information sent by the remote device.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

According to different encapsulation modes on the AC interfaces, the system processes user packets in different ways, as shown in the following tables.

- Packet processing on the inbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Removes a tag.	No action is required.
Ethernet main interfaces	No action is required.	Adds a tag.
QinQ stacking sub-interface	No action is required.	Adds a tag.
QinQ termination sub-interface (in symmetrical mode)	Removes the outer tag.	No action is required.
QinQ termination sub-interface (in asymmetrical mode)	Removes two tags.	Removes the outer tag.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Adds a tag (default VLAN ID of the interface).
VLANIF interface (added to the VLAN in non-default mode)	Removes the outer tag.	No action is required.

- Packet processing on the outbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Adds a tag.	No action is required.
Ethernet main interfaces	Adds a tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.
QinQ stacking sub-interface	No action is required.	Removes a tag.
QinQ termination sub-interface (in symmetrical mode)	Adds the outer tag.	Replaces the outer tag with the tag that is encapsulated on the outbound interface.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
QinQ termination sub-interface (in asymmetrical mode)	Adds two tags.	Removes the outer tag and then adds two tags that are encapsulated on the outbound interface.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Removes a tag.
VLANIF interface (added to the VLAN in non-default mode)	Adds the outer tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You must create dynamic VCs on PEs at both ends of a PW to connect the PEs. The destination address of a VC is the LSR ID of the peer PE.
- You can set attributes for a PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring an LDP PW, you can directly apply the PW template without specifying attributes for the PW. After setting attributes for a PW template, you can update the PW template at any time. The modified PW template takes effect only after the **reset pw** command is run.
- If a PW attribute is specified in the **mpls l2vc** command, the corresponding PW attribute in the same PW template is invalid.
- If you do not specify a tunnel policy for a Martini connection, the default tunnel policy is used. By default, the LSP tunnel is preferentially selected and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the switch and other devices.
- You must configure the primary PW before configuring the secondary PW and delete the secondary PW before deleting the primary PW.
- When creating VCs dynamically, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.
- When configuring BFD for static PW, the VC ID must be specified.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

Create a Martini connection on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.2.2.9 100
```

Create a Martini connection on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls l2vc 10.2.2.9 100
```

10.5.27 mpls l2vpn

Function

The **mpls l2vpn** command enables MPLS L2VPN and displays the MPLS L2VPN view.

The **undo mpls l2vpn** command disables MPLS L2VPN and deletes all the L2VPN configurations.

By default, the MPLS L2VPN function is disabled.

Format

mpls l2vpn

undo mpls l2vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MPLS L2VPN functions or perform configurations in the MPLS L2VPN view on the MPLS L2VPN network, run the **mpls l2vpn** command to enable MPLS L2VPN and enter the MPLS L2VPN view.

Prerequisites

Basic MPLS functions have been configured. For details, see the **mpls lsr-id** and **mpls** commands.

Precautions

When the command is configured, a P device does not need to be enabled with the MPLS L2VPN function.

After the **mpls l2vpn** command is executed:

- If MPLS L2VPN is disabled on the device, MPLS L2VPN is enabled and the MPLS L2VPN view is displayed.
- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

NOTICE

After the **undo mpls l2vpn** command is run in the system view, L2VPN services may be interrupted, and all L2VPN configurations are cleared. If you want to restore the L2VPN configurations, re-run all the deleted commands.

Example

Enable MPLS L2VPN.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn]
```

10.5.28 mpls l2vpn alarm verification disable

Function

The **mpls l2vpn alarm verification disable** command disables MPLS L2VPN alarm verification.

The **undo mpls l2vpn alarm verification disable** command enables MPLS L2VPN alarm verification.

By default, MPLS L2VPN alarm verification is enabled.

Format

mpls l2vpn alarm verification disable

undo mpls l2vpn alarm verification disable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

If MPLS L2VPN alarm verification is enabled on a device, the device regularly sends service alarms to the fault management (FM) module until these alarms are cleared. The FM then compares received alarms with locally stored alarms. If a received alarm is different from any of the locally stored alarms, the FM module reports the alarm to the NMS. If a received alarm is the same as a locally stored alarm, the FM module does not report this alarm.

Sometimes, alarms cleared on the device may still be displayed on the NMS. To ensure alarm consistency between the device and NMS, the FM module ages out such alarms after three alarm verification intervals and then instructs the NMS to delete these alarms. This function effectively eliminates alarm residue to improve alarm reliability.

If a large number of services exist, MPLS L2VPN alarm verification may regularly drive the CPU usage to a high level, affecting service performance. In this case, you can run the **mpls l2vpn alarm verification disable** command to disable MPLS L2VPN alarm verification. After MPLS L2VPN alarm verification is disabled, the device sends service alarms to the FM module only once, and the FM module cannot age out cleared alarms.

Example

Disable MPLS L2VPN alarm verification.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn alarm verification disable
```

10.5.29 mpls l2vpn default martini

Function

The **mpls l2vpn default martini** command configures the dynamic VC signaling not to carry status information.

The **undo mpls l2vpn default martini** command restores the default configuration.

By default, the dynamic VC signaling carries status information.

Format

mpls l2vpn default martini

undo mpls l2vpn default martini

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

To configure the dynamic VC signaling not to carry status information in VLL scenarios, run the **mpls l2vpn default martini** command. In other scenarios, do not run this command.

NOTE

- If the dynamic VC signaling carries status information, the local end can send Notification messages to the peer end. For details about Notification messages, see Chapter "PWE3 Principles" in the "PWE3 Configuration".
- Before using the **mpls l2vpn default martini** command, you must delete the configurations of VCs (including PWE3 VCs and VPLS VCs) that support Notification messages.

Example

Configure the dynamic VC signaling not to carry status information.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn default martini
```

Restore the default dynamic VC signaling configuration.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] undo mpls l2vpn default martini
```

10.5.30 mpls l2vpn flow-label

Function

The **mpls l2vpn flow-label** command enables flow label-based load balancing for PWs on an interface.

The **undo mpls l2vpn flow-label** command disables flow label-based load balancing for PWs on an interface.

By default, flow label-based load balancing is disabled for PWs on an interface.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label [**secondary**]

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-
secondary	Enables flow label-based load balancing for the secondary PW. If **secondary** is not configured, flow label-based load balancing is configured for the primary PW. Flow label-based load balancing can be configured for a secondary PW only if the secondary PW exists.	-
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between provider (P) devices, configure flow label-based load balancing to improve L2VPN traffic forwarding efficiency. After flow label-based load balancing is enabled on a PE, the PE adds different labels for different

L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it performs the Hash calculation and selects a forwarding path based on the flow label in the data packet. This processing implements load balancing. You can run the **mpls l2vpn flow-label** command to enable flow label-based load balancing for L2VPN on an interface.

Prerequisites

Before you enable flow label-based load balancing for an interface, create a VC connection on this interface and enable Multiprotocol Label Switching (MPLS) L2VPN.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.
- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

The **secondary** parameter indicates that flow label-based load balancing takes effect only for the secondary PW. If you specify **secondary** parameter, flow label-based load balancing takes effect only for the primary PW.

Example

Enable flow label-based load balancing for PWs on Vlanif 100.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif100] mpls l2vpn flow-label both
```

10.5.31 mpls l2vpn ip-parse enable

Function

The **mpls l2vpn ip-parse enable** command enables the IP packet parsing function of the MPLS L2VPN module.

The **undo mpls l2vpn ip-parse enable** command disables the IP packet parsing function of the MPLS L2VPN module.

By default, the IP packet parsing function of the MPLS L2VPN module is enabled.

Format

mpls l2vpn ip-parse enable

undo mpls l2vpn ip-parse enable

NOTE

This command is supported only on the S6720-EI and S6720S-EI.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Layer 2 VPN scenario, if a traffic policy is configured in the inbound direction of an AC-side interface on a device, L2VPN traffic forwarded from a PE may incorrectly match the traffic policy. As a result, traffic fails to be forwarded. To ensure normal traffic forwarding, run the **undo mpls l2vpn ip-parse enable** command to disable the IP packet parsing function of the MPLS L2VPN module.

Precautions

If the enhanced load balancing mode is configured for an Eth-Trunk, it is recommended that the IP packet parsing function of the MPLS L2VPN module be enabled.

Example

Disable the IP packet parsing function of the MPLS L2VPN module.

```
<HUAWEI> system-view
[HUAWEI] undo mpls l2vpn ip-parse enable
```

10.5.32 mpls l2vpn l2vpn-name

Function

The **mpls l2vpn** *l2vpn-name* command creates a L2VPN instance in the Kompella mode.

The **undo mpls l2vpn** *l2vpn-name* command deletes the L2VPN instance.

By default, no Kompella L2VPN instance is created.

Format

mpls l2vpn *l2vpn-name* [**encapsulation** *encapsulation* [**control-word** | **no-control-word**]]

undo mpls l2vpn *l2vpn-name*

Parameters

Parameter	Description	Value
l2vpn-name	Specifies a L2VPN instance name.	The value must be an existing VPN instance name.
encapsulation *encapsulation*	Indicates the encapsulation type of the L2VPN instance. The encapsulation type can be **ethernet** or **vlan**.	-
control-word | **no-control-word**	Enables or disables the control word. By default, the control word is disabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use this command to create a VPN.

Precautions

The specified encapsulation of an L2VPN must be the same as that of the CE interface.

Example

Create a VPN in Kompella mode.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1]
```

Enter the MPLS-L2VPN instance view.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1]
```

10.5.33 mpls l2vpn pw bfd

Function

The **mpls l2vpn pw bfd** command enables dynamic BFD for PWs and adjusts BFD parameters on an AC interface.

The **undo mpls l2vpn pw bfd** command restores default BFD parameters of dynamic BFD for PWs on an AC interface.

By default, dynamic BFD for PWs is not configured on an AC interface.

Format

mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** | **min-rx-interval** | **min-tx-interval**] * [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

Parameters

Parameter	Description	Value
detect-multiplier *multiplier*	Specifies the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.
min-rx-interval *rx-interval*	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the minimum interval for sending BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
remote-vcid *vc-id*	Specifies the VC ID of the peer device.	This parameter is mandatory when a multi-hop PW is detected. The value of this parameter is the VC ID of the remote end of the PW. The value is an integer that ranges from 1 to 4294967295.
secondary	Configures BFD and its parameters on the secondary PW. By default, BFD and its parameters are configured on the primary PW. **NOTE** The **secondary** parameter cannot be run on Loopback interface view.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where BFD is used to detect faults, run the **mpls l2vpn pw bfd** command to enable dynamic BFD for PWs and adjust BFD parameters on an AC interface.

Precautions

To reduce usage of system resources, when a BFD session is detected in Down state, the system changes the minimum interval for receiving BFD packets and the minimum interval for sending BFD packets to random values between 1000 ms and 3000 ms. When the BFD session becomes Up, the configured intervals are restored.

Example

Enable dynamic BFD for PWs on VLANIF 10 and set BFD parameters.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] mpls l2vpn pw bfd min-rx-interval 100 min-tx-interval 100
```

10.5.34 mpls l2vpn reroute

Function

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

The **undo mpls l2vpn reroute** command restores the default revertive switchover policy.

By default, delayed revertive switchover is configured in FRR or PW redundancy master/slave mode.

Format

mpls l2vpn reroute { { **delay** *delay-time* | **immediately** } [**resume** *resume-time*] | **never** }

undo mpls l2vpn reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies the revertive switchover policy for the primary and secondary PWs as delayed revertive switchover, and sets the duration for delayed switchover.	The value is an integer that ranges from 10 to 1800, in seconds. The default value is 30.

Parameter	Description	Value
immediately	Specifies the revertive switchover policy for the primary and secondary PWs as immediate revertive switchover.	-
resume *resume-time*	Specifies a delay after which the local device notifies the peer PE on the secondary PW of the recovery. You can set this parameter only in VLL FRR mode.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 10.
never	Specifies the revertive switchover policy for the primary and secondary PWs to none revertive switchover. After the primary PW recovers, traffic is not switched to it until the secondary PW is faulty.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

Prerequisites

The primary and secondary PWs have been configured in FRR or PW redundancy master/slave mode. The revertive switchover policy cannot be configured for PW redundancy independent mode.

Precautions

In VLL FRR mode and in PW redundancy master/slave mode, the PW revertive switchover policy is classified into the following modes:

- Immediate revertive switchover: When the primary PW recovers from a fault, the local PE switches traffic back to the primary PW immediately and notifies the peer PE on the secondary PW of the fault. In FRR mode, the local PE notifies the peer PE on the secondary PW of the recovery after a delay of *resume-time*. In PW redundancy master/slave mode, the parameter *resume-time* is not supported.

  This revertive switchover applies to scenarios in which users hope traffic to be restored as soon as possible.

- Delayed revertive switchover: When the primary PW recovers from a fault, traffic is switched back to the primary PW after a period specified by *delay-time*. After traffic is switched back, the local device immediately notifies the peer device on the secondary PW of the fault. If *resume-time* is configured in FRR mode, the local device notifies the peer device on the secondary PW of the recovery after a delay of *resume-time*.

  On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.
- None revertive switchover: When the primary PW recovers from a fault, traffic is not switched back to the primary PW until the secondary PW becomes faulty.

  If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive switchover.

In a CE asymmetrical networking, if the Ethernet OAM function is configured on a PE interface connected to a CE, and a revertive switchover policy is configured, the value of *resume-time* cannot be 0 seconds. The value must be equal to or greater than 1 second.

Example

Configure the device to switch traffic back to the primary PW 15 seconds after the primary PW recovers from a fault, notify the peer PE on the secondary PW of the fault when a switchover is performed, and notify the peer PE of the secondary PW of the recovery 20 seconds later.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 10.1.1.9 100
[HUAWEI-Vlanif100] mpls l2vc 10.2.2.9 200 secondary
[HUAWEI-Vlanif100] mpls l2vpn reroute delay 15 resume 20
```

10.5.35 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL service or a PWE3 service.

The **undo mpls l2vpn service-name** command deletes the configured L2VPN service name.

By default, no L2VPN service name is configured in the system.

Format

mpls l2vpn service-name *service-name*

undo mpls l2vpn service-name

Parameters

Parameter	Description	Value
service-name	Specifies the name of an L2VPN service. This parameter uniquely identifies an L2VPN service on a PE.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC or Martini VLL service or a PWE3 service is uniquely identified by the combination of the VC ID and VC type, which are hard to remember and make maintenance complex. When a service name is used to uniquely identify an L2VPN service, the name can be defined based on requirements and the NMS operator can maintain the L2VPN service by clicking the name on the NMS graphical user interface (GUI). This simplifies operation and maintenance.

Prerequisites

An SVC or Martini VLL service or a PWE3 service has been configured on a service interface. A primary PW and a secondary PW can be configured for a Martini VLL or PWE3 service.

Precautions

On each PE, an L2VPN service name is unique. If an L2VPN service name has been used by a PW, it cannot be configured for another PW, or the system will display an error message.

If an L2VPN service already has a service name, this service name will be overwritten when a new name is configured for the L2VPN service. Therefore, when changing an L2VPN service name, you can directly configure a new service name without deleting the original one.

- Because the primary and secondary PWs are configured on the same interface, they are regarded as one PW, and a service name is configured for both of them.
- On each PE, an L2VPN service name is unique.

Example

Set an L2VPN service name to **pw1** on a service interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.1.1.1 1
[HUAWEI-Vlanif10] mpls l2vpn service-name pw1
```

10.5.36 mpls l2vpn vlan-stacking

Function

The **mpls l2vpn vlan-stacking** command configures the stacked VLAN ID for a main interface.

The **undo mpls l2vpn vlan-stacking** command deletes the stacked VLAN ID from a main interface.

By default, the system does not add a VLAN ID to a packet passing through the main interface.

Format

mpls l2vpn vlan-stacking stack-vlan *vlan-id*

undo mpls l2vpn vlan-stacking stack-vlan

Parameters

Parameter	Description	Value
stack-vlan *vlan-id*	Indicates the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the following conditions are met, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for a main interface:

- The VLL or VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts packets with one more VLAN tag.
- The local PE is connected to a computer by using a GE interface, XGE interface, 25GE interface, MultiGE interface, 40GE interface, 100GE interface, or Eth-Trunk interface as the AC interface.

In this scenario, the computer sends and receives all packets. After a VLAN is specified for the main interface, the local PE performs the following operations:

- The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.
- The local PE removes the outer VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Precautions

Before binding the main interface to the VLL or VSI, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for the main interface.

To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.

Example

Configure MPLS VLL on the main interface and add VLAN tag 80 to incoming packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/13
[HUAWEI-GigabitEthernet0/0/13] undo portswitch
[HUAWEI-GigabitEthernet0/0/13] mpls l2vpn vlan-stacking stack-vlan 80
[HUAWEI-GigabitEthernet0/0/13] mpls l2vc 10.0.0.17 20 tagged
```

10.5.37 mpls l2vpn traffic-statistics enable

Function

The **mpls l2vpn traffic-statistics enable** command enables the system to collect VLL traffic statistics.

The **undo mpls l2vpn traffic-statistics enable** command disables the system from collecting VLL traffic statistics.

By default, the system is disabled from collecting VLL traffic statistics.

Format

mpls l2vpn traffic-statistics enable

undo mpls l2vpn traffic-statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect traffic statistics in a VLL networking, use this command to the system to collect VLL traffic statistics.

Precautions

The system collects traffic statistics only for VLLs that are created after this command is executed.

You can view traffic statistics by running the **display traffic-statistics l2vpn interface** command.

Example

Enable the function that collects L2VPN traffic statistics.

```
<HUAWEI>system-view
[HUAWEI] mpls l2vpn traffic-statistics enable
Info: The modification can only take effect for newly created VC.
```

10.5.38 mpls l2vpn trigger if-down

Function

The **mpls l2vpn trigger if-down** command enables the notification of physical layer faults.

The **undo mpls l2vpn trigger if-down** command disables the notification of physical layer faults.

By default, the notification of physical layer faults is disabled.

Format

mpls l2vpn trigger if-down

undo mpls l2vpn trigger if-down

Parameters

None

Views

25GE interface view, 40GE interface view,100GE interface view, GE interface view, MultiGE interface view, or XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a VLL FRR networking, an AC must detect failures of the corresponding PW to trigger link switching. This command enables the notification of physical layer faults so that ACs can detect failures of PWs.

Precautions

After the notification of physical layer faults is enabled:

- When a physical layer fault occurs on the PW side, the local AC interface is Down.
- When a physical layer fault occurs on the AC side, the local PE notifies the peer PE of the fault and the peer AC interface is Down.

After the fault is rectified, the Down AC interface automatically becomes Up.

Example

Enable the notification of physical layer faults.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls l2vc 1.1.1.1 1
[HUAWEI-GigabitEthernet0/0/1] mpls l2vpn trigger if-down
```

10.5.39 mpls static-l2vc

Function

The **mpls static-l2vc** command creates a static VC.

The **undo mpls static-l2vc** command deletes the static VCs.

By default, no static VC is created.

Format

mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

undo mpls static-l2vc

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a static PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
transmit-vpn-label *transmit-label-value*	Specifies the value of a transmit label.	The value is an integer that ranges from 0 to 1048575.
receive-vpn-label *receive-label-value*	Specifies the value of a receive label.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *tnl-policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word | **no-control-word**	Enables or disables the control word function. By default, the control word function is disabled.	-
raw	Removes the provider-tag (P-Tag) from a packet.	-
tagged	Retains the P-Tag in a packet.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an L2VPN networking, you can use this command to create a static VC between two PEs connected to CEs.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You can set attributes for a static PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring a static PW, you can directly use the static PW template without specifying attributes for the PW. After setting attributes for a static PW template, you can update the static PW template at any time. The modified static PW template takes effect only after the **reset pw** command is run.
- Static VCs must be created on PEs at both ends. The destination address of a VC is the LSR ID of the peer PE. The transmit label of the PE at one end is the receive label of the PE at the other end. If the labels do not match, traffic may fail to be forwarded even though the **static-l2vc** field is displayed as Up.
- If no tunnel policy is specified, the default tunnel policy is used. The default policy specifies that traffic is forwarded along the LSP and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- When configuring a static VC, note that the value of the transmit label ranges from 0 to 1048575. This ensures the communication between the device and different types of devices.
- When creating static VCs, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

Configure a static VC. Set the LSR ID of the peer device to 1.1.1.1, transmit label to 100, and receive label to 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
```

Configure a static VC by applying a PW template and set values of the VC ID, transmit label, and receive label to 100 respectively.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc pw-template pwt 100 transmit-vpn-label 100 receive-vpn-label 100
```

Delete a static VC.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] undo mpls static-l2vc
```

10.5.40 mtu (MPLS-L2VPN instance view)

Function

The **mtu** command sets the Maximum Transmission Unit (MTU) of a L2VPN instance.

The **undo mtu** command restores the default configuration.

By default, the MTU of a L2VPN instance is 1500 bytes.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU of a L2VPN instance.	The value is a decimal integer that ranges from 46 to 16352 bytes.

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

The VPN MTU must be unique on the whole network.

If MTUs, which belong to the same VPN, on two PEs are different, the PEs cannot exchange VC information and set up connections.

After **vpn-target** is configured for the MPLS L2VPN instance, the MTU of the MPLS L2VPN cannot be changed.

In Kompella interworking with other venders' devices that do not support the MTU matching check, to ensure the VC keeps the Up state, you can perform the following configuration on the S300, S500, S2700, S5700, and S6700:

- Configuring an MTU the same as that of other venders' devices
- Using the **ignore-mtu-match** command for the system to ignore the MTU matching check

Example

Set the MTU.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1
[HUAWEI-mpls-l2vpn-vpn1] mtu 1000
```

10.5.41 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** [**remote** *remote-ip-address peer-pw-id* | **draft6**] * [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** **remote** *remote-ip-address peer-pw-id* **sender** *sender-address* [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address* | **draft6**] * [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **normal** [**no-control-word**] [**remote** *remote-ip-address peer-pw-id*] [**ttl** *ttl-value*] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **ip-interworking**, and **vlan**.

Parameter	Description	Value
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies the peer LSR ID of a local PW. In PWE3 and Martini VLL scenarios, if the VC IDs of the primary and secondary VCs are the same, this parameter must be specified to uniquely identify a PW.	The value is in dotted decimal notation.
-c *echo-number*	Specifies the number of Echo Request messages to be sent. If the network works unstably, you can set this parameter to a larger value to test network quality based on the packet loss ratio.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the interval for sending Echo Request messages. Each time after the source sends an Echo Request message by using the **ping vc** command, it waits a period of time (2000 ms by default) before sending the next Echo Request message. You can set the interval for sending Echo Request messages through the parameter *time-value*. If the network works unstably, the value should be greater than or equal to 2000 ms.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-s *data-bytes*	Specifies the number of bytes of the sent Echo Request messages.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100.
-t *timeout-value*	Specifies the timeout period for sending Echo Request messages.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.

Parameter	Description	Value
-exp *exp-value*	Specifies the EXP value of the sent Echo Request messages. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply messages. ● 1: No MPLS Echo Reply message is returned. ● 2: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply messages are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-v	Displays the detailed information.	-
no-control-word	Disables the control word function.	-
control-word	Enables the control word function. The switching node along a multi-segment PW does not transmit ping packets. When the control word function is enabled, you can ping only the termination node of the PW. Before using the control word to ping the PW, you must enable the control word for a PW.	-
remote	Specifies information about the PW on the remote PE. Information specified by the remote PE is finally encapsulated into the ping packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the ping packets is the information about the PW on the local end, which applies to single-segment PWs.	-

Parameter	Description	Value
peer-pw-id	Specifies the ID of the PW on the peer.	The value is an integer that ranges from 1 to 4294967295. By default, the peer PW ID is the same as the local PW ID.
draft6	Specifies the command version. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06". By default, the ping operation is performed based on RFC 4379.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire MPLS domain is considered as one hop and the IP TTL of the probe packet is reduced by one on the ingress and egress respectively.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of a multi-segment PW, if the ping operation is performed in control word mode, the IP address of the termination node must be specified. In MPLS router alert mode, the IP address of any switching node or the termination node can be specified. Then, the Echo Request message is sent to the peer and then sent back.	-
label-alert	Specifies the label alert mode. The switching node along a multi-segment PW sends ping packets forcibly. In MPLS router alert mode, you can ping any switching node along the PW.	-

Parameter	Description	Value
normal	Specifies the normal mode, that is, the TTL detection mode. In this mode, control word and router alert are not encapsulated in to MPLS Echo Request messages, and TTL values are used to detect PW connectivity.	-
ttl *ttl-value*	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default value is 64.
sender *sender-address*	Specifies a source address. For end-to-end detection of a multi-segment PW, a source IP address needs to be specified for a public network device that communicates with the remote PE. Generally, the source IP address is the address of the adjacent SPE or UPE.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect.

The **ping vc** command can be used to check a PW in the following scenarios:

VLL networking

Based on VLL types, the VLL PW ping can be classified into the following types:

- PWE3 VLL PW ping: In a PWE3 VLL networking, a PW ping is initiated to check the connectivity of a PW. A PWE3 VLL PW ping can be performed in control word mode, TTL mode, or label alert mode. In a ping test, a local PE sends an Echo Request message to the peer PE. After receiving the message, the peer PE abstracts and sends FEC information to the L2VPN module to determine whether the message has reached the egress. If so, the peer PE returns an Echo Reply message.
- Kompella VLL PW ping: A VLL PW ping is initiated to check the connectivity of a PW. Different from the PWE3 networking, the Kompella VLL does not need the PW template and supports the control word, TTL, and label alert modes.

VPLS networking

Based on the VPLS types, the VPLS PW ping can be classified into the following types:

- Martini VPLS PW ping: The Martini VPLS PW ping supports only the label alert mode. On a Hierarchical Virtual Private LAN Service (HVPLS) network, the Martini VPLS PW ping can only detect single-segment PWs. If an optional PW ID is configured and specified, the PW with the PW ID is detected. If the PW ID is not specified, the PW with a specified VSI ID is detected.
- Kompella VPLS PW ping: The Kompella VPLS PW ping supports only the label alert mode.

If a PW fault is detected by using the **ping vc** command, the **tracert vc** command can be used to locate the fault. Both the **ping vc** command and the **tracert vc** command can properly check the connectivity of PWs and locate faults.

Prerequisites

The MPLS module has been enabled on the device and works properly.

Precautions

control-word is recommended to detect the entire PW. Even though **label-alert** can be used to check the entire PW, the whole process is the same as the forwarding process only when **control-word** is used.

The execution of the **ping vc** command terminates when either of the following situations occurs:

- The ping packet reaches the egress.
- The TTL value of the ping packet reaches the upper threshold.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Run the **ping vc** command in label alert mode on the device to check the connectivity of an Ethernet PW.

```
<HUAWEI> ping vc ethernet 100 -c 10 -m 10 -s 65 -t 100 -v label-alert remote 2.2.2.2
  Reply from 2.2.2.2: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
  10 packet(s) transmitted
  10 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

10.5.42 ping vc vpn-instance

Function

The **ping vc vpn-instance** command detects the status of a PW and locates the faulty node when a PW goes Down.

Format

ping vc vpn-instance *vpn-name local-ce-id remote-ce-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * { **label-alert** [**no-control-word**] | **control-word** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-name*	Specifies the VPN name.	The value is an existing VPN instance name.
local-ce-id	Specifies the ID of the local CE.	The value is a decimal integer ranging from 0 to 249.
remote-ce-id	Specifies the ID of the local CE.	The value is a decimal integer ranging from 0 to 249.
-c *echo-number*	Specifies the number of the sent Echo Request packets.	The value is a decimal integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Indicates the interval for sending Echo Request packets.	The value is a decimal integer that ranges from 1 to 10000, in milliseconds. By default, the value is 2000.
-s *data-bytes*	Specifies the number of bytes of an Echo Request packet.	The value is a decimal integer ranging from 65 to 8100. By default, the value is 100.
-t *timeout-value*	Specifies the timeout period for sending Echo Request packets.	The value is a decimal integer ranging from 0 to 65535. By default, the value is 2000.
-exp *exp-value*	Specifies the EXP value in an outer label in an Echo Request packet.	The value is an integer ranging from 0 to 7.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode of sending Echo Reply packets. The meaning of each value is as follows: - 1: indicates no reply. - 2: indicates a reply with an IPv4 or IPv6 UDP datagram. - 3: indicates a reply with an IPv4 or IPv6 datagram carrying an MPLS router alert label. - 4: indicates a reply through the control channel of the application plane.	The value is a decimal integer ranging from 1 to 4. By default, the value is 2.
-v	Displays detailed information.	-
label-alert	Indicates that in the case of a multi-hop PW, ping packets are forcibly sent on the transit node. In Label Alert mode, you can ping all transit nodes of a PW.	-
no-control-word	Disables the control word mode.	-
control-word	Indicates that in the case of a multi-hop PW, ping packets are forwarded without being resolved. In the control word mode, you can ping only the egress of the PW. The ping in control word mode can be performed only after the control word of a PW is enabled.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

If the control-word is enabled for a PW, it is recommended that you specify the **control-word** parameter to detect the connectivity of the PW. This ensures that ping packets are transmitted in the same manner as data packets on the PW.

Example

Run the **ping vc vpn-instance** command in label-alert mode on the PE to detect the connectivity of the Kompella PW.

```
<HUAWEI> ping vc vpn-instance vpn1 1 2 -v label-alert
  Reply from 4.4.4.4: bytes=100 Sequence=1 time = 110 ms Return Code 3, Subcode 1
  Reply from 4.4.4.4: bytes=100 Sequence=2 time = 90 ms Return Code 3, Subcode 1
  Reply from 4.4.4.4: bytes=100 Sequence=3 time = 60 ms Return Code 3, Subcode 1
  Reply from 4.4.4.4: bytes=100 Sequence=4 time = 60 ms Return Code 3, Subcode 1
  Reply from 4.4.4.4: bytes=100 Sequence=5 time = 90 ms Return Code 3, Subcode 1

 --- FEC: L2 VPN ENDPOINT. Sender VEID = 1, Remote VEID = 2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 60/82/110 ms
```

Table 10-73 Description of the ping vc vpn-instance command output

Item	Description
Reply from	IP address of the Echo Reply packet
bytes	Length of the Echo Reply packet
sequence	Sequence number of the Echo Reply packet
return code	Return code of the Echo Reply packet: ● 1: Malformed echo request received ● 2: One or more of the TLVs was not understood ● 3: Replying router is an egress for the FEC at stack-depth ● 4: Replying router has no mapping for the FEC at stack-depth ● 5: Downstream Mapping Mismatch ● 6: Upstream Interface Index Unknown ● 7: Reserved ● 8: Label switched at stack-depth ● 9: Label switched but no MPLS forwarding at stack-depth ● 10: Mapping for this FEC is not the given label at stack-depth ● 11: No label entry at stack-depth ● 12: Protocol not associated with interface at FEC stack-depth ● 13: Premature termination of ping due to label stack shrinking to a single label
Subcode	Subcode of the Echo Reply packet (indicating the depth of the label stack in the packet)
FEC	FEC TLV type (L2 VPN ENDPOINT indicates the Kompella PW that is negotiated by BGP)
Sender VEID	ID of the local CE
Remote VEID	ID of the remote CE

10.5.43 reset bgp l2vpn

Function

The **reset bgp l2vpn** command resets the TCP connection of the BGP L2VPN.

Format

reset bgp l2vpn { *as-number* | *peer-ip-address* | **all** | **internal** | **external** }

Parameters

Parameter	Description	Value
as-number	Indicates the number of the AS to which an L2VPN peer belongs.	-
peer-ip-address	Indicates the IP address of an L2VPN peer.	-
all	Resets all the L2VPN BGP connections.	-
internal	Resets the L2VPN BGP connection in the same AS.	-
external	Resets the L2VPN BGP connection across ASs.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After the parameters configured in the BGP-L2VPN address family view are modified, you can run the **reset bgp l2vpn** command to reset the TCP connection of the BGP L2VPN. After that, BGP re-negotiates parameters, re-sends label information, and re-establishes the session.

If the BGP L2VPN application and other applications share the same TCP connection, the **reset bgp l2vpn** command resets BGP neighbor relationship of all applications on this TCP connection.

Example

Reset all the L2VPN BGP connections.

```
<HUAWEI> reset bgp l2vpn all
```

10.5.44 reset traffic-statistics l2vpn interface

Function

The **reset traffic-statistics l2vpn interface** command resets VLL traffic statistics on a specified interface.

Format

reset traffic-statistics l2vpn interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of a VLL AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To collect new VLL traffic statistics in a VLL networking, run the **reset traffic-statistics l2vpn interface** command to reset the current VLL traffic statistics on the specified interface, and collect VLL traffic statistics again

Example

Reset VLL traffic statistics on VLANIF10.

```
<HUAWEI> reset traffic-statistics l2vpn interface vlanif 10
```

10.5.45 route-distinguisher (MPLS-L2VPN instance view)

Function

The **route-distinguisher** command configures an RD for an MPLS L2VPN instance.

By default, no RD is configured in the MPLS L2VPN instance view.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD. The formats of an RD are as follows: - 16-bit AS number:32-bit user-defined number For example, 102:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. - 32-bit IP address:16-bit user-defined number For example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535. - Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. - 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that both range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0.	-

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, an L2VPN instance takes effect only after an RD is configured.

Precautions

VPNs on the same PE have different RDs. The same VPN can have the same RD or different RDs on different PEs.

To change the RD of an L2VPN instance, delete the L2VPN instance and create a new L2VPN instance.

Kompella VLL and Kompella VPLS must use different RDs.

Example

Set the RD of an MPLS L2VPN instance to 300:1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] route-distinguisher 300:1
```

Set the RD of an MPLS L2VPN instance to 1.1.1.1:5.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn2 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn2] route-distinguisher 1.1.1.1:5
```

Set the RD of an MPLS L2VPN instance to 16.30:50.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn2 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn2] route-distinguisher 16.30:50
```

10.5.46 tracert vc

Function

The **tracert vc** command detects the status of a PW or locates a faulty node on a PW in Down state.

Format

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-ip-address* [**ptn-mode** | **full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-pw-id* **draft6** [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, and **ip-interworking**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies a peer LSR ID for the local PW. In a PWE3 or Martini VLL scenario, if the primary and secondary VCs are configured with the same VC ID, this parameter must be specified to determine a unique PW to be monitored.	The value is in dotted decimal notation.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies the initial Time-to-Live (TTL).	The value is an integer that ranges from 1 to 255, and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from 1 to 255, and must be larger than the value of *first-ttl*. The default value is 30.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets. ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated in IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated in IPv4/IPv6 /IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4.
-t *timeout-value*	Specifies the timeout interval of an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
control-word	Indicates that the control word is encapsulated in the MPLS Echo Request packet.	-
label-alert	Indicates that the router alert label is encapsulated in the MPLS Echo Request packet.	-
no-control-word	Indicates that the control word is not encapsulated in the MPLS Echo Request packet.	-
normal	Indicates the normal mode where the router alert label and control word are not encapsulated in the MPLS Echo Request packet.	-
remote	Specifies information about the PW on the remote PE.	-

Parameter	Description	Value
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. If **label-alert** is configured, you can specify the IP address of any switching node or the termination node.	-
remote-pw-id	Specifies the ID of the remote PW. By default, the ID of the local PW is used. If the tracert operation is performed in control word mode for a multi-segment PW, the IP address of the termination node must be specified.	-
ptn-mode	Specifies the PTN mode. In a multi-segment PW scenario, this parameter is indicated that trace VC packets are replied. You need to run the **lspv pw reply ptn-mode** command on both the SPE and TPE.	-
full-lsp-path	Displays the responses from all nodes along the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, only the responses from the PW nodes along the LSP are displayed.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire domain is regarded as one hop and the IP TTL of the probe packet is reduced by one on both the ingress and egress.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-

Parameter	Description	Value
draft6	Specifies the version of the **tracert vc** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379. **NOTE** Tracert VC based on **draft6** is applied only to VLL over LDP scenarios.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a fault occurs on the PW, the **ping vc** command can be used to check the connectivity of the network, and the **tracert vc** command can be used to locate the fault and provide reference for fault diagnosis. If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. If a PW is down, the **tracert vc** command must be used to locate the faulty node on the PW.

The **tracert vc** command applies to the following networking scenarios:

- PWE3 VLL PW tracert

  In PWE3 VLL networking, PW tracert can help you obtain information about SPEs and Ps along the path that the message travels from the source to the destination, check the connectivity of the PW, and locate the fault of the PW.

  A PWE3 VLL PW tracert can be performed in control word mode, label alert mode, or TTL mode. The default mode is label alert. The TTL mode and control word mode are mutually exclusive.

  To detect faults on a VLL network with control word enabled, run the **tracert vc** *pw-type pw-id* **control-word** command.

  To encapsulate packets with the router alert label and detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* **label-alert** command.

  If control word is not enabled and packets are not encapsulated with the router alert label, to detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* command.

  The TTL value of the PW Tracert Request message is incremented by 1 each time. Each time the transit node (P) receives an Echo Request message after the TTL value of the message expires, it sends the Echo Request message to the LSPV module. Then the transit node returns an Echo Reply message carrying the next hop information.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.
- The MPLS module has been enabled on each node and works properly.
- The ICMP module of each node works properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert vc** command is as follows:

1. The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
2. The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
3. The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
4. The preceding steps continue until the MPLS Echo Request packet reaches the destination.

When the device on each hop receives the MPLS Echo Request packet, it will respond with an MPLS Echo Reply packet, indicating that the tracert test ends. In the command output information of the source device, you can view the path that the packet passes through.

Configuration Impact

In control word mode, if a transit node receives an MPLS Echo Request packet whose TTL does not time out, it does not send the packet to the CPU. In this mode, the source obtains only a little PW information and cannot obtain information about the downstream devices of the transit node. This mode is recommended when the traffic volume is heavy.

In router alert mode, a transit node sends the received MPLS Echo Request packets to the CPU. In this mode, the source obtains a lot of PW information; therefore, device performance is affected when the traffic volume is heavy. This mode is recommended when the traffic volume is light.

Information specified by **remote** is encapsulated in MPLS Echo Request packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the MPLS Echo Request packets is about the PW on the local PE. This applies to single-segment PWs.

Precautions

- When the probe packet reaches the egress or the TTL reaches the upper threshold, the PW tracert is terminated.
- You can press **Ctrl + C** to terminate the execution of the **tracert vc** command.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Trace a multi-segment PW. The encapsulation type, local PW ID, and remote PW ID of the PW is ethernet, 100, and 200.

```
<HUAWEI> tracert vc ethernet 100 control-word remote 200 draft6 full-lsp-path
 TTL   Replier           Time    Type      Downstream
 0                          Ingress   10.1.1.2/[1025 ]
 1     10.1.1.2          230 ms  Transit   10.2.1.2/[3 ]
 2     10.2.1.2          230 ms  Transit   10.3.1.2/[3 ]
 3     10.3.1.2          100 ms  Transit   10.4.1.2/[3 ]
 4     10.4.1.2          150 ms  Egress
```

Table 10-74 Description of the **tracert vc** command output

Item	Description
TTL	TTL value in an Echo Request packet. It represents the number of hops along the path through which an Echo Request packet passes.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time when the packet is processed.
Type	Node type. The value can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

10.5.47 tracert vc vpn-instance

Function

The **tracert vc vpn-instance** command detects the hop-by-hop connectivity of the LSP between PEs in the Kompella networking.

Format

tracert vc -vpn-instance *vpn-name local-ce-id remote-ce-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * { **control-word** | **label-alert** [**no-control-word**] | **draft6** } [**full-lsp-path**]

Parameters

Parameter	Description	Value
-vpn-instance *vpn-name*	Specifies the VPN instance name.	The value is an existing VPN instance name.
local-ce-id	Specifies the ID of the local CE.	It is a decimal integer ranging from 0 to 249.
remote-ce-id	Specifies the ID of the remote CE.	It is a decimal integer ranging from 0 to 249.
-exp *exp-value*	specifies value of the EXP field in an outer label in an Echo Request packet.	It is a decimal integer ranging from 0 to 7.
-f *first-ttl*	Specifies the value of the first TTL.	It is a decimal integer ranging from 1 to 255 and must be smaller than *max-ttl*. By default, the value is 1.
-m *max-ttl*	Specifies the value of the maximum TTL.	It is a decimal integer ranging from 1 to 255 and must be greater than the value of *first-ttl*. By default, the value is 30.
-r *reply-mode*	Specifies the mode in which the peer responds to the Echo Reply packet. The meaning of each value is as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 datagram carrying an MPLS router alert label. ● 4: indicates a reply through the control channel of the application plane.	It is a decimal integer ranging from 1 to 4.
-t *timeout-value*	Specifies the timeout period for waiting for MPLS Echo Reply packets.	The value is a decimal integer ranging from 0 ms to 65535 ms. By default, the value is 5.

Parameter	Description	Value
control-word	Indicates the control word encapsulated in packets.	-
label-alert	Indicates the router alert label encapsulated in packets.	-
no-control-word	Disables the control word mode.	-
draft6	Indicates the version of the command. If the parameter is specified, the command is implemented according to draft-ietf-mpls-lsp-ping-06. By default, the command is implemented according to RFC 4379.	-
full-lsp-path	Displays information about responses of all nodes along the LSP that an Echo Request packet passes. If this parameter is not specified, only the response of each PW node along the LSP is displayed.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

In a Kompella networking, if any node on the backbone network fails, use this command to identify the faulty node.

The **tracert vc vpn-instance** command applies to the following networking scenarios:

- Kompella VLL PW tracert

  In Kompella VLL networking, you can start a VLL PW tracert to check PW connectivity.

  A VLL PW tracert can help you obtain information about PEs and Ps along the path that the message travels from the source to the destination, check the connectivity of the Layer 2 forwarding link, and locate faults of the PW.

  Different from the PWE3 VLL PW tracert, the Kompella VLL tracert does not need the PW template and can be performed in control word mode or label alert mode. The default mode is label alert. Like PWE3 VLL PW tracert, Kompella VLL tracert can be enabled using a command.

Precautions

If the control word is encapsulated in MPLS echo request packets on a multi-hop PW, the packets on the switch node are not sent to the CPU for processing until the TTL times out. In control word mode, the source obtains less PW information, but the performance of the node is seldom affected and the source is unaware of the downstream information about this transit node. When there are a large number of packets, the control word mode is recommended.

After the router alert is encapsulated, in the case of a multi-hop PW, on the transit node, the Echo Request packet is sent to the CPU. In Label Alert mode, the source obtains more PW information. However, when a large number of packets are transmitted, the performance of the node degrades severely. The Label Alert mode is recommended when a small number of packets are transmitted on the network.

Example

Perform the Tracert test on the VPN instance named vpn1 in label-alert mode.

```
<HUAWEI> tracert vc -vpn-instance vpn1 1 2 label-alert full-lsp-path
 TTL   Replier            Time    Type      Downstream
 0                          Ingress   20.1.1.1/[21505 1026 ]
 1     20.1.1.1          60 ms   Transit   30.1.1.1/[1026 ]
 2     30.1.1.1          50 ms   Transit   40.1.1.1/[3 ]
 3     4.4.4.4          70 ms   Egress
```

Table 10-75 Description of the **tracert vc vpn-instance** command output

Item	Description
TTL	TTL of MPLS Echo Request packets, indicating the number of hops along the tunnel that the packets pass.
Replier	Source IP address in an Echo Reply packet.
Time	How long a packet is processed
Type	Type of a node: ● Ingress ● Transit ● Egress
Downstream	Address and label of the downstream node

10.5.48 vpn-target (MPLS-L2VPN instance view)

Function

The **vpn-target** command specifies VPN targets for an L2VPN.

The **undo vpn-target** command deletes the VPN targets specified for an L2VPN.

By default, no VPN target is specified for an L2VPN.

Format

vpn-target *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**] }

Parameters

Parameter	Description	Value
vpn-target	Adds a VPN target to the VPN. A VPN target can use any of the following formats: ● 16-bit AS number:32-bit user-defined number For example, 1:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, a VPN target cannot be 0:0. ● 32-bit IP address:16-bit user-defined number For example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-
import-extcommunity	Receives routing information carrying specified extended community attributes.	-
export-extcommunity	Specifies the extended community attributes carried in routing information to be sent.	-

Parameter	Description	Value
both	Specifies the extended community attributes of the received and the sent routing information.	-
all	Deletes all the VTs.	-

Views

MPLS-L2VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Kompella VLL networking, you can use this command to set the VPN target attribute for an L2VPN instance. The VPN target is used to set up a remote PW.

Precautions

If you do not specify any keywords, **both** is used by default.

Before configuring a VPN target, configure the Route Distinguisher (RD) for the L2VPN instance.

Example

Configure the VTs for an L2VPN named vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] vpn-target 100:1
[HUAWEI-mpls-l2vpn-vpn1] vpn-target 1:1 2:2 export-extcommunity
[HUAWEI-mpls-l2vpn-vpn1] vpn-target 1.2.3.4:11 12:12 import-extcommunity
```

Delete the VT of vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] undo vpn-target 12:12 import-extcommunity
```

Delete all the VTs of vpn1.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn vpn1 encapsulation vlan
[HUAWEI-mpls-l2vpn-vpn1] undo vpn-target all
```

10.6 PWE3 Configuration Commands

10.6.1 Command Support

Only the following switch models support PWE3:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

10.6.2 bfd bind pw

Function

The **bfd bind pw** command configures a BFD session to detect a PW.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is configured to detect a PW.

Format

bfd *cfg-name* **bind pw interface** *interface-type interface-number* [**secondary**]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of the BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of the interface where the PW to be detected resides, namely, the AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates that the BFD session detects the secondary PW.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link detection mechanism on an interface. On networks demanding fast fault detection, run the **bfd bind pw** command to configure a BFD session to detect a PW.

Prerequisites

- A PW has been configured on an AC interface by running the **mpls l2vc** command.
- BFD has been enabled globally by running the **bfd** command.
- A single-segment or multi-segment PW has been configured.

Precautions

- When detecting a PW, BFD sessions must be bound to the source and destination ends of a PW.
- You need to create a BFD session to detect primary and secondary PWs separately.

NOTE

When running the **bfd bind pw** command to detect a multi-segment PW, ensure that the first-segment PW is a VLL PW configured on a non-SPE node.

When running the **bfd bind pw** command to detect a single-segment PW, ensure that the single-segment PW is configured on a non-SPE node.

Example

Create a BFD session to detect a PW.

```
<HUAWEI> system-view
[HUAWEI] bfd pe2 bind pw interface vlanif 10
```

10.6.3 bfd-detect

Function

The **bfd-detect** command enables dynamic BFD for PW in a PW template and adjusts the sending interval, receiving interval, and local detection multiplier of BFD detection packet.

The **undo bfd-detect** command restores the default configuration.

By default, dynamic BFD for PW is not enabled in a PW template.

Format

bfd-detect [**min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier*] *

undo bfd-detect

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

If the BFD session is found to be Down, the system automatically adjusts the receiving interval and sending interval of the local end to a random value ranging from 1000 ms to 3000 ms to reduce system resource utilization. When the BFD session restores the Up state, the user-defined interval is used again.

Example

Enable dynamic BFD detection, and set *min-tx-interval*, *min-rx-interval*, and *multiplier* to 100 ms, 100 ms, and 4 respectively in the PW template.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] bfd-detect min-rx-interval 100 min-tx-interval 100 detect-multiplier 4
```

10.6.4 bfd for pw enable

Function

The **bfd for pw enable** command enables the device to send BFD for PW packets to the protocol stack.

The **undo bfd for pw enable** command disables the device from sending BFD for PW packets to the protocol stack.

By default, the device does not send BFD for PW packets to the protocol stack, but discards or forwards the packets.

Format

bfd for pw enable

undo bfd for pw enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a BFD session to detect a PW on a network requiring short link detection, run the **bfd for pw enable** command to enable the device to send BFD for PW packets to the protocol stack. If this command is not used, the device discards or forwards BFD for PW packets.

Precautions

The **bfd for pw enable** command must have been executed to configure a BFD session to detect a PW. If this command is not used, the **bfd for pw enable** command does not take effect.

Example

Enable the device to send BFD for PW packets to the protocol stack.

```
<HUAWEI> system-view
[HUAWEI] bfd for pw enable
```

10.6.5 control-word

Function

The **control-word** command enables the control word in a PW template.

The **undo control-word** command disables the control word in a PW template.

By default, the control word is disabled in a PW template.

Format

control-word

undo control-word

Parameters

None

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the case of load balancing, packets received by a device may be out of order. With the control word function, the device can reassemble the packets.

PW templates simplify the configuration of PWs with similar attributes. The control word attribute can be set using commands or a PW template. If the control word is configured using both commands and a PW template, only the control word configured using commands takes effect.

Prerequisites

- MPLS L2VPN has been enabled.
- A PW template has been created.

Configuration Impact

After a PW is established using a PW template where the control word function is enabled, the control word enabling status on both ends of the PW may be different after the PW template is restarted. As a result, system performance may be affected.

Follow-up Procedure

When configuring MPLS L2VPN on an interface, use a configured PW template.

Precautions

After the control word attribute is changed in a PW template:

- If the PW is in use, you do not need to reset the PW.
- If the PW template is being referenced by PWs, the configuration takes effect only after you run the **reset pw** command. Running the **reset pw** command may cause the disconnection and re-connection of related PWs. If multiple PWs use this template at the same time, the system operation is affected.

Example

Enable the control word in the PW template named **pwt**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] control-word
```

Disable the control word in the PW template named **pwt**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] undo control-word
```

10.6.6 display mpls l2vc

Function

The **display mpls l2vc** command displays information about virtual circuits (VCs) in LDP mode.

Format

display mpls l2vc [*vc-id* | **interface** *interface-type interface-number* | **remote-info** [*vc-id* | **verbose**] | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface connected to the CE. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
remote-info	Displays information about the VC on the remote end.	-
vc-id	Displays static PW information with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays the detailed information about the VC on the remote end.	-
state { **down** | **up** }	Displays VC information based on the VC status. - **down**: Displays information about the VC in Down state. - **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc** command displays information about the VCs in LDP signaling mode, including the Martini VC and PWE3 VC.

- If the interface is specified, information about VCs on the specified AC interface is displayed.
- If **remote-info** is specified but *vc-id* is not specified, information about all VCs set up by the remote and local peers is displayed.

Example

Display information about all the LDP VCs configured on the switch.

```
<HUAWEI> display mpls l2vc
 Total LDP VC : 1     1 up       0 down
```

```
*client interface       : Vlanif1111 is up
 Administrator PW       : no
 session state          : up
 AC status              : up
 Ignore AC state        : disable
 VC state               : up
 Label state            : 0
 Token state            : 0
 VC ID                  : 101
 VC type                : VLAN
 destination            : 10.3.3.9
 local VC label         : 1026         remote VC label      : 1026
 control word           : disable
 remote control word    : disable
 forwarding entry       : exist
 local group ID         : 0
 remote group ID        : 0
 local AC OAM State     : up
 local PSN OAM State    : up
 local forwarding state : forwarding
 local status code      : 0x0
 remote AC OAM state    : up
 remote PSN OAM state   : up
 remote forwarding state: forwarding
 remote status code     : 0x0
 ignore standby state   : no
 BFD for PW             : unavailable
 VCCV State             : up
 manual fault           : not set
 active state           : active
 link state             : up
 local VC MTU           : 1500         remote VC MTU        : 1500
 local VCCV             : alert ttl lsp-ping bfd
 remote VCCV            : alert ttl lsp-ping bfd
 tunnel policy name     : --
 PW template name       : --
 primary or secondary   : primary
 load balance type      : flow
 Access-port            : false
 Switchover Flag        : false
 VC tunnel/token info   : 1 tunnels/tokens
   NO.0  TNL type       : lsp   , TNL ID : 0x48000020
   Backup TNL type      : lsp   , TNL ID : 0x0
 create time            : 0 days, 0 hours, 6 minutes, 50 seconds
 up time                : 0 days, 0 hours, 6 minutes, 34 seconds
 last change time       : 0 days, 0 hours, 6 minutes, 34 seconds
 VC last up time        : 2013/09/24 18:23:35
 VC total up time       : 0 days, 0 hours, 6 minutes, 34 seconds
 CKey                   : 16
 NKey                   : 15
 PW redundancy mode     : frr
 AdminPw interface      : --
 AdminPw link state     : --
 Diffserv Mode          : uniform
 Service Class          : be
 Color                  : --
 DomainId               : --
 Domain Name            : --
```

Table 10-76 Description of the **display mpls l2vc** command output

Item	Description
Total LDP VC	Total number of established LDP VCs, including the number of LDP VCs in Up and Down state.
client interface	AC interface and its status.

Item	Description
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface. This field can be displayed as **yes** or **no**.
session state	Status of the LDP session established between both ends of the VC: ● up: The LDP session has been established. ● down: The LDP session is not established.
AC status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. ● enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. ● disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token state	Token status: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
VC ID	ID of the VC, which uniquely identifies a VC. **NOTE** If the VC IDs on both ends are different, run the **mpls l2vc** command in the interface view to change the VC ID on one end to be the same as that on the other end.

Item	Description
VC type	Encapsulation type of the VC: ● VLAN ● Ethernet The PW can go Up only when the local and remote encapsulation types are the same.
destination	LSR ID of the VC peer device.
local VC label	Local VC label.
remote VC label	Remote VC label.
control word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.
forwarding entry	Whether forwarding entries exist.
local group ID	Local group ID.
remote group ID	Remote group ID.
manual fault	Whether a PW fault is simulated.
active state	Whether the PW is in active state. A PW in active state can forward packets.
link state	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● Status of the mPW associated with service PWs ● Status of the BFD session associated with service PWs ● PW state code ● PW status detected by VCCV ● OAM status
local VC MTU	MTU of the local VC.
remote VC MTU	MTU of the remote VC.
tunnel policy name	Name of the tunnel policy.
PW template name	Name of the PW template.
primary or secondary	Whether the VC is a primary VC or a secondary VC.

Item	Description
load balance type	Load balancing mode of Martini VLL: - flow: indicates flow-based load balancing. - packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: - true: indicates that the interface supports the access-port attribute. - false: indicates that the interface does not support the access-port attribute.
Switchover Flag	Whether a switchover has occurred.
create time	How long the VC has been created.
up time	How long the VC keeps the Up state. If the current PW status is Down, the value is 0.
last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
AdminPw interface	AC interface on which the mPW is bound to the PW. The AC interface must be a loopback interface. This field is displayed only when the PW is not an mPW: - Name of the loopback interface. - --: indicates that the PW is not bound to an mPW.
AdminPw link state	Status of the mPW bound to the PW. This field is displayed only when the PW is not an mPW. This field can be displayed as: - Up - Down - --: indicates that the PW is not bound to an mPW.
Diffserv Mode	QoS DiffServ mode.
Service Class	QoS service class.
Color	QoS color.
DomainId	ID of a domain.

Item	Description
Domain Name	Name of a domain.

Display LDP VC information about the AC interface VLANIF 100.

```
<HUAWEI> display mpls l2vc interface vlanif 100
 *client interface       : Vlanif100  is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 1
  VC type                : VLAN
  destination            : 10.2.2.2
  local group ID         : 0            remote group ID      : 0
  local VC label         : 16400        remote VC label      : 16400
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x20
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  forwarding entry       : exist
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : cw alert ttl lsp-ping bfd
  remote VCCV            : cw alert ttl lsp-ping bfd
  local control word     : enable       remote control word  : enable
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x800802
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 0 hours, 0 minutes, 29 seconds
  up time                : 0 days, 0 hours, 0 minutes, 6 seconds
  last change time       : 0 days, 0 hours, 0 minutes, 6 seconds
  VC last up time        : 2011/07/04 20:25:50
  VC total up time       : 0 days, 0 hours, 0 minutes, 6 seconds
  CKey                   : 2
  NKey                   : 1
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
  Diffserv Mode          : uniform
  Service Class          : --
  Color                  : --
  DomainId               : --
  Domain Name            : --
```

Table 10-77 Description of the **display mpls l2vc interface** command output

Item	Description
local AC OAM State	OAM status of the local AC. - up - down
local PSN OAM State	Status of the local device on the Packet Switch Network (PSN) side. - up - down
local forwarding state	Status of the local forwarding table. - forwarding - down
local status code	Status code of the local PW: - 0x0: indicates that the local PW functions as the master PW and is in Up state. - 0x20: indicates that the local PW functions as the backup PW and is in Up state. - 0x1: indicates that the local PW functions as the master PW and is in Down state. - 0x21: indicates that the local PW functions as the backup PW and is in Down state.
remote AC OAM state	OAM status of the remote AC. - up - down
remote PSN OAM state	Status of the remote device on the PSN side. - up - down
remote forwarding state	Status of the remote forwarding table. - forwarding - down
remote status code	Status code of the remote PW: - 0x0: indicates that the remote PW functions as the master PW and is in Up state. - 0x20: indicates that the remote PW functions as the backup PW and is in Up state. - 0x1: indicates that the remote PW function as the master PW and is in Down state. - 0x21: indicates that the remote PW function as the backup PW and is in Down state.

Item	Description
BFD for PW	Whether BFD for PW is enabled: - available - unavailable
VCCV State	Whether Virtual Circuit Connectivity Verification (VCCV) is enabled.
local VCCV	Type of VCCV supported on the local device. - By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. - If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
remote VCCV	Type of VCCV supported on the remote device. - By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. - If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
local control word	Whether the control word is enabled on the local device: - Disable - Enable
remote control word	Whether the control word is enabled on the remote device: - Disable - Enable
ignore standby state	Whether the status of the secondary PW is ignored.
VC Tunnel/token info: 1 tunnels/tokens	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
TNL type	Type of the tunnel used by the PW.
TNL ID	ID of the tunnel used by the PW.

Item	Description
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
PW redundancy mode	PW redundancy mode. By default, the mode is FRR. ● Independent: indicates that the PW is in negotiation mode. ● frr: indicates that the PW is in FRR mode. ● --: indicates that the PW is in master/slave mode.

Display the LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info
Total remote ldp vc : 1

Transport  Group      Peer            Remote         Remote     C   MTU/  N   S
VC ID      ID         Addr            Encap          VC Label   Bit CELLS Bit Bit

101        0          10.3.3.9        ethernet       1024       0   1500  0   0
```

Display the detailed LDP VC information received from the remote peer.

```
<HUAWEI> display mpls l2vc remote-info verbose
Total remote LDP VC : 1

VC ID             : 1
VC Type           : vlan
VC Label          : 1025
Peer Address      : 10.5.5.5
Group ID          : 0
MTU               : 1500
Control Word      : 0
Notification      : 1
Status Code       : 0
Match Local VC    : MATCH
Max ATM CELLS     : --
TDM RTP Header    : --
TDM Encap Num     : --
TDM Bit Rate      : --
```

Table 10-78 Description of the **display mpls l2vc remote-info** command output

Item	Description
Total remote ldp vc	Total number of created remote LDP VCs.
Transport VC ID	VC ID, which uniquely identifies a VC.
Group ID	ID of the group to which the L2VPN belongs. The default value is 0.
Peer Addr and Peer Address	IP address of the remote peer.

Item	Description
Remote Encap	Encapsulation type of the remote VC. - vlan - ethernet
Remote VC Label	Remote VC label.
C Bit	Whether the control word is enabled: - 1: indicates that the control word is enabled. - 0: indicates that the control word is disabled.
MTU/CELLS	MTU of the L2VPN.
N Bit and Notification	Whether the Notification message is supported: - 1: indicates the message is supported. - 0: indicates the message is not supported.
S Bit and Status Code	Status code: - 0: indicates the forwarding state. - 1: indicates the non-forwarding state. - 32: indicates the backup state.
Match Local VC	Whether the local VC ID matches the remote VC ID: - MATCH - NOT-MATCH
Max ATM CELLS	Maximum number of ATM cells that can be transmitted. If ATM encapsulation is used, the value ranges from 1 to 28, and the default value is 28. If non-ATM encapsulation is used, double hyphens (--) are displayed.
TDM RTP Header	Whether the RTP-header option is enabled: - enable: The RTP header is added to TDM packets to be transparently transmitted. - disable: The RTP header is not added to TDM packets to be transparently transmitted. This is the default value. - --: Non-TDM encapsulation is used.
TDM Encap Num	Number of frames in a TDM packet. If TDM encapsulation is used, the value is 8, 16, 24, 32 or 40, and the default value is 32. If non-TDM encapsulation is used, double hyphens (--) are displayed.

Item	Description
TDM Bit Rate	Number of timeslots in a TDM packet. Number of timeslots in a TDM packet = Number of bytes in a TDM packet/Number of frames in a TDM packet

Display information about the VCs in Up state.

```
<HUAWEI> display mpls l2vc state up
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 100
  VC type                : VLAN
  destination            : 10.2.2.9
  local VC label         : 1024         remote VC label      : 1024
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  link state             : up
  local VC MTU           : 1500         remote VC MTU        : 1500
  local VCCV             : alert ttl lsp-ping bfd
  remote VCCV            : alert ttl lsp-ping bfd
  tunnel policy name     : --
  PW template name       : --
  primary or secondary   : primary
  load balance type      : flow
  Access-port            : false
  Switchover Flag        : false
  VC tunnel/token info   : 1 tunnels/tokens
    NO.0  TNL type       : lsp   , TNL ID : 0x12
    Backup TNL type      : lsp   , TNL ID : 0x0
  create time            : 0 days, 1 hours, 0 minutes, 17 seconds
  up time                : 0 days, 0 hours, 24 minutes, 56 seconds
  last change time       : 0 days, 0 hours, 24 minutes, 56 seconds
  VC last up time        : 2013/10/10 14:29:39
  VC total up time       : 0 days, 0 hours, 24 minutes, 56 seconds
  CKey                   : 10
  NKey                   : 9
  PW redundancy mode     : frr
  AdminPw interface      : --
  AdminPw link state     : --
```

```
 Diffserv Mode          : uniform
 Service Class          : --
 Color                  : --
 DomainId               : --
 Domain Name            : --
```

10.6.7 display mpls l2vc brief

Function

The **display mpls l2vc brief** command displays brief information about LDP Layer 2 virtual circuits (L2VCs) on the device.

Format

display mpls l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc brief** command is recommended when many L2VCs are configured on a device. The command output is more concise than that of the **display mpls l2vc** command.

Example

Display brief information about all LDP L2VCs on the device.

```
<HUAWEI> display mpls l2vc brief
 Total LDP VC : 1     1 up       0 down

 *Client Interface     : Vlanif1111
  Administrator PW     : no
  AC status            : up
  Ignore AC state      : disable
  VC state             : up
  Label state          : 0
  Token state          : 0
  VC ID                : 116119
  VC Type              : VLAN
  session state        : up
  Destination          : 10.6.6.6
  link state           : up
```

Table 10-79 Description of the **display mpls l2vc brief** command output

Item	Description
Total LDP VC	Total number of LDP VCs, including the number of LDP VCs in Up and Down state.
Client Interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface.
AC status	Status of the AC: - up - down
Ignore AC state	Whether the AC status change affects the status of services on the active or standby PWE3. - enable: The impact of the AC status change on the status of services on the active or standby PWE3 is ignored. - disable: The AC status change affects the status of services on the active or standby PWE3.
VC state	Status of the VC: - up - down
Label state	Label status: - 0: The label can be used. - 1: Wait for the SMB to confirm the label status. - 2: The label is released. - 3: SMB confirming failed.
Token state	Token status: - 0: The label can be used. - 1: Wait for the SMB to confirm the label status. - 2: The label is released. - 3: SMB confirming failed.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
session state	Status of the session between peers: - up - down
Destination	Peer address.

Item	Description
link state	Status of the VC: ● up ● down

10.6.8 display mpls l2vc track admin-vc

Function

The **display mpls l2vc track admin-vc** command displays information about service PWs or switching PWs that are associated with an mPW.

Format

display mpls l2vc track admin-vc interface loopback *interface-number* [**upe**]

Parameters

Parameter	Description	Value
interface loopback *interface-number*	Specifies the loopback interface on which the mPW is configured.	-
upe	Displays information about switching PWs of the UPE type.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After service PWs or switching PWs are associated with an mPW, you can run the **display mpls l2vc track admin-vc** command to view information about these PWs, facilitating configuration and management.

Example

Display information about service PWs or switching PWs that are associated with the mPW configured on loopback 0.

```
<HUAWEI> display mpls l2vc track admin-vc interface loopback 0
Total VC         :  0    2 up      0 down

 Admin-PW state   :  up
 Peer IP          :  1.1.1.1
```

```
PW type          : UPE
Total VC         :  2     2 up      0 down

*Client Interface     : Vlanif10
 VC State             : up
 VC ID               : 1113
 VC Type              : Ethernet
 Link State           : up

*Client Interface     : Vlanif10
 VC State             : up
 VC ID               : 2223
 VC Type              : Ethernet
 Link State           : up
```

Table 10-80 Description of the display mpls l2vc track admin-vc command output

Item	Description
Total VC	Number of all the service PWs and switching PWs that are associated with the mPW.
Admin-PW state	Status of the mPW. ● down ● up
Peer IP	IP address of an mPW peer. The peers of the service or switching PWs must have the same IP address as that of the mPW.
PW type	PW type. Currently, only UPE is supported.
*Client Interface	AC interface of the service PW or switching PW.
VC State	VC status. ● down ● up
VC ID	VC ID. The VC ID uniquely identifies a VC together with the VC type.
VC Type	Encapsulation type of the VC. ● ethernet ● ip-interworking ● vlan
Link State	Forwarding status of the PW. ● down ● up

10.6.9 display mpls static-l2vc

Function

The **display mpls static-l2vc** command displays information about static VCs on the device.

Format

display mpls static-l2vc [*vc-id* | **interface** *interface-type interface-number* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
vc-id	Displays information about a static VC with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
interface *interface-type interface-number*	Displays information about all static PWs on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you run the **display mpls static-l2vc** command with the interface name specified, information about static VCs on the interface connected to a CE is displayed. If no interface is specified, information about static VCs on all interfaces is displayed.

Example

Display information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : active
  Link State           : down
  Tunnel Policy Name   : tun
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x800802
  Backup TNL type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
  VC last up time      : 2011/07/04 20:29:18
  VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
  CKey                 : 2
  NKey                 : 1
  BFD for PW           : unavailable
```

Table 10-81 Description of the **display mpls static-l2vc** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up ● down
VC State	Status of the VC: ● up ● down
VC ID	ID of the VC, which uniquely identifies a VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.

Item	Description
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Label Status	Whether the label can be used: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token Status	Whether the token can be used: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
Control Word	Whether the control word function is enabled: ● enable ● disable
VCCV Capability	Whether VCCV is enabled.
active state	Whether the PW is in active state. A PW in active state can forward packets. ● active ● inactive
Link State	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● OAM status
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.

Item	Description
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
VC Tunnel/token info	Information about the VC tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
NO.0 TNL Type	Type of the tunnel used by the PW
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

Display information about static VCs on VLANIF 10.

```
<HUAWEI> display mpls static-l2vc interface vlanif 10
 *Client Interface     : Vlanif10 is up
  AC Status            : down
  VC State             : up
  VC ID                : 1
  VC Type              : VLAN
  Destination          : 2.2.2.2
  Transmit VC Label    : 400
  Receive VC Label     : 600
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
```

```
VCCV Capability      : cw alert ttl lsp-ping bfd
active state         : active
Link State           : down
Tunnel Policy        : tun
PW Template Name     : --
Main or Secondary    : Main
load balance type    : flow
Access-port          : false
VC tunnel/token info : 1 tunnels/tokens
NO.0  TNL Type       : lsp   , TNL ID : 0x56
Backup TNL Type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 0 hours, 0 minutes, 34 seconds
UP time              : 0 days, 0 hours, 0 minutes, 31 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 31 seconds
VC last up time      : 2011/07/04 20:29:18
VC total up time     : 0 days, 0 hours, 0 minutes, 33 seconds
CKey                 : 2
NKey                 : 1
Diffserv Mode        : uniform
Service Class        : be
Color                : --
DomainId             : --
Domain Name          : --
BFD for PW           : unavailable
```

Table 10-82 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the link between the PE and its directly connected CE.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	VC label sent by the local device.
Receive VC Label	VC label received by the local device.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy	Name of the tunnel policy. The value -- indicates that no tunnel policy is configured.
PW Template Name	Name of the PW template. The value -- indicates that no PW template is configured.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
VC tunnel/token info	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.

Item	Description
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Diffserv Mode	QoS DiffServ mode for VLL services.
Service Class	QoS service class for VLL services.
Color	QoS color for VLL services.
DomainId	ID of a domain.
Domain Name	Name of a domain.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

Display information about SVCs in Up state between peers.

```
<HUAWEI> display mpls static-l2vc state up
 Total svc connections:  1,  1 up,  0 down
 *Client Interface     : Vlanif10 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 2.2.2.2
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 4 hours, 55 minutes, 41 seconds
  UP time              : 0 days, 4 hours, 55 minutes, 40 seconds
  Last change time     : 0 days, 4 hours, 55 minutes, 40 seconds
```

```
VC last up time      : 2011/09/09 10:25:22
VC total up time     : 0 days, 4 hours, 55 minutes, 40 seconds
CKey                 : 19
NKey                 : 1
BFD for PW           : unavailable
```

Table 10-83 Description of the **display mpls static-l2vc state** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured. ● timeout: timeout period after which a BFD session fails to be established

10.6.10 display mpls static-l2vc brief

Function

The **display mpls static-l2vc brief** command displays brief information about static VCs on the device.

Format

display mpls static-l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls static-l2vc brief** command is recommended when a large number of static VCs are configured on the device.

Example

Display brief information about static VCs on the device.

```
<HUAWEI> display mpls static-l2vc brief
Total svc connections:  2,  1 up,  1 down

 *Client Interface            : Eth-Trunk2  is up
  AC Status                   : up
  VC State                    : up
  VC ID                       : 0
  VC Type                     : VLAN
  Destination                 : 10.1.1.1

 *Client Interface            : Eth-Trunk3  is down
  AC Status                   : down
  VC State                    : down
  VC ID                       : 100
  VC Type                     : Ethernet
  Destination                 : 10.1.1.2
```

Table 10-84 Description of the **display mpls static-l2vc brief** command output

Item	Description
Total SVC Connections	Number of established SVCs, including the number of SVCs in Up and Down states.

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the AC: - up: An AC has been established. - down: An AC is not established.
VC State	Status of the VC: - up: A VC has been established. - down: A VC is not established.
VC ID	ID of the static VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: - VLAN - Ethernet
Destination	IPv4 address of the peer. Generally, the value is the loopback address of the peer.

10.6.11 display mpls switch-l2vc

Function

The **display mpls switch-l2vc** command displays information about PW switching, including static, dynamic, and mix PW switching.

Format

display mpls switch-l2vc [*ip-address vc-id* **encapsulation** *encapsulation-type* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of the peer PE.	-
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
encapsulation *encapsulation-type*	Specifies the PW encapsulation type.	Currently, the device supports the following types encapsulation types: **ethernet**, **vlan**, and **ip-interworking**.
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If parameters in the **display mpls switch-l2vc** command are not specified, information about all PW switching is displayed.

Example

Display information about the specified PW switching.

```
<HUAWEI> display mpls switch-l2vc 1.1.1.9 100 encapsulation ethernet
*Switch-l2vc type             : SVC<---->SVC
 Peer IP Address              : 3.3.3.9, 1.1.1.9
 VC ID                        : 100, 100
 VC Type                      : Ethernet
 VC State                     : up
 In/Out Label                 : 200/200, 100/100
 InLabel Status               : 0 , 0
 Control Word                 : Disable, Disable
 VCCV Capability              : alert ttl lsp-ping bfd, alert ttl lsp-ping bfd
 Switch-l2vc tunnel info      :
                                1 tunnels for peer 5.5.5.9
                                NO.0  TNL Type : lsp   , TNL ID : 0x11
                                1 tunnels for peer 1.1.1.9
                                NO.0  TNL Type : lsp   , TNL ID : 0xb
 CKey                         : 44, 1
 NKey                         : 43, 3
 Tunnel policy                : --,--
 Control-Word transparent     : YES
 Create time                  : 0 days, 0 hours, 7 minutes, 2 seconds
 UP time                      : 0 days, 0 hours, 7 minutes, 2 seconds
 Last change time             : 0 days, 0 hours, 7 minutes, 2 seconds
 VC last up time              : 2008/07/24 12:31:31
 VC total up time             : 0 days, 2 hours, 12 minutes, 51 seconds
```

Table 10-85 Description of the **display mpls switch-l2vc** command output (SVC-SVC)

Item	Description
Switch-l2vc Type	Switching type: - LDP-LDP - LDP-SVC - SVC-SVC When primary/secondary PWs and PW switching are configured, the value of this field must be LDP-LDP. - LDP: indicates a dynamic PW. - SVC: indicates a static PW.
Peer ip address	IP addresses of the peers at two ends of a switching PW, which are displayed in left and right columns respectively.
VC ID	ID of the VC, which uniquely identifies a VC. Here, the field indicates the two switched VC IDs.
VC Type	Encapsulation type of the VC.
VC State	Status of the VC: - Up: A VC has been established. - Down: A VC is not established.
In/Out Label	Incoming or outgoing label.
InLabel Status	Status of the inner label.
Control Word	Whether the control word function is enabled on both ends: - Disable - Enable
VCCV Capability	Type of VCCV supported on the local device. - By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. - If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.

Item	Description
Switch-l2vc tunnel info: 1 tunnels for peer 3.3.3.9 NO.0 TNL Type : lsp , TNL ID : 0x11	Information about the tunnels on both ends: ● TNL Type: indicates the type of the tunnel. ● TTNL ID: indicates the tunnel ID.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Tunnel policy	Name of the tunnel policy.
Control-Word transparent	Whether transparent transmission of the control word is enabled: ● yes ● no
Create Time	How long the VC has been created.
Up Time	How long the VC keeps the Up state.
Last Change Time	How long the VC status remains unchanged.
VC last up time :	Last time when the AC became Up.
VC total up time:	Total duration when the AC interface is Up.

Display information about the switched L2VCs in Up state between peers.

```
<HUAWEI> display mpls switch-l2vc state up
Total Switch VC : 1, 1 up, 0 down
*Switch-l2vc type             : LDP<---->LDP
 Peer IP Address              : 5.5.5.9, 1.1.1.9
 VC ID                        : 200, 100
 VC Type                      : Ethernet
 VC State                     : up
 VC StatusCode                |PSN |OAM | FW |    |PSN |OAM | FW |
                 -Local VC :| UP | UP | UP |     | UP | UP |DOWN|
                 -Remote VC:| UP | UP |DOWN|     | UP | UP | UP |
 Session State                : up, up
 Local/Remote Label           : 1025/1024, 1024/1025
 InLabel Status               : 0 , 0
 Local/Remote MTU             : 1500/1500, 1500/1500
 Local/Remote Control Word    : Disable/Disable, Disable/Disable
 Local/Remote VCCV Capability : alert ttl lsp-ping bfd /alert ttl lsp-ping bfd, alert ttl lsp-ping bfd/alert ttl lsp-
ping bfd
 Switch-l2vc tunnel info      :
                              1 tunnels for peer 5.5.5.9
                              NO.0  TNL Type : lsp   , TNL ID : 0x12
                              1 tunnels for peer 1.1.1.9
                              NO.0  TNL Type : lsp   , TNL ID : 0x15
 CKey                         : 44, 1
 NKey                         : 43, 3
 Tunnel policy                : --, --
 Control-Word transparent     : YES
 Create time                  : 0 days, 0 hours, 3 minutes, 54 seconds
 UP time                      : 0 days, 0 hours, 3 minutes, 12 seconds
 Last change time             : 0 days, 0 hours, 3 minutes, 12 seconds
 VC last up time              : 2008/07/24 12:31:31
 VC total up time             : 0 days, 2 hours, 12 minutes, 51 seconds
```

Table 10-86 Description of the **display mpls switch-l2vc** command output (LDP-LDP)

Item	Description
VC StatusCode	VC status code: - PSN: indicates the fault status at the public network side. - OAM: indicates the fault status at the AC side. - FW: indicates the forwarding status. -Local VC: indicates the local VC status. -Remote VC: indicates the remote VC status.
Session State	Status of the session: - Up: indicates that the session is successfully set up. - Down: indicates that the session is not set up. - None: indicates that no session exists.
Local/Remote Label	Incoming or outgoing label.
Local/Remote MTU	Local and remote MTU values of the PWs on two ends: - For LDP, both the local and remote MTU values are displayed. - For SVC, only the local MTU value is displayed.
Local/Remote Control Word	Whether the control word is enabled on both ends: - disable: indicates that the control word is disabled. - enable: indicates that the control word is enabled.
Local/Remote VCCV Capability	Whether VCCV is enabled on both ends: - CC: specifies the control channel type, which can be CW, alert, or TTL. - CV: specifies the connectivity verification mode, which can be LSP ping or BFD.
Control-Word transparent	Whether transparent transmission of the control word is enabled: - yes - no

Display information about all the switched L2VCs between peers.

```
<HUAWEI> display mpls switch-l2vc
Total Switch VC : 1, 1 up, 0 down

*Switch-l2vc type             : LDP<---->SVC
 Peer IP Address              : 1.1.1.9, 5.5.5.9
 VC ID                        : 100, 200
 VC Type                      : Ethernet
 VC State                     : up
 Session State                : up, None
 Local(In)/Remote(Out) Label  : 1027/1028, 100/200
 InLabel Status               : 0 , 0
 Local/Remote MTU             : 1500/1500, 1500
 Local/Remote Control Word    : Disable/Disable, Disable
 Local/Remote VCCV Capability : alert ttl lsp-ping bfd /alert ttl lsp-ping bfd, alert ttl lsp-ping bfd
 Switch-l2vc tunnel info      :
                                1 tunnels for peer 1.1.1.9
                                NO.0  TNL Type : lsp   , TNL ID : 0x9
                                1 tunnels for peer 5.5.5.9
                                NO.0  TNL Type : lsp   , TNL ID : 0xa
 CKey                         : 44, 1
 NKey                         : 43, 3
 Tunnel policy                : --, --
 Create time                  : 0 days, 0 hours, 3 minutes, 48 seconds
 UP time                      : 0 days, 0 hours, 3 minutes, 48 seconds
 Last change time             : 0 days, 0 hours, 3 minutes, 48 seconds
 VC last up time              : 2008/07/24 12:31:31
 VC total up time             : 0 days, 2 hours, 12 minutes, 51 seconds
```

10.6.12 display mpls switch-l2vc brief

Function

The **display mpls switch-l2vc brief** command displays brief information about all switching PWs, including static, dynamic, and mixed switching PWs.

Format

display mpls switch-l2vc brief

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When many switching PWs are configured on the device, you can run this command to view brief information about the switching PWs. The command output of the **display mpls switch-l2vc brief** command is more concise than that of the **display mpls switch-l2vc** command.

Example

Display brief information about switching PWs.

```
<HUAWEI> display mpls switch-l2vc brief
Total Switch VC : 1,   1 up,   0 down
*Switch-l2vc Type           : LDP<---->LDP
 Peer IP Address            : 10.1.1.9, 10.2.2.9
 VC ID                      : 200, 100
 VC Type                    : VLAN
 VC State                   : up
 Session State              : up, up
```

Table 10-87 Description of the display mpls switch-l2vc brief command output

Item	Description
Total Switch VC	Number of established Martini VCs (using the LDP signaling), including the number of Martini VCs in Up and Down states.
Switch-l2vc Type	Switching type, which can be LDP-LDP, LDP-SVC, or SVC-SVC. If the primary and secondary switching VCs are configured, the switching types of these VCs can only be LDP-LDP. ● LDP: indicates a dynamic PW. ● SVC: indicates a static PW.
Peer IP Address	IP address of the peer.
VC ID	ID of the VC, which uniquely identifies a VC. Here, the field indicates the two switched VC IDs.
VC Type	Encapsulation type of the VC.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Session state	Status of the session between peers: ● up: indicates that the session is successfully set up. ● down: indicates that the session is not set up. ● none: indicates that no session exists.

10.6.13 display pw-template

Function

The **display pw-template** command displays information about PW templates.

Format

display pw-template [*pw-template-name*]

Parameters

Parameter	Description	Value
pw-template-name	Specifies the PW template name. If this parameter is not specified, information about all PW templates is displayed.	The value is an existing PW template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *pw-template-name* is not specified, information about all PW templates is displayed.

Example

Display information about all PW templates.

```
<HUAWEI> display pw-template
Total PW template number : 2
  PW Template Name : PWT
  PeerIP           : 2.2.2.2
  Tnl Policy Name  : --
  CtrlWord         : Enable
  MTU              : 1500
  Max Atm Cells    : 28
  ATM Pack Overtime: 1000
  Seq-Number       : Disable
  Transmit ATM Cells      : 28
  TDM Encapsulation Number: 32
  Jitter-Buffer           : 20
  Jitter-Buffer-Cep       : 1125
  Payload-Compression DBA : UNEQ
  Idle-Code               : ff
  Rtp-Header              : Disable
  VCCV Capability  : cw alert ttl lsp-ping bfd
  Total PW         : 6, Static PW : 1, LDP PW : 5

  PW Template Name : pwt
  PeerIP           : --
  Tnl Policy Name  : --
  CtrlWord         : Disable
  MTU              : 1500
  Max Atm Cells    : 28
  ATM Pack Overtime: 1000
  Seq-Number       : Disable
  Transmit ATM Cells      : 28
  TDM Encapsulation Number: 32
```

```
Jitter-Buffer          : 20
Jitter-Buffer-Cep      : 1125
Payload-Compression DBA : UNEQ
Idle-Code              : ff
Rtp-Header             : Disable
VCCV Capability  : alert ttl lsp-ping bfd
Total PW         : 0, Static PW : 0, LDP PW : 0
```

Table 10-88 Description of the **display pw-template** command output

Item	Description
Total PW template number	Total number of PW templates.
PW Template Name	PW template name.
PeerIP	Peer IP address.
Tnl Policy Name	Name of the public network tunnel policy applied to the PW.
CtrlWord	Whether the control word is enabled in the PW template. ● Disable ● Enable
MTU	Maximum transmission unit.
Max ATM cells	Maximum number of transmitted ATM cells.
ATM pack overtime	Delay in packaging ATM cells.
Seq-Number	Sequence number in the control word of the PW: ● If the sequence number function is enabled, the device checks the sequence number of each packet and discards any packet with an incorrect sequence number. ● If the sequence number function is disabled, the device does not check the sequence number when processing packets.
Transmit ATM Cells	Number of ATM cells sent by the local device.
TDM Encapsulation Number	Number of encapsulated TDM frames.
Jitter-Buffer	Maximum jitter buffer depth for TDM.
Jitter-Buffer-Cep	Maximum jitter buffer depth for TDM (with CEP encapsulation).
Payload-Compression DBA	Payload compression dynamic bandwidth allocation (DBA): ● UNEQ: Send DBA packets when unequipped circuit indications are detected. ● --: Payload compression DBA is not configured.

Item	Description
Idle-Code	Idle code that is filled when a jitter buffer underflow occurs.
Rtp-Header	Whether the RTP header is added to the transparently transmitted TDM frame.
VCCV Capability	VC connection verification mode. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
Total PW	Total number of PWs using this PW template, including static and dynamic PWs.

10.6.14 lspv pw reply ptn-mode

Function

The **lspv pw reply ptn-mode** command configures the SPE and TPE to reply trace VC packets in a multi-segment PW scenario.

The **undo lspv pw reply ptn-mode** command restores the default configuration.

By default, the **lspv pw reply ptn-mode** command is not configured.

Format

lspv pw reply ptn-mode

undo lspv pw reply ptn-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the source end starts a tracert test in PTN mode to detect the connectivity of the multi-hop PW, the **lspv mpls-pw reply ptn-mode** command needs to be run on the SPE and TPE. If the PTN mode is not specified, the **lspv mpls-pw reply ptn-mode** command is not required.

Example

Run **lspv pw reply ptn-mode** command to enable the SPE and TPE to respond to tracert VC packets in PTN mode.

```
<HUAWEI> system-view
[HUAWEI] lspv pw reply ptn-mode
```

10.6.15 manual-set pw-ac-fault

Function

The **manual-set pw-ac-fault** command simulates a fault on the primary or secondary PW.

The **undo manual-set pw-ac-fault** command cancels the fault that is simulated on a primary or secondary PW.

By default, no fault is simulated on a PW.

Format

manual-set pw-ac-fault [**secondary**]

undo manual-set pw-ac-fault [**secondary**]

Parameters

Parameter	Description	Value
secondary	Simulates a fault on the secondary PW. If this parameter is not specified, a fault is simulated on the primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where the primary and secondary PWs need to be configured, you can run the **manual-set pw-ac-fault** command to simulate a fault on the primary or secondary PW to check whether services can be switched between the primary and secondary PWs.

Prerequisites

A VC has been created.

Example

Simulate a fault on the PW.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] manual-set pw-ac-fault
```

10.6.16 mpls l2vc

Function

The **mpls l2vc** command creates a Martini VLL.

The **undo mpls l2vc** command deletes the Martini VLL from an interface.

By default, no Martini L2VPN connection is created.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**group-id** *group-id* | **tunnel-policy** *policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **mtu** *mtu-value* | [**secondary** | **bypass**] | **ignore-standby-state**] *

undo mpls l2vc [**secondary** | **bypass**]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
vc-id	Specifies a L2VC ID.	The value is an integer that ranges from 1 to 4294967295.
group-id *group-id*	Specifies a VC group ID. With the VC group ID specified, the system can execute the same operation on a group of VCs; therefore, fewer packets are exchanged between PEs. Only the VCs with the same attribute can be configured with the same VC group ID; otherwise, the PW may be torn down by mistake. This parameter is valid only on sub-interfaces.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Removes the provider-tag (P-Tag) from a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-

Parameter	Description	Value
tagged	Retains the P-Tag in a packet. **NOTE** This parameter can be used only for Ethernet links. If neither **raw** nor **tagged** is specified, this command sets the **raw** mode on a main interface and the **tagged** mode on a sub-interface.	-
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
mtu *mtu-value*	Specifies the MTU value. **NOTE** This parameter can be configured only on VLANIF interfaces. The MTU of another type of interface or its sub-interface can be configured in the PW template.	The value is an integer that ranges from 46 to 9600. The default value is 1500.
secondary	Indicates a secondary VC. If this parameter is not specified, a primary VC is created. You can configure a secondary VC only when the primary VC exists on the local device.	-
bypass	Indicates that the VC is a bypass VC. The encapsulation type of the bypass VC must be the same as that of the primary VC.	-
ignore-standby-state	Indicates that the PW ignores standby state information sent by the remote device.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

According to different encapsulation modes on the AC interfaces, the system processes user packets in different ways, as shown in the following tables.

- Packet processing on the inbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Removes a tag.	No action is required.
Ethernet main interfaces	No action is required.	Adds a tag.
QinQ stacking sub-interface	No action is required.	Adds a tag.
QinQ termination sub-interface (in symmetrical mode)	Removes the outer tag.	No action is required.
QinQ termination sub-interface (in asymmetrical mode)	Removes two tags.	Removes the outer tag.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Adds a tag (default VLAN ID of the interface).
VLANIF interface (added to the VLAN in non-default mode)	Removes the outer tag.	No action is required.

- Packet processing on the outbound interface in the VLL or PWE3 scenario.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
Dot1q termination sub-interface	Adds a tag.	No action is required.
Ethernet main interfaces	Adds a tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.

AC Interface Type	Encapsulation Mode of raw	Encapsulation Mode of tagged
QinQ stacking sub-interface	No action is required.	Removes a tag.
QinQ termination sub-interface (in symmetrical mode)	Adds the outer tag.	Replaces the outer tag with the tag that is encapsulated on the outbound interface.
QinQ termination sub-interface (in asymmetrical mode)	Adds two tags.	Removes the outer tag and then adds two tags that are encapsulated on the outbound interface.
VLANIF interface (added to the VLAN in default mode)	No action is required.	Removes a tag.
VLANIF interface (added to the VLAN in non-default mode)	Adds the outer tag.	Replaces the tag with the tag that is encapsulated on the outbound interface.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You must create dynamic VCs on PEs at both ends of a PW to connect the PEs. The destination address of a VC is the LSR ID of the peer PE.
- You can set attributes for a PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring an LDP PW, you can directly apply the PW template without specifying attributes for the PW. After setting attributes for a PW template, you can update the PW template at any time. The modified PW template takes effect only after the **reset pw** command is run.
- If a PW attribute is specified in the **mpls l2vc** command, the corresponding PW attribute in the same PW template is invalid.
- If you do not specify a tunnel policy for a Martini connection, the default tunnel policy is used. By default, the LSP tunnel is preferentially selected and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the switch and other devices.
- You must configure the primary PW before configuring the secondary PW and delete the secondary PW before deleting the primary PW.

- When creating VCs dynamically, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.
- When configuring BFD for static PW, the VC ID must be specified.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

Create a Martini connection on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.2.2.9 100
```

Create a Martini connection on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls l2vc 10.2.2.9 100
```

10.6.17 mpls l2vc admin

Function

The **mpls l2vc admin** command creates a management PW (mPW).

The **undo mpls l2vc admin** command deletes an mPW.

By default, no mPW is configured.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**tunnel-policy** *policy-name* | **control-word** | **admin**] *

undo mpls l2vc [{ *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [**tunnel-policy** *policy-name* | **control-word** | **admin**] *]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the mPW peer, which is usually the LSR ID of the remote device.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies a VC ID. The VC ID must be unique on the local device, and identifies a VC together with the VC type. After a VC ID is configured, it cannot be modified. To modify a VC ID, delete the VC and configure it again. The VC IDs of the primary VC, secondary VC, and bypass VC must be different.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy. ● If the name of the tunnel policy is specified but the tunnel policy is not configured, the default tunnel policy is used. ● If the name of the tunnel policy is not specified, the default tunnel policy is used. The LSP tunnel is preferred and only one LSP is used for load balancing in the default tunnel policy. **NOTE** Before importing a tunnel policy, define the name and attribute of the tunnel policy in the system view first.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word	Enables the control word function. After the control word function is enabled, the device processes the Sequence Number, Length, and Layer-2 PDU fields in the packets.	-
admin	Designates the created PW as an mPW.	-

Views

Loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD is often configured for PWs to quickly detect PW faults. If there are a large number of service PWs with the same source and destination, you can configure mPWs with the same source and destination as those of the service PWs and associate the service PWs with the mPWs. By tracking the status of the mPWs, BFD can quickly detect faults on service PWs associated with the mPWs. BFD does not need to be configured for service PWs. This method reduces the number of BFD sessions and saves system resources and public network link bandwidth.

You can run the **mpls l2vc admin** command to create an mPW.

Prerequisites

MPLS L2VPN has been enabled using the **mpls l2vpn** command.

If **pw-template** *pw-template-name* is specified, a PW template has been created using the **pw-template** command.

Follow-up Procedure

Run the **mpls l2vc track admin-vc** command to associate service PWs with the mPWs.

Precautions

Generally, an mPW is configured on the primary PW path but not the secondary PW path.

Example

Create an mPW on loopback 0 with the remote device LSR ID 1.1.1.1 and VC ID 1.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-Loopback0] mpls l2vc 1.1.1.1 1 admin
```

10.6.18 mpls l2vc track admin-vc

Function

The **mpls l2vc track admin-vc** command associates service PWs with the mPWs.

The **undo mpls l2vc track admin-vc** command deletes the association between service PWs and mPWs.

By default, service PWs are not associated with the mPWs.

Format

mpls l2vc [**secondary** | **bypass**] **track admin-vc interface loopback** *interface-number*

undo mpls l2vc [**secondary** | **bypass**] **track admin-vc**

Parameters

Parameter	Description	Value
secondary	Associates the secondary service PW with the mPW.	-
bypass	Associates the bypass service PW with the mPW.	-
interface loopback *interface-number*	Specifies the loopback interface on which the mPW is configured.	The value is a decimal integer and must be the same as the number of the loopback interface on which the mPW is configured.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD is often configured for PWs to quickly detect PW faults. If there are a large number of service PWs with the same source and destination, you can configure mPWs with the same source and destination as those of the service PWs and associate these service PWs with the mPWs. By tracking the status of the mPWs, BFD can quickly detect faults on service PWs associated with the mPWs. BFD does not need to be configured for service PWs. This method reduces the number of BFD sessions and saves system resources and public network link bandwidth.

You can run the **mpls l2vc track admin-vc** command to associate service PWs with mPWs for service PW status monitoring.

Prerequisites

Service PWs and mPWs have been created using the **mpls l2vc** and **mpls l2vc admin** commands.

- An mPW and its associated service PW must have the same peers.
- A service PW can be associated with only one mPW.
- Multiple service PWs with the same source and destination can be associated with only one mPW.

Precautions

After service PWs are associated with an mPW, the mPW detects public network link faults in a unified manner.

- If the mPW status remains unchanged, traffic can be properly forwarded over service PWs.
- If the mPW detects a public link fault, the mPW changes its status from Up to Down and notifies all its associated service PWs.
  - If both primary and secondary service PWs exist, the mPW triggers a switchover between the primary and secondary service PWs.
  - If only one service PW exists, the service PW changes its status from Up to Down and stops forwarding data.
- After the fault is rectified, the mPW changes its status from Down to Up. If both primary and secondary service PWs exist, a switchover will be performed between them based on the configured revertive switching policy. If only one service PW exists, the service PW changes its status from Down to Up. The service PW then starts to forward traffic again.

The **mpls l2vc track admin-vc** command applies to only single-hop primary and secondary PWs and does not apply to multi-hop PWs.

Example

Associate the primary service PW with the mPW.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-Loopback0] mpls l2vc 1.1.1.1 1 admin
[HUAWEI-Loopback0] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 1.1.1.1 5
[HUAWEI-Vlanif10] mpls l2vc track admin-vc interface loopback 0
```

Associate the secondary service PW with the mPW.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-Loopback1] mpls l2vc 2.2.2.2 2 admin
[HUAWEI-Loopback1] quit
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] mpls l2vc 1.1.1.1 10
[HUAWEI-Vlanif20] mpls l2vc 2.2.2.2 6 secondary
[HUAWEI-Vlanif20] mpls l2vc secondary track admin-vc interface loopback 1
```

Associate the bypass service PW with the mPW.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 2
[HUAWEI-Loopback2] mpls l2vc 3.3.3.3 3 admin
[HUAWEI-Loopback2] quit
[HUAWEI] interface vlanif 30
[HUAWEI-Vlanif30] mpls l2vc 1.1.1.1 20 bypass
[HUAWEI-Vlanif30] mpls l2vc 3.3.3.3 7 bypass
[HUAWEI-Vlanif30] mpls l2vc bypass track admin-vc interface loopback 2
```

10.6.19 mpls l2vpn

Function

The **mpls l2vpn** command enables MPLS L2VPN and displays the MPLS L2VPN view.

The **undo mpls l2vpn** command disables MPLS L2VPN and deletes all the L2VPN configurations.

By default, the MPLS L2VPN function is disabled.

Format

mpls l2vpn

undo mpls l2vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MPLS L2VPN functions or perform configurations in the MPLS L2VPN view on the MPLS L2VPN network, run the **mpls l2vpn** command to enable MPLS L2VPN and enter the MPLS L2VPN view.

Prerequisites

Basic MPLS functions have been configured. For details, see the **mpls lsr-id** and **mpls** commands.

Precautions

When the command is configured, a P device does not need to be enabled with the MPLS L2VPN function.

After the **mpls l2vpn** command is executed:

- If MPLS L2VPN is disabled on the device, MPLS L2VPN is enabled and the MPLS L2VPN view is displayed.
- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

NOTICE

After the **undo mpls l2vpn** command is run in the system view, L2VPN services may be interrupted, and all L2VPN configurations are cleared. If you want to restore the L2VPN configurations, re-run all the deleted commands.

Example

Enable MPLS L2VPN.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn]
```

10.6.20 mpls l2vpn flow-label

Function

The **mpls l2vpn flow-label** command enables flow label-based load balancing for PWs on an interface.

The **undo mpls l2vpn flow-label** command disables flow label-based load balancing for PWs on an interface.

By default, flow label-based load balancing is disabled for PWs on an interface.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label { **both** | **send** | **receive** } [**secondary**] [**static**]

undo mpls l2vpn flow-label [**secondary**]

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-

Parameter	Description	Value
secondary	Enables flow label-based load balancing for the secondary PW. If **secondary** is not configured, flow label-based load balancing is configured for the primary PW. Flow label-based load balancing can be configured for a secondary PW only if the secondary PW exists.	-
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between provider (P) devices, configure flow label-based load balancing to improve L2VPN traffic forwarding efficiency. After flow label-based load balancing is enabled on a PE, the PE adds different labels for different L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it performs the Hash calculation and selects a forwarding path based on the flow label in the data packet. This processing implements load balancing. You can run the **mpls l2vpn flow-label** command to enable flow label-based load balancing for L2VPN on an interface.

Prerequisites

Before you enable flow label-based load balancing for an interface, create a VC connection on this interface and enable Multiprotocol Label Switching (MPLS) L2VPN.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.
- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

The **secondary** parameter indicates that flow label-based load balancing takes effect only for the secondary PW. If you specify **secondary** parameter, flow label-based load balancing takes effect only for the primary PW.

Example

Enable flow label-based load balancing for PWs on Vlanif 100.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif100] mpls l2vpn flow-label both
```

10.6.21 mpls l2vpn ip-parse enable

Function

The **mpls l2vpn ip-parse enable** command enables the IP packet parsing function of the MPLS L2VPN module.

The **undo mpls l2vpn ip-parse enable** command disables the IP packet parsing function of the MPLS L2VPN module.

By default, the IP packet parsing function of the MPLS L2VPN module is enabled.

Format

mpls l2vpn ip-parse enable

undo mpls l2vpn ip-parse enable

NOTE

This command is supported only on the S6720-EI and S6720S-EI.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Layer 2 VPN scenario, if a traffic policy is configured in the inbound direction of an AC-side interface on a device, L2VPN traffic forwarded from a PE may incorrectly match the traffic policy. As a result, traffic fails to be forwarded. To ensure normal traffic forwarding, run the **undo mpls l2vpn ip-parse enable** command to disable the IP packet parsing function of the MPLS L2VPN module.

Precautions

If the enhanced load balancing mode is configured for an Eth-Trunk, it is recommended that the IP packet parsing function of the MPLS L2VPN module be enabled.

Example

Disable the IP packet parsing function of the MPLS L2VPN module.

```
<HUAWEI> system-view
[HUAWEI] undo mpls l2vpn ip-parse enable
```

10.6.22 mpls l2vpn no-request-message

Function

The **mpls l2vpn no-request-message** command disables the device from sending L2VPN label request messages to a specified peer.

The **undo mpls l2vpn no-request-message** command re-enables the device to send L2VPN label request messages to a specified peer.

By default, the system sends L2VPN label request messages to all its peers.

Format

mpls l2vpn no-request-message peer *ip-address*

undo mpls l2vpn no-request-message peer *ip-address*

Parameters

Parameter	Description	Value
peer *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

On a PW in PWE3/Martini mode between two PEs with a Huawei device functioning as one PE and a non-Huawei device functioning as the other, if the non-Huawei device does not have the capability of processing L2VPN label requests, the **mpls l2vpn no-request-message** command needs to be run on the Huawei device to allow communication between the two devices. This command cannot be used in other cases.

Example

Disable the device from sending L2VPN label request messages to a peer with the LSR ID being 10.2.2.9.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn no-request-message peer 10.2.2.9
```

10.6.23 mpls l2vpn pw bfd

Function

The **mpls l2vpn pw bfd** command enables dynamic BFD for PWs and adjusts BFD parameters on an AC interface.

The **undo mpls l2vpn pw bfd** command restores default BFD parameters of dynamic BFD for PWs on an AC interface.

By default, dynamic BFD for PWs is not configured on an AC interface.

Format

mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** | **min-rx-interval** | **min-tx-interval**] * [**secondary**]

undo mpls l2vpn pw bfd [**detect-multiplier** *multiplier* | **min-rx-interval** *rx-interval* | **min-tx-interval** *tx-interval*] * [**remote-vcid** *vc-id*] [**secondary**]

Parameters

Parameter	Description	Value
detect-multiplier *multiplier*	Specifies the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Parameter	Description	Value
min-rx-interval *rx-interval*	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
min-tx-interval *tx-interval*	Specifies the minimum interval for sending BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-S, S5731-H and S5731S-H, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-S, S6730-H, and S6730S-H, the value ranges from 3 to 1000.
remote-vcid *vc-id*	Specifies the VC ID of the peer device.	This parameter is mandatory when a multi-hop PW is detected. The value of this parameter is the VC ID of the remote end of the PW. The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
secondary	Configures BFD and its parameters on the secondary PW. By default, BFD and its parameters are configured on the primary PW. **NOTE** The **secondary** parameter cannot be run on Loopback interface view.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where BFD is used to detect faults, run the **mpls l2vpn pw bfd** command to enable dynamic BFD for PWs and adjust BFD parameters on an AC interface.

Precautions

To reduce usage of system resources, when a BFD session is detected in Down state, the system changes the minimum interval for receiving BFD packets and the minimum interval for sending BFD packets to random values between 1000 ms and 3000 ms. When the BFD session becomes Up, the configured intervals are restored.

Example

Enable dynamic BFD for PWs on VLANIF 10 and set BFD parameters.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] mpls l2vpn pw bfd min-rx-interval 100 min-tx-interval 100
```

10.6.24 mpls l2vpn redundancy

Function

The **mpls l2vpn redundancy** command specifies the PW negotiation mode.

The **undo mpls l2vpn redundancy** command restores the default PW mode.

By default, a device determines the primary and secondary PWs locally by using FRR, without negotiating with other nodes.

Format

mpls l2vpn redundancy { **independent** | **master** }

undo mpls l2vpn redundancy { **independent** | **master** }

Parameters

Parameter	Description	Value
independent	Indicates PW redundancy in independent mode.	-
master	Indicates PW redundancy in master/slave mode.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring the primary and secondary PWs on a PE, you can specify the PW redundancy mode. The following PW redundancy modes are supported:

- FRR mode:

  The FRR mode is the default PW redundancy mode and does not need to be configured.

  The FRR mode applies to VLL FRR and PWE3 FRR scenarios. The FRR mode must be used with PW OAM and AC OAM. End-to-end FRR can be performed only after OAM mapping is enabled on the PE.
- Master/slave mode:

  The master/slave mode is often used in scenarios where VLL accesses VPLS. After the **mpls l2vpn redundancy** command is configured on a PE, the PE determines the primary/secondary status of PWs based on its local configurations. The master/slave mode can use the bypass PW to isolate PW-side failures from AC-side failures.
- Independent mode:

  The independent mode is often used with E-Trunk, and VRRP. The independent mode can use the bypass PW to isolate PW-side failures, but cannot isolate AC-side failures.

Prerequisites

The primary and secondary PWs must have been configured on the PE.

Follow-up Procedure

The FRR mode and master/slave mode support revertive policies. You can run the **mpls l2vpn reroute** command to configure a revertive policy. By default, the revertive switching is performed after a delay.

The independent mode supports only immediate switchback.

Precautions

If the **mpls l2vpn redundancy** command is run more than once, the latest configuration overrides previous ones. The **undo mpls l2vpn redundancy** command restores the FRR mode. When using the **undo mpls l2vpn redundancy** command, ensure that the parameter in this command is the same as that in the corresponding **mpls l2vpn redundancy** command.

The FRR mode applies to VLL and PWE3. The master/slave mode and independent mode apply to PWE3.

- FRR mode: After the primary and secondary PW status is configured on a PE to which a CE is single-homed, the FRR PW redundancy mode is used by default. The local PE does not notify the remote PW of the primary/secondary PW status. As a result, the remote PE is unaware of the local primary/secondary status.
- Master/slave mode: After this mode is configured, the PE determines the primary/secondary status of PWs based on local configurations and sends the Forwarding (0x00) and Forwarding Standby (0x20) status signaling to the remote PE.
- Independent mode: After this mode is configured, the PE determines the primary/secondary status of the local PWs based on the status information sent by the remote PE and sends the Forwarding (0x00) status signaling to the remote PE.

Example

Determine the primary and secondary PWs on VLANIF100 by using the PW negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 1.1.1.1 1
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 2 secondary
[HUAWEI-Vlanif100] mpls l2vpn redundancy independent
```

10.6.25 mpls l2vpn reroute

Function

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

The **undo mpls l2vpn reroute** command restores the default revertive switchover policy.

By default, delayed revertive switchover is configured in FRR or PW redundancy master/slave mode.

Format

mpls l2vpn reroute { { **delay** *delay-time* | **immediately** } [**resume** *resume-time*] | **never** }

undo mpls l2vpn reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies the revertive switchover policy for the primary and secondary PWs as delayed revertive switchover, and sets the duration for delayed switchover.	The value is an integer that ranges from 10 to 1800, in seconds. The default value is 30.
immediately	Specifies the revertive switchover policy for the primary and secondary PWs as immediate revertive switchover.	-
resume *resume-time*	Specifies a delay after which the local device notifies the peer PE on the secondary PW of the recovery. You can set this parameter only in VLL FRR mode.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 10.
never	Specifies the revertive switchover policy for the primary and secondary PWs to none revertive switchover. After the primary PW recovers, traffic is not switched to it until the secondary PW is faulty.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

Prerequisites

The primary and secondary PWs have been configured in FRR or PW redundancy master/slave mode. The revertive switchover policy cannot be configured for PW redundancy independent mode.

Precautions

In VLL FRR mode and in PW redundancy master/slave mode, the PW revertive switchover policy is classified into the following modes:

- Immediate revertive switchover: When the primary PW recovers from a fault, the local PE switches traffic back to the primary PW immediately and notifies the peer PE on the secondary PW of the fault. In FRR mode, the local PE notifies the peer PE on the secondary PW of the recovery after a delay of *resume-time*. In PW redundancy master/slave mode, the parameter *resume-time* is not supported.

  This revertive switchover applies to scenarios in which users hope traffic to be restored as soon as possible.
- Delayed revertive switchover: When the primary PW recovers from a fault, traffic is switched back to the primary PW after a period specified by *delay-time*. After traffic is switched back, the local device immediately notifies the peer device on the secondary PW of the fault. If *resume-time* is configured in FRR mode, the local device notifies the peer device on the secondary PW of the recovery after a delay of *resume-time*.

  On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.
- None revertive switchover: When the primary PW recovers from a fault, traffic is not switched back to the primary PW until the secondary PW becomes faulty.

  If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive switchover.

In a CE asymmetrical networking, if the Ethernet OAM function is configured on a PE interface connected to a CE, and a revertive switchover policy is configured, the value of *resume-time* cannot be 0 seconds. The value must be equal to or greater than 1 second.

Example

Configure the device to switch traffic back to the primary PW 15 seconds after the primary PW recovers from a fault, notify the peer PE on the secondary PW of the fault when a switchover is performed, and notify the peer PE of the secondary PW of the recovery 20 seconds later.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 10.1.1.9 100
[HUAWEI-Vlanif100] mpls l2vc 10.2.2.9 200 secondary
[HUAWEI-Vlanif100] mpls l2vpn reroute delay 15 resume 20
```

10.6.26 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL service or a PWE3 service.

The **undo mpls l2vpn service-name** command deletes the configured L2VPN service name.

By default, no L2VPN service name is configured in the system.

Format

mpls l2vpn service-name *service-name*

undo mpls l2vpn service-name

Parameters

Parameter	Description	Value
service-name	Specifies the name of an L2VPN service. This parameter uniquely identifies an L2VPN service on a PE.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC or Martini VLL service or a PWE3 service is uniquely identified by the combination of the VC ID and VC type, which are hard to remember and make maintenance complex. When a service name is used to uniquely identify an L2VPN service, the name can be defined based on requirements and the NMS operator can maintain the L2VPN service by clicking the name on the NMS graphical user interface (GUI). This simplifies operation and maintenance.

Prerequisites

An SVC or Martini VLL service or a PWE3 service has been configured on a service interface. A primary PW and a secondary PW can be configured for a Martini VLL or PWE3 service.

Precautions

On each PE, an L2VPN service name is unique. If an L2VPN service name has been used by a PW, it cannot be configured for another PW, or the system will display an error message.

If an L2VPN service already has a service name, this service name will be overwritten when a new name is configured for the L2VPN service. Therefore, when changing an L2VPN service name, you can directly configure a new service name without deleting the original one.

- Because the primary and secondary PWs are configured on the same interface, they are regarded as one PW, and a service name is configured for both of them.
- On each PE, an L2VPN service name is unique.

Example

Set an L2VPN service name to **pw1** on a service interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 10.1.1.1 1
[HUAWEI-Vlanif10] mpls l2vpn service-name pw1
```

10.6.27 mpls l2vpn stream-dual-receiving

Function

The **mpls l2vpn stream-dual-receiving** command configures an interface to receive packets from both the primary and secondary PWs.

The **undo mpls l2vpn stream-dual-receiving** command disables an interface from receiving packets from both the primary and secondary PWs.

By default, an interface cannot receive packets from the secondary PW.

Format

mpls l2vpn stream-dual-receiving

undo mpls l2vpn stream-dual-receiving

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network configured with PW Redundancy, the **mpls l2vpn stream-dual-receiving** command must be run on a PE to which the CE is single homed, so that the PE can receive packets from both the primary and secondary PWs. This prevents packet loss during the PW switchover process.

If the command is not run, the PE receives packets only from the primary PW. This causes packet loss during a traffic switchover. After the primary PW recovers and a traffic switchover is triggered, the secondary PW on the PE becomes the primary PW and the PE notifies the peer of the status change. A delay in signaling transmission causes the peer PE to send packets along the secondary PW. After the PE receiving packets from the secondary PW, the PE discards the packets, resulting in packet loss.

Prerequisites

Primary and secondary PWs have been configured.

Precautions

The **mpls l2vpn stream-dual-receiving** command applies to only PWE3 L2VPN. If H-VPLS is configured, the command cannot be configured. If you configure this command, unidirectional broadcast traffic will be looped back.

Bypass PWs cannot be configured on a PE configured with the **mpls l2vpn stream-dual-receiving** command.

Kompella VLL FRR does not support the **mpls l2vpn stream-dual-receiving** command.

Example

Enable the device to receive packets from both the primary and secondary PWs on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 1.1.1.1 1
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 2 secondary
[HUAWEI-Vlanif100] mpls l2vpn stream-dual-receiving
```

10.6.28 mpls l2vpn switchover

Function

The **mpls l2vpn switchover** command switches traffic from the primary PW to the secondary PW.

The **undo mpls l2vpn switchover** command disables traffic switchover and switches traffic back to the primary PW.

By default, traffic switchover is not configured.

Format

mpls l2vpn switchover

undo mpls l2vpn switchover

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In master/slave PW redundancy mode, the traffic is transmitted over the primary PW in normal situations. If you want the traffic to be transmitted over the secondary PW due to reasons such as device upgrade or service re-deployment, you can use the **mpls l2vpn switchover** command to forcibly switch traffic from the primary PW to the secondary PW. After the device is upgraded or services are re-deployed, you can run the **undo mpls l2vpn switchover** command to forcibly switch traffic from the secondary PW to the primary PW.

- Before running the **mpls l2vpn switchover** command, ensure that the secondary PW is normal and can forward traffic.
- Before running the **undo mpls l2vpn switchover** command, ensure that the primary PW is normal and can forward traffic.

NOTE

If the secondary PW fails after traffic is forcibly switched to the secondary PW, the traffic will be switched back to the primary PW.

Prerequisites

The primary and secondary PWs have been established and are in the Up state.

Precautions

A PW switchover will be performed after you run the **mpls l2vpn switchover** or **undo mpls l2vpn switchover** command. If the PW to be switched to is Down or unavailable, the switchover fails.

Traffic cannot be switched from the primary PW to a bypass PW.

The two commands apply to only PWs working in master/slave mode. In a VLL FRR scenario, use the **manual-set pw-ac-fault** command to forcibly switch over PWs.

Example

Switch traffic from the primary PW to the secondary PW.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls l2vc 1.1.1.1 1
[HUAWEI-Vlanif100] mpls l2vc 2.2.2.2 2 secondary
```

```
[HUAWEI-Vlanif100] mpls l2vpn redundancy master
[HUAWEI-Vlanif100] mpls l2vpn switchover
```

10.6.29 mpls l2vpn vccv bfd-cv-negotiation fault-detection-only

Function

The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type for BFD CV packets to be sent to remote peers.

The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default configuration.

By default, the device sends BFD CV packets with the encapsulation type 0x08 to all remote peers.

Format

mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address* { **enable** | **disable** }]

undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address*]

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IP address of a remote peer.	The value is in dotted decimal notation.
enable	Sets the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.	-
disable	Set the encapsulation type 0x08 for BFD CV packets to be sent to a specified remote peer.	-

Views

MPLS L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Virtual Circuit Connectivity Verification (VCCV) is a mechanism to detect and diagnose end-to-end faults on PWs. VCCV provides a control channel between a PW's ingress and egress over which connectivity verification (CV) messages can be sent. A VCCV message includes a BFD control packet encapsulated as specified by the CV type. A BFD CV packet can be transmitted over a VCCV control channel after being encapsulated using BFD IP/UDP. As defined in RFC, BFD IP/UDP encapsulation for BFD CV packets are classified into two types:

- 0x04: used only for PW fault detection.
- 0x08: used for PW fault detection and AC/PW status signaling.

To control the encapsulation type of BFD CV packets to be sent to remote peers, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command.

- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to all remote peers.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default encapsulation type 0x08 for BFD CV packets to be sent to all remote peers.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to a specified remote peer.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **disable** command sets the encapsulation type to 0x08 for BFD CV packets to be sent to a specified remote peer.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* command restores the global encapsulation type for BFD CV packets to be sent to a specified remote peer.

Dynamic PWs support VCCV by default, and can use LDP signaling to advertise local attributes to remote peers. The default encapsulation type of BFD CV packets is 0x08. If a remote peer supports the encapsulation type 0x04 and BFD is used for communication, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command to change the encapsulation type of BFD CV packets to be sent to this peer to 0x04.

Precautions

After this command is run, PWs may be re-established, which causes a short service interruption.

Example

Set the encapsulation type 0x04 for BFD CV packets to be sent to remote peers.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only
```

Set the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer 10.10.10.1 enable
```

10.6.30 mpls static-l2vc

Function

The **mpls static-l2vc** command creates a static VC.

The **undo mpls static-l2vc** command deletes the static VCs.

By default, no static VC is created.

Format

mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

undo mpls static-l2vc

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**]] *

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a static PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
transmit-vpn-label *transmit-label-value*	Specifies the value of a transmit label.	The value is an integer that ranges from 0 to 1048575.
receive-vpn-label *receive-label-value*	Specifies the value of a receive label.	The value is an integer that ranges from 16 to 1023.

Parameter	Description	Value
tunnel-policy *tnl-policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word | **no-control-word**	Enables or disables the control word function. By default, the control word function is disabled.	-
raw	Removes the provider-tag (P-Tag) from a packet.	-
tagged	Retains the P-Tag in a packet.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an L2VPN networking, you can use this command to create a static VC between two PEs connected to CEs.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You can set attributes for a static PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring a static PW, you can directly use the static PW template without specifying attributes for the PW. After setting attributes for a static PW template, you can update the static PW template at any time. The modified static PW template takes effect only after the **reset pw** command is run.
- Static VCs must be created on PEs at both ends. The destination address of a VC is the LSR ID of the peer PE. The transmit label of the PE at one end is the

receive label of the PE at the other end. If the labels do not match, traffic may fail to be forwarded even though the **static-l2vc** field is displayed as Up.

- If no tunnel policy is specified, the default tunnel policy is used. The default policy specifies that traffic is forwarded along the LSP and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- When configuring a static VC, note that the value of the transmit label ranges from 0 to 1048575. This ensures the communication between the device and different types of devices.
- When creating static VCs, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, and **no-control-word**.
- By default, link type negotiation is enabled globally on the device. If a VLANIF interface is used as an AC-side interface for L2VPN, the configuration conflicts with link type negotiation. In this case, run the **lnp disable** command in the system view to disable link type negotiation.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.

Example

Configure a static VC. Set the LSR ID of the peer device to 1.1.1.1, transmit label to 100, and receive label to 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
```

Configure a static VC by applying a PW template and set values of the VC ID, transmit label, and receive label to 100 respectively.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls static-l2vc pw-template pwt 100 transmit-vpn-label 100 receive-vpn-label 100
```

Delete a static VC.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] undo mpls static-l2vc
```

10.6.31 mpls switch-l2vc

Function

The **mpls switch-l2vc** command configures PW switching on the SPE to implement multi-segment PWs.

The **undo mpls switch-l2vc** command deletes PW switching.

The default policy is used for PW switching. In the default policy, LSP tunnels are used and the number of routes for load balancing is 1.

Format

Static PW

mpls switch-l2vc *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**control-word-transparent**]

Dynamic PW

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**control-word-transparent**]

Mixed PW

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**flow-label** { **both** | **send** | **receive** }] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] [**oam-packet pop flow-label**] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**flow-label** { **both** | **send** | **receive** }] [**control-word-transparent**]

undo mpls switch-l2vc { *ip-address vc-id* **encapsulation** *encapsulation-type* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.

Parameter	Description	Value
vc-id	Specifies the L2VC ID.	The value is an integer that ranges from 1 to 4294967295.
trans *trans-label*	Specifies the static label for sending packets.	The value is an integer that ranges from 0 to 1048575.
recv *received-label*	Specifies the static label for receiving packets.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *policy-name*	Specifies the name of a tunnel policy. If this parameter is not specified, the default tunnel policy is used, which preferentially selects the LSP tunnel and only one tunnel is used for load balancing.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
oam-packet pop flow-label	Specifies that flow labels of OAM packets are popped out. If OAM packets received from remote devices carry flow labels, the **oam-packet pop flow-label** parameter must be configured to pop out flow labels so that the SPEs can process the OAM packets. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-
between	Specifies the switching PW that corresponds to the PW	-

Parameter	Description	Value
encapsulation *encapsulation-type*	Specifies the encapsulation type of a static PW.	The encapsulation types supported by PW switching are **ethernet**, **vlan**, and **ip-interworking**. **NOTE** Static and mixed PWs support only Ethernet and VLAN encapsulation types.
mtu *mtu-value*	Specifies the MTU for negotiating dynamic PW signaling. If the non-default MTU is set when you configure a dynamic PW, you need to set the MTU manually when configuring mixed PW switching; otherwise, the signaling negotiation at the dynamic PW side may fail.	The value is an integer that ranges from 46 to 9600.
control-word	Enables the control word function. By default, the control word function is disabled.	-
no-control-word	Disable the control word function.	-
cw	Indicates the mode in which the control word function is enabled.	-
alert	Indicates the label alert tunnel for VCCV ping.	-
cv	Indicates connectivity verification, which is enabled by default.	-
lsp-ping	Indicates connectivity verification in LSP ping mode for VCs, which is enabled by default.	-

Parameter	Description	Value
control-word-transparent	Enables transparent transmission of the control word. In the scenario where a PE is dual homed to SPEs and BFD for PW is enabled, transparent transmission of the control word must be enabled on the SPEs; otherwise, the BFD negotiation fails. By default, transparent transmission of the control word is disabled.	-
all	Deletes all PW switching.	-
flow-label both	Enables flow label-based load balancing for outgoing traffic and incoming traffic. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-
flow-label send	Enables flow label-based load balancing for outgoing traffic. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-
flow-label receive	Enables flow label-based load balancing for incoming traffic. **NOTE** Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this parameter.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls switch-l2vc** command configures PW switching on the SPE to implement multi-segment PWs.

PW switching can be classified into dynamic mode, static mode, and mixed mode. You can create PW switching of different types using different commands to meet site requirements:

- **Configuring static PW switching**: The two PW segments connected by an SPE are both static PWs. Static PW switching apples when static PWs are used on the entire network.
- **Configuring dynamic PW switching**: The two PW segments connected by an SPE are both dynamic PWs. Dynamic PW switching applies when dynamic PWs are used on the entire network.
- **Configuring mixed PW switching**: A mixed PW switching applies when an SPE connects a dynamic PW and a static PW.

Precautions

You need to configure the PW label for the static PW switching and for the static PW in the mixed PW switching.

The configuration of dynamic PW switching is simple. The remote label is sent from two neighboring ends (UPE or SPE) to the SPE through signaling. The CW and the VCCV are sent from two UPE nodes to the SPE through signaling.

When you configure mixed PW switching, the value of *ip-address vc-id* before **between** in the command is for the dynamic PW, and the value of *ip-address vc-id* after **between** in the command is for the static PW. The two values cannot be interchanged.

NOTE

- The VC IDs for PW switching can be different.
- The combination of the PW ID and PW type must be unique on each node. The PW IDs at two ends of PW switching can be the same.
- When creating PW switching, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *policy-name*, **control-word-transparent**, **control-word**, **no-control-word**, **mtu** *mtu-value*, **oam-packet pop flow-label**, and **flow-label** { **both** | **send** | **receive** }.

Example

Configure dynamic PW switching.

```
<HUAWEI> system-view
[HUAWEI] mpls switch-l2vc 1.1.1.9 100 between 3.3.3.9 100 encapsulation vlan
```

Configure static PW switching.

```
<HUAWEI> system-view
[HUAWEI] mpls switch-l2vc 1.1.1.9 100 trans 100 recv 100 between 3.3.3.9 100 trans 200 recv 200
encapsulation vlan
```

Configure mixed PW switching.

```
<HUAWEI> system-view
[HUAWEI] mpls switch-l2vc 1.1.1.9 100 between 3.3.3.9 100 trans 200 recv 200 encapsulation vlan mtu
1500
```

Delete PW switching.

```
<HUAWEI> system-view
[HUAWEI] undo mpls switch-l2vc 1.1.1.9 100 encapsulation vlan
```

10.6.32 mtu (PW template view)

Function

The **mtu** command specifies the MTU in a PW template.

The **undo mtu** command restores the default setting.

By default, the MTU in a PW template is 1500.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU in a PW template.	The value is an integer that ranges from 46 to 9600.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When creating a PW template, run the **mtu** command to specify the MTU for the PW template.

Precautions

When creating a Martini VLL or PWE3 VLL, if you set the MTU value by specifying **mtu** *mtu-value* in the **mpls l2vc** command. If you do not specify **mtu** *mtu-value*, the MTU in the PW template takes effect. If you do not specify **mtu** *mtu-value* in the **mpls l2vc** command and do not set the MTU in the PW template, the device uses the default MTU value 1500.

Example

Configure the MTU for the PW template **pw1**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pw1
[HUAWEI-pw-template-pw1] mtu 1600
```

10.6.33 peer-address

Function

The **peer-address** command assigns a remote IP address to a PW template.

The **undo peer-address** command deletes the remote IP address assigned to a PW template.

By default, a PW template is not configured with a remote IP address.

Format

peer-address *ip-address*

undo peer-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the peer. Generally, *ip-address* is a loopback address of the peer and needs be the same as the destination address of the tunnel.	The value is in dotted decimal notation.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The peer IP address can be set either using a PW template or the **mpls l2vc** command. The PW template allows you to modify the peer IP address in real time. If you want to change the peer IP address using the **mpls l2vc** command, you must delete the existing peer IP address first.

After the peer IP address is changed:

- If the PW template is in use, you must run the **reset pw pw-template** command for the change to take effect. This, however, may disconnect and re-establish the PWs that apply the PW template.
- If the PW template is not in use, it does not need to restart.

Prerequisites

- MPLS L2VPN has been enabled in the system view.
- A PW template has been created in the system view.

Precautions

If the peer IP address has been configured using both a PW template and the **mpls l2vc** command, only the peer IP address configured using the **mpls l2vc** command takes effect.

Example

Assign a remote IP address to a PW template.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] peer-address 1.1.1.1
```

Modify a remote IP address in a PW template.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] undo peer-address
[HUAWEI-pw-template-pwt] peer-address 2.2.2.2
```

10.6.34 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** [**remote** *remote-ip-address peer-pw-id* | **draft6**] * [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word remote** *remote-ip-address peer-pw-id* **sender** *sender-address* [**ttl** *ttl-value*] [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address* | **draft6**] * [**pipe** | **uniform**]

ping vc *pw-type pw-id* [*peer-address*] [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **normal** [**no-**

control-word] [**remote** *remote-ip-address peer-pw-id*] [**ttl** *ttl-value*] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **ip-interworking**, and **vlan**.
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies the peer LSR ID of a local PW. In PWE3 and Martini VLL scenarios, if the VC IDs of the primary and secondary VCs are the same, this parameter must be specified to uniquely identify a PW.	The value is in dotted decimal notation.
-c *echo-number*	Specifies the number of Echo Request messages to be sent. If the network works unstably, you can set this parameter to a larger value to test network quality based on the packet loss ratio.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the interval for sending Echo Request messages. Each time after the source sends an Echo Request message by using the **ping vc** command, it waits a period of time (2000 ms by default) before sending the next Echo Request message. You can set the interval for sending Echo Request messages through the parameter *time-value*. If the network works unstably, the value should be greater than or equal to 2000 ms.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-s *data-bytes*	Specifies the number of bytes of the sent Echo Request messages.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100.

Parameter	Description	Value
-t *timeout-value*	Specifies the timeout period for sending Echo Request messages.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-exp *exp-value*	Specifies the EXP value of the sent Echo Request messages. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply messages. ● 1: No MPLS Echo Reply message is returned. ● 2: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply messages are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-v	Displays the detailed information.	-
no-control-word	Disables the control word function.	-
control-word	Enables the control word function. The switching node along a multi-segment PW does not transmit ping packets. When the control word function is enabled, you can ping only the termination node of the PW. Before using the control word to ping the PW, you must enable the control word for a PW.	-

Parameter	Description	Value
remote	Specifies information about the PW on the remote PE. Information specified by the remote PE is finally encapsulated into the ping packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the ping packets is the information about the PW on the local end, which applies to single-segment PWs.	-
peer-pw-id	Specifies the ID of the PW on the peer.	The value is an integer that ranges from 1 to 4294967295. By default, the peer PW ID is the same as the local PW ID.
draft6	Specifies the command version. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06". By default, the ping operation is performed based on RFC 4379.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire MPLS domain is considered as one hop and the IP TTL of the probe packet is reduced by one on the ingress and egress respectively.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-

Parameter	Description	Value
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of a multi-segment PW, if the ping operation is performed in control word mode, the IP address of the termination node must be specified. In MPLS router alert mode, the IP address of any switching node or the termination node can be specified. Then, the Echo Request message is sent to the peer and then sent back.	-
label-alert	Specifies the label alert mode. The switching node along a multi-segment PW sends ping packets forcibly. In MPLS router alert mode, you can ping any switching node along the PW.	-
normal	Specifies the normal mode, that is, the TTL detection mode. In this mode, control word and router alert are not encapsulated in to MPLS Echo Request messages, and TTL values are used to detect PW connectivity.	-
ttl *ttl-value*	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default value is 64.
sender *sender-address*	Specifies a source address. For end-to-end detection of a multi-segment PW, a source IP address needs to be specified for a public network device that communicates with the remote PE. Generally, the source IP address is the address of the adjacent SPE or UPE.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect.

The **ping vc** command can be used to check a PW in the following scenarios:

VLL networking

Based on VLL types, the VLL PW ping can be classified into the following types:

- PWE3 VLL PW ping: In a PWE3 VLL networking, a PW ping is initiated to check the connectivity of a PW. A PWE3 VLL PW ping can be performed in control word mode, TTL mode, or label alert mode. In a ping test, a local PE sends an Echo Request message to the peer PE. After receiving the message, the peer PE abstracts and sends FEC information to the L2VPN module to determine whether the message has reached the egress. If so, the peer PE returns an Echo Reply message.
- Kompella VLL PW ping: A VLL PW ping is initiated to check the connectivity of a PW. Different from the PWE3 networking, the Kompella VLL does not need the PW template and supports the control word, TTL, and label alert modes.

VPLS networking

Based on the VPLS types, the VPLS PW ping can be classified into the following types:

- Martini VPLS PW ping: The Martini VPLS PW ping supports only the label alert mode. On a Hierarchical Virtual Private LAN Service (HVPLS) network, the Martini VPLS PW ping can only detect single-segment PWs. If an optional PW ID is configured and specified, the PW with the PW ID is detected. If the PW ID is not specified, the PW with a specified VSI ID is detected.
- Kompella VPLS PW ping: The Kompella VPLS PW ping supports only the label alert mode.

If a PW fault is detected by using the **ping vc** command, the **tracert vc** command can be used to locate the fault. Both the **ping vc** command and the **tracert vc** command can properly check the connectivity of PWs and locate faults.

Prerequisites

The MPLS module has been enabled on the device and works properly.

Precautions

control-word is recommended to detect the entire PW. Even though **label-alert** can be used to check the entire PW, the whole process is the same as the forwarding process only when **control-word** is used.

The execution of the **ping vc** command terminates when either of the following situations occurs:

- The ping packet reaches the egress.
- The TTL value of the ping packet reaches the upper threshold.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary

PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Run the **ping vc** command in label alert mode on the device to check the connectivity of an Ethernet PW.

```
<HUAWEI> ping vc ethernet 100 -c 10 -m 10 -s 65 -t 100 -v label-alert remote 2.2.2.2
  Reply from 2.2.2.2: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
  10 packet(s) transmitted
  10 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

10.6.35 pw-template

Function

The **pw-template** command creates a PW template. In the PW template, you can set attributes for a PW, such as the peer, control word, and tunnel policy.

The **undo pw-template** command deletes a PW template.

By default, no PW template is created.

Format

pw-template *pw-template-name*

undo pw-template *pw-template-name*

Parameters

Parameter	Description	Value
pw-template-name	Specifies the PW template name.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Importing a PW template simplifies the configuration of PWs with similar attributes.

Prerequisites

L2VPN has been enabled by running the **mpls l2vpn** command.

Precautions

- If a PW template is applied to a PW, the PW template cannot be deleted.
- When a PW template is applied to a PW, the PW uses the PW attributes specified on the interface if the PW attributes specified on the interface are different from those specified in the template.
- When modifying attributes in a PW template, run the **reset pw** command to make the modification take effect. This will cause PW disconnection and reconnection.
- After a PW is bound to a link detection protocol, the remote IP address in the PW template cannot be changed. To change the remote IP address, unbind the PW from the link detection protocol.

Example

Create a PW template named **pwt1**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt1
[HUAWEI-pw-template-pwt1]
```

10.6.36 reset pw

Function

The **reset pw** command re-creates a PW or a PW template.

Format

reset pw { [**peer-address** *peer-address*] *pw-id pw-type* | **pw-template** *pw-template-name* }

Parameters

Parameter	Description	Value
peer-address *peer-address*	Specifies the IPv4 address of the target PE.	The value is in dotted decimal notation.

Parameter	Description	Value
pw-id	Specifies the ID of a VC connected to L2VPN.	The value is an integer that ranges from 1 to 4294967295.
pw-type	Specifies the encapsulation type of a PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, and **ip-interworking**.
pw-template	Re-creates all PWs in the PW template.	-
pw-template-name	Specifies the PW template name.	The value is an existing PW template name.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After changing the parameters in a PW template, you need to run the **reset pw pw-template** command to make the modification take effect. The configuration on the PW template applies to all PWs using this PW template. You can configure the attributes of a PW by using a PW template or commands. The attributes configured by using commands take precedence over those configured by using the template. If you configure PW attributes by using commands, the corresponding attributes in the PW template do not take effect. Therefore, if you run the **reset pw pw-template** and **reset pw** *pw-id* commands, the PW attributes remain unchanged. To change a PW attribute, configure the attribute in the PW template but do not configure attribute by using a command.

Example

Re-create a PW by specifying the VC ID and VC type.

```
<HUAWEI> reset pw 100 vlan
```

Re-create all PWs that use the PW template named **pwt1**.

```
<HUAWEI> reset pw pw-template pwt1
```

10.6.37 tnl-policy (PW template view)

Function

The **tnl-policy** command configures a tunnel policy for a PW template.

The **undo tnl-policy** command deletes the tunnel policy configured for a PW template.

By default, no tunnel policy is configured for a PW template.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the tunnel policy name of a PW.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

The **tnl-policy** command specifies a PWE3 tunnel policy based on which a PW selects a tunnel to be associated with.

If no policy is configured, an LSP tunnel is selected and load balancing is not performed.

Example

Configure a tunnel policy named **policy1** for a PW template named **pwt**.

```
<HUAWEI> system-view
[HUAWEI] pw-template pwt
[HUAWEI-pw-template-pwt] tnl-policy policy1
```

10.6.38 tracert vc

Function

The **tracert vc** command detects the status of a PW or locates a faulty node on a PW in Down state.

Format

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-ip-address* [**ptn-mode** | **full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-pw-id* **draft6** [**full-lsp-path**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

tracert vc *pw-type pw-id* [*peer-address*] [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**pipe** | **uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, and **ip-interworking**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
peer-address	Specifies a peer LSR ID for the local PW. In a PWE3 or Martini VLL scenario, if the primary and secondary VCs are configured with the same VC ID, this parameter must be specified to determine a unique PW to be monitored.	The value is in dotted decimal notation.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0. **NOTE** If DSCP priority has been configured by running the **set priority** command, the *exp-value* parameter does not take effect.	The value is an integer that ranges from 0 to 7.

Parameter	Description	Value
-f *first-ttl*	Specifies the initial Time-to-Live (TTL).	The value is an integer that ranges from 1 to 255, and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from 1 to 255, and must be larger than the value of *first-ttl*. The default value is 30.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets. ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated in IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated in IPv4/IPv6 /IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4.
-t *timeout-value*	Specifies the timeout interval of an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
control-word	Indicates that the control word is encapsulated in the MPLS Echo Request packet.	-
label-alert	Indicates that the router alert label is encapsulated in the MPLS Echo Request packet.	-

Parameter	Description	Value
no-control-word	Indicates that the control word is not encapsulated in the MPLS Echo Request packet.	-
normal	Indicates the normal mode where the router alert label and control word are not encapsulated in the MPLS Echo Request packet.	-
remote	Specifies information about the PW on the remote PE.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. If **label-alert** is configured, you can specify the IP address of any switching node or the termination node.	-
remote-pw-id	Specifies the ID of the remote PW. By default, the ID of the local PW is used. If the tracert operation is performed in control word mode for a multi-segment PW, the IP address of the termination node must be specified.	-
ptn-mode	Specifies the PTN mode. In a multi-segment PW scenario, this parameter is indicated that trace VC packets are replied. You need to run the **lspv pw reply ptn-mode** command on both the SPE and TPE.	-
full-lsp-path	Displays the responses from all nodes along the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, only the responses from the PW nodes along the LSP are displayed.	-
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire domain is regarded as one hop and the IP TTL of the probe packet is reduced by one on both the ingress and egress.	-

Parameter	Description	Value
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
draft6	Specifies the version of the **tracert vc** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379. **NOTE** Tracert VC based on **draft6** is applied only to VLL over LDP scenarios.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a fault occurs on the PW, the **ping vc** command can be used to check the connectivity of the network, and the **tracert vc** command can be used to locate the fault and provide reference for fault diagnosis. If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. If a PW is down, the **tracert vc** command must be used to locate the faulty node on the PW.

The **tracert vc** command applies to the following networking scenarios:

- PWE3 VLL PW tracert

  In PWE3 VLL networking, PW tracert can help you obtain information about SPEs and Ps along the path that the message travels from the source to the destination, check the connectivity of the PW, and locate the fault of the PW.

  A PWE3 VLL PW tracert can be performed in control word mode, label alert mode, or TTL mode. The default mode is label alert. The TTL mode and control word mode are mutually exclusive.

  To detect faults on a VLL network with control word enabled, run the **tracert vc** *pw-type pw-id* **control-word** command.

  To encapsulate packets with the router alert label and detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* **label-alert** command.

  If control word is not enabled and packets are not encapsulated with the router alert label, to detect faults on a VLL network, run the **tracert vc** *pw-type pw-id* command.

The TTL value of the PW Tracert Request message is incremented by 1 each time. Each time the transit node (P) receives an Echo Request message after the TTL value of the message expires, it sends the Echo Request message to the LSPV module. Then the transit node returns an Echo Reply message carrying the next hop information.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.
- The MPLS module has been enabled on each node and works properly.
- The ICMP module of each node works properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert vc** command is as follows:

1. The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
2. The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
3. The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
4. The preceding steps continue until the MPLS Echo Request packet reaches the destination.

When the device on each hop receives the MPLS Echo Request packet, it will respond with an MPLS Echo Reply packet, indicating that the tracert test ends. In the command output information of the source device, you can view the path that the packet passes through.

Configuration Impact

In control word mode, if a transit node receives an MPLS Echo Request packet whose TTL does not time out, it does not send the packet to the CPU. In this mode, the source obtains only a little PW information and cannot obtain information about the downstream devices of the transit node. This mode is recommended when the traffic volume is heavy.

In router alert mode, a transit node sends the received MPLS Echo Request packets to the CPU. In this mode, the source obtains a lot of PW information; therefore, device performance is affected when the traffic volume is heavy. This mode is recommended when the traffic volume is light.

Information specified by **remote** is encapsulated in MPLS Echo Request packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the MPLS Echo Request packets is about the PW on the local PE. This applies to single-segment PWs.

Precautions

- When the probe packet reaches the egress or the TTL reaches the upper threshold, the PW tracert is terminated.

- You can press **Ctrl + C** to terminate the execution of the **tracert vc** command.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Trace a multi-segment PW. The encapsulation type, local PW ID, and remote PW ID of the PW is ethernet, 100, and 200.

```
<HUAWEI> tracert vc ethernet 100 control-word remote 200 draft6 full-lsp-path
 TTL   Replier            Time    Type      Downstream
 0                            Ingress   10.1.1.2/[1025 ]
 1     10.1.1.2          230 ms  Transit   10.2.1.2/[3 ]
 2     10.2.1.2          230 ms  Transit   10.3.1.2/[3 ]
 3     10.3.1.2          100 ms  Transit   10.4.1.2/[3 ]
 4     10.4.1.2          150 ms  Egress
```

Table 10-89 Description of the **tracert vc** command output

Item	Description
TTL	TTL value in an Echo Request packet. It represents the number of hops along the path through which an Echo Request packet passes.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time when the packet is processed.
Type	Node type. The value can be: - Ingress: indicates an ingress node. - Transit: indicates a transit node. - Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

10.7 VPLS Configuration Commands

10.7.1 Command Support

Only the following switch models support VPLS:

S5731-S, S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-S, S6730S-H, and S6730-H

10.7.2 broadcast-suppression cir cbs (VSI view)

Function

The **broadcast-suppression cir cbs** command enables the broadcast traffic suppression function in a VSI.

The **undo broadcast-suppression** command disables the broadcast traffic suppression function in the VSI.

By default, the broadcast traffic suppression function is disabled in a VSI.

Format

broadcast-suppression cir *cir-value* **cbs** *cbs-value*

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the Committed Information Rate (CIR), that is, the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the Committed Burst Size (CBS), that is, the traffic that can pass instantly, or the depth of the first token bucket.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPLS network, broadcast packets, multicast packets, and unknown unicast packets are transmitted in broadcast mode and copied to neighboring ACs and PWs. If a large number of broadcast packets are sent to the access device on the network, the device has to make a lot of copies of these broadcast packets, which wastes bandwidth and resources, and degrades the performance of the system. You can run the **broadcast-suppression cir cbs** command to suppress the broadcast traffic in the VSI. The rate of broadcast traffic on the VPLS network is limited.

Prerequisites

A VSI has been created using the **vsi** *vsi-name* [**auto** | **static**] command.

Precautions

The **broadcast-suppression cir cbs** command can be configured in a maximum of 100 VSIs.

Example

Set the CIR to 100 kbit/s and the CBS to 18800 bytes for the broadcast traffic that can pass in **VSI1**.

```
<HUAWEI> system-view
[HUAWEI] vsi VSI1
[HUAWEI-vsi-VSI1] broadcast-suppression cir 100 cbs 18800
```

10.7.3 bfd bind pw vsi

Function

The **bfd bind pw vsi** command configures a BFD session on a non-SPE node to detect a PW.

The **undo bfd** command deletes the specified BFD session.

By default, no BFD session is configured to detect the PW.

Format

bfd *cfg-name* **bind pw vsi** *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] [**remote-peer** *remote-peer-address* **pw-ttl** { **auto-calculate** | *ttl-number* }]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Specifies the destination IP address of the VPLS PW, which is usually the LSR ID.	The value is in dotted decimal notation.
vc-id *vc-id*	Specifies the ID of a Layer 2 VC.	The value is an integer ranging from 1 to 4294967295.
remote-peer *remote-peer-address*	Specifies the IP address used as the destination address of the PW to be detected by a BFD session, which is usually the LSR ID.	The value is in dotted decimal notation. It cannot be in the format of 127.X.X.X.
pw-ttl	Indicates the BFD session detects the PW in TTL mode.	-
auto-calculate	Indicates that the number of hops along a PW is counted automatically.	-
ttl-number	Specifies the number of hops along the PW to be detected.	The value is an integer ranging from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD sessions can rapidly detect links on the network. You can run the **bfd bind pw vsi** command to detect a single-hop VPLS PW or a multi-hop PW formed by connecting a VPLS PW to a VLL PW. The **bfd bind pw vsi** command detects the VPLS PW in unicast mode and specifies the VPLS PW to be detected through the parameter **peer** *peer-address*.

- If the configured BFD session is used to detect an end-to-end single-hop VPLS PW, the value of **peer** *peer-address* and the value of **remote-peer** *remote-peer-address* are identical. In this case, you can run the **bfd** *cfg-name* **bindpw vsi** *vsi-name* **peer** *peer-address* command only. The TTL value is 255.
- If the BFD session is used to detect a multi-hop PW formed by connecting a VPLS PW to a VLL PW, you need to specify the destination IP address of the VPLS PW through **peer** *peer-address* and the destination IP address of the multi-hop PW through **remote-peer** *remote-peer-address*.
  - If **auto-calculate** is specified, the system automatically counts the number of hops along the PW to be detected based on **remote-peer** *remote-peer-address*.
  - If **ttl** *ttl-number* is specified, the number of hops along the PW to be detected is manually set.

NOTE

When running the **bfd bind pw vsi** command to detect a multi-hop PW, ensure that the first-hop PW is the VPLS PW, which must be configured on a non-SPE node.

When running the **bfd bind pw vsi** command to detect a single-hop VPLS PW, ensure that the single-hop VPLS PW is configured on a non-SPE node.

If VPLS forwards data through TE tunnels, PW detection using a BFD session is not supported.

Prerequisites

The PW to be detected must exist. The BFD session must be established between the source and destination of the PW.

Before running the **bfd bind pw vsi** command, ensure that the following configuration operations have been performed:

- The BFD function has been enabled globally through the **bfd** command.
- A single-hop VPLS PW or multi-hop PW formed by connecting a VPLS PW to a VLL PW has been created.

Precautions

This command is used to configure a BFD session to detect a VPLS PW only in TTL mode.

Example

Configure a BFD session on a non-SPE node to detect the VPLS PW in TTL mode.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd vplspw bind pw vsi vsi1 peer 2.2.2.2 vc-id 123 remote-peer 3.3.3.3 pw-ttl auto-calculate
```

10.7.4 bfd for vsi-pw enable

Function

The **bfd for vsi-pw enable** command enables the device to send BFD for VSI-PW packets to the protocol stack.

The **undo bfd for vsi-pw enable** command disables the device from sending BFD for VSI-PW packets to the protocol stack.

By default, the device does not send BFD for VSI-PW packets to the protocol stack, but discards or forwards the packets.

Format

bfd for vsi-pw enable

undo bfd for vsi-pw enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When performing BFD for VSI PW, the device needs to send BFD for VSI-PW packets to the protocol stack. Therefore, the **bfd for vsi-pw enable** command must be run.

Precautions

If you run the **undo bfd for vsi-pw enable** command to disable the device from sending BFD for VSI-PW packets to the protocol stack, the BFD for VSI-PW packets are discarded or forwarded. The **bfd for vsi-pw enable** command and other BFD commands can be run in any sequence.

After the **bfd for vsi-pw enable** command is run in the system view, the BFD for VSI-PW packets are sent to the protocol stack. If this command is not run, the BFD for VSI PW packets are discarded or forwarded, and the BFD for VSI PW function does not take effect.

Example

Enable the device to send BFD for VSI-PW packets to the protocol stack.

```
<HUAWEI> system-view
[HUAWEI] bfd for vsi-pw enable
```

Disable the device from sending BFD for VSI-PW packets to the protocol stack.

```
<HUAWEI> system-view
[HUAWEI] undo bfd for vsi-pw enable
```

10.7.5 bgp-ad

Function

The **bgp-ad** command displays the BGP-AD view.

Format

bgp-ad

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

To establish the BGP-AD VSI, you need to run the **bgp-ad** command in the VSI view to display the BGP-AD view. In the BGP-AD view, you can configure parameters such as VPLS-ID and VPN-Target.

Example

Enter the BGP-AD view.

```
<HUAWEI> system-view
[HUAWEI] vsi v100
[HUAWEI-vsi-v100] bgp-ad
[HUAWEI-vsi-v100-bgpad]
```

10.7.6 description (VSI view)

Function

The **description** command configures the description of a Virtual Switch Instance (VSI).

The **undo description** command deletes the description of a VSI.

By default, no description of the VSI is configured.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VSI.	The value is a string of 1 to 64 case-sensitive characters with spaces.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

The **description** command can be used to identify different VSIs or describe the functions of VSIs.

Example

Configure the description of the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi v100
[HUAWEI-vsi-v100] description vsi for company1
```

10.7.7 display bgp l2vpn-ad routing-table

Function

The **display bgp l2vpn-ad routing-table** command displays BGP L2VPN-AD routes.

Format

display bgp l2vpn-ad [**route-distinguisher** *route-distinguisher*] **routing-table** [**vpls-ad**] [*ipv4-address* | **statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes** [**vpls-ad**] [*ipv4-address* | **statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes** [**active**] [**statistics**]

display bgp l2vpn-ad routing-table vpws route-distinguisher *route-distinguisher* [**ce-id** *ce-id* [**label-offset** *label-offset*]]

display bgp l2vpn-ad routing-table { **vpws** | **vpls** | **all** } [**statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes vpls-ad** *ipv4-address*

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpls-ad** [**active**] [**statistics**]

display bgp l2vpn-ad routing-table vpls route-distinguisher *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset*]]

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes** { **vpws** | **vpls** | **all** } [**statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes vpws** [**statistics** | **route-distinguisher** *route-distinguisher* **ce-id** *ce-id* **label-offset** *label-offset*]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes vpls** [**statistics** | **route-distinguisher** *route-distinguisher* **site-id** *site-id* **label-offset** *label-offset*]

display bgp l2vpn-ad routing-table peer *ipv4-address* **advertised-routes all** [**statistics**]

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpls-ad** *network*

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpws route-distinguisher** *route-distinguisher* **ce-id** *ce-id* **label-offset** *label-offset*

display bgp l2vpn-ad routing-table peer *ipv4-address* **received-routes vpls route-distinguisher** *route-distinguisher* **site-id** *site-id* **label-offset** *label-offset*

Parameters

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays BGP L2VPN-AD routing information of the specified RD.	-
ipv4-address	Specifies the IPv4 network address.	-
statistics	Display the statistics of the BGP L2VPN-AD routes.	-
peer	Displays the routing information for the specified BGP peer.	-
advertised-routes	Displays the routes advertised to the specified peer.	-
received-routes	Displays the routes received from the specified peer.	-
active	Displays the active routes received from the specified peer.	-

Parameter	Description	Value
network	Specifies the IPv4 network address.	-
vpls-ad	Displays VPLS-AD route information.	-
vpws	Displays VPWS route information.	-
vpls	Displays VPLS route information.	-
all	Displays information about all types of routes.	-
ce-id *ce-id*	Specifies the CE ID.	The value is a decimal integer ranging from 0 to 65535.
site-id *site-id*	Specifies the site ID of a VSI.	The value is a decimal integer ranging from 0 to 65535.
label-offset *label-offset*	Specifies the offset of a label.	The value is a decimal integer ranging from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

Example

Display all the BGP L2VPN-AD routing information.

```
<HUAWEI> display bgp l2vpn-ad routing-table


 Local AS number : 100
```

```
 BGP Local router ID is 10.1.150.122
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete



 Total number of routes from all PE: 2
 Route Distinguisher: 1:1


      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.9/32         0.0.0.0                              0      ?
 *>i  3.3.3.9/32         3.3.3.9                    100        0      ?
```

Display the detailed routing information of a specified route.

```
<HUAWEI> display bgp l2vpn-ad routing-table 3.3.3.9


 BGP local router ID : 10.1.150.122
 Local AS number : 100

 Total routes of Route Distinguisher(1:1): 1
 BGP routing table entry information of 3.3.3.9/32:
 From: 3.3.3.9 (192.2.2.2)
 Route Duration: 00h02m09s
 Relay IP Nexthop: 172.1.1.1
 Relay IP Out-Interface: Vlanif30
 Original nexthop: 3.3.3.9
 Qos information : 0x0
 Ext-Community:RT <100 : 1>, Layer2 Info <1 : 1>
 AS-path Nil, origin incomplete, localpref 100, pref-val 0, valid, internal, bes
t, select, pre 255, IGP cost 1
 Not advertised to any peer yet
```

Display VPLS route information.

```
<HUAWEI> display bgp l2vpn-ad routing-table vpls

 BGP Local router ID is 10.1.0.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale


 Total Number of Routes: 2
      Network(RD/Site-ID/LabelOffset)        NextHop

 *>i  100:1/1/0                              1.1.1.1
 *>   100:2/2/0                              0.0.0.0
```

Display information about VPLS routes received from 1.1.1.1.

```
<HUAWEI> display bgp l2vpn-ad routing-table peer 1.1.1.1 received-routes vpls

 BGP Local router ID is 10.1.0.3
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale


 Total Number of Routes: 1
      Network(RD/Site-ID/LabelOffset)        NextHop

 *>i  100:1/1/0                              1.1.1.1
```

Table 10-90 Description of the display bgp l2vpn-ad routing-table command output

Item	Description
Network	Network address in the BGP routing table
NextHop	Next Hop address through which the packet has to be sent
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Value preferred by the protocol
Path/Ogn	AS-Path number and the attributes of Origin
BGP Local router ID	ID of the local BGP device. The ID is in the same format as an IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher	Total number of L2VPN-AD routes with a specified RD.
BGP routing table entry information of x.x.x.x/x	The following information is about a specified BGP routing entry.
From	IP address of the route originator.
Route Duration	Route duration.
Relay IP Nexthop	Recursive next-hop IP address.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information. - 0x20000000: indicates that the **apply behavior** command has been run. - 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. - 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. - 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute of BGP.

Item	Description
AS-path	AS_Path attribute. **Nil** indicates that the attribute value is null.
origin	Origin attribute of the BGP route. ● IGP: The routes imported into the BGP routing table by using the **network** command. ● EGP: The routes are obtained by EGP. ● Incomplete: The origin of the routes cannot be determined, for example, the routes imported into the BGP routing table by using the **import-route** command.
localpref	Local preference of the BGP route.
pref-val	Preferred value.
valid	Valid BGP route.
internal	Internal BGP route.
best	The BGP route is the optimal route.
select	The BGP route is a preferred route.
pre 255	The preference of the BGP route is 255.
IGP cost 1	Indicates the IGP cost is 1.
Not advertised to any peer yet	The BGP route has not been advertised to any peer.

Display detailed information about the specified invalid VPLS-AD routes.

```
<HUAWEI> display bgp l2vpn-ad routing-table 1.1.1.1
 BGP local router ID : 10.1.1.2
 Local AS number : 100

 Total routes of Route Distinguisher(1:1): 1
 BGP routing table entry information of 1.1.1.1/32:
 From: 1.1.1.1 (10.1.1.1)
 Route Duration: 00h00m30s
 Relay IP Nexthop: 10.1.1.1
 Relay IP Out-Interface: GigabitEthernet0/0/0
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 Ext-Community:RT <100 : 1>, Layer2 Info <1 : 1>

 AS-path Nil, origin incomplete, localpref 100, pref-val 0, internal, select, pre 255, invalid for route-policy
not pass
 Not advertised to any peer yet
```

Table 10-91 Description of the display bgp l2vpn-ad routing-table command output

Item	Description
BGP local router ID	ID of the local BGP router. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher(1:1)	The total number of routes with the RD of 1:1.
BGP routing table entry information of 1.1.1.1/32	The following information is about 1.1.1.1/32 routing entries.
From	IP address of the router that sends the route. 10.1.1.1 is the IP address of the source interface of the peer with which the BGP connection is established, and 1.1.1.1 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	Recursive next hop.
Relay IP Out-Interface	Recursive outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information. ● 0x20000000: indicates that the **apply behavior** command has been run. ● 0x40000001–0x40000FFF: indicates that the **apply qos-local-id** *qos-local-id* command has been run and the *qos-local-id* varies from 1 to 4095. ● 0x80000001–0x80000007: indicates that the **apply ip-precedence** *precedence* command has been run and the *precedence* varies from 1 to 7. ● 0x0: indicates that the preceding QoS configurations are not performed.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.
invalid for route-policy not pass	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to recurse to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to recurse to a tunnel.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

10.7.8 display bgp vpls

Function

The **display bgp vpls** command displays information about VPLS in the BGP routing table.

Format

display bgp vpls { **all** | **route-distinguisher** *route-distinguisher* [**site-id** *site-id* [**label-offset** *label-offset*]] }

Parameters

Parameter	Description	Value
all	Displays all VPLS information in the BGP VPLS address family.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the VSI information about the specified Route Distinguisher (RD). The formats of an RD are as follows: - 16-bit AS number:32-bit user-defined number: for example, 101:3. An AS number ranges from 0 to 65535, and a user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. That is, a VPLS ID cannot be 0:0. - Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID cannot be 0:0. - 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID cannot be 0.0:0. - 32-bit IP address:16-bit user-defined number: for example, 192.168.122.15:1. An IPv4 address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number ranges from 0 to 65535.	-
site-id *site-id*	Displays the VSI of the specified site ID.	The value is an integer that ranges from 0 to 65534.
label-offset *label-offset*	Displays the VSI information about the specified label offset.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify the parameter values of the command to view required VPLS.

When the output information is excessive, you can run the **display bgp vpls peer** command to view information about the BGP peer in the VPLS, and run the **display bgp vpls group** command to view information about the BGP peer group in the VPLS.

Example

Display the VPLS with the VSI of the BGP RD as 1.1.1.2:1.

```
<HUAWEI> display bgp vpls route-distinguisher 1.1.1.2:1
BGP Local Router ID : 10.1.1.1, Local AS Number : 100
Status codes : * - active, > - best

-------------------------------------------------------------------------------
Route Distinguisher: 1.1.1.2:1
   SiteID Offset NextHop         Range LabBase TunnelID   FromPeer        MHPref
-------------------------------------------------------------------------------
>  1      0      0.0.0.0         3     35840   0x0        0.0.0.0         0
```

Table 10-92 Description of the display bgp vpls route-distinguisher command output

Item	Description
BGP Local Router ID	ID of the BGP local router. To set the value, run the **router-id** command.
Local AS Number	Local AS number. To set the value, run the **bgp** command.
Status codes	Route status. - *: active route - >: best route
Route Distinguisher	RD of the VPN instance. To set the value, run the **route-distinguisher** command.
SiteID	Site ID of the remote VSI. To set the value, run the **site** command.
Offset	Offset of the site ID. The value is 0 or 1 and the default value is 0. To set the value, run the **site** command.
Nexthop	IP address of the next hop.

Item	Description
Range	Range of the number of sites in the VSI. The value is a decimal integer. To set the value, run the **site** command.
LabBase	Start number of the allocated labels.
Tunnel ID	Tunnel ID, which is automatically allocated by the system and is in hexadecimal notation.
FromPeer	IP address of the BGP peer.
MHPref	Multi-homing preference. To set the value, run the **multi-homing-preference** command.

10.7.9 display l2vpn ccc-interface vc-type

Function

The **display l2vpn ccc-interface vc-type** command displays information about the interface used by an L2VPN connection.

Format

display l2vpn ccc-interface vc-type { **all** | *vc-type* } [**down** | **up**]

Parameters

Parameter	Description	Value
all	Displays information about all interfaces of L2VPN connections.	-
vc-type	Specifies the type of the L2VPN connection.	The following types of the L2VPN connection are available: • ccc: Cross Circuit Connection • ldp-vc: L2VPN connection in the Martini mode • static-vc: L2VPN connection in the SVC mode • bgp-vc: L2VPN connection in the Kompella mode • vpls-vc: VPLS connection

Parameter	Description	Value
down	Displays information about interfaces of L2VPN connection in the Down state.	-
up	Displays information about interfaces of L2VPN connection in the Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating L2VPN faults, you can use the **display l2vpn ccc-interface vc-type** command to view information about the AC interface of the current L2VPN connection, the total number of AC interfaces of various L2VPN connections, interface status, interface encapsulation type, and L2VPN connection types.

Example

Display information about all the interfaces of L2VPN.

```
<HUAWEI> display l2vpn ccc-interface vc-type all
Total ccc-interface of LDP VC: 1
up (1), down (0)
Interface                 Encap Type               State      VC Type
Vlanif12                  vlan                  up         ldp-vc
```

Table 10-93 Description of the **display l2vpn ccc-interface vc-type** command output

Item	Description
Total ccc-interface of CCC : 2 up (2), down (0)	Total number of L2VPN connections is 2. Two connections is Up. No connection is Down.
Interface	Interface connected to the L2VPN connection on the switch.
Encap Type	Encapsulation type of the L2VPN connection. The encapsulation type can be VLAN encapsulation or Ethernet encapsulation.
State	Current status of the L2VPN connection. The status can be Up or Down.

Item	Description
VC Type	Type of the L2VPN connection: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● bgp-vc: L2VPN connection in the Kompella mode ● vpls-vc: VPLS connection

10.7.10 display l2vpn vsi-list tunnel-policy

Function

The **display l2vpn vsi-list tunnel-policy** command displays the correlation between tunnel policies and VSIs.

Format

display l2vpn vsi-list tunnel-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a PW tunnel policy.	The value is an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display l2vpn vsi-list tunnel-policy** *policy-name* command, you can view the names of VSIs that create a PW using the specified tunnel policy.

Example

Display the name of the tunnel policy used by the VSI.

```
<HUAWEI> display l2vpn vsi-list tunnel-policy p1
Using Tunnel-Policy p1 VSI Instance statistics:
------------------------------------------------------------------------
  vsi v1
```

```
vsi v2
vsi v3
```

Table 10-94 Description of the display l2vpn vsi-list tunnel-policy command output

Item	Description
Using Tunnel-Policy p1 VSI Instance statistics	Names of all the PW VSIs established by the specified tunnel policy.
vsi	VSI name.

10.7.11 display loop-detect

Function

The **display loop-detect** command displays blocking information about L2VPN loop detection.

Format

display loop-detect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After L2VPN loop detection is enabled on an interface by running the **loop-detect enable** command, you can run the **display loop-detect** command to check blocking information about L2VPN loop detection. The information helps determine whether loops occur on an L2VPN network, facilitating fault location.

Example

Display blocking information about L2VPN loop detection on interfaces.

```
<HUAWEI> display loop-detect
-----------------------------------------------------------------
Interface                 RecoverTime  Action     Status
-----------------------------------------------------------------
GigabitEthernet0/0/1.1       20         block      NORMAL
GigabitEthernet0/0/2.1       20         block      NORMAL
-----------------------------------------------------------------
```

Table 10-95 Description of the **display loop-detect** command output

Item	Description
Interface	Interface with L2VPN loop detection enabled. To enable L2VPN loop detection on an interface, run the **loop-detect enable** command.
RecoverTime	Period for restoring an interface to normal state. To specify this period, run the **loop-detect recovery-time** command.
Action	Action after an L2VPN loop is detected: ● BLOCK: Block this interface.
Status	Status of an interface with L2VPN loop detection enabled: ● NORMAL: No loop is detected. ● BLOCK: A loop is detected, and the interface is blocked.

10.7.12 display mpls l2vpn resource

Function

The **display mpls l2vpn resource** command displays MPLS L2VPN specifications and usage information.

Format

display mpls l2vpn resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check MPLS L2VPN specifications and usage information in routine maintenance, run the **display mpls l2vpn resource** command.

Example

Display MPLS L2VPN specifications and usage information.

```
<HUAWEI> display mpls l2vpn resource

Public Capacity Statistics
 Statistics Item                 Supported Number      Used Number
 L2VPN AC Number                       2000                  2
 L2VPN VC Number                       8000                  2

 VPWS Capacity Statistics
 Statistics Item                 Supported Number      Used Number
 L2VPN Local CCC Number                 512                    0
 L2VPN Remote CCC Number                  1008                   0
 L2VPN SVC Number                      1008                  1
 L2VPN LDP VC Number                     2000                  0
 L2VPN BGP VC Number                     2000                  0
 L2VPN Switch VC Number                  2000                  0

 VPLS Capacity Statistics
 Statistics Item                 Supported Number      Used Number
 L2VPN VSI Number                      1024                  3
 L2VPN BGP VSI Number                    1024                  0
 L2VPN VSI VC Number                    8000                  1
 L2VPN VSI PWG Number                    1024                  0
```

Table 10-96 Description of the **display mpls l2vpn resource** command output

Item	Description
Public Capacity Statistics	MPLS L2VPN capacity statistics
Statistics Item	Statistics item
Supported Number	Maximum number allowed
Used Number	Number already used
L2VPN AC Number	Number of L2VPN AC interfaces, including the maximum number allowed and number already used
L2VPN VC Number	Number of L2VPN VCs, including the maximum number allowed and number already used
VPWS Capacity Statistics	VPWS capacity statistics
L2VPN Local CCC Number	Number of VLLs in local CCC mode, including the maximum number allowed and number already used
L2VPN Remote CCC Number	Number of VLLs in remote CCC mode, including the maximum number allowed and number already used
L2VPN SVC Number	Number of VLLs in SVC mode, including the maximum number allowed and number already used
L2VPN LDP VC Number	Number of LDP VLLs, including the maximum number allowed and number already used

Item	Description
L2VPN BGP VC Number	Number of BGP VLLs, including the maximum number allowed and number already used
L2VPN Switch VC Number	Number of Switch VC, including the maximum number allowed and number already used
VPLS Capacity Statistics	VPLS capacity statistics
L2VPN VSI Number	Number of VSIs, including the maximum number allowed and number already used
L2VPN BGP VSI Number	Number of BGP VSIs, including the maximum number allowed and number used
L2VPN VSI VC Number	Number of VSI VCs, including the maximum number allowed and number already used
L2VPN VSI PWG Number	Number of protection groups for a VSI, including the maximum number allowed and number already used

10.7.13 display mpls label-stack vpls vsi

Function

The **display mpls label-stack vpls vsi** command displays information about label stacks in a VPLS scenario.

Format

display mpls label-stack vpls vsi *vsi-name* **peer** *peer-ip-address* **vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-ip-address*	Specifies the IP address of a peer.	The value is in dotted decimal notation.
vc-id *vc-id*	Specifies the VPLS PW ID.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view PW traffic forwarding information in a Martini VPLS scenario, run the **display mpls label-stack vpls vsi** command.

Example

Display stack label information in a Martini VPLS scenario with the peer IP address **1.1.1.9** and PW ID **11**.

```
<HUAWEI> display mpls label-stack vpls vsi a1 peer 1.1.1.9 vc-id 11
Label-stack  : 1
Level        : 1
Type         : VPLS
Label        : 1028
Level        : 2
Type         : LDP
Label        : --
OutInterface : Vlanif1024
```

Table 10-97 Description of the **display mpls label-stack vpls vsi** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of label layers
Type	Tunnel type
Label	Outgoing label value
OutInterface	Outbound interface name

10.7.14 display oam-mac list

Function

The **display oam-mac list** command displays the MAC address list for the diagnostic test on the MAC address learning capacity.

Format

display oam-mac list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display oam-mac list** command displays MAC address lists of all the **mac populate** or **mac purge** operations that are available on the device.

NOTE

Before performing diagnostic test of the MAC address learning capacity, you need to apply for a MAC address specialized for the diagnostic test. In this case, the diagnostic test does not impact on the normal forwarding.

At present, only the following MAC addresses are used in the diagnostic test.

- 0018-82a4-3fb1
- 0018-82a4-3fb2
- 0018-82a4-3fb3
- 0018-82a4-3fb4
- 0018-82a4-3fb5
- 0018-82a4-3fb6
- 0018-82a4-3fb7
- 0018-82a4-3fb8
- 0018-82a4-3fb9
- 0018-82a4-3fba

Example

Display the MAC address list for the diagnostic test of the MAC address learning capacity.

```
<HUAWEI> display oam-mac list
No.  Mac Address
 1  0018-82a4-3fb1
 2  0018-82a4-3fb2
 3  0018-82a4-3fb3
 4  0018-82a4-3fb4
 5  0018-82a4-3fb5
 6  0018-82a4-3fb6
 7  0018-82a4-3fb7
 8  0018-82a4-3fb8
 9  0018-82a4-3fb9
10  0018-82a4-3fba
```

10.7.15 display oam-mac statistics

Function

The **display oam-mac statistics** command displays the statistics about the number of MAC diagnostic packets.

Format

display oam-mac statistics { **populate** | **purge** | **purge-register** | **all** }

Parameters

Parameter	Description	Value
populate	Displays the statistics about the number of populate packets.	-
purge	Displays the statistics about the number of purge packets.	-
purge-register	Displays the statistics about the number of purge register packets.	-
all	Displays the statistics about the number of MAC diagnostic packets of all types.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display oam-mac statistics** command, you can view the number of MAC diagnostic packets that is counted since the **reset oam-mac statistics** command was run.

Example

Display the statistics about the number of populate packets that are received by the device.

```
<HUAWEI> display oam-mac statistics populate
Received populate packet: 3
```

Display the statistics about the number of all MAC diagnostic packets that are received by the device.

```
<HUAWEI> display oam-mac statistics all
 Received populate packet: 3
 Received purge packet: 1
 Received purge register packet: 2
```

Table 10-98 Description of the display oam-mac statistics all command output

Item	Description
Received populate packet	Number of received populate packets.
Received purge packet	Number of received purge packets.
Received purge register packet	Number of received purge register packets.

10.7.16 display traffic-statistics vsi

Function

The **display traffic-statistics vsi** command displays the statistics about the public traffic on all VPLS PWs in a specified VSI.

Format

display traffic-statistics vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS network is configured, you can run the **display traffic-statistics vsi** command to view the statistics about the traffic on all VPLS PWs in a specified VSI.

Precautions

- Currently, this command only displays the statistics about the traffic on the Martini VPLS PWs in the VSI.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the traffic on all VPLS PWs in a specified VSI.

```
<HUAWEI> display traffic-statistics vsi newvsi
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-99 Description of the display traffic-statistics vsi command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.17 display traffic-statistics vsi peer

Function

The **display traffic-statistics vsi peer** command displays the statistics about the public traffic on a VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS network is configured, you can run the **display traffic-statistics vsi peer** command to view the statistics about the traffic on the PW.

Precautions

- Currently, this command only displays the statistics about the traffic on the Martini VPLS PWs in the VSI.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the outgoing traffic on the specified VPLS PW.

```
<HUAWEI> display traffic-statistics vsi newvsi peer 10.22.33.20
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-100 Description of the display traffic-statistics vsi peer command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.18 display traffic-statistics vsi peer ldp129

Function

The **display traffic-statistics vsi peer ldp129** command displays the statistics about the public traffic on a BGP-AD VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address* **ldp129**

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI. The specified VSI must be a VSI of the BGP-AD VPLS.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-
ldp129	Specifies the statistics about the public traffic in the BGP-AD VPLS that uses LDP 129 signaling.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the BGP-AD VPLS configuration is complete, you can run the **display traffic-statistics vsi peer ldp129** command to view the statistics about the traffic on the PW.

Prerequisites

The following operations have been performed before this command is used:

1. The BGP-AD VPLS has been configured.
2. The traffic statistics function has been enabled using the **traffic-statistics enable (VSI-BGPAD view)** command or the **traffic-statistics peer enable (VSI-BGPAD)** command in the VSI-BGPAD view.

Precautions

- The **display traffic-statistics vsi peer ldp129** command only displays the statistics about the traffic on the PW in the BGP-AD VPLS.

- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the public traffic on the specified PW in the BGP-AD VPLS.

```
<HUAWEI> display traffic-statistics vsi vplsad1 peer 10.22.33.20 ldp129
vsi-name: vplsad1
Peer-address: 10.22.33.20
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-101 Description of the display traffic-statistics vsi peer ldp129 command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the peer device.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.19 display traffic-statistics vsi peer negotiation-vc-id

Function

The **display traffic-statistics vsi peer negotiation-vc-id** command displays the statistics about the public traffic on the Martini VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address* **negotiation-vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-
vc-id	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **display traffic-statistics vsi peer negotiation-vc-id** command to view the statistics about the traffic on the PW.

Prerequisites

The following operations have been performed before this command is used:

1. The Martini VPLS has been configured.
2. The traffic statistics function has been enabled using the **traffic-statistics enable (VSI-LDP view)** command or the **traffic-statistics peer enable** command in the VSI-LDP view.

Precautions

- Currently, this command only displays the statistics about the traffic on the Martini VPLS PWs in the VSI.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the traffic on the specified Martini VPLS PW.

```
<HUAWEI> display traffic-statistics vsi newvsi peer 10.22.33.20 negotiation-vc-id 2
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
```

```
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-102 Description of the display traffic-statistics vsi peer negotiation-vc-id command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.20 display traffic-statistics vsi peer remote-site

Function

The **display traffic-statistics vsi peer remote-site** command displays the statistics about the public traffic on the Kompella VPLS PW in a specified VSI.

Format

display traffic-statistics vsi *vsi-name* **peer** *peer-address* **remote-site** *site-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a specified VSI.	The value is an existing VSI.
peer-address	Specifies the peer IP address of the PW.	-
site-id	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the Kompella VPLS network is configured, you can run the **display traffic-statistics vsi peer remote-site** command to view the statistics about the traffic on the PW.

Prerequisites

The following operations have been performed before this command is used:

1. The Kompella VPLS has been configured.
2. The traffic statistics function has been enabled using the **traffic-statistics peer remote-site enable (Kompella)** command in the VSI-BGP view.

Precautions

- The Kompella VPLS PW is uniquely identified by the user-defined VSI name, the next-hop IP address, and the remote site value.
- Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the traffic on the specified Kompella VPLS PW.

```
<HUAWEI> display traffic-statistics vsi newvsi peer 10.22.33.20 remote-site 2
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 10-103 Description of the display traffic-statistics vsi peer remote-site command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Remote-site-id	Remote Site ID.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.

Item	Description
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

10.7.21 display vpls connection

Function

The **display vpls connection** command displays the VPLS connection.

Format

display vpls connection [**ldp** | **bgp** | **bgp-ad** | **vsi** *vsi-name*] [**down** | **up**] [**verbose**]

Parameters

Parameter	Description	Value
ldp	Displays information about LDP signaling connections.	-
bgp	Displays information about BGP signaling connections.	-
bgp-ad	Displays information about BGP AD signaling connections.	-
vsi *vsi-name*	Displays information about connections of the specified VSI.	The value is an existing VSI.
down	Displays information about connections in Down state.	-
up	Displays information about connections in Up state.	-
verbose	Displays detailed information about connections.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After VPLS services are configured, you can run the **display vpls connection** command with different keywords or parameters to view information about specific VPLS connections.

Prerequisites

One of the following operations has been performed before the **display vpls connection** command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS
- Configuring BGP AD VPLS

Precautions

If no keyword or parameter is specified, information about all VPLS connections in Up state is displayed.

Example

Display information about the connections of all VSIs.

```
<HUAWEI> display vpls connection

2 total connections,
connections: 2 up, 0 down, 1 ldp, 1 bgp, 0 bgpad

VSI Name: a2                          Signaling: ldp
VsiID      EncapType              PeerAddr         InLabel   OutLabel  VCState
2          vlan                  3.3.3.9          1026      1025      up
VSI Name: bgp1                          Signaling: bgp
SiteID     RD                    PeerAddr         InLabel   OutLabel  VCState
2          168.1.1.2:1            3.3.3.9          35842     35841     up
```

Table 10-104 Description of the display vpls connection command output

Item	Description
VSI Name	Name of the VSI. To set the value, run the **vsi** command.
Signaling	Signaling mode: ldp, bgp, bgpad or ldp bgpad. To set the value, run the **pwsignal** or **bgp-ad** command.
VsiID	VSI ID. To set the value, run the **vsi-id** command.

Item	Description
EncapType	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC. To set the value, run the **encapsulation** command.
PeerAddr	IP addresses of the peer.
InLabel	VC label distributed locally.
OutLabel	Local outgoing label, namely, the VC label distributed by the peer.
VCState	Status of the VC.
SiteID	Site ID of the remote VSI. To set the value, run the **site** command.
RD	RD used for identifying a VSI on the PE in the VPLS using BGP signaling. To set the value, run the **route-distinguisher** command.

Display the detailed information about all VSI connections.

```
<HUAWEI> display vpls connection verbose
VSI Name: a2                              Signaling: ldp
  **Remote Vsi ID   : 2
    VC State        : up
    Encapsulation   : vlan
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 3.3.3.9
    PW Type         : label
    Local VC Label  : 1026
    Remote VC Label : 1025
    Tunnel Policy   : --
    Tunnel ID       : 0x1
VSI Name: bgp1                             Signaling: bgp
  **Remote Site ID     : 2
    VC State           : up
    RD                 : 168.1.1.2:1
    Encapsulation      : vlan
    MTU                : 1500
    Peer Ip Address    : 3.3.3.9
    PW Type            : label
    Local VC Label     : 35842
    Remote VC Label    : 35841
    Tunnel Policy      : --
    Tunnel ID          : 0x1
    Remote Label Block : 35840/5/0
    Export vpn target  : 100:1
```

Table 10-105 Description of the display vpls connection verbose command output

Item	Description
VSI Name	Name of the VSI. To set the value, run the **vsi** command.
Signaling	Signaling mode: ldp, bgp, bgpad or ldp bgpad.
Remote Vsi ID	Remote VSI ID that is consistent with the local VSI ID.
VC State	Status of the VC, which can be Up or Down.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC. The encapsulation type is VLAN or Ethernet. To set the value, run the **encapsulation** command.
Group ID	Group identifier.
MTU	Maximum transmission unit. To set the value, run the **mtu** command.
Peer Ip Address	IP addresses of the peer.
PW Type	Type of the PW.
Local VC Label	Local VC label.
Remote VC Label	Remote VC label.
Tunnel Policy	Tunnel policy that is used by the L2VPN.
Tunnel ID	Tunnel ID.
Remote Label Block	Remote label block.
Export vpn target	Outbound extended community attribute to the target VPN.

Display the detailed information about connections of a VSI named **bgp1**

```
<HUAWEI> display vpls connection vsi bgp1 verbose
VSI Name: bgp1                            Signaling: bgp
  **Remote Site ID     : 2
    VC State           : up
    RD                 : 168.1.1.2:1
    Encapsulation      : vlan
    MTU                : 1500
    Peer Ip Address    : 3.3.3.9
    PW Type            : label
    Local VC Label     : 35842
    Remote VC Label    : 35841
    Tunnel Policy      : --
    Tunnel ID          : 0x1
    Remote Label Block : 35840/5/0
    Export vpn target  : 100:1
```

Table 10-106 Description of the display vpls connection vsi vsi-name verbose command output

Item	Description
VSI Name	Name of the VSI.
Signaling	Signaling mode: ldp, bgp, bgpad or ldp bgpad.
Remote Site ID	the Site ID of remote peer.
VC State	Status of the VC.
RD	Local router distinguisher.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC.
MTU	Maximum transmission unit.
Peer Ip Address	IP addresses of the peer.
PW Type	Type of the PW.
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.
Tunnel Policy	Tunnel policy.
Tunnel ID	Tunnel ID.
Remote Label Block	Remote label block.
Export vpn target	Outbound extended community attribute to the target VPN.

Display information about BGP AD VPLS connections with peers.

```
<HUAWEI> display vpls connection bgp-ad

1 total bgpad connections ,
connections: 1 up, 0 down

VSI Name: vplsad1                     Signaling: bgpad
VPLS ID             EncapType      PeerAddr        InLabel   OutLabel  VCState
168.1.1.1:1         vlan           3.3.3.9         1027      1026      up
```

Table 10-107 Description of the display vpls connection bgp-ad command output

Item	Description
VSI Name	Name of the VSI.

Item	Description
Signaling	VPLS signaling mode: - ldp - bgp - bgpad - ldp bgpad
VPLS ID	Identifier of a BGP AD VPLS domain.
EncapType	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: - VLAN - Ethernet
PeerAddr	IP addresses of the peer.
InLabel	VC label distributed locally.
OutLabel	Local outgoing label, namely, the VC label distributed by the peer.
VCState	Status of the VC. - up - down

Display detailed information about BGP AD connections of the VSIs that are in Up state.

```
<HUAWEI> display vpls connection bgp-ad up verbose
VSI Name: vplsad1                         Signaling: bgpad
  **VPLS ID          : 168.1.1.1:1
    VC State         : up
    Encapsulation    : vlan
    Group ID         : 0
    MTU              : 1500
    Peer Ip Address : 3.3.3.9
    PW Type          : label
    Local VC Label  : 1027
    Remote VC Label : 1026
    Tunnel Policy   : --
```

Table 10-108 Description of the display vpls connection bgp-ad up verbose command output

Item	Description
VSI Name	Name of the VSI.

Item	Description
Signaling	VPLS signaling mode: - ldp - bgp - bgpad - ldp bgpad
VPLS ID	Identifier of a BGP AD VPLS domain.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: - VLAN - Ethernet
Group ID	Group identifier
MTU	Maximum transmission unit.
Peer Ip Address	IP addresses of the peer.
Local VC Label	VC label distributed locally.
Remote VC Label	Local outgoing label, namely, the VC label distributed by the peer.
Tunnel Policy	Name of a tunnel policy used by the VPLS.

10.7.22 display vpls forwarding-info

Function

The **display vpls forwarding-info** command displays forwarding information of all VSIs.

Format

display vpls forwarding-info [**vsi** *vsi-name* [**peer** *peer-address* [**negotiation-vc-id** *vc-id* | **remote-site** *site-id*]] | **state** { **up** | **down** }] [**verbose**]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Displays forwarding information of a specified VSI.	The value is an existing VSI.

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.
state	Displays the forwarding information about VSIs based on the PW status.	-
up	Displays the forwarding information about the VSIs whose PWs are in Up state.	-
down	Displays the forwarding information about the VSIs whose PWs are in Down state.	-
verbose	Displays detailed forwarding information of the VSI.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS is configured, you can run the **display vpls forwarding-info** command to view the forwarding information of all VSIs.

Prerequisites

One of the following operations has been performed before the **display vpls forwarding-info** command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS
- Configuring BGP AD VPLS

Precautions

- The **display vpls forwarding-info vsi** *vsi-name* command is used to display forwarding information of a specified VSI (in Martini mode or Kompella mode).
- The **display vpls forwarding-info vsi** *vsi-name* **peer** *peer-address* [**negotiation-vc-id** *vc-id*] command is used to display forwarding information of a specified PW in the Martini VSI.
- The **display vpls forwarding-info vsi** *vsi-name* **peer** *peer-address* **remote-site** *site-id* command is used to display forwarding information about a specified PW in the Kompella VSI.

Example

Display brief forwarding information of all PWs in all VSIs.

```
<HUAWEI> display vpls forwarding-info
Total Number   : 2,        2  up,  0  down

Vsi-Name                       PeerIP          VcOrSiteId  PwState
a2                           3.3.3.9         2           UP
vplsad1                        3.3.3.9         0           UP
```

Display brief information about the VSI PWs in Up state.

```
<HUAWEI> display vpls forwarding-info state up
Total Number   : 2,        2  up,  0  down

Vsi-Name                       PeerIP          VcOrSiteId  PwState
a2                           3.3.3.9         2           UP
vplsad1                        3.3.3.9         0           UP
```

Table 10-109 Description of the display vpls forwarding-info command output

Item	Description
Total Number	The number of VSI.
Vsi-Name	Name of the VSI.
PeerIP	Peer IP address of the PW in the VSI.
VcOrSiteId	● VSI ID for the Martini VSI. ● Site ID for the Kompella VSI.
PwState	PW status: ● Up ● Down

Display detailed forwarding information of all PWs in all VSIs.

```
<HUAWEI> display vpls forwarding-info verbose
Total Number   : 2,        2  up,  0  down

**Vsi-Name      : a2
  Vsi Index     : 0                          PwState      : UP
  Peer IP       : 3.3.3.9                    VcOrSiteId   : 2
  InVcLabel     : 1026                         OutVcLabel   : 1025
  BroadTunnelID : 0x1                            OutInterface : Vlanif1025
```

```
  MainPwToken   : 0x1                         SlavePwToken : 0x0
  NKey          : 0x9                    CKey          : 0xa

**Vsi-Name      : vplsad1
  Vsi Index     : 2                      PwState       : UP
  Peer IP       : 3.3.3.9                 VcOrSiteId   : 0
  InVcLabel     : 1036                      OutVcLabel   : 1031
  BroadTunnelID : 0x1                         OutInterface : Vlanif1025
  MainPwToken   : 0x1                         SlavePwToken : 0x0
  NKey          : 0x9                    CKey          : 0x1b
```

Display the detailed forwarding information about the VSI PWs in Up state.

```
<HUAWEI> display vpls forwarding-info state up verbose
Total Number   : 2,        2  up,  0  down

**Vsi-Name      : a2
  Vsi Index     : 0                      PwState       : UP
  Peer IP       : 3.3.3.9                 VcOrSiteId   : 2
  InVcLabel     : 1026                      OutVcLabel   : 1025
  BroadTunnelID : 0x1                         OutInterface : Vlanif1025
  MainPwToken   : 0x1                         SlavePwToken : 0x0
  NKey          : 0x9                    CKey          : 0xa

**Vsi-Name      : vplsad1
  Vsi Index     : 2                      PwState       : UP
  Peer IP       : 3.3.3.9                 VcOrSiteId   : 0
  InVcLabel     : 1036                      OutVcLabel   : 1031
  BroadTunnelID : 0x1                         OutInterface : Vlanif1025
  MainPwToken   : 0x1                         SlavePwToken : 0x0
  NKey          : 0x9                    CKey          : 0x1b
```

Table 10-110 Description of the display vpls forwarding-info verbose command output

Item	Description
Total Number	The number of VSI.
Vsi-Name	Name of the VSI.
Vsi Index	VSI index.
PwState	PW status: ● Up ● Down
Peer IP	Peer IP address of the PW in the VSI.
VcOrSiteId	● VSI ID for the Martini VSI. ● Site ID for the Kompella VSI.
InVcLabel	Incoming label of the VC.
OutVcLabel	Outgoing label of the VC.
BroadTunnelID	ID of the tunnel used for broadcast.
OutInterface	Outbound interface.
MainPwToken	Token of the master PW.
SlavePwToken	Token of the slave PW.

Item	Description
NKey	Network key. Each NKey corresponds to one peer + tunnel policy.
CKey	User key. Each CKey corresponds to a PW.

10.7.23 display vpls multicast-ping statistics

Function

The **display vpls multicast-ping statistics** command displays the statistics on the number of sent and received MFIB Ping packets.

Format

display vpls multicast-ping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls multicast-ping statistics** command, you can view the statistics on the number of MFIB Ping packets that are received and sent by the device since the last time the **reset vpls multicast-ping statistics** command was run.

Example

Display the statistics on the number of MFIB Ping packets.

```
<HUAWEI> display vpls multicast-ping statistics
Total sent: 5 packet(s)
Total received: 5 packet(s)
Vpls Mfib-ping echo request sent: 5 packet(s), received: 0 packet(s)
Vpls Mfib-ping echo reply sent: 0 packet(s), received: 5 packet(s)
```

Table 10-111 Description of the display vpls multicast-ping statistics command output

Item	Description
Total sent	Total number of sent packets.
Total received	Total number of received packets.
Vpls Mfib-ping echo request	Number of sent and received VPLS MFIB Ping Echo Request packets.
Vpls Mfib-ping echo reply	Number of sent and received VPLS MFIB Ping Echo Reply packets.

10.7.24 display vpls multicast-trace statistics

Function

The **display vpls multicast-trace statistics** command displays the statistics on the number of sent and received MFIB Trace packets.

Format

display vpls multicast-trace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vpls multicast-trace statistics** command to view the number of sent and received MFIB Trace packets since the last time the **reset vpls multicast-trace statistics** command is executed.

Example

Display the statistics on the number of MFIB Trace packets.

```
<HUAWEI> display vpls multicast-trace statistics
Total sent: 2 packet(s)
Total received: 2 packet(s)
Vpls Mfib-trace echo request sent: 2 packet(s), received: 0 packet(s)
Vpls Mfib-trace echo reply sent: 0 packet(s), received: 2 packet(s)
```

Table 10-112 Description of the display vpls multicast-trace statistics command output

Item	Description
Total sent	Total number of sent packets.
Total received	Total number of received packets.
Vpls Mfib-trace echo request	Number of sent and received VPLS MFIB Trace Echo Request packets.
Vpls Mfib-trace echo reply	Number of sent and received VPLS MFIB Trace Echo Reply packets.

10.7.25 display vpls-ping statistics

Function

The **display vpls-ping statistics** command displays the statistics on the number of sent and received VPLS MAC Ping packets.

Format

display vpls-ping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls-ping statistics** command, you can view the statistics on the number of sent and received VPLS MAC Ping packets on the device.

Example

Display the statistics on the number of VPLS MAC Ping packets.

```
<HUAWEI> display vpls-ping statistics
Vpls-ping statistics:
Total sent: 104797 packet (s)
Total received: 104792 packet (s)
vpls-ping request sent: 13 packet (s), received: 104784 packet (s)
vpls-ping reply sent: 104784 packet (s), received: 8 packet (s)
```

Table 10-113 Description of the display vpls-ping statistics command output

Item	Description
Total sent	Total number of sent VPLS MAC Ping packets.
Total received	Total number of received VPLS MAC Ping packets.
vpls-ping request sent	Number of sent VPLS Ping Request packets.
vpls-ping reply sent	Number of sent VPLS Ping Reply packets.

10.7.26 display vpls-trace statistics

Function

The **display vpls-trace statistics** command displays the statistics on the number of sent and received VPLS MAC Trace packets.

Format

display vpls-trace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls-trace statistics** command, you can view the statistics on the number of sent and received VPLS MAC Trace packets on the device.

Example

Display the statistics on the number of VPLS MAC Trace packets.

```
<HUAWEI> display vpls-trace statistics
Vpls-trace statistics:
Total sent : 4 packet (s)
Total received : 4 packet (s)
vpls-trace request sent: 4 packet (s), received: 0 packet (s)
vpls-trace reply sent: 0 packet (s), received: 4 packet (s)
```

Table 10-114 Description of the display vpls-trace statistics command output

Item	Description
Total sent	Total number of sent VPLS MAC Trace packets.
Total received	Total number of received VPLS MAC Trace packets.
vpls-trace request sent	Number of sent VPLS MAC Trace Request packets.
vpls-trace reply sent	Number of sent VPLS MAC Trace Reply packets.

10.7.27 display vsi

Function

The **display vsi** command displays information about a VSI.

Format

display vsi [**name** *vsi-name*] [**verbose**]

display vsi [**name** *vsi-name*] **peer-info** [**statistics**]

display vsi name *vsi-name* **peer-info** *peer-ip* [**verbose**]

Parameters

Parameter	Description	Value
name *vsi-name*	Displays the name of a specified VSI.	The value is an existing VSI.
verbose	Displays detailed information about the VSI.	-
peer-info	Displays detailed information or statistics about the PW status of peers.	-
statistics	Displays statistics about the PW status of peers.	-
peer-ip	Displays detailed information about the PW status of the peer with a specified IP address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display vsi** command:

- The **display vsi** command displays information about VSIs. By default, information of all VSIs is displayed.
- The **display vsi peer-info** command displays detailed information about the PW status of peers of all VSIs.
- The **display vsi name** *vsi-name* **peer-info** command displays detailed information about the PW status of peers to a specified VSI.
- The **display vsi name** *vsi-name* **peer-info** *peer-ip* command displays detailed information about the PW status of a specific peer to a specified VSI.
- The **display vsi peer-info statistics** command displays statistics about the PW status of peers of all VSIs.
- The **display vsi name** *vsi-name* **peer-info statistics** command displays statistics about the PW status of a specific peer to a specified VSI.

Example

Display information about the VSI named **a2**.

```
<HUAWEI> display vsi name a2
Vsi                   Mem    PW   Mac       Encap     Mtu   Vsi
Name                  Disc   Type Learn     Type      Value State
--------------------------------------------------------------------------
a2                    static ldp  unqualify vlan      1500  up
```

Display information about the hybrid VSI named **vsi1**.

```
<HUAWEI> display vsi name vsi1
Vsi                   Mem    PW    Mac       Encap     Mtu   Vsi
Name                  Disc   Type  Learn     Type      Value State
--------------------------------------------------------------------------
vsi1                  --     mixed unqualify vlan      1500  up
```

Table 10-115 Description of the **display vsi** command output

Item	Description
Vsi Name	Name of the VSI. To set the value, run the **vsi** command.
Mem Disc	Member discovery mode: ● static ● auto ● --

Item	Description
PW Type	PW type: - ldp - bgp - bgpad - mixed
Mac Learn	Mode of learning the MAC address.
Encap Type	Encapsulation type. - vlan - ethernet If the encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
Mtu Value	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU values on one end to be the same as that on the other end.
Vsi State	Status of the VSI: - up - down - *down

Display detailed information about all VSIs.

```
<HUAWEI> display vsi verbose

 ***VSI Name               : a2
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 0
    PW Signaling           : ldp
    Member Discovery Style : static
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 0 days, 3 hours, 6 minutes, 43 seconds
    VSI State              : up

    VSI ID                 : 2
   *Peer Router ID         : 10.3.3.9
    Negotiation-vc-id      : 2
    primary or secondary   : primary
```

```
   ignore-standby-state   : no
   VC Label               : 1026
   Peer Type              : dynamic
   Session                : up
   Tunnel ID              : 0x1
   Broadcast Tunnel ID    : 0x1
   Broad BackupTunnel ID  : 0x0
   CKey                   : 10
   NKey                   : 9
   Stp Enable             : 0
   PwIndex                : 0
   Control Word           : disable
   BFD for PW             : unavailable

   Interface Name         : Vlanif1024
   State                  : up
   Access Port            : false
   Last Up Time           : 2012/07/06 14:00:15
   Total Up Time          : 0 days, 3 hours, 6 minutes, 20 seconds

 **PW Information:

  *Peer Ip Address        : 10.3.3.9
   PW State               : up
   Local VC Label         : 1026
   Remote VC Label        : 1025
   Remote Control Word    : disable
   PW Type                : label
   Local  VCCV            : alert lsp-ping bfd
   Remote VCCV            : alert lsp-ping bfd
   Tunnel ID              : 0x1
   Broadcast Tunnel ID    : 0x1
   Broad BackupTunnel ID  : 0x0
   Ckey                   : 0xa
   Nkey                   : 0x9
   Main PW Token          : 0x1
   Slave PW Token         : 0x0
   Tnl Type               : LSP
   OutInterface           : Vlanif1025
   Backup OutInterface    :
   Stp Enable             : 0
   PW Last Up Time        : 2012/07/06 14:01:07
   PW Total Up Time       : 0 days, 3 hours, 5 minutes, 28 seconds

***VSI Name               : bgp1
   Administrator VSI      : no
   Isolate Spoken         : disable
   VSI Index              : 6
   PW Signaling           : bgp
   Member Discovery Style : auto
   PW MAC Learn Style     : unqualify
   Encapsulation Type     : vlan
   MTU                    : 1500
   Diffserv Mode          : uniform
   Mpls Exp               : --
   DomainId               : 255
   Domain Name            :
   Ignore AcState         : disable
   P2P VSI                : disable
   Create Time            : 2 days, 20 hours, 19 minutes, 16 seconds
   VSI State              : up

   BGP RD                 : 172.16.1.1:1
   SiteID/Range/Offset    : 1/5/0
   Import vpn target      : 100:1
   Export vpn target      : 100:1
   Remote Label Block     : 35840/5/0
   Local Label Block      : 0/35840/5/0
```

```
   Interface Name         : Vlanif1022
   State                 : up
   Access Port           : false
   Last Up Time          : 2012/08/06 03:24:45
   Total Up Time         : 0 days, 0 hours, 10 minutes, 11 seconds

 **PW Information:

  *Peer Ip Address       : 10.3.3.9
   PW State              : up
   Local VC Label        : 35843
   Remote VC Label       : 35841
   PW Type               : label
   Local  VCCV           : alert lsp-ping bfd
   Remote VCCV           : alert lsp-ping bfd
   Tunnel ID             : 0x2e4d
   Broadcast Tunnel ID   : 0x2e4d
   Broad BackupTunnel ID  : 0x0
   Ckey                  : 0x17
   Nkey                  : 0x15
   Main PW Token         : 0x2e4d
   Slave PW Token        : 0x0
   Tnl Type              : LSP
   OutInterface          : Vlanif1025
   Backup OutInterface   :
   Stp Enable            : 0
   PW Last Up Time       : 2012/08/06 03:25:12
   PW Total Up Time      : 0 days, 0 hours, 9 minutes, 44 seconds

***VSI Name              : vplsad1
   Administrator VSI     : no
   Isolate Spoken        : disable
   VSI Index             : 2
   PW Signaling          : bgpad
   Member Discovery Style : --
   PW MAC Learn Style    : unqualify
   Encapsulation Type    : vlan
   MTU                   : 1500
   Diffserv Mode         : uniform
   Mpls Exp              : --
   DomainId              : 255
   Domain Name           :
   Ignore AcState        : disable
   P2P VSI               : disable
   Create Time           : 0 days, 1 hours, 28 minutes, 24 seconds
   VSI State             : up

   VPLS ID               : 172.16.1.1:1
   RD                    : 172.16.1.1:1
   Import vpn target     : 100:1
   Export vpn target     : 100:1
   VSI ID                : 1.1.1.9

  *Peer Router ID        : 10.3.3.9
   VPLS ID               : 172.16.1.1:1
   SAII                  : 1.1.1.9
   TAII                  : 10.3.3.9
   VC Label              : 1027
   Peer Type             : dynamic
   Session               : up
   Tunnel ID             : 0x1
   Broadcast Tunnel ID   : 0x1
   CKey                  : 12
   NKey                  : 9

   Interface Name        : Vlanif1023
   State                 : up
   Access Port           : false
   Last Up Time          : 2012/07/06 15:38:40
```

```
  Total Up Time          : 0 days, 1 hours, 27 minutes, 56 seconds

**PW Information:

 *Peer Ip Address        : 10.3.3.9
  PW State               : up
  Local VC Label         : 1027
  Remote VC Label        : 1026
  PW Type                : label
  Local  VCCV            : alert lsp-ping bfd
  Remote VCCV            : alert lsp-ping bfd
  Tunnel ID              : 0x1
  Broadcast Tunnel ID    : 0x1
  Broad BackupTunnel ID  : 0x0
  Ckey                   : 0xc
  Nkey                   : 0x9
  Main PW Token          : 0x1
  Slave PW Token         : 0x0
  Tnl Type               : LSP
  OutInterface           : Vlanif1025
  Backup OutInterface    :
  Stp Enable             : 0
  PW Last Up Time        : 2012/07/06 15:38:56
  PW Total Up Time       : 0 days, 1 hours, 27 minutes, 40 seconds
```

Table 10-116 Description of the **display vsi verbose** command output

Item	Description
VSI Name	Name of the VSI.
Administrator VSI	Whether the VSI is an administrator VSI: ● yes ● no
Isolate Spoken	Whether the forwarding isolation function is enabled: ● enable ● disable
VSI Index	Index of the VSI.
PW Signaling	Type of the PW signaling, which can be ldp, bgp, bgpad or ldp bgpad. To set the value, run the **pwsignal** or **bgp-ad** command.
Member Discovery Style	Member discovery mode, which can be auto or static.
PW MAC Learn Style	Mode of MAC address learning of the PW.

Item	Description
Encapsulation Type	VPLS encapsulation type of the VSI: - VLAN - Ethernet If the PW encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
MTU	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU values on one end to be the same as that on the other end.
Diffserv Mode	VSI QoS mode.
Mpls Exp	EXP priority in MPLS packets.
DomainId	ID of a domain.
Domain Name	Domain name.
Ignore AcState	Whether the **vpls ignore-ac-state** command is used to prevent the status of a VSI from being affected by the status of the Attachment Circuit (AC).
P2P VSI	A P2P VSI identifier, which can be: - enable: indicates that the VSI is a P2P VSI. - disable: indicates that the VSI is not a P2P VSI.
Create Time	Time when the VSI is created.
VSI State	Status of the VSI: - up - down - administratively down
BGP RD	Route distinguisher. The BGP RD is an identifier on the local device for identifying a VSI on the PE in BGP VPLS. This item is displayed only when the VPLS type is Kompella.
SiteID/Range/Offset	Site ID, site range (the number of sites), and initial site ID offset of the VSI on the local device. This item is displayed only when the VPLS type is Kompella.
Import vpn target	Inbound extended community attribute from the target VPN. This item is displayed only when the VPLS type is Kompella.

Item	Description
Export vpn target	Outbound extended community attribute to the target VPN. This item is displayed only when the VPLS type is Kompella.
Remote Label Block	Initial value, label range, and initial site ID offset of the remote label block. This item is displayed only when the VPLS type is Kompella.
Local Label Block	Initial value, label range, and initial site ID offset of the local label block. This item is displayed only when the VPLS type is Kompella.
VSI ID	VSI ID that is displayed only when the Martini VPLS is configured. If the VSI IDs or negotiation IDs on both ends are different, run the **vsi-id** *vsi-id* or **peer (VSI-LDP view)** command in the VSI-LDP view to change the VSI ID or negotiation ID on one end to be the same as that on the other end.
Peer Router ID	ID of the peer device. This item is displayed only when the VPLS type is Martini.
Negotiation-vc-id	VC ID for negotiation.
primary or secondary	Whether the PW is a primary PW or a secondary PW.
ignore-standby-state	Whether the PW ignores the secondary state sent from the peer device. yes: Ignore the secondary state sent from the peer device. no: Do not ignore the secondary state sent from the peer device.
VC Label	Label value of the VC. This item is displayed only when the VPLS type is Martini.
Peer Type	PW type of the peer, which can be Dynamic or Static. This item is displayed only when the VPLS type is Martini.
Session	Status of the session between the local end and its peer. The status can be Up or Down. This item is displayed only when the VPLS type is Martini.
Tunnel ID	Tunnel ID that is displayed only when the Martini VPLS is configured.
Broadcast Tunnel ID	Tunnel ID (for broadcast).
Broad BackupTunnel ID	ID of the selected backup broadcast tunnel.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.

Item	Description
Stp Enable	Whether STP for PW is enabled: - 0: disabled - 1: enable
PwIndex	PW index.
Control Word	Whether the control word is enabled for the local end on the PW: - enable: The control word is enabled. - disable: The control word is disabled.
BFD for PW	Whether BFD is configured: - unavailable: not configured - available: configured - timeout: timeout period after which a BFD session fails to be established
Interface Name	Name of the interface bound to the VSI.
Access Port	Whether the interface supports the access-port attribute: - true: indicates that the interface supports the access-port attribute. - false: indicates that the interface does not support the access-port attribute.
State	Status of the AC bound to the VSI. - up - down
Last Up Time	Last time when the AC interface goes Up.
Total Up Time	Total time when the AC interface is Up.
PW Information	Information about the PW.
Peer Ip Address	IP addresses of the peer.
PW State	Status of the PW. - up - down - backup
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.

Item	Description
Remote Control Word	Whether the control word is enabled for the remote end on the PW: ● enable: The control word is enabled. ● disable: The control word is disabled.
PW Type	Type of the PW.
Local VCCV	Type of VCCV supported on the local device.
Remote VCCV	Type of VCCV supported on the remote device.
Tunnel ID	Tunnel ID.
Main PW Token	Token of the master PW.
Slave PW Token	Token of the slave PW.
Tnl Type	Type of a tunnel. ● LSP ● CR-LSP ● GRE ● Other
OutInterface	Outbound interface.
Backup OutInterface	Outbound interface of the selected backup broadcast tunnel.
PW Last Up Time	Last time when the PW goes Up.
PW Total Up Time	Total time when the PW is Up.

Display detailed information about the BGP VSI named **bgp1**.

```
<HUAWEI> display vsi name bgp1 verbose

 ***VSI Name               : bgp1
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 6
    PW Signaling           : bgp
    Member Discovery Style : auto
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 2 days, 20 hours, 19 minutes, 16 seconds
    VSI State              : up

    BGP RD                 : 172.16.1.1:1
    SiteID/Range/Offset    : 1/5/0
```

```
  Import vpn target      : 100:1
  Export vpn target      : 100:1
  Remote Label Block     : 35840/5/0
  Local Label Block      : 0/35840/5/0

  Interface Name         : Vlanif1022
  State                  : up
  Access Port            : false
  Last Up Time           : 2012/08/06 03:24:45
  Total Up Time          : 0 days, 0 hours, 10 minutes, 11 seconds

**PW Information:

 *Peer Ip Address        : 10.3.3.9
  PW State               : up
  Local VC Label         : 35843
  Remote VC Label        : 35841
  PW Type                : label
  Local  VCCV            : alert lsp-ping bfd
  Remote VCCV            : alert lsp-ping bfd
  Tunnel ID              : 0x2e4d
  Broadcast Tunnel ID    : 0x2e4d
  Broad BackupTunnel ID  : 0x0
  Ckey                   : 0x17
  Nkey                   : 0x15
  Main PW Token          : 0x2e4d
  Slave PW Token         : 0x0
  Tnl Type               : LSP
  OutInterface           : Vlanif20
  Backup OutInterface    :
  Stp Enable             : 0
  PW Last Up Time        : 2012/08/06 03:25:12
  PW Total Up Time       : 0 days, 0 hours, 9 minutes, 44 seconds
```

Table 10-117 Description of the **display vsi name bgp1 verbose** command output

Item	Description
VSI Name	Name of the VSI.
Administrator VSI	Whether the VSI is an administrator VSI: ● yes: It is an administrator VSI. ● no: It is not an administrator VSI.
Isolate Spoken	Whether the forwarding isolation function is enabled: ● enable ● disable
VSI Index	Index of the VSI.
PW Signaling	Type of the PW signaling, which can be ldp, bgp, bgpad or ldp bgpad.
Member Discovery Style	Member discovery mode, which can be auto or static.
PW MAC Learn Style	Mode of MAC address learning of the PW.

Item	Description
Encapsulation Type	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: ● VLAN ● Ethernet If the PW encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
MTU	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU values on one end to be the same as that on the other end.
Diffserv Mode	VSI QoS mode.
Mpls Exp	EXP priority in MPLS packets.
DomainId	ID of a domain.
Domain Name	Domain name.
Ignore AcState	Whether the **vpls ignore-ac-state** command is used to prevent the status of a VSI from being affected by the status of the AC.
Create Time	Time when the VSI is created.
VSI State	Status of the VSI: ● up ● down ● administratively down
BGP RD	Route distinguisher. The BGP RD is an identifier on the local device for identifying a VSI on the PE in BGP VPLS. This item is displayed only when the VPLS type is Kompella.
SiteID/Range/Offset	Site ID, site range (the number of sites), and initial site ID offset of the VSI on the local device. This item is displayed only when the VPLS type is Kompella.
Import vpn target	Inbound extended community attribute from the target VPN.
Export vpn target	Outbound extended community attribute to the target VPN.

Item	Description
Local Label Block	Initial value, label range, and initial site ID offset of the local label block.

Display information about the BGP AD VSI named **vplsad1**.

```
<HUAWEI> display vsi name vplsad1
Vsi                          Mem    PW   Mac        Encap      Mtu   Vsi
Name                           Disc   Type Learn     Type      Value State
--------------------------------------------------------------------------
vplsad1                        --     bgpad   unqualify vlan      1500  up
```

Display detailed information about the BGP AD VSI.

```
<HUAWEI> display vsi name vplsad1 verbose

 ***VSI Name               : vplsad1
    Administrator VSI      : no
    Isolate Spoken         : disable
    VSI Index              : 2
    PW Signaling           : bgpad
    Member Discovery Style : --
    PW MAC Learn Style     : unqualify
    Encapsulation Type     : vlan
    MTU                    : 1500
    Diffserv Mode          : uniform
    Mpls Exp               : --
    DomainId               : 255
    Domain Name            :
    Ignore AcState         : disable
    P2P VSI                : disable
    Create Time            : 0 days, 1 hours, 59 minutes, 39 seconds
    VSI State              : up

    VPLS ID                : 172.16.1.1:1
    RD                     : 172.16.1.1:1
    Import vpn target      : 100:1
    Export vpn target      : 100:1
    VSI ID                 : 1.1.1.9

   *Peer Router ID         : 10.3.3.9
    VPLS ID                : 172.16.1.1:1
    SAII                   : 1.1.1.9
    TAII                   : 10.3.3.9
    VC Label               : 1027
    Peer Type              : dynamic
    Session                : up
    Tunnel ID              : 0x1
    Broadcast Tunnel ID    : 0x1
    CKey                   : 12
    NKey                   : 9

    Interface Name         : Vlanif1023
    State                  : up
    Access Port            : false
    Last Up Time           : 2012/07/06 15:38:40
    Total Up Time          : 0 days, 1 hours, 59 minutes, 11 seconds

  **PW Information:

   *Peer Ip Address        : 10.3.3.9
    PW State               : up
    Local VC Label         : 1027
    Remote VC Label        : 1026
    PW Type                : label
```

```
  Local  VCCV            : alert lsp-ping bfd
  Remote VCCV            : alert lsp-ping bfd
  Tunnel ID              : 0x1
  Broadcast Tunnel ID    : 0x1
  Broad BackupTunnel ID  : 0x0
  Ckey                   : 0xc
  Nkey                   : 0x9
  Main PW Token          : 0x1
  Slave PW Token         : 0x0
  Tnl Type               : LSP
  OutInterface           : Vlanif1025
  Backup OutInterface    :
  Stp Enable             : 0
  PW Last Up Time        : 2012/07/06 15:38:56
  PW Total Up Time       : 0 days, 1 hours, 58 minutes, 55 seconds
```

Table 10-118 Description of the **display vsi name vplsad1 verbose** command output

Item	Description
PW Signaling	Type of the PW signaling, which can be ldp, bgp, bgpad or ldp bgpad.
Member Discovery Style	Member discovery mode: ● auto: indicates automatic member discovery. When creating a VSI on a Kompella VPLS network, configure **auto** in the **vsi** command. ● static: indicates static member discovery. When creating a VSI on a Martini VPLS network, configure **static** in the **vsi** command. ● --: When creating a VSI on a BGP AD VPLS network, do not configure the member discovery mode in the **vsi** command.
VPLS ID	Identifier for identifying a BGP AD VSI on various PEs.
RD	Route Distinguisher, which is the same as the VPLS ID in the BGP AD VSI.
SAII	Source Attachment Individual Identifier, which is a local IP address used during negotiation on the creation of a PW in the BGP AD VSI.
TAII	Target Attachment Individual Identifier, which is a remote IP address used during negotiation on the creation of a PW in the BGP AD VSI.

Display detailed information of PW status of peers to all VSIs.

```
<HUAWEI> display vsi peer-info

VSI Name: a2                                   Signaling: ldp
-------------------------------------------------------------------
Peer              Transport  Local      Remote      VC
Addr              VC ID/TAII  VC Label   VC Label    State
-------------------------------------------------------------------
10.3.3.9            2         1026       1025        up
```

Display detailed information of PW status of a specific peer to a specified VSI.

```
<HUAWEI> display vsi name a2 peer-info 10.3.3.9

VSI Name: a2                              Signaling: ldp
-----------------------------------------------------------------
Peer              Transport  Local      Remote      VC
Addr              VC ID/TAII  VC Label   VC Label    State
-----------------------------------------------------------------
10.3.3.9            2          1026       1025        up
```

Table 10-119 Description of the **display vsi peer-info** command output

Item	Description
Vsi Name	Name of the VSI.
Signaling	Signaling mode, which can be ldp, bgp, bgpad or ldp bgpad.
Peer Addr	IP addresses of the peer.
Transport VC ID/TAII	● VC ID for an LDP PW ● TAII for a BGP-AD PW
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.
VC State	Status of the PW. ● up ● down

Display statistics about PW status of peers to all VSIs.

```
<HUAWEI> display vsi peer-info statistics
Total Local Peers: 1          1 Up         0 Down
-------------------------------------------------------
Vsi Name                     Up Peers      Down Peers
-------------------------------------------------------
a2                          1             0
```

Display statistics about PW status of peers to a specified VSI.

```
<HUAWEI> display vsi name a2 peer-info statistics
Vsi Name                     Up Peers      Down Peers
-------------------------------------------------------
a2                          1             0
```

Table 10-120 Description of the **display vsi peer-info statistics** command output

Item	Description
Total Local Peers	Total number of remote peers to the local end, that is, total number of PWs.
Up	Total number of PWs in Up state.
Down	Total number of PWs in Down state.

Item	Description
Vsi Name	Name of the VSI.
Up Peers	Total number of PWs in Up state in a specified VSI.
Down Peers	Total number of PWs in Down state in a specified VSI.

10.7.28 display vsi bgp-ad

Function

The **display vsi bgp-ad** command displays the VPN targets of the local and remote devices in a BGP AD VPLS domain.

Format

display vsi bgp-ad { **export-vt** | **import-vt** | **remote-export-vt** }

Parameters

Parameter	Description	Value
export-vt	Displays local export VPN targets, namely, the export VPN targets of all local BGP AD VSIs.	-
import-vt	Displays local import VPN targets, namely, the import VPN targets of all local BGP AD VSIs.	-
remote-export-vt	Displays remote export VPN targets, namely, VPN targets received from BGP AD peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When you configure or debug BGP AD VPLS, you can run the **display vsi bgp-ad** command to check the correctness of VPN targets that are locally configured or sent from peers.

Prerequisites

BGP AD VPLS member information has been configured on the local or remote end.

Precautions

When you run the **display vsi bgp-ad** command:

- To view import VPN targets that are configured locally, specify **import-vt** in the command.
- To view export VPN targets that are configured locally, specify **export-vt** in the command.
- To view export VPN targets that are sent from peers, specify **remote-export-vt** in the command.

Example

Display local import VPN targets in a BGP AD VPLS domain.

```
<HUAWEI> display vsi bgp-ad import-vt
import vpn target list:
  100:1                 192.168.12.4:100       312:250
  192.168.120.220:53364  100:100               5.5.5.5:13
  312:250
```

Display local export VPN targets in a BGP AD VPLS domain.

```
<HUAWEI> display vsi bgp-ad export-vt
export vpn target list:
  100:1                 192.168.12.4:100       312:250
  192.168.120.220:53364  100:100               5.5.5.5:13
  312:250
```

Display remote export VPN targets in a BGP AD VPLS domain.

```
<HUAWEI> display vsi bgp-ad remote-export-vt
remote export vpn target list:
  100:1                 192.168.12.4:100       312:250
  192.168.120.220:53364  100:100               5.5.5.5:13
  312:250
```

Table 10-121 Description of the display vsi command output

Item	Description
import vpn target list	List of import VPN targets configured locally.
export vpn target list	List of export VPN targets configured locally.
remote export vpn target list	List of export VPN targets sent from remote BGP AD PEs.

10.7.29 display vsi bgp-ad remote

Function

The **display vsi bgp-ad remote** command displays information about a specified remote peer of a PE in a BGP AD VPLS domain.

Format

display vsi bgp-ad remote vpls-id *vpls-id*

Parameters

Parameter	Description	Value
vpls-id *vpls-id*	Specifies the VPLS ID of a remote peer.	A VPLS ID is in one of the following formats: • 16-bit AS number: a 32-bit user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. • 32-bit IP address: a 16-bit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. • Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. • 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you configure or debug BGP AD VPLS, the **display vsi bgp-ad remote** command can be used to display information about a remote peer in a BGP AD VSI such as the VPLS ID, VSI ID, and ERT configured on that peer.

Example

Display information about a BGP AD peer with the VPLS ID of 10.1.1.1:1.

```
<HUAWEI> display vsi bgp-ad remote vpls-id 10.1.1.1:1
BGP AD Network Layer Reachability Information
----------------------------------------------
 *Peer            :3.3.3.9
  VPLS ID          :10.1.1.1:1
  VSI ID          :3.3.3.9
  VSI index        :2
  Export vpn target:100:1
----------------------------------------------
```

Table 10-122 Description of the display vsi bgp-ad remote command output

Item	Description
Peer	Peer IP address.
VPLS ID	VPLS ID configured on the remote peer. To set the value, run the **vpls-id** command.
VSI ID	VSI ID configured on the remote peer. To set the value, run the **vsi-id** command.
VSI index	Local VSI index matching BGP AD network layer reachability information sent by the remote peer.
Export vpn target	List of export VPN targets sent from the remote peer.

10.7.30 display vsi mac-withdraw loop-detect

Function

The **display vsi mac-withdraw loop-detect** command displays information about MAC withdraw loop detection.

Format

display vsi [**name** *vsi-name*] **mac-withdraw loop-detect**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you enable MAC withdraw loop detection, run the **display vsi mac-withdraw loop-detect** command to view information about MAC withdraw loop detection. If you specify **name** *vsi-name*, the command output shows information about MAC withdraw loop detection in a specified VSI. If you do not specify **name** *vsi-name*, the command output shows information about MAC withdraw loop detection in all VSIs.

Example

Display information about MAC withdraw loop detection in all VSIs.

```
<HUAWEI> display vsi mac-withdraw loop-detect
Total number of vsi detect loop is 2.
Support max hop 255.

Vsi name        : VSI1
Last loop type  : detect loop
Send peer       : 10.5.5.5
Receive peer    : 10.2.2.2
Last loop time  : 2012/10/26 11:35:59

Vsi name        : VSI2
Last loop type  : exceed max hop
Send peer       : 10.5.5.5
Receive peer    : 10.3.3.3
Last loop time  : 2012/10/26 11:35:59
```

Display information about MAC withdraw loop detection in VSI1.

```
<HUAWEI> display vsi name VSI1 mac-withdraw loop-detect
Vsi name        : VSI1
Last loop type  : detect loop
Send peer       : 10.5.5.5
Receive peer    : 10.2.2.2
Last loop time  : 2012/10/26 11:35:59
```

Table 10-123 Description of the **display vsi mac-withdraw loop-detect** command output

Item	Description
Total number of vsi detect loop	Number of MAC Withdraw message loops.
Support max hop 255	Indicates that the maximum number of hops supported by MAC Withdraw loop detection is 255.
Vsi name	Name of the VSI in which a MAC Withdraw message loop occurred.

Item	Description
Last loop type	Type of the MAC Withdraw message loop. The values are as follows: ● **detect loop**: The PE detects that a MAC Withdraw message loop occurs. ● **exceed max hop**: The number of hops for forwarding MAC Withdraw messages exceeds the maximum number of hops.
Send peer	Peer to which MAC Withdraw messages are sent.
Receive peer	Peer from which MAC Withdraw messages are received.
Last loop time	Time when the MAC Withdraw message loop occurs.

10.7.31 display vsi protect-group

Function

The **display vsi protect-group** command displays information about the PW protection group of a specified VSI.

Format

display vsi name *vsi-name* **protect-group** [*group-name* [**verbose** | **history**]]

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the VSI name.	The value is an existing VSI name.
group-name	Specifies the name of a PW protection group.	The value is an existing PW protection group.
verbose	Displays detailed information.	-
history	Displays historical switchover information about PWs in a PW protection group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a PW protection group is configured, you can run the **display vsi protect-group** command to view summary or detailed information about the PW protection group of a specified VSI and check whether PW configurations have taken effect. When maintaining a PW protection group, you can track the running status of the group by viewing historical switchover information about PWs in the group.

Prerequisites

A PW protection group has been created and the primary and secondary PWs have jointed the group.

Example

Display summary information about the PW protection group of VSI vsi1.

```
<HUAWEI> display vsi name vsi1 protect-group

Vsi name: vsi1
Protect group num: 1

Protect-group: vsi1
-------------------------------------------------------------------------------
PeerIp:VcId              Pref   Active
-------------------------------------------------------------------------------
3.3.3.3:10               2      Active
3.3.3.9:10               4      Inactive
```

Table 10-124 Description of the **display vsi protect-group** command output

Item	Description
Vsi name	VSI name.
Protect group num	Number of a PW protection group.
Protect-group	Name of a PW protection group.
PeerIp:VcId	Peer IP address of a PW:VC ID. This pair uniquely identifies a PW.
Pref	PW priority specified by running the **peer preference** command in the protect-group view.

Item	Description
Active	Forwarding status of a PW: ● Active: The PW can send service packets. ● Inactive: The PW cannot send service packets, but can send OAM packets if the PW is Up.

Display detailed information about the PW protection group group1 of VSI vsi1.

```
<HUAWEI> display vsi name vsi1 protect-group group1 verbose

Vsi name           : vsi1
Protect group      : group1
Protect mode       : PW redundancy master
Reroute policy     : delay 30s
Last change time   : 2012/11/27 11:11:55
Last change action : 3.3.3.9:10 to 3.3.3.3:10
Last change reason : config changed
Holdoff remain time: --
Reroute remain time: --

Members            :
 PeerIp:VcId                Pri/Sec   Active

 3.3.3.3:10                 Primary   Active
 3.3.3.9:10                 Secondary Inactive
```

Table 10-125 Description of the **display vsi protect-group** command output

Item	Description
Protect mode	PW redundancy mode of a PW protection group: PW redundancy master: The PW redundancy mode is master/slave.
Reroute policy	Revertive switching policy of a PW protection group. The default revertive switching delay is 30s. In master/ slave mode, you can modify the revertive switching policy by running the **reroute** command in the protect-group view.
Last change time	Last PW switching time.
Last change action	Last PW switching action. A PW is uniquely identified by peerIP:VcID.

Item	Description
Last change reason	Reason for last PW switching: ● manual force switch: The PW switching is triggered by the **protect-switch force** command. ● manual clear switch: The PW switching is triggered by the **protect-switch clear** command. ● config changed: The PW switching is triggered by configuration changes such as PW addition, PW deletion, or PW priority changes. ● fault detected: The PW switching is triggered by failures detected by BFD or VCCV. ● PW down: The PW switching occurs because the active PW goes Down. ● PW up: The PW switching occurs because the active PW goes Up again.
Holdoff remain time	Remaining time before a switching is performed. **NOTE** If the value is **--**, no switching delay is configured.
Reroute remain time	Remaining time before a revertive switching is performed. **NOTE** If the value is **--**, no revertive switching delay is configured.
Members	Displays members in a PW protection group.
Pri/Sec	Primary/secondary status of a PW: ● Primary: The PW is a primary PW. ● Secondary: The PW is a secondary PW.

Display historical switchover information about PWs in PW protection group group1 of VSI vsi1.

```
<HUAWEI> display vsi name vsi1 protect-group group1 history

Vsi name      : vsi1
Protect group : group1

Date/Time     : 2012/11/27 11:05:40
Action        : 3.3.3.9:10 to 3.3.3.3:10
Reason        : manual clear switch

Date/Time     : 2012/11/27 11:06:29
Action        : 3.3.3.3:10 to 3.3.3.9:10
Reason        : manual force switch

Date/Time     : 2012/11/27 11:06:48
Action        : 3.3.3.9:10 to 3.3.3.3:10
Reason        : PW down

Date/Time     : 2012/11/27 11:11:31
Action        : 3.3.3.3:10 to 3.3.3.9:10
Reason        : PW up
```

```
Date/Time     : 2012/11/27 11:11:55
Action        : 3.3.3.9:10 to 3.3.3.3:10
Reason        : config changed
```

Table 10-126 Description of the **display vsi protect-group history** command output

Item	Description
Date/Time	PW switching time. For example, 2011-08-09 16:31:32 indicates that PW switching occurred on 16:31:32 of August 9, 2011.
Action	PW switching action. A PW is uniquely identified by peerIP:VcID.
Reason	Reason for PW switching: ● manual force switch: The PW switching is triggered by the **protect-switch force** command. ● manual clear switch: The PW switching is triggered by the **protect-switch clear** command. ● config changed: The PW switching is triggered by configuration changes such as PW addition, PW deletion, or PW priority changes. ● fault detected: The PW switching is triggered by failures detected by BFD or VCCV. ● PW down: The PW switching occurs because the active PW goes Down. ● PW up: The PW switching occurs because the active PW goes Up again.

10.7.32 display vsi pw out-interface

Function

The **display vsi pw out-interface** command displays information about the outgoing interface of a VSI PW.

Format

display vsi pw out-interface [**vsi** *vsi-name*]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display vsi pw out-interface** command to view information about the actual outgoing interface of the PW.

Precautions

This command applies to the Martini VPLS PW and BGP-AD VPLS PW.

Example

Display information about the outgoing interface of the VSI PW.

```
<HUAWEI> display vsi pw out-interface
Total: 2
--------------------------------------------------------------------------------
Vsi Name                        peer           vcid       interface
--------------------------------------------------------------------------------
a2                          3.3.3.9         2         Vlanif1025

vplsad1                       3.3.3.9         --         Vlanif1025
```

Table 10-127 Description of the display vsi pw out-interface command output

Item	Description
Vsi Name	VSI name.
peer	VSI peer.
vcid	VC ID.
interface	Outgoing interface of a VSI PW.

10.7.33 display vsi remote

Function

The **display vsi remote** command displays information about a remote VSI.

Format

display vsi remote ldp [**router-id** *ip-address*] [**pw-id** *pw-id*]

display vsi remote bgp [**nexthop** *nexthop-address* [**export-vpn-target** *vpn-target*] | **route-distinguisher** *route-distinguisher*]

display vsi remote ldp129 [**vpls-id** *vpls-id* [**router-id** *ip-address*]]

display vsi remote fec129 [**vpls-id** *vpls-id* [**router-id** *ip-address*]] [**verbose**]

display vsi remote ldp verbose

Parameters

Parameter	Description	Value
ldp	Displays information about remote VSIs using LDP signaling.	-
bgp	Displays information about remote VSIs using BGP signaling.	-
ldp129	Displays information about remote VSIs using LDP 129 signaling.	-
fec129	Displays information about remote VSIs using FEC 129 signaling.	-
vpls-id *vpls-id*	Specifies the ID of a VPLS domain to which multiple VSIs on PEs belong.	The *vpls-id* value has four formats. For details, see **Table 10-128**.
router-id *ip-address*	Displays the information about the remote VSIs of the specified peer. *ip-address* specifies an IPv4 address of the peer.	The value is in dotted decimal notation. If you set the **router id** parameter to 255.255.255.255, the remote VSIs of all peers are displayed.
pw-id *pw-id*	Displays the information about the remote VSIs of the specified PW. *pw-id* specifies the ID of a VC, which uniquely identifies a VC.	The value is an integer that ranges from 1 to 4294967295.
nexthop *nexthop-address*	Displays the label block sent by the remote end according to the next hop address of the label block.	The value is in dotted decimal notation.

Parameter	Description	Value
export-vpn-target *vpn-target*	Displays the label block sent by the remote end according to the next hop address of the label block and the route attributes in the outgoing direction.	The value is a string that ranges from 3 to 21.
route-distinguisher *route-distinguisher*	Displays the label block sent by the remote end according to the RD.	RD is short for route distinguisher. The *route-distinguisher* value has four formats. For details, see **Table 10-128**.
verbose	Display detailed information about the remote VSIs.	-

Table 10-128 Values of *vpls-id* and *route-distinguisher*

vpls-id and *route-distinguisher* Value Format	Value	Example
16-bit AS number:32-bit user-defined number	An AS number ranges from 0 to 65535, and a user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. That is, a VPLS ID or RD cannot be 0:0.	101:3
Integral 4-byte AS number:2-byte user-defined number	An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID or RD cannot be 0:0.	65537:3
4-byte AS number in dotted notation:2-byte user-defined number. A 4-byte AS number in dotted notation is in the format of *x.y*	The *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID or RD cannot be 0.0:0.	0.0:3 or 0.1:0
32-bit IP address:16-bit user-defined number	An IPv4 address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number ranges from 0 to 65535.	192.168.122.15:1

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about remote VSIs, configure one of the following parameters in the **display vsi remote** command:

- Run the **display vsi remote ldp** command on a Martini VPLS network.
- Run the **display vsi remote bgp** command on a Kompella VPLS network.
- Run the **display vsi remote ldp129** or **display vsi remote fec129** command on a BGP AD VPLS network.

Example

Display information about the remote VSIs using LDP signaling.

```
<HUAWEI> display vsi remote ldp
Vsi       Peer          VC      Group   Encap      MTU    Vsi    State
ID        RouterID        Label   ID      Type       Value  Index  Code
2         10.3.3.9       1025     0       vlan       1500   0      FORWARD
```

Table 10-129 Description of the display vsi remote ldp command output

Item	Description
Vsi ID	ID of the VSI.
Peer RouterID	Peer IP address.
VC Label	VC label.
Group ID	Group ID.
Encap Type	PW encapsulation type: ● vlan ● ethernet
MTU Value	MTU value.
Vsi Index	Index of the VSI.

Item	Description
State Code	Remote state code: - FORWARD: indicates that forwarding is supported. - NO FORWARD: indicates that forwarding is not supported. - STANDBY: indicates the secondary PW. - AC FAULT: indicates that the peer AC interface is faulty. - PSN FAULT: indicates that a fault occurs on the public network between the local end and peer end. - -: indicates that the interworking mode negotiated between two devices is Martini.

Display information about the remote VSIs using BGP signaling.

```
<HUAWEI> display vsi remote bgp
   Total Number       : 1
 **BGP RD             : 10.1.1.2:1
   Ref Number         : 1
   NextHop            : 10.3.3.9
   EncapType          : vlan
   MTU                : 1500
   Export vpn target  : 100:1
   SiteID             : 2
   Remote Label Block : 100001/5/0
```

Table 10-130 Description of the display vsi remote bgp command output

Item	Description
Total Number	Number of the remote VSIs using BGP signaling.
BGP RD	RD of the local VSI.
Ref Number	Serial number of the remote VSI.
NextHop	Next hop address.
EncapType	Encapsulation type: - vlan - ethernet
MTU	Maximum transmission unit.
Export vpn target	RT in the outgoing direction.
SiteID	Site ID of the remote VSI.
Remote Label Block	Remote label block.

Display information about the remote VSIs using LDP 129 signaling.

```
<HUAWEI> display vsi remote fec129
Codes: C(Control word), A(Alert), T(TTL), P(LSP-Ping), B(BFD)
      S(Support), N(No support)
--------------------------------------------------------------------------------
VPLS        Peer      VC        Source    Encap          MTU   VSI   VCCV
ID          RouterID  Label     AII       Type           Value Index |C|A|T|P|B|
--------------------------------------------------------------------------------
10.1.1.1:1  10.3.3.9  1026      10.3.3.9  vlan           1500  2     |N|S|N|S|N|
```

Table 10-131 Description of the display vsi remotefec129 command output

Item	Description
VPLS ID	VPLS ID of the VSI.
VCCV	Supported VCCV detection types.

Display detailed information about remote VSIs using LDP signaling.

```
<HUAWEI> display vsi remote ldp verbose
Total remote VSI : 1

VSI ID            : 2
VSI Index         : 0
VC Type           : vlan
VC Label          : 1025
Peer Address      : 10.3.3.9
Group ID          : 0
MTU               : 1500
Status Code       : FORWARD
Match Local VC    : MATCH
Control Word      : disable
```

Table 10-132 Description of the display vsi remote ldp verbose command output

Item	Description
Total remote VSI	Total number of remote VSIs.
VSI ID	ID of a remote VSI.
VSI Index	Index of a remote VSI.
VC Type	Remote VC encapsulation type.
VC Label	Remote VC label.
Peer Address	Remote peer address.
Group ID	Remote group ID. The default value is 0.
MTU	MTU of a remote VC.

Item	Description
Status Code	Status of a remote VC: ● FORWARD: The remote VC is in the forwarding state. ● STANDBY: The remote VC is in the standby state. ● AC FAULT: The remote AC interface is faulty. ● PSN FAULT: The remote VC is faulty. ● NO FORWARD: The remote VC cannot forward packets owing to other reasons.
Match Local VC	Whether a VC matching the remote VC ID exists on the local end: ● MATCH: A VC matching the remote VC ID exists on the local end. ● NOT-MATCH: No VC matching the remote VC ID exists on the local end.
Control Word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.

10.7.34 display vsi services

Function

The **display vsi services** command displays information about the AC interface associated with the VSI.

Format

display vsi services { **all** | *vsi-name* | **interface** *interface-type interface-number* | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays the information about AC interfaces associated with all VSIs.	-
vsi-name	Displays the information about AC interfaces associated with the specified VSI.	The value is an existing VSI.

Parameter	Description	Value
interface *interface-type* *interface-number*	Specifies the type and number of the AC interface associated with the VSI. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
vlan *vlan-id*	Displays information about the specified VLAN AC interface associated with the VSI.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vsi services** command displays status of the AC interface associated with the VSI, and can be used for fault diagnosis.

Example

Display information about the AC interfaces associated with all VSIs.

```
<HUAWEI> display vsi services all
Total: 2
Code: AS(Admin Status), PS(Physical Status)
------------------------------------------------------------------------------
Interface                      Vsi Name                      AS    PS
------------------------------------------------------------------------------
GigabitEthernet0/0/1               1                            up    up
Vlanif1024                      a2                         up    up
------------------------------------------------------------------------------
```

Display information about the AC interface associated with the VSI named **a2**.

```
<HUAWEI> display vsi services a2
Total: 1
Code: AS(Admin Status), PS(Physical Status)
------------------------------------------------------------------------------
Interface                      Vsi Name                      AS    PS
------------------------------------------------------------------------------
Vlanif1024                      a2                         up    up
------------------------------------------------------------------------------
```

Display information about the GE0/0/1 interface associated with the VSI.

```
<HUAWEI> display vsi services interface gigabitethernet0/0/1
Total: 1
Code: AS(Admin Status), PS(Physical Status)
------------------------------------------------------------------------------
Interface                      Vsi Name                      AS    PS
------------------------------------------------------------------------------
```

```
GigabitEthernet0/0/1              1                          down  up
-------------------------------------------------------------------------------
```

Display information about the AC interface in VLAN 1024 associated with the VSI.

```
<HUAWEI> display vsi services vlan 1024
Total: 1
Code: AS(Admin Status), PS(Physical Status)
-------------------------------------------------------------------------------
Interface                       Vsi Name                   AS    PS
-------------------------------------------------------------------------------
Vlanif1024                       a2                        up    up
-------------------------------------------------------------------------------
```

Table 10-133 Description of the display vsi services command output

Item	Description
Interface	Name of the interface.
Vsi Name	Name of the VSI that is bound to the interface.
AS	Status of the VSI that is bound to the interface: ● up: indicates that the VSI is in Up state. ● down: indicates that the VSI is in Down state. ● *down: indicates that the VSI status is AdminDown.
PS	Physical status of the interface: ● up: indicates that the physical status of the interface is Up. ● down: indicates that the physical status of the interface is Down.

10.7.35 display vsi statistics

Function

The **display vsi statistics** command displays VSI statistics, including the PW and AC status.

Format

display vsi name *vsi-name* **statistics**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the statistics of a specified VSI, including its PW and AC status, run the **display vsi statistics** command.

Example

Display the statistics of a VSI named **vsi1**.

```
<HUAWEI> display vsi name vsi1 statistics

 VSI Name               : vsi1
 VSI State              : up
 PW                     : 1 up, 0 down, 1 backup
 BFD for PW             : 0 up, 0 down
 AC                     : 1 up, 0 down, 0 AC OAM down
 Ignore AcState         : disable
```

Table 10-134 Description of the **display vsi statistics** command output

Item	Description
VSI Name	VSI name
VSI State	VSI status
PW	Number of PWs in each state
BFD for PW	Number of PWs (tracked by BFD) in each state
AC	Number of ACs in each state
Ignore AcState	Whether the function to ignore AC status is enabled

10.7.36 encapsulation (VSI view)

Function

The **encapsulation** command configures the encapsulation type of the interface in the VSI view.

The **undo encapsulation** command restores the encapsulation type of the interface to the default setting.

By default, the encapsulation type is VLAN.

Format

encapsulation { **ethernet** | **vlan** }

undo encapsulation ethernet

Parameters

Parameter	Description	Value
ethernet	Indicates that the encapsulation type is Ethernet.	-
vlan	Indicates the VLAN encapsulation format that meets the 802.1Q standard.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure the VPLS function, run the **encapsulation** command to configure the encapsulation type of the interface.

Prerequisites

The following operations must have been performed before this command is used:

- The **pwsignal bgp** command and the **route-distinguisher** *route-distinguisher* command have been executed for Kompella VPLS.
- The **pwsignal ldp** command and the **vsi-id** *vsi-id* command have been executed for Martini VPLS.
- The **bgp-ad** command and the **vpls-id** *vpls-id* command have been executed for BGP AD VPLS.

Example

Configure the encapsulation type of the current VSI as Ethernet.

```
<HUAWEI> system-view
[HUAWEI] vsi a2 static
[HUAWEI-vsi-a2] pwsignal ldp
[HUAWEI-vsi-a2-ldp] vsi-id 101
[HUAWEI-vsi-a2-ldp] quit
[HUAWEI-vsi-a2] encapsulation ethernet
```

10.7.37 encapsulation rfc4761-compatible

Function

The **encapsulation rfc4761-compatible** command enables a device to comply with RFC 4761 to encapsulate Kompella VPLS packets.

The **undo encapsulation rfc4761-compatible** command restores the default encapsulation type of Kompella VPLS packets.

By default, Kompella VPLS packets use the Huawei proprietary encapsulation type. Huawei defines 4 for VLAN encapsulation and 5 for Ethernet encapsulation for Kompella VPLS.

Format

encapsulation rfc4761-compatible

undo encapsulation rfc4761-compatible

Parameters

None

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RFC 4761 defines that the encapsulation type of Kompella VPLS packets is 19. Huawei defines 4 for VLAN encapsulation and 5 for Ethernet encapsulation for Kompella VPLS. Therefore, the encapsulation type of Kompella VPLS packets needs to be modified when Huawei devices communicate with non-Huawei devices.

When the device sends Kompella VPLS packets, run the **encapsulation rfc4761-compatible** command to enable the device to modify the encapsulation type of Kompella VPLS packets from Type 4 or 5 to Type 19. When the device receives Kompella VPLS packets, the device modifies the encapsulation type of Kompella VPLS packets from Type 19 to Type 4 or 5 automatically without running any command.

NOTE

When the device works as a PE, the encapsulation type is determined by the CE access mode. If the CE accesses the PE in VLAN mode, the PE encapsulates packets sent by the CE in Type 4. If the CE accesses the PE in Ethernet mode, the PE encapsulates packets sent by the CE in Type 5. VLAN and Ethernet modes are described as follows:

- VLAN: Ethernet frames transmitted between the CE and PE are attached with a VLAN tag. The tag is a service delimiter required by an ISP to differentiate clients. It is also called P-tag.
- Ethernet: Ethernet frames transmitted between the CE and PE do not have a service delimiter. If the header of Ethernet frames carries a VLAN tag, this tag is the inner VLAN tag of user packets, and is of no use to the PE. It is also called U-tag.

Precautions

The **encapsulation rfc4761-compatible** command is only used for Huawei and non-Huawei devices to communicate with each other.

Example

Enable the device to comply with RFC 4761 to encapsulate Kompella VPLS packets.

```
<HUAWEI> system-view
[HUAWEI] vsi bgp1
[HUAWEI-vsi-bgp1] pwsignal bgp
[HUAWEI-vsi-bgp1-bgp] encapsulation rfc4761-compatible
```

10.7.38 flow-label (VSI-LDP view)

Function

The **flow-label** command enables flow label-based load balancing for a VSI.

The **undo flow-label** command disables flow label-based load balancing of a VSI.

By default, flow label-based load balancing for a VSI is disabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

flow-label { **both** | **send** | **receive** } [**static**]

undo flow-label [{ **both** | **send** | **receive** } [**static**]]

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-

Parameter	Description	Value
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple links exist between P devices on a PW, to improve L2VPN traffic forwarding efficiency and ease the forwarding burden on P devices, run the **flow-label** command to configure flow label-based load balancing. After flow label-based load balancing is enabled on a PE, the PE adds different flow labels for different L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it selects a forwarding path based on the flow label in the data packet. This processing implements load balancing.

To enable flow label-based load balancing for all PWs in a VSI, run the **flow-label** command in the VSI-LDP view.

Prerequisites

MPLS L2VPN has been enabled.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.
- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

If the static flow label-based load balancing configuration does not match on both ends, the device discards packets carrying a flow label, causing packet loss.

Example

Enable flow label-based load balancing for Martini VPLS.

```
<HUAWEI> system-view
[HUAWEI] vsi 1 static
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] flow-label both
```

10.7.39 flow-label (VSI-LDP-PW view)

Function

The **flow-label** command enables flow label-based load balancing for an L2VPN PW.

The **undo flow-label** command disables flow label-based load balancing of an L2VPN PW.

The **flow-label disable** command disables flow label-based load balancing of an L2VPN PW.

The **undo flow-label disable** command restores flow label-based load balancing of an L2VPN PW.

By default, if flow label-based load balancing is enabled for a VSI, the PWs in this VSI also have flow label-based load balancing enabled; if flow label-based load balancing is disabled for a VSI, the PWs in this VSI also have flow label-based load balancing disabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H support this command.

Format

flow-label { **both** | **send** | **receive** } [**static**]

undo flow-label [{ **both** | **send** | **receive** } [**static**]]

flow-label disable

undo flow-label disable

Parameters

Parameter	Description	Value
both	Enables flow label-based load balancing for outgoing traffic and incoming traffic.	-
send	Enables flow label-based load balancing for outgoing traffic.	-
receive	Enables flow label-based load balancing for incoming traffic.	-

Parameter	Description	Value
static	Statically configures flow label-based load balancing. For dynamic PWs, if **static** is not configured, the flow label-based load balancing capability of the local end is negotiated by the remote end. For static PWs, the flow label-based load balancing capability is statically configured, irrespective of whether **static** is configured.	-

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an L2VPN carrying service traffic, when multiple links exist between Ps, flow label-based load balancing can be configured to improve traffic forwarding efficiency and reduce the forwarding pressure on the Ps. After flow label-based load balancing is enabled on a PE, the PE adds different flow labels for different L2VPN data flows to distinguish the data flows. After a P device receives a data packet carrying a flow label, it selects a forwarding path based on the flow label in the data packet. This processing implements load balancing.

To enable flow label-based load balancing for VLL PWs or PWE3 PWs, run the **flow-label** command in the PW template view, and specify the configured PW template when creating VLL PWs or PWE3 PWs.

- If flow label-based load balancing is configured for both a VSI and a PW in this VSI, the configuration of the PW takes precedence.
- If the **undo flow-label** command is run in the VSI-LDP-PW view, only the flow label-based load balancing capability that has been configured using the **flow-label** command in the VSI-LDP-PW view is disabled.
- If the **flow-label** command has been run for a VSI but not for a PW, you can run the **flow-label disable** command in the VSI-LDP-PW view to disable flow label-based load balancing of the PW. If the PW needs the flow label-based load balancing capability again, you can run the **undo flow-label disable** command to restore flow label-based load balancing.

Prerequisites

MPLS L2VPN has been enabled.

Precautions

Flow label-based load balancing can be enabled only when any of the following conditions is true:

- The **receive** parameter is configured on the local PE, and the **send** parameter is configured on the remote PE.

- The **send** parameter is configured on the local PE, and the **receive** parameter is configured on the remote PE.
- Both the **send** and **receive** parameters are configured on the local and remote PEs.

If the static flow label-based load balancing configuration does not match on both ends, the device discards packets carrying a flow label, causing packet loss.

Example

Enable flow label-based load balancing for a PW.

```
<HUAWEI> system-view
[HUAWEI] vsi 1 static
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] pw p1
[HUAWEI-vsi-1-ldp-pw-p1] flow-label both
```

Disable flow label-based load balancing for the PW **pw1**.

```
<HUAWEI> system-view
[HUAWEI] vsi 1 static
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] flow-label send
[HUAWEI-vsi-1-ldp] peer 1.1.1.1
[HUAWEI-vsi-1-ldp] peer 1.1.1.1 pw pw1
[HUAWEI-vsi-1-ldp-pw-pw1] flow-label disable
```

10.7.40 holdoff (protect-group view)

Function

The **holdoff** command configures a switching delay for a PW protection group with the master/slave PW redundancy mode.

The **undo holdoff** command deletes the switching delay for a PW protection group with the master/slave PW redundancy mode.

By default, no switching delay is configured for a PW protection group with the master/slave PW redundancy mode. In this situation, if a fault occurs on the primary PW, traffic immediately switches from the primary PW to the secondary PW.

Format

holdoff *holdoff-time*

undo holdoff

Parameters

Parameter	Description	Value
holdoff-time	Specifies the switching delay.	The value is an integer ranging from 1 to 180, in seconds.

Views

protect-group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if a working path fails, traffic immediately switches to the protection path. If the working path flaps or an error occurs in the detection mechanism, traffic frequently switches between the working and protection paths. If you want to avoid this problem in a PW protection group with the master/slave PW redundancy mode, run the **holdoff** command to configure a switching delay. If the working path recovers before the specified switching delay expires, traffic does not switch to the protection path. If the working path remains faulty after the specified switching delay expires, traffic switches to the protection path.

Prerequisites

The PW redundancy mode of the PW protection group is master/slave.

Precautions

If the **holdoff** command is run multiple times, the latest configuration overrides the previous ones.

After you configure a switching delay, traffic forwarded during the delay period will be interrupted if the primary PW fails to recover before the delay period expires.

A PW protection group with the independent PW redundancy mode does not support delayed switching.

NOTE

On a VPLS network that uses BFD for fault detection, traffic immediately switches from the primary PW to the secondary PW after BFD detects a fault on the primary PW, no matter whether delayed switching is configured. It is recommended that you determine whether to use BFD or delayed switching based on your actual network requirements.

Example

Configure a switching delay of 60s for a PW protection group.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] protect-mode pw-redundancy master
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] holdoff 60
```

10.7.41 hub-mode enable

Function

The **hub-mode enable** command sets the VSI attribute of an AC interface to hub.

The **undo hub-mode enable** command sets the VSI attribute of an AC interface to spoke.

By default, the VSI attribute of an AC interface is hub.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H and S6730-H support this command.

Format

hub-mode enable

undo hub-mode enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **isolate spoken** command is run in the VSI view, forwarding isolation is enabled on AC interfaces in a VSI, and all AC interfaces in this VSI have their VSI attribute set to spoke. If one AC interface wants to communicate with other AC interfaces in the same VSI, run the **hub-mode enable** command on this AC interface to set its VSI attribute to hub.

Prerequisites

Interfaces have been bound to a VSI instance by running the **l2 binding** command.

Example

Set the VSI attribute of VLANIF100 to hub.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
```

```
[HUAWEI] vsi v100 static
[HUAWEI-vsi-v100] pwsignal ldp
[HUAWEI-vsi-v100-ldp] vsi-id 100
[HUAWEI-vsi-v100-ldp] quit
[HUAWEI-vsi-v100] isolate spoken
[HUAWEI-vsi-v100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] l2 binding vsi v100
[HUAWEI-Vlanif100] hub-mode enable
```

Set the VSI attribute of GE0/0/1 to hub.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi v101 auto
[HUAWEI-vsi-v101] pwsignal bgp
[HUAWEI-vsi-v101-bgp] route-distinguisher 100:1
[HUAWEI-vsi-v101-bgp] quit
[HUAWEI-vsi-v101] isolate spoken
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi v101
[HUAWEI-GigabitEthernet0/0/1] hub-mode enable
```

10.7.42 ignore-ac-state

Function

The **ignore-ac-state** command enables a VSI to retain in Up state regardless of the Attachment Circuit (AC) state.

The **undo ignore-ac-state** command restores the default setting.

By default, the VSI state changes with the AC state.

Format

ignore-ac-state

undo ignore-ac-state

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

To verify whether a VSI can work normally on the new network before a VPLS network migration, run the **ignore-ac-state** command in the VSI view on the new device. This command enables the VSI to retain in Up state on the new device before the AC-side device is connected to the new device. When the AC interface is Down and the PW is Up, the VSI is Up. When the AC interface is Up and the PW is Down, the VSI is still Up.

Example

Enable a VSI to retain in Up state regardless of the AC state.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] vsi-id 2
[HUAWEI-vsi-vsi1-ldp] quit
[HUAWEI-vsi-vsi1] ignore-ac-state
```

10.7.43 ignore-mtu-match (VSI view)

Function

The **ignore-mtu-match** command enables the device to ignore the MTU matching check and re-encapsulate the sent VPLS packets.

The **undo ignore-mtu-match** command disables the device from ignoring the MTU matching check and re-encapsulating the sent VPLS packets.

By default, the device does not ignore the MTU matching check or re-encapsulate sent VPLS packets.

Format

ignore-mtu-match

undo ignore-mtu-match

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the communication in Kompella mode with devices of other vendors, you can use the **ignore-mtu-match** command to ignore the MTU check for VSIs if the devices of other vendors do not support the check. By default, the PE device checks whether MTUs of the VSIs on both ends are matched. If the MTUs of the VSIs on two ends are different, the VC cannot go Up.

As defined by the latest RFC, the encapsulation type of PW in the Kompella VPLS is 19. Huawei devices support only the Ethernet encapsulation and VLAN encapsulation. In the communication in Kompella mode with devices of other vendors, you can use the **ignore-mtu-match** command if the devices of other vendors require to receive a VPLS packet with the encapsulation type as 19. After the **ignore-mtu-match command** is run, the sent VPLS packet adopts encapsulation type 19.

Prerequisites

The following operations have been performed before this command is used:

1. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.
2. The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command.

Precautions

- This command is valid only for the VPLS in Kompella mode and does not take effect in the VPLS in Martini mode. In the Martini VPLS, the MTU values of the VSIs on two ends must be the same.
- Huawei devices can interwork with devices of other vendors only when the **ignore-mtu-match** command is used together with the **vpls bgp encapsulation** command.

Example

Disable the MTU matching check of a VSI named **bgp1** and use encapsulation type 19 for the sent VPLS packet so that a Huawei device is connected to devices of other vendors.

```
<HUAWEI> system-view
[HUAWEI] vsi bgp1 auto
[HUAWEI-vsi-bgp1] pwsignal bgp
[HUAWEI-vsi-bgp1-bgp] route-distinguisher 100:1
[HUAWEI-vsi-bgp1-bgp] quit
[HUAWEI-vsi-bgp1] ignore-mtu-match
```

10.7.44 ignore-stp-loopcheck

Function

The **ignore-stp-loopcheck** command disables STP loop detection function of PW, that is, the PW that cannot be blocked by STP.

The **undo ignore-stp-loopcheck** command restores the default configuration.

By default, STP loop detection is enabled for the PW.

Format

ignore-stp-loopcheck

undo ignore-stp-loopcheck

Parameters

None

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

After STP loop detection is enabled, a PW may be blocked when an STP loop is detected. If you do not want a PW to be blocked upon an STP loop, you can run this command to disable STP loop detection.

Example

Disable STP loop detection function of the PW named pw1.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 1.1.1.1
[HUAWEI-vsi-aa-ldp] peer 1.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1] ignore-stp-loopcheck
```

10.7.45 ingress-lsp protect-mode

Function

The **ingress-lsp protect-mode** command configures the protection mode for BGP ingress LSPs.

The **undo ingress-lsp protect-mode** command restores the default setting.

By default, no protection mode is configured for BGP ingress LSPs.

Format

ingress-lsp protect-mode bgp-frr

undo ingress-lsp protect-mode

Parameters

Parameter	Description	Value
bgp-frr	Configures the protection mode for BGP ingress LSPs to BGP Auto FRR.	-

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

To protect the links between the PE and its dual-homed ASBRs and the ASBRs themselves in the same AS, you can configure the protection mode of BGP Auto FRR.

Before configuring the protection mode of BGP Auto FRR, enable the BGP Auto FRR function.

It is recommended that the selection of labeled BGP IPv4 routes be based on the **bestroute nexthop-resolved tunnel** command.

Example

Configure the protection mode of BGP Auto FRR for BGP ingress LSPs.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family unicast
[HUAWEI-bgp-af-ipv4] ingress-lsp protect-mode bgp-frr
```

10.7.46 interface-parameter-type vccv (VSI-LDP-PW view)

Function

The **interface-parameter-type vccv** command restores the default setting.

The **undo interface-parameter-type vccv** command deletes the VCCV byte right after the interface parameter in the Mapping packet.

By default, a mapping packet carries the VCCV byte.

Format

interface-parameter-type vccv

undo interface-parameter-type vccv

Parameters

None

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the switch communicates with the devices of VRP V300R001 and all branching versions, and the LDP VPLS is configured, run the **undo interface-parameter-type vccv** command.

Prerequisites

The following operations have been performed before this command is used:

1. LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.
2. The VSI ID has been configured using the **vsi-id** *vsi-id* command.
3. The peer of the VSI has been configured using the **peer** *peer-address* command.
4. The PW has been configured using the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command.

Example

When configuring the VPLS in LDP mode, delete the VCCV byte from the Mapping packet.

```
<HUAWEI1> system-view
[HUAWEI] vsi vsi1 static
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] vsi-id 100
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2 pw pw1
[HUAWEI-vsi-vsi1-ldp-pw-pw1] undo interface-parameter-type vccv
```

10.7.47 interface-status-change mac-withdraw enable

Function

The **interface-status-change mac-withdraw enable** command enables the PEs to send LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

The **undo interface-status-change mac-withdraw enable** command disables the PEs from sending LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

By default, a PE does not send LDP MAC Withdraw messages when the status of the AC interface bound to the VSI changes.

Format

interface-status-change mac-withdraw enable

undo interface-status-change mac-withdraw enable

Parameters

None

Views

VSI-LDP view, VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, you can configure this command on the PE to enable the PE to update the MAC address entry when the AC link is in Down state. In this way, the PE connected to the SPE sends LDP MAC Withdraw messages to all peers when the status of the SPE-side interface changes.

Precautions

If the local end sends MAC-Withdraw messages, the remote VSI clears local MAC addresses and learns new MAC addresses.

After you run the **interface-status-change mac-withdraw enable** command, the PE sends LDP MAC-Withdraw messages to all peers if the status of the interface bound to the VSI changes:

- From Down to Up.
- From Up to Down.

The **interface-status-change mac-withdraw enable** takes effect only when the **mac-withdraw enable** is configured.

Example

Enable the PE to send LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] interface-status-change mac-withdraw enable
```

10.7.48 isolate spoken

Function

The **isolate spoken** command enables forwarding isolation between AC interfaces in a VSI.

The **undo isolate spoken** command disables forwarding isolation between AC interfaces in a VSI.

By default, forwarding isolation between AC interfaces in a VSI is disabled.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H and S6730-H support this command.

Format

isolate spoken

undo isolate spoken

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple users are bound to the same VSI, you can use the **isolate spoken** command to enable forwarding isolation between AC interfaces. After this command is run, the VSI attribute of all AC interfaces in the VSI is spoke, preventing the users from communicating with each other.

Prerequisites

- For Martini VPLS, the **pwsignal ldp** and **vsi-id** *vsi-id* commands have been run.
- For Kompella VPLS, the **pwsignal bgp** and **route-distinguisher** *route-distinguisher* commands have been run.
- For BGP AD VPLS, the **bgp-ad** and **vpls-id** *vpls-id* commands have been run.

Example

Enable forwarding isolation between AC interfaces in a VSI in Martini VPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi v100 static
[HUAWEI-vsi-v100] pwsignal ldp
[HUAWEI-vsi-v100-ldp] vsi-id 100
[HUAWEI-vsi-v100-ldp] quit
[HUAWEI-vsi-v100] isolate spoken
```

Enable forwarding isolation between AC interfaces in a VSI in Kompella VPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
```

```
[HUAWEI] vsi v101 auto
[HUAWEI-vsi-v101] pwsignal bgp
[HUAWEI-vsi-v101-bgp] route-distinguisher 100:1
[HUAWEI-vsi-v101-bgp] quit
[HUAWEI-vsi-v101] isolate spoken
```

Enable forwarding isolation between AC interfaces in a VSI in BGP AD VPLS.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi v102
[HUAWEI-vsi-v102] bgp-ad
[HUAWEI-vsi-v102-bgpad] vpls-id 100:2
[HUAWEI-vsi-v102-bgpad] quit
[HUAWEI-vsi-v102] isolate spoken
```

10.7.49 l2 binding

Function

The **l2 binding** command binds an interface to a VSI.

The **undo l2 binding** command unbinds an interface to a VSI.

By default, the interface is not bound to any VSI.

Format

l2 binding vsi *vsi-name*

undo l2 binding vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI to be bound with an interface.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the VPLS, run the **l2 binding** command on the PE to bind the interface that is connected to the CE to the corresponding VSI.

Precautions

When an interface is bound to a VSI, the MTU can be configured in the interface view but does not take effect. The MTU configured in the VSI is used for PW MTU negotiation.

In the VPLS application, different CEs are transparently connected to each other in the same network segment of a LAN through VSIs, and the IP addresses of the CEs must be different.

NOTE

- If an interface is used as a VPLS AC-side interface and a multicast inbound interface at the same time, multicast data cannot be forwarded normally on this interface. (S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730S-H, S6730-S, S6730S-S, and S6730-H do not have this restriction.)
- If a sub-interface is bound to a VSI, you can delete the sub-interface only after unbinding it from the VSI.
- To use a 40GE, 100GE, XGE, 25GE, MultiGE, GE, or Eth-Trunk interface of the switch as an AC-side interface, run the **undo portswitch** command to change the interface to a Layer 3 interface before running the **l2 binding** command.
- Before running the **l2 binding** command on a sub-interface, add the main interface to a VLAN.
- The **l2 binding** command and the **ip address** command cannot be configured on the CE-side interface of the PE at the same time.
- If a main interface is bound to a VSI instance, the sub-interfaces of the main interface cannot be bound to the VSI instance. Similarly, if the sub-interface of a main interface is bound to a VSI instance, the main interface cannot be bound to the VSI instance.

Example

Bind a VLANIF interface to the VSI.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] l2 binding vsi company2
```

Bind a GigabitEthernet interface to a VSI.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi company2
```

10.7.50 l2vpn-ad-family

Function

The **l2vpn-ad-family** command displays the BGP L2VPN-AD address family view.

The **undo l2vpn-ad-family** command deletes all configurations in the BGP L2VPN-AD address family view.

Format

l2vpn-ad-family

undo l2vpn-ad-family

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The BGP AD VPLS shares a TCP connection with the common BGP. Most BGP AD VPLS configurations are the same as the common BGP configurations. To exchange information about BGP AD VPLS members, enable peers to exchange information about VPLS members in the BGP L2VPN-AD address family view. Run the **l2vpn-ad-family** command to enter the BGP L2VPN-AD address family view.

Prerequisites

Generally, BGP peers need to be configured in the BGP view to implement the configuration of basic BGP functions.

Example

Enter the BGP L2VPN-AD address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
[HUAWEI-bgp-af-l2vpn-ad]
```

10.7.51 loop-detect enable

Function

The **loop-detect enable** command enables L2VPN loop detection on an interface.

The **undo loop-detect enable** command disables L2VPN loop detection on the interface.

By default, L2VPN loop detection is disabled on the interface.

Format

loop-detect enable

undo loop-detect enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Redundant links are used on an Ethernet switching network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and unstable MAC address entries. This degrades communication quality or even interrupts communication. On a traditional Layer 2 network, the Spanning Tree Protocol (STP) is usually used to prevent loops.

VPLS is an L2VPN technology providing LAN-like services over the MPLS network. It allows sites in diverse locations to connect the MPLS network and communicate with each other, which frees Ethernet LAN deployment from restrictions imposed by physical locations. As a Layer 2 Ethernet technology, VPLS has the following disadvantages:

- If the customer network leases multiple lines, loops may occur due to incorrect customer configuration or in other unexpected cases, leading to broadcast storms.
- If the customer network traverses a third-party network, loops may occur due to incorrect third-party network configuration or in other unexpected cases, leading to broadcast storms.

STP needs to be deployed on CEs, having high dependency on the customer network. The complex and changing features of the customer network increase the maintenance difficulty of the carrier.

To prevent loops on an L2VPN network, you can run the **loop-detect enable** command on an AC interface of a PE to configure L2VPN loop detection on the AC interface. After this function is enabled, when detecting a loop on the L2VPN network, the PE will automatically block an interface on the loop, report an alarm, and eliminate the loop.

Prerequisites

The interface has been bound to a VSI instance using the **l2 binding** command on the interface.

NOTE

- The interface must be an AC interface bound to a specified VSI. For details about the binding between an AC interface and a VSI, see **Binding VSIs to AC Interfaces**.

Example

Enable L2VPN loop detection on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi company2
[HUAWEI-GigabitEthernet0/0/1] loop-detect enable
```

10.7.52 loop-detect detection pe-vid ce-vid

Function

The **loop-detect detection pe-vid ce-vid** command specifies a VLAN range to which a QinQ termination sub-interface sends L2VPN loop detection packets.

The **undo loop-detect detection pe-vid ce-vid** command deletes the VLAN range to which the QinQ termination sub-interface sends L2VPN loop detection packets.

By default, the QinQ termination sub-interface does not send L2VPN loop detection packets.

Format

loop-detect detection pe-vid *pe-vid* **ce-vid** *low-vid* [**to** *high-vid*]

undo loop-detect detection pe-vid *pe-vid* **ce-vid** *low-vid* [**to** *high-vid*]

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the outer VLAN ID in L2VPN loop detection packets sent by the QinQ termination sub-interface.	The value is an integer in the range of 2 to 4094.
ce-vid *low-vid*	Specifies the start inner VLAN ID in L2VPN loop detection packets sent by the QinQ termination sub-interface.	The value is an integer in the range of 1 to 4094.
high-vid	Specifies the end inner VLAN ID in L2VPN loop detection packets sent by the QinQ termination sub-interface.	The value is an integer in the range of 1 to 4094. The value of *high-vid* must be greater than that of *low-vid*.

Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, and Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **loop-detect enable** command to enable L2VPN loop detection on an interface, the QinQ termination sub-interface does not send L2VPN loop detection packets by default. You need to run the **loop-detect detection pe-vid ce-vid** command to configure the VLAN range to which the QinQ termination sub-interface sends L2VPN loop detection packets. After the VLAN range is configured, the device sends L2VPN loop detection packets to the specified VLANs. If a loop is detected in a VLAN, the sub-interface will stop sending L2VPN loop detection packets to all these VLANs.

Prerequisites

L2VPN loop detection has been enabled on the interface using the **loop-detect enable** command.

Example

Configure the QinQ termination sub-interface GigabitEthernet0/0/1.1 to send L2VPN loop detection packets to VLANs 2 to 10.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] qinq termination pe-vid 300 ce-vid 2 to 20
[HUAWEI-GigabitEthernet0/0/1.1] l2 binding vsi company2
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect enable
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect detection pe-vid 300 ce-vid 2 to 10
```

10.7.53 loop-detect detection vid

Function

The **loop-detect detection vid** command specifies a VLAN range to which a Dot1q termination sub-interface sends L2VPN loop detection packets.

The **undo loop-detect detection vid** command deletes the VLAN range to which the Dot1q termination sub-interface sends L2VPN loop detection packets.

By default, the Dot1q termination sub-interface does not send L2VPN loop detection packets.

Format

loop-detect detection vid *low-vid* [**to** *high-vid*]

undo loop-detect detection vid *low-vid* [**to** *high-vid*]

Parameters

Parameter	Description	Value
low-vid	Specifies the start VLAN ID in L2VPN loop detection packets sent by the Dot1q termination sub-interface.	The value is an integer in the range of 2 to 4094.
high-vid	Specifies the end VLAN ID in L2VPN loop detection packets sent by the Dot1q termination sub-interface.	The value is an integer in the range of 2 to 4094. The value of *high-vid* must be greater than that of *low-vid*.

Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, and Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After L2VPN loop detection is enabled on an interface using the **loop-detect enable** command, the Dot1q termination sub-interface does not send L2VPN loop detection packets by default. You need to run the **loop-detect detection vid** command to configure the VLAN range to which the Dot1q termination sub-interface sends L2VPN loop detection packets. After the VLAN range is configured, the device sends L2VPN loop detection packets to the specified VLANs. If a loop is detected in a VLAN, the sub-interface will stop sending L2VPN loop detection packets to all these VLANs.

Prerequisites

L2VPN loop detection has been enabled on the interface using the **loop-detect enable** command.

Example

Configure the Dot1q termination sub-interface GigabitEthernet0/0/1.1 to send L2VPN loop detection packets to VLANs 3 to 10.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] dot1q termination vid 2 to 10
[HUAWEI-GigabitEthernet0/0/1.1] l2 binding vsi company2
```

```
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect enable
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect detection vid 3 to 10
```

10.7.54 loop-detect recovery-time

Function

The **loop-detect recovery-time** command specifies a period for restoring an interface to normal state.

The **undo loop-detect recovery-time** command restores the default period for restoring an interface to normal state.

By default, an AC interface restores a blocked interface every 15 seconds.

Format

loop-detect recovery-time *recovery-time*

undo loop-detect recovery-time

Parameters

Parameter	Description	Value
recovery-time *recovery-time*	Specifies a period for an AC interface to restore a blocked interface.	The value is an integer in the range of 15 to 255, in seconds. By default, the value is 15 seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AC interface enabled with L2VPN loop detection detects a loop, a period can be specified for the AC interface to restore a blocked interface. That is, if a blocked interface does not receive any L2VPN loop detection packet within the period specified by *recovery-time*, it will be restored to normal state.

If a device is on multiple loops, interfaces on the device may alternate between blocked and normal states during the initial detection stage. To prevent interface status flapping, you are advised to set *recovery-time* to a larger value.

Prerequisites

L2VPN loop detection has been enabled on the interface using the **loop-detect enable** command.

Example

Configure the Dot1q termination sub-interface GigabitEthernet0/0/1.1 to restore a blocked interface every 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] vcmp role silent
[HUAWEI] interface gigabitethernet
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] dot1q termination vid 1 to 10
[HUAWEI-GigabitEthernet0/0/1.1] l2 binding vsi company2
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect enable
[HUAWEI-GigabitEthernet0/0/1.1] loop-detect recovery-time 20
```

10.7.55 local-mac remove all-but-mine

Function

The **local-mac remove all-but-mine** command enables a local provider edge (PE) device to delete user MAC address entries, except those entries associated with the PW that sends MAC Withdraw messages with the TLV type of 0x404.

The **undo local-mac remove all-but-mine** command restores the default configuration.

A PE removes all MAC addresses by default after receiving MAC Withdraw messages with the TLV type of 0x404.

Format

local-mac remove all-but-mine

undo local-mac remove all-but-mine

Parameters

None

Views

VSI view

Default Level

2: Configuration level

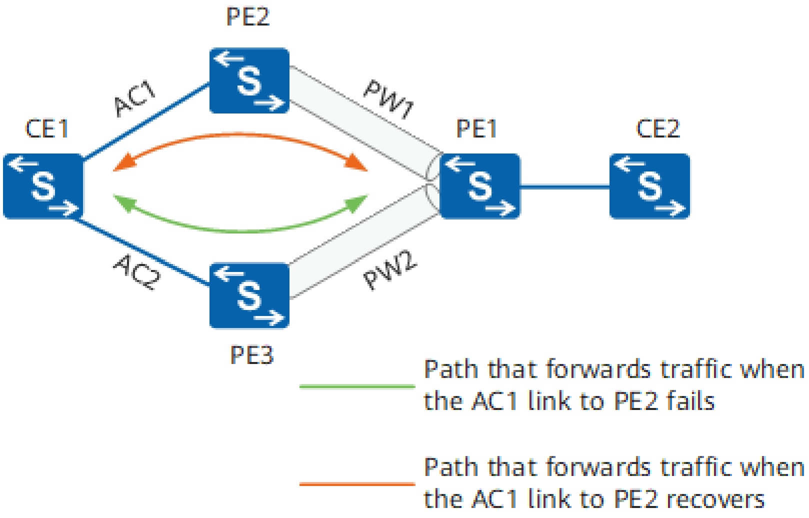
Usage Guidelines

Usage Scenario

A customer edge (CE) device is dual-homed to two PEs over pseudo wires (PWs) on a virtual private LAN service (VPLS) network. If a PE finds that an AC fault is removed, the PE sends MAC Withdraw messages with the TLV type of 0x404 to instruct a remote PE to update MAC address entries and perform a traffic switchover. For example, CE1 is connected to CE2 over primary PW1 and secondary PW2 on the network shown in **Figure 10-1**. After a fault in AC1 or PE2 is removed, PE2 sends to PE1 MAC Withdraw messages with the TLV type of 0x404 over PW1. After PE1 receives the messages, PE1 removes MAC addresses but retains those associated with PW1. The procedure complies with RFC. User traffic can then switch from PW2 to PW1.

To allow communication between a Huawei device and a non-Huawei device in compliance with RFC, run the **local-mac remove all-but-mine** command. This command is run only on PE1 shown in **Figure 10-1**.

Figure 10-1 CE dual-homing to a VPLS network



Precautions

This command takes effect on a PE that receives MAC Withdraw messages only with the TLV type of 0x404.

Example

Enable a PE to remove all MAC address entries but retain MAC address entries associated with a PW over which the PE receives MAC Withdraw messages with the TLV type of 0x404.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] local-mac remove all-but-mine
```

10.7.56 mac-address static vlanif

Function

The **mac-address static vlanif** command configures a static MAC address entry. The outgoing interface of this entry is added to the specified VLAN corresponding to the VLANIF interface. The VLANIF interface is bound to a VSI.

The **undo mac-address static vlanif** command deletes a static MAC address entry.

By default, the system does not configure any static MAC address entry.

Format

mac-address static *mac-address interface-type interface-number* **vlanif** *interface-number* **vsi** *vsi-name*

undo mac-address static *mac-address interface-type interface-number* **vlanif** *interface-number* **vsi** *vsi-name*

Parameters

Parameter	Description	Value
static	Indicates the static entry that is not aged. When a frame of a specific MAC address is received, the frame is forwarded through the outgoing interface directly. After being configured and saved, the entries are still stored in the table even if the system is reset.	-
mac-address	Specifies the unicast MAC address in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a broadcast MAC address (FFFF-FFFF-FFFF) or a multicast MAC address (the eighth bit is 1).
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlanif *interface-number*	Specifies the number of the VLANIF interface bound to a VSI.	-

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPLS provides reachability through MAC address learning. Each PE maintains a MAC address table.

The device learns source MAC addresses and then creates the MAC address table. However, the device cannot identify whether the packets are from authorized users or hackers, which brings security threats. If a hacker sets the source MAC address of attack packets to the MAC address of an authorized user and connects to another interface of the device, the device learns an incorrect MAC address entry. The packets that should be forwarded to the authorized user are forwarded to the hacker.

To improve interface security, the network administrator can manually create MAC address entries to bind MAC addresses of authorized users to specified interfaces using the **mac-address static vlanif** command. This prevents hackers from intercepting data of authorized users.

Prerequisites

The network administrator is familiar with the MAC addresses of the devices on the network that need to use static MAC address entries for communications; otherwise, the configuration will interrupt authorized users' communications.

In the **mac-address static vlanif** command, the interface must be a Layer 2 interface that has been added to the VLAN corresponding to the VLANIF interface. The VLANIF interface must be bound to the VSI configured in the command.

Precautions

After being created, the static MAC address entries will not be aged. When receiving a frame of a specific MAC address, the device forwards the frame through the outgoing interface directly. After being configured and saved, the MAC address entries are still stored in the table even if the system is reset.

A physical interface that is associated with a VSI can be bound to several VLANs. The VSI that is bound to a VLANIF interface can be associated with several physical interfaces. Therefore, you need to specify a physical interface and a VLANIF interface when configuring static MAC address entries for VSIs bound to the VLANIF interface.

Manually created MAC address entries take precedence over automatically created MAC address entries. Static MAC address entries and blackhole MAC address entries take precedence over dynamic MAC address entries.

If the user service changes, specify a new VSI bound to the interface. In this way, data of the user is not forwarded through the previously configured static MAC address entries. You need to configure new MAC address entries on the device or enable the device to learn dynamic MAC address entries to forward the data.

Example

Bind VLANIF10 to the VSI named **abc**, and add a MAC address entry with the MAC address being 00e0-fc12-3456 to the VSI. When a frame that belongs to VLAN 10 and has the destination MAC address 00e0-fc12-3456 is received, it is forwarded through the outgoing interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] vsi abc static
[HUAWEI-vsi-abc] pwsignal ldp
[HUAWEI-vsi-abc-ldp] vsi-id 1
[HUAWEI-vsi-abc-ldp] quit
[HUAWEI-vsi-abc] quit
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 10
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] l2 binding vsi abc
[HUAWEI-Vlanif10] quit
[HUAWEI] mac-address static 00e0-fc12-3456 gigabitethernet 0/0/1 vlanif 10 vsi abc
```

10.7.57 mac-address static vsi

Function

The **mac-address static vsi** command configures a static MAC address entry. The outgoing interface in this entry is bound to a specified VSI.

The **undo mac-address static vsi** command deletes a static MAC address entry.

By default, the system does not configure any static MAC address entry.

Format

mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name*

undo mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name*

undo mac-address static vsi *vsi-name*

Parameters

Parameter	Description	Value
static	Indicates the static entry that is not aged. When a frame of a specific MAC address is received, the frame is forwarded through the outgoing interface directly. After being configured and saved, the entries are still stored in the table even if the system is reset.	-
mac-address	Specifies the unicast MAC address in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a broadcast MAC address (FFFF-FFFF-FFFF) or a multicast MAC address (the eighth bit is 1).
interface-type interface-number	Specifies the type and number of an interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	The interface can be a GE interface, a GE sub-interface, an XGE interface, an XGE sub-interface, a 25GE interface, a 25GE sub-interface, a 40GE interface, a 40GE sub-interface, a 100GE interface, a 100GE sub-interface, an Eth-Trunk interface, or an Eth-Trunk sub-interface. The interface in this command is a Layer 3 interface bound to a VSI.
vsi *vsi-name*	Specifies the name of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPLS provides reachability through MAC address learning. Each PE maintains a MAC address table.

The device learns source MAC addresses and then creates the MAC address table. However, the device cannot identify whether the packets are from authorized users or hackers, which brings security threats. If a hacker sets the source MAC address of attack packets to the MAC address of an authorized user and connects to another interface of the device, the device learns an incorrect MAC address entry. The packets that should be forwarded to the authorized user are forwarded to the hacker.

To improve interface security, the network administrator can manually create MAC address entries to bind MAC addresses of authorized users to specified interfaces using the **mac-address static vlanif** command. This prevents hackers from intercepting data of authorized users.

Prerequisites

The network administrator is familiar with the MAC addresses of the devices on the network that need to use static MAC address entries for communications; otherwise, the configuration will interrupt authorized users' communications.

In the **mac-address static vsi** command, the interface must be a Layer 3 interface bound to a VSI.

Precautions

After being created, the static MAC address entries will not be aged. When receiving a frame of a specific MAC address, the device forwards the frame through the outgoing interface directly. After being configured and saved, the MAC address entries are still stored in the table even if the system is reset.

Manually created MAC address entries take precedence over automatically created MAC address entries. Static MAC address entries and blackhole MAC address entries take precedence over dynamic MAC address entries.

If the user service changes, specify a new VSI bound to the interface. In this way, data of the user is not forwarded through the previously configured static MAC address entries. You need to configure new MAC address entries on the device or enable the device to learn dynamic MAC address entries to forward the data.

Example

Add a static MAC address entry to the VSI named **abc**. When the destination MAC address of a received frame is 00e0-fc33-4455, the frame is forwarded in the VSI named **abc**.

```
<HUAWEI> system-view
[HUAWEI] vsi abc static
[HUAWEI-vsi-abc] pwsignal ldp
[HUAWEI-vsi-abc-ldp] vsi-id 1
[HUAWEI-vsi-abc-ldp] quit
[HUAWEI-vsi-abc] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] l2 binding vsi abc
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] mac-address static 00e0-fc33-4455 gigabitethernet 0/0/1 vsi abc
```

10.7.58 mac-diagnose enable

Function

The **mac-diagnose enable** command enables diagnostic test on the MAC address learning capacity.

The **mac-diagnose disable** command disables diagnostic test on the MAC address learning capacity.

The **undo mac-diagnose enable** command disables diagnostic test on the MAC address learning capacity.

By default, diagnostic test on the MAC address learning capacity is enabled.

Format

mac-diagnose enable

mac-diagnose disable

undo mac-diagnose enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To rectify a Layer 2 communication fault on the device, run the **mac-diagnose enable** command to enable diagnostic test on the MAC address learning capacity.

Precautions

Using the **mac-diagnose enable** command, you can enable diagnostic test on the MAC address learning capacity. The **mac-populate** and **mac-purge** operations can be performed only when diagnostic test on the MAC address learning capacity is enabled. Otherwise, the **mac-populate** and **mac-purge** operations cannot be performed. In addition, information and statistics on populated OAM MAC address are cleared.

Example

Enable diagnostic test on the MAC address learning capacity.

```
<HUAWEI> system-view
[HUAWEI] mac-diagnose enable
```

Disable diagnostic test on the MAC address learning capacity.

```
<HUAWEI> system-view
[HUAWEI] mac-diagnose disable
```

10.7.59 mac-learning

Function

The **mac-learning enable** command enables MAC address learning for a VSI.

The **mac-learning disable** command disables MAC address learning of a VSI.

The **undo mac-learning disable** command enables MAC address learning for a VSI.

By default, MAC address learning is enabled for a VSI.

Format

mac-learning { **enable** | **disable** }

undo mac-learning disable

Parameters

Parameter	Description	Value
enable	Enables a VSI to learn MAC addresses.	-
disable	Disables a VSI to learn MAC addresses.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To disable MAC address learning in a VSI on a VPLS network, run the **mac-learning disable** command. The VPLS network then functions similarly to a VPWS network. For example, if there are only two PEs with each connecting to one CE, disabling MAC address learning in a VSI on a PE reduces the PE's pressure.

Configuration Impact

After the **mac-learning disable** command is run for a VSI, the VSI can no longer automatically learn MAC addresses, causing packets to be broadcast on the network. Therefore, exercise caution when running this command.

Example

Disable MAC address learning of the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] mac-learning disable
```

10.7.60 mac-limit (VSI view)

Function

The **mac-limit** command configures the MAC address limit rules on a VSI.

The **undo mac-limit** command restores the default setting.

By default, none of the MAC address limit rule is configured on a VSI.

NOTE

Only the S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-S, S6730S-H and S6730-H support this command.

Format

mac-limit { **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } | **maximum** *max-number* } *

undo mac-limit

Parameters

Parameter	Description	Value
action	Indicates the action performed on packets when the number of MAC entries reaches the limit. By default, the system discards the packets.	-
discard	Indicates that after the number of MAC entries reaches the limit, the system discards the packet whose destination MAC address does not map to any entry in the MAC address table.	-
forward	Indicates that after the number of MAC entries reaches the limit, the system broadcasts a packet whose destination MAC address does not map to any entry in the MAC address table, but does not learn the destination MAC address of the packet.	-

Parameter	Description	Value
alarm	Indicates whether an alarm is generated when the number of MAC address entries reaches the limit.	-
disable	Indicates that no alarm is generated when the number of MAC address entries reaches the limit.	-
enable	Indicates that an alarm is generated in syslog mode when the number of MAC address entries reaches the limit. By default, an alarm is sent to the NM station.	-
maximum *max-number*	Specifies the maximum number of MAC address entries that the current VSI can learn. **NOTE** Set **maximum** *max-number* before you set **action** or **alarm**.	The value is an integer that ranges from 0 to 4096.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent attacks, you can run the **mac-limit** command to limit the maximum number of MAC addresses that the current VSI can learn.

Precautions

If the VSI has learned some MAC addresses, run the **undo mac-address dynamic** command to clear the learned MAC addresses. Otherwise, the **mac-limit** command cannot limit the MAC address learning accurately.

When the **mac-limit** command is executed for the first time, you can configure **action** and **alarm** only after **maximum** *max-number* is configured. If the **mac-limit** command is not executed for the first time, there is no special requirement on the configuration sequence.

Example

Set the maximum number of MAC addresses that can be learned to 100 on the VSI PW.

```
<HUAWEI> system-view
[HUAWEI] vsi 1
[HUAWEI-vsi-1] mac-limit maximum 100
```

10.7.61 mac-populate

Function

The **mac-populate** command populates an OAM MAC address to initiate a diagnostic test on the MAC address learning capacity.

Format

mac-populate vsi *vsi-name* **mac** *mac-address* [**packet-num** *num* | **flood**] *

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
mac *mac-address*	Specifies the MAC address for the diagnostic test, expressed in the format of H-H-H.	The value is in H-H-H format. The values are as follows: • 0018-82a4-3fb1 • 0018-82a4-3fb2 • 0018-82a4-3fb3 • 0018-82a4-3fb4 • 0018-82a4-3fb5 • 0018-82a4-3fb6 • 0018-82a4-3fb7 • 0018-82a4-3fb8 • 0018-82a4-3fb9 • 0018-82a4-3fba
packet-num *num*	Specifies the number of packets to be sent.	The value is a decimal integer that ranges from 1 to 5. The default value is 3.
flood	Indicates that the OAM MAC address is flooded throughout the VSI.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To rectify a Layer 2 communication fault on the device, you can run the **mac-populate** command to populate an OAM MAC address into the device to initiate a diagnostic test.

Prerequisites

The diagnostic test on the MAC address learning capacity has been enabled using the **mac-diagnose enable** command.

Precautions

The **mac-populate** command does not support BGP AD VPLS.

Using the **mac-populate** command, you can populate an OAM MAC address into the device.

- If the **mac-populate** command does not contain **flood**, an OAM MAC address is only populated into the local device.
- If the **mac-populate** command contains **flood**, an OAM MAC is flooded throughout the VSI and then populated into the peer and local devices.

NOTE

The OAM MAC address populated into the local and peer devices can control the forwarding. Under the guidance of the OAM MAC address, the peer device forwards the received packets corresponding to the OAM MAC address to the local device.

The default aging time of OAM MAC addresses is 150 seconds.

Example

Populate an OAM MAC address into the VSI named **vsi1**, flood the OAM MAC address over the domain, and set the number of packets to be sent to 3.

```
<HUAWEI> mac-populate vsi vsi1 mac 0018-82a4-3fb1 flood packet-num 3
```

10.7.62 mac-purge

Function

The **mac-purge** command purges an OAM MAC address from the forwarding table.

Format

mac-purge vsi *vsi-name* **mac** *mac-address* [**packet-num** *num* | **register** | **flood**] *

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
mac *mac-address*	Specifies the MAC address for the diagnostic test, expressed in the format of H-H-H.	The value is in H-H-H format. The values are as follows: ● 0018-82a4-3fb1 ● 0018-82a4-3fb2 ● 0018-82a4-3fb3 ● 0018-82a4-3fb4 ● 0018-82a4-3fb5 ● 0018-82a4-3fb6 ● 0018-82a4-3fb7 ● 0018-82a4-3fb8 ● 0018-82a4-3fb9 ● 0018-82a4-3fba
packet-num *num*	Specifies the number of packets to be sent.	The value is a decimal integer that ranges from 1 to 5. The default value is 3.
register	Specifies the MAC address reserved for the OAM test. **NOTE** If the preceding command contains **register**, an OAM MAC address is populated into the local device or the peer device to make the device discard received packets corresponding to the OAM MAC address.	-
flood	Indicates that the OAM MAC address is flooded throughout the VSI.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To rectify a Layer 2 communication fault on the device, you can run the **mac-purge** command to clear OAM MAC addresses populated into the device.

Prerequisites

The diagnostic test on the MAC address learning capacity has been enabled using the **mac-diagnose enable** command.

Precautions

- If *vsi-name* in the **mac-purge** command for purging an OAM MAC address is not identical with *vsi-name* in the **mac-purge** command that is previously used in populating the OAM MAC address, the OAM MAC address cannot be cleared.
- A maximum of 100 OAM MAC addresses of **populate** and **register+populate** types can be populated into a device.
- The **mac-purge** command does not support BGP AD VPLS.

Using the **mac-purge** command, you can purge the populated OAM MAC address that is specialized for the test or register an OAM MAC address to a device to make the device discard the received packets corresponding to the OAM MAC address.

Test objects vary according to parameters.

- If the **mac-purge** command contains **flood**, an OAM MAC address is flooded throughout the VSI and then purged from all devices in the VSI and the local device into which the OAM MAC address has been populated. If the preceding command does not contain **flood**, the OAM MAC address is purged only from the local device.
- If the **mac-purge** command contains **register**, an OAM MAC address is registered on the device to make the device discard the packet corresponding to the OAM MAC address after receiving them.

Example

Purge the OAM MAC address from the VSI named **vsi1**, flood the OAM MAC address over the domain, and set the number of packets to be sent to 3.

```
<HUAWEI> mac-purge vsi vsi1 mac 0018-82a4-3fb1 flood packet-num 3
```

10.7.63 mac-withdraw enable

Function

The **mac-withdraw enable** command enables a VSI to delete the local MAC address and inform all the remote peers of the deletion.

The **undo mac-withdraw enable** command disables a VSI to delete the local MAC address and inform all the remote peers of the deletion.

By default, the MAC-withdraw function is disabled.

Format

mac-withdraw enable

undo mac-withdraw enable

Parameters

None

Views

VSI-LDP view, VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, if the remote end specifies the local end as the UPE, the remote AC interface does not inform the local end to cancel the label after the AC interface is faulty. In this case, the local end is unaware of an AC fault or a UPE fault. The VSI remains Up and does not delete the corresponding MAC address entries in time. As a result, the remote end cannot receive data streams sent by the local end. After the **mac-withdraw enable** command is executed, the VSI deletes the local MAC address and informs all the remote peers of the deletion when an AC fault or a UPE fault occurs and the VSI remains Up. This solves the preceding problem.

Precautions

When an AC fault or a UPE fault occurs and the VSI remains Up, the UPE device needs to switch the VPLS traffic to another LSP if the UPE device accesses the SPE device in dual-homed mode. The SPE device then only needs to inform the other SPEs corresponding to the VSI to delete the MAC entries learnt from this VSI. After traffic switchover, the SPEs re-learn MAC entries from each other.

This command must be configured on SPEs.

The **mac-withdraw enable** command must be used together with the **interface-status-change mac-withdraw enable** command.

Example

Configure a VSI named v100 to delete the local MAC addresses and inform all the remote peers of the deletion when an AC fault or a UPE fault occurs and the VSI remains Up.

```
<HUAWEI> system-view
[HUAWEI] vsi v100 static
[HUAWEI-vsi-v100] pwsignal ldp
[HUAWEI-vsi-v100-ldp] mac-withdraw enable
```

10.7.64 mac-withdraw propagate enable

Function

The **mac-withdraw propagate enable** command enables a PE to forward a received MAC Withdraw message to peers.

The **undo mac-withdraw propagate enable** command disables a PE from forwarding a received MAC Withdraw message to peers.

By default, a PE does not forward a received MAC Withdraw message.

Format

mac-withdraw propagate enable

undo mac-withdraw propagate enable

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an LDP or BGP AD VPLS network, after a local PE receives a MAC Withdraw message, the local PE needs to forward the MAC Withdraw message to its peers. Otherwise, its peers cannot detect network topology changes or learn new MAC addresses in a timely manner. As a result, traffic loss caused by invalid MAC addresses will occur. The **mac-withdraw propagate enable** command enables a PE to forward a received MAC Withdraw message to peers.

Precautions

After you run the **mac-withdraw propagate enable** command on a PE, the PE forwards a received MAC Withdraw message to its peers according to the split horizon principle:

- The MAC Withdraw message received from a UPE will be forwarded to NPEs and other UPEs.
- The MAC Withdraw message received from an NPE will be forwarded to UPEs, but will not be forwarded to other NPEs.

Example

Configure vsi100 on a PE to forward a received MAC Withdraw message to peers.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi100
[HUAWEI-vsi-vsi100] mac-withdraw propagate enable
```

10.7.65 mpls l2vpn default vlan

Function

The **mpls l2vpn default vlan** command configures the default VLAN for a main interface.

The **undo mpls l2vpn default vlan** command deletes the default VLAN of a main interface.

Format

mpls l2vpn default vlan *vlan-id*

undo mpls l2vpn default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a main interface.	The value is an integer that ranges from 1 to 4094.

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the following conditions are met, you can run the **mpls l2vpn default vlan** command to specify the default VLAN on a main interface:

- The VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts only the tagged packets.

- The local PE is connected to a computer by using a GE interface, XGE interface, 25GE interface, MultiGE interface, 40GE interface, 100GE interface, or Eth-Trunk interface as the AC interface.

  In this scenario, the computer sends and receives only untagged packets. After the default VLAN is specified on the main interface, the local PE performs the following operations:
  - The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.
  - The local PE removes the VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Precautions

Before binding the main interface to the VSI, you need to run the **mpls l2vpn default vlan** command to specify the default VLAN of the main interface.

If the remote PE can replace the VLAN tags in the packets with the VLAN tag of the AC-side outgoing interface when terminating the PW, the default VLAN on the main interface of the local PE can be set to any VLAN ID. Otherwise, the default VLAN of the main interface must be the same as the VLAN of the AC-side outgoing interface on the remote PE.

To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.

Example

Configure the default VLAN of primary interface.

```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] undo portswitch
[HUAWEI-GigabitEthernet0/0/2] mpls l2vpn default vlan 100
```

10.7.66 mpls l2vpn ip-parse enable

Function

The **mpls l2vpn ip-parse enable** command enables the IP packet parsing function of the MPLS L2VPN module.

The **undo mpls l2vpn ip-parse enable** command disables the IP packet parsing function of the MPLS L2VPN module.

By default, the IP packet parsing function of the MPLS L2VPN module is enabled.

Format

mpls l2vpn ip-parse enable

undo mpls l2vpn ip-parse enable

NOTE

This command is supported only on the S6720-EI and S6720S-EI.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Layer 2 VPN scenario, if a traffic policy is configured in the inbound direction of an AC-side interface on a device, L2VPN traffic forwarded from a PE may incorrectly match the traffic policy. As a result, traffic fails to be forwarded. To ensure normal traffic forwarding, run the **undo mpls l2vpn ip-parse enable** command to disable the IP packet parsing function of the MPLS L2VPN module.

Precautions

If the enhanced load balancing mode is configured for an Eth-Trunk, it is recommended that the IP packet parsing function of the MPLS L2VPN module be enabled.

Example

Disable the IP packet parsing function of the MPLS L2VPN module.

```
<HUAWEI> system-view
[HUAWEI] undo mpls l2vpn ip-parse enable
```

10.7.67 mpls l2vpn mac-withdraw disable

Function

The **mpls l2vpn mac-withdraw disable** command disables the VLL from sending MAC Withdraw messages on a VPLS network with primary and secondary VLLs.

The **undo mpls l2vpn mac-withdraw disable** command restores the default setting.

By default, the VLL is enabled to send MAC Withdraw messages on a VPLS network with primary and secondary VLLs.

Format

mpls l2vpn mac-withdraw disable

undo mpls l2vpn mac-withdraw disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a VPLS scenario with primary and secondary VLLs, the primary and secondary VLLs send MAC Withdraw messages to the VPLS-enabled RSG each time a primary/secondary PW switchover is performed. After receiving the MAC Withdraw messages, the VPLS-enabled RSG clears all learned MAC addresses. Then packets will be transmitted in broadcast mode. To prevent packets from being broadcast, run the **mpls l2vpn mac-withdraw disable** command to disable the VLL in Ethernet or VLAN encapsulation mode from sending MAC-Withdraws messages during a primary/secondary PW switchover.

Precautions

This command takes effect only in a VPLS scenario with primary and secondary VLLs. In other scenarios, do not run the **mpls l2vpn mac-withdraw disable** command; otherwise, services will be interrupted.

Example

Disable the VLL in Ethernet or VLAN encapsulation mode from sending MAC Withdraw messages during a primary/secondary PW switchover.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] mpls l2vc 2.2.2.2 100
[HUAWEI-Vlanif10] mpls l2vc 4.4.4.4 200 secondary
[HUAWEI-Vlanif10] mpls l2vpn mac-withdraw disable
```

10.7.68 mpls l2vpn vlan-stacking

Function

The **mpls l2vpn vlan-stacking** command configures the stacked VLAN ID for a main interface.

The **undo mpls l2vpn vlan-stacking** command deletes the stacked VLAN ID from a main interface.

By default, the system does not add a VLAN ID to a packet passing through the main interface.

Format

mpls l2vpn vlan-stacking stack-vlan *vlan-id*

undo mpls l2vpn vlan-stacking stack-vlan

Parameters

Parameter	Description	Value
stack-vlan *vlan-id*	Indicates the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the following conditions are met, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for a main interface:

- The VLL or VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts packets with one more VLAN tag.
- The local PE is connected to a computer by using a GE interface, XGE interface, 25GE interface, MultiGE interface, 40GE interface, 100GE interface, or Eth-Trunk interface as the AC interface.

  In this scenario, the computer sends and receives all packets. After a VLAN is specified for the main interface, the local PE performs the following operations:
  - The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.
  - The local PE removes the outer VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Precautions

Before binding the main interface to the VLL or VSI, run the **mpls l2vpn vlan-stacking stack-vlan** command to specify a VLAN for the main interface.

To use an XGE interface, a GE interface, a 25GE interface, a MultiGE interface, a 40GE interface, a 100GE interface, or an Eth-Trunk interface of the device as the AC interface of the PE, run the **undo portswitch** command to change a Layer 2 interface to a Layer 3 interface.

Example

Configure MPLS VLL on the main interface and add VLAN tag 80 to incoming packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/13
[HUAWEI-GigabitEthernet0/0/13] undo portswitch
[HUAWEI-GigabitEthernet0/0/13] mpls l2vpn vlan-stacking stack-vlan 80
[HUAWEI-GigabitEthernet0/0/13] mpls l2vc 10.0.0.17 20 tagged
```

10.7.69 mpls l2vpn vsi-pw limit threshold-alarm

Function

The **mpls l2vpn vsi-pw limit threshold-alarm** command configures the upper and lower alarm thresholds for VPLS VCs.

The **undo mpls l2vpn vsi-pw limit threshold-alarm** command restores the default settings.

By default, the upper and lower alarm thresholds are 80% and 70% respectively.

Format

mpls l2vpn vsi-pw limit threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls l2vpn vsi-pw limit threshold-alarm [**upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*]

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

MPLS-L2VPN view

Default Level

2: Configuration Level

Usage Guidelines

A device supports only a limited number of VPLS VCs. If a device has too many VPLS VCs, the device performance deteriorates. The **mpls l2vpn vsi-pw limit**

threshold-alarm command allows you to flexibly adjust the upper and lower alarm thresholds for VPLS VCs to control VPLS VC usage.

Note that:

- *upper-limit-value* specifies the upper alarm threshold for VPLS VCs. If the proportion of VPLS VCs created to the maximum VPLS VCs allowed reaches this threshold, a VPLS VC threshold-crossing alarm is reported.
- *lower-limit-value* specifies the lower alarm threshold for VPLS VCs. If the proportion of VPLS VCs created to the maximum VPLS VCs allowed falls below this threshold, a VPLS VC threshold-crossing clear alarm is reported.

Example

Configure the upper and lower alarm thresholds for VPLS VCs as 90% and 70% respectively.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] mpls l2vpn vsi-pw limit threshold-alarm upper-limit 90 lower-limit 70
```

10.7.70 mtu (VSI view)

Function

The **mtu** command sets the MTU of a VSI.

The **undo mtu** command restores the default value.

The default MTU of a VSI is 1500.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU of a VSI.	The value is an integer that ranges from 328 to 65535.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MTUs of the same VSI on two PEs are different, the two PEs cannot exchange information or establish a connection. In this case, you can run the **mtu** command to set the MTU of a VSI so that VSIs created on different PEs for the same VPLS have the same MTU.

Prerequisites

The following operations have been performed before this command is used:

- The **pwsignal bgp** command and the **route-distinguisher (VSI-BGP view)** *route-distinguisher* command have been executed for Kompella VPLS.
- The **pwsignal ldp** command and the **vsi-id** *vsi-id* command have been executed for Martini VPLS.
- The **bgp-ad** command and the **vpls-id** *vpls-id* command have been executed for BGP AD VPLS.

Precautions

When configuring MTUs, note that the MTUs of the VSIs created for the same VPLS on different PEs must be the same.

Devices of some manufacturers cannot perform the MTU matching check on the VSI. When the switch interworks with a non-Huawei device in Kompella mode, you need to perform either of the following configurations to ensure that VCs are Up:

- Set the MTU of the VSI on the PE to be consistent with the MTU of the non-Huawei device.
- Run the **mtu-negotiate disable** command to ignore the check on MTU matching.

Example

Set the MTU of the VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 100
[HUAWEI-vsi-company1-ldp] quit
[HUAWEI-vsi-company1] mtu 1600
```

10.7.71 mtu-negotiate disable

Function

The **mtu-negotiate disable** command disables a PE from checking whether the MTUs for the local and remote VSIs match.

The **undo mtu-negotiate disable** command enables a PE to check whether the MTUs for the local and remote VSIs match.

By default, a PE is enabled to check whether the MTUs for the local and remote VSIs match.

Format

mtu-negotiate disable

undo mtu-negotiate disable

Parameters

None

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two PEs that are Huawei and non-Huawei devices use Kompella VPLS to communicate, and their MTUs are different, the VC cannot Up. To resolve this problem, run the **mtu-negotiate disable** command to disable the local PE from checking whether the MTUs for the local and remote VSIs match. Alternatively, run the **mtu** command to change the MTU of the local VSI to be the same as that of the remote VSI.

Precautions

The **mtu-negotiate disable** command and its undo form are valid only for Kompella VPLS.

Example

Disable the device from checking whether the MTUs named **bgp1** for the local and remote VSIs match.

```
<HUAWEI> system-view
[HUAWEI] vsi bgp1
[HUAWEI-vsi-bgp1] pwsignal bgp
[HUAWEI-vsi-bgp1-bgp] mtu-negotiate disable
```

10.7.72 multi-homing-preference

Function

The **multi-homing-preference** command configures the multi-homed priority for a VSI.

The **undo multi-homing-preference** command deletes multi-homed priority for a VSI.

By default, the multi-homed priority for a VSI is 0, which is the lowest priority.

Format

multi-homing-preference *preference-value*

undo multi-homing-preference

Parameters

Parameter	Description	Value
preference-value	Specifies the multi-homed priority of a VSI.	The value is an integer that ranges from 1 to 65535. A large value indicates a high priority.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In CE dual-homed scenarios, run the **multi-homing-preference** command to specify a primary PE and a backup PE.

Prerequisites

The following operations have been performed before this command is used:

1. A VSI has been created and the automatic member discovery mechanism has been configured using the **vsi** *vsi-name* **auto** command.
2. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.
3. The RD has been configured for the VSI using the **route-distinguisher** *route-distinguisher* command.

Precautions

Currently, only Kompella VPLS supports the multi-homed priority for a VSI. In addition, only the dual-homed CE is supported.

If you run the **multi-homing-preference** command for a Kompella VPLS, the configured preference takes effect only after the **bestroute l2vpn-preference vpls** command is run in the BGP-L2VPN-AD address family view.

At present, only one label block can be configured on the VSIs of the two dual-homed PEs. If you want to increase the range, run the **undo site** command to delete the existing site, and then specify a larger range. Only one AC can be configured for the VSIs of the dual-homed PEs.

If the VSIs of two PEs that the dual-homed CE accesses are Up, the PE with higher priority serves as the primary PE, while the PE with lower priority serves as the backup PE. The primary PE is responsible for forwarding the traffic of the CE, while the backup PE is responsible only for checking whether the VSI of the primary PE is Up. After the backup PE is selected, the VSI status of the backup PE turns Down.

If the VSI status of the primary PE turns Down, the primary PE broadcasts Unreach packets. After the backup PE receives the Unreach packets, the backup PE judges that the primary PE is faulty. The backup PE then sends Reach packets to set up a PW with other PEs. The backup PE becomes a primary PE.

If the dual-homed priorities of the two PEs in dual-homed mode are the same, after a session is set up between the PEs, the PEs detect collision. At this time, the VSI of the PE with smaller router ID is Up, while the VSI of the PE with larger router ID is Down.

If a session is set up between PE1 with the priority being "a" and PE2 with the priority being "b", and a is larger than b, the VSI of PE1 is Up and that of PE2 is Down. At this time:

- If the priority of PE1 is changed to "b" (the modification is permitted because PE1 does not have information about remote VCs on PE2), the VSI of PE1 remains Up, while the VSI of PE2 remains Down.
- If the priority of PE2 is changed to "a", the modification is rejected and alarm information is displayed.

After the session turns Down, the PW of the PE with lower priority turns Up. The PW between the two PEs turns Up.

Example

Configure the multi-homed priority of the VSI named **company1** to 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 auto
[HUAWEI-vsi-company1] pwsignal bgp
[HUAWEI-vsi-company1-bgp] route-distinguisher 100:1
[HUAWEI-vsi-company1-bgp] quit
[HUAWEI-vsi-company1] multi-homing-preference 100
```

10.7.73 multicast-suppression cir cbs (VSI view)

Function

The **multicast-suppression cir cbs** command enables the multicast suppression function on the VSI.

The **undo multicast-suppression** command disables the multicast suppression function on the VSI.

By default, the multicast traffic function is disabled on a VSI.

Format

multicast-suppression cir *cir-value* **cbs** *cbs-value*

undo multicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the CIR, that is, the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the CBS, that is, the traffic that can pass instantly, or the depth of the first token bucket.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPLS network, the broadcast, multicast, and unknown unicast packets are transmitted in broadcast mode. If large quantities of multicast packets are on the VPLS network, the device has to make a lot of copies of these multicast packets, which wastes bandwidth and resources, and degrades the performance of the system. You can run the **multicast-suppression cir cbs** command to suppress the multicast traffic in the VSI. The rate of multicast traffic on the VPLS network is limited.

Prerequisites

A VSI has been created using the **vsi** *vsi-name* [**auto** | **static**] command.

Example

Set the CIR to 100 kbit/s and the CBS to 18800 bytes for the multicast traffic that can pass in VSI1.

```
<HUAWEI> system-view
[HUAWEI] vsi VSI1
[HUAWEI-vsi-VSI1] multicast-suppression cir 100 cbs 18800
```

10.7.74 npe-upe mac-withdraw enable

Function

The **npe-upe mac-withdraw enable** command enables an SPE to forward the LDP MAC Withdraw messages received from other SPEs to UPEs.

The **undo npe-upe mac-withdraw enable** command disables an SPE from forwarding the LDP MAC Withdraw messages received from other SPEs to UPEs.

By default, an SPE does not forward the LDP MAC Withdraw messages received from other SPEs to UPEs.

Format

npe-upe mac-withdraw enable

undo npe-upe mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, you need to run the **npe-upe mac-withdraw enable** command to enable an SPE to forward the LDP MAC Withdraw messages received from other SPEs to UPEs.

Prerequisites

LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.

Precautions

The **npe-upe mac-withdraw enable** command is used on SPEs.

- An SPE refers to the network end peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] command to specify an SPE.
- A UPE refers to the user end peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** command to specify a UPE.
- If the local device is not configured with HVPLS, the **npe-upe mac-withdraw enable** command is not required.

Example

Enable the SPE to forward the LDP MAC Withdraw messages received from other SPEs the UPE.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
```

```
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] npe-upe mac-withdraw enable
```

10.7.75 peer (VSI-LDP view)

Function

The **peer** command configures a peer for a VSI.

The **undo peer** command deletes the peer of a VSI.

By default, no peer is configured for a VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] [**upe**] [**ignore-standby-state**]

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the peer. Generally, it is specified as the loopback address of the peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
tnl-policy *policy-name*	Specifies the tunnel policy name of the peer.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
upe	Identifies whether the peer is a client PE, which applies to Hierarchical Virtual Private LAN Service (HVPLS).	-

Parameter	Description	Value
ignore-standby-state	Configures the created PW to ignore the secondary state sent from the peer device.	-

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure Martini VPLS, you need to run the **peer** command to configure a peer for the VSI.

Prerequisites

The VSI ID has been configured before you run this command.

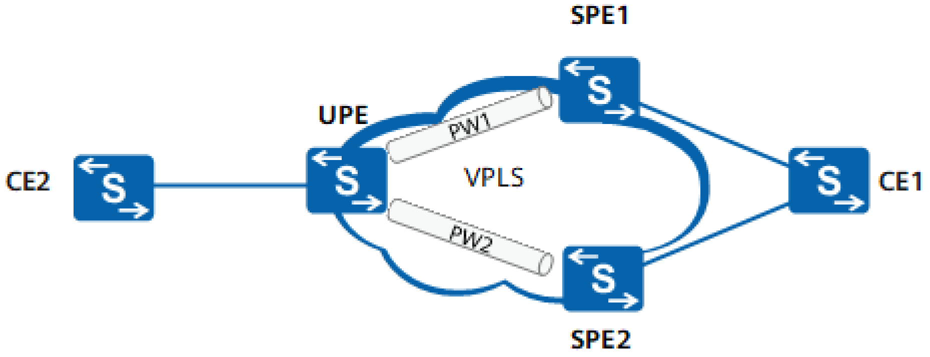
- To configure a Spoke PW on the HVPLS network, you can configure **upe** in the **peer** command. If the specified peer is a UPE, the peer is on the user side, which does not comply with split horizon. If **upe** is not configured, a hub PW is configured, meaning that a VSI peer is specified and the peer is not specified as a UPE. Split horizon applies to hub PWs. Traffic from spoke PWs can be forwarded to spoke PWs and hub PWs, but traffic from hub PWs can only be forwarded to spoke PWs and not to hub PWs.

  NOTE

  Split horizon: The data packets received from the PW on the public network are not forwarded to other PWs, but only forwarded to the private network. On a VPLS network, full mesh and split horizon are used to avoid loops. HVPLS partitions the network, and the devices of different levels forward data to each other without complying with the split horizon scheme.

- To configure a VLL to access a VPLS network, you can adopt one of the following configurations to create a PW:
  - Configure the VSI ID on the VPLS network to be the same as the VC ID of the VLL peer.
  - Configure the value of **negotiation-vc-id** *vc-id* to be the same as the VC ID of the VLL peer.
- The **ignore-standby-state** parameter can be configured for PWs dual-homing a CE to PEs on a PW redundancy network. This setting enables the secondary PW to ignore the Backup state and remain in the Up state, preventing packet loss that occurs during a primary/secondary PW switchover. **Figure 10-2** shows PW redundancy networking with CEs asymmetrically accessing PEs.

Figure 10-2 VPLS PW redundancy networking



If the primary PW1 works properly, it transmits traffic over the path CE1–>SPE1–>UPE–>CE2. If PW1 fails, either of the following situations occurs based on the **ignore-standby-state** setting:

- If **ignore-standby-state** is configured on SPE2, PW2 remains in the Up state. After PW1 fails, SPE2 can forward CE1 traffic over the path CE1–>SPE2–>UPE–>CE2.
- If **ignore-standby-state** is not configured on SPE2, PW2 is in the Backup state before switching to the Up state. After PW1 fails and CE1 sends traffic to SPE2, SPE2 fails to forward traffic to UPE because PW2 does not become Up, causing traffic loss. After PW2 switches to the Up state, SPE2 can forward CE1 traffic over the path CE1–>SPE2–>UPE–>CE2, without traffic loss.

Precautions

After you run the **undo peer** command, all PW configurations created by the peer are deleted.

If the value of **negotiation-vc-id** *vc-id* is different from the value of *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer** command to delete the VSI peer. Otherwise, the system prompts that the VSI peer cannot be deleted.

Example

Configure the peer for the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 10.3.3.3 negotiation-vc-id 10 upe
```

Delete the peer of a VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 10.3.3.3 negotiation-vc-id 10 upe
[HUAWEI-vsi-company1-ldp] undo peer 10.3.3.3 negotiation-vc-id 10
```

10.7.76 peer preference (protect-group view)

Function

The **peer preference** command adds a specified PW to a PW protection group and specifies the priority of the PW.

The **undo peer preference** command deletes a specified PW from a PW protection group.

By default, no PW is added to a PW protection group.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] **preference** *preference-value*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the VSI peer. Generally, the loopback address of the peer is used.	-
negotiation-vc-id *vc-id*	Specifies the parameter negotiated with the peer. By default, the VSI ID is used. Generally, this parameter is used in VPLS accessing VLL scenarios in which the VSI IDs of the two ends are inconsistent and the two ends are required to communicate.	The value is an integer that ranges from 1 to 4294967295.
preference-value	Specifies the priority of a peer when the peer joins a PW protection group. The smaller the value, the higher the priority. Among the two peers added to a PW protection group, the one with the higher priority serves as the primary.	The value is an integer ranging from 1 to 32.

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

After creating a PW protection group and specifying the PW redundancy mode, you can add specified PWs to the group for them to work in backup mode.

Prerequisites

A PW protection group has been created and the PW redundancy mode has been specified.

Precautions

Add PWs to a PW protection group in the descending order of PW priorities. Do not add the PW with a lower priority to the PW protection group first.

If you add the PW with a lower priority to the PW protection group first, a PW switchover will occur after you add the other PW to the PW protection group.

Example

Add a specified PW to a PW protection group and set the priority of the PW to 1.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] peer 2.2.2.2 preference 1
```

10.7.77 peer pw

Function

The **peer pw** creates a PW and displays the PW view.

The **undo peer pw** deletes the created PW.

By default, no PW is created.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*] **pw**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IPv4 address of the peer. Generally, it is specified as the loopback address of the peer.	-

Parameter	Description	Value
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
pw *pw-name*	Specifies the name of a PW. The PW name is used to distinguish the PW from other PWs, and must be unique in the same VSI. Nevertheless, the PW name can be used in other VSIs.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Martini VPLS, you need to run the **peer pw** command to configure a PW after specifying a peer.

Prerequisites

The IP address of the peer has been specified using the **peer** *peer-address* command.

Precautions

If the value of **negotiation-vc-id** *vc-id* is different from the value of *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer pw** command to delete the PW. Otherwise, the PW cannot be deleted.

Example

Create the PW view.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1]
```

Delete the PW.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1] quit
[HUAWEI-vsi-aa-ldp] undo peer 10.1.1.1 pw
```

10.7.78 peer signaling

Function

The **peer signaling** command configures the signaling mode for a specified peer or peer group.

The **undo peer signaling** command restores the default signaling mode of a specified peer or peer group.

By default, after the **peer enable** command is run in the L2VPN AD address family view, the BGP AD signaling is enabled for all peers or peer groups.

Format

peer { *peer-address* | *group-name* } **signaling** { **vpws** | **vpls** | **vpls-ad disable** }

undo peer { *peer-address* | *group-name* } **signaling** { **vpws** | **vpls** | **vpls-ad disable** }

Parameters

Parameter	Description	Value
peer-address	Specifies an IPv4 address of a peer. The loopback address of the peer is usually used as its IPv4 address.	-
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpws	Configures the signaling mode of a specified peer or peer group as VPWS.	-
vpls	Configures the signaling mode of a specified peer or peer group as VPLS.	-
vpls-ad disable	Disables BGP AD signaling for a specified peer or peer group.	-

Views

L2VPN AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Kompella VLL, Kompella VPLS, and BGP AD VPLS scenarios, configure the signaling mode for peers or peer groups in the L2VPN AD address family view so that peers can advertise routes to each other. The parameters used in different scenarios are described as follows:

- In the Kompella VLL scenario, configure **vpws** in the **peer signaling** command.
- In the Kompella VPLS scenario, configure **vpls** in the **peer signaling** command.
- In the BGP AD VPLS scenario, the BGP AD signaling is enabled for all peers or peer groups in the L2VPN AD address family view by default. Therefore, you need to run the **peer** { *peer-address* | *group-name* } **signaling vpls-ad disable** command to disable BGP AD signaling for a specified peer or peer group in Kompella VLL and Kompella VPLS scenarios.

Prerequisites

The **peer enable** command has been run to create a peer or peer group.

Precautions

For the same peer, the **peer enable** and **peer** { *peer-address* | *group-name* } **signaling** { **vpws** | **vpls** | **vpls-ad disable** } commands run in the L2VPN AD address family view are mutually exclusive with the **peer enable** command run in the VPLS address family view.

For the same peer, the **peer** { *peer-address* | *group-name* } **signaling vpws** command run in the L2VPN AD view is mutually exclusive with the **peer enable** command run in the L2VPN address family view.

The signaling mode configured for a peer is preferred over that configured for the peer group to which the peer belongs.

When a signaling mode is configured for a peer group but not configured for a peer that belongs to the peer group, the peer uses the signaling mode configured for its peer group.

Example

Configure the signaling mode for peer 1.1.1.1 in the L2VPN AD address family view when Kompella VPLS is enabled.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
```

```
[HUAWEI-bgp-l2vpn-ad] peer 1.1.1.1 enable
[HUAWEI-bgp-l2vpn-ad] peer 1.1.1.1 signaling vpls
[HUAWEI-bgp-l2vpn-ad] peer 1.1.1.1 signaling vpls-ad disable
```

10.7.79 peer static-npe

Function

The **peer static-npe** command configures the static NPE peer of the VSI in the Hierarchical Virtual Private LAN Service (HVPLS).

The **undo peer static-npe** command deletes the static NPE peer of the VSI in the HVPLS.

By default, the HVPLS has no static NPE peer of the VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **static-npe trans** *transmit-label* **recv** *receive-label*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the static NPE peer. It is generally specified as the loopback address of the peer.	-
negotiation-vc-id *vc-id*	Indicates the unique ID of a VC. Generally, this parameter is used when the VSI IDs of two ends are inconsistent and the two ends are required to communicate.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
tnl-policy *policy-name*	Specifies the tunnel-policy name of the static NPE peer.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
static-npe	Indicates whether the peer of the static VSI is the PE at the network side.	-

Parameter	Description	Value
trans *transmit-label*	Indicates the outer label that is manually configured and sent from the local device to its peer. It is the outgoing label of the static Layer 2 VC.	The value is an integer ranging from 0 to 1048575.
recv *receive-label*	Indicates the outer label that is manually configured and sent from the peer to the local device. It is the incoming label of the static Layer 2 VC.	The value is an integer that ranges from 16 to 1023.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the HVPLS network, you can run the **peer static-npe** command on the local device to configure a static NPE peer.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

If you specify **negotiation-vc-id** *vc-id* when you configure the peer of the VSI, and the specified *vc-id* and that in the configured **vsi-id** command are inconsistent, to delete the peer of the VSI, you must use the **undo peer** command with **negotiation-vc-id** *vc-id*. Otherwise, the peer cannot be deleted.

Example

Configure the static NPE peer of the current VSI. Configure the received and sent outer labels are 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 3.3.3.3 static-npe trans 100 recv 100
```

10.7.80 peer static-upe

Function

The **peer static-upe** command configures the static UPE peer of the VSI in the HVPLS.

The **undo peer static-upe** command deletes the static UPE peer of the VSI in the HVPLS.

By default, the HVPLS has no static UPE peer of the VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **static-upe trans** *transmit-label* **recv** *receive-label*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the UPE peer. Generally, it is specified as the loopback address of the peer.	-
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the IDs of other local VSIs. The negotiated VC IDs to the same peer must be different. The value is an integer ranging from 1 to 4294967295.
tnl-policy *policy-name*	Specifies the tunnel-policy name of the static UPE peer.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
static-upe	Indicates whether the static UPE is a client PE device. This parameter applies to HVPLS.	-
trans *transmit-label*	Specifies the outer label that sent from the local device to its peer.	It is the outgoing label of the static Layer 2 VC. The value is an integer that ranges from 0 to 1048575.

Parameter	Description	Value
recv *receive-label*	Specifies the outer label manually configured and sent from the peer to the local device. It is the incoming label of the static Layer 2 VC.	The value is an integer that ranges from 16 to 1023.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the HVPLS network, you can run the **peer static-upe** command on the local device to configure a static UPE peer.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

If **negotiation-vc-id** *vc-id* is used when configuring the VSI peer, and specified *vc-id* is different from *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer** command to delete the VSI peer. Otherwise, the VSI peer cannot be deleted.

Example

Configure the static UPE peer of the current VSI. The sent and received outer labels are 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
[HUAWEI-vsi-company1-ldp] peer 3.3.3.3 static-upe trans 100 recv 100
```

10.7.81 ping vpls

Function

The **ping vpls** command detects the status of the PW and reachability of the peer.

Format

ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name local-site-id remote-site-id*

ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
-c *echo-number*	Specifies the number of sent Echo Request packets.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the time to wait before sending the next packet.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000 milliseconds.
-s *data-bytes*	Specifies the number of bytes of an Echo Request packet to be sent.	The value is an integer that ranges from 65 to 8100. The default value is 100.
-t *timeout-value*	Specifies the timeout period of sending Echo Request packets.	The value is an integer that ranges from 0 to 65535. The default value is 2000.
-r *reply-mode*	Specifies the mode in which the peer sends MPLS Echo Reply packets. The value is a decimal integer. The values are as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 UDP datagram carrying a router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value ranges from 1 to 4. The default value is 2.
-exp *exp-value*	Specifies the EXP value of an Echo Request packet to be sent.	The value is an integer that ranges from 0 to 7.
-v	Displays detailed information.	-
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Parameter	Description	Value
local-site-id	Specifies the ID of the local CE.	The value is an integer that ranges from 0 to 65534.
remote-site-id	Specifies the ID of the remote CE.	The value is an integer that ranges from 0 to 65534.
peer *peer-address*	Specifies the IP address of the peer PE.	-
negotiate-vc-id *vc-id*	Specifies the ID of the local PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

After VPLS configurations are complete, you can run the **ping vpls** command to check the PW status and reachability of the peer.

- To check the PW status on a Kompella VPLS network, run the following command:

  ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name local-site-id remote-site-id*

  .
- To check the PW status on a Martini or BGP AD VPLS network, run the following command:

  ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

  .

Prerequisites

One of the following operations has been performed before the **ping vpls** command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS

- Configuring BGP AD VPLS

Precautions

The timeout period specified by **-t** is less than the waiting time specified by **-m**.

Note the following points when configuring VPLS:

- If **negotiate-vc-id** is not specified in the **peer** command, *vc-id* is unique and equal to *vsi-id*. To perform the ping operation, you do not need to specify *vc-id* because the VC is unique when **vsi** *vsi-name* and **peer** *peer-address* are specified. In the same case, however, if **negotiate-vc-id** is specified and it is not equal to the actual *vc-id* (that is, *vsi-id*), an error message is displayed.
- If **negotiate-vc-id** (multiple VC IDs can be specified) in the **peer** command, you need to specify **negotiate-vc-id** in addition to **vsi** *vsi-name* and **peer** *peer-address* when performing the ping. If **negotiate-vc-id** is not found or specified, an error message is displayed.

Example

Run the **ping vpls** command on the PE to check connectivity of the VSI named **bgp1** with remote site ID being 10.

```
<HUAWEI> ping vpls -c 10 -m 10 -s 65 -t 100 -v vsi bgp1 10 10
   Reply from 10.2.2.2: bytes=65 Sequence=1 time=2 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=2 time=2 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=3 time=3 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=4 time=2 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=5 time=3 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=6 time=41 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=7 time=4 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=8 time=4 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=9 time=3 ms Return Code 3, Subcode 1
   Reply from 10.2.2.2: bytes=65 Sequence=10 time=6 ms Return Code 3, Subcode 1

 --- FEC: L2 VPN ENDPOINT. Sender VEID = 10, Remote VEID = 10 ping statistics ---
   10 packet(s) transmitted
   10 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 2/7/41 ms
```

Table 10-135 Description of the ping vpls command output

Item	Description
Return Code	Return code. Different values have different meanings: ● 0: indicates that no return code is received. ● 1: indicates that an incorrect request is received. ● 2: indicates that an unknown TLV is received. ● 3: indicates that there is the outbound interface of one LSP. ● 4: indicates that there is no mapping on the response router. ● 5: indicates that the mapping does not match that on the downstream device. ● 6: indicates that an unknown upstream interface exists. ● 7: indicates that the field is reserved. ● 8: indicates label switching. ● 9: indicates label switching without MPLS forwarding. ● 10: indicates mapping without labels. ● 11: indicates the entity without labels. ● 12: indicates that no protocol is loaded on the interface. ● 13: indicates that the ping operation terminates because there is only one label.
Subcode	Subcode, indicating the number of layers of the labels. Usually, the value is 1.

Run the **ping vpls** command on the PE to check the connectivity of a PW in the Martini VPLS.

```
<HUAWEI> ping vpls vsi a2 peer 10.2.2.2
   Reply from 10.2.2.2: bytes=100 Sequence=1 time=3 ms
   Reply from 10.2.2.2: bytes=100 Sequence=2 time=6 ms
   Reply from 10.2.2.2: bytes=100 Sequence=3 time=6 ms
   Reply from 10.2.2.2: bytes=100 Sequence=4 time=6 ms
   Reply from 10.2.2.2: bytes=100 Sequence=5 time=6 ms

  --- FEC: FEC 128 PSEUDOWIRE (NEW). Type = vlan, ID = 10 ping statistics ---
   5 packet(s) transmitted
   5 packet(s) received
   0.00% packet loss
   round-trip min/avg/max = 3/4/6 ms
```

Table 10-136 Description of the ping vpls command output

Item	Description
Reply from x.x.x.x	Response from the destination host to each Echo Request packet: ● bytes: indicates the length of the response packet. ● sequence: indicates the sequence number of the response packet. ● time: indicates the response time, in ms. If no response packet is received after the timeout period, the message "Request time out" is displayed.
FEC: FEC 128 PSEUDOWIRE	Check on FEC 128, namely, check on a Martini VPLS PW.
Type = vlan	VLAN encapsulation on packets.
ID = 10	The VSI ID being 10.

Run the **ping vpls** command on the PE to check the connectivity of a PW in the BGP AD VPLS.

```
<HUAWEI> ping vpls vsi ad peer 10.2.2.2
    Reply from 10.2.2.2: bytes=100 Sequence=1 time=30 ms
    Reply from 10.2.2.2: bytes=100 Sequence=2 time=60 ms
    Reply from 10.2.2.2: bytes=100 Sequence=3 time=60 ms
    Reply from 10.2.2.2: bytes=100 Sequence=4 time=60 ms
    Reply from 10.2.2.2: bytes=100 Sequence=5 time=60 ms

 --- FEC: FEC 129 PSEUDOWIRE. Sender = 1.1.1.1, Remote = 10.2.2.2 ping statisti
cs ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/54/60 ms
```

Table 10-137 Description of the ping vpls command output

Item	Description
Reply from x.x.x.x	Response from the destination host to each Echo Request packet: ● bytes: indicates the length of the response packet. ● sequence: indicates the sequence number of the response packet. ● time: indicates the response time, in ms. If no response packet is received after the timeout period, the message "Request time out" is displayed.
FEC: FEC 129 PSEUDOWIRE	Check on FEC 129, namely, check on a BGP AD VPLS PW.
Sender = x.x.x.x	Address of the sender.

Item	Description
Remote = x.x.x.x	Address of the destination host.

10.7.82 ping vpls mac vsi

Function

The **ping vpls mac vsi** command checks the connectivity of Layer 2 forwarding links on the VPLS network.

Format

ping vpls mac *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id* | **-c** *count* | **-m** *time-value* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *ttl*] *

ping vpls mac *mac-address* **vsi** *vsi-name* **rapid** [**vlan** *vlan-id* | **-c** *count* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *ttl*] *

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the unicast destination MAC address of the VPLS MAC ping, expressed in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The value cannot be a broadcast or multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
vlan *vlan-id*	Specifies the ID of a VLAN	*vlan-id* specifies the VLAN ID, which is an integer that ranges from 1 to 4094.

Parameter	Description	Value
rapid	Indicates that VPLS MAC ping packets are sent in **rapid** mode. This parameter can be used if each response message is not concerned and multiple ping operations need to be performed within a shot period of time. This configuration allows all packets to be sent at the same time, and only summary statistics are displayed.	-
-c *count*	Specifies the number of VPLS MAC Ping Request packets to be sent.	The value ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the time to wait before sending the next VPLS MAC Ping Request packet.	The value ranges from 1 to 10000, in milliseconds. The default value is 2000 ms.
-s *packsize*	Specifies the size of the VPLS MAC Ping Request packet.	The value ranges from 142 to 1442, in bytes. The default value is 142 bytes.
-t *timeout*	Specifies the timeout period for waiting for a Reply packet in response to a VPLS MAC Ping Request packet.	The value ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-exp *exp*	Specifies the priority.	The value ranges from 0 to 7. The default value is 0.
-r *replymode*	Specifies the reply mode, that is, the Reply packet is sent from the control layer or the data layer. Enumerated type.	-
-h *ttl*	Specifies the TTL value of an Echo Request packet to be sent.	The value ranges from 1 to 255. The default value is 30.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Using the **ping vpls mac vsi** command, you can check the connectivity of Layer 2 forwarding links on the VPLS network.

Example

On the VPLS network, check whether the device with the MAC address of 00e0-fc12-3456 is reachable.

```
<HUAWEI> ping vpls mac 00e0-fc12-3456 vsi v123
Ping mac 00e0-fc12-3456 vsi v123 : 100 data bytes , press CTRL_C to break
    Reply from 10.1.1.1 : bytes=100 sequence=1 time = 1ms
    Reply from 10.1.1.1 : bytes=100 sequence=2 time = 1ms
    Reply from 10.1.1.1 : bytes=100 sequence=3 time = 2ms
    Reply from 10.1.1.1 : bytes=100 sequence=4 time = 3ms
    Reply from 10.1.1.1 : bytes=100 sequence=5 time = 2ms
    The IP address of the PE is 5.5.5.5 and the interface on the PE is GigabitEthernet0/0/1.

  --- vsi : v123 00e0-5952-6f01 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/2/3 ms
```

10.7.83 ping vpls multicast

Function

The **ping vpls multicast** command starts an MFIB ping test with a specified VSI in the VPLS domain.

Format

ping vpls multicast vsi *vsi-name* [**-a** *source-ip-address* | **-c** *count* | **-s** *packetsize* | **-t** *timeout* | **-m** *interval* | **-r** *replymode* | **-exp** *exp* | **-v**] * *dest-ip-address*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is an existing VSI.
-a *source-ip-address*	Specifies the multicast source IP address. By default, the multicast source IP address is the IP address of the initiator. The value is in dotted decimal notation.	-

Parameter	Description	Value
-c *count*	Specifies the number of Echo Request packets to be sent.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-s *packetsize*	Specifies the length of the payload in the Echo Request packet, which should be smaller than the MTU value.	The value ranges from 100 to 1442, in bytes. The default value is 100.
-t *timeout*	Specifies the timeout period for waiting for an Echo Reply packet.	The value ranges from 0 to 65535, in milliseconds. The default value is 2000 milliseconds.
-m *interval*	Specifies the time to wait before sending the next Echo Request packet.	The value ranges from 1 to 10000, in milliseconds. The default value is 2000 milliseconds.
-r *replymode*	Specifies the reply mode. The default value is 2. ● 1: indicates that the peer end does not respond to Echo Request packets. ● 2: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets carrying the Router Alert option. ● 4: indicates that the peer end responds to Echo Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to Echo Request packets with VPLS IPv4 UDP packets. **NOTE** Currently, the switch only supports mode 1, 2, and 5.	-

Parameter	Description	Value
-exp *exp*	Specifies the priority of Echo Request packets to be sent.	The value is an integer that ranges from 0 to 7. The default value is 0.
-v	Specifies the displayed details.	-
dest-ip-address	Specifies the multicast IP address.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **ping vpls multicast** command, you can start an MFIB ping test with a specified VSI in the VPLS domain and obtain information about the egress that is in the VPLS domain and can normally receive specified IP multicast packets. In addition, you can check whether the IGMP snooping function is normal.

Precautions

- To check whether the IGMP snooping function is normal, enable IGMP snooping of the VSI to trigger the exchange of IGMP Query packets and Report packets between the multicast source and receiver and specify a non-reserved multicast address as the destination address to initiate the VPLS multicast ping.
- The **ping vpls multicast** command does not support BGP AD VPLS.

After receiving a VPLS multicast Ping packet, the egress in the VPLS domain sends a Reply packet to the sender. The sender can determine the connectivity of the egress and the round trip delay according to the received Reply packet.

You can check the IGMP snooping function in the following scenarios:

- If IGMP snooping is enabled on a PE and the **ping vpls multicast** command run on the PE contains the **-v** parameter, the MPLS Echo packet received by the initiator carries information about interfaces at the AC side of the PE. If the initiator does not receive the Echo Reply packet of the PE, it considers the IGMP snooping function faulty.
- If a certain PE is not enabled with the IGMP snooping function, the Echo Reply packet received by the initiator does not carry information about interfaces at the AC side of the PE.

Example

Initiate an MFIB ping test with a specified VSI in the VPLS domain.

```
<HUAWEI> ping vpls multicast vsi aaa -a 11.11.11.1 -c 2 -v 225.0.0.1
ping 225.0.0.1 : 56 data bytes , press CTRL-C to break

Seq Node-id Path Size RTT
--------------------------------------------------------------------------------
[Send request Seq. 1.]
1 51.51.51.51: ge0/0/1 Self 100 0ms
1 52.52.52.52: ge0/0/2 In-Band 100 20ms
1 54.54.54.54: ge0/0/2 In-Band 100 10ms

[Send request Seq. 2.]
2 51.51.51.51: ge0/0/1 Self 100 0ms
2 52.52.52.52: ge0/0/2In-Band 100 10ms
2 54.54.54.54: ge0/0/2 In-Band 100 20ms
--------------------------------------------------------------------------------
--225.0.0.1 ping statistics--
2 packets transmitted
4 packets received
round-trip min/avg/max = 10/15/20 ms
```

Table 10-138 Description of the ping vpls multicast command output

Item	Description
Seq	Sequence number of the packet.
Node-id	Response address, which carries the port number if it contains forwarding information about the AC side.
Path	Path. ● Self: indicates that packets are sent from the local end (AC side). ● In-Band: indicates that packets are sent from the data link layer (PW side).
Size	Size of the packet.
RTT	Round trip time.

10.7.84 ping vpn-config

Function

The **ping vpn-config** command checks whether configurations on both ends of a VPN are consistent, which can help you locate faults on the VPN connection.

Format

ping vpn-config peer-address *peer-address* **vsi-name** *vsi-name* [**pw-id** *pw-id*] [**local**] [**remote**]

Parameters

Parameter	Description	Value
peer-address *peer-address*	Specifies the IP address of the peer PE.	-
vsi-name *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is an existing VSI.
pw-id *pw-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295. This parameter cannot be specified in the BGP AD VPLS networking.
local	Indicates that the Request packet is encapsulated in LSP mode.	-
remote	Indicates that the Reply packet is encapsulated in LSP mode.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **ping vpn-config** command, you can check whether configurations on both ends of a VPN are consistent, which can help you locate faults on the VPN connection.

The **ping vpn-config** command is used to send a Request packet from the local PE to the peer PE to obtain VPN configurations of the peer PE, such as the VSI name, status, PW type, MTU value, and number of CEs. After the local PE receives the VPN configuration of the peer PE, it displays the information on the local. This can help you locate the fault on the VPN.

Precautions

The **ping vpn-config** command is applied to VPLS networks, dynamic PWE3 networks, and VLL accessing the VPLS networks.

NOTE

The timeout period of the **ping vpn-config** command is 10 seconds.

Example

Run the **ping vpn-config** command to ping the peer PE in Martini VPLS networking.

```
<HUAWEI> ping vpn-config peer-address 3.3.3.9 vsi-name a2
VPN-CONFIG PING: Press CTRL_C to break.
Result Detail: Request Sent - Reply Received
Local VPN description:
Remote VPN description:
PW State: Up
                    local           remote
-----------------------------------------------
VPN Type:           Martini VPLS     Martini VPLS
VSI Name:           a2               a2
VSI ID:             2                2
Admin State:        Up               Up
Oper State:         Up               Up
MTU:                1500             1500
CE Count:           1                1
Control Word:       N/A              N/A
Primary Or Secondary: N/A            N/A

Actual IP Addr:     1.1.1.9          3.3.3.9
Expected Peer IP:   3.3.3.9          1.1.1.9
SPE:                NO               NO

PW-ID:              2                2
VC-Type:            vlan             vlan
Egress Label:       1025             1026
Ingress Label:      1026             1025

LSP Tunnel Used:    NO               NO
```

Perform a service ping operation with the destination address being 3.3.3.9 in BGP AD VPLS networking.

```
<HUAWEI> ping vpn-config peer-address 3.3.3.9 vsi-name vplsad1
VPN-CONFIG PING: Press CTRL_C to break.
Result Detail: Request Sent - Reply Received
Local VPN description:
Remote VPN description:
PW State: Up
                    local                remote
---------------------------------------------------------------
VPN Type:           BGPAD VPLS            BGPAD VPLS
VSI Name:           vplsad1               vplsad1
Admin State:        Up                    Up
Oper State:         Up                    Up
MTU:                1500                  1500
CE Count:           1                     1

Actual IP Addr:     1.1.1.9               3.3.3.9
Expected Peer IP:   3.3.3.9               1.1.1.9
SPE:                NO                    NO

VC-Type:            vlan                  vlan
Egress Label:       1026                  1027
Ingress Label:      1027                  1026

VPLS ID:            168.1.1.1:1           168.1.1.1:1
RD:                 168.1.1.1:1           168.1.1.1:1
Import VPN target:  100:1                 100:1
Export VPN target:  100:1                 100:1

LSP Tunnel Used:    NO                    NO
```

Table 10-139 Description of the ping vpn-config command output

Item	Description
Result details	Details of the command operation result.
Local VPN description	Description of the local VPN. To set the value, run the **description** command.
Remote VPN description	Description of the peer VPN.
PW State	Status of a PW.
Local	Configuration of the local PE.
Remote	Configuration of the remote PE.
VPN Type	Type of a VPN.
VSI Name	Name of a VSI.
VSI ID	ID of a VSI. To set the value, run the **vsi-id** command.
Admin State	VSI administration status.
Oper State	VSI operating status.
MTU	MTU of the VSI. In PWE3 networking, it refers to the MTU of an AC interface; in VPLS networking, it refers to the MTU of a VSI.
CE Count	Number of AC links.
Control Word	Whether the control word is enabled: ● Enable ● Disable
Primary Or Secondary	Displayed as a PW on the local end and always displayed as N/A on the remote end.
Actual IP Addr	Actual IP address.
Expect IP Addr	Expected IP address.
SPE	Whether it is a SPE
PW ID	ID of a PW.
VC-Type	Encapsulation type of the VC. ● Ethernet: indicates that the encapsulation type of the VC is Ethernet. ● VLAN: indicates that the encapsulation type of the VC is VLAN.
Egress Label	Outgoing label.

Item	Description
Ingress Label	Incoming label.
VPLS ID	VPLS ID To set the value, run the **vpls-id** command.
RD	Route tag. To set the value, run the **route-distinguisher** command.
Import VPN target	Import VPN target.
Export VPN target	Export VPN target.
LSP Tunnel Used	Whether the packet is encapsulated in LSP mode.

10.7.85 protect-group (VSI-LDP view)

Function

The **protect-group** command creates a PW protection group. If the PW protection group to be created already exists, the PW protection group view is displayed.

The **undo protect-group** command deletes a specified PW protection group.

By default, no PW protection group is created in a VSI.

Format

protect-group *group-name*

undo protect-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a PW protection group.	The value is a string of 1 to 15 case-sensitive characters without spaces or hyphens (-). When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

Multiple PWs can be created in a VSI.

You can create multiple PW protection groups for a VSI. After you add two PWs to a PW protection group, the two PWs will work in backup mode.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Follow-up Procedure

After creating PW protection groups, configure the PW redundancy mode of each PW protection group, add PWs to these groups, and configure revertive switching policies for these groups.

Example

Create a PW protection group named group1.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] vsi-id 10
[HUAWEI-vsi-vsi1-ldp] protect-group group1
```

10.7.86 protect-mode (protect-group view)

Function

The **protect-mode** command specifies the PW redundancy mode of a PW protection group.

The **undo protect-mode** command cancels the PW redundancy mode of a PW protection group.

By default, a PW protection group does not have a PW redundancy mode.

Format

protect-mode pw-redundancy master

undo protect-mode

Parameters

Parameter	Description	Value
pw-redundancy master	Specifies the PW redundancy mode of a PW protection group as master/slave.	-

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

You can configure PW protection groups to protect PW pairs of a VSI.

In the scenarios, in which the active/standby PWs cannot be determined based on the signaling sent by the remote end, you can create a PW protection group on the UPE, and specify the PW redundancy mode of the group as master/slave. The local UPE determines the active/standby PWs based on the priorities configured using the **peer preference** command.

NOTE

When the mode of the group is master/slave, the local UPE does not determine the active/standby PWs based on the signaling sent by the remote end.

Prerequisites

The PW protection group has been configured using the **protect-group** command.

Precautions

A static hub PW and a static spoke PW cannot be added to the same protection group.

After a PW protection group is configured, you must specify the PW redundancy mode before configuring other parameters. Deleting the PW redundancy mode of a PW protection group will clear all the configurations of the group.

Example

Configure the PW redundancy mode of a PW protection group as PW redundancy master/slave.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] protect-mode pw-redundancy master
```

10.7.87 protect-switch (protect-group view)

Function

The **protect-switch** command triggers a manual protection switchover or cancels the manual switchover in a protection group.

Format

protect-switch { **manual** | **clear** }

Parameters

Parameter	Description	Value
manual	Forcibly performs a PW switchover to switch traffic from the high-priority primary PW to the low-priority backup PW.	-
clear	Cancels the **manual** PW switchover to switch traffic from the low-priority backup PW back to the high-priority primary PW.	-

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

If you want to maintain the device where the primary PW in a PW protection group resides, you must use a command to switch traffic from the primary PW to the secondary PW first. After the device where the primary PW resides is stable, you need to use this command to switch traffic back from the secondary PW to the primary PW.

Prerequisites

A PW protection group has been created and the PW redundancy mode is master/slave. The primary and secondary PWs have joined the PW protection group and their status is Up.

Precautions

After you run the **protect-switch manual** command, traffic switches from the primary PW to the secondary PW. After you run the **protect-switch clear** command, traffic switches from the secondary PW to the primary PW.

After you run the **protect-switch manual** command, service traffic is always transmitted over the low-priority backup PW. To enable service traffic to be transmitted over a high-priority PW, run the **protect-switch clear** command to cancel the manual switchover. The manual switchover is also cancelled when the priorities of the primary and backup PWs change in some situations, for example, a PW is Down or you change their priority values. In these situations, the system selects the PW with a higher priority to transmit service traffic.

Example

Forcibly perform an active/standby PW switchover in the current PW protection group.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] protect-switch manual
```

10.7.88 pw

Function

The **pw** command displays the PW view.

The **undo pw** command deletes the PW view.

By default, the PW view is not displayed.

Format

pw *pw-name*

undo pw *pw-name*

Parameters

Parameter	Description	Value
pw-name	Specifies the name of a PW.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PW is created, you can run the **pw** *pw-name* command to enter the PW view.

Prerequisites

A PW has been created using the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command.

Precautions

The PW name must be unique in a VSI, and the PW name can be the same in different VSIs.

Example

Enter the PW view.

```
<HUAWEI> system-view
[HUAWEI] vsi aa static
[HUAWEI-vsi-aa] pwsignal ldp
[HUAWEI-vsi-aa-ldp] vsi-id 1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1
[HUAWEI-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[HUAWEI-vsi-aa-ldp-pw-pw1] quit
[HUAWEI-vsi-aa-ldp] pw pw1
```

10.7.89 pwsignal

Function

The **pwsignal** command configures the signaling mode for a VSI.

By default, no signaling mode is configured for a VSI.

Format

pwsignal { **bgp** | **ldp** }

Parameters

Parameter	Description	Value
bgp	Uses the BGP signing mode.	-
ldp	Uses the LDP signaling mode.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the Martini or Kompella VPLS, you need to run the **pwsignal** command to configure a signaling mode for a VSI.

Precautions

If the member discovery mode of the VSI is static, the signaling mode must be LDP. If the member discovery mode of the VSI is automatic, the signaling mode must be BGP.

After the signaling mode is configured successfully for the VSI, it cannot be modified. If you want to change the signaling mode, you must delete the VSI and re-create VSI.

Example

Configure the signaling mode of the VSI as LDP.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp]
```

Configure the signaling mode of the VSI as BGP.

```
<HUAWEI> system-view
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp]
```

10.7.90 pw spoke-mode (VSI-BGPAD view)

Function

The **pw spoke-mode** command configures all PWs of a BGP AD VSI as spoke PWs.

The **undo pw spoke-mode** command restores the default setting.

By default, all PWs of a BGP AD VSI are hub PWs.

Format

pw spoke-mode

undo pw spoke-mode

Parameters

None

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a BGP AD VPLS needs to be deployed on a network with a star or tree topology (on which one PE that serves as a server or an authorization device is configured as the hub PE, and other PEs are configured as spoke PEs), all PWs of the VSI on the hub PE must be configured as spoke PWs to disable split horizon of the PWs. Traffic from spoke PWs can be forwarded to spoke PWs and hub PWs, but traffic from hub PWs can only be forwarded to spoke PWs and not to hub PWs.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

The **pw spoke-mode** command takes effect on all the PWs of a BGP AD VSI.

After the **pw spoke-mode** command is run, all PWs of the specified VSI become spoke PWs. Split horizon does not function on spoke PWs. This means that packets sent from Spoke PWs can be forwarded to other PWs. If the **undo pw spoke-mode** command is run, all PWs of the VSI will be changed to hub PWs that comply with split horizon rules.

Example

Create a BGP AD VSI named **company1** and configure all the PWs of the VSI as spoke PWs.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 65535:1
[HUAWEI-vsi-company1-bgpad] pw spoke-mode
```

10.7.91 remote-vpn-target refresh

Function

The **remote-vpn-target refresh** command refreshes the remote VPN target manually.

Format

remote-vpn-target refresh

Parameters

None

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

When locating a Kompella VPLS fault, you can use the **remote-vpn-target refresh** command to refresh the remote VPN target manually.

Example

Refresh the remote VPN target.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] remote-vpn-target refresh
```

10.7.92 reroute (protect-group view)

Function

The **reroute** command configures a revertive switching policy for a PW protection group with the master/slave PW redundancy mode.

The **undo reroute** command deletes the revertive switching policy for a PW protection group with the master/slave PW redundancy mode.

The default revertive switching policy for a PW protection group with the master/slave PW redundancy mode is delayed switchback and the default delay is 30s.

Format

reroute { **delay** *delay-time* | **immediately** | **never** }

undo reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies that the revertive switching policy is delayed switchback.	The value is an integer ranging from 10 to 600, in seconds. The default value is 30s.
immediately	Specifies that the revertive switching policy is immediate switchback.	-
never	Specifies that the revertive switching policy is non-revertive. Traffic does not switch back to the primary PW even after the primary PW recovers. Traffic will be switched back to the primary PW only when the secondary PW fails.	-

Views

protect-group view

Default Level

2. Configuration level

Usage Guidelines

Usage Scenario

The **reroute** command can configure revertive switching policies for only PW protection groups with the master/slave PW redundancy mode. The revertive switching policy for PW protection groups with the independent PW redundancy mode is immediate switchback and cannot be modified.

Currently, three types of revertive switching policies are available:

- Delayed switchback: Traffic is switched back to the primary PW after the delay time specified in *delay-time*. After the switchover is performed, the UPE notifies the remote PE on the secondary PW of a fault. On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.
- Immediate switchback: Traffic is immediately switched back to the primary PW. This revertive switching policy applies to scenarios in which users hope traffic to be restored as soon as possible.
- Non-revertive: Traffic will not be switched back to the primary PW even after the primary PW recovers. Traffic will be switched back to the primary PW only when the secondary PW fails. If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive policy.

Prerequisites

The PW redundancy mode of the PW protection group is master/slave.

Precautions

The revertive switching policy determines the switchback behavior of the traffic after the primary PW recovers.

Example

Configure the primary and secondary PWs in a PW protection group to perform a switchback after a delay of 60s.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] reroute delay 60
```

10.7.93 reset bgp l2vpn-ad

Function

The **reset bgp l2vpn-ad** command resets the BGP connections associated with L2VPN-AD.

Format

reset bgp l2vpn-ad { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** } [**graceful**]

Parameters

Parameter	Description	Value
l2vpn-ad	Resets BGP connections associated with L2VPN-AD.	-
all	Resets all the BGP connections.	-
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the connections with a specified BGP peer.	It is in dotted decimal notation.
group *group-name*	Resets the BGP connections with the specified peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Resets all EBGP connections.	-
internal	Resets all IBGP connections.	-
graceful	Specifies to reset BGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

The **reset bgp l2vpn-ad** command is used to make new BGP configurations associated with L2VPN-AD take effect.

⚠ CAUTION

After you run this command, the TCP connection is reset, and the neighbor relationship between two peers is reestablished. So, confirm the action before you use the command.

Example

Reset all BGP L2VPN-AD connections.

```
<HUAWEI> reset bgp l2vpn-ad all
```

10.7.94 reset oam-mac statistics

Function

The **reset oam-mac statistics** command clears the statistics about the number of MAC diagnostic packets.

Format

reset oam-mac statistics { **populate** | **purge** | **purge-register** | **all** }

Parameters

Parameter	Description	Value
populate	Indicates the statistics about the number of populate packets.	-
purge	Indicates the statistics about the number of purge packets.	-
purge-register	Indicates the statistics about the number of purge + register packets.	-
all	Indicates the statistics about the number of MAC diagnostic packets.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Using the **reset oam-mac statistics** command, you can clear the statistics about the number of MAC diagnostic packets.

NOTICE

The statistics about MAC diagnostic packets cannot be restored once they are cleared. Confirm the action before you run the **reset oam-mac statistics** command.

Example

Display the statistics about the number of all MAC diagnostic packets that are received by the device.

```
<HUAWEI> display oam-mac statistics all
 Received populate packet: 3
 Received purge packet: 1
 Received purge register packet: 2
```

Clear the statistics about the number of MAC diagnostic packets that are received by the device.

```
<HUAWEI> reset oam-mac statistics all
```

Display the statistics about the number of MAC diagnostic packets that are received by the device. It is found that all the statistics are cleared.

```
<HUAWEI> display oam-mac statistics all
 Received populate packet: 0
 Received purge packet: 0
 Received purge register packet: 0
```

10.7.95 reset vpls multicast-ping statistics

Function

The **reset vpls multicast-ping statistics** command clears the statistics on the number of MFIB Ping packets.

Format

reset vpls multicast-ping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the statistics on the number of sent and received MFIB Ping packets.

Example

Reset the statistics on the number of MFIB Ping packets.

```
<HUAWEI> reset vpls multicast-ping statistics
```

10.7.96 reset vpls multicast-trace statistics

Function

The **reset vpls multicast-trace statistics** command clears the statistics on the number of MFIB Trace packets.

Format

reset vpls multicast-trace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the statistics on the number of sent and received MFIB Trace packets.

Example

Reset the statistics on the number of MFIB Trace packets.

```
<HUAWEI> reset vpls multicast-trace statistics
```

10.7.97 reset vpls-ping statistics

Function

The **reset vpls-ping statistics** command clears the statistics about the number of VPLS MAC Ping packets.

Format

reset vpls-ping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset vpls-ping statistics** command clears the statistics about the number of sent and received VPLS MAC Ping packets.

Example

Clear the statistics about the number of VPLS MAC Ping packets.

```
<HUAWEI> reset vpls-ping statistics
```

10.7.98 reset vpls-trace statistics

Function

The **reset vpls-trace statistics** command clears the statistics about the number of VPLS MAC Trace packets.

Format

reset vpls-trace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset vpls-trace statistics** command clears the statistics about the number of sent and received VPLS MAC Trace packets.

Example

Clear the statistics about the number of VPLS MAC Trace packets.

```
<HUAWEI> reset vpls-trace statistics
```

10.7.99 reset traffic-statistics vsi all

Function

The **reset traffic-statistics vsi all** command clears the statistics about all VPLS PW traffic.

Format

reset traffic-statistics vsi all

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When the **reset traffic-statistics vsi all** command is run successfully, confirm whether to proceed with the operation. If yes, enter **Y**. If no, enter **N**.

Example

Reset the statistics about all VPLS PW traffic in the user view.

```
<HUAWEI> reset traffic-statistics vsi all
Warning:Traffic-statistics information will be cleared! Continue? [Y/N]:Y
```

10.7.100 reset traffic-statistics vsi name

Function

The **reset traffic-statistics vsi name** command clears the statistics about the public traffic on all VPLS PWs in the specified VSI.

Format

reset traffic-statistics vsi name *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the VPLS configuration is complete, you can run the **display traffic-statistics vsi** command to view statistics about all PW traffic in the VSI. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name** command to clear the previous statistics.

Precautions

The **reset traffic-statistics vsi name** command is valid only in Martini VPLS.

After you run this command, statistics about all VPLS PW traffic in the VSI are cleared.

Example

Clear the statistics about all VPLS PW traffic in the specified VSI in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi
```

10.7.101 reset traffic-statistics vsi name peer

Function

The **reset traffic-statistics vsi name peer** command clears the statistics about public traffic of the PW in the specified VPLS VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the VPLS configuration is complete, you can run the **display traffic-statistics vsi peer** command to view statistics about the traffic of the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer** command to clear the previous statistics.

Precautions

The **reset traffic-statistics vsi name peer** command is valid only in Martini VPLS.

After you run this command, statistics about the traffic on the corresponding VPLS PW are cleared.

Example

Clear the statistics about the traffic on the VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.1.1.1
```

10.7.102 reset traffic-statistics vsi name peer ldp129

Function

The **reset traffic-statistics vsi name peer ldp129** command clears the statistics about the public traffic on the BGP AD VPLS PW in the specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* **ldp129**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the BGP AD VPLS configuration is complete, you can run the **display traffic-statistics vsi peer ldp129** command to view statistics about the PW traffic. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer ldp129** command to clear the previous statistics.

Prerequisites

The traffic statistics function has been enabled using the **traffic-statistics enable (VSI-BGPAD view)** command or the **traffic-statistics peer enable (VSI-BGPAD)** command in the VSI-BGPAD view.

Precautions

The **reset traffic-statistics vsi name peer ldp129** command is valid only in BGP AD VPLS.

After you run the **reset traffic-statistics vsi name peer ldp129** command, statistics about the traffic on the corresponding BGP AD VPLS PW are cleared.

Example

Clear the statistics about the traffic on the specified BGP AD VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.1.1.1 ldp129
```

10.7.103 reset traffic-statistics vsi name peer negotiation-vc-id

Function

The **reset traffic-statistics vsi name peer negotiation-vc-id** command clears the statistics about the public traffic on the Martini VPLS PW in a specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* **negotiation-vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-
negotiation-vc-id *vc-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS configuration is complete, you can run the **display traffic-statistics vsi peer negotiation-vc-id** command to view the statistics about the traffic on the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer negotiation-vc-id** command to clear the previous statistics.

Precautions

The **reset traffic-statistics vsi name peer negotiation-vc-id** command is valid only in Martini VPLS.

After you run the **reset traffic-statistics vsi name peer negotiation-vc-id** command, statistics about the traffic on the corresponding Martini VPLS PW are cleared.

Example

Reset the statistics about the traffic on the Martini VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.22.33.20 negotiation-vc-id 2
```

10.7.104 reset traffic-statistics vsi name peer remote-site

Function

The **reset traffic-statistics vsi name peer remote-site** command clears the statistics about the public traffic on the Kompella VPLS PW in the specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* **remote-site** *site-id*

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Kompella VPLS configuration is complete, you can run the **display traffic-statistics vsi peer remote-site** command to view the statistics about the traffic on the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer remote-site** command to clear the previous statistics.

Prerequisites

The traffic statistics function has been enabled using the **traffic-statistics peer remote-site enable (Kompella)** command in the VSI-BGP view.

Precautions

The **reset traffic-statistics vsi name peer remote-site** command is valid only in Kompella VPLS.

After you run the **reset traffic-statistics vsi name peer remote-site** command, statistics about the traffic on the corresponding Kompella VPLS PW are cleared.

Example

Reset the statistics about the traffic on the Kompella VPLS PW in the user view.

```
<HUAWEI> reset traffic-statistics vsi name newvsi peer 10.22.33.20 remote-site 2
```

10.7.105 route-distinguisher (VSI-BGP view)

Function

The **route-distinguisher** command configures an RD for a VSI.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD, which identifies a VSI on a PE.	The formats of an RD are as follows: ● 16-bit AS number:32-bit user-defined number: for example, 101:3. An AS number ranges from 0 to 65535, and a user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. That is, a VPLS ID cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPLS ID cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-

Parameter	Description	Value
		defined number cannot be both 0s. That is, a VPLS ID cannot be 0.0:0. - 32-bit IP address:16-bit user-defined number: for example, 192.168.122.15:1. An IPv4 address ranges from 0.0.0.0 to 255.255.255.255, and a user-defined number ranges from 0 to 65535.

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VSI in the Kompella VPLS and use the BGP as the PW signaling protocol, run the **route-distinguisher** command to configure the RD. Other parameters can be configured only after the RD is configured.

Prerequisites

The following operations have been performed before this command is used:

1. A VSI has been created using the **vsi** *vsi-name* [**auto**] command.
2. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.

Precautions

On the same PE, different VSIs have different RDs. The IDs of the same VSIs on different PEs can be either the same or different.

The RD does not have a default value. After an RD is configured successfully for the VSI, it cannot be modified. If you want to modify the RD, you need to delete the VSI and re-create a VSI.

Kompella VLL and Kompella VPLS must use different RDs.

Example

Configure an RD in the format of "16-bit ASN:32-bit user-defined number" for the VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 auto
[HUAWEI-vsi-company1] pwsignal bgp
[HUAWEI-vsi-company1-bgp] route-distinguisher 101:3
```

Configure an RD in the format of "32-bit IP address:16-bit user-defined number" for the VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 2.2.2.2:1
```

Configure an RD in the format of "4-byte AS number in dotted notation:2-byte user-defined number" for the VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 22.22:22
```

10.7.106 shutdown (VSI view)

Function

The **shutdown** command disables a VSI.

The **undo shutdown** command enables a VSI.

By default, a VSI is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For service management such as service debugging or service halting, you can disable a VSI temporarily, and add, cancel, or adjust VSI functions.

Pre-configuration Tasks

Before a VSI is disabled, the PW-Signal must be configured.

Precautions

The **shutdown** command mainly affects PW connections of a VSI. After the command is run, the AC is Down and the Layer 2 forwarding table is deleted.

Example

Disable the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] shutdown
```

Enable the current VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] undo shutdown
```

10.7.107 signaling

Function

The **signaling** command configures the signaling mode for all peers or peer groups.

The **undo signaling** command restores the default signaling mode of all peers or peer groups.

By default, after the **peer enable** is run in the L2VPN AD address family view, the BGP AD signaling is enabled for all peers or peer groups.

Format

signaling { **vpws** | **vpls** | **vpls-ad disable** }

undo signaling { **vpws** | **vpls** | **vpls-ad disable** }

Parameters

Parameter	Description	Value
vpws	Configures the signaling mode of all peers or peer groups as VPWS.	-
vpls	Configures the signaling mode of all peers or peer groups as VPLS.	-
vpls-ad disable	Disables BGP AD signaling for all peers or peer groups.	-

Views

L2VPN AD address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Kompella VLL, Kompella VPLS, and BGP AD VPLS scenarios, configure the signaling mode for peers or peer groups in the L2VPN AD address family view so that peers can advertise routes to each other. The parameters used in different scenarios are described as follows:

In the Kompella VLL scenario, configure **vpws** in the **signaling** command.

In the Kompella VPLS scenario, configure **vpls** in the **signaling** command.

In the BGP AD VPLS scenario, the BGP AD signaling is enabled for all peers or peer groups in the L2VPN AD address family view by default. Therefore, you need to run the **signaling vpls-ad disable** command to disable the BGP AD signaling for all peers or peer groups in Kompella VLL and Kompella VPLS scenarios.

Prerequisites

The **peer enable** command has been run to establish peers or peer groups.

Precautions

The signaling mode configured for a peer is preferred over that configured for the peer group to which the peer belongs. The signaling mode configured for a peer group is preferred over that configured by running the **signaling** command.

When a signaling mode is not configured for a peer or its peer group, the peer and peer group use the signaling mode configured by running the **signaling** command.

Example

Configure the signaling mode for all peers or peer groups in the L2VPN AD address family view when Kompella VPLS is enabled.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-ad-family
[HUAWEI-bgp-l2vpn-ad] signaling vpls
[HUAWEI-bgp-l2vpn-ad] signaling vpls-ad disable
```

10.7.108 site

Function

The **site** command configures a site ID for a VSI.

The **undo site** command deletes a site ID of a VSI.

By default, no site ID is configured for the VSI.

Format

site *site-id* [**range** *site-range*] [**default-offset** { **0** | **1** }]

undo site *site-id*

Parameters

Parameter	Description	Value
site-id	Specifies the site ID of a VSI.	The value is an integer that ranges from 0 to 65534.
range *site-range*	Specifies the range of the number of sites in the VSI. If this parameter is specified, the system reserves the required labels for the VSI.	The value is an integer that ranges from 1 to 8000.
default-offset	Specifies the offset of the initial site ID.	The value is an integer. It can be 0 or 1. The default value is 0.

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure an RD for the VSI in the Kompella VPLS, run the **site** command to configure site connections.

Prerequisites

The following operations have been performed before this command is used:

1. A VSI has been created using the **vsi** *vsi-name* **auto** command.
2. BGP has been configured as the PW signaling protocol using the **pwsignal bgp** command.
3. The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command.

Precautions

The same VSI on different PEs cannot be configured with the same site ID. *site-id* of the local end must be less than the sum of *site-range* and **default-offset** of the remote end. *site-id* of the local end cannot be less than **default-offset** of the remote end.

A device allocates labels to the ranges of Kompella L2VPN instances and VPLS VSIs from the same label block. Therefore, the ranges of Kompella L2VPN instances and VPLS VSIs cannot be greater than the size of the label block. Otherwise, the system prompts that the required labels exceed the permitted maximum labels, and the labels cannot be allocated. The system fails to create a CE or fails to allocate a site ID to a VSI.

Example

Configure the site ID of the VSI as 1 and the number of connected sites in this VSI as 100.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 10.1.1.1:1
[HUAWEI-vsi-company2-bgp] site 1 range 100
```

10.7.109 stream-dual-receiving

Function

The **stream-dual-receiving** command enables the secondary PW to receive and forward traffic from the peer.

The **undo stream-dual-receiving** command disables the secondary PW from receiving and forwarding traffic from the peer.

By default, the secondary PW does not receive traffic from the peer.

Format

stream-dual-receiving

undo stream-dual-receiving

Parameters

None

Views

protect-group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is unstable or a faulty occurs on the device, traffic may switch between the primary and secondary PW. In this case, you need to run the **stream-dual-receiving** command to enable the secondary PW to receive and forward traffic from the peer. This reduces number of packets lost during switching.

Prerequisites

The master/slave mode has been configured as the PW redundancy mode.

Configuration Impact

The secondary PW can forward data but does not forward data before traffic is switched from the primary PW to the secondary PW.

Example

Enable the secondary PW to receive and forward traffic from the peer.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] protect-group group1
[HUAWEI-vsi-vsi1-ldp-protect-group-group1] stream-dual-receiving
```

10.7.110 tnl-policy (VSI view)

Function

The **tnl-policy** command sets a tunnel policy for a VSI.

The **undo tnl-policy** command deletes the tunnel policy of a VSI.

By default, no tunnel policy is applied to a VSI.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the policy name of a tunnel.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the VPLS to use tunnels for packet exchange, run the **tnl-policy** command.

Prerequisites

One of the following operations has been performed before this command is used:

- The **pwsignal bgp** command and the **route-distinguisher** *route-distinguisher* command have been executed for Kompella VPLS.
- The **pwsignal ldp** command and the **vsi-id** *vsi-id* command have been executed for Martini VPLS.
- The **bgp-ad** command and the **vpls-id** *vpls-id* command have been executed for BGP AD VPLS.

Precautions

After the **tnl-policy** command is executed, the configured tunnel policy determines which tunnel between PE devices is preferred to forward traffic and whether load balancing is used. When creating a tunnel policy, specify the sequence of selecting tunnels. If no tunnel policy is configured, the default tunnel policy is used. That is, only LSP tunnels are selected and no load balancing is performed.

Example

Configure the tunnel policy name for the VSI.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 100
[HUAWEI-vsi-company1-ldp] quit
[HUAWEI-vsi-company1] tnl-policy tnlpolicyofcompany1
```

10.7.111 track hub-pw (VSI-LDP-PW view)

Function

The **track hub-pw** associates spoke PW status with hub PW status.

The **undo track hub-pw** deletes the association between spoke PW status and hub PW status.

By default, spoke PW status is not associated with hub PW status.

Format

track hub-pw

undo track hub-pw

Parameters

None

Views

VSI-LDP-PW view

Default Level

2. Configuration level

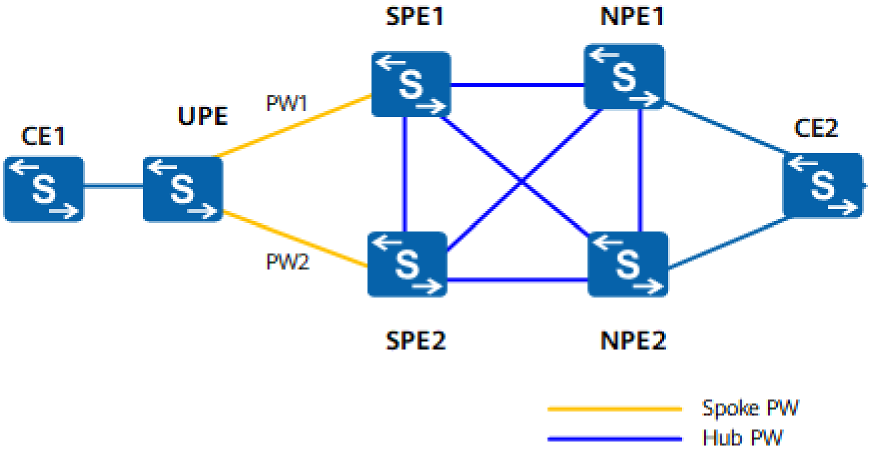
Usage Guidelines

Usage Scenario

Figure 10-3 shows a VPLS PW redundancy scenario. The UPE connects to SPE1 over PW1, a primary PW, and connects to SPE2 over PW2, a secondary PW. PW1 and PW2 work in backup mode. SPEs and NPEs are connected using hub PWs.

Under normal circumstances, if all hub PWs connected to SPE1 go Down but PW1 is Up, the upstream traffic still travels along the primary PW, PW1. As a result, traffic gets lost. To prevent traffic loss, you can run the **track hub-pw** command on SPE1 to associate spoke PW status with hub PW status. After the **track hub-pw** command is configured, SPE1 notifies the UPE of switching traffic to the secondary PW for transmission after detecting that all connected hub PWs go Down.

Figure 10-3 VPLS PW redundancy networking



Prerequisites

The **track hub-pw** command takes effect only if the following conditions are met:

- This command can only be used for a spoke PW to track the status of hub PWs. The **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** must have been run to create a spoke PW.
- The **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command must have been run to display the PW view. This is because the **track hub-pw** command can only be run in the VSI-LDP-PW view.

Example

Enable the association between spoke PW status and hub PW status.

```
<HUAWEI> system-view
[HUAWEI] vsi vsi1
[HUAWEI-vsi-vsi1] pwsignal ldp
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2 upe
```

```
[HUAWEI-vsi-vsi1-ldp] peer 2.2.2.2 pw 1
[HUAWEI-vsi-vsi1-ldp-pw-1] track hub-pw
```

10.7.112 traffic-statistics enable (VSI-LDP view)

Function

The **traffic-statistics enable** command enables the statistics about the public traffic on all Martini VPLS PWs.

The **undo traffic-statistics enable** command disables the statistics about the public traffic on all Martini VPLS PWs.

By default, the statistics function is disabled.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **traffic-statistics enable** command to enable statistics about the traffic on all PWs.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Precautions

After this command is executed and the statistics reach the upper limit, a peer can still be configured, but the traffic statistics function does not take effect on this peer. When the configuration needs to be restored after the system is restarted, configured the peer first. If the statistics exceed the upper limit after the **traffic-statistics enable** is executed, the configuration cannot be restored.

The **traffic-statistics enable** command cannot be used together with the **traffic-statistics peer enable (Martini)** command in the VSI-LDP view.

Example

Enable the statistics on all PWs in the VSI 1.

```
<HUAWEI> system-view
[HUAWEI] vsi 1
[HUAWEI-vsi-1] pwsignal ldp
[HUAWEI-vsi-1-ldp] traffic-statistics enable
```

10.7.113 traffic-statistics enable (VSI-BGPAD view)

Function

The **traffic-statistics enable** command enables the statistics about the public traffic on all BGP AD VPLS PWs.

The **undo traffic-statistics enable** command disables the statistics about the public traffic on all BGP AD VPLS PWs.

By default, the statistics function is disabled.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the BGP AD VPLS network is configured, you can run the **traffic-statistics enable** command to enable statistics about the public traffic on all BGP AD VPLS PWs in the corresponding VSI.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

The **traffic-statistics enable** command cannot be used together with the **traffic-statistics peer enable (VSI-BGPAD)** command in the VSI-BGPAD view.

Example

Enable global traffic statistics for the VSI named **company1** in the BGP AD VPLS domain.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 100:1
[HUAWEI-vsi-company1-bgpad] traffic-statistics enable
```

10.7.114 traffic-statistics peer remote-site enable (Kompella)

Function

The **traffic-statistics peer remote-site enable** command enables the statistics about the public traffic on a specified Kompella VPLS PW.

The **undo traffic-statistics peer remote-site enable** command disables the statistics about the public traffic on a specified Kompella VPLS PW.

By default, the statistics of the public traffic on the Kompella VPLS PW are disabled.

Format

traffic-statistics peer *peer-address* **remote-site** *site-id* **enable**

undo traffic-statistics peer *peer-address* **remote-site** *site-id* **enable**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	-
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Kompella VPLS network is configured, you can run the **traffic-statistics peer remote-site enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command in the VSI-BGP view.

Precautions

After you enable the statistics about the public traffic on the specified Kompella VPLS PW, run the **display traffic-statistics vsi peer remote-site** command to view the statistics about the public traffic on the specified PW.

Example

Enable the statistics about the public traffic on the specified Kompella VPLS PW.

```
<HUAWEI> system-view
[HUAWEI] vsi newvsi auto
[HUAWEI-vsi-newvsi] pwsignal bgp
[HUAWEI-vsi-newvsi-bgp] traffic-statistics peer 10.22.33.20 remote-site 2 enable
```

10.7.115 traffic-statistics peer enable (Martini)

Function

The **traffic-statistics peer enable** command enables the statistics about the public traffic on a specified Martini VPLS PW.

The **undo traffic-statistics peer enable** command disables the statistics about the public traffic on a specified Martini VPLS PW.

By default, the statistics function is disabled.

Format

traffic-statistics peer *peer-address* [**negotiation-vc-id** *vc-id*] **enable**

undo traffic-statistics peer *peer-address* [**negotiation-vc-id** *vc-id*] **enable**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	-
negotiation-vc-id *vc-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **traffic-statistics peer enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Precautions

After you enable the statistics about the public traffic on the specified Martini VPLS PW, run the **display traffic-statistics vsi peer negotiation-vc-id** command to view the statistics about the public traffic on the specified PW.

The **traffic-statistics peer enable** command cannot be used together with the **traffic-statistics enable (VSI-LDP view)** command in the VSI-LDP view.

Example

Enable the statistics about the public traffic on the specified Martini VPLS PW.

```
<HUAWEI> system-view
[HUAWEI] vsi newvsi static
[HUAWEI-vsi-newvsi] pwsignal ldp
[HUAWEI-vsi-newvsi-ldp] vsi-id 1
[HUAWEI-vsi-newvsi-ldp] traffic-statistics peer 10.22.33.20 negotiation-vc-id 2 enable
```

10.7.116 traffic-statistics peer enable (VSI-BGPAD)

Function

The **traffic-statistics peer enable** command enables the statistics about the public traffic on a specified BGP AD VPLS PW.

The **undo traffic-statistics peer enable** command disables the statistics about the public traffic on a specified BGP AD VPLS PW.

By default, the statistics about the public traffic on a BGP AD VPLS PW are disabled.

Format

traffic-statistics peer *peer-address* **enable**

undo traffic-statistics peer *peer-address* **enable**

Parameters

Parameter	Description	Value
peer-address	Specifies the peer IP address of the PW.	The value is in dotted decimal notation.

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the BGP AD VPLS network is configured, you can run the **traffic-statistics peer enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

The **traffic-statistics peer enable** command cannot be used together with the **traffic-statistics enable (VSI-BGPAD view)** command in the VSI-BGPAD view.

After you enable the statistics about the public traffic on the specified BGP AD VPLS PW, run the **display traffic-statistics vsi peer ldp129** command to view the statistics about the public traffic on the specified PW.

Example

Configure the BGP AD VPLS VSI named **company1**, and enable the statistics about the public traffic on the PW with the peer at 1.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 100:1
[HUAWEI-vsi-company1-bgpad] traffic-statistics peer 1.1.1.1 enable
```

10.7.117 trace vpls mac vsi

Function

The **trace vpls mac vsi** command checks PE and P devices on the VPLS network which packets pass through from the source to the destination. This command is used to check the connectivity of Layer 2 forwarding links and locate faults on the network.

Format

trace vpls mac *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id*] [**-t** *timeout* | **-f** *first-ttl* | **-m** *max-ttl* | **-exp** *exp* | **-r** *replymode*] *

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the unicast destination MAC address of the VPLS MAC trace, expressed in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The value cannot be a broadcast or multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
vlan *vlan-id*	Specifies the ID of a VLAN	*vlan-id* specifies the VLAN ID, which is an integer that ranges from 1 to 4094.
-t *timeout*	Specifies the timeout period for waiting for a Reply packet in response to a VPLS MAC Trace Request packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-f *first-ttl*	Specifies the initial TTL.	The value is an integer that ranges from 1 to *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from *first-ttl* to 255. The default value is 30.
-exp *exp*	Specifies the priority.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
-r *replymode*	Specifies the reply mode, that is, the Reply packet is sent from the control layer or the data layer. - 1: indicates that the peer end does not respond to MPLS MAC Trace Request packets. - 2: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets. - 3: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets containing the Router Alert TLV option. - 4: indicates that the peer end responds to MPLS MAC Trace Request packets through the control channel of the application program grade. - 5: indicates that the peer end responds to MPLS MAC Trace Request packets with VPLS IPv4 UDP packets.	Enumerated type. At present, only modes 1, 2, and 5 are supported. When mode 2 is adopted, reply packets are sent from the control layer; when mode 5 is adopted, reply packets are sent from the data layer. The default value is 5.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **trace vpls mac vsi** command, you can check the connectivity of Layer 2 forwarding links on the VPLS network, analyze roles of devices, and locate faults on the network.

Prerequisites

Before running this command, ensure that a VSI is configured and the VSI is in the Up state.

Example

On the VPLS network, trace the device with the MAC address 00e0-fc12-3456.

```
<HUAWEI> trace vpls mac 00e0-fc12-3456 vsi a2
 Traceroute to mac 00e0-fc12-3456 vsi a2, 30 hops max, press CTRL_C to break
 TTL  Num     Replier          Time     Type     Downstream              Hit
            LSR-ID          Out Interface
 -------------------------------------------------------------------------
 0    1                              Ingress  10.1.1.1/[3 ]          N
            1.1.1.9          Vlanif1025
 1    1       10.1.1.1        8 ms     Egress                         Y
            3.3.3.9
Info: Succeed in tracing the destination address 00e0-fc12-3456.
```

Table 10-140 Description of the tracert vpls multicast command output

Item	Description
TTL	Time to live.
Num	Sequence number of the packet sent at each hop.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time the packet is processed, that is, period from the time the Request packet is sent from the source node to the time a Reply packet is received by the source node.
Type	Type of the device that sends the Reply packet, which can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	Address and label of the next hop. For example, 10.1.1.1/[3] indicates that the IP address of the next hop is 10.1.1.1 and the label allocated to the next hop is 3.
Hit	Whether the Request packet reaches the destination. ● Y: The Request packet reaches the destination. ● N: The Request packet does not reach the destination.
LSR-ID	ID of the LSR.
Out Interface	Outbound interface through which packets are forwarded.

10.7.118 tracert vpls

Function

The **tracert vpls** command detects the status of a PW or locates an abnormal node on a PW in Down state.

Format

tracert vpls [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **vsi** *vsi-name* { *local-site-id remote-site-id* | **peer** *peer-address* [**negotiate-vc-id** *vc-id*] } [**full-lsp-path**]

Parameters

Parameter	Description	Value
-exp *exp-value*	Specifies the value of the EXP field in the outer label of an MPLS Echo Request packet.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies an initial TTL.	The value is an integer that ranges from 1 to 255 and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies a maximum TTL.	The value is an integer that ranges from 1 to 255 and must be greater than the value of *first-ttl*. The default value is 30.
-r *reply-mode*	Specifies the mode for the peer end to return MPLS Echo Reply packets. The values are as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 UDP datagram carrying a router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.

Parameter	Description	Value
-t *timeout-value*	Specifies the timeout period for waiting for an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
vsi *vsi-name*	Specifies the VPN name.	The value is an existing VSI.
local-site-id	Specifies the ID of the local CE.	The value is an integer that ranges from 0 to 65534.
remote-site-id	Specifies the ID of the remote CE.	The value is an integer that ranges from 0 to 65534.
full-lsp-path	Displays the responses from all nodes on the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, the responses from only the PW nodes along the LSP are displayed.	-
peer *peer-address*	Specifies the IP address of the peer PE.	-
negotiate-vc-id *vc-id*	Specifies the ID of the local PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

After the VPLS network is configured, if the VSI is in the Down state, you can run the **tracert vpls** command to locate the faulty device on the PW.

The **tracert vpls** command applies to the following networking scenarios:

- VPLS networking

  Based on VPLS types, VPLS PW tracert is classified into:

  - Martini VPLS PW tracert

Martini VPLS PW tracert only supports the label alert mode. On a Hierarchical Virtual Private LAN Service (HVPLS) network, only single-segment PWs can be detected. If a PW ID that is optional is set and specified, the PW with the specified PW ID is detected. If no PW ID is specified, the PW associated with the VSI ID is detected.

- Kompella VPLS PW tracert

  Kompella VPLS PW tracert only supports the label alert mode.

  After a faulty PW is detected using the **ping vc** command, run the **tracert vc** command to locate the fault. The **ping vc** and **tracert vc** commands can efficiently check PW connectivity and locate faults on PWs.

Prerequisites

One of the following operations has been performed before this command is used:

- Configuring Kompella VPLS
- Configuring Martini VPLS
- Configuring BGP AD VPLS

Example

Perform the tracert operation on the VPLS link with the remote site ID being 10.

```
<HUAWEI>tracert vpls vsi test 10 10 full-lsp-path
 TTL   Replier            Time    Type      Downstream
 0                           Ingress   10.1.1.2/[4032 3 ]
 1     10.0.0.181         7 ms    Egress
```

Table 10-141 Description of the tracert vpls command output

Item	Description
TTL	TTL in an MPLS Echo Request packet. It indicates the number of hops through which an MPLS Echo Request packet passes from the source node to this node.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time that the packet is processed.
Type	Type of a node: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

Perform the tracert operation to test the connectivity of the BGP AD VPLS PW.

```
<HUAWEI> tracert vpls vsi ad peer 10.2.2.2
 TTL   Replier            Time    Type      Downstream
 0                           Ingress   10.1.1.2/[1025 3 ]
 1     10.2.2.2           30 ms   Egress
```

Table 10-142 Description of the tracert vpls command output

Item	Description
TTL	TTL in an MPLS Echo Request packet. It indicates the number of hops through which an MPLS Echo Request packet passes from the source node to this node.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time the packet is processed. That is, period from the time an MPLS Echo Request packet is sent to the time an MPLS Echo Reply packet is received.
Type	Type of a node: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node. The inner label and the outer label are arranged from left to right, both are outgoing labels.

10.7.119 tracert vpls multicast

Function

The **trace vpls multicast** command starts an MFIB Trace test with a specified VSI in the VPLS domain.

Format

tracert vpls multicast vsi *vsi-name* [**-a** *source-ip-address* | **-t** *timeout* | **-r** *reply-mode* | **-exp** *exp* | **-f** *first-ttl* | **-m** *max-ttl*] * **multicast-address** *multicast-ip-address* **remote-address** *remote-ip-address*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI on which the operation is performed.	The value is an existing VSI.
-a *source-ip-address*	Specifies the IP address of the multicast source. By default, the multicast source IP address is the IP address of the initiator. The value is in dotted decimal notation.	-

Parameter	Description	Value
-t *timeout*	Specifies the timeout period for waiting for an Echo Reply packet.	The value ranges from 0 to 65535, in milliseconds. The default value is 2000 milliseconds.
-r *reply-mode*	Specifies the reply mode. The default value is 2. ● 1: indicates that the peer end does not respond to Echo Request packets. ● 2: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to Echo Request packets with IPv4 or IPv6 UDP packets carrying the Router Alert option. ● 4: indicates that the peer end responds to Echo Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to Echo Request packets with VPLS IPv4 UDP packets. **NOTE** Currently, the switch only supports mode 1, 2, and 5.	-
-exp *exp*	Specifies the priority of Echo Request packets to be sent.	The value is an integer that ranges from 0 to 7. The default value is 0.
-f *first-ttl*	Specifies the initial TTL.	The value ranges from 1 to 255.
-m *max-ttl*	Specifies the maximum TTL, which is not smaller than the initial TTL.	The value ranges from 1 to 255.
multicast-address *multicast-ip-address*	Adds a PW to the multicast group with the specified IP address.	-
remote-address *remote-ip-address*	Specifies a unicast IP address.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

You can run the **tracert vpls multicast** command on the PE, SPE, and UPE to implement the monitoring functions:

- The command is used to locate the faulty PE on the VPLS network when IGMP Snooping is enabled.
- The command is used for path discovery on the VPLS network when the IGMP Snooping is disabled.

Precautions

The **trace vpls multicast** command does not support BGP AD VPLS.

Example

Initiate a Trace test in a specified VSI with the multicast address being 226.0.0.1 in the VPLS domain.

```
<HUAWEI> tracert vpls multicast vsi a2 multicast-address 226.0.0.1 remote
-address 10.3.3.9
traceroute to 10.3.3.9 vsi a2, 30 hops max , press CTRL+C to break
-----------------------------------------------------------------
TTL  0
 Num     : 1          Replier: UNKNOWN        Upstream: UNKNOWN
 Time    : 0          Snpg   : N              Version : 2
 Proxy   : N          Port   : N              FW Mode : IP
 Hit Flag: NotInMFIB    PW Info: Y            Alert   : N
 Policy  : Permit       CAC    : N
 Query   : 0          Report : 0              Leave   : 0
-----------------------------------------------------------------
TTL  1
 Num     : 1          Replier: 10.3.3.9       Upstream: 10.1.1.9
 Time    : 7          Snpg   : N              Version : 2
 Proxy   : N          Port   : N              FW Mode : IP
 Hit Flag: NotInMFIB    PW Info: N            Alert   : N
 Policy  : Permit       CAC    : N
 Query   : 0          Report : 0              Leave   : 0
-----------------------------------------------------------------
Info: Succeed in tracing the destination address  10.3.3.9
```

Table 10-143 Description of the tracert vpls multicast command output

Item	Description
TTL	Time to live.
Num	Sequence number of the received packet.
Replier	Address of the replier.
Upstream	Address of the PE that sends or forwards the packet.

Item	Description
Time	Time the packet is processed. That is, period from the time the Request packet is sent from the source node to the time a Reply packet is received by the source node.
Snpg	Whether IGMP Snooping is enabled.
Version	Version of IGMP Snooping enabled in the VSI.
Proxy	Whether IGMP Snooping proxy is enabled.
Port	Whether the interface learning function is enabled.
FW Mode	MAC address-based forwarding mode or IP address-based forwarding mode.
Hit Flag	Whether corresponding multicast forwarding information exists in the MFIB.
PW Info	Whether the PWs forwarding the packet can be obtained according to the ingoing label.
Alert	State in which the interface only receives IGMP messages with Router-Alert options.
Policy	Whether the packet meets the deny rule or permit rule according to the ACL.
CAC	Whether connection admission control is configured in the VSI.
Query	The number of Query packets using the current IGMP version received by the replier.
Report	The number of Report packets using the current IGMP version received by the replier.
Leave	The number of Leave packets using the current IGMP version received by the replier.

10.7.120 unknown-frame

Function

The **unknown-frame** command specifies the processing mode for received unknown frames.

By default, the system broadcasts unknown multicast frames.

Format

unknown-frame multicast { **drop** | **broadcast** }

Parameters

Parameter	Description	Value
multicast	Indicates the unknown frames are of the multicast type.	-
drop	Drops the unknown frames.	-
broadcast	Broadcasts the unknown frames.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

After a VSI receives a frame, if an entry that matches the destination address cannot be found in the MAC address table, the frame is regarded as an unknown frame.

Example

Configure the VSI to discard unknown frames.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 auto
[HUAWEI-vsi-company1] unknown-frame multicast drop
```

10.7.121 unknown-unicast-suppression cir cbs (VSI view)

Function

The **unknown-unicast-suppression cir cbs** command enables unknown unicast traffic suppression in the VSI.

The **undo unknown-unicast-suppression** command disables unknown unicast traffic suppression in the VSI.

By default, unknown unicast traffic in a VSI is not suppressed.

Format

unknown-unicast-suppression cir *cir-value* **cbs** *cbs-value*

undo unknown-unicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the CIR, that is, the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the CBS, that is, the traffic that can pass instantly, or the depth of the first token bucket.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPLS network, broadcast packets, multicast packets, and unknown unicast packets are transmitted in broadcast mode and copied to neighboring ACs and PWs. If large quantities of unknown unicast packets are on the VPLS network, the device has to make a lot of copies of these unknown unicast packets, which wastes bandwidth and resources, and deteriorates system performance. You can run the **unknown-unicast-suppression cir cbs** command to suppress the unknown unicast traffic in the VSI. The rate of unknown unicast traffic on the VPLS network is limited.

Prerequisites

A VSI has been created using the **vsi** *vsi-name* [**auto** | **static**] command.

Example

Set the CIR to 100 kbit/s and the CBS to 18800 bytes for the unknown unicast traffic that can pass for VSI1.

```
<HUAWEI> system-view
[HUAWEI] vsi VSI1
[HUAWEI-vsi-VSI1] unknown-unicast-suppression cir 100 cbs 18800
```

10.7.122 upe-npe mac-withdraw enable

Function

The **upe-npe mac-withdraw enable** command enables an SPE to forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

The **undo upe-npe mac-withdraw enable** command disables an SPE from forwarding the LDP MAC Withdraw messages received from UPEs to other SPEs.

By default, an SPE does not forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

Format

upe-npe mac-withdraw enable

undo upe-npe mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, run the **upe-npe mac-withdraw enable** command to enable an SPE to forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

Prerequisites

LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.

Precautions

The **upe-npe mac-withdraw enable** command is used on SPEs.

- An SPE refers to the network-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] command to specify an SPE.
- A UPE refers to the user-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** command to specify a UPE.
- If HVPLS is not configured on the local device, the **upe-npe mac-withdraw enable** command is not required.

Example

Enable the SPE to forward the LDP MAC Withdraw messages received from UPEs to other SPEs.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
```

```
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] upe-npe mac-withdraw enable
```

10.7.123 upe-upe mac-withdraw enable

Function

The **upe-upe mac-withdraw enable** command enables an SPE to forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

The **undo upe-upe mac-withdraw enable** command disables an SPE from forwarding the LDP MAC Withdraw messages received from a UPE to other UPEs.

By default, an SPE does not forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

Format

upe-upe mac-withdraw enable

undo upe-upe mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, run the **upe-upe mac-withdraw enable** command to enable an SPE to forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

Prerequisites

LDP has been configured as the PW signaling protocol using the **pwsignal ldp** command.

Precautions

The **upe-upe mac-withdraw enable** command is used on SPEs.

- An SPE refers to the network-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] command to specify an SPE.
- A UPE refers to the user-side peer of the local VSI in HVPLS. You can run the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tnl-policy** *policy-name*] **upe** command to specify a UPE.

- If HVPLS is not configured on the local device, the **upe-upe mac-withdraw enable** command is not required.

Example

Enable the SPE to forward the LDP MAC Withdraw messages received from a UPE to other UPEs.

```
<HUAWEI> system-view
[HUAWEI] vsi v1 static
[HUAWEI-vsi-v1] pwsignal ldp
[HUAWEI-vsi-v1-ldp] upe-upe mac-withdraw enable
```

10.7.124 vpls bgp encapsulation

Function

The **vpls bgp encapsulation** command specifies the re-encapsulation mode of a VPLS packet after the local PE receives the VPLS packet whose encapsulation type is 19.

By default, the local PE re-encapsulates the received VPLS packet with the encapsulation type as 19 in VLAN mode.

Format

vpls bgp encapsulation { **ethernet** | **vlan** }

Parameters

Parameter	Description	Value
ethernet	Indicates that the received VPLS packet whose encapsulation type is 19 is re-encapsulated in Ethernet mode.	-
vlan	Indicates that the received VPLS packet whose encapsulation type is 19 is re-encapsulated in VLAN mode.	-

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vpls bgp encapsulation** command is run only when a Huawei device is connected to a non-Huawei device.

As defined by the latest RFC, the encapsulation type of PW in the Kompella VPLS is 19. Huawei devices support only the Ethernet encapsulation and VLAN encapsulation. If the **vpls bgp encapsulation** command is used, upon receiving a VPLS packet with the encapsulation type as 19, the system re-encapsulates the VPLS packet according to the configuration so that Huawei devices can interwork with non-Huawei devices.

Precautions

Huawei devices can interwork with non-Huawei devices only when the **vpls bgp encapsulation** command is used together with the **ignore-mtu-match** command.

Example

Re-encapsulate the received VPLS packet with the encapsulation type as 19 in Ethernet mode.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] vpls bgp encapsulation ethernet
```

10.7.125 vpls ignore-ac-state

Function

The **vpls ignore-ac-state** command prevents the status of a VSI from being affected by the status of the Attachment Circuit (AC).

The **undo vpls ignore-ac-state** command restores the default setting.

By default, changes in the status of the AC affect the VSI status.

Format

vpls ignore-ac-state

undo vpls ignore-ac-state

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vpls ignore-ac-state** command is used only before a service switchover between a new network and an old one. Before the devices on an old VPLS network switch to a new network, if you want to check whether the VSI on the new VPLS network can work normally, you can run this command to configure the VSI to ignore the AC status so that the VSI maintains the Up state before the switchover.

Precautions

After the **vpls ignore-ac-state** command is executed, a VSI can keep Up if the VSI PW is Up, and the VSI status is not affected by the AC status.

The AC status refers to the status of the physical or logical interface bound to the VSI.

After the devices on the old network switch to a new network, run the **undo vpls ignore-ac-state** command to restore the default setting.

Example

Configure a VSI to ignore the AC status.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] vpls ignore-ac-state
```

10.7.126 vpls-family

Function

The **vpls-family** command displays the BGP VPLS address family view.

The **undo vpls-family** command deletes all configurations of the BGP VPLS address family.

By default, the BGP VPLS address family is not configured in the BGP view.

Format

vpls-family

undo vpls-family

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

When configuring Kompella VPLS, you need to enable BGP peers to exchange VPLS information. In this case, run the **vpls-family** command to enter the BGP VPLS address family view.

Example

Enter the VPLS address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] vpls-family
[HUAWEI-bgp-af-vpls]
```

10.7.127 vpls-id

Function

The **vpls-id** command specifies the ID of a VPLS domain to which a VSI belongs.

By default, no VPLS VSI ID is specified.

Format

vpls-id *vpls-id*

Parameters

Parameter	Description	Value
vpls-id	Specifies the ID of a VPLS domain to which multiple VSIs on PEs belong.	A VPLS ID is in one of the following formats: ● 16-bit AS number: a 32-bit user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● 32-bit IP address: a 16-bit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in

Parameter	Description	Value
		dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VSIs in a BGP AD VPLS domain use BGP signaling to automatically discover members in the same VPLS domain. A VPLS domain is uniquely identified by a VPLS ID. When creating BGP AD VSIs on different PEs, specify the same VPLS ID for the VSIs so that they can join the same VPLS domain. Different BGP AD VSIs on the same PE cannot be added to the same VPLS domain.

Prerequisites

Automatic VPLS member discovery and automatic PW deployment have been configured for the current VSI using the **bgp-ad** command in the VSI view, and the VSI-BGPAD view has been displayed.

Precautions

An ID is specified for the BGP AD VSI. A VPLS domain is uniquely identified by a VPLS ID. Different VPLS IDs must be configured for different VSIs on the same PE. If the VPLS ID specified using the **vpls-id** command for a VSI on a PE has been used by another VSI on that PE, the **vpls-id** command does not take effect and an error message will be displayed. The VSIs that belong to the same VPLS domain and reside on different PEs must be configured with the same VPLS ID.

After a VPLS ID is configured for a VSI, it cannot be directly changed. To change the VPLS ID, you need to delete the VSI, re-create a VSI, and reconfigure the VPLS ID.

Example

Configure a VPLS ID in the format of 16-bit AS number:32-bit user-defined number for the VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] vsi company1
[HUAWEI-vsi-company1] bgp-ad
[HUAWEI-vsi-company1-bgpad] vpls-id 101:3
```

Configure a VPLS ID in the format of 32-bit IP address:16-bit user-defined number for the VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] bgp-ad
[HUAWEI-vsi-company2-bgpad] vpls-id 2.2.2.2:1
```

Configure a VPLS ID in the format of 32-bit AS number:16-bit user-defined number for the VSI named **company3**.

```
<HUAWEI> system-view
[HUAWEI] vsi company3
[HUAWEI-vsi-company3] bgp-ad
[HUAWEI-vsi-company3-bgpad] vpls-id 16.20:30
```

10.7.128 vpls mac-withdraw loop-detect enable

Function

The **vpls mac-withdraw loop-detect enable** command enables MAC withdraw loop detection.

The **undo vpls mac-withdraw loop-detect enable** command disables MAC withdraw loop detection.

By default, MAC withdraw loop detection is disabled.

Format

vpls mac-withdraw loop-detect enable

undo vpls mac-withdraw loop-detect enable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a dual-homing VPLS or hierarchical VPLS (HVPLS) network, MAC withdraw messages can be forwarded between hub and spoke PWs and between spoke PWs. Incorrect configurations may cause a MAC withdraw message loop, which results in traffic loss. If the loop involves a large number of MAC withdraw messages, denial of service (DoS) attacks may occur. To resolve these problems, run the **vpls mac-withdraw loop-detect enable** command to enable MAC withdraw loop detection. After you enable MAC withdraw loop detection, a PE immediately discards MAC withdraw message when it detects a MAC withdraw message loop.

Prerequisites

MPLS L2VPN has been enabled using the **mpls l2vpn** command.

Example

Enable MAC withdraw loop detection.

```
<HUAWEI> system-view
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] vpls mac-withdraw loop-detect enable
```

10.7.129 vpn-target (VSI-BGP view)

Function

The **vpn-target** command associates a VSI with one or more VPN targets.

The **undo vpn-target** command deletes a VPN target associated with a VSI.

By default, a VSI is not associated with any VPN target.

Format

vpn-target *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-16> } [**both** | **export-extcommunity** | **import-extcommunity**]

Parameters

Parameter	Description	Value
vpn-target	Specifies a VPN target that is added to a VSI.	You can choose one of the following formats to express a VPN target: ● 16-bit AS number: a 32-bit user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● 32-bit IP address: a 16-bit user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-

Parameter	Description	Value
		byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.
export-extcommunity	Indicates the extended community attributes carried in the data to be sent.	-
import-extcommunity	Indicates the extended community attributes carried in the received data.	-
both	Indicates the import routing information from the extended community of the destination VPN and the export routing information sent to the extended community of the destination VPN.	-
all	Deletes all attributes of VPN targets.	-

Views

VSI-BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending routing information to other PE devices according to the VSI, a PE device adds export VPN targets to the routing information. When receiving routing information from other PE devices, the PE determines whether to add the data to the VSI according to import VPN targets. Therefore, VPN targets can be used to control the route advertisement between nodes.

Prerequisites

The RD of the VSI has been configured using the **route-distinguisher** *route-distinguisher* command.

Example

Associate the current VSI with a VPN target.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] pwsignal bgp
[HUAWEI-vsi-company2-bgp] route-distinguisher 2.2.2.2:1
[HUAWEI-vsi-company2-bgp] vpn-target 3:3 export-extcommunity
[HUAWEI-vsi-company2-bgp] vpn-target 4:4 import-extcommunity
[HUAWEI-vsi-company2-bgp] vpn-target 5:5 both
```

10.7.130 vpn-target (VSI-BGPAD view)

Function

The **vpn-target** command associates a VSI in a BGP AD VPLS domain with one or more VPN targets.

The **undo vpn-target** command removes the VPN targets associated with the VSI.

By default, a VSI is not associated with any VPN target. The association must be configured when a VSI is created.

Format

vpn-target *vpn-target* &<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-16> } [**both** | **export-extcommunity** | **import-extcommunity**]

Parameters

Parameter	Description	Value
vpn-target	Associates a VPN target with a VSI.	The format of a VPN target can be one of the following: - 16-bit AS number:32-bit user-defined number. For example, 1:3. The AS number ranges from 0 to 65535, and the user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0. This means that the VPN target value cannot be 0:0. - 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535. - Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. - 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.
both	Specifies the extended community attributes of the received and sent routing information.	-

Parameter	Description	Value
export-extcommunity	Specifies the extended community attributes carried in routing information to be sent.	-
import-extcommunity	Receives routing information carrying specified extended community attributes.	-
all	Deletes all VPN targets.	-

Views

VSI-BGPAD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VPN targets can be used in a BGP AD VPLS domain to control the route advertisement and communication between nodes. When a PE advertises routing information to other PEs of different VSIs, it adds export VPN targets to the routing information. When the PE receives routing information from other PEs, it uses import VPN targets to determine whether to import the routing information to the VSIs on it.

Prerequisites

The VPLS ID has been configured using the **vpls-id** *vpls-id* command in the VSI-BGPAD view.

Precautions

A PW can be set up between two VSIs in a BGP AD VPLS domain only when the import VPN target associated with a VSI is the same as the export VPN target associated with the other VSI.

After the **vpn-target** command is run, the PE only advertises the routing information that contains the export VPN targets and imports the routing information that contains the import VPN targets. Two PEs are allowed to communicate with each other only when the VPN targets carried in their exchanged routing information match.

Example

Configure a VSI named **company2**, and associate the VSI with import VPN targets 4:4 and 5:5 and with export VPN targets 3:3 and 5:5.

```
<HUAWEI> system-view
[HUAWEI] vsi company2
[HUAWEI-vsi-company2] bgp-ad
[HUAWEI-vsi-company2-bgpad] vpls-id 100:1
[HUAWEI-vsi-company2-bgpad] vpn-target 3:3 export-extcommunity
[HUAWEI-vsi-company2-bgpad] vpn-target 4:4 import-extcommunity
[HUAWEI-vsi-company2-bgpad] vpn-target 5:5 both
```

10.7.131 vsi

Function

The **vsi** command creates a VSI or displays the VSI view.

The **undo vsi** command deletes a VSI.

By default, no VSI is created.

Format

vsi *vsi-name* [**auto** | **static**]

undo vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Names of the VSIs on one device cannot be identical.
auto	Indicates that the automatic member discovery mode is used in the VSI.	-
static	Indicates that the static member discovery mode is used in the VSI.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure VPLS, you need to create VSIs first. Each device in a VPLS domain needs to be configured with a VSI that belongs to the domain.

On a Martini or Kompella VPLS network, the VPLS member discovery mode for a created VSI can be set to static or auto. You can set the signaling mode using the **pwsignal** { **bgp** | **ldp** } command after a VSI is created. Use the LDP signaling mode if the static member discovery mode is used. Use the BGP signaling mode if the automatic member discovery mode is used. The member discovery mode cannot be modified. To modify the member discovery mode of the VSI, you need to delete the VSI. Then, re-create a VSI and specify the member discovery mode.

When creating a BGP AD VSI, do not specify a member discovery mode of the VSI. A VSI without a specified member discovery mode can be configured to use the LDP, BGP, or BGP AD signaling mode.

If you have specified a member discovery mode for a VSI, specify the same member discovery mode in the **vsi** command when you want to re-enter the VSI view. If the member discovery mode in the **vsi** command is different from the member discovery mode specified for the VSI, you cannot enter the VSI view.

Prerequisites

The MPLS L2VPN function has been enabled on the device.

Precautions

Note the following points when configuring VSIs in a VPLS domain:

- VSIs on different PEs can have different names.
- A VSI on a PE must be configured with a unique VSI ID or VPLS ID.
- Multiple peers can be specified for a VSI on a PE.

If the specified VSI exists, you can use the **vsi** command to enter the VSI view.

After VPLS configurations are complete, VPLS packets are forwarded based on VSIs. Exercise caution when using the **undo vsi** command because VPLS traffic will be interrupted.

Example

Create a Martini VPLS VSI named **company1**.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
```

Create a Kompella VPLS VSI named **company2**.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company2 auto
[HUAWEI-vsi-company2] pwsignal bgp
```

Create a BGP AD VPLS VSI named **company3**.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company3
```

Create a Martini VPLS VSI named **company4**, and do not specify the VSI member discovery mode.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company4
[HUAWEI-vsi-company4] pwsignal ldp
```

Create a Martini Kompella VPLS VSI named **company5**, and do not specify the VSI member discovery mode.

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 10.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls l2vpn
[HUAWEI-l2vpn] quit
[HUAWEI] vsi company5
[HUAWEI-vsi-company5] pwsignal bgp
```

10.7.132 vsi-id

Function

The **vsi-id** command sets an ID for a VSI.

By default, no VSI ID is set.

Format

vsi-id *vsi-id*

Parameters

Parameter	Description	Value
vsi-id	Specifies the unique ID of a VSI.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VSI in the Martini VPLS and use the LDP as the PW signaling protocol, run the **vsi-id** command to configure the VSI ID. Other parameters can be configured only after the VSI ID is configured.

Precautions

Different VSIs have different IDs.

VSI IDs on all devices in the same VPLS domain must be the same.

The VSI ID cannot be changed after being set. If you want to change the VSI ID, you need to delete the VSI and re-create a VSI.

Example

Set the ID of the current VSI to 1.

```
<HUAWEI> system-view
[HUAWEI] vsi company1 static
[HUAWEI-vsi-company1] pwsignal ldp
[HUAWEI-vsi-company1-ldp] vsi-id 1
```

10.8 L2VPN Access to L3VPN Configuration Commands

10.8.1 Command Support

Only the following switch models support L2VPN access to L3VPN:

S5731-S, S5731-H, S5731S-H, S5732-H, S6730-S, S6730S-H, and S6730-H

10.8.2 display virtual-ethernet ve-group

Function

The **display virtual-ethernet ve-group** command displays the binding relationship between Virtual Ethernet (VE) interfaces and a VE group.

Format

display virtual-ethernet ve-group [*ve-group-id*]

Parameters

Parameter	Description	Value
ve-group-id	Specifies the ID of a VE group.	The value is an integer ranging from 1 to 8.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is configured with many VE groups, you can use this command to view the relationship between VE interfaces and VE groups.

Example

Display the binding relationship between all VE interfaces and VE groups on a switch.

```
<HUAWEI> display virtual-ethernet ve-group
 Ve-groupID    TerminateVE                 AccessVE
 1             Virtual-Ethernet0/0/1(L2)   Virtual-Ethernet0/0/2(L3)
Total 1, 1 printed
```

Table 10-144 Description of the **display virtual-ethernet ve-group** command output

Item	Description
Ve-groupID	ID of a VE group.
TerminateVE	L2VE interface terminating an L2VPN.
AccessVE	L3VE interface accessing an L3VPN.
Total 1, 1 printed	Total number of VE groups.

10.8.3 display mpls l2vpn track route

Function

The **display mpls l2vpn track route** command displays information about the PWs that track VPNv4 route status.

Format

display mpls l2vpn track route [*ipv4-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the destination IP address of a VPNv4 route.	The value is in dotted decimal notation.
mask	Specifies a mask in dotted decimal notation.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an L2VPN access to L3VPN scenario, if all L3VPN-side links of an NPE become unavailable, a black-hole route comes into existence. The user-side UPE cannot detect the link failures and still sends traffic to the NPE. As a result, traffic loss occurs. To prevent traffic loss, run the **mpls l2vpn track route** command to configure the PW to track VPNv4 route status. Then, after the NPE detects that all its L3VPN-side links become unavailable, the NPE instructs the UPE to switch traffic to the secondary PW.

To check information about the PWs that track VPNv4 route status, run the **display mpls l2vpn track route** command.

Example

Display information about all PWs that track VPNv4 route status.

```
<HUAWEI> display mpls l2vpn track route
Total route number:1      reachable:0      unreachable:1
--------------------------------------------------------------

VPN instance name : vpna
Route             : 10.1.1.1/32
Route status      : reachable
PW number         : 1
VC ID      VC Type               Peer IP             VC State
--------------------------------------------------------------
101        VLAN                  10.1.1.2            up
```

Table 10-145 Description of the **display mpls l2vpn track route** command output

Item	Description
Total route number	Total number of VPNv4 routes tracked by a PW.
reachable	Number of reachable VPNv4 routes.
unreachable	Number of unreachable VPNv4 routes.
VPN instance name	VPN instance name.
Route	Destination IP address of a VPNv4 route.
Route status	VPNv4 route status: ● reachable ● unreachable
VC ID	ID of a VC, which uniquely identifies the VC.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Peer IP	Peer IP address.
VC State	VC status: ● up: The VC is established. ● Down: The VC is not established.

10.8.4 mpls l2vpn track route

Function

The **mpls l2vpn track route** command configures a PW to track VPNv4 route status.

The **undo mpls l2vpn track route** command configures a PW not to track VPNv4 route status.

By default, a PW does not track VPNv4 route status.

Format

mpls l2vpn track route *ipv4-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name*

undo mpls l2vpn track route

Parameters

Parameter	Description	Value
ipv4-address	Specifies the destination IP address of a VPNv4 route.	The value is in dotted decimal notation.
mask	Specifies a mask in dotted decimal notation.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

In an L2VPN access to L3VPN scenario, if all L3VPN-side links of an NPE become unavailable, a black-hole route comes into existence. The user-side UPE cannot detect the link failures and still sends traffic to the NPE. As a result, traffic loss occurs. To prevent traffic loss, run the **mpls l2vpn track route** command to configure the PW to track VPNv4 route status. Then, after the NPE detects that all its L3VPN-side links become unavailable, the NPE instructs the UPE to switch traffic to the secondary PW.

Example

Configure a PW to track VPNv4 route status.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l2-terminate
[HUAWEI-Virtual-Ethernet0/0/1] quit
[HUAWEI] interface virtual-ethernet 0/0/1.1
[HUAWEI-Virtual-Ethernet0/0/1.1] mpls l2vc 10.1.1.2 101
[HUAWEI-Virtual-Ethernet0/0/1.1] mpls l2vpn track route 10.1.1.1 32 vpn-instance vpna
```

10.8.5 statistic enable (VE interface view)

Function

The **statistic enable** command enables the traffic statistics collection function on a Virtual Ethernet (VE) interface.

The **undo statistic enable** command disables the traffic statistics collection function on a VE interface.

By default, the traffic statistics collection function is disabled on a VE interface.

Format

statistic enable { **both** | **inbound** | **outbound** }

undo statistic enable { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
both	Enables the traffic statistics collection function for incoming and outgoing traffic.	-
inbound	Enables the traffic statistics collection function for incoming traffic.	-
outbound	Enables the traffic statistics collection function for outgoing traffic.	-

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable the traffic statistics collection function on the VE interfaces if you want to check the network status or troubleshoot network faults.

Prerequisites

The VE interfaces have been bound to VE groups by using the **ve-group** command. Otherwise, the **statistic enable** command does not take effect.

Precautions

- After you run the **undo statistic enable** command on a VE interface, the switch stops collecting traffic statistics on the VE interface and the collected traffic statistics will be deleted.
- The switch uses ACL resources when collecting traffic statistics. If the traffic statistics collection function is enabled on too many VE interfaces, other services may fail to obtain ACL resources.

- The switch can only collect statistics of unicast, multicast, and broadcast packets on VE interfaces.
- On the VE interface enabled with the traffic statistics collection function, the packets such as ping packets sent from the switch cannot be counted.

Example

Enable the traffic statistics collection function for incoming and outgoing traffic on the VE interface.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l2-terminate
[HUAWEI-Virtual-Ethernet0/0/1] statistic enable both
```

10.8.6 ve-group

Function

The **ve-group** command configures a VE interface to work in multi-service access mode and binds the VE interface to a specified VE group.

The **undo ve-group** command restores a VE interface to common mode.

By default, a VE interface works in common mode.

Format

ve-group *ve-group-id* { **l2-terminate** | **l3-access** }

undo ve-group

Parameters

Parameter	Description	Value
ve-group-id	Specifies the ID of a VE group.	The value is an integer ranging from 1 to 8.
l2-terminate	Sets the VE interface to an L2VE interface that terminates the L2VPN.	-
l3-access	Sets the VE interface to an L3VE interface that accesses the L3VPN.	-

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In L2VPN access to L3VPN scenarios:

- To change a VE interface to an L2VE interface, run the **ve-group** *ve-group-id* **l2-terminate** command.
- To change a VE interface to an L3VE interface, run the **ve-group** *ve-group-id* **l3-access** command.

Precautions

- A VE group has only one L2VE interface and one L3VE interface.
- The two VE interfaces in a VE group must be on the same chassis.
- Multiple sub-interfaces can be created for each L2VE or L3VE interface to provide access for different VLAN services.

Example

Set Virtual-Ethernet 0/0/1 to an L2VE interface.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/1
[HUAWEI-Virtual-Ethernet0/0/1] ve-group 1 l2-terminate
```

Set Virtual-Ethernet 0/0/2 to an L3VE interface.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet 0/0/2
[HUAWEI-Virtual-Ethernet0/0/2] ve-group 1 l3-access
```

11 WLAN-AC Commands

11.1 WLAN Service Configuration Commands

11.1.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.1.2 ac sysnetid

Function

The **ac sysnetid** command configures an NE name for an AC.

The **undo ac sysnetid** command deletes the NE name of an AC.

By default, no NE name is configured for an AC.

Format

ac sysnetid *ac-sysnetid*

undo ac sysnetid

Parameters

Parameter	Description	Value
ac-sysnetid	Specifies the NE name of an AC.	The value is a string of 1 to 32 case-sensitive characters. The value beginning and ending with double quotation marks (" ") can contain spaces. The value can contain digits, letters, and special characters such as the asterisk (*) and number sign (#).

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrator can run the **ac sysnetid** command to configure a unique NE name for an AC. This facilitates AC management.

Configuration Impact

If you run the **ac sysnetid** command multiple times, only the latest configuration takes effect.

Example

Set the NE name of an AC to **ABC123**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac sysnetid ABC123
```

11.1.3 active-dull-client enable

Function

The **active-dull-client enable** command enables the function of preventing terminals from entering the power-saving mode.

The **undo active-dull-client enable** command disables the function.

By default, the function of preventing terminals from entering the power-saving mode is disabled.

Format

active-dull-client enable

undo active-dull-client enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to individual reasons, some terminals may not run services normally when entering the power-saving mode. You can run the **active-dull-client enable** command to enable the function of preventing terminals from entering the power-saving mode. After that, an AP frequently sends QoS data frames to these terminals to prevent them from entering the power-saving mode, ensuring normal services. This function does not take effect for some terminals and cannot prevent the terminals from entering the power-saving mode. For details, see *Test Report on Terminal Compatibility*.

Precautions

After the function is enabled, the terminals consume more power and extra bandwidth. If no terminal unexpectedly enters the power-saving state, you are advised to disable the function.

Example

Enable the function of preventing terminals from entering the power-saving mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] active-dull-client enable
```

11.1.4 active-dull-client force enable

Function

The **active-dull-client force enable** command enables the function of forcibly preventing terminals from entering the power-saving mode.

The **undo active-dull-client force enable** command disables the function of forcibly preventing terminals from entering the power-saving mode.

By default, the function of forcibly preventing terminals from entering the power-saving mode is disabled.

Format

active-dull-client force enable

undo active-dull-client force enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of preventing terminals from entering the power-saving mode is enabled, some special terminals still enter the power-saving mode, causing service packet loss. In this case, you can enable the function of forcibly preventing terminals from entering the power-saving mode to wake up these terminals and prevent them from entering the power-saving mode.

Precautions

Enabling this function increases terminal power consumption and occupies extra bandwidth. Therefore, it is recommended that this function be enabled only when there are such special terminals.

Example

Enable the function of forcibly preventing terminals from entering the power-saving mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] active-dull-client force enable
```

11.1.5 advertise-ap-name enable

Function

The **advertise-ap-name enable** command enables Beacon frames to carry the AP name.

The **undo advertise-ap-name enable** disables Beacon frames from carrying the AP name.

By default, Beacon frames do not carry the AP name.

Format

advertise-ap-name enable

undo advertise-ap-name enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

In certain scenarios, you can run the **advertise-ap-name enable** command to enable Beacon frames to carry the AP name. In this way, you can quickly locate and identify APs by identifying the AP name carried in an SSID or display the AP name on STAs that can receive and resolve the host name carried in SSIDs of multiple APs.

Example

Enable Beacon frames to carry the AP name in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] advertise-ap-name enable
```

11.1.6 agile-antenna-polarization

Function

The **agile-antenna-polarization enable** command enables self-adaptive polarization for agile antennas.

The **undo agile-antenna-polarization enable** command disables self-adaptive polarization for agile antennas.

By default, self-adaptive polarization is disabled for agile antennas.

Format

agile-antenna-polarization enable

undo agile-antenna-polarization enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Self-adaptive polarization for agile antennas can reduce interference between transmit signals of antennas, and increase the transmit power of antennas and the demodulation SNR of STAs. When providing wireless coverage, you can enable this function when the following types of STA exist:

- STA with one transmit antenna and one receive antenna in 1x1 mode
- STA with two transmit antennas and two receive antennas in 2x2 mode

After this function is enabled, the AP uses two mutually orthogonal antennas to communicate with STAs but not a third antenna.

Prerequisites

Dual-polarized antennas have been connected to radio ports A and B on the same frequency band.

Example

Enable self-adaptive polarization for agile antennas in a 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] agile-antenna-polarization enable
```

11.1.7 antenna-gain

Function

(AP group radio view) The **antenna-gain** command configures the antenna gain for all specified AP radios in an AP group.

(AP group radio view) The **undo antenna-gain** command restores the default antenna gain of all specified AP radios in an AP group.

(AP radio view) The **antenna-gain** command configures the antenna gain for an AP radio.

(AP radio view) The **undo antenna-gain** command restores the antenna gain of an AP radio to that configured in the AP group radio view.

By default, no antenna gain is configured for AP radios. The antenna gains of AP radios depend on AP types and operating channels of AP radios. To check the default antenna gains of radios on different AP types, run the **display ap-type** { **id** *type-id* | **type** *ap-type* } command.

Format

antenna-gain *antenna-gain*

undo antenna-gain

Parameters

Parameter	Description	Value
antenna-gain	Specifies the antenna gain.	The value is an integer that ranges from –10 to +30, in dB.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The antenna gain is the ratio of the power density produced by an antenna to the power density that should be obtained at the same point if the power accepted by the antenna were radiated equally. It can measure the capability for an antenna to receive and send signals in a specified direction, which is one of the most important parameters to select a BTS antenna. Under the same condition, a higher antenna gain indicates a longer transmission distance.

Precautions

- The regulatory requirements for the strength of radio signals vary in different countries and regions. Therefore, when APs and external antennas are used together, run the **antenna-gain** command to set the antenna gain based on the actual antenna specifications. Then the device software controls the transmit power based on the configured antenna gain within the range allowed by the country code.
- The antenna gain of an AP radio configured using the command takes effect only for external antennas.
- The maximum transmit power of a radio must comply with local laws and regulations. For details, see *WLAN Country Codes and Channels Compliance*. You can obtain this table at Huawei technical support website.
  - Enterprise technical support website: **https://support.huawei.com/enterprise**
  - Carrier technical support website: **https://support.huawei.com**
- The configuration in the AP radio view has a higher priority than that in the AP group radio view.
- When the antenna gain of an AP is not an integer, the AC rounds the value off and delivers the integer antenna gain. For example, if the 2.4 GHz antenna gain of an AP is 2.5 dB, the 2.4 GHz antenna gain of 3 dB is displayed on the AC.

Example

Set the antenna gain of radio 0 on AP 1 to 4.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] antenna-gain 4
```

11.1.8 ap auth-mode

Function

The **ap auth-mode** command configures the AP authentication mode.

The **undo ap auth-mode** command restores the default AP authentication mode.

By default, the AP authentication mode is MAC address authentication. In the CloudCampus Solution, for an AC in NETCONF mode, the AP authentication mode is SN authentication.

Format

ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** }

undo ap auth-mode

Parameters

Parameter	Description	Value
mac-auth	Indicates the MAC address authentication mode.	-
no-auth	Indicates the none authentication mode.	-
sn-auth	Indicates the SN authentication mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the device authenticates APs using the configured mode.

NOTE

The none authentication mode brings security risks. You are advised to set the authentication mode to MAC address or SN authentication, which is more secure.

Example

Set the AP authentication mode to MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap auth-mode mac-auth
Warning: The authentication mode is switched to MAC address authentication. Ensu
re that the APs added offline have MAC address information. Otherwise, configura
tions of these APs may be lost after the device restarts. Continue? [Y/N]:Y
```

11.1.9 ap blacklist

Function

The **ap blacklist** command adds APs to the AP blacklist.

The **undo ap blacklist** command deletes APs from the AP blacklist.

By default, no APs exist in the AP blacklist.

Format

ap blacklist mac *ap-mac1* [**to** *ap-mac2*]

undo ap blacklist mac { *ap-mac1* [**to** *ap-mac2*] | **all** }

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
to *ap-mac2*	Specifies the end MAC address during the batch operation. The value of *ap-mac2* must be larger than *ap-mac1*, and *ap-mac1* and *ap-mac2* together specify a range. A maximum of 128 MAC addresses are supported during the batch operation.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Deletes all MAC addresses from the blacklist.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

APs in the blacklist cannot go online. Online APs will be disconnected after it is blacklisted.

Precautions

The AP blacklist and whitelist can both be configured. However, the MAC address of an AP cannot be added to both of them.

If the AP whitelist and blacklist are both configured, the system checks an AP against the blacklist first.

Example

Add the AP with the MAC address of 00e0-fc07-8280 to the AP blacklist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap blacklist mac 00e0-fc07-8280
```

Add MAC addresses from 00e0-fc07-8270 to 00e0-fc07-8276 to the AP blacklist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap blacklist mac 00e0-fc07-8270 to 00e0-fc07-8276
```

11.1.10 ap data-collection enable

Function

The **ap data-collection enable** command enables the AP data caching function.

The **undo ap data-collection enable** command disables the AP data caching function and clears cached data.

By default, the AP data caching function is disabled.

Format

ap data-collection enable

undo ap data-collection enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AC needs to query performance statistics (such as AP and radio performance statistics, and STA association information on APs) from APs. The **ap data-collection enable** command can enable an AC to periodically query data on APs and cache obtained data. Upon the next data query, the AC can directly search for cached data without the need to wait for APs to return data. This greatly reduces timeout for querying AP-related statistics.

If there are a large number of APs and STAs on the AC, this function may occupy many memory resources and affect performance. Therefore, it is recommended that this function be disabled when statistics query is not required.

Precautions

After the **undo ap data-collection enable** command is executed, data of all APs is cleared. However, common Fit APs periodically report performance statistics. Therefore, even if the data cached on the device is cleared, the data can be queried after the APs periodically report data.

Example

Enable the AP data caching function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap data-collection enable
```

11.1.11 ap data-collection interval

Function

The **ap data-collection interval** command sets the AP data buffer duration.

The **undo ap data-collection interval** command restores the default AP data buffer duration.

By default, the device buffers AP data for 5 minutes.

Format

ap data-collection interval *interval*

undo ap data-collection interval

Parameters

Parameter	Description	Value
interval	Specifies the buffer duration.	The value is an integer that ranges from 5 to 60, in minutes.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the AP buffer duration on the device.

Example

Enable the device to buffer AP data and set the buffer duration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap data-collection enable
[HUAWEI-wlan-view] ap data-collection interval 57
```

11.1.12 ap modify

Function

The **ap modify** command changes information about an AP.

Format

ap modify *ap-id* **mac** *ap-mac*

Parameters

Parameter	Description	Value
ap-id	Specifies the ID of the AP to be replaced.	The AP ID must exist.
mac *ap-mac*	Specifies the MAC address of a new AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When AP hardware needs to be replaced, you can configure new AP information for an existing AP ID to prevent repetitive data configurations. In this way, the new

AP goes online using the ID of the original AP so that all data configurations of the original AP directly take effect on the new AP.

By default, you can run the **display ap** command to view the MAC address of an AP.

Precautions

This configuration enables the new AP to go online on the AC and interrupts services of the original AP.

The type of the new AP must be the same as that of the original AP.

Example

Specify the MAC address **00e0-fc12-3456** of a new AP for the AP ID 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap modify 0 mac 00e0-fc12-3456
Warning: Modify AP will influence the service that has published in AP, Whether to continue? [Y/N]y
```

11.1.13 ap rtu load

Function

The **ap rtu load** command unzips a right-to-use (RTU) license package and automatically delivers the unzipped RTU licenses to the corresponding APs.

NOTE

The RTU License is not supported by the following models.

- AirEngine x76x (Excluding the AirEngine 5760-51, AirEngine 6760-X1, AirEngine 6760-X1E)
- AirEngine x77x
- The cemtral AP (including matching RUs)
- AirEngine 9700D-S (including matching ORUs)

Format

ap rtu load filename *filename*

Parameters

Parameter	Description	Value
filename *filename*	Specifies the name of an RTU license package.	The value is a string of 1 to 64 case-sensitive characters. The package must be a .zip package and have the same name as the existing RTU license package.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RTU is an authorization mode for selling hardware capabilities in installments, such as the number of spatial streams, capacity, and ports. An RTU license cannot be migrated after being bound to a device. As a part of hardware value, RTU licenses have the same lifecycle and the same entitlement as the hardware. The quantities of spatial streams, antennas, and service ports have always been the indicators for a WLAN in the industry, among which the quantity of spatial streams is the most basic indicator. RTU licensing allows basic AP models to support features such as dual-band, three-radio, and independent scanning radio.

After applying for RTU licenses in batches, you will obtain an RTU license package. You need to manually upload the RTU license package to the AC, and then run this command to unzip the package and automatically deliver the RTU licenses to the corresponding APs.

Prerequisites

An RTU license package has been manually uploaded to the AC.

Configuration Impact

Executing this command will unzip the RTU license package locally on the device, with a list of RTU license files generated.

Precautions

To ensure that RTU-granted functions work properly, license files in the RTU license package must meet the following requirements:

- License files are .dat files downloaded from the Electronic Software Delivery Platform (ESDP).
- The name of a license file (including the file name extension) cannot exceed 64 characters.

Follow-up Procedure

Manually restart the APs to which the RTU licenses have been delivered so that these licenses can take effect.

Example

Unzip an RTU license package and automatically deliver the unzipped RTU licenses to the corresponding APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap rtu load filename rtu.zip
Info: This operation may take a few seconds. Please wait for a moment....done.
Info: Valid license file(s):2048, invalid license file(s):0
Warning: After the RTU file is downloaded to the AP, restart the AP to make RTU take effect.
```

11.1.14 ap whitelist

Function

The **ap whitelist** command adds APs to the AP whitelist.

The **undo ap whitelist** command deletes APs from the AP whitelist.

By default, no APs exist in the AP whitelist.

Format

ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }

undo ap whitelist { **mac** { *ap-mac1* [**to** *ap-mac2*] | **all** } | **sn** { *ap-sn1* [**to** *ap-sn2*] | **all** } }

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
to *ap-mac2*	Specifies the end MAC address during the batch operation. The value of *ap-mac2* must be larger than *ap-mac1*, and *ap-mac1* and *ap-mac2* together specify a range.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
sn *ap-sn1*	Specifies the SN of an AP.	The value is a string of 1 to 31 characters.
to *ap-sn2*	Specifies the end SN during the batch operation. The value of *ap-sn2* must be larger than *ap-sn1*, and *ap-sn1* and *ap-sn2* together specify a range.	The value is a string of 1 to 31 characters.
mac all	Deletes all MAC addresses from the whitelist.	-
sn all	Deletes all SNs from the whitelist.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- In MAC address authentication mode configured using the **ap auth-mode** command, if the MAC address of an AP exists in the whitelist, the AP automatically goes online, without the need of manual confirmation. If the MAC address of an AP is not in the whitelist and the AP has not been imported, the AP cannot automatically go online. In this case, you need to run the **ap-confirm** command to confirm the AP.
- When the AP authentication mode is set to SN authentication using the **ap auth-mode** command, if the SN of an online AP exists in the whitelist, the AP automatically goes online, without the need of manual confirmation. If the SN of an AP is not in the whitelist and the AP has not been imported, the AP cannot automatically go online. In this case, you need to run the **ap-confirm** command to confirm the AP.

Prerequisites

The AP authentication mode has been set to MAC address or SN authentication using the **ap auth-mode** command.

Precautions

When adding multiple SNs to the whitelist, ensure that the start SN length and the end SN length are the same.

Example

Add the AP with the MAC address of 00e0-fc07-8280 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist mac 00e0-fc07-8280
```

Add MAC addresses from 00e0-fc07-8270 to 00e0-fc07-8290 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist mac 00e0-fc07-8270 to 00e0-fc07-8290
```

Add the SN 08PE56430071 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist sn 08PE56430071
```

Add SNs from 08PE56430076 to 08PE56430081 to the AP whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap whitelist sn 08PE56430076 to 08PE56430081
```

11.1.15 ap-confirm

Function

The **ap-confirm** command confirms unauthenticated APs and allows them to go online.

Format

ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }

Parameters

Parameter	Description	Value
all	Confirms all APs.	-
mac *ap-mac*	Confirms the AP with the specified MAC address.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
sn *ap-sn*	Confirms the AP with the specified SN.	The value is a string of 1 to 31 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After viewing unauthenticated APs using the **display ap unauthorized record** command, you can run the **ap-confirm** command to confirm these unauthenticated APs if you want to connect them to the AC. After confirmation, the APs are allowed to go online, automatically added to the default region, and bound to the default AP profiles.

Example

Confirm the AP with the MAC address 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-confirm mac 00e0-fc12-3456
```

Confirm all APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-confirm all
```

11.1.16 ap-id

Function

The **ap-id** command imports an AP or displays the AP view.

By default, no AP is imported.

Format

ap-id *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }]

Parameters

Parameter	Description	Value
ap-id	Specifies an AP ID.	The value is an integer that ranges from 0 to 1023.
type-id *type-id*	Specifies an AP type ID.	The value is an integer that ranges from 0 to .
ap-type *ap-type*	Specifies an AP type.	The value is a string of 1 to 31 characters.
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-sn *ap-sn*	Specifies an AP SN.	The value is a string of 1 to 31 characters, and can only contain letters and digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set parameters for an AP imported successfully before it goes online. The parameter settings then take effect when the AP goes online.

To delete an AP, run the **undo ap** command.

Precautions

To add an AP, you must enter the MAC address, SN, or MAC address+SN of the AP. In MAC address authentication mode, enter the MAC address of the AP. In SN authentication mode, enter the SN of the AP.

To enter the AP view, you only need to enter the AP ID.

Example

Import an AP with the ID of 11, type ID of 125, and MAC address of 00e0-fc07-8270.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 11 type-id 125 ap-mac 00e0-fc07-8270
```

11.1.17 ap-mac

Function

The **ap-mac** command imports an AP or displays the AP view.

By default, no AP is imported.

Format

ap-mac *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*]

Parameters

Parameter	Description	Value
ap-mac	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
type-id *type-id*	Specifies an AP type ID.	The value is an integer that ranges from 0 to .
ap-type *ap-type*	Specifies an AP type.	The value is a string of 1 to 31 characters.
ap-id *ap-id*	Specifies an AP ID.	The value is an integer that ranges from 0 to 1023.
ap-sn *ap-sn*	Specifies an AP SN.	The value is a string of 1 to 31 characters, and can only contain letters and digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set parameters for an AP imported successfully before it goes online. The parameter settings then take effect when the AP goes online.

Precautions

When importing an AP, you must enter the MAC address of the AP. If the AP authentication mode is SN authentication, you also need to enter the SN of the AP.

To enter the AP view, you only need to enter the MAC address of the AP. If the specified MAC address does not exist, the system adds a new AP and displays the AP view.

The **ap-mac** *ap-mac* [[**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*]] and **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] commands have the same function. You can use either one according to the actual situation.

Example

Import the AP with the MAC address of 00e0-fc07-8260.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-mac 00e0-fc07-8260
```

11.1.18 association-timeout

Function

The **association-timeout** command configures the association aging time for STAs.

The **undo association-timeout** command restores the default association aging time of STAs.

By default, the association aging time of STAs is 5 minutes.

Format

association-timeout *association-timeout*

undo association-timeout

Parameters

Parameter	Description	Value
association-timeout	Specifies the association aging time of STAs.	The value is an integer that ranges from 1 to 30, in minutes.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrator can run this command to set the association aging time for STAs. If the AP receives no data packet from a STA in a specified time, the STA goes offline after the association aging time expires.

Precautions

Changing the association aging time of a STA may interrupt the STA services.

Example

Set the association aging time of STAs to 15 minutes in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] association-timeout 15
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.19 auto-off service

Function

The **auto-off service** command enables the scheduled VAP auto-off function and sets the time range within which the VAP is disabled.

The **undo auto-off service** command disables the scheduled VAP auto-off function.

By default, the scheduled VAP auto-off function is disabled.

Format

auto-off service start-time *start-time* **end-time** *end-time*

undo auto-off service

Parameters

Parameter	Description	Value
start-time *start-time*	Specifies the time when a VAP starts to be disabled.	The time is in hh:mm:ss format. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59.
end-time *end-time*	Specifies the time when a VAP stops being disabled.	The time is in hh:mm:ss format. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59.

Views

VAP profile view, 2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an enterprise does not want employees to access the internal WLAN from 01:00 to 05:00, the administrator can run the **auto-off service** command to enable the scheduled VAP auto-off function.

Precautions

- After the service mode of a VAP is enabled using the **undo service-mode disable** command, you can run the **auto-off service** command to configure the scheduled VAP auto-off function. In the scheduled time, the VAP is disabled and cannot be enabled using the **undo service-mode disable** command. To enable the VAP, run the **undo auto-off service** command.
- The scheduled VAP auto-off function takes effect in the scheduled time only after the **undo service-mode disable** command is executed. If the service mode of a VAP is disabled using the **service-mode disable** command, the VAP auto-off function does not take effect.

- The scheduled VAP auto-off function enabled in a VAP profile view takes effect only on the APs using the VAP profile, and the scheduled VAP auto-off function enabled in a radio profile view takes effect only on the APs using the radio profile.

Example

Configure the scheduled VAP auto-off function in the VAP profile **vap1**, and configure the VAP to be disabled from 1:00:00 to 7:00:00.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] auto-off service start-time 1:00:00 end-time 7:00:00
```

11.1.20 beacon-2g-rate

Function

The **beacon-2g-rate** command sets the transmit rate of 2.4 GHz management frames (including Beacon frames, Probe Response frames, Assoc/Reassoc Response frames, and Auth frames).

The **undo beacon-2g-rate** command restores the default transmit rate of 2.4 GHz management frames.

By default, the transmit rate of 2.4 GHz management frames is 5.5 Mbit/s.

Format

beacon-2g-rate *beacon-2g-rate*

undo beacon-2g-rate

Parameters

Parameter	Description	Value
beacon-2g-rate	Specifies the transmit rate of management frames.	The value is of the enumerated type: ● 1: 1 Mbit/s ● 2: 2 Mbit/s ● 5.5: 5.5 Mbit/s ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 11: 11 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s

Views

SSID profile view, Mesh profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many management frames occupy a large number of wireless resources. To reduce wireless resource occupation of management frames and improve channel utilization, you can run the **beacon-2g-rate** command to set a high transmit rate for 2.4 GHz management frames.

Precautions

The 802.11b protocol supports only 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s, and 11 Mbit/s. If you set the transmit rate of management frames to a rate not supported by the 802.11b protocol, STAs supporting only 802.11b cannot connect to the wireless network.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, *beacon-2g-rate* that takes effect on the 2 GHz radio of the AP is fixed as 1 Mbit/s, and *beacon-2g-rate* configured in the SSID profile view does not take effect on the AP.

Example

Set the transmit rate of 2.4 GHz management frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] beacon-2g-rate 18
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.21 beacon-5g-rate

Function

The **beacon-5g-rate** command sets the transmit rate of 5 GHz management frames (including Beacon frames, Probe Response frames, Assoc/Reassoc Response frames, and Auth frames).

The **undo beacon-5g-rate** command restores the default transmit rate of 5 GHz management frames.

By default, the transmit rate of 5 GHz management frames is 6 Mbit/s.

Format

beacon-5g-rate *beacon-5g-rate*

undo beacon-5g-rate

Parameters

Parameter	Description	Value
beacon-5g-rate	Specifies the transmit rate of management frames.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

SSID profile view, Mesh profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many management frames occupy a large number of wireless resources. To reduce wireless resource occupation of management frames and improve channel utilization, you can run the **beacon-5g-rate** command to set a high transmit rate for 5 GHz management frames.

Example

Set the transmit rate of 5 GHz management frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] beacon-5g-rate 18
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.22 beacon-6g-rate

Function

The **beacon-6g-rate** command sets the transmit rate of 6 GHz management frames (including Beacon frames, Probe Response frames, Assoc/Reassoc Response frames, and Auth frames).

The **undo beacon-6g-rate** command restores the default transmit rate of 6 GHz management frames.

By default, the transmit rate of 6 GHz management frames is 6 Mbit/s.

Format

beacon-6g-rate *beacon-6g-rate*

undo beacon-6g-rate

Parameters

Parameter	Description	Value
beacon-6g-rate	Specifies the transmit rate of management frames.	The value is of the enumerated type: ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s

Views

SSID profile view, Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many management frames occupy a large number of wireless resources. To reduce wireless resource occupation of management frames and improve channel utilization, you can run the **beacon-6g-rate** command to set a high transmit rate for 6 GHz management frames.

Example

Set the transmit rate of 6 GHz management frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] beacon-6g-rate 18
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.23 beacon-interval

Function

The **beacon-interval** command sets the interval for sending Beacon frames.

The **undo beacon-interval** command restores the default interval for an AP to send Beacon frames.

By default, the interval for sending Beacon frames is 100 TUs.

Format

beacon-interval *beacon-interval*

undo beacon-interval

Parameters

Parameter	Description	Value
beacon-interval	Specifies the interval for sending Beacon frames.	The value is an integer that ranges from 60 TUs to 1000 TUs. TU is a time unit equal to 1024 microseconds.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

An AP broadcasts Beacon frames at intervals to notify STAs of an existing 802.11 network. After receiving a Beacon frame, a STA can modify parameters used to connect to the 802.11 network.

A long interval for sending Beacon frames lengthens the dormancy time of STAs, while a short interval for sending Beacon frames increases air interface costs. Therefore, you are advised to set the interval for sending Beacon frames for an AP based on the VAP quantity. The following intervals for sending Beacon frames are recommended for APs with different VAP quantities on a single radio:

- No more than 4 VAPs: about 100 TUs
- 5 to 8 VAPs: about 200 TUs
- 9 to 12 VAPs: about 300 TUs
- 13 to 16 VAPs: about 400 TUs

Ensure that the air scan interval meets the following condition: scan-interval ≥ beacon-interval + 100 ms

Example

Set the interval for sending Beacon frames to 200 TUs in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] beacon-interval 200
```

11.1.24 beamforming disable

Function

The **beamforming disable** command disables the beamforming function.

The **undo beamforming disable** command enables the beamforming function.

By default, the beamforming function is enabled.

NOTE

This configuration takes effect only on APs running V200R019C10 or later.

Format

beamforming disable

undo beamforming disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Beamforming is a signal processing technique that controls signal transmission direction, and transmission and reception of radio signals. The transmit end uses weight to transmit signals. The signals are transmitted to the destination as narrow beams. Beamforming increases the demodulation signal-to-noise ratio (SNR) for the destination device.

Precautions

If nodes on a Mesh network are fixed and distant from each other, enable the beamforming function to increase the demodulation SNR of Mesh links. Mobile nodes may cause a low demodulation SNR of Mesh links in Mesh scenarios. Therefore, it is recommended that the beamforming function be disabled.

To use the MU-MIMO function, enable the beamforming function.

Example

Disable the beamforming function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] beamforming disable
```

11.1.25 beamforming enable

Function

The **beamforming enable** command enables the beamforming function.

The **undo beamforming enable** command disables the beamforming function.

By default, the beamforming function is disabled.

NOTE

This configuration takes effect only on APs running V200R019C00 or earlier.

Format

beamforming enable

undo beamforming enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Beamforming is a signal processing technique that controls signal transmission direction, and transmission and reception of radio signals. The transmit end uses weight to transmit signals. The signals are transmitted to the destination as narrow beams. Beamforming increases the demodulation signal-to-noise ratio (SNR) for the destination device.

Precautions

If nodes on a WDS or Mesh network are fixed and distant from each other, enable the beamforming function to increase the demodulation SNR of WDS or Mesh links. Mobile nodes may cause a low demodulation SNR of WDS or Mesh links in WDS or Mesh scenarios. Therefore, it is recommended that the beamforming function be disabled.

Example

Enable the beamforming function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] beamforming enable
```

11.1.26 capwap control-link-priority

Function

The **capwap control-link-priority** command configures the priority of CAPWAP management packets.

The **undo capwap control-link-priority** command restores the default priority of CAPWAP management packets.

The default priority of CAPWAP management packets is 7.

Format

capwap control-link-priority { **local** | **remote** } *priority-value*

undo capwap control-link-priority { **local** | **remote** }

Parameters

Parameter	Description	Value
local	Specifies the priority of CAPWAP management packets from the AC to the APs. The priority of CAPWAP management packets determines the reliability of links from the AC to APs.	-
remote	Priority of CAPWAP management packets from APs to the AC. The priority of CAPWAP management packets determines the reliability of links from APs to the AC.	-
priority-value	Specifies the priority of CAPWAP management packets.	The value is an integer that ranges from 0 to 7. The value 0 indicates the lowest priority, and the value 7 indicates the highest priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the DSCP priority of CAPWAP management packets. A higher priority indicates a more reliable link between the AC and APs.

The configuration of the priority of CAPWAP management packets from the AC to APs takes effect immediately. After the priority of CAPWAP management packets from an AP to the AC is changed, if the AP is online, the AC sends the priority to the AP in the Echo packet. If the AP is not online, the priority is delivered to the AP in the Echo packet when the AP goes online. The new priority takes effect immediately when the AP receives it.

Precautions

NOTICE

When setting the parameter **local** *priority-value* to configure the priority of CAPWAP management packets from the AC to APs, ensure that the value is in the range of 4 to 7 to prevent the management channel from being interrupted in case of heavy service traffic.

Example

Set the priority of CAPWAP management packets from the AC to APs to 6.

```
<HUAWEI> system-view
[HUAWEI] capwap control-link-priority local 6
```

11.1.27 capwap dtls control-link encrypt

Function

The **capwap dtls control-link encrypt** command configures DTLS encryption for CAPWAP control tunnels.

The **undo capwap dtls control-link encrypt** command restores the default configuration of DTLS encryption for CAPWAP control tunnels.

By default, DTLS encryption for CAPWAP control tunnels is disabled.

Format

capwap dtls control-link encrypt

undo capwap dtls control-link encrypt

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the Discovery phase of the CAPWAP tunnel establishment between the AP and AC, the AP obtains the AC IP address using the discovery mechanism. Then in the DTLS negotiation phase, a CAPWAP tunnel is established between the AP and AC based on this IP address. During this process, UDP packets transmitted over the CAPWAP tunnel are encrypted using DTLS.

After DTLS encryption is enabled on the local end, the local end authenticates the peer end using the configured authentication mode. After authentication succeeds, the local end negotiates a DTLS encryption key with the peer end based on the authentication mode to protect packets transmitted over the CAPWAP control tunnel. If the DTLS negotiation fails, the CAPWAP tunnel cannot be established.

Configuration Impact

After the configuration is modified, the AP and AC re-establish a CAPWAP tunnel.

Precautions

Before enabling this function, run the **capwap dtls psk** command to configure a PSK.

If this function is enabled on the peer end, authentication and DTLS encryption negotiation are still performed on the local end even if the function is disabled on the local end. If the local end fails the verification of the peer end, the CAPWAP tunnel fails to be established. To temporarily disable DTLS encryption on the local and peer ends, you can configure the function of establishing CAPWAP DTLS sessions in none authentication mode. However, this function brings security risks. Ensure that the peer and local ends are in a secure and trusted network environment. After the CAPWAP link is established, disable the function of establishing CAPWAP DTLS sessions in none authentication mode so that the local and peer ends reestablish a CAPWAP link in secure mode.

Example

Enable DTLS encryption for CAPWAP control tunnels.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls control-link encrypt
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]:y
```

11.1.28 capwap dtls cert-mandatory-match disable

Function

The **capwap dtls cert-mandatory-match disable** command disables the function of establishing CAPWAP DTLS sessions through the initial certificate.

The **undo capwap dtls cert-mandatory-match disable** command enables the function of establishing CAPWAP DTLS sessions through the initial certificate.

By default, the function of establishing CAPWAP DTLS sessions through the initial certificate is enabled.

Format

capwap dtls cert-mandatory-match disable

undo capwap dtls cert-mandatory-match disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If DTLS encryption for CAPWAP control tunnels has been enabled, when adding an AP running V200R021C00 or later, you can enable APs to establish DTLS sessions through the initial certificate so that they can properly go online. After the APs go online, they obtain new DTLS certificates to initiate DTLS sessions and go online again in secure mode. If high security is required, you can disable this function and use PSK authentication.

If an AP has been online on another WAC where the PSK for DTLS encryption is configured, the AP will fail to go online after being steered to the local WAC. In this case, you need to enable APs to establish DTLS sessions through the initial certificate so that they can properly go online. After the AP goes online, it obtains a new DTLS credential to establish a DTLS session and go online again in secure mode. Then, disable this function.

Example

Disable the function of establishing CAPWAP DTLS sessions through the initial certificate.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls cert-mandatory-match disable
```

11.1.29 capwap dtls no-auth enable

Function

The **capwap dtls no-auth enable** command enables the function of establishing CAPWAP DTLS sessions in none authentication mode.

The **undo capwap dtls no-auth enable** command disables the function of establishing CAPWAP DTLS sessions in none authentication mode.

By default, the function of establishing CAPWAP DTLS sessions in none authentication mode is disabled.

Format

capwap dtls no-auth enable

undo capwap dtls no-auth enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If DTLS encryption for CAPWAP control tunnels has been enabled, when adding an AP running a version earlier than V200R021C00, you can run this command to enable the AP to establish a DTLS session in none authentication mode so that the AP can properly go online. After the AP goes online, it obtains a new DTLS certificate to initiate a DTLS session in secure mode and go online again. To ensure network security, disable this function immediately after the AP goes online again to prevent unauthorized APs from accessing the network.

Example

Disable the function of establishing CAPWAP DTLS sessions in none authentication mode.

```
<HUAWEI> system-view
[HUAWEI] undo capwap dtls no-auth enable
```

11.1.30 capwap dtls psk

Function

The **capwap dtls psk** command configures a pre-shared key (PSK) used for DTLS encryption.

By default, no PSK used for DTLS encryption is configured.

Format

capwap dtls psk *psk-value*

Parameters

Parameter	Description	Value
psk-value	Specifies a PSK used for DTLS encryption.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#**) or a string of 8 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During CAPWAP tunnel establishment, an AP establishes a DTLS session with an AC. If DTLS encryption has been enabled for CAPWAP control, sent management packets will be encrypted using DTLS. When the PSK is used for DTLS encryption, this command can be used to modify the PSK value in the DTLS session.

Follow-up Procedure

Run the **capwap dtls control-link encrypt** command to enable DTLS encryption for CAPWAP control tunnels.

Precautions

After the **capwap dtls psk** command configuration is complete, the new PSK will be automatically synchronized to the online APs that are working properly, but the previous PSK still takes effect. The new PSK takes effect after these APs go online again.

Example

Set the PSK used for DTLS encryption to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls psk YsHsjx_202206
```

11.1.31 capwap echo

Function

The **capwap echo** command sets the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections.

The **undo capwap echo** command restores the default CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections.

By default, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 6.

If dual-link backup is enabled, the default number of CAPWAP heartbeat detections changes to 3.

Format

capwap echo { **interval** *interval-value* | **times** *times-value* } *

undo capwap echo { **interval** | **times** }

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the CAPWAP heartbeat detection interval, at which a detection packets are sent.	The value is an integer that ranges from 2 to 300, in seconds.
times *times-value*	Specifies the number of CAPWAP heartbeat detections. If no response is received after the specified number of times, the link is considered disconnected.	The value is an integer that ranges from 3 to 120.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined by CAPWAP, the AP and AC send handshake packets periodically to maintain the data channel and management channel between them. If the AP does not receive packets from the peer end within the specified number of heartbeat detection times, the AP considers that the link with the peer end is disconnected. The AP resets and releases the IP address. Then, the AP and AC reestablish a link. If the AC does not receive packets from the peer end within the specified number of heartbeat detection times, the AC disconnects the link and reports an error to the AP. After this command is executed, the AP and AC perform heartbeat detection based on the new configurations (including the detection interval and number of detections).

Precautions

If dual-link backup is enabled in a WDS scenario, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 3. In this case, the WDS link is unstable and cannot ensure normal user access. You need to run this command to set the CAPWAP heartbeat detection interval to 25 seconds and the number of CAPWAP heartbeat detections to 6.

After the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections are configured, the interval and the number of times for sending Echo packets are configured.

Radio traffic statistics packets are sent and received together with Echo packets.

If you set the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections smaller than the default values, the CAPWAP link reliability is degraded. If the two parameters are set too high, APs can go online only after a heartbeat timeout. Exercise caution when you set the values. The default values are recommended.

Example

Set the CAPWAP heartbeat detection interval to 30s and the number of CAPWAP heartbeat detections to 3.

```
<HUAWEI> system-view
[HUAWEI] capwap echo interval 30 times 3
```

11.1.32 capwap dtls cbc

Function

The **capwap dtls cbc enable** command configures the CAPWAP DTLS server to establish DTLS sessions with DTLS clients running earlier versions using the CBC cipher suite.

The **capwap dtls cbc disable** command disables the CAPWAP DTLS server from using the CBC cipher suite to establish DTLS sessions with DTLS clients running earlier versions.

By default, CAPWAP DTLS compatibility with the CBC cipher suite is disabled.

Format

capwap dtls cbc enable

capwap dtls cbc disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In versions earlier than V200R021C00, CAPWAP clients support only the DTLS CBC cipher suite, which poses security risks. To establish CAPWAP DTLS sessions with these clients, run this command to enable compatibility with earlier versions.

Precautions

This function can be used only after the weak-encryption-algorithm plug-in is installed.

After this function is enabled, the TLS1_TXT_PSK_WITH_AES_256_CBC_SHA algorithm suite is used to set up DTLS sessions with CAPWAP DTLS clients running a version earlier than V200R021C00, which poses security risks.

After this function is disabled, CAPWAP links established based on earlier DTLS versions are disconnected, which may interrupt services.

Example

Enable CAPWAP DTLS compatibility with the CBC cipher suite.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls cbc enable
```

11.1.33 capwap dtls version1.0

Function

The **capwap dtls version1.0 enable** command configures the CAPWAP DTLS server to establish DTLS 1.0 sessions with DTLS clients running earlier versions.

The **capwap dtls version1.0 disable** command disables the CAPWAP DTLS server from establishing DTLS 1.0 sessions with DTLS clients running earlier versions.

By default, CAPWAP compatibility with DTLS 1.0 is disabled.

Format

capwap dtls version1.0 enable

capwap dtls version1.0 disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In versions earlier than V200R021C00, CAPWAP clients support only the DTLS 1.0 version, which poses security risks. To establish CAPWAP DTLS sessions with clients that support only DTLS 1.0, run this command to enable compatibility with earlier versions.

Precautions

This function can be used only after the weak-encryption-algorithm plug-in is installed.

After this function is enabled, the DTLS 1.0 version is used to set up DTLS sessions with CAPWAP DTLS clients running a version earlier than V200R021C00, which poses security risks.

After this function is disabled, CAPWAP links established based on earlier DTLS versions are disconnected, which may interrupt services.

Example

Enable CAPWAP compatibility with DTLS 1.0.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls version1.0 enable
```

11.1.34 capwap echo-timeout trace logging

Function

The **capwap echo-timeout trace logging** command enables the Echo packet process trace and diagnostic log record functions upon AP Echo packet timeout.

The **undo capwap echo-timeout trace logging** command disables the Echo packet process trace and diagnostic log record functions upon AP Echo packet timeout.

By default, the Echo packet process trace and diagnostic log record functions are enabled upon AP Echo packet timeout.

Format

capwap echo-timeout trace logging

undo capwap echo-timeout trace logging

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **capwap echo-timeout trace logging** command, the Echo packet process is traced and diagnostic logs are recorded upon AP Echo packet timeout.

Example

s

Enable the Echo packet process trace and diagnostic log record functions upon AP Echo packet timeout.

```
<HUAWEI> system-view
[HUAWEI] capwap echo-timeout trace logging
```

11.1.35 capwap message-integrity psk

Function

The **capwap message-integrity psk** command configures a PSK used for checking integrity of CAPWAP packets.

The **undo capwap message-integrity psk** command restores the default PSK used for checking integrity of CAPWAP packets.

The default username and password are available in *WLAN Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

capwap message-integrity psk *psk-value*

undo capwap message-integrity psk

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK used for checking integrity of CAPWAP packets.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#**) or a string of 6 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CAPWAP packets are transmitted between the AC and APs. To prevent the packets from being forged or tampered with and prevent malformed packet attacks, you can configure integrity check of CAPWAP packets. When a PSK is used to check integrity of CAPWAP packets, you can run this command on the AC to configure a PSK.

NOTE

It is recommended that you change the PSK in a timely manner to ensure device security.

Follow-up Procedure

Run the **undo capwap message-integrity check disable** command to enable integrity check of CAPWAP packets.

Configuration Impact

After the configuration is complete, all online APs on the AC go offline.

Example

Set the PSK used for checking integrity of CAPWAP packets to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap message-integrity psk YsHsjx_202206
Warning: In a backup scenario, the PSK and status of CAPWAP message integrity check must be the same
between the master and backup e
nds. This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

11.1.36 capwap message-integrity check disable

Function

The **capwap message-integrity check disable** command disables integrity check of CAPWAP packets.

The **undo capwap message-integrity check disable** command enables integrity check of CAPWAP packets.

By default, integrity check of CAPWAP packets is enabled.

Format

capwap message-integrity check disable

undo capwap message-integrity check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CAPWAP packets are transmitted between the AC and APs. To prevent the packets from being forged or tampered with and prevent malformed packet attacks, you can configure integrity check of CAPWAP packets.

Configuration Impact

After the configuration is modified, all online APs on the AC go offline.

Example

Enable integrity check of CAPWAP packets.

```
<HUAWEI> system-view
[HUAWEI] capwap message-integrity check disable
Warning: In a backup scenario, the PSK and status of CAPWAP message integrity check must be the same
between the master and backup e
nds. This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

11.1.37 capwap sensitive-info psk

Function

The **capwap sensitive-info psk** command configures a PSK used for encrypting sensitive information.

The **undo capwap sensitive-info psk** command restores the default PSK used for encrypting sensitive information.

The default username and password are available in *WLAN Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

capwap sensitive-info psk *psk-value*

undo capwap sensitive-info psk

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK used for encrypting sensitive information.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#**) or a string of 6 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sensitive information exchanged between the AC and APs is encrypted, such as the FTP user name/password, AP login user name/password, and service configuration-related keys. You can run this command to modify the PSK used for encrypting sensitive information.

NOTE

It is recommended that you change the PSK in a timely manner to ensure device security.

After the configuration is complete, all online APs on the AC go offline and online again.

Precautions

In dual-link HSB and cold backup scenarios, ensure that the PSKs configured on the active and standby ACs are the same. Otherwise, APs cannot establish

CAPWAP tunnels with the standby ACs, causing the APs to go offline after an active/standby switchover.

When an AP is being upgraded on the AC, the PSK used for encrypting sensitive information cannot be changed.

Example

Set the PSK for encrypting sensitive information to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap sensitive-info psk YsHsjx_202206
Warning: This operation may cause devices using CAPWAP connections to go offline. Continue? [Y/N]:y
```

11.1.38 capwap source interface

Function

The **capwap source interface** command configures the interface used by the AC to establish a CAPWAP tunnel as the source interface of the AC.

The **undo capwap source interface** command disables the AC from using an interface as the source interface.

By default, no source interface is configured for the AC.

Format

capwap source interface { **loopback** *loopback-number* | **vlanif** *vlan-id* }

undo capwap source interface { **loopback** *loopback-number* | **vlanif** *vlan-id* }

Parameters

Parameter	Description	Value
loopback *loopback-number*	Configures a loopback interface as the source interface.	The value is an integer that ranges from 0 to 1023.
vlanif *vlan-id*	Configures a VLANIF interface as the source interface.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source IP address must be specified for each AC so that all access devices connected to the AC can learn this IP address for communication.

When the CAPWAP source interface or address is configured for the first time, the system checks whether security-related configurations exist, including the PSK for DTLS encryption, PSK for DTLS encryption of inter-AC tunnels, user name and password for logging in to the AP, and password for logging in to the global offline management VAP. The CAPWAP source interface or address can be successfully configured only when all these configurations exist; otherwise, the system prompts you to complete related configurations first.

Prerequisites

An IP address has been assigned to the specified loopback or VLANIF interface.

Precautions

A maximum of eight source interfaces can be configured.

If SVF is enabled, only one source interface can be configured.

When multiple source interfaces are configured, the management VLAN of the APs must be within the VLAN range corresponding to the source interfaces. Otherwise, the APs cannot go online.

The source interface cannot be bound to a VPN instance.

Changing the source interface configuration will clear statistics about CAPWAP packets in CPU attack defense.

Example

Configure a loopback interface as the source interface.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 20
[HUAWEI-LoopBack20] ip address 192.168.10.1 24
[HUAWEI-LoopBack20] quit
[HUAWEI] capwap source interface loopback 20
Set the DTLS PSK(contains 6-32 plain-text characters, or 48 or 68 cipher-text characters that must be a
combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z, digits, and
special characters):******

Set the DTLS inter-controller PSK(contains 6-32 plain-text characters, or 48 or 68 cipher-text characters that
must be a combination of at least two of the following: lowercase letters a to z, uppercase letters A to Z,
digits, and special characters):******

Set the user name for FIT APs(contains 4-31 plain-text characters, which can only include letters, digits and
underlines. And the first character must be a letter):admin

Set the password for FIT APs(plain-text password of 8-128 characters or cipher-text password of 48-188
characters that must be a combination of at least three of the following: lowercase letters a to z, uppercase
letters A to Z, digits, and special characters):********

Set the global temporary-management psk(contains 8-63 plain-text characters, or 48-108 cipher-text
characters that must be a combination of at least two of the following: lowercase letters a to z, uppercase
letters A to Z, digits, and special characters):********
```

Table 11-1 Description of the command output

Item	Description
Set the DTLS PSK	Configures the PSK for DTLS encryption.
Set the DTLS inter-controller PSK	Configures the PSK for DTLS encryption of inter-AC tunnels.
Set the user name for FIT APs Set the password for FIT APs	Configures the user name and password for logging in to the Fit AP.
Set the global temporary-management psk	Configures the password for logging in to the global offline management VAP, allowing users to connect to the offline management SSID in wireless mode.

11.1.39 channel

Function

(AP group radio view) The **channel** command configures the working bandwidth and channel for specified radios on all APs in an AP group.

(AP group radio view) The **undo channel** command restores the default working bandwidth and channel for specified radios on all APs in an AP group.

(AP radio view) The **channel** command configures the working bandwidth and channel for specified radios on an AP.

(AP radio view) The **undo channel** command restores the working bandwidth and channel on specified radios of an AP to those configured in the AP group radio view.

By default, the working bandwidth of a radio is 20 MHz, and no working channel is configured for a radio.

Format

channel { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** | **160mhz** | **320mhz** } *channel*

channel 80+80mhz *channel1 channel2*

undo channel

Parameters

Parameter	Description	Value
20mhz	Sets the working bandwidth of a radio to 20 MHz.	-
40mhz-minus	Sets the working bandwidth of a radio to 40 MHz Minus.	-
40mhz-plus	Sets the working bandwidth of a radio to 40 MHz Plus.	-
80mhz	Sets the working bandwidth of a radio to 80 MHz.	-
160mhz	Sets the working bandwidth of a radio to 160 MHz.	-
320mhz	Sets the working bandwidth of a radio to 320 MHz.	-
80+80mhz	Sets the working bandwidth of a radio to 80+80 MHz.	-
channel/ channel1/ channel2	Specifies the working channel of a radio.	The parameter is an enumeration value. The value range is determined based on the country code and radio mode.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different radios use different channels. Channels for radios also vary in different countries and regions. Select channels based on the actual situations.

Precautions

The channel parameter settings must match the radio frequency band. For details about mappings between channel parameters and frequency bands, see *Country Codes & Channels Compliance*. You can obtain this table at Huawei technical support website.

- Enterprise technical support website: **https://support.huawei.com/enterprise**

- Carrier technical support website: **https://support.huawei.com**

The configured channels must be supported by STAs; otherwise, the STAs cannot discover radio signals.

If an AP detects radar signals on a channel, the channel cannot be configured as the radio channel of the AP in 30 minutes. However, the channel can be configured as the radio channel of other APs that do not detect radar signals on it.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

If two radios of an AP work on the 5 GHz frequency band, the operating channels of the two 5 GHz radios must be separated by at least one channel to avoid interference. If two radios of an AP work on the 5 GHz and 6 GHz frequency bands, respectively, pay attention to channel planning as follows:

- For the model AirEngine 6761-22T: Do not use a 5 GHz high-frequency channel (149–165) and a 6 GHz low-frequency channel (80 MHz channels 1–13, 160 MHz channels 1–29) at the same time.
- For the model AirEngine 8771-X1T: Do not use a 5 GHz high-frequency channel (20 MHz channels 153–165, 40 MHz channels 132–161, 80 MHz channels 132–161, 160 MHz channels 100–128, 320 MHz channels 100–144) and a 6 GHz channel (160 MHz channels 1–29, 320 MHz channels 1–61) at the same time.

For example, a country supports 40 MHz+ 5G channels 36, 44, 52, and 60. When deploying 5 GHz radio channels, if one radio is deployed to work on channel 36, it is recommended that channel 52 or 60 be configured for the other radio. Channel 44 is not recommended in this case.

NOTE

- You can configure the 80 MHz, 160 MHz, 320 MHz, or 80+80 MHz bandwidth only in the 5G radio view. When 320 MHz bandwidth is configured on the 5 GHz frequency band, the available channels are fixed at 100–144 that operate with 240 MHz bandwidth.

Example

Set the working bandwidth to 20 MHz and channel to 6 for radio 0 of AP 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.40 channel-switch announcement disable

Function

The **channel-switch announcement disable** command disables an AP from sending an announcement when the channel is switched.

The **undo channel-switch announcement disable** command enables an AP to send an announcement when the channel is switched.

By default, an AP sends an announcement when the channel is switched.

Format

channel-switch announcement disable

undo channel-switch announcement disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

When the AP works on a Depth First Select (DFS) channel, a radar detection is performed. The AP automatically switches to another channel because the DFS channel frequency may interfere with the radar frequency.

After the **undo channel-switch announcement disable** command is run, if the AP channel switches, the AP sends an Action frame to instruct STAs to switch channels after multiple Beacon intervals. The AP also switches the channel after the same intervals. The AP and STAs switch channels at the same time to prevent STA reassociations and ensure rapid service recovery.

NOTE

The channel switching announcement function must be supported by both the AP and STA.

The following APs do not send Action frames during channel switching announcement. Instead, these APs carry information in Beacon frames to instruct STAs to switch channels.

- AirEngine 9700D-S (including matching ORUs)
- AirEngine X77X
- AirEngine X76X

Example

Disable the AP from sending an announcement after the channel is switched.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] channel-switch announcement disable
```

11.1.41 channel-switch mode

Function

The **channel-switch mode** command configures an announcement mode for channel switching.

The **undo channel-switch mode** command restores the default announcement mode for channel switching.

By default, data transmission from STAs continues on the current channel when the channel is switched.

Format

channel-switch mode { **stop-transmitting** | **continue-transmitting** }

undo channel-switch mode

Parameters

Parameter	Description	Value
stop-transmitting	Stops data transmission from STAs on the current channel during channel switching.	-
continue-transmitting	Continues data transmission from STAs on the current channel during channel switching.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

During channel switching, STA communication is interrupted. The administrator can stop an associated STA sending data on the current channel until channel switching is complete. Alternatively, data transmission from STAs can be continued on the current channel before channel switching is complete.

Example

Stop data transmission from STAs on the current channel during channel switching.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] channel-switch mode stop-transmitting
```

11.1.42 copy-from

Function

The **copy-from** command copies data to the current profile from a profile of the same type.

Format

copy-from *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the profile from which data is copied.	The profile name must already exist.

Views

All WLAN profile views except the WIDS profile, WIDS whitelist profile, and WIDS spoof SSID profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **copy-from** command to copy data to the current profile from a profile of the same type. This simplifies profile configuration and improves configuration efficiency.

- To create a profile that has the same configuration as an existing profile, enter the view of the profile to be created and run the **copy-from** command to copy data from the existing profile.
- To create a profile that has most configurations the same as an existing profile, enter the view of the new profile, run the **copy-from** command to copy data from the existing profile, and modify the different configurations.

Precautions

If the current profile is referenced by another profile, you cannot run the command to copy data to the current profile.

When the WAPI certificate or private key configuration exists in the security profile, you must manually perform the configuration instead of using this command to copy data.

When you copy a location profile, if the protocol used by APs to report information is set to HTTPS and the SSL policy (**private report-protocol https ssl-policy** *ssl-policy*) is specified, the configuration will not be copied.

Example

Create the VAP profile **test** and copy data from the profile **sample**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] copy-from sample
```

11.1.43 country-code

Function

The **country-code** command configures a country code.

The **undo country-code** command restores the default country code.

The default country code is **CN**.

Format

country-code *country-code*

undo country-code

Parameters

Parameter	Description	Value
country-code	Specifies a country code.	The value is a string of characters in enumerated type. For specific values, see **Table 11-2**.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Table 11-2 Country codes supported by ACs

Country Code	Country/Region
AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile
CN	China (default)
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia
EG	Egypt

Country Code	Country/Region
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GE	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong, China
HN	Honduras
HR	Croatia
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IS	Iceland
IT	Italy
JO	Jordan
JP	Japan
KE	Kenya
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania

Country Code	Country/Region
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Republic of North Macedonia
MO	Macao, China
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RS	Serbia
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia

Country Code	Country/Region
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Türkiye
TT	Trinidad and Tobago
TW	Taiwan, China
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

Usage Scenario

When an AC controls APs in different countries or regions, different country codes can be configured based on the regulatory domain profile to meet different radio requirements, such as power and channel specifications, in different countries or regions.

Configuration Impact

After the country code is changed in a regulatory domain profile, APs using the regulatory domain profile automatically restart if they run versions earlier than V200R020C00.

Example

Set the country code to **US** in the regulatory domain profile **region1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name region1
[HUAWEI-wlan-regulate-domain-region1] country-code us
Warning: Modifying the country code will clear the channel and power configurations of radios, and
requires the APs to be restarted if they run V200R019C10 or earlier. Continue?[Y/N]:y
```

11.1.44 coverage distance

Function

(AP group radio view) The **coverage distance** command configures the radio coverage distance parameter for all specified radios in an AP group.

(AP group radio view) The **undo coverage distance** command restores the default radio coverage distance parameter for all specified radios in an AP group.

(AP radio view) The **coverage distance** command configures the radio coverage distance parameter for an AP radio.

(AP radio view) The **undo coverage distance** command restores the configuration of the radio coverage distance parameter on an AP radio to that configured in the AP group radio view.

By default, the radio coverage distance parameter is 3 (unit: 100 m) for all radios.

Format

coverage distance *distance*

undo coverage distance

Parameters

Parameter	Description	Value
distance	Specifies the radio coverage distance parameter. Each distance parameter corresponds to a group of **slottime**, **acktimeout**, and **ctstimeout** values. You can configure the radio coverage distance based on the AP distance, so that APs adjust the **slottime**, **acktimeout**, and **ctstimeout** values accordingly.	The value is an integer that ranges from 1 to 400, in the unit of 100 meters.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, two APs may be deployed at a spacing of dozens of meters to dozens of kilometers. Therefore, the time to wait for ACK frames from the peer AP varies depending on the AP spacing. A proper ACK timeout setting can improve data transmission efficiency between APs.

You can configure the radio coverage distance parameter based on distances between APs. Based on this parameter, the APs can automatically adjust the values of **slottime**, **acktimeout**, and **ctstimeout** to improve data transmission efficiency.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the radio coverage distance parameter to 2 for radio 0 of AP 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] coverage distance 2
```

11.1.45 cpe-tunnel-profile (WLAN view)

Function

The **cpe-tunnel-profile** command creates a CPE tunnel profile and displays the CPE tunnel profile view, or displays the view of an existing CPE tunnel profile.

The **undo cpe-tunnel-profile** command deletes a CPE tunnel profile.

No default CPE tunnel profile is available in the system.

Format

cpe-tunnel-profile name *profile-name*

undo cpe-tunnel-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a CPE tunnel profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all CPE tunnel profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An EoGRE tunnel established between an AP and a CPE is also known as a CPE tunnel. A CPE tunnel profile is used to specify the parameters including the VLAN, GRE key, and GRE checksum used by the CPE tunnel.

Follow-up Procedure

Run the **cpe-tunnel-profile** command in the VAP profile view to bind the CPE tunnel profile to a VAP profile and run the **vap-profile** command to bind the VAP profile to an AP group, AP, AP radio, or AP group radio so that the CPE tunnel profile can take effect.

Precautions

- A CPE tunnel profile bound to a VAP profile cannot be deleted. To delete such a CPE tunnel profile, unbind it from the VAP profile first.

Example

Create the CPE tunnel profile **cpe1** and display the CPE tunnel profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cpe-tunnel-profile name cpe1
[HUAWEI-wlan-cpe-tunnel-prof-cpe1]
```

11.1.46 cpe-tunnel-profile (VAP profile view)

Function

The **cpe-tunnel-profile** command binds a CPE tunnel profile to a VAP profile.

The **undo cpe-tunnel-profile** command unbinds a CPE tunnel profile from a VAP profile.

By default, no CPE tunnel profile is bound to a VAP profile.

Format

cpe-tunnel-profile *profile-name*

undo cpe-tunnel-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a CPE tunnel profile.	The CPE tunnel profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

The EoGRE tunnel encapsulation function has been enabled on a CPE.

Usage Scenario

After a CPE tunnel profile is bound to a VAP profile, data packets of wired terminals connected to a CPE are transparently transmitted to the upper-layer wired network through the CPE tunnel.

Example

Create the CPE tunnel profile **cpe1** and bind it to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cpe-tunnel-profile name cpe1
[HUAWEI-wlan-cpe-tunnel-prof-cpe1] quit
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] cpe-tunnel-profile cpe1
```

11.1.47 deny-broadcast-probe enable

Function

The **deny-broadcast-probe enable** command configures an AP not to respond to broadcast Probe Request frames.

The **undo deny-broadcast-probe enable** command configures an AP to respond to broadcast Probe Request frames.

By default, an AP responds to broadcast Probe Request frames.

Format

deny-broadcast-probe enable

undo deny-broadcast-probe enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Probe Response frames occupy a large number of wireless resources. To reduce wireless resource occupation of the frames and improve channel usage efficiency, you can run the **deny-broadcast-probe enable** command to configure an AP not to respond to broadcast Probe Request frames.

Precautions

Configuring an AP not to respond to broadcast Probe Request frames may reduce channel scan efficiency of some STAs.

Example

Configure an AP not to respond to broadcast Probe Request frames.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] deny-broadcast-probe enable
```

11.1.48 destination (soft GRE profile view)

Function

The **destination** command configures the destination IP address for a soft GRE tunnel.

The **undo destination** command restores the default destination IP address of a soft GRE tunnel.

By default, no destination IP address is configured for a soft GRE tunnel.

Format

destination { **ip-address** *destination-ip-address* | **ipv6-address** *destination-ipv6-address* }

undo destination

Parameters

Parameter	Description	Value
ip-address *destination-ip-address*	Specifies the destination IPv4 address of a soft GRE tunnel.	The value is in dotted decimal notation.
ipv6-address *destination-ipv6-address*	Specifies the destination IPv6 address of a soft GRE tunnel.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Soft GRE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the soft GRE forwarding mode, you need to configure the destination IP address of the soft GRE tunnel, that is, the peer IP address of the tunnel, so that service data can be forwarded to the specified destination IP address.

Precautions

Ensure that the route between the AP and the destination IP address of the soft GRE tunnel is reachable.

The destination IP address of a soft GRE tunnel must be configured in a soft GRE profile. The destination IP addresses of different soft GRE profiles cannot be the same.

If the IP address type of the AP is different from the destination IP address type configured in the soft GRE profile, the AP cannot establish a soft GRE tunnel.

If this command is run more than once, the latest configuration overrides the previous one.

Example

Set the destination IP address of a soft GRE tunnel to 10.10.1.1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1] destination ip-address 10.10.1.1
```

11.1.49 dhcp client option12

Function

The **dhcp client option12** command enables or disables DHCP packets sent by APs to carry the Option 12 field and specifies AP information contained in the Option 12 field.

The **undo dhcp client option12** command restores the default AP information in the Option 12 field carried in DHCP packets sent by APs.

By default, the Option 12 field carried in DHCP packets sent by an AP contains the AP type and MAC address.

Format

dhcp client option12 { **ap-name** | **ap-type ap-mac** | **disable** }

undo dhcp client option12

Parameters

Parameter	Description	Value
ap-name	Enables DHCP packets sent by APs to carry the Option 12 field that contains the AP name.	-
ap-type ap-mac	Enables DHCP packets sent by APs to carry the Option 12 field that contains the AP type and MAC address.	-
disable	Disables DHCP packets sent by APs from carrying the Option 12 field.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP (DHCP client) obtains an IP address through DHCP, this function enables the DHCP Discover and DHCP Request packets sent by the AP to carry the Option 12 field. The Option 12 field can contain the AP type, MAC address or the AP name. After the AP obtains an IP address through DHCP, you can check information about the AP with this IP address on the DHCP server that supports display of DHCP client host information.

Precautions

This function is valid only for the APs that obtain IP addresses through DHCP.

Example

Configure the AP name contained in the Option 12 field carried in DHCP packets sent by APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] dhcp client option12 ap-name
```

11.1.50 dhcp option82 insert enable

Function

The **dhcp option82 insert enable** command enables the function of adding the Option 82 field to DHCP packets sent by STAs.

The **undo dhcp option82 insert enable** command disables the function of adding the Option 82 field to DHCP packets sent by STAs.

By default, the function of adding the Option 82 field to DHCP packets sent by STAs is disabled.

Format

dhcp option82 insert enable

undo dhcp option82 insert enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After going online, a STA obtains the IP address through DHCP. When the DHCP Request packet from the STA reaches an AP, the AP adds the Option 82 field to the packet and sends the packet to the DHCP server. The Option 82 field contains the MAC address or SSID of the associated AP. Therefore, the DHCP server knows the AP on which the STA goes online.

Prerequisites

Before enabling the function of adding the Option 82 field to DHCP packets sent by STAs, run the **undo learn-client-address disable** command to enable the STA IP address learning. By default, STA IP address learning is enabled.

Example

Enable the function of adding the Option 82 field to DHCP packets sent by STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] dhcp option82 insert enable
```

11.1.51 dhcp option82 format (VAP profile view)

Function

The **dhcp option82 format** command configures the format of the Option 82 field in DHCP messages sent from STAs.

The **undo dhcp option82 format** command restores the default format of the Option 82 field in DHCP messages sent from STAs.

By default, the format of the Option 82 field in DHCP messages sent from STAs is **ap-mac**.

Format

dhcp option82 { **circuit-id** | **remote-id** } **format** { **ap-mac** [**mac-format** { **normal** | **compact** | **hex** | **colon** }] [**user-defined** *text*] | **ap-mac-ssid** [**mac-format** { **normal** | **compact** | **colon** }] [**user-defined** *text*] | **user-defined** *text* | **ap-name** [**user-defined** *text*] | **ap-name-ssid** [**user-defined** *text*] | **ap-location** [**user-defined** *text*] | **ap-location-ssid** [**user-defined** *text*] }

dhcp option82 { **remote-id** | **circuit-id** } **format** { **ap-group-ap-mac** | **ap-group-ap-mac-ssid** } **mac-format** { **normal** | **compact** | **colon** } [**user-defined** *text*]

dhcp option82 { **remote-id** | **circuit-id** } **format** { **ap-group** | **ap-group-ap-name** | **ap-group-ap-name-ssid** | **ap-group-ap-location** | **ap-group-ap-location-ssid** } [**user-defined** *text*]

undo dhcp option82 { **circuit-id** | **remote-id** } **format**

Parameters

Parameter	Description	Value
circuit-id	Specifies the circuit-ID in the Option 82 field.	-
remote-id	Specifies the remote-ID in the Option 82 field.	-

Parameter	Description	Value
ap-mac	Indicates that Option 82 contains the AP's MAC address.	-
ap-mac-ssid	Indicates that Option 82 contains the AP's MAC address and SSID.	-
mac-format	Specifies the format of the AP's MAC address in Option 82.	-
normal	Sets the MAC address format to xx-xx-xx-xx-xx-xx.	-
compact	Sets the MAC address format to xxxx-xxxx-xxxx.	-
hex	Sets the MAC address format to XXXXXXXXXXXX in hexadecimal notation.	-
colon	Sets the MAC address format to xx:xx:xx:xx:xx:xx.	-
user-defined *text*	Specifies the user-defined format of Option 82.	The value is a string of 1 to 255 characters.
ap-name	Indicates that Option 82 contains the AP name.	-
ap-name-ssid	Indicates that Option 82 contains the AP name and SSID.	-
ap-location	Indicates that Option 82 contains the AP location.	-
ap-location-ssid	Indicates that Option 82 contains the AP location and SSID.	-
ap-group	Indicates that Option 82 contains the AP group name.	-
ap-group-ap-mac	Indicates that Option 82 contains the AP group name and AP's MAC address.	-
ap-group-ap-mac-ssid	Indicates that Option 82 contains the AP group name, AP's MAC address, and SSID.	-

Parameter	Description	Value
ap-group-ap-name	Indicates that Option 82 contains the AP group name and AP name.	-
ap-group-ap-name-ssid	Indicates that Option 82 contains the AP group name, AP name, and SSID.	-
ap-group-ap-location	Indicates that Option 82 contains the AP group name and AP location.	-
ap-group-ap-location-ssid	Indicates that Option 82 contains the AP group name, AP location, and SSID.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

After the function of adding the Option 82 field to DHCP messages sent from STAs, you can run the **dhcp option82 format** command to configure the format of the Option 82 field.

You can use the following keywords to define the Option 82 field:

- ap-mac: indicates the AP's MAC address. After DHCP messages from a STA reach an AP, the AP inserts its MAC address into the Option 82 field of the DHCP messages.
- ap-mac-ssid: indicates the MAC address and SSID of the AP. After DHCP messages from a STA reach an AP, the AP inserts its MAC address and SSID associated with the STA into the Option 82 field of the DHCP messages.
- ap-name: indicates the AP name. After DHCP messages from a STA reach an AP, the AP inserts its name into the Option 82 field of the DHCP messages.
- ap-name-ssid: indicates the AP name and SSID. After DHCP messages from a STA reach an AP, the AP inserts its name and associated SSID into the Option 82 field of the DHCP messages.
- ap-location: indicates the AP location. After DHCP messages from a STA reach an AP, the AP inserts its location into the Option 82 field of the DHCP messages.
- ap-location-ssid: indicates the AP location and SSID. After DHCP messages from a STA reach an AP, the AP inserts its location and associated SSID into the Option 82 field of the DHCP messages.
- ap-group: indicates the AP group name. After DHCP messages from a STA reach an AP, the AP inserts the name of the AP group to which it belongs into the Option 82 field of the DHCP messages.

- ap-group-ap-mac, ap-group-ap-mac-ssid, ap-group-ap-name, ap-group-ap-name-ssid, ap-group-ap-location, ap-group-ap-location-ssid: indicates the combination of the AP group name and other keywords. After DHCP messages from a STA reach an AP, the AP inserts the name of the AP group to which it belongs and information specified by other keywords into the Option 82 field of the DHCP messages.

If **mac-format** is not specified in the **dhcp option82** { **circuit-id** | **remote-id** } **format** { **ap-mac** | **ap-mac-ssid** } command, the AP's MAC address in the Option 82 field is **XXXXXXXXXXXX** in ASCII format.

The total length of the **circuit-id** and **remote-id** options in the Option 82 field cannot exceed 255 bytes. Otherwise, some Option 82 information may be lost. Note that a Chinese character may occupy 2 or 3 bytes.

Example

Set the format of the remote-ID suboption in Option 82 carried in DHCP messages sent from STAs to **ap-mac-ssid**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] dhcp option82 remote-id format ap-mac-ssid
```

11.1.52 display ac global configuration

Function

The **display ac global configuration** command displays AC global configuration.

Format

display ac global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view AC global information.

Example

Display AC global configuration.

```
<HUAWEI> display ac global configuration
------------------------------------------------------------------------------
AC sysnetid                    : AC
------------------------------------------------------------------------------
```

Table 11-3 Description of the **display ac global configuration** command output

Item	Description
AC sysnetid	NE name of an AC. To configure the NE name for an AC, run the **ac sysnetid** command.

11.1.53 display ap

Function

The **display ap** command displays AP information.

Format

display ap { **all** | **ap-group** *ap-group* }

display ap [**ap-group** *ap-group*] **by-ssid** *ssid*

display ap by-state *state* [**ap-group** *ap-group*]

Parameters

Parameter	Description	Value
all	Displays information about all APs.	-
ap-group *ap-group*	Specifies the AP group to which an AP belongs.	The AP group must exist.
by-ssid *ssid*	Specifies an SSID.	The SSID must exist.

Parameter	Description	Value
by-state *state*	Displays the status of an AP.	The value is of the enumerated type: - **commit-failed**: Displays information about APs in configuration commitment failed state. - **committing**: Displays information about APs in configuration committing state. - **config**: Displays information about APs in configuration initialization state. - **config-failed**: Displays information about APs in initialization failed state. - **download**: Displays information about APs in system software downloading state. - **fault**: Displays information about APs that failed to go online. - **idle**: Displays information about APs in initialization state before the link is established for the first time.

Parameter	Description	Value
		- **name-conflicted**: Displays information about APs having duplicate names. - **normal**: Displays information about APs in normal state. - **standby**: Displays information about APs in standby state. - **ver-mismatch**: Displays information about APs with versions that do not match the AC version. - **countrycode-mismatch**: Displays information about APs with country codes that do not match the AC's country code. - **type-mismatch**: Displays information about APs with types that are different from the actual types.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about APs, run this command.

Example

Display information about all APs.

```
<HUAWEI> display ap all
Total AP information:
nor  : normal          [2]
ExtraInfo : Extra information
P    : insufficient power supply
D    : data link exception
---------------------------------------------------------------------------------------------------
ID   MAC            Name   Group      IP              Type                  State STA Uptime      ExtraInfo Scene
---------------------------------------------------------------------------------------------------
0    00e0-fcf6-76a0 area_1 ap-group1 192.168.120.254 AirEngine8760-X1-PRO   nor   0   4H:49M:11S
P         -
1    00e0-fc74-9640 area_2 ap-group1 192.168.120.253 AirEngine8760-X1-PRO   nor   0   6H:3M:40S
-         -
---------------------------------------------------------------------------------------------------
Total: 2
```

Display information about APs bound to the SSID **guest-wlan**.

```
<HUAWEI> display ap by-ssid guest-wlan
Total AP information:
nor  : normal          [2]
ExtraInfo : Extra information
P  : insufficient power supply
D    : data link exception
---------------------------------------------------------------------------------------------------
ID   MAC            Name   Group      IP              Type                  State STA Uptime      ExtraInfo Scene
---------------------------------------------------------------------------------------------------
0    00e0-fcf6-76a0 area_1 ap-group1 192.168.120.254 AirEngine8760-X1-PRO   nor   0   4H:49M:11S
P         -
1    00e0-fc74-9640 area_2 ap-group1 192.168.120.253 AirEngine8760-X1-PRO   nor   0   6H:3M:40S
-         -
---------------------------------------------------------------------------------------------------
Total: 2
```

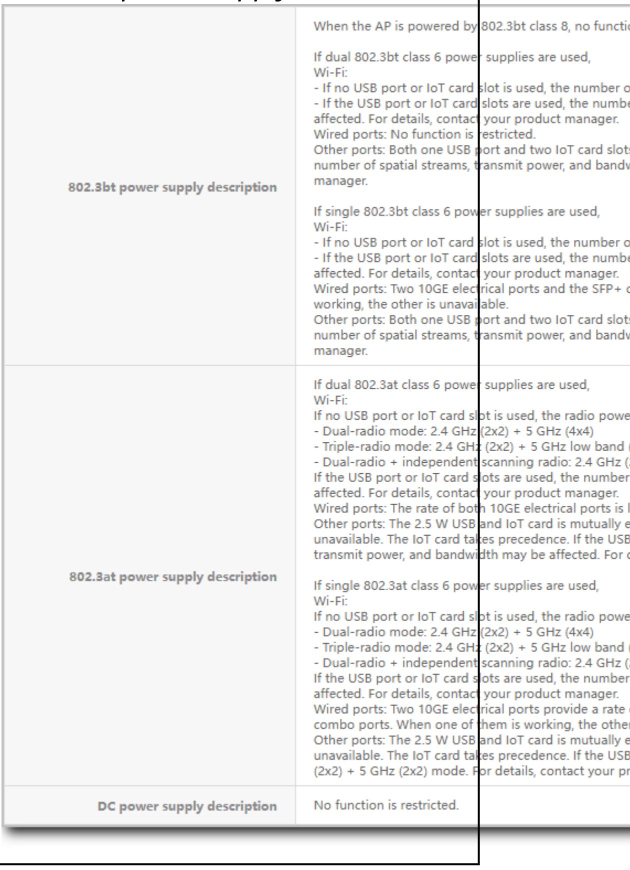
Display information about APs in normal state.

```
<HUAWEI> display ap by-state normal
Total AP information:
nor  : normal          [2]
ExtraInfo : Extra information
P  : insufficient power supply
D    : data link exception
---------------------------------------------------------------------------------------------------
ID   MAC            Name   Group      IP              Type                  State STA Uptime      ExtraInfo Scene
---------------------------------------------------------------------------------------------------
0    00e0-fcf6-76a0 area_1 ap-group1 192.168.120.254 AirEngine8760-X1-PRO   nor   0   4H:49M:11S
P         -
1    00e0-fc74-9640 area_2 ap-group1 192.168.120.253 AirEngine8760-X1-PRO   nor   0   6H:3M:40S
-         -
---------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-4 Description of the **display ap** command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.

Item	Description
Name	AP name.
Group	Name of the AP group to which an AP belongs.
IP	IP address of an AP.
Type	AP type.
State	AP state. For details, see **Table 11-5**.
STA	Number of STAs connected to an AP.
Uptime	Online duration of an AP.

Item	Description
ExtraInfo	Extra information. - **-**: indicates that no extra information is configured. - **P: insufficient power supply**: indicates that the AP is working in Limited or Insufficient state due to insufficient power supply and some functions are limited or unavailable. For the specific mode, you can run the **display ap power-workmode** command to check the value of the **Power-workmode** field. When the power supply is insufficient, the impact on the AP functions and performance varies depending on AP models. For Huawei AirEngine series APs: Check the power supply downgrade limit as follows: Visit **Info-Finder**, select a product series, and view hardware specifications in the hardware center. You can check the power supply downgrade limits at different power supply levels.  **802.3bt power supply description** When the AP is powered by 802.3bt class 8, no functi If dual 802.3bt class 6 power supplies are used, Wi-Fi: - If no USB port or IoT card slot is used, the number o - If the USB port or IoT card slots are used, the numbe affected. For details, contact your product manager. Wired ports: No function is restricted. Other ports: Both one USB port and two IoT card slots number of spatial streams, transmit power, and bandw manager. If single 802.3bt class 6 power supplies are used, Wi-Fi: - If no USB port or IoT card slot is used, the number o - If the USB port or IoT card slots are used, the numbe affected. For details, contact your product manager. Wired ports: Two 10GE electrical ports and the SFP+ c working, the other is unavailable. Other ports: Both one USB port and two IoT card slots number of spatial streams, transmit power, and bandw manager. **802.3at power supply description** If dual 802.3at class 6 power supplies are used, Wi-Fi: If no USB port or IoT card slot is used, the radio powe - Dual-radio mode: 2.4 GHz (2x2) + 5 GHz (4x4) - Triple-radio mode: 2.4 GHz (2x2) + 5 GHz low band (- Dual-radio + independent scanning radio: 2.4 GHz (If the USB port or IoT card slots are used, the number affected. For details, contact your product manager. Wired ports: The rate of both 10GE electrical ports is l Other ports: The 2.5 W USB and IoT card is mutually e unavailable. The IoT card takes precedence. If the USB transmit power, and bandwidth may be affected. For c If single 802.3at class 6 power supplies are used, Wi-Fi: If no USB port or IoT card slot is used, the radio powe - Dual-radio mode: 2.4 GHz (2x2) + 5 GHz (4x4) - Triple-radio mode: 2.4 GHz (2x2) + 5 GHz low band (- Dual-radio + independent scanning radio: 2.4 GHz (If the USB port or IoT card slots are used, the number affected. For details, contact your product manager. Wired ports: Two 10GE electrical ports provide a rate c combo ports. When one of them is working, the other Other ports: The 2.5 W USB and IoT card is mutually e unavailable. The IoT card takes precedence. If the USB (2x2) + 5 GHz (2x2) mode. For details, contact your pr **DC power supply description** No function is restricted.

Item	Description
	- **D: data link exception**: indicates that data links of RUs have not been established. Check the network connection between the AC and RUs.
Scene	Effective scenario profile on the AP. To configure this parameter, run the **scene** command. **-** indicates that no scenario profile is configured.
Total	Total number of queried APs.

Table 11-5 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed (cmtfa)	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are performed for the AP. If the link between the AP and AC is disconnected or the peer end has no response, the AP enters the commit-failed state.	Check the network connection.
committing (cmt)	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are being delivered to the AP. During this process, the AP is in committing state.	This is a normal state, and no action is required.
config (cfg)	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. During this process, the AP is in config state.	This is a normal state, and no action is required.

AP State	Description	Possible Cause	Handling Suggestion
config-failed (cfgfa)	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. If the configuration delivery fails due to various reasons (such as link disconnection), the AP enters the config-failed state.	Check the network connection.
download (dload)	An AP is in upgrade state.	When an AP is performing an upgrade, it enters the download state.	When the AP upgrade is complete, check the AP state.
fault	An AP fails to go online.	An AP fails to go online, which is usually caused by the following: ● The AP fails to obtain an IP address or obtains an incorrect IP address. ● The network between the AP and AC is faulty. ● The AP fails to be authenticated. ● The number of APs on an AC has reached the maximum value. ● The AP is faulty. ● In dual-link cold backup or N+1 backup scenario, if the link between the active and standby ACs is established properly, an AP that goes online on the active AC is in fault state on the standby AC.	Handle the AP online failure. For details, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

AP State	Description	Possible Cause	Handling Suggestion
idle	It is the initialization state of an AP before it establishes a link with the AC for the first time.	When an AP has not established a CAPWAP link with the AC, the MAC address and SN of an AP that is added offline are different from the actual MAC address and SN of the AP, or the AC cannot manage an AP due to license resource insufficiency, the AP enters the idle state.	Perform the following operations. Check whether the AP is connected to the network. If the AP connection is normal, go to next step. Check the MAC address and SN of the AP that is added offline are different from the actual MAC address and SN of the AP. If not, perform the following operations: 1. Run the **display ap all** command to check AP information. 2. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** } command to delete the AP. 3. Run the **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] or **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] command to add correct AP information. If the fault persists, expand the license capacity. Note that RUs managed by the AC do not occupy

AP State	Description	Possible Cause	Handling Suggestion
			license resources of the AC.
name-conflicted (namec)	The name of an AP conflicts with that of an existing AP.	The name of an AP conflicts with the name of another AP that has been online on the same AC.	Run the **ap-rename ap-id** *ap-id* **new-name** *ap-new-name* command to change the AP name.
normal (nor)	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby (stdby)	An AP is in normal state on the standby AC.	In the HSB scenario, if the link between the master and backup ACs is established properly, an AP is in standby state on the backup AC and in normal state on the master AC.	This is a normal state, and no action is required.
ver-mismatch (vmiss)	The version of an AP does not match that of an AC on which the AP is about to go online.	The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. ● Enterprise technical support website: **https://support.huawei.com/enterprise** ● Carrier technical support website: **https://support.huawei.com**

AP State	Description	Possible Cause	Handling Suggestion
countryCode-mismatch (cmiss)	The country codes of the AP and AC do not match.	The AP's current version does not support the country code configured on the AC. The country code of the AP is locked, and the country code configured on the AC is not supported.	The AP does not support the country code. Upgrade the AP or modify the country code configuration on the AC. The country code of the AP is locked. Replace the AP or change the country code on the AC to be the same as that of the AP.
type-mismatch (tmiss)	The AP type does not match that configured on the AC.	The AP type configured on the AC did not match the actual AP type.	Change the AP type configured on the AC.
unauth	An AP is not authenticated.	The AP fails to be authenticated.	Run the **display ap unauthorized record** command to query authenticated APs. Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.1.54 display ap blacklist

Function

The **display ap blacklist** command displays the AP blacklist.

Format

display ap blacklist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays APs in the blacklist. These APs are not allowed to go online on the AC. If an AP is online on the AC but is in the blacklist, the AP is brought offline.

Example

Display the AP blacklist.

```
<HUAWEI> display ap blacklist
--------------------------------------------------------------------------------
ID     MAC
--------------------------------------------------------------------------------
0      xxxx-xxxx-xxxx
--------------------------------------------------------------------------------
Total: 1
```

Table 11-6 Description of the **display ap blacklist** command output

Item	Description
ID	ID of the MAC address in the AP blacklist. The ID is generated automatically when the MAC address is specified.
MAC	MAC addresses of the APs that are not allowed to connect to the AC. To configure this parameter, run the **ap blacklist** command.

11.1.55 display ap config-info

Function

The **display ap config-info** command displays AP configuration.

Format

display ap config-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays configuration of the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays configuration of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap config-info** command to view AP configuration information, including the basic configuration, radio configuration, VAP configuration, and profile configuration.

Example

Display the configuration of the AP **ap1**.

```
<HUAWEI> display ap config-info ap-name ap1
------------------------------------------------------------------------------------
AP MAC                           : 00e0-fcxx-xxxx
AP SN                            : 2150083089xxxxxxxxxx
AP type                          : APxxxx
AP name                          : ap1
AP group                         : default
AP branch group                  :
Country code                     : CN
Scene                            : multi-partition-cross-room
------------------------------------------------------------------------------------
Radio 0 configurations:
 Radio enable                    : yes
 Work mode                       : normal
 WDS  mode                       : -
 Mesh mode                       : -
 Radio band                      : 2.4G
 Radio type                      : 11ax
 Flexible radio switch           : on
 Config channel/bandwidth        : -/20M
 Actual channel/bandwidth        : 11/20M
 Config EIRP                     : 127
 Actual EIRP                     : 31
 Maximum EIRP                    : 31
 CCA threshold(dBm)              : -75
 RX sensitivity(dBm)             : -100
 Beacon interval(TUs)            : 60
 Dynamic EDCA                    : enable
 Station load balance sta-number start threshold            : 10
 Station load balance sta-number gap threshold(number)      : 3
 Smart roam standing SNR threshold(dB)                      : 20
 Smart roam SNR quick-kickoff-threshold(dB)                 : 15
 Radio Calibration DCA 5G bandwidth                         : 40Mhz
 Radio Calibration TPC threshold(dBm):                      : -60
 Radio Calibrate grouping interference threshold(dBm)       : -70
 Radio Calibration maximum 2.4G calibration TX power(dBm)  : 127
 Radio Calibration maximum 5G calibration TX power(dBm)    : 127
```

```
 Radio Calibration minimum 2.4G calibration TX power(dBm)  : 9
 Radio Calibration minimum 5G calibration TX power(dBm)    : 12

 VAP configurations:
  WLAN ID 1:
   SSID                         : employee
   Forward mode                 : direct-forward
   Authen mode                  : WPA/WPA2-PSK
   Encrypt mode                 : AES
   Service vlan                 : 3
   Deny-broadcast-probe         : disable
   Active dull client           : disable
   Force active dull client     : disable
   Association timeout(min)     : 1
------------------------------------------------------------------------------------
Radio 1 configurations:
 Radio enable                   : yes
 Work mode                      : normal
 WDS  mode                      : -
 Mesh mode                      : -
 Radio band                     : 5G
 Radio type                     : 11ax
 Flexible radio switch          : on
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 157/20M
 Config EIRP                    : 127
 Actual EIRP                    : 30
 Maximum EIRP                   : 30
 CCA threshold(dBm)             : -75
 RX sensitivity(dBm)            : -100
 Beacon interval(TUs)           : 100
 Dynamic EDCA                   : enable
 Station load balance sta-number start threshold           : 10
 Station load balance sta-number gap threshold(number)     : 3
 Smart roam standing SNR threshold(dB)                     : 20
 Smart roam SNR quick-kickoff-threshold(dB)                : 15
 Radio Calibration DCA 5G bandwidth                        : 80Mhz
 Radio Calibration TPC threshold(dBm)                      : -35
 Radio Calibrate grouping interference threshold(dBm)      : -70
 Radio Calibration maximum 2.4G calibration TX power(dBm)  : 127
 Radio Calibration maximum 5G calibration TX power(dBm)    : 127
 Radio Calibration minimum 2.4G calibration TX power(dBm)  : 9
 Radio Calibration minimum 5G calibration TX power(dBm)    : 12

 VAP configurations:
  WLAN ID 1:
   SSID                         : employee
   Forward mode                 : direct-forward
   Authen mode                  : WPA/WPA2-PSK
   Encrypt mode                 : AES
   Service vlan                 : 3
   Deny-broadcast-probe         : disable
   Active dull client           : disable
   Association timeout(min)     : 1
------------------------------------------------------------------------------------
------------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
BLE profile                :
Site code                  :
AP location                :
Broadcaster content
  UUID                     : -
  Major                    : -
  Minor                    : -
  Reference RSSI           : -
Domain name                :
Ap pki profile             :
```

```
AP wired port profile
 Interface FE0              : default
 Interface FE1              : default
 Interface FE2              : default
 Interface FE3              : default
 Interface GE0              : default
 Interface GE1              : default
 Interface GE2              : default
 Interface GE3              : default
 Interface GE4              : default
 Interface GE5              : default
 Interface GE6              : default
 Interface GE7              : default
 Interface GE8              : default
 Interface GE9              : default
 Interface GE10             : default
 Interface GE11             : default
 Interface GE12             : default
 Interface GE13             : default
 Interface GE14             : default
 Interface GE15             : default
 Interface GE16             : default
 Interface GE17             : default
 Interface GE18             : default
 Interface GE19             : default
 Interface GE20             : default
 Interface GE21             : default
 Interface GE22             : default
 Interface GE23             : default
 Interface GE24             : default
 Interface GE25             : default
 Interface GE26             : default
 Interface GE27             : default
 Interface MultiGE0         : default
 Interface MultiGE2         : default
 Interface MultiGE3         : default
 Interface MultiGE4         : default
 Interface MultiGE5         : default
 Interface MultiGE6         : default
 Interface MultiGE7         : default
 Interface XGE0             : default
 Interface XGE1             : default
 Interface XGE2             : default
 Interface XGE3             : default
 Interface XGE4             : default
 Interface XGE5             : default
 Interface XGE6             : default
 Interface XGE7             : default
 Interface Eth-trunk0       : default
 Interface Eth-trunk1       : default
 Radio 0
  Radio 2.4G profile        : default
  Radio 5G profile          :
  VAP profile               :
  Mesh profile              :
  WDS profile               :
  Mesh whitelist profile    :
  WDS whitelist profile     :
  Location profile          :
 Radio switch               : enable
 Channel                    : -
 Channel bandwidth          : 20mhz
 EIRP(dBm)                  : 127
 Antenna gain(dB)           : -
 Coverage distance(100 m)   : 3
 Work mode                  : normal
 Flexible radio switch      : on
 Radio frequency            : 2.4G
 Spectrum analysis          : disable
```

```
 Channel monitor           : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Auto channel select       : enable
 Auto bandwidth select     : disable
 Auto transmit power select: enable
 Reference data-analysis   : enable
 Reference 3d-data         : enable
 Radio 1
  Radio 5G profile         : default
  VAP profile              :
  Mesh profile             :
  WDS profile              :
  Mesh whitelist profile   :
  WDS whitelist profile    :
  Location profile         :
 Radio switch              : enable
 Channel                   : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)                 : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Work mode                 : normal
 Flexible radio switch     : on
 Radio frequency           : 5G
 Spectrum analysis         : disable
 Channel monitor           : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Auto channel select       : enable
 Auto bandwidth select     : disable
 Auto transmit power select: enable
 Reference data-analysis   : enable
 Reference 3d-data         : enable
 Interference visualization: disable
Card 1
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card 2
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card 3
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card usb
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
```

```
Extended Port              : -
------------------------------------------------------------------------------------------
```

Table 11-7 Description of the **display ap config-info** command output

Item	Description
AP MAC	MAC address of an AP.
AP SN	SN of an AP.
AP type	AP type.
AP name	AP name. To configure this parameter, run the **ap-name (AP view)** or **ap-rename** command.
Domain name	Default domain name suffix of the AP. To configure this parameter, run the **ip domain-name** command.
AP group	AP group. To configure this parameter, run the **ap-group (AP view)** or **ap-regroup** command.
Country code	Country code. To configure this parameter, run the **country-code** command.
Scene	Effective scenario profile on the AP. To configure this parameter, run the **scene** command.
Radio x configurations	Radio configuration.
Radio enable	Whether a radio is enabled. To configure this parameter, run the **radio disable** command.
Work mode	Working mode of a radio. To configure this parameter, run the **work-mode** command.
WDS mode	WDS mode. To configure this parameter, run the **wds-mode** command.
Mesh mode	Mesh role of a radio. To configure this parameter, run the **mesh-role** command.

Item	Description
Radio band	Frequency band of a radio. To configure this parameter, run the **frequency** command.
Radio type	Protocol type of a radio.
Flexible radio switch	Whether the DFA function of a radio is enabled. To configure this parameter, run the **calibrate flexible-radio disable** command.
Config channel/bandwidth	Configured AP channel and bandwidth. To configure this parameter, run the **channel** command.
Actual channel/bandwidth	Actual AP channel and bandwidth.
Config EIRP	Transmit power of a radio configured in the radio profile. To configure this parameter, run the **eirp** command.
Actual EIRP	Actual transmit power of a radio.
Maximum EIRP	Maximum transmit power of a radio.
Radio Calibration DCA 5G bandwidth	5 GHz radio calibration bandwidth configuration obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
Radio Calibration TPC threshold(dBm)	Radio calibration power configuration obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
Radio Calibrate grouping interference threshold(dBm)	Interference threshold of a calibration group obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
CCA threshold(dBm)	CCA threshold for AP radios. To configure this parameter, run the **cca-threshold** command.

Item	Description
RX sensitivity(dBm)	Receiver sensitivity. To configure this parameter, run the **rx-sensitivity** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames. To configure this parameter, run the **beacon-interval** command.
Dynamic EDCA	Enabling status of dynamic EDCA obtained from the bound scenario profile. To configure this parameter, run the **scene** command.
Station load balance sta-number start threshold	Start threshold for dynamic load balancing based on the number of STAs. To configure this parameter, run the **sta-load-balance dynamic sta-number start-threshold** command.
Station load balance sta-number gap threshold(number)	Load difference threshold for dynamic load balancing based on the number of STAs. To configure this parameter, run the **sta-load-balance dynamic sta-number gap-threshold** command.
Smart roam standing SNR threshold(dB)	SNR threshold for smart roaming. To configure this parameter, run the **smart-roam roam-threshold { snr | rate }** command.
Smart roam SNR quick-kickoff-threshold(dB)	SNR threshold for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold** command.
Radio Calibration maximum 2.4G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power** command.

Item	Description
Radio Calibration maximum 5G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power radio-5g** command.
Radio Calibration minimum 2.4G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power** command.
Radio Calibration minimum 5G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power radio-5g** command.
VAP configurations	VAP configuration. VAP configuration is displayed only after a VAP profile is referenced by the AP.
WLAN ID 1	WLAN ID of a VAP. To configure this parameter, run the **vap-profile** command.
SSID	SSID name. To configure this parameter, run the **ssid** command.
Forward mode	Forwarding mode. To configure this parameter, run the **forward-mode** command.
Authen mode	Authentication mode.
Encrypt mode	Encryption mode.
Service vlan	Effective service VLAN.
Deny-broadcast-probe	Whether an AP is configured not to respond to broadcast Probe Request frames. To configure this parameter, run the **deny-broadcast-probe enable** command.

Item	Description
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure this parameter, run the **active-dull-client enable** command.
Force active dull client	Whether the function of forcibly preventing terminals from entering power-saving mode is enabled. To configure this parameter, run the **active-dull-client force enable** command.
Association timeout(min)	Specifies the association aging time of STAs. To configure this parameter, run the **association-timeout** command.
AP system profile	Name of the referenced AP system profile. To configure this parameter, run the **ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Name of the referenced regulatory domain profile. To configure this parameter, run the **regulatory-domain-profile** command.
WIDS profile	Name of the referenced WIDS profile.
BLE profile	Name of the referenced BLE profile. To configure this parameter, run the **ble-profile (AP group view and AP view)** command.
AP location	Installation position of an AP. To configure this parameter, run the **location** command.
UUID	UUID of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.

Item	Description
Major	Major field of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.
Minor	Minor field of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.
Reference RSSI	Reference RSSI of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP view)** command.
Ap pki profile	Bound AP PKI realm profile. To configure this parameter, run the **ap-pki-profile** command.
AP wired port profile	Name of the referenced AP wired port profile. To configure this parameter, run the **wired-port-profile (AP group view and AP view)** command.
Interface *interface-name*	Interface name and number.
Radio x	Radio.
Radio 2.4G profile	Name of the referenced 2G radio profile. To configure this parameter, run the **radio-2g-profile** command.
Radio 5G profile	Name of the referenced 5G radio profile. To configure this parameter, run the **radio-5g-profile** command.

Item	Description
VAP profile	Name of the referenced VAP profile. The displayed format is "VAP ID:VAP profile name (service VLAN defined when binding to the VAP profile, single VLAN, or VLAN pool)." To configure this parameter, run the **vap-profile** command.
Mesh profile	Name of the referenced Mesh profile. To configure this parameter, run the **mesh-profile radio** command.
WDS profile	Name of the referenced WDS profile. To configure this parameter, run the **wds-profile radio** command.
Mesh whitelist profile	Mesh whitelist profile referenced by an AP group. To configure this parameter, run the **mesh-whitelist-profile (AP group radio view or AP radio view)** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure this parameter, run the **wds-whitelist-profile (AP group radio view or AP radio view)** command.
Location profile	Name of the referenced location profile. To configure this parameter, run the **location-profile** command.
Radio switch	Whether a radio is enabled. To configure this parameter, run the **radio disable** command.
Channel	Working channel of a radio. To configure this parameter, run the **channel** command.
Channel bandwidth	Working bandwidth of a radio. To configure this parameter, run the **channel** command.
EIRP(dBm)	Transmit power of a radio, in dBm. To configure this parameter, run the **eirp** command.

Item	Description
Antenna gain(dB)	Antenna gain of a radio, in dB. To configure this parameter, run the **antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in the unit of 100 m. To configure this parameter, run the **coverage distance** command.
Work mode	Working mode of an AP. To configure this parameter, run the **work-mode** command.
Radio frequency	Working frequency band of a radio. To configure this parameter, run the **frequency** command.
Spectrum analysis	Whether spectrum analysis is enabled. To configure this parameter, run the **spectrum-analysis enable** command.
Channel monitor	Whether the function of monitoring the status of all channels is enabled. To configure this parameter, run the **channel-monitor enable** command.
WIDS device detect	Whether wireless device detection is enabled. To configure this parameter, run the **wids device detect enable** command.
WIDS attack detect	Whether attack detection is enabled. To configure this parameter, run the **wids attack detect** command.
WIDS contain switch	Whether rogue device containment is enabled. To configure this parameter, run the **wids contain enable** command.
Auto channel select	Whether automatic channel selection is enabled. To configure this parameter, run the **calibrate auto-channel-select** command.

Item	Description
Auto bandwidth select	Whether automatic bandwidth selection is enabled. To configure this parameter, run the **calibrate auto-bandwidth-select** command.
Auto transmit power select	Whether automatic transmit power selection is enabled. To configure this parameter, run the **calibrate auto-txpower-select** command.
Reference data-analysis	Whether big data calibration is enabled. To configure this parameter, run the **calibrate reference data-analysis { disable | enable }** command.
Reference 3d-data	Whether 3D radio calibration is enabled. To configure this parameter, run the **calibrate reference 3d-data { disable | enable }** command.
Interference visualization	Whether the interference visualization function is enabled. To configure this parameter, run the **interference-visualization enable** command.
Card 1/Card 2/Card 3/Card usb	IoT card.
Card connect type	Communication connection type between IoT cards and APs. To configure this parameter, run the **card connect-type** command.
Baud rate	Baud rate used for communication between an IoT card and the AP. To configure this parameter, run the **baud-rate** command.
Wired port profile	Bound AP wired port profile. To configure this parameter, run the **wired-port-profile (IoT card interface view)** command.

Item	Description
Iot profile	Bound IoT profile. To configure this parameter, run the **iot-profile (IoT card interface view)** command.
Protocol Type	Communication protocol between the AP and host computer.
First Port	Source port for the first channel.
Extended Port	Source port for the extended channel.

11.1.56 display ap configurable channel

Function

The **display ap configurable channel** command displays the configurable channels supported by a specified AP.

Format

display ap configurable channel { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays configurable channels supported by the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Displays configurable channels supported by the AP with the specified ID.	The AP ID must exist.
radio *radio-id*	Displays configurable channels supported by the specified radio.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Available wireless channels and power levels vary in different countries or regions. The country code configuration allows you to specify channels that can available on WLANs in the local country or region. You can run this command to view configurable channels supported by a specified AP.

Example

Display configurable channels supported by the AP named **test**.

```
<HUAWEI> display ap configurable channel ap-name test
2.4G 20M : 1,2,3,4,5,6,7,8,9,10,11,12,13.
2.4G 40M+: 1,2,3,4,5,6,7,8,9.
2.4G 40M-: 5,6,7,8,9,10,11,12,13.
5G   20M : 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165.
5G   40M+: 36,44,52,60,100,108,116,124,132,149,157.
5G   40M-: 40,48,56,64,104,112,120,128,136,153,161.
5G   80M : 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,149,153,157,161.
5G  160M : 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128.
5G 80+80M: 36+106, 36+122, 36+155, 40+106, 40+122, 40+155, 44+106, 44+122,
           44+155, 48+106, 48+122, 48+155, 52+106, 52+122, 52+155, 56+106,
           56+122, 56+155, 60+106, 60+122, 60+155, 64+106, 64+122, 64+155,
           100+42, 100+58, 100+155, 104+42, 104+58, 104+155, 108+42, 108+58,
           108+155, 112+42, 112+58, 112+155, 116+42, 116+58, 116+155, 120+42,
           120+58, 120+155, 124+42, 124+58, 124+155, 128+42, 128+58, 128+155,
           149+42, 149+58, 149+106, 149+122, 153+42, 153+58, 153+106, 153+122,
           157+42, 157+58, 157+106, 157+122, 161+42, 161+58, 161+106, 161+122.
6G   20M : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,
           93,97,101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,
           161,165,169,173,177,181,185,189,193,197,201,205,209,213,217,221,225,
       229,233
6G   40M+: 1,9,17,25,33,41,49,57,65,73,81,89,97,105,113,121,129,137,145,153,161,
           169,177,185,193,201,209,217,225
6G   40M-: 5,13,21,29,37,45,53,61,69,77,85,93,101,109,117,125,133,141,149,157,
           165,173,181,189,197,205,213,221,229
6G   80M : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,
           97,101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,161,
           165,169,173,177,181,185,189,193,197,201,205,209,213,217,221
6G  160M : 1,5,9,13,17,21,25,29,33,37,41,45,49,53,57,61,65,69,73,77,81,85,89,93,
           97,101,105,109,113,117,121,125,129,133,137,141,145,149,153,157,161,165,
           169,173,177,181,185,189,193,197,201,205,209,213,217,221
```

Table 11-8 Description of the **display ap configurable channel** command output

Item	Description
2.4G 20M	Configurable 20 MHz channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 2.4 GHz frequency band.
5G 20M	Configurable 20 MHz channels supported by the AP on the 5 GHz frequency band.
5G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 5 GHz frequency band.
5G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 5 GHz frequency band.

Item	Description
5G 80M	Configurable 80 MHz channels supported by the AP on the 5 GHz frequency band.
5G 160M	Configurable 160 MHz channels supported by the AP on the 5 GHz frequency band.
5G 80+80M	Configurable 80+80 MHz channels supported by the AP on the 5 GHz frequency band.
5G 320M	Configurable 320 MHz channels supported by the AP on the 5 GHz frequency band.
6G 20M	Configurable 20 MHz channels supported by the AP on the 6 GHz frequency band.
6G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 6 GHz frequency band.
6G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 6 GHz frequency band.
6G 80M	Configurable 80 MHz channels supported by the AP on the 6 GHz frequency band.
6G 160M	Configurable 160 MHz channels supported by the AP on the 6 GHz frequency band.
6G 320M	Configurable 320 MHz channels supported by the AP on the 6 GHz frequency band.

11.1.57 display ap global configuration

Function

The **display ap global configuration** command displays AP global configuration.

Format

display ap global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view AP global information.

Example

Display AP global configuration.

```
<HUAWEI> display ap global configuration
------------------------------------------------------------------------------
AP auth-mode                        : MAC-auth
AP LLDP switch                      : disable
AP username/password                : -/******
AP data collection                  : disable
AP data collection interval(minute): 5
------------------------------------------------------------------------------
```

Table 11-9 Description of the **display ap global configuration** command output

Item	Description
AP auth-mode	AP authentication mode. To configure this parameter, run the **ap auth-mode** command.
AP LLDP switch	Whether LLDP is enabled on an AP. To configure this parameter, run the **ap lldp enable** command.
AP username/password	User name and password for logging in to an AP. To configure this parameter, run the **ap username** command.
AP data collection	Whether data buffering is enabled on an AP. To configure this parameter, run the **ap data-collection enable** command.
AP data collection interval(minute)	AP data buffering interval. To configure this parameter, run the **ap data-collection interval** command.

11.1.58 display ap non-factory all

Function

The **display ap non-factory all** command displays Fat APs and cloud APs on the network.

Format

display ap non-factory all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the working mode of a Fit AP is switched to the Fat or cloud mode, the AP cannot be managed by the device. Fat or cloud APs detected on the current network can be displayed. Based on AP information, check whether the AP mode is switched by mistake.

Follow-up Procedure

If so, run the **ap manufacturer-config** command to switch the working mode of the AP to Fit.

Precautions

The device can detect Fat APs and cloud APs only when the following conditions are met:

- The IP address of an AP in non-Fit mode is not obtained through DHCP, or its IP address is obtained through DHCP but the AP does not obtain the AC address through the option field. In this scenario, the device can detect the AP as a non-Fit AP by the device when the AP is in the same LAN as the device.
- The IP address of an AP in non-Fit mode is obtained through DHCP, and the AP does not obtain the AC address through the option field. In this scenario, the device can detect the AP as a non-Fit AP by the device when the address for the device to manage the Fit AP is the same as the address specified in the option field.

Example

Display APs that operate in non-Fit mode on the network.

```
<HUAWEI> display ap non-factory all
Cnt: Manage FIT AP count
Mode: Actual mode/Config mode
----------------------------------------------------------------------------------------------------------------------------------------
-------
MAC           SN              IP              Type                 Mode        Cnt   Operate State     Record time
----------------------------------------------------------------------------------------------------------------------------------------
-------
00e0-fc11-2222  **********1        10.1.1.11         AirEngine8760-X1-PRO   FAT/-        1     waiting deliver
2023-07-22 17:23:17
```

```
00e0-fc11-2233  **********2        10.1.1.12        AirEngine8760-X1-PRO   CLOUD/CLOUD  0     -
2023-07-22 17:33:17
00e0-fc11-3344  **********3        10.1.1.13        AirEngine8760-X1-PRO   CLOUD/-      0     delivered
2023-07-22 17:33:17
----------------------------------------------------------------------------------------------------------------------------
-------
Total: 3
```

Table 11-10 Description of the **display ap non-factory all** command output

Item	Description
MAC	MAC address of an AP in non-Fit mode.
SN	SN of an AP in non-Fit mode.
IP	IP address of an AP in non-Fit mode.
Type	Type of an AP in non-Fit mode.
Mode	Current mode and configuration mode of an AP in non-Fit mode. The configuration mode refers to the specified mode information received by the AP through DHCP Option 148. When the configuration mode is not empty, the Fit mode cannot be restored.
Cnt	Number of managed Fit APs when the AP in non-Fit mode is the leader AP.
Operate State	State of receiving the **ap manufacturer-config** command on an AP in non-Fit mode. ● waiting deliver: The command has been delivered but has not been received on the AP. ● delivered: The AP has received the command. ● -: The command is not delivered.
Record time	Latest time when the AP is detected.
Total	Total number of times APs in non-Fit mode are detected.

11.1.59 display ap offline-record

Function

The **display ap offline-record** command displays AP offline records.

Format

display ap offline-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays offline records of all APs.	-
mac *mac-address*	Displays offline records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays AP offline records, helping the maintenance personnel manage and maintain the APs.

After the number of AP offline records reaches the maximum that can be stored, new records overwrite existing ones.

A maximum of five offline records can be stored for each AP.

Example

Display offline records of all APs.

```
<HUAWEI> display ap offline-record all
------------------------------------------------------------------------------
MAC              Last offline time       Reason
------------------------------------------------------------------------------
00e0-fc24-0080    2015-01-31/16:21:50    The AP name is modified.
00e0-fc76-e360    2015-01-31/14:02:35    The AP is replaced.
------------------------------------------------------------------------------
Total records: 2
```

Table 11-11 Description of the **display ap offline-record** command output

Item	Description
MAC	MAC address of an AP.
Last offline time	Time when the AP went offline last time.

Item	Description
Reason	Reason why the AP goes offline. For the description of offline reasons and handling suggestions, see **Table 11-12**. For more troubleshooting methods, see **An AP Goes Offline Unexpectedly** in the *Troubleshooting Guide*.

Table 11-12 Possible reasons and suggestions for APs to go offline

Reason Why an AP Goes Offline	Suggestion
The AC country code is modified.	The AP goes offline due to normal configuration changes, and no action is required.
The AP is replaced.	The AP goes offline due to normal configuration changes, and no action is required.
Reboot by ap update reset command. The AP is reset automatically after the upgrade.	The AP resets to load the new version file after the upgrade, and no action is required.
A command is delivered to reboot an AP.	The AC delivers a reboot command to the AP, and no action is required.
An AP is deleted.	The AP is deleted on the AC, and no action is required.
The license expires.	Apply for a new license. For details, see *WLAN License Usage Guide*.
Insufficient license resources.	Choose one of the following handling suggestions based on the networking: ● If license control is deployed, check whether the link between the license server and client is disconnected. If so, restore the link. ● If N+1 or dual-link backup is deployed, check whether the active and standby link is disconnected. If so, restore the link. ● If the number of APs on the network exceeds the total number of license resources, apply for a new license.
The AP is added to the blacklist.	Check whether the AP needs to be added to the blacklist.

Reason Why an AP Goes Offline	Suggestion
A CAPWAP tunnel is faulty (due to inconsistent link IDs).	The AP will automatically attempt to recover the link, and no action is required.
The DTLS configuration of the CAPWAP tunnel changes.	The AP goes offline due to normal configuration changes, and no action is required.
The AP's factory settings are restored.	The AP goes offline due to normal configuration changes, and no action is required.
The radio type is inconsistent between the AC and AP.	Run the **display ap config-info** command to verify the AP radio configuration.
Heartbeat packet transmission for the CAPWAP data tunnel between the AC and AP times out.	Check the intermediate network between the AP and AC.
Heartbeat packet transmission for the CAPWAP control tunnel between the AC and AP times out.	Check the intermediate network between the AP and AC.
The dual-link networking configuration is modified.	The configuration change causes the AP to automatically reboot, and no action is required.
The AP name is modified.	The AP goes offline due to normal configuration changes, and no action is required.
The AP group name is modified.	The AP goes offline due to normal configuration changes, and no action is required.
The management VLAN is modified.	The AP goes offline due to normal configuration changes, and no action is required.
AP provisioning parameters are set.	The AP goes offline due to normal configuration changes, and no action is required.
The CAPWAP source IP address is deleted.	The AP goes offline due to normal configuration changes, and no action is required.
The central AP goes offline.	Check the reason why the central AP goes offline.
The central AP proactively reboots RUs.	The AP goes offline due to normal configuration changes, and no action is required.

Reason Why an AP Goes Offline	Suggestion
The AP is powered off and restarts.	If the AP restarts repeatedly, check whether the AP power supply mode matches the actual power supply.
An internal error (KP) occurs.	Contact technical support personnel.
An internal error (VOS signal error) occurs.	Contact technical support personnel.
An internal error (forwarding error monitored by MFPI) occurs.	Contact technical support personnel.
An internal error (PKO error monitored by MSC) occurs.	Contact technical support personnel.
An internal error (reset due to timer expiration) occurs.	Contact technical support personnel.
An internal error (reset of the write CPLD register) occurs.	Contact technical support personnel.
The reset button is pressed to reset the AP.	Check whether the AP is manually reset.
The AP restarts due to a CANBUS reset.	Contact technical support personnel.
The AP restarts due to AP interference.	Contact technical support personnel.
The AP restarts due to a chip exception. The AP restarts due to a firmware exception.	Contact technical support personnel.
The CAPWAP sensitive-info PSK is modified.	The configuration change causes the AP to automatically reboot, and no action is required.
The CAPWAP integrity-check PSK is modified.	The configuration change causes the AP to automatically reboot, and no action is required.
The country code is inconsistent on the AC and AP.	Check the country code configuration on the AC and AP.

Reason Why an AP Goes Offline	Suggestion
The AP is forcibly disconnected.	Check the fault based on the possible causes, which may be: ● CAPWAP resources are insufficient. ● The access interface of the AP is changed. ● The Eth-Trunk connected to the AP is deleted. If the fault persists, contact technical support personnel.
The wideband status change.	The AP goes offline due to normal configuration changes, and no action is required.
Reset for a configuration delivery failure.	Check network connectivity. If no problem is found, contact technical support personnel.
Reboot for the branch group of AP change.	The AP goes offline due to normal configuration changes, and no action is required.
The AC license expires.	Re-activate the AC license.
A CAPWAP tunnel is faulty (due to a CAPWAP link entry verification failure).	The AP will automatically attempt to recover the link, and no action is required.
Batch delete	Check whether the active AC runs properly. When the active AC is restored, the AP switches to this active AC to go online.
Switch service radio to proxy scanning radio.	The configuration change causes the AP to automatically reboot, and no action is required.
Switch proxy scanning radio to service radio.	The configuration change causes the AP to automatically reboot, and no action is required.
The AP cloud license expires.	Purchase a new license and load it to iMaster NCE-Campus.
The device has been disconnected from the iMaster NCE-Campus for more than 90 days.	Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity.
The device is deleted from the iMaster NCE-Campus.	No action is required.

Reason Why an AP Goes Offline	Suggestion
The iMaster NCE-Campus does not deliver AP information.	1. Verify that AP information is correctly added to iMaster NCE-Campus, the AP is associated with the AC, and the AC is online. 2. Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity. 3. Check whether iMaster NCE-Campus fails to deliver AP information. If so, manually deliver AP information again.
An internal error (Reset for firmware abnormal) occurs.	Contact technical support personnel.
An internal error (Reset for abnormal network port self-healing) occurs.	Contact technical support personnel.
An internal error (Reset for the forcible AP disconnection in specific scenarios) occurs.	Contact technical support personnel.
An internal error (Reset for slow task switching) occurs.	Contact technical support personnel.
An internal error (Reset for MFPI detect CAP PBUF use out) occurs.	Contact technical support personnel.
An internal error (Reset for ap abnormal self-healing) occurs.	Contact technical support personnel.
An internal error (Reset for exception(redis-server exit)) occurs.	Contact technical support personnel.
An internal error (Reset for exception(confd exit)) occurs.	Contact technical support personnel.
An internal error (Reset for exception(callhome exit)) occurs.	Contact technical support personnel.
An internal error (Reset for an abnormal process) occurs.	Contact technical support personnel.
N+1 switchover of APs.	No action is required.
An internal error (Reset for an NP heartbeat message exception) occurs	Contact technical support personnel.
An internal error (exceed the extreme temperature) occurs.	Take proper measures to lower the ambient temperature, for example, by lowering the air conditioner temperature and ventilate the equipment room.

Reason Why an AP Goes Offline	Suggestion
An internal error (memory use out) occurs.	Contact technical support personnel.
An internal error (dophi-server exit) occurs.	Contact technical support personnel.
An internal error (Wi-Fi SDK self-healing failure) occurs.	Contact technical support personnel.
Reconnect by command.	No action is required.
Reset for the radio mode change.	No action is required.
Reset for RTU license activation.	No action is required.
Reset for an overdue demo license.	No action is required.
Reset for insufficient power supply.	Contact technical support personnel.
An internal error (Reset for an unexpected exit of the WPC process) occurs.	Contact technical support personnel.
Cloud licenses expire, and local license resources are insufficient	Expand the license capacity (RUs do not occupy license resources).
Incompatible DTLS version or encryption algorithm	Upgrade the AP version, or run the **capwap dtls version1.0 enable** and **capwap dtls cbc enable** commands to enable compatibility with earlier DTLS versions.
The CAPWAP DTLS authentication configuration of the AP is changed	The AP goes offline due to configuration changes, and no action is required.

11.1.60 display ap online-fail-record

Function

The **display ap online-fail-record** command displays AP online failure records.

Format

display ap online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays online failure records of all APs.	-

Parameter	Description	Value
mac *mac-address*	Displays online failure records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an AP fails to go online on the AC, you can run this command to check the failure reason, which helps locate the fault.

After the number of AP online failure records reaches the maximum that can be stored, new records overwrite existing ones.

A maximum of five online failure records can be stored for each AP.

Example

Display online failure records about the AP with the MAC address 00e0-fcb1-56a0.

```
<HUAWEI> display ap online-fail-record mac 00e0-fcb1-56a0
------------------------------------------------------------------------------
MAC             Last fail time       Reason
------------------------------------------------------------------------------
00e0-fcb1-56a0  2015-01-20/15:48:06  The AP is added to the AP blacklist.
------------------------------------------------------------------------------
Total records: 1
```

Table 11-13 Description of the **display ap online-fail-record** command output

Item	Description
MAC	MAC address of the AP that fails to go online.
Last fail time	Time of the AP online failure.
Reason	Reason why the AP fails to go online. For details about going-online failure causes and handling suggestions, see **Table 11-14**. For more troubleshooting methods, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

Table 11-14 Possible causes and suggestions for APs' failures to go online

Reason Why an AP Fails to Go Online	Suggestion
Insufficient license resources.	Expand the license capacity. Note that RUs do not occupy license resources of the AC. For details, see *WLAN License Usage Guide*.
The AP is not in the SN whitelist.	Run the **ap whitelist sn** *ap-sn1* [**to** *ap-sn2*] command to add the AP to the whitelist or run the **ap-confirm** command to enable the AP to pass authentication.
The AP is not in the MAC whitelist.	Run the **ap whitelist mac** *ap-mac1* [**to** *ap-mac2*] command to add the AP to the whitelist or run the **ap-confirm** command to enable the AP to pass authentication.
The AP is added to the AP blacklist.	Check whether the AP needs to be added to the blacklist. To delete the AP from the blacklist, run the **undo ap blacklist** command.
The MAC address and SN of the AP do not match.	Check whether the MAC address and SN of the AP match.
DTLS negotiation for CAPWAP tunnel setup fails.	Check whether the PSK used for DTLS encryption is correctly configured.
DTLS negotiation failed, because of negotiation timeout or inconsistent PSKs on two ends.	● Check whether the shared keys of the AC and AP are the same. If not, change them to the same. Alternatively, enable the function of establishing CAPWAP DTLS sessions in none authentication mode so that the APs can obtain security credentials. After the APs go online, disable this function immediately in order to prevent unauthorized APs from going online. ● Check whether ping packets are normal on the network. If not, negotiation timeout occurs because of a network exception during the DTLS negotiation. In this case, check the network. ● If this fault persists, contact technical support personnel.

Reason Why an AP Fails to Go Online	Suggestion
CAPWAP tunnel negotiation fails.	Check network connectivity. If no problem is found, contact technical support personnel.
APs cannot go online during data backup.	Wait until backup is complete.
The upgrade fails.	Run the **display ap update configuration** command to check whether the AP's upgrade file is correct. If so, rectify the fault by referring to **Fit AP Upgrade Fails** in the *Troubleshooting Guide*.
The CAPWAP tunnel fails to be established.	Check network connectivity. If no problem is found, contact technical support personnel.
The configuration fails to be delivered.	The device attempts to deliver the configuration again. If the failure persists: 1. Check whether the AC and AP can ping each other. If the network is disconnected or a large number of packets are lost, check the intermediate network. 2. Check whether the MTU between the AC and AP is correctly configured. Assume that the MTU of the intermediate network is 1500 bytes. Run the **ping** **-a** <*AC CAPWAP source IP*> **-s** *1472* **-f** <*AP IP*> command on the AC to check whether the ping operation succeeds. If packet loss occurs, run the **mtu** (AP system profile view) command to change the MTU of the AP to be the same as the MTU of the intermediate network. 3. Check whether the AC and AP can properly send and receive packets, whether the queue usage exceeds the threshold, and whether packet loss or any loop occurs on interfaces. If this fault persists, contact technical support personnel.

Reason Why an AP Fails to Go Online	Suggestion
The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. - Enterprise technical support website: **https://support.huawei.com/enterprise** - Carrier technical support website: **https://support.huawei.com**
- The AC does not support the AP type. - Unsupported AP type, AC version may need to be upgraded.	Replace the AP with that supported by the AC or replace the AC with one that supports this AP type. To enable an AC to manage APs that are new in a later version, you can manually add AP types. For details, see **Enabling a WAC to Manage New APs Running Later Versions**.
The AP name conflicts.	Run the **ap-rename** command to rename the AP.
The number of central APs reaches the upper limit.	Check whether the number of central APs reaches the maximum value.
The number of common APs reaches the upper limit.	Check whether the number of common APs reaches the maximum value. If the number of normal APs is smaller than the maximum, to allow the AP to go online, run the **undo ap** command to delete APs that are not in normal state to release resources.
The central AP is not in normal state.	Run the **display ap** command to check the central AP status and take measures accordingly.
The CAPWAP sensitive-info PSK is different on the two ends of the CAPWAP tunnel.	Ensure that the PSK for encrypting CAPWAP sensitive information is the same on the AP and AC. Alternatively, enable the AP to set up a DTLS session with the AC using the default PSK.
The CAPWAP integrity-check PSK is different on the two ends of the CAPWAP tunnel.	Ensure that the PSK for checking CAPWAP packet integrity is the same on the AP and AC. Alternatively, enable the AP to set up a DTLS session with the AC using the default PSK.

Reason Why an AP Fails to Go Online	Suggestion
The configured and reported AP types are different. The real AP type is *XXXX*. The type ID carried by the AP is different from that configured on the AC.	After the **undo AP** command is run to delete an AP, the system cannot obtain the AP type and displays a message "The configured and reported AP types are different." In this case, ensure that the configured AP type is the same as the reported one.
The AC license is not active.	Activate the AC license.
Too many APs go online concurrently, leading to a failure to create sufficient DBSS interfaces.	No action is required. The APs will attempt to go online again. If the APs still fail to go online, contact technical support personnel.
The country codes of the AP and AC are inconsistent, and the country code of the AP is locked.	The country code of some AP models cannot be modified. For example, an AP model with the suffix -US is used only in the United States, and its country code is fixed as US. Configure the country code on the AC to be the same as that on the AP.
The AP cloud license expires.	Purchase a new license and load it to iMaster NCE-Campus.
The device has been disconnected from the iMaster NCE-Campus for more than 90 days.	Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity.
The device is deleted from the iMaster NCE-Campus.	No action is required.
The iMaster NCE-Campus does not deliver AP information.	1. Verify that AP information is correctly added to iMaster NCE-Campus, the AP is associated with the AC, and the AC is online. 2. Verify the iMaster NCE-Campus address configured on the AC, and check network connectivity. 3. Check whether iMaster NCE-Campus fails to deliver AP information. If so, manually deliver AP information again.
Configuration synchronization is in progress, leading to the system busy.	No action is required.
Backing up HA data.	Wait till HA data backup ends.

Reason Why an AP Fails to Go Online	Suggestion
Insufficient LPU resources.	All the resources of the card are occupied. Go online through another card.
Invalid port on the switch connected to the AP.	Check whether a card does not support AP access or the cards are in different working groups.
Insufficient trunk resources.	The trunk resources are released.
The number of distribute APs reaches the upper limit of the central AP.	Re-plan the network and expand the network capacity by adding central APs.
The number of CAPWAP tunnels reaches the upper limit.	Run the **display as** command to check whether any online AS occupies CAPWAP resources. If so, properly allocate CAPWAP resources.
This AP type is not supported. Add it or upgrade the AC version.	Add the AP type or upgrade the AC version.
Inconsistent type IDs on the AP and AC. (Type ID reported by the AP: *xx*; AP type: *yy*)	Modify the AP type ID to be the same as that on the AC. The method is as follows: 1. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-list* | **ap-mac** *ap-mac* } command to delete all the APs using this type ID. 2. Run the **undo ap-type** *type-description* command to delete the AP type configuration. 3. Run the **ap-type** *type-description* **type-id** *type-id* command to configure the AP type correctly.
The AC version is not supported by the AP.	Upgrade the AC version.
Failed to add the reported AP type parameters.	Upgrade the AC version.
The AP is forcibly disconnected.	iMaster NCE-Campus responds with a registration failure message. In this case, add the AP on iMaster NCE-Campus.
This AP type is not supported.	Replace the AP.

Reason Why an AP Fails to Go Online	Suggestion
DTLS negotiation failed by using the preset certificate.	The function of verifying the CN field in AC certificates is configured on the AP. In an AC replacement scenario, if the CN field of the new AC is not added, APs cannot go online on the new AC. In this case, you need to add the CN field of the new AC for APs on the original AC. If the original AC is faulty and does not support the configuration, log in to each AP that fails to go online and run the **capwap dtls server-auth disable** command to disable the AC authentication function for the AP or restore the factory settings of each AP.
The AP automatic replacement function is enabled, and the AP does not carry LLDP neighbor information.	Check whether LLDP is enabled on the device connected to the AP's uplink interface.
Cloud licenses expire, and local license resources are insufficient	Expand the license capacity. (RUs do not consume license resources.)
Incompatible DTLS version or encryption algorithm	Upgrade the AP version, or run the **capwap dtls version1.0 enable** and **capwap dtls cbc enable** commands to enable compatibility with earlier DTLS versions.
Negotiation DTLS data tunnel failed	Check whether the PSK used for DTLS encryption is correctly configured.
Access through VPN is rejected	The AP cannot go online through a VPN. Ensure that no VPN configuration exists on the interface connecting the upstream device to the AP.
The radio type is inconsistent between the AC and AP	No action is required. The AP automatically restarts and the new configuration takes effect.
The total number of APs and tunnel APs reaches the maximum number of APs that can be managed	Run the **display ap all** and **display tunnel-ap all** commands to check the number of APs and the number of tunnel APs, respectively. Plan APs properly or expand the capacity based on the maximum number of APs that can be managed.

11.1.61 display ap radio-mode all

Function

The **display ap radio-mode all** command displays the effective radio mode of online APs.

Format

display ap radio-mode all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After switching the radio mode of an AP using the **radio-mode** command, you can run the **display ap radio-mode all** command to query the effective radio mode of the AP.

Example

Display the effective radio mode of online APs.

```
<HUAWEI> display ap radio-mode all
--------------------------------------------
ID      Mode
--------------------------------------------
0       2radio-standard
--------------------------------------------
Total: 1
```

Table 11-15 Description of the **display ap radio-mode all** command output

Item	Description
ID	AP ID.

Item	Description
Mode	Radio mode. ● 2radio-standard: standard dual-radio mode ● 2radio-2g-enhanced: 2G enhanced dual-radio mode ● 2radio-5g-enhanced: 5G enhanced dual-radio mode ● 2radio-independent-scan: dual-radio + independent scanning mode ● 3radio: three-radio mode ● -: The AP has not reported the radio mode switching message. **NOTE** The AirEngine 6761-21, AirEngine 6761-21E, and AirEngine 6761S-21 have a dedicated radio for scanning and can perform radio scanning even in **2radio-standard** mode.

11.1.62 display ap-rtu-status all

Function

The **display ap-rtu-status all** command displays the RTU license loading status of all APs.

NOTE

The RTU License is not supported by the following models.

- AirEngine x76x (Excluding the AirEngine 5760-51, AirEngine 6760-X1, AirEngine 6760-X1E)
- AirEngine x77x
- The cemtral AP (including matching RUs)
- AirEngine 9700D-S (including matching ORUs)

Format

display ap-rtu-status all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After loading RTU licenses to APs, you can run this command to check the RTU license loading status.

Precautions

If the number of RTU licenses exceeds the maximum number of RTU licenses supported by an AC, the excess RTU licenses cannot be displayed in the command output. To check information about these RTU licenses, run the **dir rtu/** command in the user view.

Example

Display the RTU license loading status of all APs.

```
<HUAWEI> display ap-rtu-status all
Info: This operation may take a few seconds. Please wait for a moment.done.
Active: [1] The RTU license is activated on the AP.
Activating(Init):[1] The AC has not delivered the RTU file to the AP.
Activating(Need reboot): [1] The AP has downloaded the RTU license and needs a restart for the license to
take effect.
Active fail(Flash memory not enough): [1] The flash memory on the AP is insufficient for storing the license
file. Manually clear the flash space on the AP.
Active fail(Invalid license): [1] Invalid license file. Verify that the license file is correct.
No RTU license: [1] The license file of the AP does not exist on the AC. Upload the RTU package available
for this AP and run the ap rtu load command to decompress the package.
Not support RTU:[2] The AP version or model does not support the RTU license.
Not active:[3] The RTU license on the AC does not have the corresponding AP.
------------------------------------------------------------
AP ID  AP name    RTU license SN            RTU status
------------------------------------------------------------
1      AP-1       2102351TYRW0KB001030      Active
2      AP-2       2102353KCN10L1000053      Activating(Need reboot)
3      AP-3       2102353GSF10KC00002       No license on AP
4      AP-4       -                         No RTU license
5      AP-5       2102353GSF10KC00003       Active fail(Flash memory not enough)
6      AP-6       2102353GSF10KC00004       Active fail(Invalid license)
7      AP-7       2102353GSF10KC00005       Not support RTU
8      AP-8       -                         Not support RTU
9      AP-9       2102353GSF10KC00006       Activating(Init)
-      -          2102353GSF10KC10005       Not active
-      -          2102353GSF10KC20005       Not active
-      -          2102353GSF10KC30005       Not active
------------------------------------------------------------
Total: 12
```

Table 11-16 Description of the **display ap-rtu-status all** command output

Item	Description
AP ID	AP ID.
AP name	AP name.

Item	Description
RTU license SN	ESN in the RTU license file, which is not the ESN of the AP. If no ESN or an invalid ESN is contained in a license file, the file is considered invalid and this field is displayed as -. If the license file does not contain the RTU license file for the AP, this field is displayed as -.
RTU status	RTU license loading status. ● Active: The RTU license has been activated on an AP. ● Activating(Init): The AC has not delivered the RTU license file to an AP. ● Activating(Need reboot): An AP has downloaded and stored the RTU license file, and needs a restart for the file to take effect. ● No RTU license: The AC does not have the RTU license file for an AP. You need to upload the RTU license package containing the RTU license for the AP and run the **ap rtu load** command to unzip the package. ● Active fail(Flash memory not enough): The flash memory on an AP has insufficient space to store the RTU license file. You need to manually clear the flash memory on the AP. ● Active fail(Invalid license): The RTU license file is invalid. Verify that the file is correct. ● Not support RTU: The model software version or model of an AP does not support the RTU license. ● Not active: The AC has the RTU license but the corresponding AP is not online on the AC. ● -: An AP goes online on the standby AC. Query the RTU license on the active AC.

11.1.63 display ap sta-signal strength

Function

The **display ap sta-signal strength** command displays the average signal strength of STAs connected to an AP.

Format

display ap sta-signal strength { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the average signal strength of STAs connected to the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the average signal strength of STAs connected to the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays the average signal strength of STAs connected to a specified AP radio.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the average signal strength of STAs connected to an AP.

Example

Display the average signal strength of STAs connected to AP **test**.

```
<HUAWEI> display ap sta-signal strength ap-name test
Station signal strength(dBm): 0
```

Table 11-17 Description of the **display ap sta-signal strength** command output

Item	Description
Station signal strength(dBm)	Average signal strength of STAs.

11.1.64 display ap statistics

Function

The **display ap statistics** command displays AP type statistics.

Format

display ap statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Various types of APs can be added on the device. You can run this command to view types of APs added on the device and the number of APs of various types.

Example

Display statistics about AP types.

```
<HUAWEI> display ap statistics
------------------------------------------------------------------------------
Type                Number
------------------------------------------------------------------------------
AP4050DN              1
AP5030DN              1
------------------------------------------------------------------------------
```

Table 11-18 Description of the **display ap statistics** command output

Item	Description
Type	AP type.
Number	Number of APs of a type.

11.1.65 display ap unauthorized record

Function

The **display ap unauthorized record** command displays information about unauthenticated APs.

Format

display ap unauthorized record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the MAC address or SN authentication mode is configured for an AP but the AP is neither imported nor added to the whitelist, the AC does not allow this AP to access. You can run the **display ap unauthorized record** command to view information about unauthorized APs.

Example

Display information about unauthorized APs.

```
<HUAWEI> display ap unauthorized record
Unauthorized AP record:
Total number: 1
--------------------------------------------------------------------------------
AP type: AirEngine8760-X1-PRO
AP SN: xxxxxxxxxxxxxxxxx
AP MAC address: xxxx-xxxx-xxxx
AP IP address: 192.168.109.252
Record time: 2020-01-22 17:23:17
--------------------------------------------------------------------------------
```

Table 11-19 Description of the **display ap unauthorized record** command output

Item	Description
Unauthorized AP record	Records about unauthenticated APs.
Total number	Total number of unauthenticated APs.
AP type	AP type.
AP SN	AP SN.
AP MAC address	AP's MAC address.
AP IP address	AP's IP address.
Record time	Time when an unauthorized AP was recorded.

11.1.66 display ap whitelist

Function

The **display ap whitelist** command displays AP whitelist information.

Format

display ap whitelist { **mac** | **sn** }

Parameters

Parameter	Description	Value
sn	Displays SNs in the AP whitelist.	-
mac	Displays MAC addresses in the AP whitelist.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the AP authentication mode is set to MAC address or SN authentication using the **ap auth-mode** command, you can run the **ap whitelist** command to configure an AP whitelist. Only RUs on the whitelist are allowed to go online. To check information about RUs in the whitelist, run the **display ap whitelist** command.

Example

Display MAC addresses in the AP whitelist.

```
<HUAWEI> display ap whitelist mac
--------------------------------------------------------------------------------
Index  MAC
--------------------------------------------------------------------------------
0      00e0-fcb1-56a0
1      00e0-fc24-0080
2      00e0-fc9d-0bb0
--------------------------------------------------------------------------------
Total: 3
```

Table 11-20 Description of the **display ap whitelist mac** command output

Item	Description
Index	Index.
MAC	MAC address of an AP. To add a MAC address to the AP whitelist, run the **ap whitelist mac** *ap-mac1* [**to** *ap-mac2*] command.

Display SNs in the AP whitelist.

```
<HUAWEI> display ap whitelist sn
--------------------------------------------------------------------------------
Index  SN
--------------------------------------------------------------------------------
0      210235449210CB000011
1      S0001
2      210235568010D1000032
--------------------------------------------------------------------------------
Total: 3
```

Table 11-21 Description of the **display ap whitelist sn** command output

Item	Description
Index	Index.
SN	SN of an AP. To add an SN to the AP whitelist, run the **ap whitelist sn** *ap-sn1* [**to** *ap-sn2*] command.

11.1.67 display ap-group

Function

The **display ap-group** command displays configuration and reference information about an AP groups.

Format

display ap-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP groups.	-
name *group-name*	Displays information about a specified AP group.	The AP group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap-group** command to view configuration and reference information about AP groups.

Example

Display information about all AP groups.

```
<HUAWEI> display ap-group all
------------------------------------------------------------
Name                              APs
------------------------------------------------------------
default                          1
------------------------------------------------------------
Total: 1
```

Table 11-22 Description of the **display ap-group all** command output

Item	Description
Name	Name of an AP group.
APs	Number of APs in an AP group.

Display information about the AP group **default**.

```
<HUAWEI> display ap-group name default
------------------------------------------------------------------------------------------
AP system profile           : default
Regulatory domain profile  : default
WIDS profile                : default
BLE profile                 :
AP location                 :
UUID                        :
Domain name                 :
Scene                       : multi-partition-cross-room
Ap pki profile              :
AP wired port profile
 Interface FE0              : default
 Interface FE1              : default
 Interface FE2              : default
 Interface FE3              : default
 Interface GE0              : default
......
 Interface GE27             : default
 Interface MultiGE0         : default
......
 Interface MultiGE7         : default
 Interface XGE0             : default
......
 Interface XGE7             : default
 Interface Eth-trunk0       : default
 Interface Eth-trunk1       : default
Radio 0
 Radio 2.4G profile         : default
 Radio 5G profile           : default
 VAP profile                :
 Mesh profile               :
 WDS profile                :
 Mesh whitelist profile     :
 WDS whitelist profile      :
 Location profile           :
```

```
 Radio switch              : enable
 Channel                   : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)                 : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Work mode                 : normal
 Flexible radio switch     : on
 Radio frequency           : 2.4G
 Spectrum analysis         : disable
 Channel monitor           : disable
 WIDS device detect        : disable
 WIDS attack detect        : -
 WIDS contain switch       : disable
 Auto channel select       : enable
 Auto bandwidth select     : disable
 Auto transmit power select: enable
 Reference data-analysis   : enable
 Reference 3d-data         : enable
 Beacon switch             : enable
 CTS switch                : enable
 CTS delay time(us)        : none
Radio 1
......
Radio 2
......
Card 1
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Card 2
......
Card usb
 Card connect type         : -
 Baud rate                 : -
 Wired port profile        : default
 Iot profile               :
 Protocol Type             : -
 First Port                : -
 Extended Port             : -
Traffic policy outbound    : 1
```

Table 11-23 Description of the **display ap-group name** command output

Item	Description
AP system profile	AP system profile referenced by an AP group. To configure this parameter, run the **ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Regulatory domain profile referenced by an AP group. To configure this parameter, run the **regulatory-domain-profile** command.
WIDS profile	WIDS profile referenced by an AP group.

Item	Description
BLE profile	BLE profile referenced by an AP group. To configure this parameter, run the **ble-profile (AP group view and AP view)** command.
UUID	UUID of a BLE broadcast frame sent by the AP's built-in Bluetooth module. To configure this parameter, run the **broadcasting-content (AP group view)** command.
AP location	Installation position of an AP in the AP group. To configure this parameter, run the **location** command.
Domain name	Default domain name suffix of the AP. To configure this parameter, run the **ip domain-name** command.
Scene	Scenario profile bound to an AP group. To configure this parameter, run the **scene** command.
Ap pki profile	Bound AP PKI realm profile. To configure this parameter, run the **ap-pki-profile** command.
AP wired port profile	AP wired port profile referenced by an AP group. To configure this parameter, run the **wired-port-profile (AP group view and AP view)** command.
Interface *Interface-name*	Interface name.
Radio 0/Radio 1/Radio 2	Radio ID.
Radio 2.4G profile	2G radio profile referenced by an AP group. To configure this parameter, run the **radio-2g-profile** command.
Radio 5G profile	5G radio profile referenced by an AP group. To configure this parameter, run the **radio-5g-profile** command.

Item	Description
VAP profile	VAP profile referenced by an AP group. The displayed format is "VAP ID:VAP profile name (service VLAN defined when binding to the VAP profile, single VLAN, or VLAN pool)." To configure this parameter, run the **vap-profile** command.
Mesh profile	Mesh profile referenced by an AP group. To configure this parameter, run the **mesh-profile radio** command.
WDS profile	WDS profile referenced by an AP group. To configure this parameter, run the **wds-profile radio** command.
Mesh whitelist profile	Mesh whitelist profile referenced by an AP group. To configure this parameter, run the **mesh-whitelist-profile (AP group radio view or AP radio view)** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure this parameter, run the **wds-whitelist-profile (AP group radio view or AP radio view)** command.
Location profile	Location profile referenced by an AP group. To configure this parameter, run the **location-profile** command.
Radio switch	Whether a radio is enabled. To configure this parameter, run the **radio disable** command.
Channel	Working channel of a radio. To configure this parameter, run the **channel** command.
Channel bandwidth	Working bandwidth of a radio. To configure this parameter, run the **channel** command.

Item	Description
EIRP(dBm)	Transmit power of a radio, in dBm. To configure this parameter, run the **eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dB. To configure this parameter, run the **antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in the unit of 100 m. To configure this parameter, run the **coverage distance** command.
Work mode	Working mode of a radio. To configure this parameter, run the **work-mode** command.
Flexible radio switch	Whether the DFA function of a radio is enabled. To configure this parameter, run the **calibrate flexible-radio disable** command.
Radio frequency	Working frequency band of a radio. To configure this parameter, run the **frequency** command.
Spectrum analysis	Whether spectrum analysis is enabled. To configure this parameter, run the **spectrum-analysis enable** command.
Channel monitor	Whether the function of monitoring the status of all channels is enabled. To configure this parameter, run the **channel-monitor enable** command.
WIDS device detect	Whether wireless device detection is enabled. To configure this parameter, run the **wids device detect enable** command.
WIDS attack detect	Whether attack detection is enabled. To configure this parameter, run the **wids attack detect** command.
WIDS contain switch	Whether rogue device containment is enabled. To configure this parameter, run the **wids contain enable** command.

Item	Description
Auto channel select	Whether automatic channel selection is enabled. To configure this parameter, run the **calibrate auto-channel-select** command.
Auto bandwidth select	Whether automatic bandwidth selection is enabled. To configure this parameter, run the **calibrate auto-bandwidth-select** command.
Auto transmit power select	Whether automatic transmit power selection is enabled. To configure this parameter, run the **calibrate auto-txpower-select** command.
Reference data-analysis	Whether big data calibration is enabled. To configure this parameter, run the **calibrate reference data-analysis { disable | enable }** command.
Reference 3d-data	Whether 3D radio calibration is enabled. To configure this parameter, run the **calibrate reference 3d-data { disable | enable }** command.
Beacon switch	Whether RUs are enabled to send Beacon frames. To configure this parameter, run the **beacon disable** command.
CTS switch	Whether RUs are enabled to respond to STAs with CTS packets. To configure this parameter, run the **cts disable** command.
CTS delay time(us)	Delay time after which RUs respond to STAs with CTS packets. To configure this parameter, run the **cts delay** command.
Card 1/Card 2/Card 3/Card usb	IoT card.

Item	Description
Card connect type	Communication connection type between IoT cards and APs. To configure this parameter, run the **card connect-type** command.
Baud rate	Baud rate used for communication between an IoT card and the AP. To configure this parameter, run the **baud-rate** command.
Wired port profile	AP wired port profile referenced by an AP group. To configure this parameter, run the **wired-port-profile (IoT card interface view)** command.
Iot profile	Bound IoT profile. To configure this parameter, run the **iot-profile (IoT card interface view)** command.
Protocol Type	Communication protocol between the AP and host computer.
First Port	Source port for the first channel.
Extended Port	Source port for the extended channel.
Traffic policy outbound	Traffic policy applied to an AP group.

11.1.68 display capwap configuration

Function

The **display capwap configuration** command displays the CAPWAP configuration.

Format

display capwap configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the interval for sending Keepalive packets, number of times for sending Keepalive packets, and priority of CAPWAP management packets.

Example

Display the CAPWAP configuration.

```
<HUAWEI> display capwap configuration
 ------------------------------------------------------------------
 Source interface                                : -
 Echo interval(seconds)                          : 25
 Echo times                                      : 6
 Control priority(server to client)              : 7
 Control priority(client to server)              : 7
 Control-link DTLS encrypt                       : disable
 DTLS PSK value                                  : ******
 Control-link inter-controller DTLS encrypt      : disable
 Inter-controller DTLS PSK value                 : ******
 Message-integrity PSK value                     : ******
 Message-integrity check switch                  : enable
 Sensitive-info PSK value                        : ******
 Sensitive-info inter-controller PSK value       : ******
 DTLS no-auth status                             : disable
 DTLS cert-mandatory-match status                : disable
 DTLS version1.0 status                          : disable
 DTLS cbc status                                 : disable
 ------------------------------------------------------------------
```

Table 11-24 Description of the **display capwap configuration** command output

Item	Description
Source interface	Source interface of the AC. To configure this parameter, run the **capwap source interface** command.
Echo interval(seconds)	Interval for sending Keepalive packets. To configure this parameter, run the **capwap echo interval** *interval-value* command.
Echo times	Number of times for sending Keepalive packets. If no response is received after the specified number of times, the link is considered disconnected. To configure this parameter, run the **capwap echo times** *times-value* command.

Item	Description
Control priority(server to client)	Priority of CAPWAP management packets from the AC to the APs. To configure this parameter, run the **capwap control-link-priority local** *priority-value* command.
Control priority(client to server)	Priority of CAPWAP management packets from the APs to the AC. To configure this parameter, run the **capwap control-link-priority remote** *priority-value* command.
Control-link DTLS encrypt	Whether DTLS encryption for CAPWAP control tunnels is enabled. To configure this parameter, run the **capwap dtls control-link encrypt** command.
DTLS PSK value	PSK for DTLS encryption. To configure this parameter, run the **capwap dtls psk** command.
Control-link inter-controller DTLS encrypt	Whether DTLS encryption is enabled for control tunnels between ACs. To configure this parameter, run the **capwap dtls inter-controller control-link encrypt** command.
Inter-controller DTLS PSK value	PSK for DTLS encryption of an inter-AC tunnel. To configure this parameter, run the **capwap dtls inter-controller psk** command.
Message-integrity PSK value	PSK for checking integrity of CAPWAP packets. To configure this parameter, run the **capwap message-integrity psk** command.
Message-integrity check switch	Whether integrity check of CAPWAP packets is enabled. To configure this parameter, run the **capwap message-integrity check disable** command.
Sensitive-info PSK value	PSK for encrypting sensitive information. To configure this parameter, run the **capwap sensitive-info psk** command.

Item	Description
Sensitive-info inter-controller PSK value	PSK for encrypting sensitive information between ACs. To configure this parameter, run the **capwap inter-controller sensitive-info psk** command.
DTLS no-auth status	Whether the function of establishing CAPWAP DTLS sessions in none authentication mode is enabled. To configure this parameter, run the **capwap dtls no-auth enable** command.
DTLS cert-mandatory-match status	Whether the function of establishing CAPWAP DTLS sessions through the initial certificate is enabled. To configure this parameter, run the **capwap dtls cert-mandatory-match disable** command.
DTLS version1.0 status	Whether compatibility with DTLS 1.0 is enabled. To configure this parameter, run the **capwap dtls version1.0 enable** command.
DTLS CBC status	Whether compatibility with the DTLS CBC cipher suite is enabled. To configure this parameter, run the **capwap dtls cbc enable** command.

11.1.69 display cpe-tunnel-profile

Function

The **display cpe-tunnel-profile** command displays configuration and reference information about CPE tunnel profiles.

Format

display cpe-tunnel-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all CPE tunnel profiles.	-
name *profile-name*	Displays information about a specified CPE tunnel profile.	The CPE tunnel profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration and reference information about CPE tunnel profiles.

Example

Display information about all CPE tunnel profiles.

```
<HUAWEI> display cpe-tunnel-profile all
------------------------------------------------------------------------------------------------------------
Profile name         Reference
------------------------------------------------------------------------------------------------------------
default              1
cpe-tunnel-profile1  0
------------------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-25 Description of the **display cpe-tunnel all** command output

Item	Description
Profile name	Name of a CPE tunnel profile.
Reference	Number of times a CPE tunnel profile is referenced.

Display information about the CPE tunnel profile **cpe1**.

```
<HUAWEI> display cpe-tunnel-profile name cpe1
--------------------------------------------------------------------------------
PVID VLAN                          : 100
GRE checksum                       : disable
GRE key                            : disable
Allow-pass VLAN                    : 1 100
Forward mode                       : tunnel
Wlan-slice high-reliability traffic filter info:
```

```
AppliedRecord:
----------------------------------------------------------------------------------
```

Table 11-26 Description of the **display cpe-tunnel-profile name** command output

Item	Description
PVID VLAN	PVID of the interface corresponding to the CPE tunnel.
GRE checksum	Whether the checksum function is enabled for the CPE tunnel. To configure this parameter, run the **gre checksum (CPE tunnel profile view)** command.
GRE key	GRE key status of the CPE tunnel. To configure this parameter, run the **gre key (CPE tunnel profile view)** command.
Allow-pass VLAN	VLANs from which packets are allowed to pass through the CPE tunnel.
Forward mode	Forwarding mode of the CPE tunnel. ● direct-forward: direct forwarding ● tunnel: tunnel forwarding To configure this parameter, run the **forward-mode (CPE tunnel profile view)** command.
AppliedRecord(Wlan-slice high-reliability traffic filter info)	ACL-based rule records for air interface slicing. To configure this parameter, run the **wlan-slice high-reliability acl** command.

11.1.70 display radio

Function

The **display radio** command displays AP radio information.

Format

display radio { **all** | **ap-group** *ap-group-name* | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays radio information about all APs.	-
ap-group *ap-group-name*	Displays radio information about all APs in a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays radio information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays radio information about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the working status of AP radios.

Example

Display radio information about all APs.

```
<HUAWEI> display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
WM:Working Mode (normal/monitor/monitor dual-band-scan/monitor proxy dual-band-scan)
-------------------------------------------------------------------------------------
 AP ID Name           RfID  Band  Type   ST  CH/BW    CE/ME   STA    CU    WM
-------------------------------------------------------------------------------------
 0     00e0-fc76-e360  0     2.4G  bgn    on  6/20M    24/24   0      55%   normal
 0     00e0-fc76-e360  1     5G    an     on  56/20M   25/25   0      3%    normal
-------------------------------------------------------------------------------------
Total:2
```

Table 11-27 Description of the **display radio** command output

Item	Description
AP ID	AP ID.
Name	AP name.
RfID	Radio ID.

Item	Description
Band	Operating frequency band of an AP radio.
Type	Protocol type of an AP radio. ● b: 802.11b radio type ● bg: 802.11b/g radio type ● bgn: 802.11b/g/n radio type ● a: 802.11a radio type ● an: 802.11a/n radio type ● an11ac: 802.11a/n/ac radio type ● 11ax: 802.11b/g/n/ax radio type for a 2.4 GHz radio; 802.11a/n/ac/ax radio type for a 5 GHz radio; or 802.11ax radio type for a 6 GHz radio ● 11be: 802.11b/g/n/ax/be radio type for a 2.4 GHz radio; 802.11a/n/ac/ax/be radio type for a 5 GHz radio; or 802.11ax/be radio type for a 6 GHz radio
ST	Working status of an AP radio.
CH/BW	Channel/Bandwidth of an AP radio. If no VAP profile is bound to the radio, a hyphen (-) is displayed.
CE/ME	Current transmit power of an AP radio/ Maximum transmit power of an AP radio. If no VAP profile is bound to the radio, a hyphen (-) is displayed. **NOTE** The value is calculated based on the typical gain of the antenna used by the AP.
STA	Number of STAs connected to an AP radio.

Item	Description
CU	Channel utilization. When an AP radio works in monitor mode, this parameter is displayed as **-**. ● In the AC+central AP+RU networking: RUs do not proactively report the channel utilization to the AC. To query the channel utilization of RUs, enable the data buffer function on the AC. **NOTE** The **ap data-collection enable** command enables the data buffer function on the AC. After this command is executed, a large data buffer occupies the device memory and affects device performance. It is recommended that the **undo ap data-collection enable** command be executed to disable data buffer after the query. ● In the AC+Fit AP networking: A Fit AP periodically reports the channel utilization to the AC. Therefore, the AC does not need to query the channel utilization of APs.
WM	Working mode of an AP radio. ● normal ● monitor ● monitor dual-band-scan: inter-band scanning mode ● monitor proxy dual-band-scan: proxy inter-band scanning mode

11.1.71 display radio-2g-profile

Function

The **display radio-2g-profile** command displays configuration and reference information about a 2G radio profile.

Format

display radio-2g-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all 2G radio profiles.	-
name *profile-name*	Displays information about a specified 2G radio profile.	The 2G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about a 2G radio profile.

Example

Display information about all 2G radio profiles.

```
<HUAWEI> display radio-2g-profile all
--------------------------------------------------------------------
Profile name  Config Reference  Reference radios
--------------------------------------------------------------------
default       10                4
--------------------------------------------------------------------
Total: 1
```

Table 11-28 Description of the **display radio-2g-profile all** command output

Item	Description
Profile name	Name of a 2G radio profile.
Config Reference	Number of times a 2G radio profile is referenced.
Reference radios	Number of radios that reference a 2G radio profile.

Display information of the 2G radio profile **default**.

```
<HUAWEI> display radio-2g-profile name default
------------------------------------------------------------
Radio type                        : 802.11n
```

```
Power auto adjust                       : disable
Beacon interval(TUs)                    : 100
Beamforming switch                      : disable
Support short preamble                  : support
Fragmentation threshold(Byte)           : 2346
Channel switch announcement             : enable
Channel switch mode                     : continue
Guard interval mode                     : normal
802.11ax Guard interval mode            : dot8
A-MPDU switch                           : enable
HT A-MPDU length limit                  : 3
A-MSDU switch                           : disable
RTS-CTS-mode                            : cts-to-self
RTS-CTS-threshold                       : 2347
802.11bg basic rate                     : 1 2
802.11bg support rate                   : 1 2 5 6 9 11 12 18 24 36 48 54
Multicast rate 2.4G                     : 11
Interference detect switch              : disable
Co-channel frequency interference threshold(%)        : 50
Adjacent-channel frequency interference threshold(%)  : 50
Station interference threshold          : 32
WMM switch                              : enable
Mandatory switch                        : disable
Auto-off start time                     : -
Auto-off end time                       : -
Auto-off time-range                             : -
Wifi-light mode                         : signal-strength
Utmost power switch                     : enable
Rrm-profile                             : default
Air-scan-profile                        : default
Smart-antenna                           : disable
Agile-antenna-polarization              : disable
CCA threshold(dBm)                      : -
RX sensitivity(dBm)                     : -128
AGC high threshold(dBm)                 : -82
High PER threshold(%)                           : 80
Low PER threshold(%)                            : 20
Training interval(s)                            : auto
Training mpdu num                               : 640
Throughput trigger training threshold (%)       : 10
VIP user bandwidth reservation ratio (%)        : 20
Legacy signal length compatible                 : enable
RX STBC                                         : enable
Fastpass users                                  : 5
Fastpass period(ms)                             : 20
Fastpass ratio(%)                               : 25
Radio reload time-range                         : test
------------------------------------------------------------
AP EDCA parameters:
------------------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit(32us)  Ack-Policy
AC_VO  3       2       1      47               normal
AC_VI  4       3       1      94               normal
AC_BE  6       4       3      0                normal
AC_BK  10      4       7      0                normal
------------------------------------------------------------
```

Table 11-29 Description of the **display radio-2g-profile name** command output

Item	Description
Radio type	Radio type. To configure this parameter, run the **radio-type (2G radio profile view)** command.

Item	Description
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure this parameter, run the **power auto-adjust enable** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames, in TUs. To configure this parameter, run the **beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **beamforming enable** command. This configuration takes effect only on APs running V200R019C00 or earlier.
Support short preamble	Whether the short preamble is supported. To configure this parameter, run the **short-preamble disable** command.
Fragmentation threshold(Byte)	Packet fragmentation threshold, in bytes. To configure this parameter, run the **fragmentation-threshold** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure this parameter, run the **channel-switch announcement disable** command.
Channel switch mode	Channel switch announcement mode. To configure this parameter, run the **channel-switch mode** command.
Guard interval mode	802.11n/ac GI mode. To configure this parameter, run the **guard-interval-mode** command.
802.11ax Guard interval mode	802.11ax/be GI mode. ● dot8: 0.8us ● 1dot6: 1.6us ● 3dot2: 3.2us To configure this parameter, run the **guard-interval-mode** command.

Item	Description
A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure this parameter, run the **a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure this parameter, run the **ht a-mpdu max-length-exponent** command.
A-MSDU switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. To configure this parameter, run the **a-msdu enable** command.
RTS-CTS-mode	RTS/CTS mode. To configure this parameter, run the **rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure this parameter, run the **rts-cts-threshold** command.
802.11bg basic rate	802.11bg basic rate set. To configure this parameter, run the **dot11bg basic-rate** command.
802.11bg support rate	802.11bg supported rate set. To configure this parameter, run the **dot11bg supported-rate** command.
Multicast rate 2.4G	Multicast rate of wireless packets on the 2.4 GHz radio. To configure this parameter, run the **multicast-rate** command.
Interference detect switch	Whether interference detection is enabled. To configure this parameter, run the **interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure this parameter, run the **interference co-channel threshold** command.

Item	Description
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure this parameter, run the **interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure this parameter, run the **interference station threshold** command.
WMM switch	Whether the WMM function is enabled. To configure this parameter, run the **wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure this parameter, run the **wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto-off end time	End time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Wifi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure this parameter, run the **wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure this parameter, run the **rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure this parameter, run the **air-scan-profile (radio profile view)** command.

Item	Description
Smart-antenna	Status of the smart antenna function. To configure this parameter, run the **smart-antenna { enable | disable }** command.
Agile-antenna-polarization	Status of the self-adaptive polarization for agile antennas. To configure this parameter, run the **agile-antenna-polarization** command.
CCA threshold(dBm)	CCA threshold for APs. To configure this parameter, run the **cca-threshold** command.
RX sensitivity(dBm)	Receiver sensitivity threshold. To configure this parameter, run the **rx-sensitivity** command.
AGC high threshold(dBm)	Upper AGC threshold. To configure this parameter, run the **agc-threshold** command.
High PER threshold(%)	Upper valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Low PER threshold(%)	Lower valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Training interval(s)	Smart antenna training interval. To configure this parameter, run the **smart-antenna training-interval** command.
Training mpdu num	Number of MPDUs sent by an AP to STAs during smart antenna training. To configure this parameter, run the **smart-antenna training-mpdu-number** command.

Item	Description
Throughput trigger training threshold (%)	Sudden performance change threshold that triggers smart antenna training. To configure this parameter, run the **smart-antenna throughput-triggered-training** command.
VIP user bandwidth reservation ratio (%)	Percentage of bandwidth reserved for VIP users. To configure this parameter, run the **vip-user bandwidth reservation-ratio** command.
Legacy signal length compatible	Whether the L-SIG field length compatibility function of the 802.11n protocol is enabled. To configure the parameter, run the **dot11n legacy-signal-length-compatible enable** command.
RX STBC	Whether the STBC encoding function in the receive direction is enabled. To configure this parameter, run the **rx-stbc disable** command.
Fastpass users	Number of FastPass users. This parameter is valid only for DAPs. To configure this parameter, run the **fastpass users** command.
Fastpass period(ms)	FastPass scheduling period. This parameter is valid only for DAPs. To configure this parameter, run the **fastpass users** command.
Fastpass ratio(%)	Percentage of FastPass users in the scheduling period. This parameter is valid only for DAPs. To configure this parameter, run the **fastpass users** command.
Radio reload time-range	Time range during which radios are reloaded as scheduled. To configure this parameter, run the **radio-reload time-range** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure this parameter, run the **utmost-power** command.

Item	Description
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure this parameter, run the **wmm edca-ap** command.
AC_VO	AC_VO packets. To configure this parameter, run the **wmm edca-ap** command.
AC_VI	AC_VI packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BE	AC_BE packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BK	AC_BK packets. To configure this parameter, run the **wmm edca-ap** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **wmm edca-ap** command.
TXOPLimit(32us)	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration. To configure this parameter, run the **wmm edca-ap** command.

Item	Description
Ack-Policy	ACK policy. It includes: - **normal**: During 802.11 packet exchange, the receiver sends an ACK packet to confirm the receiving of a packet from the sender. - **noack**: The receiver sends no ACK packet to confirm the receiving of a packet from the sender. It applies to scenarios where communication quality is good and interference is low. To configure this parameter, run the **wmm edca-ap** command.

11.1.72 display radio-5g-profile

Function

The **display radio-5g-profile** command displays configuration and reference information about a 5G radio profile.

Format

display radio-5g-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all 5G radio profiles.	-
name *profile-name*	Displays information about a specified 5G radio profile.	The 5G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about a 5G radio profile.

Example

Display information about all 5G radio profiles.

```
<HUAWEI> display radio-5g-profile all
-------------------------------------------------------------------------
Profile name  Config Reference  Reference radios
-------------------------------------------------------------------------
default       10                4
-------------------------------------------------------------------------
Total: 1
```

Table 11-30 Description of the **display radio-5g-profile all** command output

Item	Description
Profile name	Name of a 5G radio profile.
Config Reference	Number of times a 5G radio profile is referenced.
Reference radios	Number of radios that reference a 5G radio profile.

Display information of the 5G radio profile **default**.

```
<HUAWEI> display radio-5g-profile name default
------------------------------------------------------------
Radio type                                 : 802.11ac
Power auto adjust                          : disable
Beacon interval(TUs)                       : 100
Beamforming switch                         : disable
Fragmentation threshold(Byte)              : 2346
Channel switch announcement                : enable
Channel switch mode                        : continue
Guard interval mode                        : normal
802.11ax guard interval mode               : dot8
A-MPDU switch                              : enable
HT A-MPDU length limit                     : 3
VHT A-MPDU length limit                    : 7
A-MSDU switch                              : disable
VHT A-MSDU Max frame number                : 2
RTS-CTS-mode                               : RTS-CTS
RTS-CTS-threshold                          : 2347
802.11a basic rate                         : 6 12 24
802.11a support rate                       : 6 9 12 18 24 36 48 54
Multicast rate 5G                          : 6
VHT mcs                                    : 9 9 9 9 9 9 9 9
Interference detect switch                 : disable
Co-channel frequency interference threshold(%)        : 50
Adjacent-channel frequency interference threshold(%)  : 50
Station interference threshold             :32
WMM switch                                 : enable
Mandatory switch                           : disable
Auto-off start time                        : -
Auto-off end time                          : -
WiFi-light mode                            : signal-strength
```

```
Utmost power switch                    : enable
Rrm-profile                          : default
Air-scan-profile                     : default
Smart-antenna                          : disable
Agile-antenna-polarization             : disable
CCA threshold(dBm)                     : -
RX sensitivity(dBm)                  : -128
AGC high threshold(dBm)                : -82
High PER threshold(%)                        : 80
Low PER threshold(%)                         : 20
Training interval(s)                     : auto
Training mpdu num                          : 640
Throughput trigger training threshold (%)       : 10
VIP user bandwidth reservation ratio (%)         : 20
Legacy signal length compatible                 : enable
RX STBC                                  : enable
Radio reload time-range                         : test
DFS radar-filter sensitivity                   : 4
------------------------------------------------------------
AP EDCA parameters:
------------------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit(32us)  Ack-Policy
AC_VO  3       2       1      47               normal
AC_VI  4       3       1      94               normal
AC_BE  6       4       3      0                normal
AC_BK  10      4       7      0                normal
------------------------------------------------------------
```

Table 11-31 Description of the **display radio-5g-profile name** command output

Item	Description
Radio type	Radio type. To configure this parameter, run the **radio-type (5G radio profile view)** command.
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure this parameter, run the **power auto-adjust enable** command.
Beacon interval(TUs)	Interval at which an AP sends Beacon frames, in TUs. To configure this parameter, run the **beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **beamforming enable** command. This configuration takes effect only on APs running V200R019C00 or earlier.
Fragmentation threshold(Byte)	Packet fragmentation threshold, in bytes. To configure this parameter, run the **fragmentation-threshold** command.

Item	Description
Channel switch announcement	Whether channel switch announcement is enabled. To configure this parameter, run the **channel-switch announcement disable** command.
Channel switch mode	Channel switch announcement mode. To configure this parameter, run the **channel-switch mode** command.
Guard interval mode	802.11n/ac GI mode. To configure this parameter, run the **guard-interval-mode** command.
802.11ax guard interval mode	802.11ax/be GI mode. ● dot8: 0.8us ● 1dot6: 1.6us ● 3dot2: 3.2us To configure this parameter, run the **guard-interval-mode** command.
A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure this parameter, run the **a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure this parameter, run the **ht a-mpdu max-length-exponent** command.
VHT A-MPDU length limit	Maximum length of the frame aggregated in A-MPDU mode. To configure this parameter, run the **vht a-mpdu max-length-exponent** command.
A-MSDU switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. To configure this parameter, run the **a-msdu enable** command.
VHT A-MSDU Max frame number	Maximum number of subframes that can be aggregated into an A-MSDU. To configure this parameter, run the **vht a-msdu max-frame-num** command.

Item	Description
RTS-CTS-mode	RTS/CTS mode. To configure this parameter, run the **rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure this parameter, run the **rts-cts-threshold** command.
802.11a basic rate	802.11a basic rate set. To configure this parameter, run the **dot11a basic-rate** command.
802.11a support rate	802.11a supported rate set. To configure this parameter, run the **dot11a supported-rate** command.
Multicast rate 5G	Multicast rate of wireless packets on the 5 GHz radio. To configure this parameter, run the **multicast-rate** command.
VHT mcs	Maximum MCS value corresponding to a specific number of 802.11ac spatial streams. To configure this parameter, run the **vht mcs-map** command.
Interference detect switch	Whether interference detection is enabled. To configure this parameter, run the **interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure this parameter, run the **interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure this parameter, run the **interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure this parameter, run the **interference station threshold** command.

Item	Description
WMM switch	Whether the WMM function is enabled. To configure this parameter, run the **wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure this parameter, run the **wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto-off end time	End time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
WiFi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure this parameter, run the **wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure this parameter, run the **rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure this parameter, run the **air-scan-profile (radio profile view)** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure this parameter, run the **utmost-power** command.
Smart-antenna	Status of the smart antenna function. To configure this parameter, run the **smart-antenna { enable | disable }** command.

Item	Description
Agile-antenna-polarization	Status of the self-adaptive polarization for agile antennas. To configure this parameter, run the **agile-antenna-polarization** command.
CCA threshold(dBm)	CCA threshold for APs. To configure this parameter, run the **cca-threshold** command.
RX sensitivity(dBm)	Receiver sensitivity threshold. To configure this parameter, run the **rx-sensitivity** command.
AGC high threshold(dBm)	Upper AGC threshold. To configure this parameter, run the **agc-threshold** command.
High PER threshold(%)	Upper valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Low PER threshold(%)	Lower valid PER threshold in the smart antenna algorithm. To configure this parameter, run the **smart-antenna valid-per-scope** command.
Training interval(s)	Smart antenna training interval. To configure this parameter, run the **smart-antenna training-interval** command.
Training mpdu num	Number of MPDUs sent by an AP to STAs during smart antenna training. To configure this parameter, run the **smart-antenna training-mpdu-number** command.
Throughput trigger training threshold (%)	Sudden performance change threshold that triggers smart antenna training. To configure this parameter, run the **smart-antenna throughput-triggered-training** command.

Item	Description
VIP user bandwidth reservation ratio (%)	Percentage of bandwidth reserved for VIP users. To configure this parameter, run the **vip-user bandwidth reservation-ratio** command.
Legacy signal length compatible	Whether the L-SIG field length compatibility function of the 802.11n protocol is enabled. To configure the parameter, run the **dot11n legacy-signal-length-compatible enable** command.
RX STBC	Whether the STBC encoding function in the receive direction is enabled. To configure this parameter, run the **rx-stbc disable** command.
Radio reload time-range	Time range during which radios are reloaded as scheduled. To configure this parameter, run the **radio-reload time-range** command.
DFS radar-filter sensitivity	Sensitivity level of correction for false radar detection. To configure this parameter, run the **dfs radar-filter sensitivity** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure this parameter, run the **wmm edca-ap** command.
AC_VO	AC_VO packets. To configure this parameter, run the **wmm edca-ap** command.
AC_VI	AC_VI packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BE	AC_BE packets. To configure this parameter, run the **wmm edca-ap** command.
AC_BK	AC_BK packets. To configure this parameter, run the **wmm edca-ap** command.

Item	Description
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **wmm edca-ap** command.
TXOPLimit(32us)	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration. To configure this parameter, run the **wmm edca-ap** command.
Ack-Policy	ACK policy. It includes: ● **normal**: During 802.11 packet exchange, the receiver sends an ACK packet to confirm the receiving of a packet from the sender. ● **noack**: The receiver sends no ACK packet to confirm the receiving of a packet from the sender. It applies to scenarios where communication quality is good and interference is low. To configure this parameter, run the **wmm edca-ap** command.

11.1.73 display references radio-2g-profile

Function

The **display references radio-2g-profile** command displays reference information about a 2G radio profile.

Format

display references radio-2g-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified 2G radio profile.	The 2G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references radio-2g-profile** command to view reference information about a 2G radio profile.

Example

Display reference information about the 2G radio profile **default**.

```
<HUAWEI> display references radio-2g-profile name default
----------------------------------------------------------------------
Reference type  Reference name                Reference radio
----------------------------------------------------------------------
AP-group        ap-group1                     Radio-0
----------------------------------------------------------------------
Total:1
```

Table 11-32 Description of the **display references radio-2g-profile** command output

Item	Description
Reference type	Type of the profile by which a 2G radio profile is referenced.
Reference name	Name of the profile by which a 2G radio profile is referenced.
Reference radio	Radio to which a 2G radio profile is referenced.

11.1.74 display references radio-5g-profile

Function

The **display references radio-5g-profile** command displays reference information about a 5G radio profile.

Format

display references radio-5g-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified 5G radio profile.	The 5G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references radio-5g-profile** command to view reference information about a 5G radio profile.

Example

Display reference information about the 5G radio profile **default**.

```
<HUAWEI> display references radio-5g-profile name default
---------------------------------------------------------------------
Reference type  Reference name                  Reference radio
---------------------------------------------------------------------
AP-group        ap-group1                       Radio-0
---------------------------------------------------------------------
Total:1
```

Table 11-33 Description of the **display references radio-5g-profile** command output

Item	Description
Reference type	Type of the profile by which a 5G radio profile is referenced.

Item	Description
Reference name	Name of the profile by which a 5G radio profile is referenced.
Reference radio	Radio to which a 5G radio profile is referenced.

11.1.75 display references regulatory-domain-profile

Function

The **display references regulatory-domain-profile** command displays reference information about a regulatory domain profile.

Format

display references regulatory-domain-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified regulatory domain profile.	The regulatory domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references regulatory-domain-profile** command to view reference information about a regulatory domain profile.

Example

Display reference information about the regulatory domain profile **default**.

```
<HUAWEI> display references regulatory-domain-profile name default
------------------------------------------------------------
Reference type           Reference name
------------------------------------------------------------
AP-group                default
AP-group                1
```

```
------------------------------------------------------------
Total: 2
```

Table 11-34 Description of the **display references regulatory-domain-profile** command output

Item	Description
Reference type	Type of the profile by which a regulatory domain profile is referenced.
Reference name	Name of the profile by which a regulatory domain profile is referenced.

11.1.76 display references softgre-profile

Function

The **display references softgre-profile** command displays reference information about a soft GRE profile.

Format

display references softgre-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified soft GRE profile.	The specified soft GRE profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about a soft GRE profile.

Example

Display reference information about the soft GRE profile **soft1**.

```
<HUAWEI> display references softgre-profile name soft1
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
VAP profile                 vap1
------------------------------------------------------------------------
Total: 1
```

Table 11-35 Description of the **display references softgre-profile** command output

Item	Description
Reference type	Type of the profile by which a soft GRE profile is referenced.
Reference name	Name of the profile by which a soft GRE profile is referenced.

11.1.77 display references ssid-profile

Function

The **display references ssid-profile** command displays reference information about an SSID profile.

Format

display references ssid-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified SSID profile.	The SSID profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references ssid-profile** command to view reference information about an SSID profile.

Example

Display reference information about the SSID profile **default**.

```
<HUAWEI> display references ssid-profile name default
--------------------------------------------------------------------
Reference type                   Reference name
--------------------------------------------------------------------
VAP profile                      vap-profile1
--------------------------------------------------------------------
Total:1
```

Table 11-36 Description of the **display references ssid-profile** command output

Item	Description
Reference type	Type of the profile by which an SSID profile is referenced.
Reference name	Name of the profile by which an SSID profile is referenced.

11.1.78 display references vap-profile

Function

The **display references vap-profile** command displays reference information about a VAP profile.

Format

display references vap-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified VAP profile.	The VAP profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references vap-profile** command to view reference information about a VAP profile.

Example

Display reference information about the VAP profile **default**.

```
<HUAWEI> display references vap-profile name default
------------------------------------------------------------------------------
Reference type     Reference name                     Reference radio  WLAN ID
------------------------------------------------------------------------------
AP group          group1                        Radio-0          1
------------------------------------------------------------------------------
Total: 1
```

Table 11-37 Description of the **display references vap-profile** command output

Item	Description
Reference type	Type of the profile by which a VAP profile is referenced.
Reference name	Name of the profile by which a VAP profile is referenced.
Reference radio	AP radio by which a VAP profile is referenced.
WLAN ID	WLAN ID of a VAP.

11.1.79 display references vlan pool

Function

The **display references vlan pool** command displays reference information about a VLAN pool.

Format

display references vlan pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Displays reference information about a specified VLAN pool.	The VLAN pool must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view profiles that reference a VLAN pool.

Example

Display reference information about the VLAN pool **pool1**.

```
<HUAWEI> display references vlan pool pool1
--------------------------------------------------------------------------------
Reference type   Reference name                    Reference radio  WLAN ID
--------------------------------------------------------------------------------
AP group         default                           Radio-0          1
AP group         default                           Radio-1          1
AP group         default                           Radio-2          1
AP group         default                           Radio-0          2
AP group         default                           Radio-1          2
AP group         default                           Radio-2          2
AP ID            0                                 Radio-0          2
AP ID            0                                 Radio-1          2
VAP profile      1
user group       123
--------------------------------------------------------------------------------
Total: 10
```

Table 11-38 Description of the **display references vlan pool** command output

Item	Description
Reference type	Type of a profile that references a VLAN pool.
Reference name	Name of a profile that references a VLAN pool.
Reference radio	Radio that references a VLAN pool. This item is displayed only when a VLAN pool is configured as the service VLAN for a VAP profile applied in the AP group radio view or AP radio view.
WLAN ID	WLAN ID that references a VLAN pool. This item is displayed only when a VLAN pool is configured as the service VLAN for a VAP profile applied in the AP group radio view or AP radio view.

11.1.80 display regulatory-domain-profile

Function

The **display regulatory-domain-profile** command displays configuration and reference information about a regulatory domain profile.

Format

display regulatory-domain-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all regulatory domain profiles.	-
name *profile-name*	Displays information about a specified regulatory domain profile.	The regulatory domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display regulatory-domain-profile** command to view configuration and reference information about a regulatory domain profile.

Example

Display information about all regulatory profiles.

```
<HUAWEI> display regulatory-domain-profile all
------------------------------------------------------------
Profile name        Reference
------------------------------------------------------------
default             6
------------------------------------------------------------
Total: 1
```

Table 11-39 Description of the **display regulatory-domain-profile all** command output

Item	Description
Profile name	Regulatory domain profile name.
Reference	Number of times a regulatory domain profile is referenced.

Display information about the regulatory domain profile **default**.

```
<HUAWEI> display regulatory-domain-profile name default
------------------------------------------------------------
```

```
Profile name           : default
Country code           : CN
2.4G dca channel-set  : 1,6,11
5G dca bandwidth       : 20mhz
5G dca channel-set    : 149,153,157,161,165
6G dca bandwidth       : 20mhz
6G dca channel-set    : -
Wideband switch       : enable
Channel load mode     : outdoor
------------------------------------------------------------
```

Table 11-40 Description of the **display regulatory-domain-profile name** command output

Item	Description
Profile name	Regulatory domain profile name.
Country code	Country code. To configure the parameter, run the **country-code** command.
2.4G dca channel-set	2.4G radio calibration channel set. To configure the parameter, run the **dca-channel channel-set** command.
5G dca bandwidth	5G radio calibration bandwidth. To configure the parameter, run the **dca-channel bandwidth** command.
5G dca channel-set	5G radio calibration channel set. To configure the parameter, run the **dca-channel channel-set** command.
6G dca bandwidth	6G radio calibration bandwidth. To configure the parameter, run the **dca-channel bandwidth** command.
6G dca channel-set	6G radio calibration channel set. To configure the parameter, run the **dca-channel channel-set** command.
Wideband switch	Indicates whether the wideband function, that is, the 4.9 GHz frequency band, of the regulatory domain profile is enabled. ● enable: The wideband function is enabled. ● disable: The wideband function is disabled. To configure this parameter, run the **wideband enable** command.

Item	Description
Channel load mode	Channel load mode. ● outdoor: outdoor mode ● indoor: indoor mode To configure this parameter, run the **channel-load-mode indoor** command.

11.1.81 display softgre-profile

Function

The **display softgre-profile** command displays configuration and reference information about a soft GRE profile.

Format

display softgre-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all soft GRE profiles.	-
name *profile-name*	Displays information about a specified soft GRE profile.	The specified soft GRE profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration and reference information about soft GRE profiles.

Example

Display information about all soft GRE profiles.

```
<HUAWEI> display softgre-profile all
--------------------------------------------------------------------------------
Profile name                     Reference     IP address
--------------------------------------------------------------------------------
soft1                          0              10.10.1.1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-41 Description of the **display softgre-profile all** command output

Item	Description
Profile name	Name of a soft GRE profile.
Reference	Number of times a soft GRE profile is referenced.
IP address	Tunnel destination address configured in the soft GRE profile.

Display information about the soft GRE profile **soft1**.

```
<HUAWEI> display softgre-profile name soft1
------------------------------------------------------------------------
Destination IP-address : 10.10.1.1
Keepalive               : enable
Keepalive period        : 5(s)
Keepalive retry-times  : 3
Untagged VLAN           : 101
------------------------------------------------------------------------
```

Table 11-42 Description of the **display softgre-profile name** command output

Item	Description
Destination IP-address	Destination IP address of the soft GRE tunnel. To configure this parameter, run the **destination (soft GRE profile view)** command.
Keepalive	Whether Keepalive detection is enabled for the soft GRE tunnel. To configure this parameter, run the **keepalive** command.
Keepalive period	Interval for sending Keepalive packets. To configure this parameter, run the **keepalive period** *period* command.
Keepalive retry-times	Unreachable counter. To configure this parameter, run the **keepalive period** *period* **retry-times** *retry-times* command.

Item	Description
Untagged VLAN	VLAN tag removed from the soft GRE tunnel packets sent by an AP. To configure this parameter, run the **untagged vlan (soft GRE profile view)** command.

11.1.82 display softgre-tunnel-status

Function

The **display softgre-tunnel-status** command displays soft GRE tunnel information on a specified AP.

Format

display softgre-tunnel-status { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays soft GRE tunnel information on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays soft GRE tunnel information on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the soft GRE tunnel status and Keepalive information.

Example

Display soft GRE tunnel information on the AP named **area_1**.

```
<HUAWEI> display softgre-tunnel-status ap-name area_1
----------------------------------------------------------------------------------------------------
Destination IP-address              Status      Keepalive    Request     Response
----------------------------------------------------------------------------------------------------
```

```
10.10.1.1                          UP          enable        1           0
------------------------------------------------------------------------------------------------------
```

Table 11-43 Description of the **display softgre-tunnel-status** command output

Item	Description
Destination IP-address	Destination IP address of the soft GRE tunnel. To configure this parameter, run the **destination (soft GRE profile view)** command.
Status	Status of a soft GRE tunnel. ● DOWN: When Keepalive detection is enabled, the device detects that the peer end is unreachable and sets the soft GRE tunnel status to **DOWN**. ● UP: When Keepalive detection is disabled or Keepalive detection is enabled and the peer is reachable, the device sets the soft GRE tunnel status to **UP**.
Keepalive	Whether Keepalive detection is enabled for the soft GRE tunnel. To configure this parameter, run the **keepalive (soft GRE profile view)** command.
Request	Number of Keepalive request packets sent by the AP.
Response	Number of Keepalive response packets received by the AP.

11.1.83 display ssid-profile

Function

The **display ssid-profile** command displays configuration and reference information about SSID profiles.

Format

display ssid-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all SSID profiles.	-
name *profile-name*	Displays information about a specified SSID profile.	The SSID profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ssid-profile** command to view configuration and reference information about SSID profiles.

Example

Display information about all SSID profiles.

```
<HUAWEI> display ssid-profile all
------------------------------------------------------------------
Profile name  Beacon 2.4G/5G/6G rate(Mbps)  Reference  SSID
------------------------------------------------------------------
default       1/6                           2          GUEST-WLAN
------------------------------------------------------------------
Total: 1
```

Table 11-44 Description of the **display ssid-profile all** command output

Item	Description
Profile name	SSID profile name.
Beacon 2.4G/5G/6G rate(Mbps)	Rate of management frames on each frequency band.
Reference	Number of times an SSID profile is referenced.
SSID	SSID name.

Display information about the SSID profile **default**.

```
<HUAWEI> display ssid-profile name default
------------------------------------------------------------------
Profile ID                    : 0
```

```
SSID                                  : GUEST-WLAN
SSID hide                             : disable
Association timeout(min)              : 5
Max STA number                        : 64
Action upon reaching the max STA number : SSID broadcast
Legacy station                        : enable
DTIM interval                         : 1
Beacon 2.4G rate(Mbps)                : 1
Beacon 5G rate(Mbps)                  : 6
Beacon 6G rate(Mbps)                  : 6
802.11bg basic rate                   : 1 6 9
802.11bg support rate                 : 1 2 9 12
802.11a basic rate                    : 6 9
802.11a support rate                  :
Deny-broadcast-probe                  : disable
Probe-response-retry num              : 1
802.11r                               : disable
  802.11r authentication              : -
802.11r private                       : disable
802.11r reassociation timeout (s)     : 5
QOS CAR inbound CIR(kbit/s)           : -
QOS CAR inbound PIR(kbit/s)           : -
QOS CAR inbound CBS(byte)             : -
QOS CAR inbound PBS(byte)             : -
U-APSD                                : enable
Active dull client                    : disable
Force active dull client              : disable
MU-MIMO                               : disable
MU-MIMO optimize                      : disable
TWT switch                            : disable
QBSS load                             : disable
Single txchain                        : disable
Advertise AP name                     : disable
Service guarantee                     : performance first
Inter-AC roam switch                  : disable
Game-turbo switch                     : enable
VHT tx mcs-map nss value              : -
VHT tx mcs-map map value              : -
VHT rx mcs-map nss value              : -
VHT rx mcs-map map value              : -
HE tx mcs-map nss value               : 8
HE tx mcs-map map value               : 11
HE rx mcs-map nss value               : 8
HE rx mcs-map map value               : 11
Beamforming switch                    : enable
OFDMA downlink switch                 : enable
OFDMA uplink switch                   : enable
ER-SU                                 : enable
----------------------------------------------------------------------
WMM EDCA client parameters:
----------------------------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit(32us)
AC_VO  3       2       2      47
AC_VI  4       3       2      94
AC_BE  10      4       3      0
AC_BK  10      4       7      0
----------------------------------------------------------------------
WMM MUEDCA client parameters:
----------------------------------------------------------------------
       ECWmax  ECWmin  AIFSN  MUEDCA Timer(8TUs)
AC_VO  3       2       2      1
AC_VI  4       3       2      1
AC_BE  10      4       3      1
AC_BK  10      4       7      1
----------------------------------------------------------------------
```

Table 11-45 Description of the **display ssid-profile name** command output

Item	Description
Profile ID	ID of an SSID profile.
SSID	SSID name. To configure this parameter, run the **ssid** command.
SSID hide	SSID hiding. To configure this parameter, run the **ssid-hide enable** command.
Association timeout(min)	Association timeout period. To configure this parameter, run the **association-timeout** command.
Max STA number	Maximum number of users. To configure this parameter, run the **max-sta-number (SSID profile view)** command.
Action upon reaching the max STA number	Action to take when the number of access users reaches the maximum. ● SSID hide: hiding the SSID ● SSID broadcast: broadcasting the SSID ● priority-based STA replacement: allowing access of VIP users instead of non-VIP users based on priorities To configure this parameter, run the **reach-max-sta** command.
Legacy station	Whether to permit access of non-HT STAs. To configure this parameter, run the **legacy-station disable** command.
DTIM interval	DTIM interval. To configure this parameter, run the **dtim-interval** command.
Beacon 2.4G rate(Mbps)	Rate at which 2.4 GHz management frames are sent. To configure this parameter, run the **beacon-2g-rate** command.
Beacon 5G rate(Mbps)	Rate at which 5 GHz management frames are sent. To configure this parameter, run the **beacon-5g-rate** command.

Item	Description
Beacon 6G rate(Mbps)	Rate at which 6 GHz management frames are sent. To configure this parameter, run the **beacon-6g-rate** command
802.11bg basic rate	802.11b/g basic rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11bg basic-rate** (SSID profile view) command.
802.11bg support rate	802.11b/g supported rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11bg supported-rate** (SSID profile view) command.
802.11a basic rate	802.11a basic rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11a basic-rate** (SSID profile view) command.
802.11a support rate	802.11a supported rate set. If no information is displayed, no configuration is available and the configuration in the radio profile takes effect. To configure this parameter, run the **dot11a supported-rate** (SSID profile view) command.
Deny-broadcast-probe	Whether an AP is configured not to respond to broadcast Probe Request frames. To configure this parameter, run the **deny-broadcast-probe enable** command.

Item	Description
Probe-response-retry num	Number of times Probe Response packets are retransmitted. To configure this parameter, run the **probe-response-retry** command.
802.11r	802.11r roaming. To configure this parameter, run the **dot11r enable** command.
802.11r authentication	802.11r authentication mode. To configure this parameter, run the **dot11r enable** command.
802.11r proprietary	Whether Huawei's proprietary 802.11r function is enabled. To configure this parameter, run the **dot11r proprietary** command.
802.11r reassociation timeout (s)	802.11r reassociation timeout interval. To configure this parameter, run the **dot11r reassociate-timeout** command.
QOS CAR inbound CIR(kbit/s)	CIR in the QoS CAR profile applied to the inbound direction of an interface, which is the allowed rate at which traffic can pass through. To configure this parameter, run the **qos car (SSID profile view)** command.
QOS CAR inbound PIR(kbit/s)	PIR in the QoS CAR profile applied to the inbound direction of an interface, which is the maximum rate of traffic that can pass through an interface. To configure this parameter, run the **qos car (SSID profile view)** command.
QOS CAR inbound CBS(byte)	CBS in the QoS CAR profile applied to the inbound direction of an interface, which is the average volume of burst traffic that can pass through an interface. To configure this parameter, run the **qos car (SSID profile view)** command.

Item	Description
QOS CAR inbound PBS(byte)	PBS in the QoS CAR profile applied to the inbound direction of an interface, which is the maximum volume of burst traffic that can pass through an interface. To configure this parameter, run the **qos car (SSID profile view)** command.
U-APSD	Whether the U-APSD function is enabled. To configure this parameter, run the **u-apsd enable** command.
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure this parameter, run the **active-dull-client enable** command.
Force active dull client	Whether the function of forcibly preventing terminals from entering power-saving mode is enabled. To configure this parameter, run the **active-dull-client force enable** command.
MU-MIMO	Whether downlink MU-MIMO scheduling is enabled. To configure this parameter, run the **mu-mimo disable** command.
MU-MIMO optimize	Whether the MU-MIMO optimization function is enabled. To configure this parameter, run the **mu-mimo optimize enable** command.
TWT switch	Whether the TWT function is enabled. To configure this parameter, run the **twt enable** command.
QBSS load	Whether the QBSS load function is enabled. To configure this parameter, run the **qbss-load enable** command.

Item	Description
Single txchain	Whether to enable the single-antenna transmission mode. To configure this parameter, run the **single-txchain enable** command.
Advertise AP name	Whether Beacon frames are enabled to carry the AP name. To configure this parameter, run the **advertise-ap-name enable** command.
Service guarantee	Service guarantee mode. To configure this parameter, run the **service-guarantee** command.
Inter-AC roam switch	Whether inter-AC roaming is enabled. To configure this parameter, run the **inter-ac roam disable** command.
Game-turbo switch	Whether the game turbo function is enabled. To configure this parameter, run the **game-turbo disable** command.
VHT tx mcs-map nss value	Maximum number of spatial streams sent in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.
VHT tx mcs-map map value	Maximum MCS value of spatial streams sent in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.
VHT rx mcs-map nss value	Maximum number of spatial streams received in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.
VHT rx mcs-map map value	Maximum MCS value of spatial streams received in 802.11ac. To configure this parameter, run the **vht mcs-map (SSID profile view)** command.

Item	Description
HE tx mcs-map nss value	Maximum number of spatial streams sent in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
HE tx mcs-map map value	Maximum MCS value of spatial streams sent in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
HE rx mcs-map nss value	Maximum number of spatial streams received in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
HE rx mcs-map map value	Maximum MCS value of spatial streams received in 802.11ax. To configure this parameter, run the **he mcs-map (SSID profile view)** command.
Beamforming switch	Whether the beamforming function is enabled. To configure this parameter, run the **beamforming disable** command. This configuration takes effect only on APs running V200R019C10 or later.
OFDMA downlink switch	Whether downlink OFDMA is enabled. To configure this parameter, run the **ofdma downlink disable** command.
OFDMA uplink switch	Whether uplink OFDMA is enabled. To configure this parameter, run the **ofdma uplink disable** command.
ER-SU	Whether the extended-range single-user (ER SU) function is enabled. To configure this parameter, run the **er-su disable** command.
WMM EDCA client parameters	WMM parameters for STAs. To configure this parameter, run the **wmm edca-client (SSID profile view)** command.
AC_VO	AC_VO packets.

Item	Description
AC_VI	AC_VI packets.
AC_BE	AC_BE packets.
AC_BK	AC_BK packets.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time.
TXOPLimit(32us)	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger value indicates a longer duration.
WMM MUEDCA client parameters	MU EDCA parameters for STAs. To configure this parameter, run the **wmm mu-edca-client (SSID profile view)** command.
MUEDCA Timer(8TUs)	MU EDCA timer, which indicates the validity duration of MU EDCA parameters. When the timer is 0, the conventional EDCA parameters take effect.

11.1.84 display sta-offline-delay configuration

Function

The **display sta-offline-delay configuration** command displays the STA offline delay configuration.

Format

display sta-offline-delay configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the STA offline delay configuration.

Example

Display the STA offline delay configuration.

```
<HUAWEI> display sta-offline-delay configuration
------------------------------------------------------------------------------
Enable switch                    : disable
Aging time(s)                    : 180
Full station reject switch         : disable
Max number                        : 2048
------------------------------------------------------------------------------
```

Table 11-46 Description of the **display sta-offline-delay configuration** command output

Item	Description
Enable switch	Whether to enable the STA offline delay function. To configure the parameter, run the **sta-offline-delay enable** command.
Aging time(s)	Aging time of the STA offline delay state To configure the parameter, run the **sta-offline-delay aging-time** command.
Full station reject switch	Whether to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum. To configure the parameter, run the **sta-offline-delay full-sta-reject enable** command.
Max number	Maximum number of STAs that are allowed to delay going offline. To configure the parameter, run the **sta-offline-delay max-number** command.

11.1.85 display station

Function

The **display station** command displays access information about STAs.

Format

display station { **ap-group** *ap-group-name* | **ap-name** *ap-name* | **ap-id** *ap-id* | **ssid** *ssid* | **sta-mac** *sta-mac-address* | **vlan** *vlan-id* | **all** }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays STA access information about a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays STA access information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays STA access information about the AP with a specified ID.	The AP ID must exist.
ssid *ssid*	Displays STA access information about a specified SSID.	The SSID must exist. To specify an SSID starting with a space, include the SSID with double quotation marks (" "). For example, in the SSID **" hello"**, the double quotation marks at the start and end of the SSID occupy two characters. To specify an SSID starting with a double quotation mark ("), enter an escape character (\) before the double quotation mark. For example, in the SSID **\"hello**, the escape character (\) occupies one character.

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays access information about a STA with the specified MAC address.	The STA's MAC address must exist. STA information can be displayed only when the AP associated with the STA is in normal state.
vlan *vlan-id*	Displays STA access information about a specified VLAN.	-
all	Displays access information about all STAs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station** command to view access information about STAs. You can run the **display access-user** command to view access information about online wired and wireless users. The information includes users' authentication, authorization, and accounting information.

Capabilities of a STA displayed in the **display station sta-mac** *sta-mac-address* command output are negotiated between the STA and AP and are affected by both their capabilities, which may be different from the actual STA capabilities.

Example

Display access information about all STAs.

```
<HUAWEI> display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-------------------------------------------------------------------------------------------------------------------
STA MAC          AP ID Ap name        Rf/WLAN  Band  Type  Rx/Tx      RSSI  VLAN  IP address    SSID
Status
-------------------------------------------------------------------------------------------------------------------
00e0-fc12-3456   0     00e0-fc07-6f80 0/2      2.4G  11n   3/8        -70   10    10.10.10.253  tap1      Normal
-------------------------------------------------------------------------------------------------------------------
Total: 1 2.4G: 1 5G: 0 6G: 0
```

Table 11-47 Description of the **display station all** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	AP ID.
Ap name	AP name.
Rf/WLAN	Radio ID/VAP ID.
Band	Frequency band of a radio.
Type	Protocol type of a radio.
Rx/Tx	Rate at which the AP receives packets from the STA/Rate at which the AP sends packets to the STA.
RSSI	RSSI of signals received by an AP from a STA.
VLAN	VLAN ID of a STA.
IP address	IP address of a STA.
SSID	SSID name.
Status	Status of a STA. **Normal** indicates that the STA is in normal state, and **Delay** indicates that the STA is in offline delay state. This item is displayed only when the STA offline delay function is enabled. To enable the STA offline delay function, run the **sta-offline-delay enable** command.

Display access information about a specified STA.

```
<HUAWEI> display station sta-mac 00e0-fcb4-2689
------------------------------------------------------------------------------
Station MAC-address                          : 00e0-fc12-3456
Station IP-address                           : 10.2.2.254
                                             : FE80::20E:8EFF:FE04:2DEB
Station gateway                              : 10.2.2.2
                                             : FE80::2E97:B1FF:FEB0:6A48
Associated SSID                              : test
Station online time(ddd:hh:mm:ss)            : 000:00:03:14
The upstream SNR(dB)                         : 80.0
The upstream aggregate receive power(dBm)    : -28.0
Station connect rate(Mbps)                   : 61
Station connect channel                      : 36
Station inactivity time(ddd:hh:mm:ss)        : 000:00:00:00
Station current state
  Authorized for data transfer               : Yes
  QoS enabled                                : Yes
  HT rates enabled                           : Yes
  Power save mode enabled                    : Yes
```

```
  Auth reference held                     : No
  UAPSD enabled                           : No
  UAPSD triggerable                       : No
  UAPSD SP in progress                     : No
  This is an ATH node                     : No
  WDS workaround req                       : No
  WDS link                               : No
  PMF negotiation                         : No
Station's HT capability                   : WQ
Station capabilities                      : E
Station PMF capabilities                   : PMFC=0,PMFR=0
Station VHT capabilities
  256QAM capabilities                      : Yes
  VHT explicit beamforming capabilities       : Yes
  MU-MIMO capabilities                     : Yes
Station HE capabilities
  OFDMA capabilities                       : No
  BSS color capabilities                    : No
  HE SU beamformee capabilities              : No
Station's RM capabilities
  Neighbor Report                          : Yes
  Beacon Passive Measurement                 : Yes
  Beacon Active Measurement                  : Yes
  Beacon Table Measurement                   : Yes
  Link Measurement                         : Yes
  Transmit power adaptation                  : Yes
Station EHT capabilities
  MRU capabilities                         : Yes
  BE SU beamformee capabilities              : Yes
  DL MU-MIMO Partial Bandwidth               : Yes
  UL MU-MIMO Partial Bandwidth               : Yes
  MLO capabilities                         : Yes
Station's RSSI(dBm)                        : -28
Station's radio mode                       : 11n
Station's AP ID                          : 0
Station's AP Name                          : area_3
Station's ORU ID                          : -
Station's Radio ID                        : 1
Station's Authentication Method              : Open
Station's Cipher Type                      : NO CIPHER
Station's User Name                        : b8782eb42689
Station's Vlan ID                         : 22
Station's Channel Band-width                 : 20MHz
Station's asso BSSID                       : 00e0-fc12-3457
Station's state                          : Asso with auth
Station's QoS Mode                         : WMM
Station's HT Mode                          : HT20
Station's MCS value                        : 9
Station's NSS value                        : 2
Station's Short GI                        : nonsupport
Station's roam state                       : No
HAC CAPWAP IP                              : -
HAP CAPWAP IP                              : 10.23.100.1
Supported band                             : 2.4G/5G
Supported 2.4G channels                      : -
Supported 5G channels                        : 36,40,44,48,52,56,60,64
                                      : 149,153,157,161,165
Supported 6G channels                        : -
802.11k support                           : Yes
802.11r support                           : Yes
802.11r proprietary support                  : No
Available for roaming                       : Yes
Sticky station or not                      : No
Aimless roaming support in sticky state       : Yes
Station device type                        : -
Station identify info
  Category name                            : -
  Vendor name                              : -
  Model name                               : -
```

```
  OS                                      : -
U-APSD list:
-------------------------------------------------------
AC-VI        AC-VO       AC-BE        AC-BK
-------------------------------------------------------
not-support  not-support  not-support  not-support
-------------------------------------------------------
------------------------------------------------------------------------------
```

Table 11-48 Description of the **display station sta-mac** *sta-mac-address* command output

Item	Description
Station MAC-address	MAC address of a STA.
Station IP-address	IP address of a STA.
Station gateway	Gateway address of a STA. **NOTE** If the device obtains the STA's gateway address through DHCP, the parameter displays as the obtained gateway address; otherwise, the parameter displays as 0.0.0.0.
Associated SSID	SSID of a service set with which a STA is associated.
Station online time(ddd:hh:mm:ss)	Online duration of a STA, in the format of ddd:hh:mm:ss.
The upstream SNR(dB)	SNR of a STA received by an AP, in dB.
The upstream aggregate receive power(dBm)	Transmit power of a STA received by an AP, in dBm.
Station connect rate(Mbps)	Connection rate of a STA, in Mbit/s. Affected by wireless environments, antenna angles, and other factors, the actual connection rate of a STA cannot reach the upper limit.
Station connect channel	Channel used by a STA.
Station inactivity time(ddd:hh:mm:ss)	Idle duration of a STA, in the format of ddd:hh:mm:ss.
Station current state	Current status of a STA.
Authorized for data transfer	Whether a STA is authenticated.
QoS enabled	Whether QoS is enabled on a STA.
HT rates enabled	Whether 802.11n is enabled on a STA.
Power save mode enabled	Whether the power saving mode is enabled on a STA.

Item	Description
Auth reference held	Whether the authentication reference flag is set.
UAPSD enabled	Whether UAPSD is enabled.
UAPSD triggerable	UAPSD can be triggered, waiting for a STA to send a trigger frame to the AP.
UAPSD SP in progress	Whether the UAPSD mode is in the service period (SP).
This is an ATH node	Whether the wireless network adapter uses the Atheros chip.
WDS workaround req	Whether the AP uses a patch used to fix bugs of Atheros Owl series chips in WDS scenarios. This item indicates whether the AP uses the patch.
WDS link	STA that is a node on the WDS link.
PMF negotiation	Whether a STA implements the PMF negotiation.
Station's HT capability	HT capability of a STA. ● A: Advanced coding ● W: HT40 channel width ● P: MIMO power save disabled ● Q: Static MIMO power save ● R: Dynamic MIMO power save ● G: Greenfield preamble ● S: Short GI enabled (HT40) ● D: Delayed block ACK ● M: Max A-MSDU size
Station capabilities	Capabilities of a STA. ● E: ESS ● I: IBSS ● c: CF Pollable ● C: CF-Poll Request ● P: Privacy ● S: Short Preamble ● B: PBCC ● A: Channel Agility ● s: Short Slot Time ● D: DSSS-OFDM

Item	Description
Station PMF capabilities	PMF capability of a STA. **PMFC** indicates whether the optional mode is used, and **PMFR** indicates whether the mandatory mode is used. - PMFC=0,PMFR=0: PMF is not supported. - PMFC=1,PMFR=0: PMF in optional mode is used. - PMFC=1,PMFR=1: PMF in mandatory mode is used.
Station VHT capabilities	Whether a STA supports 802.11ac.
256QAM capabilities	Whether a STA supports 256-QAM.
VHT explicit beamforming capabilities	Whether a STA supports 802.11ac explicit beamforming.
MU-MIMO capabilities	Whether a STA supports MU-MIMO.
Station HE capabilities	Whether a STA supports 802.11ax.
OFDMA capabilities	Whether a STA supports OFDMA.
BSS color capabilities	Whether a STA supports BSS Color.
OFDMA RA capabilities	Whether a STA supports OFDMA RA.
TRS capabilities	Whether a STA can receive frames with the TRS field.
BSR capabilities	Whether a STA can receive frames with the BSR field.
DL MU-MIMO partialband capabilities	Whether a STA supports partial-bandwidth downlink MU-MIMO.
UL MU-MIMO fullband capabilities	Whether a STA supports full-bandwidth uplink MU-MIMO.
UL MU-MIMO partialband capabilities	Whether a STA supports partial-bandwidth uplink MU-MIMO.
Dynamic SMPS capabilities	Whether a STA supports Spatial Multiplexing Power Save (SMPS).
HE SU beamformee capabilities	Whether a STA supports HE beamforming.
Station's RM capabilities	Radio management capability of a STA.
Neighbor Report	Whether a STA can obtain information about neighboring APs.

Item	Description
Beacon Passive Measurement	Whether a STA can report information about neighboring APs in passive mode.
Beacon Active Measurement	Whether a STA can report information about neighboring APs in active mode.
Beacon Table Measurement	Whether a STA can report information about neighboring APs in Beacon table mode.
Link Measurement	Whether a STA supports link measurement. ● Yes: supported ● No: not supported
Transmit Power Adaptation	Whether a STA supports TPC. ● Yes: supported ● No: not supported
Station EHT capabilities	802.11be radio management capability of a STA.
MRU capabilities	Whether a STA supports MRU.
BE SU beamformee capabilities	Whether a STA supports SU beamformee.
DL MU-MIMO Partial Bandwidth	Whether a STA supports downlink MU-MIMO.
UL MU-MIMO Partial Bandwidth	Whether a STA supports uplink MU-MIMO.
MLO capabilities	Whether a STA supports MLO.
Station's RSSI(dBm)	RSSI of signals received by an AP from a STA, in dBm.
Station's radio mode	Radio mode of a STA.
Station's AP ID	AP ID associated with a STA.
Station's AP Name	Name of the AP which a STA associates with.
Station's ORU ID	ID of the ORU associated with a STA in a distributed AP scenario. Particularly, if the STA associates with the 2.4 GHz radio, two ORU IDs are displayed, with one of which the STA actually associates.
Station's Radio ID	Radio ID of a STA.

Item	Description
Station's Authentication Method	Authentication mode of a STA.
Station's Cipher Type	Encryption mode of a STA.
Station's User Name	User name of a STA.
Station's Vlan ID	VLAN ID of a STA.
Station's Channel Band-width	Channel bandwidth of a STA.
Station's asso BSSID	BSSID with which a STA is associated.
Station's state	Status of the STA.
Station's QoS Mode	QoS mode of the STA.
Station's HT Mode	HT mode of the STA. ● EHT: 802.11be ● HE: 802.11ax ● VHT: 802.11ac ● HT: 802.11n ● -: 802.11a/b/g
Station's MCS value	The maximum MCS value of the STA.
Station's NSS value	NSS value of the STA. If the STA does not support NSS or the NSS value is 0, a hyphen (-) is displayed.
Station's Short GI	Whether the STA supports the short GI.
Station's roam state	Roaming state of a STA.
HAC CAPWAP IP	CAPWAP IP address for inter-AC communication.
HAP CAPWAP IP	CAPWAP IP address for AP access.
Supported band	Frequency bands supported by the STA.
Supported 2.4G channels Supported 5G channels Supported 6G channels	Channel set supported by a STA. **NOTE** If - is displayed, possible causes include: ● The AP version is too early to report channels supported by STAs. ● The STA cannot report the support channels IE field.
802.11k support	Whether a STA supports 802.11k.
802.11r support	Whether a STA supports 802.11r.

Item	Description
802.11r proprietary support	Whether the STA supports Huawei proprietary 802.11r over-the-DS roaming.
802.11v support	Whether a STA supports 802.11v.
Available for roaming	Whether a STA can trigger the roaming process.
Sticky station or not	Whether a STA is a sticky terminal.
Station device type	Identified STA type.
Aimless roaming support in sticky state	Whether a STA is forced to roam to the target AP.
Station identify info	STA information identified by the device.
Category name	STA category identified by the device.
Vendor name	STA vendor identified by the device.
Model name	STA model identified by the device.
OS	STA operating system identified by the device.
U-APSD list	U-APSD list.
AC-VI	Whether U-APSD takes effect on AC_VI packets.
AC-VO	Whether U-APSD takes effect on AC_VO packets.
AC-BE	Whether U-APSD takes effect on AC_BE packets.
AC-BK	Whether U-APSD takes effect on AC_BK packets.

11.1.86 display station assoc-info ap-offline-record

Function

The **display station assoc-info ap-offline-record** command displays information about STAs that connect to the APs in fault state.

Format

display station assoc-info ap-offline-record { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays information about STAs that connect to all APs in fault state.	-
ap-name *ap-name*	Displays information about STAs that go online on the AP with a specified name in fault state.	The AP name must exist.
ap-id *ap-id*	Displays information about STAs that go online on the AP with a specified ID in fault state.	The AP ID must exist.
radio *radio-id*	Displays information about STAs that connect to a specified radio of an AP in fault state.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When link faults occur between the APs and AC, the APs in fault state allow access of new STAs and log the STA information. When the link between the APs and AC is re-established, the APs disconnect these STAs and send the STA information to the AC. You can run the **display station assoc-info ap-offline-record** command on the AC to check information about the STAs that connect to the APs in fault state.

Prerequisite

The APs in fault state have been enabled to allow access of new STAs using the **keep-service enable allow new-access** command.

Example

Display information about STAs that connect to all APs in fault state.

```
<HUAWEI> display station assoc-info ap-offline-record all
Offline Station information list:
------------------------------------------------------------------------------
STA MAC          AP name   RADIO ID  SSID
------------------------------------------------------------------------------
00e0-fc12-3456   ap1       0         SSID_MYWLAN
------------------------------------------------------------------------------
Total: 1
```

Table 11-49 Description of the **display station assoc-info ap-offline-record** command output

Item	Description
STA MAC	MAC address of a STA.
AP name	Name of the AP that the STA connects to.
RADIO ID	ID of the radio that the STA connects to.
SSID	SSID that the STA connects to.

11.1.87 display station online-fail-record

Function

The **display station online-fail-record** command displays records of STAs' failures to go online.

Format

display station online-fail-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac-address* }

Parameters

Parameter	Description	Value
all	Displays going-online failure records of all STAs.	-
ap-name *ap-name*	Displays records of STAs' failures to go online on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays records of STAs' failures to go online on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Displays online failure records of the STA with the specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a STA fails to go online, you can run the command to check the failure reason, which helps locate the fault.

After the number of records of STAs' failures to go online reaches the maximum that can be stored, new records overwrite existing ones.

Example

Display online failure records of all STAs.

```
<HUAWEI> display station online-fail-record all
Reason distribution
----------------------------------------------------------------------------------------
Reason                                                        Count Percent
----------------------------------------------------------------------------------------
The key is incorrect or the STA uses the cached PMK.                  1     100.00%
----------------------------------------------------------------------------------------
Total Count: 1

Recent records
Rf/WLAN: Radio ID/WLAN ID
------------------------------------------------------------------------------
STA MAC         AP ID Ap name  Rf/WLAN     Last record time            Reason
------------------------------------------------------------------------------
00e0-fc12-3456  0     area_11  0/1       2018-04-11/15:53:18         The key is incorrect or the STA uses the
cached PMK.
------------------------------------------------------------------------------
Total stations: 1 Total records: 1
```

Table 11-50 Description of the **display station online-fail-record** command output

Item	Description
Reason distribution	Distribution of STA going-online failure reasons. All the reasons after the reasons listed in **Table 11-51** are counted as **Other Reasons**. - The authentication request times out.
Count	Number of times that a reason is displayed.
Percent	Percentage of a reason.
Recent records	Recent records of reasons for the STA's failures to go online.
Radio ID/WLAN ID	ID of the radio/VAP to which the STA fails to connect.
STA MAC	MAC address of the STA that fails to go online.

Item	Description
AP ID	ID of the AP on which the STA fails to go online.
Ap name	Name of the AP on which the STA fails to go online.
Last record time	Last time when the STA failed to go online.
Reason	Reason for the STA's failure to go online. For details about STA online failure reasons and handling suggestions, see **Table 11-51**. For reasons of access authentication failures, see **Common Causes for Access Authentication Failures** in *Huawei S Series Campus Switches Troubleshooting Guide*. For troubleshooting methods, see **STAs Fail to Associate with a WLAN** in the *Troubleshooting Guide*.

Table 11-51 STAs' going-online failure reasons and handling suggestions

Reason Why a STA Fails to Go Online	Suggestion
The number of STAs exceeds the physical specifications allowed by the AP.	Expand the network capacity or retain the current configuration as required.
The number of associated STAs exceeds the maximum allowed by the AC.	Expand the WLAN capacity.
The STA associates with a heavily loaded radio.	Check whether the load balancing configuration is proper.
The STA is in the dynamic blacklist.	Check the attack records and check whether the STA has initiated attacks.
The STA's SNR is below the user CAC threshold.	Check whether the SNR-based user CAC threshold is properly set. To modify this threshold, run the **uac client-snr threshold** command and reassociate the STA with the WLAN. Alternatively, determine the STA location and provide coverage to the location.

Reason Why a STA Fails to Go Online	Suggestion
The number of STAs exceeds the maximum allowed by the AP.	Configure load balancing or expand the network capacity.
The number of STAs exceeds the maximum allowed in the VAP reported by the AP.	Increase the maximum number of users on the VAP or expand the WLAN capacity.
The STA does not send an authentication request before associating with the network.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The key is incorrect or the STA uses the cached PMK.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (2/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (4/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (WPA key negotiation failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The authentication request times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
STA authentication times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid association request packet.	Reassociate the STA with the network. If this fault persists, the STA may be incompatible. Contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
The encryption mode is inconsistent on the STA and AP.	Check whether the encryption mode is consistent on the STA and AP.
Authentication fails in the association stage.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA is not authenticated.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AP does not support the rate set specified in the association request packet of the STA.	Modify the basic rate set and supported rate set in the radio profile and reassociate the STA with the network.
The encryption algorithm is inconsistent on the STA and AP.	Check whether the encryption algorithm is consistent on the STA and AP.
Failed to decrypt the challenge packet.	Reassociate the STA with the network or check whether the STA works properly. If this fault persists, contact technical support personnel.
Access from legacy STAs is denied.	Check whether the configuration for denying access of legacy STAs is required. To modify this configuration, run the **undo legacy-station disable** command to permit access of legacy STAs.
The WMM capability of the STA and VAP does not match.	Check whether WMM is forcibly enabled in the radio profile or check the specified configuration of the STA.
STAs have a compatibility issue(Incorrect network type flag carried by STAs) .	Check whether the STA works properly. If so, reassociate the terminal with the network. If this fault persists, contact technical support personnel.
STAs have a compatibility issue(STAs do not support short timeslots).	Check whether the STA supports the 802.11g protocol.
STAs have a compatibility issue(STAs do not support DFS.)	Check whether the STA supports the 802.11h protocol.
The STA is not in the global whitelist.	Check whether the STA needs to be added to the global whitelist.
The STA is in the global blacklist.	Check whether the STA needs to be added to the global blacklist.

Reason Why a STA Fails to Go Online	Suggestion
The STA is not in the VAP's whitelist.	Check whether the STA needs to be added to the VAP's whitelist.
The STA is in the VAP's blacklist.	Check whether the STA needs to be added to the VAP's blacklist.
The association or reassociation packet check fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The number of users exceeds the maximum allowed on the VAP defined by the AC.	Expand the network capacity or run the **max-sta-number** command to increase the maximum number of STAs associated with the VAP.
The Navi AC status is abnormal.	Check the configuration and the network to Navi AC.
VAP configurations on the Local AC and Navi AC are different.	Check the VAP configurations on the Local AC and Navi AC. Check items are as follows: ● STA authentication access mode. ● SSID.
The number of associated STAs exceeds the maximum specifications of the Navi AC.	Expand the WLAN capacity.
Failed to check the configuration during STA association.	Contact technical support personnel.
Batch backup is in progress. STA access is denied.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
STA access failed due to other reasons.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Reassociation denied.	No action is required.
During roaming association, the SSID is inconsistent with that before roaming.	Check whether the SSID is the same before and after roaming. If this fault persists, contact technical support personnel.
During roaming association, the authentication mode is inconsistent with that before roaming.	Check whether the authentication mode is the same before and after roaming. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
During roaming association, the STA status is abnormal.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA fails the roaming check due to other reasons.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA uses a static IP address.	Check whether the static IP address is configured by the user. If so, configure the STA to dynamically obtain an IP address.
The number of STAs exceeds the UAC threshold of the radio.	Check whether the CAC threshold based on the number of users is properly set. To modify this threshold, run the **uac client-number threshold** command and reassociate the STA with the WLAN.
The channel utilization of the radio has reached the upper threshold.	Check whether the user CAC threshold based on the channel utilization is properly set. To modify this threshold, run the **uac channel-utilization threshold** command and reassociate the STA with the WLAN.
Exceeded the maximum number of users on the central AP.	Expand the WLAN capacity.
Authentication fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The encryption mode used by STAs is different from that used by the VAP.	Check the encryption modes used by STAs and the VAP.
The possible cause is that the STA configuration is incorrect, the signal quality on the air interface is low, or the AC forces the STA to reassociate with the network to ensure uninterrupted STA services.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The client capability does not match.	The client capability does not meet the requirements. Upgrade the client version or Wi-Fi version.
Compatibility problems exist on the wireless client. (The HT capability carried by the client is incorrect).	Upgrade the STA version or Wi-Fi module version, or run the **undo legacy-station disable** command to permit access of non-HT STAs.

Reason Why a STA Fails to Go Online	Suggestion
The client access is restricted temporarily.	To allow a wireless client to access a better AP, temporarily restrict the client to access this AP. It is normal if the terminal can connect to a better AP. If a client fails to connect to an AP for multiple consecutive times, check whether APs need to be added.
Received an Authentication frame with authentication transaction sequence number out of expected sequence.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid RSNE capabilities.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Cipher suite rejected because of security policy.	Check whether the encryption mode and key configurations on the wireless terminal are correct. If this fault persists, contact technical support personnel.
Invalid pairwise master key identifier(PMKID).	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid group cipher.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid pairwise cipher.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid MDE.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Invalid FTE.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Others reason.	Contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
802.11r EAPOL Msg 2/4 did not contain R1 name.	Check whether the station has some compatibility problems and please disable dot1x reauthenticate when enable 802.11r. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(2/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(4/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(fail to send the handshake packet).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The MAC address of the access user is different from that configured for the PPSK account.	Run the **display wlan ppsk-user all** command to check whether any PPSK account allows the access from this MAC address. If so, use this PPSK account for access. If not, configure a PPSK account mapping this MAC address and use the new PPSK account for access.
The PPSK account does not exist.	Run the **display wlan ppsk-user all** command to check whether any PPSK account maps the access SSID. If not, create the PPSK account and bind it to the SSID.
The number of PPSK users exceeds the maximum value.	Run the **display wlan ppsk-user all** command to query the maximum number of access users supported by the PPSK account, and then modify the maximum number of access users as required.
The PPSK account expires.	Run the **display wlan ppsk-user all** command to check the timeout period of the PPSK account, and change it to a valid time.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (message 2/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 1/2 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (start unicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (start multicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of WPA data packets).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (invalid length of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 4/4 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 4/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/2 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (message 4/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 4/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/2 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (packet length calculation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet length is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet is too long).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (the key body length of EAP packets is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the EAP packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (incorrect EAP packet descriptor).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid EAP packet type).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (PMK parse failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between the PMK and PMKR1Name).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the type is not FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid FTIE length).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Anonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Snonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (MIC generation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to modify the rsnie field).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to fill FTIE data).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication times out.	Check the network quality or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (re-authentication failure).	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to receive EAP key packets).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication processing error).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Fails to Go Online	Suggestion
Key negotiation fails (access security processing failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication is rejected because an Anti-CloggingToken is required.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication is rejected because the offered finite cyclic group is not supported.	Forget the network and reassociate the STA with the network. If this fault persists, contact technical support personnel.
Robust management frame policy violation	Check whether the encryption mode and pmf configuration are correct on the client.
High-reliability air interface slicing is enabled but is not supported by STA.	Associate the STA with an SSID on which high-reliability air interface slicing is not enabled.

11.1.88 display station offline-record

Function

The **display station offline-record** command displays STAs' going-offline records.

Format

display station offline-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac* }

Parameters

Parameter	Description	Value
all	Displays all STAs' going-offline records.	-
ap-name *ap-name*	Displays STAs' going-offline records on the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays STAs' going-offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Displays the going-offline records of a specified STA.	The STA's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a STA goes offline, you can use this command to check the reason why the STA goes offline.

A maximum of three going-offline records can be stored for each STA.

Example

Display all STAs' going-offline records.

```
<HUAWEI> display station offline-record all
Reason distribution
------------------------------------------------------------------------------------------
Reason                                                          Count Percent
------------------------------------------------------------------------------------------
The STA ages out.                                                   1      14.29%
Other Reasons.                                                      6      85.71%
------------------------------------------------------------------------------------------
Total Count: 7

Recent records
Rf/WLAN: Radio ID/WLAN ID
--------------------------------------------------------------------------------------
STA MAC         AP ID Ap name        Rf/WLAN    Last record time            Reason
--------------------------------------------------------------------------------------
00e0-fc3f-3db9  0         00e0-fc99-9880 1/3        2018-04-18/12:10:26      The STA is deauthenticated.
00e0-fc8e-8fa0  0         00e0-fc99-9880 0/2        2018-04-18/07:17:40      The STA disassociates with the
network.
00e0-fcd2-efc4  0         00e0-fc99-9880 1/3        2018-04-19/02:34:03      The STA disassociates with the
network.
                0         00e0-fc99-9880 1/4        2018-04-18/08:36:35      The STA disassociates with the
network.
                0         00e0-fc99-9880 1/4        2018-04-18/08:35:30      AAA cut command
00e0-fcc9-8a72  0         00e0-fc99-9880 0/2        2018-04-18/06:47:30      The STA disassociates with the
network.
00e0-fcb4-1750  0         00e0-fc99-9880 0/2        2018-04-18/14:06:41      The STA ages out.
---------------------------------------------------------------------------------------
Total stations: 5 Total records: 7
```

Table 11-52 Description of the **display station offline-record** command output

Item	Description
Reason distribution	Distribution of reasons of STAs going offline. All the reasons after the reasons listed in **Table 11-53** are counted as **Other Reasons**. - The STA ages out.
Count	Number of times that a reason is displayed.
Percent	Percentage of a reason.
Recent records	Recent reason records of STAs' going-offline.
STA MAC	MAC address of a STA.
AP ID	ID of the AP from which STAs go offline.
Ap name	Name of the AP from which STAs go offline.
Radio ID/WLAN ID	ID of the radio or WLAN ID of the VAP from which a STA goes offline.
Last record time	Time when the STA went offline last time.
Reason	Reason why the STA went offline. For description of offline reasons and handling suggestions, see **Table 11-53**.For reasons of access authentication failures, see **Common Causes for Access Authentication Failures** in *Huawei S Series Campus Switches Troubleshooting Guide*. For troubleshooting methods, see **A STA Goes Offline Unexpectedly** in the *Troubleshooting Guide*.
Total stations	Total number of STAs.
Total records	Total number of STA offline records.

Table 11-53 Possible reasons and suggestions for STAs to go offline

Reason Why a STA Goes Offline	Suggestion
STA entry addition times out or fails.	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails in the association stage.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The configuration is modified.	Check whether configuration modification records exist.
Roaming check failed(on the eSAP).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Roaming failed(because of a roaming entry failure on the forwarding side or a failure to obtain the configuration).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AP is faulty.	Check the reason why the AP goes offline, and rectify the fault accordingly. For reasons why an AP goes offline, see **display ap offline-record**.
The AP is deleted.	No action is required.
Failed to synchronize user entries between the AP and AC.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to synchronize user entries in a mobility group.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
A tunnel between ACs goes Down.	Check the network between the ACs.
The home AP goes offline or a network fault occurs.	Reassociate the STA with another AP. If this fault persists, contact technical support personnel.
The home AP is deleted.	Reassociate the STA with another AP. If this fault persists, contact technical support personnel.
The home VAP is deleted.	Reassociate the STA with another VAP. If this fault persists, contact technical support personnel.
The AC forcibly disconnects idle STAs.	Check whether this function is required. If so, no action is required. If not, run the **undo idle-cut** command in the service scheme view to modify the configuration.

Reason Why a STA Goes Offline	Suggestion
Roaming check failed because the user left the current AC during inter-AC roaming.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The keepalive packet on the home AP times out.	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
The keepalive packet between ACs times out.	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Layer 3 roaming is disabled.	Reassociate the STA with the network or enable Layer 3 roaming.
The STA MAC is added to the STA blacklist.	Verify that the STA needs to be added to the blacklist.
The STA disassociates with the network.	Check whether the STA actively goes offline or whether the STA is faulty.
The STA is deauthenticated.	Check whether the STA actively goes offline or whether the STA is faulty.
The VAP goes down because the configuration is modified.	Check whether configuration change records exist in the log.
The STA is added to the dynamic blacklist.	Check whether the STA is an attacker.
The signal strength is too low.	Check whether the threshold for quickly disconnecting STAs by smart roaming is correctly configured, and check whether the WLAN coverage area is sufficient.
No control entry exists.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
No Wi-Fi entry exists.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA roams between ACs.	No action is required.

Reason Why a STA Goes Offline	Suggestion
The STA associates or reassociates with the network but does not send a DHCP Discover message. The STA reassociates with the network but does not send a DHCP request message.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA ages out.	No action is required.
A STA goes offline properly.	No action is required.
Failed to synchronize user entries between WMP and eSAP.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA roams out of the device.	No action is required.
A STA goes offline unexpectedly.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
During inter-AC roaming, the SSID is inconsistent with that before roaming.	Check whether the SSID is the same before and after roaming. If this fault persists, contact technical support personnel.
The STA fails the roaming security check.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA fails the roaming status check.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA fails the roaming check due to other reasons.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to add FPI item.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The device in NAT mode does not support roaming.	Reassociate the STA with the network or reconfigure the network mode.
Layer 3 roaming is disabled(delay offline).	Reassociate the STA with the network or enable Layer 3 roaming.
Fail to send IPC to UCM reporting auth request.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Fail to send IPC to UCM reporting roam request.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Station roam between normal and backup AP.	No action is required.

Reason Why a STA Goes Offline	Suggestion
The PPSK configuration is modified.	Check whether the modification record can be found in the log.
Exceeded the maximum number of login STAs supported by the PPSK account.	Check the maximum number of login STAs supported by the PPSK account.
Failed to synchronize user entries between Local AC and Navi AC.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The remotely authenticated STA is disconnected after an active/standby switchover in the Local AC dual-link networking.	No action is required.
VAP configurations on the Navi AC is modified.	No action is required.
Inter-ac roaming is disabled.	No action is required.
Users go offline due to WDS link disconnection or other unknown reasons (reported by Wi-Fi).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The number of users exceeds the specifications (insufficient key slots).	Expand the AP capacity or reassociate the STA with another AP.
A user exception is detected.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA does not respond.	Check whether the STA works properly.
The STA rate is too low.	Check whether the threshold for quickly disconnecting STAs by smart roaming is correctly configured, and check whether the WLAN coverage area is sufficient.
The STA uses a bogus IP address.	Configure the STA to automatically obtain an IP address.
The AP goes online again.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Multicast key handshake failure.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Reporting the PMK negotiation result to the AC times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The STA disassociates with the network (delay offline).	Check whether the STA actively goes offline or whether the STA is faulty.
The STA is deauthenticated (delay offline).	Check whether the STA actively goes offline or whether the STA is faulty.
The STA ages out (delay offline).	No action is required.
The STA IP address changes after roaming.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
AP restores connection from escape mode.	No action is required.
The soft-GRE tunnel goes down.	Check the connectivity to the peer end of the soft-GRE tunnel. If this fault persists, contact technical support personnel.
Higher-priority STAs access the network.	Configure the STA as a high-priority STA, or increase the user CAC threshold or the maximum number of STAs on a VAP.
The number of STAs reached the CAC or VAP threshold.	Increase the user CAC threshold or the maximum number of STAs on a VAP.
The possible cause is that the STA configuration is incorrect, the signal quality on the air interface is low, or the AC forces the STA to reassociate with the network to ensure uninterrupted STA services.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The key is incorrect or the STA uses the cached PMK.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (2/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Failed to receive the handshake packet (4/4) from the STA.	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
802.11r EAPOL Msg 2/4 did not contain R1 name.	Check whether the station has some compatibility problems and please disable dot1x reauthenticate when enable 802.11r. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(2/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(the length of the key data(4/4) is invalid).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails(fail to send the handshake packet).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
The MAC address of the access user is different from that configured for the PPSK account.	Run the **display wlan ppsk-user all** command to check whether any PPSK account allows the access from this MAC address. If so, use this PPSK account for access. If not, configure a PPSK account mapping this MAC address and use the new PPSK account for access.
The PPSK account does not exist.	Run the **display wlan ppsk-user all** command to check whether any PPSK account maps the access SSID. If not, create the PPSK account and bind it to the SSID.
The number of PPSK users exceeds the maximum value.	Run the **display wlan ppsk-user all** command to query the maximum number of access users supported by the PPSK account, and then modify the maximum number of access users as required.
The PPSK account expires.	Run the **display wlan ppsk-user all** command to check the timeout period of the PPSK account, and change it to a valid time.
Key negotiation fails (message 2/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 1/2 processing error).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (start unicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (start multicast negotiation fails because of incorrect input parameters).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 authentication mode or encryption type mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of WPA data packets).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 4/4).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatched packet descriptor of the message 2/2).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (invalid length of the message 4/4 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the message 2/2 packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 4/4 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid key information in the message 2/2 packet).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 handshake status mismatch).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 4/4 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid number of message 2/2 replay times).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 4/4 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (message 2/2 MIC verification failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (packet length calculation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet length is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the EAP packet is too long).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the key body length of EAP packets is 0).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid length of the EAP packet key).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (incorrect EAP packet descriptor).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid EAP packet type).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (PMK parse failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between the PMK and PMKR1Name).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (the type is not FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (invalid FTIE length).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Anonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (mismatch between Snonce and FTIE).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
Key negotiation fails (MIC generation failure).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to modify the rsnie field).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (failure to fill FTIE data).	Check whether the key is correct or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication times out.	Check the network quality or reassociate the STA with the network. If this fault persists, contact technical support personnel.
WAPI authentication fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (re-authentication failure).	Check the intermediate network between the AP and AC or reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Re-authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to fill the start negotiation message).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (start negotiation failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (failure to receive EAP key packets).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication processing error).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Authentication fails (MAC address authentication failure).	Reassociate the STA with the network. If this fault persists, contact technical support personnel.

Reason Why a STA Goes Offline	Suggestion
The authentication request times out.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
Key negotiation fails (WPA key negotiation failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails (access security processing failure).	Verify that the correct password is entered on the STA. If this fault persists, contact technical support personnel.
Key negotiation fails.	Reassociate the STA with the network. If this fault persists, contact technical support personnel.
The AAA deletes the STA.	Check whether the AAA configuration and STA authentication information are both correct. If this fault persists, contact technical support personnel.
High-reliability air interface slicing is enabled or disable.	Associate the STA with an SSID on which high-reliability air interface slicing is not enabled.
Service tunnel VLAN is changed.	No action is required.

11.1.89 display station online-track

Function

The **display station online-track** command displays online time information about a STA.

Format

display station online-track *sta-mac-address*

Parameters

Parameter	Description	Value
sta-mac-address	Displays online time information about the STA with a specified MAC address.	The specified MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view online time information about a STA.

Example

Display online time information about a specified STA.

```
<HUAWEI> display station online-track 00e0-fc08-9abf
----------------------------------------------------------------------------
Event        Event Start(hh:mm:ss)      Event End(hh:mm:ss)      Cost(ms)
----------------------------------------------------------------------------
Association   14:20:28                 14:20:28                10
Auth         14:20:28                 14:20:30                2240
WPA          14:20:30                 14:20:31                330
DHCP         14:20:31                 14:20:31                10
----------------------------------------------------------------------------
Total cost: 2590ms
```

Table 11-54 Description of the **display station online-track** *sta-mac-address* command output

Item	Description
Event	Event type. The values are as follows: - Association: STA association - Auth: STA authentication - WPA: WPA key negotiation - DHCP: STAs obtaining IP addresses through DHCP
Event Start(hh:mm:ss)	Time when the event starts.
Event End(hh:mm:ss)	Time when the event ends.
Cost(ms)	Duration of the event.
Total cost	Total duration of all events.

11.1.90 display station statistics

Function

The **display station statistics** command displays statistics information about STAs.

Format

display station statistics [**sta-mac** *sta-mac-address* | **ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays statistics information about a STA with a specified MAC address.	The STA's MAC address must exist.
ap-name *ap-name*	Displays statistics information about STAs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays statistics information about STAs on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display station statistics** command to view statistics information about STAs.

- If no parameter is specified, statistics information about all STAs associated with the AC is displayed.
- If an AP is specified by **ap-name** or **ap-id**, the number of STAs associated with, disassociated from, and reassociated with the AP is displayed.
- If a STA is specified by **sta-mac**, the number of packets and packet transmission rate between the STA and an AP are displayed.

Prerequisites

- To view statistics information about a STA specified by **sta-mac**, ensure that the STA has been associated with an AP.
- To view statistics information about STAs associated with an AP specified by **ap-name** or **ap-id**, ensure that the AP has been added to the AC and is in normal state.

Example

Display statistics information about all STAs.

```
<HUAWEI> display station statistics
--------------------------------------------------------------------------------
 Successful associations on the AC                              :0
 AC authentication failures due to a password error             :0
 AC authentication failures due to an invalid algorithm         :0
 AC authentication failures due to timeout                      :0
 AC authentication failures due to rejection                    :0
 AC authentication failures due to other reasons                :0
 Sticky STAs detected                                           :0
```

```
Online sticky STAs                                          :0
Sticky STA rate(%)                                          :-
Total number of roamings triggered by sticky STAs                 :0
Number of roamings triggered by sticky STAs                       :0
Sticky STA-triggered roaming success rate(%)                      :-
Unavailable to trigger roam number                              :0
Unavailable to trigger roam rate(%)                             :-
STAs supporting neighbor report                               :0
STAs supporting beacon report                                 :0
    Beacon passive measurement                                 :0
    Beacon active measurement                                  :0
    Beacon table measurement                                   :0
2.4G-only STAs                                              :0
5G-only STAs                                                :0
6G-only STAs                                                :0
2.4G and 5G STAs                                              :0
2.4G, 5G and 6G STAs                                            :0
Online STAs                                                 :0
    STAs associated with 2.4G band                             :0
    STAs associated with 5G band                               :0
    STAs associated with 6G band                               :0
------------------------------------------------------------------------------
```

Table 11-55 Description of the **display station statistics** command output

Item	Description
Successful associations on the AC	Total number of successful link authentications on the AC. Every time a STA initiates a link authentication request and passes the authentication, the counter is incremented by 1. If the same STA initiates multiple authentication requests and passes all authentications, the counter is incremented cumulatively.
AC authentication failures due to a password error	Number of authentication failures due to the incorrect password.
AC authentication failures due to an invalid algorithm	Number of authentication failures due to the invalid authentication algorithm.
AC authentication failures due to timeout	Number of authentication failures due to timeout.
AC authentication failures due to rejection	Number of authentication failures due to rejected access to the AC.
AC authentication failures due to other reasons	Number of authentication failures due to other reasons.
Sticky STAs detected	Number of sticky STAs.
Online sticky STAs	Number of online sticky STAs.
Sticky STA rate(%)	Ratio of the number of sticky STAs to the total number of STAs.

Item	Description
Total number of roamings triggered by sticky STAs	Total number of the triggered smart roaming times.
Number of roamings triggered by sticky STAs	Number of the successfully triggered smart roaming times.
Sticky STA-triggered roaming success rate(%)	Success rate of triggered smart roaming.
Unavailable to trigger roam number	Number of STAs that cannot roam on the AC.
Unavailable to trigger roam rate(%)	Ratio of the number of sticky STAs that cannot roam to the total number of STAs on the AC.
STAs supporting neighbor report	Number of STAs that can obtain information about neighboring APs.
STAs supporting beacon report	Number of STAs that can report information about neighboring APs through the Beacon Report mechanism.
Beacon passive measurement	Number of STAs that can report information about neighboring APs in passive mode.
Beacon active measurement	Number of STAs that can report information about neighboring APs in active mode.
Beacon table measurement	Number of STAs that can report information about neighboring APs in Beacon table mode.
2.4G-only STAs	Number of STAs that support only the 2.4 GHz frequency band.
5G-only STAs	Number of STAs that support only the 5 GHz frequency band.
6G-only STAs	Number of STAs that support only the 6 GHz frequency band.
2.4G and 5G STAs	Number of STAs that support only the 2.4 GHz and 5 GHz frequency bands.
2.4G, 5G and 6G STAs	Number of STAs that support the 2.4 GHz, 5 GHz, and 6 GHz frequency bands.
Online STAs	Number of online STAs.

Item	Description
STAs associated with 2.4G band	Number of STAs associated with the 2.4 GHz radio. The number of STAs of different types is displayed, including 802.11b, 802.11g, 802.11be 20 MHz, 802.11be 40 MHz, 802.11ax 20 MHz, 802.11ax 40 MHz, 802.11n 20 MHz, and 802.11n 40 MHz STAs.
STAs associated with 5G band	Number of STAs associated with the 5 GHz radio. The number of STAs of different types is displayed, including 802.11a, 802.11n 20 MHz, 802.11n 40 MHz, 802.11be 20 MHz, 802.11be 40 MHz, 802.11be 80 MHz, 802.11be 160 MHz, 802.11be 320 MHz, 802.11ax 20 MHz, 802.11ax 40 MHz, 802.11ax 80 MHz, 802.11ax 160 MHz, 802.11ac 20 MHz, 802.11ac 40 MHz, 802.11ac 80 MHz, and 802.11ac 160 MHz STAs.
STAs associated with 6G band	Number of STAs associated with the 6 GHz radio. The number of STAs of different types is displayed, including 802.11be 20 MHz, 802.11be 40 MHz, 802.11be 80 MHz, 802.11be 160 MHz, 802.11be 320 MHz, 802.11ax 20 MHz, 802.11ax 40 MHz, 802.11ax 80 MHz, and 802.11ax 160 MHz STAs.

Display statistics information about the STA with the MAC address 00e0-fc33-4455.

```
<HUAWEI> display station statistics sta-mac 00e0-fc33-4455
------------------------------------------------------------------
 Packets sent to the station                          : 7
 Packets received from the station                    : 40
 Bytes sent to the station                            : 1170
 Bytes received from the station                      : 3911
 Wireless data rate sent to the station(kbps)         : 0
 Wireless data rate received from the station(kbps)   : 0
 Trigger roam total                                   : 0
 Trigger roam failed                                  : 0
 STA power save percent                               : 0%
------------------------------------------------------------------------------
```

Table 11-56 Description of the **display station statistics sta-mac** *sta-mac-address* command output

Item	Description
Packets sent to the station	Number of packets sent to the STA.

Item	Description
Packets received from the station	Number of packets received from the STA.
Bytes sent to the station	Number of bytes sent to the STA.
Bytes received from the station	Number of bytes received from the STA.
Wireless data rate sent to the station(kbps)	Rate at which packets are sent to the STA, in kbit/s.
Wireless data rate received from the station(kbps)	Rate at which packets are received from the STA, in kbit/s.
Trigger roam total	Total number of smart roaming times.
Trigger roam failed	Number of smart roaming failures.
STA power save percent	Percentage of power saved on the STA.

Display STA statistics information of a specified AP.

```
<HUAWEI> display station statistics ap-name N1-1
------------------------------------------------------------------------------
  Total online time of STAs (seconds)                          :0
  STAs associated with the AP                                  :0
  Association requests                                         :0
  Successful association requests                              :0
  Rejected association requests                                :0
  Failed association requests                                  :0
  Repeated association requests                                :0
  Reassociation requests                                       :0
  Successful reassociation requests                            :0
  Rejected reassociation requests                              :0
  Failed reassociation requests                                :0
  Repeated reassociation requests                              :0
  Disassociations initiated by STAs                            :0
  Disassociations due to STA roaming                           :0
  Disassociations STAs go offline unexpectedly                 :0
  Disassociations due to other reasons                         :0
  Disassociations due to a link authentication failure         :0
  Authentication requests                                      :0
  Deauthentication requests                                    :0
  STAs in power saving mode                                    :0
  STAs in HT mode                                              :0
  STAs in B mode                                               :0
  STAs in G mode                                               :0
  STAs in A mode                                               :0
  STAs in N mode                                               :0
  STAs in AC mode                                              :0
  STAs in AX mode                                              :0
  STAs in BE mode                                              :0
  2.4G-only STAs                                               :0
  5G-only STAs                                                 :0
  6G-only STAs                                                 :0
  2.4G and 5G STAs                                             :0
  2.4G, 5G and 6G STAs                                         :0
  2.4G and 5G STAs associated with 5G                          :0
  STAs associated with 2.4G band                               :0
  STAs associated with 5G band                                 :0
  STAs associated with 6G band                                 :0
  Band steer success rate(%)                                   :-
```

```
 Load balancing status between dual bands                     :-
 Sticky STAs detected                                    :0
------------------------------------------------------------------------------
```

Table 11-57 Description of the **display station statistics ap-name** *ap-name* command output

Item	Description
Total online time of STAs (seconds)	Total online duration of all STAs, in seconds.
STAs associated with the AP	Number of STAs currently associated with the AP, not including the number of STAs in aging status.
Association requests	Number of association requests sent to the AP.
Successful association requests	Number of successful associations.
Rejected association requests	Number of association requests rejected by the AP.
Failed association requests	Number of failed associations.
Repeated association requests	Number of times STAs repeatedly send association requests to the AP.
Reassociation requests	Number of reassociation requests sent to the AP.
Successful reassociation requests	Number of successful reassociations.
Rejected reassociation requests	Number of reassociation requests rejected by the AP.
Failed reassociation requests	Number of failed reassociations.
Repeated reassociation requests	Number of times STAs repeatedly send reassociation requests to the AP.
Disassociations initiated by STAs	Number of times STAs are disassociated from the AP because users go offline.
Disassociations due to STA roaming	Number of times STAs are disassociated from the AP because users roam to other regions.
Disassociations because STAs go offline unexpectedly	Number of times STAs are disassociated from the AP because users go offline unexpectedly.
Disassociations due to other reasons	Number of times STAs are disassociated from the AP for other reasons.

Item	Description
Disassociations due to a link authentication failure	Number of times STAs are disassociated from the AP due to link authentication failures.
Authentication requests	Number of times link authentication requests are sent.
Deauthentication requests	Number of times link deauthentication requests are sent.
STAs in power saving mode	Number of STAs working in power saving mode.
STAs in HT mode	Number of STAs working in HT mode.
STAs in B mode	Number of STAs working in 802.11b mode.
STAs in G mode	Number of STAs working in 802.11g mode.
STAs in A mode	Number of STAs working in 802.11a mode.
STAs in N mode	Number of STAs working in 802.11n mode.
STAs in AC mode	Number of STAs working in 802.11ac mode.
STAs in AX mode	Number of STAs working in 802.11ax mode.
STAs in BE mode	Number of STAs working in 802.11be mode.
2.4G-only STAs	Number of STAs that support only the 2.4 GHz frequency band.
5G-only STAs	Number of STAs that support only the 5 GHz frequency band.
6G-only STAs	Number of STAs that support only the 6 GHz frequency band.
2.4G and 5G STAs	Number of STAs that support only the 2.4 GHz and 5 GHz frequency bands.
2.4G, 5G and 6G STAs	Number of STAs that support 2.4 GHz, 5 GHz, and 6 GHz frequency bands.
2.4G and 5G STAs associated with 5G	Number of STAs that support both 2.4 and 5 GHz frequency bands and are associated with the 5 GHz radio.

Item	Description
STAs associated with 2.4G band	Number of STAs associated with the 2.4 GHz radio.
STAs associated with 5G band	Number of STAs associated with the 5 GHz radio.
STAs associated with 6G band	Number of STAs associated with the 6 GHz radio.
Band steer success rate(%)	Band steering success rate.
Load balancing status between dual bands	Status of load balancing between different frequency bands.
Sticky STAs detected	Number of the detected sticky STAs.

11.1.91 display vap

Function

The **display vap** command displays information about service VAPs.

Format

display vap { **ap-group** *ap-group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } [**ssid** *ssid*]

display vap { **all** | **ssid** *ssid* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all service VAPs in a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays information about service VAPs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays information about service VAPs on the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays information about service VAPs on a specified radio.	The value is an integer that ranges from 0 to 2.
ssid *ssid*	Displays information about service VAPs with a specified SSID.	The SSID must exist.
all	Displays information about all service VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about service VAPs.

Example

Display information about all service VAPs.

```
<HUAWEI> display vap all
WID : WLAN ID
---------------------------------------------------------------------------
AP ID AP name        RfID WID  BSSID          Status  Auth type  STA   SSID
---------------------------------------------------------------------------
3     ap1            0    1    00e0-fc12-3456 ON      Open       0     GUEST-WLAN
---------------------------------------------------------------------------
Total: 1
```

Table 11-58 Description of the **display vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
SSID	SSID name.
BSSID	MAC address of a VAP.
Status	Current status of a VAP. ● ON: The VAP service is enabled. ● OFF: The VAP service is disabled. ● -: This is the state of a VAP on the standby AC in a dual-link cold backup scenario.
Auth type	Authentication mode of a VAP.
STA	Number of STAs connected to a VAP.

11.1.92 display vap create-fail-record

Function

The **display vap create-fail-record** command displays records about VAP creation failures.

Format

display vap create-fail-record { **ap-mac** *ap-mac* | **all** }

Parameters

Parameter	Description	Value
ap-mac *ap-mac*	Displays records about VAP creation failures on an AP with the specified MAC address.	The AP's MAC address must exist.
all	Displays records about VAP creation failures on all APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vap create-fail-record** command to check records about VAP creation failures.

Example

Display all records about VAP creation failures.

```
<HUAWEI> display vap create-fail-record all
Rf/WLAN: Radio ID/WLAN ID
-------------------------------------------------------------------------------
AP MAC          Rf/WLAN  Profile Name  Source Type
VAP Type        Reason
-------------------------------------------------------------------------------
00e0-fc76-e360  0/4      1             ap-group
Service         Preshared key is not configured.
00e0-fc76-e370  1/4      1             ap-group
Service         Preshared key is not configured.
00e0-fc76-e360  0/6      1             ap-group
Service         Preshared key is not configured.
00e0-fc76-e370  1/6      1             ap-group
Service         Preshared key is not configured.
-------------------------------------------------------------------------------
Total records: 4
```

Table 11-59 Description of the **display vap create-fail-record all** command output

Item	Description
AP MAC	MAC address of an AP.
Rf/WLAN	Radio ID/WLAN ID.
Profile Name	VAP profile name.
Source Type	Object to which the VAP is bound, including: - ap-group: AP group - ap-id: AP
VAP Type	VAP type, including: - Service: Service VAP - WDS: WDS VAP - Mesh: Mesh VAP
Reason	Reason why the VAP fails to be created. **Table 11-60** describes detailed reasons.

Table 11-60 Reasons for VAP creation failures

Reason for VAP Creation Failures	Remarks	Suggestion
The VAPs using WEP encryption on an AP cannot use the same key ID.	-	Check the configuration of the VAP profile or security profile.
Invalid WEP key index.	-	Check whether the security profile is configured correctly.
Preshared key is not configured.	-	Configure a pre-shared key.
Only one management VAP profile can be bound.	-	Delete the management VAP that has been configured.
The bridge is enabled. Please undo first.	WLAN IDs 13 and 14 are used to set up a WDS bridge. Select other WLAN IDs or delete the WDS configuration.	Select another WLAN ID or delete the WDS configuration.

Reason for VAP Creation Failures	Remarks	Suggestion
WLAN ID(16) is used. Please undo first.	WLAN ID 16 is used to set up a Mesh link. Select another WLAN ID or delete the Mesh configuration.	Select another WLAN ID or delete the Mesh configuration.
Only one temporary management vap-profile can be bound to an AP.	-	Delete the offline management VAP that has been configured.
The current country code does not support 5GHz frequency band.	-	Change the country code, or do not create a 5 GHz VAP.
The current country code does not support 2.4GHz frequency band.	-	Change the country code, or do not create a 2.4 GHz VAP.
The AP type does not support the wlan id.	-	Delete unused VAPs.
This AP type does not support WDS function.	-	Replace the AP with one supporting WDS.
This AP type or version does not support Mesh function.	-	Replace the AP with a Mesh-capable AP or upgrade the AP to a Mesh-capable version.
The number of VAPs has reached the upper limit.	-	Delete excess VAPs.
The AP does not support 5GHz frequency band.	-	Change the AP, or do not create a 5 GHz VAP.
The AP does not support 2.4GHz frequency band.	-	Change the AP, or do not create a 2.4 GHz VAP.
The AP does not support 802.1X+WEP.	-	Replace the AP with one in compliance with 802.11ac Wave 2.
SFN roaming can be configured only on one VAP of each radio.	-	Create a VAP on another radio or delete the SFN roaming VAP on the current radio.
The AP does not support SFN.	-	Replace the AP with one supporting SFN roaming.

Reason for VAP Creation Failures	Remarks	Suggestion
The 5G radio of the AP does not support SFN. The radio frequency band of the AP does not support SFN.	-	Replace the AP or modify the radio configuration.
The number of VAPs has reached the card specific.	-	Reduce the number of VAPs on a card, or enable the AP to go online on another card of the switch and create VAPs.
The AP in this version does not support PPSK authentication.	-	Replace the AP with an AP that supports PPSK authentication or upgrade the AP to a version that supports PPSK authentication.
The AP in this version does not support the WPA3-Enterprise transition mode.	-	Upgrade the AP to V200R023C00 or later.
The AP in this version does not support Navi-AC VAPs.	-	Replace the AP with an AP that supports Navi AC VAPs or upgrade the AP to a version that supports Navi AC VAPs.
Unknown reason, error code is 0x%x.	-	Contact technical support personnel.
The number of WDS VAPs has reached the upper limit.	-	Delete redundant WDS VAPs.
The number of Mesh VAPs has reached the upper limit.	-	Delete redundant Mesh VAPs.
The frequency band of this radio is inconsistent with that supported by the current country code.	-	Change the country code, or do not create a VAP for the current radio.

Reason for VAP Creation Failures	Remarks	Suggestion
The AP in this version does not support the Mesh configuration on radio 2.	-	Replace the AP with an AP on which radio 2 supports Mesh or upgrade the AP to a version that supports Mesh on radio 2 of an AP.
The AP does not support OWE.	-	Replace the AP with an OWE-capable AP or upgrade the AP to an OWE-capable version.
No security policy is configured.	-	Configure a security policy.
No PSK is configured.	-	Configure a WEP key.
The 6GHz frequency band supports only the open, OWE and WPA3 security policies.	-	Modify the security policy configuration of the VAP.
The current country code does not support 6GHz frequency band.	-	Change the country code, or do not create a 6 GHz VAP.
The AP does not support 6GHz frequency band.	-	Change the AP, or do not create a 6 GHz VAP.
The 6G radio of the AP does not support SFN.	-	Replace the AP or modify the 6 GHz radio configuration.
The 6 GHz frequency band does not support WAPI, WPA, WPA2, and WEP.	-	Modify the encryption configuration of the VAP.
The AP in this version does not support RPSK authentication.	-	Replace the AP with an AP that supports RPSK authentication or upgrade the AP to a version that supports RPSK authentication.
The AP in this version does not support 802.1X +WPA3+AES.	-	Upgrade the AP to V200R023C00SPC100 or later.

11.1.93 display vap-profile

Function

The **display vap-profile** command displays configuration and reference information about VAP profiles.

Format

display vap-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all VAP profiles.	-
name *profile-name*	Displays information about a specified VAP profile.	The VAP profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration and reference information about VAP profiles.

Example

Display information about all VAP profiles.

```
<HUAWEI> display vap-profile all
FMode   : Forward mode
STA U/D : Rate limit client up/down
VAP U/D : Rate limit VAP up/down
BR2G/5G/6G : Beacon 2.4G/5G/6G rate
-----------------------------------------------------------------------------------------------------------------------
Name         FMode    Type     VLAN    AuthType  STA U/D(Kbps)  VAP U/D(Kbps)  BR2G/5G/6G(Mbps)
Reference  SSID
-----------------------------------------------------------------------------------------------------------------------
default      direct   service   VLAN 1  Open      -/-          -/-          5.5/6/6         0        GUEST-WLAN
vap-profile1  direct   service   VLAN 1  Open      -/-          -/-          5.5/6/6         0        GUEST-WLAN
-----------------------------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-61 Description of the **display vap-profile all** command output

Item	Description
Name	VAP profile name.
FMode	Service data forwarding mode.
Type	VAP profile type. ● service ● management AP ● service-backup ap-offline ● service-backup auth-server-down ● service-backup distribute
VLAN	Service VLAN ID.
AuthType	User authentication mode.
STA U/D(Kbps)	Uplink/downlink rate limit of a single STA.
VAP U/D(Kbps)	Uplink/downlink rate limit of all STAs on a specified VAP.
BR2G/5G/6G(Mbps)	Rate of Beacon frames on each frequency band.
Reference	Number of times a VAP profile is referenced.
SSID	SSID profile referenced by a VAP profile.

Display information about the VAP profile **default**.

```
<HUAWEI> display vap-profile name default
--------------------------------------------------------------------------------
Profile ID                      : 0
Service mode                      : enable
Type                           : service
Forward mode                       : direct-forward
Offline management                   : disable
Service VLAN ID                    : 1
Service VLAN Pool                   : -
Permit VLAN ID                     : 2 to 4
Auto off service switch             : disable
Auto off starttime                 : -
Auto off endtime                   : -
STA access mode                     : disable
STA blacklist profile             :
STA whitelist profile             :
Band steer                        : enable
Sta network detect                  : enable
Sta network detect(assoc)              : enable
Sta network detect(reassoc)       : enable
Learn client IPv4 address            : enable
Learn client DHCP strict            : disable
Learn client DHCP blacklist           : disable
Learn client IPv6 address            : enable
```

```
Learn client DHCPv6 strict                        : disable
Learn client DHCPv6 blacklist                     : disable
Learn client DHCPv6-SLAAC                         : disable
Learn client DHCPv6-SLAAC blacklist               : disable
IP source check                                   : disable
ARP anti-attack check                             : disable
DHCP option82 insert                              : disable
DHCP option82 remote id format                    : insert AP-MAC
  MAC format                                      : default
DHCP option82 circuit id format                   : insert AP-MAC
  MAC format                                      : default
ND trust port                                     : disable
SFN roam                                          : disable
Anti attack flood
  ARP flood switch                                : enable
  ARP flood STA rate threshold                    : 4
  ARP flood blacklist                             : disable
  ND flood switch                                 : enable
  ND flood STA rate threshold                     : 8
  ND flood blacklist                              : disable
  IGMP flood switch                               : enable
  IGMP flood STA rate threshold                   : 4
  IGMP flood blacklist                            : disable
  DHCP flood switch                               : enable
  DHCP flood STA rate threshold                   : 4
  DHCP flood blacklist                            : disable
  DHCPv6 flood switch                             : enable
  DHCPv6 flood STA rate threshold                 : 4
  DHCPv6 flood blacklist                          : disable
  mDNS flood switch                               : enable
  mDNS flood STA rate threshold                   : 4
  mDNS flood blacklist                            : disable
  Other broadcast flood switch                    : enable
  Other broadcast flood STA rate threshold        : 10
  Other broadcast flood blacklist                 : disable
  Other multicast flood switch                    : enable
  Other multicast flood STA rate threshold        : 10
  Other multicast flood blacklist                 : disable
SSID profile                                      : default
Security profile                                  : default
Traffic profile                                   : default
Authentication profile                            :
SAC profile                                       :
Hotspot2.0 profile                                :
Keep service                                      : disable
Keep service allow new access                     : disable
Keep service allow new access no auth             : disable
Service experience analysis                       : disable
SIP snooping port                                 : 5060
mDNS Snooping switch                              : disable
MU BA Trigger mode                                : MU-BAR
Dynamic flow inspection switch                    : enable
iConnect switch                                   : disable
Split tunnel ACL                                  :
User Flow syslog switch                           : enable
Multi-link operation                              : enable
Service experience analysis application list      :
------------------------------------------------------------------------------
Application ID    Application Name               UCL Group ID   UCL Group Name
------------------------------------------------------------------------------
------------------------------------------------------------------------------
S-IPFPM application list                          :
------------------------------------------------------------------------------
Application ID    Application Name               UCL Group ID   UCL Group Name
------------------------------------------------------------------------------
------------------------------------------------------------------------------
S-IPFPM flow list                                 :
------------------------------------------------------------------------------
Flow ID    Role point    Direction    Bidirecion
```

```
------------------------------------------------------------------------------
------------------------------------------------------------------------------
S-IPFPM clear color-flag ingress             : disable
------------------------------------------------------------------------------
```

Table 11-62 Description of the **display vap-profile name** command output

Item	Description
Profile ID	VAP profile ID.
Service mode	Whether the VAP service is enabled. To configure this parameter, run the **service-mode disable** command.
Type	VAP type. ● service: service type ● ap-management: management AP type ● ap-offline: AP-offline backup service type ● service-backup distribute: distributed-AP backup service type To configure this parameter, run the **type (VAP profile view)** command.
Forward mode	Service data forwarding mode. ● direct-forward: direct forwarding ● tunnel: tunnel forwarding ● Soft-GRE: soft GRE forwarding To configure this parameter, run the **forward-mode** command.
Split tunnel ACL	Split tunneling ACL number. In this manner, packets matching the ACL rules can be forwarded in direct mode when the tunnel forwarding mode is configured. To configure this parameter, run the **split-tunnel** command.
Offline management	Whether the offline management VAP and antenna alignment VAP are enabled. To configure this parameter, run the **temporary-management enable (VAP profile view)** command.
Service VLAN ID	Service VLAN ID. To configure this parameter, run the **service-vlan (VAP profile view)** command.

Item	Description
Service VLAN Pool	VLAN pool to which a service VLAN belongs. To configure this parameter, run the **service-vlan (VAP profile view)** command.
Permit VLAN ID	VLAN from which packets are allowed to pass through when the authorization VLAN verification function is enabled.
Auto off service switch	Whether the scheduled VAP auto-off function is enabled. To configure this parameter, run the **auto-off service** command.
Auto off starttime	Start time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto off endtime	End time for scheduled VAP auto-off. To configure this parameter, run the **auto-off service** command.
Auto off track link	Whether to automatically disable VAPs upon disconnection of the uplink of a cloud AP. After this function is enabled through the iMaster NCE-Campus, the SSID is automatically disabled when the uplink of the cloud AP is disconnected. Only cloud APs support this parameter.
STA access mode	STA access control mode. To configure this parameter, run the **sta-access-mode** command.
STA blacklist profile	STA blacklist profile. To configure this parameter, run the **sta-access-mode** command.
STA whitelist profile	STA whitelist profile. To configure this parameter, run the **sta-access-mode** command.
Keep service	Whether service holding upon CAPWAP link disconnection is enabled. To configure this parameter, run the **keep-service enable (VAP profile view)** command.

Item	Description
Keep service allow new access	Whether new STAs are allowed to go online when APs are offline. To configure this parameter, run the **keep-service enable (VAP profile view)** command.
Keep service allow new access no auth	Whether offline APs allow Portal or MAC address authentication STAs to go online without authentication. To configure this parameter, run the **keep-service enable (VAP profile view)** command.
Band steer	Whether the band steering function is enabled. To configure this parameter, run the **band-steer disable** command.
Sta network detect(reassoc)	Whether network detection upon STA reassociation is enabled. To configure this parameter, run the **sta-network-detect disable** command.
Sta network detect(assoc)	Whether network detection upon STA association is enabled. To configure this parameter, run the **sta-network-detect assoc enable** command.
Learn client IPv4 address	Whether STA IPv4 address learning is enabled. To configure this parameter, run the **learn-client-address disable (VAP profile view)** command.
Learn client DHCP strict	Whether strict STA IP address learning through DHCP is enabled. To configure this parameter, run the **learn-client-address dhcp-strict** command.
Learn client DHCP blacklist	Whether to add STAs with bogus IP addresses to a dynamic blacklist. To configure this parameter, run the **learn-client-address dhcp-strict** command.

Item	Description
Learn client IPv6 address	Whether STA IPv6 address learning is enabled. To configure this parameter, run the **learn-client-address disable (VAP profile view)** command.
Learn client DHCPv6 strict	Whether strict STA IP address learning through DHCPv6 is enabled. To configure this parameter, run the **learn-client-address dhcpv6-strict** command.
Learn client DHCPv6 blacklist	Whether to add STAs with bogus IPv6 addresses to a dynamic blacklist. To configure this parameter, run the **learn-client-address dhcpv6-strict** command.
Learn client DHCPv6 SLAAC	Whether STA IPv6 address learning only through DHCPv6 or SLAAC is enabled. To configure this parameter, run the **learn-client-address dhcpv6-slaac** command.
Learn client DHCPv6 SLAAC blacklist	Whether to add STAs with bogus IPv6 addresses to a dynamic blacklist. To configure this parameter, run the **learn-client-address dhcpv6-slaac** command.
IP source check	Whether IPSG is enabled. To configure this parameter, run the **ip source check user-bind enable** command.
ARP anti-attack check	Whether DAI is enabled. To configure this parameter, run the **arp anti-attack check user-bind enable** command.
DHCP option82 insert	Whether to enable APs to add the Option 82 field to DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 insert enable** command.

Item	Description
DHCP option82 remote id format	Format of the remote-ID in the Option 82 field added to DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
DHCP option82 circuit id format	Format of the circuit-ID in the Option 82 field added to DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
MAC format	Format of the AP MAC address in the Option 82 field. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
DHCP option82 remote id pattern	Field separator of remote-id suboptions for Option 82 in DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 pattern (VAP profile view)** command.
DHCP option82 circuit id pattern	Field separator of circuit-id suboptions for Option 82 in DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 pattern (VAP profile view)** command.
User defined text	User-defined format of Option 82's suboptions in DHCP packets sent by STAs. To configure this parameter, run the **dhcp option82 format (VAP profile view)** command.
ND trust port	Whether the ND trusted interface function is enabled. To configure this parameter, run the **nd trust port** command.
SFN roam	Whether agile distributed SFN roaming is enabled. To configure this parameter, run the **sfn-roam enable** command.

Item	Description
Anti attack flood	Flood detection and prevention.
ARP flood switch	Whether ARP flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
ARP flood STA rate threshold	Rate threshold for ARP flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
ARP flood blacklist	Whether the ARP flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
ND flood switch	Whether ND flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
ND flood STA rate threshold	Rate threshold for ND flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
ND flood blacklist	Whether the ND flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.

Item	Description
IGMP flood switch	Whether IGMP flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
IGMP flood STA rate threshold	Rate threshold for IGMP flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
IGMP flood blacklist	Whether the IGMP flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
DHCP flood switch	Whether DHCP flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
DHCP flood STA rate threshold	Rate threshold for DHCP flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
DHCP flood blacklist	Whether the DHCP flood blacklist function is enabled. To configure this parameter, run the **anti-attack flood blacklist enable** command. ● enable ● disable

Item	Description
DHCPv6 flood switch	Whether DHCPv6 flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
DHCPv6 flood STA rate threshold	Rate threshold for DHCPv6 flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
DHCPv6 flood blacklist	Whether the DHCPv6 flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
mDNS flood switch	Whether mDNS flood detection is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood disable** command.
mDNS flood STA rate threshold	Rate threshold for mDNS flood detection. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
mDNS flood blacklist	Whether the mDNS flood blacklist function is enabled. ● enable ● disable To configure this parameter, run the **anti-attack flood blacklist enable** command.

Item	Description
Other broadcast flood switch	Whether the flood detection function is enabled for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. - enable - disable To configure this parameter, run the **anti-attack flood disable** command.
Other broadcast flood STA rate threshold	Rate threshold for flood detection of broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.
Other broadcast flood blacklist	Whether the flood blacklist function is enabled for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. - enable - disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
Other multicast flood switch	Whether the flood detection function is enabled for multicast packets other than IGMP and mDNS packets. - enable - disable To configure this parameter, run the **anti-attack flood disable** command.
Other multicast flood STA rate threshold	Rate threshold for flood detection of multicast packets other than IGMP and mDNS packets. To configure this parameter, run the **anti-attack flood sta-rate-threshold** command.

Item	Description
Other multicast flood blacklist	Whether the flood blacklist function is enabled for multicast packets other than IGMP and mDNS packets. - enable - disable To configure this parameter, run the **anti-attack flood blacklist enable** command.
SSID profile	Name of the SSID profile referenced by a VAP profile. To configure this parameter, run the **ssid-profile (VAP profile view)** command.
Security profile	Name of the security profile referenced by a VAP profile. To configure this parameter, run the **security-profile (VAP profile view)** command.
Traffic profile	Name of the traffic profile referenced by a VAP profile. To configure this parameter, run the **traffic-profile (VAP profile view)** command.
Authentication profile	Name of the authentication profile referenced by a VAP profile.
SAC profile	Name of the SAC profile referenced by a VAP profile. To configure this parameter, run the **sac-profile (VAP profile view)** command.
Hotspot2.0 profile	Name of the Hotspot2.0 profile referenced by a VAP profile. To configure this parameter, run the **hotspot2-profile (VAP profile view)** command.
SoftGRE profile	Name of the soft GRE profile referenced by a VAP profile. To configure this parameter, run the **forward-mode softgre** *profile-name* command.

Item	Description
Service experience analysis	Whether the SEA function is enabled. To configure this parameter, run the **service-experience-analysis enable** command.
SIP snooping port	SIP listening port number. To configure this parameter, run the **service-experience-analysis sip-snooping port** command.
mDNS Snooping switch	Whether the mDNS snooping function is enabled. To configure this parameter, run the **mdns-snooping enable** command.
MU BA Trigger mode	Mode in which STAs reply with Block Ack frames. To configure this parameter, run the **mu-ba-trigger mode** command.
Dynamic flow inspection switch	Whether the DFI function is enabled. To configure this parameter, run the **dynamic flow inspection enable** command.
iConnect	Whether the iConnect SSID is enabled. To configure this parameter, run the **iconnect enable** command.
User Flow syslog switch	Whether the function of sending network access flow logs of users to a log server is enabled.
Multi-link operation	Whether the MLO function is enabled. To configure this parameter, run the **mlo disable** command.
Service experience analysis application list	List of applications monitored based on SEA on the VAP. ● Application ID ● Application Name To configure this parameter, run the **service-experience-analysis monitor application** command.

Item	Description
S-IPFPM application list	List of applications on the VAP for which iPCA 2.0 measurement is performed. ● Application ID ● Application Name To configure this parameter, run the **s-ipfpm measure application** command.
S-IPFPM flow list	iPCA 2.0 flow measurement configuration on VAPs. ● Flow ID: indicates the ID of a measurement flow. ● Role point: indicates the role of a measurement point. ● Direction: indicates the measurement flow direction. ● Bidirecion: indicates whether a measurement flow is bidirectional. To configure this parameter, run the **s-ipfpm measure flow (VAP profile view)** command.
S-IPFPM clear color-flag ingress	Whether the function of clearing the color bit in the ingress direction on the edge node is enabled. ● enable ● disable To configure this parameter, run the **s-ipfpm clear color-flag ingress** command.

11.1.94 display vap-service-backup auth-server-down

Function

The **display vap-service-backup auth-server-down** command displays the status of an authentication-server-down backup service VAP.

Format

display vap-service-backup auth-server-down [**vap-profile** *profile-name*]

Parameters

Parameter	Description	Value
vap-profile *profile-name*	Specifies the name of a VAP profile.	The VAP profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the status of an authentication-server-down backup service VAP.

Example

Display the status of an authentication-server-down backup service VAP.

```
<HUAWEI> display vap-service-backup auth-server-down
----------------------------------------------------------------------------------------------------
Vap-profile     VapSwitch      Mode      Radius-template      RadiusState
----------------------------------------------------------------------------------------------------
vap-1           ON             Auto      Radius-1             Down
vap-2           ON             Manual    Radius-2             Down
vap-3           OFF            Manual    Radius-3             Up
----------------------------------------------------------------------------------------------------
Total:3
```

Table 11-63 Description of the **display vap-service-backup auth-server-down** command output

Item	Description
Vap-profile	Name of a VAP profile.
VapSwitch	Status of the authentication-server-down backup service VAP.
Mode	Trigger mode of the authentication-server-down backup service VAP.
Radius-template	Name of a RADIUS server template.
RadiusState	Status of the RADIUS server.

11.1.95 display wlan config-errors

Function

The **display wlan config-errors** command displays WLAN configuration errors.

Format

display wlan config-errors

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check WLAN configuration errors.

Example

Display WLAN configuration errors.

```
<HUAWEI> display wlan config-errors
--------------------------------------------------------------------------------
Profile                                   Error
--------------------------------------------------------------------------------
vap-profile 1                                The authentication type specifie
d in the authentication-profile 1 does not match that in the security-profile 1.
--------------------------------------------------------------------------------
Total: 1
```

Table 11-64 Description of the **display wlan config-errors** command output

Item	Description
Profile	Profile name.
Error	Cause of a configuration error.

11.1.96 dot11a basic-rate

Function

The **dot11a basic-rate** command configures a basic rate set of the 802.11a protocol in a 5G radio profile.

The **undo dot11a basic-rate** command restores the default basic rate set of the 802.11a protocol in a 5G radio profile.

By default, a basic rate set of the 802.11a protocol in a 5G radio profile includes rates 6 Mbit/s, 12 Mbit/s, and 24 Mbit/s.

Format

dot11a basic-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a basic-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a basic rate set.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11a mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] dot11a basic-rate 6 9
```

11.1.97 dot11a basic-rate (SSID profile view)

Function

The **dot11a basic-rate** command configures a basic rate set of the 802.11a protocol in an SSID profile.

The **undo dot11a basic-rate** command restores the default basic rate set of the 802.11a protocol in an SSID profile.

By default, no basic rate set of the 802.11a protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11a basic-rate { *dot11a-rate-value* &<1-12> | **all** }

undo dot11a basic-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a basic rate set.	The value is of the enumerated type: ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command in an SSID profile to configure a basic rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11a mode, the STA must support all the rates in the basic rate set.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11a basic-rate 6 9
```

11.1.98 dot11a supported-rate

Function

The **dot11a supported-rate** command configures a supported rate set of the 802.11a protocol in a 5G radio profile.

The **undo dot11a supported-rate** command restores the default supported rate set of the 802.11a protocol in a 5G radio profile.

By default, the supported rate set of the 802.11a protocol in a 5G radio profile includes rates 6 Mbit/s, 9 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, and 54 Mbit/s.

Format

dot11a supported-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a supported-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a supported rate set.	The value is of the enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s
all	Supports all supported rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11a mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] dot11a supported-rate 6 9
```

11.1.99 dot11a supported-rate (SSID profile view)

Function

The **dot11a supported-rate** command configures a supported rate set of the 802.11a protocol in an SSID profile.

The **undo dot11a supported-rate** command restores the default supported rate set of the 802.11a protocol in an SSID profile.

By default, no supported rate set of the 802.11a protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11a supported-rate { *dot11a-rate-value* &<1-12> | **all** }

undo dot11a supported-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies a supported rate set.	The value is of the enumerated type: ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s
all	Supports all supported rates.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command in an SSID profile to configure a supported rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11a mode, the actual data transmission rate between the AP and STA is selected from the basic rate set and the rate set supported by the STA.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11a supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11a supported-rate 6 9
```

11.1.100 dot11bg basic-rate

Function

The **dot11bg basic-rate** command configures a basic rate set of the 802.11b/g protocol in a 2G radio profile.

The **undo dot11bg basic-rate** command restores the default basic rate set of the 802.11b/g protocol in a 2G radio profile.

By default, the basic rate set of the 802.11b/g protocol includes rates 1 Mbit/s and 2 Mbit/s in a 2G radio profile.

Format

dot11bg basic-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg basic-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a basic rate set.	The value is of the enumerated type: - 1: 1 Mbit/s - 2: 2 Mbit/s - 5: 5.5 Mbit/s - 6: 6 Mbit/s - 9: 9 Mbit/s - 11: 11 Mbit/s - 12: 12 Mbit/s - 18: 18 Mbit/s - 24: 24 Mbit/s - 36: 36 Mbit/s - 48: 48 Mbit/s - 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11b/g mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11b/g basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] dot11bg basic-rate 6 9
```

11.1.101 dot11bg basic-rate (SSID profile view)

Function

The **dot11bg basic-rate** command configures a basic rate set of the 802.11b/g protocol in an SSID profile.

The **undo dot11bg basic-rate** command restores the default basic rate set of the 802.11b/g protocol in an SSID profile.

By default, no basic rate set of the 802.11b/g protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11bg basic-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg basic-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a basic rate set.	The value is of the enumerated type: ● 1: 1 Mbit/s ● 2: 2 Mbit/s ● 5: 5.5 Mbit/s ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 11: 11 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s
all	Supports all basic rates.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The basic rate set includes all rates supported by both the AP and STA. A STA can associate with an AP only when the AP and STA support all rates in the basic rate set. For example, if you configure the basic rate set to contain rates 6 Mbit/s and 9 Mbit/s and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command in an SSID profile to configure a basic rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11b/g mode, the STA must support all the rates in the basic rate set.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

When the radio mode is 802.11b, only rates 1, 2, 5, and 11 Mbit/s take effect in the rate set configured in an SSID profile. If no rate in this rate set is configured in the SSID profile, the rate set configured in the radio profile is used.

Example

Configure the 802.11b/g basic rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11bg basic-rate 6 9
```

11.1.102 dot11bg supported-rate

Function

The **dot11bg supported-rate** command configures a supported rate set of the 802.11b/g protocol in a 2G radio profile.

The **undo dot11bg supported-rate** command restores the default supported rate set of the 802.11b/g protocol in a 2G radio profile.

By default, the supported rate set of the 802.11b/g protocol in a 2G radio profile includes rates 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s, 6 Mbit/s, 9 Mbit/s, 11 Mbit/s, 12 Mbit/s, 18 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s, and 54 Mbit/s.

Format

dot11bg supported-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg supported-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a supported rate set.	The value is of the enumerated type: - 1: 1 Mbit/s - 2: 2 Mbit/s - 5: 5.5 Mbit/s - 6: 6 Mbit/s - 9: 9 Mbit/s - 11: 11 Mbit/s - 12: 12 Mbit/s - 18: 18 Mbit/s - 24: 24 Mbit/s - 36: 36 Mbit/s - 48: 48 Mbit/s - 54: 54 Mbit/s
all	Supports all supported rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11b/g mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the 802.11b/g supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] dot11bg supported-rate 6 9
```

11.1.103 dot11bg supported-rate (SSID profile view)

Function

The **dot11bg supported-rate** command configures a supported rate set of the 802.11b/g protocol in an SSID profile.

The **undo dot11bg supported-rate** command restores the default supported rate set of the 802.11b/g protocol in an SSID profile.

By default, no supported rate set of the 802.11b/g protocol is configured in an SSID profile, and the configuration in the radio profile takes effect.

NOTE

Only the AirEngine series APs support this command.

Format

dot11bg supported-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg supported-rate

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies a supported rate set.	The value is of the enumerated type: - 1: 1 Mbit/s - 2: 2 Mbit/s - 5: 5.5 Mbit/s - 6: 6 Mbit/s - 9: 9 Mbit/s - 11: 11 Mbit/s - 12: 12 Mbit/s - 18: 18 Mbit/s - 24: 24 Mbit/s - 36: 36 Mbit/s - 48: 48 Mbit/s - 54: 54 Mbit/s
all	Indicates all supported rate sets.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP in addition to the basic rates. The AP and STA can transmit data at all rates specified in the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command in an SSID profile to configure a supported rate set, bind the SSID profile to a VAP profile. If a STA associates with an AP in 802.11b/g mode, the actual data transmission rate between the AP and STA is selected from the basic rate set and the rate set supported by the STA.

When the rate set configuration exists in both the SSID profile and radio profile, the configuration in the SSID profile takes effect for AirEngine series APs and that in the radio profile takes effect for other AP models.

Precautions

This configuration applies only to STAs associated with an AP in 802.11b/g mode but does not take effect on STAs associated with the AP in other modes.

When the radio mode is 802.11b, only rates 1, 2, 5, and 11 Mbit/s take effect in the rate set configured in an SSID profile. If no rate in this rate set is configured in the SSID profile, the rate set configured in the radio profile is used.

Example

Configure the 802.11b/g supported rate set to contain rates 6 Mbit/s and 9 Mbit/s in the SSID profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] dot11bg supported-rate 6 9
```

11.1.104 dtim-interval

Function

The **dtim-interval** command sets the delivery traffic indication map (DTIM) interval in an SSID profile.

The **undo dtim-interval** command restores the default DTIM interval in an SSID profile.

By default, the DTIM interval is 1.

Format

dtim-interval *dtim-interval*

undo dtim-interval

Parameters

Parameter	Description	Value
dtim-interval	Specifies the DTIM interval.	The value is an integer that ranges from 1 to 255, in Beacons.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

DTIM refers to delivery traffic indication map. After a STA enters the dormancy mode, the associated AP saves the broadcast and multicast frames for the STA. When a Beacon frame sent to the STA by the AP contains DTIM, the saved broadcast and multicast frames will be transmitted to the STA. The DTIM interval refers to the number of Beacon frames sent before the Beacon frame that contains the DTIM. To set the interval for sending Beacon frames in an SSID profile, run the **beacon-interval** command.

- When the STA is in the dormancy status, the AP saves data transmitted to the STA and notifies the STA with a bit in broadcast Beacon frames. The STA receives data according to this bit. You can run this command to set the DTIM interval in the specified SSID profile.
- The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DTIM. A long DTIM interval lengthens the dormancy time of the STA and saves power, but degrades the transmission capability of the STA. A short interval helps transmitting data in a timely manner, but the STA is woken up frequently, causing high power consumption.

Precautions

Changing the DTIM interval will restart the VAP to make the configuration take effect. During the VAP restart, services on the VAP are interrupted and STAs are disconnected.

Example

Set the DTIM interval to 5 in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dtim-interval 5
```

11.1.105 eirp

Function

(AP group radio view) The **eirp** command configures the transmit power for all specified radios in an AP group.

(AP group radio view) The **undo eirp** command restores the default transmit power for all specified radios in an AP group.

(AP radio view) The **eirp** command configures the transmit power for an AP radio.

(AP radio view) The **undo eirp** command cancels the configuration of the transmit power on an AP radio. The transmit power on the AP radio is then determined by that configured in the AP group radio view.

By default, the transmit power of a radio is 127 dBm. The transmit power that takes effect on APs is related to the AP type, country code, channel, and channel bandwidth. The transmit power in effect is the maximum transmit power that the AP radio supports under the current configuration. To check this value, run the **display radio** { **ap-name** *ap-name* | **ap-id** *ap-id* } command.

Format

eirp *eirp*

undo eirp

Parameters

Parameter	Description	Value
eirp	Specifies the transmit power.	The value is an integer that ranges from 1 to 127, in dBm.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Effective isotropic radiated power (EIRP) signifies the strength of signals transmitted from an antenna, that is, the transmit power of a radio plus the antenna gain. The transmit power of a radio configured using the **eirp** command is the EIRP plus the antenna gain on the radio.

You can configure the transmit power for a radio based on actual network environments, enabling radios to provide the required signal strength and improving signal quality on WLANs.

Precautions

The value of *antenna-gain* in the **antenna-gain** *antenna-gain* command must be consistent with the gain of the antenna connected to an AP.

If automatic transmit power selection is enabled by running the **calibrate auto-txpower-select enable** command, the transmit power configured by running the

eirp command does not take effect. The automatically selected transmit power is used.

If automatic transmit power selection is disabled by running the **calibrate auto-txpower-select disable** command, the transmit power configured by running the **eirp** command takes effect as follows:

The actual transmit power of an AP radio is determined by the configured transmit power of the radio, requirements of local laws and regulations, as well as the transmit power range supported by the AP. The actual transmit power of a radio cannot exceed the maximum transmit power required by local laws and regulations.

- If the configured transmit power of a radio is in compliance with local laws and regulations and within the transmit power range supported by the AP, the configured transmit power is the actual transmit power of the radio.
- If the configured transmit power of a radio is smaller than the minimum transmit power supported by the AP, the smaller one between the minimum transmit power supported by the AP and maximum transmit power required by local laws and regulations is the actual transmit power of the radio.
- If the configured transmit power of a radio is larger than the maximum transmit power supported by the AP, the smaller one between the maximum transmit power supported by the AP and maximum transmit power required by local laws and regulations is the actual transmit power of the radio.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the transmit power of radio 0 on AP 1 to 30 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] eirp 30
Info: The EIRP value takes effect only when automatic transmit power selection i
s disabled, and the value depends on the AP specifications and local laws and re
gulations.
```

11.1.106 er-su disable

Function

The **er-su disable** command disables the Extended Range Single User (ER-SU) function.

The **undo er-su disable** command enables the ER-SU function.

By default, the ER-SU function is enabled.

NOTE

This command is not supported by the following models.

- AirEngine x760 series APs.

Format

er-su disable

undo er-su disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

The ER-SU function improves the signal quality at the cell edge and further improves the long-distance coverage capability.

Example

Disable the ER-SU function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan view] ssid-prof name test
[HUAWEI-wlan-ssid-prof-test] er-su disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.107 forward-mode

Function

The **forward-mode** command sets the data forwarding mode in a VAP profile.

The **undo forward-mode** command restores the default data forwarding mode in a VAP profile.

By default, the direct forwarding mode is used in a VAP profile.

Format

forward-mode { **direct-forward** | **tunnel** | **softgre** *profile-name* }

undo forward-mode

Parameters

Parameter	Description	Value
direct-forward	Indicates the direct forwarding mode.	-
tunnel	Indicates the tunnel forwarding mode.	-
softgre *profile-name*	Indicates the soft GRE forwarding mode and specifies the name of the soft GRE profile bound to a VAP profile.	The specified soft GRE profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the forwarding mode in a VAP profile. The forwarding modes of each VAP profile can be different.

A soft GRE profile can be bound to a VAP profile only after the destination IP address of the soft GRE tunnel is configured in the soft GRE profile.

Example

Create the VAP profile **vap1** and set the forwarding mode to direct forwarding in the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] forward-mode direct-forward
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.108 fragmentation-threshold

Function

The **fragmentation-threshold** command sets the fragmentation threshold in a radio profile.

The **undo fragmentation-threshold** command restores the default fragmentation threshold in a radio profile.

By default, the packet fragmentation threshold is 2346 bytes.

Format

fragmentation-threshold *fragmentation-threshold*

undo fragmentation-threshold

Parameters

Parameter	Description	Value
fragmentation-threshold	Specifies the fragment threshold. If the length of a frame to be sent by the MAC layer exceeds this threshold, the frame is fragmented before being sent.	The value is an integer that ranges from 256 to 2346, in bytes. It must be an integral multiple of 2.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A proper packet fragmentation threshold can improve channel bandwidth usage. Set the fragmentation threshold as required. A large threshold is recommended.

Precautions

When the packet fragmentation threshold is too small, packets are fragmented into smaller frames. These frames are transmitted at a high extra cost, resulting in low channel efficiency.

When the packet fragmentation threshold is too large, long packets are usually not fragmented, which increases the transmission time and error probability. If an error occurs, packets are retransmitted, resulting in a waste of channel bandwidth.

Example

Set the fragmentation threshold to 1500 bytes in the 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] fragmentation-threshold 1500
```

11.1.109 frequency

Function

(AP group radio view) The **frequency** command sets the working frequency band of radios for all APs in an AP group.

(AP group radio view) The **undo frequency** command restores the default working frequency band of radios for all APs in an AP group.

(AP radio view) The **frequency** command sets the working frequency band of radios for an AP.

(AP radio view) The **undo frequency** command restores the default working frequency band of the radio on an AP to that configured in the AP group radio view.

By default, radio 0 and radio 2 in the AP group radio view work on the 2.4 GHz and 6 GHz frequency bands, respectively. If radio 2 does not support the 6 GHz frequency band, it works on the frequency band by default. There is no default value in the AP radio view, and the configuration in the AP group radio view is used.

Format

frequency { **2.4g** | **5g** | **6g** }

undo frequency

Parameters

Parameter	Description	Value
2.4g	Specifies 2.4 GHz frequency band.	-
5g	Specifies 5 GHz frequency band.	-
6g	Specifies the 6 GHz frequency band.	-

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radios of some AP models support frequency band switching but can work on only one frequency band at a time. You can configure the working frequency band of AP radios based on the frequency bands supported by STAs.

Precautions

When working in dual-5G mode, some APs support only low-band channels (36 to 64) or high-band channels (100 to 165) on the 5 GHz band.

- AirEngine 5760-51: Radio 1 on high bands and radio 2 on low bands
- AirEngine 6760-X1: Radio 1 on high bands and radio 2 on low bands
- AirEngine 6760-X1E: Radio 1 on high bands and radio 2 on low bands
- AirEngine 8760R-X1E: Radio 1 and radio 2 on all bands
- AirEngine 8760-X1-PRO: Radio 1 on high bands and radio 2 on low bands
- AirEngine 6761-21T: Radio 1 on high bands and radio 2 on low band
- AirEngine 6761S-21T: Radio 1 on high bands and radio 2 on low band
- AirEngine 5761R-11E: Radio 0 and radio 1 on all bands
- AirEngine 8771-X1T: Radio 1 on low bands and radio 2 on high band

Changing the working frequency band of radio 0 and radio 2 will delete the channel, power, and antenna gain configurations on radio 0 and radio 2. If an AP uses an external antenna, run the **antenna-gain** *antenna-gain* command to reconfigure the antenna gain to be consistent with the gain of the external antenna connected to the AP.

If the working frequency band of the AP radio set using the preceding commands is the same as that of the AP's actual working frequency band, the AP will not restart. Otherwise, the AP restarts after the preceding commands are run.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

If two radios of an AP work on the 5 GHz frequency band, the operating channels of the two 5 GHz radios must be separated by at least one channel to avoid interference. If two radios of an AP work on the 5 GHz and 6 GHz frequency bands, respectively, pay attention to channel planning as follows:

- For the model AirEngine 6761-22T: Do not use a 5 GHz high-frequency channel (149–165) and a 6 GHz low-frequency channel (80 MHz channels 1–13, 160 MHz channels 1–29) at the same time.
- For the model AirEngine 8771-X1T: Do not use a 5 GHz high-frequency channel (20 MHz channels 153–165, 40 MHz channels 132–161, 80 MHz channels 132–161, 160 MHz channels 100–128, 320 MHz channels 100–144) and a 6 GHz channel (160 MHz channels 1–29, 320 MHz channels 1–61) at the same time.

For example, a country supports 40 MHz+ 5G channels 36, 44, 52, and 60. When deploying 5 GHz radio channels, if one radio is deployed to work on channel 36, it is recommended that channel 52 or 60 be configured for the other radio. Channel 44 is not recommended in this case.

Example

Set the working frequency band of radio 0 of AP to the 5 GHz band.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0] frequency 5g
Warning: Modifying the frequency band will delete the channel, power, and antenn
a gain configurations of the current radio on the AP and reboot the AP. Continue
?[Y/N]:Y
```

11.1.110 guard-interval-mode

Function

The **guard-interval-mode** command configures the guard interval (GI) mode.

The **undo guard-interval-mode** command restores the default GI mode.

By default, the GI mode in 802.11n/ac is **short**, and the GI mode in 802.11ax/be is 0.8 us.

Format

guard-interval-mode { **short** | **normal** }

undo guard-interval-mode

guard-interval-mode dot11ax { **dot8** | **1dot6** | **3dot2** }

undo guard-interval-mode dot11ax

Parameters

Parameter	Description	Value
short	Sets the GI mode in 802.11n/ac to short GI.	-
normal	Sets the GI mode in 802.11n/ac to normal GI.	-
dot11ax { **dot8** | **1dot6** | **3dot2** }	Specifies the GI mode in 802.11ax/be.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

During data transmission, the receive and transmit ends do not receive and send data at all times. When data is received and transmitted or multiple transmissions occur, multi-path interference is generated in radio signal propagation. An interval between transmissions can reduce the impact of interference. This interval is called guard interval (GI).

A smaller GI indicates higher transmission efficiency. A larger GI indicates a higher anti-interference capability. A small GI is recommended for indoor areas with low interference, and a large GI is recommended for outdoor areas with high interference.

- In 802.11a/b/g, the GI is fixed at 800 ns.
- In 802.11n and 802.11ac, the GI can be set to 400 ns (short) or 800 ns (normal).
- In 802.11ax and 802.11be, the GI can be set to 0.8 us (800 ns), 1.6 us, or 3.2 us.

Example

Set the GI mode to short.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] guard-interval-mode short
```

11.1.111 he mcs-map (SSID Profile)

Function

The **he mcs-map** command configures the number of 802.11ax spatial streams and the Modulation and Coding Scheme (MCS) of the spatial streams in an SSID profile.

The **undo he mcs-map** command restores the default number of 802.11ax spatial streams and the default MCS of the spatial streams in an SSID profile.

By default, the number of spatial streams sent and received in 802.11ax is 8, and the MCS of the spatial streams is 11 in an SSID profile.

Format

he { **tx** | **rx** } **mcs-map nss** *nss-value* **map** *mcs-value*

undo he { **tx** | **rx** } **mcs-map**

Parameters

Parameter	Description	Value
tx	Indicates the sent data.	-
rx	Indicates the received data.	-
nss *nss-value*	Specifies the number of spatial streams.	The value is an integer that ranges from 1 to 8.

Parameter	Description	Value
map *mcs-value*	Specifies the MCS of the spatial streams.	The value can be 7, 9, or 11.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rate of an 802.11ax-capable AP depends on the index value of the MCS. A larger MCS indicates a higher transmission rate.

- When the value of *nss-value* is greater than or equal to the number of spatial streams actually supported by an AP, the MCS value corresponding to all the spatial streams of the AP is the value of *mcs-value*.
- When the value of *nss-value* is smaller than the number of spatial streams actually supported by an AP, only the MCS value corresponding to the spatial streams on the AP is the value of *mcs-value*, and the maximum MCS value corresponding to other spatial streams does not take effect.

  For example, if the value of *nss-value* is 2, and the AP supports three spatial streams, only the MCS value corresponding to spatial streams 1 and 2 is the value of *mcs-value*, and the MCS value corresponding to spatial stream 3 does not take effect.

Precautions

This configuration takes effect only when the AP communicates with STAs through 802.11ax.

Example

Set the MCS value corresponding to spatial stream 4 to 9 when data is received in an SSID profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] he rx mcs-map nss 4 map 9
```

11.1.112 a-mpdu disable

Function

The **a-mpdu disable** command disables the aggregate MAC protocol data unit (A-MPDU) function.

The **undo a-mpdu disable** command enables the A-MPDU function.

By default, the A-MPDU function is enabled.

Format

a-mpdu disable

undo a-mpdu disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11n uses A-MPDU technology that aggregates two or more MPDUs into one frame for transmission.

The 802.11ac and later protocols require that the A-MPDU mode be enabled. Therefore, this command takes effect only for 802.11n APs.

Example

Disable the A-MPDU function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] a-mpdu disable
```

11.1.113 ht a-mpdu max-length-exponent

Function

The **ht a-mpdu max-length-exponent** command sets the maximum length of an aggregated MPDU (A-MPDU) on the 802.11n radio. MPDU stands for MAC protocol data unit.

The **undo ht a-mpdu max-length-exponent** command restores the maximum length of an A-MPDU on the 802.11n radio to the default value.

By default, the index for the maximum length of an A-MPDU is 3. The maximum length of the A-MPDU is 65535 bytes.

The function is not supported by the following models.

- AirEngine series APs

Format

ht a-mpdu max-length-exponent *max-length-exponent-index*

undo ht a-mpdu max-length-exponent

Parameters

Parameter	Description	Value
max-length-exponent-index	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 3. ● 0: indicates that the maximum length of the A-MPDU is 8191 bytes. ● 1: indicates that the maximum length of the A-MPDU is 16383 bytes. ● 2: indicates that the maximum length of the A-MPDU is 32767 bytes. ● 3: indicates that the maximum length of the A-MPDU is 65535 bytes.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the index of the maximum length of the A-MPDU to 2 in the 2G radio profile **default**. The index 2 corresponds to a maximum length of 32767 bytes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] ht a-mpdu max-length-exponent 2
```

11.1.114 keepalive (soft GRE profile view)

Function

The **keepalive** command enables Keepalive detection for a soft GRE tunnel and sets Keepalive parameters.

The **undo keepalive** command disables Keepalive detection for a soft GRE tunnel and restores the default Keepalive parameters.

By default, Keepalive detection is disabled for a soft GRE tunnel, the interval for sending Keepalive packets is 5 seconds, and the maximum number of retransmission attempts is 3.

Format

keepalive [**period** *period* [**retry-times** *retry-times*]]

undo keepalive

Parameters

Parameter	Description	Value
period *period*	Specifies the interval for sending Keepalive packets.	The value is an integer that ranges from 1 to 32767, in seconds.
retry-times *retry-times*	Specifies the maximum number of Keepalive packet retransmission times.	The value is an integer that ranges from 1 to 255.

Views

Soft GRE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a network fault occurs and the remote end of a soft GRE tunnel becomes unreachable, an AP cannot detect the network fault and therefore will continue to send packets to the remote end. These packets waste device resources and bandwidth of the intermediate network. After Keepalive detection for a soft GRE tunnel is enabled, the AP can detect the soft GRE tunnel status. When detecting that the peer end of the soft GRE tunnel is unreachable, the AP stops sending packets to the peer end. Otherwise, the AP continues sending packets to the peer end. This mechanism reserves device resources and bandwidth.

After the Keepalive detection function for the soft GRE tunnel is enabled, the local AP periodically sends Keepalive packets to the peer end at specified intervals to check connectivity of the soft GRE tunnel. The value of the unreachable counter is incremented by 1 each time a Keepalive packet is sent but no response is received within the detection period. If a response is received before the value of **retry-times** is reached, the counter is reset. If the AP does not receive any response from the peer end when the counter value reaches the preset value (**retry-times**), it considers the peer unreachable and terminates the tunnel. If the AP receives a response, it considers the peer reachable and continues sending packets to the peer end.

Precautions

If only the **keepalive** command is executed and the parameter **period** *period* [**retry-times** *retry-times*] is not specified, the Keepalive detection function is enabled and the default value of **period** *period* [**retry-times** *retry-times*] parameter is used.

If you run the **keepalive** command several times, the latest configuration overrides the previous configurations.

The Keepalive detection function for a soft GRE tunnel takes effect unidirectionally. If the Keepalive detection function is required on both ends of a soft GRE tunnel, enable this function on each end of the tunnel. The Keepalive detection function takes effect on one end even if the function is disabled on the other end. However, you are advised to enable the Keepalive detection function on both ends of a tunnel.

Example

Enable the Keepalive detection function for a soft GRE tunnel using default parameters.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1] keepalive
```

11.1.115 keep-service enable (VAP profile view)

Function

The **keep-service enable** command enables service holding upon CAPWAP link disconnection.

The **undo keep-service enable** command disables service holding upon CAPWAP link disconnection.

By default, service holding upon CAPWAP link disconnection is disabled.

Format

keep-service enable [**allow new-access** [**no-auth**]]

undo keep-service enable

Parameters

Parameter	Description	Value
allow new-access	Enables offline APs to allow access of new STAs.	-
no-auth	Allows STAs using Portal or MAC address authentication to go online without authentication.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In direct forwarding mode, you can enable service holding upon CAPWAP link disconnection. In this way, when the CAPWAP link between an AP and AC is disconnected, the AP can continue to provide WLAN services, preventing service interruption and improving forwarding reliability.

Service holding upon CAPWAP link disconnection controls whether new STAs are allowed to go online. For high-security authentication modes such as MAC address authentication and Portal authentication, **no-auth** must be configured to enable STAs to go online without authentication upon CAPWAP link disconnection. Therefore, this function can be enabled in scenarios with low security requirements.

Precautions

- Service holding upon CAPWAP link disconnection can be configured in the VAP profile view and AP system profile view. The configuration in the VAP profile view takes precedence over that in the AP system profile view.
- Service holding upon CAPWAP link disconnection is applicable only to scenarios where direct forwarding is used for data services.
- The function of enabling offline APs to allow access of STAs is applicable to scenarios where service data is forwarded in direct mode and the STA authentication mode is Portal, MAC address, WEP, WPA/WPA2-PSK, or open system.

- Service holding upon CAPWAP link disconnection cannot be configured together with the AP-offline backup service VAP (configured using the **type service-backup ap-offline** command) or containment function. Service holding upon CAPWAP link disconnection does not take effect when the containment function is also configured.
- Service holding upon CAPWAP link disconnection is unavailable on a WDS network.
- After service holding upon CAPWAP link disconnection is enabled, the **display access-user** command cannot display information about NAC STAs that are online before the CAPWAP link is disconnected. To display information about such STAs, run the **display station** command.

Example

Enable service holding upon CAPWAP link disconnection in the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] keep-service enable
```

11.1.116 legacy-station disable

Function

The **legacy-station disable** command denies access of non-HT STAs.

The **undo legacy-station disable** command permits access of non-HT STAs.

By default, access of non-HT STAs is permitted.

Format

legacy-station [**only-dot11b**] **disable**

undo legacy-station disable

Parameters

Parameter	Description	Value
only-dot11b	Denies access of non-HT STAs that support only 802.11b.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Non-HT STAs support only 802.11a/b/g and provide a data transmission rate far smaller than the rate of STAs in compliance with 802.11n or later standards. If the non-HT STAs access the WLAN, the data transmission rate of STAs in compliance with 802.11n or later standards will be reduced. To prevent the transmission rate of these STAs from being affected, you can run the **legacy-station** [**only-dot11b**] **disable** command to deny access of all or only 802.11b-compliant non-HT STAs.

Configuration Impact

After the **legacy-station disable** command is run, non-HT STAs supporting only 802.11a/b/g cannot access the wireless network.

After the **legacy-station only-dot11b disable** command is run, non-HT STAs supporting only 802.11b cannot access the wireless network.

After access of non-HT STAs is denied, services may be interrupted.

Precautions

After the **legacy-station disable** command is run, the access of non-HT STAs supporting only 802.11a/b/g fails to be denied if any of the following functions is configured on the non-HT STAs:

- WMM function in a 2G or 5G radio profile disabled using the **wmm disable** command
- Pre-shared key authentication and TKIP encryption for WPA/WPA2 configured using the **security** { **wpa** | **wpa2** | **wpa-wpa2** } **psk** { **pass-phrase** | **hex** } *key-value* **tkip** command when the security profile is used
- 802.1X authentication and TKIP encryption for WPA/WPA2 configured using the **security** { **wpa** | **wpa2** | **wpa-wpa2** } **dot1x tkip** command when the security profile is used
- WEP authentication configured using the **security wep** [**share-key** | **dynamic**] command when the security profile is used
- 802.11b/g radio type in the 2G radio profile configured using the **radio-type** { **dot11b** | **dot11g** } command
- 802.11a radio type in the 5G radio profile configured using **radio-type dot11a** command

After the **legacy-station only-dot11b disable** command is run, the access of non-HT STAs supporting only 802.11b is denied. If 802.11b radio type in the 2G radio profile has been configured using the **radio-type dot11b** command, the access of non-HT STAs supporting only 802.11b fails to be denied.

Example

Deny access of non-HT STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] legacy-station disable
Warning:  If the wmm disable command, TKIP, WEP, or radio type of 802.11a/b/g is configured, the function
of denying access of legac
y STAs cannot take effect.
```

11.1.117 max-sta-number (SSID profile view)

Function

The **max-sta-number** command sets the maximum number of STAs that can be associated with a single VAP.

The **undo max-sta-number** command restores the default maximum number of STAs that can be associated with a single VAP.

By default, a VAP allows for association of a maximum of 64 STAs.

Format

max-sta-number *max-sta-number*

undo max-sta-number

Parameters

Parameter	Description	Value
max-sta-number	Specifies the maximum number of STAs that can be associated with a single VAP.	The value is an integer that ranges from 1 to 512.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

More access users on a VAP indicate fewer network resources that each user can occupy. To ensure Internet experience of users, you can run this command to properly set the maximum number of STAs that can be associated with a single VAP.

Configuration Impact

After this command is executed, online STAs are disconnected. When STAs reassociate with the VAP and the number of associated STAs on the VAP reaches the maximum, new STAs fail to associate with this VAP.

The **max-sta-number** *max-sta-number* command sets the maximum number of STAs that can be associated with a single VAP.

Precautions

The setting configured by this command refers to the maximum number of STAs that can be associated with a VAP of a single AP.

Example

Set the maximum number of STAs that can be associated with a single VAP to 50.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] max-sta-number 50
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.118 mlo enable

Function

The **mlo enable** command enables the multi-link operation (MLO) function.

The **mlo disable** command disables the MLO function.

The **undo mlo** command restores the default status of the MLO function.

By default, the MLO function is disabled.

Format

mlo { **enable** | **disable** }

undo mlo

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA communicates with an AP, the STA selects only one radio to set up a connection, for example, on the 2.4 GHz or 5 GHz frequency band. The maximum air interface rate of the STA is the maximum capability supported by the current radio. To further improve the air interface rate and reduce latency, 802.11be introduces the MLO function that allows for link setup on multiple radios for communication. To improve the air interface rate, transmit different data on different radios at the same time. Radios can back up each other so when the channel is busy on a radio, data is quickly switched to another radio for transmission, reducing air interface latency.

Precautions

After the MLO function is enabled, some incompatible STAs may fail to detect Wi-Fi signals or fail to associate with the WLAN. Such issues can be resolved after you disable the MLO function.

Currently, an AP supports a maximum of two concurrent radios, for example, 2.4 GHz + 5 GHz radios or 5 GHz + 6 GHz radios.

Both the AP and the STA need to support the MLO function. If both the AP and STA support the MLO function on the 2.4 GHz, 5 GHz, and 6 GHz frequency bands, the high-speed 5 GHz + 6 GHz radios are used to set up a link between the AP and STA. If the STA supports the MLO function only on the 2.4 GHz and 5 GHz frequency bands, the link can be set up only using 2.4 GHz + 5 GHz radios.

After the MLO function is enabled, if the configuration of one radio is modified and the modification affects MLO link renegotiation, VAP services on the two radios are interrupted, causing STAs to go offline and online again. Services of other VAPs on the radios are not affected. The configurations that affect MLO link renegotiation include: whether MLO is enabled, radio type, whether the radio is enabled, binding relationship between the VAP profile and radio, security policy, and SSID name.

After an MLO link is set up, information about the STA connected to the device can be viewed only on one radio. However, traffic statistics about the STA are still collected on the two radios. To view information about the access radio of the STA, log in to the AP associated with the STA and run the **display umac station mac** *mac-address* command in the diagnostic view to display MLO link setup information about the STA.

The MLO function takes effect only when the following conditions are met:

- A VAP profile is bound to multiple radios of an AP, and the WLAN IDs of the radios are the same.
- The radios work in 802.11be mode.
- The security policy is open (only 2.4 GHz + 5 GHz radios supported), WPA2 (only 2.4 GHz + 5 GHz radios supported), WPA3, WPA2-WPA3 (only 2.4 GHz + 5 GHz radios supported), or OWE.

The MLO and 802.11r fast roaming functions are mutually exclusive. After the 802.11r fast roaming function is enabled, the MLO function does not take effect.

Example

Enable the MLO function in the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] mlo enable
Warning: After the MLO function is enabled, some incompatible STAs may fail to detect Wi-Fi signals and
cannot associate with the WLAN. This issue can be resolved after you disable the MLO function.
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.119 mu-ba-trigger mode

Function

The **mu-ba-trigger mode** command sets the mode in which STAs reply with Block Ack frames.

The **undo mu-ba-trigger mode** command restores the default mode in which STAs reply with Block Ack frames.

By default, STAs reply with Block Ack frames in MU-BAR mode.

This command is supported on the following APs.

- AirEngine x761
- AirEngine x762
- AirEngine x771

Format

mu-ba-trigger mode { **basic-trigger** | **mu-bar** }

undo mu-ba-trigger mode

Parameters

Parameter	Description	Value
basic-trigger	A-MPDU with basic trigger	-
mu-bar	A-MPDU with MU-BAR	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

The **mu-ba-trigger mode** command sets the mode in which STAs reply with Block Ack frames.

Example

Set the mode in which STAs reply with Block Ack frames to basic-trigger.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] mu-ba-trigger mode basic-trigger
```

11.1.120 mu-mimo disable

Function

The **mu-mimo disable** command disables the downlink MU-MIMO scheduling function.

The **undo mu-mimo disable** command enables the downlink MU-MIMO scheduling function.

By default, the downlink MU-MIMO scheduling function is enabled.

Format

mu-mimo disable

undo mu-mimo disable

Parameters

None

Views

SSID profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Carrier sense multiple access with collision avoidance (CSMA-CA) allows an air interface channel to be occupied only by one STA, and other STAs cannot communicate with the AP. After downlink MU-MIMO scheduling is enabled, STAs supporting MU-MIMO can form an MU group to simultaneously receive downlink data from the same air interface channel, improving channel efficiency and overall downlink throughput.

Prerequisites

Before enabling downlink MU-MIMO scheduling, run the **undo beamforming disable** command to enable beamforming.

Precautions

- In WDS scenarios, ensure that the number of spatial streams on STA VAPs is smaller than that on AP VAPs. Otherwise, MU-MIMO cannot take effect. For example, if STA VAPs and AP VAPs are both configured with three spatial streams, an AP VAP can communicate with only one STA VAP even if MU-MIMO has been enabled.
- downlink MU-MIMO scheduling is not supported in the Mesh networking.

In VR scenarios, disabling downlink MU-MIMO scheduling is recommended.

Example

Enable in the SSID profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo mu-mimo disable
```

11.1.121 mu-mimo optimize enable

Function

The **mu-mimo optimize enable** command enables the MU-MIMO optimization function.

The **undo mu-mimo optimize enable** command disables the MU-MIMO optimization function.

By default, the MU-MIMO optimization function is disabled.

Format

mu-mimo optimize enable

undo mu-mimo optimize enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an environment with less interference, you can run the **mu-mimo optimize enable** command to enable the MU-MIMO optimization function to meet requirements for high downlink throughput of the AP. The expected effect may fail to be achieved in some scenarios.

Prerequisites

The MU-MIMO function has been enabled using the **undo mu-mimo disable** command.

NOTE

The MU-MIMO optimization function is not supported by the following models.

- AirEngine series APs

Example

Enable the MU-MIMO optimization function in the SSID profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo mu-mimo disable
[HUAWEI-wlan-ssid-prof-test] mu-mimo optimize enable
```

11.1.122 ofdma downlink disable

Function

The **ofdma downlink disable** command disables the downlink (DL) OFDMA function.

The **undo ofdma downlink disable** command enables the DL OFDMA function.

By default, the DL OFDMA function is enabled.

Format

ofdma downlink disable

undo ofdma downlink disable

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

OFDMA is a multi-user technology introduced in 802.11ax. This function improves the utilization of wireless spectrum resources, supports more concurrent STAs, and improves user experience in wireless Internet access.

Example

Enable the DL OFDMA function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo ofdma downlink disable
```

11.1.123 ofdma uplink disable

Function

The **ofdma uplink disable** command disables the uplink (UL) OFDMA function.

The **undo ofdma uplink disable** command enables the UL OFDMA function.

By default, the UL OFDMA function is enabled.

Format

ofdma uplink disable

undo ofdma uplink disable

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

OFDMA is a multi-user technology introduced in 802.11ax. This function improves the utilization of wireless spectrum resources, supports more concurrent STAs, and improves user experience in wireless Internet access.

Example

Enable the UL OFDMA function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] undo ofdma uplink disable
```

11.1.124 probe-response-retry

Function

The **probe-response-retry** command sets the number of times Probe Response packets are retransmitted.

The **undo probe-response-retry** command restores the default number of times Probe Response packets are retransmitted.

By default, the number of Probe Response retransmissions is 1.

Format

probe-response-retry *retry-time*

undo probe-response-retry

Parameters

Parameter	Description	Value
retry-time	Specifies the number of times Probe Response packets are retransmitted.	The value is an integer that ranges from 0 to 3. When the value is set to 0, Probe Response packets are not retransmitted.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Probe Response frames occupy a large number of wireless resources. To reduce wireless resource occupation of the frames, you can run the **probe-response-retry** command to set a small number of or forbid Probe Response packet retransmissions.

Precautions

A small number of Probe Response packet retransmissions may reduce the channel scan efficiency of some STAs while a large number of Probe Response packet retransmissions may lower the wireless network performance.

Example

Set the number of times Probe Response packets are retransmitted to 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] probe-response-retry 0
```

11.1.125 qbss-load enable

Function

The **qbss-load enable** command enables the function of notifying STAs of AP load information.

The **undo qbss-load enable** command disables the function of notifying STAs of AP load information.

By default, the function of notifying STAs of AP load information is disabled.

Format

qbss-load enable

undo qbss-load enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

After the **qbss-load enable** command is executed, STAs are notified of the AP load status during the STA association. The notified information includes the number of STAs associated with AP radios and channel utilization. A STA selects the optimal AP based on the load of each AP to improve air interface performance.

NOTE

This command takes effect only when dynamic load balancing is disabled, because with dynamic load balancing enabled, APs will definitely notify STAs of their loads.

Modifying this configuration will cause STAs connected to the SSID to go offline and then online, interrupting STAs' services.

Example

Enable the function of notifying STAs of AP load information in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] qbss-load enable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.126 radio

Function

The **radio** command displays the radio view.

Format

radio *radio-id*

Parameters

Parameter	Description	Value
radio-id	Specifies the radio ID.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The radio configuration in the AP group view or AP view takes effect on all radios at the same time. To configure only a specified radio, enter the view of the radio to configure its parameters.

Precautions

If you run this command in the AP group view, configurations on all specified radios in the AP group are allowed. If you run this command in the AP view, configurations only on the specified radio on the AP are allowed.

Example

Display the view of radio 0 on AP 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0]
```

11.1.127 radio disable

Function

(AP group radio view) The **radio disable** command disables specified radios on all APs in an AP group.

(AP group radio view) The **undo radio disable** command enables specified radios on all APs in an AP group.

(AP radio view) The **radio disable** command disables a specified radio on a single AP.

(AP radio view) The **undo radio disable** command restores the state of a specified radio on an AP to the radio state in the AP group radio view.

By default, radios on all AP are enabled.

Format

radio disable

undo radio disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to enable or disable a specified radio.

If radio calibration is enabled on an AP, radio calibration is triggered to fill coverage holes after the radio is disabled for 8 minutes.

Example

Disable radio 0 on AP 0 .

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] radio 0
[HUAWEI-wlan-radio-0/0] radio disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.128 radio-2g-profile (WLAN view)

Function

The **radio-2g-profile** command creates a 2G radio profile and displays the 2G radio profile view, or displays the view of an existing 2G radio profile.

The **undo radio-2g-profile** command deletes a 2G radio profile.

By default, the system provides the 2G radio profile **default**.

Format

radio-2g-profile name *profile-name*

undo radio-2g-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a 2G radio profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all 2G radio profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 2G radio profile is used to configure and optimize the 2.4 GHz radio of an AP, but does not take effect on the 5 GHz radio.

Follow-up Procedure

Run the **radio-2g-profile** command to apply the 2G radio profile in the AP view, AP group view, AP radio view, or AP group radio view so that the 2G radio profile can take effect.

Precautions

- The 2G radio profile **default** cannot be deleted.
- The 2G radio profile referenced cannot be deleted. To delete the 2G radio profile, unbind it first.

Example

Create the 2G radio profile **radio-profile1** and display the view of the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio-profile1
[HUAWEI-wlan-radio-2g-prof-radio-profile1]
```

11.1.129 radio-2g-profile

Function

The **radio-2g-profile** command binds a 2G radio profile to a 2G radio.

The **undo radio-2g-profile** command unbinds a 2G radio profile from a 2G radio.

By default, no 2G radio profile is applied in the AP view or AP radio view, but the 2G radio profile **default** is applied in the AP group view and AP group radio view.

Format

radio-2g-profile *profile-name* **radio** { *radio-id* | **all** }

undo radio-2g-profile radio { *radio-id* | **all** }

The parameter **radio** { *radio-id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 2G radio profile.	The 2G radio profile must exist.
radio *radio-id*	Specifies a radio ID.	The value can be 0 or 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 2G radio profile using the **radio-2g-profile (WLAN view)** command, bind it to a 2.4 GHz radio so that the 2G radio profile can take effect.

Precautions

After a 2G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 2.4 GHz radios on APs in the AP group or on the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

Example

Create the 2G radio profile **radio-profile1** and bind it to the AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio-profile1
[HUAWEI-wlan-radio-2g-prof-radio-profile1] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio-2g-profile radio-profile1 radio 0
```

11.1.130 radio-5g-profile (WLAN view)

Function

The **radio-5g-profile** command creates a 5G radio profile and displays the 5G radio profile view, or displays the view of an existing 5G radio profile.

The **undo radio-5g-profile** command deletes a 5G radio profile.

By default, the system provides the 5G radio profile **default**.

Format

radio-5g-profile name *profile-name*

undo radio-5g-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a 5G radio profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all 5G radio profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 5G radio profile is used to configure and optimize the 5 GHz/6 GHz radio of an AP, but does not take effect on the 2.4 GHz radio.

Follow-up Procedure

Run the **radio-5g-profile** command to apply the 5G radio profile in the AP view, AP group view, AP radio view, or AP group radio view so that the 5G radio profile can take effect.

Precautions

- The 5G radio profile **default** cannot be deleted.
- A 5G radio profile referenced cannot be deleted. To delete the 5G radio profile, unbind it first.

Example

Create the 5G radio profile **radio-profile2** and display the view of the profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name radio-profile2
[HUAWEI-wlan-radio-5g-prof-radio-profile2]
```

11.1.131 radio-5g-profile

Function

The **radio-5g-profile** command binds a 5G radio profile to a 5 GHz or 6 GHz radio.

The **undo radio-5g-profile** command unbinds a 5G radio profile from a 5 GHz or 6 GHz radio.

By default, no 5G radio profile is applied in the AP view or AP radio view, but the 5G radio profile **default** is applied in the AP group view and AP group radio view.

Format

radio-5g-profile *profile-name* **radio** { *id* | **all** }

undo radio-5g-profile radio { *id* | **all** }

The parameter **radio** { *id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 5G radio profile.	The 5G radio profile must exist.
radio *id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 5G radio profile using the **radio-5g-profile (WLAN view)** command, bind it to a 5 GHz radio so that the 5G radio profile can take effect.

Precautions

After a 5G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 5 GHz radios on APs in the AP group or on the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

Example

Create the 5G radio profile **radio-profile2** and bind it to the AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name radio-profile2
[HUAWEI-wlan-radio-2g-prof-radio-profile2] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio-5g-profile radio-profile2 radio 1
```

11.1.132 radio-mode

Function

The **radio-mode** command sets the radio mode of an AP.

The **undo radio-mode** command restores the default radio mode for an AP.

By default, no radio mode is configured on an AP, and the default radio mode of the AP is used.

Format

radio-mode { **2radio-standard** | **2radio-2g-enhanced** | **2radio-5g-enhanced** | **2radio-independent-scan** | **3radio** }

undo radio-mode

Parameters

Parameter	Description	Value
2radio-standard	Specifies the standard dual-radio mode.	-
2radio-2g-enhanced	Specifies the 2G enhanced dual-radio mode. Compared with the standard dual-radio mode, the 2.4 GHz radio in this mode provides more spatial streams and higher throughput. For details, see the specifications of the corresponding AP model.	-
2radio-5g-enhanced	Specifies the 5G enhanced dual-radio mode. Compared with the standard dual-radio mode, the 5 GHz radio in this mode provides more spatial streams and higher throughput. For details, see the specifications of the corresponding AP model.	-
2radio-independent-scan	Specifies the dual-radio + independent scanning radio mode. With the independent scanning radio, functions such as air scan can be implemented without affecting service experience.	-
3radio	Specifies the three-radio mode. A third radio (radio 2) is available to allow access of more STAs.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The **radio-mode** command sets the radio mode of an AP. Radio modes supported by APs vary depending on AP models. You can check the field **Radio mode** in the **display ap-type id** *ap-type-id* command output for the radio modes supported by a specified AP model. If an AP does not support the configured radio mode, it works in the default radio mode.

- When air interface resources are sufficient, the three-radio mode is recommended to increase the capacity.
- When air interface resources are insufficient, interference is severe, or APs are densely deployed, the dual-radio mode is recommended to reduce interference.

If allowed by the AP capability:

- Dual-radio mode: recommended in large-bandwidth scenarios. In this mode, the AP can provide high throughput.
- Three-radio mode: recommended in high-concurrency scenarios. In this mode, the AP allows for access of more STAs, improving the WLAN capacity.
- Dual-radio + independent scanning radio mode: recommended in high-interference scenarios. In this mode, the AP can use an independent radio to scan air interfaces without affecting performance, thereby achieving real-time monitoring and optimization for WLAN network quality.

NOTE

- Switching the radio mode will cause an AP to restart.
- For an AirEngine 6760-X1 or AirEngine 6760-X1E, load the RTU license to switch to the triple-radio mode or dual-radio + independent scanning mode. For an AirEngine 5760-51, load the RTU license to switch to the dual-radio + independent scanning mode.
- The independent radio scanning function applies only to the 5 GHz radios of the AirEngine 8760-X1-PRO, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, and AirEngine 5760-51. The radio scanning function on the 2.4 GHz frequency band can be implemented only through a service radio. In V200R021C10 and later versions, the independent radio scanning function of the AirEngine 6761-21, AirEngine 6761-21E and AirEngine 6761S-21 is effective for both the 2.4 GHz and 5 GHz frequency bands. (In V200R021C00, this function applies only to the 5 GHz frequency band.)
- The AirEngine 6761-21, AirEngine 6761-21E, and AirEngine 6761S-21 have a dedicated radio for scanning and can perform radio scanning even in **2radio-standard** mode.
- After the radio mode of an AirEngine 6760-51EI is switched to the 2G enhanced dual-radio mode, the 2.4 GHz radio provides four streams and the 5 GHz radio becomes unavailable. After the radio mode is switched to the 5G enhanced dual-radio mode, the 5 GHz radio provides four streams and the 2.4 GHz radio becomes unavailable.

Example

Configure the standard dual-radio mode for the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] radio-mode 2radio-standard
```

11.1.133 radio-type (2G radio profile view)

Function

The **radio-type** command sets the radio type in a 2G radio profile.

The **undo radio-type** command restores the default radio type in a 2G radio profile.

By default, the radio type in a 2G radio profile is **dot11be**.

Format

radio-type { **dot11b** | **dot11g** | **dot11n** | **dot11ax** | **dot11be** }

undo radio-type

Parameters

Parameter	Description	Value
dot11b	Specifies the 802.11b radio type.	-
dot11g	Specifies the 802.11g radio type, which is backward compatible.	-
dot11n	Specifies the 802.11n radio type, which is backward compatible.	-
dot11ax	Specifies the 802.11ax radio type, which is backward compatible.	-
dot11be	Specifies the 802.11be radio type, which is backward compatible.	-

Views

2G radio profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Usually, the default radio type is used and does not need to be modified. If the default radio mode cannot meet requirements or a fault needs to be located, configure the radio type as required.

Precautions

If the configured radio type is not supported by an AP, the actual radio type supported by the AP takes effect.

If a rate in the basic rate set or supported rate set, or the multicast rate is not supported by the 802.11b protocol, the radio type cannot be set to **dot11b**.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, the rates of management frames and multicast packets that take effect on the 2.4 GHz radio of the AP are fixed as 1 Mbit/s, and the values configured using the **beacon-2g-rate** *beacon-2g-rate* and **multicast-rate** *multicast-rate* commands do not take effect on the AP.

When the L-SIG field length compatibility function of the 802.11n protocol is enabled, the radio type cannot be set to **dot11ax** or **dot11be**.

Example

Set the radio type to **dot11g** in a 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] radio-type dot11g
```

11.1.134 radio-type (5G radio profile view)

Function

The **radio-type** command sets the radio type in a 5G radio profile.

The **undo radio-type** command restores the default radio type in a 5G radio profile.

By default, the radio type in a 5G radio profile is **dot11be**.

Format

radio-type { **dot11a** | **dot11n** | **dot11ac** | **dot11ax** | **dot11be** }

undo radio-type

Parameters

Parameter	Description	Value
dot11a	Specifies the 802.11a radio type.	-
dot11n	Specifies the 802.11n radio type, which is backward compatible.	-
dot11ac	Specifies the 802.11ac radio type, which is backward compatible.	-
dot11ax	Specifies the 802.11ax radio type, which is backward compatible.	-

Parameter	Description	Value
dot11be	Specifies the 802.11be radio type, which is backward compatible.	-

Views

5G radio profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Usually, the default radio type is used and does not need to be modified. If the default radio mode cannot meet requirements or a fault needs to be located, configure the radio type as required.

Precautions

If the configured radio type is not supported by an AP, the actual radio type supported by the AP takes effect.

When the L-SIG field length compatibility function of the 802.11n protocol is enabled, the radio type cannot be set to **dot11ax** or **dot11be**.

Example

Set the radio type to **dot11n** in a 5G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] radio-type dot11n
```

11.1.135 reach-max-sta

Function

The **reach-max-sta** command controls access of new STAs when the number of STAs of a VAP reaches the maximum value.

The **undo reach-max-sta** command cancels the configuration.

By default, when the number of access users reaches the maximum value, you can determine whether to enable SSID hiding or enable the VAP to replace low-priority STAs with high-priority STAs.

Format

reach-max-sta { **hide-ssid disable** | **priority-replace** }

undo reach-max-sta

Parameters

Parameter	Description	Value
hide-ssid disable	Disable SSID hiding.	-
priority-replace	Enable the VAP to replace low-priority STAs with high-priority STAs.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

When the number of access users reaches the maximum value, you can enable SSID hiding or enable the VAP to replace low-priority STAs with high-priority STAs. The two functions cannot be configured simultaneously.

- SSID hiding: New STAs cannot search for the SSID of the VAP and need to access other VAPs.
- Replacing low-priority STAs with high-priority STAs: A new VIP user will replace a common user. This ensures access experience of VIP users.

Example

Disable automatic SSID hiding when the number of users reaches the maximum.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] reach-max-sta hide-ssid disable
```

11.1.136 regulatory-domain-profile (WLAN view)

Function

The **regulatory-domain-profile** command creates a regulatory domain profile and displays the regulatory domain profile view, or displays the view of an existing regulatory domain profile.

The **undo regulatory-domain-profile** command deletes a regulatory domain profile.

By default, the system provides the regulatory domain profile **default**.

Format

regulatory-domain-profile name *profile-name*

undo regulatory-domain-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a regulatory domain profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all regulatory domain profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A regulatory domain profile contains settings of the country code, calibration channel, and calibration bandwidth, which take effect on APs using the regulatory domain profile.

Follow-up Procedure

Run the **regulatory-domain-profile** command to bind the regulatory domain profile to an AP or AP group so that the regulatory domain profile can take effect.

Precautions

- The regulatory domain profile **default** cannot be deleted.
- The regulatory domain profile referenced by an AP or AP group cannot be deleted. To delete the regulatory domain profile, unbind it from the AP or AP group first.

Example

Create the regulatory domain profile **domain1** and display the regulatory domain profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name domain1
[HUAWEI-wlan-regulate-domain-domain1]
```

11.1.137 regulatory-domain-profile

Function

The **regulatory-domain-profile** command binds a regulatory domain profile to an AP or AP group.

The **undo regulatory-domain-profile** command unbinds a regulatory domain profile from an AP or AP group.

By default, the regulatory domain profile **default** is bound to an AP group, but no regulatory domain profile is bound to an AP. In the default regulatory domain profile, the country code is China, 2.4G calibration channels include channels 1, 6, and 11, 5G calibration channels include channels 149, 153, 157, 161, and 165, the 5G calibration bandwidth is 20 MHz, and the wideband function is disabled.

Format

regulatory-domain-profile *profile-name*

undo regulatory-domain-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a regulatory domain profile.	The regulatory domain profile must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a regulatory domain profile using the **regulatory-domain-profile (WLAN view)** command, bind it to an AP or AP group so that the regulatory domain profile can take effect.

Precautions

After a regulatory domain profile is bound to an AP or AP group, parameter settings in the regulatory domain profile apply to all APs using the profile.

Example

Create the regulatory domain profile **domain1** and bind it to AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name domain1
[HUAWEI-wlan-regulate-domain-domain1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] regulatory-domain-profile domain1
Warning: This configuration change will clear the channel and power configurations of radios, and may
restart APs. Continue?[Y/N]:y
```

11.1.138 report-disassoc-request disable

Function

The **report-disassoc-request disable** command disables an AP from reporting disassociation request packets of STAs to the AC.

The **undo report-disassoc-request disable** command enables an AP to report disassociation request packets of STAs to the AC.

By default, an AP is enabled to report disassociation request packets of STAs to the AC.

Format

report-disassoc-request disable

undo report-disassoc-request disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a large number of STAs disassociate from the network in a certain time, the APs need to report lots of disassociation request packets to the AC, impacting the AC performance. To alleviate the impact on the AC, you can disable APs from reporting disassociation request packets of STAs to the AC.

Example

Disable an AP from reporting disassociation request packets of STAs to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ab
[HUAWEI-wlan-ap-system-prof-ab] report-disassoc-request disable
```

11.1.139 report-sta-assoc enable

Function

The **report-sta-assoc enable** command enables the function of recording STA association information or STA login information in the log.

The **undo report-sta-assoc enable** command disables the function of recording STA association information or STA login information in the log.

By default, the function of recording STA association information or STA login information in the log is disabled.

Format

report-sta-assoc enable

undo report-sta-assoc enable

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

If a STA is associated or goes online after this function is enabled, the device records the STA association or login information in the log.

NOTE

Enabling this function will generate a large number of logs. If there are a large number of STAs, log files may overwrite each other due to limited storage space, which affects fault locating. To enable this function, you are advised to configure a log server to report logs. For details, choose **Configuring Information Center** > **Configuring Log Output** in the *Configuration Guide*.

Example

Enable the function of recording STA association information or STA login information in the log.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] report-sta-assoc enable
Warning: This operation will generate a large number of logs, which may overwrite other logs.
Configuring a log server is recommended. Continue?[Y/N]:y
```

11.1.140 report-sta-info enable

Function

The **report-sta-info enable** command enables an AC to report information about STA traffic statistics and online duration on APs.

The **undo report-sta-info enable** command disables an AC from reporting information about STA traffic statistics and online duration on APs.

By default, an AC is disabled from reporting information about STA traffic statistics and online duration on APs.

Format

report-sta-info enable

undo report-sta-info enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **report-sta-info enable** command to enable an AC to report information about STA traffic statistics and online duration on APs to eSight. After this function is enabled, the AC collects and reports information about STA traffic statistics and online duration on APs to eSight through syslogs when STAs get offline or roam within the AC, which facilitates data query on eSight. The STA traffic statistics include the AC's MAC address, AC name, APs' MAC addresses, AP names, radio IDs, SSID, user names, and STAs' MAC addresses.

NOTE

Enabling this function will generate a large number of logs. If there are a large number of STAs, log files may overwrite each other due to limited storage space, which affects fault locating. To enable this function, you are advised to configure a log server to report logs. For details, choose **Configuring Information Center** > **Configuring Log Output** in the *Configuration Guide*.

Example

Enable an AC to report information about STA traffic statistics and online duration on APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] report-sta-info enable
Warning: This operation will generate a large number of logs, which may overwrite other logs.
Configuring a log server is recommended. Continue?[Y/N]:y
```

11.1.141 reset ap offline-record

Function

The **reset ap offline-record** command clears AP going-offline records.

Format

reset ap offline-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears going-offline records of all APs.	-
mac *mac-address*	Clears going-offline records of the AP with specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect AP going-offline records, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

Clear going-offline records of all APs.

```
<HUAWEI> reset ap offline-record all
```

11.1.142 reset ap online-fail-record

Function

The **reset ap online-fail-record** command clears AP online failure records.

Format

reset ap online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears online failure records of all APs.	-
mac *mac-address*	Clears online failure records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect records about AP online failures, run this command to clear existing records first.

Precautions

The cleared records cannot be restored.

Example

Clear online failure records of all APs.

```
<HUAWEI> reset ap online-fail-record all
```

11.1.143 reset ap unauthorized record

Function

The **reset ap unauthorized record** command clears information about unauthorized APs.

Format

reset ap unauthorized record

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to clear the unauthorized AP list so that removed APs or unauthenticated APs that are physically disconnected from the AC can be cleared. This helps users easily collect statistics and confirm unauthorized APs.

Precautions

If an AP physically connects to the AC but has not been authenticated, the AP is added to the unauthorized AP list after you run the **reset ap unauthorized record** command.

Example

Clear information about unauthorized APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset ap unauthorized record
Warning: Clear unauthorized AP record, continue?[Y/N]:y
```

11.1.144 reset channel switch-record

Function

The **reset channel switch-record** command deletes channel switching records on a device.

Format

reset channel switch-record all

Parameters

Parameter	Description	Value
all	Deletes all channel switching records.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing channel switching records so that the system can record new channel switching events.

Precautions

Deleted channel switching records cannot be restored.

Example

Delete all channel switching records.

```
<HUAWEI> reset channel switch-record all
```

11.1.145 reset station assoc-info ap-offline-record

Function

The **reset station assoc-info ap-offline-record** command deletes information about STAs that connect to the APs in fault state.

Format

reset station assoc-info ap-offline-record { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Deletes information about all STAs that connect to APs in fault state from the AC.	-
ap-name *ap-name*	Clears information about STAs that go online on the AP with a specified name in fault state.	The AP name must exist.
ap-id *ap-id*	Clears information about STAs that go online on the AP with a specified ID in fault state.	The AP ID must exist.
radio *radio-id*	Deletes information about STAs that connect to the specified radio of the AP in fault state.	The radio ID must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on the STAs that connect to the APs in fault state within a specific period, run the **reset station assoc-info ap-offline-record** command to delete the original STA information.

Prerequisites

The APs in fault state have been enabled to allow access of new STAs using the **keep-service enable allow new-access** command.

Function

The deleted STA information cannot be restored. Exercise caution when you run the **reset station assoc-info ap-offline-record** command.

Example

Delete information about all STAs that connect to APs in fault state from the AC.

```
<HUAWEI> reset station assoc-info ap-offline-record all
```

11.1.146 reset station offline-record

Function

The **reset station offline-record** command deletes STAs' going-offline records.

Format

reset station offline-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac* }

Parameters

Parameter	Description	Value
all	Deletes going-offline records of all STAs.	-
ap-name *ap-name*	Deletes STAs' going-offline records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Deletes STAs' going-offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Deletes going-offline records of a specified STA.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing STAs' going-offline records so that the system can record new STAs' going-offline events.

Precautions

The deleted records cannot be restored.

Example

Delete going-offline records of all STAs.

```
<HUAWEI> reset station offline-record all
```

11.1.147 reset station online-fail-record

Function

The **reset station online-fail-record** command deletes records of STAs' failures to go online.

Format

reset station online-fail-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac-address* }

Parameters

Parameter	Description	Value
all	Deletes records of all STAs' failures to go online.	-
ap-name *ap-name*	Deletes records of STAs' failures to go online on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Deletes records of STAs' failures to go online on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Deletes records of failures to go online of the STA with a specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing records of STAs' failures to go online so that the system can record new failures of STAs to go online.

Precautions

The deleted records cannot be restored.

Example

Delete records of all STAs' failures to go online.

```
<HUAWEI> reset station online-fail-record all
```

11.1.148 reset station statistics

Function

The **reset station statistics** command deletes statistics about online STAs.

Format

reset station statistics [**sta-mac** *sta-mac-address*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Specifies the MAC address of an online STA.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about online STAs, run the command to clear the existing statistics.

Precautions

After the command is run, statistics about online STAs are cleared and cannot be restored.

Example

Delete statistics about the STA with MAC address 00e0-fc88-b74f.

```
<HUAWEI> reset station statistics sta-mac 00e0-fc88-b74f
```

11.1.149 rf-ping

Function

The **rf-ping** command enables an AP to proactively detect wireless link quality.

NOTE

The rf-ping function is not supported on the following APs.

- AirEngine x762

Format

rf-ping [**-m** *time* | **-c** *number* | **-p** { **be** | **bk** | **vi** | **vo** }] * *mac-address*

Parameters

Parameter	Description	Value
-m *time*	Specifies the interval for sending probe data packets.	The value is an integer that ranges from 100 to 10000, in milliseconds. The default value is 100.
-c *number*	Specifies the number of probe data packets sent by the AP.	The value is an integer that ranges from 1 to 1000. The default value is 10.
-p { **be** | **bk** | **vi** | **vo** }	Specifies the priority of probe data packets sent by the AP, which can be AC_BE, AC_BK, AC_VI, or AC_VO. If this parameter is not specified, the default priority is AC_BE.	-
mac-address	Specifies the MAC address of a STA.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be used to obtain parameters of wireless links between APs and STAs, including the signal strength, air interface rate, and packet transmission delay.

Prerequisites

STAs have been associated with the APs and gone online.

Example

Configure an AP to automatically detect the quality of the wireless link with the STA whose MAC address is 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rf-ping 00e0-fc12-3456
 Tx rate=52.0 Mbps, Reply from 00e0-fc12-3456: RSSI=-58 dBm time < 1 ms
 1 packets transmitted, 1 received, 0% packet loss, time < 1 ms, RSSI -58 dBm
```

Table 11-65 Description of the **rf-ping** command output

Item	Description
Tx rate	Transmit rate.
Reply from	STA's MAC address.
RSSI	Received signal strength.
time	Delay.
x packets transmitted	*x* packets are transmitted.
x received	*x* packets are received.
x% packet loss	Packet loss rate.

11.1.150 rts-cts-mode

Function

The **rts-cts-mode** command sets the request to send (RTS)-clear to send (CTS) operation mode in a radio profile.

The **undo rts-cts-mode** command restores the default RTS-CTS operation mode in a radio profile.

By default, the RTS-CTS operation mode is **rts-cts**.

Format

rts-cts-mode { **cts-to-self** | **disable** | **rts-cts** }

undo rts-cts-mode

Parameters

Parameter	Description	Value
cts-to-self	Sets the RTS-CTS operation mode to **cts-to-self** (only supported in the 2G radio profile view).	-
disable	Disables RTS-CTS.	-
rts-cts	Sets the RTS-CTS operation mode to **rts-cts**.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

- In **rts-cts** mode, an AP sends an RTS frame before sending data to a STA. After receiving the RTS frame, all the devices within the coverage of the AP do not send data within the specified time. Upon receiving the RTS frame, the target STA sends a CTS frame. This ensures that all the devices within the coverage of the STA do not send data within the specified time. This mode avoids conflicts but involves transmission of two frames (RTS and CTS frames), increasing the overhead.
- In **cts-to-self** mode, an AP sends a CTS frame with the AP's own address as the receiver address (RA) before sending data to a STA. This ensures that all the devices within the coverage of the AP do not send data within the specified time. In most scenarios, this mode allows an AP to only send one frame to avoid channel conflicts. However, if there is a device within the STA's coverage area but not within the AP's coverage area, a channel conflict may still occur.

Compared to the **rts-cts** mode, the **cts-to-self** mode reduces the number of control frames transmitted on the network. In some cases, however, a channel conflict may still occur when a hidden node exists and does not receive the CTS frame from the AP. Therefore, the **rts-cts** mode is more effective in avoiding channel conflicts than the **cts-to-self** mode.

To avoid the data transmission failure caused by a channel conflict, run this command to set the RTS-CTS operation mode in a radio profile as required.

Example

Set the RTS-CTS operation mode to **rts-cts** in a 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] rts-cts-mode rts-cts
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.151 rts-cts-threshold

Function

The **rts-cts-threshold** command sets the RTS-CTS threshold in a radio profile.

The **undo rts-cts-threshold** command restores the default RTS-CTS threshold in a radio profile.

The default RTS-CTS alarm threshold is 1400 bytes.

Format

rts-cts-threshold *rts-cts-threshold*

undo rts-cts-threshold

Parameters

Parameter	Description	Value
rts-cts-threshold	Specifies the RTS-CTS threshold. If the length of a frame to be sent by the MAC Layer exceeds this threshold, an RTS frame needs to be sent before this frame.	The value is an integer that ranges from 64 to 2347, in bytes.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The IEEE 802.11 MAC protocol provides an RTS-CTS handshake protocol to prevent conflicts between channels and failure to transmit data. STA A sends an RTS frame before sending data to STA B. STA A can send data after receiving a CTS frame from STA B. If multiple STAs send RTS frames to the same STA, only the STA that receives a CTS frame can send data, and other STAs must wait for a certain period and then send RTS frames again.

If STAs implement RTS-CTS handshakes before sending data, the channel bandwidth is consumed by too much RTS frames. You can set an RTS threshold to specify the length of frames to be sent. When the length of frames to be sent by the STA is smaller than the RTS threshold, no RTS/CTS handshake is implemented.

Example

Set the RTS-CTS threshold to 2300 bytes in the 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] rts-cts-threshold 2300
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.152 rx-stbc disable

Function

The **rx-stbc disable** command disables the space-time block coding (STBC) function in the receive direction.

The **undo rx-stbc disable** command enables the STBC function in the receive direction.

By default, the STBC function in the receive direction is enabled.

NOTE

The STBC function in the receive function is unconfigurable and always enabled for the following models:

- AirEngine x761
- AirEngine x762
- AirEngine x771

Format

rx-stbc disable

undo rx-stbc disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

STBC is a coding technology used in Wi-Fi standards. It uses time and space diversity in a multi-antenna system to transmit the same data over multiple antennas to improve data transmission reliability.

If severe packet loss occurs on a STA that uses STBC to send packets, it is recommended that the STBC function be disabled in the receive direction of the AP.

Example

Disable the STBC function in the receive direction in the 2G radio profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] rx-stbc disable
```

11.1.153 service-mode disable

Function

The **service-mode disable** command disables the service mode of a VAP.

The **undo service-mode disable** command enables the service mode of a VAP.

By default, the service mode of a VAP is enabled.

Format

service-mode disable

undo service-mode disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **service-mode disable** command to disable the service mode of a VAP. After the service mode of a VAP is disabled, the VAP is disabled.

- After the service mode of a VAP is enabled, run the **auto-off service** command to enable the scheduled VAP auto-off function. In the scheduled time, the VAP is disabled. To enable the VAP, run the **undo auto-off service** command.
- After the service mode of a VAP is disabled, the scheduled VAP auto-off function does not take effect.

Example

Disable the service mode of VAP **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] service-mode disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.154 service-vlan (VAP profile view)

Function

The **service-vlan** command configures a service VLAN for a VAP.

The **undo service-vlan** command restores the default service VLAN of a VAP.

By default, VLAN 1 is the service VLAN of a VAP.

Format

service-vlan { **vlan-id** *vlan-id* | **vlan-pool** *pool-name* }

undo service-vlan

Parameters

Parameter	Description	Value
vlan-id *vlan-id*	Specifies a service VLAN ID of a VAP.	The value is an integer that ranges from 1 to 4094.
vlan-pool *pool-name*	Sets the service VLANs of a VAP to all VLANs in a VLAN pool.	The VLAN pool must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can specify a specific VLAN as the service VLAN of a VAP or all VLANs in a VLAN pool as the service VLANs of a VAP. Layer 2 data packets delivered from the VAP to an AP carry the service VLAN IDs.

- When a specific VLAN is configured as the service VLAN of a VAP, STAs connected to the VAP join the same VLAN.

- When VLANs in a VLAN pool are configured as the service VLANs of a VAP, STAs connected to the VAP join different VLANs. The VLAN assignment algorithm can be configured using the **assignment** command.

Precautions

Modifying the service VLAN of a VAP will interrupt services of STAs connected to the VAP. Exercise caution when you run the command.

Example

Set the service VLAN to VLAN 2 in the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] service-vlan vlan-id 2
```

11.1.155 short-preamble disable

Function

The **short-preamble disable** command configures a radio profile not to support the short preamble.

The **undo short-preamble disable** command configures a radio profile to support the short preamble.

By default, a radio profile supports the short preamble.

Format

short-preamble disable

undo short-preamble disable

Parameters

None

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The preamble is a section of bits in the header of a data frame. It synchronizes signals transmitted between the sender and receiver. The preamble is classified into the long preamble and short preamble. The short preamble ensures better synchronization performance and therefore is recommended. The long preamble is usually used for compatibility with earlier network adapters of clients.

Example

Configure the 2G radio profile **default** not to support the short preamble.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] short-preamble disable
```

11.1.156 single-txchain enable

Function

The **single-txchain enable** command enables the single-antenna transmission mode.

The **undo single-txchain enable** command disables the single-antenna transmission mode.

By default, the single-antenna transmission mode is disabled.

Format

single-txchain enable

undo single-txchain enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some non-HT STAs that support 802.11a/b/g cannot receive packets sent by APs using multiple antennas. As a result, network access failures, frequent STA roaming, or network instability is caused. After running the **single-txchain enable** command to enable the single-antenna transmission mode in an SSID profile, management packets on the corresponding VAP and data packets sent by the AP to non-HT STAs on the VAP will be sent in single-antenna transmission mode. For a radio that is bound to a VAP with the single-antenna transmission mode enabled, control packets of the radio are sent in single-antenna transmission mode as long as non-HT STAs is connected to the VAP. When no non-HT STA is connected to the VAP, the control packets are still sent in multi-antenna transmission mode.

Precautions

APs supporting MU-MIMO support the single-antenna transmission mode.

After the single-antenna transmission mode is enabled in an SSID profile, the RSSI of STAs may be affected.

Example

Enable the single-antenna transmission mode in SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] single-txchain enable
```

11.1.157 softgre-profile (WLAN view)

Function

The **softgre-profile** command creates a soft GRE profile and displays its view, or displays the view of an existing soft GRE profile.

The **undo softgre-profile** command deletes a soft GRE profile.

By default, no soft GRE profile exists in the system.

Format

softgre-profile name *profile-name*

undo softgre-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a soft GRE profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all soft GRE profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the data forwarding mode is set to **soft-GRE**, create a soft GRE profile and bind it to a VAP profile for the soft GRE profile to take effect.

To configure parameters in a soft GRE profile, run this command to enter the soft GRE profile view. If a soft GRE profile is no longer needed, you can delete it.

Follow-up Procedure

Run the **forward-mode** command to bind the soft GRE profile to a VAP profile so that the soft GRE profile can take effect.

Precautions

The soft GRE profile referenced by a VAP profile cannot be deleted. To delete the soft GRE profile, unbind it from the VAP profile first.

Example

Create the soft GRE profile **soft1** and enter the soft GRE profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1]
```

11.1.158 ssid

Function

The **ssid** command sets a service set identifier (SSID) for an SSID profile.

The **undo ssid** command deletes the SSID of an SSID profile.

By default, the SSID HUAWEI-WLAN is configured in an SSID profile.

Format

ssid *ssid*

undo ssid

Parameters

Parameter	Description	Value
ssid	Specifies the name of an SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters. To start an SSID with a space, you need to encompass the SSID with double quotation marks (" "), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters. SSIDs containing Chinese characters cannot be displayed on STAs that do not support the UTF-8 encoding format.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSID specifies a wireless network. When you search for available wireless networks on your wireless terminal, SSIDs are displayed to identify the available wireless networks.

Precautions

When you configure an SSID containing Chinese characters, do not delete characters by pressing the **Delete** button if you want to modify the SSID that has been entered. Otherwise, the SSID will contain garbled characters after the configuration. In this case, run the **ssid** command to reconfigure the SSID.

Example

Set the SSID to **wlan-net** in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] ssid wlan-net
```

11.1.159 ssid-hide enable

Function

The **ssid-hide enable** command enables SSID hiding in Beacon frames in an SSID profile.

The **undo ssid-hide enable** command disables SSID hiding in Beacon frames in an SSID profile.

By default, SSID hiding in Beacon frames is disabled in an SSID profile.

Format

ssid-hide enable

undo ssid-hide enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A STA listens on the Beacon frames that an AP periodically sends in each channel to obtain AP information. The STA can obtain SSIDs from Beacon frames that contain the SSIDs.

The STA can actively send a probe frame with a specified SSID, only the AP with the same SSID will respond to the STA. If the STA broadcasts a probe frame without an SSID, only the APs on which SSID hiding in Beacon frames is disabled will respond to the STA.

- After the **ssid-hide enable** command is used, an AP periodically sends Beacon frames that contain empty SSID character strings and does not reply to the broadcast probe requests sent from STAs. The STAs can send probe frames with the AP's SSID to discover the SSID.
- After the **undo ssid-hide enable** command is used, an AP periodically sends Beacon frames that contain valid SSID character strings and replies to the broadcast probe requests sent from STAs. The STAs can send probe frames with the AP's SSID to discover the SSID.

Precautions

If the **ssid-hide enable** or **undo ssid-hide enable** command is run in the SSID profile after STAs are associated with an SSID, service interruptions may occur for all online STAs.

Example

Configure SSID hiding in Beacon frames in the SSID profile **ssid1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] ssid-hide enable
```

11.1.160 ssid-profile (WLAN view)

Function

The **ssid-profile** command creates an SSID profile and displays the SSID profile view, or displays the view of an existing SSID profile.

The **undo ssid-profile** command deletes an SSID profile.

By default, the system provides the SSID profile **default**.

Format

ssid-profile name *profile-name*

undo ssid-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an SSID profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all SSID profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSID profile is used to configure STA association and access parameters based on SSIDs, including the SSID name, STA association timeout period, non-HT STA access, and QoS CAR.

Follow-up Procedure

Run the **ssid-profile (VAP profile view)** command in the VAP profile view to bind the SSID profile to the VAP profile, and then bind the VAP profile to an AP, so that the SSID profile can take effect.

Precautions

- The SSID profile **default** cannot be deleted.
- An SSID profile referenced by a VAP profile cannot be deleted. To delete the SSID profile, unbind it from the VAP profile first.
- If a VAP profile has been applied to an AP, modifying the SSID profile will interrupt services.

Example

Create an SSID profile named **ssid1** and enter the SSID profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1]
```

11.1.161 ssid-profile (VAP profile view)

Function

The **ssid-profile** command binds an SSID profile to a VAP profile.

The **undo ssid-profile** command unbinds an SSID profile from a VAP profile.

By default, the SSID profile **default** is bound to a VAP profile.

Format

ssid-profile *profile-name*

undo ssid-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an SSID profile.	The SSID profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an SSID profile using the **ssid-profile (WLAN view)** command, bind it to a VAP profile to make the SSID profile take effect.

Precautions

After an SSID profile is bound to a VAP profile, parameter settings in the SSID profile take effect on all APs using the VAP profile.

Example

Create the SSID profile **ssid1** and bind it to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] quit
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] ssid-profile ssid1
```

11.1.162 sta-ipv6-service enable

Function

The **sta-ipv6-service enable** command enables the function of processing STA IPv6 services.

The **undo sta-ipv6-service enable** command disables the function of processing STA IPv6 services.

By default, the function of processing STA IPv6 services is disabled.

Format

sta-ipv6-service enable

undo sta-ipv6-service enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, IPv4 WLANs are widely deployed. If many IPv6 packets exist on an IPv4 WLAN, the performance of the WLAN is affected, and the CPU processing capability of devices will also be degraded. To improve performance of a pure IPv4 network, you can configure devices on the network to not process IPv6 packets of STAs.

Precautions

The function of processing STA IPv6 services takes effect only when the following conditions are met:

- In tunnel forwarding mode, the device does not function as an IPv6 gateway. This condition is not required in direct forwarding mode.
- The security policy is open authentication.

After the function of processing STA IPv6 services is disabled:

- The AC and APs do not process IPv6 packets of the wireless side.
- IPv6 functions cannot be configured on the wireless side.
- IPv6 functions of the wireless side are disabled even if they are enabled in default settings.

Running the **ipv6 enable** command in the interface view only enables the IPv6 function on the wired-side interface. The command cannot enable the WLAN module to process STA IPv6 services. To enable the WLAN module to process IPv6 services of STAs, you need to run the **sta-ipv6-service enable** command in the WLAN view.

Example

Enable the function of processing STA IPv6 services.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-ipv6-service enable
```

11.1.163 sta-network-detect disable

Function

The **sta-network-detect disable** command disables network detection upon STA reassociation.

The **undo sta-network-detect disable** command enables network detection upon STA reassociation.

By default, network detection upon STA reassociation is enabled.

Format

sta-network-detect disable

undo sta-network-detect disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

When accessing a new Wi-Fi network, some STAs initiate reassociation requests but not association requests. For example, this may happen when a STA attempts to access a new Wi-Fi network with the same name as the network that the STA has accessed. In this case, the STA considers that the access to the new Wi-Fi network is normal, while it actually fails to access the network. As a result, the STA cannot access network resources. To enable STAs to access the network through the normal process, you can enable network detection upon STA reassociation. When a STA reassociates with the network, the AP forcibly disconnects the STA and enables it to reinitiate an association request to access the network if all of the following conditions are met:

- The STA does not send DHCP Request messages or receive ARP Reply packets within 5s after it reassociates with the AP and goes online.
- The STA has only uplink traffic but no downlink traffic.

Example

Enable network detection upon STA reassociation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] undo sta-network-detect disable
```

11.1.164 sta-network-detect assoc enable

Function

The **sta-network-detect assoc enable** command enables network detection upon STA association.

The **undo sta-network-detect assoc enable** command disables network detection upon STA association.

By default, network detection upon STA association is disabled.

Format

sta-network-detect assoc enable

undo sta-network-detect assoc enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Some STAs may fail to access the Internet after sending association requests. To enable STAs to access the network through the normal process, you can enable network detection upon STA association. When a STA associates with the network, the AP forcibly disconnects the STA and enables it to reinitiate an association request to access the network if both of the following conditions are met:

- The STA does not send DHCP Request messages or receive ARP Reply packets within 5s after it associates with the AP and goes online.
- The STA has only uplink traffic but no downlink traffic.

Example

Enable network detection upon STA association.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] sta-network-detect assoc enable
```

11.1.165 sta-offline-delay aging-time

Function

The **sta-offline-delay aging-time** command configures the aging time for STA offline delay.

The **undo sta-offline-delay aging-time** command restores the default aging time for STA offline delay.

The default aging time for STA offline delay is 180 seconds.

Format

sta-offline-delay aging-time *time*

undo sta-offline-delay aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time for STA offline delay.	The value is an integer that ranges from 1 to 604800, in seconds. The default value is 180.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STA offline delay function is enabled, STAs can go offline and online again in the aging time without being authenticated, reducing the load on the authentication server. You can run the **sta-offline-delay aging-time** command to set the aging time.

Set the aging time for STA offline delay based on the network requirements and device performance. A long aging time causes the STA offline delay function to occupy many resources, affecting new STA access. A short aging time cannot achieve a noticeable effect in releasing the load on the authentication server.

If 802.1X authentication is used for STAs, it is recommended that set the aging time of the STA offline delay state a value ranging from 1s to 1800s. Within this range, you can set a longer delay to improve the roaming success rate of fast roaming using PMK caching and 802.11r fast roaming.

Prerequisites

The STA offline delay function has been enabled using the **sta-offline-delay enable** command.

Example

Set the aging time for STA offline delay to 300s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
[HUAWEI-wlan-view] sta-offline-delay aging-time 300
```

11.1.166 sta-offline-delay enable

Function

The **sta-offline-delay enable** command enables the STA offline delay function.

The **undo sta-offline-delay enable** command disables the STA offline delay function.

By default, the STA offline delay function is disabled.

Format

sta-offline-delay enable

undo sta-offline-delay enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a WLAN, some online STAs may go offline due to reasons such as screen lock. When these STAs go online again, they are reauthenticated, increasing the load on the authentication server. After the STA offline delay function is enabled, if a STA goes offline normally (for example, by sending a disassociation or deauthentication request or reaching the association aging time) and online again within the aging time, it does not need to be authenticated by an external or built-in authentication server. This reduces the load on the authentication server and avoids multiple authentication operations. This function takes effect for STAs only in Portal, MAC address, 802.1X, or MAC address-prioritized Portal authentication mode.

NOTE

After the STA offline delay function is enabled, if a STA goes offline normally and online again within the aging time, no authentication is needed. This may bring security risks. Exercise caution when configuring this function.

Precautions

The STA offline delay function is implemented for new access and Layer 2 roaming STAs. When a STA reassociates with a WLAN within the aging time, the STA offline delay function is implemented only in the following scenarios:

- Non-roaming scenarios. That is, the STA goes online again on the same VAP.
- Intra-AC Layer 2 roaming in direct forwarding mode, intra-AC Layer 3 roaming in direct forwarding mode (with the tunnel endpoint on the AC), or intra-AC Layer 2/3 roaming in tunnel forwarding mode.
- Inter-AC Layer 2 roaming in direct or tunnel forwarding mode.

The STA offline delay function and online STA detection on the external Portal server are mutually exclusive.

Example

Enable the STA offline delay function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
```

11.1.167 sta-offline-delay full-sta-reject enable

Function

The **sta-offline-delay full-sta-reject enable** command disables an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

The **undo sta-offline-delay full-sta-reject enable** command enables an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

By default, an AP is enabled to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

Format

sta-offline-delay full-sta-reject enable

undo sta-offline-delay full-sta-reject enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STA offline delay function is enabled on an AP, you can run this command to enable an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

Prerequisites

Before this command is executed, the **sta-offline-delay enable** command has been executed to enable the STA offline delay function.

Example

Disable an AP to force STAs in offline delay state to go offline and allow new STAs to go online after the number of STAs reaches the maximum.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
[HUAWEI-wlan-view] sta-offline-delay full-sta-reject enable
```

11.1.168 sta-offline-delay max-number

Function

The **sta-offline-delay max-number** command sets the maximum number of STAs that are allowed to delay going offline.

The **undo sta-offline-delay max-number** command restores the default maximum number of STAs that are allowed to delay going offline.

The default maximum number of STAs that are allowed to delay going offline is one fifth of the maximum number of STAs supported by an AC.

Format

sta-offline-delay max-number *max-number*

undo sta-offline-delay max-number

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of STAs that are allowed to delay going offline.	The value is an integer that ranges from 1 to the maximum number of STAs supported by an AC. The default value is one fifth of the maximum value. If one fifth of the maximum value is a non-integer value, round down the value.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STA offline delay function is enabled, you can run this command to set the maximum number of STAs that are allowed to delay going offline.

Set the maximum number of STAs that are allowed to delay going offline based on the network requirements and device performance. A large value causes the STA offline delay function to occupy many resources, affecting new STA access. A small value cannot achieve a noticeable effect in releasing the load on the authentication server.

Prerequisites

The STA offline delay function has been enabled using the **sta-offline-delay enable** command.

Example

Set the maximum number of STAs that are allowed to delay going offline to 800.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-offline-delay enable
[HUAWEI-wlan-view] sta-offline-delay max-number 800
```

11.1.169 station connectivity-detect disable

Function

The **station connectivity-detect disable** command disables STA connectivity check on the AP.

The **undo station connectivity-detect disable** command enables STA connectivity check on the AP.

By default, STA connectivity check is enabled on the AP.

Format

station connectivity-detect disable

undo station connectivity-detect disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The STA connectivity check function is enabled on an AP by default to help locate the Internet access failure issue of some STAs in certain scenarios. The AP periodically checks the uplink and downlink unicast traffic of STAs. If an exception is detected, the AP randomly selects a certain number of STAs, pings the gateway and STAs to check network connectivity, and logs the check result. After a STA is detected, the STA will not be detected repeatedly within a certain period of time.

Example

Disable STA connectivity check.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] station connectivity-detect disable
```

11.1.170 twt enable

Function

The **twt enable** command enables the target wake time (TWT) function.

The **undo twt enable** command disables the TWT function.

By default, the TWT function is disabled.

Format

twt enable

undo twt enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

TWT is a scheduling algorithm introduced in 802.11ax. A TWT Requesting STA negotiates with a TWT Responding STA (AP) to determine TWT parameters and wake ups for some time called service period (SP). In this manner, STAs can doze always except during the SP intervals, which saves power consumption of the STA and allows an AP to manage activities in the BSS in order to minimize contention between STAs.

It is recommended that the TWT function be disabled if the STA and AP are incompatible with each other due to different protocol implementation modes.

Example

Enable the TWT function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] twt enable
```

11.1.171 type (VAP profile view)

Function

The **type** command sets the type for a VAP.

The **undo type** command restores the default VAP type.

By default, the type of a VAP is service.

Format

type { **ap-management** | **service** | **service-backup ap-offline** | **service-backup auth-server-down radius-server template** *template-name* | **service-backup distribute** }

undo type

Parameters

Parameter	Description	Value
ap-management	Sets the VAP type to AP management.	-
service	Sets the VAP type to service.	-
service-backup ap-offline	Sets the VAP type to AP-offline backup service.	-
service-backup auth-server-down	Sets the VAP type to authentication-server-down backup service.	-
radius-server template *template-name*	Specifies the name of a RADIUS server template.	The specified name of the RADIUS server template must exist.
service-backup distribute	Sets the VAP type to distributed-AP backup service. **NOTE** This parameter takes effect only for the backup AP in the zero-roaming distributed architecture.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the type of a VAP is set to **ap-management**, STAs connected to the VAP can only access APs but not network resources. AP management VAPs are used in STA access and AP management scenarios.
- If the type of a VAP is set to **service**, STAs connected to the VAP can only access network resources but not APs. Service VAPs are used in regular WLAN deployment scenarios.
- If the type of a VAP is set to **service-backup ap-offline**, STAs can access the network through the backup service VAP after the AP goes offline. For example, on a headquarters-branch network, when APs at branches connect to the AC at the headquarters through a WAN, APs may go offline due to the WAN instability. In this case, you can configure a backup service VAP to allow new STAs to access the network if the AP goes offline.

- If the type of a VAP is set to **service-backup auth-server-down**, the VAP is automatically enabled to allow network access of associated STAs when the authentication server is not accessible. When the authentication server recovers, this VAP is not automatically disabled. You can manually disable it if needed. If the authentication server is accessible but rejects user access, this VAP is not automatically enabled. You can manually enable it if needed. To enable or disable this VAP, run the **vap-service-backup auth-server-down** command.
- When the VAP type is distributed-AP backup service, the backup VAP continuously detects the signal output of the distributed VAP with the same SSID. If the signal from the distributed VAP with the same SSID is not detected within 25 Beacon intervals, the backup VAP considers the distributed AP faulty and automatically releases signals to ensure that STAs can access the network. After the distributed VAP recovers, the signal of the backup VAP is shut down, and STAs are switched back to the distributed VAP.

Precautions

- After the VAP type is configured in the VAP profile view, the VAPs generated by the VAP profile use the configured VAP type. The new VAP type will overwrite the old one.
- For an AP management VAP:
  - Portal, MAC address, and 802.1X authentication using an external server is not supported.
  - The VAP profile in which the VAP type is set to **ap-management** can be applied only to one radio of an AP or AP group.
  - If an AD9431DN-24X or AirEngine 9700D-M is used as the central AP, STAs log in to RUs through the offline management VAP. If a central AP other than the AD9431DN-24X or AirEngine 9700D-M is used, STAs log in to the central AP through the offline management VAP.
- For an AP-offline backup service VAP:
  - Only the WPA3 SAE, WPA2-WPA3 PSK-SAE, open, WEP, WPA+PSK, WPA2+PSK and WPA-WPA2+PSK authentication modes are supported.
  - Service data can be forwarded only in direct mode.
  - When the number of configured AP-offline backup service VAPs reaches the maximum on the AP, if the offline management VAP function is enabled, the offline management VAP does not take effect when the AP goes offline.
- For an authentication-server-down backup service VAP:
  - Only the WPA3 SAE, WPA2-WPA3 PSK-SAE, open, WEP, WPA+PSK, WPA2+PSK and WPA-WPA2+PSK authentication modes are supported.
  - This VAP type is exclusive with the AP management VAP and AP-offline backup service VAP.
- For a distributed-AP backup service VAP:
  - Before configuring distributed AP backup, run the **distribute-mode enable** command to enable DAP network collaboration.
  - When a STA switches between a distributed VAP and backup VAP, the process is similar to WLAN roaming, and a few packets may be lost.

Example

Create the VAP profile **vap1** and set the VAP type to AP management VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] type ap-management
```

Create the VAP profile **vap1** and set the VAP type to **authentication-server-down backup service**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] type service-backup auth-server-down radius-server template temp1
```

11.1.172 u-apsd enable

Function

The **u-apsd enable** command enables the Unscheduled Automatic Power Save Delivery (U-APSD) function.

The **undo u-apsd enable** command disables the U-APSD function.

By default, the U-APSD function is disabled.

Format

u-apsd enable

undo u-apsd enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

U-APSD is a new energy saving mode defined for WMM, which can improve the energy-saving capability of STAs.

If some STAs on the network do not support the U-APSD function, disable the U-APSD function.

Precautions

The U-APSD function takes effect only when WMM is enabled.

After the U-APSD function is enabled, services may be interrupted.

Example

Enable the U-APSD function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] u-apsd enable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.173 undo ap

Function

The **undo ap** command deletes an AP.

Format

undo ap { **ap-name** *ap-name* | **ap-id** *ap-list* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Deletes the AP with a specified AP name.	The AP name must exist.
ap-id *ap-list*	Deletes APs with the specified IDs in a batch.	The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) or hyphens (-) to separate AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.
ap-mac *ap-mac*	Deletes the AP with a specified MAC address.	The AP's MAC address must exist.
ap-group *group-name*	Deletes the APs in a specified AP group.	The AP group must exist.
all	Deletes all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you do not want a specified Fit AP to go online on the AC, run this command to delete the Fit AP from the AC. After the Fit AP is deleted, it goes offline from the AC.

Configuration Impact

Deleting an AP will interrupt services of STAs connected to the AP.

Precautions

APs that are being upgraded, stay in standby or unauth state, or are executing the **ap-ping** command cannot be deleted.

In NETCONF mode, if any of the APs managed by the switch has been registered on the iMaster NCE-Campus, you cannot delete all APs using the **undo ap all** command. AP registration on the iMaster NCE-Campus indicates that an AP has been online on the iMaster NCE-Campus or the switch successfully synchronizes the configured AP information to the iMaster NCE-Campus.

Example

Delete the AP named **Area_1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] undo ap ap-name Area_1
Warning: Deleting the AP will interrupt user services. Continue?[Y/N]:y
```

11.1.174 untagged vlan (soft GRE profile view)

Function

The **untagged vlan** command configures soft GRE tunnel packets sent by APs not to carry VLAN tags.

The **undo untagged vlan** command restores the default status of whether soft GRE tunnel packets sent by APs carry VLAN tags.

By default, soft GRE tunnel packets sent by APs carry VLAN tags.

Format

untagged vlan *vlan-id*

undo untagged vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN tag to be removed.	The value is an integer that ranges from 1 to 4094.

Views

Soft GRE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving service data packets from STAs, an AP adds a service VLAN tag to the packets and performs soft GRE tunnel encapsulation. Then the soft GRE tunnel packets sent by the AP carry the VLAN tag. However, in some scenarios, the peer device of the soft GRE tunnel connected to the AP cannot process tagged packets. After this command is run, the soft GRE interface is added to the configured VLAN in untagged mode, and the PVID is also set to the configured VLAN. If the configured VLAN is a service VLAN, the service VLAN tag is removed after packets pass through the soft GRE interface. The soft GRE tunnel packets sent by the AP are transmitted in untagged mode.

Precautions

A soft GRE profile supports only one untagged VLAN.

Example

Configure APs to remove service VLAN 101 from soft GRE tunnel packets and transmit the packets in untagged mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] softgre-profile name soft1
[HUAWEI-wlan-softgre-prof-soft1] untagged vlan 101
```

11.1.175 utmost-power

Function

The **utmost-power disable** command disables radios from sending packets at the maximum power.

The **utmost-power enable** command enables radios to send packets at the maximum power.

The **undo utmost-power** command restores the adaptive mode for radios to send packets.

By default, a radio sends packets in adaptive mode.

Format

utmost-power { **disable** | **enable** }

undo utmost-power

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is valid for all country codes. You can run the **utmost-power enable** command to enable radios to send packets at the maximum power or run the **utmost-power disable** command to enable radios to send packets at the power specified by the country code. After you run the **undo utmost-power** command to restore the adaptive mode, radios send packets at the maximum power if the country code is CN or at the power specified by other country codes.

Precautions

This function may cause AP radios to exceed the laws and regulations of the local country or region. Therefore, ensure that you have obtained permission from the local administrative department before using this function.

For APs running R024C00 or later, this function takes effect only on the 2.4 GHz and 5 GHz radios, but not on 6 GHz radios.

Example

Disable radios from sending packets at the maximum power.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] utmost-power disable
```

11.1.176 vap-profile (WLAN view)

Function

The **vap-profile** command creates a VAP profile and displays the VAP profile view, or displays the view of an existing VAP profile.

The **undo vap-profile** command deletes a VAP profile.

By default, the system provides the VAP profile **default**.

Format

vap-profile name *profile-name*

undo vap-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a VAP profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all VAP profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a radio profile is bound to an AP, the AP can send and receive radio signals. After a VAP profile is bound to an AP, the VAP is generated to provide wireless access services for STAs. You can configure parameters in the VAP profile to enable APs to provide different wireless services.

Follow-up Procedure

Run the **vap-profile** command to apply the VAP profile in the AP group view, AP view, AP radio view, or AP group radio view so that the VAP profile can take effect.

Precautions

- The VAP profile **default** cannot be deleted.
- The VAP profile referenced in the AP group view, AP view, AP radio view, or AP group radio view cannot be deleted. To delete the VAP profile, unbind it from the AP group view, AP view, AP radio view, or AP group radio view first.
- By default, the SSID profile **default**, security profile **default**, and traffic profile **default** are bound to a VAP profile.

Example

Create the VAP profile **vap1** and enter the VAP profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1]
```

11.1.177 vap-profile

Function

The **vap-profile** command binds a VAP profile to a radio.

The **undo vap-profile** command unbinds a VAP profile from a radio.

By default, no VAP profile is bound to a radio.

Format

vap-profile *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** } [**service-vlan** { **vlan-id** *vlan-id* | **vlan-pool** *pool-name* }]

undo vap-profile *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** }

The parameter **radio** { *radio-id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a VAP profile.	The VAP profile must exist.

Parameter	Description	Value
wlan *wlan-id*	Specifies the WLAN ID of a VAP.	The value is an integer that ranges from 1 to 16. **NOTE** ● The WLAN ID for the WDS service can be 13 or 14. ● The WLAN ID for the Mesh service is 16. ● The WLAN ID for the offline management VAP configuration is 15 or an integer that ranges from 1 to 12. ● For some AP models, the maximum number of VAPs supported by each radio is less than 16. If the value of *wlan-id* exceeds the AP specifications, the configuration cannot take effect and the AP cannot generate radio signals.
radio	Specifies a radio.	-
radio-id	Specifies a radio ID.	The value is an integer that ranges from 0 to 2.
all	Specifies all radios.	-
service-vlan	Specifies a service VLAN ID.	-
vlan-id *vlan-id*	Specifies a VLAN ID.	The VLAN ID must exist.
vlan-pool *pool-name*	Specifies the name of a VLAN pool.	The VLAN pool must exist.

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VAP profile using the **vap-profile (WLAN view)** command, bind it to a radio so that the VAP profile can take effect.

In some scenarios, users want to configure one VAP for all APs. However, APs use different service VLANs. To simplify the configuration, you can specify a service VLAN using the parameter **service-vlan** when binding a VAP profile. The priority of the service VLAN specified in this command is higher than that of a service VLAN configured using the **service-vlan** command.

Precautions

After a VAP profile is bound to a radio, parameter settings in the VAP profile apply to the radio using the profile.

Example

Create the VAP profile **vap1** and bind **vap1** to the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] vap-profile vap1 wlan 1 radio 0
```

11.1.178 vap-service-backup auth-server-down

Function

The **vap-service-backup auth-server-down** command manually enables or disables an authentication-server-down backup service VAP.

Format

vap-service-backup auth-server-down { **active** | **inactive** } [**vap-profile** *profile-name*]

Parameters

Parameter	Description	Value
active	Manually enables an authentication-server-down backup service VAP.	-
inactive	Manually disables an authentication-server-down backup service VAP.	-

Parameter	Description	Value
vap-profile *profile-name*	Specifies the name of a VAP profile. If this parameter is not specified, VAPs of this type on all referenced radios are enabled.	The VAP profile name must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an authentication-server-down backup service VAP is not automatically disabled after the authentication server is restored, the administrator can manually disable this VAP. When the authentication server rejects access of STAs, the administrator can manually enable an authentication-server-down backup service VAP to enable the STAs to enter the survival state.

Precautions

After an authentication-server-down backup service VAP is manually disabled, STAs associated with this VAP go offline.

Example

Manually enable an authentication-server-down backup service VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-service-backup auth-server-down active vap-profile vap1
```

11.1.179 vht a-mpdu max-length-exponent

Function

The **vht a-mpdu max-length-exponent** command sets the maximum length of an aggregated MPDU (A-MPDU) on the 802.11ac radio. MPDU stands for MAC protocol data unit.

The **undo vht a-mpdu max-length-exponent** command restores the maximum length of an A-MPDU on the 802.11ac radio to the default value.

By default, the index for the maximum length of an A-MPDU is 7. The maximum length of the A-MPDU is 1048575 bytes.

The function is not supported by the following models.

- AirEngine series APs

Format

vht a-mpdu max-length-exponent *max-length-exponent-index*

undo vht a-mpdu max-length-exponent

Parameters

Parameter	Description	Value
max-length-exponent-index	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 7. - 0: indicates that the maximum length of the A-MPDU is 8191 bytes. - 1: indicates that the maximum length of the A-MPDU is 16383 bytes. - 2: indicates that the maximum length of the A-MPDU is 32767 bytes. - 3: indicates that the maximum length of the A-MPDU is 65535 bytes. - 4: indicates that the maximum length of the A-MPDU is 131071 bytes. - 5: indicates that the maximum length of the A-MPDU is 262143 bytes. - 6: indicates that the maximum length of the A-MPDU is 524287 bytes. - 7: indicates that the maximum length of the A-MPDU is 1048575 bytes.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11ac uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the index of the maximum length of the A-MPDU to 2 in the 5G radio profile **default**. The index 2 corresponds to a maximum length of 32767 bytes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] vht a-mpdu max-length-exponent 2
```

11.1.180 a-msdu enable

Function

The **a-msdu enable** command enables the function of sending 802.11 frames in A-MSDU mode.

The **undo a-msdu** command restores the default configuration of sending 802.11 frames in A-MSDU mode.

By default, the function of sending 802.11 frames in A-MSDU mode is in self-adaptive state.

Format

a-msdu { **enable** | **disable** | **auto** }

undo a-msdu

Parameters

Parameter	Description	Value
enable	Enables the A-MSDU function.	-
disable	Disables the A-MSDU function.	-

Parameter	Description	Value
auto	Sets the A-MSDU function to the self-adaptive mode to enable or disable the A-MSDU function based on the AP capability. When this parameter is delivered to APs running a version earlier than V200R020C00, this function is disabled on the APs. When this parameter is delivered to APs running V200R020C00 or later, this function is enabled on the APs.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Aggregated MAC Service Data Unit (A-MSDU) technology aggregates multiple MAC Service Data Units (MSDUs) into an MAC Protocol Data Unit (MPDU), which reduces MAC layer costs of the 802.11 packets and improves packet transmission efficiency especially when short MSDUs are aggregated.

Precautions

The function of sending 802.11 frames in A-MSDU mode can be enabled on radios in compliance with 802.11n and later standards.

For AirEngine series APs, it is recommended that this function be enabled to improve air interface performance.

Example

Enable the function of sending 802.11 frames in A-MSDU mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] a-msdu enable
```

11.1.181 vht a-msdu max-frame-num

Function

The **vht a-msdu max-frame-num** command sets the maximum number of subframes that can be aggregated into an A-MSDU at one time.

The **undo vht a-msdu max-frame-num** command restores the default maximum number of subframes that can be aggregated into an A-MSDU at one time.

By default, a maximum of two subframes can be aggregated into an A-MSDU at one time.

The function is not supported by the following models.

- AirEngine series APs

Format

vht a-msdu max-frame-num *max-frame-number*

undo vht a-msdu max-frame-num

Parameters

Parameter	Description	Value
max-frame-number	Specifies the maximum number of subframes that can be aggregated into an A-MSDU at one time.	The value is an integer that ranges from 2 to 15.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A-MSDU technology aggregates multiple MSDUs into an MPDU, which reduces MAC layer costs of the 802.11 packets.

- When the wireless network quality is satisfactory, increase the maximum number of subframes that can be aggregated into an A-MSDU at one time to improve the network usage efficiency and wireless service performance.
- When the wireless network quality is unsatisfactory or delay-sensitive services, such as voice services are transmitted, reduce the maximum number of subframes that can be aggregated into an A-MSDU at one time to minimize the impact of packet loss on services and reduce packet transmission delay. Some STAs have restrictions on the number of subframes aggregated into a received A-MSDU. If the number of subframes sent by the AP exceeds the threshold, the STAs cannot receive the frames properly.

Prerequisites

The function of sending 802.11 frames in A-MSDU mode has been enabled using the **a-msdu enable** command.

Example

Set the maximum number of subframes that can be aggregated into an A-MSDU at one time to 3.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] vht a-msdu max-frame-num 3
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.1.182 vht mcs-map

Function

The **vht mcs-map** command configures the maximum number of spatial streams and the maximum MCS value supported by 802.11ac in the 5G radio profile.

The **undo vht mcs-map** command restores the default configuration.

By default, the maximum number of spatial streams and the maximum MCS value are not specified in the 5G radio profile.

Format

vht mcs-map nss *nss-value* **max-mcs** *max-mcs-value*

undo vht mcs-map

Parameters

Parameter	Description	Value
nss *nss-value*	Specifies the maximum number of available spatial streams.	The value is an integer ranging from 1 to 8.
max-mcs *max-mcs-value*	Specified the maximum MCS value that can be negotiated for spatial streams.	The value is an integer ranging from 7 to 9.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rates of 802.11ac APs depend on the index value of MCS. A larger MCS value indicates a higher transmission rate.

- When *nss-value* is greater than or equal to the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as the maximum number of spatial streams supported by the AP.
- When *nss-value* is smaller than the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as *nss-value* and remaining spatial streams do not take effect.

  For example, if *nss-value* is set to 2 and the AP supports a maximum of 3 spatial streams, the maximum number of available spatial streams on the AP is 2.

Precautions

The following configurations take effect in descending order of priority: Reliability-first service guarantee mode configured using the **service-guarantee reliability-first** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map (SSID Profile)** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map** command in the 5G radio profile.

This configuration takes effect only when the AP communicates with STAs through 802.11ac.

Example

In the 5G radio profile, set the maximum number of available spatial streams to 2 and the maximum MCS value to 8.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] vht mcs-map nss 2 max-mcs 8
```

11.1.183 vht mcs-map (SSID profile)

Function

The **vht mcs-map** command configures the maximum number of spatial streams and the maximum MCS value supported by 802.11ac in the SSID profile.

The **undo vht mcs-map** command restores the default configuration.

By default, the maximum number of spatial streams and the maximum MCS value are not specified in the SSID profile.

Format

vht { **tx** | **rx** } **mcs-map nss** *nss-value* **map** *mcs-value*

undo vht { **tx** | **rx** } **mcs-map**

Parameters

Parameter	Description	Value
tx	Indicates the sent data.	-
rx	Indicates the received data.	-
nss *nss-value*	Specifies the maximum number of available spatial streams.	The value is an integer that ranges from 1 to 8.
map *mcs-value*	Specified the maximum MCS value that can be negotiated for spatial streams.	The value is an integer that ranges from 7 to 9.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rates of 802.11ac APs depend on the index value of MCS. A larger MCS value indicates a higher transmission rate.

- When *nss-value* is greater than or equal to the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as the maximum number of spatial streams supported by the AP.
- When *nss-value* is smaller than the maximum number of spatial streams supported by an AP, the number of available spatial streams is the same as *nss-value* and remaining spatial streams do not take effect.

  For example, if *nss-value* is set to 2 and the AP supports a maximum of 3 spatial streams, the maximum number of available spatial streams on the AP is 2.

Precautions

The following configurations take effect in descending order of priority: Reliability-first service guarantee mode configured using the **service-guarantee reliability-first** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map (SSID Profile)** command in the SSID profile > Number of spatial streams and MCS value configured using the **vht mcs-map** command in the 5G radio profile.

This configuration takes effect only when the AP communicates with STAs through 802.11ac.

Example

In the SSID profile, set the maximum number of available spatial streams to 2 and the maximum MCS value to 8.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] vht rx mcs-map nss 2 map 8
```

11.1.184 vip-user bandwidth reservation-ratio

Function

The **vip-user bandwidth reservation-ratio** command configures the percentage of bandwidth reserved for VIP users.

The **undo vip-user bandwidth reservation-ratio** command restores the default percentage of bandwidth reserved for VIP users.

The default percentage of bandwidth reserved for VIP users is 20%.

Format

vip-user bandwidth reservation-ratio *reservation-ratio*

undo vip-user bandwidth reservation-ratio

Parameters

Parameter	Description	Value
reservation-ratio	Specifies the percentage of bandwidth reserved for VIP users.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 20.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Bandwidth reservation for VIP users enables VIP users to preferentially enjoy experience improvement brought by resource reservation in the case of air interface congestion. You can run this command to adjust the percentage of bandwidth reserved for VIP users based on radios. The reserved bandwidth is shared by all VIP users.

The specific improvement effect depends on factors such as the number of VIP users and service types. It is recommended that you set *reservation-ratio* to 75%

when the **proportion of the number of VIP users to the total number of users** is 50% or set the value to 50% when the proportion is 20%. You can adjust the value based on the site requirements.

Example

In the 2G radio profile **default**, set the percentage of bandwidth reserved for VIP users to 30%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] vip-user bandwidth reservation-ratio 30
```

11.1.185 wlan

Function

The **wlan** command displays the WLAN view.

Format

wlan

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before performing WLAN configurations, run the **wlan** command to enter the WLAN view. All WLAN configuration commands need to be used in the WLAN view or WLAN sub-view.

Example

Enter the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view]
```

11.2 AP Management Configuration Commands

11.2.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.2.2 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a STA passes authentication or successfully associates with the AP, the AP sends system logs to the NMS server. A system log contains MAC addresses of the STA, AC, and AP, AP and AC name and current time, and authentication result.

If a STA fails to associate with an AP or fails authentication, the STA attempts to go online continuously. The AP sends a large number of duplicate logs to the AC in a short period, which wastes resources and deteriorates system performance. To prevent this problem, enable system log suppression.

Example

Enable system log suppression.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain enable
```

11.2.3 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets the period of system log suppression.

The **undo access-user syslog-restrain period** command restores the default period of system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period of system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a STA is authenticated or successfully associates with an AP, the AP sends system logs to the NMS server. A system log contains the MAC addresses of the STA, AP, and AC, AP name, AC name, current time, and authentication result.

A STA retries continuously after it fails to associate with an AP or pass the authentication. When this occurs, the AC sends a large number of logs in a short time. This results in a high statistics failure rate and degrades the NMS performance. The system log suppression function reduces impact of such logs on the NMS. After the period of system log suppression is set, the AC will send only one system log to the NMS server during the suppression period, reducing the load on the server.

Example

Set the period of system log suppression to 600s.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain period 600
```

11.2.4 ac-list (AP view)

Function

The **ac-list** command configures an AC IPv4 address list for APs.

The **undo ac-list** command restores the AC IPv4 address list to the default value.

By default, no AC IPv4 address list is configured.

Format

ac-list *ipv4-address* &<1-4>

undo ac-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an AC.	The value is in dotted decimal notation.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to statically configure an AC IPv4 address list for APs.

In addition to the static configuration, APs can dynamically obtain an AC IP address list through DHCP or DNS. When an AP goes online, it sends Discovery Request unicast packets to all ACs' IP addresses that are statically or dynamically obtained. After receiving the Discovery Request packets, the ACs respond to the AP with a Discovery Response packet. Based on AC information such as the AP management capability, maximum number of access STAs, and IP address, the AP selects one AC to establish a CAPWAP tunnel. If the AP does not have the AC IP address list or receives no response to the Discovery Request packet, the AP broadcasts Discovery Request packets to discover ACs on the same network segment.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

Example

Set the AC's IPv4 address to 192.168.10.1 in the AP view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] ac-list 192.168.10.1
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.5 ac-list (AP provisioning view)

Function

The **ac-list** command configures an AC IPv4 address list for APs.

The **undo ac-list** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, no AC IPv4 address list is configured.

Format

ac-list *ipv4-address* &<1-4>

undo ac-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an AC.	The value is in dotted decimal notation.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to statically configure an AC IPv4 address list for APs.

In addition to the static configuration, APs can dynamically obtain an AC IP address list through DHCP or DNS. When an AP goes online, it sends Discovery

Request unicast packets to all ACs' IP addresses that are statically or dynamically obtained. After receiving the Discovery Request packets, the ACs respond to the AP with a Discovery Response packet. Based on AC information such as the AP management capability, maximum number of access STAs, and IP address, the AP selects one AC to establish a CAPWAP tunnel. If the AP does not have the AC IP address list or receives no response to the Discovery Request packet, the AP broadcasts Discovery Request packets to discover ACs on the same network segment.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Example

Set the AC's IPv4 address to 192.168.10.1 in the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ac-list 192.168.10.1
```

11.2.6 address-mode (AP view)

Function

The **address-mode** command sets the mode in which an AP obtains an IP address.

The **undo address-mode** command restores the default mode in which an AP obtains an IP address.

By default, the mode in which an AP obtains an IP address is not configured.

Format

address-mode { **dhcp** | **static** }

undo address-mode

Parameters

Parameter	Description	Value
dhcp	Indicates that an IP address is obtained in DHCP mode. The AP functions as a DHCP client and is assigned an IP address by the DHCP server.	-
static	Indicates that a static IP address is obtained. The AP must be configured with a static IP address.	-

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **address-mode** command to configure an AP to obtain an IP address in DHCP or static mode.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

Example

Configure an AP to obtain an IP address in DHCP mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] address-mode dhcp
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.7 address-mode (AP provisioning view)

Function

The **address-mode** command sets the mode in which an AP obtains an IP address.

The **undo address-mode** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, the mode in which an AP obtains an IP address is not configured.

Format

address-mode { **dhcp** | **static** }

undo address-mode

Parameters

Parameter	Description	Value
dhcp	Indicates that an IP address is obtained in DHCP mode. The AP functions as a DHCP client and is assigned an IP address by the DHCP server.	-

Parameter	Description	Value
static	Indicates that a static IP address is obtained. The AP must be configured with a static IP address.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **address-mode** command to configure an AP to obtain an IP address in DHCP or static mode.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Example

Configure an AP to obtain an IP address in DHCP mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] address-mode dhcp
```

11.2.8 alarm-restriction disable

Function

The **alarm-restriction disable** command disables alarm suppression for an AP.

The **undo alarm-restriction disable** command enables alarm suppression for an AP.

By default, alarm suppression is enabled for an AP.

Format

alarm-restriction disable

undo alarm-restriction disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA cannot go online due to security type mismatch, UAC, or access user upper limit exceeding, the STA will automatically re-connect to the AP. During this period, the AP sends a large number of the same STA association failure alarms to the AC, which degrades the system performance.

To solve this problem, enable alarm suppression for the AP. The AP then does not report alarms repeatedly in the alarm suppression period, preventing alarm storms.

Example

Disable alarm suppression for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] alarm-restriction disable
```

11.2.9 alarm-restriction period

Function

The **alarm-restriction period** command configures the period of alarm suppression on an AP.

The **undo alarm-restriction period** command restores the default period of alarm suppression for an AP.

The default alarm suppression period is 60 seconds on an AP.

Format

alarm-restriction period *period*

undo alarm-restriction period

Parameters

Parameter	Description	Value
period	Specifies the period of alarm suppression for an AP.	The value is an integer that ranges from 10 to 300, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap alarm-restriction period** command to configure the period of alarm suppression for an AP. The AP reports an alarm only one time in the specified period if the alarm is repeatedly generated.

Example

Set the period of alarm suppression to 200 seconds for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] alarm-restriction period 200
```

11.2.10 ap lldp enable

Function

The **ap lldp enable** command enables the Link Layer Discovery Protocol (LLDP) in the WLAN view.

The **undo ap lldp enable** command disables LLDP in the WLAN view.

By default, LLDP is enabled in the WLAN view.

Format

ap lldp enable

undo ap lldp enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LLDP is a Layer 2 discovery protocol defined in the IEEE 802.1ab standard. Using LLDP, the AC or NMS can obtain Layer 2 information about the connected APs, including APs' interfaces and connections with other devices. Additionally, the AC or NMS can obtain details about network topology and interface changes. To view the Layer 2 link status between APs, and between APs and switch or analyze the network topology, enable WLAN LLDP.

Precautions

WLAN LLDP can be enabled in the system view and the AP wired port link profile view.

- An AP can send and receive LLDP packets only after LLDP is enabled in both the WLAN view and the AP wired port link profile view.
- After LLDP is disabled in the WLAN view, the commands for enabling and disabling LLDP on the AP wired port link profile view do not take effect.

Example

Enable LLDP in the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap lldp enable
```

11.2.11 ap manufacturer-config

Function

The **ap manufacturer-config** command restores the factory settings of APs.

Format

ap manufacturer-config { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP whose factory settings need to be restored.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP whose factory settings need to be restored.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP whose factory settings need to be restored.	The AP ID must already exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When a configuration error occurs on an AP, you can run this command to clear AP configurations.

NOTICE

Restoring the factory defaults of an AP will reset the AP and restore all the default AP configurations.

Example

Restore the factory settings of AP **N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap manufacturer-config ap-name N1-2
Warning: Reset AP to the manufacturing default configuration, continue?[Y/N]:y
```

11.2.12 ap update ftp-server

Function

The **ap update ftp-server** command configures basic FTP information, including the IP address, user name, and password of the FTP server.

The **undo ap update ftp-server** command restores default FTP settings.

By default, no basic FTP information is configured.

Format

ap update ftp-server ip-address *server-ip-address* [**port** *port*] **ftp-username** *ftp-username* **ftp-password cipher** *ftp-password*

undo ap update ftp-server ip-address

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the FTP server.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port*	Specifies a port number for the FTP server. If no port number is specified, the default port 21 is used.	The value is an integer that ranges from 1 to 65535.
ftp-username *ftp-username*	Specifies the user name for logging in to the FTP server.	The value is a string of 1 to 31 characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (") or spaces.
ftp-password	Specifies the password for logging in to the FTP server.	-
cipher	Specifies the password in ciphertext.	-
ftp-password	Specifies the FTP server password.	The value is a string of characters without question marks (?), and cannot start or end with double quotation marks (") or spaces. *ftp-password* can be a string of 1 to 188 characters in ciphertext, such as **%^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#**, or a string of 1 to 128 characters in plaintext, such as **YsHsjx_202206**.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- The FTP configuration is used when the automatic upgrade and online upgrade modes are FTP. In the automatic upgrade or online upgrade, the AC sends basic FTP information to the AP, and the AP requests the FTP server for upgrade based on FTP information.
- After running the **ap update ftp-server** command, you can perform the following operations:
  a. Run the **ap update mode** command to set the upgrade mode to ftp-mode.
  b. Run the **ap update multi-load** command to upgrade APs in batches.

Precautions

- It is recommended that you use an external FTP server to upgrade APs. If the AC functions as the FTP server, a maximum of five APs can be upgraded simultaneously. If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.
- APs do not support the double quotation marks ("). Ensure that the FTP server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, the FTP upgrade fails.
- When the FTP port number is specified, the upgrade is applicable only to APs in V200R020C10 and later. If the source version of APs is earlier than V200R020C10, the FTP upgrade fails.
- The FTP server must support the REST field. Otherwise, the upgrade will fail. If the following information is displayed, the upgrade fails because the server does not support the REST field. In this case, replace the server.

```
Error: Upgrade failed because the FTP server does not support the REST command.
```

Example

Configure the IP address, user name, and password of the FTP server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update ftp-server ip-address 192.168.1.100 ftp-username admin ftp-password
cipher YsHsjx_202206
```

11.2.13 ap update ftp-server max-connect-number

Function

The **ap update ftp-server** command configures the maximum number of APs that can be upgraded simultaneously in FTP mode.

The **undo ap update ftp-server** command restores the default maximum number of APs that can be upgraded simultaneously in FTP mode.

By default, a maximum of 50 APs can be upgraded simultaneously in FTP mode.

Format

ap update ftp-server max-connect-number *max-connect-number*

undo ap update ftp-server max-connect-number

Parameters

Parameter	Description	Value
max-connect-number	Specifies the maximum number of APs that can be upgraded simultaneously.	The value is an integer that ranges from 1 to 64.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in FTP mode, you can configure the value of *max-connect-number* to change the maximum number of APs that can be upgraded simultaneously.

- If the number of APs to be upgraded is equal to or smaller than *max-connect-number*, all APs can be upgraded simultaneously.
- If the number of APs to be upgraded is larger than *max-connect-number*, only the specified number of APs can be upgraded simultaneously. After the specified number of APs are upgraded, the remaining APs are upgraded automatically until all APs are upgraded. The number of APs that are upgraded at a time cannot exceed the value of *max-connect-number*.

Precautions

An external FTP server can be used, which is recommended. The AC can also function as the FTP server.

- When an external FTP server is used, the maximum number of APs that can be upgraded simultaneously is the configured *max-connect-number*.
- If an AC is used as the FTP server, a maximum of five APs can be upgraded simultaneously even if the specified number is larger than five.

  When the AC functions as the FTP server, run the **ap update ftp-server max-connect-number** *max-connect-number* command to set the maximum number of APs that can be upgraded simultaneously. The value of *max-connect-number* is an integer ranging from 1 to 5. During the upgrade, a maximum of 1 to 5 APs can be upgraded at a time until all APs are upgraded.

  If the configured number of APs to be upgraded simultaneously is larger than five, an error message will be displayed after the first five APs are upgraded. The remaining APs cannot be automatically upgraded. You have to repeat the command until all APs are upgraded.

If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.

Example

Set the maximum number of APs that can be upgraded simultaneously in FTP mode to 10.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update ftp-server max-connect-number 10
```

11.2.14 ap update load

Function

The **ap update load** command upgrades a specified AP.

The **undo ap update load** command cancels AP upgrade.

Format

ap update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name*

undo ap update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP to be upgraded.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP to be upgraded.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP to be upgraded.	The AP ID must already exist.
update-filename *update-file-name*	Specifies the AP upgrade file.	The upgrade file name must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in batches based on AP types, if the new version fails, the version rollback takes a long period. Therefore, you can upgrade a single AP to check whether faults occur on the version, ensuring successful upgrades in batches.

Prerequisites

When the AC mode is used, the AP upgrade file has been uploaded to the AC. If the FTP or SFTP mode is used, the AP upgrade file has been uploaded to the FTP server or SFTP server.

The AP is in normal or vmiss state.

Follow-up Procedure

Run the **ap update reset** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } command to restart the AP to make the upgrade take effect.

Precautions

The **undo ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } command cancels AP upgrade. However, if the AP system software has been written to the flash memory during the upgrade, the command does not take effect. You can run the **display ap update status** { **ap-name** *ap-name* | **ap-id** *ap-id* } command to check AP upgrade progress.

Example

Upgrade the AP **N1-2** using the upgrade file **AirEngineX760-V200R021C10.cc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update load ap-name N1-2 update-filename AirEngineX760-V200R021C10.cc
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

11.2.15 ap update mode

Function

The **ap update mode** command configures the AP upgrade mode.

The **undo ap update mode** command restores the default AP upgrade mode.

The default upgrade mode is **ac-mode**.

Format

ap update mode { **ftp-mode** | **ac-mode** | **sftp-mode** }

undo ap update mode

Parameters

Parameter	Description	Value
ac-mode	Indicates the AP upgrade mode in which APs download the upgrade version file from the AC.	-
ftp-mode	Indicates the FTP mode. The AC delivers the FTP configuration to APs using the **ap update ftp-server** command, and APs download the upgrade version file from the FTP server.	-
sftp-mode	Indicates the SFTP mode. The AC delivers the SFTP configuration to APs using the **ap update sftp-server** command, and APs download the upgrade version file from the SFTP server.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

- The AC, FTP, or SFTP upgrade mode must be preset on the AP for automatic upgrade and online upgrade.
- Subsequently, you can run the **ap update multi-load** command to upgrade APs in batches.

NOTE

SFTP is recommended because it is more secure than FTP.

Example

Set the AP upgrade mode to **sftp-mode**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update mode sftp-mode
```

11.2.16 ap update multi-load

Function

The **ap update multi-load** command upgrades APs in batches.

The **undo ap update multi-load** command cancels batch upgrade of APs.

Format

ap update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

ap update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

undo ap update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

undo ap update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to .
ap-group *group-name*	Specifies an AP group.	The AP group must exist.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ap update multi-load ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] command to upgrade APs of the same type in batches in the online upgrade mode.

- If **ap-group** *group-name* is specified, only APs of the same type and in the specified AP group are upgraded.
- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs of the specified type and with the specified AP name or AP ID are upgraded
- If none of the **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* parameters are specified, all APs of the specified type are upgraded.

- If the type of APs specified by **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from **ap-type** *type-id*, the APs cannot be upgraded.

You can run the **ap update multi-load ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] command to batch upgrade APs in the specified AP group online.

- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs with the specified name or ID in the specified AP group are upgraded.
- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are upgraded.
- If APs specified by **ap-name** *ap-name* and **ap-id** *ap-id* are in different AP groups, the APs cannot be upgraded.

Prerequisites

AP upgrade files have been configured in batches using the **ap update update-filename** command.

Follow-up Procedure

Run the **ap update multi-reset** command to reset APs in batches to make AP upgrade take effect.

Precautions

The **undo ap update multi-load** command cancels batch upgrade of APs. However, if the AP system software has been written to the flash memory during the upgrade, the command does not take effect. You can run the **display ap update status all** command to check AP upgrade progress.

Example

Upgrade APs with **type-id** 56 in batches online.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-load ap-type 56
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

Upgrade all APs in the AP group **group1** in batches online.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-load ap-group group1
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]:y
```

11.2.17 ap update multi-reset

Function

The **ap update multi-reset** command resets APs in batches.

The **undo ap update multi-reset partition** command cancels the AP reset by channel-based partition.

Format

ap update multi-reset ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

ap update multi-reset ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

ap update multi-reset { **partition** { **all** | **partition-id** *partition-id* } | **ap-id** *ap-id* } [**primary-access** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }]

undo ap update multi-reset partition

Parameters

Parameter	Description	Value
ap-type *type-id*	Resets APs of the specified type ID.	The AP type ID must exist.
ap-group *group-name*	Resets APs in the specified AP group.	The AP group must exist.
ap-name *ap-name*	Resets the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Resets the AP with a specified ID.	The AP ID must exist.
partition all	Resets APs in all channel-based partitions.	-
partition partition-id *partition-id*	Resets APs in the specified channel-based partition.	The value is an integer that ranges from 0 to 255.
primary-access ipv4 *ipv4-address*	Specifies the IPv4 address of the AC with which APs re-establish links after the APs are reset.	The value is in dotted decimal notation.
primary-access ipv6 *ipv6-address*	Specifies the IPv6 address of the AC with which APs re-establish links after the APs are reset.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

This command resets APs in batches and can be used only after APs are upgraded in batches.

Run the **ap update multi-reset ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] command to batch reset APs of the specified type online.

- If **ap-group** *group-name* is specified, only APs of the specified type and in the specified AP group are reset.
- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs of the specified type and with the specified AP name or ID are reset.
- If none of the **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* parameters are specified, all APs of the specified type are reset.
- If the type of APs specified by **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from **ap-type** *type-id*, the APs cannot be reset.

You can run the **ap update multi-reset ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] command to batch reset APs in the specified AP group online.

- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs with the specified name or ID in the specified AP group are reset.
- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are reset.
- If APs specified by **ap-name** *ap-name* or **ap-id** *ap-id* are not in the AP group specified by **ap-group** *group-name*, the APs cannot be reset.

The **ap update multi-reset** { **partition** { **all** | **partition-id** *partition-id* } | **ap-id** *ap-id* } [**primary-access** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }] command is used to reset APs in a specified channel-based partition in batches. To perform an in-service upgrade for all APs on the entire network, you can divide APs into different partitions based on channels and reset the APs by partition in sequence after loading the target version files to all APs. This prevents network service interruption caused by resetting a large number of APs. When APs are reset by partition, surrounding APs automatically fill coverage holes to ensure service continuity. For service continuity, ensure that at least two APs are deployed in one place.

In dual-AC scenarios, when APs are upgraded by channel-based partition, you can specify the IP address of the AC with which APs re-establish links after the APs are reset.

If an upgrade exception occurs when the **ap update multi-reset partition all** command is used to reset all RUs by channel-based partition, you can run the **undo ap update multi-reset partition** command to cancel the subsequent RU reset by channel-based partition.

Example

Reset APs with **type-id** 56 in batches.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update multi-reset ap-type 56
Warning: Reset the APs in batches to make the upgrade take effect. Continue? [Y/N]:y
```

11.2.18 ap update reset

Function

The **ap update reset** command restarts a specified AP after it is upgraded.

Format

ap update reset { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP to be restarted.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP to be restarted.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP to be restarted.	The AP ID must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an AP has been upgraded, run the **ap update reset** command to restart it to make the AP upgrade take effect.

Prerequisites

The AP is in normal or vmiss state.

The **ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name* command has been executed to upgrade a specified AP, and the **display ap update status** command has been executed to verify that **Update Status** of the specified AP is **succeed(need reset)**.

Example

Restart AP **N1-2** after the upgrade.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap update load ap-name N1-2 update-filename AirEngineX760-V200R021C10.cc
[HUAWEI-wlan-view] ap update reset ap-name N1-2
```

11.2.19 ap update sftp-server

Function

The **ap update sftp-server** command configures basic SFTP information, including the IP address, user name, and password of the SFTP server.

The **undo ap update sftp-server** command restores default SFTP settings.

By default, no basic SFTP information is configured.

Format

ap update sftp-server ip-address *server-ip-address* [**port** *port*] **sftp-username** *sftp-username* **sftp-password cipher** *sftp-password*

undo ap update sftp-server ip-address

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the SFTP server.	The value is in dotted decimal notation.
port *port*	Specifies a port number for the SFTP server. If no port number is specified, the default port 22 is used.	The value is an integer that ranges from 1 to 65535.
sftp-username *sftp-username*	Specifies the user name for logging in to the SFTP server.	The value is a string of 1 to 31 characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (") or spaces.
sftp-password	Specifies the password for logging in to the SFTP server.	-
cipher	Specifies the password in ciphertext.	-

Parameter	Description	Value
sftp-password	Specifies the SFTP server password.	The value is a string of characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (") or spaces. *sftp-password* can be a string of 1 to 188 characters in ciphertext, such as **%^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#**, or a string of 1 to 128 characters in plaintext, such as **YsHsjx_202206**.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- The SFTP configuration is used when the automatic upgrade and online upgrade modes are SFTP. In the automatic upgrade or online upgrade, the AC sends basic SFTP information to the AP, and the AP requests the SFTP server for upgrade based on SFTP information.
- After running the **ap update sftp-server** command, you can perform the following operations:
  a. Run the **ap update mode** command to set the upgrade mode to sftp-mode.
  b. Run the **ap update multi-load** command to upgrade APs in batches.

Precautions

- It is recommended that you use an external SFTP server to upgrade APs. If the AC functions as the SFTP server, a maximum of five APs can be upgraded simultaneously. If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.

- APs do not support the double quotation marks ("). Ensure that the SFTP server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, the SFTP upgrade fails.
- When the SFTP port number is specified, the upgrade is applicable only to APs in V200R020C10 and later. If the source version of APs is earlier than V200R020C10, the SFTP upgrade fails.

Example

Configure the IP address, user name, and password of the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update sftp-server ip-address 192.168.1.100 sftp-username admin sftp-password cipher YsHsjx_202206
```

11.2.20 ap update sftp-server max-connect-number

Function

The **ap update sftp-server** command configures the maximum number of APs that can be upgraded simultaneously in SFTP mode.

The **undo ap update sftp-server** command restores the default maximum number of APs that can be upgraded simultaneously in SFTP mode.

By default, a maximum of 50 APs can be upgraded simultaneously in SFTP mode.

Format

ap update sftp-server max-connect-number *max-connect-number*

undo ap update sftp-server max-connect-number

Parameters

Parameter	Description	Value
max-connect-number	Specifies the maximum number of APs that can be upgraded simultaneously.	The value is an integer that ranges from 1 to 64.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in SFTP mode, you can configure the value of *max-connect-number* to change the maximum number of APs that can be upgraded simultaneously.

- If the number of APs to be upgraded is equal to or smaller than *max-connect-number*, all APs can be upgraded simultaneously.
- If the number of APs to be upgraded is larger than *max-connect-number*, only the specified number of APs can be upgraded simultaneously. After the specified number of APs are upgraded, the remaining APs are upgraded automatically until all APs are upgraded. The number of APs that are upgraded at a time cannot exceed the value of *max-connect-number*.

Precautions

An external SFTP server can be used, which is recommended. The AC can also function as the SFTP server.

- When an external SFTP server is used, the maximum number of APs that can be upgraded simultaneously is the configured *max-connect-number*.
- When an AC is used as the SFTP server, a maximum of five APs can be upgraded simultaneously even if the specified number of APs to be upgraded is larger than five.

  When the AC functions as the SFTP server, run the **ap update sftp-server max-connect-number** *max-connect-number* command to set the maximum number of APs that can be upgraded simultaneously. The value of *max-connect-number* is an integer ranging from 1 to 5. During the upgrade, a maximum of 1 to 5 APs can be upgraded at a time until all APs are upgraded.

  If *max-connect-number* is set larger than 5, an error message will be displayed after the first five APs are upgraded. The remaining APs cannot be automatically upgraded. You have to repeat the command until all APs are upgraded.

  If there are *n* login VTY users, the maximum number of APs that can be upgraded simultaneously is subtracted by *n* - 1.

Example

Set the maximum number of APs that can be upgraded simultaneously in SFTP mode to 10.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update sftp-server max-connect-number 10
```

11.2.21 ap update update-filename

Function

The **ap update update-filename** command configures the upgrade file name for APs of a specified type.

The **undo ap update update-filename** command deletes the upgrade file name for APs of a specified type.

Format

ap update update-filename *filename* **ap-type** *type-id* [**ap-group** *ap-group-name*]

undo ap update update-filename ap-type *type-id* [**ap-group** *ap-group-name*]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to .
filename	Specifies the AP upgrade file name.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual upgrade file name and has an extension.
ap-group *ap-group-name*	Specifies an AP group.	The AP group must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

If you specify **ap-group** *ap-group-name*, the command configures the upgrade file name only for APs of the specified type and in the specified group. The upgrade file name configured for an AP group takes precedence over that configured without an AP group specified if they are different. To cancel the upgrade file name configuration of the AP group, specify the AP group name using the parameter **ap-group** *ap-group-name* when running the **undo** command.

Run the **ap update multi-load ap-type** command to upgrade APs of the same type in batches.

Example

Set the upgrade file name for APs with the type ID 127 to **AirEngineX760-V200R021C10.cc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap update update-filename AirEngineX760-V200R021C10.cc ap-type 127
Warning: If an AP is performing the automatic upgrade, the AP will be upgraded to the latest version.
Continue?[Y/N]:y
Warning: If AP update mode is AC-mode, update-file's default path is flash:/. Continue?[Y/N]:y
```

11.2.22 ap update schedule-task

Function

The **ap update schedule-task** command configures a scheduled AP upgrade task.

The **undo ap update schedule-task** command deletes a scheduled AP upgrade task.

By default, no scheduled AP upgrade task is configured.

Format

ap update schedule-task task-id *task-id* **start-time** *start-time start-date* **stop-time** *stop-time stop-date* **ap-type** *type-id* [**ap-group** *group-name* | { { **ap-name** *ap-name* } &<1-10> } | { { **ap-id** *ap-id* } &<1-10> }]

ap update schedule-task task-id *task-id* **start-time** *start-time start-date* **stop-time** *stop-time stop-date* **ap-group** *group-name*

undo ap update schedule-task { **all** | **task-id** *task-id* }

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a scheduled AP upgrade task.	The value is an integer that ranges from 0 to 31.
start-time *start-time*	Specifies the start time of the scheduled AP upgrade task.	The value is in HH:MM format, ranging from 00:00 to 23:59.
start-date	Specifies the start date of the scheduled AP upgrade task.	The value is in YYYY/MM/DD format, ranging from 2000-01-01 to 2050-12-31.
stop-time *stop-time*	Specifies the end time of the scheduled AP upgrade task.	The value is in HH:MM format, ranging from 00:00 to 23:59.

Parameter	Description	Value
stop-date	Specifies the end date of the scheduled AP upgrade task.	The value is in YYYY/MM/DD format, ranging from 2000-01-01 to 2050-12-31. *stop-time stop-date* must be later than *start-time start-date*.
ap-type *type-id*	Specifies an AP type ID.	The value is an integer. To view all AP types, run the **display ap-type all** command.
ap-group *group-name*	Specifies an AP group name.	The value is a string of 1 to 35 characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?) or slashes (/), and cannot start or end with spaces or double quotation marks (" "). If the AP group name contains spaces, the input name must start and end with a quotation mark ("), for example, **"hello name1"**. The quotation marks at the beginning and end of the AP group name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
ap-id *ap-id*	Specifies an AP ID.	The value is an integer. The value range depends on the actual device.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure a scheduled AP upgrade task to upgrade APs in a specified time period, such as off-peak hours.

If you specify **ap-group** *group-name* in the command, the configured task will upgrade only APs in the specified AP group. Similarly, if you specify **ap-type** *type-id*, **ap-name** *ap-name*, or **ap-id** *ap-id*, the configured task will upgrade only the specified APs.

The scheduled task configuration will not be automatically deleted after a scheduled upgrade task is completed. To delete the task, run the **undo ap update schedule-task** { **all** | **task-id** *task-id* } command.

Prerequisites

The AP upgrade file has been specified using the **ap update update-filename** command.

Configuration Impact

After scheduled upgrade tasks are configured, automatic upgrade cannot be performed if not all tasks are in the DONE, OVERTIME, or DEAD state. To perform automatic upgrade, you need to delete the scheduled upgrade tasks not in DONE, OVERTIME, or DEAD state. To check the status of scheduled AP upgrade tasks, run the **display ap update schedule-task** command.

Precautions

- For scheduled AP upgrade tasks with the same start time, the task with a smaller **task-id** *task-id* is executed preferentially.
- During the scheduled AP upgrade, if the time for task B is reached before task A is completed, task B waits until task A is completed. Subsequent scheduled AP upgrade tasks wait in sequence until the previous task is completed.
- When the time specified by **stop-time** *stop-time stop-date* is reached, ongoing upgrade tasks continue until the upgrade is completed and those tasks waiting in queues stop.
- After APs in a scheduled upgrade task are all upgraded, the APs automatically restart. The APs that fail the upgrade do not restart.
- After a scheduled AP upgrade task is configured, if the AP group or all APs are deleted, the task fails to be executed, which is not recorded as upgrade failure information.
- If an AP is performing the automatic upgrade when you configure a scheduled AP upgrade task, the upgrade continues until the upgrade is completed. APs that have not started the automatic upgrade will not execute the automatic upgrade.
- If the system time is changed after you configure a scheduled AP upgrade task, the following impacts may be caused:
  - If the system time is changed **before** the scheduled AP upgrade task starts, the start time and end time of the scheduled AP upgrade task are subject to the system time **after** the change. For example, the current system time is 1:00, and the start time and end time of the scheduled AP upgrade task are 3:00 and 4:00 respectively. When the system time is changed to 2:00 at 1:05, the start time and end time of the scheduled AP upgrade task are still 3:00 and 4:00 respectively.
  - If the system time is changed **after** the scheduled AP upgrade task starts, the start time and end time of the scheduled AP upgrade task are subject to the system time **before** the change.

Example

Configure APs with **ap-type** as **54** to perform the scheduled upgrade from 01:00 to 04:00 on May 20, 2018.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap update schedule-task task-id 1 start-time 1:00 2018/5/20 stop-time 4:00
2018/5/20 ap-type 54
```

11.2.23 ap username

Function

The **ap username** command sets the user name and password for AP login.

By default, no user name or password is configured for AP login.

Format

ap username *username* **password cipher**

Parameters

Parameter	Description	Value
username	Specifies the user name for AP login.	The value is a string of 4 to 31 characters. It can contain letters, underscores, and digits, and must start with a letter.
password	Specifies the password for AP login.	-

Parameter	Description	Value
cipher	Indicates the ciphertext password.	The password can be entered in plaintext or ciphertext: ● In plaintext, the password is a string of 8 to 128 case-sensitive characters. It must contain at least three of the following types: uppercase letters, lowercase letters, digits, and special characters, without question marks (?). ● In ciphertext, the password is a string of 48 to 188 characters. It must contain at least the following types: uppercase letters, lowercase letters, digits, and special characters.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

You can run this command to change the user name and password for logging in to an AP. If the user name and password of the AP have not been configured, you must configure them first in order to log in to the AP.

Running this command will disconnect the administrator who is logging in to the AP.

NOTE

It is recommended that you change the user name and password in a timely manner to ensure device security.

The password cannot be the same as the user name or the mirror user name.

Example

Set the user name to **example** and password to **Zz123456**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap username example password cipher
Warning: This operation will disconnect administrator users logging in to the AP, Continue? [Y/N]:y
Enter the password (plain-text password of 8-128 characters or cipher-text password of 48-188 characters
that must be a combination
of at least three of the following: lowercase letters a to z, uppercase letters A to Z, digits, and special
characters):
Confirm password:
```

11.2.24 ap-group

Function

The **ap-group** command creates an AP group and displays the AP group view, or displays the view of an existing AP group.

The **undo ap-group** command deletes an AP group.

By default, the system provides the AP group **default**.

Format

ap-group name *group-name*

undo ap-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of an AP group.	The value is a string of 1 to 35 characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?) or slashes (/), and cannot start or end with spaces or double quotation marks (" "). If the AP group name contains spaces, the input name must start and end with a quotation mark ("), for example, **"hello name1"**. The quotation marks at the beginning and end of the AP group name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
all	Deletes all AP groups. **NOTE** This configuration does not delete the AP group **default** or any AP group that has APs in it.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same configuration on multiple APs, add the APs to an AP group and perform the configuration in the AP group. The configuration takes effect on all APs of the group. This prevents repetitive configuration.

Follow-up Procedure

Run the **ap-group (AP view)** or **ap-regroup** command to add APs to an AP group.

Precautions

- If the configuration of an AP in the AP view is different from that in the AP group view, the configuration in the AP view is preferentially used.
- The device supports a maximum of 256 AP groups.
- The AP group that has APs cannot be deleted. The AP group **default** cannot be deleted either.
- By default, an AP group has the following profiles bound: AP system profile **default**, 2G radio profile **default**, 5G radio profile **default**, regulatory domain profile **default**, WIDS profile **default**, and AP wired port profile **default**.

Example

Create the AP group **group1** and display the AP group view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1]
```

11.2.25 ap-group (AP view)

Function

The **ap-group** command configures an AP group.

The **undo ap-group** command restores the default AP group.

By default, no AP group is configured.

Format

ap-group *ap-group*

undo ap-group

Parameters

Parameter	Description	Value
ap-group	Specifies an AP group.	The AP group must exist.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same configuration on multiple APs, add the APs to an AP group and perform the configuration in the AP group. The configuration takes effect on all APs of the group. This prevents you from configuring each AP one by one.

Each AP must be added to an AP group. If no AP group is configured for an AP, the AP automatically joins the AP group **default**.

Example

Configure the AP group **ap-new-group** for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] ap-group ap-new-group
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and
antenna gain configurations of the radio, Whether to continue? [Y/N]:y
```

11.2.26 ap-group all vap-profile

Function

The **ap-group all vap-profile** command binds a VAP profile to all AP groups.

The **undo ap-group all vap-profile** command unbinds a VAP profile from all AP groups.

By default, no VAP profile is bound to radios of an AP group.

Format

ap-group all vap-profile *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** }

undo ap-group all vap-profile wlan *wlan-id* **radio** { *radio-id* | **all** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a VAP profile.	The value must be the name of an existing VAP profile.

Parameter	Description	Value
wlan *wlan-id*	Specifies a VAP ID.	The value is an integer that ranges from 1 to 16. **NOTE** - The WLAN ID for the WDS service can be 13 or 14. - The WLAN ID for the Mesh service is 16. - The WLAN ID for the offline management VAP configuration is 15 or an integer that ranges from 1 to 12. - For some AP models, the maximum number of VAPs supported by each radio is less than 16. If the value of *wlan-id* exceeds the AP specifications, the configuration cannot take effect and the AP cannot generate radio signals.
radio *radio-id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: - AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 - AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T - AirEngine 8771-X1T
radio all	Specifies all radios.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-group all vap-profile** command to bind a VAP profile to all AP groups.

Example

Bind the VAP profile **office01** to all AP groups.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group all vap-profile office01 wlan 1 radio 0
Info: This operation may take a few seconds, please wait.......done.
Warning: This operation is to bind the profile to 4 AP groups. Success count: 3. Failure count: 1. The failure
```

```
causes are as follows:
--------------------------------------------------------------------------------------------------------------------------
AP group                          Config fail reason
--------------------------------------------------------------------------------------------------------------------------
default                          The WLAN ID on the radio is in use. Please use an unassigned WLAN ID.
--------------------------------------------------------------------------------------------------------------------------
```

Table 11-66 Description of the **ap-group all vap-profile** command output

Item	Description
AP group	AP group to which the VAP profile fails to be bound.
Config fail reason	Binding failure cause.

11.2.27 ap-group all wids-profile

Function

The **ap-group all wids-profile** command binds a WIDS profile to all AP groups.

The **undo ap-group all wids-profile** command unbinds a WIDS profile from all AP groups.

By default, the WIDS profile **default** is bound to an AP group.

Format

ap-group all wids-profile *profile-name*

undo ap-group all wids-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a WIDS profile.	The value must be the name of an existing WIDS profile.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-group all wids-profile** command to bind a WIDS profile to all AP groups.

Example

Bind the WIDS profile **office01** to all AP groups.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group all wids-profile office01
```

11.2.28 ap-group all wired-port-profile

Function

The **ap-group all wired-port-profile** command binds an AP wired port profile to all AP groups.

The **undo ap-group all wired-port-profile** command unbinds an AP wired port profile from all AP groups.

By default, the AP wired port profile **default** is bound to an AP group.

Format

ap-group all wired-port-profile *profile-name interface-type interface-number*

undo ap-group all wired-port-profile *interface-type interface-number*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The value must be the name of an existing AP wired port profile.
interface-type interface-number	Specifies the type and number of an AP's wired interface.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-group all wired-port-profile** command to bind an AP wired port profile to all AP groups.

Example

Bind the AP wired port profile **office01** to all AP groups.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group all wired-port-profile office01 gigabitethernet 0
```

11.2.29 ap-mode

Function

The **ap-mode** command sets the working mode of an AP.

The **undo ap-mode** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, the working mode of an AP is not specified in the AP provisioning view.

Format

ap-mode { **fat** | **cloud** | **fit** }

undo ap-mode

Parameters

Parameter	Description	Value
fat	Specifies the Fat mode.	-
cloud	Specifies the cloud mode.	-
fit	Specifies the Fit mode.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The working mode of an AP is configured on the AC and delivered to the AP. After a restart, the AP will switch the working mode accordingly.

Prerequisites

- The AP has gone online on the AC in Fit mode.
- Corresponding system files have been uploaded to the AC, FTP server, or SFTP server.

Follow-up Procedure

Run the **commit** command to commit the configuration.

In V200R023C00 or a later version: To switch the working mode of a Fit AP, run the **undo ap** (WLAN view) command on the to delete the Fit AP from the before the restart is complete. If the Fit AP is not deleted, the AP may switch back to the Fit mode in accordance with the foolproof mechanism after the restart is complete.

Configuration Impact

After the working mode of the AP is switched to Fat or cloud, the AP will be out of control by the AC.

NOTICE

This command is supported only by the following models:

- AirEngine series APs (excluding RUs) (The AirEngine 8771-X1T supports only the Fit and cloud modes.)
- AirEngine series central APs

Example

Set the working mode of an AP to Fat.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ap-mode fat
Warning: When the configuration is committed, the AP mode will be switched if supported and the AP will
be out of control by the AC.Continue?[Y/N]: y
```

11.2.30 ap-name

Function

The **ap-name** command displays the AP view.

Format

ap-name *ap-name*

Parameters

Parameter	Description	Value
ap-name	Specifies the AP name.	The AP name must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After entering the AP view, you can perform personalized configuration on an AP.

Example

Display the view of the AP named **area_1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-name area_1
[HUAWEI-wlan-ap-2]
```

11.2.31 ap-name (AP provisioning view)

Function

The **ap-name** command sets the name of an AP.

The **undo ap-name** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, no AP name is configured.

Format

ap-name *ap-new-name*

undo ap-name

Parameters

Parameter	Description	Value
ap-new-name	Specifies an AP name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the name of an AP is changed and the change is delivered to the AP, the AP goes online using the new name.

Precautions

The new AP name cannot be the same as the existing AP name.

If the AP name is not configured, the default name of an AP is the AP's MAC address after the AP goes online.

Follow-up Procedure

Run the **commit** command to deliver the configuration to the AP.

Example

Change the AP name to **AP-N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] ap-name AP-N1-2
```

11.2.32 ap-name (AP view)

Function

The **ap-name** command configures an AP name.

The **undo ap-name** command restores the default AP name.

By default, no AP name is configured for an AP.

Format

ap-name *ap-name*

undo ap-name

Parameters

Parameter	Description	Value
ap-name	Specifies an AP name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate AP maintenance, management, and differentiation, you can name the AP according to actual situations.

Precautions

The new AP name cannot be the same as the existing AP name.

The new AP name cannot be the same as the MAC address of an existing AP. Otherwise, the AP name will be lost after the device saves the configuration and restarts.

If a new AP name is the same as an existing AP name, the new AP is restarted after its name is changed.

If the AP name is not configured, the default name of an AP is the AP's MAC address after the AP goes online.

Example

Change the AP name to **AP-N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] ap-name AP-N1-2
```

```
Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than
V200R009C00.
Warning: This operation may cause AP reset. Continue? [Y/N]:y
```

11.2.33 ap password policy

Function

The **ap password policy** command enables the AP login password policy function and displays the AP password policy view.

The **undo ap password policy** command disables the AP login password policy function.

By default, the AP login password policy function is disabled.

Format

ap password policy

undo ap password policy

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a password is configured using the **ap username** command, the minimum length and complexity of the password are limited. If you want to improve password security, you can run the following commands to configure a password policy for the local administrator:

- Run the **password expire** command to set the password expiration time.
- Run the **password alert before-expire** command to set the password expiration prompt days.
- Run the **password alert original** command to enable the device to prompt users to change initial passwords.
- Run the **password history record number** command to set the maximum number of historical passwords recorded for each user.

Precautions

Running the **undo ap password policy** command invalidates the password policy, posing security risks.

Example

Enable the AP login password policy function and display the AP password policy view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy]
```

11.2.34 ap-patch update load

Function

The **ap-patch update load** command loads a patch for a specified AP.

The **undo ap-patch update load** command cancels a patch upgrade from a specified AP.

Format

ap-patch update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name* [**next-startup**]

undo ap-patch update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-mac *ap-mac*	Specifies the AP's MAC address.	The specified AP's MAC address must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
update-filename *update-file-name*	Specifies the name of an AP patch file.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual patch file name, with a file name extension of .pat.
next-startup	Specifies the patch for next startup.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you load the patch for multiple APs of a specified type, a version exception will lead to a long-time patch uninstallation. In this case, before loading the patch in a batch, you can load the patch for a single AP for testing, helping detect any exception in advance and ensuring the success of subsequent batch patch loading.

If the parameter **next-startup** is specified, the patch is loaded upon next startup. If this parameter is not specified, the patch is loaded immediately and is also used for next startup.

Precautions

If the AC or AP version is earlier than V200R021C10, the patch is uninstalled when you run the **undo ap-patch update load** command to cancel the AP patch upgrade. Running this command cancels the AP patch upgrade but does not uninstall the patch only when both the AC and AP versions are V200R021C10 or later. In this case, to uninstall the patch, run the **ap-patch delete** command.

Prerequisites

In AC upgrade mode, the AP's patch file has been uploaded to the AC. In FTP or SFTP upgrade mode, the AP's patch file has been uploaded to an FTP or SFTP server.

Follow-up Procedure

Run the **display ap update status** command to check the patch loading progress.

Example

Load the patch **AirEngineX760_V200R019C10.pat** for the AP named **N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update load ap-name N1-2 update-filename
AirEngineX760_V200R019C10.pat
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]: y
```

11.2.35 ap-patch update multi-load

Function

The **ap-patch update multi-load** command batch loads the patch for APs.

The **undo ap-patch update multi-load** command cancels AP patch upgrades in batches.

Format

ap-patch update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] [**next-startup**]

ap-patch update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] [**next-startup**]

undo ap-patch update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

undo ap-patch update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies an AP type ID.	The AP type ID must exist.
ap-group *group-name*	Specifies an AP group.	The AP group must exist.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
next-startup	Specifies the patch for next startup.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ap-patch update multi-load ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] [**next-startup**] command to batch load the patch for APs by type.

- When the parameter **ap-group** *group-name* is specified, the patch is loaded only for APs of a specified type in a specified AP group.
- When the parameter **ap-name** *ap-name* or **ap-id** *ap-id* is specified, the patch is loaded only for APs of a specified type that have specified names or IDs.
- When the parameters **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* are not specified, the patch is loaded for all APs of a specified type.

- When the parameter **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from the specified **ap-type** *type-id*, the patch is not loaded.
- If the parameter **next-startup** is specified, the patch is loaded upon next startup. If this parameter is not specified, the patch is loaded immediately and is also used for next startup.

You can run the **ap-patch update multi-load ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] [**next-startup**] command to batch load the patch for APs by AP group.

- When the parameter **ap-name** *ap-name* or **ap-id** *ap-id* is specified, the patch is loaded only for APs in a specified group that have specified names or IDs.
- When the parameters **ap-name** *ap-name* and **ap-id** *ap-id* are not specified, the patch is loaded for all APs in a specified group.
- When the AP group to which an AP specified by **ap-name** *ap-name* or **ap-id** *ap-id* is different from the specified AP group, the patch is not loaded for the AP.
- If the parameter **next-startup** is specified, the patch is loaded upon next startup. If this parameter is not specified, the patch is loaded immediately and is also used for next startup.

Precautions

If the AC or AP version is earlier than V200R021C10, the patch is uninstalled when you run the **undo ap-patch update multi-load** command to cancel the AP patch upgrade. Running this command cancels the AP patch upgrade but does not uninstall the patch only when both the AC and AP versions are V200R021C10 or later. In this case, to uninstall the patch, run the **ap-patch delete** command.

Prerequisites

The patch file for batch loading has been configured using the **ap-patch update update-filename** command.

Follow-up Procedure

Run the **display ap update status** command to check the patch loading progress.

Example

Load the patch for all APs with the **type-id** of 56.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update multi-load ap-type 56
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]: y
```

Load the patch for all APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update multi-load ap-group group1
Info: The current upgrade mode is AC mode, which may affect performance and take a long time. The FTP
or SFTP upgrade mode is recommended. Continue? [Y/N]: y
```

11.2.36 ap-patch update update-filename

Function

The **ap-patch update update-filename** command specifies the patch file name for APs of a specified type.

The **undo ap-patch update update-filename** command cancels the patch file name configured for APs of a specified type.

Format

ap-patch update update-filename *filename* **ap-type** *type-id* [**ap-group** *ap-group-name*]

undo ap-patch update update-filename ap-type *type-id* [**ap-group** *ap-group-name*]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies an AP type ID.	The AP type ID must exist.
filename	Specifies the name of a patch file.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual patch file name, with a file name extension of .pat.
ap-group *ap-group-name*	Specifies an AP group.	The AP group must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

After **ap-group** *ap-group-name* is specified, the patch file name is configured only for APs of a specified type in this AP group.

After configuring the AP patch file name, you can batch load the patch for APs of the same type using the **ap–patch update multi-load ap-type** command.

Example

Set the patch file name of APs with the type ID of 56 to **AirEngineX760_V200R019C10.pat**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-patch update update-filename AirEngineX760_V200R019C10.pat ap-type 56
Warning: If an AP is performing the automatic upgrade, the AP will be upgraded to the latest version. Continue?[Y/N]:y
```

11.2.37 ap-ping

Function

The **ap-ping** command uses a specified AP to ping a network device and displays the returned result.

Format

ap-ping { **ap-name** *ap-name* | **ap-id** *ap-id* } [**-c** *count* | **-s** *packetsize* | **-m** *time* | **-t** *timeout*] * *host*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP used to ping other network devices.	The AP name must already exist.
ap-id *ap-id*	Specifies the ID of an AP used to ping other network devices.	The AP ID must already exist.
-c *count*	Specifies the number of ICMP Echo Request packets to be sent.	The value is an integer that ranges from 1 to 10. The default value is 4.
-s *packetsize*	Specifies the length of an Echo Request packet excluding the IP header and ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56 bytes.
-m *time*	Specifies the time to wait before sending the next ICMP Request packet.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 2000 ms.

Parameter	Description	Value
-t *timeout*	Specifies the timeout period for an ICMP Echo Response packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The default value is 2000 ms.
host	Specifies the domain name or IP address of the destination host.	The value is a string of 1 to 20 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- You can run this command to check the connectivity between an AP and network device by pinging a network device from an AP.
- The prerequisite is that the AP is online and has been configured with an IP address.

Precautions

- This command may cost much time because the parameters such as waiting time affects the command running.
- Only one AP can perform the ping operation at a time.

Example

Use the AP **N1-2** to perform a ping operation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-ping ap-name N1-2 10.1.1.1
Warning: This operation maybe takes several minutes, continue?[Y/N]:y
[HUAWEI-wlan-view]
  AP ping result
    Success count         : 4
    Failure count         : 0
    Average response time: 1 ms
    Minimum response time: 1 ms
    Maximum response time: 1 ms
```

11.2.38 ap-pki-profile (WLAN view)

Function

The **ap-pki-profile** command creates an AP PKI realm profile and enters the AP PKI realm profile view, or enters the view of an existing AP PKI realm profile.

The **undo ap-pki-profile** command deletes an AP PKI realm profile.

By default, no AP PKI realm profile is created on the device.

Format

ap-pki-profile name *profile-name*

undo ap-pki-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of an AP PKI realm profile.	The value is a string of 1 to 35 case-sensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").
all	Specifies all AP PKI realm profiles to be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to create an AP PKI realm profile on the AC or enter the view of an existing AP PKI realm profile to configure the AP PKI realm, facilitating unified management and maintenance of AP certificates.

Follow-up Procedure

1. Run the **pki realm (AP PKI realm profile view)** command to configure an AP PKI realm and the CA certificate, local certificate, CRL file, and private key file to be bound to the realm.
2. Run the **ap-pki-profile (AP group view and AP view)** command to bind the AP PKI realm profile to an AP or AP group.
3. Run the **load-file (WLAN view)** command to manually load a certificate file in the AP PKI realm to an AP.

Example

Create an AP PKI realm profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-pki-profile name default
[HUAWEI-wlan-ap-pki-prof-default]
```

11.2.39 ap-pki-profile (AP group view and AP view)

Function

The **ap-pki-profile** command binds an AP PKI realm profile to an AP or AP group.

The **undo ap-pki-profile** command unbinds an AP PKI realm profile from an AP or AP group.

By default, no AP PKI realm profile is bound to an AP group or AP.

Format

ap-pki-profile *profile-name*

undo ap-pki-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of an AP PKI realm profile.	The value is a string of 1 to 35 case-sensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP PKI realm profile is created and an AP PKI realm is configured, you can run this command to bind the AP PKI realm profile to an AP or AP group.

Prerequisites

1. An AP PKI realm profile has been created using the **ap-pki-profile (WLAN view)** command.
2. An AP PKI realm and the CA certificate, local certificate, CRL file, and private key file to be bound to the realm have been configured using the **pki realm (AP PKI realm profile view)** command.

Follow-up Procedure

Run the **load-file (WLAN view)** command to manually load a certificate file in the AP PKI realm to an AP.

Example

Create an AP PKI realm profile **default** and bind it to the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-pki-profile name default
[HUAWEI-wlan-ap-pki-prof-default] quit
[HUAWEI-wlan-ap-group-group1] ap-pki-profile default
```

11.2.40 ap-regroup

Function

The **ap-regroup** command changes the group that an AP joins.

Format

ap-regroup { **ap-name** *ap-name* | **ap-id** *ap-id* } **new-group** *new-group-name*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist. The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) to separate AP IDs or use hyphens (-) to indicate continuous AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.
new-group *new-group-name*	Specifies the name of the new group to which the AP is added.	The AP group must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the current AP group is not applicable to an AP or the AP is added to an incorrect group, you can run this command to delete the AP from the current AP group and add the AP to a new AP group.

Prerequisites

The AP group has been created using the **ap-group** command.

Configuration Impact

Adding an AP to a new AP group will cause the AP to restart, interrupting services. Therefore, exercise caution when performing this operation.

Example

Change the group that an AP joins to the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] quit
[HUAWEI-wlan-view] ap-regroup ap-name 00e0-fc76-e360 new-group group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and
antenna gain configurations of the radio, Whether to continue? [Y/N]:y
```

11.2.41 ap-rename

Function

The **ap-rename** command changes the name of an AP.

Format

ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*

Parameters

Parameter	Description	Value
ap-name *name*	Specifies the old name of an AP.	The AP name must exist.
ap-mac *ap-mac-address*	Specifies the MAC address of an AP.	The AP's MAC address must exist.
ap-id *ap-id*	Specifies the ID of an AP.	The AP ID must exist.

Parameter	Description	Value
new-name *ap-new-name*	Specifies the new name of an AP.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If the name of an AP conflicts with that of another or an AP requires a more proper name, you can run this command to change the name of the AP.

If a new AP name is the same as an existing AP name, the new AP is restarted after its name is changed.

Example

Change the AP name from **N1-2** to **N2-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-rename ap-name N1-2 new-name N2-2
Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than
V200R009C00.
Warning: This operation may cause AP reset. Continue? [Y/N]:y
```

11.2.42 ap-reset

Function

The **ap-reset** command resets an AP.

Format

ap-reset { **all** | **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* | **ap-group** *ap-group* | **ap-type** { **type** *type-name* | **type-id** *type-id* } }

ap-reset wait-rtu-validate

Parameters

Parameter	Description	Value
all	Resets all APs.	-
ap-name *ap-name*	Resets the AP with the specified AP name.	The AP name must exist.
ap-mac *ap-mac*	Resets the AP with the specified MAC address.	The AP's MAC address must exist.
ap-id *ap-id*	Resets the AP with the specified AP ID.	The AP ID must exist. The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) to separate AP IDs or use hyphens (-) to indicate continuous AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.

Parameter	Description	Value
ap-group *ap-group*	Resets APs in the specified AP group.	The AP group must exist.
ap-type	Resets APs of the specified AP type.	-
type *type-name*	Resets APs of the specified type name.	The AP type name must exist.
type-id *type-id*	Resets APs of the specified type ID.	The AP type ID must exist.
wait-rtu-validate	Resets APs on which RTU licenses have been loaded but have not taken effect.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After in-service upgrade of APs is complete, you can run the **ap-reset** command to reset the APs. After the command is run, the APs restart with the upgraded software version. You can also use the command to restart APs for other reasons.

Prerequisites

An AP exists on the AC.

Example

Reset the AP **N1-2**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-reset ap-name N1-2
Warning: Reset AP(s), continue?[Y/N]:y
```

11.2.43 ap-system-profile (WLAN view)

Function

The **ap-system-profile** command creates an AP system profile and displays the AP system profile view, or displays the view of an existing AP system profile.

The **undo ap-system-profile** command deletes an AP system profile.

By default, the system provides the AP system profile **default**.

Format

ap-system-profile name *profile-name*

undo ap-system-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP system profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP system profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage and maintain multiple APs in a centralized manner, add the APs in an AP group, configure parameters in an AP system profile, and apply the AP system profile to the AP group.

To manage and maintain an AP independently, configure parameters in an AP system profile and apply the AP system profile to the AP specific profile.

Follow-up Procedure

Run the **ap-system-profile (AP group view and AP view)** command to bind the AP system profile to an AP or AP group so that the AP system profile can take effect.

Precautions

- The AP system profile **default** cannot be deleted.
- The AP system profile referenced by an AP or AP group cannot be deleted. To delete the AP system profile, unbind it from the AP or AP group first.

Example

Create the AP system profile **ap-system1** and display the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1]
```

11.2.44 ap-system-profile (AP group view and AP view)

Function

The **ap-system-profile** command binds an AP system profile to an AP or AP group.

The **undo ap-system-profile** command unbinds an AP system profile from an AP or AP group.

By default, the AP system profile **default** is bound to an AP group, but no AP system profile is bound to an AP.

Format

ap-system-profile *profile-name*

undo ap-system-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP system profile.	The AP system profile must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP system profile using the **ap-system-profile (WLAN view)** command, bind it to an AP or AP group so that the AP system profile can take effect.

Precautions

After an AP system profile is bound to an AP or AP group, parameter settings in the AP system profile apply to all APs using the profile.

Example

Create the AP system profile **ap-system1** and bind it to AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] ap-system-profile ap-system1
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.2.45 ap-type

Function

The **ap-type** command creates an AP type for a new AP model.

The **undo ap-type** command deletes a specified AP type.

Format

ap-type *type-description* **type-id** *type-id*

undo ap-type *type-description*

Parameters

Parameter	Description	Value
type-description	Describes an AP type.	The value is a string of 1 to 31 case-insensitive characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (" ").
type-id *type-id*	Specifies the ID of an AP type.	The value is an integer that ranges from 0 to .

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a new AP model to connect to an AC, you can run the **ap-type** command on the AC to create an AP type for this model. If you do not need the new AP model, you can run the **undo ap-type** command to delete the AP type of this model.

Precautions

In the **ap-type** command, ensure that the value of the *type-description* or *type-id* parameter does not conflict with the description or ID of an existing AP type. You can run the **display ap-type all** command to check existing AP types, including the default AP types that have been added during initialization and AP types that are created using commands.

Note the following points when using the **undo ap-type** command:

- The default AP types that are registered during initialization cannot be deleted.
- If configurations (for example, upgrade configurations) related to an AP type exist on the AC, this AP type cannot be deleted.

After the **ap-type** command is run to create an AP type for a new AP model, the new AP model is authorized to connect to an AC of an earlier version. However, if the connection process between the new AP model and AC is changed, the new AP model cannot connect to the AC.

Generally, you are not advised to run the **ap-type** command to create an AP type for a new model. If you want to create an AP type using this command, ensure that the mapping between *type-id* and *type-description* is configured correctly. Otherwise, the new AP model fails to connect to the AC. For the mapping between *type-id* and *type-description*, see the **AP Type Names and IDs** sheet in **Quick Reference for WLAN AP Version Mapping and Models**.

The AC does not support the type of a central AP and matching RUs running a later version.

Example

Create AP type **AP9530DN** with the ID **254** for a new AP model.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-type AP9530DN type-id 254
```

11.2.46 auto create ap-type

Function

The **auto create ap-type** command automatically imports AP types.

Format

auto create ap-type { **type-id** *type-id* | **type** *type-description* | **all** }

Parameters

Parameter	Description	Value
type-id *type-id*	Automatically imports the AP type with a specified ID.	The value is an integer that ranges from 0 to .
type *type-description*	Automatically imports the AP type with a specified description.	The value is a string of 1 to 31 characters. It cannot contain question marks (?), and cannot start or end with double quotation marks (" ").
all	Automatically imports the types of all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If a new AP model cannot connect to the AC, you can check whether the AP type has been created. To list the undefined AP types, run the **display ap-type undefined record** command. Then run the **auto create ap-type** command to automatically import the AP types of these APs.

The AC does not support the type of a central AP and matching RUs running a later version.

Example

Automatically import the types of all APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] auto create ap-type all
Info: 1 succeeded, 3 failed.
List of AP types that failed to be added:
------------------------------------------------------------------------------
AP type           Type ID     Reason
------------------------------------------------------------------------------
AP5010DN          29          This AP type already exists
AP6010DN          21          This type ID already exists
AP9910DN          133          Reached the maximum specifications of the AP type
------------------------------------------------------------------------------
Total : 3
```

Table 11-67 Description of the **ap-type auto create ap-type** command output

Item	Description
AP type	AP type.
Type ID	ID of an AP type.
Reason	Cause of the failure to automatically import an AP type, which can be: ● This AP type already exists ● This type ID already exists ● Reached the maximum specifications of the AP type

11.2.47 broadcast-suppression auto-detect (AP system profile view)

Function

The **broadcast-suppression auto-detect** command configures the rate limit for broadcast packets during intelligent flow control.

The **undo broadcast-suppression auto-detect** command restores the default rate limit for broadcast packets during intelligent flow control.

By default, the rate limit for broadcast packets is 256 pps.

NOTE

This function is not supported by the following models:

- AirEngine X760 series APs (excluding the AirEngine 5760-10)
- AirEngine 9700D-S (including matching ORUs)

Format

broadcast-suppression auto-detect packets *packets*

undo broadcast-suppression auto-detect

Parameters

Parameter	Description	Value
packets *packets*	Specifies the rate limit for broadcast packets.	The value is an integer that ranges from 64 to 1024, in pps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When there are a large number of broadcast, multicast, and unknown unicast packets, the CPU becomes busy processing these packets and the buffer of the packet for receiving incoming packets is occupied. When the buffer decreases to the specified threshold, the device automatically rate-limits the broadcast, multicast, and unknown unicast packets. You can run this command to specify the rate limit for intelligent flow control as required. Rate limiting takes effect only for incoming traffic.

Example

Set the rate limit for broadcast packets during intelligent flow control to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] broadcast-suppression auto-detect packets 300
```

11.2.48 capwap dtls server-auth (AP provisioning view)

Function

The **capwap dtls server-auth** { **enable** | **disable** } command enables or disables the AC authentication function for APs.

The **undo capwap dtls server-auth** command disables the device from modifying this parameter setting for APs after the configuration is delivered using the **commit** command.

By default, the AC authentication function for APs is disabled.

Format

capwap dtls server-auth { **enable** | **disable** }

undo capwap dtls server-auth

Parameters

Parameter	Description	Value
enable	Enables the AC authentication function for APs.	-

Parameter	Description	Value
disable	Disables the AC authentication function for APs.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP attempts to go online, it receives Discovery Response packets from ACs and discover an available AC. A bogus AC may maliciously send a Discovery Response packet to the AP, causing the AP to go online on the bogus AC.

After the AC authentication function for APs is enabled, an AP initiates DTLS authentication to the AC before establishing a CAPWAP tunnel with it. The AP then uses the DTLS PSK or initial certificate to authenticate the AC. The CAPWAP tunnel can be established only after the authentication succeeds.

Follow-up Procedure

Run the **commit** command to deliver the configuration to APs and restart the APs to make the configuration take effect.

Precautions

This function is available only for APs running V200R022C00 or later, but does not take effect for APs running versions earlier than V200R022C00.

Example

Enable the AC authentication function for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] capwap dtls server-auth enable
```

11.2.49 capwap dtls server-auth cn (AP provisioning view)

Function

The **capwap dtls server-auth cn** command specifies the CN field used by APs to verify an AC's certificate.

The **undo capwap dtls server-auth cn** *cn-string* command clears the CN field used by APs to verify an AC's certificate.

The **undo capwap dtls server-auth cn** command disables the device from modifying this parameter setting for APs after the configuration is delivered using the **commit** command.

By default, no CN field is specified for APs to verify an AC's certificate.

Format

capwap dtls server-auth cn *cn-string*

undo capwap dtls server-auth cn *cn-string*

undo capwap dtls server-auth cn

Parameters

Parameter	Description	Value
cn-string	Verifies the CN field in certificates based on the specified character string.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the AC authentication function for APs is enabled, an AP authenticates the AC based on the initial certificate if DTLS PSK authentication is unavailable or fails for three consecutive times. In this case, you can run this command to specify the CN field used by APs to verify an AC's certificate.

After this command is run, when an AP authenticates the AC based on the initial certificate, the AP verifies the CN field of the certificate based on the specified character string. This ensures that the AP can go online only on the specified AC, thereby enhancing network security.

Prerequisites

The AC authentication function for APs has been enabled using the **capwap dtls server-auth enable** command in the AP provisioning view.

By default, the AC authentication function for APs is disabled.

Follow-up Procedure

Run the **commit** command to deliver the configuration to APs and restart the APs to make the configuration take effect.

Precautions

This configuration applies only to the scenario the AC device replacement scenarios. Note the following when configuring CN fields:

- Ensure that the configured CN field is the same as that in the initial certificate of the AC in the **default** realm, and run this command with assistance from technical support personnel. Otherwise, the AP may fail to go online. To query the CN field in the initial certificate in the **default** realm, run the **display pki certificate local realm** *default* command.
- You can run this command multiple times, and a maximum of five CN fields are supported.
- Ensure that at least two CN fields are configured and the CN field list covers all possible ACs on which APs will go online. The APs cannot go online on the AC out of the CN field list.
- If only one CN field is configured, this function does not take effect.

Example

Configure the CN fields **123.example.com** and **456.example.com** used by APs to verify an AC's.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] capwap dtls server-auth cn 123.example.com
Warning: This operation will enable the AP to verify the CN field in AC certificates using DTLS. Ensure that
this field be set to the same as that in the AC certificates under the guidance of technical personnel.
Otherwise, the AP cannot go online. Continue? [Y/N]:y
Warning: Ensure that at least two CNs are configured for the AP to authenticate the AC. If a multi-AC
backup networking is used or the AC needs to be replaced, ensure that the CN fields in the certificates of all
ACs are configured on the AP. Otherwise, the AP cannot go online. Continue? [Y/N]:y
[HUAWEI-wlan-provision-ap] capwap dtls server-auth cn 456.example.com
Warning: This operation will enable the AP to verify the CN field in AC certificates using DTLS. Ensure that
this field be set to the same as that in the AC certificates under the guidance of technical personnel.
Otherwise, the AP cannot go online. Continue? [Y/N]:y
Warning: Ensure that at least two CNs are configured for the AP to authenticate the AC. If a multi-AC
backup networking is used or the AC needs to be replaced, ensure that the CN fields in the certificates of all
ACs are configured on the AP. Otherwise, the AP cannot go online. Continue? [Y/N]:y
```

11.2.50 channel-load-mode indoor

Function

The **channel-load-mode indoor** command sets the AP channel mode to indoor mode.

The **undo channel-load-mode indoor** command restores the default channel mode of APs.

The default channel mode of an AP is outdoor mode.

Format

channel-load-mode indoor

undo channel-load-mode indoor

Parameters

None

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

In scenarios where indoor and outdoor boundaries are unclear, such as subway and train platforms, it is recommended that outdoor APs be deployed. When a large volume of data is transmitted, outdoor APs in outdoor channel mode have no sufficient channels to meet data transmission requirements. In this case, you can run the **channel-load-mode indoor** command to set the channel mode of the APs to indoor mode, so that data can be transmitted on more channels.

Precautions

This command will cause an AP running V200R019C10 or earlier to automatically restart. Therefore, exercise caution when running this command.

This function is supported only by outdoor AP models.

Example

Set the AP channel mode to indoor mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] regulatory-domain-profile name default
[HUAWEI-wlan-regulate-domain-default] channel-load-mode indoor
Warning: This operation may change the operating channels of APs and restart the APs that run
V200R019C00 or earlier. Continue? [Y/N]:y
```

11.2.51 clear configuration this

Function

The **clear configuration this** command clears all configurations in the AP provisioning view.

Format

clear configuration this

Parameters

None

Views

AP provisioning view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure new AP provisioning parameters, run the **clear configuration this** command in the AP provisioning view to clear existing configurations.

Configuration Impact

Configurations in the AP provisioning view cannot be restored after they are cleared. Therefore, exercise caution when running the **clear configuration this** command.

Example

Clear all configurations in the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] clear configuration this
```

11.2.52 commit (AP provisioning view)

Function

The **commit** command commits configuration to an AP, a group of APs, or all the online APs.

Format

commit { **ap-name** *ap-name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* | **ap-group** *ap-group-name* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Commits configuration to the AP with the specified AP name.	The AP name must already exist.
ap-mac *ap-mac-address*	Commits configuration to the AP with the specified MAC address.	The AP's MAC address must already exist.
ap-id *ap-id*	Commits configuration to the AP with the specified AP ID.	The AP ID must already exist.

Parameter	Description	Value
ap-group *ap-group-name*	Commits configuration to the AP in the specified AP group.	The AP group must already exist.
all	Commits configuration to all the online APs.	-

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure AP provisioning parameters on the AC, such as the AP's management VLAN, static IP address, gateway, and AC list. After the configuration is complete, run the **commit** command, and the configuration will be delivered to the AP.

Prerequisites

APs have gone online on the AC.

Precautions

- After the configuration is committed, the AP receives the configuration and compares the configuration with its local configuration.
  - If they are consistent, the AP does not process the received configuration.
  - If they are different, the AP saves the committed configuration and automatically restarts, and the received configuration takes effect.
- If the name or static IP address of an AP is specified in the AP provisioning view, the configuration is delivered only to the AP by specifying the AP name or MAC address, but cannot be delivered to APs in the specified AP group.
- If you commit configurations to a large number of APs simultaneously, some of the APs may fail to receive the configurations. In this case, you are advised to commit the configurations again.

Example

Commit the configuration to the AP with the MAC address 00e0-fc76-e360.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] commit ap-mac 00e0-fc76-e360
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and may cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.53 console ble-mode (AP system profile view)

Function

The **console ble-mode** command configures the mode of the Bluetooth serial port.

The **undo console ble-mode** command restores the default mode of the Bluetooth serial port.

The default mode of the Bluetooth serial port is dynamic.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

console ble-mode { **dynamic** | **persistent** | **disable** }

undo console ble-mode

Parameters

Parameter	Description	Value
dynamic	Sets the mode of the Bluetooth serial port to **dynamic**. In this mode, when a Fit AP is disconnected from an AC, the Bluetooth serial port is automatically enabled; when the link between the AP and AC is normal, the Bluetooth serial port is disabled.	-
persistent	Sets the mode of the Bluetooth serial port to persistent. The Bluetooth serial port remains enabled in this mode.	-
disable	Disables the Bluetooth serial port.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Bluetooth serial port is enabled on an AP, STAs can be connected to the AP through Bluetooth and use the CloudCampus APP to log in to the AP through the Bluetooth serial port, facilitating fault diagnosis and debugging of the AP.

Precautions

Console port login has been enabled on the AP using the **undo console disable** command.

Upon an AP restart, the Bluetooth function is automatically enabled before the AP starts up, facilitating AP fault diagnosis and debugging. If the Bluetooth serial port has been disabled using the **console ble-mode disable** command before the AP restarts, this function will be automatically disabled after the AP starts up.

Example

Set the mode of the Bluetooth serial port to **persistent** in the AP system profile **system1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] console ble-mode persistent
Warning: Bluetooth-based console port login cannot be used together with Bluetooth-based monitoring,
Bluetooth-based tag locating, and Bluetooth-based transparent data transmission, Whether to continue?
[Y/N]:y
```

11.2.54 console disable

Function

The **console disable** command disables a user from logging in to the AP through a console port.

The **undo console disable** command enables a user from logging in to the AP through a console port.

By default, a user can log in to the AP through a console port.

Format

console disable

undo console disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When a user cannot telnet or stelnet to the AP, the user can log in to the AP through a console port to manage and configure the AP.

After the **console disable** command is run, unauthorized users cannot log in to the AP through the console port to perform operations.

Example

Disable a user to log in to the AP through a console port.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] console disable
```

11.2.55 coordinate

Function

The **coordinate** command sets the latitude and longitude of an AP.

The **undo coordinate** command restores the latitude and longitude of an AP to empty.

By default, no latitude or longitude is configured for an AP.

NOTE

This command is not available for the following APs:

- AirEngine 5761-10W and AirEngine 5761S-10W

Format

coordinate longitude { **e** | **w** } *longitude-value* **latitude** { **s** | **n** } *latitude-value*

undo coordinate

Parameters

Parameter	Description	Value
longitude e *longitude-value*	Specifies the east longitude value of an AP.	The value supports two formats: degrees, minutes, and seconds (DMS) and decimal degrees (DD). ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.

Parameter	Description	Value
longitude w *longitude-value*	Specifies the west longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.
latitude s *latitude-value*	Specifies the south latitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.
latitude n *latitude-value*	Specifies the north latitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set the longitude and latitude of an AP for easily locating it.

Example

Set the longitude and latitude of an AP to 114.3435°E and 14.3435°S, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] coordinate longitude e 114.3435 latitude s 14.3435
```

11.2.56 cpu-usage threshold

Function

The **cpu-usage threshold** command configures a CPU usage alarm threshold for APs.

The **undo cpu-usage threshold** command restores the default CPU usage alarm threshold.

By default, the CPU usage alarm threshold of APs is 90.

Format

cpu-usage threshold *threshold*

undo cpu-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies the CPU usage alarm threshold of APs.	The value is an integer that ranges from 50 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **cpu-usage threshold** command to configure the CPU usage alarm threshold in the AP system profile view. The configuration is delivered to all APs using the profile.

- When the CPU usage of an AP exceeds the alarm threshold, .
- When the CPU usage of an AP falls below the alarm threshold,

Example

Set the CPU usage alarm threshold to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] cpu-usage threshold 60
```

11.2.57 cpu-defend packet-type

Function

The **cpu-defend packet-type** command configures a rate limit for packets sent by an AP to the CPU.

The **undo cpu-defend packet-type** command restores the default rate limit for packets sent by an AP to the CPU.

By default, an AP does not limit the rates of packets sent to the CPU.

Format

cpu-defend packet-type *packet-type* **rate-limit** *rate-value* { **wired** | **wireless** }

undo cpu-defend packet-type *packet-type* **rate-limit** { **wired** | **wireless** }

Parameters

Parameter	Description	Value
packet-type	Specifies the protocol type of packets.	The value depends on the protocol types supported by the device.
rate-limit *rate-value*	Specifies the rate limit. The value of *rate-value* indicates the rate limit for protocol packets.	The value is an integer that ranges from 1 to 4294967295, in pps.
wired	Indicates wired packets.	-
wireless	Indicates wireless packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an AP receives attack packets of a certain protocol type or a large number of normal packets destined for the CPU, you can limit the rates of these packets within a small range in the AP system profile to reduce the impact on CPU processing of normal services.

Precautions

If you run the **cpu-defend packet-type** command with the same *packet-type* value multiple times, only the latest configuration takes effect.

Example

Set the protocol type to wired ARP reply packet, and set the rate limit to 1260 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] cpu-defend packet-type arp-reply rate-limit 1260 wired
```

11.2.58 crc-alarm enable

Function

The **crc-alarm enable** command enables the alarm function for CRC errors on the AP's wired interface and specifies the alarm threshold and clear alarm threshold.

The **undo crc-alarm enable** command disables the alarm function for CRC errors on the AP's wired interface and restores the alarm threshold and clear alarm threshold to the default values.

By default, the alarm function for CRC errors is disabled on the AP's wired interface. The alarm threshold for CRC errors is 50 and the clear alarm threshold is 20.

Format

crc-alarm enable [**high-threshold** *high-threshold-value* | **low-threshold** *low-threshold-value*]*

undo crc-alarm enable

Parameters

Parameter	Description	Value
high-threshold *high-threshold-value*	Specifies the alarm threshold for CRC errors on the AP's wired interface.	The value is an integer that ranges from 1 to 100. The unit is 1/10000. The value of *high-threshold-value* must be larger than the value of *low-threshold-value*.
low-threshold *low-threshold-value*	Specifies the clear alarm threshold for CRC errors on the AP's wired interface.	The value is an integer that ranges from 1 to 100.

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

When the AP detects that the number of CRC errors exceeds the configured upper alarm threshold in a specified period (the time period can be configured using the **sample-time** command, and is 30s by default), it sends an alarm message to the AC. To prevent the AP from frequently sending alarm messages or alarm clearance messages to the AC, you need to configure the lower threshold for clearing the alarm. The AP sends an alarm clearance message to the AC only when the AP detects that the number of CRC errors is lower than the configured lower threshold.

Example

Enable the alarm function for CRC errors on the AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] crc-alarm enable
```

11.2.59 dai enable (AP wired port profile view)

Function

The **dai enable** command enables dynamic ARP inspection (DAI) on an AP's wired interface.

The **undo dai enable** command disables DAI on an AP's wired interface.

By default, DAI is disabled on an AP's wired interface.

Format

dai enable

undo dai enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable DAI using this command to prevent Man in The Middle (MITM) attacks and theft on authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device allows the packet to pass through. If the ARP packet does not match any binding entry, the device discards the packet.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on ARP packets transmitted on an AP's wired interface.

An AP's wired interface added to an Eth-Trunk does not support this function.

Example

Enable DAI on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] dai enable
```

11.2.60 description (AP wired port profile view)

Function

The **description** command configures the description of the AP's wired interface.

The **undo description** command restores the default description of the AP's wired interface.

By default, the AP's wired interface has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of the AP's wired interface.	The value is a string of 1 to 242 case-sensitive characters with spaces.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

To manage AP interfaces conveniently, run this command to set AP interface descriptions. The description of an AP interface helps you identify the AP interface and know its functions.

Example

Change the description of the AP's wired interface to **poe-power**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] description poe-power
```

11.2.61 display ap around-ssid-list

Function

The **display ap around-ssid-list** command displays SSIDs of neighbors of a specified AP.

Format

display ap around-ssid-list { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view SSIDs of neighbors of a specified AP. Neighbors of an AP include authorized and unauthorized neighbors. Authorized neighbors are other APs managed by the same AC. APs that are managed by other ACs are unauthorized neighbors.

Example

Display SSIDs of neighbors of AP **example**.

```
<HUAWEI> display ap around-ssid-list ap-name example
In control AP(2.4G):
--------------------------------------------------
SSID
--------------------------------------------------
test1
--------------------------------------------------
Total: 1
Uncontrol AP(2.4G):
--------------------------------------------------
SSID
--------------------------------------------------
test2
--------------------------------------------------
Total: 1
In control AP(5G):
--------------------------------------------------
SSID
--------------------------------------------------
test3
--------------------------------------------------
Total: 1
Uncontrol AP(5G):
--------------------------------------------------
SSID
--------------------------------------------------
test4
--------------------------------------------------
Total: 1
```

Table 11-68 Description of the **display ap around-ssid-list** command output

Item	Description
In control AP	SSIDs of authorized neighbors.
Uncontrol AP	SSIDs of unauthorized neighbors.

11.2.62 display ap asyn-message err-info

Function

The **display ap asyn-message err-info** command displays records about AP restart failures.

Format

display ap asyn-message err-info { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays records about restart failures of all APs.	-
ap-name *ap-name*	Displays records about restart failures of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays records about restart failures of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you use commands on the AC to restart an AP manually, during an upgrade, or to restore its factory settings, the restart message delivered by the AC may get lost due to transmission failures. Therefore, APs are not restarted. If an AP does not receive the restart message, the AP is still connected to the AC, which makes the AC incorrectly consider that the AP is restarted successfully. This command displays records about AP restart failures, helping you check whether the AP is restarted successfully. If the AP restart fails, restart the AP.

Example

Display records about restart failures of all APs.

```
<HUAWEI> display ap asyn-message err-info all
------------------------------------------------------------------------------
AP Name MAC            Time                  Reason
------------------------------------------------------------------------------
area_1  00e0-fc76-e360 2015-1-19 14:41:59      update
area_2  00e0-fc74-9640 2015-1-19 14:45:56      clear config
------------------------------------------------------------------------------
Total: 2
```

Table 11-69 Description of the **display ap asyn-message err-info** command output

Item	Description
AP Name	Name of an AP.
MAC	MAC address of an AP.
Time	Time when AP restart fails.
Reason	Type of AP restart failures. ● update: The AP fails to be restarted during an upgrade. ● clear config: The AP fails to be restarted when restoring factory settings. ● other: The AP fails to be restarted manually. ● reset timeout: The AP fails to be restarted because the restart command execution times out.

11.2.63 display ap coordinate

Function

The **display ap coordinate** command displays information about longitudes and latitudes of APs.

Format

display ap coordinate { **all** | **ap-group** *ap-group-name* }

Parameters

Parameter	Description	Value
all	Displays information about longitudes and latitudes of all APs.	-
ap-group *ap-group-name*	Displays information about longitudes and latitudes of APs in the specified AP group.	The AP group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view longitudes and latitudes of APs.

Example

Display information about longitudes and latitudes of all APs.

```
<HUAWEI> display ap coordinate all
--------------------------------------------------------------------------------------------------------
ID   Name            Group      Longitude           Latitude
--------------------------------------------------------------------------------------------------------
0    area_1          default    30.1111111°E        40.2222222°N
1    area_2          default    110°59’59"W         77°25'53"N
2    area_3          default    -                   -
-------------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-70 Description of the **display ap coordinate all** command output

Item	Description
ID	AP ID.
Name	AP name.
Group	AP group.
Longitude	Longitude of an AP. Its display varies depending on the format: - Example: 114°3’14’’E in the format of degree/minute/second - Example: 114.3435°E in the format of decimal degree - Hyphen (-) if it is not configured
Latitude	Latitude of an AP. - Example: 114°3’14’’S in the format of degree/minute/second - Example: 114.3435°S in the format of decimal degree - Hyphen (-) if it is not configured

11.2.64 display ap elabel

Function

The **display ap elabel** command displays electronic label information about a specified AP.

Format

display ap elabel { **ap-name** *ap-name* | **ap-id** *ap-id* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays electronic label information about the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Displays electronic label information about the AP with the specified ID.	The AP ID must exist.
all	Displays electronic label information of all APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view electronic label information about an AP. An electronic label is also called permanent configuration data or information and is written in the storage device during AP testing or commissioning. An electronic label includes the AP name, serial number, manufacture date and manufacturer information.

Example

Display electronic label information about the AP named **example**.

```
<HUAWEI> display ap elabel ap-name example
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0



 [Board Properties]
 BoardType=AirEnginexxxx
 BarCode=210235xxxxxxxxxxxxxx
 Item=0235xxxx
 Description=Assembling Components,AirEnginexxxx,AirEnginexxxx,AirEnginexxxx (11ax indoor,2+4 dual
bands,smart antenna,U
SB,BLE,PSE)
 Manufactured=2020-02-21
 VendorName=Huawei
 IssueNumber=00
```

```
CLEICode=
BOM=
```

Table 11-71 Description of the **display ap elabel** command output

Item	Description
ArchivesInfo Version	Electronic label version.
BoardType	AP type.
BarCode	Bar code of an AP.
Item	BOM code of an AP.
Description	English description of an AP.
Manufactured	Production date of an AP.
VendorName	Vendor name.
IssueNumber	Issue number of an AP.
CLEICode	CLEI code of an AP.
BOM	Sales BOM code of an AP.

Display electronic label information of all APs.

```
<HUAWEI> display ap elabel all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP elabel information:
------------------------------------------------------------------------------
ID   MAC            Name     Type          SN                  Item
------------------------------------------------------------------------------
1    00e0-fc76-e360 L1_001   AirEnginexxxx   210235xxxxxxxxxxxxxx -
2    00e0-fc76-e340 1        AirEnginexxxx   210235xxxxxxxxxxxxxx -
------------------------------------------------------------------------------
Total: 2
```

Table 11-72 Description of the **display ap elabel all** command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.
Name	AP name.
Type	AP type.
SN	SN of an AP.
Item	BOM code of an AP.

11.2.65 display ap fan

Function

The **display ap fan** command displays fan information about an AP.

Format

display ap fan { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays fan information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays fan information about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check fan information about an AP, including the fan speed, operating mode, and airflow direction.

Fan information query is supported only by the AirEngine 9700D-M, AirEngine 9700D-S, and AirEngine 9700D-M1.

Example

Display fan information about AP **0**.

```
<HUAWEI> display ap fan ap-id 0
--------------------------------------------------------------------------------
Fan   State    Speed rate   Mode   Airflow direction
--------------------------------------------------------------------------------
0     Running  40%          AUTO   Front-to-Back
1     Running  40%          AUTO   Front-to-Back
--------------------------------------------------------------------------------
```

Table 11-73 Description of the **display ap fan** command output

Item	Description
Fan	Fan ID.

Item	Description
State	Status of a fan. - Absent: The fan is not in position. - Abnormal: The fan is working abnormally. - Running: The fan is running. - Stop: The fan stops.
Speed rate	Ratio of the current fan speed to the full speed.
Mode	Operating mode of a fan. - AUTO: automatic mode - MANUAL: manual mode
Airflow direction	Airflow direction of a fan. - Front-to-Back: Air flows from the front to the rear.

11.2.66 display ap lldp neighbor

Function

The **display ap lldp neighbor** command displays LLDP neighbor information on a specified AP.

Format

display ap lldp neighbor { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**interface** *interface-type interface-number*] | **brief** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays LLDP neighbor information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays LLDP neighbor information about the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays LLDP neighbor information about a specified AP interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
brief	Displays brief LLDP neighbor information about APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view LLDP neighbor information on a specified AP, including the number of LLDP neighbors, device ID, interface ID, system name system description, and management address of each neighbor. The LLDP neighbor information is reported by an AP to the connected AC.

If no parameter is specified, LLDP neighbor information about all AP interfaces is displayed.

Prerequisites

The AP has been enabled to report LLDP neighbor information by using the **lldp report enable** command in the AP system profile view.

Example

Display LLDP neighbor information on all APs.

```
<HUAWEI> display ap lldp neighbor brief
------------------------------------------------------------------------------------------
Hostname  Neighbor device  Management address  Local intf  Neighbor intf          TTL
------------------------------------------------------------------------------------------
hello     HUAWEI         10.10.10.3          GE0        GigabitEthernet0/0/16  119
------------------------------------------------------------------------------------------
Total: 1
```

Table 11-74 Description of the **display ap lldp neighbor** command output

Item	Description
Hostname	AP name.
Neighbor device	System name of an AP neighbor.
Management address	Management address of an AP neighbor.
Local intf	Local interface of the AP.
Neighbor intf	Interface of an AP neighbor.
TTL	Time to live (TTL) of the AP neighbor information stored on the local AP.

Display LLDP neighbor information about GE0 of the AP named **hello**.

```
<HUAWEI> display ap lldp neighbor ap-name hello interface gigabitethernet 0
-------------------------------------------------------------------------------
AP 1 Port 0 has 1 neighbor(s):

Basic port information
Neighbor index              : 1
Host Name                   : hello
Chassis ID type             : macAddress
Chassis ID                  : 00e0-fc76-e360
Port ID type                : interfaceName
Port ID                     : GigabitEthernet0/0/2
Time to live                : 120s
Port description            : GigabitEthernet0/0/2
System name                 : Quidway
System description          : S5720-56C-HI
                  Huawei Versatile Routing Platform Software
                  VRP (R) software,Version 5.110 (S5720 V200R023C00)
                  Copyright (C) 2007 Huawei Technologies Co., Ltd.
System capabilities supported: wlanAccessPoint telephone
System capabilities enabled  : wlanAccessPoint telephone
Management address type      : IPv4
Management address           : 10.10.10.5

DOT3 port information
-------------------------------------------------------------------------------
OperMau                                  : speed(1000Mbps)/duplex(Full)
Power port class                         : Unknown
PSE power supported                      : No
PSE power enabled                        : No
PSE pairs control ability                : No
Power pairs                              : Unknown
Port power classification                : Unknown
Power type                               : Type 2 PSE
Power source                             : Reserved
Power priority                           : High
PD requested power value                 : 479.5(w)
PSE allocated power value                : 281.6(w)
PD requested power value Mode A          : 0.0(w)
PD requested power value Mode B          : 2335.4(w)
PSE allocated power value Alternative A  : 1055.8(w)
PSE allocated power value Alternative B  : 1488.9(w)
Power Class                              : Unknown
PSE power pairsx                         : Alternative A
Power typex                              : Type unknown
```

```
PD 4PID                                  : No
PD Load                                  : Single-signature
PSE maximum available power              : 421.6(w)
PSE Autoclass support                    : Yes
Autoclass completed                      : Idle
Autoclass request                        : Completed
Power down                               : No

Legacy port information
--------------------------------------------------------------------------------
4-pair PoE Supported                     : Yes
Spare pair Detection/Classification required: Yes
PD Spare Pair Desired State              : Disable
PSE Spare Pair Operational State         : Enable
--------------------------------------------------------------------------------
```

Table 11-75 Description of the **display ap lldp neighbor ap-name** *ap-name* **interface** *interface-type interface-number* command output

Item	Description
Neighbor index	Index of a neighbor.
Host Name	AP name.
Chassis ID type	ID subtype of a neighbor device. ● chassisComponent: chassis alias ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● interfaceName: name of the interface ● local: name of the local device
Chassis ID	ID of a neighbor device. ● A MAC address is displayed when the neighbor device ID subtype is **macAddress**. ● An IP address is displayed when the neighbor device ID subtype is **networkAddress**. ● A character string is displayed when the neighbor device ID subtype is neither **macAddress** nor **networkAddress**.

Item	Description
Port ID type	ID subtype of the neighbor interface. - interfaceAlias: interface alias - portComponent: interface or backplane alias - macAddress: MAC address - networkAddress: network address - interfaceName: name of the interface - agentCircuitID: loopback interface ID of the DHCP relay - local: name of the local device
Port ID	ID of the neighbor interface. - A MAC address is displayed when the neighbor interface ID subtype is **macAddress**. - An IP address is displayed when the neighbor interface ID subtype is **networkAddress**. - A character string is displayed when the neighbor interface ID subtype is neither **macAddress** nor **networkAddress**.
Time to live	Time to live (TTL) of the AP neighbor information stored on the local AP.
Port description	Description of the neighbor interface.
System name	System name.
System description	System description of the neighbor.
System capabilities supported	Capabilities of the neighbor device. - other: other capabilities - repeater: repeater - bridge: bridge device - wlanAccessPoint: wireless access point - router: router - telephone: wireless device - docsisCableDevice: management station - stationOnly: base station

Item	Description
System capabilities enabled	Capabilities enabled on the neighbor device. - other: other capabilities - repeater: repeater - bridge: bridge device - wlanAccessPoint: wireless access point - router: router - telephone: wireless device - docsisCableDevice: management station - stationOnly: base station
Management address type	Management address type of the neighbor.
Management address	Management address of the neighbor.
OperMau	Speed and duplex status of a neighbor interface. - The value of **speed** can be 10, 100, 1000, 2500, 5000, 10000, 40000, or **Unknown**. **Unknown** indicates that the neighbor device does not carry the interface speed. - The value of **duplex** can be **Half**, **Full**, or **Unknown**. **Unknown** indicates that the neighbor device does not carry the duplex mode.
Power port class	PoE type: - PSE: power-sourcing equipment. - PD: powered device. - Unknown: unknown PoE type.
PSE power supported	Whether the PSE power is supported. - Yes: PSE power is supported. - No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. - Yes: enabled. - No: disabled.
PSE pairs control ability	Whether the PSE control is supported. - Yes: PSE control is supported. - No: PSE control is not supported.

Item	Description
Power pairs	PoE remote power supply mode: - Signal: power supply mode of signal lines. - Spare: power supply mode of spare signal lines. - Unknown: an unknown remote power supply mode.
Port power classification	PD power control level on the interface: - Class0: indicates level 1. - Class1: indicates level 2. - Class2: indicates level 3. - Class3: indicates level 4. - Class4: indicates level 5. - Class5: indicates level 6. - Class6 indicates level 7. - Class7 indicates level 8. - Unknown: indicates an unknown control level.
Power type	PoE device type:
Power source	Power supply source. Type of the PSE: **Primary power source**, **Backup source**, **Reserved**, and **Unknown** Type of the PD: **PSE**, **Reserved**, **PSE and local**, and **Unknown**
Power priority	Power priority: - Critical: the highest priority. - High: the second highest priority. - Low: the lowest priority. - Unknown: unknown priority.
PD requested power value	Power requested by the PD.
PSE allocated power value	Power allocated by the PSE.
PD requested power value Mode A	Power requested by the PD in mode A.
PD requested power value Mode B	Power requested by the PD in mode B.
PSE allocated power value Alternative A	Power allocated by the PSE for a PD in mode A.

Item	Description
PSE allocated power value Alternative B	Power allocated by the PSE for a PD in mode B.
Power Class	Power class requested by the PD or allocated by the PSE.
PSE power pairsx	Mode in which the PSE supplies power to a PD.
Power typex	Working type of the device.
PD 4PID	Whether the PD supports all power receive types. - No: The PD does not support all power receive modes. - Yes: The PD supports all power receive types.
PD Load	Whether isolation between modes A and B is required for the PD. - No: Isolation between modes A and B is not required for the PD. - Yes: Isolation between modes A and B is required for the PD.
PSE maximum available power	Maximum output power of the PSE.
PSE Autoclass support	Whether the PSE supports Autoclass. - No: The PSE does not support Autoclass. - Yes: The PSE supports Autoclass.
Autoclass completed	Whether Autoclass is completed.
Autoclass request	Whether Autoclass is required for the PD.
Power down	Whether the PD requires power supply from the PSE.
4-pair PoE Supported	Whether the interface supports UPoE.
Spare pair Detection/Classification required	Whether the standby device supports the requirement for detection and classification.
PD Spare Pair Desired State	Requirement state of the standby PD.
PSE Spare Pair Operational State	Operation state of the standby PSE.

11.2.67 display ap led

Function

The **display ap led** command displays the indicator blinking status of an AP.

Format

display ap led { **ap-mac** *ap-mac* | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the indicator blinking status of an AP.

This function is not available for central APs.

Example

Display the indicator blinking status of the AP with the MAC address of 00e0-fc12-3456.

```
<HUAWEI> display ap led ap-mac 00e0-fc12-3456
Led status          : blink
Blink left time(s)  : 100
```

Table 11-76 Description of the **display ap led** command output

Item	Description
Led status	Blinking status of the indicator. - off: The indicator is off. - blink: The indicator is blinking. To configure the parameter, run the **led blink-time** command. - normal: The indicator is running properly. The running status of the AP is displayed according to the indicator description.
Blink left time(s)	Remaining time of the indicator blinking status.

11.2.68 display ap neighbor

Function

The **display ap neighbor** command displays information about neighbors of a radio, including authorized and unauthorized neighbors.

Format

display ap neighbor { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio*	Specifies radio ID of an AP.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

APs' neighbor information reflects the APs' locations and neighbor relationships, helping you plan the network.

If a neighboring AP is an authorized one, the system displays the RSSI of signals received from the neighboring AP as well as the path loss.

If a neighboring AP is an unauthorized one, the system displays only the RSSI of signals received from the neighboring AP.

Prerequisites

The radio calibration function has been enabled using the **calibrate enable { auto | manual | schedule time }** command.

Precautions

In auto radio calibration mode, APs continuously report and update neighboring information so that the AC can query the latest AP neighbor information. In manual or scheduled radio calibration mode, APs report neighbor information during radio calibration. Information about unauthorized neighbors ages 1 hour later, and that about authorized neighbor information ages 32 hours later. Neighbor information can be queried only before the aging time expires.

Example

Display information about neighbors of radio 0 on the AP named **hello**.

```
<HUAWEI> display ap neighbor ap-name hello radio 0
Info: This operation may take a few seconds. Please wait for a moment.done.
Radio: Radio ID of AP
CH/BW: Channel/Bandwidth
SC RSSI: Single-chain RSSI
In control AP:
------------------------------------------------------------------------------------------------------------------------
------
AP ID  AP name         Radio  CH/BW     RSSI(dBm) SC RSSI(dBm) RSSI pathloss(dB)  RSRP(dBm)  RSRP
pathloss(dB)  Last Update Time
------------------------------------------------------------------------------------------------------------------------
------
9      00e0-fc9d-c160   0      1/40M+    -61       -66         89                -71        94
2022-09-13/19:29:48
------------------------------------------------------------------------------------------------------------------------
------
Total: 1

Uncontrol AP:
----------------------------------------------------------------------------------------------------
Radio  BSSID          Channel  RSRP(dBm)  Last Update Time        SSID
----------------------------------------------------------------------------------------------------
0      00e0-fcf2-d1e0 6        -78        2022-09-13/19:27:39     hw_manage_d1e0
----------------------------------------------------------------------------------------------------
Total: 1
```

Table 11-77 Description of the **display ap neighbor** command output

Item	Description
In control AP	Authorized neighboring AP.

Item	Description
AP ID	ID of a neighboring AP.
AP name	Name of a neighboring AP.
Radio	Radio ID of a neighboring AP.
CH/BW	Working channel and bandwidth of a neighboring AP. **NOTE** The device displays only information about neighboring APs detected on the current channel.
RSSI(dBm)	Received signal strength indicator (RSSI) of a neighboring AP.
SC RSSI(dBm)	Single-chain RSSI.
RSSI pathloss(dB)	RSSI path loss.
RSRP(dBm)	Reference signal received power (RSRP) of a neighboring AP. The RSRP indicates the strength of the received reference signals.
RSRP pathloss(dB)	RSRP path loss.
Last Update Time	Last update time.
Uncontrol AP	Unauthorized neighboring AP.
Radio	Neighboring AP detected on an AP radio.
BSSID	BSSID of an unauthorized neighbor.
Channel	Channel that the unauthorized neighboring AP uses.
RSRP(dBm)	Strength of signals received from the neighboring AP.
Last Update Time	Latest time when the AP is detected.
SSID	SSID of an unauthorized neighbor.

11.2.69 display ap optical-info

Function

The **display ap optical-info** command displays optical module information.

Format

display ap optical-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays optical module information of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays optical module information of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view optical module information, including the optical module type, transmit optical power, and receive optical power.

Prerequisites

The AP has been online. You can run the **display ap** command to check the AP status.

The AP supports optical modules. You can run the **display ap-type** command to view the AP model.

NOTE

Optical module query is supported only by the following models:

- AirEngine X760 series APs (excluding the AirEngine 6760-51EI)
- AirEngine 6761-21, AirEngine 6761-21E, AirEngine 6761S-21, AirEngine 5761R-11, AirEngine 5761R-11E, AirEngine 5761RS-11, AirEngine 5761-11EI
- AirEngine 5762-15HW
- AirEngine 8771-X1T
- AirEngine 9700D-S (including matching ORUs)
- AirEngine series central APs

Precautions

If a copper module is inserted into an optical interface, diagnostic information is not supported.

Example

Display optical module information about the AP named **example**.

```
<HUAWEI> display ap optical-info ap-name example
-------------------------------------------------------------------------------
Interface name:XGE0/0/0
-------------------------------------------------------------------------------
Common information:
  Transceiver Type                    :1000_BASE_LX_SFP
  Connector                           :LC
  Wavelength(nm)                      :1310
  Transfer Distance(m)                :10000(9um)
  Copper link length(m)               :0
  Digital Diagnostic Monitoring       :NO
  Vendor name                         :FINISAR CORP.
  Vendor part number                  :FTLF1318P2BTL-HW
  Vendor IEEE company ID              :36965
  Vendor revision level               :A
  Nominal bit rate(MBits/sec)         :1200
-------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number                :PMK2K62
  Manufacturing Date                  :2012-05-09
  Vendor name                         :FINISAR CORP.
-------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)               :49
  Temp High Threshold(degree C)       :90
  Temp Low Threshold(degree C)        :-45
  Supply voltage(0.1mV)               :33161
  Volt High Threshold(0.1mV)          :37000
  Volt Low Threshold(0.1mV)           :29000
  TX bias current(mA)                 :19
  Bias High Threshold(mA)             :25430
  Bias Low Threshold(mA)              :1929
  RX power(0.1uw)                     :0
  RX Power High Threshold(0.1uw)      :5012
  RX Power Low Threshold(0.1uw)       :126
  TX power(0.1uw)                     :2886
  TX Power High Threshold(0.1uw)      :6310
  TX Power Low Threshold(0.1uw)       :708
-------------------------------------------------------------------------------
Interface name:XGE0/0/1
-------------------------------------------------------------------------------
Common information:
  Transceiver Type                    :OC3_LONG_REACH_SFP
  Connector                           :LC
  Wavelength(nm)                      :1310
  Transfer Distance(m)                :40000(9um)
  Copper link length(m)               :0
  Digital Diagnostic Monitoring       :YES
  Vendor name                         :NEOPHOTONING
  Vendor part number                  :PT7320-31-2W
  Vendor IEEE company ID              :0
  Vendor revision level               :1.0
  Nominal bit rate(MBits/sec)         :100
-------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number                :A1008036407
  Manufacturing Date                  :2008-10-09
  Vendor name                         :NEOPHOTONING
-------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)               :47
  Temp High Threshold(degree C)       :100
  Temp Low Threshold(degree C)        :-10
  Supply voltage(0.1mV)               :32808
  Volt High Threshold(0.1mV)          :34461
```

```
  Volt Low Threshold(0.1mV)           :30523
  TX bias current(mA)                :9
  Bias High Threshold(mA)             :24
  Bias Low Threshold(mA)              :0
  RX power(0.1uw)                    :0
  RX Power High Threshold(0.1uw)      :50477
  RX Power Low Threshold(0.1uw)       :152
  TX power(0.1uw)                    :5291
  TX Power High Threshold(0.1uw)      :3320
  TX Power Low Threshold(0.1uw)       :834
-------------------------------------------------------------------------------
Interface name:XGE0/0/2
-------------------------------------------------------------------------------
Common information:
  Transceiver Type                   :1000_BASE_LX_SFP
  Connector                          :LC
  Wavelength(nm)                     :1310
  Transfer Distance(m)               :10000(9um)
  Copper link length(m)              :0
  Digital Diagnostic Monitoring       :YES
  Vendor name                        :Hisense
  Vendor part number                 :LTD1302-BC+1
  Vendor IEEE company ID              :0
  Vendor revision level              :V1.0
  Nominal bit rate(MBits/sec)         :1300
-------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number               :J2220000170
  Manufacturing Date                 :2012-09-20
  Vendor name                        :Hisense
-------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)               :37
  Temp High Threshold(degree C)       :78
  Temp Low Threshold(degree C)        :-5
  Supply voltage(0.1mV)               :32776
  Volt High Threshold(0.1mV)          :35650
  Volt Low Threshold(0.1mV)           :29000
  TX bias current(mA)                :9
  Bias High Threshold(mA)             :70
  Bias Low Threshold(mA)              :0
  RX power(0.1uw)                    :4267
  RX Power High Threshold(0.1uw)      :5012
  RX Power Low Threshold(0.1uw)       :79
  TX power(0.1uw)                    :2304
  TX Power High Threshold(0.1uw)      :10000
  TX Power Low Threshold(0.1uw)       :631
-------------------------------------------------------------------------------
Interface name:XGE0/0/3
-------------------------------------------------------------------------------
Common information:
  Transceiver Type                   :1000_BASE_LX_SFP
  Connector                          :LC
  Wavelength(nm)                     :1310
  Transfer Distance(m)               :10000(9um)
  Copper link length(m)              :0
  Digital Diagnostic Monitoring       :YES
  Vendor name                        :FINISAR CORP.
  Vendor part number                 :FTLF1318P2BTL-HW
  Vendor IEEE company ID              :36965
  Vendor revision level              :A
  Nominal bit rate(MBits/sec)         :1200
-------------------------------------------------------------------------------
Manufacture information:
  Vendor serial number               :PLTOL92
  Manufacturing Date                 :2012-05-09
  Vendor name                        :FINISAR CORP.
-------------------------------------------------------------------------------
Diagnostic information:
```

```
 Temperature(degree C)                :38
 Temp High Threshold(degree C)        :90
 Temp Low Threshold(degree C)         :-45
 Supply voltage(0.1mV)                :33061
 Volt High Threshold(0.1mV)           :37000
 Volt Low Threshold(0.1mV)            :29000
 TX bias current(mA)                  :19
 Bias High Threshold(mA)              :52
 Bias Low Threshold(mA)               :4
 RX power(0.1uw)                      :1
 RX Power High Threshold(0.1uw)       :5012
 RX Power Low Threshold(0.1uw)        :126
 TX power(0.1uw)                      :3219
 TX Power High Threshold(0.1uw)       :6310
 TX Power Low Threshold(0.1uw)        :708
--------------------------------------------------------------------------------
```

Table 11-78 Description of the **display ap optical-info** command output

Item	Description
Interface name	Name of the optical module.
Transceiver Type	Type of the optical module.
Connector	Interface type.
Wavelength(nm)	Optical wavelength, in nm.
Transfer Distance(m)	Transmission distance, in meters.
Copper link length(m)	Length of the copper cable, in meters.
Digital Diagnostic Monitoring	Whether diagnostic information about the optical module is monitored.
Vendor name	Name of the vendor.
Vendor part number	Product code provided by the vendor.
Vendor IEEE company ID	Version number provided by the vendor.
Vendor revision level	Product serial number provided by the vendor.
Nominal bit rate(MBits/sec)	Bit rate of the optical module, in Mbit/s.
Vendor serial number	Vendor sequence number of the optical module.
Manufacturing Date	Manufacturing date of the optical module.
Temperature(degree C)	Current temperature of the optical module, in °C.
Temp High Threshold(degree C)	The upper threshold for the temperature of the optical module, in °C.

Item	Description
Temp Low Threshold(degree C)	The lower threshold for the temperature of the optical module, in °C.
Supply voltage(0.1mV)	Current voltage of the optical module, in 0.1 mV.
Volt High Threshold(0.1mV)	The upper threshold for the voltage of the optical module, in 0.1 mV.
Volt Low Threshold(0.1mV)	The lower threshold for the voltage of the optical module, in 0.1 mV.
TX bias current(mA)	Bias current of the optical module, in mA.
Bias High Threshold(mA)	Upper threshold for the bias current of the optical module, in mA.
Bias Low Threshold(mA)	Lower threshold for the bias current of the optical module, in mA.
RX power(0.1uw)	Receive power of the optical module, in 0.1 uW.
RX Power High Threshold(0.1uw)	Upper receive power threshold for the optical module, in 0.1 uW.
RX Power Low Threshold(0.1uw)	Lower receive power threshold for the optical module, in 0.1 uW.
TX power(0.1uw)	Transmit power of the optical module, in 0.1 uW.
TX Power High Threshold(0.1uw)	Upper transmit power threshold for the optical module, in 0.1 uW.
TX Power Low Threshold(0.1uw)	Lower transmit power threshold for the optical module, in 0.1 uW.

11.2.70 display ap performance statistics

Function

The **display ap performance statistics** command displays performance statistics about an AP.

Format

display ap performance statistics { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays performance statistics about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays performance statistics about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap performance statistics** command to view AP performance statistics to monitor AP performance.

Example

Display performance statistics about AP **huawei**.

```
<HUAWEI> display ap performance statistics ap-name huawei
------------------------------------------------------------------------------
Memory usage(%)                : 58
Memory average usage(%)        : 58
CPU usage(%)                   : 4
CPU average usage(%)           : 4
Available space size(KB)       : 1192
Device Temperature(degree C)   : 45
Environment Temperature(degree C) : -
CPU Temperature(degree C)      : -
NP Temperature(degree C)       : -
IRF0 Temperature(degree C)     : -
IRF1 Temperature(degree C)     : -
IRF2 Temperature(degree C)     : -
IRF3 Temperature(degree C)     : -
Online user number             : 0
Upstream traffic(wireless)(KB)  : 23 KB
Wireless port drop frames(RX)   : 0
Wireless port drop frames(TX)   : 0
Wireless port total bytes(RX)   : 0
Wireless port total bytes(TX)   : 0
Wireless port unicast frames(RX): 0
GigabitEthernet port 0
  port drop frames(RX)          : 0
  port drop frames(TX)          : 0
  port total Bytes(RX)          : 0
  port total Bytes(TX)          : 0
  port unknown frames(RX)       : 0
  port error frames(TX)         : 0
  port updown counts            : 0
  port output rate(Kbps)        : 0
  port input rate(Kbps)         : 1
GigabitEthernet port 1
```

```
port drop frames(RX)          : 0
port drop frames(TX)          : 0
port total Bytes(RX)          : 61210
port total Bytes(TX)          : 38218
port unknown frames(RX)       : 0
port error frames(TX)         : 0
port updown counts            : 0
port output rate(Kbps)        : 0
port input rate(Kbps)         : 1
--------------------------------------------------------------------------------
```

Table 11-79 Description of the **display ap performance statistics** command output

Item	Description
Memory usage(%)	Memory usage (%).
Memory average usage(%)	Average memory usage (%).
CPU usage(%)	CPU usage (%).
CPU average usage(%)	Average CPU usage (%).
Available space size(KB)	Available space, in KB.
Device Temperature(degree C)	AP's device temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
Environment Temperature(degree C)	AP's ambient temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
CPU Temperature(degree C)	AP's CPU temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
NP Temperature(degree C)	AP's NP module temperature (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
IRF*n* Temperature(degree C)	Temperature of IRF *n* (°C). The temperature is displayed as a hyphen (-) for APs that do not support the temperature display.
Online user number	Number of online users.
Upstream traffic(wireless)(KB)	Traffic volume on the wireless upstream interface in a specified period, in KB.

Item	Description
Wireless port drop frames(RX)	Number of discarded data frames received by the wireless interface.
Wireless port drop frames(TX)	Number of discarded data frames sent by the wireless interface.
Wireless port total bytes(RX)	Total number of bytes received by the wireless interface.
Wireless port total bytes(TX)	Total number of bytes sent by the wireless interface.
Wireless port unicast frames(RX)	Number of unicast data frames received by the wireless interface.
GigabitEthernet port x	ID of a wired interface.
port drop frames(RX)	Number of discarded data frames received by the wired interface.
port drop frames(TX)	Number of discarded data frames sent by the wired interface.
port total Bytes(RX)	Number of bytes received by the wired interface.
port total Bytes(TX)	Number of bytes sent by the wired interface.
port unknown frames(RX)	Number of unknown protocol packets received by the wired interface.
port error frames(TX)	Number of error data frames sent by the wired interface.
port updown counts	Number of times the wired interface alternates between Up and Down.
port output rate(Kbps)	Wired-side sending rate (kbps).
port input rate(Kbps)	Wired-side receiving rate (kbps).

NOTE

If the AP does not support this parameter, a hyphen (-) is displayed.

To clear wired-side statistics on an AP, run the **reset statistics** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**ssid** *ssid*] command. Alternatively, you can run **reset statistics all** the command to clear statistics on all APs.

11.2.71 display ap provision

Function

The **display ap provision** command displays the configurations for an AP to go online.

Format

display ap provision ap-id *ap-id*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you set parameters for an AP to go online in the AP view, you can run this command to view the detailed configuration.

Example

Display configurations in the AP view.

```
<HUAWEI> display ap provision ap-id 0
--------------------------------------------------------------------------------
AP name                  : area_1
AP group                 : default
AP address mode          : static
IPv4 address             : -
IPv4 mask address        : -
IPv4 gateway address     : -
IPv4 AC list             : -
Management Vlan          : 2
DTLS server-auth         : enable
DTLS server-auth cn list : -
--------------------------------------------------------------------------------
```

Table 11-80 Description of the **display ap provision ap-id** *ap-id* command output

Item	Description
AP name	AP name. To configure this parameter, run the **ap-name (AP view)** command.
AP group	AP group to which an AP belongs. To configure this parameter, run the **ap-group (AP view)** command.
AP address mode	Mode in which an AP obtains an IP address. To configure this parameter, run the **address-mode (AP view)** command.
IPv4 address	Static IPv4 address of an AP. To configure this parameter, run the **ip-address (AP view)** command.
IPv4 mask address	Static IPv4 mask of an AP. To configure this parameter, run the **ip-address (AP view)** command.
IPv4 gateway address	IPv4 gateway address of an AP. To configure this parameter, run the **ip-address (AP view)** command.
IPv4 AC list	AC IPv4 address list for APs. To configure this parameter, run the **ac-list (AP view)** command.
Management Vlan	Management VLAN tag carried in CAPWAP packets sent from the AP's wired interface. To configure this parameter, run the **management-vlan** command.
DTLS server-auth	Whether the AC authentication function is enabled for the AP. To restore the default value, run the **undo capwap dtls server-auth (AP view)** command. To enable or disable this function, run the **capwap dtls server-auth (AP provisioning view)** command and run the **commit** command to deliver the configuration.

Item	Description
DTLS server-auth cn list	CN field used by APs to verify an AC's certificate. To restore the default value, run the **undo capwap dtls server-auth cn (AP view)** command. To configure the CN field, run the **capwap dtls server-auth cn (AP provisioning view)** command and run the **commit** command to deliver the configuration.

11.2.72 display ap pki certificate

Function

The **display ap pki certificate** command displays AP certification information.

Format

display ap pki certificate ap-id *ap-id* { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays certificate information about the AP with a specified ID.	The AP ID must exist.
ca	Displays information about the CA certificate.	-
local	Displays information about the local certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate.	The value must be an existing PKI realm name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap pki certificate** command to view information about the CA or local certificate of a specified AP.

Example

Display information about the CA certificate of AP 1 in the PKI realm **abc**.

```
<HUAWEI> display ap pki certificate ap-id 1 ca realm abc
Info: This operation may take a few seconds. Please wait for a moment...done.
------------------------------------------------------------------------------
Serial Number: 0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
Issuer: CN=ca_root
Validity
    Not Before: Jun  4 14:58:17 2015 GMT
    Not After : Jun  4 15:07:10 2020 GMT
Subject: CN=ca_root
------------------------------------------------------------------------------
Total: 1
```

Table 11-81 Description of the **display ap pki certificate** command output

Item	Description
Serial Number	Serial number of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.
Subject	Subject of a certificate. The subject includes the following attributes: C: country code of a PKI entity. ST: name of the state or province to which a PKI entity belongs. L: geographic area where a PKI entity is located. O: organization to which a PKI entity belongs. OU: department to which a PKI entity belongs. CN: common name of a PKI entity.

11.2.73 display ap pki status

Function

The **display ap pki status** command displays an AP PKI realm and the certificate file status in the PKI realm.

Format

display ap pki status [**ap-id** *ap-id*]

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays the AP PKI realm by specifying an AP ID and the certificate file status in the PKI realm.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap pki status** command to view the AP PKI realm and the certificate file status in the PKI realm.

Example

Display all AP PKI realms and the certificate file status in the PKI realms.

```
<HUAWEI> display ap pki status
------------------------------------------------------------
AP-ID REALM1      REALM2   REALM3    REALM4   REALM5
------------------------------------------------------------
0     default/ok test/nok  -/-       -/-       -/-
1     default/ok test/ok  web/nok   -/-       -/-
2     default/ok test/ok  -/-       -/-       -/-
3     default/ok test/ok  web/ok    8021x/ok -/-
4     -/-        -/-      -/-       -/-       -/-
```

Display a specified AP PKI realm and the detailed certificate file status in the PKI realm.

```
<HUAWEI> display ap pki status ap-id 1
apid                                        : 1
realm1                                      : default
ca file           : 1.txt            status   : exist
local file        : 2.txt            status   : exist
private key file  : 3.txt            status   : exist
CRL file          : 4.txt            status   : exist
realm2                                      : test
ca file           : 1.txt            status   : exist
local file        : 2.txt            status   : exist
private key file  : 3.txt            status   : exist
CRL file          : 4.txt            status   : exist
realm3                                      : web
ca file           : 1.txt            status   : exist
local file        :                  status   :
private key file  : 3.txt            status   : exist
CRL file          : 4.txt            status   : exist
realm4                                      :
ca file           :                  status   :
local file        :                  status   :
private key file  :                  status   :
CRL file          :                  status   :
```

```
realm5                                        :
ca file              :                  status   :
local file           :                  status   :
private key file     :                     status   :
CRL file             :                  status   :
```

Table 11-82 Description of the **display ap pki status** command output

Item	Description
AP-ID	AP ID.
REALMX	Name of a PKI realm. The value can be **ok** or **nok**. **ok** indicates that the file is loaded, and **nok** indicates that the file is not loaded.
apid	AP ID.
realmx	Name of a PKI realm.
ca file	CA certificate file.
local file	Local certificate file.
private key file	Private key file.
CRL file	CRL file.
status	Certificate loading status.

11.2.74 display ap port

Function

The **display ap port** command displays the AP port status and traffic information.

Format

display ap port { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* }

Parameters

Parameter	Description	Value
all	Displays port status and traffic information of all APs.	-
ap-name *ap-name*	Displays port status and traffic information of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays port status and traffic information of the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-mac *ap-mac*	Displays port status and traffic information of the AP with a specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap port** command to check the port status and traffic information of online APs, which facilitates AP port maintenance and management.

Example

Display the port status and traffic information of all APs.

```
<HUAWEI> display ap port all
Info: Waiting for AP response.
------------------------------------------------------------------------------------------------------------------------------
-----
AP-ID Port   Trunk ID    State Mode Speed Duplex TX-Packets       Tx-ErrorPackets  TX-Rate(Kbps) RX-
Packets       RX-DropPackets   RX-Rate(Kbps)
------------------------------------------------------------------------------------------------------------------------------
-----
0     GE0    0(active)   up    root 1000  full   9178           0            0          12857          0             1
......
------------------------------------------------------------------------------------------------------------------------------
-----
Printed: 1
```

Table 11-83 Description of the **display ap port** command output

Item	Description
AP-ID	AP ID.
Port	AP port.

Item	Description

Trunk ID	Whether the Eth-Trunk function is configured on the AC and whether the AP port is added to an Eth-Trunk.
	- The field outside parentheses indicates the configuration on the AC.
	  – 0: The AC is configured to add AP ports to Eth-Trunk 0.
	  – -: The AC is not configured to add AP ports to an Eth-Trunk.
	- The field in parentheses indicates the effective configuration on the AP.
	  – -: The AP port does not support the Eth-Trunk function.
	  – active: The AP port has been added to an Eth-Trunk.
	  – inactive: The AP port is not added to an Eth-Trunk.
	The entire field is described as follows:
	- 0(active): The AP port is added to Eth-Trunk 0, and this configuration is in effect.
	- 0(inactive): The AC is configured to add AP ports to Eth-Trunk 0, but this configuration takes effect only after a restart. The current AP port is not in an Eth-Trunk.
	- 0(-): The AC is configured to add AP ports to Eth-Trunk 0, but the current AP port does not support the Eth-Trunk function.
	- -(-): The current AP port does not support the Eth-Trunk function, and the AC is not configured to add AP ports to an Eth-Trunk.
	- -(active): The AC is configured to remove AP ports from an Eth-Trunk, but this configuration takes effect only after a restart. The current AP port is still in an Eth-Trunk.
	- -(inactive): The AP port is configured to leave an Eth-Trunk, and this configuration is in effect.

State	Status of the AP port. - down: The AP port is Down. - up: The AP port is Up.
Mode	Working mode of the AP port. - root - middle - endpoint
Speed	Speed of the AP port, in Mbit/s.

Item	Description
Duplex	Duplex mode of the AP port, which includes the half-duplex and full-duplex modes.
TX-Packets	Number of data frames sent by the AP port.
Tx-ErrorPackets	Number of error data frames sent by the AP port.
TX-Rate(Kbps)	Uplink rate of the AP port.
RX-Packets	Number of data frames received by the AP port.
RX-DropPackets	Number of discarded data frames that are received by the AP port.
RX-Rate(Kbps)	Downlink rate of the AP port.

11.2.75 display ap power-workmode

Function

The **display ap power-workmode** command displays the current power mode of APs.

Format

display ap power-workmode { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *ap-group* }

Parameters

Parameter	Description	Value
all	Displays the current power mode of all APs.	-
ap-name *ap-name*	Displays the current power mode of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the current power mode of the AP with a specified ID.	The AP ID must exist.
ap-mac *ap-mac*	Displays the current power mode of the AP with a specified MAC address.	The AP's MAC address must exist.
ap-group *ap-group*	Displays the current power mode of APs in a specified AP group.	The AP group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an AP is supplied with DC or PoE power, the AP may work in low-power mode if the power fails to meet requirements. You can run this command to view the current power mode of the AP and verify that the current power mode can enable the AP to work with all functions.

Example

Display the current power mode of all APs.

```
<HUAWEI> display ap power-workmode all
--------------------------------------------------------------------------------------------------------------------------------------
-----
ID    MAC            Name   Group    Power-workmode     Decided by
--------------------------------------------------------------------------------------------------------------------------------------
-----
0     00e0-fc76-e360   ap_1    default   AT(Limited)       LLDP
--------------------------------------------------------------------------------------------------------------------------------------
-----
Total: 1
```

Table 11-84 Description of the **display ap power-workmode** command output

Item	Description
ID	AP ID.
MAC	AP's MAC address.
Name	AP name.
Group	AP group to which an AP belongs.

Item	Description
Power-workmode	Current power mode of an AP. - The power mode of an AP can be AF, AT, BT60, or BT90, which presents 802.3af, 802.3at, 802.3bt Class 6, and 802.3bt Class 8, respectively. - The working mode of an AP can be Normal, Limited, or Insufficient. In Normal mode, functions of the AP are unrestricted. In Limited mode, functions of the AP are partially restricted. In Insufficient mode, the AP restarts due to insufficient power supply, and you are not advised to use the AP in this mode. Limited: For impact on AP services by insufficient power supply. Visit **Info-Finder**, select a product series, and view hardware specifications in the hardware center. You can check the power supply downgrade limits at different power supply levels. Insufficient: Check the power supply capability of the PSE or contact technical support personnel. If the value of **Power-workmode** is **AF(Insufficient)** and the AP restarts for 10 consecutive times within a short period, the possible cause is that the power supply of the AP is insufficient. After the AP restarts for the eleventh time, it enters the AF power mode. One hour later, the AP automatically restarts and restores the original power mode. During the waiting period, you can check whether the PSE power supply is stable and replace the PSE power supply if it is unstable.
Decided by	The current power mode of an AP is determined by: - LLDP: LLDP negotiation result - Hardware detect: hardware detection result - AP capability: its own highest capability - Configuration: **power force work-mode** command configuration

11.2.76 display ap power

Function

The **display ap power** command displays power supply information about an AP.

Format

display ap power { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays power supply information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays power supply information about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check power supply information about an AP, including the power supply mode, rated voltage, and rated power.

Power supply information query is supported only by the AirEngine 9700D-M and AirEngine 9700D-S.

Example

Display power supply information about AP **0**.

```
<HUAWEI> display ap power ap-id 0
--------------------------------------------------------------------------------
PowerNo   Present  Mode  State   Voltage(V)  Power(W)
--------------------------------------------------------------------------------
PWRI      YES      AC    Normal  56          1000
--------------------------------------------------------------------------------
```

Table 11-85 Description of the **display ap power** command output

Item	Description
PowerNo	Number of a power module.
Present	Whether a power module is in position. ● YES: The power module is in position. ● NO: The power module is not in position.
Mode	Power supply mode of a power module. ● DC: DC power supply ● AC: AC power supply
State	Power supply status of a power module. ● Normal: The power module has current output. ● Abnormal: The power module has no current output.
Voltage(V)	Rated voltage of a power module (V).
Power(W)	Rated power of a power module (W).

11.2.77 display ap resource

Function

The **display ap resource** command displays the number of CAPWAP tunnel resources used by APs on a device.

Format

display ap resource slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a device.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the number of CAPWAP tunnel resources used by APs on a device.

Example

Display the number of CAPWAP tunnel resources used by APs on a device.

```
<HUAWEI> display ap resource slot 0
  Slot  0
------------------------------------------------------------------------
  Number Used :0
  Number Free : 1024
  Number Total: 1024
------------------------------------------------------------------------
```

Table 11-86 Description of the **display ap resource slot** *slot-id* command output

Item	Description
Number Used	Number of CAPWAP tunnel resources used by APs.
Number Free	Number of available CAPWAP tunnel resources.
Number Total	Total number of CAPWAP tunnel resources on the device.

11.2.78 display ap run-info

Function

The **display ap run-info** command displays the running status of an AP.

Format

display ap run-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the running status of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the running status of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays the AP running status. You can run this command to monitor an AP in real time.

Prerequisites

The AP works properly.

Example

Display the running status of the AP named **example**.

```
<HUAWEI> display ap run-info ap-name example
--------------------------------------------------------------------------------
AP type                      : AirEnginexxxx
Country code                 : CN
Software version             : V200R023C00
Hardware version             : Ver.A
BIOS version                 : 623
BOM version                  : 000
Memory size(MB)              : 256
Flash size(MB)               : 64
SD Card size(MB)             : -
Manufacture                  : Huawei Technologies Co., Ltd.
Software vendor              : Huawei Technologies Co., Ltd.
Online time(ddd:hh:mm:ss)    : 6H:56M:26S
Run time(ddd:hh:mm:ss)       : 6H:59M:51S
NAT IP address               : 2.2.2.1
IP address                   : 192.168.109.252
IP mask                      : 255.255.255.0
Gateway                      : 192.168.109.1
DNS server                   : 0.0.0.0
AP mode                      : campus
USB                          : enable(2.5w)
PoE                          : disable
GigabitEthernet port 0
  Port speed(Mbps)           : 1000
  Port speed mode            : auto
  Port duplex                : full
```

```
  Port duplex mode            : auto
  Port state                  : down
  STP down recovery time(ddd:hh:mm:ss)         : -
GigabitEthernet port 1
  Port speed(Mbps)            : 1000
  Port speed mode             : auto
  Port duplex                 : full
  Port duplex mode            : auto
  Port state                  : up
  STP down recovery time(ddd:hh:mm:ss)         : -
......
Card status                   : slot usb: -
------------------------------------------------------------------------------
```

Table 11-87 Description of the **display ap run-info** command output

Item	Description
AP type	AP type.
Country code	Country code.
Software version	Software version of an AP.
Hardware version	Hardware version of an AP.
BIOS version	BIOS version of an AP.
BOM version	BOM version of an AP.
Memory size(MB)	Memory size of an AP, in MB.
Flash size(MB)	Flash memory size of an AP, in MB.
SD Card size(MB)	SD card size of an AP, in MB.
Manufacture	Manufacturer of an AP.
Software vendor	AP software manufacturer.
Online time(ddd:hh:mm:ss)	AP online duration.
Run time(ddd:hh:mm:ss)	Running duration of an AP.
NAT IP address	This item is displayed only when the AP is on the private network and the AC is on the public network in NAT scenarios. The value of this parameter is the translated public IP address of the AP.
IP address	AP IPv4 address.
IP mask	IP address mask of an AP.
Gateway	Gateway IP address of an AP.
DNS server	IP address of the DNS server.

Item	Description
AP mode	AP mode. campus: The AP is not added to a branch group.
USB	Whether USB is enabled. ● disable: This function is disabled. ● enable(2.5w): USB is enabled and works at the 2.5 W power. ● enable(5w): USB is enabled and works at the 5 W power. ● -: USB is not supported.
PoE	Status of the PoE function on the interface. ● disable: This function is disabled. ● enable: This function is enabled. ● -: PoE is not supported.
XGigabitEthernet port *number*	ID of the AP's XGigabitEthernet port. This item is displayed only for an AP with an XGigabitEthernet port.
MultiGE port *number*	ID of the AP's MultiGE port. This item is displayed only for an AP with a MultiGE port.
GigabitEthernet port *number*	ID of the AP's Ethernet interface.
Ethernet port *number*	Number of the AP's Ethernet port. This item is displayed only for an AP with an Ethernet port.
Port speed(Mbps)	Rate on the upstream Ethernet interface, in Mbit/s.
Port speed mode	Rate mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.
Port duplex	Duplex type of the upstream Ethernet interface, including full duplex and half duplex.
Port duplex mode	Duplex mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.

Item	Description
Port state	AP interface status. - down: indicates that the interface is disabled. - up: indicates that the interface is enabled. - admin shutdown: indicates that the interface is shut down. - stp shutdown: indicates that STP on the interface is disabled.
STP down recovery time(ddd:hh:mm:ss)	Remaining recovery time of the STP.
Card status	IoT card status. - -: indicates that the IoT card is not in position. - present: indicates that the IoT card is in position.

11.2.79 display ap service-config acl

Function

The **display ap service-config acl** command displays the ACL configuration on a specified AP.

Format

display ap service-config acl { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the ACL configuration on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the ACL configuration on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can determine which ACLs have been delivered to the AP based on the command output, which helps locate and troubleshoot faults about user rights.

Example

Display the ACL configuration on AP **hello**.

```
<HUAWEI> display ap service-config acl ap-name hello
--------------------------------------------------------------------------------
Index          ACL number
--------------------------------------------------------------------------------
1             3000
2             3002
3             3015
4             3022
5             3030
--------------------------------------------------------------------------------
Total: 5
```

Table 11-88 Description of the **display ap service-config acl** command output

Item	Description
Index	Index.
ACL number	ACL number configured on an AP.
IPv6 ACL number	ACL6 number configured on an AP.

11.2.80 display ap traffic statistics wireless

Function

The **display ap traffic statistics wireless** command displays statistics about packets with the specified SSID on the radio of an AP.

Format

display ap traffic statistics wireless { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* [**ssid** *ssid*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio-id*	Specifies the radio ID.	The radio ID must exist.
ssid *ssid*	Specifies the SSID that STAs associate with.	The value must be an existing SSID.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap traffic statistics wireless** command to view statistics about packets with the specified SSID on the radio of an AP.

After an AP performs self-healing, packet statistics on the AP radios are cleared.

The values of some command output items are displayed as 0 due to different function support specifications.

Example

Display statistics about packets with the SSID **cmcc** on radio 0 of the AP 0.

```
<HUAWEI> display ap traffic statistics wireless ap-id 0 radio 0 ssid cmcc
------------------------------------------------------------------
Wireless bytes(RX)           : 14583149
Wireless error frames(RX)    : 10
Wireless frames(RX)          : 97419
Wireless unicast frames(RX)  : 16
Wireless dropped frames(RX)  : 0
Wireless bytes(TX)           : 1725974
Wireless error frames(TX)    : 6
Wireless frames(TX)          : 9704
Wireless unicast frames(TX)  : 9680
Wireless dropped frames(TX)  : 6
Wireless retransmitted frames: 32674
Current accessed STA number  : 0
------------------------------------------------------------------
```

Table 11-89 Description of the **display ap traffic statistics wireless** { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* **ssid** *ssid* command output

Item	Description
Wireless bytes(RX)	Total number of bytes of data frames received by the radio.
Wireless error frames(RX)	Total number of received error frames.

Item	Description
Wireless frames(RX)	Total number of received frames.
Wireless unicast frames(RX)	Total number of received unicast frames.
Wireless dropped frames(RX)	Total number of received frames that are discarded.
Wireless bytes(TX)	Total number of bytes of data frames sent by the radio.
Wireless error frames(TX)	Total number of transmitted error frames.
Wireless frames(TX)	Total number of transmitted frames.
Wireless unicast frames(TX)	Total number of transmitted unicast frames.
Wireless dropped frames(TX)	Total number of transmitted frames that are discarded.
Wireless retransmitted frames	Total number of retransmitted frames.
Current accessed STA number	Number of STAs that connect to the AP normally.

Display packet statistics on radio 0 of the AP 0.

```
<HUAWEI> display ap traffic statistics wireless ap-id 0 radio 0
----------------------------------------------------------------------
Wireless frames(RX)                              :506379
Wireless bytes(RX)                               :76567129
Wireless error frames(RX)                        :113998
Wireless physical layer error frames(RX)         :0
Wireless MIC error frames(RX)                    :0
Wireless private key and decrypt fail frames(RX) :0
Wireless unicast frames(RX)                      :30
Wireless management frames(RX)                   :506379
Wireless data frames(RX)                         :0
Wireless frames(TX)                              :4949
Wireless bytes(TX)                               :855879
Wireless RTS successes(TX)                       :0
Wireless unicast frames(TX)                      :4587
Wireless broadcast frames(TX)                    :355
Wireless failure frames(TX)                      :3406
Wireless management frames(TX)                   :4725
Wireless data frames(TX)                         :0
Wireless noise(dBm)                              :-100
Wireless port up rate(Kbps)                      :40
Wireless port down rate(Kbps)                    :1
Wireless port PS-Poll Frames                     :0
Wireless port Association Request                :0
Wireless port Association Response               :0
Wireless port ReAssociation Request              :0
Wireless port ReAssociation Response             :0
Wireless port Disassociation Frames              :0
Wireless port Deauthentication Frames            :0
Wireless retry frames                            :515
Wireless PER(%)                                  :0
```

```
Wireless PER of the last 5min(%)                   :0
Wireless port PLR(%)                          :0
Wireless port PLR of the last 5min(%)               :0
Wireless retransmitted rate(%)                   :0
Wireless retransmitted rate of the last 5min(%)       :0
Wireless channel utilization(%)                   :96
WMM AC_BE retry ratio(%)                       :0
WMM AC_BK retry ratio(%)                       :0
WMM AC_VI retry ratio(%)                       :0
WMM AC_VO retry ratio(%)                        :0
WMM AC_BE PLR(%)                             :0
WMM AC_BK PLR(%)                             :0
WMM AC_VI PLR(%)                             :0
WMM AC_VO PLR(%)                              :0
------------------------------------------------------------------------
```

Table 11-90 Description of the **display ap traffic statistics wireless** { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* command output

Item	Description
Wireless frames(RX)	Total number of data frames and management frames received by the radio.
Wireless bytes(RX)	Total number of bytes of data frames received by the radio.
Wireless error frames(RX)	Total number of error frames received by the radio.
Wireless physical layer error frames(RX)	Number of error frames received at the physical layer of the radio.
Wireless MIC error frames(RX)	Number of frames with message integrity code (MIC) received by the radio.
Wireless private key and decrypt fail frames(RX)	Number of frames with incorrect keys received by the radio.
Wireless unicast frames(RX)	Total number of received unicast frames.
Wireless management frames(RX)	Number of management frames received by the radio.
Wireless data frames(RX)	Number of data frames received by the radio.
Wireless frames(TX)	Total number of transmitted frames.
Wireless bytes(TX)	Total number of bytes of data frames sent by the radio.
Wireless RTS successes(TX)	Number of Request to Send (RTS) frames that are successfully sent by the radio.

Item	Description
Wireless unicast frames(TX)	Total number of transmitted unicast frames.
Wireless broadcast frames(TX)	Number of broadcast frames sent by the radio.
Wireless failure frames(TX)	Number of frames that the radio fails to send.
Wireless management frames(TX)	Number of management frames sent from the radio.
Wireless data frames(TX)	Number of data frames sent from the radio.
Wireless noise(dBm)	Radio noise level, in dBm.
Wireless port up rate(Kbps)	Upstream rate of the radio, in kbit/s.
Wireless port down rate(Kbps)	Downstream rate of the radio, in kbit/s.
Wireless port PS-Poll Frames	Number of data frames sent by the STA working in power saving mode.
Wireless port Association Request	Number of Association Request frames.
Wireless port Association Response	Number of Association Response frames.
Wireless port ReAssociation Request	Number of Reassociation Request frames.
Wireless port ReAssociation Response	Number of Reassociation Response frames.
Wireless port Disassociation Frames	Number of Disassociation frames.
Wireless port Deauthentication Frames	Number of Deauthentication frames.
Wireless retry frames	Number of frames that are retransmitted by the radio.
Wireless PER(%)	Packet error rate of the radio.
Wireless PER of the last 5min(%)	Packet error rate of the radio in the previous statistical period (5 minutes).
Wireless port PLR(%)	Packet loss ratio of the radio.
Wireless port PLR of the last 5min(%)	Packet loss rate of the radio in the previous statistical period (5 minutes).
Wireless retransmitted rate(%)	Retransmission rate of the radio.

Item	Description
Wireless retransmitted rate of the last 5min(%)	Retransmission rate of the radio in the previous statistical period (5 minutes).
Wireless channel utilization(%)	Channel utilization of the radio. **NOTE** When an AP radio works in monitor mode, this parameter is displayed as **-**.
WMM AC_BE retry ratio(%)	Retransmission ratio of AC_BE packets in the WMM queue.
WMM AC_BK retry ratio(%)	Retransmission rate of AC_BK packets in the WMM queue.
WMM AC_VI retry ratio(%)	Retransmission ratio of AC_VI packets in the WMM queue.
WMM AC_VO retry ratio(%)	Retransmission ratio of AC_VO packets in the WMM queue.
WMM AC_BE PLR(%)	Packet loss rate of AC_BE packets in the WMM queue.
WMM AC_BK PLR(%)	Packet loss rate of AC_BK packets in the WMM queue.
WMM AC_VI PLR(%)	Packet loss rate of AC_VI packets in the WMM queue.
WMM AC_VO PLR(%)	Packet loss rate of AC_VO packets in the WMM queue.

11.2.81 display ap uncontrol all

Function

The **display ap uncontrol all** command displays information about all uncontrolled APs that are not managed by the local AC.

Format

display ap uncontrol all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about all uncontrolled APs. The command output includes channel of the controlled AP closest to the uncontrolled AP and the strength of signals that the controlled AP received from the uncontrolled AP.

Example

View information about all uncontrolled APs.

```
<HUAWEI> display ap uncontrol all
---------------------------------------------------------
BSSID          NEAREST-AP      CHANNEL  RSSI(dBm)   SSID
---------------------------------------------------------
00e0-fc76-e360 ap-13           149      -68         test
---------------------------------------------------------
Total: 1
```

Table 11-91 Description of the **display ap uncontrol all** command output

Item	Description
BSSID	BSSID of an uncontrolled AP.
NEAREST-AP	Name of the controlled AP that is closest to the uncontrolled AP.
CHANNEL	Channel on which the uncontrolled AP is detected. If a rogue AP is detected on multiple channels, the channel with the strongest signal strength is displayed.
RSSI(dBm)	Strength of signals that the closest controlled AP receives from the uncontrolled AP, in dBm.
SSID	SSID of an uncontrolled AP.

11.2.82 display ap update configuration

Function

The **display ap update configuration** command displays AP upgrade configuration.

Format

display ap update configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the AP upgrade configuration, including the upgrade mode, FTP server configuration, and SFTP server configuration.

Example

Display the AP upgrade configuration.

```
<HUAWEI> display ap update configuration
------------------------------------------------------------------------------
AP update mode         : AC-mode
FTP configuration
 FTP IPv4 address      : -
 FTP IPv4 port         : 21
 FTP IPv4 username     :
 FTP IPv4 password     :
 FTP IPv4 max number   : 50
SFTP configuration
 SFTP IPV4 address     : -
 SFTP IPv4 port        : 22
 SFTP IPV4 username    :
 SFTP IPV4 password    :
 SFTP IPV4 max number  : 50
AP update schedule-task
 ap update schedule-task task-id 1 start-time 11:11 2017/1/1 stop-time 11:12 201 7/1/1 ap-type 54
AP type/AP-group update filename/patch filename
 AirEngine6760R-51     : AirEngineX760-V200R019C10.cc/-
------------------------------------------------------------------------------
```

Table 11-92 Description of the **display ap update configuration** command output

Item	Description
AP update mode	AP upgrade mode. ● AC-mode: indicates the AC mode. ● FTP-mode: indicates the FTP mode. ● SFTP-mode: indicates the SFTP mode. To configure this parameter, run the **ap update mode** command.
FTP configuration	FTP server configuration.

Item	Description
FTP IPv4 address	IPv4 address of the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 port	IPv4 port number of the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 username	IPv4 user name for logging in to the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 password	IPv4 password for logging in to the FTP server. To configure this parameter, run the **ap update ftp-server** command.
FTP IPv4 max number	Maximum number of APs that can be upgraded simultaneously when an IPv4 address is used to access the FTP server. To configure this parameter, run the **ap update ftp-server** command.
SFTP configuration	SFTP server configuration.
SFTP IPv4 address	IPv4 address of the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
SFTP IPv4 port	IPv4 port number of the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
SFTP IPv4 username	IPv4 user name for logging in to the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
SFTP IPv4 password	IPv4 password for logging in to the SFTP server. To configure this parameter, run the **ap update sftp-server** command.

Item	Description
SFTP IPv4 max number	Maximum number of APs that can be upgraded simultaneously when an IPv4 address is used to access the SFTP server. To configure this parameter, run the **ap update sftp-server** command.
AP update schedule-task	ID of a scheduled AP upgrade task. To configure this parameter, run the **ap update schedule-task** command.
AP type/AP-group update filename/ patch filename	Name of the upgrade file/name of the patch file for a specified AP type or group. To configure this parameter, run the **ap update update-filename** and **ap-patch update update-filename** commands.

11.2.83 display ap update schedule-task

Function

The **display ap update schedule-task** command displays information about scheduled AP upgrade tasks.

Format

display ap update schedule-task

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view information about scheduled AP upgrade tasks, and run the **undo ap update schedule-task** { **all** | **task-id** *task-id* } command to delete the scheduled tasks that have been completed or are not needed.

Example

Display information about scheduled AP upgrade tasks.

```
<HUAWEI> display ap update schedule-task
--------------------------------------------------------------------------------
 Task-ID  Task-State  Start-Time        Stop-Time         AP-Type  AP-Group
--------------------------------------------------------------------------------
 1        IDLE        2020/01/01 11:11  2020/01/02 11:12  125      -
--------------------------------------------------------------------------------
```

Table 11-93 Description of the **display ap update schedule-task** command output

Item	Description
Task-ID	ID of a scheduled AP upgrade task.
Task-State	Status of the scheduled AP upgrade task. ● DEAD: The start time of the task is earlier than the system time, or the task stops unexpectedly. ● DONE: The task is executed. ● IDLE: The task has not been activated. ● OVERTIME: The task times out. ● RUNNING: The task is running. ● WAITING: The task is in waiting state because the start time of the task has reached but a task is running.
Start-Time	Start time of the scheduled AP upgrade task.
Stop-Time	End time of the scheduled AP upgrade task.
AP-Type	Type of the APs to be upgraded.
AP-Group	AP group to which the APs to be upgraded belong.

11.2.84 display ap update status

Function

The **display ap update status** command displays the progress of upgrading Fit APs through the current AC.

Format

display ap update status { **all** | **downloading** | **failed** | **succeed** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-type** *ap-type* | **ap-group** *ap-group* | **waiting** }

Parameters

Parameter	Description	Value
all	Displays upgrade progress of all APs.	-
downloading	Displays APs that are upgrading.	-
failed	Displays APs that failed to be upgraded.	-
succeed	Displays APs that have been successfully upgraded.	-
ap-name *ap-name*	Displays upgrade progress of the AP with a specified name.	The value is a string of 1 to 63 case-sensitive characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?), and cannot start or end with spaces or double quotation marks (" "). If the AP name contains spaces, the input name must start and end with a quotation mark ("), for example, "hello name1". The quotation marks at the beginning and end of the AP name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
ap-id *ap-id*	Displays upgrade progress of the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-type *ap-type*	Displays upgrade progress of APs of a specified type.	The value is an integer. To view all AP types, run the **display ap-type all** command.
ap-group *ap-group*	Displays upgrade progress of APs in a specified AP group.	The value is a string of 1 to 35 characters, which can be Chinese characters or Chinese + English characters. It cannot contain question marks (?) or slashes (/), and cannot start or end with spaces or double quotation marks (" "). If the AP group name contains spaces, the input name must start and end with a quotation mark ("), for example, **"hello name1"**. The quotation marks at the beginning and end of the AP group name occupy two characters in total. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
waiting	Displays APs waiting for an upgrade.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After APs are upgraded on the AC, you can run this command to view the AP upgrade progress or AP information by upgrade status.

Example

Display upgrade progress of all APs.

```
<HUAWEI> display ap update status all
FT  : File Type
N : Next startup
---------------------------------------------------------------------------------------------------------------------------
------
ID    Name      AP Type           AP Group AP MAC        FT       Update Version        Last Update Time
Update Status
---------------------------------------------------------------------------------------------------------------------------
------
0     hw0       AirEngine5760-22WD default  00e0-fc76-e320 FIT       V200R019C10SPC200B002
2020-05-19/10:11:04     succeed
1     hw1       AirEngine6760R-51  default  00e0-fc76-e340 FIT       -                    -                    -
2     hw2       AirEngine6760R-51E default  00e0-fc76-e360 FIT       V200R019C10SPC100B195
2020-05-18/19:15:41     downloading(progress: 80%/0%)
3     hw3       AirEngine9700D-M   default  00e0-fc76-e380 FIT       V200R019C10SPC200B002
2020-05-19/16:37:50     downloading(progress: 100%/50%)
---------------------------------------------------------------------------------------------------------------------------
------
Total: 4
```

Table 11-94 Description of the **display ap update status all** command output

Item	Description
ID	AP ID.
Name	AP name.
AP Type	AP type.
AP Group	AP group.
AP MAC	MAC address of an AP.
FT	Type of the AP upgrade file. **PATCH(N)** indicates that the patch is specified for next startup.
Update Version	Target version to which an AP is upgraded.
Last Update Time	Last end time when an AP is upgraded.
Update Status	AP upgrade status. For details about the upgrade status and its corresponding handling suggestions, see **Table 11-95**.

Table 11-95 AP upgrade status and handling suggestions

AP Upgrade Status	Description	Handling Suggestion
Waiting download	The AP is waiting for an upgrade.	No action is required.
downloading(progress: *x* %/*y*%)	*x*% indicates the download progress of the system software package, and *y*% indicates the progress of writing the system software package to the flash memory.	No action is required.
failed(AC global caching)	The upgrade failed. ● When an AP is downloading system software package during an in-service upgrade, the system displays this message if the AP starts automatic upgrade which triggers a new process for downloading the software package. ● When multiple RUs automatically upgrade at the same time, this message may also be displayed. **NOTE** In this situation, the actual RU upgrade result depends on that displayed in the **display ap update status all** command output.	Wait until the online upgrade is completed.
failed(alloc memory for file)	The upgrade failed because the AP failed to apply for memory resources.	Clear the memory of the AC, and ensure that the memory is sufficient for the AP upgrade.
failed(AP is updating now. Please wait.)	The AC delivers an upgrade instruction again when the AP is running an upgrade task.	The AP is upgrading. Wait until the upgrade is complete. If the status persists after 5 minutes, run the upgrade command again.

AP Upgrade Status	Description	Handling Suggestion
failed(AP type in the EFS mismatch)	The upgrade failed because the AP type in the EFS file trailer of the current AP version does not match the AP.	The upgrade file is incorrect. Replace the upgrade file.
failed(AP type mismatch with batch upgrade AP type)	The upgrade failed because the AP type is different from the batch upgrade AP type.	Upgrade the AC version. If the problem persists, contact technical support personnel.
failed(AP wait for fragmentation timeout)	The upgrade failed because the time that the AP waits for fragment data expired.	Check the network connection.
failed(block full)	The upgrade failed because the number of APs simultaneously upgraded in AC mode reaches the maximum.	The number of concurrent upgrades exceeds the maximum. Wait until the upgrade of other APs is complete.
failed(change to standby)	The upgrade failed due a revertive switchover failure.	Wait until the active/ standby switchover is complete.
failed(fail to download the file)	The upgrade failed because the system software failed to be downloaded.	Check whether the network connection is normal or the system software package exists.
failed(file content error)	The upgrade failed due to incorrect system software file contents.	The upgrade file is incorrect. Replace the upgrade file.
failed(file version inconsistent)	The upgrade failed because the AP type in the EFS file trailer does not match the AP type contained in the system software package name.	The upgrade file is incorrect. Replace the upgrade file or upgrade the AC to the latest version.
failed(invalid file name)	The upgrade failed because the name of the AP version file is incorrect.	Ensure that the file name of the software package meets the specified requirement.
failed(link down)	The upgrade failed because the AP failed to communicate with the AC.	Check the network connection.

AP Upgrade Status	Description	Handling Suggestion
failed(mode changed)	The upgrade failed because the AP upgrade mode is changed during the AP automatic upgrade.	This is a normal process. Perform the upgrade again.
failed(nospace in AP memory)	The upgrade failed because the AP memory resources were insufficient.	Ensure that the AP memory can support the upgrade.
failed(not receive update result)	The upgrade failed because the AC receives no AP upgrade result.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(over max upgrade time)	The upgrade failed because the upgrade duration exceeds the maximum upgrade time allowed.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(server password is too long)	The upgrade failed because the FTP/SFTP server password is too long.	Change the password of the FTP/SFTP server to a value with a length less than the maximum.
failed(read file)	The upgrade failed because no upgrade file is available in the flash memory.	Check the upgrade file.
failed(receive file failed)	The upgrade failed because fragments failed to be received.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(retransfer over times)	The upgrade failed because the number of fragment retransmissions exceeds the threshold.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(send first file failed)	The upgrade failed because the first fragment failed to be sent.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(other reason)	The upgrade failed due to an unknown error.	Contact technical support personnel.

AP Upgrade Status	Description	Handling Suggestion
failed(upgrade timeout)	The upgrade timed out and failed.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(user canceled)	The upgrade failed because the user canceled the upgrade.	No action is required.
failed(waited for next batch)	The upgrade failed. The AP has to wait for the next upgrade.	No action is required.
failed(write flash error)	The upgrade failed because the system software package failed to be written to the flash memory.	Contact technical support personnel.
failed(file changed)	The upgrade failed because the upgrade file was modified during the automatic upgrade.	This is a normal process. Wait for the next upgrade.
failed(age time out)	The upgrade failed because the state machine aged out.	Check the network connection. If the network connection is normal, contact technical support personnel.
succeed	The upgrade succeeded.	No action is required.
succeed(auto resetting)	The upgrade succeeded and the AP is being automatically restarted.	No action is required.
succeed(need reset)	The upgrade succeeded. The AP must be restarted.	No action is required.
succeed(resetting)	The upgrade succeeded and the AP is being manually restarted.	No action is required.
succeed(no need to update)	The upgrade succeeded. There is no need to upgrade the AP.	No action is required.
succeed(need mode switch)	The upgrade succeeded. The AP mode needs to be switched.	No action is required.

AP Upgrade Status	Description	Handling Suggestion
failed(send upgrade configuration)	The upgrade failed because the upgrade configuration failed to be sent.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(send upgrade request)	The upgrade failed because the upgrade request failed to be sent.	Check the network connection. If the network connection is normal, contact technical support personnel.
failed(upgrade configuration response error)	The upgrade failed because there was an error in the AP's upgrade response.	Contact technical support personnel.
failed(process upgrade filename)	The upgrade failed because the AC failed to process the upgrade file name.	Contact technical support personnel.
failed(cannot get AP type)	The upgrade failed because the AC failed to obtain the AP type.	Contact technical support personnel.
failed(analyze the version by upgrade filename)	The upgrade failed because the device failed to analyze the version number in the file name.	Contact technical support personnel.
failed(state transition check failed for the update module)	The upgrade failed because the AC failed to check the status transition of the upgrade module.	Contact technical support personnel.
failed(flash component change)	The upgrade failed because the flash model is not supported.	Replace the device with one that supports the new flash memory model or contact technical support personnel.
failed(Backing up the system software)	The upgrade failed because the system software is being synchronized from the main area to the standby area.	Wait until the synchronization between the active and standby areas is complete.

AP Upgrade Status	Description	Handling Suggestion
failed (incompatible hardware BOM version)	The upgrade failed because the AP hardware of the target version is incompatible with the BOM version.	The AP does not support downgrade. No action is required.
failed(patch checksum error)	The upgrade failed because of a patch checksum error.	Check the integrity of the patch file.
failed(patch file error)	The upgrade failed because of a patch file error.	Check the integrity of the patch file.
failed (patch active failed)	The upgrade failed because of a failure to activate the patch.	Check whether the patch and the software package match with each other.
failed(vrp patch process active failed)	The upgrade failed because of a failure to activate the patch on the control plane.	Contact technical support personnel.
failed(vfp patch active failed)	The upgrade failed because of a failure to activate the patch on the forwarding plane.	Contact technical support personnel.
failed(kernel patch actived)	The upgrade failed because of a failure to activate the kernel patch.	Contact technical support personnel.
failed(patch inner proc error)	The upgrade failed because of an internal patch processing failure.	Contact technical support personnel.
failed(wifi target chip patch active failed)	The upgrade failed because of a failure to activate the Wi-Fi chip patch.	Contact technical support personnel.
failed(the current AP version does not support patch updates)	The upgrade failed because the AP version does not support the patch upgrade.	No action is required.
failed(insufficient space on the AP flash memory)	The upgrade failed due to insufficient space on the AP's flash memory.	Delete unnecessary files from the flash memory.

AP Upgrade Status	Description	Handling Suggestion
failed(nospace in AC memory)	The upgrade failed because the AC memory resources were insufficient.	Upgrade or restart the AP during off-peak hours.
failed(patch version mismatch)	The upgrade failed because the patch version does not match the AP version.	Check the patch version.
failed(The current AP version does not support the change of the FTP/SFTP server port.)	The upgrade failed because the FTP/SFTP port number of the AP cannot be changed.	Use the default FTP/SFTP port for the upgrade.
failed(The AP or AP version does not support the HOUP-based upgrade)	The upgrade failed because the current AP or AP version does not support the HOUP upgrade mode.	Use FTP or SFTP to perform the upgrade.
failed(The FTP server does not support the REST command)	The upgrade failed because the FTP server does not support REST commands.	Replace the FTP server.
failed(The AP version does not support the configuration for specifying the patch to take effect upon the next startup)	The upgrade failed because the current AP version does not support the configuration for specifying the patch for next startup.	When installing the patch, do not specify the parameter **next-startup** in the command.
failed(AP type not config)	The AP type is different from the AP type specified for the batch upgrade.	Perform the upgrade again or contact technical support personnel.
failed(The rate of the optical module does not match)	The upgrade failed because the rate of the optical module does not match.	The AP does not support downgrade. No action is required.
-	The AP requires no upgrade.	No action is required.

11.2.85 display ap update status partition

Function

The **display ap update status partition** command displays information about channel-based partitions.

Format

display ap update status partition { **all** | **partition-id** *partition-id* }

Parameters

Parameter	Description	Value
all	Displays information about all channel-based partitions.	-
partition-id *partition-id*	Displays information about the channel-based partition with a specified ID.	The value is an integer that ranges from 0 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ap update status partition** { **all** | **partition-id** *partition-id* } command displays information about the only that APs that need to be upgraded. The APs that need to be upgraded refer to those whose target version files have been loaded to the standby area and are waiting for reset.

Example

Display information about channel-based partition **1**.

```
<HUAWEI> display ap update status partition partition-id 1
PID : Partition ID
CH : Channel
----------------------------------------------------------------------------------------------------------------------------
----------------
PID  CH  AP ID  Name   AP Type          AP Group   AP MAC         Update Version     Last Update Time
Update Status
----------------------------------------------------------------------------------------------------------------------------
----------------
1    36  0      hw0    AirEngine6760R-51  default    00e0-fc76-e320  V200R019C10B035    2019/08/22 18:51
succeed(need reset)
2    100 1      hw1    AirEngine6760R-51  default    00e0-fc76-e340  V200R019C10B035    2019/08/22
18:51   succeed(need reset)
2    100 2      hw2    AirEngine6760R-51  default    00e0-fc76-e360  V200R019C10B035    2019/08/22
```

```
18:51   succeed(need reset)
255  -   4      hw4    AirEngine6760R-51  default    00e0-fc76-e3a0  V200R019C10B035    2019/08/22 18:51
succeed(need reset)
255  -   5      hw5    AirEngine6760R-51  default    00e0-fc76-e3c0  V200R019C10B035    2019/08/22 18:51
succeed(need reset)
------------------------------------------------------------------------------------------------------------------------
----------------
Total: 5
```

Table 11-96 Description of the **display ap update status partition** command output

Item	Description
PID	Channel-based partition ID. The value **255** indicates that a channel-based partition that does not work properly.
CH	Channel.
AP ID	AP ID.
Name	AP name.
AP Type	AP type.
AP Group	AP group.
AP MAC	AP's MAC address.
Update Version	Target version to which an AP is upgraded.
Last Update Time	Last end time when an AP is upgraded.
Update Status	AP upgrade status. For details about the upgrade status and its corresponding handling suggestions, see **Table 11-95**.

11.2.86 display ap username

Function

The **display ap username** command displays information about users logged in to the AP.

Format

display ap username

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap username** command to view information about users logged in to the AP.

Example

Display information about users logged in to the AP.

```
<HUAWEI> display ap username
----------------------------------------------------------------------------
AP username: admin
AP password: ******
Password control                  : Disable
Is original password              : YES
Password set time                  : 1970-01-01 00:00:00
  Password expiration              : Disable (90 days)
  Password history                : Disable  (5)
  Password alert before expiration : 30 days
  Password alert original          : Enable
  Password expired                : NO
----------------------------------------------------------------------------
```

Table 11-97 Description of the **display ap username** command output

Item	Description
AP username	User name for logging in to the AP. To configure this parameter, run the **ap username** command.
AP password	Password for logging in to the AP. To configure this parameter, run the **ap username** command.
Password control	Whether to enable the password policy function.
Is original password	Whether a password is the initial password.
Password set time	Password setting time
Password expiration	Password validity period.
Password history	Number of historical passwords recorded for each user.
Password alert before expiration	Number of password expiration prompt days.

Item	Description
Password alert original	Whether to enable the initial password change prompt function.
Password expired	Whether a password expires.

11.2.87 display ap version

Function

The **display ap version** command displays version information about APs.

Format

display ap version { **all** | { **ap-group** *ap-group-name* | **version-name** *version-name* } * }

Parameters

Parameter	Description	Value
all	Displays version information about all APs.	-
ap-group *ap-group-name*	Displays version information about all APs of a specified AP group.	The AP group must exist.
version-name *version-name*	Displays version information about a specified AP.	The value is string of 11 to 17 characters, in the format of **VxxxRxxxCxxx** or **VxxxRxxxCxxxSPCxxx**, for example, V200R006C00 or V200R005C10SPC200.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap version** command to check version information about APs.

Example

Display version information about all APs.

```
<HUAWEI> display ap version all
Backward compatible versions : V200R020 V200R021 V200R022
The forward compatible versions depend on the AP. For the specific versions, log in to the AP and run the
"display system-information" command.
--------------------------------------------------------------------------------------------
ID   Name           Group  Type                 Version          PatchVersion    state
--------------------------------------------------------------------------------------------
0    00e0-fc76-e360 default AirEngine8760-X1-PRO   V200R023C00      -              normal
--------------------------------------------------------------------------------------------
Total: 1
```

Table 11-98 Description of the **display ap version** command output

Item	Description
Backward compatible versions	Backward compatible version.
The forward compatible versions depend on the AP. For the specific versions, log in to the AP and run the "display system-information" command.	The forward compatible versions depend on the AP. You can log in to the AP and run the **display system-information** command to query the forward compatible versions.
ID	ID.
Name	AP name.
Group	AP group name.
Type	AP type.
Version	AP version name.
PatchVersion	AP patch version.
state	AP state. For details, see **Table 11-5**.

Table 11-99 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed (cmtfa)	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are performed for the AP. If the link between the AP and AC is disconnected or the peer end has no response, the AP enters the commit-failed state.	Check the network connection.
committing (cmt)	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are being delivered to the AP. During this process, the AP is in committing state.	This is a normal state, and no action is required.
config (cfg)	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. During this process, the AP is in config state.	This is a normal state, and no action is required.
config-failed (cfgfa)	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. If the configuration delivery fails due to various reasons (such as link disconnection), the AP enters the config-failed state.	Check the network connection.
download (dload)	An AP is in upgrade state.	When an AP is performing an upgrade, it enters the download state.	When the AP upgrade is complete, check the AP state.

AP State	Description	Possible Cause	Handling Suggestion
fault	An AP fails to go online.	An AP fails to go online, which is usually caused by the following: ● The AP fails to obtain an IP address or obtains an incorrect IP address. ● The network between the AP and AC is faulty. ● The AP fails to be authenticated. ● The number of APs on an AC has reached the maximum value. ● The AP is faulty. ● In dual-link cold backup or N+1 backup scenario, if the link between the active and standby ACs is established properly, an AP that goes online on the active AC is in fault state on the standby AC.	Handle the AP online failure. For details, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

AP State	Description	Possible Cause	Handling Suggestion
idle	It is the initialization state of an AP before it establishes a link with the AC for the first time.	When an AP has not established a CAPWAP link with the AC, the MAC address and SN of an AP that is added offline are different from the actual MAC address and SN of the AP, or the AC cannot manage an AP due to license resource insufficiency, the AP enters the idle state.	Perform the following operations. Check whether the AP is connected to the network. If the AP connection is normal, go to next step. Check the MAC address and SN of the AP that is added offline are different from the actual MAC address and SN of the AP. If not, perform the following operations: 1. Run the **display ap all** command to check AP information. 2. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** } command to delete the AP. 3. Run the **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] or **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] command to add correct AP information. If the fault persists, expand the license capacity. Note that RUs managed by the AC do not occupy

AP State	Description	Possible Cause	Handling Suggestion
			license resources of the AC.
name-conflicted (namec)	The name of an AP conflicts with that of an existing AP.	The name of an AP conflicts with the name of another AP that has been online on the same AC.	Run the **ap-rename ap-id** *ap-id* **new-name** *ap-new-name* command to change the AP name.
normal (nor)	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby (stdby)	An AP is in normal state on the standby AC.	In the HSB scenario, if the link between the master and backup ACs is established properly, an AP is in standby state on the backup AC and in normal state on the master AC.	This is a normal state, and no action is required.
ver-mismatch (vmiss)	The version of an AP does not match that of an AC on which the AP is about to go online.	The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. - Enterprise technical support website: **https://support.huawei.com/enterprise** - Carrier technical support website: **https://support.huawei.com**

AP State	Description	Possible Cause	Handling Suggestion
countryCode-mismatch (cmiss)	The country codes of the AP and AC do not match.	The AP's current version does not support the country code configured on the AC. The country code of the AP is locked, and the country code configured on the AC is not supported.	The AP does not support the country code. Upgrade the AP or modify the country code configuration on the AC. The country code of the AP is locked. Replace the AP or change the country code on the AC to be the same as that of the AP.
type-mismatch (tmiss)	The AP type does not match that configured on the AC.	The AP type configured on the AC did not match the actual AP type.	Change the AP type configured on the AC.
unauth	An AP is not authenticated.	The AP fails to be authenticated.	Run the **display ap unauthorized record** command to query authenticated APs. Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.2.88 display ap wired-port

Function

The **display ap wired-port** command displays AP wired interface configuration.

Format

display ap wired-port *interface-type interface-number* { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an AP's wired interface.	The interface type and number need to be selected according to the actual device.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view configurations on an AP's wired interface.

Example

Display the GE interface configuration of the AP named **example**.

```
<HUAWEI> display ap wired-port gigabitethernet 0 ap-name example
------------------------------------------------------------------------------
Wired port number             : 0
Wired port type               : GigabitEthernet
Wired port description        :
Wired port workmode           : endpoint
Wired port STP                : disable
Wired port user isolate       : disable
Wired port PVID VLAN          : -
Wired port VLAN tagged        : -
Wired port VLAN untagged      : -
Wired port Eth-trunk          : -
Wired port LLDP               : enable
Wired port LLDP basic TLV management address: enable
Wired port LLDP basic TLV port description  : enable
Wired port LLDP basic TLV system capability : enable
Wired port LLDP basic TLV system description: enable
Wired port LLDP basic TLV system name       : enable
Wired port CRC warn switch    : No
Wired port CRC warn high threshold : 50
Wired port CRC warn low threshold  : 20
------------------------------------------------------------------------------
Traffic Type                  Direction  AppliedRecord
--------------------------------------------------------------------------------------
traffic-filter                inbound    IPv4 ACL 3012
--------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------
```

```
Traffic Type                    Direction   RemarkType   RemarkValue   AppliedRecord
----------------------------------------------------------------------------------------
traffic-remark                  outbound    802.1p       2             IPv4 ACL 3011
------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
```

Table 11-100 Description about the **display ap wired-port gigabitethernet 0 ap-name** command output

Item	Description
Wired port number	Number of the wired interface.
Wired port type	Type of the wired interface.
Wired port description	Description of the wired interface.
Wired port workmode	Mode of the wired interface.
Wired port STP	Whether STP is enabled on the wired interface.
Wired port user isolate	Whether user isolation is enabled on the wired interface.
Wired port PVID VLAN	PVID of the wired interface.
Wired port VLAN tagged	VLAN to which the interface is added in tagged mode.
Wired port VLAN untagged	VLAN to which the interface is added in untagged mode.
Wired port Eth-trunk	Trunk ID to which the wired interface is bound.
Wired port LLDP	Whether LLDP is enabled on the wired interface.
Wired port LLDP basic TLV management address	TLV of the management IP address of the wired interface.
Wired port LLDP basic TLV port description	TLV of wired interface description.
Wired port LLDP basic TLV system capability	TLV of the wired interface capability set.
Wired port LLDP basic TLV system description	TLV of wired interface system description.
Wired port LLDP basic TLV system name	TLV of the wired interface system name.
Wired port CRC warn switch	Whether to enable the alarm function for CRC errors on the wired interface.
Wired port CRC warn high threshold	Upper alarm threshold for CRC errors on the wired interface.

Item	Description
Wired port CRC warn low threshold	Lower alarm threshold for CRC errors on the wired interface.
Traffic Type	ACL-based packet filtering and re-marking implemented by the AP wired port. ● traffic-filter ● traffic-remark
Direction	Incoming or outgoing packets.
AppliedRecord	IPv4/IPv6/L2 packet filtering and re-marking based on ACLs.
RemarkType	Protocol type. ● dscp ● dot1p
RemarkValue	Protocol type value. ● dscp: 0-63 ● dot1p: 0-7

Display the Eth-Trunk interface configuration of the AP named **example**.

```
<HUAWEI> display ap wired-port eth-trunk 0 ap-name example
------------------------------------------------------------------------------
Eth-trunk ID                 : 0
Eth-trunk description        : -
Workmode                     : root
STP                          : disable
User isolate                 : disable
PVID VLAN                    : -
VLAN tagged                  : -
VLAN untagged                : -
--------------------------------------------------------------------------------
Traffic Type                 Direction  AppliedRecord
----------------------------------------------------------------------------------------
traffic-filter               inbound    IPv4 ACL 3012
-----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------
Traffic Type                 Direction  RemarkType  RemarkValue  AppliedRecord
-----------------------------------------------------------------------------------------
traffic-remark               outbound   802.1p      2            IPv4 ACL 3011
------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------
```

Table 11-101 Description about the **display ap wired-port eth-trunk 0 ap-name** command output

Item	Description
Eth-trunk ID	ID of the Eth-trunk interface.
Eth-trunk description	Description of the Eth-trunk interface.

Item	Description
Workmode	Wired interface mode of an Eth-Trunk.
STP	Whether STP is enabled on the Eth-trunk interface.
User isolate	Whether user isolation is enabled on the Eth-trunk interface.
PVID VLAN	PVID of the Eth-trunk interface.
VLAN tagged	VLAN to which the Eth-trunk interface is added in tagged mode.
VLAN untagged	VLAN to which the Eth-trunk interface is added in untagged mode.
Traffic Type	ACL-based packet filtering and re-marking implemented by the AP wired port. ● traffic-filter ● traffic-remark
Direction	Incoming or outgoing packets.
AppliedRecord	IPv4/IPv6/L2 packet filtering and re-marking based on ACLs.
RemarkType	Protocol type. ● dscp ● dot1p
RemarkValue	Protocol type value. ● dscp: 0-63 ● dot1p: 0-7

11.2.89 display ap-pki-profile

Function

The **display ap-pki-profile** command displays information about an AP PKI realm profile.

Format

display ap-pki-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP PKI realm profiles.	-
name *profile-name*	Displays information about a specified AP PKI realm profile.	The AP PKI realm profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about an AP PKI realm profile, including the number of times the profile is referenced, PKI realms in the profile, and certificate files in the PKI realms.

Example

Display information about all AP PKI realm profiles.

```
<HUAWEI> display ap-pki-profile all
Total: 2
------------------------------------------------------------------------
Profile name                    Reference
------------------------------------------------------------------------
default                         5
mytest                          2
------------------------------------------------------------------------
```

Display detailed information about a specified AP PKI realm profile.

Table 11-102 Description of the **display ap-pki-profile** command output

Item	Description
Profile name	Name of an AP PKI realm profile.
Reference	Number of times an AP PKI realm profile is referenced.
PKI realmx name	Name of a PKI realm.
ca file format	CA certificate format.
ca file name	Name of a CA certificate file.
local file format	Format of a local certificate file.

Item	Description
local file name	Name of a local certificate file.
private key file format	Format of a private key file.
private key file name	Name of a private key file.
private key file password	Decryption password of a private key file.
CRL file	Name of a CRL file.

11.2.90 display ap-system-profile

Function

The **display ap-system-profile** command displays reference and configuration information about an AP system profile.

Format

display ap-system-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP system profiles.	-
name *profile-name*	Displays information about a specified AP system profile.	The AP system profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about an AP system profile.

Example

Display information about all AP system profiles.

```
<HUAWEI> display ap-system-profile all
----------------------------------------------------------
Profile name                  Reference
----------------------------------------------------------
default                       1
ap-system1                    0
----------------------------------------------------------
Total: 2
```

Table 11-103 Description of the **display ap-system-profile all** command output

Item	Description
Profile name	Name of an AP system profile.
Reference	Number of times an AP system profile is referenced.

Display information about the AP system profile **ap-system1**.

```
<HUAWEI> display ap-system-profile name ap-system1
------------------------------------------------------------------------------
AC priority                                  : -
Protect AC IP address                        : -
Primary AC                                   : -
Backup AC                                    : -
AP management VLAN                           : -
Keep service                                 : disable
Keep service allow new access                : disable
Keep service allow new access no auth        : disable
Temporary management switch                  : disable
Temporary management psk                     : ******
Card connect type                            : serial
Mesh role                                    : mesh-node
Mesh route aging time(s)                     : 15
STA access mode                              : disable
STA whitelist profile                        : -
STA blacklist profile                        : -
EAPOL start mode                             : multicast
EAPOL start transform                        : equal-bssid
EAPOL response mode                          : unicast learning
EAPOL response transform                     : equal-bssid
AP LLDP message transmission delay time(s)   : 2
AP LLDP message transmission hold multiplier : 4
AP LLDP message transmission interval time(s) : 30
AP LLDP restart delay time(s)                : 2
AP LLDP admin status                         : txrx
AP LLDP report interval time(s)              : 30
AP LLDP report enable                        : disable
AP device high temperature threshold (degree C): -
AP environment high temperature threshold (degree C) : -
AP CPU high temperature threshold (degree C)   : -
AP NP high temperature threshold (degree C)    : -
AP device low temperature threshold (degree C) : -
AP environment low temperature threshold (degree C)  : -
AP CPU low temperature threshold (degree C)    : -
AP NP low temperature threshold (degree C)     : -
AP CPU usage threshold(%)                    : 90
AP memory usage threshold(%)                 : 80
AP disk usage threshold(%)                   : 95
Alarm restriction                            : enable
Alarm restriction period(s)                  : 60
Log server IP address                        : -
Log server Port                              : -
Log record level                             : info
```

```
Ethernet port MTU(byte)                          : 1500
Telnet                                           : disable
STelnet server                                   : enable
SFTP server                                      : enable
Console                                          : enable
STA ARP-ND Proxy before-assoc                    : disable
Antenna output mode                              : split
Led                                              : on
Led off time range                               : -
DHCP client option12                             : ap-name
Console ble-mode                                 : dynamic
Report disassoc request                          : enable
Sample time(s)                                   : 30
Dynamic blacklist aging time(s)                  : 600
MPP active reselection                           : disable
AP report to                                     : server
Server IP                                        : 0.0.0.0
Server port                                      : -
AC port                                          : -
Device aging-time(minute)                        : 3
PoE max power(mW)                                : 380000
PoE power reserved(%)                            : -
PoE power threshold(%)                           : -
PoE af inrush                                    : disable
PoE high inrush                                  : disable
USB                                              : disable
SSH config
  Client first time                              : disable
  User interface vty 0
    Idle timeout                                 : 5min 0s
    Screen length                                : 24
    ACL inbound                                  : -
    ACL outbound                                 : -
    ACL ipv6 inbound                             : -
    ACL ipv6 outbound                            : -
  User interface vty 1
    Idle timeout                                 : 5min 0s
    Screen length                                : 24
    ACL inbound                                  : -
    ACL outbound                                 : -
    ACL ipv6 inbound                             : -
    ACL ipv6 outbound                            : -
  User interface vty 2
    Idle timeout                                 : 5min 0s
    Screen length                                : 24
    ACL inbound                                  : -
    ACL outbound                                 : -
    ACL ipv6 inbound                             : -
    ACL ipv6 outbound                            : -
  User interface vty 3
    Idle timeout                                 : 5min 0s
    Screen length                                : 24
    ACL inbound                                  : -
    ACL outbound                                 : -
    ACL ipv6 inbound                             : -
    ACL ipv6 outbound                            : -
  User interface vty 4
    Idle timeout                                 : 5min 0s
    Screen length                                : 24
    ACL inbound                                  : -
    ACL outbound                                 : -
    ACL ipv6 inbound                             : -
    ACL ipv6 outbound                            : -
AC protect link switch mode                      : priority
AC protect link switch packet loss echo probe time          : 20
AC protect link switch packet loss start threshold(%)       : 20
AC protect link switch packet loss gap threshold(%)         : 15
Traffic optimize broadcast suppression ARP      : enable
Traffic optimize broadcast suppression IGMP     : enable
```

```
Traffic optimize broadcast suppression ND      : enable
Traffic optimize broadcast suppression DHCP    : enable
Traffic optimize broadcast suppression DHCPv6  : enable
Traffic optimize broadcast suppression MDNS    : enable
Traffic optimize broadcast suppression other broadcast       : enable
Traffic optimize broadcast suppression other multicast       : enable
Traffic optimize broadcast suppression ARP rate limit(pps)   : 256
Traffic optimize broadcast suppression IGMP rate limit(pps)  : 256
Traffic optimize broadcast suppression ND rate limit(pps)    : 256
Traffic optimize broadcast suppression DHCP rate limit(pps)  : 256
Traffic optimize broadcast suppression DHCPv6 rate limit(pps): 256
Traffic optimize broadcast suppression MDNS rate limit(pps)  : 256
Traffic optimize broadcast suppression other broadcast rate limit(pps) : 256
Traffic optimize broadcast suppression other multicast rate limit(pps) : 256
Service-experience-analysis monitor interval(s) : 30
Wmi server profile
  Index 1                                 : -
  Index 2                                 : -
Broadcast suppression auto-detect packets(pps)  : 256
Multicast suppression auto-detect packets(pps)  : 256
Unicast suppression auto-detect packets(pps)    : 128
Station connectivity-detect switch              : enable
Power force work-mode                           : -
NP fast-forwarding switch                       : enable
NP CAPWAP reassembly switch                     : enable
Radio mode                                      : 3radio
Terminal identify                               : enable
S-IPFPM max user flow                           : 65535
Local management switch                         : enable
Local management IPv4 address                   : 192.168.254.254/32
Service-tunnel-profile                          : -
Distribute mode switch                          : disable
Self-healing-reset timeout(h)                   : 24
AP keep online switch                           : enable
------------------------------------------------------------------------------
```

Table 11-104 Description of the **display ap-system-profile name** *profile-name* command output

Item	Description
AC priority	AC priority. To configure this parameter, run the **priority** command.
Protect AC IP address	IP address of the standby AC. To configure this parameter, run the **protect-ac** command.
Primary AC	IP address of the primary AC. To configure this parameter, run the **primary-access** command.
Backup AC	IP address of the backup AC. To configure this parameter, run the **backup-access** command.
AP management VLAN	Management VLAN for APs To configure this parameter, run the **management-vlan** command.

Item	Description
Keep service	Whether service holding upon CAPWAP link disconnection is enabled. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **keep-service enable** command.
Keep service allow new access	Whether new STAs using the open, WEP, or WPA/WPA2-PSK security policy are allowed to go online when an AP is offline. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **keep-service enable allow new-access** command.
Keep service allow new access no auth	Whether the offline AP allows access of new STAs using Portal or MAC address authentication. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **keep-service enable allow new-access no-auth** command.
Temporary management switch	Whether the offline management VAP and antenna alignment VAP are enabled for APs. ● enable: The functions are enabled. ● disable: The functions are disabled. To configure this parameter, run the **temporary-management disable (AP system profile view)** command.
Card connect type	Communication connection type between IoT cards and APs. To configure this parameter, run the **card connect-type** command.
Temporary management psk	PSK of offline management VAP and antenna alignment VAP on APs. To configure this parameter, run the **temporary-management psk** command.

Item	Description
Mesh role	Mesh role. To configure this parameter, run the **mesh-role** command.
Mesh route aging time(s)	Aging time of a Mesh route. To configure the parameter, run the **mesh-route aging-time** command.
STA access mode	STA access mode. To configure this parameter, run the **sta-access-mode** command.
STA whitelist profile	Name of a STA whitelist profile referenced by an AP system profile. To configure this parameter, run the **sta-access-mode** command.
STA blacklist profile	Name of a STA blacklist profile referenced by an AP system profile. To configure this parameter, run the **sta-access-mode** command.
EAPOL start mode	EAPoL-Start packet encapsulation mode. To configure this parameter, run the **eapol-start dest-address transform-to** command.
EAPOL start transform	EAPoL-Start packet conversion mode. To configure this parameter, run the **eapol-start dest-address transform-condition** command.
EAPOL response mode	EAPoL-Response packet encapsulation mode. To configure this parameter, run the **eapol-response dest-address transform-to** command.
EAPOL response transform	EAPoL-Response packet conversion mode. To configure this parameter, run the **eapol-response dest-address transform-condition** command.
AP LLDP message transmission delay time(s)	Delay for an AP to send LLDP packets to neighbors. To configure this parameter, run the **lldp message-transmission delay (AP system profile view)** command.

Item	Description
AP LLDP message transmission hold multiplier	Hold time multiplier of AP information on neighbors. To configure this parameter, run the **lldp message-transmission hold-multiplier (AP system profile view)** command.
AP LLDP message transmission interval time(s)	Interval at which an AP sends LLDP packets to neighbors. To configure this parameter, run the **lldp message-transmission interval (AP system profile view)** command.
AP LLDP restart delay time(s)	Delay in re-enabling LLDP. To configure this parameter, run the **lldp restart-delay** command.
AP LLDP admin status	LLDP mode on an AP. ● tx: The AP sends but does not receive LLDP packets. ● rx: The AP receives but does not send LLDP packets. ● txrx: The AP sends and receives LLDP packets. To configure this parameter, run the **lldp admin-status** command.
AP LLDP report interval time(s)	Interval at which an AP reports LLDP neighbor information to an AC. To configure this parameter, run the **lldp report-interval** command.
AP LLDP report enable	Whether an AP is enabled to report information about its LLDP neighbors. To configure this parameter, run the **lldp report enable** command.
AP device high temperature threshold (degree C)	Upper device temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.
AP environment high temperature threshold (degree C)	Upper ambient temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.

Item	Description
AP CPU high temperature threshold (degree C)	Upper CPU temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.
AP NP high temperature threshold (degree C)	Upper NP module temperature alarm threshold of an AP. To configure this parameter, run the **high-temperature threshold** command.
AP device low temperature threshold (degree C)	Lower device temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP environment low temperature threshold (degree C)	Lower ambient temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP CPU low temperature threshold (degree C)	Lower CPU temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP NP low temperature threshold (degree C)	Lower NP module temperature alarm threshold of an AP. To configure this parameter, run the **low-temperature threshold** command.
AP CPU usage threshold(%)	CPU usage alarm threshold of an AP. To configure this parameter, run the **cpu-usage threshold** command.
AP memory usage threshold(%)	Memory usage alarm threshold of an AP. To configure this parameter, run the **memory-usage threshold** command.
AP disk usage threshold(%)	Disk usage alarm threshold of an AP. To configure this parameter, run the **disk-usage threshold** command.

Item	Description
Alarm restriction	Alarm suppression status of an AP. To configure this parameter, run the **alarm-restriction disable** command.
Alarm restriction period(s)	Alarm suppression period of an AP. To configure this parameter, run the **alarm-restriction period** command.
Log server IP address	IP address of the log server. To configure this parameter, run the **log-server** command.
Log server Port	Port number of the log server. To configure this parameter, run the **log-server** command.
Log record level	Level of AP logs to be backed up. To configure this parameter, run the **log-record-level** command.
Ethernet port MTU(byte)	MTU of Ethernet interfaces. To configure this parameter, run the **mtu** command.
Telnet	Whether AP Telnet login is enabled. To configure this parameter, run the **telnet enable** command.
STelnet server	Whether the STelnet server function of an AP is enabled. To configure this parameter, run the **stelnet server disable** command.
SFTP server	SFTP server status of an AP. To configure this parameter, run the **sftp server disable** command.
Console	Whether AP console port login is enabled. To configure this parameter, run the **console disable** command.
STA ARP-ND Proxy before-assoc	Whether an AP is enabled to send ARP/ND proxy packets for a STA before the STA is successfully associated. To configure this parameter, run the **sta arp-nd-proxy before-assoc** command.

Item	Description
Antenna output mode	Output mode of the AP's 2.4 GHz or 5 GHz antenna. To configure this parameter, run the **antenna-output** command.
Led	Whether AP indicators are allowed to turn on. - on: The AP indicators are allowed to turn on. - off: The AP indicators are forbidden to turn on. To configure this parameter, run the **led off** command.
Led off time range	Time range within which the AP indicators are forbidden to turn on. To configure this parameter, run the **led off** command.
DHCP client option12	AP information contained in Option 12 carried in DHCP messages reported by an AP. - ap-name: AP name contained in Option 12 carried in DHCP messages reported by an AP. - ap-type ap-mac: AP type and MAC address contained in Option 12 carried in DHCP messages reported by an AP. - disable: The Option 12 is not carried in DHCP messages reported by an AP. To configure this parameter, run the **dhcp client option12** command.
Console ble-mode	Bluetooth-based serial port login mode. - dynamic - persistent - disable: The Bluetooth-based serial port login function is disabled. To configure this parameter, run the **console ble-mode (AP system profile view)** command.

Item	Description
Report disassoc request	Whether an AP is enabled to report disassociation request packets of STAs to the AC. To configure this parameter, run the **report-disassoc-request disable** command.
Sample time(s)	AP's sampling interval. To configure this parameter, run the **sample-time** command.
Dynamic blacklist aging time(s)	Aging time of a dynamic blacklist entry. To configure this parameter, run the **dynamic-blacklist aging-time** command.
MPP active reselection	Active MPP reselection. To configure this parameter, run the **mpp-active-reselection enable** command.
AP report to	Mode in which an AP reports spectrum data. ● server: The AP reports spectrum data to a spectrum server directly. ● AC: The AP reports spectrum data to a spectrum server via the AC. To configure this parameter, run the **spectrum-analysis server** command.
Server IP	IP address of the spectrum server. To configure this parameter, run the **spectrum-analysis server** command.
Server port	Port number (UDP) of the spectrum server. To configure this parameter, run the **spectrum-analysis server** command.
AC port	Port number used by the AC to receive spectrum data (in UDP packets) from the AP. To configure this parameter, run the **spectrum-analysis server** command.

Item	Description
Device aging-time(minute)	Aging time of non-Wi-Fi device data on an AC. To set the aging time, run the **spectrum-analysis non-wifi-device aging-time** command.
PoE max power(mW)	Maximum output power of the central AP. To configure this parameter, run the **poe max-power (AP system profile view)** command.
PoE power reserved(%)	Percentage of reserved PoE power to the available PoE power on the central AP. To configure this parameter, run the **poe power-reserved (AP system profile view)** command.
PoE power threshold(%)	Alarm threshold of PoE power consumption percentage on the central AP. To configure this parameter, run the **poe power-threshold (AP system profile view)** command.
PoE af inrush	PoE standard of the central AP. To configure this parameter, run the **poe af-inrush enable (AP system profile view)** command.
PoE high inrush	Whether the central AP is enabled to allow high inrush current during power-on. To configure this parameter, run the **poe high-inrush enable (AP system profile view)** command.
Group address start	Start multicast group address. To configure this parameter, run the **igmp-snooping group-bandwidth (AP system profile view)** command.
Group address end	End multicast group address. To configure this parameter, run the **igmp-snooping group-bandwidth (AP system profile view)** command.

Item	Description
Bandwidth(kbps)	Bandwidth of global multicast groups on an AP. To configure this parameter, run the **igmp-snooping group-bandwidth (AP system profile view)** command.
USB	Whether USB is enabled. To configure this parameter, run the **usb enable (AP system profile view)** command.
SSH config	SSH configurations.
Client first time	Whether initial authentication is enabled on the SSH client. To configure this parameter, run the **ssh client first-time enable (AP system profile view)** command.
User interface vty X	VTY user interface *X*. The value of *X* is an integer that ranges from 0 to 4.
Idle timeout	Timeout period of user connections. To configure this parameter, run the **user-interface vty idle-timeout** command.
Screen length	Number of lines on each terminal screen. To configure this parameter, run the **user-interface vty screen-length** command.
ACL inbound	ACL that restricts STAs with a specified IPv4 address or within a specified IPv4 address segment from logging in to the device. To configure this parameter, run the **user-interface vty acl** command.
ACL outbound	ACL that restricts IPv4 STAs who have logged in to the device from logging in to other devices. To configure this parameter, run the **user-interface vty acl** command.

Item	Description
ACL ipv6 inbound	ACL that restricts STAs with a specified IPv6 address or within a specified IPv6 address segment from logging in to the device. To configure this parameter, run the **user-interface vty acl** command.
ACL ipv6 outbound	ACL that restricts IPv6 STAs who have logged in to the device from logging in to other devices. To configure this parameter, run the **user-interface vty acl** command.
AC protect link switch mode	Active/standby link switchover mode. To configure this parameter, run the **ac protect link-switch mode** command.
AC protect link switch packet loss echo probe time	Number of Echo probe packets sent within a statistics collection interval. To configure this parameter, run the **ac protect link-switch packet-loss echo-probe-time** command.
AC protect link switch packet loss start threshold(%)	Packet loss rate start threshold for an active/standby link switchover. To configure this parameter, run the **ac protect link-switch packet-loss** command.
AC protect link switch packet loss gap threshold(%)	Packet loss rate difference threshold for an active/standby link switchover. To configure this parameter, run the **ac protect link-switch packet-loss** command.
Traffic optimize broadcast suppression ARP	Whether the suppression function is enabled for ARP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression IGMP	Whether the suppression function is enabled for IGMP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.

Item	Description
Traffic optimize broadcast suppression ND	Whether the suppression function is enabled for ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression DHCP	Whether the suppression function is enabled for DHCP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression DHCPv6	Whether the suppression function is enabled for DHCPv6 packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression MDNS	Whether the suppression function is enabled for mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression other broadcast	Whether the suppression function is enabled for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression other multicast	Whether the suppression function is enabled for multicast packets other than IGMP and mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression disable (AP system profile view)** command.
Traffic optimize broadcast suppression ARP rate limit(pps)	Rate limit threshold for ARP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.

Item	Description
Traffic optimize broadcast suppression IGMP rate limit(pps)	Rate limit threshold for IGMP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression ND rate limit(pps)	Rate limit threshold for ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression DHCP rate limit(pps)	Rate limit threshold for DHCP packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression DHCPv6 rate limit(pps)	Rate limit threshold for DHCPv6 packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression MDNS rate limit(pps)	Rate limit threshold for mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression other broadcast rate limit(pps)	Rate limit threshold for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.
Traffic optimize broadcast suppression other multicast rate limit(pps)	Rate limit threshold for multicast packets other than IGMP and mDNS packets. To configure this parameter, run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command.

Item	Description
Service-experience-analysis monitor interval(s)	Sampling interval for SEA-based application monitoring. To configure this parameter, run the **service-experience-analysis monitor interval** command.
Wmi server profile	WMI profile bound to the AP system profile. ● Index 1: WMI profile with index 1 ● Index 2: WMI profile with index 2 To configure this parameter, run the **wmi-server (AP system profile view)** command.
Broadcast suppression auto-detect packets(pps)	Rate limit threshold of broadcast packets. To configure this parameter, run the **broadcast-suppression auto-detect (AP system profile view)** command.
Multicast suppression auto-detect packets(pps)	Rate limit threshold of multicast packets. To configure this parameter, run the **multicast-suppression auto-detect (AP system profile view)** command.
Unicast suppression auto-detect packets(pps)	Rate limit threshold of unknown unicast packets. To configure this parameter, run the **unicast-suppression auto-detect (AP system profile view)** command.
Station connectivity-detect switch	Whether STA connectivity check is enabled. To configure this parameter, run the **station connectivity-detect disable** command.
Power force work-mode	Power supply mode of an AP. To configure this parameter, run the **power force work-mode** command.
NP fast-forwarding switch	Whether the NP fast forwarding function is enabled. To configure this parameter, run the **np fast-forwarding disable (AP system profile view)** command.

Item	Description
NP CAPWAP reassembly switch	Whether the NP CAPWAP reassembly function is enabled. To configure this parameter, run the **np capwap-reassembly (AP system profile view)** command.
Radio mode	Radio mode of an AP. To configure this parameter, run the **radio-mode** command.
CPU defend Packet type Rate limit Type	Rate limit for packets sent by an AP to the CPU. To configure these parameters, run the **cpu-defend packet-type** command. If this command is not configured, these parameters are not displayed in the command output. ● Packet type: indicates the protocol type of packets. ● Rate limit: indicates the rate limit. ● Type: indicates the packet type (wired or wireless).
Terminal identify	Whether the terminal identification 2.0 function is enabled. To configure this parameter, run the **terminal-identify disable** command. ● enable: This function is enabled. ● disable
S-IPFPM max user flow	Maximum number of iPCA 2.0 measurement flows for each user. To configure this parameter, run the **s-ipfpm measure max-user-flow** command.
Local management switch	Whether the AP local management function is enabled. To configure this parameter, run the **local-management** command.
Local management IPv4 address	AP local management address. To configure this parameter, run the **local-management ip-address** command.
Service-tunnel-profile	Name of the bound service tunnel profile.

Item	Description
Distribute mode switch	Whether the distributed AP network collaboration function is enabled. To configure this parameter, run the **distribute-mode enable** command.
Self-healing-reset timeout(h)	Time threshold for an AP to restart for self-healing. To configure this parameter, run the **ap-keep-online self-healing-reset** command.
AP keep online switch	Whether the AP always-online function is enabled. To configure this parameter, run the **ap-keep-online disable** command.

11.2.91 display ap-type

Function

The **display ap-type** command displays AP type information.

Format

display ap-type { **all** | **id** *type-id* | **type** *ap-type* }

Parameters

Parameter	Description	Value
all	Displays all the built-in AP types on the device.	-
id *type-id*	Specifies an AP type ID.	The AP type ID must exist.
type *ap-type*	Specifies an AP type name.	The AP type name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view all the built-in AP types on the device and information about APs of the specified type.

Example

Display all the built-in AP types on the device.

```
<HUAWEI> display ap-type all
--------------------------------------------------------------------------------
ID     Type                          Configuration method
--------------------------------------------------------------------------------
......
```

Table 11-105 Description of the **display ap-type all** command output

Item	Description
ID	AP ID.
Type	AP type. The support for AP types depends on device models. For the mapping between AP types and IDs, see the tab page "AP Type Names and IDs" in **Quick Reference for WLAN AP Version Mapping and Models**.
Configuration method	AP type configuration method. • default: The AP type is registered during initialization. • configure(init): The AP type is added using a command, and no APs of such type have been online. • configure(normal): The AP type is added using a command, and the AC has synchronized AP type information from the AP.

Display the AP type with a specified AP type ID.

```
<HUAWEI> display ap-type id 125
------------------------------------------------------------------------------------
Type                                  : AirEnginexxxx
AP wired port number                       : 5
AP wired port  0 type                    : FE
AP wired port  1 type                    : FE
AP wired port  0 type                    : MultiGE
AP wired port  1 type                    : MultiGE
AP wired port  0 type                    : XGE
AP Eth-Trunk number                       : 1
Radio number                           : 3
Radio 0 type                         : 802.11bgnax
  Maximal spatial streams              : 4
  Maximal antenna number                 : 4
```

```
  Maximal VAP number                  : 16
  Antenna gain                        : 3
  Frequency switching                 : N
  Supported frequency                 : 2.4G
Radio 1 type                          : 802.11anacax
  Maximal spatial streams             : 8
  Maximal antenna number              : 12
  Maximal VAP number                  : 16
  Antenna gain                        : 3
  Frequency switching                 : N
  Dual-5G high/low band support       : High band(100~165)
  Supported frequency                 : 5G
Radio 2 type                          : 802.11anacax
  Maximal spatial streams             : 8
  Maximal antenna number              : 8
  Maximal VAP number                  : 16
  Antenna gain                        : 3
  Frequency switching                 : N
  Dual-5G high/low band support       : Low band(36~64)
  Supported frequency                 : 5G
Maximum station number                : 1152
AP environment high temperature threshold (degree C) : 100
AP CPU high temperature threshold (degree C)         : 110
AP IRF high temperature threshold (degree C)         : 110
AP environment low temperature threshold (degree C)  : -15
AP CPU low temperature threshold (degree C)          : -15
AP IRF low temperature threshold (degree C)          : -15
Outdoor                               : N
BLE                                   : Y
Number of IoT cards                   : 3
PMF                                   : Y
Optical module                        : Y
Optical module information query      : Y
Mesh                                  : Y
WDS                                   : N
Eth-Trunk                             : Y
External antenna                      : N
Frequency fast switching              : N
Radio mode                            : 2radio-standard(default)/3radio/2radio-independent-scan
----------------------------------------------------------------------------------------
```

Table 11-106 Description of the **display ap-type id** command output

Item	Description
Type	AP type.
AP wired port number	Number of wired interfaces.
AP wired port 0 type	Type of wired interfaces.
AP Eth-Trunk number	Number of Eth-Trunk interfaces.
Radio number	Number of radios.
Radio 0 type	Type of the radio. The value 0 indicates the radio ID.
Maximal spatial streams	Maximum number of spatial streams on the radio.
Maximal antenna number	Maximum number of antennas on the radio.

Item	Description
Maximal VAP number	Maximum number of VAPs on the radio.
Antenna gain	Antenna gain of the radio, in dB. When the antenna gain of an AP is not an integer, the AC rounds the value off and delivers the integer antenna gain. For example, if the 2.4 GHz antenna gain of an AP is 2.5 dB, the 2.4 GHz antenna gain of 3 dB is displayed on the AC.
Frequency switching	Whether the radio can be switched.
Supported frequency	Supported frequency band.
Dual-5G high/low band support	Working frequency band of the 5 GHz radio. ● Low band (36-64): The 5 GHz radio works at a low frequency band. ● High band (100-165): The 5 GHz radio works at a high frequency band. ● All band (36-165): The 5 GHz radio works at any frequency band.
Maximum station number	Maximum number of supported STAs.
AP device high temperature threshold (degree C)	Upper device temperature alarm threshold of an AP. **NOTICE** This parameter is not displayed for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
AP environment high temperature threshold (degree C)	Upper ambient temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine central APs.

Item	Description
AP CPU high temperature threshold (degree C)	Upper CPU temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 9700D-M.
AP NP high temperature threshold (degree C)	Upper NP module temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the AirEngine 9700D-M.
AP IRF high temperature threshold (degree C)	Upper IRF temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
AP device low temperature threshold (degree C)	Lower device temperature alarm threshold of an AP. **NOTICE** This parameter is not displayed for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
AP environment low temperature threshold (degree C)	Lower ambient temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine central APs.

Item	Description
AP CPU low temperature threshold (degree C)	Lower CPU temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 9700D-M.
AP NP low temperature threshold (degree C)	Lower NP module temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the AirEngine 9700D-M.
AP IRF low temperature threshold (degree C)	Lower IRF temperature alarm threshold of an AP. **NOTICE** This parameter is displayed only for the following models: AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760R-51, AirEngine 6760R-51E.
Outdoor	Whether the AP is an outdoor AP.
BLE	Whether Bluetooth is supported.
Number of IoT cards	Number of IoT cards.
PMF	Whether PMF is supported.
Optical module	Whether the optical module is supported.
Optical module information query	Whether optical module information can be queried.
Mesh	Whether the Mesh function is supported.
WDS	Whether the WDS function is supported.
Eth-Trunk	Whether the Eth-Trunk is supported.
External antenna	Whether external antennas are supported.
Frequency fast switching	Whether fast radio switching without the need of a restart is supported.

Item	Description
Radio mode	Radio mode supported by an AP. If multiple radio modes are supported, the default radio mode of the AP model is marked as **default**.

11.2.92 display ap-type undefined record

Function

The **display ap-type undefined record** command displays the types of the APs that fail to connect to an AC because the AC does not support these AP types.

Format

display ap-type undefined record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a new AP model cannot connect to the AC, you can check whether the AP type has been created. To list the undefined AP types, run the **display ap-type undefined record** command. Then run the **auto create ap-type** command to automatically import the AP types of these APs.

Example

Display the AP types of the APs that fail to connect to an AC because the AC does not support these AP types.

```
<HUAWEI> display ap-type undefined record
------------------------------------------------------------------------------------------
AP type      Type ID     Report AP MAC     Report Time
------------------------------------------------------------------------------------------
AP5010DN     29          00e0-fc76-e360   2019-04-28/23:39:00
------------------------------------------------------------------------------------------
Total : 1
```

Table 11-107 Description of the **display ap-type undefined record** command output

Item	Description
AP type	AP type.
Type ID	ID of an AP type.
Report AP MAC	MAC address of an AP that fails to connect to the AC the last time because the AC does not support the AP type.
Report Time	Last time when an AP fails to connect to the AC because the AC does not support the AP type.

11.2.93 display ap-type attributes abnormal-check-record

Function

The **display ap-type attributes abnormal-check-record** command displays records of AP attribute check exceptions after an AP type is created.

Format

display ap-type attributes abnormal-check-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an AP of a new version is connected to an AC, the AC verifies the attributes of the AP to prevent the following problems:

- If the AP attributes defined in the earlier version are modified, for example, a value range is modified, an incompatibility issue may be caused.
- Some attributes of the AP are missing. As a result, the AP fails to connect to the AC.

Example

Display the records of AP attribute check exceptions after an AP type is created.

```
<HUAWEI> display ap-type attributes abnormal-check-record
------------------------------------------------------------------
AP type           Type ID   Result      Reason
------------------------------------------------------------------
AP5010DN          29        risky       range conflict
AP6010DN          21        failed      lost-attributes
------------------------------------------------------------------
Total : 2
```

Table 11-108 Description of the **display ap-type attributes abnormal-check-record** command output

Item	Description
AP type	AP type.
Type ID	ID of an AP type.
Result	AP attribute check result.
Reason	Cause for the check result.

11.2.94 display channel switch-record

Function

The **display channel switch-record** command displays channel switching records on the device.

Format

display channel switch-record { **all** | **calibrate** | **ap-name** *ap-name* **radio** *radio-id* | **ap-id** *ap-id* **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Displays all channel switching records.	-
calibrate	Displays channel switching records for radio calibration.	-
ap-name *ap-name*	Displays channel switching records of the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays channel switching records of a specified AP radio.	The radio ID must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays channel switching records of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check channel switching records on a device.

Run the **display channel switch-record calibrate** command to query channel or power switching records caused by radio calibration to check the calibration results.

Example

Display all channel switching records.

```
<HUAWEI> display channel switch-record all
OldCh/NewCh: Old channel/New channel
OldBw/NewBw: Old bandwidth/New bandwidth
RfID   : Radio ID
------------------------------------------------------------------------------------------------------------------------
AP ID AP name                  RfID    OldCh/NewCh      OldBw/NewBw      Switch reason        Switch time
------------------------------------------------------------------------------------------------------------------------
15    AirEngine6760R-51_324033A6 1       -/149            20M/20M          configuration
2020-07-13/14:43:46
------------------------------------------------------------------------------------------------------------------------
Total : 1, printed : 1
```

Table 11-109 Description of the **display channel switch-record all** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
OldCh/NewCh	Channels used before and after switching.
OldBw/NewBw	Bandwidths before and after channel switching.

Item	Description
Switch reason	Reason for channel switching. - calibration: channel switching caused by radio calibration - configuration: channel switching caused by configuration - dfs: channel switching performed to avoid radar channels - dfs (In AC): channel switching caused by channel delivery by the AC to avoid radar channels - dfs recover: channel switching caused by DFS channel switchback - mesh: channel switching caused by channel negotiation on a Mesh network - unsupported: channel switching performed because the AP does not support the channel delivered from the AC - wds: channel switching caused by channel negotiation on a WDS network - iot-notification: channel switching notified by an IoT card - AP sync: channel switching caused by configuration synchronization (through AC-Fit AP channel synchronization) - Poor quality: channel switching caused by radio calibration triggered when the analyzer identifies poor-QoE APs
Switch time	Time when channel switching occurred.

Display channel calibration records.

```
<HUAWEI> display channel switch-record calibrate
PCH : Pre channel
CCH : Current channel
PBW : Pre bandwidth
CBW : Current bandwidth
PE  : Pre EIRP (dBm)
CE  : Current EIRP (dBm)
PRS : Pre RX sensitivity(dBm)
CRS : Current RX sensitivity(dBm)
PR  : Pre RSSI (dBm)
CR  : Current RSSI (dBm)
```

```
RfID: Radio ID
------------------------------------------------------------------------------------------------------------------------
----
AP ID AP name   RfID  PCH/CCH  PBW/CBW  PE/CE   PRS/CRS    PR/CR    Reason         Time
Trigger ID(Radio)
------------------------------------------------------------------------------------------------------------------------
----
0     AP1       0     11/6     80M/40M+ 27/127  -95/-82    -32/-40  Period recheck 19:30:00 2016/04/11  -
1     AP2       0     6/11     20M/20M  27/127  -95/-82    -40/-48  Bad env        19:21:53 2016/04/11  3(0)
------------------------------------------------------------------------------------------------------------------------
----
Total : 2
```

Table 11-110 Description of the **display channel switch-record calibrate** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
PCH/CCH	Channels before and after calibration. **NOTE** PCH/CCH changes may be discontinuous for a radio.
PBW/CBW	Bandwidth before and after calibration.
PE/CE	Power before and after calibration. **NOTE** PE/CE changes may be discontinuous for a radio.
PRS/CRS	Receiver sensitivity values before and after calibration.
PR/CR	Interference values before and after calibration.

Item	Description
Reason	Reason for triggering calibration. ● Period recheck: periodic calibration ● Bad env: environment deterioration ● Non-Wi-Fi report: non-Wi-Fi report ● Rogue AP report: rogue AP report ● Noise interfere: noise interference ● Global plan: network-wide plan ● AP online: The AP radio is on, the radio is switched (between 2.4 GHz and 5 GHz bands), the radio working mode changes, or the AP goes online. ● AP offline: The AP radio is off, the radio is switched (between 2.4 GHz and 5 GHz bands), the radio working mode changes, or the AP goes offline. ● Bad Channel: The channel deteriorates, causing a loss of Beacon frames. ● iot-notification: An IoT card notifies calibration. ● DFS(In AC): The AC delivers a channel to avoid radar channels. ● High interference: Severe interference occurs. ● Unknown: unknown reason
Time	Time when calibration is triggered.
Trigger ID(Radio)	ID of the AP (radio) that triggers partial radio calibration. **NOTE** If global radio calibration is triggered, this field displays -.

11.2.95 display distribute-ap

Function

The **display distribute-ap** command displays information about RUs.

Format

display distribute-ap { **all** | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-name** *ap-name* | **central-ap-id** *central-ap-id* | **central-ap-mac** *central-ap-mac* | **central-ap-name** *central-ap-name* }

Parameters

Parameter	Description	Value
all	Displays information about all RUs.	-
ap-id *ap-id*	Displays information about the RU of a specified ID.	The RU ID must exist.
ap-mac *ap-mac*	Displays information about the RU of a specified MAC address.	The MAC address must exist.
ap-name *ap-name*	Displays information about the RU of a specified name.	The RU name must exist.
central-ap-id *central-ap-id*	Displays information about the RUs connected to the central AP of a specified ID.	The central AP ID must exist.
central-ap-mac *central-ap-mac*	Displays information about the RUs connected to the central AP of a specified MAC address.	The MAC address of the central AP must exist.
central-ap-name *central-ap-name*	Displays information about the RUs connected to the central AP of a specified name.	The central AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check RU information.

Example

Display information about all RUs.

```
<HUAWEI> display distribute-ap all
Total AP information:
nor : normal          [3]
--------------------------------------------------------------------------------------------------------------
ID   MAC            Name          Group   IP        Type  State  Central-AP ID  Central-AP MAC  Central-AP
name
```

```
-----------------------------------------------------------------------------------------------------------------
1    00e0-fc76-e360 00e0-fc76-e360 group1  10.1.1.182 XXXXX nor    0             00e0-fc37-98a0  00e0-
fc37-98a0
2    00e0-fcf5-7280 00e0-fcf5-7280 group   10.1.1.158 XXXXX nor    0             00e0-fc37-98a0  00e0-
fc37-98a0
3    00e0-fcf6-0ce0 ap1            default 10.1.1.181 XXXXX nor    0             00e0-fc37-98a0  00e0-fc37-98a0
-----------------------------------------------------------------------------------------------------------------
Total: 3
```

Table 11-111 Description of the **display distribute-ap all** command output

Item	Description
ID	RU ID.
MAC	MAC address of the RU.
Name	Name of the RU.
Group	AP group to which an RU belongs.
IP	IP address of the RU.
Type	RU type.
State	RU state, which is the same as a common AP. For details, see **Table 11-5**.
Central-AP ID	ID of the central AP.
Central-AP MAC	MAC address of the central AP.
Central-AP name	Name of the central AP.

Table 11-112 AP state list

AP State	Description	Possible Cause	Handling Suggestion
commit-failed (cmtfa)	WLAN service configurations fail to be delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are performed for the AP. If the link between the AP and AC is disconnected or the peer end has no response, the AP enters the commit-failed state.	Check the network connection.

AP State	Description	Possible Cause	Handling Suggestion
committing (cmt)	WLAN service configurations are being delivered to an AP after the AP goes online on an AC.	After an AP goes online on the AC, WLAN service configurations are being delivered to the AP. During this process, the AP is in committing state.	This is a normal state, and no action is required.
config (cfg)	WLAN service configurations are being delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. During this process, the AP is in config state.	This is a normal state, and no action is required.
config-failed (cfgfa)	WLAN service configurations fail to be delivered to an AP when the AP is going online on an AC.	After an AP establishes a link with the AC, WLAN service configurations are delivered to the AP. If the configuration delivery fails due to various reasons (such as link disconnection), the AP enters the config-failed state.	Check the network connection.
download (dload)	An AP is in upgrade state.	When an AP is performing an upgrade, it enters the download state.	When the AP upgrade is complete, check the AP state.

AP State	Description	Possible Cause	Handling Suggestion
fault	An AP fails to go online.	An AP fails to go online, which is usually caused by the following: • The AP fails to obtain an IP address or obtains an incorrect IP address. • The network between the AP and AC is faulty. • The AP fails to be authenticated. • The number of APs on an AC has reached the maximum value. • The AP is faulty. • In dual-link cold backup or N+1 backup scenario, if the link between the active and standby ACs is established properly, an AP that goes online on the active AC is in fault state on the standby AC.	Handle the AP online failure. For details, see **An AP Fails to Go Online on the AC** in the *Troubleshooting Guide*.

AP State	Description	Possible Cause	Handling Suggestion
idle	It is the initialization state of an AP before it establishes a link with the AC for the first time.	When an AP has not established a CAPWAP link with the AC, the MAC address and SN of an AP that is added offline are different from the actual MAC address and SN of the AP, or the AC cannot manage an AP due to license resource insufficiency, the AP enters the idle state.	Perform the following operations. Check whether the AP is connected to the network. If the AP connection is normal, go to next step. Check the MAC address and SN of the AP that is added offline are different from the actual MAC address and SN of the AP. If not, perform the following operations: 1. Run the **display ap all** command to check AP information. 2. Run the **undo ap** { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** } command to delete the AP. 3. Run the **ap-id** *ap-id* [[**type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }] or **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] command to add correct AP information. If the fault persists, expand the license capacity. Note that RUs managed by the AC do not occupy

AP State	Description	Possible Cause	Handling Suggestion
			license resources of the AC.
name-conflicted (namec)	The name of an AP conflicts with that of an existing AP.	The name of an AP conflicts with the name of another AP that has been online on the same AC.	Run the **ap-rename ap-id** *ap-id* **new-name** *ap-new-name* command to change the AP name.
normal (nor)	An AP is working properly.	An AP successfully goes online on an AC.	This is a normal state, and no action is required.
standby (stdby)	An AP is in normal state on the standby AC.	In the HSB scenario, if the link between the master and backup ACs is established properly, an AP is in standby state on the backup AC and in normal state on the master AC.	This is a normal state, and no action is required.
ver-mismatch (vmiss)	The version of an AP does not match that of an AC on which the AP is about to go online.	The versions of the AP and AC do not match.	Log in to Huawei technical support website and download the release notes. Based on the version mapping, upgrade the AP or AC to the matching version. ● Enterprise technical support website: **https://support.huawei.com/enterprise** ● Carrier technical support website: **https://support.huawei.com**

AP State	Description	Possible Cause	Handling Suggestion
countryCode-mismatch (cmiss)	The country codes of the AP and AC do not match.	The AP's current version does not support the country code configured on the AC. The country code of the AP is locked, and the country code configured on the AC is not supported.	The AP does not support the country code. Upgrade the AP or modify the country code configuration on the AC. The country code of the AP is locked. Replace the AP or change the country code on the AC to be the same as that of the AP.
type-mismatch (tmiss)	The AP type does not match that configured on the AC.	The AP type configured on the AC did not match the actual AP type.	Change the AP type configured on the AC.
unauth	An AP is not authenticated.	The AP fails to be authenticated.	Run the **display ap unauthorized record** command to query authenticated APs. Run the **ap-confirm** command to confirm unauthenticated APs and allow them to go online.

11.2.96 display mac-address ap-all

Function

The **display mac-address ap-all** command displays MAC address entries on all APs.

Format

display mac-address *mac-address* [**verbose**] **ap-all**

Parameters

Parameter	Description	Value
mac-address	Displays MAC address entries on all APs.	The value is in H-H-H format. An H contains four hexadecimal numbers.
verbose	Displays detailed information of the dynamic entries. If *verbose* is not specified, brief information about MAC address entries is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When errors or attacks occur on the network, you can run the **display mac-address ap-all** command to locate the attack sources based on the displayed MAC addresses.

Example

Display dynamic MAC address entries of all APs.

```
<HUAWEI> display mac-address 00e0-fc09-bcf9 ap-all
Info: Waiting for AP response...done.
-------------------------------------------------------------------------------
MAC Address     VLAN/VSI        Learned-From              Type        AP ID
-------------------------------------------------------------------------------
00e0-fc09-bcf9    1/-         GigabitEthernet0/0/0      dynamic     1
00e0-fc09-bcf9    1/-         GigabitEthernet0/0/0      dynamic     0
-------------------------------------------------------------------------------
Total: 2
```

Table 11-113 Description of the **display mac-address** *mac-address* **ap-all** command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	ID of the VLAN or name of the VSI that a MAC address belongs to.

Item	Description
Learned-From	Interface on which the MAC address is learned.
Type	Type of a MAC address entry.
AP ID	AP ID.

11.2.97 display mac-address { ap-id | ap-name }

Function

The **display mac-address** { **ap-id** | **ap-name**} command displays all dynamic, dynamic secure, and sticky MAC address entries on an AP's wired interface.

Format

display mac-address { **ap-id** *ap-id* | **ap-name** *ap-name* } *interface-type interface-number*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays all dynamic, dynamic secure, and sticky MAC address entries on wired interfaces of the AP with the specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays all dynamic, dynamic secure, and sticky MAC address entries on wired interfaces of the AP with the specified name.	The AP name must exist.
interface-type interface-number	Displays all dynamic, dynamic secure, and sticky MAC address entries on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the number of the outbound interface.	The following types of outbound interfaces are supported: • Eth-Trunk • Ethernet • Gigabitethernet • MultiGE • XGigabitethernet

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mac-address** { **ap-id** | **ap-name**} command to check all dynamic, dynamic secure, and sticky MAC address entries on an AP's wired interface, including the MAC addresses and VLANs that the AP learns on specified interfaces.

Example

Display all dynamic, dynamic secure, and sticky MAC address entries on wired interfaces of the AP with ID 1.

```
<HUAWEI> display mac-address ap-id 1 ethernet 0
-----------------------------------------------------------
MAC Address     VLAN/VSI    Learned-From        Type
-----------------------------------------------------------
00e0-fc54-5a80 1/-        Ethernet0/0/0       dynamic
-----------------------------------------------------------
Total: 1
```

Table 11-114 Description of the **display mac-address ap-id** *ap-id interface-type interface-number* command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	VLAN or VSI to which the device belongs.
Learned-From	Interface on which the MAC address is learned.
Type	Type of a MAC address entry.

11.2.98 display port-link-profile

Function

The **display port-link-profile** command displays reference and configuration information about an AP wired port link profile.

Format

display port-link-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP wired port link profiles.	-
name *profile-name*	Displays information about a specified AP wired port link profile.	The AP wired port link profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display port-link-profile** command to view configuration and reference information about an AP wired port link profile.

Example

Display information about all AP wired port link profiles.

```
<HUAWEI> display port-link-profile all
----------------------------------------------------------
Profile name                  Reference
----------------------------------------------------------
default                     1
port-link-profile-1            0
----------------------------------------------------------
Total: 2
```

Table 11-115 Description of the **display port-link-profile all** command output

Item	Description
Profile name	Name of an AP wired port link profile.
Reference	Number of times an AP wired port link profile is referenced.

Display information about the AP wired port link profile **default**.

```
<HUAWEI> display port-link-profile name default
----------------------------------------------------------------------------
LLDP enable                   : enable
Management address                : enable
Port description                : enable
System capability                : enable
```

```
System description              : enable
System name                     : enable
802.3 TLV power                 : enable
802.3 TLV power format          : 802.3bt
Legacy TLV four pair power      : enable
Legacy TLV power capability     : enable
CRC error alarm                 : disable
CRC error high threshold(1/10000): 50
CRC error Low threshold(1/10000) : 20
PoE enable                      : enable
PoE legacy                      : disable
PoE priority                    : low
PoE force power                 : disable
Shutdown switch                 : disable
Speed(Mbit/s)                   : -
------------------------------------------------------------------------------
```

Table 11-116 Description of the **display port-link-profile name** *profile-name* command output

Item	Description
LLDP enable	Whether LLDP is enabled on an AP's wired interface. To configure the parameter, run the **lldp enable** command.
Management address	Whether an AP's wired interface is allowed to advertise the Management-address TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
Port description	Whether an AP's wired interface is allowed to advertise the Port-description TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
System capability	Whether an AP's wired interface is allowed to advertise the System-capability TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
System description	Whether an AP's wired interface is allowed to advertise the System-description TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.

Item	Description
System name	Whether an AP's wired interface is allowed to advertise the System-name TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
802.3 TLV power	Whether an AP's wired interface is allowed to advertise the Power via MDI TLV. To configure the parameter, run the **lldp tlv-enable (AP wired port link profile view)** command.
802.3 TLV power format	802.3 Power via MDI TLV advertised by an AP's wired interface. ● 802.1ab: The 802.3 Power via MDI TLV sent by the interface conforms to 802.1ab. ● 802.3at: The 802.3 Power via MDI TLV sent by the interface conforms to 802.3at. ● 802.3bt: The 802.3 Power via MDI TLV sent by the interface conforms to 802.3bt. ● -: Default value. To configure the parameter, run the **lldp dot3-tlv power (AP wired port link profile view)** command.
Legacy TLV four pair power	Whether an AP's wired interface is allowed to advertise Cisco's customized TLVs. To configure the parameter, run the **lldp tlv-enable legacy-tlv four-pair-power (AP wired port link profile view)** command.
Legacy TLV power capability	Whether the supported power capability is carried in LLDP packets sent by an AP. To configure the parameter, run the **lldp tlv-enable legacy-tlv power-capability (AP wired port link profile view)** command.

Item	Description
CRC error alarm	Whether the alarm function for CRC errors is enabled on an AP's wired interface. To configure the parameter, run the **crc-alarm enable** command.
CRC error high threshold(1/10000)	Alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **crc-alarm enable** command.
CRC error Low threshold(1/10000)	Clear alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **crc-alarm enable** command.
PoE enable	Whether the PoE function is enabled on the AP's interfaces. To configure the parameter, run the **poe disable (AP wired port link profile view)** command.
PoE legacy	Whether PD compatibility check is enabled on the AP. To configure the parameter, run the **poe legacy enable (AP wired port link profile view)** command.
PoE priority	Power priority of PoE interfaces on the AP. To configure the parameter, run the **poe priority (AP wired port link profile view)** command.
PoE force power	Whether forcible PoE power supply is enabled on the AP's interfaces. To configure the parameter, run the **poe force-power (AP wired port link profile view)** command.
Shutdown switch	Whether the AP's wired interface function is disabled. To configure the parameter, run the **shutdown (AP wired port link profile view)** command.

Item	Description
Speed(Mbit/s)	Rate of the AP's wired interface in non-auto negotiation mode. To configure the parameter, run the **speed (AP wired port link profile view)** command.

11.2.99 display provision-ap parameter-list

Function

The **display provision-ap parameter-list** command displays AP provisioning parameters in the AP provisioning view.

Format

display provision-ap parameter-list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running the **commit** command to deliver the AP provisioning parameters configured in the AP provisioning view, you can run the **display provision-ap parameter-list** command to check whether the parameters are correct and complete.

If a parameter is displayed as **-** in the command output, the parameter of the APs is not changed after the configuration is committed.

Example

Display AP provisioning parameters in the AP provisioning view.

```
<HUAWEI> display provision-ap parameter-list
--------------------------------------------------------------------------------
AP mode                 : -
AP name                 : -
AP address mode           : -
IPv4 address            : -
IPv4 mask address         : -
```

```
IPv4 gateway address     : -
IPv4 AC list             : -
Management Vlan          : 2
DTLS server-auth         : enable
DTLS server-auth cn list : -
------------------------------------------------------------------------------
```

Table 11-117 Description of the **display provision-ap parameter-list** command output

Item	Description
AP mode	AP mode. To set this parameter, run the **ap-mode** command.
AP name	AP name. To configure this parameter, run the **ap-name (AP provisioning view)** command.
AP address mode	Mode in which an AP obtains an IP address. To configure this parameter, run the **address-mode (AP provisioning view)** command.
IPv4 address	Static IPv4 address of an AP. To configure this parameter, run the **ip-address (AP provisioning view)** command.
IPv4 mask address	Static IPv4 address mask of an AP. To configure this parameter, run the **ip-address (AP provisioning view)** command.
IPv4 gateway address	IPv4 address gateway of the AP. To configure this parameter, run the **ip-address (AP provisioning view)** command.
IPv4 AC list	AC IPv4 address list of an AP. To configure this parameter, run the **ac-list (AP provisioning view)** command.
Management Vlan	Management VLAN tag carried in CAPWAP packets sent from the AP's wired interface. To configure this parameter, run the **management-vlan** command.

Item	Description
DTLS server-auth	Whether the AC authentication function is enabled for the AP. To configure this parameter, run the **capwap dtls server-auth (AP provisioning view)** command.
DTLS server-auth cn list	CN field in the AC certificate to be authenticated by the AP. To configure this parameter, run the **capwap dtls server-auth cn (AP provisioning view)** command.

11.2.100 display references ap-pki-profile

Function

The **display references ap-pki-profile** command displays reference information about an AP PKI realm profile.

Format

display references ap-pki-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the profile name.	The profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about an AP PKI realm profile.

Example

Display reference information about an AP PKI realm profile.

```
<HUAWEI> display references ap-pki-profile name default
Total: 5
------------------------------------------------------------
Reference type          Reference name
------------------------------------------------------------
ap-group                 default
ap-group                 mytest
ap-id                  69
ap-id                  70
ap-id                  72
------------------------------------------------------------
```

Table 11-118 Description of the **display references ap-pki-profile** command output

Item	Description
Reference type	Profile binding type. The options are as follows: ● **ap-group**: bound to an AP group ● **ap-id**: bound to an AP The **ap-group** and **ap-id** types are available.
Reference name	Name of an AP group or ID of an AP to which the profile is bound.

11.2.101 display references ap-system-profile

Function

The **display references ap-system-profile** command displays reference information about an AP system profile.

Format

display references ap-system-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP system profile.	The AP system profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references ap-system-profile** command to view reference information about an AP system profile.

Example

Display reference information of the AP system profile **default**.

```
<HUAWEI> display references ap-system-profile name default
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
AP group                   default
------------------------------------------------------------------------
Total: 1
```

Table 11-119 Description of the **display references ap-system-profile** command output

Item	Description
Reference type	Type of the profile by which an AP system profile is referenced.
Reference name	Name of the profile by which an AP system profile is referenced.

11.2.102 display references port-link-profile

Function

The **display references port-link-profile** command displays reference information about an AP wired port link profile.

Format

display references port-link-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP wired port link profile.	The AP wired port link profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references port-link-profile** command to view reference information about an AP wired port link profile.

Example

Display reference information about the AP wired port link profile **default**.

```
<HUAWEI> display references port-link-profile name default
--------------------------------------------------------------------
Reference type                Reference name
--------------------------------------------------------------------
AP wiredport profile           wired-port1
--------------------------------------------------------------------
Total:1
```

Table 11-120 Description of the **display references port-link-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port link profile is referenced.
Reference name	Name of the profile by which an AP wired port link profile is referenced.

11.2.103 display references wired-port-profile

Function

The **display references wired-port-profile** command displays reference information about an AP wired port profile.

Format

display references wired-port-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP wired port profile.	The AP wired port profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wired-port-profile** command to view reference information about an AP wired port profile.

Example

Display reference information about the AP wired port profile **default**.

```
<HUAWEI> display references wired-port-profile name default
------------------------------------------------------------------------
Reference type     Reference name                     Reference port
------------------------------------------------------------------------
AP group          default                         Ethernet0
AP group          default                         Ethernet1
AP group          default                         Ethernet2
AP group          default                         Ethernet3
AP group          default                         GigabitEthernet0
AP group          default                         GigabitEthernet1
AP group          default                         GigabitEthernet2
AP group          default                         GigabitEthernet3
AP group          default                         GigabitEthernet4
AP group          default                         GigabitEthernet5
AP group          default                         GigabitEthernet6
AP group          default                         GigabitEthernet7
AP group          default                         GigabitEthernet8
AP group          default                         GigabitEthernet9
AP group          default                         GigabitEthernet10
AP group          default                         GigabitEthernet11
AP group          default                         GigabitEthernet12
AP group          default                         GigabitEthernet13
AP group          default                         GigabitEthernet14
AP group          default                         GigabitEthernet15
AP group          default                         GigabitEthernet16
AP group          default                         GigabitEthernet17
AP group          default                         GigabitEthernet18
AP group          default                         GigabitEthernet19
AP group          default                         GigabitEthernet20
AP group          default                         GigabitEthernet21
AP group          default                         GigabitEthernet22
AP group          default                         GigabitEthernet23
AP group          default                         GigabitEthernet24
AP group          default                         GigabitEthernet25
AP group          default                         GigabitEthernet26
AP group          default                         GigabitEthernet27
AP group          default                         MultiGE0
```

```
AP group        default                 XGigabitEthernet0
AP group        default                 XGigabitEthernet1
AP group        default                 XGigabitEthernet2
AP group        default                 XGigabitEthernet3
AP group        default                 Ethernet-Trunk0
-----------------------------------------------------------------------------
Total: 38
```

Table 11-121 Description of the **display references wired-port-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port profile is referenced.
Reference name	Name of the profile by which an AP wired port profile is referenced.
Reference port	Interface by which an AP wired port profile is referenced.

11.2.104 display wired-port-profile

Function

The **display wired-port-profile** command displays reference and configuration information about an AP wired port profile.

Format

display wired-port-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP wired port profiles.	-
name *profile-name*	Displays information about a specified AP wired port profile.	The AP wired port profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about an AP wired port profile.

Example

Display information about all AP wired port profiles.

```
<HUAWEI> display wired-port-profile all
------------------------------------------------------------
Profile name                   Reference
------------------------------------------------------------
default                      1
wired-port-profile-1           0
------------------------------------------------------------
Total: 2
```

Table 11-122 Description of the **display wired-port-profile all** command output

Item	Description
Profile name	Name of an AP wired port profile.
Reference	Number of times an AP wired port profile is referenced.

Display information about the AP wired port profile **default** (Eth-trunk is not configured).

```
<HUAWEI> display wired-port-profile name default
-------------------------------------------------------------------------------
Port link profile                            : default
Description                                  :
STP                                         : disable
Port work mode                                  : -
Port Tagged VLAN                                 : -
Port untagged VLAN                                : 1
Port PVID VLAN                                  : -
User isolate mode                                : disable
DHCP trust port                                 : enable
ND trust port                                  : enable
IPSG switch                                   : disable
DAI switch                                    : disable
STP auto shutdown switch                            : disable
Auto shutdown recovery time                          : 600
Learn client IPv4 address switch                     : disable
Learn client IPv6 address switch                     : disable
IGMP-Snooping switch                              : disable
MLD-Snooping switch                               : disable
Port security switch                            : disable
Port security sticky MAC                          : disable
Port security maximum MAC                             : 1
Port security protect action                      : restrict
Traffic optimize TCP adjust MSS(bytes)          : -
Traffic optimize broadcast suppression(pps)     : -
Traffic optimize unicast suppression(pps)       : -
Traffic optimize multicast suppression(pps)     : -
-------------------------------------------------------------------------------------------
Traffic Type                       Direction   AppliedRecord
-------------------------------------------------------------------------------------------
traffic-filter                     inbound     IPv4 ACL 3012
```

```
------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
Traffic Type                   Direction   RemarkType   RemarkValue   AppliedRecord
------------------------------------------------------------------------------------------
traffic-remark                  outbound    802.1p       2             IPv4 ACL 3011
------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------
```

Display information about the AP wired port profile **dj** (Eth-trunk is configured).

```
<HUAWEI> display wired-port-profile name dj
----------------------------------------------------------------------------
Port link profile             : default
Description                   :
Ethernet trunk ID               : 0
----------------------------------------------------------------------------
```

Table 11-123 Description of the **display wired-port-profile name** *profile-name* command output

Item	Description
Port link profile	Name of the AP wired port link profile referenced by an AP wired port profile. To configure the parameter, run the **port-link-profile (AP wired port profile view)** command.
Description	Interface description. To configure the parameter, run the **description (AP wired port profile view)** command.
STP	STP status on a wired interface. To configure the parameter, run the **stp enable (AP wired port profile view)** command.
Port work mode	Working mode of a wired interface. ● root: indicates the root mode. ● endpoint: indicates the endpoint mode. ● middle: indicates the middle mode. ● -: indicates that the working mode of wired interfaces is not changed. To configure the parameter, run the **mode (AP wired port profile view)** command.
Port Tagged VLAN	VLAN to which a wired interface is added in tagged mode. To configure the parameter, run the **vlan (AP wired port profile view)** command.

Item	Description
Port untagged VLAN	VLAN to which a wired interface is added in untagged mode. To configure the parameter, run the **vlan (AP wired port profile view)** command.
Port PVID VLAN	PVID of a wired interface. To configure the parameter, run the **vlan pvid (AP wired port profile view)** command.
User isolate mode	User isolation status on a wired interface. To configure the parameter, run the **user-isolate (AP wired port profile view)** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **dhcp trust port** command.
ND trust port	Status of the ND trusted interface function. To configure the parameter, run the **nd trust port** command.
Ethernet trunk ID	ID of the Eth-Trunk interface.
IPSG switch	Whether IP source guard (IPSG) is enabled on an AP's wired interface. To configure the parameter, run the **ipsg enable (AP wired port profile view)** command.
DAI switch	Whether DAI is enabled on an AP's wired interface. To configure the parameter, run the **dai enable (AP wired port profile view)** command.
STP auto shutdown switch	Whether STP-triggered port shutdown is enabled on an AP's wired interface. To configure the parameter, run the **stp auto-shutdown enable (AP wired port profile view)** command.

Item	Description
Auto shutdown recovery time	Recovery time of the shutdown port triggered by STP. To configure the parameter, run the **stp auto-shutdown recovery-time (AP wired port profile view)** command.
Learn client IPv4 address switch	Whether terminal IPv4 address learning is enabled on an AP's wired interface. To configure the parameter, run the **learn-client-address enable (AP wired port profile view)** command.
Learn client IPv6 address switch	Whether terminal IPv6 address learning is enabled on an AP's wired interface. To configure the parameter, run the **learn-client-address enable (AP wired port profile view)** command.
IGMP-Snooping switch	Whether IGMP snooping is enabled on an AP's wired interface. To configure the parameter, run the **igmp-snooping enable (AP wired port profile view)** command.
MLD-Snooping switch	Whether MLD snooping is enabled on an AP's wired interface. To configure the parameter, run the **mld-snooping enable (AP wired port profile view)** command.
Port security switch	Whether port security is enabled on an AP's wired interface. To configure the parameter, run the **port-security enable (AP wired port profile view)** command.
Port security sticky MAC	Whether the port security and sticky MAC functions are enabled on an AP's wired interface. To configure the parameter, run the **port-security mac-address sticky (AP wired port profile view)** command.

Item	Description
Port security maximum MAC	Maximum number of secure MAC addresses that can be learned by an interface. To configure the parameter, run the **port-security max-mac-num (AP wired port profile view)** command.
Port security protect action	Protection action to be taken when the number of secure MAC addresses learned by an interface exceeds the limit. ● protect: The interface discards packets with source MAC addresses that are not in the MAC address table. ● restrict: The interface discards packets with source MAC addresses that are not in the MAC address table and sends a trap message. To configure the parameter, run the **port-security protect-action (AP wired port profile view)** command.
Traffic optimize TCP adjust MSS(bytes)	Maximum segment size (MSS) of TCP packets on an AP's wired interface. To configure the parameter, run the **traffic-optimize tcp adjust-mss** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume that can be received on an AP's wired interface. To configure the parameter, run the **traffic-optimize (AP wired port profile view)** command.
Traffic optimize unicast suppression(pps)	Maximum unknown unicast traffic volume that can be received on an AP's wired interface. To configure the parameter, run the **traffic-optimize (AP wired port profile view)** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume that can be received on an AP's wired interface. To configure the parameter, run the **traffic-optimize (AP wired port profile view)** command.

Item	Description
Traffic Type	ACL-based packet filtering and re-marking implemented by the AP wired port. ● traffic-filter ● traffic-remark
Direction	Incoming or outgoing packets.
AppliedRecord	IPv4/IPv6/L2 packet filtering and re-marking based on ACLs.
RemarkType	Protocol type. ● dscp ● dot1p
RemarkValue	Protocol type value. ● dscp: 0-63 ● dot1p: 0-7

11.2.105 display wlan ble-link-info

Function

The **display wlan ble-link-info** command displays connection information about the Bluetooth-based air interface on an AP.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

display wlan ble-link-info { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check connection information about the Bluetooth-based air interface on an AP.

Example

Display connection information about the Bluetooth-based air interface on the AP named **ap1**.

```
<HUAWEI> display wlan ble-link-info ap1
Info: This operation may take a few seconds. Please wait for a moment.done.
-------------------------------------------------------------------------------------
BLE access MAC                        : xxxx-xxxx-xxxx
Status                          : paired
Link status changed time              : 2019-04-11  09:12:46
-------------------------------------------------------------------------------------
```

Table 11-124 Description of the **display wlan ble-link-info** command output

Item	Description
BLE access MAC	MAC address of a STA accessed through Bluetooth. This address is randomly generated when the STA establishes a Bluetooth connection with the AP.
Status	Bluetooth connection status between a STA and the AP. ● link established: The link is established between the STA and AP. ● paired: The STA and AP are successfully paired.
Link status changed time	Time when the connection status is updated.

11.2.106 display wlan console ble statistics

Function

The **display wlan console ble statistics** command displays statistics about Bluetooth-based console port login on an AP.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

display wlan console ble statistics { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics about Bluetooth-based console port login on an AP.

Example

Display statistics about Bluetooth-based console port login on the AP named **huawei**.

```
<HUAWEI> display wlan console ble statistics ap-name huawei
Info: This operation may take a few seconds. Please wait for a moment.done.
------------------------------------------------------------------------------------
AP ID                                  : 0
AP Name                                : huawei
Air Frame Received (Packets)           : 11
Air Traffic Received (Bytes)           : 11
Air Frame Send (Packets)               : 8
Air Traffic Send (Bytes)               : 55
------------------------------------------------------------------------------------
```

Table 11-125 Description of the **display wlan console ble statistics** command output

Item	Description
AP ID	AP ID.
AP Name	AP name.
Air Frame Received (Packets)	Number of received air interface frames.
Air Traffic Received (Bytes)	Amount of received air interface traffic.
Air Frame Send (Packets)	Number of sent air interface frames.
Air Traffic Send (Bytes)	Amount of sent air interface traffic.

11.2.107 disk-usage threshold

Function

The **disk-usage threshold** command sets the disk usage alarm threshold of APs.

The **undo disk-usage threshold** command restores the default disk usage alarm threshold of APs.

The default disk usage alarm threshold of APs is 95.

Format

disk-usage threshold *threshold*

undo disk-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies a disk usage alarm threshold of APs.	The value is an integer that ranges from 6 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **disk-usage threshold** command to set the disk usage alarm threshold of APs. The corresponding alarm clear threshold equals the specified alarm threshold minus 5. This configuration is delivered to APs using this AP system profile view.

- When the disk usage of APs exceeds the current alarm threshold, the APs report an alarm to the AC, which displays alarm information.
- When the disk usage of APs falls below the current alarm threshold, the APs report a clear alarm to the AC, which displays clear alarm information.

Example

Set the disk usage alarm threshold of APs to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] disk-usage threshold 60
```

11.2.108 eapol-response dest-address transform-condition

Function

The **eapol-response dest-address transform-condition** command specifies the EAPOL-response packets to be encapsulated by an AP.

The **undo eapol-response dest-address transform-condition** command restores the default settings.

By default, an AP encapsulates only the EAPOL-response packets with the destination MAC addresses being the AP's BSSID.

Format

eapol-response dest-address transform-condition { **always** | **equal-bssid** }

undo eapol-response dest-address transform-condition

Parameters

Parameter	Description	Value
always	Configures the AP to encapsulate all EAPOL-response packets.	-
equal-bssid	Configures the AP to encapsulate only the EAPOL-response packets with the destination MAC address being the AP's BSSID.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, the destination MAC addresses of the EAPOL-response packets sent by some STAs are APs' BSSIDs, but the destination MAC addresses of the EAPOL-response packets sent by other STAs are not APs' BSSIDs. You need to run this command to specify the EAPOL-response packets to be encapsulated.

Example

Configure the AP to encapsulate all EAPOL-response packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-response dest-address transform-condition always
```

11.2.109 eapol-response dest-address transform-to

Function

The **eapol-response dest-address transform-to** command configures an AP to encapsulate EAPOL-response packets into broadcast, multicast, or unicast packets.

The **undo eapol-response dest-address transform-to** command restores the default settings.

By default, an AP encapsulates EAPOL-response packets into unicast packets and actively learns the destination MAC address.

Format

eapol-response dest-address transform-to { **broadcast** | **multicast** | **mac** *mac-address* | **learning** }

undo eapol-response dest-address transform-to

Parameters

Parameter	Description	Value
broadcast	Configures an AP to encapsulate EAPOL-response packets into broadcast packets.	-

Parameter	Description	Value
multicast	Configures an AP to encapsulate EAPOL-response packets into multicast packets.	-
mac *mac-address*	Configures an AP to encapsulate EAPOL-response packets into unicast packets with a specified destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
learning	Configures an AP to encapsulate EAPOL-response packets into unicast packets and actively learn the destination MAC address.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

- If the authentication server can only process EAP multicast packets, configure the AP to encapsulate EAPOL-response packets into multicast packets.
- If the authentication server can only process EAP broadcast packets, configure the AP to encapsulate EAPOL-response packets into broadcast packets.
- If the authentication server can only process EAP unicast packets, configure the AP to encapsulate EAPOL-response packets into unicast packets. When the AP is configured to encapsulate EAPOL-response packets into unicast packets, a unicast MAC address must be configured.

Example

Configure an AP to encapsulate EAPOL-response packets into broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-response dest-address transform-to broadcast
```

11.2.110 eapol-start dest-address transform-condition

Function

The **eapol-start dest-address transform-condition** command specifies the EAPOL-start packets to be encapsulated by an AP.

The **undo eapol-start dest-address transform-condition** command restores the default settings.

By default, an AP encapsulates only the EAPOL-start packets with the destination MAC addresses being the AP's BSSID.

Format

eapol-start dest-address transform-condition { **always** | **equal-bssid** }

undo eapol-start dest-address transform-condition

Parameters

Parameter	Description	Value
always	Configures the AP to encapsulate all EAPOL-start packets.	-
equal-bssid	Configures the AP to encapsulate only the EAPOL-start packets with the destination MAC address being the AP's BSSID.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During 802.1X authentication, the destination MAC addresses of the EAPOL-start packets sent by some STAs are APs' BSSIDs, but the destination MAC addresses of the EAPOL-start packets sent by other STAs are not APs' BSSIDs. You need to run this command to specify the EAPOL-start packets to be encapsulated.

Precautions

The packet types specified by the **eapol-start dest-address transform-condition** and **eapol-start dest-address transform-to** commands must be the same.

Example

Configure the AP to encapsulate all EAPOL-start packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-start dest-address transform-condition always
```

11.2.111 eapol-start dest-address transform-to

Function

The **eapol-start dest-address transform-to** command configures an AP to encapsulate EAPOL-start packets into broadcast, multicast, or unicast packets.

The **undo eapol-start dest-address transform-to** command restores the default settings.

By default, an AP encapsulates EAPOL-start packets into multicast packets.

Format

eapol-start dest-address transform-to { **broadcast** | **multicast** | **mac** *mac-address* }

undo eapol-start dest-address transform-to

Parameters

Parameter	Description	Value
broadcast	Configures an AP to encapsulate EAPOL-start packets into broadcast packets.	-
multicast	Configures an AP to encapsulate EAPOL-start packets into multicast packets.	-
mac *mac-address*	Configures an AP to encapsulate EAPOL-start packets into unicast packets.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

- If the authentication server can only process EAP multicast packets, configure the AP to encapsulate EAPOL-start packets into multicast packets.
- If the authentication server can only process EAP broadcast packets, configure the AP to encapsulate EAPOL-start packets into broadcast packets.
- If the authentication server can only process EAP unicast packets, configure the AP to encapsulate EAPOL-start packets into unicast packets. When the AP is configured to encapsulate EAPOL-start packets into unicast packets, a unicast MAC address must be configured.

Example

Configure an AP to encapsulate EAPOL-start packets into broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] eapol-start dest-address transform-to broadcast
```

11.2.112 eth-trunk (AP wired port profile view)

Function

The **eth-trunk** command adds an AP interface to an Eth-Trunk.

The **undo eth-trunk** command removes an AP interface from an Eth-Trunk.

By default, an AP interface is not added to any Eth-Trunk.

Format

eth-trunk *trunk-id*

undo eth-trunk

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is 0 or 1.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the connection reliability and increase the bandwidth, you can run this command to bind multiple interfaces into an Eth-Trunk.

Prerequisites

The physical interface to be added to an Eth-Trunk cannot have other configurations. Before adding a physical interface to an Eth-Trunk, clear all configurations on it except the interface status, descriptions, LLDP function, and alarm function for CRC errors.

Precautions

- After the configuration, you need to restart the AP to make the configured Eth-Trunk on the AP's wired interfaces take effect.
- APs that have only one physical uplink network interface do not support this command.
- Downlink interfaces on an AP do not support the Eth-Trunk function.
- Member interfaces in an Eth-Trunk do not support the PVID or user isolation configuration.
- For an AP that supports only one Eth-Trunk, the configuration takes effect only when the Eth-Trunk ID is set to 0.
- If a member interface of an Eth-Trunk is connected to a peer end, the peer interface directly connected to the local interface must also be a member interface of an Eth-Trunk.
- An Eth-Trunk cannot be added to another Eth-Trunk.
- Do not configure any member interface of an Eth-Trunk as an observing port. If this cannot be avoided, ensure that the bandwidth of service traffic on the member interface and the bandwidth of the mirrored traffic do not exceed the bandwidth limit of the interface.
- An Ethernet interface can be added to only one Eth-Trunk. To add the Ethernet interface in an Eth-Trunk to another Eth-Trunk, delete it from the original Eth-Trunk first.
- After an interface is added to an Eth-Trunk, MAC address entries and ARP entries are learned based on the Eth-Trunk but not based on member interfaces.

NOTE

The Eth-Trunk function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (except AirEngine 5761S-12, AirEngine 5761-12, and AirEngine 5761S-13)
- AirEngine 8771-X1T
- AirEngine 9700D-S (including matching ORUs)
- AirEngine series central APs

Example

Add the AP interface to Eth-Trunk 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] eth-trunk 0
```

11.2.113 high-temperature threshold

Function

The **high-temperature threshold** command sets an upper device, ambient, CPU, or NP module temperature alarm threshold for APs.

The **undo high-temperature threshold** command restores the default upper device, ambient, CPU, or NP module temperature alarm threshold of APs.

Table 11-126 Default upper temperature alarm threshold for APs

AP Model	Default Value (°C)
AirEngine 9700D-M1 (AP device/ ambient)	63/54

NOTE

This command is not supported by the following models:

- AirEngine series APs

Format

high-temperature [**ap-environment** | **cpu** | **np**] **threshold** *threshold*

undo high-temperature [**ap-environment** | **cpu** | **np**] **threshold**

Parameters

Parameter	Description	Value
ap-environment	Indicates the ambient temperature.	-
cpu	Indicates the CPU temperature.	-
np	Indicates the NP module temperature.	-

Parameter	Description	Value
threshold	Specifies the upper temperature alarm threshold.	The value is an integer that ranges from 20 to 110, in °C.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the upper temperature alarm threshold for an AP. When an AP's temperature exceeds the upper threshold, the AP generates an alarm and a log, and notifies the AC of the high temperature alarm.

The parameter **ap-environment** is supported only by the AirEngine 9700D-M and AirEngine 9700D-M1. The parameters **cpu** and **np** are supported only by the AirEngine 9700D-M.

If **ap-environment** | **cpu** | **np** is not specified, this command sets an upper temperature alarm threshold for APs.

Example

Set the upper temperature alarm threshold for APs to 65°C.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] high-temperature threshold 65
```

11.2.114 ipsg enable (AP wired port profile view)

Function

The **ipsg enable** command enables IP source guard (IPSG) on an AP's wired interface.

The **undo ipsg enable** command disables IPSG on an AP's wired interface.

By default, IPSG is disabled on an AP's wired interface.

Format

ipsg enable

undo ipsg enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attackers often use packets with the source IP addresses or MAC addresses of authorized users to access or attack networks. As a result, authorized users cannot obtain stable and secure network services. You can enable the IPSG function to prevent the situation.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on IP packets transmitted on an AP's wired interface.

An AP's wired interface added to an Eth-Trunk does not support this function.

Example

Enable IPSG on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] ipsg enable
```

11.2.115 ip-address (AP view)

Function

The **ip-address** command configures a static IPv4 address and gateway for an AP.

The **undo ip-address** command restores the default static IPv4 address and gateway for an AP.

By default, no static IPv4 address and gateway are configured for an AP.

Format

ip-address *ip-address* { *mask-length* | *mask* } [**gateway** *gateway*]

undo ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the static IPv4 address for an AP.	The value is in dotted decimal notation.
mask	Specifies the IPv4 address mask for an AP.	The value is in dotted decimal notation.
mask-length	Specifies the IPv4 address mask length for an AP.	The value is an integer that ranges from 0 to 32.
gateway *gateway*	Specifies the egress gateway for AP routes.	The value is in dotted decimal notation.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an AP to go online using a specified IPv4 address, run the command to configure a static IPv4 address for the AP.

Prerequisites

The AP has been configured to obtain an IP address in static mode using the **address-mode (AP provisioning view)** command.

Precautions

Ensure that there are reachable routes between the configured IPv4 address and the AC source address for an AP to go online. Otherwise, the AP may fail to go online.

CAPWAP packets between the central AP and RUs in versions earlier than V200R019C10 are forwarded at Layer 2 and are independent of IP addresses on an agile distributed WLAN. Therefore, the configuration of an IP address does not affect the RU going online. Ensure that a route is reachable between the IP address of the RU and the central AP source address. Otherwise, services involving IP addresses may be affected, for example, STelnet.

If the AP and AC are connected through a Layer 3 network, the egress gateway for AP routes must be configured.

Example

Set the static IPv4 address of the AP to 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] address-mode static
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
[HUAWEI-wlan-ap-0] ip-address 10.1.1.1 24
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.116 ip-address (AP provisioning view)

Function

The **ip-address** command configures a static IPv4 address and gateway for an AP.

The **undo ip-address** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, no static IPv4 address and gateway are configured for an AP.

Format

ip-address *ip-address* { *mask-length* | *mask* } [**gateway** *gateway*]

undo ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the static IPv4 address for an AP.	The value is in dotted decimal notation.
mask	Specifies the IPv4 address mask for an AP.	The value is in dotted decimal notation.
mask-length	Specifies the IPv4 address mask length for an AP.	The value is an integer that ranges from 0 to 32.
gateway *gateway*	Specifies the egress gateway for AP routes.	The value is in dotted decimal notation.

Views

AP provisioning view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an AP to go online using a specified IPv4 address, run the **ip-address** command to configure a static IPv4 address for the AP.

Prerequisites

The AP has been configured to obtain an IP address in static mode using the **address-mode (AP provisioning view)** command.

Follow-up Procedure

Run the **commit** command to deliver configuration to APs and restart the APs to make the configuration take effect.

Precautions

Ensure that there are reachable routes between the configured IPv4 address and the AC source address for an AP to go online. Otherwise, the AP may fail to go online.

CAPWAP packets between the central AP and RUs are forwarded at Layer 2 and are independent of IP addresses on an agile distributed WLAN. Therefore, the configuration of an IP address does not affect the RU going online. Ensure that a route is reachable between the IP address of the RU and the central AP source address. Otherwise, services involving IP addresses, for example, Telnet, may be affected.

If the AP and AC are connected through a Layer 3 network, the egress gateway for AP routes must be configured.

Example

Set the static IPv4 address of the AP to 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] address-mode static
[HUAWEI-wlan-provision-ap] ip-address 10.1.1.1 24
```

11.2.117 ip domain-name

Function

The **ip domain-name** command sets the default domain name suffix.

The **undo ip domain-name** command deletes the default domain name suffix.

By default, no default domain name suffix is provided.

Format

ip domain-name *domain-name*

undo ip domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name suffix.	The value is a string of 1 to 255 characters.

Views

AP view, AP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Devices with the same system name may exist in different domains. In this case, you can configure a fully qualified domain name (FQDN) for a device to uniquely identify it. The FQDN of a device consists of the default domain name suffix and device name. You can run the **ip domain-name** command to set the default domain name suffix and the **sysname** command to set the device name.

Precautions

If you run this command multiple times, the latest configuration overrides the previous ones.

Example

Set the domain name suffix to **com.cn**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] ip domain-name com.cn
```

11.2.118 igmp-snooping enable (AP wired port profile view)

Function

The **igmp-snooping enable** command enables IGMP snooping on an AP's wired interface.

The **undo igmp-snooping enable** command disables IGMP snooping on an AP's wired interface.

By default, IGMP snooping is disabled on an AP's wired interface.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping is a basic Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. IGMP snooping runs on a Layer 2 device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

Prerequisites

An AP wired port profile has been created.

Precautions

The AP wired interfaces added to an Eth-trunk interface do not support this function.

The **igmp-snooping enable** command is used to enable Layer 2 multicast services. To ensure multicast service experience, you are advised to disable the multicast packet rate limiting function by using the **traffic-optimize broadcast-suppression other-multicast disable** command in the AP system profile view.

When multicast services are enabled, the multicast services may be affected if rate limiting for multicast packets is enabled on an AP. In this case, you are advised to run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to adjust the rate limit threshold for multicast packets.

Example

Enable IGMP snooping on AP wired port profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] wired-port-profile name p1
[HUAWEI-wlan-wired-port-p1] igmp-snooping enable
```

11.2.119 keep-service enable

Function

The **keep-service enable** command enables service holding upon CAPWAP link disconnection.

The **undo keep-service enable** command disables service holding upon CAPWAP link disconnection.

By default, service holding upon CAPWAP link disconnection is disabled.

Format

keep-service enable

undo keep-service enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In direct forwarding mode, you can enable service holding upon CAPWAP link disconnection. In this way, when the CAPWAP link between an AP and AC is disconnected, the AP can continue to provide WLAN services, preventing service interruption and improving forwarding reliability.

Precautions

Service holding upon CAPWAP link disconnection can be configured in the VAP profile view and AP system profile view. The configuration in the VAP profile view takes precedence over that in the AP system profile view.

Service holding upon CAPWAP link disconnection is mutually exclusive with the containment function. Service holding upon CAPWAP link disconnection does not take effect when the containment function is also configured.

After service holding upon CAPWAP link disconnection is enabled, the **display access-user** command cannot display information about NAC STAs that are online before the CAPWAP link is disconnected. To display information about such STAs, run the **display station** command.

Example

Configure the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] keep-service enable
```

11.2.120 keep-service enable allow new-access

Function

The **keep-service enable allow new-access** command enables offline APs to allow access of new STAs.

The **undo keep-service enable** command disables offline APs from allowing access of new STAs.

By default, offline APs cannot allow access of new STAs.

Format

keep-service enable allow new-access [**no-auth**]

undo keep-service enable

Parameters

Parameter	Description	Value
no-auth	Allows access of STAs using Portal or MAC address authentication.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Service holding upon CAPWAP link disconnection controls whether new STAs are allowed to go online. For high-security authentication modes such as MAC address authentication and Portal authentication, **no-auth** must be configured to enable STAs to go online without authentication upon CAPWAP link disconnection. Therefore, this function can be enabled in scenarios with low security requirements.

Precautions

The function of enabling offline APs to allow access of STAs is applicable to scenarios where service data is forwarded in direct mode and the STA authentication mode is Portal, MAC address, WEP, WPA/WPA2-PSK, or open system.

Example

Enable offline APs to allow access of new STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] keep-service enable allow new-access
```

11.2.121 learn-client-address enable (AP wired port profile view)

Function

The **learn-client-address enable** command enables STA address learning on an AP's wired interface.

The **undo learn-client-address enable** command disables STA address learning on an AP's wired interface.

By default, STA address learning is disabled on an AP's wired interface.

Format

learn-client-address { **ipv4** | **ipv6** } **enable**

undo learn-client-address { **ipv4** | **ipv6** } **enable**

Parameters

Parameter	Description	Value
ipv4	Indicates the IPv4 address.	-
ipv6	Indicates the IPv6 address.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After STA address learning is enabled on an AP's wired interface, if a wired terminal connected to the AP's wired interface successfully obtains an IP address, the AP automatically reports the IP address of the terminal to the AC, helping to maintain the ARP binding entries of wired terminals.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

An AP's wired interface added to an Eth-Trunk does not support this function.

STA address learning on an AP's wired interface takes effect only for STAs that obtain IP addresses through DHCP, and does not take effect for STAs using static IP addresses.

If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.

Example

Enable STA IPv4 address learning on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] learn-client-address ipv4 enable
```

11.2.122 led blink-time

Function

The **led blink-time** command configures the indicator blinking function for an AP.

The **undo led blink-time** command cancels the indicator blinking configuration of an AP.

By default, the indicator blinking function is disabled on an AP.

Format

led blink-time *blink-time* { **ap-mac** *ap-mac* | **ap-name** *ap-name* | **ap-id** *ap-id* }

undo led blink-time { **ap-mac** *ap-mac* | **ap-name** *ap-name* | **ap-id** *ap-id* | **all** }

Parameters

Parameter	Description	Value
blink-time	Specifies the blinking time of an AP.	The value is an integer that ranges from 1 to 86400, in seconds.

Parameter	Description	Value
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
all	Cancels the indicator blinking configuration of all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To locate an AP, run this command on the AC to configure the AP indicator to blink.

When this function is enabled, the SYS indicator blinks red.

Precautions

Offline APs cannot be located by configuring the AP indicator to blink.

The configuration using the **led blink-time** command takes precedence over that using the **led off** command. That is, if AP indicators are configured to blink and to turn off or turn off during the specified time range, the configuration performed using the **led off** command takes effect after the RU indicators blink.

This function is not available for central APs.

Example

Configure the indicator of an AP with the MAC address of 00e0-fc12-3456 to blink for 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] led blink-time 300 ap-mac 00e0-fc12-3456
```

11.2.123 led off

Function

The **led off** command turns off AP indicators.

The **undo led off** command restores the default settings.

By default, AP indicators are allowed to turn on.

Format

led off

undo led off

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Blinking indicators of indoor APs deployed in hospitals and hotels may affect people's nighttime rest. To prevent this, run the **led off** command to turn off AP indicators.

If you need to locate AP faults by observing AP indicator status, run the **undo led off** command to allow the AP indicators to turn on.

Precautions

The configuration performed using the **led blink-time** command takes precedence over that performed using the **led off** command. That is, if AP indicators are configured to blink and to turn off or turn off during the specified time range, the configuration performed using the **led off** command takes effect after the RU indicators blink.

Example

Turn off AP indicators.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] led off
```

11.2.124 lldp admin-status

Function

The **lldp admin-status** command sets the LLDP operation mode for an AP.

The **undo lldp admin-status** command restores the default LLDP operation mode for an AP.

By default, the LLDP operation mode of an AP is TxRx.

Format

lldp admin-status { **rx** | **tx** | **txrx** }

undo lldp admin-status

Parameters

Parameter	Description	Value
rx	Specifies the LLDP operation mode as Rx. An AP only receives but does not send LLDP packets.	-
tx	Specifies the LLDP operation mode as Tx. An AP only sends but does not receive LLDP packets.	-
txrx	Specifies the LLDP operation mode as TxRx. An AP sends and receives LLDP packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can configure the LLDP operation mode for an AP based on the site requirements. For example, if you set the LLDP operation mode of an AP to Tx, the AP sends LLDP packets but cannot receive LLDP packets from neighbors. In this situation, the AP cannot discover neighbors.

Example

Set the LLDP operation mode of an AP to Tx.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp admin-status tx
```

11.2.125 lldp dot3-tlv power (AP wired port link profile view)

Function

The **lldp dot3-tlv power** command configures the standard with which the 802.3 Power via MDI TLV advertised by an AP's wired interface complies.

By default, the 802.3 Power via MDI TLV advertised by a UPoE interface and a PoE interface complies with 802.3bt and 802.3at, respectively.

Format

lldp dot3-tlv power { **802.1ab** | **802.3at** | **802.3bt** }

undo lldp dot3-tlv power

Parameters

Parameter	Description	Value
802.1ab	Indicates that the 802.3 Power via MDI TLV advertised an AP's wired interface complies with 802.1ab.	-
802.3at	Indicates that the 802.3 Power via MDI TLV advertised an AP's wired interface complies with 802.3at.	-
802.3bt	Indicates that the 802.3 Power via MDI TLV advertised an AP's wired interface complies with 802.3bt.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.3 Power via MDI TLV advertised by an AP's wired interface supports the following formats:

- 802.1ab format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class]
- 802.3at format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]
- 802.3bt format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value | PD requested power value Mode A | PD requested power value Mode B | PSE allocated power value Alternative A | PSE allocated power value Alternative B | PSE power status | System setup | PSE maximum available power | Autoclass | Power down]

Based on 802.1ab, 802.3at extends three fields: type/source/priority, PD requested power value, and PSE allocated power value. Based on 802.3at, 802.3bt extends the following fields to provide more detailed UPoE information: PD requested power value Mode A, PD requested power value Mode B, PSE allocated power value Alternative A, PSE allocated power value Alternative B, PSE power status, System setup, PSE maximum available power, Autoclass, and Power down.

Prerequisites

- The LLDP function has been enabled in both the WLAN view and AP wired port link profile view.
- APs' wired interfaces are allowed to advertise the 802.3 Power via MDI TLV.

Precautions

Before selecting a format of the 802.3 Power via MDI TLV, you need to know the TLV formats supported by the neighbors. The TLV format on the local device must be the same as that on the neighbors.

Member interfaces of the Eth-Trunk do not support this command.

Example

Configure the 802.3 Power via MDI TLV advertised by the AP's wired interface to comply with 802.3at.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp dot3-tlv power 802.3at
```

11.2.126 lldp enable

Function

The **lldp enable** command enables LLDP on an AP's wired interface.

The **undo lldp enable** command disables LLDP on an AP's wired interface.

By default, LLDP is enabled on an AP's wired interface.

Format

lldp enable

undo lldp enable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AP wired interfaces can exchange LLDP packets with neighbors to obtain neighbor status and transmit AP status to neighbors. The AP and neighbors save the received information to the Management Information Base (MIB) to query and determine the link status.

Prerequisite

The LLDP function has been enabled in the WLAN view using the **ap lldp enable** command.

Example

Enable LLDP on the AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap lldp enable
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp enable
```

11.2.127 lldp message-transmission delay (AP system profile view)

Function

The **lldp message-transmission delay** command sets the LLDP packet transmission delay.

The **undo lldp message-transmission delay** command restores the default LLDP packet transmission delay.

The default LLDP packet transmission delay is 2 seconds.

Format

lldp message-transmission delay *delay*

undo lldp message-transmission delay

Parameters

Parameter	Description	Value
delay	Specifies the LLDP packet transmission delay.	The value is an integer that ranges from 1 to 8192, in seconds. The *delay* value depends on the parameter *interval* set by the **lldp message-transmission interval** command. The *delay* value must be less than or equal to a quarter of the *interval* value.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the AP sends an LLDP packet to the neighbor when the device status changes frequently.

If the AP status changes frequently, extend the delay in preventing the AP from frequently sending packets to the neighbors. A delay suppresses the network topology flapping.

Configuration Impact

The LLDP packet transmission delay must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency when the local device status frequently changes. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.

- A small value increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time when the local device status frequently changes. However, if the value is too small, LLDP packets are exchanged frequently. This increases the system load and wastes resources.
- The default value is recommended.

Precautions

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- Decreasing the value of *delay* is not restricted by the value of *interval*. *delay* can be any number from 1 to 8192.
- The *delay* value must be less than or equal to a quarter of the *interval* value. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to at least four times the new *delay* value, and then increase the *delay* value.

NOTE

If the *interval* value is smaller than four times the *delay* value, the system displays an error message when you run the **undo lldp message-transmission delay** command. To run the **undo lldp message-transmission delay** command, increase the *interval* value to at least four times the *delay* value first.

Example

Set the LLDP packet transmission delay to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp message-transmission delay 10
```

11.2.128 lldp message-transmission hold-multiplier (AP system profile view)

Function

The **lldp message-transmission hold-multiplier** command sets the hold time multiplier of device information stored on neighbors.

The **undo lldp message-transmission hold-multiplier** command restores the default hold time multiplier of device information stored on neighbors.

The default hold time multiplier is 4.

Format

lldp message-transmission hold-multiplier *hold*

undo lldp message-transmission hold-multiplier

Parameters

Parameter	Description	Value
hold	Specifies the hold time multiplier of device information stored on neighbors.	The value is an integer that ranges from 2 to 10.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The time multiplier is used to calculate how long a packet can be saved on a neighboring node. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

TTL is the device information storage time. It is the smaller value between 65535 and (*interval* x *hold*).

interval indicates the interval at which the device sends LLDP packets to neighbors. This parameter is set by the **lldp message-transmission interval** command. *hold* indicates the hold time multiplier of device information stored on neighbors.

After the LLDP function is disabled on the device, its neighbors wait until the TTL of the device information expires, and then delete the device information. This prevents network topology flapping.

Configuration Impact

The hold time multiplier of device information stored on neighbors must be set to a proper value.

- A large value of *delay* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *delay* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the hold time multiplier of AP information stored on neighbors to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp message-transmission hold-multiplier 5
```

11.2.129 lldp message-transmission interval (AP system profile view)

Function

The **lldp message-transmission interval** command sets the LLDP packet transmission interval.

The **undo lldp message-transmission interval** command restores the default LLDP packet transmission interval.

The default LLDP packet transmission interval is 30 seconds.

Format

lldp message-transmission interval *interval*

undo lldp message-transmission interval

Parameters

Parameter	Description	Value
interval	Specifies the LLDP packet transmission interval.	The value is an integer that ranges from 5 to 32768, in seconds. The *interval* value depends on the parameter *delay* set by the **lldp message-transmission delay** command. The *interval* value must be greater than or equal to 4 times the *delay* value; otherwise, the system displays an error message when you run the **lldp message-transmission interval** command.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the LLDP status of the AP keeps unchanged or the AP does not discover new neighbors, the AP sends LLDP packets to the neighbors at a specified interval.

If you want to change the network topology detection frequency, run the **lldp message-transmission interval** command to change the LLDP packet transmission interval.

Configuration Impact

The LLDP transmission interval must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A short interval increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time. If the delay is too short, LLDP packets are exchanged frequently. This increases the system load and wastes resources.
- The default value is recommended.

Precautions

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *interval*.

- Increasing the value of *interval* is not restricted by the value of *delay*. *interval* can be any number from 5 to 32768.
- The *interval* value must be greater than or equal to four times the *delay* value. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be less than or equal to a quarter of the new *interval* value, and then reduce the *interval* value.

NOTE

If the *delay* value is larger than a quarter of the *interval* value, the system displays an error message when you run the **undo lldp message-transmission interval** command. To run the **undo lldp message-transmission interval** command, reduce the *delay* value to be less than or equal to a quarter of the *interval* value first.

Example

Set the LLDP packet transmission interval to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp message-transmission interval 60
```

11.2.130 lldp report enable

Function

The **lldp report enable** command enables an AP to report information about its LLDP neighbors.

The **undo lldp report enable** command disables an AP from reporting information about its LLDP neighbors.

By default, an AP does not report information about its LLDP neighbors.

Format

lldp report enable

undo lldp report enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **lldp report enable** command to enable an AP to report information about its LLDP neighbors.

Example

Enable an AP to report information about its LLDP neighbors.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] lldp report enable
```

11.2.131 lldp report-interval

Function

The **lldp report-interval** command sets the interval at which an AP reports LLDP neighbor information.

The **undo lldp report-interval** command restores the default interval at which an AP reports LLDP neighbor information.

By default, an AP reports LLDP neighbor information at an interval of 30 seconds.

Format

lldp report-interval *interval-time*

undo lldp report-interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which an AP reports LLDP neighbor information to an AC.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **lldp report-interval** command to adjust the interval at which an AP reports LLDP neighbor information. This prevents LLDP neighbor information from being frequently reported.

Example

Set the interval at which an AP reports LLDP neighbor information to an AC to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp report-interval 20
```

11.2.132 lldp restart-delay

Function

The **lldp restart-delay** command sets the delay in re-enabling LLDP on an AP.

The **undo lldp restart-delay** command restores the default delay in re-enabling the LLDP function on an AP.

By default, the delay in re-enabling LLDP on an AP is 2 seconds.

Format

lldp restart-delay *delay-time*

undo lldp restart-delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in re-enabling LLDP.	The value is an integer that ranges from 1 to 10, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When the LLDP status of an AP changes, the AP reports LLDP neighbor information. Setting the delay in re-enabling LLDP on the AP prevents the AP from frequently reporting LLDP neighboring information when the LLDP status of the AP frequently changes.

Example

Set the delay in re-enabling LLDP on an AP to 1 second.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] lldp restart-delay 1
```

11.2.133 lldp tlv-enable (AP wired port link profile view)

Function

The **lldp tlv-enable** command specifies the types of TLVs that an AP wired interface advertises.

The **undo lldp tlv-enable** command specifies the types of TLVs that an AP wired interface is prohibited from advertising.

By default, an AP wired interface advertises all types of TLVs.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

lldp tlv-enable dot3-tlv power

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable dot3-tlv power

Parameters

Parameter	Description	Value
basic-tlv	Indicates basic TLVs to be advertised: ● Management-address TLV ● Port Description TLV ● System Capabilities TLV ● System Description TLV ● System Name TLV	-
all	Configures the AP wired interface to advertise all types of TLVs when basic TLVs are configured.	-
management-address	Configures the AP wired interface to advertise Management-address TLVs.	-
port-description	Configures the AP wired interface to advertise Port Description TLVs.	-
system-capability	Configures the AP wired interface to advertise System Capabilities TLVs.	-
system-description	Configures the AP wired interface to advertise System Description TLVs.	-
system-name	Configures the AP wired interface to advertise System Name TLVs.	-

Parameter	Description	Value
dot3-tlv	Configures an AP's wired interface to advertise TLVs defined by IEEE 802.3.	-
power	Configures an AP's wired interface to advertise the Power Via MDI TLV defined by IEEE 802.3 and negotiate the PoE power.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs and TLVs in the IEEE 802.3 format.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.3 format are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the TLVs in the IEEE 802.3 format.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

The LLDP function has been enabled in both the WLAN view and AP wired port link profile view.

Precautions

When basic TLVs are configured, if the **all** parameter is specified, all optional basic TLVs are advertised. If the **all** parameter is not specified, TLVs of only one type can be advertised at a time. To advertise multiple types of TLVs, run this command multiple times.

Example

Configure the wired interface of AP to advertise Management-address TLVs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap lldp enable
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp tlv-enable basic-tlv management-address
```

11.2.134 lldp tlv-enable legacy-tlv four-pair-power (AP wired port link profile view)

Function

The **lldp tlv-enable legacy-tlv four-pair-power** command configures an AP's wired interface to advertise Cisco's customized TLVs.

The **undo lldp tlv-enable legacy-tlv four-pair-power** command prohibits an AP's wired interface from advertising Cisco's customized TLVs.

By default, an AP's wired interface advertises Cisco's customized TLVs.

Format

lldp tlv-enable legacy-tlv four-pair-power

undo lldp tlv-enable legacy-tlv four-pair-power

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some Cisco's switches use customized LLDP TLVs to negotiate the UPoE power supply. If such a switch is used to supply UPoE power to an AP, the AP's wired interface connected to the switch must be enabled to advertise Cisco's customized TLVs for UPoE power negotiation. Otherwise, LLDP negotiation fails. If interfaces on the Cisco's switch do not supply UPoE power, the AP is provided with insufficient input power and cannot work properly.

Example

Configure an AP's wired interface to advertise Cisco's customized TLVs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp tlv-enable legacy-tlv four-pair-power
```

11.2.135 lldp tlv-enable legacy-tlv power-capability (AP wired port link profile view)

Function

The **lldp tlv-enable legacy-tlv power-capability** command configures LLDP packets sent by an AP to carry the supported power capability.

The **undo lldp tlv-enable legacy-tlv power-capability** command configures LLDP packets sent by an AP not to carry the supported power capability.

By default, the LLDP packets sent by an AP carry the supported power capability.

Format

lldp tlv-enable legacy-tlv power-capability

undo lldp tlv-enable legacy-tlv power-capability

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When directly connected to a Huawei PoE switch, the AP can send its power capability to the switch through LLDP. If the total output power of the PoE switch exceeds the threshold, the switch adjusts the output power of the corresponding Ethernet port based on the power capability of the AP. This reduces the output power without affecting the basic functions of the AP.

Example

Configure the LLDP packets sent by an AP to carry the supported power capability.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] lldp tlv-enable legacy-tlv power-capability
```

11.2.136 location

Function

The **location** command configures the installation position of an AP.

The **undo location** command deletes the installation position of an AP.

By default, an AP's installation position is not configured.

NOTE

This command is not available for the following APs:

- AirEngine 5761-10W and AirEngine 5761S-10W

Format

location *location-value*

undo location

Parameters

Parameter	Description	Value
location-value	Specifies the installation position of an AP.	The value is a string of 1 to 63 case-sensitive characters. If the value contains space, it must start and end with double quotation marks ("), for example, **"hello name1"**. Each double quotation mark in the value occupies one character. The value cannot start or end with spaces and double quotation marks ("). For example, **" HELLO"** and **"HELLO "** are not allowed.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the installation position of an AP.

Example

Configure the installation position of an AP to **B2-5F-01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] location B2-5F-01
```

11.2.137 log-record-level

Function

The **log-record-level** command configures the level for AP logs that need to be backed up.

The **undo log-record-level** command restores the default level of AP logs that need to be backed up.

By default, the level of AP logs that need to be backed up is **info**.

Format

log-record-level { **alert** | **critical** | **debug** | **emergency** | **error** | **info** | **notice** | **warning** }

undo log-record-level

Parameters

Parameter	Description	Value
alert	Configures the level of logs as **alert**, that is, the AP backs up logs that need to be processed immediately.	-
critical	Configures the level of logs as **critical**, that is, the AP backs up critical logs.	-
debug	Configures the level of logs as **debug**, that is, the AP backs up debugging logs.	-
emergency	Configures the level of logs as **emergency**, that is, the AP backs up unavailable logs.	-
error	Configures the level of logs as **error**, that is, the AP backs up error logs.	-
info	Configures the level of logs as **info**, that is, the AP backs up normal logs.	-
notice	Configures the level of the logs as **notice**, that is, the AP backs up logs that need to be noticed.	-

Parameter	Description	Value
warning	Configures the level of logs as **warning**, that is, the AP backs up warning logs.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP periodically backs up logs to the log server. However, not all the logs need to be backed up. You can run the **log-record-level** command to configure the level of logs to be periodically backed up.

Precautions

The preference order of log levels is emergency, alert, critical, error, warning, notice, info, and debug.

After you specify the level for AP logs that need to be backed up, all logs of the specified level or a higher level will be backed up. For example, if you set the level of AP logs that need to be backed up to **critical**, the logs of the levels **emergency**, **alert**, and **critical** will be backed up.

Example

Set the level of logs that need to be backed up as **alert**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] log-record-level alert
```

11.2.138 log-server

Function

The **log-server** command configures the log server IP address and port number in the AP system profile and enables log backup on the AP.

The **undo log-server** command restores the default log server IP address and port number in the AP system profile and disables log backup on the AP.

By default, the port number of the log server is 514 in UDP mode, the log server IP address is not configured in an AP system profile, and log backup is disabled on an AP.

Format

log-server ip-address *server-ip-address* [**port** *port*]

undo log-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies the IPv4 address of the log server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of the log server.	The value is an integer that ranges from 1 to 65535. The default port number is 514.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **log-server** command to configure the log server IP address and port number in the AP system profile and enable log backup on the AP. After log backup is enabled, the AP automatically sends logs to the log server with the specified IP address.

NOTICE

Modifying the configuration of an AP system profile changes configurations of all APs using this profile.

Example

Set the IP address of the log server to 10.0.0.1 and port number to 2000 and enable log backup on the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] log-server ip-address 10.0.0.1 port 2000
```

11.2.139 low-temperature threshold

Function

The **low-temperature threshold** command sets a lower device, ambient, CPU, or NP module temperature alarm threshold for APs.

The **undo low-temperature threshold** command restores the default lower device, ambient, CPU, or NP module temperature alarm threshold of APs.

Table 11-127 Default lower temperature alarm threshold for APs

AP Model	Default Value (°C)
/AirEngine 9700D-M1 (AP device and environment)	-3

NOTE

This command is not supported by the following models:

- AirEngine series APs

Format

low-temperature [**ap-environment** | **cpu** | **np**] **threshold** *threshold*

undo low-temperature [**ap-environment** | **cpu** | **np**] **threshold**

Parameters

Parameter	Description	Value
ap-environment	Indicates the ambient temperature.	-
cpu	Indicates the CPU temperature.	-
np	Indicates the NP module temperature.	-
threshold	Specifies the lower temperature alarm threshold.	The value is an integer that ranges from -70 to +10, in °C.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the lower temperature alarm threshold for an AP. When an AP's temperature exceeds the lower threshold, the AP generates an alarm and a log, and notifies the AC of the low temperature alarm.

The parameter **ap-environment** is supported only by the AirEngine 9700D-M and AirEngine 9700D-M1. The parameters **cpu** and **np** are supported only by the AirEngine 9700D-M.

If **ap-environment** | **cpu** | **np** is not specified, this command sets a lower temperature alarm threshold for APs.

Example

Set the lower temperature alarm threshold for APs to 5°C.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] low-temperature threshold 5
```

11.2.140 mac-learning (AP wired port profile view)

Function

The **mac-learning** command configures the MAC address learning priority and packet forwarding policy of an AP's wired interface.

The **undo mac-learning** command restores the default MAC address learning priority and packet forwarding policy of an AP's wired interface.

By default, the MAC address learning priority of an AP's wired interface is 0 and the packet forwarding policy is forward.

Format

mac-learning { **priority** *priority* | **action discard** }*

undo mac-learning priority

undo mac-learning action

Parameters

Parameter	Description	Value
priority *priority*	Specifies the MAC address learning priority of an AP's wired interface.	The value is an integer that ranges from 0 to 3. A larger value indicates a higher priority.
action discard	Configures an AP's wired interface to discard the packet if a wired interface with a higher MAC address learning priority has learned the same MAC address as that carried in this packet.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP with multiple network interfaces connects to the upper-layer network through its uplink interfaces and provides access to STAs through its downlink interfaces. If the interfaces with different MAC address learning priorities learn the same MAC address, the MAC address entry learned by the interface with the highest priority overrides those learned by other interfaces, but not vice versa.

When an interface with a lower MAC address learning priority receives a packet carrying the MAC address learned by an interface with a higher priority, the local interface can be configured to discard or forward the packet.

Example

Set the MAC address learning priority to 1 in an AP wired port profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mac-learning priority 1
```

11.2.141 management-vlan (AP system profile view, AP provisioning view, AP view)

Function

The **management-vlan** command configures CAPWAP packets sent from an AP's wired interface to carry a management VLAN tag.

The **undo management-vlan** command configures CAPWAP packets sent from an AP's wired interface not to carry a management VLAN tag.

In the AP system profile view and AP view, the **undo management-vlan** command configures CAPWAP packets sent from an AP's wired interface not to carry a management VLAN tag. In the AP provisioning view, the **undo management-vlan** command disables the AC from delivering this parameter setting to APs after the configuration is delivered using the **commit** command.

By default, CAPWAP packets sent from an AP's wired interface do not carry a management VLAN tag.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of the management VLAN tag carried in CAPWAP packets sent from an AP's wired interface.	The value is an integer that ranges from 1 to 4094.

Views

AP system profile view, AP provisioning view, AP view

Default Level

2: Configuration level

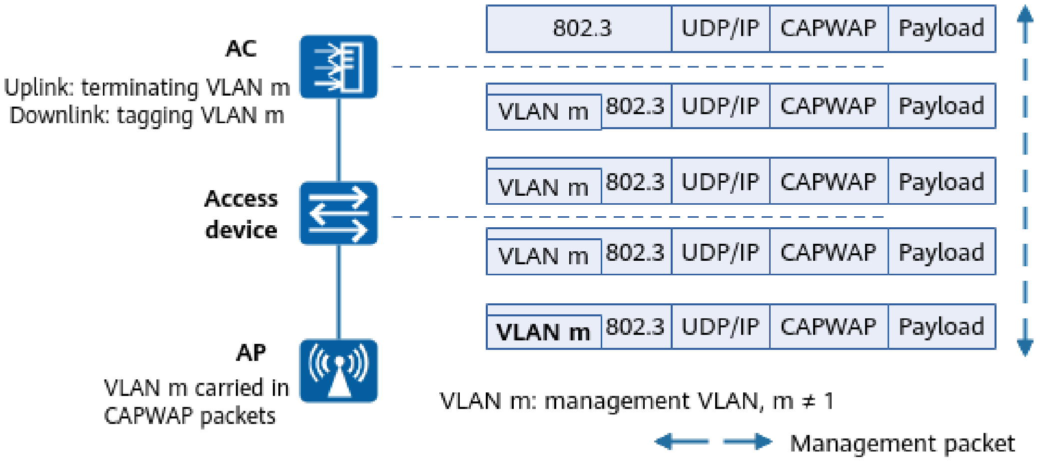
Usage Guidelines

Usage Scenario

By default, CAPWAP packets sent from an AP's wired interface do not carry a management VLAN tag. In most cases, the access switch interface directly connected to the AP adds the tag of the PVID to the CAPWAP packets as the management VLAN ID.

If the access device (for example, an unmanaged switch) does not support the VLAN function or the PVID of the device has been used for other purposes (for example, as the default VLAN ID of wired users), the access device cannot add the management VLAN tag to packets on the interface directly connected to the AP. In this case, you can configure CAPWAP packets sent by an AP's wired interface to carry the management VLAN tag so that the AP adds the management VLAN tag to the CAPWAP packets before sending them to the AC.

Figure 11-1 Flowchart for configuring CAPWAP packets sent by an AP's wired interface to carry the management VLAN tag



Precautions

This configuration takes effect only after the APs restart if the **management-vlan** command is configured in the AP system profile view or AP view.

If the **management-vlan** command is configured in the AP provisioning view, run the **commit** command to deliver the configuration. The configuration takes effect after the APs restart.

On a Mesh network, ensure that CAPWAP packets sent from all APs carry the same management VLAN. Otherwise, Mesh Points (MPs) cannot go online.

Based on the access device capability and PVID configuration, the requirements for configuring CAPWAP packets sent by an AP to carry the management VLAN tag are described in the following table.

Table 11-128 Requirements for configuring CAPWAP packets to carry the management VLAN tag

Access Device Capability and PVID Configuration	AP Configuration Requirements
The access device does not support the VLAN function.	CAPWAP packets are enabled to carry the management VLAN tag. Additionally, ensure that the AP's uplink wired interface is added to the management VLAN in tagged mode. By default, an AP's uplink wired interface joins all VLANs except VLAN 1 in tagged

Access Device Capability and PVID Configuration	AP Configuration Requirements
The access device supports the VLAN function, and the PVID of the interface directly connected to the AP is different from the management VLAN ID.	mode. Therefore, no additional configuration is required. To modify the configuration, run the **vlan tagged** *vlan-id* command in the AP wired port profile view and bind the profile to an AP or AP group.
The access device supports the VLAN function, and the PVID of the interface directly connected to the AP is the same as the management VLAN ID.	CAPWAP packets sent by an AP do not carry the management VLAN tag. The access device adds the management VLAN tag to CAPWAP packets. **NOTE** In this case, to enable CAPWAP packets to carry the management VLAN tag, run the **vlan pvid** *vlan-id* command to configure the PVID of the AP's uplink wired interface to be the same as the management VLAN ID. Otherwise, the AP cannot receive management packets, causing repeated disconnection and restart.

After the **management-vlan** *vlan-id* command is executed to configure AP's wired interfaces to send CAPWAP packets carrying the management VLAN tag (not VLAN 1), the interfaces working in **root** mode are added to VLAN 1 in tagged mode, which cannot be changed.

Example

Configure CAPWAP packets sent from an AP's wired interface to carry management VLAN 2 in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] management-vlan 2
Warning: The incorrect management VLAN configuration will cause the AP to go out of management. This
operation will make the AP reset. Continue? [Y/N]:y
```

Configure CAPWAP packets sent from a wired interface on AP 0 to carry management VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] management-vlan 2
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and ma
y cause reboot of AP(s). Continue?[Y/N]:y
```

Configure CAPWAP packets sent from an AP's wired interface to carry management VLAN 2 in the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap] management-vlan 2
Warning: The incorrect management VLAN configuration will cause the AP to go out of management.
```

```
When the configuration is committed,
 the AP will reset.Continue?[Y/N]:y
```

11.2.142 memory-usage threshold

Function

The **memory-usage threshold** command configures a memory usage alarm threshold for APs.

The **undo memory-usage threshold** command restores the default memory usage alarm threshold.

By default, the memory usage alarm threshold on an AP is 80.

Format

memory-usage threshold *threshold*

undo memory-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies the memory usage alarm threshold of an AP.	The value is an integer that ranges from 30 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **memory-usage threshold** command to configure the memory usage alarm threshold in the AP system profile view. The configuration is delivered to all APs using the profile.

- When the memory usage of an AP exceeds the alarm threshold, .
- When the memory usage of an AP falls below the alarm threshold, .

Example

Set the memory usage alarm threshold of AP 0 to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] memory-usage threshold 60
```

11.2.143 mld-snooping enable (AP wired port profile view)

Function

The **mld-snooping enable** command enables MLD snooping on an AP's wired interface.

The **undo mld-snooping enable** command disables MLD snooping on an AP's wired interface.

By default, MLD snooping is disabled on an AP's wired interface.

Format

mld-snooping enable

undo mld-snooping enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD snooping is a basic IPv6 Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. MLD snooping runs on a Layer 2 device and analyzes MLD messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

Prerequisites

An AP wired port profile has been created.

Precautions

The AP wired interfaces added to an Eth-trunk interface do not support this function.

Example

Enable MLD snooping on AP wired port profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] wired-port-profile name p1
[HUAWEI-wlan-wired-port-p1] mld-snooping enable
```

11.2.144 mode (AP wired port profile view)

Function

The **mode** command sets the working mode for an AP's wired interface.

The **undo mode** command restores the default working mode of an AP's wired interface.

By default, the working modes of APs' wired interfaces vary depending on the AP models.

Table 11-129 Working modes of APs' wired interfaces

AP Model	root	endpoint	middle
AirEngine series indoor settled APs	All interfaces (including Eth-Trunk interfaces)	-	-
AirEngine series outdoor APs	All interfaces (including Eth-Trunk interfaces)	-	-
AirEngine series wall plate APs and RUs	Uplink port	Downlink port	-
AirEngine series central APs	Uplink port	-	Downlink port
AirEngine 9700D-S	GE port	-	-

NOTE

The working modes of wired interfaces cannot be changed on the following models:

Format

mode { **root** | **endpoint** | **middle** }

undo mode

Parameters

Parameter	Description	Value
root	Sets the working mode of an AP's wired interface to root, which can connect to an AC.	-
endpoint	Sets the working mode of an AP's wired interface to endpoint, which can connect to a host.	-
middle	Sets the working mode of an AP's wired interface to middle, which allows a central AP to connect to an RU.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When working as an uplink interface to connect to an AC, an AP's wired interface must work in root mode. In root mode, the AP's wired interface automatically joins service VLANs and user-specific VLANs (for example, VLANs assigned by the RADIUS server).

When working as a downlink interface to connect to a wired terminal, the AP's wired interface must work in endpoint mode. In endpoint mode, the AP's wired interface does not join any VLAN by default.

When the central AP connects to RUs through downlink GE interfaces, the working mode of the downlink GE interfaces must be set to **middle**.

Precautions

When the AP's wired interface works in root mode, user isolation cannot be configured. User isolation can be configured on an AP's wired interface only when the interface works in endpoint or middle mode.

When the AP's wired interface works in root mode and has been configured to transmit packets carrying the management VLAN tag using the **management-vlan** *vlan-id* command, the PVID for the AP's wired interface must be configured the same as the management VLAN ID. If the AP's wired interface works in endpoint mode, the PVID can be configured directly. If the AP's wired interface works in middle mode, the PVID cannot be configured.

The configuration of the AP's wired interface takes effect after the AP is restarted.

Example

Set the working mode of the AP's wired interface ETH0 to **endpoint**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the
AP to go out of management . This fault can be recovered only by modifying the configuration on the AP.
Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired ethernet 0
```

11.2.145 mtu

Function

The **mtu** command sets the maximum transmission unit (MTU) value for the management VLANIF and CAPWAP on an AP.

The **undo mtu** command restores the default MTU value for the management VLANIF and CAPWAP on an AP.

By default, the MTU value of the management VLANIF and CAPWAP on an AP is 1500 bytes.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the maximum size of packets sent and received on the management VLANIF and CAPWAP.	The value is an integer that ranges from 1000 to 1700, in bytes.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MTU determines the maximum number of bytes in IP packets each time a sender can send. The MTU of an IP packet refers to the number of bytes from the IP header of the packet to the data.

The MTU in the AP system profile view is the maximum size of packets sent and received on the management VLANIF and CAPWAP of an AP.

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU. If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Therefore, a proper MTU is a prerequisite for normal communication on a network.

- If the configured MTU is excessively small and the packet size is larger, packets are discarded when being forwarded through the forwarding chip; packets are broken into a great number of fragments when being forwarded through the CPU, affecting proper data transmission.
- If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, aggravating the network transmission load.

The default MTU is recommended. When the size of packets to be transmitted or the device that receives packets changes, you can change the MTU based on the actual network.

Precautions

- DHCP packets cannot be fragmented. When the MTU value set using the **mtu** command is smaller than the DHCP packet length, DHCP packets cannot be forwarded. Therefore, set a larger MTU value.
- If the MTU value is smaller than the DHCP packet length, the AP may be disconnected. In this case, restart the AP.
- When the MTU is too small and the DF bit is set to 1, packets cannot be fragmented. In this case, use the forced fragmentation function.

Example

Set the MTU value of the management VLANIF and CAPWAP on an AP to 1700 bytes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] mtu 1700
```

11.2.146 multicast-rate

Function

The **multicast-rate** command configures the multicast rate of wireless packets in a radio profile.

The **undo multicast-rate** command restores the default multicast rate of wireless packets in a radio profile.

By default, the multicast rate of wireless packets is not configured in a radio profile. That is, the multicast rate is set to auto-sensing.

Format

multicast-rate *multicast-rate*

undo multicast-rate

Parameters

Parameter	Description	Value
multicast-rate	Specifies the multicast rate of wireless packets in a radio profile.	The value is of the enumerated type: The values are as follows in a 2G radio profile: ● 1: 1 Mbit/s ● 2: 2 Mbit/s ● 5: 5.5 Mbit/s ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 11: 11 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s The values are as follows in a 5G radio profile: ● 6: 6 Mbit/s ● 9: 9 Mbit/s ● 12: 12 Mbit/s ● 18: 18 Mbit/s ● 24: 24 Mbit/s ● 36: 36 Mbit/s ● 48: 48 Mbit/s ● 54: 54 Mbit/s

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After this command is run, the multicast rate of wireless packets is the configured value and irrelevant to the STA access mode.

If the configured multicast rate is not in the basic rate set and the STA does not support this rate, the STA cannot receive multicast data.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, *multicast-rate* that takes effect on the 2 GHz radio of the AP is fixed as 1 Mbit/s, and *multicast-rate* configured in the 2G radio profile view does not take effect on the AP.

Example

Set the multicast rate of wireless packets to 54 Mbit/s in the 2G radio profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] multicast-rate 54
```

11.2.147 multicast-suppression auto-detect (AP system profile view)

Function

The **multicast-suppression auto-detect** command configures the rate limit for multicast packets during intelligent flow control.

The **undo multicast-suppression auto-detect** command restores the default rate limit for multicast packets during intelligent flow control.

By default, the rate limit for multicast packets is 256 pps.

NOTE

This function is not supported by the following models:

- AirEngine X760 series APs (excluding the AirEngine 5760-10)
- AirEngine 9700D-S (including matching ORUs)

Format

multicast-suppression auto-detect packets *packets*

undo multicast-suppression auto-detect

Parameters

Parameter	Description	Value
packets *packets*	Specifies the rate limit for multicast packets.	The value is an integer that ranges from 64 to 1024, in pps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When there are a large number of broadcast, multicast, and unknown unicast packets, the CPU becomes busy processing these packets and the buffer of the packet for receiving incoming packets is occupied. When the buffer decreases to the specified threshold, the device automatically rate-limits the broadcast, multicast, and unknown unicast packets. You can run this command to specify the rate limit for intelligent flow control as required. Rate limiting takes effect only for incoming traffic.

Example

Set the rate limit for multicast packets during intelligent flow control to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] multicast-suppression auto-detect packets 300
```

11.2.148 np capwap-reassembly (AP system profile view)

Function

The **np capwap-reassembly disable** command disables the NP CAPWAP reassembly function of the AP.

The **undo np capwap-reassembly disable** command restores the default status of the NP CAPWAP reassembly function of APs.

By default, the NP CAPWAP reassembly function operates in adaptive mode for APs. That is, this function is enabled when services run properly, and is automatically disabled upon an exception.

NOTE

NP CAPWAP reassembly is supported only by AirEngine X760 series APs and AirEngine 9700D-S (including matching ORUs).

Format

np capwap-reassembly disable

undo np capwap-reassembly disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the NP CAPWAP reassembly function, the NP replaces the CPU to reassemble the received CAPWAP fragments. This speeds up the packet processing and improves the forwarding performance.

Precautions

If the **np fast-forwarding disable** command has been run, the NP CAPWAP reassembly function of the AP is also disabled. To enable NP CAPWAP reassembly of the AP, run the **undo np fast-forwarding disable** and **undo np capwap-reassembly disable** commands in sequence.

Example

Disable the NP CAPWAP reassembly function of the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] np capwap-reassembly disable
```

11.2.149 np fast-forwarding disable (AP system profile view)

Function

The **np fast-forwarding disable** command disables the NP fast forwarding function of APs.

The **undo np fast-forwarding disable** command enables the NP fast forwarding function of APs.

By default, the NP fast forwarding function of APs is enabled.

NOTE

NP fast forwarding is supported only by the following APs:

- AirEngine 9700D-M, AirEngine 8760-X1-PRO, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD
- AirEngine 9700D-S (including matching ORUs)
- AirEngine 5762 series

Format

np fast-forwarding disable

undo np fast-forwarding disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

With the NP fast forwarding function, the NP replaces the CPU to forward some packets. This speeds up the packet processing and improves the forwarding performance.

Example

Disable the NP fast forwarding function of APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] np fast-forwarding disable
```

11.2.150 password alert before-expire (AP password policy view)

Function

The **password alert before-expire** command sets the password expiration prompt days.

The **undo password alert before-expire** command restores the default password expiration prompt days.

By default, the number of password expiration prompt days is 30 days.

Format

password alert before-expire *days*

undo password alert before-expire

Parameters

Parameter	Description	Value
days	Indicates how long the system displays a prompt before the password expires. If the value is set to 0, the device does not prompt users that the passwords will expire.	The value is an integer that ranges from 0 to 999, in days. The default value is 30.

Views

AP password policy view

Default Level

3: Management level

Usage Guidelines

When a user logs in to the device, the device checks whether the validity period of the user's password is within the prompt days set by using this command. If so, the device prompts the user how long the password will expire and asks the user whether to change the password.

- If the user changes the password, the device records the new password and modification time.
- If the user does not change the password or fails to change the password, the user can still log in as long as the password does not expire.

Example

Set the number of password expiration prompt days to 90.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password alert before-expire 90
```

11.2.151 password alert original (AP password policy view)

Function

The **password alert original** command enables the device to prompt users to change initial passwords upon the login to an AP.

The **undo password alert original** command disables the device from prompting users to change initial passwords upon the login to an AP.

By default, the initial password change prompt function is enabled.

Format

password alert original

undo password alert original

Parameters

None

Views

AP password policy view

Default Level

3: Management level

Usage Guidelines

To improve device security, you can use this command to enable the device to prompt users to change initial passwords upon the login to the AP. Upon login to an AP, if the initial password is used, the system prompts users to change the password.

Executing the **undo password alert original** command will disable the initial password change prompt function upon the login to an AP, which will bring security risks.

Example

Enable the initial password change prompt function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password alert original
```

11.2.152 password expire (AP password policy view)

Function

The **password expire** command sets the password validity period.

The **undo password expire** command restores the default password validity period.

By default, the password validity period is 90 days.

Format

password expire *days*

undo password expire

Parameters

Parameter	Description	Value
days	Indicates the password validity period. If the value is 0, the password is permanently valid.	The value is an integer that ranges from 0 to 999, in days. The default value is 90.

Views

AP password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, the administrator can use this command to set the validity period for local user's password. When the validity period expires, the password becomes invalid.

If the local user still uses this password to log in to the device, the device allows the user to log in, prompts the user that the password has expired, and asks the user whether to change the password:

- If the user selects **Y** to change the password, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet requirements (password length and complexity). After the password is changed, the user can log in to the device successfully.
- If the user selects **N** or fails to change the password, the user cannot log in.

Precautions

Changing the system time will affect the password validity status.

After this command is executed, the device checks whether the password expires every one minute; therefore, there may be a time difference within one minute.

Example

Set the password validity period to 120 days.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password expire 120
```

11.2.153 password history record number (AP password policy view)

Function

The **password history record number** command sets the maximum number of historical passwords recorded for each AP login user.

The **undo password history record number** command restores the default maximum number of historical passwords recorded for each user.

By default, a maximum of five historical passwords are recorded for each user.

Format

password history record number *number*

undo password history record number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of historical passwords recorded for each user. If the value is set to 0, the device will not check whether a changed password is the same as any historical password.	The value is an integer that ranges from 0 to 12. The default value is 5.

Views

AP password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, it is not recommended that you use a previously used password. You can set the maximum number of historical passwords recorded for each user. When a user changes the password, the device compares the new password against the historical passwords stored on the device. If the new password is the same as a stored password, the device displays an error message to prompt the user that password change fails.

Precautions

When the number of recorded historical passwords reaches the maximum value, the later password will overwrite the earliest password on the device.

Example

Set the maximum number of historical passwords recorded for each AP login user to 10.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap password policy
[HUAWEI-wlan-ap-pwd-policy] password history record number 10
```

11.2.154 pki realm (AP PKI realm profile view)

Function

The **pki realm** command configures a name for an AP PKI realm and binds the CA certificate, local certificate, CRL file, and private key file to the realm.

The **undo pki realm** command deletes the configuration of a PKI realm in an AP PKI realm profile.

By default, no name is configured for an AP PKI realm, and the CA certificate, local certificate, CRL file, and private key file are not bound to the realm.

Format

pki realm *realm-name* { { **ca format** { **der** *file-name* | **pem** *file-name* | **pkcs12** *file-name* **password** *password* } } | { **local format** { **der** *file-name* | **pem** *file-name* | **pkcs12** *file-name* **password** *password* } [**private-key format** { **der** *file-name* | **pem** *file-name* **password** *password* | **pkcs12** *file-name* **password** *password* }] } } *

undo pki realm *realm-name*

pki realm *realm-name* **crl-filename** *file-name*

undo pki realm *realm-name* **crl-filename**

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The value is a string of 1 to 50 case-sensitive characters without spaces.
ca	Specifies a CA certificate.	-
local	Specifies a local certificate.	-
private-key	Specifies the private key file of a local certificate.	-
format	Specifies the file format.	-

Parameter	Description	Value
der	Sets the file format to DER.	-
pkcs12	Sets the file format to PKCS12.	-
pem	Sets the file format to PEM.	-
file-name	Specifies the name of the CA certificate, local certificate, or private key file to be imported.	The value is a string of 1 to 50 case-sensitive characters without spaces.
password *password*	Specifies the decryption password of a private key file.	The password can be entered in plaintext or ciphertext: ● A plaintext password is a string of 6 to 32 characters. ● A ciphertext password is a string of 48 or 68 characters, and must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.
crl-filename *file-name*	Specifies the name of a CRL file to be imported.	The value is a string of 1 to 50 case-sensitive characters without spaces.

Views

AP PKI realm profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the AP PKI realm profile view, configure a name for an AP PKI realm and bind the CA certificate, local certificate, CRL file, and private key file to the realm.

Prerequisites

1. An AP PKI realm profile has been created using the **ap-pki-profile (WLAN view)** command.

Follow-up Procedure

1. Run the **ap-pki-profile (AP group view and AP view)** command to bind the AP PKI realm profile to an AP or AP group.
2. Run the **load-file (WLAN view)** command to manually load a certificate file in the AP PKI realm to an AP.

Precautions

A maximum of five PKI realms can be configured in an AP PKI realm profile, and private keys can be configured in a maximum of three PKI realms. To check information about an AP PKI realm profile, run the **display ap-pki-profile** command.

To ensure network security, it is recommended that the public key length and private key length of a certificate file be greater than or equal to 3072 bits.

To update a certificate file, run the **load-file (WLAN view)** command to manually load the certificate file in the AP PKI realm to the AP. The latest configuration overrides the previous one.

Example

In the AP PKI realm profile **default**, set the PKI realm name to **r1**, and set the certificate files in the realm as follows: CA certificate file **1.txt** in **DER** format, local certificate file **2.txt** in **PEM** format, and private key file **3.txt** in **PEM** format (private key decryption password: **YsHsjx_202206**).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-pki-profile name default
[HUAWEI-wlan-ap-pki-prof-default] pki realm r1 ca format der 1.txt local format pem 2.txt private-key format pem 3.txt password YsHsjx_202206
```

11.2.155 poe af-inrush enable (AP system profile view)

Function

The **poe af-inrush enable** command configures an AP to provide PoE power in compliance with IEEE 802.3af.

The **undo poe af-inrush enable** command restores the default PoE power supply standard of an AP.

By default, an AP provides PoE power in compliance with IEEE 802.3at.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe af-inrush enable

undo poe af-inrush enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AP that conforms to IEEE 802.3at cannot power non-IEEE standard PDs that do not support inrush current. To power these PDs, configure the AP to provide power with low current in conformance to IEEE 802.3af. When all PDs connected to the AP are IEEE standard-compliant PDs, run the **undo poe af-inrush enable** command to cancel the configuration.

Precautions

- The **poe af-inrush enable** command does not take effect on an interface if the **poe force-power (AP wired port link profile view)** command has been executed on the interface.
- After this command is configured, the AP cannot provide power for IEEE 802.3at-compliant PDs.

Configuration Impact

After running the **poe af-inrush enable** command, remove the non-IEEE 802.3at PDs and then install them so that the PDs can be powered on.

Example

Set the PoE power supply standard to IEEE 802.3af for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe af-inrush enable
```

11.2.156 poe disable (AP wired port link profile view)

Function

The **poe disable** command disables the PoE function on an AP's wired interface.

The **undo poe disable** command enables the PoE function on an AP's wired interface.

By default, the PoE function is enabled on an AP's interface.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe disable

undo poe disable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using an AP to provide power for PDs connected to its interfaces, ensure that the PoE function is enabled on the interfaces. To enable the PoE function on an interface, run the **undo poe disable** command.

The power-on and power-off of interfaces are determined by the PoE power and interface power priority. When the PoE power is sufficient, the device does not power off one interface. To stop providing power for one PD, run the **poe disable** command.

Precautions

The AP only supports PoE power supply on downlink interfaces and does not support PoE power supply on uplink interfaces.

Example

Disable the PoE function on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe disable
```

11.2.157 poe force-power (AP wired port link profile view)

Function

The **poe force-power** command enables forcible PoE power supply on an interface.

The **undo poe force-power** command disables forcible PoE power supply on an interface.

By default, forcible PoE power supply is disabled on an interface.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe force-power

undo poe force-power

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is configured, an interface forcibly powers on the connected PD even if the PSE cannot identify the PD. Before powering on the interface, ensure that the system power is sufficient.

Precautions

If a PoE interface connects to a non-PoE device, use this command with caution.

Example

Enable forcible PoE power supply on an AP's interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe force-power
```

11.2.158 poe high-inrush enable (AP system profile view)

Function

The **poe high-inrush enable** command configures an interface to allow high inrush current during power-on.

The **undo poe high-inrush enable** command disables an interface from allowing high inrush current during power-on.

By default, interfaces do not allow high inrush current during power-on.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe high-inrush enable

undo poe high-inrush enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

High inrush current is generated when a non-standard PD is powered on. In this case, the PSE cuts off the power of the PD to protect itself. If the PSE is required to provide power for the PD, the PSE must allow high inrush current.

Precautions

NOTICE

The high inrush current may damage components of a PD.

Example

Enable the AP to allow high inrush current during power-on.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe high-inrush enable
```

11.2.159 poe legacy enable (AP wired port link profile view)

Function

The **poe legacy enable** command enables an AP to check compatibility of the connected PDs.

The **undo poe legacy enable** command disables an AP from checking compatibility of the connected PDs.

By default, an AP does not check compatibility of the connected PDs.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe legacy enable

undo poe legacy enable

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When compatibility check is enabled, an AP (PSE) can detect and provide power for the PDs incompliant with IEEE 802.3af or 802.3at. If compatibility check is disabled, the AP does not identify or provide power for these PDs.

Example

Enable an AP to check compatibility of the connected PDs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe legacy enable
```

11.2.160 poe max-power (AP system profile view)

Function

The **poe max-power** command sets the maximum output power of an AP.

The **undo poe max-power** command restores the maximum output power of an AP to the default value.

By default, the maximum output power of the AP is the total power that the PoE power supply provides for PDs.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe max-power *max-power*

undo poe max-power

Parameters

Parameter	Description	Value
max-power	Specifies the maximum output power of an AP.	The value ranges from 15400 mW to 750000 mW.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the system automatically obtains the maximum PoE power supported by the AP. You can run the **poe max-power** command to set the maximum output power to ensure stable PoE power supply when the total power of the AP is insufficient.

Precautions

If the maximum output power that you set is smaller than the total power required by PDs, PDs with lower priority are powered off.

The configured maximum output power must be smaller than the total power that the PoE power supply provides for PDs.

Example

Set the maximum output power of an AP to 20000 mW.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe max-power 20000
```

11.2.161 poe power-reserved (AP system profile view)

Function

The **poe power-reserved** command configures the percentage of the reserved PoE power against the total PoE power on an AP.

The **undo poe power-reserved** command restores the default percentage of the reserved PoE power against the total PoE power on an AP.

By default, the percentage of the reserved PoE power against the total PoE power on an AP is 0%.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe power-reserved *power-reserved*

undo poe power-reserved

Parameters

Parameter	Description	Value
power-reserved	Specifies the percentage of the reserved PoE power against the total PoE power.	The value is an integer that ranges from 0 to 100, in percentage.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AP can dynamically allocate power to each interface according to the power consumption of each interface. The power consumption of a PD keeps changing when the PD is running. The system periodically calculates the total power consumption of all the PDs. If the total power consumption exceeds the upper threshold of the AP, the system cuts off the power of the PDs on the interfaces of low priority to ensure that other PDs can run normally.

Sometimes, however, the power consumption increases sharply and the available power of the system cannot support the burst increase of power. At this time, the system has not calculated and found that the total power consumption exceeded the upper threshold; therefore, the system does not cut off power low-priority interfaces in time. As a result, the PoE power supply is shut down for overload protection, and all PDs are powered off.

This problem can be solved by running the **poe power-reserved** command to set proper reserved power. When there is a burst increase in power consumption, the reserved power can support the system running. Then the system has time to power off interfaces of low priority to ensure stable running of other PDs.

Precautions

You can set the maximum output power of an AP using the **poe max-power (AP system profile view)** command. The available PoE power is the configured maximum output power. If no maximum output power is configured, the available PoE power is the total power provided by the PoE power supply.

Example

Set the percentage of reserved PoE power to the total PoE power to 10%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe power-reserved 10
```

11.2.162 poe power-threshold (AP system profile view)

Function

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage.

The **undo poe power-threshold** command restores the default alarm threshold of the PoE power consumption percentage.

By default, the alarm threshold is 100%.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe power-threshold *threshold-value*

undo poe power-threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold of the PoE power consumption percentage. When the power consumption reaches this value, a PoE power alarm is generated.	The value is an integer that ranges from 0 to 100, in percentage.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **poe power-threshold** command sets the alarm threshold of the PoE power consumption percentage. If the total PoE power is 380 W and the alarm threshold is 90%, an alarm is generated when the power consumption is greater than 342 W. When the power consumption falls below 342 W, the alarm is cleared.

Example

Set the alarm threshold of the PoE power consumption percentage to 80%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] poe power-threshold 80
```

11.2.163 poe priority (AP wired port link profile view)

Function

The **poe priority** command sets the power priority of a PoE interface.

The **undo poe priority** command restores the default power priority of a PoE interface.

By default, the power supply priority of an interface is **low**.

NOTE

This function is supported only by APs that support PoE OUT.

Format

poe priority { **critical** | **high** | **low** }

undo poe priority

Parameters

Parameter	Description	Value
critical	Indicates the highest priority.	-
high	Indicates the second highest priority.	-

Parameter	Description	Value
low	Indicates the lowest priority.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the output power of a device is insufficient, the device provides power for the interfaces of the higher power supply priorities first and cuts off power of the interfaces of the lower power supply priorities. If all the interfaces are of the same priority, the power supply priority of the interface with a smaller interface number is higher.

Example

Set the power priority of an AP's interface to **Critical**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] poe priority critical
```

11.2.164 port-link-profile (WLAN view)

Function

The **port-link-profile** command creates an AP wired port link profile and displays the AP wired port link profile view, or displays the view of an existing AP wired port link profile.

The **undo port-link-profile** command deletes an AP wired port link profile.

By default, the system provides the AP wired port link profile **default**.

Format

port-link-profile name *profile-name*

undo port-link-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP wired port link profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP wired port link profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP wired port link profile offers link-layer management and configuration on AP's wired interfaces.

Follow-up Procedure

After you create an AP wired port link profile, run the **port-link-profile (AP wired port profile view)** command to bind it to an AP wired port profile and then run the **wired-port-profile (AP group view and view)** command to bind the AP wired port profile to an AP or AP group. In this way, the AP wired port link profile can take effect.

Precautions

- The AP wired port link profile **default** cannot be deleted.
- The AP wired port link profile referenced by an AP or AP group cannot be deleted. To delete the AP wired port link profile, unbind it from the AP or AP group first.

Example

Create the AP wired port link profile **port-link1** and display the AP wired port link profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1]
```

11.2.165 port-link-profile (AP wired port profile view)

Function

The **port-link-profile** command binds an AP wired port link profile to an AP wired port profile.

The **undo port-link-profile** command unbinds an AP wired port link profile from an AP wired port profile.

By default, the AP wired port link profile **default** is bound to an AP wired port profile.

Format

port-link-profile *profile-name*

undo port-link-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port link profile.	The AP wired port link profile must exist.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP wired port link profile using the **port-link-profile (WLAN view)** command, bind it to an AP wired port profile so that the AP wired port link profile can take effect.

Precautions

After an AP wired port link profile is bound to an AP wired port profile, parameter settings in the AP wired port link profile apply to specified interfaces of all APs using the AP wired port profile.

Example

Create the AP wired port link profile **port-link1** and bind it to the AP wired port profile **wired-port1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] quit
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] port-link-profile port-link1
```

11.2.166 port-security enable (AP wired port profile view)

Function

The **port-security enable** command enables the port security function on an interface.

The **undo port-security enable** command disables the port security function on an interface.

By default, port security is disabled on an interface.

Format

port-security enable

undo port-security enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. By default, secure dynamic MAC addresses will not be aged out. After the device restarts, secure dynamic MAC address entries are lost and need to be relearned.

- Prevent unauthorized users from using their computers to connect to an enterprise network.
- Prevent employees of a company from moving their computers without permission.

Precautions

The protection action, maximum number of learned secure MAC address entries, and sticky MAC function can be configured only after port security is enabled.

When the AP's wired interface works in root or middle mode, port security cannot be configured. Port security can be configured on an AP's wired interface only when the interface works in endpoint mode.

Example

Enable port security.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
```

11.2.167 port-security mac-address sticky (AP wired port profile view)

Function

The **port-security mac-address sticky** enables the sticky MAC function on an interface.

The **undo port-security mac-address sticky** disables the sticky MAC function on an interface.

By default, the sticky MAC function is disabled on an interface.

Format

port-security mac-address sticky

undo port-security mac-address sticky

Parameters

None.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the port security function is enabled on an interface using the **port-security enable** command, the MAC addresses learned by the interface are converted into dynamic secure MAC addresses.

After the sticky MAC function is enabled on the interface, the dynamic secure MAC addresses learned by the interface are converted into sticky MAC addresses.

Before the number of sticky MAC addresses reaches the limit on the interface, the MAC addresses learned subsequently are still converted into sticky MAC addresses. When the number of sticky MAC addresses reaches the limit, non-sticky MAC addresses are discarded. In addition, the system determines whether to send a trap message based on the configuration of the interface protection mode.

Prerequisites

The port security function has been enabled using the **port-security enable** command on the interface.

Example

Enable the sticky MAC function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
[HUAWEI-wlan-wired-port-wire1] port-security mac-address sticky
```

11.2.168 port-security max-mac-num (AP wired port profile view)

Function

The **port-security max-mac-num** command sets the maximum number of secure MAC addresses that can be learned by an interface.

By default, an interface can learn only one secure MAC address.

Format

port-security max-mac-num *max-number*

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of secure MAC addresses that can be learned by an interface.	The value is an integer that ranges from 1 to 64.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security on an interface, you can run the **port-security max-mac-num** command to limit the number of secure MAC addresses that can be learned by the interface bound to the AP wired port profile. After the number of secure MAC addresses exceeds the limit, the switch considers that packets with nonexistent source MAC addresses as attack packets regardless of whether the packets have destination MAC addresses. The device then takes the action specified using the **port-security protect-action** command to protect the interface. This prevents STAs with untrusted MAC addresses from communicating with the switch through this interface, improving security of the device and network.

If you run the **undo port-security enable** command to disable port security on an interface, the maximum number of secure MAC addresses that can be learned on the interface will be restored to the default value after port security is enabled again.

Prerequisites

The port security function has been enabled using the **port-security enable** command on the interface.

Precautions

If the sticky MAC function is disabled, *max-number* limits the number of secure dynamic MAC addresses learned by the interface.

If the sticky MAC function is enabled, *max-number* limits the number of sticky MAC addresses learned by the interface.

If you run the **port-security max-mac-num** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the maximum number of secure MAC addresses that can be learned by the interface bound to the AP wired port profile to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
[HUAWEI-wlan-wired-port-wire1] port-security max-mac-num 5
```

11.2.169 port-security protect-action (AP wired port profile view)

Function

The **port-security protect-action** command configures a protection action for the system to perform when the number of learned MAC addresses exceeds the limit.

The **undo port-security protect-action** command restores the default protection action.

The default action is **restrict**.

Format

port-security protect-action { **protect** | **restrict** }

undo port-security protect-action

Parameters

Parameter	Description	Value
protect	Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit.	-
restrict	Discards packets with new source MAC addresses and sends a trap message when the number of learned MAC addresses exceeds the limit.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security, you can run the **port-security protect-action** command to configure the action performed on the interface when the number of learned MAC addresses reaches the limit.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

If you run the **port-security protect-action** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the protection action on an AP's wired interface to **protect**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode con
figuration will cause the AP to go out of management. This fault can be recovere
d only by modifying the configuration on the AP. Continue? [Y/N]:y
Warning: This action will take effect after resetting AP.
[HUAWEI-wlan-wired-port-wire1] port-security enable
[HUAWEI-wlan-wired-port-wire1] port-security protect-action protect
```

11.2.170 power force work-mode

Function

The **power force work-mode** command sets the power supply mode for APs.

The **undo power force work-mode** command restores the default power supply mode of APs.

By default, no power supply mode is configured for APs.

Format

power force work-mode { **af** | **at** | **bt60** | **bt90** }

undo power force work-mode

Parameters

Parameter	Description	Value
af	Sets the power supply mode to 802.3af.	-
at	Sets the power supply mode to 802.3at.	-
bt60	Sets the power supply mode to 802.3bt class 6.	-
bt90	Sets the power supply mode to 802.3bt class 8. **NOTE** The parameters **bt60** and **bt90** are valid only for APs that support 802.3bt PoE power supply.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the power supply mode of an AP cannot be correctly identified through LLDP or hardware, you can run the **power force work-mode** command to manually adjust the PoE power supply mode of the AP so that the AP can work in the specified power supply mode.

Configuration Impact

The power supply mode configured using the **power force work-mode** command takes effect for the logic of reducing power consumption on the APs. If this command is not configured, the power supply mode identified by LLDP or hardware is used.

If an AP's input power is low (for example, the power supply mode is 802.3at) but the power supply mode is manually set to 802.3bt class 8 (**bt90**), the AP will work in 802.3bt class 8 mode, which may cause a power failure.

If an AP's input power is high (for example, the power supply mode is 802.3bt class 8) but the power supply mode is manually set to 802.3at, the AP cannot work properly due to insufficient power.

Running this command may interrupt services.

Example

Set the power supply mode for APs to **802.3at**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] power force work-mode at
Warning: If the PSE does not reach the target power supply level, executing this command may cause the
AP to repeatedly restart due to insufficient power. Continue? [Y/N]: y
```

11.2.171 provision-ap

Function

The **provision-ap** command displays the AP provisioning view.

Format

provision-ap

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In the AP provisioning view, you can configure provisioning parameters of APs, including the management VLAN, static IP address, gateway, and AC list, which facilitates remote AP management on the AC.

Example

Display the AP provisioning view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] provision-ap
[HUAWEI-wlan-provision-ap]
```

11.2.172 reset ap-type undefined record

Function

The **reset ap-type undefined record** command clears the types of the APs that fail to connect to an AC because the AC does not support these AP types.

Format

reset ap-type undefined record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the types of the APs that fail to connect to an AC because the AC does not support these AP types.

The cleared records cannot be restored.

Example

Clears the types of the APs that fail to connect to the AC because the AC does not support these AP types.

```
<HUAWEI> reset ap-type undefined record
```

11.2.173 reset mac-address

Function

The **reset mac-address** command deletes all dynamic, dynamic secure, and sticky MAC address entries from an AP's wired interface.

Format

reset mac-address { **ap-id** *ap-id* | **ap-name** *ap-name* } *interface-type interface-number*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Deletes all dynamic, dynamic secure, and sticky MAC address entries from the wired interface of the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-name *ap-name*	Deletes all dynamic, dynamic secure, and sticky MAC address entries from the wired interface of the AP with a specified name.	The AP name must exist.
interface-type interface-number	Deletes all dynamic, dynamic secure, and sticky MAC address entries from a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the number of the outbound interface.	The following types of outbound interfaces are supported: - Eth-Trunk - Ethernet - Gigabitethernet - MultiGE - XGigabitethernet

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **reset mac-address** command to delete all dynamic MAC address entries from an AP's wired interface. If the port security and sticky MAC functions are enabled, dynamic secure MAC address and sticky MAC address entries are also deleted.

Example

Delete all dynamic, dynamic secure, and sticky MAC address entries from the wired interface of the AP with ID 0.

```
<HUAWEI> reset mac-address ap-id 0 ethernet 0
```

11.2.174 reset statistics

Function

The **reset statistics** command clears device statistics.

Format

reset statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } [**ssid** *ssid*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears statistics about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Clears statistics about the AP with a specified ID.	The AP ID must exist.
ssid *ssid*	Clears statistics about a specified SSID.	The SSID must exist. To specify an SSID starting with a space, include the SSID with double quotation marks (" "). For example, in the SSID **" hello"**, the double quotation marks at the start and end of the SSID occupy two characters. To specify an SSID starting with a double quotation mark ("), enter an escape character (\) before the double quotation mark. For example, in the SSID **\"hello**, the escape character (\) occupies one character.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

You can run the **reset statistics** command to clear device statistics.

Example

Clear AP statistics.

```
<HUAWEI> system view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset statistics ap-name area1
```

11.2.175 reset wlan console ble statistics

Function

The **reset wlan console ble statistics** command clears statistics about Bluetooth-based console port login on an AP.

NOTE

The following models do not support the Bluetooth serial port function:

- AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
- AirEngine 5762-10 and AirEngine 5762-10SW
- AirEngine 9700D-M and AirEngine 9700D-M1

Format

reset wlan console ble statistics { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The AP ID must exist.
ap-name *ap-name*	Specifies the AP name.	The AP name must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear statistics about Bluetooth-based console port login on an AP.

Example

Clear statistics about Bluetooth-based console port login on an AP named **huawei**.

```
<HUAWEI> reset wlan console ble statistics ap-name huawei
```

11.2.176 sample-time

Function

The **sample-time** command sets the sampling interval for an AP.

The **undo sample-time** command restores the default sampling interval of an AP.

The default sampling interval of an AP is 30s.

Format

sample-time *sample-time*

undo sample-time

Parameters

Parameter	Description	Value
sample-time	Specifies the sampling interval.	The value is an integer that ranges from 2 to 300, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP collects statistics on data including AP-based, radio-based, and STA-based data. Collected STA-based data statistics only include those that can be displayed using the **display** command on the AC.

Example

Set the sampling interval to 50s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] sample-time 50
```

11.2.177 sftp server disable

Function

The **sftp server disable** command disables the SFTP server function on an AP.

The **undo sftp server disable** command enables the SFTP server function on an AP.

By default, the SFTP server function is enabled on an AP.

Format

sftp server disable

undo sftp server disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to an SFTP-enabled AP from a user terminal for file management. Instead, you can log in to the SFTP-enabled AP through SFTP to manage files of the AP.

Example

Disable the SFTP server function on an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] sftp server disable
```

11.2.178 shutdown (AP wired port link profile view)

Function

The **shutdown** command shuts down an AP's wired interface.

The **undo shutdown** command enables an AP's wired interface.

By default, an AP's wired interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If malicious users launch attacks to the network through an AP's wired interface, the administrator can deliver the **shutdown** command on the AC to shut down the interface.

Precautions

Data frames may be lost if you shut down an interface during data transmission. Exercise caution when you use the **shutdown** command.

The **shutdown** command still takes effect after an AP is restarted.

The **shutdown** command takes effect only on AP's wired interfaces working in **endpoint** or **middle** mode but not on those working in **root** mode.

Example

Shut down the AP's wired interface GE0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] shutdown
Warning: This command does not take effect for root interfaces.
[HUAWEI-wlan-port-link-prof-port-link1] quit
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] port-link-profile port-link1
[HUAWEI-wlan-wired-port-wired-port1] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired-port1 gigabitethernet 0
```

11.2.179 ssh client first-time enable (AP system profile view)

Function

The **ssh client first-time enable** command enables the first authentication on the SSH client.

The **undo ssh client first-time enable** command disables the first authentication on the SSH client.

By default, the first authentication is disabled on the SSH client.

Format

ssh client first-time enable

undo ssh client first-time enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the SSH client accesses the SSH server for the first time and the public key of the SSH server is not configured on the SSH client, you can enable the first authentication for the SSH client to access the SSH server and save the public key of the SSH server on the SSH client. When the SSH client accesses the SSH server next time, the saved public key of the SSH server is used to authenticate the SSH server.

Example

Enable the first authentication on the SSH client.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] ssh client first-time enable
```

11.2.180 speed (AP wired port link profile view)

Function

The **speed** command sets the rate for an AP's wired interface in non-auto negotiation mode.

The **undo speed** command restores the default rate of an AP's wired interface.

By default, an AP's wired interface works in auto-negotiation mode, and its rate is negotiated with the peer interface.

Format

speed { **100** | **1000** | **2500** | **5000** | **10000** }

undo speed

Parameters

Parameter	Description	Value
100	Sets the interface rate to 100 Mbit/s.	-
1000	Sets the interface rate to 1000 Mbit/s. **NOTE** FE electrical interfaces do not support this parameter.	-
2500	Sets the interface rate to 2500 Mbit/s. **NOTE** Only multi-GE interfaces support this parameter.	-
5000	Sets the interface rate to 5000 Mbit/s. **NOTE** Only multi-GE interfaces support this parameter.	-
10000	Sets the interface rate to 10000 Mbit/s. **NOTE** Only XGE interfaces support this parameter.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the peer interface is configured with the forcible rate, you can run this command to set the rate of the corresponding interface on the local AP to prevent communication failures.

Precautions

- Exercise caution when running this command. The default value for this command is recommended unless otherwise required. If this configuration is mandatory, do not run this command in the **default** profile to prevent the configuration from being delivered to all interfaces.
- This command is available only on the FE, GE, multi-GE, and XGE interfaces on an AP but does not take effect on other types of interfaces.
- After the **speed** command is run, the AP changes the working mode of the interface to non-auto-negotiation and changes the interface rate based on the configuration. During this process, the interface may go Down or Up. Therefore, the configuration delivery takes a long time.
- After running the **speed** command to change the negotiation mode and rate of an AP's wired interface, ensure that the remote interface works in full-duplex mode and has the same rate as the local interface; otherwise, communication is affected.

Example

Set the rate of an AP's wired interface to 100 Mbit/s in non-auto-negotiation mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] port-link-profile name port-link1
[HUAWEI-wlan-port-link-prof-port-link1] speed 100
Warning: This operation may interrupt user services. If the AP works at the power derating mode, the
configuration may fail to take effect because the rate limit is exceeded, Continue? [Y/N]:y
```

11.2.181 stelnet server disable

Function

The **stelnet server disable** command disables the STelnet server function on an AP.

The **undo stelnet server disable** command enables the STelnet server function on an AP.

By default, the STelnet server function is enabled on an AP.

Format

stelnet server disable

undo stelnet server disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to an STelnet-enabled AP from a user terminal to maintain it locally. Instead, you can log in to the STelnet-enabled AP through STelnet to remotely configure and maintain it.

Example

Disable the STelnet server function on an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] stelnet server disable
```

11.2.182 stp auto-shutdown enable (AP wired port profile view)

Function

The **stp auto-shutdown enable** command enables the STP-triggered port shutdown function on an AP's wired interface.

The **undo stp auto-shutdown enable** command disables the STP-triggered port shutdown function on an AP's wired interface.

By default, the STP-triggered port shutdown function is disabled on an AP's wired interface.

Format

stp auto-shutdown enable

undo stp auto-shutdown enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STP-triggered port shutdown function is enabled, the AP automatically shuts down the interface when STP detects a loop. The AP will periodically recover the interface and re-executes STP detection. If the loop still exists on the interface, the AP shuts down the interface again. If the loop is removed, the AP reports a clear alarm to the network management system (NMS).

Prerequisites

STP has been enabled on the AP's wired interface using the **stp enable (AP wired port profile view)** command.

Precautions

The AP wired interfaces added to an Eth-trunk do not support this function.

This function is supported only when a loop exists on the network connected to the AP's wired port, that is, a port receives STP packets sent by itself.

Example

Disable the STP-triggered port shutdown function on an AP's wired interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] stp auto-shutdown enable
Warning: The AP may become out of management after the STP-triggered port shutdown function is
enabled (if the port is an uplink por
t). Continue?[Y/N]:y
```

11.2.183 stp auto-shutdown recovery-time (AP wired port profile view)

Function

The **stp auto-shutdown recovery-time** command sets an auto-recovery interval for an AP's wired interface on which the STP-triggered port shutdown function is enabled.

The **undo stp auto-shutdown recovery-time** command restores the default auto-recovery interval for an AP's wired interface on which the STP-triggered port shutdown function is enabled.

By default, the auto-recovery interval is 600s.

Format

stp auto-shutdown recovery-time *recovery-time*

undo stp auto-shutdown recovery-time

Parameters

Parameter	Description	Value
recovery-time	Specifies the auto-recovery interval for an AP's wired interface on which the STP-triggered port shutdown function is enabled.	The value is an integer that ranges from 600 to 3600, in seconds.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the STP-triggered port shutdown function is enabled, the AP automatically shuts down the interface when STP detects a loop. The AP will periodically recover the interface and re-executes STP detection. If the loop still exists on the interface, the AP shuts down the interface again. If the loop is removed, the AP reports a clear alarm to the network management system (NMS).

Prerequisites

The STP-triggered port shutdown function has been enabled on the AP's wired interface using the **stp auto-shutdown enable (AP wired port profile view)** command.

Precautions

The AP wired interfaces added to an Eth-trunk do not support this function.

Example

Set the auto-recovery interval to 800s for an AP's wired interface on which the STP-triggered port shutdown function is enabled.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] stp auto-shutdown recovery-time 800
```

11.2.184 stp enable (AP wired port profile view)

Function

The **stp enable** command enables STP on an AP's wired interface.

The **stp disable** command disables STP on an AP's wired interface.

The **stp auto** command configures STP in auto-sensing mode on an AP's wired interface.

The **undo stp** command restores the default setting.

By default, STP works in auto-sensing mode on an AP's wired interface.

Format

stp enable

stp disable

stp auto

undo stp

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **stp enable** command to prevent or eliminate loops on a complex Layer 2 network. STP on the AP's wired interfaces takes effect only when the AP forms a single loop with wired devices. Wireless links (such as WDS or Mesh links) only transparently forward STP BPDUs. An STP-enabled AP does not forward STP BPDUs to the wireless side. STP takes effect only on the AP's wired side.

When the STP function of an AP's wired interface is in auto-sensing mode, downlink interfaces of wall plate APs and RUs are enabled with the STP function and serve as edge interfaces, but STP is disabled on wired interfaces of other APs.

Precautions

The AP wired interfaces added to an Eth-Trunk do not support STP.

Example

Enable STP on the AP's wired interface GE0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] stp enable
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.185 telnet enable

Function

The **telnet enable** command enables Telnet on an AP.

The **undo telnet enable** command disables Telnet on an AP.

By default, Telnet is disabled on an AP.

Format

telnet enable

undo telnet enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to a Telnet-enabled AP from a user terminal to maintain it locally. Instead, you can log in to the Telnet-enabled AP through Telnet to remotely configure and maintain it.

To improve login security, you are advised to run the **undo stelnet server disable** command to enable the STelnet server function and log in to the AP through STelnet.

Example

Enable Telnet on an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] telnet enable
```

11.2.186 temporary-management disable (AP system profile view)

Function

The **temporary-management disable** command disables the offline management VAP and antenna alignment VAP functions of APs.

The **undo temporary-management disable** command enables the offline management VAP and antenna alignment VAP functions of APs.

By default, the offline management VAP and antenna alignment VAP functions of APs enabled.

NOTE

The antenna alignment VAP function is not supported by AirEngine series APs.

Format

temporary-management disable

undo temporary-management disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- APs are often installed in hidden places or at high positions. When an AP becomes faulty, it is inconvenient to connect to the AP through a console port or network cable to troubleshoot faults.

  After the offline management VAP function is configured, if an AP goes offline unexpectedly, maintenance personnel only need to set the IP address of a STA to 169.254.2.*x*/24 (except 169.254.2.1, 169.254.2.100 is recommended). After the STA associates with the offline management VAP, maintenance personnel can connect the STA to the AP in Telnet or STelnet mode to locate and rectify faults, saving the need to connect to the AP through the console port or a network cable.
- During WDS or Mesh network deployment, you can configure antenna alignment VAPs for WDS or Mesh nodes to facilitate antenna alignment between neighboring APs. During onsite commissioning, you can use a mobile terminal to connect to the antenna alignment VAP and enable CloudCampus APP to obtain information such as the signal strength of the peer AP's radio. Based on the obtained information, you can easily complete antenna alignment. The SSID of the generated antenna alignment VAP is hidden and will be automatically deleted 24 hours after being created.

After the offline management VAP and antenna alignment VAP functions are configured, the VAP generated when an AP goes offline is an offline management VAP. When the AP works properly, the VAP generated in the WDS or Mesh scenario is an antenna alignment VAP.

The offline management VAP and antenna alignment VAP functions can be configured in either of the following ways:

- Configure the default offline management VAP and antenna alignment VAP. After the offline management VAP and antenna alignment VAP functions are enabled using this command, an AP automatically creates a management VAP when the AP goes offline unexpectedly. The default SSID of this VAP is **hw_manage_xxxx**, where **xxxx** is the last 4 digits of the AP's MAC address. When an AP works properly in a WDS or Mesh scenario, it automatically creates an antenna alignment VAP. The default SSID of this VAP is **hw_manage_xxxx**, where **xxxx** is the last 4 digits of the AP's MAC address.

- Create an offline management VAP and antenna alignment VAP. Any STA can use the default SSID and password to log in to an AP, which poses security risks. To improve the security of the offline management VAP and antenna alignment VAP, you can bind a security profile of a high security level to a VAP profile, and set a new SSID and password. Additionally, you can run the **temporary-management enable** command in the VAP profile view and the **undo temporary-management disable** command in the AP system profile view to configure the VAPs generated by the VAP profile as the offline management VAP and antenna alignment VAP. The default offline management VAP and antenna alignment VAP will not be created.

Precautions

- The offline management VAP takes effect only when an AP goes offline unexpectedly.
- The offline management VAP function does not take effect on 4.9 GHz radios.
- Before using the offline management VAP function, ensure that the AP has enabled with Telnet or STelnet services.
- The antenna alignment VAP is automatically deleted 24 hours after it is created. To use the deleted antenna alignment VAP, run the **temporary-management disable** command and then the **undo temporary-management disable** command in the AP system profile view to create an antenna alignment VAP again.
- After the offline management VAP function is enabled:
  - If the link between the central AP and RUs is disconnected, the RUs will not generate an offline management VAP.
  - If the link between the central AP and AC is disconnected but RUs are still connected to the central AP, all online RUs connected to the central AP automatically generate an offline management VAP. If an AD9431DN-24X or AirEngine 9700D-M is used as the central AP, STAs log in to RUs through the offline management VAP. If a central AP other than the AD9431DN-24X or AirEngine 9700D-M is used, STAs log in to the central AP through the offline management VAP.
- The central AP does not have radios and therefore do not generate an offline management VAP.
- In offline management VAP scenarios, STA address learning does not take effect.

Example

Enable the offline management VAP and antenna alignment VAP function of APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] undo temporary-management disable
```

11.2.187 temporary-management enable (VAP profile view)

Function

The **temporary-management enable** command configures a VAP as the offline management VAP and antenna alignment VAP.

The **undo temporary-management enable** command restores a VAP to the default setting.

By default, a VAP is a service VAP.

NOTE

The antenna alignment VAP function is not supported by AirEngine series APs.

Format

temporary-management enable

undo temporary-management enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- After the offline management VAP function is enabled using the **undo temporary-management disable** command in the AP system profile view, an AP automatically generates an offline management VAP when it becomes faulty. The default SSID of the offline management VAP **hw_manage_xxxx**, where **xxxx** is the last 4 digits of the AP's MAC address. The maintenance personnel can associate the maintenance device with the default VAP and log in to the AP using Telnet or STelnet to troubleshoot the fault. However, using the default management VAP brings security risks. Any wireless user may use the default SSID and password to log in to the offline AP and perform unauthorized operations.
- After the antenna alignment VAP function is enabled using the **undo temporary-management disable** command in the AP system profile view, an AP automatically generates an antenna alignment VAP when it works properly. The default SSID of the antenna alignment VAP is **hw_manage_xxxx**. **xxxx** indicates the last 4 digits of the AP's MAC address. Using the default antenna alignment VAP also brings security risks.

The default username and password are available in *WLAN Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

To improve the security of the offline management VAP and antenna alignment VAP, you can bind a security profile of a high security level to a VAP profile, set a new SSID and password, configure the VAP generated by the VAP profile as the offline management VAP and antenna alignment VAP, and bind the VAP profile to an AP group or AP to replace the default offline management VAP and antenna alignment VAP.

Follow-up Procedure

After a VAP is configured as the offline management VAP and antenna alignment VAP in a VAP profile, run the **undo temporary-management disable** command in the AP system profile view to configure the offline management VAP and antenna alignment VAP functions of APs so that the offline management VAP and antenna alignment VAP functions of APs in the VAP profile can take effect.

Precautions

- If the VAPs are configured as the offline management VAP and antenna alignment VAP in a VAP profile, the security profile referenced by the VAP profile supports only the WEP or WPA/WPA2/WPA-WPA2 PSK security policy.
- If the VAPs are configured as the offline management VAP and antenna alignment VAP in a VAP profile, VAPs generated by the VAP profile cannot be used as service VAPs for service transmission.
- The offline management VAP and antenna alignment VAP of APs cannot be dynamically modified. To modify the VAPs, delete them first, and then modify the VAP attributes in the VAP profile view.
- The offline management VAP function does not take effect on 4.9 GHz radios.
- In offline management VAP scenarios, STA address learning does not take effect.

Example

Configure the VAP generated by the VAP profile **vap1** as the offline management VAP and antenna alignment VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] temporary-management enable
```

11.2.188 temporary-management psk

Function

The **temporary-management psk** command configures the login password for the offline management VAP and antenna alignment VAP.

The **undo temporary-management psk** command restores the preset password of the offline management VAP and antenna alignment VAP.

By default, no login password is configured, and the global password is in effect.

Format

temporary-management psk *psk-value*

undo temporary-management psk

Parameters

Parameter	Description	Value
psk-value	Specifies the login password of the offline management VAP and antenna alignment VAP.	The value is a string of 48 to 108 characters in ciphertext or a string of 8 to 63 characters in plaintext. The password must contain at least two types of uppercase letters, lowercase letters, digits, and special characters.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the login password of the offline management VAP and antenna alignment VAP. If this password has not been configured, the global password is used by default, which is configured using the **temporary-management psk** (WLAN view) command. The password configured in the AP system profile has a higher priority than that configured in the WLAN view.

Example

Set the login password of the offline management VAP and antenna alignment VAP to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name default
[HUAWEI-wlan-ap-system-prof-default] temporary-management psk YsHsjx_202206
```

11.2.189 traffic-filter (AP wired port profile view)

Function

The **traffic-filter** command configures ACL-based IPv4, IPv6, or Layer 2 packet filtering on an AP's wired interface.

The **undo traffic-filter** command cancels the ACL-based IPv4, IPv6, or Layer 2 packet filtering configuration on an AP's wired interface.

By default, ACL-based IPv4, IPv6, or Layer 2 packet filtering is not configured on an AP's wired interface.

Format

traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction.	-
outbound	Configures ACL-based packet filtering in the outbound direction.	-
ipv4	Configures ACL-based IPv4 packet filtering.	-
l2	Configures ACL-based Layer 2 packet filtering.	-
ipv6	Configures ACL-based IPv6 packet filtering.	-
acl	Filters packets based on the ACL.	-

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 for IPv4 ACLs and IPv6 ACLs and from 4000 to 4031 for Layer 2 ACLs. ● 3000 to 3031: advanced ACLs ● 4000 to 4031: Layer 2 ACLs
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The ACL name must exist. The value range is the same as that of the *acl-number* parameter.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a wireless network, administrators want to provide differentiated services for wireless users. The services may include, but are not limited to the following:

- Deny or permit access of specified wireless users to specified LAN devices.
- Deny access of specified wireless users to specified invalid IP addresses.

You can configure ACL-based packet filtering on an AP's wired interface for providing differentiated services.

The rules for an AP's wired interface to filter packets based on ACLs are as follows:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

When multiple commands are configured for ACL-based packet filtering in the same direction in the same AP wired port profile view, packets are matched against ACL rules in the sequence in which the commands are configured. If packets match a rule, the system stops the matching process and executes the specified policy. Otherwise, the system continues to match packets against the next rule. If no rule is matched, packets are allowed to pass through. The following occurs depending on whether packets match ACL rules:

- If a policy contains only one ACL rule and the ACL rule is matched, the **permit** or **deny** action is performed.
- If a policy contains two ACL rules and the specified action is performed only when the two ACL rules are both matched.

  If the actions in the two ACL rules are both **permit**, the **permit** action is performed. Otherwise, the **deny** action is performed.

If an ACL contains multiple rules, packets are matched against the rules in the ascending order of rule IDs.

Prerequisites

A named ACL has been created using the **acl name** or **acl name** command.

Precautions

You can specify an empty ACL in this command, and configure this ACL later.

A maximum of eight ACL-based packet filtering policies can be configured in one direction. The policies take effect in the sequence in which they are configured. To improve match efficiency, you are advised to configure an ACL rule with a high match probability for packet filtering. When configuring each ACL rule, set a small ID for the rule with a high match probability, reducing the number of times ACL rules are matched and saving resources. To change the sequence in which packets are filtered based on ACLs, delete all related configurations and reconfigure ACL-based packet filtering.

Example

Configure the wired interface GE0 on APs in an AP group to filter incoming packets based on ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] traffic-filter inbound ipv4 acl 3000
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.190 traffic-remark (AP wired port profile view)

Function

The **traffic-remark** command configures ACL-based priority re-marking on an AP's wired interface.

The **undo traffic-remark** command cancels the ACL-based priority re-marking configuration on an AP's wired interface.

By default, ACL-based priority re-marking is not configured on an AP's wired interface.

Format

traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* } { **dot1p** *dot1p-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* } { **dot1p** *dot1p-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based priority re-marking in the inbound direction.	-
outbound	Configures ACL-based priority re-marking in the outbound direction.	-
ipv4	Configures priority re-marking for IPv4 packets.	-
ipv6	Configures priority re-marking for IPv6 packets.	-
l2	Configures priority re-marking for Layer 2 packets.	-
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 for IPv4 ACLs and IPv6 ACLs and from 4000 to 4031 for Layer 2 ACLs. • 3000 to 3031: advanced ACLs • 4000 to 4031: Layer 2 ACLs
name *acl-name*	Re-marks packet priorities based on a specified named ACL. *acl-name* indicates an ACL name.	The value is a string of 1 to 32 case-sensitive characters without spaces and must begin with a letter. The value range of *acl-number* corresponding to *acl-name* is 3000 to 3031 and 4000 to 4031.

Parameter	Description	Value
dot1p *dot1p-value*	Re-marks the 802.1p priority of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-value*	Re-marks the DSCP priorities of packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user wants to re-mark packet priorities based on ACLs to provide differentiated services. The **traffic-remark** command can be used to configure ACL-based priority re-marking.

Prerequisites

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl ipv6 (system view)**
- **acl name**
- **acl ipv6 name**

Precautions

The **traffic-remark** command can reference a numbered ACL rule that is not configured. You can configure the referenced ACL rule after running this command.

You can only configure a maximum of eight ACL-based packet re-marking rules in the same direction. The sequence in which ACL rules takes effect follows the rule configuration sequence. To change the current packet re-marking rules, delete all the related configurations and reconfigure the ACL-based packet re-marking.

When the **traffic-remark** command and the **traffic-filter (AP wired port profile view)** command are used simultaneously and the same ACL rule is associated:

- If the **deny** action is configured in the ACL rule, the **traffic-remark** command does not take effect.

- If the **permit** action is configured in the ACL rule, the command that is executed first takes effect.

Example

Configure the wired interface GE0 of **ap-group1** and configure ACL-based 802.1p priority re-marking for IPv4 packets in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] traffic-remark inbound ipv4 acl 3000 dot1p 7
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.191 traffic-optimize (AP wired port profile view)

Function

The **traffic-optimize** command sets the maximum volume of broadcast, multicast, or unknown unicast traffic on an AP's wired interface.

The **undo traffic-optimize** command restores the default maximum volume of broadcast, multicast, or unknown unicast traffic on an AP's wired interface.

By default, the volume of broadcast, multicast, or unknown unicast traffic is not suppressed on an AP's wired interface.

Format

traffic-optimize { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } **packets** *packets-rate*

undo traffic-optimize { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** }

Parameters

Parameter	Description	Value
broadcast-suppression	Specifies the maximum broadcast traffic volume that can be received on an AP's wired interface.	-
multicast-suppression	Specifies the maximum multicast traffic volume that can be received on an AP's wired interface.	-

Parameter	Description	Value
unicast-suppression	Specifies the maximum unknown unicast traffic volume that can be received on an AP's wired interface.	-
packets *packets-rate*	Specifies the maximum number of packets that can pass every second.	The value is an integer that ranges from 0 to 14881000, in pps.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of broadcast, multicast, and unknown unicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected. When the traffic volume of broadcast, multicast, and unknown unicast packets reaches the maximum on an AP's wired interface, the system discards excess packets to control the traffic volume in a proper range and prevent flooding attacks.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

The uplink interfaces of RUs do not support this command.

This command takes effect only for incoming traffic on an AP's wired interface.

Example

Set the maximum broadcast traffic volume that can be received on an AP's wired interface to 21600 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] traffic-optimize broadcast-suppression packets 21600
```

11.2.192 traffic-optimize broadcast-suppression disable (AP system profile view)

Function

The **traffic-optimize broadcast-suppression disable** command disables rate limiting for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression disable** command enables rate limiting for broadcast and multicast packets on an AP.

By default, rate limiting for broadcast and multicast packets is enabled on an AP.

Format

traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **disable**

undo traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **disable**

Parameters

Parameter	Description	Value
all	Enables or disables rate limiting for ARP, IGMP, ND, DHCP, DHCPv6, and mDNS multicast and broadcast packets.	-
arp	Enables or disables rate limiting for ARP multicast packets.	-
igmp	Enables or disables rate limiting for IGMP multicast packets.	-
nd	Enables or disables rate limiting for ND broadcast packets.	-
dhcp	Enables or disables rate limiting for DHCP broadcast packets.	-
dhcpv6	Enables or disables rate limiting for DHCPv6 broadcast packets.	-
mdns	Enables or disables rate limiting for mDNS multicast packets.	-

Parameter	Description	Value
other-broadcast	Enables or disables rate limiting for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Enables or disables rate limiting for multicast packets other than IGMP and mDNS packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When an AP receives an increasing number of packets, more network resources are occupied and services on the network are affected. To ensure normal running of network services, you can limit the rate of some protocol packets (such as DHCP and ARP packets) on an AP to a proper range.

You can run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to configure a rate limit threshold for broadcast and multicast packets of an AP, which will override the default rate threshold.

Precautions

When multicast services are enabled, the multicast services may be affected if rate limiting for multicast packets is enabled on an AP. In this case, you are advised to run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to adjust the rate limit threshold for multicast packets.

Rate limiting for broadcast and multicast packets takes effect only for incoming traffic on an AP's wired interface.

Example

Enable rate limiting for ARP broadcast packets in AP system profile **system1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] undo traffic-optimize broadcast-suppression arp disable
```

11.2.193 traffic-optimize broadcast-suppression rate-threshold (AP system profile view)

Function

The **traffic-optimize broadcast-suppression rate-threshold** command sets a rate limit threshold for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression rate-threshold** command restores the default rate limit threshold of broadcast and multicast packets on an AP.

By default, the rate limit threshold for **other-broadcast** and **other-multicast** is 16 pps, and that for other parameters is 256 pps.

Format

traffic-optimize broadcast-suppression { **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **rate-threshold** *threshold-value*

undo traffic-optimize broadcast-suppression { **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **other-broadcast** | **other-multicast** } **rate-threshold**

Parameters

Parameter	Description	Value
arp	Specifies ARP broadcast packets.	-
igmp	Specifies IGMP multicast packets.	-
nd	Specifies ND broadcast packets.	-
dhcp	Specifies DHCP broadcast packets.	-
dhcpv6	Specifies DHCPv6 broadcast packets.	-
mdns	Specifies mDNS multicast packets.	-
other-broadcast	Specifies broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Specifies multicast packets other than IGMP and mDNS packets. **NOTE** If **other-multicast** is specified, LLDPDUs are not rate-limited.	-

Parameter	Description	Value
rate-threshold *threshold-value*	Specifies a rate limit threshold.	For **arp**, **nd**, **dhcp**, and **dhcpv6**, the value is an integer that ranges from 64 to 1024, in pps. The default value is 256. For **igmp** and **mdns**, the value is an integer that ranges from 0 to 1024, in pps. The default value is 256. For **other-broadcast** and **other-multicast**, the value is an integer that ranges from 0 to 1024, in pps. The default value is 16.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before setting a rate limit threshold for broadcast and multicast packets, run the **undo traffic-optimize broadcast-suppression disable** command to enable rate limiting for broadcast and multicast packets.

After you run the **traffic-optimize broadcast-suppression rate-threshold** command to configure a rate limit threshold for broadcast and multicast packets on an AP, the configured threshold will override the default rate limit threshold. The actual rate of broadcast and multicast packets will not exceed the configured rate limit threshold. If a large rate limit threshold is set, the expected network protection effect is not achieved. If a small rate limit threshold is set, broadcast and multicast packets may be lost. In most cases, use the default rate limit threshold unless otherwise specified.

Precautions

Rate limiting for broadcast and multicast packets takes effect only for incoming traffic on an AP's wired interface.

The rate limit threshold for multicast and broadcast packets applies to the inbound direction on all AP wired interfaces. That is, the rate of multicast and broadcast packets is limited only when the total rate of multicast and broadcast packets in the inbound direction of all AP wired interfaces exceeds the rate limit.

Example

Set the rate limit threshold for ARP broadcast packets in AP system profile **system1** to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] undo traffic-optimize broadcast-suppression all disable
[HUAWEI-wlan-ap-system-prof-system1] traffic-optimize broadcast-suppression arp rate-threshold 300
```

11.2.194 undo capwap dtls server-auth (AP view)

Function

The **undo capwap dtls server-auth** command restores the default state of the AC authentication function for APs.

By default, the AC authentication function for APs is disabled.

Format

undo capwap dtls server-auth

Parameters

None

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP attempts to go online, it receives Discovery Response packets from ACs and discover an available AC. A bogus AC may maliciously send a Discovery Response packet to the AP, causing the AP to go online on the bogus AC.

After the AC authentication function for APs is enabled, an AP initiates DTLS authentication to the AC before establishing a CAPWAP tunnel with it. The AP then uses the DTLS PSK or initial certificate to authenticate the AC. The CAPWAP tunnel can be established only after the authentication succeeds.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

To enable or disable the AC authentication function for APs, run the **capwap dtls server-auth disable** and **commit** commands in the AP provisioning view to deliver the configuration.

Example

Restore the default state of the AC authentication function for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] undo capwap dtls server-auth
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and may cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.195 undo capwap dtls server-auth cn (AP view)

Function

The **undo capwap dtls server-auth cn** command restores the default CN field used by APs to verify an AC's certificate.

By default, no CN field is specified for APs to verify an AC's certificate.

Format

undo capwap dtls server-auth cn

Parameters

None

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to clear the configured CN field used by APs to verify an AC's certificate. Then APs do not verify the CN field of an AC's certificate.

Precautions

After the configuration is delivered, restart the APs to make the configuration take effect.

To configure the CN field used by APs to verify an AC's certificate, run the **capwap dtls server-auth cn** *cn-string* and **commit** commands in the AP provisioning view to deliver the configuration.

Example

Restore the default CN field used by APs to verify an AC's certificate.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] undo capwap dtls server-auth cn
Warning: The incorrect configuration will cause the AP to go out of management. This operation will
deliver parameter setting and may cause reboot of AP(s). Continue?[Y/N]:y
```

11.2.196 unicast-suppression auto-detect (AP system profile view)

Function

The **unicast-suppression auto-detect** command configures the rate limit for unknown unicast packets during intelligent flow control.

The **undo unicast-suppression auto-detect** command restores the default rate limit for unknown unicast packets during intelligent flow control.

By default, the rate limit for unknown unicast packets is 128 pps.

Format

unicast-suppression auto-detect packets *packets*

undo unicast-suppression auto-detect

Parameters

Parameter	Description	Value
packets *packets*	Specifies the rate limit for unknown unicast packets.	The value is an integer that ranges from 64 to 1024, in pps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When there are a large number of broadcast, multicast, and unknown unicast packets, the CPU becomes busy processing these packets and the buffer of the packet for receiving incoming packets is occupied. When the buffer decreases to the specified threshold, the device automatically rate-limits the broadcast, multicast, and unknown unicast packets. You can run this command to specify the rate limit for intelligent flow control as required. Rate limiting takes effect only for incoming traffic.

Example

Set the rate limit for unknown unicast packets during intelligent flow control to 300 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] unicast-suppression auto-detect packets 300
```

11.2.197 usb enable (AP system profile view)

Function

The **usb enable** command enables the USB function on an AP.

The **undo usb enable** command disables the USB function on an AP.

By default, the USB function on an AP is disabled.

NOTE

The operations of enabling and disabling the USB function are supported only by the following models:

- AirEngine 8760-X1-PRO, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 9700D-M, AirEngine 5760-22WD
- AirEngine 8761-X1, AirEngine 6761-21, AirEngine 6761-21E, AirEngine 6761-21T, AirEngine 6761S-21, AirEngine 6761S-21T, AirEngine 6761-22T, AirEngine 5761-21, AirEngine 5761S-21, AirEngine 5761-11, AirEngine 5761S-11, AirEngine 5761-11W, AirEngine 5761S-11W, AirEngine 5761-11WD, AirEngine 5761-12, AirEngine 5761-12W, AirEngine 5761S-12, AirEngine 5761S-13
- AirEngine 5762-13W, AirEngine 5762-15HW, AirEngine 5762S-13W, AirEngine 5762-16W, AirEngine 5762-17W
- AirEngine 8771-X1T

For the AirEngine 5762-15HW and AirEngine 8761-X1, the USB power can only be set to 2.5 W.

Format

usb enable [**5w** | **9w**]

undo usb enable

Parameters

Parameter	Description	Value
5w	Sets the USB power to 5 W. If **5w** or **9w** is not specified, the USB power is 2.5 W.	-
9w	Sets the USB power to 9 W. If **5w** or **9w** is not specified, the USB power is 2.5 W.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use functions of the USB interface on an AP, run the **usb enable** command to enable the USB function. When the USB function is enabled, the power consumption of the AP will increase, which may affect other functions. You are advised to run the **undo usb enable** command to disable the USB function after using it.

Precautions

The USB and other functions of an AP may be restricted at different power supply levels:

- The USB function is unavailable at specific power supply levels.
- When the USB function is available and enabled, other functions (such as the IoT card, number of spatial streams, and transmit power) may be affected differently depending on power supply levels. The affected AP functions are restored after the USB function is disabled.

For details about the restrictions, do as follows: Visit **Info-Finder**, select a product series, and view hardware specifications in the hardware center. You can check the power supply downgrade limits at different power supply levels.

Example

Enable the USB function in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] usb enable
Warning: When the USB function is enabled, the AP power consumption increases, which may affect the
number of service flows and transmit power over the air interface. Continue? [Y/N]: y
```

11.2.198 user-interface vty acl

Function

The **user-interface vty acl** command uses an ACL to restrict login rights of users on a terminal.

The **undo user-interface vty acl** command cancels the configuration.

By default, login rights are not restricted.

Format

user-interface vty *ui-number* **acl** [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo user-interface vty *ui-number* **acl** [**ipv6**] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
vty *ui-number*	Specifies the VTY user interface number.	The value is an integer that ranges from 0 to 4.
ipv6	Indicates an ACL6 number.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 3000 to 3031.
inbound	Restricts users with an address or within an address segment to log in to the device.	-
outbound	Restricts users who have logged in to the device from logging in to other devices.	-

Views

AP system profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command restricts the login rights of a user interface based on the source IP address, destination IP address, source port, or destination port. You can use this command to permit or deny access to a destination or from a source.

Prerequisites

Before running this command, run the **acl (system view)** in the system view and run the **rule (basic ACL view)** or **rule (advanced ACL view)** command to configure an ACL.

If no rule is configured, login rights on the user interface are not restricted when the **acl** command is executed.

Precautions

After the configurations of the ACL take effect, all users on the user interface are restricted by the ACL.

You can configure all of the following ACL types: IPv4 inbound, IPv4 outbound, IPv6 inbound, and IPv6 outbound on a user interface. Only one ACL of each type can be configured on a user interface, and only the latest configuration of an ACL takes effect.

Example

Restrict the Telnet login rights on user interface VTY 0.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule deny tcp source any destination-port eq telnet
[HUAWEI-acl-adv-3001] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] user-interface vty 0 acl 3001 outbound
```

11.2.199 user-interface vty idle-timeout

Function

The **user-interface vty idle-timeout** command sets the timeout period for disconnection from a user interface.

The **undo user-interface vty idle-timeout** command restores the default timeout period.

By default, the timeout period is 5 minutes.

Format

user-interface vty *ui-number* **idle-timeout** *minutes* [*seconds*]

undo user-interface vty *ui-number* **idle-timeout**

Parameters

Parameter	Description	Value
ui-number	Specifies the VTY user interface number.	The value is an integer that ranges from 0 to 4.
minutes	Specifies the idle timeout period, in minutes.	The value is an integer that ranges from 0 to 35791, in minutes.
seconds	Specifies the idle timeout period, in seconds.	The value is an integer that ranges from 0 to 59, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user logs in to the device and does not perform an operation, the user interface is occupied unnecessarily. You can run the **user-interface vty idle-timeout** command to disconnect the user's terminal from the device.

Precautions

If the parameters *minutes* and *seconds* are both set to **0**, the VTY timeout disconnection function is disabled.

Example

Set the timeout period to 1 minute and 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] user-interface vty 0 idle-timeout 1 30
```

11.2.200 user-interface vty screen-length

Function

The **user-interface vty screen-length** command sets the number of lines on each terminal screen after you run a command.

The **undo user-interface vty screen-length** command restores the default configuration.

By default, the number of lines to be displayed on a terminal screen is 24.

Format

user-interface vty *ui-number* **screen-length** *screen-length*

undo user-interface vty *ui-number* **screen-length**

Parameters

Parameter	Description	Value
ui-number	Specifies the VTY user interface number.	The value is an integer that ranges from 0 to 4.
screen-length	Specifies the number of lines displayed on a terminal screen.	The value is an integer that ranges from 0 to 512. The value **0** indicates that all command output is displayed on one screen.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If you run a command and its output is displayed in more lines than you can see on one screen, you can set a small number of lines displayed on each screen.

In most cases, you do not need to change the number of lines displayed on each screen. Setting the number of lines to 0 is not recommended. The configuration takes effect after you log in to the system again.

Example

Set the number of lines on each screen of the terminal to 30.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] user-interface vty 0 screen-length 30
```

11.2.201 user-isolate (AP wired port profile view)

Function

The **user-isolate** command enables user isolation on an AP's wired interface.

The **undo user-isolate** command disables user isolation on an AP's wired interface.

By default, user isolation is disabled on an AP's wired interface.

Format

user-isolate { **all** | **l2** }

undo user-isolate

Parameters

Parameter	Description	Value
all	Enables Layer 2 and Layer 3 user isolation.	-
l2	Enables Layer 2 user isolation.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user isolation function prevents users on the same wired interface from communicating with each other. All user traffic on the wired interface is forwarded by the gateway. Therefore, this function ensures communication security on wired interfaces and allows uniform charging for users.

Precautions

Eth-Trunk member interfaces do not support the user isolation function.

This function is supported only when the AP's wired interface works in endpoint or middle mode.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and enable Layer 2 user isolation on GE0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the
AP to go out of management . This fault can be recovered only by modifying the configuration on the AP.
Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] user-isolate l2
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.202 vlan pvid (AP wired port profile view)

Function

The **vlan pvid** command sets the PVID for an AP's wired interface.

The **undo vlan pvid** command deletes the PVID of an AP's wired interface.

By default, the PVID of an AP's wired interface is 1.

Format

vlan pvid *vlan-id*

undo vlan pvid

Parameters

Parameter	Description	Value
vlan-id	Specifies the PVID of an AP's wired interface.	The value is an integer that ranges from 1 to 4094.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

APs on a WLAN WDS network only process tagged packets.

When receiving an untagged packet from a peer device, an AP's wired interface adds a VLAN tag to the packet. After the PVID is configured on the wired interface, the interface adds the PVID to all the received untagged packets.

Precautions

Eth-Trunk member interfaces do not support PVID setting.

The PVID can be configured in different modes for an AP's wired interface.

- When the AP's wired interface works in root mode, the PVID can be directly configured.
- When the AP's wired interface works in endpoint mode, the PVID can be directly configured.
- When the AP's wired interface works in middle mode, the PVID cannot be configured.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and set the PVID of GE0 to VLAN 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the
AP to go out of management . This fault can be recovered only by modifying the configuration on the AP.
Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] vlan pvid 1
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.203 vlan (AP wired port profile view)

Function

The **vlan** command configures the VLAN to which an AP's wired interface belongs.

The **undo vlan** command deletes the VLAN to which an AP's wired interface belongs.

By default, when an AP's wired interface works in **root** mode, it joins VLAN 1 in untagged mode and joins all other VLANs in tagged mode. When the interface does not work in **root** mode, it joins VLAN 1 only in untagged mode.

NOTE

An AP's wired interface can be added to a maximum of 256 VLANs.

Format

vlan { **tagged** | **untagged** } { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan { **all** | *vlan-id1* [**to** *vlan-id2*] &<1-10> }

Parameters

Parameter	Description	Value
tagged	Adds a wired interface to a VLAN in tagged mode.	-
untagged	Adds a wired interface to a VLAN in untagged mode.	-

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the ID of the VLAN to which the wired interface belongs. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, the wired interface is added to the VLAN specified by *vlan-id1*. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	- The value of *vlan-id1* is an integer that ranges from 1 to 4094. - The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all VLANs to which the AP's wired interface belongs.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a wired interface connects to a PC or Layer 2 network, the interface is equivalent to a hybrid interface on a switch, and can forward the packets with multiple VLAN tags.

After the **vlan tagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command is executed to add the wired interface to one or more VLANs in tagged mode, the interface does not remove VLAN tags from the packets it forwarded.

After the **vlan untagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command is executed to add the wired interface to one or more VLANs in untagged mode, the interface removes VLAN tags from the packets it forwarded.

Precautions

After you run the **management-vlan** *vlan-id* command to enable CAPWAP packets to carry the management VLAN tag, ensure that the AP's uplink wired interface is added to the management VLAN in tagged mode. By default, the VLAN ID meets the requirement. To change the VLAN ID, run the **vlan tagged** *vlan-id* command.

After the **management-vlan** *vlan-id* command is executed to configure AP's wired interfaces to send CAPWAP packets carrying the management VLAN tag (not VLAN 1), the interfaces working in **root** mode are added to VLAN 1 in tagged mode, which cannot be changed.

Eth-Trunk member interfaces cannot be added to VLANs.

Example

Set the working mode of the AP wired interface GE0 to **endpoint** and add GE0 to VLANs 3, 4, 5, and 10 in **tagged** mode and to VLANs 12, 13, 14, and 20 in **untagged** mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] mode endpoint
Warning: If the AP goes online through a wired port, the incorrect port mode configuration will cause the
AP to go out of management . This fault can be recovered only by modifying the configuration on the AP.
Continue? [Y/N]:y
[HUAWEI-wlan-wired-port-wired] vlan tagged 3 to 5 10
[HUAWEI-wlan-wired-port-wired] vlan untagged 12 to 14 20
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

11.2.204 wifi-light

Function

The **wifi-light** command specifies the parameter reflected by the blinking frequency of the Wireless indicators on an AP. When a Wireless indicator blinks fast, the signal strength is strong or the service traffic volume is high.

The **undo wifi-light** command restores the default parameter reflected by the blinking frequency of the Wireless indicators on an AP.

By default,

- If the Mesh function is enabled on the AP, the blinking frequency of the Wireless indicators reflects the weakest signal strength of all neighboring APs.
- If WDS is enabled on an AP, the blinking frequency of the Wireless indicators reflects the strength of signals received from a WDS AP.
  - If the AP works in leaf mode, the blinking frequency of the Wireless indicators reflects the strength of signals received from a middle AP.
  - If the AP works in middle mode, the blinking frequency of the Wireless indicators reflects the strength of signals received from a root AP.

  - If the AP works in root mode, the blinking frequency of the Wireless indicators reflects the weakest signal strength of middle APs.
- If the WDS and Mesh functions are disabled on an AP, the blinking frequency of the Wireless indicators reflects the service traffic volume on the radio.

NOTE

Only APs with wireless indicators support this command. For details about whether an AP has wireless indicators, see the indicator description of the corresponding AP model.

Format

wifi-light { **signal-strength** | **traffic** }

undo wifi-light

Parameters

Parameter	Description	Value
signal-strength	Sets the parameter reflected by the blinking frequency of the Wireless indicators on an AP to signal strength. When a Wireless indicator blinks fast, the signal strength is strong.	-
traffic	Sets the parameter reflected by the blinking frequency of the Wireless indicators on an AP to service traffic volume. When a Wireless indicator blinks fast, the service traffic volume is high.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During installation and commissioning of APs that have the WDS or Mesh function enabled, you need to adjust WDS or Mesh AP locations and antenna directions to obtain strong signals. If the blinking frequency of the Wireless indicators shows the signal strength, onsite installation personnel can know the signal strength in real time. The **wifi-light** command allows you to specify the parameter reflected by the blinking frequency of the Wireless indicators. For example, you can specify the parameter to signal strength during installation and service traffic volume after installation.

Precautions

This command takes effect only when the AP has the WDS or Mesh function enabled. If the WDS and Mesh functions are disabled on the AP, the Wireless indicators always show service traffic volume.

Example

Set the parameter reflected by the blinking frequency of the Wireless indicators on an AP to service traffic volume.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio-profile1
[HUAWEI-wlan-radio-2g-prof-radio-profile1] wifi-light traffic
```

11.2.205 wired-port-profile (WLAN view)

Function

The **wired-port-profile** command creates an AP wired port profile and displays the AP wired port profile view, or displays the view of an existing AP wired port profile.

The **undo wired-port-profile** command deletes an AP wired port profile.

By default, the system provides the AP wired port profile **default**.

Format

wired-port-profile name *profile-name*

undo wired-port-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP wired port profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP wired port profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP wired port profile provides convenience for AP wired interface management and configuration. You can configure AP wired interface parameters in an AP wired port profile to manage APs.

Follow-up Procedure

Run the **wired-port-profile (AP group view and AP view)** command to bind the AP wired port profile to an AP or AP group so that the AP wired port profile can take effect.

Precautions

- The AP wired port profile **default** cannot be deleted.
- The AP wired port profile referenced by an AP or AP group cannot be deleted. To delete the AP wired port profile, unbind it from the AP or AP group first.

Example

Create the AP wired port profile **wired-port1** and display the AP wired port profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1]
```

11.2.206 wired-port-profile (AP group view and AP view)

Function

The **wired-port-profile** command binds an AP wired port profile to an AP or AP group.

The **undo wired-port-profile** command unbinds an AP wired port profile from an AP or AP group.

By default, the AP wired port profile **default** is bound to an AP group, but no AP wired port profile is bound to an AP.

Format

wired-port-profile *profile-name interface-type interface-number*

undo wired-port-profile *interface-type interface-number*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The AP wired port profile must exist.
interface-type interface-number	Specifies the type and number of an AP's wired interface.	-

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP wired port profile using the **wired-port-profile (WLAN view)** command, bind it to an AP or AP group so that the AP wired port profile can take effect.

Precautions

- After an AP wired port profile is bound to an AP or AP group, parameter settings in the AP wired port profile apply to specified interfaces of all APs using the AP wired port profile.
- For APs with cards, the AP wired port profile can take effect only after being applied in the card view. For detailed configuration, see **wired-port-profile (IoT card interface view)**.

Example

Create the AP wired port profile **wired-port1** and bind it to GE0 on APs in AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] wired-port-profile wired-port1 gigabitethernet 0
```

11.3 Cloud-based Management Configuration Commands

11.3.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.3.2 ap manage-mode force-tradition

Function

The **ap manage-mode force-tradition** command sets the AP management mode to the local AC mode.

The **undo ap manage-mode force-tradition** command sets the AP management mode to the same as that on the switch. That is, if the NETCONF mode is enabled on the switch, the AP is managed by iMaster NCE-Campus; if the NETCONF mode is disabled on the switch, the AP is locally managed by the switch.

By default, the AP management mode is the same as that on the switch.

Format

ap manage-mode force-tradition

undo ap manage-mode force-tradition

Parameters

None

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After NETCONF is enabled on a switch (with the native AC function enabled), Fit APs are managed by iMaster NCE-Campus by default. AP entries delivered by iMaster NCE-Campus take effect, and cloud management license resources are consumed. Additionally, the switch no longer supports the commands listed in **Table 11-130**. To locally manage APs (using local AP entries and local license resources), run the **ap manage-mode force-tradition** command to set the AP management mode to the local AC mode. Then, the commands become available on the switch.

Precautions

When a Fit AP is managed by iMaster NCE-Campus, running the **ap manage-mode force-tradition** command on the switch will disconnect the Fit AP from iMaster NCE-Campus. In this case, deleting the entry of this AP on iMaster NCE-

Campus will delete the corresponding AP entry on the switch synchronously. To enable the AP to go online on the switch, you need to manually confirm the AP by running the **ap-confirm** { **all** | **mac** *ap-mac* | **sn** *ap-sn* } command on the switch.

Table 11-130 Commands that are not supported by the switch in NETCONF mode

Command	Function Description
ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** } **undo ap auth-mode**	Configures the AP authentication mode. For a switch in NETCONF mode, the AP authentication mode is SN authentication.
ap blacklist mac *ap-mac1* [**to** *ap-mac2*] **undo ap blacklist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **all** }	Adds APs to an AP blacklist, or deletes APs from an AP blacklist.
ap modify *ap-id* **mac** *ap-mac*	Modifies the MAC address of an AP.
ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] } **undo ap whitelist** { **mac** { *ap-mac1* [**to** *ap-mac2*] | **all** } | **sn** { *ap-sn1* [**to** *ap-sn2*] | **all** } }	Adds APs to an AP whitelist, or deletes APs from an AP whitelist.
ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }	Confirms unauthorized APs and allows them to go online.
ap-name *ap-name*	Configures an AP name.
ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*	Changes the name of an AP.

Example

Set the AP management mode to the local AC mode.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] ap manage-mode force-tradition
```

11.3.3 ap up-report-cloud

Function

The **ap up-report-cloud** command reports the AP status to iMaster NCE-Campus.

Format

ap up-report-cloud { **all** | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Specifies all APs.	-
ap-id *ap-id*	Specifies an AP ID.	The AP ID must already exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In a cloud AC scenario, if the AP status on iMaster NCE-Campus is different from that on the AC, you can run this command on the AC to report the AP status to iMaster NCE-Campus again to ensure that the AP status is correctly displayed.

Example

Report the status of AP with the ID of 5 to iMaster NCE-Campus.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap up-report-cloud ap-id 5
```

11.3.4 ap-id synchronize

Function

The **ap-id synchronize** command synchronizes newly added AP IDs to the SDN controller.

Format

ap-id synchronize

Parameters

None

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an AC uses NETCONF to register with the SDN controller, if AP capacity expansion is required, you can add AP IDs offline to the AC and then run this command to synchronize the newly added AP IDs to the SDN controller.

Example

Synchronize newly added AP IDs to the SDN controller.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] ap-id synchronize
```

11.3.5 display cloud license

Function

The **display cloud license** command displays license resources delivered by iMaster NCE-Campus to the AC.

Format

display cloud license

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display cloud license** command displays license resources delivered by iMaster NCE-Campus to the AC.

In CloudCampus Solution, licenses are used to control the number of APs that can be managed by iMaster NCE-Campus and the service duration. Users need to purchase licenses from service providers and import the licenses to iMaster NCE-Campus. After an AC goes online, iMaster NCE-Campus converts license resources into the expiration date and delivers the date to the AC. If the AC is out of management by iMaster NCE-Campus, AP entries and license resources on the AC are still available within the grace period of 90 days, and the AC can still manage and configure Fit APs.

You can query only the expiration date of the license on the AC. To query the number of license resources, log in to iMaster NCE-Campus to check license information.

Only devices in NETCONF mode support this command.

Example

Display license resources delivered by iMaster NCE-Campus to the AC.

```
<HUAWEI> display cloud license
------------------------------------------------------------------------
License type          Expire time
------------------------------------------------------------------------
Indoor AP             -
Outdoor AP             2020-12-11
Indoor AP-S           2020-12-11
Outdoor AP-S           2020-12-11
Indoor AP-EC           -
Outdoor AP-EC          2020-12-11
Common AP              -
Indoor Wi-Fi 6 AP      2020-12-11
Outdoor Wi-Fi 6 AP      2020-12-11
Wi-Fi 7 AP            2020-12-11
Agile distributed AP   2020-12-11
------------------------------------------------------------------------
Total: 11
```

Table 11-131 Description of the **display cloud license** command output

Item	Description
License type	License type. - Indoor AP: license for indoor APs - Outdoor AP: license for outdoor APs - Indoor AP-S: license for indoor APs (AP models ending with -S) - Outdoor AP-S: license for outdoor APs (AP models ending with -S) - Indoor AP-EC: license for indoor APs (AP models ending with EC) - Outdoor AP-EC: license for outdoor APs (AP models ending with EC) - Common AP: common license for ACs and APs (trial license) - Indoor Wi-Fi 6 AP: license for indoor APs (Wi-Fi 6 series indoor APs) - Outdoor Wi-Fi 6 AP: license for outdoor APs (Wi-Fi 6 series outdoor APs) - Wi-Fi 7 AP: license for Wi-Fi 7 series APs - Agile distributed AP: license for central APs and distributed APs

Item	Description
Expire time	License expiration date. The value **-** indicates no license resource. **NOTE** - If license resources for **Common AP** and a series of APs both expire or do not exist, all APs of this series cannot go online on the AC.

11.4 WLAN Radio Resource Management Configuration Commands

11.4.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.4.2 agc-threshold

Function

The **agc-threshold** command sets the AGC threshold for APs.

The **undo agc-threshold** command restores the default AGC threshold for APs.

By default, the AGC threshold is not configured.

Format

agc-threshold high *high-threshold*

undo agc-threshold high

Parameters

Parameter	Description	Value
high	Configures the upper AGC threshold or restores the default value.	-
high-threshold	Specifies the upper AGC threshold.	The value is an integer that ranges from –128 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AGC threshold is used to adjust the receiver sensitivity of packets received over the air interface.

In high-density office or stadium scenarios, you can set the AGC threshold to reduce co-channel interference in some areas. The recommended value is -82 dBm. In other scenarios, you are advised to retain the default value or set this parameter under the guidance of technical support personnel.

Precautions

The anti-interference algorithm dynamically adjusts the CCA and AGC thresholds of APs. If the CCA or AGC threshold is manually configured when the anti-interference algorithm is enabled, the manually configured threshold takes effect.

Before configuring the AGC threshold, ensure that the uplink signal strength of all STAs associated with the radio is 3 dB higher than the AGC threshold. For example, if the lowest uplink signal strength of associated STAs is -83 dBm, you are advised to set the AGC threshold to -86 dBm.

Example

Set the upper AGC threshold to –70 dBm in the 2G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] agc-threshold high -70
Warning: This parameter will affect the uplink access coverage or user access.
It is recommended that the configuration be modified under the guidance of profe
ssional technical personnel. The manually configured AGC threshold takes precede
nce over the anti-interference algorithm. If the anti-interference function is e
nabled, dynamic AGC adjustment does not take effect and the manually configured
AGC threshold takes effect. Continue? [Y/N]:y
```

11.4.3 amc-policy

Function

The **amc-policy** command configures an adaptive modulation and coding (AMC) algorithm for a radio.

The **undo amc-policy** command restores the default AMC algorithm for a radio.

By default, a radio uses the AMC algorithm **auto-balance**.

NOTE

This command does not take effect for the following APs:

- AirEngine X77X
- AirEngine X761
- AirEngine X762
- Wi-Fi 5 series APs

Format

amc-policy { **auto-balance** | **high-stability** | **high-throughput** }

undo amc-policy

Parameters

Parameter	Description	Value
auto-balance	Indicates the **auto-balance** algorithm.	-
high-stability	Indicates the **high-stability** algorithm.	-
high-throughput	Indicates the **high-throughput** algorithm.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Radios need to adjust the AMC algorithm according to different scenarios to deliver the optimal user experience. Three AMC algorithms are available:

- **auto-balance**: applicable to most wireless scenarios
- **high-stability**: applicable to scenarios with continuous interference.
- **high-throughput**: applicable to scenarios with good wireless signals and non-continuous interference.

Example

Set the AMC algorithm of a radio to **high-stability**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] amc-policy high-stability
```

11.4.4 air-scan-profile

Function

The **air-scan-profile** command creates an air scan profile and displays the air scan profile view.

The **undo air-scan-profile** command deletes an air scan profile.

By default, the system provides the air scan profile **default**. You can run the **display air-scan-profile** command to view configuration of the air scan profile **default**.

Format

air-scan-profile name *profile-name*

undo air-scan-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an air scan profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all air scan profiles.	The air scan profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an air scan profile is created using the **air-scan-profile** command and bound to a radio profile, and scanning functions are enabled, such as radio calibration, smart roaming, spectrum analysis, WLAN location, and WIDS, the AP periodically scans surrounding radio signals and reports the collected information to an AC or a server. The information is used for radio calibration, smart roaming spectrum analysis, WLAN location, or WIDS data analysis.

Follow-up Procedure

Run the **air-scan-profile (radio profile view)** command to bind the air scan profile to a 2G radio profile or 5G radio profile so that the air scan profile can take effect.

Example

Create the air scan profile **air-scan01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name air-scan01
[HUAWEI-wlan-air-scan-prof-air-scan01]
```

11.4.5 air-scan-profile (radio profile view)

Function

The **air-scan-profile** command binds an air scan profile to a radio profile.

The **undo air-scan-profile** command unbinds an air scan profile from a radio profile.

By default, the air scan profile **default** is bound to a radio profile.

Format

air-scan-profile *profile-name*

undo air-scan-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an air scan profile.	The air scan profile name must already exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an air scan profile using the **air-scan-profile** command, bind it to a radio profile so that the air scan profile can take effect.

Example

Bind the air scan profile **air-scan01** to the radio profile **office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name air-scan01
[HUAWEI-wlan-air-scan-prof-air-scan01] quit
[HUAWEI-wlan-view] radio-2g-profile name office01
[HUAWEI-wlan-radio-2g-prof-office01] air-scan-profile air-scan01
```

11.4.6 antenna-mode

Function

The **antenna-mode** command configures the antenna mode for an AP.

The **undo antenna-mode** command restores the default antenna mode of an AP.

By default, the automatic antenna mode is used on an AP.

Format

antenna-mode { **omnidirection** | **direction** | **auto** }

undo antenna-mode

Parameters

Parameter	Description	Value
omnidirection	Indicates the omnidirectional antenna mode.	-
direction	Indicates the directional antenna mode.	-
auto	Indicates the automatic antenna mode.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

For APs with built-in Dynamic-Zoom Smart Antennas, 5 GHz radios can work in omnidirectional or directional antenna mode to meet the requirements of common coverage scenarios (AP spacing > 12 m) or indoor high-density coverage scenarios (AP spacing: 10 m to 12 m). This function takes effect only for 5 GHz radios but not for APs without built-in Dynamic-Zoom Smart Antennas.

Built-in dynamic-zoom smart antennas are supported only by the AirEngine 6761-21, AirEngine 8771-X1T, and AirEngine 6761S-21.

The omnidirectional antenna mode is used for omnidirectional coverage, enabling a single AP to provide wider coverage. The directional antenna mode is used for indoor high-density deployment, allowing more APs to be deployed in an area and therefore providing a larger network capacity. In automatic antenna mode, the directional or omnidirectional mode is automatically selected based on the radio calibration algorithm. In actual project delivery, select a proper antenna mode based on the deployment scenario:

- Configure the directional antenna mode in indoor high-density coverage scenarios.
- Configure the omnidirectional antenna mode in common coverage scenarios.

NOTE

For APs with built-in Dynamic-Zoom Smart Antennas, if the directional antenna mode is used, the edge RSSI decreases by 3 dB. In this case, to ensure network coverage, run the **calibrate tpc threshold** *threshold* command to increase the TPC coverage threshold by 3 dB.

When the distance between APs with built-in Dynamic-Zoom Smart Antennas is 10 m to 12 m, co-channel interference may occur in the following scenarios:

- If there is no obstacle between two APs: Another AP is deployed between the APs, and the directional antenna mode is configured on both the APs.
- If there are obstacles between two APs (for example, two neighboring APs are deployed on two sides of a corner): The attenuation caused by obstacles is between 15 dB and 20 dB, and the directional antenna mode is configured on either AP. In this case, the two APs cannot detect each other.

Example

Configure an AP to work in directional antenna mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] antenna-mode direction
Warning: The directional mode is recommended only for high-density scenarios. In
 other scenarios, this configuration may deteriorate AP coverage performance. If
 radio calibration is ongoing, this configuration takes effect after calibration
 is complete. Continue? [Y/N]y
```

11.4.7 anti-interference disable

Function

The **anti-interference disable** command disables the anti-interference algorithm.

The **undo anti-interference disable** command enables the anti-interference algorithm.

By default, the anti-interference algorithm is enabled.

Format

anti-interference disable

undo anti-interference disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the device supports the anti-interference algorithm to improve the overall throughput in the environment.

This function takes effect only for the AirEngine X760 and AirEngine 9700D-S (including matching ORUs).

Precautions

The anti-interference algorithm may cause signal deterioration or flapping. As a result, new STAs far from an AP may encounter difficulties in accessing the network.

The anti-interference algorithm dynamically adjusts the CCA and AGC thresholds of APs. If the CCA or AGC threshold is manually configured when the anti-interference algorithm is enabled, the manually configured threshold takes effect.

Example

Disable the anti-interference algorithm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] anti-interference disable
Warning: The per-packet-TPC function and AGC check function will become invalid when anti-interference
function is disable. Continue? [Y/N]y
```

11.4.8 anti-interference agc-check disable

Function

The **anti-interference agc-check disable** command disables the automatic gain control (AGC) algorithm before packet transmission.

The **undo anti-interference agc-check disable** command enables the AGC algorithm before packet transmission.

By default, the AGC algorithm before packet transmission is enabled.

NOTE

This function takes effect only for AirEngine X760 series APs.

Format

anti-interference agc-check disable

undo anti-interference agc-check disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the device uses the AGC algorithm to detect air interface conflicts before sending packets and determines whether to send packets to the air interface, thereby improving the overall throughput.

Prerequisites

The anti-interference algorithm has been enabled.

Precautions

The anti-interference algorithm may cause signal deterioration or flapping. As a result, new STAs far from the AP may encounter difficulties in accessing the network.

Example

Disable the AGC algorithm before packet transmission.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] anti-interference agc-check disable
```

11.4.9 anti-interference per-packet-tpc disable

Function

The **anti-interference per-packet-tpc disable** command disables the per-packet power adjustment function.

The **undo anti-interference per-packet-tpc disable** command enables the per-packet power adjustment function.

By default, per-packet power adjustment is enabled.

NOTE

This command takes effect only for AirEngine X760 series APs.

Format

anti-interference per-packet-tpc disable

undo anti-interference per-packet-tpc disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the per-packet power adjustment function can properly control the transmit power of radios in an area, which reduces interference to neighboring devices while meeting wireless communication requirements.

Prerequisites

The anti-interference algorithm has been enabled.

Precautions

The anti-interference algorithm may cause signal deterioration or flapping. As a result, new STAs far from the AP may encounter difficulties in accessing the network.

Example

Disable the per-packet power adjustment function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] anti-interference per-packet-tpc disable
```

11.4.10 band-steer balance gap-threshold

Function

The **band-steer balance gap-threshold** command sets the percentage threshold for access STAs on 5 GHz radios during band steering.

The **undo band-steer balance gap-threshold** command restores the default percentage threshold for access STAs on 5 GHz radios during band steering.

By default, the percentage threshold for access STAs on 5 GHz radios during band steering is 90%.

Format

band-steer balance gap-threshold *gap-threshold*

undo band-steer balance gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the percentage threshold for access STAs on 5 GHz radios during band steering.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

After the band steering function is configured on a multi-radio AP, the AP instructs STAs that support multiple frequency bands to preferentially connect to a 5 GHz radio.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access STAs on each radio.

1. If the number of access STAs on the AP does not exceed the start threshold configured using the **band-steer balance start-threshold** command, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access STAs exceeds the value specified by the start threshold, the AP calculates the percentage of access STAs on the 5 GHz radio using the formula: (number of access STAs on the 5 GHz radio/total number of access STAs) x 100%. If the percentage exceeds the percentage threshold for access STAs on the 5 GHz radio configured using the **band-steer balance gap-threshold** command, the STA randomly selects a frequency band.

NOTE

In most cases, you are advised to use the default values of the start threshold for the number of access STAs and the percentage threshold for access STAs on 5 GHz radios. If the two thresholds are set low, the AP may allow STAs to freely select the access frequency band when the number of STAs on 5 GHz radios is small. As a result, the 5G-prior access mechanism does not take effect, and the 5 GHz band utilization cannot be maximized.

Example

Set the percentage threshold for access STAs on 5 GHz radios to 85% in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer balance gap-threshold 85
```

11.4.11 band-steer balance start-threshold

Function

The **band-steer balance start-threshold** command sets the start threshold for the number of access STAs during band steering.

The **undo band-steer balance start-threshold** command restores the default start threshold for the number of access STAs during band steering.

By default, the start threshold for the number of access STAs during band steering is 100.

Format

band-steer balance start-threshold *start-threshold*

undo band-steer balance start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for the number of access STAs during band steering.	The value is an integer that ranges from 0 to 100.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

After the band steering function is configured on a multi-radio AP, the AP instructs STAs that support multiple frequency bands to preferentially connect to a 5 GHz radio.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access STAs on each radio.

1. If the number of access STAs on the AP does not exceed the start threshold configured using the **band-steer balance start-threshold** command, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access STAs exceeds the value specified by the start threshold, the AP calculates the percentage of access STAs on the 5 GHz radio using the formula: (number of access STAs on the 5 GHz radio/total number of access STAs) x 100%. If the percentage exceeds the percentage threshold for access STAs on the 5 GHz radio configured using the **band-steer balance gap-threshold** command, the STA randomly selects a frequency band.

NOTE

In most cases, you are advised to use the default values of the start threshold for the number of access STAs and the percentage threshold for access STAs on 5 GHz radios. If the two thresholds are set low, the AP may allow STAs to freely select the access frequency band when the number of STAs on 5 GHz radios is small. As a result, the 5G-prior access mechanism does not take effect, and the 5 GHz band utilization cannot be maximized.

Example

Set the start threshold for the number of access STAs during band steering to 90 in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer balance start-threshold 90
```

11.4.12 band-steer client-band-expire

Function

The **band-steer client-band-expire** command sets the aging condition for terminal band information.

The **undo band-steer client-band-expire** command restores the default aging condition for terminal band information.

By default, band information of a terminal will be aged out under conditions that an AP has consecutively received Probe frames of the terminal more than 35 times from the same frequency band.

Format

band-steer client-band-expire *probe-counters*

undo band-steer client-band-expire

Parameters

Parameter	Description	Value
probe-counters	Sets the aging condition of terminal band information to the number of times that an AP has consecutively received Probe frames of a terminal from the same frequency band.	The value is an integer that ranges from 10 to 65535.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the band steering function is enabled on an AP, the AP records frequency band information of terminals so that the terminals can preferentially access the supported and lightly loaded frequency band.

Users may change terminals' configurations, which causes the supported frequency band of terminals to change. Therefore, the AP needs to update frequency band information of terminals in a timely manner. If the AP keeps receiving Probe frames of a terminal from a specific frequency band, and the number of receiving times exceeds a certain threshold, the AP updates the frequency band information of the terminal and considers that the terminal supports only the frequency band.

For example, the supported frequency bands of a terminal are 2.4 and 5 GHz frequency bands on an AP. If the AP only receives Probe frames of the terminal from the 2.4 GHz frequency band, and the number of times that the AP consecutively receives Probe frames from the 2.4 GHz frequency band exceeds the specified threshold, the AP considers that users change the terminal configuration and the terminal supports only the 2.4 GHz frequency band.

Precautions

If you set the aging condition to a large number of times that an AP consecutively receives Probe frames of a terminal from the same frequency band, the AP detects terminal band change more slowly. A smaller number indicates quicker response. Set the aging condition according to the difference in the number of Probe frames sent from the two frequency bands.

Example

Configure the supported band information of the terminal named **default** to age out when the number of times that an AP consecutively receives Probe frames from a frequency band exceeds 80.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer client-band-expire 80
```

11.4.13 band-steer deny-threshold

Function

The **band-steer deny-threshold** command sets the maximum number of times an AP rejects association requests of a STA for band steering.

The **undo band-steer deny-threshold** command restores the default maximum number of times an AP rejects association requests of a STA for band steering.

By default, the maximum number of rejections is 0.

Format

band-steer deny-threshold *deny-threshold*

undo band-steer deny-threshold

Parameters

Parameter	Description	Value
deny-threshold	Specifies the maximum number of times an AP rejects association requests of a STA.	The value is an integer that ranges from 0 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA requests to associate with an AP from the 2.4 GHz frequency band but the AP steers the STA to the 5 GHz frequency band according to the band steering algorithm, the AP will reject the association. However, after the number of rejections exceeds the maximum value specified by the **band-steer deny-threshold** command, the AP allows the STA to associate from the 2.4 GHz frequency band.

NOTE

The following APs do not suppress Probe Response frames on the 2.4 GHz radio before STA association. However, after STAs are associated with these APs, the STAs will be steered to the 5 GHz radio.

- AirEngine 9700D-S (including matching ORUs)
- AirEngine X77X
- AirEngine X76X

Example

Set the maximum number of rejections to 8.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer deny-threshold 8
```

11.4.14 band-steer disable

Function

The **band-steer disable** command disables the band steering function.

The **undo band-steer disable** command enables the band steering function.

By default, the band steering function is enabled.

Format

band-steer disable

undo band-steer disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with the 2.4 GHz frequency band, the 5 GHz frequency band has less interference and more available channels, and provides higher access capability.

Most STAs support both 5 GHz and 2.4 GHz frequency bands and usually associate with the 2.4 GHz radio by default when connecting to the Internet. To connect the STAs to the 5 GHz radio, you must manually select the 5 GHz radio. The band steering function frees you from the manual selection.

After you enable band steering for a specific SSID on the AC, the AP preferentially associates the terminals connected to the SSID with the 5 GHz frequency band. After the 5 GHz frequency band is fully loaded, the AP steers the terminals to the 2.4 GHz frequency band.

Configuration Impact

After the band steering function is enabled, it takes a long time for dual-band terminals to associate or roam. You are advised to disable band steering for delay-sensitive services.

Precautions

If both radios of an AP use the same VAP profile, the band steering function takes effect on both radios as long as the function is enabled for an SSID on one radio of the AP. For example, if band steering is enabled for the SSID **test** on the 2.4 GHz radio but not on the 5 GHz radio, the AP preferentially steers terminals associated with the SSID to the 5 GHz radio.

Single-radio devices do not support the band steering function.

Example

Disable band steering.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] band-steer disable
```

11.4.15 band-steer snr-threshold

Function

The **band-steer snr-threshold** command configures a start SNR threshold for triggering 5G-prior access.

The **undo band-steer snr-threshold** command restores the default start SNR threshold for triggering 5G-prior access.

The default start SNR threshold for triggering 5G-prior access is 20 dB.

Format

band-steer snr-threshold *snr-threshold*

undo band-steer snr-threshold

Parameters

Parameter	Description	Value
snr-threshold	Specifies a start SNR threshold for triggering 5G-prior access.	The value is an integer that ranges from 10 to 35, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo band-steer disable** command to enable the band steer function and the **band-steer snr-threshold** command to configure a start SNR threshold for triggering 5G-prior access. When the SNR in 5G Probe frames sent by a multi-band STA to a multi-radio AP exceeds the specified threshold, the STA connects to the 5G radio preferentially, improving user experience.

Example

Set the start SNR threshold for triggering 5G-prior access in the RRM profile **default** to 20 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] band-steer snr-threshold 20
```

11.4.16 bss-color disable

Function

The **bss-color disable** command disables the basic service set (BSS) coloring function.

The **undo bss-color disable** command enables the BSS coloring function.

By default, the BSS coloring function is enabled.

Format

bss-color disable

undo bss-color disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density scenarios, the 802.11ax protocol proposes the BSS coloring mechanism to improve system performance and channel usage efficiency. When detecting 802.11ax signals, STAs can identify the signals from the overlapping basic service set (OBSS) based on the BSS color bit or MAC address, and then determine air interface conflicts and perform interference management according to related information. The BSS coloring function enables a device to distinguish between the transmissions on the local and neighboring networks. Then, it can adaptively adjust the power and the sensitivity threshold to allow dynamic adjustment of the transmit power and the signal detection threshold to increase spatial reuse efficiency and minimize co-channel interference.

Precautions

Disabling the BSS coloring function will automatically disable the spatial reuse (SR) function.

The BSS coloring function does not take effect when the radio scanning function is enabled on an AP.

Example

Disable the BSS coloring function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] bss-color disable
Warning: The spatial reuse function will become invalid when BSS color function is disable. Continue?
[Y/N]y
```

11.4.17 btm-fail-times

Function

The **btm-fail-times** command sets the maximum number of attempts to steer STAs in BTM mode.

The **undo btm-fail-times** command restores the default maximum number of attempts to steer STAs in BTM mode.

By default, the maximum number of attempts to steer STAs in BTM mode is 5.

Format

btm-fail-times *btm-fail-times*

undo btm-fail-times

Parameters

Parameter	Description	Value
btm-fail-times	Specifies the number of attempts to steer STAs in BTM mode.	The value is an integer that ranges from 0 to 10. The value 0 indicates that the BTM mode is not used to steer STAs.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device preferentially uses the BTM mode to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in BTM mode after multiple attempts. You can run the **btm-fail-times** command to set the maximum number of attempts to steer STAs in BTM mode. If the number of attempts exceeds the specified value, the device attempts to steer STAs in deauthentication mode.

Precautions

You are advised to retain the default value. If the success rate of STA steering in BTM mode is low, you can set a smaller value to improve the steering efficiency.

Example

Set the maximum number of attempts to steer STAs in BTM mode to 4.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] btm-fail-times 4
```

11.4.18 calibrate auto-bandwidth-select

Function

The **calibrate auto-bandwidth-select** { **enable** | **disable** } command enables or disables the dynamic bandwidth selection (DBS) function.

The **undo calibrate auto-bandwidth-select** command restores the default DBS state.

By default, the DBS function is disabled in the AP group radio view and not configured in the AP radio view. This command takes effect only for 5 GHz and 6 GHz radios.

Format

calibrate auto-bandwidth-select { **enable** | **disable** }

undo calibrate auto-bandwidth-select

Parameters

Parameter	Description	Value
enable	Enables the DBS function.	-
disable	Disables the DBS function.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In non-high-density indoor scenarios, the DBS function can leverage the radio calibration mechanism to automatically select proper bandwidth, improving the overall system capacity.

Prerequisites

- Radio calibration has been enabled using the **calibrate enable** { **auto** | **manual** | **schedule time** } command.
- Automatic channel selection has been enabled using the **calibrate auto-channel-select enable** command.

Precautions

- The DBS function is valid only for 5 GHz and 6 GHz radios.
- The DBS function is applicable only to indoor APs with omnidirectional antennas. The adjustment effect cannot be ensured for indoor APs with directional antennas and outdoor APs.
- The DBS function takes effect only between Fit APs connected to the same AC but not between APs connected to different ACs.
- The DBS effect is not obvious for high-density scenarios.

To view historical records of channel, bandwidth, and transmit power changes caused by radio calibration, run the **display channel switch-record calibrate** command.

Example

Enable the DBS function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 1
[HUAWEI-wlan-group-radio-default/1] calibrate auto-bandwidth-select enable
```

11.4.19 calibrate auto-channel-select

Function

The **calibrate auto-channel-select** { **enable** | **disable** } command enables or disables automatic channel selection.

The **undo calibrate auto-channel-select** command restores the automatic channel selection state.

By default, the automatic channel selection function is enabled in the AP group radio view and not configured in the AP radio view.

Format

calibrate auto-channel-select { **enable** | **disable** }

undo calibrate auto-channel-select

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Two channel selection modes are available:

- Automatic mode (enabling automatic channel selection): An AP automatically selects a proper channel based on the WLAN radio environment, removing the need to specify channels manually.
- Fixed mode (disabling automatic channel selection): Channels must be manually specified.

The automatic mode (automatic channel selection) is recommended because you do not need to specify a channel for each radio. The fixed mode provides users with an alternative way when they want to specify channels by themselves or to avoid frequent channel adjustment (this may cause intermittent service interruption).

If an AP needs radio calibration, automatic channel selection must be enabled.

To view historical records of channel, bandwidth, and transmit power changes caused by radio calibration, run the **display channel switch-record calibrate** command.

NOTE

When automatic channel selection is enabled, the manually configured channels do not take effect to ensure that the radio works in the optimal channel environment.

Example

Disable automatic channel selection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] calibrate auto-channel-select disable
```

11.4.20 calibrate auto-txpower-select

Function

The **calibrate auto-txpower-select** { **enable** | **disable** } command enables or disables automatic transmit power selection.

The **undo calibrate auto-txpower-select** command restores the automatic transmit power selection state.

By default, the automatic transmit power selection function is enabled in the AP group radio view and not configured in the AP radio view.

Format

calibrate auto-txpower-select { **enable** | **disable** }

undo calibrate auto-txpower-select

Parameters

Parameter	Description	Value
enable	Enables the automatic transmit power selection function.	-
disable	Disables the automatic transmit power selection function.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Two power selection modes are available:

- Automatic mode (enabling automatic transmit power selection): An AP automatically selects or adjusts the transmit power based on the WLAN radio environment, removing the need to specify AP power manually.
- Fixed mode (disabling automatic transmit power selection): The transmit power must be manually specified.

If an AP needs radio calibration, automatic transmit power selection must be enabled.

To view historical records of channel, bandwidth, and transmit power changes caused by radio calibration, run the **display channel switch-record calibrate** command.

Example

Disable automatic transmit power selection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] calibrate auto-txpower-select disable
```

11.4.21 calibrate enable { auto | manual | schedule time }

Function

The **calibrate enable** { **auto** | **manual** | **schedule time** } command configures the radio calibration mode.

The **undo calibrate enable** command disables radio calibration.

By default, the radio calibration mode is **auto**, the radio calibration interval is 1440 minutes, and the start time for radio calibration is 03:00:00.

Format

calibrate enable { **auto** [**interval** *interval-value* [**start-time** *start-time*]] | **manual** | **schedule time** *time-value* [**time-range** *time-range-name*] }

undo calibrate enable

Parameters

Parameter	Description	Value
auto	Sets the radio calibration mode to automatic calibration.	-
interval *interval-value*	Specifies the calibration interval in automatic radio calibration mode.	The value is an integer that ranges from 30 to 1440, in minutes. If **interval** is not specified, the radio calibration interval in auto mode is 1440 minutes.
start-time *start-time*	Specifies the start time for automatic radio calibration.	The value is in the format of hh:mm:ss. ● hh: indicates the hour. The value is an integer that ranges from 0 to 23. ● mm: indicates the minute. The value is an integer that ranges from 0 to 59. ● ss: indicates the second. The value is an integer that ranges from 0 to 59.
manual	Sets the radio calibration mode to manual calibration.	-
schedule	Sets the radio calibration mode to scheduled calibration.	-
time *time-value*	Specifies the time for triggering the scheduled radio calibration.	The value is in the format of hh:mm:ss. ● hh: indicates the hour. The value is an integer that ranges from 0 to 23. ● mm: indicates the minute. The value is an integer that ranges from 0 to 59. ● ss: indicates the second. The value is an integer that ranges from 0 to 59.

Parameter	Description	Value
time-range *time-range-name*	Specifies the name of a time range for scheduled radio calibration.	The specified time range must exist. You can run the **time-range** command to configure a time range. **NOTE** Ensure that the scheduled radio calibration time is within the time range specified by **time-range**. Otherwise, the scheduled radio calibration function does not take effect.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

There are three radio calibration modes:

- Automatic radio calibration mode: The device continuously monitors the wireless environment quality by scanning the air interface. If the air interface environment deteriorates (for example, high bit error rate or matching the policy of high noise floor), the device automatically triggers partial radio calibration to avoid interference. To prevent service interruption caused by radio calibration, you are advised to set the calibration start time during off-peak hours. To prevent frequent calibration, you are advised to set a proper calibration interval. In addition, the device performs global radio calibration periodically based on the specified start time and interval.
- Manual radio calibration mode: Global radio calibration is not automatically implemented by the device but manually triggered through the **calibrate manual startup** command.
- Schedule radio calibration mode: The device triggers radio calibration only at a specified time point (specified by **time**) or in a specified time range (specified by **time-range**).

The three modes cannot be configured simultaneously. You can choose any of the modes as required.

In any mode, you can run the **calibrate manual startup** command to trigger global radio calibration. In manual radio calibration mode, the device implements global radio calibration only after the **calibrate manual startup** command is executed.

NOTE

Regardless of the calibration mode, an AP triggers partial radio calibration when detecting the following situations:

- The packet retransmission rate exceeds the threshold. (You can run the **calibrate retransmission-rate-threshold** command to configure the threshold.)
- The air interface environment deteriorates. (You can run the **calibrate interference-check threshold** command in the diagnostic view to configure the threshold.)

Example

Set the radio calibration mode to manual calibration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable manual
```

Set the radio calibration mode to scheduled calibration and set the scheduled calibration time to 20:30:00.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable schedule time 20:30:00
```

11.4.22 calibrate environment-deterioration-blacklist

Function

The **calibrate environment-deterioration-blacklist** command sets the blacklist threshold for the number of times the channel environment deteriorates.

The **undo calibrate environment-deterioration-blacklist** command restores the default blacklist threshold for the number of times the channel environment deteriorates.

By default, the blacklist threshold for the number of times the channel environment deteriorates is 16.

Format

calibrate environment-deterioration-blacklist threshold *threshold*

undo calibrate environment-deterioration-blacklist

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the blacklist threshold for the number of times the channel environment deteriorates.	The value is an integer that ranges from 1 to 48.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When detecting that the environment of a channel deteriorates, the device generates an environment deterioration alarm and accumulates the number of environment deterioration times on the channel. If this number exceeds the threshold, the channel is added to the calibration blacklist. The device will skip this channel when performing radio calibration next time. If the number of environment deterioration times does not exceed the threshold, interference penalty is performed accordingly.

NOTE

If the number of environment deterioration times on more than half of calibration channels exceeds the threshold, the device performs interference penalty on all channels in the next calibration but does not add the channels to the blacklist.

Example

Set the blacklist threshold for the number of times the channel environment deteriorates to 20.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate environment-deterioration-blacklist threshold 20
```

11.4.23 calibrate retransmission-rate-check

Function

The **calibrate retransmission-rate-check** command configures the interval and traffic threshold for checking the retransmission rate.

The **undo calibrate retransmission-rate-check** command restores the default interval and traffic threshold for checking the retransmission rate.

The default interval and traffic threshold for checking the retransmission rate are 1 minute and 1250 kbit/s, respectively.

Format

calibrate retransmission-rate-check interval *interval* **traffic-threshold** *traffic-threshold*

undo calibrate retransmission-rate-check

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for checking the retransmission rate.	The value is an integer that ranges from 1 to 10, in minutes.
traffic-threshold *traffic-threshold*	Specifies the traffic threshold for checking the retransmission rate.	The value is an integer that ranges from 1 to 20000, in kbit/s.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **calibrate retransmission-rate-check** command to lower the sensitivity for collecting radio retransmission rate statistics. When the rate of network traffic reaches the threshold, retransmission rate check is performed at the specified interval.

Example

Set the interval and traffic threshold for checking the retransmission rate in the RRM profile **80211b** to 2 minutes and 1000 kbit/s, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name 80211b
[HUAWEI-wlan-rrm-prof-80211b] calibrate retransmission-rate-check interval 2 traffic-threshold 1000
```

11.4.24 calibrate retransmission-rate-threshold

Function

The **calibrate retransmission-rate-threshold** command sets the retransmission rate threshold.

The **undo calibrate retransmission-rate-threshold** command restores the default retransmission rate threshold.

By default, the retransmission rate threshold is 60%.

Format

calibrate retransmission-rate-threshold *retransmission-rate-threshold*

undo calibrate retransmission-rate-threshold

Parameters

Parameter	Description	Value
retransmission-rate-threshold	Specifies the retransmission rate threshold.	The value is an integer that ranges from 20 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The retransmission rate is the ratio of retransmitted packets to all packets sent by a radio.

The retransmission rate threshold determines whether the radio environment is normal. When the retransmission rate of a radio reaches the threshold, the system considers that the radio environment deteriorates. When this occurs, the system may start radio calibration or take measures to avoid signal interference.

Example

Set the retransmission rate threshold to 70% in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate retransmission-rate-threshold 70
```

11.4.25 calibrate flexible-radio

Function

The **calibrate flexible-radio** { **auto-switch** | **auto-off** } command enables global dynamic frequency assignment (DFA) and sets the mode for processing redundant radios.

The **undo calibrate flexible-radio** command disables global DFA.

By default, global DFA is disabled.

Format

calibrate flexible-radio { **auto-switch** | **auto-off** }

undo calibrate flexible-radio

Parameters

Parameter	Description	Value
auto-switch	Automatically switches redundant 2.4 GHz radios to 5 GHz radios. If no channel is available on a 5 GHz radio or the current radio cannot be switched to a 5 GHz radio, the current radio is switched to the monitor mode.	-
auto-off	Automatically disables redundant 2.4 GHz radios.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DFA applies to scenarios where indoor APs with omnidirectional antennas are densely deployed, the 2.4 GHz frequency band has severe co-channel interference, and most STAs on the network support the 5 GHz frequency band.

DFA automatically switches or disables redundant radios.

- If an AP does not support radio switchover, you are advised to specify **auto-off** in the command to reduce co-channel interference and save energy.
- If an AP supports radio switchover, you are advised to specify **auto-switch** in the command to increase network capacity. If most redundant 2.4 GHz radios are automatically switched to the monitor mode, channel resources on the current network are properly used. In this case, you can specify **auto-off** in the command.

Prerequisites

The radio calibration function has been enabled using the **calibrate enable** { **auto** | **manual** | **schedule time** } command.

Precautions

DFA reduces the deployment density of 2.4 GHz radios and increases the transmit power of 2.4 GHz radios. To ensure the 5 GHz access ratio of STAs, keep the band steering function enabled.

When DFA is disabled, redundant radios are switched back to 2.4 GHz radios and the system automatically triggers radio calibration, which may degrade wireless service experience.

Example

Enable global DFA and set the mode for processing redundant radios to automatic switchover.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate flexible-radio auto-switch
```

11.4.26 calibrate flexible-radio disable

Function

The **calibrate flexible-radio disable** command disables DFA of specified radios.

The **undo calibrate flexible-radio disable** command enables DFA of specified radios.

By default, the DFA function of a radio is enabled.

Format

calibrate flexible-radio disable

undo calibrate flexible-radio disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After global DFA is enabled, you can run this command to disable DFA of a single AP radio or radios of an AP group in some areas.

Prerequisites

Global DFA has been enabled using the **calibrate flexible-radio** { **auto-switch** | **auto-off** } command.

Example

Disable DFA of radio 0 of AP 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate flexible-radio auto-switch
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] calibrate flexible-radio disable
```

11.4.27 calibrate flexible-radio manual-recognize

Function

The **calibrate flexible-radio manual-recognize** command triggers identification of redundant radios.

Format

calibrate flexible-radio manual-recognize

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network administrator can run this command to manually trigger identification of redundant radios, and can enable DFA if discovering that redundant radios exist on the network.

Prerequisites

The radio calibration function has been enabled using the **calibrate enable** { **auto** | **manual** | **schedule time** } command.

Precautions

This command only triggers identification of redundant radios but does not switch or disable identified redundant radios.

Radio scanning is required for identifying redundant radios, which may degrade wireless service experience.

Follow-up Procedure

After redundant radios are identified, you can run the **display flexible-radio status** command to check the status of the redundant radios.

Example

Trigger identification of redundant radios.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate flexible-radio manual-recognize
```

11.4.28 calibrate grouping interference-threshold

Function

The **calibrate grouping interference-threshold** command sets the interference threshold of a calibration group.

The **undo calibrate grouping interference-threshold** command restores the default interference threshold of a calibration group.

The default interference threshold of a calibration group is –127 dBm.

Format

calibrate grouping interference-threshold *threshold*

undo calibrate grouping interference-threshold

Parameters

Parameter	Description	Value
threshold	Specifies the interference threshold of a calibration group.	The value is an integer that ranges from –127 to –1, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During radio calibration, the system adds neighboring APs to the same calibration group and allocates channels to them. If there are a large number of APs in a calibration group but only a few channels are available, the same channel may be allocated to neighboring APs. In scenarios where APs are blocked by walls or deployed regularly, such as dormitories and hotels, you can set a proper RSSI interference threshold to control the number of APs in the same calibration group. This effectively reduces the probability that neighboring APs use the same channel. If the RSSI of a neighbor working at the maximum power exceeds the threshold, the neighbor is added to the same calibration group. **In other scenarios, use the default value.**

Precautions

In typical scenarios, it is recommended that the interference threshold in a calibration group be set to –70 dBm. If severe co-channel interference exists between APs and neighboring APs, you can sample 1/10 of APs on each floor and calculate the accurate threshold so that the calibration algorithm can stagger the channels of neighboring APs. The specific calculation method is as follows:

1. Run the **display radio all** command and query the maximum power of each radio based on the **ME** field in the command output.
2. Run the **display ap neighbor** command to query information about neighboring APs of the target AP. Based on the **RSSI pathloss** field in the command output, calculate the maximum power values of the neighboring APs.
3. Sort the RSSIs of neighboring APs in descending order (for example, –58 dBm, –60 dBm, –62 dBm, –80 dBm, –84 dBm, –86 dBm, –90 dBm), and calculate the differences between RSSIs of neighboring APs (for example, 2 dB, 2 dB, 18 dB, 4 dB, 2 dB, 4 dB).
4. Find the first edge point where the RSSI difference is greater than or equal to 15 dB in descending order of neighboring APs' RSSIs. Divide the neighboring APs into two groups at the point: one group with strong detected RSSIs and the other with weak detected RSSIs.

   In the preceding example, the point where the RSSI difference is 18 dB is between the neighbors with –62 dBm and –80 dBm. Therefore, the seven neighbors of the AP are divided into two groups: a group with strong detected RSSIs (–58 dBm, –60 dBm, –62 dBm) and a group with weak detected RSSIs (–80 dBm, –84 dBm, –86 dBm, –90 dBm).
5. Calculate the average value between the minimum RSSI value of the group with strong detected RSSIs and the maximum RSSI value of the group with weak detected RSSIs. Use this average value as the RSSI threshold of the calibration group.

   In the preceding example, –62 dBm and –80 dBm are extracted from the two groups. The average value of the two values is –76 dBm, which is used as the recommended RSSI interference threshold.

NOTE

If the average threshold value calculated based on the sampled APs can meet the grouping requirements of all sampled APs, you can use this value for all APs in this scenario. Otherwise, it is recommended that different thresholds be configured for specific APs.

Example

Set the interference threshold of a calibration group to –70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate grouping interference-threshold -70
```

11.4.29 calibrate max-tx-power

Function

The **calibrate max-tx-power** command sets the maximum transmit power that can be adjusted through radio calibration.

The **undo calibrate max-tx-power** command restores the default maximum transmit power that can be adjusted through radio calibration.

By default, the maximum transmit power that can be adjusted through radio calibration is 127 dBm.

Format

calibrate max-tx-power { *2g-power* | **radio-5g** *5g-power* | **radio-6g** *6g-power* }

undo calibrate max-tx-power [**radio-5g** | **radio-6g**]

Parameters

Parameter	Description	Value
2g-power	Specifies the maximum transmit power that can be adjusted through 2.4 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.
radio-5g *5g-power*	Specifies the maximum transmit power that can be adjusted through 5 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.
radio-6g *6g-power*	Specifies the maximum transmit power that can be adjusted through 6 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After radio calibration is enabled, an AP uses the Transmit Power Control (TPC) algorithm to calculate the transmit power to be adjusted based on detected neighbor information. If the transmit power to be adjusted calculated using the

TPC algorithm is to large, signal interference between APs may occur. You can run the **calibrate max-tx-power** command to set the maximum transmit power that can be adjusted through TPC.

Precautions

The maximum radio calibration power must be greater than or equal to the minimum radio calibration power. You can run the **calibrate min-tx-power** command to set the minimum calibration power.

You can adjust the maximum and minimum calibration power values using the **calibrate max-tx-power** and **calibrate min-tx-power** commands. The valid AP power after radio calibration is between the two values.

Example

Set the maximum transmit power that can be adjusted through 2.4 GHz radio calibration to 30 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate max-tx-power 30
```

11.4.30 calibrate min-tx-power

Function

The **calibrate min-tx-power** command sets the minimum transmit power that can be adjusted through radio calibration.

The **undo calibrate min-tx-power** command restores the default minimum transmit power that can be adjusted through radio calibration.

By default, the minimum transmit power that can be adjusted through 2.4 GHz radio calibration is 9 dBm, and that through 5 GHz or 6 GHz radio calibration is 12 dBm.

Format

calibrate min-tx-power { *2g-power* | **radio-5g** *5g-power* | **radio-6g** *6g-power* }

undo calibrate min-tx-power [**radio-5g** | **radio-6g**]

Parameters

Parameter	Description	Value
2g-power	Specifies the minimum transmit power that can be adjusted through 2.4 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.

Parameter	Description	Value
radio-5g *5g-power*	Specifies the minimum transmit power that can be adjusted through 5 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.
radio-6g *6g-power*	Specifies the minimum transmit power that can be adjusted through 6 GHz radio calibration.	The value is an integer that ranges from 1 to 127, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After radio calibration is enabled, an AP uses the Transmit Power Control (TPC) algorithm to calculate the transmit power to be adjusted based on detected neighbor information. If the transmit power calculated using the TPC algorithm is too small, radio coverage requirements may not be met. You can run the **calibrate min-tx-power** command to set the minimum transmit power that can be adjusted through TPC.

Precautions

The minimum radio calibration power must be less than or equal to the maximum radio calibration power. You can run the **calibrate max-tx-power** command to set the maximum calibration power.

You can adjust the maximum and minimum calibration power values using the **calibrate max-tx-power** and **calibrate min-tx-power** commands. The valid AP power after radio calibration is between the two values.

Example

Set the minimum transmit power that can be adjusted through 2.4 GHz radio calibration to 10 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate min-tx-power 10
```

11.4.31 calibrate manual startup

Function

The **calibrate manual startup** command manually triggers radio calibration.

Format

calibrate manual startup [{ **ap-group** *group-name* }&<1-4> | **ap-id** *ap-list*]

Parameters

Parameter	Description	Value
ap-group *group-name*	Specifies an AP group. **NOTE** A maximum of four AP groups can be specified.	The AP group must exist.
ap-id *ap-list*	Specifies AP IDs in a batch.	The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) or hyphens (-) to separate AP IDs. For example, 5,8,10-13,20 indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

To trigger radio calibration immediately, run the **calibrate enable** { **auto** | **manual** | **schedule time** } command to enable radio calibration and then run the **calibrate manual startup** command to manually trigger radio calibration.

You can select an AP group or list to implement radio calibration for specified APs.

Example

Manually trigger radio calibration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate enable auto
[HUAWEI-wlan-view] calibrate manual startup
Warning: The operation may cause business interruption, Continue? [Y/N]:y
```

11.4.32 calibrate noise-floor-threshold

Function

The **calibrate noise-floor-threshold** command specifies the noise floor threshold for triggering radio calibration.

The **undo calibrate noise-floor-threshold** command restores the default noise floor threshold for triggering radio calibration.

The default noise floor threshold for triggering radio calibration is -75 dBm.

Format

calibrate noise-floor-threshold *threshold*

undo calibrate noise-floor-threshold

Parameters

Parameter	Description	Value
noise-floor-threshold *threshold*	Specifies the noise floor threshold for triggering radio calibration.	The value is an integer that ranges from -95 to 0, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The noise floor indicates the noise strength in the current environment. A high noise floor value will make noise drown out valid data, affecting user services.

The noise floor threshold for triggering radio calibration can be used to determine whether the environment noise is normal. When detecting a noise floor value higher than the threshold, an AP reports a high noise floor message to the AC. The AC then performs radio calibration to avoid channels with high noise floor values to improve user experience.

Precautions

In most cases, the default noise floor threshold is recommended. When high noise floor leads to poor user experience, you can increase the threshold based on the real-time noise floor. To check the noise floor of an AP, run the **display ap traffic statistics wireless** command.

Example

Set the noise floor threshold for triggering radio calibration to -60 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate noise-floor-threshold -60
```

11.4.33 calibrate policy

Function

The **calibrate policy** command creates a radio calibration policy.

The **undo calibrate policy** command deletes a radio calibration policy.

By default, no radio calibration policy is created.

Format

calibrate policy { **non-wifi** | **noise-floor** }

undo calibrate policy { **non-wifi** | **noise-floor** }

Parameters

Parameter	Description	Value
non-wifi	Specifies the non-Wi-Fi mode.	-
noise-floor	Specifies the noise floor mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radio calibration policies are classified into:

- Non-Wi-Fi: If non-Wi-Fi devices exist on the network, the radio calibration algorithm takes interference that may be caused by them into account when radio calibration is performed next time.
- Noise floor policy: When the noise floor of APs is high due to special external interference, service experience may deteriorate. With this radio calibration policy, the device takes actions to avoid interference. When detecting that the noise floor of the current channel exceeds the threshold for three consecutive

times, an AP notifies the AC of the high noise floor. The AC then allocates another channel to the AP and does not allocate the current channel to the AP in 30 minutes.

NOTE

Partial radio calibration triggered based on the noise floor takes effect only in automatic radio calibration mode.

The non-Wi-Fi policy is only supported by APs that support spectrum analysis.

To disable rogue interference calibration, run the **calibrate reference rogue-ap-interference disable** command.

Radio calibration triggers channel changes. Some STAs may go offline and then go online again. If these STAs exist on the network, to ensure service experience, you are advised to perform radio calibration when no service is running and disable policies that frequently trigger radio calibration. You can run the **display channel switch-record calibrate** command to check policies that frequently trigger radio calibration.

The three radio calibration policies can be used together. You can run the command multiple times to configure different radio calibration policies according to service requirements.

Prerequisites

The noise floor threshold for triggering radio calibration has been specified using the **calibrate noise-floor-threshold** *threshold* command.

Example

Create a radio calibration policy in non-Wi-Fi mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate policy non-wifi
```

11.4.34 calibrate reference 3d-data

Function

The **calibrate reference 3d-data** { **enable** | **disable** } command enables or disables the 3D radio calibration function.

The **undo calibrate reference 3d-data** command restores the default state of the 3D radio calibration function.

By default, 3D radio calibration is enabled in the AP group radio view and is not configured in the AP radio view.

Format

calibrate reference 3d-data { **enable** | **disable** }

undo calibrate reference 3d-data

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Traditional radio calibration can only construct a topology between APs based on inter-AP probe data and automatically adjust the channels and transmit power of the APs. The latest calibration algorithm can construct a 3D network topology (AP-STA-AP) based on the probe data between APs and STAs during radio calibration. This helps accurately identify the topology relationship between APs (for example, APs installed at heights). In this way, the calibration effect is improved. You can run this command to enable 3D radio calibration to achieve optimization based on the analysis result of STA measurement data.

NOTE

- The 3D radio calibration function takes effect only for APs running V200R021C10 or later.
- APs running versions earlier than V200R021C10 cannot collect or report STA measurement data. Enabling the 3D radio calibration function will affect the accuracy of identification results. If these APs exist on the network, you are advised to upgrade all APs to V200R021C10 or later, or disable the 3D radio calibration function.

Example

Enable 3D radio calibration.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-ap-group1] radio 0
[HUAWEI-wlan-group-radio-ap-group1/0] calibrate reference 3d-data enable
```

11.4.35 calibrate reference data-analysis disable

Function

The **calibrate reference data-analysis disable** disables the Big Data calibration function.

The **undo calibrate reference data-analysis** command restores the default configuration.

By default, Big Data calibration is enabled.

Format

calibrate reference data-analysis disable

undo calibrate reference data-analysis

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After Big Data calibration is enabled, the device performs calculation based on the variations in interference and load according to Big Data information obtained from the iMaster NCE-CampusInsight. This function helps better avoid interference and improve network capacity. If the Big Data calibration function is disabled, radio calibration is performed based only on the locally collected data.

The Big Data calibration function takes effect only when radio calibration is enabled.

Example

Disable the Big Data calibration function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate reference data-analysis disable
```

11.4.36 calibrate reference data-analysis

Function

The **calibrate reference data-analysis disable** command disables Big Data calibration on radio interfaces of APs and AP groups.

The **calibrate reference data-analysis enable** command enables Big Data calibration on radio interfaces of APs and AP groups.

The **undo calibrate reference data-analysis** command restores the default Big Data calibration configuration on radio interfaces of APs and AP groups.

By default, Big Data calibration is disabled on radio interfaces of APs but enabled on radio interfaces in an AP group.

Format

calibrate reference data-analysis { disable | enable }

undo calibrate reference data-analysis

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After Big Data calibration is enabled, the device performs calculation based on the variations in interference and load according to Big Data information obtained from the iMaster NCE-CampusInsight. This function helps better avoid interference and improve network capacity. If the Big Data calibration function is disabled, radio calibration is performed based only on the locally collected data.

NOTE

The Big Data calibration function takes effect on an AP only when the following configurations are performed:

- Configure the function of reporting KPIs to the Big Data analyzer.
- Enable radio calibration.
- Run the **undo calibrate reference data-analysis** command in the WLAN view to enable the global Big Data calibration function.
- Enable the Big Data calibration function on the AP. (If the Big Data calibration function is not configured on a single AP, the configuration of the AP group takes effect.)

Example

Enable Big Data calibration on radio 0 in AP group **ap-group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] radio 0
[HUAWEI-wlan-group-radio-ap-group1/0] calibrate reference data-analysis enable
```

11.4.37 calibrate reference rogue-ap-interference disable

Function

The **calibrate reference rogue-ap-interference disable** command disables rogue interference calibration so that the device performs radio calibration only based on information about authorized neighbors.

The **undo calibrate reference rogue-ap-interference disable** command enables rogue interference calibration so that the device performs radio calibration based on information about both authorized and rogue neighbors.

By default, rogue interference calibration is enabled.

Format

calibrate reference rogue-ap-interference disable

undo calibrate reference rogue-ap-interference disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Rogue neighbors often interfere with radio signals of APs. Therefore, a WLAN usually takes rogue neighbors as one of the factors for radio calibration and avoids the channels used by the rogue neighbors. If only a few channels are available, authorized APs on the same channel may be deployed too close to each other, affecting wireless network coverage. In actual delivery, if rogue interference is low (no or little interference traffic), you can run the **calibrate reference rogue-ap-interference disable** command to adjust the radio calibration policy so that the device does not consider external Wi-Fi interference from rogue neighbors during radio calibration. In this way, more channel resources are available for allocation during radio calibration.

To take non-Wi-Fi interference into account during radio calibration, run the **calibrate policy non-wifi** command.

Example

Disable rogue interference calibration so that the device performs radio calibration only based on information about authorized neighbors.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate reference rogue-ap-interference disable
```

11.4.38 calibrate sensitivity

Function

The **calibrate sensitivity** command configures the calibration sensitivity for a device.

The **undo calibrate sensitivity** command restores the default calibration sensitivity.

By default, the calibration sensitivity of the device is **medium**.

Format

calibrate sensitivity [**2.4g** | **5g** | **6g**] { **high** | **medium** | **low** | **insensitivity** | **custom-percent** *custom-percent* }

undo calibrate sensitivity [**2.4g** | **5g** | **6g**]

Parameters

Parameter	Description	Value
high	Indicates high calibration sensitivity.	-
medium	Indicates medium calibration sensitivity.	-
low	Indicates low calibration sensitivity.	-
insensitivity	Indicates calibration insensitivity.	-
custom-percent *custom-percent*	Specifies the calibration sensitivity based on the customized threshold.	The value ranges from 0 to 100, in percentage (%). A larger value indicates a lower sensitivity.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Radio calibration sensitivity is valid only in automatic radio calibration mode (enabled using the **calibrate enable auto** command). The default value is recommended.

If the percentage of radios with severe interference reaches the calibration sensitivity threshold, global channels are adjusted during radio calibration. Otherwise, the algorithm adjusts the operating channels of only radios with severe interference.

- high: equivalent to the custom threshold of 25%
- medium: equivalent to the custom threshold of 50%
- low: equivalent to the custom threshold of 75%
- insensitivity: equivalent to the custom threshold of 100%

Example

Set the calibration sensitivity to high for radios on all frequency bands.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate sensitivity high
```

11.4.39 calibrate tpc threshold

Function

The **calibrate tpc threshold** command sets the Transmit Power Control (TPC) coverage threshold.

The **undo calibrate tpc threshold** command restores the default TPC coverage threshold.

The default TPC coverage threshold is –60 dBm.

Format

calibrate tpc threshold *threshold*

undo calibrate tpc threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the TPC coverage threshold.	The value is an integer that ranges from -85 to -35, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When radio calibration is enabled, the TPC coverage threshold is different depending on AP deployment scenarios because the AP deployment distance or height differs. To ensure the optimal coverage effect, adjust the TPC coverage threshold based on the actual AP deployment situations. A large threshold indicates a wider transmit power range that can be adjusted through TPC.

Example

Set the TPC coverage threshold to -70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] calibrate tpc threshold -70
```

11.4.40 calibrate virtual-group-size

Function

The **calibrate virtual-group-size** command sets the channel calibration group size and K value.

The **undo calibrate virtual-group-size** command restores the default channel calibration group size and K value.

By default, the channel calibration group size is 50, and the K value is 70.

Format

calibrate virtual-group-size *size-value* **k-value** *k-value*

undo calibrate virtual-group-size

Parameters

Parameter	Description	Value
size-value	Sets the channel calibration group size. This parameter is an algorithm parameter. Set it under the assistance of technical support personnel.	The value is an integer that ranges from 10 to 50.
k-value *k-value*	Sets the K value. This parameter is an algorithm parameter. Set it under the assistance of technical support personnel.	The value is an integer that ranges from 20 to 100.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can set internal algorithm parameters for radio calibration to optimize radio calibration time costs and effects. Set the parameters under the assistance of technical support personnel.

Example

Set the channel calibration group size to 40 and K value to 80.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] calibrate virtual-group-size 40 k-value 80
```

11.4.41 cca-threshold

Function

The **cca-threshold** command sets the clear channel assessment (CCA) threshold for APs.

The **undo cca-threshold** command restores the default CCA threshold of APs.

By default, no CCA threshold is specified. APs use the default CCA threshold of the chip.

NOTE

The CCA threshold does not take effect for the following APs:

- AirEngine X771
- AirEngine X761
- AirEngine X762

Format

cca-threshold *cca-threshold*

undo cca-threshold

Parameters

Parameter	Description	Value
cca-threshold	Specifies the CCA threshold for APs.	The value is an integer that ranges from –85 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CCA mechanism enables a WLAN chip to determine whether the channel is idle before transmitting signals to the air interface. If so, the chip transmits signals. If not, the chip waits until the channel is idle.

The CCA threshold is used by the WLAN chip to evaluate whether a channel is idle. If the detected Wi-Fi signal strength on the current channel exceeds the threshold, the current channel is busy. Otherwise, the current channel is idle.

When deploying a WLAN, you can set a proper CCA threshold to reduce interference of co-channel Wi-Fi signals in the surrounding environment to the current AP and improve channel reuse rate.

In high-density coverage scenarios such as a stadium, you are advised to set the CCA threshold to -75 dBm. In other scenarios, you are advised to retain the default value or set this parameter under the guidance of technical support personnel.

Precautions

The anti-interference algorithm dynamically adjusts the CCA and AGC thresholds of APs. If the CCA or AGC threshold is manually configured when the anti-interference algorithm is enabled, the manually configured threshold takes effect.

Example

Set the CCA threshold for a 2G radio to -70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] cca-threshold -70
Warning:  This parameter will affect the uplink access coverage or user access.
It is recommended that the configuration be modified under the guidance of profe
ssional technical personnel. The manually configured CCA threshold takes precede
nce over the anti-interference algorithm. If the anti-interference function is e
nabled, dynamic CCA adjustment does not take effect and the manually configured
CCA threshold takes effect. Continue? [Y/N]:y
```

11.4.42 co-sr disable

Function

The **co-sr disable** command disables the Coordinated Spatial Reuse (CoSR) function.

The **undo co-sr disable** command enables the CoSR function.

By default, the CoSR function is enabled.

Format

co-sr disable

undo co-sr disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

On a high-density office network, you can run the **undo co-sr disable** command to enable the CoSR function to improve the overall network throughput.

The CoSR function is supported only by AirEngine X760 series APs.

Example

Disable the CoSR function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] co-sr disable
```

11.4.43 dca-channel bandwidth

Function

The **dca-channel bandwidth** command configures the calibration bandwidth.

The **undo dca-channel bandwidth** command restores the default calibration bandwidth.

By default, the calibration bandwidth value is **auto**.

Format

dca-channel 5g bandwidth { **20mhz** | **40mhz** | **80mhz** | **auto** }

dca-channel 6g bandwidth { **20mhz** | **40mhz** | **80mhz** | **160mhz** | **320mhz** | **auto** }

undo dca-channel 5g bandwidth

undo dca-channel 6g bandwidth

Parameters

Parameter	Description	Value
5g	Specifies the 5 GHz frequency band on which radio calibration is implemented.	-
6g	Specifies the 6 GHz frequency band on which radio calibration is implemented.	-

Parameter	Description	Value
20mhz | **40mhz** | **80mhz** | **160mhz** | **320mhz** | **auto**	Specifies the calibration bandwidth. If **auto** is specified and the number of channels supported by the country code is greater than or equal to 6, the device uses 40 MHz bandwidth on the 5 GHz frequency band and 80 MHz bandwidth on the 6 GHz frequency band by default during radio calibration. This achieves larger calibration bandwidth without manual configuration. If the number of available channels is less than 6, the device decreases the calibration bandwidth (from 80 MHz to 40 MHz and to 20 MHz) on the corresponding frequency band until the number of available channels is greater than or equal to 6 or the calibration bandwidth is reduced to 20 MHz.	-

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Richer spectrum resources are available on the 5 GHz and 6 GHz frequency bands, enabling APs to work on 40 MHz or larger-bandwidth channels in addition to 20 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

You can use the **dca-channel bandwidth** command to configure the calibration bandwidth and the **dca-channel channel-set** command to configure calibration channels as prompted.

Configuration Impact

When the calibration bandwidth is changed, the device recalculates the calibration channels.

Precautions

When configuring 40 MHz or larger calibration bandwidth, check whether channels of the corresponding bandwidth exist under the country code.

Example

Set the calibration bandwidth of 5 GHz radios to 40 MHz.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name default
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g bandwidth 40mhz
```

11.4.44 dca-channel channel-set

Function

The **dca-channel channel-set** command configures a calibration channel set.

The **undo dca-channel channel-set** command restores the default calibration channel set.

By default, a calibration channel set contains channels 1, 6, and 11 on 2.4 GHz radios and contains all channels supported by the corresponding country code on 5 GHz and 6 GHz radios. When configuring a calibration channel set, you can specify channels as prompted.

Format

dca-channel { **2.4g** | **5g** | **6g** } **channel-set** *channel-value*

undo dca-channel { **2.4g** | **5g** | **6g** } **channel-set**

Parameters

Parameter	Description	Value
2.4g | **5g** | **6g**	Specifies the frequency band on which radio calibration is performed. The options are as follows: • **2.4g**: Radios work on the 2.4 GHz frequency band. • **5g**: Radios work on the 5 GHz frequency band. • **6g**: Radios work on the 6 GHz frequency band.	-

Parameter	Description	Value
channel-set *channel-value*	Specifies a calibration channel set.	The value is a character string. You can select calibration channels as prompted. If you select multiple channels, use commas (,) to separate channel names.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Richer spectrum resources are available on the 5 GHz and 6 GHz frequency bands, enabling APs to work on 40 MHz or larger-bandwidth channels in addition to 20 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

You can run this command to specify a calibration channel set for an AP. The AP selects channels from the channel set to calibrate. This reduces the burden on the AP.

NOTE

To ensure a good calibration effect, you are advised to configure at least three calibration channels.

To prevent signal interference, ensure that adjacent APs work in non-overlapping channels. The 2.4 GHz frequency band has overlapping channels. When configuring calibration channels, you are advised to configure a non-overlapping calibration channel set containing channels 1, 6, and 11 or containing channels 1, 5, 9, and 13.

To specify a 40 MHz calibration channel, you need to specify two consecutive 20 MHz channels. To specify an 80 MHz calibration channel, you need to specify four consecutive 20 MHz channels. The combinations of 20 MHz channels making up the 40 MHz and 80 MHz channels are fixed.

You can also use the **dca-channel bandwidth** command to configure the calibration bandwidth and the **dca-channel channel-set** command to configure calibration channels as prompted.

If no calibration channel set is configured, the device probes channels based on the calibration channels corresponding to the country code.

NOTE

When configuring a calibration channel set, avoid using radar channels.

The configured channels must be supported by STAs; otherwise, the STAs cannot discover radio signals.

Channels 184, 188, 192, and 196 on the 4.9 GHz frequency band can be used for radio scanning but cannot be used for channel calibration.

If the AP has three 5 GHz radios, configure at least five calibration channels. If the AP has two 5 GHz radios, configure at least three calibration channels.

Example

Configure a calibration channel set composed of 40 MHz channels 149, 153, 157, and 161 on the 5 GHz frequency band.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name default
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g bandwidth 40mhz
[HUAWEI-wlan-regulate-domain-default] dca-channel 5g channel-set 149,153,157,161
```

11.4.45 deauth-fail-times

Function

The **deauth-fail-times** command sets the maximum number of attempts to steer STAs in deauthentication mode.

The **undo deauth-fail-times** command restores the default maximum number of attempts to steer STAs in deauthentication mode.

By default, the maximum number of attempts to steer STAs in deauthentication mode is 0.

Format

deauth-fail-times *deauth-fail-times*

undo deauth-fail-times

Parameters

Parameter	Description	Value
deauth-fail-times	Specifies the maximum number of attempts to steer STAs in deauthentication mode.	The value is an integer that ranges from 0 to 5. The value 0 indicates that the deauthentication mode is not used to steer STAs.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device attempts to use the 802.11v and deauthentication modes to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in deauthentication mode after multiple attempts. You can run the **deauth-fail-times** command to set the maximum number of attempts to steer STAs in deauthentication mode. If the number of attempts exceeds the specified value, STAs cannot be steered.

Precautions

You are advised to retain the default value. If the success rate of STA steering in deauthentication mode is low or STA services are affected, set the parameter value to 0 to disable STA steering in deauthentication mode.

Example

Set the maximum number of attempts to steer STAs in deauthentication mode to 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] deauth-fail-times 1
```

11.4.46 dfs radar-filter sensitivity

Function

The **dfs radar-filter sensitivity** command sets the sensitivity level of correction for false DFS radar detection.

The **undo dfs radar-filter sensitivity** command restores the default sensitivity level of correction for false DFS radar detection.

By default, the sensitivity level of correction for false DFS radar detection is 0.

Format

dfs radar-filter sensitivity *level*

undo dfs radar-filter sensitivity

Parameters

Parameter	Description	Value
level	Specifies the sensitivity level of correction for false DFS radar detection.	The value is an integer that ranges from 0 to 10. - Level 0: The sensitivity of correction for false DFS radar detection is moderate. - Levels 1 to 9: A larger value indicates that correction for false DFS radar detection is more sensitive. That is, DFS radar detection is less sensitive and radar signals are less likely to be detected. - Level 10: DFS radar detection is disabled.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In most cases, you are advised to retain the default sensitivity level of correction for false DFS radar detection However, some APs may frequently detect radar signals by mistake. To prevent unnecessary channel switching, you can run the **dfs radar-filter sensitivity** command to adjust the sensitivity level as required to reduce false radar detection.

If radar signals are often falsely detected, you are advised to set the sensitivity level to 5 and then adjust the value properly based on the false radar detection events. For example, if an AP often falsely detects radar signals, the sensitivity level for radar detection is high. In this case, set the sensitivity level to 5 and continuously observe the false radar detection events. If false radar detection events persist, gradually increase the sensitivity level.

Example

Set the sensitivity level of correction for false DFS radar detection to 9 in the 5G radio profile **test1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name test1
[HUAWEI-wlan-radio-5g-prof-test1] dfs radar-filter sensitivity 9
```

11.4.47 dfs recover-delay

Function

The **dfs recover-delay** command sets the delay in switching back the DFS channel.

The **undo dfs recover-delay** command restores the default delay in switching back the DFS channel.

By default, the delay in switching back the DFS channel is 0 minutes. That is, the channel is switched back to the manually planned channel when the legitimate aging time (30 minutes) expires.

Format

dfs recover-delay *delay-time*

undo dfs recover-delay

Parameters

Parameter	Description	Value
delay-time	Specifies a delay in switching back the DFS channel.	The value is an integer that ranges from 0 to 2880, in minutes.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

For an AP operating on a manually planned channel, it randomly selects a channel (calibration channel preferred) within the range defined by the country code after detecting radar signals. The AP channel will be switched back to the manually planned channel after the configured switchback delay and legitimate aging time (30 minutes). A proper delay in switching back the DFS channel will prevent frequent channel switchovers.

Example

Set the delay in switching back the DFS channel to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dfs recover-delay 10
```

11.4.48 dfs smart-selection disable

Function

The **dfs smart-selection disable** command disables the DFS smart selection function.

The **undo dfs smart-selection disable** command enables the DFS smart selection function.

By default, the DFS smart selection function is enabled.

Format

dfs smart-selection disable

undo dfs smart-selection disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DFS smart selection function is enabled, an AP working on the 5 GHz band detects radar signals. Upon detecting radar channels, the AP automatically switches to another channel to prevent radar interference.

When an AP switches its working channel upon detecting radar signals, it randomly selects a channel (the calibration channel preferentially) allowed by the country code. The selected channel may be the same as or adjacent to the working channel of surrounding 5 GHz radios, thereby causing severe interference and poor network access experience. By default, the DFS smart selection function is enabled so that the AP switches to a 5 GHz channel with the minimum interference, preventing interference.

After the **dfs smart-selection disable** command is executed, the DFS smart selection function is disabled, affecting user experience. Configure this function as required.

Precautions

The DFS smart selection function is valid only when the air scan is enabled.

Example

Disable DFS smart selection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dfs smart-selection disable
Info: This function does not take effect when air scan is disabled.
```

11.4.49 display air-scan-profile

Function

The **display air-scan-profile** command displays information about air scan profiles.

Format

display air-scan-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all air scan profiles.	-
name *profile-name*	Displays information about a specified air scan profile.	The air scan profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display air-scan-profile** command to view information about air scan profiles.

Example

Display information about all air scan profiles.

```
<HUAWEI> display air-scan-profile all
------------------------------------------------------------
Profile name        Reference
------------------------------------------------------------
default            2
test               1
------------------------------------------------------------
Total: 2
```

Table 11-132 Description of the **display air-scan-profile all** command output

Item	Description
Profile name	Name of an air scan profile.

Item	Description
Reference	Number of times that the air scan profile is referenced.

Display information about the air scan profile **test**.

```
<HUAWEI> display air-scan-profile name test
------------------------------------------------------------
Scan switch        : enable
Scan period(ms)    : 80
Scan interval(ms) : 3000
Scan channel-set  : dca-channel
Scan enhancement  : enable
------------------------------------------------------------
```

Table 11-133 Description of the **display air-scan-profile name** command output

Item	Description
Scan switch	Whether air scanning is enabled. To configure the parameter, run the **scan-disable** command.
Scan period(ms)	Air scan period. To set the air scan period, run the **scan-period** command.
Scan interval(ms)	Air scan interval. To set the air scan interval, run the **scan-interval** command.
Scan channel-set	Air scan channel set. To set the air scan channel set, run the **scan-channel-set** command.
Scan enhancement	Whether the scanning enhancement function is enabled. To configure the scanning enhancement function, run the **scan-enhancement** command.

11.4.50 display anti-interference config

Function

The **display anti-interference config** command displays the configuration of the anti-interference algorithm.

Format

display anti-interference config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display anti-interference config** command displays the configuration of the anti-interference algorithm.

Example

Display the configuration of the anti-interference algorithm.

```
<HUAWEI> display anti-interference config
------------------------------------------
Anti-interference switch       : enable
Per-packet-TPC switch          : enable
AGC check switch               : enable
Dynamic CCA upper threshold    : -70
Dynamic CCA lower threshold    : -82
Edge STA SNR threshold         : 22
Edge STA RSSI threshold        : -70
------------------------------------------
```

Table 11-134 Description of the **display anti-interference config** command output

Item	Description
Anti-interference switch	Whether the anti-interference algorithm is enabled. To configure this parameter, run the **anti-interference disable** command.
Per-packet-TPC switch	Whether the packet-based power adjustment function is enabled. To configure this parameter, run the **anti-interference per-packet-tpc disable** command.

Item	Description
AGC check switch	Whether the AGC algorithm before packet transmission is enabled. To configure this parameter, run the **anti-interference agc-check disable** command.
Dynamic CCA upper threshold	Upper dynamic CCA threshold.
Dynamic CCA lower threshold	Lower dynamic CCA threshold.
Edge STA SNR threshold	Threshold for determining an edge STA based on the SNR.
Edge STA RSSI threshold	Threshold for determining an edge STA based on the RSSI.

11.4.51 display flexible-radio status

Function

The **display flexible-radio status** command displays the status and switching result of the redundant radio.

Format

display flexible-radio status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display flexible-radio status** command to check the status and switching result of the redundant radio.

Example

Display the status and switching result of the redundant radio.

```
<HUAWEI> display flexible-radio status
Redundancy Results:
R: The current radio is a redundant radio that has not been switched
```

```
S(5G): The redundant radio is switched to the 5 GHz mode
S(monitor): The redundant radio is switched to the monitor mode
S(off): This redundant radio is disabled
-: This radio is not a redundant radio
Recognize time: 2019-06-11/16:59:52 DST
------------------------------------------------------------
AP ID  Name           RfID  Band ST  Redundancy Result
------------------------------------------------------------
2      00e0-fc12-3455  0    2.4G on  R
3      00e0-fc12-3456  0    2.4G on  S(5G)
------------------------------------------------------------
Total:4
```

Table 11-135 Description of the **display flexible-radio status** command output

Item	Description
Recognize time	Time when the redundant radio is identified. **DST** indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
AP ID	AP ID.
Name	AP name.
RfID	Radio ID.
Band	Frequency band of the radio.
ST	Radio status.
Redundancy Result	Switching result of the redundant radio. ● R: The current radio is a redundant radio that has not been switched. ● S(5G): The redundant radio is switched to the 5 GHz mode. ● S(monitor): The redundant radio is switched to the monitor mode. ● S(off): This redundant radio is disabled. ● -: This radio is not a redundant radio.

11.4.52 display flexible-radio switch-record

Function

The **display flexible-radio switch-record** command displays the switching record of the redundant radio.

Format

display flexible-radio switch-record [**detail**]

Parameters

Parameter	Description	Value
detail	Displays the detailed switching record of the redundant radio.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display flexible-radio switch-record** command to check the switching record of the redundant radio.

Example

Display the switching record of the redundant radio.

```
<HUAWEI> display flexible-radio switch-record
------------------------------------------------------------
Time                    ApID  Name          RfID  Switch
------------------------------------------------------------
2019-06-10/20:45:58 DST   5     00e0-fc12-3456  0     monitor
------------------------------------------------------------
Total : 1
```

Display the detailed switching record of the redundant radio.

```
<HUAWEI> display flexible-radio switch-record detail
------------------------------------------------------------------------------------------------------------------------------------
---------
Time                    ApID  Name          RfID  Switch   ReferenceRadio(ApID/ApName/PL)
------------------------------------------------------------------------------------------------------------------------------------
---------
2019-06-10/20:45:58 DST   5     00e0-fc12-3456  0     monitor  (0   /00e0-fc12-c220/52  ),(6   /00e0-fc12-
f7c0/40  ),(2   /00e0-fc7a-f9e0/52  )
------------------------------------------------------------------------------------------------------------------------------------
---------
Total : 1
```

Table 11-136 Description of the **display flexible-radio switch-record detail** command output

Item	Description
Time	Time when the redundant radio is switched. **DST** indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
ApID	AP ID.
Name	AP name.
RfID	Radio ID.
Switch	Switching result of the redundant radio. ● 5G: The redundant radio is switched to the 5 GHz mode. ● 2.4G: The redundant radio is switched back to the 2.4 GHz mode. ● monitor: The redundant radio is switched to the monitor mode. ● normal: The redundant radio is switched back to the normal mode. ● off: This redundant radio is disabled. ● on: This redundant radio is enabled.
ReferenceRadio(ApID/ApName/PL)	Top 3 neighbors of the redundant radio (AP ID/AP name/path loss).

11.4.53 display interference-visualization configuration

Function

The **display interference-visualization configuration** command displays information about AP radios on which interference visualization is enabled.

NOTE

Interference visualization is not available for the following models:

- AirEngine x761
- AirEngine x762

Format

display interference-visualization configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about AP radios on which interference visualization is enabled.

```
<HUAWEI> display interference-visualization configuration
-------------------------------------------------------------------------------------------------
ID AP name Radio ID
-------------------------------------------------------------------------------------------------
0  ap0     0
0  ap0     1
-------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-137 Description of the **display interference-visualization configuration** command output

Item	Description
ID	AP ID.
AP name	AP name.
Radio ID	Radio ID.

11.4.54 display references air-scan-profile

Function

The **display references air-scan-profile** command displays reference information about an air scan profile.

Format

display references air-scan-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified air scan profile.	The air scan profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references air-scan-profile** command to view reference information about an air scan profile.

Example

Display reference information about the air scan profile **test**.

```
<HUAWEI> display references air-scan-profile name test
------------------------------------------------------------
Reference type                Reference name
------------------------------------------------------------
radio-2g-profile              default
------------------------------------------------------------
Total: 1
```

Table 11-138 Description of the **display references air-scan-profile** command output

Item	Description
Reference type	Type of the profile that references the air scan profile.
Reference name	Name of the profile that references the air scan profile.

11.4.55 display references rrm-profile

Function

The **display references rrm-profile** command displays reference information about an RRM profile.

Format

display references rrm-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified RRM profile.	The RRM profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references rrm-profile** command to view reference information about an RRM profile.

Example

Display reference information about the RRM profile **default**

```
<HUAWEI> display references rrm-profile name default
------------------------------------------------------------
Reference type           Reference name
------------------------------------------------------------
radio-2g-profile         radio0
radio-5g-profile         radio1
------------------------------------------------------------
Total: 2
```

Table 11-139 Description of the **display references rrm-profile** command output

Item	Description
Reference type	Type of the profile that references the RRM profile.
Reference name	Name of the profile that references the RRM profile.

11.4.56 display references scene

Function

The **display references scene** command displays reference information about a scenario profile.

Format

display references scene name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified scenario profile.	The value is of the enumerated type. - multi-partition-cross-room: indicates an indoor multi-partition cross-room deployment scenario (capacity first). - multi-partition-cross-room-cov: indicates an indoor multi-partition cross-room deployment scenario (coverage first). - automated-guided-vehicle: indicates an AGV scenario. - high-density-stadium: indicates a high-density stadium scenario. - indoor-high-density: indicates an indoor high-density coverage scenario. - indoor-low-density: indicates an indoor low-density coverage scenario. - indoor-multi-partition: indicates an indoor multi-partition coverage scenario.

Parameter	Description	Value
		- indoor-normal-density: indicates an indoor common coverage scenario. - industrial-manufacturing: indicates an industrial manufacturing scenario. - outdoor-continuous: indicates an outdoor continuous coverage scenario. - virtual-reality: indicates a VR scenario.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about a scenario profile.

Example

Display reference information about the scenario profile **multi-partition-cross-room**.

```
<HUAWEI> display references scene name multi-partition-cross-room
------------------------------------------------------------------------------------------
Reference type               Reference name
------------------------------------------------------------------------------------------
AP group                   11
AP ID                    0
------------------------------------------------------------------------------------------
Total: 2
```

Table 11-140 Description of the **display references scene** command output

Item	Description
Reference type	Type of the entity that references a scenario profile. The type can be AP group or AP.
Reference name	Name of the entity that references a scenario profile. The name can be an AP group name or AP ID.

11.4.57 display rrm-profile

Function

The **display rrm-profile** command displays information about RRM profiles.

Format

display rrm-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all RRM profiles.	-
name *profile-name*	Displays information about a specified RRM profile.	The RRM profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rrm-profile** command to view information about RRM profiles.

Example

Display information about all RRM profiles.

```
<HUAWEI> display rrm-profile all
--------------------------------------------------------------
```

```
Profile name  Reference
------------------------------------------------------------
default       2
------------------------------------------------------------
Total:1
```

Table 11-141 Description of the **display rrm-profile all** command output

Item	Description
Profile name	Name of an RRM profile.
Reference	Number of times an RRM profile is referenced.

Display information about the RRM profile **default**.

```
<HUAWEI> display rrm-profile name default
--------------------------------------------------------------------
Retransmission rate threshold for trigger channel/power select(%)  : 55
Noise-floor threshold for trigger channel/power select(dBm)  : -75
Calibrate tpc threshold(dBm):                           : -60
Maximum 2.4G calibration TX power(dBm)                    : 127
Maximum 5G calibration TX power(dBm)                      : 127
Maximum 6G calibration TX power(dBm)                      : 127
Minimum 2.4G calibration TX power(dBm)                    : 9
Minimum 5G calibration TX power(dBm)                      : 12
Minimum 6G calibration TX power(dBm)                      : 12
Calibrate retransmission rate check interval(min)           : 1
Calibrate retransmission rate check traffic threshold(kbps)  : 1250
Calibrate grouping interference threshold(dBm)              : -127
Airtime fairness schedule                               : disable
Dynamic adjust EDCA parameter                             : disable
Dynamic EDCA be-service threshold                         : 6
UAC check client's SNR                                  : disable
UAC client's SNR threshold(dB)                            : 20
UAC check client number                                  : disable
UAC client number access threshold                         : 64
UAC client number roam threshold                           : 64
Action upon reaching the UAC threshold                      : SSID broadcast
Band steer deny threshold                                : 0
Band steer SNR threshold(dB)                              : 20
Band balance start threshold                              : 100
Band balance gap threshold(%)                              : 20
Client's band expire based on continuous probe counts        : 35
Station load balance                                    : disable
Station load balance mode                                 : sta-number
Station load balance RSSI threshold(dBm)                     : -70
Station load balance RSSI-diff-gap threshold(dBm)            : 20
Station load balance sta-number start threshold              : 10
Station load balance sta-number gap threshold(percentage)    : 20
Station load balance sta-number gap threshold(number)        : -
Station load balance deauth fail times                      : 2
Station load balance BTM fail times                         : 5
Station load balance steer-restrict restrict time(s)          : 5
Station load balance steer-restrict probe threshold           : 5
Station load balance steer-restrict auth  threshold           : 0
Station load balance probe-report interval(s)                : 30
BSS color switch                                       : enable
Spatial reuse switch                                    : enable
Smart-roam                                             : enable
Smart-roam AI mode                                      : disable
Smart-roam quick kickoff                                 : enable
Smart-roam check SNR                                    : enable
Smart-roam quick kickoff check SNR                          : enable
```

```
Smart-roam check rate                                   : disable
Smart-roam quick kickoff check rate                     : disable
Smart-roam standing SNR threshold(dB)                   : 20
Smart-roam SNR quick-kickoff-threshold(dB)              : 15
Smart-roam rate threshold(%)                            : 20
Smart-roam rate quick-kickoff-threshold(%)              : 20
Smart-roam high level SNR margin(dB)                    : 15
Smart-roam low level SNR margin(dB)                     : 6
Smart-roam SNR check interval(s)                        : 3
Smart-roam unable roam client expire time(min)          : 120
Smart-roam quick-kickoff SNR check interval(ms)         : 500
Smart-roam quick-kickoff SNR P-N observe time           : 6
Smart-roam quick-kickoff SNR P-N qualify time           : 4
Smart-roam advanced scan                                : enable
Smart-roam quick-kickoff back off time                  : 60
AMC policy                                              : auto-balance
High density AMC optimize                               : disable
Antenna-mode                                            : omnidirection
SFN roam check high threshold(dBm)                      : -55
SFN roam check low threshold(dBm)                       : -60
SFN roam check interval(ms)                             : 700
SFN roam report interval(ms)                            : 400
SFN roam check rssi-accumulate threshold(dB)            : 8
SFN roam check sta-holding times                        : 3
SFN roam check gap-rssi(dB)                             : 6
SFN roam check better-times                             : 2
DFS smart select                                        : enable
DFS recover delay time(min)                             : 0
Multimedia air optimize
  Switch                                                : disable
  Voice threshold                                       : 30
  Video threshold                                       : 100
  Voice downlink-slice-ratio                            : medium
  Video downlink-slice-ratio                            : medium
  Voice downlink-delay-guarantee                        : medium
  Video downlink-delay-guarantee                        : medium
  Best effort downlink-delay-guarantee                  : medium
  Background downlink-delay-guarantee                   : medium
  Congestion-control tcp-window-tuning switch           : enable
  Uplink-delay-guarantee                                : enable
Rate limit dynamic interval                             : 5
Rate limit dynamic threshold                            : 80
CO-SR                                                   : enable
Wlan-slice high-reliability
  Switch                                                : disable
  rtt                                                   : 20
  time-ratio                                            : 80
  FRER-enhance                                          : disable
----------------------------------------------------------------------
```

Table 11-142 Description of the **display rrm-profile name** command output

Item	Description
Retransmission rate threshold for trigger channel/power select(%)	Retransmission rate threshold for triggering channel or power adjustment. To configure this parameter, run the **calibrate retransmission-rate-threshold** command.

Item	Description
Noise-floor threshold for trigger channel/power select(dBm)	Noise-floor threshold for triggering channel or power adjustment. To configure this parameter, run the **calibrate noise-floor-threshold** command.
Calibrate tpc threshold(dBm)	Transmit Power Control (TPC) coverage threshold. To configure this parameter, run the **calibrate tpc threshold** command.
Maximum 2.4G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power** command.
Maximum 5G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power radio-5g** command.
Maximum 6G calibration TX power(dBm)	Maximum transmit power that can be adjusted through 6 GHz radio calibration. To configure this parameter, run the **calibrate max-tx-power radio-6g** command.
Minimum 2.4G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 2.4 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power** command.
Minimum 5G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 5 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power radio-5g** command.
Minimum 6G calibration TX power(dBm)	Minimum transmit power that can be adjusted through 6 GHz radio calibration. To configure this parameter, run the **calibrate min-tx-power radio-6g** command.

Item	Description
Calibrate retransmission rate check interval(min)	Interval for checking the retransmission rate. To configure this parameter, run the **calibrate retransmission-rate-check** command.
Calibrate retransmission rate check traffic threshold(kbps)	Traffic threshold for checking the retransmission rate. To configure this parameter, run the **calibrate retransmission-rate-check** command.
Calibrate grouping interference threshold(dBm)	RSSI interference threshold of a calibration group. To configure this parameter, run the **calibrate grouping interference-threshold** command.
Airtime fairness schedule	Whether airtime fair scheduling is enabled. To configure this parameter, run the **airtime-fair-schedule enable** command.
Dynamic adjust EDCA parameter	Whether dynamic EDCA parameter adjustment is enabled. To configure this parameter, run the **dynamic-edca enable** command.
Dynamic EDCA be-service threshold	Threshold for the dynamic EDCA Best-Effort service. To configure this parameter, run the **dynamic-edca threshold** command.
UAC check client's SNR	Whether user CAC based on the STA's SNR is enabled. To configure this parameter, run the **uac enable** command.
UAC client's SNR threshold(dB)	User CAC SNR threshold. To configure this parameter, run the **uac client-snr threshold** command.
UAC check client number	Whether user CAC based on the number of users is enabled. To configure this parameter, run the **uac enable** command.

Item	Description
UAC client number access threshold	User CAC access threshold based on the number of users. To configure this parameter, run the **uac client-number threshold** command.
UAC client number roam threshold	User CAC roaming threshold based on the number of users. To configure this parameter, run the **uac client-number threshold** command.
Action upon reaching the UAC threshold	Action to take when the number of access users reaches the user CAC threshold. ● SSID hide: hiding the SSID ● SSID broadcast: broadcasting the SSID ● priority-based STA replacement: allowing access of VIP users instead of non-VIP users based on priorities To configure this parameter, run the **uac reach-access-threshold** command.
Band steer deny threshold	Maximum number of times an AP rejects association requests of a STA for band steering. To configure this parameter, run the **band-steer deny-threshold** command.
Band steer SNR threshold(dB)	Start SNR threshold for triggering 5G-prior access. To configure this parameter, run the **band-steer snr-threshold** command.
Band balance start threshold	Start threshold for load balancing between radios. To configure this parameter, run the **band-steer balance start-threshold** command.
Band balance gap threshold(%)	Load difference threshold for load balancing between radios. To configure this parameter, run the **band-steer balance gap-threshold** command.

Item	Description
Client's band expire based on continuous probe counts	Aging condition of terminal band information, that is, the number of times that an AP has continuously received Probe frames of a terminal from the same frequency band. To configure this parameter, run the **band-steer client-band-expire** command.
Station load balance	Whether the load balancing function is enabled. To configure this parameter, run the **sta-load-balance dynamic disable** command.
Station load balance mode	Dynamic load balancing mode. sta-number: dynamic load balancing based on the number of STAs.
Station load balance RSSI threshold(dBm)	RSSI threshold of members in a dynamic load balancing group. To configure this parameter, run the **sta-load-balance dynamic rssi-threshold** command.
Station load balance RSSI-diff-gap threshold(dBm)	RSSI difference threshold for members in a dynamic load balancing group. To configure this parameter, run the **sta-load-balance dynamic rssi-diff-gap** command.
Station load balance sta-number start threshold	Start threshold for dynamic load balancing based on the number of users. To configure this parameter, run the **sta-load-balance dynamic sta-number start-threshold** command.
Station load balance sta-number gap threshold(percentage)	Load difference threshold for dynamic load balancing based on the percentage of users. To configure this parameter, run the **sta-load-balance dynamic sta-number gap-threshold** command.

Item	Description
Station load balance sta-number gap threshold(number)	Load difference threshold for dynamic load balancing based on the number of users. To configure this parameter, run the **sta-load-balance dynamic sta-number gap-threshold** command.
Station load balance deauth fail times	Maximum number of attempts to steer STAs in deauthentication mode. To configure this parameter, run the **sta-load-balance dynamic deauth-fail-times** command.
Station load balance BTM fail times	Maximum number of attempts to steer STAs in BTM mode. To configure this parameter, run the **sta-load-balance dynamic btm-fail-times** command.
Station load balance steer-restrict restrict time(s)	Duration within which non-target APs suppress association of STAs during STA steering. To configure this parameter, run the **sta-load-balance dynamic steer-restrict restrict-time** command.
Station load balance steer-restrict probe threshold	Maximum number of times non-target APs perform probe suppression for STAs during STA steering. To configure this parameter, run the **sta-load-balance dynamic steer-restrict probe-threshold** command.
Station load balance steer-restrict auth threshold	Maximum number of times non-target APs suppress authentication of STAs during STA steering. To configure this parameter, run the **sta-load-balance dynamic steer-restrict auth-threshold** command.
Station load balance probe-report interval(s)	Interval for reporting Probe frames. To configure this parameter, run the **sta-load-balance dynamic probe-report interval** command.
BSS color switch	Whether the BSS coloring function is enabled. To configure this parameter, run the **bss-color disable** command.

Item	Description
Spatial reuse switch	Whether the spatial reuse (SR) function is enabled. To configure this parameter, run the **spatial-reuse disable** command.
Smart-roam	Whether smart roaming is enabled. To configure this parameter, run the **smart-roam { enable | disable }** command.
Smart-roam AI mode	Whether the AI roaming function is enabled. To configure this parameter, run the **smart-roam ai-mode** command.
Smart-roam quick kickoff	Whether the function of quickly disconnecting STAs is enabled. To configure this parameter, run the **smart-roam quick-kickoff-threshold disable** command.
Smart-roam check SNR	Whether the trigger mode of smart roaming is specified as **check SNR**. To configure this parameter, run the **smart-roam roam-threshold { check-snr | check-rate }** command.
Smart-roam quick kickoff check SNR	Whether the function of quickly disconnecting STAs is triggered by checking the SNR of STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.
Smart-roam check rate	Whether the trigger mode of smart roaming is specified as **check rate**. To configure this parameter, run the **smart-roam roam-threshold { check-snr | check-rate }** command.
Smart-roam quick kickoff check rate	Whether the function of quickly disconnecting STAs is triggered by checking the rate of STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.

Item	Description
Smart-roam standing SNR threshold(dB)	SNR threshold for smart roaming. To configure this parameter, run the **smart-roam roam-threshold { snr | rate }** command.
Smart-roam SNR quick-kickoff-threshold(dB)	SNR threshold for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold** command.
Smart-roam rate threshold(%)	Rate threshold for smart roaming. To configure this parameter, run the **smart-roam roam-threshold { snr | rate }** command.
Smart-roam rate quick-kickoff-threshold(%)	Rate threshold for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff-threshold** command.
Smart-roam high level SNR margin(dB)	Higher SNR difference threshold that triggers STA roaming. To configure this parameter, run the **smart-roam snr-margin** command.
Smart-roam low level SNR margin(dB)	Lower SNR difference threshold that triggers STA roaming. To configure this parameter, run the **smart-roam snr-margin** command.
Smart-roam SNR check interval(s)	Interval for checking the SNR of STAs.
Smart-roam unable roam client expire time(min)	Aging time of "unable to roam" record. To configure this parameter, run the **smart-roam unable-roam-client expire-time** command.
Smart-roam quick-kickoff SNR check interval(ms)	Interval for checking the SNR to determine whether to quickly disconnect STAs. To configure this parameter, run the **smart-roam quick-kickoff-snr check-interval** command.

Item	Description
Smart-roam quick-kickoff SNR P-N observe time	Number of PN observation times to determine whether to quickly disconnect STAs. To configure this parameter, run the **smart-roam quick-kickoff-snr p-n criteria** command.
Smart-roam quick-kickoff SNR P-N qualify time	Number of PN observation times to determine whether to quickly disconnect STAs. To configure this parameter, run the **smart-roam quick-kickoff-snr p-n criteria** command.
Smart-roam advanced scan	Whether coordinated scanning function of smart roaming is enabled. To configure this parameter, run the **smart-roam advanced-scan disable** command.
Smart-roam quick-kickoff back off time	Backoff time for quickly disconnecting STAs. To configure this parameter, run the **smart-roam quick-kickoff back-off-time** command.
AMC policy	Adaptive modulation and coding (AMC) algorithm. To configure this parameter, run the **amc-policy** command.
High density AMC optimize	Whether the AMC optimization function in high-density scenarios is enabled. To configure this parameter, run the **high-density amc-optimize enable** command.
Antenna-mode	Antenna mode. To configure this parameter, run the **antenna-mode** command.
SFN roam check high threshold(dBm)	Upper RSSI threshold for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check high-threshold** command.

Item	Description
SFN roam check low threshold(dBm)	Lower RSSI threshold for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check low-threshold** command.
SFN roam check interval(ms)	Decision period for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check check-interval** command.
SFN roam report interval(ms)	Interval for RUs to report the STA RSSI. To configure this parameter, run the **sfn-roam report-interval** command.
SFN roam check rssi-accumulate threshold(dB)	Cumulative RSSI change threshold for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check rssi-accumulate** command.
SFN roam check sta-holding times	Number of STA holding times for agile distributed SFN roaming. To configure this parameter, run the **sfn-roam roam-check sta-holding times** command.
SFN roam check gap-rssi(dB)	RSSI gap for agile distributed SFN roaming RUs. To configure this parameter, run the **sfn-roam roam-check gap-rssi** command.
SFN roam check better-times	Number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU. To configure this parameter, run the **sfn-roam roam-check better-times** command.

Item	Description
DFS smart select	Whether DFS smart selection is enabled. ● enable: DFS smart selection is enabled. ● disable: DFS smart selection is disabled. To configure this parameter, run the **dfs smart-selection disable** command.
DFS recover delay time(min)	Delay in switching back the DFS channel. To configure this parameter, run the **dfs recover-delay** command.
Switch	Whether the intelligent multimedia scheduling algorithm is enabled. ● disable: The intelligent multimedia scheduling algorithm is disabled. ● enable: The intelligent multimedia scheduling algorithm is enabled. To configure this parameter, run the **multimedia-air-optimize disable** command.
Voice threshold	Voice packet threshold. To configure this parameter, run the **multimedia-air-optimize threshold** command.
Video threshold	Video packet threshold. To configure this parameter, run the **multimedia-air-optimize threshold** command.
Voice downlink-slice-ratio	Slicing ratio for voice packets. To configure this parameter, run the **multimedia-air-optimize downlink-slice-ratio** command.
Video downlink-slice-ratio	Slicing ratio for video packets. To configure this parameter, run the **multimedia-air-optimize downlink-slice-ratio** command.
Voice downlink-delay-guarantee	Guaranteed delay for voice packets. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.

Item	Description
Video downlink-delay-guarantee	Guaranteed delay for video packets. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.
Best effort downlink-delay-guarantee	Guaranteed delay for BE flows. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.
Background downlink-delay-guarantee	Guaranteed delay for BK flows. To configure this parameter, run the **multimedia-air-optimize downlink-delay-guarantee** command.
Congestion-control tcp-window-tuning switch	Whether the TCP window adjustment function for voice and video services is enabled. ● disable: The TCP window adjustment function for voice and video services is disabled. ● enable: The TCP window adjustment function for voice and video services is enabled. To configure this parameter, run the **multimedia-air-optimize congestion-control tcp-window-tuning disable** command.
Uplink-delay-guarantee	Whether the delay guarantee function for uplink services is enabled. ● disable: The function is disabled. ● enable: The function is enabled. To configure this parameter, run the **multimedia-air-optimize uplink-delay-guarantee disable** command.
Rate limit dynamic interval	Detection interval for dynamic rate limiting. To configure this parameter, run the **rate-limit dynamic interval** command.
Rate limit dynamic threshold	Detection threshold for dynamic rate limiting. To configure this parameter, run the **rate-limit dynamic interval** command.

Item	Description
CO-SR	Whether the CoSR function is enabled. - disable: The function is disabled. - enable: The function is enabled. To configure this parameter, run the **co-sr disable** command.
Switch	Whether the WLAN high-reliability slicing function is enabled. To configure this parameter, run the **wlan-slice high-reliability enable** command.
rtt	Expected RTT of WLAN high-reliability slicing. To configure this parameter, run the **wlan-slice high-reliability rtt** command.
time-ratio	Time proportion of WLAN high-reliability slicing. To configure this parameter, run the **wlan-slice high-reliability time-ratio** command.
FRER-enhance	Whether the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios is enabled. To configure this parameter, run the **wlan-slice high-reliability frer-enhance** command.

11.4.58 display sta-load-balance static-group

Function

The **display sta-load-balance static-group** command displays information about static load balancing groups.

Format

display sta-load-balance static-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all static load balancing groups.	-
name *group-name*	Displays information about a specified static load balancing group.	The static load balancing group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display sta-load-balance static-group** command to view information about a specified static load balancing group or all static load balancing groups.

Example

Display information about all static load balancing groups.

```
<HUAWEI> display sta-load-balance static-group all
------------------------------------------------------------
Index  Group name
------------------------------------------------------------
0      cc
1      coco
------------------------------------------------------------
Total: 2
```

Table 11-143 Description of the **display sta-load-balance static-group all** command output

Item	Description
Index	Index.
Group name	Name of a static load balancing group.

Display information about the static load balancing group **cc**.

```
<HUAWEI> display sta-load-balance static-group name cc
-------------------------------------------------------------------
Group name                            : cc
Load-balance mode                       : sta-number
Sta-number start threshold               : 40
```

```
Sta-number gap threshold(percentage)   : 20
Sta-number gap threshold(number)       : -
RSSI threshold(dBm)                    : -70
RSSI diff gap(dBm)                     : 5
Deauth fail times                      : 2
Btm fail times                         : 5
Steer-restrict restrict time(s)        : 5
Steer-restrict probe threshold         : 5
Steer-restrict auth threshold          : 2
--------------------------------------------------------------------
```

Table 11-144 Description of the **display sta-load-balance static-group name** command output

Item	Description
Group name	Name of a static load balancing group.
Load-balance mode	Static load balancing mode. - sta-number: static load balancing based on the number of users
Sta-number start threshold	Start threshold for load balancing based on the number of users in the static load balancing group. To configure this parameter, run the **sta-number start-threshold** command.
Sta-number gap threshold(percentage)	Load difference threshold for static load balancing based on the percentage of users. To configure this parameter, run the **sta-number gap-threshold** command.
Sta-number gap threshold(number)	Load difference threshold for static load balancing based on the number of users. To configure this parameter, run the **sta-number gap-threshold** command.
RSSI threshold(dBm)	RSSI threshold of members in the static load balancing group. To configure this parameter, run the **rssi-threshold** command.
RSSI diff gap(dBm)	RSSI difference threshold of members in the static load balancing group. To configure this parameter, run the **rssi-diff-gap** command.
Deauth fail times	Maximum number of attempts to steer STAs in deauthentication mode. To configure this parameter, run the **deauth-fail-times** command.

Item	Description
Btm fail times	Maximum number of attempts to steer STAs in BTM mode. To configure this parameter, run the **btm-fail-times** command.
Steer-restrict restrict time(s)	Duration within which non-target APs suppress association of STAs during STA steering. To configure this parameter, run the **steer-restrict restrict-time** command.
Steer-restrict probe threshold	Maximum number of times non-target APs suppress probing of STAs during STA steering. To configure this parameter, run the **steer-restrict probe-threshold** command.
Steer-restrict auth threshold	Maximum number of times non-target APs suppress authentication of STAs during STA steering. To configure this parameter, run the **steer-restrict auth-threshold** command.

11.4.59 display sta-load-balance fairness

Function

The **display sta-load-balance fairness** command displays the load balancing fairness.

Format

display sta-load-balance fairness

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

STAs may access 2.4 GHz or 5 GHz radios on a WLAN. Even STA access indicates high fairness.

Example

Display the load balancing fairness.

```
<HUAWEI> display sta-load-balance fairness
2.4G sta-load-balance fairness : -
5G sta-load-balance fairness   : 0.85
```

Table 11-145 Description of the **display sta-load-balance fairness** command output

Item	Description
2.4G sta-load-balance fairness	Load balancing fairness of 2.4 GHz radios. A high value indicates high fairness. The value ranges from 0 to 1. When the value is 0, **-** is displayed.
5G sta-load-balance fairness	Load balancing fairness of 5 GHz radios. A high value indicates high fairness. The value ranges from 0 to 1. When the value is 0, **-** is displayed.

11.4.60 display station neighbor

Function

The **display station neighbor** command displays the neighbor list of a specified STA.

Format

display station neighbor sta-mac *mac-address*

Parameters

Parameter	Description	Value
sta-mac *mac-address*	Specifies the MAC address of a STA.	The MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the neighbor list of the STA with a specified MAC address.

Example

Display the neighbor list of the STA with a specified MAC address.

```
<HUAWEI> display station neighbor sta-mac 00e0-fc00-0001
UL info: Uplink measurement neighbor info
DL info: Downlink measurement neighbor info
------------------------------------------------------------------------------------------------------------------------------
--
Device MAC        Device ID   Device Name        Radio ID  Channel  UL info[RSSI/DATE]        DL info[RCPI/
RSSI/RSNI/DATE]
------------------------------------------------------------------------------------------------------------------------------
--
00e0-fc76-e360     0          00e0-fc76-e360     1         165      -44/2023-03-01/09:49:39   130/-45/-/
2023-03-01/09:49:39
------------------------------------------------------------------------------------------------------------------------------
--
Total neighbors: 1, total records: 1
```

System Response

Table 11-146 Description of the **display station neighbor** command output

Item	Description
Device MAC	MAC address of a neighboring device.
Device ID	ID of a neighboring device.
Device Name	Name of a neighboring device.
Radio ID	Radio ID of a neighboring device.
Channel	Channel of a neighboring device.
UL info[RSSI/DATE]	RSSI: signal strength of the neighboring device measured in the uplink direction, in dBm. DATE: timestamp. **NOTE** If a hyphen (-) is displayed, the STA does not support or perform uplink scanning.

Item	Description
DL info[RCPI/RSSI/RSNI/DATE]	RCPI: received channel power indicator (RCPI) of the neighbor device measured in the downlink direction, in dBm. RSSI: RSSI converted from the RCPI of the neighboring device measured in the downlink direction, in dBm. RSNI: received signal-to-noise indicator (RSNI), in dB DATE: timestamp. **NOTE** If a hyphen (-) is displayed, the STA does not support or perform downlink scanning, or an invalid value is returned.

11.4.61 display station neighbor all

Function

The **display station neighbor all** command displays STA neighbor information.

Format

display station neighbor all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view STA neighbor information.

Example

Display STA neighbor information.

```
<HUAWEI> display station neighbor all
UL neighbor number    : Number of neighbors detected through uplink measurement in 5 minutes
DL neighbor number    : Number of neighbors detected through downlink measurement in 5 minutes
Last update time      : Time when neighbors are detected through uplink or downlink measurement in 5 
minutes
                        formatted: uplink/downlink
------------------------------------------------------------------------------------------------------------------
```

```
STA MAC          UL neighbor number     DL neighbor number      Last update time
--------------------------------------------------------------------------------------------------------------------
00e0-fca2-a1c5    2                     2                     2022-10-14/14:07:02/2022-10-14/14:04:06
--------------------------------------------------------------------------------------------------------------------
Total:1
```

Table 11-147 Description of the **display station neighbor all** command output

Item	Description
STA MAC	MAC address of a STA.
UL neighbor number	Number of neighbors measured in the uplink direction in 5 minutes.
DL neighbor number	Number of neighbors measured in the downlink direction in 5 minutes.
Last update time	Time when a neighbor is detected in 5 minutes (uplink/downlink measurement).

11.4.62 display station steer-history

Function

The **display station steer-history** command displays historical information about STA steering.

Format

display station steer-history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the load balancing, band steering, or smart roaming function is enabled, STAs are steered. You can run this command to check historical information about STA steering.

Example

Display historical information about steering of all STAs.

```
<HUAWEI> display station steer-history
S/T/A:Source/Target/Actual
Flag:P[AI Profiling STA] V[Voice/Video/Active STA]
BTM success times/BTM total times:2/4
Deauth success times/Deauth total times:0/0
------------------------------------------------------------------------------------------------------------------------
--------
Time                Sta             Device(S/T/A)   Radio(S/T/A)  Rssi(S/T/A)        Reason       Move-mode
BTM_CODE  Flag  Result
------------------------------------------------------------------------------------------------------------------------
--------
2019-01-11/15:56:49 00e0-fc12-3456  3/5/5          0/1/1        -27/-27/-25        BandSteer    BTM
-         -     Success
2019-01-11/15:48:49 00e0-fc12-3456  3/3/3          0/1/1        -28/-/-57         BandSteer    BTM
-         -     Success
2019-01-11/15:43:49 00e0-fc12-3456  3/5/3          0/1/0        -29/-26/-44        BandSteer    BTM
-         -     Not Move
2019-01-11/15:43:29 00e0-fc12-3456  3/5/3          0/1/0        -29/-26/-44        Sticky       BTM         -
-     Not Move
------------------------------------------------------------------------------------------------------------------------
--------
Total: 4
```

Table 11-148 Description of the **display station steer-history** command output

Item	Description
Time	Time when a STA is triggered to steer.
Sta	MAC address of a STA.
Device(S/T/A)	ID of the source device/ID of the target device/ID of the device to which a STA is actually steered.
Radio(S/T/A)	ID of the source radio/ID of the target radio/ID of the radio to which a STA is actually steered.
Rssi(S/T/A)	RSSI of the source radio/RSSI of the target radio/RSSI of the radio to which a STA is actually steered.
Reason	Reason why a STA is triggered to steer. ● Sticky: Smart roaming is enabled. ● Sticky(A): The device periodically detects whether the STA is a sticky STA to proactively trigger smart roaming. ● LoadBalance: Load balancing is enabled. ● BandSteer: Band steering is enabled. ● AI: AI roaming is enabled.
Move-mode	Steering mode of a STA. ● BTM ● Deauth

Item	Description
BTM_CODE	BTM steering status code. ● 0: Accept ● 1: Reject-Unspecified reject reason. ● 2: Reject-Insufficient Beacon or Probe Response frames received from all candidates. ● 3: Reject-Insufficient available capacity from all candidates. ● 4: Reject-BSS termination undesired. ● 5: Reject-BSS termination delay requested. ● 6: Reject-STA BSS Transition Candidate List provided. ● 7: Reject-No suitable BSS transition candidates. ● 8: Reject-Leaving ESS. ● -: A STA is steered in deauthentication mode or the device does not receive any BTM response.
Flag	● V: voice/video/active STA flag ● P: steering flag by STA profile ● -: other

Item	Description
Result	Steering result of a STA. ● Success: The steering is successful. ● Success(NT): The steering is successful but the STA is not steered to the expected target. ● Time Out: The steering times out. ● Not Move: The steering is complete, but the STA is still associated with the source AP. ● Failed: The steering fails. (The steering result does not meet the expectation. For example, the STA is not steered to the 5 GHz radio in the band steering scenario, is steered to an AP with poor signal quality in the smart roaming scenario, or is steered to a high-load AP in the load balancing scenario.) ● Protect: The AP detects that the STA is a voice, video, or active STA and protects the STA by not sending a steering message. ● Error(1) or Error(2): An internal error occurs during the steering.

11.4.63 display station steer-info

Function

The **display station steer-info** command displays STA migration information based on the weak RSSI, non-optimal load, and migration inability.

Format

display station steer-info { **all** | **weak-rssi** | **non-best-load** | **unsteerable** }

Parameters

Parameter	Description	Value
all	Displays migration information about all STAs, including the weak RSSI, non-optimal load, and migration inability.	-

Parameter	Description	Value
weak-rssi	Displays STA information based on the weak RSSI.	-
non-best-load	Displays STA information based on the non-optimal load.	-
unsteerable	Displays STA information based on the migration inability.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view STA migration information based on the weak RSSI, non-optimal load, and migration inability.

Example

Display migration information about all STAs, including the weak RSSI, non-optimal load, and migration inability.

```
<HUAWEI> display station steer-info all
-----------------------------------------------------------------------
Sta-MAC              Weak RSSI       Non-best-load    Unsteerable
-----------------------------------------------------------------------
00e0-fc12-3456        Y              N               Y
-----------------------------------------------------------------------
Total STA          : 1
Weak-RSSI STA      : 1
Non-best-load STA  : 0
Unsteerable STA    : 1
```

Table 11-149 Description of the **display station steer-info** command output

Item	Description
Sta-MAC	MAC address of a STA.
Weak RSSI	Whether a STA has a weak RSSI.
Non-best-load	Whether a STA has the non-optimal load.
Unsteerable	Whether the STA cannot be migrated.

11.4.64 display station steer-statistics

Function

The **display station steer-statistics** command displays STA steering statistics.

Format

display station steer-statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the load balancing, band steering, or smart roaming function is enabled, STAs are steered. You can run this command to check STA steering statistics.

Example

Display steering statistics of all STAs.

```
<HUAWEI> display station steer-statistics
------------------------------------------------------------------------------------------------------------------------
------
Reason                      Total/Success        Deauth(Total/Success)    BTM(Total/Accept/REJ1/REJ2/REJ3/REJ4/
REJ5/REJ6/REJ7/REJ8/TimeOut)
------------------------------------------------------------------------------------------------------------------------
------
Sticky(Tradition)             58706/30430          0/0                    58706/30430/1083/0/0/9/0/241/7805/0/6446
Sticky(Profile)              58706/30430          0/0                    58706/30430/1083/0/0/9/0/241/7805/0/6446
Sticky(Profile Blind)         58706/30430          0/0                    58706/30430/1083/0/0/9/0/241/7805/0/6446
Load-balance(Tradition)       2450/1652            0/0                    2450/1652/4/0/0/0/0/20/335/0/20
Load-balance(Profile)         2450/1652            0/0                    2450/1652/4/0/0/0/0/20/335/0/20
Load-balance(Profile Blind)   2450/1652            0/0                    2450/1652/4/0/0/0/0/20/335/0/20
Band-steer(Tradition)         7596/2226            0/0                    7596/2226/39/0/0/29/0/131/968/0/335
Band-steer(Profile)           7596/2226            0/0                    7596/2226/39/0/0/29/0/131/968/0/335
Band-steer(Profile Blind)     7596/2226            0/0                    7596/2226/39/0/0/29/0/131/968/0/335
AI                           13256/10349          0/0                    13256/10349/0/0/0/0/0/0/0/0/58
Total                        82008/44657          0/0                    82008/44657/1126/0/0/38/0/392/9108/0/6859
------------------------------------------------------------------------------------------------------------------------
------
```

Table 11-150 Description of the **display station steer-statistics** command output

Item	Description
Reason	Reason why a STA is triggered to steer. - Sticky(Tradition): The STA is sticky (STA steering triggered by traditional smart roaming). - Sticky(Profile): The STA is sticky (STA steering based on STA profiles, not blind handover). - Sticky(Profile Blind): The STA is sticky (STA steering based on STA profiles, blind handover). - Load-balance(Tradition): Load balancing is implemented (STA steering triggered by traditional smart roaming). - Load-balance(Profile): Load balancing is implemented (STA steering based on STA profiles, not blind handover). - Load-balance(Profile Blind): Load balancing is implemented (STA steering based on STA profiles, blind handover). - Band-steer(Tradition): Band steering is implemented (STA steering triggered by traditional smart roaming). - Band-steer(Profile): Band steering is implemented (STA steering based on STA profiles, not blind handover). - Band-steer(Profile Blind): Band steering is implemented (STA steering based on STA profiles, blind handover). - AI: AI roaming steering based on coordinated scanning is implemented. - Total: total steering reason count.
Total/Success	Total number of triggered STA steering times/Number of successful STA steering times.

Item	Description
Deauth(Total/Success)	Total number of times STA steering is triggered in deauthentication mode/ Number of times STA steering is successfully triggered in deauthentication mode.
BTM(Total/Accept/REJ1/REJ2/REJ3/ REJ4/REJ5/REJ6/REJ7/REJ8/TimeOut)	Total number of times STA steering is triggered in BTM mode/Number of times STA steering is successfully triggered in BTM mode/Number of times STA steering is rejected in BTM mode/Number of times STA steering is timed out in BTM mode. The options are as follows: ● REJ1: Reject-Unspecified reject reason. ● REJ2: Reject-Insufficient Beacon or Probe Response frames received from all candidates. ● REJ3: Reject-Insufficient available capacity from all candidates. ● REJ4: Reject-BSS termination undesired. ● REJ5: Reject-BSS termination delay requested. ● REJ6: Reject-STA BSS Transition Candidate List provided. ● REJ7: Reject-No suitable BSS transition candidates. ● REJ8: Reject-Leaving ESS.

11.4.65 display station unsteerable

Function

The **display station unsteerable** command displays "unable to roam" records of STAs.

Format

display station unsteerable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station unsteerable** command to check "unable to roam" records of STAs.

Example

Display "unable to roam" records of STAs.

```
<HUAWEI> display station unsteerable
--------------------------------------------------------------------------------
STA MAC              Left aging time          Status
--------------------------------------------------------------------------------
00e0-fc12-3456        3h 20m                   online
00e0-fc45-7890        2h 30m                   offline
--------------------------------------------------------------------------------
Total: 2
```

Table 11-151 Description of the **display station unsteerable** command output

Item	Description
STA MAC	MAC address of the "unable to roam" STA.
Left aging time	Remaining aging period.
Status	Status of the STA. ● online ● offline

11.4.66 display sta-profiling

Function

The **display sta-profiling** command displays STA profile information on the device.

Format

display sta-profiling

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

STAs of different models use different Wi-Fi chips and WLAN module drivers, and therefore have different roaming steering behaviors. To improve roaming experience, WLAN devices need to use different roaming steering policies for STAs of different types (distinguished by STA profiles). During the steering roaming for a STA, the system matches STA information against the existing STA profiles based on the model and operating system, and selects a more suitable roaming steering policy, improving the roaming success rate. You can run the **display sta-profiling** command to check information about the learned STA profiles on the device.

Prerequisites

The STA profiling function has been enabled using the **undo sta-profiling disable** command.

Example

Display STA profile information on the device.

```
<HUAWEI> display sta-profiling
----------------------------------------------------------------------------------------------------
Vendor   Type                    Type ID      OS               OS ID      Priority    Version
----------------------------------------------------------------------------------------------------
...
Huawei   Mate 40                 32455       Android 10       17765      1190       0
Huawei   Mate 40 Pro             32454       Android 10       17765      1188       0
Huawei   Mate 40 Pro Plus        32456       Android 10       17765      1192       0
Huawei   Mate RS                 7348        Android 10       17765      149        0
...
----------------------------------------------------------------------------------------------------
 Total:313
```

Table 11-152 Description of the **display sta-profiling** command output

Item	Description
Vendor	Terminal brand.
Type	STA model.
Type ID	STA model ID.
OS	STA operating system.
OS ID	STA operating system ID.

Item	Description
Priority	Priority of the matching between a STA profile and the STA. A smaller value indicates a higher priority. If a STA matches multiple profiles based on the model and operating system, the profile with the highest priority is used.
Version	STA profile version. This version number increases with STA profile updates.

11.4.67 display wlan calibrate channel-set

Function

The **display wlan calibrate channel-set** command displays the effective calibration channels and bandwidth.

Format

display wlan calibrate channel-set ap-group { **name** *ap-group-name* | **all** }

Parameters

Parameter	Description	Value
ap-group name *ap-group-name*	Displays the effective calibration channels and bandwidth in a specified AP group.	The AP group must exist.
ap-group all	Displays the effective calibration channels and bandwidth in all AP groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the radio calibration function, you can run the **display wlan calibrate channel-set** command to check the effective calibration channels and bandwidth.

Example

Display the calibration channels and bandwidth that take effect globally.

```
<HUAWEI> display wlan calibrate channel-set ap-group all
AP group    : default
Country code: CN
-------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
-------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
6G          20MHz      -
-------------------------------------------------------------------------------

AP group    : mainland
Country code: CN
-------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
-------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
6G          20MHz      -
-------------------------------------------------------------------------------
```

Table 11-153 Description of the **display wlan calibrate channel-set** command output

Item	Description
AP group	Name of an AP group.
Country code	Country code.
Radio band	Radio type.
Bandwidth	Effective calibration bandwidth.
Channel Set	Effective calibration channel set.

11.4.68 display wlan calibrate global configuration

Function

The **display wlan calibrate global configuration** command displays the global configuration of radio calibration.

Format

display wlan calibrate global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan calibrate global configuration** command to check the global configuration of radio calibration.

Example

Display the global configuration of radio calibration.

```
<HUAWEI> display wlan calibrate global configuration
--------------------------------------------------------------------------------
----------
Mode                                             : manual
Auto start time                                  : -
Auto interval(min)                               : -
Schedule time                                    : -
Schedule time-range                              : -
Calibration progress                             : 50%
Flexible radio mode                              : auto-switch
Policy                                           : -
2.4G sensitivity                                 : low
5G sensitivity                                   : high
6G sensitivity                                   : medium
Virtual group size                               : 50
K-value                                          : 70
Reference data analysis                          : enable
Reference rogue ap interference                  : enable
Environment deterioration blacklist threshold    : 16
--------------------------------------------------------------------------------
----------
```

Table 11-154 Description of the **display wlan calibrate global configuration** command output

Item	Description
Mode	Radio calibration mode. To configure this parameter, run the **calibrate enable** { **auto** | **manual** | **schedule time** } command.
Auto start time	Start time of automatic radio calibration (only for the automatic radio calibration mode). To configure this parameter, run the **calibrate enable auto** [**interval** *interval-value* [**start-time** *start-time*]] command.

Item	Description
Auto interval(min)	Interval for automatic radio calibration (only for the automatic radio calibration mode). To configure this parameter, run the **calibrate enable auto** [**interval** *interval-value* [**start-time** *start-time*]] command.
Schedule time	Time of scheduled radio calibration (only for the scheduled radio calibration mode). To configure this parameter, run the **calibrate enable schedule time** *time-value* command.
Schedule time-range	Time range for scheduled radio calibration (only for the scheduled radio calibration mode). To configure this parameter, run the **calibrate enable schedule time** *time-value* [**time-range** *time-range-name*] command.
Calibration progress	Progress of manual or scheduled radio calibration.
Flexible radio mode	Redundant radio switchover mode. To configure this parameter, run the **calibrate flexible-radio** { **auto-switch** | **auto-off** } command.
Policy	Radio calibration policy. To configure this parameter, run the **calibrate policy** { **non-wifi** | **noise-floor** } command.
2.4G sensitivity 5G sensitivity 6G sensitivity	Radio calibration sensitivity. To configure this parameter, run the **calibrate sensitivity** [**2.4g** | **5g** | **6g**] { **high** | **medium** | **low** | **insensitivity** | **custom-percent** *custom-percent* } command.
Virtual group size	Parameter of the radio calibration algorithm. To configure this parameter, run the **calibrate virtual-group-size** *size-value* **k-value** *k-value* command.

Item	Description
K-value	Parameter of the radio calibration algorithm. To configure this parameter, run the **calibrate virtual-group-size** *size-value* **k-value** *k-value* command.
Reference data analysis	Whether to enable Big Data calibration. To configure this parameter, run the **calibrate reference data-analysis disable** command.
Reference rogue ap interference	Whether rogue interference calibration is enabled. To configure this parameter, run the **calibrate reference rogue-ap-interference disable** command.
Environment deterioration blacklist threshold	Blacklist threshold for the number of times the channel environment deteriorates. To configure this parameter, run the **calibrate environment-deterioration-blacklist threshold** command.

11.4.69 display wlan calibrate statistics

Function

The **display wlan calibrate statistics** command displays radio calibration statistics.

Format

display wlan calibrate statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays radio calibration statistics on the specified AP name. The AP name and radio ID together identify a radio.	The AP name must already exist.
ap-id *ap-id*	Displays radio calibration statistics on the specified AP ID. The AP ID and radio ID together identify a radio.	The AP ID must already exist.

Parameter	Description	Value
radio *radio-id*	Displays radio calibration statistics on the specified radio.	The radio ID must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan calibrate statistics** command to view radio calibration statistics, helping check whether the radio environment is stable.

Example

Display calibration statistics about radio 0 on AP0.

```
<HUAWEI> display wlan calibrate statistics ap-id 0 radio 0
------------------------------------------------------------------------
Signal environment deterioration :1
Power calibration                :1
Channel calibration              :0
------------------------------------------------------------------------
```

Table 11-155 Description of the **display wlan calibrate statistics** command output

Item	Description
Signal environment deterioration	Number of times the radio environment deteriorates.
Power calibration	Number of times the power of the radio is calibrated.
Channel calibration	Number of times the channel of the radio is calibrated.

11.4.70 display wlan scene

Function

The **display wlan scene** command displays information about a scenario profile.

Format

display wlan scene { **name** *scene-name* | **all** }

Parameters

Parameter	Description	Value
name *scene-name*	Specifies the name of a scenario profile.	The value is of the enumerated type. ● multi-partition-cross-room: indicates an indoor multi-partition cross-room deployment scenario (capacity first). ● multi-partition-cross-room-cov: indicates an indoor multi-partition cross-room deployment scenario (coverage first). ● automated-guided-vehicle: indicates an AGV scenario. ● high-density-stadium: indicates a high-density stadium scenario. ● indoor-high-density: indicates an indoor high-density coverage scenario. ● indoor-low-density: indicates an indoor low-density coverage scenario. ● indoor-multi-partition: indicates an indoor multi-partition coverage scenario. ● indoor-normal-density: indicates an indoor common coverage scenario. ● industrial-manufacturing: indicates an industrial manufacturing scenario. ● outdoor-continuous: indicates an outdoor continuous coverage scenario.

Parameter	Description	Value
		- virtual-reality: indicates a VR scenario.
all	Displays all scenario profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan scene** command to view detailed information about a scenario profile to learn about wireless service parameters and their settings involved in the scenario.

Example

Display all scenario profiles.

```
<HUAWEI> display wlan scene all
--------------------------------------------------------------------------------------
Name                          Description
--------------------------------------------------------------------------------------
automated-guided-vehicle        Applicable to smart warehousing scenarios.
high-density-stadium            Applicable to high-density stadiums.
indoor-high-density             Applicable to indoor high-density scenarios, such as cafes and high-density
office.
indoor-low-density              Applicable to indoor low-density scenarios, such as retail scenarios.
indoor-multi-partition          Applicable to indoor multi-partition scenarios, such as dormitories, hotel
rooms, and wards.
indoor-normal-density           Applicable to indoor normal-density scenarios, such as normal office.
industrial-manufacturing        Applicable to industrial manufacturing scenarios.
multi-partition-cross-room      Applicable to indoor scenarios (capacity first), where one AP covers multiple
rooms and APs are blocked from each other by walls.
multi-partition-cross-room-cov  Applicable to indoor scenarios (coverage first), where one AP covers
multiple rooms and APs are blocked from each other by walls.
outdoor-continuous              Applicable to outdoor continuous coverage scenarios, such as roadways and
parks.
virtual-reality                 Applicable to VR scenarios.
--------------------------------------------------------------------------------------
Total: 11
```

Display information about the scenario profile **multi-partition-cross-room**.

```
<HUAWEI> display wlan scene name multi-partition-cross-room
--------------------------------------------------------------------------------------
Radio parameter:
  CCA threshold(dBm)                : -
  RX sensitivity(dBm)               : -
  Beacon interval(TUs)              : -
  Dynamic EDCA                      : enable
SSID parameter:
```

```
  Deny-broadcast-probe                    : -
  Active dull client                      : -
  Association timeout(min)                : -
Station load balance:
  Sta-number start threshold              : -
  Sta-number gap threshold(number)        : -
Smart roam:
  Standing SNR threshold(dB)              : 15
  SNR quick-kickoff-threshold(dB)         : 10
Radio calibration:
  DCA 5G bandwidth                        : 80Mhz
  TPC threshold(dBm)                      : -35
  Grouping interference threshold(dBm)    : -70
  Maximum 2.4G calibration TX power(dBm)  : -
  Maximum 5G calibration TX power(dBm)    : -
  Minimum 2.4G calibration TX power(dBm)  : -
  Minimum 5G calibration TX power(dBm)    : -
----------------------------------------------------------------------------------------
```

Table 11-156 Description of the **display wlan scene** command output

Item	Description
WLAN service parameters	To view the description of a specific parameter, search for the parameter and view the description in the corresponding display command. If a hyphen (-) is displayed, this parameter is not configured in the scenario profile.

11.4.71 dynamic-edca enable

Function

The **dynamic-edca enable** command enables dynamic EDCA parameter adjustment.

The **undo dynamic-edca enable** command disables dynamic EDCA parameter adjustment.

By default, dynamic EDCA parameter adjustment is disabled.

Format

dynamic-edca enable

undo dynamic-edca enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

A WLAN has only three non-overlapping channels on the 2.4 GHz frequency band. When APs are deployed densely, multiple APs have to work in the same channel, resulting in co-channel interference. This interference degrades network performance.

The dynamic EDCA parameter adjustment function allows APs to adjust EDCA parameters flexibly to reduce the possibility of collision, improve the throughput, and enhance user experience.

Example

Enable dynamic EDCA parameter adjustment.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] dynamic-edca enable
```

11.4.72 dynamic-edca threshold

Function

The **dynamic-edca threshold** command configures the threshold for the dynamic EDCA Best-Effort service.

The **undo dynamic-edca threshold** command restores the default threshold for the dynamic EDCA Best-Effort service.

The default threshold for the dynamic EDCA Best-Effort service is 6 pps.

Format

dynamic-edca threshold be-service *be-service-threshold*

undo dynamic-edca threshold be-service

Parameters

Parameter	Description	Value
be-service *be-service-threshold*	Specifies the threshold for the dynamic EDCA Best-Effort service.	The value is an integer that ranges from 1 to 1000, in pps.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When dynamic EDCA is enabled, the system dynamically adjusts EDCA parameters for the Best-Effort service and Background service based on the number of Best-Effort users, improving user experience.

If the number of Best-Effort service packets from a user in the radio's internal statistics queue exceeds the threshold (specified using the **dynamic-edca threshold** command) per unit time (1s), the user is considered a Best-Effort user.

Before running this command, you must run the **dynamic-edca enable** command to enable dynamic EDCA.

Example

Set the threshold for the dynamic EDCA Best-Effort service to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] dynamic-edca enable
[HUAWEI-wlan-rrm-prof-default] dynamic-edca threshold be-service 10
```

11.4.73 sta-number gap-threshold

Function

The **sta-number gap-threshold** command sets the load difference threshold for load balancing based on the number of users in a static load balancing group.

The **undo sta-number gap-threshold** command restores the default load difference threshold for load balancing based on the number of users in a static load balancing group.

By default, the load difference threshold of a static load balancing group is specified based on the number of users, and the default value is 3.

Format

sta-number gap-threshold { **percentage** *percentage-value* | **number** *number-value* }

undo sta-number gap-threshold

Parameters

Parameter	Description	Value
percentage *percentage-value*	Specifies the load difference threshold for static load balancing based on the percentage of users.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the percentages of users on radios.
number *number-value*	Specifies the load difference threshold for static load balancing based on the number of users.	The value is an integer that ranges from 1 to 20. It indicates the threshold of the load difference among radios in a load balancing group. The load difference refers to the difference between the numbers of users on radios.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following load balancing algorithm is used after the user access to determine whether to steer the user to a new AP:

One of the conditions for steering a user to a new AP is that the radio of the target load is lower than that of the current access radio. The radio load is identified by the number or percentage (Number of users associated with the current radio/Maximum number of access users supported by the radio x 100%) of access users. If the load difference between the target radio and current radio exceeds the specified threshold, the condition is met.

Precautions

If you configure the load difference threshold based on both the number of users and the percentage of users, only the latest configuration takes effect.

Example

Set the load difference threshold for load balancing based on the percentage of users in the static load balancing group to 40%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] sta-number gap-threshold percentage 40
```

11.4.74 high-density amc-optimize enable

Function

The **high-density amc-optimize enable** command enables the adaptive modulation and coding (AMC) optimization function in high-density scenarios.

The **undo high-density amc-optimize enable** command disables the AMC optimization function in high-density scenarios.

By default, the AMC optimization function is disabled in high-density scenarios.

Format

high-density amc-optimize enable

undo high-density amc-optimize enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In typical high-density scenarios, a large number of hidden nodes exist, which interfere in communication between APs and STAs and affect product performance. The AMC optimization function can reduce such interference and improve the AMC algorithm performance.

- It is recommended that this function be enabled in high-density scenarios where directional antennas are used.
- This function is not applicable to scenarios where STAs move fast between APs.

Precautions

- The AMC optimization in high-density scenarios is not supported by the following APs:
  - AirEngine 9700D-S (including matching ORUs)
  - AirEngine X77X
  - AirEngine X76X
- This function does not take effect in MU-MIMO mode.

Example

Enable the AMC optimization function in high-density scenarios on the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] high-density amc-optimize enable
```

11.4.75 interference adjacent-channel threshold

Function

The **interference adjacent-channel threshold** command configures the alarm threshold for adjacent-channel interference.

The **undo interference adjacent-channel threshold** command restores the default alarm threshold for adjacent-channel interference.

By default, the alarm threshold for adjacent-channel interference is 50%.

Format

interference adjacent-channel threshold *threshold-value*

undo interference adjacent-channel threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold, which is the percentage of the adjacent-channel interference power against the maximum power.	The value is an integer that ranges from 1 to 100, in percentage.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. When APs are placed too close to each other or have strong signals, more noise is produced, degrading network performance.

After the **interference detect-enable** command is executed to enable interference detection, an AP can detect adjacent-channel interference. When the AP detects that adjacent-channel interference exceeds the alarm threshold configured using the **interference adjacent-channel threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for adjacent-channel interference to 52%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference detect-enable
[HUAWEI-wlan-radio-2g-prof-radio0] interference adjacent-channel threshold 52
```

11.4.76 interference co-channel threshold

Function

The **interference co-channel threshold** command configures the alarm threshold for co-channel interference.

The **undo interference co-channel threshold** command restores the default alarm threshold for co-channel interference.

By default, the alarm threshold for co-channel interference is 50%.

Format

interference co-channel threshold *threshold-value*

undo interference co-channel threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold, which is the percentage of the co-channel interference power against the maximum power.	The value is an integer that ranges from 1 to 100, in percentage.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Two APs working in the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance.

After the **interference detect-enable** command is executed to enable interference detection, an AP can detect adjacent-channel interference. When the AP detects that co-channel interference exceeds the alarm threshold configured using the **interference co-channel threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for co-channel interference to 60%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference detect-enable
[HUAWEI-wlan-radio-2g-prof-radio0] interference co-channel threshold 60
```

11.4.77 interference detect-enable

Function

The **interference detect-enable** command enables interference detection.

The **undo interference detect-enable** command disables interference detection.

By default, interference detection is disabled.

Format

interference detect-enable

undo interference detect-enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

WLAN wireless channels are vulnerable to interference in surrounding radio environments, and the service quality is therefore degraded. If interference detection is configured, a monitor AP can know the radio environment in real time and report alarms to the AC in a timely manner.

Interference detection enables an AP to detect AP co-channel interference, AP adjacent-channel interference, and STA interference.

- AP co-channel interference: Two APs working on the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance.
- AP adjacent-channel interference: Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. Therefore, if APs are placed too close to each other or they have strong signals, more noise will be produced, degrading network performance.
- STA interference: If there are many STAs that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.

Example

Enable interference detection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference detect-enable
```

11.4.78 interference station threshold

Function

The **interference station threshold** command configures the alarm threshold for STA interference.

The **undo interference station threshold** command restores the default alarm threshold for STA interference.

By default, the alarm threshold for STA interference is 32.

Format

interference station threshold *threshold-value*

undo interference station threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold.	The value is an integer that ranges from 1 to 256.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

If there are many STAs that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.

After the **interference detect-enable** command is executed to enable interference detection, an AP can detect STAs that are managed by other APs. When the AP detects that the number of such STAs exceeds the alarm threshold configured using the **interference station threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for STA interference to 50.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name radio0
[HUAWEI-wlan-radio-2g-prof-radio0] interference station threshold 50
```

11.4.79 interference-visualization enable

Function

The **interference-visualization enable** command enables interference visualization on AP radios.

The **undo interference-visualization enable** command disables interference visualization on AP radios.

By default, interference visualization is disabled on AP radios.

NOTE

Interference visualization is not available for the following models:

- AirEngine x761
- AirEngine x762

Format

interference-visualization enable

undo interference-visualization enable

Parameters

None

Views

AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the AP is connected to an analyzer, you can enable interference visualization on radios of co-channel APs so that packet transmission information on the co-channel APs can be displayed on the analyzer, thereby showing air interface interference behavior.

Pre-configuration Tasks

Configure KPI reporting, and run the **ap log module mid** *ffdc0000* command in the WMI profile view to report logs of the interference visualization module to the analyzer.

Precautions

Interference visualization can be enabled on a maximum of 20 AP radios. To view information about all AP radios on which interference visualization is enabled, run the **display interference-visualization configuration** command.

Example

Enable interference visualization on radio 1 of AP 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 1
[HUAWEIwlan-radio-1/1] interference-visualization enable
```

11.4.80 member (static load balancing group view)

Function

The **member** command adds an AP radio to a static load balancing group.

The **undo member** command deletes an AP radio from a load balancing group.

By default, no AP radio is added to a static load balancing group.

Format

member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }&<1-16>

undo member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }&<1-16>

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP. The AP name and radio ID identify a radio.	The AP name must exist.
ap-id *ap-id*	Specifies the ID of an AP. The AP ID and radio ID identify a radio.	The AP ID must exist.
radio *radio-id*	Specifies a radio ID. The radio ID and AP name identify a radio.	The radio ID must exist.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to add an AP radio to or delete an AP radio from a static load balancing group. When a STA requests to connect to an AP radio in a static load balancing group, the AC compares the load of the radio and other working radios in the load balancing group and determines whether to allow the STA to connect to the radio according to a load balancing algorithm.

Precautions

- If dual-band APs are used, traffic is load balanced among APs working on the same frequency band.
- Each load balancing group supports a maximum of 16 AP radios.
- Under the agile distributed network architecture, you only need to add radios of the RUs to a static load balancing group. Central APs are not supported in static load balancing groups.
- A radio configured with channel 184, 188, 192, or 196 on the 4.9 GHz frequency band cannot be used for load balancing.

Example

Add radio 0 of AP **office** to the static load balancing group **coco**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] member ap-name office radio 0
```

11.4.81 power auto-adjust enable

Function

The **power auto-adjust enable** command enables signal-strength-based power adjustment for APs.

The **undo power auto-adjust enable** command disables signal-strength-based power adjustment for APs.

By default, signal-strength-based power adjustment is disabled for an AP.

NOTE

This command does not take effect for the following APs:

- AirEngine X77X
- AirEngine X76X

Format

power auto-adjust enable

undo power auto-adjust enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traditional radio power control function sets the power of an AP to a fixed value to keep the power of all STAs connecting to the AP the same.

You can run the **power auto-adjust enable** command to enable signal-strength-based power adjustment. This function enables an AP to detect the signal strength of a STA in a timely manner. If the AP detects that the signal strength of the STA is strong (for example, the STA is near the AP), the AP reduces its transmit power when sending packets. If the AP detects that the signal strength of the STA is weak (for example, the STA is far from the AP), the AP uses the normal transmit power to send radio signals.

Prerequisites

The power mode has been set to automatic using the **calibrate auto-txpower-select enable** command.

Example

Enable signal-strength-based power adjustment for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] power auto-adjust enable
```

11.4.82 radio-reload time-range

Function

The **radio-reload time-range** command enables scheduled radio reloading on APs.

The **undo radio-reload time-range** command disables scheduled radio reloading on APs.

By default, scheduled radio reloading is disabled on APs.

Format

radio-reload time-range *time-range*

undo radio-reload time-range

Parameters

Parameter	Description	Value
time-range	Specifies a time range during which radios are reloaded as scheduled.	The specified time range must exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After APs run for a long time, some unknown exceptions may occur. You can run this command to configure a scheduled policy for APs to reload radios during off-peak hours. This prevents potential exceptions or addresses existing exceptions.

Prerequisites

A time range for scheduled radio reloading has been specified by using the **time-range** command.

Precautions

After scheduled radio reloading is configured, APs reload radios in batches within the specified time range. During radio reloading on an AP, STAs associated with the AP are steered to neighboring APs. To prevent impact on services, it is recommended that radio reloading be performed during a time range when no service traffic is transmitted.

This function is not recommended in industrial scenarios where services need to run continuously for a long time.

Example

Enable the scheduled radio reloading function for 5 GHz radios of APs and specify the time range of 01:00 to 05:00 every day for scheduled radio reloading.

```
<HUAWEI> system-view
[HUAWEI] time-range test 01:00 to 05:00 daily
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name wlan-radio5g
[HUAWEI-wlan-radio-5g-prof-wlan-radio5g] radio-reload time-range test
```

11.4.83 reset ap traffic statistics wireless

Function

The **reset ap traffic statistics wireless** command clears packet statistics on a specified AP radio.

Format

reset ap traffic statistics wireless { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears packet statistics on the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Clears packet statistics on the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Clears packet statistics on a specified radio.	The radio ID must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear packet statistics on a specified AP radio.

Example

Clear packet statistics on radio 2 of the AP with the ID 0.

```
<HUAWEI> reset ap traffic statistics wireless ap-id 0 radio 2
```

11.4.84 reset station steer-history

Function

The **reset station steer-history** command deletes historical information about STA migrations.

Format

reset station steer-history

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to delete historical information about STA migrations.

Example

Delete historical information about migrations of all STAs.

```
<HUAWEI> reset station steer-history
```

11.4.85 reset flexible-radio switch-record

Function

The **reset flexible-radio switch-record** command clears switching records of redundant radios.

Format

reset flexible-radio switch-record all

Parameters

Parameter	Description	Value
all	Clears switching records of all redundant radios.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **reset flexible-radio switch-record** command to clear switching records of redundant radios.

Example

Clear switching records of all redundant radios.

```
<HUAWEI> reset flexible-radio switch-record all
```

11.4.86 reset station steer-statistics

Function

The **reset station steer-statistics** command deletes statistics about STA steering.

Format

reset station steer-statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to delete statistics about STA steering.

Example

Delete statistics about STA steering.

```
<HUAWEI> reset station steer-statistics
```

11.4.87 reset wlan calibrate statistics

Function

The **reset wlan calibrate statistics** command clears radio calibration statistics.

Format

reset wlan calibrate statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears radio calibration statistics on the AP with the specified AP name. The AP name and radio ID together identify a radio.	The AP name must exist.
ap-id *ap-id*	Clears radio calibration statistics on the AP with the specified AP ID. The AP ID and radio ID together identify a radio.	The AP ID must exist.

Parameter	Description	Value
radio *radio-id*	Clears calibration statistics about the radio with the specified radio ID. The radio ID and AP name together identify a radio.	The radio ID must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Run the **reset wlan calibrate statistics** command to clear radio calibration statistics, including the number of times the radio environment deteriorates and number of times the radio channel and power are calibrated.

Example

Clear calibration statistics about radio 0 on AP0.

```
<HUAWEI> reset wlan calibrate statistics ap-id 0 radio 0
```

11.4.88 rrm-profile (WLAN view)

Function

The **rrm-profile** command creates an RRM profile and displays the RRM profile view.

The **undo rrm-profile** command deletes an RRM profile.

By default, the system provides the RRM profile **default**.

Format

rrm-profile name *profile-name*

undo rrm-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an RRM profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all RRM profiles.	The RRM profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN technology uses radio signals (such as 2.4 GHz or 5 GHz radio waves) as transmission medium. Radio signals will attenuate when transmitted over the air, degrading service quality for wireless users. Radio resource management (RRM) enables a WLAN to adapt to changes in the radio environment by dynamically adjusting radio resources. This improves service quality for wireless users.

Follow-up Procedure

Run the **rrm-profile (radio profile view)** command to bind the RRM profile to a radio profile so that the RRM profile can take effect.

Example

Create the RRM profile **rrm01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name rrm01
[HUAWEI-wlan-rrm-prof-rrm01]
```

11.4.89 rrm-profile (radio profile view)

Function

The **rrm-profile** command binds an RRM profile to a radio profile.

The **undo rrm-profile** command unbinds an RRM profile from a radio profile.

By default, the RRM profile **default** is bound to a radio profile.

Format

rrm-profile *profile-name*

undo rrm-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an RRM profile.	The RRM profile name must already exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an RRM profile using the **rrm-profile (WLAN view)** command, bind the RRM profile to a radio profile so that the RRM profile can take effect.

Example

Bind the RRM profile **rrm01** to the radio profile **office01**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name rrm01
[HUAWEI-wlan-rrm-prof-rrm01] quit
[HUAWEI-wlan-view] radio-2g-profile name office01
[HUAWEI-wlan-radio-2g-prof-office01] rrm-profile rrm01
```

11.4.90 rssi-diff-gap

Function

The **rssi-diff-gap** command sets the RSSI difference threshold for members in a static load balancing group.

The **undo rssi-diff-gap** command restores the default RSSI difference threshold of members in a static load balancing group.

By default, the RSSI difference threshold of members in a static load balancing group is 5 dB.

Format

rssi-diff-gap *diff-gap-threshold*

undo rssi-diff-gap

Parameters

Parameter	Description	Value
diff-gap-threshold	Specifies the RSSI difference threshold of members in a static load balancing group.	The value is an integer that ranges from 0 to 15, in dB.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To achieve load balancing, an AP may steer connected STAs to other APs with smaller RSSIs. If the RSSI of the AP with which a STA currently associates minus the RSSI of the target AP is larger than the specified RSSI difference threshold, the STA is denied from being steered to the target AP; otherwise, the STA can be steered to the target AP.

Precautions

If STAs have high signal quality deterioration tolerance for the target AP, you can set a larger RSSI difference threshold to achieve better load balancing effect. If STAs have low signal quality deterioration tolerance for the target AP, set a smaller RSSI difference threshold. You are advised to retain the default value.

Example

Set the RSSI difference threshold for members in a static load balancing group to 6 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] rssi-diff-gap 6
```

11.4.91 rssi-threshold

Function

The **rssi-threshold** command sets an RSSI threshold for member devices in a static load balancing group.

The **undo rssi-threshold** command restores the default RSSI threshold of member devices in a static load balancing group.

By default, the RSSI threshold of member devices in a static load balancing group is –65 dBm.

Format

rssi-threshold *rssi-threshold*

undo rssi-threshold

Parameters

Parameter	Description	Value
rssi-threshold	Specifies the RSSI threshold of members in a static load balancing group.	The value is an integer that ranges from –75 to –55, in dBm.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting an RSSI threshold for member devices in a static load balancing group is to filter APs with weak signals, so that STAs can be load balanced between APs with better signals. This prevents STAs from associating with APs with weak signals but light loads. This function does not affect STAs' going online.

Example

Set the RSSI threshold for member devices in a static load balancing group to –70 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] rssi-threshold -70
```

11.4.92 rx-sensitivity

Function

The **rx-sensitivity** command sets the receiver sensitivity threshold of an AP.

The **undo rx-sensitivity** command restores the default receiver sensitivity threshold of an AP.

By default, the receiver sensitivity threshold of an AP is –128 dBm.

Format

rx-sensitivity *threshold*

undo rx-sensitivity

Parameters

Parameter	Description	Value
threshold	Specifies the receiver sensitivity threshold of an AP.	The value is an integer that ranges from –128 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The sensitivity threshold can be used to adjust the anti-interference capability of radios.

Precautions

The receiver sensitivity threshold cannot be set higher than the upper AGC threshold.

Modifying the receiver sensitivity threshold will affect the uplink access coverage or user access. It is recommended that the default setting be remained or the threshold be modified under the guidance of professional technical personnel.

Example

Set the receiver sensitivity threshold to –70 dBm in the 2G radio profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] radio-2g-profile name test
[HUAWEI-wlan-radio-2g-prof-test] rx-sensitivity -70
Warning: This parameter will affect the uplink access coverage or user access. I
t is recommended that the configuration be modified under the guidance of profes
sional technical personnel. Continue? [Y/N]:y
```

11.4.93 scan-channel-set

Function

The **scan-channel-set** command configures an air scan channel set.

The **undo scan-channel-set** command restores the default air scan channel set.

By default, an air scan channel set contains all channels supported by the country code of an AP.

Format

scan-channel-set { **country-channel** | **dca-channel** | **work-channel** }

undo scan-channel-set

Parameters

Parameter	Description	Value
country-channel	Specifies an air scan channel set that contains all channels supported by the country code of an AP.	-
dca-channel	Specifies a calibration channel set as the air scan channel set. To configure a calibration channel set, run the **dca-channel channel-set** command.	-
work-channel	Specifies an air scan channel set that contains working channels of APs.	-

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **scan-channel-set** command to specify an air scan channel set for an AP, the AP scans channels in the channel set. The collected information is reported to the AC or server for radio calibration, smart roaming, spectrum analysis, WLAN location, or WIDS data analysis.

Precautions

- If the air scan channel set you specified contains all channels supported by the country code of the AP, the AP scans data on many channels but the channel scanning lasts for a long time, which may affect real-time data analysis.
- If you specify a calibration channel set as the air scan channel set, the AP scans data on a few channels. This reduces the channel scanning time, increases the terminal location accuracy, and reduces burden on the device.
- If you add only working channels of an AP to the air scan channel set, the AP only scans the working channels.

Example

Configure an air scan channel set that contains all calibration channels.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-channel-set dca-channel
```

11.4.94 scan-disable

Function

The **scan-disable** command disables the air scan function.

The **undo scan-disable** command enables the air scan function.

By default, the air scan function is enabled.

Format

scan-disable

undo scan-disable

Parameters

None

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP does not require air scan, you can run the **scan-disable** command to disable the air scan function. The AP then will stop scanning surrounding wireless signals.

Precautions

Disabling air scan will affect scanning functions, such as radio calibration, spectrum analysis, terminal location, WIDS, smart roaming, and DFS smart selection.

Example

Disable the air scan function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-disable
Warning: This operation will affect scanning-related services such as radio calibration, spectrum analysis, terminal location, WIDS
function, smart roaming and DFS smart selection.Continue? [Y/N]y
```

11.4.95 scan-enhancement

Function

The **scan-enhancement** command enables the scanning enhancement function.

The **undo scan-enhancement** command disables the scanning enhancement function.

By default, the scanning enhancement function is disabled.

NOTICE

The scanning enhancement function is supported only by the AirEngine 6761-21, AirEngine 6761-21E, and AirEngine 6761S-21.

Format

scan-enhancement

undo scan-enhancement

Parameters

None

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

The third radio of some APs is used specifically for radio scanning and does not support configuration or STA access. After the scanning enhancement function is enabled, the current radio works with the third radio to perform radio scanning and provide scanning feature data. When multiple radios collect and provide data simultaneously, the scanning performance and precision are improved. After the scanning enhancement function is disabled, scanning feature data on the current radio is provided by the third radio. The third radio does not involve in scanning. Therefore, scanning features on the radio do not affect STA access.

The third radio of these APs supports scanning only on the single spatial stream. When functions such as location and WIDS detection, it is recommended that the scanning enhancement function be enabled if high performance and precision are required.

When services that are sensitive to packet loss or delay (for example, voice or video services) are used, it is recommended that the scanning enhancement function be disabled.

Example

Enable the scanning enhancement function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-enhancement
```

11.4.96 scan-interval

Function

The **scan-interval** command sets an air scan interval.

The **undo scan-interval** command restores the default air scan interval.

By default, the air scan interval is 10000 ms.

Format

scan-interval *scan-time*

undo scan-interval

Parameters

Parameter	Description	Value
scan-time	Specifies an air scan interval. With a smaller air scan interval, more sampling data can be obtained, which increases the performance overhead in turn. An air scan interval of less than 2000 ms may affect service running.	The value is an integer that ranges from 300 to 600000, in milliseconds.

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an air scan interval is specified using the **scan-interval** command, APs scan channels at the specified intervals.

When spectrum analysis is used, the air scan interval range of 3s to 10s and the air scan period of 100 ms are recommended. This helps you obtain sufficient sampled data without compromising normal services.

Precautions

The air scan interval also applies to radio calibration, smart roaming, spectrum analysis, WLAN location, and WIDS functions.

If the customer has high requirements on real-time data analysis, configure a small air scan interval using the **scan-interval** command to improve the scan frequency. However, higher scan frequency indicates much larger impact on the services.

Ensure that the air scan interval meets the following condition: scan-interval ≥ beacon-interval + 100 ms

In vehicle-ground communication scenarios, the air scan interval ranges from 300 ms to 1000 ms.

Example

Set the air scan interval to 3000 ms for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-interval 3000
```

11.4.97 scan-period

Function

The **scan-period** command sets the air scan period.

The **undo scan-period** command restores the default air scan period.

By default, the air scan period is 60 ms.

Format

scan-period *scan-time*

undo scan-period

Parameters

Parameter	Description	Value
scan-time	Specifies the air scan period.	The value is an integer that ranges from 60 to 100, in milliseconds.

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the air scan period is configured using the **scan-period** command, an AP continuously scans surrounding radio signals in the configured period. After the period expires, the AP reports the collected information to an AC or server. The information is used for radio calibration, smart roaming, spectrum analysis, WLAN location, or WIDS data analysis.

When spectrum analysis is used, the air scan interval range of 3s to 10s and the air scan period of 100 ms are recommended. This helps you obtain sufficient sampled data without compromising normal services.

Precautions

A longer air scan period indicates more collected data and a more accurate data analysis result. However, if the air scan period is set too large, WLAN services are affected. You are advised to use the default value.

Example

Set the air scan period to 80 ms for APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] air-scan-profile name test
[HUAWEI-wlan-air-scan-prof-test] scan-period 80
```

11.4.98 scene

Function

The **scene** command binds a scenario profile to an AP group or a single AP.

The **undo scene** command unbinds a scenario profile from an AP group or a single AP.

By default, no scenario profile is bound to an AP group or a single AP.

Format

scene *scene-name*

undo scene

Parameters

Parameter	Description	Value
scene-name	Specifies the name of a scenario profile.	The value is of the enumerated type. - multi-partition-cross-room: indicates an indoor multi-partition cross-room deployment scenario (capacity first). - multi-partition-cross-room-cov: indicates an indoor multi-partition cross-room deployment scenario (coverage first). - automated-guided-vehicle: indicates an AGV scenario. - high-density-stadium: indicates a high-density stadium scenario. - indoor-high-density: indicates an indoor high-density coverage scenario. - indoor-low-density: indicates an indoor low-density coverage scenario. - indoor-multi-partition: indicates an indoor multi-partition coverage scenario. - indoor-normal-density: indicates an indoor common coverage scenario. - industrial-manufacturing: indicates an industrial manufacturing scenario. - outdoor-continuous: indicates an outdoor continuous coverage scenario.

Parameter	Description	Value
		- virtual-reality: indicates a VR scenario.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In actual scenarios, there are fixed recommended settings for radio parameters such as the channel, bandwidth, and transmit power. Recommended settings for these typical scenarios are configured into scenario profiles. When configuring wireless services, you only need to bind a scenario profile to an AP group or a single AP, greatly simplifying service configuration.

To view the parameter settings in preset scenario profiles, run the **display wlan scene** command. If the value of a parameter is empty, a hyphen (-) is displayed, indicating that the parameter is not configured.

Precautions

- The service parameters on an AP take effect in the following sequence: Parameters in the scenario profile bound to an AP > Parameters directly configured for an AP > Parameters in the scenario profile identified and delivered by the analyzer to an AP > Parameters in the scenario profile bound to the AP group to which the AP belongs > Parameters directly configured for the AP group to which the AP belongs.

  The calibration bandwidth of the 5 GHz frequency band is used as an example. Assume that the parameter value in a scenario profile **a** bound to the AP is empty, the parameter value in scenario profile **b** bound to the AP group is **B**, the parameter value corresponding to scenario profile **c** identified and delivered by the analyzer to the AP is **C**, the parameter value configured for an AP is **D**, and the parameter value configured for an AP group is **E**. Then the parameter value takes effect on the AP in the following sequence: null > **D** > **C** > **B** > **E**. That is, the parameter value that takes effect is **D**.
- The wireless service parameters in a scenario profile contain the radio calibration parameter set (**Radio calibration**). After a scenario profile is configured, the radio calibration parameter settings take effect from the next radio calibration.
- Although a series of radio calibration parameters are predefined in a scenario profile, the channel, bandwidth, and transmit power are still restricted by the country code during radio calibration. Bandwidth selection depends on the number of channels allowed by the country code.

Assume that the calibration bandwidth defined in the scenario profile is A, the number of available channels under this bandwidth is B in the country code, and the calibration bandwidth configured in the regulatory domain profile is C.

- If B is greater than or equal to 3, the calibration bandwidth A takes effect.
- If B is smaller than 3, the smaller value between A and C is used as the calibration bandwidth.

Example

Bind the scenario profile **multi-partition-cross-room** to the AP group **mygroup**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name mygroup
[HUAWEI-wlan-ap-group-mygroup] scene multi-partition-cross-room
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.4.99 smart-antenna { enable | disable }

Function

The **smart-antenna** { **enable** | **disable** } command enables or disables the smart antenna selection algorithm for an AP.

The **undo smart-antenna** command restores the smart antenna selection algorithm of an AP to the default state.

By default, the smart antenna selection algorithm is enabled.

Format

smart-antenna { **enable** | **disable** }

undo smart-antenna

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With the smart antenna selection algorithm, an AP can adjust the antenna mode for transmitting signals based on STA locations and select a proper combination of antenna arrays to communicate with STAs. This improves the RSSIs of STAs and improves user experience.

Precautions

The smart antenna selection algorithm is supported only by the following APs:

- AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 5760-51, AirEngine 6760-X1, and AirEngine 8760-X1-PRO

Example

Enable the smart antenna selection algorithm for an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna enable
```

11.4.100 smart-antenna throughput-triggered-training

Function

The **smart-antenna throughput-triggered-training** command sets a sudden performance change threshold that triggers smart antenna training.

The **undo smart-antenna throughput-triggered-training** command restores the default sudden performance change threshold that triggers smart antenna training.

The default sudden performance change threshold that triggers smart antenna training is 10%.

Format

smart-antenna throughput-triggered-training threshold *threshold*

undo smart-antenna throughput-triggered-training threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies a sudden performance change threshold that triggers antenna training.	The value is an integer that ranges from 10 to 50, in percentage. In addition, the value must be a multiple of 10.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In a smart antenna system, the device monitors performance (throughput) of transmit ends. If the detected throughput of a transmit end exceeds the sudden performance change threshold specified using the **smart-antenna throughput-triggered-training** command, a new round of antenna training is triggered.

- In a good air interface environment, set a high sudden performance change threshold to prevent frequent antenna training from affecting user services.
- In a poor air interface environment, set a low sudden performance change threshold to improve the WLAN's anti-interference capability.

Example

Set the sudden performance change threshold that triggers antenna training to 10%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna throughput-triggered-training threshold 10
```

11.4.101 smart-antenna training-interval

Function

The **smart-antenna training-interval** command sets the smart antenna training interval.

The **undo smart-antenna training-interval** command restores the default smart antenna training interval.

The default smart antenna training interval is **auto**, indicating that a smart antenna is trained in self-adaptation mode.

Format

smart-antenna training-interval { *training-interval* | **auto** }

undo smart-antenna training-interval

Parameters

Parameter	Description	Value
training-interval	Indicates the smart antenna training interval.	The value is an integer that ranges from 10 to 600, in seconds.

Parameter	Description	Value
auto	Indicates that a smart antenna is trained in self-adaptation mode.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **smart-antenna training-interval** command to set the smart antenna training interval. When the period since the last round of smart antenna training exceeds the specified interval, a new round of smart antenna training is triggered.

Configure the smart antenna training interval based on actual situations.

- A short antenna training interval causes frequency antenna training and affects user services.
- A long antenna training interval causes the device's failure to switch the antenna combination in time to adapt to WLAN environment changes.

When the default smart antenna training interval is restored, that is, smart antennas are trained in self-adaptation mode, the device adaptively calculates the antenna training interval based on the number of concurrent STAs.

Example

Set the smart antenna training interval to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna training-interval 100
```

11.4.102 smart-antenna training-mpdu-number

Function

The **smart-antenna training-mpdu-number** command sets the number of MAC protocol data units (MPDUs) sent by an AP to a STA during smart antenna training.

The **undo smart-antenna training-mpdu-number** command restores the default number of MPDUs sent by an AP to a STA during smart antenna training.

By default, 640 MPDUs are sent by an AP to a STA during smart antenna training.

Format

smart-antenna training-mpdu-number *training-mpdu-number*

undo smart-antenna training-mpdu-number

Parameters

Parameter	Description	Value
training-mpdu-number	Specifies the number of MPDUs sent by an AP to a STA during smart antenna training.	The value is an integer that ranges from 10 to 1000.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In the smart antenna algorithm, an AP uses different antenna combinations to send training packets for antenna training. During smart antenna training, the transmit end (AP) sends training packets to a receive end (STA). The receive end measures the PER and RSSI in the received packets, and then sends the PER and RSSI to the transmit end. The transmit end collects information about all antenna combinations and corresponding PERs and RSSIs to determine the optimal antenna combination for the receiver.

You can run the **smart-antenna training-mpdu-number** command to set the number of MPDUs sent by an AP to a STA during smart antenna training.

If the traffic rate, bandwidth, and air interface rate of the STA are high, set a small value. Otherwise, set a large value.

Example

Set the number of MPDUs sent by an AP to a STA during smart antenna training to 600.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna training-mpdu-number 600
```

11.4.103 smart-antenna valid-per-scope

Function

The **smart-antenna valid-per-scope** command sets the upper and lower valid packet error rate (PER) thresholds in the smart antenna algorithm.

The **undo smart-antenna valid-per-scope** command restores the default upper and lower valid PER thresholds in the smart antenna algorithm.

The default upper and lower valid PER thresholds are 80% and 20%, respectively.

Format

smart-antenna valid-per-scope { **high-per-threshold** *high-per-threshold* | **low-per-threshold** *low-per-threshold* }

undo smart-antenna valid-per-scope { **high-per-threshold** | **low-per-threshold** }

Parameters

Parameter	Description	Value
high-per-threshold *high-per-threshold*	Specifies the upper valid PER threshold.	The value is an integer that ranges from 50 to 90, in percentage. In addition, the value must be a multiple of 10.
low-per-threshold *low-per-threshold*	Specifies the lower valid PER threshold.	The value is an integer that ranges from 10 to 30, in percentage. In addition, the value must be a multiple of 10.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In the smart antenna algorithm, an AP uses different antenna combinations to send training packets for antenna training. During smart antenna training, the transmit end (AP) sends training packets to a receive end (STA). The receive end measures the PER and RSSI in the received packets, and then sends the PER and RSSI to the transmit end. The transmit end collects information about all antenna combinations and corresponding PERs and RSSIs to determine the optimal antenna combination for the receiver.

The PER is a key basis for the smart antenna algorithm. After proper upper and lower valid PER thresholds are configured, the smart antenna algorithm can select a proper antenna combination to improve the coverage and anti-interference capability of a WLAN in indoor coverage scenarios.

Example

Set the upper valid PER threshold to 80%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] smart-antenna valid-per-scope high-per-threshold 80
```

11.4.104 smart-roam advanced-scan disable

Function

The **smart-roam advanced-scan disable** command disables coordinated scanning in roaming.

The **undo smart-roam advanced-scan disable** command enables coordinated scanning in roaming.

By default, coordinated scanning in roaming is enabled.

Format

smart-roam advanced-scan disable

undo smart-roam advanced-scan disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the roaming steering for sticky STAs, real-time information about neighboring APs is required to determine the target AP. If STAs do not support 802.11k radio resource measurement, you can run the **undo smart-roam advanced-scan disable** command to enable coordinated scanning in roaming. In this way, APs can collect real-time information about neighboring APs through synchronized radio resource measurement, and generate a neighbor AP table of the STAs.

After this function is enabled, radios switch channels to scan STA information while ensuring voice and video services. If voice and video services are affected, you can disable this function.

Prerequisites

The smart roaming or AI roaming function has been enabled.

Example

Enable coordinated scanning in roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] undo smart-roam advanced-scan disable
```

11.4.105 smart-roam { disable | enable | ai-mode }

Function

The **smart-roam { disable | enable | ai-mode }** command enables or disables AI roaming and smart roaming.

The **undo smart-roam** command restores the default state of AI roaming and smart roaming.

By default, AI roaming and smart roaming are enabled.

Format

smart-roam { **disable** | **enable** | **ai-mode** }

undo smart-roam

Parameters

Parameter	Description	Value
disable	Disables AI roaming and smart roaming.	-
enable	Enables smart roaming and disables AI roaming.	-
ai-mode	Enables AI roaming and smart roaming.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a traditional WLAN, when a STA is farther from an AP, the access rate of the STA becomes lower but the STA still associates with the AP without reconnecting the AP or roaming to another AP. This degrades user experience. After the smart roaming function is enabled, when an AP detects that the SNR or access rate of a STA is lower than the specified threshold, the AP sends a BTM packet or Disassociation packet to the STA. The STA then reconnects to the network or roams to an AP with stronger signals.

In practice, the roaming process depends on multiple negotiations between APs and STAs. STAs of different vendors and models have different autonomous behaviors during the negotiation process. As a result, roaming experience cannot be effectively guaranteed. To address this issue, you can enable the AI roaming function. Then the system matches the identified terminal type with the corresponding terminal profile to obtain the behavior characteristics of the terminal during roaming and perform optimization during roaming negotiation. This improves the roaming sensitivity and success rate, enhancing the roaming experience of users.

NOTE

Before enabling the AI roaming function, enable the terminal identification 2.0 function and terminal profiling functions.

If the PMF function is enabled, the AI roaming function does not take effect.

APs must support independent radio scanning to achieve roaming steering based on coordinated measurement. For APs that do not support independent radio scanning, after the AI roaming function is enabled, the STA profiling mechanism is used to perform personalized roaming steering for STAs based on the triggering logic of smart roaming.

Follow-up Procedure

Run the **smart-roam roam-threshold { check-snr | check-rate }** command to configure the trigger mode of smart roaming and the **smart-roam roam-threshold { snr | rate }** command to configure the smart roaming threshold. After that, APs forcibly disconnect STAs with SNR or access rate lower than the threshold.

Example

Enable smart roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
```

11.4.106 smart-roam quick-kickoff back-off-time

Function

The **smart-roam quick-kickoff back-off-time** command sets the backoff time for quickly disconnecting STAs.

The **undo smart-roam quick-kickoff back-off-time** command restores the default backoff time for quickly disconnecting STAs.

By default, the backoff time for quickly disconnecting STAs is 60 seconds.

Format

smart-roam quick-kickoff back-off-time *back-off-time*

undo smart-roam quick-kickoff back-off-time

Parameters

Parameter	Description	Value
back-off-time	Specifies the backoff time for quickly disconnecting STAs.	The value is an integer that ranges from 1 to 600, in seconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled, you can run the **smart-roam quick-kickoff back-off-time** command to set the backoff time for quickly disconnecting STAs to prevent STAs from being disconnected frequently. STAs are not disconnected within the backoff time.

Precautions

Do not set the backoff time to a too small value. Otherwise, STAs may be disconnected frequently.

Example

Set the backoff time for quickly disconnecting STAs to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff back-off-time 60
```

11.4.107 smart-roam quick-kickoff-threshold disable

Function

The **smart-roam quick-kickoff-threshold disable** command disables the function of quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-threshold disable** command enables the function of quickly disconnecting STAs.

By default, the function of quickly disconnecting STAs is enabled.

Format

smart-roam quick-kickoff-threshold disable

undo smart-roam quick-kickoff-threshold disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled and the threshold for quickly disconnecting STAs is specified, the AP disconnects STAs whose SNR or access rate is lower than the specified threshold. The STAs then can connect to or roam to another AP with stronger signals.

Follow-up Procedure

Run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command to set the mode for triggering the function of quickly disconnecting STAs, and the **smart-roam quick-kickoff-threshold** command to set the threshold for quickly disconnecting STAs. The AP will disconnect STAs whose SNR or access rate is lower the specified threshold.

Example

Enable the function of quickly disconnecting STAs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
```

11.4.108 smart-roam quick-kickoff-threshold { check-snr | check-rate }

Function

The **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command sets the mode for triggering the function of quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-threshold** command restores the default mode for triggering the function of quickly disconnecting STAs.

The default mode for triggering the function of quickly disconnecting STAs is **check-snr**.

Format

smart-roam quick-kickoff-threshold { **check-snr** | **check-rate** }*

undo smart-roam quick-kickoff-threshold

Parameters

Parameter	Description	Value
check-snr	Specifies that the function of quickly disconnecting STAs is triggered by checking the SNR of STAs.	-
check-rate	Specifies that the function of quickly disconnecting STAs is triggered by checking the rate of STAs. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled, you can run the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command to set the mode for triggering the function of quickly disconnecting STAs, and set the threshold for quickly disconnecting STAs. When the SNR or access rate of a STA detected by an AP is lower than the specified threshold, the AP disconnects the STA. The STA then can connect to or roam to another AP with stronger signals.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

Follow-up Procedure

Run the **smart-roam quick-kickoff-threshold** command to set the threshold for quickly disconnecting STAs.

Example

Set the mode for triggering the function of quickly disconnecting STAs to **check-rate**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold check-rate
```

11.4.109 smart-roam quick-kickoff-snr check-interval

Function

The **smart-roam quick-kickoff-snr check-interval** command configures the interval for checking the SNR to determine whether to quickly disconnect STAs.

The **undo smart-roam quick-kickoff-snr check-interval** command restores the default interval for checking the SNR to determine whether to quickly disconnect STAs.

The default interval for checking the SNR to determine whether to quickly disconnect STAs is 500 ms.

Format

smart-roam quick-kickoff-snr check-interval *check-interval*

undo smart-roam quick-kickoff-snr check-interval

Parameters

Parameter	Description	Value
check-interval *check-interval*	Specifies an interval for checking the SNR to determine whether to quickly disconnect STAs.	The value is an integer that ranges from 300 to 3000, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the mode for quickly disconnecting STAs is set to **check-snr**, you can run the **smart-roam quick-kickoff-snr check-interval** command to set the interval for checking the SNR to determine whether to quickly disconnect STAs. A shorter interval allows the system to determine whether to disconnect STAs more quickly.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

Example

Set the interval for checking the SNR to determine whether to quickly disconnect STAs to 600 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-snr check-interval 600
```

11.4.110 smart-roam quick-kickoff-snr p-n criteria

Function

The **smart-roam quick-kickoff-snr p-n criteria** command configures the PN threshold for quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-snr p-n criteria** command restores the default PN threshold for quickly disconnecting STAs.

By default, the number of PN observation times is 6, and the number of times criteria are met is 4.

Format

smart-roam quick-kickoff-snr p-n criteria observe-time *observe-value* **qualify-time** *qualify-value*

undo smart-roam quick-kickoff-snr p-n criteria

Parameters

Parameter	Description	Value
observe-time *observe-value*	Specifies the number of PN observation times.	The value is an integer that ranges from 1 to 10.

Parameter	Description	Value
qualify-time *qualify-value*	Specifies the number of PN observation times criteria are met.	The value is an integer that ranges from 1 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the mode for quickly disconnecting STAs is set to **check-snr**, you can run the **smart-roam quick-kickoff-snr p-n criteria** command to configure the PN threshold for quickly disconnecting STAs.

PN criteria: When N conditions are met in the P range, an event is triggered. Assume that the value of **observe-value** is 6 and that of **qualify-value** is 4, and the interval for checking the SNR to determine whether to quickly disconnect STAs is 500 ms. The system detects the SNR of a STA for six consecutive times and calculates the average SNR value. If the average value is smaller than the total average value four times, the STA is forced offline.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

Precautions

The value of **observe-value** must be greater than or equal to that of **qualify-value**.

Example

Set the value of **observe-value** to 10 and that of **qualify-value** to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-snr p-n criteria observe-time 10 qualify-time 5
```

11.4.111 smart-roam quick-kickoff-threshold

Function

The **smart-roam quick-kickoff-threshold** command sets the threshold for quickly disconnecting STAs.

The **undo smart-roam quick-kickoff-threshold** command restores the default threshold for quickly disconnecting STAs.

By default, the SNR-based threshold for quickly disconnecting STAs is 15 dB, and the rate-based threshold is 20%.

Format

smart-roam quick-kickoff-threshold { **snr** *snr-threshold* | **rate** *rate-threshold* }

undo smart-roam quick-kickoff-threshold { **snr** | **rate** }

Parameters

Parameter	Description	Value
snr *snr-threshold*	Specifies the SNR-based threshold for quickly disconnecting STAs.	The value is an integer that ranges from 5 to 45, in dB. If this parameter is set to the default value, the threshold for quickly disconnecting STAs on the AirEngine 5762-16W is 10 dB.
rate *rate-threshold*	Specifies the rate-based threshold for quickly disconnecting STAs. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of quickly disconnecting STAs is enabled and the threshold for quickly disconnecting STAs is specified for an AP using this command, the AP acquires a STA's SNR or rate from data packets sent from the STA. If the STA's SNR or rate is lower than the specified threshold, the AP forcibly disconnects the STA so that the STA can reinitiate a connection with the AP or roam to another AP with strong signals.

- A large threshold may cause STAs to go offline frequently.
- A small threshold may disable STAs from roaming to an AP with stronger signals.

This command is applicable to scenarios that have high requirements on real-time transmission, such as voice and video scenarios.

Prerequisites

The function of quickly disconnecting STAs has been enabled using the **undo smart-roam quick-kickoff-threshold disable** command.

The mode for triggering the function of quickly disconnecting STAs has been set using the **smart-roam quick-kickoff-threshold { check-snr | check-rate }** command.

Precautions

STAs may be forced to go offline through the smart roaming function or the function of quickly disconnecting STAs. If the SNR-based thresholds for the two functions are both configured, the function with a larger value is preferentially effective.

Example

Set the mode for triggering the function of quickly disconnecting STAs to **check-snr** and the threshold for quickly disconnecting STAs to 20 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] undo smart-roam quick-kickoff-threshold disable
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold check-snr
[HUAWEI-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold snr 20
```

11.4.112 smart-roam roam-threshold { check-snr | check-rate }

Function

The **smart-roam roam-threshold { check-snr | check-rate }** command configures the trigger mode of smart roaming.

The **undo smart-roam roam-threshold** command restores the default trigger mode of smart roaming.

By default, the trigger mode of smart roaming is **check-snr**.

Format

smart-roam roam-threshold { **check-snr** | **check-rate** }*

undo smart-roam roam-threshold

Parameters

Parameter	Description	Value
check-snr	Specifies the trigger mode of smart roaming as **check SNR**.	-
check-rate	Specifies the trigger mode of smart roaming as **check rate**. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the smart roaming function is enabled, the AP forces STAs to log out based on the configured trigger mode and threshold of smart roaming. When an AP receives a STA's data packet, the AP learns the STA's SNR or rate from the data packet. If the STA's SNR or rate is lower than the configured threshold, roaming is triggered. Then, the AP sends a Disassociation frame to the STA so that the STA can reinitiate a connection with the AP or roam to another AP with strong signals.

Prerequisites

Smart roaming or AI roaming has been enabled.

Follow-up Procedure

Run the **smart-roam roam-threshold { snr | rate }** command to configure the smart roaming threshold.

Example

Set the trigger mode of smart roaming to **check-rate**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam roam-threshold check-rate
```

11.4.113 smart-roam roam-threshold { snr | rate }

Function

The **smart-roam roam-threshold { snr | rate }** command sets the smart roaming threshold.

The **undo smart-roam roam-threshold** command restores the default smart roaming threshold.

By default, the SNR threshold for smart roaming is 20 dB, and the rate threshold is 20%.

Format

smart-roam roam-threshold { **snr** *snr-threshold* | **rate** *rate-threshold* }

undo smart-roam roam-threshold { **snr** | **rate** }

Parameters

Parameter	Description	Value
snr *snr-threshold*	Specifies the SNR threshold for smart roaming. If the SNR threshold is 25 dB and noise floor is -95 dBm, a STA's SNR is lower than the threshold when the STA's RSSI is lower than -70 dBm (25 dB + (-95 dBm) = -70 dBm). **NOTE** If the signal strength of a STA is close to the smart roaming threshold, the network experience may be poor. If the default SNR threshold is used and the signal strength of many 2.4 GHz STAs is close to the smart roaming threshold, it is recommended that the 2.4 GHz and 5 GHz radios be bound to different RRM profiles and the SNR threshold be increased to about 25 dB in the RRM profile corresponding to the 2.4 GHz radio. Wait for 1 to 2 minutes and then observe the signal strength and service experience of these STAs.	The value is an integer that ranges from 15 to 45, in dB. If this parameter is set to the default value, the STA roaming threshold on the AirEngine 5762-16W is 15 dB.

Parameter	Description	Value
rate *rate-threshold*	Specifies the rate threshold for smart roaming. The rate here refers to the negotiated rate based on the protocol and signal strength when a STA associates with an AP, instead of the actual rate of the STA. If the maximum capability of the AP and STA is 54 Mbit/s and the rate threshold is 50%, the lower rate threshold is considered 27 Mbit/s (54 Mbit/s x 50% = 27 Mbit/s).	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the smart roaming function is enabled, the AP forces STAs to log out based on the configured trigger mode and threshold of smart roaming. When an AP receives a STA's data packet, the AP learns the STA's SNR or rate from the data packet. If the STA's SNR or rate is lower than the configured threshold, smart roaming is triggered. Then, the AP sends a Disassociation frame to the STA so that the STA can reinitiate a connection with the AP or roam to another AP with strong signals.

- A large threshold may cause STAs to go offline frequently.
- A small threshold may disable STAs from roaming to an AP with stronger signals.

Prerequisites

Smart roaming or AI roaming has been enabled.

The trigger mode of smart roaming has been configured using the **smart-roam roam-threshold { check-snr | check-rate }** command.

Precautions

STAs may be forced to go offline through the smart roaming function or the function of quickly disconnecting STAs. If the SNR-based thresholds for the two functions are both configured, the function with a larger value is preferentially effective.

Example

Set the trigger mode of smart roaming to **check-snr** and set the smart roaming threshold to 25 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam roam-threshold check-snr
[HUAWEI-wlan-rrm-prof-default] smart-roam roam-threshold snr 25
```

11.4.114 smart-roam snr-margin

Function

The **smart-roam snr-margin** command sets the RSSI difference thresholds that trigger STA roaming steering.

The **undo smart-roam snr-margin** command restores the default RSSI difference thresholds that trigger STA roaming steering.

By default, the upper and lower RSSI difference thresholds that trigger STA roaming steering are 12 dB and 10 dB, respectively.

Format

smart-roam snr-margin high-level-margin *high-level-margin* **low-level-margin** *low-level-margin*

undo smart-roam snr-margin

Parameters

Parameter	Description	Value
high-level-margin *high-level-margin*	Specifies the upper RSSI difference threshold for triggering STA roaming steering.	The value is an integer that ranges from 10 to 20, in dB.
low-level-margin *low-level-margin*	Specifies the lower RSSI difference threshold for triggering STA roaming steering.	The value is an integer that ranges from 3 to 15, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In smart roaming and AI roaming scenarios, you can configure the thresholds for determining whether to steer STA roaming. When determining whether to steer a STA to roam to a neighboring AP, the AP compares the RSSIs of the STA on the neighboring AP with that on the current AP, which are reported by the STA through coordinated measurement. If the RSSI difference is higher than a specified threshold, that is, the STA has a significantly increased RSSI after associating with the neighboring AP, the AP steers the STA to roam to the neighboring AP.

The parameters **low-level-margin** and **high-level-margin** are used to determine whether to steer sticky STAs and common STAs, respectively, to roam to neighboring APs in smart roaming scenarios. In most cases, you are advised to set **high-level-margin** larger than **low-level-margin** so that sticky STAs can roam to neighboring APs with better experience as soon as possible.

In AI roaming scenarios based on coordinated measurement, only **high-level-margin** is used to determine whether to steer STAs to roam to neighboring APs.

The default difference thresholds are recommended. If APs are deployed close to each other and have high transmit power, set larger values for the upper and lower RSSI difference thresholds.

Prerequisites

Smart roaming or AI roaming has been enabled.

Example

Set the upper and lower RSSI difference thresholds that trigger STA roaming steering to 10 dB and 6 dB, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam snr-margin high-level-margin 10 low-level-margin 6
```

11.4.115 smart-roam unable-roam-client expire-time

Function

The **smart-roam unable-roam-client expire-time** command sets the aging time of the "unable to roam" record for STAs.

The **undo smart-roam unable-roam-client expire-time** command restores the default aging time of the "unable to roam" record for STAs.

By default, the aging time of an "unable to roam" record is 30 minutes.

Format

smart-roam unable-roam-client expire-time *expire-time*

undo smart-roam unable-roam-client expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of the "unable to roam" record.	The value is an integer that ranges from 30 to 2880, in minutes.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After smart roaming is enabled, you can run the **smart-roam unable-roam-client expire-time** command to set the aging time of the "unable to roam" record for STAs. When the device requests a STA to roam but the STA keeps sending association requests to the original AP or does not initiate an association request, the device records the terminal as "unable to roam" and does not trigger STA roaming within the specified time. After the aging time is reached, the "unable to roam" record for STAs is automatically cleared, and the system can trigger roaming of the STAs.

A STA is recorded as "unable to roam" due to the following reasons:

- Due to different software configurations, some STAs preferentially send association requests to APs with which they have once associated.
- In some environments, STAs cannot scan APs with strong signals.
- STAs enter the dormancy state and do not roam once they are forcibly disconnected.

The aging time to configure varies for different reasons. A large aging time is used for the software configuration reason so that the AP will trigger roaming of the STAs as less as possible. However, a small aging time is used in other situations so that the AP will attempt to trigger roaming of the STAs marked "unable to roam."

Prerequisites

Smart roaming or AI roaming has been enabled.

Example

Set the aging time of the "unable to roam" record to 50 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
```

```
[HUAWEI-wlan-rrm-prof-default] smart-roam enable
[HUAWEI-wlan-rrm-prof-default] smart-roam unable-roam-client expire-time 50
```

11.4.116 spatial-reuse disable

Function

The **spatial-reuse disable** command disables the spatial reuse (SR) function.

The **undo spatial-reuse disable** command enables the SR function.

By default, the SR function is enabled.

NOTE

The SR function is not supported by the following APs:

- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762

Format

spatial-reuse disable

undo spatial-reuse disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

The BSS coloring function has been enabled.

Precautions

Disabling the BSS coloring function will automatically disable the spatial reuse (SR) function.

Example

Disable the SR function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] spatial-reuse disable
```

11.4.117 sta-load-balance dynamic btm-fail-times

Function

The **sta-load-balance dynamic btm-fail-times** command sets the maximum number of attempts to steer STAs in BTM mode.

The **undo sta-load-balance dynamic btm-fail-times** command restores the default maximum number of attempts to steer STAs in BTM mode.

By default, the maximum number of attempts to steer STAs in BTM mode is 5.

Format

sta-load-balance dynamic btm-fail-times *btm-fail-times*

undo sta-load-balance dynamic btm-fail-times

Parameters

Parameter	Description	Value
btm-fail-times	Specifies the maximum number of attempts to steer STAs in BTM mode.	The value is an integer that ranges from 0 to 10. The value 0 indicates that the BTM mode is not used to steer STAs.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device preferentially uses the BTM mode to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in BTM mode after multiple attempts. You can run the **sta-load-balance dynamic btm-fail-times** command to set the maximum number of attempts to steer STAs in BTM mode. If the number of attempts exceeds the specified value, the device attempts to steer STAs in deauthentication mode.

Precautions

You are advised to retain the default value. If the success rate of STA steering in BTM mode is low, you can set a smaller value to improve the steering efficiency.

Example

Set the maximum number of attempts to steer STAs in BTM mode to 4 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic btm-fail-times 4
```

11.4.118 sta-load-balance dynamic deauth-fail-times

Function

The **sta-load-balance dynamic deauth-fail-times** command sets the maximum number of attempts to steer STAs in deauthentication mode.

The **undo sta-load-balance dynamic deauth-fail-times** command restores the default maximum number of attempts to steer STAs in deauthentication mode.

By default, the maximum number of attempts to steer STAs in deauthentication mode is 0.

Format

sta-load-balance dynamic deauth-fail-times *deauth-fail-times*

undo sta-load-balance dynamic deauth-fail-times

Parameters

Parameter	Description	Value
deauth-fail-times	Specifies the maximum number of attempts to steer STAs in deauthentication mode.	The value is an integer that ranges from 0 to 5. The value 0 indicates that the deauthentication mode is not used to steer STAs.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device attempts to use the 802.11v and deauthentication modes to trigger STA steering to the target AP. Due to differences of STAs, some STAs can be successfully steered in deauthentication mode after multiple attempts. You can run the **sta-load-balance dynamic deauth-fail-times** command to set the maximum number of attempts to steer STAs in deauthentication mode. If the number of attempts exceeds the specified value, STAs cannot be steered.

Precautions

You are advised to retain the default value. If the success rate of STA steering in deauthentication mode is low or STA services are affected, set the parameter value to 0 to disable STA steering in deauthentication mode.

Example

Set the maximum number of attempts to steer STAs in deauthentication mode to 1 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic deauth-fail-times 1
```

11.4.119 sta-load-balance dynamic disable

Function

The **sta-load-balance dynamic disable** command disables the dynamic load balancing function.

The **undo sta-load-balance dynamic disable** command enables the dynamic load balancing function.

By default, the dynamic load balancing function is enabled.

Format

sta-load-balance dynamic disable

undo sta-load-balance dynamic disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Static load balancing limits the maximum number of AP radios to 16 and allows only radios on the same frequency band to join a load balancing group.

Additionally, a load balancing group needs to be manually specified. Dynamic load balancing overcomes the limitations of static load balancing.

After a STA connects to an AP, the AC checks whether the AP reaches the load balancing threshold, and determines whether to steer the STA to a neighboring AP that meets load balancing requirements based on the load balancing algorithm.

Example

Disable dynamic load balancing.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic disable
```

11.4.120 sta-load-balance dynamic sta-number gap-threshold

Function

The **sta-load-balance dynamic sta-number gap-threshold** command sets the load difference threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic sta-number gap-threshold** command restores the default load difference threshold for dynamic load balancing based on the number of users.

By default, the load difference threshold of a dynamic load balancing group is specified based on the number of users, and the default value is 3.

Format

sta-load-balance dynamic sta-number gap-threshold { **percentage** *percentage-value* | **number** *number-value* }

undo sta-load-balance dynamic sta-number gap-threshold

Parameters

Parameter	Description	Value
percentage *percentage-value*	Specifies the load difference threshold for dynamic load balancing based on the percentage of users.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the percentages of users on radios.

Parameter	Description	Value
number *number-value*	Specifies the load difference threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 20. It indicates the threshold of the load difference among radios in a load balancing group. The load difference refers to the difference between the numbers of users on radios.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user requests to connect to an AP, the AP counts the total number of access users on all radios. If the total number of access users does not exceed the start threshold configured using the **sta-load-balance dynamic sta-number start-threshold** command, the AP does not implement dynamic load balancing. The AP implements dynamic load balancing only when the total number of access users on all radios exceeds the start threshold.

The following load balancing algorithm is used after the user access to determine whether to steer the user to a new AP:

One of the conditions for steering a user to a new AP is that the radio of the target load is lower than that of the current access radio. The radio load is identified by the number or percentage (Number of users associated with the current radio/Maximum number of access users supported by the radio x 100%) of access users. If the load difference between the target radio and current radio exceeds the specified threshold, the condition is met.

NOTE

The start threshold and load difference threshold for dynamic load balancing are used to adjust the sensitivity for triggering load balancing, and the default values are recommended. If the start and load difference thresholds are set low, load balancing becomes far easier to be triggered. As a result, STAs are frequently switched between APs, affecting user experience. If the start and load difference thresholds are set high, the load balancing mechanism may become invalid.

Precautions

If you configure the load difference threshold based on both the number of users and the percentage of users, only the latest configuration takes effect.

Example

Set the load difference threshold for dynamic load balancing based on the number of users to 25% in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic sta-number gap-threshold percentage 25
```

11.4.121 sta-load-balance dynamic sta-number start-threshold

Function

The **sta-load-balance dynamic sta-number start-threshold** command sets the start threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic sta-number start-threshold** command restores the default start threshold for dynamic load balancing based on the number of users.

By default, the start threshold for dynamic load balancing based on the number of users is 10.

Format

sta-load-balance dynamic sta-number start-threshold *start-threshold*

undo sta-load-balance dynamic sta-number start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 40.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a user requests to connect to an AP, the AP counts the total number of access users on all radios. If the number of access users on the requested radio does not exceed the start threshold, the AP does not implement dynamic load balancing based on the number of users. The AP implements dynamic load balancing based on the number of users only after the number of access users exceeds the start threshold.

NOTE

The start and load difference thresholds for dynamic load balancing configured using the **sta-load-balance dynamic sta-number gap-threshold** command can be used to adjust sensitivity for triggering load balancing. The default values are recommended in typical scenarios. A higher threshold is recommended in high-density scenarios. If the start and load difference thresholds are set low, load balancing becomes far easier to be triggered. As a result, STAs are frequently switched between APs, affecting user experience. If the start and load difference thresholds are set high, the load balancing mechanism may become invalid.

Example

Set the start threshold for dynamic load balancing based on the number of users to 20 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic sta-number start-threshold 20
```

11.4.122 sta-load-balance static-group

Function

The **sta-load-balance static-group** command creates a static load balancing group and displays the static load balancing group view.

The **undo sta-load-balance static-group** command deletes a static load balancing group.

By default, no static load balancing group is configured.

Format

sta-load-balance static-group name *group-name*

undo sta-load-balance static-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a load balancing group.	The value is a string of 1 to 35 plaintext characters. It does not contain any question mark (?) and cannot begin or end with double quotation marks (" ").
all	Deletes all static load balancing groups.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In static load balancing mode, APs providing the same services are manually added to a load balancing group. When a STA needs to access a WLAN, it sends an Association Request packet to an AC through an AP. The AC determines whether to allow access from the STA according to the load balancing algorithm.

To configure static load balancing, run the **sta-load-balance static-group** command in the WLAN view to create a static load balancing group and **member (static load balancing group view)** command to add APs to the group.

Example

Configure the static load balancing group named **new**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name new
[HUAWEI-wlan-sta-lb-static-new]
```

11.4.123 sta-number start-threshold

Function

The **sta-number start-threshold** command sets the start threshold for load balancing based on the number of users in a static load balancing group.

The **undo sta-number start-threshold** command deletes the configured start threshold for load balancing based on the number of users in a static load balancing group.

By default, the start threshold for load balancing based on the number of users in a static load balancing group is 10.

Format

sta-number start-threshold *start-threshold-value*

undo sta-number start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold-value*	Specifies the start threshold for load balancing based on the number of users in a static load balancing group.	The value is an integer that ranges from 1 to 40.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to set the start threshold for load balancing based on the number of users in a static load balancing group. If the load on a radio does not reach the start threshold, the device does not implement load balancing control on access STAs.

Example

Set the start threshold for load balancing based on the number of users in the static load balancing group to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] sta-number start-threshold 5
```

11.4.124 sta-load-balance dynamic probe-report interval

Function

The **sta-load-balance dynamic probe-report interval** command sets the interval for reporting Probe frames.

The **undo sta-load-balance dynamic probe-report interval** command restores the default interval for reporting Probe frames.

By default, Probe frames are reported at an interval of 120 seconds.

Format

sta-load-balance dynamic probe-report interval *interval*

undo sta-load-balance dynamic probe-report interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for reporting Probe frames.	The value is an integer that ranges from 30 to 300, in seconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP collects information about neighboring APs of STAs and reports the information to the AC for determining the target APs to which the STAs will roam. You can run this command to set the interval at which an AP reports information about neighboring APs of STAs.

Precautions

You are advised to retain the default value. If the device has high performance pressure, you can set a longer interval.

Example

Set the interval for reporting Probe frames to 125 seconds in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic probe-report interval 125
```

11.4.125 sta-load-balance dynamic rssi-diff-gap

Function

The **sta-load-balance dynamic rssi-diff-gap** command sets the RSSI difference threshold for members in a dynamic load balancing group.

The **undo sta-load-balance dynamic rssi-diff-gap** command restores the default RSSI difference threshold of members in a dynamic load balancing group.

By default, the RSSI difference threshold of members in a dynamic load balancing group is 5 dB.

Format

sta-load-balance dynamic rssi-diff-gap *diff-gap-threshold*

undo sta-load-balance dynamic rssi-diff-gap

Parameters

Parameter	Description	Value
diff-gap-threshold	Specifies the RSSI difference threshold of members in a dynamic load balancing group.	The value is an integer that ranges from 0 to 15, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To achieve load balancing, an AP may steer connected STAs to other APs with smaller RSSIs. If the RSSI of the AP with which a STA currently associates minus the RSSI of the target AP is larger than the specified RSSI difference threshold, the STA is denied from being steered to the target AP; otherwise, the STA can be steered to the target AP.

Precautions

If STAs have high signal quality deterioration tolerance for the target AP, you can set a larger RSSI difference threshold to achieve better load balancing effect. If STAs have low signal quality deterioration tolerance for the target AP, set a smaller RSSI difference threshold. You are advised to retain the default value.

Example

Set the RSSI difference threshold of members in a dynamic load balancing group to 6 dB in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic rssi-diff-gap 6
```

11.4.126 sta-load-balance dynamic rssi-threshold

Function

The **sta-load-balance dynamic rssi-threshold** command sets an RSSI threshold for member devices in a dynamic load balancing group.

The **undo sta-load-balance dynamic rssi-threshold** command restores the default RSSI threshold of member devices in a dynamic load balancing group.

By default, the RSSI threshold of member devices in a dynamic load balancing group is –65 dBm.

Format

sta-load-balance dynamic rssi-threshold *rssi-threshold*

undo sta-load-balance dynamic rssi-threshold

Parameters

Parameter	Description	Value
rssi-threshold	Specifies the RSSI threshold of member devices in a dynamic load balancing group.	The value is an integer that ranges from –75 to –55, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RSSI threshold of member devices in a dynamic load balancing group is configured, an AP compares the RSSI of a STA with the configured RSSI threshold after receiving the Probe Request packet sent by the STA. If the STA's RSSI exceeds the threshold, the AP reports STA information to the AC, and the AP is added to the dynamic load balancing group. If the STA's RSSI does not exceed the threshold, the AP directly filters STA information and does not report the information to the AC, and the AP is not added to the dynamic load balancing group.

Setting an RSSI threshold for member devices in a dynamic load balancing group is to filter APs with weak signals, so that STAs can be load-balanced between APs with better signals. This prevents STAs from associating with APs with weak signals but light loads. This function does not affect STAs' going online.

Example

Set the RSSI threshold for member devices in a dynamic load balancing group to –70 dBm in the RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic rssi-threshold -70
```

11.4.127 sta-load-balance dynamic steer-restrict auth-threshold

Function

The **sta-load-balance dynamic steer-restrict auth-threshold** command sets the maximum number of times non-target APs suppress authentication of STAs during STA steering.

The **undo sta-load-balance dynamic steer-restrict auth-threshold** command restores the default maximum number of times non-target APs suppress authentication of STAs during STA steering.

By default, the maximum number of times non-target APs suppress authentication of STAs during STA steering is 0.

Format

sta-load-balance dynamic steer-restrict auth-threshold *auth-threshold*

undo sta-load-balance dynamic steer-restrict auth-threshold

Parameters

Parameter	Description	Value
auth-threshold	Specifies the maximum number of times non-target APs suppress authentication of STAs during STA steering.	The value is an integer that ranges from 0 to 5.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict auth-threshold** command to set the maximum number of times non-target APs suppress authentication of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress authentication of STAs during STA steering to 1 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic steer-restrict auth-threshold 1
```

11.4.128 sta-load-balance dynamic steer-restrict probe-threshold

Function

The **sta-load-balance dynamic steer-restrict probe-threshold** command sets the maximum number of times non-target APs suppress probing of STAs during STA steering.

The **undo sta-load-balance dynamic steer-restrict probe-threshold** command restores the default maximum number of times non-target APs suppress probing of STAs during STA steering.

By default, the maximum number of times non-target APs suppress probing of STAs during STA steering is 5.

Format

sta-load-balance dynamic steer-restrict probe-threshold *probe-threshold*

undo sta-load-balance dynamic steer-restrict probe-threshold

Parameters

Parameter	Description	Value
probe-threshold	Specifies the maximum number of times non-target APs suppress probing of STAs during STA steering.	The value is an integer that ranges from 0 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict probe-threshold** command to set the maximum number of times non-target APs suppress probing of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress probing of STAs during STA steering to 4 in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic steer-restrict probe-threshold 4
```

11.4.129 sta-load-balance dynamic steer-restrict restrict-time

Function

The **sta-load-balance dynamic steer-restrict restrict-time** command sets the duration within which non-target APs suppress association of STAs during STA steering.

The **undo sta-load-balance dynamic steer-restrict restrict-time** command restores the default duration within which non-target APs suppress association of STAs during STA steering.

By default, the duration within which non-target APs suppress association of STAs during STA steering is 5 seconds.

Format

sta-load-balance dynamic steer-restrict restrict-time *restrict-time*

undo sta-load-balance dynamic steer-restrict restrict-time

Parameters

Parameter	Description	Value
restrict-time	Specifies the duration within which non-target APs suppress association of STAs during STA steering.	The value is an integer that ranges from 0 to 10, in seconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict restrict-time** command to set the duration within which non-target APs suppress association of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the duration within which non-target APs suppress association of STAs during STA steering to 4 seconds in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] sta-load-balance dynamic steer-restrict restrict-time 4
```

11.4.130 sta-profiling disable

Function

The **sta-profiling disable** command disables the STA profiling function.

The **undo sta-profiling disable** command enables the STA profiling function.

By default, the STA profiling function is enabled.

Format

sta-profiling disable

undo sta-profiling disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

On a traditional WLAN, when a STA is far away from an AP, the signal strength of the STA gradually weakens and the Internet access rate of the STA becomes lower and lower. If the STA is always associated with an existing AP, user experience deteriorates. With the smart roaming mechanism, the system can automatically steer STAs encountered with poor network quality to APs providing better signals. In practice, the roaming process depends on multiple negotiations between APs and STAs. STAs of different vendors and models have different autonomous behaviors during the negotiation process. As a result, roaming experience cannot be effectively guaranteed. After the STA profiling function is enabled, the system can create profiles for STAs of this type based on the STA behaviors and learn how to steer roaming for these STAs more effectively. This improves the roaming sensitivity and success rate, enhancing the roaming experience of users.

Example

Disable the STA profiling function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-profiling disable
```

11.4.131 steer-restrict auth-threshold

Function

The **steer-restrict auth-threshold** command sets the maximum number of times non-target APs suppress authentication of STAs during STA steering.

The **undo steer-restrict auth-threshold** command restores the default maximum number of times non-target APs suppress authentication of STAs during STA steering.

By default, the maximum number of times non-target APs suppress authentication of STAs during STA steering is 0.

Format

steer-restrict auth-threshold *auth-threshold*

undo steer-restrict auth-threshold

Parameters

Parameter	Description	Value
auth-threshold	Specifies the maximum number of times non-target APs suppress authentication of STAs during STA steering.	The value is an integer that ranges from 0 to 5.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict auth-threshold** command to set the maximum number of times non-target APs suppress authentication of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress authentication of STAs during STA steering to 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] steer-restrict auth-threshold 1
```

11.4.132 steer-restrict probe-threshold

Function

The **steer-restrict probe-threshold** command sets the maximum number of times non-target APs suppress probing of STAs during STA steering.

The **undo steer-restrict probe-threshold** command restores the default maximum number of times non-target APs suppress probing of STAs during STA steering.

By default, the maximum number of times non-target APs suppress probing of STAs during STA steering is 5.

Format

steer-restrict probe-threshold *probe-threshold*

undo steer-restrict probe-threshold

Parameters

Parameter	Description	Value
probe-threshold	Specifies the maximum number of times non-target APs suppress probing of STAs during STA steering.	The value is an integer that ranges from 0 to 10.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict probe-threshold** command to set the maximum number of times non-target APs suppress probing of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the maximum number of times non-target APs suppress probing of STAs during STA steering to 4.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] steer-restrict probe-threshold 4
```

11.4.133 steer-restrict restrict-time

Function

The **steer-restrict restrict-time** command sets the duration within which non-target APs suppress association of STAs during STA steering.

The **undo steer-restrict restrict-time** command restores the default duration within which non-target APs suppress association of STAs during STA steering.

By default, the duration within which non-target APs suppress association of STAs during STA steering is 5 seconds.

Format

steer-restrict restrict-time *restrict-time*

undo steer-restrict restrict-time

Parameters

Parameter	Description	Value
restrict-time	Specifies the duration within which non-target APs suppress association of STAs during STA steering.	The value is an integer that ranges from 0 to 10, in seconds.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA is triggered to steer to a specified target AP, non-target APs will suppress association of the STA temporarily to improve the STA's steering success rate. You can run the **sta-load-balance dynamic steer-restrict restrict-time** command to set the duration within which non-target APs suppress association of STAs during STA steering.

Precautions

You can set a larger value of this parameter to improve the STAs' steering success rate, which, however, may affect users' network experience.

The default value is applicable to mainstream STAs. You are advised to retain the default value. If users' service experience deteriorates due to STA steering, set a smaller value for this parameter.

Example

Set the duration within which non-target APs suppress association of STAs during STA steering to 4 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-load-balance static-group name coco
[HUAWEI-wlan-sta-lb-static-coco] steer-restrict restrict-time 4
```

11.4.134 terminal-identify disable

Function

The **terminal-identify disable** command disables the terminal identification 2.0 function on an AP.

The **undo terminal-identify disable** command enables the terminal identification 2.0 function on an AP.

By default, the terminal identification 2.0 function is enabled on an AP.

Format

terminal-identify disable

undo terminal-identify disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

After a terminal accesses an AP enabled with the terminal identification 2.0 function, the system extracts terminal type information from the DHCP, mDNS, and HTTP packets from the terminal to identify the terminal type.

NOTE

The AI roaming and terminal identification 2.0 functions are not supported by the following APs:

- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762
- AirEngine 9700D series central APs (including matching RUs)
- AirEngine 9700D-S (including matching ORUs)

Example

Enable the terminal identification 2.0 function on the target AP in the AP system profile **ap-system1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] undo terminal-identify disable
```

11.4.135 uac enable

Function

The **uac enable** command enables user CAC.

The **undo uac enable** command disables user CAC.

By default, user CAC is disabled.

Format

uac { **client-number** | **client-snr** } **enable**

undo uac { **client-number** | **client-snr** } **enable**

Parameters

Parameter	Description	Value
client-number	Controls user access based on the number of users.	-
client-snr	Controls user access based on the terminal SNR.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy resources as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user CAC function. The user CAC function allows an AP to control user access based on the number of online users or terminal SNR, which enables provisioning of high-quality network access services.

CAC is implemented in the following modes:

- User CAC based on the number of users uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.
- SNR-based user CAC controls access from weak-signal users, and is applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

CAC based on the number of users can be configured together with SNR-based CAC.

Follow-up Procedure

Run the **uac client-number threshold** command to set the user CAC threshold based on the number of users.

Run the **uac client-snr threshold** command to set the user CAC threshold based on terminal SNR.

Run the **uac reach-access-threshold** { **hide-ssid** | **priority-replace** } command to configure the action to take for subsequent access control when the number of access users reaches the user CAC threshold.

Example

Enable user CAC based on the number of users.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
```

11.4.136 uac client-number threshold

Function

The **uac client-number threshold** command configures the user CAC threshold based on the number of users.

The **undo uac client-number threshold** command restores the default user CAC threshold based on the number of users.

By default, the user CAC access and roaming thresholds based on the number of users are both 64.

Format

uac client-number threshold access *access-threshold* [**roam** *roam-threshold*]

undo uac client-number threshold

Parameters

Parameter	Description	Value
access *access-threshold*	Specifies the user CAC access threshold based on the number of users.	The value is an integer that ranges from 1 to 512.
roam *roam-threshold*	Specifies the user CAC roaming threshold based on the number of users. This threshold is the total number of users who can be associate with the AP, including all local and reassociated roaming users.	The value is an integer that ranges from 1 to 512.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy resources as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user CAC function. The user CAC function allows an AP to control user access based on the number of online users or terminal SNR, which enables provisioning of high-quality network access services.

NOTE

The user CAC access threshold is invalid for roaming users. For example, the user CAC access threshold is 20, and the user CAC roaming threshold is 24. If 20 local users have already connected to the network, not more local users can connect to the network but another four roaming users can.

CAC is implemented in the following modes:

- User CAC based on the number of users uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.

- SNR-based user CAC controls access from weak-signal users, and is applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

CAC based on the number of users can be configured together with SNR-based CAC.

Prerequisites

The user CAC function based on the number of users has been enabled using the **uac client-number enable** command.

Example

Set the user CAC access threshold based on the number of users to 50 and the roaming threshold to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
[HUAWEI-wlan-rrm-prof-test] uac client-number threshold access 50 roam 60
```

11.4.137 uac client-snr threshold

Function

The **uac client-snr threshold** command configures the user CAC threshold based on terminal SNR.

The **undo uac client-snr threshold** command restores the default user CAC threshold based on terminal SNR.

By default, the user CAC threshold based on terminal SNR is 15 dB.

Format

uac client-snr threshold *threshold*

undo uac client-snr threshold

Parameters

Parameter	Description	Value
threshold	Specifies the user CAC threshold based on terminal SNR.	The value is an integer that ranges from 5 to 45, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On WLANs where many users exist, such as WLANs in high density scenarios, users compete fiercely to occupy resources as the number of online users increases. As a result, network quality deteriorates. To ensure network access experience of online users, configure the user CAC function. The user CAC function allows an AP to control user access based on the number of online users or terminal SNR, which enables provisioning of high-quality network access services.

The configured user CAC threshold based on terminal SNR takes effect for new STAs. When a new STA (or a roaming STA) attempts to connect to an AP, the AP checks the STA's SNR. If the SNR is smaller than the threshold, the AP denies the STA's access.

CAC is implemented in the following modes:

- User CAC based on the number of users uses a simple algorithm. This mode is recommended when most users have the same type of services and similar service traffic volumes.
- SNR-based user CAC controls access from weak-signal users, and is applicable to scenarios where the WLAN has good signal coverage and weak signals only at the edge of WLAN coverage areas.

CAC based on the number of users can be configured together with SNR-based CAC.

Prerequisites

The user CAC function based on terminal SNR has been enabled using the **uac client-snr enable** command.

Example

Set the user CAC threshold based on terminal SNR to 16 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] uac client-snr enable
[HUAWEI-wlan-rrm-prof-default] uac client-snr threshold 16
```

11.4.138 uac reach-access-threshold

Function

The **uac reach-access-threshold** command configures the user CAC function and specifies the action to take when the number of access users reaches the user CAC threshold.

The **undo uac reach-access-threshold** command disables SSID hiding or priority-based user replacement.

By default, SSID hiding and priority-based user replacement are disabled.

Format

uac reach-access-threshold { **hide-ssid** | **priority-replace** }

undo uac reach-access-threshold

Parameters

Parameter	Description	Value
hide-ssid	Indicates SSID hiding.	-
priority-replace	Indicates priority-based user replacement.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user CAC is configured, you can configure the action to take when the number of access users reaches the threshold. The following actions are available:

- Deny new user access. This is the default configuration.
- Deny new user access and hide the SSID.
- Disconnect common users to make room for access of high-priority users.

Prerequisites

User CAC has been enabled using the **uac** { **client-number** | **client-snr** } **enable** command.

Precautions

- When you run the **undo uac** { **client-number** | **client-snr** } **enable** command to disable user CAC, SSID hiding is automatically canceled.
- The **uac reach-access-threshold priority-replace** command takes effect only when UAC based on the number of users is enabled.

Example

Enable SSID hiding.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
[HUAWEI-wlan-rrm-prof-test] uac reach-access-threshold hide-ssid
```

Enable priority-based user replacement.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] uac client-number enable
[HUAWEI-wlan-rrm-prof-test] uac reach-access-threshold priority-replace
Info: This configuration only takes effective when uac client-number enabled.
```

Deny new user access.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name test
[HUAWEI-wlan-rrm-prof-test] undo uac reach-access-threshold
```

11.5 WLAN Spectrum Analysis Configuration Commands

11.5.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.
- Starting from V200R020C10, AirEngine X760 series APs support spectrum analysis. To implement spectrum analysis on the following APs, upgrade them to V200R020C10 or later: AirEngine 8760-X1-PRO, AirEngine 8760R-X1, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 6760R-51, AirEngine 6760R-51E, AirEngine 5760-51, AirEngine 5760-22W, AirEngine 5760-22WD. If the AC version is earlier than V200R020C10, run the **undo ap-type** command on the AC to delete the AP type, which will cause corresponding APs to go offline. Then manually add the AP type again. Alternatively, upgrade the AC to V200R020C10 or later.
- Spectrum analysis is not supported by the following APs:
  - AirEngine 8771-X1T
  - AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD
  - AirEngine X762

11.5.2 channel-monitor enable

Function

The **channel-monitor enable** command enables the function of monitoring the status of all channels.

The **undo channel-monitor enable** command disables the function of monitoring the status of all channels.

By default, the function of monitoring the status of all channels is disabled.

Format

channel-monitor enable

undo channel-monitor enable

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During spectrum analysis, APs report air scan results to a spectrum server. Then the spectrum server analyzes interference source types and identifies non-Wi-Fi interference devices. After you run the **channel-monitor enable** command, APs can scan the status of all channels (normally occupied, Wi-Fi interference, non-Wi-Fi interference, or idle) over the air interface to identify all interference sources.

Precautions

To identify non-Wi-Fi interference, you also need to enable spectrum analysis.

Channels to be monitored are the same as those in the air scan channel set. To collect as much interference source information as possible within the range allowed by local laws and regulations, you are advised to run the **scan-channel-set country-channel** command to add all channels supported by the country code to the air scan channel set.

Follow-up Procedure

To display and analyze monitoring results on iMaster NCE-CampusInsight, configure interconnection with iMaster NCE-CampusInsight through the WMI mechanism and run the **collect-item radio-data** command to enable the function of reporting radio monitoring data to iMaster NCE-CampusInsight.

Example

Enable the function of monitoring the status of all channels.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] channel-monitor enable
```

11.5.3 display spectrum-analysis server-reporter

Function

The **display spectrum-analysis server-reporter** command displays a list of APs that report spectrum packets to the spectrum server.

Format

display spectrum-analysis server-reporter

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display spectrum-analysis server-reporter** command displays a list of APs that report spectrum packets to the spectrum server.

Example

Display all APs that report spectrum packets to the spectrum server.

```
<HUAWEI> display spectrum-analysis server-reporter
------------------------------------------------------------
ID    AP name                          Radio ID
------------------------------------------------------------
1     AP_1                          0
------------------------------------------------------------
Total: 1
```

Table 11-157 Description of the **display spectrum-analysis server-reporter** command output

Item	Description
ID	ID of the AP that reports spectrum data. To configure this parameter, run the **spectrum-report** command.
AP name	Name of the AP that reports spectrum data. To configure this parameter, run the **spectrum-report** command.
Radio ID	ID of the radio on which the function of reporting spectrum data is enabled. To configure this parameter, run the **spectrum-report** command.

11.5.4 display wlan non-wifi-device

Function

The **display wlan non-wifi-device** command displays information about detected non-Wi-Fi devices.

Format

display wlan non-wifi-device { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Displays information about the non-Wi-Fi devices detected by all APs.	-
ap-name *ap-name*	Displays information about the non-Wi-Fi devices detected by a specified AP name.	The AP name must exist.
ap-id *ap-id*	Displays information about the non-Wi-Fi devices detected by a specified AP ID.	The AP ID must exist.
radio *radio-id*	Displays information about the non-Wi-Fi devices detected by a specified AP radio.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: ● AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 ● AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T ● AirEngine 8771-X1T

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the function of reporting spectrum data is enabled on an AP radio using the **spectrum-report** command, you can run the **display wlan non-wifi-device** command to check information about the detected non-Wi-Fi devices.

Example

Display information about the non-Wi-Fi devices detected by all APs.

```
<HUAWEI> display wlan non-wifi-device all
Info: This operation may take a few seconds. Please wait for a moment.done.
----------------------------------------------------------------
Detect AP ID                           : 11
Detect AP name                         : 00e0-fc00-0011
Detect AP radio ID                     : 0
Detect AP channel                      : 1
Non-Wi-Fi device type                  : 4
Non-Wi-Fi device name                  : Bluetooth
Non-Wi-Fi device frequency type        : hop Frequency
Non-Wi-Fi device channel               : 7,11
Non-Wi-Fi device RSSI                  : -54,-53
Non-Wi-Fi device detect time last      : 2021-04-22/09:46:23
Non-Wi-Fi device center frequency(MHz) : 2443
Non-Wi-Fi device bandwidth(KHz)        : 3281
Non-Wi-Fi device duty(%)               : 66
Non-Wi-Fi device interfere level       : 3
----------------------------------------------------------------
----------------------------------------------------------------
Detect AP ID                           : 11
Detect AP name                         : 00e0-fc00-0010
Detect AP radio ID                     : 0
Detect AP channel                      : 1
Non-Wi-Fi device type                  : 8
Non-Wi-Fi device name                  : Babymonitor
Non-Wi-Fi device frequency type        : hop Frequency
Non-Wi-Fi device channel               : 7,13
Non-Wi-Fi device RSSI                  : -35,-48
Non-Wi-Fi device detect time last      : 2021-04-22/09:46:34
Non-Wi-Fi device center frequency(MHz) : 2443
Non-Wi-Fi device bandwidth(KHz)        : 10937
Non-Wi-Fi device duty(%)               : 39
Non-Wi-Fi device interfere level       : 3
----------------------------------------------------------------
Total: 2
```

Table 11-158 Description of the **display wlan non-wifi-device** command output

Item	Description
Detect AP ID	ID of the AP that has detected a non-Wi-Fi device.
Detect AP name	Name of the AP that has detected a non-Wi-Fi device.
Detect AP radio ID	ID of the AP radio on which a non-Wi-Fi device is detected.

Item	Description
Detect AP channel	ID of the AP channel on which a non-Wi-Fi device is detected.
Non-Wi-Fi device type	Type of the detected non-Wi-Fi device. ● 0: Cordless phone ● 1: Cordless phone base ● 2: ZigBee device ● 3: Microwave oven ● 4: Bluetooth ● 5: Game controller ● 6: 2.4G wireless video and audio device ● 7: 5G wireless video and audio device ● 8: Baby monitor ● 9: Fixed-frequency device
Non-Wi-Fi device name	Name of the non-Wi-Fi device.
Non-Wi-Fi device frequency type	Frequency type of the non-Wi-Fi device.
Non-Wi-Fi device channel	Channel of the non-Wi-Fi device.
Non-Wi-Fi device RSSI	RSSI of the non-Wi-Fi device.
Non-Wi-Fi device detect time last	Detection time for the non-Wi-Fi device.
Non-Wi-Fi device center frequency(MHz)	Center frequency of the non-Wi-Fi device.
Non-Wi-Fi device bandwidth(KHz)	Bandwidth of the non-Wi-Fi device.
Non-Wi-Fi device duty(%)	Duty cycle of the non-Wi-Fi device.
Non-Wi-Fi device interfere level	Interference level of the non-Wi-Fi device. The value ranges from 0 to 3. A larger value indicates stronger interference.

11.5.5 display wlan non-wifi-device history

Function

The **display wlan non-wifi-device history** command displays information about non-Wi-Fi devices in the historical list.

Format

display wlan non-wifi-device history { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Displays information about all the non-Wi-Fi devices in the historical list.	-
ap-name *ap-name*	Displays information about the non-Wi-Fi devices detected by an AP with a specified name in the historical list.	The AP name must exist.
ap-id *ap-id*	Displays information about the non-Wi-Fi devices detected by an AP with a specified ID in the historical list.	The AP ID must exist.
radio *radio-id*	Displays information about the non-Wi-Fi devices detected by a specified AP radio in the historical list.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: ● AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 ● AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T ● AirEngine 8771-X1T

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If information about a non-Wi-Fi device is not detected within the aging time configured using the **spectrum-analysis non-wifi-device aging-time** command, the AC adds the device to the historical list.

Example

Display information about non-Wi-Fi devices in the historical list.

```
<HUAWEI> display wlan non-wifi-device history all
------------------------------------------------------------------
S/No.                               : 0
Detect AP name                      : MyAP
Detect AP radio ID                  : 1
Detect AP channel                   : 44
Non-Wi-Fi device type               : 9
Non-Wi-Fi device name               : Unknown fix freq device
Non-Wi-Fi device frequency type     : Narrow bandwidth
Non-Wi-Fi device channel            : 147,148
Non-Wi-Fi device RSSI               : -59,-66
Non-Wi-Fi device detect time last   : 2014-11-19/17:05:05
Non-Wi-Fi device center frequency(MHz) : 5739
Non-Wi-Fi device bandwidth(KHz)     : 2708
Non-Wi-Fi device duty(%)            : 79
Non-Wi-Fi device interfere level    : 3
------------------------------------------------------------------
Total: 1
```

Table 11-159 Description of the **display wlan non-wifi-device history** command output

Item	Description
S/No.	No.of historical records.
Detect AP name	Name of the AP that has detected a non-Wi-Fi device.
Detect AP radio ID	ID of the AP radio on which a non-Wi-Fi device is detected.
Detect AP channel	AP channel on which a non-Wi-Fi device is detected.
Non-Wi-Fi device type	Type of the detected non-Wi-Fi device.
Non-Wi-Fi device name	Name of the non-Wi-Fi device.
Non-Wi-Fi device frequency type	Frequency type of the non-Wi-Fi device.
Non-Wi-Fi device RSSI	RSSI of the non-Wi-Fi device.
Non-Wi-Fi device channel	Channel of the non-Wi-Fi device.
Non-Wi-Fi device detect time last	Detection time for the non-Wi-Fi device.
Non-Wi-Fi device center frequency(MHz)	Center frequency of the non-Wi-Fi device.

Item	Description
Non-Wi-Fi device bandwidth(KHz)	Bandwidth of the non-Wi-Fi device.
Non-Wi-Fi device duty(%)	Duty cycle of the non-Wi-Fi device.
Non-Wi-Fi device interfere level	Interference level of the non-Wi-Fi device. The value ranges from 0 to 3. A larger value indicates stronger interference.

11.5.6 spectrum-analysis enable

Function

(AP group radio view) The **spectrum-analysis enable** command enables spectrum analysis on a specified radio in an AP group.

(AP group radio view) The **undo spectrum-analysis enable** command disables spectrum analysis on a specified radio in an AP group.

(AP radio view) The **spectrum-analysis enable** command enables spectrum analysis on a specified AP radio.

(AP radio view) The **undo spectrum-analysis enable** command restores the AP radio configuration to that in the AP group radio view.

By default, spectrum analysis is disabled on an AP radio.

Format

spectrum-analysis enable

undo spectrum-analysis enable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If interference exists on a WLAN, enable spectrum analysis on AP radios to implement spectrum scanning, sampling, and analysis on the wireless signals. The spectrum analysis function helps identify non-Wi-Fi interference on the WLAN and locate non-Wi-Fi devices to optimize the WLAN.

Precautions

If the WDS or Mesh service is configured on a radio, the command cannot be executed in the radio view.

Example

Enable spectrum analysis on radio 0 of the AP with ID 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] spectrum-analysis enable
```

11.5.7 spectrum-analysis non-wifi-device aging-time

Function

The **spectrum-analysis non-wifi-device aging-time** command configures the aging time for non-Wi-Fi device information during spectrum analysis.

The **undo spectrum-analysis non-wifi-device aging-time** command restores the default aging time for non-Wi-Fi device information during spectrum analysis.

By default, the aging time for non-Wi-Fi device information is 3 minutes.

Format

spectrum-analysis non-wifi-device aging-time *aging-time*

undo spectrum-analysis non-wifi-device aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time for non-Wi-Fi device information.	The value is an integer that ranges from 1 to 30, in minutes.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a spectrum analysis server is configured using the **spectrum-analysis server** command, the AC stores information about analyzed non-Wi-Fi device information. If information about a non-Wi-Fi device is not reported again within the aging time configured using the **spectrum-analysis non-wifi-device aging-time** command, the AC adds the non-Wi-Fi device to the historical list. You can run the **display wlan non-wifi-device history** command to check information about non-Wi-Fi devices in the historical list.

Precautions

Currently, the device cannot identify different devices of the same type. For example, when the device detects Bluetooth devices A and B, the device can only record them as Bluetooth devices and update the detection time of the Bluetooth device.

Example

Set the aging time for non-Wi-Fi device information to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] spectrum-analysis non-wifi-device aging-time 5
```

11.5.8 spectrum-analysis server

Function

The **spectrum-analysis server** command specifies the IP address and port number of a spectrum server.

The **undo spectrum-analysis server** command deletes the specified IP address and port number of a spectrum server.

By default, no spectrum server is configured.

Format

spectrum-analysis server ip-address *ip-address* **port** *port-number* [**via-ac ac-port** *ac-port-number*]

undo spectrum-analysis server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of a spectrum server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number (UDP port number) of a spectrum server.	The value is an integer that ranges from 1 to 65535. **NOTE** The port number of eSight is 32181, and that of iMaster NCE-CampusInsight is 27371.

Parameter	Description	Value
via-ac	Configures the AP to report spectrum data to the spectrum server via the AC.	-
ac-port *ac-port-number*	Specifies the port number used by the AC to receive spectrum data (in UDP packets) from the AP.	The value is an integer that ranges from 5000 to 65535.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After collecting the spectrum data, an AP encapsulates the collected data into UDP packets and sends the packets to the spectrum server. The spectrum server draws a spectrum and displays the spectrum information of the detected non-Wi-Fi devices to users through images.

- If the AP uploads the collected data directly to the spectrum server, you do not need to configure the **via-ac ac-port** *ac-port-number* command.
- If the AP uploads the collected data to the spectrum server via the AC, configure the **via-ac ac-port** *ac-port-number* command.
- If no spectrum server is available, to view the spectrum in the web system of an AC, specify a valid IP address and port number for the spectrum server (which do not take effect) and configure the **via-ac ac-port** *ac-port-number* command.

Follow-up Procedure

Run the **spectrum-report** { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* command to enable the function of reporting spectrum data on an AP radio.

Example

Set the IP address and port number of a spectrum server to 10.137.43.4 and 27371, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] spectrum-analysis server ip-address 10.137.43.4 port 27371
```

11.5.9 spectrum-analysis source

Function

The **spectrum-analysis source** command configures the source IP address of packets sent by the AC to a spectrum server.

The **undo spectrum-analysis source** command deletes the configured source IP address of packets sent by the AC to a spectrum server.

By default, the AC uses the IP address of the outbound interface on the matched route as the source IP address of packets sent to a spectrum server.

Format

spectrum-analysis source ip-address *ip-address*

undo spectrum-analysis source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the source IPv4 address of packets sent by the AC to a spectrum server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, when sending data packets to a spectrum server, the AC uses the IP address of the outbound interface on the matched route between them to communicate with the spectrum server.

After the source IP address is configured using the **spectrum-analysis source** command, the AC uses this IP address to communicate with the spectrum server.

Precautions

- Ensure that the AC's IP address manually configured on the spectrum server is the same as that configured using the **spectrum-analysis source** command.
- The configured source IP address must exist on the AC and is routable with the spectrum server.

Example

Configure 10.102.25.23 as the source IP address of packets sent by the AC to a spectrum server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] spectrum-analysis source ip-address 10.102.25.23
```

11.5.10 spectrum-report

Function

The **spectrum-report** command enables the function of reporting spectrum data on an AP radio.

The **undo spectrum-report** command disables the function of reporting spectrum data on an AP radio.

By default, the function of reporting spectrum data is disabled on an AP radio.

Format

spectrum-report { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

undo spectrum-report { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name. The AP name and radio ID identify a radio.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID. The AP ID and radio ID identify a radio.	The AP ID must exist.

Parameter	Description	Value
radio *radio-id*	Specifies a radio ID.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: ● AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 ● AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T ● AirEngine 8771-X1T
all	Specifies all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of reporting spectrum data is enabled on an AP radio, the AP encapsulates collected data into UDP packets and sends the packets to the spectrum server. After receiving the data, the spectrum server analyzes the data and then displays radio information of non-Wi-Fi devices to users through images or tables.

Prerequisites

The spectrum analysis function has been enabled on a radio using the **spectrum-analysis enable** command.

Follow-up Procedure

Run the **spectrum-analysis server** command in the spectrum profile view to specify the IP address and port number of the spectrum server.

Precautions

The **spectrum-report** command becomes invalid after the AC restarts, and needs to be configured again.

Example

Enable the function of reporting spectrum data on radio 0 of the AP named **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] spectrum-report ap-name test radio 0
```

11.5.11 reset wlan non-wifi-device

Function

The **reset wlan non-wifi-device** command clears information about detected non-Wi-Fi devices.

Format

reset wlan non-wifi-device { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Clears information about the non-Wi-Fi devices detected by all APs.	-
ap-name *ap-name*	Clears information about the non-Wi-Fi devices detected by a specified AP name.	The AP name must exist.
ap-id *ap-id*	Clears information about the non-Wi-Fi devices detected by a specified AP ID.	The AP ID must exist.

Parameter	Description	Value
radio *radio-id*	Clears information about the non-Wi-Fi devices detected by a specified AP radio.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: ● AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 ● AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T ● AirEngine 8771-X1T

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting information about detected non-Wi-Fi devices in a period, you can run this command to clear existing information so that the AC can re-collect information.

Prerequisites

The spectrum analysis function has been enabled on a radio.

Impact

The cleared non-Wi-Fi device information cannot be restored. Exercise caution when you run this command. After the command is run, you can run the **display wlan non-wifi-device history** command to view related information.

Example

Clear information about the non-Wi-Fi devices detected by all APs.

```
<HUAWEI> reset wlan non-wifi-device all
```

11.5.12 reset wlan non-wifi-device history

Function

The **reset wlan non-wifi-device history** command clears information about non-Wi-Fi devices in the historical list.

Format

reset wlan non-wifi-device history { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* }

Parameters

Parameter	Description	Value
all	Clears information about all the non-Wi-Fi devices in the historical list.	-
ap-name *ap-name*	Clears information about the non-Wi-Fi devices detected by a specified AP name in the historical list.	The AP name must exist.
ap-id *ap-id*	Clears information about the non-Wi-Fi devices detected by a specified AP ID in the historical list.	The AP ID must exist.
radio *radio-id*	Clears information about the non-Wi-Fi devices detected by a specified AP radio in the historical list.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: ● AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 ● AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T ● AirEngine 8771-X1T

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to clear information about non-Wi-Fi devices in the historical list.

Example

Clear information about the non-Wi-Fi devices detected by all APs in the historical list.

```
<HUAWEI> reset wlan non-wifi-device history all
```

11.6 WLAN Roaming Commands

11.6.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.6.2 beacon disable

Function

The **beacon disable** command disables an RU from sending Beacon frames.

The **undo beacon disable** command allows an RU to send Beacon frames.

By default, an RU is allowed to send Beacon frames.

NOTE

This command does not take effect for the following APs:

- AirEngine 9700D-S
- AirEngine X77X
- AirEngine X76X (including RUs)

Format

beacon disable

undo beacon disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure synchronization of Beacon frames in scenarios with densely deployed RUs, you can run the **beacon disable** command to disable some RUs from sending Beacon frames. This configuration is recommended on a network enabled with agile distributed SFN roaming. In other scenarios, the default configuration is recommended.

Precautions

Disabling an RU from sending Beacon frames may cause STAs to go offline due to a failure to receive Beacon frames.

Example

Disable an RU from sending Beacon frames.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] beacon disable
Warning: This configuration is recommended in SFN roaming scenarios. This action
 may cause service interruption. Continue? [Y/N]Y
```

11.6.3 capwap dtls inter-controller control-link encrypt

Function

The **capwap dtls inter-controller control-link encrypt** command configures DTLS encryption for an inter-AC control tunnel.

The **undo capwap dtls inter-controller control-link encrypt** command restores the default configuration of DTLS encryption for an inter-AC control tunnel.

By default, DTLS encryption for an inter-AC control tunnel is disabled.

Format

capwap dtls inter-controller control-link encrypt

undo capwap dtls inter-controller control-link encrypt

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

At the discovery stage of inter-AC tunnel establishment, the AC obtains the IP address of another AC through the discovery mechanism. After that, the ACs enter the DTLS negotiation stage, in which the ACs use DTLS to set up a tunnel and encrypt UDP packets forwarded in the tunnel.

After this command is executed, packets transmitted over an inter-AC control tunnel are encrypted using DTLS. The ACs implement DTLS negotiation in PSK encryption mode. If DTLS negotiation fails, the inter-AC tunnel cannot be set up.

Precautions

If you modify the DTLS configuration after an inter-AC tunnel is set up, the modification takes effect at the next tunnel setup.

When DTLS encryption is enabled for an inter-AC control tunnel on the server-side AC, the inter-AC tunnel can be set up only when this function is enabled on client-side AC. When DTLS encryption is enabled for an inter-AC control tunnel on the client-side AC, the inter-AC tunnel can be set up if even this function is disabled on the server-side AC.

Before enabling this function, run the **capwap dtls inter-controller psk** command to configure a PSK.

Example

Enable DTLS encryption for an inter-AC control tunnel.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls inter-controller control-link encrypt
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]:y
```

11.6.4 capwap dtls inter-controller psk

Function

The **capwap dtls inter-controller psk** command configures a pre-shared key (PSK) for DTLS encryption of inter-AC tunnels.

By default, no PSK is configured for DTLS encryption.

Format

capwap dtls inter-controller psk *psk-value*

Parameters

Parameter	Description	Value
psk-value	Specifies a PSK for DTLS encryption.	The value is string of 48 or 68 characters in ciphertext (for example, **%^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#**) or a string of 8 to 32 characters in plaintext (for example, **YsHsjx_202206**). The key must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios such as inter-AC roaming and centralized license control, ACs synchronize data and forward packets through CAPWAP tunnels. If DTLS encryption for inter-AC tunnels is configured, DTLS negotiation is initiated when an AC negotiates with the peer AC to establish a CAPWAP link. Subsequent UDP packets are encrypted using DTLS to improve transmission security.

DTLS supports PSK encryption. When a PSK is used for DTLS encryption, you can use this command to change the value of the PSK on the AC.

Follow-up Procedure

Run the **capwap dtls inter-controller control-link encrypt** command to enable DTLS encryption for inter-AC control tunnels.

Precautions

If you modify the PSK after an inter-AC tunnel is set up, the modification takes effect at the next tunnel setup.

DTLS encryption must be enabled on ACs at both ends of the tunnel, and the ACs must have the same PSK.

It is recommended that you configure the same PSK on the ACs at both ends before enabling DTLS encryption. In this way, the ACs have the same PSK. If you enable DTLS encryption but the ACs have different PSKs, DTLS negotiation fails. As a result, the tunnel cannot be set up between the ACs.

NOTE

To implement roaming between ACs running different versions, you must manually configure the same PSK on the ACs in the mobility group.

Example

Configure the PSK **YsHsjx_202206** for DTLS encryption of an inter-AC tunnel.

```
<HUAWEI> system-view
[HUAWEI] capwap dtls inter-controller psk YsHsjx_202206
```

11.6.5 capwap inter-controller sensitive-info psk

Function

The **capwap inter-controller sensitive-info psk** command configures a pre-shared key (PSK) used for encrypting sensitive information between ACs.

The **undo capwap inter-controller sensitive-info psk** command deletes the configured PSK used for encrypting sensitive information between ACs.

By default, no PSK is configured for encrypting sensitive information between ACs.

Format

capwap inter-controller sensitive-info psk *key-value*

undo capwap inter-controller sensitive-info psk

Parameters

Parameter	Description	Value
key-value	Specifies a PSK for encrypting sensitive information between ACs.	The value is a string of 6 to 32 case-sensitive characters without question marks (?) or spaces. For a plaintext PSK, the length must be 48 or 68 bits. If the string is enclosed in double quotation marks ("), the string can contain spaces. **NOTE** For security purposes, it is recommended that the PSK contain at least eight characters from at least two of the following types: uppercase letters, lowercase letters, digits, and special characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In multi-AC scenarios where inter-AC communication is established through CAPWAP tunnels (such as inter-AC roaming and centralized license control), ACs may need to exchange sensitive information such as the user name and password. You can configure a PSK to protect sensitive data transmitted between ACs.

Precautions

- Ensure that the ACs have the same PSK. Otherwise, the CAPWAP tunnel cannot be set up between the ACs.
- This function must be configured on the ACs at both ends of a CAPWAP tunnel, and the ACs must have the same PSK. Otherwise, the CAPWAP tunnel cannot be set up between the ACs.

Example

Set the PSK used for encrypting sensitive information between ACs to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] capwap inter-controller sensitive-info psk YsHsjx_202206
Warning: The ACs must have the same configuration. Otherwise, the link between them cannot be set up.
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue?
[Y/N]:Y
```

11.6.6 cts delay

Function

The **cts delay** command sets a delay for RUs to respond to STAs with CTS packets.

The **undo cts delay** command deletes the delay configured for RUs to respond to STAs with CTS packets.

By default, RUs respond to STAs with CTS packets with no delay.

Format

cts delay *delay-time*

undo cts delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay time after which RUs respond to STAs with CTS packets.	The value is an integer that ranges from 1 to 255, in microseconds.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

After the **undo cts disable** command is executed to enable RUs to respond to STAs with CTS packets, you can configure a response delay. When multiple RUs respond to STAs with CTS packets, you can configure the delay for some RUs to prevent conflicts.

Example

Set the delay for RUs to respond to STAs with CTS packets to 60 microseconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
```

```
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] undo cts disable
[HUAWEI-wlan-radio-1/0] cts delay 60
```

11.6.7 cts disable

Function

The **cts disable** command disables RUs from responding to STAs with CTS packets.

The **undo cts disable** command enables RUs to respond to STAs with CTS packets.

By default, RUs are enabled to respond to STAs with CTS packets.

Format

cts disable

undo cts disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent CTS conflicts in scenarios with densely deployed RUs, you can run the **cts disable** command to disable some RUs from responding to STAs with CTS packets. This configuration is recommended on a network enabled with agile distributed SFN roaming. In other scenarios, the default configuration is recommended.

Precautions

Disabling RUs from responding to STAs with CTS packets may cause STAs to go offline due to a failure to receive CTS packets.

This command does not take effect on the R250D, R250D-E, R251D, R251D-E, or R450D.

Example

Disable RUs from responding to STAs with CTS packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 1
```

```
[HUAWEI-wlan-ap-1] radio 0
[HUAWEI-wlan-radio-1/0] cts disable
Warning: This configuration is recommended in SFN roaming scenarios. This action
 may cause service interruption. Continue? [Y/N]y
```

11.6.8 display mobility-group

Function

The **display mobility-group** command displays configurations of mobility groups.

Format

display mobility-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a mobility group.	The mobility group name must already exist.
all	Specifies all mobility groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mobility-group** command to view configurations of mobility groups.

Example

Display configurations of the mobility group **hello**.

```
<HUAWEI> display mobility-group name hello
--------------------------------------------------------------------------------
State        IP address                     Description
--------------------------------------------------------------------------------
normal       192.168.10.1                     -
normal       192.168.10.2                     -
fault        192.168.10.3                     -
--------------------------------------------------------------------------------
Total: 3
```

Table 11-160 Description of the **display mobility-group** command output

Item	Description
State	Status of the CAPWAP links between members in the mobility group and the local AC. ● normal: The CAPWAP links are working properly. ● fault: The CAPWAP links are disconnected. ● vmiss: The versions of members in the mobility group and the local AC do not match. ● -: No CAPWAP link is established between members in the mobility group and the local AC.
IP address	AC's IP address.
Description	Description of the AC.

Display configurations of all mobility groups.

```
<HUAWEI> display mobility-group all
------------------------------------------------------------------------------------------
Group name
------------------------------------------------------------------------------------------
group1
mobility-test
------------------------------------------------------------------------------------------
Total: 2
```

Table 11-161 Description of the **display mobility-group all** command output

Item	Description
Group name	Mobility group name.

11.6.9 display station roam-statistics

Function

The **display station roam-statistics** command displays STA roaming statistics.

Format

display station roam-statistics [**ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays statistics about STAs associated with the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays statistics about STAs associated with the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station roam-statistics** command to view STA roaming statistics.

- If no parameter is specified, roaming statistics about all associated STAs are displayed.
- If an AP name or ID is specified, roaming statistics about all STAs associated with the AP are displayed.

Example

Display roaming statistics about all STAs.

```
<HUAWEI> display station roam-statistics
--------------------------------------------------------------------------------
 Online STAs                                                :0
 Online roaming stations                                    :0
--------------------------------------------------------------------------------
```

Table 11-162 Description of the **display station roam-statistics** command output

Item	Description
Online STAs	Number of online STAs.
Online roaming stations	Number of online roaming STAs.

Display roaming statistics about STAs associated with a specified AP.

```
<HUAWEI> display station roam-statistics ap-name N1-2
----------------------------------------------------------------------------
```

```
Online STAs                                    :0
Online roaming stations                            :0
Online L3 roam stations                            :0
L3 roam-in                                    :0
L3 roam-out                                    :0
------------------------------------------------------------------------------
```

Table 11-163 Description of the **display station roam-statistics ap-name** *ap-name* command output

Item	Description
Online STAs	Number of online STAs.
Online roaming stations	Number of online roaming STAs.
Online L3 roam stations	Number of Layer 3 roaming STAs.
L3 roam-in	Number of STAs roaming from another AP to the local AP.
L3 roam-out	Number of STAs roaming from the local AP to another AP.

11.6.10 display station roam-track

Function

The **display station roam-track** command displays the roaming track of a STA.

Format

display station roam-track sta-mac *mac-address*

Parameters

Parameter	Description	Value
sta-mac *mac-address*	Specifies the MAC address of a specified STA.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During the roaming process of a STA, the AC records the STA's roaming track (that is, information about the APs that the STA connects to). You can run the **display station roam-track** command to view the roaming track of the STA.

Example

Display the roaming track of the STA with the MAC address 00e0-fc00-0001.

```
<HUAWEI> display station roam-track sta-mac 00e0-fc00-0001
Access SSID:test
Rx/Tx:link receive rate/link transmit rate(Mbps)
s: Same Frequency Network c:PMK Cache Roam
r:802.11r Roam d:802.11r over ds Roam p:proprietary 802.11r Roam
------------------------------------------------------------------------------------------
L2/L3          AP-AC IP             AC-AC IP           AP name            Radio ID
BSSID          TIME                 In/Out RSSI        Out Rx/Tx
------------------------------------------------------------------------------------------
--             192.168.109.1         -                 test1              1
00e0-fc76-e360  2015-01-12/16:52:58    -51/-48            46/13
L2             192.168.109.1         -                 test2              1
00e0-fc74-9640  2015-01-12/16:55:45    -58/-              -/-
------------------------------------------------------------------------------------------
Number: 1
```

Table 11-164 Description of the **display station roam-track** command output

Item	Description
Access SSID	SSID associated with a STA.
Rx/Tx	Negotiated rate between the STA and AP.
L2/L3	Roaming mode. Suffix description: ● s: agile distributed SFN roaming ● c: PMK fast roaming. ● r: 802.11r fast roaming (over-the-air mode) ● d: 802.11r fast roaming (standard over-the-DS mode) ● p: 802.11r fast roaming (proprietary over-the-DS mode)
AP-AC IP	CAPWAP source IP address used by the AC that the STA is associated with for setting up a CAPWAP tunnel with the AP that the STA is associated with.
AC-AC IP	CAPWAP source IP address used by the AC that the STA is associated with for setting up CAPWAP tunnels with other ACs.

Item	Description
AP name	Name of an AP that the STA is associated with.
Radio ID	ID of a radio that the STA is associated with.
BSSID	BSSID of an AP that the STA is associated with.
TIME	Time duration when the STA is associated with an AP.
In/Out RSSI	RSSI of the AP that the STA is associated with and RSSI of the AP away from which the STA has left.
Out Rx/Tx	Negotiated rate of the STA when it disconnects from an AP.
Number	Number of STA roaming tracks.

11.6.11 dot11r enable

Function

The **dot11r enable** command enables 802.11r.

The **undo dot11r enable** command disables 802.11r.

By default, 802.11r is disabled.

Format

dot11r enable [**over-the-ds**]

undo dot11r enable

Parameters

Parameter	Description	Value
over-the-ds	Indicates 802.11r roaming in over-the-DS mode.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During roaming, the STA needs to be reauthenticated and re-negotiate a key, so services are interrupted for a short period of time. You can enable 802.11r to reduce the number of information exchanges during roaming, thus reducing latency.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.
- Over-the-DS 802.11r roaming across ACs is not supported.

Example

Enable the 802.11r function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r enable
```

11.6.12 dot11r proprietary

Function

The **dot11r proprietary** command enables the Huawei's proprietary 802.11r function (device-pipe synergy roaming).

The **undo dot11r proprietary** command disables the Huawei's proprietary 802.11r function.

By default, Huawei's proprietary 802.11r function is disabled.

Format

dot11r proprietary

undo dot11r proprietary

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to the characteristics of Wi-Fi and different behaviors of different terminals on the WLAN, the actual roaming experience for the terminals varies. The roaming experience for latency-sensitive services such as audio, video, and gaming cannot be guaranteed. Roaming optimization policies are different for terminals and APs and may conflict with each other. Therefore, simply optimization for terminals or APs cannot solve the problem. APs are optimized for Huawei's terminals running EMUI 10.0 or later. After the Huawei's proprietary 802.11r function is enabled, APs can carry the interworking IE in Beacon and Probe Response frames and perform roaming negotiation with Huawei terminals based on the specified frame format and interaction action. This function implements mutual trust and interworking between devices and pipes, reduces resource overheads during roaming negotiation, and effectively improves roaming experience.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.

Example

Enable the Huawei's proprietary 802.11r function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r proprietary
```

11.6.13 dot11r reassociate-timeout

Function

The **dot11r reassociate-timeout** command sets the 802.11r reassociation timeout period.

The **undo dot11r reassociate-timeout** command restores the default 802.11r reassociation timeout period.

By default, the 802.11r reassociation timeout period is 1s.

Format

dot11r reassociate-timeout *time*

undo dot11r reassociate-timeout

Parameters

Parameter	Description	Value
reassociate-timeout *time*	Specifies the reassociation timeout period. After successful authentication, if the STA does not initiate a reassociation request within this period, the roaming fails.	The value is an integer that ranges from 1 to 10, in seconds.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During roaming, the STA needs to be reauthenticated and re-negotiate a key, so services are interrupted for a short period of time. You can enable 802.11r to reduce the number of information exchanges during roaming, thus reducing latency.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.

Example

Set the 802.11r reassociation timeout period to 3s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r reassociate-timeout 3
```

11.6.14 member (mobility group view)

Function

The **member** command adds a member AC to a mobility group.

The **undo member** command deletes a member AC from a mobility group.

By default, no member AC is added to a mobility group.

Format

member ip-address *ipv4-address* [**description** *description*]

undo member ip-address *ipv4-address*

Parameters

Parameter	Description	Value
ip-address *ipv4-address*	Specifies the IPv4 address of a mobility group member.	The value is in dotted decimal notation.
description *description*	Description of a mobility group member.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

mobility group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a STA to roam between ACs, run the **mobility-group name** *group-name* command to configure a mobility group. The STA can roam between the ACs in the group. You can run the **member** command to add a member AC to the mobility group.

Precautions

An AC can be added only to one mobility group.

Example

Add the AC with IPv4 address 192.168.100.1 to the mobility group **mobility**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-group name mobility
[HUAWEI-mc-mg-mobility] member ip-address 192.168.100.1
```

Remove the AC with IPv4 address 192.168.100.1 from the mobility group **mobility**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-group name mobility
[HUAWEI-mc-mg-mobility] undo member ip-address 192.168.100.1
```

11.6.15 mobility-group

Function

The **mobility-group** command creates a mobility group and displays the mobility group view. If the specified mobility group exists, you can directly enter the specified mobility group view.

The **undo mobility-group** command deletes a mobility group.

By default, no mobility group is created.

Format

mobility-group name *group-name*

undo mobility-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a mobility group.	The value is a string of 1 to 31 characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates all mobility groups.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

STAs can roam between ACs in a mobility group. You can run the **mobility-group** command to create a mobility group and add required ACs to the group.

Follow-up Procedure

Run the **member ip-address** *ipv4-address* [**description** *description*] command to add member ACs to the mobility group.

Example

Create a mobility group named **mobility** and display the mobility group view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-group name mobility
[HUAWEI-mc-mg-mobility]
```

Delete a mobility group.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] undo mobility-group name mobility
Warning:The mobility group will be deleted, are you sure to continue?[Y/N]:y
```

Delete all mobility groups.

11.6.16 mobility-server local

Function

The **mobility-server local** command configures a local IP address for setting up links between ACs in a mobility group.

The **undo mobility-server local** command deletes the local IP address for setting up links between ACs in a mobility group.

By default, no local IP address is configured for setting up links between ACs in a mobility group.

Format

mobility-server local ip-address *ipv4-address*

undo mobility-server local

Parameters

Parameter	Description	Value
ip-address *ipv4-address*	Specifies an IPv4 address for setting up links between ACs in a mobility group.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In inter-AC roaming scenarios, you need to specify a local IP address for STAs to roam between ACs.

Precautions

The specified IP address must be the same as the CAPWAP source IP address. When multiple CAPWAP source addresses are configured, only one can be specified as the local IP address for setting up links between ACs.

Example

Configure 192.168.10.1 as the local IP address for setting up links between ACs in a mobility group.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mobility-server local ip-address 192.168.10.1
```

11.6.17 sfn-roam enable

Function

The **sfn-roam enable** command enables agile distributed SFN roaming.

The **undo sfn-roam enable** command disables agile distributed SFN roaming.

By default, agile distributed SFN roaming is disabled.

Format

sfn-roam enable

undo sfn-roam enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the agile distributed Wi-Fi networking, some scenarios require high network connection stability, such as healthcare scenarios. In this case, you can run the **sfn-roam enable** command to enable agile distributed SFN roaming. All RUs are deployed to work on the same channel and use the same BSSID for communicating with STAs. When the STAs move within the signal coverage of the same SSID, they are not aware of roaming and services are not interrupted.

Example

Enable agile distributed SFN roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] sfn-roam enable
Warning: This feature requires that radios work on the same channel. Enabling th
is feature will disable the channel calibration, channel scanning, and smart roa
ming functions on the AP and disconnect STAs connected to the VAP. Open, WEP, an
d WAPI encryption modes are not supported. The PSK + WPA2 mode is recommended. A
 radio allows SFN to be enabled only for one VAP. Continue?[Y/N]:y
```

11.6.18 sfn-roam report-interval

Function

The **sfn-roam report-interval** command sets an interval at which RUs report STA RSSIs.

The **undo sfn-roam report-interval** command restores the default interval at which RUs report STA RSSIs.

By default, RUs report STA RSSIs to the central AP at an interval of 400 milliseconds.

Format

sfn-roam report-interval *report-interval-value*

undo sfn-roam report-interval

Parameters

Parameter	Description	Value
report-interval-value	Specifies an interval for RUs to report STA RSSIs.	The value is an integer that ranges from 200 to 1000, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The interval at which RUs report STA RSSIs helps you adjust the roaming sensitivity. A shorter interval indicates a higher sensitivity. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance. This interval must be smaller than the decision period for agile distributed SFN roaming.

Example

Set the interval for RUs to report the STA RSSI to 500 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam report-interval 500
```

11.6.19 sfn-roam roam-check better-times

Function

The **sfn-roam roam-check better-times** command sets the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU.

The **undo sfn-roam roam-check better-times** command restores the default number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU.

By default, the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU is 2.

Format

sfn-roam roam-check better-times *better-times*

undo sfn-roam roam-check better-times

Parameters

Parameter	Description	Value
better-times	Specifies the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU.	The value is an integer that ranges from 1 to 32.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can adjust the roaming sensitivity by setting the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU. A roaming handover occurs when the RSSI of a surrounding RU is higher than that of the local RU for the specified times within the roaming decision period. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the number of times the RSSI of agile distributed SFN roaming RUs is higher than that of the local RU to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check better-times 5
```

11.6.20 sfn-roam roam-check check-interval

Function

The **sfn-roam roam-check check-interval** command sets the decision period for agile distributed SFN roaming.

The **undo sfn-roam roam-check check-interval** command restores the default decision period for agile distributed SFN roaming.

The default decision period for agile distributed SFN roaming is 700 milliseconds.

Format

sfn-roam roam-check check-interval *check-interval-value*

undo sfn-roam roam-check check-interval

Parameters

Parameter	Description	Value
check-interval-value	Specifies the decision period for agile distributed SFN roaming.	The value is an integer that ranges from 300 to 1500, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The decision period for agile distributed SFN roaming helps you adjust the roaming sensitivity. A shorter period indicates a higher sensitivity. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance. The default value is recommended. Ensure that the interval at which RUs report STA RSSIs is smaller than the decision period for agile distributed SFN roaming.

Example

Set the default decision period for agile distributed SFN roaming to 800 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check check-interval 800
```

11.6.21 sfn-roam roam-check gap-rssi

Function

The **sfn-roam roam-check gap-rssi** command sets the RSSI gap for agile distributed SFN roaming RUs.

The **undo sfn-roam roam-check gap-rssi** command restores the default RSSI gap for agile distributed SFN roaming RUs.

The default RSSI gap for agile distributed SFN roaming RUs is 6 dB.

Format

sfn-roam roam-check gap-rssi *gap-rssi*

undo sfn-roam roam-check gap-rssi

Parameters

Parameter	Description	Value
gap-rssi	Specifies the RSSI gap for agile distributed SFN roaming RUs.	The value is an integer that ranges from 1 to 32, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The RSSI gap for agile distributed SFN roaming RUs helps you adjust the roaming sensitivity. A roaming handover occurs when the RSSI gap between the local RU and a surrounding RU reaches the specified value. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the RSSI gap for agile distributed SFN roaming RUs to 10 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check gap-rssi 10
```

11.6.22 sfn-roam roam-check high-threshold

Function

The **sfn-roam roam-check high-threshold** command sets the upper RSSI threshold for agile distributed SFN roaming.

The **undo sfn-roam roam-check high-threshold** command restores the default upper RSSI threshold for agile distributed SFN roaming.

By default, the upper RSSI threshold for agile distributed SFN roaming is -55 dBm.

Format

sfn-roam roam-check high-threshold *high-threshold-value*

undo sfn-roam roam-check high-threshold

Parameters

Parameter	Description	Value
high-threshold-value	Specifies the upper RSSI threshold for agile distributed SFN roaming.	The value is an integer that ranges from -60 to -45, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the STA RSSI threshold to control the sensitivity of agile distributed SFN roaming and prevent STAs from frequently roaming at radio borders of RUs. A roaming handover occurs when the total number of records in the following conditions exceeds the value specified by the **sfn-roam roam-check better-times** command:

- When the HAP detects that the STA RSSI is lower than the lower threshold: The central AP makes a record if the SNR of the FAP is higher than that of the HAP.
- When the HAP detects that the STA RSSI is between the upper and lower thresholds: The central AP makes a record if the SNR of the FAP is 3 dB higher than that of the HAP.
- When the HAP detects that the STA RSSI is higher than the upper threshold: The central AP makes a record if the SNR of the FAP is 5 dB higher than that of the HAP.

Precautions

The lower RSSI threshold for agile distributed SFN roaming must be no higher than the upper threshold.

Example

Set the upper RSSI threshold for agile distributed SFN roaming to -50 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check high-threshold -50
```

11.6.23 sfn-roam roam-check low-threshold

Function

The **sfn-roam roam-check low-threshold** command sets the lower RSSI threshold for agile distributed SFN roaming.

The **undo sfn-roam roam-check low-threshold** command restores the default lower RSSI threshold for agile distributed SFN roaming.

By default, the lower RSSI threshold for agile distributed SFN roaming is -60 dBm.

Format

sfn-roam roam-check low-threshold *low-threshold-value*

undo sfn-roam roam-check low-threshold

Parameters

Parameter	Description	Value
low-threshold-value	Specifies the lower RSSI threshold for agile distributed SFN roaming.	The value is an integer that ranges from -70 to -55, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the STA RSSI threshold to control the sensitivity of agile distributed SFN roaming and prevent STAs from frequently roaming at radio borders of RUs. A roaming handover occurs when the total number of records in the following conditions exceeds the value specified by the **sfn-roam roam-check better-times** command:

- When the HAP detects that the STA RSSI is lower than the lower threshold: The central AP makes a record if the SNR of the FAP is higher than that of the HAP.
- When the HAP detects that the STA RSSI is between the upper and lower thresholds: The central AP makes a record if the SNR of the FAP is 3 dB higher than that of the HAP.
- When the HAP detects that the STA RSSI is higher than the upper threshold: The central AP makes a record if the SNR of the FAP is 5 dB higher than that of the HAP.

Precautions

The lower RSSI threshold for agile distributed SFN roaming must be no higher than the upper threshold.

Example

Set the lower RSSI threshold for agile distributed SFN roaming to -65 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check low-threshold -65
```

11.6.24 sfn-roam roam-check rssi-accumulate

Function

The **sfn-roam roam-check rssi-accumulate** command sets the cumulative RSSI change threshold for agile distributed SFN roaming STAs.

The **undo sfn-roam roam-check rssi-accumulate** command restores the default cumulative RSSI change threshold for agile distributed SFN roaming STAs.

By default, the cumulative RSSI change threshold of agile distributed SFN roaming STAs is 8 dB.

Format

sfn-roam roam-check rssi-accumulate threshold *rssi-accumulate-value*

undo sfn-roam roam-check rssi-accumulate

Parameters

Parameter	Description	Value
threshold *rssi-accumulate-value*	Specifies the cumulative RSSI change threshold for agile distributed SFN roaming STAs.	The value is an integer that ranges from 1 to 32, in dB.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The cumulative RSSI change threshold of agile distributed SFN roaming STAs helps you adjust the roaming sensitivity. A roaming handover occurs when the cumulative RSSI change value reaches the specified threshold. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the cumulative RSSI change threshold for agile distributed SFN roaming STAs to 10 dB.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check rssi-accumulate threshold 10
```

11.6.25 sfn-roam roam-check sta-holding times

Function

The **sfn-roam roam-check sta-holding times** command sets the number of STA holding times for agile distributed SFN roaming.

The **undo sfn-roam roam-check sta-holding times** command restores the default number of STA holding times for agile distributed SFN roaming.

By default, the number of STA holding times for agile distributed SFN roaming is 3.

Format

sfn-roam roam-check sta-holding times *sta-holding-times*

undo sfn-roam roam-check sta-holding times

Parameters

Parameter	Description	Value
sta-holding-times	Specifies the number of STA holding times for agile distributed SFN roaming.	The value is an integer that ranges from 1 to 32.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

To prevent frequent agile distributed SFN roaming handovers, you can specify a proper number of STA holding times. A large value causes a slow roaming handover, affecting user experience. A small value causes frequent roaming handovers, affecting system performance.

Example

Set the number of STA holding times for agile distributed SFN roaming to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name wlan-rrm
[HUAWEI-wlan-rrm-prof-wlan-rrm] sfn-roam roam-check sta-holding times 5
```

11.6.26 inter-ac roam disable

Function

The **inter-ac roam disable** command disables inter-AC roaming.

The **undo inter-ac roam disable** command enables inter-AC roaming.

By default, inter-AC roaming is enabled.

Format

inter-ac roam disable

undo inter-ac roam disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

If STAs roam from one AC to another, they have to be re-authenticated to access the network. To limit the STA roaming scope within an AC, you can run the **inter-ac roam disable** command to disable inter-AC roaming.

Example

Disable inter-AC roaming.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name default
[HUAWEI-wlan-ssid-prof-default] inter-ac roam disable
```

11.7 WLAN QoS Configuration Commands

11.7.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.7.2 airtime-fair-schedule enable

Function

The **airtime-fair-schedule enable** command enables airtime fair scheduling on an AP radio.

The **undo airtime-fair-schedule enable** command disables airtime fair scheduling on an AP radio.

By default, airtime fair scheduling is disabled on an AP radio.

Format

airtime-fair-schedule enable

undo airtime-fair-schedule enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a WLAN, the physical layer rates of users have great differences due to different radio modes supported by the terminals or radio environment where the terminals reside. If the users with lower physical layer rates occupy wireless channels for a long period, user experience of the entire WLAN is affected. Airtime fair scheduling calculates the channel occupation time of users transmitting the same service and preferentially schedules resources for the users who occupy the wireless channel for a shorter period. This ensures fairness in channel usage.

After airtime fair scheduling is enabled, the device collects statistics on the channel occupation time used by users connected to the same radio for sending packets, creates the mapping table for the channel occupation time of each user in accumulated mode, and establishes a sorted link table based on the time in an ascending order. Based on the mapping table, an AP transmits data with the user who occupies the channel for the shortest time, ensuring that each user can equally occupy the wireless channels. The data packets of high-speed users are transmitted quickly, which is not affected by the data transmission time of low-speed users. This improves the overall user experience.

After WMM is enabled on the device and terminals, user packets are scheduled based on different types (service types include VI, VO, BE, and BK). For example, voice packets are scheduled only with other voice packets, and video packets are scheduled only with other video packets.

Precautions

If the packets of multiple users are of different types, airtime fair scheduling is not performed. For example, two users perform packet transmission: one transmits voice packets and the other transmits video packets. In this case, airtime fair scheduling is not performed for the two users.

When the command is executed, the system displays the message "Warning: This action may cause service interruption. Continue?[Y/N]", asking you whether you want to continue.

The airtime fair scheduling function is supported by the following models (enabled by default and cannot be configured using commands):

- AirEngine X760 series APs
- AirEngine X761 series APs

- AirEngine X762 series APs
- AirEngine X771 series APs
- AirEngine series central APs and RUs
- AirEngine 9700D-S (including matching ORUs)

Example

Enable airtime fair scheduling in RRM profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name default
[HUAWEI-wlan-rrm-prof-default] airtime-fair-schedule enable
```

11.7.3 app-share remark

Function

The **app-share remark** command sets a priority for Lync desktop sharing packets.

The **undo app-share remark** command deletes the priority of Lync desktop sharing packets.

By default, the priority of Lync desktop sharing packets is not set.

Format

app-share remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo app-share remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: ● af1: 1 ● af2: 2 ● af3: 3 ● af4: 4 ● be: 0 ● cs6: 6 ● cs7: 7 ● ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **app-share remark** command to change the priority of Lync desktop sharing packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync desktop sharing packets of one Lync session.

If you run the **app-share remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync desktop sharing packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync desktop sharing packets to 1 in the UCC profile **test**.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] app-share remark dscp 1
```

11.7.4 display references traffic-profile

Function

The **display references traffic-profile** command displays reference information about a traffic profile.

Format

display references traffic-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified traffic profile.	The traffic profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the VAP profiles by which a specified traffic profile is referenced.

Example

Display reference information about the traffic profile **p1**.

```
<HUAWEI> display references traffic-profile name p1
----------------------------------------------------
Reference type     Reference name
----------------------------------------------------
VAP profile        default
VAP profile        wlan-vap
VAP profile        exam
VAP profile        test
VAP profile        wlan-vap1
VAP profile        example
VAP profile        2
----------------------------------------------------
Total: 7
```

Table 11-165 Description of the **display references traffic-profile** command output

Item	Description
Reference type	Type of the profile that references a traffic profile.
Reference name	Name of the profile that references a traffic profile.

11.7.5 display service-experience-analysis monitor-list

Function

The **display service-experience-analysis monitor-list** command displays information about applications monitored based on SEA.

Format

display service-experience-analysis monitor-list [**sta-mac** *sta-mac-address*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays information about SEA-monitored applications on the STA with a specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to check information about applications monitored based on SEA, including the STA's MAC address, AP with which the STA is associated, and 5-tuple information in the flow table.

Example

Display information about applications monitored based on SEA.

```
<HUAWEI> display service-experience-analysis monitor-list
-------------------------------------------------------------------------------------------------------------------
STA MAC         AP ID AP name Radio ID Protocol Source IP/Port Destination IP/Port
-------------------------------------------------------------------------------------------------------------------
1000-0000-0001   1     AP1     1        23       1.1.1.1/100    2.2.2.2/2000
-------------------------------------------------------------------------------------------------------------------
Total: 1
```

Table 11-166 Description of the **display service-experience-analysis monitor-list** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	ID of the AP with which a STA is associated.
AP name	Name of the AP with which a STA is associated.
Radio ID	Radio ID of the AP with which a STA is associated.
Protocol	IP protocol number.
Source IP/Port	Source IP address and source port number.
Destination IP/Port	Destination IP address and destination port number.

11.7.6 display traffic-profile

Function

The **display traffic-profile** command displays configuration information about traffic profiles.

Format

display traffic-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays configuration information about all traffic profiles.	-

Parameter	Description	Value
name *profile-name*	Displays configuration information about a specified traffic profile.	The value is a string of 1 to 35 characters without spaces and question marks (?). It cannot begin or end with a double quotation mark (").

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the default configurations of a new traffic profile or configurations of an existing traffic profile.

Example

Display configuration information about a traffic profile that maps the trusted user priority from 802.11 packets to tunnel packets when packets are sent from an AP to the AC.

```
<HUAWEI> display traffic-profile name p1
------------------------------------------------------------------------------------------
Profile ID                                    : 0
User isolate mode                             : disable
Rate limit client up(Kbps)                    : 4294967295
Rate limit client up(Kbps) with time-range    : -
Rate limit client down(Kbps)                  : 4294967295
Rate limit client down(Kbps) with time-range  : -
Rate limit VAP up(Kbps)                       : 4294967295
Rate limit VAP down(Kbps)                     : 4294967295
Rate limit client dynamic switch              : enable
Rate limit client dynamic(Mbps)               : 16
Traffic optimize ARP proxy                    : disable
Traffic optimize ND proxy                     : disable
Traffic optimize ARP unicast send             : enable
Traffic optimize ND unicast send              : enable
Traffic optimize DHCP unicast send            : enable
Traffic optimize mDNS unicast send            : enable
Traffic optimize multicast send deny          : disable
Traffic optimize mdns forward                 : enable
Traffic optimize TCP adjust MSS(bytes)        : -
Traffic optimize bcmc unicast send mismatch action : drop
MLD snooping                                  : disable
IGMP snooping                                 : disable
IGMP snooping report suppress                 : disable
Spectralink voice priority                    : disable
Priority map upstream trust                   : 8021e
IGMP snooping max bandwidth(kbps)             : -
```

```
IGMP snooping max user                               : -
Traffic optimize sta bridge forward                  : enable
Traffic optimize broadcast suppression(pps)          : -
Traffic optimize multicast suppression(pps)          : -
Traffic optimize unicast suppression(pps)            : -
Traffic optimize multicast to unicast                : disable
  Dynamic adaptive                                   : enable
Priority map tunnel upstream trust                   : 8021e
CAPWAP priority upstream map mode  : 802.11e map DSCP
                                    0 map 0
                                    1 map 8
                                    2 map 16
                                    3 map 24
                                    4 map 32
                                    5 map 40
                                    6 map 48
                                    7 map 56
CAPWAP priority upstream map mode  : 802.11e map 802.1p
                                    0 map 0
                                    1 map 1
                                    2 map 2
                                    3 map 3
                                    4 map 4
                                    5 map 5
                                    6 map 6
                                    7 map 7
Priority map downstream trust                        : DSCP
WMM priority downstream map mode   : DSCP map 802.11e
                                    0-7 map 0
                                    8-15 map 1
                                    16-23 map 2
                                    24-31 map 3
                                    32-39 map 4
                                    40-47 map 5
                                    48-55 map 6
                                    56-63 map 7
WMM priority downstream map mode   : 802.1p map 802.11e
                                    0 map 0
                                    1 map 1
                                    2 map 2
                                    3 map 3
                                    4 map 4
                                    5 map 5
                                    6 map 6
                                    7 map 7
-------------------------------------------------------------------------------------------
Traffic Type                      Direction   AppliedRecord
-------------------------------------------------------------------------------------------
traffic-filter                    inbound     IPv4 ACL 3001 & L2 ACL 4001
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------
Traffic Type                      Direction   RemarkType   RemarkValue   AppliedRecord
-------------------------------------------------------------------------------------------
traffic-remark                    inbound     802.11e      0             IPv4 ACL 3001
-------------------------------------------------------------------------------------------
Wlan-slice high-reliability traffic filter info:
AppliedRecord: IPv4 ACL 3001
```

Table 11-167 Description of the **display traffic-profile** command output

Item	Description
Profile ID	Traffic profile ID.

Item	Description
Priority map downstream trust	Mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11 user priority when 802.3 packets are sent to an AP from upper-layer devices. To configure this parameter, run the **priority-map downstream trust** command.
User isolate mode	Whether user isolation is enabled. To configure this parameter, run the **user-isolate (traffic profile view)** command.
Rate limit client up(Kbps)	Upstream rate limit configured for STAs. To configure this parameter, run the **rate-limit** command.
Rate limit client up(Kbps) with time-range	Upstream rate limit configured for STAs in a specified time range. To configure this parameter, run the **rate-limit client time-range** command.
Rate limit client down(Kbps)	Downstream rate limit configured for STAs. To configure this parameter, run the **rate-limit** command.
Rate limit client down(Kbps) with time-range	Downstream rate limit configured for STAs in a specified time range. To configure this parameter, run the **rate-limit client time-range** command.
Rate limit VAP up(Kbps)	Upstream rate limit configured for a VAP. To configure this parameter, run the **rate-limit** command.
Rate limit VAP down(Kbps)	Downstream rate limit configured for a VAP. To configure this parameter, run the **rate-limit** command.

Item	Description
Rate limit client dynamic switch	Whether dynamic rate limiting is enabled for a single STA on a VAP. To configure this parameter, run the **rate-limit client dynamic disable** command.
Rate limit client dynamic(Mbps)	Dynamic rate limit threshold for a single STA on a VAP. To configure this parameter, run the **rate-limit client dynamic** command.
Traffic optimize ARP proxy	Whether proxy ARP is enabled for STAs. To configure this parameter, run the **traffic-optimize arp-proxy enable** command.
Traffic optimize ND proxy	Whether ND proxy is enabled for STAs. To configure this parameter, run the **traffic-optimize np-proxy enable** command.
Traffic optimize ARP unicast send	Whether the air interface is enabled to convert broadcast ARP packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.
Traffic optimize ND unicast send	Whether the air interface is enabled to convert multicast ND packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.
Traffic optimize DHCP unicast send	Whether the air interface is enabled to convert broadcast DHCP packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.
Traffic optimize mDNS unicast send	Whether the air interface is enabled to convert broadcast mDNS packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send** command.

Item	Description
Traffic optimize multicast send deny	Whether the air interface is disabled from forwarding multicast packets. To configure this parameter, run the **traffic-optimize bcmc deny all** command.
Traffic optimize mdns forward	Whether the air interface allows mDNS packets to pass through. ● enable: The function of denying multicast packets on the air interface is disabled, or this function is enabled but mDNS packets are excluded. ● disable: The air interface is disabled from forwarding multicast packets and does not allow mDNS packets to pass through. To configure this parameter, run the **traffic-optimize bcmc deny all** command.
Traffic optimize sta bridge forward	Whether the air interface is configured to deny packets destined for bridge STAs. To configure this parameter, run the **traffic-optimize sta-bridge-forward disable** command.
Traffic optimize bcmc unicast send mismatch action	Action to be taken when the air interface fails to convert broadcast or multicast protocol packets into unicast packets. To configure this parameter, run the **traffic-optimize bcmc unicast-send mismatch-action drop** command.
MLD snooping	Whether MLD snooping is enabled. To configure this parameter, run the **mld-snooping enable (traffic profile view)** command.
IGMP snooping	Whether IGMP snooping is enabled. To configure this parameter, run the **igmp-snooping enable (traffic profile view)** command.

Item	Description
Spectralink voice priority	Whether SVP voice traffic optimization is enabled. To configure this parameter, run the **svp-voice enable** command.
IGMP snooping report suppress	IGMP message suppression time. To configure this parameter, run the **igmp-snooping report-suppress (traffic profile view)** command.
IGMP snooping max bandwidth(kbps)	Maximum multicast bandwidth of a VAP. To configure this parameter, run the **igmp-snooping max-bandwidth (traffic profile view)** command.
IGMP snooping max user	Maximum number of multicast group memberships on a VAP. To configure this parameter, run the **igmp-snooping max-user (traffic profile view)** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an interface. To configure this parameter, run the **traffic-optimize broadcast-suppression** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an interface. To configure this parameter, run the **traffic-optimize multicast-suppression** command.
Traffic optimize unicast suppression(pps)	Maximum unicast traffic volume allowed on an interface. To configure this parameter, run the **traffic-optimize unicast-suppression** command.
Traffic optimize multicast to unicast	Whether multicast-to-unicast conversion is enabled. To configure this parameter, run the **traffic-optimize multicast-unicast enable** command.

Item	Description
Dynamic adaptive	Whether adaptive multicast-to-unicast conversion is enabled. To configure this parameter, run the **traffic-optimize multicast-unicast dynamic-adaptive disable** command.
CAPWAP priority upstream map mode	Mapping from the WMM priority of upstream tunnel packets to the DSCP priority.
Priority map tunnel upstream trust	Trusted priority mapping from 802.11 packets to tunnel packets when data packets are sent to the AC from an AP. To configure this parameter, run the **priority-map tunnel-upstream trust** command.
Priority map upstream trust	Trusted priority mapping from 802.11 packets to 802.3 packets when data packets are sent to the AC from an AP. To configure this parameter, run the **priority-map upstream trust** command.
WMM priority downstream map mode	Mapping from the DSCP priority of downstream packets to the WMM priority.
priority upstream map mode	Tunnel upstream mapping when the trusted mapping from 802.11 packets to tunnel packets is DSCP, and data packets are sent to the AC from an AP.
Traffic Type	Traffic control type.
Direction(Traffic Type: traffic-filter)	Direction to which packet filtering is applied. To configure this parameter, run the **traffic-filter (traffic profile view)** command.
AppliedRecord(Traffic Type: traffic-filter)	Application records of ACL-based packet filtering. To configure this parameter, run the **traffic-filter (traffic profile view)** command.

Item	Description
Direction(Traffic Type: traffic-remark)	Direction to which packet priority re-marking is applied. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
RemarkType	Packet priority re-marking type. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
RemarkValue	Re-marked packet priority value. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
AppliedRecord(Traffic Type: traffic-remark)	Application records of ACL-based packet priority re-marking. To configure this parameter, run the **traffic-remark (traffic profile view)** command.
AppliedRecord(Wlan-slice high-reliability traffic filter info)	ACL-based rule records for air interface slicing. To configure this parameter, run the **wlan-slice high-reliability acl** command.

Display configurations of all traffic profiles.

```
<HUAWEI> display traffic-profile all
----------------------------------------------------
Profile name                      Reference
----------------------------------------------------
default                          3
1                                1
p1                               0
----------------------------------------------------
Total: 3
```

Table 11-168 Description of the **display traffic-profile all** command output

Item	Description
Profile name	Profile name. To configure this parameter, run the **traffic-profile (WLAN view)** command.
Reference	Number of times a traffic profile is referenced.

11.7.7 display ucc-profile

Function

The **display ucc-profile** command displays the UCC profile configuration and application.

Format

display ucc-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all UCC profiles.	-
name *profile-name*	Displays information about the specified UCC profile.	The value must be the name of an existing UCC profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a UCC profile is configured, run the **display ucc-profile** command to check the UCC profile configuration and information about the UCC profile bound to a VAP profile.

Example

Display information about all UCC profiles.

```
<HUAWEI> display ucc-profile all
----------------------------------------------------------
Profile name                  Reference
----------------------------------------------------------
test                        1
----------------------------------------------------------
```

Table 11-169 Description of the **display ucc-profile all** command output

Item	Description
Profile name	Name of the UCC profile.
Reference	Number of times the UCC profile is bound to the VAP profile.

Display information about the UCC profile **test**.

```
<HUAWEI> display ucc-profile name test
----------------------------------------------------------------------------------
Lync app share 802.1p precedence     : -
Lync app share DSCP precedence       : -
Lync app share local precedence      : -
Lync file transfer 802.1p precedence : -
Lync file transfer DSCP precedence   : -
Lync file transfer local precedence  : -
Lync video 802.1p precedence         : 6
Lync video DSCP precedence           : -
Lync video local precedence          : -
Lync voice 802.1p precedence         : -
Lync voice DSCP precedence           : -
Lync voice local precedence          : -
----------------------------------------------------------------------------------
```

Table 11-170 Description of the **display ucc-profile name test** command output

Item	Description
Lync app share 802.1p precedence	802.1p priority of Lync desktop sharing packets. To configure the 802.1p priority of Lync desktop sharing packets, run the **app-share remark** command.
Lync app share DSCP precedence	DSCP priority of Lync desktop sharing packets. To configure the DSCP priority of Lync desktop sharing packets, run the **app-share remark** command.
Lync app share local precedence	Local priority of Lync desktop sharing packets. To configure the local priority of Lync desktop sharing packets, run the **app-share remark** command.
Lync file transfer 802.1p precedence	802.1p priority of Lync file transfer packets. To configure the 802.1p priority of Lync file transfer packets, run the **file-transfer remark** command.

Item	Description
Lync file transfer DSCP precedence	DSCP priority of Lync file transfer packets. To configure the DSCP priority of Lync file transfer packets, run the **file-transfer remark** command.
Lync file transfer local precedence	Local priority of Lync file transfer packets. To configure the local priority of Lync file transfer packets, run the **file-transfer remark** command.
Lync video 802.1p precedence	802.1p priority of Lync video packets. To configure the 802.1p priority of Lync video packets, run the **video remark** command.
Lync video DSCP precedence	DSCP priority of Lync video packets. To configure the DSCP priority of Lync video packets, run the **video remark** command.
Lync video local precedence	Local priority of Lync video packets. To configure the local priority of Lync video packets, run the **video remark** command.
Lync voice 802.1p precedence	802.1p priority of Lync voice packets. To configure the 802.1p priority of Lync voice packets, run the **voice remark** command.
Lync voice DSCP precedence	DSCP priority of Lync voice packets. To configure the DSCP priority of Lync voice packets, run the **voice remark** command.
Lync voice local precedence	Local priority of Lync voice packets. To configure the local priority of Lync voice packets, run the **voice remark** command.

11.7.8 file-transfer remark

Function

The **file-transfer remark** command sets a priority for Lync file transfer packets.

The **undo file-transfer remark** command deletes the priority of Lync file transfer packets.

By default, the priority of Lync file transfer packets is not set.

Format

file-transfer remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo file-transfer remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: ● af1: 1 ● af2: 2 ● af3: 3 ● af4: 4 ● be: 0 ● cs6: 6 ● cs7: 7 ● ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **file-transfer remark** command to change the priority of Lync file transfer packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync file transfer packets of one Lync session.

If you run the **file-transfer remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync file transfer packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync file transfer packets to 1 in the UCC profile **test**.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] file-transfer remark dscp 1
```

11.7.9 game-turbo disable

Function

The **game-turbo disable** command disables the game-turbo function.

The **undo game-turbo disable** command enables the game-turbo function.

By default, the game-turbo function is enabled.

NOTE

The game turbo function is not supported by the following models:

- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W

Format

game-turbo disable

undo game-turbo disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you are playing online games through a WLAN, a network latency may easily lead to skill out-of-control or slow response to actions, deteriorating user experience. In this case, you can enable the game-turbo function to optimize game traffic and reduce the game latency.

Currently, the game-turbo function is available for the following mobile games: *Game for Peace*, *Arena of Valor*, and *World of Tanks Blitz*.

Precautions

Before enabling the game-turbo function, enable the DFI function for application identification.

Example

Enable the game-turbo function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] undo game-turbo disable
```

11.7.10 lync acl

Function

The **lync acl** command configures the switch to use an ACL to filter packets sent by the Lync server.

The **undo lync acl** command cancels the configuration.

By default, the switch does not use any ACL to filter packets sent by the Lync server.

Format

lync acl *acl-number*

undo lync acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL. The basic or advanced ACL must have been created.	The value is an integer. ● A basic ACL ranges from 2000 to 2999. ● An advanced ACL ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch communicates with the Lync server, to prevent the switch against many packets sent by bogus Lync servers, run the **lync acl** command to configure the switch to use an ACL to filter packets sent by the Lync server.

Prerequisites

A basic or advanced ACL has been created and rules have been configured.

Example

Configure ACL 2001 to allow packets that carry the source address of 192.168.32.1 and are sent by the Lync server.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.32.1 0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] lync acl 2001
```

11.7.11 lync listener

Function

The **lync listener** command configures the switch to communicate with the Lync server and specifies the port number.

The **undo lync listener** command cancels the configuration.

By default, the switch is not configured to communicate with the Lync server and the port number is not specified.

Format

lync listener { **http-port** *port-num* | **https-port** *port-num* **ssl-policy** *ssl-policy* }

undo lync listener

Parameters

Parameter	Description	Value
http-port *port-num*	Specifies the port number of the HTTP service.	The value is an integer that ranges from 1025 to 55535.
https-port *port-num*	Specifies the port number of the HTTPS service.	The value is an integer that ranges from 1025 to 55535.
ssl-policy *ssl-policy*	Specifies the SSL policy to be bound. The SSL policy must be a server SSL policy.	The value must be the name of an existing SSL policy.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. To ensure normal running of Lync software, configure the switch to communicate with the Lync server.

Precautions

To prevent the impact on the exchange with the Lync server, you are advised to use the port number that is not in use. You can run the **display ip socket register-port** command to check used port numbers.

Example

Configure the switch to communicate with the Lync server and specify HTTP port 2000.

```
<HUAWEI> system-view
[HUAWEI] lync listener http-port 2000
```

11.7.12 multimedia-air-optimize congestion-control tcp-window-tuning disable

Function

The **multimedia-air-optimize congestion-control tcp-window-tuning disable** command disables the TCP window adjustment function for voice and video services.

The **undo multimedia-air-optimize congestion-control tcp-window-tuning disable** command enables the TCP window adjustment function for voice and video services.

By default, the TCP window adjustment function for voice and video services is enabled.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize congestion-control tcp-window-tuning disable

undo multimedia-air-optimize congestion-control tcp-window-tuning disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA has heavy-traffic services of the AC_BE or AC_BK type in the uplink, packets are frequently sent, and the duration of a single packet transmission is long, the delay of key services in the downlink of the AP is significantly increased. If key downlink services are affected, the system considers performing congestion control on heavy-traffic services of the AC_BE or AC_BK type. The **multimedia-air-optimize congestion-control tcp-window-tuning disable** command is involved for AP uplink congestion control. After the **undo multimedia-air-optimize congestion-control tcp-window-tuning disable** command is executed, the TCP window adjustment function is enabled for voice and video services. If the delay of voice or video services reaches the threshold and the packet transmission duration of heavy-traffic TCP background services in the uplink reaches the threshold within the unit time (1s), the receiver window (RWND) in TCP ACK packets can be dynamically adjusted. This process takes about 5s to 10s. After the adjustment, the uplink data volume sent by STAs is reduced, thereby ensuring user experience of voice and video services.

Prerequisites

The intelligent multimedia scheduling algorithm has been enabled using the **undo multimedia-air-optimize disable** command.

Example

Enable the TCP window adjustment function for voice and video services.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize disable
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize congestion-control tcp-window-tuning
disable
```

11.7.13 multimedia-air-optimize downlink-delay-guarantee

Function

The **multimedia-air-optimize downlink-delay-guarantee** command configures the guaranteed delay for services of different categories.

The **undo multimedia-air-optimize downlink-delay-guarantee** command restores the default guaranteed delay for services of different categories.

The default guaranteed delay for services of different categories is **medium**.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize downlink-delay-guarantee { **voice** | **video** | **best-effort** | **background** } { **low** | **medium** | **high** | **off** }

undo multimedia-air-optimize downlink-delay-guarantee

Parameters

Parameter	Description	Value
voice	Specifies voice (AC_VO) packets.	-
video	Specifies video (AC_VI) packets.	-
best-effort	Specifies best-effort (AC_BE) packets.	-
background	Specifies background (AC_BK) packets.	-
low	Sets the guaranteed delay for the service of a specified category to **low**. For specific values, see **Table 11-171**.	-
medium	Sets the guaranteed delay for the service of a specified category to **medium**. For specific values, see **Table 11-171**.	-
high	Sets the guaranteed delay for the service of a specified category to **high**. For specific values, see **Table 11-171**.	-
off	Specifies no delay guarantee for the service of a specified category.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If users have requirements for the delay of voice, best-effort, background, and video services on the air interface, run the **multimedia-air-optimize downlink-delay-guarantee** command to configure the guaranteed delay for voice and video services. With this configuration, the system monitors the delay of services on the air interface in real time. When detecting the delay exceeding the guaranteed delay, the system triggers delay optimization for the corresponding service to ensure that the delay after optimization does not exceed the guaranteed delay.

Table 11-171 Delay guarantee for services

Parameter	Video (UP: 4)	Video (UP: 5)	Voice	Best-Effort	Background
low	Delay < 300 ms	Delay < 100 ms	Delay < 50 ms	Delay < 400 ms	Delay < 500 ms
medium	Delay < 200 ms	Delay < 50 ms	Delay < 20 ms	Delay < 300 ms	Delay < 400 ms
high	Delay < 100 ms	Delay < 20 ms	Delay < 5 ms	Delay < 200 ms	Delay < 300 ms
off	No delay guarantee	No delay guarantee	No delay guarantee	No delay guarantee	No delay guarantee

- UP 4: video applications that support caching, such as online network video and live streaming
- UP 5: video applications that do not support caching, such as network videoconferencing

Prerequisites

The intelligent multimedia scheduling algorithm has been enabled using the **undo multimedia-air-optimize disable** command.

Example

Set the guaranteed delay for video services to **low** and that for voice services to **high**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize disable
[HUAWEI-wlan-rrm-prof-p1] multimedia-air-optimize downlink-delay-guarantee video low
[HUAWEI-wlan-rrm-prof-p1] multimedia-air-optimize downlink-delay-guarantee voice high
```

11.7.14 multimedia-air-optimize disable

Function

The **multimedia-air-optimize disable** command disables the intelligent multimedia scheduling algorithm.

The **undo multimedia-air-optimize disable** command enables the intelligent multimedia scheduling algorithm.

By default, the intelligent multimedia scheduling algorithm is enabled.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize disable

undo multimedia-air-optimize disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the intelligent multimedia scheduling algorithm is enabled, the system optimizes the air interface traffic in the following aspects:

- Delay guarantee for downlink VI/VO/BE/BK services on an AP

  The system periodically calculates the air interface delay of downlink VI/VO/BE/BK services. When detecting that the current delay exceeds the configured guaranteed delay, the system triggers service delay optimization. The guaranteed delay for VI/VO/BE/BK services is configured using the **multimedia-air-optimize downlink-delay-guarantee** command. After delay optimization for services is complete, the system tries its best to ensure that the service delay does not exceed the guaranteed delay. In addition, the system restricts the VI/VO/BE/BK services of low-speed STAs. Low-speed STAs typically have low transmission efficiency and occupy air interface resources for a long time, increasing the overall delay of VI/VO/BE/BK services. Therefore, the transmission opportunity for such STAs needs to be reduced.

- Delay guarantee for uplink services on an AP

  The system periodically calculates the air interface delay of uplink services (mainly voice and video services, with a user priority of 5 or higher). When detecting that the current delay exceeds the guaranteed delay, the system triggers service delay optimization. The delay guarantee function for uplink services on an AP can be enabled by using the **undo multimedia-air-optimize uplink-delay-guarantee disable** command. After delay optimization for services is complete, the system tries its best to ensure that the service delay does not exceed the guaranteed delay. In addition, the system restricts the uplink services of low-speed STAs. Low-speed STAs typically have low transmission efficiency and occupy air interface resources for a long time, increasing the overall delay of uplink services. Therefore, the transmission opportunity for such STAs needs to be reduced.

- Preferential scheduling for downlink VI/VO services on an AP

  During software scheduling, VI/VO services are preferentially scheduled. That is, each time the scheduler queries queue information, if the total packet sending time of the current VI/VO queue does not exceed the threshold, the services in the video/voice queue are preferentially scheduled. The threshold is calculated based on the slicing ratio for voice and video services configured using the **multimedia-air-optimize downlink-slice-ratio** command.

- Uplink congestion control for an AP

  When a STA has heavy-traffic services of the AC_BE or AC_BK type in the uplink, packets are frequently sent, and the duration of a single packet transmission is long, the delay of key services in the downlink of the AP is significantly increased. If key downlink services are affected, the system considers performing congestion control on heavy-traffic services of the AC_BE or AC_BK type. The **multimedia-air-optimize congestion-control tcp-window-tuning disable** command is involved for AP uplink congestion control. After the **undo multimedia-air-optimize congestion-control tcp-window-tuning disable** command is executed, the TCP window adjustment function is enabled for voice and video services. If the delay of voice or video services reaches the threshold and the packet transmission duration of heavy-traffic TCP background services in the uplink reaches the threshold within the unit time (1s), the receiver window (RWND) in TCP ACK packets can be dynamically adjusted. This process takes about 5s to 10s. After the adjustment, the uplink data volume sent by STAs is reduced, thereby ensuring user experience of voice and video services.

- WMM parameter adjustment based on the number of access STAs

  After the intelligent multimedia scheduling algorithm is enabled, the system dynamically adjusts WMM parameters based on the number of access users, improving voice and video service experience.

  The number of voice/video users is identified based on the user packet threshold configured using the **multimedia-air-optimize threshold** command. If the number of voice or video packets sent by a user in the internal statistics queue of a radio within the unit time (1 second) exceeds the threshold, the user is considered a voice or video user.

Ensure that the WMM function is enabled (default). To enable the WMM function, run the **undo wmm disable**.

Precautions

After the **undo multimedia-air-optimize disable** command is executed, the **wmm edca-ap** and **wmm edca-client (SSID profile view)** commands do not take effect.

Example

Enable the intelligent multimedia scheduling algorithm in the RRM profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] undo multimedia-air-optimize disable
```

11.7.15 multimedia-air-optimize threshold

Function

The **multimedia-air-optimize threshold** command sets a user packet threshold in the intelligent multimedia scheduling algorithm.

The **undo multimedia-air-optimize threshold** command restores the default user packet threshold.

By default, the video user packet threshold is 100 pps, and the default voice user packet threshold is 30 pps.

NOTE

The intelligent multimedia scheduling algorithm is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W)
- AirEngine 9700D-S (including matching ORUs)

Format

multimedia-air-optimize threshold { **video** *video* | **voice** *voice* } *

undo multimedia-air-optimize threshold

Parameters

Parameter	Description	Value
video *video*	Specifies the video packet threshold.	The value is an integer that ranges from 10 to 1000.
voice *voice*	Specifies the voice packet threshold.	The value is an integer that ranges from 10 to 1000.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the intelligent multimedia scheduling algorithm is enabled, the system uses algorithms to dynamically adjust EDCA parameters and ACK policies based on the number of access users, improving user experience of voice and video applications.

Prerequisites

The intelligent multimedia scheduling algorithm has been enabled using the **undo multimedia-air-optimize disable** command.

Example

Set the user packet thresholds for voice and video services in the intelligent multimedia scheduling algorithm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] multimedia-air-optimize threshold video 100 voice 30
```

11.7.16 priority-map downstream dot1p

Function

The **priority-map downstream dot1p** command configures mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream dot1p** command restores the default mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets when packets are sent to an AP from upper-layer devices.

By default, 802.1p priority 0 of 802.3 packets maps to user priority 0 of 802.11 packets, 802.1p priority 1 to user priority 1, and similarly, 802.1p priority 7 to user priority 7.

Format

priority-map downstream dot1p { *dot1p-value1* [**to** *dot1p-value2*] } &<1-7> **dot11e** *dot11e-value*

undo priority-map downstream dot1p

Parameters

Parameter	Description	Value
dot1p *dot1p-value1*	Specifies the 802.1p priority in an 802.3 packet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot1p-value2*	Specifies the 802.1p priority in an 802.3 packet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. *dot1p-value2* must be greater than *dot1p-value1*.
dot11e *dot11e-value*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and VLAN tagged-802.3 packets transmitted on the Ethernet contain 802.1p priorities (also called the CoS field). When data packets are forwarded from the AC or upper-layer network to an AP, the AP needs to convert the 802.3 packets to 802.11 packets and map the 802.1p priority carried in the 802.3 packet header to the user priority of 802.11 packets. You can use the **priority-map downstream dot1p** command to configure mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets.

Example

Configure the mapping from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map downstream dot1p 0 dot11e 2
```

11.7.17 priority-map downstream dscp

Function

The **priority-map downstream dscp** command configures mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream dscp** command restores the default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets when packets are sent to an AP from upper-layer devices.

Table 11-172 describes the default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets.

Table 11-172 Default mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets

DSCP	UP
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map downstream dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map downstream dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. *dscp-value2* must be greater than *dscp-value1*.
dot11e *dot11e-value*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and IP packets transmitted on an Ethernet carry the DSCP priority (also called the ToS field). When data packets are forwarded from the central AP or upper-layer network to an RU, the RU needs to convert the 802.3 packets to 802.11 packets and map the ToS field in the IP packet header to the UP field of 802.11 packets. You can use the **priority-map downstream dscp** command to configure mapping from the DSCP priority of 802.3 packets to the user priority of 802.11 packets.

Example

Configure mapping from the DSCP priority of 802.3 packets in traffic profile **p1** to the user priority of 802.11 packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map downstream dscp 0 to 6 dot11e 0
```

11.7.18 priority-map downstream trust

Function

The **priority-map downstream trust** command configures a trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream trust** command restores the default trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

By default, the DSCP priority is used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

Format

priority-map downstream trust { **dot1p** | **dscp** }

undo priority-map downstream trust

Parameters

Parameter	Description	Value
dot1p	Specifies the 802.1p priority as the trusted priority type used in mapping from 802.3 packets to 802.11 packets.	-
dscp	Specifies the DSCP priority as the trusted priority type used in mapping from 802.3 packets to 802.11 packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field). On a wired network, VLAN packets carry the 802.1p priority and IP packets carry the DSCP priority. When data packets are forwarded from the AC or other upper-layer devices to an AP, the packets must be converted from 802.3 packets to 802.11 packets.

You can run the **priority-map downstream trust** command to configure a trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

Example

In traffic profile **p1**, configure the 802.1p priority as the trusted priority type used in mapping from 802.3 packets to 802.11 packets when packets are sent to an AP from upper-layer devices.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map downstream trust dot1p
```

11.7.19 priority-map tunnel-upstream dot11e dscp

Function

The **priority-map tunnel-upstream dot11e dscp** command configures mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dot11e dscp** command restores the default mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

Table 11-173 describes the default mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets.

NOTE

The CAPWAP header refers to the tunnel header.

Table 11-173 Default mapping from user priorities of 802.11 packets to DSCP priorities in CAPWAP headers

User Priority of 802.11 Packets	DSCP Priority in the CAPWAP Header
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Format

priority-map tunnel-upstream dot11e { *dot11e-value1* [**to** *dot11e-value2*] } &<1-7> **dscp** *dscp-value*

undo priority-map tunnel-upstream dot11e to dscp

Parameters

Parameter	Description	Value
dot11e *dot11e-value1*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot11e-value2*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. *dot11e-value2* must be greater than *dot11e-value1*.
dscp *dscp-value*	Specifies the DSCP priority of tunnel packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry the user priority (Layer 2) or DSCP priority (Layer 3), and tunnel packets carry the 802.1p priority (Layer 2) or tunnel DSCP priority (Layer 3). 802.11 packets sent to the AC from an AP must be converted into tunnel packets.

You can run the **priority-map tunnel-upstream dot11e dscp** command to configure mapping from the user priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, configure mapping from user priority 6 of 802.11 packets to DSCP priority 1 of tunnel packets when packets are sent to the AC from an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dot11e 6 dscp 1
```

11.7.20 priority-map tunnel-upstream dot11e dot1p

Function

The **priority-map tunnel-upstream dot11e dot1p** command configures mapping from user priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dot11e dot1p** command restores the default mapping from user priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

By default, user priority 0 of 802.11 packets maps to 802.1p priority 0 of tunnel packets, user priority 1 to 802.1p priority 1, and similarly, user priority 7 to 802.1p priority 7.

Format

priority-map tunnel-upstream dot11e { *dot11e-value1* [**to** *dot11e-value2*] } &<1-7> **dot1p** *dot1p-value*

undo priority-map tunnel-upstream dot11e to dot1p

Parameters

Parameter	Description	Value
dot11e *dot11e-value1*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
to *dot11e-value2*	Specifies the user priority of 802.11 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. *dot11e-value2* must be greater than *dot11e-value1*.
dot1p *dot1p-value*	Specifies the 802.1p priority of tunnel packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry user priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). Tunnel packets carry 802.1p priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). When data packets are sent from APs to the AC, 802.11 packets need to be converted to tunnel packets.

You can run the **priority-map tunnel-upstream dot11e dot1p** command to configure mapping from user priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, map user priority 6 of 802.11 packets to 802.1p priority 1 of tunnel packets when data is sent from APs to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dot11e 6 dot1p 1
```

11.7.21 priority-map tunnel-upstream dscp dot1p

Function

The **priority-map tunnel-upstream dscp dot1p** command configures mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dscp dot1p** command restores the default mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

Table 11-174 describes the default mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets.

NOTE

The CAPWAP header refers to the tunnel header.

Table 11-174 Default mapping from DSCP priorities of 802.11 packets to 802.1p priorities of in CAPWAP headers

DSCP Priority of 802.11 Packets	802.1p Priority in the CAPWAP Header
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map tunnel-upstream dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot1p** *dot1p-value*

undo priority-map tunnel-upstream dscp to dot1p

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. *dscp-value2* must be greater than *dscp-value1*.
dot1p *dot1p-value*	Specifies the 802.1p priority of tunnel packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry user priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). Tunnel packets carry 802.1p priorities (Layer 2 priorities) or DSCP priorities (Layer 3 priorities). When data packets are sent from APs to the AC, 802.11 packets need to be converted to tunnel packets.

You can run the **priority-map tunnel-upstream dscp dot1p** command to configure mapping from DSCP priorities of 802.11 packets to 802.1p priorities of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, map DSCP priorities 0 to 7 of 802.11 packets to 802.1p priority 1 of tunnel packets when data is sent from APs to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dscp 0 to 7 dot1p 1
```

11.7.22 priority-map tunnel-upstream dscp tunnel-dscp

Function

The **priority-map tunnel-upstream dscp tunnel-dscp** command configures mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream dscp tunnel-dscp** command restores the default mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

By default, DSCP priority **1** of 802.11 packets maps DSCP priority **1** of tunnel packets, DSCP priority **2** of 802.11 packets maps DSCP priority **2** of tunnel packets, and so on. DSCP priority **63** of 802.11 packets maps DSCP priority **63** of tunnel packets.

Format

priority-map tunnel-upstream dscp { *dscp-value* [**to** *dscp-value1*] } &<1-10> **tunnel-dscp** *dscp-value2*

undo priority-map tunnel-upstream dscp to tunnel-dscp

Parameters

Parameter	Description	Value
dscp *dscp-value*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Parameter	Description	Value
to *dscp-value1*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. *dscp-value1* must be greater than *dscp-value*.
tunnel-dscp *dscp-value2*	Specifies the DSCP priority of tunnel packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry the user priority (Layer 2) or DSCP priority (Layer 3), and tunnel packets carry the 802.1p priority (Layer 2) or tunnel DSCP priority (Layer 3). 802.11 packets sent to the AC from an AP must be converted into tunnel packets.

You can run the **priority-map tunnel-upstream dscp tunnel-dscp** command to configure mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, configure mapping from DSCP priority 6 of 802.11 packets to DSCP priority 1 of tunnel packets when packets are sent to the AC from an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream dscp 6 tunnel-dscp 1
```

11.7.23 priority-map tunnel-upstream trust

Function

The **priority-map tunnel-upstream trust** command configures a trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

The **undo priority-map tunnel-upstream trust** command restores the default trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

By default, the 802.11e priority is used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

Format

priority-map tunnel-upstream trust { **dot11e** | **dscp** }

undo priority-map tunnel-upstream trust

Parameters

Parameter	Description	Value
dot11e	Specifies the 802.11e priority as the trusted priority type used in mapping from 802.11 packets to tunnel packets.	-
dscp	Specifies the DSCP priority as the trusted priority type used in mapping from 802.11 packets to tunnel packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

802.11 packets sent from a WMM-capable STA carry the user priority (Layer 2) or DSCP priority (Layer 3), and tunnel packets carry the 802.1p priority (Layer 2) or tunnel DSCP priority (Layer 3). 802.11 packets sent to the AC from an AP must be converted into tunnel packets.

You can run the **priority-map tunnel-upstream trust** command to configure a trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

Precautions

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

In traffic profile **p1**, configure the DSCP priority as the trusted priority type used in mapping from 802.11 packets to tunnel packets when packets are sent to the AC from an AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map tunnel-upstream trust dscp
```

11.7.24 priority-map upstream trust

Function

The **priority-map upstream trust** command configures the priority mapping mode from 802.11 packets to 802.3 packets when packets are sent from an AP to upper-layer devices.

The **undo priority-map upstream trust** command restores the default priority mapping mode from 802.11 packets to 802.3 packets when packets are sent from an AP to upper-layer devices.

By default, the 802.11e priority is mapped from 802.11 packets to 802.3 packets when packets are sent from an AP to upper-layer devices.

Format

priority-map upstream trust { **dot11e** | **dscp** }

undo priority-map upstream trust

Parameters

Parameter	Description	Value
dot11e	Specifies the mapping from the user priority of 802.11 packets to the DSCP and 802.1p priorities of 802.3 packets.	-
dscp	Specifies the DSCP priority mapping from 802.11 packets to 802.3 packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 data packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and IP packets transmitted on an Ethernet carry the DSCP priority (also called the ToS field). When data packets are forwarded from an AP to an AC or the upper-layer network, 802.3 packets need to be converted into 802.11 packets. During the conversion, the user priority of 802.11 packets is mapped to the ToS field in the IP packet header.

Currently, the priority mappings are fixed and described in the following table.

Table 11-175 Mapping between the DSCP and 802.1p priorities

DSCP Priority of 802.11 Packets	802.1p Priority of 802.3 Packets
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Table 11-176 Mapping from the user priority to the 802.1p and DSCP priorities

User Priority of 802.11 Packets	DSCP Priority of 802.3 Packets	802.1p Priority of 802.3 Packets
0	0	0
1	8	1
2	16	2
3	24	3
4	32	4

User Priority of 802.11 Packets	DSCP Priority of 802.3 Packets	802.1p Priority of 802.3 Packets
5	40	5
6	48	6
7	56	7

Example

Configure the DSCP priority mapping from 802.11 packets to 802.3 packets in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] priority-map upstream trust dscp
```

11.7.25 qos car (SSID profile view)

Function

The **qos car** command configures QoS CAR parameters.

The **undo qos car** command deletes the configured QoS CAR parameters.

By default, no QoS CAR parameters are configured in an SSID profile.

Format

qos car inbound cir *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

undo qos car inbound

Parameters

Parameter	Description	Value
inbound	Applies a QoS CAR profile to the inbound direction of an interface.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR value must be greater than or equal to the CIR value.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default: ● If the PIR value is not set, the CBS value is 188 times the CIR value. If the value 188 times the CIR exceeds the maximum value (4294967295) of the CBS, 4294967295 is used. ● If the PIR is set, the CBS is 125 times the CIR. If the value 125 times the CIR exceeds the maximum value (4294967295) of the CBS, 4294967295 is used.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default, if the PIR is set, the PBS is 125 times the PIR. If the value 125 times the PIR exceeds the maximum value (4294967295) of the PBS, 4294967295 is used.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing discards excess traffic to limit incoming and outgoing traffic within a proper range and to protect network resources.

When traffic is transmitted from a high-speed link to a low-speed link, the inbound interface of the low-speed link is prone to severe data loss. The data traffic rate needs to be limited. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate, limiting the outgoing traffic rate in a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

The packet color is determined by parameters **cbs** *cbs-value* and **pbs** *pbs-value* of this command.

- When the size of a packet is less than the CBS value, the packet is colored green.
- When the size of a packet is greater than or equal to the CBS value but less than the PBS value, the packet is colored yellow.
- When the size of a packet is greater than or equal to the PBS value, the packet is colored red.

QoS CAR parameters can be configured in an SSID profile to implement traffic policing on user traffic on all VAPs to which the user profile is applied. These VAPs share a token bucket, and more VAPs indicate fewer network resources that each VAP can occupy.

Precautions

QoS CAR parameters configured in an SSID profile are valid only when the service data forwarding mode is set to tunnel forwarding. In tunnel forwarding mode, this function does not take effect when Layer 2 STAs associated with the same AP communicate with each other.

When the traffic policing rate is greater than the maximum rate of an interface, traffic policing does not take effect on the interface. Set the value of *cir-value* smaller than the rate of the interface.

When the CBS value is smaller than the number of bytes in a packet, packets of this type are discarded.

To ensure that the device correctly identifies packet colors, you are advised to set the PBS value greater than the CBS value.

When a user is configured as a VIP user, the QoS CAR configured in the SSID profile does not take effect.

Example

Configure traffic policing parameters for incoming packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] qos car inbound cir 64 cbs 9000 pbs 18000
```

11.7.26 rate-limit

Function

The **rate-limit** command configures the rate limit for upstream and downstream packets of all STAs or each STA on a VAP.

The **undo rate-limit** command restores the default rate limit for upstream and downstream packets of all STAs or each STA on a VAP.

By default, the rate limit for upstream and downstream packets of all STAs on a VAP is 4294967295 kbit/s, and that of each STA is 4294967295 kbit/s.

Format

rate-limit { **client** | **vap** } { **up** | **down** } *rate-value*

undo rate-limit { **client** | **vap** } { **up** | **down** }

Parameters

Parameter	Description	Value
client	Specifies a STA on a VAP.	-
vap	Specifies all STAs on a VAP.	-
up	Specifies the rate limit for upstream packets on a VAP.	-
down	Specifies the rate limit for downstream packets on a VAP.	-
rate-value	Specifies the rate limit of packets.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The value **4294967295** indicates that the rate is not limited.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit** command to limit the rate of upstream and downstream packets for all STAs or each STA on a VAP to protect network bandwidth resources.

Precautions

The limited rate does not take effect for STAs that go online before the **rate-limit** command is configured. To make this configuration take effect for a STA, enable the STA to go online again.

The rate limit configured for each STA on a VAP does not take effect for multicast packets.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

Example

Set the rate limit of upstream packets to 4294967295 kbit/s for all STAs on a VAP in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] rate-limit vap up 4294967295
```

11.7.27 rate-limit client dynamic

Function

The **rate-limit client dynamic** command sets the dynamic rate limit threshold for a single STA in a VAP.

The **undo rate-limit client dynamic** command restores the default dynamic rate limit threshold for a single STA in a VAP.

By default, the dynamic rate limit threshold for a single STA in a VAP is 16 Mbit/s.

NOTE

Dynamic rate limiting for STAs is not supported by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs
- AirEngine X762 series APs
- AirEngine X771 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

rate-limit client dynamic *rate-value*

undo rate-limit client dynamic

Parameters

Parameter	Description	Value
rate-value	Specifies the rate limit of packets.	The value is an enumerated value, which can be 8, 16, or 32, in Mbit/s. The default value is 16 Mbit/s.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA downloads or uploads large files on the live network, network access of other STAs may be affected.

After dynamic rate limiting is enabled, the device determines whether to perform three-phase rate limiting for wireless users depending on whether the air interface is congested. This improves network experience of wireless users.

Precautions

If static rate limiting has been enabled, static rate limiting takes precedence over dynamic rate limiting.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

Example

Set the dynamic rate limit threshold for a single STA in a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] undo rate-limit client dynamic disable
[HUAWEI-wlan-traffic-prof-p1] rate-limit client dynamic 32
```

11.7.28 rate-limit client dynamic disable

Function

The **rate-limit client dynamic disable** command disables dynamic rate limiting for a single STA in a VAP.

The **undo rate-limit client dynamic disable** command enables dynamic rate limiting for a single STA in a VAP.

By default, dynamic rate limiting is enabled for a single STA in a VAP.

NOTE

Dynamic rate limiting for STAs is not supported by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs
- AirEngine X762 series APs
- AirEngine X771 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

rate-limit client dynamic disable

undo rate-limit client dynamic disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA downloads or uploads large files on the live network, network access of other STAs may be affected.

After dynamic rate limiting is enabled, the device determines whether to perform three-phase rate limiting for wireless users depending on whether the air interface is congested. This improves network experience of wireless users.

Precautions

If static rate limiting has been enabled, static rate limiting takes precedence over dynamic rate limiting.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

Example

Enable dynamic rate limiting for a single STA in a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] undo rate-limit client dynamic disable
```

11.7.29 rate-limit client time-range

Function

The **rate-limit client time-range** command sets a rate limit for upstream or downstream packets of each STA on a VAP in a specified time range.

The **undo rate-limit client time-range** command restores the default rate limit of upstream or downstream packets of each STA on a VAP in a specified time range.

By default, no rate limit is set for upstream or downstream packets of each STA on a VAP in a specified time range.

Format

rate-limit client { **up** | **down** } *rate-value* **time-range** *time-range-name*

undo rate-limit client { **up** | **down** } **time-range** *time-range-name*

Parameters

Parameter	Description	Value
client	Specifies each STA on a VAP.	-
up	Specifies the rate limit for upstream packets of each STA on a VAP.	-
down	Specifies the rate limit for downstream packets of each STA on a VAP.	-

Parameter	Description	Value
rate-value	Specifies the rate limit of packets.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The value **4294967295** indicates that the packet rate is not limited.
time-range-name	Specifies the name of a time range during which the rate of packets is limited.	The value is a string of 1 to 32 characters and must begin with a letter. To avoid confusion, do not use **all** as the name of a time range.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit client time-range** command to set a rate limit for upstream or downstream packets of each STA on a VAP in a specified time range.

Precautions

The limited rate does not take effect for STAs that go online before the **rate-limit** command is configured. To make this configuration take effect for a STA, enable the STA to go online again.

The rate limit configured for each STA on a VAP does not take effect for multicast packets.

When the NP fast forwarding function is disabled, neither the **rate-limit vap** nor **rate-limit client** command configuration takes effect for VIP users. When the NP fast forwarding function is enabled, the **rate-limit vap** command configuration takes effect for VIP users, but the **rate-limit client** command configuration does not take effect for VIP users.

A maximum of eight time range–based rate limiting policies can be configured in the same direction (upstream or downstream). By default, the device has a default policy (determined by the **rate-limit client** { **up** | **down** } *rate-value* command configuration). A configured time range–based rate limiting policy takes precedence over the default policy. If multiple time range–based rate limiting policies are configured, the minimum rate limit value takes effect.

You need to run the **time-range** command in the system view to configure a time range.

Example

Set the rate limit for upstream packets of each STA on a VAP to 1000 kbit/s in the time range named **time**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] rate-limit client up 1000 time-range time
Warning: The specified time-range does not exist. You can create it later. Continue?[Y/N]y
```

11.7.30 rate-limit dynamic interval

Function

The **rate-limit dynamic interval** command sets the detection interval and threshold for dynamic rate limiting of a single STA on a VAP.

The **undo rate-limit dynamic** command restores the default detection interval and threshold for dynamic rate limiting of a single STA on a VAP.

The default detection interval and threshold for dynamic rate limiting of a single STA on a VAP are 5 and 80%, respectively.

Format

rate-limit dynamic interval *interval* **threshold** *threshold*

undo rate-limit dynamic

Parameters

Parameter	Description	Value
interval	Specifies the detection interval for dynamic rate limiting.	The value is an integer that ranges from 1 to 30.
threshold *threshold*	Specifies the detection threshold for dynamic rate limiting.	The value is an integer that ranges from 1 to 100.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to adjust the time when dynamic rate limiting takes effect.

If the channel utilization is higher than *threshold*% for a consecutive number of times specified by *interval* (that is, a period of time specified by *interval* x 2 seconds), the air interface congestion is determined.

Example

Configure the detection interval and threshold for dynamic rate limiting of a single STA on a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] rate-limit dynamic interval interval 10 threshold 60
```

11.7.31 svp-voice enable

Function

The **svp-voice enable** command enables the Spectralink Voice Priority (SVP) voice traffic optimization function.

The **undo svp-voice enable** command disables the SVP voice traffic optimization function.

By default, the SVP voice traffic optimization function is disabled.

Format

svp-voice enable

undo svp-voice enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

SpectraLink Voice is a voice protocol defined by Spectralink (a Wi-Fi phone company). To ensure SpectraLink voice transmission quality on WLANs, SpectraLink defines SpectraLink Voice Priority (SVP) to describe the requirements of SpectraLink Voice on WLANs.

On a WLAN with STAs supporting the SpectraLink Voice protocol, you are advised to enable the SVP voice traffic optimization function.

Example

Enable the SVP voice traffic optimization function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] svp-voice enable
```

11.7.32 service-experience-analysis enable

Function

The **service-experience-analysis enable** command enables the service experience analysis (SEA) function.

The **undo service-experience-analysis enable** command disables the service experience analysis (SEA) function.

By default, the SEA function is disabled.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis enable

undo service-experience-analysis enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the SIP (eSpace) service runs on a WLAN, you can enable the SEA function so that the device reports performance statistics about SIP traffic (such as IP addresses and port numbers of calling and called parties, and call quality data) to iMaster NCE-CampusInsight. In this manner, iMaster NCE-CampusInsight can analyze network performance and locate faults.

Follow-up Procedure

Run the **service-experience-analysis sip-snooping port** command to set the port number for identifying SIP packets.

Example

Enable the SEA function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name example
[HUAWEI-wlan-vap-prof-example] service-experience-analysis enable
```

11.7.33 service-experience-analysis monitor interval

Function

The **service-experience-analysis monitor interval** command configures the sampling interval for SEA-based application monitoring.

The **undo service-experience-analysis monitor interval** command restores the default sampling interval for SEA-based application monitoring.

By default, the sampling interval for SEA-based application monitoring is 10 seconds.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis monitor interval *interval*

undo service-experience-analysis monitor interval

Parameters

Parameter	Description	Value
interval	Specifies the sampling interval for SEA-based application monitoring.	The value is an integer that ranges from 2 to 30, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the sampling interval for SEA-based application monitoring.

Example

Set the sampling interval for SEA-based application monitoring to 2 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys
[HUAWEI-wlan-ap-system-prof-apsys] service-experience-analysis monitor interval 2
```

11.7.34 service-experience-analysis monitor application

Function

The **service-experience-analysis monitor application** command configures an application to be monitored based on SEA.

The **undo service-experience-analysis monitor application** command deletes an application monitored based on SEA.

By default, no application is monitored based on SEA.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis monitor application *appname*

undo service-experience-analysis monitor application *appname*

Parameters

Parameter	Description	Value
appname	Specifies an application to be monitored based on SEA.	Currently, applications that use the TCP and RTP protocols can be monitored based on SEA. RTP-based applications include: ● skype_voip ● sip ● rtp ● whatsapp ● espace_voip ● hangouts ● slack_voip ● welink_videocall ● microsoftteams ● webex_voip ● xiaoyuyilian ● huaweimeeting

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure application-based traffic quality monitoring. After the configuration is complete, the AC delivers the configuration to APs that will monitor the specified application.

Prerequisites

The security engine has been enabled using the **defence engine enable** command.

Precautions

You can configure a maximum of 16 applications to be monitored based on SEA.

For some voice and video applications, if the application control packets use TCP and the data packets use UDP, the device can monitor only the quality of application control packets (TCP).

Among user-defined applications (created using the **user-defined-application** command), SEA can monitor only user-defined TCP applications (specified by the **protocol tcp** parameter) but not user-defined UDP applications (specified by the **protocol udp** parameter).

SEA does not monitor fragmented packets.

Example

Configure an application to be monitored based on SEA.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] service-experience-analysis monitor application WeLink
```

11.7.35 service-experience-analysis monitor ucl-group

Function

The **service-experience-analysis monitor ucl-group** command specifies a UCL group or a "UCL group + application" combination monitored based on SEA.

The **undo service-experience-analysis monitor ucl-group** command deletes a UCL group or a "UCL group + application" combination monitored based on SEA.

By default, no UCL group is monitored based on SEA.

NOTE

This command is not supported by the following models:

- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis monitor ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* & <1-16>]

undo service-experience-analysis monitor ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* &<1-16>]

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer that ranges from 1 to 64000.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.

Parameter	Description	Value
application *application-name*	Specifies an application to be monitored based on SEA.	The application must exist. A maximum of 16 applications can be specified.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify a UCL group or a "UCL group + application" combination to be monitored based on SEA.

You can specify a UCL group so that the device can monitor the quality of applications of users in the specified UCL group. You can also specify a "UCL group + application" combination, so that the device can monitor the quality of the specified application of users in the specified UCL group.

Precautions

A maximum of 128 applications, UCL groups, and "UCL group + application" combinations (including 16 applications at most) can be monitored based on SEA.

Example

Specify the application **WeLink** in the UCL group **test** to be monitored based on SEA.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] service-experience-analysis monitor ucl-group test application
WeLink
```

11.7.36 service-experience-analysis sip-snooping port

Function

The **service-experience-analysis sip-snooping port** command sets the port number for identifying SIP packets.

The **undo service-experience-analysis sip-snooping port** command restores the default port number for identifying SIP packets.

The default port number for identifying SIP packets is 5060.

NOTE

This command is not supported by the following models:
- AirEngine series central APs
- AirEngine 5761-10W, AirEngine 5761-10WD, and AirEngine 5761S-10W
- AirEngine X762 series APs

Format

service-experience-analysis sip-snooping port *port-number*

undo service-experience-analysis sip-snooping port

Parameters

Parameter	Description	Value
port-number	Specifies the port number for identifying SIP packets.	The value is an integer that ranges from 1 to 65535.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

When the SIP (eSpace) service runs on a WLAN, you can enable the SEA function so that the device reports performance statistics about SIP traffic (such as IP addresses and port numbers of calling and called parties, and call quality data) to iMaster NCE-CampusInsight. In this manner, iMaster NCE-CampusInsight can analyze network performance and locate faults.

You can run this command to configure the port number for identifying SIP packets.

Before specifying the port number for identifying SIP packets, enable the SEA function using the **service-experience-analysis enable** command.

Example

Set the port number for identifying SIP packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name example
[HUAWEI-wlan-vap-prof-example] service-experience-analysis sip-snooping port 5080
```

11.7.37 traffic-filter (traffic profile view)

Function

The **traffic-filter** command configures ACL-based packet filtering in a traffic profile.

The **undo traffic-filter** command cancels the configuration of ACL-based packet filtering in a traffic profile.

By default, ACL-based packet filtering is not configured in a traffic profile.

Format

traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction.	-
outbound	Configures ACL-based packet filtering in the outbound direction.	-
ipv4	Configures ACL-based IPv4 packet filtering.	-
ipv6	Configures ACL-based IPv6 packet filtering.	-
l2	Configures ACL-based Layer 2 packet filtering.	-

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 and from 6000 to 6031 for an IPv4 ACL, from 3000 to 3031 and 6000 to 6031 for an IPv6 ACL, and from 4000 to 4031 for a Layer 2 ACL. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs ● 4000 to 4031: Layer 2 ACLs
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value is a string of 1 to 65 case-sensitive characters without spaces and must begin with a letter. The value range of *acl-number* corresponding to *acl-name* is 3000 to 3031, and 6000 to 6031.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a wireless network, administrators want to provide differentiated services for wireless users. The services may include, but are not limited to the following:

- Deny or permit access of specified wireless users to specified LAN devices.
- Deny access of specified wireless users to specified invalid IP addresses.

You can configure ACL-based packet filtering in a traffic profile for providing differentiated services to wireless users based on ACL rules.

When the **traffic-filter** command is configured in the traffic profile view, the device first matches packets against ACLs and then performs the action according to the matched policy.

When multiple **traffic-filter** commands are configured for ACL-based packet filtering in the same direction in the same traffic profile, packets are matched against the next rule in the sequence in which the commands are configured. If packets match a rule, the device executes the specified policy and stops the matching process. Otherwise, the device continues to match packets against the next rule. If no rule is matched, the packets are allowed to pass through.

If an ACL contains multiple rules, packets match against the rules in the ascending order of rule IDs. If packets match a rule, the device considers that the ACL is matched and stops the matching process. Otherwise, the device continues to match packets against the next rule. If no rule is matched, the device considers that this ACL is not matched. To improve match efficiency, you are advised to configure an ACL rule with a high match probability first and set a small ID for the rule. This will reduce the number of times ACL rules are matched and save resources.

Prerequisites

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl name**

The device has been enabled to process STA IPv6 services of STAs using the **sta-ipv6-service enable** command.

Precautions

The **traffic-filter** command can reference a numbered ACL rule that is not configured. You can configure the referenced ACL rule after running this command.

You can only configure a maximum of eight ACL rules in the same direction. The sequence in which ACL rules takes effect follows the sequence in which the rules are configured. To change the current packet filtering rules, delete all the related configurations and reconfigure the ACL-based packet filtering.

Example

Create the traffic profile **p1** and configure packet filtering in the inbound direction based on the ACL that permits packets with the source IPv4 address 192.168.0.2/32.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-filter inbound ipv4 acl 3000
```

11.7.38 traffic-profile (WLAN view)

Function

The **traffic-profile** command creates a traffic profile and displays the traffic profile view, or displays the view of an existing traffic profile.

The **undo traffic-profile** command deletes a traffic profile.

By default, the system provides the traffic profile **default**.

Format

traffic-profile name *profile-name*

undo traffic-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a traffic profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all traffic profiles.	–

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

- The **traffic-profile** command applies to the following situations:
  - To apply priority mapping and traffic suppression functions to a VAP, create a traffic profile and bind the traffic profile to the VAP profile.
  - To change priority mapping and traffic suppression functions of a VAP, enter the traffic profile view of the VAP to modify the required parameters. When a traffic profile is not required, delete it.
- After a traffic profile is created, parameters in the profile use default values.

NOTE

- The profile name is mandatory when you create a profile.
- The traffic profile referenced by a VAP profile cannot be deleted. To delete the traffic profile, unbind it from the VAP profile first.

Example

Create traffic profile **p1** and display the traffic profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1]
```

11.7.39 traffic-profile (VAP profile view)

Function

The **traffic-profile** command binds a traffic profile to a VAP profile.

The **undo traffic-profile** command unbinds a traffic profile from a VAP profile.

By default, the traffic profile **default** is bound to a VAP profile.

Format

traffic-profile *profile-name*

undo traffic-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic profile.	The traffic profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **traffic-profile** command to bind a traffic profile to a VAP profile. The traffic profile applies to all users using the VAP profile.

Prerequisites

The traffic profile has been created using the **traffic-profile (WLAN view)** command.

Example

Create VAP profile **p1** and bind traffic profile **u1** to the VAP profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name p1
[HUAWEI-wlan-vap-prof-p1] traffic-profile u1
```

11.7.40 traffic-remark (traffic profile view)

Function

The **traffic-remark** command configures ACL-based priority re-marking in a traffic profile.

The **undo traffic-remark** command cancels ACL-based priority re-marking in a traffic profile.

By default, ACL-based priority re-marking is not configured in a traffic profile.

Format

traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* } { **dot11e** *dot11e-value* | **dscp** *dscp-value* }

traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* } { **dot11e** *dot11e-value* | **dscp** *dscp-value* }

undo traffic-remark { **inbound** | **outbound** } { **ipv4** | **ipv6** | **l2** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-remark { **inbound** | **outbound** } **ipv4 acl** { *acl-number* | **name** *acl-name* } **l2 acl** { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based priority re-marking in the inbound direction.	-
outbound	Configures ACL-based priority re-marking in the outbound direction.	-
ipv4	Configures priority re-marking for IPv4 packets.	-
ipv6	Configures priority re-marking for IPv6 packets.	-
l2	Configures priority re-marking for Layer 2 packets.	-

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3031 and from 6000 to 6031 for IPv4 ACLs, from 3000 to 3031 and 6000 to 6031 for an IPv6 ACLs, and from 4000 to 4031 for Layer 2 ACLs. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs ● 4000 to 4031: Layer 2 ACLs
name *acl-name*	Re-marks packet priorities based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces and must begin with a letter. The value range of *acl-number* corresponding to *acl-name* is 3000 to 3031, and 6000 to 6031.
dot11e *dot11e-value*	Re-marks the 802.11e priority of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-value*	Re-marks the DSCP priorities of packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user wants to re-mark packet priorities based on ACLs to provide differentiated services. The **traffic-remark** command can be used to configure ACL-based priority re-marking.

Prerequisites

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl name**

The device has been enabled to process IPv6 services of STAs using the **sta-ipv6-service enable** command.

Precautions

The **traffic-remark** command can reference a numbered ACL rule that is not configured. You can configure the referenced ACL rule after running this command.

You can only configure a maximum of eight ACL-based packet re-marking rules in the same direction. The sequence in which ACL rules takes effect follows the rule configuration sequence. To change the current packet re-marking rules, delete all the related configurations and reconfigure the ACL-based packet re-marking.

When the **traffic-remark** command and the **traffic-filter (traffic profile view)** command are used simultaneously and the same ACL rule is associated:

- If the **deny** action is configured in the ACL rule, the **traffic-remark** command does not take effect.
- If the **permit** action is configured in the ACL rule, the command that is executed first takes effect.

Example

Create the traffic profile **p1** and configure ACL-based 802.11e priority re-marking for IPv4 packets in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-remark inbound ipv4 acl 3000 dot11e 7
```

11.7.41 ucc-profile (system view)

Function

The **ucc-profile** command creates a UCC profile and displays the UCC profile view, or displays the view of an existing UCC profile.

The **undo ucc-profile** command deletes a UCC profile.

By default, no UCC profile is created.

Format

ucc-profile name *profile-name*

undo ucc-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a UCC profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. The string must start with a letter.
all	Indicates all UCC profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. To ensure QoS guarantee for Lync packets and improve user experience, set the priority of Lync packets in the UCC profile.

Follow-up Procedure

Configure priorities of Lync voice, video, desktop sharing, and file transfer packets in the UCC profile and bind the UCC profile to a VAP profile.

Precautions

The UCC profile that has been bound to a VAP profile cannot be deleted. To delete the UCC profile, unbind the UCC profile from the VAP profile.

Example

Create a UCC profile named **test** and enter the UCC profile view.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test]
```

11.7.42 ucc-profile (VAP profile view)

Function

The **ucc-profile** command binds a UCC profile to a VAP profile.

The **undo ucc-profile** command unbinds a UCC profile from a VAP profile.

By default, no UCC profile is bound to a VAP profile.

Format

ucc-profile *profile-name*

undo ucc-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a UCC profile.	The UCC profile name must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

After a UCC profile is created, run the **ucc-profile** command to bind the UCC profile to a VAP profile so that the actions in the UCC profile take effect.

Example

Create a UCC profile named **test** and bind the UCC profile to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] ucc-profile test
```

11.7.43 user-isolate (traffic profile view)

Function

The **user-isolate** command enables user isolation.

The **undo user-isolate** command disables user isolation.

By default, user isolation is disabled in a traffic profile.

Format

user-isolate l2

undo user-isolate

Parameters

Parameter	Description	Value
l2	Indicates user isolation at Layer 2 and communication at Layer 3.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a traffic profile, user isolation prevents packets of users on a VAP from being forwarded to each other. That is, users on the same VAP cannot communicate with each other after user isolation is enabled. This improves user communication security and enables the gateway to centrally forward user traffic, facilitating user management.

- In tunnel forwarding mode, user isolation in the traffic profile implements Layer 2 isolation for all users on a VAP.
- In direct forwarding mode, when enabling user isolation in the traffic profile, it is recommended that port isolation be deployed on the access switch port connected to the AP.

Example

Configure Layer 2 isolation and Layer 3 communication in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] user-isolate l2
Warning: Enabling user isolation may interrupt services. Are you sure you want to continue? [Y/N]:y
```

11.7.44 video remark

Function

The **video remark** command sets a priority for Lync video packets.

The **undo video remark** command deletes the priority of Lync video packets.

By default, the priority of Lync video packets is not set.

Format

video remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo video remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: ● af1: 1 ● af2: 2 ● af3: 3 ● af4: 4 ● be: 0 ● cs6: 6 ● cs7: 7 ● ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **video remark** command to change the priority of Lync video packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync video packets of one Lync session.

If you run the **video remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync video packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync video packets to 1 in the UCC profile **test**.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] video remark dscp 1
```

11.7.45 voice remark

Function

The **voice remark** command sets a priority for Lync voice packets.

The **undo voice remark** command deletes the priority of Lync voice packets.

By default, the priority of Lync voice packets is not set.

Format

voice remark { **8021p** *8021p-value* | **dscp** { *dscp-value* | *dscp-name* } | **local-precedence** { *local-precedence-value* | *local-precedence-name* } }

undo voice remark { **8021p** | **dscp** | **local-precedence** }

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
dscp { *dscp-value* | *dscp-name* }	Specifies the DSCP priority.	The value is a Diff-Serv code that is an integer ranging from 0 to 63, or a DSCP service type that can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values of service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46

Parameter	Description	Value
local-precedence { *local-precedence-value* | *local-precedence-name* }	Specifies the local priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. Or, the value is a service type that can be af1, af2, af3, af4, be, cs6, cs7, or ef. The values of service types are as follows: ● af1: 1 ● af2: 2 ● af3: 3 ● af4: 4 ● be: 0 ● cs6: 6 ● cs7: 7 ● ef: 5

Views

UCC profile view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

Microsoft Lync is a set of communication software that provides voice, video, desktop sharing, and file transfer functions. You can run the **voice remark** command to change the priority of Lync voice packets.

Precautions

The 802.1p priority and local priority cannot be set for the Lync voice packets of one Lync session.

If you run the **voice remark** command in the same UCC profile view multiple times to set the 802.1p priority, DSCP priority, or local priority of Lync voice packets, only the latest configuration takes effect.

Example

Set the DSCP priority of Lync voice packets to 1 in the UCC profile **test**.

```
<HUAWEI> system-view
[HUAWEI] ucc-profile name test
[HUAWEI-ucc-prof-test] voice remark dscp 1
```

11.7.46 wlan-slice high-reliability enable

Function

The **wlan-slice high-reliability enable** command enables WLAN high-reliability slicing.

The **undo wlan-slice high-reliability enable** command disables WLAN high-reliability slicing.

By default, the WLAN high-reliability slicing function is disabled.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability enable

undo wlan-slice high-reliability enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In industrial and healthcare scenarios, some latency-sensitive services exist. In this case, you can run the **wlan-slice high-reliability enable** command to enable the WLAN high-reliability slicing function. After this function is enabled, the AP allocates a period of time in the time domain to latency-sensitive services based on the air interface slicing configuration (expected RTT and slicing time proportion) to meet latency requirements of these services.

Precautions

- To ensure optimal air interface slicing, ensure that channel design, device selection, capacity planning, and position design comply with network planning and design requirements.

- In WLAN high-reliability slicing scenarios, if channels are manually planned, ensure that neighboring APs of any AP in the same frequency domain are invisible to each other, that is, no co-channel interference exists between the APs. For example, there are three APs in the same frequency domain: AP1 (neighbor of AP2), AP2 (neighbor of AP1 and AP3), and AP3 (neighbor of AP2). In this case, ensure that no co-channel interference exists between AP1 and AP3.
- When the WLAN high-reliability slicing function is enabled, terminal services may be interrupted.
- The WLAN high-reliability slicing function is mutually exclusive with the air scan function. After the WLAN high-reliability slicing function is enabled, AP radios do not support air scan, and scanning-dependent services, such as smart roaming, band steering, and load balancing, are unavailable.
- If the WLAN high-reliability slicing function is enabled on an AP, port isolation cannot be configured on the switch port connected to the AP.
- WLAN high-reliability slicing and interference visualization are not supported in Mesh scenarios.
- After WLAN high-reliability slicing is enabled in an RRM profile, the profile can be bound only to a 5 GHz radio profile. Each 5 GHz radio bound to this 5 GHz radio profile supports **a maximum of two VAPs**. As WLAN high-reliability slicing uses the VAP with the WLAN ID of 15, do not configure the WLAN ID of 15 for a service VAP.
- After WLAN high-reliability slicing is enabled, CoSR, MU-MIMO, and OFDMA do not take effect on the 2.4 GHz and 5 GHz radios.
- If the WLAN high-reliability slicing function is enabled but there are no low-latency services, high-priority slices cannot be properly utilized. As a result, spectral efficiency and performance deteriorate.
- To allow terminals connected to a Wi-Fi CPE to quickly go online, ensure that multicast traffic is not suppressed during deployment. After the deployment is complete, to ensure the delay of terminals connected to the Wi-Fi CPE, configure multicast traffic suppression on the AC's uplink interface (connected to an application server) and set the rate limit to 8 pps.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1 /////Assume that GE0/0/1 is the AC's uplink interface.
[HUAWEI-GigabitEthernet0/0/1] multicast-suppression packets 8
```

- CPEs need to stay in stationary state to ensure that air interface slicing reaches the optimal state.
- Do not deliver instructions to Wi-Fi CPEs in batches when air interface slicing is enabled.

Example

Enable WLAN high-reliability slicing.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability enable
Warning: This operation will cause online STAs on the radio to go offline. Radios enabled with high-
reliability air interface slicing can provide access only to CPEs with slicing capabilities. It is recommended
that only one or two SSIDs be broadcast on a radio enabled with high-reliability air interface slicing.
Because WLAN ID 15 of the radio is used for air interface slicing, specify other WLAN IDs as required.
Continue? [Y/N] y
```

11.7.47 wlan-slice high-reliability frer-enhance

Function

The **wlan-slice high-reliability frer-enhance** command enables the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios.

The **undo wlan-slice high-reliability frer-enhance** command disables the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios.

By default, the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios is disabled.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability frer-enhance

undo wlan-slice high-reliability frer-enhance

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Table 11-177 describes the recommended application scenarios of the enhanced dual fed and selective receiving function for WLAN high-reliability slicing.

Table 11-177 Application scenarios of the enhanced dual fed and selective receiving function for WLAN high-reliability slicing

Scenario	Enhanced Dual Fed and Selective Receiving Function for WLAN High-Reliability Slicing
There are a large number of STAs, and 2.4 GHz radios are heavily loaded. Only the performance indicator of 99.999% @ 20 ms is required.	Disabled
There are a small number of STAs, and high performance requirements are imposed. The performance indicator of higher than 99.999% @ 20 ms is required.	Enabled

NOTE

To achieve 99.999% @ 20 ms, the system must ensure that the RTT of only 1 in 100,000 packets exceeds 20 ms.

Prerequisites

The WLAN high-reliability slicing function has been enabled.

Example

Enable the enhanced dual fed and selective receiving function for WLAN high-reliability slicing scenarios.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-view] wlan-slice high-reliability enable
Warning: This operation will cause online STAs on the radio to go offline. Radios enabled with high-
reliability air interface slicing can provide access only to CPEs with slicing capabilities. It is recommended
that only one or two SSIDs be broadcast on a radio enabled with high-reliability air interface slicing.
Because WLAN ID 15 of the radio is used for air interface slicing, specify other WLAN IDs as required.
Continue? [Y/N] y
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability frer-enhance
```

11.7.48 wlan-slice high-reliability rtt

Function

The **wlan-slice high-reliability rtt** command configures the expected round-trip time (RTT) of WLAN high-reliability slicing.

The **undo wlan-slice high-reliability rtt** command restores the default expected RTT of WLAN high-reliability slicing.

By default, the expected RTT of WLAN high-reliability slicing is 20 ms.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability rtt *rtt-value*

undo wlan-slice high-reliability rtt

Parameters

Parameter	Description	Value
rtt-value	Specifies the expected RTT value.	The value is an integer that ranges from 10 to 1000, in milliseconds.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is enabled, the AP allocates a period of time in the time domain to latency-sensitive services based on the air interface slicing configuration (expected RTT and slicing time proportion) to meet latency requirements of these services.

Example

Set the expected RTT of WLAN high-reliability slicing to 100 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability rtt 100
```

11.7.49 wlan-slice high-reliability time-ratio

Function

The **wlan-slice high-reliability time-ratio** command configures the time proportion for WLAN high-reliability slicing.

The **undo wlan-slice high-reliability time-ratio** command restores the default time proportion for WLAN high-reliability slicing.

The default time proportion for WLAN high-reliability slicing is 80%.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability time-ratio *time-ratio*

undo wlan-slice high-reliability time-ratio

Parameters

Parameter	Description	Value
time-ratio	Specifies the slicing time proportion.	The value is an integer that ranges from 0 to 80, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is enabled, the AP allocates a period of time in the time domain to latency-sensitive services based on the air interface slicing configuration (expected RTT and slicing time proportion) to meet latency requirements of these services.

Example

Set the time proportion for WLAN high-reliability slicing to 60%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rrm-profile name p1
[HUAWEI-wlan-rrm-prof-p1] wlan-slice high-reliability time-ratio 60
```

11.7.50 wlan-slice high-reliability acl

Function

The **wlan-slice high-reliability acl** command specifies an ACL for air interface slicing.

The **undo wlan-slice high-reliability acl** command deletes an ACL for air interface slicing.

By default, no ACL for air interface slicing is configured.

NOTE

Air interface slicing is supported only by the following models:

- AirEngine X760 series APs
- AirEngine 9700D-S (including matching ORUs)

Format

wlan-slice high-reliability { **ipv4** | **ipv6** | **l2** } **acl** *acl-number*

undo wlan-slice high-reliability { **ipv4** | **ipv6** | **l2** } **acl** *acl-number*

Parameters

Parameter	Description	Value
ipv4	Enables air interface slicing for IPv4 packets.	-
ipv6	Enables air interface slicing for IPv6 packets.	-
l2	Enables air interface slicing for Layer 2 packets.	-

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	For IPv4 and IPv6 ACLs, the value is an integer that ranges from 3000 to 3031 and 6000 to 6031 in the traffic profile. For Layer 2 ACLs, the value is an integer that ranges from 4000 to 4031. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs ● 4000 to 4031: Layer 2 ACLs

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement QoS for multiple low-latency services in a more refined manner, you can enable the air interface slicing function for specific traffic. You can specify an ACL to filter traffic so that air interface slicing takes effect only for traffic that matches the ACL.

Air interface slicing identifies service traffic using access control lists (ACLs).

- Common terminal: Run the **wlan-slice high-reliability acl** command in the traffic profile to configure an ACL for air interface slicing. The device performs robust scheduling on the service traffic that matches the ACL.

Precautions

An ACL rule has been created before this command is run.

- **acl (system view)**
- **acl ipv6 (system view)**
- **acl name**
- **acl ipv6 name**

Example

Specify an ACL for air interface slicing in a traffic profile.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
```

```
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] wlan-slice high-reliability ipv4 acl 3000
```

11.7.51 wmm edca-ap

Function

The **wmm edca-ap** command sets EDCA parameters and ACK policies for an AP.

The **undo wmm edca-ap** command restores the default EDCA parameters and ACK policies for an AP.

Table 11-178 lists the default EDCA parameter settings and ACK policies for APs.

Table 11-178 Default EDCA parameter settings and ACK policies for APs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

Format

wmm edca-ap { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *

undo wmm edca-ap

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.

Parameter	Description	Value
ecwmin *ecwmin-value*	Specifies the *ecwmin-value*. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be less than or equal to the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the *ecwmax-value*. *ecwmax-value* and *ecwmin-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than or equal to the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the TXOPLimit, which determines the maximum duration in which an AP or a STA can occupy a channel. A larger *txoplimit-value* value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the *txoplimit-value* value is 0, the STA can send only one data frame every time it occupies a channel.
ack-policy { **normal** | **noack** }	Specifies an ACK policy. ● **normal**: During 802.11 packet exchange, the receiver must return an ACK packet each time it receives a packet from the sender. ● **noack**: The receiver does not need to send an ACK message when it receives a packet from the sender. Configure this parameter only in the good air interface environment. Otherwise, severe packet loss occurs.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide different priorities for the packets. In this way, APs provide different capabilities to compete for channels, achieving differentiated services.

Precautions

- The EDCA parameters configured for the four AC queues take effect only after the WMM function is enabled. By default, the WMM function is enabled in a 2G or 5G radio profile.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.
- EDCA parameters must be configured properly. The scenarios for the reference EDCA parameter settings and ACK policies are as follows:
  a. Table 11-179 lists the reference EDCA parameter settings and ACK policies for APs in voice scenarios.

Table 11-179 Reference EDCA parameter settings and ACK policies in voice scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	5	0	normal
AC_BK	10	8	12	0	normal

  b. Table 11-180 lists the reference EDCA parameter settings and ACK policies for APs in voice and video scenarios.

Table 11-180 Reference EDCA parameter settings and ACK policies in voice and video scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	12	0	normal
AC_BK	10	8	12	0	normal

c. In high-density scenarios, it is recommended that you run the **dynamic-edca enable** command to enable dynamic EDCA parameter adjustment.

d. For other scenarios, the default settings are recommended.

Example

Set EDCA parameters and ACK policies for AC_VO packets in 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] wmm edca-ap ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit
0 ack-policy normal
```

11.7.52 wmm edca-client (SSID profile view)

Function

The **wmm edca-client** command configures EDCA parameters for STAs.

The **undo wmm edca-client** command restores the default EDCA parameter settings of STAs.

Table 11-181 lists the default EDCA parameter settings for STAs.

Table 11-181 Default EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit
AC_VO	3	2	2	47
AC_VI	4	3	2	94
AC_BE	10	4	3	0
AC_BK	10	4	7	0

Format

wmm edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo wmm edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-

Parameter	Description	Value
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 12 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be less than or equal to the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than or equal to the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue.

These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide differentiated priorities to the packets and different capabilities to compete for channels. In this way, differentiated services are implemented.

Table 11-182 describes the EDCA parameters.

Table 11-182 EDCA parameter description

Parameter	Meaning
Arbitration Interframe Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. Together, they determine the average backoff time. Large ECWmin and ECWmax values mean a long average backoff time for the STA and a low STA priority.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can only send one data frame every time it preempts a channel.

Precautions

- The EDCA parameters configured for the four AC queues take effect only after the WMM function is enabled using the **undo wmm disable** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.
- EDCA parameters must be configured properly. The scenarios for the reference EDCA parameter settings and ACK policies are as follows:
  a. **Table 11-183** lists the reference EDCA parameter settings and ACK policies for APs in voice scenarios.

Table 11-183 Reference EDCA parameter settings and ACK policies in voice scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VI	5	3	5	0	normal
AC_BE	10	6	5	0	normal
AC_BK	10	8	12	0	normal

b. Table 11-184 lists the reference EDCA parameter settings and ACK policies for APs in voice and video scenarios.

Table 11-184 Reference EDCA parameter settings and ACK policies in voice and video scenarios

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	4	2	2	0	normal
AC_VI	5	3	5	0	normal
AC_BE	10	6	12	0	normal
AC_BK	10	8	12	0	normal

c. In high-density scenarios, it is recommended that you run the **dynamic-edca enable** command to enable dynamic EDCA parameter adjustment.

d. For other scenarios, the default settings are recommended.

Example

Set EDCA parameters for AC_VO packets of STAs in SSID profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] wmm edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0
```

11.7.53 wmm mu-edca-client (SSID profile view)

Function

The **wmm mu-edca-client** command configures MU EDCA parameters for STAs.

The **undo wmm mu-edca-client** command restores the default MU EDCA parameter settings of STAs.

Table 11-185 lists the default MU EDCA parameter settings for STAs.

Table 11-185 Default MU EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	MUEDCATimer
AC_VO	3	2	2	1
AC_VI	4	3	2	1
AC_BE	10	4	3	1
AC_BK	10	4	7	1

Format

wmm mu-edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **muedcatimer** *muedcatimer-value* } *

undo wmm mu-edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 2 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be less than or equal to *ecwmax-value*.
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmax-value* and *ecwmin-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than or equal to *ecwmin-value*.

Parameter	Description	Value
muedcatimer *muedcatimer-value*	Specifies the MU EDCA timer, indicating the validity duration of MU EDCA parameters. When the timer is 0, the conventional EDCA parameters take effect.	The value is an integer that ranges from 1 to 255, in the unit of 8 TUs (1 TU = 1024 us).

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

STAs in compliance with 802.11ax or later standards (Wi-Fi 6/7 STAs) support two transmission modes: EDCA-based contention transmission and Trigger frame-based uplink transmission. In this way, Wi-Fi 6/7 STAs have more channel access opportunities than legacy STAs. To ensure channel access fairness, the MU EDCA mechanism is introduced. After being triggered by the AP to send data, Wi-Fi 6/7 STAs switch to the MU EDCA parameter set. The MU EDCA parameter set has a longer contention waiting time and a larger backoff window, and therefore has a lower priority compared with the conventional EDCA parameter set.

If Wi-Fi 6/7 STAs do not schedule Trigger frames for a long time, the STAs exit the MU EDCA mechanism and switch back to conventional EDCA parameters.

Precautions

Improper settings for MU EDCA parameters may cause poor uplink user experience.

In most scenarios, the default configurations are recommended. In MU scenarios, the recommended configurations are described in the following table.

Table 11-186 Recommended MU EDCA parameter settings for STAs in MU scenarios

Packet Type	ECWmax	ECWmin	AIFSN	MUEDCATimer
AC_VO	3	2	3	1
AC_VI	4	3	3	1
AC_BE	10	4	4	1

Packet Type	ECWmax	ECWmin	AIFSN	MUEDCATimer
AC_BK	10	4	8	1

Example

Set MU EDCA parameters for AC_VO packets of STAs in the SSID profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name p1
[HUAWEI-wlan-ssid-prof-p1] wmm mu-edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10
muedcatimer 1
```

11.7.54 wmm disable (radio profile view)

Function

The **wmm disable** command disables the Wi-Fi Multimedia (WMM) function in a 2G or 5G radio profile.

The **undo wmm disable** command enables the WMM function in a 2G or 5G radio profile.

By default, the WMM function is enabled in a 2G or 5G radio profile.

Format

wmm disable

undo wmm disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

802.11be, 802.11ax, 802.11ac and 802.11n STAs must support WMM. If the WMM function is disabled on a radio, 802.11be, 802.11ax, 802.11ac and 802.11n cannot work and STAs can access the network only in 802.11a/b/g mode.

If the WMM function is disabled, the access of non-HT STAs fails to be denied.

After the WMM function is enabled in a 2G or 5G radio profile, the AP radio to which the 2G or 5G radio profile is applied can use the WMM parameters.

Example

Enable the WMM function in 5G radio profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-5g-profile name default
[HUAWEI-wlan-radio-5g-prof-default] undo wmm disable
```

11.7.55 wmm mandatory enable

Function

The **wmm mandatory enable** disables STAs that do not support WMM from connecting to a WMM-enabled AP.

The **undo wmm mandatory enable** allows STAs that do not support WMM to connect to a WMM-enabled AP.

By default, STAs that do not support WMM are allowed to connect to a WMM-enabled AP.

Format

wmm mandatory enable

undo wmm mandatory enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

On a WLAN, wireless channels are open and all STAs have the same chance to occupy a channel. You can configure WMM to distinguish high-priority packets and enable the high-priority packets to preempt channels. You can also disable STAs that do not support WMM from connecting to a WMM-enabled AP, which prevents those STAs from preempting channels of WMM-capable STAs.

Example

Disable STAs that do not support WMM to connect to a WMM-enabled AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] wmm mandatory enable
```

11.8 DFI Configuration Commands

11.8.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

NOTE

The DFI function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, and AirEngine 5761-10WD)
- AirEngine X762 series APs running V200R021C10 or later
- AirEngine X771 series APs
- AirEngine 9700D-S (including matching ORUs)

11.8.2 dynamic flow inspection

Function

The **dynamic flow inspection** command enables or disables DFI on a VAP.

The **undo dynamic flow inspection** command restores the default DFI state on a VAP.

By default, DFI is disabled on AirEngine 5762S series models and enabled on other AP models.

Format

dynamic flow inspection { **enable** | **disable** }

undo dynamic flow inspection

Parameters

Parameter	Description	Value
enable	Enables the DFI function.	-
disable	Disables the DFI function.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DFI function is enabled on a VAP, the device identifies the traffic on this VAP and preferentially guarantees the downlink traffic of gaming and VoIP services on the air interface based on the identification result.

Precautions

Disabling the DFI function may cause the game turbo function to become invalid.

Example

Enable the DFI function on a VAP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name default
[HUAWEI-wlan-vap-prof-default] dynamic flow inspection enable
```

11.9 Application Identification Configuration Commands

11.9.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.9.2 application-group car (SAC profile view)

Function

The **application-group car** command enables rate limiting on a specified application group or a specified application in the group.

The **undo application-group car** command disables rate limiting on a specified application group or a specified application in the group.

By default, rate limiting is not configured for packets of any application in an application group.

Format

application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **car** *cir-value*

undo application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **car**

Parameters

Parameter	Description	Value
application-group *group-name*	Specifies the name of an application group.	The specified application group name must exist in the SAC signature file.
app-protocol *app-protocol-name*	Specifies the name of an application.	The specified application must exist.
all	Specifies all applications in the group.	-
car *cir-value*	Specifies the committed information rate (CIR).	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to enable rate limiting on all applications in a group or the specified application in the group.

Precautions

If **application-group remark (SAC profile view)** or **application-group car (SAC profile view)** and **application-group deny (SAC profile view)** are both configured for an application, the rate limit and priority modification policy do not take effect for the application protocol packets, and the packets are discarded.

Prerequisites

Example

Set the CIR value to 100 kbit/s of the application in the application group in the SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] application-group  app-protocol  car 100
```

11.9.3 application-group deny (SAC profile view)

Function

The **application-group deny** command enables the device to discard packets of all applications in an application group or a specific application in the group.

The **undo application-group deny** command disables the device from discarding packets of all applications in an application group or a specific application in the group.

By default, the device does not discard packets of any application in an application group.

Format

application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **deny**

undo application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **deny**

Parameters

Parameter	Description	Value
application-group *group-name*	Specifies the name of an application group.	The specified application group name must exist in the SAC signature file.
app-protocol *app-protocol-name*	Specifies the name of an application.	The specified application must exist.
all	Specifies all applications in the group.	-

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A WLAN transmits traffic of varied applications. The network administrator needs to know traffic usage of the applications to plan network capacity and locate problems on the network. In this situation, you can take application traffic control measures. If packets of a specified application need to be discarded, run the **application-group deny** command. You can also use the command to discard packets of a specified protocol type or a protocol type in a specified application group.

Precautions

If **application-group remark (SAC profile view)** or **application-group car (SAC profile view)** and **application-group deny (SAC profile view)** are both configured for an application, the rate limit and priority modification policy do not take effect for the application protocol packets, and the packets are discarded.

Prerequisites

Example

Configure the device to discard packets of the application in the SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] application-group  app-protocol  deny
```

11.9.4 application-group remark (SAC profile view)

Function

The **application-group remark** command re-marks packet priorities based on a specific application group or a specific application in the group.

The **undo application-group remark** command cancels packet priority remarking based on a specific application group or a specific application in the group.

By default, an action of re-marking packet priorities based on a specific application group or a specific application in the group is not configured in an SAC profile view.

Format

application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **remark** { **dscp** *dscp-value* | **dot1p** *dot1p-value* }

undo application-group *group-name* **app-protocol** { *app-protocol-name* | **all** } **remark** { **dscp** | **dot1p** }

Parameters

Parameter	Description	Value
application-group *group-name*	Specifies the name of an application group.	The specified application group name must exist in the SAC signature file.
app-protocol *app-protocol-name*	Specifies the name of an application.	The specified application must exist.
all	Re-marks priorities of packets of all applications in the group.	-
dscp *dscp-value*	Specifies the DSCP priority.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot1p *dot1p-value*	Specifies the 802.1p priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **application-group remark** command to re-mark packet priorities based on a specific application group or a specific application in the group. In this way, different user packets are granted the same priority, facilitating flexible user management.

Precautions

If **application-group remark (SAC profile view)** or **application-group car (SAC profile view)** and **application-group deny (SAC profile view)** are both configured for an application, the rate limit and priority modification policy do not take effect for the application protocol packets, and the packets are discarded.

Before running this command, ensure that the mode of mapping 802.3 packets (sent by upper-layer devices to APs) to 802.11 packets is the same as the packet priority re-marking type you want to configure. Specifically:

- Run the **priority-map downstream trust dot1p** command if you want to specify the parameter **dot1p** *dot1p-value*.
- Run the **priority-map downstream trust dscp** command (default) if you want to specify the parameter **dscp** *dscp-value*.

Prerequisites

Example

Re-mark DSCP priorities of packets of the application in the SAC profile **p1** as 30.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] application-group  app-protocol  remark dscp 30
```

11.9.5 category sub-category (AP user-defined application view)

Function

The **category sub-category** command configures the category and subcategory of an AP user-defined application.

The **undo category** command restores the default category and subcategory of an AP user-defined application.

The default category and subcategory of an AP user-defined application are **General** and **Other**, respectively.

Format

category *category* **sub-category** *sub-category*

undo category

Parameters

Parameter	Description	Value
category	Specifies the category of an application.	The specified category must be supported by the device.
sub-category	Specifies the subcategory of an application.	The specified subcategory must be supported by the device.

Views

AP user-defined application view

Default Level

2: Configuration level

Usage Guidelines

One category contains multiple subcategories, but one subcategory belongs to only one category.

During the configuration, you can enter a question mark (?) to display the supported categories and subcategories.

Example

Set the category and subcategory of the AP user-defined application **UD_abc** to **Business_Systems** and **Database**, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] category Business_Systems sub-category Database
```

11.9.6 defence engine enable ap-group

Function

The **defence engine enable ap-group** command enables the security engine for AP groups.

The **undo defence engine enable ap-group** command disables the security engine for AP groups.

By default, the security engine is disabled for an AP group.

Format

defence engine enable ap-group { **all** | **name** *ap-group-name* }

undo defence engine enable ap-group { **all** | **name** *ap-group-name* }

Parameters

Parameter	Description	Value
all	Enables or disables the security engine for all AP groups.	-
name *ap-group-name*	Enables or disables the security engine for the AP group with a specified name.	The AP group must exist.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a WLAN, if you need to monitor applications in real time, collect application traffic statistics, or perform QoS scheduling, run the **defence engine enable ap-group** command to enable the security engine for AP groups.

Precautions

After the **defence engine enable ap-group all** command is run to enable the security engine for all AP groups, you cannot disable the security engine for only a specified AP group. Instead, you can only run the **undo defence engine enable ap-group all** command to disable the security engine for all AP groups.

Example

Enable the security engine for the AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable ap-group name default
```

11.9.7 description (AP user-defined application rule view)

Function

The **description** command configures the description for an AP user-defined application rule.

The **undo description** command deletes the description of an AP user-defined application rule.

By default, no description is configured for a new AP user-defined application rule.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an AP user-defined application rule.	The value is a string of 1 to 128 case-sensitive characters, spaces supported.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the description for an AP user-defined application rule.

Example

Configure the description **test** for the AP user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] description test
```

11.9.8 description (AP user-defined application view)

Function

The **description** command configures the description for an AP user-defined application.

The **undo description** command deletes the description of an AP user-defined application.

By default, no description is configured for a new AP user-defined application.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an AP user-defined application.	The value is a string of 1 to 128 case-sensitive characters, spaces supported.

Views

AP user-defined application view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the description for an AP user-defined application.

Example

Configure the description **test** for the AP user-defined application **UD_abc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] description test
```

11.9.9 destination-port (AP user-defined application rule view)

Function

The **destination-port** command configures a port number for an AP user-defined application rule.

The **undo destination-port** command deletes the port number of an AP user-defined application rule.

By default, no port number is configured for a new AP user-defined application rule.

Format

destination-port *port*

undo destination-port

Parameters

Parameter	Description	Value
port	Specifies the port number for an AP user-defined application rule.	The value is an integer that ranges from 1 to 65535.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

After a port number is configured using this command, the service awareness (SA) engine will match network packets based on the configured port number as well as the transport-layer protocol and IP address (that is, 3-tuple information). If destination 3-tuple information about the traffic to be identified is determined, you can configure user-defined 3-tuple information to accelerate identification. For example, you can configure a 3-tuple user-defined rule based on the IP address, port number, and transport-layer protocol of a server, so that the rule can identify all the traffic accessing this server. A triplet rule must contain at least either one IP address or one port number. Note that only the destination port number can be specified in this command configuration.

Example

Configure the port number **80** for the AP user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] destination-port 80
```

11.9.10 display ap application

Function

The **display ap application** command displays information about applications on APs.

Format

display ap application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view information about all applications on APs.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Example

Display information about applications on APs.

```
<HUAWEI> display ap application
---------------------------------------------------------------------------------------------------------------

 AppID   Name                              Sub-category
---------------------------------------------------------------------------------------------------------------
 1       bt                             fileshare_p2p
 3       thunder                           fileshare_p2p
 5       ftp                            infrastructure
 6       ftps                           infrastructure
 9       qqlive                          peercasting
 15      kugoo                             peercasting
 41      qq_voip                           voip
 45      qq_im                             instant_message
......
---------------------------------------------------------------------------------------------------------------
 Total: 188
```

Table 11-187 Description of the **display ap application** command output

Item	Description
AppID	Application ID.
Name	Application name.
Sub-category	Subcategory to which an application belongs.

11.9.11 display ap application-group

Function

The **display ap application-group** command displays information about application groups on APs.

Format

display ap application-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays information about a specified application group. If this parameter is not specified, information about all application groups on APs is displayed.	The specified application group name must be supported by the application identification signature database file.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view information about all application groups or a specified application list on APs.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Example

Display information about all application groups on APs.

```
<HUAWEI> display ap application-group
----------------------------------------
  Index       GroupName
----------------------------------------
  1           auth_service
  2           finance
  3           data_backup
  4           database
  5           email
  6           enterprise_application
  7           internet_conferencing
  8           remote_access
  9           game
  10           instant_messaging
-----------------------------------------
 Total: 10
```

Display information about the application group **email**.

```
<HUAWEI> display ap application-group email
-----------------------------------
```

```
  Index    Application name
-----------------------------------
  9951     WebMail_AliyunMail
  10062    Webmail_DingTalkMail
  10528    Foxmail
----------------------------------
  Total: 3
```

Table 11-188 Description of the **display ap application-group** command output

Item	Description
Index	Sequence number of an application protocol in the application group.
GroupName	Name of the application group.
Application name	Name of an application protocol in the application group.

11.9.12 display apsa-sdb

Function

The **display apsa-sdb** command displays information about the AP application identification signature database.

Format

display apsa-sdb { **version** | **update information** }

Parameters

Parameter	Description	Value
version	Displays the version of the application identification signature database.	-
update information	Displays update information about the application identification signature database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Before and after updating the application identification signature database, you can run the **display apsa-sdb** { **version** | **update information** } command to view the version and update information of the signature database and check whether the update is successful.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Example

Display the version of the AP application identification signature database.

```
<HUAWEI> display apsa-sdb version
----------------------------------------------------------------
Current Version:
  Signature Database Version:2021032403
  Signature Database Size(byte):132897
  Update Time:2021-06-22 06:16:42
  Issue Time of the Update File:2021-03-24 10:11:23
----------------------------------------------------------------
```

Table 11-189 Description of the **display apsa-sdb version** command output

Item	Description
Current Version	The current signature database version is displayed in the following information.
Signature Database Version	Signature database version.
Signature Database Size(byte)	Signature database size.
Update Time	Update time of the signature database, that is, the installation time of the update package.
Issue Time of the Update File	Issue time of the update file, showing whether the update package is the latest.

Display update information about the AP application identification signature database.

```
<HUAWEI> display apsa-sdb update information
Current Update Status:  Idle.
--------------------------------------------------------
  Latest update finish time : 2021-06-22006:16:42
  Latest update result : success
 -------------------------------------------------------
```

Table 11-190 Description of the **display apsa-sdb update information** command output

Item	Description
Current Update Status	Current status of the update server. - Idle: No signature database is being updated. - Version Loading: The version is being loaded. - Live Updating: The online update is in progress. - Local Updating: The local update is in progress. - Version Rollbacking: The version is being rolled back. - Stop Updating: The update is being canceled. - Version Applying: The version is being downloaded and installed. - Version Restoring: The default version is being restored. - Version Uninstalling: The version is being uninstalled. - Update check: The update is being checked. - Engine start loading: The security engine is being loaded.
Latest update finish time	Last update finish time of the signature database.
Latest update result	Last update result of the signature database.

11.9.13 display defence engine configuration

Function

The **display defence engine configuration** command displays whether the security engine is enabled for APs.

Format

display defence engine configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **defence engine enable ap-group** command to enable the security engine for AP groups, you can run this command to check whether the security engine is enabled for APs.

Example

Display whether the security engine is enabled for APs.

```
<HUAWEI> display defence engine configuration
AP group engine state : all
------------------------------------------------------------
Group name                    State
------------------------------------------------------------
default                       Disable
------------------------------------------------------------
Total items displayed: 1
```

Table 11-191 Description of the **display defence engine configuration** command output

Item	Description
AP group engine state	Security engine state of AP groups. This field is displayed as **all** only when the security engine is enabled for all AP groups. Otherwise, no information is displayed for this field.
Group name	AP group name.
State	Whether the security engine is enabled for an AP group. - Enable: The security engine is enabled. - Disabled: The security engine is disabled.

11.9.14 display references sac-profile

Function

The **display references sac-profile** command displays the reference information of an SAC profile.

Format

display references sac-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays the reference information of a specified SAC profile.	The SAC profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the profiles by which a specified SAC profile is referenced.

Example

Display the reference information of the SAC profile **p1**.

```
<HUAWEI> display references sac-profile name p1
----------------------------------------------------
Reference type     Reference name
----------------------------------------------------
VAP profile        wlan-vap
----------------------------------------------------
Total: 1
```

Table 11-192 Description of the **display references sac-profile** command output

Item	Description
Reference type	Type of the profile that references an SAC profile.
Reference name	Name of the profile that references an SAC profile.

11.9.15 display wlan sac-profile

Function

The **display wlan sac-profile** command displays configuration and reference information about SAC profiles.

Format

display wlan sac-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all SAC profiles.	-
name *profile-name*	Displays information about the SAC profile with a specified name.	The SAC profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display sac-profile** command to view the configuration and reference information about SAC profiles.

Example

Display information about all SAC profiles.

```
<HUAWEI> display wlan sac-profile all
----------------------------------------------------------
Profile name                    Reference
----------------------------------------------------------
u1                           0
----------------------------------------------------------
Total: 1
```

Table 11-193 Description of the **display wlan sac-profile all** command output

Item	Description
Profile name	Name of an SAC profile.
Reference	Number of times an SAC profile is referenced.

Display information about the SAC profile **u1**.

```
<HUAWEI> display wlan sac-profile name u1
--------------------------------------------------------------------------------
SAC Profile name                      : u1
```

```
User statistic                 : disable
VAP statistic                  : disable
SAC Policy
--------------------------------------------------------------------------------
```

Table 11-194 Description of the **display wlan sac-profile name** command output

Item	Description
SAC Profile name	Name of an SAC profile. To configure this parameter, run the **sac-profile** command.
User statistic	User protocol statistics collection function. To configure this parameter, run the **user-protocol-statistic enable** command.
VAP statistic	Protocol statistics collection function on VAPs. To configure this parameter, run the **vap-protocol-statistic enable** command.
SAC Policy	SAC policy based on the protocol application or protocol application groups. To configure this parameter, run the **application-group car (SAC profile view)**, **application-group deny (SAC profile view)**, or **application-group remark (SAC profile view)** command.

11.9.16 display sac application user-defined

Function

The **display sac application user-defined** command displays user-defined applications deployed on an AP.

Format

display sac application user-defined { **id** *application-id* | **name** *name* | **all** }

Parameters

Parameter	Description	Value
id *application-id*	Specifies the ID of an AP user-defined application.	The value is an integer that ranges from 65000 to 65031.
name *name*	Specifies the name of an AP user-defined application.	The value is a string of case-sensitive characters, and must start with **UD_**. If the name does not contain spaces, the value is a string of 4 to 32 characters. If the name contains spaces, the value is a string of 6 to 34 characters and must be enclosed with double quotation marks (""), for example, **"UD_user for test"**. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot contain double quotation marks (").
all	Displays all AP user-defined applications.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

You can run this command to view the configuration of user-defined applications deployed on an AP.

Example

Display all AP user-defined applications.

```
<HUAWEI> display sac application user-defined all
------------------------------------------------------------------------------------------------------------
AppID Name                          Category                        Sub-category
------------------------------------------------------------------------------------------------------------
65000 UD_abc                        general                         other
------------------------------------------------------------------------------------------------------------
Total: 1
```

Table 11-195 Description of the **display sac application user-defined all** command output

Item	Description
AppID	ID of an AP user-defined application.
Name	Name of an AP user-defined application.
Category	Category of an AP user-defined application.
Sub-category	Subcategory of an AP user-defined application.

Display the configuration of the AP user-defined application **UD_abc**.

```
<HUAWEI> display sac application user-defined name UD_abc
------------------------------------------------------------------------------
User-defined application configuration:
Name             : UD_abc
ID               : 65000
Category         : general
Sub-category     : other

Rule configuration:
Rule number      : 1
Rule name        : rule1
Rule id          : 0
Rule state       : success
    IP address               : 0.0.0.0/0
    Destination port         : 0
    Protocol                 : tcp
    Signature type           : packet
    Signature direction      : both
    Signature plain-string   : abcdf
------------------------------------------------------------------------------
```

Table 11-196 Description of the **display sac application user-defined** command output

Item	Description
User-defined application configuration	
Name	Name of the AP user-defined application.
ID	ID of the AP user-defined application.
Category	Category of the AP user-defined application.
Sub-category	Subcategory of the AP user-defined application.
Description	Description of the AP user-defined application.

Item	Description
Rule configuration	
Rule number	Number of AP user-defined application rules.
Rule name	Name of an AP user-defined application rule.
Rule id	ID of an AP user-defined application rule.
Rule state	Rule delivery result. ● success: The rule is delivered successfully. ● failed: The rule delivery fails. ● committing: The rule is being delivered.
IP address	IPv4 address and subnet mask of an AP user-defined application rule.
Destination port	Port number of an AP user-defined application rule.
Protocol	Transport-layer protocol type of an AP user-defined application rule.
Signature type	Detection scope: ● packet
Signature direction	Detection direction: ● both: both request and response directions ● request: request direction ● response: response direction
Signature plain-string	Configured keyword.

11.9.17 ip-address (AP user-defined application rule view)

Function

The **ip-address** command configures an IPv4 address for an AP user-defined application rule.

The **undo ip-address** command deletes the IPv4 address of an AP user-defined application rule.

By default, no IPv4 address is configured for a new AP user-defined application rule.

Format

ip-address *ip-address* [*mask* | *mask-length*]

undo ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
mask	Specifies the subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer in the range from 1 to 32.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can configure a single IPv4 address for a user-defined application rule, or configure a network segment by specifying the subnet mask or mask length.

After an IPv4 address is configured using this command, the service awareness (SA) engine will match network packets based on the configured IPv4 address as well as the transport-layer protocol and port number (that is, 3-tuple information). If destination 3-tuple information about the traffic to be identified is determined, you can configure user-defined 3-tuple information to accelerate identification. For example, you can configure a 3-tuple user-defined rule based on the IP address, port number, and transport-layer protocol of a server, so that the rule can identify all the traffic accessing this server. A triplet rule must contain at least either one IP address or one port number. Note that only the destination IPv4 address can be specified in this command configuration.

Example

Configure the IPv4 address **10.1.1.1** for the user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] ip-address 10.1.1.1
```

11.9.18 priority-remark-default

Function

The **priority-remark-default** command enables the device to restore the default priorities of SAC applications.

The **undo priority-remark-default** command disables the device from restoring the default priorities of SAC applications.

By default, the device restores the default priorities of SAC applications.

Format

priority-remark-default

undo priority-remark-default

Parameters

None

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SAC function allows you to modify the priorities of application packets as required. However, defining the priorities of applications one by one is not user-friendly.

After this command is executed, the default priorities of all applications identified by SAC are restored based on the identification result. This ensures that applications that require high real-timeness and reliability have higher priorities when SAC is enabled.

To check the default priorities of different applications, run the **display sac default-priority** command.

Example

Enable the device to restore the default priorities of SAC applications.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI--wlan-sac-prof-p1] priority-remark-default
```

11.9.19 protocol (AP user-defined application rule view)

Function

The **protocol** command configures the transport-layer protocol for an AP user-defined application rule.

The **undo protocol** command restores the default transport-layer protocol of an AP user-defined application rule.

By default, the transport-layer protocol of an AP user-defined application rule is any, that is, the rule takes effect for both TCP and UDP packets.

Format

protocol { **tcp** | **udp** }

undo protocol

Parameters

Parameter	Description	Value
tcp	Specifies the TCP protocol.	-
udp	Specifies the UDP protocol.	-

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to configure the transport-layer protocol for an AP user-defined application rule. To make the rule take effect, however, you also need to specify other configuration items.

Example

Configure TCP as the transport-layer protocol of an AP user-defined application rule.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] protocol tcp
```

11.9.20 rule name (AP user-defined application view)

Function

The **rule name** command configures a rule for an AP user-defined application and displays the rule view.

The **undo rule** command deletes rules of an AP user-defined application.

By default, no rule is configured for a new AP user-defined application.

Format

rule name *name*

undo rule { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name *name*	Specifies the rule name.	The name is a string of case-sensitive characters. If the name does not contain spaces, the value is a string of 1 to 32 characters. If the name contains spaces, the value is a string of 3 to 34 characters and must be enclosed with double quotation marks (""), for example, **"user for test"**. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot contain double quotation marks ("). The name cannot be **any** or **all**.
all	Deletes all AP user-defined application rules.	-

Views

AP user-defined application view

Default Level

2: Configuration level

Usage Guidelines

If the specified rule name of an AP user-defined application does not exist, a new rule is created for the AP user-defined application and the rule view is displayed. If the specified rule name of the AP user-defined application already exists, the rule view is directly displayed.

A rule can be created based on 3-tuple information, keywords, or both 3-tuple information and keywords. The 3-tuple information refers to the server IP address, protocol type, and destination port number. The keywords are signatures of data packets or data flows corresponding to an application and uniquely identify the application.

- You can run the **ip-address (AP user-defined application rule view)**, **destination-port (AP user-defined application rule view)**, and **protocol (AP user-defined application rule view)** commands to specify 3-tuple information for an application.
- You can run the **signature (AP user-defined application rule view)** command to specify keywords for an application.

Multiple rules can be configured for one AP user-defined application. These rules are logically ORed. Data flows or packets belong to the application once they match one of the rules.

If the number of user-defined application rules on an AP reaches the maximum but the number of user-defined applications does not reach the maximum, you can continue to configure user-defined applications but cannot configure new rules for these applications.

Example

Create the rule **rule1** for the AP user-defined application **UD_abc** and display the rule view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1]
```

11.9.21 sac-profile

Function

The **sac-profile** command creates an SAC profile and displays the SAC profile view, or displays the view of an existing SAC profile.

The **undo sac-profile** command deletes an SAC profile. To delete a bound SAC profile, unbind the profile first.

By default, no SAC profile is available in the system.

Format

sac-profile name *profile-name*

undo sac-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an SAC profile.	The value is a string of 1 to 35 case-insensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all SAC profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **sac-profile** command to create an SAC profile. In the profile, you can perform the following configurations: discarding traffic of specified applications, setting priorities for packets of specified applications, and limiting packet rate of specified applications.

Example

Create the SAC profile **p1** and enter the SAC profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1]
```

11.9.22 signature (AP user-defined application rule view)

Function

The **signature** command configures the signature for an AP user-defined application.

The **undo signature** command deletes the signature of an AP user-defined application.

By default, no signature is configured for an AP user-defined application.

Format

signature context packet direction { **request** | **response** | **both** } **plain-string** *plain-string*

undo signature

Parameters

Parameter	Description	Value
context	Specifies the context with which the signature to be configured matches.	-
packet	Indicates the packet-based matching mode.	-
request	Indicates the request detection direction.	-
response	Indicates the response detection direction.	-
both	Indicates that the detection direction is both request and response directions.	-
plain-string *plain-string*	Indicates a plain-text string.	The value is a string of 3 to 128 case-sensitive characters. If the string contains spaces and question marks (?), the value is a string of 5 to 130 characters and must be enclosed with double quotation marks (""), for example, **"GET w?"**. If the string contains a double quotation mark ("), the double quotation mark needs to be escaped into **\x22**. For example, if the string is **abc"d**, you need to enter **abc\x22d**.

Views

AP user-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

Only one signature can be configured for an AP user-defined application rule.

If you run this command multiple times, only the latest configuration takes effect.

Example

Configure the signature **abcde** for the AP user-defined application rule **rule1**, configure the packet-based matching mode, and set the detection direction to the request direction.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc] rule name rule1
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] protocol tcp
[HUAWEI-wlan-user-def-app-UD_abc-rule-rule1] signature context packet direction request plain-string
abcde
```

11.9.23 sac-profile (VAP profile view)

Function

The **sac-profile** command binds an SAC profile to a VAP profile.

The **undo sac-profile** command unbinds an SAC profile to a VAP profile.

By default, no SAC profile is bound to a VAP profile.

Format

sac-profile *profile-name*

undo sac-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an SAC profile.	The SAC profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to bind an SAC profile to a VAP profile. The SAC profile then applies to all users using this VAP profile.

Example

Bind the SAC profile **p1** to the VAP profile **vap1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] quit
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] sac-profile p1
```

11.9.24 upgrade local apsa-sdb

Function

The **upgrade local apsa-sdb** command manually updates the local application signature database for APs.

Format

upgrade local apsa-sdb file *filename*

Parameters

Parameter	Description	Value
file *filename*	Specifies the update file, in .zip format. You need to upload the file to the flash directory of the storage device through FTP or SFTP in advance.	The value is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To update the signature database, download the update file from Huawei security center isecurity.huawei.com to the PC, upload the file to the flash directory of the storage device through FTP or SFTP, and then run this command to update the signature database.

Prerequisites

The security engine has been enabled for the specified AP group using the **defence engine enable ap-group** command.

Precautions

The update file must be placed in the flash directory, because this command does not support the file path setting.

This command cannot be used to load the signature database for APs running V200R019C00 or earlier.

Example

Manually update the local application signature database for APs using the signature file **APSA_H30071006_2021053106.zip**.

```
<HUAWEI> system-view
[HUAWEI] upgrade local apsa-sdb file APSA_H30071006_2021053106.zip
Warning: This operation will upgrade the AP signature database file. Continue? [Y/N]:y
It will take several seconds to update the AP signature database file, please wait...............
Info: The AP signature database file is successfully upgraded.
```

11.9.25 user-defined-application (WLAN view)

Function

The **user-defined-application** command creates an AP user-defined application and displays the AP user-defined application view.

The **undo user-defined-application** command deletes AP user-defined applications.

By default, no AP user-defined application is configured.

Format

user-defined-application id *application-id* [**name** *name*]

undo user-defined-application { **id** *application-id* | **name** *name* | **all** }

Parameters

Parameter	Description	Value
id *application-id*	Specifies the ID of an AP user-defined application.	The value is an integer that ranges from 65000 to 65031.

Parameter	Description	Value
name *name*	Specifies the name of an AP user-defined application.	The value is a string of case-sensitive characters, and must start with **UD_**. If the name does not contain spaces, the value is a string of 4 to 32 characters. If the name contains spaces, the value is a string of 6 to 34 characters and must be enclosed with double quotation marks (""), for example, **"UD_user for test"**. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot contain double quotation marks (").
all	Deletes all AP user-defined applications.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If the specified AP user-defined application name does not exist, a new AP user-defined application is created and the AP user-defined application view is displayed. If the specified AP user-defined application name exists, the AP user-defined application view is directly displayed. If the **name** parameter is not specified, the user-defined application named **UD_id** is created by default.

Example

Create the AP user-defined application **UD_abc**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan] user-defined-application id 65000 name UD_abc
[HUAWEI-wlan-user-def-app-UD_adc]
```

11.9.26 user-protocol-statistic enable

Function

The **user-protocol-statistic enable** command enables the user protocol statistics collection function.

The **undo user-protocol-statistic enable** command disables the user protocol statistics collection function.

By default, the user protocol statistics collection function is disabled.

Format

user-protocol-statistic enable

undo user-protocol-statistic enable

Parameters

None

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

After going online on an AP, users start various applications on STAs to access the network. By analyzing packets sent by STAs, the collects information about network usage by applications of each user and reports the collected information (including the IP and MAC addresses of STAs and the application types) to the network management system (NMS). The NMS then displays and stores the information, which the administrator can view at any time. To identify user-based applications, run the **user-protocol-statistic enable** command.

NOTE

This function takes effect only for STAs who go online after the **user-protocol-statistic enable** command is successfully executed.

Example

Enable the user protocol statistics collection function in the SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] user-protocol-statistic enable
```

11.9.27 vap-protocol-statistic enable

Function

The **vap-protocol-statistic enable** command enables the protocol statistics collection function in a VAP.

The **undo vap-protocol-statistic enable** command disables the protocol statistics collection function in a VAP.

By default, the protocol statistics collection function is disabled in a VAP.

Format

vap-protocol-statistic enable

undo vap-protocol-statistic enable

Parameters

None

Views

SAC profile view

Default Level

2: Configuration level

Usage Guidelines

After going online on an AP, users start various applications on STAs to access the network. By analyzing packets sent by STAs, the collects information about network usage by applications of each user and reports the collected information (including the IP and MAC addresses of STAs and the application types) to the network management system (NMS). The NMS then displays and stores the information, which the administrator can view at any time. To identify applications in a VAP, run the **vap-protocol-statistic enable** command.

Example

Enable the protocol statistics collection function for VAPs in SAC profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sac-profile name p1
[HUAWEI-wlan-sac-prof-p1] vap-protocol-statistic enable
```

11.10 WLAN Location Configuration Commands

11.10.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.
- The AeroScout MU location function is not supported by the following models:
  - AirEngine X760 series APs running V200R022C00 or earlier
  - AirEngine X761 series APs running V200R022C00 or earlier
  - AirEngine X762 series APs running V200R022C00 or earlier (In V200R022C10 and later versions, these APs support only single AP-based AeroScout MU location but do not support three-point location.)
  - AirEngine series central APs (including matching RUs) running V200R022C00 or earlier

  - AirEngine 9700D-S (including matching ORUs)
- The Wi-Fi tag location function is not supported by the following models:
  - AirEngine X760 series APs: do not support Ekahau tag location, and do not support AeroScout tag location in V200R022C00 or earlier.
  - AirEngine X761 series APs: do not support Ekahau tag location, and do not support AeroScout tag location in V200R022C00 or earlier.
  - AirEngine X771 series APs: do not support Ekahau tag location.
  - AirEngine X762 series APs
  - AirEngine series central APs (including matching RUs): do not support Ekahau tag location, and do not support AeroScout tag location in V200R022C00 or earlier.
  - AirEngine 9700D-S (including matching ORUs)
- Only the following models support Bluetooth terminal location, Bluetooth tag location, and Bluetooth data transparent transmission:
  - AirEngine X760 series APs
  - AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
  - AirEngine X771 series APs
  - AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later
- The Bluetooth broadcast function is supported only by the following models:
  - AirEngine X760 series APs
  - AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
  - AirEngine X771 series APs
  - AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

11.10.2 aeroscout compound-time

Function

The **aeroscout compound-time** command configures the aggregation time of AeroScout tag and mobile unit (MU) packets on the AC.

The **undo aeroscout compound-time** command restores the default aggregation time of AeroScout tag and MU packets.

The default aggregation time of AeroScout tag and MU packets is 6553.5s on the AC.

Format

aeroscout compound-time *time-value*

undo aeroscout compound-time

Parameters

Parameter	Description	Value
time-value	Specifies the packet aggregation time.	The value is an integer that ranges from 0 to 65535. The unit is in 0.1s. If *time-value* is set to 0, the AP does not aggregate packets but reports the packets in real time.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During AeroScout location, the AP does not report the received tag packets immediately to the upstream device but aggregates the packets. After a specified time, the AP reports the aggregated packets.

The AeroScout location server delivers an aggregation time of 6553.5s to the APs. The AC delivers the aggregation time to the APs using the **aeroscout compound-time** command. The AP selects a smaller aggregation time. By default, the aggregation time on the APs is 6553.5s.

If the packet aggregation time is set to a large value on the AeroScout location system, it takes a long time for the AP to report the aggregated packets, resulting in poor real-time performance and a large delay in the transmission of location packets. You can run the **aeroscout compound-time** command to set a small aggregation time to reduce the delay in location packet transmission.

Precautions

When the size of aggregated packets on an AP reaches 1k bytes, the AP immediately reports the aggregated packets.

Example

Set the aggregation time to 10s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout compound-time 100
```

11.10.3 aeroscout local

Function

The **aeroscout local** command configures a local IP address used by the AC to receive packets from a location server.

The **undo aeroscout local** command deletes the configured local IP address used by the AC to receive packets from a location server.

By default, no local IP address is configured for the AC to receive packets from a location server.

Format

aeroscout local ip-address *ip-address*

undo aeroscout local

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies a local IPv4 address used by the AC to receive packets from a location server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **aeroscout server port** *port-num* **via-ac ac-port** *ac-port-num* command is executed to configure location data to be reported through the AC, run the **aeroscout local ip-address** *ip-address* command to configure a local IP address used by the AC to receive packets from a location server. The AC can receive packets from the location server only using this IP address.

Precautions

You need to run the **source ip-address** *ip-address* command to configure the source IP address used by the AC to send packets to the location server.

Example

Configure 10.1.1.1 as the local IP address used by the AC to receive packets from a location server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] aeroscout local ip-address 10.1.1.1
```

11.10.4 aeroscout mu-enable

Function

The **aeroscout mu-enable** command enables WLAN location of AeroScout mobile units (MUs).

The **undo aeroscout mu-enable** command disables WLAN location of AeroScout MUs.

By default, WLAN location of AeroScout MUs is disabled.

Format

aeroscout mu-enable

undo aeroscout mu-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **aeroscout mu-enable** command to enable WLAN location of AeroScout MUs.

Example

Enable WLAN location of AeroScout MUs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout mu-enable
```

11.10.5 aeroscout server

Function

The **aeroscout server** command sets the port number for APs to report location packets of AeroScout tags and Mobile Units (MUs).

The **undo aeroscout server** command deletes the configured port number for APs to report location packets of AeroScout tags and MUs.

By default, no port number is configured for APs to report location packets of AeroScout tags and MUs.

Format

aeroscout server port *port-num* [**via-ac ac-port** *ac-port-num*]

undo aeroscout server

Parameters

Parameter	Description	Value
port *port-num*	Specifies a port number through which APs report location packets of AeroScout tags and MUs when APs are configured to directly report data. Specifies a port number through which the AC reports location packets of AeroScout tags and MUs when the AC is configured to forward data.	The value is an integer that ranges from 1025 to 65535.
via-ac	Indicates that the AC forwards location packets of AeroScout tags and MUs reported by APs to the AeroScout server. **NOTE** If the APs report the received tag packets and MU packets directly to the AeroScout location server, the **display wlan location statistics aeroscout** command cannot collect statistics about AeroScout tag locations and MU locations, and the **display wlan location config-info aeroscout** command cannot display the configuration delivered by the AeroScout location server to APs.	-
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report location packets of AeroScout tags and MUs.	The value is an integer that ranges from 1025 to 65535.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Location packets of AeroScout tags and MUs received by APs can be reported to the AeroScout location server directly or through the AC.

Precautions

You cannot configure a port number that has been occupied by other services. Otherwise, the destination port configuration fails.

For the same location method, via-ac can be configured only in one profile. If **via-ac** has been specified in the current location profile for a specific location method, it cannot be specified in other profiles for the same location method.

NOTE

An AeroScout server proactively establishes connections with APs. Therefore, manually add the APs and specify their MAC addresses, port numbers, and IP addresses on the AeroScout server. If the AC is configured to forward location data, you only need to specify the AC IP address. You do not need to specify the IP address of the AeroScout server on the AC.

Follow-up Procedure

If the AC is configured to forward location packets to the location server, run the **source ip-address** *ip-address* command to configure the source IP address for the AC to send packets to the location server and run the **aeroscout local ip-address** *ip-address* command to configure a local IP address for the AC to receive packets from the location server.

Example

Set the port number for APs to report location packets of AeroScout tags and MUs to 1144.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout server port 1144
```

11.10.6 aeroscout tag-enable

Function

The **aeroscout tag-enable** command enables WLAN location of AeroScout tags.

The **undo aeroscout tag-enable** command disables WLAN location of AeroScout tags.

By default, WLAN location of AeroScout tags is disabled.

Format

aeroscout tag-enable

undo aeroscout tag-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **aeroscout tag-enable** command to enable WLAN location of AeroScout tags.

Example

Enable WLAN location of AeroScout tags.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] aeroscout tag-enable
```

11.10.7 ble low-power-threshold

Function

The **ble low-power-threshold** command sets a low power alarm threshold for BLE devices or Bluetooth tags.

The **undo ble low-power-threshold** command restores the low power alarm threshold of BLE devices or Bluetooth tags to the default value.

By default, the low power alarm threshold of BLE devices or Bluetooth tags is 20%.

Format

ble low-power-threshold *low-power-threshold*

undo ble low-power-threshold

Parameters

Parameter	Description	Value
low-power-threshold	Specifies the low power alarm threshold of BLE devices or Bluetooth tags.	The value is an enumerated type. The options are as follows: • 0: 0% • 20: 20% • 40: 40% • 60: 60% • 80: 80%

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After the **sniffer enable** command is executed to enable the Bluetooth monitoring or Bluetooth tag location function of an AP's built-in Bluetooth module, the built-in Bluetooth module will scan and obtain information about surrounding BLE devices or Bluetooth tags. The information includes battery power of BLE devices or Bluetooth tags. When the obtained battery power of a BLE device or Bluetooth tag is lower than the low power alarm threshold, the AC generates an alarm indicating that the BLE device or Bluetooth tag has low battery power.

Example

Set the low power alarm threshold for BLE devices or Bluetooth tags to 40%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble low-power-threshold 40
```

11.10.8 ble monitoring-list

Function

The **ble monitoring-list** command adds specified Bluetooth devices to the Bluetooth device monitoring list.

The **undo ble monitoring-list** command deletes specified Bluetooth devices from the Bluetooth device monitoring list.

By default, no Bluetooth devices are added to the monitoring list.

Format

ble monitoring-list { **all** | **mac** *mac-address1* [**to** *mac-address2*] }

undo ble monitoring-list { **all** | **mac** *mac-address1* [**to** *mac-address2*] }

Parameters

Parameter	Description	Value
mac *mac-address1*	Specifies the MAC address of a Bluetooth device to be monitored.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
to *mac-address2*	Specifies the end MAC address of a Bluetooth device when Bluetooth devices are added to or deleted from the monitoring list in batches. The *mac-address2* value must be greater than or equal to the *mac-address1* value. *mac-address1* and *mac-address2* together specify a range of MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Indicates all Bluetooth devices.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Bluetooth monitoring, Bluetooth tag location, or Bluetooth data transparent transmission function is enabled using the **sniffer enable** command, no Bluetooth device is monitored when no Bluetooth device (BLE device, Bluetooth tag, or Bluetooth client) is added to the monitoring list. After Bluetooth devices are added to the monitoring list, only the Bluetooth devices in the list are monitored. When a Bluetooth device in the monitoring list is offline or has insufficient battery power, an alarm is triggered on the device accordingly. Bluetooth clients do not support low battery power alarms.

Precautions

After the Bluetooth monitoring, Bluetooth tag location, or Bluetooth data transparent transmission function is disabled using the **undo sniffer enable** command, an alarm is triggered on the device, indicating that Bluetooth devices are offline.

Bluetooth devices with all-0 or all-F MAC addresses cannot be added to the monitoring list.

Example

Add the Bluetooth device with the MAC address 00e0-fc12-3456 to the monitoring list.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble monitoring-list mac 00e0-fc12-3456
```

Add the Bluetooth devices with MAC addresses from 00e0-fc12-3456 to 00e0-fc12-3458 to the monitoring list.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble monitoring-list mac 00e0-fc12-3456 to 00e0-fc12-3458
```

Disable the device from monitoring Bluetooth devices.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] undo ble monitoring-list all
Warning: This operation will delete all the manually configured Bluetooth monitoring lists. Continue? [Y/
N]:y
```

11.10.9 ble report interval

Function

The **ble report interval** command sets an interval at which an AP reports Bluetooth device information.

The **undo ble report interval** command restores the default interval at which an AP reports Bluetooth device information.

By default, an AP reports Bluetooth device information at an interval of 10 minutes.

Format

ble report interval *interval-value*

undo ble report interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which an AP reports Bluetooth device information.	The value is an integer that ranges from 1 to 60, in minutes.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP collects information about 255 Bluetooth devices, the AP stops collecting information about more Bluetooth devices. When the aging time of Bluetooth device information collected by an AP expires, the AP clears aged device information and scans for new Bluetooth device information. The aging time of Bluetooth device information cannot be configured. The default aging time is 10 minutes. When the interval at which an AP reports Bluetooth device information times out, the AP reports Bluetooth device information to an AC. Bluetooth device information includes types, RSSIs, and whether Bluetooth tags are disconnected.

Example

Set the interval at which an AP reports Bluetooth device information to 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble report interval 20
```

11.10.10 ble source

Function

The **ble source** command configures a global source IP address in packets sent by an AC to a location server.

The **undo ble source** command deletes a global source IP address from packets sent by an AC to a location server.

By default, the source IP address is not configured in packets sent by an AC to a location server, and the IP address of the route outbound interface is used as the source IP address.

Format

ble source ip-address *ip-address*

undo ble source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies a source IPv4 address in packets sent by an AC to a location server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Bluetooth location scenarios, you can run the **ble source** command to configure a source IP address in packets sent by an AC to a location server.

Run the **ble source** command to configure different source IP addresses for the active and standby ACs.

When source IP addresses are configured on an AC using the **ble source** and **source** commands at the same time, the source IP address configured using the **source** command takes effect.

Precautions

- Ensure that the AC IP address manually configured on the location server is the same as that configured using the **ble source** command.
- The source IP address must exist on the AC; otherwise, the configuration does not take effect.

Example

Configure 10.102.25.23 as the source IP address of the packets sent from the AC to the location server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble source ip-address 10.102.25.23
```

11.10.11 ble-profile (AP group view and AP view)

Function

The **ble-profile** command binds a BLE profile to an AP group or AP.

The **undo ble-profile** command unbinds a BLE profile from an AP group or AP.

By default, no BLE profile is bound to an AP group or AP.

Format

ble-profile *profile-name*

undo ble-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a BLE profile.	The BLE profile name must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a BLE profile using the **ble-profile (WLAN view)** command, you need to bind the profile in the AP view or AP group view to make the settings in the profile take effect.

Precautions

After you bind a BLE profile in the AP view or AP group view, parameter settings in the BLE profile take effect for all APs using this profile.

Example

Create BLE profile **example** and bind the profile to AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] ble-profile example
```

11.10.12 ble-profile (WLAN view)

Function

The **ble-profile** command creates a BLE profile or displays the BLE profile view.

The **undo ble-profile** command deletes a BLE profile.

By default, no BLE profile is created.

Format

ble-profile name *profile-name*

undo ble-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a BLE profile, which must be unique and identifies a profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all BLE profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to create or delete a BLE profile or enter the BLE profile view to configure the profile. If the specified profile name does not exist, this command creates a new BLE profile and displays the configuration view of this profile. All parameters in this profile use default values. You can also change values of these parameters.

Follow-up Procedure

After creating a BLE profile, you need to run the **ble-profile (AP group view and AP view)** command in the AP view or AP group view to bind the profile to make the settings in the profile take effect.

Precautions

A BLE profile bound to an AP or AP group cannot be deleted. To delete a BLE profile, unbind it in the AP view or AP group view.

Example

Create BLE profile **example** and enter its view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example]
```

11.10.13 broadcaster enable

Function

The **broadcaster enable** command enables the Bluetooth broadcast function of an AP's built-in Bluetooth module.

The **undo broadcaster enable** command disables the Bluetooth broadcast function of an AP's built-in Bluetooth module.

By default, the Bluetooth broadcast function of an AP's built-in Bluetooth module is disabled.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcaster enable

undo broadcaster enable

Parameters

None

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

When an AP's built-in Bluetooth module is used as a BLE device, you can run this command to enable the Bluetooth broadcast function. After this function is enabled, the built-in Bluetooth module sends BLE broadcast frames to surrounding devices. The frame content complies with the iBeacon protocol.

Enabling both the Bluetooth scanning and broadcast functions of an AP affects the efficiency for the AP's Bluetooth module to scan surrounding BLE devices. When an AP does not serve as a Bluetooth base station, it is recommended that the broadcast function of the AP be disabled.

Example

Enable the Bluetooth broadcast function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcaster enable
```

11.10.14 broadcasting-content

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID, Major, and Minor fields in a BLE broadcast frame sent by an AP's built-in Bluetooth module are null, and the RSSI calibration value is –65 dBm.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-content { **uuid** { **uuid-character-string** *uuid-value* | **uuid-hex** *uuid-value* } | **major** { **major-character-string** *major-value* | **major-hex** *major-value* | **major-decimal** *major-value* } | **minor** { **minor-character-string** *minor-value* | **minor-hex** *minor-value* | **minor-decimal** *minor-value* } | **reference-rssi** *reference-rssi-value* }*

undo broadcasting-content [**uuid** | **major** | **minor** | **reference-rssi**]

Parameters

Parameter	Description	Value
uuid uuid-character-string *uuid-value*	Specifies the UUID field in a BLE broadcast frame. UUID is the universally unique identifier of a BLE device.	The value is a string of 1 to 16 characters. The default value is null.
uuid uuid-hex *uuid-value*	Specifies the UUID field in a BLE broadcast frame. UUID is the universally unique identifier of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 32 bytes. The default value is null.
major major-character-string *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.
major major-hex *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
major major-decimal *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
minor minor-character-string *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.

Parameter	Description	Value
minor minor-hex *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
minor minor-decimal *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
reference-rssi *reference-rssi-value*	Specifies the RSSI calibration value of a BLE device. RSSI calibration value indicates the RSSI value of a BLE device measured at a distance of 1 m. It is used to estimate the distance between the BLE device and Bluetooth terminals.	The value is an integer that ranges from –97 to –50, in dBm. The default value is -65 that is measured when the transmit power of an APs' built-in Bluetooth module is 0 dBm.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to configure the content of BLE broadcast frames sent by the module.

Precautions

The RSSI calibration value in a BLE broadcast frame is set based on the actual measurement result.

After changing the transmit power of a built-in Bluetooth module using the **tx-power (BLE profile view)** command, you need to measure and configure the RSSI calibration value again. Therefore, you are advised to run the **tx-power (BLE profile view)** command to configure the transmit power of a built-in Bluetooth module before configuring the RSSI calibration value.

Example

Configure the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module. Set **UUID uuid-hex** to **12345678123456789**, **Major major-hex** to **A22**, **Minor minor-hex** to **011**, and **reference-rssi** to **-70**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcasting-content uuid uuid-hex 12345678123456789 major
major-hex A22 minor minor-hex 011 reference-rssi -70
```

Configure the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module. Set **LocalName** to **name1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcasting-content local-name name1
```

11.10.15 broadcasting-content (AP group view)

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID of the BLE broadcast frames sent by an AP's built-in Bluetooth module is null.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-content uuid { **uuid-character-string** *uuid-value* | **uuid-hex** *uuid-value* }

undo broadcasting-content uuid

Parameters

Parameter	Description	Value
uuid uuid-character-string *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is a string of characters and used to identity devices.	The value is a string of 1 to 16 characters.
uuid uuid-hex *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is in hexadecimal notation and used to identity devices.	The value is a string of 1 to 32 hexadecimal characters.

Views

AP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to configure the UUID of BLE broadcast frames sent by the module.

Precautions

The UUIDs set in the AP view, BLE profile bound to the AP view, AP group view, and BLE profile bound to the AP group take effect in the following order:

1. UUID set in the AP view
2. UUID set in the BLE profile bound to the AP view
3. UUID set in the AP group view
4. UUID set in the BLE profile bound to the AP group view

Example

Set the UUID of the BLE broadcast frames sent by an AP's Bluetooth module in the AP group view to **12345678123456789** in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name mygroup
[HUAWEI-wlan-ap-group-mygroup] broadcasting-content uuid uuid-hex 12345678123456789
```

11.10.16 broadcasting-content (AP view)

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID, Major, Minor, and RSSI calibration fields in a BLE broadcast frame sent by an AP's built-in Bluetooth module are null.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-content { **uuid** { **uuid-character-string** *uuid-value* | **uuid-hex** *uuid-value* } | **major** { **major-character-string** *major-value* | **major-hex** *major-value* | **major-decimal** *major-value* } | **minor** { **minor-character-string** *minor-value* | **minor-hex** *minor-value* | **minor-decimal** *minor-value* } | **reference-rssi** *reference-rssi-value* }*

undo broadcasting-content [**uuid** | **major** | **minor** | **reference-rssi**]

Parameters

Parameter	Description	Value
uuid uuid-character-string *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is a string of characters and used to identity devices.	The value is a string of 1 to 16 characters.
uuid uuid-hex *uuid-value*	Specifies the UUID field of BLE broadcast frames, which is in hexadecimal notation and used to identity devices.	The value is a string of 1 to 32 hexadecimal characters.
major major-character-string *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.

Parameter	Description	Value
major major-hex *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
major major-decimal *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
minor minor-character-string *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.
minor minor-hex *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is in hexadecimal notation. The value length ranges from 1 to 4 bytes. The default value is null.
minor minor-decimal *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of a BLE device.	The value is an integer that ranges from 0 to 65535. The default value is null.
reference-rssi *reference-rssi-value*	Specifies the RSSI calibration value of a BLE device. RSSI calibration value indicates the RSSI value of a BLE device measured at a distance of 1 m. It is used to estimate the distance between the BLE device and Bluetooth terminals.	The value is an integer that ranges from –97 to –50, in dBm. The default value is null.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to configure the content of BLE broadcast frames sent by the module.

Precautions

The contents set in the AP view, BLE profile bound to the AP view, AP group view, and BLE profile bound to the AP group take effect in the following order:

1. Contents set in the AP view
2. Contents set in the BLE profile bound to the AP view
3. Contents set in the AP group view
4. Contents set in the BLE profile bound to the AP group view

Example

Set the UUID of the BLE broadcast frames sent by an AP's Bluetooth module in the AP view to **12345678123456789** in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] broadcasting-content uuid uuid-hex 12345678123456789
```

11.10.17 broadcasting-interval

Function

The **broadcasting-interval** command configures the interval for an AP's built-in Bluetooth module to send BLE broadcast frames.

The **undo broadcasting-interval** command restores the default interval for an AP's built-in Bluetooth module to send BLE broadcast frames.

By default, the built-in Bluetooth module of an AP sends BLE broadcast frames at an interval of 500 ms.

NOTE

The Bluetooth broadcast function is supported only by the following models:

- AirEngine X760 series APs
- AirEngine X761 series APs (excluding the AirEngine 5761-10W, AirEngine 5761S-10W, AirEngine 5761-10WD, and AirEngine 5761-11EI)
- AirEngine X771 series APs
- AirEngine 5762-12 and AirEngine 5762S-12 running V200R022C10 or later

Format

broadcasting-interval *broadcasting-interval-value*

undo broadcasting-interval

Parameters

Parameter	Description	Value
broadcasting-interval-value	Specifies the interval for an AP's built-in Bluetooth module to send BLE broadcast frames.	The value is an integer that ranges from 100 to 10240, in milliseconds.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run this command to set the interval for the module to send BLE broadcast frames.

Example

Set the interval for an AP's built-in Bluetooth module to send BLE broadcast frames to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] broadcasting-interval 1000
```

11.10.18 display ble-profile

Function

The **display ble-profile** command displays configuration and reference information about a BLE profile.

Format

display ble-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all BLE profiles.	-
name *profile-name*	Displays information about the BLE profile with a specified name.	The BLE profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about BLE profiles.

Example

Display information about all BLE profiles.

```
<HUAWEI> display ble-profile all
------------------------------------------------------------------------------
Profile name                     Reference
------------------------------------------------------------------------------
example                          1
------------------------------------------------------------------------------
Total: 1
```

Table 11-197 Description of the **display ble-profile all** command output

Item	Description
Profile name	BLE profile name.
Reference	Number of times a BLE profile is referenced.

Display information about the BLE profile **example**.

```
<HUAWEI> display ble-profile name example
--------------------------------------------------------------------------------
Broadcaster switch            : disable
Broadcaster interval(ms)      : 500
Broadcaster content
  UUID                        : 00000000000000012345678123456789(hex)
  Major                       : 0A22(hex)
  Minor                       : 0011(hex)
  Reference RSSI              : -70
```

```
Transmit power              : 0
Sniffer switch              : disable
Sniffer mode                : -
Source IP address           : 0.0.0.0
Report switch               : enable
Report mode                 : immediate
Report interval(s)          : 10
Report server               : 0.0.0.0
Report server port          : -
Report via-AC               : disable
Report via-AC port          : -
------------------------------------------------------------------------------
```

Table 11-198 Description of the **display ble-profile name** *profile-name* command output

Item	Description
Broadcaster switch	Whether the Bluetooth broadcast function is enabled. ● enable ● disable To configure this parameter, run the **broadcaster enable** command.
Broadcaster interval(ms)	Interval at which BLE broadcast frames are sent. To configure this parameter, run the **broadcasting-interval** command.
Broadcaster content	Content of a BLE broadcast frame. To configure this parameter, run the **broadcasting-content** command.
UUID	UUID field in a BLE broadcast frame. UUID refers to the universally unique identifier of a Bluetooth device.
Major	Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BLE device, for example, location of the BLE device.
Minor	Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BLE device, for example, location of the BLE device.

Item	Description
Reference RSSI	RSSI calibration value. This value refers to the RSSI of a BLE device measured at a distance of 1 m. It is used to calculate the distance between a BLE device and a BLE terminal or tag.
MQTT Server	MQTT server configuration. To configure this parameter, run the **mqtt-server** command.
Transmit power	Transmit power of an AP's built-in Bluetooth module. To configure this parameter, run the **tx-power (BLE profile view)** command.
Sniffer switch	Whether the Bluetooth function is enabled. ● enable ● disable To configure this parameter, run the **sniffer enable** command.
Sniffer mode	Bluetooth working mode. To configure this parameter, run the **sniffer enable** command.
Source IP address	Source IP address used to report Bluetooth packets. To configure this parameter, run the **source (BLE profile view)** command.
Report switch	Whether Bluetooth packets are reported. ● enable ● disable To configure this parameter, run the **report enable** command.
Report mode	Mode in which an AP reports Bluetooth packets. To configure this parameter, run the **report-mode** command.
Report interval(s)	Interval at which an AP reports Bluetooth packets. To configure this parameter, run the **report-mode** command.

Item	Description
Report server	IP address of a Bluetooth server. To configure this parameter, run the **report-to-server** command.
Report server port	Port number of a Bluetooth server. To configure this parameter, run the **report-to-server** command.
Report via-AC	Whether Bluetooth packets are reported to a server through the AC. ● enable: Bluetooth packets are reported through the AC. ● disable: Bluetooth packets are reported not through the AC. To configure this parameter, run the **report-to-server** command.
Report via-AC port	Port number used by the AC to report Bluetooth packets. To configure this parameter, run the **report-to-server** command.

11.10.19 display location-profile

Function

The **display location-profile** command displays configuration information about a location profile.

Format

display location-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Specifies all location profiles.	-
name *profile-name*	Specifies a location profile.	The location profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration information about a location profile to verify the configuration.

Example

Display all location profiles.

```
<HUAWEI> display location-profile all
----------------------------------------------------------
Profile name                  Reference
----------------------------------------------------------
default                         1
----------------------------------------------------------
Total: 1
```

Table 11-199 Description of the **display location-profile all** command output

Item	Description
Profile name	Name of a location profile.
Reference	Number of times a location profile is referenced.

Display the default configuration of the location profile **default**.

```
<HUAWEI> display location-profile name default
--------------------------------------------------------------------------------
Aeroscout-tag                   : disable
Aeroscout-mu                     : disable
Aeroscout ae-port                 : -
Aeroscout compound-time(100ms) : 65535
Aeroscout via-AC                 : disable
Aeroscout via-AC port             : -
Ekahau-tag                       : disable
Ekahau erc IP-address             : 0.0.0.0
Ekahau erc port                  : -
Ekahau via-AC                    : disable
Ekahau via-AC port                : -
Source IP-address                : 0.0.0.0
private mu                       : disable
private server                   : 0.0.0.0
private server domain             : -
private server port              : -
private via-AC                   : disable
private via-AC port               : -
private report-frequency(ms)   : 20000
private report-protocol          : udp
private ssl-policy name          : -
private mu protocol-version    : v3
collect location data                        : disable
collect location data RSSI threshold(dBm)  : -75
------------------------------------------------------------
```

Table 11-200 Description of the **display location-profile name default** command output

Item	Description
Aeroscout-tag	Whether WLAN location of AeroScout tags is enabled. To configure this parameter, run the **aeroscout tag-enable** command.
Aeroscout-mu	Whether WLAN location of AeroScout MUs is enabled. To configure this parameter, run the **aeroscout mu-enable** command.
Aeroscout ae-port	Port number used by APs to report location packets. To configure this parameter, run the **aeroscout server** command.
Aeroscout compound-time	Aggregation time of AeroScout location packets. To configure this parameter, run the **aeroscout compound-time** command.
Aeroscout via-AC	Whether AeroScout location packets are reported to the location server through an AC. ● enable: The AeroScout location packets are reported to the location server through an AC. ● disable: The AeroScout location packets are not reported to the location server through an AC. To configure this parameter, run the **aeroscout server** command.
Aeroscout via-AC port	Port number used by an AC to report AeroScout location packets. To configure this parameter, run the **aeroscout server** command.
Ekahau-tag	Whether WLAN location of Ekahau tags is enabled. To configure this parameter, run the **ekahau tag-enable** command.
Ekahau erc IP-address	IP address of the Ekahau location server. To configure this parameter, run the **ekahau server** command.

Item	Description
Ekahau erc port	Port number of the Ekahau location server. To configure this parameter, run the **ekahau server** command.
Ekahau via-AC	Whether Ekahau location packets are reported to the location server through an AC. - enable: The Ekahau location packets are reported to the location server through an AC. - disable: The Ekahau location packets are not reported to the location server through an AC. To configure this parameter, run the **ekahau server** command.
Ekahau via-AC port	Port number used by an AC to report Ekahau location packets. To configure this parameter, run the **ekahau server** command.
Source IP-address	Source IP address used by an AC to report location packets. To configure this parameter, run the **source (location profile view)** command.
private mu	Whether terminal location is enabled. To configure this parameter, run the **private mu-enable** command.
private server	IP address of the terminal location server. To configure this parameter, run the **private server** command.
private server domain	Domain name of the terminal location server. To configure this parameter, run the **private server** command.
private server port	Port number of the terminal location server. To configure this parameter, run the **private server** command.

Item	Description
private via-AC	Whether terminal location packets are reported to the location server through an AC. - enable: The terminal location packets are reported to the location server through an AC. - disable: The terminal location packets are not reported to the location server through an AC. To configure this parameter, run the **private server** command.
private via-AC port	Port number used by an AC to report terminal location packets. To configure this parameter, run the **private server** command.
private report-frequency(ms)	Interval at which an AP reports terminal location packets. To configure this parameter, run the **private report-frequency** command.
private report-protocol	Protocol used by an AP to report information. To configure this parameter, run the **private report-protocol** command.
private ssl-policy name	SSL policy used when the terminal location protocol is HTTPS. To configure this parameter, run the **private report-protocol** command.
private mu protocol-version	Terminal location protocol version. To configure this parameter, run the **private mu protocol-version** command.
collect location data	Whether the device is enabled to collect wireless device location data. To configure this parameter, run the **collect-location-data enable** command.
collect location data RSSI threshold(dBm)	RSSI threshold for wireless device location data. To configure this parameter, run the **collect-location-data rssi-threshold** command.

11.10.20 display references ble-profile

Function

The **display references ble-profile** command displays reference information about a BLE profile.

Format

display references ble-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified BLE profile.	The BLE profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view reference information about a BLE profile.

Example

Display reference information about BLE profile **example**.

```
<HUAWEI> display references ble-profile name example
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
AP group                   default
------------------------------------------------------------------------
Total: 1
```

Table 11-201 Description of the **display references ble-profile** command output

Item	Description
Reference type	Type of the profile that references a BLE profile.
Reference name	Name of the profile that references a BLE profile.

11.10.21 display wlan ble global configuration

Function

The **display wlan ble global configuration** command displays global configurations of Bluetooth devices.

Format

display wlan ble global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view global configurations of Bluetooth devices and know the configuration about the Bluetooth device information report function.

Example

Display global configurations of Bluetooth devices.

```
<HUAWEI> display wlan ble global configuration
--------------------------------------------------------------------------------
BLE report interval(min)       :10
BLE low power threshold(%)     :20
BLE source IP address          :0.0.0.0
--------------------------------------------------------------------------------
```

Table 11-202 Description of the **display wlan ble global configuration** command output

Item	Description
BLE report interval(min)	Interval at which an AP reports Bluetooth device information.
BLE low power threshold(%)	Low power alarm threshold of Bluetooth devices.
BLE source IP address	A global source IP address in packets sent by an AC to a location server.

11.10.22 display wlan ble monitoring-list

Function

The **display wlan ble monitoring-list** command displays the BLE device monitoring list.

Format

display wlan ble monitoring-list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **ble monitoring-list mac** command to add BLE devices to the monitoring list, you can run the **display wlan ble monitoring-list** command to check BLE devices in the monitoring list.

If you run the **ble monitoring-list all** command to monitor all BLE devices, you can run the **display wlan ble monitoring-list** command to check BLE devices scanned by APs.

Example

Display the BLE device monitoring list.

```
<HUAWEI> display wlan ble monitoring-list
--------------------------------------------------------------------------------
Index        MAC
--------------------------------------------------------------------------------
0           00e0-fc34-0000
1           00e0-fc34-7777
--------------------------------------------------------------------------------
Total: 2
```

Table 11-203 Description of the **display wlan ble monitoring-list** command output

Item	Description
Index	Index.
MAC	MAC address of a BLE device.

11.10.23 display wlan ble site-info

Function

The **display wlan ble site-info** command displays information about Bluetooth devices that are scanned by an AP's built-in Bluetooth module.

Format

display wlan ble site-info { **all** | **mac-address** *mac-address* | **host-ap** { **valid** | **host-ap-id** *ap-id* | **host-ap-name** *ap-name* } }

Parameters

Parameter	Description	Value
all	Displays information about all Bluetooth devices.	-
mac-address *mac-address*	Displays information about a specified Bluetooth device.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
host-ap valid	Displays information about APs' built-in Bluetooth modules among all Bluetooth device information.	-
host-ap host-ap-id *ap-id*	Displays information about the Bluetooth module built in an AP with the specified ID.	The AP ID must exist.
host-ap host-ap-name *ap-name*	Displays information about the Bluetooth module built in an AP with the specified name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you enable the Bluetooth monitoring function using the **sniffer enable** command, an AP's built-in Bluetooth module scans surrounding Bluetooth devices and obtains their information. You can then run this command to view obtained information about Bluetooth devices scanned by the built-in Bluetooth module.

After the Bluetooth broadcast function is enabled for an AP with the built-in Bluetooth module, the Bluetooth module works as a Bluetooth station, whose information can be found in Bluetooth device information. If the Bluetooth MAC address label of an AP is lost, it is time-consuming to locate the mapping between the AP and built-in Bluetooth module. In this case, configure the **host-ap** parameter to filter out information about the AP's built-in Bluetooth module among all Bluetooth device information.

Example

Display information about all Bluetooth devices.

```
<HUAWEI> display wlan ble site-info all
------------------------------------------------------------------------------------------------------------------------------------------
---------------------
Index  MAC            Host AP ID Host AP name RSSI  Power Type       DetachedFlag Aging-Timeout(m)
Broadcast count Advertisement data
------------------------------------------------------------------------------------------------------------------------------------------
---------------------
0      0000-0101-0202  4         AP4          -30   50%   asset-tag  N          57              10
02-02-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-fa
------------------------------------------------------------------------------------------------------------------------------------------
---------------------
Total: 1
```

Table 11-204 Description of the **display wlan ble site-info** command output

Item	Description
Index	Index.
MAC	MAC address of a Bluetooth device.
Host AP ID	ID of the AP to which a Bluetooth device belongs. The display of **--** indicates that Bluetooth device information does not belong to the built-in Bluetooth module of the AP.
Host AP name	Name of the AP to which a Bluetooth device belongs. The display of **--** indicates that Bluetooth device information does not belong to the built-in Bluetooth module of the AP.
RSSI	Signal strength of a Bluetooth device received by an AP's built-in Bluetooth module.
Power	Battery power of a Bluetooth device. If no information about battery power is obtained, this item is displayed as **--**.

Item	Description
Type	Bluetooth device type. The options are as follows: - ibeacon: Bluetooth terminal - asset-tag: Bluetooth tag - sensor-tag: Bluetooth client
DetachedFlag	Whether a Bluetooth device is disconnected. The options are as follows: - Y: The Bluetooth device is disconnected. - N: The Bluetooth device is connected. **NOTE** Bluetooth device disconnection check is not supported in Bluetooth monitoring or transparent transmission mode. This parameter is valid only when the Bluetooth device type is **asset-tag**.
Aging-Timeout(m)	Remaining aging time of a Bluetooth device. The maximum value is 60 minutes.
Broadcast count	Number of broadcast packets sent by a Bluetooth device.
Advertisement data	Content of data carried in a broadcast frame sent by a Bluetooth device. The maximum length of a displayed broadcast frame is 21 bytes.

11.10.24 display wlan location config-info aeroscout

Function

The **display wlan location config-info aeroscout** command displays configurations delivered to APs from the AeroScout location server.

Format

display wlan location config-info aeroscout { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays the LBS configuration of the AP with a specified AP ID.	The AP ID must already exist.
ap-name *ap-name*	Displays the LBS configuration of the AP with a specified AP name.	The AP name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check configurations delivered to APs from the AeroScout location server.

Prerequisites

The AeroScout location function has been enabled using the **aeroscout tag-enable** or **aeroscout mu-enable** command, the AC has been enabled to forward location packets of AeroScout tags and MUs reported by APs to the AeroScout location server, and the AeroScout location server has delivered configuration information to the APs.

If the prerequisites are not met, for example, APs directly report packets of AeroScout tags and MUs to the AeroScout location server, a hyphen (-) is displayed after this command is run.

Example

Display AeroScout location configuration on the AP named **ap_4**.

```
<HUAWEI> display wlan location config-info aeroscout ap-name ap_4
----------------------------------------------------------------------
AP ID                            : 4
AP name                          : ap_4
AP MAC address                   : 00e0-fc54-5a80
Response IP address              : 10.3.3.3
Response port                    : 1144
AP tag mode                      : start
AP MU mode                       : start
Dilution factor                  : 100
Dilution timeout(s)              : 5
Tags multicast address           : 010c-cc00-0000
Compounded message timeout(0.1s) : 12
```

Table 11-205 Description of the **display wlan location config-info aeroscout** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
AP MAC address	AP's MAC address.
Response IP address	IP address of the location server used to receive the Response packets from the AP.
Response port	Port number used by APs to report location information.
AP tag mode	Tag detection status on the AP: ● start: The AP starts tag detection. ● stop: The AP stops tag detection. **NOTE** **AP tag mode** is displayed as **start** only when **aeroscout tag-enable** is configured on the AC and tag location is configured on the AeroScout location server.
AP MU mode	MU detection status on the AP: ● start: The AP starts MU detection. ● stop: The AP stops MU detection. **NOTE** **AP MU mode** is displayed as **start** only when **aeroscout mu-enable** is configured on the AC and MU location is configured on the AeroScout location server.
Dilution factor	Count-based packet dilution. For example, the value 100 indicates that one out of 100 packets is reported.
Dilution timeout(s)	Time-based packet dilution. For example, the value 1 indicates that at least one packet is reported every second.
Tags multicast address	Multicast MAC address of the tag.
Compounded message timeout(0.1s)	Maximum time during which the AP caches tag, in the unit of 100 milliseconds.

11.10.25 display wlan location device-info tag

Function

The **display wlan location device-info tag** command displays tag location information about APs.

Format

display wlan location device-info tag { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
all	Displays tag location information about all APs.	-
ap-id *ap-id*	Displays tag location information about a specified AP ID.	The AP ID must exist.
ap-name *ap-name*	Displays tag location information about a specified AP name.	The AP name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view tag location information about APs, facilitating tag location statistics collection.

Example

Display tag location information about all APs.

```
<HUAWEI> display wlan location device-info tag all
AP ID   AP name     Tag type        Tag MAC          Channel     RSSI
------------------------------------------------------------------------------
0       ap1         AeroScout       00e0-fc76-e360    11          -50
1       ap3         Ekahau         00e0-fc76-e380    11          -50
------------------------------------------------------------------------------
Total: 2
```

Table 11-206 Description of the display wlan location device-info tag command output

Item	Description
AP ID	AP ID.
AP name	AP name.
Tag type	Type of the tag. The value is of the enumerated type. ● Ekahau: Ekahau tag ● AeroScout: AeroScout tag
Tag MAC	MAC address of the located tag.
Channel	Working channel of the located tag.
RSSI	RSSI of the located tag, in dBm.

11.10.26 display wlan location global configuration

Function

The **display wlan location global configuration** command displays global configurations of Wi-Fi location.

Format

display wlan location global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view global configurations of Wi-Fi location to learn about the configuration of reporting Wi-Fi location information.

Example

Display global configurations of Wi-Fi location.

```
<HUAWEI> display wlan location global configuration
------------------------------------------------------------------------------
Location source IP address     :0.0.0.0
Aeroscout local IP address     :-
------------------------------------------------------------------------------
```

Table 11-207 Description of the **display wlan location global configuration** command output

Item	Description
Location source IP address	Source IP address in location packets forwarded by the AC to the location server.
Aeroscout local IP address	Local IP address used by the AC to receive packets from the location server.

11.10.27 ekahau server

Function

The **ekahau server** command sets the destination IP address and port number for APs to report Ekahau tag location packets.

The **undo ekahau server** command deletes the configured destination IP address and port number for APs to report Ekahau tag location packets.

By default, no destination IP address or port number is configured for APs to report Ekahau tag location packets.

Format

ekahau server ip-address *ip-address* **port** *port-num* [**via-ac ac-port** *ac-port-num*]

undo ekahau server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of the Ekahau location server.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port-num*	Specifies the destination port number on the Ekahau location server to which APs directly report Ekahau tag location packets. Specifies the destination port number on the Ekahau location server to which APs report Ekahau tag location packets through an AC.	The value is an integer that ranges from 1025 to 65535.
via-ac	Specifies that the Ekahau tag location packets received by APs are reported to the Ekahau location server through an AC.	-
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report Ekahau tag location packets.	The value is an integer that ranges from 1025 to 65535.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Ekahau tag location packets received by APs can be reported to the Ekahau location server directly or through an AC.

Precautions

You cannot configure a port number that has been occupied by other services; otherwise, the port configuration fails.

For the same location method, via-ac can be configured only in one profile. If **via-ac** has been specified in the current location profile for a specific location method, it cannot be specified in other profiles for the same location method.

Example

Set the destination IP address and port number on the location server to which APs report Ekahau tag location packets to **192.168.1.2** and **8569**, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] ekahau server ip-address 192.168.1.2 port 8569
```

11.10.28 ekahau tag-enable

Function

The **ekahau tag-enable** command enables WLAN location of Ekahau tags.

The **undo ekahau tag-enable** command disables WLAN location of Ekahau tags.

By default, WLAN location of Ekahau tags is disabled.

Format

ekahau tag-enable

undo ekahau tag-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ekahau tag-enable** command to enable WLAN location of Ekahau tags.

Example

Enable WLAN location of Ekahau tags.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] ekahau tag-enable
```

11.10.29 location source

Function

The **location source** command configures a global source IP address in packets sent by an AC to a location server.

The **undo location source** command deletes a global source IP address from packets sent by an AC to a location server.

By default, the source IP address is not configured in packets sent by an AC to a location server.

Format

location source ip-address *ip-address*

undo location source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies a source IPv4 address in packets sent by an AC to a location server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **location source** command to configure a source IP address in UDP packets sent by an AC to a location server.

Run the **location source** command to configure different source IP addresses for the active and standby ACs.

When source IP addresses are configured on an AC using the **location source** and **source** commands at the same time, the source IP address configured using the **source** command takes effect.

Precautions

- Ensure that the AC IP address manually configured on the location server is the same as that configured using the **location source** command.
- The source IP address must exist on the AC; otherwise, the configuration does not take effect.
- The source IP address in packets sent by an AC to a location server can be a global source IP address in the WLAN view and the source IP address in the location profile. The source IP address in the location profile takes precedence over the global source IP address in the WLAN view. If the source IP address in packets sent by an AC to a location server is not configured or the source IP address version is different from the IP address version of the location server, the AC's default IP address used for communicating with the location server is used as the source IP address.

Example

Configure 10.102.25.23 as the source IP address of the UDP packets sent from the AC to the location server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location source ip-address 10.102.25.23
```

11.10.30 location-profile

Function

The **location-profile** command binds a location profile to an AP radio.

The **undo location-profile** command unbinds a location profile from an AP radio.

By default, no location profile is bound to a radio.

Format

location-profile *profile-name* **radio** { *radio-id* | **all** }

undo location-profile radio { *radio-id* | **all** }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a location profile.	The location profile name must already exist.

Parameter	Description	Value
radio *radio-id*	Specifies the ID of the radio to which the location profile is bound.	The value is an integer that ranges from 0 to 2. Three radios are available only on the following models: ● AirEngine 8760-X1-PRO, AirEngine 8760R-X1E, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 5760-51 ● AirEngine 6761-21T, AirEngine 6761S-21T, AirEngine 6761-22T ● AirEngine 8771-X1T
all	Binds the location profile to all radios.	-

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to bind a location profile to an AP group radio or AP radio. After the binding, the parameters of the location profile will be applied to the AP group radio or AP radio.

Example

Bind the location profile **default** to radio 0 of the AP group **ap-group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] location-profile default radio 0
```

11.10.31 location-profile (WLAN view)

Function

The **location-profile** command creates a location profile or displays the location profile view.

The **undo location-profile** command deletes a location profile.

By default, no location profile is created.

Format

location-profile name *profile-name*

undo location-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a location profile, which uniquely identifies a location profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all location profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

This command creates or deletes a location profile, or displays the location profile view in which you can configure the profile. If the specified profile name does not exist, the command creates a location profile and displays the view of this location profile, and all parameters in the location profile use default values. You can also change values of these parameters.

Example

Create the location profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name test
[HUAWEI-wlan-location-prof-test]
```

11.10.32 private mu protocol-version

Function

The **private mu protocol-version** command sets the terminal location protocol version.

The **undo private mu protocol-version** command restores the default terminal location protocol version.

The default terminal location protocol version is v3.

Format

private mu protocol-version { **v3** | **v5** }

undo private mu protocol-version

Parameters

Parameter	Description	Value
v3	Sets the protocol version to v3.	-
v5	Sets the protocol version to v5.	-

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the terminal location protocol version is v5, APs report more information to the location server, such as the timestamp (the time when APs scan STAs). The location server obtains the information to improve location accuracy.

Precautions

The terminal location protocol version must be the supported by the location server.

Example

Set the terminal location protocol version to v5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private mu protocol-version v5
```

11.10.33 private mu-enable

Function

The **private mu-enable** command enables terminal location of APs.

The **undo private mu-enable** command disables terminal location of APs.

By default, terminal location of APs is disabled.

Format

private mu-enable

undo private mu-enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **private mu-enable** command to enable terminal location of APs.

Example

Enable terminal location of APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private mu-enable
```

11.10.34 private report-frequency

Function

The **private report-frequency** command sets the interval at which an AP reports channel scan information.

The **undo private report-frequency** command restores the default interval at which an AP reports channel scan information.

By default, an AP reports channel scan information every 20000 ms.

Format

private report-frequency *time*

undo private report-frequency

Parameters

Parameter	Description	Value
time	Specifies the interval at which an AP reports channel scan information.	The value is an integer that ranges from 500 ms to 60000 ms.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

During terminal location, an AP periodically scans channels to collect data. The collected data is buffered and updated on the AP, then reported to the location server at specified intervals.

Example

Set the interval at which an AP reports channel scan information to 30000 ms.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private report-frequency 30000
```

11.10.35 private report-protocol

Function

The **private report-protocol** command sets a protocol type for APs to report information.

The **undo private report-protocol** command restores the default protocol type used by APs to report information.

By default, an AP uses UDP to reports information.

Format

private report-protocol { **udp** | **http** | **https ssl-policy** *ssl-policy* }

undo private report-protocol

Parameters

Parameter	Description	Value
udp	Sets the protocol type to UDP.	-
http	Sets the protocol type to HTTP.	-
https	Sets the protocol type to HTTPS.	-
ssl-policy *ssl-policy*	Specifies the name of an SSL policy.	The value is a string of 1 to 31 case-sensitive characters without spaces or question marks (**?**).

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If APs are used to report location data to a server, the protocol type can be set only to UDP.

If location data is reported to a server through the AC, the protocol type can be set to HTTP or UDP. If higher security is required, HTTPS is applicable.

Prerequisites

When the protocol type is set to HTTPS, an SSL policy must have been created and the AP has been configured to report terminal location information through an AC.

Example

Set the protocol type to HTTP for APs to report information.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private report-protocol http
```

Set the protocol type to HTTPS for APs to report information.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private report-protocol https ssl-policy policy1
```

11.10.36 private server

Function

The **private server** command configures the destination IP address and port number for APs to report STA location data.

The **undo private server** command restores the default destination IP address and port number for APs to report STA location data.

By default, no destination IP address or port number is configured for APs to report STA location data.

Format

private server { **ip-address** *ip-address* | **domain** *domain* } **port** *port-num* [**via-ac ac-port** *ac-port-num*]

undo private server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the server's IPv4 address to which APs report STA location data.	The value is in dotted decimal notation.
domain *domain*	Specifies the domain name to which APs report STA location data.	The value is a string of 1 to 255 characters.
port *port-num*	Specifies the destination port number on the location server to which APs directly report terminal location data. Specifies the destination port number on the location server to which APs report terminal location data through an AC.	The value is an integer that ranges from 1 to 65535.
via-ac	Indicates that STA location data is reported to the location server through an AC	-

Parameter	Description	Value
ac-port *ac-port-num*	Specifies the destination port number on the AC to which APs report STA location data.	The value is an integer that ranges from 5000 to 65535.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP completes channel scan, the AP can report the collected data to the location server in the following two methods.

- The AP directly reports the data to the location server.
- The AP reports the data to the location server through an AC.

When the AP and the location server are located on different LANs, the AP must report the data to the AC first. The AC must identify information about authorized and unauthorized STAs based on the location data and report the information to the location server.

If the route between the AP and location server is reachable, and the AC is not required to identify information about authorized and unauthorized STAs, configure the AP to send data to the location server directly, preventing adverse impact of the location function on AC performance and WLAN services.

Precautions

You cannot configure a port number that has been occupied by other services; otherwise, the port configuration fails.

For the same location method, via-ac can be configured only in one profile. If **via-ac** has been specified in the current location profile for a specific location method, it cannot be specified in other profiles for the same location method.

To set the protocol type to HTTP for APs to report information, specify **via-ac ac-port** *ac-port-num* in the command. If the UDP protocol is used and the domain name is specified, the parameter **via-ac ac-port** *ac-port-num* cannot be configured.

Example

Configure APs to report STA location data directly to the location server, and set the server's IP address and port number to **192.168.1.2** and **32180**, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] private server ip-address 192.168.1.2 port 32180
```

11.10.37 report enable

Function

The **report enable** command enables APs to send Bluetooth packets.

The **undo report enable** command disables APs from sending Bluetooth packets.

By default, an AP is disabled from sending Bluetooth packets.

Format

report enable

undo report enable

Parameters

None

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the Bluetooth tag location or Bluetooth data transparent transmission function is configured on an AP, run this command to enable the AP to send the Bluetooth packets to a location server or an AC.

Example

Enable APs to send Bluetooth packets.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] report enable
```

11.10.38 report-mode

Function

The **report-mode** command sets the mode and interval for APs to send Bluetooth packets.

The **undo report-mode** command cancels the configured mode and interval for APs to send Bluetooth packets.

By default, an AP sends Bluetooth packets at an interval of 10 seconds.

Format

report-mode { **immediate** | **periodic** [**interval** *interval*] }

undo report-mode

Parameters

Parameter	Description	Value
immediate	Enables APs to send Bluetooth packets immediately.	-
periodic	Enables APs to send Bluetooth packets periodically.	-
interval *interval*	Specifies an interval at which Bluetooth packets are sent.	The value is an integer that ranges from 1 to 600, in seconds.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP is enabled to report Bluetooth packet information, the AP reports Bluetooth packet information to the AC or location server. When APs are enabled to send Bluetooth packets immediately, the location accuracy is high but AP performance may be affected. When APs are enabled to send Bluetooth packets periodically, the location accuracy is low but AP performance is not affected.

Precautions

When APs are enabled to send Bluetooth packets periodically, set a proper interval at which Bluetooth packets are sent. Otherwise, location results may be inaccurate.

Example

Enable APs to send Bluetooth packets immediately.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] report-mode immediate
```

11.10.39 report-to-server

Function

The **report-to-server** command configures the destination server and port number to which APs report Bluetooth packets.

The **undo report-to-server** command restores the default destination server and port number to which APs report Bluetooth packets.

By default, no destination IP address or port number is configured for APs to report Bluetooth packets.

Format

report-to-server ip-address *ip-address* **port** *port-num* [**via-ac ac-port** *ac-port-num*]

report-to-server domain *domain* **port** *port-num*

undo report-to-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of the location server to which APs report Bluetooth packets.	The value is in dotted decimal notation.
domain *domain*	Specifies the domain name of the location server to which APs report Bluetooth packets.	The value is a string of 1 to 255 characters.
port *port-num*	Specifies the destination UDP port number on the location server to which APs directly report Bluetooth packets. Specifies the destination UDP port number on the location server to which APs report Bluetooth packets through an AC.	The value is an integer that ranges from 1 to 65535.
via-ac	Specifies that Bluetooth packets are reported to a location server through an AC.	-

Parameter	Description	Value
ac-port *ac-port-num*	Specifies the destination UDP port number on the AC to which APs report Bluetooth packets.	The value is an integer that ranges from 5000 to 65535.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Bluetooth function is enabled, APs need to report collected Bluetooth data to a server. APs report the data using either of the following two methods:

- Reporting the data directly to the server
- Reporting the data to the server through an AC

Precautions

When configuring a port number, ensure that the port is not occupied by other services. If the port is occupied by other services, the port fails to be created.

For the same Bluetooth location function, Bluetooth data reporting through an AC can be configured only in one BLE profile. If Bluetooth data reporting through an AC has been configured in the current BLE profile for a Bluetooth location mode, the forwarding mode cannot be configured in other BLE profiles for the same Bluetooth location function.

Example

Enable APs to report Bluetooth packets to the server with destination IP address **192.168.1.2** and port number **8569**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] report-to-server ip-address 192.168.1.2 port 8569
```

11.10.40 reset wlan ble site-info

Function

The **reset wlan ble site-info** command deletes information about BLE devices stored on an AC.

Format

reset wlan ble site-info { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all BLE devices.	-
mac-address *mac-address*	Deletes information about the BLE device with the specified MAC address from the device list on the AC.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the remaining aging time of BLE devices is long and some BLE devices are not in the current WLAN coverage area, but entries on the AC still exist, you can run this command to delete information about these BLE devices.

Precautions

Deleted information about BLE devices cannot be recovered. If the aging time of a BLE device is zero, information about the BLE device is automatically deleted from the device list on the AC.

Example

Delete information about all BLE devices from the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] reset wlan ble site-info all
```

11.10.41 reset wlan location device-info tag

Function

The **reset wlan location device-info tag** command clears tag information received by APs on the AC.

Format

reset wlan location device-info tag { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
all	Clears tag information received by all APs.	-
ap-id *ap-id*	Clears tag information received by a specified AP ID.	The AP ID must exist.
ap-name *ap-name*	Clears tag information received by a specified AP name.	The AP name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

When tag information is too much, you can run this command to clear tag information received by APs on the AC. Cleared information cannot be recovered.

Example

Clear tag information received by all APs.

```
<HUAWEI> reset wlan location device-info tag all
```

11.10.42 sniffer enable

Function

The **sniffer enable** command enables and configures the working mode of an AP's built-in Bluetooth module.

The **undo sniffer enable** command disables the Bluetooth function of an AP's built-in Bluetooth module.

By default, the Bluetooth function of an AP's built-in Bluetooth module is disabled.

Format

sniffer enable { **ibeacon-mode** | **tag-mode** | **transparent-mode** }

undo sniffer enable

Parameters

Parameter	Description	Value
ibeacon-mode	Enables the Bluetooth monitoring function of an AP's built-in Bluetooth module.	-
tag-mode	Enables the Bluetooth tag location function of an AP's built-in Bluetooth module.	-
transparent-mode	Enables the Bluetooth data transparent transmission function of an AP's built-in Bluetooth module.	-

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Bluetooth monitoring or Bluetooth tag location function is enabled, the built-in Bluetooth module of an AP will scan and obtain information about surrounding BLE devices or Bluetooth tags. The built-in Bluetooth module then reports the obtained information such as MAC addresses, RSSIs, BLE broadcast frame contents, and battery power.

After the Bluetooth monitoring function is enabled, an AP obtains battery power information about surrounding BLE devices at WLAN service off-peak hours, for example, from 2:00 a.m. to 2:30 a.m. (system time), and then reports the obtained information to the AC. Precisely configure the system time of an AC to ensure that WLAN services are not affected when the AC obtains battery power of BLE devices.

After the Bluetooth data transparent transmission function is enabled, the built-in Bluetooth module of an AP scans surrounding Bluetooth clients, and reports information about the scanned Bluetooth clients, such as packet data, MAC addresses, and RSSIs. For BLE devices or Bluetooth terminals of some vendors, scan response frames can carry battery power information. The Bluetooth module also supports the query for battery level information. An AP periodically (at 2:00 am of the system time) sends scan request frames to surrounding BLE devices or Bluetooth terminals. After receiving the scan request frames, the BLE devices or Bluetooth terminals send scan response frames carrying battery power information. After receiving the scan response frames, the AP transparently transmits the frames to the AC or server.

The Bluetooth broadcast and Bluetooth monitoring functions can be enabled simultaneously for an AP's built-in Bluetooth module. When the two functions are both enabled, the AP's built-in Bluetooth module is also monitored.

After you run the **undo sniffer enable** command to disable the BLE monitoring or Bluetooth tag location function, the AC will trigger an alarm indicating that BLE devices or Bluetooth tags are offline.

Precautions

Enabling both the Bluetooth scanning and broadcast functions of an AP affects the efficiency for the AP's Bluetooth module to scan surrounding BLE devices. When an AP does not serve as a Bluetooth base station, it is recommended that the broadcast function of the AP be disabled.

Example

Enable the Bluetooth monitoring function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] sniffer enable ibeacon-mode
Warning: Modifying the monitoring mode may cause BLE devices in the original monitoring mode to go
offline and age.
```

11.10.43 source (location profile view)

Function

The **source** command sets the source IP address used by the AC to send packets to a location server.

The **undo source** command deletes the configured source IP address.

By default, the source IP address used by the AC to send packets to a location server is not configured.

Format

source ip-address *ip-address*

undo source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the source IPv4 address used by the AC to send packets to a location server.	The value is in dotted decimal notation.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source IP address used by the AC to send packets to a location server is configured using the **source** command, the UDP packet sent from the AC to a location server carries this IP address as its source IP address.

Precautions

- Ensure that the AC IP address manually configured on a location server is the same as that configured using the **source** command.
- The source IP address must be a valid IP address existing on the device; otherwise, the configuration does not take effect.
- The source IP address in packets sent by an AC to a location server can be a global source IP address in the WLAN view and the source IP address in the location profile. The source IP address in the location profile takes precedence over the global source IP address in the WLAN view. If the source IP address in packets sent by an AC to a location server is not configured or the source IP address version is different from the IP address version of the location server, the AC's default IP address used for communicating with the location server is used as the source IP address.

Example

Configure the source IP address of the UDP packets sent from the AC to a location server as 10.102.25.23.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name example
[HUAWEI-wlan-location-prof-example] source ip-address 10.102.25.23
```

11.10.44 source (BLE profile view)

Function

The **source** command sets the source IP address used by the AC to send packets to a location server.

The **undo source** command deletes the configured source IP address.

By default, the source IP address used by the AC to send packets to a location server is not configured, and the IP address of the route outbound interface is used as the source IP address.

Format

source ip-address *ip-address*

undo source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the source IPv4 address used by the AC to send packets to a location server.	The value is in dotted decimal notation.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Bluetooth location scenarios, after the source IP address used by the AC to send packets to a location server is configured using the **source** command, the packet sent from the AC to a location server carries this IP address as its source IP address.

Precautions

- Ensure that the AC IP address manually configured on a location server is the same as that configured using the **source** command.
- The source IP address must be a valid IP address existing on the device; otherwise, the configuration does not take effect.
- When the **source (BLE profile view)** and **ble source** commands are both executed, the function configured using the **source (BLE profile view)** command takes effect.

Example

Configure the source IP address of UDP packets sent from the AC to a location server as 10.102.25.23.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] source ip-address 10.102.25.23
```

11.10.45 tx-power (BLE profile view)

Function

The **tx-power** command configures the transmit power of an AP's built-in Bluetooth module.

The **undo tx-power** command restores the default transmit power of an AP's built-in Bluetooth module.

The default transmit power of an AP's built-in Bluetooth module is 0 dBm.

Format

tx-power *tx-power-value*

undo tx-power

Parameters

Parameter	Description	Value
tx-power-value	Specifies the transmit power of an AP's built-in Bluetooth module.	The value is of the enumerated type. The options are –21, –18, –15, –12, –9, –6, –3, 0, 1, 2, 3, 4, and 5, in dBm.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to change the transmit power of an AP's built-in Bluetooth module. Increasing the transmit power can improve Bluetooth signal transmission quality but causes more severe interference to other wireless devices. Reducing the transmit power can reduce interference to other wireless devices but affects Bluetooth signal transmission quality. Configure the transmit power of an AP's built-in Bluetooth module properly based on site requirements.

Precautions

After changing the transmit power of an AP's built-in Bluetooth module, you need to run the **broadcasting-content** command to reconfigure the RSSI calibration value in BLE broadcast frames.

Example

Set the transmit power of an AP's built-in Bluetooth module to 2 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ble-profile name example
[HUAWEI-wlan-ble-prof-example] tx-power 2
```

11.11 WLAN Security Configuration Commands

11.11.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.11.2 anti-attack flood blacklist enable

Function

The **anti-attack flood blacklist enable** command enables the flood blacklist function.

The **undo anti-attack flood blacklist enable** command disables the flood blacklist function.

By default, the flood blacklist function is disabled.

Format

anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **blacklist enable**

undo anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **blacklist enable**

Parameters

Parameter	Description	Value
arp	Indicates whether to enable the ARP flood blacklist function.	-
dhcp	Indicates whether to enable the DHCP flood blacklist function.	-
dhcpv6	Indicates whether to enable the DHCPv6 flood blacklist function.	-
igmp	Indicates whether to enable the IGMP flood blacklist function.	-
mdns	Indicates whether to enable the mDNS flood blacklist function.	-

Parameter	Description	Value
nd	Indicates whether to enable the ND flood blacklist function.	-
other-broadcast	Indicates whether to enable the flood blacklist function for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Indicates whether to enable the flood blacklist function for multicast packets other than IGMP and mDNS packets.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the protocol-based flood blacklist function is enabled, the device considers traffic of a specified protocol (such as DHCP or ARP) with a rate higher than that specified in **anti-attack flood sta-rate-threshold** a flood attack and adds the STA to the blacklist.

Prerequisites

The flood prevention function has been enabled using the **undo anti-attack flood disable** command.

Example

Enable the DHCP flood blacklist function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-wlan-vap-prof-profile1] anti-attack flood dhcp blacklist enable
```

11.11.3 anti-attack flood disable

Function

The **anti-attack flood disable** disables the flood prevention function.

The **undo anti-attack flood disable** command enables the flood prevention function.

By default, the flood prevention function is enabled.

Format

anti-attack flood { **all** | **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **disable**

undo anti-attack flood { **all** | **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **disable**

Parameters

Parameter	Description	Value
all	Indicates whether to enable the flood prevention function for ARP, DHCP, DHCPv6, IGMP, mDNS, and ND multicast, broadcast, and unicast packets.	-
arp	Indicates whether to enable the ARP flood prevention function.	-
dhcp	Indicates whether to enable the DHCP flood prevention function.	-
dhcpv6	Indicates whether to enable the DHCPv6 flood prevention function.	-
igmp	Indicates whether to enable the IGMP flood prevention function.	-
mdns	Indicates whether to enable the mDNS flood prevention function.	-
nd	Indicates whether to enable the ND flood prevention function.	-

Parameter	Description	Value
other-broadcast	Indicates whether to enable the flood prevention function for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Indicates whether to enable the flood prevention function for multicast packets other than IGMP and mDNS packets.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a large number of packets are sent to a device in a short time, the device becomes busy processing the packets and cannot process normal services. To prevent flood attacks, you can configure protocol-based flood prevention.

Precautions

The flood prevention function takes effect only for incoming traffic on an AP's wired interface.

Example

Disable the DHCP flood prevention function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-vap-prof-profile1] anti-attack flood dhcp disable
```

11.11.4 anti-attack flood sta-rate-threshold

Function

The **anti-attack flood sta-rate-threshold** command sets the flood threshold.

The **undo anti-attack flood sta-rate-threshold** command restores the default flood threshold.

The default flood threshold is 4 pps for ARP, DHCP, DHCPv6, IGMP, and mDNS packets, 8 pps for ND packets, 10 pps for broadcast packets other than ARP, DHCP, DHCPv6, and ND packets, and 10 pps for multicast packets other than IGMP and mDNS packets.

Format

anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **sta-rate-threshold** *sta-rate-threshold*

undo anti-attack flood { **arp** | **dhcp** | **dhcpv6** | **igmp** | **mdns** | **nd** | **other-broadcast** | **other-multicast** } **sta-rate-threshold**

Parameters

Parameter	Description	Value
arp	Specifies ARP packets.	-
dhcp	Specifies DHCP packets.	-
dhcpv6	Specifies DHCPv6 packets.	-
igmp	Specifies IGMP packets.	-
mdns	Specifies mDNS packets.	-
nd	Specifies ND packets.	-
other-broadcast	Specifies broadcast packets other than ARP, DHCP, DHCPv6, and ND packets.	-
other-multicast	Specifies multicast packets other than IGMP and mDNS packets.	-
sta-rate-threshold	Specifies the rate threshold of broadcast traffic from STAs.	For **arp**, **dhcp**, **dhcpv6**, and **nd**, the value is an integer that ranges from 1 to 5000, in pps. For **igmp**, **mdns**, **other-broadcast**, and **other-multicast**, the value is an integer that ranges from 0 to 5000, in pps.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the flood prevention function is enabled, you can run this command to set the broadcast traffic threshold.

When the traffic rate exceeds the threshold, the device considers a flood attack from the STA and discards the traffic. This prevents the upper-layer network from being affected by the flood.

If the flood blacklist function is enabled using the **anti-attack flood blacklist enable** command, the device adds flood STAs to the blacklist.

Prerequisites

The flood prevention function has been enabled using the **undo anti-attack flood disable** command.

Precautions

The flood prevention function takes effect only for incoming traffic on an AP's wired interface.

Example

Set the DHCP flood threshold to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name profile1
[HUAWEI-vap-prof-profile1] anti-attack flood dhcp sta-rate-threshold 100
```

11.11.5 arp anti-attack check user-bind enable

Function

The **arp anti-attack check user-bind enable** command enables dynamic ARP inspection (DAI).

The **undo arp anti-attack check user-bind enable** command disables DAI.

By default, DAI is disabled.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

DAI allows an AP to detect the ARP Request and Reply packets transmitted on the VAPs of the AP, to discard invalid and attack ARP packets, and to send an alarm to the connected AC. This function prevents ARP packets of unauthorized users from accessing the external network through the AP, protecting authorized users against interference or spoofing, and protecting the AP.

- Invalid ARP packets: The source IP and MAC addresses of ARP Request and Reply packets do not match.
- Attack ARP packets: When an AP receives a large number of consecutive ARP packets and the number of ARP packets exceeds the ARP attack alarm threshold, an ARP attack occurs.

Example

Enable DAI.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] arp anti-attack check user-bind enable
```

11.11.6 attack-device trap enable

Function

The **attack-device trap enable** command enables the alarm function for attack detection.

The **undo attack-device trap enable** command disables the alarm function for attack detection.

By default, the alarm function for attack detection is disabled.

Format

attack-device trap enable

undo attack-device trap enable

Parameters

None

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is executed, an alarm is triggered immediately when the device detects an attack.

Prerequisites

The attack detection function has been enabled by using the **wids attack detect** command.

Precautions

If a large number of attack devices exist, enabling this function will trigger a large number of alarms and generate a large number of logs. Therefore, you are advised to use this function together with a log server.

Example

Enable the alarm function for attack detection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] attack-device trap enable
```

11.11.7 brute-force-detect interval

Function

The **brute-force-detect interval** command sets the interval for brute force key cracking detection.

The **undo brute-force-detect interval** command restores the default interval for brute force key cracking detection.

By default, the interval for brute force key cracking detection is 60 seconds.

Format

brute-force-detect interval *interval*

undo brute-force-detect interval

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for brute force key cracking detection.	The value is an integer that ranges from 10 to 120, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a brute force key cracking attack, an attacker tries all possible key combinations one by one to obtain the correct password. To improve password security, enable defense against brute force key cracking to prolong the time used to crack passwords.

An AP checks whether the number of key negotiation failures during WPA/WPA2-PSK, WAPI-PSK, or WEP-Share-Key authentication of a user exceeds the threshold configured using the **brute-force-detect threshold** command. If so, the AP considers that the user is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets from the user until the dynamic blacklist entry ages out.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the interval for brute force key cracking detection to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] brute-force-detect interval 100
```

11.11.8 brute-force-detect quiet-time

Function

The **brute-force-detect quiet-time** command sets the quiet time for an AP to report brute force key attacks to an AC.

The **undo brute-force-detect quiet-time** command restores the default quiet time for an AP to report brute force key attacks to an AC.

By default, the quiet time for an AP to report brute force key attacks to an AC is 600 seconds.

Format

brute-force-detect quiet-time *quiet-time-value*

undo brute-force-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report brute force key attacks to an AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time function for attack detection. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the quiet time for an AP to report brute force key attacks to an AC to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] brute-force-detect quiet-time 300
```

11.11.9 brute-force-detect threshold

Function

The **brute-force-detect threshold** command sets the maximum number of key negotiation failures allowed within a brute force key cracking attack detection period.

The **undo brute-force-detect threshold** command restores the default maximum number of key negotiation failures allowed within a brute force key cracking attack detection period.

By default, an AP allows a maximum of 20 key negotiation failures within a brute force key cracking attack detection period.

Format

brute-force-detect threshold *threshold*

undo brute-force-detect threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the number of key negotiation failures within a detection period.	The value is an integer that ranges from 1 to 100.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a brute force key cracking attack, an attacker tries all possible key combinations one by one to obtain the correct password. To improve password security, enable defense against brute force key cracking to prolong the time used to crack passwords.

An AP checks whether the number of key negotiation failures during WPA/WPA2-PSK, WAPI-PSK, or WEP-Share-Key authentication of a user exceeds the threshold configured using the **brute-force-detect threshold** command. If so, the AP considers that the user is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets from the user until the dynamic blacklist entry ages out. If the threshold is set to a small value, the AP may incorrectly add authorized users to the dynamic blacklist, causing the users unable to go online.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the maximum number of key negotiation failures allowed within a brute force key cracking attack detection period to 60.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] brute-force-detect threshold 60
```

11.11.10 contain

Function

The **contain** command enables containment of rogue and interfering devices based on the RSSI and number of associated STAs on the devices.

The **undo contain** command disables containment of rogue and interfering devices based on the RSSI and number of associated STAs on the devices.

By default, containment of rogue and interfering devices based on the RSSI and number of associated STAs on the devices is disabled.

Format

contain { **min-rssi** *min-rssi* | **min-sta-num** *min-sta-num* }

undo contain { **min-rssi** | **min-sta-num** }

Parameters

Parameter	Description	Value
min-rssi *min-rssi*	Specifies the minimum RSSI value.	The value is an integer that ranges from -95 to -50.
min-sta-num *min-sta-num*	Specifies the minimum number of associated STAs.	The value is an integer that ranges from 1 to 10.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After RSSI-based containment is enabled, if the RSSIs of detected rogue and interfering devices are no more than the specified minimum RSSI value, the devices are not contained. They are contained only when their RSSIs exceed the specified minimum RSSI value.

After containment based on the number of associated STAs is enabled, if the number of STAs associated with detected rogue and interfering devices is smaller than the specified minimum value, the devices are not contained. They are contained only when the number of STAs associated with them reaches the specified minimum value.

Prerequisites

Detection and containment of rogue and interfering devices have been enabled.

Precautions

This function is not supported in manual containment mode.

Example

Enable containment of rogue and interfering APs with spoofing SSIDs and set the number of associated STAs that triggers containment to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids contain enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
```

```
[HUAWEI-wlan-wids-prof-default] contain-mode spoof-ssid-ap
[HUAWEI-wlan-wids-prof-default] contain min-sta-num 5
```

11.11.11 contain-mode

Function

The **contain-mode** command sets the containment mode against rogue or interference devices.

The **undo contain-mode** command deletes the containment mode against rogue or interference devices.

By default, no containment mode against rogue or interference devices is set.

Format

contain-mode { **open-ap** | **spoof-ssid-ap** | **client** [**protect sta-whitelist-profile** *profile-name*] | **adhoc** }

undo contain-mode { **open-ap** | **spoof-ssid-ap** | **client** [**protect**] | **adhoc** }

Parameters

Parameter	Description	Value
open-ap	Sets the containment mode against open-authentication rogue or interference APs.	-
spoof-ssid-ap	Sets the containment mode against rogue or interference APs using spoofing SSIDs.	-
client	Sets the containment mode against unauthorized STAs or interference STAs.	-
protect sta-whitelist-profile *profile-name*	Protects STAs based on the STA whitelist. Authorized STAs in the whitelist are protected from connecting to rogue or interference APs.	-
adhoc	Sets the containment mode against Ad-hoc devices.	-

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Rogue or interference devices pose serious security threats to enterprise networks.

After the containment mode is set against rogue or interference APs, the monitor AP uses the identity of the rogue or interference AP to broadcast deauthentication frames to forcibly disconnect STAs. To prevent the STAs from connecting to the rogue or interference AP again, the monitor AP will periodically and continuously send deauthentication frames.

After the containment mode is set against rogue STAs, interference STAs or Ad-hoc devices, the monitor AP uses the MAC address of a rogue device to continuously send unicast deauthentication frames.

Example

Counter rogue and interference APs with spoofing SSIDs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids contain enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] contain-mode spoof-ssid-ap
```

11.11.12 device report-interval

Function

The **device report-interval** command sets the interval at which an AP reports incremental wireless device information.

The **undo device report-interval** command restores the default interval at which an AP reports incremental wireless device information.

By default, an AP reports incremental wireless device information to an AC at an interval of 300 seconds.

Format

device report-interval *interval*

undo device report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an AP reports incremental wireless device information.	The value is an integer that ranges from 60 to 3600, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The monitoring AP buffers information about detected wireless devices at the interval set using the **device report-interval** command. When the interval is reached, the monitoring AP reports the information to the AC and then clears the reported information.

Prerequisites

The device detection function has been enabled using the **wids device detect enable** command for the AP.

Example

Set the interval at which an AP reports incremental wireless device information to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids device detect enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] device report-interval 120
```

11.11.13 dhcp trust port

Function

The **dhcp trust port** command configures a DHCP trusted interface on an AP.

The **undo dhcp trust port** command cancels the configuration.

By default, the DHCP trusted interface is enabled on the AP's uplink interface in the AP wired port profile view.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before WLAN services are delivered to an AP, run the **dhcp trust port** command in the AP wired port profile view. After the command is run, the AP receives the DHCP OFFER, ACK, and NAK packets sent by the authorized DHCP server and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

The **undo dhcp trust port** command configured in the AP wired port profile view takes effect only in direct forwarding mode, but not in tunnel forwarding mode.

Precautions

When executed in the AP wired port view, this command takes effect only on uplink interfaces of an AP. To configure a downlink wired interface on an AP as a DHCP trusted interface, you only need to run the **learn-client-address enable (AP wired port profile view)** command to enable STA address learning, but do not need to run the **dhcp trust port** command.

Example

Create an AP wired port profile named **wire1**, and enable a DHCP trusted interface on an AP in this profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wire1
[HUAWEI-wlan-wired-port-wire1] dhcp trust port
```

11.11.14 display ap radio-environment

Function

The **display ap radio-environment** command displays air interface environment information about AP radios.

Format

display ap radio-environment { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays air interface environment information about radios of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays air interface environment information about radios of the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays air interface environment information about the AP radio with a specified ID.	The radio ID must exist.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When WLAN access experience is poor, you can run this command to view air interface environment information and Wi-Fi interference sources. The interference can be determined based on the noise floor, signal to interference plus noise ratio (SINR), co-channel interference, and adjacent-channel interference. After this command is executed, radio scanning of the AP is automatically enabled, and the AP starts to scan the air interface environment of radios. You can run this command again to view air interface environment scanning results.

Precautions

When you run this command for the first time, no air interface environment scanning result is displayed. To view air interface environment scanning results, run this command again.

After AP radio scanning is enabled using this command, the air interface performance of an AP is affected. If this command is not executed again after five minutes, AP radio scanning is automatically disabled.

If the **radio** *radio-id* parameter is not specified, air interface environment information about all radios of the AP is displayed.

NOTE

In the scanning result, the channel utilization, co-channel interference, and adjacent-channel interference are calculated with the impact of non-Wi-Fi interference. However, non-Wi-Fi interference devices are not displayed in the interference source list.

Example

Display air interface environment information about radio 0 of AP 1.

```
<HUAWEI> display ap radio-environment ap-id 1 radio 0
Warning: This operation will enable scanning for the specified radio, affecting AP's air interface
performance. Scanning will be automatically disabled 5 minutes after this command is run. Continue? [Y/
N]y
Info: This operation may take a few seconds. Please wait for a moment.done.
p:            permit
i:           interference
Ch:           Channel
CU:           Channel Utility
NF:           Noise Floor
CommIf:       Common-Channel Interference
AdjaceIf:     Adjacent-Channel Interference
SINR:         Signal to Interference and Noise Ratio
#Neighbors:   Number of Neighbors detected
Radio:        0
ScanChannel:  1
WorkChannel:  1
ScanCycle:    1
---------------------------------------------------------------------------
Ch  NF   CU(%) CommIf(%) AdjaceIf(%) SINR      #Neighbors
---------------------------------------------------------------------------
1   -105 75    19        -           245       57
---------------------------------------------------------------------------
Total: 1
---------------------------------------------------------------------------
Ch    MAC           Type  RSSI  SSID
---------------------------------------------------------------------------
1     00e0-fc3a-8d41 i     -65   xw9-2g-tunnel
------------------------------------------------
Total: 1
```

Table 11-208 Description of the **display ap radio-environment** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] command output

Item	Description
Radio	Radio on which the air interface environment is scanned.
ScanChannel	Scanning channel.
WorkChannel	Working channel of the AP.
ScanCycle	Scanning count.
Ch	Channel that has scanned a device.
NF	Noise floor.
CU(%)	Channel utilization.
CommIf(%)	Co-channel interference.
AdjaceIf(%)	Adjacent-channel interference.
#Neighbors	Number of scanned radio neighbors.
SINR	Signal to interference plus noise ratio (SINR).

Item	Description
MAC	MAC address of the scanned device.
Type	Type of the scanned interference device. ● i: WIDS device ● p: Non-WIDS device
RSSI	RSSI of the scanned device.
SSID	SSID to which the scanned device is connected.

NOTE

If an AP detects that a channel has a high co-channel interference (higher than 50%), another Wi-Fi device is using this channel and affects the local AP. In this case, it is recommended that the AP channel be switched using radio calibration or other methods.

11.11.15 display references wids-whitelist-profile

Function

The **display references wids-whitelist-profile** command displays reference information about a WIDS whitelist profile.

Format

display references wids-whitelist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS whitelist profile.	The WIDS whitelist profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-whitelist-profile** command to view reference information about a WIDS whitelist profile.

Example

Display reference information about the WIDS whitelist profile **default**.

```
<HUAWEI> display references wids-whitelist-profile name default
------------------------------------------------------------
Profile type                  Reference name
------------------------------------------------------------
wids-profile                  default
------------------------------------------------------------
Total: 1
```

Table 11-209 Description of the **display references wids-whitelist-profile** command output

Item	Description
Profile type	Type of the profile that references the WIDS whitelist profile.
Reference name	Name of the profile that references the WIDS whitelist profile.

11.11.16 display references wids-profile

Function

The **display references wids-profile** command displays reference information about a WIDS profile.

Format

display references wids-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS profile.	The WIDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-profile** command to view reference information about a WIDS profile.

Example

Display reference information about the WIDS profile **default**.

```
<HUAWEI> display references wids-profile name default
------------------------------------------------------------------------
Reference type              Reference name
------------------------------------------------------------------------
AP group                   default
------------------------------------------------------------------------
Total: 1
```

Table 11-210 Description of the **display references wids-profile** command output

Item	Description
Reference type	Type of the object that references the WIDS profile.
Reference name	Name of the object that references the WIDS profile.

11.11.17 display references wids-spoof-profile

Function

The **display references wids-spoof-profile** command displays reference information about a WIDS spoof SSID profile.

Format

display references wids-spoof-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-spoof-profile** command to view reference information about a WIDS spoof SSID profile.

Example

Display reference information about the WIDS spoof SSID profile **default**.

```
<HUAWEI> display references wids-spoof-profile name default
Profile type                   Reference name
-------------------------------------------------------------
wids-profile                   default
-------------------------------------------------------------
Total: 1
```

Table 11-211 Description of the **display references wids-spoof-profile** command output

Item	Description
Profile type	Type of the profile that references the WIDS spoof SSID profile.
Reference name	Name of the profile that references the WIDS spoof SSID profile.

11.11.18 display wids-whitelist-profile

Function

The **display wids-whitelist-profile** command displays information about a WIDS whitelist profile.

Format

display wids-whitelist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS whitelist profiles.	-
name *profile-name*	Displays information about a specified WIDS whitelist profile.	The WIDS whitelist profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-whitelist-profile** command to view information about a WIDS whitelist profile.

Example

Display information about all WIDS whitelist profiles.

```
<HUAWEI> display wids-whitelist-profile all
------------------------------------------------------------
Profile name                  Reference
------------------------------------------------------------
default                        1
------------------------------------------------------------
Total: 1
```

Table 11-212 Description of the **display wids-whitelist-profile all** command output

Item	Description
Profile name	Specifies the name of a WIDS whitelist profile.
Reference	Number of times a WIDS whitelist profile is referenced.

Display information about the WIDS whitelist profile **default**.

```
<HUAWEI> display wids-whitelist-profile name default
------------------------------------------------------------
Permit AP OUI SSID match : both
------------------------------------------------------------
Type          Content
```

```
------------------------------------------------------------
MAC           00e0-fc12-3456
OUI           00-e0-fc
SSID          example
------------------------------------------------------------
Total: 3
```

Table 11-213 Description of the **display wids-whitelist-profile name** command output

Item	Description
Permit AP OUI SSID match	Rules for matching OUIs and SSIDs in the WIDS whitelist: - both: Both OUIs and SSIDs can be matched. - any: Either of OUIs and SSIDs can be matched. The default value is **both**. To set the rule, run the **permit-ap oui-ssid-match** command.
Type	Type of authorized APs.
Content	Rule for authorized APs. To set the rule, run the **permit-ap** command.

11.11.19 display wids-profile

Function

The **display wids-profile** command displays information about a WIDS profile.

Format

display wids-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS profiles.	-
name *profile-name*	Displays information about a specified WIDS profile.	The WIDS profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-profile** command to view information about a WIDS profile.

Example

Display information about all WIDS profiles.

```
<HUAWEI> display wids-profile all
------------------------------------------------------------
Profile name                   Reference
------------------------------------------------------------
default                         1
------------------------------------------------------------
Total: 1
```

Table 11-214 Description of the **display wids-profile all** command output

Item	Description
Profile name	Name of a WIDS profile.
Reference	Number of times a WIDS profile is referenced.

Display information about the WIDS profile **default**.

```
<HUAWEI> display wids-profile name default
------------------------------------------------------------
Device report interval(s)            : 60
Brute force detect interval(s)       : 20
Brute force detect threshold         : 20
Brute force quiet time(s)            : 600
Flood detect interval(s)             : 10
Flood detect threshold               : 1
Flood quiet time(s)                  : 600
Weak IV quiet time(s)                : 600
Spoof quiet time(s)                  : 600
Dynamic blacklist                    : enable
Contain rogue mode                   : spoof SSID AP
                                       open-authentication rogue AP
                                       client
                                       client protect
                                       Ad hoc
Contain minimum RSSI(dBm)            : -
Contain minimum sta number           : -
Attack device trap switch            : disable
STA whitelist profile                : STA_whitelist
WIDS spoof profile                   : default
WIDS whitelist profile               : default
------------------------------------------------------------
```

Table 11-215 Description of the **display wids-profile name** command output

Item	Description
Device report interval(s)	Interval at which an AP reports the detected incremental wireless device information. To configure this parameter, run the **device report-interval** command.
Brute force detect interval(s)	Interval for brute force key cracking detection. To configure this parameter, run the **brute-force-detect interval** command.
Brute force detect threshold	Maximum number of key negotiation failures allowed within a brute force key cracking detection period. To configure this parameter, run the **brute-force-detect threshold** command.
Brute force quiet time(s)	Quiet time for an AP to report the detected brute force attacks to the AC. To configure this parameter, run the **brute-force-detect quiet-time** command.
Flood detect interval(s)	Flood attack detection interval. To configure this parameter, run the **flood-detect interval** command.
Flood detect threshold	Flood attack detection threshold. To configure this parameter, run the **flood-detect threshold** command.
Flood quiet time(s)	Quiet time for an AP to report the detected flood attacks to the AC. To configure this parameter, run the **flood-detect quiet-time** command.
Weak IV quiet time(s)	Quiet time for an AP to report the detected weak IV attacks to the AC. To configure this parameter, run the **weak-iv-detect quiet-time** command.
Spoof quiet time(s)	Quiet time for an AP to report the detected spoofing attacks to the AC. To configure this parameter, run the **spoof-detect quiet-time** command.

Item	Description
Dynamic blacklist	Whether the dynamic blacklist function is enabled. To configure this parameter, run the **dynamic-blacklist disable** command.
Contain rogue mode	Containment mode against rogue devices. To configure this parameter, run the **contain-mode** command.
Contain minimum RSSI(dBm)	Minimum RSSI value for containing rogue and interfering devices based on the RSSI of the devices. To configure this parameter, run the **contain** command.
Contain minimum sta number	Minimum number of associated STAs for containing rogue and interfering devices based on the number of STAs associated with the devices. To configure this parameter, run the **contain** command.
Attack device trap switch	Whether the alarm function for attack detection is enabled. To configure this parameter, run the **attack-device trap enable** command.
STA whitelist profile	STA protection based on a STA whitelist. To configure this parameter, run the **contain-mode** command.
WIDS spoof profile	WIDS spoof SSID profile bound to the WIDS profile. To configure this parameter, run the **wids-spoof-profile (WIDS profile view)** command.
WIDS whitelist profile	WIDS whitelist profile bound to the WIDS profile. To configure this parameter, run the **wids-whitelist-profile (WIDS profile view)** command.

11.11.20 display wids-spoof-profile

Function

The **display wids-spoof-profile** command displays information about a WIDS spoof SSID profile.

Format

display wids-spoof-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS spoof SSID profiles.	-
name *profile-name*	Displays information about a specified WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-spoof-profile** command to view information about a WIDS spoof SSID profile.

Example

Display information about all WIDS spoof SSID profiles.

```
<HUAWEI> display wids-spoof-profile all
------------------------------------------------------------
Profile name                  Reference
------------------------------------------------------------
default                        1
------------------------------------------------------------
Total: 1
```

Table 11-216 Description of the **display wids-spoof-profile all** command output

Item	Description
Profile name	Name of a WIDS spoof SSID profile.

Item	Description
Reference	Number of times a WIDS spoof SSID profile is referenced.

Display information about the WIDS spoof SSID profile **default**.

```
<HUAWEI> display wids-spoof-profile name default
------------------------------------------------------------
ID      Pattern rule
------------------------------------------------------------
0       ^HUAWE[1l]$
------------------------------------------------------------
Total: 1
```

Table 11-217 Description of the **display wids-spoof-profile name** command output

Item	Description
ID	Index.
Pattern rule	Matching rule for spoofing SSIDs. To set the matching rule, run the **spoof-ssid** command.

11.11.21 display references security-profile

Function

The **display references security-profile** command displays reference information about a security profile.

Format

display references security-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified security profile.	The security profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a security profile.

Example

Display reference information about the security profile **security-profile1**.

```
<HUAWEI> display references security-profile name security-profile1
--------------------------------------------
Reference type          Reference name
--------------------------------------------
VAP profile             vap-profile1
--------------------------------------------
Total: 1
```

Table 11-218 Description of the **display references security-profile** command output

Item	Description
Reference type	Type of the profile that references a security profile.
Reference name	Name of the profile that references a security profile.

11.11.22 display references sta-blacklist-profile

Function

The **display references sta-blacklist-profile** command displays reference information about a STA blacklist profile.

Format

display references sta-blacklist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a STA blacklist profile.	The STA blacklist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a STA blacklist profile.

Example

Display reference information about the STA blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> display references sta-blacklist-profile name sta-blacklist-profile1
--------------------------------------------
Reference type          Reference name
--------------------------------------------
VAP profile             vap-profile1
--------------------------------------------
Total: 1
```

Table 11-219 Description of the **display references sta-blacklist-profile** command output

Item	Description
Reference type	Type of the profile that references the STA blacklist profile.
Reference name	Name of the profile that references the STA blacklist profile.

11.11.23 display references sta-whitelist-profile

Function

The **display references sta-whitelist-profile** command displays reference information about a STA whitelist profile.

Format

display references sta-whitelist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a STA whitelist profile.	The STA whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a STA whitelist profile.

Example

Display reference information about the STA whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> display references sta-whitelist-profile name sta-whitelist-profile1
--------------------------------------------
Reference type          Reference name
--------------------------------------------
VAP profile             vap-profile1
--------------------------------------------
Total: 1
```

Table 11-220 Description of the **display references sta-whitelist-profile** command output

Item	Description
Reference type	Type of the profile that references the STA whitelist profile.
Reference name	Name of the profile that references the STA whitelist profile.

11.11.24 display security-profile

Function

The **display security-profile** command displays configuration and reference information about a security profile.

Format

display security-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all security profiles.	-
name *profile-name*	Displays information about a specified security profile.	The security profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view configuration and reference information about a specified security profile or all security profiles.

Example

Display information about all security profiles.

```
<HUAWEI> display security-profile all
----------------------------------------------------------
Profile name                  Reference
----------------------------------------------------------
default                   1
default-wds                 1
default-mesh                 1
security-profile1            0
----------------------------------------------------------
Total: 4
```

Table 11-221 Description of the **display security-profile all** command output

Item	Description
Profile name	Name of the security profile.
Reference	Number of times a security profile is referenced.

Display information about the security profile **default**.

```
<HUAWEI> display security-profile name default
------------------------------------------------------------
Security policy              : Open system
Encryption                   : -
------------------------------------------------------------
WEP's configuration
```

```
Key 0                   : *****
Key 1                   : *****
Key 2                   : *****
Key 3                   : *****
Default key ID          : 0
------------------------------------------------------------
WPA/WPA2's configuration
PTK update              : disable
PTK update interval(s)        : 43200
------------------------------------------------------------
WAPI's configuration
CA certificate filename       : -
ASU certificate filename      : -
AC certificate filename       : -
AC private key filename       : -
AC local key pair name        : -
WAPI source interface         : -
Authentication server IP      : -
WAI timeout(s)                : 60
BK update interval(s)         : 43200
BK lifetime threshold(%)      : 70
USK update method             : Time-based
USK update interval(s)        : 86400
MSK update method             : Time-based
MSK update interval(s)        : 86400
Cert auth retrans count       : 3
USK negotiate retrans count   : 3
MSK negotiate retrans count   : 3
------------------------------------------------------------
```

Table 11-222 Description of the **display security-profile name** command output

Item	Description
Security policy	Security policy. The following security policies are supported: - Open system: WEP open system authentication - Share key: WEP shared key authentication - WEP 802.1x: Dynamic WEP - WPA 802.1x: WPA-802.1X - WPA2 802.1x: WPA2-802.1X - WPA-WPA2 802.1x: WPA-WPA2-802.1X - WPA PSK - WPA2 PSK - WPA-WPA2 PSK - WPA PPSK - WPA2 PPSK - WPA-WPA2 PPSK - WPA3 SAE - WPA3 802.1x: WPA3-802.1X - WPA2-WPA3 PSK-SAE - WPA2-WPA3 802.1x: WPA2-WPA3-802.1X - WAPI PSK - WAPI certificate - OWE - WPA2 RPSK - -: No security policy To configure this parameter, run the **security wep**, **security dot1x**, **security psk**, **security wpa2-wpa3 psk-sae**, **security wpa3 sae**, **security wpa3 dot1x**, **security enhanced-open aes**, or **security wapi** command.

Item	Description
Encryption	Encryption mode. The following encryption modes are supported: GCMP-256, TKIP, AES, AES-TKIP, WEP-40, WEP-104, WEP-128, and SMS4. The WAPI encryption mode is fixed to SMS4, the hybrid WPA3-SAE +WPA2-WPA3 encryption mode is fixed to AES, and the WPA3-802.1X encryption mode is fixed to GCMP-256 + AES, and the OWE encryption mode is fixed to AES. To configure this parameter, run the **wep key**, **security dot1x**, **security wpa2-wpa3 psk-sae**, **security wpa3 sae**, **security wpa3 dot1x**, **security enhanced-open aes**, **security wpa2-wpa3 dot1x**, or **security psk** command.
PMF	Whether the Protected Management Frame (PMF) function of a VAP is enabled. ● **disable**: This function is disabled. ● **optional**: This function is enabled in optional mode. ● **mandatory**: This function is forcibly enabled. This line is displayed in the command output only when the authentication and encryption mode is WPA2-AES/WPA3/OWE. To configure this parameter when the authentication mode is WPA2-AES, run the **pmf** command. When the authentication mode is WPA3, this parameter is unconfigurable. The value of this parameter is fixed at **mandatory** when the authentication mode is WPA3-SAE or WPA3-802.1X and **optional** when the authentication mode is WPA2-WPA3. When the authentication mode is OWE or its transition mode, the value of this parameter is fixed at **mandatory**.
Key *key-id*	Key ID. To configure this parameter, run the **wep key** command.

Item	Description
Default key ID	Default key ID. To configure this parameter, run the **wep default-key** command.
PTK update	Whether to enable periodic PTK update in WPA, WPA2, or WPA-WPA2 authentication and encryption. ● enable: This function is enabled. ● disable: This function is disabled. To configure this parameter, run the **wpa ptk-update enable** command.
PTK update interval(s)	The interval for updating PTKs in WPA, WPA2, or WPA-WPA2 authentication and encryption. The value is an integer in seconds. To configure this parameter, run the **wpa ptk-update ptk-update-interval** command.
CA certificate filename	CA certificate file name. To configure this parameter, run the **wapi import certificate** command.
ASU certificate filename	File name of the authentication server unit (ASU) certificate. To configure this parameter, run the **wapi import certificate** command.
AC certificate filename	AC certificate file name. To configure this parameter, run the **wapi import certificate** command.
AC private key filename	AC private key file name. To configure this parameter, run the **wapi import private-key** command.
AC local key pair name	Name of the local ECC key pair on the AC. To configure this parameter, run the **wapi import private-key** command.
WAPI source interface	WAPI source interface. To configure this parameter, run the **wapi source interface** command.
Authentication server IP	IP address of the ASU certificate server. To configure this parameter, run the **wapi asu** command.

Item	Description
WAI timeout(s)	Timeout period of an association. To configure this parameter, run the **wapi sa-timeout** command.
BK update interval(s)	Interval for updating the base key (BK). To configure this parameter, run the **wapi bk** command.
BK lifetime threshold(%)	Threshold for triggering BK update. To configure this parameter, run the **wapi bk** command.
USK update method	Whether the USK is updated based on a time interval or a packet count. To configure this parameter, run the **wapi key-update** command.
USK update interval(s)	Interval for updating the unicast session key (USK). To configure this parameter, run the **wapi usk** command.
MSK update method	Whether the MSK is updated based on a time interval or a packet count. To configure this parameter, run the **wapi key-update** command.
MSK update interval(s)	Interval for updating the MBMS service key (MSK). To configure this parameter, run the **wapi msk** command.
Cert auth retrans count	Number of retransmissions of certificate authentication packets. To configure this parameter, run the **wapi cert-retrans-count** command.
USK negotiate retrans count	Number of retransmissions of USK negotiation packets. To configure this parameter, run the **wapi usk** command.
MSK negotiate retrans count	Number of retransmissions of MSK negotiation packets. To configure this parameter, run the **wapi msk** command.

11.11.25 display sta-blacklist-profile

Function

The **display sta-blacklist-profile** command displays configuration and reference information about a STA blacklist profile.

Format

display sta-blacklist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all STA blacklist profiles.	-
name *profile-name*	Displays information about a specified STA blacklist profile.	The STA blacklist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring STA blacklists on a device, you can run this command to check whether a MAC address is in the blacklists.

Example

Display reference information about all STA blacklist profiles.

```
<HUAWEI> display sta-blacklist-profile all
------------------------------------------------------------
Profile name                          Reference
------------------------------------------------------------
sta-blacklist-profile1                 1
------------------------------------------------------------
Total: 1
```

Table 11-223 Description of the **display sta-blacklist-profile all** command output

Item	Description
Profile name	Name of a STA blacklist profile.

Item	Description
Reference	Number of times a STA blacklist profile is referenced.

Display information about the STA blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> display sta-blacklist-profile name sta-blacklist-profile1
-------------------------------------------------------------
Index      MAC               Description
-------------------------------------------------------------
0          00e0-fc11-2222
-------------------------------------------------------------
Total: 1
```

Table 11-224 Description of the **display sta-blacklist-profile name** command output

Item	Description
Index	Blacklist index.
MAC	MAC address of a STA in the blacklist. To configure the parameter, run the **sta-mac** command.
Description	Description of a MAC address in the blacklist.

11.11.26 display station dynamic-blacklist

Function

The **display station dynamic-blacklist** command displays the dynamic blacklist on an AP.

Format

display station dynamic-blacklist { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays information about STAs that are denied access on the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-name *ap-name*	Displays information about STAs that are denied access on the AP with a specified name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a STA dynamic blacklist on an AP. The blacklist helps control access of STAs, for example, forbidding STAs with bogus IP addresses to go online. If a STA is not allowed to go online, the STA is added to the dynamic blacklist. Before the dynamic blacklist entry ages out, the STA cannot associate with the AP. After the aging time of a dynamic blacklist entry is reached, the dynamic blacklist entry is automatically deleted. During this period, if the STA on an entry is added to the blacklist again, the aging time of the entry is updated and recalculated.

The administrator can run this command to check STAs in the blacklist and the reasons for adding the STAs to the blacklist.

Example

Display the dynamic blacklist on AP.

```
<HUAWEI> display station dynamic-blacklist ap-name example
Total: 1
------------------------------------------------------------------------------
STA MAC          Time left(s)   Reason
------------------------------------------------------------------------------
00e0-fc12-3456    160           WIDS attack
------------------------------------------------------------------------------
```

Table 11-225 Description of the **display station dynamic-blacklist** command output

Item	Description
STA MAC	MAC address of a STA.
Time left(s)	Remaining aging period, in seconds. To configure the parameter, run the **dynamic-blacklist aging-time** command.

Item	Description
Reason	Reason why a STA is added to the dynamic blacklist. ● static IP: The AP is configured to deny access of STAs with bogus IP addresses, and the STA has a static IP address configured. ● ARP flood: The AP is configured to detect and defend against ARP flood attacks, and the STA initiates an ARP flood attack. ● IGMP flood: The AP is configured to detect and defend against IGMP flood attacks, and the STA initiates an IGMP flood attack. ● ND flood: The AP is configured to detect and defend against ND flood attacks, and the STA initiates an ND flood attack. ● DHCP flood: The AP is configured to detect and defend against DHCP flood attacks, and the STA initiates a DHCP flood attack. ● DHCPv6 flood: The AP is configured to detect and defend against DHCPv6 flood attacks, and the STA initiates a DHCPv6 flood attack. ● MDNS flood: The AP is configured to detect and defend against mDNS flood attacks, and the STA initiates an mDNS flood attack. ● other multicast flood: The AP is configured to detect and defend against flood attacks through multicast packets other than IGMP, and mDNS multicast packets, and the STA initiates such an attack. ● other broadcast flood: The AP is configured to detect and defend against flood attacks through broadcast packets other than ARP, DHCP, DHCPv6, and ND multicast packets, and the STA initiates such an attack. ● WIDS attack: The AP is configured to detect attacks on a WLAN. ● MESH key fail: Key negotiation fails during mesh link setup.

Item	Description
	● other: Other reason

11.11.27 display sta-whitelist-profile

Function

The **display sta-whitelist-profile** command displays configuration and reference information about a STA whitelist profile.

Format

display sta-whitelist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all STA whitelist profiles.	-
name *profile-name*	Displays information about a specified STA whitelist profile.	The STA whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a STA whitelist on a device, you can run this command to check whether a MAC address is in the whitelist.

Example

Display reference information about all STA whitelist profiles.

```
<HUAWEI> display sta-whitelist-profile all
------------------------------------------------------------
Profile name                         Reference
------------------------------------------------------------
sta-whitelist-profile1                 1
------------------------------------------------------------
Total: 1
```

Table 11-226 Description of the **display sta-whitelist-profile all** command output

Item	Description
Profile name	Name of a STA whitelist profile.
Reference	Number of times a STA whitelist profile is referenced.

Display information about the STA whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> display sta-whitelist-profile name sta-whitelist-profile1
-------------------------------------------------------------
Index      MAC                 Description
-------------------------------------------------------------
0         00e0-fc11-2222
-------------------------------------------------------------
Total: 1
-------------------------------------------------------------
Index      OUI                 Description
-------------------------------------------------------------
0         00-00-01
-------------------------------------------------------------
Total: 1
```

Table 11-227 Description of the **display sta-whitelist-profile name** command output

Item	Description
Index	Whitelist index.
MAC	MAC address of a STA in the whitelist. To configure the parameter, run the **sta-mac** command.
OUI	OUI of a STA in the whitelist. To configure the parameter, run the **oui** command.
Description	Description of a MAC address in the whitelist.

11.11.28 display wlan ids attack-detected

Function

The **display wlan ids attack-detected** command displays information about the detected attacking devices.

Format

display wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all types of attacking devices.	-
flood	Displays information about devices launching flood attacks.	-
spoof	Displays information about devices launching spoofing attacks.	-
wapi-psk	Displays information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays information about devices launching weak IV attacks.	-
wep-share-key	Displays information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays information about the detected attacking devices with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run this command to view information about the attacking devices.

Prerequisites

The attack detection functions of all types have been enabled using the **wids attack detect enable** command.

Example

Display information about all current attacking devices.

```
<HUAWEI> display wlan ids attack-detected all
#AP: Number of monitor APs that have detected the device
AT: Last detected attack type
CH: Channel number
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
-------------------------------------------------------------------------------
MAC address     AT    CH   RSSI(dBm)  Last detected time     #AP
-------------------------------------------------------------------------------
00e0-fc02-9c81  pbr    165  -87        2014-11-20/15:51:13    1
00e0-fc76-03e9  pbr    165  -84        2014-11-20/15:52:13    1
00e0-fc74-691f  act    165  -67        2014-11-20/15:43:33    1
00e0-fcb7-171d  pbr    165  -88        2014-11-20/15:41:43    1
00e0-fcb7-171f  act    165  -87        2014-11-20/15:44:03    1
-------------------------------------------------------------------------------
Total: 5, printed: 5
```

Table 11-228 Description of the **display wlan ids attack-detected all** command output

Item	Description
MAC address	● For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. ● For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of the attack type.
CH	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Last detected time	Last time at which an attack was detected.

Item	Description
#AP	Number of APs which detect this attack.

Display information about the attacking device with a specified MAC address.

```
<HUAWEI> display wlan ids attack-detected mac-address 00e0-fc47-aad0
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
--------------------------------------------------------------------------------
MAC address                        : 00e0-fc47-aad0
Number of detected APs             : 1
Channel                            : 165
RSSI(dBm)                          : -80
Reported AP 1
  AP name                          : ap-13
  Flood attack type                : pbr
  First detected time(Flood)       : 2014-11-20/15:50:33
  Spoof attack type                : -
  First detected time(Spoof)       : -
  First detected time(Weak-iv)     : -
  First detected time(WEP)         : -
  First detected time(WPA)         : -
  First detected time(WPA2)        : -
  First detected time(WAPI)        : -
--------------------------------------------------------------------------------
```

Table 11-229 Description of the **display wlan ids attack-detected mac-address** *mac-address* command output

Item	Description
MAC address	● For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. ● For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
Number of detected APs	Number of APs which detect this attack.
Channel	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.

Item	Description
Reported AP	Information of the AP which detects the attack.
AP name	Name of the AP which detects the attack.
Flood attack type	Flood attacks detected by the AP.
Spoof attack type	Spoofing attacks detected by the AP.
First detected time	First time when an attack is detected by an AP.

11.11.29 display wlan ids attack-detected statistics

Function

The **display wlan ids attack-detected statistics** command displays the number of attacks detected.

Format

display wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run the **display wlan ids attack-detected statistics** command to view the total number of all types of attacks.

Prerequisites

The attack detection functions of all types have been enabled using the **wids attack detect enable** command.

Example

Display the number of attacks detected.

```
<HUAWEI> display wlan ids attack-detected statistics
Attack tracking since: 2015-01-27/12:02:11
--------------------------------------------------------------------------------
Type                                                          Total
--------------------------------------------------------------------------------
Probe request frame flood attack                    : 0
Authentication request frame flood attack           : 0
Deauthentication frame flood attack                 : 0
Association request frame flood attack              : 0
Disassociation request frame flood attack           : 0
Reassociation request frame flood attack            : 0
Action frame flood attack                           : 0
EAPOL start frame flood attack                      : 0
EAPOL logoff frame flood attack                     : 0
Weak IVs detected                                   : 0
Spoofed deauthentication frame attack               : 0
Spoofed disassociation frame attack                 : 0
Other types of spoofing frame attack                : 0
WEP share-key attack                                : 0
WPA attack                                          : 0
WPA2 attack                                         : 0
WAPI attack                                         : 0
--------------------------------------------------------------------------------
```

Table 11-230 Description of the **display wlan ids attack-detected statistics** command output

Item	Description
Type	Attack type: ● Probe request frame flood attack ● Authentication request frame flood attack ● Deauthentication frame flood attack ● Association request frame flood attack ● Disassociation request frame flood attack ● Reassociation request frame flood attack ● Action frame flood attack ● EAPOL start frame flood attack ● EAPOL logoff frame flood attack ● Weak IVs detected ● Spoofed deauthentication frame attack ● Spoofed disassociation frame attack ● Other types of spoofing frame attack ● WEP share-key attack: brute force cracking attack in WEP-SK authentication mode ● WPA attack: brute force cracking attack in WPA-PSK authentication mode ● WPA2 attack: brute force cracking attack in WPA2-PSK authentication mode ● WAPI attack: brute force cracking attack in WAPI authentication mode
Total	Total number of attacks detected.

11.11.30 display wlan ids attack-history

Function

The **display wlan ids attack-history** command displays historical records about the attacking devices detected.

Format

display wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays historical records about all types of attacking devices.	-
flood	Displays historical records about devices launching flood attacks.	-
spoof	Displays historical records about devices launching spoofing attacks.	-
wapi-psk	Displays historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays historical records about devices launching weak IV attacks.	-
wep-share-key	Displays historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, information about the detected attacking devices is saved in the attacking device list. If an attacking device no longer launches an attack, the device is removed from the attacking device list and saved to the historical attacking device list. You can run the **display wlan ids attack-history** command to check historical records about the attacking devices detected.

Prerequisites

The attack detection functions of all types have been enabled using the **wids attack detect enable** command.

Example

Display historical records of all attacking devices.

```
<HUAWEI> display wlan ids attack-history all
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
AP: Name of the monitor AP that has detected the device
AT: Attack type              CH: Channel number
-------------------------------------------------------------------------------
MAC address     AT     CH   RSSI(dBm)  Last detected time    AP
-------------------------------------------------------------------------------
00e0-fc12-37ec  pbr    165  -86        2014-11-20/15:51:43   ap-13
00e0-fc12-171d  pbr    165  -88        2014-11-20/15:41:43   ap-13
00e0-fc12-0bf4  pbr    165  -81        2014-11-20/15:41:53   ap-13
-------------------------------------------------------------------------------
Total: 3, printed: 3
```

Table 11-231 Description of the **display wlan ids attack-history all** command output

Item	Description
MAC address	- For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. - For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of the attack type.
CH	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Last detected time	Last time at which an attack is detected.
AP	Name of the monitor AP.

11.11.31 display wlan ids contain

Function

The **display wlan ids contain** command displays information about contained devices.

Format

display wlan ids contain { **all** | **ap** | **adhoc** | **client** | **ssid** | **mac-address** *mac-address* | **monitor-ap** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays information about all contained devices.	-
ap	Displays information about contained APs.	-
adhoc	Displays information about contained ad-hoc devices.	-
client	Displays information about contained STAs.	-
ssid	Displays information about contained SSIDs.	-
mac-address *mac-address*	Displays information about the contained device with a specified MAC address.	The MAC address must exist.
monitor-ap ap-name *ap-name*	Displays information about contained devices that are detected by the AP with a specified name.	The AP name must exist.
monitor-ap ap-id *ap-id*	Displays information about contained devices that are detected by the AP with a specified ID.	The AP ID must exist.
monitor-ap { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*	Displays information about contained devices that are detected by the radio with a specified ID on a specified AP.	The radio ID must exist on the AP.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After WIDS or WIPS is enabled, you can run this command to view information about contained devices.

Example

Display the list of all contained devices.

```
<HUAWEI> display wlan ids contain all
#Rf: Number of monitor radios that have contained the device
CH: Channel number
--------------------------------------------------------------------------------
MAC address      CH  Authentication   Last detected time   #Rf   Reason   SSID
--------------------------------------------------------------------------------
00e0-fc12-3456   11  open            2014-11-20/16:16:57  1     manual     -
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-232 Description of the **display wlan ids contain all** command output

Item	Description
MAC address	MAC address of the contained device.
CH	Channel on which the monitor AP detected the contained device for the last time.
Authentication	Authentication mode of the contained device.
Last detected time	Last time at which the monitor AP detected the contained device.
#Rf	Number of monitor radios that have contained the device.
Reason	Reason for the device to be contained. The priorities of containment reasons are in descending order as follows: manual > open-encrypt > spoof-ap > protect-client > client > adhoc.
SSID	SSID of the contained device.

Display information about contained SSIDs.

```
<HUAWEI> display wlan ids contain ssid
#Dev: Number of devices using SSID
----------------------------------------------------------------------
 SSID                            #Dev     Last detected time
----------------------------------------------------------------------
 CMCC                              2        2012-07-27/16:41:55
----------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-233 Description of the **display wlan ids contain ssid** command output

Item	Description
SSID	Contained SSID.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID was detected.

Display information about the contained device with a specified MAC address.

```
<HUAWEI> display wlan ids contain mac-address 00e0-fc12-3456
-------------------------------------------------------------------------------
MAC address                                           : 00e0-fc12-3456
BSSID                                                 : 00e0-fc12-3456
Type                                                  : rogue client
SSID                                                  : -
Authentication                                        : -
Number of monitor radios that have contained the device : 1
Last detected channel                                 : 1
Maximum RSSI(dBm)                                     : -54
Beacon interval(TUs)                                  : 0
First detected time                                   : 2015-10-20/15:06:26

Reported AP 1
 AP name                                              : admin_ap0_admin_ap0_admin
 Radio ID                                             : 0
 MAC address                                          : 00e0-fc12-3455
 Radio type                                           : 802.11bg
 Channel                                              : 1
 RSSI(dBm)                                            : -54
 Last detected time                                   : 2015-10-20/15:06:26
 Counter measure                                      : Y
 Reason                                               : manual
-------------------------------------------------------------------------------
```

Table 11-234 Description of the **display wlan ids contain mac-address** command output

Item	Description
MAC address	MAC address of the detected device.
BSSID	BSSID of the detected device.
Type	Type of the detected device.
SSID	SSID of the detected device.

Item	Description
Authentication	Authentication mode of the detected device.
Number of monitor radios that have contained the device	Number of radios that contain the device. If WIDS is enabled on multiple APs, the type of the device may be contained by these APs' radios.
Last detected channel	Channel on which the device was detected for the last time.
Maximum RSSI(dBm)	Maximum RSSI of the detected device.
Beacon interval(TUs)	Interval at which the detected device sends Beacon frames.
First detected time	First time at which the device was detected.
Reported AP 1	Information about the monitor AP which reports detection information.
AP name	Name of the monitor AP.
Radio ID	Radio ID of the monitor AP.
MAC address	MAC address of the monitor AP.
Radio type	Radio type of the monitor AP.
Channel	Channel of the monitor AP.
RSSI(dBm)	RSSI of the monitor AP.
Last detected time	Last time when the device was detected.
Counter measure	Whether the device is contained.
Reason	Reason for the device to be contained. The priorities of containment reasons are in descending order as follows: manual > open-encrypt > spoof-ap > protect-client > client > adhoc.

```
<HUAWEI> display wlan ids contain monitor-ap ap-name example
Countermeasures Device Profile
------------------------------------------------------------------------------
AP MAC address                          : 00e0-fc12-3456
AP type                                 : xxxxxxx
AP name                                 : example
Contain device 0
  MAC address                           : 00e0-fc12-3455
  BSSID                                 : 00e0-fc12-3455
  Type                                  : rogue client
```

```
  SSID                                    : -
  Authentication                          : -
  Last detected channel by this AP        : 1
  Maximum RSSI(dBm)                       : -71
  Beacon interval(TUs)                    : 0
  First detected time                     : 2015-10-20/15:06:26
  Reason                                  : manual
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-235 Description of the **display wlan ids contain monitor-ap** command output

Item	Description
AP MAC address	MAC address of the monitor AP.
AP type	Type of the monitor AP.
AP name	Name of the monitor AP.
MAC address	MAC address of the contained device.
BSSID	BSSID of the contained device.
Type	Type of the contained device.
SSID	SSID of the contained device.
Authentication	Authentication mode of the contained device.
Last detected channel by this AP	Channel on which the monitor AP detected the contained device for the last time.
Maximum RSSI(dBm)	Maximum RSSI of the contained device.
Beacon interval()	Interval at which the contained device sends Beacon frames.
First detected time	First time at which the device was detected.
Reason	Reason for the device to be contained. The priorities of containment reasons are in descending order as follows: manual > open-encrypt > spoof-ap > protect-client > client > adhoc.

11.11.32 display wlan ids device-detected

Function

The **display wlan ids device-detected** command displays various wireless devices detected on the WLAN.

Format

display wlan ids device-detected { **all** | [**interference** | **rogue**] **ap** | [**rogue**] **bridge** | [**rogue**] **client** [**bssid** *bssid*] | **adhoc** | [**rogue**] **ssid** | **mac-address** *mac-address* | **monitor-ap** { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays all wireless devices detected on the WLAN.	-
interference	Displays interfering devices detected on the WLAN.	-
rogue	Displays rogue devices detected on the WLAN.	-
ap	Displays APs detected on the WLAN.	-
bridge	Displays bridge devices detected on the WLAN.	-
client	Displays user terminals detected on the WLAN.	-
bssid *bssid*	Displays detailed information about devices with the specified BSSID detected on the WLAN.	The format is H-H-H. An H is a hexadecimal number of 4 digits.
adhoc	Displays detected user terminals that belong to the ad-hoc network on the WLAN.	-
ssid	Displays detailed information about devices with the specified SSID detected on the WLAN.	-
mac-address *mac-address*	Displays detailed information about the device with a specified MAC address detected on the WLAN.	The MAC address must exist.
monitor-ap ap-name *ap-name*	Displays detailed information about devices detected by the monitor AP with a specified name on the WLAN.	The AP name must exist.
monitor-ap ap-id *ap-id*	Displays detailed information about devices detected by the monitor AP with a specified ID on the WLAN.	The AP ID must exist.

Parameter	Description	Value
monitor-ap { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*	Displays detailed information about devices detected by the radio with a specified ID on a specified AP on the WLAN.	The radio ID must exist on the AP.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To ensure the WLAN reliability, all the wireless devices on the current WLAN must be monitored. You can run the **display wlan ids detected** command to view information about the wireless devices detected.

Prerequisites

The device detection function has been enabled on the AP using the **wids device detect enable** command.

Example

Display all wireless devices detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected all
Flags: r: rogue, p: permit, i: interference, a: adhoc, w: AP, b: wireless-bridge, c: client
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
-------------------------------------------------------------------------------------------------
MAC address     Type    CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
-------------------------------------------------------------------------------------------------
00e0-fc20-de2b  i/w     1   -60       5       open             2014-11-20/11:03:44  1     -
-------------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 11-236 Description of the **display wlan ids device-detected all** command output

Item	Description
MAC address	MAC address of the detected device.

Item	Description
Type	Type of the detected device: - r: rogue device - p: authorized device - i: interfering device - a: user terminal on the ad-hoc network - w: AP - b: bridge device - c: user terminal
CH	Channel on which the device was detected for the last time.
RSSI(dBm)	RSSI of the detected device.
StaNum	Number of STAs associated with the detected device.
Authentication	Authentication mode of the detected device.
Last detected time	Last time when the device was detected.
#Rf	Number of radios that detect the device.
SSID	SSID of the detected device.

Display information about APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected ap
Flags: r: rogue, p: permit, i: interference
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
----------------------------------------------------------------------------------------------------
MAC address     Type  CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
----------------------------------------------------------------------------------------------------
00e0-fc20-de2b  r     1   -60       5       open             2014-11-20/11:03:44  1     -
----------------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about rogue APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected rogue ap
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
----------------------------------------------------------------------------------------------------
MAC Address     CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
----------------------------------------------------------------------------------------------------
00e0-fc20-de2b  1   -60       5       open             2014-11-20/11:03:44  1     -
```

```
---------------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about interference APs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected interference ap
Flags: r: rogue, p: permit, i: interference
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
---------------------------------------------------------------------------------------------------
MAC address     Type  CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
---------------------------------------------------------------------------------------------------
00e0-fc20-de2b  i     1   -60       5       open             2014-11-20/11:03:44  1     -
---------------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about ad-hoc devices detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected adhoc
Flags: r: rogue
#Rf: Number of monitor radios that have detected the device
CH: Channel number
RSSI(dBm): Maximum RSSI of detected device
StaNum: Number of detected STAs associated with the device
---------------------------------------------------------------------------------------------------
MAC address     Type  CH  RSSI(dBm) StaNum  Authentication   Last detected time   #Rf   SSID
---------------------------------------------------------------------------------------------------
00e0-fc20-de2d  r     6   -60       -       -                2014-11-20/11:12:58  2     -
---------------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display information about SSIDs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected ssid
#Dev: Number of devices using SSID
--------------------------------------------------------------------------------
SSID                             #Dev  Last detected time
--------------------------------------------------------------------------------
trad                             1     2014-11-20/11:01:44
CMCC-4G                          6     2014-11-20/11:14:13
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 11-237 Description of the **display wlan ids device-detected ssid** command output

Item	Description
SSID	SSID detected.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID was detected.

Display information about spoofing SSIDs detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected rogue ssid
#Dev: number of devices using rogue SSID
--------------------------------------------------------------------------------
Rogue SSID  Spoof profile  #Dev  Last detected time
          Pattern rule
--------------------------------------------------------------------------------
```

```
ao          a0            1     2014-11-20/11:14:39
          ao
al         a1           2     2014-11-20/11:14:39
          al
--------------------------------------------------------------------------------
ssid        --            1     2014-11-20/15:59:45
---------------------------------------------------------------------------------
Total: 3
```

Table 11-238 Description of the **display wlan ids device-detected rogue ssid** command output

Item	Description
Rogue SSID	Spoofing SSIDs detected, including SSIDs same as the authorized SSIDs and SSIDs matching the specified fuzzy rules.
Spoof profile	WIDS spoof SSID profile owned the fuzzy matching rule.
Pattern rule	Fuzzy matching rule for the spoofing SSID.
#Dev	Number of APs using the SSID.
Last detected time	Last time when the SSID was detected.

Display detailed information about the device with the MAC address 00e0-fce9-1c00 detected on the WLAN.

```
<HUAWEI> display wlan ids device-detected mac-address 00e0-fce9-1c00
Detected MAC List
-------------------------------------------------------------------------------
MAC address                                            : 00e0-fce9-1c00
BSSID                                                  : 00e0-fce9-1c00
Type                                                   : rogue ap
SSID                                                   : -
Authentication                                         : 802.1x
Number of monitor radios that have detected the device  : 1
Last detected channel                                  : 1
Maximum RSSI(dBm)                                      : -80
Beacon interval(TUs)                                   : -
First detected time                                    : 2015-10-20/15:07:23
Reported AP 1
 AP name                                               : admin_ap0_admin_ap0_admin
 Radio ID                                              : 0
 MAC address                                           : 00e0-fc1e-c4a0
 Radio type                                            : 802.11bg
 Channel                                               : 1
 RSSI(dBm)                                             : -80
 Last detected time                                    : 2015-10-20/15:07:23
 Counter measure                                       : Y
 Counter measure reason                                : spoof-ssid-ap
-------------------------------------------------------------------------------
```

Table 11-239 Description of the **display wlan ids device-detected mac-address** command output

Item	Description
MAC address	MAC address of the detected device.
BSSID	BSSID of the detected device.
Type	Type of the detected device.
SSID	SSID of the detected device.
Authentication	Authentication mode of the detected device.
Number of monitor radios that have detected the device	Number of radios that detect the device. If WIDS is enabled on multiple APs, the type of the device may be detected by these APs' radios.
Last detected channel	Channel of the detected device.
Maximum RSSI(dBm)	Maximum RSSI of the detected device.
Beacon interval(TUs)	Interval at which the detected device sends Beacon frames.
First detected time	First time at which the device was detected.
Reported AP 1	Information about the monitor AP which reports detection information.
AP name	Name of the monitor AP.
Radio ID	Radio ID of the monitor AP.
MAC address	MAC address of the monitor AP.
Radio type	Radio type of the monitor AP.
Channel	Channel of the monitor AP.
RSSI(dBm)	RSSI of the monitor AP.
Last detected time	Last time when the device was detected.
Counter measure	Whether the device is contained.

Item	Description
Counter measure reason	Reason why the device is contained. - open-encrypt: The authentication mode of the device is open. - spoof-ssid-ap: The device is a rogue AP or interference AP with a spoofing SSID. - protect-client: The device is a STA in the STA whitelist and is contained to prevent it from accessing a rogue AP. - client: The device is a rogue STA or interference STA. - adhoc: The device is an ad-hoc device. - manual: The device is manually contained.

11.11.33 display wlan ids device-detected statistics

Function

The **display wlan ids device-detected statistics** command displays statistics on all wireless devices detected on a WLAN.

Format

display wlan ids device-detected statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan ids device-detected statistics** command to view statistics on all wireless devices detected on a WLAN.

Example

Display statistics on wireless devices detected on a WLAN.

```
<HUAWEI> display wlan ids device-detected statistics
------------------------------------------------------------------------------------------------

Rogue Adhoc          : 0
Contain Adhoc        : 0
Rogue AP             : 0
Permit AP            : 0
Interference AP      : 0
Contain AP           : 0
Rogue client         : 2
Permit client        : 0
Interference Client  : 0
Contain client       : 2
Permit Bridge        : 2
Rogue Bridge         : 0
Interference Bridge  : 0
------------------------------------------------------------------------------------------------
```

Table 11-240 Description of the **display wlan ids device-detected statistics** command output

Item	Description
Rogue Adhoc	Number of rogue ad-hoc devices.
Contain Adhoc	Number of contained ad-hoc devices.
Rogue AP	Number of rogue APs.
Permit AP	Number of authorized APs.
Interference AP	Number of interfering APs.
Contain AP	Number of contained APs.
Rogue Client	Number of rogue terminal devices.
Permit Client	Number of authorized terminal devices.
Interference Client	Number of interfering terminal devices.
Contain Client	Number of contained terminal devices.
Permit Bridge	Number of authorized bridge devices.
Rogue Bridge	Number of unauthorized bridge devices.
Interference Bridge	Number of interfering bridge devices.

11.11.34 display wlan dynamic-blacklist

Function

The **display wlan dynamic-blacklist** command displays information about devices in the dynamic blacklist.

Format

display wlan dynamic-blacklist { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all devices in the dynamic blacklist.	-
ap-id *ap-id*	Displays information about attacking devices detected by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about attacking devices detected by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Displays information about attack devices with a specified MAC address.	The MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An AP uses attack detection and dynamic blacklist functions to add a detected attack device to the dynamic blacklist, and rejects packets sent from this device until the device entry in the dynamic blacklist ages. You can run this command to view information about devices in the dynamic blacklist.

Example

Display information about all devices in the dynamic blacklist.

```
<HUAWEI> display wlan dynamic-blacklist all
#AP: Number of monitor APs that have detected the device
```

```
LAT: Left aging time(s)
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      sti: Static IP
brf: Broadcast flood
-------------------------------------------------------------------------------
MAC address       Last detected time    Reason   #AP   LAT
-------------------------------------------------------------------------------
00e0-fc12-3451    2015-07-27/12:51:25   brf       1    100
00e0-fc12-3452    2015-07-27/12:51:25   pbr       1    200
00e0-fc12-3453    2015-07-27/12:51:25   pbr       1    200
00e0-fc12-3454    2015-07-27/12:51:25   sti       1    200
00e0-fc12-3455    2015-07-27/12:51:25   pbr       1    200
00e0-fc12-3456    2015-07-27/12:51:25   pbr       1    200
-------------------------------------------------------------------------------
Total: 6, printed: 6
```

Table 11-241 Description of the **display wlan dynamic-blacklist all** command output

Item	Description
MAC address	MAC address of the device in the dynamic blacklist.
Last detected time	Latest time when the device was added to the dynamic blacklist.
Reason	Reason why the device is added to the dynamic blacklist.
#AP	Number of APs that have detected and added the device to the dynamic blacklist.
LAT	Remaining aging time for the device in the dynamic blacklist.

Display information about all devices added to the dynamic blacklist by the AP named **wcw**.

```
<HUAWEI> display wlan dynamic-blacklist ap-name wcw
LAT: Left aging time(s)
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      sti: Static IP
brf: Broadcast flood
-------------------------------------------------------------------------------
MAC address       Last detected time    Reason   LAT
-------------------------------------------------------------------------------
00e0-fc12-3451    2015-07-27/12:51:25    sti     100
00e0-fc12-3452    2015-07-27/12:51:25    brf     200
00e0-fc12-3453    2015-07-27/12:51:30    pbr     200
00e0-fc12-3454    2015-07-27/12:51:25    pbr     300
-------------------------------------------------------------------------------
Total: 4, printed: 4
```

Display information about specified devices in the dynamic blacklist.

```
<HUAWEI> display wlan dynamic-blacklist mac-address 00e0-fc12-3454
LAT: Left aging time(s)       BT: Block time(s)
act: Action frame             asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request            rar: Reassociation request
eaps: EAPOL start frame       sti: Static IP
brf: Broadcast flood
--------------------------------------------------------------
AP name  Last detected time   Reason   LAT     BT
--------------------------------------------------------------
wcw      2015-07-27/12:51:25   pbr     100     900
wcw2     2015-07-27/12:51:25   pbr     100    1900
--------------------------------------------------------------
Total: 2, printed: 2
```

Table 11-242 Description of the **display wlan dynamic-blacklist mac-address** command output

Item	Description
AP name	Name of the monitoring AP.
Last detected time	Last time when the device was detected.
Reason	Reason why the device is added to the dynamic blacklist.
LAT	Remaining aging time for the device in the dynamic blacklist.
BT	Duration for which the device is in the dynamic blacklist.

11.11.35 display wlan ids rogue-history

Function

The **display wlan ids rogue-history** command displays historical records of rogue devices.

Format

display wlan ids rogue-history { **all** | **ap** | **bridge** | **client** | **adhoc** | **ssid** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays historical records of all rogue devices.	-
ap	Displays historical records of rogue APs.	-

Parameter	Description	Value
bridge	Displays historical records of rogue bridge devices.	-
client	Displays historical records of rogue user terminals.	-
adhoc	Displays historical records of rogue ad-hoc devices.	-
ssid	Displays historical records of contained devices with unauthorized SSIDs.	-
mac-address *mac-address*	Displays historical records of devices with specified MAC addresses.	The MAC addresses must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display wlan ids rogue-history** command to view the historical records of rogue devices.

Prerequisites

The device detection function has been enabled on the AP using the **wids device detect enable** command.

Example

Display historical records of all rogue devices.

```
<HUAWEI> display wlan ids rogue-history all
Flags: a: adhoc, w: AP, b: wireless-bridge, c: client
CH: Channel number
--------------------------------------------------------------------------------
MAC address     Type  CH  Authentication   Last detected time   SSID
--------------------------------------------------------------------------------
00e0-fc12-3456  w     11  open             2014-11-20/11:20:37  wlan
00e0-fc12-3457  c     11  -                2014-11-20/11:16:07  -
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 11-243 Description of the **display wlan ids rogue-history all** command output

Item	Description
MAC address	MAC address of the rogue device listed in the historical record list.
Type	Type of the rogue device listed in the historical record list: ● a: user terminal on the ad-hoc network ● w: AP ● b: bridge device ● c: user terminal
CH	Channel in which the device is detected for the last time.
Authentication	Authentication mode of the rogue device listed in the historical record list.
Last detected time	Last time when the device is detected.
SSID	SSID of the detected device.

Display historical records of rogue APs.

```
<HUAWEI> display wlan ids rogue-history ap
CH: channel number
------------------------------------------------------------------------------
MAC address     CH  Authentication   Last detected time   SSID
------------------------------------------------------------------------------
00e0-fc12-3458  11  open             2014-11-20/11:20:37  wlan
00e0-fc12-3459  11  open             2014-11-20/11:20:44  -
------------------------------------------------------------------------------
Total: 2, printed: 2
```

Display historical records of SSIDs.

```
<HUAWEI> display wlan ids rogue-history ssid
#Dev: number of devices using SSID
------------------------------------------------------------------------------
SSID                             #Dev  Last detected time
------------------------------------------------------------------------------
trad                            1      2014-11-20/11:01:44
CMCC-4G                              6      2014-11-20/11:14:13
X+Z_007                            1      2014-11-20/11:20:15
tntjoyo                          1      2014-11-20/11:18:42
------------------------------------------------------------------------------
Total: 4, printed: 4
```

Table 11-244 Description of the **display wlan ids rogue-history ssid** command output

Item	Description
SSID	SSID of the detected device.
#Dev	Number of devices that use the SSID.
Last detected time	Last time at which the device using the SSID is detected.

Display historical records of an AP or STA with a specified MAC address.

```
<HUAWEI> display wlan ids rogue-history mac-address 00e0-fc03-0206
-------------------------------------------------------------------
 MAC address                          : 00e0-fc03-0206
 SSID                            : wlan
 Type                            : rogue ap
 Authentication                       : 802.1x
 Last detected time                    : 2012-10-25/09:22:29
-------------------------------------------------------------------
```

Table 11-245 Description of the **display wlan ids rogue-history mac-address** command output

Item	Description
MAC address	MAC address of the detected device.
Type	Type of the detected device.
SSID	SSID of an ESS.
Authentication	Authentication mode of the detected device.
Last detected time	Last time when the device is detected.

11.11.36 display wlan ids spoof-ssid fuzzy-match

Function

The **display wlan ids spoof-ssid fuzzy-match** command displays fuzzy matching rules for spoofing SSIDs.

Format

display wlan ids spoof-ssid fuzzy-match regex *regex-value*

Parameters

Parameter	Description	Value
regex *regex-value*	Specifies the matching rules for spoofing SSIDs and displays spoofing SSIDs that match the rules.	The rules must exist. The value is in text format and can contain 1 to 48 case-sensitive characters. It supports Chinese characters or mixture of Chinese and English characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view SSIDs that match a specific rule, run the **display wlan ids spoof-ssid fuzzy-match regex** *regex-value* command.

Example

Display SSIDs that match a specific rule.

```
<HUAWEI> display wlan ids spoof-ssid fuzzy-match regex ^HUAWE[1l]$
#Dev: Number of devices using SSID
--------------------------------------------------------------------------------
Match SSID                       #Dev  Last detected time   WIDS spoof profile
--------------------------------------------------------------------------------
HUAWE1                             2    2014-03-06/12:44:37  example
HUAWEl                             1    2014-03-06/12:44:50  example
--------------------------------------------------------------------------------
Total: 2
```

Table 11-246 Description of the **display wlan ids spoof-ssid fuzzy-match regex** command output

Item	Description
Match SSID	SSID matching a specific rule.
#Dev	Number of APs using the matching SSID.
Last detected time	Latest time when the SSID is detected.
WIDS spoof profile	WIDS spoof profile to which the rules belong.

11.11.37 display wlan wapi certificate

Function

The **display wlan wapi certificate** command displays the content of a certificate file.

Format

display wlan wapi certificate file-name *file-name*

Parameters

Parameter	Description	Value
file-name *file-name*	Specifies a certificate file name.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) and cannot start or end with double quotation marks (" ") or spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view content of certificate files imported to the device.

In the command, *file-name* must specify the complete path of a certificate file. For example, if the certificate file **as.cer** is saved in the flash memory, run **display wlan wapi certificate file-name flash:/as.cer** command.

Example

Display content of certificate file **as.cer**.

```
<HUAWEI> display wlan wapi certificate file-name flash:/as.cer
Certificate:
Data:
  Version: V3
  Serial number:
      50 FA CF CA
  Signature algorithm: sha256ECDSA192
  Issuer:
      C = CN
      O = 0003
      OU = CUCC
      CN = as_test_1@ASU
  Validity:
    Not before: 2013-01-19 16:54:34 UTC
    Not after : 2033-01-19 16:54:34 UTC
  Subject:
      C = CN
      O = 0003
      OU = CUCC
      CN = as_test_1@ASU
  Subject public key information:
    Public key algorithm: ECC
    Public key: (392 bit)
      04 31 AB F2 76 AE E4 BD EF E6 ED CA 93 C0 04 C8
      C9 C9 BF 6F A3 6A F9 A1 9E 35 3E 9B 08 21 EF 20
      5E 82 C1 42 2D A9 42 C3 CE 91 98 7F 21 83 7C 71
      3A
```

Table 11-247 Description of the **display wlan wapi certificate** command output

Item	Description
Version	Version of the X.509 certificate.
Serial number	Serial number of the certificate.
Signature algorithm	Signature algorithm used by the certificate.
Issuer	Certificate issuer.
Validity	Valid period of the certificate, specified by the start date and end date.
Subject	Subject of the certificate.
Subject public key information	Information about the public key of the certificate.

11.11.38 dynamic-blacklist aging-time

Function

The **dynamic-blacklist aging-time** command sets an aging time for a dynamic blacklist.

The **undo dynamic-blacklist aging-time** command restores the aging time of a dynamic blacklist to the default value.

By default, the aging time of a dynamic blacklist is 300 seconds.

Format

dynamic-blacklist aging-time *time*

undo dynamic-blacklist aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time at the expiry of which a specified MAC address is removed from the dynamic blacklist.	The value is an integer that ranges from 180 to 3600, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When detecting attacks from a STA, an AP reports the STA to the AC, forbids the STA to go online, and rejects any packets sent from the STA. As long as the STA is blacklisted, it cannot go online again even if it no longer launches attacks. To avoid that, you can run the **dynamic-blacklist aging-time** command to configure an aging time for the dynamic blacklist. If the configured aging time expires and the AP detects no attack from the STA, the STA is once again allowed to go online.

Example

Set the aging time of the dynamic blacklist to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name example
[HUAWEI-wlan-ap-system-prof-example] dynamic-blacklist aging-time 200
```

11.11.39 dynamic-blacklist disable

Function

The **dynamic-blacklist disable** command disables the dynamic blacklist function.

The **undo dynamic-blacklist disable** command enables the dynamic blacklist function.

By default, the dynamic blacklist function is enabled.

Format

dynamic-blacklist disable

undo dynamic-blacklist disable

Parameters

None

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attack detection is enabled to detect flood attacks, weak IV attacks, spoofing attacks, and brute force key cracking attacks. When detecting attacks initiated by a device, an AP reports an alarm to the AC. In addition, you can run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function on the AC for handling flood attacks and brute force key cracking attacks. The AC then automatically adds the attacking device to a dynamic blacklist and discards packets sent from the attacking device till the dynamic blacklist ages out.

An AP can use the dynamic blacklist to filter out the blacklisted wireless devices to avoid malicious attacks.

Follow-up Procedure

Run the **dynamic-blacklist aging-time** command to set an aging time for the dynamic blacklist.

Example

Enable the dynamic blacklist function.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] undo dynamic-blacklist disable
```

11.11.40 flood-detect interval

Function

The **flood-detect interval** command sets the flood attack detection interval.

The **undo flood-detect interval** command restores the default flood attack detection interval.

By default, the flood attack detection interval is 10 seconds.

Format

flood-detect interval *interval*

undo flood-detect interval

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for flood attack detection.	The value is an integer that ranges from 10 to 120, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A flood attack occurs when an AP receives a large number of packets of the same type within a short period. As a result, the AP is flooded by too many attack packets to process service packets from authorized wireless terminals.

After the flood attack detection function is enabled, an AP counts the number of packets of the same type that it receives from a user at regular intervals. When the number exceeds a specified threshold, the AP considers that the user launches a flood attack. If the dynamic blacklist function is enabled, the user will be added to a dynamic blacklist.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection interval to 120s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect flood enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] flood-detect interval 120
```

11.11.41 flood-detect quiet-time

Function

The **flood-detect quiet-time** command sets the quiet time for an AP to report the detected flood attacks to the AC.

The **undo flood-detect quiet-time** command restores the quiet time for an AP to report the detected flood attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected flood attacks to the AC.

Format

flood-detect quiet-time *quiet-time-value*

undo flood-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected flood attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the quiet time to 300 seconds for an AP to report the detected flood attacks to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect flood enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] flood-detect quiet-time 300
```

11.11.42 flood-detect threshold

Function

The **flood-detect threshold** command sets the flood attack detection threshold. A flood attack occurs when an AP receives a large number of packets of the same type within a short period.

The **undo flood-detect threshold** command restores the default flood attack detection threshold.

By default, the flood attack detection threshold is 500.

Format

flood-detect threshold *threshold*

undo flood-detect threshold

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the flood attack detection threshold.	The value is an integer that ranges from 1 to 1000.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A flood attack occurs when a device receives a large number of packets of the same type within a short period. As a result, the device is flooded by too many attack packets to process service packets from authorized wireless terminals.

After the flood attack detection function is enabled, a device counts the number of packets of the same type that it receives from a user at regular intervals. When the number exceeds a specified threshold, the device considers that the user launches a flood attack. If the dynamic blacklist function is enabled, the user will be added to a dynamic blacklist. If the threshold is set to a small value, the device may incorrectly add authorized users to the dynamic blacklist, causing the users unable to go online.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection threshold to 350.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect flood enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] flood-detect threshold 350
```

11.11.43 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP source guard (IPSG) on APs.

The **undo ip source check user-bind enable** command disables IPSG on APs.

By default, IPSG is disabled on APs.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Users can configure static IP addresses for their clients and connect to the Internet after passing 802.1X authentication. To defend against source IP address spoofing attacks, you need to enable IPSG on APs.

To prevent IP packets of unauthorized users from entering external networks through an AP, enable IPSG in a VAP profile and bind the VAP profile to an AP or AP group. The IPSG function can filter incoming packets on an AP radio interface, preventing unauthorized packets from passing through the AP.

Example

Enable IPSG on APs.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] ip source check user-bind enable
```

11.11.44 learn-client-address dhcp-strict

Function

The **learn-client-address dhcp-strict** command enables strict STA IP address learning through DHCP.

The **undo learn-client-address dhcp-strict** command disables strict STA IP address learning through DHCP.

By default, strict STA IP address learning through DHCP is disabled.

Format

learn-client-address dhcp-strict [**blacklist enable**]

undo learn-client-address dhcp-strict

Parameters

Parameter	Description	Value
blacklist enable	Adds STAs with bogus IP addresses to a blacklist. By default, STAs with bogus IP addresses are not added to a blacklist.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA associates with an AP, the following situation occurs after strict STA IP address learning through DHCP is enabled:

- If the STA obtains an IP address through DHCP, the AP will automatically report the IP address to the AC. The STA IP address can be used to maintain the mapping between STA IP addresses and MAC addresses.
- For a STA using a static IP address:
  - If **blacklist enable** is specified, the STA will be added to a dynamic blacklist of the AP and cannot associate with the AP before the blacklist entry ages.
  - If **blacklist enable** is not specified, the STA can associate with the AP but the AP does not learn the IP address of the STA.

Prerequisites

STA address learning has been enabled using the **undo learn-client-address ipv4 disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **ip source check user-bind enable** and **arp anti-attack check user-bind enable** commands to enable IPSG and DAI so that STAs can communicate with the network only after obtaining an IP address through DHCP.

If this function is disabled, you can manually configure a static IP address. However, if a STA obtains an IP address dynamically using DHCP, goes online, and then is assigned a static IP address, the administrator cannot detect the IP address change of this STA.

Example

Enable strict STA IP address learning through DHCP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] learn-client-address dhcp-strict
```

11.11.45 learn-client-address { dhcpv6-strict | dhcpv6-slaac }

Function

The **learn-client-address { dhcpv6-strict | dhcpv6-slaac }** command enables strict STA IPv6 address learning.

The **undo learn-client-address { dhcpv6-strict | dhcpv6-slaac }** command disables strict STA IPv6 address learning.

By default, strict STA IPv6 address learning is disabled.

Format

learn-client-address { **dhcpv6-strict** | **dhcpv6-slaac** } [**blacklist enable**]

undo learn-client-address { **dhcpv6-strict** | **dhcpv6-slaac** }

Parameters

Parameter	Description	Value
dhcpv6-strict	Enables the STA IPv6 address learning function only through DHCPv6.	-
dhcpv6-slaac	Enables the STA IPv6 address learning function only through DHCPv6 or SLAAC in DHCPv6 + SLAAC scenarios.	-
blacklist enable	Adds STAs with bogus IPv6 addresses to a blacklist. By default, STAs with bogus IPv6 addresses are not added to a blacklist.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA associates with an AP, the following situation occurs after strict STA IPv6 address learning is enabled:

- If the STA obtains an IPv6 address through DHCPv6 or SLAAC, the AP will proactively report the STA's IPv6 address to the AC to maintain the STA's IPv6 address and MAC address binding entry.
- For a STA using a static IPv6 address:
  - If **blacklist enable** is specified, the STA will be added to a dynamic blacklist of the AP and cannot associate with the AP before the blacklist entry ages.
  - If **blacklist enable** is not specified, the STA can associate with the AP but the AP does not learn the IPv6 address of the STA.

Prerequisites

The ND trusted interface of the AP has been disabled using the **undo nd trust port** command in the VAP profile view.

STA address learning has been enabled using the **undo learn-client-address ipv6 disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **ip source check user-bind enable** and **arp anti-attack check user-bind enable** commands to enable IPSG and DAI so that STAs can communicate with the network only after obtaining an IPv6 address.

If this function is disabled, you can manually configure a static IP address. However, if a STA obtains an IP address dynamically using DHCPv6 or SLAAC, goes online, and then is assigned a static IP address, the administrator cannot detect the IP address change of this STA.

If you run this command multiple times, only the latest configuration takes effect.

Example

Enable strict STA IPv6 address learning only through DHCPv6 or SLAAC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] learn-client-address dhcpv6-slaac
```

11.11.46 learn-client-address disable (VAP profile view)

Function

The **learn-client-address disable** command disables STA address learning.

The **undo learn-client-address disable** command enables STA address learning.

By default, STA address learning is enabled.

Format

learn-client-address { **ipv4** | **ipv6** } **disable**

undo learn-client-address { **ipv4** | **ipv6** } **disable**

Parameters

Parameter	Description	Value
ipv4	Indicates the IPv4 address.	-
ipv6	Indicates the IPv6 address.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a STA is associated with a STA address learning-enabled AP and obtains an IP address, the AP proactively reports the STA's IP address to the AC to maintain the IP address-MAC address binding entry of the STA. In addition, when a STA requests an IP address using DHCP, the AP can learn the IPv4 address of the STA gateway.

Prerequisites

- Before enabling STA address learning, ensure that the ND trusted interface of the AP for the IPv6 address has been disabled using the **undo nd trust port** command.
- Before disabling STA address learning, ensure that strict STA IPv4 address learning has been disabled using the **undo learn-client-address dhcp-strict** command and strict STA IPv6 address learning disabled using the **undo learn-client-address dhcpv6-strict** command.

Precautions

- The device enabled with STA address learning can learn only a limited number of IPv6 addresses; therefore, you are advised to configure only one IPv6 prefix for the IPv6 gateway. If you configure too many IPv6 prefixes, the number of IPv6 addresses exceeds the upper limit, and extra IPv6 addresses cannot be learned by the device. IPv6 addresses that are not learned by the device cannot be used for communication.

- If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.
- Disabling STA address learning will lead to a Portal authentication failure.
- When a STA requests an IP address using DHCP, the STA address learning-enabled AP can only learn the IPv4 gateway address but cannot learn the IPv6 gateway address.
- If no STA connected to a STA address learning-enabled AP requests an IP address using DHCP, the AP cannot learn the gateway IP address.

Example

Disable STA IPv4 address learning.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] learn-client-address ipv4 disable
```

11.11.47 nd trust port

Function

The **nd trust port** command enables the ND trusted interface on an AP.

The **undo nd trust port** command cancels the configuration.

By default, the ND trusted interface is disabled on an AP

Format

nd trust port

undo nd trust port

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a bogus ND server is deployed at the user side, STAs may obtain incorrect IPv6 addresses and network configuration parameters and cannot communicate properly. After the **undo nd trust port** command is executed in the VAP profile view, an AP discards the ND OFFER, ACK, and NAK packets sent by the bogus ND server and the IPv6 address of the unauthorized ND server.

Before WLAN services are delivered to an AP, run the **nd trust port** command in the AP wired port profile view. After the command is run, the AP receives the ND OFFER, ACK, and NAK packets sent by the authorized ND server and forwards the packets to STAs so that the STAs can obtain valid IPv6 addresses and go online.

Prerequisites

The function of processing STA IPv6 services has been enabled using the **sta-ipv6-service enable** command.

Before enabling the ND trusted interface, ensure that STA IPv6 address learning has been disabled using the **learn-client-address ipv6 disable** command.

Example

Create the VAP profile **vap1** and enable the ND trusted interface on the AP in the VAP profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] nd trust port
```

11.11.48 oui

Function

The **oui** command configures an organizationally unique identifier (OUI) for STAs in the whitelist.

The **undo oui** command deletes the OUI of a specified STA or all STAs in the whitelist.

By default, no OUI is configured for STAs in the whitelist.

Format

oui *oui* [**description** *description*]

undo oui { *oui* | **all** }

Parameters

Parameter	Description	Value
oui	Specifies the OUI of STAs in the whitelist.	The value is in H-H-H format. An H is a hexadecimal number of 2 digits. For example, **11-22-33** indicates a STA whose first 6 bits of the MAC address are 11-22-33.
description	Specifies the OUI description of STAs in the whitelist.	The value is a string of 1 to 80 characters.
all	Deletes the OUI of all STAs in the whitelist.	-

Views

STA whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

After the whitelist function is enabled, all STAs in the whitelist can connect to the WLAN. In some scenarios, all STAs with a specified OUI need to be added to the whitelist. You can run the **oui** command to add STAs with a specified OUI to the whitelist.

Example

Configure the OUI **00-11-22** for STAs in the whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-whitelist-profile name sta-whitelist-profile1
[HUAWEI-wlan-whitelist-prof-sta-whitelist-profile1] oui 00-11-22
```

11.11.49 permit-ap

Function

The **permit-ap** command configures a WIDS whitelist.

The **undo permit-ap** command deletes entries in the WIDS whitelist.

By default, no WIDS whitelist is configured.

Format

permit-ap { **mac-address** *mac-address* | **oui** *oui* | **ssid** *ssid* }

undo permit-ap { **mac-address** { *mac-address* | **all** } | **oui** { *oui* | **all** } | **ssid** { **name** *ssid* | **all** } }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Adds or deletes an authorized MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
mac-address all	Deletes an authorized MAC address list.	-
oui *oui*	Adds or deletes an authorized OUI.	The value is in H-H-H format. An H is a hexadecimal number of 2 digits.
oui all	Deletes an authorized OUI list.	-

Parameter	Description	Value
ssid name *ssid*	Deletes an authorized SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters. To start an SSID with a space, you need to encompass the SSID with double quotation marks (" "), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character.

Parameter	Description	Value
ssid *ssid*	Adds an authorized SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters. To start an SSID with a space, you need to encompass the SSID with double quotation marks (" "), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, **\"hello**. The backslash occupies one character.
ssid all	Deletes an authorized SSID list.	-

Views

WIDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After WIDS/WIPS is enabled, rogue APs can be detected and contained. However, there may be APs of other vendors or other networks working in the existing signal coverage areas. If these APs are contained, their services will be affected. To prevent this situation, configure an authorized AP list, including an authorized MAC address list, OUI list, and SSID list. If a rogue AP is detected but matches the authorized AP list, the AP is considered an authorized AP and will not be contained.

For example, APs of other vendors are deployed on the existing WLAN to expand network capacity. To prevent the APs from being contained, add OUIs of the vendors to a whitelist and add SSIDs of these APs to a whitelist. In this way, the device will consider the APs as authorized APs.

The device determines whether a detected AP is authorized as follows:

1. Check whether the AP's MAC address is in the authorized MAC address list.
   - If so, the AP is an authorized AP.
   - If not, go to step 2.
2. Check whether the AP's OUI and SSID are in the OUI and SSID lists.
   - If only the SSID is configured, check whether the AP's SSID is in the authorized SSID list.
     - If so, the AP is an authorized AP.
     - If not, the AP is a rogue AP.
   - If only the OUI is configured, check whether the AP's OUI is in the authorized OUI list.
     - If so, the AP is an authorized AP.
     - If not, the AP is a rogue AP.
   - If OUI and SSID of an AP are configured and both of them are matched, check whether the AP's OUI and SSID are in the authorized OUI and SSID lists.
     - If so, the AP is an authorized AP.
     - If neither or only one of them is in the list, the AP is a rogue AP.
   - If both OUI and SSID of an AP are configured and either of them can be matched, check whether either of AP's OUI and SSID are in the authorized OUI list or SSID list.
     - If both or one of them is in the list, the AP is an authorized AP.
     - If neither of them is in the list, the AP is a rogue AP.

Precautions

If you add or delete an entry, the device will re-check the validity of the rogue APs. If a rogue AP becomes authorized, the device stops containing it. If an authorized AP becomes rogue, the device starts to contain it.

Example

Add an MAC address, an OUI, and an SSID to the WIDS whitelist.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name default
[HUAWEI-wlan-wids-whitelist-default] permit-ap mac-address 00e0-fc12-3456
```

```
[HUAWEI-wlan-wids-whitelist-default] permit-ap oui 00-11-22
[HUAWEI-wlan-wids-whitelist-default] permit-ap ssid example
```

11.11.50 permit-ap oui-ssid-match

Function

The **permit-ap oui-ssid-match** command configures an OUI and SSID matching policy in a WIDS whitelist.

The **undo permit-ap oui-ssid-match** command deletes the OUI and SSID matching policy in a WIDS whitelist.

By default, both OUIs and SSIDs are matched in a WIDS whitelist.

Format

permit-ap oui-ssid-match { **both** | **any** }

undo permit-ap oui-ssid-match

Parameters

Parameter	Description	Value
both	Matches both OUIs and SSIDs in a WIDS whitelist.	-
any	Matches either of OUIs and SSIDs in a WIDS whitelist.	-

Views

WIDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After WIDS or WIPS is enabled, you can run the **permit-ap** command to configure a WIDS whitelist, including the authorized MAC address list, authorized OUI list, and authorized SSID list. If a rogue AP is detected but matches the authorized AP list, the AP is considered an authorized AP and will not be contained.

This command is used to configure a policy for matching OUIs and SSIDs in the WIDS whitelist.

- Both: Both the OUI and SSID of an AP are matched against the authorized OUI list and authorized SSID list. If no match is found in the lists, the AP is considered a rogue AP. If only one of authorized OUI and SSID lists is configured in the WIDS whitelist, the device matches the OUI or SSID of the AP only against the configured list.

- Any: The OUI and SSID of an AP is matched against the authorized OUI list or the authorized SSID list accordingly. If a match is found in either of the lists, the AP is considered an authorized AP; if not, the AP is considered a rogue AP.

Precautions

After the OUI and SSID matching policy is modified, the device checks whether the AP is authorized. If not, the device determines the containment policy. If a rogue AP becomes authorized, the device stops containing it. If an authorized AP becomes rogue, the device starts to contain it.

Example

Set the OUI and SSID matching policy in a WIDS whitelist to **any**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name default
[HUAWEI-wlan-wids-whitelist-default] permit-ap oui 00-11-22
[HUAWEI-wlan-wids-whitelist-default] permit-ap ssid example
[HUAWEI-wlan-wids-whitelist-default] permit-ap oui-ssid-match any
```

11.11.51 pmf

Function

The **pmf** command enables the Protected Management Frame (PMF) function of a VAP.

The **undo pmf** command disables the PMF function for a VAP.

By default, the PMF function is disabled for a VAP.

Format

pmf { **optional** | **mandatory** }

undo pmf

Parameters

Parameter	Description	Value
optional	Indicates the optional mode, in which STAs can access the VAP regardless of whether the STAs support PMF or not, but the VAP encrypts only management frames of PMF-capable STAs.	-

Parameter	Description	Value
mandatory	Indicates the mandatory mode, in which the VAP permits access only from PMF-capable STAs.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PMF is a specification released by Wi-Fi Alliance (WFA) based on IEEE 802.11w standards. It aims to apply security measures defined in WPA2, WPA3, OWE to unicast and multicast management action frames to improve network credibility.

If management frames transmitted on WLANs are not encrypted, the following security problems may be introduced. PMF can address the problems.

- Hackers intercept management frames exchanged between the APs and users.
- Hackers pretend to be APs and send Disassociation and Deauthentication frames to disconnect users.
- Hackers pretend to be users and send Disassociation frames to APs to disconnect the users.

Precautions

The authentication and encryption mode in a security profile must be set to WPA2–AES/WPA2-WPA3/WPA3/OWE.

If the authentication mode is WPA3, this command does not take effect. If the authentication mode is WPA3-SAE or WPA3-802.1X, the PMF mode is fixed at **mandatory**. If the authentication mode is WPA2-WPA3, the PMF mode is fixed at **optional**.

If the authentication mode is OWE or its transition mode, this command does not take effect, and the PMF mode is fixed at **mandatory**.

Modifying configuration in the security profile will disconnect all users on the VAP that uses the security profile. The users need to reassociate with the VAP to go online.

The PMF function cannot be deployed on Mesh networks.

Example

Enable the PMF function in optional mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2 psk pass-phrase abcdfffffg aes
[HUAWEI-wlan-sec-prof-p1] pmf optional
```

11.11.52 reset wlan ids attack-detected

Function

The **reset wlan ids attack-detected** command deletes information about the attacking devices detected.

Format

reset wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all types of attacking devices.	-
flood	Deletes information about devices launching flood attacks.	-
spoof	Deletes information about devices launching spoofing attacks.	-
wapi-psk	Deletes information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes information about devices launching weak IV attacks.	-
wep-share-key	Deletes information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes information about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, information about attacking devices detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected** command to delete the information.

Example

Delete information about all the current attacking devices.

```
<HUAWEI> reset wlan ids attack-detected all
```

11.11.53 reset wlan ids attack-detected statistics

Function

The **reset wlan ids attack-detected statistics** command deletes the number of attacks detected.

Format

reset wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, the number of attacks detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected statistics** command to delete the information.

Example

Delete the number of attacks detected.

```
<HUAWEI> reset wlan ids attack-detected statistics
```

11.11.54 reset wlan ids attack-history

Function

The **reset wlan ids attack-history** command deletes historical records about the attacking devices detected.

Format

reset wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes historical records about all types of attacking devices.	-
flood	Deletes historical records about devices launching flood attacks.	-
spoof	Deletes historical records about devices launching spoofing attacks.	-
wapi-psk	Deletes historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes historical records about devices launching weak IV attacks.	-
wep-share-key	Deletes historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes historical records about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, historical records about attacking devices detected are recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-history** command to delete the information.

Example

Delete historical records about all the current attacking devices.

```
<HUAWEI> reset wlan ids attack-history all
```

11.11.55 reset wlan dynamic-blacklist

Function

The **reset wlan dynamic-blacklist** command deletes information about devices in the dynamic blacklist.

Format

reset wlan dynamic-blacklist { **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* | **all** }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Deletes the dynamic blacklist information reported by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Deletes the dynamic blacklist information reported by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Deletes the device with a specified MAC address from the dynamic blacklist.	The MAC address must exist.
all	Deletes all information in the dynamic blacklist.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset wlan dynamic-blacklist** command is applicable to the following scenarios:

- To re-collect the dynamic blacklist information, run the **reset wlan dynamic-blacklist all** command to delete all information in the dynamic blacklist. After that, the AC re-collects the information.
- To remove an authorized device from the dynamic blacklist, run the **reset wlan dynamic-blacklist mac-address** command to remove the MAC address of the device from the dynamic blacklist. After that, information sent from the device is not rejected.

Precautions

Running the **reset wlan dynamic-blacklist** command affects packet receiving of APs. Exercise caution when running this command.

Example

Delete the device with the MAC address 00E0-FC12-3456 from the dynamic blacklist.

```
<HUAWEI> reset wlan dynamic-blacklist mac-address 00e0-fc12-3456
```

11.11.56 reset wlan ids rogue-history

Function

The **reset wlan ids rogue-history** command deletes historical records of rogue devices.

Format

reset wlan ids rogue-history { **all** | **ap** | **bridge** | **client** | **adhoc** | **ssid** [*ssid*] | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes historical records of all rogue devices.	-
ap	Deletes historical records of rogue APs.	-
bridge	Deletes historical records of rogue bridge devices.	-

Parameter	Description	Value
client	Deletes historical records of rogue user terminals.	-
adhoc	Deletes historical records of rogue ad-hoc devices.	-
ssid [*ssid*]	Deletes historical records of devices with specified SSIDs.	The SSID must exist. To specify an SSID starting with a space, include the SSID with double quotation marks (" "). For example, in the SSID **" hello"**, the double quotation marks at the start and end of the SSID occupy two characters. To specify an SSID starting with a double quotation mark ("), enter an escape character (\) before the double quotation mark. For example, in the SSID **\"hello**, the escape character (\) occupies one character.
mac-address *mac-address*	Deletes historical records of devices with specified MAC addresses.	The value must be an existing MAC address.

Views

All views

Default Level

3: Management level

Usage Guidelines

When there are excessive historical records of rogue devices or their historical records are useless, you can run the **reset wlan ids rogue-history** command to delete the historical records.

Example

Delete all detected historical records of the rogue devices.

```
<HUAWEI> reset wlan ids rogue-history all
```

11.11.57 rogue-device log enable

Function

The **rogue-device log enable** command enables the function of recording rogue device information in the log.

The **undo rogue-device log enable** command disables the function of recording rogue device information in the log.

By default, the function of recording rogue device information in the log is disabled.

Format

rogue-device log enable

undo rogue-device log enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a rogue device is detected after this function is enabled, information about the device is recorded in the log.

Example

Enable the function of recording rogue device information in the log.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] rogue-device log enable
```

11.11.58 security dot1x

Function

The **security dot1x** command configures 802.1X authentication and encryption for WPA and WPA2.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security { **wpa** | **wpa2** | **wpa-wpa2** } **dot1x** { **aes** | **tkip** | **aes-tkip** }

security wpa-wpa2 dot1x tkip aes

undo security

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
wpa-wpa2	Configures WPA-WPA2 authentication. STAs can be authenticated using WPA or WPA2.	-
aes	Configures AES encryption.	-
tkip	Configures TKIP encryption.	-
aes-tkip	Configures AES-TKIP encryption. After successful authentication, STAs can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two types of WPA/WPA2 authentication: WPA/WPA2-PSK authentication (also called WPA/WPA2-Personal) and WPA/WPA2-802.1X authentication (also called WPA/WPA2-Enterprise). 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 802.1X authentication, run the **security dot1x** command. If multiple types of STAs connect to the network and they support different authentication and encryption modes, you can configure hybrid encryption and authentication modes.

The **security wpa-wpa2 dot1x tkip aes** command indicates that WPA and WPA2 use TKIP and AES for data encryption, respectively.

Precautions

TKIP and AES-TKIP are insecure encryption algorithms. For data encryption, AES is recommended.

The following STAs do not support the WPA2 802.1X authentication and cannot access the AP. You must configure other security policies for the STAs.

- Nokia: N8
- HP: Pre 3

The authentication type in the security profile and authentication profile must both be set to 802.1X authentication. You can run the **display wlan config-errors** command to check whether error messages are generated for authentication type mismatch between the security profile and authentication profile.

The system displays the message only when the security profile has been bound to the other profiles.

If 802.1X authentication and TKIP or AES-TKIP encryption for WPA/WPA2 are configured, the access of non-HT STAs fails to be denied.

The offline management VAP does not support 802.1X authentication and encryption modes. Therefore, if the offline management VAP is enabled for a VAP profile, the VAP profile cannot be bound to a security profile with WPA/WPA2 802.1X authentication and encryption configured. If the VAP profile has been bound to a security profile, the authentication and encryption modes of the security profile cannot be changed to WPA/WPA2 802.1X.

Example

Configure WPA (802.1X authentication and TKIP encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa dot1x tkip
```

Configure WPA2 (802.1X authentication and TKIP encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2 dot1x tkip
```

Configure WPA-WPA2 (802.1X authentication and TKIP-AES encryption).

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
```

11.11.59 security enhanced-open

Function

The **security enhanced-open** command configures Opportunistic Wireless Encryption (OWE) authentication or authentication and encryption in OWE transition mode.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security enhanced-open aes [**transition-ssid** *ssid*]

undo security

Parameters

Parameter	Description	Value
aes	Configures AES encryption.	-
transition-ssid *ssid*	Specifies an SSID to use open authentication in OWE transition mode. ● If this parameter is not specified, OWE authentication is used. ● If this parameter is specified, the OWE transition mode is used. **NOTE** In OWE transition mode, you need to configure two VAP profiles on the same radio and set their authentication modes to OWE and open, respectively. Ensure that the parameter **transition-ssid** is set the same as the SSID in the VAP profile using the open security policy but different from the SSID in the VAP profile using OWE authentication. The OWE transition mode takes effect only when a VAP profile on the same radio uses the same SSID as **transition-ssid** and the open security policy, and the corresponding VAP is enabled. If such effective conditions are not met, the device uses OWE authentication.	The value is a string of 1 to 32 case-sensitive characters without spaces. If spaces are contained in the SSID, enclose the string using double quotation marks ("). For example, if an SSID is **a bc**, enter **"a bc"** when specifying this parameter. In this case, the string can contain a maximum of 30 characters. If the first character of an SSID is a double quotation mark ("), add a backslash (\) to the SSID as the prefix. For example, if an SSID is **"abc**, enter **\"abc** when specifying this parameter. In this case, the string can contain a maximum of 31 characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OWE is a Wi-Fi Enhanced Open authentication mode that allows users to access the network without entering the password. In OWE authentication mode, the device uses the AES encryption algorithm to encrypt data on the network, thereby protecting data exchange between STAs and the Wi-Fi network. The OWE transition mode provides backward compatibility with STAs that do not support OWE authentication. That is, these STAs access the network in open-system authentication mode, while OWE-capable STAs access the network in OWE authentication mode.

Precautions

- OWE authentication or its transition mode automatically enables the PMF function in mandatory mode. That is, the **pmf** { **optional** | **mandatory** } command configuration does not take effect in OWE authentication or its transition mode.
- OWE authentication depends on the PMF function, but 802.11n APs do not support the PMF function. Therefore, 802.11n APs do not support OWE authentication.
- OWE authentication and 802.11r cannot be enabled at the same time.
- OWE authentication is not supported in WDS and Mesh scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.
- Some STAs may fail to access the network in OWE or OWE transition mode due to compatibility issues.
- Some OWE-capable STAs may still access the network through open system authentication in OWE transition mode due to compatibility issues.

Example

Set the authentication mode to the OWE transition mode and the SSID using the open-system authentication mode to **wlan-net**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security enhanced-open aes transition-ssid wlan-net
```

11.11.60 security open

Function

The **security open** command configures open-system authentication.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security open

undo security

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Open-system authentication is applicable to public venues where users move frequently and do not need to be authenticated, such as airports and stations. That is, users can access the network without authentication and encryption.

Precautions

It is not secure to use open system authentication independently. Any wireless terminals can access the network without authentication. You are advised to configure open system authentication together with Portal authentication or MAC address authentication.

Example

Configure open-system authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security open
```

11.11.61 security psk

Function

The **security psk** command configures WPA/WPA2 PSK authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security { **wpa** | **wpa2** | **wpa-wpa2** } **psk** { **pass-phrase** | **hex** } *key-value* { **aes** | **tkip** | **aes-tkip** }

security wpa-wpa2 psk { **pass-phrase** | **hex** } *key-value* **tkip aes**

undo security

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
wpa-wpa2	Configures WPA-WPA2 authentication. STAs can be authenticated using WPA or WPA2.	-
psk	Configures PSK authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommended.	-

Parameter	Description	Value
key-value	Specifies a password in cipher text.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. The question mark (?) is supported, which you can enter by pressing **Ctrl+T**. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.
aes	Configures AES encryption.	-
tkip	Configures TKIP encryption.	-
aes-tkip	Configures AES-TKIP encryption. After successful authentication, STAs can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two types of WPA/WPA2 authentication: WPA/WPA2-PSK authentication (also called WPA/WPA2-Personal) and WPA/WPA2 802.1X authentication (also called WPA/WPA2-Enterprise). 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 PSK authentication, run the **security psk** command. If multiple types of STAs are available, you can configure the WPA-WPA2 and AES-TKIP security policy for authentication and data encryption.

The **security wpa-wpa2 psk** { **pass-phrase** | **hex** } *key-value* **tkip aes** command indicates that WPA and WPA2 use TKIP and AES for data encryption, respectively.

Precautions

TKIP and AES-TKIP are insecure encryption algorithms. For data encryption, AES is recommended.

If the key is in hexadecimal notation, you can enter hexadecimal characters without entering 0x.

If a security profile is bound to multiple VAP profiles, it will take a few minutes to configure WPA/WPA2 PSK authentication and encryption in the security profile.

The system displays the message only when the security profile has been bound to the other profiles.

If PSK authentication and TKIP or AES-TKIP encryption for WPA/WPA2 is configured, the access of non-HT STAs fails to be denied.

If the password is changed to one starting or ending with a space (for example, **YsHsjx_202206**) on the device, some STAs (such as STAs running Windows 7) may filter out the space when you change the password on the STAs. This will lead to an association failure. Therefore, it is not recommended that a password starting or ending with a space be set on the device. If such a password has been configured on the device, delete the existing WLAN configuration on a STA, reassociate the STA with the SSID, and enter the password. For detailed terminal types, refer to the *Test Report on Terminal Compatibility*.

Example

Configure WPA-PSK authentication and the authentication key.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa psk pass-phrase YsHsjx_202206 aes
```

Configure WPA2-PSK authentication and the authentication key.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2 psk pass-phrase YsHsjx_202206 aes
```

Configure WPA-WPA2 hybrid encryption and PSK authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 psk pass-phrase YsHsjx_202206 aes-tkip
```

11.11.62 security wapi

Function

The **security wapi** command configures the WAPI authentication mode.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wapi psk { **pass-phrase** | **hex** } *key-value*

security wapi certificate

undo security

Parameters

Parameter	Description	Value
certificate	Configures WAPI certificate authentication.	-
psk	Configures WAPI pre-shared key authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommended.	-

Parameter	Description	Value
key-value	Specifies a password in cipher text.	In pass-phrase mode, the key is a string of 8 to 63 characters in plaintext, or 48 or 68 or 88 or 108 characters in ciphertext. In hex mode, the key is a string of 8 to 32 hexadecimal numbers, in which the length of the string must be an even, or a string of 48 or 68 characters in ciphertext. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WAPI supports two authentication modes: certificate authentication and pre-shared key authentication. When pre-shared key authentication is used, a pre-shared key must be configured.

- If WAPI authentication is specified as a security policy in a security profile, you can run the **wapi authentication-method** command to configure the WAPI authentication mode.
- The **wapi authentication-method** command determines the WAPI authentication and key management mode. When certificate authentication and key management are configured, authentication involves identity authentication and key negotiation, and the authentication server and certificate need to be configured. When pre-shared key authentication is configured, a pre-shared key needs to be configured, and STAs also need to know the pre-shared key. In this situation, authentication just involves key negotiation.

Precautions

The system displays the message only when the security profile has been bound to the other profiles.

Example

Set the WAPI authentication mode to pre-shared key authentication and specify the key.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wapi psk pass-phrase YsHsjx_202206
```

11.11.63 security wep

Function

The **security wep** command configures the WEP authentication mode.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wep [**share-key** | **dynamic**]

undo security

Parameters

Parameter	Description	Value
security wep	Sets the WEP authentication mode to open-system and encrypts service packets using WEP.	-
security wep share-key	When the WEP authentication mode is set to shared-key authentication: ● If the parameter is present, WEP uses the configured shared key to authenticate wireless terminals and encrypt service packets. ● If the parameter is not present, WEP only uses the configured shared key to encrypt the service packets. A shared key is configured on the wireless terminals regardless of whether the parameter is present.	-
security wep dynamic	Sets the WEP authentication mode to dynamic WEP.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can select security policies on a WLAN based on the security level. WEP is a security policy used earlier and has security risks. It can be used in open scenarios that do not require high security.

Table 11-248 Comparing authentication modes

Configuration	Link Authentication Mode	Encryption Mode	Advantage	Disadvantage
security open	open	Not encrypted	Wireless devices can connect to a network without authentication.	STA identities are not checked, bringing security risks. Service data is not WEP-encrypted.
security wep	open	Static WEP encryption	Service data is WEP-encrypted.	STA identities are not checked, bringing security risks.
security wep share-key	Shared key authentication	Static WEP encryption	A shared key is used to enhance security. Service data is WEP-encrypted.	● A long key string must be configured on each device and is difficult to expand. ● A static key is used, which is easy to decipher.
security wep dynamic	open	Dynamic WEP encryption	Dynamic WEP encryption for service data provides higher security.	802.1X authentication is also required. The configuration is complex.

Precautions

- If the **security wep** [**share-key**] command is executed, you can run the **wep key** command to configure the pre-shared key. Otherwise, the default pre-shared key is used.
- If the **security wep dynamic** command is executed to configure dynamic WEP, you also need to configure 802.1X authentication. Otherwise, dynamic WEP does not take effect.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same.

- The system displays the message only when the security profile has been bound to the other profiles.
- If WEP authentication is configured, the function of denying access of non-HT STAs fails to take effect.
- Mobile phones do not support dynamic WEP.
- RUs do not support dynamic WEP.
- The WEP encryption algorithm is insecure. WPA2 or WPA3 is recommended in scenarios that have high security requirements.

Example

Create security profile **p1** and set the authentication mode to **share-key**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wep share-key
```

11.11.64 security wpa2-wpa3 psk-sae

Function

The **security wpa2-wpa3 psk-sae** command configures WPA2-WPA3-SAE authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa2-wpa3 psk-sae pass-phrase *key-value* **aes**

undo security

Parameters

Parameter	Description	Value
pass-phrase *key-value*	Specifies the password for WPA2-WPA3-SAE authentication.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA2 is still widely used. To allow STAs that do not support WPA3 to access the WPA3 network, the device supports the WPA3-Personal transition mode, that is, WPA2-WPA3-SAE authentication.

WPA3-Personal supports hybrid authentication, allowing for only WPA2-WPA3 authentication and AES encryption.

Precautions

- WPA2-WPA3 hybrid authentication automatically enables the PMF function in optional mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA2-WPA3 hybrid authentication scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure WPA2-WPA3-SAE authentication and set the user password to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2-wpa3 psk-sae pass-phrase YsHsjx_202206 aes
```

11.11.65 security wpa2-wpa3 dot1x

Function

The **security wpa2-wpa3 dot1x** command configures WPA2-WPA3-802.1X authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa2-wpa3 dot1x aes

undo security

Parameters

Parameter	Description	Value
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA2 is still widely used. To allow STAs that do not support WPA3 to access the WPA3 network, the device supports the WPA3-Enterprise transition mode, that is, WPA2-WPA3-802.1X authentication.

WPA3-Enterprise supports hybrid authentication, allowing for only WPA2-WPA3 authentication and AES encryption.

Precautions

- WPA2-WPA3 hybrid authentication automatically enables the PMF function in optional mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA2-WPA3 hybrid authentication scenarios.

- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure WPA2-WPA3-802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2-wpa3 dot1x aes
```

11.11.66 security wpa3 dot1x

Function

The **security wpa3 dot1x** command configures WPA3-802.1X authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa3 dot1x { **gcmp256** | **aes** }

undo security

Parameters

Parameter	Description	Value
gcmp256	Indicates the AES-GCM encryption algorithm using a 256-bit key.	-
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA3 authentication is classified into the enterprise edition and personal edition, that is, WPA3-802.1X authentication and WPA3-SAE authentication.

Compared with WPA2-802.1X authentication, WPA3-802.1X authentication enhances the algorithm strength by increasing the key length to 192 bits (WPA2 uses a 128-bit encryption key). WPA3-802.1X authentication is applicable to scenarios with high security requirements, such as governments and large enterprises.

WPA3-802.1X authentication has specific requirements on terminals and servers. To deploy WPA3-802.1X authentication, you may need to upgrade related hardware.

Precautions

- WPA3 authentication automatically enables the PMF function in mandatory mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA3 authentication scenarios.
- WPA3-802.1X authentication is supported only by APs in compliance with 802.11ac Wave 2 or higher standards.
- WPA3 and 802.11r cannot be used at the same time.
- WPA3 authentication is not supported in WDS and mesh scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure the WPA3-802.1X authentication mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 dot1x gcmp256
```

11.11.67 security wpa3 sae

Function

The **security wpa3 sae** command configures WPA3-SAE authentication and encryption.

The **undo security** command restores the default security policy.

By default, no security policy is configured.

Format

security wpa3 sae pass-phrase *key-value* **aes**

undo security

Parameters

Parameter	Description	Value
pass-phrase *key-value*	Specifies the password for WPA3-SAE authentication.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx 202206**, enter **"YsHsjx 202206"**. **NOTE** For security purposes, you are advised to configure a key that contains at least two of the following: digits, lowercase letters, uppercase letters, and special characters.
aes	Configures AES encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WPA3 authentication is classified into the enterprise edition and personal edition, that is, WPA3-802.1X authentication and WPA3-SAE authentication.

Similar to WPA/WPA2-PSK authentication, WPA3-SAE authentication applies to small office networks that do not require high network security or authentication server deployment. However, WPA3-SAE introduces the SAE handshake protocol. Compared with WPA/WPA2-PSK authentication, WPA3-SAE can effectively defend against offline dictionary attacks and increase the difficulty of brute force cracking. In addition, the SAE handshake protocol provides forward secrecy. Even if an attacker knows the password on the network, the attacker cannot decrypt or obtain traffic, greatly improving the security of the WPA3 personal network.

Precautions

- WPA3 authentication automatically enables the PMF function in mandatory mode. That is, configuring the **pmf** { **optional** | **mandatory** } command does not take effect in WPA3 authentication scenarios.
- WPA3-SAE authentication depends on the PMF function, but 802.11n APs do not support the PMF function. Therefore, 802.11n APs do not support WPA3-SAE authentication.
- WPA3-SAE does not support PPSK authentication.
- WPA3 and 802.11r cannot be used at the same time.
- WPA3 authentication is not supported in WDS and mesh scenarios.
- If the security profile is bound to another profile, running this command may interrupt services.

Example

Configure WPA3-SAE authentication and set the user password to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 sae pass-phrase YsHsjx_202206 aes
```

11.11.68 security-profile (WLAN view)

Function

The **security-profile** command creates a security profile or enters the security profile view.

The **undo security-profile** command deletes a security profile according to the ID or name.

By default, security profiles **default**, **default-wds** and **default-mesh** are available in the system.

Format

security-profile name *profile-name*

undo security-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a security profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Parameter	Description	Value
all	Deletes all security profiles. **NOTE** Security profiles **default**, **default-wds** and **default-mesh** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure access security. A security profile must be configured before you specify an authentication mode in the profile. To delete a security profile, run the **undo security-profile** command.

The system configures the new profile, the default value is no authentication and no encryption.

Example

Configure a security profile named **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1]
```

11.11.69 security-profile (VAP profile view)

Function

The **security-profile** command binds a security profile to a VAP profile.

The **undo security-profile** command unbinds a security profile from a VAP profile.

By default, the security profile **default** is bound to a VAP profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a security profile.	The security profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to bind a security profile to a VAP profile. The security profile then applies to all users using this VAP profile.

By default, no security policy is configured in a security profile. A VAP can be created on a radio only after a security policy is configured.

Example

Create VAP profile **ChinaNet** and bind security profile **security-profile1** to the VAP profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name ChinaNet
[HUAWEI-wlan-vap-prof-ChinaNet] security-profile security-profile1
```

11.11.70 spoof-detect quiet-time

Function

The **spoof-detect quiet-time** command sets the quiet time for an AP to report the detected spoofing attacks to the AC.

The **undo spoof-detect quiet-time** command restores the default quiet time for an AP to report the detected spoofing attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected spoofing attacks to the AC.

Format

spoof-detect quiet-time *quiet-time-value*

undo spoof-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected spoofing attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time to 300 seconds for an AP to report the detected spoofing attacks to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect spoof enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] spoof-detect quiet-time 300
```

11.11.71 spoof-ssid

Function

The **spoof-ssid** command configures a fuzzy matching rule for spoofing SSIDs.

The **undo spoof-ssid** command deletes a fuzzy matching rule for spoofing SSIDs.

By default, no fuzzy matching rule is configured for spoofing SSIDs.

Format

spoof-ssid fuzzy-match regex *regex-value*

undo spoof-ssid { **fuzzy-match regex** *regex-value* | **all** }

Parameters

Parameter	Description	Value
fuzzy-match	Configures a fuzzy matching rule to identify spoofing SSIDs.	-
regex *regex-value*	Specifies the regular expression for an SSID. If an SSID matches the regular expression, the SSID is considered a spoofing SSID.	The value is in text format and can contain 1 to 48 case-sensitive characters. It supports Chinese characters or mixture of Chinese and English characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
all	Deletes all fuzzy matching rules.	-

Views

WIDS spoof SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN services are available in public places, such as banks and airports. Users can connect to the WLANs after associating with corresponding SSIDs. If a rogue AP is deployed and provides spoofing SSIDs similar to authorized SSIDs, the users may be misled and connect to the rogue AP, which brings security risks. To address this problem, configure a fuzzy matching rule to identify spoofing SSIDs. The device compares a detected SSID with the matching rule. If the SSID matches the rule, the SSID is considered a spoofing SSID. The AP using the spoofing SSID is a rogue AP. After rogue AP containment is configured, the device contains the rogue AP and disconnects users from the spoofing SSID.

Precautions

To make fuzzy matching rules for spoofing SSIDs take effect, enable device detection and rogue device containment so that the device can take countermeasures against rogue APs.

To contain all SSIDs except those on the local device, set the fuzzy matching rule to * and then run the **contain-mode** command to set the containment mode to **spoof-ssid-ap**.

Example

Configure a fuzzy matching rule using the regular expression **^TES[1l]$** to identify spoofing SSIDs **TEST1** or **TESL** similar to **TEST**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-spoof-profile name default
[HUAWEI-wlan-wids-spoof-default] spoof-ssid fuzzy-match regex ^TES[1l]$
```

11.11.72 sta arp-nd-proxy before-assoc

Function

The **sta arp-nd-proxy before-assoc** command enables an AP to send ARP/ND proxy packets for a STA before the STA is successfully associated.

The **undo sta arp-nd-proxy before-assoc** command disables an AP from sending ARP/ND proxy packets for a STA before the STA is successfully associated.

By default, an AP does not send ARP/ND proxy packets for a STA before the STA is successfully associated.

Format

sta arp-nd-proxy before-assoc

undo sta arp-nd-proxy before-assoc

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an AP is enabled to send ARP/ND proxy packets for a STA before the STA succeeds in authentication or key negotiation, the Layer 2 switch connected to the

AP will learn the MAC address of the STA. If an attack floods thousands of STA MAC addresses, the MAC address table on the switch will be seriously corrupted, bringing security risks. To avoid this issue, you can run the **undo sta arp-nd-proxy before-assoc** command to configure the AP to send ARP/ND proxy packets for a STA after the STA succeeds in authentication or key negotiation.

In scenarios with low security requirements, you can run the **sta arp-nd-proxy before-assoc** command to configure the AP to send ARP/ND proxy packets for a STA before the STA is successfully associated to improve link update efficiency.

Precautions

After the **undo sta arp-nd-proxy before-assoc** command is run on an AP, the AP does not send ARP/ND proxy packets for a STA that goes online in open or WEP mode.

Example

Configure an AP to send ARP/ND proxy packets for a STA before the STA is successfully associated.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] sta arp-nd-proxy before-assoc
```

11.11.73 sta-access-mode

Function

The **sta-access-mode** command binds STA blacklist and STA whitelist profiles to VAP profiles or AP system profiles.

The **undo sta-access-mode** command unbinds STA blacklist and STA whitelist profiles from VAP profiles or AP system profiles.

By default, no STA blacklist and STA whitelist profiles are bound to a VAP profile and an AP system profile.

Format

sta-access-mode { **blacklist** | **whitelist** } *profile-name*

undo sta-access-mode

Parameters

Parameter	Description	Value
blacklist	Specifies a STA blacklist profile.	-
whitelist	Specifies a STA whitelist profile.	-
profile-name	Specifies the names of STA blacklist and whitelist profiles.	The STA blacklist and whitelist profiles must exist.

Views

VAP profile view, AP system profile view

Default Level

2: Configuration level

Usage Guidelines

STA blacklists and whitelists configured by using the **sta-mac** command take effect only after the STA blacklist and whitelist profiles are bound to VAP profiles or AP system profiles using the **sta-access-mode** command.

When STA blacklist and whitelist profiles are bound to different profiles, the effective scope of the STA blacklists and whitelists differs.

- VAP profile: The STA blacklist and whitelist take effect on the corresponding VAP.
- AP system profile: The STA blacklist and whitelist take effect on the corresponding AP.
- VAP profile and AP system profile: A STA cannot go online if it cannot meet any of access requirements.

If a STA blacklist or whitelist profile is bound to a VAP profile or an AP system profile, only one STA blacklist or whitelist profile takes effect in the VAP profile or AP system profile.

Example

Bind the STA blacklist profile **sta-blacklist-profile1** to the VAP profile **vap-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] sta-access-mode blacklist sta-blacklist-profile1
```

11.11.74 sta-blacklist-profile

Function

The **sta-blacklist-profile** command creates a STA blacklist profile or displays the STA blacklist profile view.

The **undo sta-blacklist-profile** command deletes one or more STA blacklist profiles.

By default, no STA blacklist profile is created.

Format

sta-blacklist-profile name *profile-name*

undo sta-blacklist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a STA blacklist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all STA blacklist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MAC address of a STA is in the blacklist, the STA cannot go online. If the STA blacklist profile is not referenced or the MAC address of a STA is not in the blacklist, the STA is allowed to go online.

The configured blacklist takes effect only after the STA blacklist profile is bound to a VAP profile or an AP system profile using the **sta-access-mode** command.

If a STA is added to the blacklist, the system automatically disconnects the STA.

Precautions

If STA blacklist profiles are bound to a VAP profile and an AP system profile, a STA cannot go online when the MAC address of the STA is in either of the STA blacklist profile.

Example

Create the STA blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[HUAWEI-wlan-blacklist-prof-sta-blacklist-profile1]
```

11.11.75 sta-mac

Function

The **sta-mac** command adds the MAC addresses of a STA to the blacklist or whitelist.

The **undo sta-mac** command deletes a specified STA MAC address or all STA MAC addresses from the blacklist or whitelist.

By default, the MAC address of a STA is not added to the blacklist or whitelist.

Format

sta-mac *mac-address* [**description** *description*]

undo sta-mac { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Adds a MAC address to the blacklist or whitelist.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
description	Adds MAC address description to a blacklist or whitelist.	The value is a string of 1 to 80 case-insensitive characters that can include Chinese or Chinese+English characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters.
all	Deletes all MAC addresses from the blacklist or whitelist.	-

Views

STA blacklist profile view, STA whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

If the blacklist function is enabled, all STAs in the blacklist cannot connect to the WLAN.

If the whitelist function is enabled, only STAs in the whitelist can connect to the WLAN.

If a STA is added to the blacklist, the system automatically disconnects the STA.

STAs that have gone online before a whitelist is configured are not forced to go offline even if they are not on the whitelist.

Example

Add the MAC address 00e0-fc12-3456 of a STA to the blacklist profile **sta-blacklist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[HUAWEI-wlan-blacklist-prof-sta-blacklist-profile1] sta-mac 00e0-FC12-3456
```

11.11.76 sta-whitelist-profile

Function

The **sta-whitelist-profile** command creates a STA whitelist profile or displays the STA whitelist profile view.

The **undo sta-whitelist-profile** command deletes one or more STA whitelist profiles.

By default, no STA whitelist profile is created.

Format

sta-whitelist-profile name *profile-name*

undo sta-whitelist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a STA whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Parameter	Description	Value
all	Deletes all STA whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The configured whitelist takes effect only after the STA whitelist profile is bound to a VAP profile or an AP system profile using the **sta-access-mode** command.

If the configured whitelist takes effect, only STAs in the whitelist can access the WLAN.

STAs that have gone online before a whitelist is configured are not forced to go offline even if they are not on the whitelist.

Example

Create the STA whitelist profile **sta-whitelist-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-whitelist-profile name sta-whitelist-profile1
[HUAWEI-wlan-whitelist-prof-sta-whitelist-profile1]
```

11.11.77 wapi asu

Function

The **wapi asu** command specifies an IP address for an authentication server unit (ASU) server.

The **undo wapi asu** command deletes the IP address of the ASU server.

By default, no IP address is specified for the ASU server.

Format

wapi asu ip *ip-address*

undo wapi asu ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the ASU server.	The value is in dotted decimal notation.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If WAPI certificate authentication is configured, an AC sends WAPI authentication packets to the ASU server at the specified IP address.

Prerequisites

If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi asu** command to specify an IP address for the ASU server.

Precautions

The **wapi asu** command helps to determine to which ASU server WAPI packets are sent. Users must ensure the correctness of both ASU certificates and ASU servers; otherwise, they may fail in user authentication.

The system displays the message only when the security profile has been bound to the other profiles.

Example

Specify IP address 10.164.10.10 for the ASU server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi asu ip 10.164.10.10
```

11.11.78 wapi bk

Function

The **wapi bk** command sets the interval for updating a BK and the BK lifetime percentage.

The **undo wapi bk** command restores the default interval for updating a BK and the BK lifetime percentage.

By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.

Format

wapi { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-update-interval* }

undo wapi { **bk-threshold** | **bk-update-interval** }

Parameters

Parameter	Description	Value
bk-threshold *bk-threshold*	Specifies the BK lifetime percentage.	The value is an integer that ranges from 1 to 100.
bk-update-interval *bk-update-interval*	Specifies the interval for updating a BK.	The value is an integer that ranges from 600 to 604800, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can set the intervals for updating a BK to ensure security.

The value obtained by multiplying the interval for updating a BK by the BK lifetime percentage should be greater than or equal to 300 seconds. If the interval for updating a BK is less than 300s, the BK may be updated before negotiation is complete due to low STA performance. In this case, some STAs may be forced offline or cannot go online.

Example

Set the interval for updating a BK to 10000s and the BK lifetime percentage to 80%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi bk-update-interval 10000
Warning: If the product of bk-update-interval and bk-threshold is smaller than 300s, users may be forced
offline. Continue? [Y/N]:y
[HUAWEI-wlan-sec-prof-p1] wapi bk-threshold 80
```

11.11.79 wapi cert-retrans-count

Function

The **wapi cert-retrans-count** command sets the number of retransmissions of certificate authentication packets.

The **undo wapi cert-retrans-count** command restores the default number of retransmissions of certificate authentication packets.

By default, the number of retransmissions is 3.

Format

wapi cert-retrans-count *cert-count*

undo wapi cert-retrans-count

Parameters

Parameter	Description	Value
cert-count	Specifies the number of retransmissions of certificate authentication packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

If WAPI authentication is specified as a security policy, run the **wapi cert-retrans-count** command to set the number of retransmissions of certificate authentication packets.

Example

Set the number of retransmissions of certificate authentication packets to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi cert-retrans-count 5
```

11.11.80 wapi import certificate

Function

The **wapi import certificate** command imports the AC certificate file, certificate of the AC certificate issuer, and ASU certificate file.

The **undo wapi certificate** command deletes the imported AC certificate file, certificate of the AC certificate issuer, or ASU certificate file.

By default, the AC certificate file, certificate of the AC certificate issuer, and ASU certificate file are not imported.

Format

wapi import certificate { **ac** | **asu** | **issuer** } **format pkcs12 file-name** *file-name* **password** *password*

wapi import certificate { **ac** | **asu** | **issuer** } **format pem file-name** *file-name*

undo wapi certificate { **ac** | **asu** | **issuer** }

Parameters

Parameter	Description	Value
ac	Specifies the AC certificate.	-
asu	Specifies the ASU certificate.	-
issuer	Specifies the certificate of a specified certificate issuer.	-
format pkcs12	Imports a certificate in P12 format.	-
format pem	Imports a certificate in PEM format.	-
file-name *file-name*	Specifies a certificate file name, which the complete path of a certificate file must be specified.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) and cannot start or end with double quotation marks (" ") or spaces.

Parameter	Description	Value
password *password*	Specifies the key of the P12 certificate.	The password can be in plain text or cipher text. ● A plain text password is a string of 1 to 32 characters. ● A cipher text password is a string of 48 or 68 characters.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, you can run this command to specify the AC certificate, issuer certificate, and ASU certificate. STAs will fail to be authenticated if you do not run this command. The issuer certificate helps to check whether the AC certificate is modified.
- Before using this command, store the AC certificate and ASU certificate to the storage of the device, and import the certificates and private key using SFTP. Certificates must be X509 V3 certificates and comply with the WAPI standard. Otherwise, certificates cannot be imported.
- After this command is run:
  - When an issuer certificate is configured, the system checks correctness of the AC certificate.
  - If the authentication system uses only two certificates, the issuer certificate and ASU certificate have the same certificate file name and are the same certificate. If the authentication system uses three certificates, the issuer certificate and ASU certificate are different from each other and both must be imported.

NOTE

- The ASU certificate and issuer certificate must be imported.
- Certificates to be imported must be valid and correct.
- If the certificates with the same name but different contents have been imported by other security profiles, delete the earlier certificate first.

Example

Import the AC certificate.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi import certificate ac format pem file-name flash:/local_ac.cer
```

11.11.81 wapi import private-key

Function

The **wapi import private-key** command imports the AC private key file.

The **undo wapi private-key** command deletes the imported AC private key file.

By default, no AC private key file is imported.

Format

wapi import private-key format pkcs12 file-name *file-name* **password** *password*

wapi import private-key format pem file-name *file-name*

undo wapi private-key

Parameters

Parameter	Description	Value
format pkcs12	Imports a private key file in P12 format.	-
format pem	Imports a private key file in PEM format.	-
file-name *file-name*	Specifies the name of a private key file.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) and cannot start or end with double quotation marks (" ") or spaces.

Parameter	Description	Value
password *password*	Specifies the password in the private key file of the P12 format.	The password can be in plain text or cipher text. ● A plain text password is a string of 1 to 32 characters. ● A cipher text password is a string of 48 or 68 characters.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi import private-key** command to specify the private key file for the AC certificate.
- Before using this command, store the AC private key file to the storage medium of the device, and import the private key file using SFTP.
- After this command is used, the system obtains the private key file and establishes the mapping between the certificate and private key.

NOTE

The certificate and private key to be imported must be valid and correct.

Example

Import the AC private key file **ac_key.key**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi import private-key format pem file-name flash:/ac_key.key
```

11.11.82 wapi key-update

Function

The **wapi key-update** command sets the USK and MSK update mode.

The **undo wapi key-update** command restores the default USK and MSK update mode.

By default, USKs and MSKs are updated based on time.

Format

wapi { **usk** | **msk** } **key-update** { **disable** | **time-based** }

undo wapi { **usk** | **msk** } **key-update**

Parameters

Parameter	Description	Value
usk	Indicates USK update.	-
msk	Indicates MSK update.	-
disable	Disables key update.	-
time-based	Indicates time-based update. You can run the **wapi msk** and **wapi usk** commands to respectively set the intervals for updating an MSK and a USK.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- To ensure network security, update keys in a timely manner. There are several key update modes.
- The **wapi key-update** command sets the USK and MSK update mode. If the interval for updating an MSK or a USK is too long, key security cannot be ensured.
- If **disable** is specified, keys will not be updated.

Example

Set the USK update mode to time-based update.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi usk key-update time-based
```

11.11.83 wapi msk

Function

The **wapi msk** command sets the interval for updating an MSK, and number of retransmissions of MSK negotiation packets.

The **undo wapi msk** command restores the default interval for updating an MSK, and number of retransmissions of MSK negotiation packets.

By default, the interval for updating an MSK is 86400s; the number of retransmissions of MSK negotiation packets is 3.

Format

wapi { **msk-update-interval** *msk-interval* | **msk-retrans-count** *msk-count* }

undo wapi { **msk-update-interval** | **msk-retrans-count** }

Parameters

Parameter	Description	Value
msk-update-interval *msk-interval*	Specifies the interval for updating an MSK. When the MSK update mode is set to time-based update using the **wapi key-update** command, the interval for updating an MSK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
msk-retrans-count *msk-count*	Specifies the number of retransmissions of MSK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends.

Example

Set the interval for updating an MSK to 10000s, and number of retransmissions of MSK negotiation packets to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi msk key-update time-based
[HUAWEI-wlan-sec-prof-p1] wapi msk-update-interval 10000
[HUAWEI-wlan-sec-prof-p1] wapi msk-retrans-count 5
```

11.11.84 wapi sa-timeout

Function

The **wapi sa-timeout** command sets the security association (SA) timeout period for key encryption.

The **undo wapi sa-timeout** command restores the default SA timeout period for key encryption.

The default SA timeout period for key encryption is 60s.

Format

wapi sa-timeout *sa-time*

undo wapi sa-timeout

Parameters

Parameter	Description	Value
sa-time	Specifies the SA timeout period.	The value is an integer that ranges from 1 to 255, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can prolong the WAPI timeout period to increase the authentication success ratio.

Example

Set the SA timeout period to 100s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi sa-timeout 100
```

11.11.85 wapi source interface

Function

The **wapi source interface** command configures a source interface for an AC to communicate with an ASU server.

The **undo wapi source interface** command cancels the source interface for an AC to communicate with an ASU server.

By default, no source interface is configured for an AC to communicate with an ASU server.

Format

wapi source interface { **vlanif** *vlan-id* | **loopback** *loopback-number* }

undo wapi source interface

Parameters

Parameter	Description	Value
vlanif *vlan-id*	Configures a VLANIF interface as the source interface.	The value is an integer that ranges from 1 to 4094.
loopback *loopback-number*	Configures a loopback interface as the source interface.	The value is an integer that ranges from 0 to 1023.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In WLAN applications, to use WAPI authentication and enable socket communication between an AC and an ASU server, the AC needs a WAPI source IP address using which all packets are sent to the ASU server.

Prerequisites

An IP address has been assigned to the specified loopback or VLANIF interface.

Precautions

The IP address of the WAPI source interface on the AC must be on the same network segment as the IP address of the ASU server. If no WAPI source interface is configured, the IP address of the AC source interface is used as the source IP address for sending WAPI packets to the WAPI server by default.

Example

Configure a VLANIF interface as the source interface for the AC to communicate with the ASU server.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.10.1 24
[HUAWEI-Vlanif100] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi source interface Vlanif 100
```

11.11.86 wapi usk

Function

The **wapi usk** command sets the interval for updating a USK, and number of retransmissions of USK negotiation packets.

The **undo wapi usk** command restores the default interval for updating a USK, and number of retransmissions of USK negotiation packets.

By default, the interval for updating a USK is 86400s; the number of retransmissions of USK negotiation packets is 3.

Format

wapi { **usk-update-interval** *usk-interval* | **usk-retrans-count** *usk-count* }

undo wapi { **usk-update-interval** | **usk-retrans-count** }

Parameters

Parameter	Description	Value
usk-update-interval *usk-interval*	Specifies the interval for updating a USK. When the USK update mode is set to time-based update using the **wapi key-update** command, the interval for updating a USK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
usk-retrans-count *usk-count*	Specifies the number of retransmissions of USK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends.

Example

Set the interval for updating a USK to 10000s, and number of retransmissions of USK negotiation packets to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wapi usk key-update time-based
[HUAWEI-wlan-sec-prof-p1] wapi usk-update-interval 10000
[HUAWEI-wlan-sec-prof-p1] wapi usk-retrans-count 5
```

11.11.87 weak-iv-detect quiet-time

Function

The **weak-iv-detect quiet-time** command sets the quiet time for an AP to report the detected weak IV attacks to the AC.

The **undo weak-iv-detect quiet-time** command restores the default quiet time for an AP to report the detected weak IV attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected weak IV attacks to the AC.

Format

weak-iv-detect quiet-time *quiet-time-value*

undo weak-iv-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected weak IV attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repeated alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time to 300 seconds for an AP to report the detected weak IV attacks to the AC.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect weak-iv enable
[HUAWEI-wlan-group-radio-default/0] quit
[HUAWEI-wlan-ap-group-default] quit
[HUAWEI-wlan-view] wids-profile name default
[HUAWEI-wlan-wids-prof-default] weak-iv-detect quiet-time 300
```

11.11.88 wep default-key

Function

The **wep default-key** command sets the default key ID for WEP authentication or encryption.

The **undo wep default-key** command restores the default key ID for WEP authentication or encryption.

By default, key 0 is used for WEP authentication or encryption.

Format

wep default-key *key-id*

undo wep default-key

Parameters

Parameter	Description	Value
key-id	Specifies the default key ID.	The key ID must exist.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- A maximum of four WEP keys can be configured, and only one WEP key is used for authentication and encryption. This command specifies which key to use.
- After a key ID is specified, the specified key is used for authentication or encryption.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same.
- The system displays the message only when the security profile has been bound to the other profiles.

Example

Set the default key ID to 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wep default-key 1
```

11.11.89 wep key

Function

The **wep key** command sets a WEP key.

The **undo wep key** command deletes the specified key.

By default, WEP-40 is used. The default username and password are available in *WLAN Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

wep key *key-id* { **wep-40** | **wep-104** | **wep-128** } { { **pass-phrase** | **hex** } *key-value* | **dot1x** }

undo wep key *key-id*

Parameters

Parameter	Description	Value
key-id	Specifies the key ID.	The value is an integer that ranges from 0 to 3.
wep-40	Configures WEP-40 authentication.	-
wep-104	Configures WEP-104 authentication.	-
wep-128	Configures WEP-128 authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number.	-

Parameter	Description	Value

key-value	Specifies a password in cipher text.	The password can be in plain text or cipher text.
		- A plain text password is a string of case-sensitive characters.
		  - If WEP-40 is used, the WEP key is 10 hexadecimal characters or 5 ASCII characters.
		  - If WEP-104 is used, the WEP key is 26 hexadecimal characters or 13 ASCII characters.
		  - If WEP-128 is used, the WEP key is 32 hexadecimal characters or 16 ASCII characters.
		- A cipher text password is a string of 48 or 68 characters.
		A password cannot contain the space and double quotation mark (") at the same time. When the password contains a space, add the double quotation mark (") to the beginning and end of the string when entering the password. For example, if the password is **YsHsjx**

Parameter	Description	Value
		202206, enter **"YsHsjx 202206"**.
dot1x	Specifies dynamic WEP encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To connect to a WLAN device in WEP shared-key authentication mode or dynamic WEP mode, run the **wep key** command to set a WEP key.

NOTE

If the key is in hexadecimal notation, you can enter hexadecimal characters without entering 0x.

Precautions

The system displays the message only when the security profile has been bound to the other profiles.

Example

Configure a WEP key and its ID.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] wep key 1 wep-128 hex 12345678123456781234567812345678
```

11.11.90 wids attack detect

Function

(AP group radio view) The **wids attack detect enable** command enables attack detection on all specified radios in an AP group.

(AP group radio view) The **wids attack detect disable** command disables attack detection on all specified radios in an AP group.

(AP group radio view) The **undo wids attack detect enable** command restores the default attack detection configuration on all specified radios in an AP group.

(AP radio view) The **wids attack detect enable** command enables attack detection on an AP radio.

(AP radio view) The **wids attack detect disable** command disables attack detection on an AP radio.

(AP radio view) The **undo wids attack detect** command cancels the configuration of the attack detection function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, attack detection is disabled on an AP radio; flood attack detection, weak IV attack detection, and spoofing attack detection are disabled on radios in the AP group; and brute force key cracking attack detection is enabled on radios in the AP group.

Format

wids attack detect { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** } { **enable** | **disable** }

undo wids attack detect { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

Parameters

Parameter	Description	Value
all	Indicates all attack detection functions.	-
flood	Indicates flood attack detection.	-
weak-iv	Indicates weak IV attack detection.	-
spoof	Indicates spoofing attack detection.	-
wpa-psk	Indicates brute force attack detection in WPA-PSK authentication.	-
wpa2-psk	Indicates brute force attack detection in WPA2-PSK authentication.	-
wapi-psk	Indicates brute force attack detection in WAPI-PSK authentication.	-
wep-share-key	Indicates brute force attack detection in shared key authentication.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor and prevent malicious or unintentional attacks on WLANs in real time, network administrators can enable the following attack detection functions based on actual requirements:

- **flood**: indicates flood attack detection used to detect whether an AP receives a large number of packets of the same type in a short period.
- **weak-iv**: indicates weak IV attack detection used to detect whether weak IV is used for WEP encryption on a WLAN.
- **spoof**: indicates spoofing attack detection used to detect whether a potential attacker pretends to be an AP to broadcast Deauthentication and Disassociation packets.
- **wpa-psk**, **wpa2-psk**, **wapi-psk**, or **wep-share-key**: indicates brute force attack detection. If the WPA-PSK, WPA2-PSK, WAPI-PSK, or WEP-SK security policy is configured on a WLAN, brute force attack detection can be enabled to increase the time required for password cracking and improve password security.

Precautions

- The configuration in the AP radio view has a higher priority than that in the AP group radio view.
- After the attack detection function is enabled using the **wids attack detect enable** command, the detected data is stored only on the local device. To report the data to the iMaster NCE-Campus, run the **collect-item user-data enable** command in the SMI view to enable the device to report intelligent O&M data to the iMaster NCE-Campus.
- If no attack detection function is enabled in the AP radio view, the configuration in the AP group radio view is inherited. If any attack detection function is enabled in the AP radio view, the configuration in the AP group radio view does not take effect and the configuration in the AP radio view is inherited. For example, when all attack detection functions are enabled in the AP group radio view:
  - If no attack detection function is enabled in the AP radio view, the configuration in the AP group radio view takes effect. That is, all attack detection functions are enabled on the AP radio.
  - If spoofing attack detection is enabled in the AP radio view, the configuration in the AP radio view takes effect. That is, only spoofing attack detection is enabled on the AP radio.

Follow-up Procedure

Run the **undo dynamic-blacklist disable** command to enable the dynamic blacklist function.

Run the **attack-device trap enable** command to enable the alarm function for attack detection.

Example

Enable brute force attack detection in WPA-PSK authentication on radio 0 in AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids attack detect wpa-psk enable
```

11.11.91 wids manual-contain

Function

The **wids manual-contain** command manually contains specified devices.

The **undo wids manual-contain** command disables containment of specified devices.

By default, no device is manually contained.

Format

wids manual-contain device-mac *device-mac*

undo wids manual-contain { **all** | **device-mac** *device-mac* }

Parameters

Parameter	Description	Value
device-mac *device-mac*	Specifies the MAC address of a device to be contained.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Contains all devices.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **wids manual-contain** command in the WLAN view to manually contain a specified device in a complicated environment.

Precautions

Wireless bridges are not contained.

Example

Contain the AP with the MAC address 00e0-fc04-0004.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids manual-contain device-mac 00e0-fc04-0004
```

11.11.92 wids contain enable

Function

(AP group radio view) The **wids contain enable** command enables rogue or interference device containment on all specified radios in an AP group.

(AP group radio view) The **undo wids contain enable** command disables rogue or interference device containment on all specified radios in an AP group.

(AP radio view) The **wids contain enable** command enables rogue or interference device containment on an AP radio.

(AP radio view) The **undo wids contain enable** command cancels the configuration of the rogue or interference device containment function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, rogue or interference device containment is disabled on AP radios.

Format

wids contain enable

undo wids contain enable

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rogue or interference devices pose serious security threats to enterprise networks.

After the containment mode is set against rogue or interference APs, the monitor AP uses the identity of the rogue or interference AP to broadcast deauthentication frames to forcibly disconnect STAs. To prevent the STAs from connecting to the rogue or interference AP again, the monitor AP will periodically and continuously send deauthentication frames.

After the containment mode is set against rogue or interference STAs or ad-hoc devices, the monitor AP uses the MAC address of a rogue or interference device to continuously send unicast deauthentication frames.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

After the **keep-service enable** command is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disconnect STAs from the AP. Therefore, service holding upon CAPWAP link disconnection does not take effect in this case.

After command **keep-service enable allow new-access** is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disable the AP from allowing access of new STAs. Therefore, the function of enabling an offline AP to allow access of new STAs does not take effect in this case.

Follow-up Procedure

Run the **contain-mode** command to set the rogue or interference device containment mode.

Example

Enable rogue or interference device containment on radio 0 in AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids contain enable
```

11.11.93 wids device detect enable

Function

(AP group radio view) The **wids device detect enable** command enables device detection on all specified radios in an AP group.

(AP group radio view) The **undo wids device detect enable** command disables device detection on all specified radios in an AP group.

(AP radio view) The **wids device detect enable** command enables device detection on an AP radio.

(AP radio view) The **undo wids device detect enable** command cancels the configuration of the device detection function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, device detection is disabled on AP radios.

Format

wids device detect enable

undo wids device detect enable

Parameters

None

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the wireless device detection function is enabled, the monitoring AP detects information about wireless devices in its coverage range and reports the information to the AC. The AC determines whether unauthorized devices exist on the WLAN.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

After the **keep-service enable** command is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disconnect STAs from the AP. Therefore, service holding upon CAPWAP link disconnection does not take effect in this case.

After command **keep-service enable allow new-access** is executed, if the **wids device detect enable** and **wids contain enable** commands are configured to enable rogue or interference device detection and containment, the AP will continue providing data services after going offline. However, the AC considers the AP as a rogue or interference device and adds it to the containment list. The containment mechanism will disable the AP from allowing access of new STAs. Therefore, the function of enabling an offline AP to allow access of new STAs does not take effect in this case.

After the device detection function is enabled using this command, the detected data is stored only on the local device. To report the data to the iMaster NCE-Campus, run the **collect-item user-data enable** command in the SMI view to enable the device to report intelligent O&M data to the iMaster NCE-Campus.

Example

Enable device detection on radio 0 in AP group **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] wids device detect enable
```

11.11.94 wids-whitelist-profile (WLAN view)

Function

The **wids-whitelist-profile** command creates a WIDS whitelist profile and enters the WIDS whitelist profile view.

The **undo wids-whitelist-profile** command deletes a WIDS whitelist profile.

By default, the system provides the WIDS whitelist profile **default**.

Format

wids-whitelist-profile name *profile-name*

undo wids-whitelist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" "). Only the default profile **default** is supported.
all	Deletes all WIDS whitelist profiles.	The default WIDS whitelist profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After WIDS/WIPS is enabled, rogue APs can be detected and countered. However, there may be APs of other vendors or on other networks working in the existing signal coverage areas. If these APs are countered, their services will be affected. To prevent this situation, configure an authorized AP list, including an authorized MAC address list, OUI list, and SSID list. If an unauthorized AP is detected but matches the authorized AP list, the AP is considered an authorized AP and will not be countered. After you create and a WIDS whitelist profile using the **wids-whitelist-profile** command, run the **permit-ap** command to configure an authorized AP list.

Follow-up Procedure

Run the **wids-whitelist-profile (WIDS profile view)** command to bind the WIDS whitelist profile to a WIDS profile so that the WIDS whitelist profile can take effect.

Example

Create the WIDS whitelist profile **default**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-whitelist-profile name default
[HUAWEI-wlan-wids-whitelist-default]
```

11.11.95 wids-profile (WLAN view)

Function

The **wids-profile** command creates a WIDS profile and enters the WIDS profile view.

The **undo wids-profile** command deletes a WIDS profile.

By default, the system provides the WIDS profile **default**.

You can run the **display wids-profile** command to view the configuration of the WIDS profile **default**.

Format

wids-profile name *profile-name*

undo wids-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" "). Only the default profile **default** is supported.
all	Deletes all WIDS profiles.	The default WIDS profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the WIDS function on a device to detect and counter rogue devices on a WLAN. The WIDS function also enables the device to detect attacks and add devices launching the attacks to a dynamic blacklist. Packets sent from the blacklisted devices will be rejected to protect authorized users.

After you create and a WIDS profile using the **wids-profile** command, you can configure APs to detect and counter rogue or interference devices, and detect attacks in the profile.

Follow-up Procedure

Run the **wids-profile (AP group view and AP view)** command to bind the WIDS profile to an AP group or AP so that the WIDS profile can take effect.

Example

Create the WIDS profile **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-profile name office
[HUAWEI-wlan-wids-prof-office]
```

11.11.96 wids-spoof-profile (WLAN view)

Function

The **wids-spoof-profile** command creates a WIDS spoof SSID profile and enters the WIDS spoof SSID profile view.

The **undo wids-spoof-profile** command deletes a WIDS spoof SSID profile.

By default, the system has a default WIDS spoof SSID profile **default**.

Format

wids-spoof-profile name *profile-name*

undo wids-spoof-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS spoof SSID profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" "). Only the default profile **default** is supported.
all	Deletes all WIDS spoof SSID profiles.	The default WIDS spoof SSID profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN services are available in public places, such as banks and airports. Users can connect to the WLANs after associating with corresponding SSIDs. If a rogue AP is deployed and provides spoofing SSIDs similar to authorized SSIDs, the users may be misled and connect to the rogue AP, which brings security risks. To address this problem, configure a fuzzy matching rule to identify spoofing SSIDs. After you create and a WIDS spoof SSID profile using the **wids-spoof-profile** command, run the **spoof-ssid** command to configure a fuzzy matching rule to identify spoofing SSIDs.

Follow-up Procedure

Run the **wids-spoof-profile (WIDS profile view)** command to bind the WIDS spoof SSID profile to a WIDS profile to make the WIDS spoof SSID profile take effect.

Example

Create the WIDS spoof SSID profile **office**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wids-spoof-profile name office
[HUAWEI-wlan-wids-spoof-office]
```

11.11.97 work-mode

Function

(AP group radio view) The **work-mode** command sets the working mode of all specified AP radios in an AP group.

(AP group radio view) The **undo work-mode** command restores the default working mode of all specified AP radios in an AP group.

(AP radio view) The **work-mode** command sets the working mode of a specified radio on an AP in an AP group.

(AP radio view) The **undo work-mode** command restores the working mode of a specified radio on an AP to the working mode configured in the AP group radio view.

By default, AP radios work in normal mode.

Format

work-mode { **monitor** [[**proxy-scan**] **dual-band-scan enable**] | **normal** }

undo work-mode

Parameters

Parameter	Description	Value
monitor	Indicates the monitor mode.	-
dual-band-scan enable	Indicates inter-band scanning.	-
proxy-scan dual-band-scan enable	Indicates proxy scanning.	-
normal	Indicates the normal mode.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP can work in two modes:

- **normal**: indicates the normal mode.
  - If air scan functions (such as WIDS, spectrum analysis, and terminal location) are disabled on a radio, the radio is used to transmit common WLAN services.
  - If air scan functions (such as WIDS, spectrum analysis, and terminal location) are enabled on a radio, the radio transmits common WLAN services and also provides the monitoring function. A transient increase in the WLAN service latency may occur, which does not affect network access. However, if any latency-sensitive service (such as videoconferencing) is running, it is recommended that a separate radio be used for air scan.
- **monitor**: indicates the monitor mode.

  In this mode, the radio can only transmit WLAN services scanned by the air interface but cannot transmit common WLAN services.

Precautions

- The change of the radio working mode can lead to service interruption. Users cannot associate with the AP when its radio works in monitor mode.
- The configuration in the AP radio view has a higher priority than that in the AP group radio view.
- In monitor mode, the working channels and power of AP radios change at any time. In this situation, the working channels and power of the AP radios display as **-**.

- Radio 1 does not support inter-band scanning.
- The switching between the proxy scanning mode and other modes may lead to an AP restart.
- If the inter-band or proxy scanning configuration is delivered to an AP that does not support these two modes, the monitor mode takes effect on the AP.

Example

Set the working mode of radio 0 in AP group **default** to **monitor**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] radio 0
[HUAWEI-wlan-group-radio-default/0] work-mode monitor
Warning: Modify the work mode may cause business interruption, continue?[y/n]
:y
```

11.11.98 wpa ptk-update enable

Function

The **wpa ptk-update enable** command enables periodic PTK update in WPA or WPA2 authentication and encryption.

The **undo wpa ptk-update enable** command disables periodic PTK update.

By default, periodic PTK update is disabled.

Format

wpa ptk-update enable

undo wpa ptk-update enable

Parameters

None

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In WPA or WPA2 authentication and encryption, a Pairwise Transient Key (PTK) is generated at the key negotiation stage to encrypt unicast radio packets. To ensure secure encryption, enable periodic PTK update so that the AP and STA use a new PTK to encrypt radio packets after a regular interval.

Precautions

When periodic PTK update is implemented, some STAs may encounter service interruptions or go offline due to individual problems.

Follow-up Procedure

Run the **wpa ptk-update ptk-update-interval** command to configure the periodic PTK update interval.

Example

Enable the periodic PTK update function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name example
[HUAWEI-wlan-sec-prof-example] wpa ptk-update enable
```

11.11.99 wpa ptk-update ptk-update-interval

Function

The **wpa ptk-update ptk-update-interval** command configures an interval for updating PTKs in WPA or WPA2 authentication and encryption.

The **undo wpa ptk-update ptk-update-interval** command restores the default PTK update interval.

By default, the interval for updating PTKs is 43200 seconds.

Format

wpa ptk-update ptk-update-interval *ptk-rekey-interval*

undo wpa ptk-update ptk-update-interval

Parameters

Parameter	Description	Value
ptk-rekey-interval	Specifies the PTK update interval.	The value is an integer ranging from 43200 to 86400, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure secure encryption during WPA or WPA2 authentication, enable periodic PTK update. You can run this command to configure the PTK update interval. A smaller interval indicates faster PTK update and more secure data encryption. However, if the PTK update interval is set too small, the STA and AP implement more negotiations, affecting the throughput.

Precautions

The configured periodic PTK update interval takes effect only after you enable the periodic PTK update function using the **wpa ptk-update enable** command.

Example

Set the periodic PTK update interval to 50,000 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name example
[HUAWEI-wlan-sec-prof-example] wpa ptk-update ptk-update-interval 50000
```

11.12 WLAN WDS Configuration Commands

The WDS function is not supported by the following AP models:

- AirEngine series APs
- Central APs (including matching RUs)

11.12.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.12.2 dhcp trust port (WDS profile view)

Function

The **dhcp trust port** command enables a DHCP trusted port in a WDS profile.

The **undo dhcp trust port** command disables a DHCP trusted port in a WDS profile.

By default, a DHCP trusted port is enabled in a WDS profile.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

After a DHCP trusted port is enabled in a WDS profile and the WDS profile is applied to an AP, the AP receives the DHCP OFFER, ACK, and NAK packets sent by authorized DHCP servers and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

Example

Enable a DHCP trusted port in the WDS profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] dhcp trust port
```

11.12.3 display references wds-profile

Function

The **display references wds-profile** command displays reference information about a WDS profile.

Format

display references wds-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wds-profile** command to check reference information about a WDS profile.

Example

Display reference information about the WDS profile **test**.

```
<HUAWEI> display references wds-profile name test
------------------------------------------------------------------------------
Reference type     Reference name                          Reference radio  WLAN ID
------------------------------------------------------------------------------
AP group          group-1                            Radio-0         13
AP group          group-1                            Radio-0         14
------------------------------------------------------------------------------
Total: 2
```

Table 11-249 Description of the **display references wds-profile name** command output

Parameter	Description
Reference type	Type of the profile to which the WDS profile is bound.
Reference name	Name of the profile to which the WDS profile is bound. ● Run the **wds-profile radio** command in the AP group view or view of the AP with a specified ID to apply a WDS profile. ● Run the **wds-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view to apply a WDS profile.
Reference radio	AP radio to which the WDS profile is applied.
WLAN ID	WLAN ID to which the WDS profile is bound.

11.12.4 display references wds-whitelist-profile

Function

The **display references wds-whitelist-profile** command displays reference information about a WDS whitelist profile.

Format

display references wds-whitelist-profile name *whitelist-name*

Parameters

Parameter	Description	Value
name *whitelist-name*	Displays reference information about a specified WDS whitelist profile.	The WDS whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wds-whitelist-profile** command to check reference information about a specified WDS whitelist profile.

Example

Display reference information about the WDS whitelist profile **test**.

```
<HUAWEI> display references wds-whitelist-profile name test
------------------------------------------------------------------------------
Reference type                Reference name
------------------------------------------------------------------------------
AP group                    profile-1
AP group                    profile-2
------------------------------------------------------------------------------
Total: 2
```

Table 11-250 Description of the **display references wds-whitelist-profile** command output

Parameter	Description
Reference type	Type of the profile to which the WDS whitelist profile is bound.
Reference name	Name of the profile to which the WDS whitelist profile is bound. Run the **wds-whitelist-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view to apply a WDS whitelist profile.

11.12.5 display wds-profile

Function

The **display wds-profile** command displays reference or configuration information about a WDS profile.

Format

display wds-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all WDS profiles.	-
name *profile-name*	Displays information about a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds-profile** command to view the number of times a WDS profile is referenced or configuration information of a specified WDS profile.

Example

Display reference information about all WDS profiles.

```
<HUAWEI> display wds-profile all
--------------------------------------------------------------------------------
Profile name                   Reference
--------------------------------------------------------------------------------
default                      0
test                         2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-251 Description of the **display wds-profile all** command output

Item	Description
Profile name	WDS profile name. To create a WDS profile, run the **wds-profile** command.
Reference	Number of times a WDS profile is referenced.

Display information about the WDS profile **test**.

```
<HUAWEI> display wds-profile name test
------------------------------------------------------------------------------
WDS name                   : HUAWEI-WLAN-WDS
WDS work mode              : root
Security profile           : test
DHCP trust port            : enable
ND trust port              : enable
MU-MIMO                    : disable
Tagged vlan                : -
Priority map trust         : DSCP
Priority map mode          : DSCP map 802.11e
                             0-7 map 0
                             8-15 map 1
                             16-23 map 2
                             24-31 map 3
                             32-39 map 4
                             40-47 map 5
                             48-55 map 6
                             56-63 map 7
Beacon 2.4G rate(Mbps)     : 1                          Beacon 5G rate(Mbps)       :
6
------------------------------------------------------------------------------
```

Table 11-252 Description of the **display wds-profile name** command output

Item	Description
WDS name	WDS name. To set a WDS name, run the **wds-name** command.
WDS work mode	WDS working mode. To set the WDS working mode, run the **wds-mode** command.
Security profile	Security profile bound to a WDS profile. To bind a security profile to a WDS profile, run the **security-profile (WDS profile view)** command.

Item	Description
DHCP trust port	Whether to enable a DHCP trusted port in a WDS profile. - enable: A DHCP trusted port is enabled. - disable: A DHCP trusted port is disabled. To enable a DHCP trusted port in a WDS profile, run the **dhcp trust port (WDS profile view)** command.
ND trust port	Whether to enable an ND trusted port in a WDS profile. - enable: An ND trusted port is enabled. - disable: An ND trusted port is disabled. To enable an ND trusted port in a Mesh profile, run the **nd trust port (WDS profile view)** command.
MU-MIMO	Whether the MU-MIMO function is enabled. To configure the parameter, run the **mu-mimo disable** command.
Tagged vlan	VLAN configured in a WDS profile. To configure a VLAN in a WDS profile, run the **vlan tagged (WDS profile view)** command.
Priority map trust	Priority mapping trusted by the WDS air interface. To configure the parameter, run the **priority-map trust (WDS profile view)** command.
Priority map mode	Mapping from DSCP priorities to 802.11e user priorities on the WDS air interface. To configure the parameter, run the **priority-map dscp (WDS profile view)** command.
Beacon 2.4G rate	Transmit rate of 2.4 GHz management frames configured in the WDS profile. To configure the parameter, run the **beacon-2g-rate** command.

Item	Description
Beacon 5G rate	Transmit rate of 5 GHz management frames configured in the WDS profile. To configure the parameter, run the **beacon-5g-rate** command.

11.12.6 display wds-whitelist-profile

Function

The **display wds-whitelist-profile** command displays reference or configuration information about a WDS whitelist profile.

Format

display wds-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all WDS whitelist profiles.	-
name *whitelist-name*	Displays information about a specified WDS whitelist profile.	The WDS whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds-whitelist-profile** command to view the number of times a WDS whitelist profile is referenced or MAC addresses added in a specified WDS whitelist profile.

Example

Display reference information about all WDS whitelist profiles.

```
<HUAWEI> display wds-whitelist-profile all
--------------------------------------------------------------------------------
```

```
Profile name                    Reference
------------------------------------------------------------------------------
default                           0
test                              2
------------------------------------------------------------------------------
Total: 2
```

Table 11-253 Description of the **display wds-whitelist-profile all** command output

Item	Description
Profile name	Name of a WDS whitelist profile. To create a WDS whitelist profile, run the **wds-whitelist-profile** command.
Reference	Number of times a WDS whitelist profile is referenced.

Display information about the WDS whitelist profile **test**.

```
<HUAWEI> display wds-whitelist-profile name test
------------------------------------------------------------------------------
WDS whitelist name: test
WDS whitelist MAC list information:
------------------------------------------------------------------------------
Index     MAC
------------------------------------------------------------------------------
0         00e0-fcb1-56a0
------------------------------------------------------------------------------
Total: 1
```

Table 11-254 Description of the **display wds-whitelist-profile name** command output

Item	Description
Index	WDS whitelist ID in a WDS whitelist profile.
MAC	MAC address on a WDS whitelist. To add a MAC address to a WDS whitelist, run the **peer-ap mac (WDS whitelist profile view)** command.

11.12.7 display wds vap

Function

The **display wds vap** command displays information about a WDS VAP.

Format

display wds vap { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**wds-name** *wds-name*]

display wds vap { **all** | **wds-name** *wds-name* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all WDS VAPs in a specified AP group.	The AP group must exist.
ap-id *ap-id*	Displays information about WDS VAPs on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about WDS VAPs on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about WDS VAPs of a specified AP radio.	The radio ID must exist.
wds-name *wds-name*	Displays information about WDS VAPs of a specified WDS name.	The WDS name must exist.
all	Displays information about all WDS VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds vap** command to display information about a WDS VAP.

Example

Display information about all WDS VAPs.

```
<HUAWEI> display wds vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name      RfID WID        WDS name            BSSID          WDS links
--------------------------------------------------------------------------------
1     AP2           0  14          wds                 00e0-fc12-3456  0
1     AP2           0  13          wds                 00e0-fc12-3457  0
0     AP1           0  14          wds                 00e0-fc12-3467  1
0     AP1           0  13          wds                 00e0-fc12-3468  1
```

```
--------------------------------------------------------------------------------------
Total: 4
```

Table 11-255 Description of the **display wds vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
WDS name	WDS name. To set a WDS name, run the **wds-name** command.
BSSID	MAC address of a VAP.
WDS links	Number of WDS links.

11.12.8 display wlan wds link

Function

The **display wlan wds link** command displays information about a WDS link.

Format

display wlan wds link { **all** | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] | **wds-profile** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WDS links.	-
ap-id *ap-id*	Displays information about WDS links on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about WDS links on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about WDS links of a specified AP radio.	The radio ID must exist.
wds-profile *profile-name*	Displays information about WDS links in a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan wds link** command to view information about a WDS link.

Example

Display information about all WDS links.

```
<HUAWEI> display wlan wds link all
Rf   : radio ID              Dis  : coverage distance(100m)
Ch   : channel               Per  : drop percent(%)
TSNR : total SNR(dB)         P-   : peer
WDS  : WDS mode              Re   : retry ratio(%)
RSSI : RSSI(dBm)             MaxR : max RSSI(dBm)
----------------------------------------------------------------------------------------------------
APName  P-APName        Rf Dis   Ch   WDS     P-Status    RSSI  MaxR  Per  Re   TSNR  SNR(Ch0~3:dB)
----------------------------------------------------------------------------------------------------
AP_1                  1  3    36   root    -          -77   -40   100  100  0    -/-/-/-
AP_2                  1  3    36   root    -          -72   -40   56   99   23   21/19/-/-
----------------------------------------------------------------------------------------------------
Total: 2
```

Table 11-256 Description of the **display wlan wds link** command output

Item	Description
APName	Name of the local AP.
P-APName	Name of the peer AP.
Rf	Radio ID of the local AP.
Dis	Radio coverage distance parameter of the local AP.
Ch	Working channel of a WDS link.
WDS	WDS role of the local AP.
P-Status	Status of the peer AP.
RSSI	RSSI of the peer AP.
MaxR	Maximum RSSI threshold of a WDS link.
Per	Packet error ratio of a WDS link.
Re	Packet retransmission ratio of a WDS link.

Item	Description
TSNR	Total SNR of a WDS link.
SNR(Ch0~3:dB)	SNR of each spatial stream of a WDS link.

11.12.9 nd trust port (WDS profile view)

Function

The **nd trust port** command enables an ND trusted port in a WDS profile.

The **undo nd trust port** command disables an ND trusted port in a WDS profile.

By default, an ND trusted port is enabled in a WDS profile.

Format

nd trust port

undo nd trust port

Parameters

None

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

After an ND trusted port is enabled in a WDS profile and the WDS profile is applied to an AP, the AP receives valid ND protocol packets and forwards the packets to STAs or peer APs so that the STAs can obtain valid IPv6 addresses and go online.

Example

Enable an ND trusted port in the WDS profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] nd trust port
```

11.12.10 peer-ap mac (WDS whitelist profile view)

Function

The **peer-ap mac** command adds MAC addresses of neighboring APs that are allowed to connect to an AP to a WDS whitelist profile.

The **undo peer-ap mac** command deletes the MAC addresses of neighboring APs from a WDS whitelist profile.

By default, no MAC address of a neighboring AP is added to a WDS whitelist profile.

Format

peer-ap mac *mac-address*

undo peer-ap mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a neighboring AP to be added to a WDS whitelist profile.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS whitelist profile is created, you can run the **peer-ap mac** command to add neighboring APs' MAC addresses to the profile.

If a WDS whitelist profile is bound to a WDS profile, only APs with MAC addresses in the WDS whitelist profile can access the local AP, and other APs are denied access.

Precautions

A maximum of six MAC addresses can be added to a WDS whitelist profile.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **00e0-fc01-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-whitelist-profile name whitelist
[HUAWEI-wlan-wds-whitelist-whitelist] peer-ap mac 00e0-fc01-0001
[HUAWEI-wlan-wds-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

11.12.11 priority-map dscp (WDS profile view)

Function

The **priority-map dscp** command configures the mapping from DSCP priorities to 802.11e user priorities on the WDS air interface.

The **undo priority-map dscp** command restores the default mapping from DSCP priorities to 802.11e user priorities on the WDS air interface.

Table 11-257 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 11-257 Mapping from DSCP priorities to 802.11e user priorities

DSCP Priority	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot11e *dot11e-value*	Specifies the 802.11e user priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

On a WDS network, you can run this command to configure the mapping from DSCP priorities to 802.11e user priorities on the WDS air interface of an AP.

Example

Map DSCP priorities 0-6 to 802.11e user priority 0 on the WDS air interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] priority-map dscp 0 to 6 dot11e 0
```

11.12.12 priority-map trust (WDS profile view)

Function

The **priority-map trust** command configures the priority mapping to be trusted by the WDS air interface.

The **undo priority-map trust** command restores the default priority mapping to be trusted by the WDS air interface.

By default, the WDS air interface trusts the mapping from DSCP priorities to 802.11e user priorities.

Format

priority-map trust { **dot1p** | **dscp** }

undo priority-map trust

Parameters

Parameter	Description	Value
dot1p	Indicates that the WDS air interface trusts the mapping from 802.1p priorities to 802.11e user priorities.	-
dscp	Indicates that the WDS air interface trusts the mapping from DSCP priorities to 802.11e user priorities.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

On a WDS network, when 802.1p or DSCP priorities in data packets need to be mapped to 802.11e user priorities and the packets are transmitted through a WDS link, run this command.

Example

Configure the WDS air interface to trust the mapping from 802.1p priorities to 802.11e user priorities.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] priority-map trust dot1p
```

11.12.13 security-profile (WDS profile view)

Function

The **security-profile** command binds a security profile to a WDS profile.

The **undo security-profile** command restores the default security profile bound to a WDS profile.

By default, the security profile **default-wds** is bound to a WDS profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the security profile bound to a WDS profile.	The security profile must exist.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a WDS profile is applied to an AP radio to set up WDS links, the WDS profile must have a security profile bound to ensure WDS link security.

Precautions

After a security profile is bound to a WDS profile, the authentication policy and encryption mode in the security profile cannot be changed, but the authentication key can be changed.

A WDS profile can only have one security profile bound. If you run the command multiple times in the same WDS profile view, the latest configuration overwrites the old one.

Example

Create the security profile **sec** and set the security policy to WPA2+PSK+AES. Create the WDS profile **test** and bind the security profile to the WDS profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name sec
[HUAWEI-wlan-sec-prof-sec] security wpa2 psk pass-phrase YsHsjx_202206 aes
[HUAWEI-wlan-sec-prof-sec] quit
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] security-profile sec
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.14 vlan tagged (WDS profile view)

Function

The **vlan tagged** command adds one or a group of VLANs to a WDS profile in tagged mode.

The **undo vlan tagged** command deletes VLANs from a WDS profile.

By default, no VLAN is configured in a WDS profile.

NOTE

Currently, VLANs can only be added to a WDS profile in tagged mode.

Format

vlan tagged { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan tagged { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the tagged VLAN ID. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters determine a VLAN range. If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is added to the WDS profile in tagged mode. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	- The value of *vlan-id1* is an integer that ranges from 1 to 4094. - The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all tagged VLANs from a WDS profile.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Adding VLANs to a WDS profile is equivalent to adding hybrid interfaces to a VLAN. After one or a group of VLANs is added to a WDS profile, the WDS link forwards only the packets with these VLAN IDs from STAs and peer APs.

NOTE

A maximum of 256 VLANs can be added to a WDS profile.

Example

Create the WDS profile **test** and add VLANs 3, 4, 5, 6, 10, and 12 to the WDS profile in **tagged** mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] vlan tagged 3 to 6 10 12
```

11.12.15 wds-mode

Function

The **wds-mode** command sets the WDS mode in a WDS profile.

By default, the WDS mode in a WDS profile is **leaf**.

Format

wds-mode { **root** | **middle** | **leaf** }

Parameters

Parameter	Description	Value
root	Sets the WDS mode to root.	-
middle	Sets the WDS mode to middle.	-
leaf	Sets the WDS mode to leaf.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To connect an AP to an AC through WDS links, use this command to set the WDS mode for an AP radio based on the location of the AP on a WDS network.

In the downlink direction, a root node can connect to a middle or leaf node, and a middle node can connect to a leaf node. A leaf node is the termination node of a WDS link.

Precautions

After changing the WDS mode in a WDS profile, reset the APs using the profile to make the changed WDS mode take effect.

Example

Create the WDS profile **test** and set the WDS mode of the profile to **middle**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] wds-mode middle
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.16 wds-name

Function

The **wds-name** command sets a WDS name for a WDS profile.

The **undo wds-name** command deletes the WDS name of a WDS profile.

By default, the WDS name of a WDS profile is **HUAWEI-WLAN-WDS**.

Format

wds-name *name*

undo wds-name

Parameters

Parameter	Description	Value
name	Specifies the character string that indicates the WDS name.	The value is a string of 1 to 32 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

A WDS name is similar to an SSID. On a WDS network, an AP radio discovers WDS services provided by other APs based on the WDS name.

Each WDS profile must have a WDS name. The default WDS name of a WDS profile is **HUAWEI-WLAN-WDS**. You can run the **wds-name** command to set a WDS name for a WDS profile.

Example

Create the WDS profile **test** and set the WDS name of the profile to **bridge**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] wds-name bridge
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.17 wds-profile

Function

The **wds-profile** command creates a WDS profile or displays the WDS profile view.

The **undo wds-profile** command deletes a WDS profile.

By default, the system provides the WDS profile **default**.

Format

wds-profile name *profile-name*

undo wds-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WDS profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all WDS profiles. **NOTE** The WDS profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each WDS profile must have a WDS name. The default WDS name of a WDS profile is **HUAWEI-WLAN-WDS**. You can run the **wds-name** command to set a WDS name for a WDS profile.

Example

Create the WDS profile **test** and set the WDS name of the profile to **bridge**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-profile name test
[HUAWEI-wlan-wds-prof-test] wds-name bridge
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.18 wds-profile radio

Function

The **wds-profile radio** command binds a WDS profile to an AP group or AP.

The **undo wds-profile radio** command deletes a WDS profile from an AP group or AP.

By default, no WDS profile is bound to an AP group or AP.

Format

wds-profile *profile-name* **radio** { **all** | *radio-id* }

undo wds-profile radio { **all** | *radio-id* }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the WDS profile bound to an AP or AP group.	The WDS profile must exist.
all	Binds a WDS profile to all AP radios.	-
radio-id	Binds a WDS profile to a specified AP radio.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS profile is bound to an AP or AP group, the AP radio will generate a WDS VAP to provide WDS services. The WDS VAP provides hidden SSIDs for WDS nodes to set up connections.

Prerequisites

A WDS profile has been created and configured properly.

Precautions

Among the VAPs created after a WDS profile is bound to an AP radio, the VAPs with the WLAN IDs 13 and 14 cannot be occupied.

An AP radio can only have one WDS profile bound.

Since the WLAN WDS and Mesh functions are mutually exclusive, the WDS and Mesh profiles cannot be applied to an AP radio at the same time.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] wds-profile test radio 0
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.19 wds-profile (AP group radio view or AP radio view)

Function

The **wds-profile** command binds a WDS profile to an AP radio.

The **undo wds-profile** command unbinds a WDS profile from an AP radio.

By default, no WDS profile is bound to an AP radio.

Format

wds-profile *profile-name*

undo wds-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the WDS profile bound to an AP radio.	The WDS profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS profile is bound to an AP radio, the radio will generate a WDS VAP to provide WDS services. The WDS VAP provides hidden SSIDs for WDS nodes to set up connections.

Prerequisites

A WDS profile has been created and configured properly.

Precautions

Among the VAPs created after a WDS profile is bound to an AP radio, the VAPs with the WLAN IDs 13 and 14 cannot be occupied.

An AP radio can only have one WDS profile bound.

This command has the same function as the **wds-profile radio** command. You can use either of them.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-profile test
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.12.20 wds-whitelist-profile

Function

The **wds-whitelist-profile** command creates a WDS whitelist profile or displays the WDS whitelist profile view.

The **undo wds-whitelist-profile** command deletes a WDS whitelist profile.

By default, no WDS whitelist profile is available in the system.

Format

wds-whitelist-profile name *whitelist-name*

undo wds-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
name *whitelist-name*	Specifies the name of a WDS whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all WDS whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a WDS whitelist profile is created using the **wds-whitelist-profile** command, you can run the **peer-ap mac (WDS whitelist profile view)** command in the WDS whitelist profile view to add MAC addresses of peer APs that are allowed to set up WDS links with the local AP to the profile.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **00e0-fc01-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-whitelist-profile name whitelist
[HUAWEI-wlan-wds-whitelist-whitelist] peer-ap mac 00e0-fc01-0001
[HUAWEI-wlan-wds-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

11.12.21 wds-whitelist-profile (AP group radio view or AP radio view)

Function

The **wds-whitelist-profile** command binds a WDS whitelist profile to an AP radio.

The **undo wds-whitelist-profile** command unbinds a WDS whitelist profile from an AP radio.

By default, no WDS whitelist profile is bound to an AP radio.

Format

wds-whitelist-profile *whitelist-name*

undo wds-whitelist-profile

Parameters

Parameter	Description	Value
whitelist-name	Specifies the name of the WDS whitelist profile bound to an AP radio.	The WDS whitelist profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After a WDS whitelist profile is applied to an AP radio, the AP radio can only set up WDS links with neighboring APs whose MAC addresses are in the WDS whitelist profile. If no WDS whitelist profile is bound to an AP radio, the AP radio can establish WDS links with any neighboring APs.

NOTE

On a WDS network, a root or middle node controls subnode access by MAC addresses added to the WDS whitelist profile. However, a leaf node does not require a whitelist.

An AP radio can only have one WDS whitelist profile bound. If you run the command multiple times on the same AP radio, the latest configuration overwrites the old one.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **00e0-fc01-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wds-whitelist-profile name whitelist
[HUAWEI-wlan-wds-whitelist-whitelist] peer-ap mac 00e0-fc01-0001
[HUAWEI-wlan-wds-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

11.13 WLAN Mesh Configuration Commands

11.13.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.13.2 dhcp trust port (Mesh profile view)

Function

The **dhcp trust port** command enables a DHCP trusted port in a Mesh profile.

The **undo dhcp trust port** command disables a DHCP trusted port in a Mesh profile.

By default, a DHCP trusted port is enabled in a Mesh profile.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

After a DHCP trusted port is enabled in a Mesh profile and the Mesh profile is applied to an AP, the AP receives the DHCP OFFER, ACK, and NAK packets sent by authorized DHCP servers and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

Example

Enable a DHCP trusted port in the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] dhcp trust port
```

11.13.3 display mesh-profile

Function

The **display mesh-profile** command displays reference or configuration information about Mesh profiles.

Format

display mesh-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all Mesh profiles.	-
name *profile-name*	Displays reference information about a specified Mesh profile.	The Mesh profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mesh-profile** command to view the number of times a Mesh profile is referenced or configuration information of a specified Mesh profile.

Example

Display reference information about all Mesh profiles.

```
<HUAWEI> display mesh-profile all
--------------------------------------------------------------------------------
Profile name                     Reference
--------------------------------------------------------------------------------
default                          0
test                             2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-258 Description of the **display mesh-profile all** command output

Item	Description
Profile name	Mesh profile name. To configure this parameter, run the **mesh-profile** command.
Reference	Number of times a Mesh profile is referenced.

Display information about the Mesh profile **test**.

```
<HUAWEI> display mesh-profile name test
--------------------------------------------------------------------------------
Mesh handover profile          :
Security profile               : default-mesh
Mesh ID                        : HUAWEI-WLAN-MESH
Max link number                : 32
Link RSSI threshold(dBm)       : -90
Link report interval(s)        : 30
Link aging timeout(s)          : 60
FWA switch                     : enable
FWA EDCA mode                  : manual
DHCP trust port                : enable
ND trust port                  : enable
Tagged VLAN                    : 10
Priority map trust             : DSCP
Priority map mode              : DSCP map 802.11e
                                 0-7 map 0
                                 8-15 map 1
                                 16-23 map 2
                                 24-31 map 3
                                 32-39 map 4
                                 40-47 map 5
                                 48-55 map 6
                                 56-63 map 7
Client mode                    : disable
```

```
Beacon 2.4G rate(Mbps)           : 1
Beacon 5G rate(Mbps)             : 6
Beacon 6G rate(Mbps)             : 6
------------------------------------------------------------------------------
Mesh WMM EDCA client parameters:
------------------------------------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit
AC_VO  10      4       7      0
AC_VI  4       3       2      94
AC_BE  10      4       3      0
AC_BK  10      4       7      0
------------------------------------------------------------------------------
```

Table 11-259 Description of the **display mesh-profile name** command output

Item	Description
Mesh handover profile	Mesh handover profile bound to a Mesh profile. To configure this parameter, run the **mesh-handover-profile (Mesh profile view)** command.
Security profile	Security profile bound to a Mesh profile. To configure this parameter, run the **security-profile (Mesh profile view)** command.
Mesh ID	Mesh ID of a Mesh profile. To configure this parameter, run the **mesh-id** command.
Max link number	Maximum number of Mesh links allowed on an AP. To configure this parameter, run the **max-link-number** command.
Link RSSI threshold	RSSI threshold of a Mesh link. To configure this parameter, run the **link-rssi-threshold** command.
Link report interval	Interval for reporting Mesh link information. To configure this parameter, run the **link-report-interval** command.
Link aging timeout	Aging time of a Mesh link. To configure this parameter, run the **link-aging-time** command.

Item	Description
FWA switch	FWA status in a Mesh profile. ● enable: The FWA is enabled. ● disable: The FWA is disabled. To configure this parameter, run the **fwa enable** command.
FWA EDCA mode	EDCA mode. ● auto: indicates the automatic mode. ● manual: indicates the manual mode. To configure this parameter, run the **fwa wmm edca-mode** command.
DHCP trust port	Whether to enable a DHCP trusted port in a Mesh profile. ● enable: A DHCP trusted port is enabled. ● disable: A DHCP trusted port is disabled. To configure this parameter, run the **dhcp trust port (Mesh profile view)** command.
ND trust port	Whether to enable an ND trusted port in a Mesh profile. ● enable: An ND trusted port is enabled. ● disable: An ND trusted port is disabled. To configure this parameter, run the **nd trust port (Mesh profile view)** command.
Tagged VLAN	VLAN configured in a Mesh profile. To configure this parameter, run the **vlan tagged (Mesh profile view)** command.
Priority map trust	Priority mapping trusted by the Mesh air interface. To configure this parameter, run the **priority-map trust (Mesh profile view)** command.

Item	Description
Priority map mode	Mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface. To configure this parameter, run the **priority-map dscp (Mesh profile view)** command.
Client mode	Whether to enable the Mesh client mode. - enable: The Mesh client mode is enabled. - disable: The Mesh client mode is disabled.
Beacon 2.4G rate	Transmit rate of 2.4 GHz management frames configured in the Mesh profile. To configure this parameter, run the **beacon-2g-rate** command.
Beacon 5G rate	Transmit rate of 5 GHz management frames configured in the Mesh profile. To configure this parameter, run the **beacon-5g-rate** command.
Beacon 6G rate	Transmit rate of 6 GHz management frames configured in the Mesh profile. To configure this parameter, run the **beacon-6g-rate** command.
AC_VO	AC_VO packets.
AC_VI	AC_VI packets.
AC_BE	AC_BE packets.
AC_BK	AC_BK packets.
ECWmax	Exponent form of the maximum contention window (ECWmax). ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **fwa wmm edca-client** command.
ECWmin	Exponent form of the minimum contention window (ECWmin). ECWmin and ECWmax determine the average backoff time. To configure this parameter, run the **fwa wmm edca-client** command.

Item	Description
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure this parameter, run the **fwa wmm edca-client** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel. To configure this parameter, run the **fwa wmm edca-client** command.

11.13.4 display mesh-whitelist-profile

Function

The **display mesh-whitelist-profile** command displays reference or configuration information about a Mesh whitelist profile.

Format

display mesh-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all Mesh whitelist profiles.	-
name *whitelist-name*	Displays information about a specified Mesh whitelist profile.	The Mesh whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mesh-whitelist-profile** command to view the number of times a Mesh whitelist profile is referenced or MAC addresses added in a specified Mesh whitelist profile.

Example

Display reference information about all Mesh whitelist profiles.

```
<HUAWEI> display mesh-whitelist-profile all
--------------------------------------------------------------------------------
Profile name                          Reference
--------------------------------------------------------------------------------
default                              0
test                                 2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-260 Description of the **display mesh-whitelist-profile all** command output

Item	Description
Profile name	Name of a Mesh whitelist profile. To configure this parameter, run the **mesh-whitelist-profile** command.
Reference	Number of times a Mesh whitelist profile is referenced.

Display information about the Mesh whitelist profile **test**.

```
<HUAWEI> display mesh-whitelist-profile name test
--------------------------------------------------------------------------------
Mesh whitelist name: test
Mesh whitelist MAC list information:
--------------------------------------------------------------------------------
Index     MAC
--------------------------------------------------------------------------------
0         00e0-fc76-e360
1         00e0-fc74-9640
--------------------------------------------------------------------------------
Total: 2
```

Table 11-261 Description of the **display mesh-whitelist-profile name** command output

Item	Description
Index	Mesh whitelist ID in a Mesh whitelist profile.

Item	Description
MAC	MAC address on a Mesh whitelist. To configure this parameter, run the **peer-ap mac (Mesh whitelist profile view)** command.

11.13.5 display mesh vap

Function

The **display mesh vap** command displays information about a Mesh VAP.

Format

display mesh vap { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**mesh-id** *mesh-id*]

display mesh vap { **all** | **mesh-id** *mesh-id* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all Mesh VAPs in a specified AP group.	The AP group must exist.
ap-id *ap-id*	Displays information about Mesh VAPs on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about Mesh VAPs on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about Mesh VAPs of a specified AP radio.	The radio ID must exist.
mesh-id *mesh-id*	Displays information about Mesh VAPs of a specified Mesh ID.	The Mesh ID must exist.
all	Displays information about all Mesh VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about a specified Mesh VAP or all Mesh VAPs.

Example

Display information about all Mesh VAPs.

```
<HUAWEI> display mesh vap all
WID : WLAN ID
----------------------------------------------------------------------------------------------
AP ID AP name       RfID WID  Mesh ID          BSSID          Auth type  Mesh links
----------------------------------------------------------------------------------------------
1     AP2           0    16   mesh             00E0-FC74-964F WPA2-PSK   0
0     AP1           0    16   mesh             00E0-FC74-964F Open       0
----------------------------------------------------------------------------------------------
Total: 2
```

Table 11-262 Description of the **display mesh vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
Mesh ID	Mesh ID. To configure this parameter, run the **mesh-id** command.
BSSID	MAC address of a VAP.
Auth type	Authentication type.
Mesh links	Number of Mesh links.

11.13.6 display references mesh-profile

Function

The **display references mesh-profile** command displays reference information about a Mesh profile.

Format

display references mesh-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Mesh profile.	The Mesh profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references mesh-profile** command to check reference information about a Mesh profile.

Example

Display reference information about the Mesh profile **test**.

```
<HUAWEI> display references mesh-profile name test
--------------------------------------------------------------------------------
Reference type     Reference name                       Reference radio  WLAN ID
--------------------------------------------------------------------------------
AP group           test1                                Radio-0          16
--------------------------------------------------------------------------------
Total: 1
```

Table 11-263 Description of the **display references mesh-profile** command output

Item	Description
Reference type	Type of the profile to which the Mesh profile is bound.
Reference name	Name of the profile to which the Mesh profile is bound. - Run the **mesh-profile radio** command in the AP group view or view of the AP with a specified ID to apply a Mesh profile. - Run the **mesh-profile (AP group radio view or AP radio view)** command in the AP group radio view to apply a Mesh profile.
Reference radio	AP radio to which a Mesh profile is applied.

Item	Description
WLAN ID	WLAN ID to which a Mesh profile is bound.

11.13.7 display references mesh-whitelist-profile

Function

The **display references mesh-whitelist-profile** command displays reference information about a Mesh whitelist profile.

Format

display references mesh-whitelist-profile name *whitelist-name*

Parameters

Parameter	Description	Value
name *whitelist-name*	Displays reference information about a specified Mesh whitelist profile.	The Mesh whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references mesh-whitelist-profile** command to check reference information about a specified Mesh whitelist profile.

Example

Display reference information about the Mesh whitelist profile **test**.

```
<HUAWEI> display references mesh-whitelist-profile name test
--------------------------------------------------------------------------------
Reference type                  Reference name
--------------------------------------------------------------------------------
AP group                        default
--------------------------------------------------------------------------------
Total: 1
```

Table 11-264 Description of the **display references mesh-whitelist-profile** command output

Item	Description
Reference type	Type of the profile by which a Mesh whitelist profile is referenced.
Reference name	Name of the profile by which a Mesh whitelist profile is referenced. To configure this parameter, run the **mesh-whitelist-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view.

11.13.8 display wlan mesh link

Function

The **display wlan mesh link** command displays information about a Mesh link.

Format

display wlan mesh link { **all** | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] | **mesh-profile** *profile-name* | **peer-mac** *peer-mac* }

Parameters

Parameter	Description	Value
all	Displays information about all Mesh links.	-
ap-id *ap-id*	Displays information about Mesh links on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about Mesh links on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about Mesh links of a specified AP radio.	The radio ID must exist.
mesh-profile *profile-name*	Displays information about Mesh links in a specified Mesh profile.	The Mesh profile must exist.
peer-mac *peer-mac*	Displays information about the Mesh link on a specified peer MAC address.	The MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan mesh link** command to view information about a Mesh link.

Example

Display information about all Mesh links.

```
<HUAWEI> display wlan mesh link all
Rf   : radio ID              Dis  : coverage distance(100m)
Ch   : channel               Per  : drop percent(%)
TSNR : total SNR(dB)         P-   : peer
Mesh : Mesh mode             Re   : retry ratio(%)
RSSI : RSSI(dBm)             MaxR : max RSSI(dBm)
--------------------------------------------------------------------------------------------------------------------------
----
APName          P-APName        P-APMAC         Rf Dis   Ch      Mesh     P-Status       RSSI  MaxR  Per  Re
TSNR  SNR(dB)
Tx(Mbps)    Rx(Mbps)
--------------------------------------------------------------------------------------------------------------------------
----
00e0-fcdd-ef80  area_2         00e0-fc04-b500  0  3     6       node     normal         -40   -20   1    17   59
56/55
54          54
area_2          00e0-fcdd-ef80  00e0-fcdd-ef80  0  3     6       portal  normal         -48   -7    0    18   45
34/35/44
54          54
--------------------------------------------------------------------------------------------------------------------------
----
Total: 2
```

Display information about the Mesh link on a specified peer MAC address.

```
<HUAWEI> display wlan mesh link peer-mac 00e0-fc04-b500
Rf   : radio ID              Dis  : coverage distance(100m)
Ch   : channel               Per  : drop percent(%)
TSNR : total SNR(dB)         P-   : peer
Mesh : Mesh mode             Re   : retry ratio(%)
RSSI : RSSI(dBm)             MaxR : max RSSI(dBm)
--------------------------------------------------------------------------------------------------------------------------
-----------------
IP Address               : 192.168.200.121
--------------------------------------------------------------------------------------------------------------------------
-----------------
Link Rf  : 1
Channel utilization       : 45
Channel interference      : 20
--------------------------------------------------------------------------------------------------------------------------
-------
APName          P-APName        P-APMAC         Rf Dis   Ch      Mesh     P-Status       RSSI  MaxR  Per  Re
TSNR  SNR(dB)
Tx(Mbps)    Rx(Mbps)   LinkStatus
--------------------------------------------------------------------------------------------------------------------------
-------
00e0-fcdd-ef80  area_2         00e0-fc04-b500  0  3     6       node     normal         -40   -20   1    17   59
56/55
```

```
54         54        active
00e0-fcdd-0000  area_2        00e0-fc04-b500  0  3     6       node    normal         -41   -20   1    17   59
56/55
54         54        inactive
-----------------------------------------------------------------------------------------------------------------------------------------
-------
```

Table 11-265 Description of the **display wlan mesh link** command output

Item	Description
APName	Name of the local AP.
P-APMAC	MAC address of the peer AP.
P-APName	Name of the peer AP.
Rf	Radio ID of the local AP.
Dis	Radio coverage distance parameter of the local AP.
Ch	Working channel of a Mesh link.
Mesh	Mesh role of the local AP. ● portal: mesh-portal ● node: mesh-node ● node(leaf): mesh-node (leaf mode)
P-Status	Status of the peer AP.
RSSI	RSSI of the peer AP.
MaxR	Maximum RSSI threshold of a Mesh link.
Per	Packet error ratio of a Mesh link.
Re	Packet retransmission ratio of a Mesh link.
TSNR	Total SNR of Mesh links.
SNR(dB)	SNR of each spatial stream of a Mesh link.
Tx(Mbps)	Transmit rate.
Rx(Mbps)	Receive rate.
LinkStatus	Link status. ● active: active in Mesh handover mode ● inactive: inactive in Mesh handover mode ● -: client mode or a common Mesh network

Item	Description
IP Address	IP address of a vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.
Link Rf	Radio used by the vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.
Channel utilization	Channel utilization of the vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.
Channel interference	Co-channel interference of the vehicle-mounted AP. This item is displayed only when the specified MAC address indicates a vehicle-mounted Fat AP.

11.13.9 display wlan mesh route

Function

The **display wlan mesh route** command displays AP routing information on a Mesh network.

Format

display wlan mesh route { **ap-id** *ap-id* | **ap-name** *ap-name* | **all** }

Parameters

Parameter	Description	Value
ap-id	Displays routing information of the AP with a specified ID on a Mesh network.	The AP ID must exist.
ap-name	Displays routing information of the AP with a specified name on a Mesh network.	The AP name must exist.
all	Displays all APs' routing information on a Mesh network.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view specified or all APs' routing information on a Mesh network, which helps you locate faults on the Mesh network.

Example

Display all APs' routing information on a Mesh network.

```
<HUAWEI> display wlan mesh route all
-------------------------------------------------------------------------------
AP name/MAC/Mesh role/Radio          Next-hop name/MAC/Mesh role/Radio
-------------------------------------------------------------------------------
ap1/00e0-fc74-9640/MP/0             ap2/00e0-fc76-e360/MPP/0
-------------------------------------------------------------------------------
Total: 1
```

Table 11-266 Description of the **display wlan mesh route** command output

Item	Description
AP name	Name of an AP.
MAC	MAC address of the AP.
Mesh role	Role of the AP on the Mesh network.
Radio	Radio ID of the AP.
Next-hop name	Name of the next-hop AP.

11.13.10 fwa wmm edca-client

Function

The **fwa wmm edca-client** command configures EDCA parameters used by the remote AP to negotiate with the AT.

The **undo fwa wmm edca-client** command restores the default EDCA parameters used by the remote AP to negotiate with the AT.

Table 11-267 lists the default EDCA parameter settings.

Table 11-267 Default EDCA parameter settings

Packet Type	Parameters	Description
AC_VO	ECWmax	3
	ECWmin	2
	AIFSN	2
	TXOPLimit	47
AC_VI	ECWmax	4
	ECWmin	3
	AIFSN	2
	TXOPLimit	94
AC_BE	ECWmax	10
	ECWmin	4
	AIFSN	3
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	4
	AIFSN	7
	TXOPLimit	0

Format

fwa wmm edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo fwa wmm edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-

Parameter	Description	Value
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be smaller than the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the transmission opportunity limit (TXOPLimit), which determines the maximum duration in which a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide differentiated priorities to the packets and different capabilities to compete for channels. In this way, differentiated services are implemented.

Table 11-268 describes the EDCA parameters.

Table 11-268 EDCA parameter description

Parameter	Meaning
Arbitration Interframe Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. Together, they determine the average backoff time. Large ECWmin and ECWmax values mean a long average backoff time for the STA and a low STA priority.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can only send one data frame every time it preempts a channel.

Precautions

- The EDCA parameters configured using the **fwa wmm edca-client** command take effect only after you set the EDCA mode to manual mode using the **fwa wmm edca-mode manual** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.

You need to configure EDCA parameters according to actual scenarios. **Table 11-269** shows the configuration of EDCA parameters in voice scenarios, and **Table 11-270** shows the configuration in voice and video hybrid scenarios.

Table 11-269 Recommended configuration of EDCA parameters in voice scenarios

Packet Type	Parameters	Description
AC_VO	ECWmax	4
	ECWmin	2
	AIFSN	2
	TXOPLimit	0

Packet Type	Parameters	Description
AC_VI	ECWmax	5
	ECWmin	3
	AIFSN	5
	TXOPLimit	0
AC_BE	ECWmax	10
	ECWmin	6
	AIFSN	5
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	8
	AIFSN	12
	TXOPLimit	0

Table 11-270 Recommended configuration of EDCA parameters in voice and video hybrid scenarios

Packet Type	Parameters	Description
AC_VO	ECWmax	4
	ECWmin	2
	AIFSN	2
	TXOPLimit	0
AC_VI	ECWmax	5
	ECWmin	3
	AIFSN	5
	TXOPLimit	0
AC_BE	ECWmax	10
	ECWmin	6
	AIFSN	12
	TXOPLimit	0
AC_BK	ECWmax	10
	ECWmin	8

Packet Type	Parameters	Description
	AIFSN	12
	TXOPLimit	0

Example

Configure EDCA parameters of AC_VO packets used by the remote AP to negotiate with the AT.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] fwa wmm edca-mode manual
[HUAWEI-wlan-mesh-prof-test] fwa wmm edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit
0
```

11.13.11 fwa wmm edca-mode

Function

The **fwa wmm edca-mode** command sets the Enhanced Distributed Channel Access (EDCA) mode.

By default, the automatic EDCA mode is used.

Format

fwa wmm edca-mode { **auto** | **manual** }

Parameters

Parameter	Description	Value
auto	Sets the EDCA mode to automatic. In automatic EDCA mode, ATs automatically adjust EDCA parameters based on the number of ATs connecting to the remote AP.	-

Parameter	Description	Value
manual	Sets the EDCA mode to manual. In manual mode, you can run the **fwa wmm edca-client** command to configure EDCA parameters of the AT. The remote AP negotiates with the AT according to the configured parameters.	-

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where the AT connects to the remote AP through Mesh links, if the EDCA mode is **auto**, ATs automatically adjust EDCA parameters based on the number of ATs connecting to the remote APif the EDCA mode is **manual**, you can run the **fwa wmm edca-client** command to configure EDCA parameters of the AT. The remote AP then negotiates with the AT according to the configured parameters.

NOTE

- The **fwa wmm edca-mode** command takes effect only after the FWA mode is enabled in the Mesh profile using the **fwa enable** command.
- In automatic EDCA mode, the EDCA parameters manually configured using the **fwa wmm edca-client** command do not take effect on the AP.
- This command applies only to scenarios where the AT connects to the remote AP through Mesh links.

Example

Set the EDCA mode to auto.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] fwa wmm edca-mode auto
```

11.13.12 fwa enable

Function

The **fwa enable** command enables fixed wireless access (FWA) in a Mesh profile.

The **undo fwa enable** command disables FWA in a Mesh profile.

By default, FWA is disabled in a Mesh profile.

FWA is not supported by AirEngine series APs.

Format

fwa enable

undo fwa enable

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An outdoor Access Terminal (AT) needs to set up a Mesh link with a remote AP to provide network access for downlink STAs connected to the AT. In this case, configure the Mesh service on the remote AP and enable FWA in the Mesh profile so that the AT can connect to the remote AP.

Configuration Impact

The FWA configuration has the following impacts:

- FWA and vehicle-ground fast link handover are mutually exclusive in a Mesh profile.
- The default value of the parameter *link-num* in the **max-link-number** *link-num* command is 32, and the value is in the range of 1 to 32.
- The default RSSI threshold of a Mesh link is fixed at –90 dBm, which cannot be changed using the **link-rssi-threshold** command.
- The Mesh service configuration can be performed without the need to bind a Mesh whitelist profile to the Mesh profile.
- A radio bound to the Mesh profile allows access from only ATs. If ATs are not used, do not enable FWA, which prevents a Mesh service configuration failure.

Example

Enable FWA for the Mesh profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] fwa enable
```

Disable FWA for the Mesh profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] undo fwa enable
```

11.13.13 link-aging-time

Function

The **link-aging-time** command sets the aging time of a Mesh link.

The **undo link-aging-time** command restores the default aging time of a Mesh link.

The default aging time of a Mesh link is 10 seconds.

Format

link-aging-time *aging-time*

undo link-aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of a Mesh link.	The value is an integer that ranges from 5 to 60, in seconds.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

If a Mesh node cannot receive keepalive packets from a neighboring node for a period of time greater than or equal to the aging time of a Mesh link, the Mesh node considers the Mesh link disconnected and will reselect a link.

In a fast changing radio environment, if the aging time of a Mesh link is set to a small value, Mesh links may be frequently disconnected or reselected, causing network flapping. If the aging time of a Mesh link is set to a large value, a Mesh node cannot reselect Mesh links in a timely manner, causing service interruption. Therefore, you need to configure a proper aging time for Mesh links based on actual situations.

Example

Set the aging time of a Mesh link to 10s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] link-aging-time 10
```

11.13.14 link-report-interval

Function

The **link-report-interval** command sets the interval at which an MP reports Mesh link information to the AC.

The **undo link-report-interval** command restores the default interval at which an MP reports Mesh link information to the AC.

By default, an MP reports Mesh link information to the AC at an interval of 30 seconds.

Format

link-report-interval *report-interval*

undo link-report-interval

Parameters

Parameter	Description	Value
report-interval	Specifies the interval at which an MP reports Mesh link information to the AC.	The value is an integer that ranges from 5 to 3600, in seconds. The default value is 30.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is unstable, an MP may frequently send Mesh link establishment or teardown information to the AC, affecting AC's processing of user services. To solve this problem, run the **link-report-interval** command to configure an MP to periodically send Mesh link information to the AC. After the command is executed, the MP sends link information to the AC only at specified intervals, ensuring normal processing of user services.

Example

Set the interval at which an MP reports Mesh link information to the AC to 20s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] link-report-interval 20
```

11.13.15 link-rssi-threshold

Function

The **link-rssi-threshold** command sets the received signal strength indicator (RSSI) threshold of a mesh link.

The **undo link-rssi-threshold** command restores the default RSSI threshold of a mesh link.

By default, the RSSI threshold of a mesh link is -75 dBm. After the FWA mode is enabled in a Mesh profile, the RSSI threshold of a Mesh link is fixed as -90 dBm.

Format

link-rssi-threshold *threshold-value*

undo link-rssi-threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the RSSI threshold of a mesh link.	The value is an integer that ranges from -90 to -20, in dBm. The default value is -75. After the FWA mode is enabled in a Mesh profile, the RSSI threshold of a Mesh link is fixed as -90 dBm.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSSI threshold of a mesh link indicates the minimum RSSI of the mesh link. If the RSSI of an MP that joins a WMN is lower than the RSSI threshold configured using the **link-rssi-threshold** command, the routing information table of the mesh link is updated and routing information about the MP is deleted.

The RSSI threshold of a mesh link depends on the distance between two MPs that establish the mesh link. If the two MPs are far from each other, a smaller RSSI threshold is recommended. If the two MPs are close to each other, a larger RSSI threshold is recommended.

Example

Set the RSSI threshold of mesh links to -60 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] link-rssi-threshold -60
```

11.13.16 max-link-number

Function

The **max-link-number** command sets the maximum number of mesh links that can be established between APs.

The **undo max-link-number** command restores the default maximum number of mesh links that can be established between APs.

By default, a maximum of eight mesh links can be established between APs. After you enable FWA for a mesh profile using the **fwa enable** command, a maximum of 32 mesh links can be established between APs by default.

Format

max-link-number *link-num*

undo max-link-number

Parameters

Parameter	Description	Value
link-num	Specifies the maximum number of mesh links that can be established between APs.	The value is an integer that ranges from 1 to 32. **NOTE** After you enable FWA for a mesh profile using the **fwa enable** command, the default value of *link-num* is 32, and the value ranges from 1 to 32.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP sets up too many Mesh links with neighboring APs, network indicators, such as the throughput cannot meet customer needs, affecting user experience. To improve user experience, you can run the **max-link-number** command to set the maximum number of mesh links that can be established between APs according to actual situations.

Impact

If the number of mesh links of an AP has reached the maximum, the AP does not set up new mesh links with neighboring APs.

Example

Set the maximum number of mesh links that can be established between APs to **3**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] max-link-number 3
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.17 mesh-id

Function

The **mesh-id** command sets a Mesh ID for a Mesh profile.

The **undo mesh-id** command restores the Mesh ID of a Mesh profile to the default value.

By default, the Mesh ID of a Mesh profile is **HUAWEI-WLAN-MESH**.

Format

mesh-id *name*

undo mesh-id

Parameters

Parameter	Description	Value
name	Specifies the Mesh ID of a Mesh profile.	The value is a string of 1 to 32 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

The Mesh ID of a Mesh profile is similar to the SSID. On a Mesh network, AP radios discover available Mesh services of other APs based on the Mesh ID.

Each Mesh profile must have a Mesh ID. The default Mesh ID of a Mesh profile is **HUAWEI-WLAN-MESH**. You can run the **mesh-id** command to set a Mesh ID for a Mesh profile.

Example

Create the Mesh profile **test** and set the Mesh ID of the profile to **mesh-net**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-id mesh-net
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.18 mesh-profile

Function

The **mesh-profile** command creates a Mesh profile or displays the Mesh profile view.

The **undo mesh-profile** command deletes a Mesh profile.

By default, the system provides the Mesh profile **default**.

Format

mesh-profile name *profile-name*

undo mesh-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Mesh profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Mesh profiles. **NOTE** The Mesh profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh profile is applied to an AP radio, Mesh VAPs are created on the radio.

Each Mesh profile must have a Mesh ID. The default Mesh ID of a Mesh profile is **HUAWEI-WLAN-MESH**. You can run the **mesh-id** command to set a Mesh ID for a Mesh profile.

Example

Create the Mesh profile **test** and set the Mesh ID of the profile to **mesh-net**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-id mesh-net
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.19 mesh-profile radio

Function

The **mesh-profile radio** command binds a Mesh profile to an AP group or AP.

The **undo mesh-profile radio** command unbinds a Mesh profile from an AP group or AP.

By default, no Mesh profile is bound to an AP group or AP.

Format

mesh-profile *profile-name* **radio** { **all** | *radio-id* }

undo mesh-profile radio { **all** | *radio-id* }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the Mesh profile bound to an AP group or AP.	The Mesh profile must exist.
all	Binds a Mesh profile to all AP radios.	-
radio-id	Binds a Mesh profile to a specified AP radio.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh profile is bound to an AP group or AP, a Mesh VAP will be generated on AP radios to provide Mesh services for users.

Prerequisites

A Mesh profile has been created and properly configured.

Precautions

Among the VAPs created after a Mesh profile is bound to a radio, the VAP with the WLAN ID 16 cannot be occupied.

An AP radio can only have one Mesh profile bound.

Since the WLAN WDS and Mesh functions are mutually exclusive, the WDS and Mesh profiles cannot be applied to an AP radio at the same time.

Example

Bind the Mesh profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] mesh-profile test radio 0
```

11.13.20 mesh-profile (AP group radio view or AP radio view)

Function

The **mesh-profile** command binds a Mesh profile to an AP radio.

The **undo mesh-profile** command unbinds a Mesh profile from an AP radio.

By default, no Mesh profile is bound to an AP radio.

Format

mesh-profile *profile-name*

undo mesh-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the Mesh profile bound to an AP radio.	The Mesh profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh profile is bound to an AP group radio or an AP radio, a Mesh VAP will be generated on the specified AP radio to provide Mesh services for users.

Prerequisites

A Mesh profile has been created and properly configured.

Precautions

Among the VAPs created after a Mesh profile is bound to a radio, the VAP with the WLAN ID 16 cannot be occupied.

An AP radio can only have one Mesh profile bound.

This command has the same function as the **mesh-profile radio** command. You can use either of them.

Example

Bind the Mesh profile **test** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-profile test
```

11.13.21 mesh-role

Function

The **mesh-role** command configures a Mesh role for an AP in the AP system profile.

The **undo mesh-role** command restores the default Mesh role of an AP in the AP system profile.

By default, the Mesh role of an AP is **mesh-node** not in leaf mode in the AP system profile.

Format

mesh-role { **mesh-portal** | **mesh-node** [**leaf**] }

undo mesh-role

Parameters

Parameter	Description	Value
mesh-portal	Sets the Mesh role of an AP to **mesh-portal** in the AP system profile.	-
mesh-node	Sets the Mesh role of an AP to **mesh-node** in the AP system profile.	-
leaf	Configures a Mesh node to work in leaf mode. If this parameter is not specified, the node works in non-leaf mode.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

APs on a Mesh network can be classified as the following types:

- MP (**mesh-node**): Any Mesh points (MPs) that can support AP functions. They provide both Mesh service and user access service.

  If an MP needs to support low-speed mobility, configure the **mesh-node** AP to work in leaf mode. In leaf mode, the MP functions only as the termination point of a Mesh route and cannot establish a link with an MP that has not gone online and is not enabled with offline service holding.
- MPP (**mesh-portal**): Mesh points that connect the Mesh network to other types of networks and forward communication traffic on a Mesh network.

Configure Mesh roles of APs based on service requirements. If an AP needs to provide both Mesh and user access services, set the Mesh role of the AP to **mesh-node**. If an AP is located at the Mesh network ingress or needs to connect MPs on the local Mesh network to external networks, set the Mesh role of the AP to **mesh-portal**.

NOTE

To ensure the overall Mesh network performance, you are not advised to configure the user access service on a **mesh-portal** AP.

Example

Set the Mesh role of an AP to **mesh-portal** in the AP system profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name test
[HUAWEI-wlan-ap-system-prof-test] mesh-role mesh-portal
```

11.13.22 mesh-route aging-time

Function

The **mesh-route aging-time** command sets the aging time of a Mesh route.

The **undo mesh-route aging-time** command restores the default aging time of a Mesh route.

By default, the aging time of a Mesh route is 5 seconds.

Format

mesh-route aging-time *aging-time*

undo mesh-route aging-time

Parameters

Parameter	Description	Value
aging-time *aging-time*	Specifies the aging time of a Mesh route.	The value is an integer that ranges from 1 to 15, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a Mesh node cannot receive routing frames from a neighboring node for a period of time greater than or equal to the aging time of a Mesh route, the Mesh node considers the Mesh route unreachable and will reselect a route.

If services are interrupted due to great changes in the radio environment, a smaller value for the aging time of a Mesh route can shorten the service interruption time. However, this may cause frequent route reselection, leading to network flapping. Therefore, you need to configure a proper aging time for Mesh routes based on actual situations.

In Mesh link failover scenarios, you can set the aging time of Mesh routes to 1 second so that Mesh routes can be aged out quickly, achieving fast link failover.

Example

Set the aging time of a Mesh route to 10s.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan view] ap-system-profile name test
[HUAWEI-wlan-ap-system-prof-test] mesh-route aging-time 10
```

11.13.23 mesh-whitelist-profile

Function

The **mesh-whitelist-profile** command creates a Mesh whitelist profile or displays the Mesh whitelist profile view.

The **undo mesh-whitelist-profile** command deletes a Mesh whitelist profile.

By default, no Mesh whitelist profile is available in the system.

Format

mesh-whitelist-profile name *whitelist-name*

undo mesh-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
name *whitelist-name*	Specifies the name of a Mesh whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Mesh whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a Mesh whitelist profile is created, run the **peer-ap mac (Mesh whitelist profile view)** command in the Mesh whitelist profile view to add MAC addresses of the allowed peer APs to the profile.

Example

Create the Mesh whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the Mesh whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-whitelist-profile name whitelist
[HUAWEI-wlan-mesh-whitelist-whitelist] peer-ap mac 0001-0001-0001
[HUAWEI-wlan-mesh-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-whitelist-profile whitelist
```

11.13.24 mesh-whitelist-profile (AP group radio view or AP radio view)

Function

The **mesh-whitelist-profile** command binds a Mesh whitelist profile to an AP radio.

The **undo mesh-whitelist-profile** command unbinds a Mesh whitelist profile from an AP radio.

By default, no Mesh whitelist profile is bound to an AP radio.

Format

mesh-whitelist-profile *whitelist-name*

undo mesh-whitelist-profile

Parameters

Parameter	Description	Value
whitelist-name	Specifies the name of the Mesh whitelist profile bound to an AP radio.	The Mesh whitelist profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After a Mesh whitelist profile is applied to an AP radio, the AP radio can only set up Mesh links with neighboring APs whose MAC addresses are in the Mesh whitelist profile.

NOTE

On a Mesh network where ATs are deployed, after FWA is enabled in a Mesh profile using the **fwa enable** command, you can complete the Mesh service configuration without the need to bind a Mesh whitelist profile to an AP radio. However, in other Mesh application scenarios, an AP radio must have a Mesh whitelist profile bound, and the Mesh whitelist profile must have MAC addresses configured.

An AP radio can only have one Mesh whitelist profile bound. If you run the command multiple times on the same AP radio, the latest configuration overwrites the old one.

Example

Create the Mesh whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the Mesh whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-whitelist-profile name whitelist
[HUAWEI-wlan-mesh-whitelist-whitelist] peer-ap mac 0001-0001-0001
[HUAWEI-wlan-mesh-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-whitelist-profile whitelist
```

11.13.25 mpp-active-reselection disable

Function

The **mpp-active-reselection disable** command disables active MPP reselection.

The **undo mpp-active-reselection** command enables active MPP reselection.

By default, active MPP reselection is enabled.

Format

mpp-active-reselection disable

undo mpp-active-reselection

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After active MPP reselection is enabled on an MP, the MP evaluates MPPs of the same Mesh ID and on the same channel based on the signal strength of Mesh links, the number of link hops, and the number of Mesh links. If a more preferable MPP is available, the MP selects the MPP as its Mesh gateway.

If active MPP reselection is disabled, an MP can only passively reselect MPPs. When the minimum RSSI of all Mesh links on the optimal route to the current MPP is lower than the RSSI threshold of a Mesh link, the MPP reselection process is triggered.

Precautions

This configuration is invalid for the MPP.

In train-to-ground communication scenarios, this configuration takes effect only on vehicle-mounted APs working in client mode but not those working in Mesh handover mode. This is because in Mesh handover mode, vehicle-mounted APs use the link handover algorithm to select the MPP.

Active MPP reselection will cause service loss. Configure the function according to actual needs.

Example

Disable active MPP reselection.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name test
[HUAWEI-wlan-ap-system-prof-test] mpp-active-reselection disable
```

11.13.26 nd trust port (Mesh profile view)

Function

The **nd trust port** command enables an ND trusted port in a Mesh profile.

The **undo nd trust port** command disables an ND trusted port in a Mesh profile.

By default, an ND trusted port is enabled in a Mesh profile.

Format

nd trust port

undo nd trust port

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

After an ND trusted port is enabled in a Mesh profile and the Mesh profile is applied to an AP, the AP receives valid ND protocol packets and forwards the packets to STAs or peer APs so that the STAs can obtain valid IPv6 addresses and go online.

Example

Enable an ND trusted port in the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] nd trust port
```

11.13.27 peer-ap mac (Mesh whitelist profile view)

Function

The **peer-ap mac** command adds MAC addresses of neighboring APs that are allowed to connect to an AP to a Mesh whitelist profile.

The **undo peer-ap mac** command deletes the MAC addresses of neighboring APs from a Mesh whitelist profile.

By default, no MAC address of a neighboring AP is added to a Mesh whitelist profile.

Format

peer-ap mac *mac-address*

undo peer-ap mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a neighboring AP to be added to a Mesh whitelist profile.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

Mesh whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Mesh whitelist profile is created, you can run the **peer-ap mac** command to add neighboring APs' MAC addresses to the profile.

If a Mesh whitelist profile is bound to a Mesh profile, only APs with MAC addresses in the Mesh whitelist profile can access the local AP, and other APs are denied access.

Precautions

A maximum of 64 MAC addresses can be added to a Mesh whitelist.

Example

Create the Mesh whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the Mesh whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-whitelist-profile name whitelist
[HUAWEI-wlan-mesh-whitelist-whitelist] peer-ap mac 0001-0001-0001
[HUAWEI-wlan-mesh-whitelist-whitelist] quit
[HUAWEI-wlan-view] ap-group name group1
[HUAWEI-wlan-ap-group-group1] radio 0
[HUAWEI-wlan-group-radio-group1/0] mesh-whitelist-profile whitelist
```

11.13.28 priority-map dscp (Mesh profile view)

Function

The **priority-map dscp** command configures the mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface.

The **undo priority-map dscp** command restores the default mapping from DSCP priorities to 802.11e user priorities on the Mesh air interface.

Table 11-271 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 11-271 Mapping from DSCP priorities to 802.11e user priorities

DSCP Priority	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3

DSCP Priority	802.11e User Priority
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot11e *dot11e-value*	Specifies the 802.11e user priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

On a Mesh network, you can run this command to configure the mapping from DSCP priorities of 802.3 packets to 802.11e user priorities on the Mesh air interface of an AP.

Example

Map DSCP priorities 0-6 to 802.11e user priority 0 on the Mesh air interface.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] priority-map dscp 0 to 6 dot11e 0
```

11.13.29 priority-map trust (Mesh profile view)

Function

The **priority-map trust** command configures the priority mapping to be trusted by the Mesh air interface.

The **undo priority-map trust** command restores the default priority mapping to be trusted by the Mesh air interface.

By default, the Mesh air interface trusts the mapping from DSCP priorities to 802.11e user priorities.

Format

priority-map trust { **dot1p** | **dscp** }

undo priority-map trust

Parameters

Parameter	Description	Value
dot1p	Indicates that the Mesh air interface trusts the mapping from 802.1p priorities to 802.11e user priorities.	-
dscp	Indicates that the Mesh air interface trusts the mapping from DSCP priorities to 802.11e user priorities.	-

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

On a Mesh network, when 802.1p or DSCP priorities in data packets need to be mapped to 802.11e user priorities and the packets are transmitted through a Mesh link, run this command.

Example

Configure the Mesh air interface to trust the mapping from 802.1p priorities to 802.11e user priorities.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] priority-map trust dot1p
```

11.13.30 security-profile (Mesh profile view)

Function

The **security-profile** command binds a security profile to a Mesh profile.

The **undo security-profile** command restores the default security profile bound to a Mesh profile.

By default, the security profile **default-mesh** is bound to a Mesh profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the security profile bound to a Mesh profile.	The security profile must exist.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a Mesh profile is applied to an AP radio to establish Mesh links, the Mesh profile must have a security profile bound to ensure Mesh link security.

Precautions

After a security profile is bound to a Mesh profile, the authentication policy and encryption mode in the security profile cannot be changed, but the authentication key can be changed.

A Mesh profile can only have one security profile bound. If you run the command multiple times in the same Mesh profile view, the latest configuration overwrites the old one.

Example

Create the security profile **sec** and set the security policy to WPA2+PSK+AES. Create the Mesh profile **test** and bind the security profile to the Mesh profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name sec
[HUAWEI-wlan-sec-prof-sec] security wpa2 psk pass-phrase YsHsjx_202206 aes
[HUAWEI-wlan-sec-prof-sec] quit
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] security-profile sec
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.13.31 vlan tagged (Mesh profile view)

Function

The **vlan tagged** command adds one or a group of VLANs to a Mesh profile in tagged mode.

The **undo vlan tagged** command deletes VLANs from a Mesh profile.

By default, no VLAN is configured in a Mesh profile.

Format

vlan tagged { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan tagged { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the tagged VLAN ID. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is added to the Mesh profile in tagged mode. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	- The value of *vlan-id1* is an integer that ranges from 1 to 4094. - The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all tagged VLANs from a Mesh profile.	-

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Mesh network, different VAPs may be configured on the MPP and MPs, or VLANs may be dynamically authorized to STAs on the MPs. If the VLAN or VLANs used by an MP are not created on the MPP, STA packets are discarded on the MPP. To address this, you can run the **vlan tagged** command to create VLANs used by the MPs on the MPP to ensure normal forwarding of STA packets.

Precautions

The VLAN or VLANs specified using the **vlan tagged** command take effect only on the MPP.

A maximum of 256 VLANs can be added to a Mesh profile.

Example

Create the Mesh profile **test** and add VLANs 3, 4, 5, 6, 10, and 12 to the Mesh profile in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] vlan tagged 3 to 6 10 12
```

11.13.32 wideband enable

Function

The **wideband enable** command enables the wideband function, that is, the 4.9 GHz frequency band, of the regulatory domain profile.

The **undo wideband enable** command disables the wideband function, that is, the 4.9 GHz frequency band, of the regulatory domain profile.

By default, the wideband function of the regulatory domain profile is disabled.

The 4.9 GHz frequency band is not supported by AirEngine series APs.

NOTE

Before using the 4.9 GHz frequency band, ensure that you have obtained the 4.9 GHz license from the local administrative department and use the band properly.

Format

wideband enable

undo wideband enable

Parameters

None

Views

Regulatory domain profile

Default Level

2: Configuration level

Usage Guidelines

The wideband function enables AP radios on the 5 GHz frequency band to use the 4.9 GHz frequency band. The 4.9 GHz frequency band is applicable only to outdoor backhaul scenarios but not wireless coverage services. It is mainly used by WDS and Mesh backhaul links. The 4.9 GHz frequency band is not within the DFS reselection channel range.

The following table lists channels and frequency distribution of the 4.9 GHz frequency band.

Channel ID	Parameter	Description
184	Frequency band	4.9 GHz

Channel ID	Parameter	Description
	Center frequency (MHz)	4920
	Upper frequency (MHz)	4910
	Lower frequency (MHz)	4930
188	Frequency band	4.9 GHz
	Center frequency (MHz)	4940
	Upper frequency (MHz)	4930
	Lower frequency (MHz)	4950
192	Frequency band	4.9 GHz
	Center frequency (MHz)	4960
	Upper frequency (MHz)	4950
	Lower frequency (MHz)	4970
196	Frequency band	4.9 GHz
	Center frequency (MHz)	4980
	Upper frequency (MHz)	4970
	Lower frequency (MHz)	4990

The 4.9 GHz frequency band supports channel bandwidths of 20 MHz and 40 MHz. Channels 184+188 or 192+196 can be bundled into a 40 MHz channel. Similar to the 5 GHz frequency band, the 4.9 GHz frequency band complies with 802.11a/n/ac.

After the wideband function of the regulatory domain profile is enabled, APs bound to this profile are automatically reset.

Example

Enable the wideband function of the regulatory domain profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] regulatory-domain-profile name test
[HUAWEI-wlan-regulate-domain-test] wideband enable
Warning: To use the 4.9 GHz frequency band, apply for a license from the related department. When this
frequency band takes effect,
the AP will be reset. Continue? [Y/N]y
```

11.14 Vehicle-Ground Fast Link Handover Configuration Commands

11.14.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.14.2 antenna-output

Function

The **antenna-output** command configures an output mode of a 2.4G/5G antenna.

The **undo antenna-output** command restores the default output mode of a 2.4G/5G antenna.

By default, a 2.4G/5G antenna uses split output.

Format

antenna-output { **split** | **combine** }

undo antenna-output

Parameters

Parameter	Description	Value
split	Indicates the split mode of a 2.4G/5G antenna.	-
combine	Indicates the combination mode of a 2.4G/5G antenna.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In train-ground communication scenarios, you can use the **antenna-output split** command to configure the split mode of a 2.4G/5G antenna. The antenna uses either the 2.4 GHz radio to provide wireless coverage in the carriage, or the 5 GHz radio to provide wireless bridging between carriages.

In train-ground communication scenarios, you can use the **antenna-output combine** command to configure the combination mode of a 2.4G/5G antenna. The antenna uses the 2.4 GHz and 5 GHz radios to simultaneously provide wireless bridging between carriages.

Precautions

This command is supported only by APs supporting antenna combination and split modes.

Example

Configure the combination mode of a 2.4G/5G antenna.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys1
[HUAWEI-wlan-ap-system-prof-apsys1] antenna-output combine
```

11.14.3 client-mode enable

Function

The **client-mode enable** command enables the Mesh client mode.

The **undo client-mode enable** command disables the Mesh client mode.

By default, the Mesh client mode is disabled.

Format

client-mode enable

undo client-mode enable

Parameters

None

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Mesh client is enabled for vehicle-mounted APs, trackside APs must also have the Mesh client enabled to set up a Mesh link.

Precautions

The Mesh handover mode and Mesh client mode are mutually exclusive in a Mesh profile.

A vehicle-ground communication scenario supports either the Mesh handover mode or the Mesh client mode, but not both. Ensure that the same Mesh mode (handover or client) is configured on vehicle-mounted APs and trackside APs. Otherwise, Mesh links may fail to be set up for vehicle-ground communication, or services are affected even if Mesh links can be set up.

Radios of a trackside AP cannot have both the Mesh handover and client modes configured. For example, if radio 1 and radio 2 of a trackside AP have the Mesh handover mode and Mesh client mode configured, respectively, the AP will fail to set up a Mesh link with a vehicle-mounted AP.

Example

Enable the Mesh client mode for Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] client-mode enable
```

11.14.4 display mesh-handover-profile

Function

The **display mesh-handover-profile** command displays reference or configuration information about a Mesh handover profile.

Format

display mesh-handover-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all Mesh handover profiles.	-
name *profile-name*	Displays information about a specified Mesh handover profile.	The Mesh handover profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mesh-handover-profile** command to view the number of times a Mesh handover profile is referenced by a Mesh profile or parameter settings of a specified Mesh handover profile.

Example

Display reference information about all Mesh handover profiles.

```
<HUAWEI> display mesh-handover-profile all
--------------------------------------------------------------------------------
Profile name                          Reference
--------------------------------------------------------------------------------
default                              0
test                                 2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-272 Description of the **display mesh-handover-profile all** command output

Item	Description
Profile name	Name of a Mesh handover profile. To configure this parameter, run the **mesh-handover-profile** command.
Reference	Number of times a Mesh handover profile is referenced by a Mesh profile.

Display information about the Mesh handover profile **test**.

```
<HUAWEI> display mesh-handover-profile name test
--------------------------------------------------------------------------------
Handover location based algorithm switch            : disable
Handover probe interval(ms)                         : 100
Doppler optimize switch                             : enable
Doppler optimize level                              : low
Hal half-band switch                                : enable
--------------------------------------------------------------------------------
```

Table 11-273 Description of the **display mesh-handover-profile name** command output

Item	Description
Handover location based algorithm switch	Status of the location-based enhanced fast link handover algorithm. ● disable: The algorithm is disabled. ● enable: The algorithm is enabled. To configure this parameter, run the **location-based-algorithm enable** command.
Handover probe interval	Mesh link probe interval. To configure this parameter, run the **link-probe-interval** command.
Doppler optimize switch	Whether Doppler optimization is enabled in a Mesh handover scenario. ● disable: This function is disabled. ● enable: This function is enabled. To configure this parameter, run the **doppler-optimize disable** command.
Doppler optimize level	Doppler optimization mode in a Mesh handover scenario. To configure this parameter, run the **doppler-optimize level** command.
Hal half-band switch	Whether the half-band function is enabled on AP radios in Mesh handover scenarios. ● disable: This function is disabled. ● enable: This function is enabled. To configure this parameter, run the **hal half-band disable** command.

11.14.5 display mesh-neighbor-rssi

Function

The **display mesh-neighbor-rssi** command displays RSSI information collected by an AP.

Format

display mesh-neighbor-rssi [**ap-name** *ap-name* **radio** *radio-id* | **ap-id** *ap-id* **radio** *radio-id*] [**max-neighbor-number** *max-number*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays RSSI information collected by the AP with a specified name. If this parameter is not specified, RSSI information collected by all APs is displayed.	The AP name must exist.
ap-id *ap-id*	Displays RSSI information collected by the AP with a specified ID. If this parameter is not specified, RSSI information collected by all APs is displayed.	The AP ID must exist.
radio *radio-id*	Displays RSSI information collected by a specified radio.	The radio ID must exist.
max-neighbor-number *max-number*	Specifies the maximum number of neighboring APs of which RSSI information collected by the AP can be displayed. If this parameter is not specified, RSSI information about all neighboring APs collected by the AP is displayed.	The value is an integer that ranges from 1 to 256.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command applies only to APs on a Mesh network. A local AP can collect RSSI information of a neighboring AP only when the neighboring AP and local AP are added to Mesh whitelists of each other.

Example

Display RSSI information collected by all APs.

```
<HUAWEI> display mesh-neighbor-rssi
Info: This operation may take a few seconds, please wait.done.
AP name/MAC/Radio/Location-ID  Neighbor AP/MAC/Location-ID  RSSI  Update Time
--------------------------------------------------------------------------------
area_1/00e0-fc12-3456/0/1      -/00e0-fc12-3457/-           -43   20:55:16
--------------------------------------------------------------------------------
Total: 1
```

Table 11-274 Description of the **display mesh-neighbor-rssi** command output

Item	Description
AP name/MAC/Radio/Location-ID	Name, MAC address, radio ID, and location ID of the local AP. **NOTE** If APs are named based on their locations, this field displays as AP name/MAC/Radio/Location-ID; otherwise, this field displays as hyphen (-).
Neighbor AP/MAC/Location-ID	Name, MAC address, and location ID of a neighboring AP. **NOTE** If APs are named based on their locations, this field displays as AP name/MAC/Radio/Location-ID; otherwise, this field displays as hyphen (-).
RSSI	RSSI of a neighboring AP.
Update Time	Time when RSSI information is collected.

11.14.6 display references mesh-handover-profile

Function

The **display references mesh-handover-profile** command displays information about Mesh profiles by which a specified Mesh handover profile is referenced.

Format

display references mesh-handover-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays information about the Mesh profiles by which a specified Mesh handover profile is referenced.	The Mesh handover profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references mesh-handover-profile** command to check the Mesh profiles by which a Mesh handover profile is referenced.

Example

Display information about Mesh profiles by which the Mesh handover profile **test** is referenced.

```
<HUAWEI> display references mesh-handover-profile name test
--------------------------------------------------------------------------------
Reference type                 Reference name
--------------------------------------------------------------------------------
Mesh profile                   profile-1
Mesh profile                   profile-2
--------------------------------------------------------------------------------
Total: 2
```

Table 11-275 Description of the **display references mesh-handover-profile** command output

Item	Description
Reference type	Type of the profile by which a Mesh handover profile is referenced. A Mesh handover profile can only be referenced by a Mesh profile.
Reference name	Name of the profile by which a Mesh handover profile is referenced. To configure this parameter, run the **mesh-handover-profile (Mesh profile view)** command in the Mesh profile view.

11.14.7 doppler-optimize disable

Function

The **doppler-optimize disable** command disables the Doppler optimization function in a Mesh handover scenario.

The **undo doppler-optimize disable** command enables the Doppler optimization function in a Mesh handover scenario.

By default, the Doppler optimization function is enabled in a Mesh handover scenario.

Format

doppler-optimize disable

undo doppler-optimize disable

Parameters

None

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Doppler optimization function reduces the impact of the Doppler effect on radio signals in vehicle-ground communication scenarios, thereby improving air interface performance.

Precautions

In Mesh vehicle-ground communication scenarios, it is recommended that the Doppler optimization function be disabled when vehicles are stationary to prevent impact on air interface performance.

Example

Disable the Doppler optimization function in a Mesh handover scenario.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] doppler-optimize disable
```

11.14.8 doppler-optimize level

Function

The **doppler-optimize level** command configures the Doppler optimization mode in a Mesh handover scenario.

The **undo doppler-optimize level** command restores the default Doppler optimization mode in a Mesh handover scenario.

The default Doppler optimization mode is low in a Mesh handover scenario.

Format

doppler-optimize level { **low** | **medium** }

undo doppler-optimize level

Parameters

Parameter	Description	Value
low	Sets the Doppler optimization mode to low. This configuration is recommended when the average vehicle speed is less than or equal to 80 km/h.	-
medium	Sets the Doppler optimization mode to medium. This configuration is recommended when the average vehicle speed is greater than 80 km/h.	-

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

The Doppler optimization function reduces the impact of the Doppler effect on radio signals in vehicle-ground communication scenarios, thereby improving air interface performance.

In practice, the Doppler optimization mode needs to be adjusted based on the main speed range of vehicles.

Example

Set the Doppler optimization mode to medium.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] doppler-optimize level medium
```

11.14.9 hal half-band disable

Function

The **hal half-band disable** command disables the half-band function on AP radios.

The **undo hal half-band disable** command enables the half-band function on AP radios.

By default, the half-band function is enabled on AP radios.

Format

hal half-band disable

undo hal half-band disable

Parameters

None

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

In vehicle-ground communication Mesh handover scenarios, some RF ports on an AP may have no antennas installed. In this case, information on these ports will be lost when information is transmitted based on the half-band algorithm, deteriorating performance. To address this issue, you can run this command to disable the half-band function.

Example

Disable the half-band function on AP radios.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] hal half-band disable
```

11.14.10 location-based-algorithm enable

Function

The **location-based-algorithm enable** command enables the location-based enhanced link handover algorithm.

The **undo location-based-algorithm enable** command disables the location-based enhanced link handover algorithm.

By default, the location-based enhanced link handover algorithm is disabled.

Format

location-based-algorithm enable

undo location-based-algorithm enable

Parameters

None

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

After the location-based enhanced link handover algorithm is enabled, the vehicle-mounted AP will switch the active link to the nearest trackside AP that meets handover requirements.

In vehicle-ground communication scenarios, signals of a trackside AP distant from a train may be temporarily better than the trackside AP near the train due to radio environment changes. If an active link handover occurs at this time, the active link may be incorrectly switched to the distant trackside AP. To prevent incorrect handovers and improve vehicle-ground communication quality, you can use the location-based enhanced link handover algorithm. This algorithm requires that trackside APs be named in ascending or descending order of sequence numbers.

Trackside APs should be named in *head-name_sequence-number* format. *head-name* describes track line information and can be different for trackside APs on the same track. It is recommended that you set the same *head-name* for APs on a track to differentiate tracks. *sequence-number* of APs along a track must be in descending or ascending order. The sequence numbers of trackside APs can be set with unequal steps. *head-name* and *sequence-number* are separated using an underscore (_), for example, L1_001, L1_002, L1_005, L1_010.

Example

Enable the location-based enhanced link handover algorithm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] location-based-algorithm enable
```

11.14.11 link-probe-interval

Function

The **link-probe-interval** command sets a Mesh link probe interval in a Mesh handover profile.

The **undo link-probe-interval** command restores the default Mesh link probe interval in a Mesh handover profile.

By default, the Mesh link probe interval is 100 ms in a Mesh handover profile.

Format

link-probe-interval *value*

undo link-probe-interval

Parameters

Parameter	Description	Value
value	Specifies the interval for detecting Mesh links.	The value is an integer that ranges from 50 to 6000, in milliseconds. The default value is 100.

Views

Mesh handover profile view

Default Level

2: Configuration level

Usage Guidelines

In vehicle-ground communication scenarios, a trackside AP periodically sends unicast probe frames to detect RSSIs of Mesh links and executes the handover algorithm based on the detection result. A larger interval delays link handover, interrupting vehicle-ground communications. A smaller interval increases air port costs and burden. Therefore, you need to configure a proper interval for detecting Mesh links according to train operating conditions.

Precautions

You are advised to set the same Mesh link probe interval for vehicle-mounted APs and trackside APs.

Example

Set the Mesh link probe interval to 150 ms in the Mesh handover profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name test
[HUAWEI-wlan-mesh-handover-test] link-probe-interval 150
```

11.14.12 mesh-handover-profile

Function

The **mesh-handover-profile** command creates a Mesh handover profile or displays the Mesh handover profile view.

The **undo mesh-handover-profile** command deletes a Mesh handover profile.

By default, the system provides the Mesh handover profile **default**.

Format

mesh-handover-profile name *profile-name*

undo mesh-handover-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Mesh handover profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Mesh handover profiles. **NOTE** The Mesh handover profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a Mesh handover profile is bound to a Mesh profile, the Mesh profile can provide the vehicle-ground fast link handover function and apply to vehicle-ground communication scenarios.

Example

Create the Mesh handover profile **handover** and bind it to the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name handover
[HUAWEI-wlan-mesh-handover-handover] quit
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-handover-profile handover
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.14.13 mesh-handover-profile (Mesh profile view)

Function

The **mesh-handover-profile** command binds a Mesh handover profile to a Mesh profile.

The **undo mesh-handover-profile** command unbinds a Mesh handover profile from a Mesh profile.

By default, no Mesh handover profile is bound to a Mesh profile.

Format

mesh-handover-profile *profile-name*

undo mesh-handover-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the Mesh handover profile bound to a Mesh profile.	The Mesh handover profile must exist.

Views

Mesh profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **mesh-handover-profile** command to bind a Mesh handover profile to a Mesh profile so that the Mesh profile can provide the vehicle-ground fast link handover function and apply to vehicle-ground communication scenarios.

Example

Create the Mesh handover profile **handover** and bind it to the Mesh profile **test**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] mesh-handover-profile name handover
[HUAWEI-wlan-mesh-handover-handover] quit
[HUAWEI-wlan-view] mesh-profile name test
[HUAWEI-wlan-mesh-prof-test] mesh-handover-profile handover
Warning: This action may cause service interruption. Continue?[Y/N]y
```

11.15 Hotspot 2.0 Configuration Commands

NOTE

Hotspot 2.0 is not supported by the following APs.

- AirEngine 9700D-S (including matching ORUs)
- AirEngine X77X
- AirEngine X76X

11.15.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.15.2 cellular-network-profile

Function

The **cellular-network-profile** command creates a cellular network profile or displays the view of an existing cellular network profile.

The **undo cellular-network-profile** command deletes a cellular network profile.

By default, no cellular network profile exists in the system.

Format

cellular-network-profile name *profile-name*

undo cellular-network-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a cellular network profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Delete all cellular network profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot 2.0 services on cellular networks. When connecting to the networks, user terminals can obtain network information from APs, which helps them to select desired networks.

Follow-up Procedure

Run the **plmn-id** command to configure the PLMN identifier and run the **cellular-network-profile (Hotspot2.0 profile view)** command to bind the cellular network profile to a Hotspot2.0 profile to make the cellular network profile take effect.

Example

Create the cellular network profile **cellular-network-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cellular-network-profile name cellular-network-profile1
[HUAWEI-wlan-cellular-net-cellular-network-profile1]
```

11.15.3 cellular-network-profile (Hotspot2.0 profile view)

Function

The **cellular-network-profile** command binds a cellular network profile to a Hotspot2.0 profile.

The **undo cellular-network-profile** command unbinds a cellular network profile from a Hotspot2.0 profile.

By default, no cellular network profile is bound to a Hotspot2.0 profile.

Format

cellular-network-profile *profile-name*

undo cellular-network-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a cellular network profile.	The cellular network profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot 2.0 services on a cellular network. When connecting to the network, user terminals need to obtain the cellular network identifier (3GPP Cellular PLMN) from APs to select desired networks. You can run the **cellular-network-profile** command to create a cellular network profile and the **plmn-id** command to configure the Public Land Mobile Network (PLMN) identifier of the network operator, and then bind the cellular network profile to a Hotspot 2.0 profile to make the configuration take effect.

Example

Bind cellular network profile **cellular-network-profile1** to the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] cellular-network-profile cellular-network-profile1
```

11.15.4 connection-capability-profile

Function

The **connection-capability-profile** command creates a connection capability profile or displays the view of an existing connection capability profile.

The **undo connection-capability-profile** command deletes a connection capability profile.

By default, no connection capability profile exists in the system.

Format

connection-capability-profile name *profile-name*

undo connection-capability-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a connection capability profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all connection capability profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When user terminals connect to the networks, they can obtain network connection capability information from APs, including allowed protocols and ports, which helps them to select desired networks.

Follow-up Procedure

Run the **connection-capability-profile (Hotspot2.0 profile view)** command to bind the connection capability profile to a Hotspot2.0 profile so that the connection capability profile can take effect.

Example

Create the connection capability profile **connection-capability-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] connection-capability-profile name connection-capability-profile1
[HUAWEI-wlan-co-cap-prof-connection-capability-profile1]
```

11.15.5 connection-capability-profile (Hotspot2.0 profile view)

Function

The **connection-capability-profile** command binds a connection capability profile to a Hotspot2.0 profile.

The **undo connection-capability-profile** command unbinds a connection capability profile from a Hotspot2.0 profile.

By default, no connection capability profile is bound to a Hotspot2.0 profile.

Format

connection-capability-profile *profile-name*

undo connection-capability-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a connection capability profile.	The connection capability profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When user terminals connect to the networks, they can obtain network connection capability information from APs, including allowed protocols and ports, which helps them to select desired networks. You can run the **connection-capability-profile** command to create a connection capability profile and run the **connection-capability** command to set whether networks support specific IP protocols and ports. After that, you bind the connection capability profile to a Hotspot2.0 profile.

Example

Bind the connection capability profile **connection-capability-profile1** to the Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] connection-capability-profile connection-capability-profile1
```

11.15.6 connection-capability

Function

The **connection-capability** command sets whether Hotspot2.0 networks support common IP protocols and ports.

The **undo connection-capability** command restores the default setting.

By default, no supported protocol is specified in a connection capability profile.

Format

connection-capability { **esp** | **icmp** | **tcp-ftp** | **tcp-http** | **tcp-pptp-vpn** | **tcp-ssh** | **tcp-tls-vpn** | **tcp-voip** | **udp-ike2-4500** | **udp-ike2-500** | **udp-voip** } { **on** | **off** }

undo connection-capability { **esp** | **icmp** | **tcp-ftp** | **tcp-http** | **tcp-pptp-vpn** | **tcp-ssh** | **tcp-tls-vpn** | **tcp-voip** | **udp-ike2-4500** | **udp-ike2-500** | **udp-voip** }

Parameters

Parameter	Description	Value
esp	Sets the supported protocol to ESP and port number to 0.	-
icmp	Sets the supported protocol to ICMP and port number to 0.	-
tcp-ftp	Sets the supported protocol to FTP and port number to 20. FTP is not a secure protocol, and it is not recommended.	-

Parameter	Description	Value
tcp-http	Sets the supported protocol to HTTP and port number to 80. HTTP is not a secure protocol, and it is not recommended.	-
tcp-pptp-vpn	Sets the protocol for VPN services to PPTP and port number to 1723.	-
tcp-ssh	Sets the supported protocol to SSH.	-
tcp-tls-vpn	Sets the supported protocol to the TLS VPN protocol and port number to 443.	-
tcp-voip	Sets the supported protocol to the TCP VoIP protocol and port number to 5060.	-
udp-ike2-4500	Sets the supported protocol to the IKEv2 protocol and port number to 4500.	-
udp-ike2-500	Sets the supported protocol to the IKEv2 protocol and port number to 500.	-
udp-voip	Sets the supported protocol to the UDP VoIP protocol and port number to 5060.	-
on	Supports specified IP protocols and ports.	-
off	Indicates that specified IP protocols and ports are not supported.	-

Views

Connection capability profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **connection-capability** command to set whether Hotspot2.0 networks support common IP protocols and ports.

You can use the **connection-capability** command to set multiple supported protocols at the same time.

Example

Set the supported protocol to ICMP.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] connection-capability-profile name connection-capability-profile1
[HUAWEI-wlan-co-cap-prof-connection-capability-profile1] connection-capability icmp on
```

11.15.7 display cellular-network-profile

Function

The **display cellular-network-profile** command displays information about a cellular network profile.

Format

display cellular-network-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all cellular network profiles.	-
name *profile-name*	Displays information about a specified cellular network profile.	The cellular network profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cellular-network-profile** command to view information about cellular network profiles.

Example

Display information about all cellular network profiles.

```
<HUAWEI> display cellular-network-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
cellular-network-profile1          1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-276 Description of the **display cellular-network-profile all** command output

Item	Description
Profile name	Name of a cellular network profile.
Reference	Number of times a cellular network profile is referenced.

Display information about the cellular network profile **cellular-network-profile1**.

```
<HUAWEI> display cellular-network-profile name cellular-network-profile1
--------------------------------------------------------------------------------
Index     PLMN ID
--------------------------------------------------------------------------------
0         10001
--------------------------------------------------------------------------------
Total: 1
```

Table 11-277 Description of the **display cellular-network-profile name** *profile-name* command output

Item	Description
Index	Index.
PLMN ID	Public land mobile network (PLMN) ID. To configure this parameter, run the **plmn-id** command.

11.15.8 display connection-capability-profile

Function

The **display connection-capability-profile** command displays information about a connection capability profile.

Format

display connection-capability-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all connection capability profiles.	-

Parameter	Description	Value
name *profile-name*	Displays information about a specified connection capability profile.	The connection capability profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display connection-capability-profile** command to view information about connection capability profiles.

Example

Display information about all connection capability profiles.

```
<HUAWEI> display connection-capability-profile all
--------------------------------------------------------------------------------
Profile name                          Reference
--------------------------------------------------------------------------------
connection-capability-profile1       1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-278 Description of the **display connection-capability-profile all** command output

Item	Description
Profile name	Name of a connection capability profile.
Reference	Number of times a connection capability profile is referenced.

Display information about the connection capability profile **connection-capability-profile1**.

```
<HUAWEI> display connection-capability-profile name connection-capability-profile1
--------------------------------------------------------------------------------
ESP                     : -
ICMP                    : on
TCP-FTP                 : -
TCP-HTTP                : -
TCP-PPTP-VPN            : -
TCP-SSH                 : -
TCP-TLS-VPN             : -
TCP-VoIP                : -
```

```
UDP-IKEv2 port 4500    : -
UDP-IKEv2 port 500     : -
UDP-VoIP               : -
------------------------------------------------------------------------------
```

Table 11-279 Description of the **display connection-capability-profile name** *profile-name* command output

Item	Description
ESP	Whether ESP (port number 0) is supported. To configure this parameter, run the **connection-capability** command.
ICMP	Whether ICMP (port number 0) is supported. To configure this parameter, run the **connection-capability** command.
TCP-FTP	Whether FTP (port number 20) is supported. To configure this parameter, run the **connection-capability** command.
TCP-HTTP	Whether HTTP (port number 80) is supported. To configure this parameter, run the **connection-capability** command.
TCP-PPTP-VPN	Whether PPTP for VPN services (port number 1723) is supported. To configure this parameter, run the **connection-capability** command.
TCP-SSH	Whether SSH is supported. To configure this parameter, run the **connection-capability** command.
TCP-TLS-VPN	Whether TLS VPN (port number 443) is supported. To configure this parameter, run the **connection-capability** command.
TCP-VoIP	Whether TCP VoIP (port number 5060) is supported. To configure this parameter, run the **connection-capability** command.
UDP-IKEv2 port 4500	Whether IKEv2 (port number 4500) is supported. To configure this parameter, run the **connection-capability** command.

Item	Description
UDP-IKEv2 port 500	Whether IKEv2 (port number 500) is supported. To configure this parameter, run the **connection-capability** command.
UDP-VoIP	Whether UDP VoIP (port number 5060) is supported. To configure this parameter, run the **connection-capability** command.

11.15.9 display hotspot2-profile

Function

The **display hotspot2-profile** command displays the Hotspot 2.0 profile configuration.

Format

display hotspot2-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Hotspot 2.0 profile.	The Hotspot 2.0 profile must exist.
all	Displays all Hotspot 2.0 profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot 2.0 services, you can run this command to view the Hotspot 2.0 profile configuration.

Example

Display all Hotspot 2.0 profiles on the device.

```
<HUAWEI> display hotspot2-profile all
------------------------------------------------------------------------------
Profile name                       Reference
------------------------------------------------------------------------------
hotspot                           1
------------------------------------------------------------------------------
Total: 1
```

Table 11-280 Description of the **display hotspot2-profile all** command output

Item	Description
Profile name	Name of a Hotspot 2.0 profile.
Reference	Number of times a Hotspot 2.0 profile is referenced.

Display the configuration of the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> display hotspot2-profile name hotspot
------------------------------------------------------------------------------
Network type                    : public-free
Internet access                 : enable
Venue group code                  : 3
Venue type code                  : 3
HESSID                          : 00e0-fc50-89e0
IPv4 address availability        : available
IPv6 address availability        : available
Network authentication type      : online-enroll
Redirect URL                    :
P2P information element          : disable
cellular-network-profile         : cellular-network-profile1
connection-capability-profile    : connection-capability-profile1
operator-name-profile            : operator-name-profile1
operating-class-profile          : operating-class-profile1
operator-domain-profile          : operator-domain-profile1
NAI-realm-profile                : nai-realm-profile1
venue-name-profile               : venue-name-profile1
roaming-consortium-profile       : roaming-consortium-profile1
------------------------------------------------------------------------------
```

Table 11-281 Description of the **display hotspot2-profile name** *profile-name* command output

Item	Description
Network type	Type of a Hotspot 2.0 network. To configure this parameter, run the **network-authen-type** command.
Internet access	Whether a Hotspot 2.0 network supports Internet access. To configure this parameter, run the **network-authen-type** command.

Item	Description
Venue group code	Venue group code of a Hotspot 2.0 network. To configure this parameter, run the **venue-type** command.
Venue type code	Venue type code of a Hotspot 2.0 network. To configure this parameter, run the **venue-type** command.
HESSID	HESSID of a Hotspot 2.0 network. To configure this parameter, run the **hessid** command.
IPv4 address availability	Types of IPv4 addresses on a Hotspot 2.0 network. To configure this parameter, run the **ipv4-address-avail** command.
IPv6 address availability	Types of IPv6 addresses on a Hotspot 2.0 network. To configure this parameter, run the **ipv6-address-avail** command.
Network authentication type	Hotspot 2.0 network authentication type. To configure this parameter, run the **network-authen-type** command.
Redirect URL	Redirection URL if the Hotspot 2.0 network authentication type is set to Portal authentication. To configure this parameter, run the **network-authen-type** command.
P2P information element	Whether a Hotspot 2.0 network allows for cross connections between P2P devices. To configure this parameter, run the **p2p-cross-connect disable** command.
cellular-network-profile	Cellular network profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **cellular-network-profile (Hotspot 2.0 profile view)** command.

Item	Description
connection-capability-profile	Connection capability profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **connection-capability-profile (Hotspot 2.0 profile view)** command.
operator-name-profile	Operator name profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **operator-name-profile (Hotspot 2.0 profile view)** command.
operating-class-profile	Operating class profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **operating-class-profile (Hotspot 2.0 profile view)** command.
operator-domain-profile	Operator domain profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **operator-domain-profile (Hotspot 2.0 profile view)** command.
NAI-realm-profile	NAI realm profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **nai-realm-profile (Hotspot 2.0 profile view)** command.
venue-name-profile	Venue name profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **venue-name-profile (Hotspot 2.0 profile view)** command.
roaming-consortium-profile	Roaming consortium profile bound to a Hotspot 2.0 profile. To configure this parameter, run the **roaming-consortium-profile (Hotspot 2.0 profile view)** command.

11.15.10 display nai-realm-profile

Function

The **display nai-realm-profile** command displays the configuration of a NAI realm profile.

Format

display nai-realm-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays all NAI realm profiles.	-
name *profile-name*	Displays the configuration of a specified NAI realm profile.	The NAI realm profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view the configuration of NAI realm profiles.

Example

Display the configuration of all NAI realm profiles.

```
<HUAWEI> display nai-realm-profile all
------------------------------------------------------------
Profile name        Reference
------------------------------------------------------------
nai-realm-profile1  1
------------------------------------------------------------
Total: 1
```

Table 11-282 Description of the **display nai-realm-profile all** command output

Item	Description
Profile name	Name of a NAI realm profile.
Reference	Number of times a NAI realm profile is referenced.

Display the configuration of the NAI realm profile **nai-realm-profile1**.

```
<HUAWEI> display nai-realm-profile name nai-realm-profile1
--------------------------------------------------------------------------------
Index              Method                  ID/Parameter           Realm-name
--------------------------------------------------------------------------------
0                  All                     -/-                    attwireless.com
--------------------------------------------------------------------------------
```

Table 11-283 Description of the **display nai-realm-profile name** *profile-name* command output

Item	Description
Index	Index of a NAI realm member.
Method	Extensible Authentication Protocol (EAP) authentication method of a NAI realm. To configure this parameter, run the **nai-realm** command.
ID/Parameter	EAP authentication ID and parameters of a NAI realm. To configure this parameter, run the **nai-realm** command.
Realm-name	Name of a NAI realm. To configure this parameter, run the **nai-realm** command.

11.15.11 display operating-class-profile

Function

The **display operating-class-profile** command displays the configuration of an operating class profile.

Format

display operating-class-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all operating class profiles.	-
name *profile-name*	Displays the configuration of a specified operating class profile.	The operating class profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view the configuration of operating class profiles.

Example

Display the configuration of all operating class profiles.

```
<HUAWEI> display operating-class-profile all
------------------------------------------------------------------------------
Profile name                      Reference
------------------------------------------------------------------------------
operating-class-profile1             1
------------------------------------------------------------------------------
Total: 1
```

Table 11-284 Description of the **display operating-class-profile all** command output

Item	Description
Profile name	Name of an operating class profile.
Reference	Number of times an operating class profile is referenced.

Display the configuration of the operating class profile **operating-class-profile1**.

```
<HUAWEI> display operating-class-profile name operating-class-profile1
------------------------------------------------------------------------------
Operating class indication:
95
------------------------------------------------------------------------------
Total: 1
```

Table 11-285 Description of the **display operating-class-profile name** *profile-name* command output

Item	Description
Operating class indication	Operating class indication configured in the profile. To configure this parameter, run the **operating-class-indication** command.

11.15.12 display operator-domain-profile

Function

The **display operator-domain-profile** command displays the configuration of an operator domain profile.

Format

display operator-domain-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all operator domain profiles.	-
name *profile-name*	Displays the configuration of a specified operator domain profile.	The operator domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view the configuration of operator domain profiles.

Example

Display the configuration of all operator domain profiles.

```
<HUAWEI> display operator-domain-profile all
------------------------------------------------------------
Profile name                    Reference
------------------------------------------------------------
operator-domain-profile1        1
------------------------------------------------------------
Total: 1
```

Table 11-286 Description of the **display operator-domain-profile all** command output

Item	Description
Profile name	Name of an operator domain profile
Reference	Number of times an operator domain profile is referenced.

Display the configuration of the operator domain profile **operator-domain-profile1**.

```
<HUAWEI> display operator-domain-profile name operator-domain-profile1
------------------------------------------------------------
```

```
Index                   Domain name
------------------------------------------------------------
0                      attwireless.com
------------------------------------------------------------
```

Table 11-287 Description of the **display operator-domain-profile name** *profile-name* command output

Item	Description
Index	Index of an operator domain
Domain name	Name of an operator domain. To configure this parameter, run the **domain-name** command.

11.15.13 display operator-name-profile

Function

The **display operator-name-profile** command displays information about an operator name profile.

Format

display operator-name-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all operator name profiles.	-
name *profile-name*	Displays information about a specified operator name profile.	The operator name profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display operator-name-profile** command to view information about an operator name profile.

Example

Display information about all operator name profiles.

```
<HUAWEI> display operator-name-profile all
------------------------------------------------------------------------------
Profile name                      Reference
------------------------------------------------------------------------------
operator-name-profile1                1
------------------------------------------------------------------------------
Total: 1
```

Table 11-288 Description of the **display operator-name-profile all** command output

Item	Description
Profile name	Name of an operator name profile.
Reference	Number of times an operator name profile is referenced.

Display information about the operator name profile **operator-name-profile1**.

```
<HUAWEI> display operator-name-profile name operator-name-profile1
------------------------------------------------------------------------------
Index                   Language-code                 Name
------------------------------------------------------------------------------
0                     en                          att
------------------------------------------------------------------------------
```

Table 11-289 Description of the **display operator-name-profile name** *profile-name* command output

Item	Description
Index	Index of a friendly operator name.
Language-code	Language type. To configure this parameter, run the **operator-friendly-name** command.
Name	Friendly operator name. To configure this parameter, run the **operator-friendly-name** command.

11.15.14 display references cellular-network-profile

Function

The **display references cellular-network-profile** command displays reference information about a cellular network profile.

Format

display references cellular-network-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified cellular network profile.	The cellular network profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references cellular-network-profile** command to view reference information about a cellular network profile.

Example

Display reference information about the cellular network profile **cellular-network-profile1**.

```
<HUAWEI> display references cellular-network-profile name cellular-network-profile1
------------------------------------------------------------------------------
Reference type                Reference name
------------------------------------------------------------------------------
hotspot2-profile              hotspot
------------------------------------------------------------------------------
Total: 1
```

Table 11-290 Description of the **display references cellular-network-profile** command output

Item	Description
Reference type	Type of the profile to which the cellular network profile is bound.
Reference name	Name of the profile to which the cellular network profile is bound.

11.15.15 display references connection-capability-profile

Function

The **display references connection-capability-profile** command displays reference information about a connection capability profile.

Format

display references connection-capability-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified connection capability profile.	The connection capability profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references connection-capability-profile** command to view reference information about a connection capability profile.

Example

Display reference information about the connection capability profile **connection-capability-profile1**.

```
<HUAWEI> display references connection-capability-profile name connection-capability-profile1
--------------------------------------------------------------------------------
Reference type                  Reference name
--------------------------------------------------------------------------------
hotspot2-profile                hotspot
--------------------------------------------------------------------------------
Total: 1
```

Table 11-291 Description of the **display references connection-capability-profile** command output

Item	Description
Reference type	Type of the profile to which the connection capability profile is bound.

Item	Description
Reference name	Name of the profile to which the connection capability profile is bound.

11.15.16 display references hotspot2-profile

Function

The **display references hotspot2-profile** command displays reference information about a Hotspot2.0 profile.

Format

display references hotspot2-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Hotspot2.0 profile.	The Hotspot2.0 profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view reference information about a Hotspot2.0 profile.

Example

Display reference information about the Hotspot2.0 profile **hotspot**.

```
<HUAWEI> display references hotspot2-profile name hotspot
-------------------------------------------------------------------
Reference type                 Reference name
-------------------------------------------------------------------
VAP profile                    vap-profile1
-------------------------------------------------------------------
Total:1
```

Table 11-292 Description of the **display references hotspot2-profile name** *profile-name* command output

Item	Description
Reference type	Type of the profile to which the Hotspot2.0 profile is bound. ● VAP profile. To configure it, run the **hotspot2-profile (VAP profile view)** command.
Reference name	Name of the profile to which the Hotspot2.0 profile is bound. To configure it, run the **hotspot2-profile (VAP profile view)** command.

11.15.17 display references nai-realm-profile

Function

The **display references nai-realm-profile** command displays reference information about a NAI realm profile.

Format

display references nai-realm-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified NAI realm profile.	The NAI realm profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a NAI realm profile.

Example

Display reference information about the NAI realm profile **nai-realm-profile1**.

```
<HUAWEI> display references nai-realm-profile name nai-realm-profile1
-------------------------------------------------------------------------------
Reference type        Reference name
-------------------------------------------------------------------------------
hotspot2-profile      hotspot
-------------------------------------------------------------------------------
Total: 1
```

Table 11-293 Description of the **display references nai-realm-profile** command output

Item	Description
Reference type	Type of the profile to which the NAI realm profile is bound.
Reference name	Name of the profile to which the NAI realm profile is bound.

11.15.18 display references operating-class-profile

Function

The **display references operating-class-profile** command displays reference information about an operating class profile.

Format

display references operating-class-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	# Display reference information about a specified operating class profile.	The operating class profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about an operating class profile.

Example

Display reference information about the operating class profile **operating-class-profile1**.

```
<HUAWEI> display references operating-class-profile name operating-class-profile1
--------------------------------------------------------------------------------
Reference type        Reference name
--------------------------------------------------------------------------------
hotspot2-profile      hotspot
--------------------------------------------------------------------------------
Total: 1
```

Table 11-294 Description of the **display references operating-class-profile** command output

Item	Description
Reference type	Type of the profile to which the operating class profile is bound.
Reference name	Name of the profile to which the operating class profile is bound.

11.15.19 display references operator-domain-profile

Function

The **display references operator-domain-profile** command displays reference information about an operator domain profile.

Format

display references operator-domain-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified operator domain profile.	The operator domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about an operator domain profile.

Example

Display reference information about the operator domain profile **operator-domain-profile1**.

```
<HUAWEI> display references operator-domain-profile name operator-domain-profile1
------------------------------------------------------------------------------
Reference type        Reference name
------------------------------------------------------------------------------
hotspot2-profile      hotspot
------------------------------------------------------------------------------
Total: 1
```

Table 11-295 Description of the **display references operator-domain-profile** command output

Item	Description
Reference type	Type of the profile to which the operator domain profile is bound.
Reference name	Name of the profile to which the operator domain profile is bound.

11.15.20 display references operator-name-profile

Function

The **display references operator-name-profile** command displays reference information about an operator name profile.

Format

display references operator-name-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified operator name profile.	The operator name profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references operator-name-profile** command to view reference information about an operator name profile.

Example

Display reference information about the operator name profile **operator-name-profile1**.

```
<HUAWEI> display references operator-name-profile name operator-name-profile1
--------------------------------------------------------------------
Reference type                 Reference name
--------------------------------------------------------------------
hotspot2-profile               hotspot
--------------------------------------------------------------------
Total:1
```

Table 11-296 Description of the **display references operator-name-profile** command output

Item	Description
Reference type	Type of the profile to which the operator name profile is bound.
Reference name	Name of the profile to which the operator name profile is bound.

11.15.21 display references roaming-consortium-profile

Function

The **display references roaming-consortium-profile** command displays reference information about a roaming consortium profile.

Format

display references roaming-consortium-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a roaming consortium profile.	The roaming consortium profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view reference information about a roaming consortium profile.

Example

Display reference information about the roaming consortium profile **roaming-consortium-profile1**.

```
<HUAWEI> display references roaming-consortium-profile name roaming-consortium-profile1
------------------------------------------------------------------------
Reference type                  Reference name
------------------------------------------------------------------------
hotspot2-profile                hotspot
------------------------------------------------------------------------
Total:1
```

Table 11-297 Description of the **display references roaming-consortium-profile name** *profile-name* command output

Item	Description
Reference type	Type of the profile to which the roaming consortium profile is bound. - hotspot2-profile: Hotspot2.0 profile. To configure it, run the **roaming-consortium-profile (Hotspot2.0 profile view)** command.
Reference name	Name of the profile to which the roaming consortium profile is bound. To configure it, run the **roaming-consortium-profile (Hotspot2.0 profile view)** command.

11.15.22 display references venue-name-profile

Function

The **display references venue-name-profile** command displays reference information about a venue name profile.

Format

display references venue-name-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a venue name profile.	The venue name profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view reference information about a venue name profile.

Example

Display reference information about the venue name profile **venue-name-profile1**.

```
<HUAWEI> display references venue-name-profile name venue-name-profile1
------------------------------------------------------------------------
Reference type                  Reference name
------------------------------------------------------------------------
hotspot2-profile                hotspot
------------------------------------------------------------------------
Total:1
```

Table 11-298 Description of the **display references venue-name-profile name** *profile-name* command output

Item	Description
Reference type	Type of the profile to which the venue name profile is bound. - hotspot2-profile: Hotspot2.0 profile. To configure it, run the **venue-name-profile (Hotspot2.0 profile view)** command.
Reference name	Name of the profile to which the venue name profile is bound. To configure it, run the **venue-name-profile (Hotspot2.0 profile view)** command.

11.15.23 display roaming-consortium-profile

Function

The **display roaming-consortium-profile** command displays the configuration of a roaming consortium profile.

Format

display roaming-consortium-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a roaming consortium profile.	The roaming consortium profile must exist.
all	Displays the configuration of all roaming consortium profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view the configuration of a roaming consortium profile.

Example

Display the configuration of all roaming consortium profiles on a device.

```
<HUAWEI> display roaming-consortium-profile all
-------------------------------------------------------------------------------
Profile name                         Reference
-------------------------------------------------------------------------------
roaming-consortium-profile1          1
-------------------------------------------------------------------------------
Total: 1
```

Table 11-299 Description of the **display roaming-consortium-profile all** command output

Item	Description
Profile name	Name of a roaming consortium profile.
Reference	Number of times a roaming consortium profile is referenced.

Display the configuration of the roaming consortium profile **roaming-consortium-profile1**.

```
<HUAWEI> display roaming-consortium-profile name roaming-consortium-profile1
-------------------------------------------------------------------------------
Index     Roaming consortium OI     In beacon
-------------------------------------------------------------------------------
0         00-11-22                  Y
-------------------------------------------------------------------------------
Total: 1
```

Table 11-300 Description of the **display roaming-consortium-profile name** *profile-name* command output

Item	Description
Index	Index of a roaming consortium member.
Roaming consortium OI	OI of a roaming consortium member. To configure this parameter, run the **roaming-consortium-oi** command.

Item	Description
In beacon	Whether Beacon and Probe Response frames sent from APs carry OIs of roaming consortium members. - Y: Yes - N: No To configure this parameter, run the **roaming-consortium-oi** command.

11.15.24 display venue-name-profile

Function

The **display venue-name-profile** command displays the configuration of a venue name profile.

Format

display venue-name-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a venue name profile.	The venue name profile must exist.
all	Displays the configuration of all venue name profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, you can run this command to view the configuration of venue name profiles.

Example

Display the configuration of all venue name profiles on a device.

```
<HUAWEI> display venue-name-profile all
--------------------------------------------------------------------------------
Profile name                        Reference
--------------------------------------------------------------------------------
venue-name-profile1                    1
--------------------------------------------------------------------------------
Total: 1
```

Table 11-301 Description of the **display venue-name-profile all** command output

Item	Description
Profile name	Name of a venue name profile.
Reference	Number of times a venue name profile is referenced.

Display the configuration of the venue name profile **venue-name-profile1**.

```
<HUAWEI> display venue-name-profile name venue-name-profile1
--------------------------------------------------------------------------------
Index                  Language code                Name
--------------------------------------------------------------------------------
0                    en                          CenterStation
--------------------------------------------------------------------------------
```

Table 11-302 Description of the **display venue-name-profile name** *profile-name* command output

Item	Description
Index	Index of venue name information.
Language code	Language type. To configure this parameter, run the **venue-name** command.
Name	Venue name. To configure this parameter, run the **venue-name** command.

11.15.25 domain-name

Function

The **domain-name** command configures a domain name for a hotspot operator.

The **undo domain-name** command deletes the domain name of a hotspot operator.

By default, no domain name is configured for a hotspot operator.

Format

domain-name *domain-name*

undo domain-name *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name of a hotspot operator.	The value is a string of 1 to 63 characters in compliance with RFC1035. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Views

Operator domain profile view

Default Level

2: Configuration level

Usage Guidelines

After a domain name is configured for a hotspot operator, terminals can query the domain name through ANQP to select desired networks.

Example

Configure domain name **attwireless.com** for a hotspot operator.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-domain-profile name operator-domain-profile1
[HUAWEI-wlan-op-domain-prof-operator-domain-profile1] domain-name attwireless.com
```

11.15.26 hessid

Function

The **hessid** command configures a Homogenous Extended Service Set Identifier (HESSID) for a Hotspot2.0 network.

The **undo hessid** command deletes an HESSID.

By default, no HESSID is configured.

Format

hessid *mac-address*

undo hessid

Parameters

Parameter	Description	Value
mac-address	Specifies an HESSID.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Hotspot2.0 networks are available, user terminals need to identify service providers of the connected networks. An SSID is not as unique as an HESSID, which can uniquely identify APs of the same service provider. Among the APs, the BSSID of one AP is used as the HESSID. The HESSID is an optional parameter in a Hotspot2.0 profile. Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to determine whether network parameters need to be renewed.

Precautions

If the HESSID is configured repeatedly, only the latest HESSID takes effect.

Example

Set the HESSID to **00e0-fc12-3456** in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] hessid 00e0-fc12-3456
```

11.15.27 hotspot2-profile

Function

The **hotspot2-profile** command creates a Hotspot2.0 profile or displays the view of an existing Hotspot2.0 profile.

The **undo hotspot2-profile** command deletes a Hotspot2.0 profile.

By default, no Hotspot2.0 profile is available.

Format

hotspot2-profile name *profile-name*

undo hotspot2-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Hotspot2.0 profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all Hotspot2.0 profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure Hotspot2.0 services, create a Hotspot2.0 profile, configure network parameters in the Hotspot2.0 profile view, and bind the Hotspot2.0 profile to a VAP profile.

Follow-up Procedure

Configure the network type, roaming consortium list, and NAI realm list in the Hotspot2.0 profile and bind the Hotspot2.0 profile to a VAP profile to make the configuration take effect.

Precautions

- In a Hotspot2.0 profile, network parameters and Internet access status are mandatory and can be configured using the **network-type** command.
- Ensure that at least one of the following ANQP parameters is configured in a Hotspot2.0 profile.
  - Roaming consortium list: Run the **roaming-consortium-profile (Hotspot2.0 profile view)** command to bind a roaming consortium profile to the Hotspot2.0 profile.
  - NAI realm list: Run the **nai-realm-profile (Hotspot2.0 profile view)** command to bind a NAI realm profile to the Hotspot2.0 profile.
  - 3GPP cellular network: Run the **cellular-network-profile (Hotspot2.0 profile view)** command to bind a cellular network profile to the Hotspot2.0 profile.
- The following ANQP parameters are recommended.
  - Roaming consortium list: Run the **roaming-consortium-profile (Hotspot2.0 profile view)** command to bind a roaming consortium profile to the Hotspot2.0 profile.
  - Domain name list: Run the **operator-domain-profile (Hotspot2.0 profile view)** command to bind an operator domain profile to the Hotspot2.0 profile.

Example

Create Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot]
```

11.15.28 hotspot2-profile (VAP profile view)

Function

The **hotspot2-profile** command binds a Hotspot 2.0 profile to a VAP profile.

The **undo hotspot2-profile** command unbinds a Hotspot 2.0 profile from a VAP profile.

By default, no Hotspot 2.0 profile is bound to a VAP profile.

Format

hotspot2-profile *profile-name*

undo hotspot2-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a Hotspot 2.0 profile.	The Hotspot 2.0 profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure network parameters through Hotspot 2.0 profiles. After Hotspot 2.0 profiles are applied, STAs can obtain network information from APs and access the networks. After a Hotspot 2.0 profile is configured, bind it to a VAP profile to make the configuration take effect.

Precautions

The Hotspot 2.0 service configuration requires the authentication mode of WPA2-802.1X. Ensure that the security profile bound to the VAP profile meets this requirement.

When you perform the following operations on a VAP bound to a radio, services are interrupted:

- Bind a Hotspot 2.0 profile to the VAP profile.
- Unbind a Hotspot 2.0 profile from the VAP profile.
- Modify the parameters in a Hotspot 2.0 profile bound to the VAP profile.

Therefore, exercise caution when performing these operations.

Example

Bind the Hotspot 2.0 profile **hotspot** to the VAP profile **vap-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] hotspot2-profile hotspot
```

11.15.29 ipv4-address-avail

Function

The **ipv4-address-avail** command configures available types of IPv4 addresses on a Hotspot2.0 network.

The **undo ipv4-address-avail** command deletes available types of IPv4 addresses on a Hotspot2.0 network.

By default, no available type of IPv4 addresses is configured.

Format

ipv4-address-avail { **not-available** | **available** | **port-restricted** [**single-nat** | **double-nat**] | **private** { **single-nat** | **double-nat** } | **unknown** }

undo ipv4-address-avail

Parameters

Parameter	Description	Value
not-available	Indicates that IPv4 addresses are not available.	-
available	Indicates that IPv4 addresses are available.	-
port-restricted [**single-nat** | **double-nat**]	Indicates port restricted IPv4 addresses are available. ● **single-nat**: Single-NATed and port-restricted IPv4 addresses are available. ● **single-nat**: Double-NATed and port-restricted IPv4 addresses are available.	-
private { **single-nat** | **double-nat** }	Indicates that private IPv4 addresses are available. ● **single-nat**: Single-NATed private IPv4 addresses are available. ● **double-nat**: Double-NATed private IPv4 addresses are available.	-
unknown	Indicates that availability of the IPv4 address type is not known.	-

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When user terminals connect to a Hotspot2.0 network, Hotspot2.0 can transfer available IPv4 address types as ANQP parameters to the user terminals through

APs. In this way, the user terminals can know the IP address types they can obtain after connecting to the network.

Example

Set IPv4 addresses to **available** in hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] ipv4-address-avail available
```

11.15.30 ipv6-address-avail

Function

The **ipv6-address-avail** command configures available types of IPv6 addresses on a Hotspot 2.0 network.

The **undo ipv6-address-avail** command deletes available types of IPv6 addresses on a Hotspot 2.0 network.

By default, no available type of IPv6 addresses is configured.

Format

ipv6-address-avail { **not-available** | **available** | **unknown** }

undo ipv6-address-avail

Parameters

Parameter	Description	Value
not-available	Indicates that IPv6 addresses are not available.	-
available	Indicates that IPv6 addresses are available.	-
unknown	Indicates that the availability of IPv6 address types is not known.	-

Views

Hotspot 2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When STAs connect to a Hotspot 2.0 network, Hotspot 2.0 can transfer available IPv6 address types as ANQP parameters to the STAs through APs. In this way, the STAs can know the IPv6 address types they can obtain after connecting to the network.

Example

Configure IPv6 addresses to be available in the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] ipv6-address-avail available
```

11.15.31 nai-realm-profile

Function

The **nai-realm-profile** command creates a NAI realm profile or displays the view of an existing NAI realm profile.

The **undo nai-realm-profile** command deletes a NAI realm profile.

By default, no NAI realm profile is available in the system.

Format

nai-realm-profile name *profile-name*

undo nai-realm-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a NAI realm profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all NAI realm profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A NAI realm profile is used to configure the network access identifier (NAI) realm name, authentication mode, and authentication parameters for networks accessible to users.

Example

Create NAI realm profile **nai-realm-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] nai-realm-profile name nai-realm-profile1
[HUAWEI-wlan-nai-realm-prof-nai-realm-profile1]
```

11.15.32 nai-realm-profile (Hotspot2.0 profile view)

Function

The **nai-realm-profile** command binds a NAI realm profile to a Hotspot2.0 profile.

The **undo nai-realm-profile** command unbinds a NAI realm profile from a Hotspot2.0 profile.

By default, no NAI realm profile is bound to a Hotspot2.0 profile.

Format

nai-realm-profile *profile-name*

undo nai-realm-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a NAI realm profile.	The NAI realm profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services on a non-cellular network. When connecting to the non-cellular network, user terminals can obtain service provider information of the network, including the NAI realm name and authentication mode. This facilitates terminal access. You can run the **nai-realm-profile** command to create a NAI realm profile and the **nai-realm** command in the NAI realm profile view to configure NAI realms, and then bind the NAI realm profile to a Hotspot2.0 profile to make the configuration take effect.

Example

Bind NAI realm profile **nai-realm-profile1** to Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] nai-realm-profile nai-realm-profile1
```

11.15.33 nai-realm

Function

The **nai-realm** command configures a network access identifier (NAI) realm.

The **undo nai-realm** command deletes a NAI realm.

By default, no NAI realm is configured.

Format

nai-realm realm-name *realm-name* [**eap-method-type** *eap-method-type* [**eap-authen-id** *eap-authen-id* **eap-authen-para** *eap-authen-para*]]

undo nai-realm realm-name *realm-name* [**eap-method-type** *eap-method-type* [**eap-authen-id** *eap-authen-id*]]

Parameters

Parameter	Description	Value
realm-name *realm-name*	Specifies a NAI realm name.	The value is a string of 1 to 63 characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Parameter	Description	Value
eap-method-type *eap-method-type*	Specifies an EAP authentication mode for a NAI realm.	Enumerated value: - eap-aka: EAP-AKA authentication - eap-sim: GSM Subscriber Identity Modules - eap-tls: EAP-TLS - eap-ttls: EAP-TTLS
eap-authen-id *eap-authen-id*	Specifies an EAP authentication ID for a NAI realm.	The value is an integer that ranges from 0 to 255.
eap-authen-para *eap-authen-para*	Specifies the EAP authentication parameter of a NAI realm.	The value is an integer that ranges from 0 to 255.

Views

NAI realm profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure a NAI realm, terminals can access the configured operator network.

Precautions

- If you configure the same name for NAI realms, the NAI realm with fuzzy command configuration will overwrite the NAI realm with exact command configuration.

  For example, the **nai-realm realm-name attwireless.com** command configuration will overwrite the **nai-realm realm-name attwireless.com eap-method-type eap-aka** command configuration, and the **nai-realm realm-name attwireless.com eap-method-type eap-aka** command configuration will overwrite the **nai-realm realm-name attwireless.com eap-method-type eap-aka eap-authen-id 1 eap-authen-para 1** command configuration.
- NAI realms are deleted according to the longest matching rule.

For example, the NAI realm configured using the **nai-realm realm-name attwireless.com** command cannot be deleted using the **undo nai-realm realm-name attwireless.com eap-method-type eap-aka** command.

Example

Configure NAI realm **attwireless.com**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] nai-realm-profile name nai-realm-profile1
[HUAWEI-wlan-nai-realm-prof-nai-realm-profile1] nai-realm realm-name attwireless.com
```

11.15.34 network-authen-type

Function

The **network-authen-type** command sets a network authentication type for a Hotspot2.0 profile.

The **undo network-authen-type** command deletes a network authentication type.

By default, no network authentication type is configured.

Format

network-authen-type { **acceptance** [**redirect-url** *url*] | **dns-redirection** | **http-https-redirection redirect-url** *url* | **online-enroll** }

undo network-authen-type

Parameters

Parameter	Description	Value
acceptance	Indicates acceptance of terms and conditions.	-
redirect-url *url*	Specifies the redirected URL address.	-
dns-redirection	Indicates DNS redirection.	-
http-https-redirection	Indicates HTTP and HTTPS redirection.	-
online-enroll	Indicates online enrollment.	-

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to discover and select proper networks. If the network operator requests user terminals to execute specified actions, for example, opening a web page for Portal authentication, the Additional Steps Required for Access (ASRA) field must be set to 1, indicating that user terminals must implement extra authentication when connecting to a network. You can run the **network-authen-type** command to specify a network authentication type.

Example

Set the network authentication type to online enrollment in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] network-authen-type online-enroll
```

11.15.35 network-type

Function

The **network-type** command sets a network type and Internet access status in a Hotspot2.0 profile.

The **undo network-type** command restores the default network type and Internet access status.

By default, the network type is set to **wildcard**, and Internet access is not supported.

Format

network-type { **emergency-service** | **personal-device** | **private** | **private-guest** | **public-chargeable** | **public-free** | **test** | **wildcard** } [**internet-access**]

undo network-type

Parameters

Parameter	Description	Value
emergency-service	Indicates an emergency service network.	-

Parameter	Description	Value
personal-device	Indicates a personal device network.	-
private	Indicates a private network.	-
private-guest	Indicates a private network with guest access.	-
public-chargeable	Indicates a chargeable public network.	-
public-free	Indicates a free public network.	-
test	Indicates a test network.	-
wildcard	Indicates a wildcard network.	-
internet-access	Indicates that Internet access is supported.	-

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Hotspot2.0 networks are available, user terminals need to obtain information of each network to select the network to access. The network type and Internet access status are mandatory in a Hotspot2.0 profile. Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to discover and select proper networks.

Precautions

If the command is executed repeatedly, only the latest configuration takes effect.

Example

Set the network type to free public network and configure the network to provide Internet access in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] network-type public-free internet-access
```

11.15.36 operating-class-indication

Function

The **operating-class-indication** command configures an operating class indication.

The **undo operating-class-indication** command deletes an operating class indication.

By default, no operating class indication is configured in the system.

Format

operating-class-indication *operating-class-value*

undo operating-class-indication *operating-class-value*

Parameters

Parameter	Description	Value
operating-class-value	Indicates the operating class indication.	The value is an integer that ranges from 1 to 255.

Views

Operating class profile view

Default Level

2: Configuration level

Usage Guidelines

After an operating class indication is configured, users can obtain the indication through ANQP for network selection.

You can configure a maximum of 32 operating class indications using this command.

Example

Set the operating class indication to **95**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operating-class-profile name operating-class-profile1
[HUAWEI-wlan-op-class-prof-operating-class-profile1] operating-class-indication 95
```

11.15.37 operating-class-profile

Function

The **operating-class-profile** command creates an operating class profile or displays the view of an existing operating class profile.

The **undo operating-class-profile** command deletes an operating class profile.

By default, no operating class profile is configured in the system.

Format

operating-class-profile name *profile-name*

undo operating-class-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of the operating class profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates to delete all operating class profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The operating class profile is used to configure the operating class indication of AP in on the hotspot2.0 network. When a STA accesses the network, it can obtain channel information used to access a Wi-Fi frequency from AP so that the STA can set up a connection.

Example

Create an operating class profile named **operating-class-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operating-class-profile name operating-class-profile1
[HUAWEI-wlan-op-class-prof-operating-class-profile1]
```

11.15.38 operating-class-profile (Hotspot2.0 profile view)

Function

The **operating-class-profile** command binds the specified operating class profile to a Hotspot2.0 profile view.

The **undo operating-class-profile** command unbinds the specified operating class profile from a Hotspot2.0 profile view.

By default, no operating class profile is bound to a Hotspot2.0 profile view.

Format

operating-class-profile *profile-name*

undo operating-class-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of the operating class profile.	The value must be the name of an existing operating class profile.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses a Hotspot2.0 network, it can obtain channel information used to access a Wi-Fi frequency from the AP so that the STA can set up a connection. Before binding an operating class profile to a Hotspot2.0 profile, you need to run the **operating-class-profile** command to create an operating class profile and run the **operating-class-indication** command in the profile view to configure an operating class indication.

Example

Bind the operating class profile **operating-class-profile1** to the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] operating-class-profile operating-class-profile1
```

11.15.39 operator-domain-profile

Function

The **operator-domain-profile** command creates a network domain name profile or displays the view of an existing network domain name profile.

The **undo operator-domain-profile** command deletes a network domain name profile.

By default, no network domain name profile is available in the system.

Format

operator-domain-profile name *profile-name*

undo operator-domain-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the network domain name profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates to delete all network domain name profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A network domain name profile is used to configure the operator domain profile. STAs can obtain the domain name information through ANQP, which is used as a basis for network selection.

Example

Create a network domain name profile named **operator-domain-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-domain-profile name operator-domain-profile1
[HUAWEI-wlan-op-domain-prof-operator-domain-profile1]
```

11.15.40 operator-domain-profile (Hotspot2.0 profile view)

Function

The **operator-domain-profile** command binds the specified operator domain profile to a Hotspot2.0 profile view.

The **undo operator-domain-profile** command unbinds the specified operator domain profile from a Hotspot2.0 profile view.

By default, no operator domain profile is bound to a Hotspot2.0 profile.

Format

operator-domain-profile *profile-name*

undo operator-domain-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of the operator domain profile.	The value must be the name of an existing operator domain profile.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses the Hotspot2.0 network, it can obtain the network operator domain name information from the AP so that the STA can select a network. Before binding an operator domain profile to a Hotspot2.0 profile, run the **operator-domain-profile** command to create an operator domain profile and run the **domain-name** command in the profile view to configure the operator name.

Example

Bind the operator domain profile **operator-domain-profile1** to the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] operator-domain-profile operator-domain-profile1
```

11.15.41 operator-friendly-name

Function

The **operator-friendly-name** command configures the operator friendly name.

The **undo operator-friendly-name** command deletes the operator friendly name.

By default, no operator friendly name is configured in an operator name profile view.

Format

operator-friendly-name language-code *language-code* **name** *name*

undo operator-friendly-name language-code *language-code* **name** *name*

Parameters

Parameter	Description	Value
language-code *language-code*	Indicates the language.	The value is a string of 2 to 3 characters. For the value of each language, see the definition in ISO639-2 *Codes for the Representation of Names of Languages*. For example, the value is **chi**, **zho**, or **zh** for Chinese, and **eng** for English.

Parameter	Description	Value
name *name*	Indicates the operator friendly name.	The value is a string of 1 to 64 case-sensitive characters. ● English venue name: The value is a string of visible characters without question marks (?) and spaces. It cannot begin or end with double quotation marks (" "). ● Non-English venue name: It cannot contain half-width question marks (?). To enter a non-English venue name, ensure that the remote login terminal supports the UTF-8 encoding format; otherwise, the name cannot be displayed.

Views

Operator name profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses the Hotspot2.0 network, it can obtain the operator name from the AP. This command configures the language environment names so that users can select a proper language.

If you need to enter a non-English name, you must use a tool to convert it into hexadecimal UTF-8 code.

Precautions

If you run the **operator-friendly-name** multiple times, multiple operator friendly names are configured. A maximum of 32 names can be configured.

Example

Set the operator friendly name to **operator-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-name-profile name operator-name-profile1
[HUAWEI-wlan-op-name-prof-operator-name-profile1] operator-friendly-name language-code eng
name att
```

11.15.42 operator-name-profile

Function

The **operator-name-profile** command creates an operator name profile or displays the view of an existing operator name profile.

The **undo operator-name-profile** command deletes the operator name profile.

By default, no operator name profile is available in the system.

Format

operator-name-profile name *profile-name*

undo operator-name-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of the operator name profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Indicates to delete all operator name profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can specify different friendly names for different languages so that users can select networks.

Follow-up Procedure

Run the **operator-name-profile (Hotspot2.0 profile view)** command to apply the created operator name profile to a Hotspot2.0 profile.

Example

Create an operator name profile named **operator-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] operator-name-profile name operator-name-profile1
[HUAWEI-wlan-op-name-prof-operator-name-profile1]
```

11.15.43 operator-name-profile (Hotspot2.0 profile view)

Function

The **operator-name-profile** command binds the specified operator name profile to a Hotspot2.0 profile view.

The **undo operator-name-profile** command unbinds the specified operator name profile from a Hotspot2.0 profile view.

By default, no operator name profile is bound to a Hotspot2.0 profile.

Format

operator-name-profile *profile-name*

undo operator-name-profile

Parameters

Parameter	Description	Value
profile-name	Indicates the name of the operator name profile.	The value must be the name of an existing operator name profile.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA accesses the Hotspot2.0 network, it can obtain the operator name from the AP. Before binding an operator name profile to a Hotspot2.0 profile, run the **operator-name-profile** command to create an operator name profile and run the **operator-friendly-name** command in the profile view to configure the operator name.

Example

Bind the operator name profile **operator-name-profile1** to the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] operator-name-profile operator-name-profile1
```

11.15.44 p2p-cross-connect disable

Function

The **p2p-cross-connect disable** command configures P2P management information to prevent cross connections of P2P devices.

The **undo p2p-cross-connect disable** command deletes P2P management information.

By default, P2P management information is not configured.

Format

p2p-cross-connect disable

undo p2p-cross-connect disable

Parameters

None.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hotspot2.0 provides security measures for STAs. It prevents direct access between STAs to reduce the STA attack possibility. The P2P protocol allows direct communication between STAs; therefore, a Hotspot2.0-supported AP can add P2P management information into Beacon. In the management information, STAs are not allowed to set up P2P connections with each other.

Precautions

The **p2p-cross-connect disable** command is not recommended. An AP does not support the P2P protocol or process P2P packets; therefore, it is unnecessary to remove P2P management information from packets.

Example

Configure P2P management information in the **hotspot** profile.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] p2p-cross-connect disable
```

11.15.45 plmn-id

Function

The **plmn-id** command configures the Public Land Mobile Network (PLMN) identifier.

The **undo plmn-id** command deletes the PLMN identifier.

By default, no PLMN identifier is configured in the cellular network profile.

Format

plmn-id *plmn-id*

undo plmn-id *plmn-id*

Parameters

Parameter	Description	Value
plmn-id	Indicates the PLMN identifier.	The value is an integer that ranges from 10000 to 999999.

Views

Cellular network profile view

Default Level

2: Configuration level

Usage Guidelines

After the **plmn-id** command is executed, the AP notifies STAs of the operator information on the Hotspot2.0 network. The STAs can obtain the PLMN identifier to determine whether to select the cellular network according to the Hotspot2.0 network.

If you run the **plmn-id** multiple times, multiple PLMN identifiers are configured. A maximum of 32 PLMN identifiers can be configured.

Example

Set the PLMN identifier to 10001.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] cellular-network-profile name cellular-network-profile1
[HUAWEI-wlan-cellular-net-cellular-network-profile1] plmn-id 10001
```

11.15.46 roaming-consortium-oi

Function

The **roaming-consortium-oi** command configures the roaming consortium identifier of the Hotspot2.0 network.

The **undo roaming-consortium-oi** command deletes the roaming consortium identifier of the Hotspot2.0 network.

By default, no roaming consortium identifier is configured for the Hotspot2.0 network.

Format

roaming-consortium-oi *oi-value* [**in-beacon**]

undo roaming-consortium-oi *oi-value*

Parameters

Parameter	Description	Value
oi-value	Indicates the roaming consortium identifier, which is used to identify operators.	The format is HH-HH-HH or HH-HH-HH-HH-HH, in which H is in the hexadecimal format.
in-beacon	Indicates that the Beacon and probe-response frames sent by the AP contain the roaming consortium identifier.	-

Views

Roaming consortium profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If STAs may roam between the Hotspot2.0 network and a network of another operator, you can configure the OI of the operator that provides the roaming service so that STAs can select networks.

Precautions

If you run this command multiple times, multiple OIs are configured. A maximum of 32 OIs can be configured in a roaming consortium profile. To configure OIs in the roaming consortium profile, the first OI must carry the **in-beacon** parameter. A maximum of three OIs can be configured to carry the **in-beacon** parameter.

Example

Add an OI **00-11-22** to the profile **roaming-consortium-profile1** and add the OI to the Beacon and probe-response frames sent by the AP.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] roaming-consortium-profile name roaming-consortium-profile1
[HUAWEI-wlan-ro-co-prof-roaming-consortium-profile1] roaming-consortium-oi 00-11-22 in-beacon
```

11.15.47 roaming-consortium-profile

Function

The **roaming-consortium-profile** command creates a roaming consortium profile or displays the view of an existing roaming consortium profile.

The **undo roaming-consortium-profile** command deletes a roaming consortium profile.

By default, no roaming consortium profile is created.

Format

roaming-consortium-profile name *profile-name*

undo roaming-consortium-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a roaming consortium profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all roaming consortium profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, configure network parameters according to operator requirements. When connecting to networks, user terminals can obtain the network parameters to select desired networks. If the user terminals need to roam among Hotspot2.0 networks of different operators, configure a roaming consortium profile and add the organization identifiers (OIs) of the operators to the roaming consortium profile. In this way, after the user terminals connect to a network of an operator in the profile, they can roam to networks of the other operators while maintaining online.

Follow-up Procedure

Run the **roaming-consortium-oi** command to configure the roaming consortium OI in the roaming consortium profile.

Example

Create the roaming consortium profile **roaming-consortium-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] roaming-consortium-profile name roaming-consortium-profile1
[HUAWEI-wlan-ro-co-prof-roaming-consortium-profile1]
```

11.15.48 roaming-consortium-profile (Hotspot2.0 profile view)

Function

The **roaming-consortium-profile** command binds a roaming consortium profile to a Hotspot2.0 profile.

The **undo roaming-consortium-profile** command unbinds a roaming consortium profile from a Hotspot2.0 profile.

By default, no roaming consortium profile is bound to a Hotspot2.0 profile.

Format

roaming-consortium-profile *profile-name*

undo roaming-consortium-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a roaming consortium profile.	The roaming consortium profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When user terminals connect to the networks, they can obtain OIs of the operators used for STA roaming, which helps them select desired networks. You can run the **roaming-consortium-profile** command to create a roaming consortium profile and the **roaming-consortium-oi** command in the roaming consortium profile view to configure operator OIs, and then bind the roaming consortium profile to a Hotspot2.0 profile to make the configuration take effect.

Example

Bind roaming consortium profile **roaming-consortium-profile1** to the Hotspot 2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] roaming-consortium-profile roaming-consortium-profile1
```

11.15.49 venue-name-profile

Function

The **venue-name-profile** command creates a venue name profile or displays the view of an existing venue name profile.

The **undo venue-name-profile** command deletes a venue name profile.

By default, no venue name profile is created.

Format

venue-name-profile name *profile-name*

undo venue-name-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a venue name profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all venue name profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Hotspot2.0 services, configure network parameters according to operator requirements. When connecting to networks, user terminals can obtain the network parameters to select desired networks. The venue name describes physical locations of a network and is an optional parameter.

Follow-up Procedure

Run the **venue-name** command in the venue name profile view to configure the venue name. After creating a venue name profile, bind it to a Hotspot2.0 profile.

Example

Create the venue name profile **venue-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] venue-name-profile name venue-name-profile1
[HUAWEI-wlan-ve-na-prof-venue-name-profile1]
```

11.15.50 venue-name-profile (Hotspot2.0 profile view)

Function

The **venue-name-profile** command binds a venue name profile to a Hotspot2.0 profile.

The **undo venue-name-profile** command unbinds a venue name profile from a Hotspot2.0 profile.

By default, no venue name profile is bound to a Hotspot2.0 profile.

Format

venue-name-profile *profile-name*

undo venue-name-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a venue name profile.	The venue name profile must exist.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Hotspot2.0 services for networks. When connecting to the networks, user terminals can obtain location information of the networks from APs, which helps them to select desired networks. You can run the **venue-name-profile** command to create a venue name profile and the **venue-name** command in the venue name profile view to configure venue names, and then bind the venue name profile to a Hotspot2.0 profile to make the configuration take effect.

Example

Bind venue name profile **venue-name-profile1** to Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] venue-name-profile venue-name-profile1
```

11.15.51 venue-name

Function

The **venue-name** command configures a venue name for a Hotspot 2.0 network.

The **undo venue-name** command deletes the configured venue name.

By default, no venue name is configured.

Format

venue-name language-code *language-code* **name** *venue-name*

undo venue-name language-code *language-code* **name** *venue-name*

Parameters

Parameter	Description	Value
language-code *language-code*	Specifies the language type.	The value is a string of 2 to 3 characters. For the value of each language, see the definition in ISO639-2 *Codes for the Representation of Names of Languages*. For example, the value is **chi**, **zho**, or **zh** for Chinese, and **eng** for English.

Parameter	Description	Value
name *venue-name*	Specifies the venue name.	The value is a string of 1 to 64 case-sensitive characters. ● English venue name: The value is a string of visible characters without question marks (?) and spaces. It cannot begin or end with double quotation marks (" "). ● Non-English venue name: It cannot contain half-width question marks (?). To enter a non-English venue name, ensure that the remote login terminal supports the UTF-8 encoding format; otherwise, the name cannot be displayed.

Views

Venue name profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the command to configure venue names for Hotspot 2.0 networks to identify physical locations of the networks, which helps user terminals select desired networks. You can set the venue names in multiple languages for user groups of different languages.

Precautions

This command can be configured repeatedly. A maximum of 32 venue names can be configured in a venue name profile.

Example

Set the language to English and configure the venue name **CenterStation** in venue name profile **venue-name-profile1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] venue-name-profile name venue-name-profile1
[HUAWEI-wlan-ve-na-prof-venue-name-profile1] venue-name language-code eng name CenterStation
```

11.15.52 venue-type

Function

The **venue-type** command configures the venue type of a Hotspot2.0 network.

The **undo venue-type** command deletes the configured venue type.

By default, no venue type information is configured for a Hotspot2.0 network.

Format

venue-type group-code *venue-group* **type-code** *type-code-value*

undo venue-type

Parameters

Parameter	Description	Value
group-code *venue-group*	Specifies the venue group type.	The value is an integer that ranges from 0 to 255. For meanings of different venue group values, see **7.3.1.34 Venue Info field** defined in IEEE Std 802.11u-2011.
type-code *type-code-value*	Specifies the venue subtype.	The value is an integer that ranges from 0 to 255. For meanings of different venue subtype values, see **7.3.1.34 Venue Info field** defined in IEEE Std 802.11u-2011.

Views

Hotspot2.0 profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Hotspot2.0 networks are available, user terminals need to obtain information of each network to select the network to access. The venue type information is optional in a Hotspot2.0 profile. Beacon and Probe Response frames sent from Hotspot2.0-capable APs carry network parameter information, which helps user terminals to discover and select proper networks.

group-code and **type-code** determine the venue type and identify the network location. As predefined in the 802.11u protocol:

- If **group-code** is set to 2 (Business) and **type-code** to 3, the venue type indicates **Fire Station**.
- If **group-code** is set to 3 (Educational) and **type-code** to 3, the venue type indicates **University or College**.

Precautions

If the command is executed repeatedly, only the latest configuration takes effect.

Example

Set the venue type to **University or College** in Hotspot2.0 profile **hotspot**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] hotspot2-profile name hotspot
[HUAWEI-wlan-hotspot2-prof-hotspot] venue-type group-code 3 type-code 3
```

11.16 IoT AP Configuration Commands

11.16.1 Command Support

- WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.
- IoT cards are supported only by the following models:
  - AirEngine 5760-22W, AirEngine 5760-22WD, AirEngine 5760-51, AirEngine 6760-X1, AirEngine 6760-X1E, AirEngine 8760-X1-PRO
  - AirEngine 5761-11W, AirEngine 5761-11WD, AirEngine 5761-12W, AirEngine 5761-21, AirEngine 5761S-11, AirEngine 5761S-11W, AirEngine 5761S-21, AirEngine 6761-21T, AirEngine 6761S-21T
  - AirEngine 5761-11, AirEngine 5761S-12, AirEngine 5761S-13, AirEngine 6761-21, AirEngine 6761S-21, AirEngine 6761-21E
  - AirEngine 5762-13W, AirEngine 5762-15HW, AirEngine 5762S-13W
  - AirEngine 5762-16W
  - AirEngine 8761-X1
  - AirEngine 5762-17W
  - AirEngine 8771-X1T

Only intrinsically safe APs (AirEngine 5761-11EI) support the baud rate configuration for communication between APs and IoT cards.

11.16.2 antenna-status

Function

The **antenna-status** command configures an IoT card to use the external or built-in antenna of an AP's IoT module.

The **undo antenna-status** command restores the default antenna selection policy for an IoT card.

By default, an IoT card is not configured to use the external or built-in antenna of an AP's IoT module.

Format

antenna-status { **external** | **internal** }

undo antenna-status

Parameters

Parameter	Description	Value
external	Configures an IoT card to use the external antenna of an AP's IoT module.	-
internal	Configures an IoT card to use the built-in antenna of an AP's IoT module.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

By default, an IoT card uses the built-in 2.4 GHz antenna of an AP's IoT module for communication. You can install the external antenna as required and run the **antenna-status external** command to configure the IoT card to use the external antenna for communication.

NOTE

The external and built-in antennas cannot be used together in an IoT module. If there are multiple IoT cards, the cards must use the same type of antennas for communication. For configuration details, see Card 1.

When the **display ap-card all** or **display ap** *ap-id* **card** { **all** | *card-number* | **usb** } command is run to check information about an IoT card, whether the card uses the built-in or external antenna for communication is also displayed in the command output.

Example

Configure an IoT card to use the external antenna of an AP's IoT module.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1] antenna-status external
```

11.16.3 baud-rate

Function

The **baud-rate** command configures the baud rate used by an AP to communicate with an IoT card.

The **undo baud-rate** command restores the default baud rate used by an AP to communicate with an IoT card.

By default, no baud rate is configured, and an AP can automatically adapt to the baud rate.

NOTE

This function is supported only by intrinsically safe APs (AirEngine 5761-11EI) that support communication with the uninterruptible power supply (UPS).

Format

baud-rate { **9600** | **19200** | **38400** | **57600** | **115200** | **921600** }

undo baud-rate

Parameters

Parameter	Description	Value
9600 | **19200** | **38400** | **57600** | **115200** | **921600**	Specifies the baud rate used by an AP to communicate with an IoT card.	-

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

APs with common cards can automatically adapt to the baud rate of an IoT card. However, for some cards, such as those with RS485 serial ports, APs cannot automatically adapt to the card baud rate. In this case, run this command to set the baud rate to the same as that of the corresponding cards.

Example

Set the baud rate used by APs in an AP group to communicate with an IoT card to 9600 bit/s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1]  baud-rate 9600
```

Set the baud rate used by an AP to communicate with an IoT card to 9600 bit/s.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-id 0
[HUAWEI-wlan-ap-0] card 1
[HUAWEI-wlan-card-0/1] baud-rate 9600
```

11.16.4 card connect-type

Function

The **card connect-type** command configures the connection type between IoT cards and APs.

The **undo card connect-type** command restores the default connection type between IoT cards and APs.

By default, IoT cards communicate with APs through serial interfaces.

Format

card connect-type { **ethernet** | **serial** | **container** }

undo card connect-type

Parameters

Parameter	Description	Value
ethernet	Configures IoT cards to communicate with APs through Ethernet interfaces.	-
serial	Configures IoT cards to communicate with APs through serial interfaces.	-
container	Configures IoT cards to communicate with a third-party server by loading the third-party container image.	-

Views

AP system profile view, IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When **serial** is configured for communication between IoT cards and APs, the communication rate does not exceed the maximum baud rate of serial interfaces, that is, 115200 bit/s. This connection type applies to scenarios with a light traffic volume. The connection type of **ethernet** applies to scenarios where electronic shelf labels (ESLs) are deployed.

Before using IoT cards of other vendors, contact the vendors to confirm the connection types supported by the cards.

Precautions

- The configurations in different views take effect in descending priority as follows: IoT card interface view of an AP > IoT card interface view of an AP group > AP system profile view.

Example

Configure IoT cards to communicate with APs through Ethernet interfaces.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ab
[HUAWEI-wlan-ap-system-prof-ab] card connect-type ethernet
```

11.16.5 config-agent permit ip-address

Function

The **config-agent permit ip-address** command configures trusted host computers.

The **undo config-agent permit ip-address** command deletes the configuration of trusted host computers.

By default, no trusted host computer is configured.

Format

config-agent permit ip-address *ip-address* { *net-mask* | *mask-len* }

undo config-agent permit ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a trusted host computer.	The value is in dotted decimal notation.
net-mask	Specifies the mask of the IP address of a trusted host computer.	The value is in dotted decimal notation.
mask-len	Specifies the mask length.	The value is an integer that ranges from 0 to 32.

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized devices from attacking an AP, you can configure trusted host computers. In this way, only hosts within the specified IP address range can communicate with the AP functioning as a server and send the AP the configuration to be delivered to the IoT card.

If no trusted host computer is configured, any host computers with reachable routes to the AP can communicate with the AP, which brings security risks to the AP.

Precautions

After the **type cas-edu** command is executed to set the card type to **cas-edu**, the **config-agent permit ip-address** command cannot be executed.

Example

Configure the IP address of a trusted host computer and its mask.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name wlan-iot
[HUAWEI-wlan-iot-prof-wlan-iot] config-agent permit ip-address 10.2.3.4 255.255.255.0
```

11.16.6 display ap card

Function

The **display ap card** command displays details about AP cards.

Format

display ap *ap-id* **card** { **all** | *card-number* | **usb** }

Parameters

Parameter	Description	Value
ap-id	Specifies an AP ID.	The AP ID must exist.
all	Specifies all AP cards.	-
card-number	Specifies an IoT card interface number.	The interface number must exist.
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ap card** command to view details about AP cards.

Example

Display details about AP cards.

```
<HUAWEI> display ap 0 card all
Connected-status: The match status indicates that the card connection type matches
that on the device. Otherwise, mismatch is displayed. To modify the effective connection
type, run the card connect-type {serial|ethernet|container} command and restart the device.
--------------------------------------------------------------------------------
 Card                    : 1
--------------------------------------------------------------------------------
 IOT card status          : absent
--------------------------------------------------------------------------------
 Card                    : 2
--------------------------------------------------------------------------------
 IOT card status          : present
```

```
Card connect type        : Serial
Connected status         : mismatch

Physical connection type : PCIe
Support card information : YES
Protocol version         : 1
Wireless standard        : RFID
Frequency                : 433M
Vendor name              : ENJOYOR
Card type                : TOEAPV1.2
Hardware version         : VA
Firmware version         : 0.1.0.1
Card serial number       : 0000000000000001
Baud-rate                : 115200
Frame-version            : 1.0
Antenna status           : External
Card IP                  : 10.2.3.4
Card MAC                 : 00e0-fc44-5566
Central frequency        : 2413MHz
Card bandwidth           : 2413MHz
Connect server status    : connected
Server name              : -
Subnet mask              : 16
Gateway address          : 10.2.3.5
------------------------------------------------------------------------------
Card                     : 3
------------------------------------------------------------------------------
IOT card status          : absent
------------------------------------------------------------------------------
Card                     : usb
------------------------------------------------------------------------------
USB status               : disable
IOT card status          : absent
------------------------------------------------------------------------------
```

Table 11-303 Description of the **display ap card** command output

Item	Description
IOT card status	Card status. - present: A card is installed in the slot. - absent: No card is installed in the slot.
Card connect type	Connection type between an IoT card and the AP.
Physical connection type	Connection type between the IoT card and AP.
Connected status	Whether the actual connection type of an IoT card matches the current initialized connection type of the AP.
Support card information	Whether card information can be queried.
Protocol version	Protocol version. The current version number is 1.

Item	Description
Wireless standard	Wireless protocol supported by a card. The value is a 10-byte ASCII character set, for example, RFID, ANT, ZigBee, BT4.0, and Weightless.
Frequency	Card frequency. The value is an 8-byte ASCII character set, for example, 2.4G, 900M, 2.4/5G, or any value from 433M to 915M.
Vendor name	Vendor code. The value is an 8-byte ASCII character set, for example, ENJOYOR.
Card type	Card model. The value is a 12-byte ASCII character set, for example, TOEAPV1.2.
Hardware version	Hardware version of the card. The value is a 2-byte ASCII character set. The value is fixed in the following pattern: VA for the first version, VB for the second version, VC for the third version, and so on.
Firmware version	Firmware version of the card. The value is a 4-byte number, for example, 00.01.00.01.
Card serial number	Module ID of the card. The value is a 16-byte BCD character set.
Baud-rate	Baud rate for serial communication on an IoT card slot.
Frame-version	Frame format of an extension interface.
Antenna status	Whether an IoT card uses the built-in or external antenna. ● External: external antenna ● Internal: built-in antenna
Card IP	IP address of a card.
Card MAC	MAC address of an IoT card.
Central frequency	Center frequency of an IoT card.
Card bandwidth	Bandwidth of an IoT card.
Connect server status	Connection status between an IoT card and the server.

Item	Description
Server name	Name of the server connected to an IoT card.
Subnet mask	Subnet mask length.
Gateway address	Gateway address.
USB status	Actual working status of the USB function on an AP.

11.16.7 display ap-card statistics

Function

The **display ap-card statistics** command displays statistics on the packets received and sent by cards on APs.

Format

display ap-card statistics { **all** | **ap-id** *ap-id* [**card** { *card-number* | **usb** }] }

Parameters

Parameter	Description	Value
all	Specifies cards on all APs.	-
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-number*	Specifies an IoT card interface number.	The interface number must exist.
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on the packets received and sent by cards on APs. Only statistics about IoT cards with the serial connection type can be displayed.

Example

Display statistics on the packets received and sent by cards on all APs.

```
<HUAWEI> display ap-card statistics all
----------------------------------------------------------------------------------------------------
AP ID  Card-number  RX-packets  TX-packets  RX-bytes  TX-bytes
----------------------------------------------------------------------------------------------------
0      1            1           2           100       200
----------------------------------------------------------------------------------------------------
Total: 1
```

Display statistics on the packets received and sent by cards on AP 0.

```
<HUAWEI> display ap-card statistics ap-id 0
----------------------------------------------------------------------------------------------------
AP ID  Card-number  Card-status  RX-packets  TX-packets  RX-bytes  TX-bytes
----------------------------------------------------------------------------------------------------
0      1            present      1           2           100       200
0      2            absent       2           1           89        14
0      3            absent       0           0           0         0
0      usb           absent       0           0           0         0
----------------------------------------------------------------------------------------------------
Total: 4
```

Table 11-304 Description of the **display ap-card statistics** command output

Item	Description
AP ID	AP ID.
Card-number	Card number.
Card-status	Whether a card is installed in the slot. - absent: No card is installed in the slot. - present: A card is installed in the slot.
RX-packets	Number of packets sent to a card.
TX-packets	Number of packets received from a card.
RX-bytes	Number of bytes sent to a card.
TX-bytes	Number of bytes received from a card.

11.16.8 display ap-card all

Function

The **display ap-card all** command displays brief information about cards on all the APs.

Format

display ap-card all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To query brief information about cards on all the APs, run the **display ap-card all** command.

Precautions

No result is displayed if a card does not support query.

Example

Display brief information about cards on all the APs.

```
<HUAWEI> display ap-card all
Connected-status: The match status indicates that the card connection type matches
that on the device. Otherwise, mismatch is displayed. To modify the effective connection
type, run the card connect-type {serial|ethernet|container} command.
Frame-version: Frame format on extended interfaces.
------------------------------------------------------------------------------------------------------------------------------
-------
---------------------------
AP ID  Card-number  Wireless-standard  Vendor-name  Card-type     Card-connect-type  Connected-status
Antenna-status  Baud-rate  Fr
ame-version  Serial-number
------------------------------------------------------------------------------------------------------------------------------
-------
---------------------------
0      1           RFID             ENJOYOR      TOEAPV1.2      ethernet(up)       match            External
9600       2.
0          0000000000000001
------------------------------------------------------------------------------------------------------------------------------
-------
---------------------------
Total: 1
```

Table 11-305 Description of the **display ap-card all** command output

Item	Description
AP ID	AP ID.
Card-number	Card ID.

Item	Description
Wireless-standard	Wireless protocol supported by a card. The value is a 10-byte ASCII character set, for example, RFID, ANT, ZigBee, BT4.0, and Weightless.
Vendor-name	Vendor code. The value is an 8-byte ASCII character set, for example, ENJOYOR.
Card-type	Card model. The value is a 12-byte ASCII character set, for example, TOEAPV1.2.
Card-connect-type	Connection type between an IoT card and the AP.
Connected-status	Whether the actual connection type of an IoT card matches the current initialized connection type of the AP.
Antenna-status	Whether an IoT card uses the built-in or external antenna. ● External: external antenna ● Internal: built-in antenna
Baud-rate	Baud rate used for communication between the card and AP.
Frame-version	Frame format of an extension interface.
Serial-number	Module ID of a card. The value is a 16-byte BCD character set.

11.16.9 display iot-card iot-command-result

Function

The **display iot-card iot-command-result** command displays the execution results of commands transparently transmitted to IoT cards.

Format

display iot-card iot-command-result all

display iot-card iot-command-result ap ap-id *ap-id* **card** { *card-id* | **usb** }

Parameters

Parameter	Description	Value
all	Displays command execution results on all cards of all APs.	-
ap ap-id *ap-id*	Displays command execution results on cards of the AP with a specified ID.	The AP ID must exist.
card *card-id*	Displays command execution records on the card with a specified ID.	The value is an integer that ranges from 1 to 3.
card usb	Displays command execution results on USB cards.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a command is transparently transmitted to a card, you can run the **display iot-card iot-command-result** command to check the command execution result on the card.

Precautions

Example

Display execution results of commands transparently transmitted to all IoT cards.

```
<HUAWEI> display iot-card iot-command-result all
Ap information:
Total  :     [7]
Waiting:     [1]
Success:     [1]
Fail   :     [5]
------------------------------------------------------------------------------------------------------------------------
AP-ID Card Time                  Command  Transparent transmission result
Card Response
------------------------------------------------------------------------------------------------------------------------
13    1    2019.10.10 16:14:46  status   Fail(Time Out)
13    1    2019.10.10 16:31:24  status   Success
++++++++++++++++++++++++++++++
- Network:
DHCP:           BOUND
IP:             10.10.10.54
Netmask:        255.255.255.0
```

```
Gateway:        10.10.10.1
Nameserver:     0.0.0.0
Nameserver2:    0.0.0.0
- ESL SCD:
ID:             42002

++++++++++++++++++++++++++++++
11    1    2019.10.10 16:14:46  status   Fail(Card is not installed)
12    1    2019.10.10 16:14:46  status   Fail(Card is busy)
14    1    2019.10.10 16:14:46  status   Fail(Other reason)
15    1    2019.10.10 16:14:46  status   Fail(Time out)
15    1    2019.10.10 16:14:46  status   Waiting
------------------------------------------------------------------------------------------------------------------------
Total: 7
```

Table 11-306 Description of the **display iot-card iot-command-result all** command output

Item	Description
Total	Total number of command execution results.
Waiting	Number of command execution results that a card is waiting for from the AP.
Success	Number of commands that have been successfully executed.
Fail	Number of commands that fail to be executed.
AP-ID	ID of the AP where a card resides.
Card	Card ID.
Time	Time when the device transparently transmits a command to a card.
Command	Content of a command transparently transmitted to a card.

Item	Description
Transparent transmission result	Execution result of a command on a card: ● Success: The command has been successfully executed. ● Waiting: The card is waiting for a response from the AP. ● Fail: The command fails to be transmitted to the card. The failure reasons are as follows: – Card does not support this command: The card does not support this command. – Card is not installed: The card is not properly installed. – Time Out: The response of the card times out. Check the version of the card. If the card version does not support transparent transmission of commands, the command execution times out. – Card is busy: The card is executing another command. – Other reason: A system error occurs.
Card Response	Response of a card. The response is defined by the card vendor. For details, contact the card vendor.

11.16.10 display iot-profile

Function

The **display iot-profile** command displays the IoT profile configuration.

Format

display iot-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an IoT profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Specifies all IoT profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the IoT profile configuration.

Example

Display the configuration of all IoT profiles.

```
<HUAWEI> display iot-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
1                               0
profile1                        0
wlan-IoT                        1
--------------------------------------------------------------------------------
Total:3
```

Table 11-307 Description of the **display iot-profile all** command output

Item	Description
Profile name	Name of an IoT profile.
Reference	Number of times an IoT profile is referenced.

Display the configuration of the IoT profile **wlan-IoT** .

```
<HUAWEI> display iot-profile name wlan-IoT
-------------------------------------------------------------------------------
Type                             : common
Agent permit IP address          : 10.23.102.253
Agent permit net-mask            : 255.255.255.0
Management server IP address     : 10.23.102.254
Management server port           : 3000
ExtManagement server IP address  : -
ExtManagement server port        : -
Share key                        : ******
Antenna status                   : -
-------------------------------------------------------------------------------
```

Table 11-308 Description of the **display iot-profile name wlan-IoT** command output

Item	Description
Type	Card type. To configure this parameter, run the **type (IoT profile view)** command.
Agent permit IP address	IP address of a trusted host computer. To configure this parameter, run the **config-agent permit ip-address** command.
Agent permit net-mask	Mask of the IP address of a trusted host computer. To configure this parameter, run the **config-agent permit ip-address** command.
Management server IP address	IP address of the host computer. To configure this parameter, run the **management-server** command.
Management server port	Port number of the host computer. To configure this parameter, run the **management-server** command.
ExtManagement server IP address	IP address of the host computer on the extended channel. To configure this parameter, run the **management-server** command.
ExtManagement server port	Port number of the host computer on the extended channel. To configure this parameter, run the **management-server** command.
Share key	Shared key. To configure this parameter, run the **share-key** command.

Item	Description
Antenna status	Whether an IoT card uses the built-in or external antenna. ● External: external antenna ● Internal: built-in antenna

11.16.11 display references iot-profile

Function

The **display references iot-profile** command displays reference information about an IoT profile.

Format

display references iot-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an IoT profile.	The IoT profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view reference information about an IoT profile.

Example

Display reference information about the IoT profile **wlan-IoT**.

```
<HUAWEI> display references iot-profile name wlan-IoT
--------------------------------------------------------------------------------
Reference type     Reference name                       Reference card
--------------------------------------------------------------------------------
AP group           default                              Card-1
--------------------------------------------------------------------------------
Total:1
```

Table 11-309 Description of the **display references iot-profile name wlan-IoT** command output

Item	Description
Reference type	Type of the object to which the IoT profile is bound.
Reference name	Name of the object to which the IoT profile is bound.
Reference card	Card to which the IoT profile is bound.

11.16.12 card

Function

The **card** command displays the IoT card interface view.

Format

card { *card-number* | **usb** }

Parameters

Parameter	Description	Value
card-number	Specifies an IoT card interface number.	The value is an integer that ranges from 1 to 3.
usb	Specifies the USB interface for an IoT card.	-

Views

AP group view, AP specific view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the communication parameters are configured between an AP and an IoT card, and between an AP and a host computer, you need to bind corresponding configuration profiles in the IoT card interface view to make the parameters take effect.

Prerequisites

The USB function of the AP has been enabled using the **usb enable** command.

Precautions

IoT cards of the cas-edu type do not support the USB interface.

Example

Display the IoT card interface view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1]
```

11.16.13 iconnect enable

Function

The **iconnect enable** command enables the iConnect function on an AP so that the AP releases an iConnect SSID.

The **undo iconnect enable** command disables the iConnect function.

By default, the iConnect function is disabled.

Format

iconnect enable

undo iconnect enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the iConnect function is enabled on an AP, the AP releases an iConnect SSID, through which IoT terminals can access the network. This implements plug-and-play of IoT terminals and enables the terminals to automatically load digital certificates.

Precautions

In the Navi AC scenario, an SSID cannot be configured as an iConnect SSID.

Example

Enable the iConnect function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1
[HUAWEI-wlan-vap-prof-vap1] iconnect enable
```

11.16.14 iot-card reboot

Function

The **iot-card reboot** command resets an IoT card of an AP.

Format

iot-card reboot ap ap-id *ap-id* **card** { *card-id* | **usb** }

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card-id	Specifies the IoT card interface number.	The value is an integer that ranges from 1 to 3.
usb	Specifies the USB interface of an IoT card.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

The **iot-card reboot** command resets an IoT card of an AP.

Example

Reset an IoT card on the USB interface of the AP with ID 0.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card reboot ap ap-id 0 card usb
```

11.16.15 iot-card reset-factory-configuration

Function

The **iot-card reset-factory-configuration** command restores factory defaults of an IoT card.

Format

iot-card reset-factory-configuration ap ap-id *ap-id* **card** *card-id*

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-id*	Specifies the ID of an IoT card.	The IoT card ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an IoT card cannot communicate with the AP due to an error in IoT card parameter settings, you can run this command to restore factory defaults of the IoT card.

Example

Restore factory defaults of an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card reset-factory-configuration ap ap-id 1 card 1
```

11.16.16 iot-card reset-network-configuration

Function

The **iot-card reset-network-configuration** command resets network parameters of an IoT card.

Format

iot-card reset-network-configuration ap ap-id *ap-id* **card** { *card-id* | **usb** }

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-id*	Specifies the ID of an IoT card.	The IoT card ID must exist.
card usb	Specifies an IoT card of the USB type.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An IoT card involves network parameters for communicating with a host computer (such as the card IP address, server IP address, and DNS address) and air interface parameters in a wireless environment. In most cases, when the wireless environment becomes stable, air interface parameters remain unchanged. When the wired environment changes, you can only run the **iot-card reset-network-configuration** command to reset network parameters of the IoT card. During this process, the air interface parameters remain unchanged.

This command is supported only by **Ethernet port cards**.

Example

Reset network parameters of an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card reset-network-configuration ap ap-id 1 card 1
```

11.16.17 iot-card switch-firmware

Function

The **iot-card switch-firmware** command switches the active and standby partitions of an IoT card.

Format

iot-card switch-firmware ap ap-id *ap-id* **card** *card-id*

Parameters

Parameter	Description	Value
ap ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-id*	Specifies the ID of an IoT card.	The IoT card ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Upon a fault on the current partition of an IoT card, you can run this command to switch to the other partition.

Example

Switch the active and standby partitions of an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-card switch-firmware ap ap-id 1 card 1
```

11.16.18 iot-profile (WLAN view)

Function

The **iot-profile** command creates an IoT profile and displays the IoT profile view.

The **undo iot-profile** command deletes an IoT profile.

By default, no IoT profile is created.

Format

iot-profile name *profile-name*

undo iot-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an IoT profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Specifies all IoT profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP functions as a server or client to communicate with the host computer in bi-directional mode. When the AP reports data to the host computer, the AP functions as a client and the host computer functions as a server. When the AP receives data from the host computer, the AP functions as a server and the host computer functions as a client.

Example

Create IoT profile **profile1** and display the IoT profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1]
```

11.16.19 iot-profile (IoT card interface view)

Function

The **iot-profile** command binds an IoT profile to an IoT card interface, and configures the local port number mapping the IoT card interface.

The **undo iot-profile** command unbinds an IoT profile from an IoT card interface.

By default, no IoT profile is bound to an IoT card interface.

Format

iot-profile *profile-name* **config-agent** { **tcp** | **udp** } [**port** *port*] [**ext-port** *ext-port*]

undo iot-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an IoT profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
tcp	Configures the AP to communicate with the host computer using TCP.	-
udp	Configures the AP to communicate with the host computer using UDP.	-
port *port*	Specifies the source port for the first channel.	The value is an integer that ranges from 1025 to 55535. By default, the port number is a random port number in the range of 49152 to 65535. **NOTE** A port number within the range from 50200 to 50202 is recommended. If another port number is used, a port conflict may occur and an alarm is generated.

Parameter	Description	Value
ext-port *ext-port*	Specifies the source port for the extended channel.	The value is an integer that ranges from 1025 to 55535. By default, the port number is a random port number in the range of 49152 to 65535. **NOTE** A port number within the range from 50200 to 50202 is recommended. If another port number is used, a port conflict may occur and an alarm is generated.

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to bind an IoT profile, configure the communication protocol between the AP and host computer, and configure the source port number for the IoT card interface.

Example

Bind IoT profile **profile1** and set the local UDP port number to 50200.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1] iot-profile profile1 config-agent udp port 50200
```

11.16.20 management-server

Function

The **management-server** command configures a host computer.

The **undo management-server** command deletes the host computer configuration.

By default, no host computer is configured.

Format

management-server { **domain** *domain-name* | **server-ip** *server-ip* } **server-port** *server-port-num* [**ext-channel**]

undo management-server { **domain** *domain-name* | **server-ip** *server-ip* } [**server-port** *server-port-num*] [**ext-channel**]

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of a host computer.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, and underscores (_) or dots (**.**).
server-ip *server-ip*	Specifies the IP address of a host computer.	The value is in dotted decimal notation.
server-port *server-port-num*	Specifies the port number of a host computer.	The value is an integer that ranges from 1 to 65535.
ext-channel	Specifies an extension channel.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP functions as a server or client to communicate with a host computer in bi-directional mode. When the AP reports data (Huawei APs only transparently transmit data to the host computer, and do not parse or collect data) to the host computer, the AP functions as a client and the host computer functions as a server. When the AP receives data from the host computer, the AP functions as a server and the host computer functions as a client. The domain name/IP address and one port of at least one host computer must be configured. Otherwise, serial data reported by the AP will be discarded.

Precautions

You can configure multiple host computers. An IoT card of the **common** type supports a maximum of four host computers. After four host computers have been configured, you need to delete a host computer before adding a new host computer. Host computers can only be deleted or added, but cannot be modified. An IoT card of the **cas-edu** type supports only one host computer.

When a ZigBee card is used, information about two host computers must be configured. The channel of the second host computer is an extension channel specified by the **ext-channel** parameter. Only one extension channel can be configured. The two channels cannot be configured with the same port number and IP address, or the same port number and domain name.

When multiple host computers are configured, the device automatically selects one available host computer for link establishment rather than establish links with multiple host computers.

Example

Configure an IP address and a port number for a host computer.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1] management-server server-ip 10.1.1.2 server-port 3000
```

11.16.21 reset ap-card statistics

Function

The **reset ap-card statistics** command clears statistics on the packets received and sent by cards on APs.

Format

reset ap-card statistics { **all** | **ap-id** *ap-id* [**card** { *card-number* | **usb** }] }

Parameters

Parameter	Description	Value
all	Specifies cards on all APs.	-
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
card *card-number*	Specifies an IoT card interface number.	The interface number must exist.

Parameter	Description	Value
usb	Specifies the USB interface on an IoT card.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to clear statistics on the packets received and sent by cards on APs. Only statistics about IoT cards with the serial connection type can be cleared.

Precautions

The statistics cannot be restored after being cleared.

Example

Clear statistics on the packets received and sent by cards on all APs.

```
<HUAWEI> reset ap-card statistics all
```

11.16.22 share-key

Function

The **share-key** command configures a shared key.

The **undo share-key** command deletes a shared key.

By default, no shared key is configured.

Format

share-key *key-value*

undo share-key

Parameters

Parameter	Description	Value
key-value	Specifies a shared key.	The value is a string of characters. ● The key in plaintext contains 6 to 32 characters. ● The key in ciphertext contains 48 or 68 characters. **NOTE** To ensure security, a shared key must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters.

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure a shared key to improve data communication security and ensure completeness of packets exchanged between an AP and host computers. The shared key must be the same on the AP and host computers.

Precautions

After the **type cas-edu** command is executed to set the card type to **cas-edu**, the **share-key** command cannot be executed.

Example

Set the shared key to **aabb0011@11**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name profile1
[HUAWEI-wlan-iot-prof-profile1] share-key aabb0011@11
```

11.16.23 type (IoT profile view)

Function

The **type** command sets the type of an IoT card.

The **undo type** command restores the default IoT card type.

The default type of an IoT card is **common**.

Format

type { **cas-edu** | **common** }

undo type

Parameters

Parameter	Description	Value
cas-edu	Indicates an IoT card that complies with IoT standards of the China Academy of Science.	-
common	Indicates an IoT card that complies with Huawei's IoT standards.	-

Views

IoT profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an interconnection with the education system solution of the China Academy of Science, set the IoT card type to **cas-edu**. In other scenarios, set the IoT card type to **common**.

Precautions

After the IoT card type is modified in an IoT profile, other parameters in this IoT profile will restore to the default values.

If the **iot-profile (IoT card interface view)** command has been executed to bind an IoT profile, the IoT card type cannot be modified. The IoT card type can be modified only after the IoT profile is unbound.

After the **type cas-edu** command is executed to set the card type to **cas-edu**, the **config-agent permit ip-address** and **share-key** commands cannot be executed.

Example

Set the IoT card type to **cas-edu**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] iot-profile name wlan-iot
[HUAWEI-wlan-iot-prof-wlan-iot] type cas-edu
Warning: After the card type is modified, related configuration items in the profile are cleared. Continue?
[Y/N]:y
```

11.16.24 wired-port-profile (IoT card interface view)

Function

The **wired-port-profile** command binds a specified AP wired port profile to an IoT card.

The **undo wired-port-profile** command unbinds the AP wired port profile from an IoT card.

By default, no AP wired port profile is bound to an IoT card.

Format

wired-port-profile *profile-name*

undo wired-port-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The AP wired port profile must exist.

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IoT card communicates with an AP through an Ethernet interface, to configure this Ethernet interface, you can set parameters in an AP wired port profile and bind it to the IoT card.

Prerequisites

The IoT card has been configured to communicate with the AP through an Ethernet interface using the **card connect-type ethernet** command.

Example

Bind the AP wired port profile **wired-port1** to an IoT card.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wired-port-profile name wired-port1
[HUAWEI-wlan-wired-port-wired-port1] quit
[HUAWEI-wlan-view] ap-group name default
[HUAWEI-wlan-ap-group-default] card 1
[HUAWEI-wlan-group-card-default/1] wired-port-profile wired-port1
```

11.17 WLAN Traffic Optimization Commands

11.17.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.17.2 display wlan igmp-snooping vap-cac

Function

The **display wlan igmp-snooping vap-cac** command displays the multicast CAC configuration and statistics on a VAP.

Format

display wlan igmp-snooping vap-cac { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the multicast CAC configuration and statistics on a VAP, including the bandwidth and user statistics.

Example

Display the multicast CAC configuration and statistics on VAPs of the AP with ID 0.

```
<HUAWEI> display wlan igmp-snooping vap-cac ap-id 0
Info: This operation may take a few seconds, please wait.done.
Rf            : Radio ID                 WID             : WLAN ID
CurBw         : Current bandwidth(kbps)   MaxBw           : Max bandwidth(kbps)
CurUser       : Current user number       MaxUser         : Max user number
BwUtilization : Bandwidth utilization     UserUtilization : User utilization
--------------------------------------------------------------------------------
Rf  WID  CurBw/MaxBw        BwUtilization  CurUser/MaxUser  UserUtilization
--------------------------------------------------------------------------------
0   1    0/11                 0%             0/6              0%
--------------------------------------------------------------------------------
Total: 1
```

Table 11-310 Description of the **display wlan igmp-snooping vap-cac** command output

Item	Description
Rf	Radio ID.
WID	WLAN ID.
CurBw/MaxBw	Current multicast bandwidth/ Maximum multicast bandwidth of a VAP.
BwUtilization	Multicast bandwidth utilization.
CurUser/MaxUser	Current number of multicast users/ Maximum number of multicast users on a VAP.
UserUtilization	Multicast user utilization.

11.17.3 igmp-snooping group-bandwidth (AP system profile view)

Function

The **igmp-snooping group-bandwidth** command configures the bandwidth of global multicast groups on an AP.

The **undo igmp-snooping group-bandwidth** command deletes the bandwidth of global multicast groups on an AP.

By default, the bandwidth of global multicast groups is not configured on an AP.

Format

igmp-snooping group-bandwidth start-group-address *start-group-address* **end-group-address** *end-group-address* **bandwidth** *bandwidth-value*

undo igmp-snooping group-bandwidth start-group-address *start-group-address* **end-group-address** *end-group-address*

Parameters

Parameter	Description	Value
start-group-address *start-group-address*	Specifies the start multicast group address.	The value is in dotted decimal notation.
end-group-address *end-group-address*	Specifies the end multicast group address.	The value is in dotted decimal notation.
bandwidth *bandwidth-value*	Specifies the bandwidth of multicast groups.	The value is an integer that ranges from 1 to 100000, in kbps.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the bandwidth of multicast groups in an AP system profile according to the actual bandwidth of a multicast program. This configuration takes effect for the APs or AP groups to which this AP system profile is bound. When users request to order this multicast program, the collects statistics on the current multicast bandwidth of the VAP according to the configured bandwidth of global multicast groups, and compares the current bandwidth with the configured maximum bandwidth to determine whether to allow users to order this multicast program.

Precautions

You can configure the bandwidth for a maximum of 32 multicast group address segments. Addresses in one address segment must be different from those in another address segment. The configured address segments must contain valid multicast program addresses.

Example

Set the bandwidth to 100 kbps for multicast group address segment from 224.0.1.0 to 224.255.255.255.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] igmp-snooping group-bandwidth start-group-address
224.0.1.0 end-group-address 224.255.255.255 bandwidth 100
```

11.17.4 igmp-snooping max-bandwidth (traffic profile view)

Function

The **igmp-snooping max-bandwidth** command configures the maximum multicast bandwidth for a VAP.

The **undo igmp-snooping max-bandwidth** command deletes the maximum multicast bandwidth of a VAP.

By default, the maximum multicast bandwidth is not configured for a VAP.

Format

igmp-snooping max-bandwidth *max-bandwidth*

undo igmp-snooping max-bandwidth

Parameters

Parameter	Description	Value
max-bandwidth	Specifies the maximum multicast bandwidth of a VAP.	The value is an integer that ranges from 1 to 10000000, in kbit/s.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum multicast bandwidth is configured for a VAP in a traffic profile to limit the multicast traffic forwarding capacity of the VAP to which this traffic profile is bound. When the available multicast bandwidth of a VAP is insufficient, new users are prevented from joining multicast groups.

Precautions

After configuring the maximum multicast bandwidth for a VAP, run the **igmp-snooping group-bandwidth (AP system profile view)** command to configure the bandwidth of global multicast groups on the AP.

If the specified maximum multicast bandwidth is smaller than the actual volume of running multicast services, user services may be interrupted.

Example

Set the maximum multicast bandwidth to 500 kbit/s in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping max-bandwidth 500
```

11.17.5 igmp-snooping max-user (traffic profile view)

Function

The **igmp-snooping max-user** command configures the maximum number of multicast group memberships for a VAP.

The **undo igmp-snooping max-user** command deletes the maximum number of multicast group memberships for a VAP.

By default, the maximum number of multicast group memberships is not configured for a VAP.

Format

igmp-snooping max-user *max-user*

undo igmp-snooping max-user

Parameters

Parameter	Description	Value
max-user	Specifies the maximum number of multicast group memberships on a VAP.	The value is an integer that ranges from 1 to 1000.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum number of multicast group memberships on a VAP is configured in a traffic profile to limit access of multicast users on the VAP to which this traffic profile is bound. When the number of multicast group memberships on a VAP reaches the maximum value, new users are prevented from joining multicast groups.

Precautions

If the specified maximum number of multicast group memberships is smaller than the actual number of access multicast users, user services may be interrupted.

Example

Set the maximum number of multicast group memberships to 10 on the VAP to which traffic profile **p1** is bound.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping max-user 10
```

11.17.6 igmp-snooping enable (traffic profile view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a traffic profile.

The **undo igmp-snooping enable** command disables IGMP snooping in a traffic profile.

By default, IGMP snooping is disabled in a traffic profile.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping is a basic Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. IGMP snooping runs on a Layer 2 device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

After you disable IGMP snooping in a traffic profile using the **undo igmp-snooping enable** command, all IGMP snooping configurations in the traffic profile are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping again, all IGMP snooping configurations are restored to the default settings on the device.

Prerequisites

The traffic profile has been created using the **traffic-profile (WLAN view)** command.

This command is used to enable Layer 2 multicast services. To ensure multicast service experience, you are advised to run the **traffic-optimize broadcast-suppression other-multicast disable** command in the AP system profile view to disable rate limiting for multicast packets. In addition, run the **anti-attack flood igmp disable** and **anti-attack flood other-multicast disable** commands in the VAP profile view to disable floor attack defense for multicast packets.

When multicast services are enabled, the multicast services may be affected if rate limiting for multicast packets is enabled on an AP. In this case, you are advised to run the **traffic-optimize broadcast-suppression rate-threshold (AP system profile view)** command to adjust the rate limit threshold for multicast packets.

When multicast services are enabled, the multicast services may be affected if flood attack defense is disabled in the VAP profile view. In this case, you are advised to run the **anti-attack flood { igmp | other-multicast } sta-rate-threshold** *sta-rate-threshold* command to adjust the flood attack threshold for multicast packets.

Example

Enable IGMP snooping in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping enable
```

11.17.7 igmp-snooping report-suppress (Traffic profile view)

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave message in a traffic profile.

The **undo igmp-snooping report-suppress** command cancels configuration of IGMP Report and Leave message suppression in a traffic profile.

By default, IGMP Report and Leave message suppression is disabled in a traffic profile.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages in the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Leave messages from the member hosts.

After this function is configured, a Layer 2 device forwards only one IGMP Membership Report message to the upstream device in the following scenarios: When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device then creates or maintains the matching forwarding entry based on the Report message. When the last member of a group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry. This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled using the **igmp-snooping enable (traffic profile view)** command.

Example

Enable suppression of IGMP Report and Leave messages in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping enable
[HUAWEI-wlan-traffic-prof-p1] igmp-snooping report-suppress
```

11.17.8 mld-snooping enable (traffic profile view)

Function

The **mld-snooping enable** command enables MLD snooping in a traffic profile.

The **undo mld-snooping enable** command disables MLD snooping in a traffic profile.

By default, MLD snooping is disabled in a traffic profile.

Format

mld-snooping enable

undo mld-snooping enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mld-snooping enable** command to enable MLD snooping in a traffic profile.

After you disable MLD snooping in a traffic profile using the **undo mld-snooping enable** command, all MLD snooping configurations in the traffic profile are deleted. When you run the **mld-snooping enable** command to enable MLD snooping again, all MLD snooping configurations are restored to the default settings in the traffic profile.

Prerequisites

A traffic profile has been created.

Before enabling MLD snooping in a traffic profile, run the **sta-ipv6-service enable** commands to enable the function of processing STA IPv6 services in the WLAN view.

Example

Enable MLD snooping in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] mld-snooping enable
```

11.17.9 service-guarantee

Function

The **service-guarantee** command configures the service guarantee mode.

The **undo service-guarantee** command restores the default service guarantee mode.

The default service guarantee mode is performance-first.

Format

service-guarantee { **performance-first** | **reliability-first** }

undo service-guarantee

Parameters

Parameter	Description	Value
performance-first	Sets the service guarantee mode to performance-first.	-
reliability-first	The service guarantee mode is set to reliability-first.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP is connected to a VR device, retransmission of lost packets has a great impact on user experience. Therefore, you can set the service guarantee mode to reliability first. That is, when the VR throughput requirement is met, the air interface rate can be lowered properly to reduce jitter and delay caused by packet loss and retransmission, improving user experience. It is recommended that the service assurance mode be set to reliability first in VR gaming scenarios and to performance first in VR video scenarios.

Precautions

Changing the service guarantee mode will interrupt services of associated STAs.

Traffic optimization in VR scenarios is supported only by APs in compliance with 802.11ac Wave 2, 802.11ax and later standards.

Example

Set the service guarantee mode to reliability-first.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] service-guarantee reliability-first
```

11.17.10 traffic-optimize arp-proxy enable

Function

The **traffic-optimize arp-proxy enable** command enables ARP proxy on the device.

The **undo traffic-optimize arp-proxy enable** command disables ARP proxy on the device.

By default, ARP proxy is disabled.

Format

traffic-optimize arp-proxy enable

undo traffic-optimize arp-proxy enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an ARP Request packet is sent from a user or the network to another user, the AC or AP enabled with ARP proxy can reply to this packet. Compared with the function of converting ARP multicast packets to ARP unicast packets, ARP proxy can reduce the number of times a sleeping terminal is awakened to save power.

Precautions

The ARP proxy function is not available for roaming users.

Example

Enable ARP proxy on the device in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize arp-proxy enable
```

11.17.11 traffic-optimize bcmc deny all

Function

The **traffic-optimize bcmc deny all** command configures the air interface to deny downlink broadcast and multicast packets.

The **undo traffic-optimize bcmc deny all** command cancels the configuration of denying downlink broadcast and multicast packets on the air interface.

By default, the air interface does not deny downlink broadcast or multicast packets.

Format

traffic-optimize bcmc deny all [**except mdns**]

undo traffic-optimize bcmc deny all

Parameters

Parameter	Description	Value
except mdns	If this parameter is configured, mDNS packets are allowed to pass through when the air interface is configured to deny broadcast and multicast packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IP network, the ARP, ND, and DHCP protocols are the basic network protocols and serve as the basis for packet forwarding on the entire network.

Broadcast or multicast packets of protocols other than the ARP, ND, and DHCP protocols are optional on the IP network. When no services rely on transmission of these broadcast or multicast packets on the network, you can run the command to configure the air interface to deny all broadcast and multicast packets to improve the air interface performance.

Precautions

Before using the **traffic-optimize bcmc deny all** command to configure the air interface to deny downlink broadcast and multicast packets on the AP, run the **undo learn-client-address { ipv4 | ipv6 } disable** command to enable STA address learning and the **traffic-optimize bcmc unicast-send** { **arp** | **nd** | **dhcp** | **mdns** } * command to configure the broadcast/multicast-to-unicast conversion function on the air interface. Otherwise, the ARP, ND, and DHCP packets may fail to be forwarded.

Example

Configure the air interface to deny downstream broadcast and multicast packets in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize bcmc deny all
```

11.17.12 traffic-optimize bcmc unicast-send

Function

The **traffic-optimize bcmc unicast-send** { **arp** | **nd** | **dhcp** | **mdns** }* command configures the broadcast/multicast-to-unicast conversion function on the air interface.

The **undo traffic-optimize bcmc unicast-send** { **arp** | **nd** | **dhcp** | **mdns** }* command cancels the configuration of the broadcast/multicast-to-unicast conversion function on the air interface.

The **undo traffic-optimize bcmc unicast-send** command restores the default configuration.

By default, the broadcast/multicast-to-unicast conversion function is enabled for ARP, ND, and DHCP packets but disabled for mDNS packets on the air interface.

Format

traffic-optimize bcmc unicast-send { **arp** | **nd** | **dhcp** | **mdns** }*

undo traffic-optimize bcmc unicast-send { **arp** | **nd** | **dhcp** | **mdns** }*

undo traffic-optimize bcmc unicast-send

Parameters

Parameter	Description	Value
arp	Specifies ARP packets.	-
nd	Specifies ND packets.	-
dhcp	Specifies DHCP packets.	-
mdns	Specifies mDNS packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an air interface sends a large number of broadcast or multicast packets when being busy, the performance of the air interface will drop. To prevent this situation, you can configure the broadcast/multicast-to-unicast conversion function to reduce the number of broadcast or multicast packets transmitted on the air interface. This improves air interface performance at the price of increased CPU usage.

Prerequisites

The **undo learn-client-address { ipv4 | ipv6 } disable** command has been executed to enable STA address learning.

Example

Configure the broadcast/multicast-to-unicast conversion function for **DHCP** packets in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize bcmc unicast-send dhcp
```

11.17.13 traffic-optimize bcmc unicast-send mismatch-action drop

Function

The **traffic-optimize bcmc unicast-send mismatch-action drop** command discards broadcast or multicast packets that fail to be converted into unicast packets on air interfaces.

The **undo traffic-optimize bcmc unicast-send mismatch-action drop** command restores the default action, that is, send broadcast or multicast packets that fail to be converted into unicast packets on air interfaces to all users in unicast mode.

By default, if broadcast or multicast packets fail to be converted into unicast packets on air interfaces, the packets are discarded.

Format

traffic-optimize bcmc unicast-send mismatch-action drop

undo traffic-optimize bcmc unicast-send mismatch-action drop

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if broadcast or multicast packets fail to be converted into unicast packets on air interfaces, the packets are discarded. To enable the system to send these packets to all users, run the **undo traffic-optimize bcmc unicast-send mismatch-action drop** command.

Prerequisites

- The **traffic-optimize bcmc unicast-send** command has been executed to configure the function of converting broadcast or multicast packets to unicast packets on an air interface.
- The **undo learn-client-address { ipv4 | ipv6 } disable** command has been executed to enable STA address learning.

Example

Configure the system to send the broadcast or multicast packets that fail to be converted into unicast packets on air interfaces to all users.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] undo traffic-optimize bcmc unicast-send mismatch-action drop
```

11.17.14 traffic-optimize broadcast-suppression

Function

The **traffic-optimize broadcast-suppression** command sets the maximum traffic volume of broadcast packets that can pass through a traffic profile.

The **undo traffic-optimize broadcast-suppression** command cancels the limit on the maximum traffic volume of broadcast packets that can pass through a traffic profile.

By default, broadcast packets are not suppressed in a traffic profile.

Format

traffic-optimize broadcast-suppression packets *packets-rate*

undo traffic-optimize broadcast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value is an integer that ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of broadcast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To prevent broadcast storms, you can run the **traffic-optimize broadcast-suppression** command to configure the maximum traffic volume of broadcast packets that can pass through a traffic profile. When the traffic volume of broadcast packets reaches the maximum in a traffic profile, the system discards excess broadcast packets to control the traffic volume in a proper range.

Precautions

Traffic suppression on the wireless side takes effect only for incoming traffic on the AP's air interface.

Example

Set the maximum traffic volume of broadcast packets that can pass through to 21600 pps in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets 21600
```

11.17.15 traffic-optimize multicast-suppression

Function

The **traffic-optimize multicast-suppression** command sets the maximum traffic volume of multicast packets in a traffic profile.

The **undo traffic-optimize multicast-suppression** command cancels the limit on the maximum traffic volume of multicast packets in a traffic profile.

By default, multicast packets are not suppressed in a traffic profile.

Format

traffic-optimize multicast-suppression packets *packets-rate*

undo traffic-optimize multicast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of multicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To ensure normal service transmission on a network, you can run the **traffic-optimize multicast-suppression** command to configure the maximum multicast traffic volume in a traffic profile. When the traffic volume of multicast packets reaches the maximum, the system discards excess multicast packets to control the traffic volume in a proper range.

Precautions

Traffic suppression on the wireless side takes effect only for incoming traffic on the AP's air interface.

Example

Set the maximum traffic volume of multicast packets to 21600 pps in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-suppression packets 21600
```

11.17.16 traffic-optimize multicast-unicast enable

Function

The **traffic-optimize multicast-unicast enable** command enables the multicast-to-unicast conversion function in a traffic profile.

The **undo traffic-optimize multicast-unicast enable** command disables the multicast-to-unicast conversion function in a traffic profile.

By default, the multicast-to-unicast conversion function is disabled in a traffic profile.

NOTE

Multicast-to-unicast conversion of data packets on the air interface is not supported by the following model:

- AirEngine 8771-X1T

Format

traffic-optimize multicast-unicast enable

undo traffic-optimize multicast-unicast enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable the multicast-to-unicast conversion function in scenarios that have high requirements on multicast stream transmission, such as high-definition (HD) video on demand (VOD) scenarios.

After this function is enabled, an AP listens on Report and Leave packets to maintain multicast-to-unicast entries. When sending multicast packets to STAs, the AP converts the multicast packets into unicast packets based on the multicast-to-unicast entries to improve multicast stream transmission efficiency.

Example

Enable the multicast-to-unicast conversion function in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-unicast enable
```

11.17.17 traffic-optimize multicast-unicast dynamic-adaptive disable

Function

The **traffic-optimize multicast-unicast dynamic-adaptive disable** command disables adaptive multicast-to-unicast conversion in a traffic profile.

The **undo traffic-optimize multicast-unicast dynamic-adaptive disable** command enables adaptive multicast-to-unicast conversion in a traffic profile.

By default, adaptive multicast-to-unicast conversion is enabled in a traffic profile.

NOTE

Multicast-to-unicast conversion of data packets on the air interface is not supported by the following model:

- AirEngine 8771-X1T

Format

traffic-optimize multicast-unicast dynamic-adaptive disable

undo traffic-optimize multicast-unicast dynamic-adaptive disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After adaptive multicast-to-unicast conversion is enabled, when the air interface performance becomes a bottleneck during multicast-to-unicast conversion, an AP automatically switches the multicast group containing the minimum number of STAs to the multicast mode. After the air interface performance is improved and keeps being improved for a period of time, the AP automatically switches the multicast group containing the maximum number of STAs to the unicast mode. In this way, the air interface performance is automatically adjusted without manual intervention, improving wireless user experience.

Pre-configuration Tasks

The multicast-to-unicast conversion function has been enabled in the traffic profile using the **traffic-optimize multicast-unicast enable** command.

Example

Disable adaptive multicast-to-unicast conversion in traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-unicast enable
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize multicast-unicast dynamic-adaptive disable
```

11.17.18 traffic-optimize nd-proxy enable

Function

The **traffic-optimize nd-proxy enable** command enables ND proxy on the device.

The **undo traffic-optimize nd-proxy enable** command disables ND proxy on the device.

By default, ND proxy is disabled.

Format

traffic-optimize nd-proxy enable

undo traffic-optimize nd-proxy enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an ND Request packet is sent from a user or the network to another user, the AC or AP enabled with ND proxy can reply to this packet. Compared with the function of converting ND multicast packets to unicast packets, ND proxy can reduce the number of times a sleeping terminal is awakened to save power.

Precautions

The ND proxy function is not available for roaming users.

Example

Enable ND proxy on the device in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize nd-proxy enable
```

11.17.19 traffic-optimize sta-bridge-forward disable

Function

The **traffic-optimize sta-bridge-forward disable** command configures the function of denying packets destined for bridge STAs on the air interface.

The **undo traffic-optimize sta-bridge-forward disable** command cancels the function of denying packets destined for bridge STAs on the air interface.

By default, the air interface does not deny packets destined for bridge STAs.

Format

traffic-optimize sta-bridge-forward disable

undo traffic-optimize sta-bridge-forward disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Some terminals on the wireless network can provide bridging functions. The terminals associate with APs with their MAC addresses and connect to multiple Layer 3 wired devices in the downlink direction. The connected Layer 3 wired devices can also obtain IP addresses and forward traffic through the APs. The APs consider that the associated terminals have multiple IP addresses. You can run the command to configure the function of denying packets destined for bridge STAs on the air interface. This can reduce the number of packets transmitted on the air interfaces and improve the air interface performance.

Example

Configure the function of denying packets destined for bridge STAs on the air interface in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize sta-bridge-forward disable
```

11.17.20 traffic-optimize tcp adjust-mss

Function

The **traffic-optimize tcp adjust-mss** command sets the maximum segment size (MSS) of TCP packets in a traffic profile.

The **undo traffic-optimize tcp adjust-mss** command deletes the configured MSS of TCP packets in a traffic profile.

By default, the MSS of TCP packets in a traffic profile is not configured.

Format

traffic-optimize tcp adjust-mss *value*

undo traffic-optimize tcp adjust-mss

Parameters

Parameter	Description	Value
value	Specifies the MSS of TCP packets in a traffic profile.	The value is an integer that ranges from 128 to 2048, in bytes.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MSS is an option defined in the TCP protocol and refers to the maximum length of TCP packets that can be received by a device. When setting up a TCP connection, the local and peer devices negotiate an MSS value to determine the maximum data length of TCP packets. If the length of TCP packets sent from the peer device exceeds the MSS value, the packets are fragmented.

Precautions

- To prevent TCP packets from being fragmented, you must configure a proper MSS based on the maximum transmission unit (MTU). The MTU is the option to determine whether IP packets will be fragmented. If the size of an IP packet exceeds the MTU, the IP packet will be fragmented. To ensure that a complete packet is transmitted properly, the MSS value plus all the header lengths (TCP header and IP header) cannot exceed the MTU. For example, a CAPWAP-encapsulated TCP packet consists of an outer IP header (20 bytes), a UDP header (8 bytes), a CAPWAP header (8 bytes), an ETH header (18 bytes), an inner IP header (20 bytes), a TCP header (20 bytes), and TCP data. If the default MTU is 1500 on the device, the MSS value can be set to a maximum of 1406 bytes so that the CAPWAP-encapsulated TCP packet is not fragmented by the device. In case that the CAPWAP header or TCP header carries option fields, it is recommended that you set the MSS to 1380 bytes.
- The MSS configured by the **traffic-optimize tcp adjust-mss** command takes effect on the AP as a TCP client or server. Additionally, if packets of other devices as clients pass through the AP, the negotiation result is modified based on the MSS configured using this command only when the MSS received by the AP is larger than that configured using this command.
- If you run the **traffic-optimize tcp adjust-mss** command in the same interface view multiple times, only the latest configuration takes effect.

Example

Set the MSS of TCP packets to 1200 bytes in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize tcp adjust-mss 1200
```

11.17.21 traffic-optimize unicast-suppression

Function

The **traffic-optimize unicast-suppression** command sets the maximum traffic volume of unknown unicast packets in a traffic profile.

The **undo traffic-optimize unicast-suppression** command cancels the limit on the maximum traffic volume of unknown unicast packets in a traffic profile.

By default, unknown unicast packets are not suppressed in a traffic profile.

Format

traffic-optimize unicast-suppression packets *packets-rate*

undo traffic-optimize unicast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of unknown unicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To prevent broadcast storms, you can run the **traffic-optimize unicast-suppression** command to configure the maximum traffic volume of unknown unicast packets that can pass through an interface. When the traffic volume of unknown unicast packets reaches the maximum on an interface, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Precautions

Traffic suppression on the wireless side takes effect only for incoming traffic on the AP's air interface.

Example

Set the maximum traffic volume of unknown unicast packets to 21600 pps in the traffic profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] traffic-profile name p1
[HUAWEI-wlan-traffic-prof-p1] traffic-optimize unicast-suppression packets 21600
```

11.18 Centralized License Control Commands

11.18.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.18.2 license centralized enable

Function

The **license centralized enable** command enables centralized license control.

The **undo license centralized enable** command disables centralized license control.

By default, centralized license control is disabled.

Format

license centralized enable

undo license centralized enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When centralized license control is enabled on both the license server and license clients, licenses in the license resource pool can be centrally controlled on the license server and shared by both the license server and license clients.

Example

Enable centralized license control.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] license centralized enable
```

11.18.3 license server

Function

The **license server** command specifies the IP address of the license server on a license client. This IP address must be the same as the CAPWAP source address configured on the license server.

The **undo license server** command deletes the local IP address of the license server on a license client.

By default, no IP address is set for the license server.

Format

license server ip-address *ip-address*

undo license server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IPv4 address of the license server.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After centralized license control is enabled, you can run the **license server** command on a license client to set an IP address for the license server, so that the license client can set up a link with the license server and be managed by the license server.

Prerequisites

The local IP address of the license client has been configured. Run the **license client source ip-address** *ip-address* command to configure the local IP address of the license client.

- When multiple CAPWAP source addresses exist, use this configuration to specify one CAPWAP source address as the local address.
- If the license client is a single device, the source address configuration is not required. Instead, the CAPWAP source address is used as the local address of the license client by default.

Example

Set the IP address for the license server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] license server ip-address 10.1.1.1
```

11.18.4 license client source

Function

The **license client source** command configures a local IP address for a license client.

The **undo license client source** command deletes the local IP address of a license client.

By default, the first CAPWAP source IP address is used as the local IP address of a license client.

Format

license client source ip-address *ip-address*

undo license client source

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the local IPv4 address of the license client.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When multiple CAPWAP source addresses exist, use this configuration to specify one CAPWAP source address as the local address.
- If the license client is a single device, the source address configuration is not required. Instead, the CAPWAP source address is used as the local address of the license client by default.

Example

Set the local IP address of a license client to 10.1.2.1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] license client source ip-address 10.1.2.1
```

11.18.5 display license centralized configuration

Function

The **display license centralized configuration** command displays the configuration of centralized license control.

Format

display license centralized configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether centralized license control is enabled and the IP address of the license server.

Example

Display the configuration of centralized license control on the license server.

```
<HUAWEI> display license centralized configuration
------------------------------------------------
License centralized server enable :    enable
License server IP                 :    -
------------------------------------------------
```

Display the configuration of centralized license control on a license client.

```
<HUAWEI> display license centralized configuration
------------------------------------------------
License centralized server enable :    enable
License server IP                 :    10.1.1.1
License local IP                  :    10.1.1.2
------------------------------------------------
```

Table 11-311 Description of the **display license centralized configuration** command output

Item	Description
License centralized server enable	Whether centralized license control is enabled. - enable: Centralized license control is enabled. - disable: Centralized license control is disabled. To configure this parameter, run the **license centralized enable** command.
License server IP	IP address of the license server. To configure this parameter on a license client, run the **license server** command.
License local IP	Local IP address of the license client. To configure this parameter on a license client, run the **license client source** command. If this parameter is not configured, **-** is displayed.

11.18.6 display license resource usage detail

Function

The **display license resource usage detail** command displays the license resource usage in the license resource pool or on a single AC.

Format

display license resource usage detail

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

- If centralized license control is enabled, you can run this command on the license server to check the license resource usage in the license resource pool, on all license servers, and on all license clients. On a license client, you can run this command to check the license resource usage in the license resource pool and on the local AC.
- When centralized license control is disabled, you can run this command to check the license resource usage on the local AC and backup AC.

Example

Display the license resource usage on a license server.

```
<HUAWEI> display license resource usage detail
Remain(days): Remaining days of the license resource pool after the client goes offline
Current role        :  server
Used/Total resource:  300/1100
----------------------------------------------------------------------------------------------------
MAC              Role           State     Local License  Used     Remain(days)    IP
----------------------------------------------------------------------------------------------------
0000-0000-0015     server         normal   100          200      -             -
0000-0000-0017     client         normal   600          100      -             1.1.1.3
0000-0000-0018     client         fault    100          -        20            1.1.1.5
----------------------------------------------------------------------------------------------------
Total records: 4
```

Display the license resource usage on a license client.

```
<HUAWEI> display license resource usage detail
Remain(days): Remaining days of the license resource pool after the client goes offline
Current role        :  client
Used/Total resource:  300/1100
----------------------------------------------------------------------------------------------------
MAC            Role           State     Local License  Used     Remain(days)    IP
----------------------------------------------------------------------------------------------------
0000-0000-0023   client         normal   600          100      -             1.1.1.3
----------------------------------------------------------------------------------------------------
Total records: 1
```

Display the license resource usage on an AC when centralized license control is not in effect.

```
<HUAWEI> display license resource usage detail
Remaining days: Remaining days of the backup license
Used/Total resource    :    0/4
----------------------------------------------------------------------------------------------------
 AC MAC           License     Backup Time                  Remaining Days    Backup Mode
----------------------------------------------------------------------------------------------------
 Local AC         4           -                            -               -
----------------------------------------------------------------------------------------------------
Total records: 1
```

Table 11-312 Description of the **display license resource usage detail** command output

Item	Description
Current role	Role of the current AC. ● server ● client

Item	Description
Used/Total resource	License resource usage, that is, ratio of the number of used licenses to the total number of licenses.
MAC	MAC address of an AC.
Role	Role of an AC. ● server ● client
State	State of the link between a license client and the license server. ● normal: The license client is properly connected to the license server. ● fault: The license client is disconnected from the license server.
Local License	Number of loaded licenses on an AC.
Used	Number of used licenses on an AC.
Remain(days)	Remaining days of the license resource pool after the license client is disconnected from the license server.
IP	IP address used by a license client to set up a link with the license server.
AC MAC	MAC address of the backup AC. **Local AC** indicates the local AC.
License	Number of loaded licenses on the AC.
Backup Time	Time when licenses are backed up. This field is unavailable currently and is displayed as **-**.
Remaining Days	Remaining days of the backup license. This field is unavailable currently and is displayed as **-**.
Backup Mode	Backup mode. This field is unavailable currently and is displayed as **-**.

11.19 WLAN Reliability Commands

11.19.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.19.2 ac protect alarm-restrain enable

Function

The **ac protect alarm-restrain enable** command enables AP Fault alarm suppression.

The **undo ac protect alarm-restrain enable** command disables AP Fault alarm suppression.

By default, AP Fault alarm suppression is disabled.

Format

ac protect alarm-restrain enable

undo ac protect alarm-restrain enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In dual-link cold backup scenarios, after an AP becomes **Fault** on the active AC, switches to the standby AC, and works properly, the active AC generates an AP Fault alarm. If AP Fault alarms are not needed in this case, you can run this command to enable AP Fault alarm suppression.

After AP Fault alarm suppression is enabled, the active and standby ACs generate AP Fault alarms only when both ACs detect that an AP becomes faulty on them.

Precautions

The active and standby ACs notify each other of the AP status by exchanging packets. If communication between the ACs fails, AP Fault alarm suppression cannot take effect.

AP Fault alarm suppression can only suppress the AP Fault alarms caused by heartbeat timeout. If an AP is deleted or restarted using the **undo ap** or **ap-reset** command, the alarms cannot be suppressed.

Example

Enable AP Fault alarm suppression.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect alarm-restrain enable
```

11.19.3 ac protect cold-backup kickoff-station

Function

The **ac protect cold-backup kickoff-station** command enables the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured.

The **undo ac protect cold-backup kickoff-station** command restores the default setting.

By default, STAs using open system authentication remain connected to APs when an active/standby AC switchover is implemented.

Format

ac protect cold-backup kickoff-station

undo ac protect cold-backup kickoff-station

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

An active/standby switchover between two ACs that have dual-link cold backup configured causes a short service interruption.

- STAs not using open system authentication are disconnected from APs and need to go online again after the active/standby switchover.
- By default, STAs using open system authentication remain connected to APs and do not need to go online again after the active/standby switchover. You can run the **ac protect cold-backup kickoff-station** command to configure the STAs to be disconnected when an active/standby AC switchover is implemented.

Example

Enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect cold-backup kickoff-station
```

11.19.4 ac protect link-switch packet-loss echo-probe-time

Function

The **ac protect link-switch packet-loss echo-probe-time** command specifies the number of Echo packets sent within a statistics collection interval.

The **undo ac protect link-switch packet-loss echo-probe-time** command restores the default number of Echo packets sent within a statistics collection interval.

By default, the number of Echo packets sent within a statistics collection interval is 20.

Format

ac protect link-switch packet-loss echo-probe-time *echo-probe-time*

undo ac protect link-switch packet-loss echo-probe-time

Parameters

Parameter	Description	Value
echo-probe-time	Specifies the number of Echo packets.	The value is an integer that ranges from 6 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active/standby link switchover mode is set to the network stabilization mode, ACs periodically check whether the network stabilization of active and standby links meets the condition for triggering an active/standby link switchover and collect statistics about the specified number of Echo packets at each interval to calculate the network stabilization.

In N+1 backup scenarios, only one of the primary and backup ACs sets up a CAPWAP link with an AP at the same time. The network stabilization of this link can be calculated through Echo packets. The network stabilization of the link between the AP and another AC can be calculated through Primary Discovery packets. Statistics about Primary Discovery packets can also be collected by setting the parameter *echo-probe-time*.

Prerequisites

The active/standby link switchover mode has been set to the network stabilization mode using the **ac protect link-switch mode network-stabilization** command.

Example

Set the number of Echo packets sent within a statistics collection interval to 30.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name abc
[HUAWEI-wlan-ap-system-prof-abc] ac protect link-switch packet-loss echo-probe-time 30
```

11.19.5 ac protect link-switch mode

Function

The **ac protect link-switch mode** command configures the active/standby link switchover mode.

The **undo ac protect link-switch mode** command restores the default active/standby link switchover mode.

By default, the active/standby link switchover mode is the priority mode.

Format

ac protect link-switch mode { **priority** | **network-stabilization** }

undo ac protect link-switch mode

Parameters

Parameter	Description	Value
priority	Sets the active/standby link switchover mode to the priority mode.	-
network-stabilization	Sets the active/standby link switchover mode to the network stabilization mode.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In dual-link cold backup or hot standby scenarios, an AP simultaneously sets up active and standby links with active and standby ACs, respectively. If the active link is faulty, the AP switches service traffic to the standby link and goes online on the standby AC. When the active link recovers, the AP detects that this link has a higher priority than the other one and triggers a revertive switchover. After 20 Echo intervals, the AP switches service traffic back to the active AC.

- To enable an AP to preferentially switch service traffic to the active link, set the active/standby link switchover mode to the priority mode.
- To allow an AP to use a link with high network stabilization, set the active/standby link switchover mode to the network stabilization mode. When the condition for triggering an active/standby link switchover is met, the AP preferentially switches service traffic to the link on a network with higher stabilization. In this case, whether an active/standby link switchover is performed is only related to the network stabilization of links but not related to the active and standby roles of links. You can run the **ac protect link-switch packet-loss** { **gap-threshold** *gap-threshold* | **start-threshold** *start-threshold* } command to configure the condition for triggering an active/standby link switchover.

In N+1 backup scenarios, APs set up links only with the primary ACs. When a link between an AP and a primary AC fails, the AP sets up a link with the backup AC and goes online on the backup AC. When the primary AC is recovered, a revertive switchover is triggered. The AP switches the link back to the primary AC after 20 Echo intervals.

- To enable an AP to preferentially go online on the primary AC, set the active/standby link switchover mode to the priority mode.
- To allow an AP to use a link with high network stabilization, set the active/standby link switchover mode to the network stabilization mode.

Precautions

The active/standby link switchover mode applies to active and standby ACs configured using the **ac protect protect-ac** and **priority** commands, or the **primary-access** and **backup-access** commands.

Example

Set the active/standby link switchover mode to the network stabilization mode.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name abc
[HUAWEI-wlan-ap-system-prof-abc] ac protect link-switch mode network-stabilization
```

11.19.6 ac protect link-switch packet-loss

Function

The **ac protect link-switch packet-loss** command configures the packet loss rate start and difference thresholds for an active/standby link switchover.

The **undo ac protect link-switch packet-loss** command restores the default packet loss rate start and difference thresholds for an active/standby link switchover.

By default, the packet loss rate start and difference thresholds for an active/standby link switchover are 20% and 15%, respectively.

Format

ac protect link-switch packet-loss { **gap-threshold** *gap-threshold* | **start-threshold** *start-threshold* }

undo ac protect link-switch packet-loss { **gap-threshold** | **start-threshold** }

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the packet loss rate difference threshold for an active/standby link switchover.	The value is an integer that ranges from 5 to 60, in percentage.
start-threshold *start-threshold*	Specifies the packet loss rate start threshold for an active/standby link switchover.	The value is an integer that ranges from 5 to 60, in percentage.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active/standby link switchover mode is set to the network stabilization mode, ACs check whether the network stabilization of active and standby links meets the condition for triggering an active/standby link switchover. If so, service traffic is switched to the link with higher network stabilization. If not, the switchover is not performed.

In dual-link cold backup and hot standby scenarios, the network stabilization of active and standby links is determined based on the Echo packet loss rate. The active/standby link switchover is performed when the following conditions are met:

1. APs collect statistics about the specified number of Echo packets forwarded through the link in use at each interval and find that the calculated packet loss rate is higher than the packet loss rate start threshold.
2. The packet loss rate of the link in use is higher than that of the other link, and the difference between the two links' packet loss rates is higher than the packet loss rate difference threshold.

In N+1 backup scenarios, the network stabilization of the link between an AP and the current AC is determined by the Echo packet loss rate, and that of the link between the AP and another AC is determined by the Primary Discovery packet loss rate. The conditions for triggering an active/standby switchover are the same as those for dual-link cold backup and hot standby scenarios.

Prerequisites

The active/standby link switchover mode has been set to the network stabilization mode using the **ac protect link-switch mode network-stabilization** command.

Example

Set the packet loss rate start threshold for an active/standby link switchover to 30%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name abc
[HUAWEI-wlan-ap-system-prof-abc] ac protect link-switch packet-loss start-threshold 30
```

11.19.7 ac protect enable

Function

The **ac protect enable** command enables dual-link backup globally and disables N+1 backup.

The **undo ac protect enable** command disables dual-link backup globally and enables N+1 backup.

By default, dual-link backup is disabled globally, and N+1 backup is enabled.

Format

ac protect enable

undo ac protect enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure service stability, an AP needs to establish connections with two ACs. The two ACs work in active/standby mode. The active AC provides services for APs, whereas the standby AC is a backup to the active AC.

Follow-up Procedure

After dual-link backup or N+1 backup is enabled globally, configure the AC priority and standby AC IP address to implement dual-link backup or N+1 backup.

Precautions

Ensure that active and standby ACs deliver the same WLAN service configuration to an AP that connects to the two ACs.

Example

Enable dual-link backup globally and disable N+1 backup.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]:y
```

11.19.8 ac protect priority

Function

The **ac protect priority** command configures the AC priority in the WLAN view.

The **undo ac protect priority** command restores the default AC priority in the WLAN view.

By default, the AC priority in the WLAN view is 0.

Format

ac protect priority *priority*

undo ac protect priority

Parameters

Parameter	Description	Value
priority	Specifies the AC priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP goes online, ACs deliver their priorities to the AP. The AP selects the AC with a higher priority as the active AC and establishes a CAPWAP tunnel with the active AC.

To implement dual-link backup on all the APs connected to an AC, configure the AC priority and standby AC IP address in the WLAN view to reduce the configuration workload.

Precautions

If the AC priority is configured in the WLAN view and AP system profile view before an AP goes online, the AC priority configured in the AP system profile view is delivered to the AP. If no AC priority is configured in the AP system profile view, the AC priority configured in the WLAN view is delivered to the AP.

Example

Set the AC priority to 3 in the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect priority 3
```

11.19.9 ac protect protect-ac

Function

The **ac protect protect-ac** command configures the standby AC IP address in the WLAN view.

The **undo ac protect protect-ac** command restores the default standby AC IP address in the WLAN view.

By default, no standby AC IP address is configured in the WLAN view.

Format

ac protect protect-ac *ip-address*

undo ac protect protect-ac

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address for the standby AC.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement dual-link backup on all the APs connected to an AC, configure the AC priority and standby AC IP address in the WLAN view to reduce the configuration workload.

Precautions

If standby AC IP addresses are configured in both the WLAN view and AP system profile view before an AP goes online, the standby AC IP address configured in the AP system profile view is delivered to an AP. If no standby AC IP address is configured in the AP system profile view, the standby AC IP address configured in the WLAN view is delivered to an AP. If no standby AC IP address is configured in the WLAN view, dual-link backup is disabled.

The standby AC's IP address must be set to the same as the CAPWAP source address of the standby AC.

Example

Set the standby AC IP address to 10.33.12.56 in the WLAN view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect protect-ac 10.33.12.56
```

11.19.10 ac protect restore disable

Function

The **ac protect restore disable** command disables global revertive switching.

The **undo ac protect restore disable** command enables global revertive switching.

By default, global revertive switching is enabled.

Format

ac protect restore disable

undo ac protect restore disable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AC1 is the active AC and AC2 is the standby AC. When the link between AC1 and an AP fails, AC2 takes the active role.

When the link between AC1 and the AP recovers, the AP detects that AC1 priority is higher than AC2 and instructs AC1 and AC2 to perform revertive switching. AC1 then becomes the active AC again.

Precautions

- The **undo wlan ac protect restore disable** command must be used before an AP goes online and dual-link backup is implemented. In this way, the AC delivers the revertive switching configuration to the AP when the AP goes online.
- If global revertive switching is disabled, traffic of an AP cannot be switched back to AC1 when the link between AC1 and the AP restores.
- The command takes effect after an AP restart.

Example

Disable global revertive switching.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ac protect restore disable
```

11.19.11 backup-access

Function

The **backup-access** command configures a backup AC IP address.

The **undo backup-access** command restores the default backup AC IP address.

By default, no backup AC IP address is configured.

Format

backup-access ip-address *ip-address*

undo backup-access

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address of the backup AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In AC backup scenarios, a backup AC IP address is configured so that APs can establish CAPWAP tunnels to the backup AC if they fail to establish CAPWAP tunnels to the primary AC.

Precautions

- The configurations of **primary-access** and **backup-access** take effect only if both the commands are run to configure different IP addresses.
- **primary-access** and **backup-access** cannot be configured with **priority** or **protect-ac**.
- It is not recommended that **primary-access** and **backup-access** be configured with **ac protect protect-ac** or **ac protect priority**.
- The configuration takes effect only after the AP is restarted.
- The IP addresses specified by **primary-access** and **backup-access** must be configured the same as CAPWAP source IP addresses. If the CAPWAP source addresses have been translated using NAT, set the **primary-access** and **backup-access** IP addresses to the translated addresses.

Example

Set the backup AC IP address to 10.33.12.78.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap-system-profile name sys1
[HUAWEI-wlan-ap-system-prof-sys1] backup-access ip-address 10.33.12.78
```

11.19.12 display ac protect

Function

The **display ac protect** command displays AC dual-link backup configuration.

Format

display ac protect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view AC dual-link backup configuration.

Example

Display AC dual-link backup configuration.

```
<HUAWEI> display ac protect
------------------------------------------------------------
Protect state             : disable
Protect AC                : -
Priority                  : 0
Protect restore           : enable
Coldbackup kickoff station: disable
Alarm restrain            : disable
------------------------------------------------------------
```

Table 11-313 Description of the **display ac protect** command output

Item	Description
Protect state	Whether global dual-link backup and N+1 backup are enabled. ● disable: Global dual-link backup is disabled, and N+1 backup is enabled. ● enable: Global dual-link backup is enabled, and N+1 backup is disabled. To configure the parameter, run the **ac protect enable** command.
Protect AC	Standby AC IP address. To configure the parameter, run the **ac protect protect-ac** command.
Priority	Priority of the local AC. To configure the parameter, run the **ac protect priority** command.
Protect restore	Whether global revertive switching is enabled on the AC. To configure the parameter, run the **ac protect restore disable** command.
Coldbackup kickoff station	Whether to enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured. To configure the parameter, run the **ac protect cold-backup kickoff-station** command.
Alarm restrain	Whether to enable AP fault alarm suppression. To configure the parameter, run the **ac protect alarm-restrain enable** command.

11.19.13 primary-access

Function

The **primary-access** command configures a primary AC IP address.

The **undo primary-access** command restores the default primary AC IP address.

By default, no primary AC IP address is configured.

Format

primary-access ip-address *ip-address*

undo primary-access

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address of the primary AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In AC backup scenarios, a primary AC IP address is configured. When APs attempt to go online, they preferentially associate with the primary AC and establish CAPWAP tunnels.

Precautions

- The configurations of **primary-access** and **backup-access** take effect only if both the commands are run to configure different IP addresses.
- **primary-access** and **backup-access** cannot be configured with **priority** or **protect-ac**.
- It is not recommended that **primary-access** and **backup-access** be configured with **ac protect protect-ac** or **ac protect priority**.
- The configuration takes effect only after the AP is restarted.
- The IP addresses specified by **primary-access** and **backup-access** must be configured the same as CAPWAP source IP addresses. If the CAPWAP source addresses have been translated using NAT, set the **primary-access** and **backup-access** IP addresses to the translated addresses.

Example

Set the primary AC IP address to 10.33.12.56.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name sys1
[HUAWEI-wlan-ap-system-prof-sys1] primary-access ip-address 10.33.12.56
```

11.19.14 priority

Function

The **priority** command sets the AC priority in the AP system profile view.

The **undo priority** command restores the AC priority to the default setting in the AP system profile view.

By default, no AC priority is configured in the AP system profile view.

Format

priority *priority-level*

undo priority

Parameters

Parameter	Description	Value
priority-level	Specifies the AC priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP goes online, ACs deliver their priorities to the AP. The AP selects the AC with the highest priority as the active AC and establishes a CAPWAP tunnel with the active AC.

Precautions

If the AC priority is configured in the WLAN view and AP system profile view before an AP goes online, the AC priority configured in the AP system profile view is delivered to the AP. If no AC priority is configured in the AP system profile view, the AC priority configured in the WLAN view is delivered to the AP.

If ACs deliver the same priorities to the AP, the AP selects the AC with the lowest AP load as the active AC. If both AC priorities and AP load are the same, the AP selects the AC with the lowest STA load as the active AC. If AC priorities, AP load, and STA load are the same, the AP selects the AC with the smallest IP address as the active AC to establish a CAPWAP tunnel. The AP or STA load equals the number of allowed APs or STAs minus the number of existing APs or STAs.

Example

Set the AC priority to 3 in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] priority 3
```

11.19.15 protect-ac

Function

The **protect-ac** command configures the standby AC's IP address in the AP system profile view.

The **undo protect-ac** command restores the standby AC's IP address to the default setting in the AP system profile view.

By default, no standby AC's IP address is configured in the AP system profile view.

Format

protect-ac ip-address *ip-address*

undo protect-ac

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address for the standby AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable an AP to establish connections with two ACs (active and standby ACs) to implement dual-link backup, you can run this command to configure the standby AC IP address in the AP system profile view.

Precautions

If standby AC's IP addresses are configured in both the WLAN view and AP system profile view, the standby AC's IP address configured in the AP system profile view is delivered to an AP. If no standby AC's IP address is configured in the AP system profile view, the standby AC's IP address configured in the WLAN view is delivered to an AP.

The IP address of the standby AC cannot be specified as the IP address of the local device. Otherwise, the backup function does not take effect.

The standby AC's IP address must be set to the same as the CAPWAP source address of the standby AC.

Example

Set the standby AC's IP address to 10.3.3.3 in the AP system profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1
[HUAWEI-wlan-ap-system-prof-ap-system1] protect-ac ip-address 10.3.3.3
```

11.20 WMI Commands

11.20.1 Command Support

WLAN-AC commands are supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

11.20.2 ap log module

Function

The **ap log module** command enables APs to report logs of the module with a specified ID to a WMI server.

The **undo ap log module mid** *mid* command disables APs from reporting logs of the module with a specified ID to a WMI server.

The **undo ap log module all** command disables APs from reporting logs of all modules to a WMI server.

By default, APs do not report logs of any module to a WMI server.

Format

ap log module mid *mid* [**name** *name*]

undo ap log module { **mid** *mid* | **all** }

Parameters

Parameter	Description	Value
mid *mid*	Specifies a module ID.	The value is in hexadecimal notation. Set the value to the ID of a module registered with the information center. **NOTE** You can enter **mid ?** to obtain the predefined ID of a module and the module name. You can run the **display info-center statistics** command on an AP to query more module IDs.
name *name*	Specifies a module name. The value must correspond to the value of **mid**.	The value is a string of 1 to 24 characters.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

If APs need to report logs to a WMI server, specify the ID of a module whose logs are to be reported and enable the log report function. Otherwise, the APs do not report logs of this module.

To enable APs to report logs of multiple modules, run this command repeatedly to specify multiple module IDs.

Example

Enable APs to report logs of the module **C1480000** to a WMI server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] ap log module mid c1480000
```

11.20.3 collect-item (WMI profile view)

Function

The **collect-item** command configures whether APs report collected data to a WMI server and specifies the data collection interval.

The **undo collect-item** command restores the default configuration for APs to report collected data to a WMI server and restores the default data collection interval.

Table 11-314 lists the default state of whether APs report data to the WMI server and the default data collection intervals. (The default values are recommended.)

Table 11-314 Default settings of the data reporting function and data collection interval

Data Type	Default State	Default Data Collection Interval (Unit: Second)
Site guest data	Enabled	300
CPCAR data	Enabled	300
Device monitoring data	Enabled	10
Enhanced Media Delivery Index (eMDI) data	Enabled	10
Interface monitoring data	Enabled	60
Wireless device location data	Disabled	60
Log data	Enabled	300
Radio data of neighboring wireless devices	Enabled	60
Radio monitoring data	Enabled	10
SSID monitoring data	Enabled	60
STA data	Enabled	10
AI roaming data	Enabled	300
DHCP option information about STAs	Disabled	300
User agent (UA) information in the HTTP packets sent by STAs.	Disabled	300
Service information in the mDNS packets sent by STAs	Disabled	300
DNS data	Disabled	60
Non-Wi-Fi device information	Disabled	60

Data Type	Default State	Default Data Collection Interval (Unit: Second)
iPCA 2.0 measurement information	Enabled	Real-time
LLDP neighbor data	Enabled	Real-time
Spectrum analysis data	Disabled	Real-time

Format

collect-item { **application-statistics-data** | **cpcar-data** | **device-data** | **emdi-data** | **interface-data** | **log-data** | **neighbor-device-data** | **radio-data** | **ssid-data** | **terminal-data** | **ai-roam-data** } { **interval** *interval* | **disable** }

undo collect-item { **application-statistics-data** | **cpcar-data** | **device-data** | **emdi-data** | **interface-data** | **log-data** | **neighbor-device-data** | **radio-data** | **ssid-data** | **terminal-data** | **ai-roam-data** }

collect-item { **location-data** | **terminal-dhcp-option-data** | **terminal-http-ua-data** | **terminal-mdns-data** | **dns-data** | **non-wifi-data** } { **interval** *interval* | **enable** }

undo collect-item { **location-data** | **terminal-dhcp-option-data** | **terminal-http-ua-data** | **terminal-mdns-data** | **dns-data** | **non-wifi-data** }

collect-item { **s-ipfpm-data** | **lldp-data** } **disable**

undo collect-item { **s-ipfpm-data** | **lldp-data** } **disable**

collect-item spectrum-data enable

undo collect-item spectrum-data enable

Parameters

Parameter	Description	Value
application-statistics-data	Indicates site guest data. This parameter is not supported by RUs.	-
cpcar-data	Indicates CPCAR data.	-
device-data	Indicates device monitoring data.	-
emdi-data	Indicates eMDI data. This parameter is not supported by Fit central APs or RUs.	-

Parameter	Description	Value
interface-data	Indicates interface monitoring data.	-
location-data	Indicates wireless device location data. This parameter is not supported by Fit central APs.	-
log-data	Indicates log data.	-
neighbor-device-data	Indicates radio data of neighboring wireless devices. This parameter is not supported by Fit central APs.	-
radio-data	Indicates radio monitoring data. This parameter is not supported by Fit central APs.	-
ssid-data	Indicates SSID monitoring data. This parameter is not supported by Fit central APs.	-
terminal-data	Indicates STA data. This parameter is not supported by Fit central APs.	-
ai-roam-data	Indicates AI roaming data.	-
terminal-dhcp-option-data	Indicates DHCP Option information (Options 12, 55, and 60) in the DHCP packets sent by STAs.	-
terminal-http-ua-data	Indicates UA information in the HTTP packets sent by STAs.	-
terminal-mdns-data	Indicates service information in the mDNS packets sent by STAs.	-
dns-data	Indicates DNS information. **NOTE** DNS information can be reported from APs only to iMaster NCE-CampusInsight.	-

Parameter	Description	Value
non-wifi-data	Indicates non-Wi-Fi device information.	-
s-ipfpm-data	Indicates iPCA 2.0 measurement information.	-
lldp-data	Indicates LLDP neighbor data. **NOTE** LLDP neighbor data of APs can be reported only to iMaster NCE-Campus.	-
spectrum-data	Indicates spectrum analysis data.	-
interval *interval*	Specifies the data collection interval.	The value is an integer, in seconds. The value range is as follows: ● **location-data**: 1 to 1800 ● Other data: 5 to 1800
disable	Disables APs from reporting collected data to the WMI server.	-
enable	Enables APs to report collected data to the WMI server.	-

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure APs to report collected data to the WMI server and set the data collection interval as required. You can run this command multiple times to configure APs to report different types of data to the WMI server.

Precautions

For APs that can only transparently report collected information, the collection interval is fixed at 5 minutes, and is unconfigurable.

Example

Set the interval for collecting device monitoring data to 500 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] collect-item device-data interval 500
```

11.20.4 collect-location-data enable

Function

The **collect-location-data enable** command enables the device to collect wireless device location data.

The **undo collect-location-data enable** command disables the device from collecting wireless device location data.

By default, the device does not collect wireless device location data.

Format

collect-location-data enable

undo collect-location-data enable

Parameters

None

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enable the device to collect and report wireless device location data to a WMI server for customer flow analysis.

Example

Enable the device to collect wireless device location data.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name default
[HUAWEI-wlan-location-prof-default] collect-location-data enable
```

11.20.5 collect-location-data rssi-threshold

Function

The **collect-location-data rssi-threshold** command configures the RSSI threshold for wireless device location data.

The default RSSI threshold for wireless device location data is -75 dBm.

Format

collect-location-data rssi-threshold *rssi-threshold*

Parameters

Parameter	Description	Value
rssi-threshold	Specifies an RSSI threshold.	The value is an integer that ranges from -95 to 0, in dBm.

Views

Location profile view

Default Level

2: Configuration level

Usage Guidelines

After the device is enabled to collect wireless device location data, only data with the RSSI of higher than the threshold is collected.

Example

Set the RSSI threshold for wireless device location data to -72 dBm.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] location-profile name default
[HUAWEI-wlan-location-prof-default] collect-location-data rssi-threshold -72
```

11.20.6 display references wmi-server

Function

The **display references wmi-server** command displays reference information about a WMI profile.

Format

display references wmi-server name *wmi-server-name*

Parameters

Parameter	Description	Value
name *wmi-server-name*	Displays reference information about a specified WMI profile.	The WMI profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wmi-server** command to view reference information about a WMI profile.

Example

Display reference information about the WMI profile **abc**.

```
<HUAWEI> display references wmi-server name abc
------------------------------------------------------------------------
Reference type              Reference name              Reference Index
------------------------------------------------------------------------
AP system profile           a                           1
------------------------------------------------------------------------
Total: 1
```

Table 11-315 Description of the **display references wmi-server name** *wmi-server-name* command output

Item	Description
Reference type	Type of the profile by which a WMI profile is referenced.
Reference name	Name of the profile by which a WMI profile is referenced.
Reference Index	Index for referencing a WMI profile to the AP system profile.

11.20.7 display wmi-server

Function

The **display wmi-server** command displays configuration and reference information about a WMI profile.

Format

display wmi-server { **all** | **name** *wmi-server-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WMI profiles.	-
name *wmi-server-name*	Displays information about a specified WMI profile.	The WMI profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration and reference information about a WMI profile.

Example

Display information about all WMI profiles.

```
<HUAWEI> display wmi-server all
----------------------------------------------------
Profile name                       Reference
----------------------------------------------------
abc                           0
----------------------------------------------------
Total: 1
```

Table 11-316 Description of the **display wmi-server all** command output

Item	Description
Profile name	Name of a WMI profile.
Reference	Number of times a WMI profile is referenced.

Display information about the WMI profile **abc**.

```
<HUAWEI> display wmi-server name abc
------------------------------------------------------------------------------
Server ip                          : 10.10.10.10
Server port                         : 10032
```

```
Server backup ip                      : 10.10.10.11
Server backup port                    : 10032
Report interval(s)                    : 60
Max packet-size(Kbyte)                : 5
Alive interval(min)                   : 3
Retry interval(min)                   : 5
Retry number                          : 0
Device enable                         : enable
Device data interval(s)               : 10
Ssid enable                           : enable
Ssid data interval(s)                 : 60
Radio enable                          : enable
Radio data interval(s)                : 10
Interface enable                      : enable
Interface data interval(s)            : 60
Terminal enable                       : enable
Terminal data interval(s)             : 10
Log enable                            : enable
Log data interval(s)                  : 300
Location enable                       : disable
Neighbor device enable                : enable
Neighbor device data interval(s)      : 60
CP-CAR enable                         : enable
CP-CAR data interval(s)               : 300
EMDI enable                           : enable
EMDI data interval(s)                 : 10
Application statistics enable         : enable
Application statistics data interval(s): 300
Terminal DHCP option enable           : enable
Terminal DHCP option data interval(s)  : 300
Terminal HTTP UA enable               : enable
Terminal HTTP UA data interval(s)     : 300
Terminal mDNS enable                  : enable
Terminal mDNS data interval(s)        : 300
DNS enable                            : enable
DNS data interval(s)                  : 50
Non WiFi data enable                  : enable
Non WiFi data interval(s)             : 60
Log module ID                         : C1480000
S-ipfpm enable                        : enable
AI roam data enable                   : enable
AI roam data interval(s)              : 300
Lldp enable                           : enable
PKI realm                             : default
Spectrum data enable                  : disable
------------------------------------------------------------------------------
```

Table 11-317 Description of the **display wmi-server name** command output

Item	Description
Server ip	IP address of the primary WMI server. To configure this parameter, run the **server ip-address** *ip-address* **port** *port* (WMI profile view) command.
Server port	Port number of the primary WMI server. To configure this parameter, run the **server ip-address** *ip-address* **port** *port* (WMI profile view) command.
Server backup ip	IP address of the backup WMI server. To configure this parameter, run the **server backup ip-address** *ip-address* **port** *port* (WMI profile view) command.

Item	Description
Server backup port	Port number of the backup WMI server. To configure this parameter, run the **server backup ip-address** *ip-address* **port** *port* (WMI profile view) command.
Report interval(s)	Data report interval. To configure this parameter, run the **report-interval** *interval* (WMI profile view) command.
Max packet-size(Kbyte)	Maximum size of reported data. To configure this parameter, run the **max-packet-size** *size* (WMI profile view) command.
Alive interval(min)	Interval at which the AP attempts to connect to the WMI server. To configure this parameter, run the **keepalive interval** *interval* (WMI profile view) command.
Retry interval(min)	Interval at which the AP attempts to reconnect to the WMI server. To configure this parameter, run the **keepalive retry-interval** *retry-interval* (WMI profile view) command.
Retry number	Number of attempts the AP reconnects to the WMI server. To configure this parameter, run the **keepalive retry-number** *retry-number* (WMI profile view) command.
Device enable	Whether device monitoring data collection is enabled. To configure this parameter, run the **collect-item device-data disable** command.
Device data interval(s)	Interval at which device monitoring data is collected. To configure this parameter, run the **collect-item device-data interval** *interval* command.
Ssid enable	Whether SSID monitoring data collection is enabled. To configure this parameter, run the **collect-item ssid-data disable** command.
Ssid data interval(s)	Interval at which SSID monitoring data is collected. To configure this parameter, run the **collect-item ssid-data interval** *interval* command.
Radio enable	Whether radio monitoring data collection is enabled. To configure this parameter, run the **collect-item radio-data disable** command.

Item	Description
Radio data interval(s)	Interval at which radio monitoring data is collected. To configure this parameter, run the **collect-item radio-data interval** *interval* command.
Interface enable	Whether interface monitoring data collection is enabled. To configure this parameter, run the **collect-item interface-data disable** command.
Interface data interval(s)	Interval at which interface monitoring data is collected. To configure this parameter, run the **collect-item interface-data interval** *interval* command.
Terminal enable	Whether STA data collection is enabled. To configure this parameter, run the **collect-item terminal-data disable** command.
Terminal data interval(s)	Interval at which STA data is collected. To configure this parameter, run the **collect-item terminal-data interval** *interval* command.
Log enable	Whether log data collection is enabled. To configure this parameter, run the **collect-item log-data disable** command.
Log data interval(s)	Interval at which log data is collected. To configure this parameter, run the **collect-item log-data interval** *interval* command.
Location enable	Whether wireless device location data collection is enabled. To configure this parameter, run the **collect-item location-data enable** command.
Location data interval(s)	Interval at which wireless device location data is collected. To configure this parameter, run the **collect-item location-data interval** *interval* command.
Neighbor device enable	Whether surrounding radio data collection is enabled. To configure this parameter, run the **collect-item neighbor-device-data disable** command.
Neighbor device data interval(s)	Interval at which surrounding radio data is collected. To configure this parameter, run the **collect-item neighbor-device-data interval** *interval* command.
CP-CAR enable	Whether CPCAR data collection is enabled. To configure this parameter, run the **collect-item cpcar-data disable** command.

Item	Description
CP-CAR data interval(s)	Interval at which CPCAR data is collected. To configure this parameter, run the **collect-item cpcar-data interval** *interval* command.
EMDI enable	Whether eMDI data collection is enabled. To configure this parameter, run the **collect-item emdi-data disable** command.
EMDI data interval(s)	Interval at which eMDI data is collected. To configure this parameter, run the **collect-item emdi-data interval** *interval* command.
Application statistics enable	Whether site guest data collection is enabled. To configure this parameter, run the **collect-item application-statistics-data disable** command.
Application statistics data interval(s)	Interval at which site guest data is collected. To configure this parameter, run the **collect-item application-statistics-data interval** *interval* command.
Terminal DHCP option enable	Whether collection of DHCP Option information (Options 12, 55, and 60) in the DHCP packets sent by STAs is enabled. To configure this parameter, run the **collect-item terminal-dhcp-option-data enable** command.
Terminal DHCP option data interval(s)	Interval at which DHCP Option information (Options 12, 55, and 60) in the DHCP packets sent by STAs is collected. To configure this parameter, run the **collect-item terminal-dhcp-option-data interval** *interval* command.
Terminal HTTP UA enable	Whether collection of UA information in the HTTP packets sent by STAs is enabled. To configure this parameter, run the **collect-item terminal-http-ua-data enable** command.
Terminal HTTP UA data interval(s)	Interval at which UA information in the HTTP packets sent by STAs is collected. To configure this parameter, run the **collect-item terminal-http-ua-data interval** *interval* command.
Terminal mDNS enable	Whether collection of service information in the mDNS packets sent by STAs is enabled. To configure this parameter, run the **collect-item terminal-mdns-data enable** command.

Item	Description
Terminal mDNS data interval(s)	Interval at which service information in the mDNS packets sent by STAs is collected. To configure this parameter, run the **collect-item terminal-mdns-data interval** *interval* command.
DNS enable	Whether DNS data collection is enabled. To configure this parameter, run the **collect-item dns-data enable** command.
DNS data interval(s)	Interval at which DNS data is collected. To configure this parameter, run the **collect-item dns-data interval** *interval* command.
Non WiFi data enable	Whether collection of non-Wi-Fi device data is enabled. To configure this parameter, run the **collect-item non-wifi-data enable** command.
Non WiFi data interval(s)	Interval at which non-Wi-Fi device data is collected. To configure this parameter, run the **collect-item non-wifi-data interval** *interval* command.
Log module ID	ID of the module whose logs are to be reported. To configure this parameter, run the **ap log module mid** *mid* [**name** *name*] command.
S-ipfpm enable	Whether iPCA 2.0 measurement information collection is enabled. To configure this parameter, run the **collect-item s-ipfpm-data disable** command.
AI roam data enable	Whether AI roaming data collection is enabled. To configure this parameter, run the **collect-item ai-roam-data disable** command.
AI roam data interval(s)	Interval at which AI roaming data is collected. To configure this parameter, run the **collect-item ai-roam-data interval** *interval* command.
Lldp enable	Whether LLDP neighbor data collection is enabled. To configure this parameter, run the **collect-item lldp-data disable** command.
PKI realm	PKI realm used for interconnection with a WMI server. To configure this parameter, run the **pki realm** *realm-name* command.
Spectrum data enable	Whether spectrum analysis data collection is enabled. To configure this parameter, run the **collect-item spectrum-data enable** command.

11.20.8 keepalive (WMI profile view)

Function

The **keepalive** command configures connection parameters between APs and the WMI server.

The **undo keepalive** command restores the default settings of connection parameters between APs and the WMI server.

By default, the heartbeat interval is 3 minutes, the reconnection interval is 5 minutes, and the number of reconnection attempts is 0.

Format

keepalive { **interval** *interval* | **retry-interval** *retry-interval* | **retry-number** *retry-number* } *

undo keepalive

Parameters

Parameter	Description	Value
interval *interval*	Specifies the heartbeat interval.	The value is an integer that ranges from 1 to 60, in minutes.
retry-interval *retry-interval*	Specifies the reconnection interval after an AP is disconnected from the server.	The value is an integer that ranges from 5 to 60, in minutes.
retry-number *retry-number*	Specifies the number of reconnection attempts.	The value is an integer that ranges from 0 to 4294967295. The value 0 indicates that the server and APs always attempt to reconnect to each other.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of reconnection attempts to 5.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] keepalive retry-number 5
```

11.20.9 max-packet-size (WMI profile view)

Function

The **max-packet-size** command configures the maximum data length of KPI information sent by APs to a WMI server.

The **undo max-packet-size** command restores the default maximum data length of KPI information sent by APs to a WMI server.

By default, the maximum data length of KPI information sent by APs to a WMI server is 5 KB.

Format

max-packet-size *size*

undo max-packet-size

Parameters

Parameter	Description	Value
size	Specifies the maximum data length of reported information.	The value is an integer that ranges from 4 to 256, in KB.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Based on the network status, you can run the **max-packet-size** command to configure the maximum data length of KPI information sent by APs to a WMI server.

Example

Set the maximum data length of KPI information sent by APs to a WMI server to 6 KB.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] max-packet-size 6
```

11.20.10 mdns-snooping enable

Function

The **mdns-snooping enable** command enables the mDNS snooping function.

The **undo mdns-snooping enable** command disables the mDNS snooping function.

By default, mDNS snooping is disabled.

Format

mdns-snooping enable

undo mdns-snooping enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

In terminal type identification scenarios, you can enable mDNS snooping on a VAP. In this manner, the device can collect information from mDNS packets sent by terminals connected to the VAP and report the collected information to a WMI server for terminal type identification.

Example

Enable mDNS snooping.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name abc
[HUAWEI-wlan-vap-prof-abc] mdns-snooping enable
```

11.20.11 pki realm (WMI profile view)

Function

The **pki realm** command configures a PKI realm for interconnection between APs and a WMI server.

The **undo pki realm** command restores the default PKI realm for interconnection between APs and a WMI server.

By default, the PKI realm for interconnection between APs and a WMI server is **default**.

Format

pki realm *realm-name*

undo pki realm

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The PKI realm name must exist.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure a PKI realm for interconnection between APs and a WMI server.

Example

Configure the PKI realm **test** for interconnection between APs and a WMI server.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wmi-server] pki realm test
```

11.20.12 report-interval (WMI profile view)

Function

The **report-interval** command sets the interval for APs to report KPI information to a WMI server.

The **undo report-interval** command restores the default interval for APs to report KPI information to a WMI server.

By default, APs report KPI information to a WMI server at an interval of 60 seconds.

Format

report-interval *interval*

undo report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for APs to report KPI information to a WMI server.	The value is an integer that ranges from 10 to 300, in seconds.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

You can configure the interval for APs to report KPI information to a WMI server based on the device usage, network resource usage, and the server's requirements for real-time information collection. A shorter interval indicates that data is more frequently data, which occupies more device and network resources. A long interval cannot ensure real-time information on the server.

Example

Set the interval for APs to report KPI information to a WMI server to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] report-interval 30
```

11.20.13 server (WMI profile view)

Function

The **server** command configures the destination address and port number of the primary WMI server to which APs report KPI information.

The **undo server** command restores the default destination address and port number of the primary WMI server to which APs report KPI information.

By default, the destination address and port number of the primary WMI server to which APs report KPI information are not configured.

Format

server ip-address *ip-address* **port** *port*

undo server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address of the server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of the server.	The value is an integer that ranges from 1 to 65535. - Use port 10032 to report data to iMaster NCE-Campus. - Use port 27371 to report data to iMaster NCE-CampusInsight.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure a correct IP address and port number of a WMI server, APs can correctly report KPI information to the specified server.

NOTE

DNS information can be reported from APs only to iMaster NCE-CampusInsight.

Precautions

When the primary/backup WMI server scheme is used, run the **server backup ip-address** *ip-address* **port** *port* (WMI profile view) command to configure the destination address and port number of the backup WMI server after configuring the primary WMI server. If the primary/backup WMI server scheme is not used, you only need to configure the destination address and port number of the primary WMI server. Do not configure the backup server before configuring the primary server.

If the backup WMI server has been configured and you run the **undo server** command to restore the primary WMI server to the default value, the backup WMI server is also restored to the default value.

Example

Configure the destination IP address and port number for APs to report KPI information.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] server ip-address 10.10.11.11 port 10032
```

11.20.14 server backup (WMI profile view)

Function

The **server backup** command configures the destination IP address and port number of the backup WMI server to which APs report KPI information.

The **undo server backup** command restores the default destination IP address and port number of the backup WMI server to which APs report KPI information.

By default, the destination IP address and port number of the backup WMI server to which APs report KPI information are not configured.

Format

server backup ip-address *ip-address* **port** *port*

undo server backup ip-address

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address of the server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of the server.	The value is an integer that ranges from 1 to 65535. ● Use port 10032 to report data to iMaster NCE-Campus. ● Use port 27371 to report data to iMaster NCE-CampusInsight.

Views

WMI profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the primary/backup WMI server scheme is used, you can run this command to configure the destination IP address and port number of the backup WMI server so that the APs can report KPI information to the specified backup WMI server.

After the primary/backup scheme is configured, if an AP fails to connect to the primary WMI server, the AP attempts to connect to the backup WMI server. If the connection still fails, the AP attempts to reconnect to the primary and backup WMI servers until the connection is successful.

NOTE

DNS information can be reported from APs only to iMaster NCE-CampusInsight.

Precautions

The destination IP address and port number of the primary WMI server have been configured using the **server ip-address** *ip-address* **port** *port* (WMI profile view) command.

Example

Configure the destination IP address and port number of the backup WMI server to which APs report KPI information.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc] server ip-address 10.10.11.11 port 10032
[HUAWEI-wlan-wmi-server-prof-abc] server backup ip-address 10.10.11.12 port 10032
```

11.20.15 wmi-server (AP system profile view)

Function

The **wmi-server** command binds a WMI profile to the AP system profile.

The **undo wmi-server** command unbinds a WMI profile from the AP system profile.

By default, no WMI profile is bound to an AP system profile.

Format

wmi-server *profile-name* **index** *index*

undo wmi-server index *index*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WMI profile.	The WMI profile name must exist.

Parameter	Description	Value
index *index*	Specifies an index.	The value is an integer that can be 1 or 2. **NOTE** To report KPI information to iMaster NCE-Campus, specify index 1. To report KPI information to iMaster NCE-CampusInsight, specify index 2.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

A WMI profile can take effect only after being bound to an AP system profile.

NOTE

Do not bind two WMI profiles with the same destination address and port number to avoid waste of destination server resources.

Example

Bind WMI profile **abc** to the AP system view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys
[HUAWEI-wlan-ap-system-prof-apsys] wmi-server abc index 1
```

11.20.16 wmi-server (WLAN view)

Function

The **wmi-server** command creates a WMI profile and displays the WMI profile view.

The **undo wmi-server** command deletes a WMI profile.

By default, no WMI profile is created.

Format

wmi-server name *profile-name*

undo wmi-server { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WMI profile.	The value is a string of 1 to 35 case-insensitive characters, without spaces or quotation marks (?). It cannot start or end with double quotation masks (").
all	Specifies all WMI profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can set parameters for APs to report KPI information to the WMI server in the WMI profile.

Example

Create a WMI profile **abc** and display the WMI profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] wmi-server name abc
[HUAWEI-wlan-wmi-server-prof-abc]
```

11.21 Configuration Commands for the Zero-Roaming Distributed Wi-Fi Solution

11.21.1 display ap oru status

Function

The **display ap oru status** command displays the status of ORUs and AUs connected to DAPs.

NOTE

ORU management is supported only by the DAP AirEngine 9700D-S.

Format

display ap oru status { **all** | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays the status of ORUs and AUs connected to all DAPs.	-
ap-id *ap-id*	Displays the status of ORUs and AUs connected to a specified DAP.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to query the IDs, status, and versions of ORUs and AUs connected to a specified DAP or all DAPs.

Example

Display the status of ORUs and AUs connected to all DAPs.

```
<HUAWEI> display ap oru status all
Y: Normal N: Absent A: Abnormal U: Upgrading D: Disabled -: Unknown
ORUx: ORUx status(AU0 status/AU1 status/AU2 status/AU3 status/AU4 status/AU5 status/AU6 status/AU7
status)
-----------------------------------------------------------------------------------------------------------------------------
-----------------------------------
AP ID   ORU0              ORU1              ORU2              ORU3              ORU4              ORU5
ORU6              ORU7
-----------------------------------------------------------------------------------------------------------------------------
-----------------------------------
5       N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) Y(Y/Y/N/N/N/N/N/N)
N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N) N(N/N/N/N/N/N/N/N)
-----------------------------------------------------------------------------------------------------------------------------
-----------------------------------
```

Table 11-318 Description of the **display ap oru status all** command output

Item	Description
AP ID	AP ID.

Item	Description
ORUx	Status of ORU*x* and its connected AUs. The possible status of an ORU includes: ● Y: Normal ● N: Absent ● A: Abnormal ● U: Upgrading ● D: Disabled ● -: Unknown The possible status of an AU includes: ● Y: Normal ● N: Absent ● -: Unknown

Display the status of ORUs and AUs connected to the DAP with the ID of 1.

```
<HUAWEI> display ap oru status ap-id 1
Y: Normal N: Absent -: Unknown
------------------------------------------------------------------------------------------
ORU  SN        Status    AU status           Temperature(degree C)  Version
------------------------------------------------------------------------------------------
0    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
1    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
2    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
3    XXX       Normal     Y/Y/N/N/N/N/N/N       35                 7
4    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
5    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
6    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
7    XXX       Absent    N/N/N/N/N/N/N/N        -                 0
------------------------------------------------------------------------------------------
Total: 8
```

Table 11-319 Description of the **display ap oru status ap-id** command output

Item	Description
ORU	ORU ID.
SN	ORU SN.
Status	ORU status.
AU status	AU status.
Temperature(degree C)	ORU temperature. When the ORU state is **Absent** or **Disabled**, the temperature is displayed as a hyphen (-).
Version	Version number of the ORU.

11.21.2 distribute-mode enable

Function

The **distribute-mode enable** command enables the DAP network collaboration function.

The **undo distribute-mode enable** command restores the default state of the DAP network collaboration function.

By default, the DAP network collaboration function is disabled.

NOTE

Network collaboration functions (including intranet and extranet collaboration, and DAP backup) are supported only by the AirEngine 6761-21E with external antennas.

Format

distribute-mode enable

undo distribute-mode enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

This command is used to enable the DAP network coordination function. After an extranet AP or backup AP is connected to a DAP, you can run this command to enable the distributed AP network collaboration function. In this way, the extranet AP or backup AP can share the ORUs and AUs connected to the DAP, thereby achieving the backup solution or the integrated deployment of the intranet and extranet within the same coverage area.

Precautions

When configuring a backup solution, you also need to run the **type service-backup distribute** command to set the VAP type of the backup AP to distributed-AP backup service.

Example

Enable the DAP network collaboration function.

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] ap-system-profile name system1
[HUAWEI-wlan-ap-system-prof-system1] distribute-mode enable
```

11.21.3 oru reboot

Function

The **oru reboot** command restarts ORUs.

NOTE

ORU management is supported only by the DAP AirEngine 9700D-S.

Format

oru reboot ap-id *ap-id* [**oru-id** *oru-id*]

Parameters

Parameter	Description	Value
ap-id *ap-id*	Restarts the ORUs connected to a DAP with a specified ID.	The AP ID must exist.
oru-id *oru-id*	Restarts the ORU with a specified ID. If this parameter is not specified, all ORUs connected to the specified DAP are restarted.	The value is an integer that ranges from 0 to 7.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When maintaining ORUs, you can run this command to restart ORUs as required.

Example

Restart the ORU connected to the DAP with the ID of 1.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] oru reboot ap-id 1
```

11.21.4 fastpass users

Function

The **fastpass users** command configures the FastPass function for VIP users on a DAP.

The **undo fastpass** command restores the default status of the FastPass function for VIP users on a DAP.

By default, the FastPass function for VIP users is enabled on the 2.4 GHz radio, the number of FastPass users is 5, the FastPass scheduling period is 20 ms, and the percentage of FastPass users in the scheduling period is 25%.

NOTE

The VIP FastPass function is supported only by the DAP AirEngine 9700D-S.

The FastPass function for VIP users applies only to the 2.4 GHz frequency band, and does not take effect after the configuration is delivered in the 5G radio profile view.

Format

fastpass users *value* [**period** *period-value* **ratio** *ratio-value*]

undo fastpass

Parameters

Parameter	Description	Value
value	Specifies the number of FastPass users.	The value is an integer that ranges from 0 to 10. When this parameter is set to 0, this function is disabled. The default value is 5.
period *period-value*	Specifies the FastPass scheduling period.	The value is of enumerated type, which can be 20, 40, 60, 80, or 100, in milliseconds. The default value is 20.
ratio *ratio-value*	Specifies the percentage of FastPass users in the scheduling period.	The value is an integer that ranges from 5 to 75, in percentage. The default value is 25.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

In a zero-roaming distributed scenario, when the 2.4 GHz frequency band experiences severe interference and the channel utilization exceeds 60%, you can configure the FastPass function for VIP users to prevent packet loss and frame freezing, thereby preferentially ensuring user experience of important intranet services.

When the number of FastPass users specified by the parameter *value* is set to 0, this function is disabled.

When the channel utilization exceeds 60%, you are advised to set the number of FastPass users to 10, the FastPass scheduling period to 60 ms, and the percentage of FastPass users to 75%.

Example

Set the number of FastPass users to 10, the FastPass scheduling period to 60 ms, and the percentage of FastPass users in the scheduling period to 75%.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] radio-2g-profile name default
[HUAWEI-wlan-radio-2g-prof-default] fastpass users 10 period 60 ratio 75
```

12 Reliability Commands

12.1 BFD Configuration Commands

12.1.1 Command Support

Only the following switch models support BFD:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

12.1.2 authentication-mode (BFD)

Function

The **authentication-mode** command configures BFD session authentication information.

The **undo authentication-mode** command deletes the configured BFD session authentication information.

By default, BFD session authentication information is not configured.

Format

authentication-mode met-sha1 key-id *key-id-value* **cipher** *cipher-text* **nego-packet** [**timeout-interval** *interval-value*]

undo authentication-mode

Parameters

Parameter	Description	Value
met-sha1	Specifies MSHA1 to decrypt and authenticate.	-
key-id *key-id-value*	Specifies the authentication key ID of a BFD session.	The value is an integer that ranges from 1 to 255.
cipher *cipher-text*	Specifies a ciphertext BFD authentication password. You can enter either a simple or ciphertext password, but the password is displayed in ciphertext in the configuration file.	The value is a string of characters. ● The value is a string of 1 to 20 characters for simple authentication passwords. ● The value is a string of 20 to 148 characters for ciphertext authentication passwords. **NOTE** The characters exclude question marks (?) and spaces. However, if a password string is between a pair of quotation marks, the string can contain spaces.
nego-packet	Authenticates BFD negotiation packets.	-
timeout-interval *interval-value*	Specifies the negotiation timeout period of a BFD session.	The value is an integer ranging from 1 to 10000, in seconds. This parameter has no default value. **NOTE** After a BFD negotiation timeout period is configured, the BFD negotiation timeout timer is started when the BFD session goes Down (the event is not triggered by a link fault detected). If the timer has expired but the BFD session is still Down, the link protocol of the associated interface goes Down.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding higher security, run the **authentication-mode** command to configure BFD session authentication information to improve network security. In a specific access scenario, for example, when a multicast BFD session is associated with the protocol status of an interface, you need to configure authentication information for the BFD session on the interface. BFD negotiation can succeed, the BFD-associated protocol status of the interface can be activated, and users can access the device through this interface only when the BFD session authentication information on both ends is consistent.

Prerequisites

BFD has been globally enabled using the **bfd** command in the system view.

A BFD session used to detect the physical link status has been created using the **bfd bind peer-ip default-ip** command in the system view.

Precautions

If you run the **authentication-mode** command to configure BFD session authentication information, BFD renegotiation will be performed. BFD renegotiation can succeed only when the BFD session authentication information on both ends is consistent.

Adding, modifying, or deleting BFD session authentication information may interrupt the service associated with the BFD session.

Example

Configure multicast BFD session authentication information.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface GigabitEthernet0/0/1
[HUAWEI-bfd-session-test] authentication-mode met-sha1 key-id 5 cipher YsHsjx_202206 nego-packet
timeout-interval 5
```

12.1.3 bfd

Function

The **bfd** command enables the global Bidirectional Forwarding Detection (BFD) function and displays the BFD view.

The **undo bfd** command disables global BFD.

By default, global BFD is disabled.

Format

bfd

undo bfd

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect link faults, run the **bfd** command in the system view to enable global BFD.

Precautions

BFD must be enabled globally before BFD parameters are configured.

NOTICE

Running the **undo bfd** command in the system view may affect services associated with BFD and deletes all BFD sessions on the device. To restore the BFD function, you have to re-configure BFD sessions.

Example

Enable the global BFD function.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd]
```

12.1.4 bfd bind peer-ip

Function

The **bfd bind peer-ip** command creates a BFD session, specifies the peer IP address, and displays the BFD session view.

The **undo bfd** *session-name* command deletes a specified BFD session and cancels the peer IP address.

By default, BFD binding is not created.

Format

bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] [**source-ip** *ip-address*]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	-
vpn-instance *vpn-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the type and number of the interface bound to the BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. ● During BFD session negotiation, if the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address is reachable. The IP address of this outbound interface is used as the source IP address of the BFD packets sent by the local end. ● When a BFD session is detecting links, if this parameter is not specified, the system uses a fixed source IP address in BFD packets. When BFD is used with the Unicast Reverse Path Forwarding (URPF) function, you must manually configure the source IP address in BFD packets because the URPF function checks the source IP address in received packets. **NOTE** For details about URPF, see URPF Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Security*.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect and monitor links, create BFD sessions.

To create a BFD binding, pay attention to the following points:

- If only the peer IP address is specified, BFD is configured to detect the multi-hop link.
- If the peer IP address and local interface are specified, BFD is configured to detect the single-hop link, that is, a specific route with this interface as the outbound interface and with the peer IP address as the next-hop address.
- If both the peer IP address and the VPN instance are specified, BFD is configured to detect the multi-hop link in the VPN instance.
- The single-hop link in the VPN instance is detected if both the peer IP address, VPN instance, and local interface are specified.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Follow-up Procedure

- Run the **discriminator** command to set the local and remote discriminators for the current BFD session.

Precautions

- When creating a single-hop BFD session, bind the single-hop BFD session to the peer IP address and the local address. You only need to bind a multi-hop BFD session to the peer IP address.
- When the BFD configuration items are created, the system checks only the format of the IP address. The BFD session cannot be established if an incorrect peer IP address or source IP address is bound.
- When a multi-hop BFD session is configured, the value of **peer-ip** or **source-ip** cannot be the IP address of a GRE tunnel interface.
- When a multi-hop BFD session is configured and the peer IP address is the same as the 32-bit destination IP address of an LDP or static LSP, the BFD session is associated with the LSP. That is, if the BFD session detects a fault, an LSP switchover is performed.

Example

Create a BFD session named **atob** to detect the single-hop link from VLANIF100 to the peer IP address at 10.10.10.2.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip 10.10.10.2 interface vlanif 100
```

Create a BFD session named **atoc** to detect the multi-hop link to the peer IP address 10.10.20.2.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atoc bind peer-ip 10.10.20.2
```

12.1.5 bfd bind peer-ip default-ip

Function

The **bfd bind peer-ip default-ip** command creates a BFD binding for detecting the physical status of a link.

The **undo bfd** *session-name* command deletes a specified BFD session and the created BFD binding.

By default, no BFD binding for monitoring physical status of a link is configured.

Format

bfd *session-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *ip-address*] [**auto**]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the session name of BFD.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip default-ip	Indicates the default multicast IP address that is bound to a BFD session.	By default, BFD uses the multicast IP address 224.0.0.184. You can set the multicast IP address by running the **default-ip-address** command.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. If the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address can be reached. The IP address of this outbound interface is used as the source IP address of BFD packets sent by the local end. Generally, this parameter is not required. When BFD is used with the Unicast Reverse Path Forwarding (URPF) function, you must manually configure the source IP address in BFD packets because the URPF function checks the source IP address in received packets. **NOTE** For details about URPF, see URPF Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Security*.	-
auto	Enables automatic negotiation of local and remote discriminators.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If **source-ip** is specified, the URPF-enabled device does not incorrectly discard BFD packets. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.

Precautions

When the **bfd bind peer-ip default-ip** command is used to configure a BFD session, ring protocols cannot be configured on the interface bound to the BFD session. Otherwise, MAC address flapping may occur.

If the IP address of an outbound interface is changed after a BFD session is configured, the source IP address of BFD packets is not updated.

NOTE

If automatic negotiation of local and remote discriminators is not configured, run the **commit** command to commit the configuration to make the configuration take effect.

Unlike common static BFD sessions, static BFD sessions with automatically negotiated discriminators have separate characteristics:

- The **bfd bind peer-ip source-ip auto** command can be run and immediately create a static BFD session with automatically negotiated discriminators, without the **commit** command executed.
- Parameters of a static BFD session with automatically negotiated discriminators take effect immediately after being modified, without the **commit** command executed. The parameters include the minimum interval at which BFD packets are sent and received and the detection multiplier.
- The **commit** command can be run for a static BFD session with automatically negotiated discriminators to support the forward version compatibility.

Example

Create a BFD session named **test**, and then detect the one-hop link that is bound to the local interface GigabitEthernet0/0/1 through the default multicast IP address.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-test]
```

12.1.6 bfd bind peer-ip source-ip auto

Function

The **bfd bind peer-ip source-ip auto** command creates a static BFD session with automatically negotiated discriminators.

The **undo bfd** *session-name* command deletes a specified BFD session.

By default, no static BFD session with automatically negotiated discriminators is established.

Format

bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] **source-ip** *ip-address* **auto**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	-
vpn-instance *vpn-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value must be an existing VPN instance name.
interface-type interface-number	Specifies the type and number of the interface bound to the BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets, that is, IP address of the outbound interface.	-
auto	Enables automatic negotiation of local and remote discriminators.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local device where a BFD session with automatically negotiated parameters is configured can negotiate with the remote device where a dynamic BFD session is configured; however, the local device enabled with static BFD can establish a BFD session with the remote device enabled with static BFD only. When configuring a BFD session with automatically negotiated parameters or a static BFD session, you can specify the BFD session name. The name of a dynamic BFD session is generated dynamically. When the network changes, the name of the dynamic BFD session may change.

When the remote end is configured with dynamic BFD and the local end needs to be configured with association between BFD and static route (BFD session name needs to be specified during association configuration), a BFD session with automatically negotiated parameters can be configured on the local end. Then the local end can establish a BFD session with the remote end enabled with dynamic BFD and association between BFD and static route can be implemented.

When creating a static BFD session with automatically negotiated discriminators, pay attention to the following points:

- If only the peer IP address is specified, BFD is configured to detect the multi-hop link.
- If the peer IP address and local interface are specified, BFD is configured to detect the single-hop link, that is, a specific route with this interface as the outbound interface and with the peer IP address as the next-hop address.
- Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.

- If both the peer IP address and the VPN instance are specified, BFD is configured to detect the multi-hop link in the VPN instance.
- If the peer IP address, VPN instance, and local interface are specified, BFD is configured to detect the single-hop link in the VPN instance.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Precautions

- When creating a BFD session, bind the BFD session to the peer IP address and the local address.
- When the BFD configuration items are created, the system checks only the format of the IP address. The BFD session cannot be established if an incorrect peer IP address or source IP address is bound.

NOTE

Unlike common static BFD sessions, static BFD sessions with automatically negotiated discriminators have separate characteristics:

- The **bfd bind peer-ip source-ip auto** command can be run and immediately create a static BFD session with automatically negotiated discriminators, without the **commit** command executed.
- Parameters of a static BFD session with automatically negotiated discriminators take effect immediately after being modified, without the **commit** command executed. The parameters include the minimum interval at which BFD packets are sent and received and the detection multiplier.
- The **commit** command can be run for a static BFD session with automatically negotiated discriminators to support the forward version compatibility.

Example

Create a static BFD session with automatically negotiated discriminators.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip 10.1.1.2 interface vlanif 100 source-ip 10.1.1.1 auto
```

12.1.7 bfd bind peer-ipv6

Function

The **bfd bind peer-ipv6** command creates a BFD6 session to detect IPv6 links.

The **undo bfd** *bfd-name* command deletes a specified BFD6 session.

By default, no BFD6 session is created for IPv6 links.

Format

bfd *session-name* **bind peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD6 session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ipv6 *ipv6-address*	Specifies the peer IPv6 address bound to a BFD6 session.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance bound to a BFD6 session.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the local Layer 3 outbound interface bound to a BFD6 session. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets. Generally, you do not need to set this parameter. If you do not specify the source IP address, the system automatically sets the source IP address according to the following rules: ● During BFD for IPv6 session negotiation, if the source IPv6 address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address is reachable. The IPv6 address of this outbound interface is used as the source IP address of the BFD packets sent by the local end. ● If this parameter is not specified when a BFD for IPv6 session is detecting links, the system uses a fixed source IPv6 address in BFD packets. **NOTE** When BFD is used with Unicast Reverse Path Forwarding (URPF), you must manually configure the source IPv6 address in BFD packets because URPF checks the source IPv6 address in received packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect and monitor IPv6 links, you can create BFD for IPv6 sessions.

When creating a BFD for IPv6 binding, pay attention to the following points:

- If only the peer IPv6 address is specified, BFD is configured to detect the multi-hop link.
- A single-hop link is detected if both the peer IPv6 address and the local interface are specified. That is, a BFD6 session detects a specific route with this interface as the outbound interface and with the peer IPv6 address as the next hop address.
- If both the peer IPv6 address and the VPN instance are specified, the created BFD6 session detects the multi-hop links in the VPN instance.

- The single-hop links in a VPN instance are detected if both the peer IPv6 address, VPN instance, and local interface are specified.

NOTE

The **source-ipv6** parameter prevents BFD packets from being discarded incorrectly by URPF. The system checks only the source IPv6 address type (it cannot be a multicast or broadcast address), but does not check the address correctness. Therefore, you must manually check the correctness of the source IPv6 address.

When a multi-hop BFD6 session is configured, the value of **peer-ipv6** or **source-ipv6** cannot be the IPv6 address of a GRE tunnel interface.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Follow-up Procedure

After creating a BFD for IPv6 session and entering its view, perform the following mandatory operations:

1. Run the **discriminator** command to set the local and remote discriminators for the BFD for IPv6 session.
2. Run the **commit** command to commit the configuration.

Perform the following optional operations according to your needs:

- Run the **description** command to configure description for the BFD for IPv6 session.
- Run the **min-tx-interval** command to set the interval for sending BFD for IPv6 packets.
- Run the **min-rx-interval** command to set the interval for receiving BFD for IPv6 packets.
- Run the **detect-multiplier** command to set the local detection multiplier.
- Run the **process-pst** command to configure the Port State Table (PST) of the BFD session.
- Run the **wtr** command to set the Wait-to-Recovery (WTR) time for the BFD for IPv6 session.

Precaution

- The BFD for IPv6 session detects links bidirectionally, so the **bfd bind peer-ipv6** command must be run on both ends of each link.
- After a BFD for IPv6 session is created:
  - If you change the source IPv6 address of outbound interface during session negotiation, the source IPv6 address in BFD packets is also changed.
  - If you change the source IPv6 address of outbound interface during session detection, the source IPv6 address in BFD packets is not changed.

Example

Create a BFD6 session named **atob** to detect a single-hop link.

```
<HUAWEI> system-view
[HUAWEI] bfd
```

```
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ipv6 2001:db8:1::1 interface vlanif 10
[HUAWEI-bfd-session-atob] discriminator local 1
[HUAWEI-bfd-session-atob] discriminator remote 2
[HUAWEI-bfd-session-atob] commit
```

Create a BFD6 session named **atoc** to detect a multi-hop link from which BFD6 packets reach 2001:db8:1::1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atoc bind peer-ipv6 2001:db8:1::1
[HUAWEI-bfd-session-atoc] discriminator local 3
[HUAWEI-bfd-session-atoc] discriminator remote 4
[HUAWEI-bfd-session-atoc] commit
```

12.1.8 bfd bind peer-ipv6 source-ipv6 auto

Function

The **bfd bind peer-ipv6 source-ipv6 auto** command creates a static BFD6 session with automatically negotiated discriminators.

The **undo bfd** *bfd-name* command deletes a specified BFD6 session.

By default, no static BFD6 session with automatically negotiated discriminators.

Format

bfd *session-name* **bind peer-ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] **source-ipv6** *ipv6-address* **auto**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD6 session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ipv6 *ipv6-address*	Specifies the peer IPv6 address bound to a BFD6 session.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance bound to a BFD6 session.	The value must be an existing VPN instance name.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the local Layer 3 outbound interface bound to a BFD6 session. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local device where a BFD session with automatically negotiated parameters is configured can negotiate with the remote device where a dynamic BFD session is configured; however, the local device enabled with static BFD can establish a BFD session with the remote device enabled with static BFD only. When configuring a BFD session with automatically negotiated parameters or a static BFD session, you can specify the BFD session name. The name of a dynamic BFD session is generated dynamically. When the network changes, the name of the dynamic BFD session may change.

When the remote end is configured with dynamic BFD and the local end needs to be configured with association between BFD and static route (BFD session name needs to be specified during association configuration), a BFD session with automatically negotiated parameters can be configured on the local end. Then the local end can establish a BFD session with the remote end enabled with dynamic BFD and association between BFD and static route can be implemented.

When creating a static BFD for IPv6 session with automatically negotiated discriminators, pay attention to the following points:

- If only the peer IPv6 address is specified, BFD is configured to detect the multi-hop link.
- A single-hop link is detected if both the peer IPv6 address and the local interface are specified. That is, a BFD6 session detects a specific route with this interface as the outbound interface and with the peer IPv6 address as the next hop address.
- If both the peer IPv6 address and the VPN instance are specified, the created BFD6 session detects the multi-hop links in the VPN instance.

- If the peer IPv6 address, VPN instance, and local interface are specified, the created BFD6 session detects the single-hop links in the VPN instance.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Follow-up Procedure

After creating a static BFD for IPv6 session with automatically negotiated discriminators and entering its view, perform the following mandatory operations:

- Run the **description** command to configure description for the BFD for IPv6 session.
- Run the **min-tx-interval** command to set the interval for sending BFD packets.
- Run the **min-rx-interval** command to set the interval for receiving BFD packets.
- Run the **detect-multiplier** command to set the local detection multiplier.
- Run the **process-pst** command to configure the Port State Table (PST) of the BFD session.
- Run the **wtr** command to set the Wait-to-Recovery (WTR) time for the BFD for IPv6 session.

Precaution

A static BFD for IPv6 session and a static BFD6 session with automatically negotiated discriminators have the following differences:

- The local and remote discriminators must be specified for a static BFD for IPv6 session.
- The local and remote discriminators are optional for a static BFD6 session with automatically negotiated discriminators.

If the IPv6 address of outbound interface is changed for a BFD for IPv6 session, the source IPv6 address in BFD packets is not changed.

The source address is mandatory for a static BFD6 session with automatically negotiated discriminators.

Example

Create a static BFD6 session named **atob** with the automatically negotiated discriminators to detect a single-hop link.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ipv6 2001:db8:1::1 interface gigabitethernet 0/0/1 source-ipv6
2001:db8:1::1 auto
[HUAWEI-bfd-session-atob]
```

Create a static BFD6 session named **atoc** with the automatically negotiated discriminators to detect the multi-hop link from which BFD6 packets reach 2001:db8:1::1.

```
<HUAWEI> system-view
[HUAWEI] bfd
```

```
[HUAWEI-bfd] quit
[HUAWEI] bfd atoc bind peer-ipv6 2001:db8:1::1 source-ipv6 2001:db8:1::1 auto
[HUAWEI-bfd-session-atoc]
```

12.1.9 bfd one-arm-echo

Function

The **bfd one-arm-echo** command configures the BFD echo function.

The **undo bfd** command deletes a specified BFD session and cancels the binding.

By default, the BFD echo function is not configured.

Format

bfd *session-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] **one-arm-echo**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session supporting the BFD echo function.	The value is a string of 1 to 15 case-insensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip *peer-ip*	Specifies the peer IP address bound to the BFD session.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value must be an existing VPN instance name.
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. This parameter should be configured.	-
one-arm-echo	Indicates a BFD session supporting the BFD echo function.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Among two directly connected devices, one device supports BFD, whereas the other device does not support BFD. To rapidly detect forwarding failures between the two devices, configure a BFD session supporting the BFD echo function on the BFD-supporting device. The BFD-supporting device sends an Echo Request packet to the remote device. The remote device sends the Echo Request packet back along the same path to detect the forwarding link connectivity.

When you configure a BFD session supporting the BFD echo function:

- Specify **source-ip** *ip-address*. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness. When URPF is enabled, ensure that **source-ip** *ip-address* can be pinged from the remote device so that the URPF-enabled device does not incorrectly discard BFD packets.
- On a network, some devices discard packets with the same source and destination IP addresses, so you are advised to set the value of **source-ip** *ip-address* to be different from the IP address of the outbound interface.
- If a VPN instance is specified, BFD is configured to detect the one-hop link in the VPN instance.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Precautions

The difference between a BFD session supporting the BFD echo function and a common BFD session is as follows:

- When configuring a BFD session supporting the BFD echo function, you can only specify **local** *discr-value* in the **discriminator** command.
- You can only run the **min-echo-rx-interval** command to change the interval for receiving BFD packets.

NOTE

- If the IP address of an outbound interface is changed after a BFD session is configured, the source IP address of BFD packets is not updated.
- The BFD echo function is only applicable to single-hop BFD sessions.
- After the **bfd one-arm-echo** command is executed, run the **commit** command to commit the configuration to make the configuration take effect.

Example

Configure a BFD session **test** supporting the BFD echo function.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip 10.10.10.1 interface vlanif 100 source-ip 10.10.10.2 one-arm-echo
[HUAWEI-bfd-session-test] discriminator local 100
[HUAWEI-bfd-session-test] commit
```

12.1.10 bfd session-name

Function

The **bfd** command displays the view of a specified BFD session.

The **undo bfd** command deletes a specified BFD session.

Format

bfd *session-name*

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the created BFD session, run the **bfd** *session-name* command to enter the specified BFD session view.

Prerequisites

A BFD session has been created by using either of the following commands:

- **bfd bind peer-ip**
- **bfd bind peer-ip default-ip**
- **bfd bind peer-ip source-ip auto**
- **bfd one-arm-echo**

Precautions

The **bfd** *session-name* command displays the BFD session view regardless of whether the BFD session status is Up.

After the functional parameters of the BFD session are set, you must run the **commit** command to make (expect static BFD session with automatically negotiated discriminators), the configurations take effect.

If the BFD session is in the Down state, after you run the **bfd** *session-name* command to enter the BFD session view and set functional parameters, the configurations can immediately take effect after being committed using the **commit** command.

Example

Enter the view of the BFD session named **session**.

```
<HUAWEI> system-view
[HUAWEI] bfd session
[HUAWEI-bfd-session-session]
```

12.1.11 bfd session nonexistent-config-check

Function

The **bfd session nonexistent-config-check enable** command enables the device to check whether the associated BFD session is deleted.

The **undo bfd session nonexistent-config-check disable** command enables the device to check whether the associated BFD session is deleted.

The **bfd session nonexistent-config-check disable** command disables the device from checking whether the associated BFD session is deleted.

By default, the device is enabled to check whether the associated BFD session is deleted.

Format

bfd session nonexistent-config-check enable

undo bfd session nonexistent-config-check disable

bfd session nonexistent-config-check disable

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

After BFD for IPv4/IPv6 static routes and association between VRRP/VRRP6/E-Trunk and BFD are configured, deleting the BFD session may cause the association function to become ineffective. You can run the **bfd session nonexistent-config-check enable** command to enable the device to check whether the associated BFD session is deleted. When the associated BFD session is being deleted, the system displays a message indicating that the BFD session cannot be deleted. This function prevents the associated BFD session from being deleted incorrectly.

Example

Disable the device from checking whether the associated BFD session is deleted.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] bfd session nonexistent-config-check disable
```

12.1.12 commit

Function

The **commit** command commits the BFD session configuration.

Format

commit

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the modification on a BFD session take effect, you must run the **commit** command.

Precautions

- To establish a BFD session, the interface bound to the BFD session must be Up and there is a reachable route to the peer IP address.
- If conditions for BFD session setup are not met, the system keeps the configuration entries of the BFD session. The BFD session, however, cannot be established when you use the **commit** command.
- The system periodically scans BFD configuration entries that are committed but not used to establish sessions. If conditions are met, a session is established.
- The number of BFD sessions that can be established in the system is limited. When the number of established BFD sessions reaches the upper limit and you use the **commit** command to commit the configurations of a new BFD session, the system generates a log indicating that the BFD session cannot be established and sends traps.
- After creating a BFD session, if you need to modify session parameters, such as **process-pst**, **process-interface-status**, **min-tx-interval**, **min-rx-interval**, **detect-multiplier**, **tos-exp (BFD session view)**, **wtr**, **description**, **authentication-mode (BFD)**, **trigger if-down delay** or **receiving-admindown trigger if-down** you can directly run the corresponding commands without running the **commit** command, and the modification takes effect immediately.
- After running the **bfd bind peer-ip source-ip auto** command to create configurations for a static BFD session with automatically negotiated discriminators, you do not need to run the **commit** command to commit the configurations. BFD sessions can be automatically established, and relevant configurations are labeled with the commit tags. The **commit** command can still be used but does not take effect.

Example

Commit the BFD session configuration.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-test] discriminator local 22
[HUAWEI-bfd-session-test] discriminator remote 33
[HUAWEI-bfd-session-test] commit
```

12.1.13 dampening timer-interval

Function

The **dampening timer-interval** command configures BFD session flapping suppression timers.

The **undo dampening timer-interval** command restores the default configuration.

BFD session flapping suppression timers start by default.

The default initial, secondary, and maximum BFD session flapping suppression timer values are 2000 ms, 5000 ms, and 12000 ms, respectively.

Format

dampening timer-interval maximum *maximum-milliseconds* **initial** *initial-milliseconds* **secondary** *secondary-milliseconds*

undo dampening timer-interval [**maximum** *maximum-milliseconds* **initial** *initial-milliseconds* **secondary** *secondary-milliseconds*]

Parameters

Parameter	Description	Value
maximum *maximum-milliseconds*	Specifies a maximum BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 12000.
initial *initial-milliseconds*	Specifies an initial BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 2000.
secondary *secondary-milliseconds*	Specifies a secondary BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 5000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If BFD detects link Down, services are switched. A penalty mechanism is provided to delay BFD session negotiation and prevent frequent service switchovers, protecting link resources and reducing link resource consumption.

To configure BFD session flapping suppression timers, run the **dampening timer-interval** command.

Prerequisites

BFD has been globally enabled using the **bfd** command in the system view.

Configuration Impact

After the **dampening timer-interval** command is run:

1. When a BFD session flaps for the first time, the initial BFD session flapping suppression timer starts. If the BFD session flaps again before the initial BFD session flapping suppression timer expires, BFD session renegotiation is triggered after the initial BFD session flapping suppression timer expires.
2. After the initial BFD session flapping suppression timer ends, the secondary BFD session flapping suppression timer starts. If the BFD session flaps before the secondary BFD session flapping suppression timer expires, BFD session renegotiation is triggered after the secondary BFD session flapping suppression timer expires. After that, the timer value is *secondary-milliseconds* x $2^{(n-1)}$, where *n* is the number of times that the secondary BFD session flapping suppression timer starts.
3. After the timer value of *secondary-milliseconds* x $2^{(n-1)}$ is greater than or equal to the value specified by *maximum-milliseconds*, the BFD session uses the value specified by *maximum-milliseconds* as a flapping delay three consecutive times. Then, the BFD session flapping delay is recalculated based on Step 1.

Precautions

The configured maximum BFD session flapping suppression timer value must be greater than the configured initial or secondary BFD session flapping suppression timer value. Otherwise, the configuration fails.

Do not configure both the **dampening timer-interval** and **wtr** commands. Otherwise, the BFD session recovery period becomes long.

Example

Set a maximum, initial, and secondary BFD session flapping suppression timer values to 20000 ms, 1000 ms, and 3000 ms, respectively.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] dampening timer-interval maximum 20000 initial 1000 secondary 3000
```

12.1.14 default-ip-address

Function

The **default-ip-address** command configures the default multicast IP address used by all BFD sessions.

The **undo default-ip-address** command restores the default multicast IP address.

By default, BFD uses the multicast IP address 224.0.0.184.

Format

default-ip-address *ip-address*

undo default-ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default multicast IP address.	The value ranges from 224.0.0.107 to 224.0.0.250.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using BFD to detect the physical status of a link, you may not specify the peer IP address. In certain situations, the peer such as the member link of the Eth-Trunk is not assigned an IP address. In this case, you need to bind a BFD session to a multicast IP address and send BFD control packets to the multicast IP address.

You must change the default multicast IP address in the following situations:

- On the network, other protocols use the multicast IP address.
- If multiple BFD sessions exist on a path, for example, Layer 3 interfaces are connected through Layer 2 switching devices that support BFD, configure different default multicast IP addresses for the devices where different BFD sessions are established. In this manner, BFD packets can be correctly forwarded.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

If the **bfd bind peer-ip default-ip** command has been run in the system view, the **default-ip-address** command cannot be used to change the default BFD multicast address.

Example

Set the default multicast IP address to 224.0.0.150.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] default-ip-address 224.0.0.150
```

12.1.15 description (BFD session view)

Function

The **description** command configures the description of a BFD session.

The **undo description** command deletes the description of a BFD session.

By default, the description of a BFD session is empty.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a BFD session.	The value is a string of 1 to 51 case-sensitive characters with spaces.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, multiple BFD sessions need to be configured. To differentiate BFD sessions, run the **description** command to configure a description for a BFD session. A meaningful description is recommended.

Configuration Impact

It is difficult to identify a BFD session that is not configured or whose description is deleted.

Precautions

If you run the **description** command in the same BFD session view multiple times, only the latest configuration takes effect.

The **description** command takes effect only for statically configured BFD sessions but does not take effect for dynamic BFD sessions or BFD sessions with automatically negotiated discriminators.

Example

Set the description of the BFD session named **atoc**.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] description SwitchA_to_SwitchC
```

12.1.16 detect-multiplier

Function

The **detect-multiplier** command sets the local detection multiplier.

The **undo detect-multiplier** command restores the default local detection multiplier.

By default, the local detection multiplier is 3.

Format

detect-multiplier *multiplier*

undo detect-multiplier

Parameters

Parameter	Description	Value
multiplier	Specifies the local detection multiplier of a BFD session.	The value is an integer that ranges from 3 to 50.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

You can increase or reduce the local detection multiplier based on actual networking. On a stable link, there is no need to frequently detect the link status, so you can increase the local detection multiplier.

If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Configuration Impact

- On an unstable link, if the local detection multiplier is small, the BFD session may flap. It is recommended that a larger local detection multiplier be used.
- When other protocols are associated with BFD, if a larger local detection multiplier is used, the BFD session takes a long period of time to detect faults on the link and traffic is switched to the backup link after the specified period. Packets may be lost during this period.

Precautions

Both ends of a BFD session can use different local detection multipliers.

Example

Set the local detection multiplier of the BFD session **atoc** to 10.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] detect-multiplier 10
```

12.1.17 discriminator

Function

The **discriminator** command sets local and remote discriminators for a static BFD session.

Format

discriminator { **local** *discr-value* | **remote** *discr-value* }

Parameters

Parameter	Description	Value
local *discr-value*	Specifies the local discriminator of a BFD session	The value is an integer that ranges from 1 to 8191.
remote *discr-value*	Specifies the remote discriminator of a BFD session	The value is an integer that ranges from 1 to 4294967295.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When creating a static BFD session, run the **discriminator** command to set local and remote discriminators. Otherwise, the static BFD session cannot be set up. The local and remote discriminators differentiate BFD sessions between two systems.

Precautions

- Only static BFD sessions require settings of local and remote discriminators.
- The local discriminator of the local system and the remote discriminator of the remote system must be the same. If the local discriminator of the local system and the remote discriminator of the remote system are different, a static BFD session cannot be set up.
- After the local and remote discriminators of a static BFD session are configured, the local and remote discriminators cannot be modified. To modify the local and remote discriminators of a static BFD session, delete the BFD session and reconfigure the local and remote discriminators.

Example

Set the local discriminator of a BFD session to 80 and the remote discriminator to 800.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] discriminator local 80
[HUAWEI-bfd-session-atoc] discriminator remote 800
```

12.1.18 display bfd configuration

Function

The **display bfd configuration** command displays the BFD session configuration.

Format

display bfd configuration { **all** | **static** } [**for-lsp** | **for-pw** | **for-te** | **for-vsi-pw**] [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration { **ldp-lsp peer-ip** *ip-address* **nexthop** *nexthop* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* } [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration mpls-te interface *interface-type interface-number* [**te-lsp**] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration pw interface *interface-type interface-number* [**secondary**] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration vsi-pw vsi *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd configuration passive-dynamic [**peer-ip** *ip-address* **remote-discriminator** *discriminator*] [**verbose**] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

display bfd configuration { **static name** *session-name* | **dynamic** | **static-auto** | **peer-ip** { **default-ip** | *ip-address* [**vpn-instance** *vpn-instance-name*] } | **discriminator** *local-discr-value* } [**verbose**]

display bfd configuration peer-ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**verbose**]

display bfd configuration { **all** | **static** } **[for-ip** | **for-ipv6**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays the configurations of all BFD sessions.	-
static	Displays the configurations of static BFD sessions.	-

Parameter	Description	Value
for-vsi-pw	Displays the configurations of the BFD sessions for detecting VSI PWs.	-
for-ip	Displays the configurations of the BFD sessions for detecting IP links.	-
for-lsp	Displays the configurations of the BFD sessions for detecting LSPs.	-
for-pw	Displays the configurations of the BFD sessions for detecting PWs.	-
for-te	Displays the configurations of the BFD sessions for detecting TE tunnels.	-
vsi-pw	Displays the configurations of the BFD sessions for detecting VSI PWs.	-
vsi *vsi-name*	Displays the configuration of the BFD session with the specified VSI instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Displays the configuration of the BFD session for detecting a VSI PW with the specified peer IPv4 address.	The value is in dotted decimal notation.
peer-ip *ip-address*	Displays the configuration of the BFD session bound to the specified peer IP address.	-

Parameter	Description	Value
vc-id *vc-id*	Displays the configuration of the BFD session with the specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
passive-dynamic	Displays the configurations of the BFD sessions dynamically created by the end in passive mode.	-
remote-discriminator *discriminator*	Displays the configuration of the BFD session with the local discriminator of the source device initiating the BFD session.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays detailed BFD configurations.	-
name *session-name*	Displays the configuration of the static BFD session with the specified name.	The value is a string of 1 to 15 characters without spaces. **NOTE** If the string is enclosed within double quotation marks ("), the string can contain spaces.
dynamic	Displays dynamic BFD configurations and the configurations of static BFD sessions with automatically negotiated discriminators.	-
discriminator *local-discr-value*	Displays the configuration of the BFD session with the specified local discriminator.	The value is an integer that ranges from 1 to 16383.
default-ip	Displays statistics about multicast BFD sessions.	-
vpn-instance *vpn-instance-name*	Displays the configuration of the BFD session bound to a specified VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
static-auto	Displays the configuration of the static BFD session with the automatically negotiated discriminators.	-
ldp-lsp	Displays the configurations of the BFD sessions for detecting LDP LSPs.	-
nexthop *nexthop*	Displays the configuration of the BFD session with the specified next hop address.	The value is in dotted decimal notation.
interface-type interface-number	Displays BFD binding information on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
static-lsp	Displays the configurations of the BFD sessions for detecting static LSPs.	-
lsp-name	Displays the configuration of the BFD session for detecting the static LSP with the specified name.	The value is a string of 1 to 19 case-sensitive characters.
mpls-te	Displays the configurations of the BFD sessions for detecting MPLS TE tunnels.	-
te-lsp	Displays the configuration of the BFD session for detecting the primary LSP bound to a TE tunnel.	-

Parameter	Description	Value
pw	Displays the configurations of the BFD sessions for detecting PWs.	-
secondary	Displays the configuration of the BFD session for detecting the secondary PW.	-
peer-ipv6 *ipv6-address*	Displays the configuration of the BFD6 session bound to a specified IPv6 address.	-
for-ipv6	Displays the configurations of static or all BFD6 sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When multiple BFD sessions exist, you can view information about certain BFD sessions by specifying the parameters such as the type, name, and peer IP address.

Precautions

If a static BFD session with automatically negotiated discriminators and a dynamic BFD session share the same configurations, you can view that the shared session configurations by BFD session type (static and dynamic).

Example

Display the configurations of all BFD sessions.

```
<HUAWEI> display bfd configuration all
--------------------------------------------------------------------------------
CFG Name        CFG Type       LocalDiscr MIndex    SessNum  Commit   AdminDown
--------------------------------------------------------------------------------
atob            S_IP_PEER      -          512       0        False    False
test            S_IP_PEER      1          513       0        False    False
zzz             S_IP_IF        3          514       0        False    False
--------------------------------------------------------------------------------
    Total Commit/Uncommit CFG Number : 0/3
```

Table 12-1 Description of the display bfd configuration command output

Item	Specification
CFG Name	BFD session name.
CFG Type	BFD session setup type: ● S_IP_IF: indicates a single-hop BFD session that is established statically and bound to an interface. ● S_IP_PEER: indicates a multi-hop BFD session that is established statically. ● S_STA_LSP: indicates a BFD session that is established statically and used for detecting an LSP. ● S_LDP_LSP: indicates a BFD session that is established statically and used for detecting an LDP LSP. ● S_TE_LSP: indicates a BFD session that is statically established and used for detecting a TE LSP. ● S_TE_TNL: indicates a BFD session that is statically established and used for detecting a TE tunnel. ● S_PW: indicates a BFD session that is statically established and used for detecting a PW. ● S_VSI_PW: indicates a BFD session that is statically established and used for detecting a VSI PW. ● Dynamic: indicates a BFD session that is dynamically established. ● Entire_Dynamic: indicates a BFD session that is entirely and dynamically established. ● S_AUTO_IF: indicates a static single-hop BFD session with automatically negotiated discriminators. ● S_AUTO_PEER: indicates a static multi-hop BFD session with automatically negotiated discriminators.
LocalDiscr	Local discriminator of the BFD session. To set the local discriminator of the BFD session, run the **discriminator** command.
MIndex	Configuration entry index of a BFD session.
SessNum	Number of BFD sessions in a configuration entry.
Commit	Flag of enabling a BFD session. After you run the **commit** command to commit configurations in the BFD session view, the flag is displayed as **True**. Otherwise, it is displayed as **False**.

Item	Specification
AdminDown	Flag of the management status of a BFD session. After you run the **shutdown (BFD session view)** command to disable the local session in the BFD session view, the flag is displayed as **True**. Otherwise, it is displayed as **False**.
Total Commit/ Uncommit CFG Number	Total number of BFD sessions that are committed through the **commit** command in the BFD session view and total number of BFD sessions that are not committed.

Display detailed configurations of all BFD sessions.

```
<HUAWEI> display bfd configuration all verbose
--------------------------------------------------------------------------------
 BFD Session Configuration Name : atob
--------------------------------------------------------------------------------
 Local Discriminator    : -                Remote Discriminator   : -
 BFD Bind Type          : Peer IP Address
 Bind Session Type      : Static
 Bind Peer IP Address   : 192.168.1.9
 Bind Interface         : -
 Select Board           : -
 Track Interface        : -
 TOS-EXP                : 7                Local Detect Multi     : 3
 Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
 WTR Interval (ms)      : -                Process PST            : Disable
 Proc Interface Status  : Disable
 Bind Application       : No Application Bind
 Session Description    : -
 Session Create Status  : Failed(65532)
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
 BFD Session Configuration Name : test
--------------------------------------------------------------------------------
 Local Discriminator    : 1                Remote Discriminator   : 2
 BFD Bind Type          : Peer IP Address
 Bind Session Type      : Static
 Bind Peer IP Address   : 192.168.10.2
 Bind Interface         : -
 Select Board           : -
 Track Interface        : -
 TOS-EXP                : 7                Local Detect Multi     : 3
 Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
 WTR Interval (ms)      : -                Process PST            : Disable
 Proc Interface Status  : Disable
 Bind Application       : No Application Bind
 Session Description    : -
 Session Create Status  : Failed(65532)
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
 BFD Session Configuration Name : zzz
--------------------------------------------------------------------------------
 Local Discriminator    : 3                Remote Discriminator   : 4
 BFD Bind Type          : Interface(GigabitEthernet0/0/1)
 Bind Session Type      : Static
 Bind Peer IP Address   : 192.168.20.4
 Bind Interface         : GigabitEthernet0/0/1
 TOS-EXP                : 7                Local Detect Multi     : 3
```

```
 Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
 WTR Interval (ms)      : -               Process PST           : Disable
 Auth Key ID            : -               Auth Timer            : -
 Meticulous Auth        : False           Auth Type             : None
 Proc Interface Status  : Enable
 Bind Application       : IFNET
 Session Description    : -
 Session Create Status  : Failed(65532)
--------------------------------------------------------------------------------

   Total Commit/Uncommit CFG Number : 0/3
```

Table 12-2 Description of the display bfd configuration all verbose command output

Item	Specification
BFD Session Configuration Name	BFD session name.
Local Discriminator	Local discriminator of a BFD session. To set the local discriminator of a BFD session, run the **discriminator** command.
Remote Discriminator	Remote discriminator of a BFD session. To set the remote discriminator of a BFD session, run the **discriminator** command.
BFD Bind Type	BFD session binding type: ● Peer IP Address: indicates multi-hop BFD for an IP link. ● Interface: indicates single-hop BFD for an IP link. ● STATIC_LSP: indicates that a static LSP is detected. ● LDP_LSP: indicates that an LDP LSP is detected. ● TE_LSP: indicates that an LSP bound to a TE tunnel is detected. ● TE_TUNNEL: indicates that a TE tunnel is detected. ● PW: indicates that a PW is detected. ● VSI_PW: indicates that a VSI PW is detected.

Item	Specification
Bind Session Type	Mode in which a BFD session is established: - Static: indicates the BFD sessions that are established through the static configurations. - Dynamic: indicates the BFD sessions that are triggered dynamically. - Static_Auto: indicates the statically established BFD sessions with automatically negotiated discriminators. - Entire_Dynamic: indicates the BFD sessions that are entirely and dynamically triggered.
Bind Peer Ip Address	Peer IP address of a BFD session or multicast IP address bound to a BFD session.
Bind Interface	Local interface bound to a BFD session.
Track Interface	Interface tracked by the BFD session.
TOS-EXP	Priority of a BFD packet. To set the priority of a BFD packet, run the **tos-exp** command.
Local Detect Multi	Local detection multiplier. To set the local detection multiplier, run the **detect-multiplier** command.
Min Tx Interval (ms)	Minimum interval for sending BFD packets. To set the minimum interval for sending BFD packets, run the **min-tx-interval** command.
Min Rx Interval (ms)	Minimum interval for receiving BFD packets. To set the minimum interval for receiving BFD packets, run the **min-rx-interval** command.
WTR Interval (ms)	WTR time. To set the WTR time, run the **wtr** command.
Process PST	Flag for processing the Port Status Table (PST). If the **process-pst** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Auth Key ID	Authentication key ID of a BFD session.
Auth Timer	Negotiation timeout period of a BFD session, in seconds.
Meticulous Auth	Authentication flag - **True**: strict - **False**: non-strict

Item	Specification
Auth Type	BFD authentication type: - **NONE**: no authentication - **SIMPLE**: simple password authentication - **MD5**: MD5 authentication - **MMD5**: meticulous MD5 authentication - **SHA1**: SHA1 authentication - **MSHA1**: meticulous SHA1 authentication
Proc interface status	Flag of association between the BFD session status and the interface status. If the **process-interface-status** command is configured, this field is displayed as Enable. Otherwise, it is displayed as **Disable**.
Bind Application	Application bound to the BFD session.
Session Description	Description of the BFD session. To set the description of the BFD session, run the **description** command.
Session Create Status	Status of BFD session creation: - Success - Failed
Total Commit/Uncommit CFG Number	Total number of BFD sessions that are committed through the **commit** command in the BFD session view and total number of BFD sessions that are not committed.

12.1.19 display bfd interface

Function

The **display bfd interface** command displays information about a BFD-enabled interface.

Format

display bfd interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to the BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd interface** command displays information about a BFD-enabled interface, including the BFD session bound to the interface and the BFD session status.

Example

Display information about a BFD-enabled interface.

```
<HUAWEI> display bfd interface
--------------------------------------------------------------------------------
Interface Name          MIndex       Sess-Count      BFD-State
--------------------------------------------------------------------------------
Vlanif100               256          1               up
--------------------------------------------------------------------------------
    Total Interface Number : 1
```

Table 12-3 Description of the display bfd interface command output

Item	Description
Interface Name	Name of the BFD-enabled interface.
MIndex	Index of the interface entry.
Sess-Count	Number of BFD sessions bound to the interface.

Item	Description
BFD-State	BFD status of an interface. The value can be up or down. **NOTE** If a BFD session is bound to the interface and configured with the **process-interface-status** command, the BFD session's status is displayed (The interface is up when the BFD session is in the AdminDown or Receive AdminDown state). Otherwise, the interface's physical status is displayed. If multiple BFD sessions are bound to the interface, only one BFD session can be configured with the **process-interface-status** command.
Total Interface Number	Number of the BFD-enabled interface.

12.1.20 display bfd session

Function

The **display bfd session** command displays information about BFD sessions.

Format

display bfd session { **dynamic** | **discriminator** *discr-value* | **peer-ip** { **default-ip** | *ip-address* [**vpn-instance** *vpn-instance-name*] } | **static-auto** } [**verbose**]

display bfd session { **all** | **static** } [**for-lsp** | **for-pw** | **for-te** | **for-vsi-pw**] [**verbose**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session { **ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* } [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session mpls-te interface *interface-type interface-number* [**te-lsp**] [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session pw interface *interface-type interface-number* [**secondary**] [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session passive-dynamic [**peer-ip** *ip-address* **remote-discriminator** *remote-discr-value*] [**verbose**] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

display bfd session { **vsi-pw vsi** *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] } [**verbose**] (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd session peer-ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**verbose**]

display bfd session { **all** | **static** } **[for-ip** | **for-ipv6**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all BFD sessions.	-
static	Displays information about all static BFD sessions.	-
for-ip	Displays information about the BFD sessions for detecting IP links.	-
for-lsp	Displays information about the BFD sessions for detecting LSPs.	-
for-pw	Displays information about the BFD sessions for detecting PWs.	-
for-te	Displays information about the BFD sessions for detecting TE tunnels.	-
for-vsi-pw	Displays information about the BFD sessions for detecting VSI PWs.	-
vsi-pw	Displays information about the BFD session for detecting a VSI PW.	-
vsi-name	Displays information about the BFD session with the specified VSI instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Displays information about the BFD session for detecting a VSI PW with the specified peer IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
nexthop *ip-address*	Displays information about the BFD session with the specified next hop address.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Displays information about the BFD session with the specified outbound interface.	-
vc-id *vc-id*	Displays information about the BFD session with the specified VC ID.	The value is a decimal integer ranging from 1 to 4294967295.
verbose	Displays detailed information about BFD sessions.	-
dynamic	Displays information about all dynamic BFD sessions and static BFD sessions negotiated with discriminators.	-
passive-dynamic	Displays information about all dynamic BFD sessions created on the end in passive mode.	-
discriminator *discr-value*	Displays information about the BFD session with a specified discriminator. You can specify only a local discriminator.	The value is an integer that ranges from 1 to 16383.
remote-discriminator *remote-discr-value*	Displays information about the BFD session with a specified discriminator. You can specify only a remote discriminator.	The value is an integer that ranges from 1 to 4294967295.
peer-ip *ip-address*	Displays information about the BFD session bound to the specified peer IP address.	The value is in dotted decimal notation.
default-ip	Displays statistics about multicast BFD sessions.	-

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the BFD session bound to the specified VPN instance.	The value must be an existing VPN instance name.
static-auto	Displays the information about the static BFD sessions with the automatically negotiated discriminators.	-
ldp-lsp	Displays information about the BFD sessions for detecting LDP LSPs.	-
static-lsp	Displays information about the BFD sessions for detecting static LSPs.	-
lsp-name	Displays information about the BFD session for detecting the static LSP with the specified name.	The value is a string of 1 to 19 case-sensitive characters without spaces.
mpls-te	Displays information about the BFD sessions for detecting MPLS TE tunnels.	-
te-lsp	Displays information about the BFD session for detecting the primary LSP bound to a TE.	-
pw	Displays information about the BFD sessions for detecting PWs.	-
secondary	Displays information about the BFD session for detecting the secondary PW.	-
peer-ipv6 *ipv6-address*	Displays information about the BFD6 session bound to a specified IPv6 address.	-
for-ipv6	Displays information about static or all BFD6 sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd session** command displays information about BFD sessions.

Prerequisites

BFD has been enabled globally.

Precautions

- When a BFD session changes from Down to Up, if the WTR time of the session is not 0, BFD sends a notification that the session becomes Up only after the WTR time expires.
- If a static BFD session with automatically negotiated discriminators and a dynamic BFD session are bound to the same peer IP address, the **display bfd session** command displays the same entry for the static BFD session or dynamic BFD session.

Example

Display the summary of all BFD sessions.

```
<HUAWEI> display bfd session all
--------------------------------------------------------------------------------
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
10    11         10.10.10.2      Up        S_IP_IF     Vlanif31
8192  0          10.10.10.2      Down      S_AUTO_IF   Vlanif31
--------------------------------------------------------------------------------
     Total UP/DOWN Session Number : 1/1
```

Table 12-4 Description of the display bfd session command output

Item	Description
Local	Local discriminator of the BFD session. To set the local discriminator, run the **discriminator** command.
Remote	Remote discriminator of the BFD session. To set the remote discriminator, run the **discriminator** command.
PeerIpAddr	Peer IP address bound to the BFD session.

Item	Description
InterfaceName	Outbound interface bound to the BFD session. In multi-hop BFD, this field is displayed as - because no interface is bound to a BFD session.
State	BFD session status: ● Init: The BFD session is in the initialized state. ● Up: indicates that the BFD session is in Up state. ● Down: indicates that the BFD session is in Down state. ● AdmDown: indicates that a BFD session is AdminDown when the **shutdown (BFD session view)** command is run.

Item	Description
Type	BFD session type: ● S_TE_LSP: indicates a BFD session that is established statically and bound to a TE LSP. ● S_TE_TNL: indicates a BFD session that is established statically and bound to a TE tunnel. ● S_IP_PEER: indicates a BFD session that is established statically and bound to an IP link. ● S_IP_IF: indicates a BFD session that is established statically and bound to an interface. ● S_LDP_LSP: indicates a BFD session that is established statically and bound to a dynamic LSP. ● S_PW(M): indicates a BFD session that is established statically and bound to the primary PW. ● S_PW(S): indicates a BFD session that is established statically and bound to the secondary PW. ● S_STA_LSP: indicates a BFD session that is established statically and bound to a static LSP. ● S_VSI_PW: indicates a BFD session that is established statically and bound to a VSI PW. ● D_IP_PEER: indicates a BFD session that is created dynamically and bound to an IP link. ● D_IP_IF: indicates a BFD session that is established dynamically and bound to an interface. ● D_LDP_LSP: indicates a BFD session that is established dynamically and bound to a dynamic LSP. ● D_TE_LSP: indicates a BFD session that is established dynamically and bound to a TE LSP. ● D_PW(S): indicates a BFD session that is established dynamically and bound to the secondary PW. ● D_PW(M): indicates a BFD session that is established dynamically and bound to the primary PW. ● E_Dynamic: indicates a BFD session that is established entirely and dynamically. After you enable the function of dynamically establishing a BFD session on the destination of an LSP, this session type is created. ● S_AUTO_IF: indicates a static single-hop BFD session with automatically negotiated discriminators. ● S_AUTO_PEER: indicates a static multi-hop BFD session with automatically negotiated discriminators.
Total UP/ DOWN Session Number	Number of BFD sessions in Up or Down state.

Display detailed information about all BFD sessions.

```
<HUAWEI> display bfd session all verbose
--------------------------------------------------------------------------------
Session MIndex : 16384     (One Hop) State : Up        Name : test
------------------------------------------------------------------------------
  Local Discriminator    : 111              Remote Discriminator   : 222
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(Vlanif500)
  Bind Session Type      : Static
  Bind Peer IP Address   : 224.0.0.184
  NextHop Ip Address     : 224.0.0.184
  Bind Interface         : Vlanif500
  FSM Board Id           : 6                TOS-EXP                : 6
  Min Tx Interval (ms)   : 10               Min Rx Interval (ms)   : 10
  Actual Tx Interval (ms): 10               Actual Rx Interval (ms): 10
  Local Detect Multi     : 3                Detect Interval (ms)   : 30
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 255
  Proc Interface Status  : Disable          Process PST            : Disable
  WTR Interval (ms)      : -
  Active Multi           : 3                DSCP                   : -
  Auth Key ID            : 1                Auth Timer             : 0
  Meticulous Auth        : True             Auth Type              : MSHA1
  Xmit Auth Seq          : 0x5cb3cbed       Rcv Auth Seq           : 0x28909183
  Error Packet Info      : Correct Pkt
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : -                Session Detect TmrID   : -
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-B030000 | RCV-0 | IF-B030000 | TOKEN-0
  Session Description    : -
  Trigger If-down Delay Time (s)      : -
  Receiving-admindown Trigger If-down : Disable
------------------------------------------------------------------------------

     Total UP/DOWN Session Number : 1/0
```

Table 12-5 Description of the display bfd session all verbose command output

Item	Description
Session MIndex	Index of BFD session entries.
State	Status of a BFD session.
Name	Name of a BFD session.
Local Discriminator	Local discriminator of the BFD session. To set the local discriminator of the BFD session, run the **discriminator** command.
Remote Discriminator	Remote discriminator of the BFD session. To set the remote discriminator of the BFD session, run the **discriminator** command.

Item	Description
Session Detect Mode	BFD detection modes: ● Asynchronous Mode Without Echo Function: indicates the asynchronous mode without the echo function. ● Demand Mode Without Echo Function: indicates the demand mode without the echo function.
BFD Bind Type	BFD session binding type: ● STATIC_LSP: indicates that a static LSP is detected. ● LDP_LSP: indicates that an LDP LSP is detected. ● TE_TUNNEL: indicates that a TE tunnel is detected. ● TE_LSP: indicates that an LSP bound to a TE is detected. ● PW: indicates that a PW is detected. ● Peer IP Address: indicates that a multi-hop IP link is detected. ● When one-hop BFD is used to detect an IP link, this field is displayed as **Interface** and the name of the bound local interface. ● VSI_PW: indicates that a VSI PW is detected. ● Static_Auto: indicates the BFD session with automatically negotiated discriminators.
Bind Session Type	Indicates the ways of establishing BFD sessions: ● Static: indicates that a BFD session is established manually. ● Dynamic: indicates that a BFD session is established dynamically. ● Static_Auto: indicates that a BFD session is established with automatically negotiated discriminators. ● Entire_Dynamic: indicates that a BFD session is triggered entirely and dynamically. After you enable the function of dynamically establishing a BFD session on the destination of an LSP, this session type is created.
Bind Peer Ip Address	Peer IP address bound to the BFD session.
NextHop Ip Address	IP address of the next hop.
Bind Interface	Outbound interface bound to the BFD session.

Item	Description
Bind Source Ip Address	Source IP address of the local interface bound to the BFD session. This field can be displayed only when the source IP address is specified for the BFD session that is created by running the **bfd bind peer-ip** or **bfd bind peer-ip default-ip** command.
FSM Board Id	Number of the processing board where the state machine works.
TOS-EXP	Priority of a BFD packet. To set the priority of a BFD packet, run the **tos-exp** command.
Min Tx Interval (ms)	Configured minimum interval for sending BFD packets. To set the minimum interval for sending BFD packets, run the **min-tx-interval** command.
Min Rx Interval (ms)	Configured minimum interval for receiving BFD packets. To set the minimum interval for receiving BFD packets, run the **min-rx-interval** command.
Actual Tx Interval (ms)	Actual minimum interval for sending BFD packets.
Actual Rx Interval (ms)	Actual minimum interval for receiving BFD packets.
Local Detect Multi	Local detection multiplier. To set the local detection multiplier, run the **detect-multiplier** command.
Detect Interval (ms)	BFD detection time.
Echo Passive	Whether the BFD passive Echo function is enabled: ● Enable ● Disable
Acl Number	ACL rule number
Destination Port	Number of the destination port of the BFD session packet. The single-hop BFD control packet uses destination port 3784 and the multi-hop BFD control packet uses 3784 or 4784.
TTL	TTL value of the BFD packet.
WTR Interval (ms)	WTR time of the BFD session. To set the WTR time of the BFD session, run the **wtr** command.

Item	Description
Process PST	Flag for processing the Port Status Table (PST). If the **process-pst** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Proc interface status	Flag of association between the BFD session status and the interface status. If the **process-interface-status** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Active Multi	Detection multiplier that is effective.
DSCP	DSCP value in the BFD session. The value ranges from 1 to 63. The value - indicates that the DSCP value does not take effect in the BFD session.
Auth Key ID	Authentication key ID of a BFD session
Auth Timer	Negotiation timeout period of a BFD session, in seconds
Meticulous Auth	Authentication flag ● **True**: strict ● **False**: non-strict
Auth Type	BFD authentication type: ● **NONE**: no authentication ● **SIMPLE**: simple password authentication ● **MD5**: MD5 authentication ● **MMD5**: meticulous MD5 authentication ● **SHA1**: SHA1 authentication ● **MSHA1**: meticulous SHA1 authentication
Xmit Auth Seq	Local sequence number of a BFD authentication session
Rcv Auth Seq	Remote sequence number of a BFD authentication session

Item	Description
Error Packet Info	Packet error information: - **Correct Pkt**: The packet is correct. - **Incorrect authentication type**: The authentication type is incorrect. - **Incorrect authentication length**: The authentication length is incorrect. - **Incorrect sequence number**: The sequence number is incorrect. - **Authentication failed**: The authentication fails. - **Incorrect authentication keyid**: The authentication key ID is incorrect. - **Local does not configure authentication**: Authentication is not configured at the local end. - **Remote does not configure authentication**: Authentication is not configured at the remote end.
Last Local Diagnostic	Local diagnostic cause for the last BFD session in Down state.
Bind Application	Application bound to the BFD session.
Session TX TmrID	Timer used for a BFD session to send packets.
Session Detect TmrID	BFD session detection timer.
Session Init TmrID	Timer for state machine initialization of a BFD session.
Session WTR TmrID	WTR timer of a BFD session.
Session Echo Tx TmrID	Timer used for a BFD session to send Echo packets.
PDT Index	Product information.
Session Description	Description of the BFD session. To set the description of the BFD session, run the **description** command.
Trigger If-down Delay Time (s)	Delay for a device to instruct the interface protocol to go down after the device detects a BFD down event, in seconds.
Receiving-admindown Trigger If-down	Whether the local device is enabled to instruct the interface protocol to go down upon receipt of an AdminDown packet.
Total UP/DOWN Session Number	Number of BFD sessions in Up or Down state.

12.1.21 display bfd statistics

Function

The **display bfd statistics** command displays global BFD statistics.

Format

display bfd statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd statistics** command displays global BFD statistics.

Precautions

Before using the **display bfd statistics** command to view BFD statistics within a specified period, run the **reset bfd statistics** command to clear existing statistics.

Example

Display global BFD statistics.

```
<HUAWEI> display bfd statistics
Current Display Board Number : Main; Current Product Register Type : S5730-36C-HI
IP Multihop Destination Port : 3784
Total Up/Down Session Number : 1/1
Current Session Number :
    Static session      : 2                Dynamic session        : 0
    E_Dynamic session  : 0                 STATIC_AUTO session    : 0
    LDP_LSP session    : 0                 STATIC_LSP session     : 0
    TE_TUNNEL session  : 0                 TE_LSP session         : 0
    PW session         : 0                 IP session             : 2
    VSI PW session     : 0                 LDP_TUNNEL session     : 0
    BGP_TUNNEL session : 0
--------------------------------------------------------------------------------
PAF/LCS Name                   Maxnum        Minnum        Create
--------------------------------------------------------------------------------
BFD_CFG_NUM                      256           1             2
BFD_IF_NUM                     256           1             1
BFD_SESSION_NUM                  256           1             2
BFD_IO_SESSION_NUM               256           1             -
BFD_PER_TUNNEL_CFG_NUM           8             1             -
--------------------------------------------------------------------------------
IO Board Current Created Session Statistics Information :(slot/number)
```

```
--------------------------------------------------------------------------------
           0/2
--------------------------------------------------------------------------------
Current Total Used Discriminator Num              : 2
--------------------------------------------------------------------------------
IO Board Reserved Sessions Number Information :(slot/number)
--------------------------------------------------------------------------------
           0/0
--------------------------------------------------------------------------------
BFD HA Information :
--------------------------------------------------------------------------------
Core Current HA Status                          : Slave Not Ready
Shell Current HA Status                         : Slave Not Ready
--------------------------------------------------------------------------------
BFD for LSP Information :
--------------------------------------------------------------------------------
Ability of auto creating BFD session on egress     : Disable
Period of LSP Ping                              : 60
System Session Delay Up Timer                     : OFF
--------------------------------------------------------------------------------
```

Table 12-6 Description of the display bfd statistics command output

Item	Description
Current Display Board Number	Number of the board where information is displayed.
Current Product Register Type	Type of the current product.
IP Multihop Destination Port	UDP port number.
Total Up/Down Session Number	Total number of BFD sessions in Up or Down state.
Current Session Number	Number of current BFD sessions.
Static session	Number of static BFD sessions.
Dynamic session	Number of dynamic BFD sessions.
E_Dynamic session	Number of entirely dynamic sessions.
STATIC_AUTO session	Number of BFD sessions with automatically negotiated discriminators.
LDP_LSP session	Number of BFD sessions for detecting an LDP LSP.
STATIC_LSP session	Number of BFD sessions for detecting a static LSP.
TE_TUNNEL session	Number of BFD sessions for detecting a TE tunnel.
TE_LSP session	Number of BFD sessions for detecting a TE LSP.
PW session	Number of BFD sessions for detecting a PW.
IP session	Number of BFD sessions for detecting an IP address.

Item	Description
LDP_TUNNEL session	Number of current BFD sessions for LDP tunnel
BGP_TUNNEL session	Number of current BFD sessions for BGP tunnel
PAF/LCS Name	Project name of the license file.
BFD_CFG_NUM	Maximum number of BFD sessions that can be globally configured.
BFD_IF_NUM	Maximum number of BFD sessions that can be bound to an interface.
BFD_SESSION_NUM	Maximum number of BFD sessions that can be globally established.
BFD_IO_SESSION_NUM	Maximum number of BFD sessions that can be established globally.
BFD_PER_TUNNEL_CFG_NUM	Maximum number of BFD sessions that can be configured on a tunnel.
IO Board Current Created Session Statistics Information : (slot/number)	Number of BFD sessions that are established.
Current Total Used Discriminator Num	Total number of currently configured discriminators.
IO Board Reserved Sessions Number Information : (slot/ number)	Number of BFD sessions that are reserved.
BFD HA Information	-
Core Current HA Status	HA status in the core: ● Normal: indicates that the HA status is normal. ● Batch Backup Going: indicates that backup is being performed. ● Slave Not Ready: indicates that the slave board is not ready. ● Smooth Going: indicates that smooth processing is being performed.

Item	Description
Shell Current HA Status	HA status in the shell: - Normal: indicates that the HA status is normal. - Batch Backup Going: indicates that backup is being performed. - Slave Not Ready: indicates that the slave board is not ready. - Smooth Going: indicates that smooth processing is being performed.
Ability of auto creating BFD session on egress	Whether the capability to establish an entirely dynamic BFD session is enabled.
Period of LSP Ping	Interval for sending LSP ping packets of dynamic BFD sessions for detecting an LSP/PW.
System Session Delay Up Timer	Status of the delay Up timer: - OFF: indicates that the system works properly. - Xs: indicates that the system recovers after X seconds and a BFD session can be Up.

12.1.22 display bfd statistics session

Function

The **display bfd statistics session** command displays BFD session statistics.

Format

display bfd statistics session { **all** | **static** } [**for-lsp** | **for-pw** | **for-te** | **for-vsi-pw**](S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd statistics session { **ldp-lsp peer-ip** *ip-address* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* | **mpls-te interface** *interface-type interface-number* [**te-lsp**] | **pw interface** *interface-type interface-number* [**secondary**] } (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd statistics session { **vsi-pw vsi** *vsi-name* **peer** *peer-address* [**vc-id** *vc-id*] } (S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H and S6730-H)

display bfd statistics session { **dynamic** | **discriminator** *discr-value* | **peer-ip default-ip** | **peer-ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **static-auto** }

display bfd statistics session peer-ipv6 *ipv6-address* [**vpn-instance** *vpn-instance-name*]

display bfd statistics session { **all** | **static** } [**for-ip** | **for-ipv6**]

Parameters

Parameter	Description	Value
all	Displays statistics about all BFD sessions.	-
static	Displays statistics about static BFD sessions.	-
dynamic	Displays statistics about dynamic BFD sessions and static BFD sessions with automatically negotiated discriminators.	-
discriminator *discr-value*	Displays statistics about the BFD sessions with a local discriminator.	The value is an integer that ranges from 1 to 16383.
peer-ip default-ip	Displays statistics about multicast BFD sessions.	-
peer-ip *ip-address*	Displays statistics about the BFD session bound to the specified peer IP address.	-
static-auto	Displays statistics about the static BFD session with the automatically negotiated discriminators.	-
vpn-instance *vpn-instance-name*	Displays statistics about the BFD sessions bound to a specified VPN instance.	The value must be an existing VPN instance name.
for-ip	Displays statistics about the BFD sessions for detecting IP links.	-
for-pw	Displays statistics about the BFD sessions for detecting PWs.	-
for-lsp	Displays statistics about the BFD sessions for detecting LSPs.	-

Parameter	Description	Value
for-te	Displays statistics about the BFD sessions for detecting a TE tunnel.	-
for-vsi-pw	Displays statistics about the BFD sessions for detecting VSI PWs.	-
vsi *vsi-name*	Displays statistics about the BFD session with the specified VSI PW instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-address*	Displays statistics about the BFD session for detecting a VSI PW with the specified peer IPv4 address.	The value is expressed in dotted decimal notation.
vc-id *vc-id*	Displays statistics about the BFD session with the specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
ldp-lsp	Displays statistics about the BFD sessions for detecting LDP LSPs.	-
nexthop *nexthop-address*	Displays statistics about the BFD session with the specified next hop address.	The value is expressed in dotted decimal notation.
interface-type interface-number	Displays statistics about the BFD session with the specified outbound interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
static-lsp	Displays statistics about the BFD sessions for detecting static LSPs.	-

Parameter	Description	Value
lsp-name	Displays statistics about the BFD session for detecting the static LSP with the specified name.	The value is a string of 1 to 19 case-sensitive characters without spaces.
mpls-te	Displays statistics about the BFD sessions for detecting MPLS TE tunnels.	-
te-lsp	Displays statistics about the BFD session for detecting the primary LSP bound to a TE.	-
pw	Displays statistics about the BFD sessions for detecting PWs.	-
secondary	Displays statistics about the BFD session for detecting the secondary PW.	-
peer-ipv6 *ipv6-address*	Displays statistics about the BFD6 session bound to a specified IPv6 address.	-
for-ipv6	Displays statistics about static or all BFD6 sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd statistics session** command displays BFD session statistics.

Precautions

- If static BFD with automatically negotiated discriminators and dynamic BFD share a session, you can specify **all**, **static-auto**, or **dynamic** for query.

- Before using the **display bfd statistics session** command to view BFD session statistics, run the **reset bfd statistics** command to clear existing statistics.

Example

Display statistics on all BFD sessions.

```
<HUAWEI> display bfd statistics session all
--------------------------------------------------------------------------------
Session MIndex : 16397        (Multi Hop)State : Up          Name : dyn_8196
--------------------------------------------------------------------------------
  Session Type                      : Dynamic
  Bind Type                         : IP
  Local/Remote Discriminator        : 8100/8101
  Received Packets                  : 1710577
  Send Packets                      : 1710593
  Received Bad Packets              : 0
  Send Bad Packets                  : 0
  Down Count                        : 0
  ShortBreak Count                  : 0
  Send Lsp Ping Count               : 0
  Dynamic Session Delete Count      : 0
  Create Time                       : 2011-10-23 14:28:34
  Last Down Time                    : 0000-00-00 00:00:00
  Total Time From Last DOWN         : ---D:--H:--M:--S
  Last Up Time                      : 2011-11-14 11:06:52+08:00
  Last Up Lasting Time              : 002D:16H:49M:17S
  Total Time From Create            : 000D:04H:45M:35S
  Auth Time (ms)                    : 0
  Auth Seq Known (ms)               : 0
  Trigger If-down Delay Time (ms)   : 0
--------------------------------------------------------------------------------

     Total Session Number : 1
```

Table 12-7 Description of the display bfd statistics session command output

Item	Description
Session MIndex	Index of BFD session entries.
State	Status of a BFD session.
Name	Name of a BFD session.
Session Type	Mode in which a BFD session is established: ● Static: indicates that a BFD session is established statically. ● Dynamic: indicates that a BFD session is established dynamically. ● Static_Auto: indicates that a BFD session is established with automatically negotiated discriminators. ● Entire_Dynamic: indicates the BFD sessions that are triggered entirely dynamically. After dynamic BFD session setup is enabled on the sink point of an LSP, a BFD session of this type is created.
Bind Type	BFD session binding type.

Item	Description
Local/Remote Discriminator	Local and remote discriminator of a BFD session. To set the local and remote discriminators of a BFD session, run the **discriminator** command.
Received Packets	Number of BFD packets received at the local end. This field can be deleted using the **reset bfd statistics** command.
Send Packets	Number of BFD packets sent by the local end. This field can be deleted using the **reset bfd statistics** command.
Received Bad Packets	Number of received error packets.
Send Bad Packets	Number of sent error packets.
Down Count	Number of times that a BFD session became Down.
ShortBreak Count	Number of times that a BFD session was transiently disconnected.
Send Lsp Ping Count	Number of LSP ping packets sent by the local end.
Dynamic Session Delete Count	Number of dynamic BFD sessions deleted.
Create Time	Time when a BFD session was created.
Last Down Time	Last time when a BFD session became Down.
Total Time From Last DOWN Down Status Lasting Time	Period from last time when a BFD session became Down to the current time. If a BFD session is Up, "Total Time From Last DOWN" is displayed. If a BFD session is Down, "Down Status Lasting Time" is displayed.
Last Up Time	Last time the BFD session becomes Up.
Last Up Lasting Time	Period from the last time when a BFD session is Up to the current time.
Total Time From Create	Period from the time when a BFD session was created to the current time.
Total Session Number	Number of BFD sessions.
Auth Time (ms)	Remaining time of the authentication timeout timer, in milliseconds
Auth Seq Known (ms)	Remaining time of the sequence number learning timer, in milliseconds

Item	Description
Trigger If-down Delay Time (ms)	Remaining time of the delay timer after which BFD instructs the interface to go down, in milliseconds
Total Session Number	Total number of BFD sessions

12.1.23 display bfd ttl

Function

The **display bfd ttl** command displays the globally configured TTL.

Format

display bfd ttl

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd ttl** command displays the globally configured TTL.

Example

Display information about all globally configured TTLs.

```
<HUAWEI> display bfd ttl
------------------------------------------------------------------------
Peer IP                              Mask       Type          Value
------------------------------------------------------------------------
10.10.10.0                            24        single-hop     255
```

Table 12-8 Description of the display bfd ttl command output

Item	Specification
Peer IP	IP segment address.

Item	Specification
Mask	Mask length.
Type	Type of the BFD session. The value can be single-hop or multi-hop.
Value	Initial value of the global TTL value.

12.1.24 min-echo-rx-interval

Function

The **min-echo-rx-interval** command configures the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.

The **undo min-echo-rx-interval** command restores the default minimum interval.

By default, the minimum interval is 1000 ms.

Format

min-echo-rx-interval *interval*

undo min-echo-rx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.	The value is an integer that ranges from 100 to 1000, in milliseconds. - After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. - After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a BFD session supporting the BFD echo function, you can set the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.

Prerequisites

A BFD session supporting the echo function has been configured using the **bfd one-arm-echo** command.

Example

Set the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function to 100 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd test
[HUAWEI-bfd-session-test] min-echo-rx-interval 100
```

12.1.25 min-rx-interval

Function

The **min-rx-interval** command sets the minimum interval for receiving BFD packets.

The **undo min-rx-interval** command restores the default minimum interval for receiving BFD packets.

By default, the minimum interval for receiving BFD packets is 1000 ms.

Format

min-rx-interval *interval*

undo min-rx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

Precaution

- You can increase or reduce the minimum interval for receiving BFD packets based on actual networking. The minimum interval for receiving BFD packets determines the detection time of a BFD session. On an unstable link, if the minimum interval for receiving BFD packets is small, the BFD session may flap. You can increase the minimum interval for receiving BFD packets. The default value is recommended. Do not randomly change the minimum interval for receiving BFD packets.
- If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the minimum interval for receiving BFD packets is smaller than 100 ms and the working mode of the switch is normal, the original BFD session needs to be deleted. Then set the working mode of the switch and reconfigure the BFD session.

Example

Set the minimum interval for receiving BFD packets to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd session
[HUAWEI-bfd-session-session] min-rx-interval 500
```

12.1.26 min-tx-interval

Function

The **min-tx-interval** command sets the minimum interval for sending BFD packets.

The **undo min-tx-interval** command restores the default minimum interval for sending BFD packets.

By default, the minimum interval for sending BFD packets is 1000 ms.

Format

min-tx-interval *interval*

undo min-tx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for sending BFD packets.	The value is an integer that ranges from 100 to 1000, in milliseconds. ● After the **set service-mode enhanced** command is configured on the S5731-H, S5731-S, S5731S-H, and S5731S-S, the value ranges from 3 to 1000. ● After the **set service-mode enhanced-bfd** command is configured on the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the value ranges from 3 to 1000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

Precaution

- You can increase or reduce the minimum interval for sending BFD packets based on actual networking. The minimum interval for sending BFD packets determines the detection time of a BFD session. On an unstable link, if the minimum interval for sending BFD packets is small, the BFD session may flap. You can increase the minimum interval for sending BFD packets. The default value is recommended. Do not randomly change the minimum interval for sending BFD packets.
- If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the minimum interval for sending BFD packets is smaller than 100 ms and the working mode of the switch is normal, the original BFD session needs to be deleted. Then set the working mode of the switch and reconfigure the BFD session.

Example

Set the minimum interval for sending BFD packets to 500 ms.

```
<HUAWEI> system-view
[HUAWEI] bfd session
[HUAWEI-bfd-session-session] min-tx-interval 500
```

12.1.27 multi-hop

Function

The **multi-hop** command configures the destination port number for a multi-hop BFD session.

The **undo multi-hop** command restores the default destination port number for a multi-hop BFD session.

By default, destination port 3784 is used in multi-hop BFD control packets.

Format

multi-hop destination-port { **3784** | **4784** }

undo multi-hop destination-port

Parameters

Parameter	Description	Value
3784	Indicates that destination port 3784 is used in multi-hop BFD control packets.	-
4784	Indicates that destination port 4784 is used in multi-hop BFD control packets.	-

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in the BFD draft, destination port 4784 is used by multi-hop BFD control packets. When the device running the latest version interworks with devices running earlier versions, destination port 3784 is used by multi-hop BFD control packets. When the device interworks with non-Huawei devices, destination port 4784 is used by multi-hop BFD control packets.

Precautions

- If destination port 4784 is used by multi-hop BFD control packets, the device fails to negotiate with the remote device on which destination port 3784 is used by multi-hop BFD control packets.
- If destination port 3784 is used by multi-hop BFD control packets, the device can successfully negotiate with the remote device on which destination port 4784 is used by multi-hop BFD control packets. On the device that is configured with destination port 3784, destination port 3784 is automatically updated to destination port 4784.
- If destination port 3784 is used by both multi-hop and single-hop BFD control packets, the single-hop and multi-hop BFD control packets are processed according to their TTLs.

- When a large number of multi-hop BFD sessions are set up, updating the destination ports may take a long time. Therefore, when a smaller interval for configuring multi-hop BFD sessions is used, the system displays a message indicating that the BFD session is being updated and you may try later.
- When the number of the destination port used in a multi-hop BFD control packet is updated, the BFD session in Up state may change to Down and then the BFD session is renegotiated.

NOTE

Determine to use port 3784 or 4784 before configuring a multi-hop BFD session between a Huawei device and a non-Huawei device. If the port number is not specified, you must change the port number after the BFD session becomes Up. Before changing the port number, shut down the BFD session. This is because changing the port number may cause all multi-hop BFD session to flap and affect services.

Example

Set the default destination port number to 4784 for multi-hop BFD control packets.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] multi-hop destination-port 4784
```

12.1.28 oam-bind ingress bfd-session trigger if-down egress interface

Function

The **oam-bind ingress bfd-session trigger if-down egress interface** command enables a BFD session to report faults to an interface.

The **undo oam-bind ingress bfd-session trigger if-down egress interface** command disables a BFD session from reporting faults to an interface.

By default, a BFD session is not enabled to report faults to an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

oam-bind ingress bfd-session *bfd-session-id* **trigger if-down egress interface** *interface-type interface-number*

undo oam-bind ingress bfd-session *bfd-session-id* **trigger if-down egress interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
bfd-session *bfd-session-id*	Specifies the local discriminator.	The value is an integer that ranges from 1 to 8191.
trigger if-down	Indicates that an interface goes Down when the BFD session associated with the interface detects a fault.	-
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a BFD session to report faults to an interface, run the **oam-bind ingress bfd-session trigger if-down egress interface** command.

Precautions

Before configuring a BFD session to report faults to an interface, pay attention to the following points:

- A BFD session has been created and its status is Up.
- The BFD session is a static BFD session.
- The BFD session and the interface are associated with each other. That is, after an interface is associated with BFD session 1, the interface cannot be associated with other BFD sessions. Similarly, BFD session 1 cannot be associated with other interfaces.

The ingress BFD session reports faults to the egress interface.

Example

Configure BFD session 1 to report faults to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress bfd-session 1 trigger if-down egress interface gigabitethernet
0/0/1
```

12.1.29 peer-ip ttl

Function

The **peer-ip ttl** command configures the TTL value in BFD packets.

The **undo peer-ip ttl** command restores the default TTL value in BFD packets.

By default, the TTL value in BFD packets varies with the BFD session type. By default, for a static BFD session, the TTL value of a single-hop BFD packet is 255 and the TTL value of a multi-hop BFD packet is 254. For a dynamic BFD session, the TTL value of a single-hop BFD packet is 255 and the TTL value of a multi-hop BFD packet is 253.

Format

peer-ip *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** } *ttl-value*

undo peer-ip *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** }

Parameters

Parameter	Description	Value
peer-ip	Specifies the peer IP address bound to the BFD session.	-
mask-length	Specifies the mask length of the IP address.	The value is an integer that ranges from 8 to 32.
single-hop	Indicates the single-hop BFD session.	-
multi-hop	Indicates the multi-hop BFD session.	-
ttl-value	Specifies the TTL value in BFD packets.	The value is an integer that ranges from 1 to 255.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the TTL value in BFD packets to enable the Huawei device to interwork with each other in different versions, with upgraded devices, and with non-Huawei devices.

Precautions

- The length of the IP segment address must match the mask. A long mask takes precedence over a short mask.
- The same IP segment addresses, masks, and TTL values of specified BFD session types cannot be configured simultaneously.
- When the IP network segment addresses and mask lengths are the same, the TTL value of a single-hop BFD session must be greater than the TTL value of a multi-hop BFD session.
- When a large number of BFD sessions are set up, updating the TTL value may take a long time. Therefore, when a smaller interval for configuring BFD sessions is used, the system displays a message indicating that the BFD session is being updated and you may try later.
- After the TTL value in multi-hop BFD packets is configured, you must configure the same peer IP address, mask length longer than the mask length for the TTL value in multi-hop BFD packets, and TTL value in single-hop BFD packets. This is because the TTL value in multi-hop BFD packets affects dynamic single-hop BFD sessions.

Example

Set the TTL value of single-hop BFD sessions to 254, the IP segment address to 10.10.10.0, and the mask length to 24.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] peer-ip 10.10.10.0 24 ttl single-hop 254
```

12.1.30 process-interface-status

Function

The **process-interface-status** command associates the BFD session status with the bound interface status.

The **undo process-interface-status** command restores the default setting.

By default, the BFD session status is not associated with the interface status. That is, the change of the BFD session status does not affect the interface status.

Format

process-interface-status [**reboot-no-impact**] [**protocol-down**]

undo process-interface-status [**reboot-no-impact**] [**protocol-down**]

Parameters

Parameter	Description	Value
reboot-no-impact	Disables the association between a multicast BFD session and interface during device startup.	-
protocol-down	After **protocol-down** is configured, when a BFD session detects a fault and enters the Down state, the protocol status of the associated interface becomes Down. In this case, the interface discards Layer 2 and Layer 3 packets but permits BFD packets.	-

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link protocol on an interface. The link protocol status of a trunk or VLANIF interface depends on the link protocol status of member interfaces.

To help BFD rapidly report the detection result to the application, a BFD status attribute is added to the interface management module of each interface. This attribute indicates the status of the BFD session that is bound to the interface. The system obtains the interface status based on the link status, protocol status, and BFD status on the interface, and then reports the interface status to the application.

Precautions

When configuring the **process-interface-status** command, pay attention to the following points:

- The **process-interface-status** command takes effect for only the single-hop BFD session that uses the default multicast address. The BFD session can be associated to an interface status.
- After the **trigger if-down delay** and **commit** commands are run in sequence, if BFD negotiation fails, the Down state is reported to the interface.
- If multiple BFD sessions are bound to an interface, you can use the **process-interface-status** command for only one BFD session. The change of only one BFD session changes the status of the bound interface.
- The BFD session does not report the BFD status to the bound interface immediately after the **commit** command is executed because the BFD session may not be set up or not Up. This prevents the BFD session from reporting an incorrect state to the interface. When the BFD status changes, the BFD session reports the BFD status to the interface to trigger the interface status change.
- If the **process-interface-status** command is saved in the configuration file, the BFD session for which the **process-interface-status** command is run notifies an interface that the BFD session becomes Down when the device is restarted. This is because the initial status of the interface is Down.
- Before the BFD session status is associated with the interface status, the BFD configurations on two ends must be correct and matched. If the BFD session status on the local interface is Down, check whether the BFD configuration on the peer end is correct or whether the BFD session is shut down.
- If the BFD session must be synchronized to an interface immediately, ensure that the BFD configurations on the two ends are the same and run the **shutdown (BFD session view)** and **undo shutdown (BFD session view)** commands on the BFD session. When the **undo shutdown (BFD session view)** command is executed for a BFD session, a BFD session detection timer is started. If the BFD session becomes Up through negotiation before the timer times out, the BFD session notifies an interface of the Up state. Otherwise, the BFD session considers the link faulty and notifies the interface of the Down state. The status of a BFD session and the status of an interface can be synchronized in real time.
- After a master/slave main control board switchover is performed, BFD notifies the associated interface to update the interface status during data smoothing based on the post-switchover BFD session status and diagnostic information. Specifically:
    a. If the BFD session is up, BFD notifies the interface to go up.
    b. If the BFD session is down, BFD differentiates between authentication and non-authentication scenarios.
        - BFD notifies the interface to go down in an authentication scenario.
        - In a non-authentication scenario, if the diagnostic word is "Receive AdminDown" and the receiving-admindown trigger if-down command is run before the switchover is performed, BFD notifies the interface to go down. If the diagnostic word is not "Receive AdminDown", BFD notifies the interface to go down.

Example

Associate the BFD session with an interface to which the BFD session is bound.

```
<HUAWEI> system-view
[HUAWEI] bfd test
[HUAWEI-bfd-session-test] process-interface-status
```

12.1.31 process-pst

Function

The **process-pst** command enables the system to modify the port status table (PST) when the BFD session status changes.

The **undo process-pst** command restores the default configuration.

By default, the device is disabled from modifying the PST.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

process-pst

undo process-pst

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a BFD session that is enabled to modify the PST detects a BFD session Down event, the system modifies the corresponding entry in the PST.

Precautions

- You can only run the **process-pst** command in the BFD session view that is bound to LDP LSP, Static LSP, or MPLS TE.
- When configuring static BFD-based LDP FRR, you must configure the **process-pst** command.
- When configuring static BFD for CR-LSP and static BFD for TE, you must configure the **process-pst** command.
- For applications in which a fault detected by BFD is not sensed through the PST, you do not need to configure the **process-pst** command.

- In IP FRR scenarios, the PST function is automatically enabled for dynamic BFD sessions but cannot be configured for IP static BFD sessions bound to the same interface.

Example

Enable the system to modify the PST when the BFD session status changes.

```
<HUAWEI> system-view
[HUAWEI] bfd 4ldplsp bind ldp-lsp peer-ip 10.10.9.9 nexthop 10.10.10.10
[HUAWEI-bfd-lsp-session-4ldplsp] process-pst
```

12.1.32 receiving-admindown trigger if-down

Function

The **receiving-admindown trigger if-down** command enables a local device to instruct the interface protocol to go down immediately after receiving an admindown packet.

The **undo receiving-admindown trigger if-down** command disables a local device from instructing the interface protocol to go down immediately after receiving an admindown packet.

By default, the local device is disabled from instructing the interface protocol to go down immediately after receiving an admindown packet.

Format

receiving-admindown trigger if-down

undo receiving-admindown trigger if-down

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

After the **process-interface-status** command associates a BFD session with the status of an interface bound to the BFD session, a local device does not instruct the interface protocol to go down after the device receives an admindown packet. To enable an immediate notification, run the **receiving-admindown trigger if-down** command.

Prerequisites

The BFD session status has been associated with the status of the interface bound to the BFD session using the **process-interface-status** command.

Precautions

- This command is supported in both BFD authentication and non-authentication scenarios.
- This command takes effect only on multicast BFD.
- If the **trigger if-down delay** command is run, the local device can instruct the interface protocol to go down immediately after receiving an admindown packet.

Example

Enable the local device to instruct the interface protocol to go down immediately after receiving an admindown packet.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet0/0/1
[HUAWEI-bfd-session-test] process-interface-status
[HUAWEI-bfd-session-test] receiving-admindown trigger if-down
```

12.1.33 reset bfd statistics

Function

The **reset bfd statistics** command clears statistics on received and sent packets of a BFD session.

Format

reset bfd statistics { **all** | **discriminator** *discr-value* }

Parameters

Parameter	Description	Value
all	Clears statistics on received and sent packets of all the BFD sessions.	-
discriminator *discr-value*	Clears statistics on received and sent packets of a BFD session with a specified discriminator.	The value is an integer that ranges from 1 to 16383.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset bfd statistics** command clears statistics on received and sent packets of a BFD session.

Precautions

The deleted statistics on received and sent packets of a BFD session cannot be restored. Exercise caution when you use this command.

Example

Clear statistics on packets of all BFD sessions.

```
<HUAWEI> reset bfd statistics all
```

12.1.34 session-damping disable

Function

The **session-damping disable** command disables BFD session flapping suppression.

The **undo session-damping disable** command enables BFD session flapping suppression.

By default, BFD session flapping suppression is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

session-damping disable

undo session-damping disable

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a BFD session frequently flaps, frequent link switchovers may occur, which results in packet loss. If multiple BFD sessions frequently flap on a device within a certain time, many device resources are consumed. When BFD session flapping suppression is enabled, the system establishes a more intelligent punishment mechanism for each BFD session, properly reducing the establishment of the BFD session. The system also periodically checks the flapping of all BFD sessions on the device, and more strictly suppresses the sessions with the most frequent flapping if necessary.

To allow the system to immediately start the next negotiation after a BFD session goes Down (excluding AdminDown), run the **session-damping disable** command to disable BFD session flapping suppression.

Precautions

When BFD session flapping suppression is enabled, the device can adjust the flapping suppression time based on the penalty value in addition to the value of the intelligent timer (**dampening timer-interval**). The penalty value is adjusted as follows:

1. When a BFD session goes Down each time, the penalty value of the BFD session increases by 20. The initial value is 0 and the maximum penalty value is 240.
2. When a BFD session keeps Up for 1s each time, the penalty value decreases by 1. The minimum penalty value is 0.
3. If the penalty value of a BFD session exceeds 45, the flapping suppression time is twice (that is, 2^1) the value of *maximum-milliseconds*. If the penalty value of a BFD session exceeds 90, the flapping suppression time is four times (that is, 2^2) the value of *maximum-milliseconds*, and so on. The *maximum-milliseconds* is configured using the **dampening timer-interval** command.
4. If a BFD session is suppressed by the intelligent timer, the penalty value is adjusted based on rules 1 and 2 and the BFD session does not enter the penalty suppression state. That is, rule 3 does not take effect. Rule 3 takes effect only when suppression by the intelligent timer ends.

When multiple BFD sessions exist on the device, the penalty value is adjusted considering Down events of all BFD sessions in a period of time.

The **session-damping disable** command takes effect for all types of BFD sessions.

Example

Disable BFD session flapping suppression.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] session-damping disable
```

12.1.35 shutdown (BFD session view)

Function

The **shutdown** command enables the BFD session to enter the AdminDown state.

The **undo shutdown** command enables a BFD session.

By default, a BFD session is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shutdown** command enables the BFD session to enter the AdminDown state.

Prerequisites

A BFD session has been created.

Precautions

- To modify the configuration of a BFD session, run the **shutdown** command to disable the BFD session. After the configuration is modified successfully, run the **undo shutdown** command to enable the BFD session again.
- To disable a BFD session without affecting the upper-layer application, run the **shutdown** command to enable the BFD session to enter the AdminDown state.
- If a BFD session is associated with an interface, the status of the BFD session is not reported to the interface when the BFD session is shut down.

Example

Stop the BFD session **atoc**.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] shutdown
```

12.1.36 snmp-agent bfd trap-interval

Function

The **snmp-agent bfd trap-interval** command sets the interval at which traps are sent.

The **undo snmp-agent bfd trap-interval** command restores the default interval at which traps are sent.

By default, the interval at which traps are sent is 120s.

Format

snmp-agent bfd trap-interval *interval*

undo snmp-agent bfd trap-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which traps are sent.	The value is an integer that ranges from 1 to 600, in seconds.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the BFD module is enabled with the SNMP alarm function, the NMS will receive BFD Up or Down messages. If the BFD session flaps, the NMS receives a large number of traps. In this case, BFD traps need to be suppressed. Run the **snmp-agent bfd trap-interval** command to set the interval at which traps are sent to prevent overflow of traps.

Prerequisites

Global BFD has been enabled using the **bfd** command.

Example

Set the interval at which traps are sent to 100s.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] snmp-agent bfd trap-interval 100
```

12.1.37 tos-exp

Function

The **tos-exp** command sets the priority of BFD packets.

The **undo tos-exp** command restores the default priority of BFD packets.

By default, the priority of BFD packets is 7.

Format

tos-exp *tos-value*

undo tos-exp

Parameters

Parameter	Description	Value
tos-value	Specifies the priority of BFD packets. A larger value indicates a higher priority of BFD packets.	The value is an integer that ranges from 0 to 7. The default value is 7.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can change the priority of BFD packets in the following scenarios:

- Detect whether packets with different priorities on a link can be forwarded.
- Ensure that BFD packets with a higher priority are forwarded first.

Precautions

When congestion occurs, the system first sends BFD packets with a higher priority.

Only the priority of BFD packets of the BFD session that is established using single-hop BFD, multi-hop BFD, and BFD Echo function can be changed. The priority of BFD packets of the BFD session that is established through automatically negotiated discriminators cannot be changed.

Example

Set the priority of BFD packets for the BFD session **atob** to 5.

```
<HUAWEI> system-view
[HUAWEI] bfd atob
[HUAWEI-bfd-session-atob] tos-exp 5
```

12.1.38 trigger if-down delay

Function

The **trigger if-down delay** command sets a delay time after which a local device instructs the interface protocol to go down after the device detects a BFD down event.

The **undo trigger if-down delay** command restores the default delay time.

The default delay time is 0s.

Format

trigger if-down delay *delay-time*

undo trigger if-down delay

Parameters

Parameter	Description	Value
delay-time	Sets the delay time, after which a local device instructs the interface protocol to go down after the device detects a BFD down event.	The value is an integer ranging from 1 to 10000, in seconds.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

If no link fault is detected and negotiation of a BFD session times out, the BFD session goes down. In this case, if the BFD session is associated with the status of the interface bound to the BFD session, the link protocol of the interface also goes down. To delay the associated notification, run the **trigger if-down delay** command. If the BFD session is still down after the delay time elapses, the link status of the associated interface goes down.

Prerequisites

The BFD session status has been associated with the status of the interface bound to the BFD session using the **process-interface-status** command.

Precautions

- This command takes effect on multicast BFD only in BFD non-authentication scenarios and is mutually exclusive with the **authentication-mode** command.
- If the **receiving-admindown trigger if-down** command is run, the local device can instruct the interface protocol to go down immediately after receiving an admindown packet.

Example

Set the delay time to 50s, after which a local device instructs the interface protocol to go down after the device detects a BFD down event.

```
<HUAWEI> system-view
[HUAWEI] bfd test bind peer-ip default-ip interface gigabitethernet0/0/1
[HUAWEI-bfd-session-test] process-interface-status
[HUAWEI-bfd-session-test] trigger if-down delay 50
```

12.1.39 unlimited-negotiate

Function

The **unlimited-negotiate** command enables unlimited negotiation for a multicast BFD session.

The **undo unlimited-negotiate** command disables unlimited negotiation for a multicast BFD session.

By default, unlimited negotiation is disabled for a multicast BFD session.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

unlimited-negotiate

undo unlimited-negotiate

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

If a multicast BFD session is bound to a Layer 3 interface to which the line protocol current state of the interface is Down, the status of the session is set to Down. You can run the **unlimited-negotiate** command to restart session negotiation. If the link is normal, the session can go Up through negotiation.

Example

Enable unlimited negotiation for a multicast BFD session.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd atob bind peer-ip default-ip interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-atob] unlimited-negotiate
```

12.1.40 wtr

Function

The **wtr** command sets the WTR time of a BFD session.

The **undo wtr** command restores the default WTR time of a BFD session.

By default, the WTR time is 0, indicating that the status change of a BFD session is reported immediately.

Format

wtr *wtr-value*

undo wtr

Parameters

Parameter	Description	Value
wtr-value	Specifies the WTR time of a BFD session.	The value is an integer that ranges from 0 to 60, in minutes. The default value is 0.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a BFD session flaps, the WTR time prevents frequent active/standby switchovers of the application associated with the BFD session.

Precautions

- If the WTR time is set, the system reports the BFD session Up event to the upper-layer application only after the WTR timer expires. Other status change events are reported immediately, which are not affected by the WTR time.
- Both ends must use the same WTR time. Otherwise, when the session status changes at one end, applications at both ends detect different BFD session status.
- If the WTR time is set and a BFD session goes Down within the WTR time, the **Down Count** value is recorded, but the **Last Up Time** and **Last Up Lasting Time** values are not recorded.

Example

Set the WTR time of a BFD session to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] bfd atoc
[HUAWEI-bfd-session-atoc] wtr 10
```

12.2 VRRP Configuration Commands

12.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.2.2 admin-vrrp vrid

Function

The **admin-vrrp vrid** command specifies an mVRRP group.

The **undo admin-vrrp vrid** command deletes the specified mVRRP group.

By default, no mVRRP group is configured.

Format

admin-vrrp vrid *virtual-router-id*

undo admin-vrrp vrid *virtual-router-id*

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the virtual router ID (VRID) of an mVRRP group.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An mVRRP group can be bound to VRRP groups. Once bound, the mVRRP group determines the master and backup status of the bound VRRP groups. mVRRP is used when multiple VRRP groups coexist, decreasing the number of VRRP Advertisement packets sent and minimize network bandwidth and system resource consumption.

NOTE

mVRRP provides the following functions:

- An mVRRP group used as the gateway can process both VRRP Advertisement packets and service packets.
- An mVRRP group that is not used as the gateway can only process VRRP Advertisement packets.

Precautions

An mVRRP group cannot be bound to another mVRRP group.

Example

Create VRRP group 1 on VLANIF 10 and configure it as an mVRRP group.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.1.1 24
[HUAWEI-Vlanif10] vrrp vrid 1 virtual-ip 10.1.1.111
[HUAWEI-Vlanif10] admin-vrrp vrid 1
```

Create VRRP group 1 on GE0/0/1 and configure it as an mVRRP group.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.111
[HUAWEI-GigabitEthernet0/0/1] admin-vrrp vrid 1
```

12.2.3 admin-vrrp6 vrid

Function

The **admin-vrrp6 vrid** command configures a VRRP6 group as an mVRRP6 group.

The **undo admin-vrrp6 vrid** command deletes the specified mVRRP6 group.

By default, no mVRRP6 group is configured.

Format

admin-vrrp6 vrid *virtual-router-id*

undo admin-vrrp6 vrid *virtual-router-id*

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the virtual router ID (VRID) of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An mVRRP6 group can be bound to common VRRP6 groups. Once bound, the mVRRP6 group determines the status of the bound VRRP6 groups based on the binding. mVRRP6 is used when multiple VRRP6 groups coexist, decreasing the number of VRRP Advertisement packets sent and minimizing network bandwidth consumption.

NOTE

mVRRP6 provides the following functions:

- An mVRRP6 group used as the gateway can process both VRRP6 Advertisement packets and service packets.
- An mVRRP6 group that is not used as the gateway can only process VRRP6 Advertisement packets.

Precautions

An mVRRP6 group cannot be bound to another mVRRP6 group.

Example

Create VRRP6 group 1 on VLANIF 10 and configure it as an mVRRP6 group.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] ipv6 address FC00::1 64
[HUAWEI-Vlanif10] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[HUAWEI-Vlanif10] admin-vrrp6 vrid 1
```

Create a VRRP6 group 1 on GE0/0/1 and configure it as an mVRRP6 group.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address FC00::1 64
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::1 link-local
[HUAWEI-GigabitEthernet0/0/1] admin-vrrp6 vrid 1
```

12.2.4 arp learning passive enable

Function

The **arp learning passive enable** command enables passive ARP that allows a backup device in a VRRP backup group to learn ARP entries when receiving an ARP request message sent to a virtual IP address.

The **undo arp learning passive enable** command disables passive ARP.

By default, passive ARP is disabled so that a backup device in a VRRP backup group does not learn ARP entries when receiving an ARP request message sent to a virtual IP address.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp learning passive enable

undo arp learning passive enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the master and backup devices in a VRRP backup group receive an ARP request message sent to a virtual IP address, only the master device learns ARP entries and responds to the sender with the virtual MAC address. If a link or device fault causes the VRRP backup group to perform a master/backup switchover, a backup device must learn ARP entries on the user side before taking over traffic. As a result, service traffic is interrupted for a short time.

After you run the **arp learning passive enable** command to enable passive ARP, a backup device in a VRRP backup group learns ARP entries when receiving an ARP request message sent to a virtual IP address. If a VRRP backup group performs a master/backup switchover, the new master device can take over traffic without needing to relearn ARP entries, ensuring service continuity.

Precautions

Passive ARP cannot be configured together with strict ARP entry learning.

The passive ARP function is invalid for a VRRP group created on a VLANIF interface.

Example

Enable passive ARP.

```
<HUAWEI> system-view
[HUAWEI] arp learning passive enable
```

12.2.5 clear admin-vrrp

Function

The **clear admin-vrrp** command deletes the binding of an mVRRP group on the subcard that is not functioning.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

clear admin-vrrp binding interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP group is configured.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An mVRRP group is often bound to VRRP groups on an interface. If the subcard on which the mVRRP group is configured fails or is not properly installed, the binding is retained and will take effect when the subcard begins working properly. You can run the **display vrrp binding admin-vrrp member-vrrp** command to check whether configuration recovery is successful.

If the binding is not required, run the **clear admin-vrrp** command to delete the binding.

Prerequisites

The mVRRP group has been configured and VRRP groups have been bound to the mVRRP group.

Precautions

If the binding between the mVRRP group and VRRP groups is deleted, the status of the mVRRP group no longer determines the status of the bound VRRP groups.

The binding deleted using the **clear admin-vrrp** command cannot be restored.

Ensure that the interface name is correct when executing the **clear admin-vrrp** command. This is because the system does not verify the interface name.

Example

Delete the binding of the mVRRP group on the specified subcard that is not properly installed.

```
<HUAWEI> system-view
[HUAWEI] clear admin-vrrp binding interface gigabitethernet 0/0/1 vrid 1
```

12.2.6 clear admin-vrrp6

Function

The **clear admin-vrrp6** command deletes the binding of an mVRRP6 group on the member switch that is not functioning in a stack.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

clear admin-vrrp6 binding interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP6 group is configured.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a stack, an mVRRP6 group is often bound to VRRP6 groups on an interface. If the member switch on which the mVRRP6 group is configured fails or is not properly installed, the binding is retained and will take effect when the member switch begins working properly. You can run the **display vrrp6 binding admin-vrrp6 member-vrrp** command to check whether configuration recovery is successful.

If the binding is not required, run the **clear admin-vrrp6** command to delete the binding.

Prerequisites

The mVRRP6 group has been configured and VRRP6 groups have been bound to the mVRRP6 group.

Precautions

If the binding between the mVRRP6 group and VRRP6 groups is deleted, the status of the mVRRP6 group no longer determines the status of the bound VRRP6 groups.

The binding deleted using the **clear admin-vrrp6** command cannot be restored.

Ensure that the interface name is correct when executing the **clear admin-vrrp6** command. This is because the system does not verify the interface name.

Example

Delete the binding of the mVRRP6 group on the specified member switch that is not properly installed.

```
<HUAWEI> system-view
[HUAWEI] clear admin-vrrp6 binding interface gigabitethernet 0/0/1 vrid 1
```

12.2.7 display vrrp

Function

The **display vrrp** command displays the status and configuration parameters of VRRP groups.

Format

display vrrp [**interface** *interface-type interface-number*] [*virtual-router-id*] [**brief**]

display vrrp { **interface** *interface-type interface-number* [*virtual-router-id*] | *virtual-router-id* } **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the status of all VRRP groups on the specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
virtual-router-id	Displays the status of a VRRP group with the specified VRID.	The VRID of the VRRP group must have been created.

Parameter	Description	Value
brief	Displays brief information about a specified VRRP group. If this parameter is not specified, detailed information about a VRRP group is displayed.	-
verbose	Displays detailed information about a VRRP group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp** command displays information about VRRP groups.

Example

Display information about all VRRP groups on the switch.

```
<HUAWEI> display vrrp
Vlanif100 | Virtual Router 1
    State : Master
    Virtual IP : 10.1.1.100
    Master IP : 10.1.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 20 s
    TimerRun : 2 s
    TimerConfig : 2 s
    Auth type : MD5   Auth key : ******
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track IF : Eth-Trunk0   Priority reduced : 60
    IF state : UP
    Track BFD : 69                    Priority reduced : 10
    BFD-session state : UP
    Create time : 2011-10-07 15:43:42 UTC-08:00
    Last change time : 2011-10-07 15:44:03 UTC-08:00
```

Table 12-9 Description of the **display vrrp** command output

Item	Description
Vlanif100 | Virtual Router 1	Interface where the VRRP group is configured and VRID of the VRRP group.
State	VRRP status of the device: ● Master: The device functions as the master in the VRRP group. ● Backup: The device functions as the backup in the VRRP group. ● Initialize: All VRRP groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP group status is switched to Initialize.
Virtual IP	Virtual IP address of a VRRP group. To configure a virtual IP address for a VRRP group, run the **vrrp vrid virtual-ip** command.
Master IP	Primary IP address of the interface configured with the VRRP group on the master.
PriorityRun	Priority of the switch when the VRRP group runs. If the switch is the IP address owner in a VRRP group, the running priority of the switch in the group is displayed as **255**.
PriorityConfig	Priority configured for the switch using the **vrrp vrid priority** command. If the switch is the IP address owner and this value is not configured, the default priority 100 but not 255 is displayed.
MasterPriority	Priority of the master in the VRRP group. If the switch is the IP address owner in a VRRP group, the priority of the switch in the group is displayed as **255**.
Preempt	Preemption mode: ● YES: preemption ● NO: no preemption To disable the preemption mode, run the **vrrp vrid preempt-mode disable** command.
Delay Time	Preemption delay, in seconds. To set the preemption delay, run the **vrrp vrid preempt-mode timer delay** command.
TimerRun	Interval at which the master in the VRRP group sends VRRP Advertisement packets, in seconds.

Item	Description
TimerConfig	Configured interval at which the master in the VRRP group sends VRRP Advertisement packets, in seconds. To set the interval at which the master in the VRRP group sends VRRP Advertisement packets, run the **vrrp vrid timer advertise** command.
Auth type	VRRP Advertisement packet authentication mode: ● NONE: non-authentication ● SIMPLE: simple authentication ● MD5: MD5 authentication To set an authentication mode, run the **vrrp vrid authentication-mode** command. VRRPv3 does not support authentication.
Auth key	Authentication key. If authentication is configured, ****** is displayed. If no authentication is configured, this field is not displayed.
Virtual MAC	Virtual MAC address of the VRRP group.
Check TTL	Whether the TTL value of a VRRP Advertisement packet is checked: ● YES: The TTL value of a VRRP Advertisement packet is checked. ● NO: The TTL value of a VRRP Advertisement packet is not checked. To configure the switch to check the TTL value in a VRRP Advertisement packet, run the **vrrp un-check ttl** command.
Config type	VRRP group type: ● normal-vrrp: common VRRP group ● admin-vrrp: mVRRP group ● member-vrrp: service VRRP group
Backup-forward	Whether the backup is enabled to forward traffic: ● enabled ● disabled To configure the backup to forward traffic, run the **vrrp vrid backup-forward** command.
Track IF	Name of a monitored interface when the interface monitoring function of VRRP backup group is enabled. To configure the parameter, run the **vrrp vrid track interface** command.

Item	Description
Priority reduced or Priority increased	Value to which the device decreases or increases a priority if the tracked interface, BFD session, or EFM session goes Down. When the interface, BFD session, or EFM session tracked by the VRRP backup group goes Down, and the priority of the VRRP backup group is configured to increase, **Priorityincreased** is displayed. To configure the parameter, run the **vrrp vrid track bfd-session** or **vrrp vrid track interface** command.
IF state	Status of the interface monitored by VRRP: ● UP ● DOWN ● REMOVE
Track BFD	Local discriminator or name of the BFD session associated with the VRRP group. This field is displayed when only the BFD session is associated with the VRRP group. To configure the BFD session associate with the VRRP group, run the **vrrp vrid track bfd-session** command.
BFD-session state	Status of the BFD session associated with the VRRP group: ● UP: A BFD session is in Up state. ● DOWN: A BFD session is in Down state. ● AdminDown: A BFD session is in AdminDown state.
Create time	Time when the VRRP group was created.
Last change time	Last time the VRRP group status changed.

Display brief information about all VRRP groups on the switch.

```
<HUAWEI> display vrrp brief
Total:1     Master:0     Backup:0     Non-active:1
VRID  State        Interface                Type     Virtual IP
----------------------------------------------------------------
1     Initialize   Vlanif23                 Normal   10.1.1.100
```

Table 12-10 Description of the **display vrrp brief** command output

Item	Description
VRID	VRID of the VRRP group.

Item	Description
State	VRRP status of the switch: ● Master: The switch functions as the master in the VRRP group. ● Backup: The switch functions as the backup in the VRRP group. ● Initialize: All VRRP groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP group status changes to Initialize.
Interface	Interface configured with the VRRP group.
Type	Type of a VRRP group: ● normal-vrrp: common VRRP group ● admin-vrrp: mVRRP group ● member-vrrp: service VRRP group
Virtual IP	Virtual IP address of the VRRP group.
Total	Number of VRRP groups.
Master	Number of VRRP groups in Master state.
Backup	Number of VRRP groups in Backup state.
Non-active	Number of VRRP groups in Non-active state.

12.2.8 display vrrp admin-vrrp

Function

The **display vrrp admin-vrrp** command displays the status and configuration of all mVRRP groups.

Format

display vrrp admin-vrrp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can view basic information about an mVRRP group, including the interface where the mVRRP group is configured, and the VRID and status of the mVRRP group.

Example

Display the status and configuration of all mVRRP groups on the device.

```
<HUAWEI> display vrrp admin-vrrp
Admin-vrrp number: 1
Interface: Vlanif10,  admin-vrrp vrid: 1, state: Master
```

Table 12-11 Description of the **display vrrp admin-vrrp** command output

Item	Description
Admin-vrrp number	Number of mVRRP groups.
Interface	Name and number of the interface where the mVRRP group is configured.
admin-vrrp vrid	VRID of the mVRRP group.
state	Status of the mVRRP group: ● Master ● Backup ● Initialize

12.2.9 display vrrp binding admin-vrrp

Function

The **display vrrp binding admin-vrrp** command displays the binding of an mVRRP group, including member VRRP groups and interfaces where member VRRP groups are configured.

Format

display vrrp binding admin-vrrp [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP group is configured. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vrrp binding admin-vrrp** command to view the binding of an mVRRP group.

Example

Display the binding of an mVRRP group.

```
<HUAWEI> display vrrp binding admin-vrrp
Interface: Vlanif10,  admin-vrrp vrid: 1, state:Master
  Member-vrrp number: 3
    Interface: Vlanif11, vrid: 1, state: Master
    Interface: Vlanif12, vrid: 2, state: Master
    Interface: Vlanif13, vrid: 3, state: Master
```

Table 12-12 Description of the **display vrrp binding admin-vrrp** command output

Item	Description
Interface	Interface configured with the mVRRP group.
admin-vrrp vrid	VRID of the mVRRP group.

Item	Description
state	Status of the mVRRP group: - Master - Backup - Initialize
Member-vrrp number	Number of member VRRP groups bound to the mVRRP group.
Interface	Interface where the member VRRP group bound to the mVRRP group is configured.
vrid	VRID of the member VRRP group bound to the mVRRP group.
state	Status of the member VRRP group bound to the mVRRP group: - Master - Backup - Initialize

12.2.10 display vrrp binding admin-vrrp member-vrrp

Function

The **display vrrp binding admin-vrrp member-vrrp** command displays information about the binding between an mVRRP group and member VRRP groups.

Format

display vrrp binding admin-vrrp [**interface** *interface-type1 interface-number1*] [**vrid** *virtual-router-id1*] **member-vrrp** [**interface** *interface-type2 interface-number2*] [**vrid** *virtual-router-id2*]

Parameters

Parameter	Description	Value
interface *interface-type1 interface-number1*	Specifies the type and number of an interface configured with an mVRRP group. - *interface-type1* specifies the interface type. - *interface-number1* specifies the interface number.	-

Parameter	Description	Value
vrid *virtual-router-id1*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.
interface *interface-type2 interface-number2*	Specifies the type and number of an interface configured with a member VRRP group. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-
vrid *virtual-router-id2*	Specifies the VRID of a member VRRP group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display vrrp binding admin-vrrp member-vrrp** command to view information about the binding between an mVRRP group and member VRRP groups.

Example

Display information about the binding between an mVRRP group and member VRRP groups.

```
<HUAWEI> display vrrp binding admin-vrrp member-vrrp
Interface: Vlanif11,  admin-vrrp vrid: 1, state: Master
  Member-vrrp number: 3
    Interface: Vlanif10, vrid: 1, state: Master
    Interface: Vlanif10, vrid: 2, state: Master
    Interface: Vlanif12, vrid: 3, state: Master
```

Table 12-13 Description of the **display vrrp binding admin-vrrp member-vrrp** command output

Item	Description
Interface	Interface configured with the mVRRP group.
admin-vrrp vrid	VRID of the mVRRP group.
state	Status of the mVRRP group: ● Master ● Backup ● Initialize
Member-vrrp number	Number of member VRRP groups bound to the mVRRP group.
Interface	Interface where the member VRRP group bound to the mVRRP group is configured.
vrid	VRID of the member VRRP group bound to the mVRRP group.
state	Status of the member VRRP group bound to the mVRRP group: ● Master ● Backup ● Initialize

12.2.11 display vrrp protocol-information

Function

The **display vrrp protocol-information** command displays VRRP information.

Format

display vrrp protocol-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vrrp protocol-information** command to view VRRP information.

Example

Display VRRP information.

```
<HUAWEI> display vrrp protocol-information
 VRRP protocol information is shown as below:
    VRRP protocol version : V2
    Send advertisement packet mode : send v2 only
```

Table 12-14 Description of the **display vrrp protocol-information** command output

Item	Description
VRRP protocol version	VRRP version number: ● V2 ● V3 To configure a VRRP version number, run the **vrrp version** command.
Send advertisement packet mode	Mode in which VRRP Advertisement packets are sent: ● send v2 only: Only VRRPv2 Advertisement packets are sent. ● send v3 only: Only VRRPv3 Advertisement packets are sent. It is displayed only when VRRPv3 is used. ● send v2v3 both: VRRPv2 and VRRPv3 Advertisement packets are sent. It is displayed only when VRRPv3 is used. To configure the mode in which VRRP Advertisement packets are sent, run the **vrrp vrid version-3 send-packet-mode** command in the interface view or run the **vrrp version-3 send-packet-mode** command in the system view.

12.2.12 display vrrp state-change interface vrid

Function

The **display vrrp state-change interface vrid** command displays status changes of a specified VRRP group. This command can display a maximum of 10 of the latest status changes of a VRRP group.

Format

display vrrp state-change interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface where status changes of a VRRP group are displayed. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The VRID of the VRRP group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the VRRP status becomes abnormal, run the **display vrrp state-change interface vrid** command to view the last 10 status changes of the VRRP group, including the time at which the VRRP group status changed, the VRRP group status before and after the change, and the cause of the VRRP group status change. The command output helps you locate faults.

Example

Display status changes of VRRP group 1 on VLANIF 100.

```
<HUAWEI> display vrrp state-change interface vlanif 100 vrid 1
 Time                    SourceState   DestState     Reason
 ---------------------------------------------------------------
 2012-01-27 15:29:45       Backup        Master        Protocol timer expired
 2012-01-27 15:29:42       Initialize    Backup        Interface UP
```

Table 12-15 Description of the **display vrrp state-change interface vrid** command output

Item	Description
Time	Time when the VRRP group status changed.
SourceState	VRRP group status before the change: ● Master ● Backup ● Initialize
DestState	VRRP group status after the change: ● Master ● Backup ● Initialize
Reason	Cause of the VRRP status change: ● Admin-vrrp drove ● BFD configure deleted ● CFM session down ● CFM session up ● EFM configure deleted ● EFM session down ● EFM session up ● Interface up ● Interface down ● Ignore interface down ● Link BFD session down ● Link BFD session up ● Link BFD session deleted ● Link BFD down-number changed ● Peer BFD session down ● Priority calculation ● Protocol timer expired ● Track interface ● Track BFD session

12.2.13 display vrrp statistics

Function

The **display vrrp statistics** command displays statistics about sent and received packets of VRRP groups.

Format

display vrrp [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about sent and received packets of all VRRP groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are displayed.	-
virtual-router-id	Displays statistics about sent and received packets of a specified VRRP group. If this parameter is not specified, statistics about sent and received packets of all VRRP groups on the device or a specified interface are displayed.	The VRID of the VRRP group must have been created.
statistics	Displays statistics about sent and received packets of a VRRP group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp statistics** command displays information about sent and received packets of VRRP groups.

Example

Display statistics about sent and received packets of VRRP group 1 on VLANIF100.

```
<HUAWEI> display vrrp interface vlanif 100 1 statistics
  Vlanif 100 | Virtual Router 1
                              Transited to master : 1
                              Transited to backup : 1
                          Transited to initialize : 0
                          Received advertisements : 0
                              Sent advertisements : 1000
                    Advertisement interval errors : 0
                   Failed to authentication check : 0
                           Received ip ttl errors : 0
              Received packets with priority zero : 0
                  Sent packets with priority zero : 0
                    Received invalid type packets : 0
         Received unmatched address list packets : 0
             Unknown authentication type packets : 0
                  Mismatched authentication type : 0
                              Packet length errors : 0
       Discarded packets since track admin-vrrp : 0
                       Received attacking packets : 0
                        Received selfsend packets : 0
```

Display statistics about all VRRP Advertisement packets on the device.

```
<HUAWEI> display vrrp statistics
  Checksum errors : 0
   Version errors : 0
      Vrid errors : 0
     Other errors : 0

  Vlanif 100 | Virtual Router 1
                              Transited to master : 1
                              Transited to backup : 1
                          Transited to initialize : 0
                          Received advertisements : 0
                              Sent advertisements : 1000
                    Advertisement interval errors : 0
                   Failed to authentication check : 0
                           Received ip ttl errors : 0
              Received packets with priority zero : 0
                  Sent packets with priority zero : 0
                    Received invalid type packets : 0
         Received unmatched address list packets : 0
             Unknown authentication type packets : 0
                  Mismatched authentication type : 0
                              Packet length errors : 0
       Discarded packets since track admin-vrrp : 0
                       Received attacking packets : 0
                        Received selfsend packets : 0
```

Table 12-16 Description of the display vrrp statistics command output

Item	Description
Checksum errors	CRC error count.
Version errors	Version error count.
Vrid errors	Number of VRID errors.
Other errors	Number of other errors.
Vlanif 100 | Virtual Router 1	Interface where the VRRP group is configured and VRID of the VRRP group.
Transited to master	Number of times the switch transitions to the Master state.
Transited to backup	Number of times the switch transitions to the Backup state.
Transited to initialize	Number of times the switch transitions to the Initialize state.
Received advertisements	Number of received VRRP Advertisement packets.
Sent advertisements	Number of sent VRRP Advertisement packets.
Advertisement interval errors	Number of times VRRP Advertisement packets are sent at an incorrect interval.
Failed to authentication check	Number of authentication failures.
Received ip ttl errors	Number of packets with TTL errors.
Received packets with priority zero	Number of received VRRP Advertisement packets with the priority of 0.
Sent packets with priority zero	Number of sent VRRP Advertisement packets with the priority of 0.
Received invalid type packets	Number of received VRRP Advertisement packets of invalid type.
Received unmatched address list packets	Number of packets with incorrect virtual IP address lists.
Unknown authentication type packets	Number of packets with an unknown authentication mode.
Mismatched authentication type	Number of packets with a non-matched authentication mode.
Packet length errors	Number of packets with incorrect length.
Discarded packets since track admin-vrrp	Number of received packets that are discarded after a VRRP group is bound to a management VRRP (mVRRP) group.

Item	Description
Received attacking packets	Number of received attack packets.
Received selfsend packets	Number of received packets sent by the switch.

12.2.14 display vrrp track bfd gratuitous-arp information

Function

The **display vrrp track bfd gratuitous-arp information** command displays information when a sub-interface is enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

Format

display vrrp track bfd gratuitous-arp information

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp track bfd gratuitous-arp information** command displays information when a sub-interface is enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

Example

Display information when a sub-interface is enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

```
<HUAWEI> display vrrp track bfd gratuitous-arp information
--------------------------------------------------------------------------------
Interface                     Vrid      BFD-session Name        Status
```

```
--------------------------------------------------------------------------------
GigabitEthernet0/0/19.1          32        atob                  Active
--------------------------------------------------------------------------------
Total:1            Active:1            InActive:0
```

Table 12-17 Description of the **display vrrp track bfd gratuitous-arp information** command output

Item	Description
Interface	Interface configured with the VRRP group.
Vrid	VRID of the VRRP group.
BFD-session Name	Name of a BFD session.
Status	Status of the BFD session.
Total	Total number of peer BFD sessions.
Active	Number of BFD sessions in active state.
InActive	Number of BFD sessions in inactive state.

12.2.15 display vrrp6

Function

The **display vrrp6** command displays the status and configuration parameters of VRRP6 groups.

Format

display vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] [**brief**]

display vrrp6 { **interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **vrid** *virtual-router-id* } **verbose**

Parameters

Parameter	Description	Description
interface *interface-type interface-number*	Displays the status of all VRRP6 groups on the specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If this parameter is not specified, information about all VRRP6 groups is displayed.	-
vrid *virtual-router-id*	Displays the status of a VRRP6 group with the specified VRID.	The VRID of the VRRP6 group must have been created.
brief	Displays brief information about a specified VRRP6 group.	-
verbose	Displays detailed information about a specified VRRP6 group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and configuration of all VRRP6 groups based on networking, including interfaces where mVRRP6 groups are configured, and VRIDs and statuses of VRRP6 groups.

Example

Display information about all VRRP6 groups on the switch with VRID 4.

```
<HUAWEI> display vrrp6 vrid 4
Vlanif100 | Virtual Router 4
    State            : Master
    Virtual IP       : FE80::1:2
    Master IP : FE80::218:82FF:FED3:2AF1
```

```
  PriorityRun      : 200
  PriorityConfig   : 200
  MasterPriority   : 200
  Preempt          : YES                   Delay Time : 0 s
  TimerRun         : 100 cs
  TimerConfig      : 100 cs
  Virtual Mac      : 0000-5e00-0101
  Check hop limit  : YES
  Config type      : normal-vrrp
  Backup-forward   : disabled
  Create time      : 2012-05-22 17:40:56 UTC-08:00
  Last change time : 2012-05-22 17:41:03 UTC-08:00
```

Table 12-18 Description of the display vrrp6 command output

Item	Description
Vlanif100 | Virtual Router 4	Interface where the VRRP6 group is configured and VRID of the VRRP6 group.
State	VRRP6 status of the device: ● Master: The device functions as the master in the VRRP6 group. ● Backup: The device functions as the backup in the VRRP6 group. ● Initialize: All VRRP6 groups begin in Initialize state. When the status of an interface is Down or administratively Down, the VRRP6 group status changes to Initialize.
Virtual IP	Virtual IP address of the VRRP6 group. To configure a virtual IP address for a VRRP6 group, run the **vrrp6 vrid virtual-ip** command.
Master IP	Primary IP address of the interface configured with the VRRP6 group on the master.
PriorityRun	Priority of the switch when the VRRP6 group runs. If the switch is the IP address owner in a VRRP6 group, the running priority of the switch in the group is displayed as **255**.
PriorityConfig	Priority configured for the switch using the **vrrp6 vrid priority** command. If the switch is the IP address owner, the default priority 100 but not 255 is displayed.
MasterPriority	Priority of the master in the VRRP6 group. If the switch is the IP address owner in a VRRP6 group, the priority of the switch in the group is displayed as **255**.
Preempt	Preemption mode: ● YES: preemption ● NO: no preemption To disable the preemption mode, run the **vrrp6 vrid preempt-mode disable** command.

Item	Description
Delay Time	Preemption delay, in seconds. To set the preemption delay, run the **vrrp6 vrid preempt-mode timer delay** command.
TimerRun	Interval at which the master in the VRRP6 group sends VRRP Advertisement packets, in centiseconds.
TimerConfig	Configured interval at which the master in the VRRP6 group sends VRRP6 Advertisement packets, in centiseconds. To set the interval at which the master in the VRRP6 group sends VRRP6 Advertisement packets, run the **vrrp6 vrid timer advertise** command.
Virtual Mac	Virtual MAC address of the VRRP6 group.
Check hop limit	Whether the TTL value of a VRRP6 Advertisement packet is checked: ● YES: The TTL value of a VRRP6 Advertisement packet is checked. ● NO: The TTL value of a VRRP6 Advertisement packet is not checked. To configure the device to check the TTL value in a VRRP6 Advertisement packet, run the **vrrp6 un-check hop-limit** command.
Config type	Type of a VRRP6 group: ● normal-vrrp: common VRRP6 group ● admin-vrrp: mVRRP6 group ● member-vrrp: service VRRP6 group
Backup-forward	Whether the backup is enabled to forward traffic: ● enabled ● disabled
Create time	Time when the VRRP6 group was created.
Last change time	Last time the VRRP6 group status changed.

Display brief information about all VRRP6 groups on the device.

```
<HUAWEI> display vrrp6 brief
Total:2     Master:2     Backup:0     Non-active:0
VRID  State        Interface                Type     Virtual IP
----------------------------------------------------------------
1     Master       Vlanif66                 Normal   FE80::1
2     Master       Vlanif67                 Normal   FE80::1:3
```

Table 12-19 Description of the display vrrp6 brief command output

Item	Description
VRID	VRID of the VRRP6 group.
State	VRRP6 status of the switch: ● Master: The device functions as the master in the VRRP6 group. ● Backup: The device functions as the backup in the VRRP6 group. ● Initialize: All VRRP6 groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP6 group status is switched to Initialize.
Interface	Interface configured with the VRRP6 group.
Type	Type of a VRRP6 group: ● normal-vrrp: common VRRP6 group ● admin-vrrp: mVRRP6 group ● member-vrrp: service VRRP6 group
Virtual IP	Virtual IP address of the VRRP6 group.
Total	Number of VRRP6 groups.
Master	Number of VRRP6 groups in Master state.
Backup	Number of VRRP6 groups in Backup state.
Non-active	Number of VRRP6 groups in Non-active state.

12.2.16 display vrrp6 admin-vrrp6

Function

The **display vrrp6 admin-vrrp6** command displays the status and configuration of all mVRRP6 groups.

Format

display vrrp6 admin-vrrp6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and configuration of all mVRRP6 groups, including interfaces where mVRRP6 groups are configured, and VRIDs and statuses of the mVRRP6 groups.

Example

Display the status and configuration of all mVRRP6 groups on the device.

```
<HUAWEI> display vrrp6 admin-vrrp6
  Admin-vrrp6 number: 1
Interface: Vlanif100,  admin-vrrp6 vrid: 1, state: Master
```

Table 12-20 Description of the **display vrrp6 admin-vrrp6** command output

Item	Description
Admin-vrrp6 number	Number of mVRRP6 groups.
Interface	Interface configured with the mVRRP6 group.
admin-vrrp6 vrid	VRID of the mVRRP6 group.
state	Status of the mVRRP6 group: ● Master ● Backup ● Initialize

12.2.17 display vrrp6 binding admin-vrrp6

Function

The **display vrrp6 binding admin-vrrp6** command displays the binding of an mVRRP6 group and its member VRRP6 groups.

Format

display vrrp6 binding admin-vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where an mVRRP6 group is configured.	-
vrid *virtual-router-id*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the **interface** *interface-type interface-number* parameter is not specified, the **display vrrp6 binding admin-vrrp6** command displays the binding of mVRRP6 groups on all interfaces of the device.

Example

Display the binding of mVRRP6 groups on all interfaces.

```
<HUAWEI> display vrrp6 binding admin-vrrp6
Interface: Vlanif100,  admin-vrrp6 vrid: 1, state:Master
  Member-vrrp6 number: 1
    Interface: Vlanif200, vrid: 2, state: Master
```

Table 12-21 Description of the **display vrrp6 binding admin-vrrp6** command output

Item	Description
Interface	Interface configured with the mVRRP6 group.
admin-vrrp6 vrid	VRID of the mVRRP6 group.
state	Status of the mVRRP6 group: ● Master ● Backup ● Initialize
Member-vrrp6 number	Number of member VRRP6 groups bound to the mVRRP6 group.
Interface	Interface configured with a member VRRP6 group that is bound to the mVRRP6 group.

Item	Description
vrid	VRID of a member VRRP6 group bound to the mVRRP6 group.
state	Status of a member VRRP6 group bound to the mVRRP6 group: ● Master ● Backup ● Initialize

12.2.18 display vrrp6 binding admin-vrrp6 member-vrrp

Function

The **display vrrp6 binding admin-vrrp6 member-vrrp** command displays information about the binding between an mVRRP6 group and member VRRP6 groups.

Format

display vrrp6 binding admin-vrrp6 [**interface** *interface-type1 interface-number1*] [**vrid** *virtual-router-id1*] **member-vrrp** [**interface** *interface-type2 interface-number2*] [**vrid** *virtual-router-id2*]

Parameters

Parameter	Description	Value
interface *interface-type1 interface-number1*	Specifies the type and number of an interface configured with an mVRRP6 group.	-
vrid *virtual-router-id1*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.
interface *interface-type2 interface-number2*	Specifies the type and number of an interface configured with a member VRRP6 group.	-
vrid *virtual-router-id2*	Specifies the VRID of a member VRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp6 binding admin-vrrp6 member-vrrp** command displays the bindings between mVRRP6 backup groups and member VRRP6 backup groups on the network as required.

- If *interface-type1 interface-number1* is merely specified in the command, the command output displays all the bindings between mVRRP6 backup groups and member VRRP6 backup groups on the specified interface.
- If the command is specified with only *virtual-router-id1*, the command output displays the bindings between the specified mVRRP6 backup group and member VRRP6 backup groups.
- If the command is specified with only *interface-type1 interface-number1* and *virtual-router-id1*, the command output displays the bindings between the specified mVRRP6 backup group on the specified interface and member VRRP6 backup groups.
- If the command is only specified with *interface-type2 interface-number2*, the command output displays the bindings between member VRRP6 backup groups on the specified interface and mVRRP6 backup groups.
- If the command is specified with only *virtual-router-id2*, the command output displays the bindings between the specified member VRRP6 backup group and mVRRP6 backup groups.
- If the command is specified with only *interface-type2 interface-number2* and *virtual-router-id2*, the command output displays the bindings between the specified member VRRP6 backup group on the specified interface and mVRRP6 backup groups, and information about the mVRRP6 backup groups.

Example

Display information about the binding between an mVRRP6 group and member VRRP6 groups.

```
<HUAWEI> display vrrp6 binding admin-vrrp6 member-vrrp
Interface: Vlanif100, admin-vrrp6 vrid: 1, state: Master
  Member-vrrp number: 2
    Interface: Vlanif101, vrid: 2, state: Master
    Interface: Vlanif102, vrid: 3, state: Master
```

Display information about the binding between mVRRP6 group 1 and member VRRP6 groups on VLANIF 10.

```
<HUAWEI> display vrrp6 binding admin-vrrp6 interface vlanif 10 vrid 1 member-vrrp
Interface: Vlanif10,  admin-vrrp6 vrid: 1, state:Master
  Member-vrrp number: 3
          Interface: Vlanif100, vrrp6 vrid: 1, state: Master
          Interface: Vlanif101, vrrp6 vrid: 2, state: Master
          Interface: Vlanif102, vrrp6 vrid: 3, state: Master
```

Table 12-22 Description of the **display vrrp6 binding admin-vrrp6 member-vrrp** command output

Item	Description
Interface	Interface configured with the mVRRP6 group.
admin-vrrp6 vrid	VRID of the mVRRP6 group.
state	Status of the mVRRP6 group: - Master - Backup - Initialize
Member-vrrp number	Number of member VRRP6 groups bound to the mVRRP6 group.
Interface	Interface configured with the member VRRP6 group.
vrrp6 vrid	VRID of the member VRRP6 group.
state	Status of the member VRRP6 group.

12.2.19 display vrrp6 state-change interface vrid

Function

The **display vrrp6 state-change interface vrid** command displays status changes of a specified VRRP6 group. This command can display a maximum of the latest 10 status changes of a VRRP6 group.

Format

display vrrp6 state-change interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface where status changes of a VRRP6 group are displayed.	-
virtual-router-id	Specifies the VRID of a VRRP6 group.	The VRID of the VRRP6 group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the VRRP6 status becomes abnormal, run the **display vrrp6 state-change interface vrid** command to view the latest 10 status changes of the VRRP6 group. The command output includes the time when the VRRP6 group status changed, VRRP6 group status before and after each change, and causes of the status changes. The command output helps you locate faults.

Example

Display status changes of VRRP6 group 1 on VLANIF 100.

```
<HUAWEI> display vrrp6 state-change interface vlanif 100 vrid 1
Time                       SourceState  DestState   Reason
-------------------------------------------------------------------------------
2012-05-19 20:36:44            Initialize   Backup      interface up
2012-05-19 20:37:07            Backup       Master      protocol timer expired
```

Table 12-23 Description of the **display vrrp6 state-change interface vrid** command output

Item	Description
Time	Time when the VRRP6 status changed.
SourceState	Status before the change: ● Master ● Backup ● Initialize
DestState	Status after the change: ● Master ● Backup ● Initialize

Item	Description
Reason	Reason of the change in the status of the VRRP6 backup group: ● Admin-vrrp drove ● BFD configure deleted ● Interface up ● Interface down ● Link BFD session down ● Link BFD session up ● Link BFD session deleted ● Peer BFD session down ● Priority calculation ● Protocol timer expired ● Track interface ● Track BFD session

12.2.20 display vrrp6 statistics

Function

The **display vrrp6 statistics** command displays statistics about sent and received packets of VRRP6 groups.

Format

display vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about sent and received packets of all VRRP6 groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the switch are displayed.	-
vrid *virtual-router-id*	Displays statistics about sent and received packets of a specified VRRP6 group. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups on the switch or a specified interface are displayed.	The VRID of the VRRP6 group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp6 statistics** command displays information about sent and received packets of VRRP6 groups.

Example

Display statistics about all VRRP6 Advertisement packets on the switch.

```
<HUAWEI> display vrrp6 statistics
  Checksum errors : 0
   Version errors : 0
      Vrid errors : 0
     Other errors : 0

  Vlanif100 | Virtual Router 1
                          Transited to master : 1
                          Transited to backup : 1
                      Transited to initialize : 0
                      Received advertisements : 0
                          Sent advertisements : 1000
                Advertisement interval errors : 0
               Failed to authentication check : 0
                       Received ip ttl errors : 0
           Received packets with priority zero : 0
               Sent packets with priority zero : 0
                 Received invalid type packets : 0
        Received unmatched address list packets : 0
            Unknown authentication type packets : 0
                 Mismatched authentication type : 0
                           Packet length errors : 0
     Discarded packets since track admin-vrrp : 0
                    Received attacking packets : 0
                     Received selfsend packets : 0
```

Table 12-24 Description of the **display vrrp6 statistics** command output

Item	Description
Checksum errors	CRC error count.
Version errors	Version error count.
Vrid errors	Number of VRID errors.
Other errors	Number of other errors.
Vlanif100 | Virtual Router 1	Interface where the VRRP6 group is configured and VRID of the VRRP6 group.
Transited to master	Number of times the switch transitions to the Master state.
Transited to backup	Number of times the switch transitions to the Backup state.
Transited to initialize	Number of times the switch transitions to the Initialize state.
Received advertisements	Number of received VRRP Advertisement packets.
Sent advertisements	Number of sent VRRP Advertisement packets.
Advertisement interval errors	Number of times VRRP Advertisement packets are sent at an incorrect interval.
Failed to authentication check	Number of authentication failures.
Received ip ttl errors	Number of packets with TTL errors.

Item	Description
Received packets with priority zero	Number of received VRRP Advertisement packets with the priority of 0.
Sent packets with priority zero	Number of sent VRRP Advertisement packets with the priority of 0.
Received invalid type packets	Number of received VRRP6 Advertisement packets of invalid type.
Received unmatched address list packets	Number of packets with incorrect virtual IPv6 address lists.
Unknown authentication type packets	Number of invalid authentication packets.
Mismatched authentication type	Number of packets with mismatching authentication types.
Packet length errors	Number of packets with incorrect length.
Discarded packets since track admin-vrrp	Number of received packets that are discarded after a VRRP6 group is bound to a management VRRP6 (mVRRP6) group.
Received attacking packets	Number of received attack packets.
Received selfsend packets	Number of received packets sent by the switch.

12.2.21 reset vrrp statistics

Function

The **reset vrrp statistics** command clears statistics about received and sent packets of VRRP groups.

Format

reset vrrp [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about sent and received packets of all VRRP groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are cleared.	-
vrid *virtual-router-id*	Clears statistics about sent and received packets of a specified VRRP group. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are cleared.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about VRRP Advertisement packets, run the **reset vrrp statistics** command to clear existing statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when executing the **reset vrrp statistics** command.

Example

Clear statistics about sent and received packets of VRRP group 1 on VLANIF100.

```
<HUAWEI> reset vrrp interface vlanif 100 vrid 1 statistics
```

Clear statistics about all the packets of VRRP group 1.

```
<HUAWEI> reset vrrp vrid 1 statistics
```

Clear statistics about packets of all VRRP groups on the switch.

```
<HUAWEI> reset vrrp statistics
```

12.2.22 reset vrrp6 statistics

Function

The **reset vrrp6 statistics** command clears statistics about received and sent packets of VRRP6 groups.

Format

reset vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about sent and received packets of all VRRP6 groups on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the device are cleared.	-

Parameter	Description	Value
vrid *virtual-router-id*	Clears statistics about sent and received packets of a specified VRRP6 group. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the device are cleared.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about VRRP6 Advertisement packets, run the **reset vrrp6 statistics** command to clear existing statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when executing the **reset vrrp6 statistics** command.

Example

Clear statistics about sent and received packets of VRRP6 group 1 on VLANIF100.

```
<HUAWEI> reset vrrp6 interface vlanif 100 vrid 1 statistics
```

Clear statistics about all the packets of VRRP6 group 1.

```
<HUAWEI> reset vrrp6 vrid 1 statistics
```

Clear statistics about packets of all VRRP6 groups on the switch.

```
<HUAWEI> reset vrrp6 statistics
```

12.2.23 set vrrp max-group-number

Function

The **set vrrp max-group-number** command sets the maximum number of allowed VRRP groups (sum of VRRP4 and VRRP6 groups).

The **undo set vrrp max-group-number** command restores the default maximum number of allowed VRRP groups.

By default, a maximum of 64 VRRP groups can be configured.

Format

set vrrp max-group-number *max-group-number*

undo set vrrp max-group-number

Parameters

Parameter	Description	Value
max-group-number	Specifies the maximum number of allowed VRRP groups.	Enumerated type. The values are as follows: ● S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: 64, 128, 192, 256, 320, 384, 448, 512, or 1000 ● S6735-S, S6720S-EI and S6720-EI: 64, 128, 192, 256, 320, or 384 ● S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S: 64, 128, 192, or 256 ● S1720GW-E, S1720GWR-E, SS5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, and S5720S-LI: 64 or 128

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When more than 64 VRRP groups need to be configured, run this command to set the maximum number of allowed VRRP groups.

Precautions

- You are not advised to configure more than 64 VRRP groups.
- When more than 64 VRRP groups are configured, to reduce the frequency of sending VRRP Advertisement packets and the impact of VRRP Advertisement packets on network bandwidth and CPU performance, perform one of the following operations as prompted in addition to executing the **set vrrp max-group-number** command (You are advised to configure an mVRRP group):
  - Run the **vrrp vrid timer advertise** command to increase the interval for sending VRRP Advertisement packets (recommended interval: > 3s), and run the **cpu-defend dynamic-car enable** command to enable a switch to dynamically adjust the default CIR value for protocol packets.
  - Run the **vrrp vrid timer advertise** command to increase the interval for sending VRRP Advertisement packets (recommended interval: > 3s), and run the

    car { **packet-type** *packet-type* | **user-defined-flow** *flow-id* } **cir** *cir-value* [**cbs** *cbs-value*]

    command to increase the CPCAR for VRRP Advertisement packets. Adjust the CPCAR value as prompted. Improper CPCAR settings will affect services on your network.
  - Run the **admin-vrrp vrid** command to configure an mVRRP group.
  - For the S5735S-H, S5736-S, and S6720S-S:
    - When the number of VRRP groups on the device exceeds a specified value, ACL resources are occupied. In this situation, MAC mirroring may become invalid.
    - When a VRRP group is configured for a super-VLAN, the device delivers virtual MAC address entries corresponding to sub-VLANs of the super-VLAN. This occupies many resources. When configuring a VRRP group for a super-VLAN, pay attention to the following points:
      - The VRRP group can be configured for a maximum of 16 super-VLANs on the device.
      - The device allows a maximum of 312 virtual MAC address entries for VRRP. For example, there are 10 sub-VLANs in super-VLAN 100. When a VRRP group is configured on VLANIF 100, 11 virtual MAC address entries are occupied (1 super-VLAN + 10 sub-VLANs).

Example

Set the maximum number of allowed VRRP groups to 192.

```
<HUAWEI> system-view
[HUAWEI] set vrrp max-group-number 192
```

12.2.24 vrrp advertise send-mode

Function

The **vrrp advertise send-mode** command configures a mode in which the master sends VRRP Advertisement packets in a super-VLAN.

The **undo vrrp advertise send-mode** command restores the default mode in which the master sends VRRP Advertisement packets in a super-VLAN.

By default, the master sends VRRP Advertisement packets to a sub-VLAN that is Up and has the smallest VLAN ID in a super-VLAN.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vrrp advertise send-mode { *sub-vlan-id* | **all** }

undo vrrp advertise send-mode

Parameters

Parameter	Description	Value
sub-vlan-id	Specifies the ID of a sub-VLAN where the master sends VRRP Advertisement packets.	The value is an integer that ranges from 1 to 4094.
all	Indicates that the master sends VRRP Advertisement packets to all sub-VLANs in a super-VLAN.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VRRP group is configured in a super-VLAN, run the **vrrp advertise send-mode** command to configure the master to send VRRP Advertisement packets to a specified sub-VLAN or all sub-VLANs in the super-VLAN. If there are a large number of sub-VLANs in a super-VLAN, to save bandwidth, configure the master to send VRRP Advertisement packets to a specified sub-VLAN.

Prerequisites

A VRRP group has been configured on the VLANIF interface corresponding to the super-VLAN.

Precautions

Using **all** is not recommended. If **all** is configured, a super VLAN broadcasts a VRRP Advertisement packet to all its Sub-VLANs. This causes CPU usage to increase.

If both VRRP and static ARP are configured on a device, note the following issues:

- If VRRP is enabled on a VLANIF interface, a virtual IP address cannot be an IP address that maps to a MAC address in a static ARP entry. If a virtual IP address maps to a MAC address in a static ARP entry, a forwarding failure occurs. For example, if a MAC address in a static ARP entry on a VLANIF interface maps to an IP address of 10.1.1.1, the IP address of 10.1.1.1 cannot be a virtual IP address of a VRRP IPv4 backup group configured on the VLANIF interface.
- After a VLANIF interface is configured with a VRRP IPv4 backup group and a static ARP entry, the virtual IP address of the VRRP IPv4 backup group cannot be an IP address that maps to the MAC address in the static ARP entry. Otherwise, a forwarding failure occurs. For example, if a VRRP IPv4 backup group on a VLANIF interface is assigned an IP address of 10.1.1.1, the IP address of 10.1.1.1 cannot map to a MAC address in a static ARP entry configured on the VLANIF interface.

Example

Configure the master to broadcast VRRP Advertisement packets to sub-VLAN 50 in super-VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] aggregate-vlan
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.10.10.10
[HUAWEI-Vlanif100] vrrp advertise send-mode 50
```

12.2.25 vrrp arp send-mode simple

Function

The **vrrp arp send-mode simple** command configures the master on a QinQ termination sub-interface to send gratuitous ARP packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag.

The **undo vrrp arp send-mode simple** command restores the default setting.

By default, the master on a QinQ termination sub-interface sends gratuitous ARP packets to the VLAN specified by the outer VLAN tag and all VLANs in the VLAN range specified by the inner VLAN tag.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vrrp arp send-mode simple

undo vrrp arp send-mode simple

Parameters

None

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When VRRP is deployed on a QinQ termination sub-interface, the system sends double-tagged ARP packets. If the inner VLAN tag specifies a VLAN range, the system sends ARP packets to all the VLANs in the VLAN range specified by the inner VLAN tag. This ensures that MAC address entries on the downstream device are updated immediately, but causes a heavy burden. The **vrrp arp send-mode simple** command configures the master on a QinQ termination sub-interface to send gratuitous ARP packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag. This prevents excess gratuitous ARP packets from affecting the system.

NOTE

The **vrrp arp send-mode simple** command takes effect in VLANs specified only by the inner VLAN tag but not VLANs specified by the outer VLAN tag. For example, the VLAN ID in the outer tag ranges from 1 to 10 and the VLAN ID in the inner tag ranges from 1 to 10. After the **vrrp arp send-mode simple** command is run, gratuitous ARP packets are transmitted in only VLAN 1 (specified by the inner VLAn tag). A total of 10 gratuitous ARP packets (10 outer VLAN IDs x 1 inner VLAN ID) are sent.

Precautions

The **vrrp arp send-mode simple** command must be executed on a QinQ termination sub-interface.

Example

Configure VE sub-interface Virtual-Ethernet0/0/2.1 to send gratuitous ARP packets in VLAN 3.

```
<HUAWEI> system-view
[HUAWEI] interface virtual-ethernet0/0/2
[HUAWEI-Virtual-Ethernet0/0/2] ve-group 1 l3-access
[HUAWEI-Virtual-Ethernet0/0/2] quit
[HUAWEI] interface virtual-ethernet0/0/2.1
[HUAWEI-Virtual-Ethernet0/0/2.1] qinq termination pe-vid 5 ce-vid 3 to 20
[HUAWEI-Virtual-Ethernet0/0/2.1] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-Virtual-Ethernet0/0/2.1] vrrp arp send-mode simple
```

12.2.26 vrrp gratuitous-arp timeout

Function

The **vrrp gratuitous-arp timeout** command configures an interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets.

The **undo vrrp gratuitous-arp timeout** command restores the default interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets.

The default interval is 120 seconds.

Format

vrrp gratuitous-arp timeout *time*

undo vrrp gratuitous-arp timeout

Parameters

Parameter	Description	Value
timeout *time*	Specifies an interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets.	The value is an integer that ranges from 30 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets to its connected downstream switch to update the MAC entries on the downstream switch.

Precautions

- If a short interval is used, bandwidth resources will be consumed. If a long interval is used, MAC address entries on the downstream switch cannot be updated immediately.
- The interval at which the master sends gratuitous ARP or ND packets must be shorter than the aging time of MAC address entries on user devices.

Set the interval based on actual networking:

- To restore the default interval at which the master sends gratuitous ARP or ND packets, run the **undo vrrp gratuitous-arp timeout** command in the system view.
- If gratuitous ARP or ND packet do not need to be sent, run the **vrrp gratuitous-arp timeout disable** command in the system view.

Example

Set the interval at which the master in a VRRP group sends gratuitous ARP packets or the master in a VRRP6 group sends ND packets to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] vrrp gratuitous-arp timeout 100
```

12.2.27 vrrp gratuitous-arp timeout disable

Function

The **vrrp gratuitous-arp timeout disable** command disables the master device in a Virtual Router Redundancy Protocol for IPv4 (VRRP4) backup group from sending gratuitous ARP packets or the master device in a Virtual Router Redundancy Protocol for IPv6 (VRRP6) backup group from sending ND packets.

By default, the master device in a VRRP4 (or VRRP6) backup group sends gratuitous ARP (or ND) packets every 120 seconds.

Format

vrrp gratuitous-arp timeout disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master device in a VRRP4 (or VRRP6) backup group sends gratuitous ARP (or ND) packets to its connected downstream switch to update the MAC entries on the downstream switch. Because ARP and NDP do not provide any security mechanisms, attackers can send spoofed ARP or ND packets to attack network devices. If high network security is required, run the **vrrp gratuitous-arp timeout disable** command to disable the master device in a VRRP4 backup group from sending gratuitous ARP packets or the master device in a VRRP6 backup group from sending ND packets.

Precautions

After the **vrrp gratuitous-arp timeout disable** command is run, the master device in a VRRP4 (or VRRP6) backup group no longer periodically sends gratuitous ARP (or ND) packets to its connected downstream switch. If a master/backup switchover occurs, the MAC entries on the downstream switch cannot be promptly updated. As a result, traffic is interrupted.

Example

Disable the master device in a VRRP4 backup group from sending gratuitous ARP packets or the master device in a VRRP6 backup group from sending ND packets.

```
<HUAWEI> system-view
[HUAWEI] vrrp gratuitous-arp timeout disable
```

12.2.28 vrrp recover-delay

Function

The **vrrp recover-delay** command sets the delay before a VRRP or VRRP6 group recovers.

The **undo vrrp recover-delay** command restores the default delay before a VRRP or VRRP6 group recovers.

By default, the delay before a VRRP or VRRP6 group recovers is 0.

Format

vrrp recover-delay *delay-value*

undo vrrp recover-delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay before a VRRP or VRRP6 group recovers.	The value is an integer that ranges from 0 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface or a BFD session associated with a VRRP or VRRP6 group alternates between Up and Down states, the VRRP or VRRP6 group status may flap, causing user traffic loss. To solve this problem, run the **vrrp recover-delay** command to set the delay before a VRRP or VRRP6 group recovers. A VRRP or VRRP6 group then only responds to the interface or BFD session Up event after the delay expires.

Precautions

- When the device in a VRRP or VRRP6 group restarts, the VRRP or VRRP6 group status may flap. It is recommended that the delay be set based on actual networking.
- After an interface or a BFD session associated with a VRRP or VRRP6 group alternates between Up and Down states, the system only records logs and alarms at one time during each delay. This prevents the same alarms from being displayed repeatedly.

Example

Set the delay before a VRRP group recovers to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] vrrp recover-delay 5
```

12.2.29 vrrp smooth-switching timer

Function

The **vrrp smooth-switching timer** command enables VRRP smooth switching and sets the interval contained in VRRP Advertisement packets during VRRP smooth switching.

The **undo vrrp smooth-switching timer** command disables VRRP smooth switching.

By default, VRRP smooth switching is enabled and the interval contained in VRRP Advertisement packets is 100s.

Format

vrrp smooth-switching timer *timer-value*

undo vrrp smooth-switching timer

Parameters

Parameter	Description	Value
timer-value	Specifies the interval contained in VRRP Advertisement packets during VRRP smooth switching. After VRRP smooth switching is enabled on the master, the master sends VRRP Advertisement packets at this interval during an active/standby switchover.	The value is an integer that ranges from 1 to 255, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an active/standby switchover occurs on the master in the stack system in a VRRP group, the master and backup may fail to communicate with each other during the switchover. During the switchover, the backup with the highest priority becomes the new master if backups receive no VRRP Advertisement packet after the VRRP Advertisement packet sending interval expires. In this situation, two masters coexist. After the active/standby switchover is complete on the original master, the original master switches to the master because its priority is higher than the new master. During this process, services are switched twice, causing unstable service transmission.

After VRRP smooth switching is enabled on the device in the stack system, backups learn the smooth switching time. This implementation extends the timeout interval for receiving VRRP Advertisement packets during VRRP smooth switching, ensuring stability of the VRRP group status.

Prerequisites

The device has been enabled to learn the interval for sending VRRP Advertisement packets using the **vrrp timer-advertise learning enable** command.

Precautions

After receiving VRRP Advertisement packets from the master, the non-master device checks the interval in VRRP Advertisement packets. If the interval in VRRP Advertisement packets is different from the interval of the non-master device, the non-master device learns the interval and adjusts its own interval to be the same as the learned interval.

- *timer-value* must be greater than the interval at which VRRP Advertisement packets are sent. Otherwise, the master may be busy during the switchover and unable to send VRRP Advertisement packets in a timely manner. As a result, a backup switches to the master.
- After the **undo vrrp timer-advertise learning enable** command is executed, VRRP smooth switching is also disabled.

Example

Enable VRRP smooth switching and set the interval contained in VRRP Advertisement packets during VRRP smooth switching to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] vrrp smooth-switching timer 20
```

12.2.30 vrrp timer-advertise learning enable

Function

The **vrrp timer-advertise learning enable** command enables the device to learn the interval for sending VRRP Advertisement packets.

The **vrrp timer-advertise learning disable** command disables the device from learning the interval for sending VRRP Advertisement packets.

The **undo vrrp timer-advertise learning enable** command disables the device from learning the interval for sending VRRP Advertisement packets.

By default, the device is enabled to learn the interval for sending VRRP Advertisement packets.

Format

vrrp timer-advertise learning enable

vrrp timer-advertise learning disable

undo vrrp timer-advertise learning enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a link fault triggers an active/standby switchover, VRRP smooth switching is enabled to prevent traffic loss. Before enabling VRRP smooth switching, run the **vrrp timer advertise learning enable** command to enable the device to learn the interval for sending VRRP Advertisement packets. Then non-master devices in the VRRP group will learn the interval at which VRRP Advertisement packets are sent and update their interval to be the same as the learned interval.

Prerequisites

A VRRP group has been created.

Precautions

If VRRP smooth switching has been enabled, running the **undo vrrp timer-advertise learning enable** command disables VRRP smooth switching.

The **undo vrrp timer-advertise learning enable** command is valid only for VRRPv2. If VRRPv3 is enabled using the **vrrp version** command, this function does not take effect.

Example

Enable the device to learn the interval for sending VRRP Advertisement packets.

```
<HUAWEI> system-view
[HUAWEI] vrrp timer-advertise learning enable
```

12.2.31 vrrp track bfd gratuitous-arp send enable

Function

The **vrrp track bfd gratuitous-arp send enable** command enables a sub-interface to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

The **undo vrrp track bfd gratuitous-arp send enable** command cancels the configuration.

By default, a sub-interface is not enabled to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

Format

vrrp track bfd gratuitous-arp send enable

undo vrrp track bfd gratuitous-arp send enable

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where association between a VRRP group and a peer BFD session is configured, when the peer BFD session on the backup detects a fault on the active link, the peer BFD session notifies the VRRP group of performing an active/standby switchover. The new master sends gratuitous ARP packets to its downstream Layer 2 device through the software protocol stack so that traffic is switched to the new master.

To speed up traffic switching, run this command to enable a sub-interface to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session. When the peer BFD session on the backup detects the fault on the active link, the hardware rapidly sends gratuitous ARP packets to its downstream Layer 2 device so that traffic is switched to the new master.

Prerequisites

The **vrrp vrid** *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } **peer** command has been configured on the sub-interface.

Precautions

Each peer BFD session triggers only one VRRP group to send gratuitous ARP packets.

Example

Enable gigabitethernet0/0/1.1 to rapidly send gratuitous ARP packets during an active/standby switchover of a VRRP group triggered by its associated peer BFD session.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] vrrp vrid 1 track bfd-session 1 peer
[HUAWEI-GigabitEthernet0/0/1.1] vrrp track bfd gratuitous-arp send enable
```

12.2.32 vrrp un-check ttl

Function

The **vrrp un-check ttl** command disables the device from checking the TTL value in VRRP Advertisement packets.

The **undo vrrp un-check ttl** command enables the device to check the TTL value in VRRP Advertisement packets.

By default, the system checks the TTL value in VRRP Advertisement packets.

Format

vrrp un-check ttl

undo vrrp un-check ttl

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The device checks the TTL value in received VRRP Advertisement packets. If the TTL value in a VRRP Advertisement packet is not 255, the device discards the VRRP Advertisement packet and generates a log about the VRRP Advertisement packet error.

On certain networks, especially on a network where the device interworks with non-Huawei devices, valid packets may be discarded if TTL check is enabled. You can configure the device not to check the TTL value in VRRP Advertisement packets.

Example

Disable the switch from checking the TTL value in VRRP Advertisement packets on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp un-check ttl
```

Disable the switch from checking the TTL value in VRRP Advertisement packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp un-check ttl
```

12.2.33 vrrp version

Function

The **vrrp version** command configures a VRRP version number.

The **undo vrrp version** command restores the default VRRP version number.

By default, VRRPv2 is used.

Format

vrrp version { **v2** | **v3** }

undo vrrp version

Parameters

Parameter	Description	Value
v2	Indicates that VRRPv2 is used.	-
v3	Indicates that VRRPv3 is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If VRRPv2 and VRRPv3 are used on a network and devices running VRRPv2 need to communicate with devices running VRRPv3, run the **vrrp version** command to specify a VRRP version number.

Precautions

A VRRPv2 group can only send and receive VRRPv2 Advertisement packets. It discards the received VRRPv3 Advertisement packets.

A VRRPv3 group can send and receive both VRRPv2 and VRRPv3 Advertisement packets. You can configure a mode in which VRRPv3 Advertisement packets are sent so that devices running VRRPv2 and VRRPv3 can communicate.

Follow-up Procedure

After VRRPv3 is used, run the **vrrp version-3 send-packet-mode** command in the system view or the **vrrp vrid version-3 send-packet-mode** command in the interface view to configure a mode in which VRRP Advertisement packets are sent.

Example

Set the VRRP version of the device to VRRPv3.

```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
```

12.2.34 vrrp version-3 send-packet-mode

Function

The **vrrp version-3 send-packet-mode** command configures a mode in which VRRPv3 Advertisement packets are sent.

The **undo vrrp version-3 send-packet-mode** command restores the default mode in which VRRPv3 Advertisement packets are sent.

By default, the mode is **v3-only**.

Format

vrrp version-3 send-packet-mode { **v2-only** | **v3-only** | **v2v3-both** }

undo vrrp version-3 send-packet-mode

Parameters

Parameter	Description	Value
v2-only	Indicates that the device sends only VRRPv2 Advertisement packets.	-
v3-only	Indicates that the device sends only VRRPv3 Advertisement packets.	-
v2v3-both	Indicates that the device sends both VRRPv2 and VRRPv3 Advertisement packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices in a VRRP group use different VRRP version numbers, the VRRP group may fail to negotiate the status. This is because a VRRPv2-enabled device can only receive VRRPv2 Advertisement packets and discards the received VRRPv3 Advertisement packets. You can configure a mode in which VRRP Advertisement packets are sent so that devices running VRRPv2 and VRRPv3 in the VRRP group can negotiate the status.

Precautions

- Only VRRPv3 supports this command.
- If both the **vrrp version-3 send-packet-mode** and **vrrp vrid version-3 send-packet-mode** commands are run, the **vrrp vrid version-3 send-packet-mode** command takes precedence over the **vrrp version-3 send-packet-mode** command.

NOTE

If a large number of VRRP groups are configured, **v2v3-both** is not recommended.

Example

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only**.

```
<HUAWEI> system-view
[HUAWEI] vrrp version-3 send-packet-mode v2-only
```

12.2.35 vrrp virtual-ip ping enable

Function

The **vrrp virtual-ip ping enable** command enables the master to respond to ping packets sent to a virtual IP address.

The **vrrp virtual-ip ping disable** command disables the master from responding to ping packets sent to a virtual IP address.

The **undo vrrp virtual-ip ping enable** command disables the master from responding to ping packets sent to a virtual IP address.

By default, the master is enabled to respond to ping packets sent to a virtual IP address.

Format

vrrp virtual-ip ping enable

vrrp virtual-ip ping disable

undo vrrp virtual-ip ping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch allows user devices to ping a virtual IP address to serve the following purposes:

- Monitors the operating status of the master in a VRRP group.
- Monitors communication between a user device and a network connected by a default gateway using the virtual IP address.

Precautions

If the ping to a virtual IP address is enabled, a device on an external network can ping a virtual IP address. This imposes the switch to ICMP-based attacks.

After the **undo vrrp virtual-ip ping enable** command is run to disable the master from responding to ping packets sent to a virtual IP address, the host route for the virtual IP address is deleted. As a result, services transmitted using the host route are interrupted. For example, after the **undo vrrp virtual-ip ping enable** command is run, the GRE tunnel with the source IP address of a virtual IP address goes Down.

Example

Disable the master from responding to ping packets.

```
<HUAWEI> system-view
[HUAWEI] undo vrrp virtual-ip ping enable
```

12.2.36 vrrp virtual-ip route-advertise disable

Function

The **vrrp virtual-ip route-advertise disable** command disables a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

The **undo vrrp virtual-ip route-advertise disable** command enables a dynamic routing protocol to advertise routes generated by the virtual IP address of a VRRP group.

By default, a dynamic routing protocol is enabled to advertise routes generated by the virtual IP address of a VRRP group.

Format

vrrp virtual-ip route-advertise disable [**isis** | **ospf** | **rip**] *

undo vrrp virtual-ip route-advertise disable

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **isis**.

Parameters

Parameter	Description	Value
isis	Disables IS-IS from advertising the routes generated by the virtual IP address of a VRRP group.	-
ospf	Disables OSPF from advertising the routes generated by the virtual IP address of a VRRP group.	-
rip	Disables RIP from advertising the routes generated by the virtual IP address of a VRRP group.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Direct routes generated by the virtual IP address of a VRRP group can be imported to a dynamic routing protocol. By default, these routes are advertised by a dynamic routing protocol to neighbors. In practice, a large number of routes may be generated by the virtual IP address of a VRRP group. If a dynamic routing protocol imports theses routes and advertises them to neighbors, there is a heavy burden on network devices and network performance deteriorates. You can run the **vrrp virtual-ip route-advertise disable** command to disable a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

Prerequisites

- A virtual IP address has been configured for a VRRP group.
- A dynamic routing protocol has imported routes generated by the virtual IP address of the VRRP group.

Precautions

After the **vrrp virtual-ip route-advertise disable** command is executed, routes generated by virtual IP addresses of all VRRP groups cannot be advertised by a dynamic routing protocol.

The **vrrp virtual-ip route-advertise disable** command is only valid for OSPF and IS-IS.

If routes generated by the virtual IP address of a VRRP group must be advertised by a dynamic routing protocol, do not run the **vrrp virtual-ip route-advertise disable** command.

Example

Disable a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

```
<HUAWEI> system-view
[HUAWEI] vrrp virtual-ip route-advertise disable
```

12.2.37 vrrp vrid authentication-mode

Function

The **vrrp vrid authentication-mode** command configures an authentication mode and an authentication key for a VRRP group.

The **undo vrrp vrid authentication-mode** command cancels the authentication mode and authentication key for a VRRP group.

By default, a VRRP group uses non-authentication.

Format

vrrp vrid *virtual-router-id* **authentication-mode** { **simple** { *key* | **plain** *key* | **cipher** *cipher-key* } | **md5** *md5-key* }

undo vrrp vrid *virtual-router-id* **authentication-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
simple	Indicates simple authentication.	-
key	Specifies the authentication key in simple authentication mode.	The value is a string of 1 to 8 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
plain *key*	Specifies the authentication key in plain text authentication mode. **NOTE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of 1 to 8 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *cipher-key*	Specifies the authentication key in cipher text authentication mode.	The value a string of case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Passwords are saved in ciphertext in the configuration file with the length of 48. Either of the following passwords can be set: ● A simple text password is a string of 1 to 8 characters. ● A ciphertext password is a string of 32 or 48 characters. **NOTE** A 32-character ciphertext password configured in an earlier version is also supported in this version.
md5 *md5-key*	Specifies the authentication key in MD5 authentication mode.	The value a string of case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Passwords are saved in ciphertext in the configuration file with the length of 48. Either of the following passwords can be set: ● A simple text password is a string of 1 to 8 characters. ● A ciphertext password is a string of 24, or 32, or 48 characters. **NOTE** A 32-character ciphertext password configured in an earlier version is also supported in this version.

NOTE

For security purposes, you are advised to use MD5 as the authentication algorithm of VRRP.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To be compatible with VRRP defined in earlier version and interwork with other devices, VRRP provides simple authentication and MD5 authentication. The **vrrp vrid authentication-mode** command configures an authentication mode and an authentication key for a VRRP group.

Prerequisites

A VRRP group has been configured on a specified interface.

Precautions

Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

Set the authentication mode of the VRRP group with VRID 2 on VLANIF100 to MD5 authentication and set the authentication key to **Huawei-1**.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.1
[HUAWEI-Vlanif100] vrrp vrid 2 authentication-mode md5 Huawei-1
```

Set the authentication mode of the VRRP group with VRID 2 on GE0/0/1 to MD5 authentication and set the authentication key to **Huawei-1**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 2 virtual-ip 10.1.1.1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 2 authentication-mode md5 Huawei-1
```

12.2.38 vrrp vrid backup-forward

Function

The **vrrp vrid backup-forward** command enables the backup device in a VRRP backup group to forward traffic.

The **undo vrrp vrid backup-forward** command disables the backup device in a VRRP backup group from forwarding traffic.

By default, the backup device in a VRRP backup group is disabled from forwarding traffic.

Format

vrrp vrid *virtual-router-id* **backup-forward**

undo vrrp vrid *virtual-router-id* **backup-forward**

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the ID of a VRRP backup group.	The value is an integer ranging from 1 to 255.

Views

GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On large aggregation networks of enterprises, terminal users use active and standby links to access aggregation devices that have a VRRP backup group deployed. The aggregation device connects to the active link is the master device, and that connects to the standby link is the backup device. If the active link or the master device fails, a link switchover occurs. However, the master/backup switchover in the VRRP backup group has not yet completed. Therefore, a traffic interruption occurs and lasts for a short period.

To prevent traffic interruptions in such scenarios, run the **vrrp vrid backup-forward** command to enable the backup device in a VRRP backup group to forward traffic. This configuration ensures carrier-class reliability.

Prerequisites

A VRRP backup group has been created using the **vrrp vrid virtual-ip** command in the interface view.

Precautions

The backup device can forward traffic with the destination MAC address being the virtual MAC address. If a downstream switch broadcasts a packet with the destination MAC address being the virtual MAC address, the backup device will also forward this packet. Therefore, two copies of this packet will be sent. To prevent duplicate traffic, do not run the **vrrp vrid backup-forward** command in scenarios other than the one where high reliability is required on large aggregation networks of enterprises.

Example

Create VRRP backup group 1 on GE0/0/2.1 and enable the backup device in the VRRP backup group to forward traffic.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2.1
[HUAWEI-GigabitEthernet0/0/2.1] vrrp vrid 1 virtual-ip 10.1.1.100
[HUAWEI-GigabitEthernet0/0/2.1] vrrp vrid 1 backup-forward
```

12.2.39 vrrp vrid preempt-mode disable

Function

The **vrrp vrid preempt-mode disable** command configures the device in a VRRP group in non-preemption mode.

The **undo vrrp vrid preempt-mode** command restores the default preemption mode.

By default, the device uses the immediate preemption mode.

Format

vrrp vrid *virtual-router-id* **preempt-mode disable**

undo vrrp vrid *virtual-router-id* **preempt-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device with higher priority in a VRRP group to be the master, set the preemption mode on the device. In non-preemption mode, as long as the master is working properly, the backup with higher priority cannot be the master.

NOTE

When non-preemption is disabled, the preemption delay is restored to 0 seconds immediately.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Example

Configure VRRP group 1 in non-preemption mode on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-Vlanif100] vrrp vrid 1 preempt-mode disable
```

Configure VRRP group 1 in non-preemption mode on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 preempt-mode disable
```

12.2.40 vrrp vrid preempt-mode timer delay

Function

The **vrrp vrid preempt-mode timer delay** command sets the preemption delay for the device in a VRRP group.

The **undo vrrp vrid preempt-mode timer delay** command restores the default preemption delay for the device in a VRRP group.

By default, the preemption delay is 0 seconds.

Format

vrrp vrid *virtual-router-id* **preempt-mode timer delay** *delay-value*

undo vrrp vrid *virtual-router-id* **preempt-mode timer delay**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
delay *delay-value*	Specifies the preemption delay.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the backup in a VRRP group does not receive VRRP Advertisement packets from the master within a specified period of time, the backup becomes the master. On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP group status will flap and traffic is lost. To prevent frequent switching of the VRRP group status, run the **vrrp vrid preempt-mode timer delay** command to set the preemption delay so that the backup becomes the master only after the delay expires.

Precautions

You are advised to set the preemption delay of the backup in a VRRP group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 15s. These settings allow a period of time for status synchronization between the uplink and downlink on devices in a VRRP group on an unstable network. If the preceding settings are not used, two masters coexist and user devices may learn an incorrect master address. As a result, traffic is interrupted.

- The preemption delay refers to the delay before the backup switches to the master. Therefore, the IP address owner is irrelevant to the preemption delay. After the IP address owner recovers, it becomes the master immediately, without any delay.
- On a stable network, a short preemption delay is recommended. When the master is faulty, the backup with the highest priority can rapidly switch to the master. This prevents traffic loss. On an unstable network, a long preemption delay is recommended. This prevents traffic loss caused by frequent switching of the VRRP group status.

Example

Set the preemption delay of VRRP group 1 to 5 seconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 preempt-mode timer delay 5
```

Set the preemption delay of VRRP group 1 to 5 seconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 preempt-mode timer delay 5
```

12.2.41 vrrp vrid priority

Function

The **vrrp vrid priority** command sets the priority of the device in a VRRP group.

The **undo vrrp vrid priority** command restores the default priority of the device in a VRRP group.

By default, the priority of the device in a VRRP group is 100.

Format

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
priority *priority-value*	Specifies the priority of the device in a VRRP group.	The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the device in a VRRP group as the default gateway, run the **vrrp vrid priority** command to specify the highest priority for the device so that the device can become the master.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed to create a VRRP group.

Precautions

- Priority 0 is reserved in the system. Priority 255 is reserved for the IP address owner.
- When devices in a VRRP group have the same priority, the device that first changes to master state becomes the master. If devices attempt to be the master simultaneously, the device where the interface with the largest IP address is located becomes the master.

Example

Set the priority of the switch in VRRP group 1 to 150 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-Vlanif100] vrrp vrid 1 priority 150
```

Set the priority of the switch in VRRP group 1 to 150 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 priority 150
```

12.2.42 vrrp vrid timer advertise

Function

The **vrrp vrid timer advertise** command sets the interval at which the master sends VRRP Advertisement packets.

The **undo vrrp vrid timer advertise** command restores the default interval at which the master sends VRRP Advertisement packets.

By default, the master sends VRRP Advertisement packets every 1 second.

Format

vrrp vrid *virtual-router-id* **timer advertise** *advertise-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
advertise *advertise-interval*	Specifies the interval at which the master sends VRRP Advertisement packets.	The value is an integer, in seconds. In VRRPv2, the value ranges from 1 to 255. In VRRPv3, the value ranges from 1 to 40.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP group sends VRRP Advertisement packets to backups at intervals to notify that it is working properly. If the backup with the highest priority does not receive any VRRP Advertisement packets from the master at the specified interval, it considers the master faulty and becomes the master. The **vrrp vrid timer advertise** command sets the interval at which the master sends VRRP Advertisement packets.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Precautions

If a longer interval is used, backups in the same VRRP group cannot detect the fault on the master in a timely manner, causing packet loss. If a shorter interval is used, system resources are occupied. In addition, when network traffic is heavy or the network is unstable, backups may not receive packets after the Master_Down_Interval timer expires. As a result, the VRRP group status is incorrectly switched. Set the interval based on actual networking. The algorithm for calculating the value of the Master_Down_Interval timer is as follows:

Master_Down_Interval = (3 x Advertisement_Interval) + Skew_time

Skew_Time = (256 – Priority) / 256

When the interval for sending VRRP Advertisement packets on the master and backup in the same VRRP group is different, the master sends VRRP Advertisement packets at the configured interval.

Example

Set the interval at which the master in VRRP group 1 sends VRRP Advertisement packets to 5 seconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-Vlanif100] vrrp vrid 1 timer advertise 5
```

Set the interval at which the master in VRRP group 1 sends VRRP Advertisement packets to 5 seconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 timer advertise 5
```

12.2.43 vrrp vrid track admin-vrrp vrid

Function

The **vrrp vrid track admin-vrrp vrid** command binds a VRRP group to an mVRRP group.

The **undo vrrp vrid track admin-vrrp** command unbinds a VRRP group from an mVRRP group.

By default, no VRRP group is bound to an mVRRP group.

Format

vrrp vrid *virtual-router-id1* **track admin-vrrp interface** *interface-type interface-number* **vrid** *virtual-router-id2* **unflowdown**

undo vrrp vrid *virtual-router-id1* **track admin-vrrp**

Parameters

Parameter	Description	Value
vrid *virtual-router-id1*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
vrid *virtual-router-id2*	Specifies the VRID of an mVRRP group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface configured with an mVRRP group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
unflowdown	Allows the interface where a VRRP group bound to an mVRRP group is configured to remain in Up state if the mVRRP group is in Backup or Initialize state.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple VRRP groups are configured on the device, each group sends VRRP Advertisement packets to maintain its state machine. As a result, a large number of VRRP Advertisement packets are generated, which occupy network bandwidth resources and cause CPU performance to deteriorate. To solve the problem, run the **vrrp vrid track admin-vrrp vrid** command to bind a VRRP group to an mVRRP group. After a VRRP group is bound to an mVRRP group, the VRRP group does not send VRRP Advertisement packets to negotiate the Master and Backup states. The mVRRP group determines the status of the bound VRRP group. This method greatly reduces the impact of VRRP Advertisement packets on network bandwidth and CPU performance.

This mode is used on a network where uplink and downlink traffic can be transmitted along different paths. **unflowdown** can be configured to allow the mVRRP group to determine the status of its bound VRRP group. Uplink traffic travels through the master and then reaches the upper-layer network, and downlink traffic travels through either the master or backup to reach users.

Prerequisites

A VRRP group and an mVRRP group have been created.

Precautions

The **vrrp vrid track admin-vrrp vrid** command can be used only on the interface where the bound VRRP group is configured. This command cannot be used on the interface where an mVRRP group is configured.

VRRP4 and VRRP6 can be configured on an interface simultaneously. However, there are limitations:

- A VRRP4 group can be bound to only an mVRRP4 group, and a VRRP6 group can be bound to only an mVRRP6 group.

- At most one VRRP4 group and one VRRP6 group can be configured on an interface. In addition, **unflowdown** must be used. An interface cannot be configured with multiple VRRP4 or VRRP6 groups.

If multiple service VRRP backup groups are configured on an interface, a single service VRRP backup group can be bound to the mVRRP backup group.

Example

Bind VRRP group 1 to mVRRP group 2 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp vrid 1 track admin-vrrp interface vlanif 20 vrid 2 unflowdown
```

Bind VRRP group 1 to mVRRP group 2 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track admin-vrrp interface GigabitEthernet 0/0/2 vrid 2
unflowdown
```

12.2.44 vrrp vrid track bfd-session

Function

The **vrrp vrid track bfd-session** command associates a VRRP group with a BFD session.

The **undo vrrp vrid track bfd-session** command disassociates a VRRP group from a BFD session.

By default, a VRRP group is not associated with a BFD session.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vrrp vrid *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track bfd-session** [*bfd-session-id* | **session-name** *bfd-configure-name*]

vrrp vrid *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } **peer** (Only the sub-interfaces of the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command)

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
bfd-session-id	Specifies the local discriminator of the monitored BFD session.	The value is an integer that ranges from 1 to 8191.
session-name *bfd-configure-name*	Specifies the name of the monitored BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
increased *value-increased*	Specifies the value by which the priority increases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored BFD session becomes Down, the VRRP priority decreases by 10.
peer	Indicates that the monitored BFD session is a peer BFD session.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between a VRRP group and a BFD session implements the following functions:

1. Rapid active/standby switchover: When the link of a VRRP group or the master is faulty, the backup becomes the master after a certain period of time (second level), causing packet loss. You can associate the VRRP group with a BFD session on the backup so that the BFD session can rapidly detect communication faults of the VRRP group. When the BFD session detects a fault, it notifies the VRRP group that the priority of the backup needs to be increased. Then an active/standby switchover is triggered immediately. This millisecond-level switchover reduces traffic loss. When the monitored BFD session recovers, the original priority of the device in the VRRP group is restored.
2. Monitoring the uplink: Because VRRP cannot detect faults on the uplink of a VRRP group, services are interrupted. You can associate the VRRP group with a BFD session on the master so that the BFD session monitors the uplink status of the master. When the BFD session detects a fault on the uplink, it notifies the VRRP group that the priority of the master needs to be decreased. Then an active/standby switchover is triggered immediately. This reduces the impact of the uplink fault on service forwarding. When the monitored BFD session recovers, the original priority of the device in the VRRP group is restored.

Prerequisites

A VRRP group has been created and a static BFD session or a static BFD session with automatically negotiated discriminators has been created.

Precautions

After a VRRP group is associated with a BFD session, the BFD session type cannot be modified. Before deleting the BFD session type, you must delete all original configurations.

After a VRRP group is associated with a BFD session, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored BFD session becomes Down.

Multiple VRRP groups can monitor a BFD session, and a VRRP group can monitor a maximum of eight BFD sessions simultaneously.

NOTE

When associating a VRRP group with a BFD session, note the following points:

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If an IP address owner exists in the VRRP group, the VRRP group cannot monitor the BFD session.
- If **session-name** *bfd-configure-name* is specified, the VRRP group can be bound to only the static BFD session with automatically negotiated discriminators.
- If *bfd-session-id* is specified, the VRRP group can be bound to only the static BFD session.

Example

Configure VRRP group 1 to monitor the BFD session with local discriminator 1 on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd abc bind peer-ip 10.1.1.1 interface vlanif 100
[HUAWEI-bfd-session-abc] discriminator local 1
[HUAWEI-bfd-session-abc] discriminator remote 2
[HUAWEI-bfd-session-abc] commit
[HUAWEI-bfd-session-abc] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track bfd-session 1 reduced 40
```

Configure VRRP group 1 to monitor the BFD session with local discriminator 1 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bfd abc bind peer-ip 10.1.1.1 interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-abc] discriminator local 1
[HUAWEI-bfd-session-abc] discriminator remote 2
[HUAWEI-bfd-session-abc] commit
[HUAWEI-bfd-session-abc] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.12
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track bfd-session 1 reduced 40
```

Configure VRRP group 1 to monitor the BFD session **hello** on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd hello bind peer-ip 10.2.1.1 interface vlanif 100 source-ip 10.2.1.2 auto
[HUAWEI-bfd-session-hello] commit
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.2.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track bfd-session session-name hello reduced 40
```

Configure VRRP group 1 to monitor the BFD session **hello** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bfd hello bind peer-ip 10.2.1.1 interface gigabitethernet 0/0/1 source-ip 10.2.1.2 auto
[HUAWEI-bfd-session-hello] commit
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.2.1.12
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track bfd-session session-name hello reduced 40
```

12.2.45 vrrp vrid track interface

Function

The **vrrp vrid track interface** command associates a VRRP group with an interface.

The **undo vrrp vrid track interface** command disassociates a VRRP group from an interface.

By default, a VRRP group is not associated with an interface.

Format

vrrp vrid *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of an interface monitored by a VRRP group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** A VRRP backup group can track Layer 2 and Layer 3 interfaces. ● If the tracked interface is a Layer 2 interface, the VRRP backup group tracks the physical status of the Layer 2 interface and changes its own priority based on the tracked physical status. ● If the tracked interface is a Layer 3 interface, the VRRP backup group tracks the protocol status of the Layer 3 interface and changes its own priority based on the tracked protocol status.	-
increased *value-increased*	Specifies the value by which the priority increases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.

Parameter	Description	Value
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored interface goes Down, the VRRP priority of the device decreases by 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VRRP can only detect the status change of the interface on which a VRRP group is configured. VRRP cannot detect faults on the uplink interface, causing service interruption. You can run the **vrrp vrid track interface** command to associate a VRRP group with a device interface not in the VRRP group. When the monitored interface becomes Down, the priority of the device is adjusted and an active/standby switchover is triggered. Therefore, services can be forwarded correctly. When the status of the monitored interface recovers, the original priority of the device in the VRRP group is restored.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Precautions

After a VRRP group is associated with an interface, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored interface becomes Down.

NOTE

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If the device is the IP address owner (the virtual router IP address is used as the actual interface address), you cannot associate a VRRP group with an interface.
- Multiple VRRP groups can monitor an interface, and a VRRP group can monitor a maximum of 8 interfaces simultaneously.

Example

Associate VRRP group 1 with VLANIF 10 and set **reduced** *value-reduced* to 50 when VLANIF 10 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 20
[HUAWEI-Vlanif20] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-Vlanif20] vrrp vrid 1 track interface vlanif 10 reduced 50
```

Associate VRRP group 1 with GE0/0/2 and set reduced *value-reduced* to 50 when GE0/0/2 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 track interface gigabitethernet0/0/2 reduced 50
```

12.2.46 vrrp vrid track ip route

Function

The **vrrp vrid track ip route** command associates a VRRP group with a route.

The **undo vrrp vrid track ip route** command disassociates a VRRP group from a route.

By default, a VRRP group is not associated with a route.

Format

vrrp vrid *virtual-router-id* **track ip route** *ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*] [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track ip route** [*ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
ip-address	Specifies the destination address of the monitored route.	The value is in dotted decimal notation.
mask-address	Specifies the mask of the destination address of the monitored route.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination address of the monitored route.	The value is an integer that ranges from 0 to 32.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
reduced *value-reduced*	Specifies the value by which the master's priority decreases if the monitored route is withdrawn or becomes inactive.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, the master's priority decreases by 10 if the associated route is withdrawn or becomes inactive.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP is enabled on these gateways to determine their Master and Backup states. Although a VRRP group has been configured, access devices may not detect route changes caused by the faulty uplink or network topology change. Consequently, data traffic is lost.

You can associate a VRRP group with a route for forwarding uplink traffic. When the route is withdrawn or becomes inactive, the master' priority is adjusted and an active/standby switchover is performed. When the status of the monitored route recovers, the original priority of the master in the VRRP group is restored.

Pre-configuration Tasks

A VRRP group and a routing protocol such as OSPF or IS-IS have been configured.

Precautions

The VRRP group to be associated with a route cannot contain an IP address owner.

The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and non-0 on the master.

When associating a VRRP group with a route in a VPN instance, note the following points:

- If the VPN instance does not exist, association between the VRRP group and the VPN route cannot work.
- If the VPN instance is deleted after the VRRP group is associated with the VPN route, association between the VRRP group and the VPN route is also deleted.

Multiple VRRP groups can monitor a route, and a VRRP group can monitor a maximum of eight routes simultaneously.

Example

Configure VRRP group 1 to monitor the route on 10.2.1.0, and set the value by which the master's priority decreases if the monitored route is withdrawn or becomes inactive to 20.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track ip route 10.2.1.0 24 reduced 20
```

12.2.47 vrrp vrid track nqa

Function

The **vrrp vrid track nqa** command associates a VRRP group with an NQA test instance to implement a rapid active/standby switchover.

The **undo vrrp vrid track nqa** command disassociates a VRRP group from an NQA test instance.

By default, a VRRP group is not associated with an NQA test instance.

Format

vrrp vrid *virtual-router-id* **track nqa** *admin-name test-name* [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track nqa** [*admin-name test-name*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
admin-name	Specifies the administrator name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
reduced *value-reduced*	Specifies the value by which the master's priority reduces if the NQA test instance detects that the uplink is unavailable.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, the master's priority value decreases by 10 if the associated NQA test instance detects that the uplink is unavailable.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP is enabled on these gateways to determine their Master and Backup states. Although a VRRP group has been configured, the uplink may be unreachable and access devices may not detect the faulty uplink. Consequently, data traffic is lost.

You can associate a VRRP group with an NQA test instance to solve this problem. The NQA test instance periodically sends ICMP packets to detect whether the destination IP address of the uplink is reachable. When the destination IP address is unreachable, the NQA test instance reports the fault to the associated VRRP group and instructs the VRRP group to adjust the priority, implementing an active/standby switchover. When the status of the monitored NQA test instance recovers, the original priority of the master in the VRRP group is restored.

Prerequisites

An NQA test instance of ICMP has been configured.

Precautions

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and non-0 on the master.
- The VRRP group to be associated with a route cannot contain an IP address owner.
- The VRRP group can only be associated with an NQA test instance of ICMP.
- A VRRP group can monitor a maximum of eight NQA test instances.

Example

Associate a VRRP group with NQA test instance **user user1** on VLANIF100 and set **reduced** *value-reduced* to 20 when the destination IP address is unreachable.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user user1
[HUAWEI-nqa-user-user1] test-type icmp
[HUAWEI-nqa-user-user1] destination-address ipv4 10.1.1.1
[HUAWEI-nqa-user-user1] frequency 10
[HUAWEI-nqa-user-user1] probe-count 2
[HUAWEI-nqa-user-user1] start now
[HUAWEI-nqa-user-user1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.2.1.12
[HUAWEI-Vlanif100] vrrp vrid 1 track nqa user user1 reduced 20
```

12.2.48 vrrp vrid version-3 send-packet-mode

Function

The **vrrp vrid version-3 send-packet-mode** command configures a mode in which VRRPv3 Advertisement packets are sent on an interface.

The **undo vrrp vrid version-3 send-packet-mode** command restores the default mode.

By default, VRRPv3 Advertisement packets are sent in **v3-only** mode.

Format

vrrp vrid *virtual-router-id* **version-3 send-packet-mode** { **v2-only** | **v3-only** | **v2v3-both** }

undo vrrp vrid *virtual-router-id* **version-3 send-packet-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
v2-only	Indicates that only VRRPv2 Advertisement packets are sent.	-

Parameter	Description	Value
v3-only	Indicates that only VRRPv3 Advertisement packets are sent.	-
v2v3-both	Indicates that both VRRPv2 and VRRPv3 Advertisement packets are sent.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices in a VRRP group use different VRRP version numbers, the VRRP group may fail to negotiate the status. This is because a VRRPv2-enabled device can only receive VRRPv2 Advertisement packets and discards the received VRRPv3 Advertisement packets. You can set the mode in which VRRP Advertisement packets are sent on the VRRPv3-enabled device so that the VRRPv2-enabled and VRRPv3-enabled devices can negotiate the status.

Precautions

- Only VRRPv3 supports this command.
- If the **vrrp version-3 send-packet-mode** command is used in the system view and interface view simultaneously, the configuration in the interface view takes effect.

NOTE

If a large number of VRRP groups are configured, **v2v3-both** is not recommended.

Example

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
[HUAWEI] vrrp version-3 send-packet-mode v2-only
Warning: The globally configured packet sending mode will take effect for every VRRP backup
group.Continue?[Y/N]:y
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 24 version-3 send-packet-mode v2-only
```

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] vrrp version v3
[HUAWEI] vrrp version-3 send-packet-mode v2-only
Warning: The globally configured packet sending mode will take effect for every VRRP backup
group.Continue?[Y/N]:y
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 24 version-3 send-packet-mode v2-only
```

12.2.49 vrrp vrid virtual-ip

Function

The **vrrp vrid virtual-ip** command creates a VRRP group and assigns a virtual IP address to the group.

The **undo vrrp vrid virtual-ip** command deletes the virtual IP address of a VRRP group.

By default, no VRRP group is created.

Format

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
virtual-ip *virtual-address*	Specifies the virtual IP address of a VRRP group.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, hosts use the default gateway to communicate with external networks. As value-added services such as IPTV or video conferencing services are widely deployed, hosts may fail to communicate with external networks if the default gateway fails. Configuring dynamic routing protocols such as RIP, OSPF, or ICMP can improve system reliability. However, it is difficult to configure dynamic routing protocols and some hosts may not support dynamic routing protocols. VRRP virtualizes multiple routing devices into a virtual router without changing the networking. The virtual router IP address is configured as the default gateway address.

If users on a network have the same reliability requirements, configure multiple virtual IP addresses for a VRRP group. By doing this, one virtual IP address serves one separate user group, and the default gateway address remains consistent regardless of changes in VRRP device locations. A VRRP group can be assigned a maximum of 16 virtual IP addresses.

Precautions

The MAC address of the VBDIF must differ from the virtual MAC address of the VRRP group. (The last two bits of the VRRP virtual MAC address are determined by the VRID. For example, The VRID of the virtual router composed of SwitchA and SwitchB is 3, so the MAC address of the VRRP group is 00-00-5E-00-01-03).

If all the virtual IP addresses in a VRRP group are deleted, the VRRP group is deleted automatically.

For VRRP4 or VRRP6 groups configured on a device, each VRID can be bound to a maximum of 16 ports.

After the **vrrp vrid virtual-ip** command is run on an interface, when the ARP entries learned by the interface are aged, the device sends ARP aging probe packets with the source IP address being the interface's IP address. The virtual IP address of the interface is not used as the source IP address.

When VRRP and static ARP are configured simultaneously, note the following points:

- When VRRP is configured on a VLANIF interface or Ethernet interface, the IP address corresponding to the VLANIF interface or Ethernet interface in a static ARP entry cannot be set to the virtual IP address of a VRRP group. Otherwise, services cannot be forwarded between devices. For example, if a static ARP entry contains IP address 10.1.1.1, the IP address 10.1.1.1 cannot be used as the virtual IP address.
- When VRRP is configured on a VLANIF interface or Ethernet interface, the virtual IP address of a VRRP group cannot be used as the IP address corresponding to the VLANIF interface or Ethernet interface in a static ARP entry. Otherwise, services cannot be forwarded between devices. For example, if the VRRP group uses virtual IP address 10.1.1.1, the IP address 10.1.1.1 cannot be used in a static ARP entry.

NOTE

- VRRP groups must use different virtual IP addresses.
- Two devices in a VRRP group must be configured with the same VRID.
- VRRP groups on different interfaces of a device can be configured with the same VRID.
- A virtual IP address must be different from the IP address of a user host. If the user host IP address is the same as the virtual IP address, all packets on the local network segment are sent to the user host. As a result, data of this network segment cannot be forwarded correctly.

Example

Create a VRRP group on VLANIF 100 with ID 1 and virtual IP address 10.10.10.10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.10.10.10
```

Create a VRRP group with VRID 1 and virtual IP address 10.10.10.10 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.10.10.10
```

12.2.50 vrrp6 nd send-mode simple

Function

The **vrrp6 nd send-mode simple** command enables a sub-interface for QinQ VLAN tag termination to send double-tagged ND packets carrying only the minimal inner VLAN ID when the VRRP status of the sub-interface in the Virtual Router Redundancy Protocol for IPv6 (VRRP6) backup group is master.

The **undo vrrp6 nd send-mode simple** command enables a sub-interface for QinQ VLAN tag termination to send double-tagged ND packets to all VLANs specified by the outer VLAN IDs and inner VLAN IDs when the VRRP status of the sub-interface in the VRRP6 backup group is master.

By default, double-tagged ND packets are sent to all VLANs specified by the outer VLAN IDs and inner VLAN IDs.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vrrp6 nd send-mode simple

undo vrrp6 nd send-mode simple

Parameters

None

Views

Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

A sub-interface for QinQ VLAN tag termination sends double-tagged ND packets when the VRRP status of the sub-interface in the VRRP backup group is master. If there is a range for the inner VLAN IDs, the sub-interface sends ND packets to all VLANs in this range to update VRRP backup group's MAC address entry on a downstream switch, exposing a heavy burden on the system. To prevent this problem, you can use the **vrrp6 nd send-mode simple** command to allow an ND packet carrying only the minimal inner VLAN ID to be sent, reducing the number of ND packets to be sent.

NOTE

The **vrrp6 nd send-mode simple** command takes effect within VLANs specified only by inner VLAN IDs rather than outer VLAN IDs. For example, VLAN IDs in the outer tag range from 1 to 10 and VLAN IDs in the inner tag range from 1 to 10. After the **vrrp6 nd send-mode simple** command is run, ND packets carrying only inner VLAN 1 and outer VLAN IDs ranging from 1 to 10 are sent. 10 ND packets (10 outer VLAN IDs x 1 inner VLAN ID) are sent.

The **vrrp6 nd send-mode simple** command is configured only on a sub-interface for QinQ VLAN tag termination.

Example

Allow ND packets carrying only inner VLAN 1 to be sent.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] qinq termination pe-vid 5 ce-vid 1 to 10
[HUAWEI-GigabitEthernet0/0/1.1] quit
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1.1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1.1] vrrp6 nd send-mode simple
```

12.2.51 vrrp6 un-check hop-limit

Function

The **vrrp6 un-check hop-limit** command disables the device from checking the TTL value in VRRP6 Advertisement packets.

The **undo vrrp6 un-check hop-limit** command enables the device to check the TTL value in VRRP6 Advertisement packets.

By default, the system checks the TTL value in VRRP6 Advertisement packets.

Format

vrrp6 un-check hop-limit

undo vrrp6 un-check hop-limit

Parameters

None

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

The device checks the TTL value in received VRRP6 Advertisement packets. If the TTL value of a VRRP6 Advertisement packet is not 255, the device discards the packet.

On certain networks, especially on a network where the device interworks with non-Huawei devices, valid packets may be discarded if TTL check is enabled. You can configure the device not to check the TTL value in VRRP6 Advertisement packets.

Example

Disable the device from checking the TTL value in VRRP6 Advertisement packets on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 un-check hop-limit
```

Disable the device from checking the TTL value in VRRP6 Advertisement packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 un-check hop-limit
```

12.2.52 vrrp6 vrid preempt-mode disable

Function

The **vrrp6 vrid preempt-mode disable** command configures the device in a VRRP6 group in non-preemption mode.

The **undo vrrp6 vrid preempt-mode** command restores the default preemption mode.

By default, the device uses the immediate preemption mode.

Format

vrrp6 vrid *virtual-router-id* **preempt-mode disable**

undo vrrp6 vrid *virtual-router-id* **preempt-mode**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device with higher priority in a VRRP6 group to be the master, set the preemption mode on the device. In non-preemption mode, as long as the master is working properly, the backup with higher priority cannot be the master.

NOTE

When non-preemption is disabled, the preemption delay is restored to 0 seconds immediately.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Example

Configure VRRP6 group 1 in non-preemption mode on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 preempt-mode disable
```

Configure VRRP6 group 1 in non-preemption mode on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 preempt-mode disable
```

12.2.53 vrrp6 vrid preempt-mode timer delay

Function

The **vrrp6 vrid preempt-mode timer delay** command sets the preemption delay for the device in a VRRP6 group.

The **undo vrrp6 vrid preempt-mode timer delay** command restores the default preemption delay for the device in a VRRP6 group.

By default, the preemption delay is 0 seconds, indicating immediate preemption.

Format

vrrp6 vrid *virtual-router-id* **preempt-mode timer delay** *delay-value*

undo vrrp6 vrid *virtual-router-id* **preempt-mode timer delay**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
delay *delay-value*	Specifies the preemption delay.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the backup in a VRRP6 group does not receive VRRP6 Advertisement packets from the master within a specified period of time, the backup becomes the master. On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP6 group status will flap and traffic is lost. To prevent frequent switching of the VRRP6 group status, run the **vrrp6 vrid preempt-mode timer delay** command to set the preemption delay so that the backup becomes the master only after the delay expires.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed to create a VRRP6 group.

Precautions

You are advised to set the preemption delay of the backup in a VRRP6 group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 15s. These settings allow a period of time for status synchronization between the uplink and downlink on devices on an unstable network. If the preceding settings are not used, two masters coexist and user devices may learn an incorrect master address. As a result, traffic is interrupted.

- The preemption delay refers to the delay before the backup switches to the master. Therefore, the IP address owner is irrelevant to the preemption delay. After the IP address owner recovers, it becomes the master immediately without a delay.
- On a stable network, a short preemption delay is recommended. When the master is faulty, the backup can rapidly switch to the master. This prevents traffic loss. On an unstable network, a long preemption delay is recommended. This prevents traffic loss caused by frequent switching of the VRRP6 group status.

Example

Set the preemption delay of VRRP6 group 1 to 10 seconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 preempt-mode timer delay 10
```

Set the preemption delay of VRRP6 group 1 to 10 seconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 preempt-mode timer delay 10
```

12.2.54 vrrp6 vrid priority

Function

The **vrrp6 vrid priority** command sets the priority of the device in a VRRP6 group.

The **undo vrrp6 vrid priority** command restores the default priority of the device in a VRRP6 group.

By default, the priority of the device in a VRRP6 group is 100.

Format

vrrp6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp6 vrid *virtual-router-id* **priority**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
priority *priority-value*	Specifies the priority of the device in a VRRP6 group.	The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the device in a VRRP6 group as the default gateway, run the **vrrp6 vrid priority** command to specify the highest priority for the device so that the device can become the master.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed to create a VRRP6 group.

Precautions

- Priority 0 is reserved in the system. Priority 255 is reserved for the IP address owner.
- When devices in a VRRP6 group have the same priority, the device that first changes to master state becomes the master. If devices attempt to be the master simultaneously, the device where the interface with the largest IP address is located becomes the master.

Example

Set the priority of the switch in VRRP6 group 2 to 120 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
```

```
[HUAWEI-Vlanif100] vrrp6 vrid 2 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 2 priority 120
```

Set the priority of the switch in VRRP6 group 2 to 120 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 2 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 2 priority 120
```

12.2.55 vrrp6 vrid timer advertise

Function

The **vrrp6 vrid timer advertise** command sets the interval at which the master sends VRRP6 Advertisement packets.

The **undo vrrp6 vrid timer advertise** command restores the default interval at which the master sends VRRP6 Advertisement packets.

By default, the master sends VRRP6 Advertisement packets every 1 second.

Format

vrrp6 vrid *virtual-router-id* **timer advertise** *advertise-interval*

undo vrrp6 vrid *virtual-router-id* **timer advertise**

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
advertise *advertise-interval*	Specifies the interval at which the master sends VRRP6 Advertisement packets.	The value is an integer that ranges from 100 to 4095, in centiseconds.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP6 group sends VRRP6 Advertisement packets to backups at intervals to notify that it is working properly. If the backup with the highest priority does not receive any VRRP6 Advertisement packets from the master at the specified interval (usually, three times the interval for sending VRRP6 Advertisement packets), it considers the master faulty and becomes the master. The **vrrp6 vrid timer advertise** command sets the interval at which the master sends VRRP6 Advertisement packets.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Precautions

If a longer interval is used, backups in the same VRRP6 group cannot detect the fault on the master in a timely manner, causing packet loss. If a shorter interval is used, system resources are occupied. In addition, when network traffic is heavy or the network is unstable, backups may not receive packets after the Master_Down_Interval timer expires. As a result, the VRRP6 group status is incorrectly switched. Set the interval based on actual networking.

NOTE

- For VRRP for IPv4, set the same interval for sending VRRP Advertisement packets for members in a VRRP group to prevent multiple masters in the VRRP group.
- For VRRP for IPv6, even if you set different intervals for sending VRRP Advertisement packets for members in a VRRP6 group, there is only one master in a VRRP6 group.

Example

Set the interval at which the master in VRRP6 group 1 sends VRRP6 Advertisement packets to 200 centiseconds on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 timer advertise 200
```

Set the interval at which the master in VRRP6 group 1 sends VRRP6 Advertisement packets to 200 centiseconds on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 timer advertise 200
```

12.2.56 vrrp6 vrid track admin-vrrp6 vrid

Function

The **vrrp6 vrid track admin-vrrp6 vrid** command binds a VRRP6 group to an mVRRP6 group.

The **undo vrrp6 vrid track admin-vrrp6** command unbinds a VRRP6 group from an mVRRP6 group.

By default, no VRRP6 group is bound to an mVRRP6 group.

Format

vrrp6 vrid *virtual-router-id1* **track admin-vrrp6 interface** *interface-type interface-number* **vrid** *virtual-router-id2* **unflowdown**

undo vrrp6 vrid *virtual-router-id1* **track admin-vrrp6**

Parameters

Parameter	Description	Value
vrid *virtual-router-id1*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
vrid *virtual-router-id2*	Specifies the VRID of an mVRRP6 group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface configured with an mVRRP6 group.	-
unflowdown	Allows the interface where a VRRP6 group bound to an mVRRP6 group is configured to retain the Up state if the mVRRP6 group is in Backup or Initialize state.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple VRRP6 groups are configured on the device, each group sends VRRP6 Advertisement packets to maintain its state machine. As a result, a large number of VRRP6 Advertisement packets are generated, which occupy network bandwidth resources and cause CPU performance to deteriorate. To solve the problem, run the **vrrp6 vrid track admin-vrrp6 vrid** command to bind a VRRP6 group to an mVRRP6 group. After a VRRP6 group is bound to an mVRRP6 group, the VRRP6 group does not send VRRP6 Advertisement packets to negotiate the Master and Backup states. The mVRRP6 group determines the status of the bound VRRP6 group. This method greatly reduces the impact of VRRP6 Advertisement packets on network bandwidth and CPU performance.

This mode is used on a network where uplink and downlink traffic can be transmitted along different paths. **unflowdown** can be configured to allow the mVRRP6 group to determine the status of its bound VRRP6 group. Uplink traffic travels through the master and then reaches the upper-layer network, and downlink traffic travels through either the master or backup to reach users.

Prerequisites

A VRRP6 group and an mVRRP6 group have been created.

Precautions

The **vrrp6 vrid track admin-vrrp6 vrid** command can be used only on the interface where the bound VRRP6 group is configured. This command cannot be used on the interface where an mVRRP6 group is configured.

VRRP4 and VRRP6 can be configured on an interface simultaneously. However, there are limitations:

- A VRRP4 group can be bound to only an mVRRP4 group, and a VRRP6 group can be bound to only an mVRRP6 group.
- At most one VRRP4 group and one VRRP6 group can be configured on an interface. An interface cannot be configured with multiple VRRP4 or VRRP6 groups.

Example

Bind VRRP6 group 1 to mVRRP6 group 2 on the VLANIF interface.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] vrrp6 vrid 1 track admin-vrrp6 interface vlanif 11 vrid 2 unflowdown
```

Bind VRRP6 group 1 to mVRRP6 group 2 on the Ethernet interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 track admin-vrrp6 interface gigabitethernet 0/0/2 vrid 2
unflowdown
```

12.2.57 vrrp6 vrid track bfd-session

Function

The **vrrp6 vrid track bfd-session** command associates a VRRP6 group with a BFD session.

The **undo vrrp6 vrid track bfd-session** command disassociates a VRRP6 group from a BFD session.

By default, a VRRP6 group is not associated with a BFD session.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

vrrp6 vrid *virtual-router-id* **track bfd-session** { *session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track bfd-session** [*session-id* | **session-name** *bfd-configure-name*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
session-id	Specifies the local discriminator of the monitored BFD session.	The value is an integer that ranges from 1 to 8191.
session-name *bfd-configure-name*	Specifies the name of the monitored BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
increased *value-increased*	Specifies the value by which the priority increases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored BFD session becomes Down, the VRRP6 priority decreases by 10.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between a VRRP6 group and a BFD session implements the following functions:

1. Rapid active/standby switchover: When the link of a VRRP6 group or the master is faulty, the backup becomes the master after a certain time (second level), causing packet loss. You can associate the VRRP6 group with a BFD session on the backup so that the BFD session can rapidly detect communication faults of the VRRP6 group. When the BFD session detects a fault, it notifies the VRRP6 group that the priority of the backup needs to be increased. Then an active/standby switchover is triggered immediately. This millisecond-level switchover reduces traffic loss. When the monitored BFD session recovers, the original priority of the device in the VRRP6 group is restored.
2. Monitoring the uplink: Because VRRP6 cannot detect faults on the uplink of a VRRP6 group, services are interrupted. You can associate the VRRP6 group with a BFD session on the master so that the BFD session monitors the uplink status of the master. When the BFD session detects a fault on the uplink, it notifies the VRRP6 group that the priority of the master needs to be decreased. Then an active/standby switchover is triggered immediately. This reduces the impact of the uplink fault on service forwarding. When the monitored BFD session recovers, the original priority of the device in the VRRP6 group is restored.

Prerequisites

A VRRP6 group has been created and a static BFD session or a static BFD session with automatically negotiated discriminators has been created.

Precautions

Currently, the device supports only association between VRRP6 and BFD for IPv4.

After a VRRP6 group is associated with a BFD session, the BFD session type cannot be modified. Before deleting the BFD session type, you must delete all original configurations.

After a VRRP6 group is associated with a BFD session, set an appropriate value of **increased** *value-increased* or **reduced** *value-reduced*. This setting ensures that an active/standby switchover is performed immediately when the monitored BFD session becomes Down.

Multiple VRRP6 groups can monitor a BFD session, and a VRRP6 group can monitor a maximum of eight BFD sessions simultaneously.

NOTE

When associating a VRRP6 group with a BFD session, note the following points:

- If an IPv6 address owner exists in the VRRP6 group, the VRRP6 group cannot monitor the BFD session.
- If **session-name** *bfd-configure-name* is specified, the VRRP6 group can be bound to only the static BFD session with automatically negotiated discriminators.
- If *session-id* is specified, the VRRP6 group can bind to only a static BFD session.

Example

Associate VRRP6 group 1 with the BFD session **hello** on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd hello bind peer-ip 10.1.1.1 interface vlanif 100
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FC00::100
[HUAWEI-Vlanif100] vrrp6 vrid 1 track bfd session-name hello reduced 40
```

Associate VRRP6 group 1 with the BFD session **hello** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd hello bind peer-ip 10.1.1.1 interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-hello] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FC00::100
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 track bfd session-name hello reduced 40
```

12.2.58 vrrp6 vrid track interface

Function

The **vrrp6 vrid track interface** command associates a VRRP6 group with an interface.

The **undo vrrp6 vrid track interface** command disassociates a VRRP6 group from an interface.

By default, a VRRP6 group is not associated with an interface.

Format

vrrp6 vrid *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface monitored by a VRRP6 group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
increased *value-increased*	Specifies the value by which the priority increases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored interface goes Down, the VRRP6 priority of the device decreases by 10.

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VRRP6 can only detect the status change of the interface on which a VRRP6 group is configured. VRRP6 cannot detect faults on the uplink interface of the master, causing service interruption. You can associate a VRRP6 group with a device interface that is not in the VRRP6 group. When the monitored interface is faulty, the priority of the master is reduced. This triggers an active/standby switchover and reduces the impact of services on the uplink interface. When the fault is rectified, the original master restores its priority and switches to the master to forward traffic.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Precautions

After a VRRP6 group is associated with an interface, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored interface becomes Down.

NOTE

- The master and backup in the VRRP6 group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If the device is the IPv6 address owner (the virtual router IPv6 address is used as the actual interface address), you cannot associate a VRRP6 group with an interface.
- If the IPv4 protocol status on the monitored interface configured with an IPv4 address changes, a new master in the VRRP6 group is selected. If the IPv6 protocol status on the monitored interface configured with an IPv6 address changes, the VRRP6 group remains unchanged.

Example

Associate VRRP6 group 1 with VLANIF 100 and set **reduced** *value-reduced* to 50 when VLANIF 100 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 200
[HUAWEI-Vlanif200] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-Vlanif200] vrrp6 vrid 1 virtual-ip FC00::2
[HUAWEI-Vlanif200] vrrp6 vrid 1 track interface vlanif 100 reduced 50
```

Associate VRRP6 group 1 with GE0/0/2 and set reduced *value-reduced* to 50 when GE0/0/2 becomes Down.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FC00::2
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 track interface gigabitethernet0/0/2 reduced 50
```

12.2.59 vrrp6 vrid virtual-ip

Function

The **vrrp6 vrid virtual-ip** command creates a VRRP6 group and assigns a virtual IPv6 address to the group.

The **undo vrrp6 vrid virtual-ip** command deletes the virtual IPv6 address of a VRRP6 group.

By default, no VRRP6 group is created.

Format

vrrp6 vrid *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]

undo vrrp6 vrid *virtual-router-id* [**virtual-ip** *virtual-ipv6-address* [**link-local**]]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
virtual-ip *virtual-ipv6-address*	Specifies the virtual IPv6 address of a VRRP6 group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
link-local	Indicates that a link-local address is used as the virtual IPv6 address of a VRRP6 group. The first virtual IPv6 address of a VRRP6 group must be a link-local address.	-

Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, MultiGE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, hosts use the default gateway to communicate with external networks. As value-added services such as IPTV or video conferencing services are widely deployed, hosts may fail to communicate with external networks if the default gateway fails. Configuring dynamic routing protocols such as RIPng, OSPFv3, or ICMPv6 can improve system reliability. However, it is difficult to configure dynamic routing protocols and some hosts may not support dynamic routing protocols. VRRP6 virtualizes multiple routing devices into a virtual router without changing the networking. The virtual router IPv6 address is configured as the default gateway address.

If users on a network have the same reliability requirements, configure multiple virtual IPv6 addresses for a VRRP6 group. By doing this, one virtual IPv6 address serves one separate user group, and the default gateway address remains consistent regardless of changes in VRRP6 device locations. A VRRP6 group can be assigned a maximum of 16 virtual IPv6 addresses.

Precautions

For VRRP4 or VRRP6 groups configured on a device, each VRID can be bound to a maximum of 16 ports.

If all the virtual IPv6 addresses in a VRRP6 group are deleted, the VRRP6 group is deleted automatically.

NOTE

- The first virtual IPv6 address of a VRRP6 group must be a link-local address. That is, you must run the **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* **link-local** command before assigning other virtual IPv6 addresses to the VRRP6 group.
- VRRP6 groups must use different virtual IP addresses.
- Two devices in a VRRP6 group must be configured with the same VRID.
- VRRP6 groups on different interfaces of a device can be configured with the same VRID.
- The VLANIF interface of a super VLAN does not support VRRP6.

Example

Configure a VRRP6 group on VLANIF 100 and configure the virtual IPv6 address FE80::7.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp6 vrid 1 virtual-ip FE80::7 link-local
```

Configure a VRRP6 group on GE0/0/1 and configure the virtual IPv6 address FE80::7.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
```

12.3 HSB Configuration Commands

12.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.3.2 bind-service

Function

The **bind-service** command binds an HSB service to an HSB group.

The **undo bind-service** command unbinds the HSB service from the HSB group.

By default, no HSB service is bound to an HSB group.

Format

bind-service *service-index*

undo bind-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The value is fixed as 0.

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB group synchronizes backup information and responds to link status changes through the HSB channel established by the HSB service. To make the HSB group work properly, bind an HSB service to the HSB group.

Prerequisites

An HSB group has been configured.

Example

Bind HSB service 0 to an HSB group.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] bind-service 0
```

12.3.3 display hsb statistics hsb-group

Function

The **display hsb statistics hsb-group** command displays statistics on processes of an HSB group.

Format

display hsb statistics hsb-group *group-index* **event**

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The fixed value is 0.
event	Indicates process statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hsb statistics hsb-group** command displays statistics on processes. Two main processes are involved: negotiation process and switching process.

Example

Display statistics on processes of the HSB public mechanism.

```
<HUAWEI> display hsb statistics hsb-group 0 event
Hot Standby Statistic Event:
----------------------------------------------------------
Hot Standby Group Dealed Vrrp Group Record:
  Local_Vrrp Peer_Vrrp  Batch_Status Systime
  BACKUP     BACKUP     Ind          2019-8-23 11:55:2
  MASTER     BACKUP     Ind          2019-8-23 11:55:8

Hot Standby Group Event Record:
  Run Independent Event    : 0
  Realtime Sync Event      : 0
  Delete Event(Snd, Recv)  : 0, 0
  Add Event(Snd, Recv)     : 0, 0
  Switch Event(Snd, Recv)  : 0, 0
  Finish Status(Cur, Total): 0, 0

Hot Standby Group Process Record:
```

```
Negotiate Start Entry                : 0
Negotiate Has Started                 : 0
Negotiate Start Send Pkt Failed       : 0

Negotiate Req Entry                  : 0
Negotiate Req Failed                 : 0
Negotiate Req Batch Status Error      : 0
Negotiate Req Vrrp Status Error       : 0
Negotiate Req Check Para Failed       : 0
Negotiate Req Notify Event Failed     : 0

Negotiate Del Entry                  : 0
Negotiate Del Batch Status Error      : 0
Negotiate Del Vrrp Status Error       : 0
Negotiate Del Send Pkt Failed         : 0


Negotiate Ack Entry                  : 0
Negotiate Ack Failed                 : 0
Negotiate Ack Batch Status Error      : 0
Negotiate Ack Vrrp Status Error       : 0
Negotiate Ack Notify Event Failed     : 0

Negotiate Add Entry                  : 0
Negotiate Add Batch Status Error      : 0
Negotiate Add Vrrp Status Error       : 0
Negotiate Add Send Pkt Failed         : 0

Negotiate End Entry                  : 0
Negotiate End Failed                 : 0
Negotiate End Batch Status Error      : 0
Negotiate End Vrrp Status Error       : 0
Negotiate End Batch Backup Mid Count  : 0

Switch Start Entry                   : 0
Switch Has Started                    : 0
Switch Start Send Pkt Failed          : 0

Switch Req Entry                     : 0
Switch Req Failed                    : 0
Switch Req Batch Status Error         : 0
Switch Req Notify Event Failed        : 0

Switch Switching Entry               : 0
Switch Switching Batch Status Error   : 0
Switch Switching Send Pkt Failed      : 0
Switch Switching Vrrp Changed         : 0
Switch Switching Notify Vrrp Failed   : 0

Switch End Entry                     : 0
Switch End Failed                    : 0
Switch End Batch Status Error         : 0
Switch End Vrrp Changed               : 0
Switch End Notify Vrrp Failed         : 0

HSB Group Vrrp All Master             : 0
HSB Group Vrrp All Backup             : 0
HSB Group Received All Master Event   : 0
HSB Group Received All Backup Event   : 0

HSB Group Notify All Group Event Error: 0
HSB Group Notify One Group Event Error: 0
HSB Group Receive Group Event Error   : 0
HSB Group Vrrp State Change Event     : 2
HSB Group Vrrp State Received Event   : 0
HSB Group Vrrp State Dealed Event     : 0
HSB Group Packet To Task Error        : 0
HSB Group Packet To Task Failed       : 0
```

```
 HSB Batch Backup Mid Error Count      : 0
----------------------------------------------------------
```

Table 12-25 Description of the display hsb statistics hsb-group command output

Item	Description
HSB Process/HSB Process ID	ID of an HSB process.
Hot Standby Statistic Event	Statistics about received and handled events of an HSB group.
Hot Standby Group Dealed Vrrp Group Record	Record of the VRRP group of which services are received and processed by the HSB group.
Local_Vrrp	Local VRRP group.
Peer_Vrrp	Remote VRRP group.
Batch_Status	Backup process status.
Systime	System time.
Hot Standby Group Event Record	Record of events notified by the backup service module and received events.
Run Independent Event	Number of events running independently.
Realtime Sync Event	Number of events synchronized in real time.
Delete Event(Snd, Recv)	Number of deleted events that are received or sent.
Add Event(Snd, Recv)	Number of added events that are received or sent.
Switch Event(Snd, Recv)	Number of switched events that are received or sent.
Finish Status(Cur, Total)	Number of current backup services or total number of backup services of which the backup process is complete.
Hot Standby Group Process Record	Statistics on backup processes of the HSB public mechanism.
Negotiate Start Entry	The master device starts to be negotiated.
Negotiate Has Started	Negotiating master and backup devices has started.
Negotiate Start Send Pkt Failed	Sending negotiation packets fails.
Negotiate Req Entry	Batch deletion of backup devices starts.
Negotiate Req Failed	The master device fails to send negotiation-start packets to the backup device.

Item	Description
Negotiate Req Batch Status Error	The backup process status is incorrect. The backup process status of the current backup group is not Independent.
Negotiate Req Vrrp Status Error	The VRRP group status is incorrect and is not Backup.
Negotiate Req Check Para Failed	The backup device checks that some backup parameters from the master device are invalid.
Negotiate Req Notify Event Failed	The backup device notifies that batch deleting backup services fails.
Negotiate Del Entry	Batch deleting firewall services on the backup device is complete.
Negotiate Del Batch Status Error	The backup device fails to check the negotiation process and is not none.
Negotiate Del Vrrp Status Error	The backup device fails to check the VRRP group status and is not Backup.
Negotiate Del Send Pkt Failed	The backup device fails to send batch deletion complete messages to the master device.
Negotiate Ack Entry	Batch backup on the master device starts.
Negotiate Ack Failed	The backup device notifies the master device that the negotiation end message fails to be sent.
Negotiate Ack Batch Status Error	The master device fails to check the negotiation process and is not Batch-Started.
Negotiate Ack Vrrp Status Error	The VRRP group status of the master device is incorrect and is not Master.
Negotiate Ack Notify Event Failed	The master device fails to notify batch backup events on the firewall forwarding plane.
Negotiate Add Entry	The master device receives a message indicating that batch backup on the firewall forwarding plane is complete.
Negotiate Add Batch Status Error	The master device fails to check the negotiation process and is not Batch-Adding.
Negotiate Add Vrrp Status Error	The master device fails to check the VRRP group status and is not Backup.

Item	Description
Negotiate Add Send Pkt Failed	The master device fails to send batch deletion complete messages to the backup device.
Negotiate End Entry	Negotiation ends.
Negotiate End Failed	The master device notifies the backup device that the negotiation end message fails to be sent.
Negotiate End Batch Status Error	The master device fails to check the negotiation process and is not Batch-Adding.
Negotiate End Vrrp Status Error	The VRRP group status is incorrect and is not Master.
Negotiate End Batch Backup Mid Count	Statistics about the services that indicate that batch backup ends and are received by the active device from the standby device.
Switch Start Entry	Switching starts.
Switch Has Started	Switch Has Started.
Switch Start Send Pkt Failed	Sending switching-start messages fails.
Switch Req Entry	The original master device responds to switching messages.
Switch Req Failed	The original backup device fails to initiate switching.
Switch Req Batch Status Error	The original master device fails to check the switching process status and is not Realtime.
Switch Req Notify Event Failed	The original master device fails to notify switching of backup services.
Switch Switching Entry	Switching is complete.
Switch Switching Batch Status Error	The original master device fails to check the switching process status and is not Switching.
Switch Switching Send Pkt Failed	The original backup service fails to send a message indicating that the switching is complete.
Switch Switching Vrrp Changed	During switching, the VRRP status of the original backup device changes.
Switch Switching Notify Vrrp Failed	During switching, the VRRP status of the backup device changes and is not Master. The change is notified to the remote device.
Switch End Entry	Switching ends.

Item	Description
Switch End Failed	The original backup device receives a message indicating the switching failure.
Switch End Batch Status Error	The original master device fails to check the switching process status and is not Switching.
Switch End Vrrp Changed	During switching, the VRRP status of the original backup device changes.
Switch End Notify Vrrp Failed	During switching, the VRRP status of the backup device changes and is not Backup. The change is notified to the remote device.
HSB Group Vrrp All Master	Number of times two master devices exist in a VRRP group.
HSB Group Vrrp All Backup	Number of times two backup devices exist in a VRRP group.
HSB Group Received All Master Event	Number of dual-active events received by the HSB group.
HSB Group Received All Backup Event	Number of dual-standby events received by the HSB group.
HSB Group Notify All Group Event Error	The HSB group fails to notify backup events of all VRRP groups.
HSB Group Notify One Group Event Error	The HSB group fails to notify backup events of a single VRRP group.
HSB Group Receive Group Event Error	The HSB group fails to receive a notification indicating that the backup service is complete.
HSB Group Vrrp State Change Event	VRRP group status change event.
HSB Group Vrrp State Received Event	Number of VRRP status events received by the HSB group.
HSB Group Vrrp State Dealed Event	Number of VRRP status change events processed and responded by the HSB group.
HSB Group Packet To Task Error	An error occurs when the HSB group delivers HSB service packets.
HSB Group Packet To Task Failed	The HSB group fails to deliver HSB service packets.
HSB Batch Backup Mid Error Count	Statistics about the IDs of the services that are processed incorrectly after batch backup ends.

12.3.4 display hsb statistics hsb-service

Function

The **display hsb statistics hsb-service** command displays statistics on packets or processes of the HSB public mechanism.

Format

display hsb statistics hsb-service *service-index* { **event** | **packet** }

Parameters

Parameter	Description	Value
service-index	Specifies the index of an HSB service.	The fixed value is 0.
packet	Indicates packet statistics.	-
event	Indicates process statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hsb statistics hsb-service** command displays statistics on received, sent, and discarded packets or processes of the HSB public mechanism.

Example

Display statistics on packets of the HSB public mechanism.

```
<HUAWEI> display hsb statistics hsb-service 0 packet
Hot Standby Service Packet Statistics:
---------------------------------------------------------
  Packet Sent      : 0
  Packet Received  : 0
  Packet ID Error : 0
  Packet Sent Dropped    : 0
  Packet Received Dropped : 0
---------------------------------------------------------
      Group and Group Register Module Packet:
   Group-ID/Module-ID  Packet Sent         Packet Recived
   0                    0                    0
   400c0000             0                    0
  ---------------------------------------------------------
```

Display statistics on processes of the HSB public mechanism.

```
<HUAWEI> display hsb statistics hsb-service 0 event
Hot Standby Service Process Record:
----------------------------------------------------------
  HSB Service Packet To Group Failed    : 0
  HSB Service Packet To Group Error     : 0
  HSB Service Packet To Task Error      : 0
  HSB Service Packet To Outer Error     : 0
  HSB Service Tunnel State Event        : 1
----------------------------------------------------------
```

Table 12-26 Description of the **display hsb statistics hsb-service** command output

Item	Description
Hot Standby Service Packet Statistics	Statistics on packets of the HSB public mechanism.
Packet Sent	Number of sent packets.
Packet Received	Number of received packets.
Packet ID Error	Packet loss times recorded in PKD ID detection when the HSB receives packets.
Packet Sent Dropped	Number of sent packets that are discarded.
Packet Received Dropped	Number of received packets that are discarded.
Group and Group Register Module Packet	Number of packets of the HSB group or of the module bound to the HSB group.
Group-ID/Module-ID	HSB group ID or module ID.
Hot Standby Service Process Record	Statistics on processes of the HSB public mechanism.
HSB Service Packet To Group Failed	An error occurs when the HSB service delivers HSB service packets to the HSB group.
HSB Service Packet To Group Error	Failure to deliver HSB service packets to the HSB group.
HSB Service Packet To Task Error	Failure to deliver HSB service packets to the backup service.
HSB Service Packet To Outer Error	Failure to deliver HSB service packets to the external module (HSB group or HSB service).
HSB Service Tunnel State Event	HSB service tunnel status event.

12.3.5 display hsb-group

Function

The **display hsb-group** command displays information about an HSB group.

Format

display hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the ID of an HSB group.	The value is 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about an HSB group.

Example

Display information about HSB group 0.

```
<HUAWEI> display hsb-group 0
Hot Standby Group Information:
----------------------------------------------------------
  HSB-group ID                : 0
  Vrrp Group ID               : 2
  Vrrp Interface              : Vlanif100
  Service Index               : 0
  Group Vrrp Status           : Master
  Group Status                : Active
  Group Backup Process        : Realtime
  Backup State                : Ended
  Peer Group Device Name      : -
  Peer Group Software Version : -
  Group Backup Modules        : -
```

Table 12-27 Description of the **display hsb-group** command output

Item	Description
HSB-group ID	ID of an HSB group.

Item	Description
Vrrp Group ID	VRRP group ID.
Vrrp Interface	Interface configured with the VRRP group.
Service Index	HSB service ID.
Group Vrrp Status	Status of the VRRP group: ● Master ● Backup ● Initialize ● None
Group Status	HSB group status: ● Active ● Inactive ● Independent ● Switching
Group Backup Process	Backup process status: ● Independent: independent backup state ● Batch-Started: batch backup negotiation state ● Batch-Deleting: batch deletion state ● Batch-Delete-End: batch deletion end state ● Batch-Adding: batch backup state ● Realtime: real-time backup state ● Switching: switching state
Backup State	Backup status of the HSB group: ● Processing: Backup has been completed for the main core but is still ongoing for the sub core. ● Ended: Backup has been completed for both the main core and sub core. ● -: Backup has not been completed for the main core.
Peer Group Device Name	Device name corresponding to the peer HSB group.
Peer Group Software Version	Software version corresponding to the peer HSB group.

Item	Description
Group Backup Modules	Service module bound to the HSB group.

12.3.6 display hsb-service

Function

The **display hsb-service** command displays information about an HSB service.

Format

display hsb-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The value is fixed as 0.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about an HSB service.

Example

Display the HSB service configuration.

```
<HUAWEI> display hsb-service 0
Hot Standby Service Information:
----------------------------------------------------------
  Local IP Address       : 192.168.4.1
  Peer IP Address        : 192.168.4.2
  Source Port            : 10245
  Destination Port       : 10245
  Keep Alive Times       : 5
  Keep Alive Interval    : 3
  Service State          : Not Valid
  Service Batch Modules  :
  Shared-key             : ******
----------------------------------------------------------
```

Table 12-28 Description of the **display hsb-service** command output

Item	Description
Local IP Address	IP address of the local device. To set this parameter, run the **service-ip-port** command.
Peer IP Address	IP address of the peer device. To set this parameter, run the **service-ip-port** command.
Source Port	Local port number. To set this parameter, run the **service-ip-port** command.
Destination Port	Destination port number. To set this parameter, run the **service-ip-port** command.
Keep Alive Times	Number of times that heartbeat packets are sent. To set this parameter, run the **service-keep-alive detect** command.
Keep Alive Interval	Interval for sending heartbeat packets. To set this parameter, run the **service-keep-alive detect** command.
Service State	Status of the HSB service: ● Connected ● Disconnected ● Not Valid
Service Batch Modules	Service modules bound to an HSB service.
Shared-key	Key used by the HSB devices. To set this parameter, run the **key** command.

12.3.7 display hsb-resource map

Function

The **display hsb-resource map** command displays HSB resource mapping information.

Format

display hsb-resource map

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view mappings between HSB logical resources and interfaces, run the **display hsb-resource map** command.

Example

Display HSB resource mapping information.

```
<HUAWEI> display hsb-resource map
Hot Standby Backup interface map Information:
HSB-interface           Interface
----------------------------------------------------------
hsb-interface512        Vlanif100
hsb-interface1          GigabitEthernet0/0/1
----------------------------------------------------------
Total number: 2
```

Table 12-29 Description of the **display hsb-resource map** command output

Item	Description
Hot Standby Backup interface map Information	Mapping information of the HSB backup interface.
HSB-interface	HSB logical interface.
Interface	Interface name.
Total number	Total number of interface mappings.

12.3.8 display hsb-service-type dhcp hsb-group

Function

The **display hsb-service-type dhcp hsb-group** command displays information about the HSB group bound to DHCP servers.

Format

display hsb-service-type dhcp hsb-group

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display hsb-service-type dhcp hsb-group** command to view information about the HSB group bound to DHCP servers.

Example

Display information about the HSB group bound to DHCP servers.

```
<HUAWEI> display hsb-service-type dhcp hsb-group
DHCP HSB Group Information:
----------------------------------------------------------
   DHCP HSB Group : 0
----------------------------------------------------------
```

Table 12-30 Description of the **display hsb-service-type dhcp hsb-group** command output

Item	Description
DHCP HSB Group	ID of the HSB group.

12.3.9 hsb enable

Function

The **hsb enable** command enables hot standby (HSB) in an HSB group.

The **undo hsb enable** command disables HSB in an HSB group.

By default, HSB is disabled.

Format

hsb enable

undo hsb enable

Parameters

None.

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB group takes effect and notifies the service modules of status changes only after the HSB group is enabled. You need to run the **hsb enable** command to enable HSB in an HSB group after the HSB group configuration is complete.

Precautions

Do not run the **undo hsb enable** command when the master and backup devices are performing batch backup.

The master and backup devices must be the same device type and use the same software version. Otherwise, the HSB function may become unavailable.

Example

Enable HSB in HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] hsb enable
```

12.3.10 hsb-group

Function

The **hsb-group** command creates an HSB group.

The **undo hsb-group** command deletes an HSB group.

By default, no HSB group is created.

Format

hsb-group *group-index*

undo hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the ID of an HSB group.	The value is fixed as 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure HSB functions, create an HSB group first. An HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization. An HSB group supports status negotiation and event notification functions, implementing service synchronization on master and backup devices.

Precautions

After HSB is enabled for an HSB group, an HSB service cannot be bound to the HSB group.

Example

Create HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0]
```

12.3.11 hsb-resource map

Function

The **hsb-resource map** command configures HSB resource mapping information.

The **undo hsb-resource map** command deletes HSB resource mapping information.

By default, no HSB resource mapping is configured.

Format

hsb-resource map interface *interface-type interface-number* **hsb-interface** *hsb-interface-number*

undo hsb-resource map interface *interface-type interface-number* **hsb-interface** *hsb-interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface: - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
hsb-interface *hsb-interface-number*	Specifies the index of an HSB logical interface.	The value is an integer in the range from 1 to 512.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the interface types and numbers on the active and standby devices are different, the standby device cannot back up interface-related entry information of the active device by default. As a result, services are interrupted after an active/ standby switchover. To solve this problem, run the **hsb-resource map** command on the active and standby devices to configure mappings between interfaces and HSB logical interfaces. The configuration will map interfaces of the active and standby devices to the same HSB logical interface so that the standby device can back up interface-related entry information of the active device based on the mappings.

Example

Configure mappings between interfaces and a specific HSB logical interface.

```
<HUAWEI> system-view
[HUAWEI] hsb-resource map interface vlanif 10 hsb-interface 1
```

12.3.12 hsb-service

Function

The **hsb-service** command creates an HSB service and displays the HSB service view.

The **undo hsb-service** command deletes an HSB service.

By default, no HSB service is created.

Format

hsb-service *service-index*

undo hsb-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The fixed value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An HSB service establishes an HSB channel for transmitting packets of other services and maintains the link status by notifying the HSB group of the faulty link. Only after an HSB group is bound to an HSB service, the HSB function can be implemented.

Example

Create HSB service 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0]
```

12.3.13 hsb-service-type dhcp hsb-group

Function

The **hsb-service-type dhcp hsb-group** command binds DHCP services to an HSB group.

The **undo hsb-service-type dhcp hsb-group** command unbinds DHCP services from an HSB group.

By default, DHCP services are not bound to an HSB group.

Format

hsb-service-type dhcp hsb-group *group-index*

undo hsb-service-type dhcp hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a DHCPv6 prefix delegation (PD) scenario, to ensure reachable routes between the DHCPv6 relay agent and terminals, you need to run the **hsb-service-type dhcp hsb-group** command to bind DHCP services to a specific HSB group. This configuration ensures that prefix routing information on the DHCPv6 relay agent can be backed up by the HSB group.

Prerequisites

An HSB group has been created using the **hsb-group** command.

Precautions

Services can be bound to an HSB group only before the HSB group is enabled.

This command applies only to the DHCPv6 PD scenario and must be configured on the DHCPv6 relay agent.

Example

Bind DHCP services to an HSB group.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] quit
[HUAWEI] hsb-service-type dhcp hsb-group 0
```

12.3.14 key

Function

The **key** command configures the key used by the HSB devices.

The **undo key** command deletes the key used by the HSB devices.

By default, the key used by HSB devices is not configured.

Format

key cipher *key-string*

undo key

Parameters

Parameter	Description	Value
cipher *key-string*	Indicates the key used by the HSB devices.	The value can be a string of 48 characters in cipher text or a string of 8 to 16 characters in plain text.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security of HSB information negotiation and service backup and prevent the attacks initiated by using bogus packets or modifying packets, run the **key** command to configure the key used by HSB devices. The key provides authentication and verification mechanisms.

Precautions

- Configuring a shared key for HSB devices is not recommended in a secure network environment, as this configuration will degrade the HSB performance.
- The **key** command must be configured before the **service-ip-port** command. Otherwise, the **key** configuration will fail.
- The two HSB devices must be configured with the same shared key. Inconsistent keys on two ends will cause frequent interruption of the HSB channel.

Example

Set the key used by HSB devices to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0] key cipher YsHsjx_202206
```

12.3.15 reset hsb statistics hsb-group

Function

The **reset hsb statistics hsb-group** command clears statistics on HSB processes.

Format

reset hsb statistics hsb-group *group-index* **event**

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The value is fixed as 0.
event	Indicates process statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting HSB statistics within a certain period, run this command to clear the existing HSB statistics. You can run this command to clear statistics about HSB processes. Two main processes are involved: HSB negotiation process and HSB switching process.

Example

Clear statistics about HSB processes.

```
<HUAWEI> reset hsb statistics hsb-group 0 event
```

12.3.16 reset hsb statistics hsb-service

Function

The **reset hsb statistics hsb-service** command clears statistics on packets or processes of the HSB public mechanism.

Format

reset hsb statistics hsb-service *service-index* { **packet** | **event** }

Parameters

Parameter	Description	Value
service-index	Specifies the index of an HSB service.	The value is fixed as 0.
packet	Indicates packet statistics.	-
event	Indicates process statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting HSB statistics within a certain period, run this command to clear the existing HSB statistics. You can run this command to clear statistics on packets or processes of the HSB public mechanism.

Example

Clear statistics on packets of the HSB public mechanism.

```
<HUAWEI> reset hsb statistics hsb-service 0 packet
```

Clear statistics on processes of the HSB public mechanism.

```
<HUAWEI> reset hsb statistics hsb-service 0 event
```

12.3.17 service-ip-port

Function

The **service-ip-port** command configures the IP address and port number of an HSB channel.

The **undo service-ip-port** command deletes the IP address and port number of an HSB channel.

By default, the IP address and port number of an HSB channel are not configured.

Format

service-ip-port local-ip { *local-ipv4-address* | *local-ipv6-address* } **peer-ip** { *peer-ipv4-address* | *peer-ipv6-address* } **local-data-port** *local-port* **peer-data-port** *peer-port*

undo service-ip-port local-ip { *local-ipv4-address* | *local-ipv6-address* } **peer-ip** { *peer-ipv4-address* | *peer-ipv6-address* } **local-data-port** *local-port* **peer-data-port** *peer-port*

Parameters

Parameter	Description	Value
local-ip { *local-ipv4-address* | *local-ipv6-address* }	Specifies the local IPv4 or IPv6 address of the HSB service.	- *local-ipv4-address*: The value is in dotted decimal notation. - *local-ipv6-address*: The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
peer-ip { *peer-ipv4-address* | *peer-ipv6-address* }	Specifies the peer IPv4 or IPv6 address of the HSB service.	- *peer-ipv4-address*: The value is in dotted decimal notation. - *peer-ipv6-address*: The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
local-data-port *local-port*	Specifies the local port number of the HSB service.	The value is an integer that ranges from 10240 to 49152.
peer-data-port *peer-port*	Specifies the peer port number of the HSB service.	The value is an integer that ranges from 10240 to 49152.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an HSB service using the **hsb-service** command, run the **service-ip-port** command to configure IP addresses and port numbers for the local and peer devices. When the configuration is complete, the HSB service establishes a Transmission Control Protocol (TCP) channel to transmit packets of other services and notifies service modules of link status changes.

Prerequisites

An HSB service has been created.

Precautions

It is recommended that the HSB channel be configured on an independent and highly reliable physical link.

If the command configuration fails to be restored, you cannot view the unrestored configuration information. In this case, you are advised to check whether the port is occupied by other services.

Example

Configure IP addresses and port numbers for the local and peer devices for the HSB service 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0] service-ip-port local-ip 192.168.1.1 peer-ip 192.168.1.2 local-data-port 10240
peer-data-port 10240
```

12.3.18 service-keep-alive detect

Function

The **service-keep-alive detect** command sets the retransmission times and interval of HSB packets.

The **undo service-keep-alive** command restores the default retransmission times and interval of HSB packets.

The default retransmission times is 5, and the default retransmission interval is 3 seconds.

Format

service-keep-alive detect retransmit *retransmit-times* **interval** *interval-value*

undo service-keep-alive [**detect retransmit** *retransmit-times* **interval** *interval-value*]

Parameters

Parameter	Description	Value
retransmit *retransmit-times*	Specifies the retransmission times of HSB packets.	The value is an integer that ranges from 1 to 20.
interval *interval-value*	Specifies the retransmission interval of HSB packets.	The value is an integer that ranges from 1 to 10, in seconds.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB service sends and retransmits HSB packets to prevent long TCP interruption that is not detected by the protocol stack. If a device does not receive an HSB packet from the peer device within the period (value of *retransmit-times* x value of *interval-value*), the local device receives a message indicating the exception and then re-establishes a channel to the peer.

Prerequisites

An HSB service has been configured.

Precautions

It is recommended that the product of the retransmission times of HSB packets multiplied by the retransmission interval of HSB packets be greater than or equal to the value of **Master_Down_Interval**. The value of **Master_Down_Interval** is calculated using the following formula: Master_Down_Interval = 3 x Advertisement_Interval + Skew_time, in seconds. For details, see **vrrp vrid timer advertise** and **vrrp6 vrid timer advertise**. It is recommended that the retransmission times and retransmission interval of HSB packets be set to their default values.

Example

Set the retransmission times of HSB service 0 to 5, and the retransmission interval to 1 second.

```
<HUAWEI> system-view
[HUAWEI] hsb-service 0
[HUAWEI-hsb-service-0] service-keep-alive detect retransmit 5 interval 1
```

12.3.19 track vrrp

Function

The **track vrrp** command binds an IPv4 VRRP group to an HSB group.

The **undo track vrrp** command unbinds an IPv4 VRRP group from an HSB group.

By default, no HSB group is bound to an IPv4 VRRP group.

Format

track vrrp vrid *virtual-router-id* **interface** *interface-type interface-number*

undo track vrrp [**vrid** *virtual-router-id* **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the ID of an IPv4 VRRP group bound to an HSB group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of the interface in an IPv4 VRRP group. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **track vrrp** command to bind a VRRP group to an HSB group. The HSB group negotiates the service status based on the VRRP status. By monitoring the changes in the bound HSB channel status and VRRP status, the HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization.

Prerequisites

An HSB group has been configured.

Example

Bind VLANIF100 in IPv4 VRRP group 4 to HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] track vrrp vrid 4 interface vlanif 100
```

12.3.20 track vrrp6

Function

The **track vrrp6** command binds an IPv6 VRRP group to an HSB group.

The **undo track vrrp6** command unbinds the IPv6 VRRP group from the HSB group.

By default, no IPv6 VRRP group is bound to an HSB group.

Format

track vrrp6 vrid *virtual-router-id* **interface** *interface-type interface-number*

undo track vrrp6 [**vrid** *virtual-router-id* **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the ID of an IPv6 VRRP group bound to an HSB group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of the interface in an IPv6 VRRP group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the HSB service is used, you need to run this command to bind a VRRP group to an HSB group. The HSB group negotiates the service status based on the VRRP status. By monitoring the changes in the bound HSB channel status and

VRRP status, the HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization.

Prerequisites

An HSB group has been configured.

Example

Bind IPv6 VRRP group 4 on VLANIF100 to HSB group 0.

```
<HUAWEI> system-view
[HUAWEI] hsb-group 0
[HUAWEI-hsb-group-0] track vrrp6 vrid 4 interface vlanif 100
```

12.4 DLDP Configuration Commands

12.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.4.2 display dldp

Function

The **display dldp** command displays the DLDP status of an interface or global DLDP status.

Format

display dldp [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DLDP status of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display dldp** command to view the DLDP status on the device.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

DLDP has been enabled in the interface view using the **dldp enable** command.

Precaution

You can run the **display dldp** command to view DLDP status only after enabling DLDP globally using the **dldp enable** command.

Example

Display the DLDP status on the device.

```
<HUAWEI> display dldp
DLDP global status: enable
DLDP interval: 10s
DLDP work-mode: enhance
DLDP authentication-mode: sha, password is ******
DLDP unidirectional-shutdown: auto
DLDP delaydown-timer: 4s
The number of enabled ports is: 1
The number of global neighbors is: 1
The max number of global neighbors is: 512
Interface GigabitEthernet0/0/1
 DLDP port state: advertisement
 DLDP link state: up
 The neighbor number of the port is: 1.
   Neighbor mac address:80fb-0636-792d
   Neighbor port index:49
   Neighbor state:two way
   Neighbor aged time(s):16
```

Display the DLDP status on GE0/0/1.

```
<HUAWEI> display dldp interface gigabitethernet 0/0/1
Interface GigabitEthernet0/0/1
 DLDP port state: advertisement
 DLDP link state: up
 The neighbor number of the port is: 1.
   Neighbor mac address:0001-0001-0001
   Neighbor port index:26
   Neighbor state:two way
   Neighbor aged time(s):206
```

Table 12-31 Description of the display dldp command output

Item	Description
DLDP global status	Global DLDP status. The value can be: ● enable: DLDP is enabled. ● disable: DLDP is disabled. To enable DLDP, use the **dldp enable** command.
DLDP interval	Interval for sending the Advertisement packets, in seconds. To set the interval, use the **dldp interval** command.
DLDP work-mode	Working mode of DLDP. The value can be: ● enhance ● normal To set the working mode of DLDP, use the **dldp work-mode** command.
DLDP authentication-mode	Authentication mode of DLDP packets. The value can be: ● none: DLDP packets are not authenticated. ● simple: DLDP packets are authenticated using plain-text passwords. ● md5: DLDP packets are authenticated using MD5. ● sha: DLDP packets are authenticated using SHA2-256. To set DLDP authentication mode, use the **dldp authentication-mode** command.
DLDP unidirectional-shutdown	Interface shutdown mode. The value can be: ● manual: Interfaces are manually shut down. ● auto: Interfaces are automatically shut down. To set the interface shutdown mode, use the **dldp unidirectional-shutdown** command.

Item	Description
DLDP delaydown-timer	Delay of an interface's response to a Port-Down event, in seconds. To set the delay, use the **dldp delaydown-timer** command.
The number of enabled ports is	Number of interfaces on which DLDP is enabled on a device.
The number of global neighbors is	Number of DLDP neighbors.
The max number of global neighbors is	The max number of global DLDP neighbors.

Item	Description
DLDP port state	Current DLDP status of an interface. The value can be: ● inactive: DLDP is enabled but the link is Down. ● active: DLDP is enabled and the link is Up, or entries of neighbors have been cleared. ● advertisement: All neighbors have established bidirectional connections or have been in Active state for at least 5 seconds. The link in this state is stable. ● probe: The interface receives a packet from an unknown neighbor. The interface then sends a probe packet to check whether the link is a unidirectional link. When an interface enters this state, DLDP starts the probe timer and starts an echo timer for each neighbor to be detected. ● disable: DLDP detects a unidirectional link or a neighbor disappears when DLDP works in enhanced mode. An interface in this state receives and forwards only BPDUs, not user traffic. ● delaydown: When DLDP is in Active, Advertisement, or Probe state, it has not entered the Inactive state when receiving a Port-Down event. An interface in delaydown state retains the DLDP neighbor information and starts the DelayDown timer. ● loop: Indicates that a loop occurs on the interface because the Rx and Tx of an optical module are connected by the same optical fiber.
DLDP link state	Status of the interface. ● up ● down
The neighbor number of the port	Number of neighbors of an interface.
Neighbor mac address	MAC address of a peer device.

Item	Description
Neighbor port index	Index of a peer port.
Neighbor state	Peer status. - unknown - one way - two way
Neighbor aged time(s)	Time period after which a peer ages, in seconds.

12.4.3 display dldp statistics

Function

The **display dldp statistics** command displays the statistics about DLDP packets on an interface.

Format

display dldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about DLDP packets on a specified DLDP interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If no interface is specified, the statistics about DLDP packets on all DLDP interfaces are displayed. If an interface is specified, the statistics about DLDP packets on the specified interface are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If DLDP negotiation fails, you can use the **display dldp statistics** command to check the statistics about DLDP packets. This command can be used to display the statistics about DLDP packets after the statistics about DLDP packets are cleared using the **reset dldp statistics** command.

Prerequisites

DLDP has been enabled globally and on interfaces using the **dldp enable** command.

Example

Display the statistics about DLDP packets on the device.

```
<HUAWEI> display dldp statistics
Interface : GigabitEthernet0/0/1
 Packets sent: 15
 Packets received: 0
 Invalid packets received: 0
 Loop packets received: 0
 Authentication failed packets received: 0
 Valid packets received: 0
```

Display the statistics about DLDP packets on GE0/0/1.

```
<HUAWEI> display dldp statistics interface gigabitethernet 0/0/1
Interface : GigabitEthernet0/0/1
 Packets sent: 0
 Packets received: 0
 Invalid packets received: 0
 Loop packets received: 0
 Authentication failed packets received: 0
 Valid packets received: 0
```

Table 12-32 Description of the **display dldp statistics** command output

Item	Description
Interface	Name of the port on which DLDP is enabled.
Packets sent	Number of DLDP sent packets.
Packets received	Number of DLDP received packets.
Invalid packets received	Number of DLDP erroneous packets that are received.

Item	Description
Loop packets received	Number of DLDP loop packets that are received.
Authentication failed packets received	Number of DLDP received packets that fail to pass the authentication.
Valid packets received	Number of DLDP valid packets that are received.

12.4.4 dldp authentication-mode

Function

The **dldp authentication-mode** command configures a DLDP authentication mode.

The **undo dldp authentication-mode** command restores the default DLDP authentication mode.

By default, DLDP packets are not authenticated.

Format

dldp authentication-mode { **md5** *md5-password* | **simple** *simple-password* | **sha** *sha-password* | **none** }

undo dldp authentication-mode [**md5** *md5-password* | **simple** *simple-password* | **sha** *sha-password* | **none**]

Parameters

Parameter	Description	Value
md5 *md5-password*	Uses MD5 to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *md5-password* specifies the MD5 authentication password. **NOTE** The password is saved in the configuration file in cipher text for security.	The value is a string of 6 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces. **NOTE** Ciphertext passwords with various lengths configured in an earlier version are also supported in the existing version.

Parameter	Description	Value
simple *simple-password*	Uses the plain text to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *simple-password* specifies the plain-text authentication password. **NOTE** The password is saved in the configuration file in cipher text for security.	The value is a string of 6 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces. **NOTE** Ciphertext passwords with various lengths configured in an earlier version are also supported in the existing version.
none	Performs no authentication on DLDP packets exchanged between the interfaces on the local and neighbor devices.	-
sha *sha-password*	Uses SHA2-256 mode to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *sha-password* specifies the SHA2-256 authentication password. **NOTE** The password is saved in the configuration file in cipher text for security.	The value is a string of 6 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces. **NOTE** Ciphertext passwords with various lengths configured in an earlier version are also supported in the existing version.

NOTE

For security purposes, you are advised to use SHA2-256 as the authentication algorithm of DLDP.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure packet validity on an insecure network, users can configure one of the following authentication modes for DLDP packets:

- None: The sender sets the authentication key of the DLDP packets to all 0s and the authentication type field to 0. The receiver compares the authentication key and authentication type with those set on the local end. If the settings on the two ends are different, the receiver discards the DLDP packets.
- Plain text: The sender sets the authentication key of the DLDP packets to the plain-text password set on the local end and the authentication type field to 1. The receiver compares the authentication key and authentication type with those set on the local end. If the settings on the two ends are different, the receiver discards the DLDP packets.
- MD5: The sender sets the authentication key of the DLDP packets to the summary of the cipher text obtained from the password set on the local end using the MD5 algorithm, and sets the authentication type field to 2. The receiver compares the authentication key and authentication type with the summary of the cipher text obtained on the local end using the MD5 algorithm. If the settings on the two ends are different, the receiver discards the DLDP packets.
- SHA2-256 authentication: The sender sets the authenticator field of the DLDP packets to the digest of the cipher text obtained from the password set on the local end using the SHA2-256 algorithm, and sets the authentication type field to 3. The receiver compares the authenticator and authentication type with the digest of the cipher text obtained on the local end using the SHA2-256 algorithm. If the settings on the two ends are different, the receiver discards the DLDP packets.

When the device that uses MD5 authentication is upgraded from V200R001 or V200R002 to V200R008 or later, to ensure compatibility, upgrade the DLDP authentication mode to MD5-compatible. You can run the **undo dldp authentication-mode md5-compatible** command to cancel MD5-compatible authentication.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

If the **dldp authentication-mode** command is executed while DLDP is running, the local device deletes information about the DLDP neighbor device and triggers the neighbor device to clear information about the local device. In this way, the negotiation can be re-performed.

If the DLDP authentication mode is set, ensure that the local and neighbor devices are configured with the same DLDP authentication mode and password. If they use different DLDP authentication modes or passwords, DLDP packets cannot be authenticated. DLDP can work properly only when the two interfaces are authenticated.

Example

Configure simple authentication for DLDP packets exchanged between two devices. Set the SHA2-256 password to YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dldp authentication-mode sha YsHsjx_202206
```

12.4.5 dldp compatible-mode enable

Function

The **dldp compatible-mode enable** command enables the DLDP compatible mode.

The **undo dldp compatible-mode enable** command disables the DLDP compatible mode.

By default, the DLDP compatible mode is disabled.

Format

dldp compatible-mode enable

undo dldp compatible-mode enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This configuration is required if the device works with the following Huawei switches to provide the DLDP function:

- S8500
- S7800
- S6500
- S5600 series

- S5100-EI
- S3900 series
- S3500 series
- S3100 series

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

If two devices are connected by two cross-connected links, the DLDP compatible mode must be enabled or disabled on both the two interfaces.

If two devices are Huawei devices (not preceding models), the DLDP compatible mode must be enabled or disabled on both the two interfaces.

Example

Enable the DLDP compatible mode on interfaceGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp enable
[HUAWEI-GigabitEthernet0/0/1] dldp compatible-mode enable
```

12.4.6 dldp compatible-mode local-mac

Function

The **dldp compatible-mode local-mac** command configures the switch to send DLDP packets containing source MAC addresses in the DLDP compatible mode.

The **undo dldp compatible-mode local-mac** command restores the source MAC addresses of the DLDP packets to the default MAC address.

By default, the MAC address of a DLDP packet is the system MAC address.

Format

dldp compatible-mode local-mac *mac-address*

undo dldp compatible-mode local-mac [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address of the DLDP packets sent in the DLDP compatible mode.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits. **NOTE** The source MAC address cannot be a multicast MAC address, a broadcast MAC address, or a reserved address.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run **dldp compatible-mode local-mac** command to configure the source MAC addresses for DLDP packets sent in DLDP compatible mode. This prevents the DLDP flapping due to discovery of multiple neighbors when the device needs to work with the following Huawei switches:

- S8500
- S7800
- S6500
- S5600 series switches
- S5100-EI
- S3900 series switches
- S3500 series switches
- S3100 series switches

Prerequisites

The DLDP compatible mode has been enabled using the **dldp compatible-mode enable** command.

Precautions

When the configuration is complete, the newly configured MAC address is used as the source MAC addresses of the sent DLDP packets.

Example

Set the source MAC address of the DLDP packets sent by interface GE0/0/1 in DLDP compatible mode to 00e0-fc12-0011.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp enable
[HUAWEI-GigabitEthernet0/0/1] dldp compatible-mode enable
[HUAWEI-GigabitEthernet0/0/1] dldp compatible-mode local-mac 00e0-fc12-0011
```

12.4.7 dldp delaydown-timer

Function

The **dldp delaydown-timer** command sets the timeout value of the DelayDown timer.

The **undo dldp delaydown-timer** command restores the default timeout value of the DelayDown timer.

The default timeout value of the DelayDown timer is 1 second.

Format

dldp delaydown-timer *time*

undo dldp delaydown-timer [*time*]

Parameters

Parameter	Description	Value
time	Specifies the timeout value of the DelayDown timer.	The value is an integer ranging from 1 to 5, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a DLDP interface in Active, Advertisement, or Probe state receives a Port-Down event, the interface enters Inactive state and clears the neighbor information. In some cases, the interface is Down for a short time. For example, failure of the Tx fiber on a port may cause jitter of optical signals on the Rx fiber, which makes the port Down and then Up again. To prevent the neighbor information from being deleted immediately in this case, the DLDP interface first enters the DelayDown state and starts the DelayDown timer. Before the DelayDown timer times out, the interface retains the neighbor information and responds to only Port-Up events. You can use the **dldp delaydown-timer** command to set the timeout value of the DelayDown timer.

- If the DLDP interface does not receive any Port-Up event when the DelayDown timer times out, the interface deletes the neighbor entry and enters the Inactive state.
- If the DLDP interface receives the Port-Up event before the DelayDown timer times out, the interface returns to the previous state.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

After the **dldp delaydown-timer** command is executed, the DLDP status is not affected by the Up/Down jitter within the timeout value of the DelayDown timer.

Example

Set the timeout value of the DelayDown timer to 2 seconds.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp delaydown-timer 2
```

12.4.8 dldp enable

Function

The **dldp enable** command enables DLDP.

The **undo dldp enable** command disables DLDP.

By default, DLDP is disabled globally and on each interface.

Format

dldp enable

undo dldp enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sometimes unidirectional links occur on networks. On a unidirectional link, the local device can receive packets from the peer device at the link layer, but the peer device cannot receive packets from the local device. Unidirectional links result in problems such as loops on an STP topology.

DLDP is used to monitor the link status of optical fibers or copper twisted pairs. If a unidirectional link exists, DLDP automatically shuts down the interface or prompts users to manually shut down the interface to prevent network faults.

To enable DLDP, run the **dldp enable** command to globally enable DLDP and then run this command on the interface.

Prerequisites

DLDP takes effect only when the physical link is connected; therefore, securely connect optical fibers or copper twisted pairs before enabling DLDP.

Precautions

- After you enable DLDP using the **dldp enable** command in the system view, run this command again on the interfaces to enable DLDP so that the interfaces can properly transmit and receive DLDP packets.
- If DLDP is disabled in the system view, DLDP is disabled on all interfaces, and all the DLDP configurations are deleted, which cannot be restored.
- Unidirectional links can be detected only for GE optical modules.

Example

Enable DLDP globally.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
```

Enable DLDP on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp enable
```

12.4.9 dldp interval

Function

The **dldp interval** command sets the interval for sending Advertisement packets.

The **undo dldp interval** command restores the default interval for sending Advertisement packets.

The default interval for sending Advertisement packets is 5 seconds.

Format

dldp interval *interval*

undo dldp interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Advertisement packets.	The value is an integer ranging from 1 to 100, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

An interface in Advertisement state sends Advertisement packets. DLDP creates a neighbor entry, starts the entry timer, and transits to the Probe state if the neighbor entry does not exist on the peer interface. DLDP updates the entry timer if the neighbor entry exists.

You can adjust the interval for sending Advertisement packets to allow DLDP to detect unidirectional links on different networks.

The interval for sending Advertisement packets must be smaller than one third of the STP convergence time.

- If the interval is too long, STP loops occur before a unidirectional link is shut down on a DLDP interface, which may lead to forwarding of many error packets.
- If the interval is too short, the traffic volume on the network increases.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

After the **dldp interval** command is executed, the local device running DLDP deletes information about the peer device and triggers the peer device to clear information about the local device. In this way, the negotiation can be re-performed.

Ensure that the interval for sending Advertisement packets is set to the same value on the local and peer devices connected through optical fibers or copper twisted pairs.

Example

Set the interval for sending Advertisement packets to 20 seconds on all DLDP interfaces.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp interval 20
```

12.4.10 dldp reset

Function

The **dldp reset** command resets the DLDP status of an interface so that the interface re-detects unidirectional links.

Format

dldp reset

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a unidirectional link is detected, the corresponding interface enters the Disable state. The system prompts you to shut down the interface or automatically sets the interface state to DLDP Down according to the configuration. To enable the interface to detect unidirectional links again, you can reset the DLDP status of the interface as follows:

- If the interface is shut down using the **shutdown (interface view)** command, run the **undo shutdown (interface view)** command to enable the interface to detect unidirectional links again. If the system automatically sets the interface state to DLDP Down, wait the interface to recover using the auto recovery mechanism after the link state becomes bidirectional using the auto recovery mechanism.

- Run the **dldp reset** command to restore the interface. The DLDP status of the interface after recovery depends on the physical status of the port. If the physical status is Down, the DLDP status of the interface changes to Inactive. If the physical status is Up, the DLDP status changes to Active.

You can reset the DLDP status globally or on the interfaces.

- When you run the **dldp reset** command in the interface view, the command takes effect only on this interface.
- When you run the **dldp reset** command in the system view, the command takes effect on all disabled interfaces.

Prerequisites

- If you run this command in the system view, ensure that DLDP has been enabled globally using the **dldp enable** command.
- If you run this command in the interface view, ensure that DLDP has been enabled globally and on the interfaces using the **dldp enable** command.

Example

Reset the DLDP status of all disabled interfaces.

```
<HUAWEI> system-view
[HUAWEI] dldp reset
```

Reset the DLDP status of disabled interfaceGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dldp reset
```

12.4.11 dldp unidirectional-shutdown

Function

The **dldp unidirectional-shutdown** command sets the shutdown mode if DLDP detects a unidirectional link on an interface.

The **undo dldp unidirectional-shutdown** command restores the default shutdown mode if DLDP detects a unidirectional link on an interface.

By default, an interface is shut down automatically if DLDP detects a unidirectional link on the interface.

Format

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown [**auto** | **manual**]

Parameters

Parameter	Description	Value
auto	Specifies the automatic mode.	-

Parameter	Description	Value
manual	Specifies the manual mode. When the traffic is heavy or CPU usage is high, the manual shutdown mode is recommended.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When DLDP detects a unidirectional link on an interface, run the **dldp unidirectional-shutdown** command to configure the shutdown mode for the interface. The following shutdown modes are available:

- Manual mode: This mode can prevent DLDP from shutting down the port immediately when the network performance is poor. This leads to failure in packet forwarding. It is a compromise mode used to prevent interface shutdown due to incorrect judgment of the system. In this mode, DLDP detects unidirectional links, and the network administrator manually shuts down the interface. When the DLDP state machine detects a unidirectional link, the system sends trap messages to prompt the network administrator to shut down the interface. Then the DLDP state machine changes to the Disable state.
- Automatic mode: It is the default mode. When a unidirectional link is detected, the DLDP state machine changes to the Disable state, records the trap messages, and sets the interface status to Blocking.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Precautions

When the traffic is heavy or CPU usage is high, the manual shutdown mode is recommended.

Example

Configure DLDP to automatically shut down an interface when a unidirectional link is detected.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp unidirectional-shutdown auto
```

12.4.12 dldp work-mode

Function

The **dldp work-mode** command sets the working mode of DLDP.

The **undo dldp work-mode** command restores the default working mode of DLDP.

By default, the working mode of DLDP is enhance.

Format

dldp work-mode { **enhance** | **normal** }

undo dldp work-mode [**enhance** | **normal**]

Parameters

Parameter	Description	Value
enhance	Indicates enhance mode of DLDP.	-
normal	Indicates normal mode of DLDP.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A unidirectional link fault may be caused by cross connections of optical fibers or disconnection of one optical fiber. You can use the **dldp work-mode** command to set the working mode of DLDP to detect the preceding two types of unidirectional links.

DLDP can work in either of the following working modes:

- Normal: DLDP does not automatically detect a neighbor when aging out a neighbor entry. In this mode, the system can identify only unidirectional links caused by cross connections of optical fibers. When the aging timer of a neighbor times out, the local end deletes the entry of the neighbor and sends an Advertisement packet with an RSY tag.

- Enhance: DLDP automatically detects a neighbor when aging out a neighbor entry. In this mode, the system can identify unidirectional links caused by cross connections of optical fibers or disconnection of one optical fiber. In this mode, when the aging timer of a neighbor times out, the local end starts the enhance timer and consecutively sends eight Probe packets to detect the neighbor, at the rate of one packet per second. If the local end does not receive any Echo packet from the neighbor when the Echo timer times out, DLDP enters the Disable state.

Prerequisites

DLDP has been enabled globally using the **dldp enable** command.

Example

Set the working mode of DLDP to enhance.

```
<HUAWEI> system-view
[HUAWEI] dldp enable
[HUAWEI] dldp work-mode enhance
```

12.4.13 reset dldp statistics

Function

The **reset dldp statistics** command deletes the statistics about DLDP packets on an interface.

Format

reset dldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Deletes the statistics about DLDP packets on a specified DLDP interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If no interface is specified, the statistics about DLDP packets on all DLDP interfaces are deleted. If an interface is specified, the statistics about DLDP packets on the interface are deleted.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting statistics about DLDP packets on an interface in a specified period, you can run the **reset dldp statistics** command to delete the existing DLDP packet statistics on the interface.

Precautions

The **reset dldp statistics** command deletes the statistics about DLDP packets. Exercise caution when running this command.

Example

Delete the statistics about DLDP packets on all DLDP interfaces.

```
<HUAWEI> reset dldp statistics
```

12.5 Smart Link And Monitor Link Configuration Commands

12.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.5.2 display monitor-link group

Function

The **display monitor-link group** command displays information about a specified Monitor Link group or all Monitor Link groups.

Format

display monitor-link group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays information about all Monitor Link groups.	-
group-id	Displays information about the specified Monitor Link groups.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After creating a Monitor Link group and adding uplink and downlink interfaces to the group, run this command to view the information about the group. The displayed information includes the name and status of each member interface.

Prerequisites

A Monitor Link group has been created using the **monitor-link group** command, and uplink and downlink interfaces have been added to the Monitor Link group using the **port** command.

Example

Display information about Monitor Link group 1.

```
<HUAWEI> display monitor-link group 1
Monitor Link group 1 information :
Recover-timer is 3 sec.
----------------------------------------------------------------------------------------------------
Member                 Role     State Last-up-time                    Last-down-time
----------------------------------------------------------------------------------------------------
GigabitEthernet0/0/1   UpLk     DOWN  0000/00/00 00:00:00 UTC+00:00      0000/00/00 00:00:00 UTC
+00:00
GigabitEthernet0/0/2   DwLk[1]  DOWN  0000/00/00 00:00:00 UTC+00:00      0000/00/00 00:00:00 UTC
+00:00
<HUAWEI> display monitor-link group 1
Monitor Link group 1 information :
Recover-timer is 3 sec.
----------------------------------------------------------------------------------------------------
Member                 Role     State Last-up-time                    Last-down-time
----------------------------------------------------------------------------------------------------
GigabitEthernet0/0/1   UpLk     DOWN  0000/00/00 00:00:00 UTC+00:00      0000/00/00 00:00:00 UTC
+00:00
GigabitEthernet0/0/2   UpLk     DOWN  0000/00/00 00:00:00 UTC+00:00      0000/00/00 00:00:00 UTC
+00:00
GigabitEthernet0/0/3   DwLk[1]  DOWN  0000/00/00 00:00:00 UTC+00:00      0000/00/00 00:00:00 UTC
+00:00
```

Table 12-33 Description of the display monitor-link group command output

Item	Description
Recover-timer	Wait-to-Restore time of the Monitor Link group, expressed in seconds. Use the **timer recover-time** command to set this parameter.
Member	Member interface of a Monitor Link group.
Role	Role of a member interface. ● UpLk: An uplink. ● DwLk[1]: A downlink. The number within the square brackets specifies a downlink ID.
State	Physical status of a member interface. ● UP: The member interface is in the Up state. ● DOWN: The number interface is in the Down state.

Item	Description
Last-up-time	Time when the member interface becomes Up for the last time. The format is YYYY/MM/DD HH:MM:SS UTC+HH:MM. If no record indicates that the interface is switched from Down to Up, the time is displayed as 0000/00/00 00:00:00 UTC +00:00.
Last-down-time	Time when the member interface becomes Down for the last time. The format is YYYY/MM/DD HH:MM:SS UTC+HH:MM. If no record indicates that the interface is switched from Up to Down, the time is displayed as 0000/00/00 00:00:00 UTC +00:00.

12.5.3 display monitor-link protocol-parameter group

Function

The **display monitor-link protocol-parameter group** command displays internal data of all Monitor Link groups or a specified Monitor Link group, including member interface information and Monitor Link configuration.

Format

display monitor-link protocol-parameter group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays internal data of all Monitor Link groups.	-
group-id	Displays internal data of a specified Monitor Link group.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays internal data of Monitor Link groups for diagnosis. You can use this command to check internal status data of a Monitor Link group.

Example

Display the internal data of Monitor Link group 1.

```
<HUAWEI> display monitor-link protocol-parameter group 1
MONITOR-LINK Group 1:
********************************
 *RecoverTime:        3 sec.
 *TimeCounter:        0 sec.
 *Uplink Info:
  IfIndex:            357(GigabitEthernet4/0/40/0/4)
  PortType:           2(MTLK_PORT_SWITCH)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Downlink 1 Info:
  IfIndex:            358(GigabitEthernet4/0/50/0/5)
  LinkStatus:         0(down)
  IsShutdown:         1(shutdown)
<HUAWEI> display monitor-link protocol-parameter group 1
MONITOR-LINK Group 1:
********************************
 *RecoverTime:        3 sec.
 *TimeCounter:        0 sec.
 *Uplink Info:
  IfIndex:            357(GigabitEthernet4/0/40/0/4)
  PortType:           2(MTLK_PORT_SWITCH)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Uplink Info:
  IfIndex:            358(GigabitEthernet4/0/50/0/5)
  PortType:           2(MTLK_PORT_SWITCH)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:     0
   MTLK Group ID:     1
   Role:              4(uplink)
 *Downlink 1 Info:
  IfIndex:            359(GigabitEthernet4/0/60/0/6)
  LinkStatus:         0(down)
  IsShutdown:         1(shutdown)
```

Table 12-34 Description of the display monitor-link protocol-parameter group command output

Item	Description
MONITOR-LINK Group 1	ID of a Monitor Link group.

Item	Description
RecoverTime	Wait-to-restore (WTR) time of the Monitor Link group The WTR time can be set using the **timer recover-time** command.
TimeCounter	WTR timer counter value.
Uplink Info	Information about the uplink interface in the Monitor Link group.
IfIndex	Interface index.
PortType	Type of the interface. ● 0(MTLK_PORT_UNKOWN): invalid interface type ● 1(MTLK_PORT_SMLK): Smart Link group ● 2(MTLK_PORT_SWITCH): Ethernet or Eth-Trunk interface
LinkStatus	Link status of an interface: ● 0(down) ● 1(up)
IFNET_S	Mnemonic symbol, indicating information saved on an interface.
SMLK Group ID	ID of a Smart Link group.
MTLK Group ID	ID of a Monitor Link group.
Role	Role of an interface in the Monitor link group.
Ctrl Vlan	Control VLAN.
Password	Password of Flush packets.
Downlink 1 Info	Information about downlink interface 1.
IsShutdown	Whether the downlink interface is shut down.

12.5.4 display smart-link flush

Function

The **display smart-link flush** command displays information about received Flush packets.

Format

display smart-link flush

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display smart-link flush** command displays information about received Flush packets, which helps you learn about link switchover information and identify interface faults. To delete information about received Flush packets, run the **reset smart-link flush** command.

Precautions

The master and slave interfaces of the Smart Link group are both in Down state. When the master interface or slave interface becomes Up, statistics on Flush packets may be inaccurate.

Prerequisites

The downstream device has been enabled to send Flush packets using the **flush send** command and the local device has been enabled to receive Flush packets using the **smart-link flush receive** command.

Follow-up Procedure

If the current information about Flush packets is no longer needed, run the **reset smart-link flush** command to delete the information.

Example

Display information about the received Flush packets.

```
<HUAWEI> display smart-link flush
Receive flush packets count:              1191
Receive last flush interface:             GigabitEthernet0/0/1
Receive last flush packet time:           02:42:37 UTC+03:00 2009/11/27
Receive last flush packet source mac:     00e0-fc00-0140
Receive last flush packet control vlan ID: 311
```

Table 12-35 Description of the display smart-link flush command output

Item	Description
Receive flush packets count	Number of Flush packets received.
Receive last flush interface	Interface that receives the latest Flush packet.

Item	Description
Receive last flush packet time	Time when the latest Flush packet is received, in any of the following formats: - HH:MM:SS YYYY-MM-DD - HH:MM:SS UTC±HH:MM DST YYYY-MM-DD - HH:MM:SS UTC±HH:MM YYYY-MM-DD - HH:MM:SS DST YYYY-MM-DD UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Receive last flush packet source mac	Source MAC address of the latest Flush packet received.
Receive last flush packet control vlan ID	Control VLAN ID of the latest Flush packet received.

12.5.5 display smart-link group

Function

The **display smart-link group** command displays information about all Smart Link groups or a specified Smart Link group.

Format

display smart-link group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays information about all Smart Link groups.	-
group-id	Displays information about a specified Smart Link group.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display smart-link group** command displays information about a Smart Link group, including member interfaces in the Smart Link group and link status. If a Smart Link group fails, you can find the cause of the fault according to the displayed information.

Prerequisites

A Smart Link group has been created by using the **smart-link group** command, and member interfaces have been added to the Smart Link group by using the **port** command.

Example

Display information about Smart Link group 1.

```
<HUAWEI> display smart-link group 1
Smart Link group 1 information :
  Smart Link group was enabled
  Load-Balance Instance: 5 7 9 to 10
  Protected-vlan reference-instance: 4 to 10
  DeviceID: 00e0-fc12-3456  Control-vlan ID: 1011
  Member                 Role   InstanceID State    Flush Count Last-Flush-Time
  --------------------------------------------------------------------------------

  GigabitEthernet0/0/1    Master 4         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1    Master 5         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1    Master 6         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1    Master 7         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1    Master 8         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1    Master 9         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/1    Master 10        Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  4         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  5         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  6         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  7         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  8         Inactive 0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  9         Active   0          0000/00/00 00:00:00 UTC+00:00
  GigabitEthernet0/0/2    Slave  10        Active   0          0000/00/00 00:00:00 UTC+00:00
```

Table 12-36 Description of the display smart-link group command output

Item	Description
Smart Link group	Whether a Smart Link group is enabled. ● enabled: The Smart Link group is enabled. ● disabled: The Smart Link group is disabled. Run the **smart-link enable** command to modify this parameter.

Item	Description
Wtr-time	WTR time of a Smart Link group. Run the **timer wtr** command to modify this parameter.
Link status	Interface on which the data streams of a Smart Link group are locked. ● lock: Data streams are locked on the master interface. ● force: Data streams are locked on the slave interface. Run the **smart-link** command to modify this parameter.
Load-Balance Instance	ID of the load balancing instance. Run the **load-balance instance** command to modify this parameter.
Protected-vlan reference-instance	ID of the protection VLAN instance. Run the **protected-vlan reference-instance** command to modify this parameter.
DeviceID	MAC address of the local device.
Control-vlan ID	Control VLAN ID of a Smart Link group. Run the **flush send** command to modify this parameter.
Member	Member interfaces added to a Smart Link group. Run the **port** command to modify this parameter.
Role	Role of a member interface in a Smart Link group. ● Master: master interface ● Slave: slave interface Run the **port** command to modify this parameter.
InstanceID	Protection instance ID. Run the **protected-vlan reference-instance** command to modify this parameter. If **protected-vlan reference-instance** is not configured, instance 0 and all instances created by **instance** are displayed.

Item	Description
State	Status of a member interface. ● Active: The member interface is forwarding packets. ● Inactive: The member interface is blocked. ● Unknown: The status of the member interface is unknown (for example, the Smart Link group is disabled or no member interface is added to the group).
Flush Count	Number of Flush packets sent.
Last-Flush-Time	Time when the latest Flush packet is sent. The format is YYYY/MM/DD HH:MM:SS UTC+HH:MM. If no Flush packet has ever been sent, the time is displayed as 0000/00/00 00:00:00 UTC+00:00.

12.5.6 display smart-link protocol-parameter group

Function

The **display smart-link protocol-parameter group** command displays internal data of all Smart Link groups or a specified Smart Link group, including member interface information and Smart Link configuration.

Format

display smart-link protocol-parameter group { **all** | *group-id* }

Parameters

Parameter	Description	Value
all	Displays internal data of all Smart Link groups.	-
group-id	Displays internal data of a specified Smart Link group.	The value is an integer that ranges from 1 to 16.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays internal data of Smart Link groups for diagnosis. You can use this command to check internal status data of a Smart Link group.

Example

Display the internal data of Smart Link group 1.

```
<HUAWEI> display smart-link protocol-parameter group 1
SMART-LINK Group 1:
********************************
 *Master Port Info:
  IfIndex:            0()
  PortStatus:         1(unknown)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:      0
   MTLK Group ID:      0
   Role:              0(invalid)
   Ctrl Vlan:          0
   Password:
 *Slave Port Info:
  IfIndex:            0()
  PortStatus:         1(unknown)
  LinkStatus:         0(down)
  IFNET_S
   SMLK Group ID:      0
   MTLK Group ID:      0
   Role:              0(invalid)
   CTRL Vlan:          0
   Password:
 *FSM Info:
  CurrentState:       0(Idle)
  TransEvent:         0(Invalid)
  TransIfIndex:       0()
 *Other Config:
  Lock|Force:         0(unknown)
  WtrTime:            60 sec.
  RevertEnable:       0(disable)
  GroupActive:        0(inactive)
  MTLK Uplink:        0
  RvtTimeCounter:     0 sec.
 *Flush Send Info:
  CTRL Vlan:          0
  Password:
 *1AG Event Info:
  Event Type:         0
```

Table 12-37 Description of the display smart-link protocol-parameter group command output

Item	Description
SMART-LINK Group 1	ID of a Smart Link group.
Master Port Info	Information about the master interface in the Smart Link group.
IfIndex	Interface index.

Item	Description
PortStatus	Physical status of an interface: - 1(unknown) - 2(active) - 3(inactive)
LinkStatus	Link status of an interface: - 0(down) - 1(up)
IFNET_S	Mnemonic symbol, indicating information saved on an interface.
SMLK Group ID	ID of a Smart Link group.
MTLK Group ID	ID of a Monitor Link group.
Role	Role of a member interface in a Smart Link group: - 0(invalid) - 1(master) - 2(slave)
Ctrl Vlan	Control VLAN. When the device sends Flush packets, run the **flush send** command to specify this parameter. When the device receives Flush packets, run the **smart-link flush receive** command to specify this parameter.
Password	Password of Flush packets. When the device sends Flush packets, run the **flush send** command to specify this parameter. When the device receives Flush packets, run the **smart-link flush receive** command to specify this parameter.
Slave Port Info	Information about a slave interface.
FSM Info	Finite state machine (FSM) information.
CurrentState	Current state of the state machine: - 0(Idle) - 1(Init) - 2(Master) - 3(Slave) - 0(MultiIdle) (used in load balancing scenarios)

Item	Description
TransEvent	Latest state machine transition event.
TransIfIndex	Index of the interface where the latest state machine transition event occurs.
Other Config	Other configuration.
Lock|Force	Interface where data streams are locked. ● lock: indicates that data streams are locked on the master interface. ● force: indicates that data streams are locked on the slave interface.
WtrTime	Wait-to-restore (WTR) time of a Smart Link group. The WTR time can be changed using the **timer wtr** command.
RevertEnable	Whether revertive switching is enabled. To configure the revertive switching function, run the **restore enable** command.
GroupActive	Whether the current Smart Link group is enabled.
MTLK Uplink	Uplink interface of a Monitor Link group.
RvtTimeCounter	WTR timer counter.
Flush Send Info	Information about Flush packets.
1AG Event Info	802.1ag event information.
Event Type	Type of an 802.1ag event.

12.5.7 flush send

Function

The **flush send** command enables a Smart Link group to send Flush packets.

The **undo flush send** command disables a Smart Link group from sending Flush packets.

By default, a Smart Link group is disabled from sending Flush packets.

Format

flush send control-vlan *vlan-id* [**password** { **simple** | **sha** } *password*]

undo flush send [**control-vlan** *vlan-id* [**password** { **simple** | **sha** } *password*]]

Parameters

Parameter	Description	Value
control-vlan *vlan-id*	Specifies the control VLAN ID of the Flush packets to be sent.	The value is an integer that ranges from 1 to 4094.
password simple	Indicates that the Flush packets sent from the Smart Link group contain a password in plain text. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password sha	Indicates that the Flush packets sent from the Smart Link group contain an SHA2-256-encrypted password. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password	Specifies the password carried in Flush packets.	The value is a string of 8 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces.

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switchover occurs between the master and slave links in a Smart Link group, the existing forwarding entries do not apply to the new topology. All the

MAC address entries and ARP entries on the network need to be updated. Therefore, the Smart Link group sends Flush packets to request other devices to update their MAC address tables and ARP tables.

The **flush send** command enables a Smart Link group to send Flush packets and sets the encryption mode, control VLAN ID, and password for Flush packets.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Follow-up Procedure

Run the **smart-link flush receive** command on the upstream device interface to enable the interface to receive Flush packets. Ensure that the control VLAN ID and password set for the Flush packets received by the upstream device are the same as those set for the Flush packets sent by the local device. That is, the control VLAN ID and password in Flush packets sent by a device must be the same as those in Flush packets received by the device.

Precautions

- The specified control VLAN exists on the device. If it does not exist, the Flush packets fail to send.
- The control VLAN cannot be the VLAN mapped by a VBST dynamic instance.
- The control VLAN must be in the protected instance list configured by the **protected-vlan reference-instance** command.
- The Flush packets mentioned here are used only for communication between Huawei S series switches and CE series switches. Other manufacturers may define the Flush packet format differently. The peer device must be enabled to receive Flush packets.
- The original encryption mode and password are deleted after you run this command to configure the new ones.
- For security purposes, you are advised to use SHA2-256 as the authentication algorithm of Smart Link.
- The original password cannot be retrieved after it is encrypted using the SHA2-256 algorithm. If you forget your password, configure a new password.

Example

Enable Smart Link group 1 to send Flush packets with control VLAN ID 100 and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] flush send control-vlan 100 password sha YsHsjx_202206
```

12.5.8 load-balance instance

Function

The **load-balance instance** command sets the load-balancing instances for a Smart Link group.

The **undo load-balance instance** command deletes load-balancing instances for a Smart Link group.

Format

load-balance instance { *instance-id1* [**to** *instance-id2*] } &<1-10> **slave**

undo load-balance instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> [**slave**] }

Parameters

Parameter	Description	Value
instance-id1 [**to** *instance-id2*]	Specifies ID of a Smart Link instance. ● *instance-id1* specifies the first instance ID. The value is an integer that ranges from 0 to 4094. ● **to** *instance-id2* specifies the last instance ID. The value of *instance-id2* is an integer that ranges from 0 to 4094. The value of *instance-id2* must be greater than the value of *instance-id1*. The *instance-id1* and *instance-id2* parameters identify a range of instances. If **to** *instance-id2* is not specified, only one instance specified by *instance-id1* is configured.	-
slave	Indicates that the slave interface sends packets of the specified Smart Link instances.	-
all	Deletes all load-balancing instances of a Smart Link group.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If load balancing is not configured for a Smart Link group, only the active link transmits data traffic and the standby link is idle.

The **load-balance instance** command implements load balancing in a Smart Link group. When both links in the Smart Link group are Up, the standby link transmits the traffic from the VLANs mapping the specified instances.

The instances specified in the command are Multiple Spanning Tree Protocol (MSTP) instances. Each instance maps a range of VLANs. Multiple instances can be bound to the standby link to implement load balancing.

Prerequisites

A Smart Link group has been created using the **smart-link group** command, and VLANs have been mapped to the specified instances using the **instance** command.

Follow-up Procedure

After configuring load balancing in a Smart Link group, you can use the **display smart-link group** command to verify the configuration.

Precautions

- The VLANs mapping the instances in the command cannot be used as the control VLAN ID of Flush packets sent by the local device.
- Before you run the **load-balance instance** command in a Smart Link group, the Smart Link group must be disabled.
- The load balancing instance specified by the **load-balance instance** command must be in the protected instance list by the **protected-vlan reference-instance** command.

Example

Configure load balancing in Smart Link group 3. Configure the standby link to transmit the traffic from the VLANs mapping the instance 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 3
[HUAWEI-smlk-group3] load-balance instance 1 slave
```

12.5.9 monitor-link group

Function

The **monitor-link group** command creates a Monitor Link group and displays the Monitor Link group view. If the specified Monitor Link group exists, the command directly displays the Monitor Link group view.

The **undo monitor-link group** command deletes a Monitor Link group.

By default, no Monitor Link group exists.

Format

monitor-link group *group-id*

undo monitor-link group *group-id*

Parameters

Parameter	Description	Value
group-id	Specifies the ID of a Monitor Link group.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitor Link extends link redundancy of Smart Link. It synchronizes the downlink interface status with the uplink interface status so that the downstream device can be notified quickly when the uplink interface fails. The downstream device then triggers a link switchover in the Smart Link group. This prevents packet loss caused by the uplink interface failure. Before using the Monitor Link group, you must create a Monitor Link group and enter the Monitor Link group view.

Follow-up Procedure

Add uplink and downlink interfaces to the created Monitor Link group.

Precautions

Before deleting a Monitor Link group that has member interfaces, run the **undo port** command to delete all the member interfaces.

Example

Create Monitor Link group 1.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1]
```

Delete Monitor Link group 2.

```
<HUAWEI> system-view
[HUAWEI] undo monitor-link group 2
```

12.5.10 port (Monitor Link group view)

Function

The **port** command adds an interface to a Monitor Link group and specifies the link connected to the interface as an uplink or a downlink.

The **undo port** command deletes an uplink or a downlink interface from a Monitor Link group.

By default, a Monitor Link group has no member interface.

Format

port *interface-type interface-number* { **downlink** [*downlink-id*] | **uplink** }

undo port [*interface-type interface-number*] { **downlink** *downlink-id* | **uplink** }

undo port all

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be added to a Monitor Link group. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
downlink [*downlink-id*]	Configures the current interface as a downlink interface and specifies the downlink ID.	The value is an integer that ranges from 1 to 512. If the *downlink-id* parameter is not specified, the system allocates an ID to the interface in an ascending order.
uplink	Configures the current interface as an uplink interface.	-
all	Deletes all member interfaces from a Monitor Link group.	-

Views

Monitor Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Monitor Link group consists of an uplink interface or two uplink interfaces and several downlink interfaces. If the uplink interface fails, the Monitor Link group automatically disables all the downlink interfaces. After configuring a Monitor Link group, add uplink and downlink interfaces to the group. The Monitor Link group then can synchronize the downlink interface status with the uplink interface status.

Prerequisites

A Monitor Link group has been created by using the **monitor-link group** command.

Precautions

A Monitor Link group supports a maximum of two uplink interfaces (physical interfaces, Eth-Trunk interfaces, or a combination of them) or one Smart Link group.

The uplink interface status determines the downlink interface status.

- If there is only one uplink interface and the uplink interface is in Up state in the Monitor Link group or the uplink interface changes from the Down state to the Up state in the group, all downlink interfaces go Up. If there are two uplink interfaces and both of them are Down, all downlink interfaces are shut down. If only one uplink interface is Down, the downlink interfaces are Up.
- If there is only one uplink interface and the uplink interface is deleted from the Monitor Link group or the uplink interface changes from the Up state to the Down state in the group, all downlink interfaces are shut down. If there are two uplink interfaces and only one of them is Down, all downlink interfaces are shut down.

If an uplink interface exists in the Monitor Link group, run the **undo port** command to delete this interface before adding a new one.

An interface cannot be added to a Monitor Link group in the following situations:

- The interface has been added to an Eth-Trunk.
- The interface has been added to a Smart Link group.
- The interface has been added to another Monitor Link group.

Example

Add GE0/0/1 to Monitor Link group 1 and specify this interface as the uplink interface.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1] port gigabitethernet 0/0/1 uplink
```

Add GE0/0/2 to a Monitor Link group and specify this interface as the downlink interface and the link ID as 1.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1] port gigabitethernet 0/0/2 downlink 1
```

12.5.11 port (Smart Link group view)

Function

The **port** command adds an interface to a Smart Link group and specifies the interface as the master or slave interface.

The **undo port** command deletes a master or slave interface from a Smart Link group.

By default, a Smart Link group has no member interface.

Format

port *interface-type interface-number* { **master** | **slave** }

undo port *interface-type interface-number* { **master** | **slave** }

undo port { **all** | **master** | **slave** }

Parameters

Parameter	Description	Value
interface-type interface-number	• *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
master	Specifies an interface as a master interface.	-
slave	Specifies an interface as a slave interface.	-
all	Deletes all the interfaces in a Smart Link group.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Smart Link function implements link redundancy and rapid link status transition on a dual-homed network. When a device is connected to upstream devices by two uplink interfaces, one link is blocked and functions as the backup of the other link. When the active link fails, traffic is switched to the other link. To implement the Smart Link function, create a Smart Link group and add two interfaces to the Smart Link group, one as the master interface, and the other as the slave interface. The master interface is in active state; the slave interface is in inactive state.

Prerequisites

A Smart Link group has been created using the **smart-link group** command. The Spanning Tree Protocol (STP) has been disabled on the interfaces to be added to the Smart Link group by using the **stp disable** command.

Follow-up Procedure

Run the **smart-link enable** command to enable the Smart Link group. Run the **flush send** command to enable the Smart Link group to send Flush packets, and run the **smart-link flush receive** command on the upstream device interface to enable the interface to receive Flush packets.

Precautions

If port security is also configured, packets will be discarded when the number of MAC addresses learned by an interface reaches the upper limit. In this case, Smart Link Flush packets may fail to be received. To prevent this, you are advised not to use both Smart Link and port security.

Before adding a new master or slave interface to a Smart Link group, delete the previous one from the Smart Link group.

The slave interface is blocked when the Smart Link group is enabled.

An interface can be added to only one Smart Link group.

If an interface has been added to a Smart Link group, the following configurations cannot be performed on the interface. If any of the following configurations is performed on an interface, the interface cannot be added to a Smart Link group:

- RRPP, SEP, or ERPS
- STP
- Adding an interface to an Eth-Trunk
- Adding an interface to a Monitor Link group
- Adding an interface to another Smart Link group
- Service loopback (for an Eth-Trunk)

Example

Add GE0/0/1 to Smart Link group 1 and specify the interface as the master interface.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] port gigabitethernet 0/0/1 master
```

12.5.12 protected-vlan reference-instance

Function

The **protected-vlan reference-instance** command configures the protection instances for a Smart Link group.

The **undo protected-vlan reference-instance** command deletes the protection instances of a Smart Link group.

Format

protected-vlan reference-instance { *instance-id1* [**to** *instance-id2*] }&<1-10>

undo protected-vlan reference-instance { **all** | { *instance-id1* [**to** *instance-id2*] }&<1-10> }

Parameters

Parameter	Description	Value
instance-id1 [**to** *instance-id2*]	Specifies the protection instance ID of a Smart Link group. ● *instance-id1* specifies the first instance ID. The value is an integer that ranges from 0 to 4094. ● **to** *instance-id2* specifies the last instance ID. The value of *instance-id2* is an integer that ranges from 0 to 4094. The value of *instance-id2* cannot be smaller than the value of *instance-id1*. The *instance-id1* and *instance-id2* parameters identify a range of protection instances. If **to** *instance-id2* is not specified, only the protection instance specified by *instance-id1* is configured.	-
all	Specifies IDs for deleting all protection instances of a Smart Link group.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **protected-vlan reference-instance** command enables Smart Link to transmit or block the data packets from the VLAN mapping the protection instances. The Smart Link function takes effect only on the VLANs mapping the protection instances. The **protected-vlan reference-instance** command enables users to unbind some VLANs from protection instances. Transmitting the data from these VLANs is not restricted by Smart Link.

Prerequisites

A Smart Link group has been created using the **smart-link group** command, and VLANs have been mapped to the specified instances using the **instance** command.

Precautions

Before you run the **protected-vlan reference-instance** command in a Smart Link group, the Smart Link group must be disabled.

The instances specified in the **protected-vlan reference-instance** command cannot be the VBST dynamic instances.

The Smart Link function takes effect only on the VLANs mapped to the protection instances. Therefore, the users' service data VLANs and VLANs mapped to load-balancing instances must be contained in the VLANs mapped to protection instances.

The VLANs not mapped to protection instances may cause network storms.

Example

Set the protection instance ID of a Smart Link group to 10.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] protected-vlan reference-instance 10
```

12.5.13 reset smart-link flush

Function

The **reset smart-link flush** command clears statistics about Flush packets.

Format

reset smart-link flush

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect the statistics in a specified period, you can run the **reset smart-link flush** command to clear historical data before collecting the statistics. For example, a Smart Link group sends a large number of Flush packets after a failover occurs. You can view the Flush packet statistics to locate the fault. After locating the fault, you can use the **reset smart-link flush** command to clear the statistics so that you can collect new statistics for fault location when another failover occurs.

Precautions

The cleared statistics cannot be restored. Run the **display smart-link flush** command to view Flush packet statistics before clearing the statistics.

Example

Clear statistics about Flush packets.

```
<HUAWEI> reset smart-link flush
```

12.5.14 restore enable

Function

The **restore enable** command enables the revertive switching of a Smart Link group.

The **undo restore enable** command disables the revertive switching of a Smart Link group.

By default, the revertive switching of a Smart Link group is disabled.

Format

restore enable

undo restore enable

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active link in a Smart Link group fails, traffic is switched to the standby link. The original active link remains blocked after recovery. To enable the original active link to transmit traffic, enable the revertive switching function in the Smart Link group. Traffic is switched back to the original active link when the WTR timer expires.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Follow-up Procedure

By default, the WTR timer is 60 seconds. You can run the **timer wtr** command to change the value.

Precautions

- Link switching is performed only when both member interfaces in the Smart Link group are in Up state.
- Do not run the **undo restore enable** command during revertive switching because this will cause a revertive switching failure.

Example

Enable the revertive switching of Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] restore enable
```

12.5.15 smart-link

Function

The **smart-link** command enables a Smart Link group to lock data streams and specifies the locking interface.

The **undo smart-link** command disables a Smart Link group from locking data streams.

By default, a Smart Link group is disabled from locking data streams.

Format

smart-link { **force** | **lock** }

undo smart-link { **force** | **lock** }

Parameters

Parameter	Description	Value
force	Locks data streams on the slave interface.	-
lock	Locks data streams on the master interface.	-

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **smart-link** command to lock data streams on the master or slave link. During the maintenance, the active link in the Smart Link group needs to be inspected. To prevent the inspection from affecting normal services, configure the data stream policy for the Smart Link group. Then the device forcibly locks data streams to the standby link and switches them back to the active link after the inspection is complete.

Prerequisites

The Smart Link group has been enabled by using the **smart-link enable** command.

Precautions

After data streams are locked on a specified link, traffic cannot be switched to the other link even the specified link fails.

The **lock** and **force** keywords are mutually exclusive and only one of them can be entered each time. The **lock** keyword takes precedence over the **force** keyword. If you specify **force** and then **lock**, data streams are locked on the master interface. If you specify **lock** first, the configuration fails when you specify **force** in the command.

Example

Smart Link group 1 is configured to lock data streams and lock data streams on the slave interface.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link enable
[HUAWEI-smlk-group1] smart-link force
```

12.5.16 smart-link enable

Function

The **smart-link enable** command enables a Smart Link group.

The **undo smart-link enable** command disables a Smart Link group.

By default, a Smart Link group is disabled.

Format

smart-link enable

undo smart-link enable

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Smart Link group takes effect and blocks the slave interface only after it is enabled. After the Smart Link group is disabled, the slave interface is unblocked.

After creating a Smart Link group and adding interfaces to the group, you must enable the Smart Link group to make it effective.

Precautions

After a Smart Link group is enabled, the slave interface is blocked only if the master and slave interfaces are both in Up state.

Example

Enable Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link enable
```

12.5.17 smart-link flush receive

Function

The **smart-link flush receive** command enables an interface to receive Flush packets and specifies the control VLAN ID and password for Flush packets.

The **undo smart-link flush receive** command disables an interface from receiving Flush packets.

By default, an interface rejects Flush packets.

Format

smart-link flush receive control-vlan { { *vlan-id* } &<1-10> [**password** { **simple** | **sha** } *password*] | **all** }

undo smart-link flush receive [**control-vlan** { *vlan-id* | **all** }] (interface view)

undo smart-link flush receive (port group view)

Parameters

Parameter	Description	Value
control-vlan *vlan-id*	Specifies the control VLAN ID of Flush packets that can be received.	The value is an integer that ranges from 1 to 4094.
password simple	Indicates that the password for sending Flush packets is in plain text. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password sha	Indicates that Flush packets sent from the Smart Link group contain an SHA2-256-encrypted password. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password	Specifies the password carried in Flush packets.	The value is a string of 8 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces.
all	Indicates that all control VLANs allow Flush packets.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view and port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switchover occurs between the master and slave links in a Smart Link group, the existing forwarding entries do not apply to the new topology. All the MAC address entries and ARP entries on the network need to be updated. The Smart Link group sends Flush packets to notify upstream devices of the topology change. Upstream devices can update their MAC address entries and ARP entries only if they are enabled to receive Flush packets. If a device rejects Flush packets, it cannot forward packets correctly after a link failover occurs in the Smart Link group.

Precautions

- The Flush packets mentioned here are used only for communication between Huawei CE series and S series switches. Other manufacturers may define different Flush packet formats.
- The **smart-link flush receive** command does not add member interfaces of the Smart Link group to the control VLAN. You need to configure the member interfaces to allow the control VLAN. The interface accepts a Flush packet only if the control VLAN ID and password in the packet are the same as those configured on the local interface.
- A maximum of 256 control VLANs used to receive Flush packets can be configured on an interface.
- The original encryption mode and password are deleted after you run this command to configure the new ones. If the control VLAN ID is changed, the password must be reconfigured.
- For security purposes, you are advised to use SHA2-256 as the authentication algorithm of Smart Link.
- If the password is encrypted in the SHA2-256 mode, it cannot be retrieved. Set a new password after the original one is lost.

Example

Enable GE0/0/1 to receive Flush packets with control VLAN ID 100 and password **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] smart-link flush receive control-vlan 100 password sha YsHsjx_202206
```

12.5.18 smart-link flush receive password

Function

The **smart-link flush receive password** command specifies an encryption mode and a password for Flush packets on all interfaces.

The **undo smart-link flush receive password** command deletes the encryption mode and a password for Flush packets on all interfaces.

By default, no encryption mode or password is configured for Flush packets on all interfaces.

Format

smart-link flush receive password { **simple** | **sha** } *password*

undo smart-link flush receive password

Parameters

Parameter	Description	Value
simple	Indicates that the password for sending Flush packets is in plain text. **NOTE** The password is saved in the configuration file in cipher text for security.	-
sha	Indicates that the password for sending Flush packets is in SHA2-256 mode. **NOTE** The password is saved in the configuration file in cipher text for security.	-
password	Specifies the password carried in Flush packets.	The value is a string of 8 to 16 case-sensitive characters in plain text and consists of at least two of the following: lowercase letters, uppercase letters, digits, and special characters excluding question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **smart-link flush receive password** command to specify an encryption mode and a password for Flush packets on all interfaces.

Prerequisites

The downstream device has been enabled to send Flush packets by using the **flush send** command.

Precautions

- The password configured in a control VLAN on an interface that is enabled to receive flush packets takes precedence over the password configured globally. If the password on an interface is not configured, the interface configured globally is used.
- For security purposes, you are advised to use SHA2-256 as the authentication algorithm of Smart Link.

Example

Specify YsHsjx_202206 for Flush packets.

```
<HUAWEI> system-view
[HUAWEI] smart-link flush receive password sha YsHsjx_202206
```

12.5.19 smart-link hold-time

Function

The **smart-link hold-time** command sets the holdtime for reporting the Interface-Up or Interface-Down event in a Smart Link group.

The **undo smart-link hold-time** command deletes the holdtime for reporting the Interface-Up or Interface-Down event in a Smart Link group.

By default, a port-Up or port-Down event is reported immediately.

Format

smart-link hold-time *hold-time*

undo smart-link hold-time [*hold-time*]

Parameters

Parameter	Description	Value
hold-time	Specifies the holdtime for reporting the Interface-Up or Interface-Down event in a Smart Link group.	The value is an integer that ranges from 0 to 60, in 100 ms.

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If services are frequently switched between links in a Smart Link group because of temporary link disconnection, packets may be lost and system performance deteriorates. To prevent frequent switchover caused by temporary link disconnection, run the **smart-link hold-time** command to set the holdtime for reporting an Interface-Up or Interface-Down event. When the member interfaces of the Smart Link group alternate between Up and Down, the Smart Link group waits until the holdtime expires, and then triggers a switchover.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Precautions

If you run the **smart-link hold-time** command multiple times in the same Smart Link group view, only the latest configuration takes effect.

Example

Set the holdtime of Smart Link failover in Smart Link group 1 to 300 ms.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link hold-time 3
```

12.5.20 smart-link group

Function

The **smart-link group** command creates a Smart Link group and enters the Smart Link group view. If the Smart Link group already exists, you can enter the Smart Link group view directly.

The **undo smart-link group** command deletes a Smart Link group that already exists.

By default, no Smart Link group is created on the device.

Format

smart-link group *group-id*

undo smart-link group *group-id*

Parameters

Parameter	Description	Value
group-id	Specifies a Smart Link group ID.	The value is an integer that ranges from 1 to 16.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Smart Link function implements link backup and rapid switchover on a dual-homed network. To use the Smart Link function, you must create a Smart Link group first.

Follow-up Procedure

After creating a Smart Link group, perform the following actions:

1. Configure master and slave interfaces in the Smart Link group.
2. Enable the Smart Link group to send Flush packets.
3. Enable the Smart Link group.

Precautions

Run the **undo port** command to delete all the member interfaces before deleting a Smart Link group that has member interfaces.

Example

Create Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1]
```

12.5.21 smart-link group uplink

Function

The **smart-link group uplink** command adds a Smart Link group to a Monitor Link group as the uplink interface.

The **undo smart-link group uplink** command deletes a Smart Link group from a Monitor Link group.

Format

smart-link group *group-id* **uplink**

undo smart-link group *group-id* **uplink**

Parameters

Parameter	Description	Value
group-id	Specifies a Smart Link group ID.	The value is an integer that ranges from 1 to 16.

Views

Monitor Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Cascading of Smart Link and Monitor Link improves link backup reliability. When the uplink interface is a Smart Link group, the uplink interface is considered faulty and the Monitor Link group forcibly disables the downlink interfaces only if both the master and slave interfaces of the Smart Link group are in Inactive or Down state.

Prerequisites

A Smart Link group has been created using the **smart-link group** command.

Precautions

A Smart Link group can be added to only one Monitor Link group.

A Smart Link can function only as the uplink interface in a Monitor Link group.

When the uplink interface fails, all the downlink interfaces in the Monitor Link group are shut down.

Before adding a Smart Link group to a Monitor Link group, delete the previous uplink interface from the Monitor Link group.

Example

Add Smart Link group 1 to Monitor Link group 2 as the uplink interface.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 2
[HUAWEI-mtlk-group2] smart-link group 1 uplink
```

12.5.22 smart-link link-switch send-broadcast enable

Function

The **smart-link link-switch send-broadcast enable** command enables a device to send broadcast packets to trigger the peer device to re-learn MAC addresses.

The **undo smart-link link-switch send-broadcast enable** command cancels the configuration.

By default, the function of sending broadcast packets to trigger the peer device to re-learn MAC addresses is disabled.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

smart-link link-switch send-broadcast enable

undo smart-link link-switch send-broadcast enable

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Smart Link interface is connected to a non-Huawei device that does not support Smart Link and the active link goes Down, MAC address information on the network cannot be quickly updated. In this case, you can run this command to enable a device to send broadcast packets to trigger the peer device to re-learn MAC addresses.

Prerequisites

This function takes effect only when Smart Link is enabled and the master and slave interfaces are configured.

Example

Enable the function of sending broadcast packets for Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
```

```
[HUAWEI-smlk-group1] smart-link enable
[HUAWEI-smlk-group1] smart-link link-switch send-broadcast enable
```

12.5.23 smart-link manual switch

Function

The **smart-link manual switch** command enables the device to switch services from the active link to the standby link in a Smart Link group.

Format

smart-link manual switch

Parameters

None

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active link in a Smart Link group fails, traffic is switched to the standby link. The original active link remains blocked after recovery. Generally, a stable link is used as the active link. Therefore, after the original active link recovers, you can perform the following operations to switch traffic back to this link:

- Enable the revertive switching of a Smart Link group. The system performs switching after the revertive switching timer times out.
- Run the **smart-link manual switch** command to switch traffic back.

However, the minimum revertive switching time is 30s, and the default value is 60s. You can run the **smart-link manual switch** command to manually switch traffic back to the active link.

Prerequisites

To implement an active/standby switchover between links, ensure that:

- The active interface and standby interface exist and are both in Up state.
- Traffic is not blocked on either interface by using the **smart-link** command.

Precautions

Millisecond-level packet loss will occur during the switchover.

Example

Perform an active/standby switchover between links of Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] smart-link manual switch
```

12.5.24 smart-link { vpls-notify | vll-notify } enable

Function

The **smart-link** { **vpls-notify** | **vll-notify** } **enable** command enables an interface to notify the VPLS/VLL module when the interface receives a Flush packet.

The **undo smart-link** { **vpls-notify** | **vll-notify** } **enable** command cancels the configuration.

By default, an interface does not notify the VPLS/VLL module when receiving a Flush packet.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H, S6730-H, S5731-S, S5731S-S, S6730-S, and S6730S-S support this command.

Format

smart-link { **vpls-notify** | **vll-notify** } **enable**

undo smart-link { **vpls-notify** | **vll-notify** } **enable**

Parameters

Parameter	Description	Value
vpls-notify	Enables an interface to notify the VPLS module when receiving Flush packets.	-
vll-notify	Enables an interface to notify the VLL module when receiving Flush packets.	-

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a customer edge (CE) device is dual homed to a VPLS or VLL network through VLANIF interfaces or dot1q sub-interfaces of a provider edge (PE) device, associate Smart Link with VPLS on the corresponding physical interfaces of the PE device. If the VLANIF interfaces or dot1q sub-interfaces are bound to VSI or VLL run the **smart-link flush receive** and **smart-link { vpls-notify | vll-notify } enable** commands on the corresponding physical interfaces. Then the physical interfaces can notify the VPLS or VLL module when receiving a Flush packet. The VPLS or VLL module then deletes the MAC addresses learned from the VSI or VLL bound to the VLANIF interfaces or dot1q sub-interfaces, and sends messages to remote devices, instructing them to update MAC address entries.

Prerequisites

The VPLS or VLL configuration has been completed on the backbone network. The Smart Link configuration has been completed on the CE interfaces connected to the PE device. The VLANIF interfaces or dot1q sub-interfaces of the PE device connected to the CE device have been bound to VSI or VLL. The physical interfaces connected to the CE device have been enabled to accept Flush packets by using the **smart-link flush receive** command.

Precautions

You can associate Smart Link with VPLS or VLL only when a CE device is connected to the VPLS or VLL network through VLANIF interfaces or dot1q sub-interfaces of a PE device. Smart Link cannot be associated with VPLS or VLL when the CE device is connected to the VPLS or VLL network through physical interfaces.

Example

Enable XGE0/0/1 to notify the VPLS module when the interface receives a Flush packet.

```
<HUAWEI> system-view
[HUAWEI] interface xgigabitethernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] smart-link vpls-notify enable
```

12.5.25 timer recover-time

Function

Using the **timer recover-time** command, you can set the wait to restore (WTR) time of a Monitor Link group.

Using the **undo timer recover-time** command, you can restore the default WTR time of a Monitor Link group.

By default, the WTR time of a Monitor Link group is 3 seconds.

Format

timer recover-time *recover-time*

undo timer recover-time [*recover-time*]

Parameters

Parameter	Description	Value
recover-time	Specifies the WTR time of a Monitor Link group.	The value is an integer that ranges from 3 to 60, in seconds. The default value is 3.

Views

Monitor Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the downlink interface status changes frequently in a Monitor Link group because of temporary uplink disconnection, packets are lost and system performance deteriorates. To prevent frequent failover caused by temporary link disconnection, you can use the **timer recover-time** command to set the WTR time of the Monitor Link group. The Monitor Link group does not restore downlink interfaces immediately after the uplink interface recovers. The downlink interfaces become Up until the WTR time expires.

recover-time indicates the internal switching time of a Monitor Link group. That is, the system starts the interface Up operation after the internal switching time is reached. The actual interface Up time is also affected by the interface Up performance.

Prerequisites

A Monitor Link group has been created by using the **monitor-link group** command.

Example

Set the WTR time to 6 seconds for Monitor Link group 1.

```
<HUAWEI> system-view
[HUAWEI] monitor-link group 1
[HUAWEI-mtlk-group1] timer recover-time 6
```

12.5.26 timer wtr

Function

The **timer wtr** command sets the WTR time of a Smart Link group.

The **undo timer wtr** command restores the default WTR time of a Smart Link group.

By default, the WTR time of a Smart Link group is 60 seconds.

Format

timer wtr *wtr-time*

undo timer wtr [*wtr-time*]

Parameters

Parameter	Description	Value
wtr-time	Specifies the WTR time.	The value is an integer that ranges from 30 to 1200, in seconds. The default WTR time is 60 seconds.

Views

Smart Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the active link in a Smart Link group fails, traffic is switched to the standby link. The original active link remains blocked after recovery. To enable the original active link to transmit traffic, enable the revertive switching function in the Smart Link group. Traffic is switched back to the original active link when the WTR timer expires.

Precautions

If the network is unstable or has no requirement for the transmission delay, set a longer WTR time to prevent frequent switching.

Example

Set the WTR time to 120 seconds for Smart Link group 1.

```
<HUAWEI> system-view
[HUAWEI] smart-link group 1
[HUAWEI-smlk-group1] timer wtr 120
```

12.6 MAC Swap Loopback Configuration Commands

12.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.6.2 display loopback swap-mac information

Function

The **display loopback swap-mac information** command displays the MAC swap loopback configuration.

Format

display loopback swap-mac information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To ensure a successful loopback test, use this command to check the loopback configuration before the loopback test. After the loopback test is complete, use this command to view the number of loopback test packets and the number of discarded test packets, and compare them with the number of packets sent from the tester to check network performance.

Pre-configuration Tasks

The local MAC swap loopback function has been configured by using the **loopback local swap-mac** command or the local MAC swap loopback function has been configured by using the **loopback remote swap-mac** command.

Example

Display the MAC swap loopback configuration.

Models excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S:

```
<HUAWEI> display loopback swap-mac information
  Loopback type              : local
  Loopback state             : running
  Loopback test time(s)      : 60
  Loopback interface         : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/2
  Loopback source MAC        : 0001-0001-0001
  Loopback destination MAC  : 0002-0002-0002
  Loopback vlan              : 10
  Loopback inner vlan        : 0
  Loopback packets           : 0
  Drop packets               : 3
```

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S:

```
<HUAWEI> display loopback swap-mac information
  Loopback type              : remote
  Loopback state             : running
  Loopback test time(s)      : 60
  Loopback interface         : GigabitEthernet0/0/1
  Loopback output interface : GigabitEthernet0/0/2
```

Table 12-38 Description of the display loopback swap-mac information command output

Item	Description
Loopback type	Type of the MAC swap loopback test: - local: local MAC swap loopback test - remote: remote MAC swap loopback test Run the following commands to configure loopback type. **loopback local swap-mac** **loopback remote swap-mac**
Loopback state	Status of the MAC swap loopback function: - running: The MAC swap loopback function is enabled. - stop: The MAC swap loopback function is disabled. Run the following commands to configure loopback state. **loopback swap-mac**
Loopback test time(s)	Timeout period of the loopback test. If the value is none, the loopback test timeout function is disabled.

Item	Description
Loopback interface	Interface where the loopback test is performed.
Loopback output interface	Outbound interface that sends test packets back to the tester.
Loopback source MAC	Source MAC address of test packets.
Loopback destination MAC	Destination MAC address of test packets.
Loopback vlan	VLAN ID of test packets.
Loopback inner vlan	Inner VLAN ID of test packets.
Loopback packets	Number of received loopback packets.
Drop packets	Number of discarded packets. This field is displayed only when a local MAC swap loopback test is performed.

12.6.3 loopback local swap-mac

Function

The **loopback local swap-mac** command enables local MAC swap loopback.

The **undo loopback local swap-mac** command disables local MAC swap loopback.

By default, local MAC swap loopback is disabled on an interface.

NOTE

The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S-I, S5735S-S, and S5735-S do not support this command.

Format

loopback local swap-mac source-mac *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] **interface** *interface-type interface-number* [**timeout** { *time-value* | **none** }]

undo loopback local swap-mac

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **inner-vlan** *inner-vlan-id* parameter.

Parameters

Parameter	Description	Value
source-mac *source-mac-address*	Specifies the source MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
dest-mac *dest-mac-address*	Specifies the destination MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
vlan *vlan-id*	Specifies the VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
inner-vlan *inner-vlan-id*	Specifies the inner VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies the outbound interface that sends loopback packets back to the tester. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
timeout *time-value*	Specifies the timeout period of a loopback test. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test stops after the timeout period of the loopback test expires.	The value is an integer that ranges from 5 to 300, in seconds. The default value is 60.

Parameter	Description	Value
timeout none	Indicates that the loopback test timeout function is disabled. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test cannot automatically stop after its timeout period expires. Instead, you must run the **loopback swap-mac stop** command to manually stop the MAC swap loopback test.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using the Switch to provide services for users, perform a local MAC swap loopback test on the Switch to check whether the Switch can provide services properly. This test checks connectivity and QoS CAR of the network between the Switch downlink interface and a remote device. The local MAC swap loopback test can also check whether VLAN mapping and VLAN stacking are configured successfully on the downlink interface.

A local MAC swap loopback test checks connectivity and performance of the network between a tester and a tested switch, and performance of the tested switch.

In a local MAC swap loopback test, a tester sends test packets to the Switch. When test packets reach the downlink interface, the Switch swaps the source and destination MAC addresses of test packets and sends the packets back to the tester through a specified outbound interface.

Follow-up Procedure

Run the **loopback swap-mac start** command to enable the MAC swap loopback function.

Precautions

NOTICE

When a local loopback test is performed on an interface, all services on the interface are interrupted.

- An Eth-Trunk interface in LACP mode does not support the local MAC swap loopback function. An Eth-Trunk member interface does not support the MAC swap loopback function.
- Before enabling the local MAC swap loopback function, you need to run the **undo stp enable** command to disable STP on the interface.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- If a large number of test packets are sent, test packets occupy bandwidth of other services on the interface that sends test packets.

Example

Configure local MAC swap loopback.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback local swap-mac source-mac 00e0-fc00-0085 dest-mac 00e0-
fc00-1004 vlan 100 interface gigabitethernet 0/0/2
```

12.6.4 loopback remote swap-mac

Function

The **loopback remote swap-mac** command enables remote MAC swap loopback.

The **undo loopback remote swap-mac** command disables remote MAC swap loopback.

By default, remote MAC swap loopback is disabled on an interface.

Format

Models excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S-I, S5735S-S, and S5735-S:

loopback remote swap-mac source-mac *source-mac-address* **dest-mac** *dest-mac-address* **vlan** *vlan-id* [**inner-vlan** *inner-vlan-id*] [**timeout** { *time-value* | **none** }]

undo loopback remote swap-mac

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S500, S5735-S-I, S5735S-S, and S5735-S:

loopback remote swap-mac [**timeout** { *time-value* | **none** }]

undo loopback remote swap-mac

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **inner-vlan** *inner-vlan-id* parameter.

Parameters

Parameter	Description	Value
source-mac *source-mac-address*	Specifies the source MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
dest-mac *dest-mac-address*	Specifies the destination MAC address of test packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The source and destination MAC addresses must be unicast MAC addresses.
vlan *vlan-id*	Specifies the VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
inner-vlan *inner-vlan-id*	Specifies the inner VLAN ID of test packets.	The value is an integer that ranges from 1 to 4094.
timeout *time-value*	Specifies the timeout period of a loopback test. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test stops after the timeout period of the loopback test expires.	The value is an integer that ranges from 5 to 300, in seconds. The default value is 60.

Parameter	Description	Value
timeout none	Indicates that the loopback test timeout function is disabled. If the **loopback swap-mac start** command is run to enable MAC swap loopback, a MAC swap loopback test cannot automatically stop after its timeout period expires. Instead, you must run the **loopback swap-mac stop** command to manually stop the MAC swap loopback test.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using the Switch to provide services for users, perform a remote MAC swap loopback test to check whether the Switch can provide services properly. This test checks connectivity and performance of the network between the Switch uplink interface and a remote device. The remote MAC swap loopback test can also check whether VLAN mapping and VLAN stacking are configured successfully on the uplink interface.

A remote MAC swap loopback test checks connectivity and performance of the network between a tester and a tested switch but does not check performance of the tested switch.

In a remote MAC swap loopback test, a tester sends test packets to the Switch. When test packets reach the uplink interface, the Switch swaps the source and destination MAC addresses of test packets and sends the packets back to the tester through this interface.

Follow-up Procedure

Run the **loopback swap-mac start** command to enable the MAC swap loopback function.

Precautions

- An Eth-Trunk interface supports the MAC swap loopback function but an Eth-Trunk member interface does not.
- The port is not a Layer 3 port. If the port is a Layer 3 port, run the **portswitch** command to switch the port to the Layer 2 mode.
- The **loopback remote swap-mac** and **single-fiber enable** commands cannot be used on the same interface.
- If the switch does not receive any test packet within the timeout period after the remote MAC swap loopback test starts, perform the test again. And then run the **loopback swap-mac start** command.
- If **timeout none** is specified in the command, you can perform a loopback test at any time until the MAC swap loopback function is disabled by using the **loopback swap-mac stop** command.

Example

Configure remote MAC swap loopback.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback remote swap-mac source-mac xxxx-xxxx-xxxx dest-mac xxxx-xxxx-xxxx vlan 100
```

12.6.5 loopback swap-mac

Function

The **loopback swap-mac** command enables or disables the MAC swap loopback function.

By default, the MAC swap loopback function is disabled.

Format

loopback swap-mac { **start** | **stop** }

Parameters

Parameter	Description	Value
start	Enables the MAC swap loopback function.	-
stop	Disables the MAC swap loopback function.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Both local and remote loopback tests deteriorate network performance. To minimize impact of a loopback test, enable the MAC swap loopback function when the loopback test begins and disable it immediately after the loopback test is complete.

A MAC swap loopback test stops when you disable the MAC swap loopback function or the loopback test times out. To perform the loopback test again, run the **loopback swap-mac start** command.

Pre-configuration Tasks

The local MAC swap loopback function has been configured by using the **loopback local swap-mac** command or the local MAC swap loopback function has been configured by using the **loopback remote swap-mac** command.

Precautions

An Eth-Trunk interface supports the MAC swap loopback function but an Eth-Trunk member interface does not.

An Eth-Trunk interface in LACP mode does not support the local MAC swap loopback function.

To ensure service provisioning on the interface, disable the MAC swap loopback function immediately after the loopback test is complete.

The **loopback swap-mac** command is a one-time command and is not saved in the configuration file.

Example

Enable the MAC swap loopback function.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] loopback swap-mac start
```

12.7 EFM Configuration Commands

12.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.7.2 clear mgr inactive-configuration slot

Function

The **clear mgr inactive-configuration slot** command deletes the inactive Ethernet OAM configurations from the switch that does not register.

Format

clear mgr inactive-configuration slot *slot-id* [**card** *card-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a switch that does not register.	The value is an integer and the value range depends on device model.
card *card-id*	Specifies the offline card ID.	The value is an integer and the value range depends on device model.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a subcard has been replaced, using the **clear mgr inactive-configuration slot** command deletes the configurations of the subcard that does not register if these configurations do not need to be saved.

Running the **clear mgr inactive-configuration slot** command can delete the inactive configurations.

Before using this command, note the following points:

- When the device is in the CSS, ensure that the specified card on which configurations are to be deleted does not register.
- Ensure that the specified subcard on which configurations are to be deleted does not register.

Example

Delete the configurations of the card that does not register in slot 1.

```
<HUAWEI> system-view
[HUAWEI] clear mgr inactive-configuration slot 1
Warning: The inactive oam-mgr configuration related to the interfaces of the slot or card will be deleted
and cannot be restored, continue? [Y/N]:y
Info: Operation succeeded.
```

12.7.3 display efm

Function

The **display efm** command displays the EFM configuration on an interface.

Format

display efm { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays the EFM configuration on all the interfaces enabled with EFM.	-
interface-type interface-number	Displays the EFM configuration of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the EFM configuration on the device, run the **display efm** command.

- If **all** is specified, all EFM configuration is displayed.
- If **interface** *interface-type interface-number* is specified, the EFM configuration of a specified interface is displayed.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Display the EFM configuration on GigabitEthernet0/0/1.

```
<HUAWEI> display efm interface gigabitethernet 0/0/1
 Item                          Value
 ----------------------------------------------------
 Interface:                     GigabitEthernet0/0/1
 EFM Enable Flag:               enable
 Mode:                          active
 Loopback IgnoreRequest:        no
 OAMPDU MaxSize:                128
 OAMPDU Timeout:                5000
 OAMPDU Interval:               1000
 Parser:                        forward
 Multiplexer:                   forward
 ErrCodeNotification:           disable
 ErrCodePeriod:                 1
 ErrCodeThreshold:              1
 ErrFrameNotification:          disable
 ErrFramePeriod:                1
 ErrFrameThreshold:             1
 ErrFrameSecondNotification:    disable
 ErrFrameSecondPeriod:          60
 ErrFrameSecondThreshold:       1
 Hold Up Time:                  10
 ThresholdEvtTriggerErrDown:    enable
 TriggerIfDown:                 disable
 TriggerMacRenew:               disable
 Remote MAC:                    --
 Remote EFM Enable Flag:        --
 Remote Mode:                   --
 Remote MaxSize:                --
 Remote Loopback IgnoreRequest: --
 Remote State:                  --
 Remote Parser:                 --
 Remote Multiplexer:            --
 ErrFramePeriodNotification:    disable
 ErrFramePeriodPeriod:          200000
 ErrFramePeriodThreshold:       1
 Loopback Remain Time:          1189
```

Table 12-39 Description of the display efm command output

Item	Description
Interface	Interface name.
EFM Enable Flag	Whether EFM is enabled on an interface: - disable: indicates that EFM is disabled on an interface. - enable: indicates that EFM is enabled on an interface. To enable or disable EFM on an interface, run the **efm enable** command.
Mode	Operation mode of EFM on an interface: - active: indicates that EFM works in active mode. - passive: indicates that EFM works in passive mode. To set the operation mode of EFM on an interface, run the **efm mode** command.

Item	Description
Loopback IgnoreRequest	Whether loopback requests from the remote end are ignored: - yes: Loopback requests from the remote end are ignored. - no: Loopback requests from the remote end are processed. To set the parameter, run the **efm loopback ignore-request** command.
OAMPDU MaxSize	Maximum size of an EFM OAMPDU on an interface. The value ranges from 64 to 1518, in bytes. The default value is 128 bytes. To set the maximum size of an EFM OAMPDU on an interface, run the **efm packet max-size** command.
OAMPDU Timeout	Timeout interval at which an interface receives EFM OAMPDUs. The value is an integer that ranges from 3000 to 30000, in milliseconds. It must be an integer multiple of 1000. The default value is 5000 ms. To set the timeout interval at which an interface receives EFM OAMPDUs, run the **efm timeout** command.
OAMPDU Interval	Timeout interval at which an interface sends EFM OAMPDUs. The value is fixed as 1000, in milliseconds.
Parser	Parser: - forward: device is forwarding non-OAMPDUs to the lower sublayer. - loopback: device is looping back non-OAMPDUs to lower sublayer. - discard: device is discarding non-OAMPDUs.
Multiplexer	Multiplexer: - forward: device is forwarding non-OAMPDUs to higher sublayer. - discard: device is discarding non-OAMPDUs.

Item	Description
ErrCodeNotification	Whether detection of EFM errored codes is enabled: ● disable: indicates that detection of EFM errored codes is disabled. ● enable: indicates that detection of EFM errored codes is enabled. To enable or disable the detection of EFM errored codes, run the **efm error-code notification enable** command.
ErrCodePeriod	Period for detecting EFM errored codes on an interface. The value ranges from 1 to 60, in seconds. The default value is 1s. To set the period for detecting EFM errored codes on an interface, run the **efm error-code period** command.
ErrCodeThreshold	Threshold for detecting EFM errored codes on an interface. The value ranges from 0 to 65535. The default value is 1. To set the threshold for detecting EFM errored codes on an interface, run the **efm error-code threshold** command.
ErrFrameNotification	Whether detection of EFM errored frames is enabled: ● disable: indicates that detection of EFM errored frames is disabled. ● enable: indicates that detection of EFM errored frames is enabled. To enable or disable the detection of EFM errored frames, run the **efm error-frame notification enable** command.
ErrFramePeriod	Period for detecting EFM errored frames on an interface. The value ranges from 1 to 60, in seconds. The default value is 1s. To set the period for detecting EFM errored frames on an interface, run the **efm error-frame period** command.
ErrFrameThreshold	Threshold for detecting EFM errored frames on an interface. The value ranges from 0 to 65535. The default value is 1. To set the threshold for detecting EFM errored frames on an interface, run the **efm error-frame threshold** command.

Item	Description
ErrFrameSecondNotification	Whether detection of EFM errored frame seconds is enabled: - disable: indicates that detection of EFM errored frame seconds is disabled. - enable: indicates that detection of EFM errored frame seconds is enabled. To enable or disable the detection of EFM errored frame seconds, run the **efm error-frame-second notification enable** command.
ErrFrameSecondPeriod	Period for detecting EFM errored frame seconds on an interface. The value ranges from 10 to 900, in seconds. The default value is 60s. To set the period for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second period** command.
ErrFrameSecondThreshold	Threshold for detecting EFM errored frame seconds on an interface. The value ranges from 0 to 900. The default value is 1. To set the threshold for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second threshold** command.
Hold Up Time	Value of the EFM faulty-state holdup timer. The value ranges from 0 to 50, in seconds. The default value is 0. To set the value of the EFM faulty-state holdup timer, run the **efm holdup-timer** command.
ThresholdEvtTriggerErrDown	Whether a threshold crossing event is associated with an interface: - disable: A threshold crossing event is not associated with an interface. - enable: A threshold crossing event is associated with an interface. To set the parameter, run the **efm threshold-event trigger error-down** command.

Item	Description
TriggerIfDown	Whether an interface is blocked when the interface detects a fault on the link between the local and peer interfaces: - disable: The system does not block an interface when detecting a fault on the link between the local and peer interfaces. - enable: The system blocks an interface when detecting a fault on the link between the local and peer interfaces. To set the parameter, run the **efm trigger if-down** command.
TriggerMacRenew	Whether the MAC address entry on an interface is updated when the interface detects a fault on the link between the local and peer interfaces: - disable: The system does not update the MAC address entry when detecting a fault on the link between the local and peer interfaces. - enable: The system updates the MAC address entry when detecting a fault on the link between the local and peer interfaces. To set the parameter, run the **efm trigger mac-renew** command.
Remote MAC	MAC address of the remote interface. The value -- indicates that the system cannot obtain the MAC address of the remote interface.
Remote EFM Enable Flag	Whether EFM is enabled on the remote interface: - disable: indicates that EFM is disabled on the remote interface. - enable: indicates that EFM is enabled on the remote interface. - --: indicates that the system cannot obtain the EFM status on the remote device.
Remote Mode	Operation mode of EFM on the remote interface: - active: indicates that EFM works in active mode. - passive: indicates that EFM works in passive mode. - --: indicates that the system cannot obtain the operation mode of EFM on the remote device.
Remote MaxSize	Maximum size of an OAMPDU on the remote interface, in bytes. The value -- indicates that the system cannot obtain the maximum size of an OAMPDU on the remote interface.

Item	Description
Remote Loopback IgnoreRequest	Whether the remote interface ignores loopback requests from the local end: ● --: The system cannot obtain the mode in which the remote interface processes loopback requests from the local end. ● yes: The remote interface ignores loopback requests from the local end. ● no: The remote interface processes loopback requests from the local end.
Remote State	Active/Standby information of the peer device. The value -- indicates that the system cannot obtain the active/standby information of the peer device.
Remote Parser	Remote parser: ● forward: device is forwarding non-OAMPDUs to the lower sublayer. ● discard: device is discarding non-OAMPDUs.
Remote Multiplexer	Remote Multiplexer: ● forward: device is forwarding non-OAMPDUs to higher sublayer. ● loopback: device is looping back non-OAMPDUs to lower sublayer. ● discard: device is discarding non-OAMPDUs.
ErrFramePeriodNotification	Whether detection of EFM errored frame periods is enabled: ● disable: indicates that detection of EFM errored frame periods is disabled. ● enable: indicates that detection of EFM errored frame periods is enabled.
ErrFramePeriodPeriod	Period for detecting errored frame periods on the interface. The value is an integer that ranges from 20000 to 4294967295. The default value is 200000.
ErrFramePeriodThreshold	Threshold for detecting errored frame periods on the interface. The value is an integer that ranges from 0 to 900. The default value is 1.

Item	Description
Loopback Remain Time	Remaining time of remote loopback: - --: The interface does not send a remote loopback request. - Never Timeout: The interface sends a remote loopback request. The value of **timeout** is 0, indicating that the interface is always in remote loopback state. - Loopback Remain Time: The interface sends a remote loopback request, and the timeout interval of remote loopback is specified.

12.7.4 display efm link-event local

Function

The **display efm link-event local** command displays statistics about local link events.

Format

display efm link-event local { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays statistics about local link events of all interfaces.	-
interface-type interface-number	Displays statistics about local link events of a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After error code detection, error frame detection, or error frame second detection is configured, you can run the **display efm link-event local** command to view statistics about local link events.

Precautions

After the **display efm link-event local** command is run, a hyphen (-) is displayed if error code detection, error frame detection, or error frame second detection is not configured in the interface view.

Example

Displays statistics about local link events on GigabitEthernet0/0/1.

```
<HUAWEI> display efm link-event local interface gigabitethernet 0/0/1
Item                    Value
----------------------------------------------------
Interface:              GigabitEthernet0/0/1
-------------------------
Errored-code
Errors:                 0
Error Running Total :     0
Event Running Total :     0
-------------------------
Errored-frame
Errors:                 0
Error Running Total :     0
Event Running Total :     0
-------------------------
Errored-frame-period
Errors:                 0
Error Running Total :     0
Event Running Total :     0
-------------------------
Errored-frame-seconds
Errors:                 0
Error Running Total :     0
Event Running Total :     0
```

Table 12-40 Description of the display efm link-event local command output

Item	Description
Interface	Interface enabled with EFM.
Errored-code	Information about error code.
Errored-frame	Information about error frame.
Errored-frame-period	Information about error frame period.
Errored-frame-seconds	Information about error frame second.
Errors	Number of currently detected error codes, error frames, error frame period, or error frame seconds.
Error Running Total	Total number of detected error codes, error frames, error frame period, or error frame seconds.

Item	Description
Event Running Total	Count of detected error codes, error frames, error frame period, or error frame seconds.

12.7.5 display efm session

Function

The **display efm session** command displays information about an EFM session between the specified interface and the peer.

Format

display efm session { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays information about EFM sessions between all interfaces configured with EFM and the peers.	-
interface-type interface-number	Displays information about the EFM session between the specified interface and the peer. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether an EFM session configured on a device is negotiated successfully, run the **display efm session** command. The command output includes the EFM status and timeout interval of a loopback test.

- If **all** is specified, information about all EFM sessions configured on the device is displayed.
- If **interface** *interface-type interface-number* is specified, information about EFM sessions configured on a specified interface is displayed.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Display information about EFM sessions between all interfaces and the peers.

```
<HUAWEI> display efm session all
Interface              EFM State              Loopback Timeout
----------------------------------------------------------------------
GigabitEthernet0/0/1      discovery                   --
```

Table 12-41 Description of the display efm session command output

Item	Description
Interface	Interface name.
EFM State	EFM protocol status on the interface: ● disabled: The EFM protocol is disabled on the interface. ● discovery: The interface is in OAM discovery state. ● detect: The interface is in Detect state. ● loopback (control): The interface initiates remote loopback and discards the packets looped back. ● loopback (be controlled): The interface responds to remote loopback.
Loopback Timeout	Timeout interval of a loopback test.

12.7.6 display test-packet result

Function

The **display test-packet result** command displays information about sent test packets.

Format

display test-packet result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After remote loopback is enabled and the **test-packet start** command is used to configure a device to send test packets, the **display test-packet result** command can be used to view information about sent test packets. You can determine link performance based on the information about test packets.

Example

Display information about sent test packets.

```
<HUAWEI> display test-packet result
 TestResult             Value
--------------------------------------------------------
 PacketsSend :            5
 PacketsReceive :          5
 PacketsLost :            0
 BytesSend :              320
 BytesReceive :            320
 BytesLost :             0
 StartTime :             06-13-2012 14:44:13 UTC+03:00
 EndTime :               06-13-2012 14:44:14 UTC+03:00
```

Table 12-42 Description of the display test-packet result command output

Item	Description
PacketsSend	Number of sent test packets.
PacketsReceive	Number of received test packets.
PacketsLost	Number of discarded test packets.
BytesSend	Total length of sent test packets, in bytes.
BytesReceive	Total length of received test packets, in bytes.
BytesLost	Total length of discarded test packets, in bytes.
StartTime	Start time test packets are sent.
EndTime	End time test packets are sent.

12.7.7 efm enable

Function

The **efm enable** command enables EFM globally or on an interface.

The **undo efm enable** command disables EFM globally or on an interface.

By default, EFM is disabled globally. That is, EFM is disabled on all interfaces.

Format

efm enable

undo efm enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using EFM functions, you must enable EFM globally.

After EFM is enabled on an interface, the interface starts to send OAMPDUs to perform point-to-point EFM link detection. EFM link detection can be implemented between two interfaces only after EFM is enabled on the peer interface.

Precautions

When you use the **undo efm enable** command to disable EFM globally, the device deletes all EFM configurations. When the device is implementing remote loopback and sending a great deal of test packets, running the **undo efm enable** command will cause packets to be forwarded.

NOTE

Eth-Trunks do not support EFM.

Example

Enable EFM globally.

```
<HUAWEI> system-view
[HUAWEI] efm enable
Info: Operation succeeded.
```

Enable EFM on Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
Info: Operation succeeded.
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
Info: Operation succeeded.
```

Enable EFM on Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
Info: Operation succeeded.
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
Info: Operation succeeded.
```

12.7.8 efm error-code notification enable

Function

The **efm error-code notification enable** command enables an interface to detect EFM errored codes.

The **undo efm error-code notification enable** command disables an interface from detecting EFM errored codes.

By default, an interface is not enabled to detect EFM errored codes.

Format

efm error-code notification enable

undo efm error-code notification enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.

- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-code notification enable** command enables an interface to detect EFM errored codes. The local device considers a link faulty if the number of detected errored codes within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAMPDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Layer 2 interface GigabitEthernet0/0/1 to detect errored codes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-code notification enable
Info: Operation succeeded.
```

Enable Layer 3 interface GigabitEthernet0/0/1 to detect errored codes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-code notification enable
Info: Operation succeeded.
```

12.7.9 efm error-code period

Function

The **efm error-code period** command sets the period for detecting EFM errored codes on an interface.

The **undo efm error-code period** command restores the default period for detecting EFM errored codes on an interface.

By default, the period for detecting EFM errored codes on an interface is 1s.

Format

efm error-code period *period*

undo efm error-code period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored codes.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 1s.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-code period** *period* command is run to set the period for detecting EFM errored codes, run the **efm error-code notification enable** command to enable an interface to detect EFM errored codes. When the number of detected errored codes during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored codes on Layer 2 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-code period 20
Info: Operation succeeded.
```

Set the period for detecting EFM errored codes on Layer 3 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-code period 20
Info: Operation succeeded.
```

12.7.10 efm error-code threshold

Function

The **efm error-code threshold** command sets the threshold for detecting EFM errored codes on an interface.

The **undo efm error-code threshold** command restores the default threshold for detecting EFM errored codes on an interface.

By default, the threshold for detecting EFM errored codes on an interface is 1.

Format

efm error-code threshold *threshold*

undo efm error-code threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored codes.	The value is an integer that ranges from 0 to 65535. The default value is 1. The value 0 is not recommended.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-code period** *period* command is executed to set the period for detecting EFM errored codes, run the **efm error-code threshold** *threshold* command to set the threshold for detecting errored codes. Run the **efm error-code notification enable** command to enable an interface to detect EFM errored codes. When the number of detected errored codes during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored codes on Layer 2 interfaceGigabitEthernet0/0/1 to 100.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-code threshold 100
Info: Operation succeeded.
```

Set the threshold for detecting EFM errored codes on Layer 3 interface GigabitEthernet0/0/1 to 100.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-code threshold 100
Info: Operation succeeded.
```

12.7.11 efm error-frame notification enable

Function

The **efm error-frame notification enable** command enables an interface to detect EFM errored frames.

The **undo efm error-frame notification enable** command disables an interface from detecting EFM errored frames.

By default, an interface is not enabled to detect EFM errored frames.

Format

efm error-frame notification enable

undo efm error-frame notification enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-frame notification enable** command enables an interface to detect EFM errored frames. The local device considers a link faulty if the number of detected errored frames within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAMPDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Layer 2 interfaceGigabitEthernet0/0/1 to detect errored frames.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame notification enable
Info: Operation succeeded.
```

Enable Layer 3 interface GigabitEthernet0/0/1 to detect errored frames.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame notification enable
Info: Operation succeeded.
```

12.7.12 efm error-frame period

Function

The **efm error-frame period** command sets the period for detecting EFM errored frames on an interface.

The **undo efm error-frame period** command restores the default period for detecting EFM errored frames on an interface.

By default, the period for detecting EFM errored frames on an interface is 1s.

Format

efm error-frame period *period*

undo efm error-frame period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored frames.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 1s.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-code period** *period* command is run to set the period for detecting EFM errored frames on an interface, run the **efm error-frame notification enable** command to enable an interface to detect EFM errored frames. When the number of detected errored frames during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored frames on Layer 2 interface GigabitEthernet0/0/1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame period 20
Info: Operation succeeded.
```

Set the period for detecting EFM errored frames on Layer 3 interface GigabitEthernet0/0/1 to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-frame period 20
Info: Operation succeeded.
```

12.7.13 efm error-frame threshold

Function

The **efm error-frame threshold** command sets the threshold for detecting EFM errored frames on an interface.

The **undo efm error-frame threshold** command restores the default threshold for detecting EFM errored frames on an interface.

By default, the threshold for detecting EFM errored frames on an interface is 1.

Format

efm error-frame threshold *threshold*

undo efm error-frame threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored frames.	The value is an integer that ranges from 0 to 65535. The default value is 1. The value 0 is not recommended.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-frame period** *period* command is executed to set the period for detecting EFM errored frames on an interface, run the **efm error-frame threshold** *threshold* command to set the threshold for detecting errored frames. Run the **efm error-frame notification enable** command to enable an interface to detect EFM errored frames. When the number of detected errored frames during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored frames on interface GigabitEthernet0/0/1 to 100.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame threshold 100
Info: Operation succeeded.
```

12.7.14 efm error-frame-second notification enable

Function

The **efm error-frame-second notification enable** command enables an interface to detect EFM errored frame seconds.

The **undo efm error-frame-second notification enable** command disables an interface from detecting EFM errored frame seconds.

By default, an interface is not enabled to detect EFM errored frame seconds.

Format

efm error-frame-second notification enable

undo efm error-frame-second notification enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-frame-second notification enable** command enables an interface to detect EFM errored frame seconds. The local device considers a link faulty if the number of detected errored frame seconds within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAMPDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Layer 2 interface GigabitEthernet0/0/1 to detect errored frame seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second notification enable
Info: Operation succeeded.
```

Enable Layer 3 interface GigabitEthernet0/0/1 to detect errored frame seconds.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second notification enable
Info: Operation succeeded.
```

12.7.15 efm error-frame-second period

Function

The **efm error-frame-second period** command sets the period for detecting EFM errored frame seconds on an interface.

The **undo efm error-frame-second period** command restores the default period for detecting EFM errored frame seconds on an interface.

By default, the period for detecting EFM errored frame seconds on an interface is 60s.

Format

efm error-frame-second period *period*

undo efm error-frame-second period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored frame seconds.	The value is an integer that ranges from 10 to 900, in seconds. The default value is 60s.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-frame-second period** *period* command is run to set the period for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second notification enable** command to enable an interface to detect EFM errored frame seconds. When the number of detected errored frame seconds during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored frame seconds on Layer 2 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second period 20
Info: Operation succeeded.
```

Set the period for detecting EFM errored frame seconds on Layer 3 interface GigabitEthernet0/0/1 to 20s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second period 20
Info: Operation succeeded.
```

12.7.16 efm error-frame-second threshold

Function

The **efm error-frame-second threshold** command sets the threshold for detecting EFM errored frame seconds on an interface.

The **undo efm error-frame-second threshold** command restores the default threshold for detecting EFM errored frame seconds on an interface.

By default, the threshold for detecting EFM errored frame seconds on an interface is 1.

Format

efm error-frame-second threshold *threshold*

undo efm error-frame-second threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored frame seconds.	The value is an integer that ranges from 0 to 900. The default value is 1. The value 0 is not recommended.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-frame-second period** *period* command is executed to set the threshold for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second threshold** *threshold* command to set the threshold for detecting errored frame seconds. Run the **efm error-frame-second notification enable** command to enable an interface to detect EFM errored frame seconds. When the number of detected errored frame seconds during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored frame seconds on Layer 2 interface GigabitEthernet0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second threshold 10
Info: Operation succeeded.
```

Set the threshold for detecting EFM errored frame seconds on Layer 3 interface GigabitEthernet0/0/1 to 10.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm error-frame-second threshold 10
Info: Operation succeeded.
```

12.7.17 efm holdup-timer

Function

The **efm holdup-timer** command sets the value of the EFM faulty-state holdup timer on an interface.

The **undo efm holdup-timer** command restores the default value interval of the EFM faulty-state holdup timer on an interface.

By default, the value of the EFM faulty-state holdup timer is 0s.

Format

efm holdup-timer *time*

undo efm holdup-timer

Parameters

Parameter	Description	Value
time	Specifies the value of the EFM faulty-state holdup timer on an interface.	The value is an integer that ranges from 0 to 50, in seconds. The default value is 0.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm trigger if-down** command is used to associate EFM with an interface, run the **efm holdup-timer** command to set the value of the EFM faulty-state holdup timer for connectivity faults detected by EFM. The faulty state remains unchanged within the value of the holdup timer. EFM does not detect whether the connectivity fault is cleared until the faulty-state holdup timer expires.

After the failed link recovers, EFM works as follows:

- If *time* is not specified, EFM immediately changes the link status to Up.
- If *time* is specified, EFM changes the link status to Up only after the time specified by *time* expires. This prevents the link from frequently alternating between Up and Down.

Prerequisites

EFM has been enabled globally and on interfaces using the **efm enable** command.

It is recommended that you run the **efm trigger if-down** command to associate EFM with an interface before running the **efm holdup-timer** command to set the value of EFM faulty-state holdup timer on the interface. Otherwise, the holdup timer does not take effect.

Example

Set the value of EFM faulty-state holdup timer on GigabitEthernet0/0/1 to 10s.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger if-down
[HUAWEI-GigabitEthernet0/0/1] efm holdup-timer 10
```

12.7.18 efm loopback

Function

The **efm loopback** command configures an interface to initiate or end an EFM remote loopback.

Format

efm loopback { **start** [**timeout** *timeout*] | **stop** }

Parameters

Parameter	Description	Value
start	Initiate an EFM remote loopback.	-
timeout *timeout*	Specifies the timeout interval of an EFM remote loopback.	The value is an integer that ranges from 0 to 1000, in minutes. The default value is 20. The value 0 indicates that no timeout interval is set. That is, the interface remains in remote loopback state.
stop	Ends an EFM remote loopback.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

NOTE

The S6735-S, S6720-EI and S6720S-EI can only initiate EFM OAM remote loopback requests.

Usage Scenario

EFM remote loopback is used to locate link failures and test the link quality. After remote loopback is enabled, configure the local device to send test packets to the peer device. Based on the statistics about sent and received test packets, you can check connectivity and performance of a specified link.

- If **start** is specified, an interface on the local device sends a remote loopback message to the peer device. After receiving the message, the peer device enters the loopback state. In loopback state, the peer sends back all received packets, except EFM OAMPDUs, to the local device through the interface that has received these packets.
- If **stop** is specified, an interface on the local device sends a remote loopback stop message to the peer device. After receiving the message, the peer device exits from the loopback state.
- If remote loopback is left enabled, the remote device keeps looping back service data, causing a service interruption. To prevent this problem, a capability can be configured to disable remote loopback automatically after a specified timeout interval. By default, the timeout interval for remote loopback is 20 minutes. The remote loopback test stops after 20 minutes. You can set the timeout interval to 0 to keep a link in remote loopback state.

NOTE

The link in remote loopback state will not forward service data. Therefore, execute caution when you set the timeout interval to 0.

Prerequisites

- EFM has been enabled and is in detect state.
- The device has been configured to work in active mode using the **efm mode active** command.

Precautions

After remote loopback is enabled, all packets except EFM OAMPDUs are looped back on the remote device. EFM OAM remote loopback must be implemented on the link that does not need to forward service data. Otherwise, service data forwarding is affected.

Remote loopback is implemented successfully only when EFM protocols at the local end and the peer are in handshake state and EFM at the local end works in active mode. You can use the **display efm session** command to check whether EFM OAM protocols on the local interface and the peer are in handshake state.

Example

Configure Layer 2 interface GigabitEthernet0/0/1 to initiate an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback start
```

Set the timeout interval for an EFM OAM remote loopback on Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback start timeout 10
```

Configure Layer 2 interface GigabitEthernet0/0/1 to stop an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback stop
```

Configure Layer 3 interface GigabitEthernet0/0/1 to initiate an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm loopback start
```

Set the timeout interval for an EFM OAM remote loopback on Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm loopback start timeout 10
```

Configure Layer 3 interface GigabitEthernet0/0/1 to stop an EFM OAM remote loopback.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm loopback stop
```

12.7.19 efm loopback ignore-request

Function

The **efm loopback ignore-request** command enables an interface to ignore loopback requests sent by the remote end.

The **undo efm loopback ignore-request** command restores the default setting for the loopback function on an interface.

By default, an interface supports remote loopback. After receiving a loopback request from a remote end, the interface enters the loopback state.

Format

efm loopback ignore-request

undo efm loopback ignore-request

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Remote loopback is used to monitor link quality and locate link faults. Periodic loopback detection helps detect network faults in a timely manner.

If an interface is in loopback state, the interface loops back all received traffic, causing service interruption and imposing attacks. To solve this problem, run the

efm loopback ignore-request command to enable the interface to reject the remote Ethernet OAM loopback request carried in a Loopback Control OAMPDU sent by a remote interface.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command and the interface is not in loopback state.

Precautions

After the **efm loopback ignore-request** command is run, the interface will discard an OAMPDU carrying a remote loopback request.

Example

Enable Layer 2 interface GigabitEthernet0/0/1 to ignore loopback requests sent by a specified remote interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm loopback ignore-request
```

Enable Layer 3 interface GigabitEthernet0/0/1 to ignore loopback requests sent by a specified remote interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm loopback ignore-request
```

12.7.20 efm mode

Function

The **efm mode** command configures the working mode of EFM on an interface.

The **undo efm mode** command restores the default working mode of EFM on an interface.

By default, EFM on an interface works in active mode.

Format

efm mode { **active** | **passive** }

undo efm mode

Parameters

Parameter	Description	Value
active	Indicates that EFM on an interface works in active mode.	-
passive	Indicates that EFM on an interface works in passive mode.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

EFM supports two connection modes: active and passive. By setting the working mode of EFM OAM, you can configure whether a device can send or receive a specified type of EFM OAMPDU. **Table 12-43** describes the differences between the active and passive modes.

Table 12-43 Capabilities for processing OAMPDUs in active and passive modes

Event	Active Mode	Passive Mode
Initiate a connection request by sending an Information OAMPDU during the discovery process	Supported	Not supported
Respond to a connection request during the discovery process	Supported	Supported
Send Information OAMPDUs	Supported	Supported
Send Event Notification OAMPDUs	Supported	Supported
Send Loopback Control OAMPDUs	Supported	Not supported
Respond to Loopback Control OAMPDUs	Supported (The remote EFM entity must work in active mode.)	Supported

Precautions

- The working mode of EFM can be set on an interface only after EFM is enabled globally and before EFM is enabled on the interface. The working mode of EFM on an interface cannot be changed after EFM is enabled on the interface. Before changing the working mode of EFM on an interface, run the **undo efm enable** command to disable EFM on the interface.

- An EFM connection can only be initiated by an OAM entity working in active mode. An OAM entity working in passive mode waits to receive a connection request from its peer entity.
- Two OAM entities both working in passive mode cannot establish an EFM connection between them.

Example

Configure EFM OAM on Layer 2 interface GigabitEthernet0/0/1 to work in passive mode.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm mode passive
```

Configure EFM OAM on Layer 3 interface GigabitEthernet0/0/1 to work in passive mode.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm mode passive
```

12.7.21 efm packet max-size

Function

The **efm packet max-size** command sets the maximum size of an EFM OAMPDU on an interface. All EFM OAMPDUs that exceed the maximum size on an interface are discarded as invalid packets.

The **undo efm packet max-size** command restores the default maximum size of an EFM OAMPDU on an interface.

By default, the maximum size of an EFM OAMPDU on an interface is 128 bytes.

Format

efm packet max-size *size*

undo efm packet max-size

Parameters

Parameter	Description	Value
size	Specifies the maximum size of an EFM OAMPDU. The size contains the length of Layer 2 frame header and the length of the cyclic redundancy check (CRC) field.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 128 bytes.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **efm packet max-size** command to adjust the maximum size of an EFM OAMPDU so that non-Huawei devices can communicate.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Precautions

The local device and the peer determine the actual value of the maximum size of an EFM OAMPDU through negotiation. The smaller maximum size of an EFM OAMPDU set on the local interface or the peer is used.

Example

Set the maximum size of an EFM OAMPDU on Layer 2 interface GigabitEthernet0/0/1 to 120 bytes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm packet max-size 120
```

Set the maximum size of an EFM OAMPDU on Layer 3 interface GigabitEthernet0/0/1 to 120 bytes.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm packet max-size 120
```

12.7.22 efm src-mac

Function

The **efm src-mac** command configures an interface or bridge MAC address as the source MAC address in an OAMPDU.

The **undo efm src-mac** command restores the default configuration.

By default, a bridge MAC address is used as the source MAC address in an OAMPDU.

Format

efm src-mac { **port** | **bridge** }

undo efm src-mac

Parameters

Parameter	Description	Value
port	Configures an interface MAC address as the source MAC address in an OAMPDU.	-
bridge	Configures a bridge MAC address as the source MAC address in an OAMPDU.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

OAMPDUs support interface or bridge MAC addresses as source MAC addresses. You can run the **efm src-mac** command to configure an interface or bridge MAC address as the source MAC address in an OAMPDU before enabling EFM globally.

Example

Configure an interface MAC address as the source MAC address in an OAMPDU.

```
<HUAWEI> system-view
[HUAWEI] efm src-mac port
```

12.7.23 efm timeout

Function

The **efm timeout** command sets the timeout interval at which EFM OAMPDUs are received.

The **undo efm timeout** command restores the default timeout interval.

By default, the timeout interval at which EFM OAMPDUs are received is 5000 milliseconds.

Format

efm timeout *timeout-value*

undo efm timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the timeout interval at which an interface receives EFM OAMPDUs.	The value is an integer that ranges from 3000 to 30000, in milliseconds. The step is 1000 milliseconds. The default value is 5000 milliseconds.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the timeout interval at which OAMPDUs are received, you can change the time required for connectivity fault detection.

Prerequisites

EFM OAM has been enabled globally but is not enabled on an interface.

Precautions

After the timeout interval expires, the EFM OAM protocol switches back to the discovery state. Ensure that interfaces on both ends of a link use the same timeout interval. Otherwise, EFM session negotiation may fail, or the EFM session may flap.

After EFM OAM is enabled on an interface, the timeout interval cannot be changed.

- A shorter timeout interval indicates a shorter time required for connectivity fault detection.
- A longer timeout interval indicates a longer time required for connectivity fault detection.

Example

Set the timeout interval at which EFM OAMPDUs are received on Layer 2 interface GigabitEthernet0/0/1 to 3000 ms.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm timeout 3000
```

Set the timeout interval at which EFM OAMPDUs are received on Layer 3 interface GigabitEthernet0/0/1 to 3000 ms.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm timeout 3000
```

12.7.24 efm threshold-event trigger error-down

Function

The **efm threshold-event trigger error-down** command associates an EFM threshold crossing event with an interface.

The **undo efm threshold-event trigger error-down** command disassociates an EFM threshold crossing event from an interface.

By default, a threshold crossing event is not associated with an interface.

Format

efm threshold-event trigger error-down

undo efm threshold-event trigger error-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. In this case, you can run the **efm threshold-event trigger error-down** command to associate a threshold crossing event with an interface so that the system sets the administrative state of the interface to Down. As a result, all services on the interface are interrupted.

Prerequisites

EFM has been enabled on an interface using the **efm enable** command.

Follow-up Procedure

Configure the interface to go administratively Up by using either of the following methods:

- Run the **error-down auto-recovery** command to set the auto-recovery delay before an interface goes administratively Up.
- Run the **shutdown** command and then the **undo shutdown** command to restore the administrative state of the interface to Up.

Example

Associate a threshold crossing event with Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm threshold-event trigger error-down
```

Associate a threshold crossing event with Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm threshold-event trigger error-down
```

12.7.25 efm trigger clear-arp vlan

Function

The **efm trigger clear-arp vlan** command clears an ARP entry corresponding to a VLANIF interface.

The **undo efm trigger clear-arp vlan** command cancels the configuration.

By default, an interface does not clear an ARP entry.

Format

efm trigger clear-arp vlan *vlan-id*

undo efm trigger clear-arp vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID in an ARP entry.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

NOTE

The **efm trigger clear-arp vlan** command takes effect only on Layer 2 Ethernet interfaces.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a fault, the EFM module notifies the OAM management module of the fault. The OAM management module searches the EFM fault relationship table based on the interface number and VLAN ID, and then clears the ARP entry that corresponds to the VLANIF interface.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable GigabitEthernet0/0/1 in VLAN 10 to clear ARP entries.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger clear-arp vlan 10
```

12.7.26 efm trigger error-down

Function

The **efm trigger error-down** command associates an error event with an interface.

The **undo efm trigger error-down** command disassociates an error event from an interface.

By default, an error event is not associated with an interface.

Format

efm { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**

undo efm { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**

Parameters

Parameter	Description	Value
critical-event	Indicates an unspecified critical event. It usually refers to a fault on the interface associated with MGR.	-
dying-gasp	Indicates an unrecoverable failure. It usually refers to device restart or power-off.	-
link-fault	Indicates a physical link fault. It usually refers to a fault on an interface.	-
timeout	Indicates the timeout interval at which EFM OAMPDUs are received.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When EFM OAM associated with an interface detects a connectivity fault on a link, the protocol status of the interface goes Down. The interface goes Up after the faulty link recovers.

After the **efm trigger error-down** command is used, the administrative status of the interface goes Down when EFM OAM detects remote **critical-event**, **dying-gasp**, or **link-fault** events, or local **timeout** event. Traffic will not be switched back after the faulty link recovers. Check link quality before switching traffic back to the original link.

Prerequisites

EFM OAM has been enabled globally and on an interface using the **efm enable** command.

Follow-up Procedure

When the protocols status of an interface goes Down because error events are associated with the interface. The protocol status of the interface will not go Up even if the faulty link recovers. In this case, perform either of the following operations:

- Run the **restart (interface view)** command to restart the interface.
- Run the **shutdown (interface view)** and **undo shutdown (interface view)** commands to manually restore the interface.

- Run the **undo efm trigger error-down** command to disable association between error events and an interface.

To configure the shutdown interface to go Up automatically, run the **error-down auto-recovery cause efm-remote-failure interval** *interval-value* command in the system view to enable an interface to go Up and set a recovery delay before the interface enters the error-down state. The interface goes Up automatically after the delay.

Precautions

An interface can be associated with various types of error events. For example, if both **efm critical-event trigger error-down** and **efm dying-gasp trigger error-down** are used, the protocol status of the interface becomes Down when the device receives EFM OAM packets indicating **critical-event** or **dying-gasp** faults.

- Dying Gasp fault notification function supports models such as **Table 12-44** shows.

Table 12-44 Models that support Dying Gasp fault notification

Device Series	Model Unless otherwise specified: • The models listed in the table can send Dying Gasp messages to the remote device and send Dying Gasp alarms (EFM_1.3.6.1.4.1.2011.5.25.136.1.6.5_hwDot3ahEfmNonThresholdEvent) to the NMS. • All interfaces of the device can send Dying Gasp fault notification.
S5720-LI	All models support except S5720-16X-PWH-LI-AC, S5720-28P-LI-AC, S5720-28P-PWR-LI-AC, S5720-28X-PWH-LI-AC, S5720-52P-LI-AC, S5720-52P-PWR-LI-AC, S5720-52X-PWR-LI-ACF
S5720S-LI	S5720S-12TP-LI-AC, S5720S-12TP-PWR-LI-AC, S5720S-28TP-PWR-LI-ACL, and S5720S-28X-LI-24S-AC NOTE • They can send Dying Gasp messages to the remote device only, but cannot send Dying Gasp alarms to the NMS. • A maximum of 30 interfaces can send Dying Gasp messages.
S5720I-SI	All models
S5735-L	All models
S5735S-L	All models support except S5735S-L48P4S-A and S5735S-L48P4X-A
S5735-L1	S5735-L24P4X-A1, S5735-L24T4X-A1, S5735-L24T4X-D1, S5735-L24T4X-QA1, S5735-L32ST4X-A1, S5735-L32ST4X-D1, S5735-L48T4X-A1, S5735-L8P4X-A1, and S5735-L8T4X-A1 support

Device Series	Model **Unless otherwise specified:** **● The models listed in the table can send Dying Gasp messages to the remote device and send Dying Gasp alarms (EFM_1.3.6.1.4.1.2011.5.25.136.1.6.5_hwDot3ahEfmNonThresholdEvent) to the NMS.** **● All interfaces of the device can send Dying Gasp fault notification.**
S5735S-L1	S5735S-L32ST4X-A1 support
S5735S-L-M	All models
S5735-L-I	All models
S500-32ST4X	S500-32ST4X support

- The **efm critical-event trigger error-down** command is used and the remote interface associated with MGR goes Down. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **critical-event** fault.
- The **efm dying-gasp trigger error-down** command is used and the board where the remote interface resides is reset or the system restarts. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **dying-gasp** fault.
- The **efm link-fault trigger error-down** command is used and the physical link of the remote device is faulty. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **link-fault** fault.
- The **efm timeout trigger error-down** command is used on the local device. The local device will set the protocol status of the corresponding interface to Down if it does not receive packets from the remote device in a specified period of time (5s by default).

NOTE

The **efm trigger if-down** and **efm trigger error-down** commands cannot be used simultaneously, and the **efm trigger mac-renew** and **efm trigger error-down** commands cannot be used simultaneously.

Example

Associate **dying-gasp** faults with Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm dying-gasp trigger error-down
```

Associate **dying-gasp** faults with Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm dying-gasp trigger error-down
```

12.7.27 efm trigger if-down

Function

The **efm trigger if-down** command associates EFM with an interface.

The **undo efm trigger if-down** command disassociates EFM from an interface.

By default, EFM OAM is not associated with any interface.

Format

efm trigger if-down

undo efm trigger if-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

EFM can be associated with interfaces. On a scenario with primary and backup links, if EFM detects a fault on the primary link, it will set the protocol status of the associated interface to ETHOAM Down, speeding up routing convergence. Traffic can be fast switched to the backup link.

Prerequisites

EFM has been enabled globally and on an interface, and is in detect state.

Precautions

If EFM is associated with an interface and detects a link fault, the protocol status of the interface becomes ETHOAM Down, and no packet except EFM OAMPDUs can be forwarded by the interface, and all Layer 2 and Layer 3 services are blocked. Therefore, associating EFM with an interface may greatly affect services. When the interface detects link recovery using EFM, the interface can forward all packets and unblocks Layer 2 and Layer 3 services.

If Layer 2 and Layer 3 services are blocked due to a misoperation, run the **undo efm trigger if-down** command in the interface view to restore services.

Example

Associate EFM with Layer 2 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger if-down
```

Associate EFM with Layer 3 interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger if-down
```

12.7.28 efm trigger mac-renew

Function

The **efm trigger mac-renew** command configures the device to clear the MAC address table on a physical interface.

The **undo efm trigger mac-renew** command cancels the configuration.

By default, an interface is not enabled to clear the MAC address table.

Format

efm trigger mac-renew

undo efm trigger mac-renew

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view

NOTE

The **efm trigger mac-renew** command takes effect only on Layer 2 Ethernet interfaces.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you need to configure the device to clear the MAC address table on a physical interface, run the **efm trigger mac-renew** command.

Precautions

EFM has been enabled globally and on an interface using the **efm enable** command.

NOTE

The **efm trigger mac-renew** and **efm trigger if-down** commands cannot be used simultaneously on an interface.

Example

Configure GigabitEthernet0/0/1 to delete the corresponding MAC entry after a fault notification is received.

```
<HUAWEI> system-view
[HUAWEI] efm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] efm enable
[HUAWEI-GigabitEthernet0/0/1] efm trigger mac-renew
```

12.7.29 oam-bind efm interface efm interface

Function

The **oam-bind efm interface efm interface** command enables bidirectional fault notification between EFM modules.

The **undo oam-bind efm interface efm interface** command cancels the configuration.

By default, bidirectional transmission of information about a fault between EFM OAM sessions is not configured.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support this function.

Format

oam-bind efm interface *interface-type interface-number* **efm interface** *interface-type interface-number*

undo oam-bind efm interface *interface-type interface-number* **efm interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface configured with bidirectional fault notification between EFM modules. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at both sides of a device, associate EFM modules on the device to ensure reliable service transmission.

Association between EFM and EFM is bidirectional. EFM modules notify each other of faults.

The following commands are used to associate EFM modules:

- **oam-bind efm interface efm interface**
- **oam-bind ingress efm interface egress efm interface**

Choose the preceding commands in different scenarios according to **Table 12-45**.

Table 12-45 Association between EFM modules

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM modules	Run the **oam-bind efm interface efm interface** command.	Use the following commands: ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM sessions	Choose either of the following commands based on the transmission direction: ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.	None

Prerequisites

The following conditions must be met:

- EFM OAM has been enabled on specified interfaces.
- Two EFM OAM sessions have been associated with each other. When an EFM OAM session is associated with another EFM OAM session, the EFM OAM session cannot be associated with other EFM OAM sessions.

Example

Configure bidirectional fault notification between EFM OAM sessions.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind efm interface gigabitethernet0/0/1 efm interface gigabitethernet0/0/2
```

12.7.30 oam-bind efm interface trigger if-down interface

Function

The **oam-bind efm interface trigger if-down interface** command enables bidirectional fault notification between EFM and an interface.

The **undo oam-bind efm interface trigger if-down interface** command cancels the configuration.

By default, bidirectional transmission of information about a fault between EFM OAM and an interface is not configured.

Format

oam-bind efm interface *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*

undo oam-bind efm interface *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-46 describes the implementation of association between EFM and an interface.

Table 12-46 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): ● To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. ● To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: ● **oam-bind ingress efm interface trigger if-down egress interface** ● **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: ● To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. ● To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Precautions

When configuring bidirectional fault notification between EFM and an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type1 interface-number1*.

- EFM and an interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

Example

Configure bidirectional fault notification between an EFM session and GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind efm interface gigabitethernet 0/0/1 trigger if-down interface
gigabitethernet 0/0/2
```

12.7.31 oam-bind ingress efm interface egress efm interface

Function

The **oam-bind ingress efm interface egress efm interface** command enables an EFM OAM session to report faults to another EFM OAM session.

The **undo oam-bind ingress efm interface egress efm interface** command disables an EFM OAM session from reporting faults to another EFM OAM session.

By default, unidirectional transmission of information about a fault from one EFM OAM session to another EFM OAM session is not configured.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support this function.

Format

oam-bind ingress efm interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2*

undo oam-bind ingress efm interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM OAM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-

Parameter	Description	Value
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. • *interface-type2* specifies the interface type. • *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at both sides of a device, associate EFM modules on the device to ensure reliable service transmission.

Association between EFM and EFM is bidirectional. EFM modules notify each other of faults.

The following commands are used to associate EFM modules:

- **oam-bind efm interface efm interface**
- **oam-bind ingress efm interface egress efm interface**

Choose the preceding commands in different scenarios according to **Table 12-47**.

Table 12-47 Association between EFM modules

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM modules	Run the **oam-bind efm interface efm interface** command.	Use the following commands: ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM sessions	Choose either of the following commands based on the transmission direction: ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device. ● Run the **oam-bind ingress efm interface egress efm interface** command to configure EFM for the link at one side of the device to notify EFM for the link at the other side of the device of faults. **ingress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at one side of the device, and **egress efm interface** *interface-type interface-number* specifies the EFM-capable interface on the link at the other side of the device.	None

Precautions

Ingress EFM OAM reports faults to egress EFM OAM.

Example

Configure an EFM OAM session to report faults to another EFM OAM session.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
```

```
[HUAWEI-oam-mgr] oam-bind ingress efm interface gigabitethernet 0/0/1 egress efm interface
gigabitethernet 0/0/2
```

12.7.32 oam-bind ingress efm interface trigger if-down egress interface

Function

The **oam-bind ingress efm interface trigger if-down egress interface** command enables EFM to report faults to an interface.

The **undo oam-bind ingress efm interface trigger if-down egress interface** command cancels the configuration.

By default, unidirectional transmission of information about a fault from EFM OAM to an interface is not configured.

Format

oam-bind ingress efm interface *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*

undo oam-bind ingress efm interface *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. • *interface-type1* specifies the interface type. • *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. • *interface-type2* specifies the interface type. • *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-48 describes the implementation of association between EFM and an interface.

Table 12-48 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): - To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. - To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: - **oam-bind ingress efm interface trigger if-down egress interface** - **oam-bind ingress interface egress efm interface trigger if-down**

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: ● To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. ● To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Precautions

Before enabling EFM to report faults to an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and the interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

Ingress EFM reports faults to the specified interface.

Example

Configure EFM to report a fault to GigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress efm interface gigabitethernet 0/0/1 trigger if-down egress
interface gigabitethernet 0/0/2
```

12.7.33 oam-bind ingress interface egress efm interface trigger if-down

Function

The **oam-bind ingress interface egress efm interface trigger if-down** command enables an interface to report faults to EFM OAM.

The **undo oam-bind ingress interface egress efm interface trigger if-down** command cancels the configuration.

By default, unidirectional transmission of information about a fault from an interface to EFM OAM is disabled.

Format

oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**

undo oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an inward MEP is configured, bidirectional association between EFM and an EFM-incapable interface of a device can be configured in the OAM management view. This ensures that service traffic can be switched to the backup link if the primary link fails.

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-49 describes the implementation of association between EFM and an interface.

Table 12-49 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): - To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. - To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: - **oam-bind ingress efm interface trigger if-down egress interface** - **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: - To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. - To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Configuration Impact

After an interface goes Down, the status of the associated EFM OAM session does not change. However, the device configured with association sends a message to inform the peer of the fault and triggers the peer to generate an alarm.

Precautions

Before enabling an interface to report faults to EFM OAM, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and an interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

The ingress interface reports faults to egress EFM.

Example

Configure GigabitEthernet0/0/1 to report a fault to EFM.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress interface gigabitethernet 0/0/1 egress efm interface
gigabitethernet 0/0/2 trigger if-down
```

12.7.34 oam-bind interface efm interface trigger if-down

Function

The **oam-bind interface efm interface trigger if-down** command enables bidirectional transmission of fault messages between an interface and EFM OAM.

The **undo oam-bind interface efm interface trigger if-down** command cancels the configuration.

By default, bidirectional transmission of information about a fault between an interface and EFM OAM is not configured.

Format

oam-bind interface *interface-type1 interface-number1* **efm interface** *interface-type2 interface-number2* **trigger if-down**

undo oam-bind interface *interface-type1 interface-number1* **efm interface** *interface-type2 interface-number2* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an inward MEP is configured, bidirectional association between EFM and an EFM-incapable interface of a device can be configured in the OAM management view. This ensures that service traffic can be switched to the backup link if the primary link fails.

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 12-50 describes the implementation of association between EFM and an interface.

Table 12-50 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): - To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. - To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: - **oam-bind ingress efm interface trigger if-down egress interface** - **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: - To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. - To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Prerequisites

Basic EFM OAM functions have been configured.

Precautions

When configuring bidirectional transmission of fault messages between EFM and an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and the interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.
- Association between EFM and an EFM-capable interface and association between EFM and an EFM-incapable interface cannot be configured together.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

Example

Configure bidirectional transmission of fault messages between EFM and GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind interface gigabitethernet 0/0/1 efm interface gigabitethernet 0/0/2
trigger if-down
```

12.7.35 oam-mgr

Function

The **oam-mgr** command displays the OAM management view.

The **undo oam-mgr** command exits from the OAM management view.

Format

oam-mgr

undo oam-mgr

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

CFM can advertise fault information to interfaces or protocol modules. Ethernet OAM fault advertisement is implemented by an OAM manager, application modules, and detection modules. An OAMMGR module associates one module with another. A detection module monitors link status and network performance. If a detection module detects a fault, it instructs the OAMMGR module to notify an application module or another detection module of the fault. After receiving the notification, the application or detection module takes measures to prevent a communication interruption or service quality deterioration. Run the **oam-mgr** command to display the MGR view before associating the CFM module and other modules.

Example

Enter the OAM management view.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr]
```

12.7.36 test-packet start

Function

The **test-packet start** command configures the device to send test packets.

Format

test-packet start interface *interface-type interface-number* [**-c** *count* | **-s** *size*] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface of test packets. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
-c *count*	Specifies the number of test packets to be sent.	The value is an integer that ranges from 1 to 65535. The default value is 5.
-s *size*	Specifies the length of a test packet.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After remote loopback is enabled on the device, run the **test-packet start** command on an interface in active mode to configure the device to send test packets. Then check link connectivity and performance based on returned test packets.

Press **Ctrl+C** to stop sending test packets. After using this command to send test packets, use the **display test-packet result** command to view the test result.

Precautions

During test packet transmission, parameters of sent test packets cannot be changed.

Example

Send test packets from outbound interface GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] test-packet start interface gigabitethernet 0/0/1
```

12.8 CFM Configuration Commands

12.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.8.2 active time

Function

The **active time** command sets the RMEP activation time.

The **undo active time** command deletes the RMEP activation time.

By default, the RMEP activation time is 0 seconds.

Format

active time *time*

undo active time

Parameters

Parameter	Description	Value
time *time*	Specifies the RMEP activation time.	The value ranges from 0 to 600, in seconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **remote-mep ccm-receive enable** command to enable the local device to receive CCMs from an RMEP in the same MA, the local device generates an RMEP connectivity fault alarm in the following situations:

- A connectivity fault is detected between the local MEP and the RMEP using CC.
- The physical link works normally between the local MEP and the RMEP. The remote device is not configured with a MEP when connectivity check is performed or the MEP configuration is later than connectivity check. In this case, if the local MEP does not receive the CCM from the RMEP in consecutive three intervals for sending CCMs, the local device considers that a connectivity fault occurs between the local MEP and the RMEP.

  The RMEP connectivity fault alarm is generated incorrectly. To solve the problem, set the RMEP activation time.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

If the RMEP activation time is set on the local device that is enabled to receive CCMs from a certain RMEP, the local device can receive CCMs at the configured RMEP activation time. That is, the activation time is the time reserved for configuring the RMEP.

At the RMEP activation time, if the local MEP does not receive any CCMs in three consecutive sending intervals, a connectivity fault occurs between the local MEP and the RMEP. Then the local device generates an alarm about the RMEP connectivity fault.

If the local device uses the default RMEP activation time, the local MEP receives CCMs from the RMEP immediately after the local device is enabled to receive CCMs from the RMEP.

NOTE

The RMEP activation time takes effect only for subsequent RMEPs in an MA, but is invalid for existing RMEPs in the MA.

Example

Set the RMEP activation time to 30s.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] active time 30
```

12.8.3 alarm finish time

Function

The **alarm finish time** command sets the clear alarm anti-jitter time.

The **undo alarm finish time** command restores the default clear alarm anti-jitter time.

By default, the clear alarm anti-jitter time is 10000 ms.

Format

alarm finish time *time*

undo alarm finish time

Parameters

Parameter	Description	Value
time *time*	Specifies the clear alarm anti-jitter time.	The value ranges from 0 to 30000, in milliseconds. The step is 500, for example, the anti-jitter time can be 500, 1000, or 1500.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a link fault or link recovery, CFM will send an alarm to the NMS. If CFM frequently detects a link fault or link recovery, alarm flapping occurs. To suppress alarm flapping, run the **alarm finish time** command to set the clear alarm anti-jitter time. This prevents the NMS or system from being affected by frequently reported alarms.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

When detecting link recovery, CFM compares the current link recovery time with the last time the fault was generated. CFM sends an alarm to the NMS only when the time difference is not smaller than the clear alarm anti-jitter time.

Example

Set the clear alarm anti-jitter time to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm finish time 2000
```

12.8.4 alarm occur time

Function

The **alarm occur time** command sets the alarm anti-jitter time.

The **undo alarm occur time** command restores the default alarm anti-jitter time.

By default, the alarm anti-jitter time is 2500 ms.

Format

alarm occur time *time*

undo alarm occur time

Parameters

Parameter	Description	Value
time *time*	Specifies the alarm anti-jitter time.	The value ranges from 0 to 30000, in milliseconds. The step is 500, for example, the anti-jitter time can be 500, 1000, or 1500.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a link fault or link recovery, CFM will send an alarm to the NMS. If CFM frequently detects a link fault or link recovery, alarm flapping occurs. To suppress alarm flapping, run the **alarm occur time** command to set the alarm anti-jitter time. This prevents the NMS or system from being affected by frequently reported alarms.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

When detecting a fault, CFM compares the current fault generation time with the last time the fault was rectified. CFM sends an alarm to the NMS only when the time difference is not smaller than the alarm anti-jitter time.

Example

Set the alarm anti-jitter time to 2000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm occur time 2000
```

12.8.5 alarm rdi track-action disable

Function

The **alarm rdi track-action disable** command disables CFM from being triggered when an RDI alarm is generated.

The **undo alarm rdi track-action disable** command enables CFM to be triggered when an RDI alarm is generated.

By default, CFM is triggered when an RDI alarm is generated.

Format

alarm rdi track-action oam-mgr disable

undo alarm rdi track-action oam-mgr disable

Parameters

Parameter	Description	Value
oam-mgr	Indicates that CFM is associated with another feature in the OAM management view.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CFM is associated with other functions such as EFM and the device receives an RDI alarm, run the **alarm rdi track-action disable** command to disable CFM from being triggered.

Prerequisites

An MD has been created using the **cfm md** *md-name* command, and an MA has been created using the **ma** *ma-name* command.

Example

Disable CFM from being triggered in the OAM MGR view when an RDI alarm is generated.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm rdi track-action oam-mgr disable
```

12.8.6 alarm suppression track-action oam-mgr enable

Function

The **alarm suppression track-action oam-mgr enable** command configures the function of disabling the MGR module from being notified upon processing of LOC alarms in scenarios where both LOC clear alarms and RDI fault alarms exist.

The **undo alarm suppression track-action oam-mgr enable** command disables this function.

By default, this function is disabled on a device.

Format

alarm suppression track-action oam-mgr enable

undo alarm suppression track-action oam-mgr enable

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where both LOC clear alarms and RDI fault alarms are generated on a device, to prevent link flapping, you can configure the device not to notify the MGR module upon processing of LOC clear alarms. Instead, the device reports LOC clear alarms when processing RDI fault alarms.

Precautions

You are advised to run this command only in scenarios where CFM is associated with an interface bidirectionally. Otherwise, fault recovery performance may be affected.

Example

Disable the MGR module from being notified of LOC clear alarms in scenarios where both LOC clear alarms and RDI fault alarms are generated on a device.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] alarm suppression track-action oam-mgr enable
```

12.8.7 ccm-interval

Function

The **ccm-interval** command sets the interval at which a Maintenance Association End Point (MEP) sends or detects Continuity Check Messages (CCMs) in an MA.

The **undo ccm-interval** command restores the default interval.

By default, a MEP in an MA sends or detects CCMs every 1000 ms.

Format

ccm-interval *interval*

undo ccm-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a MEP sends or detects CCMs.	The value is an integer, in milliseconds. The value is as follows: - S6735-S, S6720-EI and S6720S-EI: 100, 1000, or 10000 - S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: 3.3, 10, 100, 1000, or 10000 To use the value of 3.3 or 10, first run the **set service-mode** command to configure the device to work in enhanced mode. - SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S: 1000 or 10000

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To set the interval at which a MEP in an MA sends or detects CCMs, use this command.

Precautions

All the MEPs in an MA must send or detect CCMs at the same interval.

The interval at which CCMs are sent or detected cannot be changed on the device in an MA if one of the following operations is performed:

- The device is enabled to send CCMs using the **mep ccm-send enable** command.
- The device is enabled to receive CCMs using the **remote-mep ccm-receive enable** command.

The **undo mep ccm-send** or **undo mep ccm-receive** command must be run before the interval is reconfigured.

Example

Set the interval for sending or detecting CCMs to 1000 ms within the MA **ma1** where the device is not enabled to send or receive CCMs.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ccm-interval 1000
```

Set the interval for sending or detecting CCMs to 1000 ms within the MA **ma1** where the device is enabled to send and receive CCMs.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] undo mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] undo remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] ccm-interval 1000
```

12.8.8 cfm default md

Function

The **cfm default md** command creates the default MD.

The **undo cfm default md** command deletes the default MD.

By default, the default MD is not created.

Format

cfm default md [**level** *level*]

undo cfm default md

Parameters

Parameter	Description	Value
level *level*	Specifies the level of the default MD.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher MD priority. By default, the level of the default MD is 7 (highest level).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on an MP or a link in an MD, create the default MD.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

The level of the default MD must be higher than that of all MDs to which MEPs configured on the local device belong. In addition, the default MD must be of the same level as the higher-level MD. The default MD transmits higher-level CCMs and creates MIPs to send LTR messages.

On the device configured with the default MD, a MIP can be created based on the default MD in the MA that is not associated with a VLAN. The interface where the default MD is configured generates a MIP based on the MIP creation rule.

To modify the MD level, delete the default MD and reconfigure it.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Create the default MD at level 6.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm default md level 6
```

12.8.9 cfm destination-mac

Function

The **cfm destination-mac** command configures the destination MAC address of a CCM.

The **undo cfm destination-mac** command restores the default setting.

As defined in IEEE 802.1ag/Draft 7.0, the default destination MAC address of a CCM is 0180-C2FF-FFF0.

Format

cfm destination-mac *mac-address*

undo cfm destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address of a CCM.	The value is in the format of H-H-H. A MAC address must start with 0180-c2 and end with 0, and the last three bytes must be greater than 2F. The default value is 0180-C2FF-FFF0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

No specific multicast MAC address is defined in IEEE 802.1ag/Draft 7.0, so devices of different vendors may send CCMs with different multicast MAC addresses. To allow devices of different vendors to interconnect, you must use the same multicast MAC address on these devices. Otherwise, CCMs cannot be transmitted between these devices.

Prerequisites

- The **cfm enable** command has been run to enable CFM globally.
- The **cfm version draft7** command has been run to switch the Ethernet CFM version to IEEE 802.1ag Draft 7.

Example

Set the destination MAC address of a CCM to 0180-C210-FFF0.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm version draft7
[HUAWEI] cfm destination-mac 0180-c210-fff0
```

12.8.10 cfm enable (system view)

Function

The **cfm enable** command enables Connectivity Fault Management (CFM) globally.

The **undo cfm enable** command disables CFM globally.

By default, CFM is disabled globally.

Format

cfm enable

undo cfm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on links, enable CFM globally.

Precautions

After you use the **undo cfm enable** command to disable CFM globally, the device automatically deletes all the CFM configurations, including the configurations of MDs, MAs, MEPs, MIPs, and RMEPs.

All the configuration commands related to the CFM function are valid only after CFM is enabled globally.

Example

Enable CFM globally.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
```

12.8.11 cfm if-down trigger ccm-send-stop

Function

The **cfm if-down trigger ccm-send-stop** command triggers the MEP on an interface to stop sending CCMs when the interface goes Down.

The **undo cfm if-down trigger ccm-send-stop** command restores the default configuration.

By default, the MEP on an interface is not triggered to stop sending CCMs when the interface goes Down.

Format

cfm if-down trigger ccm-send-stop

undo cfm if-down trigger ccm-send-stop

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 12-1 VLAN stacking scenario with an inward-facing MEP configured

As shown in **Figure 12-1**, in a VLAN stacking scenario with an inward-facing MEP configured, a VLL is configured between Switch1 and Switch2, 802.1ag detection is configured between Switch2 and Switch3, and the MEP on Switch3 is inward-facing. If the interface where the MEP resides goes Down, to prevent the MEP from continuing to send CCMs so that other services can detect the fault information detected by CC, run the **cfm if-down trigger ccm-send-stop** command in the interface view.

Prerequisites

Run the **cfm enable** command to enable CFM globally.

Example

Trigger the MEP on GE 0/0/1 to stop sending CCMs when the interface goes Down.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm if-down trigger ccm-send-stop
```

12.8.12 cfm md

Function

The **cfm md** command creates an MD and displays the MD view, or displays the view of an existing MD.

The **undo cfm md** command deletes an MD.

Format

cfm md *md-name* [**format** { **no-md-name** | **dns** *dns-md-format-name* | **mac-address** *mac-md-format-name* | **string** *string-md-format-name* }] [**level** *level*]

undo cfm md [*md-name*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The name of an MD on a device must be unique. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
no-md-name	Indicates that the MA ID field of a sent packet does not contain an MD name.	-
dns *dns-md-format-name*	Specifies the DNS name used as the MD name carried in packets.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mac-address *mac-md-format-name*	Specifies an MD name carried in packets, in the format of H-H-H:U<0-65535>, for example, 0001-0001-0001:1.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
string *string-md-format-name*	Specifies an ASCII MD name.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
level *level*	Specifies the level of an MD.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher MD priority. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure CFM to identify and locate faults on links, use this command to create an MD.

Precautions

All the CFM-enabled devices of an ISP can be added to the same MD.

NOTE

When 802.1ag packets in a low-level MD enter a high-level MD, the 802.1ag packets will be discarded. 802.1ag packets in a high-level MD can traverse a low-level MD. 802.1ag packets in an MD cannot traverse the MD of the same level.

Only IEEE Standard 802.1ag-2007 supports **format**, **no-md-name**, **dns** *dns-md-format-name*, **mac-address** *mac-md-format-name*, and **string** *string-md-format-name*.

The MD name format can be specified during the MD configuration, as defined in IEEE Standard 802.1ag-2007. Each MD can be configured with only one name format and one level. You can use the **cfm md** command to enter the view of the existing MD but cannot change the name format and level of the existing MD. To change the name format and level of the existing MD, delete the MD and then use the **cfm md** command to create a new MD.

As defined in IEEE 802.1ag Draft 7, after creating an MD, you cannot use the **cfm md** command to change the level of the MD. To change the level of the MD, you need to delete the MD and then create an MD again.

When an MD is deleted, a device automatically deletes all the configurations of MAs, MEPs, MIPs, and RMEPs within the MD.

The MA, MEP, and RMEP must be created within an MD, so you must create an MD before creating the MA, MEP, and RMEP.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Create an MD named **mdcustomer** at level 4.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md mdcustomer level 4
```

Change the level of **mdcustomer** from 4 to 6.

```
<HUAWEI> system-view
[HUAWEI] undo cfm md mdcustomer
```

```
Warning: Deleting the MD(s) will delete all information about the MA(s). Continue?[Y/N]:y
[HUAWEI] cfm md mdcustomer level 6
```

Create an MD named **mdcustomer** at level 4, with the MD name in **no-md-name** format.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md mdcustomer format no-md-name level 4
```

12.8.13 cfm mip

Function

The **cfm mip level** command creates a MIP on an interface.

The **undo cfm mip** command deletes a MIP on an interface.

By default, no MIP is created.

Format

cfm mip level *level-value*

undo cfm mip

Parameters

Parameter	Description	Value
level *level-value*	Specifies the level of a MIP.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on an MP or a link in an MD, create a MIP in the MD.

A MIP is located inside the MD. It can process and respond to CCMs, but cannot send CCMs. When a MIP receives a packet carrying a level higher than its own, the MIP does not process the packet and forwards it along the original path. A MIP forwards only the packet in which the level is lower than or equal to its own.

If a MIP is created and an MP performs LB or LT, the MIP will reply with LBMs or LTMs to identify and locate faults for the MP or link in the MD.

A MIP can be created manually or automatically:

- The **cfm mip level** *level-value* command can be used to manually create a MIP. This configuration is simple, but it is difficult to manage many MIPs and configuration errors may occur.
- The **mip create-type (MD view)** command can be used to define the rule for creating a MIP and enable the device to automatically create a MIP based on the rule. Configuring creation rules is complex, but properly configured rules ensure correct MIP settings.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

Only IEEE Std 802.1ag-2007 supports the manual MIP configuration.

Example

Create a MIP at level 4.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm mip level 4
```

12.8.14 cfm portid-tlv type

Function

The **cfm portid-tlv type** command sets the portid-tlv type for trace packets.

The **undo cfm portid-tlv type** command restores the default portid-tlv type for trace packets.

By default, the portid-tlv type in trace packets is in character string format.

Format

cfm portid-tlv type { **interface-name** | **local** }

undo cfm portid-tlv type

Parameters

Parameter	Description	Value
interface-name	Indicates that the portid-tlv type is in character string format.	-
local	Indicates that the portid-tlv type is in Huawei proprietary format.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using the trace function, you need to specify the type of inbound and outbound interface names. You can use the **cfm portid-tlv type** command to set the type of interface names.

Precautions

NOTE

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007. Before using the **cfm portid-tlv type** command, you must use the **cfm version** command to set the Ethernet CFM version to IEEE Standard 802.1ag-2007.

Vendors may use different TLV types. To implement interworking between Huawei and non-Huawei devices, configure **interface-name** to specify the interface name type in character string format.

If all the devices running on the entire network are Huawei data communications devices, to interwork with devices running different versions, configure **local** to specify the interface name type in Huawei proprietary format.

Example

Configure the portid-tlv type in character string format.

```
<HUAWEI> system-view
[HUAWEI] cfm portid-tlv type interface-name
```

12.8.15 cfm protocol

Function

The **cfm protocol** command configures the EtherType value of a CCM.

The **undo cfm protocol** command restores the default setting.

As defined in IEEE 802.1ag/Draft 7, the default EtherType value of a CCM is 0xBBB0.

Format

cfm protocol *ethertype-value*

undo cfm protocol

Parameters

Parameter	Description	Value
ethertype-value	Specifies the EtherType value of a CCM.	The value is an integer that ranges from 0600 to FFFF. The default value is BBB0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

No specific protocol type is defined in IEEE 802.1ag/Draft 7, so devices of different vendors may use different protocols to encapsulate CCMs. To allow devices of different vendors to interwork with each other, you must run the **cfm protocol** command to configure the same protocol types on these devices. Otherwise, these devices cannot communicate.

NOTE

You must run the **cfm enable** command to enable CFM globally before configuring the protocol type.

Example

Set the EtherType value of a CCM to 0900.

```
<HUAWEI> system-view
[HUAWEI] cfm protocol 0900
```

12.8.16 cfm trigger if-down

Function

The **cfm trigger if-down** command associates Ethernet CFM with an interface.

The **undo cfm trigger if-down** command disassociates Ethernet CFM from an interface.

By default, an interface is not associated with Ethernet CFM.

Format

cfm md *md-name* **ma** *ma-name* **remote-mep mep-id** *mep-id* **trigger if-down**

undo cfm md *md-name* **ma** *ma-name* **remote-mep mep-id** *mep-id* **trigger if-down**

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD in an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
remote-mep mep-id *mep-id*	Specifies ID of an RMEP.	The value is an integer that ranges from 1 to 8191.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CFM can be associated with interfaces. On a scenario with active and standby links, when CFM detects a fault on the active link, the OAM management module shuts down the interface and enables the interface 7 seconds later. This speeds up route convergence. In addition, traffic can be fast switched to the standby link.

Precautions

An interface can be bound to only one RMEP. To modify the association between the interface and the RMEP, delete the current configuration and then configure the new association.

Prerequisites

An outward-facing MEP has been created in the specified MA and the MEP has been created on the interface.

Example

Associate Ethernet CFM with GigabitEthernet0/0/1. The MD name, MA name, and RMEP ID are **md1**, **ma1**, and 2 respectively.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm md md1 ma ma1 remote-mep mep-id 2 trigger if-down
```

12.8.17 cfm trigger clear-arp vlan

Function

The **cfm trigger clear-arp vlan** command clears an ARP entry corresponding to a VLANIF interface.

The **undo cfm trigger clear-arp vlan** command cancels the configuration.

By default, an interface is disabled from clearing an ARP entry.

Format

cfm md *md-name* **ma** *ma-name* **trigger clear-arp vlan** *vlan-id*

undo cfm md *md-name* **ma** *ma-name* **trigger clear-arp vlan** *vlan-id*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD in an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
vlan *vlan-id*	Specifies the VLAN ID in an ARP entry.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a fault, the CM module notifies the OAM management module of the fault. The OAM management module searches the CM fault relationship table based on the interface number and VLAN ID, and then clears the ARP entry that corresponds to the VLANIF interface.

Precautions

Before associating Ethernet CFM with an interface, you must create an outward-facing MEP in the specified MA and ensure that the MEP is on the interface.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Enable GigabitEthernet0/0/1 to clear an ARP entry matching VLANIF 10 after receiving a fault notification.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] cfm md md1 ma ma1 trigger clear-arp vlan 10
```

12.8.18 cfm trigger vlan mac-renew

Function

The **cfm trigger vlan mac-renew** command clears MAC address entries of a range of VLANs associated with Ethernet CFM after Ethernet CFM detects a fault.

The **undo cfm trigger vlan mac-renew** command cancels the configuration.

Format

cfm trigger vlan { { *vlan-id* [**to** *vlan-id*] } &<1-10> } **mac-renew**

undo cfm trigger vlan { { *vlan-id* [**to** *vlan-id*] } &<1-10> } **mac-renew**

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **cfm trigger vlan mac-renew** command is run, CFM deletes MAC address entries of a range of configured VLANs when detecting a fault so that services can be switched between links.

Precautions

A maximum of 10 VLAN ranges can be configured. The VLAN ranges cannot overlap.

When CFM detects a fault in a VLAN associated with the MA in the range specified in this command, the MAC address entries of this VLAN are deleted. If a fault is detected in a VLAN out of the specified range, the MAC address entries of this VLAN are not deleted.

If the **cfm trigger vlan mac-renew** command is run multiple times, MAC addresses of VLANs specified by the commands are deleted.

Example

Configure the device to clear MAC address entries of VLANs 100 to 200 after CFM detects a fault.

```
<HUAWEI> system-view
[HUAWEI] cfm trigger vlan 100 to 200 mac-renew
```

12.8.19 cfm version

Function

The **cfm version** command switches an Ethernet CFM version between IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007.

The **undo cfm version** command restores the default Ethernet CFM version.

By default, IEEE Standard 802.1ag-2007 is enabled on a device.

Format

cfm version { **draft7** | **standard** }

undo cfm version

Parameters

Parameter	Description	Value
draft7	Indicates IEEE 802.1ag Draft 7.	-
standard	Indicates IEEE Standard 802.1ag-2007.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to switch IEEE 802.1ag between the two versions when the device supports both IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007.

Precautions

To ensure that CFM works properly, all devices on the entire network must run IEEE 802.1ag of the same version. During switching between IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007, all 802.1ag functions are unavailable. You can run the **cfm enable (system view)** command to enable CFM globally only after all devices use the same IEEE 802.1ag version.

Example

Switch IEEE Standard 802.1ag-2007 to IEEE 802.1ag Draft 7.

```
<HUAWEI> system-view
[HUAWEI] cfm version draft7
```

12.8.20 display cfm default md

Function

The **display cfm default md** command displays information about the default MD.

Format

display cfm default md

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm default md** command to view information about the level of the default MD, MIP creation rule, Sender ID TLV type, and IDs of VLANs associated with the default MD.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Display information about the default MD.

```
<HUAWEI> display cfm default md
Level   MIP-Create-type   SenderID TLV-type   VLAN-List
-------------------------------------------------------------------------------------
7       default           defer               100 to 200 2049
```

Table 12-51 Description of the **display cfm default md** command output

Item	Description
Level	Level of the default MD. The value ranges from 0 to 7. A higher level represents a higher priority of the default MD.
MIP-Create-type	MIP creation rule: ● default ● explicit ● none
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: ● none ● chassis ● manage ● chassisManage ● defer
VLAN-List	IDs of VLANs associated with the default MD.

12.8.21 display cfm error-info

Function

The **display cfm error-info** command displays the incorrect configuration of the specified error type.

Format

display cfm error-info error-type unexpected-mep [**md** *md-name* **ma** *ma-name* **mep-id** *mep-id*]

Parameters

Parameter	Description	Value
error-type unexpected-mep	Indicates the error about an unexpected MEP ID.	-

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The name of an MD is unique. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
mep-id *mep-id*	Specifies the ID of a MEP. The ID identifies a MEP. The MEP ID must be unique in an MA and in a VLAN.	The value is an integer that ranges from 1 to 8191.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If CFM cannot work properly, run the **display cfm error-info** command to check received CCMs with unknown MEP IDs. The information helps diagnose a fault.

- If no parameter is configured in the **display cfm error-info** command, the device displays CCMs with unexpected MEP IDs received by all MEPs.

- If an MD name, an MA name, or a MEP ID is specified, the device displays CCMs with unexpected MEP IDs received by a specified MEP.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Display information about received CCMs with unexpected MEP IDs saved on the device.

```
<HUAWEI> display cfm error-info error-type unexpected-mep
 The total number of unexpected MEPs is : 1
--------------------------------------------------
 MD Name            : md
 Level              : 0
 MA Name            : ma
 MEP ID             : 1
 Unexpected MEP List:
 Unexpected MEP ID  : 2
 MAC Address        : 00e0-fc44-81a4
```

Table 12-52 Description of the **display cfm error-info** command output

Item	Description
MD Name	MD name in CCMs.
Level	Level of an MA.
MA Name	MA name in CCMs.
MEP ID	ID of a MEP in CCMs.
Unexpected MEP List	Unexpected MEP information.
Unexpected MEP ID	Unexpected MEP ID.
MAC Address	MAC address in CCMs.

12.8.22 display cfm ma

Function

The **display cfm ma** command displays detailed information about an MA.

Format

display cfm ma [**md** *md-name* [**ma** *ma-name*]]

Parameters

Parameter	Description	Value
md *md-name*	Displays detailed MA information in a specified MD. *md-name* specifies the name of the MD. If the parameter is not specified, detailed information about all MAs in all MDs is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Displays detailed information about the specified MA. *ma-name* specifies the name of the MA. If *md-name* is specified but this parameter is not specified, detailed information about all the MAs in the specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an MA is configured or CFM cannot work properly, use the **display cfm ma** command to check the MA configuration and the number of MEPs and RMEPs in the MA.

Example

Display detailed information about the MA named **ma1** in the MD named **md1**.

```
<HUAWEI> display cfm ma md md1 ma ma1
 MD Name             : md1
 MD Name Format      : string
 Level               : 0
 MIP Create-type     : none
 SenderID TLV-type   : defer
 MA Name             : ma1
 MA Name Format      : string
```

```
 Interval           : 1000
 Priority           : 7
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MEP Number         : 1
 RMEP Number        : 1
 Suppressing Alarms : No
 Sending AIS Packet : No
 Interface TLV      : disabled
 RDI Track-action   : all-enabled
```

Display detailed information about all the MAs in the specified MD.

```
<HUAWEI> display cfm ma md md1
The total number of MAs is : 2
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA Name            : ma1
 MA Name Format     : string
 Interval           : 1000
 Priority           : 7
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MEP Number         : 1
 RMEP Number        : 1
 Suppressing Alarms : No
 Sending AIS Packet : No
 Interface TLV      : disabled
 RDI Track-action   : all-enabled
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA Name            : ma2
 MA Name Format     : string
 Interval           : 1000
 Priority           : 7
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MEP Number         : 1
 RMEP Number        : 1
  Suppressing Alarms : No
 Sending AIS Packet : No
 Interface TLV      : disabled
 RDI Track-action   : all-enabled
```

Display detailed information about all the MAs in the MD named **md** in **no-md-name** format.

```
<HUAWEI> display cfm ma md md
The total number of MAs is : 2
--------------------------------------------------
 MD Name            : md
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA Name            : ma
 MA Name Format     : no-md-name
 Interval           : 1000
 Priority           : 7
 VLAN ID            : --
```

```
VSI Name           : --
L2VC ID            : --
MEP Number         : 0
RMEP Number        : 1
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV      : disabled
RDI Track-action   : all-enabled

MD Name            : md
MD Name Format     : string
Level              : 0
MIP Create-type    : none
SenderID TLV-type  : defer
MA Name            : ma
MA Name Format     : no-md-name
Interval           : 1000
Priority           : 7
VLAN ID            : --
VSI Name           : --
L2VC ID            : --
MEP Number         : 0
RMEP Number        : 1
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV      : disabled
RDI Track-action   : all-enabled
```

Table 12-53 Description of the **display cfm ma** command output

Item	Description
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string To set the format of the MD name, run the **cfm md** command.
Level	MD level. The value ranges from 0 to 7. To set the MD level, run the **cfm md** command.
MIP Create-type	MIP creation rule: ● default ● explicit ● none To set the MIP creation rule, run the **mip create-type** or **mip create-type** command.

Item	Description
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: - none - chassis - manage - chassisManage - defer To set the type of the Sender ID TLV filled in the CCM, run the **senderid-tlv-type** command.
MA Name	Name of the MA. To set the name of the MA, run the **ma** command.
MA Name Format	Format of the MA name: - icc-based - string To set the format of the MA name, run the **ma** command.
Interval	Interval at which CCMs are sent in an MA. To set the interval at which CCMs are sent in an MA, run the **ccm-interval** command.
Priority	802.1p priority of CFM packets in an MA. The value ranges from 0 to 7. A larger value indicates a higher priority. The default value is 7. To set the 802.1p priority of CFM packets in an MA, run the **packet-priority** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the L2VC associated with an MA.
MEP Number	Number of MEPs in an MA.
RMEP Number	Number of RMEPs in an MA.

Item	Description
Suppressing Alarms	Whether the device is enabled to suppress alarms.
Sending AIS Packet	Whether the device is sending AIS PDUs.
Interface TLV	Whether the CCM TLV is enabled: ● disabled ● enabled
RDI Track-action	Whether the device is RDI Track-action.

12.8.23 display cfm md

Function

The **display cfm md** command displays MD information, including the MD name and level.

Format

display cfm md [*md-name*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD. If *md-name* is not specified, information about all MDs created on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm md** command to view MD information, including the MD level, MD name format, MIP creation rule in the MD, and Sender ID TLV type. In addition, you can view brief information about MAs in the MD, such as the MA name, interval at which CCMs are sent, ID of the VLAN associated with the MA, and name of the VSI associated with the MA. If *md-name* is not specified, information about all the created MDs is displayed.

Example

Display information about the MD named **mdcustomer** on the device running IEEE Standard 802.1ag-2007.

```
<HUAWEI> display cfm md mdcustomer
 MD Name            : mdcustomer
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA list            :
        MA Name            : ma
        MA Name Format     : string
        Interval           : 1000
        VLAN ID            : 100
        VSI Name           : --
        L2VC ID            : --
```

Table 12-54 Description of the **display cfm md** command output

Item	Description
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string To set the format of the MD name, run the **cfm md** command.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority. To set the level of the MD, run the **cfm md** command.

Item	Description
MIP Create-type	MIP creation rule: - default - explicit - none To set the MIP creation rule, run the **mip create-type** command.
SenderID TLV-type	Type of the Sender ID TLV in the CCM: - none - chassis - manage - chassisManage - defer To set the type of the Sender ID TLV in the CCM, run the **senderid-tlv-type** command.
MA list	Information about MAs in the MD.
MA Name	Name of the MA. To set the MAs in the MD, run the **ma** command.
MA Name Format	Format of the MA name: - icc-based - string To set the format of the MA name, run the **ma** command.
Interval	Interval at which CCMs are sent. To set the interval at which CCMs are sent, run the **ccm-interval** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA. The switch does not support this function.
L2VC ID	ID of the L2VC associated with an MA. The switch does not support this function.

12.8.24 display cfm mep

Function

The **display cfm mep** command displays information about a MEP in a specified MD and MA.

Format

display cfm mep [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]

Parameters

Parameter	Description	Value
md *md-name*	Displays information about MEPs in a specified MD. *md-name* specifies the name of the MD. If this parameter is not specified, information about MEPs in all MDs and MAs on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Displays information about MEPs in a specified MA. *ma-name* specifies the name of the MA. If this parameter is not specified, information about MEPs in all the MAs of a specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mep-id *mep-id*	Displays information about a specified MEP. *mep-id* specifies the ID of the MEP.	The value is an integer that ranges from 1 to 8191.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a MEP is configured or CFM cannot work properly, use the **display cfm mep** command to check the MEP configuration.

Example

Display information about the MEP with an ID of 10 in the MA named **ma1** of the MD named **md1**.

```
<HUAWEI> display cfm mep md md1 ma ma1 mep-id 10
```

```
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma1
 MEP ID             : 2
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 00e0-fc03-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```

Display information about all MEPs in the MA named **ma1** of the MD named **md1**.

```
<HUAWEI> display cfm mep md md1 ma ma1
The total number of MEPs is : 1
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma1
 MEP ID             : 2
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 00e0-fc03-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```

Display information about all MEPs in the MD named **md1**.

```
<HUAWEI> display cfm mep md md1
The total number of MEPs is : 2
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma1
 MEP ID             : 2
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 00e0-fc03-0161
 MEP Pe-vid         : --  MEP Ce-vid         : --  MEP Vid            : --  Alarm Status       : LOC  Alarm AIS          :
enabled  Alarm RDI          : enabled
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma2
 MEP ID             : 4
 VLAN ID            : --
 VSI Name           : --
```

```
L2VC ID            : --
Interface Name     : GigabitEthernet0/0/2
CCM Send           : enabled
Direction          : outward
MAC Address        : 00e0-fc03-0161
MEP Pe-vid         : --
MEP Ce-vid         : --
MEP Vid            : --
Alarm Status       : LOC
Alarm AIS          : enabled
Alarm RDI          : enabled
```

Table 12-55 Description of the **display cfm mep** command output

Item	Description
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: - no-md-name - dns - mac-address - string To set the format of the MD name, run the **cfm md** command.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority of the MD. To set the MD level, run the **cfm md** command. **NOTE** If the level of a MEP on an intermediate node is higher than or equal to that on the source node, run the **cfm md** command to decrease the level of the MEP on the intermediate node to be lower than that on the source node.
MA Name	Name of the MA. To set the name of the MA, run the **ma** command.
MEP ID	ID of the MEP. To set the ID of the MEP, run the **mep mep-id** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the L2VC associated with an MA.

Item	Description
Interface Name	Interface where a MEP is configured. If a MEP is based on VLANIF interfaces, this field is displayed as --.
CCM Send	Whether the MEP is enabled to send CCMs: - enabled: The MEP is enabled to send CCMs. - disabled: The MEP is disabled from sending CCMs. To set the parameter, run the **mep ccm-send enable** command.
Direction	Type of the MEP: - inward: indicates an inward-facing MEP. An inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA, but does not send 802.1ag packets to the interface where the MEP is configured. - outward: indicates an outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured. **NOTE** If the MEP direction is incorrect, run the **mep mep-id** command to configure a correct direction.
MAC Address	MAC address of the MEP.
MEP Pe-vid	Outer VLAN ID of the QinQ interface where the MEP is configured.
MEP Ce-vid	Inner VLAN ID of the QinQ interface where the MEP is configured.
MEP Vid	VLAN ID of the Dot1q interface where the MEP is configured.
Alarm Status	Alarm type: - unexpectedMEP: The MEP receives CCMs with an unexpected flag. - mismerge: The MEG ID in received CCMs is different from that configured for the MEP. - unexpectedPeriod: The interval in the received CCMs is different from the configured interval. - unexpectedMAC: The MEP MAC address in the received CCM is different from at least one MAC address of the RMEP. - LOC: At least one session between the MEP and an RMEP is terminated. - RDI: The MEP receives CCMs with the RDI.

Item	Description
Alarm AIS	Whether the alarm reporting function of a specific alarm indication signal (AIS) is enabled: - enable - disable
Alarm RDI	Whether the alarm reporting function of a specific remote defect indication (RDI) is enabled: - enable - disable

12.8.25 display cfm mip

Function

The **display cfm mip** command displays MIP information.

Format

display cfm mip [**interface** *interface-type interface-number* | **level** *level*]

Parameters

Parameter	Description	Value
level *level*	Displays information about a MIP of a specified level. *level* specifies the level of the MIP.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher level.
interface-type interface-number	Displays MIP information on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm mip** command to check MIPs, interfaces where MIPs are configured, and levels of the MIPs on the device.

Precautions

If **level** *level* and **interface** *interface-type interface-number* are not specified, information about all MIPs on the device is displayed.

Example

Display information about all MIPs.

```
<HUAWEI> display cfm mip
Interface Name              Level      MAC
-------------------------------------------------------
GigabitEthernet0/0/1          0         00e0-fc02-377f
GigabitEthernet0/0/1          0         00e0-fc02-375f
```

Display information about the MIP at level 7.

```
<HUAWEI> display cfm mip level 7
Interface Name              Level      MAC
-------------------------------------------------------
GigabitEthernet0/0/1          7         00e0-fc02-367f
GigabitEthernet0/0/1          7         00e0-fc02-365f
```

Display information about MIPs on GigabitEthernet0/0/1.

```
<HUAWEI> display cfm mip interface gigabitethernet 0/0/1
Interface Name              Level      MAC
-------------------------------------------------------
GigabitEthernet0/0/1          0        00e0-fc02-368f
```

Display information about MIPs on the GigabitEthernet0/0/1.

```
<HUAWEI> display cfm mip interface gigabitethernet 0/0/1
Info: The MIP does not exist.
```

Table 12-56 Description of the **display cfm mip** command output

Item	Description
Interface Name	Name of the interface where a MIP is configured.
Level	Level of the MIP. The value ranges from 0 to 7. A larger value indicates a higher priority. To set the level of the MIP, run the **cfm mip** command.
MAC	MAC address of the MIP.

12.8.26 display cfm mp-info

Function

The **display cfm mp-info** command displays information about CFM objects on a specified interface or in a VLAN.

Format

display cfm mp-info [**interface** *interface-type interface-number*] [**level** *md-level*] [**inward** | **outward**] [**vlan** *vlanid* | **no-associated-vlan**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays CFM information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
level *md-level*	Specifies the level of an MD.	The value is an integer that ranges from 0 to 7. By default, the value is 0.
inward	Indicates the inward-facing MEP. An inward-facing MEP sends 802.1ag packets through all interfaces in a VLAN associated with an MA, except the interface on which the MEP is configured. That is, the inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA.	-
outward	Indicates the outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured.	-
vlan *vlanid*	Displays CFM information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
no-associated-vlan	Indicates the MP that is not associated with a VLAN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display cfm mp-info** command to view information about CFM objects and the relationship between MPs on the interface so that you can configure MEPs correctly.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Multiple MEPs can be configured and multiple MIPs can be generated on an interface; however, the levels of MEPs or MIPs must be the same. If the configuration is incorrect, CCM leak occurs or LBR or LTR messages cannot be sent correctly.

Example

Display information about the specified interface, MD level, MEP type, and VLAN.

```
<HUAWEI> display cfm mp-info interface gigabitethernet 0/0/1
The total number of MPs is : 1
The number of MEPs is : 1. The number of MIPs is : 0.
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma2
 MEP ID             : 4
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : GigabitEthernet0/0/1
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 00e0-fc03-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```

Table 12-57 Description of the **display cfm mp-info** command output

Item	Description
Interface Name	Name of the interface.
MD Name	Name of the MD. To set the name of the MD, run the **cfm md** command.
MD Name Format	Format of the MD name: - no-md-name - dns - mac-address - string To set the format of the MD name, run the **cfm md** command.
Level	Level of the MD, MA, or MP. The value ranges from 0 to 7. A higher level indicates a higher priority. To set the MD level, run the **cfm md** command.
MA Name	Name of the MA. To set the name of the MA, run the **ma** command.
MEP ID	ID of the MEP. To set the ID of the MEP, run the **mep mep-id** command.
CCM Send	Whether the MEP is enabled to send CCMs: - enabled - disabled To set the parameter, run the **mep ccm-send enable** command.
Direction	Type of the MEP: - inward - outward To set the type of the MEP, run the **mep mep-id** command.
VLAN ID	ID of the VLAN associated with an MA. To set the ID of the VLAN associated with an MA, run the **map** command.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the L2VC associated with an MA.

Item	Description
MAC Address	MAC address of the MEP or MIP. **NOTE** An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.
MEP Pe-vid	VLAN ID in the outer tag of a VLAN frame.
MEP Ce-vid	VLAN ID in the inner tag of a VLAN frame.
MEP Vid	ID of a VLAN.
Alarm Status	Type of alarm: ● unexpectedMEGLevel: The MD level carried in a CCM sent by the RMEP was different from that specified on the MEP. ● unexpectedMEP: The trap about inconsistency between the MD level carried in a CCM sent by the RMEP and that specified on the MEP was cleared. ● mismerge: An MD or MA name carried in a CCM sent by the RMEP was different from that specified on the MEP. ● unexpectedPeriod: The CCM interval carried in a CCM sent by the RMEP was different from that specified on the MEP. ● unexpectedMAC: The source MAC address carried in a CCM sent by the RMEP was different from the RMEP's MAC address specified on the MEP. ● LOC: At least one session between the MEP and an RMEP is terminated. ● exceptionalMACstatus: TLV information carried in a CCM sent by the RMEP within a specified interval showed that the interface connecting the RMEP to the MEP became abnormal. ● RDI: The RMEP sent a CCM carrying the RDI flag with the value of 1 to the MEP.
Alarm AIS	Whether the alarm reporting function of a specific alarm indication signal (AIS) is enabled: ● enable ● disable

Item	Description
Alarm RDI	Whether the alarm reporting function of a specific remote defect indication (RDI) is enabled: ● enable ● disable

12.8.27 display cfm remote-mep

Function

The **display cfm remote-mep** command displays information about RMEPs in a specified MD and MA.

Format

display cfm remote-mep md *md-name* **ma** *ma-name* **mep-id** *mep-id*

display cfm remote-mep [**md** *md-name* [**ma** *ma-name*]] [**cfm-state** { **up** | **down** | **disable** }]

Parameters

Parameter	Description	Value
md *md-name*	Displays information about RMEPs in a specified MD. *md-name* specifies the name of the MD. If this parameter is not specified, information about RMEPs in all MDs and MAs on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?).
ma *ma-name*	Displays information about RMEPs in a specified MA. *ma-name* specifies the name of the MA. If this parameter is not specified, information about RMEPs in all MAs in a specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?).
mep-id *mep-id*	Displays information about a specified RMEP. *mep-id* specifies the ID of the RMEP.	The value is an integer that ranges from 1 to 8191.
cfm-state	Displays RMEP information based on the CFM status.	-

Parameter	Description	Value
up	Displays information about RMEPs in Up state.	-
down	Displays information about RMEPs in Down state.	-
disable	Displays information about RMEPs in disabled state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an RMEP is configured or CFM cannot work properly, use the **display cfm remote-mep** command to check the RMEP configuration, including:

- Name and level of the MD
- Name of the MA and VLAN associated with the MA
- ID of the RMEP
- MAC address of the RMEP
- Whether the MEP is enabled to receive CCMs from the RMEP
- Alarm status

You can specify **cfm-state** to view RMEP information in the specified CFM state.

Example

Display information about the RMEP with an ID of 50 in the MA named **ma1** within the MD named **md1**.

```
<HUAWEI> display cfm remote-mep md md1 ma ma1 mep-id 50
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 5
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : enabled
 CFM Status         : down
 Alarm Status       : LOC
 Interface TLV      : --
 Connect Status     : up
```

Display information about all RMEPs in the MA named **ma1** within the MD named **md1**.

```
<HUAWEI> display cfm remote-mep md md1 ma ma1
The total number of RMEPs is : 1
The status of RMEPs : 0 up, 1 down, 0 disable
--------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 5
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : enabled
 CFM Status         : down
 Alarm Status       : LOC
 Interface TLV      : --
 Connect Status     : up
```

Display information about all RMEPs configured on the device.

```
<HUAWEI> display cfm remote-mep
The total number of RMEPs is : 1
The status of RMEPs : 0 up, 0 down, 1 disable
--------------------------------------------------
 MD Name            : md
 Level              : 0
 MA Name            : ma
 RMEP ID            : 1
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : disabled
 Trigger-If-Down    : disabled
 CFM Status         : disabled
 Alarm Status       : none
 Interface TLV      : --
 Connect Status     : up
```

Display information about all RMEPs in Down state.

```
<HUAWEI> display cfm remote-mep cfm-state down
The total number of RMEPs is : 2
The status of RMEPs : 0 up, 2 down, 0 disable
--------------------------------------------------
 MD Name            : md
 Level              : 0
 MA Name            : ma
 RMEP ID            : 1111
 VLAN ID            : 1111
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : down
 Alarm Status       : none
 Interface TLV      : --
 Connect Status     : up

 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 2
 VLAN ID            : 100
 VSI Name           : --
```

```
L2VC ID            : --
MAC                : 00e0-fc41-5410
CCM Receive        : enabled
Trigger-If-Down    : disabled
CFM Status         : down
Alarm Status       : LOC
Interface TLV      : --
Connect Status     : up
```

Table 12-58 Description of the display cfm remote-mep command output

Item	Description
The total number of RMEPs is	Number of RMEPs.
MD Name	Name of the MD.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority of the MD.
MA Name	Name of the MA.
RMEP ID	ID of the RMEP.
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with an MA.
L2VC ID	ID of the VC.
MAC	MAC address of the RMEP. **NOTE** An RMEP's MAC address can be a bridge MAC address or the MAC address of the interface where the RMEP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an RMEP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an RMEP uses the MAC address of the interface where the RMEP is configured.
CCM Receive	Whether the MEP is enabled to receive CCMs from the RMEP: ● disabled: The MEP is disabled from receiving CCMs from the RMEP. ● enabled: The MEP is enabled to receive CCMs from the RMEP. To configure the CCM reception function, run the **remote-mep ccm-receive enable** command.

Item	Description
Trigger-If-Down	Whether the block/unblock function is configured on the interface: - disable: indicates that the block/unblock function is disabled on the interface for the RMEP. - enable: indicates that the block/unblock function is enabled on the interface for the RMEP. When a MEP detects a connectivity fault between the MEP and the RMEP in the same MA, the system blocks the interface on which the MEP is configured and then unblocks it. To configure the block/unblock function, run the **cfm trigger if-down** command.
CFM Status	CFM status: - up: indicates that CC works properly. - down: No MEP is configured on the device or the interface where the MEP is configured is unavailable. The reason why the interface is unavailable is one of the following: The subcard is not installed or has been restarted. The Eth-Trunk has no member interface or all member interfaces are Down. - disable: indicates that CFM is not configured, that is, the MEP is not enabled to send CCMs and the RMEP is not enabled to receive CCMs.
Alarm Status	CFM alarm status: - unexpectedPeriod: The interval carried in a CCM sent by the RMEP is different from that configured on the MEP. - unexpectedMAC: The source MAC address carried in a CCM sent by the RMEP is different from the RMEP's MAC address configured on the MEP. - LOC: The session is terminated. - exceptionalMACstatus: TLV information carried in a CCM sent by the RMEP within a specified interval indicates that the interface connecting the RMEP to the MEP is abnormal. - RDI: The MEP receives CCMs with RDI. - none: No alarm is generated. **NOTE** If the device is configured with no MEP but an RMEP, the CFM status is Down. However, no alarm is generated. That is, the field is none.

Item	Description
Interface TLV	Status of an interface type-length-value (TLV). The value can be: - - -: The default value is 0. No TLV status is available on the interface. - up: The interface status is Up, and the interface can transmit packets. - down: The interface status is Down, and the interface cannot transmit packets. - testing: The TLV status of the interface is testing. - unknown: The interface status is unknown. - dormant: The interface is blocked and is waiting for an external event. - notPresent: Information about the interface components is lost. - lowerLayerDown: The lower layer status of the interface is Down. **NOTE** - The packets carrying the interface TLV field with the value Up or Down can be sent. - The received packets carrying the interface TLV field with any value can be parsed.
Connect Status	The connect status of RMEP: - none: Detection is not started on the RMEP. - start: The RMEP is configured, but the remote device does not receive valid CCMs within the timeout period. - up: The physical link is working properly, and the remote device can receive correct CCMs. - down: The local device cannot receive correct CCMs.

12.8.28 display mip create-type

Function

The **display mip create-type** command displays MIP creation rules globally or on a specified interface.

Format

display mip create-type [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays MIP creation rules on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If this parameter is not specified, MIP creation rules on a device are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE 802.1ag Draft 7.

After MIP creation rules are configured using the **mip create-type (system view)** command or CFM does not work properly, use the **display mip create-type** command to check MIP creation rules.

Example

Display MIP creation rules on GigabitEthernet0/0/1.

```
<HUAWEI> display mip create-type interface gigabitethernet 0/0/1
Interface Name              MIP Create-Type  MIP Create-Type On Interface
---------------------------------------------------------------------------
GigabitEthernet0/0/1          default          --
```

Table 12-59 Description of the **display mip create-type** command output

Item	Description
Interface Name	Name of the interface.
MIP Create-Type	MIP creation rule on the device: - default: A MIP can be created on the interface without a higher-level MEP and a lower-level MIP. - explicit: A MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. - none: No MIP is created automatically.

Item	Description
MIP Create-Type On Interface	MIP creation rule on an interface: ● default: A MIP can be created on the interface without a higher-level MEP and a lower-level MIP. ● explicit: A MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. ● none: No MIP is created automatically. ● --: The MIP creation rule on an interface is the same as that on the device.

12.8.29 display oam global configuration

Function

The **display oam global configuration** command displays the global configuration of Ethernet OAM.

Format

display oam global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display oam global configuration** command to check the global configuration of Ethernet OAM, including:

- Whether Ethernet CFM is enabled globally
- Whether GMAC ping is enabled
- Whether GMAC trace is enabled
- Whether EFM OAM is enabled globally

- Ethernet CFM version information
- MP address model

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007.

NOTE

Run the **cfm version** command to switch Ethernet CFM 802.1ag between IEEE 802.1ag Draft 7 and IEEE Std 802.1ag-2007.

Example

Display the global configuration of Ethernet OAM on the device.

```
<HUAWEI> display oam global configuration
Global Configuration                         Value
-------------------------------------------------------
CFM Status                                  enabled
Ping MAC Status                               disabled
Trace MAC Status                              disabled
CFM MAC-tunnel MIP Trace Status                       disabled
EFM Status                                  enabled
CFM Protocol                                standard
CFM MP-address-model                               bridge
```

Table 12-60 Description of the **display oam global configuration** command output

Item	Description
CFM Status	Whether Ethernet CFM is enabled globally: ● disabled: Ethernet CFM is disabled globally. ● enabled: Ethernet CFM is enabled globally. To configure the parameter, run the **cfm enable** command.
Ping MAC Status	Whether GMAC ping is enabled: ● disabled: GMAC ping is disabled. ● enabled: GMAC ping is enabled. To configure the parameter, run the **ping mac enable** command.
Trace MAC Status	Whether GMAC trace is enabled: ● disabled: GMAC trace is disabled. ● enabled: GMAC trace is enabled. To configure the parameter, run the **trace mac enable** command.

Item	Description
CFM MAC-tunnel MIP Trace Status	Whether the intermediate node in the MAC tunnel is enabled to respond to MAC trace messages: - disabled: The intermediate node in the MAC tunnel is disabled from responding to MAC trace messages. - enabled: The intermediate node in the MAC tunnel is enabled to respond to MAC trace messages. **NOTE** The switch does not support this parameter.
EFM Status	Whether EFM OAM is enabled globally: - disabled: EFM OAM is disabled globally. - enabled: EFM OAM is enabled globally. To configure the parameter, run the **efm enable** command.
CFM Protocol	Ethernet CFM version. - standard: IEEE Standard 802.1ag-2007. - bbb0: IEEE 802.1ag Draft 7. To configure the parameter, run the **cfm version** command.
CFM MP-address-model	MP address model: - bridge: shared MP address model - individual: independent MP address model **NOTE** Currently, only the shared MP address model is supported.

12.8.30 ma

Function

The **ma** command creates an MA in an MD and displays the MA view, or directly displays view of an existing MA.

The **undo ma** command deletes an MA.

Format

MD view, MA view:

ma *ma-name* [**format** { **icc-based** *iccbased-ma-format-name* | **string** *ma-format-name* }]

MD view:

undo ma [*ma-name*]

Parameters

Parameter	Description	Value
ma-name	Specifies the name of an MA. The name of an MA in an MD is unique.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 case-sensitive characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
icc-based *iccbased-ma-format-name*	Specifies an ICC-based MA name carried in CCMs to be sent. ITU carrier codes (ICCs) are assigned to network operators or service providers and maintained by ITU-T Telecommunication Standardization Bureau (TSB) in compliance with ITU-T M.1400 Recommendation.	The value is a string of 1 to 13 case-sensitive characters without spaces, hyphens (-), and question marks (?).
string *ma-format-name*	Specifies a string-based MA name carried in CCMs to be sent.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).

Views

MD view, MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, services are deployed based on VLANs on a network. If CFM is required to monitor link connectivity, run the **ma** *ma-name* command to create an MA. Then CFM can be implemented in the MA.

Prerequisites

An MD has been created using the **cfm md** *md-name* command.

Precautions

- When an MA is deleted, the device automatically deletes all MEPs and RMEPs in the MA, stops CC, and clears MA-related alarms.
- An ICC-based MA can only be configured in the MD with the MD name in **no-md-name** format.

Example

Create an MA named **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1]
```

12.8.31 map

Function

The **map** command associates a VLAN with an MA.

The **undo map** command disassociates a VLAN from an MA.

By default, an MA is not associated with any VLAN.

Format

map vlan *vlan-id*

undo map vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ethernet CFM detects connectivity faults in each MA. After an MA is associated with a VLAN, Ethernet CFM can detect connectivity faults in the VLAN.

Precautions

If CFM is used to detect connectivity faults between two directly connected devices, the MA does not need to be associated with a VLAN.

An MA can be associated with only one VLAN.

NOTICE

You can create or delete the association between an MA and a VLAN only when no MEP or RMEP is configured in the MA.

Before changing the VLAN associated with an MA, use the **undo map** command to disassociate the MA from the VLAN.

Example

Associate an MA with VLAN 10. The MA is not associated with any VLAN before the configuration.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
```

12.8.32 mep mep-id

Function

The **mep mep-id** command creates a MEP.

The **undo mep mep-id** command deletes a MEP.

Format

mep mep-id *mep-id* **interface** *interface-type interface-number* [**pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** }

undo mep mep-id *mep-id*

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. The ID identifies a MEP. The MEP ID must be unique in an MA and in a VLAN.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the type and number of the interface where a MEP is configured. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
pe-vid *pe-vid*	Specifies the outer VLAN ID of a PE.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN ID of a CE.	The value is a decimal integer that ranges from 1 to 4094.
inward	Indicates an inward-facing MEP. An inward-facing MEP sends 802.1ag packets through all interfaces in a VLAN associated with an MA, except the interface on which the MEP is configured. That is, the inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA.	-
outward	Indicates an outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To create a MEP, run the **mep mep-id** command.

Precautions

Inward- and outward-facing MEPs are classified based on the scope where 802.1ag packets are sent.

The MEP level of the associated VLAN must be greater than the MEP level of the non-associated VLAN based on the same physical interface or Eth-Trunk member interface. The MEP level is determined by the MD level. You can run the **cfm md** *md-name* command to configure the MD level.

The requirements for the number and type of MEPs created in an MA are as follows:

- The inward- and outward-facing MEPs cannot coexist.
- You can create multiple inward-facing interface-based MEPs but only one outward-facing interface-based MEP. Only one inward-facing interface-based MEP can be created on an interface.

Example

Create an inward-facing MEP on GigabitEthernet0/0/1 in MA **ma1** of MD **md1** and set the MEP ID to 15.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] port gigabitethernet 0/0/1
[HUAWEI-vlan100] quit
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 15 interface gigabitethernet 0/0/1 inward
```

12.8.33 mep alarm disable

Function

The **mep alarm disable** command disables a MEP from reporting alarms.

The **undo mep alarm disable** command enables a MEP to report alarms.

By default, a MEP is enabled to report alarms.

Format

mep mep-id *mep-id* **alarm** { **rdi** | **ais** } **disable**

undo mep mep-id *mep-id* **alarm** { **rdi** | **ais** } **disable**

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **ais**.

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. A MEP ID identifies a MEP. Each MEP must have a unique ID in an MA or a VLAN.	The value is an integer that ranges from 1 to 8191.
alarm rdi	Disables a MEP from reporting remote defect indication (RDI) alarms.	-
alarm ais	Disables a MEP from reporting AIS alarms.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an NMS manages many MEPs on a network, it may receive a large number of RDI and AIS alarms. To reduce such alarms, you can disable the MEPs from reporting alarms. After a MEP is disabled from reporting of RDI or AIS alarms, AIS or RDI alarms of this MEP are no longer sent to the NMS. This reduces the load of the NMS and local device.

Prerequisites

The following operations have been performed:

1. Run the **cfm md** command to create an MD.
2. Run the **ma** command to create an MA.
3. Run the **mep mep-id** command to create a MEP.

Example

Disable MEP 1 in the MA **ma1** of the MD **md1** from reporting RDI alarms.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 alarm rdi disable
```

12.8.34 mep ccm-send enable

Function

The **mep ccm-send enable** command enables a MEP in an MA to send CCMs.

The **undo mep ccm-send enable** command disables a MEP in an MA from sending CCMs.

By default, a MEP is disabled from sending CCMs.

Format

mep ccm-send [**mep-id** *mep-id*] **enable**

undo mep ccm-send [**mep-id** *mep-id*] **enable**

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. If this parameter is not specified, all the MEPs in the MA are enabled to send CCMs or disabled from sending CCMs.	The value of *mep-id* is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you use the **mep mep-id** command to configure a MEP, use this command to enable the MEP to send CCMs.

Precautions

The interval at which CCMs are sent or received cannot be modified on the device in an MA if one of the following operations is performed:

- The **mep ccm-send enable** command is run to enable a MEP in an MA to send CCMs.
- The **remote mep ccm-receive enable** command is run to enable a MEP in an MA to receive CCMs.

The **undo mep ccm-send enable** or **remote mep ccm-receive enable** command must be run before the interval is reconfigured.

Example

Enable MEP 10 in the MA named **ma1** to send CCMs.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep ccm-send mep-id 10 enable
```

12.8.35 mip create-type (MD view)

Function

The **mip create-type** command configures a MIP creation rule in an MD or the default MD.

The **undo mip create-type** command restores the default MIP creation rule in an MD or the default MD.

By default, the MIP creation rule in an MD or the default MD is **none**. That is, MIPs are not created.

Format

mip create-type { **default** | **explicit** | **none** }

undo mip create-type

Parameters

Parameter	Description	Value
default	Indicates that a MIP can be created on the interface without a higher-level MEP and a lower-level MIP. In this mode, MIPs can be created when no MEP is configured on the interface.	-
explicit	Indicates that a MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. In this mode, a MIP can be created on an interface only when a lower-level MEP has been configured on this interface.	-
none	Indicates that the MIP creation rule on an interface is none, that is, a MIP is not created automatically.	-

Views

MD view, default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When all devices in an MD are enabled to send CCMs, MEPs send CCMs periodically. If a MEP receives no CCMs from an RMEP within three consecutive intervals for sending CCMs, a connectivity fault between the MEP and RMEP occurs. A MIP needs to be used to locate the fault.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

After the MIP creation rule is set in an MD or the default MD, all interfaces in the MD or default MD use this rule to create a MIP.

If the MIP creation rule is **default** or **explicit**, the device creates a MIP automatically according to the rule.

NOTE

The **mip create-type** command can be used only on the Layer 2 interfaces to which the MD or default MD belongs.

Example

Set the MIP creation rule to **none** in the MD named **customer**.

```
<HUAWEI> system-view
[HUAWEI] cfm md customer level 1
[HUAWEI-md-customer] mip create-type none
```

Set the MIP creation rule to **default** in the default MD.

```
<HUAWEI> system-view
[HUAWEI] cfm default md
[HUAWEI-default-md] mip create-type default
```

12.8.36 mip create-type (system view)

Function

The **mip create-type** command configures a MIP creation rule on the device or a specified interface.

The **undo mip create-type** command restores the default MIP creation rule on a specified interface.

By default, the MIP creation rule on the device is **none** and all the interfaces use this rule to generate MIPs.

Format

mip create-type { **default** | **explicit** | **none** } [**interface** *interface-type interface-number*]

undo mip create-type [[**default** | **explicit** | **none**] **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
default	Indicates that the MIP creation rule on an interface is **default**. That is, a MIP can be created on the interface without a higher-level MEP and a lower-level MIP. In this mode, MIPs can be created when no MEP is configured on the interface.	-
explicit	Indicates that the MIP creation rule on an interface is **explicit**. That is, a MIP can be created on an interface with a lower-level MEP but without a higher-level MEP or a lower-level MIP. In this mode, a MIP can be created on an interface only when a lower-level MEP has been configured on this interface.	-
none	Indicates that the MIP creation rule on an interface is **none**. That is, a MIP is not created automatically.	-
interface-type interface-number	Specifies the type and number of an interface where a MIP creation rule is configured. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the MIP creation rule takes effect globally.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a MIP creation rule on the device, run the **mip create-type** command.

Precautions

NOTE

The command is only applicable to IEEE 802.1ag Draft 7.

If the MIP creation rule is **default** or **explicit**, the device creates a MIP automatically according to the rule.

Generally, you need to configure MIP nodes only when the 802.1ag MAC ping or trace operation is performed on a non-MEP node in an MA.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Set the MIP creation rule to **default** on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] mip create-type default interface gigabitethernet 0/0/1
```

12.8.37 oam-bind cfm md ma efm interface

Function

The **oam-bind cfm md ma efm interface** command configures EFM and Ethernet CFM to report faults to each other.

The **undo oam-bind cfm md ma efm interface** command cancels the configuration.

By default, EFM OAM and Ethernet CFM are not configured to report faults to each other.

Format

oam-bind cfm md *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*

undo oam-bind cfm md *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*

NOTE

This command is not supported by only the SS1720GW-E, and S1720GWR-E.

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Specifies the type and number of an Ethernet interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and CFM is deployed at another side of a device, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- When EFM detects a link fault, it will notify CFM of the fault.
- When CFM detects a link fault, it will notify EFM of the fault.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands in different scenarios according to **Table 12-61**.

Table 12-61 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands at a random order (each command configures fault transmission in a single direction): - The **oam-bind ingress efm interface egress cfm md ma** command is used to configure EFM to report faults to CFM. - The **oam-bind ingress cfm md ma egress efm interface** command is used to configure CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: - Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. - Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Precautions

The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.

Example

Configure EFM and CFM to report faults to each other through the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind cfm md mdcustomer ma customer efm interface gigabitethernet 0/0/1
```

12.8.38 oam-bind cfm md ma trigger if-down interface

Function

The **oam-bind cfm md ma trigger if-down interface** command enables Ethernet CFM and an interface to report faults to each other.

The **undo oam-bind cfm md ma trigger if-down interface** command cancels the configuration.

By default, Ethernet CFM and an interface are not configured to report faults to each other.

Format

oam-bind cfm md *md-name* **ma** *ma-name* **trigger if-down interface** *interface-type interface-number*

undo oam-bind cfm md *md-name* **ma** *ma-name* **trigger if-down interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
if-down	Indicates that an interface goes Down when Ethernet CFM on the interface detects a fault.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to CFM. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with an interface, run the **oam-bind cfm md ma trigger if-down interface** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-62**.

Table 12-62 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): ● If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. ● If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse directions of fault transmission.	Run the following commands at a random order (each command configures fault transmission in a single direction): ● **oam-bind ingress cfm md ma egress interface** ● **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: ● To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. ● To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure Ethernet CFM to report faults to the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind cfm md md1 ma ma1 trigger if-down interface gigabitethernet 0/0/1
```

12.8.39 oam-bind ingress cfm md ma egress interface

Function

The **oam-bind ingress cfm md ma egress interface** command configures Ethernet CFM to report faults to an interface.

The **undo oam-bind ingress cfm md ma egress interface** command cancels the configuration.

By default, Ethernet CFM is not configured to report faults to an interface.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **trigger if-down egress interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **trigger if-down egress interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
if-down	Indicates that an interface goes Down when Ethernet CFM on the interface detects a fault.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to CFM. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with an interface, run the **oam-bind ingress cfm md ma egress interface** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- Fault messages are transmitted from the ingress to the egress.
- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-63**.

Table 12-63 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): ● If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. ● If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse directions of fault transmission.	Run the following commands at a random order (each command configures fault transmission in a single direction): ● **oam-bind ingress cfm md ma egress interface** ● **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: ● To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. ● To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure CFM to report faults to the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface
gigabitethernet 0/0/1
```

12.8.40 oam-bind ingress cfm md ma egress sep segment

Function

The **oam-bind ingress cfm md ma egress sep segment** command configures CFM to report faults to a SEP segment.

The **undo oam-bind ingress cfm md ma egress sep segment** command cancels the configuration.

By default, CFM is not configured to report faults to a SEP segment.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress sep segment** *segment-id* **interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress sep segment** *segment-id* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ingress egress	Configures CFM to report faults to a SEP segment.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
segment *segment-id*	Specifies the ID of a SEP segment.	The value is an integer that ranges from 1 to 1024.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an Ethernet interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. The Ethernet interface must have been added to the SEP segment.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with SEP, run the **oam-bind ingress cfm md ma egress sep segment** command.

Precautions

When a device running SEP at the access layer connects to the aggregation layer, pay attention to the following points:

- When a fault occurs at the access layer, configure topology change notification so that the aggregation layer can detect the fault at the access layer. Devices in the SEP segment can update their MAC address tables and ARP tables in a timely manner.
- If a fault occurs at the aggregation layer, associate SEP with Ethernet CFM on the device between the access layer and aggregation layer so that the access layer can detect the fault at the aggregation layer. Devices at the access layer can update their MAC address tables and ARP tables.

Prerequisites

This command can take effect only when the following configurations are completed:

- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create a MEP.

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.
- The interface specified in this command has been added to the SEP segment.

Example

Configure CFM to report faults to SEP segment 10.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress cfm md md1 ma ma1 egress sep segment 10 interface
gigabitethernet 0/0/1
```

12.8.41 oam-bind ingress cfm md ma egress efm interface

Function

The **oam-bind ingress cfm md ma egress efm interface** command configures Ethernet CFM to report faults to EFM OAM.

The **undo oam-bind ingress cfm md ma egress efm interface** command cancels the configuration.

By default, Ethernet CFM is not configured to report faults to EFM OAM.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*

NOTE

This command is not supported by only the SS1720GW-E, and S1720GWR-E.

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).

Parameter	Description	Value
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters.
interface-type interface-number	Specifies the type and number of an Ethernet interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and CFM is deployed at another side of a device, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- When EFM detects a link fault, it will notify CFM of the fault.
- When CFM detects a link fault, it will notify EFM of the fault.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands in different scenarios according to **Table 12-64**.

Table 12-64 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands at a random order (each command configures fault transmission in a single direction): - The **oam-bind ingress efm interface egress cfm md ma** command is used to configure EFM to report faults to CFM. - The **oam-bind ingress cfm md ma egress efm interface** command is used to configure CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: - Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. - Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Example

Configure Ethernet CFM to report faults to EFM through the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress cfm md mdcustomer ma customer egress efm interface
gigabitethernet 0/0/1
```

12.8.42 oam-bind ingress efm interface egress cfm md ma

Function

The **oam-bind ingress efm interface egress cfm md ma** command configures EFM OAM to report faults to Ethernet CFM.

The **undo oam-bind ingress efm interface egress cfm md ma** command cancels the configuration.

By default, EFM OAM is not configured to report faults to Ethernet CFM.

Format

oam-bind ingress efm interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

undo oam-bind ingress efm interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

NOTE

This command is not supported by only the SS1720GW-E, and S1720GWR-E.

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an Ethernet interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and CFM is deployed at another side of a device, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- When EFM detects a link fault, it will notify CFM of the fault.
- When CFM detects a link fault, it will notify EFM of the fault.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands in different scenarios according to **Table 12-65**.

Table 12-65 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands at a random order (each command configures fault transmission in a single direction): - The **oam-bind ingress efm interface egress cfm md ma** command is used to configure EFM to report faults to CFM. - The **oam-bind ingress cfm md ma egress efm interface** command is used to configure CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: - Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. - Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Example

Configure EFM to report faults to CFM through the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress efm interface gigabitethernet 0/0/1 egress cfm md mdcustomer
ma customer
```

12.8.43 oam-bind ingress interface egress cfm md ma trigger if-down

Function

The **oam-bind ingress interface egress cfm md ma trigger if-down** command configures an interface to report faults to Ethernet CFM.

The **undo oam-bind ingress interface egress cfm md ma trigger if-down** command cancels the configuration.

By default, an interface is not configured to report faults to Ethernet CFM.

Format

oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down**

undo oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
if-down	Indicates that the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end of the fault when an interface goes Down.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate an interface with CFM, run the **oam-bind ingress interface egress cfm md ma trigger if-down** command.

Precautions

If CFM is associated with an interface on a device and a device interface goes Down, the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end of the fault.

Prerequisites

Unidirectional fault transmission from an interface to Ethernet CFM can be configured only when the following requirements are met:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be the one that CFM monitors. If CFM is associated with a physical interface that it monitors, the link is locked.

Configure unidirectional or bidirectional fault transmission between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-66**.

Table 12-66 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): - If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. - If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order (each command configures fault transmission in a single direction): - **oam-bind ingress cfm md ma egress interface** - **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: - To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. - To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure Ethernet CFM to report faults to the GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind ingress interface gigabitethernet 0/0/1 egress cfm md md1 ma ma1
trigger if-down
```

12.8.44 oam-bind interface cfm md ma trigger if-down

Function

The **oam-bind interface cfm md ma trigger if-down** command configures an interface and Ethernet CFM to report faults to each other.

The **undo oam-bind interface cfm md ma trigger if-down** command cancels the configuration.

By default, an interface and Ethernet CFM are not configured to report faults to each other.

Format

oam-bind interface *interface-type interface-number* **cfm md** *md-name* **ma** *ma-name* **trigger if-down**

undo oam-bind interface *interface-type interface-number* **cfm md** *md-name* **ma** *ma-name* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
if-down	Indicates that the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end of the fault when an interface goes Down.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate an interface with CFM, run the **oam-bind interface cfm md ma trigger if-down** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional fault transmission between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind cfm md ma trigger if-down interface**
- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands in different scenarios according to **Table 12-67**.

Table 12-67 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Select either of the following commands (the two commands have the same function): • If you prefer to specify the MD and MA before the interface, use the **oam-bind cfm md ma trigger if-down interface** command. • If you prefer to specify the interface before the MD and MA, use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind cfm md ma trigger if-down interface** or **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse directions of fault transmission.	Run the following commands at a random order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: ● To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. ● To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Enable the GigabitEthernet0/0/1 to report faults to Ethernet CFM.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr] oam-bind interface gigabitethernet 0/0/1 cfm md md1 ma ma1 trigger if-down
```

12.8.45 oam-mgr

Function

The **oam-mgr** command displays the OAM management view.

The **undo oam-mgr** command exits from the OAM management view.

Format

oam-mgr

undo oam-mgr

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

CFM can advertise fault information to interfaces or protocol modules. Ethernet OAM fault advertisement is implemented by an OAM manager, application modules, and detection modules. An OAMMGR module associates one module with another. A detection module monitors link status and network performance. If a detection module detects a fault, it instructs the OAMMGR module to notify an application module or another detection module of the fault. After receiving the notification, the application or detection module takes measures to prevent a communication interruption or service quality deterioration. Run the **oam-mgr** command to display the MGR view before associating the CFM module and other modules.

Example

Enter the OAM management view.

```
<HUAWEI> system-view
[HUAWEI] oam-mgr
[HUAWEI-oam-mgr]
```

12.8.46 packet-priority

Function

The **packet-priority** command sets the 802.1p priority of 802.1ag packets in an MA.

The **undo packet-priority** command restores the default 802.1p priority of 802.1ag packets in an MA.

Format

packet-priority *priority*

undo packet-priority

Parameters

Parameter	Description	Value
priority	Specifies the 802.1p priority of 802.1ag packets.	The value is an integer that ranges from 0 to 7. The default value is 7. A larger value indicates a higher priority.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.1ag packets are the Continuity Check Message (CCM), Loopback Message (LBM), Loopback Reply (LBR), Linktrace Message (LTM), and Linktrace Reply (LTR).

The 802.1ag packets with different 802.1p priorities are transmitted differently on networks. You can use this command to change the transmission quality of 802.1ag packets on networks.

Example

Set the 802.1p priority of 802.1ag packets in an MA to 3.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] packet-priority 3
```

12.8.47 ping mac-8021ag

Function

The **ping mac-8021ag** command enables 802.1ag MAC ping to detect connectivity faults between a MEP and an RMEP or a MIP in an MA.

Format

All views except the MA view:

ping mac-8021ag mep mep-id *mep-id* **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

MA view

ping mac-8021ag mep mep-id *mep-id* { **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } | **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

Parameters

Parameter	Description	Value
mep mep-id *mep-id*	Specifies the ID of a MEP. The MEP must have been created using the **mep mep-id** command.	The value is an integer that ranges from 1 to 8191.

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters.
mac *mac-address*	Specifies the MAC address of the destination node. The destination node can be a MEP or MIP. *mac-address* specifies the MP's MAC address. **NOTE** An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address.
remote-mep mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
-c *count*	Specifies the number of ping attempts.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface on the local device for sending ping packets. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
-s *packetsize*	Specifies the size of a ping packet.	The value is an integer that ranges from 95 to 9000, in bytes. The default value is 95.
-t *timeout*	Specifies the timeout interval for waiting for a response packet.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
-p *priority-value*	Specifies the priority of ping packets.	The value is an integer that ranges from 0 to 7. The default value is the same as the 802.1p priority of 802.1ag packets specified in the MA view.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Similar to ping, 802.1ag MAC ping enables the local device to send test packets and wait for a response to check whether the destination device is reachable. In addition, the ping operation time can be calculated at the transmit end for network performance analysis.

A device is usually configured with multiple MDs and MAs. To accurately detect connectivity of a link between two or more devices, perform either of the following operations:

- Run the **ping mac-8021ag** command in the MA view.
  - Run the **ping mac-8021ag** command without **md** *md-name* **ma** *ma-name* specified to check connectivity of links in a specified MA.
  - Run the **ping mac-8021ag** command with **md** *md-name* and **ma** *ma-name* specified to check connectivity of links based on the configured MA and MD.
- Run the **ping mac-8021ag** command in all views except the MA view to check connectivity of links based on the configured MA and MD.

Prerequisites

- The MA has been associated with a VLAN.
- The MEP has been configured in the MA.

Precautions

802.1ag MAC ping is initiated by the local MEP in the MA and destined for a MEP or a MIP of the same level on other devices. The source node and the destination node can be located in different MAs.

If the outbound interface is specified, it cannot be configured with an inward-facing MEP.

Example

Ping the MIP with a bridge MAC address of 00e0-fc00-0204 twice on the MEP in **ma1** and set the size of ping packets to 112 bytes.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ping mac-8021ag mep mep-id 1 mac 00e0-fc00-0204 -c 2 -s 112
Pinging 00e0-fc00-0204 with 112 bytes of data:
Reply from 00e0-fc00-0204: bytes = 112 time = 9ms
Reply from 00e0-fc00-0204: bytes = 112 time = 11ms
Packets: Sent = 2, Received = 2, Lost = 0  <0% Lost >
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 12-68 Description of the **ping mac-8021ag** command output

Item	Description
Reply from 00e0-fc00-0204: bytes = 112 time = 9ms	Size and response time of ping packets sent by the destination device. When the response time is less than 1 ms, "time < 1ms" is displayed.
Packets: Sent = 2, Received = 2, Lost = 0 <0% Lost >	Number of sent ping packets, number of received reply packets, and number and percentage of discarded packets.
Minimum	Minimum round-trip time (RTT).
Maximum	Maximum RTT.
Average	Average RTT.

12.8.48 remote-mep

Function

The **remote-mep** command configures an RMEP in an MA.

The **undo remote-mep** command deletes an RMEP from an MA.

Format

remote-mep mep-id *mep-id* [**mac** *mac-address*]

undo remote-mep mep-id *mep-id*

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an RMEP, use this command.

Precautions

To detect CFM connectivity faults between a device and an RMEP in an MA, complete the following tasks:

- Run the **remote-mep** command to configure an RMEP in an MA.
- Run the **remote-mep ccm-receive enable** command to enable the MEP to receive CCMs from the RMEP.

To modify the bridge MAC address of the RMEP, you must delete the RMEP from an MA and then reconfigure the RMEP.

The RMEP ID must be different from the MEP ID configured on a local interface.

NOTICE

- If multiple MEPs exist in an MA, the configured RMEP corresponds to multiple MEPs.
- If one MEP exists in an MA, one or more configured RMEPs correspond to one MEP.

Example

Configure RMEP 10 in **ma1** on the device with the bridge MAC address of 00e0-fc00-0204.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 10 mac 00e0-fc00-0204
```

12.8.49 remote-mep ccm-receive enable

Function

The **remote-mep ccm-receive enable** command enables a MEP on the device to receive CCMs from an RMEP in the same MA or MAC tunnel.

The **undo remote-mep ccm-receive enable** command cancels the configuration.

By default, a MEP does not receive CCMs from an RMEP.

Format

remote-mep ccm-receive [**mep-id** *mep-id*] **enable**

undo remote-mep ccm-receive [**mep-id** *mep-id*] **enable**

Parameters

Parameter	Description	Value
mep-id *mep-id*	Enables a MEP to receive CCMs from the specified RMEP. If this parameter is not specified, a MEP can receive CCMs from all RMEPs in the same MA.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remote-mep ccm-receive enable** command enables a MEP on the device to receive CCMs from an RMEP in the same MA or MAC tunnel.

Precautions

The interval at which CCMs are sent or detected cannot be changed on the device in an MA if one of the following operations is performed:

- The device is enabled to send CCMs using the **mep ccm-send enable** command.
- The device is enabled to receive CCMs using the **remote-mep ccm-receive enable** command.

The **undo mep ccm-send enable** or **undo remote mep ccm-receive enable** command must be run before the interval is reconfigured.

Prerequisites

A MEP and an RMEP have been created in the MA.

Example

Enable the device to receive CCMs from RMEP 10 in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 10 mac 00e0-fc00-0204
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive mep-id 10 enable
```

12.8.50 senderid-tlv-type

Function

The **senderid-tlv-type** command sets the type of the Sender ID TLV in CFM packets.

The **undo senderid-tlv-type** command restores the default type of the Sender ID TLV in CFM packets.

By default, the type of the Sender ID TLV is **defer**.

Format

senderid-tlv-type { **none** | **chassis** | **manage** | **chassis-manage** | **defer** }

undo senderid-tlv-type

Parameters

Parameter	Description	Value
none	Indicates that a sent CFM packet does not contain the Sender ID TLV.	-
chassis	Indicates that a sent CFM packet contains the chassis ID.	-
manage	Indicates that a sent CFM packet contains the management address.	-
chassis-manage	Indicates that a sent CFM packet contains the chassis ID and management address.	-
defer	Indicates that the content of the Sender ID TLV is determined by the MD object.	-

Views

MD view, default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **senderid-tlv-type** command to configure the type of the Sender ID TLV in CFM packets in the MD view or default MD view.

Example

Set the type of the Sender ID TLV to **manage**.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm default md
[HUAWEI-default-md] senderid-tlv-type manage
```

12.8.51 trace mac-8021ag

Function

The **trace mac-8021ag** command enables 802.1ag MAC trace to detect connectivity faults between a MEP and an RMEP or a MIP in an MA.

Format

All views except the MA view:

trace mac-8021ag mep mep-id *mep-id* **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *

MA view:

trace mac-8021ag mep mep-id *mep-id* { **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } | **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *

Parameters

Parameter	Description	Value
mep mep-id *mep-id*	Specifies the ID of a MEP. The MEP must have been created using the **mep mep-id** command.	The value is an integer that ranges from 1 to 8191.
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
mac *mac-address*	Specifies the MAC address of the destination node. The destination node can be a MEP or MIP. *mac-address* specifies the MP's MAC address. The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address. **NOTE** An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: - If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. - If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	-
remote-mep mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface on the local device for sending LTMs. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. This parameter must be specified if the forwarding entry of the destination node does not exist in the MAC address table or there is more than one interface in a VLAN.	-
-t *timeout*	Specifies the timeout interval for waiting for an LTR.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
ttl *ttl*	Specifies the maximum hop of LTMs.	The value is an integer that ranges from 1 to 255. The default value is 64.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Similar to traceroute (tracert for short), 802.1ag MAC trace tests the path between the local device and the destination device or locates failure points by sending test packets and receiving reply packets.

A device is usually configured with multiple MDs and MAs. To locate failure points or detect connectivity of a link between one MEP to another MEP or a MIP in the same MA, perform either of the following operations:

- Run the **trace mac-8021ag** command in the MA view.

  - Run the **trace mac-8021ag** command without **md** *md-name* and **ma** *ma-name* specified to test the actual forwarding patch and locate failure points in a specified MA.
  - Run the **md** *md-name* **ma** *ma-name* command with **md** *md-name* and **ma** *ma-name* specified to test the actual forwarding patch and locate failure points based on the configured MA and MD.
- Run the **trace mac-8021ag md** *md-name* **ma** *ma-name* command in all views except the MA view to test the actual forwarding patch and locate failure points based on the configured MA and MD.

Prerequisites

- The MA has been associated with a VLAN.
- The MEP has been configured in the MA.

Precautions

A MEP initiates an 802.1ag MAC trace test to monitor reachability of the MEP's or MIP's destination address. These nodes have the same level and can be located in the same MA or different MAs.

If the outbound interface is specified, it cannot be configured with an inward-facing MEP.

Example

Trace the MEP with the MAC address of aa99-6600-5600 from the MEP in the MA **macustomer**, with the TTL of 64.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md mdcustomer
[HUAWEI-md-mdcustomer] ma macustomer
[HUAWEI-md-mdcustomer-ma-macustomer] trace mac-8021ag mep mep-id 1 mac aa99-6600-5600 ttl
64
Tracing the route to aa99-6600-5600 over a maximum of 64 hops:
--------------------------------------------------------------------------------
 Hops  Ingress Mac        Ingress Port              Ingress Action      Relay Action
       Egress Mac         Egress Port               Egress Action       Ismep
---------------------------------------------------------------------------------
1      00e0-fc01-3302     Vlanif0/0/1     IngOK              RlyFDB
       00e0-fce2-36db     Vlanif0/0/1     EgrOK              NoMep
```

Table 12-69 Description of the **trace mac-8021ag** command output

Item	Description
Hops	Number of hops.
Ingress Mac	MAC address of the inbound interface for receiving LTMs on the intermediate node or destination node.
Ingress Port	Inbound interface for receiving LTMs on the intermediate node or destination node.

Item	Description
Ingress Action	Action taken by the inbound interface to process LTMs: ● IngOK: The inbound interface forwards LTMs successfully. ● If this field is empty, the inbound interface fails to forward LTMs.
Reply Action	Action taken by the device to process LTMs: ● RlyFDB: The device forwards LTMs to the next hop device. ● RlyHit: The device forwards LTMs to the destination device.
Egress Mac	MAC address of the outbound interface for forwarding LTMs on the intermediate node.
Egress Port	Outbound interface for forwarding LTMs on the intermediate node.
Egress Action	Action taken by the outbound interface to process LTMs: ● EgrOK: The outbound interface forwards LTMs successfully. ● If this field is empty, the outbound interface does not or fails to forward LTMs.
Ismep	Whether the mode of the outbound interface is a MEP: ● NoMep: no ● IsMep: yes

12.8.52 vlan (default MD view)

Function

The **vlan** command creates a VLAN in the default MD.

The **undo vlan** command deletes a VLAN from the default MD.

Format

vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

undo vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

Parameters

Parameter	Description	Value
vlan-id1	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094.
vlan-id2	Specifies the end VLAN ID.	The value is an integer that ranges from 1 to 4094. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.

Views

Default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **vlan** command in the default MD view, all the interfaces in the specified VLAN can generate MIPs based on the configured MIP creation rule in the default MD.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

If the **vlan** command is run multiple times, all configurations take effect.

NOTE

The specified VLAN cannot be associated with any MA.

Example

Associate VLAN 100 to VLAN 200 with the default MD.

```
<HUAWEI> system-view
[HUAWEI] cfm default md
[HUAWEI-default-md] vlan 100 to 200
```

12.9 Y.1731 Configuration Commands

12.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

12.9.2 ais enable

Function

The **ais enable** command enables alarm indication signal (AIS) in an MA.

The **undo ais enable** command disables AIS in an MA.

By default, AIS is disabled.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais enable

undo ais enable

Parameters

None

Views

MD view, MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. Enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS.

Precautions

The **ais enable** command can be used on only the device running IEEE Standard 802.1ag-2007.

When the device processes many AIS packets, the CPU usage will become high. When the device is enabled with AIS, it is recommended that nestling layers in an

MD should be reduced and the number of interfaces associated with VLANs in an MA should be reduced.

Prerequisites

An MD has been created using the **cfm md** command and an MA has been created using the **ma** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and enable the AIS function in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais enable
```

12.9.3 ais interval

Function

The **ais interval** command sets the interval at which a MEP in an MA sends AIS PDUs to a MEP in a high-level MA.

The **undo ais interval** command restores the default interval.

By default, the interval at which AIS PDUs are sent is 1s.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais interval *interval-value*

undo ais interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which AIS PDUs are sent.	The value is an integer that ranges from 1 to 60, in seconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. You can enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS. After AIS is enabled, set the interval at which AIS PDUs are sent according to the networking.

Precautions

The **ais interval** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the interval at which AIS PDUs are sent in **ma1** to 60s.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais interval 60
```

12.9.4 ais level

Function

The **ais level** command sets the level of AIS PDUs to be sent by a MEP in an MA.

The **undo ais level** command deletes the level of AIS PDUs to be sent by a MEP in an MA.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais level *level-value*

undo ais level

Parameters

Parameter	Description	Value
level-value	Specifies the level of AIS PDUs to be sent.	The value is an integer that ranges from 0 to 7.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. You can enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS. After AIS is enabled, set the level of AIS PDUs to be sent according to the networking.

Precautions

The **ais level** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the level of AIS PDUs to be sent to 2 in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais level 2
```

12.9.5 ais link-status

Function

The **ais link-status** command configures AIS to monitor interfaces.

The **undo ais link-status** command cancels the configuration.

By default, AIS does not monitor any interface.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais link-status interface *interface-type interface-number*

undo ais link-status interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface to be monitored by AIS. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, if a MEP in a low-level MD detects a fault, the MEP sends a trap to the NMS. After a certain period, a MEP in the MD of a higher level also detects the fault and sends the same trap to the NMS. You can enable the AIS function in low-level and high-level MDs to suppress the MEP of the high-level MD from sending traps to the NMS. To speed up AIS PDU transmission, run the **ais link-status** command to configure AIS to monitor interfaces. In this manner, a MEP sends an AIS PDU immediately after the monitored interface goes Down. The MEP does not need to wait for the timeout of CCMs. In addition, the MEP in a high-level MD is suppressed from sending the same trap to the NMS.

NOTE

Both inward- and outward-facing MEPs can receive AIS PDUs in MD scenarios.

Precautions

The **ais link-status** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and configure AIS to monitor an interface in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais link-status interface gigabitethernet 0/0/1
```

12.9.6 ais suppress-alarm

Function

The **ais suppress-alarm** command enables alarm suppression on the device.

The **undo ais suppress-alarm** command disables alarm suppression on the device.

By default, alarm suppression is disabled on the device.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais suppress-alarm

undo ais suppress-alarm

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MD nesting scenarios, after a MEP in a high-level MD receives an AIS PDU, the MEP does not send an alarm to the NMS. If the MEP does not receive any AIS PDU within the period 3.5 times as long as the interval at which AIS PDUs are sent, the alarm suppression function is disabled automatically on the local device.

- If a MEP detects a link fault and sends an alarm to the NMS before receiving an AIS PDU, run the **ais suppress-alarm** command to enable the alarm suppression function. The MEP sends only an alarm indicating that the link fault is rectified if the MEP detects that the link fault is rectified.
- If a MEP does not detect a link fault before receiving an AIS PDU, after the **ais suppress-alarm** command is used to enable the alarm suppression function, the MEP does not send an alarm to the NMS if the MEP detects a link fault.

Precautions

The **ais suppress-alarm** command can be used on only the device running IEEE Standard 802.1ag-2007.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and enable alarm suppression in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais suppress-alarm
```

12.9.7 ais vlan

Function

The **ais vlan** command sets the range of VLANs to which the MEP of an MA sends AIS PDUs.

The **undo ais vlan** command cancels the configuration.

NOTE

Only the S6730-S, S6730S-S, S6730-H, S6730S-H, S6720S-S, S6720-EI, S6720S-EI, S6735-S, S5731-S, S5731S-H, S5731S-S, S5732-H, S5731-H, S5735S-H, S5736-S, S5735-S-I, S5735S-S, S500, S5720I-SI and S5735-S support this command.

Format

ais vlan vid { *low-vid* [**to** *high-vid*] } &<1-10> **mep** *mep-id*

ais vlan pe-vid *pe-vid* **ce-vid** { *low-ce-vid* [**to** *high-ce-vid*] } &<1-10> **mep** *mep-id*

undo ais vlan vid { *low-vid* [**to** *high-vid*] } &<1-10> **mep** *mep-id*

undo ais vlan pe-vid *pe-vid* **ce-vid** { *low-ce-vid* [**to** *high-ce-vid*] } &<1-10> **mep** *mep-id*

undo ais vlan [**vid** | **pe-vid** *pe-vid*] **mep** *mep-id*

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the VLAN ID in the outer tag of a VLAN frame.	The value is an integer that ranges from 1 to 4094.
ce-vid *low-ce-vid*	Specifies the lower limit of the VLAN ID in the inner tag of a VLAN frame.	The value is an integer that ranges from 1 to 4094.
high-ce-vid	Specifies the upper limit of the VLAN ID in the inner tag of a VLAN frame.	The value is an integer that ranges from 1 to 4094.
vid *low-vid*	Specifies the lower limit of the VLAN ID in an AIS PDU.	The value is an integer that ranges from 1 to 4094.
high-vid	Specifies the upper limit of the VLAN ID in an AIS PDU.	The value is an integer that ranges from 1 to 4094.
mep *mep-id*	Specifies the ID of a MEP. The ID identifies a MEP. The MEP ID must be unique in an MA and in a VLAN.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **ais vlan** command to set the range of VLANs to which the AIS PDUs to be sent. This prevents the MEP from sending AIS PDUs to all VLANs and reduces the load of the system.

Precautions

The **ais vlan** command can be used on only the device running IEEE Standard 802.1ag-2007.

If the **ais vlan** command is run more than once, all configurations take effect.

Prerequisites

An MD has been created using the **cfm md** command, an MA has been created using the **ma** command, and AIS has been enabled using the **ais enable** command.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the outer VLAN ID in outgoing AIS PDUs to 10 and set the inner VLAN ID range to 1 to 100.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais vlan pe-vid 10 ce-vid 1 to 100 mep 1
```

Create an MD named **md1**, create an MA named **ma1** in the MD, and set the range of VLANs to which AIS PDUs are to be sent to 1 to 100 in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] ais vlan vid 1 to 100 mep 1
```

12.9.8 delay-measure one-way continual

Function

The **delay-measure one-way continual** command configures proactive one-way frame delay measurement.

The **undo delay-measure one-way continual** command cancels the configuration.

By default, proactive one-way frame delay measurement is not configured in an MA.

Format

delay-measure one-way continual send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }

undo delay-measure one-way continual send [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.
interval { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }	Specifies the interval at which DM frames are sent.	The value is 1000, 10000, 30000, 60000, 150000, and 300000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Proactive OAM indicates that OAM actions are carried out continuously.

One-way frame delay measurement is implemented between two MEPs by exchanging DM frames. A MEP periodically sends DM frames carrying TxTimeStampf. After receiving a DM frame, the RMEP parses TxTimeStampf and compares this value with RxTimef (the time when the 1DM frame was received). The RMEP calculates the one-way frame delay based on these values using the following formula: Frame delay = RxTimef - TxTimeStampf

When clocks of the MEPs at both ends of a link are synchronized, the **delay-measure one-way continual** command can be used to implement proactive one-way frame delay measurement for a VLAN.

To implement proactive one-way frame delay measurement, specify the RMEP ID or destination MAC address, and interval at which DM frames are sent:

- If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for frame delay measurement.
- If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

- IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.
- One-way frame delay measurement can be implemented only after the MEP synchronizes the time with its RMEP.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

In a VLAN, enable proactive one-way frame delay measurement and set the destination MAC address to 01-22-33 and the interval at which DM frames are sent to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way continual send mep 1 mac 01-22-33 interval 1000
```

In a VLAN, enable proactive one-way frame delay measurement and set the RMEP ID to 2 and the interval at which DM frames are sent to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way continual send mep 1 remote-mep 2 interval
1000
```

12.9.9 delay-measure one-way continual receive

Function

The **delay-measure one-way continual receive** command configures the RMEP to receive DM frames to implement proactive one-way frame delay measurement.

The **undo delay-measure one-way continual receive** command cancels the configuration.

By default, the RMEP enabled with proactive one-way frame delay measurement in an MA is not configured to receive DM frames.

Format

delay-measure one-way continual receive mep *mep-id*

undo delay-measure one-way continual receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used in the VLAN scenario to enable the RMEP to receive DM frames to implement proactive one-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

Precautions

After the configuration is complete, the remote device can receive DMMs to implement proactive one-way frame delay measurement.

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Configure the RMEP to receive DM frames in a VLAN.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md2
[HUAWEI-md-md2] ma ma2
[HUAWEI-md-md2-ma-ma2] map vlan 2
[HUAWEI-md-md2-ma-ma2] mep mep-id 2 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md2-ma-ma2] delay-measure one-way continual receive mep 2
```

12.9.10 delay-measure one-way send

Function

The **delay-measure one-way send** command configures on-demand one-way frame delay measurement.

By default, on-demand one-way frame delay measurement is not configured in an MA.

Format

delay-measure one-way send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interval	Specifies the interval at which DM frames are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the one-way frame delay measurement count. **NOTE** *count-value* must be configured. There is no default value.	The value is an integer that ranges from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On-demand OAM indicates that OAM actions are initiated by manual configuration in a limited period of time. On-demand OAM may cause singular or periodic OAM actions during the diagnostic period. DM frames can be used for on-demand OAM to test the link delay.

One-way frame delay measurement is implemented between two MEPs by exchanging DM frames. A MEP periodically sends DM frames carrying

TxTimeStampf. After receiving a DM frame, the RMEP parses TxTimeStampf and compares this value with RxTimef (the time when the 1DM frame was received). The RMEP calculates the one-way frame delay based on these values using the following formula: Frame delay = RxTimef - TxTimeStampf

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- In a VLAN, outward-facing MEPs are supported. Perform the following operation to create a MEP in the MA view:
  - Run the **mep mep-id** command with *outward* specified to create an outward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way mep** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

- One-way frame delay measurement can be implemented only after the MEP synchronizes the time with its RMEP.
- To implement one-way frame delay measurement, specify the RMEP ID or destination MAC address, interval at which DM frames are sent, and measurement count:
  - If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for one-way frame delay measurement.
  - If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for one-way frame delay measurement.
- IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

In a VLAN, enable one-way frame delay measurement and set the destination MAC address to 01-22-33, interval at which DM frames are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way send mep 1 mac 01-22-33 interval 10000 count 60
```

In a VLAN, enable one-way frame delay measurement and set the RMEP ID to 2, interval at which DM frames are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure one-way send mep 1 remote-mep 2 interval 10000 count
60
```

12.9.11 delay-measure one-way receive

Function

The **delay-measure one-way receive** command enables the RMEP to receive DM frames to implement one-way frame delay measurement.

The **undo delay-measure one-way receive** command cancels the configuration.

By default, the RMEP is not enabled to receive DM frames.

Format

delay-measure one-way receive mep *mep-id*

undo delay-measure one-way receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used in a VLAN to enable the RMEP to receive DM frames to implement one-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Configure the RMEP to receive DM frames in a VLAN.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md3
[HUAWEI-md-md3] ma ma3
[HUAWEI-md-md3-ma-ma3] map vlan 10
[HUAWEI-md-md3-ma-ma3] mep mep-id 3 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md3-ma-ma3] delay-measure one-way receive mep 3
```

12.9.12 delay-measure one-way threshold

Function

The **delay-measure one-way threshold** command sets the alarm threshold for one-way frame delay measurement.

The **undo delay-measure one-way threshold** command cancels the configuration.

Format

delay-measure one-way threshold *threshold-value*

undo delay-measure one-way threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for one-way frame delay measurement.	The value is an integer that ranges from 1 to 4294967295, in microseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **delay-measure one-way threshold** command sets an alarm threshold for one-way frame delay measurement between a MEP and an RMEP. When the one-way frame delay exceeds the alarm threshold, an alarm is generated.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

This command is applicable to VLANs.

NOTE

Before setting the alarm threshold, you must correctly configure the MD and MA.

Example

Set the alarm threshold for one-way frame delay measurement in the VLAN to 10.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure one-way threshold 10
```

12.9.13 delay-measure two-way continual

Function

The **delay-measure two-way continual** command configures proactive two-way frame delay measurement.

The **undo delay-measure two-way continual** command cancels the configuration.

By default, proactive two-way frame delay measurement is not configured in an MA.

Format

delay-measure two-way continual send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }

undo delay-measure two-way continual send [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interval { **1000** | **10000** | **30000** | **60000** | **150000** | **300000** }	Specifies the interval at which DMMs frames are sent.	The value is 1000, 10000, 30000, 60000, 150000, and 300000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Proactive OAM indicates that OAM actions are carried out continuously.

Two-way frame delay measurement is performed by a local MEP to send a DMM to its RMEP and then receive a DMR from the RMEP. After the two-way frame delay measurement is configured, a MEP periodically sends DMMs carrying TxTimeStampf (the time when the DMM was sent). After receiving the DMM, the RMEP replies with a DMR. The DMR carries RxTimeStampf (the time when the DMM was received) and TxTimeStampb (the time when the DMR was sent). The value in every field of the DMM is copied to the DMR except that the source and destination MAC addresses were interchanged. Upon receiving the DMR, the MEP calculates the two-way frame delay by using the following formula: Frame delay = (RxTimeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)

When clocks of the MEPs at both ends of a link are not synchronized, the **delay-measure two-way continual** command can be used to implement proactive two-way frame delay measurement for a VLAN.

To implement proactive two-way frame delay measurement, you need to specify the RMEP ID or destination MAC address, interval at which DMMs are sent, and measurement count:

- If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for two-way frame delay measurement.

- If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for two-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command with *inward* specified in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure two-way continual** command, the following configurations need to be completed in addition to the preceding configurations:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

In a VLAN, enable proactive two-way frame delay measurement and set the destination MAC address to 01-22-33 and the interval at which DMMs are sent to 30s.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way continual send mep 1 mac 01-22-33 interval
30000
```

In a VLAN, enable proactive two-way frame delay measurement and set the RMEP ID to 2 and the interval at which DMMs are sent to 30s.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way continual send mep 1 remote-mep 2 interval
30000
```

12.9.14 delay-measure two-way continual send test-id

Function

The **delay-measure two-way continual send test-id** command configures two-way proactive frame delay measurement (DM).

The **undo delay-measure two-way continual send test-id** command deletes the configuration.

By default, two-way proactive frame DM is not configured in an MA.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-measure two-way continual send test-id *test-id* **interval** { **1000** | **10000** | **15000** | **30000** } [**packet-size** *packet-size*]

undo delay-measure two-way continual send test-id *test-id*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
interval { **1000** | **10000** | **15000** | **30000** }	Specifies the interval at which DMMs are sent.	Enumerated value, in milliseconds: ● 1000 ● 10000 ● 15000 ● 30000
packet-size *packet-size*	Specifies the size of the sent packets.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLAN scenarios, to implement two-way proactive frame DM, run the **delay-measure two-way continual** command. This command does not take effect in point-to-multipoint link scenarios. To implement two-way proactive frame DM for point-to-multipoint links, run the **delay-measure two-way continual send test-id** command.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The **delay-measure two-way continual send test-id** and **delay-measure two-way continual** commands are mutually exclusive.

Example

Configure two-way proactive frame DM with the test instance of 1 and DMM transmission interval of 30s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way continual send test-id 1 interval 30000
```

12.9.15 delay-measure two-way delay-threshold test-id

Function

The **delay-measure two-way delay-threshold test-id** command configures alarm thresholds for two-way proactive frame delay measurement (DM).

The **undo delay-measure two-way delay-threshold test-id** command deletes the alarm thresholds configured for two-way proactive frame DM.

By default, no alarm thresholds are configured for two-way proactive frame DM.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-measure two-way delay-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo delay-measure two-way delay-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
upper-limit *upper-limit*	Specifies an upper alarm threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds.
lower-limit *lower-limit*	Specifies a lower alarm threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds. The lower alarm threshold must be less than the upper alarm threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure upper and lower alarm thresholds for two-way proactive frame DM that monitors link quality, run the **delay-measure two-way delay-threshold test-id** command. After configuring upper and lower alarm thresholds, you can obtain data (such as the number of times that a threshold-crossing event occurs) within a sampling period to monitor network performance.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

Thresholds can be configured only for two-way proactive frame DM and cannot be configured for two-way on-demand frame DM.

Example

Set lower and upper alarm thresholds for two-way proactive frame DM in VLAN scenarios to 200 microseconds and 400 microseconds, respectively.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
```

```
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way delay-threshold test-id 1 upper-limit 400 lower-limit 200
```

12.9.16 delay-measure two-way send

Function

The **delay-measure two-way send** command configures on-demand two-way frame delay measurement.

By default, on-demand two-way frame delay measurement is not configured in an MA.

Format

delay-measure two-way send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	-
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interval	Specifies the interval at which DMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the number of sent DMMs.	The value is an integer that ranges from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On-demand OAM indicates that OAM actions are initiated by manual configuration in a limited period of time. On-demand OAM may cause singular or periodic OAM actions during the diagnostic period. DM frames can be used for on-demand OAM to test the link delay.

Two-way frame delay measurement is performed by a local MEP to send a DMM to its RMEP and then receive a DMR from the RMEP. After the two-way frame delay measurement is configured, a MEP periodically sends DMMs carrying TxTimeStampf (the time when the DMM was sent). After receiving the DMM, the RMEP replies with a DMR. The DMR carries RxTimeStampf (the time when the DMM was received) and TxTimeStampb (the time when the DMR was sent). The value in every field of the DMM is copied to the DMR except that the source and destination MAC addresses were interchanged. Upon receiving the DMR, the MEP calculates the two-way frame delay by using the following formula: Frame delay = (RxTimeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.

If **remote-mep** *mep-id* is specified in this command, the following configurations need to be completed in addition to the preceding configurations:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Precautions

- IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.
- To implement on-demand two-way frame delay measurement, you need to specify the RMEP ID or destination MAC address, interval at which DMMs are sent, and measurement count:
  - If the local MEP has not learned the RMEP MAC address, you must specify the destination MAC address for two-way frame delay measurement.
  - If the local MEP has learned the RMEP MAC address, you can specify the RMEP ID for two-way frame delay measurement.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

In a VLAN, enable on-demand two-way frame delay measurement and set the destination MAC address to 01-22-33, interval at which DMMs are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure two-way send mep 1 mac 01-22-33 interval 10000 count
60
```

In a VLAN, enable on-demand two-way frame delay measurement and set the RMEP ID to 2, interval at which DMMs are sent to 10000 ms, and measurement count to 60.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure two-way send mep 1 remote-mep 2 interval 10000 count
60
```

12.9.17 delay-measure two-way receive

Function

The **delay-measure two-way receive** command enables the RMEP to receive DMMs to implement two-way frame delay measurement.

The **undo delay-measure two-way receive** command cancels the configuration.

By default, the RMEP in an MA is not enabled to receive DMMs.

Format

delay-measure two-way receive mep *mep-id*

undo delay-measure two-way receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to enable the RMEP to receive DMMs to implement proactive or on-demand two-way frame delay measurement. This command is used in a VLAN where an outward-facing MEP is configured with two-way frame delay measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **remote-mep** command in the MA view to create an RMEP.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

Example

Enable the RMEP to receive DMMs in the MA **ma1** and MD **md1**, with the VLAN ID as 100.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 outward
[HUAWEI-md-md1-ma-ma1] delay-measure two-way receive mep 1
```

12.9.18 delay-measure two-way receive test-id

Function

The **delay-measure two-way receive test-id** command enables a Remote Maintenance Association End Point (RMEP) to receive Delay Measure Messages (DMMs) for two-way frame delay measurement (DM).

The **undo delay-measure two-way receive test-id** command disables an RMEP from receiving DMMs for two-way frame DM.

By default, the RMEP in a Maintenance Association (MA) is disabled from receiving DMMs.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-measure two-way receive test-id *test-id*

undo delay-measure two-way receive [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **delay-measure two-way continual send test-id** or **delay-measure two-way send test-id** command to enable a MEP to send DMMs for two-way frame DM, run the **delay-measure two-way receive test-id** command to enable the RMEP to receive DMMs.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The **delay-measure two-way receive test-id** and **delay-measure two-way receive** commands are mutually exclusive.

Example

Enable the RMEP to receive DMMs for two-way frame DM with the test instance of 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
```

```
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way receive test-id 1
```

12.9.19 delay-measure two-way send test-id

Function

The **delay-measure two-way send test-id** command configures on-demand two-way frame delay measurement based on the test instance.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-measure two-way send test-id *test-id* **interval** { **1000** | **10000** } **count** *count* [**packet-size** *packet-size*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
interval { **1000** | **10000** }	Specifies the interval at which DMMs are sent.	The value is either 1000 or 10000, expressed in milliseconds.
count *count*	Specifies the number of times that DMMs are sent.	The value is an integer ranging from 1 to 60.
packet-size *packet-size*	Specifies the size of the sent packets.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLAN scenarios, to implement two-way on-demand frame DM, run the **delay-measure two-way send** command. This command does not take effect in point-to-multipoint link scenarios.

To implement two-way on-demand frame DM for point-to-multipoint links, run the **delay-measure two-way send test-id** command.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The **delay-measure two-way send test-id** and **delay-measure two-way send** commands are mutually exclusive.

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

Configure two-way frame DM with the test instance ID of 1, DMM transmission interval of 10s, and measurement times of 60.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way send test-id 1 interval 10000 count 60
```

12.9.20 delay-measure two-way threshold

Function

The **delay-measure two-way threshold** command sets the alarm threshold for two-way frame delay measurement.

The **undo delay-measure two-way threshold** command cancels the configuration.

Format

delay-measure two-way threshold *threshold-value*

undo delay-measure two-way threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold for two-way frame delay measurement.	The value is an integer that ranges from 1 to 4294967295, in microseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applicable to VLANs. You can set the alarm threshold for two-way frame delay measurement on the MEP or RMEP. When the two-way delay exceeds the alarm threshold, an alarm is generated.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007.

NOTE

Before setting the alarm threshold, you must correctly configure the MD and MA.

Example

Set the alarm threshold for two-way frame delay measurement in the VLAN to 10.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] delay-measure two-way threshold 10
```

12.9.21 delay-measure two-way trigger if-down

Function

The **delay-measure two-way trigger if-down** command triggers an interface to go ETHOAM down when the delay or delay variation based on a test instance ID exceeds a specified threshold.

The **undo delay-measure two-way trigger if-down** command restores the default configuration.

By default, an interface is not triggered to go ETHOAM down when the delay or delay variation based on a test instance ID exceeds a specified threshold.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-measure two-way { **delay-threshold** | **variation-threshold** } **test-id** *test-id* **trigger if-down**

undo delay-measure two-way { **delay-threshold** | **variation-threshold** } **test-id** *test-id* **trigger if-down**

Parameters

Parameter	Description	Value
delay-threshold	Indicates that an interface is triggered to go ETHOAM down when the delay exceeds a specified threshold.	-
variation-threshold	Indicates that an interface is triggered to go ETHOAM down when the delay variation exceeds a specified threshold.	-
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no service is bound to the MA, the interface where the MEP resides is an Eth-Trunk interface's primary member interface. To ensure the quality of the primary link, run the **delay-measure two-way trigger if-down** command on the interface where the MEP resides. If the delay or delay variation based on a test instance ID exceeds the threshold configured using the **delay-measure two-way delay-threshold test-id** or **delay-measure two-way variation-threshold test-id** command, the primary link has poor quality. In this case, the interface is triggered to go ETHOAM down, triggering an active/standby Eth-Trunk link switchover.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Example

Trigger the Eth-Trunk member interface GE 0/0/1 to go Down when the two-way delay based on a test instance ID of 2 exceeds a specified threshold.

```
<HUAWEI> system-view
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep mep-id 8 interface gigabitethernet 0/0/1 outward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 9
[HUAWEI-md-md1-ma-ma1] test-id 2 mep 8 remote-mep 9
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 1
[HUAWEI-GigabitEthernet0/0/1] delay-measure two-way delay-threshold test-id 2 trigger if-down
```

12.9.22 delay-measure two-way variation-threshold test-id

Function

The **delay-measure two-way variation-threshold test-id** command configures variation thresholds for two-way proactive frame delay measurement (DM).

The **undo delay-measure two-way variation-threshold test-id** command deletes the variation thresholds configured for two-way proactive frame DM.

By default, no variation thresholds are configured for two-way proactive frame DM.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

delay-measure two-way variation-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo delay-measure two-way variation-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
upper-limit *upper-limit*	Specifies an upper variation threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds.
lower-limit *lower-limit*	Specifies a lower variation threshold for two-way proactive frame DM.	The value is an integer ranging from 0 to 4294967295, in microseconds. The lower variation threshold must be less than the upper variation threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure upper and lower variation thresholds for two-way proactive frame DM that monitors link quality, run the **delay-measure two-way variation-threshold test-id** command. After configuring upper and lower variation thresholds, you can obtain data (such as the number of times that a threshold-crossing event occurs) within a sampling period to monitor network performance.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

The configured threshold makes sense only after the proactive measurement is configured.

Example

Set lower and upper variation thresholds for two-way proactive frame DM in VLAN scenarios to 200 microseconds and 400 microseconds, respectively.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
```

```
[HUAWEI-md-md1-ma-ma1] mep ccm-send enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive enable
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] delay-measure two-way variation-threshold test-id 1 upper-limit 400
lower-limit 200
```

12.9.23 display y1731 statistic-type

Function

The **display y1731 statistic-type** command displays performance statistics collected through Y.1731.

Format

display y1731 statistic-type { **oneway-delay** | **twoway-delay** } **md** *md-name* **ma** *ma-name* [**count** *count-value*]

display y1731 statistic-type { **single-loss** | **dual-loss** } **md** *md-name* **ma** *ma-name* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

display y1731 statistic-type single-loss test-id *test-id* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

display y1731 statistic-type single-synthetic-loss test-id *test-id* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

display y1731 statistic-type twoway-delay test-id *test-id* [**count** *count-value*] (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

Parameters

Parameter	Description	Value
dual-loss	Displays statistics about dual-ended frame loss measurement.	-
single-loss	Displays statistics about single-ended frame loss measurement.	-
oneway-delay	Displays statistics about the one-way frame delay.	-
twoway-delay	Displays statistics about the two-way frame delay.	-

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 characters without spaces, hyphens (-), and question marks (?). MD names on a device are unique.
ma *ma-name*	Specifies the name of an MA.	The value is a string of characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD must be within 44 characters. Names of MAs in an MD are unique.
count *count-value*	Specifies the number of statistics entries to be displayed. If the parameter is not specified, the command output displays all the statistics.	The value is an integer in the range from 1 to 60.
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.
single-synthetic-loss	Displays statistics about single-ended SLM.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display y1731 statistic-type** command to display performance statistics collected through Y.1731, including single-ended frame loss statistics, dual-ended frame loss statistics, single-ended SLM statistics, one-way frame delay statistics, and two-way frame delay statistics.

Prerequisites

The **cfm enable (system view)** command has been run to enable the CFM function globally.

Example

Display the statistics about the one-way frame delay in the MA **ma1** in the MD **md1**.

```
<HUAWEI> display y1731 statistic-type oneway-delay md md1 ma ma1
Latest one-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)     Delay variation(usec)
--------------------------------------------------------------------------------
    1         10000                    -
    2         10000                    0
    3         10000                    0
    4         10000                    0
    5         10000                    0
    6         10000                    0
    7         10000                    0
    8         10000                    0
    9         10000                    0
   10          10000                    0
   11          10000                    0
   12          40000                30000
   13          10000                30000
   14          10000                    0
   15          10000                    0
   16          10000                    0
   17          10000                    0
--------------------------------------------------------------------------------
Average delay(usec) :      11764    Average delay variation(usec) :       3750
Maximum delay(usec) :      40000    Maximum delay variation(usec) :      30000
Minimum delay(usec) :      10000    Minimum delay variation(usec) :          0
```

Table 12-70 Description of the **display y1731 statistic-type** command output

Item	Description
Latest one-way delay statistics	Statistics about the one-way frame delay.
Index	Measurement index.
Delay(usec)	One-way delay, in microseconds.
Delay variation(usec)	One-way delay variation, in microseconds.
Average delay(usec)	Average one-way delay, in microseconds.
Average delay variation(usec)	Average one-way delay variation, in microseconds.
Maximum delay(usec)	Maximum one-way delay, in microseconds.
Maximum delay variation(usec)	Maximum one-way delay variation, in microseconds.
Minimum delay(usec)	Minimum one-way delay, in microseconds.
Minimum delay variation(usec)	Minimum one-way delay variation, in microseconds.

Display the statistics about the two-way frame delay in the MA **ma2** in the MD **md2**.

```
<HUAWEI> display y1731 statistic-type twoway-delay md md2 ma ma2
Latest two-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)     Delay variation(usec)
--------------------------------------------------------------------------------
    1            0                    -
    2            0                    0
    3            0                    0
    4            0                    0
    5            0                    0
    6            0                    0
    7            0                    0
    8            0                    0
    9            0                    0
   10            0                    0
--------------------------------------------------------------------------------
Average delay(usec) :          0    Average delay variation(usec) :          0
Maximum delay(usec) :          0    Maximum delay variation(usec) :          0
Minimum delay(usec) :          0    Minimum delay variation(usec) :          0
```

Table 12-71 Description of the **display y1731 statistic-type** command output

Item	Description
Latest two-way delay statistics	Statistics about the two-way frame delay.
Index	Measurement index.
Delay(usec)	Two-way delay, in microseconds.
Delay variation(usec)	Two-way delay variation, in microseconds.
Average delay(usec)	Average two-way delay, in microseconds.
Average delay variation(usec)	Average two-way delay variation, in microseconds.
Maximum delay(usec)	Maximum two-way delay, in microseconds.
Maximum delay variation(usec)	Maximum two-way delay variation, in microseconds.
Minimum delay(usec)	Minimum two-way delay, in microseconds.
Minimum delay variation(usec)	Minimum two-way delay variation, in microseconds.

Display proactive single-ended SLM statistics in test instance 2.

```
<HUAWEI> display y1731 statistic-type single-synthetic-loss test-id 2
--------------------------------------------------------------------------------
Index       L-send R-send L-recv Unack  L-loss R-loss L-loss-ratio R-loss-ratio
--------------------------------------------------------------------------------
667         1000   1000   1000   0          0      0      0.0000%      0.0000%
668         1000   1000   1000   0          0      0      0.0000%      0.0000%
669         1000   1000   1000   0          0      0      0.0000%      0.0000%
670         1000   1000   1000   0          0      0      0.0000%      0.0000%
671         1000   1000   1000   0          0      0      0.0000%      0.0000%
672         1000   1000   1000   0          0      0      0.0000%      0.0000%
673         1000   1000   1000   0          0      0      0.0000%      0.0000%
674         1000   1000   1000   0          0      0      0.0000%      0.0000%
675         1000   1000   1000   0          0      0      0.0000%      0.0000%
676         1000   1000   1000   0          0      0      0.0000%      0.0000%
```

```
677        1000   1000   1000   0          0      0      0.0000%      0.0000%
678        1000   1000   1000   0          0      0      0.0000%      0.0000%
679        1000   1000   1000   0          0      0      0.0000%      0.0000%
680        1000   1000   1000   0          0      0      0.0000%      0.0000%
681        1000   1000   1000   0          0      0      0.0000%      0.0000%
682        1000   1000   1000   0          0      0      0.0000%      0.0000%
683        1000   1000   1000   0          0      0      0.0000%      0.0000%
684        1000   1000   1000   0          0      0      0.0000%      0.0000%
--------------------------------------------------------------------------------
Average Local-loss  :          0    Average Local-loss Ratio  :         0.0000%
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :         0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :         0.0000%
Average Remote-loss :          0    Average Remote-loss Ratio :         0.0000%
Maximum Remote-loss :          0    Maximum Remote-loss Ratio :         0.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :         0.0000%
```

Table 12-72 Description of the **display y1731 statistic-type** command output

Item	Description
Index	Measurement index.
L-send	Number of packets sent from the local end in each round.
R-send	Number of packets sent from the remote end in each round.
L-recv	Number of packets received by the local end in each round.
Unack	Number of unacknowledged packets.
L-loss	Number of lost packets on the local end in each round.
R-loss	Number of lost packets on the remote end in each round.
L-loss-ratio	Packet loss rate on the local end in each round.
R-loss-ratio	Packet loss rate on the remote end in each round.
Average Local-loss	Average number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.

Item	Description
Average Remote-loss	Average number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

Display on-demand single-ended SLM statistics.

```
<HUAWEI> display y1731 statistic-type single-synthetic-loss test-id 1
Measurement Start Time : 2014-05-23 16:32:13-08:00
--------------------------------------------------------------------------------
Index       L-send R-send L-recv Unack  L-loss R-loss L-loss-ratio R-loss-ratio
--------------------------------------------------------------------------------
1          10     10     10     0          0      0      0.0000%      0.0000%
--------------------------------------------------------------------------------
Average Local-loss  :          0    Average Local-loss Ratio  :         0.0000%
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :         0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :         0.0000%
Average Remote-loss :          0    Average Remote-loss Ratio :         0.0000%
Maximum Remote-loss :          0    Maximum Remote-loss Ratio :         0.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :         0.0000%
```

Table 12-73 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	Measurement index.
L-send	Number of packets sent from the local end in each round.
R-send	Number of packets sent from the remote end in each round.
L-recv	Number of packets received by the local end in each round.
Unack	Number of unacknowledged packets.
L-loss	Number of lost packets on the local end in each round.

Item	Description
R-loss	Number of lost packets on the remote end in each round.
L-loss-ratio	Packet loss rate on the local end in each round.
R-loss-ratio	Packet loss rate on the remote end in each round.
Average Local-loss	Average number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

Display statistics about on-demand two-way frame delay measurement.

```
<HUAWEI> display y1731 statistic-type twoway-delay test-id 1
Measurement Start Time : 2017-07-29 08:43:12
Latest two-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)    Delay variation(usec)
--------------------------------------------------------------------------------
   1          202                    -
   2          237                   35
   3          219                   18
   4          234                   15
   5          243                    9
   6          262                   19
   7          263                    1
```

```
  8          245                   18
  9          229                   16
  10          237                   8
--------------------------------------------------------------------------------
Average delay(usec) :        237    Average delay variation(usec) :         15
Maximum delay(usec) :        263    Maximum delay variation(usec) :         35
Minimum delay(usec) :        202    Minimum delay variation(usec) :          1
```

Table 12-74 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Latest two-way delay statistics	Statistics about the two-way frame delay.
Index	Measurement index.
Delay(usec)	Two-way delay, in microseconds.
Delay variation(usec)	Two-way delay variation, in microseconds.
Average delay(usec)	Average two-way delay, in microseconds.
Maximum delay(usec)	Maximum two-way delay, in microseconds.
Minimum delay(usec)	Minimum two-way delay, in microseconds.
Average delay variation(usec)	Average two-way delay variation, in microseconds.
Maximum delay variation(usec)	Maximum two-way delay variation, in microseconds.
Minimum delay variation(usec)	Minimum two-way delay variation, in microseconds.

Display dual-ended frame loss measurement statistics in the MA **ma2** in the MD **md2**.

```
<HUAWEI> display y1731 statistic-type dual-loss md md2 ma ma2
Measurement Start Time : 2018-09-28 16:48:39
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index    Local-loss    Local-loss ratio    Remote-loss    Remote-loss ratio
--------------------------------------------------------------------------------
  1          0            0.0000%             0             0.0000%
  2          0            0.0000%             0             0.0000%
  3          0            0.0000%             0             0.0000%
  4          0            0.0000%             0             0.0000%
  5          0            0.0000%             0             0.0000%
  6          0            0.0000%             0             0.0000%
  7          0            0.0000%             0             0.0000%
  8          0            0.0000%             0             0.0000%
  9          0            0.0000%             0             0.0000%
  10          0            0.0000%             0             0.0000%
  11          0            0.0000%             0             0.0000%
  12          0            0.0000%             0             0.0000%
  13          0            0.0000%             0             0.0000%
  14          0            0.0000%             0             0.0000%
  15          0            0.0000%             0             0.0000%
--------------------------------------------------------------------------------
Average Local-loss  :          0    Average Local-loss Ratio  :   0.0000%
```

```
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :   0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :   0.0000%
Average Remote-loss :          0    Average Remote-loss Ratio :   0.0000%
Maximum Remote-loss :          0    Maximum Remote-loss Ratio :   0.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :   0.0000%
```

Table 12-75 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	Measurement index.
Local-loss	Number of lost packets on the local end.
Local-loss ratio	Packet loss rate on the local end.
Remote-loss	Number of lost packets on the remote end.
Remote-loss ratio	Packet loss rate on the remote end, Packet loss rate on the remote end = Number of packets lost on the remote end/Number of packets sent by the local end.
Average Local-loss	Average number of lost packets on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

Display single-ended frame loss measurement statistics in the MA **ma2** in the MD **md2**.

```
<HUAWEI> display y1731 statistic-type single-loss md md2 ma ma2
Measurement Start Time : 2018-09-28 16:48:39
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index    Local-loss    Local-loss ratio    Remote-loss    Remote-loss ratio
--------------------------------------------------------------------------------
   1           0            0.0000%            0             0.0000%
   2           0            0.0000%            0             0.0000%
   3           5           50.0000%           10             50.0000%
   4           0            0.0000%            0             0.0000%
   5           5           50.0000%           10             50.0000%
   6          10            50.0000%            5             50.0000%
   7           5           50.0000%           10             50.0000%
   8          10            50.0000%            5             50.0000%
   9          10            50.0000%            5             50.0000%
  10           5            50.0000%           10             50.0000%
  11           5            50.0000%           10             50.0000%
  12          10             50.0000%            5             50.0000%
  13           5            50.0000%           10             50.0000%
  14          10             50.0000%            5             50.0000%
  15           5            50.0000%           10             50.0000%
  16          10             50.0000%            5             50.0000%
--------------------------------------------------------------------------------
Average Local-loss  :          5    Average Local-loss Ratio  :  40.6250%
Maximum Local-loss  :         10    Maximum Local-loss Ratio  :  50.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :   0.0000%
Average Remote-loss :          6    Average Remote-loss Ratio :  40.6250%
Maximum Remote-loss :         10    Maximum Remote-loss Ratio :  50.0000%
Minimum Remote-loss :          0    Minimum Remote-loss Ratio :   0.0000%
```

Table 12-76 Description of the **display y1731 statistic-type** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	Measurement index.
Local-loss	Number of lost packets on the local end.
Local-loss ratio	Packet loss rate on the local end.
Remote-loss	Number of lost packets on the remote end.
Remote-loss ratio	Packet loss rate on the remote end, Packet loss rate on the remote end = Number of packets lost on the remote end/Number of packets sent by the local end.
Average Local-loss	Average number of lost packets on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss rate on the local end.

Item	Description
Maximum Local-loss Ratio	Maximum packet loss rate on the local end.
Minimum Local-loss Ratio	Minimum packet loss rate on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss rate on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss rate on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss rate on the remote end.

12.9.24 display y1731 test-info

Function

The **display y1731 test-info** command displays information about test instances for Y.1731 statistics collection.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display y1731 test-info [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id *test-id*	Displays information about a specified test instance.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about test instances for Y.1731 statistics collection, run the **display y1731 test-info** command.

Example

Display information about test instance 1 for Y.1731 statistics collection on a device.

```
<HUAWEI> display y1731 test-info test-id 1
-----------------------------------------------------------
 TestId 1 information:
-----------------------------------------------------------
 MD Name                      : md1
 MA Name                      : ma
 MEP ID                       : 1
 Local Mac                    : xxxx-xxxx-xxxx
 Remote MEP ID                : 2
 Bind Mac                     : --
 Send Mac                     : --
 8021p                        : --
 Uplink 8021p                 : --
 Downlink 8021p               : --
 Single LM                    : disabled
 Single LM Interval           : --
 Single LM Count              : --
 Single LM Receive            : disabled
 OneWay DM                    : disabled
 OneWay DM Interval           : --
 OneWay DM Count              : --
 OneWay DM Packet Size        : --
 OneWay DM Receive            : disabled
 TwoWay DM                    : disabled
 TwoWay DM Interval           : --
 TwoWay DM Count              : --
 TwoWay DM Packet Size        : --
 TwoWay DM Receive            : disabled
 Single SLM                   : continual
 Single SLM Interval          : 10ms
 Single SLM SendingCount      : 10
 Single SLM SendTimeout       : 5s
 Single SLM Receive           : disabled
 Single SLM RecvTimeout       : --
```

Table 12-77 Description of the **display y1731 test-info** command output

Item	Description
TestId 1 information	Information about test instance 1.
MD Name	Name of the MD.
MA Name	Name of the MA.
MEP ID	MEP ID.
Local Mac	Local MAC address.

Item	Description
Remote MEP ID	RMEP ID.
Bind Mac	MAC address of the RMEP.
Send Mac	MAC address carried in frames.
8021p	802.1p priority value specified in a specified test instance. To set the 802.1p priority value specified in a specified test instance, run the **test-id** command.
Uplink 8021p	Priority value of upstream packets. The switch does not support this function.
Downlink 8021p	Priority value of downstream packets. The switch does not support this function.
Single LM	Whether Y.1731 packet sending is enabled for single-ended frame LM. ● enabled ● disabled To enable Y.1731 packet sending for single-ended frame LM, run the **loss-measure single-ended send test-id** or **loss-measure single-ended continual send test-id** command.
Single LM Interval	Interval at which Y.1731 packets are sent for single-ended frame LM. To set the interval at which Y.1731 packets are sent for single-ended frame LM, run the **loss-measure single-ended send test-id** or **loss-measure single-ended continual send test-id** command.
Single LM Count	Number of Y.1731 packets that are to be sent for single-ended frame LM. To set the number of Y.1731 packets sent for single-ended frame LM, run the **loss-measure single-ended send test-id** command.
Single LM Receive	Whether Y.1731 packet receiving is enabled for single-ended frame LM. ● enabled ● disabled To enable SLM frame sending for single-ended SLM, run the **loss-measure single-ended receive test-id** command.

Item	Description
OneWay DM	Whether Y.1731 packet sending is enabled for one-way frame DM. - enabled - disabled The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Interval	Interval at which Y.1731 packets are sent for one-way frame DM. The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Count	Number of Y.1731 packets sent for one-way frame DM. The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Packet Size	Size of Y.1731 packets transmitted for one-way frame DM. The switch does not support one-way frame delay measurement based on test instances.
OneWay DM Receive	Whether Y.1731 packet receiving is enabled for one-way frame DM. - enabled - disabled The switch does not support one-way frame delay measurement based on test instances.
TwoWay DM	Whether Y.1731 packet sending is enabled for two-way frame DM. - enabled - disabled To enable Y.1731 packet sending for two-way frame DM, run the **delay-measure two-way send test-id** or **delay-measure two-way continual send test-id** command.

Item	Description
TwoWay DM Interval	Interval at which Y.1731 packets are sent for two-way frame DM. To set the interval at which Y.1731 packets are sent for two-way frame DM, run the **delay-measure two-way send test-id** or **delay-measure two-way continual send test-id** command.
TwoWay DM Count	Number of Y.1731 packets sent for two-way frame DM. To set the number of Y.1731 packets sent for two-way frame DM, run the **delay-measure two-way send test-id** command.
TwoWay DM Packet Size	Size of Y.1731 packets transmitted for two-way frame DM. To set the size of Y.1731 packets transmitted for two-way frame DM, run the **delay-measure two-way send test-id** or **delay-measure two-way continual send test-id** command.
TwoWay DM Receive	Whether Y.1731 packet receiving is enabled for two-way frame DM. ● enabled ● disabled To enable Y.1731 packet receiving for two-way frame DM, run the **delay-measure two-way receive test-id** command.
Single SLM	Whether Y.1731 packet sending is enabled for single-ended SLM. ● enabled ● disabled To enable Y.1731 packet sending for single-ended SLM, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.
Single SLM Interval	Interval at which SLM frames are sent for single-ended SLM. To set the interval at which SLM frames are sent for single-ended SLM, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.

Item	Description
Single SLM SendingCount	Number of SLM frames to be sent for single-ended SLM within each measurement period. To set the number of SLM frames to be sent for single-ended SLM within each measurement period, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.
Single SLM SendTimeout	Timeout period for the transmit end to receive SLM frames. To set the timeout period for the transmit end to receive SLM frames, run the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command.
Single SLM Receive	Whether SLM frame sending is enabled for single-ended SLM. ● enabled ● disabled To enable SLM frame sending for single-ended SLM, run the **loss-measure single-ended-synthetic receive** command.
Single SLM RecvTimeout	Timeout period for the receive end to receive SLM frames. To set the timeout period for the receive end to receive SLM frames, run the **loss-measure single-ended-synthetic receive** command.

12.9.25 loss-measure dual-ended continual

Function

The **loss-measure dual-ended continual** command enables proactive dual-ended frame loss measurement.

The **undo loss-measure dual-ended continual** command disables proactive dual-ended frame loss measurement.

By default, dual-ended frame loss measurement is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure dual-ended continual mep *mep-id* **remote-mep** *mep-id*

undo loss-measure dual-ended continual [**mep** *mep-id* [**remote-mep** *mep-id*]]

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The dual-ended frame loss measurement function is service-oriented. You can estimate quality of services based on the calculated packet loss rate.

Dual-ended frame loss measurement is deployed on end-to-end MEPs. In Y.1731, frame loss statistics are collected based on the transmit and receive counters carried in CCMs.

NOTE

The interval for collecting dual-ended frame loss statistics does not need to be configured separately, because it equals the interval at which CCMs are sent.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Example

Enable dual-ended frame loss measurement in the VLAN scenario.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet0/0/1 outward
[HUAWEI-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[HUAWEI-md-md1-ma-ma1] loss-measure dual-ended continual mep 1 remote-mep 2
```

12.9.26 loss-measure single-ended continual send

Function

The **loss-measure single-ended continual send** command enables proactive single-ended frame loss measurement.

The **undo loss-measure single-ended continual send** command disables proactive single-ended frame loss measurement.

By default, proactive single-ended frame loss measurement is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended continual send mep *mep-id* { **mac** *mac-address* | **remote-mep** *mep-id* } **interval** { **1000** | **10000** | **30000** }

undo loss-measure single-ended continual send [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in the format of H-H-H, where H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.
interval	Specifies the interval at which LMMs are sent.	The value is 1000, 10000, or 30000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The collection interval can be specified to collect statistics about and analyze packet loss data in a period of time.

NOTE

Single-ended frame loss measurement is implemented for the link between the local MEP and an RMEP identified by an ID or a MAC address.

- If the local MEP has not learned the MAC address of the RMEP, the MAC address of the RMEP must be specified to implement single-ended frame loss measurement.
- If the local MEP has learned the MAC address of the RMEP, the ID of the RMEP can be used to implement single-ended frame loss measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Example

Enable single-ended frame loss measurement in the VLAN scenario and set the RMEP ID to 2 and interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended continual send mep 1 remote-mep 2 interval
30000
```

12.9.27 loss-measure single-ended continual send test-id

Function

The **loss-measure single-ended continual send test-id** command enables single-ended frame loss measurement based on the test instance.

The **undo loss-measure single-ended continual send test-id** command disables on-demand single-ended frame loss measurement.

By default, on-demand single-ended frame loss measurement is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended continual send test-id *test-id* **interval** { **1000** | **10000** | **30000** }

undo loss-measure single-ended continual send [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.
interval	Specifies the interval at which LMMs are sent.	The value is 1000, 10000, or 30000, in milliseconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Statistics based on a test instance are mainly used in the P2MP scenario. You can run this command to collect non-stop packet loss statistics.

Prerequisites

The **test-id** *test-id* command has been run in the MA view to create a test instance.

Example

Enable single-ended frame loss measurement based on test instance 1 in the VLAN scenario and set the interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended continual send test-id 1 interval 30000
```

12.9.28 loss-measure single-ended receive

Function

The **loss-measure single-ended receive** command enables the remote device to receive LMMs to implement single-ended frame loss measurement.

The **undo loss-measure single-ended receive** command disables the remote device from receiving LMMs.

By default, the remote device is disabled from receiving LMMs in an MA.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended receive mep *mep-id*

undo loss-measure single-ended receive [**mep** *mep-id*]

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of an MEP.	The value is an integer in the range from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the packet loss rate is detected on a link to evaluate the link performance, you can run this command to enable the remote device to receive LMMs. This command is used to configure the remote device in the single-ended frame loss measurement in the VLAN scenario.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

Example

Configure the remote device to receive LMMs in a VLAN.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet0/0/1 outward
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended receive mep 1
```

12.9.29 loss-measure single-ended receive test-id

Function

The **loss-measure single-ended receive test-id** command enables the remote device to receive LMMs based on the test instance to implement single-ended frame loss measurement.

The **undo loss-measure single-ended receive test-id** command disables the remote device from receiving LMMs based on the test instance.

By default, the remote device is disabled from receiving LMMs in an MA.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended receive test-id *test-id*

undo loss-measure single-ended receive [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Statistics based on a test instance are mainly used in the P2MP scenario. When the packet loss rate is detected on a link to evaluate the link performance, you can run this command to enable the remote device to receive LMMs.

Prerequisites

The **test-id** *test-id* command has been run in the MA view to create a test instance.

Example

Configure the remote device to receive LMMs based on the test instance.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended receive test-id 1
```

12.9.30 loss-measure single-ended send

Function

The **loss-measure single-ended send** command enables single-ended frame loss measurement.

By default, single-ended frame loss measurement is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended send mep *mep-id* [**mac** *mac-address* | **remote-mep** *mep-id*] **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer in the range from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in the format of H-H-H, where H is a hexadecimal number of 1 to 4 digits.
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer in the range from 1 to 8191.
interval	Specifies the interval at which LMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the single-ended frame loss measurement count.	The value is an integer in the range from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

When the packet loss rate is detected on a link to evaluate the link performance, you can run this command to enable the remote device to receive LMMs.

NOTE

Single-ended frame loss measurement is implemented for the link between the local MEP and an RMEP identified by an ID or a MAC address.

- If the local MEP has not learned the MAC address of the RMEP, the MAC address of the RMEP must be specified to implement single-ended frame loss measurement.
- If the local MEP has learned the MAC address of the RMEP, the ID of the RMEP can be used to implement single-ended frame loss measurement.

Prerequisites

The command takes effect only after the following configurations are completed:

- Run the **cfm version standard** command in the system view to specify IEEE Standard 802.1ag-2007 for CFM.
- Run the **cfm enable (system view)** command to enable CFM globally.
- Run the **cfm md** command in the system view to create an MD.
- Run the **ma** command in the MD view to create an MA.
- Run the **mep mep-id** command in the MA view to create an inward-facing MEP.

If **remote-mep** *mep-id* is specified in the **delay-measure one-way continual** command, the following configurations must be completed:

- Run the **remote-mep** command in the MA view to create an RMEP.
- Run the **mep ccm-send enable** command in the MA view to enable the local MEP in the MA to send CCMs.
- Run the **remote-mep ccm-receive enable** command in the MA view to enable the MEP to receive CCMs from the RMEP in the same MA.

Example

In the VLAN scenario, enable single-ended frame loss measurement and set the RMEP ID to 2, measurement interval to 10 seconds, and measurement count to 60 times.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet0/0/1 outward
[HUAWEI-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[HUAWEI-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended send mep 1 remote-mep 2 interval 10000
count 60
```

12.9.31 loss-measure single-ended send test-id

Function

The **loss-measure single-ended send test-id** command enables single-ended frame loss measurement based on the test instance.

By default, single-ended frame loss measurement based on the test instance is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended send test-id *test-id* **interval** { **1000** | **10000** } **count** *count-value*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer in the range from 1 to 4294967295.
interval	Specifies the interval at which LMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count-value*	Specifies the single-ended frame loss measurement count.	The value is an integer in the range from 1 to 60.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Statistics collection based on the test instance is applicable to the P2MP scenario. You can run this command to check the packet loss on the link periodically or once only.

Prerequisites

The **test-id** *test-id* command has been run in the MA view to create a test instance.

Example

In the VLAN scenario, enable single-ended frame loss measurement based on the test instance 1 and set the measurement interval to 10 seconds and measurement count to 60 times.

```
<HUAWEI> system-view
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 10
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended send test-id 1 interval 10000 count 60
```

12.9.32 loss-measure single-ended-synthetic continual send

Function

The **loss-measure single-ended-synthetic continual send** command enables proactive single-ended synthetic loss measurement (SLM).

The **undo loss-measure single-ended-synthetic continual send** command disables proactive single-ended SLM.

By default, proactive single-ended SLM is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended-synthetic continual send test-id *test-id* **interval** { **3.3** | **10** | **100** | **1000** | **10000** } [**sending-count** *count-value*] [**time-out** *timeout*] [**packet-size** *packet-size*]

undo loss-measure single-ended-synthetic continual send test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
interval { **3.3** | **10** | **100** | **1000** | **10000** }	Specifies the interval at which SLM frames are sent.	Enumerated value, in milliseconds: ● 3.3 ● 10 ● 100 ● 1000 ● 10000
sending-count *count-value*	Specifies the times that SLM frames are sent within each measurement period.	The value is an integer ranging from 1 to 1000. The default value is 10.
timeout *timeout*	Specifies the timeout period during which the device waits for a response.	The value is an integer ranging from 1 to 10, in seconds. The default value is 5s.
packet-size *packet-size*	Specifies the size of the SLM frames.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect accurate frame loss statistics on a point-to-multipoint network, run the **loss-measure single-ended-synthetic continual send** command to configure proactive single-ended SLM.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Example

Configure SLM with **test id** of 1 and statistics collection interval of 10s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic continual send test-id 1 interval 10
```

12.9.33 loss-measure single-ended-synthetic local-ratio-threshold test-id

Function

The **loss-measure single-ended-synthetic local-ratio-threshold test-id** command configures local packet loss ratio thresholds for single-ended synthetic loss measurement (SLM).

The **undo loss-measure single-ended-synthetic local-ratio-threshold test-id** command deletes the local packet loss ratio thresholds configured for single-ended SLM.

By default, no local packet loss ratio thresholds are configured for single-ended SLM.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended-synthetic local-ratio-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo loss-measure single-ended-synthetic local-ratio-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
upper-limit *upper-limit*	Specifies an upper local packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages.
lower-limit *lower-limit*	Specifies a lower local packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages. The lower local packet loss ratio threshold must be less than the upper local packet loss ratio threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a point-to-multipoint or multipoint-to-multipoint network, run the **loss-measure single-ended-synthetic local-ratio-threshold test-id** command to configure local packet loss ratio thresholds for single-ended SLM. After configuring upper and lower local packet loss ratio thresholds, you can obtain data (such as the number of times that a threshold-crossing event occurs) within a sampling period to monitor network performance.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

Thresholds can be configured only for proactive single-ended SLM and cannot be configured for on-demand single-ended SLM.

Example

Set lower and upper local packet loss ratio thresholds for single-ended SLM to 10.1111 and 11.1111 respectively for test instance 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
```

```
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic local-ratio-threshold test-id 1 upper-
limit 11.1111 lower-limit 10.1111
```

12.9.34 loss-measure single-ended-synthetic receive

Function

The **loss-measure single-ended-synthetic receive** command enables a device to receive synthetic loss measurement (SLM) frames for single-ended SLM.

The **undo loss-measure single-ended-synthetic receive** command disables the device from receiving SLM frames.

By default, no device in a maintenance association (MA) is enabled to receive SLM frames.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended-synthetic receive test-id *test-id* [**time-out** *timeout-value*]

undo loss-measure single-ended-synthetic receive test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
time-out *timeout-value*	Specifies the timeout period for the receive end to receive SLM frames.	The value is an integer that ranges from 10 to 300, in seconds. The default value is 300.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **loss-measure single-ended-synthetic send** command is run to configure on-demand single-ended SLM or the **loss-measure single-ended-synthetic continual send** command is run to configure proactive single-ended SLM, run the **loss-measure single-ended-synthetic receive** command to enable the device to receive SLM frames.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

If you delete or modify the configuration on the receive end more than once, the statistical data may become incorrect. Therefore, do not delete or modify the statistical task after the configuration is complete.

To modify the configuration, disable the device from receiving SLM frames and then perform reconfiguration.

For a proactive single-ended SLM task, set **time-out** on the receive end to a value greater than the value of **interval** on the transmit end.

Example

Configure the remote end to receive SLM frames, set the value of **test id** to 1, and set the timeout period for the receive end to receive SLM frames to 200s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic receive test-id 1 time-out 200
```

12.9.35 loss-measure single-ended-synthetic remote-ratio-threshold test-id

Function

The **loss-measure single-ended-synthetic remote-ratio-threshold test-id** command configures remote packet loss ratio thresholds for single-ended synthetic loss measurement (SLM).

The **undo loss-measure single-ended-synthetic remote-ratio-threshold test-id** command deletes the remote packet loss ratio thresholds configured for single-ended SLM.

By default, no remote packet loss ratio thresholds are configured for single-ended SLM.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended-synthetic remote-ratio-threshold test-id *test-id* **upper-limit** *upper-limit* **lower-limit** *lower-limit*

undo loss-measure single-ended-synthetic remote-ratio-threshold test-id *test-id* [**upper-limit** *upper-limit* **lower-limit** *lower-limit*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
upper-limit *upper-limit*	Specifies an upper remote packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages.
lower-limit *lower-limit*	Specifies a lower remote packet loss ratio threshold for single-ended SLM.	The value is a string of 1 to 8 characters in the format of *xxx.xxxx*, in percentages. The lower remote packet loss ratio threshold must be less than the upper remote packet loss ratio threshold.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a point-to-multipoint or multipoint-to-multipoint scenario, you can run this command to configure remote packet loss ratio thresholds for single-ended SLM. After the thresholds are configured, you can obtain data such as the number of times that a threshold-crossing event occurs.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

Thresholds can be configured only for proactive single-ended SLM and cannot be configured for on-demand single-ended SLM.

Example

Set lower and upper remote packet loss ratio thresholds for single-ended SLM to 10.1111 and 11.1111 respectively for test instance 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic remote-ratio-threshold test-id 1
upper-limit 11.1111 lower-limit 10.1111
```

12.9.36 loss-measure single-ended-synthetic send

Function

The **loss-measure single-ended-synthetic send** command configures on-demand single-ended synthetic loss measurement (SLM).

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended-synthetic send test-id *test-id* **interval** { **3.3** | **10** | **100** | **1000** | **10000** } [**sending-count** *count-value*] [**time-out** *time-out-value*] [**packet-size** *packet-size*] [**measurement-count** *measurement-count*]

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
interval { **3.3** | **10** | **100** | **1000** | **10000** }	Specifies the interval at which SLM frames are sent.	Enumerated value, in milliseconds: - 3.3 - 10 - 100 - 1000 - 10000
sending-count *count-value*	Specifies the times that SLMs are sent within each measurement period.	The value is an integer ranging from 1 to 1000. The default value is 10.
time-out *time-out-value*	Specifies the timeout period during which the device waits for a reply.	The value is an integer ranging from 1 to 10, in seconds. The default value is 5s.
packet-size *packet-size*	Specifies the size of the sent packet.	The value is an integer ranging from 64 to 1518, in bytes. The default value is 64.
measurement-count *measurement-count*	Specifies the number of measurements.	The value is an integer ranging from 1 to 60. The default value is 1.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When implementing frame loss measurement (LM), Maintenance Association End Points (MEPs) exchange ETH-LM frames. However, single-ended frame LM cannot collect accurate frame loss statistics on a point-to-multipoint or multipoint-to-multipoint network. To resolve this issue, configure on-demand single-ended SLM.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Precautions

If the configuration changes during on-demand statistics, you can view only the pre-change statistics results. You are advised to run the command for on-demand statistics again for query.

Example

Configure single-ended SLM with the test ID of 1, SLM frame transmission interval of 1s, SLM frame transmission times of 10, and timeout period waiting for a reply of 5s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 2
[HUAWEI-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[HUAWEI-md-md1-ma-ma1] loss-measure single-ended-synthetic send test-id 1 interval 1000 sending-count 10 time-out 5
```

12.9.37 loss-measure single-ended-synthetic trigger if-down

Function

The **loss-measure single-ended-synthetic trigger if-down** command triggers an interface to go ETHOAM down when the near- or far-end frame loss ratio based on a test instance ID exceeds a specified threshold.

The **undo loss-measure single-ended-synthetic trigger if-down** command restores the default configuration.

By default, an interface is not triggered to go ETHOAM down when the near- or far-end frame loss ratio based on a test instance ID exceeds a specified threshold.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

loss-measure single-ended-synthetic { **local-ratio-threshold** | **remote-ratio-threshold** } **test-id** *test-id* **trigger if-down**

undo loss-measure single-ended-synthetic { **local-ratio-threshold** | **remote-ratio-threshold** } **test-id** *test-id* **trigger if-down**

Parameters

Parameter	Description	Value
local-ratio-threshold	Indicates that an interface is triggered to go ETHOAM down when the near-end frame loss ratio exceeds a specified threshold.	-
remote-ratio-threshold	Indicates that an interface is triggered to go ETHOAM down when the far-end frame loss ratio exceeds a specified threshold.	-
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no service is bound to the MA, the interface where the MEP resides is an Eth-Trunk interface's primary member interface. To ensure the quality of the primary link, run the **loss-measure single-ended-synthetic trigger if-down** command on the interface where the MEP resides. If the near- or far-end frame loss ratio based on a test instance ID exceeds the threshold configured using the **loss-measure single-ended-synthetic local-ratio-threshold test-id** or **loss-measure single-ended-synthetic remote-ratio-threshold test-id** command, the primary link has poor quality. In this case, the interface is triggered to go ETHOAM down, triggering a primary/secondary Eth-Trunk link switchover.

Prerequisites

A test instance has been created using the **test-id** command in the MA view.

Example

Trigger the Eth-Trunk member interface GE 0/0/1 to go ETHOAM down when the near-end frame loss ratio based on a test instance ID of 2 exceeds a specified threshold.

```
<HUAWEI> system-view
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
```

```
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep mep-id 8 interface gigabitethernet 0/0/1 outward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 9
[HUAWEI-md-md1-ma-ma1] test-id 2 mep 8 remote-mep 9
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] eth-trunk 1
[HUAWEI-GigabitEthernet0/0/1] loss-measure single-ended-synthetic local-ratio-threshold test-id 2
trigger if-down
```

12.9.38 ping mac multicast

Function

The **ping mac multicast** command configures multicast MAC ping in the current MA.

Format

ping mac multicast mep *mep-id* [**-c** *count* | **-p** *priority-value* | **-t** *timeout*] *

Parameters

Parameter	Description	Value
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer ranging from 1 to 8191.
-c *count*	Specifies the number of multicast Loopback Messages (LBMs) to be sent.	The value is an integer ranging from 1 to 4294967295. The default value is 3.
-p *priority-value*	Specifies the priority of the multicast LBM.	The value is an integer ranging from 0 to 7. The default value is the same as the 802.1p priority of the 802.1ag packets which is specified in MA view (**packet-priority**).
-t *timeout*	Specifies the timeout period for waiting for a Loopback Reply (LBR).	The value is an integer that ranges from 1 to 65535, in milliseconds. By default, the value is 5000 milliseconds.

Views

MA view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The destination MAC address of multicast MAC ping is a multicast MAC address. Multicast MAC ping provides two functions, that is, acknowledging faults and discovering RMEPs.

- Acknowledging faults: Multicast MAC ping provides the fault acknowledgement function similar to that provided by 802.1ag MAC ping. In a multicast MAC ping test, test packets are sent to test whether the path from the local device to the destination device is reachable. Multicast MAC ping can acknowledge the faults of links between multiple MEPs once.
- Discovering RMEPs: All RMEPs in the MA can be discovered.

  For example, there are three MEPs in an MA: MEP1, MEP2, and MEP3. After multicast MAC ping is configured on MEP1, MEP1 sends multicast LBMs. After MEP2 and MEP3 receive the LBM, they reply with an LBR. The LBR carries the MAC address of MEP2 or MEP3, MEP ID, and delay. Before configuring the **remote-mep** command on MEP1, you can configure multicast MAC ping to detect all RMEPs in an MA.

Prerequisites

A MEP has been created using the **mep mep-id** command.

Precautions

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007. Before using the **ping mac multicast** command, you must use the **cfm version** command to set the Ethernet CFM version to IEEE Standard 802.1ag-2007.

Example

Create an MD named **md1**, create an MA named **ma1** in the MD, and configure multicast MAC ping in **ma1**.

```
<HUAWEI> system-view
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] mep mep-id 1 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] ping mac multicast mep 1 -p 6 –c 1 –t 3
Reply from 00e0-fc00-0204 mep id 10: time = 9ms
Reply from 00e0-fc00-0269 mep id 11: time = 11ms
Packets: Sent = 1, Received = 2
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 12-78 Description of the **ping mac multicast** command output

Item	Description
Reply from	MAC address of the RMEP.
mep id	MEP ID.
time	Delay, in millisecond.

Item	Description
Sent	Number of sent multicast LBMs.
Received	Number of received LBRs.
Minimum	Minimum delay, in millisecond.
Maximum	Maximum delay, in millisecond.
Average	Average delay, in millisecond.

12.9.39 reset y1731 statistic-type

Function

The **reset y1731 statistic-type** command clears statistics collected through Y. 1731.

Format

reset y1731 statistic-type { **oneway-delay** | **twoway-delay** } **md** *md-name* **ma** *ma-name*

reset y1731 statistic-type { **single-loss** | **dual-loss**} **md** *md-name* **ma** *ma-name* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

reset y1731 statistic-type twoway-delay test-id *test-id* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

reset y1731 statistic-type single-synthetic-loss test-id *test-id* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

reset y1731 statistic-type single-loss test-id *test-id* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

Parameters

Parameter	Description	Value
oneway-delay	Clears statistics about one-way frame delay measurement.	-
twoway-delay	Clears statistics about two-way frame delay measurement.	-

Parameter	Description	Value
single-loss	Clears statistics about single-ended frame loss measurement.	-
dual-loss	Clears statistics about dual-ended frame loss measurement.	-
md *md-name*	Clears statistics about a specified MD.	The MD must exist.
ma *ma-name*	Clears statistics about a specified MA.	The MA must exist.
test-id *test-id*	Clears statistics about a specified test instance.	The test instance ID must exist.
single-synthetic-loss	Clears single-ended SLM statistics.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain Y.1731 statistics within a specified period of time, run the **reset y1731 statistic-type** command to delete existing Y.1731 statistics, and then run the **display y1731 statistic-type** command after a period of time.

Precautions

After the **reset y1731 statistic-type** command is executed, statistics are cleared and cannot be restored. Exercise caution when you run the command.

Example

Clear statistics about the one-way frame delay.

```
<HUAWEI> reset y1731 statistic-type oneway-delay md mdname ma maname
```

12.9.40 test-id

Function

The **test-id** command creates a test instance for Y.1731 statistics collection.

The **undo test-id** command deletes a test instance.

By default, no test instance is created in an MA for Y.1731 statistics collection.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

test-id *test-id* **mep** *mep-id* { **remote-mep** *mep-id* } [**8021p** *8021p-value*] [**description** *description*]

undo test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer ranging from 1 to 4294967295.
mep *mep-id*	Specifies the MEP ID.	The value is an integer that ranges from 1 to 8191.
remote-mep *mep-id*	Specifies the RMEP ID.	The value is an integer that ranges from 1 to 8191.
8021p *8021p-value*	Specifies a priority value for packets.	The value is an integer that ranges from 0 to 7.
description *description*	Specifies the description of a test instance.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement single-ended SLM, run the **test-id** command to create a test instance.

During two-way frame delay measurement in point-to-multipoint scenarios, you need to run this command to configure a test instance.

During two-way frame delay measurement, if the size or priority of outgoing DMMs needs to be specified or there is the high requirement on the detection accuracy, you can run this command to configure a test instance.

Prerequisites

- A MEP has been created using the **mep mep-id** command in the MA view.
- An RMEP has been created using the **remote-mep** command in the MA view.

Precautions

To configure a test instance, run the **set service-mode** command in the system view to configure the device to work in enhanced (S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S is enhanced-oam) mode before enabling CFM globally.

IEEE 802.1ag has two versions: IEEE 802.1ag Draft 7 and IEEE Standard 802.1ag-2007. This command can be used only on the device running IEEE Standard 802.1ag-2007. Before using the **test-id** command, you must use the **cfm version** command to set the Ethernet CFM version to IEEE Standard 802.1ag-2007.

When you run this command in the same MA view to configure multiple test instances, the RMEPs of the local MEP must be different switches.

Example

Configure test instance 200, and specify the MEP ID as 8 and RMEP ID as 9.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] set service-mode enhanced
Warning: This command will effect forward performance. Continue? [Y/N]:y
[HUAWEI] cfm enable
[HUAWEI] cfm md md1
[HUAWEI-md-md1] ma ma1
[HUAWEI-md-md1-ma-ma1] map vlan 100
[HUAWEI-md-md1-ma-ma1] mep mep-id 8 interface gigabitethernet 0/0/1 inward
[HUAWEI-md-md1-ma-ma1] remote-mep mep-id 9
[HUAWEI-md-md1-ma-ma1] test-id 200 mep 8 remote-mep 9
```

13 User Access and Authentication Commands

13.1 AAA Configuration Commands

13.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.1.2 aaa

Function

The **aaa** command displays the AAA view.

Format

aaa

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Using the **aaa** command in the system view, you can enter the AAA view and perform the following security configurations for access users:

- Creating users
- Configuring user levels
- Creating an authentication scheme
- Creating an authorization scheme
- Creating a domain

Example

Access the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa]
```

13.1.3 aaa abnormal-offline-record

Function

The **aaa abnormal-offline-record** command enables the device to record users' abnormal logout information.

The **undo aaa abnormal-offline-record** command disables the device from recording users' abnormal logout information.

By default, the device records users' abnormal logout information.

Format

aaa abnormal-offline-record

undo aaa abnormal-offline-record

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If users abnormally log out, run **aaa abnormal-offline-record** command to enable the record function for fault locating.

After the **undo aaa abnormal-offline-record** command is run, no abnormal logout information is recorded unless the **aaa abnormal-offline-record** command is run.

Example

Enable the device to record users' abnormal logout information.

```
<HUAWEI> system-view
[HUAWEI] aaa abnormal-offline-record
```

Disable the device from recording users' abnormal logout information.

```
<HUAWEI> system-view
[HUAWEI] undo aaa abnormal-offline-record
```

13.1.4 aaa offline-record

Function

The **aaa offline-record** command enables the device to record users' normal logout information.

The **undo aaa offline-record** command disables the device from recording users' normal logout information.

By default, the device is enabled to record user normal logout information.

Format

aaa offline-record

undo aaa offline-record

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If users fail to get online, run **aaa offline-record** command to enable the record function for fault locating.

After the **undo aaa offline-record** command is run, no logout information is recorded unless the **aaa offline-record** command is run.

Example

Enable the device to record users' normal logout information.

```
<HUAWEI> system-view
[HUAWEI] aaa offline-record
```

Disable the device from recording users' normal logout information.

```
<HUAWEI> system-view
[HUAWEI] undo aaa offline-record
```

13.1.5 aaa online-fail-record

Function

The **aaa online-fail-record** command enables the device to record users' online failures.

The **undo aaa online-fail-record** command disables the device from recording users' online failures.

By default, the device records users' online failures.

Format

aaa online-fail-record

undo aaa online-fail-record

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you want to query the login failure records to find out unauthorized users, run the **aaa online-fail-record** command to enable the device to record users' online failures.

After the **undo aaa online-fail-record** command is run, no online failure is recorded unless the **aaa online-fail-record** command is run.

Example

Enable the device to record users' online failures.

```
<HUAWEI> system-view
[HUAWEI] aaa online-fail-record
```

Disable the device from recording users' online failures.

```
<HUAWEI> system-view
[HUAWEI] undo aaa online-fail-record
```

13.1.6 aaa-authen-bypass

Function

The **aaa-authen-bypass** command sets the bypass authentication timeout interval.

The **undo aaa-authen-bypass** command cancels the bypass authentication timeout interval.

By default, no bypass authentication timeout interval is set.

Format

aaa-authen-bypass enable time *time-value*

undo aaa-authen-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote bypass authentication.	-
time *time-value*	Specifies the bypass authentication timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast authentication response. When a user in a user domain where multiple authentication modes (for example, RADIUS authentication and local authentication) are configured, bypass authentication is enabled, and the bypass authentication timeout interval is configured, the user will be authenticated using the local authentication mode and the bypass authentication timer is enabled simultaneously if the RADIUS server does not respond to the authentication request. When other users in the same domain are authenticated during the configured bypass authentication timeout interval, the users are directly authenticated using the local authentication mode, so that the users can be authenticated without waiting until the RADIUS server responds to their authentication requests, accelerating the authentication response.

Precautions

When only one authentication mode is configured in a user domain and the bypass authentication timer is enabled, other users in the same domain are directly considered to fail the authentication during the bypass authentication timeout interval.

Example

Set the bypass authentication timeout interval to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa-authen-bypass enable time 3
```

13.1.7 aaa-author-bypass

Function

The **aaa-author-bypass** command sets the bypass authorization timeout interval.

The **undo aaa-author-bypass** command cancels the bypass authorization timeout interval.

By default, no bypass authorization timeout interval is set.

Format

aaa-author-bypass enable time *time-value*

undo aaa-author-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote bypass authorization.	-
time *time-value*	Specifies the bypass authorization timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast authorization response. When a user in a user domain where multiple authorization modes (for example, HWTACACS authorization and local authorization) are configured, bypass authorization is enabled, and the bypass authorization timeout interval is configured, the user will be authorized using the local authorization mode and the bypass authorization timer is enabled simultaneously if the HWTACACS server does not respond to the authorization request. When other users in the same domain are authorized during the configured bypass authorization timeout interval, the users are directly authorized using the local authorization mode, so that the users can be authorized without waiting until the HWTACACS server responds to their authorization requests, accelerating the authorization response.

Precautions

When only one authorization mode is configured in a user domain and the bypass authorization timer is enabled, other users in the same domain are directly considered to fail the authorization during the bypass authorization timeout interval.

Example

Set the bypass authorization timeout interval to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa-author-bypass enable time 3
```

13.1.8 aaa-author-cmd-bypass

Function

The **aaa-author-cmd-bypass** command sets the command-line bypass authorization timeout interval.

The **undo aaa-author-cmd-bypass** command cancels the command-line bypass authorization timeout interval.

By default, no command-line bypass authorization timeout interval is set.

Format

aaa-author-cmd-bypass enable time *time-value*

undo aaa-author-cmd-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote command-line bypass authorization.	-
time *time-value*	Specifies the command-line bypass authorization timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast command-line authorization response. When a user in a user domain where multiple command-line authorization modes (for example, HWTACACS authorization and local authorization) are configured, command-line bypass authorization is enabled, and the command-line bypass authorization timeout interval is configured, the user will be authorized using the local authorization mode and the command-line bypass authorization timer is enabled simultaneously if the HWTACACS server does not respond to the command-line authorization request. When other users in the same domain are authorized during the configured command-line bypass authorization timeout interval, the users are directly authorized using the local authorization mode, so that the users can be authorized without waiting until the

HWTACACS server responds to their authorization requests, accelerating the authorization response.

Precautions

When only one command-line authorization mode is configured in a user domain and the command-line bypass authorization timer is enabled, other users in the same domain are directly considered to fail the command-line authorization during the command-line bypass authorization timeout interval.

Example

Set the command-line bypass authorization timeout interval to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa-author-cmd-bypass enable time 3
```

13.1.9 aaa-author session-timeout invalid-value enable

Function

The **aaa-author session-timeout invalid-value enable** command prevents a device from disconnecting or reauthenticating users when the RADIUS server delivers session-timeout with value 0.

The **undo aaa-author session-timeout invalid-value enable** command restores the default setting.

By default, when the RADIUS server delivers session-timeout with value 0, this attribute does not take effect.

Format

aaa-author session-timeout invalid-value enable

undo aaa-author session-timeout invalid-value enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

When the RADIUS server delivers session-timeout with value 0:

- If the **aaa-author session-timeout invalid-value enable** command is not configured, the session-timeout attribute delivered by the server does not take effect and the period for disconnecting or reauthenticating users depends on the device configuration.

- If the **aaa-author session-timeout invalid-value enable** command is configured, the session-timeout attribute delivered by the server takes effect and the device does not disconnect or reauthenticate users.

You can run the **dot1x timer reauthenticate-period** *reauthenticate-period-value* or **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command to configure the period for disconnecting or reauthenticating users on the device.

Example

Prevent the device from disconnecting or reauthenticating users when the RADIUS server delivers session-timeout with value 0.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] aaa-author session-timeout invalid-value enable
```

13.1.10 aaa-quiet administrator except-list

Function

The **aaa-quiet administrator except-list** command configures a user to access the network using a specified IP address when the user account is locked.

The **undo aaa-quiet administrator except-list** command restores the default setting.

By default, a user cannot access the network when the account is locked.

Format

aaa-quiet administrator except-list { *ipv4-address* | *ipv6-address* } &<1-32>

undo aaa-quiet administrator except-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address. A user can access the network using this IPv4 address when the user account is locked.	The value must be a valid unicast address in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address. A user can access the network using this IPv6 address when the user account is locked.	The total length of the value is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format of X:X:X:X:X:X:X:X.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In AAA view, after the function of locking the account of an AAA local authentication user or AAA remote authentication user is configured using the **local-aaa-user wrong-password** or **administrator remote authen-fail** command, if a user consecutively enters an incorrect password and the number of times that the user enters an incorrect password reaches the allowed maximum number of times, the user account is locked and the user cannot access the network when the account is locked. To facilitate maintenance and management, you can run the **aaa-quiet administrator except-list** command to configure the user to access the network using a specified IP address when the user account is locked.

Precautions

- This function takes effect only for the administrators.
- A maximum of 64 IPv4 and IPv6 addresses can be configured.

Example

Configure a user to access the network using the specified IP address 10.1.1.1 when the user account is locked.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] aaa-quiet administrator except-list 10.1.1.1
```

13.1.11 access-limit user-name max-num

Function

The **access-limit user-name max-num** command configures the maximum number of users who are allowed to access the network using the same user name.

The **undo access-limit user-name max-num** command restores the default setting.

By default, the number of users who are allowed to access the network using the same user name is not limited, and is determined by the maximum number of access users supported by the device.

Format

access-limit user-name max-num *number*

undo access-limit user-name max-num

Parameters

Parameter	Description	Value
number	Specifies the maximum number of users who are allowed to access the network using the same user name.	The value is an integer and is determined by the maximum number of access users supported by the device.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

By default, the number of users who are allowed to access the network using the same user name is not limited. To limit the number of users who are allowed to access the network using a user name, run the **access-limit user-name max-num** command. For example, the bandwidth share mode is configured for all terminal users in a small office network access scenario. To facilitate maintenance, the server delivers the same user name to replace the user names entered by terminal users. The number of access users needs to be limited based on the user name to ensure the network access experience of all terminal users.

For RADIUS authentication users, configurations for limiting the number of access users based on the user name are carried in the HW-UserName-Access-Limit (26-18) attribute.

NOTE

Only users who are successfully authenticated support the configurations for limiting the number of access users based on the same user name, and pre-connection users do not support such configurations.

This command does not take effect in inter-AC roaming scenarios.

Example

In the service scheme **s1**, set the maximum number of users who are allowed to access the network using the same user name to 15.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] access-limit user-name max-num 15
```

13.1.12 accounting dual-stack separate

Function

The **accounting dual-stack separate** command enables separate statistics collection or separate rate limiting of IPv4 and IPv6 user traffic.

The **undo accounting dual-stack separate** command disables separate statistics collection or separate rate limiting of IPv4 and IPv6 user traffic.

By default, the device does not distinguish between IPv4 and IPv6 user traffic when collecting traffic statistics or rate limiting IPv4 and IPv6 user traffic.

NOTE

This command is supported only on the following switch models:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI

Format

accounting dual-stack separate

undo accounting dual-stack separate

Parameters

None

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect statistics about IPv4 and IPv6 user traffic separately or perform accounting for IPv4 and IPv6 users separately based on traffic, run the **statistic enable (AAA domain view)** command to enable traffic statistics collection, and then run the **accounting dual-stack separate** command to enable separate traffic statistics collection for IPv4 and IPv6 users.

If you want to separately limit the rate of IPv4 and IPv6 users based on traffic, authorize CAR to the users, and then run the **accounting dual-stack separate** command to enable separate rate limiting for IPv4 and IPv6 users.

Precautions

You are advised to configure this function before users go online. If this function is configured after users go online, separate traffic statistic collection or rate limiting may be inaccurate. You are advised to collect traffic statistics or limit the rate again after users go offline.

Example

Enable separate statistics collection or separate rate limiting of IPv4 and IPv6 user traffic.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain example
[HUAWEI-aaa-domain-example] accounting dual-stack separate
Warning: This operation may cause online users' traffic statistics inaccurate, Re-online is recommended
after this operation, continue?[Y/N]y
```

13.1.13 accounting interim-fail

Function

The **accounting interim-fail** command sets the maximum number of real-time accounting failures and configures a policy used after the number of real-time accounting failures exceeds the maximum.

The **undo accounting interim-fail** command restores the default maximum number of real-time accounting failures and the default policy.

By default, the maximum number of real-time accounting failures is 3 and the device keeps users online after the number of real-time accounting failures exceeds the maximum.

Format

accounting interim-fail [**max-times** *times*] { **offline** | **online** }

undo accounting interim-fail

Parameters

Parameter	Description	Value
max-times *times*	Specifies the maximum number of real-time accounting failures. If the maximum number of real-time accounting failures is reached and the next accounting request still has no response, the device considers that accounting fails and takes a policy for users.	The value is an integer that ranges from 1 to 255. The default value is 3.
offline	Disconnects users if real-time accounting fails.	-
online	Keeps users online if real-time accounting fails.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the real-time accounting function takes effect, the device sends real-time accounting requests to an accounting server, and the accounting server responds to the accounting requests. If the network is unstable, for example, a jitter occurs, the device may not receive response packets. As a result, accounting is interrupted for a short period of time. To reduce or prevent accounting interruption, run the **accounting interim-fail** command to set the maximum number of real-time accounting failures. The device considers that real-time accounting fails only after the number of consecutive real-time accounting failures exceeds the maximum.

Choose one of the following policies to be applied after the maximum number of real-time accounting failures is reached:

- **online**: To prevent users from being affected by network faults, use the **online** policy to allow paid users to go online.
- **offline**: To stop providing services when accounting fails, use the **offline** policy to force paid users to go offline.

Prerequisites

The real-time accounting function has been enabled by using the **accounting realtime** command.

Precautions

The **accounting interim-fail** command does not take effect for online users, but takes effect for the users who go online after the command is executed.

Example

In the accounting scheme **scheme1**, set the maximum number of real-time accounting failures to 5 and use the **offline** policy.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting realtime 3
[HUAWEI-aaa-accounting-scheme1] accounting interim-fail max-times 5 offline
```

13.1.14 accounting realtime

Function

The **accounting realtime** command enables the real-time accounting function and sets the interval for real-time accounting in an accounting scheme.

The **undo accounting realtime** command disables the real-time accounting function.

By default, the device performs accounting based on user online duration, the real-time accounting function is disabled.

Format

accounting realtime *interval*

undo accounting realtime

Parameters

Parameter	Description	Value
interval	Specifies the interval for real-time accounting.	The value is an integer that ranges from 0 to 65535, in minutes. When the value is set to 0, real-time accounting is disabled. The default value is 0.

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the users who are charged based on online duration. If a user goes offline unexpectedly, the accounting server cannot receive the accounting-stop packet, so it keeps charging the user while they are not receiving a service. To solve the problem, configure the real-time accounting function on the device. After the real-time accounting function is configured, the device periodically sends real-time accounting packets to the accounting server. After receiving the real-time accounting packets, the accounting server charges the user. If the device detects that the user goes offline, it stops sending real-time accounting packets and the accounting server stops accounting. The result of real-time accounting is precise.

Precautions

- When the accounting interval is set using both the **accounting realtime** command and the Acct-Interim-Interval attribute, if the Acct-Interim-Interval value range is 60-3932100, the interval set by Acct-Interim-Interval has a higher priority. Otherwise, the interval set by the **accounting realtime** command takes effect.
- If an accounting scheme is applied to a domain, the **accounting realtime** command does not affect online users, but only takes effect for the users who go online after the command is executed.
- If *interval* is set to 0 and the IP address of the client is changed, the device still sends a real-time accounting packet carrying the changed IP address information to the RADIUS server.
- A short interval for real-time accounting requires high performance of the device and accounting server. If there are more than 1000 users, setting a long interval for real-time accounting is recommended. The following table lists the suggested real-time accounting intervals for different user quantities.

Table 13-1 Real-time accounting interval for different user quantities

User Quantity	Interval for Real-Time Accounting (Minutes)
1-99	3
100-499	6
500-999	12
≥ 1000	≥ 15

Example

In the accounting scheme **scheme1**, enable the real-time accounting function and set the interval for real-time accounting to 6 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting realtime 6
```

13.1.15 accounting start-fail

Function

The **accounting start-fail** command configures a policy for accounting-start failures.

The **undo accounting start-fail** command restores the default policy for accounting-start failures.

By default, users cannot go online if accounting-start fails. That is, the **offline** policy is used.

Format

accounting start-fail { **offline** | **online** }

undo accounting start-fail

Parameters

Parameter	Description	Value
offline	Rejects users' online requests if accounting-start fails.	-
online	Allows users to go online if accounting-start fails.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user goes online after an accounting scheme is applied, the device sends an accounting-start packet to an accounting server. When the network is working properly, the accounting server responds to the accounting-start packet. If a fault occurs on the network, the device may not receive the response packet from the accounting server. As a result, accounting fails. The device provides the following policies for accounting failures:

- **online**: To prevent users from being affected by network faults, use the **online** policy to allow paid users to go online.
- **offline**: To stop providing services when accounting fails, use the **offline** policy to force paid users to go offline.

Precautions

The command takes effect only when the accounting mode configured using the **accounting-mode** command is HWTACACS or RADIUS.

Example

In the accounting scheme **scheme1**, use the **online** policy for accounting-start failures.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting start-fail online
```

13.1.16 accounting-mode

Function

The **accounting-mode** command configures an accounting mode in an accounting scheme.

The **undo accounting-mode** command restores the default accounting mode in an accounting scheme.

By default, the accounting mode is **none**.

Format

accounting-mode { **hwtacacs** | **none** | **radius** | **haca** }

undo accounting-mode

Parameters

Parameter	Description	Value
hwtacacs	Indicates that accounting is performed by an HWTACACS server.	-
none	Indicates non-accounting.	-
radius	Indicates that accounting is performed by a RADIUS server.	-

Parameter	Description	Value
haca	Indicates that accounting is performed by an HACA server. **NOTE** Only the following switch models support HACA: S200, S1730S-S1 S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H and S6720S-S	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Enterprises or carriers need to generate revenue by charging users who are accessing the Internet.

When a user goes online, accounting starts after the user is authenticated and authorized. When the user goes offline, accounting stops. The client sends the account packet containing the user's online duration to the accounting server.

To charge users, set the accounting mode to RADIUS or HWTACACS. Generally, the accounting mode is consistent with the authentication mode. If you do not need to charge users, set the accounting mode to none.

Precautions

The device does not support local accounting. When the authentication scheme configured using the **authentication-mode** command defines local authentication, you need to run the **accounting-mode none** command to configure non-accounting or run the **accounting start-fail** command to configure a policy for accounting-start failures.

Follow-up Procedure

Apply the accounting scheme to a domain to enable the device to charge the users in the domain using the **domain** command in the AAA view.

Example

Set the accounting mode to RADIUS in the accounting scheme **scheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1] accounting-mode radius
```

13.1.17 accounting-scheme (AAA domain view)

Function

The **accounting-scheme** command applies an accounting scheme to a domain.

The **undo accounting-scheme** command restores the default accounting scheme of a domain.

By default, the accounting scheme named **default** is applied to a domain. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Format

accounting-scheme *accounting-scheme-name*

undo accounting-scheme

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The accounting scheme must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To charge users in a domain, create an accounting scheme and perform configurations in the accounting scheme, for example, set the accounting mode and policy for accounting-start failures. Run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to the domain.

Prerequisites

An accounting scheme has been created and configured using the **accounting-scheme** command. For example, the accounting mode and policy for accounting-start failures have been configured.

Example

Apply the accounting scheme **account1** to the domain **isp1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme account1
[HUAWEI-aaa-accounting-account1] quit
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] accounting-scheme account1
```

Restore the default accounting scheme of the domain **isp2**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain isp2
[HUAWEI-aaa-domain-isp2] undo accounting-scheme
```

13.1.18 accounting-scheme (AAA view)

Function

The **accounting-scheme** command creates an accounting scheme and displays the accounting scheme view.

The **undo accounting-scheme** command deletes an accounting scheme.

By default, there is an accounting scheme named **default** in the system. This default accounting scheme can be modified but cannot be deleted. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Format

accounting-scheme *accounting-scheme-name*

undo accounting-scheme *accounting-scheme-name*

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To charge users in a domain, create and configure an accounting scheme, for example, the accounting mode and policy for accounting-start failures. Run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to the domain.

Follow-up Procedure

After an accounting scheme is created:

- Run the **accounting interim-fail** command to set the maximum number of real-time accounting failures and configure a policy used after a real-time accounting failure.
- Run the **accounting realtime** command to enable the real-time accounting function and set the interval for real-time accounting in an accounting scheme.
- Run the **accounting start-fail** command to configure a policy for accounting-start failures.
- Run the **accounting-mode** command to configure an accounting mode in an accounting scheme.

After an accounting scheme is configured, run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to a domain.

Precautions

If the configured accounting scheme does not exist, the **accounting-scheme** command in the AAA view creates an accounting scheme and displays the accounting scheme view. If the configured accounting scheme already exists, the **accounting-scheme** command in the AAA view displays the accounting scheme view directly.

To delete an accounting scheme applied to a domain, run the **undo accounting-scheme (AAA domain view)** command.

Example

Create an accounting scheme named **scheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] accounting-scheme scheme1
[HUAWEI-aaa-accounting-scheme1]
```

Enter the default accounting scheme view.

```
<HUAWEI> system-view
[HUAWEI] aaa
```

```
[HUAWEI-aaa] accounting-scheme default
[HUAWEI-aaa-accounting-default]
```

13.1.19 access-user remote authen-fail

Function

The **access-user remote authen-fail** command enables the account locking function for access users who fail remote authentication.

The **undo access-user remote authen-fail** command disables the account locking function for access users who fail remote authentication.

By default, the account locking function is disabled for access users who fail remote authentication.

Format

access-user remote authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo access-user remote authen-fail

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the authentication retry interval after a remote authentication failure.	The value is an integer in the range from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the maximum number of consecutive authentication failures.	The value is an integer in the range from 3 to 65535.
block-time *block-time*	Specifies the account locking period.	The value is an integer in the range from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure account and password security, enable the account locking function for access users who fail remote authentication. If a user reaches the incorrect account or password attempt limit within the specified authentication retry period, the user is locked and will be automatically unlocked after a certain period.

Precautions

- This command takes effect only for remotely authenticated access users.
- When an active/standby switchover is performed, the originally locked account is automatically unlocked.
- After you run the **undo access-user remote authen-fail** command to disable the account locking function for access users who fail remote authentication, the locked account is automatically unlocked.
- If a remote authentication user does not reach the consecutive authentication attempt limit configured using the **access-user remote authen-fail** command, the user is not locked. If you run the **access-user remote authen-fail** command to change the consecutive authentication attempt limit to be less than the number of consecutive authentication failures, the user has one chance to be authenticated.

Example

Enable the account locking function for access users who fail remote authentication, and set the authentication retry interval to 5 minutes, maximum number of consecutive authentication failures to 3, and account locking period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] access-user remote authen-fail retry-interval 5 retry-time 3 block-time 5
```

13.1.20 administrator remote authen-fail

Function

The **administrator remote authen-fail** command enables the account locking function for administrators who fail remote authentication.

The **undo administrator remote authen-fail** command disables the account locking function for administrators who fail remote authentication.

By default, the account locking function is enabled for administrators who fail remote authentication, the authentication retry interval is 5 minutes, the maximum number of consecutive authentication failures is 30, and the account locking period is 5 minutes.

Format

administrator remote authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo administrator remote authen-fail

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the authentication retry interval after a remote authentication failure.	The value is an integer in the range from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the maximum number of consecutive authentication failures.	The value is an integer in the range from 3 to 65535.
block-time *block-time*	Specifies the account locking period.	The value is an integer in the range from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure account and password security of administrators, enable the account locking function for administrators who fail remote authentication. If an administrator enters incorrect account and password more than the maximum number of consecutive authentication failures within the given period, the account is locked. After a certain period, the account is unlocked.

Precautions

- This command takes effect only for remotely authenticated administrators.
- When an active/standby switchover is performed, the originally locked account is automatically unlocked.
- After you run the **undo administrator remote authen-fail** command to disable the account locking function for administrators that fail remote authentication, the locked account is automatically unlocked.
- If a remote authentication user does not reach the consecutive authentication attempt limit configured using the **administrator remote authen-fail** command, the user is not locked. If you run the **administrator remote authen-fail** command to change the consecutive authentication attempt limit to be less than the number of consecutive authentication failures, the user has one chance to be authenticated.

Example

Enable the account locking function for administrators who fail remote authentication, and set the authentication retry interval to 5 minutes, maximum number of consecutive authentication failures to 3, and account locking period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] administrator remote authen-fail retry-interval 5 retry-time 3 block-time 5
```

13.1.21 admin-user privilege level

Function

The **admin-user privilege level** command configures a user as an administrator to log in to the device and sets the user privilege level.

The **undo admin-user privilege level** command cancels the default user privilege level.

By default, the user privilege level is not specified.

Format

admin-user privilege level *level*

undo admin-user privilege level

Parameters

Parameter	Description	Value
level	Specifies a user privilege level. A larger value indicates a higher user privilege level. After logging in to the device, a user can run only the commands at the same or lower privilege levels.	The value is an integer that ranges from 0 to 15.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device provides hierarchical management of commands. A command has a privilege level, and a user can run only the commands at the same or lower privilege levels. By using the **admin-user privilege level** command to set the user privilege level, the device controls commands used by users.

By default, commands are classified into the following privilege levels:

- Level 0 (visit level): Commands at level 0 include diagnosis commands such as ping and tracert commands and commands that are used to access a remote device such as the STelnet client. Commands at level 0 cannot be used to save configuration files.
- Level 1 (monitoring level): Commands at level 1 are used for system maintenance, including display commands. Commands at level 1 cannot be used to save configuration files.
- Level 2 (configuration level): Commands at level 2 are used for service configuration, including routing commands and commands at each network layer to provide network services for users.
- Level 3 (management level): Commands at level 3 are used for basic operations of the system to support services, including file system, FTP, Trivial File Transfer Protocol (TFTP), configuration file switching commands, slave board control commands, user management commands, command level configuration commands, and debugging commands.

To manage users in a refined manner, upgrade command privilege levels to levels 0 to 15. You can run the **command-privilege level** command to upgrade command privilege levels in a batch. You can also run the **command-privilege level rearrange** command to increase privilege levels.

- If non-authentication is used, the administrator privilege level is specified using the **user privilege** command in the VTY interface view.
- If local authentication is used, the user privilege level of the administrator is the local user privilege level configured using the **local-user privilege level** command.
- If remote authentication is performed, the administrator privilege level can be set in the following ways, in descending order of priority:
  a. Using the user privilege level sent by an authentication server to the device after authentication has succeeded
  b. Running the **admin-user privilege level** command to set the administrator privilege level in a service scheme
  c. Running the **user privilege** command to set the user privilege level in VTY mode
- If both remote authentication and local authentication are configured and remote authentication is performed before local authentication, the administrator privilege level is that used in remote authentication. If local authentication is performed because the remote server does not respond, the administrator privilege level is the local user privilege level configured using the **local-user privilege level** command.

The device can update the configuration in a domain dynamically. After a service scheme is applied to a domain, you can directly modify the user privilege level in the service scheme but cannot unbind the service scheme from the domain. To delete the service scheme, run the **undo service-scheme (AAA domain view)** command.

Follow-up Procedure

Run the **display service-scheme** command to view the user privilege level in a service scheme.

Example

Configure a user as an administrator to log in to the device and set the administrator privilege level to 15.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] admin-user privilege level 15
```

13.1.22 assignment

Function

The **assignment** command configures the VLAN assignment algorithm in a VLAN pool.

The **undo assignment** command restores the default VLAN assignment algorithm in a VLAN pool.

By default, the VLAN assignment algorithm is **hash** in a VLAN pool.

Format

assignment { **even** | **hash** }

undo assignment

Parameters

Parameter	Description	Value
even	Sets the VLAN assignment algorithm to **even**.	-
hash	Sets the VLAN assignment algorithm to **hash**.	-

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When the VLAN assignment algorithm is set to **even**, service VLANs are assigned to users from the VLAN pool based on the order in which users go online. Address pools mapping the service VLANs evenly assign IP addresses to users. If a user goes online many times, it obtains different IP addresses.
- When the VLAN assignment algorithm is set to **hash**, VLANs are assigned to users from the VLAN pool based on the hash result of their MAC addresses. As long as the VLANs in the VLAN pool do not change, the users obtain fixed VLAN. A user is preferentially assigned the same IP address when going online at different times.

Precautions

For the **even** VLAN assignment algorithm, the aging time of IP addresses is set large on the DHCP server. A user is assigned different IP addresses when going online at different times. As a result, a user may occupy many IP addresses, which wastes IP addresses. Additionally, frequent IP address changes may lower user experience.

Configuration Impact

The VLAN assignment algorithm configuration affects only newly connected users, but not those that have been connected to the network.

Example

Set the VLAN assignment algorithm to **even** in the VLAN pool **test**.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment even
```

13.1.23 authentication-mode (authentication scheme view)

Function

The **authentication-mode** command configures an authentication mode for an authentication scheme.

The **undo authentication-mode** command restores the default authentication mode in an authentication scheme.

By default, local authentication is used. The names of local users are case-insensitive.

Format

authentication-mode { **hwtacacs** | [**local** | **local-case**] | **radius** | **haca** } * [**none**]

authentication-mode none

undo authentication-mode

NOTE

Only the following switch models support HACA:

S200, S1730S-S1

S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H and S6720S-S

Parameters

Parameter	Description	Value
hwtacacs	Authenticates users using an HWTACACS server. To perform HWTACACS authentication, configure an HWTACACS authentication server in an HWTACACS server template.	-
local	Authenticates users locally and sets local user names to case-insensitive.	-
local-case	Authenticates users locally and sets local user names to case-sensitive.	-
radius	Authenticates users using a RADIUS server. To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template.	-
haca	Authenticates users using a Huawei Agile Cloud Authentication (HACA) server.	-
none	Indicates non-authentication. That is, users access the network without being authenticated.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users, configure an authentication mode in an authentication scheme.

If multiple authentication modes are configured in an authentication scheme, the authentication modes are used according to the sequence in which they were configured.

- In the sequence of local authentication followed by remote authentication:

  If a login account is not created locally but exists on the remote server, the authentication mode is changed from local authentication to remote authentication.

  If a login account is created locally and on the remote server, and local authentication fails because the password is incorrect, remote authentication will not be performed.

- In the sequence of remote authentication followed by local authentication:

  If a login account is created locally but not on the remote server, remote authentication fails and local authentication will not be performed.

  A user is authenticated using the local authentication mode only when the remote server is Down or does not respond to the user's authentication request.

  NOTE

  Normally, if the remote server is Down or does not respond, local authentication is used. If a large number of users need to go online through the device, the device may be unable to process responses from the server in a timely manner. As a result, the AAA module of the device cannot receive responses from the server until the protection timer expires. These users then cannot go online and cannot be authenticated using local authentication. In this case, reconnect these offline users to the device.

You can configure multiple authentication modes in an authentication scheme to reduce authentication failure possibilities.

- After the **authentication-mode radius local** command is used, the device cannot complete RADIUS authentication if it fails to connect to the RADIUS authentication server. In this case, the device starts local authentication.
- After the **authentication-mode local radius** command is used, if the entered user name exists on the device but the entered password is incorrect, the user fails the authentication; if the entered user name does not exist on the device, the user is redirected to the RADIUS authentication mode and is authenticated based on user information on the RADIUS server.

NOTE

- When both RADIUS authentication and non-authentication are configured, if the user fails the RADIUS authentication, non-authentication cannot be used. As a result, a user fails to log in.
- If you run the **authentication-mode** command to configure non-authentication and run the **authentication-mode (user interface view)** command to configure AAA authentication, the device does not allow administrators to log in from the user interface view.
- If none authentication is configured or none authentication is configured as the backup authentication mode, you need to run the **accounting start-fail online** or **accounting-mode none** command in the accounting scheme view to prevent users from going offline due to accounting failures.

Precautions

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. Therefore, to protect the device and improve network security, you are advised to enable authentication, allowing only authenticated users to access the device or network.

It is not recommended that HACA authentication be configured together with another authentication (except non-authentication). Otherwise, the two configured authentication modes cannot take effect simultaneously. For example, if the **authentication-mode haca radius** command is configured, users can log in after passing HACA authentication; if users fail HACA authentication, RADIUS authentication will not be performed on them.

Example

Configure the authentication scheme named **scheme1** to use RADIUS authentication.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme scheme1
[HUAWEI-aaa-authen-scheme1] authentication-mode radius
```

13.1.24 authentication-scheme (AAA domain view)

Function

The **authentication-scheme** command applies an authentication scheme to a domain.

The **undo authentication-scheme** command restores the default configuration of the authentication scheme in a domain.

By default, the authentication scheme named **radius** is applied to the **default** domain, the authentication scheme named **default** is applied to the **default_admin** domain, and the authentication scheme named **radius** is applied to other domains.

Format

authentication-scheme *scheme-name*

undo authentication-scheme

Parameters

Parameter	Description	Value
scheme-name	Specifies the name of an authentication scheme.	The value must be an existing authentication scheme name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users in a domain, run the **authentication-scheme (AAA domain view)** command to apply an authentication scheme to a domain.

Prerequisites

An authentication scheme has been created and configured with required parameters, for example, the authentication mode and authentication mode for upgrading user levels.

Example

Apply the authentication scheme named **scheme1** to a domain named **domain1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain domain1
[HUAWEI-aaa-domain-domain1] authentication-scheme scheme1
```

13.1.25 authentication-scheme (AAA view)

Function

The **authentication-scheme** command creates an authentication scheme and displays its view.

The **undo authentication-scheme** command deletes an authentication scheme.

By default, the default authentication scheme is used. This default authentication scheme can be modified but cannot be deleted. In the default authentication scheme:

- Local authentication is used.
- The **offline** policy is used for authentication failures.

By default, the system also provides the authentication scheme **radius**. The **radius** authentication scheme can be modified, but cannot be deleted. In the **radius** authentication scheme:

- RADIUS authentication is used.
- The **offline** policy is used for authentication failures.

Format

authentication-scheme *scheme-name*

undo authentication-scheme *scheme-name*

Parameters

Parameter	Description	Value
scheme-name	Specifies the name of an authentication scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users, run the **authentication-scheme** command to create an authentication scheme. Creating an authentication scheme is necessary before performing authentication-relevant configurations.

Follow-up Procedure

After an authentication scheme is created, run the **authentication-mode (authentication scheme view)** command to configure an authentication mode in an authentication scheme.

After an authentication scheme is configured, run the **authentication-scheme (AAA domain view)** command to apply the authentication scheme to a domain.

Precautions

If the configured authentication scheme does not exist, the **authentication-scheme** command creates an authentication scheme and displays the authentication scheme view. If the configured authentication scheme already exists, the **authentication-scheme** command directly displays the authentication scheme view.

To delete an authentication scheme applied to a domain, run the **undo authentication-scheme (AAA domain view)** command.

Example

Create an authentication scheme named **newscheme**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme newscheme
[HUAWEI-aaa-authen-newscheme]
```

Access the default authentication scheme view.

```
<HUAWEI> system-view
[HUAWEI] aaa
```

```
[HUAWEI-aaa] authentication-scheme default
[HUAWEI-aaa-authen-default]
```

13.1.26 authentication-super

Function

The **authentication-super** command configures an authentication mode for upgrading user levels in an authentication scheme.

The **undo authentication-super** command restores the default authentication mode for upgrading user levels in an authentication scheme.

By default, the **super** mode is used. That is, local authentication is used.

Format

authentication-super { **hwtacacs** | **radius** | **super** } * [**none**]

authentication-super none

undo authentication-super

Parameters

Parameter	Description	Value
hwtacacs	Uses HWTACACS authentication to upgrade user levels.	-
radius	Uses RADIUS authentication to upgrade user levels.	-
super	Uses local authentication to upgrade user levels.	-
none	Indicates that user levels can be upgraded without authentication.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If users in a domain need to upgrade their levels, the device requests the users to enter the password to authenticate the users. If AAA authentication has been configured using the **authentication-mode (user interface view)** command, run the **authentication-super** command to configure an authentication mode for upgrading user levels.

When you use the **super** command to switch a user level to a lower level or the same level, no authentication is required. When you use the **super** command to switch a user level to a higher level, authentication is required. The user can be granted rights only after being authenticated.

- If **super** is used and the local authentication is specified, run the **local-user** command in the AAA view to create a local user and set parameters for the local user.
- If **hwtacacs** is used and the HWTACACS authentication is specified, perform configurations relevant to HWTACACS authentication.
- If **radius** is used and the RADIUS authentication is specified, perform configurations relevant to RADIUS authentication.
- If **radius** is specified, the RADIUS authentication mode is used to upgrade the user level. The user name to be sent is $enab+user level. Ensure that the user has been configured on the server.
- If **none** is used, no authentication is required.

Precautions

If multiple authentication modes are configured in an authentication scheme, these authentication modes are used in the sequence in which they were configured. The device uses another authentication mode only when it does not receive any response in the current authentication. The device does not switch to another authentication mode if the user fails to pass one authentication mode.

Example

Set the authentication mode to HWTACACS authentication in the authentication scheme **scheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme scheme1
[HUAWEI-aaa-authen-scheme1] authentication-super hwtacacs
```

13.1.27 authentication-type radius chap access-type admin

Function

The **authentication-type radius chap access-type admin** command replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators.

The **undo authentication-type radius chap access-type admin** command restores PAP authentication when RADIUS authentication is performed on administrators.

By default, PAP authentication is used when RADIUS authentication is performed on administrators.

Format

authentication-type radius chap access-type admin [**ftp** | **ssh** | **telnet** | **terminal** | **http**] *

undo authentication-type radius chap access-type admin

Parameters

Parameter	Description	Value
ftp	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using FTP.	-
ssh	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using SSH.	-
telnet	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using Telnet.	-
terminal	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using a terminal.	-

Parameter	Description	Value
http	Replaces PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using a web management system.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

CHAP is ciphertext authentication protocol. During CHAP authentication, the NAS device sends the user name, encrypted password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user. CHAP is more secure and reliable than PAP.

If no parameter is specified when you run the **authentication-type radius chap access-type admin** command, the configuration takes effect on the administrators who access the device using FTP, SSH, Telnet, Terminal, and HTTP.

When the device is connected to the RADIUS server that supports CHAP authentication, this function needs to be configured.

Example

Replace PAP authentication with CHAP authentication when RADIUS authentication is performed on administrators who access the device using FTP.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme scheme1
[HUAWEI-aaa-authen-scheme1] authentication-type radius chap access-type admin ftp
```

13.1.28 authorization-cmd

Function

The **authorization-cmd** command configures command-specific authorization for an administrator of a specific level. After command-specific authorization is enabled and an administrator of a specific privilege level logs in to the device, the commands that the administrator enters can be executed only after being authorized by the HWTACACS server.

The **undo authorization-cmd** command disables command-specific authorization for an administrator of a specific privilege level.

By default, the command-specific authorization is disabled. That is, an administrator of any level can execute only commands of or below its privilege level after logging in to the device.

Format

authorization-cmd *privilege-level* **hwtacacs** [**local**] [**none**]

undo authorization-cmd *privilege-level*

Parameters

Parameter	Description	Value
privilege-level	Specified the administrator privilege level.	The value is an integer that ranges from 0 to 15.
hwtacacs	Indicates HWTACACS authorization.	-
local	Indicates local authorization.	-
none	Indicates that command line authorization is directly performed for a user if the HWTACACS server does not respond to the authorization request of the user.	-

Views

Authorization scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After being authorized, the users at a certain privilege level can run the commands of the same or lower privilege levels. Command line authorization can be configured to implement minimum user rights control. When command line authorization is enabled, each command entered by users can be executed only after being authorized. After command line authorization is enabled for users at a certain privilege level, the commands run by the users at that privilege level must be authorized by an HWTACACS server.

Precautions

- You are advised to configure local authorization as a backup of command line authorization. If command line authorization cannot be performed because of a failure on an HWTACACS server, the device starts local authorization.
- After the **authorization-cmd** command is executed, command line authorization does not take effect immediately. Command line authorization takes effect only when an authorization scheme containing command line authorization is applied to administrator view correctly.
- Commands whose privilege levels are higher than the administrator privilege level cannot be authorized and fail to be executed.
- When configuring the **authorization-cmd** *privilege-level* **hwtacacs local** command, you must create a local account. The device then performs authentication based on the local account configuration.

NOTICE

After an authorization scheme containing command line authorization is applied to administrator view, if you run the **undo authorization-cmd** command, an online administrator at a certain privilege level cannot run any commands except for the **quit** command. The administrator needs to log in again.

Example

Configure command line authorization for administrators at the privilege level 2.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme scheme1
[HUAWEI-aaa-author-scheme1] authorization-cmd 2 hwtacacs
```

13.1.29 authorization-info check-fail policy

Function

The **authorization-info check-fail policy** command determines whether the device allows users to go online after the authorization information check fails.

The **undo authorization-info check-fail policy** command restores the default configuration.

By default, the device allows users to go online after the authorization information check fails.

Format

authorization-info check-fail policy { **online** | **offline** }

undo authorization-info check-fail policy

Parameters

Parameter	Description	Value
online	Indicates that the device allows users to go online after the authorization information check fails.	-
offline	Indicates that the device prohibits users from going online after the authorization information check fails.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device supports user authorization through the ACL, UCL Group, User Group and VLAN delivered from the RADIUS server. If the ACL, UCL Group, User Group and VLAN delivered from the RADIUS server are not configured on the device, the authorization information check fails on the device.

You can use this command to configure the users to go online and the authorization information delivered by the RADIUS server does not take effect.

Example

Configure the device to allow users to go online after the authorization information check fails.

```
<HUAWEI> system-view
[HUAWEI] authorization-info check-fail policy online
```

13.1.30 authorization-mode

Function

The **authorization-mode** command configures an authorization mode for an authorization scheme.

The **undo authorization-mode** command restores the default authorization mode in an authorization scheme.

By default, local authorization is used. The names of local users are case-insensitive.

Format

authorization-mode { **hwtacacs** | **if-authenticated** | { **local** | **local-case** } } * [**none**]

authorization-mode none

undo authorization-mode

Parameters

Parameter	Description	Value
hwtacacs	Indicates that the user is authorized by an HWTACACS server.	-
if-authenticated	Indicates that only the user who succeeds in authentication is authorized. The configuration of if-authenticated authorization does not take effect in RADIUS authentication.	-
local	Authenticates users locally and sets local user names to case-insensitive.	-
local-case	Authenticates users locally and sets local user names to case-sensitive.	-
none	Indicates non-authorization.	-

Views

Authorization scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authorize users, configure an authorization mode in an authorization scheme.

You can configure multiple authorization modes in an authorization scheme to reduce the chance of authorization failures.

After the **authorization-mode hwtacacs local** command is used, if it fails to connect to the HWTACACS authentication server and HWTACACS authorization cannot be performed, the device starts local authorization.

Precautions

- If multiple authorization modes are used in an authorization scheme, the **if-authenticated** mode or **none** mode must be used as the last authorization mode.
- If the authorization mode is set to **if-authenticated** or **none**, the local authentication administrator does not inherit the level configured using the **local-user privilege level** command after login. The administrator first inherits the level configured using the **admin-user privilege level** command in the service scheme bound to the domain. If the level is not configured in the domain, the administrator inherits the level configured using the **user privilege** command in the VTY view.

  By default, users who log in to a device in the VTY view of the console interface are at level 15 and users who log in to a device in other VTY views are at level 0.
- If multiple authorization modes are configured in an authorization scheme, the authorization modes are used according to the sequence in which they were configured. The device uses another authorization mode only when it does not receive any response in the current authorization mode.

Example

Configure the authorization scheme named **scheme1** to apply HWTACACS authorization.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme scheme1
[HUAWEI-aaa-author-scheme1] authorization-mode hwtacacs
```

13.1.31 authorization-modify mode

Function

The **authorization-modify mode** command configures the update mode for user authorization information delivered by the authorization server.

The **undo authorization-modify mode** command restores the default update mode for user authorization information delivered by the authorization server.

By default, the update mode of user authorization information delivered by the authorization server is **overlay**. That is, the new user authorization information overwrites all existing user authorization information.

Format

authorization-modify mode { **modify** | **overlay** }

undo authorization-modify mode

Parameters

Parameter	Description	Value
modify	Indicates the **modify** mode.	-
overlay	Indicates the **overlay** mode.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

The authorization server can deliver all or part of user authorization information, such as the ACL rule and dynamic VLAN.

You can run the **authorization-modify mode** command to configure one of the following update modes for user authorization information delivered by the authorization server:

- **modify**: modification mode indicating that new user authorization information overwrites only existing user authorization information of the same type.
- **overlay**: overwriting mode indicating that new user authorization information overwrites all existing user authorization information.

If the authorization server has delivered ACL 3001 to a user, and the administrator needs to deliver new authorization information:

- In the **modify** mode, if the new authorization information is ACL 3002, the authorization information of the user is ACL 3002. If the new authorization information is VLAN 100, the authorization information of the user is ACL 3001 and VLAN 100.
- In the **overlay** mode, no matter whether the new authorization information is ACL 3002 or VLAN 100, the authorization information of the user is the new ACL or VLAN.

This command takes effect for only the authorization information delivered by the RADIUS server.

After a user group or service scheme is authorized to a user on the device and a certain attribute configured in the user group or service scheme is modified on the server, if other configured attributes need to be modified, the authorization information on the server must contain the previously modified attribute. Otherwise, the original attribute value in the user group or service scheme will be restored. For example, to modify an attribute in a user group:

1. The device authorizes the user group configured with the VLAN and ACL attributes to a user.
2. To modify the VLAN attribute, authorize the new VLAN attribute to the user through the RADIUS server.
3. To modify the ACL attribute after the VLAN attribute is modified, you must authorize the modified VLAN attribute and new ACL attribute through the RADIUS server. Otherwise, the original VLAN attribute in the user group will be restored.

NOTE

For user re-authentication:

- If the Session-Timeout attribute is delivered during RADIUS CoA authorization, the original re-authentication timer is deleted and the timer carried by the Session-Timeout attribute is started.
- If the Session-Timeout attribute is not delivered during RADIUS CoA authorization:
  - When the **modify** mode is used, the original re-authentication timer is not deleted; instead, the timer is suspended during user authorization and continues to take effect after the authorization completes.
  - When the **overlay** mode is used:

    If the original re-authentication timer is locally configured, the original re-authentication timer is not deleted; instead, the timer is suspended during user authorization and continues to take effect after the authorization completes.

    If the original timer is delivered by the server, the original timer is deleted and re-authentication is performed depending on whether the local re-authentication timer is configured on the device.

Example

Set the update mode of user authorization information delivered by the authorization server to **modify**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-modify mode modify
```

13.1.32 authorization-scheme (AAA domain view)

Function

The **authorization-scheme** command applies an authorization scheme to a domain.

The **undo authorization-scheme** command unbinds an authorization scheme from a domain.

By default, no authorization scheme is applied to a domain.

Format

authorization-scheme *authorization-scheme-name*

undo authorization-scheme

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The authorization scheme must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RADIUS integrates authentication and authorization; therefore, RADIUS authorization and authentication must be used together. HWTACACS separates authentication from authorization; therefore, you can configure another authorization type even if HWTACACS authentication, local authentication, or non-authentication is used.

To authorize users in a domain, run the **authorization-scheme (AAA domain view)** command.

Prerequisites

An authorization scheme has been created and configured with required parameters, for example, the authorization mode and command line authorization.

Example

Apply the authorization scheme **author1** to the domain **isp1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme author1
[HUAWEI-aaa-author-author1] quit
[HUAWEI-aaa] domain isp1
[HUAWEI-aaa-domain-isp1] authorization-scheme author1
```

13.1.33 authorization-scheme (AAA view)

Function

The **authorization-scheme** command creates an authorization scheme and enters the authorization scheme view, or directly enters an existing authorization scheme view.

The **undo authorization-scheme** command deletes an authorization scheme.

By default, the default authorization scheme is used. This default authorization scheme can be modified but cannot be deleted. In the default authorization scheme, local authorization is used and command line authorization is disabled.

Format

authorization-scheme *authorization-scheme-name*

undo authorization-scheme *authorization-scheme-name*

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RADIUS integrates authentication and authorization; therefore, RADIUS authorization and authentication must be used together. HWTACACS separates authentication from authorization; therefore, you can configure another authorization type even if HWTACACS authentication, local authentication, or non-authentication is used. You must run the **authorization-scheme** command to create an authorization scheme before performing authorization-relevant configurations, for example, setting the authorization mode and command line authorization function.

Follow-up Procedure

After an authorization scheme is created:

- Run the **authorization-mode** command to configure an authorization mode in an authorization scheme.
- Run the **authorization-cmd** command to configure command line authorization for users at a certain level.

After an authorization scheme is configured, run the **authorization-scheme (AAA domain view)** command to apply the authorization scheme to a domain.

Precautions

- If the configured authorization scheme does not exist, the **authorization-scheme (AAA view)** command creates an authorization scheme and displays the authorization scheme view.
- If the configured authorization scheme already exists, the **authorization-scheme (AAA view)** command directly displays the authorization scheme view.

To delete the authorization scheme applied to a domain, run the **undo authorization-scheme (AAA domain view)** command.

Example

Create an authorization scheme named **scheme0**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme scheme0
[HUAWEI-aaa-author-scheme0]
```

Enter the default authorization scheme view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authorization-scheme default
[HUAWEI-aaa-author-default]
```

13.1.34 cmd recording-scheme

Function

The **cmd recording-scheme** command applies a policy in a recording scheme to record the commands executed on the device.

The **undo cmd recording-scheme** command deletes a policy from a recording scheme.

By default, the commands that are used on the device are not recorded.

Format

cmd recording-scheme *recording-scheme-name*

undo cmd recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During the device configuration, incorrect operations may result in network faults. After the **cmd recording-scheme** command is executed, you can view records of the commands executed on the device to locate the network faults.

Prerequisites

A recording scheme has been created by using the **recording-scheme** command and a recording mode has been configured by using the **recording-mode hwtacacs** command.

Example

Configure a policy in the recording scheme **scheme0** to record the commands executed on the device.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template hw1
[HUAWEI-hwtacacs-hw1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme0
[HUAWEI-aaa-recording-scheme0] recording-mode hwtacacs hw1
[HUAWEI-aaa-recording-scheme0] quit
[HUAWEI-aaa] cmd recording-scheme scheme0
```

13.1.35 cut access-user

Function

The **cut access-user** command terminates one or multiple access user connections, also forcibly disconnecting online users.

Format

cut access-user { **domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **access-slot** *slot-id* | **user-id** *begin-number* [*end-number*] | **username** *user-name* }

cut access-user ssid *ssid-name* (This command is only supported by the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.)

cut access-user access-type admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**] [**username** *user-name*]

Parameters

Parameter	Description	Value
domain *domain-name*	Disconnects sessions in a specified domain.	The value must be the name of an existing domain.
interface *interface-type interface-number*	Disconnects sessions on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vlan *vlan-id* [**qinq** *qinq-vlan-id*]	Disconnects sessions in a specified VLAN. - *vlan-id* specifies the ID of a VLAN. In QinQ applications, this parameter specifies the inner VLAN ID. - *qinq-vlan-id* specifies the outer VLAN ID.	The values of *vlan-id* and *qinq-vlan-id* are integers that range from 1 to 4094.
ip-address *ip-address*	Disconnects sessions initiated by a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value must be an existing VPN instance name.
mac-address *mac-address*	Disconnects sessions initiated by a specified MAC address.	The value is in H-H-H format. An H contains 4 hexadecimal digits.
service-scheme *service-scheme-name*	Terminates connections based on the service scheme.	The value must be the name of an existing service scheme.
access-slot *slot-id*	Disconnects sessions on a specified device.	The value range depends on the model of the device.
ssid *ssid-name*	Disconnects sessions initiated by a service set identifier (SSID) for a service set.	The SSID must already exist. **NOTE** SSID is supported only in the NAC unified mode.
user-id *begin-number* [*end-number*]	Disconnects sessions of a specified user.	The user-id must exist on the device.

Parameter	Description	Value
username *user-name*	Disconnects sessions of a user with a specified user name.	The value must be the name of an existing user.
access-type	Displays information about the users using the specified authentication mode.	-
admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**]	Displays information about the administrators using the specified authentication mode. ● **ftp**: FTP user ● **ssh**: SSH user ● **telnet**: Telnet user ● **terminal**: Terminal user ● **web**: Web user	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Performing some configurations, such as AAA, on the device, requires that no users be online. You can run the **cut access-user** command to disconnect sessions.

Precautions

- The **cut access-user** command interrupts all services of the user whose session is torn down.
- For administrators, lower-level users cannot tear down the connections of higher-level users.
- If the character string of the user name contains spaces (for example, a b), you can run the **display access-user username "a b"** command to view online users.
- If the character string of the user name contains spaces and quotation marks ("") simultaneously, you cannot use the user name to view online users. In this case, you can run the **display access-user | include** *username* command to view the user ID of the online user, and then run the **display access-user**

user-id *user-id* command to view the user. Alternatively, you can run the **cut access-user user-id** *user-id* command to force the user to go offline.

Example

Tear down the session initiated by the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] cut access-user ip-address 10.1.1.1
```

13.1.36 display aaa

Function

The **display aaa** command displays information about normal logout, abnormal logout, and login failures.

Format

display aaa { **offline-record** | **abnormal-offline-record** | **online-fail-record** } { **all** | **reverse-order** | **domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac-address** *mac-address* | **access-slot** *slot-number* | **time** *start-time end-time* [**date** *start-date end-date*] | **username** *user-name* [**time** *start-time end-time* [**date** *start-date end-date*]] } [**brief**]

Parameters

Parameter	Description	Value
offline-record	Displays normal logout records.	-
abnormal-offline-record	Displays abnormal logout records.	-
online-fail-record	Displays login failure records.	-
all	Displays all login and logout records.	-
reverse-order	Displays the records in order of newest to oldest.	-
domain *domain-name*	Specifies the name of a domain.	The value is a string of 1 to 64 case-insensitive characters, excluding spaces, *, ?, and ".
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Parameter	Description	Value
vlan *vlan-id*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.
qinq *qinq-vlan-id*	Specifies the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
mac-address *mac-address*	Specifies a MAC address.	The value is in H-H-H format. An H is a 4-digit hexadecimal number.
access-slot *slot-number*	Specifies a slot ID.	The value is an integer. The value range depends on the model of the device.
username *user-name*	Specifies a user.	The value must be an existing user.
time *start-time end-time*	Specifies a time range.	The format is HH:MM:SS, indicating hour:minute:second.
date *start-date end-date*	Specifies a date.	The format is YYYY/MM/DD. YYYY is the year, MM is the month, and DD is the day.
brief	Displays brief login and logout information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command allows you to view information about user normal logouts, abnormal logouts, and login failures based on the domain name, interface, IP address, VPN instance, MAC address, or slot ID.

Precautions

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

NOTE

For the meanings, causes, and handling suggestions of abnormal user logins and logouts, see "**Common Causes of Access Authentication**" in the *Huawei S Series Campus Switches Troubleshooting Guide*.

Example

Display information about normal user logouts in the domain **rds**.

```
<HUAWEI> display aaa offline-record domain rds
 -------------------------------------------------------------------
  User name             : test@rds
  Domain name           : rds
  User MAC              : 00e0-fc01-b67c
  User access type      : 802.1x
  User access interface : Wlan-Dbss1
  Qinq vlan/User vlan   : 0/1
  User IP address       : 192.168.2.2
  User IPV6 address     : -
  User ID               : 19
  User login time       : 2008/10/01 04:49:39
  User offline time     : 2008/10/01 04:59:43
  User offline reason   : EAPOL user request
  User name to server   : test@rds
  AP ID                 : 0
  Radio ID              : 0
  AP MAC                : b001-0000-ac01
  SSID                  : ssid1
  -------------------------------------------------------------------
  Are you sure to display some information?(y/n)[y]:
```

Display all unexpected user logout records.

```
<HUAWEI> display aaa abnormal-offline-record all
  ------------------------------------------------------------------------------
  User name             : cdw
  Domain name           : l2bng
  User MAC              : 00e0-fc01-4f2b
  User access type      : MAC
  User access interface : Wlan-Dbss1
  Qinq vlan/User vlan   : 0/2012
  User IP address       : 10.17.17.219
  User IPV6 address     : -
  User ID               : 18
  User login time       : 2017/03/16 19:40:18
  User offline time     : 2017/03/16 19:43:20
  User offline reason   : AAA cut command
  User name to server   : cdw@l2bng
  AP ID                 : 1
  Radio ID              : 0
  AP MAC                : 00e0-fc01-ac01
  SSID                  : ssid1
```

```
 ------------------------------------------------------------------------------
 Are you sure to display some information?(y/n)[y]:
```

Display brief information about unexpected user logout records.

```
<HUAWEI> display aaa abnormal-offline-record all brief
 ------------------------------------------------------------------------------
 UserID    Username                        IP address      MAC
Reason
          SSID                                       User offline time

-------------------------------------------------------------------------------------------

 16010     zcm                            10.1.2.10   -                    Idle cut
          -                                        2022/05/09 14:55:47

-------------------------------------------------------------------------------------------

 Total: 1,Printed: 1
```

Display online failure information of all users.

```
<HUAWEI> display aaa online-fail-record all
 ------------------------------------------------------------------------------
 User name              : test
 Domain name            : default
 User MAC               : 00e0-fc01-85bc
 User access type        : MAC
 User access interface   : Eth-Trunk10
 Qinq vlan/User vlan     : 116/100
 User IP address         : 10.1.1.10
 User IPV6 address       : -
 User ID                : 326678
 User login time         : 2019/09/20 10:06:32
 User online fail reason : Radius authentication reject
 Authen reply message    : ErrorReason is The access quanti...
 User name to server     : zxx
 ------------------------------------------------------------------------------
 Are you sure to display some information?(y/n)[y]:
```

Display information about user login failures. In this example, the login failure cause is IP address conflict.

```
<HUAWEI> display aaa online-fail-record mac-address 00e0-fc01-85bc
 ------------------------------------------------------------------------------
 User name              : test
 Domain name            : default
 User MAC               : 00e0-fc01-85bc
 User access type        : None
 User access interface   : Eth-Trunk10
 Qinq vlan/User vlan     : 116/100
 User IP address         : -
 Conflict IP address     : 192.168.10.1
 User IPV6 address       : -
 User ID                : 326678
 User login time         : 2020/09/20 10:06:32
 User online fail reason : IP address conflict
 Authen reply message    : -
 ------------------------------------------------------------------------------
 Are you sure to display some information?(y/n)[y]:
```

Table 13-2 Description of the **display aaa** command output

Item	Description
User name	User name.
Domain name	Domain of a user.

Item	Description
User MAC or MAC	MAC address of a user.
User access type	Access type of a user: - 802.1x indicates that the user accesses the network through 802.1X. - API indicates that the user accesses the network through the API. - FTP indicates that the user accesses the network through FTP. - Telnet indicates that the user accesses the network through Telnet. - Terminal indicates that the user accesses the network through terminal. - SSH indicates that the user accesses the network through SSH. - x25-pad indicates that the user accesses the network through x25-pad. - HTTP indicates that the user accesses the network through HTTP. - Web indicates that the user accesses the network through web. For the related command, see **local-user service-type**.
User access interface	Access interface of a user.
Qinq vlan/User vlan	VLAN that a user belongs to. - In QinQ application, QinQvlan indicates the outer VLAN ID and Uservlan indicates the inner VLAN ID. - For a common VLAN, Uservlan indicates the VLAN ID, and QinQvlan is 0.
User IP address or IP address	IP address of a user.
User IPV6 address	IPv6 address of a user.
User ID	Index of a user.
User login time	Time when a user goes online.
User offline time	Time when a user goes offline.

Item	Description
User offline reason, User online fail reason, or Reason	Reason why a user fails to go online or offline. The common reasons are as follows: ● The value "EAPOL user request" indicates that an 802.1X user requests to go offline. ● The value "PPP user request" indicates that a PPP user requests to go offline. ● The value "Web user request" indicates that a web user requests to go offline. ● The value "AAA cut command" indicates that a user is deleted using command line. ● The value "Session time out" indicates that a session times out. ● The value "Idle cut" indicates that a user is disconnected because the user does not perform any operation within a specified period. ● The value "PPP authentication fail" indicates a PPP authentication failure. ● The value "STA disassociation" indicates that a STA is disassociated. ● The value "STA disassociation(delay offline)" indicates that the STA disassociation is delayed. ● The value "console reset or disable port" indicates that the management interface is Down. ● The value "Interface net down" indicates that an interface is Down. ● The value "Local authentication reject" indicates that the local authentication password is incorrect. ● The value "AS detect fail" indicates that an AS detection failure occurs on an access device in the policy association scenario. ● The value "AS smooth fail" indicates that an AS smoothing

Item	Description
	failure occurs on an access device in the policy association scenario. - The value "AS configuration changed on interface" indicates that the user goes offline because the configuration of an AS interface on an access device changes in the policy association scenario. - The value "IP address conflict" indicates that IP addresses conflict. - The value "Add FPI item timeout(LPU)" indicates that the LPU authorization times out. - The value "EAPOL client timeout" indicates that the client times out to respond. - The value "low RSSI" indicates that the wireless signal strength is weak. - The value "No authentication server configured" indicates that no authentication server is configured. - The value "No radius-server template bound" indicates that no RADIUS server template is bound. - The value "No tacacs-server template bound" indicates that no TACACS server template is bound. - The value "No accounting server configured" indicates that no accounting server is configured. - The value "Accounting server no response" indicates that the accounting server does not respond. - The value "EAPOL client restart associate" indicates that the 802.1X client re-triggers an association. - The value "Users with low priorities go offline" indicates that users go offline because their priorities are low. - The value "Resources are insufficient" indicates that

Item	Description
	resources of the device are insufficient. - The value "Local Authentication user block" indicates that the local user is locked. - The value "Roaming is prohibited" indicates that user roaming is forbidden. - The value "AP fault" indicates that a wireless user is forced offline due to AP disconnection. - The value "Remote user is blocked" indicates that the remotely authenticated user is locked. - The value "Not support authorization with car" indicates that upstream CAR authorization is not supported for the user group. - The value "Not support authorization with user-group" indicates that re-mark authorization is not supported for the user group. - The value "Radius authentication reject" indicates that the RADIUS server responds with an Access-Reject packet. - The value "Data flow or online time exceed threshold" indicates that the online duration or used traffic of the user reaches the threshold. - The value "AS access interface down" indicates that the interface connecting an access device to a user goes Down in an SVF or policy association scenario. - The value "Server response times out" indicates that the server does not respond due to timeout. - The value "The shared keys on the device and Portal server are different" indicates that the shared key configured on the device is different from that configured on the Portal server.

Item	Description
	● "The acl locally delivered by AAA is invalid or does not exist": The ACL delivered by AAA is invalid or does not exist. ● "The description of the acl sent by Radius is incorrect": The description of the ACL delivered by RADIUS is incorrect. ● "The Rediect ACL delivered by AAA is incorrectly checked": The redirect ACL delivered by AAA is incorrect. ● "AAA gets service scheme error": AAA failed to obtain SERVICE_SCHEME. ● "AAA get author info error": AAA failed to obtain authentication information. ● "AAA check author vlan error": AAA failed to check the authorized VLAN. ● The value "AAA authorization dynamic vlan error" indicates that the dynamic VLAN authorized by AAA is incorrect. ● The value "SAM failed to deliver authorized VLAN" indicates that SAM failed to deliver the authorized VLAN. ● "SAM failed to deliver QOS": SAM failed to deliver QoS. ● "SAM failed to deliver port mac limit": SAM failed to deliver the port MAC limit. ● "SAM failed to deliver vm car": SAM failed to deliver VM CAR. ● "User flow detect fail": User traffic detection fails.

Item	Description
Authen reply message	Authentication response message. If the Access-Reject packet returned by the RADIUS server carries this field, this field is filled with the message carried in the Access-Reject packet. The length of this field cannot exceed 32 bytes. Otherwise, the message "Authentication fail,user is blocked" or "Authentication fail" is displayed.
User name to server	User name sent by the device to the server.
AP ID	ID of the AP that a wireless user associates with.
Radio ID	ID of the radio that a wireless user associates with.
AP MAC	MAC address of the AP that a wireless user associates with.
SSID	SSID that a wireless user associates with.
Conflict IP address/Conflict IPv6 address	Conflicting IPv4 or IPv6 address.

13.1.37 display aaa configuration

Function

The **display aaa configuration** command displays the AAA configurations, for example, the domain, authentication scheme, authorization scheme, and accounting scheme.

Format

display aaa configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

AAA configurations are limited by system specifications. Before performing AAA configurations, run the **display aaa configuration** command to check whether there are sufficient resources.

Example

Display the AAA summary.

```
<HUAWEI> display aaa configuration
  Domain Name Delimiter                    : @
  Domainname parse direction               : Left to right
  Domainname location                      : After-delimiter
  Administrator user default domain        : default_admin
  Normal user default domain               : default
  Domain                                   : total: 32      used: 5
  Authentication-scheme                    : total: 33      used: 4
  Accounting-scheme                        : total: 32      used: 3
  Authorization-scheme                     : total: 32      used: 2
  Service-scheme                           : total: 32      used: 0
  Recording-scheme                         : total: 64      used: 0
  Local-user                               : total: 1000    used: 1
  Local-user block retry-interval          : 5 Min(s)
  Local-user block retry-time              : 3
  Local-user block time                    : 5 Min(s)
  Remote-admin-user block retry-interval   : 5 Min(s)
  Remote-admin-user block retry-time       : 30
  Remote-admin-user block time             : 5 Min(s)
  Session timeout invalid enable           : No
  Navigator first login state              : No
```

Table 13-3 Description of the **display aaa configuration** command output

Item	Description
Domain Name Delimiter	Domain name delimiter, which can be any of the following characters: \ / : < > | @ ' %. The default domain name delimiter is @. To configure a domain name delimiter, run the **domain-name-delimiter** command.
Domain	Number of domains. ● total: indicates the total number of domains that can be created. ● used: indicates the number of domains that have been created.
Domainname parse direction	Parsing direction of the domain name. ● Left to right ● Right to left To configure this parameter, run the **domainname-parse-direction** command.

Item	Description
Domainname location	Domain name location. - After-delimiter: The domain name is placed behind the domain name delimiter. - Before-delimiter: The domain name is placed before the domain name delimiter. To configure this parameter, run the **domain-location** command.
Administrator user default domain	Domain name of administrator users.
Normal user default domain	Domain name of normal users.
Authentication-scheme	Number of authentication schemes. - total: indicates the total number of authentication schemes that can be created. - used: indicates the number of authentication schemes that have been created.
Accounting-scheme	Number of accounting schemes. - total: indicates the total number of accounting schemes that can be created. - used: indicates the number of accounting schemes that have been created.
Authorization-scheme	Number of authorization schemes. - total: indicates the total number of authorization schemes that can be created. - used: indicates the number of authorization schemes that have been created.
Service-scheme	Number of service schemes. - total: indicates the total number of service schemes that can be created. - used: indicates the number of service schemes that have been created.
Recording-scheme	Number of recording schemes. - total: indicates the total number of recording schemes that can be created. - used: indicates the number of recording schemes that have been created.

Item	Description
Local-user	Number of local users. - total: indicates the total number of local users that can be created. - used: indicates the number of local users that have been created.
Local-user block retry-interval	Authentication retry interval of a local account. To configure this parameter, run the **local-aaa-user wrong-password** command.
Local-user block retry-time	Maximum number of consecutive authentication failures for a local account. To configure this parameter, run the **local-aaa-user wrong-password** command.
Local-user block time	Locking time of a local account. To configure this parameter, run the **local-aaa-user wrong-password** command.
Remote-access-user block retry-interval	Authentication retry interval for access users who fail remote authentication. To configure this parameter, run the **access-user remote authen-fail** command.
Remote-access-user block retry-time	Maximum number of consecutive authentication failures for access users. To configure this parameter, run the **access-user remote authen-fail** command.
Remote-access-user block time	Locking time for access users who fail remote authentication. To configure this parameter, run the **access-user remote authen-fail** command.
Remote-admin-user block retry-interval	Authentication retry interval for administrators who fail remote authentication. To configure this parameter, run the **administrator remote authen-fail** command.
Remote-admin-user block retry-time	Maximum number of consecutive authentication failures for administrator. To configure this parameter, run the **administrator remote authen-fail** command.
Remote-admin-user block time	Locking period for administrators who fail remote authentication. To configure this parameter, run the **administrator remote authen-fail** command.

Item	Description
Session timeout invalid enable	- Yes: The device will not disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0. - No: The device will disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0. To configure this parameter, run the **aaa-author session-timeout invalid-value enable** command.
Navigator first login state	Indicates the first login status of the factory device.

13.1.38 display aaa statistics offline-reason

Function

The **display aaa statistics offline-reason** command displays the reasons why users go offline.

Format

display aaa statistics offline-reason

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display aaa statistics offline-reason** command helps you know the reason why a user goes offline. You can locate network faults according to the command output.

Example

Display reasons why users go offline.

```
<HUAWEI> display aaa statistics offline-reason
 19  User request to offline                                                    :2
 87  AAA cut command                                                              :1
```

Table 13-4 Description of the display aaa statistics offline-reason command output

Item	Description
19/87	Reason code.
User request to offline	A user requested to go offline.
2/1	Number of times users go offline.
AAA cut command	A user is disconnected by the **cut access-user** command.

13.1.39 display aaa-quiet administrator except-list

Function

The **display aaa-quiet administrator except-list** command displays IP addresses that a user can use to access the network when the user account is locked.

Format

display aaa-quiet administrator except-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After a user is configured to access the network using a specified IP address when the user account is locked using the **aaa-quiet administrator except-list** command, you can run the **display aaa-quiet administrator except-list** command to check information about the specified IP addresses.

Example

Display IP addresses that a user can use to access the network when the user account is locked.

```
<HUAWEI> display aaa-quiet administrator except-list
--------------------------------------------------------------------------------
 Admin silent whitelist
--------------------------------------------------------------------------------
```

```
10.2.2.1
10.2.2.2
--------------------------------------------------------------------------------
Total: 2, printed: 2
```

Table 13-5 Description of the **display aaa-quiet administrator except-list** command output

Item	Description
Admin silent whitelist	IP addresses configured in a whitelist.

13.1.40 display access-user (all views)

Function

The **display access-user** command displays information about online users (including access users and administrators).

Format

display access-user [**domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6-address** *ipv6-address* | **access-slot** *slot-id* | **wired** | **wireless**] [**detail**]

display access-user username *user-name* [**detail**]

display access-user ssid *ssid-name* (This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.)

display access-user [**mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **user-id** *user-id*]

display access-user statistics

display access-user access-type admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**] [**username** *user-name*]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **wireless** parameter.

Parameters

Parameter	Description	Value
domain *domain-name*	Displays information about users in a specified domain.	The domain name must already exist.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about users on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vlan *vlan-id* [**qinq** *qinq-vlan-id*]	Displays information about users in a VLAN. - *vlan-id* specifies the ID of a VLAN. In QinQ applications, this parameter specifies the inner VLAN ID. - *qinq-vlan-id* specifies the outer VLAN ID. In the authorized ISP VLAN scenario, you can view the user information only when the specified VLAN ID is the ISP VLAN ID.	The values of *vlan-id* and *qinq-vlan-id* are integers that range from 1 to 4094.
ip-address *ip-address*	Displays information about the user with a specified IP address. **NOTE** For NAC or static users, details about the users are displayed. For other users, brief information about the users is displayed.	The value of *ip-address* is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value must be an existing VPN instance name.
ipv6-address *ipv6-address*	Displays information about the user with a specified IPv6 address.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal digits in the format X:X:X:X:X:X:X:X.
mac-address *mac-address*	Displays information about the user with a specified MAC address.	The value is in H-H-H format. An H contains four hexadecimal digits.

Parameter	Description	Value
service-scheme *service-scheme-name*	Displays information about the user with a specified service scheme.	The service scheme must already exist.
access-slot *slot-id*	Displays information about users connecting to a specified device.	The value range depends on the model of the device.
ssid *ssid-name*	Specifies the SSID for a service set.	The SSID must already exist. **NOTE** SSID is supported only in the NAC unified mode.
username *user-name*	Displays information about the user with a user name.	The user name must already exist.
statistics	Displays user statistics on the device. - Historical wireless user statistics: displays historical wireless user statistics on the device. - Current online user statistics: displays current user statistics on the device.	The keyword **statistics** is supported only in the NAC unified mode.
user-id *user-id*	Displays information about sessions of a specified user. If this parameter is specified, detailed information about the user is displayed.	The user-id must exist on the device.
detail	Displays detailed information about users.	-
access-type	Displays information about the users using the specified authentication mode.	-

Parameter	Description	Value
admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**]	Displays information about the administrators using the specified authentication mode. ● **ftp**: FTP user ● **ssh**: SSH user ● **telnet**: Telnet user ● **terminal**: Terminal user ● **web**: Web user	-
wired	Displays information about wired users.	-
wireless	Displays information about wireless users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays information about user sessions on the device.

Precautions

Administrators with low privilege levels cannot view information about administrators with high privilege levels.

If the character string of the user name contains spaces (for example, a b), you can run the **display access-user username "a b"** command to view online users.

If the character string of the user name contains spaces and quotation marks ("") simultaneously, you cannot use the user name to view online users. In this case, you can run the **display access-user | include** *username* command to view the user ID of the online user, and then run the **display access-user user-id** *user-id* command to view the user. Alternatively, you can run the **cut access-user user-id** *user-id* command to disconnect the user.

When displaying VPN user entries based on user IP address, you must set the **vpn-instance** *vpn-instance-name* parameter to specify the VPN instance to which the IP address belongs.

If **user-id** is specified, detailed information about the specified user is displayed. If **user-id** is not specified, brief information about all online users is displayed, including the user ID, user name, IP address, and MAC address of each user.

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When you run the **display access-user** command without specifying any parameter to view user information and the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following the 19th character; that is, only 22 characters are displayed. When you run the **display access-user** command with parameters specified to view detailed information about the user table, all the characters of **username** are displayed, and the rule for converting special characters remains unchanged.

When **interface** is specified, the device displays the connection information of online wired users on the interface.

When querying user information based on interfaces, MAC addresses, or VLANs, the device only displays information about 802.1X, Portal, or MAC address authentication users.

Example

Display information about user sessions on the device.

```
<HUAWEI> display access-user
 ------------------------------------------------------------------------------------------
 UserID Username                    IP address                MAC           Status
 ------------------------------------------------------------------------------------------
 1      normal@local                -                         xxxx-xxxx-xxxx    Success
 62     005500000001                192.168.1.121             xxxx-xxxx-xxx1    Open
 32675  fztest                      -                         xxxx-xxxx-xxx2    Success
 16019  b002404                     192.168.1.2               xxxx-xxxx-xxx3    Success
 ------------------------------------------------------------------------------------------
 Total: 4, printed: 4
```

NOTE

If you specify the **include** or **exclude** parameter in the command, the values of **Total** and **printed** are still the total number of users.

Display information about the user with the user ID 1.

```
<HUAWEI> display access-user user-id 1
Basic:
  User ID                         : 1
  User name                       : normal
  Domain-name                     : rds
  User MAC                        : xxxx-xxxx-xxxx
  User IP address                 : 10.124.1.253
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : GigabitEthernet0/0/1
  User vlan event                 : Success
  QinQVlan/UserVlan               : 0/20
  User vlan source                : user request
  User access time                : 2014/03/31 15:38:55
```

```
  User accounting session ID      : esap_lm000000000001245****8016032
  Option82 information            : -
  User access type                : MAC
  HTTP User_Agent                 : Mozilla/4.0 (compatible; MSIE 7.0; Windows N
                                   T 5.1; Trident/4.0; aff-kingsoft-ciba; .NET4
                                   .0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR
                                   3.0.4506.2152; .NET CLR 3.5.30729)
  DHCP option ID                  : 12
  DHCP option content             : [ASCII]
  DHCP option ID                  : 55
  DHCP option content             : [HEX]010F03062C2E2F
  DHCP option ID                  : 60
  DHCP option content             : [ASCII]MSFT 5.0
  User Privilege                  : 15
  Terminal Device Type            : Data Terminal
  Dynamic ACL ID(Effective)       : 3100
  Dynamic group index(Effective)  : 10
  Dynamic group name(Effective)   : group10
  Session Timeout                 : 1800(s) (local), Remaining: 1740(s)
  Termination Action              : RE-AUTHENTICATION

AAA:
  User authentication type        : MAC authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```

Display the user with the user ID 62.

```
<HUAWEI> display access-user user-id 62
Basic:
  User ID                         : 62
  User name                       : test
  Domain-name                     : -
  User MAC                        : xxxx-xxxx-xxxx
  User IP address                 : 192.168.1.121
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : Wlan-Dbss3:152
  User vlan event                 : Open
  QinQVlan/UserVlan               : 0/125
  User vlan source                : user request
  User access time                : 2015/07/10 11:27:12
  User accounting session ID      : esap_lm000000000001245****8016032
  Option82 information            : -
  User access type                : None
  HTTP User_Agent                 : Mozilla/4.0 (compatible; MSIE 7.0; Windows N
                                   T 5.1; Trident/4.0; aff-kingsoft-ciba; .NET4
                                   .0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR
                                   3.0.4506.2152; .NET CLR 3.5.30729)
  DHCP option ID                  : 12
  DHCP option content             : [ASCII]
  DHCP option ID                  : 55
  DHCP option content             : [HEX]010F03062C2E2F
  DHCP option ID                  : 60
  DHCP option content             : [ASCII]MSFT 5.0
  Redirect ACL ID(Effective)      : 3001
  User Privilege                  : 15
  AP ID                           : 152
  AP name                         : ap-152
  Radio ID                        : 0
  AP MAC                          : 00e0-fc76-e360
  SSID                            : 57-open
  Online time                     : 23(s)
  iConnect info                   : https://example.com:1000/XXXX

AAA:
  User authentication type        : None
  Current authentication method   : None
```

```
  Current authorization method    : Local
  Current accounting method       : None
```

Display the user with the user ID 32675.

```
<HUAWEI> display access-user user-id 32675
Basic:
  User ID                         : 32675
  User name                       : fztest
  Domain-name                     : fz
  User MAC                        : xxxx-xxxx-xxxx
  User IP address                 : -
  User IPv6 address               : -
  User access Interface           : Eth-Trunk1
  User vlan event                 : Success
  QinQVlan/UserVlan               : 0/18
  User vlan source                : user request
  User access time                : 2015/02/11 21:51:58
  User accounting session ID      : esap_lm000000000001245****8016032
  Option82 information            : -
  User access type                : 802.1x
  Redirect ACL ID(Effective)      : 3001
  User Privilege                  : 15
  AS ID                           : 1
  AS name                         : test
  AS IP                           : 192.168.1.11
  AS MAC                          : 00e0-fc76-ee60
  AS Interface                    : GigabitEthernet0/0/1
  Terminal Device Type            : Data Terminal

AAA:
  User authentication type        : 802.1x authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```

Display the user with the user ID 16019.

```
<HUAWEI> display access-user user-id 16019
Basic:
  User ID                         : 16019
  User name                       : b002404
  Domain-name                     : abc
  User MAC                        : xxxx-xxxx-xxxx
  User IP address                 : 192.168.1.2
  User vpn-instance               : -
  User IPv6 address               : FC00:3::5689:98FF:FE01:583D
  User IPv6 link local address    : FE80::5689:98FF:FE01:583D
  User access Interface           : GigabitEthernet0/0/1
  User vlan event                 : Success
  QinQVlan/UserVlan               : 20/21
  User vlan source                : user request
  User access time                : 2016/08/16 18:32:16
  User accounting session ID      : HUAWEI000000000001245****8016032
  Option82 information            : -
  User PIR(Kbps)                  : 5000
  User flow mapping name          : zt
  User flow queue name            : zt
  User access type                : MAC
  Redirect ACL ID(Effective)      : 3001
  Terminal Device Type            : Data Terminal
  User inbound data flow(Packet)  : -
  User inbound data flow(Byte)    : -
  User outbound data flow(Packet) : -
  User outbound data flow(Byte)   : -
  User Lease                      : 600(s)
  ISP   VLAN                      : 1000
  ISP Interface                   : GigabitEthernet60/1/17
AAA:
  User authentication type        : MAC authentication
```

```
Current authentication method   : RADIUS
Current authorization method    : -
Current accounting method       : None
```

NOTE

When an Eth-Trunk contains a card that does not support a specified function, the message "The Eth-Trunk contains a card that does not support this function" is displayed behind the corresponding item.

Table 13-6 Description of the **display access-user** command output

Item	Description
Basic	Basic information about a user.
UserID/User ID	Index of a user.
Username/User name	User name.
Domain-name	User domain.
MAC/User MAC	MAC address of a user.
IP address/User IP address	IP address of a user.
User vpn-instance	User VPN instance.
User IPv6 address	IPv6 address of a user.
User IPv6 link local address	IPv6 link-local address.
User access Interface	Access interface connected to a user.
Status/User vlan event	Whether a user joins a VLAN. ● Open: For a wired user, the user goes online through the open function upon authentication failure. For wireless users, no authentication is performed. ● Success: authentication is successful ● Pre-authen: pre-authentication ● Client-no-resp: the client does not respond ● Fail-authorized: authorization upon authentication failure ● Web-server-down: web server is Down ● Aaa-server-down: AAA server is Down

Item	Description
QinQVlan/UserVlan	VLAN that a user belongs to. ● In QinQ applications, QinQVlan indicates the outer VLAN ID and UserVlan indicates the inner VLAN ID. ● For a common VLAN, UserVlan indicates the VLAN ID, and QinQVlan is 0.
User vlan source	Source of a user VLAN. ● server vlan: The VLAN is delivered by the remote server. ● server vlan pool: VLAN pool delivered by the remote server ● user group vlan: the VLAN is bound to a user group. This parameter is available only in common mode. ● user group vlan pool: VLAN pool bound to a user group This parameter is available only in common mode. ● service scheme vlan: The VLAN is configured in the service scheme view. ● local event vlan: The authorized VLAN (guest or survival) is configured locally. ● user request: The VLAN is carried in the user request (authentication request).
User access time	Time when a user goes online. If a time zone is configured and the daylight saving time begins, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST.
User accounting session ID	ID of an accounting session.
Option82 information	Option 82 of a user.
User PIR(Kbps)	Peak Information Rate (PIR) in kbit/s.
User flow mapping name	Name of the user flow mapping template.
User flow queue name	Name of the user flow queue.

Item	Description
User access type	Access type of a user. For the related command, see **local-user service-type**.
Redirect ACL ID(Effective)	User redirect ACL ID: - Effective: The ACL takes effect. - Ineffective: The ACL does not take effect. The possible reason is that the ACL is not configured on the device.
User Privilege	Level of a user.
Terminal Device Type	Terminal device type of a user.
HTTP User_Agent	User-Agent information in HTTP packets.
DHCP option ID	Value of a DHCP option.
DHCP option content	Content of a DHCP option. **NOTE** If a DHCP option contains invisible characters, it is displayed in hexadecimal format and starts with [HEX]. Otherwise, it is displayed as a character string and starts with [ASCII].
Dynamic group index(Effective)	ID of a UCL group. This option is available only in NAC unified mode.
Dynamic group name(Effective)	Name of a UCL group. This option is available only in NAC unified mode.
Session Timeout	Timeout interval of sessions. - *xx*(s) (local): reauthentication interval of a locally configured MAC or 802.1X user. - *xx*(s) (server): Session-Timeout (27) attribute delivered by the RADIUS server. This attribute indicates the remaining time of the service provided to a user.
Remaining	Remaining session time.
Termination Action	Action taken when a session times out. - RE-AUTHENTICATION: authentication is performed again - OFFLINE: the user is disconnected.
AP ID	ID of the AP connected to users.

Item	Description
AP name	Name of the AP connected to users.
Radio ID	ID of the radio.
AP MAC	MAC address of the AP connected to users.
SSID	SSID of a STA.
Online time	STA online time.
iConnect info	Identity information of iConnect terminals.
AAA	AAA information about a user.
User authentication type	Authentication type of a user, which depends on the access type of the user.
Current authentication method	Authentication method used for a user.
Current authorization method	Current authorization method.
Current accounting method	Current accounting method.
AS ID	ID of the access devices in policy association network.
AS name	Name of the access devices in policy association network.
AS IP	IP address of the access devices in policy association network.
AS MAC	MAC address of the access devices in policy association network.
AS Interface	Interface of the access devices in policy association network.
User inbound data flow(Packet)	Data traffic (number of packets) from users to the device.
User inbound data flow(Byte)	Data traffic (number of bytes) from users to the device.
User outbound data flow(Packet)	Data traffic (number of packets) from the device to users.
User outbound data flow(Byte)	Data traffic (number of bytes) from the device to users.
User Lease	User lease.
ISP VLAN	Authorized outbound interface VLAN.
ISP Interface	Authorized outbound interface.

Item	Description
Number of user-group car	Number of users whose rate is limited by the CAR value authorized. If this item is not displayed, there are no such users.
web-server IP address	Portal server IP address. This field is displayed only when the Portal or HACA protocol is used for Portal authentication.
User flow mapping name	Authorized flow mapping profile.
SAC profile name	Authorized SAC profile.
DACL group name	Name of the authorized DACL group. It is delivered by the RADIUS server through the RADIUS attribute 26-82 (HW-Data-Filter). ● Effective: The DACL group name has taken effect. ● Ineffective. The DACL group name does not take effect.

13.1.41 display access-user user-name-table statistics

Function

The **display access-user user-name-table statistics** command displays statistics on users who access the network after the number of users is limited based on the user name.

Format

display access-user user-name-table statistics { **all** | **username** *username* }

Parameters

Parameter	Description	Value
all	Displays statistics on all users.	-
username *username*	Displays statistics on users with a specified user name.	The value is an existing user name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the number of access users is limited based on the user name using the **access-limit user-name max-num** command, you can run the **display access-user user-name-table statistics** command to check related statistics including the maximum number of access users and IP and MAC addresses of access users.

NOTE

Statistics about pre-connection users are not included in the statistics displayed in this command output.

Example

Display statistics on all users who access the network after the number of access users is limited based on the user name.

```
<HUAWEI> display access-user user-name-table statistics all
-------------------------------------------------------------------------------
 Username              Current num      Access limit max num
-------------------------------------------------------------------------------
 test@123              8                8
-------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Display detailed statistics on users with the user name **test@123** who access the network after the number of access users is limited based on the user name.

```
<HUAWEI> display access-user user-name-table statistics username test@123

Basic Info:
 User name                  : test@123
 Current num                : 8
 Access limit max num       : 8
Detail Info:
-------------------------------------------------------------------------------
 UserID      Username             IP address      MAC
-------------------------------------------------------------------------------
 16016       test@123             192.168.8.139   00e0-fcf1-0794

 16017       test@123             192.168.8.140   00e0-fcf1-0795

 16018       test@123             192.168.8.141   00e0-fcf1-0796

 16019       test@123             192.168.8.142   00e0-fcf1-0797

 16020       test@123             192.168.8.143   00e0-fcf1-0798

 16021       test@123             192.168.8.144   00e0-fcf1-0799

 16022       test@123             192.168.8.145   00e0-fcf1-079a

 16023       test@123             192.168.8.146   00e0-fcf1-079b

-------------------------------------------------------------------------------
 Total: 8, printed: 8
```

Table 13-7 Description of the **display access-user user-name-table statistics** command output

Item	Description
Basic Info	Basic information.
User name or Username	User name.
Current num	Number of current access users.
Access limit max num	Maximum number of access users.
Detail Info	Detailed information.
UserID	User ID.
IP address	User's IP address.
MAC	User's MAC address.
Total: *m*, printed: *n*	Total number (*m*) of entries and number (*n*) of displayed entries.

13.1.42 display accounting-scheme

Function

The **display accounting-scheme** command displays the configuration of accounting schemes, including accounting scheme names and accounting modes.

Format

display accounting-scheme [*accounting-scheme-name*]

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The accounting scheme must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the accounting scheme configuration is complete, run the **display accounting-scheme** command to check whether the accounting scheme configuration is correct.

Before applying an accounting scheme to a domain, run the **display accounting-scheme** command to check whether configuration of the accounting scheme is correct.

Precautions

If the name of an accounting scheme is specified, the **display accounting-scheme** command displays the detailed accounting scheme configuration. Otherwise, this command displays only the summary of accounting schemes.

Example

Display the summary of all accounting schemes.

```
<HUAWEI> display accounting-scheme
  -------------------------------------------------------------------
  Accounting-scheme-name           Accounting-method        scheme-index
  -------------------------------------------------------------------
  default                          None                     0
  radius-1                         RADIUS                    1
  tacas-1                          HWTACACS                   3

  -------------------------------------------------------------------
  Total of accounting-scheme: 3
```

Display the detailed configuration of the default accounting scheme.

```
<HUAWEI> display accounting-scheme default

  Accounting-scheme-name               : default
  Accounting-method                    : None
  Realtime-accounting-switch           : Disabled
  Realtime-accounting-interval(min)    : -
  Start-accounting-fail-policy         : Offline
  Realtime-accounting-fail-policy      : Online
  Realtime-accounting-failure-retries  : 3
```

Table 13-8 Description of the **display accounting-scheme** command output

Item	Description
scheme-index	Scheme index.
Accounting-scheme-name	Name of an accounting scheme. To create an accounting scheme, run the **accounting-scheme (AAA view)** command.

Item	Description
Accounting-method	Accounting mode in the accounting scheme: - HWTACACS: indicates that an HWTACACS server performs accounting. - None: indicates that accounting is not performed. - RADIUS: indicates that a RADIUS server performs accounting. - HACA: indicates that an HACA server performs accounting. To configure the accounting mode, run the **accounting-mode** command.
Realtime-accounting-switch	Whether the real-time accounting function is enabled: - Disabled: indicates that the real-time accounting function is disabled. - Enabled: indicates that the real-time accounting function is enabled. To configure the real-time accounting function, run the **accounting realtime** command.
Realtime-accounting-interval(min)	Real-time accounting interval. To configure the real-time accounting interval, run the **accounting realtime** command.
Start-accounting-fail-policy	Policy used in case of accounting-start failures: - Offline: indicates that the device disconnects users. - Online: indicates that the device keeps users online. To configure a policy used in case of accounting-start failures, run the **accounting start-fail** command.

Item	Description
Realtime-accounting-fail-policy	Policy used in case of real-time accounting failures: ● Offline: indicates that the device disconnects users. ● Online: indicates that the device keeps users online. To configure a policy used in case of real-time accounting failures, run the **accounting interim-fail** command.
Realtime-accounting-failure-retries	Number of retries before a real-time accounting failure is confirmed. To configure the number of retries, run the **accounting interim-fail** command.

13.1.43 display authentication-scheme

Function

The **display authentication-scheme** command displays the configuration of authentication schemes.

Format

display authentication-scheme [*authentication-scheme-name*]

Parameters

Parameter	Description	Value
authentication-scheme-name	Specifies the name of an authentication scheme.	The authentication scheme must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether an authentication scheme is configured correctly, run the **display authentication-scheme** command.

Precautions

If the **display authentication-scheme** command is executed in the authentication scheme view or the name of an authentication scheme is specified in the command, this command displays detailed authentication scheme configuration. Otherwise, this command displays only summary information of authentication schemes.

Example

Display summary information of all authentication schemes.

```
<HUAWEI> display authentication-scheme
  -------------------------------------------------------------------
 Authentication-scheme-name          Authentication-method      scheme-index
  -------------------------------------------------------------------
  default                            Local                  0
  radius                             RADIUS                  1
  -------------------------------------------------------------------
  Total of authentication scheme: 2
```

Display detailed configuration of the authentication scheme named **default**.

```
<HUAWEI> display authentication-scheme default

  Authentication-scheme-name          : default
  Authentication-method               : Local
  Radius authentication-type of admin : PAP(all)
  server no-response accounting       : NO
  server no-response authorization    : NO
  Location after radius reject        : None
```

Table 13-9 Description of the **display authentication-scheme** command output

Item	Description
scheme-index	Scheme index.
Authentication-scheme-name	Name of an authentication scheme. To create an authentication scheme, run the **authentication-scheme (AAA view)** command.
Authentication-method	Authentication mode in an authentication scheme. To configure an authentication mode in an authentication scheme, run the **authentication-mode (authentication scheme view)** command.

Item	Description
Radius authentication-type of admin	Access type of administrators on whom CHAP authentication is performed during RADIUS authentication. The value can be: ● PAP(all): PAP authentication is performed on administrators of all access types when they are authenticated using RADIUS. ● CHAP(ftp) PAP (other): CHAP authentication is performed on FTP users whose access types are displayed in brackets () when they are authenticated using RADIUS, and PAP authentication is performed on the administrators of other access types. To configure the access type, run the **authentication-type radius chap access-type admin** command.
server no-response accounting	Whether the device continues to send accounting packets after local authentication is performed for a user who does not receive any response from the server. The value can be: ● YES: The device continues to send accounting packets. ● NO: The device does not send accounting packets. To configure this function, run the **server no-response accounting** command.
server no-response authorization	Whether the device continues to send authorization packets after local authentication is performed for a user who does not receive any response from the server. The value can be: ● YES: The device continues to send authorization packets. ● NO: The device does not send authorization packets. To configure this function, run the **server no-response authorization** command.

Item	Description
Location after radius reject	Whether a user is authenticated using another authentication mode after the user's RADIUS authentication request is rejected. The value can be: ● None: The user is not authenticated using another authentication mode after the user's RADIUS authentication request is rejected and the authentication process ends. ● Local: The user is authenticated using the local authentication mode after the user's RADIUS authentication request is rejected. To configure this parameter, run the **radius-reject local** command.

13.1.44 display authorization-scheme

Function

The **display authorization-scheme** command displays the configuration of authorization schemes.

Format

display authorization-scheme [*authorization-scheme-name*]

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The authorization scheme must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the authorization scheme configuration is complete, run the **display authorization-scheme** command to check whether the authorization scheme configuration is correct.

Before applying an authorization scheme to a domain, run the **display authorization-scheme** command to check whether the authorization scheme meets requirements.

Precautions

If the name of an authorization scheme is specified, this command displays the detailed configuration of the authorization scheme. Otherwise, this command displays only the summary of authorization schemes.

Example

Display the summary of authorization schemes.

```
<HUAWEI> display authorization-scheme
  -------------------------------------------------------------------
  Authorization-scheme-name         Authorization-method        scheme-index
  -------------------------------------------------------------------
   default                          Local                    0
   scheme0                           Local                    1
  -------------------------------------------------------------------
   Total of authorization-scheme: 2
```

Display the detailed configuration of the authorization scheme **scheme0**.

```
<HUAWEI> display authorization-scheme scheme0
--------------------------------------------------------------------------
 Authorization-scheme-name   : scheme0
 Authorization-method        : Local
 Authorization-cmd level  0   : Disabled
 Authorization-cmd level  1   : Disabled
 Authorization-cmd level  2   : Disabled
 Authorization-cmd level  3   : Disabled
 Authorization-cmd level  4   : Disabled
 Authorization-cmd level  5   : Disabled
 Authorization-cmd level  6   : Disabled
 Authorization-cmd level  7   : Disabled
 Authorization-cmd level  8   : Disabled
 Authorization-cmd level  9   : Disabled
 Authorization-cmd level 10   : Disabled
 Authorization-cmd level 11   : Disabled
 Authorization-cmd level 12   : Disabled
 Authorization-cmd level 13   : Disabled
 Authorization-cmd level 14   : Disabled
 Authorization-cmd level 15   : Disabled
 Authorization-cmd no-response-policy    : Online
--------------------------------------------------------------------------
```

Table 13-10 Description of the **display authorization-scheme** command output

Item	Description
scheme-index	Scheme index.
Authorization-scheme-name	Name of an authorization scheme. To configure this parameter, run the **authorization-scheme (AAA view)** command.

Item	Description
Authorization-method	Authorization mode configured for an authorization scheme. To configure this parameter, run the **authorization-mode** command.
Authorization-cmd level	Whether the command authorization function is enabled for a user with a specified level: ● Disabled: The command authorization function is disabled. ● Enabled: The command authorization function is enabled. To configure this parameter, run the **authorization-cmd** command.
Authorization-cmd no-response-policy	Policy used when command authorization fails: allows users to go online.

13.1.45 display domain

Function

The **display domain** command displays the domain configuration.

Format

display domain [**name** *domain-name*]

Parameters

Parameter	Description	Value
name *domain-name*	Specifies the domain name. If this parameter is not specified, brief information about all domains is displayed.	The domain name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a domain is created using the **domain** command and is configured, you can run the **display domain** command to view the domain configuration.

Example

Display brief information about all domains.

```
<HUAWEI> display domain
 -------------------------------------------------------------------------
 index    DomainName
 -------------------------------------------------------------------------
 0        default
 1        default_admin
 -------------------------------------------------------------------------
 Total: 2
```

Table 13-11 Description of the **display domain** command output

Item	Description
index	Domain index. To configure this parameter, run the **domain (AAA view)** command.
DomainName	Domain name. To configure this parameter, run the **domain (AAA view)** command.

Display the configuration of the domain **default**.

```
<HUAWEI> display domain name default

 Domain-name                      : default
 Domain-index                     : 0
 Domain-state                     : Active
 Authentication-scheme-name       : default
 Accounting-scheme-name           : default
 Authorization-scheme-name        : -
 Service-scheme-name              : -
 RADIUS-server-template           : -
 Accounting-copy-RADIUS-template : -
 HWTACACS-server-template         : -
 HACA-server-template             : -
 User-group                       : -
 Push-url-address                 : -
 Accounting-DualStack-Separate   : -
```

Table 13-12 Description of the **display domain name** command output

Item	Description
Domain-name	Domain name. To configure this parameter, run the **domain (AAA view)** command.

Item	Description
Domain-index	Domain index. To configure this parameter, run the **domain (AAA view)** command.
Domain-state	Domain status. - Active: indicates that the domain is activated. - Block: indicates that the domain is blocked. To configure this parameter, run the **state (AAA domain view)** command.
Authentication-scheme-name	Name of the authentication scheme used in a domain. To configure this parameter, run the **authentication-scheme (AAA domain view)** command.
Accounting-scheme-name	Name of the accounting scheme used in a domain. To configure this parameter, run the **accounting-scheme (AAA domain view)** command.
Authorization-scheme-name	Name of the authorization scheme used in a domain. To configure this parameter, run the **authorization-scheme (AAA domain view)** command.
Service-scheme-name	Name of the service scheme used in a domain. To configure this parameter, run the **service-scheme (AAA domain view)** command.
RADIUS-server-template	Name of the RADIUS server template used in a domain. To configure this parameter, run the **radius-server (AAA domain view)** command.
Accounting-copy-RADIUS-template	RADIUS server template for level-2 accounting used in a domain. To configure this parameter, run the **accounting-copy radius-server** command.
HWTACACS-server-template	Name of the HWTACACS server template used in a domain. To configure this parameter, run the **hwtacacs-server** command.
HACA-server-template	Name of the HACA server template used in a domain.
User-group	Name of the user group for users in a domain. To configure this parameter, run the **user-group (AAA domain view)** command.

Item	Description
Push-url-address	Pushed URL used in a domain. To configure this parameter, run the **force-push** command.
Accounting-DualStack-Separate	Whether separate statistics collection or separate rate limiting of IPv4 and IPv6 traffic is enabled: ● enable: The function is enabled. ● -: The function is disabled. To configure this parameter, run the **accounting dual-stack separate** command.

13.1.46 display local-user

Function

The **display local-user** command displays information about local users.

Format

display local-user [**domain** *domain-name* | **state** { **active** | **block** } | **username** *user-name*] *

Parameters

Parameter	Description	Value
domain *domain-name*	Displays information about local users in a specified domain.	The domain name must already exist.
state { **active** | **block** }	Displays the attributes of local users in the specified state. ● **active**: indicates the active state. ● **block**: indicates the blocking state.	-
username *user-name*	Displays information about a specified local user name.	The user name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display local-user** command output helps you check the configuration of local users and isolate faults related to the local users.

Precautions

If no parameter is specified, brief information about all local users is displayed. If a parameter is specified, detailed information about the specified local user is displayed.

Low-level users cannot view information about high-level users.

Example

Display brief information about local users.

```
<HUAWEI> display local-user
  ----------------------------------------------------------------------------
  User-name                    State  AuthMask  AdminLevel
  ----------------------------------------------------------------------------
  user-a                       A      A         0
  user-c                       A      A         0
  ----------------------------------------------------------------------------
  Total 2 user(s)
```

Display detailed information about the local user **user-a**.

```
<HUAWEI> display local-user username user-a
  The contents of local user(s):
  Password             : ****************
  State                : active
  Service-type-mask    : A
  Privilege level      : -
  Ftp-directory        : -   HTTP-directory       : -
  Access-limit         : Yes
  Access-limit-max     : 4294967295
  Accessed-num         : 0
  Idle-timeout         : -
  User-group           : -
  Original-password    : No
  Password-set-time    : 2019-12-01 18:42:57+01:00 DST
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
  Last login ip        : 192.168.240.235
  Last login time      : 2019-03-21 09:38:24+08:00
  Login fail count     : 0
  Password expire in   : -
  Ftp-privilege        : write
```

NOTE

For a local user who fails to log in to the device but is not locked, **Retry-time-left** is displayed. For a local user whose initial password is changed, **Change password retry-count-left** is displayed. When the number of continuous login failures or the number of initial password change failures reaches the limit specified using the **local-aaa-user wrong-password** command, the user is locked.

When the number of user login failures or the number of initial password change failures does not reach the limit specified using the **local-aaa-user wrong-password** command, the user is not locked. If the limit is changed using the **local-aaa-user wrong-password** command, and the new limit is smaller than the number of user login failures or the number of initial password change failures, the user still has a change to try to log in to the device or change the password. In this case, **Retry-time-left** or **Change password retry-count-left** is displayed as 1.

Display information about local user **user1** who fails to log in to the device.

```
<HUAWEI> display local-user username
user1
  The contents of local user(s):
  Password             : ****************
  State                : active
  Service-type-mask    : T
  Privilege level      : 0
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 0
  Idle-timeout         : -
  Retry-interval       : 4 Min(s)
  Retry-time-left      : 1
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
  Password expire in   : -
  Ftp-privilege        : write
```

Display information about local user **user1** whose initial password fails to be changed.

```
<HUAWEI> display local-user username user1
  The contents of local user(s):
  Password             : ****************
  State                : active
  Service-type-mask    : T
  Privilege level      : 0
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 1
  Idle-timeout         : -
  Change password retry-interval  : 4 Min(s)
  Change password retry-count-left: 3
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
  Password expire in   : -
  Ftp-privilege        : write
```

Display information about local users in blocking state.

```
<HUAWEI> display local-user state block
  ----------------------------------------------------------------------------
  User-name                  State  AuthMask  AdminLevel
BlockTime
  ----------------------------------------------------------------------------
  test2                      B      T         0           2018-04-10 01:55:11-00:00
```

```
 -------------------------------------------------------------------------------
 Total 1 user(s)
```

Display information about local user **test2** in blocking state.

```
<HUAWEI> display local-user state block username test2
 The contents of local user(s):
 Password             : ****************
 State                : block
 Service-type-mask    : T
 Privilege level      : 0
 Ftp-directory        : -
 HTTP-directory       : -
 Access-limit         : -
 Accessed-num         : 0
 Idle-timeout         : -
 Block-time-left      : 8 Min(s)
 Original-password    : Yes
 Password-set-time    : 2019-01-27 13:26:55+08:00
 Password-expired     : No
 Password-expire-time : -
 Account-expire-time  : -
 Password expire in   : -
 Ftp-privilege        : write
```

Table 13-13 Description of the **display local-user** command output

Item	Description
User-name	Name of the local user. To configure this parameter, run the **local-user** command.
State	State of the local user: ● A: Active ● B: Block To configure this parameter, run the **local-user** command.

Item	Description
AuthMask	Access type of the local user. ● T: indicates the Telnet users. ● M: indicates the terminal users, which usually refer to the console users. ● S: indicates the SSH users. ● F: indicates the FTP users. ● W: indicates the web users. ● X: indicates the 802.1X users. ● A: indicates all access types. ● H: indicates the HTTP users. ● D: indicates the X25-PAD users. ● P: indicates the PPP users. ● Combination: For example, MH indicates either a terminal user or an HTTP user. ● I: indicates the API user, which is typically used for NETCONF access. To configure this parameter, run the **local-user service-type** command.
AdminLevel	Local user level. To configure this parameter, run the **local-user** command.
Password	Password of the local user. To configure this parameter, run the **local-user** command.
Service-type-mask	Service type of the local user. Same as the AuthMask type. To configure this parameter, run the **local-user service-type** command.
Privilege level	Local user level. To configure this parameter, run the **local-user** command.
Ftp-directory	FTP directory of the local user. To configure this parameter, run the **local-user** command.
Ftp-privilege	The Permission to operate the FTP directory of the local user. To configure this parameter, run the **local-user username ftp-privilege** command.

Item	Description
HTTP-directory	HTTP directory of the local user. To configure this parameter, run the **local-user** command.
Access-limit	Whether the maximum number of sessions of the local user is configured. To configure this parameter, run the **local-user** command.
Access-limit-max	Maximum number of sessions of the local user. To configure this parameter, run the **local-user** command.
Accessed-num	Number of established sessions.
Idle-timeout	Idle timeout interval. To configure this parameter, run the **local-user** command.
User-group	Authorization information of the user group to which the local user is bound. To configure this parameter, run the **local-user** command.
Original-password	Whether the password of a local user is the initial password: ● Yes ● No To configure this parameter, run the **password alert original** command.
Password-set-time	Time when the local user's password is created. The value is in format local time + DST offset.
Password-expired	Whether a local user's password has expired: ● Yes ● No
Password-expire-time	Time when the local user's password expires. The value is in format local time + DST offset. To configure this parameter, run the **password expire** command.
Account-expire-time	Expiry time of a local user account. The value is in format local time + DST offset. To configure this parameter, run the **local-user expire-date** command.
Last login ip	IP address for user login. This item can be displayed only for administrators.

Item	Description
Last login time	User login time. This item can be displayed only for administrators.
Login fail count	Number of user login failures. This item can be displayed only for administrators.
Password expire in	Validity period of the password for a local user to log in to the device.
BlockTime/Block-time-left	Remaining time of locked local users. (Local users are locked because the entered password is incorrect consecutively.)
Retry-interval	Login retry interval before a local user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.
Retry-time-left	Remaining number of login retries before a local user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.
Change password retry-interval	Retry interval for changing the initial password of a local user before the user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.
Change password retry-count-left	Remaining number of initial password change retries before a local user is locked. To configure this parameter, run the **local-aaa-user wrong-password** command.

13.1.47 display local-user expire-time

Function

The **display local-user expire-time** command displays the time when local accounts expire.

Format

display local-user expire-time

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The command output helps you diagnose and rectify the faults related to local user passwords.

Example

Display the time when local accounts expire.

```
<HUAWEI> display local-user expire-time
 -----------------------------------------------------------------------------
 Username              Password-expire      Account-expire          Expired
 -----------------------------------------------------------------------------
 zsh                2014-12-01 21:25:44    -                       NO
 mm001                 2014-12-01 21:29:58    -                       NO
 -----------------------------------------------------------------------------
 Total: 2, printed: 2
```

Table 13-14 Description of the **display local-user expire-time** command output

Item	Description
Username	Local account name. To configure this parameter, run the **local-user** command.
Password-expire	Number of days after which the password expires. To configure this parameter, run the **password expire** command.
Account-expire	Account expiration time. To configure this parameter, run the **local-user expire-date** command.
Expired	Whether the local account has expired: ● YES ● NO **NOTE** The displayed value and actual value may have a difference within one minute; there is a possibility that the password has expired, but the displayed value is **NO**. When the local user account or password has expired, the local user becomes invalid.

13.1.48 display local-aaa-user password policy

Function

The **display local-aaa-user password policy** command displays the password policy of local user.

Format

display local-aaa-user password policy { **access-user** | **administrator** }

Parameters

Parameter	Description	Value
access-user	Indicates the password policy of local access users.	-
administrator	Indicates the password policy of local administrator.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the password policy for local users, you can run the **display local-aaa-user password policy** command to check whether the configuration is correct.

Example

Display the password policy of local access users.

```
<HUAWEI> display local-aaa-user password policy access-user
  Password control                  : Enable
  Password history                  : Enable (history records:5)
```

Table 13-15 Description of the **display local-aaa-user password policy access-user** command output

Item	Description
Password control	Whether the password control function is enabled: - Enable - Disable To configure this function, run the **local-aaa-user password policy access-user** command.

Item	Description
Password history	Whether the historical password recording function is enabled and the maximum number of historical passwords of each user. To configure this function, run the **password history record number** command.

Display the password policy of local administrator.

```
<HUAWEI> display local-aaa-user password policy administrator
  Password control                  : Enable
  Password expiration                : Enable (180 days)
  Password history                  : Enable (history records:5)
  Password alert before expiration : 30 days
  Password alert original           : Enable
```

Table 13-16 Description of the **display local-aaa-user password policy administrator** command output

Item	Description
Password control	Whether the password control function is enabled: ● Enable ● Disable To configure this function, run the **local-aaa-user password policy administrator** command.
Password expiration	Whether the password expiration function is enabled and password expiration time. To configure this function, run the **password expire** command.
Password history	Whether the historical password recording function is enabled and the maximum number of historical passwords of each user. To configure this function, run the **password history record number** command.
Password alert before expiration	Password expiration prompt days. To configure this function, run the **password alert before-expire** command.
Password alert original	Whether the device prompt users to change the initial passwords: ● Enable ● Disable To configure this function, run the **password alert original** command.

13.1.49 display recording-scheme

Function

The **display recording-scheme** command displays the configuration of recording schemes.

Format

display recording-scheme [*recording-scheme-name*]

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display recording-scheme** command displays the configuration of recording schemes.

Example

Display the configuration of the recording scheme **scheme0**.

```
<HUAWEI> display recording-scheme scheme0
-------------------------------------------------------------------
 Recording-scheme-name            : scheme0
 HWTACACS-template-name           : tacas-1
------------------------------------------------------------------
```

Table 13-17 Description of the **display recording-scheme** command output

Item	Description
Recording-scheme-name	Name of the recording scheme. To create a recording scheme, run the **recording-scheme** command.

Item	Description
HWTACACS-template-name	Name of the HWTACACS server template associated with the recording scheme. To associate an HWTACACS server template with a recording scheme, run the **recording-mode hwtacacs** command.

13.1.50 display remote-user authen-fail

Function

The **display remote-user authen-fail** command displays the accounts that fail in remote AAA authentication.

Format

display remote-user authen-fail [**blocked** | **username** *username*]

Parameters

Parameter	Description	Value
blocked	Displays all the remote AAA authentication accounts that have been locked.	-
username *username*	Displays details about the accounts that fail in remote AAA authentication. If the *username* parameter is not specified, basic information about all accounts that fail in remote AAA authentication is displayed.	It is a string of 1 to 253 case-insensitive characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the account locking function is enabled for the users who fail in AAA remote authentication, the device records all failed accounts, including:

- The accounts that failed in authentication and are locked, for example, when the user entered the wrong account name or password too many times.
- The accounts that failed in authentication, but are not locked, for example, when the number of times the account name or password was entered incorrectly did not exceed the limit.

Prerequisites

The **access-user remote authen-fail** command has been executed to enable the account locking function for access users who fail remote authentication. Alternatively, the **administrator remote authen-fail** command has been executed to enable the account locking function for administrators who fail remote authentication.

Precautions

The device cannot back up a recorded account that fails the AAA authentication. If an active/standby switchover policy has been configured on the device, all user entries are cleared when the device completes an active/standby switchover.

Example

Display all accounts that have failed in remote AAA authentication.

```
<HUAWEI> display remote-user authen-fail
  Interval: Retry Interval(Mins)
  TimeLeft: Retry Time Left
  BlockDuration: Block Duration(Mins)
  -------------------------------------------------------------------------------------------
  Username                Interval  TimeLeft  BlockDuration  UserType
  -------------------------------------------------------------------------------------------
  www@test                 0         0         65414          administrator
  -------------------------------------------------------------------------------------------
  Total 1, 1 printed
```

Display all locked accounts.

```
<HUAWEI> display remote-user authen-fail blocked
Interval: Retry Interval(Mins)
TimeLeft: Retry Time Left
BlockDuration: Block Duration(Mins)
--------------------------------------------------------------------------------------------------------
Username                Interval  TimeLeft  BlockDuration  BlockTime                  UserType
--------------------------------------------------------------------------------------------------------
www@test                 0         0         65414          2018-04-23 17:22:09+08:00 administrator
--------------------------------------------------------------------------------------------------------
Total 1, 1 printed
```

Display details about the account **test** that failed in remote AAA authentication.

```
<HUAWEI> display remote-user authen-fail username test
  The contents of the user:
  User-type              : Administrator
  Retry interval(Mins)   : 29
  Retry time left        : 4
  Block time left(Mins) : 0
  User state             : Block
```

Table 13-18 Description of the **display remote-user authen-fail** command output

Item	Description
Username	User name.
Interval or Retry interval(Mins)	Authentication retry interval, in minutes. To configure this parameter, run the **access-user remote authen-fail** or **administrator remote authen-fail** command.
TimeLeft or Retry Time Left	Remaining number of consecutive authentication failures. To configure this parameter, run the **access-user remote authen-fail** or **administrator remote authen-fail** command.
BlockDuration or Block time left(Mins)	User account locking duration, in minutes. To configure this parameter, run the **access-user remote authen-fail** or **administrator remote authen-fail** command.
UserType	User type: ● administrator ● access-user
BlockTime	User account locking time.
Block-time-left	Remaining locking time of an account.
User-state	User status: ● Block ● Active

13.1.51 display security weak-password-dictionary

Function

The **display security weak-password-dictionary** command displays information about weak passwords on the device.

Format

display security weak-password-dictionary

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a weak password dictionary is loaded to the device, you can run this command to view information about weak passwords on the device.

Example

Display information about the weak password dictionary on the device.

```
<HUAWEI> display security weak-password-dictionary
-------------------------------------------------------------------------------
 Weak Password
-------------------------------------------------------------------------------
 test1
 test2
 test3
-------------------------------------------------------------------------------
 Total: 3
```

Table 13-19 Description of the **display security weak-password-dictionary** command output

Item	Description
Weak Password	Weak password.

13.1.52 display service-scheme

Function

The **display service-scheme** command displays the configuration of service schemes.

Format

display service-scheme [**name** *name*]

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a service scheme.	The service scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display service-scheme** command displays the configuration of service schemes.

Before applying a service scheme to a domain, run the **display service-scheme** command to check whether the service scheme is correct.

Precautions

The **display service-scheme** command displays the detailed configuration if the command is executed in the service scheme view or the name of a service scheme is specified. Otherwise, this command displays only the summary of service schemes.

Example

Display information about all service schemes.

```
<HUAWEI> display service-scheme
 -------------------------------------------------------------------
 service-scheme-name                    scheme-index
 -------------------------------------------------------------------
 svcscheme1                           0
 svcscheme2                           1
 -------------------------------------------------------------------
 Total of service scheme: 2
```

Display the configuration of the service scheme **svcscheme1**.

```
<HUAWEI> display service-scheme name svcscheme1

 service-scheme-name            : svcscheme1
 service-scheme-primary-dns     : -
 service-scheme-secondary-dns  : -
 service-scheme-adminlevel      : 15
 service-scheme-uclgroup-ID     : 10
 service-scheme-uclgroup-name  : u1
 service-scheme-acl-id          : 3001
 service-scheme-ipv6-acl-id     : 3001
 service-scheme-redirect-acl-id: 3001
 service-scheme-vlan            : 10
 service-scheme-priority        : 0
 service-scheme-voicevlan       : enable
 access-limit-username-maxnum  : 10
 service-scheme-qosprofile      : -
 service-scheme-sacprofile      : -
 service-scheme-idlecut-time   : 10
 service-scheme-idlecut-flow   : 20
 service-scheme-idlecut-direct : Inbound and Outbound
```

Table 13-20 Description of the **display service-scheme** command output

Item	Description
service-scheme-name	Name of a service scheme. To create a service scheme, run the **service-scheme (AAA view)** command.
scheme-index	Index of a service scheme.
service-scheme-primary-dns	Address of the primary DNS server. To configure this item, run the **dns** command.
service-scheme-secondary-dns	Address of the secondary DNS server. To configure this item, run the **dns** command.
service-scheme-adminlevel	Level of an administrator. To configure this item, run the **admin-user privilege level** command.
service-scheme-uclgroup-ID	Index of the bound UCL group. To configure this item, run the **ucl-group** command.
service-scheme-uclgroup-name	Name of the bound UCL group. To configure this item, run the **ucl-group** command.
service-scheme-acl-id	Bound ACL number. To configure this item, run the **acl-id** command.
service-scheme-ipv6-acl-id	Bound IPv6 ACL number. To configure this item, run the **acl-id** command.
service-scheme-redirect-acl-id	Number of the ACL used for redirection in the service scheme. To configure this item, run the **redirect-acl** command.
service-scheme-vlan	User VLAN ID. To configure this item, run the **user-vlan** command.
service-scheme-priority	User priority in the service scheme. To configure this item, run the **priority** command.
service-scheme-voicevlan	Whether voice VLAN is enabled. To configure this item, run the **voice-vlan** command.
access-limit-username-maxnum	Maximum number of users who are allowed to access the network using the same user name. To configure this item, run the **access-limit user-name max-num** command.

Item	Description
service-scheme-qosprofile	Name of the bound QoS profile. To configure this item, run the **qos-profile** command.
service-scheme-sacprofile	Name of the bound SAC profile. To configure this item, run the **sac-profile (service scheme view)** command.
service-scheme-idlecut-time	Idle-cut timeout interval, in minutes. To configure this item, run the **idle-cut** command.
service-scheme-idlecut-flow	Threshold for idle-cut traffic, in Kbytes. To configure this item, run the **idle-cut** command.
service-scheme-idlecut-direct	Direction in which idle-cut takes effect for traffic: ● Inbound: Idle-cut takes effect for uplink traffic. ● Outbound: Idle-cut takes effect for downlink traffic. ● Inbound and Outbound: Idle-cut takes effect for uplink and downlink traffic. To configure this item, run the **idle-cut** command.

13.1.53 display vlan pool

Function

The **display vlan pool** command displays configuration of VLAN pools.

Format

display vlan pool { **name** *pool-name* | **all** [**verbose**] }

Parameters

Parameter	Description	Value
name *pool-name*	Displays configuration of a specified VLAN pool.	The VLAN pool must exist.
all [**verbose**]	Displays configuration of all VLAN pools. List of VLANs in the VLAN pool will be displayed if **verbose** is specified.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configuration of VLAN pools, which facilitates VLAN pool management and maintenance.

Example

Display brief configuration of all VLAN pools.

```
<HUAWEI> display vlan pool all
--------------------------------------------------------------------------------
Name                          Assignment                        VLAN total
--------------------------------------------------------------------------------
name                         hash                         0
test                       hash                        128
marketing                     hash                         2
--------------------------------------------------------------------------------
Total: 3
```

Table 13-21 Description of the **display vlan pool all** command output

Item	Description
Name	Name of a VLAN pool. To configure the parameter, run the **vlan pool** command.
Assignment	VLAN assignment algorithm in a VLAN pool: ● even: The VLAN assignment algorithm is **even**. ● hash: The VLAN assignment algorithm is **hash**. To configure the parameter, run the **assignment** command.
VLAN total	Number of VLANs in the VLAN pool.
Total	Total number of VLAN pools.

Display configuration of the VLAN pool **test**.

```
<HUAWEI> display vlan pool name test
--------------------------------------------------------------------------------
Name                  : test
Total                 : 21
Assignment            : hash
VLAN Block Time(min)  : 10
Threshold Notify Count: 5
VLAN ID               : 10 to 30
Blocked VLAN ID       : -
--------------------------------------------------------------------------------
```

Table 13-22 Description of the **display vlan pool name** *pool-name* command output

Item	Description
Name	Name of the VLAN pool. To configure the parameter, run the **vlan pool** command.
Total	Number of VLANs in the VLAN pool.
Assignment	VLAN assignment algorithm in a VLAN pool: ● even: The VLAN assignment algorithm is **even**. ● hash: The VLAN assignment algorithm is **hash**. To configure the parameter, run the **assignment** command.
VLAN Block Time(min)	Lockout time of VLANs, in minutes. To configure the parameter, run the **vlan block-time** command. If the default lockout time is used, this field is not displayed.
Threshold Notify Count	Number of times the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN. To configure the parameter, run the **dhcp update vlan assignment threshold** command. If the default parameter value is used, this field is not displayed.
VLAN ID	List of VLANs in the VLAN pool. To configure the parameter, run the **vlan (VLAN pool view)** command.
Blocked VLAN ID	List of VLANs that are locked. After the **dhcp update vlan assignment** command is run, a VLAN is locked and cannot be assigned to users within the specified lockout time if all IP addresses in the VLAN have been assigned. **NOTE** This field takes effect only for wired users. To check the VLAN list of wireless users, run the **display vlan pool name status** command.

13.1.54 dhcp update vlan assignment

Function

The **dhcp update vlan assignment** command enables the function of reassigning VLANs in a VLAN pool.

The **undo dhcp update vlan assignment** command disables the function of reassigning VLANs in a VLAN pool.

By default, the function of reassigning VLANs in a VLAN pool is disabled.

Format

dhcp update vlan assignment

undo dhcp update vlan assignment

Parameters

None

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VLAN assignment algorithm is **hash**, the VLAN pool assigns VLANs to users based on the hash results of the users' MAC addresses. If the hash results of multiple MAC addresses are the same, available IP addresses in a specific VLAN may be insufficient. To solve this problem, run the **dhcp update vlan assignment** command to lock the VLAN in which all IP addresses have been assigned for a period of time so that the device selects another VLAN from the VLAN pool to assign IP addresses.

Prerequisites

The VLAN assignment algorithm has been set to **hash** using the **assignment hash** command.

Precautions

Before configuring this function, enable DHCP snooping on the interface through which users go online.

This function takes effect only for wired users.

Authentication access devices in the policy association scenario do not support this function.

After the **assignment even** command is run, the **assignment hash** command configuration will be cleared. Exercise caution when running the **assignment even** command.

The locked VLAN will be unlocked in advance if any of the following operations is performed:

- Run the **assignment even** command in the VLAN pool view to set the VLAN assignment algorithm to **even**.
- Run the **undo vlan** command in the VLAN pool view to delete the VLAN from the VLAN pool.
- Run the **undo dhcp update vlan assignment** command in the VLAN pool view to disable the function of reassigning VLANs in the VLAN pool.

Example

Enable the function of reassigning VLANs in a VLAN pool.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment hash
[HUAWEI-vlan-pool-test] dhcp update vlan assignment
```

13.1.55 dhcp update vlan assignment interval

Function

The **dhcp update vlan assignment interval** command sets the interval at which the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.

The **undo dhcp update vlan assignment interval** command restores the default value.

By default, if the number of times that the VLAN pool module receives the notification from the DHCP module within 3 minutes reaches the value specified using the **dhcp update vlan assignment threshold** command, the VLAN is locked.

NOTE

This command is supported only on the This feature is supported only by the following models: S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

dhcp update vlan assignment interval *interval-value*

undo dhcp update vlan assignment interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.	The value is an integer in the range of 0 to 1440, in minutes. The default value is 3. If the parameter value is set to 0, the VLAN locking function does not take effect.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VLAN assignment algorithm is **hash**, the VLAN pool assigns VLANs to users based on the hash results of the users' MAC addresses. If the function of reassigning VLANs in the VLAN pool is enabled on the device, the DHCP module notifies the VLAN pool module that a user fails to obtain an IP address from the IP address pool for a specific VLAN when the user cannot obtain an IP address from the address pool.

To set the interval at which the VLAN pool module receives such a notification, run the **dhcp update vlan assignment interval** command. When the VLAN pool module receives the notification from the DHCP module for the number of times specified using the **dhcp update vlan assignment threshold** command within the specified period, the corresponding VLAN is locked for a period of time. The device then re-authorizes an available VLAN in the VLAN pool to the user. If all VLANs in the VLAN pool are locked, the device authorizes the user with the default VLAN for the interface through which the user goes online.

Precautions

This function takes effect only for wireless users.

Authentication access devices in the policy association scenario do not support this function.

Example

Configure the device to lock a VLAN after the VLAN pool module receives a notification from the DHCP module three times within 5 minutes, indicating that wireless users fail to obtain IP addresses from the IP address pool for the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] dhcp update vlan assignment threshold 3
[HUAWEI-vlan-pool-test] dhcp update vlan assignment interval 5
```

13.1.56 dhcp update vlan assignment threshold

Function

The **dhcp update vlan assignment threshold** command sets the number of times the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.

The **undo dhcp update vlan assignment threshold** command restores the default value.

By default, when the VLAN pool module receives a notification from the DHCP module three times, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN, the VLAN is locked.

Format

dhcp update vlan assignment threshold *count*

undo dhcp update vlan assignment threshold

Parameters

Parameter	Description	Value
count	Specifies the number of times that the VLAN pool module receives a notification from the DHCP module, indicating that users fail to obtain IP addresses from the IP address pool for a specific VLAN.	The value is an integer in the range of 1 to 255. The recommended value is 3.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VLAN assignment algorithm is **hash**, the VLAN pool assigns VLANs to users based on the hash results of the users' MAC addresses. If the function of reassigning VLANs in the VLAN pool is enabled on the device, the DHCP module notifies the VLAN pool module that a user fails to obtain an IP address from the IP address pool for a specific VLAN when the user cannot obtain an IP address from the address pool.

To set the number of times the VLAN pool module receives such a notification from the DHCP module, run the **dhcp update vlan assignment threshold** command. When the number of times that the VLAN pool module receives the notification from the DHCP module reaches the configured value, the VLAN is locked for a certain period. The device then authorizes the user with an available VLAN in the VLAN pool. If all VLANs in the VLAN pool are locked, the device authorizes the user with the default VLAN for the interface through which the user goes online.

Prerequisites

For wired users, you must run the **assignment hash** command to set the VLAN assignment algorithm to hash. For wireless users, the device must support the WLAN-AC function.

Precautions

For wireless users, you can also run the **dhcp update vlan assignment interval** command to configure the interval at which the VLAN pool module receives such a notification from the DHCP module. Otherwise, the default interval is used.

Before configuring this function for wired users, run the **dhcp update vlan assignment** command to enable the function of reassigning VLANs in the VLAN pool. Otherwise, the function of locking a specific VLAN does not take effect.

Before enabling the function of reassigning VLANs in the VLAN pool for wired users, you need to enable DHCP snooping on the interface through which users go online.

Authentication access devices in the policy association scenario do not support this function.

Example

Configure the device to lock a VLAN after the VLAN pool module receives a notification from the DHCP module five times, indicating that wired users fail to obtain IP addresses from the IP address pool for the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment hash
[HUAWEI-vlan-pool-test] dhcp update vlan assignment
[HUAWEI-vlan-pool-test] dhcp update vlan assignment threshold 5
```

Configure the device to lock a VLAN after the VLAN pool module receives a notification from the DHCP module five times within 4 minutes, indicating that wireless users fail to obtain IP addresses from the IP address pool for the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] dhcp update vlan assignment threshold 5
[HUAWEI-vlan-pool-test] dhcp update vlan assignment interval 4
```

13.1.57 dns (service scheme view)

Function

The **dns** command configures the primary or secondary DNS server in a service scheme.

The **undo dns** command cancels the configuration of the primary or secondary DNS server in a service scheme.

By default, no primary or secondary DNS server is configured in a service scheme.

Format

dns *ip-address* [**secondary**]

undo dns [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the DNS server.	The value is a valid unicast address in dotted decimal notation.
secondary	Indicates the secondary DNS server.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

If no DNS server is specified when a local address pool, DHCP server, or RADIUS server assigns IP addresses to users, the DNS server configured in the service scheme view is used.

Example

Set the IP address of the primary DNS server in the service scheme **svcscheme1** to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] dns 10.10.10.1
```

Set the IP address of the secondary DNS server in the service scheme **svcscheme1** to 10.10.20.1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] dns 10.10.20.1 secondary
```

13.1.58 domain (AAA view)

Function

The **domain** command creates a domain and displays its view.

The **undo domain** command deletes a domain.

By default, the device has two domains: **default** and **default_admin**. The two domains can be modified but cannot be deleted.

Format

domain *domain-name* [**domain-index** *domain-index*]

undo domain *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a domain.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces or the following symbols: * ? ". The value cannot be - or --.
domain-index *domain-index*	Specifies the index of a domain.	The value is an integer that ranges from 0 to 31.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can manage users through domains. A domain is the minimum user management unit. A domain name can be an ISP name or the name of a service provided by an ISP. A domain can use the default authorization attribute, and be configured with a RADIUS template and authentication and accounting schemes.

If the domain to be configured already exists, the **domain** command displays the domain view.

Running the **undo domain** command to delete a domain will cause online users that belong to this domain to go offline. Confirm the operation before running this command.

Prerequisites

To perform AAA for access users, you need to apply the authentication schemes, authorization schemes, and accounting schemes in the domain view. Therefore, authentication, authorization, and accounting schemes must be configured in the AAA view in advance.

Precautions

- The domain **default** is a global default common domain for user access, for example, NAC. By default, the domain is activated, and is bound to the authentication scheme **radius** and accounting scheme **default**, but is not bound to any authorization scheme.

- The domain **default_admin** is a global default management domain for users who log in to the device through HTTPS, SSH, Telnet, and the Web system, namely, administrators. By default, the domain is activated, and is bound to the authentication scheme **default** and accounting scheme **default**, but is not bound to any authorization scheme.

Example

Specify the domain named **domain1** and access the domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain domain1
[HUAWEI-aaa-domain-domain1]
```

13.1.59 domain (system view)

Function

The **domain** command configures a global default domain.

The **undo domain** command restores the default setting.

By default, there are two global default domains: common domain **default** and administrative domain **default_admin**. The former is used as the global default domain of access users, while the latter as the global default domain of administrators.

Format

Common domain **default**:

domain *domain-name*

undo domain

Administrative domain **default_admin**:

domain *domain-name* **admin**

undo domain admin

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a global default domain.	The domain must already exist.

Parameter	Description	Value
admin	Configures a domain for administrators. If this parameter is not specified, the domain for common access users is configured.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the global default domain is configured, a user must be managed by the global default domain if their domain cannot be identified.

Precautions

You must create a domain before configuring the domain as the global default domain.

Example

Create domain **abc** and configure it as the global default common domain.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain abc
[HUAWEI-aaa-domain-abc] quit
[HUAWEI-aaa] quit
[HUAWEI] domain abc
```

13.1.60 domain-location

Function

The **domain-location** command configures the position of a domain name.

The **undo domain-location** command restores the default position of a domain name.

By default, the domain name in the AAA view is placed behind the domain name delimiter, and no position is configured in the authentication profile view.

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command in the authentication profile view.

Format

domain-location { **after-delimiter** | **before-delimiter** }

undo domain-location

Parameters

Parameter	Description	Value
after-delimiter	Indicates that the domain name is placed behind the domain name delimiter.	-
before-delimiter	Indicates that the domain name is placed before the domain name delimiter.	-

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

The format of a user name is **user name@domain name**. If **before-delimiter** is specified, the format **domain name@user name** is used.

You can use the **domain-location** command only when there is no online user.

Precautions

If you run the **domain-location** command in the AAA view, the position of a domain is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the domain name before the domain name delimiter.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain-location before-delimiter
```

13.1.61 domain-name-delimiter

Function

The **domain-name-delimiter** command configures a domain name delimiter.

The **undo domain-name-delimiter** command restores the default domain name delimiter.

By default, the domain name delimiter in the AAA view is @, and no delimiter is available in the authentication profile view.

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command in the authentication profile view.

Format

domain-name-delimiter *delimiter*

undo domain-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a domain name delimiter of only one bit.	The value can only be one of the following characters: \ / : < > | @ ' %.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

Different AAA servers may use different domain name delimiters. To ensure that an AAA server obtains the correct user name and domain name, configure the same domain name delimiter on the device and the AAA server.

For example, if the domain name delimiter is %, the user name of **user1** in the domain **dom1** is **user1%dom1** or **dom1%user1**.

Precautions

Before using the **domain-name-delimiter** command, ensure that no local user exists.

If you run the **domain-name-delimiter** command in the AAA view, the domain name delimiter is configured globally and the configuration takes effect for all users.

The delimiter for a security string cannot be the same as the domain name delimiter.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the domain name delimiter as / in the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain-name-delimiter /
```

13.1.62 domainname-parse-direction

Function

The **domainname-parse-direction** command configures the direction in which a domain name is parsed.

The **undo domainname-parse-direction** command restores the default direction in which a domain name is parsed.

By default, the domain name is parsed in the AAA view from left to right, and no direction is configured in which a domain name is parsed.

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command in the authentication profile view.

Format

domainname-parse-direction { **left-to-right** | **right-to-left** }

undo domainname-parse-direction

Parameters

Parameter	Description	Value
left-to-right	Parses a domain name form left to right.	-
right-to-left	Parses a domain name form right to left.	-

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

In AAA implementations, users belong to different domains. A network access server (NAS) centrally manages users in a domain. During a user's login, the NAS parses the entered user name. A user is authenticated only when the user has the correct user name and domain name. When configuring an AAA scheme, run the **domainname-parse-direction** { **left-to-right** | **right-to-left** } command to configure the direction in which a domain name is parsed.

Assume that the user name is **username@dom1@dom2**.

- If the **domain-location** command configures the domain name behind the domain name delimiter:
  - When **left-to-right** is specified, the user name is **username** and the domain name is **dom1@dom2**.
  - When **right-to-left** is specified, the user name is **username@dom1** and the domain name is **dom2**.
- If the **domain-location** command configures the domain name before the domain name delimiter:
  - When **left-to-right** is specified, the user name is **dom1@dom2** and the domain name is **username**.
  - When **right-to-left** is specified, the user name is **dom2** and the domain name is **username@dom1**.

Precautions

If you run the **domainname-parse-direction** command in the AAA view, the direction in which a domain name is parsed is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the device to parse a domain name from right to left in the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domainname-parse-direction right-to-left
```

13.1.63 hash mac-vlan lease

Function

The **hash mac-vlan lease** command sets the aging time of user entries in a VLAN pool.

The **undo hash mac-vlan lease** command restores the default configuration.

By default, the aging time of user entries in a VLAN pool is 8 days.

Format

hash mac-vlan lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo hash mac-vlan lease

Parameters

Parameter	Description	Value
day *day*	Specifies the aging time, in days.	The value is an integer in the range from 0 to 999, in days. The default value is 8 days.
hour *hour*	Specifies the aging time, in hours.	The value is an integer in the range from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the aging time, in minutes.	The value is an integer in the range from 0 to 59, in minutes. The default value is 0.
unlimited	Indicates that entries will not be aged.	-

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

To ensure that an offline user still belongs to the original VLAN when the user goes online again, the device records the mapping between the user MAC address and the VLAN. When the user goes online again, the system searches for a matching entry to determine the VLAN to which the user once belonged. If the entry exists and the number of users in the VLAN does not reach the upper limit, the user still belongs to the original VLAN. If the entry does not exist or the number of users in the VLAN reaches the upper limit, the system assigns another available VLAN to the user. To adjust the aging time of entries, run the **hash mac-vlan lease** command.

NOTE

- The **hash mac-vlan lease** command takes effect only for users authorized a VLAN pool.
- The **hash mac-vlan lease** command takes effect only when the VLAN assignment algorithm of a VLAN pool is **hash**.
- The aging time takes effect only for entries of offline users.
- The configured aging time must be greater than or equal to 10 minutes.

Example

Set the aging time of offline user entries in a VLAN pool to 7 days.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] hash mac-vlan lease day 7
```

13.1.64 idle-cut (service scheme view)

Function

The **idle-cut** command enables the idle-cut function for domain users and sets the idle-cut parameters.

The **undo idle-cut** command disables the idle-cut function.

By default, the idle-cut function is disabled for domain users.

Format

idle-cut *idle-time flow-value* [**inbound** | **outbound**]

undo idle-cut

Parameters

Parameter	Description	Value
idle-time	Specifies the period in which an idle user can stay online.	The value is an integer that ranges from 1 to 1440, in minutes.
flow-value	Specifies the traffic threshold for idle-cut function. When the traffic of a user stays below this threshold for a certain period, the device considers that the user is in idle state.	The value is an integer that ranges from 0 to 4294967295, in Kbytes.
inbound	Indicates that the idle-cut function takes effect for only upstream traffic of users.	-
outbound	Indicates that the idle-cut function takes effect for only downstream traffic of users. **NOTE** If neither **inbound** nor **outbound** is specified, the idle-cut function takes effect for both upstream and downstream traffic. In addition, if only the traffic in one direction meets the idle-cut condition (the traffic volume is less than the threshold specified by *flow-value* within the time specified by *idle-time*), the idle-cut function takes effect and the user connection is disconnected.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user uses no or a little network traffic for a long time, the user still occupies certain bandwidth, which reduces access rate of other users. The idle-cut function disconnects the users whose traffic volume stays below the traffic threshold within the idle time, to save resources and improve service experience of other users.

Precautions

- The **idle-cut** command configured in the service scheme view takes effect only for wireless users.
- When idle-cut in the service scheme view and RADIUS attribute 28 (Idle-Timeout) delivered by the remote RADIUS server exist simultaneously, RADIUS

attribute 28 has a higher priority. RADIUS attribute 28 can be used together with the traffic and direction configured using this command.

Example

Enable the idle-cut function for the domain, and set the idle time to 1 minute and the traffic threshold to 10 Kbytes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] idle-cut 1 10
```

13.1.65 local-aaa-user wrong-password

Function

The **local-aaa-user wrong-password** command enables local account locking function and sets the retry interval, consecutive incorrect password attempts, and locking duration.

The **undo local-aaa-user wrong-password** command disables local account locking function.

By default, the local account locking function is enabled, retry interval is 5 minutes, maximum number of consecutive incorrect password attempts is 3, and account locking period is 5 minutes.

Format

local-aaa-user wrong-password retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo local-aaa-user wrong-password

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the retry interval of a local account.	The value is an integer that ranges from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the consecutive incorrect password attempts.	The value is an integer that ranges from 3 to 65535.
block-time *block-time*	Specifies the local account locking duration. In actual application, there is a one minute difference in locking time.	The value is an integer that ranges from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the following scenarios:

- The command locks a local account to improve password security of the local user. If the password is entered incorrectly more than a certain number of times within the given retry period, the account is locked. The device does not authenticate the user when the account is locked.
- The command locks a local account to ensure that the password will not be cracked by a brute force from a malicious user. When attempting to change the password, if the original password is entered incorrectly more than a certain number of times within the given retry period, the account is locked. The user cannot modify the password when the account is locked.

Follow-up Procedure

After a local account is locked, you can run the **local-user** *user-name* **state active** command to unlock the local account.

Precautions

Only entering the incorrect password can lock the account. Other local authentication failures will not lock the account.

When the number of login failures or initial password change failures of the local user does not reach the limit specified using the **local-aaa-user wrong-password** command, the user is not locked. In this case, if the limit is changed using the **local-aaa-user wrong-password** command and the new limit is smaller than the number of login failures or initial password change failures of the user, the user still has a chance to log in to the device or change the password.

Example

Enable local account locking, and set the authentication retry interval to 5 minutes, maximum number of consecutive incorrect password attempts to 3, and account locking period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
```

13.1.66 local-user

Function

The **local-user** command creates a local user and sets parameters of the local user.

The **undo local-user** command deletes a local user.

By default, no local user is created. The privilege level of a new local user is 0, and no service type is configured.

Format

local-user *user-name* { **password** { **cipher** | **irreversible-cipher** } *password* [**old-password** *old-password*] | **access-limit** *max-number* | **ftp-directory** *directory* | **idle-timeout** *minutes* [*seconds*] | **privilege level** *level* | **state** { **block** | **active** } | **user-group** *group-name* } *

local-user *user-name* **http-directory** *directory*

undo local-user *user-name* [**access-limit** | **ftp-directory** | **http-directory** | **idle-timeout** | **privilege level** | **user-group**]

Parameters

Parameter	Description	Value
user-name	Specifies the user name. If the user name contains a domain name delimiter such as @, the character before @ is the user name and the character behind @ is the domain name. If the value does not contain @, the entire character string is the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Parameter	Description	Value

		NOTE
		● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		● Note the following when configuring case sensitivity for user names:
		  ● Only the user name is case-sensitive and the domain name is case-insensitive.
		  ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user

Parameter	Description	Value
password { **cipher** | **irreversible-cipher** } *password*	Specifies the password of a local user. - The **cipher** parameter indicates that the user password is encrypted using the reversible encryption algorithm. Unauthorized users can obtain the plain text by using the corresponding decryption algorithm, leading to low security. When the **cipher** parameter is specified, the AES reversible encryption algorithm is used. - The **irreversible-cipher** parameter indicates that the user password is encrypted using the irreversible encryption algorithm. Unauthorized users cannot obtain the plain text by using the decryption algorithm, ensuring user security. When the **irreversible-cipher** parameter is specified, the Scrypt irreversible encryption algorithm is used.	The value is a case-sensitive character string without question marks (?), single quotation marks ('), and spaces. - If the **cipher** parameter is specified, the value of *password* can be a cleartext password of 8 to 128 characters or a ciphertext password of 48, 68, 88, 108, 128, 148, 168, or 188 characters. - If the **irreversible-cipher** parameter is specified, the value of *password* can be a cleartext password of 8 to 128 characters or a ciphertext password of 68 characters. A simple password may bring security risks. The cleartext password entered by a user must contain at least two types of the following characters: uppercase letters, lowercase letters, digits, and special characters. In addition, the password cannot repeat or reverse the user name.

Parameter	Description	Value
	NOTE - It is recommended that you set the user password when creating a user. The interaction method using the **local-user password** command is recommended. - If a user is allowed to encrypt the local user password using the irreversible encryption algorithm, the device does not support CHAP authentication for the user. - In V200R019C10 and later versions, if the local user password is encrypted using irreversible algorithms, the **password** configuration of the local user will be lost and cannot be restored after a downgrade to a version earlier than V200R019C10.	
old-password *old-password*	Specifies the old password of a local user.	The value is a case-sensitive character string without question marks (?), single quotation marks ('), and spaces. The value is a string of 1 to 128 characters in plain text.
access-limit *max-number*	Specifies the number of connections that can be created with a specified user name. If this parameter is not specified, a user can establish a maximum of 4294967295 connections by default.	The value is an integer that ranges from 1 to 4294967295. The actual number of connections is the smaller value between *max-number* and the maximum number of users of a specific type on different models.

Parameter	Description	Value
ftp-directory *directory*	Specifies the directory that an FTP user is allowed to access. If this parameter is not specified, the FTP directory of the local user is empty. The device will check whether the default FTP directory is configured using the **set default ftp-directory** command. If no FTP directory exists, FTP users cannot log in to the device. **NOTE** Ensure that the configured FTP directory is an absolute path; otherwise, the configuration does not take effect.	The value is a string of 1 to 64 case-sensitive characters without spaces.
http-directory *directory*	Specifies the directory that HTTP users are allowed to access. If this parameter is not specified, the HTTP directory of the local user is empty.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Parameter	Description	Value
idle-timeout *minutes* [*seconds*]	Specifies the timeout period for disconnection of the user. - *minutes* is the period when the user interface is disconnected in minutes. - *seconds* is the period when the user interface is disconnected in seconds. If this parameter is not specified, the device uses the idle timeout interval configured by the **idle-timeout** command in the user interface view. If *minutes* [*seconds*] is set to **0 0**, the idle disconnection function is disabled. **NOTICE** If the idle timeout interval is set to 0 or a large value, the terminal will remain in the login state, resulting in security risks. You are advised to run the **lock** command to lock the current connection.	*minutes*: The value is an integer ranging from 0 to 35791 minutes. *seconds*: The value is an integer ranging from 0 to 59 seconds.
privilege level *level*	Specifies the privilege level of a local user. After logging in to the device, a user can run only the commands of the same privilege level or lower privilege levels. **NOTE** If this parameter is not specified, the privilege level of a local user is 0. The permission of API users is not controlled by this parameter. Therefore, you do not need to configure this parameter.	The value is an integer that ranges from 0 to 15. The greater the value, the higher the privilege level of a user.

Parameter	Description	Value
state { **active** | **block** }	Indicates the state of a local user. - **active** indicates that a local user is in active state. The device accepts and processes the authentication request from the user, and allows the user to change the password. - **block** indicates that a local user is in blocking state. The device rejects the authentication request from the user and does not allow the user to change the password. If a user has established a connection with the device, when the user is set in blocking state, the connection still takes effect but the device rejects subsequent authentication requests from the user. If this parameter is not specified, the status of a local user is active.	-
user-group *group-name*	Specifies the name of a user group. **NOTE** This parameter is supported only by the switches in NAC common mode.	The value is a string of 1 to 64 case-sensitive characters without spaces. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To facilitate device maintenance, create a local user and set parameters such as the password, FTP directory and user privilege level.

Prerequisites

Before adding a local user to a user group, ensure that the user group has been created using the **user-group** command.

Precautions

- For device security purposes, change the password periodically.
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPS. The self-signed certificate may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.
- After a local administrator logs in to the device, the administrator can create, modify, or delete attributes of other local users of the same or a lower privilege level. The attributes include the password, user privilege level, maximum number of access users, and account validity period.

  After you change the rights (for example, the password, FTP directory, idle timeout interval, or status) of a local account, the rights of online users do not change, and the change takes effect for new online users.

  A local administrator who goes online using local authorization will go offline after the user privilege level of the administrator is changed. If no authorization template is configured, a local administrator who goes online using local authentication will also go offline after the user privilege level of the administrator is changed.
- Online users cannot be deleted. When the user is offline or the **cut access-user username** *user-name* command is executed in the AAA view to disconnect the user, delete the user.
- The user name function may be invalid due to improper configuration of the domain name delimiter.
- One user group can be used by multiple local users. However, a local user belongs to only one user group. If the user groups have been configured for the local user and in the service template, only the user group configured for the local user takes effect. The user groups that are used by a local user or an online user cannot be deleted.
- After the device is restarted, the locked account is automatically unlocked.
- During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Create a local user **user1**, and set the domain name to **vipdomain**, the password to YsHsjx_202206 in ciphertext, the maximum number of connections to 100, and the idle timeout interval to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain password irreversible-cipher YsHsjx_202206 access-limit
100 idle-timeout 10
```

13.1.67 local-user change-password

Function

The **local-user change-password** command enables local users to change their passwords.

Format

local-user change-password

Parameters

None

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If you are a low-level administrator, to ensure security of the password, you can run the **local-user change-password** command in the user view to change your password after passing the authentication.

Precautions

- To modify the password, a local user must enter the old password.
- Only the user who passes local authentication can change the password using this command. After a local user successfully changes the password, the user needs to enter the new password for authentication upon the next login.
- The **local-user change-password** command is used to change the password of a local user. It does not save the configuration, but the result of changing the password is saved through the **local-user password** command. If the server does not receive old password, new password, or confirmed password from the user within 30 seconds, it terminates the password change process. When the user presses **Ctrl+C** to cancel password change, the password change process is terminated.

- A simple local user password may bring security risks. When a local user changes the password, the password must be a string of 8 to 128 characters and contain at least two types of the following characters: uppercase letters, lowercase letters, digits, and special characters. In addition, the password cannot repeat or reverse the user name.
- For device security purposes, change the password periodically.
- During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Configure a user that passes local authentication to change the password.

```
<HUAWEI> local-user change-password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters,
uppercase letters, numerals and special characters.
Plese enter old password:
Please enter new password:
Please confirm new password:
Info: The password is changed successfully.
```

13.1.68 local-aaa-user change-password verify

Function

The **local-aaa-user change-password verify** command enables the function of verifying the original password when local administrators change their own passwords.

The **undo local-aaa-user change-password verify** command disables the function of verifying the original password when local administrators change their own passwords.

By default, the function of verifying the original password is enabled when local administrators change their own passwords.

Format

local-aaa-user change-password verify

undo local-aaa-user change-password verify

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

By default, when local administrators change their passwords using the **local-aaa-user change-password verify** command in the AAA view, the administrators need to enter the original password for verification. During management and O&M, you can determine whether to run the **undo local-aaa-user change-password verify** command to disable password verification as required.

- If the **command-privilege level rearrange** command has been run in the system view, levels of level-2 and level-3 commands are increased to 10 and 15 in a batch, respectively. After the **undo local-aaa-user change-password verify** command is run, the system does not verify the original password only when level-15 administrators change their own passwords.
- If the **command-privilege level rearrange** command is not run in the system view and the **undo local-aaa-user change-password verify** command has been run, the system does not verify the original password when administrators of levels 3 to 15 change their own passwords, and the system still needs to verify the original password when administrators of other levels change their own passwords.

Example

Enable the function of verifying the original password when local administrators change their own passwords.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo local-aaa-user change-password verify
Warning: This command will disable the function of verifying the old password when administrators
changes their own passwords. Continue?[Y/N]
```

13.1.69 local-user device-type

Function

The **local-user device-type** command configures the type of terminals allowed to access the network.

The **undo local-user device-type** command deletes the type of terminals allowed to access the network.

By default, the type of terminals allowed to access the network is not configured.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

local-user *user-name* **device-type** *device-type* &<1-8>

undo local-user *user-name* **device-type**

Parameters

Parameter	Description	Value

user-name	Specifies the name of a local user.
	When querying and modifying the user account, you can use the wildcard *, for example, *@isp, user@*, and *@*.
		The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
		NOTE
		- During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		- Note the following when configuring case sensitivity for user names:
		  - Only the user name is case-sensitive and the domain name is case-insensitive.
		  - For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  - When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

device-type	Specifies a terminal type.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

You can run the **local-user device-type** command to configure the type of terminals allowed to access the network. In local authentication and authorization, the device checks whether a terminal is allowed to access the network. If so, the device checks the user name and password of the terminal.

Example

Set the type of the terminal that local user **hello** uses to access the network to **iphone**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello device-type iphone
```

13.1.70 local-user expire-date

Function

The **local-user expire-date** command sets the expiration date of a local account.

The **undo local-user expire-date** command restores the default expiration date of a local account.

By default, a local account is permanently valid.

Format

local-user *user-name* **expire-date** *expire-date*

undo local-user *user-name* **expire-date**

Parameters

Parameter	Description	Value
user-name	Specifies a local account.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark. **NOTE** ● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive. ● Note the following when configuring case sensitivity for user names: ● Only the user name is case-sensitive and the domain name is case-insensitive. ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name. ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.
expire-date	Specifies the expiration date of the local account.	The value is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value ranges from 2000/1/1 to 2099/12/31.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local account is created, the account has no expiration date by default. You can run the **local-user expire-date** command to set the expiration date of a local account. When the expiration date is reached, the account expires. This configuration enhances network security.

Precautions

- For example, if the expiration date of the local account is set to 2013-10-1, the account becomes invalid at 00:00 on 2013-10-1.
- This function takes effect only for users who go online after this function is successfully configured.

Example

Set the expiration date of local account **hello@163.net** to 2013/10/1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello@163.net expire-date 2013/10/1
```

13.1.71 local-user ftp-privilege

Function

The **local-user ftp-privilege** command configures the FTP permissions for a local user.

The **undo local-user ftp-privilege** command restores the default FTP permissions of a local user.

By default, FTP permissions of a local user are the read, write, and execute permissions.

Format

local-user *user-name* **ftp-privilege** [*directoryfilename*] { **read** | **write** | **execute** }*

undo local-user *user-name* **ftp-privilege** [*directoryfilename*]

Parameters

Parameter	Description	Value
user-name	Specifies the user name of a local user. If the user name contains a delimiter of at sign (@), the character string before the at sign is the user name and the character string following the at sign is the domain name. If the user name does not contain the at sign, the entire character string represents the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisks (*), double quotation marks ("), or question marks (?).
directoryfilename	Specifies the directory or file name of the FTP operation.	The value is a string of 1 to 160 case-sensitive characters. It cannot contain spaces.
read	Indicates that local users have only read permission.	-
write	Indicates that local users have only write permission.	-
execute	Indicates that local users have only execute permission.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To facilitate device maintenance, the administrator can run this command to configure FTP permissions for local users so that different users have different permissions to operate different directories or files.

Different FTP commands require different FTP permissions:

- The read permission is required for running the **pwd**, **dir**, and **ls** commands.
- The write permission is required for running the **mkdir**, **rmdir**, **delete**, **put**, and **mpu** commands.
- The execute permission is required for running the **cd**, **cdup**, **get**, **ascii**, and **binary** commands.
- Running the **mget** command must meet the following requirements: The execute permission is required for the current directory; the read permission is required for operating all files (including the files matching the wildcard *); the execute permission is required for running the **mget** command on each file.

Precautions

- If *directoryfilename* is not specified, this command configures the permissions on the FTP directory that local users can access.
- Directory matching complies with the longest match principle. For example, if both the **local-user 1 ftp-privilege flash:/logfile/ read** and **local-user 1 ftp-privilege flash:/logfile/log.log execute** commands are configured on the device, the local user has the execute permission on the file **flash:/logfile/log.log** and the read permission on other files in the directory **flash:/logfile/**. If no permission is configured for a specified directory or file, the directory or file inherits the permission of the upper-level directory.
- The specified directory or file name must be an absolute path.For example, "flash:/my/test/"

Example

Grant the read permission on the FTP directory to the local user **user1@vipdomain**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain ftp-privilege read
```

Grant the read and write permissions on the directory **logfile** to the local user **user1@vipdomain**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain ftp-privilege flash:/logfile/ read write
```

13.1.72 local-user password

Function

The **local-user password** command configures a password for a local account.

By default, the password of a local account is empty.

Format

local-user *user-name* **password**

NOTE

This command is an interactive command. After you enter **local-user** *user-name* **password** and press **Enter**, you can set the password as prompted. The local user password is a string of 8 to 128 case-sensitive characters.

Parameters

Parameter	Description	Value
user-name	Specifies the local user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark. **NOTE** ● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive. ● Note the following when configuring case sensitivity for user names: ● Only the user name is case-sensitive and the domain name is case-insensitive. ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name. ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

If no password is configured when a local user is created, the password is empty, and the local user cannot log in to the device.

NOTICE

A simple local user password may bring security risks. The user password must consist of two types of characters, including uppercase letters, lowercase letters, digits, and special characters. In addition, the password cannot repeat or reverse the user name.

Example

Set the password to **YsHsjx_202206** for the local account **hello@163.net**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello@163.net password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:              //Enter the password
YsHsjx_202206
Please confirm password:            //Confirm the password YsHsjx_202206
Info: Add a new user.
```

13.1.73 local-user password change-offline enable

Function

The **local-user password change-offline enable** command enables the interactive confirmation function when a local administrator changes the password.

The **undo local-user password change-offline enable** command disables the interactive confirmation function when a local administrator changes the password.

By default, the interactive confirmation function is enabled when a local administrator changes the password.

Format

local-user password change-offline enable

undo local-user password change-offline enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

By default, when a local administrator runs the **local-user** *user-name* **password** command in the AAA view to change the password, the device is enabled to interact with the user. In this case, the device displays a message indicating that the user account will be deregistered and the user needs to log in again. During management and O&M, you can determine whether to run the **undo local-user password change-offline enable** command to disable the interactive confirmation function as required.

Example

Enable the interactive confirmation function when a local administrator changes the password.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user password change-offline enable
[HUAWEI-aaa] local-user admin password irreversible-cipher YsHsjx_202206
Warning: The user using this account will be logged out, and needs to log in again. Do you want to
continue? [Y/N]y
```

13.1.74 local-aaa-user password policy access-user

Function

The **local-aaa-user password policy access-user** command enables the password policy for local access users and enters the local access user password policy view.

The **undo local-aaa-user password policy access-user** command disables the password policy of local access users.

By default, the password policy of local access users is disabled.

Format

local-aaa-user password policy access-user

undo local-aaa-user password policy access-user

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a local user is created using the **local-user** command, the minimum length and complexity of the password are limited. If you want to improve password security, run this command to configure password policy. The new password cannot be the same as any previously used password stored on the device.

Example

Enable the local access user password policy and enter the local access user password policy view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy access-user
[HUAWEI-aaa-lupp-acc]
```

13.1.75 local-aaa-user password policy administrator

Function

The **local-aaa-user password policy administrator** command enables the password policy for local administrators and enters the local administrator password policy view.

The **undo local-aaa-user password policy administrator** command disables the password policy of local administrators.

By default, the password policy for local administrators is enabled.

Format

local-aaa-user password policy administrator

undo local-aaa-user password policy administrator

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local user is created using the **local-user** command, the minimum length and complexity of the password are limited. If you want to improve password security, you can run the following commands to configure the password policy for local administrators:

- Run the **password expire** command to set the password validity period.
- Run the **password alert before-expire** command to set the password expiration prompt days.

- Run the **password alert original** command to enable the device to prompt users to change initial passwords.
- Run the **password history record number** command to set the maximum number of previously used passwords recorded for each user.

Precautions

After the **undo local-aaa-user password policy administrator** command is executed, the administrator password policy will be disabled, causing a security risk.

After the device is restored to factory settings, the password policy for local administrators is enabled by default.

When the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **local-aaa-user password policy administrato** command to enable the password policy for local administrators.
- Run the **password expire 0** command to configure the passwords of local administrators to be permanently valid.
- Run the **password history record number 0** command to configure the device not to check whether a changed password of a local administrator is the same as any historical password.

Example

Enable the password policy for local administrators and enter the local administrator password policy view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin]
```

13.1.76 local-user service-type

Function

The **local-user service-type** command sets the access type for a local user.

The **undo local-user service-type** command restores the default access type for a local user.

By default, a local user cannot use any access type.

Format

local-user *user-name* **service-type** { **8021x** | **api** | **ftp** | **http** | **ppp** | **ssh** | **telnet** | **terminal** | **web** | **x25-pad** } *

undo local-user *user-name* **service-type**

NOTE

All models support the api parameter, except S1720GW-E, S1720GWR-E, and S1720X-E.

Parameters

Parameter	Description	Value
user-name	Specifies a user name. If the user name contains a domain name delimiter such as @, the character before @ is the user name and the character behind @ is the domain name. If the value does not contain @, the entire character string is the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Parameter	Description	Value

		NOTE
		- During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		- Note the following when configuring case sensitivity for user names:
		  - Only the user name is case-sensitive and the domain name is case-insensitive.
		  - For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  - When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Parameter	Description	Value
8021x	Indicates an 802.1X user.	-
api	Indicates an API user, which is typically used for NETCONF access. **NOTE** If the access type of a user is API, the user name cannot be set to **root**.	-
ftp	Indicates an FTP user.	-
http	Indicates an HTTP user, which is usually used for web system login.	-
ppp	Indicates a PPP user.	-
ssh	Indicates an SSH user.	-
telnet	Indicates a Telnet user, which is usually a network administrator.	-
terminal	Indicates a terminal user, which is usually a user connected using a console port.	-
web	Indicates a Portal authentication user.	-
x25-pad	Indicates an X25-PAD user. **NOTE** Currently, the device does not support X25-PAD.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can manage access types of local users. After you specify the access type of a user, the user can successfully log in only when the configured access type is the same as the actual access type of the user.

Local users have the following access types:

- Administrative: api, FTP, HTTP, SSH, Telnet, x25-pad, and Terminal
- Common: 802.1X, ppp, and web

Precautions

- When MAC authentication users use AAA local authentication, the device does not match or check the access type of local users. However, the access type must be configured; otherwise, local authentication for MAC address authentication users fails.
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPS. The self-signed certificate may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.
- Common access types cannot be configured together with administrative access types.

  The API access type cannot be configured together with other access types.

  If a user has been created and the password uses an irreversible encryption algorithm, the access type can only be set to an administrative one.

  If a user has been created and the password uses a reversible encryption algorithm, the access type can be set to an administrative or common one. When the access type is set to an administrative one, the encryption algorithm of the password is automatically converted into an irreversible encryption algorithm.

Example

Set the access type of the local user **user1@vipdomain** to SSH.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain service-type ssh
```

13.1.77 local-user time-range

Function

The **local-user time-range** command sets the access permission time range for a local user.

The **undo local-user time-range** command deletes the access permission time range for a local user.

By default, a local account can access the network anytime.

Format

local-user *user-name* **time-range** *time-name*

undo local-user *user-name* **time-range**

Parameters

Parameter	Description	Value
user-name	Indicates the local account.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark. **NOTE** ● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive. ● Note the following when configuring case sensitivity for user names: ● Only the user name is case-sensitive and the domain name is case-insensitive. ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name. ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.
time-name	Indicates the access permission time range of the local account. *time-name* specifies the name of the access permission time range.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word **all** cannot be specified as a time range name.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Use Scenario

After a local account is created, the account has no expiration date by default. To restrict the network access time of a local account, run the **local-user time-range** command. After the command is executed, the account can access network resources only in the specified time range.

Prerequisite

The time range has been created using the **time-range** command.

Precautions

If you run the **local-user time-range** and **local-user expire-date** commands in the AAA view multiple times, only the latest configuration takes effect.

After the access permission time range of an online local user is changed, the access permission time range of the user will take effect only when the user goes online next time.

Example

Set the access permission time segment of local account hello@163.net to 9:00-18:00 from Monday to Friday.

```
<HUAWEI> system-view
[HUAWEI] time-range test 9:00 to 18:00 working-day
[HUAWEI] aaa
[HUAWEI-aaa] local-user hello@163.net time-range test
```

13.1.78 local-user user-type netmanager

Function

The **local-user user-type netmanager** command configures a local user as the NMS user.

The **undo local-user user-type netmanager** command cancels to configure a local user as the NMS user.

By default, no local user is configured as the NMS user.

Format

local-user *user-name* **user-type netmanager**

undo local-user *user-name* **user-type netmanager**

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark. **NOTE** ● During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive. ● Note the following when configuring case sensitivity for user names: ● Only the user name is case-sensitive and the domain name is case-insensitive. ● For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name. ● When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user names is used.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a VTY user logging in to the device is an NMS user, you need to run this command to set the user type. When the number of login VTY users has reached the maximum, an NMS user can log in using the reserved VTY numbers 16-20. The NMS user is allowed to log in to the device only after passing the AAA local authentication.

Prerequisite

The local user has been created using the **local-user** command. This user must pass the AAA local authentication.

Example

Configure the local user user1@vipdomain as the NMS user.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user user1@vipdomain password cipher YsHsjx_202206
[HUAWEI-aaa] local-user user1@vipdomain user-type netmanager
```

13.1.79 load security weak-password-dictionary

Function

The **load security weak-password-dictionary** command loads a weak password dictionary.

Format

load security weak-password-dictionary *filename*

Parameters

Parameter	Description	Value
filename	Specifies the name of a weak password dictionary file.	The value is a string of case-insensitive characters, including uppercase letters, lowercase letters, digits, and special characters. It cannot contain spaces. The value is a string of 1 to 64 characters (including the file name extension). The following special characters are not supported: ~ ? * / \ : " | < > [ ]. The first or last character cannot be a period (.). The file name extension must be .txt.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

No weak password is preset on the device by default. You can run this command to load a weak password dictionary to the memory for weak password check during the configuration of the management plane password.

Prerequisites

Before loading a weak password dictionary, make a .txt weak password dictionary file and upload it to the device. Otherwise, the weak password dictionary file fails to be loaded.

Precautions

1. When you run this command, the system checks the file validity:
   - The system checks whether the file exists. Only the files in the directory where the .cc package is located can be verified. If the file does not exist, the command fails to be executed.
   - The system checks whether the file size is less than or equal to 1 MB. If the file size is greater than 1 MB, the command fails to be executed.
   - The system checks whether the file is a .txt file. If not, the command fails to be executed.
   - The system checks whether the file contains empty lines. If so, the command fails to be executed.
   - The system checks whether the same configuration exists. If so, the system displays a message indicating that the same configuration exists, and the command is executed successfully.
2. After the file validity is checked, the system reads the file content by line, loads the file content to the memory, and checks the file content:
   - If there is a password that contains more than 128 characters in the file, the command fails to be executed.
   - If the file contains more than 1000 lines, the command fails to be executed.
   - If there are empty lines in the file, the command fails to be executed.
3. After the command is executed successfully, pay attention to the following points:
   - For protection purposes, the file specified by *filename* cannot be modified or deleted.
   - If a slave main control board is installed, the weak password dictionary file is backed up to the slave main control board. For protection purposes, the file cannot be modified or deleted.

Example

Load the weak password dictionary file named **pass1.txt**.

```
<HUAWEI> system-view
[HUAWEI] load security weak-password-dictionary pass1.txt
Info: Success to import the weak password dictionary. The weak password number is 6.
```

13.1.80 navigator first-login enable

Function

The **navigator first-login enable** command enables the browser to display the user registration page during the first login of a web user or enables the system to prompt the creation of a user during the first login of a console port user.

Format

navigator first-login enable

Parameters

None

Views

System view

Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no local user is created on the device. Therefore, the factory configuration file of the device contains the **navigator first-login enable** command. When a user logs in to the device through the web system for the first time, the browser displays the user creation page. After a user is created, the browser does not display the user creation page when the user logs in to the device again through the web system.

In addition, after a user logs in to the device through the console port, the browser does not display the user creation page but displays the user login page, when the user logs in to the device through the web system for the first time. Therefore, if you need to log in to the device through the web system, create a local user for web-based login during a login through the console port.

The factory configuration file of the device contains the **navigator first-login enable** command, removing the need to manually configure this command. The **navigator first-login enable** command can be delivered only through the configuration file, cannot be entered or executed on the device, and is not recorded in buildrun information.

Precautions

When you create an administrator in the factory settings of the device, the creation fails if the specification is reached. In this case, you need to modify the factory configuration file to reserve the specification.

13.1.81 outbound recording-scheme

Function

The **outbound recording-scheme** command applies a policy to a recording scheme to record the connection information.

The **undo outbound recording-scheme** command deletes a policy from a recording scheme. Connection information is not recorded then.

By default, connection information is not recorded.

Format

outbound recording-scheme *recording-scheme-name*

undo outbound recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Incorrect connections may result in network faults, for example, loops. The connection information recorded on a server helps you monitor devices. When network faults occur, you can locate faults based on the connection information recorded on the server.

Prerequisites

A recording scheme has been created using the **recording-scheme** command in the AAA view and an HWTACACS server template has been associated with a recording scheme using the **recording-mode hwtacacs** command in the recording scheme view.

Example

Apply a policy to the recording scheme **scheme** to record the connection information.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template hw1
[HUAWEI-hwtacacs-hw1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme
[HUAWEI-aaa-recording-scheme] recording-mode hwtacacs hw1
[HUAWEI-aaa-recording-scheme] quit
[HUAWEI-aaa] outbound recording-scheme scheme
```

13.1.82 password alert before-expire

Function

The **password alert before-expire** command sets the number of days in advance users are notified that their passwords are about to expire.

The **undo password alert before-expire** command restores the default number of days in advance users are notified that their passwords are about to expire.

By default, the number of days in advance users are notified that their passwords are about to expire is 30 days. In the factory configuration file, the number of days in advance users are notified that their passwords are about to expire is 0.

Format

password alert before-expire *day*

undo password alert before-expire

Parameters

Parameter	Description	Value
day	Sets the number of days in advance users are notified that their passwords are about to expire. If the value is set to 0, the device does not notify users that their passwords will expire.	The value is an integer that ranges from 0 to 999, in days. The default value is 30 days.

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

When a user logs in to the device, the device checks how many days the password is valid for. If the number of days is less than the prompt days set in the command, the device notifies the user in how many days the password will expire and asks the user whether to change the password.

- If the user changes the password, the device records the new password and updates the time of password change.
- If the user does not change the password or fails to change the password, the user can still log in as long as the current password is still valid.

Example

Set the number of days in advance users are notified that their passwords are about to expire to 90.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password alert before-expire 90
```

13.1.83 password alert original

Function

The **password alert original** command enables the device to prompt users to change initial passwords.

The **undo password alert original** command disables the device from prompting users to change initial passwords.

By default, the device prompts users to change initial passwords.

Format

password alert original

undo password alert original

Parameters

None

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve device security, use this command to enable the initial password change prompt function. When a user logs in to the device:

- If the user enters the initial password, the device displays a message to ask whether to change the initial password. The user can select **Y** or **N**:
  - If the user selects **Y** to change the password, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet requirements (password length and complexity). After the password is changed, the user can log in to the device successfully.
  - If the user selects **N** or fails to change the password, the device does not allow the user to log in.

- If the entered password is not the initial password, the device does not display any message and the user can successfully log in.

After the **undo password alert original** command is executed, the initial password alert will be disabled, causing a security risk.

NOTE

The initial password may be the default password, the password created by a local user in the first login, or the password changed by another user (for example, user B changes user A's password, and user A uses the changed password to log in).

Precautions

This function is only valid for Telnet users, HTTP users, SSH users, and terminal users.

Example

Enable the device to prompt users to change initial passwords.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password alert original
```

13.1.84 password expire

Function

The **password expire** command sets the password validity period.

The **undo password expire** command restores the default password validity period.

By default, the password validity period is 90 days.In the factory configuration file, the password validity period is 0 days.

Format

password expire *day*

undo password expire

Parameters

Parameter	Description	Value
day	Specifies the password validity period. If the value is 0, the password is permanently valid.	The value is an integer that ranges from 0 to 999, in days. The default value is 90 days.

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, the administrator can use this command to set the validity period for the local user password. When the validity period expires, the password becomes invalid.

If the local user still uses this password to log in to the device, the device allows the user to log in, prompts the user that the password has expired, and asks the user whether to change the password:

- If the user enters Y, the user needs to enter the old password, new password, and confirm password. The password can only be successfully changed when the old password is correct, the new password and confirm password are the same, and the new password meets the password length and complexity requirements. After the password is changed, the user can log in to the device successfully.
- If the user enters N or fails to change the password, the user cannot log in to the device.

Precautions

Changing the system time will affect the password validity status.

After this command is run, the device checks whether the password expires every minute; therefore, there may be a time difference of less than 1 minute.

When the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **local-aaa-user password policy administrato** command to enable the password policy for local administrators.
- Run the **password expire 0** command to configure the passwords of local administrators to be permanently valid.
- Run the **password history record number 0** command to configure the device not to check whether a changed password of a local administrator is the same as any historical password.

Example

Set the password validity period to 120 days.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password expire 120
```

13.1.85 password history record number

Function

The **password history record number** command sets the maximum number of historical passwords recorded for each user.

The **undo password history record number** command restores the default maximum number of historical passwords recorded for each user.

By default, a maximum of five historical passwords are recorded for each user. In the factory configuration file, the maximum number of historical passwords recorded for each user is 0.

Format

password history record number *number*

undo password history record number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of historical passwords recorded for each user. If the value is set to 0, the device will not check whether a changed password is the same as any historical password.	The value is an integer that ranges from 0 to 12. The default value is 5.

Views

Local administrator password policy view, local access user password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, it is not recommended that you use a previously used password. You can set the maximum number of historical passwords recorded for each user. When a user changes the password, the device compares the new password against the historical passwords stored on the device. If the new password is the same as a stored password, the device displays an error message to prompt the user that password change fails.

Precautions

When the number of recorded historical passwords reaches the maximum value, the later password will overwrite the earliest password on the device.

After the historical password recording function is disabled, the device does not record historical passwords; however, the passwords that have been stored are retained.

If the **save** command is not run for the historical record of the new user password, the historical record of the new user password is not saved after the device is restarted.

When the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **local-aaa-user password policy administrato** command to enable the password policy for local administrators.
- Run the **password expire 0** command to configure the passwords of local administrators to be permanently valid.
- Run the **password history record number 0** command to configure the device not to check whether a changed password of a local administrator is the same as any historical password.

Example

Set the maximum number of historical passwords recorded for each local administrator to 10.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy administrator
[HUAWEI-aaa-lupp-admin] password history record number 10
```

Set the maximum number of historical passwords recorded for each local access user to 10.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user password policy access-user
[HUAWEI-aaa-lupp-acc] password history record number 10
```

13.1.86 permit-domain

Function

The **permit-domain** command specifies permitted domains for WLAN users.

The **undo permit-domain** command deletes the permitted domains of WLAN users.

By default, no permitted domain is specified for WLAN users.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

permit-domain name *domain-name* &<1-4>

undo permit-domain { **name** *domain-name* | **all** }

Parameters

Item	Description	Value
name *domain-name*	Specifies the name of a permitted domain for WLAN users.	The domain must already exist.

Item	Description	Value
all	Deletes the permitted domain for all WLAN users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a permitted domain is specified on an authentication profile, only the WLAN users in the permitted domain can be authenticated, authorized, or charged.

Prerequisites

Permitted domains have been created using the **domain** command.

Precautions

This command applies only to wireless users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

This command is only available in the NAC unified mode.

Example

Specify permitted domain **dom** for WLAN users to the authentication profile **john**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain dom
[HUAWEI-aaa-domain-dom] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name john
[HUAWEI-authen-profile-john] permit-domain name dom
```

13.1.87 priority (service scheme view)

Function

The **priority** command configures the

The **undo priority** command restores the default setting.

By default, the user priority is 0.

Format

priority *priority-value*

undo priority

Parameters

Parameter	Description	Value
priority-value	Specifies the user priority.	The value is an integer that ranges from 0 to 1. A larger value indicates a higher priority.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, priorities of all users are the same on a device. As a result, if a large number of common users access an AP in a user-intensive campus office scenarios and the number of users accessed to the AP reaches the upper limit, the subsequent VIP users cannot go online. In this case, you can authorize high priorities for the VIP users using a service scheme to ensure the access success rate of the VIP users. If the number of users accessed to an AP reaches the upper limit and users have been authenticated, the device checks priorities of the users. If the priorities are high, the device forcibly disconnects users with low priorities and allows these users to go online; if the priorities are low, the device does not allow these users to go online.

Precautions

When a CAR configuration for user authorization is delivered by the server or configured in a domain, the CAR configuration does not take effect for VIP users. The following example configures CAR for user authorization in a domain.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name abc
[HUAWEI-qos-abc] car cir 10000 cbs 10240 pbs 10240 inbound //Configure CAR in the QoS profile abc.
[HUAWEI-qos-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] qos-profile abc  //Bind the QoS profile abc to the service scheme test.
[HUAWEI-aaa-service-test] quit
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] service-scheme test   //Bind the service scheme test to the domain test.
```

In a policy association scenario, this function does not take effect on authentication access devices.

Example

Set the user priority in service scheme **s1** to 1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] priority 1
```

13.1.88 recording-mode hwtacacs

Function

The **recording-mode hwtacacs** command associates an HWTACACS server template with a recording scheme.

The **undo recording-mode** command unbinds an HWTACACS server template from a recording scheme.

By default, no HWTACACS server template is associated with a recording scheme.

Format

recording-mode hwtacacs *template-name*

undo recording-mode

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

Recording scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device needs to send the records such as the executed commands, connection information, and system events to the specified HWTACACS accounting server; therefore, an HWTACACS server template needs to be associated with a recording scheme.

Prerequisites

The HWTACACS server template has been created by using the **hwtacacs-server template** command.

Example

Associate the recording scheme **scheme0** with the HWTACACS server template **tacacs1**.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template tacacs1
[HUAWEI-hwtacacs-tacacs1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme0
[HUAWEI-aaa-recording-scheme0] recording-mode hwtacacs tacacs1
```

13.1.89 recording-scheme

Function

The **recording-scheme** command creates a recording scheme and displays the recording scheme view.

The **undo recording-scheme** command deletes a recording scheme.

By default, no recording scheme is configured on the device.

Format

recording-scheme *recording-scheme-name*

undo recording-scheme *recording-scheme-name*

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a recording scheme takes effect, you can view the records such as the executed commands, connection information, and system-level events on the recording server. The records help you locate network faults. Because a recording scheme needs to be associated with an HWTACACS server template, the recording scheme is configured only when HWTACACS authentication or authorization is performed.

Creating a recording template using the **recording-scheme** command is mandatory for configuration.

Follow-up Procedure

Run the **recording-mode hwtacacs** command to associate an HWTACACS server template with the recording scheme.

After a recording scheme is created and associated with an HWTACACS server template, perform the following configurations in the AAA view:

- Run the **cmd recording-scheme** command to apply a policy in a recording scheme to record the commands executed on the device.
- Run the **outbound recording-scheme** command to apply a policy in a recording scheme to record the connection information.
- Run the **system recording-scheme** command to apply a policy in a recording scheme to record the system events.

Precautions

If the recording scheme to be configured does not exist, the **recording-scheme** command creates a recording scheme and displays the recording scheme view. If the recording scheme to be configured already exists, the **recording-scheme** command displays the recording scheme view.

Before deleting a recording scheme, ensure that the scheme has not been referenced by the **cmd recording-scheme** or **outbound recording-scheme** or **system recording-scheme** command.

Example

Create a recording scheme **scheme0**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme0
[HUAWEI-aaa-recording-scheme0]
```

13.1.90 redirect-acl

Function

The **redirect-acl** command configures the ACL used for redirection in a service scheme.

The **undo redirect-acl** command deletes the ACL used for redirection in a service scheme.

By default, no ACL for redirection is configured in the service scheme.

Format

redirect-acl [**ipv6**] { *acl-number* | **name** *acl-name* }

undo redirect-acl [**ipv6**]

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1, S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S6720-EI, S6735-S, , S6720S-EI support the **ipv6** parameter.

Only wired users support the authorization of the IPv6 ACL used for redirection.

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 ACL used for redirection.	-
acl-number	Specifies the number of the ACL used for redirection.	The value ranges from 3000 to 3999 for wired users and from 3000 to 3031 for wireless users, and it must exist.
name *acl-name*	Specifies the name of the ACL used for redirection.	The ACL name must exist. The length ranges from 1 to 64.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In some authentication scenarios, after users succeed in authentication, the administrator needs to redirect HTTP/HTTPS traffic matching ACL permit rules to the Portal authentication page where users are authenticated again.

Precautions

Before running this command, you are advised to run the **acl** or **acl name** command to create an ACL.

If the ACL is not created before and after this command is run, the redirection ACL will fail to be delivered.

To redirect HTTPS traffic, run the **authentication https-redirect enable** command to configure the HTTPS redirection function.

After the **authentication mode multi-share** command is configured in the authentication profile, authorization redirection ACLs will not be supported.

Example

Configure ACL 3001 for redirection in the service scheme **svcscheme1**.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme svcscheme1
[HUAWEI-aaa-service-svcscheme1] redirect-acl 3001
```

13.1.91 remote-user authen-fail unblock

Function

The **remote-user authen-fail unblock** command unlocks remote AAA authentication accounts.

Format

remote-user authen-fail unblock { **all** | **username** *username* }

Parameters

Parameter	Description	Value
all	Unlocks all accounts that fail the remote AAA authentication.	-
username *username*	Unlocks a specified account that fails the remote AAA authentication.	The value is a string of 1 to 253 case-insensitive characters without spaces.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

You may need to unlock remote AAA authentication accounts in the following situations:

- When a user enters an incorrect user name or password fewer times than the maximum permitted, run the **remote-user authen-fail unblock** command to unlock the user and delete the incorrect record of the user from the device.
- When a user is incorrectly locked or needs to be unlocked due to special reasons, run the **remote-user authen-fail unblock** command to unlock the user.

Example

Unlock the remote AAA authentication account **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] remote-user authen-fail unblock username test
```

13.1.92 reset aaa

Function

Using the **reset aaa** command, you can clear records of abnormal offline, user offline and failure to get online.

Format

reset aaa { **abnormal-offline-record** | **offline-record** | **online-fail-record** }

Parameters

Parameter	Description	Value
abnormal-offline-record	Clears records of user abnormal offline.	-
offline-record	Clears records of user offline.	-
online-fail-record	Clears records of user failure to get online.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command allows you to clear records of user offline, abnormal offline, and failure to get online. After the records are cleared, the function of recording information is enabled.

Example

Clear user offline records.

```
<HUAWEI> system-view
[HUAWEI] reset aaa offline-record
```

13.1.93 reset aaa statistics offline-reason

Function

Using the **reset aaa statistics offline-reason** command, you can clear the statistics about reasons why users go offline.

Format

reset aaa statistics offline-reason

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **reset aaa statistics offline-reason** command to delete the statistics about reasons why users go offline, and then collect new statistics.

Example

Clear the statistics about reasons why users go offline.

```
<HUAWEI> reset aaa statistics offline-reason
```

13.1.94 reset access-user statistics

Function

The **reset access-user statistics** command deletes the statistics on access user authentication.

Format

reset access-user statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When diagnosing and locating faults related to access user authentication, you need to collect statistics on user login and logout information within a period of time. Before the statistics collection, you can run the **reset access-user statistics** command to clear the historical statistics, and then run the **display access-user statistics** command to view the current statistics.

Example

Delete the statistics on access user authentication.

```
<HUAWEI> reset access-user statistics
Info: Successful to reset access-user statistics.
```

13.1.95 reset local-user password history record

Function

The **reset local-user password history record** command clears historical passwords stored for the local user.

Format

reset local-user [*user-name*] **password history record**

Parameters

Parameter	Description	Value
user-name	Clears the historical passwords of the specified user. If this parameter is not specified, the historical passwords of all local users are cleared.	The local user must exist on the device.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the administrator wants to record historical passwords of local users again, this command can be used to clear existing historical passwords.

Precautions

After this command is used, all historical passwords on the device are deleted and cannot be restored. This operation has security risks, so exercise caution when using it.

Example

Clear historical passwords of all local users.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] reset local-user password history record
Warning: Clear history password records, there is a security risk. Continue?[Y/N] y
```

13.1.96 server no-response accounting

Function

The **server no-response accounting** command configures a device to continue sending accounting packets when the accounting function is configured and a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request.

The **undo server no-response accounting** command restores the default setting.

By default, when the accounting function is configured, the device does not send accounting packets when the server does not respond to a user's authentication request and the user then is authenticated using local authentication.

Format

server no-response accounting

undo server no-response accounting

Parameters

None

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Typically, a server functions as both the remote accounting server and the authentication server. If the authentication server does not respond, the accounting server also does not respond. When accounting and authentication + local authentication are configured on a device, a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request. Because the accounting server also does not respond, after the user is authenticated using the local authentication mode, the device still sends accounting packets. As a result, the user goes offline because of accounting-start failures. To prevent this issue, the device does not send accounting packets by default when a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request.

Example

Configure a device not to send accounting packets when the accounting function is configured and a user is authenticated using the local authentication mode after the server does not respond to the user's authentication request.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme authen1
[HUAWEI-aaa-authen-authen1] authentication-mode radius local
[HUAWEI-aaa-authen-authen1] undo server no-response accounting
[HUAWEI-aaa-authen-authen1] quit
[HUAWEI-aaa] accounting-scheme acc1
[HUAWEI-aaa-accounting-acc1] accounting-mode radius
```

13.1.97 server no-response authorization

Function

The **server no-response authorization** command configures the device to perform authorization in the configured authorization sequence after local authentication is used when the server does not respond to users' authentication requests and both server authentication and local authentication are configured.

The **undo server no-response authorization** command configures the device to request local authorization after local authentication is used when the server does not respond to users' authentication requests and both server authentication and local authentication are configured.

By default, when both server authentication and local authentication are configured, the device requests local authorization after local authentication is used when the server does not respond to users' authentication requests.

Format

server no-response authorization

undo server no-response authorization

Parameters

None

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

In most cases, if both remote authentication and local authentication are configured on a device and remote authentication does not respond, the device selects local authentication. After local authentication is performed on a user, the device requests local authorization. After the **server no-response authorization** command is run, the device still uses the configured authorization mode.

Precautions

RADIUS authentication and authorization are integrated. Therefore, when RADIUS authentication and local authentication are configured, if remote authentication does not respond, remote authorization does not respond, and the device still uses local authorization.

You can run the **display access-user user-id** command to check the authentication mode and authorization mode after this command is configured.

Example

When HWTACACS+local authentication and authorization are configured, the device requests authorization in the configured authorization mode instead of requesting local authorization after local authentication is used if the server does not respond.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme authen1
[HUAWEI-aaa-authen-authen1] authentication-mode hwtacacs local
[HUAWEI-aaa-authen-authen1] server no-response authorization
[HUAWEI-aaa-authen-authen1] quit
```

13.1.98 security-name enable

Function

The **security-name enable** command enables the security string function.

The **undo security-name enable** command disables the security string function.

By default, the security string function is enabled.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

security-name enable

undo security-name enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Some special clients use user names in the format of **username@domain*securitystring** in which a security string and a security string delimiter (*) are added to the user name. To ensure that the AAA server can identify such user names, run the **security-name enable** command to enable the security string function on the device. When sending a user name to the AAA server, the device deletes ***securitystring** and only uses **username@domain** for authentication.

You can run the **security-name-delimiter** command to modify the security string delimiter.

Example

Enable the security string function.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] security-name enable
```

13.1.99 security-name-delimiter

Function

The **security-name-delimiter** command configures a delimiter for a security string.

The **undo security-name-delimiter** command restores the default delimiter for a security string.

By default, the delimiter for a security string in the AAA view is *, and no delimiter is available in the authentication profile view.

NOTE

This command only applies to 802.1X users. If CHAP or PAP authentication is configured for 802.1X users, the device removes the security string, but does not encapsulate it into the HW-SecurityStr attribute. If EAP authentication is configured for 802.1X users, the device removes the security string and encapsulates it into the HW-SecurityStr attribute.

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

security-name-delimiter *delimiter*

undo security-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a delimiter for a security string.	The value is of the enumerated type. The value can be \ / : < > | @ ' % or *.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

Some STAs may use the user name in the format of **username@domain*securitystring**. * is the security string delimiter. To enable the AAA server to identify this type of user name, you need to configure a delimiter for a security string on the device. In this way, when sending the user name to the AAA server, the device deletes ***securitystring** and only uses **username@domain** for authentication.

If the server needs to identify a security string, for example *, you need to configure other security string delimiters except *. For example, if a client is configured with a user name in the format of **username@domain*securitystring**, the device needs to be configured with other security string delimiters except *. In this way, when sending the user name to the server, the device still uses the user name in the format of **username@domain*securitystring** for authentication.

Precautions

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

The delimiter for a security string cannot be the same as the domain name delimiter.

If you run the **security-name-delimiter** command in the AAA view, the delimiter for a security string is configured globally.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

Example

Configure the delimiter for a security string as / in the AAA view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] security-name-delimiter /
```

13.1.100 service-scheme (aaa domain view)

Function

The **service-scheme** command applies a service scheme to a domain.

The **undo service-scheme** command unbinds a service scheme from a domain.

By default, no service scheme is bound to a domain.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The value must be an existing service scheme name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The authorization configuration in a service scheme takes effect only when the service scheme is applied to a domain.

Prerequisites

A service scheme has been created and configured with required parameters.

Example

Apply the service scheme **srvscheme1** to the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme srvscheme1
[HUAWEI-aaa-service-srvscheme1] quit
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] service-scheme srvscheme1
```

13.1.101 service-scheme (AAA view)

Function

The **service-scheme** command creates a service scheme and displays the service scheme view.

The **undo service-scheme** command deletes a service scheme.

By default, no service scheme is configured.

Format

service-scheme *service-scheme-name*

undo service-scheme *service-scheme-name*

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: /, \, :, *, ?, ", <, >, |, @, ', and %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The service scheme is used to assign IP address pool and DNS server parameters to users.

Follow-up Procedure

Run the **service-scheme (AAA domain view)** command to apply the service scheme to a domain.

Precautions

In traditional NAC mode, the authorization scheme is not supported.

If the service scheme to be configured does not exist, the **service-scheme (AAA view)** command creates a service scheme and displays the service scheme view. If the service scheme to be configured already exists, the **service-scheme (AAA view)** command displays the service scheme view.

To delete or modify the service scheme applied to a domain, run the **undo service-scheme (AAA domain view)** command to unbind the service scheme from the domain.

Example

Create a service scheme **srvscheme1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme srvscheme1
[HUAWEI-aaa-service-srvscheme1]
```

13.1.102 state (AAA domain view)

Function

The **state** command configures the state of a domain.

The **undo state** command restores the state of a domain.

By default, a domain is in active state after being created.

Format

state { **active** | **block** [**time-range** *time-name* &<1-4>] }

undo state [**block time-range** [*time-name* &<1-4>]]

Parameters

Parameter	Description	Value
active	Sets the domain state to active.	-

Parameter	Description	Value
block	Sets the domain state to blocking.	-
time-range *time-name*	Indicates the block time range of the domain. *time-name* specifies the name of the block time range. If this parameter is not specified, the domain is always blocked.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word **all** cannot be specified as a time range name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If exceptions occur during service configuration, set the domain in blocking state to block access of new users. After the service configuration is complete, set the domain in active state.

Prerequisite

Before specifying the *time-name* parameter, ensure that the time range has been created using the **time-range** command.

Precautions

After the **state block** command is run to set the domain state to block, online users in the domain are not affected.

After the **state block time-range** command is run to set the state of a domain including online users to block, the domain state turns from active to block within the specified time range, and online users are forced to go offline.

Example

Set the state of the domain **vipdomain** to blocking.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain vipdomain
[HUAWEI-aaa-domain-vipdomain] state block
```

Set the name of the time range in which the **vipdomain** domain state turns to block to **tim**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain vipdomain
[HUAWEI-aaa-domain-vipdomain] state block time-range tim
Warning: This operation may cause online users to go offline. Continue? [Y/N]Y
```

13.1.103 statistic enable (AAA domain view)

Function

The **statistic enable** command enables traffic statistics collection for domain users.

The **undo statistic enable** command disables traffic statistics collection for domain users.

By default, traffic statistics collection is disabled for domain users.

NOTE

After the **statistic enable** command is executed, statistics about both IPv4 and IPv6 upstream and downstream traffic will be collected. After the **accounting dual-stack separate** command is executed, IPv4 and IPv6 traffic statistics will be collected separately. The following describes the traffic statistics function.

- On the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, statistics about both IPv4 and IPv6 upstream and downstream traffic can be collected only when the user access mode is the **multi-share** mode.
- On the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, after an authentication profile in which the user access mode is set to **multi-share** is applied to an Eth-Trunk interface, the device does not support the collection of statistics about both IPv4 and IPv6 upstream and downstream traffic for the users bound to the authentication profile.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, after an authentication profile in which the user access mode is set to **multi-share** is applied to an Eth-Trunk interface, the device does not support the collection of statistics about both IPv4 and IPv6 upstream and downstream traffic for the users bound to the authentication profile.
- In a single-MAC multi-IP scenario, only IPv4 traffic statistics can be collected.
- The device does not support Layer 3 IPv6 Portal authentication or traffic statistics collection of Layer 3 IPv6 Portal authentication users.
- If a device does not support Layer 2 IPv6 Portal authentication, the device can collect statistics about IPv4 and IPv6 upstream and downstream traffic after Portal authentication is triggered for IPv4 users. The following devices do not support Layer 2 IPv6 Portal authentication: S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, and S6720S-S.

Format

statistic enable

undo statistic enable

Parameters

None

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement traffic-based accounting, you can use this command to enable traffic statistics collection for a domain. Then the device collects traffic statistics for the users in the domain. If an accounting server is configured, the device sends traffic statistics to the accounting server through accounting packets so that the server performs accounting for the users based on traffic statistics.

Follow-up Procedure

Run the **display access-user** command to view traffic statistics of users.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

For the S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, if users are authorized with CAR during the configuration of traffic statistics collection, only CAR takes effect, and traffic statistics collection does not take effect.

This command collects service statistics for domain users. The device sends the statistics to the accounting server.

On the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI:

- Traffic statistics are collected based on interfaces.
- The traffic statistics collection is valid for domain users only when interfaces are physical interface and each interface connects to only one domain user.
- The interface traffic statistics for the first 15s when a user goes online are not collected.
- When users are online, you cannot run the **reset_counters_interface** command to clear interface traffic statistics. Otherwise, the user traffic statistics are inaccurate.

Example

Enable traffic statistics collection for domain users.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] statistic enable
```

13.1.104 system recording-scheme

Function

The **system recording-scheme** command applies a policy in a recording scheme to record the system events.

The **undo system recording-scheme** command deletes a policy from a recording scheme. System events are not recorded then.

By default, system events are not recorded.

Format

system recording-scheme *recording-scheme-name*

undo system recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system events recorded on an HWTACACS server help you monitor devices. When network faults occur, you can isolate faults based on the system events recorded on the HWTACACS server.

Prerequisites

A recording scheme has been created using the **recording-scheme** command in the AAA view and an HWTACACS server template has been associated with a recording scheme using the **recording-mode hwtacacs** command in the recording scheme view.

Precautions

Currently, the device can record only the events caused by the **reboot** command.

Example

Apply a policy in the recording scheme **scheme** to record the system events.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template hw1
[HUAWEI-hwtacacs-hw1] quit
[HUAWEI] aaa
[HUAWEI-aaa] recording-scheme scheme
[HUAWEI-aaa-recording-scheme] recording-mode hwtacacs hw1
[HUAWEI-aaa-recording-scheme] quit
[HUAWEI-aaa] system recording-scheme scheme
```

13.1.105 unload security weak-password-dictionary

Function

The **unload security weak-password-dictionary** command uninstalls a weak password dictionary.

Format

unload security weak-password-dictionary

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to uninstall the weak password dictionary from the system.

Example

Unload a weak password dictionary.

```
<HUAWEI> system-view
[HUAWEI] unload security weak-password-dictionary
```

13.1.106 user-group (AAA domain view)

Function

The **user-group** command binds the users in a domain to the authorization information of a user group.

The **undo user-group** command unbinds the users in a domain from the authorization information of a user group.

By default, no authorization information of a user group is bound to the users in a domain.

NOTE

This command is supported only in the NAC common mode.

Format

user-group *group-name*

undo user-group

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The user group name must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **user-group** command in the AAA domain to bind the users in a domain to the authorization information of a user group.

Precautions

- The user group to be specified using the **local-user user-group** command must have been created using the **user-group** command.
- A user group cannot be deleted after being referenced to a domain using this command.
- Huawei proprietary attribute 82 delivered by RADIUS cannot be used together with the function of binding authentication information of a user group to a domain.
- The priority of the authorization information delivered using this command is lower than that of the authorization information delivered using the **portal free-rule** *rule-id* **source ip** *ip-address* **mask** { *mask-length* | *ip-mask* } [**mac** *mac-address*] [**interface** *interface-type interface-number*] **destination user-group** *group-name* command.

Example

Bind the user group **group1** to the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] user-group group1
```

13.1.107 user-password complexity-check

Function

The **user-password complexity-check** command enables password complexity check.

The **undo user-password complexity-check** command disables password complexity check.

By default, password complexity check is enabled on a device. A password must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

Format

user-password complexity-check [**three-of-kinds** | enhance]

undo user-password complexity-check

Parameters

Parameter	Description	Value
three-of-kinds	Indicates that a password must contain at least three of the following: uppercase letters, lowercase letters, digits, and special characters.	-
enhance	Indicates enhanced password complexity check. A password must contain at least eight characters, including at least three of the following: digits, lowercase letters, uppercase letters, and special characters. The password and user name cannot contain each other (regardless of the case). Otherwise, the password cannot pass the complexity check.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the versions earlier than V200R003, the device uses simple user name and password rules, so the user names and passwords are easy to manage and remember; however, weak passwords have security risks. In V200R003 and later versions, the device poses stricter requirements on user names and passwords. After you create a local user using the **local-user** command, the password must pass a complexity check performed by the device.

You can choose whether to enable password complexity check in V200R005 and later versions.

Precautions

To ensure device security, ensure that password complexity check is enabled and change the password periodically.

Example

Disable password complexity check.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo user-password complexity-check
```

13.1.108 vlan block-time

Function

The **vlan block-time** command sets the lockout time of VLANs in a VLAN pool.

The **undo vlan block-time** command restores the default lockout time of VLANs in a VLAN pool.

By default, the lockout time of VLANs in a VLAN pool is 30 minutes.

Format

vlan block-time *block-time*

undo vlan block-time

Parameters

Parameter	Description	Value
block-time	Specifies the lockout time of VLANs.	The value is an integer in the range of 5 to 1440, in minutes.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the VLAN assignment algorithm in a VLAN pool is set to **hash** and the **dhcp update vlan assignment** command has been run to enable the function of reassigning VLANs in the VLAN pool, a VLAN will be locked for 30 minutes by default and cannot be assigned to users after all IP addresses in the VLAN have been assigned. To adjust the lockout time of VLANs in the VLAN pool, run the **vlan block-time** command.

Prerequisites

The VLAN assignment algorithm has been set to **hash** using the **assignment hash** command.

Precautions

The **vlan block-time** command takes effect after the **dhcp update vlan assignment** command is run to enable the function of reassigning VLANs in the VLAN pool.

After the **assignment even** command is run, the **assignment hash** command configuration will be cleared. Exercise caution when running the **assignment even** command.

This function takes effect only for wired users.

Authentication access devices in the policy association scenario do not support this function.

Example

Set the lockout time of VLANs in a VLAN pool to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] assignment hash
[HUAWEI-vlan-pool-test] dhcp update vlan assignment
[HUAWEI-vlan-pool-test] vlan block-time 5
```

13.1.109 vlan pool

Function

The **vlan pool** command creates a VLAN pool and displays the VLAN pool view, or displays the view of an existing VLAN pool.

The **undo vlan pool** command deletes a VLAN pool.

By default, no VLAN pool is created on a device.

Format

vlan pool *pool-name*

undo vlan pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of a VLAN pool.	The value is a string of 1 to 31 characters. It cannot contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ")

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VLAN pool is a combination of multiple VLANs and is used to simplify network deployment. The administrator plans the VLANs of users in a department as a VLAN pool. After a user passes the authentication, the authentication server authorizes the VLAN pool to the user. The device allocates VLANs in the VLAN pool to users based on the VLAN assignment algorithm. In this way, VLANs can be planned for multiple departments without the need of calculating the number of users of each department.

On a WLAN, the access modes and access locations of wireless users are flexible. Users often connect to the same WLAN at a site such as the office entrance or stadium entrance, and then roam to WLANs covered by other APs. If each SSID has only one service VLAN to deliver wireless access to wireless users, IP address resources may become insufficient in areas where many wireless users access the WLAN, and IP addresses in the other areas are wasted. The VLAN pool can be configured as the service VLAN for wireless users so that one SSID can support multiple service VLANs simultaneously. New users are dynamically assigned to VLANs in the VLAN pool, which reduces the number of users in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

Follow-up Procedure

1. Run the **vlan** command to add VLANs to the VLAN pool.
2. Set the standard RADIUS attribute **Tunnel-Private-Group-ID** assigned to users who pass authentication by the RADIUS server so that wired users can be added to the specified VLAN pool.
3. For wireless users, three methods are available to apply a VLAN pool:
   - Run the **vap-profile** *profile-name* **wlan** *wlan-id* **radio** { *radio-id* | **all** } **service-vlan vlan-pool** *pool-name* command to configure the specified VLAN pool as the service VLAN of wireless users in the specified VAP profile.

  - Run the **service-vlan vlan-pool** *pool-name* command in the VAP profile view to configure the VLAN pool as the service VLAN of wireless users in the VAP profile.
  - On the RADIUS server, configure the standard RADIUS attribute **Tunnel-Private-Group-ID** for authenticated users to add the users to the specified VLAN pool.

Precautions

- After a VLAN pool is configured as a service VLAN for wireless users, the VLAN pool cannot be configured as the VLAN pool assigned to users who pass authentication by the RADIUS server.
- After a VLAN pool is configured as a service VLAN for wireless users, VLANs in the VLAN pool cannot be deleted. To delete the VLAN pool, cancel the service VLAN configuration of the VLAN pool.
- If a VLAN or the VLAN pool to which a VLAN belongs has been configured as a service VLAN for the WLAN network, the VLAN cannot be configured as a super-VLAN. Similarly, if a VLAN has been configured as a super-VLAN, the VLAN or the VLAN pool to which the VLAN belongs cannot be configured as a service VLAN for the WLAN network. In addition, if a VLAN pool has been configured as a service VLAN for a WLAN network, a super-VLAN cannot be added to the VLAN pool.
- In scenarios where a dual-stack address pool is configured, a user successfully obtains an IP address if the VLAN pool has assigned an IPv4 or IPv6 address to it. In this case, the VLAN pool will not assign a new VLAN to this user.

Example

Create the VLAN pool **test** and display the VLAN pool view.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test]
```

13.1.110 vlan (VLAN pool view)

Function

The **vlan** command adds VLANs to a VLAN pool.

The **undo vlan** command deletes VLANs from a VLAN pool.

By default, no VLAN is available in a VLAN pool.

Format

vlan { *start-vlan* [**to** *end-vlan*] } &<1-10> [**max-user** *number*]

undo vlan { { *start-vlan* [**to** *end-vlan*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
start-vlan [**to** *end-vlan*]	Specifies the range of VLAN IDs. *start-vlan* and *end-vlan* determine a VLAN range. *start-vlan* must be equal to or smaller than *end-vlan*.	The value is an integer in the range from 1 to 4094.
max-user *number*	Specifies the maximum number of users in a VLAN.	The value is an integer, varies according to the device model.

Views

VLAN pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VLAN pool is a combination of multiple VLANs. It is used to simplify network deployment. To add specified VLANs to a VLAN pool, run the **vlan (VLAN pool view)** command.

If the VLAN assignment algorithm of a VLAN pool is **hash**, you can specify **max-user** *number* to set the maximum number of users allowed in a specific VLAN based on the number of IP addresses in the IP address pool on the DHCP server. When the number of online users in the VLAN reaches the upper limit, users will not go online through the VLAN. This ensures that all online users can obtain IP addresses.

Precautions

- A maximum of 128 VLANs can be added to a VLAN pool.
- Deleting a VLAN will interrupt services of users using the VLAN. Exercise caution when you perform this operation.
- A nonexistent VLAN can also be added to a VLAN pool. However, you need to create the VLAN after adding a nonexistent VLAN to a VLAN pool; otherwise, the VLAN does not take effect.
- The VLAN reserved for a stack cannot be added to a VLAN pool.
- **max-user** *number* is valid only for users authorized a VLAN pool and takes effect only when the VLAN assignment algorithm of a VLAN pool is **hash**.

Example

Add VLANs 9, 12, 13, and 14 to the VLAN pool **test**.

```
<HUAWEI> system-view
[HUAWEI] vlan pool test
[HUAWEI-vlan-pool-test] vlan 9 12 to 14
```

13.2 RADIUS Configuration Commands

13.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.2.2 accounting-copy radius-server

Function

The **accounting-copy radius-server** command enables the RADIUS accounting packet copy function and configures a RADIUS server template for level-2 accounting.

The **undo accounting-copy radius-server** command disables the RADIUS accounting packet copy function.

By default, the RADIUS accounting packet copy function is disabled.

Format

accounting-copy radius-server *template-name*

undo accounting-copy radius-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The existing RADIUS server on the network performs authentication, authorization, and accounting for users. User login and logout information is sent to the server through accounting packets. Users want to deploy an independent RADIUS accounting server (called the level-2 RADIUS accounting server) to obtain user login and logout information for analyzing user behavior and managing users' access to the network. However, the device currently does not send accounting packets to the level-2 RADIUS accounting server. In this case, you can configure the RADIUS accounting packet copy function on the device. After this function is configured, the device sends user login and logout information to the level-2 RADIUS accounting server through accounting packets for third-party user behavior analysis.

Prerequisites

The RADIUS server template has been created using the **radius-server template** command.

Precautions

- Ensure that the IP address of the configured level-2 RADIUS accounting server is different from that of the level-1 RADIUS accounting server (including the active/standby RADIUS accounting server).
- Ensure that the level-2 RADIUS accounting server template configured in the domain is different from the RADIUS server template for authentication and accounting in the domain. If they are the same, the accounting-copy radius-server command cannot be configured and the system displays an error message during the command configuration.

Example

In the **test** domain, set the IP addresses of the RADIUS authentication and accounting servers to 10.1.1.1, their port numbers to 1813 and 1814, respectively, and RADIUS server template to **t1**. Set the IP address and port number of the RADIUS server for level-2 accounting to 10.1.1.2 and 1814, respectively, and the RADIUS server template to **t2**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template t1
[HUAWEI-radius-t1] radius-server authentication 10.1.1.1 1813
[HUAWEI-radius-t1] radius-server accounting 10.1.1.1 1814
[HUAWEI-radius-t1] quit
[HUAWEI] radius-server template t2
[HUAWEI-radius-t2] radius-server accounting 10.1.1.2 1814
[HUAWEI-radius-t2] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] radius-server t1
[HUAWEI-aaa-domain-test] accounting-copy radius-server t2
```

13.2.3 called-station-id mac-format

Function

The **called-station-id mac-format** command sets the encapsulation format of the MAC address in the called-station-id (Type 30) attribute of RADIUS packets.

The **undo called-station-id mac-format** command restores the default encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets.

By default, the encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets is XX-XX-XX-XX-XX-XX, in uppercase.

Format

called-station-id mac-format { **dot-split** | **hyphen-split** | **colon-split**} [**mode1** | **mode2**] [**lowercase** | **uppercase**]

called-station-id mac-format unformatted [**lowercase** | **uppercase**]

undo called-station-id mac-format

Parameters

Parameter	Description	Value
dot-split	Indicates that the dot (.) is used as the separator in a MAC address.	-
hyphen-split	Indicates that the hyphen (-) is used as the separator in a MAC address.	-
colon-split	Indicates that the colon (:) is used as the separator in a MAC address.	-
unformatted	Indicates that no separator is used in a MAC address.	-
mode1	Indicates that the MAC address in the calling-station-id attribute uses the XXXX-XXXX-XXXX, XXXX:XXXX:XXXX, or XXXX.XXXX.XXXX format.	-
mode2	Indicates that the MAC address in the calling-station-id attribute uses the XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, or XX.XX.XX.XX.XX.XX format.	-
lowercase	Indicates that the MAC address in the called-station-id attribute uses the lowercase.	-
uppercase	Indicates that the MAC address in the called-station-id attribute uses the uppercase.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Called-station-id (Type 30) attribute indicates the MAC address and SSID of an AP. The default format of the MAC address in the called-station-id attribute of RADIUS packets from the device is XX-XX-XX-XX-XX-XX. If the RADIUS server does not support the default format, run the **called-station-id mac-format** command to change the format.

Example

Set the dot as the separator in a MAC address and the encapsulation format of the MAC address in the called-station-id attribute to XX.XX.XX.XX.XX.XX in uppercase.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] called-station-id mac-format dot-split mode2 uppercase
```

13.2.4 called-station-id wlan-user-format

Function

The **called-station-id wlan-user-format** command sets the encapsulation content of the Called-station-id (30) attribute in RADIUS packets.

The **undo called-station-id wlan-user-format** command restores the default encapsulation content of the Called-station-id (30) attribute in RADIUS packets.

By default, the encapsulation content of the Called-station-id (30) attribute is the AP's MAC address and SSID separated with a colon (:), in the format of ap-mac:ssid.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this function.

Format

called-station-id wlan-user-format { **ap-mac** | **ac-mac** | **ac-ip** | **ap-name** | **ap-group-name** | **vlanid** | **ap-location** } [**include-ssid** [**delimiter** *delimiter*]]

undo called-station-id wlan-user-format

Parameters

Parameter	Description	Value
ap-mac	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AP's MAC address.	-

Parameter	Description	Value
ac-mac	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AC's MAC address.	-
ac-ip	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AC's IP address.	-
ap-name	Indicates that the encapsulation content of the Called-station-id (30) attribute is the AP name.	-
ap-group-name	Indicates that the encapsulation content of the Called-station-id (30) attribute is the name of the AP group to which the AP belongs.	-
vlanid	Indicates that the encapsulation content of the Called-station-id (30) attribute is the outer VLAN through which the user goes online.	-
ap-location	Indicates that the encapsulation content of the Called-station-id (30) attribute is location information of the AP.	-
include-ssid	Indicates that the encapsulation content of the Called-station-id (30) attribute contains the SSID. If this parameter is not specified, the encapsulation content of the Called-station-id (30) attribute does not contain the SSID.	-
delimiter *delimiter*	Specifies the delimiter before the SSID when the encapsulation content of the Called-station-id (30) attribute contains the SSID.	The value is of enumerated type. The value can be \ / : < > | @ ' % * + - & ! # ^ or ~. The default value is :.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Called-station-id (30) attribute indicates the number of the NAS. For wireless users, the default encapsulation content of this attribute is the AP's MAC address and SSID, in the format of ap-mac:ssid. You can run the **called-station-id wlan-user-format** command to modify the encapsulation content of this attribute based on the format of this attribute supported by the RADIUS server.

You can run the **called-station-id mac-format** command to set the encapsulation format of the MAC address of the AP or AC.

Example

Set the encapsulation content of the Called-station-id (30) attribute in RADIUS packets to the AC's MAC address without the SSID.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] called-station-id wlan-user-format ac-mac
```

13.2.5 calling-station-id mac-format

Function

The **calling-station-id mac-format** command sets the encapsulation format of the MAC address in the calling-station-id (Type 31) attribute of RADIUS packets.

The **undo calling-station-id mac-format** command restores the default encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets.

By default, the encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets is xxxx-xxxx-xxxx, in lowercase.

Format

calling-station-id mac-format { **dot-split** | **hyphen-split** | **colon-split** } [**mode1** | **mode2**] [**lowercase** | **uppercase**]

calling-station-id mac-format unformatted [**lowercase** | **uppercase**]

calling-station-id mac-format bin

undo calling-station-id mac-format

Parameters

Parameter	Description	Value
dot-split	Indicates that the dot (.) is used as the separator in a MAC address.	-
hyphen-split	Indicates that the hyphen (-) is used as the separator in a MAC address.	-
colon-split	Indicates that the colon (:) is used as the separator in a MAC address.	-
unformatted	Indicates that no separator is used in a MAC address.	-
mode1	Indicates that the MAC address in the calling-station-id attribute uses the XXXX-XXXX-XXXX, XXXX:XXXX:XXXX, or XXXX.XXXX.XXXX format.	-
mode2	Indicates that the MAC address in the calling-station-id attribute uses the XX-XX-XX-XX-XX-XX, XX:XX:XX:XX:XX:XX, or XX.XX.XX.XX.XX.XX format.	-
lowercase	Indicates that the MAC address in the calling-station-id attribute uses the lowercase.	-
uppercase	Indicates that the MAC address in the calling-station-id attribute uses the uppercase.	-
bin	Indicates that the MAC address in the calling-station-id attribute uses the binary form.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The default format of the MAC address in the calling-station-id (Type 31) attribute of RADIUS packets from the device is xxxx-xxxx-xxxx. If the RADIUS server does not support the default format, run the **calling-station-id mac-format** command to change the format.

Example

Set the dot as the separator in a MAC address and the encapsulation format of the MAC address in the calling-station-id attribute to XX.XX.XX.XX.XX.XX in uppercase.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] calling-station-id mac-format dot-split mode2 uppercase
```

13.2.6 display radius-attribute

Function

The **display radius-attribute** command displays the RADIUS attributes supported by the device.

Format

display radius-attribute [**name** *attribute-name* | **type** { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* }]

Parameters

Parameter	Description	Value
name *attribute-name*	Displays a specified RADIUS attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
type { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* }	Displays the RADIUS attribute of a specified type: - *attribute-number1* specifies the standard attribute. - **huawei** *attribute-number2* specifies a Huawei attribute. - **microsoft** *attribute-number3* specifies a Microsoft attribute. - **dslforum** *attribute-number4* specifies a Digital Subscriber Line Forum attribute.	The value of *attribute-number1*, *attribute-number2*, *attribute-number3*, or *attribute-number4* is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before connecting the device to a RADIUS server, run the **display radius-attribute** command to view the RADIUS attributes supported by the device. If the device and RADIUS server support different RADIUS attributes according to the command output, run the **radius-attribute disable** command on the device to disable RADIUS attributes that are not supported by the RADIUS server or run the **radius-attribute translate** command to translate RADIUS attributes.

Example

Display the RADIUS attributes supported by the device.

```
<HUAWEI> display radius-attribute
  Codes: Auth(Authentication), Acct(Accounting)
         Req(Request), Accp(Accept), Rej(Reject)
         Resp(Response), COA(Change-of-Authorization)
         0(Can not exist in this packet)
         1(Can exist in this packet)
-------------------------------------------------------------------------------
Attribute                Service   Auth Auth Auth Acct Acct COA COA
Name(Type)                  Type     Req  Accp Rej  Req  Resp Req Ack
-------------------------------------------------------------------------------
User-Name(1)                All      1    0    0    1    0    1   1
User-Password(2)            All      1    0    0    0    0    0   0
CHAP-Password(3)            All      1    0    0    0    0    0   0
NAS-IP-Address(4)           All      1    0    0    1    0    1   1
NAS-Port(5)                 All      1    0    0    1    0    1   1
Service-Type(6)             All      1    1    0    0    0    0   0
......
```

NOTE

The preceding information is an example. The displayed attribute type depends on the actual situation.

Table 13-23 Description of the **display radius-attribute** command output

Item	Description
0(Can not exist in this packet)	Attribute not supported in packets.
1(Can exist in this packet)	Attribute supported in packets.
Attribute Name(Type)	Attribute name and type.
Service Type	Protocol type of the attribute.
Auth Req	Authentication request packet.
Auth Accp	Authentication accept packet.

Item	Description
Auth Rej	Authentication reject packet.
Acct Req	Accounting request packet.
Acct Resp	Accounting response packet.
COA Req	Change of Authorization (COA) request packet.
COA Ack	COA acknowledgement packet.

Display the RADIUS attribute numbered 2.

```
<HUAWEI> display radius-attribute type 2
 Radius Attribute Type        : 2
 Radius Attribute Name        : User-Password
 Radius Attribute Description : This Attribute indicates the password of the user to be authenticated. Only 
valid for the PAP authentication.
 Supported Packets            : Auth Request
```

Table 13-24 Description of the **display radius-attribute type** command output

Item	Description
Radius Attribute Type	Type of the RADIUS attribute.
Radius Attribute Name	Name of the RADIUS attribute.
Radius Attribute Description	Description of the RADIUS attribute.
Supported Packets	Packets that support the RADIUS attribute.

13.2.7 display radius-attribute check

Function

The **display radius-attribute check** command displays the attributes to be checked in RADIUS Access-Accept packets.

Format

display radius-attribute [**template** *template-name*] **check**

Parameters

Parameter	Description	Value
template *template-name*	Displays the RADIUS attribute check configuration of a specified RADIUS server template.	The RADIUS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **radius-attribute check** command is executed to configure the attributes to be checked in RADIUS Access-Accept packets, you can use the **display radius-attribute check** command to view these attributes.

Example

Check the attributes to be checked in RADIUS Access-Accept packets.

```
<HUAWEI> display radius-attribute check
Server-template-name: test1
--------------------------------------------------
check-attr
--------------------------------------------------
Framed-Protocol
--------------------------------------------------
```

Table 13-25 Description of the **display radius-attribute check** command output

Item	Description
Server-template-name	Name of the RADIUS server template.
check-attr	Attributes to be checked in RADIUS Access-Accept packets.
Framed-Protocol	Encapsulation protocol for services of the Frame type.

13.2.8 display radius-attribute disable

Function

The **display radius-attribute disable** command displays the disabled RADIUS attributes.

Format

display radius-attribute [**template** *template-name*] **disable**

Parameters

Parameter	Description	Value
template *template-name*	Displays the disabled RADIUS attributes in a specified RADIUS server template. If this parameter is not specified, the disabled RADIUS attributes in all the RADIUS server templates are displayed.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display radius-attribute disable** command to view the RADIUS attributes disabled by using the **radius-attribute disable** command.

To enable a RADIUS attribute, run the **undo radius-attribute disable** command in the RADIUS server template view.

Example

Display the disabled RADIUS attributes on the device.

```
<HUAWEI> display radius-attribute disable
Packet-Type: Type of the RADIUS packets to be modified. 1 indicates valid; 0 ind
icates invalid. Bit 1 to bit 4 indicate the authentication request, authenticati
on accept, accounting request, and accounting response packets.

Server-template-name: d
--------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
```

```
-------------------------------------------------------------------------------
0            7           0           0          send      0 0 0 0
-------------------------------------------------------------------------------
```

Table 13-26 Description of the display radius-attribute disable command output

Item	Description
Server-template-name	RADIUS server template name.
Source-Vendor-ID	Vendor ID of the source attribute.
Source-Sub-ID	ID of the source attribute's sub-attribute.
Dest-Vendor-ID	Vendor ID of the destination attribute.
Dest-Sub-ID	ID of the destination attribute's sub-attribute.
Direct	Direction in which the attribute is translated. ● receive: Translates RADIUS attributes for received packets. ● send: Translates RADIUS attributes for sent packets.
Packet-Type	Type of RADIUS packets. ● 0: The RADIUS attributes of this type of packets are not translated. ● 1: The RADIUS attributes of this type of packets are translated.

13.2.9 display radius-attribute translate

Function

The **display radius-attribute translate** command displays the RADIUS attribute translation configuration.

Format

display radius-attribute [**template** *template-name*] **translate**

Parameters

Parameter	Description	Value
template *template-name*	Displays the RADIUS attribute translation configuration of a specified RADIUS server template. *template-name* specifies the name of the RADIUS server template that is created using the **radius-server template** command. If this parameter is not specified, the disabled RADIUS attributes translation configuration in all the RADIUS server templates are displayed.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **radius-attribute translate** command to configure the device to translate RADIUS attributes, run the **display radius-attribute translate** command to check the configuration.

Example

Display the RADIUS attribute translation configuration.

```
<HUAWEI> display radius-attribute translate
Packet-Type: Type of the RADIUS packets to be modified. 1 indicates valid; 0 indicates invalid. Bit 1 to bit 4
indicate the authentication request, authentication accept, accounting request, and accounting response
packets.

Server-template-name: rds
--------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
--------------------------------------------------------------------------------
0                6             0              40           receive     0 0 0 0
--------------------------------------------------------------------------------
Server-template-name: eee
--------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
--------------------------------------------------------------------------------
234567           123           2011           20           --          0 1 0 1
--------------------------------------------------------------------------------
```

Table 13-27 Description of the **display radius-attribute translate** command output

Item	Description
Server-template-name	Server template name.
Source-Vendor-ID	Vendor ID of the source attribute.
Source-Sub-ID	ID of the source attribute's sub-attribute.
Dest-Vendor-ID	Vendor ID of the destination attribute.
Dest-Sub-ID	ID of the destination attribute's sub-attribute.
Direct	Direction in which the attribute is translated. ● receive: Translates RADIUS attributes for received packets. ● send: Translates RADIUS attributes for sent packets.
Packet-Type	Type of RADIUS packets. ● 0: The RADIUS attributes of this type of packets are not translated. ● 1: The RADIUS attributes of this type of packets are translated.

13.2.10 display radius-server accounting-stop-packet

Function

The **display radius-server accounting-stop-packet** command displays information about accounting-stop packets on the RADIUS server.

Format

display radius-server accounting-stop-packet { **all** | **ip** { *ip-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Displays all the accounting-stop packets.	-
ip *ip-address*	Displays the accounting-stop packets with the specified IP address.	The value of *ip-address* is in dotted decimal notation.

Parameter	Description	Value
ip *ipv6-address*	Displays the accounting-stop packets with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display radius-server accounting-stop-packet** command output helps you check configurations or isolate faults.

Example

Display the accounting-stop packets with the IP address being 10.138.104.32.

```
<HUAWEI> display radius-server accounting-stop-packet ip 10.138.104.32
 ------------------------------------------------------------------------------
 Time Stamp  Resend Times  Session Time  Username
 ------------------------------------------------------------------------------
 1980409     6             22            g@rds
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

NOTE

When there are a large number of accounting-stop packets, the total number of accounting-stop packets (indicated by the **Total** field) is accurate. However, only some detailed data is displayed to ensure the user-friendly display on the CLI.

Table 13-28 Description of the display radius-server accounting-stop-packet command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.
Resend Times	Number of times that accounting-stop packets have been retransmitted. **NOTE** In active/standby mode, the number of retransmission times on the standby control board is not updated.
Session Time	Session time, in seconds.
Username	User name.

13.2.11 display radius-server authorization configuration

Function

The **display radius-server authorization configuration** displays the configuration of a RADIUS authorization server.

Format

display radius-server authorization configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check whether the configuration of a RADIUS authorization server is correct.

Example

Display the configuration of RADIUS authorization servers.

```
<HUAWEI> display radius-server authorization configuration
-----------------------------------------------------------------------------
 Attribute decode same as template    :  N
 Attribute encode same as template    :  Y
 User information match type          :  all
 Calling-station-id decode MAC-format :  xx-xx-xx-xx-xx-xx
 Port                                 :  3799

 Bounce port disable                  :  Y
 Down port disable                    :  N
-----------------------------------------------------------------------------
 Domain name       : test.com
 IP address        : -
 Shared-key        : ****************
 Group             : -
 Protect           : Y
 VPN-instance      : -
 ------------------------------------------------------------------------------
 1 RADIUS authorization server(s) in total
```

Table 13-29 Description of the **display radius-server authorization configuration** command output

Item	Description
Attribute decode same as template	Whether the device parses attributes in the RADIUS dynamic authorization packet based on the configuration in the RADIUS server template. To set this parameter, run the **radius-server authorization attribute-decode-sameastemplate** command.
Attribute encode same as template	Whether the device encapsulates attributes in the CoA or DM Response packet based on the configuration in the RADIUS server template. To set this parameter, run the **radius-server authorization attribute-encode-sameastemplate** command.
User information match type	Method in which a device checks whether the RADIUS attributes in the received CoA or DM Request packet match user information on the device: ● all: The device checks whether all RADIUS attributes in the received CoA or DM Request packet match user information on the device. ● any: The device checks whether a RADIUS attribute in the received CoA or DM Request packet matches user information on the device. To set this parameter, run the **radius-server authorization match-type** command.
Calling-station-id decode MAC-format	Format of the MAC address that can be parsed by the device and is configured in the system view in the Calling-Station-Id field of the CoA or DM Response packet. To set this parameter, run the **radius-server authorization calling-station-id decode-mac-format** command.
Port	Port number of a RADIUS authorization server. To set this parameter, run the **radius-server authorization port** command.

Item	Description
Bounce port disable	Whether the function of ignoring the authorization attribute indicating that the port is intermittently interrupted in a CoA packet is disabled. To set this parameter, run the **radius-server authorization hw-ext-specific command bounce-port disable** command.
Down port disable	Whether the function of ignoring the authorization attribute indicating that the port is disabled in a CoA packet is disabled. To set this parameter, run the **radius-server authorization hw-ext-specific command down-port disable** command.
Domain name	Domain name of a RADIUS accounting server.
IP-Address	IP address of a RADIUS authorization server. To set this parameter, run the **radius-server authorization** command.
Shared-key	Shared key of the RADIUS authorization server. To set this parameter, run the **radius-server authorization** command.
Group	RADIUS server group matching the RADIUS authorization server. To set this parameter, run the **radius-server authorization** command.
Protect	Whether the security hardening function is enabled. To set this parameter, run the **radius-server authorization** command.
vpn-instance	Name of the VPN instance that the RADIUS authorization server is bound to. To set this parameter, run the **radius-server authorization** command.

13.2.12 display radius-server configuration

Function

The **display radius-server configuration** command displays configuration information about a RADIUS server template.

Format

display radius-server configuration [**template** *template-name*]

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of a RADIUS server template. If this parameter is not specified, configuration information of all RADIUS server templates is displayed.	The RADIUS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the configuration of a RADIUS server template is completed or a RADIUS fault needs to be rectified, you can run this command to check whether the configuration of the RADIUS server template is correct.

Example

Display configuration information about the RADIUS server template named **shiva**.

```
<HUAWEI> display radius-server configuration template shiva
  ------------------------------------------------------------------------------
  Server-template-name          :  shiva
  Server-template-index         :  1
  Protocol-version              :  standard
  Traffic-unit                  :  B
  Shared-secret-key             :  ******
  Group-filter                  :  class
  Timeout-interval(in second)   :  5
  Retransmission                :  2
  EndPacketSendTime             :  0
```

```
  Dead time(in minute)          :  5
  Domain-included               :  YES
  NAS-IP-Address                :  -
  Calling-station-id MAC-format :  xxxx-xxxx-xxxx
  Called-station-id MAC-format  :  XX.XX.XX.XX.XX.XX
  NAS-Port-ID format            :  New
  Service-type                  :  -
  WLAN Called-station-id format :  ap-mac:ssid
  NAS-IPv6-Address              :  ::
  Server algorithm              :  master-backup
  Detect-interval(in second)    :  60
  Detect up-server(in second)   :  0
  Detect timeout(in second)     :  3
  Testuser-username             :  test
  Testuser-ciperpwd             :  %^%#.5*EDl^j_WXg[#Z>plj8;k|8.s*ju<_F~g9k`0*9%^%#
  Chargeable-user-identity      :  Not Support
  CUI Not reject                :  No
  Enable framed-ip-address      :  Yes
  Enable IPv4 traffic-statistics encapsulation :  No
  Authentication Server 1       :  10.7.66.66     Port:1812  Weight:80  [up]
                                   Vrf:- LoopBack:NULL Vlanif:NULL
                                   Source IP: ::
                                   Domain name: test.com
  Authentication Server 2       :  10.7.66.67     Port:1812  Weight:80  [up]
                                   Vrf:- LoopBack:NULL Vlanif:NULL
                                   Source IP: ::
                                   Domain name: test.com
  Accounting Server     1       :  10.7.66.66     Port:1813  Weight:80  [up]
                                   Vrf:- LoopBack:NULL Vlanif:NULL
                                   Source IP: ::
  Accounting Server     2       :  10.7.66.67     Port:1813  Weight:80  [up]
                                   Vrf:- LoopBack:NULL Vlanif:NULL
                                   Source IP: ::
  ------------------------------------------------------------------------------
```

Table 13-30 Description of the **display radius-server configuration template** *template-name* command output

Item	Description
Server-template-name	Name of a RADIUS server template. To set this parameter, run the **radius-server template** command.
Server-template-index	Index of a RADIUS server template.
Protocol-version	RADIUS protocol version: ● standard ● huawei ● iphotel ● portal

Item	Description
Traffic-unit	Traffic unit in the RADIUS server template. - B: Byte - KB: Kilobyte - MB: Megabyte - GB: Gigabyte To set this parameter, run the **radius-server traffic-unit** command.
Shared-secret-key	Shared key in the RADIUS server template. To set this parameter, run the **radius-server shared-key** command.
Group-filter	Filtering field of a user group. Currently, only the class field can be used as the filtering field of a user group.
Timeout-interval(in second)	Response timeout period of a RADIUS server. To set this parameter, run the **radius-server retransmit timeout** command.
Retransmission	Number of times RADIUS packets are retransmitted. To set this parameter, run the **radius-server retransmit timeout** command.
EndPacketSendTime	Number of times RADIUS accounting-stop packets are retransmitted. To set this parameter, run the **radius-server accounting-stop-packet resend** command.
Dead time(in minute)	Interval for the primary RADIUS server to revert to the active state. To set this parameter, run the **radius-server retransmit timeout** command.
Domain-included	Whether the RADIUS user name contains the domain name. - YES: The user name contains the domain name. - NO: The user name does not contain the domain name. - Original: The device does not modify the user name entered by the user. To set this parameter, run the **radius-server user-name domain-included** command.

Item	Description
NAS-IP-Address	NAS IP address in RADIUS packets.
Calling-station-id MAC-format	Encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets.
Called-station-id MAC-format	Encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets. To set this parameter, run the **called-station-id mac-format** command.
NAS-Port-ID format	Format of the NAS-Port-ID attribute on the RADIUS server. ● New: Uses the new format of the NAS-Port-ID attribute. ● New client-option82: Specifies that the content of the circuit ID suboption in the Option 82 field is encapsulated into the NAS-Port-ID attribute in a RADIUS packet. The format of the NAS-Port-ID attribute is the same as that of the suboption. ● Old: Uses the old format of the NAS-Port-ID attribute. ● vendor 9: Uses the NAS-Port-ID format of Cisco. To set this parameter, run the **radius-server nas-port-id-format** command.
Service-type	Service type.
WLAN Called-station-id format	Encapsulation content of the called-station-id (30) attribute in RADIUS packets. To set this parameter, run the **called-station-id wlan-user-format** command. **NOTE** Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this item.
NAS-IPv6-Address	NAS IPv6 address in RADIUS packets.

Item	Description
Server algorithm	Algorithm for selecting RADIUS servers: ● master-backup: specifies the algorithm for selecting RADIUS servers as packet-based primary/secondary. ● master-backup based-user: specifies the algorithm for selecting RADIUS servers as single user-based primary/secondary. ● loading-share: specifies the algorithm for selecting RADIUS servers as packet-based load balancing. ● loading-share based-user: specifies the algorithm for selecting RADIUS servers as single user-based load balancing. To set this parameter, run the **radius-server algorithm** command.
Detect-interval(in second)	Automatic detection interval for RADIUS servers in Down state. To set this parameter, run the **radius-server detect-server** command.
Detect up-server(in second)	Automatic detection interval for RADIUS servers in Up state. To set this parameter, run the **radius-server detect-server up-server interval** command.
Detect timeout(in second)	Timeout period for automatic RADIUS server detection packets. To set this parameter, run the **radius-server detect-server timeout** command.
Chargeable-user-identity	Whether the device supports the CUI attribute. The value can be: ● Not Support: The device does not support the CUI attribute. ● Support: The device supports the CUI attribute. To set this parameter, run the **radius-server support chargeable-user-identity** command.

Item	Description
CUI Not reject	Whether the device does not process the CUI attribute. The value can be: - No: The device processes the CUI attribute. - Yes: The device does not process the CUI attribute. To set this parameter, run the **radius-server support chargeable-user-identity** command.
Enable framed-ip-address	Whether the device is enabled to encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address. The value can be: - No: disabled - Yes: enabled To set this parameter, run the **radius-server framed-ip-address no-user-ip enable** command.
Enable IPv4 traffic-statistics encapsulation	Whether the function of separately encapsulating IPv4 traffic is enabled in the RADIUS server template: - Yes - No
Testuser-username	User name for automatic RADIUS server detection. To set this parameter, run the **radius-server testuser** command.
Testuser-ciperpwd	User password for automatic RADIUS server detection. To set this parameter, run the **radius-server testuser** command.
Authentication Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS authentication server. To set this parameter, run the **radius-server authentication** command.
Authentication Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS authentication server. To set this parameter, run the **radius-server authentication** command.

Item	Description
Accounting Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS accounting server. To set this parameter, run the **radius-server accounting** command.
Accounting Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS accounting server. To set this parameter, run the **radius-server accounting** command.
Domain name	Domain name of a RADIUS accounting server.

13.2.13 display radius-server dead-interval dead-count detect-cycle

Function

The **display radius-server dead-interval dead-count detect-cycle** command displays configuration information about the RADIUS server detection interval, number of times the RADIUS server detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval.

Format

display radius-server { **dead-interval** | **dead-count** | **detect-cycle** }

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the RADIUS server detection interval, number of times the RADIUS server detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval are configured using the **radius-server dead-**

interval dead-count detect-cycle command, you can run the **display radius-server** { **dead-interval** | **dead-count** | **detect-cycle** } command to check configuration information about the RADIUS server detection interval, number of times the RADIUS server detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval.

Example

Display configuration information about the RADIUS server detection interval.

```
<HUAWEI> display radius-server dead-interval
Radius server state detected internal is 5.
```

Display configuration information about the maximum number of consecutive packets that are not acknowledged by the RADIUS server in each detection interval.

```
<HUAWEI> display radius-server dead-count
Radius server state detected count is 2.
```

Display configuration information about the number of times the RADIUS server detection interval cycles.

```
<HUAWEI> display radius-server detect-cycle
Radius server down detect cycle is 2.
```

Table 13-31 Description of the **display radius-server** { **dead-interval** | **dead-count** | **detect-cycle** } command output

Item	Description
Radius server state detected internal is	Detection interval of the current RADIUS server.
Radius server state detected count is	Maximum number of consecutive packets that are not acknowledged by the RADIUS server.
Radius server down detect cycle is	Number of times the RADIUS server detection interval cycles.

13.2.14 display radius-server item

Function

The **display radius-server item** command shows the RADIUS server configuration.

Format

display radius-server item { **ip-address** { *ipv4-address* | *ipv6-address* } { **accounting** | **authentication** } | **template** *template-name* }

Parameters

Parameter	Description	Value
ip-address { *ipv4-address* | *ipv6-address* }	Specifies the IP address of the RADIUS server.	*ipv4-address*: The value is in dotted decimal notation. *ipv6-address*: The value is a 32-digit hexadecimal number.
accounting	Indicates the RADIUS accounting server.	-
authentication	Indicates the RADIUS authentication server.	-
template *template-name*	Specifies the RADIUS server template name.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display radius-server item** command shows the RADIUS server configuration.

Example

Display the configuration of RADIUS server template **rds**.

```
<HUAWEI> display radius-server item template rds
 ------------------------------------------------------------------------------
  STState     = STState-up
  STChgTime   = -
  Type        = auth-server
  State       = state-up
  AlarmFlag   = false
  STUseNum    = 1
  IPAddress   = 192.168.30.1
  AlarmTimer  = 0xffffffff
  Head        = 1057
  Tail        = 1311
  ProbeID     = 255
  Type        = acct-server
  State       = state-up
  AlarmFlag   = false
  STUseNum    = 1
  IPAddress   = 192.168.30.1
  AlarmTimer  = 0xffffffff
  Head        = 1057
```

```
 Tail       = 1311
 ProbeID    = 255
 Domain name   = test.com
------------------------------------------------------------------------------
```

Table 13-32 Description of the **display radius-server item** template command output

Item	Description
STState	RADIUS server template status: ● STState-up: indicates that the RADIUS server template is UP status. ● STState-down: indicates that the RADIUS server template is DOWN status.
STChgTime	Time when the RADIUS server template status changes.
Type	RADIUS server type: authentication or accounting server. ● auth-server: indicates authentication server. ● acct-server: indicates accounting server.
State	RADIUS server status: ● state-up: indicates the Up state. ● state-down: indicates the Down state. ● state-force-up: indicates the forcible Up state. ● state-probe: indicates the detection state.
AlarmFlag	Alarm flag. ● true: indicates that an alarm about status change has been sent. ● false: indicates that an alarm about status change is not sent.
STUseNum	RADIUS server template ID.
IPAddress	RADIUS server IP address.
AlarmTimer	ID of the alarm timer.
Head	Head pointer used to allocate the ID to RADIUS packets.
Tail	Tail pointer used to allocate the ID to RADIUS packets.
ProbeID	ID of probe packets.
Domain name	Domain name of a RADIUS accounting server.

13.2.15 display radius-server max-unresponsive-interval

Function

The **display radius-server max-unresponsive-interval** command displays configuration information about the longest unresponsive interval of a RADIUS server.

Format

display radius-server max-unresponsive-interval

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the longest unresponsive interval of a RADIUS server is configured using the **radius-server max-unresponsive-interval** command, you can run the **display radius-server max-unresponsive-interval** command to display configuration information about the longest unresponsive interval of the RADIUS server.

Example

Display configuration information about the longest unresponsive interval of the RADIUS server.

```
<HUAWEI> display radius-server max-unresponsive-interval
Radius server max non-response interval(in seconds) is 400.
```

Table 13-33 Description of the **display radius-server max-unresponsive-interval** command output

Item	Description
Radius server max non-response interval(in seconds) is	Longest unresponsive interval of the current RADIUS server.

13.2.16 display radius-server session-manage configuration

Function

The **display radius-server session-manage configuration** command displays session management configuration on the RADIUS server.

Format

display radius-server session-manage configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After session management is enabled using the **radius-server session-manage** command on the RADIUS server, you can run this command to view session management configuration.

Example

Display session management configuration on the RADIUS server.

```
<HUAWEI> display radius-server session-manage configuration
 ------------------------------------------------------------------------------
 Session Manage Enable : True    Session Manage AnyServer : False
 ------------------------------------------------------------------------------
 IP Address      VPN Instance                     Shared-key
 ------------------------------------------------------------------------------
 10.1.1.1        -                           ****************
 ------------------------------------------------------------------------------
 1 Radius session manage server(s) in total
```

Table 13-34 Description of the **display radius-server session-manage configuration** command output

Item	Description
Session Manage Enable	Whether session management is enabled: - True: enabled - False: disabled To set this parameter, run the **radius-server session-manage** command.

Item	Description
Session Manage AnyServer	Whether any RADIUS session management server is configured: ● True: configured ● False: not configured
IP Address	IP address of the RADIUS session management server.
VPN Instance	Name of the VPN instance bound to the RADIUS session management server.
Shared-key	Shared key of the RADIUS session management server.
Radius session manage server(s) in total	Number of the RADIUS session management servers.

13.2.17 radius-attribute check

Function

The **radius-attribute check** command enables the device to check the specified attributes in the received RADIUS Access-Accept packets.

The **undo radius-attribute check** command disables the device from checking the specified attributes in the received RADIUS Access-Accept packets.

By default, the device does not check whether a RADIUS Access-Accept packet contains the specified attributes.

Format

radius-attribute check *attribute-name*

undo radius-attribute check [*attribute-name*]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of the RADIUS attribute. If this parameter is specified, the RADIUS Access-Accept packets are checked based on attribute names.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **radius-attribute check** command is executed, the device checks whether the received RADIUS Access-Accept packets contain the specified attributes. If yes, the device considers that authentication was successful; if not, the device considers that authentication failed and discards the packet. For example, after the **radius-attribute check filter-id** command is executed, the device checks the filter-id attribute in the received RADIUS Access-Accept packets. If a RADIUS packet does not contain this attribute, authentication fails.

Precautions

- When you use the **undo radius-attribute check** command with parameters, the device checks the specified attributes in the RADIUS Access-Accept packets. When you use the **undo radius-attribute check** command without any parameter, the device does not check RADIUS Access-Accept packets.
- The **display radius-attribute** can display RADIUS attribute names.

Example

Check whether the RADIUS Access-Accept packets contain the framed-protocol attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-attribute check framed-protocol
```

13.2.18 radius-attribute cut hw-portal-url

Function

The **radius-attribute cut hw-portal-url** command deletes the specified content from the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

The **undo radius-attribute cut hw-portal-url** command configures the device not to process the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

By default, the device does not process the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

Format

radius-attribute cut hw-portal-url *key-words* [**end** *mark*]

undo radius-attribute cut hw-portal-url

Parameters

Parameter	Description	Value
key-words	Specifies the start keyword of the content to be deleted.	The value is a string of 3 to 64 characters. It must start with an ampersand (&) and end with an equal sign (=). Spaces are not allowed.
end *mark*	Specifies the end character of the content to be deleted. If no end character is configured, all the characters following *key-words* in the URL will be deleted.	Currently, the end character can only be an ampersand (&).

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

This command is used to perform special processing on the URL delivered by the RADIUS server using the Huawei RADIUS attribute 26-156 (HW-Portal-URL) to meet interconnection requirements. Generally, this command does not need to be configured.

Example

Delete the character string **&portal=** and the content following **&portal=** from the URL contained in the Huawei RADIUS attribute 26-156 (HW-Portal-URL).

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-attribute cut hw-portal-url &portal=
```

13.2.19 radius-server max-unresponsive-interval

Function

The **radius-server max-unresponsive-interval** command displays the maximum interval during which the RADIUS server does not respond.

The **undo radius-server max-unresponsive-interval** command restores the default setting.

By default, the maximum interval during which the RADIUS server does not respond is 300 seconds.

Format

radius-server max-unresponsive-interval *interval*

undo radius-server max-unresponsive-interval

Parameters

Parameter	Description	Value
interval	Specifies the maximum interval during which the RADIUS server does not respond.	The value is an integer in the range of 10 to 7200, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the user access frequency is low and the device receives only a few authentication request packets sourced from users, the device cannot detect the RADIUS server status by periodically detecting authentication request packets. In this case, you can configure the function of setting the RADIUS server status to Down if no response is received from the server for a long period of time to ensure that users can obtain escape authorization. When the interval between two consecutive unresponded authentication request packets is greater than the interval configured using the **max-unresponsive-interval** command, the RADIUS server is set to Down.

Precautions

To check the RADIUS server status, run the **display radius-server configuration** command. If the RADIUS server status is Down, the device records logs and alarms. For details about logs, see **RDS/4/RDAUTHDOWN**. For details about alarms, see **RDS_1.3.6.1.4.1.2011.5.25.40.15.2.2.1.2 hwRadiusAuthServerDown**.

Example

Set the maximum interval during which the RADIUS server does not respond to 100s.

```
<HUAWEI> system-view
[HUAWEI] radius-server max-unresponsive-interval 100
```

13.2.20 radius-attribute disable

Function

The **radius-attribute disable** command disables a RADIUS attribute.

The **undo radius-attribute disable** command enables a disabled RADIUS attribute.

By default, no RADIUS attribute is disabled.

Format

radius-attribute disable *attribute-name* { **receive** | **send** } *

undo radius-attribute disable [*attribute-name*]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of a RADIUS attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
receive	Disables a RADIUS attribute for received packets.	-
send	Disables a RADIUS attribute for sent packets.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Generally, a RADIUS server connects to multiple network devices, which can be one vendor's devices or different vendors' devices. If some vendors' devices require the RADIUS server to deliver an attribute to support a specified feature but other vendors' device do not support the delivered attribute, the RADIUS attribute may fail to be parsed.

The device may communicate with RADIUS servers of different vendors. Some RADIUS servers require the device to send some attributes but other RADIUS servers cannot process the attributes. Errors may occur.

The **radius-attribute disable** command disables RADIUS attributes on the device. You can configure the device to ignore incompatible attributes when receiving RADIUS packets to prevent parsing failures. You can also configure the device to disable RADIUS attributes when sending RADIUS packets. When the device sends RADIUS packets, it does not encapsulate the disabled RADIUS attributes in the RADIUS packets.

Prerequisites

The RADIUS attribute translation function has been enabled using the **radius-server attribute translate** command.

Precautions

Before disabling RADIUS attributes, run the **display radius-attribute** command to view the RADIUS attributes supported by the device.

Example

Disable the Frame-Route attribute in sent packets.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server attribute translate
[HUAWEI-radius-test1] radius-attribute disable framed-route send
```

13.2.21 radius-attribute nas-ip

Function

The **radius-attribute nas-ip** command sets the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.

The **undo radius-attribute nas-ip** command deletes the configured NAS-IP-Address attribute.

By default, the source IP address of the NAS is the NAS-IP-Address attribute value.

Format

radius-attribute nas-ip { *ip-address* | **ap-info** }

undo radius-attribute nas-ip [**ap-info**]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ap-info** parameter.

Parameters

Parameter	Description	Value
ip-address	Specifies the NAS-IP-Address attribute value in RADIUS packets sent by the device. In wireless scenarios, when a device functions as an AC, the IP address of the AC is specified as the NAS-IP-Address attribute value in RADIUS packets sent by the device.	The value is a valid unicast address in dotted decimal notation.
ap-info	The IP address of the AP is specified as the NAS-IP-Address attribute value in RADIUS packets sent by the device when the device functions as an AC in a wireless scenario.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A RADIUS server uses the NAS-IP-Address attributes in RADIUS packets sent by NASs to identify NASs. You can run the **radius-attribute nas-ip** command in the RADIUS server template view to set the NAS-IP-Address attribute.

When the RADIUS server interconnected with the device requires that the NAS-IP-Address attribute value is the IP address of the AP when the device functions as an AC in a wireless scenario, you need to run the **radius-attribute nas-ip ap-info** command.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Precautions

If the RADIUS NAS-IP-Address attribute is set to an invalid IP address, the configuration fails and an error message is displayed.

Example

Set the RADIUS NAS-IP-Address attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-attribute nas-ip 10.3.3.3
```

13.2.22 radius-attribute nas-ipv6

Function

The **radius-attribute nas-ipv6** command sets the NAS-IPv6-Address attribute in a RADIUS packet sent from a network access server (NAS).

The **undo radius-attribute nas-ipv6** command deletes the configured NAS-IPv6-Address attribute.

By default, no NAS-IPv6-Address attribute is configured.

Format

radius-attribute nas-ipv6 *ipv6-address*

undo radius-attribute nas-ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies the NAS-IPv6-Address attribute in a RADIUS packet.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The RADIUS server uses IP addresses to identify different NASs. The NAS-IPv6-Address attribute in a RADIUS packet can be configured using the **radius-attribute nas-ipv6** command in the RADIUS template.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Precautions

If the RADIUS NAS-IP-Address attribute is set to an invalid IP address, the configuration fails and an error message is displayed.

Example

Set the RADIUS NAS-IPv6-Address attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-attribute nas-ipv6 FC00::7
```

13.2.23 radius-attribute service-type with-authenonly-reauthen

Function

The **radius-attribute service-type with-authenonly-reauthen** command sets the reauthentication mode to reauthentication only.

The **undo radius-attribute service-type with-authenonly-reauthen** command restores the reauthentication mode to reauthentication and reauthorization.

By default, the reauthentication mode is reauthentication and reauthorization.

Format

radius-attribute service-type with-authenonly-reauthen

undo radius-attribute service-type with-authenonly-reauthen

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user needs to be reauthenticated, the device delivers authorization information to all online users after the user is successfully authenticated. If many online users and authorization configurations exist on the device, the device cannot promptly deliver authorization information, causing an authorization failure and user disconnection. After the **radius-attribute service-type with-authenonly-reauthen** command is run in the RADIUS server template view, the device only reauthenticates users during reauthentication, and does not redeliver authorization information, preventing users from going offline due to authorization failures.

Precautions

After the **radius-attribute service-type with-authenonly-reauthen** command is configured, users still use the original authorization information after being successfully reauthenticated even if the user authorization information changes.

This function takes effect only when the Service-Type attribute of a RADIUS server is **Authenticate Only**.

After the reauthentication mode is set to reauthentication only, the user name remains unchanged during reauthentication.

If server authorization packets carry the following attributes during reauthentication, this function does not take effect, but changes to the following authorization are still supported:

- User-Name authorized by the server
- CUI attribute authorized by the server
- Maximum number of users who are allowed to access the network using the same user name

Example

Set the reauthentication mode to reauthentication only.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] radius-attribute service-type with-authenonly-reauthen
```

13.2.24 radius-attribute set

Function

The **radius-attribute set** command modifies the RADIUS attributes.

The **undo radius-attribute set** command restores the default RADIUS attributes.

By default, values of the RADIUS attributes are not modified.

Format

radius-attribute set *attribute-name attribute-value* [**auth-type** { **dot1x** | **mac** | **portal** } | **user-type ipsession**]

undo radius-attribute set *attribute-name* [**auth-type** { **dot1x** | **mac** | **portal** } | **user-type ipsession**]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of the attribute to be modified.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name. Common attribute names are as follows: ● NAS-Identifier ● NAS-Port ● NAS-Port-Id ● NAS-Port-Type ● NAS-Identifier ● NAS-Port ● NAS-Port-Id ● NAS-Port-Type ● NAS-Identifier ● NAS-Port For details about other attribute names and values, see RADIUS Attributes.
attribute-value	Indicates the value of the attribute to be modified.	The value of *attribute-value* is automatically displayed.
auth-type { **dot1x** | **mac** | **portal** }	Specifies the user authentication type: ● **dot1x**: 802.1X authentication ● **mac**: MAC address authentication ● **portal**: Portal authentication Only the Service-Type attribute supports this parameter.	-
user-type ipsession	Specifies the users with user type being IP session. Only the Service-Type attribute supports this parameter.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The RADIUS attribute values of different vendors are different. To ensure that Huawei device can successfully communicate with the devices of other vendors, run the **radius-attribute set** command to modify the RADIUS attribute values.

For example, the Huawei device uses Service-Type value 2 to indicate an authentication request from a common user by default, while a non-Huawei RADIUS server uses Service-Type value 1 to indicate an authentication request from a common user; you can run the **radius-attribute set service-type 1** command to change the Service-Type value on the device so that the device can communicate with the RADIUS server.

Precautions

- The **radius-attribute set** command can modify only the RADIUS attributes in the authentication or accounting request packets sent from a device to the RADIUS server, and cannot modify the RADIUS attributes in the packets sent from the RADIUS server to a device.

  If you run the **display radius-attribute** command to check the RADIUS attributes supported by a device and the **Auth Req** or **Acct Req** field in the command output displays 1, the RADIUS attributes supported by the device can be carried in the authentication or accounting request packets sent from the device to the RADIUS server.

  Among the RADIUS attributes that can be carried in the authentication or accounting packets sent from the device to the RADIUS server, you cannot run the **radius-attribute set** command to modify the following attributes: User-Password, Agent-Circuit-Id, Agent-Remote-Id, NAS-IP-Address, NAS-IPv6-Address, CHAP-Password, CHAP-Challenge, EAP-Message, Framed-Interface-Id, Framed-IPv6-Prefix, Message-Authenticator, State, and Class.
- The type of the attribute modified by the **radius-attribute set** command cannot be changed.
- During MAC address authentication, the default value of the RADIUS attribute Service-Type is 10. When a fixed user name is used for MAC address authentication, you need to run the **radius-attribute set service-type 2 auth-type mac** command to set the RADIUS attribute Service-Type to 2.

Example

Create the template **temp1** and set the Service-Type attribute value to 1.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-attribute set service-type 1
```

13.2.25 radius-attribute translate

Function

The **radius-attribute translate** command configures a RADIUS attribute to be translated.

The **undo radius-attribute translate** command cancels the configuration.

By default, no RADIUS attribute is translated.

Format

radius-attribute translate *src-attribute-name dest-attribute-name* { **receive** | **send** | **access-accept** | **access-request** | **account-request** | **account-response** } *

radius-attribute translate extend vendor-specific *src-vendor-id src-sub-id dest-attribute-name* { **access-accept** | **account-response** } *

radius-attribute translate extend *src-attribute-name* **vendor-specific** *dest-vendor-id dest-sub-id* { **access-request** | **account-request** } *

undo radius-attribute translate [*src-attribute-name*]

undo radius-attribute translate extend *src-attribute-name*

undo radius-attribute translate extend vendor-specific *src-vendor-id src-sub-id*

Parameters

Parameter	Description	Value
src-attribute-name	Specifies the name of the source attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
dest-attribute-name	Specifies the name of the destination attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
receive	Translates RADIUS attributes for received packets.	-

Parameter	Description	Value
send	Translates RADIUS attributes for sent packets.	-
access-request	Translates RADIUS attributes for Authentication Request packets.	-
account-request	Translates RADIUS attributes for Accounting Request packets.	-
access-accept	Translates RADIUS attributes for Authentication Accept packets.	-
account-response	Translates RADIUS attributes for Accounting Response packets.	-
extend	Translates extended RADIUS attributes.	-
vendor-specific *src-vendor-id src-sub-id*	Specifies the source extended attribute to be translated. ● *src-vendor-id*: The vendor ID in the extended RADIUS attributes needs to be translated. ● *src-sub-id*: The sub ID in the RADIUS attributes needs to be translated.	● The value of *src-vendor-id* is an integer ranging from 1 to 4294967295. ● The value of *src-sub-id* is an integer ranging from 1 to 255.
vendor-specific *dest-vendor-id dest-sub-id*	Specifies the destination extended attribute to be translated. ● *dest-vendor-id*: The vendor ID in the extended RADIUS attributes needs to be translated. ● *dest-sub-id*: The sub ID in the extended RADIUS attributes needs to be translated.	● The value of *dest-vendor-id* is an integer ranging from 1 to 4294967295. ● The value of *dest-sub-id* is an integer ranging from 1 to 255.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Currently, RADIUS servers of different vendors may support different RADIUS attributes and have vendor-specific RADIUS attributes. To communicate with different RADIUS servers, the device provides the RADIUS attribute translation function. After RADIUS attribute translation is enabled, the device can translate RADIUS attributes when sending or receiving packets.

RADIUS attribute translation is used in the following modes:

- Format translation for the same attribute

  This mode is widely applied. It solves the problem of compatibility because different users have different requirements for the format of a RADIUS attribute.
- Translation between different attributes

  This mode is used because different vendors have different implementations of RADIUS attributes.

  For example, the device delivers the priority of the administrator by using the Huawei proprietary attribute HW-Exec-Privilege (26-29), whereas another vendor's device delivers it by using the Login-service (15) attribute. When the device and the vendor's device use the same RADIUS server on a network, the device is required to deliver the priority of the administrator by using the Login-service (15) attribute. After the **radius-attribute translate** command is configured, the device automatically processes the Login-service attribute in the received RADIUS authentication response packet as the HW-Exec-Privilege attribute.

Prerequisites

RADIUS attribute translation has been enabled by using the **radius-server attribute translate** command.

Before configuring RADIUS attribute translation, run the **display radius-attribute** command to view the RADIUS attributes supported by the device.

Precautions

- When the device sends packets, if attribute A is to be translated to attribute B, the type of the encapsulated attribute is the same as that of attribute B but the attribute content and format are the same as those of attribute A.
- When the device receives packets, if attribute A is to be translated to attribute B, the device parses the received attribute A as attribute B.

- When the device receives packets, it cannot translate the attributes of CoA packets.
- Three commands are available to translate RADIUS attributes:
  - To translate the attributes supported by the device to other attributes also supported by the device, run the **radius-attribute translate** command.
  - To translate the non-Huawei attributes not supported by the device to the attributes supported by the device, run the **radius-attribute translate extend vendor-specific** command.
  - To translate the attributes supported by the device to the non-Huawei attributes not supported by the device, run the **radius-attribute translate extend** command.
- The RADIUS attribute consists of Type, Length, and Value fields. A device can translate a non-Huawei RADIUS attribute (specified using the *src-sub-id* and *dest-sub-id* parameters) only when the length of the Type field in the RADIUS attribute is 1 byte.
- The device can translate the RADIUS attribute only when the type of the source RADIUS attribute is the same as that of the destination RADIUS attribute. For example, the types of NAS-Identifier and NAS-Port-Id attributes are string, and they can be translated into each other. The types of NAS-Identifier and NAS-Port attributes are string and integer respectively, they cannot be translated into each other.

Example

Configure the device to translate NAS-Identifier into NAS-Port-Id when sending RADIUS packets.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-server attribute translate
[HUAWEI-radius-temp1] radius-attribute translate nas-identifier nas-port-id send
```

Translate the Cisco No. 2 attribute (vendor ID 9) in Authentication Accept and Accounting Response packets to Huawei No. 155 extended attribute HW-URL-Flag.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-server attribute translate
[HUAWEI-radius-temp1] radius-attribute translate extend Vendor-Specific 9 2 HW-URL-Flag access-accept account-response
```

Translate the Huawei No. 153 extended attribute HW-Access-Type in Authentication Request and Accounting Request packets to Cisco No. 11 attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template temp1
[HUAWEI-radius-temp1] radius-server attribute translate
[HUAWEI-radius-temp1] radius-attribute translate extend HW-Access-Type vendor-specific 9 11 access-request account-request
```

13.2.26 radius-reject local

Function

The **radius-reject local** command configures the device to perform local authentication on administrators if administrators are rejected during RADIUS authentication.

The **undo radius-reject local** command restores the default configuration.

By default, the device does not perform local authentication on administrators if administrators are rejected during RADIUS authentication.

Format

radius-reject local

undo radius-reject local

Parameters

None

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, after the RADIUS server responds to a user with an Access-Reject packet, the authentication process ends and the user fails the authentication. If you want administrators to go online through local authentication after they are rejected during RADIUS authentication, run the **radius-reject local** command.

Precautions

- This function takes effect only for administrators.
- The authentication method must be RADIUS authentication+local authentication.

Example

Configure the device to perform local authentication on administrators if administrators are rejected during RADIUS authentication.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] authentication-scheme authen1
[HUAWEI-aaa-authen-authen1] authentication-mode radius local
[HUAWEI-aaa-authen-authen1] radius-reject local
```

13.2.27 radius-server (aaa domain view)

Function

The **radius-server** command applies a RADIUS server template to a domain.

The **undo radius-server** command unbinds an RADIUS server template from a domain.

By default, the RADIUS server template **default** is bound to a configured domain and the domain **default**, and no RADIUS server template is bound to the domain **default_admin**.

Format

radius-server *template-name*

undo radius-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform RADIUS authentication and accounting for users in a domain, apply a RADIUS server template to the domain. A RADIUS server template takes effect only after the RADIUS server template is applied to a domain.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Example

Apply the RADIUS server template **template1** to the domain **radius1**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
```

```
[HUAWEI-radius-template1] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain radius1
[HUAWEI-aaa-domain-radius1] radius-server template1
```

13.2.28 radius-server accounting

Function

The **radius-server accounting** command configures the RADIUS accounting server.

The **undo radius-server accounting** command deletes the configuration.

By default, no RADIUS accounting server is configured.

Format

radius-server accounting *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server accounting *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server accounting *domain-name port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

undo radius-server accounting [*ipv4-address* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

undo radius-server accounting [*ipv6-address* [*port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight**]]]

undo radius-server accounting [*domain-name* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS accounting server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
domain-name	Specifies the domain name of a RADIUS accounting server.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain spaces. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
port	Specifies the port number of a RADIUS accounting server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS accounting server is bound to.	The value must be an existing VPN instance name.
source loopback *interface-number*	Specifies the number of a loopback interface.	The loopback interface must exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS accounting server. If this parameter is specified, ensure that the value of this parameter is the same as the client's IPv4 address specified on the RADIUS accounting server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.

Parameter	Description	Value
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS accounting server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS accounting server. This address cannot be a virtual IPv6 address of a VRRP6 group.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source vlanif *interface-number*	Specifies the IP address of a VLANIF interface as the source IP address. *interface-number* specifies the number of a VLANIF interface.	The VLANIF interface must exist.
weight *weight-value*	Specifies the weight of a RADIUS accounting server. When multiple servers are available, the device uses the server with the highest weight to perform accounting. If the servers have the same weights, the device uses the server configured first to perform accounting. If this parameter is not specified, the default weight of an accounting server is 80.	The value is an integer that ranges from 0 to 100. The default value is 80.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform accounting for users, configure a RADIUS accounting server. The device communicates with a RADIUS accounting server to obtain accounting information, and performs accounting for users based on the accounting information. The device sends accounting packets to the RADIUS accounting server only after the IP address and port number of the RADIUS accounting server are specified in the RADIUS server template.

Precautions

- The IP address of the primary accounting server must be different from the IP address of the secondary accounting server; otherwise, the configuration fails.
- When the **radius-server algorithm master-backup** command has been executed to set the algorithm for selecting RADIUS servers to primary/secondary and both the primary and secondary accounting servers have been configured, the device sends accounting request packets to the secondary accounting server when the following two conditions are met:
  a. The primary server does not send any accounting response packet.
  b. The maximum number of times that the device retransmits authentication and accounting packets is reached.
- For the RADIUS server in Down status, if configuration parameters except **weight** of the RADIUS server are modified, the server status will change from Down to Up.
- The modification of the weight parameter takes effect only for the users who go online after the modification. The users who go online before the modification still send authentication and accounting packets to the selected RADIUS server.
- If the source IP address configured using this command does not exist locally, this IP address does not take effect.

  NOTE

  This restriction applies only to the following models:

  S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S
- When configuring the IP address of a RADIUS accounting server, you can configure both an IPv4 and an IPv6 address but do not configure both a domain name and IP address.
- Only IPv4 addresses can be resolved for domain names.

Example

Configure the primary RADIUS accounting server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server accounting 10.163.155.12 1813
```

Configure the secondary RADIUS accounting server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server accounting 10.163.155.15 1813 weight 50
```

Configure the domain name of a RADIUS accounting server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server accounting www.example.com 1813
```

13.2.29 radius-server accounting-stop-packet resend

Function

The **radius-server accounting-stop-packet resend** command enables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted each time.

The **undo radius-server accounting-stop-packet resend** command disables retransmission of accounting-stop packets.

By default, retransmission of accounting-stop packets is enabled, and the retransmission times is 3.

NOTE

The default settings are recommended. If accounting-stop packets need to be retransmitted many times, the RADIUS authentication performance of the switch will be affected and even cause a failure to send accounting-stop packets.

Format

radius-server accounting-stop-packet resend [*resend-times*]

undo radius-server accounting-stop-packet resend

Parameters

Parameter	Description	Value
resend-times	Specifies the number of accounting-stop packets that can be retransmitted each time.	The value is an integer that ranges from 0 to 300.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

When accounting-stop packets cannot be sent to the RADIUS server that is unreachable, you can run the **radius-server accounting-stop-packet resend** command to save the accounting-stop packets in the buffer and send them at the preset intervals until the number of allowed retransmission times is reached or the packets are sent successfully.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted each time to 50.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server accounting-stop-packet resend 50
```

13.2.30 radius-server algorithm

Function

The **radius-server algorithm** command configures the algorithm for selecting RADIUS servers.

The **undo radius-server algorithm** command restores the default algorithm for selecting RADIUS servers.

By default, the algorithm for selecting RADIUS servers is the single user-based primary/secondary algorithm.

Format

radius-server algorithm { **loading-share** | **master-backup** } [**based-user**]

undo radius-server algorithm

Parameters

Parameter	Description	Value
loading-share	Sets the algorithm for selecting RADIUS servers to load balancing.	-
master-backup	Sets the algorithm for selecting RADIUS servers to primary/secondary.	-

Parameter	Description	Value
based-user	Sets the algorithm for selecting RADIUS servers to the single user-based algorithm. If this parameter is not specified, the algorithm for selecting RADIUS servers is the packet-based algorithm.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When two or more than two RADIUS servers are available, you can use the **radius-server algorithm** command to set the algorithm for selecting RADIUS servers.

- When **master-backup** is specified, the weight is used to determine the primary and secondary RADIUS authentication or accounting servers. The server with a larger weight value is the primary server. If devices have the same weight, the server that was first configured is the primary server.
- When **loading-share** is specified, the device sends a packet to a server according to the weights configured on servers. For example, if the weights of RADIUS server A, RADIUS server B, and RADIUS server C are 80, 80, and 40 respectively, the probabilities of sending packets to RADIUS server A, RADIUS server B, and RADIUS server C are as follows:
  - RADIUS server A: 80/(80 + 80 + 40) = 40%
  - RADIUS server B: 80/(80 + 80 + 40) = 40%
  - RADIUS server C: 40/(80 + 80 + 40) = 20%

Authentication server information is saved in the authentication phase. If the authentication server is also the accounting server, accounting requests are first sent to this server in the accounting phase. If the accounting packets of the authentication server are unreachable, the accounting server is reselected in the accounting phase. In this case, authentication and accounting of the same user may be performed on different servers.

Precautions

If you run the **radius-server algorithm** command multiple times in the same RADIUS server template view, only the latest configuration takes effect.

Example

Set the algorithm for selecting RADIUS servers to load balancing.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server algorithm loading-share
```

13.2.31 radius-server attribute message-authenticator access-request

Function

The **radius-server attribute message-authenticator access-request** command carries the Message-Authenticator attribute in RADIUS authentication packets sent by the device.

The **undo radius-server attribute message-authenticator access-request** command cancels the Message-Authenticator attribute from RADIUS authentication packets sent by the device.

By default, RADIUS authentication packets do not carry the Message-Authenticator attribute.

Format

radius-server attribute message-authenticator access-request

undo radius-server attribute message-authenticator access-request

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Message-Authenticator attribute is used to identify and verify authentication packets to prevent invalid packets.

NOTE

- This command is used when the PAP or CHAP authentication is enabled.
- When EAP authentication is enabled, RADIUS packets contain the Message-Authenticator attribute by default. You do not need to run this command.

Example

Configure the Message-Authenticator attribute to RADIUS authentication packets.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server attribute message-authenticator access-request
```

13.2.32 radius-server attribute translate

Function

The **radius-server attribute translate** command enables RADIUS attribute translation.

The **undo radius-server attribute translate** command disables RADIUS attribute translation.

By default, RADIUS attribute translation is disabled.

Format

radius-server attribute translate

undo radius-server attribute translate

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Currently, RADIUS servers of different vendors may support different RADIUS attributes and have vendor-specific RADIUS attributes. To communicate with different RADIUS servers, the device provides the RADIUS attribute translation function. After RADIUS attribute translation is enabled, the device can translate RADIUS attributes when sending or receiving packets.

Follow-up Procedure

After RADIUS attribute translation is enabled, perform either of the following operations to make the function to take effect:

- Run the **radius-attribute translate** command to specify the RADIUS attributes that you want to translate.

- Run the **radius-attribute disable** command to specify the RADIUS attributes that you do not want to translate.

Example

Enable RADIUS attribute translation.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server attribute translate
```

13.2.33 radius-server authentication

Function

The **radius-server authentication** command configures a RADIUS authentication server.

The **undo radius-server authentication** command deletes the configured RADIUS authentication server.

By default, no RADIUS authentication server is specified.

Format

radius-server authentication *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server authentication *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server authentication *domain-name port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

undo radius-server authentication [*ipv4-address* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

undo radius-server authentication [*ipv6-address* [*port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight**]]]

undo radius-server authentication [*domain-name* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
domain-name	Specifies the domain name of a RADIUS authentication server.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain spaces. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
port	Specifies the port number of a RADIUS authentication server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authentication server is bound to.	The value must be an existing VPN instance name.
source loopback *interface-number*	Specifies the IP address of the loopback interface taken as the source IP address. *interface-number* specifies the number of a loopback interface.	The loopback interface must already exist.

Parameter	Description	Value
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is specified, ensure that the value of this parameter is the same as the client's IPv4 address specified on the RADIUS authentication server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. This address cannot be a virtual IPv6 address of a VRRP6 group.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source vlanif *interface-number*	Specifies the IP address of a VLANIF interface as the source IP address. *interface-number* specifies the number of a VLANIF interface.	The VLANIF interface must exist.

Parameter	Description	Value
weight *weight-value*	Specifies the weight of a RADIUS authentication server. When multiple servers are available, the device uses the server with the highest weight to perform authentication. If the servers have the same weights, the device uses the server configured first to perform authentication.	The value is an integer that ranges from 0 to 100. The default value is 80.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template. The device uses the RADIUS protocol to communicate with a RADIUS authentication server to obtain authentication information, and authenticates users based on the authentication information. The device sends authentication packets to the RADIUS authentication server only after the IP address and port number of the RADIUS authentication server are specified in the RADIUS server template.

When the **radius-server algorithm master-backup** command has been executed to set the algorithm for selecting RADIUS servers to primary/secondary and both the primary and secondary authentication servers have been configured, the device sends authentication request packets to the secondary authentication server when the following two conditions are met:

1. The primary authentication server does not send any authentication response packet.
2. The maximum number of times that the device retransmits authentication request packets is reached.

When the 802.1X authentication mode is set to EAP, the device and RADIUS authentication servers exchange packets multiple times. During the first exchange process, the device sends a request packet to the primary RADIUS authentication server. If the device resends the request packet for the maximum number of times but does not receive a response packet from the primary RADIUS authentication server, the device sends a request packet to the secondary RADIUS authentication server. If the secondary RADIUS authentication server sends a response packet to the device, the device will directly send request packets to the secondary RADIUS authentication server in the following exchange processes. In this way, the device does not need to send a request packet to the primary RADIUS authentication server first in the following exchange processes, shortening the authentication time and preventing the user authentication connection from being disconnected because the client does not receive a response packet for a long time.

Precautions

- For the RADIUS server in Down status, if configuration parameters except **weight** of the RADIUS server are modified, the server status will change from Down to Up.
- If an interface connecting the device to a server has multiple IP addresses configured and can communicate with the server only through some of these IP addresses, one IP address among these reachable IP addresses needs to be specified as the source IP address based on the routing table to ensure that the device can communicate with the server.
- The modification of the weight parameter takes effect only for the users who go online after the modification. The users who go online before the modification still send authentication and accounting packets to the selected RADIUS server.
- You are advised to configure different RADIUS servers for the source VLANIF interface, source IP address, and source loopback interface and bind the servers to the same RADIUS template. Otherwise, the device creates multiple RADIUS servers even if the source and destination IP addresses of RADIUS request packets sent by different RADIUS templates are the same. As a result, only the first created RADIUS server receives RADIUS response packets, while other RADIUS servers cannot. To check the RADIUS server configuration, run the **display radius-server item ip-address** { *ipv4-address* | *ipv6-address* } **authentication** command.
- The management interface MEth0/0/1 cannot be used as the source interface for RADIUS authentication.
- If the source IP address configured using this command does not exist locally, this IP address does not take effect.

  NOTE

  This restriction applies only to the following models:

  S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S
- When configuring the IP address of a RADIUS authentication server, you can configure both an IPv4 and an IPv6 address but do not configure both a domain name and IP address.
- Only IPv4 addresses can be resolved for domain names.

Example

Configure the IP address of the primary RADIUS authentication server to 10.163.155.13 and the port number to 1812.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server authentication 10.163.155.13 1812
```

Configure the IP address of the secondary RADIUS authentication server to 10.163.155.15, the port number to 1812 and the weigh to 50.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server authentication 10.163.155.15 1812 weight 50
```

Set the domain name and port number of a RADIUS authentication server to **www.example.com** and 1812.

```
<HUAWEI> system-view
[HUAWEI] radius-server template group1
[HUAWEI-radius-group1] radius-server authentication www.example.com 1812
```

13.2.34 radius-server authorization

Function

The **radius-server authorization** command configures the RADIUS authorization server.

The **undo radius-server authorization** command deletes the configured RADIUS authorization server.

By default, no RADIUS authorization server is configured.

Format

radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* **shared-key cipher** *key-string* | **shared-key cipher** *key-string* [**server-group** *group-name*] } [**protect enable**]

radius-server authorization *domain-name* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* **shared-key cipher** *key-string* | **shared-key cipher** *key-string* [**server-group** *group-name*] } [**protect enable**]

undo radius-server authorization { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] }

undo radius-server authorization { **all** | *domain-name* [**vpn-instance** *vpn-instance-name*] }

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a RADIUS authorization server.	The value is a unicast address in dotted decimal notation.

Parameter	Description	Value
domain-name	Specifies the domain name of a RADIUS authorization server.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain spaces. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authorization server is bound to.	The value must be an existing VPN instance name.
server-group *group-name*	Specifies the name of a RADIUS group corresponding to a RADIUS server template.	The value is a string of 1 to 32 characters, including letters (case-sensitive), numerals (0 to 9), periods (.), hyphens (-), and underscores (_). The value cannot be - or --.
shared-key cipher *key-string*	Specifies the shared key of a RADIUS server.	The value is a case-sensitive character string without spaces or question marks (?). *key-string* can be a string of 1 to 128 characters in plaintext or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in ciphertext.
protect enable	Enables the security hardening function.	-
all	Deletes all RADIUS authorization servers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An independent RADIUS authorization server can be used to authorize online users. RADIUS provides two authorization methods: Change of Authorization (CoA) and Disconnect Message (DM).

- CoA: After a user is successfully authenticated, you can modify the rights of the online user through the RADIUS authorization server. For example, a VLAN ID can be delivered to access users of a certain department through CoA packets, so that they belong to the same VLAN no matter which interfaces they connect to.
- DM: The administrator can forcibly disconnect a user through the RADIUS authorization server.

After the parameters such as IP address and shared key are configured for the RADIUS authorization server, the device can receive authorization requests from the server and grant rights to users according to the authorization information. After authorization is complete, the device returns authorization response packets carrying the results to the server.

After the security hardening function is enabled by specifying the **protect enable** parameter, the following occurs:

- When a CoA or DM request packet carries the Message-Authenticator attribute, the device checks the Message-Authenticator attribute. If the check fails, the device discards the request packet and does not respond the packet. If the check succeeds, the device sends a CoA or DM response packet (ACK or NAK) that carries the Message-Authenticator attribute.
- When a CoA or DM request packet does not carry the Message-Authenticator attribute, the device does not check the attribute and sends a CoA or DM response packet (ACK or NAK) that does not carry the Message-Authenticator attribute.

NOTE

When a CoA or DM request packet carries the Message-Authenticator attribute, if the **radius-attribute disable message-authenticator receive** command is configured, the device does not check the attribute and sends a response packet that does not carry the Message-Authenticator attribute; if the **radius-attribute disable message-authenticator send** command is configured, the device sends a response packet that does not carry the Message-Authenticator attribute even if the attribute check succeeds.

Precautions

To improve security, it is recommended that the password contains at least three types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

You also need to run the **radius-server authorization server-source** command in V200R020C10SPC100 and later versions to configure an IPv4 address for receiving and responding to request packets of a RADIUS authorization server so that the function of the RADIUS authorization server can take effect.

During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

When configuring the IP address of a RADIUS authorization server, do not configure both a domain name and IP address. Otherwise, the system prompts that the configuration fails.

Example

Specify a RADIUS authorization server.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization 10.1.1.116 shared-key cipher YsHsjx_202206
```

Configure the domain name of a RADIUS authorization server.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization www.example.com shared-key cipher YsHsjx_202206
```

13.2.35 radius-server authorization attribute-decode-sameastemplate

Function

The **radius-server authorization attribute-decode-sameastemplate** command configures the device to parse RADIUS dynamic authorization packet attributes based on the configuration in RADIUS server template.

The **undo radius-server authorization attribute-decode-sameastemplate** command restores the default method of parsing RADIUS authorization packet attributes.

By default, the device parses the MAC address in the calling-station-id attribute carried in RADIUS dynamic authorization packets based on the MAC address length, without considering the MAC address format and delimiter.

Format

radius-server authorization attribute-decode-sameastemplate

undo radius-server authorization attribute-decode-sameastemplate

Parameters

None.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device parses the MAC address in the Calling-Station-Id attribute in RADIUS dynamic authorization packets. By default, the MAC address format that can be parsed is configured using the **radius-server authorization calling-station-id decode-mac-format** command in the system view. When the device is connected to multiple RADIUS servers, the MAC address formats are different in the Calling-Station-Id attribute in dynamic authorization packets sent by different RADIUS servers. In this case, the MAC address may fail to be parsed if the same parse mode is used, resulting in that the device fails to be connected to some RADIUS servers. You can run the **radius-server authorization attribute-decode-sameastemplate** command to configure the device to parse RADIUS dynamic authorization packet attributes based on the Calling-Station-Id attribute encapsulation mode configured in each RADIUS server template, making the device be successfully connected to multiple RADIUS servers.

Prerequisites

This function is used to make the Calling-Station-Id attribute parse mode the same as the Calling-Station-Id attribute encapsulation mode configured in RADIUS server template. Therefore, make sure that the following steps have been performed before using this function.

1. The **calling-station-id mac-format** command has been run in the RADIUS server template view to configure the encapsulation mode of the MAC address in the Calling-Station-Id attribute.
2. The **radius-server authorization** command has been run in the system view to configure the authorization server to use the RADIUS server template **server-group**.

NOTE

If the RADIUS server template used by the authorization server is not specified, this function cannot be implemented on a device. You can run the **radius-server authorization calling-station-id decode-mac-format** command in the system view to configure the Calling-Station-Id attribute parse mode.

Precautions

The configuration in a RADIUS server template has a higher priority than the global configuration.

Example

Configure the RADIUS authorization server to parse attributes depending on the configuration in a RADIUS template.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization attribute-decode-sameastemplate
```

13.2.36 radius-server authorization attribute-encode-sameastemplate

Function

The **radius-server authorization attribute-encode-sameastemplate** command configures a device to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template.

The **undo radius-server authorization attribute-encode-sameastemplate** command restores the default setting.

By default, a device is not configured to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template.

Format

radius-server authorization attribute-encode-sameastemplate

undo radius-server authorization attribute-encode-sameastemplate

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The attribute match check function is configured on the RADIUS servers of some vendors. The attribute match check succeeds and the RADIUS server successfully interconnects with a device to implement dynamic authorization or offline operations only when the attribute encapsulation formats in the COA or DM Response packet received by the RADIUS server are the same as those parsed from the RADIUS authentication Response packets. The RADIUS server encapsulates the attributes parsed from the RADIUS Response packet based on the configurations in the RADIUS server template. To ensure that the attribute formats in the COA or DM Response packet are the same as those parsed by the RADIUS server from the RADIUS packet, you can run the **radius-server authorization attribute-encode-sameastemplate** command to configure the device to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template, so that the device is successfully interconnected with the RADIUS server.

Attributes whose encapsulation formats need to be configured in the COA or DM Response packet include Calling-Station-Id (31), NAS-IP-Address (4), and User-Name (1).

Precautions

- This function is used to configure the encapsulation modes of the Calling-Station-Id (31), NAS-IP-Address (4), and User-Name (1) attributes in the COA or DM Response packet to be the same as those configured in the RADIUS server template. Therefore, perform the following steps before using this function.
  a. Configure the encapsulation modes of attributes in the RADIUS server template view.

        - Run the **calling-station-id mac-format** command to configure the encapsulation mode of the MAC address in the Calling-Station-Id attribute.
        - Run the **radius-attribute nas-ip** command to configure the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.
        - Run the **radius-server user-name domain-included** command to configure whether the user name carried in the RADIUS packet contains a domain name.
    b. Run the **radius-server authorization** command in the system view to configure the authorization server to use the RADIUS server template **server-group**.
- After this function is configured, the priority of the NAS IP address in the NAS-IP-Address (4) attribute is as follows: NAS IP address configured in the RADIUS server template>source IP address configured on the accounting server>source IP address configured on the authentication server>destination IP address of the Request packet
- If the **radius-server authorization attribute-encode-sameastemplate** command is not configured, no RADIUS server template is bound to the authorization server, or no attribute format configuration exists in the RADIUS server template, the formats of COA or DM response packets are as follows:
    - MAC address in the Calling-Station-Id (31) attribute: The MAC address is encapsulated in the default format XXXXXXXXXXXX.
    - NAS IP address in the NAS-IP-Address (4) attribute: destination IP address in the Request packet
    - User name in the User-Name (1) attribute: The user name in the Request packet is used.

Example

Configure the RADIUS authorization server to parse attributes based on the configurations in the RADIUS server template.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization attribute-encode-sameastemplate
```

13.2.37 radius-server authorization calling-station-id decode-mac-format

Function

The **radius-server authorization calling-station-id decode-mac-format** command sets the format of MAC address that can be parsed by a device in the calling-station-id (Type 31) attribute carried in RADIUS authorization packets.

The **undo radius-server authorization calling-station-id decode-mac-format** command restores the default format of the MAC address in the calling-station-id (Type 31) attribute.

By default, the device parses the MAC address in the calling-station-id attribute carried in RADIUS dynamic authorization packets into ASCII format, and the MAC address does not contain separators. In addition, the device parses the MAC address in the calling-station-id attribute carried in RADIUS dynamic authorization packets based on the MAC address length, without considering the MAC address format and delimiter.

Format

radius-server authorization calling-station-id decode-mac-format { **bin** | **ascii** { **unformatted** | { **dot-split** | **hyphen-split** } [**common** | **compress**] } }

undo radius-server authorization calling-station-id decode-mac-format

Parameters

Parameter	Description	Value
bin	Indicates that the MAC address in the calling-station-id attribute uses the binary format.	-
ascii	Indicates that the MAC address in the calling-station-id attribute uses the ASCII format.	-
unformatted	Indicates that no separator is used in the MAC address in the calling-station-id field.	-
dot-split	Indicates that dots are used as the separators in MAC address.	-
hyphen-split	Indicates that the hyphens are used as the separators in MAC address.	-
common	Indicates that the MAC address in the calling-station-id attribute uses the xx-xx-xx-xx-xx-xx or xx.xx.xx.xx.xx.xx format.	-
compress	Indicates that the MAC address in the calling-station-id attribute uses the xxxx-xxxx-xxxx or xxxx.xxxx.xxxx format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the MAC address format in the calling-station-id attribute carried in RADIUS dynamic authorization packets is xxxxxxxxxxxx. If the MAC address format in the calling-station-id attribute sent by the RADIUS server is not the default format used on the device, run the **radius-server authorization calling-station-id decode-mac-format** command to change the MAC address format on the device.

When a device connects to multiple RADIUS servers, the RADIUS servers may send MAC addresses in different formats in the calling-station-id attribute to the device. You need to run the **radius-server authorization attribute-decode-sameastemplate** command to configure the device to parse the RADIUS authorization packet attributes based on the configuration in RADIUS server template, so that the device can work with these RADIUS servers.

Precautions

The configuration in a RADIUS server template has a higher priority than the global configuration.

Example

Set the format of MAC address that can be parsed by the device in the calling-station-id attribute to binary.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization calling-station-id decode-mac-format bin
```

13.2.38 radius-server authorization hw-ext-specific command bounce-port disable

Function

The **radius-server authorization hw-ext-specific command bounce-port disable** command configures the function of ignoring the authorization attribute indicating that the port goes Down intermittently in a CoA packet.

The **undo radius-server authorization hw-ext-specific command bounce-port disable** command restores the default setting.

By default, the device supports the authorization attribute indicating that the port goes Down intermittently in a CoA packet.

Format

radius-server authorization hw-ext-specific command bounce-port disable

undo radius-server authorization hw-ext-specific command bounce-port disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet can be:

- 1: Indicates that user reauthentication will be performed.
- 2: Indicates that the port where the authorized user resides goes Down intermittently.
- 3: Indicates that the port where the authorized user resides is disabled.

After the server authorizes a VLAN, the VLAN to which the terminal belongs will be changed. However, the terminal does not proactively trigger an IP address reapplication event using DHCP and you must manually trigger such an event on the terminal. Such operations cannot be directly performed on dumb terminals such as printers. You can disconnect the authentication port intermittently to trigger terminals connected to the authentication port to re-apply for an IP address. To configure the function of intermittently disconnecting the authentication port, you need to run the **undo radius-server authorization hw-ext-specific command bounce-port disable** command on the device, and set the value of the RADIUS attribute HW-Ext-Specific (26-238) on the server to user-command=2.

Precautions

Pay attention to the following points if the value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet sent by the RADIUS server is 2 or 3:

- Ensure that only one user resides on the authentication port or the user to be authenticated is directly connected to the authentication port; otherwise, other users on the authentication port will be affected if the port goes Down intermittently or disabled.
- Only a physical port can function as the authentication port, while an Eth-Trunk interface cannot.
- When the value is 2, SVF and policy association are both supported. When the value is 3, SVF and policy association are not supported.

Example

Configure the function of ignoring the authorization attribute indicating that the port goes Down intermittently in a CoA packet.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization hw-ext-specific command bounce-port disable
```

13.2.39 radius-server authorization hw-ext-specific command down-port disable

Function

The **radius-server authorization hw-ext-specific command down-port disable** command configures the function of ignoring the authorization attribute indicating that the port is disabled in a CoA packet.

The **undo radius-server authorization hw-ext-specific command down-port disable** command restores the default setting.

By default, the device supports the authorization attribute indicating that the port is disabled in a CoA packet.

Format

radius-server authorization hw-ext-specific command down-port disable

undo radius-server authorization hw-ext-specific command down-port disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet can be:

- 1: Indicates that user reauthentication will be performed.
- 2: Indicates that the port where the authorized user resides goes Down intermittently.
- 3: Indicates that the port where the authorized user resides is disabled.

When the value of the user-command field in a CoA packet sent by the RADIUS server is 3, users go offline and their network access rights are blocked. The most obvious impact of this is that the port where the authorized user resides is disabled. If you want to enable this port, you have to log in to the device to manually enable it. To avoid unintentionally making users go offline, you can disable the authorization attribute in a CoA packet indicating that the port is disabled by running the **radius-server authorization hw-ext-specific command down-port disable** command.

Precautions

Pay attention to the following points if the value of the user-command field in the RADIUS attribute **HW-Ext-Specific(26-238)** carried in a CoA packet sent by the RADIUS server is 2 or 3:

- Ensure that only one user resides on the authentication port or the user to be authenticated is directly connected to the authentication port; otherwise, other users on the authentication port will be affected if the port goes Down intermittently or disabled.
- Only a physical port can function as the authentication port, while an Eth-Trunk interface cannot.
- When the value is 2, SVF and policy association are both supported. When the value is 3, SVF and policy association are not supported.

Example

Configure the function of ignoring the authorization attribute indicating that the port is disabled in a CoA packet.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization hw-ext-specific command down-port disable
```

13.2.40 radius-server authorization match-type

Function

The **radius-server authorization match-type** command configures the method in which the device checks whether the RADIUS attributes in the received CoA or DM Request packet match user information on the device.

The **undo radius-server authorization match-type** command restores the default setting.

By default, a device checks whether the RADIUS attributes in the received CoA or DM Request packet match user information on the device using the **any** method, namely, the device checks whether a specific RADIUS attribute in the received CoA or DM Request packet matches user information on the device.

Format

radius-server authorization match-type { **any** | **all** }

undo radius-server authorization match-type

Parameters

Parameter	Description	Value
any	Indicates that the device checks whether a specified attribute matches user information on the device.	-

Parameter	Description	Value
all	Indicates that the device checks whether all attributes match user information on the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A device checks whether the RADIUS attributes in the CoA or DM Request packet match user information on the device to identify users in the following two methods:

- **any** method: The device checks whether an attribute matches user information on the device. The priority of identifying the RADIUS attributes used by the users is as follows: Acct-Session-ID (44) > Calling-Station-Id (31) > Framed-IP-Address (8). The device searches for the attributes in the Request packet based on the priority, and matches the first found attribute against user information on the device. If the attribute is successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.
- **all** method: The device checks whether all attributes match user information on the device. It identifies the following RADIUS attributes used by users in the listed order: Acct-Session-ID (44), Calling-Station-Id (31), Framed-IP-Address (8), and User-Name (1). The device matches one or more of the preceding attributes in the Request packet against user information on the device. If all the attributes are successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.

Precautions

When the RADIUS attribute translation function is configured in the RADIUS template using the **radius-attribute translate** command, the match will fail.

Currently, the **any** method supports only the Acct-Session-ID (44), Calling-Station-Id (31), and Framed-IP-Address (8) attributes. The device does not match other attributes against user information on the device.

Example

Configure the device to check whether all RADIUS attributes in the received CoA or DM Request packet match user information on the device.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization match-type all
```

13.2.41 radius-server authorization port

Function

The **radius-server authorization port** command configures the port ID of the RADIUS authorization server.

The **undo radius-server authorization Port** command restores the default setting.

By default, the port ID of the RADIUS authorization server is 3799.

Format

radius-server authorization port *port-id*

undo radius-server authorization port

Parameters

Parameter	Description	Value
port-id	Specifies the port ID of the RADIUS authorization server.	The value is an integer that ranges from 1024 to 55535, and the default value is 3799.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **radius-server authorization port** *port-id* command to configure the port ID that a device uses when sending packets to the RADIUS authorization server. The device then uses the configured port ID as the destination port ID to send Response packets to the RADIUS authorization server after receiving COA or DM Request packets from the RADIUS authorization server.

Example

Set the port ID of the RADIUS authorization server to 3700.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization port 3700
```

13.2.42 radius-server authorization server-source

Function

The **radius-server authorization server-source** command configures an IPv4 address for receiving and responding to request packets of a RADIUS authorization server.

The **undo radius-server authorization server-source** command restores the default setting.

By default, the device does not receive or respond to any request packet of a RADIUS authorization server.

Format

radius-server authorization server-source { **ip-address** *ip-address* | **all-interface** }

undo radius-server authorization server-source { **ip-address** *ip-address* | **all-interface** | **all** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.
all-interface	Specifies the IPv4 address as 0.0.0.0. That is, the device receives and responds to request packets of a RADIUS authorization server through any IPv4 address.	-
all	Indicates all IPv4 addresses specified by **ip-address** *ip-address*.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no IPv4 address can be used to receive or respond to request packets of the RADIUS authorization server. When the device needs to establish a connection with a RADIUS authorization server, you can run the **radius-server authorization server-source** command to specify an IPv4 address for the device to receive and respond to request packets of the RADIUS authorization server.

Precautions

- After you run this command to configure an IPv4 address for the device to receive and respond to request packets of a RADIUS authorization server, the RADIUS authorization server can communicate with the device only through this IPv4 address. Ensure that the RADIUS authorization server can communicate with the device through this IPv4 address at Layer 3.
- After the **radius-server authorization server-source all-interface** command is run, the device receives and responds to request packets of a RADIUS authorization through any IPv4 address, which increases system security risks. Therefore, you are advised not to run this command.
- After the **radius-server authorization server-source all-interface** command is run, all the configurations of the **radius-server authorization server-source ip-address** *ip-address* command are cleared.
- If the **radius-server authorization server-source all-interface** command has been configured on the device, the **radius-server authorization server-source ip-address** *ip-address* command configured later does not take effect.

Example

Specify 10.1.1.1 as the IPv4 address used to receive and respond to request packets of a RADIUS authorization server.

```
<HUAWEI> system-view
[HUAWEI] radius-server authorization server-source ip-address 10.1.1.1
```

13.2.43 radius-server dead-detect-condition by-server-ip

Function

The **radius-server dead-detect-condition by-server-ip** command configures the device to perform keepalive detection on the RADIUS authentication and accounting servers with the same IP address.

The **undo radius-server dead-detect-condition by-server-ip** command configures the device to perform keepalive detection on only the RADIUS authentication server.

By default, keepalive detection is performed on the RADIUS authentication and accounting servers with the same IP address.

Format

radius-server dead-detect-condition by-server-ip

undo radius-server dead-detect-condition by-server-ip

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device periodically sends authentication request packets to the RADIUS server in Down state. If the RADIUS server responds, the device sets the RADIUS authentication server status to Up. The device does not perform keepalive detection for RADIUS accounting servers in Down state. Instead, the device sets the RADIUS accounting server status to Up only when the server recovery time expires.

To allow the device to promptly detect the status of RADIUS accounting servers that are in Down state, run the **radius-server dead-detect-condition by-server-ip** command. After the command is executed, the device performs keepalive detection on RADIUS servers based on the RADIUS server IP address, so that the status of RADIUS accounting server is associated with the status of authentication server.

Precautions

After the **radius-server dead-detect-condition by-server-ip** command is executed, run the **radius-server testuser** command to configure automatic user detection.

After the **radius-server dead-detect-condition by-server-ip** command is executed, if the authentication and accounting servers sharing the same IP address are in the same VPN instance, the device accumulates the number of authentication and accounting packets sent by the servers. In addition, the status of RADIUS authentication server with the same IP address in the same VPN instance is updated.

Example

Configure the device to perform keepalive detection on the RADIUS authentication and accounting servers with the same IP address.

```
<HUAWEI> system-view
[HUAWEI] radius-server dead-detect-condition by-server-ip
```

13.2.44 radius-server dead-interval dead-count detect-cycle

Function

The **radius-server dead-interval dead-count detect-cycle** command configures the RADIUS server detection interval, number of times the detection interval cycles, and maximum number of consecutive unacknowledged packets in each detection interval.

The **undo radius-server dead-interval dead-count detect-cycle** command restores the default settings.

By default, the RADIUS server detection interval is 5 seconds, the number of times the detection interval cycles is 2, and the maximum number of consecutive unacknowledged packets in each detection interval is 2.

Format

radius-server { **dead-interval** *dead-interval* | **dead-count** *dead-count* | **detect-cycle** *detect-cycle* }

undo radius-server { **dead-interval** | **dead-count** | **detect-cycle** }

Parameters

Parameter	Description	Value
dead-interval	Specifies the RADIUS server detection interval.	The value is an integer that ranges from 1 to 300, in seconds.
dead-count	Specifies the maximum number of consecutive unacknowledged packets in each detection interval.	The value is an integer that ranges from 1 to 65535.
detect-cycle	Specifies the number of times the detection interval cycles.	The value is an integer that ranges from 1 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the system starts, the RADIUS server status detection timer runs. The device sets the RADIUS server status to Up. When the device sends a RADIUS request packet to the RADIUS server, if the conditions for setting the RADIUS server status to Down are met, the device sets the RADIUS server status to Down; if the conditions are not met, the RADIUS server status remains to be Up.

If the device does not receive any response packet from the RADIUS server after sending the first RADIUS Access-Request packet to the server and the condition that the number of times the device does not receive any response packet from the server (n) is greater than or equal to the maximum number of consecutive unacknowledged packets (*dead-count*) is met in a detection interval, a communication interruption is recorded. If the device still does not receive any response packet from the RADIUS server, the device sets the RADIUS server status to Down when recording the communication interruption for the same times as the detection interval cycles.

Precautions

- If the device has reported a RADIUS server Up alarm and needs to report a RADIUS server Down alarm, the device will send the Down alarm 10 seconds after the Up alarm is sent, even if the RADIUS server Down detection interval is shorter than 10 seconds (for example, the value of *dead-interval* is set to 4 seconds, and the RADIUS server Down detection interval is 8 seconds). This function prevents frequent alarm sending.
- You are advised to set the RADIUS server detection interval, maximum number of consecutive unacknowledged packets in each detection interval, and number of times the detection interval cycles to be greater than the default values on the device to prevent the RADIUS server status from being set to Down.
- To check the RADIUS server status, run the **display radius-server configuration** command. If the RADIUS server status is Down, the device records logs and alarms. For details about logs, see **RDS/4/RDAUTHDOWN**. For details about alarms, see **RDS_1.3.6.1.4.1.2011.5.25.40.15.2.2.1.2 hwRadiusAuthServerDown**.

Example

Set the RADIUS server detection interval to 10 seconds, number of times the detection interval cycles to 2, and maximum number of consecutive unacknowledged packets in each detection interval to 2.

```
<HUAWEI> system-view
[HUAWEI] radius-server dead-interval 10
[HUAWEI] radius-server dead-count 2 [HUAWEI] radius-server detect-cycle 2
```

13.2.45 radius-server detect-server interval

Function

The **radius-server detect-server interval** command configures an automatic detection interval for RADIUS servers in Down status.

The **undo radius-server detect-server interval** command restores the default settings.

The default automatic detection interval is 60 seconds.

Format

radius-server detect-server interval *interval*

undo radius-server detect-server interval

Parameters

Parameter	Description	Value
interval	Specifies the automatic detection interval for RADIUS servers in Down status.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After the automatic detection function is enabled using the **radius-server testuser** command, you can run the **radius-server detect-server interval** command to adjust the automatic detection interval for RADIUS servers in Down status.

Example

Set the automatic detection interval for RADIUS servers in Down status to 100 seconds in the RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server detect-server interval 100
```

13.2.46 radius-server detect-server timeout

Function

The **radius-server detect-server timeout** command configures the timeout period for RADIUS detection packets.

The **undo radius-server detect-server timeout** command restores the default settings.

By default, the timeout period for RADIUS detection packets is 3 seconds.

Format

radius-server detect-server timeout *timeout*

undo radius-server detect-server timeout

Parameters

Parameter	Description	Value
timeout	Specifies the timeout period for RADIUS detection packets.	The value is an integer that ranges from 1 to 10, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the automatic detection function is enabled using the **radius-server testuser** command and the device sends detection packets to the RADIUS server, the device determines whether to switch the RADIUS server status based on whether it receives response packets from the RADIUS server within the timeout period. The following table lists the switchover conditions.

After the automatic detection function is enabled, automatic detection is classified into the following conditions depending on differences of the RADIUS server status.

Server Status	Whether Automatic Detection Is Supported	Time When an Automatic Detection Packet Is Sent	Condition for Switching the Server Status
Down	Automatic detection is supported by default.	An automatic detection packet is sent after the automatic detection period expires.	If the device receives a response packet from the RADIUS server within the timeout period for detection packets, the device marks the RADIUS server status as Up; otherwise, the RADIUS server status remains Down.

Server Status	Whether Automatic Detection Is Supported	Time When an Automatic Detection Packet Is Sent	Condition for Switching the Server Status
Up	Automatic detection can be enabled using the **radius-server detect-server up-server interval** command.	An automatic detection packet is sent after the automatic detection period expires.	If the conditions for marking the RADIUS server status as Down are met, the device marks the RADIUS server status as Down; otherwise, the RADIUS server status remains Up.
Force-up	Automatic detection is supported by default.	An automatic detection packet is sent immediately.	If the device receives a packet from the RADIUS server within the timeout period, the device marks the RADIUS server status as Up; otherwise, the device marks the RADIUS server status as Down.

NOTE

On a large-scale network, you are advised not to enable automatic detection for RADIUS servers in Up state. This is because if automatic detection is enabled on multiple NAS devices, the RADIUS server periodically receives a large number of detection packets when processing RADIUS Access-Request packets source from users, which may deteriorate processing performance of the RADIUS server.

After the **radius-server testuser** command is configured, the dead-time timer configured using the **radius-server dead-time** command does not take effect.

Precautions

You can run the **radius-server detect-server timeout** command to adjust the timeout period for RADIUS detection packets based on the actual response rate of the RADIUS server. You are advised to set a timeout period for RADIUS detection packets smaller than the automatic detection interval to prevent the device from sending a detection packet again before completing processing the response packet from the RADIUS server. If the configured timeout period for RADIUS detection packets is longer than the automatic detection interval, the smaller value of the two is used as the timeout period.

- For the RADIUS server in Down state, the smaller one between the values configured using the **radius-server detect-server timeout** and **radius-server detect-server interval** commands is the timeout period for detection packets.
- For the RADIUS server in Up state, the smaller one between the values configured using the **radius-server detect-server timeout** and **radius-server detect-server up-server interval** command is the timeout period for detection packets.

Example

Set the timeout period for RADIUS detection packets to 5 seconds in the RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server detect-server timeout 5
```

13.2.47 radius-server detect-server up-server interval

Function

The **radius-server detect-server up-server interval** command enables automatic detection for RADIUS servers in Up status and configures the automatic detection interval.

The **undo radius-server detect-server up-server interval** command restores the default settings.

By default, a device does not automatically detect RADIUS servers in Up status.

Format

radius-server detect-server up-server interval *interval*

undo radius-server detect-server up-server interval

Parameters

Parameter	Description	Value
interval	Specifies the automatic detection interval for RADIUS servers in Up status.	The value is an integer that ranges from 0 or 2 to 3600, in seconds. The value 0 indicates that the device does not automatically detect RADIUS servers in Up status.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After automatic detection is enabled using the **radius-server testuser** command, the device automatically detects only RADIUS servers in Down status by default.

To make the device automatically detect RADIUS servers in Up status, run the **radius-server detect-server up-server interval** command to enable automatic detection for RADIUS servers in Up status and configure the automatic detection interval.

Precautions

On a large-scale network, you are advised not to enable automatic detection for RADIUS servers in Up state. This is because if automatic detection is enabled on multiple NAS devices, the RADIUS server periodically receives a large number of detection packets when processing RADIUS Access-Request packets source from users, which may deteriorate processing performance of the RADIUS server.

Example

Enable automatic detection for RADIUS servers in Up status and set the automatic detection interval to 100 seconds in the RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server detect-server up-server interval 100
```

13.2.48 radius-server dead-time

Function

The **radius-server retransmit timeout dead-time** command sets the number of times that RADIUS request packets are interval for the server to revert to the active status.

The **undo radius-server retransmit timeout dead-time** command restores the default interval for the server to revert to the active status.

By default, the interval for the server to revert to the active status is 5 minutes.

Format

radius-server dead-time *dead-time*

undo radius-server dead-time [*dead-time*]

Parameters

Parameter	Description	Value
dead-time	Specifies the interval for the server to revert to the active status.	The value is an integer that ranges from 1 to 65535, in minutes.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **radius-server dead-time** *dead-time* command to configure the duration for which the RADIUS server remains Down. After the device sets the RADIUS server status to Down and the interval specified by *dead-time* expires, the device resets the server status to Force-up. Servers in Force-up and Up states have the same priority and participate in RADIUS server selection based on the algorithm specified by **radius-server algorithm**. If a new user needs to be authenticated in RADIUS mode and no RADIUS server is available, the device attempts to re-establish a connection with a RADIUS server in Force-up status. The Force-up status is defined to prevent servers in Down status from remaining idle.

NOTE

After the **radius-server testuser** command is configured, the dead-time timer configured using the **radius-server dead-time** command does not take effect.

This command can improve the reliability of RADIUS authentication.

Example

Set the interval for the server to revert to the active status to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server dead-time 10
```

13.2.49 radius-server encapsulation ipv4 traffic-statistics enable

Function

The **radius-server encapsulation ipv4 traffic-statistics enable** command enables a device to encapsulate the standard RADIUS attributes 42, 43, 47, 48, 52, and 53 only into IPv4 traffic.

The **undo radius-server encapsulation ipv4 traffic-statistics enable** command restores the default configuration.

By default, a device encapsulates both IPv4 and IPv6 traffic with the standard RADIUS attributes 42, 43, 47, 48, 52, and 53.

Format

radius-server encapsulation ipv4 traffic-statistics enable

undo radius-server encapsulation ipv4 traffic-statistics enable

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After this command is run, the device encapsulates the standard RADIUS attributes 42, 43, 47, 48, 52, and 53 only into IPv4 traffic. If the **accounting dual-stack separate** command is run to enable separate traffic statistics collection or rate limiting for IPv4 and IPv6 users, the device encapsulates IPv6 traffic with the Huawei proprietary attributes 26-166, 26-167, 26-168, 26-169, 26-170, and 26-171.

Example

In the RADIUS server template **acs**, enable the function of encapsulating the standard RADIUS attributes 42, 43, 47, 48, 52, and 53 only into IPv4 traffic.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server encapsulation ipv4 traffic-statistics enable
Warning: This operation may cause online users' traffic statistics inaccurate, Re-online is recommended
after this operation, continue?[Y/N]y
```

13.2.50 radius-server format-attribute

Function

The **radius-server format-attribute** command configures the format of the NAS-Port attribute.

The **undo radius-server format-attribute** command deletes the configured attribute format.

By default, the format of the NAS-Port attribute is **new**.

Format

radius-server format-attribute nas-port *nas-port-sting* [**decimal**]

undo radius-server format-attribute nas-port

Parameters

Parameter	Description	Value
nas-port *nas-port-sting*	Specifies the format of the NAS-Port attribute. In the *nas-port-string* parameter in binary format: ● The keywords **s**, **t**, **p**, **o**, and **i** indicate slot, subslot, port, out-vlan (qinqvlan)/vpi, and vlan (user-vlan)/vci respectively. The keywords **n** and **z** are used as paddings. The keyword **n** indicates 1 and the keyword **z** indicates 0. ● The keywords **s**, **t**, **p**, **o**, and **i** must be followed by numbers, and the numbers must range from 1 to 32. The keywords **s**, **t**, **p**, **o**, and **i** can appear in the format string only once. ● The keywords **s**, **t**, **p**, **o**, **i**, **n**, and **z** must range from 1 to 9. ● **n** and **z** can appear multiple times at any position. They are followed by numbers. For example, **n12** indicates that this position is filled in with twelve 1s, and **z12** indicates that this position is filled in with twelve 0s. ● The character string must contain 32 bits. ● The format string must start with **s**, **t**, **p**, **o**, **i**, **n**, or **z** and end with a number.	The value is a character string. When the *nas-port-string* parameter is in binary format, the value is a string of 1 to 32 characters. When the *nas-port-string* parameter is in decimal format, the value is a string of 1 to 9 characters.

Parameter	Description	Value
	- If no VLAN exists, you can add **n** or **z** before **o** or **i** to indicate whether this position is filled in with 0s or 1s. That is, **n** and **z** can be followed by numbers, **o**, or **i** in this case, and the numbers must range from 1 to 32. - To specify the format string, determine the interface type, and then determine the encapsulation type of the interface. If the format string does not contain **o** or **i**, the NAS-Port attribute does not contain the QinQ VLAN or user VLAN field. If the format string contains **o** or **i** but no outer VLAN exists, the outer VLAN field is filled in with 0s. If **n** is added before **o** or **i**, this field is filled in with 1s when no outer VLAN or inner VLAN exists. In the *nas-port-string* parameter in decimal format: - The keywords **s**, **t**, **p**, **o**, and **i** indicate slot, subslot, port, out-vlan (qinqvlan)/vpi, and vlan (user-vlan)/vci respectively. - The keywords **s**, **t**, **p**, **o**, and **i** must be followed by a number ranging from 1 to 9. Each keyword can appear only once. - If **s**, **t**, **p**, **o**, and **i** is followed by a number,	

Parameter	Description	Value
	the first number must range from 1 to 9 and cannot be 0. - The string can contain at most 9 digits. - The string must start with **s**, **t**, **p**, **o**, or **i** and end with a number. - If no VLAN exists, this field is filled in with 0. In the decimal string, this field cannot be filled in with 1. - To specify the format string, determine the interface type, and then determine the encapsulation type of the interface. If the format string does not contain **o** or **i**, the NAS-Port attribute does not contain the QinQ VLAN or user VLAN field. If the format string contains **o** or **i** but no outer VLAN exists, the outer VLAN field is filled in with 0 by default. If no VLAN exists, both the inner and outer VLAN fields are filled in with 0 by default.	
decimal	Indicates that *nas-port-string* is in decimal format. If this parameter is not specified, *nas-port-string* is in binary format.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The NAS port format affects the information about the physical port. The NAS port format can be used by the RADIUS server to process services, such as binding the user name and port. This attribute is developed by Huawei, which is used to ensure connectivity and service cooperation among Huawei devices.

If the **radius-server nas-port-format** command sets the format of the NAS-Port attribute to **new** (the default format is **new**), the device will check whether the **radius-server format-attribute nas-port** command configuration exists. If so, the device will assemble the NAS-Port attribute in the format configured by the **radius-server format-attribute nas-port** command. If no, the device will assemble the NAS-Port attribute in the **new** format. If the **radius-server nas-port-format** command sets the format of the NAS-Port attribute to **old**, the device will assemble the NAS-Port attribute in the **old** format, regardless of whether the **radius-server format-attribute nas-port** command configuration exists.

Example

Configure the format of the NAS-Port attribute to s2t2p6no10ni12 in binary format. That is, the NAS-Port attribute consists of a 2-bit slot field, a 2-bit subslot field, a 6-bit port field, a 10-bit outer VLAN field, and a 12-bit inner VLAN field. If the outer VLAN does not exist, this field is filled in with ten 1s. If the inner VLAN does not exist, this field is filled in with twelve 1s. Therefore, the NAS-port attribute contains 32 bits.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server format-attribute nas-port s2t2p6no10ni12
```

Configure the format of the NAS-Port attribute to s1t1p2o1i1 in decimal format. That is, the NAS-Port attribute consists of a 1-bit slot field, a 1-bit subslot field, a 2-bit port field, a 1-bit outer VLAN field, and a 1-bit inner VLAN field. If the outer VLAN does not exist, this field is filled in with 0. If the inner VLAN does not exist, this field is filled in with 0.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server format-attribute nas-port s1t1p2o1i1 decimal
```

13.2.51 radius-server framed-ip-address no-user-ip enable

Function

The **radius-server framed-ip-address no-user-ip enable** command enables the device to encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

The **undo radius-server framed-ip-address no-user-ip enable** command disables the device from encapsulating the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

By default, the device does not encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

Format

radius-server framed-ip-address no-user-ip enable

undo radius-server framed-ip-address no-user-ip enable

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

In MAC address authentication triggered through DHCP packets, a user can obtain an IP address only after being successfully authenticated. The RADIUS authentication request packet sent by the user does not carry the IP address of the user. By default, the device does not encapsulate the RADIUS attribute Framed-IP-Address into the RADIUS authentication request packet sent by the user when forwarding the packet. If the RADIUS server connected to the device requires that the received RADIUS authentication request packets contain the RADIUS attribute Framed-IP-Address, run the **radius-server framed-ip-address no-user-ip enable** command. Then the device uses the IP address 0.0.0.0 to encapsulate the RADIUS attribute Framed-IP-Address when receiving the RADIUS authentication request packets that do not contain the user IP address.

Example

Enable the device to encapsulate the RADIUS attribute Framed-IP-Address into a RADIUS authentication request packet when the RADIUS authentication request packet sent by a user does not carry the user IP address.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server framed-ip-address no-user-ip enable
```

13.2.52 radius-server hw-ap-info-format include-ap-ip

Function

The **radius-server hw-ap-info-format include-ap-ip** command configures the AP's IP address carried in Huawei extended attribute HW-AP-Information.

The **undo radius-server hw-ap-info-format** command restores the default setting.

By default, Huawei extended attribute HW-AP-Information does not carry AP's IP address.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

radius-server hw-ap-info-format include-ap-ip

undo radius-server hw-ap-info-format

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

RADIUS is a fully extensible protocol. Device vendors can expand the No. 26 attribute defined in the protocol to implement functions not supported by standard RADIUS attributes. Huawei defines the No. 141 sub-attribute (HW-AP-Information) in the No. 26 attribute to indicate AP information, including the MAC and IP addresses of an AP. The HW-AP-Information attribute is carried in the authentication or accounting request packet send by a device, so that the RADIUS server can use the AP's MAC and IP addresses as the filter criterion to select a policy template to be delivered.

When an AP's IP address is carried in the HW-AP-Information attribute, the encapsulation format of the attribute is AP-MAC AP-IP.

Example

#Configure the AP's IP address in Huawei extended attribute HW-AP-Information.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] radius-server hw-ap-info-format include-ap-ip
```

13.2.53 radius-server hw-dhcp-option-format

Function

The **radius-server hw-dhcp-option-format** command sets the format of the Huawei extended attribute HW-DHCP-Option.

The **undo radius-server hw-dhcp-option-format** command restores the default setting.

By default, the format of HW-DHCP-Option is old.

Format

radius-server hw-dhcp-option-format { **new** | **old** }

undo radius-server hw-dhcp-option-format

Parameters

Parameter	Description	Value
new	Sets the format of Huawei extended attribute HW-DHCP-Option to new.	-
old	Sets the format of Huawei extended attribute HW-DHCP-Option to old.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The RADIUS protocol has good extensibility. Device vendors can expand the No. 26 RADIUS attribute to implement new functions. Huawei defines that the No.158 sub-attribute in the No.26 attribute represents DHCP option and is encapsulated through Type, Length, Value (TLV). The device adds this attribute in authentication request or accounting request packets and sends the DHCP option information to the RADIUS server.

To connect to different types of RADIUS server, the device supports two HW-DHCP-Option formats: **new** and **old**.

- **new**: When the attribute is encapsulated through TLV, the Type field length is 1 byte. This format is applicable when the device connects to most types of RADIUS servers.
- **old**: When the attribute is encapsulated through TLV, the Type field length is 2 bytes. This format is applicable when the device connects to special RADIUS servers, for example, Huawei RADIUS server.

Example

Set the format of Huawei extended attribute HW-DHCP-Option to new.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test
[HUAWEI-radius-test] radius-server hw-dhcp-option-format new
```

13.2.54 radius-server nas-identifier-format

Function

The **radius-server nas-identifier-format** command sets the encapsulation format of the NAS-Identifier attribute.

The **undo radius-server nas-identifier-format** command restores the default encapsulation format of the NAS-Identifier attribute.

By default, the NAS-Identifier attribute encapsulation format is the NAS device's hostname.

Format

radius-server nas-identifier-format { **hostname** | **vlan-id** | **ap-info** }

undo radius-server nas-identifier-format

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ap-info** parameter.

Parameters

Parameter	Description	Value
hostname	Sets the encapsulation format of NAS-Identifier to the NAS device's host name.	-
vlan-id	Sets the encapsulation format of NAS-Identifier to a user's VLAN ID.	-
ap-info	Sets the encapsulation format of NAS-Identifier to the AP's MAC address.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

A RADIUS server uses the NAS-Identifier attributes to identify NASs. The NASs also use the NAS-Identifier attributes carried in the sent RADIUS packets to identify themselves.

When the RADIUS server interconnected with the device requires that the NAS-Identifier attribute value is the MAC address of the AP when the device functions as an AC in a wireless scenario, you need to run the **radius-server nas-identifier-format ap-info** command.

Example

Set the NAS-Identifier encapsulation format to VLAN ID.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server nas-identifier-format vlan-id
```

13.2.55 radius-server nas-port-format

Function

The **radius-server nas-port-format** command sets the format of the NAS port attribute.

The **undo radius-server nas-port-format** command restores the default format of the NAS port attribute.

By default, the new NAS port format is used.

Format

radius-server nas-port-format { **new** | **old** }

undo radius-server nas-port-format

Parameters

Parameter	Description	Value
new	Uses the new format of an NAS port. The new format of the NAS port attribute is slot number (8 bits) + subslot number (4 bits) + port number (8 bits) + VLAN ID (12 bits).	-

Parameter	Description	Value
old	Uses the old format of an NAS port. The old format of the NAS port attribute is slot number (12 bits) + port number (8 bits) + VLAN ID (12 bits).	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NAS port format affects the information about the physical port. The NAS port format can be used by the RADIUS server to process services, such as binding the user name and port. This attribute is developed by Huawei, which is used to ensure connectivity and service cooperation among Huawei devices.

Precautions

The difference between the two NAS port formats lies in the physical ports connected to Ethernet access users.

- The new format of the NAS port attribute is slot number (8 bits) + subslot number (4 bits) + port number (8 bits) + VLAN ID (12 bits).
- The old format of the NAS port attribute is slot number (12 bits) + port number (8 bits) + VLAN ID (12 bits).

The format of the NAS port attribute for Asymmetric Digital Subscriber Line (ADSL) access users is slot number (4 bits) + subslot number (2 bits) + port number (2 bits) + VPI (8 bits) + VCI (16 bits). This format is not affected by the command.

Example

Set the format of the NAS port attribute to **new**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server nas-port-format new
```

13.2.56 radius-server nas-port-id-format

Function

The **radius-server nas-port-id-format** command sets the format of the NAS port ID attribute.

The **undo radius-server nas-port-id-format** command restores the default format of the NAS port ID attribute.

By default, the new format of the NAS port ID attribute is used.

Format

radius-server nas-port-id-format { **new** [**client-option82**] | **old** | **vendor** *vendor-id* }

undo radius-server nas-port-id-format

Parameters

Parameter	Description	Value
new	Uses the new format of the NAS port ID.	-
client-option82	Uses the content of the Option82 field as the format of the NAS-Port-Id attribute.	-
old	Uses the old format of the NAS port ID.	-
vendor *vendor-id*	Uses the NAS port ID format that is customized by the vendor.	The value is an integer. Currently, the value can only be 9.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NAS port format and the NAS port ID format are developed by Huawei, which are used to ensure connectivity and service cooperation among Huawei devices.

Precautions

Port of the NAS that is authenticating the user. The NAS-Port-Id attribute has the following formats:

- New:

  For Ethernet access users, the NAS-Port-Id is in the format "slot=xx; subslot=xx; port=xxx; vlanid=xxxx; interfaceName=*port*", in which "slot" is 64 or ranges from 0 to 15, "subslot" ranges from 0 to 15, "port" ranges from 0 to 255, "vlanid" ranges from 1 to 4094, "interfaceName" indicates the user access interface, including the interface type and number.

  For ADSL access users, the NAS-Port-Id is in the format "slot=xx; subslot=x; port=x; VPI=xxx; VCI=xxxxx; interfaceName=*port*", in which "slot" ranges from 0 to 15, "subslot" 0 to 9, "port" 0 to 9, "VPI" 0 to 255, and "VCI" 0 to 65535, "interfaceName" indicates the user access interface, including the interface type and number.

- New client-option82:

  When a PPPoE or DHCP user goes online, if the PPPoE or DHCP packet sent by the user contains the Option 82 field, the device encapsulates the content of the circuit ID suboption in the Option 82 field into the NAS-Port-Id (87) attribute of a RADIUS packet, and then sends the RADIUS packet to the RADIUS server, binding the user account to the access location and preventing an account from being shared by multiple users. In this case, the format of NAS-Port-Id (87) attribute in the RADIUS packet is the same as that of the circuit ID suboption in the Option 82 field. To configure the format of the circuit ID suboption, run the **dhcp option82 format** or **pppoe intermediate-agent information format** command.

  NOTE

  - If the PPPoE or DHCP packet does not contain the Option 82 field, the format of the NAS-Port-Id (87) attribute in the RADIUS packet is **new**.
  - If the **new client-option82** parameter is selected, the device encapsulates the content of the first 128 bytes in the Circuit ID suboption of the Option 82 field into the NAS-Port-Id (87) attribute of a RADIUS packet. If the first 128 bytes contain 0, the device only encapsulates bytes before the first 0. If the first byte of the Circuit ID value is 0 or no Circuit ID value exists, the format of the NAS-Port-Id (87) attribute in RADIUS packets is **new**.

- Old:

  For Ethernet access users, the NAS-Port-Id is in the format "port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VLAN ID (9 characters)."

  For ADSL access users: port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VPI (8 characters) + VCI (16 characters). The fields are prefixed with 0s if they contain fewer bytes than specified.

- vendor *vendor-id*:

  The NAS port ID format is customized by the vendor. The value of *vendor-id* currently can only be 9. It is in the format of interface type+interface number, indicating a user access interface. To check the access interface of a specified user, run the **display access-user user-id** *user-id* command. In the command output, the **User access Interface** field indicates the access interface of a user.

NOTE

If this attribute carries Chinese characters, it cannot be delivered using the **radius-attribute set** *attribute-name attribute-value* command.

Example

Set the format of the NAS port ID attribute to **new**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server nas-port-id-format new
```

13.2.57 radius-server retransmit timeout

Function

The **radius-server retransmit timeout** command sets the number of times that RADIUS request packets are retransmitted, timeout period.

The **undo radius-server retransmit timeout** command restores the default number of retransmission times, the default timeout period.

By default, the number of retransmission times is 5, timeout period is 2 seconds.

Format

radius-server { **retransmit** *retry-times* | **timeout** *time-value* } *

undo radius-server { **retransmit** [*retry-times*] | **timeout** [*time-value*] } *

Parameters

Parameter	Description	Value
retransmit *retry-times*	Specifies the number of retransmission times. The value is the total number of times a packet is transmitted.	The value is an integer that ranges from 1 to 5.
timeout *time-value*	Specifies the timeout period.	The value is an integer that ranges from 1 to 100, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The retransmission upon timeout mechanism is configured for a device to forward RADIUS Access-Request packets sourced from users to the server. The overall retransmission time depends on the retransmission interval, retransmission times, RADIUS server status, and number of servers configured in the RADIUS server template.

You can configure the number of times that RADIUS request packets are retransmitted and the timeout period using the **radius-server retransmit** *retry-times* and **radius-server timeout** *time-value* commands, respectively. If a device sends an authentication request packet to the RADIUS server and does not receive any response packet from the server during the timeout period, the device sends an authentication request packet again.

This command can improve the reliability of RADIUS authentication.

Precautions

- The request packet retransmission time (number of retransmission times x timeout period) of the RADIUS server must be shorter than the request packet retransmission time of the Portal server.
- If more than 8 authentication server IP addresses are configured in the RADIUS server template, reduce the number of retransmission times and timeout period.

Example

Set the number of retransmission times to 3, the timeout period to 2s.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server retransmit 3 timeout 2
```

13.2.58 radius-server session-manage

Function

The **radius-server session-manage** command enables session management on the RADIUS server.

The **undo radius-server session-manage** command disables session management on the RADIUS server.

By default, session management is disabled on the RADIUS server.

Format

radius-server session-manage { *ip-address* [**vpn-instance** *vpn-instance-name*] **shared-key cipher** *share-key* | **any** }

undo radius-server session-manage [*ip-address* [**vpn-instance** *vpn-instance-name*] | **all**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the RADIUS session management server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance bound to the RADIUS session management server.	The value must be the name of an existing VPN instance.
shared-key cipher *share-key*	Specifies the shared key of the RADIUS session management server.	The value is a string of case-sensitive characters that cannot contain spaces and question marks. *share-key* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
any	Indicates that no RADIUS session management server is specified.	-
all	Deletes all RADIUS session management servers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve device security, run this command to enable session management on the RADIUS server. After this function is enabled, the device checks the source IP addresses and shared keys for the received session management packets. When the source IP addresses and shared keys match the configured values, the packets are processed; otherwise, the packets are discarded.

Precautions

- This command has been supported since V200R010C00. When a device is upgraded from a version earlier than V200R010C00 to V200R010C00 or a later version, the **radius-server session-manage any** command is configured by default.
- When the **any** parameter is specified, there is a security risk. You are advised to configure the IP address and shared key for a specified RADIUS session management server.
- In V200R020C10SPC100 and later versions, you also need to run the **radius-server session-manage server-source** command to configure an IPv4 address for receiving and responding to request packets of a RADIUS session management server so that the session management function of the RADIUS server can take effect.

Example

Enable session management on the RADIUS server, and set the IP address and shared key of the RADIUS session management server to 10.1.1.1 and **YsHsjx_202206** respectively.

```
<HUAWEI> system-view
[HUAWEI] radius-server session-manage 10.1.1.1 shared-key cipher YsHsjx_202206
```

13.2.59 radius-server session-manage server-source

Function

The **radius-server session-manage server-source** command configures an IPv4 address for receiving and responding to request packets of a RADIUS session management server.

The **undo radius-server session-manage server-source** command restores the default setting.

By default, the device does not receive or respond to any request packet of a RADIUS session management server.

Format

radius-server session-manage server-source { **ip-address** *ip-address* | **all-interface** }

undo radius-server session-manage server-source { **ip-address** { *ip-address* | **all** } | **all-interface** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation. The value range depends on the device types.

Parameter	Description	Value
all-interface	Specifies the IPv4 address as 0.0.0.0. That is, the device receives and responds to request packets of a RADIUS session management server through any IPv4 address.	-
all	Indicates all IPv4 addresses specified by **ip-address** *ip-address*.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no IPv4 address can be used to receive or respond to request packets of a RADIUS session management server. When the device needs to establish a connection with a RADIUS session management server, you can run this command to specify an IPv4 address for receiving and responding to request packets of the RADIUS session management server.

Precautions

- After you run this command to configure an IPv4 address for the device to receive and respond to request packets of a RADIUS session management server, the RADIUS session management server can communicate with the device only through this IPv4 address. Ensure that the RADIUS session management server can communicate with the device through this IPv4 address at Layer 3.
- After the **radius-server session-manage server-source all-interface** command is run, the device receives and responds to request packets of a RADIUS session management through any IPv4 address, which increases system security risks. Therefore, you are advised not to run this command.
- After the **radius-server session-manage server-source all-interface** command is run, all the configurations of the **radius-server session-manage server-source ip-address** *ip-address* command are cleared.
- If the **radius-server session-manage server-source all-interface** command has been configured on the device, the **radius-server session-manage server-source ip-address** *ip-address* command configured later cannot be delivered.

- If the device is upgraded from a version earlier than V200R020C10SPC100 and the session management function is enabled for the RADIUS server, the device delivers the **radius-server session-manage server-source all-interface** command by default to enable the session management function for the RADIUS server with an all-zero address.
- In versions earlier than V200R020C10SPC100, if the session management function of the RADIUS server is enabled, you need to enable the session management function when using the session management function of the RADIUS server in versions later than V200R020C10SPC100. That is, run the **radius-server session-manage server-source all-interface** command to enable the session management function of the RADIUS server with an all-zero IP address or run the **radius-server session-manage server-source ip-address** *ip-address* command to enable the session management function of the RADIUS server with a specified IP address.
- In V200R020C10SPC100 and later versions, you also need to run the **radius-server session-manage server-source** command to configure an IPv4 address for receiving and responding to request packets of a RADIUS session management server so that the session management function of the RADIUS server can take effect.

Example

Specify 10.1.1.1 as the IPv4 address used to receive and respond to request packets of a RADIUS session management server.

```
<HUAWEI> system-view
[HUAWEI] radius-server session-manage server-source ip-address 10.1.1.1
```

13.2.60 radius-server shared-key (RADIUS server template view)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The **undo radius-server shared-key** command deletes the shared key of a RADIUS server.

By default, no shared key of RADIUS server is configured.

Format

radius-server shared-key cipher *key-string*

undo radius-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-

Parameter	Description	Value
key-string	Specifies the shared key of a RADIUS server.	The value is a case-sensitive character string without spaces, single quotation marks ('), or question marks (?). *key-string* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with a RADIUS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. To ensure validity of both communication parties, the device and RADIUS server must be configured with the same shared key.

Precautions

For security purposes, change the default shared key immediately. It is recommended that the new shared key contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Set the shared key of a RADIUS server to **YsHsjx_202206** in cipher text.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server shared-key cipher YsHsjx_202206
```

13.2.61 radius-server shared-key (system view)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The **undo radius-server shared-key** command deletes the shared key of a RADIUS server.

By default, no global shared key is configured for the RADIUS server.

Format

radius-server ip-address { *ipv4-address* | *ipv6-address* } **shared-key cipher** *key-string*

undo radius-server ip-address { *ipv4-address* | *ipv6-address* } **shared-key**

Parameters

Parameter	Description	Value
ip-address { *ipv4-address* | *ipv6-address* }	Specifies the IPv4 or IPv6 address of the RADIUS server.	- *ipv4-address*: The value is in dotted decimal notation. - *ipv6-address*: The value is a 32-bit hexadecimal string in format X:X:X:X:X:X:X:X.
cipher *key-string*	Specifies the shared key in cipher text.	The value is a case-sensitive character string without spaces, single quotation marks ('), or question marks (?). *key-string* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with a RADIUS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. To ensure validity of both communication parties, the device and RADIUS server must be configured with the same shared key.

You can run the **radius-server shared-key** command in the RADIUS server template view to configure the shared keys. However, after this command is run, all RADIUS servers in the template use the same shared key. To configure different shared keys for RADIUS servers, run the **radius-server shared-key** command in the system view.

Precautions

To improve security, it is recommended that the shared key contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

When the shared keys are configured in both the RADIUS server template and system view, the configuration in the system view takes effect.

Example

Set the shared key for RADIUS server to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] radius-server ip-address 10.1.1.1 shared-key cipher YsHsjx_202206
```

13.2.62 radius-server support chargeable-user-identity

Function

The **radius-server support chargeable-user-identity** command configures a device to support the CUI attribute.

The **undo radius-server support chargeable-user-identity** command restores the default settings.

By default, a device does not support the CUI attribute.

Format

radius-server support chargeable-user-identity [**not-reject**]

undo radius-server support chargeable-user-identity

Parameters

Parameter	Description	Value
not-reject	Configures the device not to process the CUI attribute.	-

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

In a scenario where roaming accounting is performed on a carrier network, the same user may have register different user names in different network environments. Therefore, the user name cannot be used as the unique ID for accounting. In this case, you can use the RADIUS Chargeable-User-Identity (CUI) attribute defined in the RFC to resolve this issue. RADIUS authentication servers can provide users with unique CUI attribute values that function as the users' accounting IDs.

By default, RADIUS Access-Request packets sent by a device do not carry the CUI attribute. If Access-Accept packets responded by the RADIUS server carry the CUI attribute, the device retains this attribute in the Accounting-Request(Start), Accounting-Request(Interim-update), and Accounting-Request(Stop) packets without any processing.

After the **radius-server support chargeable-user-identity** [**not-reject**] command is configured, the RADIUS Access-Request packets sent by the device carry the CUI attribute and the attribute value is Null.

- If Access-Accept packets responded by the RADIUS server carry the CUI attribute, the device retains this attribute in the Accounting-Request(Start), Accounting-Request(Interim-update), and Accounting-Request(Stop) packets without any processing; the previously delivered CUI attribute is carried in the Access-Request packets triggered by the subsequent reauthentication, authentication coverage, and roaming for users.
- If Access-Accept packets responded by the RADIUS server does not carry the CUI attribute or carry the CUI attribute whose value is Null:
  - If the **not-reject** parameter is not specified, user authentication fails.
  - If the **not-reject** parameter is specified, the device ignores the CUI attribute and user authentication succeeds.

Example

Configure a device to support the CUI attribute.

```
<HUAWEI> system-view
[HUAWEI] radius-server template test1
[HUAWEI-radius-test1] radius-server support chargeable-user-identity
```

13.2.63 radius-server template

Function

The **radius-server template** command creates a RADIUS server template and displays the RADIUS server template view.

The **undo radius-server template** command deletes a RADIUS server template.

By default, the device contains the RADIUS server template **default**. The template can be modified, but cannot be deleted.

Format

radius-server template *template-name*

undo radius-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The value is a string of 1 to 32 case-sensitive characters, including letters (case-sensitive), numerals (0 to 9), periods (.), hyphens (-), and underscores (_). The value cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Creating a RADIUS server template is the prerequisite for configuring RADIUS authentication and accounting. You can perform RADIUS configurations, such as the configuration of authentication servers, accounting servers, and shared key only after a RADIUS server template is created.

Follow-up Procedure

Configure an authentication server, an accounting server, and shared key in the RADIUS server template view, and then run the **radius-server** command to apply the RADIUS server template.

Example

Create a RADIUS server template **template1** and enter the RADIUS server template view.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1]
```

13.2.64 radius-server testuser

Function

The **radius-server testuser** command enables the automatic detection function and configures an automatic detection account.

The **undo radius-server testuser** command restores the default settings.

By default, the automatic detection function is disabled.

Format

radius-server testuser username *user-name* **password cipher** *password*

undo radius-server testuser

Parameters

Parameter	Description	Value
username *user-name*	Specifies a user name used for automatic detection.	The value is a string of 1 to 253 case-sensitive characters. If the user name contains spaces, you must enclose the name with double quotation marks ("), for example, "user for test".
password cipher *password*	Specifies the user password for automatic detection.	The value is a character string of 1 to 128 characters without spaces and question marks. It is case sensitive. If it is in cipher text, the password is a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After the RADIUS server status is set to Down, you can configure the automatic detection function to test the RADIUS server reachability.

For the automatic status detection function, only the automatic detection user name and password need to be configured in the RADIUS server template on the device, and the automatic detection account does not need to be configured on the RADIUS server. Authentication success is not mandatory. If the device can receive the authentication failure response packet, the RADIUS server is properly working.

On a large-scale network, you are advised not to enable automatic detection for RADIUS servers in Up state. This is because if automatic detection is enabled on multiple NAS devices, the RADIUS server periodically receives a large number of detection packets when processing RADIUS Access-Request packets source from users, which may deteriorate processing performance of the RADIUS server.

You can run the **radius-server detect-server timeout** command to configure the timeout period for detection packets.

Example

Create a user account with the user name **test** and password **YsHsjx_202206** in RADIUS server template **acs**.

```
<HUAWEI> system-view
[HUAWEI] radius-server template acs
[HUAWEI-radius-acs] radius-server testuser username test password cipher YsHsjx_202206
```

13.2.65 radius-server traffic-unit

Function

The **radius-server traffic-unit** command sets the traffic unit used by a RADIUS server.

The **undo radius-server traffic-unit** command restores the default traffic unit used by a RADIUS server.

The default RADIUS traffic unit is byte on the device.

Format

radius-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

undo radius-server traffic-unit

Parameters

Parameter	Description	Value
byte	Indicates that the traffic unit is byte.	-
kbyte	Indicates that the traffic unit is kilobyte.	-
mbyte	Indicates that the traffic unit is megabyte.	-
gbyte	Indicates that the traffic unit is gigabyte.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Different RADIUS servers may use different traffic units; therefore, you need to set the traffic unit for each RADIUS server group on the router and the traffic unit must be the same as that on the RADIUS server.

Example

Set the traffic unit used by a RADIUS server to kilobyte.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] radius-server traffic-unit kbyte
```

13.2.66 radius-server user-name domain-included

Function

The **radius-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in the packets sent to a RADIUS server.

The **radius-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to a RADIUS server.

The **undo radius-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name in the packets sent to a RADIUS server.

The **undo radius-server user-name domain-included except-eap** command configures the device not to encapsulate the domain name in the user name in the packets sent to a RADIUS server (applicable to authentication modes except EAP authentication).

By default, the device does not modify the user name entered by the user in the packets sent to a RADIUS server.

Format

radius-server user-name domain-included

radius-server user-name original

undo radius-server user-name domain-included

undo radius-server user-name domain-included except-eap

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter. The domain name delimiter can also be any of the following symbols: \ / : < > | ' %.

If the RADIUS server does not accept the user name with the domain name, run the **undo radius-server user-name domain-included** command to delete the domain name from the user name.

Precautions

If the user names in the RADIUS packets sent from the device to RADIUS server contain domain names, ensure that the total length of a user name (user name + domain name delimiter + domain name) is not longer than 253 characters; otherwise, the user name cannot be contained in RADIUS packets. As a result, authentication will fail.

Example

Configure the device not to encapsulate the domain name in the user name in the packets sent to a RADIUS server.

```
<HUAWEI> system-view
[HUAWEI] radius-server template template1
[HUAWEI-radius-template1] undo radius-server user-name domain-included
```

13.2.67 reset radius-server accounting-stop-packet

Function

The **reset radius-server accounting-stop-packet** command clears statistics on the remaining buffer information of RADIUS accounting-stop packets.

Format

reset radius-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets.	-
ip *ipv4-address*	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets with the specified IPv4 address.	The value of *ipv4-address* is in dotted decimal notation.
ip *ipv6-address*	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command can clear statistics on the remaining buffer information of RADIUS accounting-stop packets. The deleted statistics cannot be restored.

Example

Clear statistics on the remaining buffer information of all RADIUS accounting-stop packets.

```
<HUAWEI> reset radius-server accounting-stop-packet all
```

13.2.68 test-aaa

Function

The **test-aaa** command tests the connectivity between the device and the authentication server or accounting server, and tests whether a user can be authenticated using authentication server and whether the accounting server can charge a user.

Format

test-aaa *user-name user-password* **radius-template** *template-name* [**chap** | **pap**] [**called-station-id** [**ssid** *ssid*]]

test-aaa *user-name user-password* **radius-template** *template-name* [**accounting** [**start** | **realtime** | **stop**]]

test-aaa *user-name user-password* **hwtacacs-template** *template-name* [**accounting** [**start** | **realtime** | **stop**]]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ssid** parameter.

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 253 case-insensitive characters. When the user name contains spaces, you must put the string in double quotation marks (""). **NOTE** When the HWTACACS, or RADIUS server is detected, the user name cannot contain spaces.

Parameter	Description	Value
user-password	Specifies a user password.	The value is a string of 1 to 128 case-sensitive characters.
radius-template *template-name*	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.
chap	Indicates Challenge Handshake Authentication Protocol (CHAP) authentication. The NAS device sends the user name, password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user.	-
pap	Indicates Password Authentication Protocol (PAP) authentication. The NAS device adds the user name and encrypted password to the corresponding fields of authentication request packets, and then sends the packets to the RADIUS server. The NAS device determines whether to allow the user go online based on the result returned by the RADIUS server.	-

Parameter	Description	Value
called-station-id	Specifies the called-station-id attribute. When the device detects that an authentication packet carries the called-station-id attribute, it automatically encapsulates its MAC address XX-XX-XX-XX-XX-XX. The MAC address format is configured in the RADIUS server template.	-

Parameter	Description	Value
ssid *ssid*	Specifies the SSID.	The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or the combination of Chinese and English characters, without tab characters. To start an SSID with a space, you need to enclose the SSID with double quotation marks ("), for example, **" hello"**. The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to put a backslash (\\) before the double quotation mark, for example, **\\"hello**. The backslash occupies one character.
accounting	Indicates accounting. By default, an accounting-start packet is sent.	-

Parameter	Description	Value
start	Indicates that the sent packet is an accounting-start packet.	-
realtime	Indicates that the sent packet is a real-time accounting packet.	-
stop	Indicates that the sent packet is an accounting-stop packet.	-
hwtacacs-template *template-name*	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The test-aaa command tests service reachability of the server. The device sends an authentication or accounting request packet to the server. If the server returns an authentication or accounting success packet, the device and server can communicate with each other. If the server's response times out, the device and server cannot communicate with each other.

When the controller functions as an authentication server and the **test-aaa** command is run to test accounts, authentication packets must carry the user name, password, device MAC address, and SSID (for wireless terminals) so that the controller can match the packets with the corresponding authentication template. This ensures that the function of the **test-aaa** command is working properly.

Prerequisites

The authentication server template or accounting server template has been created, and the authentication server or accounting server has been configured in the template. In addition, the authentication server or accounting server has been configured.

Follow-up Procedure

If the test result indicates that the user fails to be authenticated by using server authentication or the accounting server fails to charge the user, check whether the configuration of the authentication server template and the authentication server is correct, and check the connectivity between the device and the server.

Precautions

chap and **pap** are two authentication modes, CHAP authentication is used by default.

- PAP: The NAS device adds the user name and encrypted password to the corresponding fields of authentication request packets, and then sends the packets to the RADIUS server. The NAS device determines whether to allow the user go online based on the result returned by the RADIUS server.
- CHAP: The NAS device sends the user name, password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user.

Before running the **test-aaa** command, you only need to create a RADIUS server template and specify an authentication server or accounting server in the RADIUS server template.

Example

Test whether the user **user1** can be authenticated using CHAP authentication in the RADIUS server template **test**.

```
<HUAWEI> test-aaa user1 userkey radius-template test chap
Info: The server template does not exist.
```

13.3 HWTACACS Configuration Commands

13.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.3.2 display hwtacacs-server accounting-stop-packet

Function

The **display hwtacacs-server accounting-stop-packet** command displays information about Accounting-Stop packets sent by an HWTACACS server.

Format

display hwtacacs-server accounting-stop-packet { **all** | *number* | **ip** { *ipv4-address* | *ipv6-address* }}

Parameters

Parameter	Description	Value
all	Displays information about all Accounting-Stop packets.	-
number	Specifies the number of pieces of Accounting-Stop information that can be queried by each process.	The value is an integer that ranges from 1 to 65535.
ip *ipv4-address*	Displays information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv4 address.	The value is in dotted decimal notation.
ip *ipv6-address*	Displays information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

3: Management level

Usage Guidelines

During HWTACACS troubleshooting, you can run this command to check information about Accounting-Stop packets sent by the HWTACACS server.

NOTE

After an active/standby switchover, statistics about Accounting-Stop packets will be cleared.

Example

Display information about all Accounting-Stop packets.

```
<HUAWEI> display hwtacacs-server accounting-stop-packet all
-----------------------------------------------------------
NO. SendTime      IP Address                       Template
1   10            192.168.1.110                    tac
-----------------------------------------------------------
Whole accounting stop packet to resend:1
```

Table 13-35 Description of the **display hwtacacs-server accounting-stop-packet** command output

Item	Description
NO.	Number of the Accounting-Stop packet.
SendTime	Number of times that Accounting-Stop packets are sent.
IP Address	IP address of the HWTACACS server.
Template	Name of the HWTACACS server template.
Whole accounting stop packet to resend	Total number of Accounting-Stop packets sent by a device.

13.3.3 display hwtacacs-server template

Function

The **display hwtacacs-server template** command displays the configurations of HWTACACS server templates.

Format

display hwtacacs-server template [*template-name*]

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hwtacacs-server template** command output helps you check the configurations of HWTACACS server templates and locate faults.

NOTE

The device determines whether its communication with the HWTACACS server is proper based on the response timeout mechanism of HWTACACS request packets, and always marks the status of the last HWTACACS server as Up.

Example

Display the configuration of the HWTACACS server template **template0**.

```
<HUAWEI> display hwtacacs-server template template0
 ---------------------------------------------------------------------------
 HWTACACS-server template name        : template0
 HWTACACS-server template index       : 0
 Primary-authentication-server        : -:49 Vrf:- Status:-

 Primary-authentication-ipv6-server   : -:49 Vrf:- Status:-
 Primary-authorization-server         : -:49 Vrf:- Status:-
 Primary-authorization-ipv6-server    : -:49 Vrf:- Status:-
 Primary-accounting-server            : -:49 Vrf:- Status:-
 Primary-accounting-ipv6-server       : -:49 Vrf:- Status:-
 Secondary-authentication-server      : -:49 Vrf:- Status:-
 Secondary-authentication-ipv6-server : -:49 Vrf:- Status:-
 Secondary-authorization-server       : -:49 Vrf:- Status:-
 Secondary-authorization-ipv6-server  : -:49 Vrf:- Status:-
 Secondary-accounting-server          : -:49 Vrf:- Status:-
 Secondary-accounting-ipv6-server     : -:49 Vrf:- Status:-
 Third-authentication-server          : -:49 Vrf:- Status:-
 Third-authentication-ipv6-server     : -:49 Vrf:- Status:-
 Third-authorization-server           : -:49 Vrf:- Status:-
 Third-authorization-ipv6-server      : -:49 Vrf:- Status:-
 Third-accounting-server              : -:49 Vrf:- Status:-
 Third-accounting-ipv6-server         : -:49 Vrf:- Status:-
 Fourth-authentication-server         : -:49 Vrf:- Status:-
 Fourth-authentication-ipv6-server    : -:49 Vrf:- Status:-
 Fourth-authorization-server          : -:49 Vrf:- Status:-
 Fourth-authorization-ipv6-server     : -:49 Vrf:- Status:-
 Fourth-accounting-server             : -:49 Vrf:- Status:-
 Fourth-accounting-ipv6-server        : -:49 Vrf:- Status:-
 Current-authentication-server        : -:49 Vrf:- Status:-
 Current-authentication-ipv6-server   : -:49 Vrf:- Status:-
 Current-authorization-server         : -:49 Vrf:- Status:-
 Current-authorization-ipv6-server    : -:49 Vrf:- Status:-
 Current-accounting-server            : -:49 Vrf:- Status:-
 Current-accounting-ipv6-server       : -:49 Vrf:- Status:-
 Source-IP-address                    : -
 Source-LoopBack                      : -
 Source-Vlanif                        : -
 Source-IPv6-address                  : -
 IPv6 Source-LoopBack                 : -
 IPv6 Source-Vlanif                   : -
 Shared-key                           : -
 Quiet-interval(min)                  : 5
 Response-timeout-Interval(sec)       : 5
 Domain-included                      : Original
 Traffic-unit                         : B
 User name in authen-start message    : Yes
 ---------------------------------------------------------------------------
```

Table 13-36 Description of the **display hwtacacs-server template** command output

Item	Description
HWTACACS-server template name	Name of an HWTACACS server template.
HWTACACS-server template index	Index of an HWTACACS server template.
Primary-authentication-server	IPv4 address, port number, VPN instance, and status of the primary authentication server.
Primary-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the primary authentication server.
Primary-authorization-server	IPv4 address, port number, VPN instance, and status of the primary authorization server.
Primary-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the primary authorization server.
Primary-accounting-server	IPv4 address, port number, VPN instance, and status of the primary accounting server.
Primary-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the primary accounting server.
Secondary-authentication-server	IPv4 address, port number, VPN instance, and status of the second authentication server.
Secondary-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the second authentication server.
Secondary-authorization-server	IPv4 address, port number, VPN instance, and status of the second authorization server.
Secondary-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the second authorization server.
Secondary-accounting-server	IPv4 address, port number, VPN instance, and status of the second accounting server.
Secondary-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the second accounting server.
Third-authentication-server	IPv4 address, port number, VPN instance, and status of the third authentication server.
Third-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the third authentication server.
Third-authorization-server	IPv4 address, port number, VPN instance, and status of the third authorization server.

Item	Description
Third-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the third authorization server.
Third-accounting-server	IPv4 address, port number, VPN instance, and status of the third accounting server.
Third-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the third accounting server.
Fourth-authentication-server	IPv4 address, port number, VPN instance, shared key, and status of the fourth authentication server.
Fourth-authentication-ipv6-server	IPv6 address, port number, VPN instance, shared key, and status of the fourth authentication server.
Fourth-authorization-server	IPv4 address, port number, VPN instance, shared key, and status of the fourth authorization server.
Fourth-authorization-ipv6-server	IPv6 address, port number, VPN instance, shared key, and status of the fourth authorization server.
Fourth-accounting-server	IPv4 address, port number, VPN instance, shared key, and status of the fourth accounting server.
Fourth-accounting-ipv6-server	IPv6 address, port number, VPN instance, shared key, and status of the fourth accounting server.
Current-authentication-server	IPv4 address, port number, VPN instance, and status of the authentication server in use.
Current-authentication-ipv6-server	IPv6 address, port number, VPN instance, and status of the authentication server in use.
Current-authorization-server	IPv4 address, port number, VPN instance, and status of the authorization server in use.
Current-authorization-ipv6-server	IPv6 address, port number, VPN instance, and status of the authorization server in use.
Current-accounting-server	IPv4 address, port number, VPN instance, and status of the accounting server in use.
Current-accounting-ipv6-server	IPv6 address, port number, VPN instance, and status of the accounting server in use.
Source-IP-address	Source IPv4 address for communication between the device and the HWTACACS server.
Source-LoopBack	Number of the loopback interface. The IPv4 address of the loopback interface is used as the source IPv4 address for communication between the device and the HWTACACS server.

Item	Description
Source-Vlanif	Number of the VLANIF interface. The IPv4 address of the VLANIF interface is used as the source IPv4 address for communication between the device and the HWTACACS server.
Source-IPv6-address	Source IPv6 address for communication between the device and the HWTACACS server.
IPv6 Source-LoopBack	Number of the loopback interface. The IPv6 address of the loopback interface is used as the source IPv6 address for communication between the device and the HWTACACS server.
IPv6 Source-Vlanif	Number of the VLANIF interface. The IPv6 address of the VLANIF interface is used as the source IPv6 address for communication between the device and the HWTACACS server.
Shared-key	Shared key of the HWTACACS server.
Quiet-interval(min)	Interval for the primary server to return to the active state, in minutes.
Response-timeout-Interval(sec)	Response timeout interval of the HWTACACS server, in seconds.
Domain-included	Whether the user name contains an authentication domain name. ● Yes: The user name contains the domain name. ● No: The user name does not contain the domain name. ● Original: The device does not modify the user name entered by the user.
Traffic-unit	Traffic unit used by the HWTACACS server, in bytes.
User name in authen-start message	Whether the Authentication-Start packet of an administrator carries a user name: ● Yes: The Authentication-Start packet of an administrator carries a user name. ● No: The Authentication-Start packet of an administrator does not carry a user name.

13.3.4 display hwtacacs-server template verbose

Function

The **display hwtacacs-server template verbose** command displays statistics on HWTACACS authentication, accounting, and authorization.

Format

display hwtacacs-server template *template-name* **verbose**

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

By viewing statistics on HWTACACS authentication, accounting, and authorization, administrators can better understand the interaction between modules, facilitating fault locating and troubleshooting.

You can run the **reset hwtacacs-server statistics** { **all** | **accounting** | **authentication** | **authorization** } command to delete statistics on HWTACACS authentication, accounting, and authorization.

Precautions

In the HWTACACS server template, you can query the relevant statistics only after the IP address of the authentication server, the IP address of the authorization server, or the IP address of the accounting server is configured.

Example

Display statistics on HWTACACS authentication, accounting, and authorization in the HWTACACS server template *test1*.

```
<HUAWEI> display hwtacacs-server template test1 verbose
---[HWTACACS template test1 primary
authentication]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS authen client access request packet number:
0
HWTACACS authen client access response packet number:
0
HWTACACS authen client unknown type number:
0
HWTACACS authen client timeout number: 0
```

```
HWTACACS authen client packet dropped number:
0
HWTACACS authen client access request change password number:
0
HWTACACS authen client access request login number:
0
HWTACACS authen client access request send authentication number:
0
HWTACACS authen client access request send password number:
0
HWTACACS authen client access connect abort number:
0
HWTACACS authen client access connect packet number:
0
HWTACACS authen client access response error number:
0
HWTACACS authen client access response failure number:
0
HWTACACS authen client access response follow number:
0
HWTACACS authen client access response getdata number:
0
HWTACACS authen client access response getpassword number:
0
HWTACACS authen client access response getuser number:
0
HWTACACS authen client access response pass number:
0
HWTACACS authen client access response restart number:
0
HWTACACS authen client malformed access response number:
0
HWTACACS authen client round trip time(s): 0
---[HWTACACS template test1 primary
authorization]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS author client request packet number:
0
HWTACACS author client response packet number:
0
HWTACACS author client timeout number: 0
HWTACACS author client packet dropped number:
0
HWTACACS author client unknown type number:
0
HWTACACS author client request EXEC number:
0
HWTACACS author client request PPP number: 0
HWTACACS author client request VPDN number:
0
HWTACACS author client response error number:
0
HWTACACS author client response EXEC number:
0
HWTACACS author client response PPP number:
0
HWTACACS author client response VPDN number:
0
HWTACACS author client round trip time(s): 0
---[HWTACACS template test1 primary
accounting]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS account client request packet number:
0
HWTACACS account client response packet number:
```

```
0
HWTACACS account client unknown type number:
0
HWTACACS account client timeout number: 0
HWTACACS account client packet dropped number:
0
HWTACACS account client request command level number:
0
HWTACACS account client request connection number:
0
HWTACACS account client request EXEC number:
0
HWTACACS account client request network number:
0
HWTACACS account client request system event number:
0
HWTACACS account client request update number:
0
HWTACACS account client response error number:
0
HWTACACS account client round trip time(s): 0
```

Table 13-37 Description of the **display hwtacacs-server template verbose** command output

Item	Description
HWTACACS template test1 primary authentication	Statistics on the primary authentication server in the HWTACACS server template *test1*. If the secondary and third authentication servers are configured, the relevant statistics are also displayed, including: ● HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up ● HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected ● HWTACACS authen client access request packet number: Number of HWTACACS client authentication request packets ● HWTACACS authen client access response packet number: Number of HWTACACS client authentication response packets ● HWTACACS authen client unknown type number: Number of unknown HWTACACS client authentication messages ● HWTACACS authen client timeout number: Number of HWTACACS client authentication timeouts ● HWTACACS authen client packet dropped number: Number of times that HWTACACS client authentication packets are dropped ● HWTACACS authen client access request change password number: Number of password change requests from an HWTACACS client ● HWTACACS authen client access request login number: Number of HWTACACS client login requests ● HWTACACS authen client access request send authentication number: Number of authentication requests sent by an HWTACACS client ● HWTACACS authen client access request send password number: Number of times that an HWTACACS client sends passwords ● HWTACACS authen client access connect abort number: Number of connection-stop packets sent by an HWTACACS client ● HWTACACS authen client access connect packet number: Number of continuous packets sent by an HWTACACS client ● HWTACACS authen client access response error number: Number of error packets received by an HWTACACS client

Item	Description
	- HWTACACS authen client access response failure number: Number of authentication failure packets received by an HWTACACS client - HWTACACS authen client access response follow number: Number of packets that an HWTACACS client receives from the server for re-authentication - HWTACACS authen client access response getdata number: Number of packets that an HWTACACS client receives from the server for user information - HWTACACS authen client access response getpassword number: Number of packets that an HWTACACS client receives from the server for user password - HWTACACS authen client access response getuser number: Number of packets that an HWTACACS client receives from the server for user name - HWTACACS authen client access response pass number: Number of authentication success packets received by an HWTACACS client - HWTACACS authen client access response restart number: Number of authentication restart packets that an HWTACACS client receives from the server - HWTACACS authen client malformed access response number: Number of invalid response packets received by an HWTACACS client - HWTACACS authen client round trip time(s): Last authentication response time of the HWTACACS server

Item	Description
HWTACACS template test1 primary authorization	Statistics on the primary authorization server in the HWTACACS server template *test1*. If the secondary and third authorization servers are configured, the relevant statistics are also displayed, including: ● HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up ● HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected ● HWTACACS author client request packet number: Number of HWTACACS client authorization request packets ● HWTACACS author client response packet number: Number of HWTACACS client authorization response packets ● HWTACACS author client timeout number: Number of HWTACACS client authorization timeouts ● HWTACACS author client packet dropped number: Number of times that HWTACACS client authorization packets are dropped ● HWTACACS author client unknown type number: Number of unknown authorization packets on an HWTACACS client ● HWTACACS author client request EXEC number: Number of EXEC user request packets authorized by an HWTACACS client ● HWTACACS author client request PPP number: Number of PPP user request packets authorized by an HWTACACS client ● HWTACACS author client request VPDN number: Number of VPDN user request packets authorized by an HWTACACS client ● HWTACACS author client response error number: Number of error authorization response packets received by an HWTACACS client ● HWTACACS author client response EXEC number: Number of authorized EXEC user response packets received by an HWTACACS client ● HWTACACS author client response PPP number: Number of authorized PPP user response packets received by an HWTACACS client ● HWTACACS author client response VPDN number: Number of authorized VPDN user response packets received by an HWTACACS client ● HWTACACS author client round trip time(s): Last authorization response time of the HWTACACS server

Item	Description
HWTACACS template test1 primary accounting	Statistics on the primary accounting server in the HWTACACS server template *test1*. If the secondary and third accounting servers are configured, the relevant statistics are also displayed, including: ● HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up ● HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected ● HWTACACS account client request packet number: Number of HWTACACS client accounting request packets ● HWTACACS account client response packet number: Number of HWTACACS client accounting response packets ● HWTACACS account client unknown type number: Number of unknown HWTACACS client accounting packets ● HWTACACS account client timeout number: Number of HWTACACS client accounting timeouts ● HWTACACS account client packet dropped number: Number of times that HWTACACS client accounting packets are dropped ● HWTACACS account client request command level number: Number of HWTACACS client accounting requests for command line packets ● HWTACACS account client request connection number: Number of HWTACACS client accounting requests for connection ● HWTACACS account client request EXEC number: Number of HWTACACS client accounting requests for EXEC packets ● HWTACACS account client request network number: Number of HWTACACS client accounting requests for Network packets ● HWTACACS account client request system event number: Number of HWTACACS client accounting requests for system event packets ● HWTACACS account client request update number: Number of HWTACACS client accounting requests for update packets ● HWTACACS account client response error number: Number of HWTACACS client accounting requests for error packets

Item	Description
	- HWTACACS account client round trip time(s): Response time of the last accounting packet of the HWTACACS server

13.3.5 hwtacacs enable

Function

The **hwtacacs enable** command enables Huawei Terminal Access Controller Access Control System (HWTACACS).

The **undo hwtacacs enable** command disables HWTACACS.

By default, HWTACACS is enabled.

Format

hwtacacs enable

undo hwtacacs enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To use HWTACACS authentication, authorization, or accounting, run the **hwtacacs enable** command to enable the HWTACACS function.

Precautions

If the **undo hwtacacs enable** command is run when a user is performing HWTACACS authentication, authorization, or accounting, the command does not take effect.

Example

Disable HWTACACS.

```
<HUAWEI> system-view
[HUAWEI] undo hwtacacs enable
```

13.3.6 hwtacacs-server

Function

The **hwtacacs-server** command applies an HWTACACS server template to a domain.

The **undo hwtacacs-server** command deletes an HWTACACS server template from a domain.

By default, no HWTACACS server template is applied to a domain.

Format

hwtacacs-server *template-name*

undo hwtacacs-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform HWTACACS authentication, authorization, and accounting for users in a domain, configure an HWTACACS server template in the domain. After the HWTACACS server template is configured in the domain, the configuration in the HWTACACS server template takes effect.

Prerequisites

An HWTACACS server template has been created by using the **hwtacacs-server template** command.

Example

Apply the HWTACACS server template **tacacs1** to the domain **tacacs1**.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template tacacs1
[HUAWEI-hwtacacs-tacacs1] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain tacacs1
[HUAWEI-aaa-domain-tacacs1] hwtacacs-server tacacs1
```

13.3.7 hwtacacs-server accounting

Function

The **hwtacacs-server accounting** command configures an HWTACACS accounting server.

The **undo hwtacacs-server accounting** command cancels the configuration.

By default, no HWTACACS accounting server is configured.

Format

hwtacacs-server accounting { *ipv4-address* | *ipv6-address* } [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third** | **fourth**]

undo hwtacacs-server accounting [**secondary** | **third** | **fourth**] { **ip-address** | **ipv6-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS accounting server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of an HWTACACS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS accounting server.	The value is an integer that ranges from 1 to 65535. The default value is 49.
public-net	Indicates that the HWTACACS accounting server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS accounting server is bound to.	The value must be an existing VPN instance name.

Parameter	Description	Value
secondary	Configures the second HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-
third	Specifies the third HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-
fourth	Specifies the fourth HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-
ip-address	Deletes the primary HWTACACS accounting server with a specified IPv4 address. If the secondary server is specified, the secondary HWTACACS accounting server with the specified IPv4 address is deleted.	-
ipv6-address	Deletes the primary HWTACACS accounting server with a specified IPv6 address. If the secondary server is specified, the secondary HWTACACS accounting server with the specified IPv4 address is deleted.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device does not support local accounting; therefore, you need to configure an HWTACACS accounting server to perform accounting. The device sends accounting packets to an HWTACACS accounting server only after the accounting server is specified in an HWTACACS server template.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same IP protocol stack and type (for example, the servers are all IPv4 primary servers), only the latest configuration takes effect.
- IPv4 and IPv6 servers are configured at the same time in the same HWTACACS server template. The order for selecting servers is as follows: primary IPv4 server -> primary IPv6 server -> second secondary IPv4 server -> second secondary IPv6 server -> third secondary IPv4 server -> third secondary IPv6 server -> fourth secondary IPv4 server -> fourth secondary IPv6 server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Configure the primary HWTACACS accounting server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server accounting 10.163.155.12 52
```

13.3.8 hwtacacs-server accounting-stop-packet resend

Function

The **hwtacacs-server accounting-stop-packet resend** command enables or disables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted each time.

By default, 100 accounting-stop packets can be retransmitted each time.

Format

hwtacacs-server accounting-stop-packet resend { **disable** | **enable** *number* }

Parameters

Parameter	Description	Value
disable	Disables the retransmission of accounting-stop packets.	-
enable *number*	Enables the retransmission of accounting-stop packets, and specifies the number of packets that can be retransmitted each time.	The value is an integer that ranges from 1 to 300.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a user goes offline, the device sends an accounting-stop packet to an accounting server. After the accounting server receives the accounting-stop packet, it stops accounting for the user. If the accounting server does not receive the accounting-stop packet because of network faults, it continues to perform accounting for the user. As a result, the user is charged incorrectly. To solve this problem, configure the device to send accounting-stop packets multiple times.

Precautions

- If **disable** is configured, an accounting-stop packet is transmitted only once even when packet transmission fails.

- If **enable** *number* is configured, *number* specifies the number of accounting-stop packets that can be retransmitted each time when the device does not receive any response packet from the HWTACACS server or fails to receive the response packet.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted each time to 50.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server accounting-stop-packet resend enable 50
```

13.3.9 hwtacacs-server authentication

Function

The **hwtacacs-server authentication** command configures the HWTACACS authentication server.

The **undo hwtacacs-server authentication** command deletes configurations of the HWTACACS authentication server.

By default, no HWTACACS authentication server is configured.

Format

hwtacacs-server authentication { *ipv4-address* | *ipv6-address* } [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third** | **fourth**]

undo hwtacacs-server authentication [**secondary** | **third** | **fourth**] { **ip-address** | **ipv6-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authentication server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of an HWTACACS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS authentication server.	The value is an integer that ranges from 1 to 65535. The default value is 49.

Parameter	Description	Value
public-net	Indicates that the HWTACACS authentication server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS authentication server is bound to.	The value must be an existing VPN instance name.
secondary	Configures the second HWTACACS authentication server as the secondary server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-
third	Configures the third HWTACACS authentication server as the secondary server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-
fourth	Specifies the fourth HWTACACS authentication server as the secondary server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-
ip-address	Deletes the primary HWTACACS authentication server with a specified IPv4 address. If the secondary server is specified, the secondary HWTACACS authentication server with the specified IPv4 address is deleted.	-

Parameter	Description	Value
ipv6-address	Deletes the primary HWTACACS authentication server with a specified IPv6 address. If the secondary server is specified, the secondary HWTACACS authentication server with the specified IPv6 address is deleted.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users in HWTACACS mode, you must configure the HWTACACS authentication server. When both the primary and secondary authentication servers are configured, the device sends an authentication request packet to the secondary authentication server in any of the following situations:

- The device fails to send a request packet to the primary authentication server.
- If the device does not receive any authentication response packet from the primary server:
- The primary authentication server requires re-authentication.
- The primary authentication server considers that the received authentication request packet is incorrect.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same IP protocol stack and type (for example, the servers are all IPv4 primary servers), only the latest configuration takes effect.
- IPv4 and IPv6 servers are configured at the same time in the same HWTACACS server template. The order for selecting servers is as follows: primary IPv4 server -> primary IPv6 server -> second secondary IPv4 server -> second secondary IPv6 server -> third secondary IPv4 server -> third

secondary IPv6 server -> fourth secondary IPv4 server -> fourth secondary IPv6 server.

- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Configure the primary HWTACACS authentication server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server authentication 10.163.155.12 49
```

13.3.10 hwtacacs-server authentication user-name in-authentication-start

Function

The **hwtacacs-server authentication user-name in-authentication-start** command configures a user name to be carried in the Authentication Start packet of an administrator.

The **undo hwtacacs-server authentication user-name in-authentication-start** command configures a user name not to be carried in the Authentication Start packet of an administrator.

By default, the Authentication Start packet of an administrator does not carry a user name.

Format

hwtacacs-server authentication user-name in-authentication-start

undo hwtacacs-server authentication user-name in-authentication-start

Parameters

None

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the Authentication Start packet sent by the device to the HWTACACS server does not carry a user name. When the device connects to a specific server, the server identifies whether a user is an administrator based on the user name carried in the Authentication Start packet received from the device. To configure a user name to be carried in the Authentication Start packet of an administrator, run the **hwtacacs-server authentication user-name in-authentication-start** command.

Precautions

- This function takes effect only for administrators.
- This command does not take effect if it is independently executed. It takes effect only after the **undo hwtacacs-server user-name domain-included** command is executed.

Example

Configure a user name to be carried in the Authentication Start packet of an administrator.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server authentication user-name in-authentication-start
```

13.3.11 hwtacacs-server authorization

Function

The **hwtacacs-server authorization** command configures the HWTACACS authorization server.

The **undo hwtacacs-server authorization** command deletes configurations of the HWTACACS authorization server.

By default, no HWTACACS authorization server is configured.

Format

hwtacacs-server authorization { *ipv4-address* | *ipv6-address* } [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third** | **fourth**]

undo hwtacacs-server authorization [**secondary** | **third** | **fourth**] { **ip-address** | **ipv6-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authorization server.	The value is in dotted decimal notation. It must be a valid unicast address.
ipv6-address	Specifies the IPv6 address of an HWTACACS authorization server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS authorization server.	The value is an integer that ranges from 1 to 65535. The default value is 49.
public-net	Indicates that the HWTACACS authorization server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS authorization server is bound to.	The value must be an existing VPN instance name.
secondary	Configures the second HWTACACS authorization server as the secondary server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-
third	Configures the third HWTACACS authorization server as the secondary server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-

Parameter	Description	Value
fourth	Specifies the fourth HWTACACS authorization server as the secondary server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-
ip-address	Deletes the primary HWTACACS authorization server with a specified IPv4 address. If the secondary server is specified, the secondary HWTACACS authorization server with the specified IPv4 address is deleted.	-
ipv6-address	Deletes the primary HWTACACS authorization server with a specified IPv6 address. If the secondary server is specified, the secondary HWTACACS authorization server with the specified IPv6 address is deleted.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authorize users in HWTACACS mode, you must configure the HWTACACS authorization server.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.

- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same IP protocol stack and type (for example, the servers are all IPv4 primary servers), only the latest configuration takes effect.
- IPv4 and IPv6 servers are configured at the same time in the same HWTACACS server template. The order for selecting servers is as follows: primary IPv4 server -> primary IPv6 server -> second secondary IPv4 server -> second secondary IPv6 server -> third secondary IPv4 server -> third secondary IPv6 server -> fourth secondary IPv4 server -> fourth secondary IPv6 server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Configure the primary HWTACACS authorization server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server authorization 10.163.155.12 49
```

13.3.12 hwtacacs-server shared-key

Function

The **hwtacacs-server shared-key** command sets a shared key for an HWTACACS server.

The **undo hwtacacs-server shared-key** command cancels the configuration.

By default, the HWTACACS server is not configured with any shared key.

Format

hwtacacs-server shared-key cipher *key-string*

undo hwtacacs-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-
key-string	Specifies a shared key.	The value is a string of case-sensitive characters. It cannot contain question marks (?) and spaces. The key is processed as cipher text no matter whether the **cipher** keyword is specified. The *key-string* may be a plain text consisting of 1 to 255 characters or a cipher text consisting of 20 to 392 characters.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with an HWTACACS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. The device and HWTACACS server must use the same key to ensure their validity in the authentication.

Precautions

For security purposes, it is recommended that the password contains at least two types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least 8 characters.

You can modify this configuration only when the HWTACACS server template is not in use.

During the configuration of this command, the weak password verification function is added to check whether a password is weak. If the password is weak, the command fails to be executed.

Example

Set the shared key of the HWTACACS server to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server shared-key cipher YsHsjx_202206
```

13.3.13 hwtacacs-server source-ip

Function

The **hwtacacs-server source-ip** command specifies the source IPv4 address used by a device to communicate with an HWTACACS server.

The **undo hwtacacs-server source-ip** command cancels the configuration.

By default, the device uses the IPv4 address of the actual outbound interface as the source IPv4 address encapsulated in HWTACACS packets.

Format

hwtacacs-server source-ip *ip-address*

hwtacacs-server source-ip source-loopback *interface-number*

hwtacacs-server source-ip source-vlanif *interface-number*

undo hwtacacs-server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address for communication between the device and HWTACACS server.	The value is a valid unicast address in dotted decimal notation.
source-loopback *interface-number*	Specifies the IPv4 address of the loopback interface as the source IPv4 address for communication between the device and HWTACACS server.	The loopback interface must already exist.
source-vlanif *interface-number*	Specifies the IPv4 address of the VLANIF interface as the source IPv4 address for communication between the device and HWTACACS server.	The VLANIF interface must already exist.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

You can configure all HWTACACS packets sent by the device to use the same source IPv4 address. In this way, an HWTACACS server uses only one IPv4 address to communicate with the device.

If an interface connecting the device to a server has multiple IP addresses configured and can communicate with the server only through some of these IP addresses, one IP address among these reachable IP addresses needs to be specified as the source IP address based on the routing table to ensure that the device can communicate with the server.

If you run this command multiple times, only the latest configuration takes effect.

Example

Specify the source IPv4 address 10.1.1.1 for communication between the device and HWTACACS server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server source-ip 10.1.1.1
```

13.3.14 hwtacacs-server source-ipv6

Function

The **hwtacacs-server source-ipv6** command specifies the source IPv6 address used by a device to communicate with an HWTACACS server.

The **undo hwtacacs-server source-ipv6** command cancels the configuration.

By default, the device uses the IPv6 address of the actual outbound interface as the source IPv6 address encapsulated in HWTACACS packets.

Format

hwtacacs-server source-ipv6 *ipv6-address*

hwtacacs-server source-ipv6 source-loopback *interface-number*

hwtacacs-server source-ipv6 source-vlanif *interface-number*

undo hwtacacs-server source-ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address for communicating with the HWTACACS server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
source-loopback *interface-number*	Specifies the IPv6 address of the loopback interface as the source IPv6 address for communicating with the HWTACACS server.	The loopback interface must already exist.
source-vlanif *interface-number*	Specifies the IPv6 address of the VLANIF interface as the source IPv6 address for communicating with the HWTACACS server.	The VLANIF interface must already exist.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

After you specify the source IPv6 address in HWTACACS packets, the device uses this IPv6 address to communicate with the HWTACACS server.

If an interface connecting the device to a server has multiple IP addresses configured and can communicate with the server only through some of these IP addresses, one IP address among these reachable IP addresses needs to be specified as the source IP address based on the routing table to ensure that the device can communicate with the server.

If you run this command multiple times, only the latest configuration takes effect.

Example

Specify the source IPv6 address fc00::1 in HWTACACS packets.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server source-ipv6 fc00::1
```

13.3.15 hwtacacs-server template

Function

The **hwtacacs-server template** command creates an HWTACACS server template and enters the HWTACACS server template view.

The **undo hwtacacs-server template** command deletes an HWTACACS server template.

By default, no HWTACACS server template is configured.

Format

hwtacacs-server template *template-name*

undo hwtacacs-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The value is a string of 1 to 32 case-sensitive characters. The name contains only letters, digits (0-9), dots (.), underscores (_) and hyphens (-), and a combination of the above characters. The value cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can perform HWTACACS configurations, such as the configuration of authentication servers, authorization servers, accounting servers, and shared key, only after an HWTACACS server template is created.

Follow-up Procedure

Configure an authentication server, accounting server, and shared key in the HWTACACS server template view, and run the **hwtacacs-server** command in the domain view to apply the HWTACACS server template.

Precautions

You can delete a template only when the template is not in use.

Example

Create an HWTACACS server template **template1** and enter the HWTACACS server template view.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1]
```

13.3.16 hwtacacs-server timer quiet

Function

The **hwtacacs-server timer quiet** command sets the quiet interval before the primary server reverts to the active state.

The **undo hwtacacs-server timer quiet** command restores the default quiet interval before the primary server reverts to the active state.

By default, the quiet interval before the primary HWTACACS server reverts to the active state is 5 minutes.

Format

hwtacacs-server timer quiet *interval*

undo hwtacacs-server timer quiet

Parameters

Parameter	Description	Value
interval	Specifies the quiet interval before the primary server reverts to the active state.	The value is an integer ranging from 0 to 255, in minutes.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the primary server is unavailable, the device automatically switches services to the standby server and sends packets to the standby server. After the quiet interval before the primary server reverts to the active state expires, the device attempts to establish a connection with the primary server.

- If the primary server is still unavailable, the device continues to send packets to the standby server until the next interval expires. Such a process repeats.
- If the primary server is available, the device switches services to the primary server and sends packets to the primary server.

The quiet interval before the primary server reverts to the active state ensures that the primary server can be restored immediately and reduces the number of detection times during the switchover.

The default value is recommended.

Precautions

When the quiet interval of the active server is set to 0, if the active server fails, the device sends packets to the standby server. When the active server is recovered, the device does not connect to the active server, but still sends packets to the standby server until the standby server fails.

When you run the **hwtacacs-server timer quiet** command to change the quiet interval before the primary server reverts to the active state, the device does not check whether the HWTACACS server template is in use.

Example

Set the quiet interval before the primary server reverts to the active state to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1] hwtacacs-server timer quiet 3
```

13.3.17 hwtacacs-server timer response-timeout

Function

The **hwtacacs-server timer response-timeout** command sets the response timeout interval of an HWTACACS server.

The **undo hwtacacs-server timer response-timeout** command restores the default response timeout interval of an HWTACACS server.

By default, the response timeout interval for an HWTACACS server is 5 seconds.

Format

hwtacacs-server timer response-timeout *interval*

undo hwtacacs-server timer response-timeout

Parameters

Parameter	Description	Value
interval	Specifies the response timeout interval of an HWTACACS server.	The value is an integer ranging from 1 to 300, in seconds.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the device sends a request packet to the HWTACACS server, if the device does not receive any response packet from the server within the specified response timeout interval:

- If only one HWTACACS server is configured, the device does not retransmit the request to this server.
- If both active/standby HWTACACS servers are available and the TCP link between them works normally, the device retransmits the request to the standby server after timeout. If the TCP link is broken during the timeout interval, the device immediately retransmits the request to the standby server.

This improves reliability of HWTACACS authentication, authorization, and accounting.

The default value is recommended.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

Example

Set the response timeout interval of an HWTACACS server to 30s.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server timer response-timeout 30
```

13.3.18 hwtacacs-server traffic-unit

Function

The **hwtacacs-server traffic-unit** command sets the traffic unit used by an HWTACACS server.

The **undo hwtacacs-server traffic-unit** command restores the default traffic unit used by the HWTACACS server.

By default, the traffic unit is byte on the device.

Format

hwtacacs-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

undo hwtacacs-server traffic-unit

Parameters

Parameter	Description	Value
byte	Indicates that the traffic unit is byte.	-
kbyte	Indicates that the traffic unit is KByte.	-
mbyte	Indicates that the traffic unit is MByte.	-
gbyte	Indicates that the traffic unit is GByte.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Different HWTACACS servers may use different traffic units; therefore, you need to set the traffic unit for each HWTACACS server group on the device and the traffic unit must be the same as that on the HWTACACS server.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

Example

Set the traffic unit used by an HWTACACS server to KByte.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1] hwtacacs-server traffic-unit kbyte
```

13.3.19 hwtacacs-server user-name domain-included

Function

The **hwtacacs-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in HWTACACS packets to be sent to an HWTACACS server.

The **hwtacacs-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the HWTACACS server.

The **undo hwtacacs-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

By default, the device encapsulates the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

By default, the device does not modify the user name entered by the user in the packets sent to the HWTACACS server.

Format

hwtacacs-server user-name domain-included

hwtacacs-server user-name original

undo hwtacacs-server user-name domain-included

Parameters

None

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter.

If the HWTACACS server does not accept the user name with the domain name, run the **undo hwtacacs-server user-name domain-included** command to delete the domain name from the user name.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

If the user names in the HWTACACS packets sent from the device to HWTACACS server contain domain names, ensure that the total length of a user name (user name + domain name delimiter + domain name) is not longer than 64 characters; otherwise, the user name cannot be contained in HWTACACS packets. As a result, authentication will fail.

Example

Configure the device to encapsulate the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template template1
[HUAWEI-hwtacacs-template1] hwtacacs-server user-name domain-included
```

13.3.20 hwtacacs-user change-password hwtacacs-server

Function

The **hwtacacs-user change-password hwtacacs-server** command enables the device to change the passwords saved on the HWTACACS server.

Format

hwtacacs-user change-password hwtacacs-server *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To change the password saved on the HWTACACS server, users can run the **hwtacacs-user change-password hwtacacs-server** command on the device. You do not need to change the configuration on the HWTACACS server.

Precautions

- Users are HWTACACS authenticated and the HWTACACS server template is configured.
- Users can run this command to change the passwords only when the user names and passwords saved on the HWTACACS do not expire. When a user whose password has expired logs in to the device, the HWTACACS server does not allow the user to change the password and displays a message indicating that the authentication fails.

- The system wait period is 30 seconds. If the TACACS server does not receive the user name, new password, or confirmed password from the user within such a period, it terminates the password change process.
- Users can also press **Ctrl+C** to cancel password change.
- HWTACACS users who pass AAA authentication can use the **hwtacacs-user change-password hwtacacs-server** command to change the passwords before the passwords expire. If a user needs to run this command to change the passwords of other users, the user must have the administrative rights.

Example

Enable the user that passes HWTACACS authentication to change the password.

```
<HUAWEI> hwtacacs-user change-password hwtacacs-server example
Username:cj@example
Old Password:
New Password:
Re-enter New password:
Info: The password has been changed successfully.
```

13.3.21 reset hwtacacs-server accounting-stop-packet

Function

The **reset hwtacacs-server accounting-stop-packet** command clears statistics on Accounting Stop packets.

Format

reset hwtacacs-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears the statistics about all accounting-stop packets.	-
ip *ipv4-address*	Clears the statistics about the Accounting-Stop packets sent by the HWTACACS server with a specified IPv4 address.	The value is in dotted decimal notation.
ip *ipv6-address*	Clears the statistics about the Accounting-Stop packets sent by the HWTACACS server with a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

Statistics cannot be restored once being cleared.

Example

Clear statistics on all Accounting Stop packets.

```
<HUAWEI> reset hwtacacs-server accounting-stop-packet all
```

13.3.22 reset hwtacacs-server statistics

Function

The **reset hwtacacs-server statistics** command clears the statistics on HWTACACS authentication, accounting, and authorization.

Format

reset hwtacacs-server statistics { **all** | **accounting** | **authentication** | **authorization** }

Parameters

Parameter	Description	Value
all	Clears all the statistics.	-
accounting	Clears the statistics on HWTACACS accounting.	-
authentication	Clears the statistics on HWTACACS authentication.	-
authorization	Clears the statistics on HWTACACS authorization.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If statistics about HWTACACS authentication, accounting, and authorization need to be collected in a specified period of time, you must clear the original statistics first.

Precautions

- After the **reset hwtacacs-server statistics** command is run, all the statistics about HWTACACS authentication, accounting, and authorization is cleared. In addition, the statistics cannot be restored once being cleared. Therefore, exercise caution when you decide to run this command.
- You can run the **display hwtacacs-server template** *template-name* **verbose** command to check statistics about HWTACACS authentication, accounting, and authorization in the specified server template.

Example

Clear all the statistics.

```
<HUAWEI> reset hwtacacs-server statistics all
```

13.4 HACA Configuration Commands

13.4.1 Command Support

Only the following switch models support HACA:

S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H and S6720S-S

13.4.2 display haca-server accounting-stop-packet all

Function

The **display haca-server accounting-stop-packet all** command displays information about all accounting-stop packets on the HACA server.

Format

display haca-server accounting-stop-packet all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display haca-server accounting-stop-packet all** command output helps you check configurations or locate HACA server faults.

Example

View information about all accounting-stop packets on the HACA server.

```
<HUAWEI> display haca-server accounting-stop-packet all
------------------------------------------------------------------------------
 Time Stamp  Resend Times  Session Time
Username
 ------------------------------------------------------------------------------
 3245884970  32           49           123
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-38 Description of the **display haca-server accounting-stop-packet all** command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.
Resend Times	Number of times that accounting-stop packets have been retransmitted.
Session Time	Session time, in seconds.
Username	User name.

13.4.3 display haca-server configuration

Function

The **display haca-server configuration** command displays the HACA server template configuration.

Format

display haca-server configuration [**template** *template-name*]

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of an HACA server template. If this parameter is not specified, the configurations of all HACA server templates are displayed.	The HACA server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an HACA server template is configured or during HACA troubleshooting, you can run this command to check whether the HACA server template is correctly configured.

Example

Display the HACA server template configuration.

```
<HUAWEI> display haca-server configuration
 ------------------------------------------------------------------------
 HACA-server template name : default
 HACA-server server-address dynamic : Enable
 HACA-server server-ip-address(port) : 1.2.3.4(50300)
 HACA-server pki-realm-name : default
 HACA-server status : IDLE
 HACA-server escape-state : UP
 HACA-server down-delay-interval in use(sec) : -
 HACA-server heart-beat-interval in use(min) : -
 HACA-server reconnection-interval in use(min) : -
 HACA-server register-sync-interval in use(min) : -
 HACA-bak-server server-ip-address(port) : -(0)
 HACA-bak-server pki-realm-name : -
 HACA-bak-server status : -
 HACA-bak-server escape-state : -
 HACA-bak-server down-delay-interval in use(sec) : -
 HACA-bak-server heart-beat-interval in use(min) : -
 HACA-bak-server reconnection-interval in use(min) : -
 HACA-bak-server register-sync-interval in use(min) : -
 Configured source-ip-address : -
 Configured down-delay-interval(sec) : 30
 Configured response-timeout-interval(sec) : 5
 Configured domain-included : ORIGINAL
 Configured heart-beat-interval(min) : 5
 Configured reconnection-interval(min) : 1
 Configured user-syn-interval(min) : 10
 Configured register-sync-interval(min) : 15
```

```
Configured accounting-stop-packet resend : 3
------------------------------------------------------------------------------
```

Table 13-39 Description of the **display haca-server configuration** command output

Item	Description
HACA-server template name	Name of an HACA server template. To configure this parameter, run the **haca-server template** command.
HACA-server server-address dynamic	Whether the HACA server dynamic address function to support dynamic IP address switching is enabled. ● Enable ● Disable
HACA-server server-ip-address(port)	IP address and port number of the HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-server pki-realm-name	PKI realm name of the HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-server Status	Status of the HACA server: ● IDLE: idle state ● INIT: initial state ● UP: Up state ● REGISTER: registration state ● DOWN: Down state
HACA-server escape-state	HACA server escape state: ● UP: The escape path will not be used. ● ESCAPE: The escape path is being prepared. ● -: The server is in initial state, and the escape path will not be used.
HACA-server down-delay-interval in use(sec)	Delay after which the HACA server in use is disconnected, in seconds. To configure this parameter, run the **haca-server timer down-delay** command.

Item	Description
HACA-server heart-beat-interval in use(min)	Interval at which heartbeat packets of the HACA server in use are sent, in minutes. To configure this parameter, run the **haca-server timer heart-beat** command.
HACA-server reconnection-interval in use(min)	Interval at which the HACA server in use is reconnected, in minutes. To configure this parameter, run the **haca-server timer reconnection**.
HACA-server register-sync-interval in use(min)	Interval at which registration synchronization packets of the HACA server in use are sent, in minutes. To configure this parameter, run the **haca-server timer register-sync** command.
HACA-bak-server server-ip-address(port)	IP address and port number of the secondary HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-bak-server pki-realm-name	PKI realm name of the secondary HACA server. To configure this parameter, run the **haca-server server-address** command.
HACA-bak-server Status	Status of the secondary HACA server: ● IDLE: idle state ● INIT: initial state ● UP: Up state ● REGISTER: registration state ● DOWN: Down state
HACA-bak-server escape-state	Escape state of the secondary HACA server: ● UP: The escape path will not be used. ● ESCAPE: The escape path is being prepared. ● -: The server is in initial state, and the escape path will not be used.

Item	Description
HACA-bak-server down-delay-interval in use(sec)	Delay after which the secondary HACA server in use is disconnected, in seconds. To configure this parameter, run the **haca-server timer down-delay** command.
HACA-bak-server heart-beat-interval in use(min)	Interval at which heartbeat packets of the secondary HACA server in use are sent, in minutes. To configure this parameter, run the **haca-server timer heart-beat** command.
HACA-bak-server reconnection-interval in use(min)	Interval at which the secondary HACA server in use is reconnected, in minutes. To configure this parameter, run the **haca-server timer reconnection**.
HACA-bak-server register-sync-interval in use(min)	Interval at which registration synchronization packets of the secondary HACA server are sent, in minutes. To configure this parameter, run the **haca-server timer register-sync** command.
Configured source-ip-address	Source IP address of HACA packets. To configure this parameter, run the **haca-server source-ip** command.
Configured down-delay-interval(sec) :	Delay after which an HACA server is disconnected, in seconds. To configure this parameter, run the **haca-server timer down-delay** command.
Configured response-timeout-interval(sec)	HACA packet response timeout period, in seconds. To configure this parameter, run the **haca-server timer response-timeout** command.

Item	Description
Configured domain-included	HACA user name format (whether a user name contains a domain name): - YES: The user name contains a domain name. - NO: The user name does not contain a domain name. - ORIGINAL: The device does not modify the user name entered by the user. To configure this parameter, run the **haca-server user-name** command.
Configured heart-beat-interval(min)	Interval at which HACA heartbeat packets are sent, in minutes. To configure this parameter, run the **haca-server timer heart-beat** command.
Configured reconnection-interval(min)	Interval at which an HACA server is reconnected, in minutes. To configure this parameter, run the **haca-server timer reconnection** command.
Configured user-syn-interval(min)	Interval at which HACA user information is synchronized, in minutes. To configure this parameter, run the **haca-server timer user-syn** command.
Configured register-sync-interval(min)	Interval at which registration synchronization packets are sent, in minutes. To configure this parameter, run the **haca-server timer register-sync** command.
Configured accounting-stop-packet resend	Number of times that HACA Accounting-Stop packets are retransmitted. To set this parameter, run the **haca-server accounting-stop-packet resend** command.

13.4.4 display haca-server statistics

Function

The **display haca-server statistics** command displays HACA packet statistics.

Format

display haca-server statistics { **all** | **message** | **packet** [**authentication** | **authorization** | **accounting** | **cut-notify** | **cut-request** | **register** | **user-syn**] } [**template** *template-name*]

Parameters

Parameter	Description	Value
all	Displays statistics about all packets.	-
message	Displays statistics about messages.	-
packet	Displays statistics about the specified type of packets.	-
authentication	Displays statistics about authentication packets.	-
authorization	Displays statistics about authorization packets.	-
accounting	Displays statistics about accounting packet.	-
cut-notify	Displays statistics about logout notification packets.	-
cut-request	Displays statistics about logout request packets.	-
register	Displays statistics about registration packets.	-
user-syn	Displays statistics about user synchronization packets.	-
template *template-name*	Displays packet statistics about the specified HACA server template.	The HACA server template must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

During fault location, you can run this command to view statistics about HACA packets.

Example

Display HACA packet statistics.

```
<HUAWEI> display haca-server statistics all
--------------------------------------------------------------
Haca-server Template haca Statistics:
--------------------------------------------------------------
Authen_Request_Messages                              = 0
Authen_Accept_Messages                               = 0
Authen_Reject_Messages                               = 0
Author_Request_Messages                              = 0
Author_Accept_Messages                               = 0
Author_Reject_Messages                               = 0
Coa_Request_Messages                                 = 0
Coa_Accept_Messages                                  = 0
Coa_Reject_Messages                                  = 0
Account_Start_Messages                               = 0
Account_RT_Messages                                  = 0
Account_Stop_Messages                                = 0
Account_StartAck_Messages                            = 0
Account_RTAck_Messages                               = 0
Account_StopAck_Messages                             = 0
Account_StartAckFail_Messages                        = 0
Account_RTAckFail_Messages                           = 0
Account_StopAckFail_Messages                         = 0
UserSyn_Request_To_Server_Messages                   = 0
UserSyn_Response_From_Server_Messages                = 0
UserSyn_Request_From_Server_Messages                 = 0
UserSyn_Response_To_Server_Messages                  = 0
Cut_Request_Messages                                 = 0
Cut_Response_Messages                                = 0
Cut_Notify_Messages                                  = 0
Send_to_HacaServer_RegRequest_Packets                = 0
Received_from_HacaServer_RegResponse_Packets         = 0
Error_Send_to_HacaServer_RegRequest_Packets          = 0
Error_Received_from_HacaServer_RegResponse_Packets   = 0
Send_to_HacaServer_AuthenRequest_Packets             = 0
Received_from_HacaServer_AuthenAccept_Packets        = 0
Received_from_HacaServer_AuthenReject_Packets        = 0
Error_Send_to_HacaServer_AuthenRequest_Packets       = 0
Error_Received_from_HacaServer_AuthenAccept_Packets  = 0
Error_Received_from_HacaServer_AuthenReject_Packets  = 0
Received_from_HacaServer_AuthorRequest_Packets       = 0
Send_to_HacaServer_AuthorAccept_Packets              = 0
Send_to_HacaServer_AuthorReject_Packets              = 0
Error_Received_from_HacaServer_AuthorRequest_Packets = 0
Error_Send_to_HacaServer_AuthorAccept_Packets        = 0
Error_Send_to_HacaServer_AuthorReject_Packets        = 0
Received_from_HacaServer_CoaRequest_Packets          = 0
Send_to_HacaServer_CoaAccept_Packets                 = 0
Send_to_HacaServer_CoaReject_Packets                 = 0
Error_Received_from_HacaServer_CoaRequest_Packets    = 0
Error_Send_to_HacaServer_CoaAccept_Packets           = 0
Error_Send_to_HacaServer_CoaReject_Packets           = 0
Received_from_HacaServer_AcctSucc_Packets            = 0
Send_to_HacaServer_AcctSend_Packets                  = 0
Error_Received_from_HacaServer_AcctFail_Packets      = 0
```

```
Error_Send_to_HacaServer_AcctSendFail_Packets            = 0
Send_to_HacaServer_UserSynRequest_Packets                = 0
Received_from_HacaServer_UserSynResponse_Packets         = 0
Send_to_HacaServer_UserSynRespons_Packets                = 0
Received_from_HacaServer_UserSynRequest_Packets          = 0
Error_Send_to_HacaServer_UserSynRequest_Packets          = 0
Error_Received_from_HacaServer_UserSynResponse_Packets   = 0
Error_Send_to_HacaServer_UserSynRespons_Packets          = 0
Error_Received_from_HacaServer_UserSynRequest_Packets    = 0
Send_to_HacaServer_CutNotify_Packets                     = 0
Error_Send_to_HacaServer_CutNotify_Packets               = 0
Received_from_HacaServer_CutRequest_Packets              = 0
Send_to_HacaServer_CutResponse_Packets                   = 0
Error_Received_from_HacaServer_CutRequest_Packets        = 0
Error_Send_to_HacaServer_CutResponse_Packets             = 0
----------------------------------------------------------------
```

Table 13-40 Description of the **display haca-server statistics** command output

Item	Description
Haca-server Template haca Statistics	Statistics about the HACA server template haca.
Authen_Request_Messages	Statistics about authentication request messages.
Authen_Accept_Messages	Statistics about access-accept messages.
Authen_Reject_Messages	Statistics about access-reject messages.
Author_Request_Messages	Statistics about authorization request messages.
Author_Accept_Messages	Statistics about authorization-accept messages.
Author_Reject_Messages	Statistics about authorization-reject messages.
Coa_Request_Messages	Statistics about CoA request messages.
Coa_Accept_Messages	Statistics about CoA-accept messages.
Coa_Reject_Messages	Statistics about CoA-reject messages.
Account_Start_Messages	Statistics about accounting-start request messages.
Account_RT_Messages	Statistics about real-time accounting request messages.
Account_Stop_Messages	Statistics about accounting-stop request messages.
Account_StartAck_Messages	Statistics about accounting-start response success messages.

Item	Description
Account_RTAck_Messages	Statistics about real-time accounting response success messages.
Account_StopAck_Messages	Statistics about accounting-stop response success messages.
Account_StartAckFail_Messages	Statistics about accounting-start response failure messages.
Account_RTAckFail_Messages	Statistics about real-time accounting response failure messages.
Account_StopAckFail_Messages	Statistics about accounting-stop response failure messages.
UserSyn_Request_To_Server_Messages	Statistics about user synchronization request messages sent to the HACA server.
UserSyn_Response_From_Server_Messages	Statistics about user synchronization response messages received from the HACA server.
UserSyn_Request_From_Server_Messages	Statistics about user synchronization request messages received from the HACA server.
UserSyn_Response_To_Server_Messages	Statistics about user synchronization response messages sent to the HACA server.
Cut_Request_Messages	Statistics about logout request messages.
Cut_Response_Messages	Statistics about logout response messages.
Cut_Notify_Messages	Statistics about logout notification messages.
Send_to_HacaServer_RegRequest_Packets	Statistics about registration request messages sent to the HACA server.
Received_from_HacaServer_RegResponse_Packets	Statistics about registration response messages received from the HACA server.
Error_Send_to_HacaServer_RegRequest_Packets	Statistics about error registration request messages sent to the HACA server.
Error_Received_from_HacaServer_RegResponse_Packets	Statistics about error registration response messages received from the HACA server.
Send_to_HacaServer_AuthenRequest_Packets	Statistics about authentication request messages sent to the HACA server.
Received_from_HacaServer_AuthenAccept_Packets	Statistics about authentication response messages received from the HACA server.

Item	Description
Received_from_HacaServer_AuthenReject_Packets	Statistics about access-reject messages received from the HACA server.
Error_Send_to_HacaServer_AuthenRequest_Packets	Statistics about error authentication request messages sent to the HACA server.
Error_Received_from_HacaServer_AuthenAccept_Packets	Statistics about error authentication response messages received from the HACA server.
Error_Received_from_HacaServer_AuthenReject_Packets	Statistics about error access-reject messages received from the HACA server.
Received_from_HacaServer_AuthorRequest_Packets	Statistics about authorization request messages received from the HACA server.
Send_to_HacaServer_AuthorAccept_Packets	Statistics about authorization response messages sent to the HACA server.
Send_to_HacaServer_AuthorReject_Packets	Statistics about authorization-reject messages sent to the HACA server.
Error_Received_from_HacaServer_AuthorRequest_Packets	Statistics about error authorization request messages received from the HACA server.
Error_Send_to_HacaServer_AuthorAccept_Packets	Statistics about error authorization response messages sent to the HACA server.
Error_Send_to_HacaServer_AuthorReject_Packets	Statistics about error authorization-reject messages sent to the HACA server.
Received_from_HacaServer_CoaRequest_Packets	Statistics about CoA request messages received from the HACA server.
Send_to_HacaServer_CoaAccept_Packets	Statistics about CoA response messages sent to the HACA server.
Send_to_HacaServer_CoaReject_Packets	Statistics about CoA-reject messages sent to the HACA server.
Error_Received_from_HacaServer_CoaRequest_Packets	Statistics about error CoA request messages received from the HACA server.
Error_Send_to_HacaServer_CoaAccept_Packets	Statistics about error CoA response messages sent to the HACA server.

Item	Description
Error_Send_to_HacaServer_CoaReject_Packets	Statistics about error CoA-reject messages sent to the HACA server.
Received_from_HacaServer_AcctSucc_Packets	Statistics about the received accounting response success messages.
Send_to_HacaServer_AcctSend_Packets	Statistics about the sent accounting request success messages.
Error_Received_from_HacaServer_AcctFail_Packets	Statistics about the received accounting request failure messages.
Error_Send_to_HacaServer_AcctSendFail_Packets	Statistics about the sent accounting request failure messages.
Send_to_HacaServer_UserSynRequest_Packets	Statistics about user synchronization request messages sent to the HACA server.
Received_from_HacaServer_UserSynResponse_Packets	Statistics about user synchronization response messages received from the HACA server.
Send_to_HacaServer_UserSynRespons_Packets	Statistics about user synchronization response messages sent to the HACA server.
Received_from_HacaServer_UserSynRequest_Packets	Statistics about user synchronization request messages received from the HACA server.
Error_Send_to_HacaServer_UserSynRequest_Packets	Statistics about error user synchronization request messages sent to the HACA server.
Error_Received_from_HacaServer_UserSynResponse_Packets	Statistics about error user synchronization response messages received from the HACA server.
Error_Send_to_HacaServer_UserSynRespons_Packets	Statistics about error user synchronization response messages sent to the HACA server.
Error_Received_from_HacaServer_UserSynRequest_Packets	Statistics about error user synchronization request messages received from the HACA server.
Send_to_HacaServer_CutNotify_Packets	Statistics about user logout notification messages sent to the HACA server.

Item	Description
Error_Send_to_HacaServer_CutNotify_Packets	Statistics about error user logout notification messages sent to the HACA server.
Received_from_HacaServer_CutRequest_Packets	Statistics about error user logout request messages received from the HACA server.
Send_to_HacaServer_CutResponse_Packets	Statistics about user logout request messages sent to the HACA server.
Error_Received_from_HacaServer_CutRequest_Packets	Statistics about error user logout request messages received from the HACA server.
Error_Send_to_HacaServer_CutResponse_Packets	Statistics about error user logout response messages sent to the HACA server.

13.4.5 haca enable

Function

The **haca enable** command enables the HACA function.

The **undo haca enable** command disables the HACA function.

By default, HACA is disabled.

Format

haca enable

undo haca enable

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The authentication server is located on the cloud, so packets between the device and server must traverse the NAT device. However, Portal protocol packets cannot traverse the NAT device. HACA implements communication between the device and server, and then Portal authentication can be performed.

If you require HACA authentication, run the **haca enable** command to enable HACA.

Prerequisites

The IP address and port number of the HACA server have been configured using the **haca-server server-address** command.

Example

Enable HACA.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server server-address 10.1.1.1 default
[HUAWEI-haca-haca] haca enable
```

13.4.6 haca-server (AAA domain view)

Function

The **haca-server** command applies an HACA server template to a domain.

The **undo haca-server** command unbinds an HACA server template from a domain.

By default, no HACA server template is configured in a domain.

Format

haca-server *template-name*

undo haca-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HACA server template.	The HACA server template must exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform HACA authentication for users in a domain, apply an HACA server template to the domain. An HACA server template takes effect only after the HACA server template is applied to the domain.

Precautions

An HACA server template has been created by using the **haca-server template** command.

Example

Apply the HACA server template **haca** to the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] haca-server haca
```

13.4.7 haca-server accounting-stop-packet resend

Function

The **haca-server accounting-stop-packet resend** command enables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted.

The **undo haca-server accounting-stop-packet resend** command disables retransmission of accounting-stop packets.

By default, three accounting-stop packets can be retransmitted.

Format

haca-server accounting-stop-packet resend [*resend-times*]

undo haca-server accounting-stop-packet resend

Parameters

Parameter	Description	Value
resend-times	Specifies the number of retransmitted accounting-stop packets.	The value is an integer that ranges from 0 to 300.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Accounting-stop packets cannot be forwarded to an HACA server that is unreachable. You can run the **haca-server accounting-stop-packet resend** command to save the accounting-stop packets in the buffer and send them at the preset intervals until the number of allowed retransmission times is reached or the packets are sent successfully.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted to 50.

```
<HUAWEI> system-view
[HUAWEI] haca-server template test1
[HUAWEI-haca-test1] haca-server accounting-stop-packet resend 50
```

13.4.8 haca-server server-address

Function

The **haca-server server-address** command configures the IP address and port number for the HACA server.

The **undo haca-server server-address** command deletes the IP address and port number configured for the HACA server.

By default, the IP address and port number of the HACA server are not configured on the device.

Format

haca-server server-address *ip-address* [*port*] *pki-realm-name* [**backup**]

undo haca-server server-address [*ip-address* [*port*]] [**backup**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an HACA server.	The value is in dotted decimal notation. It must be a valid unicast address.

Parameter	Description	Value
port	Specifies the port number of an HACA server. If the parameter is not specified, the default value is used.	The value is an integer that ranges from 1 to 65535. The default value is 50300.
pki-realm-name	Specifies the name of a PKI domain.	The value must be an existing PKI domain name. **NOTE** If the specified PKI domain is the default domain, there may be security risks.
backup	Specifies the secondary HACA server.	-

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device needs to be connected to an HACA server for authentication. The HACA server is located on the Internet. Therefore, the device sends authentication packets to the HACA server only after the IP address and port number of the HACA server are specified.

Precautions

When you run the **haca enable** command, the system checks whether there is the primary HACA server. The standby HACA server takes effect only when the primary HACA server is configured.

Example

Configure the IP address of the HACA server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server server-address 10.1.1.1 abc
```

13.4.9 haca-server server-address dynamic

Function

The **haca-server server-address dynamic** command enables the HACA server dynamic address function to support dynamic IP address switching.

The **undo haca-server server-address dynamic** command disables the HACA server dynamic address function.

By default, the HACA server dynamic address function is disabled.

Format

haca-server server-address dynamic [*port*] *pki-realm-name*

undo haca-server server-address [**dynamic** [*port*]]

Parameters

Parameter	Description	Value
port	Specifies the port number of an HACA server. If this parameter is not specified, the default value is used.	The value is an integer that ranges from 1 to 65535. The default port number is 50300.
pki-realm-name	Specifies the name of a PKI realm.	The value must be an existing PKI realm name. **NOTE** If the specified PKI realm is the default realm, there may be security risks.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the iMaster NCE-Campus active/standby scenario, devices establish connections with the HACA server. When the active device is not operational, the HACA server IP address on the device must support dynamic switching so that the standby device can take on the active role and re-establish a connection with the HACA server. In this case, run this command to enable the HACA server dynamic address function to support dynamic IP address switching.

Precautions

In the VRRP hot standby scenario, a PKI realm needs to be created on the backup device to be bound to the HACA server.

The **haca-server server-address** *ip-address* [*port*] *pki-realm-name* [**backup**] and **haca-server server-address dynamic** [*port*] *pki-realm-name* commands are mutually exclusive and cannot be both configured.

Example

Enable the HACA server dynamic address function to support dynamic IP address switching.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server server-address dynamic 50301 default
```

13.4.10 haca-server source-ip

Function

The **haca-server source-ip** command configures a source IP address for the device to communicate with an HACA server.

The **undo haca-server source-ip** restores the default setting.

By default, no source IP address is configured for HACA packets. The device uses the IP address of the actual outbound interface as the source IP address of HACA packets.

Format

haca-server source-ip *ip-address*

undo haca-server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with an HACA server.	The value is in dotted decimal notation. It must be a valid unicast address.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

To communicate with an HACA server, the device sends packets encapsulated with source IP addresses. By default, the device uses the IP addresses of the actual outbound interfaces as the source IP address. This leads to a waste of IP addresses, and complicates the configuration. To simplify the configuration, run the **haca-server source-ip** command to set a same source IP address for all HACA packets. In this way, the HACA server can use only one IP address to communicate with the device.

Example

Set the source IP address for communication between the device and an HACA server to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server source-ip 10.1.1.1
```

13.4.11 haca-server template

Function

The **haca-server template** command creates an HACA server template and displays the HACA server template view.

The **undo haca-server template** command deletes an HACA server template.

By default, no HACA server template is created.

Format

haca-server template *template-name*

undo haca-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HACA server template.	The value is a string of 1 to 32 case-sensitive characters. The name contains only letters, digits (0-9), dots (.), underscores (_) and hyphens (-). It cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure HACA authentication, you must create an HACA server template. You can perform HACA configurations, such as setting the IP address and interval of HACA heartbeat packets, only after an HACA server template is created.

Follow-up Procedure

After creating an HACA template, set the HACA server IP address and interval of the HACA heartbeat packets in the HACA server template view, and perform other configurations. Then, run the **haca-server** in the domain view to apply the HACA server template.

Example

Create an HACA server template **haca** and display the HACA server template view.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca]
```

13.4.12 haca-server timer down-delay

Function

The **haca-server timer down-delay** command sets the delay after which an HACA server is disconnected.

The **undo haca-server timer down-delay** command restores the default delay in which an HACA server is disconnected.

By default, the delay after which an HACA server is disconnected is 30s.

Format

haca-server timer down-delay *interval*

undo haca-server timer down-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay after which an HACA server is disconnected.	The value is an integer that ranges from 0 to 600, in seconds. Value 0 indicates that no delay is set for HACA server disconnection.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

If the communication between an HACA server and an access device is interrupted, authenticated users enter best-effort paths. That is, the users are allowed to access the network and will be reauthenticated after the communication re-establishes. If the HACA server is disconnected and connected frequently in a short period, a large number of users will be reauthenticated, which consumes device resources.

Therefore, set the delay after which an HACA server is disconnected to enable best-effort paths during the interval. When communication between the access devices and server is interrupted, the previously authenticated users will not be reauthenticated until the delay ends. This setting prevents resource exhaustion caused by frequent disconnection and reconnection.

Example

Set the delay after which an HACA server is disconnected to 60s.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer down-delay 60
```

13.4.13 haca-server timer heart-beat

Function

The **haca-server timer heart-beat** command sets the interval for sending HACA heartbeat packets.

The **undo haca-server timer heart-beat** command restores the default value of the interval for sending HACA heartbeat packets.

By default, the interval for sending HACA heartbeat packets is 5 minutes.

Format

haca-server timer heart-beat *interval*

undo haca-server timer heart-beat

Parameters

Parameter	Description	Value
interval	Specifies the interval at which HACA heartbeat packets are sent.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

A firewall may exist between the access device and HACA server. If the firewall does not detect packets for a long time, it may interrupt the connection. Run the **haca-server timer heart-beat** command to set the interval at which the client sends HACA heartbeat packets to ensure a proper connection.

Example

Set the interval for sending HACA heartbeat packets to 6 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer heart-beat 6
```

13.4.14 haca-server timer reconnection

Function

The **haca-server timer reconnection** command sets the reconnection interval for an HACA server.

The **undo haca-server timer reconnection** command restores the default value of the reconnection interval for an HACA server.

By default, the interval for reconnecting to an HACA server is one minute.

Format

haca-server timer reconnection *interval*

undo haca-server timer reconnection

Parameters

Parameter	Description	Value
interval	Specifies the interval for reconnecting to an HACA server.	The value is an integer that ranges from 1 to 255, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

If the communication between an access device and an HACA server is interrupted, the device reconnects to the server immediately. If that reconnection fails, the device reconnects to HACA at the HACA reconnection interval until the connection succeeds.

Example

Set the reconnection interval for the HACA server to 2 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer reconnection 2
```

13.4.15 haca-server timer register-sync

Function

The **haca-server timer register-sync** command configures the interval for a device to send HACA registration synchronization packets to iMaster NCE-Campus.

The **undo haca-server timer register-sync** command restores the default settings.

By default, a device sends HACA registration synchronization packets to iMaster NCE-Campus at an interval of 15 minutes.

Format

haca-server timer register-sync *interval*

undo haca-server timer register-sync

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a device sends HACA registration synchronization packets to iMaster NCE-Campus.	The value is an integer in the range from 0 to 60, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

You can run this command on a device so that the device sends HACA registration synchronization packets to iMaster NCE-Campus at the specified interval.

Example

Set the interval for a device to send HACA registration synchronization packets to iMaster NCE-Campus to 10 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer register-sync 10
```

13.4.16 haca-server timer response-timeout

Function

The **haca-server timer response-timeout** command sets the response timeout interval for an HACA server.

The **undo haca-server timer response-timeout** command restores the default value of the response timeout interval for an HACA server.

By default, the response timeout interval for an HACA server is 5 seconds.

Format

haca-server timer response-timeout *interval*

undo haca-server timer response-timeout

Parameters

Parameter	Description	Value
interval	Specifies the response timeout interval of an HACA server.	It is an integer that ranges from 1 to 300, in seconds.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

A device may not receive the response packets from HACA after sending request packets to the server. After a response timeout interval is set, if a device does not receive response packets from the HACA server in that specified time after sending request packets, the device will send request packets again. This improves the reliability of HACA authentication.

Example

Set the response timeout interval for an HACA server to 30s.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server timer response-timeout 30
```

13.4.17 haca-server timer user-syn

Function

The **haca-server timer user-syn** command sets the interval for synchronizing user information for an HACA server.

The **undo haca-server timer user-syn** command restores the default value of the interval for synchronizing user information for an HACA server.

By default, the user information synchronization interval for an HACA server is 10 minutes.

Format

haca-server timer user-syn *interval*

undo haca-server timer user-syn

Parameters

Parameter	Description	Value
interval	Specifies the user information synchronization interval for an HACA server.	The value can be 0 or range from 3 to 65535, in minutes. The value **0** indicates that user information synchronization is disabled.

Views

System view

Default Level

3: Management level

Usage Guidelines

In HACA authentication application, if communication between the device and HACA server is interrupted due to a network failure or HACA server failure, online HACA users cannot go offline normally. As a result, user information on the device may be different from that on the HACA server, causing inaccurate accounting. Run the **haca-server timer user-syn** *interval* command to enable user information synchronization. Then user information will be synchronized between the device and HACA server at the interval, which ensures user information consistency.

Example

Set the user information synchronization interval for the HACA server to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] haca-server timer user-syn 30
```

13.4.18 haca-server user-name

Function

The **haca-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in HACA packets sent to an HACA server.

The **haca-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the HACA server.

The **undo haca-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending HACA packets to an HACA server.

By default, the device does not modify the user name entered by the user in the packets sent to the HACA server.

Format

haca-server user-name domain-included

haca-server user-name original

undo haca-server user-name domain-included

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device manages access users based on domains. Each access user belongs to a domain. The users are authenticated in the specified domain when the entered user names contain domain names, or in the default domain when entered user names do not contain domain names. If a user name contains a domain name, the user belongs to that domain; otherwise, the user belongs to the default domain. When access users are authenticated in different domains, run the **haca-server user-name domain-included** command to configure the domain name encapsulated by the device in the user name in HACA packets to be sent to an HACA server.

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter. The domain name delimiter can also be any of the following symbols: \ / : < > | ' %.

If the HACA server does not accept the user name with the domain name, run the **undo haca-server user-name domain-included** command to delete the domain name from the user name.

Precautions

During Portal authentication, the **haca-server user-name domain-included** command does not take effect. During MAC address-prioritized Portal authentication, the **haca-server user-name domain-included** command takes effect only when users reconnect to the network through MAC address authentication.

Example

Configure the device not to encapsulate the domain name in the user name when sending HACA packets to an HACA server.

```
<HUAWEI> system-view
[HUAWEI] haca-server template haca
[HUAWEI-haca-haca] haca-server user-name domain-included
```

13.4.19 reset haca-server statistics

Function

The **reset haca-server statistics** command clears HACA packet statistics.

Format

reset haca-server statistics { **all** | **message** | **packet** [**register** | **accounting** | **authentication** | **authorization** | **user-syn** | **cut-notify** | **cut-request**] } [**template** *template-name*]

Parameters

Parameter	Description	Value
all	Clears all the statistics.	-
message	Clears all HACA message debugging information.	-
packet	Clears information about the specified type of packets.	-
register	Clears information about the registration packets.	-
accounting	Clears all statistics about HACA accounting.	-
authentication	Clears all statistics about HACA authentication.	-
authorization	Clears all statistics about HACA authorization.	-
user-syn	Clears all HACA user synchronization information.	-
cut-notify	Clears all HACA logout notifications.	-
cut-request	Clears all HACA logout requests.	-

Parameter	Description	Value
template *template-name*	Clears statistics about the specified HACA server template.	The HACA server template must already exist.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During fault location, you may need to collect statistics about the HACA packets in a certain period. Before collecting new statistics, clear the existing statistics. Then run the **display haca-server statistics** command to view HACA statistics.

Precautions

The **reset haca-server statistics** command clears statistics about HACA packets, and the cleared statistics cannot be restored. Therefore, exercise caution when running this command.

Example

Clear all HACA statistics.

```
<HUAWEI> reset haca-server statistics all
```

13.4.20 reset haca-server accounting-stop-packet all

Function

The **reset haca-server accounting-stop-packet all** command clears the remaining buffer information of all HACA accounting-stop packets.

Format

reset haca-server accounting-stop-packet all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **reset haca-server accounting-stop-packet all** command to clear the remaining buffer information of all HACA accounting-stop packets. Exercise caution when running this command because the information cannot be restored after being cleared.

Example

Clear the remaining buffer information of HACA accounting-stop packets.

```
<HUAWEI> reset haca-server accounting-stop-packet all
```

13.5 NAC Configuration Commands (Unified Mode)

13.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.5.2 access-context profile enable

Function

The **access-context profile enable** command enables the user context identification function.

The **undo access-context profile enable** command disables the user context identification function.

By default, the user context identification function is disabled.

Format

access-context profile enable

undo access-context profile enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User context refers to association information of a user, such as the user name, user VLAN, and access interface.

To simplify the authentication server configuration, the administrator can add the users with the same network access rights to the same user context profile based on the user context, and configure the network access rights for the users based on the user context profile. When a user goes online after the user context identification function is enabled, the device can identify the user context information and add the user to the corresponding context profile based on the identification result.

- If the user is authenticated successfully, the authentication server can assign the network access rights mapping the user context profile to the user based on the user context reported by the device.
- If the user fails to be authenticated, the device assigns the user the network access rights in each phase before authentication success, which are bound to the context profile in the user authentication event authorization policy.

For example, on some enterprise networks, VLANs are used to divide the entire network into different areas with various security levels. The administrator requires that a user should obtain different network access rights when the user connects to the network from different areas. In this case, the user context identification function can be enabled on access devices, and a group of VLANs that belong to the same area are added to the same user context profile. The administrator then assigns the mapping network access rights to different user context profiles based on the security level of each area. When a user connects to the network from different areas, the user is added to different user context profiles matching their access VLANs and therefore obtains different network access rights.

Follow-up Procedure

1. In the system view, run the **access-context profile name** *profile-name* command to create a user context profile.
2. In the user context profile view, run the **if-match vlan-id** { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10> command to configure the user identification policy based on VLAN IDs.

Precautions

- The device can only identify user VLANs.

Example

Enable the user context identification function.

```
<HUAWEI> system-view
[HUAWEI] access-context profile enable
```

13.5.3 access-context profile name

Function

The **access-context profile name** command creates a user context profile and displays the user context profile view.

The **undo access-context profile name** command deletes the created user context profile.

By default, no user context profile is created.

Format

access-context profile name *profile-name*

undo access-context profile name *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user context profile.	The value is a string of 1 to 32 case-sensitive characters without any space. The value cannot be set to - or --, and cannot contain the following characters: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To simplify the authentication server configuration, the administrator can add the users with the same network access rights to the same user context profile based on the user context, and assign the network access rights to the users based on the user context profile.

Follow-up Procedure

In the user context profile view, run the **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] &<1-10> command to configure the user identification policy based on VLAN IDs.

Example

Creates the user context profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] access-context profile name p1
```

13.5.4 access-author policy global

Function

The **access-author policy global** command applies a user authentication event authorization policy.

The **undo access-author policy global** command restores the default configuration.

By default, no user authentication event authorization policy is applied.

Format

access-author policy *policy-name* **global**

undo access-author policy *policy-name* **global**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user authentication event authorization policy.	The value must be the name of an existing user authentication event authorization policy on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users need basic network access rights before they are authenticated. For example, the users need to download 802.1X clients and update the antivirus database. A user authentication event authorization policy can be used to bind the network access rights of users in each phase before authentication success to a user context profile. When a user goes online after a user authentication event authorization policy is applied to the device, the device adds the user to the context profile based on the user context identification result, and assigns the network access rights to the user based on the user authentication result.

Prerequisites

A user authentication event authorization policy has been created using the **access-author policy name** *policy-name* command in the system view.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only one user authentication event authorization policy can be applied globally. If you run this command multiple times, only the latest configuration takes effect.

Example

Globally apply the user authentication event authorization policy **a1**.

```
<HUAWEI> system-view
[HUAWEI] access-author policy name a1
[HUAWEI-access-author-a1] quit
[HUAWEI] access-author policy a1 global
```

13.5.5 access-author policy name

Function

The **access-author policy name** command creates a user authentication event authorization policy and displays the user authentication event authorization policy view.

The **undo access-author policy name** command deletes the created user authentication event authorization policy.

By default, no user authentication event authorization policy is created.

Format

access-author policy name *policy-name*

undo access-author policy name *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user authentication event authorization policy.	The value is a string of 1 to 32 case-sensitive characters without any space. The value cannot be set to - or --, and cannot contain the following characters: / \ : * ? " < > | @ ' %. **NOTE** The value of *profile-name* cannot be set to the first character or first several characters of the name, and the name itself, and it also cannot be the uppercase and lowercase combination of the first character, first several characters, and the name. This prevents the conflict with the **access-author policy global** command.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users need basic network access rights before they are authenticated. For example, the users need to download 802.1X clients and update the antivirus database. A user authentication event authorization policy can be used to bind the network access rights of users in each phase before authentication success to a user context profile. When a user goes online after a user authentication event authorization policy is applied to the device, the device adds the user to the context profile based on the user context identification result, and assigns the network access rights to the user based on the user authentication result.

Follow-up Procedure

1. In the user authentication event authorization policy view, run the **match access-context-profile action** command to configure the network access rights for users in each phase before authentication success.

2. In the system view, run the **access-author policy global** command to apply the user authentication event authorization policy.

Precautions

A maximum of two user authentication event authorization policies can be configured.

Example

Create the user authentication event authorization policy **a1**.

```
<HUAWEI> system-view
[HUAWEI] access-author policy name a1
```

13.5.6 access-domain

Function

The **access-domain** command configures a default or forcible domain in an authentication profile for users.

The **undo access-domain** command deletes a configured default or forcible domain in an authentication profile.

By default, no default or forcible domain is configured in an authentication profile.

Format

access-domain *domain-name* [**dot1x** | **mac-authen** | **portal**] * [**force**]

undo access-domain [**dot1x** | **mac-authen** | **portal**] * [**force**]

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name.	The value must be the name of an existing domain.
dot1x	Specifies a default or forcible domain for 802.1X authentication users.	-
mac-authen	Specifies a default or forcible domain for MAC address authentication users.	-
portal	Specifies a default or forcible domain for Portal authentication users.	-

Parameter	Description	Value
force	Specifies the configured domain as a forcible domain. If this parameter is not specified, the configured domain is a default domain.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device manages users in domains. For example, AAA schemes and authorization information are bound to domains. During user authentication, the device assigns users to specified domains based on the domain names contained in user names. However, user names entered by many users on actual networks do not contain domain names. In this case, you can configure a default domain in an authentication profile. If users using this profile enter user names that do not contain domain names, the device manages the users in the default domain.

On actual networks, user names entered by some users contain domain names and those entered by other users do not. The device uses different domains to manage the users. Because authentication, authorization and accounting (AAA) information in the domains are different, users use different AAA information. To ensure that users using the same authentication profile use the same AAA information, you can configure a forcible domain in the authentication profile for the users. The device then manages the users in the forcible domain regardless of whether entered user names contain domain names or not.

Prerequisites

A domain has been configured using the **domain** command in the AAA view.

Precautions

When you configure a default or forcible domain in an authentication profile, the domain takes effect as follows:

- If you do not specify the user authentication mode (**dot1x**, **mac-authen**, or **portal**), the domain takes effect for all access authentication users using the authentication profile.
- If both a default domain and a forcible domain are configured, the device authenticates users in the forcible domain.

- This function takes effect only for users who go online after this function is successfully configured.
- In a wireless scenario, RADIUS accounting is performed only for AAA users who do not need to pass authentication in a forcible domain, and cannot be performed for such users in the default domain.

Example

Configure the forcible domain **test** in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] access-domain test force
```

13.5.7 access-user arp-detect

Function

The **access-user arp-detect** command sets the source IP address and source MAC address of offline detection packets in a VLAN.

The **undo access-user arp-detect** command deletes the source IP address and source MAC address of offline detection packets in a VLAN.

By default, the source IP address and source MAC address are not specified for offline detection packets in a VLAN.

Format

access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

undo access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies the source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or 255.255.255.255 or other valid IP address.

Parameter	Description	Value
mac-address *mac-address*	Specifies the source MAC address of offline detection packets.	The MAC address must be a unicast MAC address. The value is a hexadecimal number in the format H-H-H. Each H contains 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

If the VLAN to which the user belongs does not have a VLANIF interface or the VLANIF interface does not have an IP address, the device sends an offline detection packet using 0.0.0.0 as the source IP address. If a user cannot respond to an ARP probe packet with the source IP address 0.0.0.0, you can specify a source IP address for the offline detection packet.

In addition, a Windows client sends an ARP probe packet with the source IP address 0.0.0.0 after obtaining an IP address. In this case, if the device also sends an ARP probe packet with the source IP address 0.0.0.0, an IP address conflict occurs. In this case, you can specify an IP address as the source IP address of ARP probe packets sent by the device.

You are advised to specify the user gateway IP address and its corresponding MAC address as the source IP address and source MAC address of ARP probe packets sent by the device. If the gateway device changes, update the source MAC address of the ARP probe packets sent by the device in a timely manner. Otherwise, the gateway ARP entry on terminals may be incorrect, causing network disconnection.

Precautions

Only wired users support this function.

This function does not take effect for users who use Layer 3 Portal authentication.

For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:

Example

Set the source IP address and MAC address of offline detection packets for users in VLAN 10 to 192.168.1.1 and 00e0-fc11-1234 respectively.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect vlan 10 ip-address 192.168.1.1 mac-address 00e0-fc11-1234
```

13.5.8 authentication arp-reply trigger

Function

The **authentication arp-reply trigger** command enables the function of triggering authentication by ARP response packets.

The **undo authentication arp-reply trigger** command disables the function of triggering authentication by ARP response packets.

By default, the function of triggering authentication by ARP response packets is enabled.

Format

authentication arp-reply trigger

undo authentication arp-reply trigger

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a client in sleep mode receives an ARP request packet, it replies with an ARP response packet, which triggers authentication. However, the authentication fails because no user name or password is entered when the client is in sleep mode. If the client is awakened before the re-authentication interval (specified by the **authentication timer re-authen authen-fail** *re-authen-time* command) expires, the user has to wait for a period of time before triggering authentication again. In this case, you can disable the function of triggering authentication by ARP response packets so that authentication is not triggered by ARP response packets sent by clients in sleep mode.

Precautions

This function is supported only for wired users.

When the function of triggering authentication by ARP packets is disabled, the function of triggering authentication by ARP response packets becomes ineffective.

The function of triggering authentication by ARP response packets takes precedence over the function of triggering authentication by any packets. When the function of triggering authentication by ARP response packets is disabled and the function of triggering authentication by any packets is enabled, authentication cannot be triggered by ARP response packets.

This function does not apply to MAC address authentication on VLANIF interfaces or Portal authentication.

Example

Enable the function of triggering authentication by ARP response packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication arp-reply trigger
```

13.5.9 access-user arp-detect default ip-address

Function

The **access-user arp-detect default ip-address** command sets the default source IP address of offline detection packets.

The **undo access-user arp-detect default ip-address** command restores the default setting.

By default, the default source IP address of offline detection packets is 0.0.0.0.

Format

access-user arp-detect default ip-address *ip-address*

undo access-user arp-detect default ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or other valid IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

Precautions

- Only wired users support this function.
- This function does not take effect for users who use Layer 3 Portal authentication.
- In the SVF or policy association scenario, you are advised to run the **access-user arp-detect default ip-address** command to set the source IP address of offline detection packets to 0.0.0.0. In the SVF scenario, the command must be configured on the control device and takes effect only for control device detection. The default source IP address of offline detection packets for access device detection is 0.0.0.0. In the policy association scenario, you can directly configure the command on access devices.
- In normal situations, after a device sends an ARP probe packet with a default source IP address, online clients will immediately respond with ARP reply packets. If online clients do not respond with ARP reply packets, the device logs them out unexpectedly. To resolve this problem, use either of the following methods:
  - Run the **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address* command to specify a VLAN ID, source IP address, and source MAC address for ARP probe packets.
  - Run the **authentication timer handshake-period** *handshake-period* command to increase the handshake period so that the device can detect gratuitous ARP packets that these clients send at an irregular period. Once the device detects such packets, it does not log them out.
- The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:
  - **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*
  - **access-user arp-detect fallback** *ip-address* { *mask* | *mask-length* }
  - **access-user arp-detect default ip-address** *ip-address*

  If two or more of the commands are configured, the source IP or MAC address with a higher priority takes effect.
- For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

Example

Set the default source IP address of offline detection packets to 0.0.0.0.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect default ip-address 0.0.0.0
```

13.5.10 access-user dot1x-identity speed-limit

Function

The **access-user dot1x-identity speed-limit** command configures the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

The **undo access-user dot1x-identity speed-limit** command restores the default rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

By default, the maximum of Identity packets for 802.1X authentication can be sent to the CPU every second depends on the device.

Format

access-user dot1x-identity speed-limit *value*

undo access-user dot1x-identity speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.	The value is an integer in the range of 5 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a large number of Identity packets for 802.1X authentication are sent to the CPU of a switch, the CPU usage is high and other services are affected. To prevent this problem, run the **access-user dot1x-identity speed-limit** command to configure the rate limit of Identity packets for 802.1X authentication to be sent to the CPU, so that the switch discards excess Identity packets.

Example

Set the rate limit of Identity packets for 802.1X authentication to be sent to the CPU to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user dot1x-identity speed-limit 10
```

13.5.11 access-user arp-detect delay

Function

The **access-user arp-detect delay** command configures the delay in sending offline detection packets.

The **undo access-user arp-detect delay** command restores the default configuration.

By default, the delay in sending offline detection packets is 10 seconds.

Format

access-user arp-detect delay *delay*

undo access-user arp-detect delay

Parameters

Parameter	Description	Value
delay	Specifies the delay in sending offline detection packets.	The value is an integer in the range from 10 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A Windows client on the network sends a detection packet with the source address 0.0.0.0 after obtaining an IP address. If the device also initiates an ARP probe with the source address 0.0.0.0, a conflict occurs. To prevent this conflict, you can run the **access-user arp-detect delay** command to set the delay in sending offline detection packets. Typically, detection initiated by a Windows client takes 10 seconds. Therefore, a delay longer than 10 seconds is recommended.

Precautions

This function takes effect only for users who go online after it is configured.

This function takes effect in both ARP probe and ND probe scenarios.

NOTE

Delay after which the device sends the first ARP probe packet = Delay in sending offline detection packets + One-third of the handshake interval between the device and pre-connection or authorized users (configured using the **authentication timer handshake-period** command)

Example

Set the delay for sending offline detection packets to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect delay 20
```

13.5.12 access-user arp-detect fallback

Function

The **access-user arp-detect fallback** command configures an IP address required for calculating the source address of offline detection packets.

The **undo access-user arp-detect fallback** command deletes the IP address configured for calculating the source address of offline detection packets.

By default, no IP address is configured for the device to calculate the source address of offline detection packets.

Format

access-user arp-detect fallback *ip-address* { *mask* | *mask-length* }

undo access-user arp-detect fallback

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address required for calculating the source address of offline detection packets.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation. After the mask is converted into a binary number, all bits before the last 1 must be 1s. That is, 1s in the mask must be continuous and there cannot be any 0s before the last 1.
mask-length	Specifies the mask length of the IP address.	The value is an integer in the range from 0 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device does not function as a gateway, it can send offline detection packets with the source address on the same network segment as clients. This source address is calculated based on the client network segment and the IP address specified in the **access-user arp-detect fallback** command. The operation AND is performed between this specified IP address and the wildcard mask to obtain result 1. Then result 1 is added to the network segment of clients to get the source address of offline detection packets. For example, if the network segment of clients is 192.168.1.0/24 and **access-user arp-detect fallback 0.0.0.11 24** is configured, the source address of offline detection packets is 192.168.1.11. The calculated source address must be excluded from the address pool of the DHCP server to prevent IP address conflicts.

Precautions

Only wired users support this function.

This function does not take effect for users who use Layer 3 Portal authentication.

For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

- The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:
  - **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*
  - **access-user arp-detect fallback** *ip-address* { *mask* | *mask-length* }
  - **access-user arp-detect default ip-address** *ip-address*

  If two or more of the commands are configured, the source IP or MAC address with a higher priority takes effect.

Example

Set the IP address required for calculating the source address of offline detection packets to 0.0.0.11.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect fallback 0.0.0.11 24
```

13.5.13 access-user car-mode

Function

The **access-user car-mode** command configures the CAR mode for user access.

The **undo access-user car-mode** command restores the CAR mode for user access to **default**.

By default, the CAR mode for user access is **default**.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

access-user car-mode { **dual-stack** | **default** }

undo access-user car-mode

Parameters

Parameter	Description	Value
dual-stack	Specifies this CAR mode in scenarios where there are only wired or wireless dual-stack users on the network and authorization and accounting are performed on these users.	When this mode is specified, the rate limits are adjusted for the following types of packets: 8021x-start, 8021x-identity, nac-arp-request, capwap-association, capwap-disassoc, nac-nd, and nac-dhcpv6.
default	Specifies the default CAR mode in scenarios where authorization or accounting is not performed on users.	When this mode is specified, the system restores the default rate limits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the CAR mode for user access is **default**. This mode applies to scenarios where user authentication is performed but user authorization or accounting is not performed. In this mode, users can be quickly authenticated and go online.

When the device connects to the iMaster NCE-Campus controller, the controller delivers some authorization, accounting, and device and user statistics reporting configurations to the device by default, affecting the CPU usage of the device. To reduce the CPU load on the device, you need to adjust the user access rate. For example:

- When the device is deployed at the core layer and functions as the access authentication point for wireless users, you can specify **dual-stack** based on whether IPv6 users exist.
- When the device is deployed at the access or aggregation layer and functions as the access authentication point for wired users, you can specify **dual-stack** based on whether IPv6 users exist.

After the CAR mode for user access is configured, you can run the **display cpu-defend configuration** command to query the rate limits of packets.

Precautions

If the rate limits of specific packet types adjusted by this command conflict with those adjusted by the **car (attack defense policy view)** command, the rate limits adjusted by the **car (attack defense policy view)** command take effect.

Example

Set the CAR mode for user access to **dual-stack**.

```
<HUAWEI> system-view
[HUAWEI] access-user car-mode dual-stack
```

13.5.14 access-user https speed-limit

Function

The **access-user https speed-limit** command sets the limit of the rate at which HTTPS protocol packets are sent to the CPU.

The **undo access-user https speed-limit** command restores the default limit of the rate at which HTTPS protocol packets are sent to the CPU.

By default, the limit of the rate at which HTTPS protocol packets are sent to the CPU depends on the device model.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

access-user https speed-limit *value*

undo access-user https speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit.	The value is an integer in the range from 3 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a switch processes two many HTTPS protocol packets, the CPU usage may become high and other services are affected. To address this issue, run the **access-user https speed-limit** command to set the limit of the rate at which HTTPS protocol packets are sent to the CPU. If the rate at which HTTPS protocol packets are sent to the CPU exceeds the specified value, the switch discards the excessive HTTPS protocol packets.

Example

Set the limit of the rate at which HTTPS protocol packets are sent to the CPU to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user https speed-limit 50
```

13.5.15 access-user portal speed-limit

Function

The **access-user portal speed-limit** command sets the limit of the rate at which Portal protocol packets are sent to the CPU.

The **undo access-user portal speed-limit** command restores the default limit of the rate at which Portal protocol packets are sent to the CPU.

By default, the limit of the rate at which Portal protocol packets are sent to the CPU depends on the device model.

Format

access-user portal speed-limit *value*

undo access-user portal speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit.	The value is an integer in the range from 5 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a switch processes two many Portal protocol packets, the CPU usage may become high and other services are affected. To address this issue, run the **access-user portal speed-limit** command to set the limit of the rate at which Portal protocol packets are sent to the CPU. If the rate at which Portal protocol packets are sent to the CPU exceeds the specified value, the switch discards the excessive Portal protocol packets.

Example

Set the limit of the rate at which Portal protocol packets are sent to the CPU to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user portal speed-limit 50
```

13.5.16 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a user fails in authentication or goes offline, the device records a system log. The system log contains the MAC addresses of access device and access user and the authentication time.

If a user repeatedly attempts to go online after authentication failures or frequently goes online and offline in a short period, a lot of system logs are generated, which waste system resources and degrade system performance. System log suppression can address this problem. After the device generates a system log, it will not generate the same log within the suppression period (set by **access-user syslog-restrain period**).

NOTE

The same system logs refer to the system logs containing the same MAC addresses. For example, after the device generates a system log for a user failing in authentication, the device will not generate new system log for this user in the suppression period if the user fails in authentication again. The system logs for users logging offline are generated in the same way. If a system log has no MAC address, such system logs are suppressed based on the user name.

Example

Enable system log suppression.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain enable
```

13.5.17 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets a period for system log suppression.

The **undo access-user syslog-restrain period** command restores the default period for system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period for system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the system log suppression function is enabled using the **access-user syslog-restrain enable** command, use this command to set the system log suppression period. After generating a system log, the device will not generate the same log within the suppression period.

Example

Set the period for system log suppression to 600s.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain period 600
```

13.5.18 acl authorization statistics enable

Function

The **acl authorization statistics enable** command enables statistics collection on packets that match the ACLs assigned for authorization.

The **undo acl authorization statistics enable** command disables statistics collection on packets that match the ACLs assigned for authorization.

By default, statistics collection on packets that match the ACLs assigned for authorization is disabled.

Format

acl authorization statistics enable

undo acl authorization statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, the authentication server may assign ACLs to users who pass NAC authentication to grant the users access to the network. You can run the **acl authorization statistics enable** command to check the number of user packets that match the assigned ACLs.

Precautions

The function takes effect only for users who go online after this function is enabled, and for the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, and S5720-LI, this function cannot be used to collect statistics on packets that match the permit rules in redirection ACLs.

Example

Enable statistics collection on packets that match the ACLs assigned for authorization.

```
<HUAWEI> system-view
[HUAWEI] acl authorization statistics enable
```

13.5.19 acl-id (service scheme view)

Function

The **acl-id** command binds an ACL to a service scheme.

The **undo acl-id** command unbinds the ACL from the service scheme.

By default, no ACL is bound to a service scheme.

Format

acl-id [**ipv6**] *acl-number*

undo acl-id { [**ipv6**] *acl-number* | **all** }

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1, S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S6720-EI, S6735-S, , S6720S-EI support the **ipv6** parameter.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL bound to a service scheme.	The ACL number for wired users ranges from 3000 to 3999. The ACL number for wireless users ranges from 3000 to 3999 in tunnel forwarding mode, or from 3000 to 3031 in direct forwarding mode. **NOTE** In terms of authorization ACLs configured on a server, the ACL number for wired users ranges from 2000 to 3999, and the redirect ACL number ranges from 3000 to 3999; the ACL number for wireless users ranges from 2000 to 3999 in tunnel forwarding mode, or from 3000 to 3031 in direct forwarding mode.
ipv6	Indicates that the ACL bound to a service scheme is an IPv6 ACL. If this parameter is not specified, the ACL bound to a service scheme is an IPv4 ACL.	The IPv6 ACL number ranges from 3000 to 3999.
all	Deletes the numbers of all ACLs bound to a service scheme.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **acl-id** command to bind an ACL to the service scheme. The user assigned with the service scheme will have the ACL rules.

Prerequisites

An IPv4 ACL must have been created using the **acl** or **acl name** command.

An IPv6 ACL has been created using the **acl ipv6** or **acl ipv6 name** command.

Precautions

If the ACL authorized to users who go online through S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S is not a user-defined one, the attribute of the source IP address in the ACL rule does not take effect. In all other cases, the IP address in the ACL rule is replaced with the user's IP address. The IP address in the ACL rule will be replaced with the user's IP address.

Number of ACLs that can be bound to a service scheme:

- S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1. If you run this command multiple times, only the latest configuration takes effect.
- The other models: 4

The maximum number of IPv6 ACLs that can be bound to a service scheme is 1. If you run this command multiple times, only the latest configuration takes effect.

In the policy association scenario, if multiple ACLs are configured using this command on the authentication control device, only the first configured one takes effect on the authentication access device.

An ACL can be configured with a maximum of 129 rules. In wireless scenarios If the rule specification contains a matching port range (destination-port range or source-port range), extra hardware resources are occupied. As a result, the maximum number of rules cannot be delivered.

Ensure that the bound ACL has been created. Otherwise, ACL authorization fails for users who go online through the service scheme, and users may fail to go online.

Example

Bind ACL 3001 to the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] acl-id 3001
```

13.5.20 authentication handshake

Function

The **authentication handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

Format

authentication handshake

undo authentication handshake

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates entries for pre-connection users, users who fail to be authenticated and are assigned network access rights, and users who are authenticated. After users go offline in normal situations, the system immediately deletes the corresponding user entries. However, if some users go offline due to exceptions such as network disconnections, the system cannot immediately delete the corresponding user entries. If there are too many such user entries, other users may fail to access the network.

To solve this problem, run the **authentication handshake** command to enable the handshake with pre-connection users and authorized users. If a user does not respond to the handshake request from the device within the handshake interval, the device deletes the user entry.

Precautions

- The handshake interval for MAC address authentication users, Layer 3 Portal authentication users, and 802.1X authentication users is configured using the **authentication timer handshake-period** command. The handshake interval for Layer 2 Portal authentication users is configured using the **portal timer offline-detect** command.
- For Layer 3 Portal authentication users, only those who go online through S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.
- This function takes effect only for wired users. For users without IP addresses, the device sends probe packets after a delay of 30 minutes. If the device receives no reply packet from such users within a handshake interval, it logs out the users.

- When the configuration changes, the configuration takes effect only for new online wired users.
- The handshake function is implemented using ARP probe packets or neighbor discovery (ND) probe packets.
- The handshake function can also be implemented by detecting whether there is user traffic on the access device. Assuming that the handshake interval is **3n**, the device will detect user traffic at **n** and **2n**. The following uses the **0-n** period as an example. The process during the **n-2n** period is similar to that during **0-n**. (This process applies only to authentication users who go online from the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI. Other switch models do not detect user traffic and send probe packets at **n** and **2n**.)
  - If user traffic passes the device during the **0-n** period, the device considers that the user is online at **n**, so it will not send a probe packet to the user, but resets the handshake interval.
  - If no user traffic passes the device during the **0-n** period, the device cannot determine whether the user is online at **n**, so it sends a probe packet to the user. If the device receives the reply packet from the user, it considers the user online and resets the handshake interval. If no reply packet is received, it considers the user offline.
  - If user traffic passes the device during the **2n-3n** period, the device considers that the user is online at **3n** and resets the handshake interval.
  - If no user traffic passes the device during the **2n-3n** period, the device cannot determine whether the user is online at **3n** and considers that the user is offline.

  If the device considers that the user is offline at **n**, **2n**, and **3n**, the device deletes all entries related to the user. To prevent the user from going offline unexpectedly when no operation is performed on the PC, do not set a short handshake period.

Example

In the authentication profile **p1**, enable the handshake with pre-connection users and authorized users.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication handshake
```

13.5.21 authentication control-direction

Function

The **authentication control-direction** command configures the direction of traffic controlled by the device.

By default, the device only controls the upstream traffic.

Format

authentication control-direction { **all** | **inbound** }

Parameters

Parameter	Description	Value
all	Configures bidirectional traffic control.	-
inbound	Controls only the upstream traffic.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the access authentication device discards all the traffic sent from the users who fail the 802.1x authentication or MAC address authentication. However, these users can still receive packets broadcast from network devices to successfully authenticated users in the same VLAN. To disable the users who fail the authentication from receiving the broadcast packets, run the **authentication control-direction all** command to configure bidirectional traffic control. To restore the default situation, run the **authentication control-direction inbound** command so that the device only controls the traffic sent from the users who fail the authentication.

Precaution

- This function applies only to 802.1x authentication and MAC address authentication.
- This function takes effect only when an access switch functions as the authentication device and an interface of the switch is connected to only one IP phone or PC.
- This function does not take effect when users have pre-connection entries or authentication event entries. You are advised to run the **undo authentication pre-authen-access enable** command disable the function of keeping users who fail to be authenticated and do not have any network access rights in the pre-connection state, and do not run the **authentication event** command to configure the device to assign network access rights to users in each phase before authentication succeeds.
- When there are both successfully authenticated users and users who fail to be authenticated on the same interface in the same VLAN, bidirectional traffic control does not take effect on this interface.
- Layer 3 interfaces do not support bidirectional traffic control.
- You are advised to run the **stp edged-port enable** command to configure the interface on which the function is applied as an edge port. The interface can be added to a maximum of four VLANs.

- The SVF and policy association scenarios do not support this function.
- WLAN scenarios do not support this function.
- When this function is configured, the recommended STP mode is VBST. If the STP mode is changed after users go online, traffic will be interrupted for a short time. If the STP mode is set to MSTP or STP, run the **instance** command to map VLANs to different spanning tree instances (MSTIs).
- A user VLAN cannot be specified as an RRPP or ERPS control VLAN.
- After bidirectional traffic control is configured using the **authentication control-direction all** command, authentication can still be triggered even if a loop occurs on the downstream interface.

Example

Configure bidirectional traffic control in the authentication profile **authen1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication control-direction all
```

13.5.22 authentication device-type voice authorize

Function

The **authentication device-type voice authorize** command enables voice terminals to go online without authentication.

The **undo authentication device-type voice authorize** command disables voice terminals from going online without authentication.

By default, voice terminals are disabled from going online without authentication.

Format

authentication device-type voice authorize [**service-scheme** *scheme-name*]

undo authentication device-type voice authorize [**service-scheme**]

Parameters

Parameter	Description	Value
service-scheme *scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to voice terminals.	The value must be an existing service scheme name.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both data terminals (such as PCs) and voice terminals (such as IP phones) are connected to devices, NAC is configured on the devices to manage and control the data terminals. The voice terminals, however, only need to connect to the network without being managed and controlled. In this case, you can configure the voice terminals to go online without authentication on the devices. Then the voice terminals identified by the devices can go online without authentication.

Precautions

When a RADIUS server is used for dynamic VLAN delivery, the following RADIUS attributes must be used: (064) Tunnel-Type (which must be set to VLAN or 13), (065) Tunnel-Medium-Type (which must be set to 802 or 6), and (081) Tunnel-Private-Group-ID (which can be set to the VLAN ID, VLAN description, VLAN name, or VLAN pool). To ensure that the RADIUS server delivers VLAN attributes correctly, all the three RADIUS attributes must be used. In addition, the Tunnel-Type and Tunnel-Medium-Type attributes must be set to the specified values. When a voice VLAN is delivered, the RADIUS attribute (26-33) HW-Voice-Vlan must also be used.

To enable the switches to identify the voice terminals, enable LLDP or configure OUI for the voice VLAN on the switches. For details, see "Configuring Basic LLDP Functions" in "LLDP Configuration" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Network Management and Monitoring* or "Configuring a Voice VLAN Based on a MAC Address" in "Voice VLAN Configuration" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Ethernet Switching*. If a voice device supports only CDP but does not support LLDP, configure CDP-compatible LLDP on the switch using **lldp compliance cdp receive** command.

After the voice VLAN function is enabled on an interface using the **voice-vlan enable** command, authenticated voice terminals are authorized to use the voice VLAN if the VLAN of the voice terminals is the same as the voice VLAN.

If an 802.1X user initiates authentication through a voice terminal, a device preferentially processes the authentication request. If the authentication succeeds, the terminal obtains the corresponding network access rights. If the authentication fails, the device identifies the terminal type and enables the terminal to go online without authentication.

If you run this command repeatedly, the latest configuration overrides the previous ones.

This function takes effect only for users who go online after this function is successfully configured.

When voice terminals access the network without authentication, accounting is not supported.

Example

In the authentication profile **p1**, enable the device to allow voice terminals to go online without authentication and assign the service scheme **s1** to voice terminals that are not authenticated.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication device-type voice authorize service-scheme s1
```

13.5.23 authentication device-type iconnect authorize

Function

The **authentication device-type iconnect authorize** command enables iConnect terminals to go online without being authenticated.

The **undo authentication device-type iconnect authorize** command disables iConnect terminals from going online without being authenticated.

By default, iConnect terminals cannot go online without being authenticated.

NOTE

Only S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

authentication device-type iconnect authorize [**service-scheme** *scheme-name*]

undo authentication device-type iconnect authorize [**service-scheme**]

Parameters

Parameter	Description	Value
service-scheme *scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to iConnect terminals.	The value must be the name of an existing service scheme.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

iConnect is the name of an ecosystem at the network layer in the CloudCampus Solution. iConnect terminals refer to IoT terminals that use the iConnect ecosystem. NAC is required for most terminals, but not iConnect terminals. To enable iConnect terminals to go online without being authenticated, run the **authentication device-type iconnect authorize** command.

Precautions

This function takes effect only for MAC address authentication and Portal authentication users in wireless scenarios. This function cannot be configured in MAC+802.1X authentication scenarios.

This function has a higher priority than pre-connection authorization and authorization upon authentication failures.

This function does not take effect for open users.

If you run this command multiple times, only the latest configuration takes effect.

This function takes effect only for users who go online after this function is successfully configured.

Example

In the authentication profile **p1**, enable the device to allow iConnect terminals to go online without authentication and assign the service scheme **s1** to iConnect terminals that are not authenticated.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication device-type iconnect authorize service-scheme s1
```

13.5.24 authentication dot1x-mac-bypass

Function

The **authentication dot1x-mac-bypass** command enables MAC address bypass authentication.

The **undo authentication dot1x-mac-bypass** command disables MAC address bypass authentication.

By default, MAC address bypass authentication is disabled.

Format

authentication dot1x-mac-bypass

undo authentication dot1x-mac-bypass

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure MAC address bypass authentication to authenticate terminals such as printers that cannot have the 802.1X client installed.

After MAC address bypass authentication is enabled in an authentication profile, the device performs 802.1X authentication for users using the authentication profile. If the user name request times out, the device starts the MAC address authentication process for the users.

Precautions

MAC address bypass authentication involves 802.1X authentication and MAC address authentication. Before enabling this function in an authentication profile, ensure that an 802.1X access profile and a MAC access profile have been bound to the authentication profile.

Example

In the authentication profile **p1**, enable MAC address bypass authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication dot1x-mac-bypass
```

13.5.25 authentication drop dhcp-packet user-no-online enable

Function

The **authentication drop dhcp-packet user-no-online enable** command enables a device to discard DHCP packets when an 802.1X authentication user is offline or being re-authenticated.

The **undo authentication drop dhcp-packet user-no-online enable** command disables a device from discarding DHCP packets when an 802.1X authentication user is offline or being re-authenticated.

By default, the device does not discard DHCP packets when an 802.1X authentication user is offline or being re-authenticated.

Format

authentication drop dhcp-packet user-no-online enable

undo authentication drop dhcp-packet user-no-online enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where MAC address + 802.1X authentication is configured, the device permits DHCP Request packets from an 802.1X client and replies with DHCP ACK packets even when 802.1X authentication fails. In this case, the client failing the 802.1X authentication can still obtain an IP address through DHCP. As a result, the DHCP process is not triggered during subsequent MAC address authentication. To resolve this problem, you can run the **authentication drop dhcp-packet user-no-online enable** command to enable the device to discard DHCP and DHCPv6 packets when an 802.1X authentication user is offline or being re-authenticated. In this way, the DHCP process can be triggered when MAC address authentication is performed after an 802.1X authentication failure.

Prerequisites

An 802.1X access profile has been bound to an authentication profile.

Precautions

1. When the **authentication drop dhcp-packet user-no-online enable** command is configured in the VLANIF interface view where authentication is enabled, the configuration does not take effect.
2. When the **authentication drop dhcp-packet user-no-online enable** command is configured and DHCP packets match an authentication-free rule, the authentication-free rule preferentially takes effect; that is, DHCP packets are forwarded or discarded according to the authentication-free rule.

Example

Enable the device to discard DHCP packets when an 802.1X authentication user is offline or being re-authenticated in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication drop dhcp-packet user-no-online enable
```

13.5.26 authentication event action authorize

Function

The **authentication event action authorize** command configures authentication event authorization information.

The **undo authentication event action authorize** command restores the default setting.

By default, authentication event authorization information is not configured.

Format

User authorization in the case of pre-connections:

authentication event pre-authen action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* }

undo authentication event pre-authen action authorize

User authorization when authentication fails:

authentication event authen-fail action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* } [**response-fail**]

undo authentication event authen-fail action authorize

User authorization when the authentication server is Down:

authentication event authen-server-down action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* } [**response-fail**]

authentication event authen-server-down action authorize keep [**no-response** | **response-fail**]

undo authentication event authen-server-down action authorize

User authorization when the authentication server does not respond:

authentication event authen-server-noreply action authorize keep [**no-response** | **response-fail**]

undo authentication event authen-server-noreply action authorize

Parameters

Parameter	Description	Value
pre-authen	Configures the device to assign network access rights to users when the users establish pre-connections with the device.	-

Parameter	Description	Value
authen-fail	Configures the device to assign network access rights to users when the authentication server sends authentication failure packets to the device.	-
authen-server-down	Configures the device to assign network access rights to users when the authentication server is Down or the server is in the forcible Up state.	-
authen-server-noreply	Configures the device to assign network access rights to users when the authentication server does not respond.	-
response-fail	Configures the device to send authentication failure packets to users after assigning network access rights to the users. If this parameter is not specified, the device by default sends authentication success packets to users and therefore the users cannot know the fact that they fail to be authenticated. To solve this problem, specify this parameter so that the device will send authentication failure packets for the users to know their authentication results. **NOTE** When both the **authentication event authen-server-down action authorize** and **authentication event authen-server-down action authorize keep** commands are configured and the **response-fail** parameter is specified, both commands take effect.	-

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, users can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094. The VLAN must exist on the device. Otherwise, the configuration does not take effect.
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be an existing service scheme name on the device.
ucl-group *ucl-group-name*	Specifies the name of the UCL group based on which network access rights are assigned to users.	The value must be an existing UCL group name on the device.
keep	Configures online uses to retain original network access rights. **NOTE** If an online user is re-authenticated in a different authentication mode from the original one, the online user cannot retain the original network access permissions.	-
no-response	Configures the device not to send response packets to users after assigning network access rights to the users. If this parameter is not specified, the device sends an authentication success packet to users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If users establish pre-connections with the device or fail to be authenticated, they have no network access rights.

To meet these users' basic network access requirements such as updating the antivirus database and downloading a client, configure authentication event authorization information. The device will assign network access rights to these users based on the user authentication phase.

Precautions

Wireless 802.1X authentication only supports the **keep** parameter.

If no network access right is configured for users who fail authentication or when the authentication server is Down, the users establish pre-connections with the device after the authentication fails and then have the network access rights mapping pre-connection users.

VLAN-based authorization does not apply to the authentication users who access through VLANIF interfaces.

To use VLAN-based authorization (excluding authentication of pre-connection users), run the **undo authentication pre-authen-access enable** command to disable the pre-connection function first.

An authorized VLAN cannot be delivered to online Portal users.

If a user uses Portal authentication, the **keep** parameter cannot be configured.

The configured **vlan**, **service-scheme**, or **ucl-group** parameter takes effect only for new online users.

For S6720-EI, S6720S-EI, if the user upstream rate limit is configured in the QoS profile bound to a service scheme, do not configure the device to use the service scheme to grant network access rights to users in the pre-connection phase. Otherwise, users go offline.

When the authentication server is in Down state, user authentication fails, or the user is in pre-connection state, the redirect ACL function is not supported. For details about this function, see **redirect-acl**.

In 802.1X authentication for wired users, when the RADIUS server is Down, some new clients do not have escape rights. For example, when a new Windows client receives a Success packet from the device but does not receive the authentication packets exchanged with the RADIUS server, the client will fail the authentication and cannot go online. Currently, the following clients have escape rights when they go online for the first time: H3C iNode clients using EAP-MD5 or PEAP and Cisco AnyConnect clients using EAP-FAST or PEAP. For Windows clients, for example, Windows 7, choose "Local Area Connection> Properties> Authentication> Fallback to unauthorized network access".

Authentication event authorization information cannot be configured for static users identified by IP addresses.

If Portal authentication has been configured, VLAN-based authorization used when the authentication server is Down or configured for users who are in pre-connection state or fail the authentication does not take effect.

Example

In the authentication profile **authen1**, configure the device to assign network access rights specified in VLAN 10 to pre-connection users.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication event pre-authen action authorize vlan 10
```

13.5.27 authentication event authen-server-down action close re-authen

Function

The **authentication event authen-server-down action close re-authen** command disables re-authentication when the authentication server is Down.

The **undo authentication event authen-server-down action close re-authen** command restores the default setting.

By default, re-authentication is enabled when the authentication server is Down.

Format

authentication event authen-server-down action close re-authen

undo authentication event authen-server-down action close re-authen

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

In a re-authentication scenario, after the **authentication event action authorize keep** command is run, online users retain the original network access rights when the authentication server is Down. If re-authentication is performed on these users, the client frequently initiates re-authentication and may remain silent after multiple times. As a result, these users cannot access the network. To prevent this problem, you are advised to run the **authentication event authen-server-down action close re-authen** command to disable re-authentication when the authentication server is Down.

Example

Disable re-authentication when the authentication server is Down.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication event authen-server-down action close re-authen
```

13.5.28 authentication event authen-server-up action re-authen

Function

The **authentication event authen-server-up action re-authen** command enables the device to re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to Up.

The **undo authentication event authen-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to UP.

Format

authentication event authen-server-up action re-authen

undo authentication event authen-server-up action re-authen

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The users in the survival state can only access limited network resources after the device assigns specified network access rights to users who fail authentication because the authentication server is Down. To meet the users' normal network access requirements, the device needs to re-authenticate users in the survival state in real time when the authentication server turns Up.

After the status of the RADIUS server is set to Down, you can run the **radius-server dead-time** *dead-time* command to set the interval for the RADIUS server to return to the active state. When the value of *dead-time* expires, the status of the RADIUS server is set to forcible Up. When the server successfully transmits and receives packets, the status is set to Up. The device can re-authenticate users in the survival state when the server changes from Down or forcible Up to Up. Re-authentication cannot be triggered when the server turns from Down to forcible Up.

Prerequisites

The **radius-server testuser** command has been configured in the RADIUS server template so that the device can detect that the authentication server changes from Down to Up.

Example

In the authentication profile **authen1**, enable the device to re-authenticate users when the authentication server turns Up from Down or forcible Up.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication event authen-server-up action re-authen
```

13.5.29 authentication event client-no-response action authorize

Function

The **authentication event client-no-response action authorize** command configures network access rights for users when the 802.1X client does not respond.

The **undo authentication event client-no-response action authorize** command restores the default setting.

By default, no network access right is configured for users when the 802.1X client does not respond.

Format

authentication event client-no-response action authorize { **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* | **vlan** *vlan-id* }

undo authentication event client-no-response action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme-name*	Specifies the name of a service scheme based on which network access rights are assigned.	The value must be an existing service scheme name on the device.

Parameter	Description	Value
ucl-group *ucl-group-name*	Specifies the name of a UCL group based on which network access rights are assigned.	The value must be an existing UCL group name on the device.
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, users can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the 802.1X client does not respond, users cannot pass authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for the users when the 802.1X client does not respond, so that the users can access specified network resources.

Precautions

Wireless 802.1X authentication does not support this function.

This function takes effect only for users who go online after this function is successfully configured.

When an 802.1X client does not respond, the redirect ACL function is not supported. For details about the function, see **redirect-acl**.

In multi-mode authentication mode, if the function of assigning network access rights to users when the 802.1X client does not respond, the user status changes between Pre-authen and Client-no-resp, causing the function not to take effect.

Example

In the 802.1X access profile **d1**, configure the device to assign the network access rights specified in VLAN 10 for users when the 802.1X client does not respond.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] authentication event client-no-response action authorize vlan 10
```

13.5.30 authentication event portal-server-down action authorize

Function

The **authentication event portal-server-down action authorize** command configures network access rights for users when the Portal server is Down.

The **undo authentication event portal-server-down action authorize** command deletes the network access rights configured for users when the Portal server is Down.

By default, no network access right is configured for users when the Portal server is Down.

Format

authentication event portal-server-down action authorize { **service-scheme** *service-scheme-name* | **ucl-group** *ucl-group-name* }

undo authentication event portal-server-down action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be an existing service scheme name.
ucl-group *ucl-group-name*	Specifies the name of the UCL group based on which network access rights are assigned to users.	The value must be an existing UCL group name.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Portal server is Down, users cannot pass the authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for the users when the Portal server is Down, so that the users can access specified network resources.

Prerequisites

A UCL group has been created using the **ucl-group** command in the system view.

A service scheme has been created using the **service-scheme** command in the AAA view.

Precautions

- This function takes effect only for users who go online after this function is successfully configured.
- This function is not supported in Policy Association scenarios.
- Only HTTP/HTTPS messages-triggered portal authentication users support this function.
- Before enabling the access device to assign network access rights to users when the Portal server is Down, enable the heartbeat detection function on the Portal server and run the **server-detect** command on the access device to enable the Portal server detection function.
- When the Portal server is in Down state, the redirect ACL function is not supported. For details about this function, see **redirect-acl**.
- When both the network access permission and user authentication failure authorization are configured, and the user fails to be authenticated. If the Portal Server Down message is triggered, the user obtains the network access permission when the Portal server is Down. If the Portal Server Down message is not triggered, the user obtains the network access permission

Example

In the Portal access profile **p1**, configure the device to assign network access rights based on the service scheme **s1** to users when the Portal server is Down.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] authentication event portal-server-down action authorize service-scheme s1
```

13.5.31 authentication event portal-server-up action re-authen

Function

The **authentication event portal-server-up action re-authen** command enables the device to re-authenticate users when the Portal server turns Up from Down.

The **undo authentication event portal-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the Portal server turns Up from Down.

Format

authentication event portal-server-up action re-authen

undo authentication event portal-server-up action re-authen

Parameters

None

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is configured to assign network access rights to users when the Portal server is Down, users can access limited network resources after the device detects that the Portal server is Down. To ensure that users can obtain normal network access rights after the Portal server goes Up, you can enable the device to re-authenticate users when the Portal server changes from Down to Up. After the Portal server goes Up, the device sets the status of users who display **web-server-down** to pre-connection. The re-authentication process starts when the users visit any web page. If the authentication succeeds, the device assigns normal network access rights to the users.

Precautions

- This command does not apply to users connected to the route main interface.
- This function takes effect only for users who go online after this function is successfully configured.
- Before enabling the access device to assign network access rights to users when the Portal server is Down, enable the heartbeat detection function on the Portal server and run the **server-detect** command on the access device to enable the Portal server detection function.

Example

In the Portal access profile **p1**, enable the device to re-authenticate users when the Portal server turns Up from Down.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] authentication event portal-server-up action re-authen
```

13.5.32 authentication https-redirect enable

Function

The **authentication https-redirect enable** command enables HTTPS redirection for Portal or 802.1X authentication.

The **undo authentication https-redirect enable** command disables HTTPS redirection for Portal or 802.1X authentication.

By default, HTTPS redirection for Portal or 802.1X authentication is enabled.

Format

authentication https-redirect enable

undo authentication https-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Portal authentication scenarios, many well-known websites, such as Google and Baidu, use HTTPS. When a user accesses an HTTPS website, the user must be redirected to the Portal authentication page so that the user can be authenticated and access the Internet. After HTTPS redirection for Portal authentication is enabled, the device redirects unauthenticated Portal users to the Portal authentication page when they access HTTPS websites.

In 802.1X or Portal authentication scenarios, if the web page push function is deployed for HTTPS packets, run the **authentication https-redirect enable** command to enable the HTTPS redirection function. Otherwise, the web page push function does not take effect.

Precautions

- When Portal authentication is triggered while a user accesses an HTTPS website, the browser displays a security prompt, requiring the user to click **Continue** to complete Portal authentication.
- Redirection is not supported if the browser or website runs HTTP Strict Transport Security (HSTS).
- If the destination port number of the HTTPS request packet sent by the user is not a well-known port number (443), redirection cannot be performed.

- To enable HTTPS redirection of Portal authentication for wired Portal authentication users, run the **authentication https-redirect enable** command, and then run the **portal https-redirect wired enable** command.
- This function takes effect only for new Portal or 802.1X authentication users.
- For the S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I, the user access rate of the HTTPS redirection function is low. Therefore, this function is not recommended when a large number of users go online.

Example

Enable HTTPS redirection for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication https-redirect enable
```

13.5.33 authentication ip-address in-accounting-start

Function

The **authentication ip-address in-accounting-start** command enables the function of carrying users' IP addresses in Accounting-Start packets.

The **undo authentication ip-address in-accounting-start** command disables the function of carrying users' IP addresses in Accounting-Start packets.

By default, the function of carrying users' IP addresses in Accounting-Start packets is enabled.

Format

authentication ip-address in-accounting-start

undo authentication ip-address in-accounting-start

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device reports access information and basic network information (IP address) of users through Accounting-Start packets. Therefore, the device needs to support carrying users' IP addresses in Accounting-Start packets.

Precautions

If the device cannot learn IP addresses of users, the device does not send Accounting-Start packets.

This command takes effect only for 802.1X authentication and MAC address authentication users. By default, Accounting-Start packets for Portal authentication carry users' IP addresses.

This command takes effect on both IPv4 and IPv6 users. You can run the **authentication ipv4-address in-accounting-start mandatory** command to configure the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

In the earlier V200R020C10 versions, the function of carrying users' IP addresses in Accounting-Start packets is disabled by default. In the V200R020C10 and later versions, the function of carrying users' IP addresses in Accounting-Start packets is enabled by default. After a device running V200R020C10 or an earlier version is upgraded to V200R020C10 or a later version, to ensure compatibility, the **undo authentication ip-address in-accounting-start** command is automatically generated in the configuration file of a switch.

Example

Enable the function of carrying users' IP addresses in Accounting-Start packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ip-address in-accounting-start
```

13.5.34 authentication ipv4-address in-accounting-start mandatory

Function

The **authentication ipv4-address in-accounting-start mandatory** command enables the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

The **undo authentication ipv4-address in-accounting-start mandatory** command disables the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

By default, the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets is enabled.

Format

authentication ipv4-address in-accounting-start mandatory

undo authentication ipv4-address in-accounting-start mandatory

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

After you run the **authentication ipv4-address in-accounting-start** command to enable the function of carrying users' IP addresses in Accounting-Start packets, you can run the **authentication ipv4-address in-accounting-start mandatory** command to configure the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets. The following table lists the effectiveness of the two functions.

authentication ip-address in-accounting-start	authentication ipv4-address in-accounting-start mandatory	Effectiveness
Enabled	Enabled	The device sends an Accounting-Start packet only when a user has an IPv4 address.
Enabled	Disabled	The device sends an Accounting-Start packet only when a user has an IPv4 or IPv6 address.
Disabled	Enabled or disabled	The device can send an Accounting-Start packet regardless of whether a user has an IPv4 or IPv6 address.

Example

Enable the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ipv4-address in-accounting-start mandatory
```

13.5.35 authentication ip-conflict-check enable

Function

The **authentication ip-conflict-check enable** command enables the client IP address conflict detection function.

The **undo authentication ip-conflict-check enable** command disables the client IP address conflict detection function.

By default, the device detects whether client IP addresses conflict with each other.

Format

authentication ip-conflict-check enable

undo authentication ip-conflict-check enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP address conflict detection is performed based on an IP hash table. If the hash value of a client IP address conflicts with a value in the IP hash table on the device, the client cannot be authenticated. To prevent unauthorized users from accessing the network using forged IP addresses, you can enable the IP address conflict detection function. Some clients may use the same fixed source IP address to send ARP probe packets. If multiple such clients exist on the network, an IP address conflict occurs. In this case, you can disable the IP address conflict detection function.

Precautions

The **undo authentication ip-conflict-check enable** command is mutually exclusive with and takes precedence over the following configurations:

- Portal authentication
- Pushed URL configured using the **force-push** command
- Redirect URL configured using the **dot1x url** command for 802.1X authentication

After IP address conflict detection is disabled:

- After users with the same IPv4 address but different MAC addresses go online, the IPv4 address is displayed only for the first online user in the user table on the device. The second user displays a conflicting IP address.
- After users with the same IPv6 address but different MAC addresses go online, the IPv6 address is displayed for each user in the user table on the device. The second user displays a conflicting IP address

Example

Enable the client IP address conflict detection function.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ip-conflict-check enable
```

13.5.36 authentication ipv6-control enable

Function

The **authentication ipv6-control enable** command enables network admission control for IPv6 users.

The **undo authentication ipv6-control enable** command disables network admission control for IPv6 users.

By default, the network admission control function is disabled for IPv6 users.

NOTE

On the S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI that functions as the parent in an SVF system, the configuration of this command does not take effect and is delivered to ASs.

The following models do not support this command: S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I

Format

authentication ipv6-control enable

undo authentication ipv6-control enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, after NAC authentication is enabled on the device, IPv6 users can access the network without being authenticated in some scenarios. To ensure security, access right control can be enabled for IPv6 users, so that IPv6 users can access the network after being authenticated.

Precautions

The following table lists how different products process IPv6 packets for users in different authentication states.

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI	802.1X authentication on Layer 2 Ethernet interfaces	Not permitted	Not permitted	Permitted	This command does not take effect.		
	MAC address authentication on VLANIF interfaces	Not permitted	Not permitted	Permitted			
	MAC address authentication on Layer 2 Ethernet interfaces	Not permitted	Not permitted	Permitted			
	Layer 2 Portal authentication on VLANIF interfaces	Not permitted	Not permitted	Permitted			
	Layer 2 Portal authentication on Layer 2 Ethernet interfaces	Not permitted	Not permitted	Permitted			

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	Layer 3 Portal authentication on VLANIF interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted			
	Layer 3 Portal authentication on Layer 3 Ethernet interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted			
S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S	802.1X authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	MAC address authentication on VLANIF interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	MAC address authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 2 Portal authentication on VLANIF interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 2 Portal authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 3 Portal authentication on VLANIF interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	Layer 3 Portal authentication on Layer 3 Ethernet interfaces	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted
All products excluding S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S5731-L, S5731S-L	802.1X authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	MAC address authentication on VLANIF interfaces	Permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	MAC address authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 2 Portal authentication on VLANIF interfaces	Permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted

Product	Authentication Mode	Network Admission Control Disabled for IPv6 Users (by Default)			Network Admission Control Enabled for IPv6 Users		
		Unauthenticated/ Pre-connection Disabled	Pre-connected	Successfully Authenticated	Not Authenticated	Pre-connected	Successfully Authenticated
	Layer 2 Portal authentication on Layer 2 Ethernet interfaces	Not permitted	Permitted	Permitted	Not permitted	Not permitted	Permitted
	Layer 3 Portal authentication on VLANIF interfaces	Permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted
	Layer 3 Portal authentication on Layer 3 Ethernet interfaces **NOTE** This authentication mode is supported only on the S6720-EI, S6735-S, S6720S-EI.	Permitted	Layer 3 Portal authentication does not support pre-connection.	Permitted	Not permitted	Layer 3 Portal authentication does not support pre-connection.	Not permitted

For Portal users who access the network through devices that support this command: When network permission control for IPv6 users is disabled and Portal authentication redirection is enabled, CPU-bound IPv6 HTTP packets are still redirected.

Example

Enable network admission control for IPv6 users.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication ipv6-control enable
```

13.5.37 authentication mode

Function

The **authentication mode** command configures the user access mode.

The **undo authentication mode** command restores the default user access mode.

By default, the user access mode is **multi-authen**.

Format

authentication mode { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number* [**dot1x** | **mac-authen** | **portal** | **none**] *] }

undo authentication mode [**multi-authen max-user** [**dot1x** | **mac-authen** | **portal** | **none**] *]

Parameters

Parameter	Description	Value
single-terminal	Configures an interface to allow only one user to go online.	-
single-voice-with-data	Configures an interface to allow only one data user and one voice user to go online. This mode applies when a data user connects to a network through a voice terminal.	-
multi-share	Configures an interface to allow multiple users to go online. In this mode, the device authenticates only the first access user. If the first user passes authentication, subsequent users share the same network access rights with the first user. If the first user goes offline, other users also go offline.	-

Parameter	Description	Value
multi-authen	Configures an interface to allow multiple users to go online. In this mode, the device authenticates each access user. If users pass authentication, the users are given individual network access rights. If a user goes offline, other users will not be affected.	-
max-user *max-user-number*	Specifies the maximum number of access users on the interface in **multi-authen** mode.	The value is an integer and the value range varies depending on devices.
dot1x	Specifies the maximum number of 802.1X authenticated users allowed to connect to the interface in **multi-authen** mode.	-
mac-authen	Specifies the maximum number of MAC authenticated users allowed to connect to the interface in **multi-authen** mode.	-
portal	Specifies the maximum number of Portal authenticated users allowed to connect to the interface in **multi-authen** mode.	-
none	Specifies the maximum number of pre-connection users allowed to connect to the interface in **multi-authen** mode.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After NAC authentication is enabled, you can configure the user access mode on an interface based on the user access on the interface.

- **single-terminal**: applies when only one data terminal is connected to the network through the interface.

- **single-voice-with-data**: applies when only one data terminal is connected to the network on the interface through a voice terminal.
- **multi-share**: applies when multiple data terminals are connected to the network on the interface and high security is not required.
- **multi-authen**: applies when multiple data terminals are connected to the network on the interface and high security is required. In this access mode, you can configure the maximum number of access users based on the actual user quantity on the interface. This prevents malicious users from occupying a large amount of device resources and ensures that the users on other interfaces can normally go online.

Precautions

- VLANIF interfaces do not support this function.
- If there are online users in the authentication profile, the user access mode cannot be changed.
- This function takes effect only for wired users.
- If the **multi-share** mode is configured on an Eth-Trunk of the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the upstream rate limit cannot be delivered to users who go online through this Eth-Trunk.
- If the first access user fails authentication on a physical interface and sets up a pre-connection after the **multi-share** mode is configured on the physical interface, new access users will also fail authentication on the interface. Therefore, the following operations are recommended if the first access user may fail authentication after the **multi-share** mode is configured on a physical interface.
  - Disable the pre-connection function using the **undo authentication pre-authen-access enable** when 802.1X or MAC authentication is used.
  - Do not use the **multi-share** mode with Portal authentication.
- In policy association scenarios, the **authentication mode multi-authen max-user** *max-user-number* command configured on an AS does not take effect. To set the maximum number of access users on an AS, run the **authentication access-point max-user** *max-user-number* command to set the maximum number of access users allowed on the interface of the access device.
- When **authentication mode** is set to **multi-authen** in the authentication profile, to configure authorized VLANs, set the interface type to hybrid or trunk in policy association scenarios, and to hybrid in other scenarios.
- When the user access mode is set to **multi-share** on the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, the following situation may occur before MAC address learning is triggered by user packets: The **display access-user** command output contains user entries but the **display mac-address** command output does not contain user MAC address entries. The **display mac-address** command displays MAC address entries only after MAC address learning is triggered by user packets.
- If the user access mode is **multi-share**, authorization redirection ACLs or authorized voice VLANs are not supported.
- If the user access mode is set to **multi-share**, authorization based on an ISP VLAN is not supported.

- If the user access mode is set to **multi-share**, authorization based on the HW-Forwarding-Interface attribute is not supported.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, if the authentication profile in which the user access mode is set to **multi-share** is applied to a physical interface and the **statistic enable** or **accounting dual-stack separate** command is configured on the interface, IPv4 and IPv6 traffic statistics are not differentiated and both counted as IPv4 traffic statistics displayed using the **display access-user** command.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500. S5735-S-I, S5735S-S, , if the authentication profile in which the user access mode is set to **multi-authen** is applied and both the **car** and **statistic enable** commands are configured, only the **car** command takes effect.

Example

In the authentication profile **p1**, set the user access mode to **multi-authen**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication mode multi-authen
```

13.5.38 authentication mac-authen-first force

Function

The **authentication mac-authen-first force** command configures forcible MAC address authentication before 802.1X authentication.

The **undo authentication mac-authen-first force** command restores the default setting.

By default, the forcible MAC address authentication is not configured before 802.1X authentication.

Format

authentication mac-authen-first force

undo authentication mac-authen-first force

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command.

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If high security is required, users who access the network must use registered terminals for 802.1X authentication. To prevent users from using unregistered terminals to perform 802.1X authentication and occupying device and server resources, you can configure this function to force the users to perform MAC address authentication first. 802.1X authentication can be performed only after MAC address authentication succeeds. For an unregistered terminal, users go offline directly after MAC address authentication fails, and 802.1X authentication is not performed.

Precautions

This function is only supported in the wireless scenario.

This command takes effect only when an 802.1X access profile and a MAC access profile have been configured in the authentication profile where the command is configured.

Example

Configure forcible MAC address authentication before 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication mac-authen-first force
```

13.5.39 authentication mac-move enable

Function

The **authentication mac-move enable** command enables MAC address migration.

The **undo authentication mac-move enable** command disables MAC address migration.

By default, MAC address migration is disabled.

Format

authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

undo authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

Parameters

Parameter	Description	Value
vlan	Specifies the VLAN range for enabling MAC address migration.	-
all	Enables MAC address migration in all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Enables MAC address migration in the specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. ● If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is created.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a user is authenticated and accesses the network from one interface of the device, the Ethernet cable is pulled out from the interface and plugged in another interface on the device; or a user switches between different VLANs on the same interface. In this case, the user cannot immediately initiate authentication and access the network. The user can initiate authentication on the current interface only after the user offline detection interval expires or the authentication interface is manually enabled and shut down to clear user online entries. To improve user experience, MAC address migration is enabled so that the user can immediately initiate authentication and access the network after be switched to another access interface.

MAC address migration allows online NAC authentication users to immediately initiate authentication and access the network after they are switched to other access interfaces. If the user is authenticated successfully on the new interface, the online user entry on the original interface is deleted immediately to ensure that only one interface records the online user entry.

In addition, VLANs need to be specified for users in MAC address migration. The VLANs before and after the migration can be specified for the users, and they can be the same or different.

Precautions

- In normal case, enabling MAC address migration is not recommended. It should be enabled only when users have migration requirements during roaming. This prevents unauthorized users from forging MAC addresses of online users and sending ARP, 802.1X, or DHCP packets on other authentication control interfaces to trigger the MAC address migration function and force authorized user offline.
- In the Policy Association and SVF scenario, the device does not support MAC address migration.
- In the Layer 2 BNG scenario, the device does not support MAC address migration.
- Cascading migration through intermediate devices is not supported, because ARP and DHCP packets are not sent after the cascading migration.
- The device does not support MAC address migration for a terminal with one MAC address and multiple IP addresses.
- MAC address migration is not supported for Layer 3 Portal authentication users.
- A user is switched from an interface configured with NAC authentication to another interface not configured with NAC authentication. In this case, the user can access the network only after the original online entry is aged because the new interface cannot send authentication packets to trigger MAC migration.
- In common mode, Portal authentication is triggered only after users who go online through a VLANIF interface send ARP packets and go offline; otherwise, the users can go online again only after the original user online entries age out. Portal authentication cannot be triggered after users who go online through physical interfaces migrate. The users can go online again only after the original user online entries age out.
- After a user who goes online from a VLANIF interface is quieted because of multiple MAC address migrations, MAC address migration can be performed for the quieted user only after the quiet period expires and the ARP entry is aged out.
- When an authorized VLAN is specified in the **authentication mac-move enable vlan** command, you are advised to enable the function of detecting the user status before user MAC address migration.
- When a device functions as a third-party AC for wireless-to-wire authentication and a native AC, MAC address migration is not supported when the terminal switches from the third-party Wi-Fi to the native AC Wi-Fi. The terminal can go online only after the wired authentication entry ages 5 minutes. In this scenario, you are advised to move the authentication point to a third-party AC and do not deploy wireless-to-wire authentication.

Example

Enable MAC address migration in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move enable vlan all
```

13.5.40 authentication mac-move detect enable

Function

The **authentication mac-move detect enable** command enables a device to detect users' online status before user MAC address migration.

The **undo authentication mac-move detect enable** command disables a device from detecting users' online status before user MAC address migration.

By default, a device is disabled from detecting users' online status before user MAC address migration.

Format

authentication mac-move detect enable

undo authentication mac-move detect enable

Parameters

None

Views

System view, authentication profile view

Default Level

2: Configuration level

Usage Guidelines

To prevent unauthorized users from spoofing online users to attack a device, run the **authentication mac-move detect enable** command to enable the device to detect users' online status before user MAC address migration. If no users are online, the device permits MAC address migration and allows users to go online from a new access interface. If a user is online, the device terminates MAC address migration and does not allow the user to go online from a new access interface.

You can also run the **authentication mac-move detect retry-interval retry-time** command to set the detection interval and maximum number of detections before user MAC address migration.

By default, the user status detection function before user MAC address migration is disabled in the system view, but it is enabled in the authentication profile view. This function takes effect only when it is enabled both in the system view and authentication profile view. To disable the device from detecting the online status of users connected to certain interfaces before user MAC address migration, run the **undo authentication mac-move detect enable** command in the authentication profiles bound to these interfaces.

After the **authentication mac-move detect enable** command is configured in an authentication profile, the authentication profile cannot be bound to a VAP profile.

Example

Enable a device to detect users' online status before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect enable
```

13.5.41 authentication mac-move detect retry-interval retry-time

Function

The **authentication mac-move detect retry-interval retry-time** command sets the detection interval and maximum number of detections before user MAC address migration.

The **undo authentication mac-move detect retry-interval retry-time** command restores the default setting.

By default, a device detects users' online status once. The detection interval is 3 seconds.

Format

authentication mac-move detect { **retry-interval** *interval* | **retry-time** *times* } *

undo authentication mac-move detect { **retry-interval** | **retry-time** } *

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a device detects users' online status before user MAC address migration.	The value is an integer that ranges from 1 to 5, in seconds.
times	Specifies the maximum number of detections before user MAC address migration.	The value is an integer that ranges from 1 to 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a device is enabled to detect users' online status before user MAC address migration, if no users are online, the device permits MAC address migration and allows users to go online from a new access interface. If a user is online, the device terminates MAC address migration and does not allow the user to go online from a new access interface. You can run the **authentication mac-move detect** { **retry-interval** *interval* | **retry-time** *times* } * command to modify the default detection interval and maximum number of detections.

Example

Configure a device to detect users' online status twice at an interval of 5 seconds before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect retry-interval 5 retry-time 2
```

13.5.42 authentication mac-move quiet-log enable

Function

The **authentication mac-move quiet-log enable** command enables the device to record logs about MAC address migration quiet.

The **undo authentication mac-move quiet-log enable** command disables the device from recording logs about MAC address migration quiet.

By default, the device is enabled to record logs about MAC address migration quiet.

Format

authentication mac-move quiet-log enable

undo authentication mac-move quiet-log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can record logs when adding or deleting MAC address migration quiet entries. This helps the administrator to find out the cause for MAC address migration failure, and improves maintainability of the MAC address migration quiet function.

Example

Enable the device to record logs about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-log enable
```

13.5.43 authentication mac-move quiet-times quiet-period

Function

The **authentication mac-move quiet-times quiet-period** command configures the quiet period and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.

The **undo authentication mac-move quiet-times quiet-period** command restores the default settings.

The default quiet period is 0 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state is 3.

Format

authentication mac-move { **quiet-times** *times* | **quiet-period** *quiet-value* } *

undo authentication mac-move { **quiet-times** | **quiet-period** } *

Parameters

Parameter	Description	Value
times	Specifies the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.	The value is an integer that ranges from 1 to 10.

Parameter	Description	Value
quiet-value	Specifies the quiet period for MAC address migration users.	The value is an integer that ranges from 0 to 3600. The value 0 indicates that the MAC address migration quiet function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When users frequently switch access interfaces (especially frequent switching due to loops), the device needs to process a large number of authentication packets and entries, which results in high CPU usage. To solve this problem, configure the MAC address migration quiet function.

If the number of MAC address migration times for a user within 60 seconds exceeds the value (*times*) after the MAC address migration quiet function is enabled, the device quiets the user for a certain period (*quiet-value*). During the quiet period, the device does not allow users to perform MAC address migration.

Example

Configure the quiet period to 120 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state to 5.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-times 5 quiet-period 120
```

13.5.44 authentication mac-move quiet-user-alarm enable

Function

The **authentication mac-move quiet-user-alarm enable** command enables the device to send alarms about MAC address migration quiet.

The **undo authentication mac-move quiet-user-alarm enable** command disables the device from sending alarms about MAC address migration quiet.

By default, the device is disabled from sending alarms about MAC address migration quiet.

Format

authentication mac-move quiet-user-alarm enable

undo authentication mac-move quiet-user-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Example

Enable the device to send alarms about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm enable
```

13.5.45 authentication mac-move quiet-user-alarm percentage

Function

The **authentication mac-move quiet-user-alarm percentage** command configures the upper and lower alarm thresholds for the percentage of MAC address migration users in quiet state.

The **undo authentication mac-move quiet-user-alarm percentage** command restores the default setting.

By default, the lower alarm threshold is 50 and upper alarm threshold is 100.

Format

authentication mac-move quiet-user-alarm percentage *lower-threshold upper-threshold*

undo authentication mac-move quiet-user-alarm percentage

Parameters

Parameter	Description	Value
lower-threshold	Specifies the lower alarm threshold.	The value is an integer that ranges from 1 to 100.
upper-threshold	Specifies the upper alarm threshold.	The value is an integer that ranges from 1 to 100. The value must be greater than that of *lower-threshold*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **authentication mac-move quiet-user-alarm enable** command can be run to enable the device to send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Precautions

When a user goes online at a rate exceeding the upper limit, the alarm may not be generated.

Example

Configure the upper alarm threshold to 80 and lower alarm threshold to 40.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm percentage 40 80
```

13.5.46 authentication no-ip-check

Function

The **authentication no-ip-check** command disables the device from creating an IP hash table for client IP addresses.

The **undo authentication no-ip-check** command allows the device to create an IP hash table for client IP addresses.

By default, the device creates an IP hash table for client IP addresses.

Format

authentication no-ip-check

undo authentication no-ip-check

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After users obtain IP addresses, the device creates an IP hash table. If the hash value of a client IP address conflicts with a value in the IP hash table on the device, the client cannot be authenticated. When two branches are connected to the device, the address pools of the branches may overlap. As a result, two clients in different branches may have the same IP address. When the device detects conflicting IP addresses, the clients fail to go online. To address this problem, you can run the **authentication no-ip-check** command to disable the device from creating an IP hash table for client IP addresses.

Precautions

You are advised not to configure the **authentication no-ip-check** command. If this command is configured and two clients with the same IP address go online through the same interface, the rules (such as ACL rules and static UCL groups) configured based on this IP address may be mismatched.

This function cannot be used with Portal authentication together.

This function cannot be configured with **ip-static-user enable** together.

After this function is enabled, network access permissions are granted only to users in the ARP table.

After the **authentication no-ip-check** command is run, IP address–based CoA cannot be implemented.

Example

Disable the device from creating an IP hash table for client IP addresses.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication no-ip-check
```

13.5.47 authentication no-replace dot1x

Function

The **authentication no-replace dot1x** command configures the device not to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

The **undo authentication no-replace dot1x** command configures the device to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

By default, the device responds to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

Format

authentication no-replace dot1x [**device-type voice**]

undo authentication no-replace dot1x [**device-type voice**]

Parameters

Parameter	Description	Value
device-type voice	Configures the function to be effective only for voice terminals. When this parameter is not specified, the function is effective for all terminals.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After passing MAC address authentication, some voice terminals still send EAP start packets. If the device returns response packets, the voice terminals go offline. To address this problem, you can configure the device not to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

Precautions

This function is effective only for wired users.

No matter whether this function is configured, the device responds to EAP Start packets sent from 802.1X users.

Example

Configure the device not to respond to the EAP start packets sent from users who have successfully passed MAC address authentication or Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication no-replace dot1x device-type voice
```

13.5.48 authentication order mac dot1x

Function

The **authentication order mac dot1x** command configures MAC address authentication to take precedence over 802.1X authentication when the device receives EAP-Start packets.

The **undo authentication order mac dot1x** command cancels the configuration.

By default, the sequence of authentication modes triggered by EAP-Start packets is not configured.

Format

authentication order mac dot1x

undo authentication order mac dot1x

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some terminals send EAP-Start packets to trigger 802.1X authentication, but do not respond to EAP-Request/Identity packets returned by the device. As a result, traffic is interrupted and the terminals cannot be authenticated. To authenticate these terminals, you can run the **authentication order mac dot1x** command to enable the device to perform MAC address authentication first after receiving EAP-Start packets. If the terminals fail the MAC address authentication, the device then performs 802.1X authentication.

If a terminal sends multiple EAP-Start packets, the device continues to return EAP-Response/Identity packets even after MAC address authentication using the first EAP-Start packet is successful. However, the terminal no longer responds to the subsequent EAP-Response/Identity packets, causing traffic interruption. To prevent this problem, run the **authentication no-replace dot1x** command to configure the device not to respond to the EAP-Start packets sent from users who have successfully passed MAC address authentication.

Precautions

This function is supported only for new wired users.

This command controls only the sequence of authentication modes triggered by EAP-Start packets. After this command is run, MAC address authentication or 802.1X authentication will not be automatically enabled.

This command takes precedence over the **authentication dot1x-mac-bypass** command.

Example

Configure MAC address authentication to take precedence over 802.1X authentication when the device receives EAP-Start packets.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication order mac dot1x
```

13.5.49 authentication pre-authen-access enable

Function

The **authentication pre-authen-access enable** command enables the pre-connection function.

The **undo authentication pre-authen-access enable** command disables the pre-connection function.

By default, the pre-connection function is enabled. That is, the device keeps users who are not successfully authenticated and do not have any network access permissions in the pre-connection state.

Format

authentication pre-authen-access enable

undo authentication pre-authen-access enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user terminal connects to an NAC-enabled interface on the device, a pre-connection is set up between the terminal and device. If the device is not configured to grant network access rights to users in pre-connection or authentication failure state, users who fail to be authenticated remain in the pre-connection state by default. Because the device allows DHCP packets from pre-connection users to pass through, the users can still obtain IP addresses although they do not have any network access rights, wasting IP addresses and bringing network security risks.

If users do not need any network access rights before being authenticated successfully, disable the pre-connection function. Users will then not have any network access rights before being authenticated successfully and will not obtain IP addresses.

Precautions

- This function does not take effect for users who use Portal authentication or combined authentication (including Portal authentication).
- The **undo authentication pre-authen-access enable** command does not take effect for pre-connection users for whom network access permissions are configured.
- When the **lldp sensor-ap authentication disable** command is configured in the authentication profile view, the **undo authentication pre-authen-access enable** command does not take effect.
- When 802.1X authentication or MAC address authentication is configured on a physical interface, the **free-rule** command configuration will not take effect after the pre-connection function is disabled.
- If the device connects to some terminals such as a MacBook laptop that is not authenticated after obtaining an IP address, it is recommended that you run the **undo authentication pre-authen-access enable** command on the device to disable the pre-connection function and then connect the terminal to the network again.
- If a user in pre-connection state attempts to go online using DHCP packets containing the Option 82 field but fails to go online, it is recommended that

you run the **undo authentication pre-authen-access enable** command on the device to disable the pre-connection function.

- When Layer 2 Portal authentication is deployed on a non-gateway device, do not run the **undo authentication pre-authen-access enable** command to disable the pre-connection function. Otherwise, Layer 2 Portal authentication will not take effect.
- When MAC address authentication or Portal authentication is configured on a physical interface, no pre-connection entry is generated, but users can go online successfully.

Example

Disable the pre-connection function.

```
<HUAWEI> system-view
[HUAWEI] undo authentication pre-authen-access enable
```

13.5.50 authentication port-vlan-modify user-online

Function

The **authentication port-vlan-modify user-online** command enables the function of keeping users online when the port type or VLAN is changed.

The **undo authentication port-vlan-modify user-online** command restores the default setting.

By default, the function of keeping users online when the port type or VLAN is changed is disabled.

Format

authentication port-vlan-modify user-online

undo authentication port-vlan-modify user-online

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user access authentication succeeds, you can change the VLAN allowed to access or the access interface type through the RADIUS server. For example, you can assign VLANs to clients through the server for network planning and deployment. After the deployment is complete, to reduce the impact of link faults and device restart on the network and implement rapid network restoration, you can change the user access VLAN to the authorized VLAN. In this case, you can enable the function of keeping users online when the port type or VLAN is changed to modify interface or VLAN configurations.

Precautions

This function is only supported by MAC and 802.1X authentication.

This function is only supported by wired users.

Example

Enable the function of keeping users online when the port type or VLAN is changed.

```
<HUAWEI> system-view
[HUAWEI] authentication port-vlan-modify user-online
```

13.5.51 authentication { roam-accounting | update-info-accounting | update-ip-accounting } * enable

Function

The **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command enables a device to send accounting packets for roaming, terminal information updating and address updating.

The **undo authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command disables a device from sending accounting packets for roaming, terminal information updating and address updating.

By default, the device is enabled to send accounting packets for roaming, terminal information updating and address updating.

Format

authentication { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable**

undo authentication { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable**

NOTE

Only the following models support **roam-accounting**:

S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the device sends accounting packets for roaming, terminal information, and address updating to the accounting server. Some accounting servers may not require the accounting packets. In this case, resources on the device are occupied. You can run the **undo authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command to disable a device from sending accounting packets for roaming, terminal information updating and address updating, saving resources on the device. After roaming, terminal information updating, and address updating are complete, the device sends accounting packets again and the accounting function is not affected.

In the command:

- **roam-accounting** indicates that accounting packets are immediately sent during roaming.
- Only wireless user devices support the **roam-accounting** parameter.
- **update-info-accounting** indicates that accounting packets are immediately sent during terminal information updating.

  To configure this function, the terminal type identification function must be configured simultaneously.
- **update-ip-accounting** indicates that accounting packets are immediately sent during address updating.
- If the terminal information (including the DHCP Option, user agent, or LLDP information) is updated for the first time, the device immediately triggers real-time accounting. If the terminal information is not updated for the first time, the device only updates the user entry and reports the new terminal information through subsequent accounting messages.
- After the **undo authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command is configured, the device does not send the accounting packet immediately after obtaining the packet, and waits until the real-time accounting timer expires.

Example

Disable a device from sending accounting packets for address updating.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] undo authentication update-ip-accounting enable
```

13.5.52 authentication roam pre-authen mac-authen enable

Function

The **authentication roam pre-authen mac-authen enable** command enables MAC address authentication for roaming STAs.

The **undo authentication roam pre-authen mac-authen enable** command disables MAC address authentication for roaming STAs.

By default, MAC address authentication is disabled for roaming STAs.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command.

Format

authentication roam pre-authen mac-authen enable

undo authentication roam pre-authen mac-authen enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A STA connects to the network through MAC address authentication or MAC address-prioritized Portal authentication. If the STA roams, MAC address authentication is triggered after successful roaming. However, MAC address authentication may fail, and the STA enters the pre-connection state and no longer has the original access permission. To prevent this problem, the MAC address authentication is disabled for roaming STAs by default. You are not advised to retain the default configuration.

Precautions

MAC address authentication for roaming STAs takes effect only when the following authentication event authorization information is configured:

- Authorization for STAs in pre-connection users
- Authorization for STAs that fail the authentication
- Authorization for STAs if the authorization server goes Down

- Authorization for STAs if the Portal server goes Down

Example

Enable MAC address authentication for roaming STAs.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name test
[HUAWEI-authen-profile-test] authentication roam pre-authen mac-authen enable
```

13.5.53 authentication redirect-acl original-url enable

Function

The **authentication redirect-acl original-url enable** command configures the redirect URL to carry the original URL when Portal-authenticated users who match a redirect ACL are forcibly redirected for another forcible Portal authentication.

The **undo authentication redirect-acl original-url enable** command restores the default configuration.

By default, the redirect URL does not carry the original URL.

Format

authentication redirect-acl original-url enable

undo authentication redirect-acl original-url enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrator may need to redirect the Portal-authenticated users who match a redirect ACL to a specified web page for another forcible Portal authentication. By default, the redirect URL does not carry the original URL accessed by users. After successful forcible authentication, the authentication server cannot obtain the original URL, causing the failure to access the original URL. To resolve this problem, run the **authentication redirect-acl original-url enable** command to configure the redirect URL to carry the original URL.

Precautions

Only the users who have passed Portal authentication and match a redirect ACL can be redirected to a specified web page for another forcible Portal authentication.

Before the function takes effect, you must run the **url-parameter** command in the Portal server template view to configure the original URL parameter to be carried in the redirect URL.

Example

Configure the redirect URL to carry the original URL.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication redirect-acl original-url enable
```

13.5.54 authentication single-access

Function

The **authentication single-access** command configures the device to allow users to access in only one authentication mode.

The **undo authentication single-access** command restores the default setting.

By default, the device allows users to access in different authentication modes.

Format

authentication single-access

undo authentication single-access

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

After hybrid authentication is configured, the device by default allows users to access in different authentication modes. You can run the **authentication single-access** command to disable this default function. The device then allows users to access in only one authentication mode and does not process the packets of other authentication modes.

Example

In the authentication profile **authen1**, configure the device to allow users to access in only one authentication mode.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication single-access
```

13.5.55 authentication single-stack-control enable

Function

The **authentication single-stack-control enable** command enables the single-stack authentication function.

The **undo authentication single-stack-control enable** command disables the single-stack authentication function.

By default, the single-stack authentication function is disabled.

NOTE

This command takes effect only on the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

This command does not take effect on other switch models. However, it can be run to deliver configurations to ASs when the device functions as an SVF parent.

Format

authentication single-stack-control { **ipv4** | **ipv6** } **enable**

undo authentication single-stack-control enable

Parameters

Parameter	Description	Value
ipv4	Enables the single-stack authentication function for IPv4 traffic.	-
ipv6	Enables the single-stack authentication function for IPv6 traffic.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, access control is not performed for IPv4 or IPv6 traffic. You can use this command to configure single-stack authentication to control IPv4 or IPv6 traffic separately.

Precautions

This function takes effect only on wired Portal users.

Example

Enable single-stack authentication for IPv6 traffic in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication single-stack-control ipv6 enable
```

13.5.56 authentication speed-limit auto

Function

The **authentication speed-limit auto** command enables the device to dynamically adjust the rate of packets from NAC users.

The **undo authentication speed-limit auto** command disables the device from dynamically adjusting the rate of packets from NAC users.

By default, the device does not dynamically adjust the rate of packets from NAC users.

Format

authentication speed-limit auto

undo authentication speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lot of NAC users send authentication or log off requests to the device, the CPU usage may be overloaded especially when the CPU or memory usage is already high (for example, above 80%). After the device is enabled to dynamically adjust the rate of packets from NAC users, the device limits the number of NAC packets received per second if the CPU or memory usage is high. This function reduces loads on the device CPU.

Example

Enable the device to dynamically adjust the rate of packets from NAC users.

```
<HUAWEI> system-view
[HUAWEI] authentication speed-limit auto
```

13.5.57 authentication termination-action reauthenticate

Function

The **authentication termination-action reauthenticate** command configures the device to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

The **undo authentication termination-action** command restores the default setting.

By default, the device is not configured to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

Format

authentication termination-action reauthenticate

undo authentication termination-action

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RADIUS server uses the **Session-Timeout** attribute to control the remaining online time of a user, and uses the **Termination-Action** attribute to determine whether to re-authenticate the user when the timeout interval expires. By default, if the RADIUS server delivers **Session-Timeout** but no **Termination-Action**, the device disconnects users when the time exceeds the value of **Session-Timeout**. To re-authenticate users without modifying the server configuration, you can run this command to configure the device to re-authenticate users when the timeout interval expires.

Precautions

Only 802.1X authentication and MAC address authentication on Layer 2 interfaces support this function.

Example

In authentication profile **authen1**, configure the device to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication termination-action reauthenticate
```

13.5.58 authentication timer handshake-period

Function

The **authentication timer handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer handshake-period** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer handshake-period *handshake-period*

undo authentication timer handshake-period

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer in the range from 5 to 7200, in seconds.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the handshake with pre-connection users and authorized users using the **authentication handshake** command, you can run the **authentication timer handshake-period** command to set the handshake interval. After that, if a user does not respond to the handshake request from the device within the handshake interval, the device deletes the user entry.

Precautions

- This command applies only to MAC address authentication, Layer 3 Portal authentication and 802.1X authentication.
- For Layer 3 Portal authentication users, only those who go online through S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.
- This function takes effect only for the wired users. For wired users who do not obtain IP addresses within 30 minutes, traffic detection will be performed (detection process can be seen as the following precautions). If traffic passes through the device, users are online. If no traffic passes through the device, users go offline.
- This function takes effect only for users who go online after this function is successfully configured.
- The handshake function is implemented using ARP probe packets or neighbor discovery (ND) probe packets.
- The handshake function can also be implemented by detecting whether there is user traffic on the access device. Assuming that the handshake interval is **3n**, the device will detect user traffic at **n** and **2n**. The following uses the **0-n** period as an example. The process during the **n-2n** period is similar to that during **0-n**. (This process applies only to authentication users who go online from the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI. Other switch models do not detect user traffic and send probe packets at **n** and **2n**.)
  - If user traffic passes the device during the **0-n** period, the device considers that the user is online at **n**, so it will not send a probe packet to the user, but resets the handshake interval.
  - If no user traffic passes the device during the **0-n** period, the device cannot determine whether the user is online at **n**, so it sends a probe packet to the user. If the device receives the reply packet from the user, it considers the user online and resets the handshake interval. If no reply packet is received, it considers the user offline.
  - If user traffic passes the device during the **2n-3n** period, the device considers that the user is online at **3n** and resets the handshake interval.
  - If no user traffic passes the device during the **2n-3n** period, the device cannot determine whether the user is online at **3n** and considers that the user is offline.

  If the device considers that the user is offline at **n**, **2n**, and **3n**, the device deletes all entries related to the user. To prevent the user from going offline unexpectedly when no operation is performed on the PC, do not set a short handshake period.

- For the models that do not support the handshake function implemented by detecting whether there is user traffic on the access device, if the number of ARP probe packets exceeds the default CAR value, the probe fails and the users are logged out (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.). To resolve the problem, the following methods are recommended:
  - Increase the handshake interval based on the number of users. The default handshake interval is recommended when there are less than 8000 users; the handshake interval should be no less than 600 seconds when there are more than 8000 users.
  - Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

Example

In the authentication profile **p1**, set the handshake interval of the device with pre-connection users and authorized users to 200 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer handshake-period 200
```

13.5.59 authentication timer authen-fail-aging

Function

The **authentication timer authen-fail-aging** command configures the aging time for entries of the users who fail to be authenticated.

The **undo authentication timer authen-fail-aging** command restores the default aging time for entries of the users who fail to be authenticated.

By default, the aging time for entries of the users who fail to be authenticated is 23 hours.

Format

authentication timer authen-fail-aging *aging-time*

undo authentication timer authen-fail-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After network access policies are configured for users who fail to be authenticated, the device creates entries for these users. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.

The entries of the users who fail to be authenticated share device resources with the entries of the users who are authenticated. If there are excess entries of the users who fail to be authenticated, other users fail to be authenticated. To solve this problem, run the **authentication timer authen-fail-aging** command to reduce the aging time for entries of the users who fail to be authenticated. In addition, if the time that the users who fail to be authenticated have network access policies should be shortened, you can run this command to decrease the aging time for the user entries.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only wired users support this function.

This function controls the aging time of user entries in the **Client-no-resp**, **Aaa-server-down** or **web-server-down** state.

Example

In the authentication profile **p1**, configure the aging time for entries of the users who fail to be authenticated to 3600 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer authen-fail-aging 3600
```

13.5.60 authentication timer authorize-keep-aging

Function

The **authentication timer authorize-keep-aging** command configures the aging time for entries of online users who retain original network access rights.

The **undo authentication timer authorize-keep-aging** command restores the default setting.

By default, the aging time for entries of online users who retain the original network access rights is 0. That is, these entries are not aged out by default.

Format

authentication timer authorize-keep-aging *aging-time*

undo authentication timer authorize-keep-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **authentication event action authorize keep** command is run, if the authentication server is Down or does not respond, online users retain the original network access rights. In this case, the device creates entries for the online users who retain the original network access rights. If the authentication server is always Down or does not respond, these users always retain the original network access rights. To prevent this problem, run the **authentication timer authorize-keep-aging** command to adjust the aging time of these online user entries. When the aging time expires, these online users are logged out.

Precautions

The **authentication timer authorize-keep-aging** command configuration takes effect after the **authentication event authen-server-down action close re-authen** command is executed to disable re-authentication when the authentication server is Down.

Example

Set the aging time for entries of online users who retain the original network access rights to 600s.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer authorize-keep-aging 600
```

13.5.61 authentication timer pre-authen-aging

Function

The **authentication timer pre-authen-aging** command configures the aging time for pre-connection user entries.

The **undo authentication timer pre-authen-aging** command restores the default aging time for pre-connection user entries.

By default, the aging time for pre-connection user entries is 23 hours.

Format

authentication timer pre-authen-aging *aging-time*

undo authentication timer pre-authen-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a pre-connection is established between the device and a user, the device creates the pre-connection user entry. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.

The pre-connection user entries share device resources with the entries of the users who are authenticated. If there are excess pre-connection user entries, other users fail to be authenticated. To solve this problem, run the **authentication timer pre-authen-aging** command to reduce the aging time for the pre-connection user entries. In addition, if the time that the pre-connection users have network access policies should be extended, you can run this command to increase the aging time for the pre-connection user entries.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only wired users support this function.

Example

In the authentication profile **p1**, configure the aging time for the pre-connection user entries to 3600 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] authentication timer pre-authen-aging 3600
```

13.5.62 authentication timer re-authen

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail authentication.

The **undo authentication timer re-authen** command restores the default setting.

By default, for wired users, the device re-authenticates pre-connection users or users who fail authentication at an interval of 60 seconds; for wireless users, the device re-authenticates pre-connection users or users who fail authentication at an interval of 0 seconds, that is, the re-authentication function is disabled for pre-connection users or users who fail authentication; for wireless users, the device re-authenticates pre-connection users or users who fail authentication at an interval of 300 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* [**wlan-user**] | **authen-fail** *re-authen-time* [**wlan-user**] }

undo authentication timer re-authen { **pre-authen** [**wlan-user**] | **authen-fail** [**wlan-user**] }

NOTE

Only S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **wlan-user** parameter.

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value can be 0 or an integer in the range from 30 to 7200, in seconds. The value 0 indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail authentication.	The value can be 0 or an integer in the range from 30 to 7200, in seconds. The value 0 indicates that the re-authentication function is disabled for users who fail authentication.

Parameter	Description	Value
wlan-user	Indicates wireless users. If this parameter is not specified, the user type is wired users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates user entries when network access rights are assigned to pre-connection users or users who fail authentication. To enable users to pass authentication in real time, the device periodically re-authenticates pre-connection users or users who fail authentication according to user entries. Administrators can adjust the re-authentication interval based on the actual network requirements.

Precautions

This command applies only to 802.1X authentication and MAC address authentication.

This function takes effect only for users who go online after this function is successfully configured.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

If a static user that has 802.1X authentication configured enters the pre-connection state after failing authentication, 802.1X authentication will be performed. During 802.1X authentication, the re-authentication interval specified by the **pre-authen** *re-authen-time* parameter does not take effect. If 802.1X authentication fails, the re-authentication interval takes effect, and re-authentication will be triggered for the static user based on this interval.

If both 802.1X authentication and MAC address authentication are configured, within the re-authentication interval specified by the **pre-authen** *re-authen-time* parameter, MAC address authentication is performed first, and 802.1X authentication is performed if MAC address authentication fails.

Example

In the authentication profile **authen1**, set the interval for re-authenticating users who fail authentication to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] authentication timer re-authen authen-fail 300
```

13.5.63 authentication traffic-control strict

Function

The **authentication traffic-control strict** command enables strict control on IPv4 traffic of users in pre-connection state.

The **undo authentication traffic-control strict** command restores the default configuration.

By default, strict control on IPv4 traffic of users in pre-connection state is disabled.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S support this function.

Format

authentication traffic-control strict

undo authentication traffic-control strict

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IPv4 traffic of users in pre-connection state is processed as follows:

- IPv4 unicast packets: discarded
- IPv4 multicast, broadcast, ARP, and DHCP packets: forwarded

After the **authentication traffic-control strict** command is run to enable strict control on IPv4 traffic of users in pre-connection state, IPv4 multicast, broadcast, ARP, and DHCP packets of these users are also discarded in addition to IPv4 unicast packets.

Precautions

- For details about IPv6 traffic forwarding behaviors and control, see the **authentication ipv6-control enable** command.

- In the following scenarios, the default IPv4 traffic forwarding behaviors are retained for users in pre-connection state, regardless of whether the **authentication traffic-control strict** command is configured:
  - Authentication is configured on a VLANIF interface.
  - The device functions as an AS in the policy association or SVF scenario.
  - An authentication-free rule is configured globally.
  - Portal authentication is configured in an authentication profile.
  - Authorization is configured for users in pre-connection state.

Example

Enable strict control on IPv4 traffic of users in pre-connection state.

```
<HUAWEI> system-view
[HUAWEI] authentication traffic-control strict
```

13.5.64 authentication trigger-condition (802.1X authentication)

Function

The **authentication trigger-condition** command configures the packet types that can trigger 802.1X authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger 802.1X authentication.

Format

authentication trigger-condition { **dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet** } *

undo authentication trigger-condition [**dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet**] *

Parameters

Parameter	Description	Value
dhcp	Triggers 802.1X authentication through DHCP packets.	-
arp	Triggers 802.1X authentication through ARP packets.	-
dhcpv6	Triggers 802.1X authentication through DHCPv6 packets.	-
nd	Triggers 802.1X authentication through ND packets.	-

Parameter	Description	Value
any-l2-packet	Triggers 802.1X authentication through any packets. For multicast packets, the corresponding protocol needs to be enabled, otherwise 802.1X authentication cannot be triggered. **NOTE** If only this parameter is specified in the command, DHCP, ARP, DHCPv6, and ND packets cannot trigger 802.1X authentication.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After 802.1X authentication is enabled, the device can trigger 802.1X authentication on users by default when receiving DHCP, DHCPv6, ND, or ARP packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger 802.1X authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger 802.1X authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger 802.1X authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

If a static IPv4 address is configured for a client, 802.1X authentication cannot be triggered because they do not exchange DHCP, DHCPv6, ND, or ARP packets. You can run the **authentication trigger-condition any-l2-packet** command to trigger 802.1X authentication through any packets. To prevent unauthorized users from occupying user entries on the device maliciously, you are advised to configure the function of triggering 802.1X authentication through any packets on the access device, and run the **authentication mode max-user** *max-user-number* command in the authentication profile view to configure the maximum number of access users allowed on an interface. The recommended value is 10.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

To allow BPDUs to trigger 802.1X authentication, you must enable the function corresponding to the BPDUs globally. For example, to allow LLDPDUs to trigger 802.1X authentication, run the **lldp enable** command to enable LLDP globally.

When **any-l2-packet** is configured and 802.1X authentication is enabled on an interface, EAP packets sent from a client trigger 802.1X authentication first.

In a policy association scenario, 802.1X authentication can only be triggered by EAP or DHCP or ARP or DHCPv6 or ND packets.

When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the **ip-static-user enable** and **authentication trigger-condition any-l2-packet** commands are both configured, user authentication cannot be triggered by any packets.

When the pre-connection function is disabled and only 802.1X authentication is enabled on the interface, you need to use the **dot1x unicast-trigger** command to enable 802.1X authentication triggered by unicast packets so that the packet type configured in this command can trigger authentication.

Example

In the 802.1X access profile **d1**, configure the device to use DHCP packets to trigger 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] authentication trigger-condition dhcp
```

13.5.65 authentication trigger-condition (MAC address authentication)

Function

The **authentication trigger-condition** command configures the packet types that can trigger MAC address authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger MAC address authentication.

Format

authentication trigger-condition { **dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet** } *

undo authentication trigger-condition [**dhcp** | **arp** | **dhcpv6** | **nd** | **any-l2-packet**] *

Parameters

Parameter	Description	Value
dhcp	Triggers MAC address authentication through DHCP packets.	-
arp	Triggers MAC address authentication through ARP packets.	-
dhcpv6	Triggers MAC address authentication through DHCPv6 packets.	-
nd	Triggers MAC address authentication through ND packets.	-
any-l2-packet	Triggers MAC address authentication through any packets. For multicast packets, the corresponding protocol needs to be enabled, otherwise MAC authentication cannot be triggered. **NOTE** If only this parameter is specified in the command, DHCP, ARP, DHCPv6, and ND packets cannot trigger MAC address authentication.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication is enabled, the device can trigger MAC address authentication on users by default when receiving DHCP/ARP/DHCPv6/ND packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger MAC address authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger MAC address authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger MAC address authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

If a static IPv4 address is configured for a client, MAC address authentication cannot be triggered because they do not exchange DHCP or ARP packets. You can run the **authentication trigger-condition any-l2-packet** command to trigger MAC address authentication through any packets. To prevent unauthorized users from occupying user entries on the device maliciously, you are advised to configure the function of triggering MAC address authentication through any packets on the access device, and run the **authentication mode max-user** *max-user-number* command in the authentication profile view to configure the maximum number of access users allowed on an interface. The recommended value is 10.

Precautions

- MAC address authentication configured on a VLANIF interface can be triggered by ARP or ND packets if the device has learned the ARP or ND entries of user terminals.
- This function takes effect only for users who go online after this function is successfully configured.
- There is a situation that you should notice. A device is configured to trigger MAC address authentication through DHCP packets and DHCP options are used as the user names for MAC address authentication (for the configuration of user names in MAC address authentication, see **mac-authen username**). If the authentication server delivers Huawei extended RADIUS attribute HW-Forwarding-VLAN (No. 26-161) to the device, the user packet must carry double VLAN tags and the outer VLAN ID cannot be the same as the ID of HW-Forwarding-VLAN; otherwise, the delivered attribute cannot take effect.
- Only wired users support MAC address authentication triggered by DHCP/ARP/DHCPv6/ND/any packets. For wireless users, MAC address authentication is triggered by association packets.
- After the **authentication trigger-condition** { **dhcp** | **dhcpv6** | **nd** } * command is run, static users cannot go online.
- To allow BPDUs to trigger MAC address authentication, you must enable the function corresponding to the BPDUs globally. For example, to allow LLDPDUs to trigger MAC address authentication, run the **lldp enable** command to enable LLDP globally.
- In a policy association scenario, MAC address authentication can only be triggered by DHCP or ARP or DHCPv6 or ND packets.
- When MAC address authentication is performed for IP phones and the voice VLAN service is deployed, if the **authentication trigger-condition any-l2-packet** command is run to configure the device to trigger MAC address authentication through any packets, you need to run the **authentication mac-move enable** command to configure MAC address migration and run the **authentication mac-move detect enable** command to configure the device to detect users' online status before MAC address migration.
- When **any-l2-packet** is configured and 802.1X authentication is enabled on an interface, EAP packets sent from a client trigger 802.1X authentication first.
- When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the **ip-static-user enable** and **authentication trigger-condition any-l2-packet** commands are both configured, user authentication cannot be triggered by any packets.

Example

In the MAC access profile **m1**, configure the device to trigger MAC address authentication only through ARP packets.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] authentication trigger-condition arp
```

13.5.66 authentication trigger-condition dhcp dhcp-option

Function

The **authentication trigger-condition dhcp dhcp-option** command enables the device to send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

The **undo authentication trigger-condition dhcp dhcp-option** command restores the default configuration.

By default, the device does not send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

Format

authentication trigger-condition dhcp dhcp-option *option-code*

undo authentication trigger-condition dhcp dhcp-option *option-code*

Parameters

Parameter	Description	Value
option-code	Specifies the option that the device sends to the authentication server.	The value is fixed as 82.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Option82 records information about DHCP user locations and services (voice and data services). After this command is run, if the device can trigger MAC address authentication though DHCP packets, it sends Option82 information to the authentication server when triggering MAC address authentication through DHCP packets. Based on the user information recorded in Option82, the authentication server then assigns different network access rights to users with different services in different locations. This implements accurate control on the network access rights of each user.

Precautions

- MAC address authentication users who go online through VLANIF interfaces do not support this function.
- This function takes effect only for users who go online after this function is successfully configured.
- Only wired users support MAC address authentication triggered by DHCP/ARP/DHCPv6/ND/any packets. For wireless users, MAC address authentication is triggered by association packets.

Example

In the MAC access profile **m1**, enable the device to send Option82 information to the authentication server when triggering MAC address authentication through DHCP packets.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] authentication trigger-condition dhcp dhcp-option 82
```

13.5.67 authentication unified-mode

Function

The **authentication unified-mode** command switches the NAC mode to unified mode.

The **undo authentication unified-mode** command switches the NAC mode to common mode.

By default, the unified NAC configuration mode is used.

Format

authentication unified-mode

undo authentication unified-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with the common mode, the unified mode uses the modular configuration, making the configuration clearer and configuration model easier to understand.

Considering advantages of the unified mode, you are advised to deploy NAC in unified mode. You can run the **authentication unified-mode** command to switch the NAC mode to unified mode.

Precautions

- Starting from V200R005C00, the default NAC mode changes from common mode to unified mode. Therefore, if the system software of a switch is upgraded from a version earlier than V200R005C00 to V200R005C00 or a later version, the switch automatically runs the **undo authentication unified-mode** command to configure the NAC mode to common mode.
- After the common mode and unified mode are switched, the device automatically restarts, causing service interruption.
- In V200R008C00, some NAC commands do not differentiate the common and unified modes. Their formats and views remain unchanged after being switched from one mode to the other. After devices are switched from the common mode in V200R008C00 or later versions to the unified mode in V200R009C00 or later versions, these NAC commands can be switched to the unified mode.
- In the unified mode, only the commands of the common mode are unavailable; in the common mode, only the commands of the unified mode are unavailable. In addition, after the configuration mode is switched, the commands supported by both the common mode and unified mode still take effect.

Example

Switch the NAC mode to unified mode.

```
<HUAWEI> system-view
[HUAWEI] authentication unified-mode
```

13.5.68 authentication user-alarm percentage

Function

The **authentication user-alarm percentage** command sets alarm thresholds for the percentage of successfully authenticated NAC users.

The **undo authentication user-alarm** command restores the default alarm thresholds for the percentage of successfully authenticated NAC users.

By default, the lower alarm threshold for the percentage of successfully authenticated NAC users is 50, and the upper alarm threshold is 100.

Format

authentication user-alarm percentage *percent-lower-value percent-upper-value*

undo authentication user-alarm

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100, and must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the number of successfully authenticated NAC users reaches a specified percentage, the device generates an alarm. You can run the **authentication user-alarm percentage** command to set the upper and lower alarm thresholds for this percentage.

When the percentage of successfully authenticated NAC users against the maximum number of users allowed by the device is greater than or equal to the upper alarm threshold, the device generates an alarm. When this percentage reaches or falls below the lower alarm threshold, the device generates a clear alarm.

Example

Set the lower and upper alarm thresholds for the percentage of successfully authenticated NAC users to 30 and 80, respectively.

```
<HUAWEI> system-view
[HUAWEI] authentication user-alarm percentage 30 80
```

13.5.69 authentication-profile (Interface view or VAP profile view)

Function

The **authentication-profile** command applies an authentication profile to the interface or VAP profile.

The **undo authentication-profile** command restores the default setting.

By default, no authentication profile is applied to the interface or VAP profile.

Format

authentication-profile *authentication-profile-name*

undo authentication-profile

Parameters

Parameter	Description	Value
authentication-profile-name	Specifies the name of an authentication profile.	The value must be an existing authentication profile name.

Views

Interface view, or VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An authentication profile uniformly manages NAC configuration. The authentication profile is bound to the interface or VAP profile view to enable NAC, implementing access control on the users in the interface or VAP profile. The authentication type of the users in the interface or VAP profile is determined by the access profile bound to the authentication profile.

Prerequisites

An authentication profile has been created using the **authentication-profile** command in the system view.

Precautions

When configuring NAC, pay attention to the following points:

- VLANIF interfaces, Ethernet interfaces, GE interfaces, MultiGE interfaces, XGE interfaces, 25GE interface, 40GE interfaces, 100GE interfaces, Eth-Trunks, port groups, and VAP profiles support NAC. The support for NAC on different interfaces is as follows:
  - The VLANIF interface does not support 802.1X authentication.
  - Layer 2 interfaces and VLANIF interfaces support MAC address authentication. When MAC address authentication is enabled on a VLANIF interface, the IP address in the ARP packet that triggers MAC address authentication must be on the same network segment as the IP address of the VLANIF interface. (Only S5720I-SI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.)
  - The support for Portal authentication varies depending on different interfaces, routed main interfaces (Only S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI) support only Layer 3 Portal authentication, Layer 2 interfaces support only Layer 2 Portal authentication, and VLANIF interfaces support both Layer 2 and Layer 3 Portal authentication.
  - The VLANIF interface corresponding to the super VLAN does not support Portal authentication.
- When the user VLAN or interface type needs to be switched for an online user or a user in pre-connection state, you are advised to log out the user or shut down the interface first. Otherwise, the client may send an ARP packet to go online in VLAN 1 during the switching. As a result, the IP address of the user cannot be updated later.
- For the access of wireless users through APs, ensure that the APs can be authenticated (for example, adding the APs to static users) when NAC authentication is deployed for users. Otherwise, the wireless users cannot be authenticated.
- For S5731-S, S5731S-S, S5720I-SI, S5720-LI, and S5720S-LI, the priority of a traffic policy is higher than that of an authentication policy. As a result, users may be able to access the network before being authenticated.
- NAC authentication cannot be enabled both on a Layer 2 Ethernet interface and the VLANIF interface mapping the VLAN of the Ethernet interface. Otherwise, the users have no network access rights after connecting to the network. In wireless scenarios, NAC authentication cannot be enabled both in VAP profiles and on VLANIF interfaces. In direct forwarding mode, NAC authentication configured on a VLANIF interface takes effect only when the device is connected in off-path mode.
- After enabling NAC on an interface, you cannot run the following commands on the interface. Similarly, after running the following commands on an interface, you cannot enable NAC on the interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.

Command	Function
mac-address learning disable	Disables MAC address learning on an interface.
port link-type dot1q-tunnel	Sets the link type of an interface to QinQ.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Configures VLAN mapping on an interface.
port vlan-stacking	Configures selective QinQ.
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.
user-bind ip sticky-mac	Enables the device to generate snooping MAC entries.

- After the encapsulation mode of packets allowed to pass a Layer 2 sub-interface is set to default using the **encapsulation** command, NAC cannot be configured on the main interface of the Layer 2 sub-interface.
- After NAC is configured on the main interface, the **bridge-domain (Layer 2 sub-interface view)** command cannot be executed on its Layer 2 sub-interface to associate with BDs. Similarly, NAC cannot be executed on the main interface if the **bridge-domain (Layer 2 sub-interface view)** command is configured on its Layer 2 sub-interface to associate with BDs.

Example

Apply the authentication profile **m1** to VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name m1
[HUAWEI-authen-profile-m1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] authentication-profile m1
```

13.5.70 authentication-profile (system view)

Function

The **authentication-profile** command creates an authentication profile and displays the authentication profile view.

The **undo authentication-profile** command deletes the authentication profile.

By default, the device has six built-in authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile.

Format

authentication-profile name *authentication-profile-name*

undo authentication-profile name *authentication-profile-name*

Parameters

Parameter	Description	Value
name *authentication-profile-name*	Specifies the name of an authentication profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NAC can implement access control on users. The device uses authentication profiles to uniformly manage NAC configuration so that users can easily configure NAC functions. The parameters (for example, the bound access profile and authentication type) in the authentication profile can be configured to provide various access control modes for different users. After the configuration is complete, the authentication profile is applied to the interface or VAP profile to enable NAC.

Follow-up Procedure

1. Configuring authentication profiles: Configure the access profile, and authorization information in the authentication profiles.
2. Applying authentication profiles: Run the authentication-profile **(Interface view or VAP profile view)** command to apply the authentication profiles to the interface or VAP profile.

Precautions

- The built-in authentication profile **default_authen_profile** and the compatibility profile converted after an upgrade are not counted in the configuration specification. The six built-in authentication profiles (default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile) can be modified and applied, but cannot be deleted.

- Before deleting an authentication profile, ensure that this profile is not bound to any interface or VAP profile. You can run the **display authentication-profile configuration** command to check whether the authentication profile is bound to an interface or VAP profile

Example

Create the authentication profile named **mac_authen_profile1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name mac_authen_profile1
```

13.5.71 band-width share-mode

Function

The **band-width share-mode** command enables the bandwidth share mode.

The **undo band-width share-mode** command restores the default configuration.

By default, the bandwidth share mode is disabled.

NOTE

This command is only supported by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

band-width share-mode

undo band-width share-mode

Parameters

None

Views

System view, AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On a home network, all family members go online using the same account. To improve service experience of family members, you can enable the bandwidth share mode so that all members can share the bandwidth.

Precautions

- This function is not supported in the direct forwarding mode of wireless traffic.
- If this command is run in the system view, it takes effect for all new online users who connected to the device. If this command is run in the AAA domain view, it takes effect only for new online users in the domain.
- If the local or remote RADIUS server does not assign CAR settings to the users who will go online and the online users, the share mode is invalid to the users.
- If the bandwidth share mode is enabled and different users use the same account for authentication, the users going online with no CAR settings assigned will not be affected when CAR settings are assigned to the users who go online later.

Example

Enable the bandwidth share mode in the system view.

```
<HUAWEI> system-view
[HUAWEI] band-width share-mode
```

Enable the bandwidth share mode in the AAA domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] band-width share-mode
```

13.5.72 capwap fragment

Function

The **capwap fragment** command configures the rate for wireless packet fragmentation.

The **undo capwap fragment** command cancels the rate configuration for wireless packet fragmentation.

By default, the rate for wireless packet fragmentation is not configured.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this function.

Format

capwap fragment cir *cir-value* [**cbs** *cbs-value*]

undo capwap fragment

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is an integer ranging from 24 to 104857600, in kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the committed volume of burst traffic that can pass through an interface.	The value is an integer ranging from 10000 to 134217728, in bytes. By default, the CBS is 125 times the CIR. If the CIR multiplied by 125 is less than 10000, the default CBS is 10000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In wireless scenarios, a large number of burst ultra-long packets (longer than 1500 bytes) may exist and exceed the device forwarding performance. To ensure correct packet forwarding in such cases, you can run the **capwap fragment** command to configure the rate for wireless packet fragmentation. If the rate is not configured, packets are fragmented at the maximum rate supported by the device.

Precautions

Limiting the rate for fragmenting wireless packets affects wireless packet forwarding performance.

Example

Set the CIR to 10000 kbit/s for wireless packet fragmentation.

```
<HUAWEI> system-view
[HUAWEI] capwap fragment cir 10000
```

13.5.73 capwap unknown-unicast

Function

The **capwap unknown-unicast** command configures the rate for forwarding unknown unicast packets in wireless scenarios.

The **undo capwap unknown-unicast** command restores the default rate for forwarding unknown unicast packets in wireless scenarios.

By default, the CIR is 1600000 kbit/s and the CBS is 250000 bytes for unknown wireless unicast packets.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this function.

Format

capwap unknown-unicast cir *cir-value* [**cbs** *cbs-value*]

undo capwap unknown-unicast

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is 0 or an integer ranging from 24 to 104857600, in kbit/s. The value 0 indicates that no rate limit is configured for forwarding unknown unicast packets in wireless scenarios and these packets are forwarded at the maximum rate supported by the device.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the committed volume of burst traffic that can pass through an interface.	The value is an integer ranging from 10000 to 134217728, in bytes. By default, the CBS is 125 times the CIR. If the CIR multiplied by 125 is less than 10000, the default CBS is 10000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In wireless scenarios, a large number of burst unknown unicast packets may exist and exceed the device forwarding performance. To ensure correct packet replication and forwarding in such cases, you can run the **capwap unknown-unicast** command to configure the rate for forwarding unknown unicast packets.

Precautions

Limiting the rate for forwarding wireless unknown unicast packets affects wireless packet forwarding performance.

Example

Set the CIR to 2000000 kbit/s and the CBS to 300000 bytes for forwarding unknown wireless unicast packets.

```
<HUAWEI> system-view
[HUAWEI] capwap unknown-unicast cir 2000000 cbs 300000
```

13.5.74 cut access-user ucl-group

Function

The **cut access-user ucl-group** command forces UCL group users offline.

Format

cut access-user ucl-group { *group-index* | **name** *group-name* }

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The UCL group must exist.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a user goes online, if you want to modify the user's network access rights or detect that the user is unauthorized, run this command to force the user offline.

Example

Force UCL group users offline.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] cut access-user ucl-group name test
```

13.5.75 device-type

Function

The **device-type** command sets a terminal type identifier.

The **undo device-type** command deletes a terminal type identifier that has been set.

By default, no terminal type identifier exists in the system.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

device-type *device-name*

undo device-type

Parameters

Parameter	Description	Value
device-name	Specifies a terminal type identifier.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value cannot be - or --, and cannot contain ?, ', ".

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a terminal type identifier is configured in a terminal type identification profile, the terminal type can be identified in the profile. Assume that the terminal type identifier is set to **test**. If the MAC address, user agent, or DHCP Option information that an AC receives from a terminal matches the identification rule configured in the terminal type profile, the terminal type is **test**. This helps administrators to perform access control and rights management for the terminal based on the identified terminal type.

Precautions

The **device-type** command is cyclic in nature, and only the latest configuration takes effect.

Example

In the terminal type identification profile **test**, configure the terminal type identifier **test_1**.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] device-type test_1
```

13.5.76 device-profile

Function

The **device-profile** command creates a terminal type identification profile and enters the terminal type identification profile view, or directly enters the view of a terminal type identification profile that has already been created.

The **undo device-profile** command deletes a terminal type identification profile that has been created.

By default, no terminal type identification profile is created.

NOTE

This function is supported only by the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H and takes effect only for wireless access users.

Format

device-profile profile-name *profile-name*

undo device-profile { **all** | **profile-name** *profile-name* }

Parameters

Parameter	Description	Value
profile-name *profile-name*	Specifies the name of a terminal type identification profile.	The value is a string of 1 to 31 case-sensitive characters without characters including spaces and the following:/ \ : * ? " < > | @ ' %. The value cannot be - or --.
all	Deletes all terminal type identification profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

With the development of Internet, many enterprises allow employees to wirelessly access the enterprise intranet using their own intelligent devices such as cellphones, tablets, and laptops, which satisfies employees' pursuit of new technology and desire of being unique, and improves their efficiency as well. This is called Bring Your Own Device (BYOD). However, access to enterprise intranet through PCs may cause potential security risks, and traditional security technology based on user identity authentication and authorization can no longer guarantee network security. It is in such a background that the terminal type identification technology comes out. With this technology, the types of the devices that employees use to access the intranet can be identified, facilitating access control. During the implementation of BYOD, administrators can limit intranet access rights to specified types of mobile devices and perform authentication and authorization based on users, device types, access time, access points, and environment information about the devices.

A terminal type identification profile is configured with terminal types that can be identified by devices, and identification rules. With the configured identification rules, the types of devices using which employees access the intranet can be identified, helping administrators to control employees' access rights.

Example

Create a terminal type identification profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
```

13.5.77 device-sensor dhcp option

Function

The **device-sensor dhcp option** command enables the DHCP-based terminal type awareness function.

The **undo device-sensor dhcp option** command disables the DHCP-based terminal type awareness function.

By default, the DHCP-based terminal type awareness function is disabled.

Format

device-sensor dhcp option *option-code* &<1-6>

undo device-sensor dhcp option *option-code* &<1-6>

Parameters

Parameter	Description	Value
option-code	Specifies the DHCP option field that the device needs to resolve. The option fields in a DHCP packet carry the control information and parameters, for example, terminal type.	The value is an integer that ranges from 1 to 254.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

After the DHCP-based terminal type awareness function is enabled, the device can resolve the option fields that carry terminal type information in the received DHCP Request packets. The device then sends the option information to the RADIUS server through RADIUS accounting packets. Through the option information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- To make this command take effect, you must run the **dhcp snooping enable** command on the interfaces or in VLANs.

Example

Set the option fields to be resolved by the device to option 60.

```
<HUAWEI> system-view
[HUAWEI] device-sensor dhcp option 60
```

13.5.78 device-sensor lldp tlv

Function

The **device-sensor lldp tlv** command enables the LLDP-based terminal type awareness function.

The **undo device-sensor lldp tlv** command disables the LLDP-based terminal type awareness function.

By default, the LLDP-based terminal type awareness function is disabled.

Format

device-sensor lldp tlv *tlv-type* &<1-4>

undo device-sensor lldp tlv

Parameters

Parameter	Description	Value
tlv-type	Specifies the LLDP TLV type as the terminal type to be aware of the device.	The value is an integer that can be 1, 2, 5, 6, 7, 8, and 127. The values are as follows: ● 1: Chassis ID TLV, indicating the bridge MAC address of the device ● 2: Port ID TLV, indicating the port identifying the LLD PDU sending end ● 5: System Name TLV, indicating the device name ● 6: System Description TLV, indicating the system description ● 7: System Capabilities TLV, indicating the system capabilities ● 8: Management Address TLV, indicating the management address ● 127: Organization Specific TLV, indicating the user-defined organization information. You can run the **lldp tlv-enable med-tlv** command on the physical interface for user access to set this parameter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

Using the LLDP-based terminal type awareness function, the device parses the required TLV type containing terminal type information from the received LLDP packets. The device then sends the TLV type information to the RADIUS server through a RADIUS accounting packet. Through the TLV type information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- The command takes effect only when the LLDP function is enabled on the device and the connected peer device.
- This command takes effect only when terminals connect to the device through physical interfaces, instead of logical interfaces such as Eth-Trunk interfaces.

Example

Enable the terminal type awareness function based on LLDP TLV type 5.

```
<HUAWEI> system-view
[HUAWEI] device-sensor lldp tlv 5
```

13.5.79 device-sensor cdp tlv

Function

The **device-sensor cdp tlv** command enables the CDP-based terminal type awareness function.

The **undo device-sensor cdp tlv** command disables the CDP-based terminal type awareness function.

By default, the CDP-based terminal type awareness function is disabled.

Format

device-sensor cdp tlv *tlv-type* &<1-6>

undo device-sensor cdp tlv

Parameters

Parameter	Description	Value
tlv-type	Specifies the CDP TLV type as the terminal type to be aware of the device.	The value is an integer that can be 1, 2, 3, 4, 5, and 6. The values are as follows ● 1: Device ID TLV, indicating a device ID. ● 2: Address TLV, indicating the address of the interface that sends CDP packets. ● 3: Port ID TLV, indicating the ID of the interface that sends CDP packets. ● 4: Function TLV, indicating the device function. ● 5: Version TLV, indicating the software version. ● 6: Platform, indicating the hardware platform.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

Using the CDP-based terminal type awareness function, the device parses the required TLV type containing terminal type information from the received CDP packets. The device then sends the TLV type information to the RADIUS server through a RADIUS accounting packet. Through the TLV type information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- The command takes effect only when the CDP function is enabled on the device and the connected peer device.
- This command takes effect only when terminals connect to the device through physical interfaces, instead of logical interfaces such as Eth-Trunk interfaces.

Example

Enable the terminal type awareness function based on CDP TLV type 5.

```
<HUAWEI> system-view
[HUAWEI] device-sensor cdp tlv 5
```

13.5.80 display aaa statistics access-type-authenreq

Function

The **display aaa statistics access-type-authenreq** command displays the number of requests for MAC, Portal, or 802.1X authentication.

Format

display aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, or 802.1X authentications.

To view the number of requests for MAC, Portal, or 802.1X authentication, run the **display aaa statistics access-type-authenreq** command.

Example

Display the number of requests for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> display aaa statistics access-type-authenreq
mac     authentication request     :2
portal  authentication request     :0
dot1x   authentication request     :0
```

Table 13-41 Description of the **display aaa statistics access-type-authenreq** command output

Item	Description
mac authentication request	Number of MAC authentication requests.
portal authentication request	Number of Portal authentication requests.
dot1x authentication request	Number of 802.1X authentication requests.

13.5.81 display access-context profile

Function

The **display access-context profile** command displays the configuration of a user context profile.

Format

display access-context profile [**name** *profile-name*]

Parameters

Parameter	Description	Value
name *profile-name*	Displays the configuration of the user context profile with a specified name. If **name** *profile-name* is not specified, all user context profiles configured on the device are displayed.	The value must be the name of an existing user context profile on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a user context profile, you can run this command to check whether the configuration is correct.

Example

Display all user context profiles configured on the device.

```
<HUAWEI> display access-context profile
-------------------------------------------------------------------------------
   ID        Access-context profile name
-------------------------------------------------------------------------------
    0        p1
    1        aA
-------------------------------------------------------------------------------
   Total 2, printed 2
```

Display the configuration of the user context profile **p1**.

```
<HUAWEI> display access-context profile name p1
  Profile name                : p1
  if-match vlan-id           : 13 to 20
```

Table 13-42 Description of the **display access-context profile** command output

Item	Description
ID	Index of a user context profile.
Access-context profile name or Profile name	Name of a user context profile. To configure the parameter, run the **access-context profile name** command.

Item	Description
if-match vlan-id	VLAN matching a user context profile. To configure the parameter, run the **if-match vlan-id** command.

13.5.82 display access-author policy

Function

The **display access-author policy** command displays the configuration of a user authentication event authorization policy.

Format

display access-author policy [**name** *policy-name*]

Parameters

Parameter	Description	Value
name *policy-name*	Displays the configuration of the user authentication event authorization policy with a specified name. If **name** *policy-name* is not specified, all user authentication event authorization policies configured on the device are displayed.	The value must be the name of an existing user authentication event authorization policy on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a user authentication event authorization policy, you can run this command to check whether the configuration is correct.

Example

Display all user authentication event authorization policies configured on the device.

```
<HUAWEI> display access-author policy
-------------------------------------------------------------------------------
```

```
  ID       Access-author policy name
--------------------------------------------------------------------------------
   0       a1
   1       a2
--------------------------------------------------------------------------------
  Total 2, printed 2
```

Display the configuration of the user authentication event authorization policy **a1**.

```
<HUAWEI> display access-author policy name a1
  Policy name               : a1
  match access-context-profile p1 action authen-fail service-scheme s1
```

Table 13-43 Description of the **display access-author policy** command output

Item	Description
ID	Index of a user authentication event authorization policy.
Access-author policy name or Policy name	Name of a user authentication event authorization policy. To configure the parameter, run the **access-author policy name** command.
match access-context-profile *profile-name* action authen-fail service-scheme *scheme-name*	User authorization information specified based on a user context profile. To configure the parameter, run the **match access-context-profile action** command.

13.5.83 display access-user

Function

The **display access-user** command displays information about NAC access users.

Format

display access-user service-scheme *service-scheme*

display access-user access-type static

display access-user access-type { **dot1x** | **mac-authen** | **portal** | **none** } [**wired** | **wireless**]

display access-user event { **pre-authen** | **authen-fail** | **client-no-response** | **authen-server-down** }

display access-user ucl-group { *group-index* | **name** *ucl-group-name* } [**detail**]

display access-user option82 { **circuit-id** *text* | **remote-id** *text* }

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **wireless** parameter.

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Displays information about users assigned with a specified service scheme.	The value must be the name of an existing service scheme.
access-type	Displays information about users using a specified authentication mode.	-
dot1x	Displays information about users who pass 802.1X authentication.	-
mac-authen	Displays information about users who pass MAC address authentication.	-
portal	Displays information about users who pass Portal authentication.	-
none	Displays information about users whose AAA scheme is non-authentication.	-
static	Displays static user information.	-
event	Displays information about users in a specified authentication phase.	-
pre-authen	Displays information about users in the pre-connection phase.	-

Parameter	Description	Value
authen-fail	Displays information about users who fail to be authenticated and are assigned network access policies when the authentication server sends authentication failure packets to the device.	-
client-no-response	Displays information about 802.1X authentication users who fail to be authenticated and are assigned network access policies when the 802.1X client does not respond.	-
authen-server-down	Displays information about users who fail to be authenticated due to the Down status of the authentication server and are assigned network access policies.	-
ucl-group	Displays information about users in a specified UCL group.	-
group-index	Specifies the index of a UCL group.	The value must be an existing UCL group index.
name *ucl-group-name*	Specifies the name of a UCL group.	The value must be an existing UCL group name.
detail	Displays detailed user information.	-
option82	Displays information about MAC address authentication users who use the Option 82 field as user names.	-
circuit-id *text*	Displays information about MAC address authentication users who specify the circuit ID as user names.	The value must be existing circuit-id information.

Parameter	Description	Value
remote-id *text*	Displays information about MAC address authentication users who specify the remote ID as user names.	The value must be existing remote-id information.
wired	Displays information about wired users.	-
wireless	Displays information about wireless users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online NAC users.

Example

Display information about users who are assigned the service scheme **test**.

```
<HUAWEI> display access-user service-scheme test
------------------------------------------------------------------------------
 UserID Username               IP address       MAC            Status
------------------------------------------------------------------------------
 16018  zqm                  10.12.12.254     00e0-fcc2-0175 Pre-authen
------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Display information about users in the pre-connection phase.

```
<HUAWEI> display access-user event pre-authen
------------------------------------------------------------------------------
 UserID Username               IP address       MAC            Status
------------------------------------------------------------------------------
 16018  zqm                  10.12.12.254     00e0-fcc2-0175 Pre-authen
------------------------------------------------------------------------------
 Total: 1, printed: 1
```

NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When you run the **display access-user** command without specifying any parameter to view user information and the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following the 19th character; that is, only 22 characters are displayed. When you run the **display access-user** command with parameters specified to view detailed information about the user table, all the characters of **username** are displayed, and the rule for converting special characters remains unchanged.

Table 13-44 Description of the **display access-user** command output

Item	Description
UserID	ID automatically allocated to an online user by the device.
Username	User name.
IP address	User IP address. When both IPv4 and IPv6 addresses exist, only the IPv4 address is recorded. When only IPv6 addresses exist, only the latest updated IPv6 address is recorded.
MAC	User MAC address.
Status	User status. ● Open: For a wired user, the user goes online through the open function upon authentication failure. For wireless users, no authentication is performed. ● Success: authentication is successful ● Pre-authen: pre-authentication ● Client-no-resp: the client does not respond ● Fail-authorized: authorization upon authentication failure ● Web-server-down: web server is Down ● Aaa-server-down: AAA server is Down

13.5.84 display access-user dot1x-identity statistics

Function

The **display access-user dot1x-identity statistics** command displays statistics about Identity packets for 802.1X authentication on a switch.

Format

display access-user dot1x-identity statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the statistics about Identity packets for 802.1X authentication on a switch.

Example

Display statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> display access-user dot1x-identity statistics
----------------------------------------------------------------------
Receive(Packet)    Pass(Packet)    Drop(Packet)    Last-dropping-time
----------------------------------------------------------------------
0                  0               0               -
----------------------------------------------------------------------
```

Table 13-45 Description of the **display access-user dot1x-identity statistics** command output

Item	Description
Receive(Packet)	Total number of Identity packets for 802.1X authentication received by the switch.
Pass(Packet)	Number of Identity packets for 802.1X authentication sent to and processed by the CPU of the switch.
Drop(Packet)	Number of Identity packets for 802.1X authentication discarded by the switch.

Item	Description
Last-dropping-time	Latest time when the switch discarded Identity packets for 802.1X authentication. If no packet loss record exists on the switch, this field displays **-**.

13.5.85 display access-user https statistics

Function

The **display access-user https statistics** command displays statistics about HTTPS protocol packets sent to the CPU.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display access-user https statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display statistics about HTTPS protocol packets sent to the CPU.

```
<HUAWEI> display access-user https statistics
------------------------------------------------------------------------
Received packets:
    Tcp-syn:519

Passed packets:
    Tcp-syn:391
```

```
Dropped packets:
    Last dropping time:2019-03-12 09:26:46
    Duplicate tcp-syn within 1 second:0
    Rate-limited packets:128
```

Table 13-46 Description of the **display access-user https statistics** command output

Item	Description
Received packets: Tcp-syn	Number of HTTPS TCP handshake packets received by the switch.
Passed packets: Tcp-syn	Number of HTTPS TCP handshake packets sent to the CPU on the switch.
Dropped packets	Number of HTTPS TCP handshake packets dropped by the switch.
Last dropping time	Number of latest HTTPS TCP handshake packets dropped by the switch. If - is displayed, packet loss did not occur on the switch.
Duplicate tcp-syn within 1 second	Number of duplicate TCP handshake packets dropped by the switch within 1 second.
Rate-limited packets	Number of TCP handshake packets dropped by the switch due to rate limiting.

13.5.86 display access-user portal statistics

Function

The **display access-user portal statistics** command displays statistics about Portal protocol packets sent to the CPU.

Format

display access-user portal statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display statistics about Portal protocol packets sent to the CPU.

```
<HUAWEI> display access-user portal statistics
----------------------------------------------------------------------
Receive(Packet)    Pass(Packet)    Drop(Packet)    Last-dropping-
time
----------------------------------------------------------------------
0                  0               0               -
----------------------------------------------------------------------
...
```

Table 13-47 Description of the **display access-user portal statistics** command output

Item	Description
Receive(Packet)	Total number of Portal protocol packets received by the switch.
Pass(Packet)	Number of Portal protocol packets sent to the CPU.
Drop(Packet)	Number of Portal protocol packets discarded by the switch.
Last-dropping-time	Last time when the switch discards Portal protocol packets. If no Portal protocol packet is discarded, this parameter is displayed as **-**.

13.5.87 display access-user roam-table

Function

The **display access-user roam-table** command displays the roaming table information of a roaming user.

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support this command.

Format

display access-user roam-table [**mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **acct-session-id** *acct-session-id*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Displays the roaming table information of a roaming user with a specified MAC address.	The value is in the H-H-H format, where H is a 4-digit hexadecimal number.
ip-address *ip-address*	Displays the roaming table information of a roaming user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays the roaming table information of a roaming user with a specified IP address in a specified VPN instance.	The value must be an existing VPN instance name on the device.
acct-session-id *acct-session-id*	Displays the roaming table information of a roaming user with a specified accounting ID.	The value must be the current accounting ID of the user. For details, run the **display access-user user-id** *user-id* command to check the **User accounting session ID** field.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a user roams between different ACs, the user roaming table is generated on the AC (authentication point) before the user is re-authenticated. You can run this command to view the user roaming table information.

Precautions

In 802.1X authentication and MAC address authentication, roaming tables are generated only for accounting users, not non-accounting users.

Example

Display the roaming table information of a roaming user.

```
<HUAWEI> display access-user roam-table
 ------------------------------------------------------------------------------
 MAC            IP address                   FAC address
------------------------------------------------------------------------------
 00e0-fc12-3456  10.1.1.2                     10.137.213.119
 ------------------------------------------------------------------------------
<HUAWEI> display access-user roam-table ip-address 10.1.1.2
  User MAC                              : 00e0-fc12-3456
  User accounting session ID               : AP6050-00000000000102fa****0000023
  User IP address                       : 10.1.1.2
  IP address of foreign AC                 : 10.137.213.119
```

Table 13-48 Description of the **display access-user roam-table** command output

Item	Description
User accounting session ID	User accounting ID.
IP address/User IP address	User IP address.
MAC/User MAC	User MAC address.
FAC address/IP address of foreign AC	IP address of the AC where the user roams.

13.5.88 display access-user-num

Function

The **display access-user-num** command displays the number of current online users on a virtual access point (VAP).

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

display access-user-num [**interface wlan-dbss** *wlan-dbss-interface-id*]

Parameters

Parameter	Description	Value
interface wlan-dbss *wlan-dbss-interface-id*	Displays the number of current online users on a VAP. If this parameter is not specified, the number of current online users on all VAPs are displayed.	The value is an existing WLAN-DBSS interface id.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display access-user-num** command to view the number of current online users.

Example

Display the number of current online users on all VAPs.

```
<HUAWEI> display access-user-num
2016-09-30 11:09:27.790
----------------------------------------------------------------------
 Interface name                              online-user-num
----------------------------------------------------------------------
 Wlan-Dbss0                                          10
 Wlan-Dbss1                                           0
----------------------------------------------------------------------
 Total: 8, printed: 2
```

Table 13-49 Description of the **display access-user-num** command output

Item	Description
Interface name	WLAN-DBSS interface id.
online-user-num	Number of current online users.
Total	Total number of interfaces.
printed	Number of printed entries.

13.5.89 display ap port-auth-state

Function

The **display ap port-auth-state** command displays the authentication status of an 802.1X client.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

display ap port-auth-state { **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the authentication status of an 802.1X client with the specified AP name.	The AP name must already exist.
ap-id *ap-id*	Displays the authentication status of an 802.1X client with the specified AP ID.	The AP ID must already exist.
ap-mac *ap-mac*	Displays the authentication status of an 802.1X client with the specified AP MAC address.	The AP MAC address must already exist.
all	Displays the authentication status of all APs that are authenticated as 802.1X clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an AP is authenticated as an 802.1X client, you can run this command to check the authentication status of the AP.

Example

Display the authentication status of all APs that are authenticated as 802.1X clients.

```
<HUAWEI> display ap port-auth-state all
------------------------------------------------------------------------
AP-ID Port       Dot1x client State
------------------------------------------------------------------------
23    GE0        init
------------------------------------------------------------------------
Printed: 1
```

Table 13-50 Description of the **display ap port-auth-state** command output

Item	Description
AP-ID	AP ID.
Port	Port number.

Item	Description
Dot1x client State	Authentication status of an 802.1X client. ● init: initial ● authenticating: authenticating ● success: succeeded ● fail: failed

13.5.90 display authentication mac-move configuration

Function

The **display authentication mac-move configuration** command displays the MAC address migration configuration.

Format

display authentication mac-move configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mac-move configuration** command to view the MAC address migration configuration. The configuration includes the number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state, the period that MAC address migration users stay in the quiet state, the interval at which a device detects users' online status before user MAC address migration, and the number of detections before user MAC address migration.

Example

Display the MAC address migration configuration.

```
<HUAWEI> display authentication mac-move configuration
Mac-move vlan config:all
Mac-move quiet times:1
Mac-move quiet period(s):120
Mac-move quiet log:ENABLE
```

```
Mac-move quiet user alarm:ENABLE
Mac-move quiet user alarm lower percentage(%):
50
Mac-move quiet user alarm upper percentage(%):100
Mac-move detect:DISABLE
Mac-move detect retry-interval(s):3
Mac-move detect retry-time:1
```

Table 13-51 Description of the **display authentication mac-move configuration** command output

Item	Description
Mac-move vlan config	VLAN ID range in which MAC address migration is enabled. For details, see the **authentication mac-move enable** command.
Mac-move quiet times	Number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.
Mac-move quiet period(s)	Period that MAC address migration users stay in the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.
Mac-move quiet log	Whether a device is enabled to record logs about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-log enable** command.
Mac-move quiet user alarm	Whether a device is enabled to send alarms about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-user-alarm enable** command.

Item	Description
Mac-move quiet user alarm lower percentage(%)	Lower alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move quiet user alarm upper percentage(%)	Upper alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move detect	Whether a device is enabled to detect users' online status before user MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move detect enable** command.
Mac-move detect retry-interval(s)	Interval at which a device detects users' online status before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.
Mac-move detect retry-time	Number of detections before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.

13.5.91 display authentication mac-move quiet-user

Function

The **display authentication mac-move quiet-user** command displays information about MAC address migration users in quiet state.

Format

display authentication mac-move quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address migration users in quiet state.	-
mac-address *mac-address*	Displays information about MAC address migration users in quiet state with a specified MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run this command to view information about MAC address migration users in quiet state.

Example

Display information about all MAC address migration users in quiet state.

```
<HUAWEI> display authentication mac-move quiet-user all
Quiet MAC Information
-------------------------------------------------------------------------------
Quiet MAC                                      Quiet Remain Time(Sec)
-------------------------------------------------------------------------------
xxxx-xxxx-xxxx                                 143
-------------------------------------------------------------------------------
1 quiet MAC found, 1 printed.
```

Table 13-52 Description of the **display authentication mac-move quiet-user all** command output

Item	Description
Quiet MAC	MAC address of MAC address migration users in quiet state.
Quiet Remain Time(Sec)	Remaining quiet time of MAC address migration users in quiet state, in seconds.

13.5.92 display authentication interface

Function

The **display authentication interface** command displays the configuration of the NAC authentication mode on an interface.

Format

display authentication interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the configuration of the NAC authentication mode on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the NAC authentication mode, you can run this command to check the configuration.

Example

Display the configuration of the NAC authentication mode on GE0/0/1.

```
<HUAWEI> display authentication interface gigabitethernet 0/0/1
Authentication profile: p1
Authentication access-point: Enable
Authentication access-point max-user: 10
Port authentication order:
                    MAC
                    DOT1X
                    WEB
```

Table 13-53 Description of the **display authentication interface** command output

Item	Description
Authentication profile	Name of the authentication profile applied to the interface.
Authentication access-point	Whether the interface functions as an access control point. **NOTE** This field is displayed only on access devices used in policy association solutions.
Authentication access-point max-user	Maximum number of users who are allowed to log in through an access point **NOTE** This field is displayed only on access devices used in policy association solutions.
Port authentication order	Authentication mode configured in the authentication profile applied to the interface. Authentication modes include: ● MAC: indicates the MAC address authentication mode. ● DOT1X: indicates the 802.1X authentication mode. ● WEB: indicates the Portal authentication mode. **NOTE** ● On a standalone device, if MAC address bypass authentication is enabled in the authentication profile using the **authentication dot1x-mac-bypass** command, **DOT1X** is displayed before **MAC**. If MAC address bypass authentication is disabled, **MAC** is displayed before **DOT1X**. ● On an AS device in an SVF system or a policy association scenario, this item only indicates authentication modes configured in the authentication profile, and does not indicate the authentication sequence.

13.5.93 display authentication mode

Function

The **display authentication mode** command displays the current NAC configuration mode and the mode after restart.

Format

display authentication mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mode** command to view the current NAC configuration mode.

Example

Display the current NAC configuration mode and the mode after restart.

```
<HUAWEI> display authentication mode
  Current authentication mode is unified-mode
  Next authentication mode is unified-mode
```

Table 13-54 Description of the **display authentication mode** command output

Item	Description
Current authentication mode is unified-mode	Current NAC configuration mode.
Next authentication mode is unified-mode	NAC configuration mode after the device restarts. Run the **authentication unified-mode** command to switch the NAC mode to unified mode. Run the **undo authentication unified-mode** command to switch the NAC mode to common mode.

13.5.94 display authentication user-alarm configuration

Function

The **display authentication user-alarm configuration** command displays alarm thresholds for the percentage of successfully authenticated NAC users.

Format

display authentication user-alarm configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the alarm thresholds for the percentage of successfully authenticated NAC users.

Example

Display the alarm thresholds for the percentage of successfully authenticated NAC users.

```
<HUAWEI> display authentication user-alarm configuration
  Current Alarm Percent:100
  Current Alarm Resume Percent:60
```

Table 13-55 Description of the **display authentication user-alarm configuration** command output

Item	Description
Current Alarm Percent	Upper alarm threshold for the percentage of successfully authenticated NAC users.
Current Alarm Resume Percent	Lower alarm threshold for the percentage of successfully authenticated NAC users.

13.5.95 display authentication-profile configuration

Function

The **display authentication-profile configuration** command displays the configuration of an authentication profile.

Format

display authentication-profile configuration [**name** *authentication-profile-name*]

Parameters

Parameter	Description	Value
name *authentication-profile-name*	Displays the configuration of a specified authentication profile. If **name** *authentication-profile-name* is not specified, the device displays all the authentication profiles configured on the device.	The value must be the name of an existing authentication profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an authentication profile, you can run this command to check whether the configuration is correct.

NOTE

The built-in authentication profile **default_authen_profile** is not counted in the configuration specification. The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is also not counted in the configuration specification.

Example

Display all the authentication profiles configured on the device.

```
<HUAWEI> display authentication-profile configuration
-------------------------------------------------------------------------------
  ID       Auth-profile name
-------------------------------------------------------------------------------
   0       default_authen_profile
   1       dot1x_authen_profile
   2       mac_authen_profile
   3       portal_authen_profile
   4       dot1xmac_authen_profile
   5       multi_authen_profile
   6       p1
-------------------------------------------------------------------------------
  Total 7, printed 7
```

Table 13-56 Description of the **display authentication-profile configuration** command output

Item	Description
ID	Authentication profile ID.
Auth-profile name	Authentication profile name.

Display the configuration of the authentication profile **p1**.

```
<HUAWEI> display authentication-profile configuration name p1
  Profile name                     : p1
  Dot1x access profile name            : -
  Mac access profile name              : -
  Portal access profile name          : testdel
  Free rule template                : -
  Force domain                      : -
  Dot1x force domain                  : -
  Mac-authen force domain               : -
  Portal force domain                : -
  Default domain                    : 110
  Dot1x default domain                : -
  Mac-authen default domain              : -
  Portal default domain               : -
  Permit domain                     : -
  Authentication handshake              : Enable
  Authentication handshake period         : 300s
  Auth-fail re-auth period           : 60s
  Pre-auth Re-auth period             : 60s
  Auth-fail re-auth period wlan-user     : 0s
  Auth-fail aging time               : 82800s
  Pre-auth aging time                : 82800s
  Author-keep aging time               : 0s
  Dot1x-mac-bypass                    : Disable
  Mac authen before 802.1x authen force     : Enable
  Mac authen before 802.1x authen         : Enable
  Single-access                   : Disable
  Device-type authorize service-scheme     : -
  Iconnect device authorize service-scheme    : example_iconnect
  Mac move detect enable               : Enable
  Authentication mode                 : multi-authen
  Authen-fail authorize service-scheme    : -
  Authen-server-down authorize service-scheme : -
  Authen-server-down authorize keep        : response-success
  Authen-server-noreply authorize keep     : response-success
  Authen-server-down close re-authen       : N
  Pre-authen authorize service-scheme      : -
  Security-name-delimiter             : -
  Domain-name-delimiter                 : -
  Domain-location                    : -
  Domainname-parse-direction             : -
  Bound vap profile                 : -
  SVF flag                       : Disable
  Ip-static-user                  : Disable
  Roam-realtime-accounting              : Enable
  Update-IP-realtime-accounting          : Enable
  IP-address in-accounting-start       : Enable
  IPv4-address in-accounting-start mandatory  : Enable
  Linkdown offline delay time          : 10
  Termination action                 : reauthenticate
  Control direction                : Inbound
  Redirect ACL original url          : Enable
  Update-Info-realtime-accounting         : Enable
  IPv6 Control Flag                 : N
  No IP Check Flag                  : N
```

```
IP Conflict Check Flag                    : Y
Authentication roam pre-authen mac-authen   : Enable
Authentication single-stack-control enable  : IPv6
Authentication no-replace dot1x             : -
Lldp sensor-ap authentication disable       : Disable
Drop dhcp-packet user-no-online             : Enable
```

Table 13-57 Description of the **display authentication-profile configuration name** command output

Item	Description
Profile name	Authentication profile name.
Dot1x access profile name	802.1X access profile bound to the authentication profile. To bind an 802.1X access profile, run the **dot1x-access-profile** command in the authentication profile view.
Mac access profile name	MAC access profile bound to the authentication profile. To bind a MAC access profile, run the **mac-access-profile** command in the authentication profile view.
Portal access profile name	Portal access profile bound to the authentication profile. To bind a Portal access profile, run the **portal-access-profile** command in the authentication profile view.
Free rule template	Authentication-free rule profile bound to the authentication profile. To bind an authentication-free rule profile, run the **free-rule-template** command in the authentication profile view.
Force domain	Forcible domain for users. To configure a forcible domain, run the **access-domain** command.
Dot1x force domain	Forcible domain for 802.1X authentication users. To configure a forcible domain for 802.1X authentication users, run the **access-domain** command.
Mac-authen force domain	Forcible domain for MAC address authentication users. To configure a forcible domain for MAC address authentication users, run the **access-domain** command.

Item	Description
Portal force domain	Forcible domain for Portal authentication users. To configure a forcible domain for Portal authentication users, run the **access-domain** command.
Default domain	Default domain for users. To configure a default domain for users, run the **access-domain** command.
Dot1x default domain	Default domain for 802.1X authentication users. To configure a default domain for 802.1X authentication users, run the **access-domain** command.
Mac-authen default domain	Default domain for MAC address authentication users. To configure a default domain for MAC address authentication users, run the **access-domain** command.
Portal default domain	Default domain for Portal authentication users. To configure a default domain for Portal authentication users, run the **access-domain** command.
Permit domain	Permitted domain for users. To configure a permitted domain, run the **permit-domain** command.
Authentication handshake	Whether the handshake function is enabled. ● Enable ● Disable To enable the handshake function, run the **authentication handshake** command.
Authentication handshake period	Handshake interval. To configure a handshake interval, run the **authentication timer handshake-period** command.

Item	Description
Auth-fail re-auth period	Interval for re-authenticating wired users who fail to be authenticated. To configure the interval, run the **authentication timer re-authen** command.
Pre-auth re-auth period	Interval for re-authenticating pre-connection users. To configure the interval, run the **authentication timer re-authen** command.
Auth-fail re-auth period wlan-user	Interval for re-authenticating wireless users who fail to be authenticated. To configure the interval, run the **authentication timer re-authen** command.
Auth-fail aging Time	Aging time for entries of the users who fail to be authenticated. To configure the aging time, run the **authentication timer authen-fail-aging** command.
Pre-auth aging Time	Aging time for pre-connection user entries. To configure the aging time, run the **authentication timer pre-authen-aging** command.
Author-keep aging time	Aging time for entries of online users who are authorized to retain the original network access rights. To configure the aging time, run the **authentication timer authorize-keep-aging** command.
Dot1x-mac-bypass	Whether MAC address bypass authentication is enabled. ● Enable ● Disable To configure the function, run the **authentication dot1x-mac-bypass** command.

Item	Description
Mac authen before 802.1x authen force	Whether forcible MAC address authentication is enabled before 802.1X authentication. ● Enable ● Disable To enable the function, run the **authentication mac-authen-first force** command.
Mac authen before 802.1x authen	Whether the sequence of authentication modes triggered by EAP-Start packets is configured to be MAC address authentication prior to 802.1X authentication. ● Enable ● Disable To configure this function, run the **authentication order mac dot1x** command.
Single-access	Whether the device allows users to access in only one authentication mode. To configure the function, run the **authentication single-access** command.
Device-type authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to voice terminals that are not authenticated. To configure the name, run the **authentication device-type voice authorize** command.
Iconnect device authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to iConnect terminals that are not authenticated. To configure the name, run the **authentication device-type iconnect authorize** command.
Authentication mode	User access mode. To configure the mode, run the **authentication mode** command.

Item	Description
Authen-fail authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users who fail to be authenticated. To configure the name, run the **authentication event action authorize** command.
Authen-server-down authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users when the authentication server is Down. To configure the name, run the **authentication event action authorize** command.
Authen-server-down authorize keep	The device retains the original network access rights of users and responds to users when the authentication server is Down. ● response-success: The device returns an authentication success packet to users. ● response-fail: The device returns an authentication failure packet to users. ● no-response: The device does not respond to users. To configure the function, run the **authentication event action authorize**.
Authen-server-noreply authorize keep	The device retains the original network access rights of users and responds to users when the authentication server does not respond. ● response-success: The device returns an authentication success packet to users. ● response-fail: The device returns an authentication failure packet to users. ● no-response: The device does not respond to users. To configure the function, run the **authentication event action authorize**.

Item	Description
Authen-server-down close re-authen	Whether to disable the re-authentication function when the authentication server is Down. ● Y ● N To configure the function, run the **authentication event authen-server-down action close re-authen**.
Pre-authen authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users who are in the pre-connection state. To configure the name, run the **authentication event action authorize** command.
Security-name-delimiter	Security string delimiter. To configure the delimiter, run the **security-name-delimiter** command.
Domain-name-delimiter	Domain name delimiter. To configure the delimiter, run the **domain-name-delimiter** command.
Domain-location	Domain name location. To configure the location, run the **domain-location** command.
Domainname-parse-direction	Domain name resolution direction. To configure the direction, run the **domainname-parse-direction** command.
Bound vap profile	VAP profile to which the authentication profile is bound. To configure a VAP profile, run the **authentication-profile** command.
SVF flag	Whether SVF is enabled. ● Enable ● Disable
Ip-static-user	Whether the function of identifying static users through IP addresses is enabled. ● Enable ● Disable To configure the function, run the **ip-static-user enable** command.

Item	Description
Roam-realtime-accounting	Whether a device is enabled to send accounting packets during roaming. ● Enable ● Disable To configure the function, run the **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command.
Update-IP-realtime-accounting	Whether a device is enabled to send accounting packets during address updating. ● Enable ● Disable To configure the function, run the **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command.
Linkdown offline delay time	User logout delay when an interface link is faulty. To configure the delay, run the **link-down offline delay** command.
IP-address in-accounting-start	Whether the function of carrying users' IP addresses in accounting-start packets is enabled. ● Enable ● Disable To configure the function, run the **authentication ip-address in-accounting-start** command.
IPv4-address in-accounting-start mandatory	Whether the function of forcibly carrying users' IPv4 addresses in Accounting-Start packets is enabled. ● Enable ● Disable To configure the function, run the **authentication ipv4-address in-accounting-start mandatory** command.

Item	Description
Termination action	Whether the device is configured to reauthenticate users when the time exceeds the value of Session-Timeout delivered by the RADIUS server. - reauthenticate To configure the function, run the **authentication termination-action reauthenticate** command.
Control direction	Direction of packets controlled by the device. - Inbound: Only upstream traffic is controlled. - All: Bidirectional traffic is controlled. To configure the function, run the **authentication control-direction** command.
Redirect ACL original url	Whether the redirect URL is configured to carry the original URL when Portal-authenticated users who match a redirect ACL are forcibly redirected for another forcible Portal authentication. - Enable - Disable To configure the function, run the **authentication redirect-acl original-url enable** command.
Update-Info-realtime-accounting	Whether a device is enabled to send accounting packets for terminal information updates. - Enable - Disable To configure the function, run the **authentication** { **roam-accounting** | **update-info-accounting** | **update-ip-accounting** } * **enable** command.
IPv6 Control Flag	Whether network admission control is enabled for IPv6 users. - Y: The function is enabled. - N: The function is disabled. To configure the function, run the **authentication ipv6-control enable** command.

Item	Description
No IP Check Flag	Whether the device is enabled not to create any IP hash tables for the client IP address. ● Y ● N To configure the function, run the **authentication no-ip-check** command.
IP Conflict Check Flag	Whether the device is enabled not to check IP address conflicts for client IP addresses. ● Y ● N To configure the function, run the **authentication ip-conflict-check enable** command.
Authentication roam pre-authen mac-authen	Whether MAC address authentication is enabled for roaming STAs. ● Enable ● Disable To configure this function, run the **authentication roam pre-authen mac-authen enable** command.
Mac move detect enable	Whether the device is enabled to detect users' online status before user MAC address migration: ● Enable ● Disable To enable this function, run the **authentication mac-move detect enable** command.
Authentication single-stack-control enable	Whether the single-stack authentication function is enabled. ● IPv4 ● IPv6 ● Disable To configure the single-stack authentication function, run the **authentication single-stack-control enable** command.

Item	Description
Authentication no-replace dot1x	Whether the device is enabled not to respond to the EAP-Start packets sent from users who have successfully passed MAC address authentication or Portal authentication. - dot1x: The function is enabled. - -: The function is disabled. - voice-device: The function is enabled and takes effect only for voice terminals. To configure this function, run the **authentication no-replace dot1x** command.
Lldp sensor-ap authentication disable	Whether the switch is enabled to allow Huawei LLDP-identified APs to access the network without authentication. - Enable - Disable To configure the function, run the **lldp sensor-ap authentication disable** command.
Drop dhcp-packet user-no-online	Whether to discard DHCP packets when 802.1x authentication users are offline or during re-authentication. - Enable - Disable To configure the function, run the **authentication drop dhcp-packet user-no-online enable** command.

13.5.96 display device-profile

Function

The **display device-profile** command displays the configuration of a specified terminal type identification profile or all terminal type identification profiles.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

display device-profile { **all** | **profile-name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays summary of all terminal type identification profiles.	-
profile-name *profile-name*	Displays detailed information about a specified terminal type identification profile.	The value must be the name of an existing terminal type identification profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring terminal type identification, you can run the **display device-profile** command to view the terminal type identification profile configuration, including the profile name, terminal type identifier, and ACL rule.

Example

Display summary of all terminal type identification profiles.

```
<HUAWEI> display device-profile all

-------------------------------------------------------------------------------------------

  Index     Name                              Device type                      Rule num
State

---------------------------------------------------------------------------------------------------

  0       test                            example                         1            enable

---------------------------------------------------------------------------------------------------

  Total count : 1
```

Display detailed information about the terminal type identification profile **test**.

```
<HUAWEI> display device-profile profile-name test
  ----------------------------------------------------------------------------
  Name         : test
  Device type : example
  State        : disabled
  Rule         :
    rule 1 mac xxxx-xxxx-xxxx mask 12
  Match        :
    if-match rule id 1
  ----------------------------------------------------------------------------
```

Table 13-58 Description of the **display device-profile** command output

Item	Description
Name	Name of a terminal type identification profile. To set a terminal type identification profile name, run the **device-profile** command.
Device type	Terminal type identifier. To set a terminal type identifier, run the **device-type** command.
Rule num	Number of ACL rules.
State	Whether to enable terminal type identification: ● enable: Terminal type identification is enabled. ● disabled: Terminal type identification is disabled. To enable terminal type identification, run the **enable** command.
Rule	Terminal identification rule. To set a terminal identification rule, run the **rule** command.
Match	Matching mode of terminal type identification rules. To set a matching mode of terminal type identification rules, run the **if-match** command.

13.5.97 display dot1x

Function

The **display dot1x** command displays 802.1X authentication information.

Format

display dot1x statistics

display dot1x [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
statistics	Displays statistics on 802.1X authentication. The statistics about 802.1X authentication is displayed only when this parameter is specified.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays 802.1X authentication information of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. If this parameter is not specified, 802.1X authentication information of all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dot1x** command to view configuration results of all configuration commands in 802.1X authentication and statistics about 802.1X packets.

The command output helps you to check whether the current 802.1X authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

The **display dot1x** command displays the statistics on 802.1X packets. You can locate the fault according to the packet statistics. When the fault is rectified, run the **reset dot1x statistics** command to clear the packet statistics. After a period of time, run the **display dot1x** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display 802.1X authentication information.

```
<HUAWEI> display dot1x
 Max users: 10000
 Current users: 1
 Global default domain is jqq
 Dot1x abnormal-track cache-record-num: 20
 Quiet function is Disabled
 Mc-trigger port-up-send is Disabled
 Parameter set:Quiet Period          180s   Quiet-times          1
               Tx Period             30s    Mac-By-Pass Delay   10s
 Dot1x URL: 123456


GigabitEthernet10/0/1Wlan-Dbss0 status: UP  802.1x protocol is Enabled
 Dot1x access profile is jqq
 Authentication mode is multi-authen
 Authentication method is EAP
 Reauthentication is enabled
 Reauthen period: 300s
 Dot1x retry times: 2
 Authenticating users: 0
 Current users: 0

 Authentication Success: 0          Failure: 0
 Enter Enquence        : 0
 EAPOL Packets: TX     : 68         RX     : 0
 Sent       EAPOL Request/Identity Packets  : 3
            EAPOL Request/Challenge Packets : 0
            Multicast Trigger Packets       : 64
            EAPOL Success Packets           : 0
            EAPOL Failure Packets           : 1
 Received  EAPOL Start Packets              : 0
            EAPOL Logoff Packets            : 0
            EAPOL Response/Identity Packets : 0
            EAPOL Response/Challenge Packets: 0

Online user(s) info:
UserId   MAC/VLAN            AccessTime               UserName
------------------------------------------------------------------------------
1047     xxxx-xxxx-xxxx/27   2018/12/06 19:27:54      jqq
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display 802.1X statistics.

```
<HUAWEI> display dot1x statistics
 Dropped   EAPOL Access Flow Control       : 0
           EAPOL Check Sysmac Error        : 0
           EAPOL Get Vlan ID Error         : 0
           EAPOL Packet Flow Control       : 0
           EAPOL Online User Reach Max     : 0
           EAPOL Static or BlackHole Mac   : 0
           EAPOL Get Vlan Mac Error        : 0
           EAPOL Temp User Exist           : 0
           EAPOL no replace dot1x          : 0

 DHCP      Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 ARP       Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 ND        Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 DHCPv6    Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 ANYL2     Enter Enqueue                   : 0
           Processed Packet                : 0
           Dropped Packet                  : 0

 Sent      Authentication Request          : 0
           Cut Request                     : 0
           Cut Command Ack                 : 0
           Authentication Ack Fail Aff     : 0
           Update Ip                       : 0
           Wlan Eap Authentication Request      : 0
           Wlan Eap Authentication Request Ack  : 0
           Wlan Eap Send Pmk               : 0
           Wlan Eap Reauthenticate Send Pmk     : 0
           Update User Online Time         : 0

 Received  Authentication Ack              : 0
           Reauthenticate Command          : 0
           Cut Command                     : 0
           Cut Ack                         : 0
           Sam Nac Ack                     : 0
           Notify Server Up                : 0
           Wlan Eap Authentication Request      : 0
           Wlan Mac Authentication Request      : 0
           Notify Vlanif Mac Authentication     : 0
```

Table 13-59 Description of the **display dot1x** command output

Item	Description
Max users	Maximum number of global online users, the value varies according to device models.
Current users	Number of current online users.
Global default domain is	Global default authentication domain. To configure the global default authentication domain, run the **domain** command.

Item	Description
Dot1x abnormal-track cache-record-num	Number of EAP packets for abnormal 802.1X authentication that can be recorded by the device. For details, see **dot1x abnormal-track cache-record-num**.
Quiet function is	Whether the quiet function is enabled. ● Enabled. ● Disabled. To configure the quiet function, run the **dot1x quiet-period** command.
Mc-trigger port-up-send is	Whether the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is enabled. ● Enabled. ● Disabled. To configure the function, run the **dot1x mc-trigger port-up-send enable** command.
Parameter set	Settings of 802.1X parameters: ● Quiet Period: specifies the quiet period set by the quiet timer. To configure the quiet period, run the **dot1x timer quiet-period** command. ● Quiet-times: specifies the maximum number of authentication failures before the device quiets a user. To configure the maximum value, run the **dot1x quiet-times** command. ● Tx Period: specifies the interval for sending authentication requests. To configure the interval, run the **dot1x timer tx-period** command. ● Mac-By-Pass Delay: specifies the value of the delay timer for MAC address bypass authentication.
Dot1x URL	Redirect-to URL for HTTP access of 802.1X users. To configure the redirect-to URL, run the **dot1x url** command.
interface status	Interface status: ● UP: The interface is enabled. ● DOWN: The interface is shut down.
802.1x protocol is	Whether 802.1X authentication is enabled on the interface. ● Enabled. ● Disabled.

Item	Description
Dot1x access profile is	802.1X access profile name. To configure the 802.1X access profile name, run the **dot1x-access-profile** command.
Authentication mode is	User access mode. To configure the user access mode, run the **authentication mode** command.
Authentication method is	Authentication mode of 802.1X users. To configure the authentication mode of 802.1X users, run the **dot1x authentication-method** command.
Reauthentication is	Whether re-authentication is enabled for online 802.1X users. To configure the function, run the **dot1x reauthenticate** command.
Dot1x retry times	Maximum number of attempts to send authentication requests to 802.1X users. To configure maximum number of attempts to send authentication requests to 802.1X users, run the **dot1x retry** command.
Authenticating users	Number of users who are being authenticated.
Current users	Number of online users on the interface.
Authentication Success	Number of successful authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Failure	Number of authentication failures. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication. The statistics do not include authentication failures caused by EAP-Request/Identity request timeouts and EAP-Request/MD5 Challenge request timeouts.
Enter Enquence	Number of packets entering the queue.
EAPOL Packets	Number of globally EAPOL packets. ● TX: Number of sent EAPOL packets. ● RX: Number of received EAPOL packets.
Sent	Statistics of sent packet.
EAPOL Request/ Identity Packets	Number of globally EAPOL Request/Identity packets.

Item	Description
EAPOL Request/ Challenge Packets	Number of globally EAPOL Request/Challenge packets.
Multicast Trigger Packets	Number of multicast packets that trigger authentication.
EAPOL Success Packets	Number of globally EAPOL Success packets.
EAPOL Failure Packets	Number of globally EAPOL Failure packets.
Received	Statistics of received packet.
EAPOL Start Packets	Number of globally EAPOL Start packets.
EAPOL Logoff Packets	Number of globally EAPOL LogOff packets.
EAPOL Response/ Identity Packets	Number of globally EAPOL Response/Identity packets.
EAPOL Response/ Challenge Packets	Number of globally EAPOL Response/Challenge packets.
Online user(s) info	Online user information: ● UserId: User ID. ● MAC/VLAN: MAC address/VLAN ID. ● AccessTime: Access time. ● UserName: User name. ● Total: Total number of online users. ● printed: Number of displayed online users.

Item	Description
Dropped	Number of discarded EAP packets. ● EAPOL Access Flow Control: number of packets that are discarded because the user access rate is exceeded. ● EAPOL Check Sysmac Error: number of packets that are discarded because the device MAC address is incorrect. ● EAPOL Get Vlan ID Error: number of packets that are discarded because the obtained VLAN ID is incorrect. ● EAPOL Packet Flow Control: number of packets that are discarded because the packet access rate is exceeded. ● EAPOL Online User Reach Max: number of packets that are discarded because the number of online users reaches the maximum. ● EAPOL Static or BlackHole Mac: number of packets that are discarded because the packet MAC address is a static MAC address or blackhole MAC address. ● EAPOL Get Vlan Mac Error: number of packets that are discarded because the obtained VLAN MAC address is incorrect. ● EAPOL Temp User Exist: number of packets that are discarded because the temporary user exists. ● EAPOL no replace dot1x: number of EAP Start packets that are discarded due to 802.1X authentication of successfully authenticated MAC or Portal users.
DHCP	DHCP packet statistics.
ARP	ARP packet statistics.
ND	ND packet statistics.
DHCPv6	DHCPv6 packet statistics.
ANYL2	Any Layer 2 packet statistics.
Processed Packet	Number of processed packets.
Dropped Packet	Number of discarded packets.
Authentication Request	Number of authentication request messages.
Cut Request	Number of logout request messages.
Cut Command Ack	Number of acknowledgment messages to logout command request messages.
Authentication Ack Fail Aff	Number of the user is disconnected after the wireless user authentication fails.

Item	Description
Update Ip	Number of IP address update messages.
Wlan Eap Authentication Request	Number of EAP authentication request messages initiated by the WLAN module.
Wlan Eap Authentication Request Ack	Number of acknowledgment messages to EAP authentication request messages initiated by the WLAN module.
Wlan Eap Send Pmk	Number of PMK messages sent when the WLAN module performs EAP authentication.
Wlan Eap Reauthenticate Send Pmk	Number of PMK messages sent when the WLAN module performs EAP re-authentication.
Update User Online Time	Number of the user online time is updated.
Authentication Ack	Number of authentication acknowledgment messages.
Reauthenticate Command	Number of re-authentication messages.
Cut Command	Number of logout command request messages.
Cut Ack	Number of acknowledgment messages to logout request messages.
Sam Nac Ack	Number of EAP messages replied by the SAM module.
Notify Server Up	Number of RADIUS server Up messages.
Wlan Mac Authentication Request	Number of MAC authentication request messages initiated by the WLAN module.
Notify Vlanif Mac Authentication	Number of MAC authentication request messages of a VLANIF interface.

13.5.98 display dot1x-access-profile configuration

Function

The **display dot1x-access-profile configuration** command displays the configuration of an 802.1X access profile.

Format

display dot1x-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of an 802.1X access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the 802.1X access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified 802.1X access profile.	The value must be the name of an existing 802.1X access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an 802.1X access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the 802.1X access profiles configured on the device.

```
<HUAWEI> display dot1x-access-profile configuration
-------------------------------------------------------------------------------
 ID            Dot1x-Access-Profile Name
-------------------------------------------------------------------------------
 0             dot1x_access_profile
 1             d1
 2             d2
 3             d3
 4             d4
-------------------------------------------------------------------------------
 Total: 5 printed: 5.
```

Table 13-60 Description of the **display dot1x-access-profile configuration** command output

Item	Description
ID	802.1X access profile ID.
Dot1x-Access-Profile Name	802.1X access profile name.

Display the configuration of the 802.1X access profile **d1**.

```
<HUAWEI> display dot1x-access-profile configuration name d1
  Profile Name                  : d1
  Authentication method         : EAP
  Port control                  : authorized-force
  Re-authen                     : Enable
  Client-no-response authorize : -
  Trigger condition             : arp
  Unicast trigger               : Enable
  Trigger dhcp-bind             : Enable
  Handshake                     : Disable
  Handshake packet-type         : request-identity
  Max retry value               : 2
  Reauthen Period               : 3600s
  Client Timeout                : 5s
  Handshake Period              : 60s
  Eth-trunk handshake period   : 120s
  Dot1x no-response authorize  : Disable
  Dot1x eap-success response   : Disable
  Bound authentication profile : -
```

Table 13-61 Description of the **display dot1x-access-profile configuration name** command output

Item	Description
Profile Name	802.1X access profile name.
Authentication method	Authentication mode of 802.1X users: - CHAP - PAP - EAP To configure the authentication mode, run the **dot1x authentication-method** command.
Port control	802.1X authentication interface's authorization status: - auto - authorized-force - unauthorized-force To set an authorization state for an interface, run the **dot1x port-control** command.

Item	Description
Re-authen	Whether re-authentication for online 802.1X users is enabled: - Enable - Disable To configure the re-authentication function, run the **dot1x reauthenticate** command.
Client-no-response authorize	Network access rights granted to users when the 802.1X client does not respond. - service-scheme: The name of a service scheme based on which network access rights are assigned. - ucl-group: The name of a UCL group based on which network access rights are assigned. - vlan: The VLAN based on which network access rights are assigned. To configure the network access rights, run the **authentication event client-no-response action authorize** command.
Trigger condition	Packet type that can trigger 802.1X authentication: - dhcp - arp - dhcpv6 - nd - any-l2-packet To configure the packet type, run the **authentication trigger-condition** (802.1X authentication) command.
Unicast trigger	Whether 802.1X authentication triggered by unicast packets is enabled: - Enable - Disable To configure the function, run the **dot1x unicast-trigger** command.

Item	Description
Trigger dhcp-bind	Whether the device is enabled to automatically generate DHCP snooping binding entries for users with static IP addresses: ● Enable ● Disable To configure the function, run the **dot1x trigger dhcp-binding** command.
Handshake	Whether handshake with online 802.1X authentication users is enabled: ● Enable ● Disable
Handshake packet-type	Type of 802.1X authentication handshake packets: ● request-identity ● srp-sha1-part2
Max retry value	Maximum number of attempts to send authentication requests to 802.1X users. To configure the maximum value, run the **dot1x retry** command.
Reauthen Period	Re-authentication interval for online 802.1X users. To configure the re-authentication interval, run the **dot1x timer** command.
Client Timeout	Authentication timeout period for 802.1X clients. To configure the authentication timeout period, run the **dot1x timer** command.
Handshake Period	Interval at which the device handshakes with an 802.1X client on a non-Eth-Trunk interface. To configure the interval, run the **dot1x timer** command.
Eth-trunk handshake period	Interval at which the device handshakes with an 802.1X client on an Eth-Trunk. To configure the interval, run the **dot1x timer** command.

Item	Description
Dot1x no-response authorize	Whether the function of not responding to the EAPoL-Start packets sent by clients when the AAA server is Down is enabled: ● Enable ● Disable To configure the function, run the **dot1x no-response authorize authen-server-down** command.
Dot1x eap-success response	Enable the device to respond to EAP-Success messages when 802.1X authentication fails. ● Enable ● Disable To configure the function, run the **dot1x authentication-reject response eap-success** command.
Bound authentication profile	Authentication profile to which the 802.1X access profile is bound. To configure the authentication profile, run the **dot1x-access-profile** command.

13.5.99 display dot1x-client-profile configuration

Function

The **display dot1x-client-profile configuration** command displays the configuration of an 802.1X client profile.

NOTE

Only the following models support this command: S5735-L-I, S5735-L1, S5735S-L1, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S.

Format

display dot1x-client-profile configuration [**name** *client-profile-name*]

Parameters

Parameter	Description	Value
name *client-profile-name*	Displays the configuration of an 802.1X client profile with a specified name. If **name** *client-profile-name* is not specified, all 802.1X client profiles configured on the device are displayed. If **name** *client-profile-name* is specified, the detailed configuration of the specified 802.1X client profile is displayed.	The value must be the name of an existing 802.1X client profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an 802.1X client profile, you can run this command to check whether the configuration is correct.

Example

Display all 802.1X client profiles configured on the device.

```
<HUAWEI> display dot1x-client-profile configuration
-------------------------------------------------------------------------------
   ID        Dot1x-client-profile name
-------------------------------------------------------------------------------
    0        dot1x_client_profile_1
    1        dot1x_client_profile_2
-------------------------------------------------------------------------------
```

Table 13-62 Description of the **display dot1x-client-profile configuration** command output

Item	Description
ID	ID of an 802.1X client profile.
Dot1x-client-profile name	Name of an 802.1X client profile.

Display the configuration of the 802.1X client profile **d1**.

```
<HUAWEI> display dot1x-client-profile configuration name d1
  Profile name                          : d1
  EAP Method                              : PEAP
  EAP username                             : example
  EAP password                            : ******
  PKI realm name                           : -
```

Table 13-63 Description of the **display dot1x-client-profile configuration name** command output

Item	Description
Profile name	Name of an 802.1X client profile.
EAP Method	Access mode of the 802.1X client.
EAP username	User name used by an 802.1X client for authentication.
EAP password	Password used by an 802.1X client for authentication.
PKI realm name	Name of the PKI realm used for TLS authentication.

13.5.100 display dot1x-client statistics

Function

The **display dot1x-client statistics** command displays packet statistics of 802.1X clients.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dot1x-client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays packet statistics of the 802.1X client on a specified interface. If this parameter is not specified, packet statistics of 802.1X clients on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view packet statistics of 802.1X clients.

Example

Display packet statistics of 802.1X clients.

```
<HUAWEI> display dot1x-client statistics
  Dot1x-client message statistics on interface GigabitEthernet0/0/1 :
  EAPOL Packets: TX     : 0          RX     : 68
  Dot1x-client message statistics on interface GigabitEthernet0/0/2 :
  EAPOL Packets: TX     : 57         RX     : 67
```

Table 13-64 Description of the **display dot1x-client statistics** command output

Item	Description
Dot1x-client statistics on interface *interface-type interface-number*	Packet statistics of 802.1X clients on an interface.
EAPOL Packets	EAPoL packet statistics.
TX	Number of sent packets.
RX	Number of received packets.

Display packet statistics of 802.1X clients on a specified interface.

```
<HUAWEI> display dot1x-client statistics interface gigabitEthernet 0/0/1
  EAPOL Packets: TX     : 8214       RX     : 9703
  Send      EAPOL Start Packets             : 4714
```

```
         EAPOL Logoff Packets            : 15
         EAPOL Response/Identity Packets : 1415
         EAPOL Response/Challenge Packets: 3954
Received  EAPOL Request/Identity Packets  : 2322
         EAPOL Request/Challenge Packets : 3954
         EAPOL Success Packets           : 35
      EAPOL Failure Packets           : 1508
```

Table 13-65 Description of the **display dot1x-client statistics interface** command output

Item	Description
Sent	Number of sent packets of the following types: - EAPOL Start Packets - EAPOL Logoff Packets - EAPOL Response/Identity Packets - EAPOL Response/Challenge Packets
Received	Number of received packets of the following types: - EAPOL Request/Identity Packets - EAPOL Request/Challenge Packets - EAPOL Success Packets - EAPOL Failure Packets

13.5.101 display dot1x-client status

Function

The **display dot1x-client status** command displays status information of 802.1X clients.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dot1x-client status [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays status information of 802.1X clients on a specified interface. If this parameter is not specified, the status information of 802.1X clients on all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view status information of 802.1X clients.

Example

Display status information of 802.1X clients.

```
<HUAWEI> display dot1x-client status
  Dot1x-client status on interface GigabitEthernet0/0/1 :
  Access-status: Success
  Access-Time  : 2019/4/19 15:41:35
```

Table 13-66 Description of the **display dot1x-client status** command output

Item	Description
Dot1x-client status on interface *interface-type interface-number*	Status of the 802.1X client on an interface.
Access-status	Access status: ● Init: The 802.1X client is in initialization state. ● Success: The 802.1X client accesses the network successfully. ● Failure: The 802.1X client fails to access the network. ● Authenticating: The 802.1X client is being authenticated.

Item	Description
Access-Time	Access time.

13.5.102 display dot1x quiet-user

Function

The **display dot1x quiet-user** command displays information about 802.1X authentication users who are quieted.

Format

display dot1x quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all 802.1X authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a quiet 802.1X authentication user with a specified MAC address.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about 802.1X authentication users who are quieted.

Example

Display information about all 802.1X authentication users who are quieted.

```
<HUAWEI> display dot1x quiet-user all
-------------------------------------------------------------------------------
MacAddress                User Status              Quiet Remain Time(Sec)
-------------------------------------------------------------------------------
```

```
00e0-fc02-0003            Block                  50
--------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1   Active: 0
```

Table 13-67 Description of the **display dot1x quiet-user all** command output

Item	Description
MacAddress	MAC address of an 802.1X authentication user who is quieted.
User Status	User status: ● Block: The user is in silent state. ● Active: The user is not in silent state.
Quiet Remain Time(Sec)	● If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. ● If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.5.103 display dns snooping interface enable-list

Function

The **display dns snooping interface enable-list** command displays information about the interfaces enabled with DNS snooping.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dns snooping interface enable-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about the interfaces enabled with DNS snooping.

Example

Display information about the interfaces enabled with DNS snooping.

```
<HUAWEI> display dns snooping interface enable-list
-------------------------------------------------------------
 Total count : 1
-------------------------------------------------------------
 Interface Name
 GigabitEthernet0/0/1
-------------------------------------------------------------
```

Table 13-68 Description of the **display dns snooping interface enable-list** command output

Item	Description
Total count	Number of interfaces enabled with DNS snooping.
Interface Name	Name of an interface.

13.5.104 display dns snooping dn-ip-cache

Function

The **display dns snooping dn-ip-cache** command displays information about DNS snooping IP address and domain name entries.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dns snooping dn-ip-cache

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about DNS snooping IP address and domain name entries.

Example

Display information about DNS snooping IP address and domain name entries.

```
<HUAWEI> display dns snooping dn-ip-cache
-------------------------------------------------------------------------------
 Total count    : 1
 TTL delay-time : 22    minute
-------------------------------------------------------------------------------
 IP-address           TTL(minute)  Domain Name
  10.1.1.2            2400         www.example.com
-------------------------------------------------------------------------------
```

Table 13-69 Description of the **display dns snooping dn-ip-cache** command output

Item	Description
Total count	Total number of DNS snooping IP address and domain name entries.
TTL delay-time	Delay in aging DNS snooping IP address and domain name entries, in minutes.
IP-address	IP address obtained through domain name resolution.
TTL(minute)	Time to live (TTL) of IP address and domain name entries, in minutes. **NOTE** The maximum value is 17938897.
Domain Name	Domain name.

13.5.105 display dns snooping dn-rule-list

Function

The **display dns snooping dn-rule-list** command displays information about DNS snooping domain name rule entries.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display dns snooping dn-rule-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about DNS snooping domain name rule entries.

Example

Display information about DNS snooping domain name rule entries.

```
<HUAWEI> display dns snooping dn-rule-list
-------------------------------------------------------------------------------
 Total count : 1
-------------------------------------------------------------------------------
 Index    Priority      Domain Name
   1         11         example.com
-------------------------------------------------------------------------------
```

Table 13-70 Description of the **display dns snooping dn-rule-list** command output

Item	Description
Total count	Total number of DNS snooping domain name rule entries.
Index	Index.
Priority	Priority of a domain name.
Domain Name	Domain name.

13.5.106 display free-rule

Function

The **display free-rule** command displays whether an authentication-free rule defined by ACL is delivered.

Format

display free-rule

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display free-rule** command to view the delivery status of an authentication-free rule defined by ACL.

Example

Display whether an authentication-free rule defined by ACL is delivered.

```
<HUAWEI> display free-rule
 ------------------------------------------------------------------------------
    Slot-ID                     Acl-ID                      Status
 ------------------------------------------------------------------------------
       0                       6000                      SUCCESS
 ------------------------------------------------------------------------------
Total 1 free-rule(s)
```

Table 13-71 Description of the **display free-rule** command output

Item	Description
Slot-ID	Slot ID.
Acl-ID	ACL number.
Status	Whether an authentication-free rule defined by ACL is successfully delivered to a slot.

13.5.107 display free-rule-template configuration

Function

The **display free-rule-template configuration** command displays the configuration of an authentication-free rule profile.

Format

display free-rule-template configuration [**name** *free-rule-name*]

Parameters

Parameter	Description	Value
name *free-rule-name*	Displays the configuration of an authentication-free rule profile with a specified name. If **name** *free-rule-name* is not specified, the device displays all the authentication-free rule profiles configured on the device. If **name** *free-rule-name* is specified, the device displays the configuration of a specified authentication-free rule profile.	The value must be the name of an existing authentication-free rule profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an authentication-free rule profile, you can run this command to check whether the configuration is correct.

Example

Display all the authentication-free rule profiles configured on the device.

```
<HUAWEI> display free-rule-template configuration
--------------------------------------------------------------------------------
 ID             Free-rule-template Name
--------------------------------------------------------------------------------
 0              default_free_rule
--------------------------------------------------------------------------------
 Total: 1 printed: 1.
```

Table 13-72 Description of the **display free-rule-template configuration** command output

Item	Description
ID	ID of an authentication-free rule profile.

Item	Description
Free-rule-template Name	Name of an authentication-free rule profile.

13.5.108 display mac-address authen

Function

The **display mac-address authen** command displays the current authen MAC address entries in the system.

Format

display mac-address authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MAC address authentication or 802.1X authentication is configured successfully, the administrator can run this command to check the existing authen MAC address entries on the device. The administrator can check information about user access based on these MAC address entries to locate user access faults. The **authen** entry is generated after a user passes MAC address authentication or 802.1X authentication.

Precautions

If there are a lot of **authen** MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all authen MAC address entries in the system.

```
<HUAWEI> display mac-address authen
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                      Learned-From        Type
-------------------------------------------------------------------------------
xxxx-xxxx-xxxx 3000/-/-                        GE0/0/1           authen
xxxx-xxxx-xxx1 3000/-/-                        GE0/0/1           authen
xxxx-xxxx-xxx2 3000/-/-                        GE0/0/1           authen
-------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-73 Description of the **display mac-address authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the outbound interface belongs to.
Learned-From	Interface on which a MAC address is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.5.109 display mac-address pre-authen

Function

The **display mac-address pre-authen** command displays the current pre-authen MAC address entries in the system.

Format

display mac-address pre-authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the existing MAC address entries of the pre-connection type to obtain access information about pre-connection users and locate faults.

Precautions

If there are a lot of pre-authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all pre-authen MAC address entries in the system.

```
<HUAWEI> display mac-address pre-authen
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                       Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc00-0100 3000/-/-                          GE0/0/1             pre-authen
00e0-fc00-0400 3000/-/-                          GE0/0/1             pre-authen
00e0-fc00-0200 3000/-/-                          GE0/0/1             pre-authen
-------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-74 Description of the **display mac-address pre-authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the interface belongs to.
Learned-From	Interface on which a MAC address of a user to be authenticated is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.5.110 display mac-access-profile configuration

Function

The **display mac-access-profile configuration** command displays the configuration of a MAC access profile.

Format

display mac-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of a MAC access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the MAC access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified MAC access profile.	The value must be the name of an existing MAC access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a MAC access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the MAC access profiles configured on the device.

```
<HUAWEI> display mac-access-profile configuration
-------------------------------------------------------------------------------
 ID            Mac-Access-Profile Name
-------------------------------------------------------------------------------
 0             mac_access_profile
 1             m1
 2             m2
 3             m3
 4             m4
-------------------------------------------------------------------------------
 Total: 5 printed: 5.
```

Table 13-75 Description of the **display mac-access-profile configuration** command output

Item	Description
ID	MAC access profile ID.
Mac-Access-Profile Name	MAC access profile name.

Display the configuration of the MAC access profile **m1** (the MAC address authentication user configures a password).

```
<HUAWEI> display mac-access-profile configuration name m1
  Profile Name                 : m1
  Authentication method        : CHAP
  Username format              : fixed username: a1
  Password type                : cipher
  Re-authen                    : Disable
  Trigger condition            : arp dhcp nd dhcpv6
  Offline dhcp-release         : Disable
  Re-authen dhcp-renew         : Disable
  Trigger dhcp-bind            : Enable
  Reauthen Period              : 1800s
  Bound authentication profile : -
```

Display the configuration of the MAC access profile **m2** (the MAC address authentication user does not configure a password).

```
<HUAWEI> display mac-access-profile configuration name m2
  Profile Name                 : m2
  Authentication method        : CHAP
  Username format              : fixed username: a1
  Password                     : not configured
  Re-authen                    : Disable
  Trigger condition            : arp dhcp nd dhcpv6
  Offline dhcp-release         : Disable
  Re-authen dhcp-renew         : Disable
  Trigger dhcp-bind            : Enable
  Reauthen Period              : 1800s
  Bound authentication profile : -
```

Table 13-76 Description of the **display mac-access-profile configuration name** command output

Item	Description
Profile Name	MAC access profile name.
Authentication method	Authentication mode for MAC address authentication. ● CHAP ● PAP To configure the authentication mode, run the **mac-authen authentication-method** command.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address that does not contain hyphens (-), for example, 0005e01c02e3. ● use MAC address with-hyphen as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-e01c-02e3. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-e0-1c-02-e3. ● use MAC address without-hyphen upper as username: A user name is a MAC address in the uppercase format that does not contain hyphens (-), for example, 0005E01C02E3. ● use MAC address with-hyphen upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-E01C-02E3. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-E0-1C-02-E3. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every four digits, for example, 0005:e01c:02e3. ● use MAC address with-hyphen normal colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:e0:1c:02:e3.

Item	Description
	- use MAC address with-hyphen colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every four digits, for example, 0005:E01C:02E3. - use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:E0:1C:02:E3. - fixed username: The user name is fixed. - use option82 as username: The content of the Option 82 field is used as the user name. - not configured: The user name format is not configured. To configure the user name format, run the **mac-authen username** command.
Password type	Password display mode for MAC address authentication. - cipher To configure the password display mode, run the **mac-authen username** command.
password	Password of the MAC address authentication user. This field has the following fixed value: - not configured: indicates that the MAC address authentication user does not configure a password.
Re-authen	Whether re-authentication for online MAC address authentication users is enabled: - Enable: indicates that re-authentication is enabled. - Disable: indicates that re-authentication is disabled. To configure the re-authentication function, run the **mac-authen reauthenticate** command.

Item	Description
Trigger condition	Packet type that can trigger MAC address authentication. To configure the packet type, run the **authentication trigger-condition** command.
Offline dhcp-release	Whether the device is enabled to clear user entries when receiving DHCP release packets from MAC address authentication users. ● Enable ● Disable To configure the function, run the **mac-authen offline dhcp-release** command.
Re-authen dhcp-renew	Whether the device is enabled to re-authenticate MAC address authentication users when receiving DHCP lease renewal packets from the users. ● Enable ● Disable To configure the function, run the **mac-authen reauthenticate dhcp-renew** command.
Trigger dhcp-bind	Whether the device is enabled to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-connection phase: ● Enable ● Disable To configure the function, run the **mac-authen trigger dhcp-binding** command.
Reauthen Period	Re-authentication interval for online MAC address authentication users. To configure the re-authentication interval, run the **mac-authen timer reauthenticate-period** command.
Bound authentication profile	Authentication profile to which the MAC access profile is bound. To configure the authentication profile, run the **mac-access-profile** command.

13.5.111 display mac-authen

Function

The **display mac-authen** command displays information about MAC address authentication.

Format

display mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **configuration**]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays information about MAC address authentication on a specified interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. If this parameter is not specified, MAC authentication information of all interfaces is displayed.	-
configuration	Displays the global information about MAC address authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mac-authen** command to view configuration results of all configuration commands in MAC address authentication. The command output helps you to check whether the MAC address authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

You can locate the fault according to the packet statistics that is displayed using the **display mac-authen** command. When the fault is rectified, run the **reset mac-authen statistics** command to clear the packet statistics. After a period of time, run the **display mac-authen** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display the configuration of MAC address authentication.

```
<HUAWEI> display mac-authen
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Maximum users: 16384
  Current users: 1
  Global default domain is default

 GigabitEthernet0/0/1 state: UP.  MAC address authentication is enabled
  MAC access profile is mac_access_profile
  Reauthentication is disabled
  Reauthen Period: 60s
  Maximum users: 16384
  Current users: 1
  Username format: fixed username: gcs
  Password type: cipher
  Authentication Success: 22, Failure: 85
  0 silent mac address(es) found, 0 printed.

 Online user(s) info:
 UserId   MAC/VLAN            AccessTime              UserName
 ------------------------------------------------------------------------------
 37223    00e0-fc12-3456/2003 2014/09/28 15:45:45      gcs
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-77 Description of the **display mac-authen** command output

Item	Description
Quiet period	Quiet period during which the device quiets a user who fails to be authenticated. The default value of the quiet timer is 60 seconds. To configure the quiet period, run the **mac-authen timer quiet-period** command.
Authentication fail times before quiet	Maximum number of authentication failures before the device quiets a user. To configure the maximum value, run the **mac-authen quiet-times** command.
Maximum users	Maximum number of users allowed on the device. The value varies according to device models.
Current users	Number of online users.
Global default domain	Global default authentication domain. To configure the global default authentication domain, run the **domain** command in the system view.
interface state	Interface status: ● UP: The interface is enabled. ● DOWN: The interface is shut down.
MAC address authentication	Whether MAC address authentication is enabled on the interface. ● enabled ● disabled
MAC access profile	MAC access profile name. To configure the MAC access profile name, run the **mac-access-profile** command in the system view.

Item	Description
Reauthentication	Whether re-authentication for MAC address authentication users is enabled. ● enabled ● disabled To configure whether re-authentication for MAC address authentication users is enabled, run the **mac-authen reauthenticate** command.
Reauthen Period	Re-authentication interval for online MAC address authentication users. To configure the re-authentication interval, run the **mac-authen timer reauthenticate-period** command.
Current users	Number of current online users on the interface.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address without hyphens (-), for example, 00e0fc123456. ● use MAC address with-hyphen as username: A user name is a MAC address that contains a hyphen (-) in between every four digits, for example, 00e0-fc12-3456. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains a hyphen (-) in between every two digits, for example, 00-e0-fc-12-34-56. ● use MAC address without-hyphen upper as username: A user name is a MAC address in uppercase format without hyphens (-), for example, 00E0FC123456. ● use MAC address with-hyphen upper as username: A user name is a MAC address in uppercase format that contains a hyphen (-) in between every four digits, for example, 00E0-FC12-3456. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in uppercase format that contains a hyphen (-) in between every two digits, for example, 00-E0-FC-12-34-56. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) in between every four digits, for example, 00e0:fc12:3456. ● use MAC address with-hyphen normal colon as username: A user name is a MAC address that contains a colon (:) in between every two digits, for example, 00:e0:fc:12:34:56. ● use MAC address with-hyphen colon upper as username: A user

Item	Description
	name is a MAC address in uppercase format that contains a colon (:) in between every four digits, for example, 00E0:FC12:3456. - use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in uppercase format that contains a colon (:) in between every two digits, for example, 00:E0:FC:12:34:56. - fixed username: The user name is fixed. - use option82 as username: The content of the Option 82 field is used as the user name. - not configured: The user name format is not configured. To configure the user name format for MAC address authentication, run the **mac-authen username** command.
Password type	Password display mode for MAC address authentication. - cipher To configure the password display mode for MAC address authentication, run the **mac-authen username** command.
Authentication Success: *m*, Failure: *n*	Numbers of successful authentications (*m*) and failed authentications (*n*) on the interface.
m silent mac address(es) found, *n* printed	Numbers of successful authentications (*m*) and failed authentications (*n*) on the interface.
Online user(s) info	Information about online users: - UserId: ID of an online user. - MAC/VLAN: MAC address and VLAN of an online user. - AccessTime: access time of an online user. - UserName: name of an online user. - Total: total number of online users. - printed: number of displayed online users.

13.5.112 display mac-authen quiet-user

Function

The **display mac-authen quiet-user** command displays information about MAC address authentication users who are quieted.

Format

display mac-authen quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a specified MAC address authentication user who is quieted.	The value is in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about MAC address authentication users who are quieted.

Example

Display information about all MAC address authentication users who are quieted.

```
<HUAWEI> display mac-authen quiet-user all
-------------------------------------------------------------------------------
MacAddress              User Status                     Quiet Remain Time(Sec)
-------------------------------------------------------------------------------
xxxx-xxxx-xxxx          Block                           50
-------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1   Active: 0
```

Table 13-78 Description of the **display mac-authen quiet-user all** command output

Item	Description
MacAddress	MAC address of a MAC address authentication user who is quieted.
User status	User status: - Block: The user is in a silent state. - Active: The user is not in a silent state.
Quiet Remain Time(Sec)	- If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. - If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.5.113 display portal

Function

The **display portal** command displays the Portal authentication configuration.

Format

display portal [**interface** *interface-type interface-number* | **configuration**]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays Portal authentication information of a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If this parameter is not specified, Portal authentication information of all interfaces is displayed.	-
configuration	Displays the global Portal authentication information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal** command to view the Portal authentication configuration and check whether the configuration is correct.

Example

Display the Portal authentication configuration.

```
<HUAWEI> display portal
  Portal max-user number:16384
  Quiet function is Enabled
  Different-server is Enabled
  Parameter set:Quiet Period        60s   Quiet-times          3
  Logout packets resend: Resend-times 3  Timeout 5s
  Portal Https Redirect: Enable
  Portal JS Redirect   : Enable
  Portal 302 Redirect  : Enable
  Portal Pass Dns      : Enable

  Vlanif10 protocol status: down, web-auth-server layer2(direct)
<HUAWEI> display portal configuration
  Portal CnaBypass      : Enable
```

```
Portal CnaAdaptive    : Disable
Portal max-user number:16384
Quiet function is Enabled
Different-server is Enabled
Parameter set:Quiet Period        60s   Quiet-times          3
Logout packets resend: Resend-times 3  Timeout 5s
Portal Https Redirect: Enable
```

Table 13-79 Description of the **display portal** command output

Item	Description
Portal CnaBypass	Whether the CNA bypass function for iOS terminals is enabled: ● Enabled ● Disabled To enable the CNA bypass function for iOS terminals, run the **portal captive-bypass enable** command.
Portal CnaAdaptives	Whether the Captive Network Assistant (CNA) adaptive function for iOS terminals is enabled: ● Enabled ● Disabled To enable the Captive Network Assistant (CNA) adaptive function for iOS terminals, run the **portal captive-adaptive enable** command.
Portal max-user number	Maximum number of concurrent Portal authentication users allowed to access the device, the value varies according to device models. To set the maximum number of concurrent Portal authentication users allowed to access the device, run the **portal max-user** command.
Quiet function is Enabled or Quiet function is Disabled	Whether the quiet function in Portal authentication is enabled: ● Enabled ● Disabled To enable the quiet function, run the **portal quiet-period** command.

Item	Description
Different-server is Enabled or Different-server is Disabled	Whether a device is enabled to process user logout requests sent by a Portal server other than the one from which users log in: ● Enabled ● Disabled To configure a device to process user logout requests sent by a Portal server other than the one from which users log in, run the **portal logout different-server enable** command.
Parameter set	Parameter settings of the quiet function in Portal authentication. ● Quiet Period: indicates the quiet period in Portal authentication. To set the quiet period in Portal authentication, run the **portal timer quiet-period** command. ● Quiet-times: indicates the maximum number of authentication failures within 60 seconds before a Portal authentication user enters the quiet state. To set the maximum number of authentication failures, run the **portal quiet-times** command.
Logout packets resend	Configuration of the logout packet re-transmission function for Portal authentication users. ● Resend-times: indicates the number of re-transmission times for Portal authentication user logout packets. ● Timeout: indicates the re-transmission interval of Portal authentication user logout packets. To set the re-transmission interval, run the **portal logout resend timeout** command.
Portal Https Redirect	Whether HTTPS redirection of Portal authentication is enabled: ● Enable ● Disable To enable this function, run the **authentication https-redirect enable** command.

Item	Description
Portal JS Redirect	Whether the function of inserting a JavaScript file during Portal redirection is enabled. - Enable - Disable To enable this function, run the **portal redirect js enable** command.
Portal 302 Redirect	Whether redirection based on the status code 302 is enabled for Portal authentication: - Enable - Disable To configure this function, run the **portal redirect-302 enable** command.
Portal Pass Dns	Whether the device allows DNS packets to pass through during Portal authentication: - Enable: The device allows DNS packets to pass through during Portal authentication. - Disable: The device does not allow DNS packets to pass through during Portal authentication. To configure this function, run the **portal pass dns enable** command.
interface protocol status	Link layer protocol state of the interface and the enabled Portal authentication mode. - up: indicates that the interface is running properly. - down: indicates that the interface is disabled. - web-auth-server layer3: indicates that the authentication mode is set to Layer 3 Portal authentication on a specified interface. - web-auth-server layer2(direct): indicates that the authentication mode is set to Layer 2 Portal authentication on a specified interface.

13.5.114 display portal https-redirect blacklist

Function

The **display portal https-redirect blacklist** command displays IPv4 addresses in the HTTPS redirection blacklist.

The **display portal https-redirect ipv6 blacklist** command displays IPv6 addresses in the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect blacklist

display portal https-redirect ipv6 blacklist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection blacklist are correct.

Example

Display IPv4 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect blacklist
--------------------------------------
IP Address        Aging Time
--------------------------------------
 10.1.1.1        2018-06-26 21:01:59
--------------------------------------
 Total:1   Print:1
```

Display IPv6 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect ipv6 blacklist
------------------------------------------------------------
IPv6 Address                        Aging Time
```

```
-------------------------------------------------------------
FC00::1                                2019-02-23 09:47:05
-------------------------------------------------------------
 Total:1   Print:1
```

Table 13-80 Description of the **display portal https-redirect blacklist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the blacklist, which is configured using the **portal https-redirect blacklist** command or is added after the condition specified by the **portal https-redirect blacklist packet-rate** or **portal https-redirect blacklist retry-times interval** command is met.
Aging Time	Time when an address in the blacklist is aged out (that is, time when an address is removed from the blacklist). You can run the **portal https-redirect blacklist aging-time** command to configure the aging time of addresses in the blacklist.
Total:*m* Print:*n*	Total number of addresses in the blacklist, and number of addresses displayed.

13.5.115 display portal https-redirect whitelist

Function

The **display portal https-redirect whitelist** command displays IPv4 addresses in the HTTPS redirection whitelist.

The **display portal https-redirect ipv6 whitelist** command displays IPv6 addresses in the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect whitelist

display portal https-redirect ipv6 whitelist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection whitelist are correct.

Example

Display IPv4 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect whitelist
IP Address:
-------------------------------
 10.1.2.1
-------------------------------
 Total:1   Print:1
```

Display IPv6 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect ipv6 whitelist
IPv6 Address:
--------------------------------------------------------------
FC00::2
--------------------------------------------------------------
 Total:1   Print:1
```

Table 13-81 Description of the **display portal https-redirect whitelist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the whitelist, which are configured using the **portal https-redirect whitelist** command.
Total:*m* Print:*n*	Total number of addresses in the whitelist, and number of addresses displayed.

13.5.116 display portal-access-profile configuration

Function

The **display portal-access-profile configuration** command displays the configuration of a Portal access profile.

Format

display portal-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of a Portal access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the Portal access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified Portal access profile.	The value must be the name of an existing Portal access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a Portal access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the Portal access profiles configured on the device.

```
<HUAWEI> display portal-access-profile configuration
-------------------------------------------------------------------------------
 ID            Portal-access-profile Name
-------------------------------------------------------------------------------
 0             portal_access_profile
 1             p1
 2             p2
-------------------------------------------------------------------------------
 Total: 3 printed: 3.
```

Table 13-82 Description of the **display portal-access-profile configuration** command output

Item	Description
ID	Portal access profile ID.
Portal-access-profile Name	Portal access profile name.

Display the configuration of the Portal access profile **p1**.

```
<HUAWEI> display portal-access-profile configuration name p1
  Profile name                      : p1
  Portal timer offline-detect length: 300
  Service-scheme name               : -
  Ucl-group name                    : -
  Re-auth                           : Disable
  Network IP Num                    : 1
  Network IP List                   : 10.1.1.0 255.255.255.0
  Web-auth-server Name              : abc
  Layer                             : Layer two portal
  Bound authentication profile      : p1
```

Table 13-83 Description of the **display portal-access-profile configuration name** command output

Item	Description
Profile name	Portal access profile name.
Portal timer offline-detect length	Offline detection interval for Portal authentication users. To configure the interval, run the **portal timer offline-detect** command.
Service-scheme name	Name of the service scheme based on which the device assigns network access rights to users when the Portal server is Down. To configure the service scheme name, run the **authentication event portal-server-down action authorize** command.
Ucl-group name	Name of the UCL group based on which the device assigns network access rights to users when the Portal server is Down. To configure the UCL group name, run the **authentication event portal-server-down action authorize** command.

Item	Description
Re-auth	Whether the device is enabled to re-authenticate users when the Portal server changes from Down to Up. ● Enable ● Disable To configure the function, run the **authentication event portal-server-up action re-authen** command.
Network IP Num	Number of source IP address segments for Portal authentication. To configure the number, run the **portal auth-network** command.
Network IP List	Source IP address segment for Portal authentication. To configure the source IP address segment, run the **portal auth-network** command.
Web-auth-server Name	Portal server template bound to the Portal access profile. To configure the Portal server template, run the **web-auth-server** command.
Layer	Portal authentication mode. ● Layer two portal: Layer 2 authentication mode. ● Layer three portal: Layer 3 authentication mode. To configure the Portal authentication mode, run the **web-auth-server** command.
Bound authentication profile	Authentication profile to which the Portal access profile is bound. To configure the authentication profile, run the **portal-access-profile** command.

13.5.117 display portal quiet-user

Function

The **display portal quiet-user** command displays information about Portal authentication users in quiet state.

Format

display portal quiet-user { **all** | **user-ip** *ip-address* | **server-ip** *ip-address* }

Parameters

Parameter	Description	Value
all	Displays information about all Portal authentication users in quiet state.	-
user-ip *ip-address*	Displays information about the quiet user with the specified IP address.	The value is in dotted decimal notation.
server-ip *ip-address*	Displays information about all the users in quiet state authenticated by the Portal authentication server with a specified IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the quiet timer is enabled, you can run the **display portal quiet-user** command to view information about Portal authentication users who are in quiet state.

Example

Display information about all Portal authentication users in quiet state.

```
<HUAWEI> display portal quiet-user all
Quiet IP information
---------------------------------------------------------------------------------------
Quiet ip                    User status                    Quiet Remain Time(Sec)
--------------------------------------------------------------------------------------
192.168.1.1                Active                         10
192.168.1.2                Block                          20
--------------------------------------------------------------------------------------
Total: 2  Printed: 2  Block: 1   Active: 1
```

Display information about the user in quiet state at 192.168.1.1.

```
<HUAWEI> display portal quiet-user user-ip 192.168.1.1
  Quiet remain seconds: 50
  User Status: Block
```

Table 13-84 Description of the **display portal quiet-user** command output

Item	Description
Quiet IP information	Information about the user in quiet state.
Quiet ip	IP address of the user in quiet state.
User status	User status: ● Block: The user is in silent state. ● Active: The user is not in silent state. Currently, only users in silent state can be displayed.
Quiet Remain Time(Sec)	● If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. ● If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.
Quiet remain seconds	Remaining quiet period of the user in quiet state, in seconds.

13.5.118 display portal url-encode configuration

Function

The **display portal url-encode configuration** command displays the configuration of URL encoding and decoding.

Format

display portal url-encode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring URL encoding and decoding, you can run the **display portal url-encode configuration** command to check the configuration.

Example

Display the configuration of URL encoding and decoding.

```
<HUAWEI> display portal url-encode configuration
  Portal URL Encode : Disable
```

Table 13-85 Description of the **display portal url-encode configuration** command output

Item	Description
Portal URL Encode	Whether URL encoding and decoding are enabled: ● Disable ● Enable To configure the function, run the **portal url-encode enable** command.

13.5.119 display portal user-logout

Function

The **display portal user-logout** command displays temporary logout entries of Portal authentication users.

Format

display portal user-logout [**ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Displays temporary logout entries of the Portal authentication user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays temporary logout entries of the Portal authentication user with a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a Portal authentication user goes offline, the device sends an offline request packet to the Portal server. If the device does not receive an ACK packet from the Portal server, it records a temporary logout entry of the user. You can run the **display portal user-logout** command to check temporary logout entries of Portal authentication users.

If the parameter **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] is not specified, the temporary logout entries of all Portal authentication users are displayed.

Example

Display the temporary logout entries of all Portal authentication users.

```
<HUAWEI> display portal user-logout
 ---------------------------------------------------------------
 UserIP          Vrf     Resend Times TableID
 ---------------------------------------------------------------
 192.168.111.100  1        3           0
 ---------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-86 Description of the **display portal user-logout** command output

Item	Description
UserIP	IP address of the Portal authentication user.
Vrf	VPN instance that the Portal authentication user belongs to.
Resend Times	Number of logout packet re-transmission times. To set the number of logout packet re-transmission times, run the **portal logout resend timeout** command.
TableID	Index of the temporary logout entry.
Total: *m*, printed: *n*	Total number of temporary logout entries and number of displayed entries.

13.5.120 display portal-server state

Function

The **display portal-server state** command displays the status of a Portal server.

Format

display portal-server state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server template. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When Portal server is used for Portal authentication, you can run the **display portal-server state** command to check information about the Portal server status.

Example

Display information about the Portal server status configured in the Portal server template **abc**.

```
<HUAWEI> display portal-server state web-auth-server abc
  Web-auth-server     :    abc
  Total-servers       :    4
  Live-servers        :    1
  Critical-num        :    0
  Status              :    Normal
  Ip-address               Status
  192.168.2.1              UP
  192.168.2.2              DOWN
  192.168.2.3              DOWN
  192.168.2.4              DOWN
```

Table 13-87 Description of the **display portal-server state** command output

Item	Description
Web-auth-server	Name of the Portal server template.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.

Item	Description
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than this value, enable the survival function in the corresponding Portal server template view.
Status	Status of the Portal server. The values are as follows: ● Normal: indicates that the Portal server is in normal state. When the value of **Live-servers** in the command output is greater than the value of **Critical-num**, **Status** is displayed as **Normal**. If the **server-ip** *server-ip-address* &<1-10> command is not run in the Portal server template view to configure an IP address for the Portal server, **Status** is displayed as **Normal**. ● Abnormal: indicates that the Portal server is in abnormal state. When the value of **Live-servers** in the command output is less than or equal to the value of **Critical-num, Status** is displayed as **Abnormal**.
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: ● UP: reachable ● DOWN: unreachable

13.5.121 display server-detect state

Function

The **display server-detect state** command displays the status of a Portal server.

Format

display server-detect state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server template. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When Portal server is used for Portal authentication, you can run the **display server-detect state** command to check information about the Portal server status.

You are advised to run the **display portal-server state** command to check information of the Portal server status.

Example

Display information about the Portal server status configured in the Portal server template **abc**.

```
<HUAWEI> display server-detect state web-auth-server abc
  Web-auth-server     :    abc
  Total-servers       :    4
  Live-servers        :    1
  Critical-num        :    0
  Status              :    Normal
  Ip-address               Status
  192.168.2.1              UP
  192.168.2.2              DOWN
  192.168.2.3              DOWN
  192.168.2.4              DOWN
```

Table 13-88 Description of the **display server-detect state** command output

Item	Description
Web-auth-server	Name of the Portal server template.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.

Item	Description
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than or equal to this value, enable the survival function in the corresponding Portal server template view.
Status	Status of the Portal server. The values are as follows: ● Normal: indicates that the Portal server is in normal state. When *Live-servers* in the command output is larger than *Critical-num*, *Status* is displayed as **Normal**. If the **server-ip** *server-ip-address* &<1-10> command is not run in the Portal server template view to configure an IP address for the Portal server, *Status* is displayed as **Normal**. ● Abnormal: indicates that the Portal server is in abnormal state. When *Live-servers* in the command output is less than or equal to *Critical-num*, *Status* is displayed as **Abnormal**.
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: ● UP: reachable ● DOWN: unreachable

13.5.122 display static-user

Function

The **display static-user** command displays static user information.

Format

display static-user [**domain-name** *domain-name* \| **interface** *interface-type interface-number* \| **ip-address** *start-ip-address* [*end-ip-address*] \| **vpn-instance** *vpn-instance-name*] * [**detail**]

Parameters

Parameter	Description	Value
domain-name *domain-name*	Displays static user information in a specified domain.	The value must be an existing domain name on the device.
interface *interface-type interface-number*	Displays static user information on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ip-address *start-ip-address* [*end-ip-address*]	Displays static user information in a specified IP address range.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays static user information in a specified VPN instance.	The value must be an existing VPN instance name on the device.
detail	Displays detailed information about static users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a static user is configured, you can run the **display static-user** command to view the static user information.

Example

Display information about all static users configured.

```
<HUAWEI> display static-user
 Not-update-ip enable status: No
 IP-address       Interface       MAC-address     VPN
------------------------------------------------------------------------------
 10.1.1.6         GE0/0/1         00e0-fc12-3456 -
 10.1.1.7         GE0/0/1         00e0-fc12-3456 -
```

```
 10.1.1.8        GE0/0/1        00e0-fc12-3456 -
 10.1.1.10       -              00e0-fc12-3478 -
 10.1.1.11       -              00e0-fc12-3478 -
 10.1.1.12       -              00e0-fc12-3478 -
--------------------------------------------------------------------------------
Total item(s) number= 6, displayed number= 6
 Ip-static-user enable status:
--------------------------------------------------------------------------------
Vlanif10 : success
--------------------------------------------------------------------------------
Total item(s) number= 1, displayed number= 1
```

Display detailed information about all static users.

```
<HUAWEI> display static-user detail
 Not-update-ip enable status: No
--------------------------------------------------------------------------------
  IP address                    : 10.1.1.2
  IP static user                : Yes
  Vpn-instance                  : -
  Domain-name                   : local
  Interface                     : -
  MAC address                   : -
  VLAN                          : 10
  Detect                        : Disable
  Keep-online                   : Disable
--------------------------------------------------------------------------------
  IP address                    : 10.1.1.4
  IP static user                : Yes
  Vpn-instance                  : -
  Domain-name                   : -
  Interface                     : -
  MAC address                   : -
  VLAN                          : 10
  Detect                        : Disable
  Keep-online                   : Enable
--------------------------------------------------------------------------------
Total item(s) number= 2, displayed number= 2

Ip-static-user enable status:
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Total item(s) number= 0, displayed number= 0
```

Table 13-89 Description of the **display static-user** command output

Item	Description
Not-update-ip enable status	Whether the device is disabled from updating IP addresses of static users: ● Yes ● No To configure the function, run the **static-user not-update-ip enable** command.
IP-address/IP address	IP address of a static user.
Interface	Interface connected to a static user.
MAC-address/MAC address	MAC address of a static user.
VPN/Vpn-instance	VPN instance to which a static user belongs.

Item	Description
Total item(s) number= *m*, displayed number= *n*	The total number of entries is *m* and the number of displayed entries is *n*.
Ip-static-user enable status	Whether the function of identifying static users through IP addresses is enabled. To configure the function, run the **ip-static-user enable** command.
if-n : success	The function of identifying static users through IP addresses is enabled on interface *if-n*.
IP static user	Whether the user is a static user: ● Yes ● No
Domain-name	Domain to which a static user belongs. To configure the function, run the **static-user** command.
VLAN	VLAN to which a static user belongs. To configure the function, run the **static-user** command.
Detect	Whether the device is enabled to send ARP packets to trigger MAC address authentication for offline static users: ● Enable ● Disable To configure the function, run the **static-user** command.
Keep-online	Whether a static user is kept online, with offline detection not performed. ● Enable ● Disable To configure the function, run the **static-user** command.

13.5.123 display ucl-group all

Function

The **display ucl-group all** command displays information about all UCL groups that are created.

Format

display ucl-group all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After creating UCL groups using the **ucl-group** command, you can run the **display ucl-group all** command to check information about the UCL groups.

Example

Display information about all UCL groups.

```
<HUAWEI> display ucl-group all
ID       UCL group name
--------------------------------------------------------------------------------
10       example
--------------------------------------------------------------------------------
Total : 1
```

Table 13-90 Description of the **display ucl-group all** command output

Item	Description
ID	Index of a UCL group.
UCL group name	Name of a UCL group.

13.5.124 display ucl-group ip domain

Function

The **display ucl-group ip domain** command displays information about IP addresses and domain names of static UCL groups.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI.

Format

display ucl-group ip *ip-address* { *mask-length* | *ip-mask* }

display ucl-group ip { *group-index* | **name** *group-name* | **static** | **local-access-user** | **push** | **escape** | **all** } [**verbose**]

display ucl-group domain domain-name *domain-name*

display ucl-group ip domain-ip [**verbose**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support domain names in static UCL groups.

Parameters

Parameter	Description	Value
ip-address	Displays information about the static UCL group with a specified IP address.	The value must be the IP address of an existing static UCL group.
mask-length	Specifies the mask length of an IP address.	The value must be the IP address mask length of an existing static UCL group.
ip-mask	Specifies the mask of the IP address.	The value must be the IP address mask of an existing static UCL group.
group-index	Displays information about the static UCL group with a specified index.	The value must be the index of an existing static UCL group.
name *group-name*	Displays information about the static UCL group with a specified name.	The value must be the name of an existing static UCL group.

Parameter	Description	Value
static	Displays information about static UCL groups.	-
local-access-user	Displays information about dynamic UCL groups.	-
push	Displays information about pushed UCL groups.	-
escape	Displays information about escape UCL groups.	-
all	Displays information about all static UCL groups.	-
domain-name *domain-name*	Displays information about the static UCL group with a specified domain name.	The value must be an existing domain name on the device.
domain-ip	Displays information about IP addresses generated based on domain names in UCL groups.	-
verbose	Displays detailed information about static UCL groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view UCL groups' IP addresses that are manually added (using the **ucl-group ip** command) and dynamically generated when users go online and are granted UCL groups. When a user goes online successfully, the device grants a UCL group to the user and adds the user's IP address (with a 32-bit mask) to the UCL group. When the user goes offline or the user's IP address changes, the device deletes the corresponding IP address from the UCL group.

Example

Display IP address information of all UCL groups.

```
<HUAWEI> display ucl-group ip all
L: local-access-user, P: push, S: static, D: domain, E: escape
IP/Mask            ID    UCL group name                  Type
-------------------------------------------------------------------------------
10.9.9.4/32         1     g1                             S
10.10.0.0/16        2     g2                             S
10.9.9.6/32         1     g1                             L
-------------------------------------------------------------------------------
Total : 3       Local-access-user : 1       Push : 0     Static : 2       Domain : 0       Escape : 0
```

Display detailed information about all static UCL groups.

```
<HUAWEI> display ucl-group ip static verbose
-------------------------------------------------------------------------------
IP/Mask              : 10.9.9.4/32
UCL group ID         : 1
UCL group name       : g1
Type                 : static
Status on slot 0     : Success
IP/Mask              : 10.10.0.0/16

UCL group ID         : 2
UCL group name       : g2
Type                 : static
Status on slot 0     : Success
-------------------------------------------------------------------------------
Total : 2       Local-access-user : 0       Push : 0     Static : 2       Domain : 0       Escape : 0
```

Display domain name information of static UCL groups.

```
<HUAWEI> display ucl-group domain domain-name example.com
Domain-name      : example.com
UCL group ID     : 1
UCL group name   : g1
------------------------------------------------------------
IP               : 10.9.9.10
IP               : 10.9.9.12
------------------------------------------------------------
Total : 2
```

Display information about IP addresses generated based on domain names in all static UCL groups.

```
<HUAWEI> display ucl-group ip domain-ip
L: local-access-user, P: push, S: static, D: domain, E: escape
IP/Mask            ID    UCL group name                  Type
```

```
-------------------------------------------------------------------------------
9.9.9.4/32          1     g1                         D
9.9.9.5/32          1     g1                         D
10.10.0.0/16        2     g2                         D
-------------------------------------------------------------------------------
Total : 3  Local-access-user : 0   Push : 0  Static : 0   Domain : 3  Escape : 0
```

Table 13-91 Description of the **display ucl-group ip domain** command output

Item	Description
IP/Mask	IP address and mask of a UCL group.
ID	UCL group index.
UCL group ID	UCL group index.
UCL group name	UCL group name.
Type	UCL group type: • Static: static UCL group • Local-access-user: UCL group to which local users belong • Push: pushed UCL group • Escape: escape UCL group • Domain: domain name
Domain-name	Domain name.
Status on slot *n*	UCL group status in slot *n*.

13.5.125 display url-template

Function

The **display url-template** command displays information about URL templates.

Format

display url-template { **all** | **name** *template-name* }

Parameters

Parameter	Description	Value
all	Displays information about all configured URL templates.	-
name *template-name*	Displays information about the URL template with a specified name.	The value must be the name of an existing URL template.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a URL template is configured, you can run the **display url-template** command to view information about the URL template.

Example

Display information about all configured URL templates.

```
<HUAWEI> display url-template all
-----------------------------------------------------------------------------------------
 Name                          URL     Start  Assignment  Isolate        Index
                            Number  Mark   Mark        Mark
------------------------------------------------------------------------------------------
 test                        0       ?      =           &              0
 test2                        0       ?      =           &              1
------------------------------------------------------------------------------------------
 Total 2
```

Display information about the URL template **example**.

```
<HUAWEI> display url-template name example
 Name : example
 URL  :
 Start mark      : ?
 Assignment mark : =
 Isolate mark    : &
 Device IP
 Device MAC      :
 AP IP           :
 AP MAC          :
 SSID            :
 User MAC        :
 Redirect URL    :
 User IP address :
 Sysname         :
 User VLAN       :
 Delimiter       :
 Format          :
 Login URL Key   : logiurl
 Login URL       : http:\\example.com
 AP Name         :
 AP Location     :
 AP Group Name   :
 Device IP Value : 10.1.1.1
```

Table 13-92 Description of the **display url-template** command output

Item	Description
Index	Index of a URL template.
Name	Name of a URL template.
URL Number	Number of URLs.

Item	Description
URL	URL of the Portal server. To configure this parameter, run the **url** command in the URL template view.
Start mark/Start Mark	Start character in the URL. To configure this parameter, run the **parameter** command.
Assignment mark/Assignment Mark	Assignment character in the URL. To configure this parameter, run the **parameter** command.
Isolate mark/Isolate Mark	Delimiter between URLs. To configure this parameter, run the **parameter** command.
Device IP	Name of **device-ip** in the URL. To configure this parameter, run the **url-parameter** command.
Device MAC	Name of **device-mac** in the URL. To configure this parameter, run the **url-parameter** command.
AP IP	Name of **ap-ip** in the URL. To configure this parameter, run the **url-parameter** command.
AP MACUser VLAN	Name of **ap-mac** in the URL. To configure this parameter, run the **url-parameter** command.
SSID	Name of **ssid** in the URL. To configure this parameter, run the **url-parameter** command.
User MAC	Name of **user-mac** in the URL. To configure this parameter, run the **url-parameter** command.
Redirect URL	Name of **redirect-url** in the URL. To configure this parameter, run the **url-parameter** command.
User IP address	Name of **user-ipaddress** in the URL. To configure this parameter, run the **url-parameter** command.
Sysname	Name of **sysname** in the URL. To configure this parameter, run the **url-parameter** command.
User VLAN	Name of **user-vlan** in the URL. To configure this parameter, run the **url-parameter** command.

Item	Description
Delimiter	Delimiter between MAC addresses in the URL. To configure this parameter, run the **url-parameter mac-address format** command.
Format	Format of MAC addresses in the URL. To configure this parameter, run the **url-parameter mac-address format** command.
Login URL Key	Identification keyword for the login URL sent to the Portal server during redirection. To configure this parameter, run the **url-parameter** command.
Login URL	Device login URL. To configure this parameter, run the **url-parameter** command.
AP Name	Name of **ap-name** in the URL. To configure this parameter, run the **url-parameter** command.
AP Location	Name of **ap-location** in the URL. To configure this parameter, run the **url-parameter** command.
AP Group Name	Name of **ap-group-name** in the URL. To configure this parameter, run the **url-parameter** command.
Device IP Value	Value of the redirection parameter **device-ip**. To configure this parameter, run the **url-parameter set** command.
AP IP Value	Value of an AP IP address carried in the redirection URL.

13.5.126 display web-auth-server configuration

Function

The **display web-auth-server configuration** command displays the Portal server configuration.

Format

display web-auth-server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Portal server template is configured, the **display web-auth-server configuration** command displays the Portal server configuration.

Example

Display the Portal server configuration.

```
<HUAWEI> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
  Server-Source         : -
 ------------------------------------------------------------------------------
  Enabled protocol      : https
  Listening port        : 8443
  SSL policy            : default_policy
  Server-Source          : -
------------------------------------------------------------------------------
  Web-auth-server Name : example
  Web-auth-server Index: 0
  IP-address           :
  IPv6 Address         :
  Shared-key           :
  Source-IP            : -
  Port / PortFlag      : 50100 / NO
  Server-Source        : 10.1.1.1
  URL                  : https://192.168.2.10:8443/webauth
  URL Template         :
  URL Template ParaName:
  URL Template IVName  :
  URL Template Key     :
  Redirection          : Enable
  Sync                 : Disable
  Sync Seconds         : 300
  Sync Max-times       : 3
  Detect               : Disable
  Detect Seconds       : 60
  Detect Max-times     : 3
  Detect Critical-num  : 0
  Detect Action        :
  Detect Type          : portal
  VPN Instance         :
  Bound Portal profile :
  Protocol             : http
  Http Get-method      : disable
  Password Encrypt     : none
  Cmd ParseKey         : cmd
  Username ParseKey    : username
  Password ParseKey    : password
  MAC Address ParseKey : macaddress
```

```
IP Address ParseKey  : ipaddress
Initial URL ParseKey : initurl
Login Cmd            : login
Logout Cmd            : logout
Login Success
     Reply Type      : redirect initial URL
     Redirect URL    :
     Message         : LoginSuccess!
Login Fail
     Reply Type      : redirect login URL
     Redirect URL    :
     Message         : LoginFail!
Logout Success
     Reply Type      : message
     Redirect URL    :
     Message         : LogoutSuccess!
Logout Fail
     Reply Type      : message
     Redirect URL    :
     Message         : LogoutFail!
-------------------------------------------------------------------------------
 1 Web authentication server(s) in total
```

Table 13-93 Description of the **display web-auth-server configuration** command output

Item	Description
Listening port	Listening port for Portal protocol packets. To configure a listening port, run the **web-auth-server listening-port** command.
Portal	Portal protocol version. ● version 1, version 2: The device supports both the versions V1.0 and V2.0. ● version 2: The device supports the versions V2.0. To configure the Portal protocol version, run the **web-auth-server version** command.
Include reply message	Whether the packets sent from the device to the Portal server contain authentication responses. ● enabled ● disabled To configure this function, run the **web-auth-server reply-message** command.

Item	Description
Server-Source	Local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled. To configure this parameter, run the **web-auth-server server-source (system view)** command.
Enabled protocol	Enabled HTTP or HTTPS protocol. ● http ● https To enable the HTTP or HTTPS protocol, run the **portal web-authen-server** command.
Listening port	HTTP or HTTPS port number. To configure the HTTP or HTTPS port number, run the **portal web-authen-server** command.
SSL policy	SSL policy referenced by the HTTPS protocol. To configure the SSL policy referenced by the HTTPS protocol, run the **portal web-authen-server** command.
Server-Source	Local gateway address used by the device to receive and respond to the packets sent by the user terminals when the Portal interconnection function of the HTTP or HTTPS protocol is enabled. To configure this parameter, run the **portal web-authen-server server-source** command.
Web-auth-server Name	Name of the Portal server template. To configure the Portal server template name, run the **web-auth-server (system view)** command.
Web-auth-server Index	Index of the Portal server template.
IP-address	IPv4 address of the Portal server. To configure this parameter, run the **server-ip** command in the Portal server template view.

Item	Description
IPv6 Address	IPv6 address of the Portal server. To configure this parameter, run the **server-ip** command in the Portal server template view.
Shared-key	Shared key of the Portal server. To configure this parameter, run the **shared-key** command in the Portal server template view.
Source-IP	IP address used for communication with the Portal server. To configure this parameter, run the **source-ip** command in the Portal server template view.
Port / PortFlag	● Port: indicates the port number of the Portal server. ● PortFlag: indicates whether packets are always sent through this port. To configure this parameter, run the **port** command in the Portal server template view.
Server-Source	Local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled. To configure this parameter, run the **server-source** command in the Portal server template view.
URL	URL of the Portal server. To configure this parameter, run the **url** command in the Portal server template view.
URL Template	URL template bound to the Portal server template. To configure this parameter, run the **url-template** command in the Portal server template view.
URL Template ParaName	Encrypted URL parameter name. To configure this parameter, run the **url-template** command in the Portal server template view.

Item	Description
URL Template IVName	Initialization vector (IV) used in URL parameter encryption. To configure this parameter, run the **url-template** command in the Portal server template view.
URL Template Key	Key used in URL parameter encryption. To configure this parameter, run the **url-template** command in the Portal server template view.
Redirection	Redirection status of Portal authentication. ● Disable: Redirection of Portal authentication is disabled. ● Enable: Redirection of Portal authentication is enabled. To configure this parameter, run the **web-redirection disable** command in the Portal server template view.
Sync	User information synchronization. To enable user information synchronization, run the **user-sync** command.
Sync Seconds	User information synchronization interval. To set the user information synchronization interval, run the **user-sync** command.
Sync Max-times	Maximum number of times that user information synchronization fails. To set the maximum number of times that user information synchronization fails, run the **user-sync** command.
Detect	Portal server detection function. To configure Portal server detection function, run the **server-detect** command.
Detect Seconds	Detection interval of the Portal server. To set the detection interval of the Portal server, run the **server-detect** command.
Detect Max-times	Maximum number of detection failures. To set the maximum number of detection failures, run the **server-detect** command.

Item	Description
Detect Critical-num	Minimum number of Portal servers in Up state. To configure this function, run the **server-detect** command.
Detect Action	Action taken after the number of detection failures exceeds the maximum. - log: The device sends logs after the number of detection failures exceeds the maximum. - trap: The device sends traps after the number of detection failures exceeds the maximum. To configure an action taken after the number of detection failures exceeds the maximum, run the **server-detect** command.
Detect Type	Portal server detection mode. - Portal: Portal-based Portal server detection mode - HTTP: HTTP-based Portal server detection mode To configure the Portal server detection mode, run the **server-detect type** command.
VPN Instance	VPN instance used in Portal authentication. To configure this parameter, run the **vpn-instance** command in the Portal server template view.
Bound Portal profile	Portal access profile to which the Portal server template is bound. To configure this parameter, run the **web-auth-server** command in the Portal server template view.
Http Get-method	Whether users submit user name and password information to the device in GET mode: - disable: GET mode is not used. - enable: GET mode is used. To configure the GET mode, run the **http get-method enable** command.

Item	Description
Protocol	Protocol used in Portal authentication. ● portal ● http ● haca To configure the protocol used in Portal authentication, run the **protocol** command.
Password Encrypt	Password encoding mode: ● none: The password is not encoded. ● uam: The password is encoded using ASCII characters. To configure the password encoding mode, run the **protocol** command.
Cmd ParseKey	Command identification keyword. To configure the command identification keyword, run the **http-method post** command.
Username ParseKey	User name identification keyword. To configure the user name identification keyword, run the **http-method post** command.
Password ParseKey	User password identification keyword. To configure the user password identification keyword, run the **http-method post** command.
MAC Address ParseKey	User MAC address identification keyword. To configure the user MAC address identification keyword, run the **http-method post** command.
IP Address ParseKey	User IP address identification keyword. To configure the user IP address identification keyword, run the **http-method post** command.
Initial URL ParseKey	User initial login URL identification keyword. To configure the user initial login URL identification keyword, run the **http-method post** command.

Item	Description
Login Cmd	User login identification keyword. To configure the user login identification keyword, run the **http-method post** command.
Logout Cmd	User logout identification keyword. To configure the user logout identification keyword, run the **http-method post** command.
Login Success	User login success.
Reply Type	Redirection response type. ● redirect initial URL: A user is redirected to the initial login URL after successful login. ● redirect login URL: A user is redirected to the login URL after a login failure. ● message: specifies the displayed message. ● redirect URL: A user is redirected to a specified URL. To configure the redirection response type, run the **http-method post** command.
Redirect URL	Redirect URL. To configure the redirect URL, run the **http-method post** command.
Message	Displayed message. To configure the displayed message, run the **http-method post** command.
Login Fail	User login failure.
Logout Success	User logout success.
Logout Fail	User logout failure.

13.5.127 display webmng configuration

Function

The **display webmng configuration** command displays the configuration of the WEBMNG module.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S support this command.

Format

display webmng configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring user management based on HTTP or HTTPS, you can run this command to check the configuration of the WEBMNG module.

Example

Display the configuration of the WEBMNG module.

```
<HUAWEI> display webmng configuration
  Manager Type           : http
  Ssl-policy             : -
  Port                   : 8080
  Acl                    : -
```

Table 13-94 Description of the **display webmng configuration** command output

Item	Description
Manager Type	Management type. ● http: user management based on HTTP ● https: user management based on HTTPS To configure the management type, run the **remote-access-user manage** command.

Item	Description
Ssl-policy	SSL policy used by the built-in Portal server. To configure the SSL policy, run the **remote-access-user manage** command.
Port	Port number for user management based on HTTP or HTTPS. To configure the port number, run the **remote-access-user manage** command.
Acl	ACL number. You can use an ACL to specify users to be managed. To configure the ACL number, run the **remote-access-user manage** command.

13.5.128 domain mac-authen force

Function

The **domain mac-authen force** command configures a forcible domain for MAC address authentication users.

The **undo domain mac-authen force** command deletes a configured forcible domain for MAC address authentication users.

By default, no forcible domain is configured for MAC address authentication users.

Format

domain *domain-name* **mac-authen force mac-address** *mac-address* **mask** *mask*

undo domain *domain-name* **mac-authen force mac-address** *mac-address*

Parameters

Parameter	Description	Value
domain-name	Specifies the forcible domain name.	The value must be an existing domain name on the device.

Parameter	Description	Value
mac-address *mac-address* **mask** *mask*	Specifies a MAC address range within which the MAC address authentication users use the forcible domain. - **mac-address** *mac-address*: specifies the user MAC address. - **mask** *mask*: specifies the MAC address mask. **NOTE** A maximum of 128 MAC address ranges can be specified.	Both the MAC address and mask are in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure a forcible domain for MAC address authentication users within a specified MAC address range in the system view.

Prerequisites

A domain has been created using the **domain** command.

Precautions

The priorities of the forcible domain, domain carried in the user name, and default domain in different views are as follows in descending order: forcible domain with a specified authentication mode in an authentication profile > forcible domain in an authentication profile > authentication domain carried in the user name > default domain with a specified authentication mode in an authentication profile > default domain in an authentication profile > global default domain. Note that a forcible domain specified for MAC address authentication users within a MAC address range has the highest priority and takes precedence over that configured in an authentication profile.

This function takes effect only for users who go online after this function is successfully configured.

Example

In the system view, configure the forcible domain **example** for MAC address authentication users within the MAC address range specified using MAC address 00e0-fc95-7231 and mask FFFF-FFFF-FF00.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain example
[HUAWEI-aaa-domain-example] quit
[HUAWEI-aaa] quit
[HUAWEI] domain example mac-authen force mac-address 00e0-fc95-7231 mask ffff-ffff-ff00
```

13.5.129 dot1x abnormal-track cache-record-num

Function

The **dot1x abnormal-track cache-record-num** command sets the maximum number of EAP packets that can be recorded for abnormal 802.1X authentication.

The **undo dot1x abnormal-track cache-record-num** command restores the default maximum number of EAP packets that can be recorded for abnormal 802.1X authentication.

By default, the device can record a maximum of 20 EAP packets for abnormal 802.1X authentication.

Format

dot1x abnormal-track cache-record-num *cache-record-num*

undo dot1x abnormal-track cache-record-num

Parameters

Parameter	Description	Value
cache-record-num	Specifies the maximum number of EAP packets that can be recorded for abnormal 802.1X authentication.	The value is an integer in the range from 0 to 30. The value 0 indicates that no EAP packet is recorded for abnormal 802.1X authentication.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If 802.1X authentication fails, you need to check the EAP packets to locate the fault. This command allows you to set the maximum number of EAP packets that the device can record for abnormal 802.1X authentication.

Example

Set the maximum number of EAP packets that can be recorded for abnormal 802.1X authentication to 30.

```
<HUAWEI> system-view
[HUAWEI] dot1x abnormal-track cache-record-num 30
```

13.5.130 dot1x authentication-method

Function

The **dot1x authentication-method** command configures an 802.1X authentication mode.

The **undo dot1x authentication-method** command restores the default configuration.

The default 802.1X authentication mode is **eap**, which indicates Extensible Authentication Protocol (EAP) relay authentication.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Specifies EAP termination authentication using the Challenge Handshake Authentication Protocol (CHAP).	-
pap	Specifies EAP termination authentication using the Password Authentication Protocol (PAP).	-
eap	Specifies Extensible Authentication Protocol (EAP) relay authentication.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the packet to the RADIUS server for authentication. EAP termination is classified into PAP or CHAP authentication.
  - PAP: The device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
  - CHAP: The device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.
- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server. The device does not parse the received EAP packets but encapsulates them into RADIUS packets. This mechanism is called EAP over Radius (EAPoR).

The processing capability of the RADIUS server determines whether EAP termination or EAP relay is used. If the RADIUS server has a higher processing capability and can parse a large number of EAP packets before authentication, the EAP relay mode is recommended. If the RADIUS server has a processing capability not good enough to parse a large number of EAP packets and complete authentication, the EAP termination mode is recommended and the device parses EAP packets for the RADIUS server. When the authentication packet processing method is configured, ensure that the client and server both support this method; otherwise, the users cannot pass authentication.

NOTE

- The EAP relay can be configured for 802.1X users only when RADIUS authentication is used.
- If AAA local authentication is used, the authentication mode for 802.1X users can only be set to EAP termination.
- Because mobile phones do not support EAP termination mode (PAP and CHAP), the 802.1X authentication + local authentication mode cannot be configured for mobile phones. Terminals such as laptop computers support EAP termination mode only after having third-party clients installed.
- If the 802.1X client uses the MD5 encryption mode, the user authentication mode on the device can be set to EAP or CHAP; if the 802.1X client uses the PEAP authentication mode, the authentication mode on the device can be set to EAP.
- In a wireless access scenario, if WPA or WPA2 authentication mode is configured in the security policy profile, 802.1X authentication does not support pre-authentication domain-based authorization.
- If an interface has online 802.1X users and the authentication mode is changed between EAP termination and EAP relay in the 802.1X access profile bound to the interface, the online 802.1X users will be logged out. If the authentication mode is changed between CHAP and PAP in EAP termination mode, the online 802.1X users will not be logged out.

Example

In the 802.1X access profile **d1**, configure the device to use PAP authentication for 802.1X users.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x authentication-method pap
```

13.5.131 dot1x authentication-reject response eap-success

Function

The **dot1x authentication-reject response eap-success** command enables a device to send EAP-Success packets when 802.1X authentication fails.

The **undo dot1x authentication-reject response eap-success** command disables a device from sending EAP-Success packets when 802.1X authentication fails.

By default, the device does not send EAP-Success packets when 802.1X authentication fails.

Format

dot1x authentication-reject response eap-success

undo dot1x authentication-reject response eap-success

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

In MAC address + 802.1X hybrid authentication scenarios, a terminal with a built-in 802.1X authentication client displays a message indicating an 802.1X authentication failure when MAC address authentication succeeds. To prevent the message from being displayed, run the **dot1x authentication-reject response eap-success** command to enable the device to send EAP-Success packets when 802.1X authentication fails.

Example

In the 802.1X access profile **d1**, configure the device to send EAP-Success packets when 802.1X authentication fails.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x authentication-reject response eap-success
```

13.5.132 dot1x eap-notify-packet

Function

The **dot1x eap-notify-packet** command configures the device to send EAP packets with a code number to 802.1X users.

The **undo dot1x eap-notify-packet** command restores the default configuration.

By default, the device does not send EAP packets with a code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies the code number in EAP packets sent by the device.	The value is an integer that ranges from 5 to 255, the default value is 255.
data-type *type-number*	Specifies the data type in EAP packets sent by the device.	The value is an integer that ranges from 1 to 255, the default value is 255.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a non-Huawei device used as the RADIUS server sends RADIUS packets with attribute 61, EAP packet code number 0xa (hexadecimal notation, 10 in decimal notation), and data type being 0x19 (hexadecimal notation, 25 in decimal notation) to the device, run the **dot1x eap-notify-packet** command on the device so that the device can send EAP packets with code number 0xa and data type 0x19 to users. If the **dot1x eap-notify-packet** command is not executed, the device does not process EAP packets of this type and users are disconnected.

Precautions

The device can only send EAP packets with code number 10 and data type 25.

Example

In the 802.1X access profile **d1**, configure the device to send EAP packets with code number 10 and data type 25 to users.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x eap-notify-packet eap-code 10 data-type 25
```

13.5.133 dot1x-client-profile (AP wired port profile view)

Function

The **dot1x-client-profile** command binds a specified 802.1X client profile to an AP wired port profile.

The **undo dot1x-client-profile** command removes the binding relationship between an 802.1X client profile and an AP wired port profile.

By default, no 802.1X client profile is bound to an AP wired port profile.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

dot1x-client-profile *client-profile-name*

undo dot1x-client-profile

Parameters

Parameter	Description	Value
client-profile-name	Specifies the name of an 802.1X client profile.	The 802.1X client profile must already exist.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an 802.1X client profile is created using the **dot1x-client-profile (system view)** command, the profile takes effect only after being bound to an AP wired port profile.

Precautions

- The 802.1X client profile can be bound only to the upstream wired port of an AP.
- The **eth-trunk** and **dot1x-client-profile (AP wired port profile view)** commands cannot be both configured in the AP wired port profile view.

Example

Create an 802.1X client profile named **dot1x_client_profile1**, bind the profile to the AP wired port profile named **wired**, and apply the AP wired port profile to GE0.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name dot1x_client_profile1
[HUAWEI-dot1x-client-profile-dot1x_client_profile1] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] quit
[HUAWEI-wlan-view] wired-port-profile name wired
[HUAWEI-wlan-wired-port-wired] dot1x-client-profile dot1x_client_profile1
[HUAWEI-wlan-wired-port-wired] quit
[HUAWEI-wlan-view] ap-group name ap-group1
[HUAWEI-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

13.5.134 dot1x-client-profile (interface view)

Function

The **dot1x-client-profile** command applies an 802.1X client profile to an interface.

The **undo dot1x-client-profile** command cancels applying an 802.1X client profile to an interface.

By default, no 802.1X client profile is applied to an interface.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dot1x-client-profile *client-profile-name*

undo dot1x-client-profile *client-profile-name*

Parameters

Parameter	Description	Value
client-profile-name	Specifies the name of an 802.1X client profile.	The 802.1X client profile must exist.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating an 802.1X client profile using the **dot1x-client-profile** (system view) command, you need to apply the profile to an interface to make it take effect.

Precautions

An 802.1X client profile can be applied only to physical interfaces and Eth-Trunks.

Example

Apply an 802.1X client profile named **dot1x_client_profile1** to an interface.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name dot1x_client_profile1
[HUAWEI-dot1x-client-profile-dot1x_client_profile1] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] dot1x-client-profile dot1x_client_profile1
```

13.5.135 dot1x-client-profile (system view)

Function

The **dot1x-client-profile** command creates an 802.1X client profile and displays the 802.1X client profile view.

The **undo dot1x-client-profile** command deletes an 802.1X client profile.

By default, no 802.1X client profile is created.

NOTE

Only the following models support this command: S5735-L-I, S5735-L1, S5735S-L1, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S.

Format

dot1x-client-profile name *client-profile-name*

undo dot1x-client-profile name *client-profile-name*

Parameters

Parameter	Description	Value
name *client-profile-name*	Specifies the name of an 802.1X client profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following special characters: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses an 802.1X client profile to manage all configurations of the 802.1X client.

Precautions

802.1X client authentication and 802.1X access authentication are mutually exclusive. That is, the two functions cannot be configured simultaneously.

Example

Create the 802.1X client profile **dot1x_client_profile1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name dot1x_client_profile1
```

13.5.136 dot1x mc-trigger

Function

The **dot1x mc-trigger** command enables multicast-triggered 802.1X authentication.

The **undo dot1x mc-trigger** command disables multicast-triggered 802.1X authentication.

By default, multicast-triggered 802.1X authentication is enabled.

Format

dot1x mc-trigger

undo dot1x mc-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a client (for example, the built-in 802.1X client of the Windows operating system) cannot send an EAPOL-Start packet to perform 802.1X authentication, you can enable multicast-triggered 802.1X authentication. After that, the device multicasts an EAP-Request/Identity packet to the client to trigger authentication.

Example

Enable multicast-triggered 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger
```

13.5.137 dot1x mc-trigger port-up-send enable

Function

The **dot1x mc-trigger port-up-send enable** command enables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

The **undo dot1x mc-trigger port-up-send enable** command disables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

By default, the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled.

Format

dot1x mc-trigger port-up-send enable

undo dot1x mc-trigger port-up-send enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the device periodically multicasts EAP-Request/Identity packets to clients so that the clients are triggered to send EAPOL-Start packets for 802.1X authentication. If the device interface connecting to a client changes from Down to Up, the client needs to send EAPOL-Start packets again for 802.1X authentication, which takes a long time. You can run the **dot1x mc-trigger port-up-send enable** command on the device to enable the device interface to multicast EAP-Request/Identity packets to the client to trigger 802.1X authentication immediately after the interface goes Up. This configuration shortens the re-authentication time.

Example

Enable the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger port-up-send enable
```

13.5.138 dot1x no-response authorize authen-server-down

Function

The **dot1x no-response authorize authen-server-down** command enables the function of not responding to authentication triggering packets sent by clients when the AAA server is Down.

The **undo dot1x no-response authorize authen-server-down** command disables the function.

By default, the device responds to the authentication triggering packets sent by clients when the AAA server is Up.

Format

dot1x no-response authorize authen-server-down

undo dot1x no-response authorize authen-server-down

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When Cisco AnyConnect is used to perform EAP-FAST authentication, the device responds to the authentication triggering packets sent by the client. If the AAA server is Down, the client enters an abnormal state after receiving response packets from the device and cannot access the network. To prevent this problem, you can run the **dot1x no-response authorize authen-server-down** command to disable the device from responding to the authentication triggering packets sent by the client when the AAA server is Down. In this way, the client can obtain the access permission granted when the AAA server is Down.

802.1X authentication, MAC Address + 802.1X Hybrid Authentication can be triggered in the following scenarios:

- A client sends an EAPoL-Start packet.
- A client sends a DHCP, ARP, DHCPv6, ND, or any other packet.
- The access device sends an EAP-Request/Identity packet.

Precautions

This function is only applicable to MAC and 802.1X mixed authentication scenarios.

This function is effective only for new users who go online after the function is configured.

Only wired users support this function.

For new users having no corresponding entry on the device, this function takes effect only after a forcible domain is configured for the users using the **access-domain** *domain-name* [**dot1x**] **force** command in the authentication profile view.

The function takes effect only after the **authentication event authen-server-down action authorize** command is run in the authentication profile view to configure network access rights granted to users when the authentication server does not respond.

You are advised to run both the **dot1x no-response authorize authen-server-down** and **authentication event authen-server-up action re-authen** commands. This enables the authentication server to re-authenticate users in escape state in a timely manner when the server becomes Up so that these users can access the network.

Example

Enable the function of not responding to the authentication triggering packets sent by clients when the AAA server is Down.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x no-response authorize authen-server-down
```

13.5.139 dot1x port-control

Function

The **dot1x port-control** command sets the authorization state of an interface.

The **undo dot1x port-control** command restores the default authorization state of an interface.

By default, the authorization state of an interface is **auto**.

Format

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** }

undo dot1x port-control

Parameters

Parameter	Description	Value
auto	Indicates that the authorization state of an interface is automatically set. An interface is initially in unauthorized state. In this state, the interface can send and receive authentication packets only, and does not allow users to access network resources. After users are authenticated, the interface transitions to the authorized state and allows the users to access network resources.	-
authorized-force	Sets the authorization state of an interface to forcibly authorized. In this state, the interface does not process authentication packets, and allows users to access network resources without authentication or authorization.	-
unauthorized-force	Sets the authorization state of an interface to forcibly unauthorized. In this state, the interface does not process authentication packets, and denies user access to network resources.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **auto** mode is recommended. Only authenticated users can access network resources. To trust all users on an interface without authentication, configure the **authorized-force** mode. To disable access rights of all users on an interface to ensure security, configure the **unauthorized-force** mode.

Precautions

If 802.1X users on an interface have gone online, changing the authorization state in the 802.1X access profile bound to the interface will make the online 802.1X users go offline.

It is recommended that you set the authorization state of an interface in the early stage of network deployment. When the network is running properly, run the **cut access-user** command to disconnect all users from the interface before changing the authorization state.

Example

Configure the authorization state of an interface as **unauthorized-force** in 802.1X access profile **d1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x port-control unauthorized-force
```

13.5.140 dot1x quiet-period

Function

The **dot1x quiet-period** command enables the quiet function for 802.1X authentication users.

The **undo dot1x quiet-period** command disables the quiet function for 802.1X authentication users.

By default, the quiet function is enabled for 802.1X authentication users.

Format

dot1x quiet-period

undo dot1x quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function is enabled, if the number of authentication failures of an 802.1X user exceeds a specified value (set using the **dot1x quiet-times** command) within 60 seconds, the user enters a quiet period. During the quiet period, the device discards the 802.1X authentication request packets from the user. This prevents the impact on the system due to frequent user authentication.

The value of the quiet timer is set using the **dot1x timer quiet-period** command. When the quiet timer expires, the device re-authenticates the user.

Example

Enable the quiet timer.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-period
```

13.5.141 dot1x quiet-times

Function

The **dot1x quiet-times** command sets the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state.

The **undo dot1x quiet-times** command restores the default setting.

By default, an 802.1X user enters the quiet state after 10 authentication failures within 60 seconds.

Format

dot1x quiet-times *fail-times*

undo dot1x quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before the 802.1X user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function of the device is enabled using the **dot1x quiet-period** command, if the number of authentication failures of an 802.1X user exceeds the value that is set using the **dot1x quiet-times** command within 60 seconds, the user enters the quiet state. This prevents the impact on the system due to frequent user authentication.

Example

Set the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-times 4
```

13.5.142 dot1x reauthenticate mac-address

Function

The **dot1x reauthenticate mac-address** command enables re-authentication for an online 802.1X user with the specified MAC address.

By default, re-authentication is disabled for an online 802.1X user with the specified MAC address.

Format

dot1x reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of an 802.1X user to be re-authenticated.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **dot1x reauthenticate**.

The **dot1x reauthenticate mac-address** and **dot1x reauthenticate** commands re-authenticate online 802.1X users and their difference is as follows:

- The **dot1x reauthenticate mac-address** command configures the device to re-authenticate a specified user for once.
- The **dot1x reauthenticate** command configures the device to re-authenticate all users at intervals.
- The **dot1x reauthenticate mac-address** command does not support re-authentication for 802.1X users in pre-connection state.

Example

Enable re-authentication for an 802.1X user with the MAC address of 00e0-fc01-0005.

```
<HUAWEI> system-view
[HUAWEI] dot1x reauthenticate mac-address 00e0-fc01-0005
```

13.5.143 dot1x reauthenticate

Function

The **dot1x reauthenticate** command configures re-authentication for online 802.1X authentication users.

The **undo dot1x reauthenticate** command restores the default configuration.

By default, re-authentication is not configured for online 802.1X authentication users.

Format

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying the authentication parameters of a user on the authentication server, the administrator must re-authenticate the user in real time to ensure user validity if the user has been online.

After the user goes online, the device saves authentication parameters of the user. After re-authentication is configured for online 802.1X authentication users using the **dot1x reauthenticate** command in the 802.1X access profile, the device automatically sends the user authentication parameters in the 802.1X access profile to the authentication server at an interval (specified using the **dot1x timer reauthenticate-period** *reauthenticate-period-value* command) for re-authentication. If the user authentication information on the authentication server remains unchanged, the users are kept online. If the information has been changed, the users are disconnected and need to be re-authenticated based on the changed authentication parameters.

Precautions

After re-authentication is configured for online 802.1X authentication users, a large number of 802.1X authentication logs are generated.

This function takes effect only for users who go online after this function is successfully configured.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

In the 802.1X access profile **d1**, configure re-authentication for online 802.1X authentication users.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x reauthenticate
```

13.5.144 dot1x receive-packet vlan-ignore

Function

The **dot1x receive-packet vlan-ignore** command enables the VLAN replacement function for EAP packets received by an authentication device.

The **undo dot1x receive-packet vlan-ignore** command disables the VLAN replacement function for EAP packets received by an authentication device.

By default, VLAN replacement is disabled for EAP packets received by an authentication device.

Format

dot1x receive-packet vlan-ignore

undo dot1x receive-packet vlan-ignore

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

If there is a VLANIF interface corresponding to the VLAN allowed by the interconnection interfaces between an 802.1X client and an authentication device, the authentication device generates MAC-VLAN entries corresponding to the VLANIF interface for users in pre-connection state. When the 802.1X client triggers 802.1X authentication again, the authentication device does not return response packets if the VLAN ID carried in the received EAP packet does not match any VLAN information in user entries.

To resolve this problem, you can run this command to enable VLAN replacement for EAP packets received by the authentication device. When receiving an EAP packet with the same MAC address and interface information but a different VLAN ID from that in a user entry, the authentication device replaces the VLAN ID in the packet with that in the user entry, so that 802.1X authentication can proceed.

Example

Enable VLAN replacement for EAP packets received by an authentication device.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x receive-packet vlan-ignore
```

13.5.145 dot1x retry

Function

The **dot1x retry** command configures the number of times an authentication request is retransmitted to an 802.1X user.

The **undo dot1x retry** command restores the default configuration.

By default, the device can retransmit an authentication request to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the number of times an authentication request is retransmitted to an 802.1X user.	The value is an integer that ranges from 1 to 10.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device does not receive any response from a user within a specified time after sending an authentication request to the user, the device sends the authentication request again. If the authentication request has been sent for the maximum retransmission times and no response is received, the user authentication fails. In this process, the total number of authentication requests sent by the device is *max-retry-value* plus 1.

Precautions

Repeated authentication requests occupy a lot of system resources. When using the **dot1x retry** command, you can set the maximum number of times according to user requirements and device resources. The default value is recommended.

The following table lists the intervals at which the device retransmits different types of packets and related commands.

Packet Type	Interval for Retransmitting Packets	Command
EAP-Request/Identity packet (MAC address bypass authentication is disabled)	*tx-period-value*	**dot1x timer tx-period** *tx-period-value*
EAP-Request/Identity packet (MAC address bypass authentication is enabled)	Integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)	**dot1x timer mac-bypass-delay** *delay-time-value*
EAP-Request/MD5 Challenge packet	*client-timeout-value*	**dot1x timer client-timeout** *client-timeout-value*

Example

In the 802.1X access profile **d1**, configure the number of times an authentication request can be retransmitted to 802.1X users to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x retry 4
```

13.5.146 dot1x send-packet untagged

Function

The **dot1x send-packet untagged** command enables an access device to remove VLAN tags from 802.1X packets to be sent to terminals.

The **undo dot1x send-packet untagged** command disables an access device from removing VLAN tags from 802.1X packets to be sent to terminals.

By default, an access device does not remove VLAN tags from 802.1X packets to be sent to terminals.

Format

dot1x send-packet untagged

undo dot1x send-packet untagged

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some terminals (mainly some models of IP phones) cannot identify the tagged 802.1X packets received from access devices, resulting in 802.1X authentication failures. To resolve this problem, you can run the **dot1x send-packet untagged** command to enable access devices to remove VLAN tags from 802.1X packets to be sent to terminals.

Precautions

- This command is not supported in SVF, policy association, and wireless scenarios.
- If both the **dot1x send-packet untagged** and **authentication control-direction all** commands are configured in the authentication profile view, only the **authentication control-direction all** command takes effect.

Example

In the 802.1X access profile **d1**, enable the access switch to remove VLAN tags from 802.1X packets to be sent to terminals.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x send-packet untagged
```

13.5.147 dot1x send-packet vlan

Function

The **dot1x send-packet vlan** command configures the VLAN ID to be carried in EAP packets sent by an 802.1X client.

The **undo dot1x send-packet vlan** command cancels the configuration.

By default, EAP packets sent by an 802.1X client do not carry VLAN information.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dot1x send-packet vlan *vlan-id*

undo dot1x send-packet vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID to be carried in EAP packets	The value is an integer in the range from 1 to 4094.

Views

802.1X client profile view

Default Level

2: Configuration level

Usage Guidelines

By default, EAP packets sent by a device functioning as an 802.1X client do not carry VLAN information. If the interface of the authentication device connected to the client is a trunk interface and is not configured with the default VLAN, the interface discards the EAP packets received from the client, causing authentication failures.

You can run this command to configure the EAP packets sent by the 802.1X client to carry the VLAN ID allowed by the connected interface of the authentication device. In this way, the authentication device can properly process the EAP packets sent by the client.

Example

Set the VLAN ID to be carried in EAP packets sent by the 802.1X client to 30.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name d1
[HUAWEI-dot1x-client-profile-d1] dot1x send-packet vlan 30
```

13.5.148 dot1x timer

Function

The **dot1x timer** command configures the parameters of each 802.1X timer.

The **undo dot1x timer** command restores the default settings.

For the default parameter settings of each 802.1X timer, see the parameter description.

Format

dot1x timer { **client-timeout** *client-timeout-value* | **reauthenticate-period** *reauthenticate-period-value* }

undo dot1x timer { **client-timeout** | **reauthenticate-period** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the client authentication timeout interval. You are advised to set this parameter to 30 seconds for wired users. **NOTE** On the network, some terminals may delay in responding to EAP-Request/MD5 Challenge packets sent from the device. If the delay is long, you can increase **client-timeout** *client-timeout-value* so that these terminals can go online. The adjustment rule is as follows: 3 x **client-timeout** *client-timeout-value* > Terminal response delay	The value is an integer in the range from 1 to 120, in seconds. By default, the client authentication timeout interval is 5 seconds.
reauthenticate-period *reauthenticate-period-value*	Specifies the periodic re-authentication period for online 802.1X users.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the periodic re-authentication period is 3600 seconds for online 802.1X users.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, multiple timers are started to implement proper and orderly interactions between access users, access devices, and the authentication server. You can change the values of timers by running the **dot1x timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. It is recommended that you retain the default settings of the timers.

This command only sets the values of the timers. To enable the timers, perform corresponding configurations or use default settings.

- The client authentication timeout timer and the interval for sending authentication requests are enabled by default. You can run the **dot1x retry** command to configure the number of retransmissions of authentication request packets when the client authentication times out.
- The re-authentication timer for online 802.1X users is disabled by default. To enable this timer, run the **dot1x reauthenticate** command.
- The online 802.1X user handshake function is disabled by default. You can run the **dot1x handshake** command to enable the online 802.1X user handshake function. The handshake function takes effect only for the wired users.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

In the 802.1X access profile **d1**, set the client authentication timeout interval to 90 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x timer client-timeout 90
```

13.5.149 dot1x timer mac-bypass-delay

Function

The **dot1x timer mac-bypass-delay** command configures the 802.1X authentication timeout timer after which MAC address authentication is performed.

The **undo dot1x timer mac-bypass-delay** command restores the default configuration.

By default, the device performs MAC address authentication if 802.1X authentication is not successful within 30 seconds.

Format

dot1x timer mac-bypass-delay *delay-time-value*

undo dot1x timer mac-bypass-delay

Parameters

Parameter	Description	Value
delay-time-value	Specifies the value of the 802.1X authentication timeout timer after which MAC address authentication is performed.	The value is an integer in the range 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After MAC address bypass authentication is configured, the device performs 802.1X authentication first and starts the timer configured using the **dot1x timer mac-bypass-delay** *delay-time-value* command. If 802.1X authentication is not successful before the timer expires, the device performs MAC address authentication on users. You can run the **dot1x retry** *max-retry-value* command to set the number of times an authentication request is retransmitted to an 802.1X user. The retransmission interval is the integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)

Example

Configure the device to perform MAC address authentication if 802.1X authentication is not successful within 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer mac-bypass-delay 60
```

13.5.150 dot1x timer quiet-period

Function

The **dot1x timer quiet-period** command configures the quiet period for 802.1X users who fail to be authenticated.

The **undo dot1x timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for 802.1X users who fail to be authenticated.

Format

dot1x timer quiet-period *quiet-period-times*

undo dot1x timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-times	Sets the quiet period for 802.1X users who fail to be authenticated.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If an 802.1X authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled using the **dot1x quiet-period** command, if the number of times that an 802.1X user fails to be authenticated within 60s exceeds the upper limit (configured using the **dot1x quiet-times** command), the device discards the user's 802.1X authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for 802.1X users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer quiet-period 100
```

13.5.151 dot1x trigger dhcp-binding

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-connection phase.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through 802.1X authentication, the unauthorized users can obtain the same identities as the authorized users and connect to the network without authentication. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG and DAI. These two functions are implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After the static IP users who pass 802.1X authentication or are at the pre-authentication phase send EAP packets to trigger generation of the user information table, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface recorded in the table.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass 802.1X authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.

- In the interface view, run the **arp anti-attack check user-bind enable** command to enable DAI.

Precautions

- To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the 802.1X access profile is bound to enable the DHCP snooping function on the interface and globally.
- The EAP protocol does not specify a standard attribute to carry IP address information. Therefore, if the EAP request packet sent by a static IP user does not contain an IP address, the IP address information in the DHCP snooping binding table is obtained from the user' first ARP request packet with the same MAC address as the user information table after the user passes authentication. On a network, unauthorized users may forge authorized users' MAC addresses to initiate ARP snooping attacks to devices, and the DHCP snooping binding table generated accordingly may be unreliable. Therefore, the **dot1x trigger dhcp-binding** command is not recommended and you are advised to run the **user-bind static** command to configure the static binding table.
- For users who are assigned IP addresses using DHCP, you do not need to run the **dot1x trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.
- The IP address in the DHCP snooping binding table is extracted from the ARP request packet (the first ARP request packet sent by the user after the user is authenticated or in the pre-connection state that has the same MAC address in the user information table). If the static IP address of a user is changed, the user needs to be authenticated again.

Example

In the 802.1X access profile **d1**, enable the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x trigger dhcp-binding
```

13.5.152 dot1x timer tx-period

Function

The **dot1x timer tx-period** command sets the interval at which the device sends authentication requests.

The **undo dot1x timer tx-period** command restores the default configuration.

By default, the device sends authentication requests at an interval of 30 seconds.

Format

dot1x timer tx-period *tx-period-value*

undo dot1x timer tx-period

Parameters

Parameter	Description	Value
tx-period-value	Specifies the interval for sending authentication requests.	The value is an integer that ranges from 1 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device starts the **tx-period** timer in either of the following situations:

- When the client initiates authentication and MAC address bypass authentication is not configured, the device sends a unicast Request/Identity packet to the client and starts the **tx-period** timer. If the client does not respond within the period set by the timer, the device retransmits the authentication request.
- To authenticate the 802.1X clients that cannot initiate authentication, the device periodically sends multicast Request/Identity packets through the 802.1X-enabled interface to the clients at the interval set by the **tx-period** timer.

After MAC address bypass authentication is enabled on a device, the interval at which the device sends unicast Request/Identity packets to clients is determined by *delay-time-value* configured in the **dot1x timer mac-bypass-delay** command and *max-retry-value* configured in the **dot1x retry** command. The retransmission interval is the integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)

Normally, it is recommended that you retain the default setting of the timer.

Example

Set the interval at which the device sends authentication requests to 90 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer tx-period 90
```

13.5.153 dot1x unicast-trigger

Function

The **dot1x unicast-trigger** command enables the device to send unicast authentication packets to clients.

The **undo dot1x unicast-trigger** command disables the device from sending unicast authentication packets to clients.

By default, the device is disabled from sending unicast authentication packets to clients.

Format

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the pre-connection function is disabled and the **dot1x unicast-trigger** command is run on a device, the device sends a unicast authentication packet to respond to the received ARP , DHCPv6, ND, or DHCP Request packet from a client, which triggers authentication. If the client does not respond within the timeout interval (set by the **dot1x timer client-timeout** *client-timeout-value* command), the device retransmits the unicast packet (the maximum of retransmission times is set by the **dot1x retry** *max-retry-value* command). This function allows users to use the 802.1X client provided by the operating system for authentication, helping quickly deploy an 802.1X network.

After receiving a packet that triggers 802.1X authentication from a client, the device sends a unicast packet to the client. For clients that cannot send packets to trigger 802.1X authentication, configure multicast packets to trigger 802.1X authentication.

Prerequisites

The **undo authentication pre-authen-access enable** command has been run in the system view to disable the pre-connection function globally.

Example

In the 802.1X access profile **d1**, enable 802.1X authentication triggered by unicast packets.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name d1
[HUAWEI-dot1x-access-profile-d1] dot1x unicast-trigger
```

13.5.154 dot1x url

Function

The **dot1x url** command configures a redirect URL in 802.1X authentication.

The **undo dot1x url** command cancels the redirect URL configuration in 802.1X authentication.

By default, no redirect URL is configured in 802.1X authentication.

Format

dot1x url *url-string*

undo dot1x url

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the early stage of network deployment, 802.1X client deployment is difficult and requires heavy workload. You can run the **dot1x url** command to set a redirect URL to the web page address for downloading the 802.1X client. When a user attempts to access an IP subnet that requires authentication, the device redirects the user to the redirect URL where the user can download and install the 802.1X client software.

Follow-up Procedure

Run the **free-rule** command to configure the network segment where the redirect URL used in 802.1X authentication belongs or configure the IP address segment of the DNS server as an authentication-free IP subnet.

Precautions

This command applies when users use the 802.1X client software that is not provided by the system.

Wireless users do not support the redirect URL configuration in 802.1X authentication.

The device does not support the triggering of a redirect URL through HTTPS packets.

Example

Set the redirect URL in 802.1X authentication to http://10.1.1.1:8080/download.

```
<HUAWEI> system-view
[HUAWEI] dot1x url http://10.1.1.1:8080/download
```

13.5.155 dot1x-access-profile (authentication profile view)

Function

The **dot1x-access-profile** command binds an authentication profile to an 802.1X access profile.

The **undo dot1x-access-profile** command unbinds an authentication profile from an 802.1X access profile.

By default, an authentication profile is not bound to an 802.1X access profile.

Format

dot1x-access-profile *access-profile-name*

undo dot1x-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of an 802.1X access profile.	The value must be the name of an existing 802.1X access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to an 802.1X access profile, the authentication profile is enabled with 802.1X authentication. After the authentication profile is applied to the interface or VAP profile, 802.1X authentication can be performed on online users.

Prerequisites

An 802.1X access profile has been created using the **dot1x-access-profile (system view)** command.

Follow-up Procedure

Run the **authentication-profile** (Interface view or VAP profile view) command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one 802.1X access profile.

Example

Bind the authentication profile **dot1x_authen_profile1** to the 802.1X access profile **dot1x_access_profile1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name dot1x_access_profile1
[HUAWEI-dot1x-access-profile-dot1x_access_profile1] quit
[HUAWEI] authentication-profile name dot1x_authen_profile1
[HUAWEI-authen-profile-dot1x_authen_profile1] dot1x-access-profile dot1x_access_profile1
```

13.5.156 dot1x-access-profile (system view)

Function

The **dot1x-access-profile** command creates an 802.1X access profile and displays the 802.1X access profile view.

The **undo dot1x-access-profile** command deletes an 802.1X access profile.

By default, the device has a built-in 802.1X access profile named dot1x_access_profile.

Format

dot1x-access-profile name *access-profile-name*

undo dot1x-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of an 802.1X access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses 802.1X access profiles to uniformly manage all 802.1X users access configurations. To perform 802.1X authentication for the users in the interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to an 802.1X access profile.

Follow-up Procedure

Run the **dot1x-access-profile** command in the authentication profile view to bind the authentication profile to an 802.1X access profile.

Precautions

- The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in 802.1X access profile dot1x_access_profile can be modified and applied, but cannot be deleted.
- Before deleting an 802.1X access profile, ensure that this profile is not bound to any authentication profile.
- 802.1X client authentication and 802.1X access authentication are mutually exclusive. The two functions cannot be configured at the same time.

Example

Create the 802.1X access profile named **dot1x_access_profile1**.

```
<HUAWEI> system-view
[HUAWEI] dot1x-access-profile name dot1x_access_profile1
```

13.5.157 dns snooping enable

Function

The **dns snooping enable** command enables DNS snooping.

The **undo dns snooping enable** command disables DNS snooping.

By default, DNS snooping is disabled.

NOTE

Only the following switch models support this command:
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dns snooping enable

undo dns snooping enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **ucl-group domain** command is run to configure a domain name of a static UCL group, you also need to run the **dns snooping enable** command to enable the DNS snooping function. After this function is enabled, the device parses the received DNS response packets to obtain IP addresses and generates mappings between the IP addresses and domain names.

Precautions

DNS snooping needs to be applied on the interface connected to the DNS server.

Example

Enable DNS snooping.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dns snooping enable
```

13.5.158 dns snooping server-ip-address

Function

The **dns snooping server-ip-address** command configures the IP address of a DNS server.

The **undo dns snooping server-ip-address** command deletes the configuration of a DNS server IP address.

By default, no DNS server IP address is configured on the device.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dns snooping server-ip-address *server-ip-address*

undo dns snooping server-ip-address *server-ip-address*

Parameters

Parameter	Description	Value
server-ip-address	Specifies the IP address of a DNS server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After DNS snooping is enabled, the device parses the received DNS response packets to obtain IP addresses and generates mappings between the IP addresses and domain names. To prevent attacks initiated by DNS response packets, you can run the **dns snooping server-ip-address** command to specify the IP address of a DNS server. The device then processes only the DNS response packets with the configured DNS server IP address as the source IP address.

Example

Configure the DNS server IP address 10.1.1.1 on the device.

```
<HUAWEI> system-view
[HUAWEI] dns snooping server-ip-address 10.1.1.1
```

13.5.159 dns snooping ttl delay-time

Function

The **dns snooping ttl delay-time** command configures the delay in aging DNS snooping IP address and domain name entries.

The **undo dns snooping ttl delay-time** command restores the default configuration.

By default, the delay in aging DNS snooping IP address and domain name entries is 5760 minutes.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

dns snooping ttl delay-time *delay-time*

undo dns snooping ttl delay-time

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in aging IP address and domain name entries.	The value is an integer in the range from 0 to 43200, in minutes. If the value is set to 0, IP address and domain name entries do not age.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After DNS snooping is enabled using the **dns snooping enable** command, the device parses the received DNS response packets to obtain IP addresses and the aging time, and generates mappings between IP addresses and domain names. By default, the delay in aging IP address and domain name entries is 5760 minutes. You can run the **dns snooping ttl delay-time** command to adjust the delay.

Example

Set the delay in aging DNS snooping IP address and domain name entries to 5700 minutes.

```
<HUAWEI> system-view
[HUAWEI] dns snooping ttl delay-time 5700
```

13.5.160 eap-method

Function

The **eap-method** command sets the authentication mode of the device functioning as an 802.1X client.

The **undo eap-method** command deletes the authentication mode of the device functioning as an 802.1X client.

By default, no authentication mode is configured for the device functioning as an 802.1X client.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

eap-method { **eap-peap username** *username* **password cipher** *password* | **eap-tls username** *username* }

undo eap-method

Parameters

Parameter	Description	Value
eap-peap username *username*	Specifies the user name used for PEAP authentication.	The value is a string of 1 to 127 characters.
password cipher *password*	Specifies the password used for PEAP authentication.	The value is a string of 1 to 127 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
eap-tls username *username*	Specifies the user name used for TLS authentication.	The value is a string of 1 to 127 characters.

Views

802.1X client profile view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as an 802.1X client, you need to configure the 802.1X authentication mode. Both PEAP authentication and TLS authentication use the EAP relay mode. TLS authentication has higher security than PEAP authentication because:

- In PEAP authentication, the digital certificate is loaded only on the server.
- In TLS authentication, the digital certificate is loaded on both the server and client.

Example

Set the authentication mode of the device functioning as an 802.1X client to PEAP.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name d1
[HUAWEI-dot1x-client-profile-d1] eap-method eap-peap username test password cipher YsHsjx_202206
```

13.5.161 enable (terminal type identification profile view)

Function

The **enable** command enables terminal type identification.

The **undo enable** command disables terminal type identification.

By default, terminal type identification is disabled.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

enable

undo enable

Parameters

None

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The terminal type identification profile takes effect immediately when terminal type identification is enabled. The AC analyzes the terminal's MAC address, DHCP Option, and user agent information. If the information matches the rules configured in the profile, the AC identifies the terminal type.

Prerequisite

A terminal type identifier has been configured using the **device-type** command.

Example

Enable terminal type identification.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] device-type test
[HUAWEI-device-profile-test] enable
```

13.5.162 free-rule

Function

The **free-rule** command configures authentication-free rules for NAC authentication users.

The **undo free-rule** command restores the default settings.

By default, no authentication-free rule is configured for NAC authentication users.

Format

Common authentication-free rule:

free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } *

undo free-rule { *rule-id* | **all** }

Authentication-free rule defined by ACL:

free-rule acl { *acl-id* | **acl-name** *acl-name* | **ipv6** *ipv6-acl-id* }

undo free-rule { **acl** { *acl-id* | **acl-name** *acl-name* | **ipv6** *ipv6-acl-id* } | **all** }

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support authentication-free rules defined by IPv6 ACLs.

Parameters

Parameter	Description	Value
rule-id	Specifies the number of an authentication-free rule for NAC authentication users.	The value is an integer. S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I: The value range is 0 to 31. S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S : The value range is 0 to 511. S6735-S, S6720-EI, S6720S-EI: The value range is 0 to 255.
destination	Specifies the destination network resource that NAC authentication users can access without authentication.	-
source	Specifies source information for NAC authentication users without authentication.	-
any	Indicates any condition. When **any** is used together with different keywords, the effect of the command is different.	-
interface *interface-type interface-number*	Specifies a source interface in the rule. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** The source interface cannot be a management interface.	-

Parameter	Description	Value
ip *ip-address*	Specifies the source or destination IP address depending on the keyword.	The value is in dotted decimal notation. The configured IP address cannot be 255.255.255.255, all 0s, class D address, class E address, or loopback address. If the IP address is a class A address, the network ID cannot be all 0s.
mask *mask-length*	Specifies the mask length of the source or destination IP address depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the mask of the source or destination IP address depending on the keyword.	The value is in dotted decimal notation.
tcp destination-port *port*	Specifies a TCP destination port number.	The value is an integer that ranges from 1 to 65535.
udp destination-port *port*	Specifies a UDP destination port number.	The value is an integer that ranges from 1 to 65535.
vlan *vlan-id*	Specifies the VLAN ID of source packets.	The value is an integer that ranges from 1 to 4094.
acl	Specifies an authentication-free rule defined by ACL.	-
acl-id	Specifies the number of an IPv4 ACL.	The value is an integer that ranges from 6000 to 6031.
acl-name *acl-name*	Specifies the name of an IPv4 ACL.	The value must be the name of an existing IPv4 ACL with a number in the range from 6000 to 6031.
ipv6 *ipv6-acl-id*	Specifies the number of an IPv6 ACL.	The value is an integer that ranges from 3000 to 3031.
all	Specifies all rules.	-

Views

Authentication-free rule profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before being authenticated, users need to obtain some network access rights to meet basic network access requirements such as downloading the 802.1X client and updating the antivirus database. After running the **free-rule-template** command in the system view to create an authentication-free rule profile, run the **free-rule** command to configure authentication-free rules in the profile. The users then can obtain some network access rights without authentication.

An authentication-free rule can be a common authentication-free rule or an authentication-free rule defined by an ACL. A common authentication-free rule is determined by parameters such as IP address, MAC address, interface, and VLAN. An authentication-free rule defined by an ACL is determined by the ACL rule (configured using the **rule** command). The destination IP address that users can access without authentication can be specified in both a common authentication-free rule and an authentication-free rule defined by an ACL. In addition, the destination domain name that users can access without authentication can be specified in an authentication-free rule defined by an ACL.

Compared with the authentication-free rule defined by IP address, the one defined by domain name is sometimes simple and convenient. For example, some authentication users who do not have an authentication account must first log in to the official website of a carrier and apply for a member account, or log in using the account of a third party such as Twitter or Facebook. This requires that the users can access specified websites before successful authentication. The domain name of a website is easier to remember than the IP address; therefore, the authentication-free rule defined by ACL can be configured to enable the users to access the domain names of websites without authentication.

Prerequisites

To use the authentication-free rule defined by ACL: An ACL rule has been configured using the **rule** command. This ACL rule can be based on an IP address or a domain name. If the rule is defined by IP address, the **source** and **destination** parameters can be configured; if the rule is defined by domain name, only the **destination** parameter can be configured.

NOTE

If the user ACL is created using a name (specified by *acl-name*), a named ACL has been created and the ACL number (6000-6031) has been specified using the **acl name** *acl-name acl-number* command.

Follow-up Procedure

The domain name specified in an ACL only supports dynamic DNS resolution. Therefore, when you define the authentication-free rule by domain name, configure dynamic DNS resolution on the device. The procedure is as follows:

1. Run the **dns resolve** command in the system view to enable dynamic DNS resolution.
2. Run the **dns server** *ip-address* command in the system view to specify an IP address for the DNS server.

Precautions

Wireless 802.1X authentication does not support this function.

When 802.1X authentication or MAC address authentication is configured on a physical interface, the **free-rule** configuration will not take effect after the **undo authentication pre-authen-access enable** command is configured to disable the pre-connection function.

Pay attention to the following when you use common authentication-free rules:

- When multiple authentication-free rules are configured simultaneously, the system matches the rules one by one.
- In a wireless scenario or an SVF system, only the authentication-free rules with IDs in the range of 0 to 127 on the AP or AS can take effect. On the AC or parent, all configured authentication-free rules take effect.
- In a wireless scenario, the VLAN ID and interface number cannot be specified in authentication-free rules configured on an AP. You are advised to set the authentication-free rule ID to 128 or a larger value when specifying the VLAN ID and interface number. If the ID of an authentication-free rule is less than 128, Portal redirection cannot be performed.
- In an SVF system, interface information in an authentication-free rule is invalid.
- If you specify both the VLAN ID and interface number in an authentication-free rule, the interface must belong to the VLAN. Otherwise, the rule is invalid.
- If the destination port number is configured in an authentication-free rule, fragments cannot match the rule and packets cannot be forwarded.
- No authentication-free rule needs to be configured for DHCP, CAPWAP, ARP, and HTTP packets, because these packets can be processed or forwarded before user authentication. Authentication-free rules must be configured for other protocol packets that need to be forwarded. When the packets need to be processed locally, authentication-free rules need to be configured on only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. Authentication-free rules are not required if the **portal pass dns enable** command has been run to allow DNS packets to pass during Portal authentication. However, this mode is not recommended because the command allows all DNS packets to pass.
  - DHCP packet: If authentication and DHCP are enabled on an interface, authentication can be triggered by DHCP packets and the device acts as the DHCP relay or DHCP server to forward or process DHCP packets. If only authentication is configured on the interface and the DHCP function is not configured, authentication can be triggered by DHCP packets and the device broadcasts the DHCP packets.

  - CAPWAP packet: CAPWAP packets are classified into control packets and data packets. Generally, NAC is still effective for CAPWAP data packets after they are decapsulated, and the authentication-free rule takes effect (except for ARP and DHCP packets that are encapsulated in CAPWAP data packets). CAPWAP control packets are sent to the CPU for processing (such as SVF and wireless scenarios). If authentication is enabled on the physical interface connected to an AP, you need to configure the authentication-free rule to transmit packets from the management VLAN. In this scenario, the server may be overloaded due to multiple times of re-authentication. Therefore, this scenario is not recommended.
  - ARP packet: No authentication-free rule needs to be configured for ARP packets, which can be directly processed or forwarded.
  - HTTP packet: If Portal authentication is enabled on an interface and the destination URL of HTTP packets is not the URL of the Portal server, the device redirects HTTP packets to the Portal server for authentication. If the destination URL matches an authentication-free rule, redirection is not triggered. When both an authentication-free rule and an ACL are configured for authorization, only the authentication-free rule takes effect.

Pay attention to the following when you use authentication-free rules defined by ACLs:

- Authentication-free rules based on domain names are valid for only wireless users. Static UCL group and DNS snooping can be configured for wired users to be authenticated based on domain names.
- When SVF is enabled, authentication-free rules defined by ACL cannot be delivered to an AS.
- An authentication-free rule can be dynamically modified. The authentication-free rule performs the **permit** action no matter whether the action in an ACL rule (configured using the **rule** command) is set to **deny** or **permit**. The ACL rule number ranges from 0 to 127.
- If multiple domain names correspond to the same IP address and one matches the authentication-free rule, other domain names also match the authentication-free rule.

The **free-rule** command configures a rule for specifying the resources accessible to users before authentication. However, this command does not mean that users matching the rule do not need to be authenticated. To free specified users from authentication, run the **access-context profile enable** command to enable the user context identification function, and run the **if-match vlan-id** { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10> command in the user context profile to configure the VLAN ID-based user identification policy. In addition, run the **authentication-mode none** command to enable non-configuration in the authentication scheme bound in the authentication domain of the users.

Example

In the authentication-free rule profile **default_free_rule**, allow all NAC authentication users to access the network with the IP address 10.1.1.1/24 without authentication.

```
<HUAWEI> system-view
[HUAWEI] free-rule-template name default_free_rule
[HUAWEI-free-rule-default_free_rule] free-rule 1 destination ip 10.1.1.1 mask 24 source ip any
```

13.5.163 free-rule-template (authentication profile view)

Function

The **free-rule-template** command binds an authentication-free rule profile to an authentication profile.

The **undo free-rule-template** command unbinds an authentication-free rule profile from an authentication profile.

By default, no authentication-free rule profile is bound to an authentication profile.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

free-rule-template *free-rule-template-name*

undo free-rule-template

Parameters

Parameter	Description	Value
free-rule-template-name	Specifies the name of an authentication-free rule profile.	The value must be the name of an existing authentication-free rule profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before being authenticated, users need to obtain some network access rights to meet basic network access requirements such as downloading the 802.1X client and updating antivirus database. The device uses an authentication-free rule profile to uniformly manage authorization information for authentication-free users. You can define some network access rules in the profile to determine network access rights that can be obtained by authentication-free users. You need to bind a configured authentication-free rule profile to an authentication profile.

Users using the authentication profile then can obtain authentication-free authorization information.

Prerequisites

An authentication-free rule profile has been created using the **free-rule-template** command.

When a large number of APs are online, do not run the **free-rule-template** or **undo free-rule-template** command repeatedly because the device takes time to execute the command. Otherwise, users cannot go online or offline properly in a short period of time.

This command is not supported in AS mode.

For wireless users, the configured authentication-free rule in an authentication-free rule profile takes effect only after the profile is bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

For wired users, an authentication-free rule profile takes effect for all wired users after it is created in the system view. The authentication-free rule profile does not need to be bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

Example

Bind the authentication-free rule profile **default_free_rule** to the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] free-rule-template default_free_rule
```

13.5.164 free-rule-template (system view)

Function

The **free-rule-template** command creates an authentication-free rule profile and displays the authentication-free rule profile view.

By default, the device has a built-in authentication-free rule profile named **default_free_rule**.

Format

free-rule-template name *free-rule-template-name*

Parameters

Parameter	Description	Value
name *free-rule-template-name*	Specifies the name of an authentication-free rule profile.	Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To meet basic network access requirements of users who have not passed authentication, the users need to obtain some network access rights without authentication, for example, download 802.1X client software and update the antivirus database. After creating an authentication-free rule profile using the **free-rule-template** command, you can configure authentication-free rules in the profile to allow the users to access the specified network resources without authentication.

Follow-up Procedure

Run the **free-rule** command in the authentication-free rule profile view to configure authentication-free rules for users.

Precautions

Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

For wireless users, the configured authentication-free rule in an authentication-free rule profile takes effect only after the profile is bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

For wired users, an authentication-free rule profile takes effect for all wired users after it is created in the system view. The authentication-free rule profile does not need to be bound to an authentication profile using the **free-rule-template** command in the authentication profile view.

Example

Display the view of the authentication-free rule profile **default_free_rule**.

```
<HUAWEI> system-view
[HUAWEI] free-rule-template name default_free_rule
[HUAWEI-free-rule-default_free_rule]
```

13.5.165 http parse user-agent enable

Function

The **http parse user-agent enable** command enables the function of extracting User-Agent field information.

The **undo http parse user-agent enable** command disables the function of extracting User-Agent field information.

By default, the function of extracting User-Agent field information is disabled.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

http parse user-agent enable

undo http parse user-agent enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User Agent (UA) is a field in the HTTP packet header. This field carries the following information: operating system used by the device, operating system version, CPU type, browser type, browser version, language used by the browser, and browser plug-in.

If a terminal passes authentication and the UA function is enabled, the AC extracts the UA field from the HTTP Get packet sent from the terminal and sends the extracted information to the terminal type identification module, so that the module can identify the terminal type based on UA information, MAC address, and DHCP Option information.

Precautions

The device can parse the UA field with a maximum of 247 bytes.

This function takes effect only for wireless users.

Example

Enable the UA function.

```
<HUAWEI> system-view
[HUAWEI] http parse user-agent enable
```

13.5.166 http get-method enable

Function

The **http get-method enable** command configures the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

The **undo http get-method enable** command restores the default setting.

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication.

Format

http get-method enable

undo http get-method enable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication. You can run the **http get-method enable** command to configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

Precautions

The GET mode has the risk of password disclosure. Therefore, the POST mode is recommended.

This command only applies to scenarios in which HTTP or HTTPS is used for Portal connection establishment.

Example

Configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http get-method enable
```

13.5.167 http-method post

Function

The **http-method post** command configures parameters for parsing and replying to POST or GET request packets of the HTTP or HTTPS protocol.

The **undo http-method post** command restores the default configuration.

By default, the system has configured parameters for parsing and replying to POST or GET request packets of the HTTP or HTTPS protocol. For details, see the "Parameters" table.

Format

http-method post { **cmd-key** *cmd-key* [**login** *login-key* | **logout** *logout-key*] * | **init-url-key** *init-url-key* | **login-fail response** { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] } | **login-success response** { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* } | **logout-fail response** { **msg** *msg* | **redirect-url** *redirect-url* } | **logout-success response** { **msg** *msg* | **redirect-url** *redirect-url* } | **password-key** *password-key* | **user-mac-key** *user-mac-key* | **userip-key** *userip-key* | **username-key** *username-key* } *

undo http-method post { **all** | { **cmd-key** | **init-url-key** | **login-fail** | **login-success** | **logout-fail** | **logout-success** | **password-key** | **user-mac-key** | **userip-key** | **username-key** } * }

Parameters

Parameter	Description	Value
cmd-key *cmd-key*	Specifies the command identification keyword. The default value is **cmd**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
login *login-key*	Specifies the user login identification keyword. The default value is **login**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
logout *logout-key*	Specifies the user logout identification keyword. The default value is **logout**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
init-url-key *init-url-key*	Specifies the identification keyword for the user initial login URL. The default value is **initurl**. The value must be the same as that configured on the Portal server. **NOTE** If this parameter is configured together with other parameters, place this parameter at the end of all parameters.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-fail response { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] }	Specifies the response message upon a user login failure. - **err-msg authenserve-reply-message**: The response message returned by the authentication server is displayed upon a user login failure. - **err-msg msg** *msg*: A specified message is displayed upon a user login failure. - **redirect-login-url**: A user is redirected to the login URL upon a login failure. This mode is used by default. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a login failure. - **append-reply-message** *msgkey*: The redirect URL carries the identification keyword for the response message returned by the authentication server.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?). - *msgkey*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-success response { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* }	Specifies the response message upon successful user login. - **msg** *msg*: A specified message is displayed upon successful user login. - **redirect-init-url**: A user is redirected to the initial login URL upon successful login. This mode is used by default. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful login.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-fail response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon a user logout failure. - **msg** *msg*: A specified message is displayed upon a user logout failure. The default value is **LogoutFail!**. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a logout failure.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-success response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon successful user logout. - **msg** *msg*: A specified message is displayed upon successful user logout. The default value is **LogoutSuccess!**. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful logout.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).

Parameter	Description	Value
password-key *password-key*	Specifies the password identification keyword. The default value is **password**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
user-mac-key *user-mac-key*	Specifies the identification keyword for the user MAC address. The default value is **macaddress**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
userip-key *userip-key*	Specifies the identification keyword for the user IP address. The default value is **ipaddress**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
username-key *username-key*	Specifies the user name identification keyword. The default value is **username**. The value must be the same as that configured on the Portal server.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
all	Indicates all parameters.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

When the device uses the HTTP or HTTPS protocol to communicate with the Portal server, a user sends POST or GET request packets (carrying parameters such as the user name and MAC address) to the device as required by the Portal server.

After receiving the POST or GET request packets, the device parses parameters in the packets. If identification keywords of the parameters differ from those configured on the device, the user authentication fails. Therefore, you need to run the **http-method post** command to configure the identification keywords based on the Portal server configuration.

After successful user login or logout, or a user login or logout failure, the device sends the login or logout result to the user based on the **http-method post** command configuration. For example, the device sends the **LogoutSuccess!** message to a user who logs out successfully by default.

Example

Change the command identification keyword to **cmd1** on the device when the command identification keyword in POST request packets is **cmd1** on the connected Portal server.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http-method post cmd-key cmd1
```

13.5.168 force-push

Function

The **force-push** command enables a pushed URL template or pushed URL.

The **undo force-push** command disables a pushed URL template or pushed URL.

By default, no pushed URL template or pushed URL is enabled.

Format

force-push { **url-template** *template-name* | **url** *url-address* }

undo force-push

Parameters

Parameter	Description	Value
url-template *template-name*	Specifies the name of a pushed URL template.	The value must be the name of an existing URL template.
url *url-address*	Specifies a pushed URL.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a user sends an HTTP or HTTPS packet to access a web page for the first time after the user is successfully authenticated, the device forcibly redirects the user to a specified web page. In addition to pushing advertisement pages, the device obtains user terminal information through the HTTP or HTTPS packets sent by users, and applies the information to other services. There are two ways to push web pages:

1. URL: pushes the URL of the specified web page.
2. URL template: pushes a URL template. The URL template must have been created and contains the URL of the pushed web page and URL parameters.

Prerequisites

The URL configured using the **url** command in the URL template view cannot be a redirect URL; otherwise, the **force-push** command does not take effect.

Precautions

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the forcible web page push function takes effect only for the first HTTP or HTTPS packet sent from users. If an application that actively sends HTTP or HTTPS packets is installed on a user terminal and the terminal has sent HTTP or HTTPS packets before the user accesses a web page, the user is unaware of the web page push process.

For switches except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: The forcible web page push function takes effect only when it is used together with a redirect ACL. If a redirect ACL exists in the user table, a web page is forcibly pushed when HTTP or HTTPS packets from users match the redirect ACL rule. Usually, you can configure the RADIUS server to authorize the Huawei extended RADIUS attribute **HW-Redirect-ACL** or **HW-IPv6-Redirect-ACL** to users for redirect ACL implementation, or run the **redirect-acl** command to configure a redirect ACL.

A pushed URL configured in a domain needs to be used together with a redirect ACL or push flag attribute. The redirect ACL has a higher priority than the push flag attribute. By default, a pushed URL configured in a domain carries the push flag attribute. Users will be redirected to the pushed URL when they are successfully authenticated.

When an IPv4 redirect ACL is configured for an IPv6 user or an IPv6 redirect ACL is configured for an IPv4 user, the **Push URL content** field in the **display access-user** command output displays the pushed URL, but the browser of the user cannot redirect to the pushed URL.

Switches except the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support concurrent use of the pushed URL and redirection ACL6 functions. If both functions are configured, the **Push URL content** field in the **display access-user** command output displays the pushed URL; however, the terminal browser cannot be redirected to the pushed URL.

Example

Enable the pushed URL template **abc** in the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] url-template name abc
[HUAWEI-url-template-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] force-push url-template abc
```

13.5.169 if-match vlan-id

Function

The **if-match vlan-id** command configures the VLAN ID-based user identification policy.

The **undo if-match vlan-id** command deletes the VLAN ID-based user identification policy.

By default, no VLAN ID-based user identification policy is configured.

Format

if-match vlan-id { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10>

undo if-match vlan-id { *start-vlan-id* [**to** *end-vlan-id*] } &<1-10>

Parameters

Parameter	Description	Value
start-vlan-id [**to** *end-vlan-id*]	Specifies the start and end user VLAN IDs. The value of *end-vlan-id* must be equal to or greater than that of *start-vlan-id*. If the parameter **to** *end-vlan-id* is not specified, users are classified based on the VLAN ID specified by *start-vlan-id*.	The value of *start-vlan-id* or *end-vlan-id* is an integer that ranges from 1 to 4094.

Views

User context profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On some enterprise networks, VLANs are used to divide the entire network into different areas with various security levels. The administrator requires that a user should obtain different network access rights when the user connects to the network from different areas. In this case, the user context identification function can be enabled on access devices, and a group of VLANs that belong to the same area are added to the same user context profile. The administrator then assigns the mapping network access rights to different user context profiles based on the security level of each area. When a user connects to the network from different areas, the user is added to different user context profiles matching their access VLANs and therefore obtains different network access rights.

Prerequisites

A user context profile has been created using the **access-context profile name** *profile-name* command in the system view.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Example

In the user context profile **p1**, configure the user identification policy of matching users in VLAN 10 to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] access-context profile name p1
[HUAWEI-access-context-p1] if-match vlan-id 10 to 20
```

13.5.170 if-match

Function

The **if-match** command configures the matching mode of terminal type identification rules.

The **undo if-match** command deletes the matching mode of terminal type identification rules.

By default, no matching mode of terminal type identification rules is configured.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

if-match rule *rule-id* [{ **and** | **or** } **rule** *rule-id*] &<1-7>

undo if-match

Parameters

Parameter	Description	Value
rule *rule-id*	Specifies the ID of a terminal type identification rule.	The value is an integer that ranges from 0 to 7.
and	Specifies the matching mode as "and" (that is, a terminal type can be identified only when the terminal information matches all rules configured).	-
or	Specifies the matching mode as "or" (that is, a terminal type can be identified when the terminal information matches any of the rules).	-

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **if-match** command allows you to flexibly combine terminal type identification rules.

Prerequisite

The specified terminal type identification rules have been configured using the **rule** command.

Precautions

If the **and** parameter is specified and the terminal information does not match the first rule, the AC sends a matching failure response and stops matching the following rules.

The priority of **and** is higher than that of **or**. For example, you run the **if-match rule 1 or rule 2 and rule 3 or rule 4 and rule 5 or rule 6 and rule 7 or rule 0** command. If the terminal information matches any of the five rule combinations, which are rule 1, rule 2 and rule 3, rule 4 and rule 5, rule 6 and rule 7, and rule 0, the matching operation succeeds.

Example

Specify that terminal information must match terminal type identification rule 1.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] if-match rule 1
```

13.5.171 ip-static-user enable

Function

The **ip-static-user enable** command enables the function of identifying static users through IP addresses.

The **undo ip-static-user enable** command restores the default configuration.

By default, the function of identifying static users through IP addresses is disabled, and the device identifies static users through MAC addresses.

NOTE

This command is supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

ip-static-user enable

undo ip-static-user enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device identifies static users through MAC addresses. However, a terminal may have only one MAC address and multiple IP addresses. The terminal can go online only after its multiple IP addresses pass authentication. If the device identifies terminals through MAC addresses, entry information about a terminal's IP address that is authenticated later overwrites entry information about the terminal's another IP address that is authenticated earlier. As a result, the terminal cannot go online. To resolve this problem, run the **ip-static-user enable** command to enable the device to identify static users through IP addresses, so that terminals with one MAC address and multiple IP addresses can go online.

Prerequisites

A static user has been configured before this function is enabled.

1. A static user has been configured using the **static-user** *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*] [**ip-user**] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**detect**] | **mac-address** *mac-address* | **vlan** *vlan-id*] * command.
2. The authentication user name has been configured for the static user using the **static-user username format-include** { **ip-address** | **mac-address** | **system-name** } command.
3. The authentication password has been configured for the static user using the **static-user password cipher** *password* command.

Precautions

- For a terminal with one MAC address and multiple IP addresses, you must configure the terminal as a static user and enable the function of identifying static users through IP addresses so that the terminal can pass authentication and go online. If **ip-user** is not specified when you configure static users, all static users are processed by assuming they have one MAC address and multiple IP addresses. To precisely identify and process static users with one MAC address and multiple IP addresses, specify **ip-user** when configuring these static users.
- The device does not support traffic statistics collection for a terminal with one MAC address and multiple IP addresses.
- This function is supported only for wired users.
- This function takes effect only for new users who go online after the function is configured. After the configuration on an interface is modified, online users on the interface go offline.
- The device supports this function only when the user access mode is **multi-authen**. For details about how to configure the user access mode, see **authentication mode**.
- Static users who are identified through IP addresses will go offline if they fail the authentication. In this case, the **display access-user (all views)** command cannot display any information about these users, including their states: pre-authentication or authentication failure.
- Static users identified through IP addresses do not support MAC address flapping.
- Static users identified through IP addresses do not support permission control during Layer 2 forwarding.
- Static users identified through IP addresses support only IP address-based upstream authorization services (such as UCL-based authorization, isolation between Layer 3 groups, CAR, and priority for upstream traffic), and do not support downstream authorization services (such as CAR, re-marking action, dynamic VLAN-based authorization, and HQoS for downstream traffic).
- In the policy association scenario, if the control point mode is set to **open** using the **authentication control-point open** command, the device does not support the function of identifying static users through IP addresses.

- For a terminal with one MAC address and multiple IP addresses, only ARP packets can trigger authentication. Therefore, ensure that the device can perform authentication triggered by ARP packets; for example, the types of packets that can trigger authentication must include ARP.
- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the **ip-static-user enable** and **authentication trigger-condition any-l2-packet** commands are both configured, user authentication cannot be triggered by any Layer 2 packets.
- If user A with multiple IP addresses and one MAC address goes online and then user B with multiple IP addresses and multiple MAC addresses (including user A's MAC address) in a different VLAN from user A also goes online, user A cannot access the network.
- If user A with multiple IP addresses and one MAC address is online and then web user B with the same MAC address is successfully authenticated, the entry of user A is overwritten by that of user B. In this case, user A still has network access rights.

Example

Enable the function of identifying static users through IP addresses in the authentication profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] ip-static-user enable
```

13.5.172 link-down offline delay

Function

The **link-down offline delay** command configures the user logout delay when an interface link is faulty.

The **undo link-down offline delay** command restores the default configuration.

By default, the user logout delay is 10 seconds when an interface link is faulty.

Format

link-down offline delay { *delay-value* | **unlimited** }

undo link-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when an interface link is faulty.	The value is an integer that ranges from 0 to 60, in seconds. If the value is 0, users are logged out immediately when an interface link is faulty.

Parameter	Description	Value
unlimited	Indicates that users are not logged out when an interface link is faulty.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a link is faulty, the interface is interrupted and users are directly logged out. To solve this problem, you can configure the user logout delay function. When the interface link is faulty, the users remain online within the delay. In this case, if the link is restored, the users do not need to be re-authenticated. If the users are disconnected after the delay and the link is restored, the users need to be re-authenticated.

Precautions

- This function takes effect only for wired users who go online on Layer 2 physical interfaces that have been configured with NAC authentication.
- To make the function take effect, it is recommended that the configured interval be greater than the time during which the interface is in Up state. If the link frequently flaps within a short period, it is recommended that the interval be set to **unlimited**.

Example

In the authentication profile **p1**, set the user logout delay to 5 seconds when the link is faulty.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name p1
[HUAWEI-authen-profile-p1] link-down offline delay 5
```

13.5.173 lldp sensor-ap authentication disable

Function

The **lldp sensor-ap authentication disable** command disables an NAC-enabled interface of a switch from performing authentication on Huawei APs identified through LLDP.

The **undo lldp sensor-ap authentication disable** command restores the default configuration.

By default, an NAC-enabled interface on a switch needs to authenticate Huawei APs identified through LLDP.

Format

lldp sensor-ap authentication disable

undo lldp sensor-ap authentication disable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In wired and wireless convergence scenarios, an NAC-enabled interface on a switch authenticates APs and terminals (such as printers and PCs) that go online on this interface. If APs and connected terminals on the live network are secure and do not require NAC authentication, you can run this command to disable authentication on the APs and terminals.

Precautions

- If an AP already has online wireless users, these users will go online after you run the **undo lldp sensor-ap authentication disable** command.
- This command takes effect only when the authentication profile is applied to a Layer 2 interface.
- This function does not take effect in policy association and SVF scenarios.
- This function takes effect only for Huawei APs.
- When an authentication profile configured with this command is bound to an interface, all terminals using this authentication profile can connect to the network without being authenticated.

Example

Disable a switch from performing authentication on Huawei APs identified through LLDP in the view of the authentication profile **authen1**.

```
<HUAWEI> system-view
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] lldp sensor-ap authentication disable
```

13.5.174 load-file (WLAN view)

Function

The **load-file** command manually loads a certificate file on an AP.

The **undo load-file** command cancels manual certificate file loading on an AP.

By default, no certificate file is manually loaded on an AP.

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Format

load-file { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** }

undo load-file { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Loads a certificate file on an AP with the specified AP ID.	The AP ID must already exist.
ap-group *ap-group*	Loads a certificate file on APs in the specified AP group.	The AP group must already exist.
all	Loads a certificate file on all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When certificate files are configured on an AC, the AC automatically delivers all the certificate files to an AP after the AP goes online. However, if a certificate file is modified or deleted, or a certificate file is added after the AP goes online, the AC cannot automatically deliver the certificate file again. You can run this command to manually deliver the certificate file to the AP.

Precautions

- After the **undo load-file** { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** } command is run, certificate files are no longer delivered to the current AP and subsequent APs. This does not affect the certificate files that have been delivered to APs.
- After the **load-file** { **ap-id** *ap-id* | **ap-group** *ap-group* | **all** } command is run, if a certificate file fails to be loaded on an AP, certificate file re-loading is automatically triggered. By default, a certificate file can be re-loaded three times.
- If a certificate file is being loaded on an AP, the command cannot be run repeatedly.

Example

Manually load certificate files to APs in the AP group named **ap-group1**.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] load-file ap-group ap-group1
```

13.5.175 mac-access-profile (authentication profile view)

Function

The **mac-access-profile** command binds an authentication profile to a MAC access profile.

The **undo mac-access-profile** command unbinds an authentication profile from a MAC access profile.

By default, an authentication profile is not bound to a MAC access profile.

Format

mac-access-profile *access-profile-name*

undo mac-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of a MAC access profile.	The value must be the name of an existing MAC access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to a MAC access profile, the authentication profile is enabled with MAC address authentication. After the authentication profile is applied to the interface or VAP profile, MAC address authentication can be performed on online users.

Prerequisites

A MAC access profile has been created using the **mac-access-profile (system view)** command.

Follow-up Procedure

Run the **authentication-profile** command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one MAC access profile.

Example

Bind the authentication profile **mac_authen_profile1** to the MAC access profile **mac_access_profile**.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] quit
[HUAWEI] authentication-profile name mac_authen_profile1
[HUAWEI-authen-profile-mac_authen_profile1] mac-access-profile mac_access_profile
```

13.5.176 mac-access-profile (system view)

Function

The **mac-access-profile** command creates a MAC access profile and displays the MAC access profile view.

The **undo mac-access-profile** command deletes the MAC access profile.

By default, the device has a built-in MAC access profile named **mac_access_profile**.

Format

mac-access-profile name *access-profile-name*

undo mac-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of a MAC access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses MAC access profiles to uniformly manage all MAC users access configurations. To perform MAC address authentication for the users in the interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to a MAC access profile.

Follow-up Procedure

Run the **mac-access-profile** command in the authentication profile view to bind the authentication profile to a MAC access profile.

Precautions

- The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in MAC access profile **mac_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a MAC access profile, ensure that this profile is not bound to any authentication profile.

Example

Create the MAC access profile named **mac_access_profile**.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
```

13.5.177 mac-authen authentication-method

Function

The **mac-authen authentication-method** command configures the authentication mode for MAC address authentication.

The **undo mac-authen authentication-method** command restores the default configuration.

By default, the authentication mode for MAC address authentication is set to PAP.

Format

mac-authen authentication-method { **chap** | **pap** }

undo mac-authen authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the Challenge Handshake Authentication Protocol (CHAP) authentication mode.	-
pap	Indicates the Password Authentication Protocol (PAP) authentication mode.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MAC address authentication, the access device exchanges RADIUS packets with the authentication server. Differences between authentication modes PAP and CHAP are as follows:

- PAP is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.
- CHAP is a three-way handshake authentication protocol. It transmits only user names but not passwords in RADIUS packets.

By default, the authentication mode for MAC address authentication is set to PAP.

Precautions

The authentication server must support CHAP when the authentication mode is set to CHAP.

Example

In the MAC access profile **mac_access_profile**, set the authentication mode for MAC address authentication to CHAP.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen authentication-method chap
```

13.5.178 mac-authen offline dhcp-release

Function

The **mac-authen offline dhcp-release** command enables the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

The **undo mac-authen offline dhcp-release** command restores the default configuration.

By default, the device does not clear user entries when receiving DHCP Release packets from MAC address authentication users.

Format

mac-authen offline dhcp-release

undo mac-authen offline dhcp-release

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication users who send DHCP Release packets go offline, the corresponding user entries on the device cannot be deleted immediately. This occupies device resources and possibly prevents other users from going online. You can run this command to enable the device to clear the user entries in real time when MAC address authentication users go offline.

Precautions

MAC address authentication users who go online through VLANIF interfaces do not support this function.

If the device functions as a DHCP relay agent, configure the DHCP snooping function on the device; otherwise, this command does not take effect.

Example

In the MAC access profile **m1**, enable the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen offline dhcp-release
```

13.5.179 mac-authen permit mac-address

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.

Parameter	Description	Value
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a new MAC address entry is generated on the device after MAC address authentication is enabled on a VLANIF interface, MAC address authentication will be performed for the corresponding user. To actually control the users who can be authenticated using MAC addresses on the VLANIF interface, use this command to specify a MAC address range for MAC address authentication.

Precautions

Only MAC address authentication users who go online through VLANIF interfaces support this function.

A maximum of eight MAC address ranges are allowed for MAC address authentication on a VLANIF interface.

Example

In the MAC access profile **m1**, set the MAC address to 00e0-fc01-0101 and the MAC address mask length to 24 for MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen permit mac-address 00e0-fc01-0101 mask 24
```

13.5.180 mac-authen quiet-times

Function

The **mac-authen quiet-times** command configures the maximum number of authentication failures within 60 seconds before a MAC address authentication user enters the quiet state.

The **undo mac-authen quiet-times** command restores the maximum number of authentication failures to the default value.

By default, the maximum number of authentication failures is 10.

Format

mac-authen quiet-times *fail-times*

undo mac-authen quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a MAC address authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The quiet function for MAC address authentication is enabled on a device by default. When the maximum number of authentication failures exceeds 10 within 60 seconds, the device quiets a MAC address authentication user and does not process authentication requests from the user, reducing impact on the system caused by attackers.

Precautions

After the maximum number of authentication failures is set to a value larger than the configured value, the user in quiet state can initiate reauthentication only after the quiet period expires. If the user enters an incorrect user name or password again, the user authentication fails. The device does not quiet the user but allows the user to initiate reauthentication immediately.

The quiet function for MAC address authentication users takes effect only after the pre-connection function is disabled using the **undo authentication pre-authen-access enable** command and the device is disabled from assigning network access rights to users in each phase before authentication succeeds using the **undo authentication event action authorize** command.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] mac-authen quiet-times 4
```

13.5.181 mac-authen reauthenticate mac-address

Function

The **mac-authen reauthenticate mac-address** command enables re-authentication for an online MAC address authentication user with a specified MAC address.

By default, re-authentication for an online MAC address authentication user with a specified MAC address is disabled.

Format

mac-authen reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies all valid unicast MAC addresses.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **mac-authen reauthenticate**.

The **mac-authen reauthenticate mac-address** and **mac-authen reauthenticate** commands re-authenticate online MAC address authentication users and their difference is as follows:

- The **mac-authen reauthenticate mac-address** command configures the device to immediately re-authenticate a user with a specified MAC address for once.
- The **mac-authen reauthenticate** command configures the device to re-authenticate all online MAC address authentication users at intervals.
- The **mac-authen reauthenticate mac-address** command does not support re-authentication for MAC address authentication users in pre-connection state.

Example

Enable re-authentication for an online MAC address authentication user with the MAC address 00e0-fc02-0003.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate mac-address 00e0-fc12-3456
```

13.5.182 mac-authen reauthenticate

Function

The **mac-authen reauthenticate** command enables re-authentication for online MAC address authentication users.

The **undo mac-authen reauthenticate** command restores the default configuration.

By default, re-authentication for online MAC address authentication users is disabled.

Format

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the administrator modifies the authentication parameters of an online user on the authentication server, the user must be re-authenticated to ensure user validity.

After the user goes online, the device saves authentication parameters of the user. After re-authentication is configured for online MAC address authentication users, the device automatically sends the user authentication parameters in the MAC access profile to the authentication server at an interval (specified using the **mac-authen timer reauthenticate-period** command) for re-authentication. If the user authentication information on the authentication server remains unchanged, the users are kept online. If the information has been changed, the users are disconnected and need to be re-authenticated based on the changed authentication parameters.

Precautions

After periodic re-authentication is configured for online MAC address authentication users, a large number of MAC address authentication logs are generated.

This function takes effect only for users who go online after this function is successfully configured.

MAC address authentication users who go online through a VLANIF interface do not support re-authentication.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

In the MAC access profile **mac_access_profile**, configure re-authentication for online MAC address authentication users.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen reauthenticate
```

13.5.183 mac-authen reauthenticate dhcp-renew

Function

The **mac-authen reauthenticate dhcp-renew** command enables the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

The **undo mac-authen reauthenticate dhcp-renew** command restores the default setting.

By default, the device does not re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Format

mac-authen reauthenticate dhcp-renew

undo mac-authen reauthenticate dhcp-renew

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After users go online, the administrator may modify the users' authentication parameters or network access rights on the authentication server. To ensure user validity or update the users' network access rights in real time, you can run this command to enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Precautions

MAC address authentication users who go online through a VLANIF interface do not support re-authentication.

This function applies only to Layer 2 BNG scenarios.

Example

In the MAC access profile **m1**, enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen reauthenticate dhcp-renew
```

13.5.184 mac-authen timer quiet-period

Function

The **mac-authen timer quiet-period** command configures the quiet period for MAC address authentication users who fail to be authenticated.

The **undo mac-authen timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for MAC address authentication users who fail to be authenticated.

Format

mac-authen timer quiet-period *quiet-period-value*

undo mac-authen timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Sets the quiet period for MAC address authentication users who fail to be authenticated.	The value is an integer that ranges from 0 to 3600, in seconds. **NOTE** If the value of *quiet-period-value* is 0, the quiet function is disabled for MAC address authentication users.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a MAC address authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled, if the number of times that a MAC address authentication user fails to be authenticated within 60s exceeds the upper limit (configured using the **mac-authen quiet-times** command), the device discards the user's MAC address authentication request packets for a period to avoid frequent authentication failures.

NOTE

The quiet function for MAC address authentication users takes effect only after the pre-connection function is disabled using the **undo authentication pre-authen-access enable** command and the device is disabled from assigning network access rights to users in each phase before authentication succeeds using the **undo authentication event action authorize** command.

Example

Set the quiet period to 100 seconds for MAC address authentication users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] mac-authen timer quiet-period 100
```

13.5.185 mac-authen timer reauthenticate-period

Function

The **mac-authen timer reauthenticate-period** command configures the re-authentication interval for online MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default setting.

By default, the re-authentication period is 1800 seconds for online MAC address authentication users.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the interval for re-authenticating online MAC address authentication users.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring the re-authentication function for online MAC address authentication users using the **mac-authen reauthenticate** command, run the **mac-authen timer reauthenticate-period** command to configure the re-authentication interval. The device then re-authenticates online users at the specified interval, ensuring that only authorized users can keep online.

Precautions

Generally, the default re-authentication interval is recommended. If many ACL rules need to be delivered during user authorization, to improve the device processing performance, you are advised to disable re-authentication or increase the re-authentication internal. When remote authentication and authorization are used and a short re-authentication interval is used, the CPU usage may become high.

MAC address authentication users who go online through a VLANIF interface do not support re-authentication.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

In the MAC access profile **mac_access_profile**, configure the re-authentication interval for online MAC address authentication users to 2000 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen timer reauthenticate-period 2000
```

13.5.186 mac-authen trigger dhcp-binding

Function

The **mac-authen trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-connection phase.

The **undo mac-authen trigger dhcp-binding** command restores the default configuration.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

Format

mac-authen trigger dhcp-binding

undo mac-authen trigger dhcp-binding

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through MAC address authentication, the unauthorized users can obtain the same identities as the authorized users. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG. This function is implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After this function is enabled, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface information of static IP users who pass MAC address authentication or are at the pre-authentication phase.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass MAC address authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.

Precautions

- To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the mac access profile is bound to enable the DHCP snooping function on the interface and globally.
- The authentication profile bound to the MAC access profile in which the command is configured must be applied to a Layer 2 interface. If the authentication profile is applied to a Layer 3 interface, the command does not take effect.
- For users who are assigned IP addresses using DHCP, you do not need to run the **mac-authen trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function. For static IP users (for example, users who trigger authentication by sending ARP packets carrying IP addresses), run the **mac-authen trigger dhcp-binding** command and configure DHCP snooping on the device to generate DHCP snooping binding entries.
- The IP address in the DHCP snooping binding table is extracted from the ARP request packet (the first ARP request packet sent by the user after the user is authenticated or in the pre-connection state that has the same MAC address in the user information table).
- This function trusts only the first ARP packet in the authentication process. If a client sends an ARP packet with a non-static IP address during authentication and then sends an ARP packet with the real IP address, the

DHCP snooping binding table is not updated. After this function is enabled, online users cannot change their static IP addresses. If the static IP address of a user is changed, the user needs to be authenticated again.

Example

In the MAC access profile **m1**, enable the device to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name m1
[HUAWEI-mac-access-profile-m1] mac-authen trigger dhcp-binding
```

13.5.187 mac-authen username

Function

The **mac-authen username** command configures the user name for MAC address authentication.

The **undo mac-authen username** command restores the default setting.

By default, the MAC address without hyphens (-) or colons (:) is used as the user name and password for MAC address authentication.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* { **circuit-id** | **remote-id** } * [**separate** *separate*] [**format-hex**] **password cipher** *password* }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* [**circuit-id** | **remote-id**] * [**password cipher** *password*]]

Parameters

Parameter	Description	Value
fixed *username*	Specifies a fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
password cipher *password*	Specifies the password in cipher text for MAC address authentication. ● You do not need to set a password for a fixed user name if the authentication mode is none. In this case, the user can log in without a password. However, this poses security risks and is not recommended. ● If no password is set when the MAC address is used as the user name, the user can log in using the MAC address as the password. A password must be configured when local authentication is used in the AAA scheme. ● The password must be configured when the user name for MAC address authentication is in the DHCP option format.	The value is a string of case-sensitive characters without spaces. The password is either a plain-text string of 1 to 128 characters or a cipher-text string of 48 to 188 characters. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** For security purposes, change the default password in real time. The new password must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters. In addition, the password must consist of six or more than eight characters.

Parameter	Description	Value
macaddress	Specifies the MAC address as the user name for MAC address authentication.	-
format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** }	Specifies the MAC address format. - **with-hyphen**: indicates that the MAC address contains hyphens (-), the format is xxxx-xxxx-xxxx. - **with-hyphen normal**: indicates that the MAC address contains hyphens (-), the format is xx-xx-xx-xx-xx-xx. - **with-hyphen colon**: indicates that the MAC address contains colons (:), the format is xxxx:xxxx:xxxx. - **with-hyphen normal colon**: indicates that the MAC address contains colons (:), the format is xx:xx:xx:xx:xx:xx. - **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), the format is xxxxxxxxxxxx.	-
uppercase	Indicates that the name of a MAC address authentication user is in uppercase.	-
dhcp-option *option-code*	Specifies the name of the MAC address authentication user to a specified DHCP option. - **circuit-id**: Specifies the circuit ID in the DHCP Option82 field as the user name in MAC address authentication. - **remote-id**: Specifies the remote ID in the DHCP Option82 field as the user name in MAC address authentication. If both **circuit-id** and **remote-id** are configured, the user name for MAC address authentication can be set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field.	The value is an integer. In the current version, the value is fixed as 82.

Parameter	Description	Value
separate *separate*	Specifies the delimiter in the user name for MAC address authentication. This parameter is configured when the user name for MAC address authentication is set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field.	The value is a character and can be set to a letter, digit, or another valid character.
format-hex	Indicates that the user name for MAC address authentication is in hexadecimal format.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following user name formats are available for MAC address authentication:

- Fixed user name: A user uses the fixed user name and password configured by the administrator for authentication.
- MAC address: A user uses the MAC address as the user name for authentication. In addition, the MAC address or user-defined character string can be used as the password.
- When the DHCP option format is used for MAC address authentication, the device uses the DHCP option it obtains and password set by the administrator for authentication. In this mode, ensure that the device supports MAC address authentication triggered through DHCP packets.

By default, the device sends the user MAC address as the user name and password to the authentication server for authentication. However, the users cannot be easily identified and managed in this case. To flexibly identify and manage users, run the **mac-authen username** command to configure fixed user names and passwords for MAC address authentication users.

Precautions

- When configuring the user name format for MAC address authentication, ensure that the authentication server supports the user name format.
- If MAC address authentication is enabled on a VLANIF interface, on an Eth-Trunk, in a port group, or in a VAP profile, and MAC address authentication users use fixed user names, passwords must be configured. If MAC address

authentication is enabled in a port group and MAC addresses are used as user names, passwords cannot be configured. If MAC address authentication is enabled on a VLANIF interface or in a VAP profile, user names for MAC address authentication cannot be set to specified DHCP option information.

Example

In the MAC access profile **mac_access_profile**, configure the device to use the MAC address containing hyphens (-) as the user name.

```
<HUAWEI> system-view
[HUAWEI] mac-access-profile name mac_access_profile
[HUAWEI-mac-access-profile-mac_access_profile] mac-authen username macaddress format with-hyphen
```

13.5.188 match access-context-profile action

Function

The **match access-context-profile action** command configures the network access rights for specified users in each phase before authentication success based on user context profiles.

The **undo match access-context-profile action** command deletes the configured network access rights.

By default, no network access right is configured for specified users in each phase before authentication success.

Format

match access-context-profile *profile-name* **action** { **authen-fail service-scheme** *service-scheme-name* | **authen-server-down service-scheme** *service-scheme-name* | **authen-server-up re-authen** | **client-no-response service-scheme** *service-scheme-name* | **portal-server-down service-scheme** *service-scheme-name* | **portal-server-up re-authen** | **pre-authen service-scheme** *service-scheme-name* } *

undo match access-context-profile *profile-name* **action** { **authen-fail** | **authen-server-down** | **authen-server-up** | **client-no-response** | **portal-server-down** | **portal-server-up** | **pre-authen** } *

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a user context profile.	The value must be the name of an existing user context profile.

Parameter	Description	Value
authen-fail	Configures the device to assign network access rights to users when the authentication server sends authentication failure packets to the device.	-
authen-server-down	Configures the device to assign network access rights to users when the authentication server is unreachable and thereby the users fail to be authenticated.	-
authen-server-up	Re-authenticates users when the authentication server can be reachable again.	-
client-no-response	Configures the device to assign network access rights to users when clients do not respond and thereby the users fail to be authenticated.	-
portal-server-down	Configures the device to assign network access rights to users when the Portal server is unreachable and thereby the users fail to be authenticated.	-
portal-server-up	Re-authenticates users when the Portal server can be reachable again.	-
pre-authen	Configures the device to assign network access rights to users when the users establish pre-connections with the device.	-
re-authen	Re-initializes user rights.	-
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be the name of an existing service scheme name on the device.

Views

User authentication event authorization policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users need basic network access rights before they are authenticated. For example, the users need to download 802.1X clients and update the antivirus database. A user authentication event authorization policy can be used to bind the network access rights of users in each phase before authentication success to a user context profile. When a user goes online after a user authentication event authorization policy is applied to the device, the device adds the user to the context profile based on the user context identification result, and assigns the network access rights to the user based on the user authentication result. The **match access-context-profile action** command can be used to configure the network access rights for users in each phase (including an authentication failure, an authentication server fault, and no response from the users) before authentication success.

Prerequisites

- A service scheme has been created using the **service-scheme** command in the AAA view.
- A user context profile has been created using the **access-context profile name** *profile-name* command in the system view.

Follow-up Procedure

In the global view, run the **access-author policy global** command to apply the user authentication event authorization policy.

Precautions

The priority of user authorization based on a user context profile is higher than that of user authorization in an authentication profile.

This function takes effect only for users who go online after this function is successfully configured.

Example

Match the user authentication event authorization policy **a1** with the identification result of the user context profile **p1**, and use the service scheme **s1** to authorize the users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] access-context profile name p1
[HUAWEI-access-context-p1] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme s1
[HUAWEI-aaa-service-s1] quit
[HUAWEI-aaa] quit
[HUAWEI] access-author policy name a1
[HUAWEI-access-author-a1] match access-context-profile p1 action authen-fail service-scheme s1
```

13.5.189 match access-context-profile action access-domain

Function

The **match access-context-profile action access-domain** command configures the access user's authentication domain based on the user context profile.

The **undo match access-context-profile action access-domain** command deletes the access user's authentication domain based on the user context profile.

By default, no access user's authentication domain is configured based on the user context profile.

Format

match access-context-profile *profile-name* **action access-domain** *domain-name* [**dot1x** | **mac-authen** | **portal**] * [**force**]

undo match access-context-profile *profile-name* **action access-domain** [**dot1x** | **mac-authen** | **portal**] * [**force**]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the matching user context profile.	The value must be the name of an existing user context profile.
domain-name	Specifies the domain name.	The value must be the name of an existing domain on the device.
dot1x	Specifies a default or forcible domain for 802.1X authentication users.	-
mac-authen	Specifies a default or forcible domain for MAC address authentication users.	-
portal	Specifies a default or forcible domain for Portal authentication users.	-
force	Specifies the configured domain as a forcible domain. If this parameter is not specified, the configured domain is a default domain.	-

Views

User authentication event authorization policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some enterprise networks, VLAN is divided into multiple areas with different security levels. The administrator assigns different network access rights to access users in different areas. The device uses the domain to manage users, so the access user's authentication domain can be configured based on the user context profile. Based on different context profiles matching with access VLANs, users in different areas have different authentication domains and are assigned different network access rights.

Prerequisites

- A domain has been configured using the **domain** command in the AAA view.
- A user context profile has been configured using the **access-context profile name** *profile-name* command in the system view.

Precautions

The priorities of the forcible domain, domain carried in the user name, and default domain in different views are as follows in descending order: forcible domain with a specified authentication mode in an authentication profile > forcible domain in an authentication profile > forcible domain with a specified authentication mode based on a user context profile > forcible domain based on a user context profile > domain carried in the user name > default domain with a specified authentication mode in an authentication profile > default domain in an authentication profile > default domain with a specified authentication mode based on a user context profile > default domain based on a user context profile > global default domain.

Example

In the user authentication event authorization policy view, configure the user's forcible domain **test** based on the user context profile **p1**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] access-context profile name p1
[HUAWEI-access-context-p1] quit
[HUAWEI] access-author policy name a1
[HUAWEI-access-author-a1] match access-context-profile p1 action access-domain test force
```

13.5.190 mdns snooping enable

Function

The **mdns snooping enable** command enables the mDNS snooping function.

The **undo mdns snooping enable** command disables the mDNS snooping function.

By default, mDNS snooping is disabled.

Format

mdns snooping enable

undo mdns snooping enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, VLAN view, Eth-Trunk interface view, port group view.

Default Level

2: Configuration level

Usage Guidelines

In terminal type identification scenarios, if the IP address, MAC address, and service name of a terminal need to be identified based on information in the mDNS packets sent by the terminal, run the **mdns snooping enable** command to enable mDNS snooping on the device. After mDNS snooping is enabled, the device obtains the preceding information and reports it to the controller.

This command cannot be configured on Layer 3 interfaces.

Example

Enable mDNS snooping.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mdns snooping enable
```

13.5.191 parameter

Function

The **parameter** command configures the characters used in URL.

The **undo parameter** command restores the default settings.

By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&).

Format

parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

undo parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

Parameters

Parameter	Description	Value
start-mark *parameter-value*	Specifies the start character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
assignment-mark *parameter-value*	Specifies the assignment character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
isolate-mark *parameter-value*	Specifies the delimiter between URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

You can run the **parameter** command to modify the characters in URLs.

By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&). However, the **url (URL template view)** command does not support a URL containing a question mark (?). Therefore, you can replace the question mark (?) in a URL with another character in the **url (URL template view)** command configuration, and then run the **parameter start-mark** *parameter-value* command to specify this replacement character as the start character of URL parameters.

In the following example, the replacement character is a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.11:8080/portal#device-ip=10.1.1.22
[HUAWEI-url-template-test] parameter start-mark #
[HUAWEI-url-template-test] url-parameter user-mac umac user-ipaddress uaddress
```

Processing on the device is as follows:

1. The device automatically replaces the first number sign (#) in the URL with the start character of URL parameters — a question mark (?), and adds a parameter separator "&" at the end of the URL. If the URL does not contain a number sign (#), a question mark (?), instead of an ampersand (&), is added to the end of the URL.
2. The device adds parameters configured by the **url-parameter** command to the end of the URL. The resulting redirect URL is http://10.1.1.11:8080/portal?device-ip=10.1.1.22&umac=00e0-fc02-0002&uaddress=192.168.1.16.

Example

Set the start character for URL parameters to a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] parameter start-mark #
```

13.5.192 pki key-pair-with-cert

Function

The **pki key-pair-with-cert** command configures the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client.

The **undo pki key-pair-with-cert** command deletes the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client.

By default, the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client is not configured.

Format

pki key-pair-with-cert file-format { **pkcs12** | **pem** } **filename** *filename* **password** *password*

undo pki key-pair-with-cert

NOTE

This command is supported only on the S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H.

Parameters

Parameter	Description	Value
file-format pkcs12	Indicates that the format of a certificate file is PKCS12.	-
file-format pem	Indicates that the format of a certificate file is PEM.	-
filename *filename*	Specifies the name of a certificate file.	The value is a string of 1 to 63 characters.
password *password*	Specifies the password of a certificate file.	The password can be in plain text or cipher text. ● A plain text password is a string of 6 to 32 characters. ● A cipher text password is a string of 48 or 68 characters that must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an AP is authenticated as an 802.1X client using TLS, you need to load a certificate file on the AP. You can run this command to configure a certificate file. After the AP goes online, the AC automatically delivers the certificate file to the AP.

Precautions

If the certificate file is modified or deleted, or a certificate file is added after the AP goes online, the AC cannot automatically deliver the certificate file again. In this case, you can run the **load-file (WLAN view)** command to manually deliver the certificate file to the AP.

Example

Configure the certificate file to be loaded on an AP when the AP is authenticated as an 802.1X client. Set the format, name, and password of the certificate file to **PEM**, **serverlocal.pem**, and YsHsjx_202206, respectively.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap_system1
[HUAWEI-wlan-ap-system-prof-ap_system1] pki key-pair-with-cert file-format pem filename
serverlocal.pem password YsHsjx_202206
```

13.5.193 pki-realm

Function

The **pki-realm** command configures the PKI realm used for TLS authentication.

The **undo pki-realm** command deletes the PKI realm used for TLS authentication.

By default, no PKI realm is configured for TLS authentication.

NOTE

Only the following models support this command:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

pki-realm *pki-realm*

undo pki-realm

Parameters

Parameter	Description	Value
pki-realm *pki-realm*	Specifies the PKI realm used for TLS authentication. The name of the PKI realm must be **user-define** or **default**.	The value is a string of 1 to 64 characters. **NOTE** If the specified PKI domain is the default domain, there may be security risks.

Views

802.1X client profile view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as an 802.1X client and uses TLS authentication, you can run this command to configure a PKI realm for loading the digital certificate on the 802.1X client.

This configuration will not be delivered to APs.

Example

Configure a PKI realm used for TLS authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x-client-profile name d1
[HUAWEI-dot1x-client-profile-d1] pki-realm user-define
```

13.5.194 port (Portal server template view)

Function

The **port** command sets the port number that a Portal server uses to receive notification packets from the device.

The **undo port** command restores the default port number.

By default, a Portal server uses port number 50100 to receive packets from the device.

Format

port *port-number* [**all**]

undo port [**all**]

Parameters

Parameter	Description	Value
port-number	Specifies the port number that the Portal server uses to receive and encapsulate UDP packets from the device.	The value is an integer that ranges from 1 to 65535. By default, the value is 50100.

Parameter	Description	Value
all	Indicates that the device always uses the destination port number specified by *port-number* to encapsulate UDP packets. **NOTE** After this keyword is specified, when receiving UDP packets from a Portal server, the device does not obtain the source port number in the UDP packets as the destination port number of UDP packets to be sent to the Portal server. If the value of *port-number* is different from the source port number of the Portal server, the Portal server cannot receive the UDP packets sent by the device. Therefore, this keyword is not recommended.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server** command, configure parameters for the template.

Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device. After receiving a Portal authentication request packet from a user, the device sends the packet to the Portal server using the specified destination port number.

Precautions

Ensure that the port number configured on the device is the same as that used by the Portal server.

Example

Set the port number that a Portal server uses to receive packets from the device to 10000 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] port 10000
```

13.5.195 portal auth-network

Function

The **portal auth-network** command configures the source subnet for Portal authentication.

The **undo portal auth-network** command restores the default setting.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies a Portal authentication subnet.	The value is in dotted decimal notation.
mask-length | *mask-address*	Specifies the mask length or mask of the Portal authentication subnet. - *mask-length*: specifies the mask length. - *mask-address*: specifies the mask.	- The value of *mask-length* is an integer that ranges from 1 to 32. - The value of *mask-address* is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source subnet for Portal authentication is configured, only user packets from the subnet can trigger Portal authentication. If an unauthenticated user is not on a Portal authentication subnet and packets from the user do not match any Portal authentication-free rule, the device discards the user's packets.

Precautions

The command takes effect only for Layer 3 Portal authentication. In Layer 2 Portal authentication, users on all subnets must be authenticated.

Example

In the Portal access profile **p1**, set the source authentication subnet to 10.1.1.0/24.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] portal auth-network 10.1.1.0 24
```

13.5.196 portal captive-adaptive enable

Function

The **portal captive-adaptive enable** command enables the Captive Network Assistant (CNA) adaptive function for iOS terminals.

The **undo portal captive-adaptive enable** command disables the CNA adaptive function for iOS terminals.

By default, the CNA adaptive function is disabled for iOS terminals.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

portal captive-adaptive enable

undo portal captive-adaptive enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

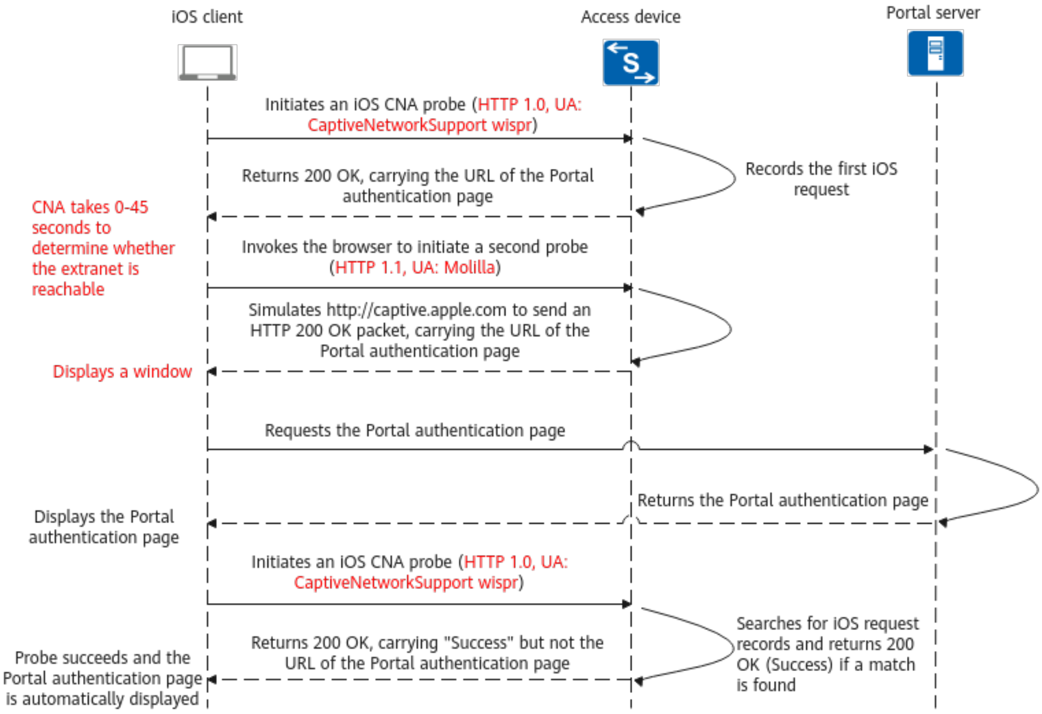
When a user uses an iOS terminal (iPhone, iPad, or iMac) to connect to a WLAN, the CNA of the iOS terminal detects connectivity to http://captive.apple.com. If the network connectivity is normal, the iOS terminal will receive a response indicating success. Otherwise, the iOS terminal invokes the browser to perform a probe again and automatically displays the authentication page. The specific process is as follows:

1. After the terminal associates with an SSID, it sends an HTTP 1.0 request to http://captive.apple.com. The **User-Agent** field in the packet is **CaptiveNetworkSupport wispr**.

2. If the pushed page is not the expected http://www.apple.com/library/test/success.html, the terminal considers a network connection failure and invokes the browser to send an HTTP 1.1 request packet to http://captive.apple.com. The **User-Agent** field in the packet is as follows: **Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_3 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Mobile/13G34**. The field value may slightly vary according to iOS terminals and versions.
3. The Portal authentication page is automatically displayed on the terminal. After the user enters the user name and password, the terminal connects to the WLAN.

The preceding describes the implementation of the CNA mechanism on iOS terminals. Whether the browser can re-send an HTTP request (in step 2) is the key to automatically pushing the Portal authentication page. If the browser is not invoked or is invoked after a long delay, the Portal authentication page will fail to be pushed or will be pushed after a long time. **Figure 13-1** shows the CNA process.

Figure 13-1 CNA process of an iOS terminal



If the CNA probe of an iOS terminal fails, there will be no Wi-Fi symbol on the iOS terminal. You can use either of the following methods to resolve this problem:

- Method 1: Run the **portal captive-bypass enable** command in the system view to enable the device to construct a response carrying **Success** for all requests with the **User-Agent** field being **CaptiveNetworkSupport wispr**. In this way, iOS terminals consider that the network is connected and display the Wi-Fi symbol. The disadvantage of this configuration is that the authentication page cannot be automatically displayed on iOS terminals. Users need to manually open the browser to access a website so that the authentication page can be displayed through redirection.

- Method 2: Run the **portal captive-adaptive enable** command in the system view to enable the device to perform a probe and redirection for the first request with the **User-Agent** field being **CaptiveNetworkSupport wispr** and return a Success (200 OK) message for subsequent requests with the **User-Agent** field being **CaptiveNetworkSupport wispr**. In this way, iOS terminals can automatically display the authentication page and show the Wi-Fi symbol.

Precautions

When applications on iOS mobile terminals are used to perform Portal authentication, you can run only the **portal captive-bypass enable** command to enable the CNA bypass function. After this function is enabled, users who have logged in to the applications can be automatically authenticated and connect to networks, without entering their user names and passwords.

If you run both the **portal captive-adaptive enable** and **portal captive-bypass enable** commands, the command executed later takes effect.

Due to restrictions of iOS 9.3.1, mobile terminals using iOS 9.3.1 cannot connect to WLANs after the CNA adaptive function is enabled. To solve this problem, run the **portal captive-bypass enable** command to enable the CNA bypass function. Terminal users then can be redirected to the application-based Portal authentication page after they open the browser and access a web page.

Authentication-free resources accessed by users cannot contain the URL captive.apple.com; otherwise, terminals cannot automatically display the Portal authentication page.

If the Portal authentication page is of the HTTPS type, terminals can automatically display the Portal authentication page only when an HTTPS URL is used and the domain name certificate is valid.

Example

Enable the CNA adaptive function for iOS terminals.

```
<HUAWEI> system-view
[HUAWEI] portal captive-adaptive enable
```

13.5.197 portal captive-bypass enable

Function

The **portal captive-bypass enable** command enables the CNA bypass function for iOS terminals.

The **undo portal captive-bypass enable** command disables the CNA bypass function.

By default, the CNA bypass function is disabled for iOS terminals.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

portal captive-bypass enable

undo portal captive-bypass enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The iOS operating system provides the Captive Network Assistant (CNA) function. With the CNA function, the iOS terminals (including iPhone, iPad, and iMAC) automatically detects wireless network connectivity after associating with a wireless network. If the network connection cannot be set up, the iOS terminals ask users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the wireless network.

However, Portal authentication allows users to access certain resources before authentication is successful. If the iOS terminals are disconnected, users cannot access the specified resources. The CNA bypass function addresses this problem. If the users do not enter user names and passwords immediately, the CNA bypass function keeps the iOS terminals online before the Portal authentication is successful. Therefore, the iOS users are allowed to access authentication-free resources.

Precautions

After the CNA bypass function is enabled for iOS terminals, the Portal authentication page will not be automatically displayed for iOS terminals.

Example

Enable the CNA bypass function for iOS terminals.

```
<HUAWEI> system-view
[HUAWEI] portal captive-bypass enable
```

13.5.198 portal https-redirect blacklist

Function

The **portal https-redirect blacklist** command adds an address to the HTTPS redirection blacklist. After an address is added to the HTTPS redirection blacklist, HTTPS redirection is not performed for HTTPS access to this address of Portal users.

The **undo portal https-redirect blacklist** command removes an address from the HTTPS redirection blacklist.

By default, no address is added to the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist ip *start-ip-address* [*end-ip-address*]

portal https-redirect blacklist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect blacklist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect blacklist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: ● *start-ip-address* specifies the start IPv4 address. ● *end-ip-address* specifies the end IPv4 address.	-
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: ● *start-ipv6-address* specifies the start IPv6 address. ● *end-ipv6-address* specifies the end IPv6 address.	-
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection blacklist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. To disable HTTPS redirection for HTTPS access to a specified address, run the **portal https-redirect blacklist** command to add this address to the HTTPS redirection blacklist.

Precautions

If an address has been added to the HTTPS redirection whitelist using the **portal https-redirect whitelist** command, this address cannot be added to the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.1.1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ip 10.1.1.1
```

Add FC00::1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ipv6 FC00::1
```

13.5.199 portal https-redirect blacklist aging-time

Function

The **portal https-redirect blacklist aging-time** command configures the aging time of addresses in the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist aging-time** command restores the default aging time of addresses in the HTTPS redirection blacklist.

By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds, that is, 72 hours.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist aging-time *aging-time*

undo portal https-redirect blacklist aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of addresses in the HTTPS redirection blacklist.	The value is an integer in the range from 30 to 4294967295, in seconds. The default value is 259200 seconds, that is, 72 hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an address (except the address of the Portal server) is added to the HTTPS redirection blacklist, HTTPS access from Portal users to this address does not trigger HTTPS redirection. By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds. When the aging time expires, this address will be removed from the blacklist. You can use the **portal https-redirect blacklist aging-time** command to adjust the aging time of addresses in the HTTPS redirection blacklist.

Example

Configure the aging time of addresses in the HTTPS redirection blacklist to 86400 seconds, that is, 24 hours.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist aging-time 86400
```

13.5.200 portal https-redirect blacklist packet-rate

Function

The **portal https-redirect blacklist packet-rate** command configures the maximum rate at which a Portal user accesses an address through HTTPS. If the user access rate reaches the maximum, the switch adds the destination address to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist packet-rate** command restores the default maximum rate at which a Portal user accesses an address through HTTPS.

By default, the maximum rate at which a Portal user accesses an address through HTTPS is 40 times per minute.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist packet-rate *packet-rate*

undo portal https-redirect blacklist packet-rate

Parameters

Parameter	Description	Value
packet-rate	Specifies the maximum rate at which a Portal user accesses an address through HTTPS.	The value is an integer in the range from 5 to 600, in times per minutes. The default value is 40.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the rate of packets sent from a Portal user for accessing an address through HTTPS reaches the maximum rate specified by the **portal https-redirect blacklist packet-rate** command, the switch adds the destination address to the HTTPS redirection blacklist. This prevents repeated HTTPS redirection caused by frequent access from malicious users to an address, and therefore saves resources of the switch.

Prerequisites

The function of inserting a JavaScript file during Portal redirection has been enabled using the **portal redirect js enable** command.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum rate at which a Portal user accesses an address through HTTPS to 30 times per minute.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist packet-rate 30
```

13.5.201 portal https-redirect blacklist retry-times interval

Function

The **portal https-redirect blacklist retry-times interval** command configures the maximum number of times and the detection period. Within the detection period, if the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum, the address is added to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist retry-times interval** command restores the default maximum number of times and the default detection period.

By default, the maximum number of times is 10 and the detection period is 3 minutes.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist retry-times *retry-times* **interval** *interval*

undo portal https-redirect blacklist retry-times interval

Parameters

Parameter	Description	Value
retry-times	Specifies the maximum number of times.	The value is an integer in the range from 1 to 600. The default value is 10.
interval	Specifies the detection period.	The value is an integer in the range from 1 to 600, in minutes. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the function of inserting a JavaScript file during Portal redirection is enabled on the switch using the **portal redirect js enable** command, the HTTP or HTTPS response packets sent from the switch to clients carry the JavaScript file.

- The clients can be redirected to the Portal login page only after they correctly parse the JavaScript file.
- If a client fails to parse the JavaScript file, the switch adds the destination address to the provisional HTTPS redirection blacklist. HTTP and HTTPS redirection can still be triggered for addresses in the provisional HTTPS redirection blacklist.

The detection period specified in the **portal https-redirect blacklist retry-times interval** command starts from the time when an address is added to the provisional HTTPS redirection blacklist. If the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum within the detection period, this address is added to the HTTPS redirection blacklist.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum number of times to 15 and the detection period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist retry-times 15 interval 5
```

13.5.202 portal https-redirect tls1.1 enable

Function

The **portal https-redirect tls1.1 enable** command configures TLS 1.1 for HTTPS redirection in Portal authentication.

The **undo portal https-redirect tls1.1 enable** command cancels the configuration.

By default, TLS 1.2 is used for HTTPS redirection in Portal authentication.

NOTE

Only the following switch models support this command:

S200, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect tls1.1 enable

undo portal https-redirect tls1.1 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to configure whether the TLS 1.1 protocol is used for HTTPS redirection in Portal authentication.

Precautions

In versions earlier than V200R021C00, the TLS 1.1 protocol is used for HTTPS redirection in Portal authentication by default; however, the TLS 1.2 protocol is used by default in V200R021C00 and later versions. If the device is upgraded from an earlier version to V200R021C00 or later, the **portal https-redirect tls1.1 enable** command is automatically generated in the system configuration file to ensure compatibility.

In V200R021C00, this command takes effect only for wired users. In V200R021C10 and later versions, this command takes effect for both wired and wireless users.

TLS 1.2 is recommended because it is more secure than TLS 1.1.

Example

Configure TLS 1.1 for HTTPS redirection in Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect tls1.1 enable
```

13.5.203 portal https-redirect whitelist

Function

The **portal https-redirect whitelist** command adds an address to the HTTPS redirection whitelist.

The **undo portal https-redirect whitelist** command removes an address from the HTTPS redirection whitelist.

By default, no address is added to the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect whitelist ip *start-ip-address* [*end-ip-address*]

portal https-redirect whitelist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect whitelist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect whitelist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: ● *start-ip-address* specifies the start IPv4 address. ● *end-ip-address* specifies the end IPv4 address.	-
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: ● *start-ipv6-address* specifies the start IPv6 address. ● *end-ipv6-address* specifies the end IPv6 address.	-

Parameter	Description	Value
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection whitelist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. If an address is added to the HTTPS redirection blacklist by mistake, HTTPS access to this address will not trigger HTTPS redirection. To ensure that HTTPS redirection is performed for HTTPS access to specified addresses, use the **portal https-redirect whitelist** command to add these addresses to the HTTPS redirection whitelist.

Configuration Impact

If an address has been added to the HTTPS redirection whitelist, this address cannot be added to the HTTPS redirection blacklist using the **portal https-redirect blacklist** command.

Precautions

If an address in the HTTPS redirection blacklist is added to the HTTPS redirection whitelist, the switch removes the address from the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.2.1 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ip 10.1.2.1
```

Add FC00::2 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ipv6 FC00::2
```

13.5.204 portal https-redirect wired enable

Function

The **portal https-redirect wired enable** command enables HTTPS redirection for wired Portal authentication users.

The **undo portal https-redirect wired enable** command disables HTTPS redirection for wired Portal authentication users.

By default, HTTPS redirection is disabled for wired Portal authentication users.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect wired enable

undo portal https-redirect wired enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After HTTPS redirection is disabled for wired Portal authentication users, Portal authentication cannot be triggered when a wired Portal authentication user uses HTTPS to access a website. As a result, the user cannot go online. To allow Portal authentication be triggered when a wired Portal authentication user uses HTTPS to access a website, run the **portal https-redirect wired enable** command to enable HTTPS redirection for wired Portal authentication users.

Prerequisites

HTTPS redirection of Portal authentication has been enabled using the **authentication https-redirect enable** command.

Configuration Impact

If a non-Huawei AC and non-Huawei APs are connected to the switch, APs and users are associated with the AC, and the switch performs Portal authentication for access users, users will go online at a slow rate after HTTPS redirection is enabled for wired Portal authentication users. Therefore, it is recommended that you disable HTTPS redirection for wired Portal authentication users in this scenario.

Precautions

After HTTPS redirection is disabled for wired Portal authentication users, Portal authentication can still be triggered when a wired Portal authentication user uses HTTP to access a website.

This function takes effect only for new wired Portal authentication users.

Example

Enable HTTPS redirection for wired Portal authentication users.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect wired enable
```

13.5.205 portal logout different-server enable

Function

The **portal logout different-server enable** command configures a device to process user logout requests sent by a Portal server other than the one from which users log in.

The **undo portal logout different-server enable** command restores the default configuration.

By default, a device does not process user logout requests sent by Portal servers other than the one from which users log in.

Format

portal logout different-server enable

undo portal logout different-server enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where Portal server load balancing is configured, by default, a device does not process user logout requests sent by Portal servers other than the one from which users log in and responds ACK messages only to the Portal server from which users log in. Users in arrears then can still stay online. To prevent this problem, run **portal logout different-server enable** command to configure the device to process user logout requests sent by a Portal server other than the one from which users log in. Upon receipt of a user logout request from such a Portal server, the device starts a user logout process. After completing the logout event, the device responds an ACK message to the Portal server, thereby ensuring that the user logs out properly.

Precautions

The user logout requests that a device can process must be sent by Portal servers bound to an access interface. These servers include all the Portal servers configured in the master and backup Portal server templates bound to the interface.

Example

Enable a device to process user logout requests a Portal server other than the one from which users log in.

```
<HUAWEI> system-view
[HUAWEI] portal logout different-server enable
```

13.5.206 portal logout resend timeout

Function

The **portal logout resend timeout** command configures the re-transmission times and interval for the Portal authentication user logout packet.

The **undo portal logout resend timeout** command restores the default setting.

By default, the Portal authentication user logout packet can be re-transmitted three times within five seconds.

Format

portal logout resend *times* **timeout** *period*

undo portal logout { **resend** | **timeout** } *

Parameters

Parameter	Description	Value
times	Specifies the number of re-transmission times for the Portal authentication user logout packet.	The value is an integer that ranges from 0 to 15. The value 0 indicates that the re-transmission function is disabled.
period	Specifies the re-transmission interval of the Portal authentication user logout packet.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After disconnecting a Portal authentication user, the device sends a user logout packet (NTF-LOGOUT) to instruct the Portal server to delete the user information. If the network between the device and Portal server is not stable or packets are lost, the Portal server may fail to receive the user logout packet from the device after the Portal authentication user is disconnected. In this case, the user is displayed as disconnected on the device but still as online on the Portal server. To enable the Portal server to receive the user logout packet and ensure that the online user information on the Portal server is correct, the administrator can enable the user logout packet re-transmission function on the device and configure the re-transmission times and interval.

Example

Configure the re-transmission times to 5 and interval to 10 seconds for the Portal authentication user logout packet.

```
<HUAWEI> system-view
[HUAWEI] portal logout resend 5 timeout 10
```

13.5.207 portal max-user

Function

The **portal max-user** command sets the maximum number of concurrent Portal authentication users allowed to access the device.

The **undo portal max-user** command restores the default maximum number of concurrent Portal authentication users.

By default, the number of Portal authentication users is the maximum number of Portal authentication users supported by the device.

Format

portal max-user *user-number*

undo portal max-user

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of concurrent Portal users.	The value is an integer that varies depending on product models.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **portal max-user** command to set the maximum number of concurrent Portal authentication users.

Example

Set the maximum number of concurrent Portal authentication users to 25.

```
<HUAWEI> system-view
[HUAWEI] portal max-user 25
```

13.5.208 portal pass dns enable

Function

The **portal pass dns enable** command enables a device to allow DNS packets to pass through during Portal authentication.

The **undo portal pass dns enable** command restores the default configuration.

By default, a device does not allow DNS packets to pass through during Portal authentication.

Format

portal pass dns enable

undo portal pass dns enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you use a domain name to access the network, run the **portal pass dns enable** command to allow DNS packets destined for the DNS server to pass through. However, after this command is executed, all DNS packets are permitted.

You are recommended to run the **free-rule** command to configure the IP address of the DNS server as the source accessible to users without authentication.

Example

Enable a device to allow DNS packets to pass through during Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal pass dns enable
```

13.5.209 portal quiet-period

Function

The **portal quiet-period** command enables the quiet timer for Portal authentication.

The **undo portal quiet-period** command disables the quiet timer of Portal authentication.

By default, the quiet timer for Portal authentication is enabled.

Format

portal quiet-period

undo portal quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer for Portal authentication. If the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. During the quiet period, the device discards Portal authentication requests from the user. This prevents the impact of frequent authentications on the system.

The quiet period for Portal authentication can be set using the **portal timer quiet-period** command. After the quiet period is reached, the device re-authenticates the user.

Example

Enable the quiet timer for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-period
```

13.5.210 portal quiet-times

Function

The **portal quiet-times** command sets the maximum number of authentication failures within 60s before a Portal authentication user is kept in quiet state.

The **undo portal quiet-times** command restores the default maximum number of authentication failures within 60s before a Portal authentication user enters the quiet state.

By default, the device allows a maximum of ten authentication failures within 60s before a Portal authentication user enters the quiet state.

Format

portal quiet-times *fail-times*

undo portal quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a Portal authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer, if the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. This prevents the impact of frequent authentications on the system.

Example

Set the maximum number of Portal authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-times 4
```

13.5.211 portal redirect-302 enable

Function

The **portal redirect-302 enable** command enables redirection based on the status code 302 for Portal authentication.

The **undo portal redirect-302 enable** command disables redirection based on the status code 302 for Portal authentication.

By default, redirection based on the status code 302 is disabled for Portal authentication.

Format

portal redirect-302 enable

undo portal redirect-302 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HTTP status codes 200 and 302 correspond to different redirection modes. During redirection based on the status code 200 OK, the URL information is in the **URL** field of an HTTP packet. During redirection based on the status code 302, the URL information is in the **Location** field of an HTTP packet. By default, the device performs redirection based on the status code 200 OK. Some applications need to use redirection based on the status code 302. In this case, you can run this command to enable this function.

Precautions

After redirection based on the status code 302 is configured for Portal authentication, the **portal redirect js enable** configuration is invalidated.

Example

Enable redirection based on the status code 302 for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal redirect-302 enable
```

13.5.212 portal redirect js enable

Function

The **portal redirect js enable** command enables the function of inserting a JavaScript file during Portal redirection.

The **undo portal redirect js enable** command disables the function of inserting a JavaScript file during Portal redirection.

By default, the function of inserting a JavaScript file during Portal redirection is disabled.

Format

portal redirect js enable

undo portal redirect js enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the device redirects the HTTP or HTTPS requests sent from clients to the Portal server. To prevent heavy burdens on the server caused by a large number of HTTP or HTTPS requests sent from the clients and to ensure proper display of the Portal login page, enable the function of inserting a JavaScript file during Portal redirection. After this function is enabled, the HTTP or HTTPS response packets sent from the server carry a JavaScript file. The client browser parses the JavaScript file for redirection, and then performs Portal authentication.

Precautions

The client browser must support and enable the JavaScript function.

Example

Enable the function of inserting a JavaScript file during Portal direction.

```
<HUAWEI> system-view
[HUAWEI] portal redirect js enable
```

13.5.213 portal redirect-http-port

Function

The **portal redirect-http-port** command configures a user-defined destination port number of HTTP packets that trigger Portal redirection.

The **undo portal redirect-http-port** command deletes a user-defined destination port number of HTTP packets that trigger Portal redirection.

By default, the device redirects users to the Portal authentication page only when their browsers send HTTP packets with the destination port number 80.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720-LI, and S5720S-LI support this command.

Format

portal redirect-http-port *port-number* &<1-10>

undo portal redirect-http-port [*port-number* &<1-10>]

Parameters

Parameter	Description	Value
port-number	Specifies a user-defined destination port number of HTTP packets that trigger Portal redirection.	The value is an integer that ranges from 1024 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device redirects users to the Portal authentication page only when their browsers send HTTP packets with the destination port number 80. If a user's browser has a web proxy server configured and the destination port number of HTTP packets is modified, the device discards HTTP packets from the user and does not redirect the user to the Portal authentication page. You can run the **portal redirect-http-port** command to configure a user-defined destination port number of HTTP packets that trigger Portal redirection. The device then redirects users to the Portal authentication page after receiving HTTP packets with the destination port number 80 or a user-defined destination port number.

Precautions

If a user's browser has a web proxy server configured, configure the Portal server address (configured on the device using the **server-ip** command) as an exception address on the user's browser, to prevent HTTP packets to the Portal server from being sent to the web proxy server.

If the specified destination port number is 65535, some browsers consider this port as an insecure port, resulting a redirection failure.

This command applies only when Portal authentication is performed on VLANIF interfaces and does not take effect in other scenarios.

Example

Set the user-defined destination port number to 8080 for HTTP packets that trigger Portal redirection.

```
<HUAWEI> system-view
[HUAWEI] portal redirect-http-port 8080
```

13.5.214 portal timer quiet-period

Function

The **portal timer quiet-period** command configures the quiet period for Portal authentication users who fail to be authenticated.

The **undo portal timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for Portal authentication users who fail to be authenticated.

Format

portal timer quiet-period *quiet-period-value*

undo portal timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Sets the quiet period for Portal authentication users who fail to be authenticated.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a Portal authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled using the **portal quiet-period** command, if the number of times that a Portal authentication user fails to be authenticated within 60s exceeds the upper limit (configured using the **portal quiet-times** command), the device discards the user's Portal authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for Portal authentication users who fail to be authenticated.

```
<HUAWEI> system-view
[HUAWEI] portal timer quiet-period 100
```

13.5.215 portal timer offline-detect

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a Portal user goes offline due to power failure or network interruption, the device and Portal server may still store the user information, which causes incorrect accounting. Additionally, a limit number of users can access the device. If a user goes offline improperly but the device still stores user information, other users cannot access the network.

After the Portal user offline detection interval is set, if the user does not respond within the interval, the device considers the Portal user offline. The device and Portal server then delete the user information and release resources to ensure an efficient resource use.

Precautions

This command only applies to Layer 2 Portal authentication. When the configuration is changed, the new configuration takes effect only for new access users.

The heartbeat detection function of the authentication server can be used to ensure the normal online status of PC users for whom Layer 3 Portal authentication is used. If the authentication server detects that a user goes offline, it instructs the device to disconnect the user.

If the number of offline detection packets (ARP packets) exceeds the default CAR value, the detection fails and the users are logged out (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.). To resolve the problem, the following methods are recommended:

- Increase the detection interval based on the number of users. The default detection interval is recommended when there are less than 8000 users; the detection interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

If user traffic (such as service packets) passes through the device within the Portal user offline detection period, the device does not consider the user offline even if the user does not respond to user offline detection packets.

Example

In the Portal access profile **p1**, set the offline detection interval of Portal authentication users to 400s.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] portal timer offline-detect 400
```

13.5.216 portal url-encode enable

Function

The **portal url-encode enable** command enables URL encoding and decoding.

The **undo portal url-encode enable** command disables URL encoding and decoding.

By default, URL encoding and decoding are enabled.

Format

portal url-encode enable

undo portal url-encode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. To enable URL encoding and decoding, run the **portal url-encode enable** command. Some special characters in redirect URLs are then converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented.

Precautions

After the URL encoding and decoding function is enabled, some servers may not support the escape characters converted from special characters in redirect URLs. Therefore, check whether servers support the escape characters before configuring special characters in redirect URLs.

Example

Enable URL encoding and decoding.

```
<HUAWEI> system-view
[HUAWEI] portal url-encode enable
```

13.5.217 portal user-alarm percentage

Function

The **portal user-alarm percentage** command sets alarm thresholds for the Portal authentication user count percentage.

The **undo portal user-alarm percentage** command restores the default alarm thresholds for the Portal authentication user count percentage.

By default, the lower alarm threshold for the Portal authentication user count percentage is 50, and the upper alarm threshold for the Portal authentication user count percentage is 100.

Format

portal user-alarm percentage *percent-lower-value percent-upper-value*

undo portal user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **portal max-user** command to set the maximum number of online Portal authentication users allowed on a device, you can run the **portal user-alarm percentage** command to set alarm thresholds for the Portal authentication user count percentage.

When the percentage of online Portal authentication users against the maximum number of users allowed by the device exceeds the upper alarm threshold, the device generates an alarm. When the percentage of online Portal authentication users against the maximum number of users allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

If the configured upper alarm threshold for the Portal authentication user count percentage is 100, the device generates an alarm when the number of online users reaches the maximum number of users allowed by the device.

Example

Set the lower alarm threshold for the Portal authentication user count percentage to 30, and the upper alarm threshold for the Portal authentication user count percentage to 80.

```
<HUAWEI> system-view
[HUAWEI] portal user-alarm percentage 30 80
```

13.5.218 portal web-authen-server

Function

The **portal web-authen-server** command enables Portal interconnection using the HTTP or HTTPS protocol.

The **undo portal web-authen-server** command disables Portal interconnection using the HTTP or HTTPS protocol.

By default, Portal interconnection using the HTTP or HTTPS protocol is disabled.

Format

portal web-authen-server { **http** | **https ssl-policy** *policy-name* } [**port** *port-number*]

undo portal web-authen-server [**port**]

Parameters

Parameter	Description	Value
http	Configures the HTTP protocol for Portal authentication. **NOTE** The HTTP protocol poses security risks. The HTTPS protocol is recommended.	-
https	Configures the HTTPS protocol for Portal authentication.	-
ssl-policy *policy-name*	Specifies the name of an SSL policy.	The value must be the name of an existing SSL policy.
port *port-number*	Specifies a port number.	The value is an integer that ranges from 1025 to 65535. The default HTTP port number is 8000, and the default HTTPS port number is 8443.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to the Portal server that supports only the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable Portal interconnection using the HTTP or HTTPS protocol.

Follow-up Procedure

Run the **protocol** command to set the protocol used in Portal authentication to HTTP or HTTPS.

Precautions

- Modifying the **port** parameter will cause users in pre-connection state to go offline.
- In V200R020C10SPC100 and later versions, you must also run the **portal web-authen-server server-source** command to configure the local gateway address used by the device to receive and respond to the packets sent by the user terminals. Otherwise, the Portal interconnection function cannot be used.

Example

Enable Portal interconnection using the HTTPS protocol.

```
<HUAWEI> system-view
[HUAWEI] ssl policy test
[HUAWEI-ssl-policy-test] quit
[HUAWEI] portal web-authen-server https ssl-policy test port 8443
```

13.5.219 portal web-authen-server server-source

Function

The **portal web-authen-server server-source** command configures the local gateway address used by the device to receive and respond to the packets sent by the user terminals when the Portal interconnection function of the HTTP or HTTPS protocol is enabled.

The **undo portal web-authen-server server-source** command restores the default configuration.

By default, the device does not receive or respond to all packets sent by the user terminals when the Portal interconnection function of the HTTP or HTTPS protocol is enabled.

Format

portal web-authen-server server-source { **all-interface** | **ip-address** *ip-address* }

undo portal web-authen-server server-source { **all-interface** | **ip-address** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.
all-interface	Indicates that the IPv4 address is set to 0.0.0.0. That is, the device can receive and respond to all packets sent by the user terminals.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to a Portal server that supports only the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable the Portal interconnection function of the HTTP or HTTPS protocol. In V200R020C10SPC100 and later versions, you must also run the **portal web-authen-server server-source** command to configure the local gateway address used by the device to receive and respond to the packets sent by the user terminals. Otherwise, the Portal interconnection function cannot be used.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and the Portal interconnection function of the HTTP or HTTPS protocol is enabled, the device delivers the **portal web-authen-server server-source all-interface** command by default to receive and respond to all packets sent by the user terminals.
- After the **portal web-authen-server server-source all-interface** command is configured, the device receives and responds to all packets sent by the user terminals, which increases system security risks. Therefore, you are not advised to configure this command.
- After the **portal web-authen-server server-source all-interface** command is run, the system clears all configurations of the **portal web-authen-server server-source ip-address** *ip-address* command.
- If the **portal web-authen-server server-source all-interface** command has been configured on the device, the **portal web-authen-server server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

Configure 10.1.1.1 as the local gateway address used by the device to receive and respond to the packets sent by the user terminals when the Portal interconnection function is enabled.

```
<HUAWEI> system-view
[HUAWEI] portal web-authen-server server-source ip-address 10.1.1.1
```

13.5.220 portal-access-profile (authentication profile view)

Function

The **portal-access-profile** command binds a Portal access profile to an authentication profile.

The **undo portal-access-profile** command unbinds a Portal access profile from an authentication profile.

By default, an authentication profile is not bound to a Portal access profile.

Format

portal-access-profile *access-profile-name*

undo portal-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of a Portal access profile.	The value must be the name of an existing Portal access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to a Portal access profile, the authentication profile is enabled with Portal authentication. After the authentication profile is applied to the interface or VAP profile, Portal authentication can be performed on online users.

Prerequisites

The Portal server template used by the Portal access profile has been configured using the **web-auth-server** command.

Follow-up Procedure

Run the **authentication-profile** (Interface view or VAP profile view) command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one Portal access profile.

If an authentication event authorization VLAN and MAC address, 802.1X, and Portal hybrid authentication are configured in an authentication profile, Portal authentication fails.

If both authentication event authorization VLAN and Portal authentication are configured in an authentication profile, the authentication event authorization VLAN does not take effect.

Example

Bind the authentication profile **portal_authen_profile1** to the Portal access profile **portal_access_profile1**. The IP address of the Portal server is 192.168.10.1, and Layer 2 Portal authentication is used.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server1
[HUAWEI-web-auth-server-server1] server-ip 192.168.10.1
[HUAWEI-web-auth-server-server1] quit
[HUAWEI] portal-access-profile name portal_access_profile1
[HUAWEI-portal-acces-profile-portal_access_profile1] web-auth-server server1 direct
[HUAWEI-portal-acces-profile-portal_access_profile1] quit
[HUAWEI] authentication-profile name portal_authen_profile1
[HUAWEI-authen-profile-portal_authen_profile1] portal-access-profile portal_access_profile1
```

13.5.221 portal-access-profile (system view)

Function

The **portal-access-profile** command creates a Portal access profile and displays the Portal access profile view.

The **undo portal-access-profile** command deletes the Portal access profile.

By default, the device has a built-in Portal access profile named **portal_access_profile**.

Format

portal-access-profile name *access-profile-name*

undo portal-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of a Portal access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses Portal access profiles to uniformly manage all Portal users access configurations. To perform Portal authentication for the users in an interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to a Portal access profile.

Follow-up Procedure

Run the **web-auth-server** command to configure the Portal server template for the Portal access profile.

Precautions

- The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in Portal access profile **portal_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a Portal access profile, ensure that this profile is not bound to any authentication profile.

Example

Create Portal access profile named **portal_access_profile1**.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name portal_access_profile1
```

13.5.222 protocol (Portal server template view)

Function

The **protocol** command configures the protocol used in Portal authentication.

The **undo protocol** command restores the default configuration.

By default, the Portal protocol is used in Portal authentication.

Format

protocol { **http** [**password-encrypt** { **none** | **uam** }] | **portal** | **haca** }

undo protocol

Parameters

Parameter	Description	Value
http	Sets the protocol used in Portal authentication to HTTP or HTTPS.	-
password-encrypt { **none** | **uam** }	Specifies the password encoding mode. Select a mode based on the Portal server configuration. - **none**: The password is not encoded. - **uam**: The password is encoded using ASCII characters. When **http** is specified, the default password encoding mode is **none**.	-
portal	Sets the protocol used in Portal authentication to Portal.	-
haca	Sets the protocol used in Portal authentication to HACA.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

In Portal authentication, the device can use the following protocols to communicate with the Portal server. You can set the protocol according to the protocol supported by the Portal server.

- HACA protocol
- Portal protocol
- HTTP or HTTPS protocol

Central cloud APs do not support HTTP or HTTPS for Portal authentication.

Example

According to the Portal server configuration, set the protocol used in Portal authentication to HTTP or HTTPS and set the password encryption mode to **uam** on the device.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] protocol http password-encrypt uam
```

13.5.223 qos-profile (service scheme view)

Function

The **qos-profile** command binds a QoS profile to a service scheme.

The **undo qos-profile** command unbinds the QoS profile from the service scheme.

By default, no QoS profile is bound to a service scheme.

NOTE

Only S5731-H,S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

qos-profile *profile-name*

undo qos-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the QoS profile bound to the service scheme.	The value must be the name of an existing QoS profile.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme (AAA view)** command, you can run the **qos-profile** command to bind a QoS profile to the service scheme. The user assigned with the service scheme will have the attributes in the QoS profile.

Precautions

For S6720-EI, S6720S-EI, if the user upstream rate limit is configured in the QoS profile bound to a service scheme, do not configure the device to use the service scheme to grant network access rights to users in the pre-connection phase. Otherwise, users go offline.

If the server delivers both the downlink bandwidth limit (equivalent to the RADIUS attribute HW-Output-Committed-Information-Rate) and the RADIUS attribute HW-Subscriber-QoS-Profile for user authorization, only the RADIUS attribute HW-Subscriber-QoS-Profile takes effect.

If the server delivers both the uplink or downlink bandwidth limit (equivalent to the RADIUS attribute HW-Input-Committed-Information-Rate or HW-Output-Committed-Information-Rate) and the RADIUS attribute HW-Qos-Data for user authorization, only the uplink or downlink bandwidth limit take effect.

Example

Bind the QoS profile **abc** to the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name abc
[HUAWEI-qos-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] qos-profile abc
```

13.5.224 reset aaa statistics access-type-authenreq

Function

The **reset aaa statistics access-type-authenreq** command clears the number of requesting for MAC, Portal, or 802.1X authentication.

Format

reset aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, and 802.1X authentications.

To clear the number of requesting for MAC, Portal, or 802.1X authentication, run the **reset aaa statistics access-type-authenreq** command.

Example

Clear the number of requesting for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> reset aaa statistics access-type-authenreq
```

13.5.225 reset access-user dot1x-identity statistics

Function

The **reset access-user dot1x-identity statistics** command clears statistics about Identity packets for 802.1X authentication on a switch.

Format

reset access-user dot1x-identity statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To display statistics about Identity packets for 802.1X authentication on a switch within a specified period of time, run the **reset access-user dot1x-identity**

statistics command to clear the existing statistics first, and then run the **display access-user dot1x-identity statistics** command to display the new statistics.

Example

Clear statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> system-view
[HUAWEI] reset access-user dot1x-identity statistics
```

13.5.226 reset access-user https statistics

Function

The **reset access-user https statistics** command clears statistics about HTTPS protocol packets sent to the CPU.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

reset access-user https statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before checking statistics about HTTPS protocol packets sent to the CPU within a specified period, you must run the **reset access-user https statistics** command to clear the existing statistics. After new statistics are collected, run the **display access-user https statistics** command to check the new statistics.

Example

Clear statistics about HTTPS protocol packets sent to the CPU.

```
<HUAWEI> system-view
[HUAWEI] reset access-user https statistics
```

13.5.227 reset access-user portal statistics

Function

The **reset access-user portal statistics** command clears statistics about Portal protocol packets sent to the CPU.

Format

reset access-user portal statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before checking statistics about Portal protocol packets sent to the CPU within a specified period, you must run the **reset access-user portal statistics** command to clear the existing statistics. After new statistics are collected, run the **display access-user portal statistics** command to check the new statistics.

Example

Clear statistics about Portal protocol packets sent to the CPU.

```
<HUAWEI> system-view
[HUAWEI] reset access-user portal statistics
```

13.5.228 reset access-user traffic-statistics

Function

The **reset access-user traffic-statistics** command clears statistics on traffic of users.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

reset access-user traffic-statistics { **user-id** *begin-id* [*end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance*] }

Parameters

Parameter	Description	Value
user-id *begin-id* [*end-id*]	Specifies IDs of online users. ● *begin-id*: indicates the ID of the start user. ● *end-id*: indicates the ID of the end user. The value of *end-id* must be equal to or greater than that of *begin-id*.	The value is an integer that varies depending on the product model.
mac-address *mac-address*	Specifies the MAC address of an online user.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
ip-address *ip-address*	Specifies the IP address of an online user.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the name of a VPN instance that an online user belongs to.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

After traffic policing is configured in a service scheme, the device collects traffic statistics for the users assigned with the service scheme. You can run the **reset access-user traffic-statistics** command to clear traffic statistics of online users.

Example

Clear statistics on traffic of the user with the IP address 10.1.1.1.

```
<HUAWEI> reset access-user traffic-statistics ip-address 10.1.1.1
```

13.5.229 reset dot1x statistics

Function

The **reset dot1x statistics** command clears 802.1X authentication statistics.

Format

reset dot1x statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears 802.1X authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, 802.1X authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The 802.1X authentication statistics contain the number of times that the authentication succeeded and failed and the number of sent and received packets.

The **reset dot1x statistics** command is used in the following scenarios:

- Redeploy services. After the statistics are cleared, collect the 802.1X authentication statistics again, and run the **display dot1x** command to check whether the authentication function works properly and whether packets are correctly sent and received.
- Rectify a fault. After the fault is rectified, run the **reset dot1x statistics** command to clear the statistics, collect the statistics on 802.1X authentication again, and then run the **display dot1x** command to verify the authentication result and check whether packets are correctly sent and received. If the authentication is successful and packets are correctly sent and received, the fault is rectified.

Example

Clear 802.1X authentication statistics.

```
<HUAWEI> reset dot1x statistics
```

13.5.230 reset dot1x-client statistics

Function

The **reset dot1x-client statistics** command clears packet statistics about 802.1X clients.

NOTE

Only the following switch models support this function:

S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

reset dot1x-client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears packet statistics about the 802.1X client on a specified interface. If this parameter is not specified, packet statistics about 802.1X clients on all interfaces are cleared.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to clear packet statistics about 802.1X clients, and then run the **display dot1x-client statistics** command to view the new statistics.

Example

Clear packet statistics about 802.1X clients.

```
<HUAWEI> reset dot1x-client statistics
```

13.5.231 reset mac-authen statistics

Function

The **reset mac-authen statistics** command clears MAC address authentication statistics.

Format

reset mac-authen statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears MAC address authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, MAC address authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset mac-authen statistics** command is used in the following scenarios:

- Re-deploy services. After the statistics are cleared, collect the MAC address authentication statistics again, and run the **display mac-authen** command to check whether the authentication function is normal.
- Rectify a fault. After the fault is rectified, run the **reset mac-authen statistics** command to clear statistics, collect MAC address authentication statistics

again, and run the **display mac-authen** command to check the authentication result. If the authentication is successful, the fault is rectified.

Example

Clear MAC address authentication statistics.

```
<HUAWEI> reset mac-authen statistics
```

13.5.232 rule (terminal type identification profile view)

Function

The **rule** command configures a terminal type identification rule.

The **undo rule** command deletes a terminal type identification rule.

By default, a terminal type identification rule is not configured.

NOTE

This function is supported only by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Format

rule *rule-id* { **mac** *mac-address* **mask** { *mask-length* | *mask* } | **dhcp-option** *option-id* { **sub-match** | **all-match** } { **ascii** *option-text* | **hex** *option-hex-string* } | **user-agent** { **sub-match** | **all-match** } *user-agent-text* }

undo rule *rule-id*

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a terminal type identification rule.	The value is an integer that ranges from 0 to 7.
mac *mac-address*	Specifies a terminal MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
mask { *mask-length* | *mask* }	Indicates the mask or mask length of a terminal MAC address.	The value of *mask* is in H-H-H format. An H is a hexadecimal number of 4 digits. The value of *mask-length* is an integer that ranges from 1 to 48.

Parameter	Description	Value
dhcp-option *option-id*	Identifies the terminal type using a DHCP option. *option-id* specifies the ID of a DHCP option.	The value is an integer that ranges from 1 to 254. **NOTE** Currently, the identification rule takes effect only when the value is set to 12, 55, or 60.
sub-match	Indicates partial match. The user agent (UA) or Option information detected by the AC must be the same as or contain the value of *option-text* or *user-agent-text*.	-
all-match	Indicates exact match. The UA or Option information detected by the AC must be the same as the value of *option-text* or *user-agent-text*.	-
ascii *option-text*	Specifies the Option information that a terminal must match as an ASCII string.	The value is a string of 1 to 247 case-sensitive characters, spaces supported.
hex *option-hex-string*	Specifies the Option information that a terminal must match as a hexadecimal string.	The value is a string of 1 to 254 case-insensitive characters without spaces and supports only digits and letters (A to F or a to f).
user-agent	Identifies the terminal type using UA information.	-
user-agent-text	Specifies the UA information that a terminal must match.	The value is a string of 1 to 247 case-sensitive characters.

Views

Terminal type identification profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A terminal type identification rule is set based on the terminal's MAC address, UA, and DHCP Option information.

- Match the first 24 bits of a terminal's MAC address, which is known as the Organizationally Unique Identifier (OUI), to identify the corresponding manufacturer.
- Use the UA information carried in HTTP packets from a terminal to identify the operating system and its version, the CPU type, browser type, and browser version.
- Use the manufacturer information carried in Option12, Option55, and Option60 in DHCP packets from a terminal to identify the terminal's host name and manufacturer type.

A terminal type can be identified by checking whether the terminal information matches the identification rule configured. Once the identification is performed, user rights can be delivered or access control can be implemented based on terminal types.

Precautions

- To match an identification rule, the terminal information must be the same as all the configuration items in the rule.
- If the specified *rule-id* already exists and the new rule conflicts with the original rule, the new rule replaces the original one in the conflicting part, which is the same as editing an existing rule.
- To modify a rule that already contains *rule-id*, delete the old rule and create a rule. Otherwise, the configuration result may be incorrect.
- When a terminal's information meets conditions of identification rules in multiple terminal type identification profiles, the terminal type identification profile that contains MAC address-based identification rules is preferentially matched.

Example

Configure terminal type identification rule 1 in the terminal type identification profile **test**.

```
<HUAWEI> system-view
[HUAWEI] device-profile profile-name test
[HUAWEI-device-profile-test] rule 1 mac 00e0-fc59-1ee0 mask 12
```

13.5.233 remote-access-user manage

Function

The **remote-access-user manage** command enables user management through Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS).

The **undo remote-access-user manage** command disables HTTP- or HTTPS-based user management.

By default, HTTP- or HTTPS-based user management is disabled.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

remote-access-user manage { **http** | **https ssl-policy** *policy-name* } **port** *port-num* [**acl** *acl-number*]

undo remote-access-user manage { **http** | **https ssl-policy** *policy-name* } **port** *port-num* [**acl** *acl-number*]

Parameters

Parameter	Description	Value
http	Specifies HTTP-based user management.	-
https	Specifies HTTPS-based user management.	-
ssl-policy *policy-name*	Specifies the SSL policy used by the built-in Portal server.	The value must be the name of an existing SSL policy. The SSL policy type must be set to server SSL policy.
port *port-num*	Specifies a port number.	● For HTTP, the value can be 80 or any integer in the range of 1025 to 55535. ● For HTTPS, the value can be 443 or any integer in the range of 1025 to 55535.
acl *acl-number*	Specifies the number of an ACL.	The value is an integer in the range from 3000 to 3999 and must be an existing ACL number. **NOTE** A maximum of 64 ACLs can be delivered. If more than 64 ACLs are configured, only the first 64 ACLs take effect.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **remote-access-user manage** command is run, you can manage access users through HTTP or HTTPS on a remote host or server, including forcibly logging out users and deregistering users (by modifying the user status to pre-connection). You can also configure an ACL in the command to specify which remote hosts or servers can be used to manage users.

Prerequisites

Before enabling HTTPS-based user management, run the **ssl policy** *policy-name* command in the system view to create an SSL policy.

Precautions

- If an ACL is specified, the source IP addresses defined in the ACL rules must use service ports, instead of management ports, to communicate with the device.
- In V200R020C10SPC100 and later versions, after HTTP- or HTTPS-based user management is enabled, you must also run the **remote-access-user manage server-source** command to configure the local gateway address used by the device to receive and respond to packets. Otherwise, HTTP- or HTTPS-based user management cannot be used.

Example

Enable HTTP-based user management.

```
<HUAWEI> system-view
[HUAWEI] remote-access-user manage http port 8080
```

13.5.234 remote-access-user manage server-source

Function

The **remote-access-user manage server-source** command configures the local gateway address used by the device to receive and respond to packets when HTTP- or HTTPS-based user management is enabled.

The **undo remote-access-user manage server-source** command restores the default configuration.

By default, the device does not receive or respond to any packets when HTTP- or HTTPS-based user management is enabled.

NOTE

Only the following switch models support this command:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

remote-access-user manage server-source { **all-interface** | **ip-address** *ip-address* }

undo remote-access-user manage server-source { **all-interface** | **ip-address** }

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.
all-interface	Indicates that the IPv4 address is set to 0.0.0.0. That is, the local gateway address used by the device to receive and respond to packets can be any address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In V200R020C10SPC100 and later versions, after HTTP- or HTTPS-based user management is enabled, you must also run the **remote-access-user manage server-source** command to configure the local gateway address used by the device to receive and respond to packets. Otherwise, HTTP- or HTTPS-based user management cannot be used.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and HTTP- or HTTPS-based user management is enabled, the device delivers the **remote-access-user manage server-source all-interface** command by default to set the local gateway address used by the device to receive and respond to packets to any address.
- After the **remote-access-user manage server-source all-interface** command is configured, the local gateway address used by the device to receive and respond to packets can be any address, which increases system security risks. Therefore, you are not advised to configure this command.

- After the **remote-access-user manage server-source all-interface** command is run, the system clears all configurations of the **remote-access-user manage server-source ip-address** *ip-address* command.
- If the **remote-access-user manage server-source all-interface** command has been configured on the device, the **remote-access-user manage server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

Configure 10.1.1.1 as the local gateway address for user management.

```
<HUAWEI> system-view
[HUAWEI] remote-access-user manage server-source ip-address 10.1.1.1
```

13.5.235 server-detect

Function

The **server-detect** command enables the Portal server detection function.

The **undo server-detect** command disables the Portal server detection function.

By default, the Portal server detection function is disabled.

Format

server-detect [**interval** *interval-period* | **max-times** *times* | **critical-num** *critical-num* | **action** { **log** | **trap** } *] *

undo server-detect [**interval** | **max-times** | **critical-num** | **action** { **log** | **trap** } *]

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the detection interval of the Portal server.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 60.
max-times *times*	Specifies the maximum number of times that the detection fails.	The value is an integer that ranges from 1 to 255. The default value is 3.
critical-num *critical-num*	Specifies the minimum number of Portal servers in Up state.	The value is an integer that ranges from 0 to 128. The default value is 0. The default value is recommended.

Parameter	Description	Value
action	Specifies the action to be taken after the number of detection failures exceeds the maximum.	-
log	Indicates that the device sends a log after the number of detection failures exceeds the maximum.	-
trap	Indicates that the device sends a trap after the number of detection failures exceeds the maximum.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

If the communication is interrupted because the network between the device and Portal server is faulty or the Portal server is faulty, new Portal authentication users cannot go online. This brings great inconvenience to users.

After the Portal server detection function is enabled in the Portal server template, the device detects all Portal servers configured in the Portal server template. If the number of times that the device fails to detect a Portal server exceeds the upper limit, the status of the Portal server is changed from Up to Down. If the number of Portal servers in Up state is less than or equal to the minimum number (specified by the **critical-num** parameter), the device performs the corresponding operation to allow the administrator to obtain the real-time Portal server status or ensure that the users have certain network access rights.

NOTE

The detection interval of the Portal server multiplied by the maximum number of detection failures cannot be less than the keepalive heartbeat interval of the Portal server. It is recommended that the configured detection interval of the Portal server be greater than the keepalive heartbeat interval of the Portal server.

The device does not support IPv6 Portal server detection.

If the Portal server does not support detection, you do not need to configure this command.

- You are advised to use the default value of the **critical-num** parameter for the following reasons:
  - If the number of Portal servers in Up state is less than or equal to the value of **critical-num**, the value of **Status** in the **display server-detect state** command output is **Abnormal**. If the authentication escape function is configured, users are granted limited network access rights.
  - If the number of Portal servers in Up state is greater than the value of **critical-num**, the value of **Status** in the **display server-detect state** command output is **Normal**.
  - If there is only one Portal server and **critical-num** is set to 1, the number of Portal servers in Up state is equal to the value of **critical-num** when the Portal server goes Up. In this case, the value of **Status** in the **display server-detect state** command output is **Abnormal**. In such scenarios, you need to set **critical-num** to the default value **0** so that the value of **Status** is **Normal**.

Example

Enable the Portal server detection and keepalive function in the Portal server template **abc**, set the detection interval to 100s, set the maximum number of failures to 5, and specify the log sent after the number of failures exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect interval 100 max-times 5 action log
```

13.5.236 server-detect type

Function

The **server-detect type** command configures the mode in which a device detects Portal server status.

The **undo server-detect type** command restores the default Portal server detection mode.

By default, the Portal-based Portal server detection mode is configured.

Format

server-detect type { **portal** | **http** }

undo server-detect type

Parameters

Parameter	Description	Value
portal	Specifies the Portal-based Portal server detection mode.	-
http	Specifies the HTTP-based Portal server detection mode.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Precautions

In Portal-based Portal server detection mode, the Portal server periodically (the time is determined by the server) sends heartbeat packets to the access device, which then determines the server reachability based on the heartbeat packets. If the access device receives Portal heartbeat packets or other authentication packets from the Portal server within the detection interval (configured using **server-detect interval** *interval-period*) and the packets are verified to be correct, the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In HTTP-based Portal server detection mode, the access device periodically sends HTTP packets to the Portal server and expects a response packet from the Portal server. If the access device receives a response packet within the specified detection interval (configured using **server-detect interval** *interval-period*), the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In Portal-based Portal server detection mode, the Portal server must use the Portal protocol and support sending Portal heartbeat packets. If the Portal server does not meet these requirements, you can configure the HTTP-based detection mode. In this way, if the device detects that the Portal server is Down, the device grants new users the corresponding network access rights.

Precautions

HTTP-based Portal server detection applies to both wireless access scenarios and wired access scenarios using MAC+Portal authentication.

Example

Configure the device to detect Portal server status using HTTP.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect type http
```

13.5.237 server-ip (Portal server template view)

Function

The **server-ip** command configures an IP address for a Portal server.

The **undo server-ip** command deletes an IP address for a Portal server.

By default, no IP address is configured for a Portal server.

Format

server-ip *server-ip-address* &<1-10>

server-ip ipv6 *server-ipv6-address* &<1-3>

undo server-ip { *server-ip-address* | **all** }

undo server-ip ipv6 { *server-ipv6-address* | **all** }

NOTE

The **ipv6** *server-ipv6-address* parameter is only supported by the following models:

S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI

Parameters

Parameter	Description	Value
server-ip-address	Specifies an IPv4 address of a Portal server.	The value is in dotted decimal notation.
ipv6 *server-ipv6-address*	Specifies an IPv6 address of a Portal server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all IPv4 addresses of a Portal server.	-
ipv6 all	Deletes all IPv6 addresses of a Portal server.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server (system view)** command, configure parameters for the template.

Run the **server-ip** command to configure an IP address for the Portal server in the Portal server template view. When receiving a Portal authentication request packet from a user, the device sends a response packet to the Portal server with the configured IP address. Multiple IP addresses can be configured in a Portal server template. This configuration allows Portal authentication users to access the same Portal authentication page using multiple IP addresses, making the authentication process more flexible.

Precautions

- After the IP address corresponding to a Portal server is configured in the Portal server template, users are allowed to access the IP address. If the destination URL in an HTTP packet matches this IP address, redirection is not triggered.
- If multiple IP addresses are configured for a Portal server in the Portal server template, you are advised to run the **url (Portal server template view)** command to configure a URL for the Portal server. If no URL is configured, the device uses the first IP address as the URL by default, and the other IP addresses do not take effect. When the switch functions as the AC, configured server IP addresses will be automatically delivered to APs and authentication-free rules will be generated. Currently, only the first four IPv4 addresses and the first four IPv6 addresses take effect on the APs.
- When you run the **server-ip** command to specify IPv6 addresses, you must also specify IPv4 addresses. This is because the device does not support IPv6 Portal protocol exchange.

Example

Set the Portal server IP address in the Portal server template **test** to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] server-ip 10.10.10.1
```

13.5.238 server-source (Portal server template view)

Function

The **server-source** command configures the local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled.

The **undo server-source** command restores the default configuration.

By default, the device does not receive any packets from the Portal server.

Format

server-source ip-address *ip-address*

undo server-source ip-address

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address.	The value is in dotted decimal notation.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

V200R020C10SPC100 and later versions: If Portal authentication is enabled on the device, you must configure the local gateway address used by the device to receive and respond to the packets sent by the Portal server. You can use either of the following methods to configure the address:

- Run the **web-auth-server server-source all-interface** command in the system view.
- Run the **server-source ip-address** *ip-address* command in the Portal server template view.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and Portal authentication is enabled, the device delivers the **web-auth-server server-source all-interface** command by default.

- After the **web-auth-server server-source all-interface** command is run, the system clears all configurations of the **server-source ip-address** *ip-address* command.
- If the **web-auth-server server-source all-interface** command has been configured on the device, the **server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

In the Portal server template **server1**, configure 10.1.1.1 as the local gateway address used by the device to receive and respond to the packets sent by the Portal server.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server1
[HUAWEI-web-auth-server-server1] server-source ip-address 10.1.1.1
```

13.5.239 shared-key (Portal server template view)

Function

The **shared-key** command configures the shared key that the device uses to exchange information with a Portal server.

The **undo shared-key** command restores the default setting.

By default, no shared key that the device uses to exchange information with a Portal server is configured.

Format

shared-key cipher *key-string*

undo shared-key

Parameters

Parameter	Description	Value
cipher	Displays a shared key in cipher text.	-
key-string	Specifies the shared key.	The value is a string of case-sensitive characters without spaces. It can be a string of 1 to 255 characters in plain text, or a string of 20 to 392 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a shared key is configured using the **shared-key** command, the Portal packet exchanged between the device and Portal server carries an authenticator generated according to the shared key, and the authenticator is used to check whether the Portal packet at the receiver is correct. This effectively improves the information exchange security.

Precautions

To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

Example

Configure the shared key in the Portal server template **test** to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] shared-key cipher YsHsjx_202206
```

13.5.240 source-ip (Portal server template view)

Function

The **source-ip** command configures the source IP address for the device to communicate with a Portal server.

The **undo source-ip** command restores the default setting.

By default, no source IP address is configured for the device to communicate with a Portal server.

Format

source-ip *ip-address*

undo source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with a Portal server.	The value is in dotted decimal notation.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication between the device and Portal server, run the **source-ip** command to configure a source IP address on the device.

If the device is configured with a loopback IP address and a common IP address, the device can communicate with the Portal server only when the loopback IP address and common IP address are the same. The **source-ip** command configures a source IP address on the device in the Portal server template view to allow communication between the device and a Portal server.

Precautions

Ensure that the configured source IP address is the device IP address. The source IP address cannot be 255.255.255.255, all 0s, class D address, class E address, or loopback address.

Example

Set the source IP address for communication between the device and a Portal server to 192.168.1.100 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] source-ip 192.168.1.100
```

13.5.241 source-interface (Portal server template view)

Function

The **source-interface** command configures an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server.

The **undo source interface** command restores the default configuration.

By default, no source IP address is configured for the device.

Format

source-interface *interface-type interface-number*

undo source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Configures an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server: ● *interface-type* specifies the interface type. **NOTE** The interface must be a loopback interface. ● *interface-number* specifies the interface number.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to communicate with the Portal server normally, ensure that the source IP address in the packets sent by the device to the Portal server is consistent with the device IP address configured on the Portal server. By default, the device uses the IP address of an outbound interface as the source IP address to communicate with the Portal server. When there are multiple outbound interfaces and the outbound interface sending packets changes, the source IP address in the packets sent by the device to the Portal server becomes inconsistent with the device IP address configured on the Portal server. In this situation, communication between the device and Portal server is interrupted. To address this problem, run the **source-interface** command on the device to specify the IP address of a loopback interface as the source IP address used by the device to communicate with the Portal server.

Precautions

The specified interface must be a Layer 3 interface with an IP address configured.

Example

Configure an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.2.25 24
[HUAWEI-LoopBack1] quit
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] source-interface loopback 1
```

13.5.242 static-user

Function

The **static-user** command configures a static user.

The **undo static-user** command deletes the configured static user.

By default, no static user is configured.

Format

static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*] [**ip-user**] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**detect**] | **mac-address** *mac-address* | **vlan** *vlan-id* | **keep-online**] *

undo static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
start-ip-address [*end-ip-address*]	Specifies the IP address range to which a static user belongs. If *end-ip-address* is not specified, the static user is specified by *start-ip-address*.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which a static user belongs.	The value must be an existing VPN instance name.
ip-user	Identifies a static user using an IP address. **NOTE** This parameter is only supported by the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.	-

Parameter	Description	Value
domain-name *domain-name*	Specifies the domain to which a static user belongs. If this parameter is specified, the user name of the static user is in the format of user name@domain name. In this case, @ is the default domain name delimiter. The location of delimiter and domain name can be set as required.	The value must be an existing domain name.
interface *interface-type interface-number*	Specifies the interface connected to a static user. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** A management interface cannot be configured as the interface to which a static user belongs.	-
detect	Permits the device to send ARP packets to trigger MAC address authentication for offline static users.	-
mac-address *mac-address*	Specifies the MAC address for a static user.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Specifies the VLAN to which a static user belongs.	The value is an integer that ranges from 1 to 4094.
keep-online	Keeps a static user online, with offline detection not performed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In network deployment, static IP addresses are assigned to dumb terminals such as printers and servers. These users can be configured as static users for flexible authentication.

After static users are configured, the device can use static user information such as their IP addresses as the user names to authenticate the users only if one of the 802.1X authentication, MAC address authentication, and Portal authentication modes is enabled on the interfaces connected to the static users.

When **ip-user** is specified, IP addresses are used to identify static users and control their permission.

- When some terminals have multiple IP addresses and one MAC address, and they can access the network only after each IP address is authenticated, specify the **ip-user** parameter to identify these users and configure the **ip-static-user enable** command in the authentication template bound to the user access interfaces.
- When all terminals have multiple IP addresses and can access the network only after each IP address is authenticated, only configure the **ip-static-user enable** command in the authentication template bound to the user access interfaces.

Precautions

If a **static-user** command with **ip-user** specified is configured, other **static-user** command configurations without **ip-user** specified become invalid. To enable the **static-user** commands without **ip-user** to take effect, cancel the **static-user** command configuration with **ip-user**, or specify **ip-user** in all **static-user** commands.

After the **static-user** command is executed to modify the configuration, if a new user cannot log in due to an IP address conflict with an existing user, you need to run the **cut access-user** command to force the existing user to log out.

When the interface (**interface** *interface-type interface-number*) mapping static users is specified, the VLAN (**vlan** *vlan-id*) to which the interface belongs must be configured.

This function takes effect only for users who go online after this function is successfully configured.

Only when static users have the **ip-user** parameter configured and connect to the interfaces bound to the authentication template in which the **ip-static-user enable** command configured, IP addresses can be used to identify these users and control their permission.

After this command is configured to specify the VLAN to which a static user belongs, and the user is authenticated and the VLAN is authorized, if the authorized VLAN is different from the previously specified VLAN, the user is added to the new authorized VLAN and is no longer a static user.

When the command is configured on the UC device and directly delivered to the ASs in the SVF scenario, the command must be in the following format: **static-user** *start-ip-address* [*end-ip-address*] { **vlan** *vlan-id* | **mac-address** *mac-address* } or **static-user** *start-ip-address* [*end-ip-address*] **vlan** *vlan-id* **mac-address** *mac-address*.

In SVF mode, when the **direct-command view command static-user** command is executed on the control device to deliver the static-user configuration to access devices, the configuration must be the same as the **static-user** command configuration on the control device. If they are different, the **static-user** command configuration on the control device takes effect.

In policy association scenarios, the **static-user** command is optional on access devices. When this command is configured, the static-user configuration must be the same as that on the control device. If they are different, the **static-user** command configuration on the control device takes effect.

Example

Configure the IP address range of 10.1.1.1 to 10.1.1.10, authentication domain **test**, and VLAN 10 for static users.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] static-user 10.1.1.1 10.1.1.10 domain-name test vlan 10
```

13.5.243 static-user not-update-ip enable

Function

The **static-user not-update-ip enable** command disables the device from updating IP addresses of static users.

The **undo static-user not-update-ip enable** command allows the device to update IP addresses of static users.

By default, the device cannot update IP addresses of static users.

Format

static-user not-update-ip enable

undo static-user not-update-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IP addresses for static users are configured, terminals using these IP addresses are authenticated as static users. After these terminals go online, they may send abnormal ARP packets whose source IP addresses are not the IP addresses of static users to the authentication device. After receiving the packets, the device updates terminal IP addresses in CIB entries. As a result, the terminals are no longer static users and go offline. To prevent this problem, you can run the **static-user not-update-ip enable** command to disable the device from updating IP addresses of static users.

Precautions

When the **undo static-user not-update-ip enable** command is configured and the function of identifying static users through IP addresses is enabled, only the function of identifying static users through IP addresses takes effect.

Example

Disable the device from updating IP addresses of static users.

```
<HUAWEI> system-view
[HUAWEI] static-user not-update-ip enable
```

13.5.244 static-user password

Function

The **static-user password** command sets the password for a static user in authentication.

The **undo static-user password** command restores the default password for the static user.

By default, the password for a static user in authentication not set.

Format

static-user password cipher *password*

undo static-user password

Parameters

Parameter	Description	Value
cipher	Indicates that the password is displayed in cipher text.	-
password	Specifies the password of a static user.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a static user triggers authentication through an ARP packet, you can run the **static-user password** command to set the password for the static user. The access device then sends the password to the authentication server.

Precautions

To improve security, change the default password immediately and update the password periodically. It is recommended that the new password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

This function takes effect only for users who go online after this function is successfully configured.

Example

Set YsHsjx_202206 as the static user password for authentication.

```
<HUAWEI> system-view
[HUAWEI] static-user password cipher YsHsjx_202206
```

13.5.245 static-user username format-include

Function

The **static-user username format-include** command sets the user name for a static user in authentication.

The **undo static-user username format-include** command restores the default user name for the static user.

By default, the name of a static user consists of **system-name** and **ip-address**. For example, if the access device name is **test** and user IP address is 1.1.1.1, the static user name is **test1.1.1.1**.

Format

static-user username format-include { **ip-address** | **mac-address** | **system-name** }

undo static-user username format-include

Parameters

Parameter	Description	Value
ip-address	Specifies the user IP address as the static user name.	-
mac-address	Specifies the user MAC address as the static user name.	-
system-name	Specifies the access device name as the static user name. To configure the device name, run the **sysname** command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a static user triggers authentication through an ARP packet, you can run the **static-user username format-include** command to set the user name for the static user. The access device then sends the user name to the authentication server.

NOTE

If the user name of a static user contains a device name whose length exceeds 16 bytes, the system uses only the first 16 bytes of the device name.

This function takes effect only for users who go online after this function is successfully configured.

Example

Set the user IP address as the static user name for authentication.

```
<HUAWEI> system-view
[HUAWEI] static-user username format-include ip-address
```

13.5.246 static-user username macaddress format

Function

The **static-user username macaddress format** command sets the user name for authenticating a static user to a MAC address.

The **undo static-user username macaddress format** command restores the default setting.

By default, the user name for authenticating a static user is not set to a MAC address.

Format

static-user username macaddress format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password-with-macaddress**]

undo static-user username macaddress format

Parameters

Parameter	Description	Value
with-hyphen [**normal**] [**colon**] | **without-hyphen**	Specifies the format of a MAC address. - **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 00e0-fc12-3456. - **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-e0-fc-12-34-56. - **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 00e0:fc12:3456. - **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:e0:fc:12:34:56. - **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 00e0fc123456.	-
uppercase	Configures a MAC address in uppercase format as the user name for authentication. If this parameter is not specified, a MAC address in lowercase format is used.	-

Parameter	Description	Value
password-with-macaddress	Configures a MAC address as the password. If this parameter is not specified, the password configured in the **static-user password cipher** *password* command is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In network deployment, static IP addresses are assigned to dumb terminals such as printers, that is, their users are configured as static users. To authenticate a static user, you can run this command to set the user name and password for authentication to a MAC address. This command takes priority over the **static-user username format-include** { **ip-address** | **mac-address** | **system-name** } command and **static-user password cipher** *password* command.

Example

Set the MAC address with hyphens (-) as the user name and password for authenticating a static user.

```
<HUAWEI> system-view
[HUAWEI] static-user username macaddress format with-hyphen password-with-macaddress
```

13.5.247 traffic-filter acl

Function

The **traffic-filter acl** command configures ACL-based packet filtering.

The **undo traffic-filter acl** command deletes the ACL configured for packet filtering.

By default, ACL-based packet filtering is not configured.

Format

traffic-filter inbound acl [**ipv6**] { *acl-number* | **name** *acl-name* }

undo traffic-filter inbound acl [**ipv6**] { *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
inbound	Configures packet filtering in the inbound direction of the interface.	-
acl-number	Specifies the ID of the user ACL or user ACL6 configured for packet filtering.	The value is an integer in the range from 6000 to 9999. If the configured user ACL or user ACL6 does not exist, ACL-based packet filtering does not take effect.
ipv6	Specifies the IPv6 ACL configured for packet filtering.	- **NOTE** The S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S does not support IPv6 UCL.
name *acl-name*	Specifies the name of the user ACL or user ACL6 configured for packet filtering.	The value is a string of 1 to 64 case-sensitive characters without spaces and must begin with a letter. If the configured user ACL or user ACL6 does not exist, ACL-based packet filtering does not take effect.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In NAC network deployment, you can run the **ucl-group** command to classify users and configure user ACL or user ACL6 rules numbered from 6000 to 9999. You can then implement intra-group isolation (users in a group cannot communicate with each other) and inter-group isolation (users in the user group cannot communicate with users in other user groups.), and control network access rights based on the UCL group.

After configuring ACL rules 6000 to 9999, you must run the **traffic-filter acl** command to configure ACL-based packet filtering. The ACL rules then can take effect for the users in the UCL group.

Precautions

If you want to configure packet filtering through an authorized UCL group, run the **traffic-filter** command in a traffic profile to configure packet filtering and bind the traffic profile to a VAP profile. This ensures that packet filtering takes effect for the wireless users that go online on the same AP in the same VLAN.

If the user ACL specified in the **traffic-filter inbound acl** command or the user ACL or user ACL6 delivered by the authentication server is incorrectly configured to block all user traffic, the switch cannot be connected and network-side protocols such as OSPF and BGP are interrupted.

For a stack of S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, and S5720-LI: If the value of **RunningTemplate** is not **nac** in the **display system resource-template** command output on a member switch that forwards traffic out, user ACL6-based packet filtering configured using the **traffic-filter inbound acl ipv6** { *acl-number* | **name** *acl-name* } command in the system view does not take effect on the member switch.

Example

Configure the device to filter the packets in the inbound direction of the interface based on ACL 6001.

```
<HUAWEI> system-view
[HUAWEI] traffic-filter inbound acl 6001
```

13.5.248 traffic-redirect acl

Function

The **traffic-redirect acl** command configures ACL-based packet redirection.

The **undo traffic-redirect acl** command disables ACL-based packet redirection.

By default, ACL-based packet redirection is not configured.

NOTE

This command is supported only by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI.

Format

traffic-redirect inbound acl { *acl-number* | **name** *acl-name* } [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *nexthop-address*

traffic-redirect inbound acl { *acl-number* | **name** *acl-name* } **vpn-instance** *vpn-instance-name*

undo traffic-redirect inbound acl { *acl-number* | **name** *acl-name* }

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **traffic-redirect inbound acl** { *acl-number* | **name** *acl-name* } **vpn-instance** *vpn-instance-name* command.

Parameters

Parameter	Description	Value
inbound	Configures packet redirection in the inbound direction of the interface.	-
acl *acl-number*	Specifies the ID of the ACL configured for packet redirection.	The value is an integer in the range from 6000 to 9999. If the configured user ACL does not exist, ACL-based packet redirection does not take effect.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces and must begin with a letter. If the configured user ACL does not exist, ACL-based packet redirection does not take effect.
vpn-instance *vpn-instance-name*	Redirects packets to a VPN instance.	The value must be the name of an existing VPN instance.
ip-nexthop *nexthop-address*	Redirects packets to a next-hop IPv4 address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In NAC network deployment, you can run the **ucl-group** command to classify users and configure user ACLs with numbers in the range of 6000 to 9999. You can then implement intra-group isolation (users in a group cannot communicate with each other) and inter-group isolation (users in the user group cannot communicate with users in other user groups), and control network access rights based on the UCL group.

After configuring ACLs with numbers in the range of 6000 to 9999, you can run the **traffic-redirect acl** command to configure ACL-based packet redirection. The ACLs then can take effect for the users in the UCL group.

When the **traffic-redirect** command and the **traffic-filter acl** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is redirected.

Precautions

If the destination address information about the packets to be filtered based on a user ACL rule contains UCL group, the ACL rule takes effect only for S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

If the destination address information about the packets to be filtered based on a user ACL rule contains UCL group, the ACL rule does not take effect.

Example

Configure the device to redirect the packets in the inbound direction of the interface based on ACL 6001.

```
<HUAWEI> system-view
[HUAWEI] traffic-redirect inbound acl 6001 ip-nexthop 192.168.1.1
```

13.5.249 ucl-group (service scheme view)

Function

The **ucl-group** command binds a UCL group to a service scheme.

The **undo ucl-group** command unbinds the UCL group from the service scheme.

By default, no UCL group is bound to a service scheme.

Format

ucl-group { *group-index* | **name** *group-name* }

undo ucl-group

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The UCL group must exist.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **ucl-group** command to bind a UCL group to the service scheme. The user assigned with the service scheme will have the functions of the UCL group.

Prerequisites

A UCL group has been created using the **ucl-group** command.

Example

Bind the UCL group **abc** to the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 10 name abc
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] ucl-group name abc
```

13.5.250 ucl-group domain

Function

The **ucl-group domain** command configures a domain name in a static UCL group.

The **undo ucl-group domain** command deletes a domain name from a static UCL group.

By default, no domain name is configured in a static UCL group.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support domain names in static UCL groups.

Format

ucl-group domain domain-name *domain-name* { *group-index* | **name** *group-name* }

undo ucl-group domain { **domain-name** *domain-name* | *group-index* | **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
domain-name *domain-name*	Specifies a domain name in a static UCL group.	The value is a string of 3 to 255 case-sensitive characters that can contain letters, digits, and special characters (_ . - *), but not spaces. A maximum of one asterisk (*) is supported. If a domain name contains an asterisk (*) at the beginning, the second character must be a period (.). If a domain name contains an asterisk (*) at the end, the last second character must be a period (.).
group-index	Specifies the index of a static UCL group.	The value is an integer in the range from 1 to 64000 for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 48 for the S6720-EI, S6720S-EI.
name *group-name*	Specifies the name of a static UCL group.	The value must be an existing UCL group name on the device.
all	Specifies all static UCL groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an enterprise network, a server that provides resources has a fixed domain name. The administrator can identify this server using a UCL group and associate the server domain name with the UCL group to form a static UCL group.

After a domain name of a resource server is configured in a static UCL group, the server IP addresses can be obtained based on this domain name and the user access policies can be managed based on the static UCL group, simplifying network deployment.

Prerequisites

A UCL group has been created using the **ucl-group** command.

Follow-up Procedure

Run the **dns snooping enable** command to enable DNS snooping.

Precautions

In the ubiquitous service solution, this command does not need to be run on the device, and it is configured on the controller and delivered to the device.

If the IP address obtained based on a domain name conflicts with the IP address configured using the **ucl-group ip** command, the configured IP address takes effect.

Currently, only IPv4 addresses can be obtained based on domain names.

In policy association and SVF scenarios, access devices do not support this command.

UCL groups do not support IP address overlapping. The device cannot allocate users or resources with the same IP addresses in different VPNs to different UCL groups, and can only allocate these users or resources to the same UCL group.

Example

Set the domain name in the static UCL group **email** to **example.com**.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name email
[HUAWEI] ucl-group domain domain-name example.com name email
```

13.5.251 ucl-group ip

Function

The **ucl-group ip** command configures an IP address in a static UCL group. The static UCL group is also called the static resource group.

The **undo ucl-group ip** command deletes an IP address from a static UCL group.

By default, no IP address is configured in a static UCL group.

NOTE

IP addresses in static UCL groups are only supported by S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI.

Format

ucl-group ip *ip-address* { *mask-length* | *ip-mask* } { *group-index* | **name** *group-name* } [**escape**]

undo ucl-group ip { *ip-address* { *mask-length* | *ip-mask* } | *group-index* | **name** *group-name* | **all** }

undo ucl-group ip { *ip-address* { *mask-length* | *ip-mask* } | *group-index* | **name** *group-name* } **escape**

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a static UCL group. **NOTE** You can specify the IP address configured for the local device.	The value is in dotted decimal notation in the format X.X.X.X.
mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 1 to 32.
ip-mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.
group-index	Specifies the index of a static UCL group.	The value is an integer in the range from 1 to 64000 for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 48 for the S6720-EI, S6720S-EI.
name *group-name*	Specifies the name of a static UCL group.	The value must be an existing UCL group name on the device.
escape	Specifies an escape static UCL group.	-
all	Specifies all static UCL groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an enterprise network, a server that provides resources has a fixed IP address. The administrator can identify this server using a UCL group and associate the server IP address with the UCL group to form a static UCL group.

After a static UCL group is created for a resource server, the user access policies can be managed based on the static UCL group to simplify network deployment.

Prerequisites

A UCL group has been created using the **ucl-group** command.

Precautions

In the ubiquitous service solution, this command does not need to be run on the device, and it is configured on the controller and delivered to the device.

UCL groups do not support IP address overlapping. The device cannot allocate users or resources with the same IP addresses in different VPNs to different UCL groups, and can only allocate these users or resources to the same UCL group.

Example

Configure the static UCL group named **email** with the IP address 10.1.1.1/24.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name email
[HUAWEI] ucl-group ip 10.1.1.1 24 name email
```

13.5.252 ucl-group (system view)

Function

The **ucl-group** command creates a UCL group.

The **undo ucl-group** command deletes the configured UCL group.

By default, no UCL group is created.

Format

ucl-group *group-index* [**name** *group-name*]

undo ucl-group { **all** | *group-index* | **name** *group-name* }

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer in the range from 1 to 30 on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S. The value is an integer in the range from 1 to 48 on the S6720-EI, S6735-S, S6720S-EI. The value is an integer in the range from 1 to 64000 on the S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S5731-H, S5731S-H, S5731-S, S5731S-S.

Parameter	Description	Value
name *group-name*	Specifies the name of a UCL group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value cannot be -, --, a, an, or any, and cannot contain the following special characters: / \ : * ? " < > | @ ' %
all	Specifies the all UCL group.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In NAC network deployment, there are a large number of users and each user may be configured with many ACL rules. The ACL resources on the device are limited and therefore are insufficient to meet the demand of each user. If ACL rules are independently deployed for each user, the workload is heavy.

In actual NAC application, there are a large number of access users but the user types (users of a type have the same network access rights) are limited. The users can be classified using UCL groups (identify user types), and a group of ACL rules are deployed for users of the same type.

After you create UCL groups on the device and configure a UCL group for a user on the authentication server, the authentication server delivers the user's UCL group to the device when authenticating the user. In this way, the device obtains the mapping between users and UCL groups, and accordingly adds users to different UCL groups so that the users in each group can share the same ACL rules.

Follow-up Procedure

A UCL group only identifies a user type and does not control users' network access rights. To control the network access rights, you must first configure ACL rules numbered from 6000 to 9999 and then configure ACL-based packet filtering.

1. Run the **acl** command to create an ACL with the number range of 6000 to 9999.
2. Run the **rule (user ACL view)** to create rules for the ACL.
3. Run the **traffic-filter acl** command to configure ACL-based packet filtering.

Precautions

A UCL group cannot be deleted after it is referenced using any command for the S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI . For other models, a UCL group cannot be deleted after it is referenced using any command except **rule (user ACL view)**.

The UCL group and iStack functions are mutually exclusive for the S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI . A UCL group can be configured on the device only when it is deployed in a single-node system, the stack ID is 0, no stack port is configured, and no dedicated stack cable is installed. If a UCL group has been configured on the device, the stack ID cannot be changed, no stack port can be configured, and a stack cannot be automatically set up even if a dedicated stack cable is installed.

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S:

- In L3VPN scenarios, both static and dynamic UCL groups can be used to control packets sent from PEs to CEs, but only static UCL groups can be used to control packets sent from CEs to PEs.
- When IP packets are forwarded through MPLS LDP tunnels or MPLS TE tunnels, both static and dynamic UCL groups can be used to control the packets leaving the tunnels.
- In L2VPN scenarios, UCL groups cannot be used to control packets.

In the eMDI scenario, after the UCL group is successfully authorized for wireless users, modifying the UCL group configuration does not affect authorized users.

Example

Create a UCL group named **abc** with the group ID 10.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 10 name abc
```

13.5.253 user-queue single-user-mode

Function

The **user-queue single-user-mode** command sets the user queue scheduling mode to single-user mode.

The **undo user-queue single-user-mode** command restores the default configuration.

By default, user queue scheduling uses the user sharing mode.

NOTE

Only the S5731-S, S5731S-S, S5731-H, and S5731S-H switches support this command.

Format

user-queue single-user-mode

undo user-queue single-user-mode

Parameters

None

Views

System view, AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When HQoS is used to implement fine-granularity scheduling for authenticated users, the same user queue is used for scheduling traffic of users who use the same account for login by default. To implement fine-granularity scheduling for each user, run the **user-queue single-user-mode** command to set the user queue scheduling mode to single-user mode.

Follow-up Procedure

Run the **user-queue** command to create a user queue in the QoS profile to implement HQoS scheduling. The RADIUS server then delivers the QoS profile for new online users.

Precautions

- This command is not supported for wireless users.
- If you run this command in the system view, the configuration takes effect for all new users who go online on this device. If you run this command in an AAA domain, the configuration takes effect only for the new users in the AAA domain.
- When HQoS-based authorization is configured for wireless users, only the single-user mode is supported for user queue scheduling.

Example

Set the user queue scheduling mode to single-user mode in the system view.

```
<HUAWEI> system-view
[HUAWEI] user-queue single-user-mode
```

Set the user queue scheduling mode to single-user mode in the AAA domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] user-queue single-user-mode
```

13.5.254 url (URL template view)

Function

The **url** command configures a redirect URL or pushed URL.

The **undo url** command cancels a redirect URL or pushed URL.

By default, no redirect URL or pushed URL is configured.

Format

url [**push-only** | **redirect-only**] *url-string* [**ssid** *ssid*]

undo url [**push-only** | **redirect-only**] [**ssid** *ssid*]

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the **ssid** *ssid* parameter.

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL or pushed URL.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
push-only	Specifies the URL only as a pushed URL.	-
redirect-only	Specifies the URL only as a redirect URL.	-
ssid *ssid*	Specifies the SSID that users associate with. This parameter is valid only for wireless access users. The SSID that users associate with must be the same as that configured on the device; otherwise, the device cannot push URLs to users.	The SSID must already exist.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **url-template name** command, you can run this command to configure a redirect URL or pushed URL. The difference between a redirect URL and a pushed URL is as follows:

- Redirect URL: When a user without network access permission attempts to access the network, the Portal authentication device redirects the user to the redirect URL for authentication.
- Pushed URL: After an authenticated user accesses the network through web for the first time, the access device pushes the web page corresponding to the URL to the user. The web access request from the user is redirected to the specified URL, and then the user is allowed to access network resources.

When you configure a URL on the device, question marks (?) are not supported. If a URL contains a question mark (?), you can run the **parameter start-mark #** command in the URL template view to replace the question mark (?) with a number sign (#).

Precautions

If the **push-only** and **redirect-only** parameters are not specified, the configured URL is used as both a redirect URL and a pushed URL. You can configure a pushed URL using the **force-push** command, or use the **url-template** command to bind a URL template to the Portal server template to configure a redirect URL.

Example

Set the redirect URL to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1
```

13.5.255 url (Portal server template view)

Function

The **url** command configures a URL for a Portal server.

The **undo url** command restores the default configuration.

By default, no URL is configured for a Portal server.

Format

url *url-string*

undo url

Parameters

Parameter	Description	Value
url-string	Specifies a URL for a Portal server.	The value is a string of 1 to 247 case-sensitive characters, with spaces and question marks (?) not supported. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IP address of a Portal server is configured using the **server-ip** command (in the Portal server template view), the Portal server URL (http://*server-ip*) is generated by default on the device. If the actual URL of the Portal server is inconsistent with the default one or the domain name of the Portal server needs to be used for network access, you can run the **url** command to modify the URL of the Portal server on the device.

Precautions

A Portal server has only one URL.

Example

Set the URL of a Portal server to http://www.example.com in the Portal server template named **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url http://www.example.com
```

13.5.256 url-parameter mac-address format

Function

The **url-parameter mac-address format** command configures the MAC address format in URL.

The **undo url-parameter mac-address format** command restores the default MAC address format in URL.

By default, the MAC address format in URL is XXXXXXXXXXXX.

Format

url-parameter mac-address format delimiter *delimiter* { **normal** | **compact** }

undo url-parameter mac-address format

Parameters

Parameter	Description	Value
delimiter *delimiter*	Specifies the delimiter in MAC address.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
normal	Sets the MAC address format to XX-XX-XX-XX-XX-XX.	-
compact	Sets the MAC address format to XXXX-XXXX-XXXX.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Portal servers or websites may require different MAC address formats. You can run the **url-parameter mac-address format** command to set MAC address formats in URL to meet the requirements of Portal servers or website.

Example

Set the delimiter to - and format to XXXX-XXXX-XXXX.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter mac-address format delimiter - compact
```

13.5.257 url-parameter

Function

The **url-parameter** command sets parameters in a URL.

The **undo url-parameter** command deletes parameters in a URL.

By default, a URL does not carry any parameters.

Format

url-parameter { **device-ip** *device-ip-value* | **device-mac** *device-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **ssid** *ssid-value* | **login-url** *url-key url* | **redirect-url** *redirect-url-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **user-vlan** *user-vlan-value* | **ap-group-name** *ap-group-name-value* | **ap-location** *ap-location-value* | **ap-name** *ap-name-value* } *

undo url-parameter

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support the following parameters: **ap-ip** *ap-ip-value*, **ap-mac** *ap-mac-value*, **ssid** *ssid-value*, **user-vlan** *user-vlan-value*, **ap-group-name** *ap-group-name-value*, **ap-location** *ap-location-value*, and **ap-name** *ap-name-value*.

Parameters

Parameter	Description	Value
device-ip *device-ip-value*	Specifies the IP address of the device carried in the URL and sets the parameter name displayed in the URL. In the wireless access scenario, the value of **device-ip** carried in the URL is the CAPWAP gateway address. In wired scenarios, the device cannot automatically obtain the device IP address, you can run the **url-parameter set device-ip** *ip-address* to specify the IP address.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
device-mac *device-mac-value*	Specifies the MAC address of the device carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
ap-ip *ap-ip-value*	Specifies the AP IP address carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. **NOTE** When this parameter is specified in the AC + Fit central AP + RU scenario, the URL carries the name of the Fit central AP.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-mac *ap-mac-value*	Specifies the AP MAC address carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. **NOTE** When this parameter is specified in the AC + Fit central AP + RU scenario, the URL carries the name of the Fit central AP.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ssid *ssid-value*	Specifies the users' associated SSID carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. Supported Chinese characters.If the string is enclosed in double quotation marks (" "), the string can contain spaces.
login-url *url-key url*	Specifies the login URL of an access device. • *url-key*: specifies the identification keyword for the login URL sent to the Portal server during redirection. • *url*: is a specified URL on the access device.	• *url-key*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *url*: The value is a string of 1 to 247 case-sensitive characters without spaces or Chinese characters.

Parameter	Description	Value
redirect-url *redirect-url-value*	Specifies the original URL that a user accesses carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
sysname *sysname-value*	Specifies the device system name carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-ipaddress *user-ipaddress-value*	Specifies the user IP address carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-mac *user-mac-value*	Specifies the user MAC address carried in the URL and sets the parameter name displayed in the URL. **NOTE** This parameter is recommended for inter-AC roaming scenarios.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. Cannot contain question marks. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
user-vlan *user-vlan-value*	Specifies the user VLAN carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wired users.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-group-name *ap-group-name-value*	Specifies the AP group name carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users.	The value is a string of 1 to 16 case-sensitive characters, without spaces or Chinese characters, and the following special characters not supported: =, ?, &.
ap-location *ap-location-value*	Specifies the AP location carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. This parameter takes effect only for fit APs. Before setting this parameter, run the **location** command to configure the installation position of the AP.	The value is a string of 1 to 16 case-sensitive characters, without spaces or Chinese characters, and the following special characters not supported: =, ?, &.
ap-name *ap-name-value*	Specifies the AP name carried in the URL and sets the parameter name displayed in the URL. This parameter is valid only for wireless access users. **NOTE** When this parameter is specified in the AC + Fit central AP + RU scenario, the URL carries the name of the Fit central AP.	The value is a string of 1 to 16 case-sensitive characters, without spaces or Chinese characters, and the following special characters not supported: =, ?, &.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **url-template name** command and URL is configured using the **url** command, you can use the **url-parameter** command to set the parameters in the URL. When a user accesses the Portal server according to the URL, the Portal server obtains user terminal information through the parameters in the URL. The Portal server then provides the corresponding web authentication page for the user according to user terminal information.

In addition, when users are redirected to a website rather than the Portal server according to the pushed URL, the website provides different web pages for the users according to user terminal information carried in the URL.

Precautions

In the wired access scenario, the **device-ip** parameter must be carried in a URL. In addition, you need to run the **url-parameter set device-ip** *ip-address* command to configure the value of **device-ip**, which is typically set to a WAN interface address.

In the policy association scenario, ASs do not support the **device-mac** and **sysname** parameters.

In policy association and SVF scenarios, the device does not support the **user-vlan** parameter.

URL parameter names configured on the device must be the same as those supported by the server. In this example, the device is connected to Agile Controller-Campus or iMaster NCE-Campus.

URL Parameter	URL Parameter Name Supported by Agile Controller-Campus / iMaster NCE-Campus
device-ip	ac-ip
ap-mac	apmac/ap-mac
ssid	ssid
redirect-url	url/redirect-url
user-ipaddress	userip/uaddress
user-mac	usermac/umac
user-vlan	uservlan

Example

Set the user MAC address and access device's system name in the URL.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter user-mac umac sysname test
```

13.5.258 url-parameter set

Function

The **url-parameter set** command sets redirection parameter values.

The **undo url-parameter set** command restores the default setting.

By default, the device automatically obtains redirection parameter values.

Format

url-parameter set device-ip *ip-address*

undo url-parameter set device-ip

Parameters

Parameter	Description	Value
device-ip *ip-address*	Sets the value of the redirection parameter **device-ip**.	The value is in dotted decimal notation.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Assume that a URL template is created using the **url-template name** command, and a URL is configured in the URL template using the **url** command. In the wireless access scenario, the default value of **device-ip** is the CAPWAP gateway address when STAs communicate with the Portal server. In the wired access scenario, the value of **device-ip** cannot be automatically obtained. In the wireless access scenario where communication using the default value fails or in the wired access scenario, run the **url-parameter set device-ip** *ip-address* command to set the redirection parameter (to the WAN interface address typically). When user terminals use the URL to access the Portal server, the Portal server then can obtain user terminal information according to parameters in the URL.

Example

Set the value of the redirection parameter **device-ip** to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter set device-ip 10.1.1.1
```

13.5.259 url-template name

Function

The **url-template name** command creates a URL template or displays an existing URL template view.

The **undo url-template name** command deletes a URL template.

By default, no URL template exists on the device.

Format

url-template name *template-name*

undo url-template name *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a URL template.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a Portal authentication server template is created using the **web-auth-server** command, you can bind a URL template to the Portal authentication server template. The URL template contains the redirect URL and redirect URL parameters.

The **url-template name** command creates a URL template or displays an existing URL template view.

Example

Create a URL template named **test** and enter the template view.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
```

13.5.260 url-template (Portal server template view)

Function

The **url-template** command binds a URL template to a Portal server template.

The **undo url-template** command unbinds a URL template from a Portal server template.

By default, no URL template is bound to a Portal server template.

Format

url-template *url-template* [**ciphered-parameter-name** *ciphered-parameter-name* **iv-parameter-name** *iv-parameter-name* **key cipher** *key-string*]

undo url-template

Parameters

Parameter	Description	Value
url-template	Specifies the name of a URL template.	The value must be an existing URL template name.
ciphered-parameter-name *ciphered-parameter-name*	Specifies the name of the encrypted URL template parameter.	The value is a string of 1 to 16.
iv-parameter-name *iv-parameter-name*	Specifies the encryption vector name of the URL template parameter.	The value is a string of 1 to 16.
key cipher *key-string*	Specifies the shared key for encrypting the URL template parameter.	The value is a string of 1 to 16 plain-text characters or 48 cipher-text characters.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the parameters of a URL template are configured, the URL template must be bound to a Portal authentication server template so that users can be authenticated on the Portal authentication server corresponding to the redirect URL.

To ensure security, you can encrypt the parameter information in the URL template bound to the Portal server template.

Prerequisites

A URL template has been created using the **url-template name** command.

Precautions

If a URL template is bound to the Portal authentication server template and the **url** command is executed to configure the redirect URL corresponding to the Portal authentication server, only the parameters in the URL template take effect.

The URL configured using the **url** command in the URL template view cannot be a pushed URL; otherwise, the command does not take effect.

The device support encryption of parameter information in the URL template only when it connects to the Agile Controller-Campus or iMaster NCE-Campus.

Example

Bind the URL template **abc** to the Portal authentication server template.

```
<HUAWEI> system-view
[HUAWEI] url-template name abc
[HUAWEI-url-template-abc] quit
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url-template abc
```

13.5.261 user-sync

Function

The **user-sync** command enables Portal authentication user information synchronization.

The **undo user-sync** command disables Portal authentication user information synchronization.

By default, Portal authentication user information synchronization is disabled.

Format

user-sync [**interval** *interval-period* | **max-times** *times*] *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the user information synchronization interval.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 300.
max-times *times*	Specifies the maximum number of user information synchronization failures.	The value is an integer that ranges from 2 to 255. The default value is 3.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If communication is interrupted because the network between the device and Portal server is disconnected or the Portal server is faulty, online Portal authentication users cannot go offline. Therefore, user information on the device and on the Portal server may be inconsistent and accounting may be inaccurate.

The **user-sync** command enables user information synchronization so that user information on the device and Portal server is synchronized at intervals to ensure user information consistency.

During information synchronization, the device does not disconnect the user immediately after detecting that the device has certain user information while the server does not have such information. Instead, the device disconnects the user when the maximum number of user information synchronization failures is reached.

Precautions

If users go online during the keepalive interval of the Portal server, the Portal server does not have their entries. After the Portal server goes Up and starts synchronizing user information, the device does not disconnect these users even if synchronization fails. The device retails these users until next time these users go online and performs Portal authentication, ensuring good user experience.

The value of *interval-period** *times* configured on the device must be greater than the interval for the Portal server to send synchronization packets. Otherwise, the device may force users offline when it cannot receive any synchronization packet from the Portal server after the maximum failure number is reached.

When you run the **user-sync** command, make sure that the Portal server supports this function. Otherwise, the users will go offline.

Example

Enable user information synchronization in the Portal server template **abc**, set the interval for user information synchronization to 100s, and set the maximum number of synchronization failures to 5.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] user-sync interval 100 max-times 5
```

13.5.262 user-vlan (service scheme view)

Function

The **user-vlan** command configures a user VLAN in a service scheme.

The **undo user-vlan** command deletes the user VLAN configured in the service scheme.

By default, no user VLAN is configured in the service scheme.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **vlan** command to configure a user VLAN in the service scheme. The user assigned with the service scheme will be added to the user VLAN and obtain network resources in the VLAN.

Precautions

An authorized VLAN cannot be delivered to online Portal users.

This command does not take effect for users who are already online.

If the user access mode is not **multi-share**, to make the **user-vlan** command take effect, you must configure the link type of access switches' interfaces connected to users to hybrid. Access switches will send untagged frames to users in the user VLAN even when interfaces connected users are added to this user VLAN in tagged mode.

For the S6735-S, S6720-EI, S6720S-EI When a user goes online through an interface and is authorized to a VLAN, the interface cannot access a BD in untagged mode. Otherwise, traffic cannot be forwarded.

Example

Configure user VLAN 100 in the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] user-vlan 100
```

13.5.263 voice-vlan (service scheme view)

Function

The **voice-vlan** command enables the voice VLAN in a service scheme.

The **undo voice-vlan** command restores the default setting.

By default, the voice VLAN is disabled in the service scheme.

Format

voice-vlan

undo voice-vlan

Parameters

None

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **service-scheme** command, you can run the **voice-vlan** command to enable the voice VLAN in the service scheme. The voice user assigned with the service scheme will be added to the voice VLAN and obtain network resources in the VLAN.

Precautions

- An authorized VLAN cannot be delivered to online Portal users.
- To make this command take effect, you must have run the **voice-vlan enable** command to configure a specified VLAN as the voice VLAN and enable the voice VLAN on the interface.
- If the user access mode is set to **multi-share**, authorized voice VLANs are not supported.
- This command takes effect only to authorization of users who fail to be authenticated (configured using the **authentication event authen-fail action authorize** or **authentication event authen-server-down action authorize** command, and the **voice-vlan mac-address** command must be run to configure the OUI of the voice VLAN) or voice terminals who can go online without authentication (configured using the **authentication device-type voice authorize** command).
- This command takes effect only for the following users:
  - Users for whom the **authentication event authen-fail action authorize** or **authentication event authen-server-down action authorize** command is run to configure authorization in case of authorization failures or authentication server Down events and the **voice-vlan mac-address** command is run to configure the OUI address of the voice VLAN
  - Users for whom the **authentication device-type voice authorize** command is run to enable voice terminals to go online without authentication
- The following authorized VLANs are listed in descending order of their priorities: voice VLAN configured using the **lldp tlv-enable med-tlv network-policy voice-vlan** command > voice VLAN authorized by the server > voice VLAN authorized locally > data VLAN authorized by the server > data VLAN authorized locally.

Example

Enable the voice VLAN in the service scheme **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] voice-vlan
```

13.5.264 vpn-instance (Portal server template view)

Function

The **vpn-instance** command configures a VPN instance used for communication between the device and Portal server.

The **undo vpn-instance** command restores the default setting.

By default, no VPN instance is configured for communication between the device and Portal server.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VPN implements interconnection within the same department and between different departments in an enterprise. To enable the Portal authentication service in the VPN, run the **vpn-instance** command to bind a Portal server template to a VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the Portal server template must be the same as that bound to the Portal server.

The users in VPN instances bound to different Portal server templates cannot use the same IP addresses because users with the same IP addresses cannot go online or offline.

Example

Bind the Portal server template **abc** to the VPN instance **vpn1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
```

```
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] vpn-instance vpn1
```

13.5.265 web-auth-server listening-port

Function

The **web-auth-server listening-port** command sets the number of the port through which a device listens on Portal protocol packets.

The **undo web-auth-server listening-port** command restores the default listening port.

By default, the device uses port 2000 to listen on Portal protocol packets.

Format

web-auth-server listening-port *port-number*

undo web-auth-server listening-port

Parameters

Parameter	Description	Value
port-number	Specifies the number of the listening port.	The value is an integer that ranges from 1024 to 55535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device exchanges user authentication information with the Portal server using the Portal protocol, you must configure the listening port on the device to receive Portal packets.

You can run the **web-auth-server listening-port** command to set the number of the port through which the device listens on Portal packets. The port number must be the same as the destination port number in Portal packets sent by the Portal server and must be unique.

NOTE

If a specified port is occupied by another service or is a reserved port, the configuration fails. Ensure that the specified port is available when running this command.

Example

Set the number of the port through which a device listens on Portal protocol packets to 3000.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server listening-port 3000
```

13.5.266 web-auth-server (Portal access profile view)

Function

The **web-auth-server** command configures the Portal server template used by a Portal access profile.

The **undo web-auth-server** command restores the default setting.

By default, a Portal access profile does not use any Portal server template.

Format

web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

undo web-auth-server

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server template.	The value must be an existing Portal server template name.
bak-server-name	Specifies the name of a backup Portal server template. **NOTE** The name of the backup Portal server template cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server template name.
direct	Sets the Portal authentication mode to Layer 2 authentication.	-
layer3	Sets the Portal authentication mode to Layer 3 authentication.	-

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Portal server template is configured on the device, this profile must be bound to a Portal access profile. When users who use the Portal access profile attempt to access charged network resources, the HTTP requests are forcibly redirected to the authentication page of the Portal server to implement Portal authentication.

To improve Portal authentication reliability, the backup Portal server template can also be bound to the Portal access profile. When the primary Portal server is disconnected, the users are redirected to the backup Portal server for authentication. This function can take effect only when the Portal server detection function is enabled using the **server-detect** command and heartbeat detection is enabled on the Portal server.

The following Portal authentication modes are available:

- **direct**: When there is no Layer 3 forwarding device between the device and a user, the device can learn the user's MAC address. You can configure the Layer 2 authentication mode so that the device can identify the user using the MAC address.
- **layer3**: Whether Layer 3 forwarding devices exist between the user and device, the MAC address table of the device cannot learn the user's MAC address and can only identify the user using the IP address. You need to configure the Layer 3 authentication mode.

Prerequisites

A Portal server template has been created using **web-auth-server** and the IP address of the Portal server has been configured using **server-ip**.

Precautions

- After a Portal access profile is bound to an authentication profile, the Portal server template used in the Portal access profile cannot be deleted, but can be modified.
- The support for Portal authentication varies depending on different interfaces, routed main interfaces (Only S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI) support only Layer 3 Portal authentication, Layer 2 interfaces support only Layer 2 Portal authentication, and VLANIF interfaces support both Layer 2 and Layer 3 Portal authentication.
- This command does not take effect on the VLANIF interface corresponding to the super VLAN.
- When the direct forwarding mode is used for wireless users and Portal authentication is enabled on the VLANIF interface, the branched networking must be used for the device to make Portal authentication take effect.

Example

Bind the Portal access profile **p1** to the Portal server templates **server1** and **server2** (backup Portal server template), and configure the Layer 2 authentication mode.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server1
[HUAWEI-web-auth-server-server1] server-ip 10.10.1.1
[HUAWEI-web-auth-server-server1] quit
[HUAWEI] web-auth-server server2
[HUAWEI-web-auth-server-server2] server-ip 10.10.2.1
[HUAWEI-web-auth-server-server2] quit
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] web-auth-server server1 server2 direct
```

13.5.267 web-auth-server reply-message

Function

The **web-auth-server reply-message** command enables the device to transparently transmit users' authentication responses sent by the authentication server to the Portal server.

The **undo web-auth-server reply-message** command disables the device from transparently transmitting users' authentication responses sent by the authentication server to the Portal server.

By default, the device transparently transmits users' authentication responses sent by the authentication server to the Portal server.

Format

web-auth-server reply-message

undo web-auth-server reply-message

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The AAA server requires that the authentication messages sent to the Portal server contain the authentication reply; therefore, the **web-auth-server reply-message** command is required. In certain situations, the authentication messages are not required to carry the reply. In this case, run the **undo web-auth-server reply-message** command.

By default, the device directly forwards the authentication result message from the RADIUS server to the Portal server without processing. This is called transparent transmission.

Example

Disable the device from transparently transmitting users' authentication responses to the Portal server.

```
<HUAWEI> system-view
[HUAWEI] undo web-auth-server reply-message
```

13.5.268 web-auth-server (system view)

Function

The **web-auth-server** command creates a Portal server template or displays the Portal server template view.

The **undo web-auth-server** command deletes a Portal server template.

By default, no Portal server template exists.

Format

web-auth-server *server-name*

undo web-auth-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --. **NOTE** *server-name* cannot be set to listening-port, reply-message, version, server-source, or the first character or several leftmost characters of these character strings.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Portal user goes online, the device redirects the user to a specified website (also called the portal website). The user can access resources in the website for free. When the user attempts to access charged network resources, the user must pass authentication on the website. The specific process is as follows:

1. The user opens Internet Explorer and enters a URL in the address box. When receiving the HTTP request sent by the user, the device redirects it to the Portal authentication page of the Portal server.
2. The user enters user information on the authentication page or in the authentication dialog box, and the Portal server forwards the user information to the device.
3. After receiving the user information from the Portal server, the device sends the information to the authentication server for authentication and accounting.
4. After the user is authenticated, the device allows the user to access the Internet if no security policy is enforced.

After a Portal server template is created on the device by using the **web-auth-server** command, run other commands to create a route from the device to the Portal server.

Follow-up Procedure

Run the following commands in the Portal server template view to configure related attributes:

- Run the **server-ip** command to configure the IP address of a Portal server.
- Run the **url** command to configure the URL of a Portal server.
- Run the **port** command to set the port number that a Portal server uses to receive packets from the device.
- Run the **shared-key** command to configure the shared key that the device uses to exchange information with the Portal server.

Precautions

You are advised to back up the Portal server data to prevent authentication failure caused by the Portal server fault.

V200R020C10SPC100 and later versions: If Portal authentication is enabled on the device, you must configure the local gateway address used by the device to receive and respond to the packets sent by the Portal server. You can use either of the following methods to configure the address:

- Run the **web-auth-server server-source all-interface** command in the system view.
- Run the **server-source ip-address** *ip-address* command in the Portal server template view.

Example

Create Portal server template named **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
```

13.5.269 web-auth-server server-source (system view)

Function

The **web-auth-server server-source** command configures the local gateway address used by the device to receive and respond to the packets sent by the Portal server when Portal authentication is enabled.

The **undo web-auth-server server-source** command restores the default configuration.

By default, the device does not receive any packets from the Portal server.

Format

web-auth-server server-source all-interface

undo web-auth-server server-source all-interface

Parameters

Parameter	Description	Value
all-interface	Indicates that the IPv4 address is set to 0.0.0.0. That is, the device can receive and respond to all packets sent by the Portal server.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

V200R020C10SPC100 and later versions: If Portal authentication is enabled on the device, you must configure the local gateway address used by the device to receive and respond to the packets sent by the Portal server. You can use either of the following methods to configure the address:

- Run the **web-auth-server server-source all-interface** command in the system view.
- Run the **server-source ip-address** *ip-address* command in the Portal server template view.

Precautions

- If the system software of the device is upgraded from a version earlier than V200R020C10SPC100 to a later version and Portal authentication is enabled, the device delivers the **web-auth-server server-source all-interface** command by default.
- After the **web-auth-server server-source all-interface** command is run, the system clears all configurations of the **server-source ip-address** *ip-address* command.
- If the **web-auth-server server-source all-interface** command has been configured on the device, the **server-source ip-address** *ip-address* command configured later will fail to be delivered.

Example

In the system view, configure the device to receive and respond to all packets sent by the Portal server.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server server-source all-interface
```

13.5.270 web-auth-server version

Function

The **web-auth-server version** command sets the Portal protocol version supported by the device.

The **undo web-auth-server version** command restores the default setting.

By default, the device supports both the versions V1.0 and V2.0.

Format

web-auth-server version v2 [**v1**]

undo web-auth-server version

Parameters

Parameter	Description	Value
v2	Indicates that the device supports the Portal protocol version V2.0. The major version currently used is V2.0.	-
v1	Indicates that the device supports the Portal protocol version V1.0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Currently, the Portal protocol has two versions: V1.0 and V2.0. The device and Portal server must use the Portal protocol of the same version to ensure normal communication. You can run the **web-auth-server version** command to set the Portal protocol version supported by the device.

NOTE

The version V2.0 is widely used currently.

To ensure smooth communication, the device supports both versions by default.

Example

Configure the device to use only the Portal protocol V2.0.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server version v2
```

13.5.271 web-redirection disable (Portal server template view)

Function

The **web-redirection disable** command disables the Portal authentication redirection function.

The **undo web-redirection disable** command enables the Portal authentication redirection function.

By default, the Portal authentication redirection function is enabled.

Format

web-redirection disable

undo web-redirection disable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

The device redirects all unauthenticated users to the Portal authentication page when the users send access requests to external networks. For example, when the user needs to enter the URL of the authentication page manually, the **web-redirection disable** command can be executed so that unauthorized users are not forcibly redirected to the Portal authentication page.

Example

Disable the Portal authentication redirection function.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server nac
[HUAWEI-web-auth-server-nac] web-redirection disable
```

13.6 NAC Configuration Commands (Common Mode)

13.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.6.2 access-user arp-detect

Function

The **access-user arp-detect** command sets the source IP address and source MAC address of offline detection packets in a VLAN.

The **undo access-user arp-detect** command deletes the source IP address and source MAC address of offline detection packets in a VLAN.

By default, the source IP address and source MAC address are not specified for offline detection packets in a VLAN.

Format

access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

undo access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies the source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or 255.255.255.255 or other valid IP address.
mac-address *mac-address*	Specifies the source MAC address of offline detection packets.	The value is a unicast MAC address in H-H-H format, where H can be one to four hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

If the VLAN to which the user belongs does not have a VLANIF interface or the VLANIF interface does not have an IP address, the device sends an offline detection packet using 0.0.0.0 as the source IP address. If a user cannot respond to an ARP probe packet with the source IP address 0.0.0.0, you can specify a source IP address for the offline detection packet. You are advised to specify the user gateway IP address and its corresponding MAC address as the source IP address and source MAC address of offline detection packets.

Precautions

This function does not take effect for users who use Layer 3 Portal authentication.

If a user on a physical interface is online, this command takes effect only after the user goes online again or the device re-authenticates the user.

Example

Set the source IP address and MAC address of offline detection packets for users in VLAN 10 to 192.168.1.1 and 2222-1111-1234 respectively.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect vlan 10 ip-address 192.168.1.1 mac-address 00e0-fc11-1234
```

13.6.3 access-user arp-detect default ip-address

Function

The **access-user arp-detect default ip-address** command sets the default source IP address of offline detection packets.

The **undo access-user arp-detect default ip-address** command restores the default setting.

By default, the default source IP address of offline detection packets is 0.0.0.0.

Format

access-user arp-detect default ip-address *ip-address*

undo access-user arp-detect default ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or other valid IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

Precautions

This function does not take effect for users who use Layer 3 Portal authentication.

Example

Set the default source IP address of offline detection packets to 0.0.0.0.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect default ip-address 0.0.0.0
```

13.6.4 access-user arp-detect delay

Function

The **access-user arp-detect delay** command configures the delay in sending offline detection packets.

The **undo access-user arp-detect delay** command restores the default configuration.

By default, the delay in sending offline detection packets is 10 seconds.

Format

access-user arp-detect delay *delay*

undo access-user arp-detect delay

Parameters

Parameter	Description	Value
delay	Specifies the delay in sending offline detection packets.	The value is an integer in the range from 10 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A Windows client on the network sends a detection packet with the source address 0.0.0.0 after obtaining an IP address. If the device also initiates an ARP probe with the source address 0.0.0.0, a conflict occurs. To prevent this conflict, you can run the **access-user arp-detect delay** command to set the delay in sending offline detection packets. Typically, detection initiated by a Windows client takes 10 seconds. Therefore, a delay longer than 10 seconds is recommended.

Precautions

This function takes effect only for users who go online after it is configured.

This function takes effect in both ARP probe and ND probe scenarios.

NOTE

Delay after which the device sends the first ARP probe packet = Delay in sending offline detection packets + One-third of the handshake interval between the device and pre-connection or authorized users (configured using the **authentication timer handshake-period** command)

Example

Set the delay for sending offline detection packets to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect delay 20
```

13.6.5 access-user arp-detect fallback

Function

The **access-user arp-detect fallback** command configures an IP address required for calculating the source address of offline detection packets.

The **undo access-user arp-detect fallback** command deletes the IP address configured for calculating the source address of offline detection packets.

By default, no IP address is configured for the device to calculate the source address of offline detection packets.

Format

access-user arp-detect fallback *ip-address* { *mask* | *mask-length* }

undo access-user arp-detect fallback

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address required for calculating the source address of offline detection packets.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation. After the mask is converted into a binary number, all bits before the last 1 must be 1s. That is, 1s in the mask must be continuous and there cannot be any 0s before the last 1.

Parameter	Description	Value
mask-length	Specifies the mask length of the IP address.	The value is an integer in the range from 0 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device does not function as a gateway, it can send offline detection packets with the source address on the same network segment as clients. This source address is calculated based on the client network segment and the IP address specified in the **access-user arp-detect fallback** command. The operation AND is performed between this specified IP address and the wildcard mask to obtain result 1. Then result 1 is added to the network segment of clients to get the source address of offline detection packets. For example, if the network segment of clients is 192.168.1.0/24 and **access-user arp-detect fallback 0.0.0.11 24** is configured, the source address of offline detection packets is 192.168.1.11. The calculated source address must be excluded from the address pool of the DHCP server to prevent IP address conflicts.

Precautions

Only wired users support this function.

This function does not take effect for users who use Layer 3 Portal authentication.

For online users on physical interfaces, this command takes effect only after the users go online again or the device re-authenticates the users. For online users on Eth-Trunk interfaces, this command takes effect immediately.

- The source IP or MAC addresses configured for offline detection packets using the following commands are listed in descending order of priority:
  - **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*
  - **access-user arp-detect fallback** *ip-address* { *mask* | *mask-length* }
  - **access-user arp-detect default ip-address** *ip-address*

  If two or more of the commands are configured, the source IP or MAC address with a higher priority takes effect.

Example

Set the IP address required for calculating the source address of offline detection packets to 0.0.0.11.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect fallback 0.0.0.11 24
```

13.6.6 access-user dot1x-identity speed-limit

Function

The **access-user dot1x-identity speed-limit** command configures the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

The **undo access-user dot1x-identity speed-limit** command restores the default rate limit of Identity packets for 802.1X authentication to be sent to the CPU.

By default, the maximum of Identity packets for 802.1X authentication can be sent to the CPU every second depends on the device.

Format

access-user dot1x-identity speed-limit *value*

undo access-user dot1x-identity speed-limit [*value*]

Parameters

Parameter	Description	Value
value	Specifies the rate limit of Identity packets for 802.1X authentication to be sent to the CPU.	The value is an integer in the range of 5 to 2000, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a large number of Identity packets for 802.1X authentication are sent to the CPU of a switch, the CPU usage is high and other services are affected. To prevent this problem, run the **access-user dot1x-identity speed-limit** command to configure the rate limit of Identity packets for 802.1X authentication to be sent to the CPU, so that the switch discards excess Identity packets.

Example

Set the rate limit of Identity packets for 802.1X authentication to be sent to the CPU to 10 pps.

```
<HUAWEI> system-view
[HUAWEI] access-user dot1x-identity speed-limit 10
```

13.6.7 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a user fails in authentication or goes offline, the device records a system log. The system log contains the MAC addresses of access device and access user and the authentication time.

If a user repeatedly attempts to go online after authentication failures or frequently goes online and offline in a short period, a lot of system logs are generated, which waste system resources and degrade system performance. System log suppression can address this problem. After the device generates a system log, it will not generate the same log within the suppression period (set by **access-user syslog-restrain period**).

NOTE

The same system logs refer to the system logs containing the same MAC addresses. For example, after the device generates a system log for a user failing in authentication, the device will not generate new system log for this user in the suppression period if the user fails in authentication again. The system logs for users logging offline are generated in the same way.

Example

Enable system log suppression.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain enable
```

13.6.8 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets a period for system log suppression.

The **undo access-user syslog-restrain period** command restores the default period for system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period for system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the system log suppression function is enabled using the **access-user syslog-restrain enable** command, use this command to set the system log suppression period. After generating a system log, the device will not generate the same log within the suppression period.

Example

Set the period for system log suppression to 600s.

```
<HUAWEI> system-view
[HUAWEI] access-user syslog-restrain period 600
```

13.6.9 acl authorization statistics enable

Function

The **acl authorization statistics enable** command enables statistics collection on packets that match the ACLs assigned for authorization.

The **undo acl authorization statistics enable** command disables statistics collection on packets that match the ACLs assigned for authorization.

By default, statistics collection on packets that match the ACLs assigned for authorization is disabled.

Format

acl authorization statistics enable

undo acl authorization statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, the authentication server may assign ACLs to users who pass NAC authentication to grant the users access to the network. You can run the **acl authorization statistics enable** command to check the number of user packets that match the assigned ACLs.

Precautions

The function takes effect only for users who go online after this function is enabled, and for the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, and S5720-LI, this function cannot be used to collect statistics on packets that match the permit rules in redirection ACLs.

Example

Enable statistics collection on packets that match the ACLs assigned for authorization.

```
<HUAWEI> system-view
[HUAWEI] acl authorization statistics enable
```

13.6.10 acl-id (user group view)

Function

The **acl-id** command binds an ACL to a user group.

The **undo acl-id** command unbinds an ACL from a user group.

By default, no ACL is bound to a user group.

Format

acl-id *acl-number*

undo acl-id { *acl-number* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL bound to a user group.	The value is an integer that ranges from 3000 to 3999.
all	Deletes all ACL rules bound to a user group.	-

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a user group is created using the **user-group** command, you can run the **acl-id** *acl-number* command to bind an ACL to the user group, so that users in the user group share an ACL.

NOTE

Before an ACL is bound to the user group, do not run the **user-group enable** command to enable the user group; otherwise, the ACL cannot be bound to the user group.

When the user group function is enabled on models except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, ACL rules are delivered to each user and the user group function cannot be used to save ACL resources.

Prerequisites

The ACL has been created using the **acl** or **acl name** command and ACL rules have been configured using the **rule** command.

Precautions

- The ACL bound to a user group cannot be modified or deleted in the system view.
- If no ACL rule is configured for a user group, the device does not restrict the network access rights of users in the user group.
- When configuring ACL rules in a user group, create a rule that rejects all network access requests and ensure that the rule can take effect.
- If all users in a group are required to have the same access rights, do not specify the source IP address in the ACL bound to the user group. If an ACL bound to a user group has defined the source IP address, only users with the same IP address as the source IP address in the ACL can match the ACL in the user group.

Example

Bind ACL 3001 to the user group **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule 5 deny ip destination 192.168.5.0 0.0.0.255
[HUAWEI-acl-adv-3001] quit
[HUAWEI] user-group abc
[HUAWEI-user-group-abc] acl-id 3001
```

13.6.11 authentication critical eapol-success

Function

The **authentication critical eapol-success** command configures the device to send an EAPoL-Success packet to a user after the user is added to the critical VLAN.

The **undo authentication critical eapol-success** command configures the device to send an EAPoL-Fail packet to a user after the user is added to the critical VLAN.

By default, an EAPoL-Fail packet is sent to a user after the user is added to the critical VLAN.

Format

In the system view:

authentication critical eapol-success interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication critical eapol-success interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication critical eapol-success

undo authentication critical eapol-success

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After a user is added to the critical VLAN because the authentication server does not respond, the device can be configured to send an EAPoL-Success or EAPoL-Fail packet to the user to prevent the user from continuously sending access request packets. After receiving the EAPoL-Success packet or EAPoL-Fail packet, the user stops attempting to go online by sending the access request packet repeatedly, which prevents the device performance from degrading.

The user receiving the EAPoL-Success packet can still obtain the IP address through a DHCP packet, while the user receiving the EAPoL-Fail packet fails to do so. The administrator can configure the device to send an EAPoL-Success or EAPoL-Fail packet as required.

Example

Configure the device to send an EAPoL-Success packet to a user after the user is added to the critical VLAN on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication critical eapol-success
```

13.6.12 authentication critical-vlan

Function

The **authentication critical-vlan** command configures a critical VLAN on an interface.

The **undo authentication critical-vlan** command deletes a critical VLAN from an interface.

By default, no critical VLAN is configured on an interface.

Format

In the system view:

authentication critical-vlan *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication critical-vlan [*vlan-id*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication critical-vlan *vlan-id*

undo authentication critical-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a critical VLAN.	The value is an integer that ranges from 1 to 4094.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A critical VLAN is authorized for users when the authentication server does not respond.

When the access device cannot communicate with the RADIUS server or the RADIUS server fails, the authentication process on the network is interrupted and users cannot pass the authentication. After the critical VLAN function of the device is enabled, the device sets the state flag of the authentication server to Down and adds the users to the critical VLAN. In this way, the users can access resources in the critical VLAN without being authenticated.

Precautions

- This command is only valid for 802.1X authentication and MAC address authentication.
- If the free-ip function is configured, the critical VLAN function becomes invalid immediately.
- To make the VLAN authorization function take effect, the link type and access control mode of the authentication interface must meet the following requirements:
  - When the link type is hybrid in untagged mode, the access control mode can be based on the MAC address or interface.
  - When the link type is access or trunk, the access control mode can only be based on the interface.

Example

In the system view, configure 802.1X authentication for the users using Port address-based access method on GE0/0/1 and set the critical VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
[HUAWEI] authentication critical-vlan 20 interface gigabitethernet 0/0/1
```

In the interface view, enable MAC address authentication on GE0/0/1 and set the critical VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] mac-authen
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] mac-authen
[HUAWEI-GigabitEthernet0/0/1] authentication critical-vlan 20
```

13.6.13 authentication device-type voice authorize

Function

The **authentication device-type voice authorize** command enables voice terminals to go online without authentication.

The **undo authentication device-type voice authorize** command disables voice terminals from going online without authentication.

By default, voice terminals are disabled from going online without authentication.

Format

authentication device-type voice authorize [**user-group** *group-name*]

undo authentication device-type voice authorize [**user-group**]

Parameters

Parameter	Description	Value
user-group *group-name*	Specifies the name of the user group based on which network access rights are assigned to voice terminals.	The value must be an existing user group name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both data terminals (such as PCs) and voice terminals (such as IP phones) are connected to switches, NAC is configured on the switches to manage and control the data terminals. The voice terminals, however, only need to connect to the network without being managed and controlled. In this case, you can configure the voice terminals to go online without authentication on the switches. Then the voice terminals identified by the switches can go online without authentication.

Precautions

To enable the switches to identify the voice terminals, enable LLDP or configure OUI for the voice VLAN on the switches. For details, see "Configuring Basic LLDP Functions" in "LLDP Configuration" in the *S300, S500, S2700, S5700, and S6700*

V200R023C00 Configuration Guide - Network Management and Monitoring or "Configuring a Voice VLAN Based on a MAC Address" in "Voice VLAN Configuration" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Ethernet Switching*. If a voice device supports only CDP but does not support LLDP, configure CDP-compatible LLDP on the switch using **lldp compliance cdp receive** command.

If an 802.1X user initiates authentication through a voice terminal, a switch preferentially processes the authentication request. If the authentication succeeds, the terminal obtains the corresponding network access rights. If the authentication fails, the switch identifies the terminal type and enables the terminal to go online without authentication.

Voice terminals can obtain the corresponding network access rights after they pass authentication and go online, when **user-group** *group-name* is not specified. When **user-group** *group-name* is specified, voice terminals can obtain the network access rights specified by the user group after they go online. To use a user group to define network access rights for voice terminals, run the **user-group** *group-name* command to create a user group and configure network authorization information for the users in the group. Note that the user group takes effect only after it is enabled.

If you run this command repeatedly, the latest configuration overrides the previous ones.

This function takes effect only for users who go online after this function is successfully configured.

Example

Enable voice terminals to go online without authentication.

```
<HUAWEI> system-view
[HUAWEI] authentication device-type voice authorize
```

13.6.14 authentication event

Function

The **authentication event** command grants network access rights to users in different authentication stages.

The **undo authentication event** command cancels network access rights of users in different authentication stages.

By default, no network access right is granted to users in different authentication stages.

Format

- Command for 802.1X authentication:

  System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** } { **vlan** *vlan-id* | **user-group** *group-name* }

undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** }

- Command for MAC address authentication:

  System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } { **vlan** *vlan-id* | **user-group** *group-name* }

  undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** }

  VLANIF interface view:

  authentication event { **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **authen-fail** | **authen-server-down** }

- Command for external Portal authentication:

  System view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** }

  VLANIF interface view:

  authentication event { **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **authen-fail** | **authen-server-down** }

- Command for built-in Portal authentication:

  System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view:

  authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } { **vlan** *vlan-id* | **user-group** *group-name* }

  undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** }

  VLANIF interface view:

  authentication event { **authen-fail** | **authen-server-down** } **user-group** *group-name*

  undo authentication event { **authen-fail** | **authen-server-down** }

Parameters

Parameter	Description	Value
pre-authen	Specifies the network access rights granted to users before authentication starts. In an 802.1X authentication, when a device receives an ARP or DHCP request packet sent from a user terminal, but not an authentication request packet from an 802.1X client, the device grants the **pre-authen** right to the user. If only this parameter is specified but the network access rights are not configured for other events, the device grants the **pre-authen** right to the users failing in authentication. In a MAC address or Portal authentication, if only this parameter is specified but the network access rights are not configured for other events, the device grants the **pre-authen** right to the users failing in authentication.	-
authen-fail	Specifies the network access rights granted to users when authentication fails. The device grants this right to all users who have failed in authentication.	-
authen-server-down	Specifies the network access rights granted to users when the authentication server does not respond. If both the **authen-server-down** and **authen-fail** parameters are specified, the **authen-server-down** parameter takes effect if the authentication server does not respond.	-
client-no-response	Specifies the network access rights granted to users when the 802.1X client does not respond. If both the **client-no-response** and **authen-fail** parameters are specified, the **client-no-response** parameter takes effect if the 802.1X client does not respond.	-

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, the user can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094. The VLAN must exist on the device. Otherwise, the configuration does not take effect.
user-group *group-name*	Specifies a user group. When this parameter is specified, the user can access the resources defined for the user group.	The value must be an existing service scheme name.

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To grant different network access rights to users in different stages, you can use this command.

Prerequisites

The 802.1X authentication, MAC address authentication, or Portal authentication has been enabled.

Precautions

- If the command is executed in both the interface view and system view, the configuration in interface view takes effect.
- This function takes effect only for users who go online after this function is successfully configured.
- If the **user-group** parameter is specified in the command, only the network access rights (that is, the ACL and VLAN bound to the user group) configured for the user group take effect.
- If the network access rights specified in the **authentication event** command were defined by a user group, the **dot1x free-ip** command configured in the system view cannot take effect and the **dot1x free-ip** command configured in the interface view does not take effect for the interface.

- If the **user-group** parameter is specified in the command and the destination network access rights in the authentication-free rule configured by **portal free-rule** is the same as that defined for the user group, the authentication-free rule does not take effect.

Example

On GE0/0/1, allow users to access resources in VLAN 10 when authentication fails.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication event authen-fail vlan 10
```

13.6.15 authentication event response-fail

Function

The **authentication event response-fail** command configures the device to return an authentication failure packet when a user fails in authentication or the authentication server does not respond.

The **undo authentication event response-fail** command restores the default configuration.

By default, the device returns an authentication success packet when a user fails in authentication or the authentication server does not respond.

Format

authentication event { **authen-fail** | **authen-server-down** } **response-fail**

undo authentication event { **authen-fail** | **authen-server-down** } **response-fail**

Parameters

Parameter	Description	Value
authen-fail	Specifies that the device returns an authentication failure packet to the 802.1X client or Portal server when a user fails in authentication.	-
authen-server-down	Specifies that the device returns an authentication failure packet to the 802.1X client or Portal server when the authentication server does not respond.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **authentication event** command is executed to configure the network access right used when a user fails in authentication or the authentication server does not respond, the device returns an authentication success packet to the 802.1X client or Portal server by default. Therefore, the user does not know the authentication failure and only limited network resources can be accessed. The user cannot use the expected service.

You can use this command to configure the device to return an authentication failure packet to the 802.1X client or Portal server. In 802.1X authentication, the 802.1X client notifies the user of authentication failure. In Portal authentication, the Portal server pushes an authentication failure message to the user. The user then choose whether to perform reauthentication.

Precautions

- If the command is executed in both the interface view and system view, the configuration in interface view takes effect.
- This function takes effect only for users who go online after this function is successfully configured.
- This command is only applicable to the 802.1X authentication and Portal authentication.

Example

Configure GE0/0/1 to return an authentication failure packet to the 802.1X client or Portal server when a user fails in authentication.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication event authen-fail response-fail
```

13.6.16 authentication event session-timeout

Function

The **authentication event session-timeout** command sets the timeout period of network access rights granted to users in different authentication stages.

The **undo authentication event session-timeout** command restores the default timeout period.

By default, the timeout period of network access rights granted to users is 15 minutes.

Format

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** } **session-timeout** *session-time*

undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** | **client-no-response** } **session-timeout**

VLANIF interface view

authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } **session-timeout** *session-time*

undo authentication event { **pre-authen** | **authen-fail** | **authen-server-down** } **session-timeout**

Parameters

Parameter	Description	Value
pre-authen	Specifies the timeout period of the network access rights granted to users before authentication starts.	-
authen-fail	Specifies the timeout period of the network access rights granted to users when authentication fails.	-
authen-server-down	Specifies the timeout period of the network access rights granted to users when the authentication server does not respond.	-
client-no-response	Specifies the timeout period of the network access rights granted to users when the 802.1X client does not respond. This parameter is only valid for 802.1X authentication.	-
session-time	Specifies the value of timeout period. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.	The value is an integer that ranges from 0 to 71581, in minutes.

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **authentication event** command to grant the network access rights to users in different authentication stages, you can run the **authentication event session-timeout** command to specify the timeout period for the network access rights. Users can access the authorized resources within the timeout period, and will be forced to go offline after the timeout period expires.

If the aging time is set to 0, the network access rights granted to the user will not expire. To disconnect the user from the network, run the **cut access-user** command on the device or configure the authentication server to deliver an offline message to the user.

Precautions

The timeout period set in the VLANIF interface view is not applicable to 802.1X authentication.

If this command is only run in the system view, the configuration takes effect on all interfaces. If this command is run in both the system view and interface view, the configuration on interfaces takes precedence over the global configuration.

This function takes effect only for users who go online after this function is successfully configured.

Example

On interface GE0/0/1, set the timeout period of the network access rights granted to users when authentication fails to 100 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication event authen-fail session-timeout 100
```

13.6.17 authentication guest-vlan

Function

The **authentication guest-vlan** command configures a guest VLAN on an interface.

The **undo authentication guest-vlan** command deletes a guest VLAN from an interface.

By default, no guest VLAN is configured on an interface.

Format

In the system view:

authentication guest-vlan *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication guest-vlan [*vlan-id*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication guest-vlan *vlan-id*

undo authentication guest-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a guest VLAN.	The value is an integer that ranges from 1 to 4094.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During 802.1X authentication and MAC address authentication, a guest VLAN allows users to access limited resources without authentication. The device supports the guest VLAN function.

Users in the guest VLAN can access resources in the guest VLAN without authentication but must be authenticated when they access external resources.

NOTE

- The restrict VLAN is for the users who fail the authentication, while the guest VLAN is for the users who are not authenticated.
- If only a guest VLAN is configured but no restrict VLAN is configured, the users who fail the authentication are added to the guest VLAN.

Prerequisites

The VLAN to be configured as the guest VLAN must have been created.

802.1X authentication has been enabled globally and on the interface using the **dot1x enable** command, or MAC address authentication has been enabled globally and on the interface using the **mac-authen** command.

Precautions

- The guest VLAN function can take effect only in 802.1X and MAC address authentication.
- A super VLAN cannot be configured as a guest VLAN.
- When free IP subnets are configured, the guest VLAN function becomes invalid immediately.
- The guest VLAN function takes effect only when a user sends untagged packets to the device.
- Different interfaces can be configured with different guest VLANs. After a guest VLAN is configured on an interface, the guest VLAN cannot be deleted.
- To make the VLAN authorization function take effect, the link type and access control mode of the authentication interface must meet the following requirements:
  - When the link type is hybrid in untagged mode, the access control mode can be based on the MAC address or interface.
  - When the link type is access or trunk, the access control mode can only be based on the interface.

Example

In the system view, configure 802.1X authentication for the users using Port-based access method on GE0/0/1 and set the guest VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
[HUAWEI] authentication guest-vlan 20 interface gigabitethernet 0/0/1
```

In the interface view, enable MAC address authentication on GE0/0/1 and set the guest VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] mac-authen
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] mac-authen
[HUAWEI-GigabitEthernet0/0/1] authentication guest-vlan 20
```

13.6.18 authentication mac-move enable

Function

The **authentication mac-move enable** command enables MAC address migration.

The **undo authentication mac-move enable** command disables MAC address migration.

By default, MAC address migration is disabled.

Format

authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

undo authentication mac-move enable vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } & <1–10> }

Parameters

Parameter	Description	Value
vlan	Specifies the VLAN range for enabling MAC address migration.	-
all	Enables MAC address migration in all VLANs.	-
vlan-id1 [**to** *vlan-id2*]	Enables MAC address migration in the specified VLANs. ● *vlan-id1* specifies the ID of the first VLAN. ● *vlan-id2* specifies the ID of the second VLAN. The value of *vlan-id2* must be greater than that of *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user is authenticated and accesses the network from one interface of the device, the network cable is pulled out from the interface and plugged in another interface on the device, then the user cannot immediately initiate authentication and access the network. The user can initiate authentication on the current interface only after the user offline detection interval expires or the authentication interface is manually enabled and shut down to clear user online entries. To improve user experience, MAC address migration is enabled so that the user can immediately initiate authentication and access the network after be switched to another access interface.

MAC address migration allows online NAC authentication users to immediately initiate authentication and access the network after they are switched to other access interfaces. If the user is authenticated successfully on the new interface, the online user entry on the original interface is deleted immediately to ensure that only one interface records the online user entry.

In addition, VLANs need to be specified for users in MAC address migration. The VLANs before and after the migration can be specified for the users, and they can be the same or different.

Precautions

- In normal case, enabling MAC address migration is not recommended. It should be enabled only when users have migration requirements during roaming. This prevents unauthorized users from forging MAC addresses of online users and sending ARP, 802.1X, or DHCP packets on other authentication control interfaces to trigger the MAC address migration function and force authorized user offline.
- Cascading migration through intermediate devices is not supported, because ARP and DHCP packets are not sent after the cascading migration.
- MAC address migration is not supported for Layer 3 Portal authentication users.
- In the Layer 2 BNG scenario, the device does not support MAC address migration.
- A user is switched from an interface configured with NAC authentication to another interface not configured with NAC authentication. In this case, the user can access the network only after the original online entry is aged because the new interface cannot send authentication packets to trigger MAC migration.
- In common mode, Portal authentication is triggered only after users who go online through a VLANIF interface send ARP packets and go offline; otherwise, the users can go online again only after the original user online entries age out. Portal authentication cannot be triggered after users who go online through physical interfaces migrate. The users can go online again only after the original user online entries age out.

- After a user who goes online from a VLANIF interface is quieted because of multiple MAC address migrations, MAC address migration can be performed for the quieted user only after the quiet period expires and the ARP entry is aged out.
- When an authorized VLAN is specified in the **authentication mac-move enable vlan** command, you are advised to enable the function of detecting the user status before user MAC address migration.

Example

Enable MAC address migration in all VLANs.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move enable vlan all
```

13.6.19 authentication mac-move detect enable

Function

The **authentication mac-move detect enable** command enables a device to detect users' online status before user MAC address migration.

The **undo authentication mac-move detect enable** command disables a device from detecting users' online status before user MAC address migration.

By default, a device is disabled from detecting users' online status before user MAC address migration.

Format

authentication mac-move detect enable

undo authentication mac-move detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To prevent unauthorized users from spoofing online users to attack a device, run the **authentication mac-move detect enable** command to enable the device to detect users' online status before user MAC address migration. If no users are online, the device permits MAC address migration and allows users to go online from a new access interface. If a user is online, the device terminates MAC address migration and does not allow the user to go online from a new access interface.

You can also run the **authentication mac-move detect retry-interval retry-time** command to set the detection interval and maximum number of detections before user MAC address migration.

Example

Enable a device to detect users' online status before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect enable
```

13.6.20 authentication mac-move detect retry-interval retry-time

Function

The **authentication mac-move detect retry-interval retry-time** command sets the detection interval and maximum number of detections before user MAC address migration.

The **undo authentication mac-move detect retry-interval retry-time** command restores the default setting.

By default, a device detects users' online status once. The detection interval is 3 seconds.

Format

authentication mac-move detect { **retry-interval** *interval* | **retry-time** *times* } *

undo authentication mac-move detect { **retry-interval** | **retry-time** } *

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a device detects users' online status before user MAC address migration.	The value is an integer that ranges from 1 to 5, in seconds.
times	Specifies the maximum number of detections before user MAC address migration.	The value is an integer that ranges from 1 to 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a device is enabled to detect users' online status before user MAC address migration, you can run the **authentication mac-move detect** { **retry-interval** *interval* | **retry-time** *times* } * command to modify the default detection interval and maximum number of detections.

Example

Configure a device to detect users' online status twice at an interval of 5 seconds before user MAC address migration.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move detect retry-interval 5 retry-time 2
```

13.6.21 authentication mac-move quiet-log enable

Function

The **authentication mac-move quiet-log enable** command enables the device to record logs about MAC address migration quiet.

The **undo authentication mac-move quiet-log enable** command disables the device from recording logs about MAC address migration quiet.

By default, the device is enabled to record logs about MAC address migration quiet.

Format

authentication mac-move quiet-log enable

undo authentication mac-move quiet-log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can record logs when adding or deleting MAC address migration quiet entries. This helps the administrator to find out the cause for MAC address migration failure, and improves maintainability of the MAC address migration quiet function.

Example

Enable the device to record logs about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-log enable
```

13.6.22 authentication mac-move quiet-times quiet-period

Function

The **authentication mac-move quiet-times quiet-period** command configures the quiet period and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.

The **undo authentication mac-move quiet-times quiet-period** command restores the default settings.

The default quiet period is 0 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state is 3.

Format

authentication mac-move { **quiet-times** *times* | **quiet-period** *quiet-value* } *

undo authentication mac-move { **quiet-times** | **quiet-period** } *

Parameters

Parameter	Description	Value
times	Specifies the maximum number of MAC address migration times within 60 seconds before users enter the quiet state.	The value is an integer that ranges from 1 to 10.
quiet-value	Specifies the quiet period for MAC address migration users.	The value is an integer that ranges from 0 to 3600. The value 0 indicates that the MAC address migration quiet function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When users frequently switch access interfaces (especially frequent switching due to loops), the device needs to process a large number of authentication packets and entries, which results in high CPU usage. To solve this problem, configure the MAC address migration quiet function.

If the number of MAC address migration times for a user within 60 seconds exceeds the value (*times*) after the MAC address migration quiet function is enabled, the device quiets the user for a certain period (*quiet-value*). During the quiet period, the device does not allow users to perform MAC address migration.

Example

Configure the quiet period to 120 seconds and the maximum number of MAC address migration times within 60 seconds before users enter the quiet state to 5.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-times 5 quiet-period 120
```

13.6.23 authentication mac-move quiet-user-alarm enable

Function

The **authentication mac-move quiet-user-alarm enable** command enables the device to send alarms about MAC address migration quiet.

The **undo authentication mac-move quiet-user-alarm enable** command disables the device from sending alarms about MAC address migration quiet.

By default, the device is disabled from sending alarms about MAC address migration quiet.

Format

authentication mac-move quiet-user-alarm enable

undo authentication mac-move quiet-user-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Example

Enable the device to send alarms about MAC address migration quiet.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm enable
```

13.6.24 authentication mac-move quiet-user-alarm percentage

Function

The **authentication mac-move quiet-user-alarm percentage** command configures the upper and lower alarm thresholds for the percentage of MAC address migration users in quiet state.

The **undo authentication mac-move quiet-user-alarm percentage** command restores the default setting.

By default, the lower alarm threshold is 50 and upper alarm threshold is 100.

Format

authentication mac-move quiet-user-alarm percentage *lower-threshold upper-threshold*

undo authentication mac-move quiet-user-alarm percentage

Parameters

Parameter	Description	Value
lower-threshold	Specifies the lower alarm threshold.	The value is an integer that ranges from 1 to 100.
upper-threshold	Specifies the upper alarm threshold.	The value is an integer that ranges from 1 to 100. The value must be greater than that of *lower-threshold*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **authentication mac-move quiet-user-alarm enable** command can be run to enable the device to send alarms about MAC address migration quiet to improve maintainability of the MAC address migration quiet function. The device sends alarms when the percentage of the actual user amount in the MAC address migration quiet table against the maximum number of users exceeds the upper alarm threshold configured. If the percentage decreases to be equal to or smaller than the lower alarm threshold, the device sends a clear alarm. The upper and lower alarm thresholds are configured using the **authentication mac-move quiet-user-alarm percentage** command.

Precautions

When a user goes online at a rate exceeding the upper limit, the alarm may not be generated.

Example

Configure the upper alarm threshold to 80 and lower alarm threshold to 40.

```
<HUAWEI> system-view
[HUAWEI] authentication mac-move quiet-user-alarm percentage 40 80
```

13.6.25 authentication max-reauth-req

Function

The **authentication max-reauth-req** command sets the maximum number of re-authentication attempts for users in a critical VLAN.

The **undo authentication max-reauth-req** command restores the default setting.

By default, the maximum number of re-authentication attempts is 20 for users in a critical VLAN.

Format

In the system view:

authentication max-reauth-req *times* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication max-reauth-req [*times*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication max-reauth-req *times*

undo authentication max-reauth-req [*times*]

Parameters

Parameter	Description	Value
times	Specifies the maximum number of re-authentication attempts.	The value is an integer that ranges from 1 to 20. The default value is 20.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *Interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

When the authentication server maintained by the device turns to the Up state, the device triggers re-authentication for users already added to the critical VLAN. If the authentication is successful, the users exit the critical VLAN. However, if the re-authentication fails due to reasons such as the fault of the access user's client, the repeated re-authentication degrades the device performance. After the maximum number of re-authentication attempts is set for users in the critical VLAN, the device forces the user to exit the critical VLAN if the user fails the authentication the specified number of times.

Example

Set the maximum number of re-authentication attempts for users in the critical VLAN to 5 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] authentication max-reauth-req 5 interface gigabitethernet 0/0/1
```

13.6.26 authentication open

Function

The **authentication open** command enables the NAC open function.

The **undo authentication open** command disables the NAC open function.

By default, the NAC open function is disabled on an interface.

Format

In the system view:

authentication open interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication open interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication open

undo authentication open

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a new NAC network is set up, the network administrator should pay attention to the number of potential access users and authentication method but does not need to control user access, because the administrator needs to configure user names, passwords, and authorization information on the authentication server. After 802.1X or MAC address authentication is configured on the access device, only authenticated users can access the network, so the administrator cannot obtain information about the users who do not have user names and passwords on the authentication server.

The NAC open function allows the users who failed in authentication to access the network.

Precautions

- The NAC open function is only applied to 802.1X and MAC address authentication.
- The NAC open function is only applied to RADIUS remote authentication.
- The NAC open function is valid only when the MAC address-based mode is used as the access control mode of the interface. After this function is enabled, users can be added to VLANs except a guest VLAN after they log in.
- After NAC open is enabled on an interface and fixed user names are used for MAC address authentication, the users on the interface are allowed to access the network even if they have used incorrect user names or passwords.

Example

Enable the NAC open function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] authentication open interface gigabitethernet 0/0/1
```

13.6.27 authentication port-vlan-modify user-online

Function

The **authentication port-vlan-modify user-online** command enables the function of keeping users online when the port type or VLAN is changed.

The **undo authentication port-vlan-modify user-online** command restores the default setting.

By default, the function of keeping users online when the port type or VLAN is changed is disabled.

Format

authentication port-vlan-modify user-online

undo authentication port-vlan-modify user-online

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user access authentication succeeds, you can change the VLAN allowed to access or the access interface type through the RADIUS server. For example, you can assign VLANs to clients through the server for network planning and deployment. After the deployment is complete, to reduce the impact of link faults and device restart on the network and implement rapid network restoration, you can change the user access VLAN to the authorized VLAN. In this case, you can enable the function of keeping users online when the port type or VLAN is changed to modify interface or VLAN configurations.

Precautions

This function is only supported by MAC and 802.1X authentication.

This function is only supported by wired users.

Example

Enable the function of keeping users online when the port type or VLAN is changed.

```
<HUAWEI> system-view
[HUAWEI] authentication port-vlan-modify user-online
```

13.6.28 authentication restrict-vlan

Function

The **authentication restrict-vlan** command configures a restrict VLAN on an interface.

The **undo authentication restrict-vlan** command deletes the restrict VLAN from an interface.

By default, no restrict VLAN is configured on an interface.

Format

In the system view:

authentication restrict-vlan *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo authentication restrict-vlan [*vlan-id*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

authentication restrict-vlan *vlan-id*

undo authentication restrict-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a restrict VLAN.	The value is an integer that ranges from 1 to 4094.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the restrict VLAN on the device interface, so that the users can still access some network resources (for example, update the virus library) when the users fail the authentication. The users who fail the authentication are added to the restrict VLAN to access the resources in the restrict VLAN. Note that, the user fails the authentication because the authentication server rejects the user for some reasons, for example, the user enters an incorrect user password, not because the authentication times out or the network is disconnected.

NOTE

- The restrict VLAN is for the users who fail the authentication, while the guest VLAN is for the users who are not authenticated.
- If only a guest VLAN is configured but no restrict VLAN is configured, the users who fail the authentication are added to the guest VLAN.

Prerequisites

The VLAN to be configured as the restrict VLAN must have been created.

Precautions

- A super VLAN cannot be configured as a restrict VLAN.
- When free IP subnets are configured, the restrict VLAN function becomes invalid immediately.
- The restrict VLAN function takes effect only when a user sends untagged packets to the device.
- To make the VLAN authorization function take effect, the link type and access control mode of the authentication interface must meet the following requirements:
  - When the link type is hybrid in untagged mode, the access control mode can be based on the MAC address or interface.
  - When the link type is access or trunk, the access control mode can only be based on the interface.

Example

In the system view, configure 802.1X authentication for the users using Port-based access method on GE0/0/1 and set the restrict VLAN to VLAN 20.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 20
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
[HUAWEI] authentication restrict-vlan 20 interface gigabitethernet 0/0/1
```

13.6.29 authentication speed-limit auto

Function

The **authentication speed-limit auto** command enables the device to dynamically adjust the rate of packets from NAC users.

The **undo authentication speed-limit auto** command disables the device from dynamically adjusting the rate of packets from NAC users.

By default, the device does not dynamically adjust the rate of packets from NAC users.

Format

authentication speed-limit auto

undo authentication speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lot of NAC users send authentication or log off requests to the device, the CPU usage may be overloaded especially when the CPU or memory usage is already high (for example, above 80%).

After this command is executed, the device limits the number of NAC packets received per second if the CPU or memory usage is high. This function reduces loads on the device CPU.

Example

Enable the device to dynamically adjust the rate of packets from NAC users.

```
<HUAWEI> system-view
[HUAWEI] authentication speed-limit auto
```

13.6.30 authentication timer re-authen

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail to be authenticated.

The **undo authentication timer re-authen** command restores the default setting.

By default, pre-connection users and users who fail to be authenticated are re-authenticated at an interval of 60 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* }

undo authentication timer re-authen { **pre-authen** | **authen-fail** }

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value is an integer that ranges from 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail to be authenticated.	The value is an integer that ranges from 30 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates the mapping user entries when network access policies are assigned to users who are in the pre-connection phase or fail authentication. To enable users to pass authentication in real time, the device periodically re-authenticates the users who are in the pre-connection phase or fail authentication according to the user entries. The administrator can adjust the re-authentication interval based on the actual network requirements.

Precautions

This command only applies to 802.1X authentication and MAC address authentication.

This function takes effect only for users who go online after this function is successfully configured.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

Configures the interval for re-authenticating users who fail to be authenticated to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication timer re-authen authen-fail 300
```

13.6.31 authentication user-alarm percentage

Function

The **authentication user-alarm percentage** command sets alarm thresholds for the percentage of successfully authenticated NAC users.

The **undo authentication user-alarm** command restores the default alarm thresholds for the percentage of successfully authenticated NAC users.

By default, the lower alarm threshold for the percentage of successfully authenticated NAC users is 50, and the upper alarm threshold is 100.

Format

authentication user-alarm percentage *percent-lower-value percent-upper-value*

undo authentication user-alarm

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of successfully authenticated NAC users.	The value is an integer in the range from 1 to 100, and must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the number of successfully authenticated NAC users reaches a specified percentage, the device generates an alarm. You can run the **authentication user-alarm percentage** command to set the upper and lower alarm thresholds for this percentage.

When the percentage of successfully authenticated NAC users against the maximum number of users allowed by the device is greater than or equal to the upper alarm threshold, the device generates an alarm. When this percentage reaches or falls below the lower alarm threshold, the device generates a clear alarm.

Example

Set the lower and upper alarm thresholds for the percentage of successfully authenticated NAC users to 30 and 80, respectively.

```
<HUAWEI> system-view
[HUAWEI] authentication user-alarm percentage 30 80
```

13.6.32 band-width share-mode

Function

The **band-width share-mode** command enables the bandwidth share mode.

The **undo band-width share-mode** command restores the default configuration.

By default, the bandwidth share mode is disabled.

NOTE

This command is only supported by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

band-width share-mode

undo band-width share-mode

Parameters

None

Views

System view, AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On a home network, all family members go online using the same account. To improve service experience of family members, you can enable the bandwidth share mode so that all members can share the bandwidth.

Precautions

- If this command is run in the system view, it takes effect for all new online users who connected to the device. If this command is run in the AAA domain view, it takes effect only for new online users in the domain.
- If the local or remote RADIUS server does not assign CAR settings to the users who will go online and the online users, the share mode is invalid to the users.

- If the bandwidth share mode is enabled and different users use the same account for authentication, the users going online with no CAR settings assigned will not be affected when CAR settings are assigned to the users who go online later.

Example

Enable the bandwidth share mode in the system view.

```
<HUAWEI> system-view
[HUAWEI] band-width share-mode
```

Enable the bandwidth share mode in the AAA domain view.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] band-width share-mode
```

13.6.33 car (user group view)

Function

The **car** command enables traffic control for users in a user group.

The **undo car** command disables traffic control for users in a user group.

By default, traffic control is disabled for users in a user group.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command, and the user group CAR can only be applied in the interface outbound direction (**outbound**) on the S6720-EI, S6720S-EI.

Format

car { **outbound** | **inbound** } **cir** *cir-value* [**pir** *pir-value* | **cbs** *cbs-value* | **pbs** *pbs-value*] *

undo car { **outbound** | **inbound** }

Parameters

Parameter	Description	Value
outbound	Applies the user group CAR to the outgoing packets on an interface to restrict the outgoing packet rate.	-

Parameter	Description	Value
inbound	Applies the user group CAR to the incoming packets on an interface to restrict the incoming packet rate.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR value must be greater than or equal to the CIR value. The default PIR value is equal to the CIR value.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 10000 to 4294967295, in bytes. The default value of *cbs-value* is 188 x *cir-value*.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 10000 to 4294967295, in bytes. The value of *pbs-value* must be larger than that of *cbs-value* and is equal to 188 times of the value of *pir-value* by default.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user groups are created using the **user-group** command, you can run the **car outbound** command to configure traffic control for users in a user group so that users in different groups are allocated different bandwidths.

Precautions

- The **car** command takes effect on each user in a user group.
- This function takes effect only for users who go online after this function is successfully configured.

Example

Set the CIR to 10000 Kbit/s and the CBS to 50000 bytes for outgoing packets of users in a user group.

```
<HUAWEI> system-view
[HUAWEI] user-group test
[HUAWEI-user-group-test] car outbound cir 10000 cbs 50000
```

13.6.34 cut access-user

Function

The **cut access-user** command forces users offline.

Format

cut access-user open

cut access-user user-group *group-name*

Parameters

Parameter	Description	Value
open	Forces open users offline.	-
user-group *group-name*	Specifies the user group based on which the users are forced offline.	The value must be an existing user group name.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a user goes online, if you want to modify the user's network access rights or detect that the user is unauthorized, run this command to force the user offline.

Example

Force open users offline.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] cut access-user open
```

13.6.35 display aaa statistics access-type-authenreq

Function

The **display aaa statistics access-type-authenreq** command displays the number of requests for MAC, Portal, or 802.1X authentication.

Format

display aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, or 802.1X authentications.

To view the number of requests for MAC, Portal, or 802.1X authentication, run the **display aaa statistics access-type-authenreq** command.

Example

Display the number of requests for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> display aaa statistics access-type-authenreq
mac     authentication request     :2
portal  authentication request     :0
dot1x   authentication request     :0
```

Table 13-95 Description of the **display aaa statistics access-type-authenreq** command output

Item	Description
mac authentication request	Number of MAC authentication requests.
portal authentication request	Number of Portal authentication requests.

Item	Description
dot1x authentication request	Number of 802.1X authentication requests.

13.6.36 display authentication mode

Function

The **display authentication mode** command displays the current NAC configuration mode and the mode after restart.

Format

display authentication mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mode** command to view the current NAC configuration mode.

Example

Display the current NAC configuration mode and the mode after restart.

```
<HUAWEI> display authentication mode
  Current authentication mode is unified-mode
  Next authentication mode is unified-mode
```

Table 13-96 Description of the **display authentication mode** command output

Item	Description
Current authentication mode is unified-mode	Current NAC configuration mode.

Item	Description
Next authentication mode is unified-mode	NAC configuration mode after the device restarts. Run the **authentication unified-mode** command to switch the NAC mode to unified mode. Run the **undo authentication unified-mode** command to switch the NAC mode to common mode.

13.6.37 display access-user

Function

The **display access-user** command displays information about online NAC users.

Format

display access-user open

display access-user option82 { **circuit-id** *text* | **remote-id** *text* }

display access-user user-group *group-name* [**detail**]

NOTE

The **detail** parameter is only supported by the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
open	Displays open user information.	-
option82	Displays information about MAC address authentication users who use the Option 82 field as user names.	-
circuit-id *text*	Displays information about MAC address authentication users who specify the circuit ID as user names.	The value must be existing circuit-id information.

Parameter	Description	Value
remote-id *text*	Displays information about MAC address authentication users who specify the remote ID as user names.	The value must be existing remote-id information.
user-group *group-name*	Displays information about users in a specified user group.	The value must be an existing user group index.
detail	Displays detailed information about users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online NAC users.

Example

Display open user information.

```
<HUAWEI> display access-user open
------------------------------------------------------------------------------
 UserID Username               IP address         MAC            Status
 ------------------------------------------------------------------------------
 16016  1@radius              10.8.7.5          00e0-fc12-3456  Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1, Open: 1, printed: 1
```

NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When you run the **display access-user** command without specifying any parameter to view user information and the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following the 19th character; that is, only 22 characters are displayed. When you run the **display access-user** command with parameters specified to view detailed information about the user table, all the characters of **username** are displayed, and the rule for converting special characters remains unchanged.

Display detailed information about users in user group 1.

```
<HUAWEI> display access-user user-group 1 detail
 ------------------------------------------------------------------------------
```

```
Basic:
  User ID                         : 114
  User name                       : lx
  Domain-name                     : lx
  User MAC                        : 00e0-fc01-0105
  User IP address                 : 10.1.1.5
  User vpn-instance               : -
  User IPv6 address               : -
  User access Interface           : GigabitEthernet0/0/5
  User vlan event                 : Success
  QinQVlan/UserVlan               : 0/200
  User vlan source                : user request
  User access time                : 2015/02/08 14:35:02
  User accounting session ID      :
5735_S0000500000020072****0000072
  Option82 information            : -
  User access type                : MAC
  Terminal Device Type            : Data Terminal
  Dynamic group name(Effective)   : 1
  Session Timeout                 : 1800(s) (local), Remaining: 330(s)
  Termination Action              : RE-AUTHENTICATION
  Service Scheme Priority         : 0

AAA:
  User authentication type        : MAC authentication
  Current authentication method   : None
  Current authorization method    : -
  Current accounting method       : None

 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-97 Description of the display access-user command output

Item	Description
UserID/User ID	ID that is assigned to a user after the user goes online.
Username/User name	User name.
IP address	User IP address.
MAC	User MAC address.

Item	Description
Status,User vlan event	User access status. • Open: For a wired user, the user goes online through the open function upon authentication failure. For wireless users, no authentication is performed. • Success: authentication is successful • Pre-authen: pre-authentication • Client-no-resp: the client does not respond • Fail-authorized: authorization upon authentication failure • Web-server-down: web server is Down • Aaa-server-down: AAA server is Down
Domain-name	User domain.
User MAC	User MAC address.
User IP address	User IP address.
User vpn-instance	VPN instance to which the user belongs.
User IPv6 address	User IPv6 address.
User access Interface	User access interface.
QinQVlan/UserVlan	VLAN to which the user belongs. • In QinQ application, **QinQVlan** indicates the outer VLAN ID, and **UserVlan** indicates the inner VLAN ID. • For a common VLAN, **UserVlan** indicates the VLAN to which the user belongs, and the value of **QinQVlan** is 0.

Item	Description
User vlan source	Source of the user VLAN. - server vlan: The VLAN is delivered by the remote server. - user group vlan: the VLAN is bound to a user group. - service scheme vlan: The VLAN is configured in the service scheme view. - local event vlan: The VLAN is a locally configured authorized VLAN (for guests or NAC escape). - user request: The VLAN is carried in the user authentication request.
User access time	Time when a user goes online. If the system is configured with a time zone and uses DST, the time is displayed in the format of YYYY-MM-DD HH:MM:SS UTC±HH:MM DST.
User accounting session ID	ID of an accounting session.
Option82 information	Option 82 information.
User access type	User access type: **IPoE** indicates an IP session user.
Terminal Device Type	Terminal device type.
Dynamic group name(Effective)	Name of a UCL group.
Session Timeout	Session timeout period. - xx(s) (local): indicates the locally configured reauthentication interval for MAC or 802.1X authentication users. - xx(s) (server): indicates that the RADIUS server delivers the Session-Timeout (27) attribute, which indicates the maximum number of seconds a user should be allowed to remain connected.

Item	Description
Termination Action	Whether the device is configured to reauthenticate users when the time exceeds the value of Session-Timeout delivered by the RADIUS server. ● reauthenticate: Reauthentication is performed. To configure this function, run the **authentication termination-action reauthenticate** command.
Service Scheme Priority	User priority in a service scheme.
AAA	AAA information of the user.
User authentication type	User authentication type, which depends on the access type of the user.
Current authentication method	Current authentication mode.
Current authorization method	Current authorization mode.
Current accounting method	Current accounting mode.
Total	Total number of online users.
printed	Number of displayed online users.

13.6.38 display access-user dot1x-identity statistics

Function

The **display access-user dot1x-identity statistics** command displays statistics about Identity packets for 802.1X authentication on a switch.

Format

display access-user dot1x-identity statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the statistics about Identity packets for 802.1X authentication on a switch.

Example

Display statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> display access-user dot1x-identity statistics
------------------------------------------------------------------------
Receive(Packet)    Pass(Packet)    Drop(Packet)    Last-dropping-time
------------------------------------------------------------------------
0                  0               0               -
------------------------------------------------------------------------
```

Table 13-98 Description of the **display access-user dot1x-identity statistics** command output

Item	Description
Receive(Packet)	Total number of Identity packets for 802.1X authentication received by the switch.
Pass(Packet)	Number of Identity packets for 802.1X authentication sent to and processed by the CPU of the switch.
Drop(Packet)	Number of Identity packets for 802.1X authentication discarded by the switch.
Last-dropping-time	Latest time when the switch discarded Identity packets for 802.1X authentication. If no packet loss record exists on the switch, this field displays **-**.

13.6.39 display authentication mac-move configuration

Function

The **display authentication mac-move configuration** command displays the MAC address migration configuration.

Format

display authentication mac-move configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display authentication mac-move configuration** command to view the MAC address migration configuration. The configuration includes the number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state, the period that MAC address migration users stay in the quiet state, the interval at which a device detects users' online status before user MAC address migration, and the number of detections before user MAC address migration.

Example

Display the MAC address migration configuration.

```
<HUAWEI> display authentication mac-move configuration
Mac-move vlan config:all
Mac-move quiet times:1
Mac-move quiet period(s):120
Mac-move quiet log:ENABLE
Mac-move quiet user alarm:ENABLE
Mac-move quiet user alarm lower percentage(%):
50
Mac-move quiet user alarm upper percentage(%):100
Mac-move detect:DISABLE
Mac-move detect retry-interval(s):3
Mac-move detect retry-time:1
```

Table 13-99 Description of the **display authentication mac-move configuration** command output

Item	Description
Mac-move vlan config	VLAN ID range in which MAC address migration is enabled. For details, see the **authentication mac-move enable** command.
Mac-move quiet times	Number of times that MAC address migration users are allowed to migrate their MAC addresses 60s before they enter the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.

Item	Description
Mac-move quiet period(s)	Period that MAC address migration users stay in the quiet state. For details, see the **authentication mac-move quiet-times quiet-period** command.
Mac-move quiet log	Whether a device is enabled to record logs about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-log enable** command.
Mac-move quiet user alarm	Whether a device is enabled to send alarms about user quietness triggered by MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move quiet-user-alarm enable** command.
Mac-move quiet user alarm lower percentage(%)	Lower alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move quiet user alarm upper percentage(%)	Upper alarm threshold for the percentage of MAC address migration users in quiet state. For details, see the **authentication mac-move quiet-user-alarm percentage** command.
Mac-move detect	Whether a device is enabled to detect users' online status before user MAC address migration: ● ENABLE ● DISABLE For details, see the **authentication mac-move detect enable** command.

Item	Description
Mac-move detect retry-interval(s)	Interval at which a device detects users' online status before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.
Mac-move detect retry-time	Number of detections before user MAC address migration. For details, see the **authentication mac-move detect retry-interval retry-time** command.

13.6.40 display authentication mac-move quiet-user

Function

The **display authentication mac-move quiet-user** command displays information about MAC address migration users in quiet state.

Format

display authentication mac-move quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address migration users in quiet state.	-
mac-address *mac-address*	Displays information about MAC address migration users in quiet state with a specified MAC address.	The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run this command to view information about MAC address migration users in quiet state.

Example

Display information about all MAC address migration users in quiet state.

```
<HUAWEI> display authentication mac-move quiet-user all
Quiet MAC Information
------------------------------------------------------------------------------
Quiet MAC                                        Quiet Remain Time(Sec)
------------------------------------------------------------------------------
00e0-fc02-0003                                    143
------------------------------------------------------------------------------
1 quiet MAC found, 1 printed.
```

Table 13-100 Description of the **display authentication mac-move quiet-user all** command output

Item	Description
Quiet MAC	MAC address of MAC address migration users in quiet state.
Quiet Remain Time(Sec)	Remaining quiet time of MAC address migration users in quiet state, in seconds.

13.6.41 display authentication user-alarm configuration

Function

The **display authentication user-alarm configuration** command displays alarm thresholds for the percentage of successfully authenticated NAC users.

Format

display authentication user-alarm configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the alarm thresholds for the percentage of successfully authenticated NAC users.

Example

Display the alarm thresholds for the percentage of successfully authenticated NAC users.

```
<HUAWEI> display authentication user-alarm configuration
  Current Alarm Percent:100
  Current Alarm Resume Percent:60
```

Table 13-101 Description of the **display authentication user-alarm configuration** command output

Item	Description
Current Alarm Percent	Upper alarm threshold for the percentage of successfully authenticated NAC users.
Current Alarm Resume Percent	Lower alarm threshold for the percentage of successfully authenticated NAC users.

13.6.42 display dot1x

Function

The **display dot1x** command displays 802.1X authentication information.

Format

display dot1x statistics

display dot1x [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
statistics	Displays statistics on 802.1X authentication. The statistics about 802.1X authentication is displayed only when this parameter is specified.	-

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays 802.1X authentication information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. 802.1X authentication information on all device interfaces is displayed if this parameter is not specified.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dot1x** command to view configuration results of all configuration commands in 802.1X authentication and statistics about 802.1X packets.

The command output helps you to check whether the current 802.1X authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

The **display dot1x** command displays the statistics on 802.1X packets. You can locate the fault according to the packet statistics. When the fault is rectified, run the **reset dot1x statistics** command to clear the packet statistics. After a period of time, run the **display dot1x** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display 802.1X authentication information.

```
<HUAWEI> display dot1x
 Global 802.1x is Enabled
 Authentication method is CHAP
 Max users: 1024
 Current users: 1
 DHCP-trigger is Disabled
 Handshake is Enabled
 Quiet function is Enabled
 Mc-trigger port-up-send is Disabled
 Parameter set:Dot1x Handshake Period       16s   Reauthen Period     60s
              Arp Handshake Period          0s   Client Timeout      10s
              Quiet Period                600s   Quiet-times          2
              Eth-Trunk Handshake Period   120s   Tx Period           30
              Mac-By-Pass Delay            30s
 Dot1x URL: www.***.com.cn
 Free-ip configuration(IP/mask):    192.168.1.0     /255.255.255.0
GigabitEthernet0/0/3 status: UP  802.1x protocol is Enabled
 Port control type is Auto
 Authentication mode is MAC-based
 Authentication method is CHAP
 Reauthentication is disabled
 Dot1x retry times: 2
 Authenticating users: 1
 Current users: 1

 Authentication Success: 1          Failure: 0
 Enter Enquence        : 0
 EAPOL Packets: TX     : 19         RX     : 0
 Sent      EAPOL Request/Identity Packets       : 1
          EAPOL Request/Challenge Packets      : 0
          Multicast Trigger Packets            : 18
          EAPOL Success Packets                : 0
          EAPOL Failure Packets                : 0
 Received  EAPOL Start Packets                  : 0
          EAPOL Logoff Packets                 : 0
          EAPOL Response/Identity Packets      : 0
          EAPOL Response/Challenge Packets     : 0

Online user(s) info:
UserId   MAC/VLAN           AccessTime             UserName
------------------------------------------------------------------------------
17487    00e0-fc12-3456/34   2018/07/30 09:49:15     lss
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Display 802.1X statistics.

```
<HUAWEI> display dot1x statistics
 Dropped   EAPOL Access Flow Control       : 0
          EAPOL Check Sysmac Error        : 0
          EAPOL Get Vlan ID Error         : 0
          EAPOL Packet Flow Control       : 0
          EAPOL Online User Reach Max     : 0
```

```
          EAPOL Static or BlackHole Mac   : 0
          EAPOL Get Vlan Mac Error        : 0
          EAPOL Temp User Exist           : 0
          EAPOL no replace dot1x          : 0

DHCP      Enter Enqueue                   : 0
          Processed Packet                : 0
          Dropped Packet                  : 0

ARP       Enter Enqueue                   : 0
          Processed Packet                : 0
          Dropped Packet                  : 0

ND        Enter Enqueue                   : 0
          Processed Packet                : 0
          Dropped Packet                  : 0

DHCPv6    Enter Enqueue                   : 0
          Processed Packet                : 0
          Dropped Packet                  : 0

ANYL2     Enter Enqueue                   : 0
          Processed Packet                : 0
          Dropped Packet                  : 0

Sent      Authentication Request          : 0
          Cut Request                     : 0
          Cut Command Ack                 : 0
          Authentication Ack Fail Aff     : 0
          Update Ip                       : 0
          Wlan Eap Authentication Request      : 0
          Wlan Eap Authentication Request Ack  : 0
          Wlan Eap Send Pmk               : 0
          Wlan Eap Reauthenticate Send Pmk     : 0
          Update User Online Time         : 0

Received  Authentication Ack              : 0
          Reauthenticate Command          : 0
          Cut Command                     : 0
          Cut Ack                         : 0
          Sam Nac Ack                     : 0
          Notify Server Up                : 0
          Wlan Eap Authentication Request      : 0
          Wlan Mac Authentication Request      : 0
          Notify Vlanif Mac Authentication     : 0
```

Table 13-102 Description of the **display dot1x** command output

Item	Description
Global 802.1x is Enabled	802.1X authentication is enabled globally. To enable 802.1X authentication, run the **dot1x enable** command.
Authentication method is CHAP	CHAP authentication is enabled. The authentication methods include EAP, CHAP, and PAP To enable CHAP authentication, run the **dot1x authentication-method** command.
Max users	Maximum number of global online users, the value varies according to device models. To set the maximum number of global online users, run the **dot1x max-user** command.

Item	Description
Current users	Number of current online users.
DHCP-trigger is Disabled	Authentication triggering through DHCP packets is disabled. To trigger authentication using DHCP packets, run the **dot1x dhcp-trigger** command.
Handshake is Enabled	The handshake function is enabled for online users.
Quiet function is Disabled	The quiet function is disabled for users. To enable the quiet function, run the **dot1x quiet-period** command.
Mc-trigger port-up-send is Disabled	The function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled. To configure the function, run the **dot1x mc-trigger port-up-send enable** command.
Parameter set	Settings of 802.1X authentication parameters.
Dot1x Handshake Period	Handshake interval between the device and 802.1X authentication client connected to a non-Eth-Trunk interface. To set the handshake interval, run the **dot1x timer** command.
Reauthen Period	Re-authentication interval. To set the re-authentication interval, run the **dot1x timer** command.
Arp Handshake Period	Handshake interval of the device with pre-connection users and authorized users.
Client Timeout	Timeout interval of a client. To set the timeout interval of a client, run the **dot1x timer** command.
Quiet Period	Value of the quiet timer. To set the value of the quiet timer, run the **dot1x timer** command.
Quiet-times	Maximum number of authentication failures before an 802.1X user enters the quiet state. To set the maximum number of authentication failures, run the **dot1x quiet-times** command.

Item	Description
Eth-Trunk Handshake Period	Handshake interval between the device and 802.1X authentication client connected to an Eth-Trunk. To set the handshake interval, run the **dot1x timer** command.
Tx Period	The interval for sending authentication requests. To set the timeout interval of a client, run the **dot1x timer** command.
Mac-By-Pass Delay	The value of the delay timer for MAC address bypass authentication. To set the timeout interval of a client, run the **dot1x timer** command.
Dot1x URL	Redirect-to URL. To set the redirect-to URL, run the **dot1x url** command.
Free-ip configuration(IP/mask)	Free IP subnet. To set the free IP subnet, run the **dot1x free-ip** command.
GigabitEthernet0/0/1 state	State of an interface. ● UP: The interface is started. ● DOWN: The interface is shut down.
802.1x protocol is Enabled[mac-bypass]	802.1X authentication is enabled on the interface. To enable 802.1X authentication, run the **dot1x enable** command. To configure MAC address bypass authentication, run the **dot1x mac-bypass** command. If MAC address bypass authentication is configured, [mac-bypass] is displayed.
Port control type is Auto	The control mode on the interface is **auto** for 802.1X authentication user access. The access control modes include **auto**, **authorized-force**, and **unauthorized-force**. To set the control mode, run the **dot1x port-control** command.
Authentication mode is MAC-based	The MAC address-based authentication method is used on the interface. To set the authentication method on the interface, run the **dot1x port-method** command.
Reauthentication is disabled	802.1x user re-authentication is disabled on the interface. To enable 802.1X user re-authentication, run the **dot1x reauthenticate** command.

Item	Description
Dot1x retry times	Maximum number of times an authentication request is sent to an 802.1X user. To set the maximum number of times an authentication request is sent to an 802.1X user, run the **dot1x retry** command.
Authenticating users	Number of users who are being authenticated.
Current users	Number of current online users on the interface.
Authentication Success	Number of successful authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Failure	Number of failed authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Enter Enquence	Number of packets entering the queue.
EAPOL Packets	Number of globally EAPOL packets. ● TX: Number of sent EAPOL packets. ● RX: Number of received EAPOL packets.
Sent	Statistics of sent packet.
EAPOL Request/ Identity Packets	Number of globally EAPOL Request/Identity packets.
EAPOL Request/ Challenge Packets	Number of globally EAPOL Request/Challenge packets.
Multicast Trigger Packets	Number of multicast packets that trigger authentication.
EAPOL Success Packets	Number of globally EAPOL Success packets.
EAPOL Failure Packets	Number of globally EAPOL Failure packets.
Received	Statistics of received packet.
EAPOL Start Packets	Number of globally EAPOL Start packets.
EAPOL Logoff Packets	Number of globally EAPOL LogOff packets.
EAPOL Response/ Identity Packets	Number of globally EAPOL Response/Identity packets.

Item	Description
EAPOL Response/ Challenge Packets	Number of globally EAPOL Response/Challenge packets.
Online user(s) info	Online user information: ● UserId: User ID. ● MAC/VLAN: MAC address/VLAN ID. ● AccessTime: Access time. ● UserName: User name. ● Total: Total number of online users. ● printed: Number of displayed online users.
Dropped	Number of discarded EAP packets. ● EAPOL Access Flow Control: number of packets that are discarded because the user access rate is exceeded. ● EAPOL Check Sysmac Error: number of packets that are discarded because the device MAC address is incorrect. ● EAPOL Get Vlan ID Error: number of packets that are discarded because the obtained VLAN ID is incorrect. ● EAPOL Packet Flow Control: number of packets that are discarded because the packet access rate is exceeded. ● EAPOL Online User Reach Max: number of packets that are discarded because the number of online users reaches the maximum. ● EAPOL Static or BlackHole Mac: number of packets that are discarded because the packet MAC address is a static MAC address or blackhole MAC address. ● EAPOL Get Vlan Mac Error: number of packets that are discarded because the obtained VLAN MAC address is incorrect. ● EAPOL Temp User Exist: number of packets that are discarded because the temporary user exists. ● EAPOL no replace dot1x: number of EAP Start packets that are discarded due to 802.1X authentication of successfully authenticated MAC or Portal users.
DHCP	DHCP packet statistics.
ARP	ARP packet statistics.
ND	ND packet statistics.
DHCPv6	DHCPv6 packet statistics.
ANYL2	Any Layer 2 packet statistics.

Item	Description
Processed Packet	Number of processed packets.
Dropped Packet	Number of discarded packets.
Authentication Request	Number of authentication request messages.
Cut Request	Number of logout request messages.
Cut Command Ack	Number of acknowledgment messages to logout command request messages.
Authentication Ack Fail Aff	Number of the user is disconnected after the wireless user authentication fails.
Update Ip	Number of IP address update messages.
Wlan Eap Authentication Request	Number of EAP authentication request messages initiated by the WLAN module.
Wlan Eap Authentication Request Ack	Number of acknowledgment messages to EAP authentication request messages initiated by the WLAN module.
Wlan Eap Send Pmk	Number of PMK messages sent when the WLAN module performs EAP authentication.
Wlan Eap Reauthenticate Send Pmk	Number of PMK messages sent when the WLAN module performs EAP re-authentication.
Update User Online Time	Number of the user online time is updated.
Authentication Ack	Number of authentication acknowledgment messages.
Reauthenticate Command	Number of re-authentication messages.
Cut Command	Number of logout command request messages.
Cut Ack	Number of acknowledgment messages to logout request messages.
Sam Nac Ack	Number of EAP messages replied by the SAM module.
Notify Server Up	Number of RADIUS server Up messages.
Wlan Mac Authentication Request	Number of MAC authentication request messages initiated by the WLAN module.
Notify Vlanif Mac Authentication	Number of MAC authentication request messages of a VLANIF interface.

13.6.43 display dot1x quiet-user

Function

The **display dot1x quiet-user** command displays information about 802.1X authentication users who are quieted.

Format

display dot1x quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all 802.1X authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a quiet 802.1X authentication user with a specified MAC address.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about 802.1X authentication users who are quieted.

Example

Display information about all 802.1X authentication users who are quieted.

```
<HUAWEI> display dot1x quiet-user all
-------------------------------------------------------------------------------
MacAddress                  User Status              Quiet Remain Time(Sec)
-------------------------------------------------------------------------------
00e0-fc02-0003               Block                   50
-------------------------------------------------------------------------------
Total: 1  Printed: 1  Block: 1   Active: 0
```

Table 13-103 Description of the **display dot1x quiet-user all** command output

Item	Description
MacAddress	MAC address of an 802.1X authentication user who is quieted.
User Status	User status: ● Block: The user is in silent state. ● Active: The user is not in silent state.
Quiet Remain Time(Sec)	● If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. ● If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.6.44 display mac-address authen

Function

The **display mac-address authen** command displays the current authen MAC address entries in the system.

Format

display mac-address authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-

Parameter	Description	Value
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The authen MAC address entries are generated for pre-connection users or after users pass authentication. The administrator can run this command to check the existing authen or guest MAC address entries on the device. The administrator can check information about user access based on these MAC address entries to locate user access faults.

Precautions

If there are a lot of authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all authen MAC address entries in the system.

```
<HUAWEI> display mac-address authen
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                       Learned-From        Type
-------------------------------------------------------------------------------
xxxx-xxxx-xxxx 3000/-/-                          GE0/0/1             authen
xxxx-xxxx-xxx1 3000/-/-                          GE0/0/1             authen
xxxx-xxxx-xxx2 3000/-/-                          GE0/0/1             authen
-------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-104 Description of the **display mac-address authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the outbound interface belongs to.

Item	Description
Learned-From	Interface on which a MAC address is learned.
Type	Type of MAC addresses.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.6.45 display mac-address pre-authen

Function

The **display mac-address pre-authen** command displays the current pre-authen MAC address entries in the system.

Format

display mac-address pre-authen [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the existing MAC address entries of the pre-connection type to obtain access information about pre-connection users and locate faults.

Precautions

If there are a lot of pre-authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all pre-authen MAC address entries in the system.

```
<HUAWEI> display mac-address pre-authen
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                       Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc00-0100 3000/-/-                          GE0/0/1           pre-authen
00e0-fc00-0400 3000/-/-                          GE0/0/1           pre-authen
00e0-fc00-0200 3000/-/-                          GE0/0/1           pre-authen
-------------------------------------------------------------------------------
Total items displayed = 3
```

Table 13-105 Description of the **display mac-address pre-authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/VSI/BD	VLAN/VSI/BD that the outbound interface belongs to.
Learned-From	Interface on which a MAC address is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

13.6.46 display mac-authen

Function

The **display mac-authen** command displays information about MAC address authentication.

Format

display mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> | **configuration**]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays information about MAC address authentication on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. MAC address authentication information on all device interfaces is displayed if this parameter is not specified.	-
configuration	Displays the global information about MAC address authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mac-authen** command to view configuration results of all configuration commands in MAC address authentication. The command output helps you to check whether the MAC address authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

You can locate the fault according to the packet statistics that is displayed using the **display mac-authen** command. When the fault is rectified, run the **reset mac-authen statistics** command to clear the packet statistics. After a period of time, run the **display mac-authen** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

View all information about MAC address authentication.

```
<HUAWEI> display mac-authen
  MAC address authentication is Enabled.
  Username format: use MAC address without-hyphen as username
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Offline detect period is 300s
  Reauthenticate period is 1000s
  Guest user reauthenticate period is 60s
  Maximum users: 100
  Current users: 1
  Global domain is not configured
  Trigger condition: dhcp arp dhcpv6 nd

 GigabitEthernet0/0/1 state : UP. MAC address authentication is enabled
  Reauthentication is enabled
  Reauthen Period: 1000s
  Maximum users: 100
  Current users: 1
  Authentication Success: 0, Failure: 0

 Online user(s) info:
 UserId   MAC/VLAN           AccessTime              UserName
 ------------------------------------------------------------------------------
 16016    00e0-fc12-3456/2003 2014/01/26 09:22:49     wlan
 ------------------------------------------------------------------------------
 Total 1,1 printed
```

Table 13-106 Description of the **display mac-authen** command output

Item	Description
Mac address authentication is Enabled	MAC address authentication is enabled. To enable MAC address authentication, run the **mac-authen** command.

Item	Description
Username format	User name format for MAC address authentication. - use MAC address without-hyphen as username: A user name is a MAC address that does not contain hyphens (-), for example, 00e0fc123456. - use MAC address with-hyphen as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 00e0-fc12-3456. - use MAC address with-hyphen normal as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-e0-fc-12-34-56. - use MAC address without-hyphen upper as username: A user name is a MAC address in the uppercase format that does not contain hyphens (-), for example, 00E0FC123456. - use MAC address with-hyphen upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 00E0-FC12-3456. - use MAC address with-hyphen normal upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-E0-FC12-34-56. - use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every four digits, for example, 00e0:fc12:3456. - use MAC address with-hyphen normal colon as username: A user name is a MAC address that

Item	Description
	contains colons (:) and the colons are inserted between every two digits, for example, 00:e0:fc12:34:56. - use MAC address with-hyphen colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every four digits, for example, 00E0:FC12:3456. - use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every two digits, for example, 00:E0:FC12:34:56. - fixed username: The user name is fixed. - use option82 as username: The content of the Option 82 field is used as the user name. - not configured: The user name format is not configured. To configure a user name, run the **mac-authen username** command.
Quiet period	Quiet timer value, during which the user waits for re-authentication after the maximum number of authentication failures is exceeded. The default value of the quiet timer is 60 seconds. To set the quiet period, run the **mac-authen timer** command.
Authentication fail times before quiet	Maximum number of authentication failures before a MAC address authentication user enters the quiet state.
Offline detect period	Interval for detecting online users. The timer is used to periodically check whether a user is offline. The default interval is 300 seconds. To set the interval for detecting online users, run the **mac-authen timer** command.

Item	Description
Reauthenticate period is 1000s	Interval at which users are re-authenticated. The default interval is 1800 seconds. To set the re-authentication period, run the **mac-authen timer** command.
Guest user reauthenticate period is 60s	Interval at which users in a guest VLAN are re-authenticated. The default interval is 60 seconds. To set the guest VLAN user re-authentication period, run the **mac-authen timer** command.
Maximum users	Maximum number of online users allowed by the device, the value varies according to devices. To set the maximum number of MAC address authentication users on an interface, run the **mac-authen max-user** command.
Current users	Number of current online users.
Global domain	Current authentication domain. By default, no authentication domain is specified for users. If you do not specify any domain for users, the default domain in the system is used. To configure an authentication domain, run the **mac-authen domain** command.
Trigger condition	Packet type that can trigger MAC address authentication. To configure the packet type, run the **mac-authen trigger** command.
GigabitEthernet0/0/1 current state	Interface state. ● UP: The interface is started. ● DOWN: The interface is shut down.
MAC address authentication is Enabled	MAC address authentication is enabled on the interface. To enable MAC address authentication, run the **mac-authen** command.
Reauthentication is enabled	MAC address reauthentication is enabled. To enable the MAC address reauthentication, run the **mac-authen reauthenticate** command.

Item	Description
Reauthen Period	Interval at which users are re-authenticated. The default interval is 1800 seconds. To set the re-authentication period, run the **mac-authen timer reauthenticate-period** command.
Maximum users	Maximum number of MAC address authentication users on the interface. To set the maximum number of MAC address authentication users on an interface, run the **mac-authen max-user** command.
Current users	Number of current online users on the interface.
Authentication Success: 0, Failure: 0	Numbers of successful and failed authentications on the interface.
UserId	ID of an online user.
MAC/VLAN	MAC address and VLAN of a user. **NOTE** If the AAA server delivers an authorized VLAN, information about the authorized VLAN is displayed.
AccessTime	Access time of a user.
UserName	Name of a user.

13.6.47 display mac-authen quiet-user

Function

The **display mac-authen quiet-user** command displays information about MAC address authentication users who are quieted.

Format

display mac-authen quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a specified MAC address authentication user who is quieted.	The value is in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about MAC address authentication users who are quieted.

Example

Display information about all MAC address authentication users who are quieted.

```
<HUAWEI> display mac-authen quiet-user all
 ------------------------------------------------------------------------------
 MacAddress              User status                      Quiet Remain Time(Sec)
 ------------------------------------------------------------------------------
 00e0-fc02-0003           Block                          50
 ------------------------------------------------------------------------------
 Total: 1  Printed: 1  Block: 1   Active: 0
```

Table 13-107 Description of the **display mac-authen quiet-user all** command output

Item	Description
MacAddress	MAC address of a MAC address authentication user who is quieted.
User status	User status: - Block: The user is in a silent state. - Active: The user is not in a silent state.

Item	Description
Quiet Remain Time(Sec)	- If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. - If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.

13.6.48 display port connection-type access all

Function

The **display port connection-type access all** command displays all current downlink interfaces on the device.

Format

display port connection-type access all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check all current downlink interfaces on the device.

Example

Display all current downlink interfaces on the device.

```
<HUAWEI> display port connection-type access all
Slot 0:
GigabitEthernet0/0/1      GigabitEthernet0/0/2      GigabitEthernet0/0/3
GigabitEthernet0/0/4      GigabitEthernet0/0/5      GigabitEthernet0/0/6
GigabitEthernet0/0/7      GigabitEthernet0/0/8      GigabitEthernet0/0/9
GigabitEthernet0/0/10     GigabitEthernet0/0/11     GigabitEthernet0/0/12
GigabitEthernet0/0/13     GigabitEthernet0/0/14     GigabitEthernet0/0/15
GigabitEthernet0/0/16     GigabitEthernet0/0/17     GigabitEthernet0/0/18
GigabitEthernet0/0/19     GigabitEthernet0/0/20     GigabitEthernet0/0/21
GigabitEthernet0/0/22     GigabitEthernet0/0/23     GigabitEthernet0/0/24
```

Table 13-108 Description of the display port connection-type access all command output

Item	Description
Slot 0	Slot ID.
GigabitEthernet0/0/1	Interface name.

13.6.49 display portal

Function

The **display portal** command displays the Portal authentication configuration.

Format

display portal [**interface** *interface-type interface-number* | **configuration**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays Portal authentication configuration on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. Portal authentication configuration in the system view or on all interfaces is displayed if this parameter is not specified.	-
configuration	Displays the global Portal authentication configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal** command to view the Portal authentication configuration and check whether the configuration is correct.

Example

Display the Portal authentication configuration.

```
<HUAWEI> display portal
 Portal timer offline-detect length:500
 Portal max-user number:100
 Quiet function is Disabled
 Different-server is Disabled
 Parameter set: Quiet Period      60s   Quiet-times         3
 Logout packets resend: Resend-times 3  Timeout 5s
 Portal user(s) on slot 0:1

 Vlanif10 protocol status: up, web-auth-server layer2(direct)
   Portal domain: tsm
   Auth-network:
       10.3.3.3          255.255.255.255
       10.8.0.0          255.255.0.0
```

Display the Portal authentication configuration on VLANIF10.

```
<HUAWEI> display portal interface vlanif 10

 Vlanif10 protocol status: up, web-auth-server layer2(direct)
    Portal domain: tsm
    Auth-network:
       10.3.3.3          255.255.255.255
       10.8.0.0          255.255.0.0
```

Table 13-109 Description of the **display portal** command output

Item	Description
Portal timer offline-detect length	Portal authentication user offline detection interval. To set the user offline detection interval, run the **portal timer offline-detect** command.
Portal max-user number	Maximum number of concurrent Portal authentication users allowed to access the device, the value varies according to device models. To set the maximum number of concurrent Portal authentication users allowed to access the device, run the **portal max-user** command.
Quiet function is Enabled or Quiet function is Disabled	Whether the quiet function in Portal authentication is enabled. ● Enabled ● Disabled To enable the quiet function, run the **portal quiet-period** command.

Item	Description
Different-server is Enabled or Different-server is Disabled	Whether a device is enabled to process user logout requests sent by a Portal server other than the one from which users log in: ● Enabled ● Disabled To configure a device to process user logout requests sent by a Portal server other than the one from which users log in, command, run the **portal logout different-server enable** command.
Parameter set	Parameter settings of the quiet function in Portal authentication. ● Quiet Period: indicates the quiet period in Portal authentication. To set the quiet period in Portal authentication, run the **portal timer quiet-period** command. ● Quiet-times: indicates the maximum number of authentication failures within 60 seconds before a Portal authentication user enters the quiet state. To set the maximum number of authentication failures, run the **portal quiet-times** command.
Logout packets resend	Configuration of the logout packet re-transmission function for Portal authentication users. ● Resend-times: indicates the number of re-transmission times for Portal authentication user logout packets. ● Timeout: indicates the re-transmission interval of Portal authentication user logout packets. To set the re-transmission interval, run the **portal logout resend timeout** command.

Item	Description
Portal user(s) on slot 0	Statistics on Portal authentication users on the device. **NOTE** This parameter is unavailable when no Portal authentication user is online. When Portal authentication users go online through an Eth-Trunk, the number of Portal authentication users on the device where Eth-Trunk member interfaces are located is the same as the actual number of Portal authentication users on the device.
Vlanif10 protocol status	Link layer protocol state of the VLANIF interface. ● up: indicates that the interface is running properly. ● down: indicates that the interface is disabled. ● web-auth-server layer2(direct): indicates that the authentication mode is set to Layer 2 Portal authentication on a specified interface.
Portal domain	Name of a forcible Portal authentication domain. To set a forcible Portal authentication domain, run the **portal domain** command.
Auth-network	Portal authentication subnet. To set the Portal authentication subnet, run the **portal auth-network** command.

13.6.50 display portal free-rule

Function

The **display portal free-rule** command displays authentication-free rules for Portal authentication users.

Format

display portal free-rule [*rule-id*]

Parameters

Parameter	Description	Value
rule-id	Displays the ID of an authentication-free rule. If the rule ID is not specified, the configuration of all authentication-free rules is displayed.	The value is an integer of which the range depends on product models.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display portal free-rule** command shows the configuration of authentication-free rules. You can locate faults according to the command output.

Example

Display the configuration of authentication-free rules.

```
<HUAWEI> display portal free-rule
portal free-rule 0 destination ip 10.1.1.1 mask 255.255.255.255
portal free-rule 10 destination ip 10.1.1.2 mask 255.255.255.255
Total 2 free-rules
```

Display the configuration of authentication-free rule 10.

```
<HUAWEI> display portal free-rule 10
portal free-rule 10 destination ip 10.1.1.1 mask 255.255.255.255
```

13.6.51 display portal https-redirect blacklist

Function

The **display portal https-redirect blacklist** command displays IPv4 addresses in the HTTPS redirection blacklist.

The **display portal https-redirect ipv6 blacklist** command displays IPv6 addresses in the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect blacklist

display portal https-redirect ipv6 blacklist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection blacklist are correct.

Example

Display IPv4 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect blacklist
--------------------------------------
IP Address        Aging Time
--------------------------------------
 10.1.1.1         2018-06-26 21:01:59
--------------------------------------
 Total:1   Print:1
```

Display IPv6 addresses in the HTTPS redirection blacklist.

```
<HUAWEI> display portal https-redirect ipv6 blacklist
--------------------------------------------------------------
IPv6 Address                          Aging Time
--------------------------------------------------------------
FC00::1                               2019-02-23 09:47:05
--------------------------------------------------------------
 Total:1   Print:1
```

Table 13-110 Description of the **display portal https-redirect blacklist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the blacklist, which is configured using the **portal https-redirect blacklist** command or is added after the condition specified by the **portal https-redirect blacklist packet-rate** or **portal https-redirect blacklist retry-times interval** command is met.

Item	Description
Aging Time	Time when an address in the blacklist is aged out (that is, time when an address is removed from the blacklist). You can run the **portal https-redirect blacklist aging-time** command to configure the aging time of addresses in the blacklist.
Total:*m* Print:*n*	Total number of addresses in the blacklist, and number of addresses displayed.

13.6.52 display portal https-redirect whitelist

Function

The **display portal https-redirect whitelist** command displays IPv4 addresses in the HTTPS redirection whitelist.

The **display portal https-redirect ipv6 whitelist** command displays IPv6 addresses in the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

display portal https-redirect whitelist

display portal https-redirect ipv6 whitelist

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check whether the addresses in the HTTPS redirection whitelist are correct.

Example

Display IPv4 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect whitelist
IP Address:
-------------------------------
 10.1.2.1
-------------------------------
 Total:1   Print:1
```

Display IPv6 addresses in the HTTPS redirection whitelist.

```
<HUAWEI> display portal https-redirect ipv6 whitelist
IPv6 Address:
----------------------------------------------------------------
FC00::2
----------------------------------------------------------------
 Total:1   Print:1
```

Table 13-111 Description of the **display portal https-redirect whitelist** command output

Item	Description
IP Address/IPv6 Address	IPv4/IPv6 addresses in the whitelist, which are configured using the **portal https-redirect whitelist** command.
Total:*m* Print:*n*	Total number of addresses in the whitelist, and number of addresses displayed.

13.6.53 display portal quiet-user

Function

The **display portal quiet-user** command displays information about Portal authentication users in quiet state.

Format

display portal quiet-user { **all** | **server-ip** *ip-address* | **user-ip** { *ip-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Displays information about all Portal authentication users in quiet state.	-

Parameter	Description	Value
user-ip *ip-address*	Displays information about the quiet user with the specified IP address.	The value is in dotted decimal notation.
user-ip *ipv6-address*	Displays information about the quiet user with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
server-ip *ip-address*	Displays information about all the users in quiet state authenticated by the Portal authentication server with a specified IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the quiet timer is enabled, you can run the **display portal quiet-user** command to view information about Portal authentication users in quiet state.

Example

Display information about all Portal authentication users in quiet state.

```
<HUAWEI> display portal quiet-user all
Quiet IP information
------------------------------------------------------------------------------------
Quiet ip                  User status                  Quiet Remain Time(Sec)
------------------------------------------------------------------------------------
192.168.1.1               Active                    10
192.168.1.2               Block                     20
------------------------------------------------------------------------------------
Total: 2  Printed: 2  Block: 1   Active: 1
```

Display information about the user in quiet state at 192.168.1.1.

```
<HUAWEI> display portal quiet-user user-ip 192.168.1.1
  Quiet remain seconds: 50
  User Status: Active
```

Table 13-112 Description of the **display portal quiet-user** command output

Item	Description
Quiet IP information	Information about the user in quiet state.

Item	Description
Quiet ip	IP address of the user in quiet state.
User status	User status: - Block: The user is in silent state. - Active: The user is not in silent state. Currently, only users in silent state can be displayed.
Quiet Remain Time(Sec)	- If the user is in block state, this field indicates the remaining quiet period of the user, in seconds. - If the user is in active state, this field indicates the remaining period before the user transitions to the quiet state, in seconds.
Quiet remain seconds	Remaining quiet period of the user in quiet state, in seconds.

13.6.54 display portal user-logout

Function

The **display portal user-logout** command displays temporary logout entries of Portal authentication users.

Format

display portal user-logout [**ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Displays temporary logout entries of the Portal authentication user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays temporary logout entries of the Portal authentication user with a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device records temporary entries after Portal authentication users are disconnected. The network administrator can run this command to check temporary logout entries to locate faults.

If the parameter **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] is not specified, the temporary logout entries of all Portal authentication users are displayed.

Example

Display the temporary logout entries of all Portal authentication users.

```
<HUAWEI> display portal user-logout
 ----------------------------------------------------------------
 UserIP           Vrf      Resend Times TableID
 ----------------------------------------------------------------
 192.168.111.100  1        3            0
 ----------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-113 Description of the **display portal user-logout** command output

Item	Description
UserIP	IP address of the Portal authentication user.
Vrf	VPN instance that the Portal authentication user belongs to.
Resend Times	Number of logout packet re-transmission times. To set the number of logout packet re-transmission times, run the **portal logout resend timeout** command.
TableID	Index of the temporary logout entry.
Total: *m*, printed: *n*	Total number of temporary logout entries and number of displayed entries.

13.6.55 display portal url-encode configuration

Function

The **display portal url-encode configuration** command displays the configuration of URL encoding and decoding.

Format

display portal url-encode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring URL encoding and decoding, you can run the **display portal url-encode configuration** command to check the configuration.

Example

Display the configuration of URL encoding and decoding.

```
<HUAWEI> display portal url-encode configuration
  Portal URL Encode : Disable
```

Table 13-114 Description of the **display portal url-encode configuration** command output

Item	Description
Portal URL Encode	Whether URL encoding and decoding are enabled: ● Disable ● Enable To configure the function, run the **portal url-encode enable** command.

13.6.56 display server-detect state

Function

The **display server-detect state** command displays the status of a Portal server.

Format

display server-detect state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server template. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server template name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

ou can run the **display server-detect state** command to check information about the Portal server status.

Example

Display information about the Portal server status configured in the Portal server template **abc**.

```
<HUAWEI> display server-detect state web-auth-server abc
 Web-auth-server     :    abc
 Total-servers       :    4
 Live-servers        :    1
 Critical-num        :    0
 Status              :    Normal
 Ip-address               Status
 192.168.2.1              UP
 192.168.2.2              DOWN
 192.168.2.3              DOWN
 192.168.2.4              DOWN
```

Table 13-115 Description of the **display server-detect state** command output

Item	Description
Web-auth-server	Name of the Portal server template.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than this value, enable the survival function in the corresponding Portal server template view.
Status	Status of the Portal server. The values are as follows: ● Normal: normal state ● Abnormal: indicates that the Portal server is in abnormal state ● Permit-all: survival state
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: ● UP: reachable ● DOWN: unreachable

13.6.57 display static-user

Function

The **display static-user** command displays static user information.

Format

display static-user [**domain-name** *domain-name* | **interface** *interface-type interface-number* | **ip-address** *start-ip-address* [*end-ip-address*] | **vpn-instance** *vpn-instance-name*] * [**detail**]

Parameters

Parameter	Description	Value
domain-name *domain-name*	Displays static user information in a specified domain.	The value is a string of 1 to 64 case-sensitive characters without spaces, asterisk (*), question mark (?), and double quotation marks ("). The value cannot be - or --.
interface *interface-type interface-number*	Displays static user information on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ip-address *start-ip-address* [*end-ip-address*]	Displays static user information in a specified IP address range.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays static user information in a specified VPN instance.	The value must be an existing VPN instance name.
detail	Displays detailed information about static users.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a static user is configured, you can run the **display static-user** command to view the static user information.

Example

Display information about all static users configured.

```
<HUAWEI> display static-user
 Not-update-ip enable status: No
 IP-address       Interface       MAC-address    VPN
-----------------------------------------------------------------------------
 10.1.1.1         GE0/0/3         -              -
 10.1.1.2         GE0/0/3         -              -
 10.1.1.3         GE0/0/3         -              -
 10.1.1.5         GE0/0/5         00e0-fc12-3456 -
 10.1.1.6         GE0/0/5         00e0-fc12-3456 -
 10.1.1.7         GE0/0/5         00e0-fc12-3456 -
 10.1.1.8         GE0/0/5         00e0-fc12-3456 -
 10.1.1.10        -               00e0-fc12-3478 -
 10.1.1.11        -               00e0-fc12-3478 -
 10.1.1.12        -               00e0-fc12-3478 -
-----------------------------------------------------------------------------
Total item(s) displayed = 10
```

Display detailed information about all static users.

```
<HUAWEI> display static-user detail
 Not-update-ip enable status: No
-----------------------------------------------------------------------------
  IP address                      : 10.1.1.2
  IP static user                  : Yes
  Vpn-instance                    : -
  Domain-name                     : local
  Interface                       : -
  MAC address                     : -
  VLAN                            : 10
  Detect                          : Disable
  Keep-online                     : Disable
-----------------------------------------------------------------------------
  IP address                      : 10.1.1.4
  IP static user                  : Yes
  Vpn-instance                    : -
  Domain-name                     : -
  Interface                       : -
  MAC address                     : -
  VLAN                            : 10
  Detect                          : Disable
  Keep-online                     : Enable
-----------------------------------------------------------------------------
Total item(s) number= 2, displayed number= 2

Ip-static-user enable status:
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Total item(s) number= 0, displayed number= 0
```

Table 13-116 Description of the **display static-user** command output

Item	Description
Not-update-ip enable status	Whether the device is disabled from updating IP addresses of static users: - Yes - No
IP-address/IP address	IP address of a static user.
Interface	Interface connected to a static user.
MAC-address/MAC address	MAC address of a static user.

Item	Description
VPN/Vpn-instance	VPN instance to which a static user belongs.
Total item(s) number= *m*, displayed number= *n*	The total number of entries is *m* and the number of displayed entries is *n*.
Ip-static-user enable status	Whether the function of identifying static users through IP addresses is enabled.
IP static user	Whether the user is a static user: ● Yes ● No
Domain-name	Domain to which a static user belongs.
VLAN	VLAN to which a static user belongs.
Detect	Whether the device is enabled to send ARP packets to trigger MAC address authentication for offline static users: ● Enable ● Disable
Keep-online	Whether a static user is kept online, with offline detection not performed. ● Enable ● Disable

13.6.58 display url-template

Function

The **display url-template** command displays information about URL templates.

Format

display url-template { **all** | **name** *template-name* }

Parameters

Parameter	Description	Value
all	Displays information about all configured URL templates.	-

Parameter	Description	Value
name *template-name*	Displays information about the URL template with a specified name.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a URL template is configured, run the **display url-template** command to view information about the URL template.

Example

Display information about all configured URL templates.

```
<HUAWEI> display url-template all
-------------------------------------------------------------------------------
 Index    Name                          URL     Start  Assignment  Isolate
                                     Number  Mark   Mark        Mark
-------------------------------------------------------------------------------
 0        test                         0       ?      =          &
 1        test2                         0       ?      =          &
-------------------------------------------------------------------------------
 Total 2
```

Display information about the URL template **test**.

```
<HUAWEI> display url-template name test
 Name : test
 URL  :
   1. http://10.1.1.1
 Start mark      : !
 Assignment mark : j
 Isolate mark    : =
 User MAC        :
 Redirect URL    :
 User IP address :
 Sysname         :
 Delimiter       : %
 Format          : normal    Login URL Key   : logiurl   Login URL       : http:\\example.com
```

Table 13-117 Description of the **display url-template** command output

Item	Description
Index	Index of a URL template.
Name	Name of a URL template.
URL	URL of the Portal server. For details, see **url**.
Start mark	Start character in the URL address. For details, see **parameter**.
Assignment mark	Assignment character in the URL address. For details, see **parameter**.
Isolate mark	Delimiter between URL addresses. For details, see **parameter**.
User MAC	MAC address of a user. For details, see **url-parameter**.
Redirect URL	URL in the original user packet. For details, see **url-parameter**.
User IP address	User IP address. For details, see **url-parameter**.
Sysname	Device name. For details, see **url-parameter**.
Delimiter	Delimiter between MAC addresses in URL. For details, see **url-parameter mac-address format**.
Format	Format MAC addresses in URL. For details, see **url-parameter mac-address format**.
Login URL Key	Identification keyword for the login URL sent to the Portal server during redirection. For details, see **url-parameter**.
Login URL	Device login URL. For details, see **url-parameter**.

13.6.59 display user-group

Function

The **display user-group** command displays the configuration of a user group.

Format

display user-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified user group. The configurations of all user groups are displayed if this parameter is not specified.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display user-group** command to obtain the user group configuration and locate faults according to the command output.

Example

Display the configuration of all user groups.

```
<HUAWEI> display user-group
 ------------------------------------------------------------------------------
 ID    Group name                    Rule-num   User-num  Status
 ------------------------------------------------------------------------------
 0     abc                        0          0         disabled
 ------------------------------------------------------------------------------
 Total 1
```

NOTE

When the length of **Group name** exceeds 14 characters, the name is displayed in abridged mode.

Display the configuration about the user group **abc**.

```
<HUAWEI> display user-group abc
  User group ID           : 0   Group name             : abc   ACL ID                  :   ACL rule number         : 0
User-num                : 0   VLAN                    :   Remark dscp             :   Remark 8021p            :
Status                  : disabled
```

Table 13-118 Description of the **display user-group** command output

Item	Description
ID	ID of the user group.
Rule-num	Number of ACL rules.
User group ID	ID of the user group.
Group name	Name of the user group.
ACL ID	ID of the ACL bound to the user group. To set the ACL ID, run the **acl-id** command.
ACL rule number	Number of ACL rules.
User-num	Number of online users bound to the user group.
VLAN	VLAN of the user group. To set the VLAN, run the **user-vlan** command.
Remark dscp	Priorities for processing IP packets. To set the priorities, run the **remark** command.
Remark 8021p	Priorities for processing Ethernet Layer 2 packets. To set the priorities, run the **remark** command.
Status	Status of the user group. ● disabled: The user group is disabled. ● enabled: The user group is enabled.

13.6.60 display web-auth-server configuration

Function

The **display web-auth-server configuration** command displays the Portal server configuration.

Format

display web-auth-server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Portal server template is configured, the **display web-auth-server configuration** displays the Portal server configuration.

Example

Display the Portal server configuration.

```
<HUAWEI> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled
 ------------------------------------------------------------------------------
   Enabled protocol      : https
   Listening port        : 8443
   SSL policy            : default_policy
------------------------------------------------------------------------------
  Web-auth-server Name : test
  Web-auth-server Index: 0
  IP-address           :
  IPv6 Address         :
  Shared-key           :
  Source-IP            : -
  Port / PortFlag      : 50100 / NO
  URL                  : https://192.168.2.10:8443/webauth
  URL Template         :
  URL Template ParaName:
  URL Template IVName  :
  URL Template Key     :
  Redirection          : Enable
  Sync                 : Disable
  Sync Seconds         : 300
  Sync Max-times       : 3
  Detect               : Disable
  Detect Seconds       : 60
  Detect Max-times     : 3
  Detect Critical-num  : 0
  Detect Action        :
  Detect Type          : portal
  VPN Instance         :
  Bound Vlanif         :
  Bound Interface      :
  Protocol             : http
  Http Get-method      : disable
  Password Encrypt     : none
  Cmd ParseKey         : cmd
  Username ParseKey    : username
  Password ParseKey    : password
  MAC Address ParseKey : macaddress
  IP Address ParseKey  : ipaddress
  Initial URL ParseKey : initurl
  Login Cmd            : login
  Logout Cmd           : logout
  Login Success
       Reply Type      : redirect initial URL
       Redirect URL    :
```

```
    Message        : LoginSuccess!
Login Fail
    Reply Type     : redirect login URL
    Redirect URL   :
    Message        : LoginFail!
Logout Success
    Reply Type     : message
    Redirect URL   :
    Message        : LogoutSuccess!
Logout Fail
    Reply Type     : message
    Redirect URL   :
    Message        : LogoutFail!
-------------------------------------------------------------------------------
 1 Web authentication server(s) in total
```

Table 13-119 Description of the **display web-auth-server configuration** command output

Item	Description
Listening port	Listening port for Portal protocol packets. To configure a listening port, run the **web-auth-server listening-port** command.
Portal	Portal protocol version. ● version 1, version 2: The device supports both the versions V1.0 and V2.0. ● version 2: The device supports the versions V2.0. To configure the Portal protocol version, run the **web-auth-server version** command.
Include reply message	Whether the packets sent from the device to the Portal server contain authentication responses. ● enabled ● disabled To enable the device to transparently transmit authentication responses of users sent by the authentication server to the Portal server, run the **web-auth-server reply-message** command.
Enabled protocol	Enabled HTTP or HTTPS protocol. ● http ● https To enable the HTTP or HTTPS protocol, run the **portal web-authen-server** command.

Item	Description
Listening port	HTTP or HTTPS port number. To configure the HTTP or HTTPS port number, run the **portal web-authen-server** command.
SSL policy	SSL policy referenced by the HTTPS protocol. To configure the SSL policy referenced by the HTTPS protocol, run the **portal web-authen-server** command.
Web-auth-server Name	Name of the Portal server template. To configure the Portal server template name, run the **web-auth-server** command.
Web-auth-server Index	Index of the Portal server template.
IP-address	IPv4 address of the Portal server. To configure the IP address of the Portal server, run the **server-ip** command.
IPv6 Address	IPv6 address of the Portal server. To configure the IP address of the Portal server, run the **server-ip** command.
Shared-key	Shared key of the Portal server. To configure the shared key of the Portal server, run the **shared-key** command.
Source-IP	IP address used for communication with the Portal server. To configure the IP address used for communication with the Portal server, run the **source-ip** command.
Port / PortFlag	● Port: indicates the port number of the Portal server. ● PortFlag: indicates whether packets are always sent through this port. To configure the port number of the Portal server, run the **port** command.
URL	URL of the Portal server. To configure the URL of the Portal server, run the **url** command.

Item	Description
URL Template	URL template bound to the Portal server template. To configure the URL template, run the **url-template** command.
Redirection	Redirection status of Portal authentication. ● Disable: Redirection of Portal authentication is disabled. ● Enable: Redirection of Portal authentication is enabled. To configure redirection of Portal authentication, run the **web-redirection disable** command.
Sync	User information synchronization. ● Disable ● Enable To enable user information synchronization, run the **user-sync** command.
Sync Seconds	User information synchronization interval. To set the user information synchronization interval, run the **user-sync** command.
Sync max-times	Maximum number of times that user information synchronization fails. To set the maximum number of times that user information synchronization fails, run the **user-sync** command.
Detect	Portal server detection and keepalive functions. ● Disable ● Enable To configure Portal server detection and keepalive functions, run the **server-detect** command.
Detect Seconds	Detection interval of the Portal server. To set the detection interval of the Portal server, run the **server-detect** command.
Detect max-times	Maximum number of detection failures. To set the maximum number of detection failures, run the **server-detect** command.

Item	Description
Detect Critical-num	Minimum number of Portal servers in Up state. If the number of running Portal servers is less than the minimum, enable the survival function in the corresponding Portal server template view. To configure this function, run the **server-detect** command.
Detect Action	Action taken after the number of detection failures exceeds the maximum. ● log: The device sends logs after the number of detection failures exceeds the maximum. ● trap: The device sends traps after the number of detection failures exceeds the maximum. ● permit-all: Portal authentication on the interface is disabled after the number of detection failures exceeds the maximum. To configure an action taken after the number of detection failures exceeds the maximum, run the **server-detect** command.
Detect Type	Portal server detection mode. ● Portal: Portal-based Portal server detection mode ● HTTP: HTTP-based Portal server detection mode
Bound Vlanif	VLANIF interface to which the Portal server template is bound. To bind the Portal server template to a VLANIF interface, run the **web-auth-server (Portal access profile view)**.
VPN instance	VPN instance used for Portal authentication. To configure a VPN instance, run the **vpn-instance** command.
Bound Interface	Ethernet interface or Eth-Trunk to which the Portal server template is bound. To bind the Portal server template to an Ethernet interface or Eth-Trunk, run the **web-auth-server (Portal access profile view)** command.

Item	Description
Http Get-method	Whether users submit user name and password information to the device in GET mode: ● disable: GET mode is not used. ● enable: GET mode is used. To configure the GET mode, run the **http get-method enable** command.
Protocol	Protocol used in Portal authentication. ● portal ● http To configure the protocol used in Portal authentication, run the **protocol** command.
Password Encrypt	Password encoding mode: ● none: The password is not encoded. ● uam: The password is encoded using ASCII character. To configure the password encoding mode, run the **protocol** command.
Cmd ParseKey	Command identification keyword. To configure the command identification keyword, run the **http-method post** command.
Username ParseKey	User name identification keyword. To configure the user name identification keyword, run the **http-method post** command.
Password ParseKey	User password identification keyword. To configure the user password identification keyword, run the **http-method post** command.
MAC Address ParseKey	User MAC address identification keyword. To configure the user MAC address identification keyword, run the **http-method post** command.
IP Address ParseKey	User IP address identification keyword. To configure the user IP address identification keyword, run the **http-method post** command.

Item	Description
Initial URL ParseKey	User initial login URL identification keyword. To configure the user initial login URL identification keyword, run the **http-method post** command.
Login Cmd	User login identification keyword. To configure the user login identification keyword, run the **http-method post** command.
Logout Cmd	User logout identification keyword. To configure the user logout identification keyword, run the **http-method post** command.
Login Success	User login success.
Reply Type	Redirection response type. ● redirect initial URL: A user is redirected to the initial login URL after successful login. ● redirect login URL: A user is redirected to the login URL after a login failure. ● message: specifies the displayed message. ● redirect URL: A user is redirected to a specified URL. To configure the redirection response type, run the **http-method post** command.
Redirect URL	Redirect URL. To configure the redirect URL, run the **http-method post** command.
Message	Displayed message. To configure the displayed message, run the **http-method post** command.
Login Fail	User login failure.
Logout Success	User logout success.
Logout Fail	User logout failure.

13.6.61 device-sensor dhcp option

Function

The **device-sensor dhcp option** command enables the DHCP-based terminal type awareness function.

The **undo device-sensor dhcp option** command disables the DHCP-based terminal type awareness function.

By default, the DHCP-based terminal type awareness function is disabled.

Format

device-sensor dhcp option *option-code* &<1-6>

undo device-sensor dhcp option *option-code* &<1-6>

Parameters

Parameter	Description	Value
option-code	Specifies the DHCP option field that the device needs to resolve. The option fields in a DHCP packet carry the control information and parameters, for example, terminal type.	The value is an integer that ranges from 1 to 254.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

After the DHCP-based terminal type awareness function is enabled, the device can resolve the option fields that carry terminal type information in the received DHCP Request packets. The device then sends the option information to the RADIUS server through RADIUS accounting packets. Through the option information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- To make this command take effect, you must run the **dhcp snooping enable** command on the interfaces or in VLANs.

Example

Set the option fields to be resolved by the device to option 60.

```
<HUAWEI> system-view
[HUAWEI] device-sensor dhcp option 60
```

13.6.62 device-sensor lldp tlv

Function

The **device-sensor lldp tlv** command enables the LLDP-based terminal type awareness function.

The **undo device-sensor lldp tlv** command disables the LLDP-based terminal type awareness function.

By default, the LLDP-based terminal type awareness function is disabled.

Format

device-sensor lldp tlv *tlv-type* &<1-4>

undo device-sensor lldp tlv

Parameters

Parameter	Description	Value
tlv-type	Specifies the LLDP TLV type as the terminal type to be aware of the device.	The value is an integer that can be 1, 2, 5, 6, 7, 8, and 127. The values are as follows: ● 1: Chassis ID TLV, indicating the bridge MAC address of the device ● 2: Port ID TLV, indicating the port identifying the LLD PDU sending end ● 5: System Name TLV, indicating the device name ● 6: System Description TLV, indicating the system description ● 7: System Capabilities TLV, indicating the system capabilities ● 8: Management Address TLV, indicating the management address ● 127: Organization Specific TLV, indicating the user-defined organization information. You can run the **lldp tlv-enable med-tlv** command on the physical interface for user access to set this parameter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device usually connects to many types of terminals. You may need to assign different network access rights or packet processing priorities to the terminals of different types. For example, the voice devices, such as IP phones, should be assigned a high packet processing priority because voice signals require low delay and jitter.

Using the LLDP-based terminal type awareness function, the device parses the required TLV type containing terminal type information from the received LLDP packets. The device then sends the TLV type information to the RADIUS server through a RADIUS accounting packet. Through the TLV type information, the RADIUS server knows the terminal types and controls the network access rights and packet processing priorities of the terminals.

Precautions

- The command takes effect only when the authentication or accounting mode in the AAA scheme is RADIUS.
- The command takes effect only when the LLDP function is enabled on the device and the connected peer device.

Example

Enable the terminal type awareness function based on LLDP TLV type 5.

```
<HUAWEI> system-view
[HUAWEI] device-sensor lldp tlv 5
```

13.6.63 dot1x authentication-method

Function

The **dot1x authentication-method** command sets the authentication mode for 802.1X users.

The **undo dot1x authentication-method** command restores the default authentication mode for 802.1X users.

By default, the global 802.1X user authentication mode is CHAP authentication and the 802.1X user authentication mode on interfaces is the same as the mode globally configured.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the CHAP-based EAP termination authentication mode.	-
pap	Indicates the PAP-based EAP termination authentication mode.	-
eap	Indicates that the EAP relay mode.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the RADIUS packet to the RADIUS server for authentication. In EAP termination authentication mode, the device and RADIUS server exchange information using PAP or CHAP.
  - PAP: The device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
  - CHAP: The device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.

  After the device directly parses EAP packets, user information in the EAP packets is authenticated by a local AAA module, or sent to the RADIUS or HWTACACS server for authentication.
- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server, but does not parse the received EAP packets that include user authentication information. This mechanism is called EAP over Radius (EAPOR).

The EAP relay mechanism requires that the RADIUS server be capable of parsing a lot of EAP packets and carrying out authentication; therefore, if the RADIUS server has high processing capabilities, the EAP relay is used. If the RADIUS server is incapable of parsing a lot of EAP packets and carrying out authentication, EAP termination is recommended, and the device helps the RADIUS server to parse EAP packets.

NOTE

- The authentication mode can be set to EAP relay for 802.1X authentication users only when the RADIUS authentication is used.
- If the 802.1X client uses the MD5 encryption mode, the user authentication mode on the device can be set to EAP or CHAP; if the 802.1X client uses the PEAP authentication mode, the authentication mode on the device can be set to EAP.

Example

Set the authentication mode to EAP for 802.1X users in the device in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x authentication-method eap
```

Set the authentication mode to EAP for 802.1X users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x authentication-method eap
```

13.6.64 dot1x dhcp-trigger

Function

The **dot1x dhcp-trigger** command enables DHCP-triggered 802.1X authentication.

The **undo dot1x dhcp-trigger** command disables DHCP-triggered 802.1X authentication.

By default, DHCP-triggered 802.1X authentication is disabled.

Format

dot1x dhcp-trigger

undo dot1x dhcp-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP-triggered 802.1X authentication is enabled using the **dot1x dhcp-trigger** command, the device sends an 802.1X authentication-start packet to the user when receiving a DHCP Request message from the user. When the user receives the 802.1X authentication-start packet from the device, the 802.1X authentication page is displayed on the client device and prompts the user to enter the user name and password for authentication. During 802.1X network deployment, DHCP-triggered 802.1X authentication enables 802.1X users to start 802.1X authentication without dial-up using the client software, which facilitates network deployment.

NOTE

After receiving the request packet from an 802.1X user, the device starts authenticating the user. If the user is authenticated, the device allocates an IP address to the user through a DHCP server; if the user fails the authentication, the user cannot obtain a dynamic IP address from the DHCP server.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

The **dot1x dhcp-trigger** command can be used only when the client supports DHCP and 802.1X authentication.

Example

Enable DHCP-triggered 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x dhcp-trigger
```

13.6.65 dot1x domain

Function

The **dot1x domain** command configures a forcible domain for 802.1X authentication users.

The **undo dot1x domain** command restores the default setting of a forcible domain for 802.1X authentication users.

By default, no forcible domain is configured for 802.1X authentication users.

Format

dot1x domain *domain-name*

undo dot1x domain

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a forcible domain.	The value must be an existing domain name on the device.

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During authentication, if the user name entered by a user does not contain a domain name, the user will be authenticated in the default domain; if the user name contains a domain name, the user will be authenticated in the specified domain.

If the user names entered by many users do not contain domain names, excess users are authenticated in the default domain, making the authentication scheme inflexible. If all users on an interface need to use the same AAA scheme when the user names entered by some users contain domain name and those entered by other users do not, the device also cannot meet such requirement. To address this issue, you can configure a forcible domain. Then all users on the interface will be authenticated in the forcible domain no matter whether the user names entered by the users contain domain names.

Prerequisites

A domain has been created using the **domain** command.

Example

Configure the forcible domain **test** for 802.1X authentication users on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] quit
[HUAWEI-aaa] quit
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x domain test
```

13.6.66 dot1x eap-notify-packet

Function

The **dot1x eap-notify-packet** command enables the device to send an EAP packet code number to users.

The **undo dot1x eap-notify-packet** command disables the device from sending an EAP packet code number to users.

By default, the device is disabled from sending an EAP packet code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies an EAP packet code number sent to users.	The value is an integer that ranges from 5 to 255.
data-type *type-number*	Specifies the data type in EAP packets sent to users.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a non-Huawei device used as the RADIUS server sends RADIUS packets with attribute 61, EAP packet code number 0xa (hexadecimal notation, 10 in decimal notation), and data type 0x19 (hexadecimal notation, 25 in decimal notation) to the device, run the **dot1x eap-notify-packet** command on the device so that the device can send EAP packets with code number 0xa and data type 0x19 to users. If the **dot1x eap-notify-packet** command is not executed, the device does not process EAP packets of this type and users are disconnected.

Precautions

The device can only process EAP packets with code number 10 and data type 25.

Example

Allow the device to send EAP packets with code number 10 and data type 25 to users.

```
<HUAWEI> system-view
[HUAWEI] dot1x eap-notify-packet eap-code 10 data-type 25
```

13.6.67 dot1x enable

Function

The **dot1x enable** command enables 802.1X authentication on a device.

The **undo dot1x enable** command disables 802.1X authentication on a device.

By default, 802.1X authentication is disabled on a device.

Format

In the system view:

dot1x enable [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo dot1x enable [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

dot1x enable

undo dot1x enable

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Enables 802.1X authentication on the specified interface of the device. - *interface-type* specifies the interface type. - *interface-number1* specifies the number of the first interface. - *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. Global 802.1X authentication is enabled if this parameter is not specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IEEE 802.1X standard (802.1X for short) is a port-based network access control protocol. You can run the **dot1x enable** command to enable 802.1X authentication globally and on an interface.

To make the 802.1X configuration effective on an interface, enable the global 802.1X authentication function and perform either of the following operations:

- Run the **dot1x enable** command in the interface view.
- Run the **dot1x enable interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> command in the system view.

Precautions

- All users have been disconnected before the **undo** operation is executed.
- After the static MAC address entry is configured using the **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id* command, the user corresponding to the entry cannot pass 802.1X authentication.
- If 802.1X authentication is enabled on an interface, the following commands cannot be used on the same interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.
mac-address learning disable	Disables MAC address learning on an interface.
port link-type dot1q-tunnel	Sets the link type of an interface to QinQ.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Configures VLAN mapping on an interface.
port vlan-stacking	Configures selective QinQ.
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.

Command	Function
user-bind ip sticky-mac	Enables the device to generate snooping MAC entries.

Example

Enable 802.1X authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] dot1x enable interface gigabitethernet 0/0/1
```

Enable 802.1X authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] dot1x enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x enable
```

13.6.68 dot1x free-ip

Function

The **dot1x free-ip** command configures a free IP subnet.

The **undo dot1x free-ip** command deletes the configured free IP subnet.

By default, no free IP subnet is configured.

Format

dot1x free-ip *ip-address* { *mask-length* | *mask-address* }

undo dot1x free-ip { *ip-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies a free IP subnet.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 1 to 32.
mask-address	Specifies the mask of the IP address.	The value is in dotted decimal notation.
all	Deletes all free IP subnets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

802.1X users can access networks only after being authenticated. You can configure a free IP subnet, so that users can access network resources in the free IP subnet before being authenticated.

Precautions

- 802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.
- To ensure that pre-connection users can be aged out normally, you need to run the **dot1x timer free-ip-timeout** command to set the aging time of authentication-free user entries.
- After the free-ip function is configured, the guest VLAN, critical VLAN, and restrict VLAN are no longer effective.
- The free IP subnet takes effect only when the interface authorization state is auto.
- If a user who does not pass 802.1X authentication wants to obtain an IP address dynamically through the DHCP server, the network segment of the DHCP server needs to be configured to a free IP subnet so that the user can access the DHCP server.
- After 802.1X users go offline, they are not allowed to access network resources on free IP subnets within a specified period to prevent malicious attacks.
- After users succeed in 802.1X-based fast deployment, they can only access resources in the IP free subnets and some resources on the device.

Example

Configure 192.168.1.0/24 as a free IP subnet that users can access before they pass 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x free-ip 192.168.1.0 24
```

13.6.69 dot1x mac-bypass

Function

The **dot1x mac-bypass** command enables MAC address bypass authentication on an interface.

The **undo dot1x mac-bypass** command disables MAC address bypass authentication on an interface.

By default, MAC address bypass authentication is disabled on an interface.

Format

In the system view:

dot1x mac-bypass { **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> }

undo dot1x mac-bypass { **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> }

In the interface view:

dot1x mac-bypass

undo dot1x mac-bypass

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Enables MAC address bypass authentication on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable MAC address bypass authentication for terminals (for example, printers) on which the 802.1X client software cannot be installed or used.

After MAC address bypass authentication is enabled on the interface using the **dot1x mac-bypass** command, the device first performs 802.1X authentication on users. If the user name request times out, the device starts the MAC address authentication process for the users. When 802.1X authentication fails, the device does not start the MAC address authentication process.

NOTE

Running the **dot1x mac-bypass** command also enables 802.1X authentication on an interface, and running the **undo dot1x mac-bypass** command also disables 802.1X authentication on an interface. When you run the **dot1x mac-bypass** command on an interface that has been enabled with 802.1X authentication, the authentication mode on the interface changes to MAC address bypass authentication.

Prerequisites

802.1X authentication has been enabled globally using the **dot1x enable** command.

Example

Enable MAC address bypass authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x mac-bypass interface gigabitethernet 0/0/1
```

Enable MAC address bypass authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x mac-bypass
```

13.6.70 dot1x mac-bypass access-port

Function

The **dot1x mac-bypass access-port** command enables MAC address bypass authentication on all downlink interfaces of the device.

The **undo dot1x mac-bypass access-port** command disables MAC address bypass authentication on all downlink interfaces of the device.

By default, MAC address bypass authentication is disabled on all downlink interfaces of the device.

Format

dot1x mac-bypass access-port all

undo dot1x mac-bypass access-port all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable MAC address bypass authentication for terminals (such as printers) on which the 802.1X client software cannot be installed or used.

After MAC address bypass authentication is enabled, the device performs 802.1X authentication on a user. Once 802.1X authentication fails, the device sends the user's MAC address as the user name and password to the authentication server.

NOTE

MAC address bypass authentication involves 802.1X authentication. That is, the **dot1x mac-bypass access-port all** command also enables 802.1X authentication on the interfaces; the **undo dot1x mac-bypass access-port all** command also disables 802.1X authentication on the interfaces. If 802.1X authentication has been enabled on the interfaces, the authentication mode on the interfaces is changed to MAC address bypass authentication after you run the **dot1x mac-bypass access-port all** command.

Prerequisites

802.1X authentication has been enabled globally and on the interfaces using the **dot1x enable** command.

Example

In the system view, enable MAC address bypass authentication on all downlink interfaces of the device.

```
<HUAWEI> system-view
[HUAWEI] dot1x mac-bypass access-port all
```

13.6.71 dot1x mac-bypass mac-auth-first

Function

The **dot1x mac-bypass mac-auth-first** command enables the device to perform MAC address authentication first during MAC address bypass authentication.

The **undo dot1x mac-bypass mac-auth-first** command disables the device from performing MAC address authentication first during MAC address bypass authentication.

By default, the MAC address authentication is not performed first during MAC address bypass authentication.

Format

In the system view:

dot1x mac-bypass mac-auth-first interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x mac-bypass mac-auth-first interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x mac-bypass mac-auth-first

undo dot1x mac-bypass mac-auth-first

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Enables the device to perform MAC address authentication first on a specified interface during MAC address bypass authentication. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both the clients that do not support 802.1X authentication (such as printers) and the clients that support 802.1X authentication (such as PCs) are connected to the interface enabled with MAC address bypass authentication, you can run the **dot1x mac-bypass mac-auth-first** command to enable the device to perform MAC address authentication first during MAC address bypass authentication. After that, the device first starts the MAC address authentication process for users, and triggers 802.1X authentication only if MAC address authentication fails.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Follow-up Procedure

Run the **dot1x mac-bypass** command to enable MAC address bypass authentication on the interface.

Example

Enable the device to first perform MAC address authentication on GE0/0/1 during MAC address bypass authentication in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x mac-bypass mac-auth-first interface gigabitethernet 0/0/1
```

Enable the device to first perform MAC address authentication on GE0/0/1 during MAC address bypass authentication in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x mac-bypass mac-auth-first
```

13.6.72 dot1x max-user

Function

The **dot1x max-user** command sets the maximum number of 802.1X authentication users allowed on an interface.

The **undo dot1x max-user** command restores the default maximum number of 802.1X authentication users allowed on an interface.

By default, the number of 802.1X authentication users is the maximum number of 802.1X authentication users supported by the device.

Format

In the system view:

dot1x max-user *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x max-user [*user-number*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x max-user *user-number*

undo dot1x max-user [*user-number*]

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of 802.1X authentication users on an interface.	The value is an integer that varies depending on the product model.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the maximum number of 802.1X authentication users allowed on an interface, run the **dot1x max-user** command.

Prerequisites

The 802.1X authentication function has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

If the user access mode on an interface is interface-based (configured using the **dot1x port-method** command), the maximum number of 802.1X authentication users allowed on the interface is 1. Before running the **dot1x max-user** command to set the maximum number of 802.1X authentication users allowed on the interface, run the **undo dot1x port-method** command to restore the user access mode on the interface to MAC address-based.

Example

In the system view, set the maximum number of 802.1X authentication users allowed on GE0/0/1 to 7.

```
<HUAWEI> system-view
[HUAWEI] dot1x max-user 7 interface gigabitethernet 0/0/1
```

In the interface view, set the maximum number of 802.1X authentication users allowed on GE0/0/1 to 7.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x max-user 7
```

13.6.73 dot1x mc-trigger

Function

The **dot1x mc-trigger** enables multicast-triggered 802.1X authentication.

The **undo dot1x mc-trigger** disables multicast-triggered 802.1X authentication.

By default, multicast-triggered 802.1X authentication is enabled.

Format

dot1x mc-trigger

undo dot1x mc-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a client (for example, the built-in 802.1X client of the Windows operating system) cannot send an EAPOL-Start packet to perform 802.1X authentication, you can enable multicast-triggered 802.1X authentication. After that, the device multicasts an Identity EAP-Request frame to the client to trigger authentication.

Prerequisites

802.1X authentication has been enabled globally and on the interface using the **dot1x enable** command.

Example

Enable multicast-triggered 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger
```

13.6.74 dot1x mc-trigger port-up-send enable

Function

The **dot1x mc-trigger port-up-send enable** command enables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

The **undo dot1x mc-trigger port-up-send enable** command disables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

By default, the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled.

Format

dot1x mc-trigger port-up-send enable

undo dot1x mc-trigger port-up-send enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device periodically multicasts EAP-Request/Identity packets to clients so that the clients are triggered to send EAPOL-Start packets for 802.1X authentication. If the device interface connecting to a client changes from Down to Up, the client needs to send EAPOL-Start packets again for 802.1X authentication, which takes a long time. You can run the **dot1x mc-trigger port-up-send enable** command on the device to enable the device interface to multicast EAP-Request/Identity packets to the client to trigger 802.1X authentication immediately after the interface goes Up. This configuration shortens the re-authentication time.

Precautions

When the access control mode on the device interface is based on the MAC address, the **dot1x mc-trigger port-up-send enable** command does not take effect.

Example

Enable the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

```
<HUAWEI> system-view
[HUAWEI] dot1x mc-trigger port-up-send enable
```

13.6.75 dot1x port-control

Function

The **dot1x port-control** command sets the authorization state of an interface.

The **undo dot1x port-control** command restores the default authorization state of an interface.

By default, the authorization state of an interface is **auto**.

Format

In the system view:

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x port-control interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** }

undo dot1x port-control

Parameters

Parameter	Description	Value
auto	Indicates the auto identification mode. In this mode, an interface is initially in Unauthorized state and only allows users to send and receive authentication packets. Users cannot access network resources. After the users are authenticated, the interface becomes authorized and allows the users to access network resources.	-
authorized-force	Indicates the forcible authorization mode. In this mode, the interface is always in Authorized state, does not handle authentication packets, and allows users to access network resources without authentication or authorization.	-

Parameter	Description	Value
unauthorized-force	Indicates the forcible unauthorized mode. In this mode, the interface is always in Unauthorized state, does not handle authentication packets, and prohibits users from accessing network resources.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **auto** mode is recommended. Only authenticated users can access network resources. To trust all users on an interface without authentication, configure the **authorized-force** mode. To disable access rights of all users on an interface to ensure security, configure the **unauthorized-force** mode.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

When there are online 802.1X users on an interface, the **dot1x port-control** command must not be run; otherwise, the system displays alarm information.

It is recommended that you set the authorization state of an interface in the early stage of network deployment. When the network is running properly, run the **cut access-user** command to disconnect all users from the interface before changing the authorization state.

Example

Set the authorization state of GE0/0/1 to **unauthorized-force** in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x port-control unauthorized-force interface gigabitethernet 0/0/1
```

Set the authorization state of GE0/0/1 to **unauthorized-force** in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x port-control unauthorized-force
```

13.6.76 dot1x port-method

Function

The **dot1x port-method** command sets the 802.1X access control method of an interface.

The **undo dot1x port-method** command sets the default 802.1X access control method of an interface.

By default, 802.1X access control on an interface is based on MAC addresses.

Format

In the system view:

dot1x port-method { **mac** | **port** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x port-method interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x port-method { **mac** | **port** }

undo dot1x port-method

Parameters

Parameter	Description	Value
mac	Indicates that users are authenticated based on their MAC addresses.	-
port	Indicates that users are authenticated based on their access interfaces.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Indicates the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

802.1X access control can be based on MAC addresses or interfaces.

- When the **mac** method is used, all 802.1X users on an interface are authenticated one by one. If a user goes offline, other users on this interface are not affected. The **mac** method is applicable to individual users.
- When the **port** method is used, all the other 802.1X users on an interface can use network resources as long as one user is authenticated successfully. When the authenticated user goes offline, other users cannot use network resources. The **port** method is applicable to group users.

Prerequisites

802.1X authentication has been enabled globally and on an interface using the **dot1x enable** command.

Precautions

- When there are online 802.1X users on an interface, do not run the **dot1x port-method** command to change the access control method on the interface.
- If the access control method of an interface is set to **port**, only one 802.1X users can access the interface. After you run the **undo dot1x port-method** command, MAC address-based access control is enabled, but still only one user can access the interface. You can run the **dot1x max-user** command to increase the maximum number of 802.1X users as required.

Example

Set the 802.1X access control method on GE0/0/1 in the system view to **port**.

```
<HUAWEI> system-view
[HUAWEI] dot1x port-method port interface gigabitethernet 0/0/1
```

Set the 802.1X access control method on GE0/0/1 in the interface view to **port**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x port-method port
```

13.6.77 dot1x quiet-period

Function

The **dot1x quiet-period** command enables the quiet timer function.

The **undo dot1x quiet-period** command disables the quiet timer function.

By default, the quiet timer function is enabled.

Format

dot1x quiet-period

undo dot1x quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the quiet timer function is enabled, if the number of authentication failures of an 802.1X user exceeds a specified value (set using the **dot1x quiet-times** command) within 60 seconds, the user enters a quiet period. During the quiet period, the device discards the 802.1X authentication request packets from the user. This prevents the impact on the system due to frequent user authentication.

The value of the quiet timer is set using the **dot1x timer** command. When the quiet timer expires, the device re-authenticates the user.

Precautions

To make the configuration take effect, run the **dot1x enable** command twice to enable global and interface-based 802.1X user authentication.

Example

Enable the quiet timer.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-period
```

13.6.78 dot1x quiet-times

Function

The **dot1x quiet-times** command sets the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state.

The **undo dot1x quiet-times** command restores the default setting.

By default, an 802.1X user enters the quiet state after ten authentication failures within 60 seconds.

Format

dot1x quiet-times *fail-times*

undo dot1x quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before the 802.1X user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function of the device is enabled using the **dot1x quiet-period** command, if the number of authentication failures of an 802.1X user exceeds the value that is set using the **dot1x quiet-times** command within 60 seconds, the user enters the quiet state. This prevents the impact on the system due to frequent user authentication.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x quiet-times 4
```

13.6.79 dot1x reauthenticate

Function

The **dot1x reauthenticate** command enables periodic 802.1X re-authentication on an interface.

The **undo dot1x reauthenticate** command disables periodic 802.1X re-authentication on an interface.

By default, periodic 802.1X re-authentication is disabled on an interface.

Format

In the system view:

dot1x reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying the authentication information of an online user on the authentication server, the administrator needs to re-authenticate the user in real time to ensure user validity.

After the user goes online, the device saves user authentication information. After 802.1X re-authentication is enabled using the **dot1x reauthenticate** command, the device sends the stored authentication information of the online user to the authentication server for re-authentication at an interval. If the authentication information of the user does not change on the authentication server, the user is online normally. If the authentication information has been changed, the user is forced to go offline. The user then needs to be re-authenticated according to the changed authentication information.

NOTE

The re-authentication interval is set using the **dot1x timer reauthenticate-period** command.

This function takes effect only for users who go online after this function is successfully configured.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Precautions

If periodic 802.1X re-authentication is enabled, a large number of 802.1X authentication logs are generated.

Example

Enable periodic 802.1X re-authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x reauthenticate interface gigabitethernet 0/0/1
```

Enable periodic 802.1X re-authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x reauthenticate
```

13.6.80 dot1x reauthenticate mac-address

Function

The **dot1x reauthenticate mac-address** command enables re-authentication for an online 802.1X user with the specified MAC address.

By default, re-authentication is disabled for an online 802.1X user with the specified MAC address.

Format

dot1x reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of an 802.1X user to be re-authenticated.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **dot1x reauthenticate**.

The **dot1x reauthenticate mac-address** and **dot1x reauthenticate** commands re-authenticate online 802.1X users and their difference is as follows:

- The **dot1x reauthenticate mac-address** command configures the device to re-authenticate a specified user for once.
- The **dot1x reauthenticate** command configures the device to re-authenticate all users on a specified interface at intervals.
- The **dot1x reauthenticate mac-address** command does not support re-authentication for 802.1X users in pre-connection state.

Example

Enable re-authentication for an 802.1X user with the MAC address of 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] dot1x reauthenticate mac-address 00e0-fc12-3456
```

13.6.81 dot1x retry

Function

The **dot1x retry** command configures the number of times an authentication request is retransmitted to an 802.1X user.

The **undo dot1x retry** command restores the default configuration.

By default, the device can retransmit an authentication request to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the number of times an authentication request is retransmitted to an 802.1X user.	The value is an integer that ranges from 1 to 10. By default, the device can retransmit an authentication request to an 802.1X user twice. The default value is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the device does not receive any response from a user within a specified time after sending an authentication request to the user, the device sends the authentication request again. If the authentication request has been sent for the maximum retransmission times and no response is received, the user authentication fails. In this process, the total number of authentication requests sent by the device is *max-retry-value* plus 1.

NOTE

- After you run the **dot1x retry** command, the setting takes effect on all interfaces enabled with 802.1X authentication.
- Repeated authentication requests occupy a lot of system resources. When using the **dot1x retry** command, you can set the maximum number of times according to user requirements and device resources. The default value is recommended.
- The interval for sending authentication requests is set using the **dot1x timer** command. The interval for sending authentication requests to offline users is controlled by the **tx-period** and **client-timeout** timer, and the interval for sending authentication requests to online users is controlled by the **handshake-period** timer.
- The **dot1x retry** command is used together with the guest VLAN function (for details, see **authentication guest-vlan**). If a user does not respond within the specified maximum number of times, the user is added to the guest VLAN so that the user can access resources in the guest VLAN without being authenticated.

Example

Set the number of times an authentication request can be retransmitted to 802.1X users to 4.

```
<HUAWEI> system-view
[HUAWEI] dot1x retry 4
```

13.6.82 dot1x timer

Function

The **dot1x timer** command sets values of timers used in 802.1X authentication.

The **undo dot1x timer** command restores the default settings of timers used in 802.1X authentication.

For the default settings of timers used in 802.1X authentication, see the table in "Parameters".

Format

dot1x timer { **client-timeout** *client-timeout-value* | **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **mac-bypass-delay** *delay-time-value* | **free-ip-timeout** *free-ip-time-value* }

undo dot1x timer { **client-timeout** | **quiet-period** | **tx-period** | **mac-bypass-delay** | **free-ip-timeout** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the timeout interval of the authentication response from the client. You are advised to set this parameter to 30 seconds. **NOTE** On the network, some terminals may delay in responding to EAP-Request/MD5 Challenge packets sent from the device. If the delay is long, you can increase **client-timeout** *client-timeout-value* so that these terminals can go online. The adjustment rule is as follows: 3 x **client-timeout** *client-timeout-value* > Terminal response delay	The value is an integer that ranges from 1 to 120, in seconds. By default, the timeout interval of the authentication response from the client is 5 seconds.

Parameter	Description	Value
quiet-period *quiet-period-value*	Specifies the quiet period. For details, see **dot1x quiet-period**.	The value is an integer that ranges from 1 to 3600, in seconds. By default, the quiet period of a user who fails authentication is 60 seconds.
tx-period *tx-period-value*	Specifies the interval for sending authentication requests. The device starts the **tx-period** timer in either of the following situations: ● When the client initiates authentication, the device sends a unicast Request/Identity request packet to the client and starts the **tx-period** timer. If the client does not respond within the period set by the timer, the device retransmits the authentication request packet. ● To authenticate the 802.1X clients that cannot initiate authentication, the device sends multicast Request/Identity packets through the 802.1X-enabled interface to the clients at the interval set by the **tx-period** timer.	The value is an integer that ranges from 1 to 120, in seconds. By default, the interval for sending authentication requests is 30 seconds.

Parameter	Description	Value
mac-bypass-delay *delay-time-value*	Specifies the value of the delay timer for MAC address bypass authentication. After MAC address bypass authentication is configured, the device performs 802.1X authentication and starts the delay timer for MAC address bypass authentication. If 802.1X authentication fails after the value of the delay timer is reached, the device performs MAC address bypass authentication.	The value is an integer that ranges from 1 to 300, in seconds. By default, the value of the delay timer for MAC address bypass authentication is 30s.
free-ip-timeout *free-ip-time-value*	Specifies the aging time of authentication-free user entries. When the 802.1X free IP subnet is configured, the device creates authentication-free user entries after receiving ARP/DHCP packets from 802.1X users. If users go offline abnormally, the authentication-free user entries cannot be deleted. To prevent this problem, the aging time of authentication-free user entries can be configured.	The value is an integer that ranges from 0 to 71581, in minutes. The value 0 indicates that authentication-free user entries do not age. By default, the value of the aging time for authentication-free user entries is 1380 minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, multiple timers implement systematic interactions between access users, access devices, and the authentication server. You can change the values of the timers using the **dot1x timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. Generally, the default settings of the timers are recommended.

Example

Set the timeout interval of the authentication response from the client to 90s.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer client-timeout 90
```

13.6.83 dot1x timer arp-detect

Function

The **dot1x timer arp-detect** command sets the timeout interval of the ARP detect.

The **undo dot1x timer arp-detect** command restores the default settings.

By default, the timeout interval of the ARP detect is 120 seconds.

Format

dot1x timer arp-detect *arp-detect-value*

undo dot1x timer arp-detect

Parameters

Parameter	Description	Value
arp-detect *arp-detect-value*	Specifies the timeout interval of the ARP detect.	The value is 0 or an integer that ranges from 5 to 7200, in seconds. 0 indicates that the ARP detect function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The ARP probe function can also be implemented by detecting whether there is user traffic on the access device. If the ARP probe interval is **n**, the device detects user traffic at **n** and **2n**. The following uses the **0-n** period as an example. The process during the **n-2n** period is the same as that during **0-n**. (This process applies only to users who go online from the S5731-H,?S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI. Other device models do not support user traffic detection, and they send ARP probe packets at **n** and **2n**.)

- If user traffic passes through the device within the **0-n** period, the device considers that the user is online at **n**, and will not send ARP probe packets. Additionally, the device resets the ARP probe interval.
- If no user traffic passes through the device within the **0-n** period, the device cannot determine whether the user is online at **n**. In this case, the device sends an ARP probe packet. If the device receives an ARP reply packet from the user, it considers the user online and resets the ARP probe interval. If no ARP reply packet is received, the device considers the user offline.
- If user traffic passes through the device or the device receives an ARP reply packet from the user within the **2n-3n** period, the device considers that the user is online at **3n** and resets the ARP probe interval.
- If no user traffic passes through the device and the device receives no ARP reply packet from the user within the **2n-3n** period, the device cannot determine whether the user is online at **3n** and considers the user offline.

If the device considers that the user is offline at **n**, **2n**, and **3n**, the device deletes all entries related to the user. To prevent the user from going offline unexpectedly when no operation is performed on the PC, do not set a short ARP probe interval.

Example

Set the timeout interval of the ARP detect to 90s.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer arp-detect 90
```

13.6.84 dot1x timer reauthenticate-period

Function

The **dot1x timer reauthenticate-period** command sets the re-authentication interval for 802.1X authentication users.

The **undo dot1x timer reauthenticate-period** command restores the default re-authentication interval.

By default, the re-authentication interval is 3600 seconds.

Format

dot1x timer reauthenticate-period *reauthenticate-period-value*

undo dot1x timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for 802.1X address authentication users. To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After enabling the re-authentication function for online 802.1X authentication users using the **dot1x reauthenticate** command, run the **dot1x timer reauthenticate-period** command to set the re-authentication interval. The device then authenticates online users at the specified interval, ensuring that only authorized users can keep online.

If the command is executed in the system view, the function takes effect on all interfaces. If the command is executed in both system view and interface view, the function takes effect on the interface.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

Set the 802.1X re-authentication interval to 7200 seconds.

```
<HUAWEI> system-view
[HUAWEI] dot1x timer reauthenticate-period 7200
```

13.6.85 dot1x trigger dhcp-binding

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through 802.1X authentication, the unauthorized users can obtain the same identities as the authorized users and connect to the network without authentication. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG and DAI. These two functions are implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After the static IP users who pass 802.1X authentication send EAP packets to trigger generation of the user information table, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface recorded in the table.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass 802.1X authentication. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.
- In the interface view, run the **arp anti-attack check user-bind enable** command to enable DAI.

Precautions

- Before configuring the device to generate the DHCP snooping binding table for static IP users, you must have enabled 802.1X authentication and DHCP snooping globally and on interfaces using the **dot1x enable** and **dhcp snooping enable** commands.
- The EAP protocol does not specify a standard attribute to carry IP address information. Therefore, if the EAP request packet sent by a static IP user does not contain an IP address, the IP address information in the DHCP snooping binding table is obtained from the user' first ARP request packet with the same MAC address as the user information table after the user passes authentication. On a network, unauthorized users may forge authorized users' MAC addresses to initiate ARP snooping attacks to devices, and the DHCP snooping binding table generated accordingly may be unreliable. Therefore, the **dot1x trigger dhcp-binding** command is not recommended and you are advised to run the **user-bind static** command to configure the static binding table.
- For users who are assigned IP addresses using DHCP, you do not need to run the **dot1x trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.

Example

Enable the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dot1x trigger dhcp-binding
```

13.6.86 dot1x unicast-trigger

Function

The **dot1x unicast-trigger** command enables 802.1X authentication triggered by unicast packets.

The **undo dot1x unicast-trigger** command disables 802.1X authentication triggered by unicast packets.

By default, 802.1X authentication triggered by unicast packets is disabled.

Format

In the system view:

dot1x unicast-trigger interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo dot1x unicast-trigger interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dot1x unicast-trigger** command is used on the device, the device sends a unicast packet to respond to the received ARP or DHCP Request packet from a client. If the client does not respond within the timeout interval (set by the **dot1x timer** command), the device retransmits the unicast packet (the maximum of retransmission count is set by the **dot1x retry** command). During 802.1X-based network deployment, 802.1X users can start 802.1X authentication without installing specified client dial-in software, which facilitates network deployment.

NOTE

The **dot1x unicast-trigger** command has the same function as the **dot1x dhcp-trigger** command.

Example

Enable 802.1X authentication triggered by unicast packets on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] dot1x unicast-trigger interface gigabitethernet 0/0/1
```

13.6.87 dot1x url

Function

The **dot1x url** command configures a redirect URL in 802.1X authentication.

The **undo dot1x url** command cancels the redirect URL configuration in 802.1X authentication.

By default, no redirect URL is configured in 802.1X authentication.

Format

dot1x url *url-string*

undo dot1x url

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL.	The value is a string of 1 to 247 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the early stage of network deployment, 802.1X client deployment is difficult and requires heavy workload. You can run the **dot1x url** command to set a redirect URL to the web page address for downloading the 802.1X client. When a user uses a browser to access resources that are not in the authentication-free IP subnet, the device redirects the URL that the user attempts to access to the 802.1X client download web URL after the device receives HTTP packets from the user. The user then can download and install the 802.1X client.

Follow-up Procedure

Run the **dot1x free-ip** command to configure the network segment where the redirect URL used in 802.1X authentication belongs or configure the IP address segment of the DNS server as an authentication-free IP subnet. To ensure that pre-connection users can be aged out normally, you need to run the **dot1x timer free-ip-timeout** command to set the aging time of authentication-free user entries.

Precautions

This command applies when users use the 802.1X client software that is not provided by the system.

The redirect URL must be within the authentication-free IP subnet. Otherwise, the URL will be inaccessible.

When 802.1X-based fast deployment is configured, the device supports redirection triggered only by HTTP packets with HTTP port 80.

Example

Set the redirect URL in 802.1X authentication to http://10.1.1.1:8080/download.

```
<HUAWEI> system-view
[HUAWEI] dot1x url http://10.1.1.1:8080/download
```

13.6.88 force-push

Function

The **force-push** command enables a pushed URL template or pushed URL.

The **undo force-push** command disables a pushed URL template or pushed URL.

By default, no pushed URL template or pushed URL is enabled.

Format

force-push { **url-template** *template-name* | **url** *url-address* }

undo force-push

Parameters

Parameter	Description	Value
url-template *template-name*	Specifies the name of a pushed URL template.	The value must be the name of an existing URL template.
url *url-address*	Specifies a pushed URL.	The value is a string of 1 to 247 case-sensitive characters without spaces and question marks (?). If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a user sends an HTTP/HTTPS packet to access a web page for the first time after the user is successfully authenticated, the device forcibly redirects the user to a specified web page. In addition to pushing advertisement pages, the device obtains user terminal information through the HTTP/HTTPS packets sent by users, and applies the information to other services. There are two ways to push web pages:

1. URL: pushes the URL of the specified web page.
2. URL template: pushes a URL template. The URL template must have been created and contains the URL of the pushed web page and URL parameters.

Prerequisites

The URL configured using the **url** command in the URL template view cannot be a redirect URL; otherwise, the **force-push** command does not take effect.

Precautions

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the forcible web page push function takes effect only for the first HTTP or HTTPS packet sent from users. If an application that actively sends HTTP or HTTPS packets is installed on a user terminal and the terminal has sent HTTP or HTTPS packets before the user accesses a web page, the user is unaware of the web page push process.

For switches except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S: The forcible web page push function takes effect only when it is used together with a redirect ACL. If a redirect ACL exists in the user table, a web page is forcibly pushed when HTTP or HTTPS packets from users match the redirect ACL rule. Usually, you can configure the RADIUS server to authorize the Huawei extended RADIUS attribute **HW-Redirect-ACL** or **HW-IPv6-Redirect-ACL** to users for redirect ACL implementation, or run the **redirect-acl** command to configure a redirect ACL.

A pushed URL configured in a domain needs to be used together with a redirect ACL or push flag attribute. The redirect ACL has a higher priority than the push flag attribute. By default, a pushed URL configured in a domain carries the push flag attribute. Users will be redirected to the pushed URL when they are successfully authenticated.

When an IPv4 redirect ACL is configured for an IPv6 user or an IPv6 redirect ACL is configured for an IPv4 user, the **Push URL content** field in the **display access-user** command output displays the pushed URL, but the browser of the user cannot redirect to the pushed URL.

Switches except the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support concurrent use of the pushed URL and redirection ACL6 functions. If both functions are configured, the **Push URL content** field in the **display access-user** command output displays the pushed URL; however, the terminal browser cannot be redirected to the pushed URL.

Example

Enable the pushed URL template **abc** in the domain **test**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] domain test
[HUAWEI-aaa-domain-test] force-push url-template abc
```

13.6.89 http get-method enable

Function

The **http get-method enable** command configures the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

The **undo http get-method enable** command restores the default setting.

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication.

Format

http get-method enable

undo http get-method enable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication. You can run the **http get-method enable** command to configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

Precautions

The GET mode has the risk of password disclosure. Therefore, the POST mode is recommended.

This command only applies to scenarios in which HTTP or HTTPS is used for Portal connection establishment.

Example

Configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http get-method enable
```

13.6.90 http-method post

Function

The **http-method post** command configures parameters for parsing and replying to POST request packets of the HTTP or HTTPS protocol.

The **undo http-method post** command restores the default configuration.

By default, the system has configured parameters for parsing and replying to POST request packets of the HTTP or HTTPS protocol. For details, see the "Parameters" table.

Format

http-method post { **cmd-key** *cmd-key* [**login** *login-key* | **logout** *logout-key*] * | **init-url-key** *init-url-key* | **login-fail response** { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] } | **login-success response** { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* } | **logout-fail response** { **msg** *msg* | **redirect-url** *redirect-url* } | **logout-success response** { **msg** *msg* | **redirect-url** *redirect-url* } |

password-key *password-key* | **user-mac-key** *user-mac-key* | **userip-key** *userip-key* | **username-key** *username-key* } *

undo http-method post { **all** | { **cmd-key** | **init-url-key** | **login-fail** | **login-success** | **logout-fail** | **logout-success** | **password-key** | **user-mac-key** | **userip-key** | **username-key** } * }

Parameters

Parameter	Description	Value
cmd-key *cmd-key*	Specifies the command identification keyword. The default value is **cmd**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
login *login-key*	Specifies the user login identification keyword. The default value is **login**.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
logout *logout-key*	Specifies the user logout identification keyword. The default value is **logout**.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
init-url-key *init-url-key*	Specifies the identification keyword for the user initial login URL. The default value is **initurl**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-fail response { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] }	Specifies the response message upon a user login failure. • **err-msg authenserve-reply-message**: The response message returned by the authentication server is displayed upon a user login failure. • **err-msg msg** *msg*: A specified message is displayed upon a user login failure. • **redirect-login-url**: A user is redirected to the login URL upon a login failure. This mode is used by default. • **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a login failure. • **append-reply-message** *msgkey*: The redirect URL carries the identification keyword for the response message returned by the authentication server.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces. • *msgkey*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

Parameter	Description	Value
login-success response { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* }	Specifies the response message upon successful user login. - **msg** *msg*: A specified message is displayed upon successful user login. - **redirect-init-url**: A user is redirected to the initial login URL upon successful login. This mode is used by default. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful login.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-fail response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon a user logout failure. - **msg** *msg*: A specified message is displayed upon a user logout failure. The default value is **LogoutFail!**. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon a logout failure.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).
logout-success response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon successful user logout. - **msg** *msg*: A specified message is displayed upon successful user logout. The default value is **LogoutSuccess!**. - **redirect-url** *redirect-url*: A user is redirected to a specified URL upon successful logout.	- *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *redirect-url*: The value is a string of 1 to 247 case-sensitive characters without spaces or question marks (?).

Parameter	Description	Value
password-key *password-key*	Specifies the password identification keyword. The default value is **password**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
user-mac-key *user-mac-key*	Specifies the identification keyword for the user MAC address. The default value is **macaddress**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
userip-key *userip-key*	Specifies the identification keyword for the user IP address. The default value is **ipaddress**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
username-key *username-key*	Specifies the user name identification keyword. The default value is **username**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
all	Indicates all parameters.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

When the device uses the HTTP or HTTPS protocol to communicate with the Portal server, a user sends POST request packets (carrying parameters such as the user name and MAC address) to the device as required by the Portal server. After receiving the POST request packets, the device parses parameters in the packets. If identification keywords of the parameters differ from those configured on the device, the user authentication fails. Therefore, you need to run the **http-method post** command to configure the identification keywords based on the Portal server configuration.

After successful user login or logout, or a user login or logout failure, the device sends the login or logout result to the user based on the **http-method post** command configuration. For example, the device sends the **LogoutSuccess!** message to a user who logs out successfully by default.

Example

Set the command identification keyword to **cmd1** for parsing POST request packets of the HTTP or HTTPS protocol.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] http-method post cmd-key cmd1
```

13.6.91 link-down offline delay

Function

The **link-down offline delay** command configures the user logout delay when an interface link is faulty.

The **undo link-down offline delay** command restores the default configuration.

By default, the user logout delay is 10 seconds when an interface link is faulty.

Format

link-down offline delay { *delay-value* | **unlimited** }

undo link-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when an interface link is faulty.	The value is an integer that ranges from 0 to 60, in seconds. If the value is 0, users are logged out immediately when an interface link is faulty.
unlimited	Indicates that users are not logged out when an interface link is faulty.	-

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a link is faulty, the interface is interrupted and users are directly logged out. To solve this problem, you can configure the user logout delay function. When the interface link is faulty, the users remain online within the delay. In this case, if the link is restored, the users do not need to be re-authenticated. If the users are disconnected after the delay and the link is restored, the users need to be re-authenticated.

Precautions

- This function takes effect only for wired users who go online on Layer 2 physical interfaces that have been configured with NAC authentication.
- To make the function take effect, it is recommended that the configured interval be greater than the time during which the interface is in Up state. If the link frequently flaps within a short period, it is recommended that the interval be set to **unlimited**.

Example

Configure the user logout delay to 5 seconds when the link of GE0/0/1 is faulty.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] link-down offline delay 5
```

13.6.92 mac-authen

Function

The **mac-authen** command enables MAC address authentication globally or on an interface.

The **undo mac-authen** command disables MAC address authentication globally or on an interface.

By default, MAC address authentication is disabled globally and on an interface.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.

Format

In the system view:

mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

mac-authen

undo mac-authen

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MAC address authentication controls network access rights of a user based on the user's access interface and MAC address. During MAC address authentication, the user name and password are the user's MAC address. MAC address authentication is applicable to the scenario where MAC addresses are unchanged and high security is not required, and is used to authenticate terminals such as printers where the authentication client cannot be installed.

If you run the **mac-authen** command in the system view without any interfaces specified, MAC address authentication is enabled globally. The configurations of MAC address authentication take effect only after global MAC address authentication is enabled. MAC address bypass authentication is not controlled by this command.

To enable MAC address authentication on an interface, you can perform either of the following operations:

- Run the **mac-authen** command in the interface view.
- Run the **mac-authen interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10> command in the system view.

Precautions

- Before running the **undo mac-authen** command, ensure that there is no online MAC address authentication user; otherwise, you cannot run this command. Online MAC address authentication users do not include online users using MAC address bypass authentication.
- After MAC address authentication is enabled on a VLANIF interface, the guest VLAN, critical VLAN, or dynamic VLAN authorization is invalid to the MAC address authentication users on the VLANIF interface.
- Before enabling MAC address authentication on the VLANIF interface, ensure that the strict ARP entry learning function is disabled using the **undo arp learning strict** command. If the function is enabled, the users cannot go online.
- After the static MAC address entry is configured using the **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id* command, the user corresponding to the entry cannot pass MAC address authentication.
- If MAC address authentication is enabled on an interface, the following commands cannot be used on the same interface. If the following commands are configured on an interface, MAC address authentication cannot be enabled on the same interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.
mac-address learning disable	Disables MAC address learning on an interface.
port link-type dot1q-tunnel	Sets the link type of an interface to QinQ.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Configures VLAN mapping on an interface.
port vlan-stacking	Configures selective QinQ.

Command	Function
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.
user-bind ip sticky-mac	Enables the device to generate snooping MAC entries.

Example

Enable global MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] mac-authen
```

Enable MAC address authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen
[HUAWEI] mac-authen interface gigabitethernet 0/0/1
```

Enable MAC address authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen
```

13.6.93 mac-authen trigger

Function

The **mac-authen trigger** command configures the packet types that can trigger MAC address authentication.

The **undo mac-authen trigger** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger MAC address authentication.

Format

In the system view:

mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } * [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } * [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } *

undo mac-authen { **dhcp-trigger** | **arp-trigger** | **dhcpv6-trigger** | **nd-trigger** } *

Parameters

Parameter	Description	Value
dhcp-trigger	Triggers MAC address authentication through DHCP packets.	-
arp-trigger	Triggers MAC address authentication through ARP packets.	-
dhcpv6-trigger	Triggers MAC address authentication through DHCPv6 packets.	-
nd-trigger	Triggers MAC address authentication through ND packets.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. If this parameter is not specified, the command takes effect on all interfaces.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication is enabled, the device can trigger MAC address authentication on users by default when receiving DHCP/ARP/DHCPv6/ND packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger MAC address authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger MAC address authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger MAC address authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

Precautions

If the command is configured globally, the configuration takes effect on multiple interfaces. If the command is configured globally and on an interface, the configuration on the interface takes precedence.

The **mac-authen trigger** command also enables MAC address authentication. When both the **mac-authen trigger** and **mac-authen** commands are configured on an interface, the last configured one takes effect. If the **mac-authen** configuration takes effect on the interface, DHCP, ARP, DHCPv6, and ND packets can trigger MAC address authentication.

Example

Configure the device to trigger MAC address authentication only through DHCP packets in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen dhcp-trigger
```

13.6.94 mac-authen dhcp-trigger dhcp-option

Function

The **mac-authen dhcp-trigger dhcp-option** command enables the device to send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

The **undo mac-authen dhcp-trigger dhcp-option** command restores the default configuration.

By default, the device does not send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

Format

In the system view:

mac-authen dhcp-trigger dhcp-option *option-code* [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

undo mac-authen dhcp-trigger dhcp-option *option-code* [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

In the interface view:

mac-authen dhcp-trigger dhcp-option *option-code*

undo mac-authen dhcp-trigger dhcp-option *option-code*

Parameters

Parameter	Description	Value
option-code	Specifies the option that the device sends to the authentication server.	The value is fixed as 82.
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. - *interface-type* specifies the interface type. - *interface-number1* specifies the number of the first interface. - *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Option82 record information about DHCP user locations and services (voice and data services). After this command is run, if the device supports the function of triggering MAC address authentication through DHCP packets, it sends Option82 information to the authentication server when triggering MAC address authentication through DHCP packets. Based on the user information recorded in Option82, the authentication server then assigns different network access rights to users with different services in different locations. This implements accurate control on the network access right of each user.

Example

Globally enable the device to send Option82 information to the authentication server when triggering MAC address authentication through DHCP packets.

```
<HUAWEI> system-view
[HUAWEI] mac-authen dhcp-trigger dhcp-option 82
```

13.6.95 mac-authen domain

Function

The **mac-authen domain** command configures an authentication domain for MAC address authentication users.

The **undo mac-authen domain** command restores the global default authentication domain for MAC address authentication users.

The default authentication domain for MAC address authentication users is the global default domain.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.

Format

In the system view:

mac-authen domain *isp-name* [**mac-address** *mac-address* **mask** *mask*]

undo mac-authen domain [*isp-name* [**mac-address** *mac-address*] | [**mac-address** { *mac-address* | **all** }]]

In the interface view:

mac-authen domain *isp-name*

undo mac-authen domain

Parameters

Parameter	Description	Value
isp-name	Specifies the ISP domain name.	The value is a string of 1 to 64 case-insensitive characters without any space, asterisk (*), question mark (?), quotation mark ("), hyphen (-) or consecutive hyphens (--).
mac-address *mac-address*	Specifies an authentication domain for the MAC address authentication user with a specified MAC address. **NOTE** A maximum of 16 MAC address ranges can be specified.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the mask of a MAC address.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
all	Restores the global default domain for all MAC address authentication users.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When user names for MAC address authentication do not contain domain names, the device authenticates users using the **default** domain if no authentication domain is configured on the device or interface. The authentication scheme is not flexible because all users are authenticated in the **default** domain. The **mac-authen domain** command specifies the authentication domains for MAC address authentication users. Different interfaces can be located in different authentication domains. This command can specify the authentication domains for the specified MAC addresses. Therefore, this command allows users with different authentication requirements to adopt various authentication schemes.

NOTE

- If the user name contains a domain name (configured using **mac-authen username**), the user is authenticated in this domain.
- The specified user names and domain names must be the same as those configured in the AAA view.
- The authentication schemes in the domains are configured in the AAA view.

Prerequisites

The domain to be configured as an authentication domain has been created using the **domain (AAA view)** command.

MAC address authentication has been enabled globally and on an interface using the **mac-authen** command.

Precautions

If authentication domains are configured in both the system view and interface view, the domain configured in the interface view takes effect. If no authentication domain is configured in the interface view, the domain configured in the system view takes effect.

You must specify a unicast MAC address in the **mac-authen domain** command. A user with an all-0 MAC address is not authenticated.

The configured authentication domain is applied to the MAC addresses calculated with the mask. Therefore, the **undo mac-authen domain** command will delete the authentication domain of the calculated MAC addresses. Before running the **undo mac-authen domain** command, run the **display this** command to view the calculated MAC addresses.

On a network configured with both 802.1X authentication and MAC address bypass authentication, an 802.1X user failing the 802.1X authentication will be authenticated in the manner of MAC address bypass authentication. If the authentication scheme of MAC address bypass authentication is none authentication, the user can go online successfully without being authenticated. To prevent such unauthorized authentication, use the **mac-authen domain** command to specify different domains for the two authentication methods.

Example

Configure the **cams** domain as the authentication domain for MAC address authentication users in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen domain cams
```

Configure the **cams** domain as the authentication domain for MAC address authentication users in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen domain cams
```

13.6.96 mac-authen max-user

Function

The **mac-authen max-user** command sets the maximum number of MAC address authentication users on an interface.

The **undo mac-authen max-user** command restores the default value of the maximum number of MAC address authentication users on an interface.

By default, the number of MAC address authentication users is the maximum number of MAC address authentication users supported by the device.

Format

In the system view:

mac-authen max-user *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen max-user [*user-number*] **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen max-user *user-number*

undo mac-authen max-user [*user-number*]

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of MAC address authentication users on an interface.	The value is an integer that varies depending on the product model.

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. - *interface-type* specifies the interface type. - *interface-number1* specifies the number of the first interface. - *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the number of MAC address authentication users on an interface, run the **mac-authen max-user** command. When the number of access users on an interface reaches the limit, the device will not trigger authentication for the users newly connected to the interface; therefore, these users cannot access the network.

Prerequisites

MAC address authentication has been enabled globally and on an interface using the **mac-authen** command.

Example

Set the maximum number of MAC address authentication users on GE0/0/1 to 8 in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen max-user 8 interface gigabitethernet 0/0/1
```

Set the maximum number of MAC address authentication users on GE0/0/1 to 8 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen max-user 8
```

13.6.97 mac-authen offline dhcp-release

Function

The **mac-authen offline dhcp-release** command enables the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

The **undo mac-authen offline dhcp-release** command restores the default configuration.

By default, the device does not clear user entries when receiving DHCP Release packets from MAC address authentication users.

Format

In the system view:

mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen offline dhcp-release

undo mac-authen offline dhcp-release

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the type and number of an interface. - *interface-type* specifies the interface type. - *interface-number1* specifies the number of the first interface. - *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number2* and *interface-number1* together specify an interface range.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication users who send DHCP Release packets go offline, the corresponding user entries on the device cannot be deleted immediately. This occupies device resources and possibly prevents other users from going online. You can run this command to enable the device to clear the user entries in real time when MAC address authentication users go offline.

Precautions

If the device functions as a DHCP relay agent, configure the DHCP snooping function on the device; otherwise, this command does not take effect.

Example

In the system view, enable the device to clear user entries when receiving DHCP Release packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mac-authen offline dhcp-release interface gigabitethernet 0/0/1
```

In the interface view, enable the device to clear user entries when receiving DHCP Release packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen offline dhcp-release
```

13.6.98 mac-authen permit mac-address

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

By default, any new MAC address is allowed for MAC address authentication after MAC address authentication is enabled on a VLANIF interface. To actually control the users who can be authenticated using MAC addresses on the VLANIF interface, use this command to specify a MAC address range for MAC address authentication.

Example

Set the MAC address to 00e0-fc01-0101 and the MAC address mask length to 24 for MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 10
[HUAWEI-Vlanif10] mac-authen permit mac-address 00e0-fc01-0101 mask 24
```

13.6.99 mac-authen quiet-times

Function

The **mac-authen quiet-times** command configures the maximum number of authentication failures within 60 seconds before a MAC authentication user enters the quiet state.

The **undo mac-authen quiet-times** command restores the maximum number of authentication failures to the default value.

By default, the maximum number of authentication failures is 10.

Format

mac-authen quiet-times *fail-times*

undo mac-authen quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a MAC authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The quiet function for MAC address authentication is enabled on a device by default. When the maximum number of authentication failures exceeds 1, the device quiets a MAC authentication user and does not process authentication requests from the user, reducing impact on the system caused by attackers.

Precautions

After the maximum number of authentication failures is set to a value larger than the configured value, the user in quiet state can initiate reauthentication only after the quiet period expires. If the user enters an incorrect user name or password again, the user authentication fails. The device does not quiet the user but allows the user to initiate reauthentication immediately.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] mac-authen quiet-times 4
```

13.6.100 mac-authen reauthenticate

Function

The **mac-authen reauthenticate** command enables periodic MAC address re-authentication on a specified interface.

The **undo mac-authen reauthenticate** command disables periodic MAC address re-authentication on a specified interface.

By default, periodic MAC address re-authentication is enabled on a specified interface.

Format

In the system view:

mac-authen reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After modifying the authentication information of an online user on the authentication server, the administrator needs to re-authenticate the user in real time to ensure user validity.

After the user goes online, the device saves user authentication information. After periodic re-authentication for all online MAC address authentication users on a specified interface is enabled using the **mac-authen reauthenticate** command, the device sends the stored authentication information of the online user on the interface to the authentication server for re-authentication at an interval. If the user's authentication information does not change on the authentication server, the user is online normally. If the authentication information has been changed, the user is forced to go offline. The user then needs to be re-authenticated according to the changed authentication information.

NOTE

The re-authentication interval is set using the **mac-authen timer reauthenticate-period** command.

This function takes effect only for users who go online after this function is successfully configured.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

Enable periodic MAC address re-authentication on GE0/0/1 in the system view.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate interface gigabitethernet 0/0/1
```

Enable periodic MAC address re-authentication on GE0/0/1 in the interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen reauthenticate
```

13.6.101 mac-authen reauthenticate dhcp-renew

Function

The **mac-authen reauthenticate dhcp-renew** command enables the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

The **undo mac-authen reauthenticate dhcp-renew** command restores the default setting.

By default, the device does not re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Format

In the system view:

mac-authen reauthenticate dhcp-renew interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen reauthenticate dhcp-renew interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen reauthenticate dhcp-renew

undo mac-authen reauthenticate dhcp-renew

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the type and number of an interface. - *interface-type* specifies the interface type. - *interface-number1* specifies the number of the first interface. - *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number2* and *interface-number1* together specify an interface range.	-

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After users go online, the administrator may modify the users' authentication parameters or network access rights on the authentication server. To ensure user validity or update the users' network access rights in real time, you can run this command to enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

NOTE

This function applies only to L2 BNG scenarios.

Example

In the system view, enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate dhcp-renew interface gigabitethernet 0/0/1
```

In the interface view, enable the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-authen reauthenticate dhcp-renew
```

13.6.102 mac-authen reauthenticate mac-address

Function

The **mac-authen reauthenticate mac-address** command enables re-authentication for an online MAC address authentication user with a specified MAC address.

By default, re-authentication for an online MAC address authentication user with a specified MAC address is disabled.

Format

mac-authen reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies all valid unicast MAC addresses.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **mac-authen reauthenticate**.

The **mac-authen reauthenticate mac-address** and **mac-authen reauthenticate** commands re-authenticate online MAC address authentication users and their difference is as follows:

- The **mac-authen reauthenticate mac-address** command configures the device to immediately re-authenticate a user with a specified MAC address for once.
- The **mac-authen reauthenticate** command configures the device to re-authenticate all online MAC address authentication users on a specified interface at intervals.
- The **mac-authen reauthenticate mac-address** command does not support re-authentication for MAC address authentication users in pre-connection state.

Example

Enable re-authentication for an online MAC address authentication user with the MAC address 00e0-fc02-0003.

```
<HUAWEI> system-view
[HUAWEI] mac-authen reauthenticate mac-address 00e0-fc02-0003
```

13.6.103 mac-authen timer

Function

The **mac-authen timer** command configures parameters of timers for MAC address authentication.

The **undo mac-authen timer** command restores the default parameter values of timers for MAC address authentication.

Format

mac-authen timer { **guest-vlan reauthenticate-period** *interval* | **offline-detect** *offline-detect-value* | **quiet-period** *quiet-value* }

undo mac-authen timer { **guest-vlan reauthenticate-period** | **offline-detect** | **quiet-period** }

Parameters

Parameter	Description	Value
guest-vlan reauthenticate-period *interval*	Specifies the interval for re-authenticating users in the Guest VLAN.	The value is an integer that ranges from 60 to 3600, in seconds. The default value is 60.

Parameter	Description	Value
offline-detect *offline-detect-value*	Specifies the interval for detecting online users. The timer is used to periodically check whether a user is offline. **NOTE** The timer takes effect for both MAC address authentication users and static users.	The value is an integer that ranges from 30 to 7200, and 0, in seconds. The default value is 300. 0 means disable detecting online users.
quiet-period *quiet-value*	Specifies the value of the quiet timer. If a user fails authentication, the device does not process the user's authentication requests until the quiet timer expires. During the quiet period, the device does not process the user's authentication requests.	The value is an integer that ranges from 0 to 3600, in seconds. By default, the quiet period of a user who fails authentication is 60 seconds. **NOTE** When the quiet timer is set to 0, the quiet function is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During MAC address authentication, multiple timers implement systematic interactions between access users or devices and the authentication server. You can change the values of the timers by running the **mac-authen timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. Generally, the default settings of the timers are recommended.

NOTE

If the number of offline detection packets (ARP packets) exceeds the default CAR value, the detection fails and the users are logged out. (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.) To resolve the problem, the following methods are recommended:

- Increase the detection interval based on the number of users. The default detection interval is recommended when there are less than 8000 users; the detection interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

Example

Set the value of the quiet timer to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-authen timer quiet-period 60
```

13.6.104 mac-authen timer reauthenticate-period

Function

The **mac-authen timer reauthenticate-period** command sets the re-authentication interval for MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default re-authentication interval.

The default re-authentication interval for MAC address authentication users in the system view is 1800 seconds, and the re-authentication interval in the interface view is the same as the re-authentication interval configured in the system view.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for MAC address authentication users.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After enabling the re-authentication function for online MAC address authentication users using the **mac-authen reauthenticate** command, run the **mac-authen timer reauthenticate-period** command to set the re-authentication interval. The device then authenticates online users at the specified interval, ensuring that only authorized users can keep online.

If the command is executed in the system view, the function takes effect on all interfaces. If the command is executed in both system view and interface view, the function takes effect on the interface.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

Set the re-authentication interval for online MAC address authentication users to 3600 seconds.

```
<HUAWEI> system-view
[HUAWEI] mac-authen timer reauthenticate-period 3600
```

13.6.105 mac-authen username

Function

The **mac-authen username** command configures the user name format for MAC address authentication.

The **undo mac-authen username** restores the default user name format.

By default, the MAC address without hyphens (-) or colons (:) is used as the user name and password for MAC address authentication.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support configuration of MAC address authentication on VLANIF interfaces.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* { **circuit-id** | **remote-id** } * [**separate** *separate*] [**format-hex**] **password cipher** *password* }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] | **dhcp-option** *option-code* [**password cipher** *password*]]

Parameters

Parameter	Description	Value
fixed *username*	Specifies the fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
password cipher *password*	Specifies the password displayed in cipher text for MAC address authentication. ● The user with a fixed name can log in without a password if no password is set. This brings a security risk and is not recommended. ● When a MAC address is used as the user name, the MAC address can be used as the password if no password is set. When local authentication is specified in the AAA authentication scheme, you must set a password. ● If the DHCP option is used as the user name, you must set a password. **NOTE** If fixed user names are configured in the VLANIF interface view, Eth-Trunk interface view or port group view, the password must be set. If a MAC address is configured as the user name in the port group view, the password cannot be set.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** For security purposes, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

Parameter	Description	Value
macaddress	Specifies that the user name in MAC address authentication is the MAC address.	-
format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** }	Specifies the MAC address format. - **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 00e0-fc1c-02e3. - **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-e0-fc-1c-02-e3. - **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 00e0:fc1c:02e3. - **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:e0:fc:1c:02:e3. - **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 00e0fc1c02e3.	-
uppercase	Indicates that the name of a MAC address authentication user is in uppercase.	-

Parameter	Description	Value
dhcp-option *option-code*	Specifies the name of the MAC address authentication user to a specified DHCP option. ● **circuit-id**: Specifies the circuit ID in the DHCP Option82 field as the user name in MAC address authentication. ● **remote-id**: Specifies the remote ID in the DHCP Option82 field as the user name in MAC address authentication. If both **circuit-id** and **remote-id** are configured, the user name for MAC address authentication can be set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field. **NOTE** In VLANIF interface view, the parameter does not support.	The value is an integer. In the current version, the value is fixed as 82.
separate *separate*	Specifies the delimiter in the user name for MAC address authentication. This parameter is configured when the user name for MAC address authentication is set to a character string that is a combination of the **circuit-id** and **remote-id** in the DHCP Option82 field.	The value is a character and can be set to a letter, digit, or another valid character.
format-hex	Indicates that the user name for MAC address authentication is in hexadecimal format.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

MAC address authentication uses three user name formats:

- When the MAC address is used as the user name for MAC address authentication, the password can be the MAC address or a self-defined character string.
- When the fixed user name is used for MAC address authentication, the user uses the fixed user name and password set by the administrator for authentication.
- When the DHCP option format is used for MAC address authentication, the device uses the DHCP option it obtains and password set by the administrator for authentication. In this mode, ensure that the device supports MAC address authentication triggered through DHCP packets.

By default, the device uses the user's MAC address as the user name and password, and sends the MAC address to the authentication server for authentication. Therefore, it is inconvenient to identify and manage users. You can run the **mac-authen username** command to configure the fixed name and password for MAC address authentication users, which facilities user identification and management.

NOTE

When the user names for MAC address authentication are in the DHCP option format, the DHCP Option82 cannot be configured in the extend format or a customized format (non-character string) by using the **dhcp option82 format** command.

When the user name format in MAC address authentication is configured, ensure that the authentication server supports this format.

Example

Configure the user name to **vipuser** and the password to **pass123** for MAC address authentication.

```
<HUAWEI> system-view
[HUAWEI] mac-authen username fixed vipuser password cipher pass123
```

13.6.106 parameter

Function

The **parameter** command configures the characters used in URL.

The **undo parameter** command restores the default settings.

By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&).

Format

parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

undo parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

Parameters

Parameter	Description	Value
start-mark *parameter-value*	Specifies the start character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
assignment-mark *parameter-value*	Specifies the assignment character for URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
isolate-mark *parameter-value*	Specifies the delimiter between URL parameters.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

You can run the **parameter** command to modify the characters in URLs.

For example, in a Portal server template, a user with IP address 10.1.1.11 and MAC address 00e0-fc02-0002 is configured to be authenticated by an access device with the system name of **test**. By default, the start character of URL parameters is a question mark (?), the assignment character of URL parameters is an equal sign (=), and the delimiter between URL parameters is an ampersand (&). When default settings are used, the access device redirects the user to the URL http://10.1.1.1?user_mac=00e0-fc02-0002&user_ip=10.1.1.11&sysname=test. However, the device does not support question marks (?) in the **url (URL template view)** command configuration. To resolve this problem, replace the question mark (?) in the URL with another character in the **url (URL template view)** configuration, and run the **parameter start-mark** *parameter-value* command to specify this replacement character as the start character of URL parameters. In the following example, the replacement character is a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1#user_mac=00e0-
fc02-0002&user_ip=10.1.1.11&sysname=test
[HUAWEI-url-template-test] parameter start-mark #
```

Alternatively, you can run the **url** command in the URL template view to set the URL to **http://10.1.1.1**, and run the **url-parameter** command to add parameters such as the user MAC address, user IP address, and device system name to the URL. In this case, the **parameter** command does not need to be configured.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1
[HUAWEI-url-template-test] url-parameter sysname test user-ipaddress 10.1.1.11 user-mac 00e0-
fc02-0002
```

Example

Set the start character for URL parameters to a number sign (#).

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] parameter start-mark #
```

13.6.107 port connection-type access

Function

The **port connection-type access** command configures the specified interfaces as downlink interfaces.

The **undo port connection-type access** command configures the specified interfaces as uplink interfaces.

Format

port { *interface-type start-interface-number* [**to** *interface-type end-interface-number*] } &<1-10> **connection-type access**

undo port { *interface-type start-interface-number* [**to** *interface-type end-interface-number*] } &<1-10> **connection-type access**

Parameters

Parameter	Description	Value
interface-type start-interface-number [**to** *interface-type end-interface-number*]	Specifies interfaces. ● *interface-type* specifies the interface type. ● *start-interface-number* specifies the number of the first interface. ● *end-interface-number* specifies the number of the last interface. If the **to** *interface-type end-interface-number* parameter is not specified, only the interfaces specified by *start-interface-number* are created. You can specify 10 interface ranges at one time.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, downlink interfaces are access ones and uplink interfaces are non-access ones. You can run the **port connection-type access** or **undo port connection-type access** command to modify the interface access type. For example, you can batch configure the downlink interfaces supported by the device, and run the **dot1x mac-bypass access-port** command to enable MAC address bypass authentication on all the downlink interfaces.

After the default interface access type is modified, the device generates the interface buildrun information in the system view.

Precautions

If stack interface information exists within the interface range, the command does not take effect. Therefore, there should be no interface with stack configuration in the interface range. If the access type of an interface is changed, stack configuration cannot be performed for the interface. That is, if an interface needs to be configured as a stack interface, the default interface access type cannot be modified.

Example

Configure interfaces as downlink interfaces in the system view.

```
<HUAWEI> system-view
[HUAWEI] port GigabitEthernet 0/0/1 to GigabitEthernet 0/0/6 connection-type access
```

13.6.108 port (Portal server template view)

Function

The **port** command sets the port number that a Portal server uses to receive notification packets from the device.

The **undo port** command restores the default port number.

By default, a Portal server uses port number 50100 to receive packets from the device.

Format

port *port-number* [**all**]

undo port [**all**]

Parameters

Parameter	Description	Value
port-number	Specifies the port number that the Portal server uses to receive and encapsulate UDP packets from the device.	The value is an integer that ranges from 1 to 65535. By default, the value is 50100.
all	Indicates that the device always uses the destination port number specified by **port-number** to encapsulate UDP packets. **NOTE** After this keyword is specified, when receiving UDP packets from a Portal server, the device does not obtain the source port number in the UDP packets as the destination port number of UDP packets to be sent to the Portal server. If the value of *port-number* is different from the source port number of the Portal server, the Portal server cannot receive the UDP packets sent by the device. Therefore, this keyword is not recommended.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server** command, configure parameters for the template.

Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device. After receiving a Portal authentication request packet from a user, the device sends the packet to the Portal server using the specified destination port number.

Precautions

Ensure that the port number configured on the device is the same as that used by the Portal server.

Example

Set the port number that a Portal server uses to receive packets from the device to 10000 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] port 10000
```

13.6.109 portal auth-network

Function

The **portal auth-network** command configures a source subnet for Portal authentication.

The **undo portal auth-network** command restores the default source subnet for Portal authentication.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies the IP address of the source subnet for Portal authentication.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 1 to 32.
mask-address	Specifies the mask of the source subnet for Portal authentication.	The value is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

Views

GE interface view, MultiGE interface viewXGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk, interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source subnet for Portal authentication is configured, only user packets from the source subnet can trigger Portal authentication. If an unauthenticated user is not on the source subnet for Portal authentication, the device discards the user's packets that do not match Portal authentication free rules.

NOTE

The command cannot be run on Layer 2 interfaces.

The **portal auth-network** command takes effect only for Layer 3 Portal authentication. In Layer 2 authentication, users on all network segments must be authenticated.

Prerequisites

Before running this command on an interface, ensure that the Portal service template is bound to the interface.

Example

Set the source subnet for Portal authentication to 192.168.1.0/24 on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] server-ip 10.1.1.1
[HUAWEI-web-auth-server-test] quit
```

```
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] web-auth-server test layer3
[HUAWEI-Vlanif10] portal auth-network 192.168.1.0 24
```

Set the source subnet for Portal authentication to 192.168.1.0/24 on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] server-ip 10.1.1.1
[HUAWEI-web-auth-server-test] quit
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] web-auth-server test layer3
[HUAWEI-GigabitEthernet0/0/1] portal auth-network 192.168.1.0 24
```

13.6.110 portal domain

Function

The **portal domain** specifies a forcible Portal authentication domain.

The **undo portal domain** command deletes a forcible Portal authentication domain.

By default, no forcible Portal authentication domain is specified.

Format

portal domain *domain-name*

undo portal domain

Parameters

Parameter	Description	Value
domain-name	Specifies the forcible Portal authentication domain.	The value is a string of 1 to 64 case-insensitive characters without any space, asterisk (*), question mark (?), or quotation mark (").

Views

GE interface view,MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

To flexibly deploy access policies for Portal authentication users, the administrator can run the **portal domain** command to configure a forcible Portal authentication domain.

After a forcible Portal authentication domain is configured on an interface, the device uses the specified authentication domain to authenticate, authorize, and charge Portal authentication users on the interface, ignoring the domain names carried in the user names. The administrator can specify different authentication domains for different interfaces as needed.

NOTE

The command cannot be run on Layer 2 interfaces.

Example

Set the forcible Portal authentication domain to **abc** on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] portal domain abc
```

Set the forcible Portal authentication domain to **abc** on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] portal domain abc
```

13.6.111 portal free-rule

Function

The **portal free-rule** command configures the Portal authentication-free rule for users.

The **undo portal free-rule** command restores the default configuration.

By default, no Portal authentication-free rule is configured.

Format

portal free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } *

portal free-rule *rule-id* **source ip** *ip-address* **mask** { *mask-length* | *ip-mask* } [**mac** *mac-address*] [**interface** *interface-type interface-number*] **destination user-group** *group-name*

undo portal free-rule { *rule-id* | **all** }

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of the Portal authentication-free rule.	The value is an integer of which the range depends on product models.
destination	Specifies the destination network resources that the authentication-free users can access.	-
source	Specifies the source information of the authentication-free users.	-
any	Specifies any condition. When **any** is used together with different keywords, the effect of the command is different.	-
ip *ip-address*	Specifies the IP address in the rule. This parameter can specify the source or destination address depending on the keyword.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of an IP address. This parameter can specify the source or destination address mask depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the IP address mask. This parameter can specify the source or destination address mask depending on the keyword.	The value is in dotted decimal notation.
tcp destination-port *port*	Specifies the TCP destination port number.	The value is an integer that ranges from 1 to 65535.
udp destination-port *port*	Specifies the UDP destination port number.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the source interface in the rule. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies the VLAN ID of the source packet in the rule.	The value is an integer that ranges from 1 to 4094.
all	Specifies all rules.	-
mac *mac-address*	Specifies the MAC address of the Portal authentication user who is allowed to access destination network resources without authentication.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
user-group *group-name*	Allows Portal authentication users to access the network resources in the user group.	It is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user cannot access the network before being authenticated successfully. You can configure an authentication-free rule for specified users to access certain network resources without passing the Portal authentication. An authentication-free rule can be determined by parameters such as the IP address, MAC address, interface, and VLAN. An authentication-free rule can also be determined by ACL rules. The destination IP address that users can access without authentication can be specified in an authentication-free rule defined by either of the two methods. In addition, the destination domain name that users can access without authentication can be specified in an authentication-free rule defined by ACL.

For example, some authentication users who do not have an authentication account must first log in to the official website of a carrier and apply for a member account, or log in using the account of a third party such as Twitter or

Facebook. This requires that the users can access specified websites before successful authentication. The domain name of a website is easier to remember than the IP address; therefore, the authentication-free rule defined by ACL can be configured to enable the users to access the domain names of websites without authentication.

Precautions

- When multiple authentication-free rules are configured, the system matches the rules one by one.
- If the **vlan** parameter determines where users reside for an authentication-free rule, the Portal server must have been bound to the VLANIF interface of the VLAN using the **web-auth-server (interface view)** command; otherwise, the configured authentication-free rule does not take effect for users in the VLAN.
- If you specify both VLAN and interface when running the **portal free-rule** command, the interface must belong to the VLAN; otherwise, the configuration is invalid.
- If you specify the destination port number in an authentication-free rule, fragmented packets cannot match the rule and cannot be forwarded.
- You can only add or delete rules, but cannot modify the created rules. To modify a rule with a certain *rule-id*, run the **undo portal free-rule** command to delete the rule and re-configure it.
- To allow Portal authentication users to access the network resources in the user group, pay attention to the following points:
  - The user group has been created before it is referenced by the Portal authentication-free rule.
  - The Portal authentication-free rule takes effect only after the referenced user group is enabled.
  - A user can only join one user group. If multiple rules are configured, the rule with the smallest *rule-id* has the highest priority.
  - If multiple rules are applied to a user, the Portal authentication-free rule referencing the user group has the highest priority.
  - The rule of the user group can only contain whitelists. That is, the deny action cannot be used.
  - After configuring authorization for a user using the **destination user-group** *group-name* command, you cannot configure authorization in other modes for the user.

Example

Enable all Portal users to access the network 10.1.1.1/24 without authentication.

```
<HUAWEI> system-view
[HUAWEI] portal free-rule 1 destination ip 10.1.1.1 mask 24 source ip any
```

Add the devices on network segment 10.2.100.0/24 to the user group **static-user**, and allow the devices to access resources on this network segment without authentication.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100
[HUAWEI-acl-adv-3100] rule 5 permit ip source 10.2.100.0 255.255.255.0
[HUAWEI-acl-adv-3100] quit
```

```
[HUAWEI] user-group static-user
[HUAWEI-user-group-static-user] acl-id 3100
[HUAWEI-user-group-static-user] quit
[HUAWEI] user-group static-user enable
[HUAWEI] portal free-rule 0 source ip 10.2.100.0 mask 24 destination user-group static-user
```

13.6.112 portal https-redirect blacklist

Function

The **portal https-redirect blacklist** command adds an address to the HTTPS redirection blacklist. After an address is added to the HTTPS redirection blacklist, HTTPS redirection is not performed for HTTPS access to this address of Portal users.

The **undo portal https-redirect blacklist** command removes an address from the HTTPS redirection blacklist.

By default, no address is added to the HTTPS redirection blacklist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist ip *start-ip-address* [*end-ip-address*]

portal https-redirect blacklist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect blacklist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect blacklist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: - *start-ip-address* specifies the start IPv4 address. - *end-ip-address* specifies the end IPv4 address.	-

Parameter	Description	Value
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: ● *start-ipv6-address* specifies the start IPv6 address. ● *end-ipv6-address* specifies the end IPv6 address.	-
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection blacklist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. To disable HTTPS redirection for HTTPS access to a specified address, run the **portal https-redirect blacklist** command to add this address to the HTTPS redirection blacklist.

Precautions

If an address has been added to the HTTPS redirection whitelist using the **portal https-redirect whitelist** command, this address cannot be added to the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.1.1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ip 10.1.1.1
```

Add FC00::1 to the HTTPS redirection blacklist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist ipv6 FC00::1
```

13.6.113 portal https-redirect blacklist aging-time

Function

The **portal https-redirect blacklist aging-time** command configures the aging time of addresses in the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist aging-time** command restores the default aging time of addresses in the HTTPS redirection blacklist.

By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds, that is, 72 hours.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist aging-time *aging-time*

undo portal https-redirect blacklist aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of addresses in the HTTPS redirection blacklist.	The value is an integer in the range from 30 to 4294967295, in seconds. The default value is 259200 seconds, that is, 72 hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an address (except the address of the Portal server) is added to the HTTPS redirection blacklist, HTTPS access from Portal users to this address does not trigger HTTPS redirection. By default, the aging time of addresses in the HTTPS redirection blacklist is 259200 seconds. When the aging time expires, this address will be removed from the blacklist. You can use the **portal https-redirect blacklist**

aging-time command to adjust the aging time of addresses in the HTTPS redirection blacklist.

Example

Configure the aging time of addresses in the HTTPS redirection blacklist to 86400 seconds, that is, 24 hours.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist aging-time 86400
```

13.6.114 portal https-redirect blacklist packet-rate

Function

The **portal https-redirect blacklist packet-rate** command configures the maximum rate at which a Portal user accesses an address through HTTPS. If the user access rate reaches the maximum, the switch adds the destination address to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist packet-rate** command restores the default maximum rate at which a Portal user accesses an address through HTTPS.

By default, the maximum rate at which a Portal user accesses an address through HTTPS is 40 times per minute.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist packet-rate *packet-rate*

undo portal https-redirect blacklist packet-rate

Parameters

Parameter	Description	Value
packet-rate	Specifies the maximum rate at which a Portal user accesses an address through HTTPS.	The value is an integer in the range from 5 to 600, in times per minutes. The default value is 40.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the rate of packets sent from a Portal user for accessing an address through HTTPS reaches the maximum rate specified by the **portal https-redirect blacklist packet-rate** command, the switch adds the destination address to the HTTPS redirection blacklist. This prevents repeated HTTPS redirection caused by frequent access from malicious users to an address, and therefore saves resources of the switch.

Prerequisites

The function of inserting a JavaScript file during Portal redirection has been enabled using the **portal redirect js enable** command.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum rate at which a Portal user accesses an address through HTTPS to 30 times per minute.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist packet-rate 30
```

13.6.115 portal https-redirect blacklist retry-times interval

Function

The **portal https-redirect blacklist retry-times interval** command configures the maximum number of times and the detection period. Within the detection period, if the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum, the address is added to the HTTPS redirection blacklist.

The **undo portal https-redirect blacklist retry-times interval** command restores the default maximum number of times and the default detection period.

By default, the maximum number of times is 10 and the detection period is 3 minutes.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect blacklist retry-times *retry-times* **interval** *interval*

undo portal https-redirect blacklist retry-times interval

Parameters

Parameter	Description	Value
retry-times	Specifies the maximum number of times.	The value is an integer in the range from 1 to 600. The default value is 10.
interval	Specifies the detection period.	The value is an integer in the range from 1 to 600, in minutes. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the switch redirects the HTTP or HTTPS requests sent from clients to the Portal login page. When the function of inserting a JavaScript file during Portal redirection is enabled on the switch using the **portal redirect js enable** command, the HTTP or HTTPS response packets sent from the switch to clients carry the JavaScript file.

- The clients can be redirected to the Portal login page only after they correctly parse the JavaScript file.
- If a client fails to parse the JavaScript file, the switch adds the destination address to the provisional HTTPS redirection blacklist. HTTP and HTTPS redirection can still be triggered for addresses in the provisional HTTPS redirection blacklist.

The detection period specified in the **portal https-redirect blacklist retry-times interval** command starts from the time when an address is added to the provisional HTTPS redirection blacklist. If the number of times an address is added to the provisional HTTPS redirection blacklist reaches the maximum within the detection period, this address is added to the HTTPS redirection blacklist.

Precautions

This command takes effect only for the HTTPS protocol.

This command takes effect for both IPv4 and IPv6 addresses.

Example

Set the maximum number of times to 15 and the detection period to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect blacklist retry-times 15 interval 5
```

13.6.116 portal https-redirect whitelist

Function

The **portal https-redirect whitelist** command adds an address to the HTTPS redirection whitelist.

The **undo portal https-redirect whitelist** command removes an address from the HTTPS redirection whitelist.

By default, no address is added to the HTTPS redirection whitelist.

NOTE

Only the following switch models support this command:

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-I, S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

Format

portal https-redirect whitelist ip *start-ip-address* [*end-ip-address*]

portal https-redirect whitelist ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]

undo portal https-redirect whitelist ip { *start-ip-address* [*end-ip-address*] | **all** }

undo portal https-redirect whitelist ipv6 { *start-ipv6-address* [**to** *end-ipv6-address*] | **all** }

Parameters

Parameter	Description	Value
ip *start-ip-address* [*end-ip-address*]	Specifies an IPv4 address or an IPv4 address range: ● *start-ip-address* specifies the start IPv4 address. ● *end-ip-address* specifies the end IPv4 address.	-

Parameter	Description	Value
ipv6 *start-ipv6-address* [**to** *end-ipv6-address*]	Specifies an IPv6 address or an IPv6 address range: ● *start-ipv6-address* specifies the start IPv6 address. ● *end-ipv6-address* specifies the end IPv6 address.	-
all	Removes all IPv4 addresses or IPv6 addresses from the HTTPS redirection whitelist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before users pass Portal authentication, HTTPS access to a website other than the Portal server triggers HTTPS redirection by default. If an address is added to the HTTPS redirection blacklist by mistake, HTTPS access to this address will not trigger HTTPS redirection. To ensure that HTTPS redirection is performed for HTTPS access to specified addresses, use the **portal https-redirect whitelist** command to add these addresses to the HTTPS redirection whitelist.

Configuration Impact

If an address has been added to the HTTPS redirection whitelist, this address cannot be added to the HTTPS redirection blacklist using the **portal https-redirect blacklist** command.

Precautions

If an address in the HTTPS redirection blacklist is added to the HTTPS redirection whitelist, the switch removes the address from the HTTPS redirection blacklist.

If an address (except the address of the Portal server) is not in the HTTPS redirection blacklist, HTTPS access to this address will always trigger HTTPS redirection before users pass Portal authentication.

Example

Add 10.1.2.1 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ip 10.1.2.1
```

Add FC00::2 to the HTTPS redirection whitelist.

```
<HUAWEI> system-view
[HUAWEI] portal https-redirect whitelist ipv6 FC00::2
```

13.6.117 portal logout different-server enable

Function

The **portal logout different-server enable** command configures a device to process user logout requests sent by a Portal server other than the one from which users log in.

The **undo portal logout different-server enable** command restores the default configuration.

By default, a device does not process user logout requests sent by Portal servers other than the one from which users log in.

Format

portal logout different-server enable

undo portal logout different-server enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where Portal server load balancing is configured, by default, a device does not process user logout requests sent by Portal servers other than the one from which users log in and responds ACK messages only to the Portal server from which users log in. Users in arrears then can still stay online. To prevent this problem, run **portal logout different-server enable** command to configure the device to process user logout requests sent by a Portal server other than the one from which users log in. Upon receipt of a user logout request from such a Portal server, the device starts a user logout process. After completing the logout event, the device responds an ACK message to the Portal server, thereby ensuring that the user logs out properly.

Precautions

The user logout requests that a device can process must be sent by Portal servers bound to an access interface. These servers include all the Portal servers configured in the master and backup Portal server templates bound to the interface.

Example

Enable a device to process user logout requests a Portal server other than the one from which users log in.

```
<HUAWEI> system-view
[HUAWEI] portal logout different-server enable
```

13.6.118 portal logout resend timeout

Function

The **portal logout resend timeout** command configures the re-transmission times and interval for the Portal authentication user logout packet.

The **undo portal logout resend timeout** command restores the default setting.

By default, the Portal authentication user logout packet can be re-transmitted three times within five seconds.

Format

portal logout resend *times* **timeout** *period*

undo portal logout { **resend** | **timeout** } *

Parameters

Parameter	Description	Value
times	Specifies the number of re-transmission times for the Portal authentication user logout packet.	The value is an integer that ranges from 0 to 15. The value 0 indicates that the re-transmission function is disabled.
period	Specifies the re-transmission interval of the Portal authentication user logout packet.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After disconnecting a Portal authentication user, the device sends a user logout packet (NTF-LOGOUT) to instruct the Portal server to delete the user information. If the network between the device and Portal server is not stable or packets are lost, the Portal server may fail to receive the user logout packet from the device after the Portal authentication user is disconnected. In this case, the user is displayed as disconnected on the device but still as online on the Portal server. To enable the Portal server to receive the user logout packet and ensure that the online user information on the Portal server is correct, the administrator can enable the user logout packet re-transmission function on the device and configure the re-transmission times and interval.

Example

Configure the re-transmission times to 5 and interval to 10 seconds for the Portal authentication user logout packet.

```
<HUAWEI> system-view
[HUAWEI] portal logout resend 5 timeout 10
```

13.6.119 portal max-user

Function

The **portal max-user** command sets the maximum number of concurrent Portal authentication users allowed to access the device.

The **undo portal max-user** command restores the default maximum number of concurrent Portal authentication users.

By default, the number of Portal authentication users is the maximum number of Portal authentication users supported by the device.

Format

portal max-user *user-number*

undo portal max-user

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of concurrent Portal users.	The value is an integer that varies depending on product models.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **portal max-user** command to set the maximum number of concurrent Portal authentication users.

Example

Set the maximum number of concurrent Portal authentication users to 25.

```
<HUAWEI> system-view
[HUAWEI] portal max-user 25
```

13.6.120 portal quiet-period

Function

The **portal quiet-period** command enables the quiet timer for Portal authentication.

The **undo portal quiet-period** command disables the quiet timer of Portal authentication.

By default, the quiet timer for Portal authentication is enabled.

Format

portal quiet-period

undo portal quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer for Portal authentication. If the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. During the quiet period, the device discards Portal authentication requests from the user. This prevents the impact of frequent authentications on the system.

The quiet period for Portal authentication can be set using the **portal timer quiet-period** command. After the quiet period is reached, the device re-authenticates the user.

Example

Enable the quiet timer for Portal authentication.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-period
```

13.6.121 portal quiet-times

Function

The **portal quiet-times** command sets the maximum number of authentication failures within 60s before a Portal authentication user is kept in quiet state.

The **undo portal quiet-times** command restores the default maximum number of authentication failures within 60s before a Portal authentication user enters the quiet state.

By default, the device allows a maximum of ten authentication failures within 60s before a Portal authentication user enters the quiet state.

Format

portal quiet-times *fail-times*

undo portal quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a Portal authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer, if the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. This prevents the impact of frequent authentications on the system.

Example

Set the maximum number of Portal authentication failures within 60 seconds to 4.

```
<HUAWEI> system-view
[HUAWEI] portal quiet-times 4
```

13.6.122 portal redirect js enable

Function

The **portal redirect js enable** command enables the function of inserting a JavaScript file during Portal redirection.

The **undo portal redirect js enable** command disables the function of inserting a JavaScript file during Portal redirection.

By default, the function of inserting a JavaScript file during Portal redirection is disabled.

Format

portal redirect js enable

undo portal redirect js enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before Portal users are authenticated, the device redirects the HTTP or HTTPS requests sent from clients to the Portal server. To prevent heavy burdens on the server caused by a large number of HTTP or HTTPS requests sent from the clients and to ensure proper display of the Portal login page, enable the function of inserting a JavaScript file during Portal redirection. After this function is enabled, the HTTP or HTTPS response packets sent from the server carry a JavaScript file. The client browser parses the JavaScript file for redirection, and then performs Portal authentication.

Precautions

The client browser must support and enable the JavaScript function.

Example

Enable the function of inserting a JavaScript file during Portal direction.

```
<HUAWEI> system-view
[HUAWEI] portal redirect js enable
```

13.6.123 portal timer offline-detect

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a Portal user goes offline due to power failure or network interruption, the device and Portal server may still store the user information, which causes incorrect accounting. Additionally, a limit number of users can access the device. If a user goes offline improperly but the device still stores user information, other users cannot access the network.

After the Portal user offline detection interval is set, if the user does not respond within the interval, the device considers the Portal user offline. The device and Portal server then delete the user information and release resources to ensure an efficient resource use.

Precautions

This command only applies to Layer 2 Portal authentication. When the configuration is changed, the new configuration takes effect only for new access users.

The heartbeat detection function of the authentication server can be used to ensure the normal online status of PC users for whom Layer 3 Portal authentication is used. If the authentication server detects that a user goes offline, it instructs the device to disconnect the user.

If the number of offline detection packets (ARP packets) exceeds the default CAR value, the detection fails and the users are logged out. (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.) To resolve the problem, the following methods are recommended:

- Increase the detection interval based on the number of users. The default detection interval is recommended when there are less than 8000 users; the detection interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

If user traffic (such as service packets) passes through the device within the Portal user offline detection period, the device does not consider the user offline even if the user does not respond.

Example

Set the Portal user offline detection interval to 400s.

```
<HUAWEI> system-view
[HUAWEI] portal timer offline-detect 400
```

13.6.124 portal timer quiet-period

Function

The **portal timer quiet-period** command sets the quiet period for Portal authentication.

The **undo portal timer quiet-period** command restores the default quiet period for Portal authentication.

By default, the quiet period for Portal authentication is 60s.

Format

portal timer quiet-period *quiet-period-value*

undo portal timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Specifies the quiet period for Portal authentication.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer, run the **portal timer quiet-period** command to set the quiet period for Portal authentication. If a Portal authentication user is kept in quiet state, the device discards Portal authentication requests from the user during the quiet period.

Example

Set the quiet period to 2000s.

```
<HUAWEI> system-view
[HUAWEI] portal timer quiet-period 2000
```

13.6.125 portal url-encode enable

Function

The **portal url-encode enable** command enables URL encoding and decoding.

The **undo portal url-encode enable** command disables URL encoding and decoding.

By default, URL encoding and decoding are enabled.

Format

portal url-encode enable

undo portal url-encode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. To enable URL encoding and decoding, run the **portal url-encode enable** command. Some special characters in redirect URLs are then converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented.

Precautions

After the URL encoding and decoding function is enabled, some servers may not support the escape characters converted from special characters in redirect URLs. Therefore, check whether servers support the escape characters before configuring special characters in redirect URLs.

Example

Enable URL encoding and decoding.

```
<HUAWEI> system-view
[HUAWEI] portal url-encode enable
```

13.6.126 portal user-alarm percentage

Function

The **portal user-alarm percentage** command sets alarm thresholds for the Portal authentication user count percentage.

The **undo portal user-alarm percentage** command restores the default alarm thresholds for the Portal authentication user count percentage.

By default, the lower alarm threshold for the Portal authentication user count percentage is 50, and the upper alarm threshold for the Portal authentication user count percentage is 100.

Format

portal user-alarm percentage *percent-lower-value percent-upper-value*

undo portal user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **portal max-user** command to set the maximum number of online Portal authentication users allowed on a device, you can run the **portal user-alarm percentage** command to set alarm thresholds for the Portal authentication user count percentage.

When the percentage of online Portal authentication users against the maximum number of users allowed by the device exceeds the upper alarm threshold, the device generates an alarm. When the percentage of online Portal authentication users against the maximum number of users allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

If the configured upper alarm threshold for the Portal authentication user count percentage is 100, the device generates an alarm when the number of online users reaches the maximum number of users allowed by the device.

Example

Set the lower alarm threshold for the Portal authentication user count percentage to 30, and the upper alarm threshold for the Portal authentication user count percentage to 80.

```
<HUAWEI> system-view
[HUAWEI] portal user-alarm percentage 30 80
```

13.6.127 portal web-authen-server

Function

The **portal web-authen-server** command enables the Portal interconnection function of the HTTP or HTTPS protocol.

The **undo portal web-authen-server** command disables the Portal interconnection function of the HTTP or HTTPS protocol.

By default, the Portal interconnection function of the HTTP or HTTPS protocol is disabled.

Format

portal web-authen-server { **http** | **https ssl-policy** *policy-name* } [**port** *port-number*]

undo portal web-authen-server [**port**]

Parameters

Parameter	Description	Value
http	Sets the HTTP protocol for Portal authentication. **NOTE** The HTTP protocol poses security risks. The HTTPS protocol is recommended.	-
https	Sets the HTTPS protocol for Portal authentication.	-
ssl-policy *policy-name*	Specifies the name of an SSL policy.	The value must be the name of an existing SSL policy.
port *port-number*	Specifies a port number.	The value is an integer that ranges from 1025 to 55535. The default HTTP port number is 8000 and the default HTTPS port number is 8443.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to the Portal server that only supports the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable the Portal interconnection function of the HTTP or HTTPS protocol.

Follow-up Procedure

Run the **protocol** command to set the protocol used in Portal authentication to HTTP or HTTPS.

Precautions

Modifying the **port** parameter causes the pre-connected user to go offline.

Example

Enable the Portal interconnection function of the HTTPS protocol.

```
<HUAWEI> system-view
[HUAWEI] ssl policy huawei
[HUAWEI-ssl-policy-huawei] quit
[HUAWEI] portal web-authen-server https ssl-policy huawei port 8443
```

13.6.128 protocol (Portal server template view)

Function

The **protocol** command configures the protocol used in Portal authentication.

The **undo protocol** command restores the default configuration.

By default, the Portal protocol is used in Portal authentication.

Format

protocol { **http** [**password-encrypt** { **none** | **uam** }] | **portal** }

undo protocol

Parameters

Parameter	Description	Value
http	Sets the protocol used in Portal authentication to HTTP or HTTPS.	-

Parameter	Description	Value
password-encrypt { **none** | **uam** }	Specifies the password encoding mode. ● **none**: The password is not encoded. ● **uam**: The password is encoded using ASCII characters.	-
portal	Sets the protocol used in Portal authentication to Portal.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

In Portal authentication, the device can use the following protocols to communicate with the Portal server. You can set the protocol according to the protocol supported by the Portal server.

- Portal protocol
- HTTP or HTTPS protocol

Example

Set the protocol used in Portal authentication to HTTP or HTTPS.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] protocol http password-encrypt uam
```

13.6.129 remark

Function

The **remark** command configures the user group priority.

The **undo remark** command cancels the user group priority configuration.

By default, no user group priority is configured.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

undo remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the priority for processing Layer 2 Ethernet packets.	The value is an integer that ranges from 0 to 7.
dscp *dscp-value*	Specifies the priority for processing IP packets.	The value is an integer that ranges from 0 to 63.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the user group priority is configured, users in the user group inherit the priority. That is, different user packets have different priorities. In this way, the administrator can manage different types of users more flexibly.

Precautions

When the **remark** and **voice-vlan remark** commands are used together to modify the user packet priority, if the services conflict:

- For S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the priority configured using the **remark** command takes effect.
- For S6720-EI, S6720S-EI, the priority configured using the **voice-vlan remark** command takes effect.

Example

Set the priority for processing IP packets to 3 in the user group **abc**.

```
<HUAWEI> system-view
[HUAWEI] user-group abc
[HUAWEI-user-group-abc] remark dscp 3
```

13.6.130 reset aaa statistics access-type-authenreq

Function

The **reset aaa statistics access-type-authenreq** command clears the number of requesting for MAC, Portal, or 802.1X authentication.

Format

reset aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, and 802.1X authentications.

To clear the number of requesting for MAC, Portal, or 802.1X authentication, run the **reset aaa statistics access-type-authenreq** command.

Example

Clear the number of requesting for MAC, Portal, or 802.1X authentication.

```
<HUAWEI> reset aaa statistics access-type-authenreq
```

13.6.131 reset access-user dot1x-identity statistics

Function

The **reset access-user dot1x-identity statistics** command clears statistics about Identity packets for 802.1X authentication on a switch.

Format

reset access-user dot1x-identity statistics

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To display statistics about Identity packets for 802.1X authentication on a switch within a specified period of time, run the **reset access-user dot1x-identity statistics** command to clear the existing statistics first, and then run the **display access-user dot1x-identity statistics** command to display the new statistics.

Example

Clear statistics about Identity packets for 802.1X authentication on the switch.

```
<HUAWEI> system-view
[HUAWEI] reset access-user dot1x-identity statistics
```

13.6.132 reset access-user traffic-statistics

Function

The **reset access-user traffic-statistics** command clears statistics on traffic of online users in a user group.

NOTE

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this command.

Format

reset access-user traffic-statistics { **user-id** *begin-id* [*end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance*] }

Parameters

Parameter	Description	Value
user-id *begin-id* [*end-id*]	Specifies IDs of online users. - *begin-id* specifies the start ID of online users. - *end-id* specifies the end ID of online users. The value of *end-id* must be equal to or greater than that of *begin-id*. To view IDs of online users, run the **display access-user** command.	The value is an integer that varies depending on the product model.

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of an online user.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
ip-address *ip-address*	Specifies the IP address of an online user.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the VPN instance that an online user belongs to.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

After traffic control is configured for users in a user group using the **car** command, the device collects statistics on traffic of each user in the user group. You can run the **reset access-user traffic-statistics** command to clear statistics on traffic of online users in a user group.

NOTE

After you run the **reset access-user traffic-statistics** command to clear traffic statistics, the cleared user traffic statistics are not included in the accounting packets sent by the device to the accounting server.

Example

Clear statistics on traffic of the user with the IP address as 10.1.1.1.

```
<HUAWEI> reset access-user traffic-statistics ip-address 10.1.1.1
```

13.6.133 reset dot1x statistics

Function

The **reset dot1x statistics** command clears 802.1X authentication statistics.

Format

reset dot1x statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears 802.1X authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, 802.1X authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The 802.1X authentication statistics contain the number of times that the authentication succeeded and failed on an interface and the number of sent and received packets.

The **reset dot1x statistics** command is used in the following scenarios:

- Redeploy services. After the statistics are cleared, collect the 802.1X authentication statistics again, and run the **display dot1x** command to check whether the authentication function works properly and whether packets are correctly sent and received.
- Rectify a fault. After the fault is rectified, run the **reset dot1x statistics** command to clear the statistics, collect the statistics on 802.1X authentication again, and then run the **display dot1x** command to verify the authentication result and check whether packets are correctly sent and received. If the authentication is successful and packets are correctly sent and received, the fault is rectified.

Example

Clear 802.1X authentication statistics on GE0/0/1.

```
<HUAWEI> reset dot1x statistics interface gigabitethernet 0/0/1
```

13.6.134 reset mac-authen statistics

Function

The **reset mac-authen statistics** command clears MAC address authentication statistics.

Format

reset mac-authen statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears MAC address authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, MAC address authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset mac-authen statistics** command is used in the following scenarios:

- Re-deploy services. After the statistics are cleared, collect the MAC address authentication statistics again, and run the **display mac-authen** command to check whether the authentication function is normal.
- Rectify a fault. After the fault is rectified, run the **reset mac-authen statistics** command to clear statistics, collect MAC address authentication statistics again, and run the **display mac-authen** command to check the authentication result. If the authentication is successful, the fault is rectified.

Example

Clear MAC address authentication statistics on GE0/0/1.

```
<HUAWEI> reset mac-authen statistics interface gigabitethernet 0/0/1
```

13.6.135 server-detect

Function

The **server-detect** command enables the Portal server detection function.

The **undo server-detect** command disables the Portal server detection function.

By default, the Portal server detection function is disabled.

Format

server-detect [**interval** *interval-period* | **max-times** *times* | **critical-num** *critical-num* | **action** { **log** | **trap** | **permit-all** } *] *

undo server-detect [**interval** | **max-times** | **critical-num** | **action** { **log** | **trap** | **permit-all** } *]

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the detection interval of the Portal server.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 60.
max-times *times*	Specifies the maximum number of times that the detection fails.	The value is an integer that ranges from 1 to 255. The default value is 3.
critical-num *critical-num*	Specifies the minimum number of Portal servers in Up state.	The value is an integer that ranges from 0 to 128. The default value is 0. The default value is recommended.
action	Specifies the action to be taken after the number of detection failures exceeds the maximum.	-

Parameter	Description	Value
log	Indicates that the device sends a log after the number of detection failures exceeds the maximum.	-
trap	Indicates that the device sends a trap after the number of detection failures exceeds the maximum.	-
permit-all	Cancels Portal authentication on an interface after the number of detection failures exceeds the maximum.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

If the communication is interrupted because the network between the device and Portal server is faulty or the Portal server is faulty, new Portal authentication users cannot go online. This brings great inconvenience to users.

After the Portal server detection function is enabled in the Portal server template, the device detects all Portal servers configured in the Portal server template. If the number of times that the device fails to detect a Portal server exceeds the upper limit, the status of the Portal server is changed from Up to Down. If the number of Portal servers in Up state is less than or equal to the minimum number (specified by the **critical-num** parameter), the device performs the corresponding operation to allow the administrator to obtain the real-time Portal server status or ensure that the users have certain network access rights.

NOTE

The detection interval of the Portal server multiplied by the maximum number of detection failures cannot be less than the keepalive heartbeat interval of the Portal server. It is recommended that the configured detection interval of the Portal server be greater than the keepalive heartbeat interval of the Portal server.

If the Portal server does not support detection, you do not need to configure this command.

Example

Enable the Portal server detection function in the Portal server template abc. Configure the detection interval to 100 seconds, the maximum number of detection failures to 5. Configure the device to send log information when the number of detection failures exceeds the upper limit.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect interval 100 max-times 5 action log
```

13.6.136 server-detect type

Function

The **server-detect type** command configures the mode in which a device detects Portal server status.

The **undo server-detect type** command restores the default Portal server detection mode.

By default, the Portal-based Portal server detection mode is configured.

Format

server-detect type { **portal** | **http** }

undo server-detect type

Parameters

Parameter	Description	Value
portal	Specifies the Portal-based Portal server detection mode.	-
http	Specifies the HTTP-based Portal server detection mode.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Precautions

In Portal-based Portal server detection mode, the Portal server periodically (the time is determined by the server) sends heartbeat packets to the access device, which then determines the server reachability based on the heartbeat packets. If the access device receives Portal heartbeat packets or other authentication packets from the Portal server within the detection interval (configured using **server-detect interval** *interval-period*) and the packets are verified to be correct, the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In HTTP-based Portal server detection mode, the access device periodically sends HTTP packets to the Portal server and expects a response packet from the Portal server. If the access device receives a response packet within the specified detection interval (configured using **server-detect interval** *interval-period*), the detection is successful. Otherwise, the detection fails. When the number of consecutive detection failures reaches the maximum number specified by the **server-detect max-times** *times* command, the access device changes the status of the Portal server from Up to Down.

In Portal-based Portal server detection mode, the Portal server must use the Portal protocol and support sending Portal heartbeat packets. If the Portal server does not meet these requirements, you can configure the HTTP-based detection mode. In this way, if the device detects that the Portal server is Down, the device grants new users the corresponding network access rights.

Precautions

HTTP-based Portal server detection applies to both wireless access scenarios and wired access scenarios using MAC+Portal authentication.

Example

Configure the device to detect Portal server status using HTTP.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] server-detect type http
```

13.6.137 server-ip (Portal server template view)

Function

The **server-ip** command configures an IP address for a Portal server.

The **undo server-ip** command deletes an IP address for a Portal server.

By default, no IP address is configured for a Portal server.

Format

server-ip *server-ip-address* &<1-10>

server-ip ipv6 *server-ipv6-address* &<1-3>

undo server-ip { *server-ip-address* **ipv6** *server-ipv6-address* | **all** }

NOTE

The **ipv6** *server-ipv6-address* parameter is only supported by the following models:

S1720GW-E, S1720GWR-E, S5720S-LI, S5720I-SI, S5736-S, S5735S-H, S6720S-S, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S5735S-L1, S300, S5735-L, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, S5735-S-I, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720-EI, S6720S-EI

Parameters

Parameter	Description	Value
server-ip-address	Specifies an IPv4 address of a Portal server.	The value is in dotted decimal notation.
ipv6 *server-ipv6-address*	Specifies an IPv6 address of a Portal server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
all	Deletes all IP addresses of a Portal server.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server template on the device using the **web-auth-server (system view)** command, configure parameters for the template.

Run the **server-ip** command to configure an IP address for the Portal server in the Portal server template view. When receiving a Portal authentication request packet from a user, the device sends a response packet to the Portal server with the configured IP address.

Precautions

- After the IP address corresponding to a Portal server is configured in the Portal server template, users are allowed to access the IP address.
- When a Portal server template is bound to an interface, server IP addresses can be added, but cannot be deleted. If multiple IP addresses are configured for a Portal server in the Portal server template, you are advised to run the **url (Portal server template view)** command to configure a URL for the Portal server. If no URL is configured, the device uses the first IP address as the URL by default, and the other IP addresses do not take effect.

- When you run the **server-ip** command to specify IPv6 addresses, you must also specify IPv4 addresses. This is because the device does not support IPv6 Portal protocol exchange.

Example

Set the Portal server IP address in the Portal server template **test** to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server huawei
[HUAWEI-web-auth-server-huawei] server-ip 10.10.10.1
```

13.6.138 shared-key (Portal server template view)

Function

The **shared-key** command configures the shared key that the device uses to exchange information with a Portal server.

The **undo shared-key** command restores the default setting.

By default, no shared key that the device uses to exchange information with a Portal server is configured.

Format

shared-key cipher *key-string*

undo shared-key

Parameters

Parameter	Description	Value
cipher	Displays a shared key in cipher text.	-
key-string	Specifies the shared key.	The value is a string of case-sensitive characters without spaces. It can be a string of 20 to 392 characters in cipher text, or a string of 1 to 255 characters in plain text.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a shared key is configured using the **shared-key** command, the Portal packet exchanged between the device and Portal server carries an authenticator generated according to the shared key, and the authenticator is used to check whether the Portal packet at the receiver is correct. This effectively improves the information exchange security.

Precautions

To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

Example

Configure the shared key in the Portal server template **test** to YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] shared-key cipher YsHsjx_202206
```

13.6.139 source-ip (Portal server template view)

Function

The **source-ip** command configures the source IP address for the device to communicate with a Portal server.

The **undo source-ip** command restores the default setting.

By default, no source IP address is configured for the device to communicate with a Portal server.

Format

source-ip *ip-address*

undo source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with a Portal server.	The value is in dotted decimal notation.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication between the device and Portal server, run the **source-ip** command to configure a source IP address on the device.

If the device is configured with a loopback IP address and a common IP address, the device can communicate with the Portal server only when the loopback IP address and common IP address are the same. The **source-ip** command configures a source IP address on the device in the **web-auth-server** view to allow communication between the device and a Portal server.

Precautions

Ensure that the configured source IP address is the device IP address. The source IP address cannot be all 0s, 255.255.255.255, class D address, class E address, or loopback address.

Example

Set the source IP address for communication between the device and a Portal server to 192.168.1.100 in the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] source-ip 192.168.1.100
```

13.6.140 static-user

Function

The **static-user** command configures a static user.

The **undo static-user** command deletes the configured static user.

By default, no static user is configured.

Format

static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*] [**domain-name** *domain-name* | **interface** *interface-type interface-number* [**detect**] | **mac-address** *mac-address* | **vlan** *vlan-id* | **keep-online**] *

undo static-user *start-ip-address* [*end-ip-address*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
start-ip-address [*end-ip-address*]	Specifies the IP address range that a static user belongs to. If *end-ip-address* is not specified, a static user is specified by *start-ip-address*.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that a static user belongs to.	The value must be an existing VPN instance name.
domain-name *domain-name*	Specifies the domain that a static user belongs to.	The value must be an existing domain name.
interface *interface-type interface-number*	Specifies the interface connected to a static user. ● *interface-type* specifies the interface type. **NOTE** A management interface cannot be configured as the interface to which a static user belongs. ● *interface-number* specifies the interface number.	-
detect	Permits the device to send ARP packets to trigger Portal authentication for static users in offline state.	-
mac-address *mac-address*	Specifies the MAC address of a static user.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Specifies the ID of a VLAN that a static user belongs to.	The value is an integer that ranges from 1 to 4094.
keep-online	Keeps a static user online, with offline detection not performed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In network deployment, static IP addresses are assigned to dumb terminals such as printers and servers. These users can be configured as static users for flexible authentication.

After static users are configured, the device can use static user information such as their IP addresses as the user names to authenticate the users only when Portal authentication is enabled on the interfaces connected to the static users.

Precautions

When the interface (**interface** *interface-type interface-number*) mapping static users is specified, the VLAN (**vlan** *vlan-id*) that the interface belongs to must be configured.

This function takes effect only for users who go online after this function is successfully configured.

Example

Specify the IP address range 10.1.1.1-10.1.1.10, authentication domain **test**, and VLAN 10 that static users belong to.

```
<HUAWEI> system-view
[HUAWEI] static-user 10.1.1.1 10.1.1.10 domain-name test vlan 10
```

13.6.141 static-user not-update-ip enable

Function

The **static-user not-update-ip enable** command disables the device from updating IP addresses of static users.

The **undo static-user not-update-ip enable** command allows the device to update IP addresses of static users.

By default, the device cannot update IP addresses of static users.

Format

static-user not-update-ip enable

undo static-user not-update-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After IP addresses for static users are configured, terminals using these IP addresses are authenticated as static users. After these terminals go online, they may send abnormal ARP packets whose source IP addresses are not the IP addresses of static users to the authentication device. After receiving the packets, the device updates terminal IP addresses in CIB entries. As a result, the terminals are no longer static users and go offline. To prevent this problem, you can run the **static-user not-update-ip enable** command to disable the device from updating IP addresses of static users.

Precautions

When the **undo static-user not-update-ip enable** command is configured and the function of identifying static users through IP addresses is enabled, only the function of identifying static users through IP addresses takes effect.

Example

Disable the device from updating IP addresses of static users.

```
<HUAWEI> system-view
[HUAWEI] static-user not-update-ip enable
```

13.6.142 static-user password

Function

The **static-user password** command sets the password for a static user in authentication.

The **undo static-user password** command restores the default password for the static user.

By default, the password for a static user in authentication not set.

Format

static-user password cipher *password*

undo static-user password

Parameters

Parameter	Description	Value
cipher	Displays a password in cipher text.	-
password	Specifies the password of a static user.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a static user triggers authentication through an ARP packet, you can run the **static-user password** command to set the password for the static user. The access device then sends the password to the authentication server.

Precautions

To improve security, change the default password immediately and update the password periodically. It is recommended that the new password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

This function takes effect only for users who go online after this function is successfully configured.

Example

Configure the password **YsHsjx_202206** for static users.

```
<HUAWEI> system-view
[HUAWEI] static-user password cipher YsHsjx_202206
```

13.6.143 static-user username format-include

Function

The **static-user username format-include** command sets the user name for a static user in authentication.

The **undo static-user username format-include** command restores the default user name for the static user.

By default, the name of a static user consists of **system-name** and **ip-address**. For example, if the access device name is **test** and user IP address is 1.1.1.1, the static user name is **test1.1.1.1**.

Format

static-user username format-include { **ip-address** | **mac-address** | **system-name** }

undo static-user username format-include

Parameters

Parameter	Description	Value
ip-address	Indicates that the user IP address is used as the user name.	-
mac-address	Indicates that the user MAC address is used as the user name.	-
system-name	Indicates that the access device name is used as the user name. To set the device name, run the **sysname** command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a static user triggers authentication through an ARP packet, you can run the **static-user username format-include** command to set the user name for the static user. The access device then sends the user name to the authentication server.

Example

Set the user IP address as the static user name for authentication.

```
<HUAWEI> system-view
[HUAWEI] static-user username format-include ip-address
```

13.6.144 static-user username macaddress format

Function

The **static-user username macaddress format** command sets the user name for authenticating a static user to a MAC address.

The **undo static-user username macaddress format** command restores the default setting.

By default, the user name for authenticating a static user is not set to a MAC address.

Format

static-user username macaddress format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password-with-macaddress**]

undo static-user username macaddress format

Parameters

Parameter	Description	Value
with-hyphen [**normal**] [**colon**] | **without-hyphen**	Specifies the format of a MAC address. - **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 0005-e01c-02e3. - **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-05-e0-1c-02-e3. - **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 0005:e01c:02e3. - **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:05:e0:1c:02:e3. - **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 0005e01c02e3.	-
uppercase	Configures a MAC address in uppercase format as the user name for authentication. If this parameter is not specified, a MAC address in lowercase format is used.	-

Parameter	Description	Value
password-with-macaddress	Configures a MAC address as the password. If this parameter is not specified, the password configured in the **static-user password cipher** *password* command is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In network deployment, static IP addresses are assigned to dumb terminals such as printers, that is, their users are configured as static users. To authenticate a static user, you can run this command to set the user name and password for authentication to a MAC address. This command takes priority over the **static-user username format-include** { **ip-address** | **mac-address** | **system-name** } command and **static-user password cipher** *password* command.

Example

Set the MAC address with hyphens (-) as the user name and password for authenticating a static user.

```
<HUAWEI> system-view
[HUAWEI] static-user username macaddress format with-hyphen password-with-macaddress
```

13.6.145 url (Portal server template view)

Function

The **url** command configures a URL for a Portal server.

The **undo url** command restores the default configuration.

By default, no URL is configured for a Portal server.

Format

url *url-string*

undo url

Parameters

Parameter	Description	Value
url-string	Specifies a URL for a portal server.	The value is a string of 1 to 247 characters.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IP address of a Portal server is configured using the **server-ip** command (in the Portal server template view), the Portal server URL (http://*server-ip*) is generated by default on the device. If the actual URL of the Portal server is inconsistent with the default one or the domain name of the Portal server needs to be used for network access, you can run the **url** command to modify the URL of the Portal server on the device.

Precautions

- A Portal server has only one URL.

Example

Set the URL of a Portal server to http://www.***.com in the Portal server template named **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url http://www.***.com
```

13.6.146 url (URL template view)

Function

The **url** command configures a redirect URL or pushed URL.

The **undo url** command cancels a redirect URL or pushed URL.

By default, no redirect URL or pushed URL is configured.

Format

url [**push-only** | **redirect-only**] *url-string*

undo url [**push-only** | **redirect-only**]

Parameters

Parameter	Description	Value
url-string	Specifies a redirect URL or pushed URL.	The value is a string of 1 to 247 case-sensitive characters without spaces.
push-only	Specifies the URL only as a pushed URL.	-
redirect-only	Specifies the URL only as a redirect URL.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **url-template name** command, you can run this command to configure the redirect URL or pushed URL. When a user without network access permission connects to the network, the Portal authentication device redirects the user to the specified URL for authentication. The difference between a redirect URL and a pushed URL is as follows:

- Redirect URL: When a user without network access permission attempts to access the network, the Portal authentication device redirects the user to the redirect URL for authentication.
- Pushed URL: After an authenticated user accesses the network through web for the first time, the access device pushes the web page corresponding to the URL to the user. The web access request from the user is redirected to the specified URL, and then the user is allowed to access network resources.

Precautions

When you configure a URL on the device, question marks (?) are not supported. If a URL contains a question mark (?), you can run the **parameter start-mark #** command in the URL template view to replace the question mark (?) with a number sign (#).

If the **push-only** and **redirect-only** parameters are not specified, the configured URL is used as both a redirect URL and a pushed URL. You can configure pushed URL using the **force-push** command, or use the **url-template** command to bind a URL template to the Portal server template to configure redirect URL.

Example

Set the redirect URL to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url http://10.1.1.1
```

13.6.147 url-parameter

Function

The **url-parameter** command sets parameters in a URL.

The **undo url-parameter** command deletes parameters in a URL.

By default, a URL does not carry any parameters.

Format

url-parameter { **redirect-url** *redirect-url-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **login-url** *url-key url* } *

undo url-parameter

Parameters

Parameter	Description	Value
redirect-url *redirect-url-value*	Specifies the original URL that a user accesses in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.
user-ipaddress *user-ipaddress-value*	Specifies the user IP address carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.
sysname *sysname-value*	Specifies the device system name carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.
user-mac *user-mac-value*	Specifies the user MAC address carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces.

Parameter	Description	Value
login-url *url-key url*	Specifies the login URL of an access device. - *url-key*: specifies the identification keyword for the login URL sent to the Portal server during redirection. - *url*: is a specified URL on the access device.	- *url-key*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). - *url*: The value is a string of 1 to 247 case-sensitive characters without spaces.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

After a URL template is created using the **url-template name** command and URL is configured using the **url** command, you can use the **url-parameter** command to set the parameters in the URL. When a user accesses the Portal server according to the URL, the Portal server obtains user terminal information through the parameters in the URL. The Portal server then provides the corresponding web authentication page for the user according to user terminal information.

In addition, when users are redirected to a website rather than the Portal server according to the pushed URL, the website provides different web pages for the users according to user terminal information carried in the URL.

Example

Set the user MAC address and access device's system name in the URL.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter user-mac usermac sysname test
```

13.6.148 url-parameter mac-address format

Function

The **url-parameter mac-address format** command configures the MAC address format in URL.

The **undo url-parameter mac-address format** command restores the default MAC address format in URL.

By default, the MAC address format in URL is XXXXXXXXXXXX.

Format

url-parameter mac-address format delimiter *delimiter* { **normal** | **compact** }

undo url-parameter mac-address format

Parameters

Parameter	Description	Value
delimiter *delimiter*	Specifies the delimiter in MAC address.	The value is one case-sensitive character. It cannot be a space, quotation mark ("), or question mark (?).
normal	Sets the MAC address format to XX-XX-XX-XX-XX-XX.	-
compact	Sets the MAC address format to XXXX-XXXX-XXXX.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Portal servers or websites may require different MAC address formats. You can run the **url-parameter mac-address format** command to set MAC address formats in URL to meet the requirements of Portal servers.

Example

Set the delimiter to - and format to XXXX-XXXX-XXXX.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
[HUAWEI-url-template-test] url-parameter mac-address format delimiter - compact
```

13.6.149 url-template (Portal server template view)

Function

The **url-template** command binds a URL template to a Portal server template.

The **undo url-template** command unbinds a URL template from a Portal server template.

By default, no URL template is bound to a Portal server template.

Format

url-template *url-template* [**ciphered-parameter-name** *ciphered-parameter-name* **iv-parameter-name** *iv-parameter-name* **key cipher** *key-string*]

undo url-template

Parameters

Parameter	Description	Value
url-template	Specifies the name of a URL template.	The value must be an existing URL template name.
ciphered-parameter-name *ciphered-parameter-name*	Specifies the name of the encrypted URL template parameter.	The value is a string of 1 to 16.
iv-parameter-name *iv-parameter-name*	Specifies the encryption vector name of the URL template parameter.	The value is a string of 1 to 16.
key cipher *key-string*	Specifies the shared key for encrypting the URL template parameter.	The value is a string of 1-16 plain-text characters or 48 cipher-text characters.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the parameters of a URL template are configured, the URL template must be bound to a Portal authentication server template so that users can be authenticated on the Portal authentication server corresponding to the redirect URL.

To ensure security, you can encrypt the parameter information in the URL template bound to the Portal server template.

Prerequisites

A URL template has been created using the **url-template name** command.

Precautions

If a URL template is bound to the Portal authentication server template and the **url** command is executed to configure the redirect URL corresponding to the Portal authentication server, only the parameters in the URL template take effect.

The device support encryption of parameter information in the URL template only when it connects to the Huawei Agile Controller-Campus or iMaster NCE-Campus.

Example

Bind the URL template **abc** to the Portal authentication server template.

```
<HUAWEI> system-view
[HUAWEI] url-template name abc
[HUAWEI-url-template-abc] quit
[HUAWEI] web-auth-server test
[HUAWEI-web-auth-server-test] url-template abc
```

13.6.150 url-template name

Function

The **url-template name** command creates a new URL template or enter an existing URL template view.

The **undo url-template name** command deletes a URL template.

By default, no URL template exists on the device.

Format

url-template name *template-name*

undo url-template name *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a URL template.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a Portal authentication server template is created using the **web-auth-server** command, you can bind a URL template to the Portal authentication server template. The URL template contains the redirect URL and redirect URL parameters.

The **url-template name** command creates a new URL template or enter an existing URL template view.

Example

Create a URL template named **test** and enter the template view.

```
<HUAWEI> system-view
[HUAWEI] url-template name test
```

13.6.151 user-group

Function

The **user-group** command creates a user group or displays the user group view.

The **undo user-group** command deletes a user group.

By default, no user group is configured.

Format

user-group *group-name*

undo user-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The value is a string of 1-64 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practical NAC applications, there are many access users and a large number of ACL rules need to be configured for each user. However, the number of user types is limited.

You can run the **user-group** command to create user groups on the device and associate each user group to a group of ACL rules (for details, see **acl-id**). In this way, users in the same group share a group of ACL rules. The limited ACL resources can support a large number of access users.

NOTE

When the user group function is enabled on models except the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, ACL rules are delivered to each user and the user group function cannot be used to save ACL resources.

Precautions

- When you create a user group, ensure that the user group name is different from the number of an existing ACL. You can run the **display acl all** command to view the configuration of all ACL rules on the device.
- If you want to delete the user group when the ACL bound to the user takes effect, run the **cut access-user user-group** *group-name* command to disconnect all users bound to the user group, and run the **undo user-group** *group-name* **enable** command to disable the user group function.
- The priority of the user group authorization information delivered by the authentication server is higher than that of the user group authorization information applied in the AAA domain. If the user group authorization information delivered by the authentication server cannot take effect, the user group authorization information applied in the AAA domain is used. For example, if only user group B is configured on the device and the group authorization information is applied in the AAA domain when the authentication server delivers authorization information about user group A,

the authorization information about user group A cannot take effect and the authorization information about user group B is used. To make the user group authorization information delivered by the authentication server take effect, ensure that this user group is configured on the device.

Example

Create a user group **test1**.

```
<HUAWEI> system-view
[HUAWEI] user-group test1
```

13.6.152 user-group enable

Function

The **user-group enable** command enables the user group function.

The **undo user-group enable** command disables the user group function.

By default, the user group function is disabled.

Format

user-group *group-name* **enable**

undo user-group *group-name* **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user group has been created using the **user-group** command, run the **user-group enable** command to enable the user group function.

Precautions

After the user group function is enabled, the binding relationship between a user group and an ACL cannot be modified.

If the user group function is not enabled, users going online through Layer 2 interfaces can access the network without restriction, while users going online through VLANIF interfaces are not allowed to access the network.

Example

Enable the user group **test**.

```
<HUAWEI> system-view
[HUAWEI] user-group test enable
```

13.6.153 user-sync

Function

The **user-sync** command enables user information synchronization.

The **undo user-sync** command disables user information synchronization.

By default, user information synchronization is disabled.

Format

user-sync [**interval** *interval-period* | **max-times** *times*] *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the user information synchronization interval.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 300.
max-times *times*	Specifies the maximum number of user information synchronization failures.	The value is an integer that ranges from 2 to 255. The default value is 3.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If communication is interrupted because the network between the device and Portal server is disconnected or the Portal server is faulty, online Portal authentication users cannot go offline. Therefore, user information on the device and on the Portal server may be inconsistent and accounting may be inaccurate.

The **user-sync** command enables user information synchronization so that user information on the device and Portal server is synchronized at intervals to ensure user information consistency.

NOTE

During information synchronization, the device does not disconnect the user immediately after detecting that the device has certain user information while the server does not have such information. Instead, the device disconnects the user when the maximum number of user information synchronization failures is reached.

Precautions

If users go online during the keepalive interval of the Portal server, the Portal server does not have their entries. After the Portal server goes Up and starts synchronizing user information, the device does not disconnect these users even if synchronization fails. The device retails these users until next time these users go online and performs Portal authentication, ensuring good user experience.

The value of *interval-period** *times* configured on the device must be greater than the interval for the Portal server to send synchronization packets. Otherwise, the device forces users offline when it cannot receive any synchronization packet from the Portal server after the maximum failure number is reached.

Example

Enable user information synchronization in the Portal server template **abc**, set the interval for user information synchronization to 100s, and set the maximum number of synchronization failures to 5.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] user-sync interval 100 max-times 5
```

13.6.154 user-vlan (user group view)

Function

The **user-vlan** command configures a user group VLAN.

The **undo user-vlan** restores the default setting.

By default, no user group VLAN is configured.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a user group VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a user group is created using the **user-group** command, you can run the **user-vlan** command to configure a user group VLAN, so that users in different user groups have different network access permissions. When a user in a user group goes online, the user is added to the user group VLAN to obtain the network access permission of this user group.

Prerequisites

The user group VLAN has been created using the **vlan** command.

Precautions

- An authorized VLAN cannot be delivered to online Portal users.
- The **user-vlan** command does not take effect for the users who are already online.
- Access switches will send untagged frames to users in the user VLAN even when interfaces connected users are added to this user VLAN in tagged mode.

Example

Set the VLAN of the user group **abc** to 10.

```
<HUAWEI> system-view
[HUAWEI] user-group abc
[HUAWEI-user-group-abc] user-vlan 10
```

13.6.155 vpn-instance (Portal server template view)

Function

The **vpn-instance** command configures a VPN instance used for communication between the device and Portal server.

The **undo vpn-instance** command restores the default setting.

By default, no VPN instance is configured for communication between the device and Portal server.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VPN implements interconnection within the same department and between different departments in an enterprise. To enable the Portal authentication service in the VPN, run the **vpn-instance** command to bind a Portal server template to a VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the Portal server template must be the same as that bound to the Portal server; otherwise, the device cannot perform Portal authentication for access users.

The users in VPN instances bound to different Portal server templates cannot use the same IP addresses because users with the same IP addresses cannot go online or offline.

Example

Bind the Portal server template **abc** to the VPN instance **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server abc
[HUAWEI-web-auth-server-abc] vpn-instance test
```

13.6.156 web-auth-server version

Function

The **web-auth-server version** command sets the Portal protocol version supported by the device.

The **undo web-auth-server version** command restores the default setting.

By default, the device supports both the versions V1.0 and V2.0.

Format

web-auth-server version v2 [**v1**]

undo web-auth-server version

Parameters

Parameter	Description	Value
v2	Indicates that the device supports the Portal protocol version V2.0. The major version currently used is V2.0.	-
v1	Indicates that the device supports the Portal protocol version V1.0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Currently, the Portal protocol has two versions: V1.0 and V2.0. The device and Portal server must use the Portal protocol of the same version to ensure normal communication. You can run the **web-auth-server version** command to set the Portal protocol version supported by the device.

NOTE

The version V2.0 is widely used currently.

To ensure smooth communication, the device supports both versions by default.

Example

Configure the device to use only the Portal protocol V2.0.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server version v2
```

13.6.157 web-auth-server (interface view)

Function

The **web-auth-server** command binds a Portal server template to an interface.

The **undo web-auth-server** command unbinds a Portal server template from an interface.

By default, no Portal server template is bound to an interface.

Format

- VLANIF interface view:

  web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

  undo web-auth-server [*server-name* [*bak-server-name*]] { **direct** | **layer3** }
- Layer 3 Ethernet interface view: (Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI support this)

  web-auth-server *server-name* [*bak-server-name*] **layer3**

  undo web-auth-server [*server-name* [*bak-server-name*] **layer3**]

Parameters

Parameter	Description	Value
server-name	Specifies the name of the Portal server template.	The value must be an existing Portal server template name.
bak-server-name	Specifies the name of the secondary Portal server template. **NOTE** The name of the secondary Portal server template cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server template name.
direct	Indicates Layer 2 authentication.	-
layer3	Indicates Layer 3 authentication.	-

Views

VLANIF interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A configured Portal server template must be bound to the interface. In this way, the users connected to this interface can be authenticated by the Portal server.

When the Portal server template is bound to the interface using the **web-auth-server** command and a user attempts to access charged network resources, the user is forcibly redirected to the configured Portal authentication page for Portal authentication.

After the primary and secondary Portal server templates are configured, the users who send HTTP requests are redirected to the network access page provided by the secondary Portal server when the primary Portal server is faulty or cannot be accessed. This meets the users' network access requirements. This function can take effect only when the primary Portal server detection function is enabled using the **server-detect** command and heartbeat detection is enabled on the Portal server.

Portal authentication modes are as follows:

- **direct**: When there is no Layer 3 forwarding device between the user and device, the device can learn the user's MAC address. The device identifies the user using the MAC address.
- **layer3**: Whether Layer 3 forwarding devices exist between the user and device, the MAC address table of the device cannot learn the user's MAC address. The device identifies the user using the IP address uniquely.

Prerequisites

A Portal server template has been created using the **web-auth-server** command and an IP address has been configured for the Portal server using the **server-ip** command.

Precautions

- You can bind only one Portal server template to an interface. To modify a Portal server template that has been bound to an interface, remove the template from the interface, modify the template, and bind the modified template to the interface again.
- If 802.1X authentication, MAC address authentication, MAC address bypass authentication is enabled on a Layer 2 interface, this command cannot be executed on the VLANIF interface of a VLAN to which the Layer 2 interface is added.
- This command does not take effect on the VLANIF interface corresponding to the super VLAN.

Example

Bind the Portal server template Server1 to VLANIF10, and set the authentication mode to Layer 2 authentication.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] web-auth-server Server1
[HUAWEI-web-auth-server-Server1] server-ip 10.10.1.1
```

```
[HUAWEI-web-auth-server-Server1] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] web-auth-server Server1 direct
```

13.6.158 web-auth-server listening-port

Function

The **web-auth-server listening-port** command sets the number of the port through which a device listens on Portal protocol packets.

The **undo web-auth-server listening-port** command restores the default listening port.

By default, the device uses port 2000 to listen on Portal protocol packets.

Format

web-auth-server listening-port *port-number*

undo web-auth-server listening-port

Parameters

Parameter	Description	Value
port-number	Specifies the number of the listening port.	The value is an integer that ranges from 1024 to 55535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device exchanges user authentication information with the Portal server using the Portal protocol, you must configure the listening port on the device to receive Portal packets.

You can run the **web-auth-server listening-port** command to set the number of the port through which the device listens on Portal packets. The port number must be the same as the destination port number in Portal packets sent by the Portal server and must be unique.

NOTE

If a specified port is occupied by another service or is a reserved port, the configuration fails. Ensure that the specified port is available when running this command.

Example

Set the number of the port through which a device listens on Portal protocol packets to 3000.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server listening-port 3000
```

13.6.159 web-auth-server reply-message

Function

The **web-auth-server reply-message** command enables the device to transparently transmit users' authentication responses sent by the authentication server to the Portal server.

The **undo web-auth-server reply-message** command disables the device from transparently transmitting users' authentication responses sent by the authentication server to the Portal server.

By default, the device transparently transmits users' authentication responses sent by the authentication server to the Portal server.

Format

web-auth-server reply-message

undo web-auth-server reply-message

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The AAA server requires that the authentication messages sent to the Portal server contain the authentication reply; therefore, the **web-auth-server reply-message** command is required. In certain situations, the authentication messages are not required to carry the reply. In this case, run the **undo web-auth-server reply-message** command.

By default, the device directly forwards the authentication result message from the RADIUS server to the Portal server without processing. This is called transparent transmission.

Example

Disable the device from transparently transmitting users' authentication responses to the Portal server.

```
<HUAWEI> system-view
[HUAWEI] undo web-auth-server reply-message
```

13.6.160 web-auth-server (system view)

Function

The **web-auth-server** command creates a Portal server template or displays the Portal server template view.

The **undo web-auth-server** command deletes a Portal server template.

By default, no Portal server template is created.

Format

web-auth-server *server-name*

undo web-auth-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server.	The value is a string of 1 to 31 case-sensitive characters without spaces. **NOTE** *server-name* cannot be set to listening-port, reply-message, version, or the first character or several leftmost characters of these character strings.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an unauthenticated Portal user goes online, the device forces the user to log in to a specified website (also called the Portal website). The user can access resources in the Portal website for free. When the user attempts to access charged network resources, the user must pass authentication on the Portal website. The specific process is as follows:

1. The unauthorized user opens Internet Explorer and enters a URL in the address box. When receiving the HTTP request sent by the user, the device redirects it to the Portal authentication page of the Portal server.
2. The user enters user information on the authentication page or in the authentication dialog box, and the Portal server forwards the user information to the device.
3. After receiving the user information from the Portal server, the device sends the information to the authentication server for authentication and accounting.
4. After the user is authenticated, the device allows the user to access the Internet if no security policy is enforced.

After a Portal server template is created on the device by using the **web-auth-server** command, run other commands to create a route from the device to the Portal server.

Follow-up Procedure

Run the following commands to configure related attributes of the Portal server template:

- Run the **server-ip** command to configure an IP address for the Portal server.
- Run the **url** command to configure a URL of the Portal server.
- Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device.
- Run the **shared-key** command configures the shared key that the device uses to exchange information with the Portal server.

Precautions

You are advised to back up the Portal server data to prevent authentication failure caused by the Portal server fault.

If you want to run the **undo web-auth-server** command to delete a Portal server template, ensure that the Portal server template is not bound to the interface.

Example

Create the Portal server template **test**.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server test
```

13.6.161 web-redirection disable (Portal server template view)

Function

The **web-redirection disable** command disables the Portal authentication redirection function.

The **undo web-redirection disable** command enables the Portal authentication redirection function.

By default, the Portal authentication redirection function is enabled.

Format

web-redirection disable

undo web-redirection disable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

The device redirects all unauthenticated users to the Portal authentication page when the users send access requests to external networks. For example, when the user needs to enter the URL of the authentication page manually, the **web-redirection disable** command can be executed so that unauthorized users are not forcibly redirected to the Portal authentication page.

NOTE

If the Portal server template has been bound to the VLANIF interface, this command cannot be executed.

After this command is executed, if multiple server IP addresses are configured in the Portal server template and no URL is configured, the device does not display error information when the Portal server template is bound to the VLANIF interface.

Example

Disable the Portal authentication redirection function.

```
<HUAWEI> system-view
[HUAWEI] web-auth-server nac
[HUAWEI-web-auth-server-nac] web-redirection disable
```

13.7 Policy Association Configuration Commands

13.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.7.2 access-user arp-detect control-point mac-ip enable

Function

The **access-user arp-detect control-point mac-ip enable** command configures the source IP address and source MAC address of detection packets sent by an AS to be the same as those used by an authentication control device for detection.

The **undo access-user arp-detect control-point mac-ip enable** command cancels the configuration.

By default, the source IP address and source MAC address of detection packets sent by an AS are not configured to be the same as those used by an authentication control device for detection.

Format

access-user arp-detect control-point mac-ip enable

undo access-user arp-detect control-point mac-ip enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In policy association and SVF scenarios, you can run this command on an authentication control device to configure the source IP address and source MAC address of detection packets sent by an AS to be the same as those used by the authentication control device for detection, simplifying the configuration on the AS.

Precautions

This command is supported only on authentication control devices.

This function takes effect only for users who go online after this command is successfully configured.

For details about how to configure source addresses of detection packets sent by an authentication control device, see "Setting the Source Address of Offline Detection Packets" in the "NAC Configuration" chapter.

Example

Configure the source IP address and source MAC address of detection packets sent by an AS to be the same as those used by an authentication control device for detection.

```
<HUAWEI> system-view
[HUAWEI] access-user arp-detect control-point mac-ip enable
```

13.7.3 as access controller ip-address

Function

The **as access controller ip-address** command specifies an IP address for an authentication control device on an authentication access device.

The **undo as access controller ip-address** command deletes the IP address specified for an authentication control device from an authentication access device.

By default, no IP address is specified for an authentication control device on an authentication access device.

Format

as access controller ip-address *ip-address*

undo as access controller ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for an authentication control device.	The value is in dotted decimal notation.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the policy association solution is deployed, authentication access devices and authentication control devices establish connections through CAPWAP tunnels. When an authentication access device dynamically obtains an IP address through the DHCP server, Option 43 is used to notify the authentication access device of the IP address for the authentication control device with which the authentication access device establishes a CAPWAP tunnel. When an IP address is statically configured for an authentication access device, the **as access controller ip-address** *ip-address* command is used to specify the IP address for the authentication control device with which the authentication access device establishes a CAPWAP tunnel.

Precautions

This command is supported only on authentication access devices.

Example

Specify an IP address for an authentication control device.

```
<HUAWEI> system-view
[HUAWEI] as access controller ip-address 10.1.1.1
```

13.7.4 as access interface

Function

The **as access interface** command specifies source interface for establishing CAPWAP tunnels on an authentication access device.

The **undo as access interface** command deletes the source interface specified for establishing CAPWAP tunnels from an authentication access device.

By default, no source interface is specified for establishing CAPWAP tunnels on an authentication access device.

Format

as access interface vlanif *vlan-id*

undo as access interface

Parameters

Parameter	Description	Value
vlanif *vlan-id*	Specifies a source interface for establishing CAPWAP tunnels.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the policy association solution is deployed, CAPWAP tunnels are used for connection establishment, user association, message communication, user authorization policy delivery, and user synchronization between authentication control devices and authentication access devices. On an authentication access device, run the **as access interface vlanif** *vlan-id* command to specify a source interface for establishing CAPWAP tunnels.

Precautions

This command is supported only on authentication access devices.

The management VLAN of the CAPWAP tunnel cannot be the same as the management VLAN or PnP VLAN of the switches managed by iMaster NCE-Campus.

In policy association, the management VLAN of a CAPWAP tunnel connects authentication access devices to the network. It is not recommended to perform other service configurations except basic configurations in the management VLAN and the corresponding VLANIF interface. If such configurations are performed, authentication access devices may fail to connect to the network.

Example

Specify a source interface for establishing CAPWAP tunnels.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] quit
[HUAWEI] as access interface vlanif 10
```

13.7.5 authentication access-point

Function

The **authentication access-point** command enables remote authentication access control on the interface of an authentication access device.

The **undo authentication access-point** command disables remote authentication access control on the interface of an authentication access device.

By default, remote access control is disabled on the interface of an authentication access device.

Format

authentication access-point [**open**]

undo authentication access-point [**open**]

Parameters

Parameter	Description	Value
open	Disables right control of the access point.	-

Views

Ethernet interface view, MultiGE interface view, 40GE interface view, GE interface view, XGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you deploy policy association, configure the interface of each authentication access device as the access point and enable remote access control on the interface.

To configure right control on an authentication control device instead of an authentication access device, you can disable right control of the access point on the authentication access device (by specifying the **open** parameter).

Precautions

This command is supported only on authentication access devices.

NOTE

The **authentication access-point open** and **authentication access-point** command must be run together; otherwise, the **authentication access-point open** command cannot take effect.

The interface types vary according to device models.

If there is a terminal with one MAC address and multiple IP addresses on the live network, you need to configure the function of identifying static users through IP addresses on the authentication control device. However, because the authentication access device cannot generate multiple entries for the terminal, you cannot implement right control on the authentication access device. In this case, you need to disable right control of the access point on the authentication access device. Otherwise, packets of the terminal will not be forwarded.

Example

Configure GE0/0/1 as the access point.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication access-point
```

13.7.6 authentication access-point max-user

Function

The **authentication access-point max-user** command sets the maximum number of access users allowed on an interface of an authentication access device.

The **undo authentication access-point max-user** command restores the default setting.

By default, an authentication access device does not limit the maximum number of users who are allowed to log in through its interfaces.

Format

authentication access-point max-user *max-user-number*

undo authentication access-point max-user

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of access users allowed on an interface of an authentication access device.	The value is an integer that ranges from 1 to 512 for S6735-S, S6720-EI, and S6720S-EIfrom 1 to 1000 for S5731-S and S5731S-S, from 1 to 1024 for S5731-H, S6730-H, S6730S-H, S5731S-H, S5732-H, S6730-S, and S6730S-S, and from 1 to 300 for other models.

Views

Ethernet interface view, MultiGE interface view, 40GE interface view, GE interface view, XGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the maximum number of access users allowed on an interface of an authentication access device, run the **authentication access-point max-user** command.

Precautions

This command is supported only on authentication access devices.

This command takes effect only for users who attempt to log in for the first time.

The interface types vary according to device models.

Example

Set the maximum number of access users allowed on GE 0/0/1 to 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication access-point max-user 100
```

13.7.7 authentication associate alarm-restrain enable

Function

The **authentication associate alarm-restrain enable** command enables an authentication access device to suppress alarms that are generated due to excess associated users.

The **undo authentication associate alarm-restrain enable** command disables alarm suppression.

By default, an authentication access device is enabled to suppress alarms that are generated due to excess associated users.

Format

authentication associate alarm-restrain enable

undo authentication associate alarm-restrain enable

Parameters

None

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If associated users fail to log in to an authentication access device due to the configured limitation on the access number, the device generates alarms about the login failure event.

These alarms consume device resources and affect system performance. To prevent the device from generating too many repeated alarms in a short period, run the **authentication associate alarm-restrain enable** command to enable suppression on these alarms. The device then does not generate alarms of the same type within a specified suppression period (set using the **authentication associate alarm-restrain period** command).

Precautions

This command is supported only on authentication access devices.

Example

Enable an authentication access device to suppress alarms that are generated due to excess associated users.

```
<HUAWEI> system-view
[HUAWEI] authentication associate alarm-restrain enable
```

13.7.8 authentication associate alarm-restrain period

Function

The **authentication associate alarm-restrain period** command sets a suppression period for alarms that an authentication access device generates due to excess associated users.

The **undo authentication associate alarm-restrain period** command restores the default setting.

By default, an authentication access device suppresses such alarms for 300 seconds.

Format

authentication associate alarm-restrain period *period-value*

undo authentication associate alarm-restrain period

Parameters

Parameter	Description	Value
period-value	Specifies a suppression period for alarms that an authentication access device generates due to excess associated users.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an authentication access device is enabled to suppress alarms that are generated due to excess associated users using the **authentication associate alarm-restrain enable** command, run the **authentication associate alarm-restrain period** command to set a suppression period for these alarms. The device then does not generate alarms of the same type within the suppression period.

Precautions

This command is supported only on authentication access devices.

Example

Set the suppression period to 600s for alarms that an authentication access device generates due to excess associated users.

```
<HUAWEI> system-view
[HUAWEI] authentication associate alarm-restrain period 600
```

13.7.9 authentication control-point

Function

The **authentication control-point** command configures an interface as the control point.

The **undo authentication control-point** command restores the default setting.

By default, an interface does not function as a control point.

Format

authentication control-point [**open**]

undo authentication control-point

Parameters

Parameter	Description	Value
open	Enables the forwarding function of the control point.	-

Views

VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When policy association is configured, the interface on an authentication control device is configured as the control point. If the **open** parameter is configured, the control point directly forwards user traffic. If the **open** parameter is not configured, the control point manages the forwarding rights for user traffic through NAC authentication.

Precautions

- This command is supported only on authentication control devices.
- When the VLANIF interface is configured as the NAC authentication interface, the VLANIF interface and its mapping physical interface must be configured as control points. However, NAC authentication cannot be configured on the physical interface. The **open** parameter cannot be configured for a VLANIF interface.
- When the interface below functions as the control point, it can only directly forward user traffic. That is, only the **authentication control-point open** command can be configured.
  - An interface on the S6720S-SS6720-EI or S6720S-EI, S6735-S
  - An Eth-Trunk interface containing interfaces on the S6720S-SS6720-EI or S6720S-EI, S6735-S

Example

Configure GE0/0/1 as the control point.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] authentication control-point
```

13.7.10 authentication open ucl-policy enable

Function

The **authentication open ucl-policy enable** command configures a control point where the **authentication control-point open** command has been configured to filter user traffic based on a user ACL before forwarding the traffic.

The **undo authentication open ucl-policy enable** command restores a control point where **authentication control-point open** has been configured to directly forwarding user traffic.

By default, a control point where **authentication control-point open** has been configured directly forwards user traffic.

NOTE

Only the S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S5731-H, S5731S-HX series cards support this command.

Format

authentication open ucl-policy enable

undo authentication open ucl-policy enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is applicable to the following scenarios:

- When only independent policy association is used, the **authentication control-point open** command has been configured on a control point.
- When policy association is used in an SVF system, the **authentication control-point open** command is configured on a control point by default.

A control point directly forwards traffic from wired users who go online on an interface of the access device without authentication and the traffic from users who pass NAC authentication but do not obtain the authority granted to the UCL group and the traffic from wireless users in direct forwarding mode. To enable the control point to filter user traffic based on a user ACL, run the **authentication open ucl-policy enable** command.

Precautions

This command can be executed only on the control device.

- In versions earlier than V200R012, rRun the **traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } command on the control device to configure user ACL-based packet filtering before running the **authentication open ucl-policy enable** command.
- In V200R012 and later versions, the **authentication open ucl-policy enable** command is optional if the **traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } command has been configured on the control device to configure user ACL-based packet filtering.

  To disable user ACL-based packet filtering, run the **undo traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } and **undo authentication open ucl-policy enable** commands.

Example

Configure the control point GE1/0/1 where the **authentication control-point open** command has been configured to filter user traffic based on a user ACL before forwarding the traffic.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet1/0/1
[HUAWEI-GigabitEthernet1/0/1] authentication control-point open
[HUAWEI-GigabitEthernet1/0/1] authentication open ucl-policy enable
```

13.7.11 authentication speed-limit

Function

The **authentication speed-limit** command configures the rate limit for an authentication access device to send user association and disassociation request messages.

The **undo authentication speed-limit** command restores the default rate limit for an authentication access device to send user association and disassociation request messages.

By default, an authentication access device sends a maximum of 60 user association and disassociation request messages within 30 seconds.

Format

authentication speed-limit max-num *max-num-value* **interval** *interval-value*

undo authentication speed-limit

Parameters

Parameter	Description	Value
max-num *max-num-value*	Specifies the maximum number of user association and disassociation request messages.	The value is an integer that ranges from 1 to 65535. The default value is 60.
interval *interval-value*	Specifies the interval for an authentication access device to send user association and disassociation request messages.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 30.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An authentication control device can connect to multiple authentication access devices. If the rate limit for an authentication access device to send user association and disassociation request messages is not specified, there will be a heavy load on the authentication control device. You can run this command to adjust the rate limit.

Precautions

This command is supported only on authentication access devices.

In an SVF system, commands cannot be configured on authentication access devices. When the access rate of users is high, they may fail to go online due to a rate limit. To lower the rate limit, run the **direct-command** command on the authentication control device to deliver the **authentication speed-limit** command configuration to the authentication access devices. This requires that the authentication access devices run V200R013C00 or a later version.

Example

Configure the authentication access device to send a maximum of 100 association and disassociation request messages within 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] authentication speed-limit max-num 100 interval 10
```

13.7.12 control-down offline delay (authentication access device)

Function

The **control-down offline delay** command configures the user logout delay on an authentication access device when a control tunnel is faulty.

The **undo control-down offline delay** command deletes the user logout delay on an authentication access device when a control tunnel is faulty.

By default, the user logout delay is not configured on an authentication access device when a control tunnel is faulty, indicating that the users on an authentication access device go offline immediately when a control tunnel is faulty.

Format

control-down offline delay { *delay-value* | **unlimited** }

undo control-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when a control tunnel is faulty.	The value is an integer that ranges from 1 to 60, in seconds.
unlimited	Specifies the user logout delay as unlimited. That is, users do not go offline when a control tunnel is faulty.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **control-down offline delay** command to configure the user logout delay on an authentication access device when a control tunnel is faulty. In this way, the users will not directly go offline upon a tunnel fault. If the fault persists after the delay, the users go offline; if the fault is rectified within the delay, the users keep online.

Precautions

This command is supported only on authentication access devices.

You are advised to configure the same user logout delay on authentication control devices and authentication access devices.

Example

Configure the user logout delay to 10 seconds on an authentication access device after the control tunnel is faulty.

```
<HUAWEI> system-view
[HUAWEI] control-down offline delay 10
```

13.7.13 control-down offline delay (authentication control device)

Function

The **control-down offline delay** command configures the user logout delay on an authentication control device when a control tunnel is faulty.

The **undo control-down offline delay** command deletes the user logout delay on an authentication control device when a control tunnel is faulty.

By default, the user logout delay is not configured on an authentication control device when a control tunnel is faulty, indicating that users on an authentication control device go offline immediately when a control tunnel is faulty.

Format

control-down offline delay { *delay-value* | **unlimited** }

undo control-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when a control tunnel is faulty.	The value is an integer that ranges from 1 to 60, in seconds.
unlimited	Specifies the user logout delay as unlimited. That is, users do not go offline when a control tunnel is faulty.	-

Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **control-down offline delay** command to configure the user logout delay on an authentication control device when a control tunnel is faulty. In this way, the users will not directly go offline upon a tunnel fault. If the fault persists after the delay, the users go offline; if the fault is rectified within the delay, the users keep online.

Precautions

This command is supported only on authentication control devices.

You are advised to configure the same user logout delay on authentication control devices and authentication access devices.

When you configure users not to go offline upon a channel tunnel failure, you also need to configure **link-down offline delay unlimited** command in the authentication profile view.

Example

Configure the user logout delay to 10 seconds on GE0/0/1 of the authentication control device after a control tunnel is faulty.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] control-down offline delay 10
```

13.7.14 display access-user as-name

Function

The **display access-user as-name** command displays information about online users on a specified authentication access device.

Format

display access-user as-name *as-name*

Parameters

Parameter	Description	Value
as-name	Specifies the name of an authentication access device.	The value is the name of an existing authentication access device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online access users on an authentication control device.

The actual name of an authentication access device may differ from the name displayed on the authentication control device (using the **display as all** command). When an authentication access device goes online, its name is processed as follows:

- If the authentication access device uses the default name, its name is changed to *default name*-*MAC address of the authentication access device* on the authentication control device.
- If the authentication access device name contains spaces or double quotation masks ("), the spaces are changed to hyphens (-) and the double quotation masks (") are changed to single quotation masks (') on the authentication control device.

Example

Display information about users on the authentication access device **test_as**.

```
<HUAWEI> display access-user as-name test_as
------------------------------------------------------------------------------
```

```
UserID Username              IP address       MAC           Status
------------------------------------------------------------------------------
16019  fdsa@none              192.168.6.5      xxxx-xxxx-xxxx Success
------------------------------------------------------------------------------
Total: 1, printed: 1
```

NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

Table 13-120 Description of the **display access-user as-name** command output

Item	Description
UserID	ID that is assigned to a user after the user goes online.
Username	Name of a user.
IP address	IP address of a user.
MAC	MAC address of a user.
Status	Status of a user.

13.7.15 display access-user arp-detect control-point mac-ip

Function

The **display access-user arp-detect control-point mac-ip** command displays whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection.

Format

display access-user arp-detect control-point mac-ip

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection.

Precautions

This command is supported only on authentication control devices.

Example

Display whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection.

```
<HUAWEI> display access-user arp-detect control-point mac-ip
 access-user arp-detect control-point mac-ip: Enable
```

Table 13-121 Description of the **display access-user arp-detect control-point mac-ip** command output

Item	Description
access-user arp-detect control-point mac-ip	Whether the source IP address and source MAC address of detection packets sent by an AS are configured to be the same as those used by an authentication control device for detection: - Enable: yes - Disable: no

13.7.16 display associate-user

Function

The **display associate-user** command displays associated users on devices.

Format

display associate-user

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check associated users on authentication access devices and authentication control devices.

Precautions

There are no longer associated users on authentication control devices after the users are successfully authenticated or added to domains. You can run the **display access-user** command to check user information.

Example

Display the associated users on an authentication control device.

```
<HUAWEI> display associate-user
------------------------------------------------------------------
UserID IP address       MAC            SA MAC
------------------------------------------------------------------
27     192.168.12.1     00e0-fc88-143f 00e0-fc43-e00a
------------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-122 Description of the **display associate-user** command output

Item	Description
UserID	ID that is assigned to a user after the user is associated.
IP address	IP address of a user.
MAC	MAC address of a user.
SA MAC	MAC address of an authentication access device.

Display the associated users on an authentication access device.

```
<HUAWEI> display associate-user
------------------------------------------------------------------------------
UserID IP address       MAC            Status        Trigger type
------------------------------------------------------------------------------
27     192.168.12.1     00e0-fc88-143f Associated    Arp
------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 13-123 Description of the **display associate-user** command output

Item	Description
UserID	ID that is assigned to a user after the user is associated.
IP address	IP address of a user.
MAC	MAC address of a user.
Status	Status of a user. ● Up: indicates that the authentication access device has received the authentication success notification from the authentication control device and enabled data forwarding rights for users. ● Associated: indicates that the authentication access device has received the association success response from the authentication control device and is waiting for the authentication success notification from the authentication control device. ● Idle: indicates that the authentication access device detects that the user has been connected and periodically sends an association request or is waiting for the association response from the authentication control device. ● Deleting: indicates that the user has been added to the logout queue and is waiting for logout.

Item	Description
Trigger type	Triggering type. - Arp: indicates that ARP packets are sent to trigger creation of the association table. - Dot1x: indicates that dot1x packets are sent to trigger creation of the association table. - Http: indicates that HTTP packets are sent to trigger creation of the association table. - Dhcp: indicates that DHCP packets are sent to trigger creation of the association table. - Dhcpv6: indicates that DHCPv6 packets are sent to trigger creation of the association table. - Nd: indicates that Nd packets are sent to trigger creation of the association table.

13.7.17 display associate-user statistics

Function

The **display associate-user statistics** command displays statistics about associated users on an interface.

Format

display associate-user statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about associated users on a specified interface. - *interface-type* specifies the type of the interface. - *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check statistics about associated users on an interface, run the **display associate-user statistics** command.

Precautions

This command is supported only on authentication access devices.

Example

Display statistics about associated users on an interface.

```
<HUAWEI> display associate-user statistics
-------------------------------------------------------------------------------
Interface                   number
-------------------------------------------------------------------------------
GigabitEthernet0/0/1         3
TotalNumber                  3
-------------------------------------------------------------------------------
   Total 1
```

Table 13-124 Description of the **display associate-user statistics** command output

Item	Description
Interface	Interface that functions as an access point.
number	Number of associated users on a specified access point.
TotalNumber	Total number of associated users on all access points.
Total: *m*	Total number of interfaces with which users are associated.

13.7.18 display authentication associate

Function

The **display authentication associate** command displays the global configurations of associated users.

Format

display authentication associate

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the global configurations of associated users, run the **display authentication associate** command. The command output contains the suppression status of alarms that an authentication access device generates due to excess associated users and the configured alarm suppression period.

Precautions

This command is supported only on authentication access devices.

Example

Display the global configurations of associated users.

```
<HUAWEI> display authentication associate
 authentication associate alarm-restrain: Enable
 authentication associate alarm-restrain period: 300
```

Table 13-125 Description of the **display authentication associate** command output

Item	Description
authentication associate alarm-restrain	Suppression status of alarms that an authentication access device generates due to excess associated users: ● Enable ● Disable To configure a suppression status, run the **authentication associate alarm-restrain enable** command.

Item	Description
authentication associate alarm-restrain period	Suppression period for alarms that an authentication access device generates due to excess associated users. To configure a suppression period, run the **authentication associate alarm-restrain period** command.

13.7.19 display authentication associate alarm-restrain-table

Function

The **display authentication associate alarm-restrain-table** command displays suppression table information of alarms that are generated due to excess associated users.

Format

display authentication associate alarm-restrain-table { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays alarm suppression table information on all interfaces.	-
interface *interface-type interface-number*	Displays alarm suppression table information on a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an authentication access device is enabled to suppress alarms that are generated due to excess associated users using the **authentication associate alarm-restrain enable** command, run the **display authentication associate alarm-restrain-table** command to check the alarm suppression table information.

Precautions

This command is supported only on authentication access devices.

Example

Display alarm suppression table information on all interfaces.

```
<HUAWEI> display authentication associate alarm-restrain-table all
--------------------------------------------------------------------------------
Interface                   alarm time
--------------------------------------------------------------------------------
GigabitEthernet0/0/1          --
--------------------------------------------------------------------------------
   Total 1
```

Table 13-126 Description of the **display authentication associate alarm-restrain-table all** command output

Item	Description
Interface	Interface that functions as an access point.
alarm time	Date and time when alarms were generated.
Total: *m*	Total number of suppressed entries *m*.

13.7.20 local-authorize

Function

The **local-authorize** command specifies the user authorization information to be delivered to an authentication control device.

The **undo local-authorize** command restores the default user authorization information to be delivered to an authentication control device.

By default, all user authorization information can be delivered to an authentication control device.

Format

local-authorize { **none** | { **acl** | **car** | **priority** | **ucl-group** | **vlan** } * }

undo local-authorize

Parameters

Parameter	Description	Value
acl	Delivers ACL authorization information.	-
car	Delivers CAR authorization information.	-
priority	Delivers priority authorization information.	-
ucl-group	Delivers UCL group authorization information. **NOTE** When you authorize the ACL or UCL group, configure the corresponding ACL or UCL group on authentication control devices to ensure that the authorization information takes effect on the authentication control devices.	-
vlan	Delivers VLAN authorization information.	-

Parameter	Description	Value
none	Delivers no authorization information, including: ● ACL-based authorization information ● CAR-based authorization information ● Priority-based authorization information ● UCL-based authorization information ● VLAN-based authorization information	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable an authentication control device to implement specified user access policies, you can run this command to specify user authorization information to be delivered to the authentication control device. By default, all authorization information is delivered to an authentication control device.

Precautions

This command is supported only on authentication control devices.

This command takes effect for all user authorization types, such as local authorization, remote authorization, and RADIUS dynamic authorization.

For VLAN authorization in a policy association scenario, VLAN authorization information must be delivered. You must configure the **local-authorize vlan** command or do not configure the **local-authorize** command, that is, use the default settings. By default, all user authorization information can be delivered to an authentication control device.

Example

Deliver only UCL group authorization information to the authentication control device.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] local-authorize ucl-group
```

13.7.21 remote-authorize

Function

The **remote-authorize** command specifies the user authorization information to be delivered to an authentication access device.

The **undo remote-authorize** command restores the default user authorization information to be delivered to an authentication access device.

By default, all user authorization information cannot be delivered to authentication access devices.

Format

remote-authorize { **acl** | **car** | **ucl-group** } *

undo remote-authorize

Parameters

Parameter	Description	Value
acl	Delivers ACL authorization information.	-
car	Delivers CAR authorization information.	-
ucl-group	Delivers UCL group authorization information. **NOTE** When you authorize the ACL or UCL group, configure the corresponding ACL or UCL group on authentication access devices to ensure that the authorization information takes effect on the authentication access devices.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable an authentication access device to implement specified user access policies, you can run this command to specify user authorization information to be delivered to the authentication access device. By default, no authorization information is delivered to the authentication access device.

Precautions

This command is supported only on authentication access devices.

This command takes effect for all user authorization information, including local authorization, remote authorization, and RADIUS dynamic authorization information.

In SVF centralized configuration mode, authentication access devices do not support ACL-based authorization or UCL groups.

Example

Deliver only ACL authorization information to the authentication access device.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme test
[HUAWEI-aaa-service-test] remote-authorize acl
```

13.7.22 user-detect

Function

The **user-detect** command enables the online user detection function on an authentication access device.

The **undo user-detect** command disables the online user detection function on an authentication access device.

By default, the online user detection function is enabled on an authentication access device, the detection interval is 100 seconds, and the number of packet retransmission attempts is 3.

Format

user-detect { **interval** *interval-value* | **retry** *retry-value* } *

undo user-detect

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the detection interval.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 100.
retry *retry-value*	Specifies the number of packet retransmission attempts.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user goes offline due to a power failure or network interruption, the authentication access device and authentication control device may still store information about this user, which results in a heavy load on the authentication control device. In addition, a limited number of users can access the device. If a user goes offline unexpectedly but the device still stores information of this user, other users cannot access the network.

After the detection interval is set, the device considers a user to be offline if the user does not respond within the interval. Then the authentication access device and authentication control device delete the saved information about the user, ensuring effective resource usage.

Precautions

This command is supported only on authentication access devices.

You are advised to keep this function enabled on authentication access devices.

This function takes effect only for users who go online after it is configured.

Example

Enable online user detection in the system view, and set the detection interval to 10 seconds and number of packet retransmission attempts to 5.

```
<HUAWEI> system-view
[HUAWEI] user-detect interval 10 retry 5
```

13.7.23 user-sync (authentication access device)

Function

The **user-sync** command enables the user synchronization function on an authentication access device.

The **undo user-sync** command disables the user synchronization function on an authentication access device.

By default, user synchronization is enabled on an authentication access device and the synchronization interval is 60 seconds.

Format

user-sync interval *interval-value*

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the user synchronization interval.	The value is an integer that ranges from 60 to 3600, in seconds. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user is disconnected from an authentication access device due to online detection or a failure to send a disconnection request message, the user information on the authentication control device and authentication access device cannot be synchronized.

After the user synchronization interval is reached, the authentication access device sends a synchronization message containing MAC addresses of all online users to the authentication control device. After receiving the synchronization message, the authentication control device responds with a synchronization failure message if it finds that some users are offline. The authentication access device forcibly disconnects the corresponding users according to the synchronization failure message.

Precautions

This command is supported only on authentication access devices.

The user synchronization function needs to be enabled on both authentication access devices and authentication control devices to ensure that the function works properly. In addition, the user synchronization interval configured on authentication access devices must be shorter than or equal to that configured on authentication control devices, preventing users from being disconnected due to incorrect synchronization.

The user synchronization function of authentication access devices depends on whether the control tunnel is available. When the control tunnel is faulty, the user synchronization function becomes abnormal.

Example

Set the user synchronization interval to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] user-sync interval 100
```

13.7.24 user-sync (authentication control device)

Function

The **user-sync** command enables the user synchronization function on an authentication control device.

The **undo user-sync** command disables the user synchronization function on an authentication control device.

By default, user synchronization is enabled on an authentication control device, the synchronization interval is 60 seconds, and the number of synchronization attempts is 10.

Format

user-sync { **interval** *interval-value* | **retry** *retry-value* } *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the user synchronization interval.	The value is an integer that ranges from 60 to 3600, in seconds. The default value is 60.
retry *retry-value*	Specifies the maximum number of synchronization attempts.	The value is an integer that ranges from 5 to 300. The default value is 10.

Views

VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user is disconnected from an authentication access device due to online detection or a failure to send a disconnection request message, the user information on the authentication control device and authentication access device cannot be synchronized.

After the user synchronization interval is reached, the number of synchronization attempts is added by 1. If the number of synchronization attempts reaches the maximum, the user is forced offline. If the authentication access device detects that the user is online by sending a synchronization message, the number of synchronization attempts is set to 0.

Precautions

This command is supported only on authentication control devices.

The user synchronization function needs to be enabled on both authentication access devices and authentication control devices to ensure that the function works properly. In addition, the user synchronization interval configured on authentication access devices must be shorter than or equal to that configured on authentication control devices, preventing users from being disconnected due to incorrect synchronization.

Example

Set the user synchronization interval to 100 seconds and maximum number of synchronization attempts to 15 on GE0/0/1 of the authentication control device.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] user-sync interval 100 retry 15
```

13.8 Kerberos Snooping Configuration Commands

13.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

13.8.2 display kerberos-snooping-profile

Function

The **display kerberos-snooping-profile** command displays the configuration of a Kerberos snooping profile.

Format

display kerberos-snooping-profile [**name** *profile-name*]

Parameters

Parameter	Description	Value
name *profile-name*	Displays the configuration of a specified Kerberos snooping profile. If this parameter is not specified, all Kerberos snooping profiles configured on the device are displayed. If this parameter is specified, the detailed configuration of the specified Kerberos snooping profile is displayed.	The value must be the name of an existing Kerberos snooping profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a Kerberos snooping profile is configured, you can run this command to check whether the configuration of the Kerberos snooping profile is correct.

Example

Display the configuration of all Kerberos snooping profiles configured on the device.

```
<HUAWEI> display kerberos-snooping-profile
-----------------------------------------------
```

```
ID           Profile Name
-----------------------------------------------
0            p1
1            p2
-----------------------------------------------
 Total: 2 printed: 2.
```

Display the configuration of the Kerberos snooping profile **p1**.

```
<HUAWEI> display kerberos-snooping-profile name p1
  Profile Name                : p1
  TCP/UDP Port                 : 99
  Server IP                   : 10.1.1.1
```

Table 13-127 Description of the **display kerberos-snooping-profile** command output

Item	Description
ID	ID of a Kerberos snooping profile.
Profile Name	Name of a Kerberos snooping profile. To configure a Kerberos snooping profile, run the **kerberos-snooping-profile** command in the system view.
Total	Number of Kerberos snooping profiles.
printed	Number of displayed Kerberos snooping profiles.
TCP/UDP Port	Port number of a Kerberos server. To configure the port number of a Kerberos server, run the **port** command in the Kerberos snooping profile view.
Server IP	IP address of a Kerberos server. To configure the IP address of a Kerberos server, run the **server-ip** command in the Kerberos snooping profile view.

13.8.3 display access-user access-type kerberos-snooping

Function

The **display access-user access-type kerberos-snooping** command displays information about online Kerberos users.

Format

display access-user access-type kerberos-snooping

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online Kerberos users.

Example

Display information about online Kerberos users.

```
<HUAWEI> display access-user access-type kerberos-snooping
 ------------------------------------------------------------------------------
 UserID Username                IP address       MAC             Status
 ------------------------------------------------------------------------------
 16018  test                10.1.1.2         00e0-fc12-3456 Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 13-128 Description of the **display access-user access-type kerberos-snooping** command output

Item	Description
UserID	ID that is assigned to a user after the user goes online.
Username	User name.
IP address	User IP address.
MAC	User MAC address.
Status	User status. ● Success: User authentication is successful.
Total	Number of users.
printed	Number of users displayed in the command output.

13.8.4 kerberos-snooping-profile (authentication profile view)

Function

The **kerberos-snooping-profile** command binds a Kerberos snooping profile to an authentication profile.

The **undo kerberos-snooping-profile** command unbinds a Kerberos snooping profile from an authentication profile.

By default, no Kerberos snooping profile is bound to an authentication profile.

Format

kerberos-snooping-profile *profile-name*

undo kerberos-snooping-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a Kerberos snooping profile.	The value must be the name of an existing Kerberos snooping profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After a Kerberos snooping profile is bound to an authentication profile, Kerberos snooping is enabled on the interface to which the authentication profile is applied. The interface then can control network access rights of users.

Prerequisites

A Kerberos snooping profile has been created using the **kerberos-snooping-profile** command in the system view.

Follow-up Procedure

Run the **authentication-profile** command in the interface view and VAP profile view to apply the authentication profile to a Layer 2 physical interface.

Precautions

An authentication profile can have only one Kerberos snooping profile bound.

Example

Bind the Kerberos snooping profile **profile1** to the authentication profile **authen1**.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1] quit
[HUAWEI] authentication-profile name authen1
[HUAWEI-authen-profile-authen1] kerberos-snooping-profile profile1
```

13.8.5 kerberos-snooping-profile (system view)

Function

The **kerberos-snooping-profile** command creates a Kerberos snooping profile and displays the Kerberos snooping profile view.

The **undo kerberos-snooping-profile** command deletes a Kerberos snooping profile.

By default, no Kerberos snooping profile is created.

Format

kerberos-snooping-profile name *profile-name*

undo kerberos-snooping-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a Kerberos snooping profile.	The value is a string of 1 to 31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following special characters: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In a Kerberos authentication scenario, you need to enable Kerberos snooping on the device, so that the device can control network access rights of users. Only authenticated users can access network resources. To achieve this, you need to create a Kerberos snooping profile on the device and set parameters in the profile first.

Example

Create a Kerberos snooping profile named **profile1**.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1]
```

13.8.6 port (Kerberos snooping profile view)

Function

The **port** command configures the port number used by a Kerberos server to send packets.

The **undo port** command restores the default configuration.

By default, a Kerberos server uses port 88 to send packets.

Format

port *port-number*

undo port

Parameters

Parameter	Description	Value
port-number	Specifies the port number used by a Kerberos server to send packets.	The value is an integer in the range from 1 to 65535.

Views

Kerberos snooping profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Kerberos snooping, you need to run the **port** command to configure the port number used by a Kerberos server to send packets. The device identifies the Kerberos packets sent by a Kerberos server based on the configured IP address and port number of the Kerberos server. If the device receives a KRB_AS_REP, KRB_TGS_REP, or KRB_AP_REP packet from the Kerberos server, it considers that the user has been authenticated and allows the user to access network resources.

In addition, the device identifies and allows the Kerberos packets sent by clients to pass through if the destination port number of packets is the port number of a Kerberos server.

Precautions

Ensure that the port number configured on the device is the same as that used by the Kerberos server.

Example

Set the port number used by the Kerberos server to send packets to 10000.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1] port 10000
```

13.8.7 server-ip (Kerberos snooping profile view)

Function

The **server-ip** command configures the IP address of a Kerberos server.

The **undo server-ip** command deletes the configuration of the Kerberos server IP address.

By default, no Kerberos server IP address is configured on the device.

Format

server-ip *server-ip-address* &<1-10>

undo server-ip { *server-ip-address* | **all** }

Parameters

Parameter	Description	Value
server-ip-address	Specifies the IP address of a Kerberos server.	The value is in dotted decimal format.
all	Deletes all Kerberos server IP addresses.	-

Views

Kerberos snooping profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring Kerberos snooping, you need to run the **server-ip** command to configure the IP address of a Kerberos server. The device identifies the Kerberos packets sent by a Kerberos server based on the configured IP address and port number of the Kerberos server. If the device receives a KRB_AS_REP, KRB_TGS_REP, or KRB_AP_REP packet from the Kerberos server, it considers that the user has been authenticated and allows the user to access network resources.

Precautions

Ensure that the IP address configured on the device is the same as that used by the Kerberos server.

Example

Configure the Kerberos server IP address 10.1.1.1 on the device.

```
<HUAWEI> system-view
[HUAWEI] kerberos-snooping-profile name profile1
[HUAWEI-krb-snooping-profile-profile1] server-ip 10.1.1.1
```

14 Security Commands

14.1 ACL Configuration Commands

14.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.1.2 acl ip-pool

Function

The **acl ip-pool** command creates an ACL IP address pool and enters the ACL IP address pool view.

The **undo acl ip-pool** command deletes an ACL IP address pool.

By default, no ACL IP address pool has been created on the device.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

acl ip-pool *acl-ip-pool-name*

undo acl ip-pool *acl-ip-pool-name*

Parameters

Parameter	Description	Value
acl-ip-pool-name	Specifies the name of the ACL IP address pool to be created.	The value is a string of 1 to 32 characters without spaces and starting with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL IP address pool applies when policy-based routing (PBR) is used to redirect packets to multiple next hops. An ACL IP address pool can be invoked by the **redirect ip-multihop** command to redirect packets to the next hop specified by the ACL IP address pool.

Follow-up Procedure

Run the **ip-address (ACL IP address pool view)** command multiple times to specify multiple IP addresses.

Precautions

The switch supports a maximum of 12 ACL IP address pools. Each ACL IP address pool supports a maximum of 4 IP addresses.

In the scenario when PBR is used to redirect packets to multiple next hops, if the device has no ARP entry matching the specified next hop IP address, the redirection does not take effect. The device still forwards packets to the original destination until the ARP entry matching the specified next hop IP address is generated on the device. You can run the **display acl ip-pool** command to check whether the next hop IP address specified in the ACL IP address pool takes effect.

Example

Create an ACL IP address pool named **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl ip-pool abc
```

14.1.3 acl ipv6 ip-pool

Function

The **acl ipv6 ip-pool** command creates an ACL IPv6 address pool and enters the ACL IPv6 address pool view.

The **undo acl ipv6 ip-pool** command deletes an ACL IPv6 address pool.

By default, no ACL IPv6 address pool has been created on the device.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

acl ipv6 ip-pool *acl-ipv6-pool-name*

undo acl ipv6 ip-pool *acl-ipv6-pool-name*

Parameters

Parameter	Description	Value
acl-ipv6-pool-name	Specifies the name of the ACL IPv6 address pool to be created.	The value is a string of 1 to 32 characters without spaces and starting with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL IPv6 address pool applies when policy-based routing (PBR) is used to redirect packets to multiple next hops. An ACL IPv6 address pool can be invoked by the **redirect ipv6-multihop** command to redirect packets to the next hop specified by the ACL IPv6 address pool.

Follow-up Procedure

Run the **ipv6 address (ACL IPv6 address pool view)** command multiple times to specify multiple IPv6 addresses.

Precautions

The switch supports a maximum of 12 ACL IPv6 address pools. Each ACL IPv6 address pool supports a maximum of 4 IPv6 addresses.

In the scenario where PBR is used to redirect packets to multiple next hops, if the device does not match the neighbor entry corresponding to the next hop IPv6 address, the device sends NS packets to check whether the neighbor is reachable. If the neighbor is unreachable, packets are forwarded based on the original path and redirection does not take effect. You can run the **display acl ipv6 ip-pool** command to check whether the next hop IPv6 address specified in the ACL IPv6 address pool takes effect.

Example

Create an ACL IPv6 address pool named **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 ip-pool abc
```

14.1.4 acl ipv6 name

Function

The **acl ipv6 name** command creates a named ACL6 and enters the ACL6 view.

The **undo acl ipv6 name** command deletes a named ACL6.

By default, no named ACL6 is created.

Format

acl ipv6 name *acl6-name* [**advance** | **basic** | **ucl** | *acl6-number*] [**match-order** { **auto** | **config** }]

undo acl ipv6 name *acl6-name*

Parameters

Parameter	Description	Value
acl6-name	Specifies the name of an ACL6.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
advance	Indicates an advanced ACL6.	-
basic	Indicates a basic ACL6.	-
ucl	Indicates a user ACL6.	-
acl6-number	Specifies the number of an ACL6.	The value is an integer. The value range is as follows: ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999. ● The value of a user ACL6 ranges from 6000 to 9999.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. - **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL6 rules are of the same depth first order, they are matched in ascending order of rule IDs. - **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6s are mainly used in QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services for which packets need to be filtered.

Precautions

- The Switch allocates a number to named ACL6s that have no specified number. The number allocated depends on the following:
  - If only the type of a named ACL6 is specified, the number of the named ACL6 allocated by the Switch is the maximum value of the named ACL6 of the type.
  - If the number and the type of a named ACL6 are not specified, the Switch considers the named ACL6 as the advanced ACL6 and allocates the maximum value as the number of the named ACL6.
- After you create a named ACL6 by using the **acl ipv6 name** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6 name** *acl6-name* or **undo acl ipv6** *acl6-number* command to delete the ACL6.
- When you delete an ACL6 that has been referenced by other services, the services will be interrupted. Therefore, before deleting an ACL6, ensure that the ACL6 is not in use.
- For the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S, before creating a user ACL6, the ACL resource allocation mode device must be set to NAC mode using the **assign resource-template acl-mode**, restarted to make the NAC mode take effect.
- For versions earlier than V200R019C00, if the rule IDs of basic or advanced ACL6 rules are disordered, after the version is upgraded to V200R019C00 or a later version, all rule IDs are updated at a step of 5.

Example

Create basic ACL6 2001 named **test2**.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 name test2 2001
```

14.1.5 acl ipv6 (system view)

Function

The **acl ipv6** command creates a numbered ACL6 and enters the ACL6 view.

The **undo acl ipv6** command deletes a numbered ACL6.

By default, no numbered ACL6 is created.

Format

acl ipv6 [**number**] *acl6-number* [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | [**number**] *acl6-number* }

Parameters

Parameter	Description	Value
number	Indicates the number that identifies an ACL6.	-
acl6-number	Specifies an ACL6 number.	The value is an integer. The value range is as follows: - The value of a basic ACL6 ranges from 2000 to 2999. - The value of an advanced ACL6 ranges from 3000 to 3999. - The value of a user ACL6 ranges from 6000 to 9999.
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. - **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL6 rules are of the same depth first order, they are matched in ascending order of rule IDs. - **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-
all	Indicates that all the configured ACL6s are deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6 rules can be referenced by modules. ACL6s are applicable to QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services for which packets need to be filtered.

Precautions

- After you create a named ACL6 using the **acl ipv6** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6** *acl6-number* command to delete the ACL6.
- When you delete an ACL6 that has been referenced by other services, the services will be interrupted. Before deleting an ACL6, ensure that the ACL6 is not in use.
- All ACL6s can be deleted on the device in one go, but this method is not recommended.
- For the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S, before creating a user ACL6, the ACL resource allocation mode device must be set to NAC mode using the **assign resource-template acl-mode**, restarted to make the NAC mode take effect.
- For versions earlier than V200R019C00, if the rule IDs of basic or advanced ACL6 rules are disordered, after the version is upgraded to V200R019C00 or a later version, all rule IDs are updated at a step of 5.

Example

Create an advanced ACL6 with the number of 3000.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3000
```

14.1.6 acl name

Function

The **acl name** command creates a named ACL and enters the ACL view.

The **undo acl name** command deletes a named ACL.

By default, no ACL is created.

Format

acl name *acl-name* [**advance** | **basic** | **link** | **ucl** | **user** | *acl-number*] [**match-order** { **auto** | **config** }]

undo acl name *acl-name*

Parameters

Parameter	Description	Value
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
advance	Indicates an advanced ACL.	-
basic	Indicates a basic ACL.	-
link	Indicates a Layer 2 ACL.	-
ucl	Indicates a user ACL.	-
user	Indicates a user-defined ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user-defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. - **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. - **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services for which packets need to be filtered.

Precautions

After you create a named ACL by using the **acl name** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl name** *acl-name* or **undo acl** *acl-number* command to delete the ACL.

When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.

The device automatically allocates a number to the named ACLs that have no number specified. The number allocated depends on the following:

- If the type of a named ACL is specified, the number of the named ACL allocated by the device is the maximum value of the named ACL of the type.
- If the number and the type of a named ACL are not specified, the device considers the named ACL as the advanced ACL and allocates the maximum value as the number of the named ACL.

The Switch does not allocate the number to a named ACL repeatedly.

Example

Create basic ACL 2001 named **test1**.

```
<HUAWEI> system-view
[HUAWEI] acl name test1 2001
```

14.1.7 acl (system view)

Function

The **acl** command creates an ACL with the specified number and enters the ACL view.

The **undo acl** command deletes a specified ACL.

By default, no ACL is created.

Format

acl [**number**] *acl-number* [**match-order** { **auto** | **config** }]

undo acl { [**number**] *acl-number* | **all** }

Parameters

Parameter	Description	Value
number	Specifies the number that identifies an ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. ● **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-
all	Indicates that all ACLs are deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services for which packets need to be filtered.

Precautions

- After you create an ACL using the **acl** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl** *acl-number* command to delete the ACL.
- When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.
- You are advised not to delete all ACLs because this operation may cause a service interruption.

Example

Create an ACL numbered 2000.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
```

14.1.8 acl threshold-alarm

Function

The **acl threshold-alarm** command configures the alarm threshold percentage of ACL, Meter or Counter resource usage.

The **undo acl threshold-alarm** command restores the default alarm threshold percentage of ACL, Meter or Counter resource usage.

By default, the lower alarm threshold percentage is 70, and the upper alarm threshold percentage is 80.

Format

acl [**meter** | **counter**] **threshold-alarm** { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* } *

undo acl [**meter** | **counter**] **threshold-alarm**

Parameters

Parameter	Description	Value
meter	Indicates the alarm threshold percentage of Meter resource usage.	-
counter	Indicates the alarm threshold percentage of Counter resource usage.	-
upper-limit *upper-limit*	Indicates the upper alarm threshold percentage.	The value is an integer that ranges from 1 to 100.
lower-limit *lower-limit*	Indicates the lower alarm threshold percentage.	The value is an integer that ranges from 1 to 100.

NOTE

- If neither **meter** nor **counter** is specified, the alarm threshold percentage of ACL resource usage is configured.
- The value of **upper-limit** must be greater than that of **lower-limit**. If the offset between the value of the two parameters is too small, trap information may be frequently displayed.
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I does not support **counter** parameter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ACL resources are occupied by ACL or ACL6 services, Meter resources are occupied by traffic rate limiting services, and Counter resources are occupied by traffic statistics service. You can run the this command to configure the alarm threshold percentage of ACL, Meter or Counter resources usage.

When the ACL, Meter or Counter resource usage is equivalent to or higher than the threshold, the device generates an alarm. When the ACL, Meter or Counter resource usage becomes equivalent to or lower than the lower threshold, the device generates a clear alarm.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

The upper threshold must be equivalent to or greater than the lower threshold.

Example

Configure the lower alarm threshold percentage to 30 and the upper alarm threshold percentage to 50.

```
<HUAWEI> system-view
[HUAWEI] acl threshold-alarm upper-limit 50 lower-limit 30
```

14.1.9 assign resource-template acl-mode { enhanced-acl | nac | normal }

Function

The **assign resource-template acl-mode** command sets the ACL resource allocation mode.

The **undo assign resource-template acl-mode** command restores the default ACL resource allocation mode.

By default, the ACL resource allocation mode is Normal.

NOTE

This function only supported by SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6735-S and S5736-S :

The **nac** parameter is available only on the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S. The **enhanced-acl** parameter is available only on the S6735-S.

Format

assign resource-template acl-mode { **enhanced-acl** | **nac** | **normal** } [**slot** *slot-id*]

undo assign resource-template acl-mode [**slot** *slot-id*]

Parameters

Parameter	Description	Value
enhanced-acl	Specifies the Enhanced ACL resource allocation mode.	-
nac	Specifies the NAC ACL resource allocation mode.	-
normal	Specifies the Normal ACL resource allocation mode.	-

Parameter	Description	Value
slot *slot-id*	• Specifies the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured. If *slot-id* is not specified, the ACL resource allocation mode of all stacked switches is displayed.	The value must be set according to the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The default ACL resource allocation mode is Normal. In Normal mode, the ACL does not support matching of destination IPv6 addresses. If matching destination IPv6 addresses is required, switch the ACL resource allocation mode to NAC. On the S6735-S, you can switch the resource allocation mode to the **enhanced-acl** mode to increase the number of ACLs.

Precautions

- The ACL specifications in NAC and Normal ACL resource allocation modes are the same.
- In NAC mode, matching MAC addresses of IPv6 packets is not supported. As a result, the configuration of the corresponding function matching the source and destination MAC addresses of IPv6 packets in Normal mode may be lost or not take effect.
- After configuring the ACL resource allocation mode, save the configuration, and restart the device for the configuration to take effect.

Example

Change the ACL resource allocation mode to NAC.

```
<HUAWEI> system-view
[HUAWEI] assign resource-template acl-mode nac
```

14.1.10 description

Function

The **description** command configures the description of an ACL or ACL6.

The **undo description** command deletes the description of an ACL or ACL6.

By default, no description is configured for an ACL or ACL6.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Describes an ACL or ACL6.	The value is a string of 1 to 127 case-sensitive characters with spaces supported.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an ACL or ACL6, for example, the usage or application scenario of the ACL. It is used to differentiate ACLs.

Prerequisites

The ACL or ACL6 to be described has been created.

Configuration Impact

If you run the **description** command multiple times in the same ACL view or ACL6 view, only the latest configuration takes effect.

Example

Configure the description of ACL 2100.

```
<HUAWEI> system-view
[HUAWEI] acl 2100
[HUAWEI-acl-basic-2100] description This acl is used in QoS policy
[HUAWEI-acl-basic-2100] display acl 2100
Basic ACL 2100, 0 rule
This acl is used in QoS policy
Acl's step is 5
```

Configure the description of ACL6 3100.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 3100
[HUAWEI-acl6-adv-3100] description This acl is used in QoS policy
[HUAWEI-acl6-adv-3100] display acl ipv6 3100

Advanced IPv6 ACL 3100, 0 rule
This acl is used in QoS policy
```

14.1.11 display acl

Function

The **display acl** command displays the ACL configuration.

Format

display acl { *acl-number* | **name** *acl-name* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The values for different types of ACLs are as follows: • 2000 to 2999: basic ACLs • 3000 to 3999: advanced ACLs • 4000 to 4999: Layer 2 ACLs • 5000 to 5999: user-defined ACLs • 6000 to 9999: user ACLs
name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
all	Indicates all ACLs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display acl** command displays the ACL configuration.

Example

Display the configuration of the ACL named **test**.

```
<HUAWEI> display acl name test
Advanced ACL test 3999, 1 rule, match-order is auto
Acl's step is 5
 rule 5 permit ip destination 10.10.10.1 0 time-range worktime (Active)
```

Display the configuration of all ACLs.

```
<HUAWEI> display acl all
 Total nonempty ACL number is 1

Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip dscp cs1
```

Table 14-1 Description of the **display acl** command output

Item	Description
Advanced ACL test 3999, 1 rule, match-order is auto	Advanced ACL 3999 named **test** contains one rule and uses the automatic order.
Acl's step is 5	The step between ACL rule numbers is 5. For the related command, see **step**.
rule 5 permit ip destination 10.10.10.1 0 time-range worktime (Active)	Rule 5, which allows the packets with the destination IP address 10.10.10.1 to take effect in the **worktime** time range. If the time of the device is within the defined **time-range**, **time-range** in the ACL rule is displayed as **Active**; otherwise, **time-range** in the ACL rule is displayed as **Inactive**. To configure an advanced ACL rule, run the **rule (advanced ACL view)** command.
Total nonempty ACL number is 1	There is one ACL.
Advanced ACL 3000, 1 rule	Advanced ACL 3000 that contains one rule is created.

Item	Description
rule 5 permit ip dscp cs1	Rule 5 that matches packets with DSCP priorities. To configure an advanced ACL rule, run the **rule (advanced ACL view)** command.

14.1.12 display acl ip-pool

Function

The **display acl ip-pool** command displays the configuration and status of an ACL IP address pool.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

display acl ip-pool *acl-ip-pool-name* [**multihop-status** [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
acl-ip-pool-name	Specifies the name of the ACL IP address pool that you want to check.	The ACL IP address pool name must exist.
multihop-status	Displays the status of the next hop IP address specified in the ACL IP address pool.	-
vpn-instance *vpn-instance-name*	Displays the ACL IP address pool of a specified VPN instance.	The VPN instance name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an ACL IP address pool is configured, you can run the **display acl ip-pool** command to check the configuration of the ACL IP address pool and whether the next hop IP address takes effect.

In the scenario when PBR is used to redirect packets to multiple next hops, if the device has no ARP entry matching the specified next hop IP address, the redirection does not take effect. The device still forwards packets to the original destination until the ARP entry matching the specified next hop IP address is generated on the device. You can run the **display acl ip-pool** command to check whether the next hop IP address specified in the ACL IP address pool takes effect.

Example

Display the configuration and status of the ACL IP address pool named **abc**.

```
<HUAWEI> display acl ip-pool abc multihop-status
-----------------------------------------------------------------------------------------
IP Address      NQA AdminName                   NQA TestName                   Status
-----------------------------------------------------------------------------------------
10.3.3.3        --                              --                             invalid
192.168.200.1   user                            test                           valid
192.168.150.1   user                            test                           valid
-----------------------------------------------------------------------------------------
Total: 3
```

Table 14-2 Description of the **display acl ip-pool abc multihop-status** command output

Item	Description
IP Address	IP address in the ACL IP address pool.
NQA AdminName	Administrator of an NQA test instance.
NQA TestName	Name of the NQA test instance.

Item	Description
Status	Status of the next hop IP address. - valid: indicates that the next hop IP address already takes effect. - invalid: indicates that the next hop IP address is not effective. **NOTE** When associating NQA with the next-hop IP address configured using the **ip-address (ACL IP-pool view)** command in an ACL IP pool, ensure that an NQA test instance has been correctly configured and started. Otherwise, you cannot obtain the correct **Status** field value and cannot determine whether the next-hop IP address takes effect.

14.1.13 display acl ipv6 ip-pool

Function

The **display acl ipv6 ip-pool** command displays the configuration and status of an ACL IPv6 address pool.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

display acl ipv6 ip-pool *acl-ipv6-pool-name* [**multihop-status** [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
acl-ipv6-pool-name	Specifies the name of the ACL IPv6 address pool that you want to check.	The ACL IPv6 address pool name must exist.
multihop-status	Displays the status of the next hop IPv6 address specified in the ACL IP address pool.	-
vpn-instance *vpn-instance-name*	Displays the ACL IPv6 address pool of a specified VPN instance.	The VPN instance name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an ACL IPv6 address pool is configured, you can run the **display acl ipv6 ip-pool** command to check the configuration of the ACL IPv6 address pool and whether the next hop IPv6 address takes effect.

In the scenario when PBR is used to redirect packets to multiple next hops, if the device does not match the neighbor entry corresponding to the next hop IPv6 address, the device sends NS packets to check whether the neighbor is reachable. If the neighbor is unreachable, packets are forwarded based on the original path and redirection does not take effect. You can run the **display acl ipv6 ip-pool** command to check whether the next hop IPv6 address specified in the ACL IPv6 address pool takes effect.

Example

Display the configuration and status of the ACL IPv6 address pool named **abc**.

```
<HUAWEI> display acl ipv6 ip-pool abc multihop-status
---------------------------------------------------------------------------------------------------------------

IPv6 Address                    NQA AdminName                   NQA TestName
Status
---------------------------------------------------------------------------------------------------------------

2001:DB8::1                     --                    --                    invalid
2001:DB8::2                     --                    --                    invalid
---------------------------------------------------------------------------------------------------------------

Total: 2
```

Table 14-3 Description of the **display acl ipv6 ip-pool abc multihop-status** command output

Item	Description
IPv6 Address	IPv6 address in the ACL IPv6 address pool.
NQA AdminName	Administrator of an NQA test instance.
NQA TestName	Name of the NQA test instance.
Status	Status of the next hop IPv6 address. ● valid: indicates that the next hop IPv6 address already takes effect. ● invalid: indicates that the next hop IPv6 address is not effective. **NOTE** When associating NQA with the next-hop IPv6 address configured using the **ipv6 address (ACL IPv6 address pool view)** command in an ACL IPv6 address pool, ensure that an NQA test instance has been correctly configured and started. Otherwise, you cannot obtain the correct **Status** field value and cannot determine whether the next-hop IPv6 address takes effect.

14.1.14 display acl ipv6

Function

The **display acl ipv6** command displays the configuration of a specific ACL6 or all ACL6s.

Format

display acl ipv6 { *acl6-number* | **name** *acl6-name* | **all** }

Parameters

Parameter	Description	Value
acl6-number	Specifies an ACL6 number.	The value is an integer. The value range is as follows: ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999. ● The value of a user ACL6 ranges from 6000 to 9999.
name *acl6-name*	Displays the ACL6 with a specified name.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
all	Displays the configurations of all ACL6s.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display acl ipv6** command displays the ACL6 configuration.

Example

Display the configuration about the ACL6 with the number of 2000.

```
<HUAWEI> display acl ipv6 2000

Basic IPv6 ACL 2000, 2 rules
 rule 1 permit source 2001:db8:1::1/64
 rule 0 deny source 2001:db8:1::2/64
```

Display the ACL6 configuration.

```
<HUAWEI> display acl ipv6 all
 Total nonempty acl6 number is 1
```

```

Basic IPv6 ACL 2000, 2 rules
 rule 1 permit source 2001:db8:1::1/64
 rule 0 deny source 2001:db8:1::2/64

Advanced IPv6 ACL 3999 name test, 0 rule

Ucl group IPv6 ACL 6000, 0 rule
```

Table 14-4 Description of the **display acl ipv6** command output

Item	Description
Total nonempty acl6 number is 1	One ACL6 contains rules.
Basic IPv6 ACL 2000, 2 rules	ACL6 2000, which is a basic ACL6 and has two rules.
rule 0 deny source 2001:db8:1::2/64	ACL6 rule 0, which denies packets with the source IPv6 address 2001:db8:1::2/64. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.
rule 1 permit source 2001:db8:1::1/64	ACL6 rule 1, which permits packets with the source IPv6 address 2001:db8:1::1/64. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.
Advanced IPv6 ACL 3999 name test, 0 rule	ACL6 3999, named **test**, which is an advanced ACL6 and has 0 rule.
Ucl group IPv6 ACL 6000, 0 rule	ACL6 6000, which is a user ACL6 and has 0 rule.

14.1.15 display acl resource

Function

The **display acl resource** command displays information about ACL resources.

Format

display acl resource [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- This parameter specifies the slot ID if stacking is not configured. - This parameter specifies the stack ID if stacking is enabled.	The value is an integer. The value range depends on the configuration of a device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

ACL resource information includes: :

- ACL resources: used to store ACL rules. Each ACL entry stores an ACL rule.
- Meter/Car resources: used to limit the traffic rate.
- Counter resources: used to collect traffic statistics.

If ACL configuration fails, all the ACL, Meter, or Counter resources on the device may have been used up. You can run the **display acl resource** command to check whether there are available ACL, Meter, or Counter resources (including ACL4 and ACL6).

Precautions

- After ACL is applied to the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5735S-H, and S5736-S, the ACL resources are applied to both incoming and outgoing traffic. For example, if a traffic policy is applied to only the incoming traffic, the **Outbound-ACL** value and **Inbound-ACL** value in the **display acl resource** command output are the same.
- On the S6735-S, S6720-EI and S6720S-EI, ACL resources are divided in slice mode. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, ACL resources are divided in block mode. Each slice and block contains a certain number of ACL resources. Different types of services apply for different slices or blocks when ACLs are applied. When ACL resource insufficiency is displayed while ACL resources are applied to a service, but the **Free** field shows there are still free ACL resources, this indicates that ACL resources in the slice or block occupied by the service are insufficient, and new slices or blocks cannot be obtained. The free resources in the **Free** field are ACL resources in the slice or block occupied by other services.

Example

Display information about ACL resources in slot 0 (S5720-LI is used as an example).

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/12
                  Vlan-ACL    Inbound-ACL  Outbound-ACL
--------------------------------------------------------------------------
  Rule Used              0          65          65
  Rule Free            512        3007        3007
  Rule Total           512        3072        3072

  Meter Used             0           0           0
  Meter Free             0         768         128
  Meter Total            0         768         128

  Counter Used           0           0           0
  Counter Free           0         768         128
  Counter Total          0         768         128
--------------------------------------------------------------------------
Slot  0
```

Display information about ACL resources in slot 0 (S5731-H is used as an example).

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/24
XGigabitEthernet0/0/1 to XGigabitEthernet0/0/4
                  Used          Free         Total
--------------------------------------------------------------------------
  ACL Unallocated   -             -           2048
  ACL Allocated     2333          227          2560
    Srv     ACL     2047          -            -
    Sec     ACL     286           -            -

  Car             396          32372        32768
  Counter         486          65050        65536
--------------------------------------------------------------------------
```

Display information about ACL resources in slot 0 (S6720-EI is used as an example).

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/48
XGigabitEthernet0/0/1 to XGigabitEthernet0/0/4
                 Used          Free         Total
--------------------------------------------------------------------------
  VACL Slice       1             3            4
  VACL             8             2040         2048

  IACL Slice       11            1            12
  IACL Unallocated -             -            3072
  IACL Allocated   -             -            1024
    Srv    ACL     10            502          512
    Sec    ACL     348           164          512

  EACL Slice       0             4            4
  EACL Unallocated -             -            1024
  EACL Allocated   -             -            0

  Ingress Meter    36            4060         4096
  Egress  Meter    0             1024         1024
  Ingress Counter  155           3941         4096
  Egress  Counter  0             1024         1024
```

```
 Ingress UDF      0            8           8
-------------------------------------------------------------------------------
```

Display information about ACL resources in slot 0 (S5735-S is used as an example).

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/16
                    Used          Free         Total
-------------------------------------------------------------------------------
 VACL Block           2            -            -
 IACL Block          25            -            -
 EACL Block           3            -            -
 Block              30            2           32
 ACL Unallocated      -             -           256
 ACL Allocated       2370         1470        3840
   Ingress L2ACL      2049          127          2176
   Sec     VACL       4            252          256
   Sec     IACL      240           784          1024
   Sec     EACL       77           307          384

 Car                42           470          512
   Sec     Car       42           118          160
   Srv     Car       0            352          352
-------------------------------------------------------------------------------
```

Table 14-5 Description of the **display acl resource** command output

Item	Description
Slot	Stack ID.
GigabitEthernet 0/0/1 to GigabitEthernet 0/0/x XGigabitEthernet 0/0/1 to XGigabitEthernet 0/0/x	Interface to which an ACL is applied.

Item	Description
Vlan-ACL	Inbound ACL resources delivered before Layer 2 forwarding process starts. - For the services related to VLAN translation, for example, VLAN mapping (configured by using the **port vlan-mapping vlan map-vlan** command) and VLAN stacking (configured by using the **port vlan-stacking** command), the device delivers Vlan-ACL resources. - When a traffic policy is applied to the **inbound** direction and bound to a traffic behavior containing a VLAN-related action (except **remark 8021p**), for example, if the action in a traffic behavior is to remark the VLAN tag on VLAN packets (configured by using the **remark vlan-id** command), the device delivers Vlan-ACL resources. This applies to the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.
Inbound-ACL	Inbound ACL resources delivered after Layer 3 forwarding process is complete. Generally, the device delivers Inbound-ACL resources in either of the following situations: - The ACL is applied to a service irrelevant to direction, for example, a user group. - The traffic policy is applied to the inbound direction and contains a traffic behavior irrelevant to VLAN.
Outbound-ACL	ACL resources in outbound direction. The device delivers Outbound-ACL resources when the traffic policy applied to the outbound direction contains a traffic behavior which is not **mirroring to observe-port**. If the traffic behavior contained in the traffic policy is **mirroring to observe-port**, the device delivers Inbound-ACL resources.
Reserved-ACL	ACL resources reserved for CPCAR.
Rule Used	Number of used ACL rules.
Rule Free	Number of free ACL rules.

Item	Description
Rule Total	Total number of ACL rules.
Meter Used	Number of used rate limiting resources.
Meter Free	Number of idle rate limiting resources.
Meter Total	Total number of rate limiting resources.
Counter Used	Number of used counters.
Counter Free	Number of free counters.
Counter Total	Total number of counters, including those for collecting statistics on traffic policies, VLAN traffic, VLANIF interface traffic, and packets sent to the CPU.
Car	Traffic monitoring resources. ● Srv ACL: ACL resources of service type. ● Sec ACL: ACL resources of security type.
Counter	Traffic statistics collection resources.
Used	Number of used resources.
Free	Number of free resources.
Total	Total number of resources.
ACL Unallocated	Unallocated common ACL resources.
ACL Allocated	Number of ACL resources: ● Vlan ACL: ACL resources used by VLAN. ● Ingress ACL: Resources used by inbound traffic policy, ACL-based simplified traffic policy, and IPSG. ● Egress ACL: Resources used by outbound traffic policy and ACL-based simplified traffic policy. ● Ingress UCL: Resources used by traffic from user terminals to switch. ● Egress UCL: Resources used by traffic from switch to user terminals. ● Srv ACL: Resources used by inbound and outbound iPCA and voice VLAN. ● Sec ACL: Inbound secure ACL resources.
EXT Unallocated	Unallocated extended ACL resources.

Item	Description
EXT Allocated	Number of extended ACL resources: - Ingress ACL: Resources used by inbound traffic policy and ACL-based simplified traffic policy. - Egress ACL: Resources used by outbound traffic policy and ACL-based simplified traffic policy.
VACL Slice	Inbound slice resources delivered before Layer 2 forwarding process starts.
VACL	Inbound ACL resources delivered before Layer 2 forwarding process starts.
IACL Slice	Inbound slice resources.
IACL Unallocated	Unallocated inbound ACL resources.
IACL Allocated	Inbound ACL resources are allocated, including: - L2 ACL: ACL resources of L2 type. - IPv4 ACL: ACL resources of IPv4 type. - IPv6 ACL: ACL resources of IPv6 type. - L2IPv4 ACL: ACL resources of L2 IPv4 type. - L2IPv6 ACL: ACL resources of L2 IPv6 type. - UDF ACL: user-defined ACL resources. - Srv ACL: ACL resources of service type. - Sec ACL: ACL resources of security type. - Ext ACL: extended ACL resources.
EACL Slice	Outbound slice resources.
EACL Unallocated	Unallocated outbound ACL resources.

Item	Description
EACL Allocated	Outbound ACL resources are allocated, including: ● L2 ACL: ACL resources of L2 type. ● IPv4 ACL: ACL resources of IPv4 type. ● IPv6 ACL: ACL resources of IPv6 type. ● L2IPv4 ACL: ACL resources of L2 IPv4 type. ● L2IPv6 ACL: ACL resources of L2 IPv6 type. ● UDF ACL: user-defined ACL resources. ● Srv ACL: ACL resources of service type. ● Ext ACL: extended ACL resources.
Ingress Meter	Inbound rate limiting resources.
Egress Meter	Outbound rate limiting resources.
Ingress Counter	Inbound statistics collection resources.
Egress Counter	Outbound statistics collection resources.
Ingress UDF	Inbound user-defined ACL resources. **NOTE** This item is not supported on the S6735-S.
VACL Block	Inbound block resources delivered before Layer 2 forwarding process starts.
IACL Block	Inbound block resources.
EACL Block	Outbound block resources.
Block	Total number of block resources.

14.1.16 display time-range

Function

The **display time-range** command displays the configuration and status of the current time range.

Format

display time-range { **all** | *time-name* }

Parameters

Parameter	Description	Value
all	Indicates all the configured time ranges.	-
time-name	Specifies the name of a time range during which ACL rules take effect.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To specify a time range during which ACL rules take effect, run the **time-range** command and reference the time range name when you configure an ACL.

Before using a time range to filter data packets, run the **display time-range** command to view the time range configuration to avoid duplicate time ranges.

NOTE

The device updates the status of ACLs with a delay of about 30 seconds. The **display time-range** command adopts the current time range to determine the status of ACLs; therefore, you may find that the ACL using an active time range is inactive. This is normal.

Example

Display the configuration and status of all time ranges.

```
<HUAWEI> display time-range all
Current time is 14:48:13 10-17-2012 Wednesday

Time-range : abc (Active)
from 23:23 2012/9/9 to 23:59 2012/12/31
Total time-range number is 1
```

Table 14-6 Description of the **display time-range** command output

Item	Description
Current time is 14:48:13 10-17-2012 Wednesday	The current time is Wednesday 14:48:13 10-17-2012.

Item	Description
Time-range:abc (Active)	The time range is named **abc** and is active. The time range can be: - Active. - Inactive.
from 23:23 2012/9/9 to 23:59 2012/12/31	Time range abc is from 23:23 2012/9/9 to 23:59 2012/12/31.
Total time-range number	The total time-range number.

14.1.17 ip address (ACL IP address pool view)

Function

The **ip address** command configures an IP address in an ACL IP address pool.

The **undo ip address** command deletes an IP address from an ACL IP address pool.

By default, no IP address is configured in an ACL IP address pool.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

ip address *ip-address* [*mask-length* | *wildcard* | **track-nqa** *admin-name test-name*]

undo ip address *ip-address* [*mask-length* | *wildcard* | **track-nqa** *admin-name test-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address in the ACL IP address pool.	The value is in dotted decimal notation.
mask-length	Specifies the subnet mask. **NOTE** If the ACL IP address pool is invoked by the **redirect ip-multihop** command, ensure that the subnet mask is 32-bit long. Otherwise, redirection to the next hop will fail.	The value is an integer that ranges from 0 to 32.
wildcard	Specifies the wildcard of the IP address.	The value is in dotted decimal notation.
track-nqa	Specifies an NQA test instance to be associated with the ACL IP address pool.	-
admin-name	Specifies the administrator of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), hyphens (-), and quotation marks (").
test-name	Specifies the name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), hyphens (-), and quotation marks (").

Views

ACL IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ACL IP address pool is created, you can run the **ip address** command to specify an IP address for the ACL IP address pool. The ACL IP address pool can be invoked by the **redirect ip-multihop** command to redirect packets to the next hop specified in the ACL IP address pool.

Prerequisites

An ACL IP address pool has been created by running the **acl ip-pool** command.

Precautions

The switch supports a maximum of 12 ACL IP address pools. Each ACL IP address pool supports a maximum of 4 IP addresses.

In the scenario when PBR is used to redirect packets to multiple next hops, if the device has no ARP entry matching the specified next hop IP address, the redirection does not take effect. The device still forwards packets to the original destination until the ARP entry matching the specified next hop IP address is generated on the device. You can run the **display acl ip-pool** command to check whether the next hop IP address specified in the ACL IP address pool takes effect.

Example

Specify five IP addresses for the ACL IP address pool named **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl ip-pool abc
[HUAWEI-acl-ip-pool-abc] ip address 192.168.10.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.20.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.30.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.40.1 32
[HUAWEI-acl-ip-pool-abc] ip address 192.168.50.1 32
```

14.1.18 ipv6 address (ACL IPv6 address pool view)

Function

The **ipv6 address** command configures an IPv6 address in an ACL IPv6 address pool.

The **undo ipv6 address** command deletes an IPv6 address from an ACL IPv6 address pool.

By default, no IPv6 address is configured in an ACL IPv6 address pool.

Product	Support
S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S	Supported
S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S	Not supported

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

ipv6 address *ipv6-address*

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

undo ipv6 address *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address in the ACL IPv6 address pool.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address. **NOTE** If the ACL IPv6 address pool is invoked by the **redirect ipv6-multihop** command, ensure that the prefix length is 128. Otherwise, redirection to the next hop will fail.	The value is an integer that ranges from 1 to 128.

Views

ACL IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ACL IPv6 address pool is created, you can run the **ipv6 address** command to specify an IPv6 address for the ACL IPv6 address pool. The ACL IPv6 address pool can be invoked by the **redirect ipv6-multihop** command to redirect packets to the next hop specified in the ACL IPv6 address pool.

Prerequisites

An ACL IPv6 address pool has been created by running the **acl ipv6 ip-pool** command.

Precautions

The switch supports a maximum of 12 ACL IPv6 address pools. Each ACL IPv6 address pool supports a maximum of 4 IPv6 addresses.

In the scenario when PBR is used to redirect packets to multiple next hops, if the device does not match the neighbor entry corresponding to the next hop IPv6 address, the device sends NS packets to check whether the neighbor is reachable. If the neighbor is unreachable, packets are forwarded based on the original path and redirection does not take effect. You can run the **display acl ipv6 ip-pool** command to check whether the next hop IPv6 address specified in the ACL IPv6 address pool takes effect.

Example

Specify four IPv6 addresses for the ACL IPv6 address pool named **abc**.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 ip-pool abc
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::1 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::2 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::3 128
[HUAWEI-acl6-ip-pool-abc] ipv6 address 2001:db8::4 128
```

14.1.19 reset acl counter

Function

The **reset acl counter** command clears statistics about ACLs.

Format

reset acl counter { **name** *acl-name* | *acl-number* | **all** }

Parameters

Parameter	Description	Value
name *acl-name*	Specifies the name of an ACL whose statistics need to be cleared.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
acl-number	Specifies the number of an ACL whose statistics need to be cleared.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of a numbered advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user-defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999.
all	Clears all the ACL statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL statistics generated in a certain period, run the **reset acl counter** command to clear existing statistics and start statistics collection.

NOTICE

After the **reset acl counter** command is executed, the system does not prompt you the statistics deletion.

Before using the **reset acl counter** command, determine whether you intend to clear ACL statistics.

Follow-up Procedure

After running the **reset acl counter** command to clear the previous ACL statistics, you can use the **display acl match-counter** command in the diagnostic view to check ACL rules and statistics on the packets matching the ACL rules in the current period.

Example

Clear statistics about ACL 2000.

```
<HUAWEI> reset acl counter 2000
```

14.1.20 reset acl ipv6 counter

Function

The **reset acl ipv6 counter** command clears the ACL6 statistics.

Format

reset acl ipv6 counter { **name** *acl6-name* | *acl6-number* | **all** }

Parameters

Parameter	Description	Value
name *acl6-name*	Specifies the name of an ACL6 whose statistics need to be cleared.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
acl6-number	Specifies the number of an ACL6 whose statistics need to be cleared.	The value is an integer. The value range is as follows: ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999. ● The value of a user ACL6 ranges from 6000 to 9999.
all	Clears all the ACL6 statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL6 statistics in a certain period, run the **reset acl ipv6 counter** command to clear existing statistics and start statistics collection.

NOTICE

Before using the **reset acl ipv6 counter** command, determine whether you intend to clear ACL6 statistics.

After the **reset acl ipv6 counter** command is executed, the system does not prompt you the statistics deletion.

Follow-up Procedure

After running the **reset acl ipv6 counter** command to clear the previous ACL statistics, you can use the **display acl ipv6** command to view ACL rules and statistics on the packets matching the ACL rules in the current period.

Example

Clear the statistics about basic ACL6 2000.

```
<HUAWEI> reset acl ipv6 counter 2000
```

14.1.21 rule (advanced ACL view)

Function

The **rule** command adds or modifies an advanced ACL rule.

The **undo rule** command deletes an advanced ACL rule.

By default, no advanced ACL rule is configured.

Format

- When the parameter *protocol* is specified as the Internet Control Message Protocol (ICMP), the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **icmp-type** { *icmp-name* | *icmp-type* [*icmp-code*] } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

  undo rule { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **icmp-type** { *icmp-name* | *icmp-type* [*icmp-code*] } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

- When the parameter *protocol* is specified as the Transmission Control Protocol (TCP), the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port*

| **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

undo rule { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

- When the parameter *protocol* is specified as the User Datagram Protocol (UDP), the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

  undo rule { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

- When the parameter *protocol* is specified as another protocol rather than GRE, IGMP, IP, IPINIP, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

  undo rule { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | { **vpn-instance** *vpn-instance-name* | **public** }] *

- To delete an advanced ACL rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | { { **precedence** | **tos** } * | **dscp** } | { **fragment** | **first-fragment** } | **logging** | **icmp-type** | **source** | **source-port** | **tcp-flag** | **time-range** | **ttl-expired** | { **vpn-instance** | **public** }] *

NOTE

- Only the S6735-S, S6720S-EI and S6720-EI support **ttl-expired**.
- The following switch models support **public** only when software-based ACLs are applied: S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, , S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide – Security* ACL Configuration - ACL Fundamentals.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **first-fragment**. For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, an ACL containing the **first-fragment** can only be used in the inbound direction.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.

Parameter	Description	Value
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
gre	Indicates that the protocol type is GRE. The value 47 indicates the GRE protocol.	-
igmp	Indicates that the protocol type is IGMP. The value 2 indicates the IGMP protocol.	-
ip	Indicates that the protocol type is IP.	-
ipinip	Indicates that the protocol type is IPINIP. The value 4 indicates the IPINIP protocol.	-
ospf	Indicates that the protocol type is OSPF. The value 89 indicates the OSPF protocol.	-

Parameter	Description	Value
protocol-number	Indicates the protocol type expressed by name or number. **NOTE** Parameters in an ACL vary with the protocol type. The combination of **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } and **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } is applicable to TCP and UDP only.	The value expressed by number is an integer that ranges from 1 to 255.
destination { *destination-address destination-wildcard* | **any** }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. - *destination-address*: specifies the destination IP address of data packets. - *destination-wildcard*: specifies the wildcard mask of the destination IP address. - **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 or the value of *destination-wildcard* is 255.255.255.255.	*destination-address*: The value is in dotted decimal notation. *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.

Parameter	Description	Value
icmp-type { *icmp-name* | *icmp-type* [*icmp-code*] }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. - *icmp-name*: specifies the name of ICMP packets. - *icmp-type*: specifies the type of ICMP packets. - *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. The value of *icmp6-name* and the corresponding The value of ICMP name and the corresponding ICMP type and ICMP code are as **Table 14-8**.
source { *source-address* *source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. - *source-address*: specifies the source IP address of packets. - *source-wildcard*: specifies the wildcard mask of the source IP address. - **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address*: The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.

Parameter	Description	Value
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value is a string of 1 to 32 characters.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: - **eq** *port*: equivalent to the destination port number. - **gt** *port*: greater than the destination port number. - **lt** *port*: smaller than the destination port number. - **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. - When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*. - When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port*. - When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. **Table 14-9** and **Table 14-10** list the mapping between the well-known source or destination port numbers of UDP or TCP and values of *port*.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: - **eq** *port*: equivalent to the source port number. - **gt** *port*: greater than the source port number. - **lt** *port*: smaller than the source port number. - **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. - When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* - When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* - When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. **Table 14-9** and **Table 14-10** list the mapping between the well-known source or destination port numbers of UDP or TCP and values of *port*.
dscp *dscp*	Specifies the value of a Differentiated Services Code Point (DSCP). **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value is an integer or a name. - The value ranges from 0 to 63 when it is an integer. - When it is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

Parameter	Description	Value
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. - The value can be 0, 1, 2, 4, or 8 when it is an integer. - When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 14-7** describes the mapping between ToS names and values.
precedence *precedence*	Indicates that packets are filtered based on the precedence field. *precedence* specifies the precedence value.	The value ranges from 0 to 7. The values 0 to 7 correspond to *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network*.
fragment	Indicates that the rule is valid only for non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments.	-
first-fragment	Indicates that the rule is valid for only initial fragments. If this parameter is specified, the rule is valid for only initial fragments.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** and **traffic-secure** commands reference ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, **deny** must be specified for the **logging** parameter to take effect.	-
ttl-expired	Matches packets with the TTL value 1. If this keyword is not specified, the ACL rule matches packets with any TTL value.	-

Parameter	Description	Value
vpn-instance *vpn-instance-name* | **public**	- **vpn-instance** *vpn-instance-name*: Specifies the name of a VPN instance, indicating that the ACL rule matches private network packets. - **public**: Indicates that the ACL rule matches public network packets. **NOTE** These two parameters cannot be configured together. If neither **vpn-instance** nor **public** is specified, both public and private network packets are matched.	-

Table 14-7 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 14-8 Values of ICMP name and the corresponding ICMP type and ICMP code

ICMP name	ICMP type	ICMP code
Echo	8	0
Echo-reply	0	0
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0

ICMP name	ICMP type	ICMP code
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0

Table 14-9 Mapping between well-known source or destination port numbers of UDP and values of *port*

Parameter	Value of *port*	Protocol	Description
7	echo	Echo	Port for the Echo service.
9	discard	Discard	Port for the null service, which is used for connectivity test.
37	time	Time	Port for the time protocol.
42	nameserver	Host Name Server	Port for the host name service.
53	dns	Domain Name Service (DNS)	DNS port.
65	tacacs-ds	TACACS-Database Service	Port for the TACACS database service.

Parameter	Value of *port*	Protocol	Description
67	bootps	Bootstrap Protocol (BOOTP) Server	Port for the BOOTP server, which is also used by DHCP servers.
68	bootpc	Bootstrap Protocol (BOOTP) Client	Port for the BOOTP client, which is also used by DHCP clients.
69	tftp	Trivial File Transfer Protocol (TFTP)	TFTP port.
90	dnsix	DNSIX Security Attribute Token Map	Port for DoD Network Security for Information Exchange (DNSIX) Security Attribute Token Map.
111	sunrpc	SUN Remote Procedure Call (SUN RPC)	Port for the RPC protocol of SUN. It is used to remotely execute commands and used by the NFS.
123	ntp	Network Time Protocol (NTP)	NTP port, which may be utilized by worm virus.
137	netbios-ns	NETBIOS Name Service	Port for the NetBIOS name service.
138	netbios-dgm	NETBIOS Datagram Service	Port for the NetBIOS datagram service.
139	netbios-ssn	NETBIOS Session Service	Port for the NetBIOS session service.
161	snmp	SNMP	Port for the Simple Network Management Protocol (SNMP).
162	snmptrap	SNMPTRAP	Port for SNMP trap.
177	xdmcp	X Display Manager Control Protocol (XDMCP)	XDMCP port.
434	mobilip-ag	MobileIP-Agent	Port for the mobile IP agent.

Parameter	Value of *port*	Protocol	Description
435	mobilip-mn	MobileIP-MN	Port for mobile IP management.
512	biff	Mail notify	Port used to notify user of received emails.
513	who	Who	Port for the login user list.
514	syslog	Syslog	Port for the UNIX system log service.
517	talk	Talk	Port used to remotely talk with servers and clients.
520	rip	Routing Information Protocol	RIP port.

Table 14-10 Mapping between well-known source or destination port numbers of TCP and values of *port*

Port Number	Value of *port*	Protocol	Description
7	echo	Echo	Port for the Echo service.
9	discard	Discard	Port for the null service, which is used for connectivity test.
13	daytime	Daytime	Port used to send the date and time to the requesting host.
19	CHARgen	Character generator	Port for the Character Generator Protocol.
20	ftp-data	FTP data connections	FTP data port.
21	ftp	File Transfer Protocol (FTP)	FTP port.
23	telnet	Telnet	Port for the Telnet service.

Port Number	Value of *port*	Protocol	Description
25	smtp	Simple Mail Transport Protocol (SMTP)	SMTP port.
37	time	Time	Port for the time protocol.
43	whois	Nicname (WHOIS)	Port for the directory service.
49	tacacs	TAC Access Control System (TACACS)	Port for the access control system based on TCP/IP authentication (TACACS login host protocol).
53	domain	Domain Name Service (DNS)	DNS port.
70	gopher	Gopher	Port for the information index protocol (document searching and indexing on the Internet).
79	finger	Finger	Port for the Finger service, which is used to query information, such as online users of remote hosts.
80	www	World Wide Web (HTTP) **NOTE** If the HTTPS protocol is used, the port number is 443.	HTTP port for the WWW service, which is used to browse web pages.
101	hostname	NIC hostname server	Host name service port on the NIC machine.
109	pop2	Post Office Protocol v2	Port for the email protocol version 2.
110	pop3	Post Office Protocol v3	Port for the email protocol version 3.

Port Number	Value of *port*	Protocol	Description
111	sunrpc	Sun Remote Procedure Call (RPC)	Port for the RPC protocol of SUN. It is used to remotely execute commands and used by the network file system (NFS).
119	nntp	Network News Transport Protocol (NNTP)	NNTP port, which carries USENET.
179	bgp	Border Gateway Protocol (BGP)	BGP port.
194	irc	Internet Relay Chat (IRC)	Port for the IRC protocol.
512	exec	Exec (rsh)	Port used to authenticate remote processes.
513	login	Login (rlogin)	Port for remote login.
514	cmd	Remote commands	Port used to execute non-interactive commands on a remote system (rshell, rcp).
515	lpd	Printer service	Port for the Line Printer Daemon protocol.
517	talk	Talk	Port used to remotely talk with servers and clients.
540	uucp	Unix-to-Unix Copy Program	Port for the Unix-to-Unix copy protocol.
543	klogin	Kerberos login	Port for Kerberos remote login protocol version 5.
544	kshell	Kerberos shell	Port for Kerberos remote shell protocol version 5.

Views

Advanced ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An advanced ACL matches packets based on information such as source and destination IP addresses, source and destination port numbers, and protocol types.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. (If a simplified traffic policy references a specified rule in an ACL, this command does not take effect.) Before deleting a rule, ensure that the rule is not being referenced.

The parameter **fragment** cannot be set together with **source-port**, **destination-port**, **icmp-type**, and **tcp-flag**; otherwise, the following error message is displayed:

```
Error: The fragment cannot be configured together with the source-port, destination-port, icmp-type and tcp-flag.
```

Example

Add a rule to ACL 3000 to filter ICMP packets.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 1 permit icmp
```

Delete a rule from ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] undo rule 1
```

Add a rule to ACL 3000 to filter IGMP packets.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 2 permit igmp
```

Add a rule to ACL 3000 to filter packets with DSCP priorities.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 3 permit ip dscp cs1
```

Add a rule to ACL 3001 to filter all the IP packets sent from hosts at 10.9.0.0 to hosts at 10.38.160.0.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit ip source 10.9.0.0 0.0.255.255 destination 10.38.160.0 0.0.0.255
```

Add a rule to ACL 3001 to filter the packets with source UDP port number 128 from 10.9.8.0 to 10.38.160.0.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit udp source 10.9.8.0 0.0.0.255 destination 10.38.160.0 0.0.0.255
destination-port eq 128
```

14.1.22 rule (advanced ACL6 view)

Function

The **rule** command adds or modifies an advanced ACL6 rule.

The **undo rule** command deletes an advanced ACL6 rule.

By default, no advanced ACL6 rule is created.

Format

- When the protocol is set to TCP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

  undo rule { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-*

start port-end } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

- When the protocol is set to UDP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **udp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

  undo rule { **deny** | **permit** } { **udp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

- When the protocol is set to ICMPv6, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **icmpv6** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **icmp6-type** { *icmp6-name* | *icmp6-type* [*icmp6-code*] } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

  undo rule { **deny** | **permit** } { **icmpv6** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **icmp6-type** { *icmp6-name* | *icmp6-type* [*icmp6-code*] } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

- When the protocol is set to other protocols, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **ipv6** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-*

address/prefix-length | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

undo rule { **deny** | **permit** } { *protocol-number* | **gre** | **ipv6** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

- To delete an advanced ACL6 rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **icmp6-type** | **logging** | { { **precedence** | **tos** } * | **dscp** } | **routing** | **source** | **source-port** | **tcp-flag** | **time-range** | { **vpn-instance** | **public** }] *

NOTE

- The following switch models support **vpn-instance** and **public** only when software-based ACLs are applied: S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, S6730S-S. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Security* ACL Configuration - ACL Fundamentals.
- For details about the parameters that are not supported when ACL rules are hardware-based ACLs, see **Table 14-11**.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **routing** [**routing-type** *routing-type*].
- Only the SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I support **dscp**, **precedence**, and **tos**.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **destination** and **first-fragment**. For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, an ACL containing the **first-fragment** can only be used in the inbound direction.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL6 rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, a rule is created using the ID and ordered based on the configured sequence. ● If the rule ID is not specified, the device allocates an ID to the new rule. By default, the increment of ACL6 is 5 and cannot be changed. Therefore, the device allocates IDs at an increment of 5 to ACL6 rules. **NOTE** ACL rule IDs assigned automatically by the device starts from the increment value. The default increment value is 5. With this increment, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
tcp	Indicates that the protocol type is TCP.	-
udp	Indicates that the protocol type is UDP.	-
icmpv6	Indicates that the protocol type is ICMPv6.	-

Parameter	Description	Value
protocol-number	Specifies the protocol type that is expressed as a name or a number.	The value ranges from 1 to 255. The protocol type expressed as a name can be GRE, ICMPv6, IPv6, OSPF, TCP, and UDP.
destination { *destination-ipv6-address prefix-length* | *destination-ipv6-address/ prefix-length* | **any** }	Indicates the destination address and prefix of a packet.	*destination-ipv6-address* is expressed in colon hexadecimal notation. The value of *prefix-length* is an integer that ranges from 1 to 128. You can also use **any** to represent any destination address.
destination *destination-ipv6-address* **postfix** *postfix-length*	Indicates the destination address and the length of destination address postfix.	*destination-ipv6-address* indicates the destination address and is expressed in colon hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.
destination *destination-ipv6-address wildcard*	Indicates the destination address and wildcard mask.	*destination-ipv6-address* indicates the destination address and is expressed in colon hexadecimal notation. *wildcard* is expressed in colon hexadecimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter. The values 1 and 0 can be discontinuous. For example, the IPv6 address FC00::1 and the wildcard mask 0::2 indicate that the address is FC00::00*x*1, where *x* can be any value from 0 to F in hexadecimal notation.

Parameter	Description	Value
dscp *dscp*	Specifies the Differentiated Services Code Point (DSCP) value. **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value of *dscp* can be an integer or a name. When the value is an integer, the value ranges from 0 to 63. When the value is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
routing [**routing-type** *routing-type*]	Specifies the IPv6 header in ACL6. The *routing-type* parameter specifies the routing-type field in the IPv6 header.	The value of *routing-type* is an integer that ranges from 0 to 255.
fragment	Indicates that the rule is valid only for non-first fragments.	-
first-fragment	Indicates that the rule is valid only for first fragments.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** command references ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, **deny** must be specified for the **logging** parameter to take effect.	-
precedence *precedence*	Indicates that the packets are filtered according to the precedence field.	**precedence** can be expressed as a name or a number. The value ranges from 0 to 7.
source { *source-ipv6-address prefix-length* | *source-ipv6-address/ prefix-length* | **any** }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in colon hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128. You can also use **any** to represent any source address.
source *source-ipv6-address* **postfix** *postfix-length*	Indicates the source address and the length of source address postfix.	*source-ipv6-address* indicates the source address and is expressed in colon hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.

Parameter	Description	Value
source *source-ipv6-address wildcard*	Indicates the source address and wildcard mask.	*source-ipv6-address* indicates the source address and is expressed in colon hexadecimal notation. *wildcard* is expressed in colon hexadecimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter. The values 1 and 0 can be discontinuous. For example, the IPv6 address FC00::1 and the wildcard mask 0::2 indicate that the address is FC00::00*x*1, where *x* can be any value from 0 to F in hexadecimal notation.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: - **eq** *port*: equivalent to the destination port number. - **gt** *port*: greater than the destination port number. - **lt** *port*: smaller than the destination port number. - **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. - When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* - When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* - When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. **Table 14-15** and **Table 14-14** list the mapping between the well-known source or destination port numbers of UDP or TCP and values of *port*.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: - **eq** *port*: equivalent to the source port number. - **gt** *port*: greater than the source port number. - **lt** *port*: smaller than the source port number. - **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. - When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* - When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* - When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. **Table 14-15** and **Table 14-14** list the mapping between the well-known source or destination port numbers of UDP or TCP and values of *port*.
icmp6-type { *icmp6-name* | *icmp6-type* [*icmp6-code*] }	Indicates the type and code of ICMPv6 packets, which are valid only when the protocol of packets is ICMPv6. If this parameter is not specified, all ICMPv6 packets are matched. - *icmp6-name*: specifies the name of ICMPv6 packets. - *icmp6-type*: specifies the type of ICMPv6 packets. - *icmp6-code*: specifies the code of ICMPv6 packets.	*icmp6-type* is an integer that ranges from 0 to 255. *icmp6-code* is an integer that ranges from 0 to 255. The value of *icmp6-name* and the corresponding ICMPv6 type and ICMPv6 code are as described in **Table 14-13**.

Parameter	Description	Value
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the type of the SYN Flag in the TCP packet header is ack (010000).	-
established	Indicates that the type of the SYN Flag in the TCP packet header is ack (010000) or rst (000100).	-
fin	Indicates that the type of the SYN Flag in the TCP packet header is fin (000001).	-
psh	Indicates that the type of the SYN Flag in the TCP packet header is psh (001000).	-
rst	Indicates that the type of the SYN Flag in the TCP packet header is rst (000100).	-
syn	Indicates that the type of the SYN Flag in the TCP packet header is syn (000010).	-
urg	Indicates that the type of the SYN Flag in the TCP packet header is urg (100000).	-

Parameter	Description	Value
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. - The value ranges from 0 to 15 when it is an integer. - When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 14-12** describes the mappings between ToS names and values.

Parameter	Description	Value
vpn-instance *vpn-instance-name* | **public**	- **vpn-instance** *vpn-instance-name*: Specifies the name of a VPN instance, indicating that the ACL6 rule matches private network packets. - **public**: Indicates that the ACL6 rule matches public network packets. **NOTE** The two parameters cannot be configured together. If neither **vpn-instance** nor **public** is specified, both public and private network packets are matched.	-

Table 14-11 Parameter support regarding different protocols when ACL rules configured are implemented on hardware

Parameter	TCP	UDP	ICMPv6	Other Protocols
destination	Supported	Supported	Supported	Supported
source	Supported	Supported	Supported	Supported
destination-port	Supported	Supported	Not supported	Not supported
source-port	Supported	Supported	Not supported	Not supported
icmp6-type	N/A	N/A	Supported	N/A
precedence	Not supported	Not supported	Not supported	Supported
tos	Not supported	Not supported	Not supported	Supported
dscp	Not supported	Not supported	Not supported	Supported
tcp-flag	Supported	N/A	N/A	N/A
routing	Not supported	Not supported	Not supported	Not supported

Parameter	TCP	UDP	ICMPv6	Other Protocols
fragment | **first-fragment**	Not supported	Not supported	Not supported	Not supported
time-range	Supported	Supported	Supported	Supported
logging	Supported	Supported	Supported	Supported
vpn-instance *vpn-instance-name* | **public**	Not supported	Not supported	Not supported	Not supported

Table 14-12 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 14-13 Values of *icmp6-name* and the corresponding ICMPv6 type and ICMPv6 code

ICMPv6 Name	ICMPv6 Type	ICMPv6 Code
Redirect	137	0
Echo	128	0
Echo-reply	129	0
Err-Header-field	4	0
Frag-time-exceeded	3	1
Hop-limit-exceeded	3	0
Host-admin-prohib	1	1
Host-unreachable	1	3
Neighbor-advertisement	136	0
Neighbor-solicitation	135	0
Network-unreachable	1	0
Packet-too-big	2	0

ICMPv6 Name	ICMPv6 Type	ICMPv6 Code
Port-unreachable	1	4
Router-advertisement	134	0
Router-solicitation	133	0
Unknown-ipv6-opt	4	2
Unknown-next-hdr	4	1

Table 14-14 Mapping between well-known source or destination port numbers of TCP and values of *port*

Port Number	Value of *port*	Protocol	Description
7	echo	Echo	Port for the Echo service.
9	discard	Discard	Port for the null service, which is used for connectivity test.
13	daytime	Daytime	Port used to send the date and time to the requesting host.
19	CHARgen	Character generator	Port for the Character Generator Protocol.
20	ftp-data	FTP data connections	FTP data port.
21	ftp	File Transfer Protocol (FTP)	FTP port.
23	telnet	Telnet	Port for the Telnet service.
25	smtp	Simple Mail Transport Protocol (SMTP)	SMTP port.
37	time	Time	Port for the time protocol.
43	whois	Nicname (WHOIS)	Port for the directory service.

Port Number	Value of *port*	Protocol	Description
49	tacacs	TAC Access Control System (TACACS)	Port for the access control system based on TCP/IP authentication (TACACS login host protocol).
53	domain	Domain Name Service (DNS)	DNS port.
70	gopher	Gopher	Port for the information index protocol (document searching and indexing on the Internet).
79	finger	Finger	Port for the Finger service, which is used to query information, such as online users of remote hosts.
80	www	World Wide Web (HTTP) **NOTE** If the HTTPS protocol is used, the port number is 443.	HTTP port for the WWW service, which is used to browse web pages.
101	hostname	NIC hostname server	Host name service port on the NIC machine.
109	pop2	Post Office Protocol v2	Port for the email protocol version 2.
110	pop3	Post Office Protocol v3	Port for the email protocol version 3.
111	sunrpc	Sun Remote Procedure Call (RPC)	Port for the RPC protocol of SUN. It is used to remotely execute commands and used by the network file system (NFS).
119	nntp	Network News Transport Protocol (NNTP)	NNTP port, which carries USENET.

Port Number	Value of *port*	Protocol	Description
179	bgp	Border Gateway Protocol (BGP)	BGP port.
194	irc	Internet Relay Chat (IRC)	Port for the IRC protocol.
512	exec	Exec (rsh)	Port used to authenticate remote processes.
513	login	Login (rlogin)	Port for remote login.
514	cmd	Remote commands	Port used to execute non-interactive commands on a remote system (rshell, rcp).
515	lpd	Printer service	Port for the Line Printer Daemon protocol.
517	talk	Talk	Port used to remotely talk with servers and clients.
540	uucp	Unix-to-Unix Copy Program	Port for the Unix-to-Unix copy protocol.
543	klogin	Kerberos login	Port for Kerberos remote login protocol version 5.
544	kshell	Kerberos shell	Port for Kerberos remote shell protocol version 5.

Table 14-15 Mapping between well-known source or destination port numbers of UDP and values of *port*

Parameter	Value of *port*	Protocol	Description
7	echo	Echo	Port for the Echo service.
9	discard	Discard	Port for the null service, which is used for connectivity test.

Parameter	Value of *port*	Protocol	Description
37	time	Time	Port for the time protocol.
42	nameserver	Host Name Server	Port for the host name service.
53	dns	Domain Name Service (DNS)	DNS port.
65	tacacs-ds	TACACS-Database Service	Port for the TACACS database service.
67	bootps	Bootstrap Protocol (BOOTP) Server	Port for the BOOTP server, which is also used by DHCP servers.
68	bootpc	Bootstrap Protocol (BOOTP) Client	Port for the BOOTP client, which is also used by DHCP clients.
69	tftp	Trivial File Transfer Protocol (TFTP)	TFTP port.
90	dnsix	DNSIX Security Attribute Token Map	Port for DoD Network Security for Information Exchange (DNSIX) Security Attribute Token Map.
111	sunrpc	SUN Remote Procedure Call (SUN RPC)	Port for the RPC protocol of SUN. It is used to remotely execute commands and used by the NFS.
123	ntp	Network Time Protocol (NTP)	NTP port, which may be utilized by worm virus.
137	netbios-ns	NETBIOS Name Service	Port for the NetBIOS name service.
138	netbios-dgm	NETBIOS Datagram Service	Port for the NetBIOS datagram service.
139	netbios-ssn	NETBIOS Session Service	Port for the NetBIOS session service.

Parameter	Value of *port*	Protocol	Description
161	snmp	SNMP	Port for the Simple Network Management Protocol (SNMP).
162	snmptrap	SNMPTRAP	Port for SNMP trap.
177	xdmcp	X Display Manager Control Protocol (XDMCP)	XDMCP port.
434	mobilip-ag	MobileIP-Agent	Port for the mobile IP agent.
435	mobilip-mn	MobileIP-MN	Port for mobile IP management.
512	biff	Mail notify	Port used to notify user of received emails.
513	who	Who	Port for the login user list.
514	syslog	Syslog	Port for the UNIX system log service.
517	talk	Talk	Port used to remotely talk with servers and clients.
520	rip	Routing Information Protocol	RIP port.

Views

Advanced ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Advanced ACL6s classify data packets based on the source IP address, destination IP address, source port number, destination port number, and protocol type.

The **rule** command defines the time range to flexibly configure the time during which ACL6 rules take effect.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Use this command with caution, especially when you delete an ACL6 rule that has been referenced.

The parameter **fragment** cannot be set together with **source-port**, **destination-port**, **icmp6-type**, and **tcp-flag**.

Example

Add a rule to ACL6 3000 to deny the packets with the destination UDP port number that is greater than 128 from fc00:1::1 to fc00:3::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 3000
[HUAWEI-acl6-adv-3000] rule deny udp source fc00:1::1 64 destination fc00:3::1 64 destination-port gt
128
```

14.1.23 rule (basic ACL view)

Function

The **rule** command adds or modifies a basic ACL rule.

The **undo rule** command deletes a basic ACL rule.

By default, no basic ACL rule is configured.

Format

rule [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

undo rule { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | { **vpn-instance** | **public** }] *

NOTE

The following switch models support **public** only when software-based ACLs are applied: S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, , S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide – Security* ACL Configuration - ACL Fundamentals.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. - If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. - If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the increment. The increment value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the increment value. The default increment value is 5. With this increment, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-

Parameter	Description	Value
source { *source-address source-wildcard* | **any** }	Specifies the source address of packets that match an ACL rule. If no source address is specified, packets with any source addresses are matched. The meaning of each field is as follows: - *source-address*: specifies the source address of packets. - *source-wildcard*: specifies the wildcard of the source address. - **any**: indicates any source address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address*: The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard of the source address can be 0, which is equivalent to 0.0.0.0, indicating that the source address is a host address. **NOTE** In a binary wildcard, the value 0 indicates that this bit needs to be matched and the value 1 indicates that this bit does not need to be matched. 0s and 1s in a wildcard can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 indicate the address 192.168.1.x0x0xx01, among which x can be 0 or 1.
fragment	Indicates that the rule is valid only for non-first fragments. If **fragment** is contained, the rule is valid for non-first fragments and invalid for non-fragments and the first fragment. **NOTE** Rules that do not contain **fragment** are valid for all the packets.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: - An ACL-based simplified traffic policy is configured and the **traffic-filter** and **traffic-secure** commands reference ACLs. - MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, **deny** must be specified for the **logging** parameter to take effect.	-
time-range *time-name*	Specifies the time range during which an ACL rule takes effect. *time-name* specifies the name of a time range. If no time range is specified, the ACL rule is always valid. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value is a string of 1 to 32 characters.
vpn-instance *vpn-instance-name* | **public**	- **vpn-instance** *vpn-instance-name*: specifies the name of a VPN instance, indicating that the ACL rule matches private network packets. - **public**: indicates that the ACL rule matches public network packets. **NOTE** The two parameters cannot be configured together. If neither **vpn-instance** nor **public** is specified, both public and private network packets are matched.	-

Views

Basic ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL matches packets based on information such as source IP addresses, fragment flags, and time ranges.

The **rule** command defines the time range and flexibly configures the time when ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified *rule-id* already exists and the new rule conflicts with the original one, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new one. Otherwise, the configuration result will be incorrect.

The **undo rule** command can delete an ACL rule even if this rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.

Example

Add a rule in ACL 2001 to permit the packets from 192.168.32.1.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.32.1 0
```

Delete rule 5 from ACL 2001.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] undo rule 5
```

14.1.24 rule (basic ACL6 view)

Function

The **rule** command adds or modifies basic ACL6 rules.

The **undo rule** command deletes a basic ACL6 rule.

By default, no basic ACL6 rule is configured.

Format

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

undo rule { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | **time-range** *time-name* | { **vpn-instance** *vpn-instance-name* | **public** }] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | { **vpn-instance** | **public** }] *

NOTE

The following switch models support **vpn-instance** and **public** only when software-based ACLs are applied: S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, S6730S-S. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide – Security* ACL Configuration - ACL Fundamentals.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL6 rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, a rule is created using the ID and ordered based on the configured sequence. ● If the rule ID is not specified, the device allocates an ID to the new rule. By default, the increment of ACL6 is 5 and cannot be changed. Therefore, the device allocates IDs at an increment of 5 to ACL6 rules. **NOTE** ACL rule IDs assigned automatically by the device starts from the increment value. The default increment value is 5. With this increment, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
fragment	Indicates that the rule is valid only for non-first fragments.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** command references ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, **deny** must be specified for the **logging** parameter to take effect.	-
source { *source-ipv6-address prefix-length* | *source-ipv6-address/ prefix-length* }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in colon hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128.
source *source-ipv6-address* **postfix** *postfix-length*	Indicates the source address and the length of source address postfix.	*source-ipv6-address* indicates the source address and is expressed in colon hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.

Parameter	Description	Value
source *source-ipv6-address wildcard*	Indicates the source address and wildcard mask.	*source-ipv6-address* indicates the source address and is expressed in colon hexadecimal notation. *wildcard* is expressed in colon hexadecimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter. The values 1 and 0 can be discontinuous. For example, the IPv6 address FC00::1 and the wildcard mask 0::2 indicate that the address is FC00::00*x*1, where *x* can be any value from 0 to F in hexadecimal notation.
any	Indicates any source address.	-
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.

Parameter	Description	Value
vpn-instance *vpn-instance-name* | **public**	- **vpn-instance** *vpn-instance-name*: Specifies the name of a VPN instance, indicating that the ACL6 rule matches private network packets. - **public**: Indicates that the ACL6 rule matches public network packets. **NOTE** The two parameters cannot be configured together. If neither **vpn-instance** nor **public** is specified, both public and private network packets are matched.	-

Views

Basic ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL6 matches packets based on information such as source IP addresses, fragment flags, and time ranges.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Use this command with caution, especially when you delete an ACL6 rule that has been referenced.

Example

Add a rule for the ACL6 with a number of 2000 to prohibit the passing of packets from the source fc00:1::1/64.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule deny source fc00:1::1/64
```

14.1.25 rule (layer 2 ACL view)

Function

The **rule** command adds or modifies a Layer 2 ACL rule.

The **undo rule** command deletes a Layer 2 ACL rule.

By default, there is no rule in the related Layer 2 ACL view.

Format

rule [*rule-id*] { **permit** | **deny** } [[**ether-ii** | **802.3** | **snap**] | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **cvlan-id** *cvlan-id* [*cvlan-id-mask*] | **cvlan-8021p** *802.1p-value* | **double-tag** | **time-range** *time-name*] *

undo rule { **permit** | **deny** } [[**ether-ii** | **802.3** | **snap**] | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **cvlan-id** *cvlan-id* [*cvlan-id-mask*] | **cvlan-8021p** *802.1p-value* | **double-tag** | **time-range** *time-name*] *

undo rule *rule-id*

NOTE

The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735-S-I, and S5735S-S do not support **cvlan-id** *cvlan-id* [*cvlan-id-mask*], **cvlan-8021p** *802.1p-value*, and **double-tag**.

The S5735S-H, and S5736-S do not support **cvlan-8021p** *802.1p-value*.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule overwrites the old rule. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match a rule.	-
permit	Permits the packets that match a rule.	-

Parameter	Description	Value
ether-ii | **802.3** | **snap**	Indicates the encapsulation format of a packet that matches the rule. - *ether-ii*: specifies the Ethernet II encapsulation. - *802.3*: specifies the 802.3 encapsulation. - *snap*: specifies the SNAP encapsulation. **NOTE** On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735-S-I, and S5735S-S, when an ACL rule is configured to match the packets with encapsulation format **ether-ii** or **snap**, the ACL rule matches all the packets with encapsulation formats Ethernet II and SNAP, including IPv4 and IPv6 packets. On the S5735S-H, S5736-S, when the ACL matching the encapsulation format **ether-ii** or **snap** is configured, the ACL matches the IPv6 packets encapsulated with Ethernet II and SNAP, but matches the IPv4 packets encapsulated with either **ether-ii** or **snap**.	-

Parameter	Description	Value
l2-protocol *type-value* [*type-mask*]	Indicates the type of a Layer 2 protocol. This parameter corresponds to the Ethernet type of Ethernet_II frames and the type-code domain of Ethernet_SNAP frames. - *type-value*: specifies the type value of a Layer 2 protocol. - *type-mask*: specifies the type mask of a Layer 2 protocol.	*type-value* can be a hexadecimal number of 3 to 6 bits that ranges from 0x0000 to 0xFFFF or the following protocol name: - ARP: corresponding to 0x0806 - IP: corresponding to 0x0800 - IPv6: corresponding to 0x86dd - MPLS: corresponding to 0x8847 - RARP: corresponding to 0x8035 The default value of *type-mask* is 0xffff.
destination-mac *dest-mac-address* [*dest-mac-mask*]	Specifies the destination MAC address of packets that matches ACL rules. - *dest-mac-address* specifies the destination MAC address of packets. - *dest-mac-mask* specifies the mask of the destination MAC address of packets.	*dest-mac-address* and *dest-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *dest-mac-mask* is ffff-ffff-ffff. You can obtain the required destination MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.

Parameter	Description	Value
source-mac *source-mac-address* [*source-mac-mask*]	Specifies the source MAC address of packets that matches ACL rules. ● *source-mac-address* specifies the source MAC address of packets. ● *source-mac-mask* specifies the mask of the source MAC address of packets. If this parameter is not specified, the mask is ffff-ffff-ffff.	*source-mac-address* and *source-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *source-mac-mask* is ffff-ffff-ffff. You can obtain the required source MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.
vlan-id *vlan-id* [*vlan-id-mask*]	Indicates the outer VLAN ID contained in a packet that matches the rule. ● *vlan-id*: specifies the number of the VLAN ID. ● *vlan-id-mask*: specifies the mask of the VLAN ID.	The value of *vlan-id* is an integer ranging from 1 to 4094. The value of the *vlan-id-mask* is a hexadecimal number ranging from 0x0 to 0xFFF. The default value is 0xFFF.
8021p *802.1p-value*	Indicates the 802.1p priority in the outer VLAN tag of a packet that matches the rule.	The value is an integer ranging from 0 to 7.
cvlan-id *cvlan-id* [*cvlan-id-mask*]	Indicates the inner VLAN ID of a packet that matches the rule. ● *cvlan-id*: specifies the number of the inner VLAN ID. ● *cvlan-id-mask*: specifies the mask of the inner VLAN ID.	The value of *cvlan-id* is an integer ranging from 1 to 4094. The value of the *cvlan-id-mask* is a hexadecimal number ranging from 0x0 to 0xFFF. The default value is 0xFFF.

Parameter	Description	Value
cvlan-8021p *802.1p-value*	Indicates the 802.1p priority in the inner VLAN tag of a packet that matches the rule.	The value is an integer ranging from 0 to 7.
double-tag	Indicates that only packets with double tags match the rule.	-
time-range *time-name*	Defines the time range during which an ACL rule is valid. *time-name* specifies the name of a time range. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value of *time-name* is a string of 1 to 32 characters.

Views

layer 2 ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 ACL matches packets based on Layer 2 information of the packets, such as source MAC addresses, destination MAC addresses, and Layer 2 protocol types.

The **rule** command defines the time range and flexibly configures the time when the ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists, the new rule overwrites the old rule no matter whether the rules conflict.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.

Example

Add a rule to ACL 4001 to match packets with the destination MAC address being 0000-0000-0001, source MAC address being 0000-0000-0002, and the value of the Layer 2 protocol type being 0x0800.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-
protocol 0x0800
```

14.1.26 rule (user-defined ACL view)

Function

The **rule** command adds or modifies a user-defined ACL rule.

The **undo rule** command deletes an ACL rule.

By default, no ACL rule is configured.

Format

rule [*rule-id*] { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **ipv6-head** | **l4-head** { **udp** | **tcp** | **vxlan** }] { *rule-string rule-mask offset* } &<1-8> | **time-range** *time-name*] *

undo rule { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **ipv6-head** | **l4-head** { **udp** | **tcp** | **vxlan** }] { *rule-string rule-mask offset* } &<1-8> | **time-range** *time-name*] *

undo rule *rule-id*

To add or modify an MPLS-based ACL rule, run the following command:

rule [*rule-id*] { **permit** | **deny** } **mpls** { **untag** | **dot1q** | **qinq** } { **one-label** | **two-labels** } **l2vpn** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **cvlan-id** *cvlan-id* } *

undo rule [*rule-id*] { **permit** | **deny** } **mpls** { **untag** | **dot1q** | **qinq** } { **one-label** | **two-labels** } **l2vpn** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **cvlan-id** *cvlan-id* } *

rule [*rule-id*] { **permit** | **deny** } **mpls** { **untag** | **dot1q** | **qinq** } { **one-label** | **two-labels** } **l3vpn** { **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

undo rule [*rule-id*] { **permit** | **deny** } **mpls** { **untag** | **dot1q** | **qinq** } { **one-label** | **two-labels** } **l3vpn** { **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

rule [*rule-id*] { **permit** | **deny** } **mpls** { **untag** | **dot1q** | **qinq** } { **one-label** | **two-labels** } **l3vpn ip-protocol** { **tcp** | **udp** } [**source-ip***source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

undo rule [*rule-id*] { **permit** | **deny** } **mpls** { **untag** | **dot1q** | **qinq** } { **one-label** | **two-labels** } **l3vpn ip-protocol** { **tcp** | **udp** } [**source-ip***source-address source-*

wildcard | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

To add or modify a VXLAN-based ACL rule, run the following command:

Matching packets without VLAN tags:

rule [*rule-id*] { **permit** | **deny** } **vxlan untag** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

undo rule { **permit** | **deny** } **vxlan untag** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

rule [*rule-id*] { **permit** | **deny** } **vxlan untag ip-protocol** { **tcp** | **udp** } [**source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

undo **rule** { **permit** | **deny** } **vxlan untag ip-protocol** { **tcp** | **udp** } [**source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*]*

Matching packets with a single VLAN tag:

rule [*rule-id*] { **permit** | **deny** } **vxlan dot1q** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

undo rule { **permit** | **deny** } **vxlan dot1q** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

rule [*rule-id*] { **permit** | **deny** } **vxlan dot1q ip-protocol** { **tcp** | **udp** } [**source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

undo rule { **permit** | **deny** } **vxlan dot1q ip-protocol** { **tcp** | **udp** } [**source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

Matching packets with double VLAN tags:

rule [*rule-id*] { **permit** | **deny** } **vxlan qinq** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] |

vlan-id *vlan-id* | **cvlan-id** *cvlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

undo rule { **permit** | **deny** }**vxlan qinq** { **source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **cvlan-id** *cvlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* } *

rule [*rule-id*] { **permit** | **deny** } **vxlan qinq ip-protocol** { **tcp** | **udp** } [**source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **cvlan-id** *cvlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

undo rule { **permit** | **deny** } **vxlan qinq ip-protocol** { **tcp** | **udp** } [**source-mac** *source-mac-address* [*source-mac-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **vlan-id** *vlan-id* | **cvlan-id** *cvlan-id* | **source-ip** *source-address source-wildcard* | **destination-ip** *destination-address destination-wildcard* | **source-port** *source-port* | **destination-port** *destination-port*] *

NOTE

The following switch models do not support &<1-8> and **ipv6-head**: S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S6720S-S, S5736-S

The **udp**, **tcp**, and **vxlan** parameters are supported only by the S6735-S.

The MPLS and VXLAN rules can be added or modified on the following switch models: S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule overwrites the old rule. If the specified rule ID does not exist, the device creates a new rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the increment. The increment value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the increment value. The default increment value is 5. With this increment, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-

Parameter	Description	Value
l2-head | **ipv4-head** | **ipv6-head** | **l4-head** { **udp** | **tcp** | **vxlan** }	Indicates the position from which the offset starts. For example: ● **l2-head**: indicates that the offset begins from the Layer 2 header. ● **ipv4-head**: indicates that the offset begins from the IPv4 header. ● **ipv6-head**: indicates that the offset begins from the IPv6 header. ● **l4-head**: indicates that the offset begins from the Layer 4 header; **udp** indicates that **udp** packets can be matched; **tcp** indicates that TCP packets can be matched; and **vxlan** indicates that VXLAN packets can be matched.	-
rule-string	Specifies the customized rule string.	The value is a hexadecimal string of 3 to 10 characters. A maximum of four bytes are supported. **NOTE** The **rule** (user-defined ACL view) command matches four bytes each time. If the length of the configured *rule-string* parameter is less than four bytes, 0s are added.
rule-mask	Specifies the mask of the rule string.	The value is a hexadecimal string of 3 to 10 characters. A maximum of four bytes are supported. When the mask bit of the customized character string is 1, the ACL matches the bit. When the mask bit of the customized character string is 0, the ACL does not match the bit.

Parameter	Description	Value
offset	Specifies the value of the offset.	The value is an integer, in bytes. The value of the offset varies with the offset position. - For **l2-head**, the value of offset is 4N+2. N is an integer starting from 0. - For other offset positions, the value of offset is 4N. N is an integer starting from 0. **NOTE** For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: Values of offsets at all offset positions are 2N, and N is an integer starting from 0.
time-range *time-name*	Defines the time range during which an ACL rule takes effect. *time-name* specifies the name of the time range during which an ACL rule takes effect.	The value is a string of 1 to 32 characters.
mpls	Specifies MPLS packets.	-
vxlan	Specifies VXLAN packets.	-
untag | **dot1q** | **qinq**	Specifies an ACL rule to match the outer VLAN tag in MPLS or VXLAN packets. **untag**: indicates untagged packets. **dot1q**: indicates single-tagged packets. **qinq**: indicates double-tagged packets.	-
one-label | **two-labels**	Specifies an ACL rule to match MPLS or VXLAN packet labels. **one-label**: indicates packets with single MPLS labels. **two-labels**: indicates packets with double MPLS labels.	-
l2vpn	Specifies L2VPN packets.	-

Parameter	Description	Value
l3vpn	Specifies L3VPN packets.	-
source-mac *source-mac-address* [*source-mac-mask*]	Specifies the source MAC address information. - *source-mac-address*: indicates the source MAC address of the packet. - *source-mac-mask*: specifies the mask of the source MAC address. If this parameter is not set, the mask is ffff-ffff-ffff.	Both *source-mac-address* and *source-mac-mask* are in the H-H-H format where H is a hexadecimal number of 1 to 4 digits. The default value of *source-mac-mask* is ffff-ffff-ffff. The two parameters determine a source MAC address range. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies the MAC address 00e0-fc01-0101, and 00e0-fc01-0101 ffff-ffff-0000 specifies the MAC address range 00e0-fc01-0000 to 00e0-fc01-ffff.
destination-mac *dest-mac-address* [*dest-mac-mask*]	Specifies the destination MAC address information. - *dest-mac-address*: specifies the destination MAC address of packets. - *dest-mac-mask*: specifies the mask of the destination MAC address. If this parameter is not set, the mask is ffff-ffff-ffff.	Both *dest-mac-address* and *dest-mac-mask* are in the H-H-H format where H is a hexadecimal number of 1 to 4 digits. The default value of *dest-mac-mask* is ffff-ffff-ffff. The two parameters determine a destination MAC address range. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies the MAC address 00e0-fc01-0101, and 00e0-fc01-0101 ffff-ffff-0000 specifies the MAC address range 00e0-fc01-0000 to 00e0-fc01-ffff.
vlan-id *vlan-id*	Specifies the outer VLAN ID of packets.	The value is an integer in the range from 1 to 4094.
cvlan-id *cvlan-id*	Specifies the inner VLAN ID of packets.	The value is an integer in the range from 1 to 4094.

Parameter	Description	Value
source-ip *source-address source-wildcard*	Specifies the source IP address information. - *source-address*: specifies the source IP address of packets. - *source-wildcard*: specifies the wildcard of the source IP address.	The value of *source-address* is in dotted decimal notation. *source-wildcard* is in dotted decimal notation. Note: In a binary wildcard, the value 0 indicates that this bit needs to be matched and the value 1 indicates that this bit does not need to be matched. 0s and 1s in a wildcard can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 indicate the address 192.168.1.x0x0xx01, among which x can be 0 or 1.
destination-ip *destination-address destination-wildcard*	Specifies the destination IP address information. - *destination-address*: specifies the destination IP addresses of packets. - *destination-wildcard*: specifies the wildcard of the destination IP address.	*destination-address* is in dotted decimal notation. *destination-wildcard* is in dotted decimal notation. Note: In a binary wildcard, the value 0 indicates that this bit needs to be matched and the value 1 indicates that this bit does not need to be matched. 0s and 1s in a wildcard can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 indicate the address 192.168.1.x0x0xx01, among which x can be 0 or 1.
source-port *source-port*	Specifies the source port of UDP or TCP packets. The value is valid only when the packet protocol is TCP or UDP.	The value is an integer ranging from 0 to 65535.
destination-port *destination-port*	Specifies the destination port of UDP or TCP packets. The value is valid only when the packet protocol is TCP or UDP.	The value is an integer ranging from 0 to 65535.

Views

User-defined ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user-defined ACL defines rules by setting the offset position and value of the packet. User-defined ACLs are mainly used for matching rules in a traffic classifier.

The **rule** command defines the time range and flexibly configures the time when ACL rules take effect.

NOTE

The user-defined ACL is applicable only to the incoming traffic.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

- If the specified *rule-id* already exists and the new rule conflicts with the original one, the new rule replaces the original rule. To modify an existing rule, delete the old rule, and then create a new one. Otherwise, the configuration result will be incorrect.
- To change the offset in a user-defined ACL rule, delete the existing rule and reconfigure a new one.
- The **undo rule** command can delete an ACL rule even if this rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.
- On the S5735S-H and S5736-S, an ACL rule is specified to perform the offset matching based on the Layer 2 packet header. In this case, if the packets passing through the GE electrical interface to which the ACL rule is applied do not carry tags, a tag needs to be added to the packets before the offset value is calculated.
- On the S6735-S, the packet type must be specified when an ACL rule is specified to perform the offset matching based on the Layer 4 packet header.

Example

Add a rule to ACL 5001 to match a 4-byte character string whose content is 0x0180C200 with a 14-byte offset beginning from the Layer 2 packet header.

```
<HUAWEI> system-view
[HUAWEI] acl 5001
[HUAWEI-acl-user-5001] rule permit l2-head 0x0180C200 0xFFFFFFFF 14
```

Add a rule to ACL 5002 to match VXLAN packets with the destination IP address of 10.10.10.10 and single VLAN tag.

```
<HUAWEI> system-view
[HUAWEI] acl 5002
[HUAWEI-acl-user-5002] rule 5 permit vxlan dot1q destination-ip 10.10.10.10 0.0.0.0
```

14.1.27 rule (user ACL view)

Function

The **rule** command configures a user ACL rule.

The **undo rule** command deletes a user ACL rule.

By default, no user ACL rule is configured.

Format

- When the parameter *protocol* is specified as the ICMP, the command format is as follows:

  rule [*rule-id*] { **permit** | **deny** } { **icmp** | *protocol-number* } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { **name** *destination-ucl-group-name* | *destination-ucl-group-index* } } } * | **fqdn** *fqdn-name* } | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-name* } | **vpn-instance** *vpn-instance-name* | **time-range** *time-name*] *

  undo rule { **permit** | **deny** } { **icmp** | *protocol-number* } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { **name** *destination-ucl-group-name* | *destination-ucl-group-index* } } } * | **fqdn** *fqdn-name* } | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-name* } | **vpn-instance** *vpn-instance-name* | **time-range** *time-name*] *

- When the parameter *protocol* is specified as the TCP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **tcp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the UDP, the command format is as follows:

rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule { **deny** | **permit** } { *protocol-number* | **udp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the GRE, IGMP, IP, IPINIP, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- To delete an ACL rule, run:

  undo rule *rule-id*

NOTE

The S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720S-EI, and S6720-EI do not support **destination** { **fqdn** *fqdn-name* }, **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* }, and **vpn-instance** *vpn-instance-name*.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-

Parameter	Description	Value
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
gre	Indicates that the protocol type is GRE. The value 47 indicates the GRE protocol.	-
igmp	Indicates that the protocol type is IGMP. The value 2 indicates the IGMP protocol.	-
ip	Indicates that the protocol type is IP.	-
ipinip	Indicates that the protocol type is IPINIP. The value 4 indicates the IPINIP protocol.	-
ospf	Indicates that the protocol type is OSPF. The value 89 indicates the OSPF protocol.	-
protocol-number	Indicates the protocol type expressed by number.	The value expressed by number is an integer that ranges from 1 to 255.

Parameter	Description	Value
source { { *source-address source-wildcard* | **any** } | { [**source**] **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } *	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. - *source-address*: specifies the source IP address of packets. - *source-wildcard*: specifies the wildcard mask of the source IP address. - **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 and the value of *source-wildcard* is 255.255.255.255. - **ucl-group** *source-ucl-group-index*: specifies the ID of the UCL group to which the source IP address of packets belongs. - **ucl-group name** *source-ucl-group-name*: specifies the name of the UCL group to which the source IP address of packets belongs.	- *source-address*: The value is in dotted decimal notation. - *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1. - The value of *source-ucl-group-name* must be the name of an existing UCL group. - *source-ucl-group-index* is an integer, the value varies according to different devices. When the value is 0, the source address of packet matching the ACL rule is beyond the UCL group range.

Parameter	Description	Value
destination { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. - *destination-address*: specifies the destination IP address of data packets. - *destination-wildcard*: specifies the wildcard mask of the destination IP address. - **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 and the value of *destination-wildcard* is 255.255.255.255. - **ucl-group** *destination-ucl-group-index*: specifies the ID of the UCL group to which the destination IP address of packets belongs. - **ucl-group name** *destination-ucl-group-name*: specifies the name of the UCL group to which the destination IP address of packets belongs. - **fqdn** *fqdn-name*: specifies the name of a domain. The precise matching and fuzzy matching (using *) are supported. In fuzzy matching, the domain name must be in the format of *.XXX, for example,	- *destination-address*: The value is in dotted decimal notation. - *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1. - The value of *destination-ucl-group-name* must be the name of an existing UCL group. - *destination-ucl-group-index* is an integer, the value varies according to different devices. When the value is 0, the source address of packet matching the ACL rule is beyond the UCL group range. - The value of *fqdn-name* is a string of 1 to 64 characters.

Parameter	Description	Value
	*.abc.com. The fuzzy domain name and full domain name cannot include each other. For example, if **www.abc.com** has been configured on the device, ***.abc.com** cannot be configured, but ***.aaa.com** can be configured. Similarly, if ***.abc.com** has been configured on the device, ***.www.abc.com** cannot be configured, but **www.aaa.com** can be configured. This parameter is available for only wireless users.	
icmp-type { *icmp-name* | *icmp-type* [*icmp-code*] }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. - *icmp-name*: specifies the name of ICMP packets. - *icmp-type*: specifies the type of ICMP packets. - *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. The value of ICMP name and the corresponding ICMP type and ICMP code are as **Table 14-16**.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: ● **eq** *port*: equal operator. ● **gt** *port*: greater than operator. ● **lt** *port*: smaller than operator. ● **range** *port-start port-end*: within the range.*port-start* specifies the start port number.*port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equal operator. ● **gt** *port*: greater than operator. ● **lt** *port*: smaller than operator. ● **range** *port-start port-end*: within the range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-

Parameter	Description	Value
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value is a string of 1 to 32 characters.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance on the inbound interface.	The value must be an existing VPN instance name.

Table 14-16 Values of ICMP name and the corresponding ICMP type and ICMP code

ICMP name	ICMP type	ICMP code
Echo	8	0
Echo-reply	0	0
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0

ICMP name	ICMP type	ICMP code
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0

Views

User ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user ACL defines rules to filter IPv4 packets based on the source IP addresses or source User Control List (UCL) groups, destination IP addresses or destination UCL groups, IP protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and time ranges.

Currently, the user ACL can be applied only to the UCL groups of the NAC mode. To control the network access rights of users based on user groups, you can perform the following operations: configure a UCL group, associate user ACL rules with the UCL group so that the ACL rules apply to all users in the user group, configure packet filtering based on the user ACL to make the ACL take effect, and then apply the UCL group to the AAA service scheme.

Prerequisites

If the **ucl-group name** *source-ucl-group-name* or **ucl-group name** *destination-ucl-group-name* parameter is configured for a rule, the source and destination UCL groups must have been created by the **ucl-group** command.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. (If a simplified traffic policy references a specified rule in an ACL, this command does not take effect.) Before deleting a rule, ensure that the rule is not being referenced.

Example

Add a rule to ACL 6000 to reject all the IP packets sent from UCL group group1 to network segment 10.9.9.0/24.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name group1
[HUAWEI] acl 6000
[HUAWEI-acl-ucl-6000] rule deny ip source ucl-group name group1 destination 10.9.9.0 0.0.0.255
```

14.1.28 rule (user ACL6 view)

Function

The **rule** command configures a user ACL6 rule.

The **undo rule** command deletes a user ACL6 rule.

By default, no user ACL6 rule is configured.

Format

- When the protocol is set to ICMPv6, the command format is as follows:

  rule [*rule-id*] { **permit** | **deny** } { **icmpv6** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **icmp6-type** { *icmp6-type* [*icmp6-code*] | *icmp6-name* } | **vpn-instance** *vpn-instance-name* | **time-range** *time-name*] *

  undo rule { **permit** | **deny** } { **icmpv6** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **icmp6-type** { *icmp6-type* [*icmp6-code*] | *icmp6-name* } | **vpn-instance** *vpn-instance-name* | **time-range** *time-name*] *

- When the protocol is set to TCP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-*

address **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule { **deny** | **permit** } { **tcp** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the protocol is set to UDP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **udp** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { **udp** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the protocol is set to GRE, IPv6, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **gre** | **ipv6** | **ospf** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule { **deny** | **permit** } { **gre** | **ipv6** | **ospf** | *protocol-number* } [**source** { { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- To delete a user ACL6 rule, run:

  undo rule *rule-id*

NOTE

The S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6720S-S, S6735-S, S6720S-EI, and S6720-EI do not support **vpn-instance** *vpn-instance-name*.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL6 rule. - If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, a rule is created using the ID and ordered based on the configured sequence. - If the rule ID is not specified, the device allocates an ID to the new rule. By default, the increment of ACL6 is 5 and cannot be changed. Therefore, the device allocates IDs at an increment of 5 to ACL6 rules. **NOTE** ACL rule IDs assigned automatically by the device starts from the increment value. The default increment value is 5. With this increment, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
icmpv6	Indicates that the protocol type is ICMPv6. The value 58 indicates the ICMPv6 protocol.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates the TCP protocol.	-

Parameter	Description	Value
udp	Indicates that the protocol type is UDP. The value 17 indicates the UDP protocol.	-
gre	Indicates that the protocol type is GRE. The value 47 indicates the GRE protocol.	-
ipv6	Indicates that the protocol type is IPv6.	-
ospf	Indicates that the protocol type is OSPF. The value 89 indicates the OSPF protocol.	-
protocol-number	Indicates the protocol type expressed by number.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
source { { *source-ipv6-address prefix-length* | *source-ipv6-address/ prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | *source-ipv6-address wildcard* | **any** } | { **ucl-group** { **name** *source-ucl-group-name* | *source-ucl-group-index* } } } *	Indicates the source IPv6 address of packets that match an ACL6 rule. If this parameter is not specified, packets with any source IPv6 address are matched. - *source-ipv6-address*: specifies the source IPv6 address of data packets. - *prefix-length*: specifies the prefix of the source IPv6 address. - **postfix** *postfix-length*: specifies the length of source address postfix. - *wildcard*: specifies the wildcard mask of the address. - **any**: indicates any source IPv6 address of packets. - **ucl-group name** *source-ucl-group-name*: specifies the name of the UCL group to which the source IPv6 address of packets belongs. - **ucl-group** *source-ucl-group-index*: specifies the ID of the UCL group to which the source IPv6 address of packets belongs. **NOTE** In a stack, if the source IP address of the S5735S-H and S5736-S is specified as **ucl-group**, inter-card traffic forwarding does not take effect.	- *source-ipv6-address*: The value is in colon hexadecimal notation. - *prefix-length*: The value is an integer that ranges from 1 to 128. - *postfix-length*: The value is an integer that ranges from 1 to 64. - *wildcard*: The value is in colon hexadecimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter. The values 1 and 0 can be discontinuous. For example, the IPv6 address FC00::1 and the wildcard mask 0::2 indicate that the address is FC00::00*x*1, where *x* can be any value from 0 to F in hexadecimal notation. - *source-ucl-group-name*: The value must be the name of an existing UCL group. - *source-ucl-group-index*: The value is an integer and must be the index of an existing UCL group. When the value is 0, the source address of packet matching the ACL rule is beyond the UCL group range.

Parameter	Description	Value
destination { *destination-ipv6-address prefix-length* | *destination-ipv6-address/ prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | *destination-ipv6-address wildcard* | **any** }	Indicates the destination IPv6 address of packets that match ACL6 rules. If this parameter is not specified, packets with any destination IPv6 address are matched. • *destination-ipv6-address*: specifies the destination IPv6 address of data packets. • *prefix-length*: specifies the prefix of the destination IPv6 address. • **postfix** *postfix-length*: specifies the length of destination address postfix. • *wildcard*: specifies the wildcard mask of the address. • **any**: indicates any destination IPv6 address of packets.	• *destination-ipv6-address*: The value is in colon hexadecimal notation. • *prefix-length*: The value is an integer that ranges from 1 to 128. • *postfix-length*: The value is an integer that ranges from 1 to 64. • *wildcard*: The value is in colon hexadecimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter. The values 1 and 0 can be discontinuous. For example, the IPv6 address FC00::1 and the wildcard mask 0::2 indicate that the address is FC00::00*x*1, where *x* can be any value from 0 to F in hexadecimal notation.

Parameter	Description	Value
icmp6-type { *icmp6-name* | *icmp6-type* [*icmp6-code*] }	Indicates the type and code of ICMPv6 packets, which are valid only when the protocol of packets is ICMPv6. If this parameter is not specified, all ICMPv6 packets are matched. - *icmp6-name*: specifies the name of ICMPv6 packets. - *icmp6-type*: specifies the type of ICMPv6 packets. - *icmp6-code*: specifies the code of ICMPv6 packets.	*icmp6-type* is an integer that ranges from 0 to 255. *icmp6-code* is an integer that ranges from 0 to 255. The value of *cmp6-name* and the corresponding ICMPv6 type and ICMPv6 code are as described in **Table 14-17**.
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: - **eq** *port*: equal operator. - **gt** *port*: greater than operator. - **lt** *port*: smaller than operator. - **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. - When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* - When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* - When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: - **eq** *port*: equal operator. - **gt** *port*: greater than operator. - **lt** *port*: smaller than operator. - **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. - When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* - When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* - When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack (010000) or rst (000100).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-

Parameter	Description	Value
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL6 rules take effect. If this parameter is not specified, ACL6 rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value is a string of 1 to 32 characters.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance on the inbound interface.	The value must be an existing VPN instance name.

Table 14-17 Values of *cmp6-name* and the corresponding ICMPv6 type and ICMPv6 code

ICMPv6 Name	ICMPv6 Type	ICMPv6 Code
Echo	128	0
Echo-reply	129	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3

ICMPv6 Name	ICMPv6 Type	ICMPv6 Code
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Views

User ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user ACL6 defines rules to filter IPv6 packets based on the source IPv6 addresses or source User Control List (UCL) groups, destination IPv6 addresses, IPv6 protocol types, ICMPv6 types, TCP source/destination port numbers, UDP source/destination port numbers, and time ranges.

Currently, the user ACL6 can be applied only to the UCL groups of the NAC mode. To control the network access rights of users based on user groups, you can perform the following operations: configure a UCL group, associate user ACL6 rules with the UCL group so that the ACL6 rules apply to all users in the user group, configure packet filtering based on the user ACL6 to make the ACL6 take effect, and then apply the UCL group to the AAA service scheme.

Prerequisites

If the **ucl-group name** *source-ucl-group-name* parameter is configured for a rule, the source UCL groups must have been created by the **ucl-group** command.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Use this command with caution, especially when you delete an ACL6 rule that has been referenced.

Example

Add a rule to ACL6 6000 to reject all the IPv6 packets sent from UCL group group1 to network segment fc00:1::/64.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name group1
[HUAWEI] acl ipv6 6000
[HUAWEI-acl6-ucl-6000] rule deny ipv6 source ucl-group name group1 destination fc00:1:: 64
```

14.1.29 rule description

Function

The **rule description** command configures the description of an ACL rule.

The **undo rule description** command deletes the description of an ACL rule.

By default, no description is configured for an ACL rule.

Format

rule *rule-id* **description** *description*

undo rule *rule-id* **description**

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule.	The value must be an existing rule ID.
description *description*	Specifies the description of an ACL rule. You can configure the description to record an ACL rule in detail.	The value is a character string and contains a maximum of 127 characters.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

The *rule-id* parameter identifies a rule, but cannot describe the meaning and usage of the rule. The description with a character string can be used to solve the problem.

Prerequisites

The ACL rule has been created. If the ACL rule does not exist, the system displays an error message when you run this command.

Precautions

If the **rule description** command is run repeatedly, the latest configuration takes effect.

After you run the **undo rule** *rule-id* command, the rule and rule description are deleted.

Example

Configure the description for rule 5 in acl 2001, which permits the packets from 192.168.32.1.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 permit source 192.168.32.1 0
[HUAWEI-acl-basic-2001] rule 5 description permit 192.168.32.1
[HUAWEI-acl-basic-2001] display acl 2001
Basic ACL 2001, 1 rule
Acl's step is 5
 rule 5 permit source 192.168.32.1 0
 rule 5 description permit 192.168.32.1
```

14.1.30 step

Function

The **step** command sets the step between ACL rule IDs.

The **undo step** command restores the default step between ACL rule IDs.

By default, the step between ACL rule IDs is 5.

Format

step *step*

undo step

Parameters

Parameter	Description	Value
step	Specifies the step between ACL rule IDs.	The value is an integer that ranges from 1 to 20.

Views

ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The step is the difference between rule IDs when the system automatically assigns rule IDs. For example, if the ACL step value is set to 5, rules are numbered 5, 10, 15, and so on.

To add a rule between existing rules, you need to reset the step. For example, an ACL in **config** mode contains three rules with IDs being 5, 10, and 15. To insert a new rule after rule 5 (the first rule), run the **rule 7** *xxxx* command to insert rule 7.

If the step value is changed, ACL rule IDs are arranged automatically. For example, if the original rule IDs are 5, 10, and 15, the rule IDs become 2, 4, and 6 after you change the step value to 2.

NOTE

The **undo step** command can be used to realign ACL rule IDs immediately based on the default step. For example, ACL rule group 3001 contains four rules with IDs being 1, 3, 5, and 7, and the step is 2. After the **undo step** command is executed, the rule IDs become 5, 10, 15, and 20 and the step value is restored to 5.

Prerequisites

An ACL has been created by running the **acl** command.

Precautions

The ACL6 does not support the step.

Example

Set the step between rules in ACL 3101 to 2.

```
<HUAWEI> system-view
[HUAWEI] acl 3101
[HUAWEI-acl-adv-3101] step 2
```

14.1.31 time-range

Function

The **time-range** command sets a time range.

The **undo time-range** command deletes a time range.

By default, no time range is set.

Format

time-range *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*] }

undo time-range *time-name* [*start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*]]

Parameters

Parameter	Description	Value
time-name	Specifies the name of a time range.	The value is a string of case-sensitive characters without spaces and must begin with a letter. The value ranges from 1 to 32. To avoid confusion, do not use "all" as the name of a time range.
start-time	Specify the start time of a time range.	The format is hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59.
end-time	Specify the end time of a time range.	The format is hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59.

Parameter	Description	Value
days	Specifies the date on which the time range takes effect.	The value can be one of the following: ● The numbers 0 to 6 indicate that the time range takes effect from Sunday to Saturday. The number 0 refers to Sunday. ● A weekday includes Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. ● The value "Daily" indicates that the time range takes effect during the seven days in a week. ● The value "off-day" indicates that the time range takes effect on weekends including Saturday and Sunday. ● The value "Working-day" indicates that the time range takes effect in five days from Monday to Friday.

Parameter	Description	Value
from *time1 date1*	Specifies the time for the time range to take effect.	*time1* is in the format of hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59. *date1* is in the format of yyyy/mm/dd. ● *yyyy* specifies the year. The value is an integer that ranges from 1970 to 2099. ● *mm* specifies the month. The value is an integer that ranges from 1 to 12. ● *dd* specifies the day. The value is an integer that ranges from 1 to 31.
to *time2 date2*	Specifies the end of a time range.	The formats *time2* and *date2* are the same as those of the start time. The end time must be later than the start time. If the end time is not set, the device takes the maximum value allowed by the system.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If some services or functions need to be started at intervals or periodically, you can run the **time-range** command to set the time range. When configuring ACL or ACL6 rules, you can reference the names of time ranges.

The time range is classified into the following types:

- Relative time range (periodic time range): It is specified by *start-time* and *end-time*. The weekday when the time range takes effect is determined by *days*.
- Absolute time range: It is specified by **from** and **to**. The absolute time range can be used to limit the periodic time range.

You can set the same name for multiple time ranges to describe a special period. If multiple time ranges have the same name, the periodic time ranges are ORed, and a periodic time range and a definite time range are ANDed. For example, three time ranges are set with the same name **test**:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** takes effect at 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in the year 2010.

Precautions

There may be a time difference of no more than 10 seconds between the configured time range and the time range that actually takes effect.

Example

Set a time range named **test** that takes effect from 2010-01-01 00:00 to 2010-12-31 23:59.

```
<HUAWEI> system-view
[HUAWEI] time-range test from 0:0 2010/1/1 to 23:59 2010/12/31
```

Set a time range named **test** that takes effect at 8:00-18:00 from Monday to Friday.

```
<HUAWEI> system-view
[HUAWEI] time-range test 8:00 to 18:00 working-day
```

Set a time range named **test** that takes effect from 14:00 to 18:00 on every Saturday and Sunday.

```
<HUAWEI> system-view
[HUAWEI] time-range test 14:00 to 18:00 off-day
```

14.2 Local Attack Defense Configuration Commands

14.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.2.2 auto-defend attack-packet sample

Function

The **auto-defend attack-packet sample** command sets the packet sampling ratio for attack source tracing.

The **undo auto-defend attack-packet sample** command restores the default packet sampling ratio.

By default, the packet sampling ratio is 5. That is, one packet is sampled in every 5 packets.

Format

auto-defend attack-packet sample *sample-value*

undo auto-defend attack-packet sample

Parameters

Parameter	Description	Value
sample-value	Specifies the packet sampling ratio for attack source tracing.	The value is an integer that ranges from 1 to 1024.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attack source tracing samples packets to identify attacks. Errors may occur in attack packet identification or packet rate calculation. A proper packet sampling ratio can reduce errors. A small sampling ratio makes the attack source tracing result accurate, but increases CPU usage. For example, when the sampling ratio is set to 1, every packet is sampled. The attack source tracing result is accurate, but the CPU usage is high because every packet is resolved.

The **auto-defend attack-packet sample** command sets the sampling ratio. You can set a proper value based on the requirements of attack source tracing precision and CPU usage.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

When a smaller attack source tracing threshold is used, the sampling ratio has greater impact on the attack source tracing result.

Example

Set the sampling ratio for attack source tracing in the attack defense policy named **test** to 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend attack-packet sample 2
```

14.2.3 auto-defend enable

Function

The **auto-defend enable** command enables automatic attack source tracing.

The **undo auto-defend enable** command disables automatic attack source tracing.

By default, attack source tracing is enabled.

Format

auto-defend enable

undo auto-defend enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of attack packets may attack the device CPU. Attack source tracing enables the device to trace attack sources and send logs or alarms to notify the administrator so that the administrator can take measures to defend against the attacks. By default, logs are sent to notify the administrator if attack source tracing is enabled.

After automatic attack source tracing is enabled, the device traces the source of the specified packets sent to the CPU. The packet type can be set using the **auto-defend protocol** command.

Precautions

Attack source tracing configured in an attack defense policy takes effect only when the attack defense policy is applied in the system view.

If the system software of a switch in a version earlier than V200R009C00 is upgraded to V200R009C00 or later version, an **undo auto-defend enable** configuration is automatically generated.

Example

Enable attack source tracing in the attack defense policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
```

14.2.4 auto-defend action

Function

The **auto-defend action** command enables the attack source **punish** function and specifies a **punish** action.

The **undo auto-defend action** command disables the attack source **punish** function.

By default, the attack source **punish** function is disabled.

Format

auto-defend action { **deny** [**timer** *time-length*] | **error-down** }

undo auto-defend action

Parameters

Parameter	Description	Value
deny	Discards packets sent from an attack source.	-
timer *time-length*	Specifies the period during which packets sent from an identified attack source are discarded.	The value ranges from 1 to 86400, in seconds. The default value is 300.
error-down	Sets the interface that receives attack packets to the error-down state.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend action** command is applied to taking attack source **punish** actions. The device discards the packets sent from the identified source or sets the interface receiving attack packets to the error-down state.

NOTE

If the auto-defend action is set to **error-down**, run the **error-down auto-recovery cause auto-defend interval** *interval-value* command to set a recovery delay before the device is attacked. This command is invalid for the interface in error-down state.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend action** command multiple times, only the latest configuration takes effect.

After the auto-defend action is set to **deny**, the device discards packets when being attacked. The configuration result can be verified using the **display auto-defend attack-source** command.

The device does not take **punish** actions on attack sources of whitelist users.

Attack source tracing configured in an attack defense policy takes effect only when the attack defense policy is applied in the system view.

NOTICE

If the device sets the interface that receives the attack packets to the error-down state, services of authorized users on the interface are interrupted. Exercise caution when you configure the device to set the interface to the error-down state.

Example

Configure the device to discard packets from the identified source every 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend action deny timer 10
Info: This configuration may cause packet loss.
```

14.2.5 auto-defend alarm enable

Function

The **auto-defend alarm enable** command enables the event reporting function for attack source tracing.

The **undo auto-defend alarm enable** command disables the event reporting function for attack source tracing.

By default, the event reporting function for attack source tracing is disabled.

Format

auto-defend alarm enable

undo auto-defend alarm enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of packets of a specified protocol from an attack source exceeds the threshold in a specified period, the device reports an event to the administrator so that the administrator can take measures to protect the device.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Follow-up Procedure

Run the **auto-defend threshold** command to set the event reporting threshold for attack source tracing.

Example

Enable the event reporting function in the attack defense policy **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend alarm enable
```

14.2.6 auto-defend protocol

Function

The **auto-defend protocol** command specifies the types of protocol packets that the device monitors in attack source tracing.

The **undo auto-defend protocol** command deletes specified types of protocol packets that the device monitors in attack source tracing.

By default, the device traces sources of 8021X, ARP, DHCP, DHCPv6, ICMP, ICMPv6, IGMP, MLD, ND, TCP, TCPv6, and Telnet packets in attack source tracing.

Format

auto-defend protocol { **all** | { **8021x** | **arp** | **dhcp** | **dhcpv6** | **icmp** | **icmpv6** | **igmp** | **mld** | **nd** | **tcp** | **tcpv6** | **telnet** | **ttl-expired** | **udp** | **udpv6** | **ospf** | **isis** | **rip** }* }

undo auto-defend protocol { **8021x** | **arp** | **dhcp** | **dhcpv6** | **icmp** | **icmpv6** | **igmp** | **mld** | **nd** | **tcp** | **tcpv6** | **telnet** | **ttl-expired** | **udp** | **udpv6** | **ospf** | **isis** | **rip** }*

NOTE

The **tcpv6** parameter is not supported by the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S5735S-S, S500, and S5735-S-I.

Parameters

Parameter	Description	Value
all	Configures the device to trace sources of 8021X, ARP, DHCP, DHCPv6, ICMP, ICMPv6, IGMP, MLD, ND, TCP, TCPv6, Telnet, TTL-expired, UDPv6, and UDP packets in attack source tracing.	-
8021x	Adds 8021X packets to the list of traced packets or removes 8021X packets from the list.	-
arp	Adds ARP packets to the list of traced packets or removes ARP packets from the list.	-
dhcp	Adds DHCP packets to the list of traced packets or removes DHCP packets from the list.	-

Parameter	Description	Value
dhcpv6	Adds DHCPv6 packets to the list of traced packets or removes DHCPv6 packets from the list.	-
icmp	Adds ICMP packets to the list of traced packets or removes ICMP packets from the list.	-
icmpv6	Adds ICMPv6 packets to the list of traced packets or removes ICMPv6 packets from the list.	-
igmp	Adds IGMP packets to the list of traced packets or removes IGMP packets from the list.	-
mld	Adds MLD packets to the list of traced packets or removes MLD packets from the list.	-
nd	Adds ND packets to the list of traced packets or removes ND packets from the list.	-
tcp	Adds TCP packets to the list of traced packets or removes TCP packets from the list.	-
tcpv6	Adds TCPv6 packets to the list of traced packets or removes TCPv6 packets from the list.	-
telnet	Adds Telnet packets to the list of traced packets or removes Telnet packets from the list.	-
ttl-expired	Adds TTL-expired packets to the list of traced packets or removes TTL-expired packets from the list.	-

Parameter	Description	Value
udp	Adds UDP packets to the list of traced packets or removes UDP packets from the list.	-
udpv6	Adds UDPv6 packets to the list of traced packets or removes UDPv6 packets from the list.	-
ospf	Adds OSPF packets to the list of traced packets or removes OSPF packets from the list.	-
isis	Adds IS-IS packets to the list of traced packets or removes IS-IS packets from the list.	-
rip	Adds RIP packets to the list of traced packets or removes RIP packets from the list.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend protocol** command is applied to the packet parsing phase. When an attack occurs, you cannot identify the type of attack packets. The **auto-defend protocol** command allows you to flexibly specify the types of traced packets.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

- If you run this command multiple times, only the latest configuration takes effect.

- If a packet type is specified, when the device is attacked and the attack source is traced, you can run the **display auto-defend attack-source** command to view attack source information.

Example

Delete IGMP and TTL-expired packets from the list of traced packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] undo auto-defend protocol igmp ttl-expired
```

14.2.7 auto-defend threshold

Function

The **auto-defend threshold** command sets the checking threshold and event reporting threshold for attack source tracing.

The **undo auto-defend threshold** command restores the default checking threshold and event reporting threshold for attack source tracing.

By default, the checking threshold and event reporting threshold for attack source tracing is 60 pps.

Format

auto-defend threshold *threshold*

undo auto-defend threshold

Parameters

Parameter	Description	Value
threshold	Specifies the checking threshold and event reporting threshold for attack source tracing.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack source tracing is enabled, you can set the checking threshold and event reporting threshold for attack source tracing. When the number of sent protocol packets from an attack source in a specified period exceeds the checking threshold, the device traces and logs the attack source.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend threshold** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

After the **auto-defend enable** command is executed, the device traces the attack source based on the default threshold even if the **auto-defend threshold** command is not used.

Example

Set the checking threshold and event reporting threshold for attack source tracing in the attack defense policy named **test** to 200 pps.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend threshold 200
```

14.2.8 auto-defend trace-type

Function

The **auto-defend trace-type** command configures an attack source tracing mode.

The **undo auto-defend trace-type** command deletes an attack source tracing mode.

By default, attack source tracing is based on source IP addresses and source MAC addresses.

Format

auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

undo auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

Parameters

Parameter	Description	Value
source-mac	Configures attack source tracing based on source MAC addresses so that the device classifies and collects statistics based on the source MAC address and identifies the attack source.	-

Parameter	Description	Value
source-ip	Configures attack source tracing based on source IP addresses so that the device classifies and collects statistics based on the source IP address and identifies the attack source.	-
source-portvlan	Configures attack source tracing based on source ports +VLANs so that the device classifies and collects statistics based on the source port and VLAN and identifies the attack source.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling attack source tracing, you can specify one or more attack source tracing modes. The device then uses the specified modes to trace attack sources.

The device supports the following attack source tracing modes:

- Source IP address-based tracing: defends against Layer 3 attack packets.
- Source MAC address-based tracing: defends against Layer 2 attack packets with a fixed source MAC address.
- Source port+VLAN based tracing: defends against Layer 2 attack packets with different source MAC addresses.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

In VXLAN scenarios, the source port+VLAN based tracing mode is not supported. In addition, for the S6735-S, S6720-EI and S6720S-EI, the source IP address-based tracing mode is not supported.

Table 14-18 lists the attack source tracing modes supported for different types of packets.

Table 14-18 Attack source tracing modes supported for different types of packets

Packet Type	Attack Source Tracing Mode
802.1X	Based on source MAC addresses and based on source ports+VLANs
ARP, DHCP, IGMP, ND, DHCPv6, MLDv6	Based on source MAC addresses, based on IP addresses, and based on source ports+VLANs
ICMP, TTL-expired, Telnet, TCP, UDP, UDPv6	Based on source IP addresses and based on source ports+VLANs

If you run this command multiple times, only the latest configuration takes effect.

A switch supports different numbers if attack source tracing modes for different protocol packets. For details, see the default modes described above.

After the attack source tracing function is enabled on the device, you can run the **display auto-defend attack-source** command to view attack source tracing information if an attack occurs.

When the attack source tracing mode is **source-ip** and action is **error-down**, if multiple interfaces receive the attack packets with the same source IP address and the packet rate exceeds the threshold, the switch shuts down only one interface, and then checks packet rate again. If the packet rate is still higher than the threshold, the switch shuts down another interface. The switch repeats the operations until the packet rate falls below the threshold.

Example

Configure attack source tracing based on source MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] undo auto-defend trace-type source-ip source-portvlan
```

14.2.9 auto-defend whitelist

Function

The **auto-defend whitelist** command configures an attack source tracing whitelist. The switch does not trace the source of users in the whitelist.

The **undo auto-defend whitelist** command deletes an attack source tracing whitelist.

By default, no whitelist is configured for attack source tracing. If any of the following conditions is met, however, the switch uses the condition as the whitelist matching rule, regardless of whether attack source tracing is enabled. After attack source tracing is enabled, the switch does not perform attack source tracing for the packets matching such rules.

- If an application uses the TCP protocol and has set up a TCP connection with the switch, the switch will not consider TCP packets with the matching source IP address as attack packets. If no TCP packets match a source IP address within 1 hour, the rule that specifies this source IP address will be aged out.
- If an interface has been configured as a DHCP trusted interface using the **dhcp snooping trusted** command, the switch will not consider DHCP packets received from this interface as attack packets.
- If an interface has been configured as a MAC forced forwarding (MFF) network-side interface using the **mac-forced-forwarding network-port** command, the switch will not consider ARP packets received from this interface as attack packets.

For the preceding conditions, the switch supports a maximum of 16 whitelist matching rules based on source IP addresses and interfaces, and a maximum of 8 whitelist matching rules based on source IP addresses of TCP packets.

Format

auto-defend whitelist *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* }

undo auto-defend whitelist *whitelist-number* [**acl** *acl-number* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
whitelist-number	Specifies the number of a whitelist.	The value is an integer that ranges from 1 to 16.
acl *acl-number*	Specifies the number of an ACL referenced by a whitelist.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs
interface *interface-type interface-number*	Specifies the interface to which the whitelist is applied. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attack source tracing helps locate and punish sources of denial of service (DoS) attacks. If some users do not need to be traced regardless of whether an attack occurs, run the **auto-defend whitelist** command to configure a whitelist for users.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

Before referencing an ACL in a whitelist, create the ACL and configure rules.

If the ACL referenced by the whitelist specifies some protocols, ensure that packets of these protocols can be traced. You can run the **display auto-defend configuration** command to view the protocols supported by attack source tracing. If a protocol is not supported by attack source tracing, you can run the **auto-defend protocol** command to configure attack source tracing to support the protocol.

Example

Add source IP addresses 10.1.1.1 and 10.1.1.2 to the attack source tracing whitelist.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.2 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend whitelist 1 acl 2000
```

14.2.10 auto-port-defend aging-time

Function

The **auto-port-defend aging-time** command configures the aging time for port attack defense.

The **undo auto-port-defend aging-time** command restores the default aging time for port attack defense.

By default, the aging time for port attack defense is 300 seconds.

Format

auto-port-defend aging-time *time*

undo auto-port-defend aging-time [*time*]

Parameters

Parameter	Description	Value
aging-time *time*	Specifies the aging time for port attack defense.	The value is an integer that ranges from 30 to 86400, and must be a multiple of 10. The unit is second.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a device with port attack defense function enabled detects an attack on a port, the device traces the source and limits the rate of the attack packets on the port within the aging time (T seconds). When the aging time expires, the device calculates the protocol packet rate on the port again. If the rate is still above the protocol rate threshold, the device keeps tracing the source and limits the rate of the attack packets; otherwise, the device stops the operations.

If the aging time is too short, the device frequently starts packet rate detection on ports, which consumes CPU resources. If the aging time is too long, protocol packets cannot be promptly processed by the CPU, which affects services. Therefore, you need to run the **auto-port-defend aging-time** command to set an appropriate aging time according to the CPU usage and service status.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Precautions

If you run the **auto-port-defend aging-time** command multiple times in the same attack defense policy view, only the latest configuration takes effect.

Example

Set the aging time in the attack defense policy **test** view to 350 seconds.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend aging-time 350
```

14.2.11 auto-port-defend alarm enable

Function

The **auto-port-defend alarm enable** command enables the report of port attack defense events.

The **undo auto-port-defend alarm enable** command disables the report of port attack defense events.

By default, port attack defense events are not reported.

Format

auto-port-defend alarm enable

undo auto-port-defend alarm enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a port undergoes a DoS attack, the malicious attack packets sent from this port to the CPU occupy bandwidth. As a result, the CPU cannot process the protocol packets sent from other ports, and services are interrupted. In this situation, you can enable the report of port attack defense events. When the rate of protocol packets on a port exceeds the check threshold, the switch reports an event to notify the network administrator, so that the administrator can promptly take measures to protect the switch.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Follow-up Procedure

Run the **auto-port-defend protocol threshold** command to set the threshold for protocol packet check in port attack defense.

Example

Enable the report of port attack defense events in the attack defense policy **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend alarm enable
```

14.2.12 auto-port-defend enable

Function

The **auto-port-defend enable** command enables the port attack defense function.

The **undo auto-port-defend enable** command disables the port attack defense function.

By default, the port attack defense function is enabled.

Format

auto-port-defend enable

undo auto-port-defend enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker initiates a DoS attack on a port, the malicious attack packets sent from this port to the CPU occupy bandwidth. As a result, the CPU cannot process the protocol packets sent from other ports, and services are interrupted.

The port attack defense function effectively limits the number of packets sent to the CPU, and prevents DoS attacks aiming at the CPU.

This function is enabled by default. If the number of packets received by a port within one second exceeds the protocol rate threshold, the device considers that an attack occurs on the port. Then the device traces the source and limits the rate of attack packets, and records an attack log to avoid impact on other ports.

Precautions

After the port attack defense function is enabled in an attack defense policy, the attack defense policy must be applied in the system view.

Example

Enable the port attack defense function in the attack defense policy **test** view.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
```

14.2.13 auto-port-defend protocol

Function

The **auto-port-defend protocol** command specifies the types of protocol packets to which port attack defense is applied.

The **undo auto-port-defend protocol** command cancels port attack defense for certain types of protocol packets.

By default, port attack defense is applicable to ARP Request, Unicast ARP Request packets, ARP Reply, DHCP, ICMP, IGMP, IP fragment, and ND packets.

Format

auto-port-defend protocol { **all** | { **arp-request** | **arp-request-uc** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** | **nd** } * }

undo auto-port-defend protocol { **arp-request** | **arp-request-uc** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** | **nd** } *

NOTE

- S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, and S5736-S do not support **arp-request-uc** parameter.
- S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, and S5736-S do not support **icmp** and **ip-fragment** parameter.
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S do not support **nd** parameter.

Parameters

Parameter	Description	Value
all	Applies port attack defense to ARP Request, Unicast ARP request, ARP Reply, DHCP, ICMP, IGMP, IP fragment, and ND packets.	-
arp-request	Applies port attack defense to ARP Request packets or cancels port attack defense for ARP Request packets.	-

Parameter	Description	Value
arp-request-uc	Applies port attack defense to Unicast ARP Request packets or cancels port attack defense for Unicast ARP request packets.	-
arp-reply	Applies port attack defense to ARP Reply packets or cancels port attack defense for ARP Reply packets.	-
dhcp	Applies port attack defense to DHCP packets or cancels port attack defense for DHCP packets.	-
icmp	Applies port attack defense to ICMP packets or cancels port attack defense for ICMP packets.	-
igmp	Applies port attack defense to IGMP packets or cancels port attack defense for IGMP packets.	-
ip-fragment	Applies port attack defense to IP fragment packets or cancels port attack defense for IP fragment packets.	-
nd	Applies port attack defense to ND packets or cancels port attack defense for ND packets.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device calculates the rate of all protocol packets, including ARP Request, ARP Reply, DHCP, ICMP, IGMP, and IP fragment packets, received by a port, and traces the source and limits the rate of attack packets. If the packets exceeding protocol rate threshold contain only a few attack packets, you can run the **undo auto-port-defend protocol** command to cancel port attack defense for unneeded protocol types. If the device limits the rate of too many protocols, services are affected.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Precautions

If you run this command multiple times in the same attack defense policy view, only the latest configuration takes effect.

After port attack defense is applied to a type of protocol packets, the **display auto-port-defend attack-source** command can display the attack source tracing information if the port is attacked by the specified protocol packets.

Example

In the attack defense policy **test**, cancel port attack defense for ARP Reply packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] undo auto-port-defend protocol arp-reply
```

14.2.14 auto-port-defend protocol threshold

Function

The **auto-port-defend protocol threshold** command sets the protocol packet rate threshold for port attack defense.

The **undo auto-port-defend protocol threshold** command restores the default protocol packet rate threshold for port attack defense.

The following table lists the default rate thresholds for different protocols.

Packet Type	Rate Threshold
arp-request	60 pps for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-EI, S6735-S, and S6720-EI, 120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, and 30 pps for other switch models

Packet Type	Rate Threshold
arp-request-uc	60 pps for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-EI, S6735-S, and S6720-EI, 120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S
arp-reply	60 pps for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-EI, S6735-S, and S6720-EI, 120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, and 30 pps for other switch models
dhcp	● 60 pps for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-EI, S6735-S, and S6720-EI, 120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, and 30 pps for other switch models
icmp	120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, and 60 pps for other switch models
igmp	120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, and 60 pps for other switch models
ip-fragment	30 pps
nd	60 pps for the S6720S-EI, S6735-S and S6720-EI, 120 pps for the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, and 30 pps for other switch models

Format

auto-port-defend protocol { **all** | **arp-request** | **arp-request-uc** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** | **nd** } **threshold** *threshold*

undo auto-port-defend protocol { **all** | **arp-request** | **arp-request-uc** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** | **nd** } **threshold** [*threshold*]

NOTE

- S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, and S5736-S do not support **arp-request-uc** parameter.
- S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, and S5736-S do not support **icmp** and **ip-fragment** parameter.
- S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S do not support **nd** parameter.

Parameters

Parameter	Description	Value
all	Sets the rate thresholds for ARP Request, Unicast ARP Request, ARP Reply, DHCP, ICMP, IGMP, IP fragment, and ND packets.	-
arp-request	Specifies the rate threshold for ARP Request packets.	-
arp-request-uc	Specifies the rate threshold for Unicast ARP request packets.	-
arp-reply	Specifies the rate threshold for ARP Reply packets.	-
dhcp	Specifies the rate threshold for DHCP packets.	-
icmp	Specifies the rate threshold for ICMP packets.	-
igmp	Specifies the rate threshold for IGMP packets.	-
ip-fragment	Specifies the rate threshold for IP fragment packets.	-
nd	Specifies the rate threshold for ND packets.	-
threshold *threshold*	Specifies the protocol rate threshold.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port attack defense is enabled on a port, the device calculates the rate of affected protocol packets received by the port. If the packet rate exceeds the protocol rate threshold, the device considers that an attack occurs. Then the device traces the source and limits the rate of attack packets on the port, and records a log. The device moves the packets within the protocol rate limit (CPCAR in attack defense policies) to the low-priority queue, and then sends them to the CPU.Port Attack Defense The device discards the excess packets.

You need to set an appropriate rate threshold for port attack defense according to service requirements. If the CPU fails to process many protocol packets promptly after port attack defense is enabled, set a large packet rate threshold. If the CPU is busy processing the packets of a protocol, set a small rate threshold for this protocol to avoid impact on other services.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Precautions

If you run the **auto-port-defend protocol threshold** command multiple times in the same attack defense policy view, only the latest configuration takes effect.

Example

In the attack defense policy **test**, set the rate threshold for ARP Request packets to 40 pps.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend protocol arp-request threshold 40
```

14.2.15 auto-port-defend sample

Function

The **auto-port-defend sample** command sets the protocol packet sampling ratio for port attack defense.

The **undo auto-port-defend sample** command restores the default protocol packet sampling ratio for port attack defense.

By default, the protocol packet sampling ratio for port attack defense is 5. That is, one packet is sampled when every 5 packets are received.

Format

auto-port-defend sample *sample-value*

undo auto-port-defend sample [*sample-value*]

Parameters

Parameter	Description	Value
sample *sample-value*	Specifies the protocol packet sampling ratio for port attack defense.	The value is an integer that ranges from 1 to 1024.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device with port attack defense enabled identifies attacks by analyzing sampled packets. There may be errors in attack packet identification or packet rate calculation. Errors influence the attack defense effect. An appropriate sampling ratio helps you control attack defense accuracy.

A small sampling ratio improves attack defense accuracy, but consumes more CPU resources. When the sampling ratio is set to 1, the device analyzes every packet. The attack packets can be detected quickly, but CPU usage becomes high and services are affected. Therefore, make a balance between the attack defense requirement and CPU usage to decide a sampling ratio.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Precautions

If the protocol packet rate threshold for port attack defense is set to a small value, the attack identification error caused by packet sampling ratio is large.

Example

Set the protocol packet sampling ratio to 4 in the attack defense policy **test** view.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend sample 4
```

14.2.16 auto-port-defend whitelist

Function

The **auto-port-defend whitelist** command configures a whitelist for port attack defense.

The **undo auto-port-defend whitelist** command deletes a whitelist for port attack defense.

By default, no whitelist is configured for port attack defense. If any of the following conditions is met, however, the switch uses the condition as the whitelist matching rule, regardless of whether port attack defense is enabled. After port attack defense is enabled, the switch does not perform port attack defense for the packets matching such rules.

- If an interface has been configured as a DHCP trusted interface using the **dhcp snooping trusted** command, the switch will not consider DHCP packets received from this interface as attack packets.
- If an interface has been configured as a MAC forced forwarding (MFF) network-side interface using the **mac-forced-forwarding network-port** command, the switch will not consider ARP packets received from this interface as attack packets.

For the preceding conditions, the switch supports a maximum of 16 whitelist matching rules based on source IP addresses and interfaces.

Format

auto-port-defend whitelist *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* }

undo auto-port-defend whitelist *whitelist-number* [**acl** *acl-number* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
whitelist-number	Specifies the number of the whitelist configured for port attack defense.	The value is an integer that ranges from 1 to 16.
acl *acl-number*	Specifies the number of the ACL applied to the whitelist.	The value of *acl-number* is an integer that ranges from 2000 to 4999. • 2000 to 2999: basic ACLs • 3000 to 3999: advanced ACLs • 4000 to 4999: Layer 2 ACLs

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface to which the whitelist is applied. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The port attack defense function is enabled by default on the device, so the device calculates protocol packet rates on all interfaces, and traces the source and limits the rate of attack packets. In some services, network-side interfaces need to receive a lot of valid protocol packets. You should add these interfaces or network nodes connecting to these interfaces to the whitelist. The device does not trace the source or limit the rate of protocol packets received by the interfaces in the whitelist.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Precautions

To define the whitelist using an ACL, you must create an ACL and configure rules for the ACL.

Before configuring an ACL whitelist for some protocols, ensure that the port attack defense function supports these protocols. Use the **auto-port-defend protocol** command to specify the protocols to which port attack defense is applied.

Example

In the attack defense policy **test**, configure a whitelist that references an ACL. The ACL permits the packets from the users with IP addresses 10.1.1.1 and 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.2 0
[HUAWEI-acl-basic-2000] quit
```

```
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend whitelist 1 acl 2000
```

In the attack defense policy **test**, add interface GE0/0/1 to the whitelist for port attack defense.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend whitelist 1 interface gigabitethernet 0/0/1
```

14.2.17 blacklist

Function

The **blacklist** command configures a blacklist.

The **undo blacklist** command deletes a blacklist.

By default, no blacklist is configured.

Format

IPv4 blacklist:

blacklist *blacklist-id* **acl** *acl-number1*

undo blacklist *blacklist-id*

IPv6 blacklist:

blacklist *blacklist-id* **acl ipv6** *acl-number2*

undo blacklist *blacklist-id*

Blacklist that discards the packets matching ACL rules in the forwarding chip:

blacklist *blacklist-id* **acl** *acl-number3* **hard-drop**

undo blacklist *blacklist-id*

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6720S-S, and S5736-S support the blacklist that discards the packets matching ACL rules in the forwarding chip.

Parameters

Parameter	Description	Value
blacklist-id	Specifies the ID of a blacklist.	The value is an integer that ranges from 1 to 8.

Parameter	Description	Value
acl *acl-number1*	Specifies the number of an Access Control List (ACL) referenced by a blacklist.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs
acl ipv6 *acl-number2*	Specifies the ACL matching the IPv6 blacklist.	The value of *acl-number2* is an integer that ranges from 3000 to 3999.
acl *acl-number3*	Specifies the ACL matching the IPv4 blacklist.	The value of *acl-number3* is an integer that ranges from 3000 to 3999.
hard-drop	Discards the packets matching the blacklist in the forwarding chip.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

To defend against malicious packet attacks, the device uses ACLs to add users with the specific characteristic into a blacklist and discards the packets from the users in the blacklist. In addition, for SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6720S-S, and S5736-S, packets matching the IPv4 blacklist are sent to the CPU first, and then discarded. To discard the packets directly without sending them to the CPU, you can run the **blacklist** *blacklist-id* **acl** *acl-number3* **hard-drop** command. This function can reduce impact of malicious packets on the CPU usage, and applies to only IPv4 packets.

An attack defense policy can contain a maximum of eight blacklists (including IPv4 and IPv6 blacklists and the blacklist that discards the packets matching ACL rules).

For S6735-S, S6720-EI, and S6720S-EI, packets sent from blacklisted users are discarded after traffic statistics are collected; therefore, you can run the **display cpu-defend statistics** command to view statistics on the packets sent from blacklisted users. For other device models, the statistics on discarded packets collected by the **display cpu-defend statistics** command do not contain the statistics on the packets sent from blacklisted users.

Example

Specify ACL 2001 as the rule of blacklist 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist 2 acl 2001
Info: This configuration may cause packet loss.
```

Apply ACL 3001 to IPv6 blacklist 3.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist 3 acl ipv6 3001
Info: This configuration may cause packet loss.
```

Apply ACL 3006 to blacklist 5 to discard the packets matching ACL 3006 in the forwarding chip.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist 5 acl 3006 hard-drop
Info: This configuration may cause packet loss.
```

14.2.18 car (attack defense policy view)

Function

The **car** command sets the rate limit for packets sent to the CPU.

The **undo car** command restores the default rate limit for packets sent to the CPU.

By default, the CIR value for user-defined flows is 64 kbit/s. You can run the **display cpu-defend configuration** command to check the CAR values for protocol packets.

Format

car { **packet-type** *packet-type* | **user-defined-flow** *flow-id* } **cir** *cir-value* [**cbs** *cbs-value*]

undo car { **packet-type** *packet-type* | **user-defined-flow** *flow-id* }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the type of packets.	The supported packet type depends on the device.

Parameter	Description	Value
user-defined-flow *flow-id*	Specifies the ID of the user-defined flow. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter.	The value is an integer that ranges from 1 to 8.
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer. - The value of **packet-type** *packet-type* varies according to packet types. The value range can be displayed after you press ? following the command. - The value of **user-defined-flow** *flow-id* ranges from 24 to 4096 for the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S and from 8 to 4096 for the S6720-EI and S6720S-EI, in kbit/s. **NOTE** The minimum value that can take effect for different models may be greater than the configurable minimum value. If the configured value is smaller than the minimum value that can take effect, the minimum value that can take effect will be used. You can run the **display cpu-defend applied** command to view the value that actually takes effect.
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer. - The value of **packet-type** *packet-type* varies according to packet types. The value range can be displayed after you press ? following the command. If the **cbs** is not set, the default *cbs-value* is 188 times the *cir-value*. - The value of **user-defined-flow** *flow-id* ranges from 10000 to 800000, in bytes. If the **cbs** is not set, the default *cbs-value* is 188 times the *cir-value*.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch has default CAR values for each type of protocol packet. You can adjust CAR values for specified types of protocol packets based on services and network environment.

After an attack defense policy is created, you can limit the rate of protocol packets using the policy:

- Reduce the CAR values in the following situation: When a network undergoes an attack, reduce the CAR values of the corresponding protocol, to reduce impact on the system CPU.
- Increase the CAR values in the following situation: When service traffic volume on the network increases, a large number of protocol packets need to be sent to the CPU. Increase the CAR values of the corresponding protocols to meet service requirements.

NOTICE

Improper CPCAR settings will affect services on your network. If you need to adjust CPCAR settings, you are advised to contact technical support personnel for help.

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S the device limits the rate of some protocol packets in pps mode. That is, the actual CPCAR value is the number of packets allowed to pass per second, which is calculated as follows:

CIR value x 1024/(8 x Packet length)

For example, if the CIR value of https-syn packets is set to 64 kbit/s, 40 https-syn packets are allowed to pass per second. The number 40 is calculated as follows:

64 x 1024/(8 x 200) = 40.96 (rounded down to the integer 40)

The following table lists the types and lengths of packets that support rate limiting in pps mode.

Packet Type	Packet Length (Including Preamble and IFG)
nac-arp-reply, nac-arp-request, 8021x, 8021x-wireless, 8021x-start-wlan, 8021x-ident-wlan, 8021x-start, 8021x-ident, nac-nd, dot1x, dot1x identity	88
eap-key, capwap-other, capwap-ap-update, capwap-keepalive, capwap-airoaming	100
capwap-association, capwap-smart-roam, capwap-disassoc, capwap-station, capwap-ac-roam-syn	120
hw-tacacs, wapi, capwap-rf-neighbor, capwap-regular-rep, capwap-ap-auth, capwap-license-mng, capwap-ac-auth	128
portal	152
wlan-not-capwap, https-syn, ipsec-passby	200
capwap-discov-bc, capwap-discov-uc	256
dhcp-server	374
capwap-echo, radius, nac-dhcpv6	400
https-other, https-portal	500
sip	800

Precautions

If you run the **deny** command and then the **car** command, the **car** command takes effect; if you run the **car** command, and then the **deny** command, the **deny** command takes effect.

NOTE

When the actual and configured rates of packets sent to the CPU are large, the CPU usage may be high and the performance may deteriorate. In the worst situation, the stack breaks.

The S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S use the CAR values configured for FIB-hit packets to limit the rate of ND packets destined for the MAC address of the local switch, and limit rates of BPDU and CDP packets by using the CPCAR configured by the **car packet-type bpdu-tunnel cir** *cir-value* [**cbs** *cbs-value*] command.

Example

Set the rate limit in the attack defense policy named **test** for ARP Reply packets: set the CIR value to 64 kbit/s and the CBS value to 33000 bytes.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] car packet-type arp-reply cir 64 cbs 33000
Warning: Improper parameter settings may affect stable operating of the system. Use this command under
```

```
assistance of Huawei engineer
s. Continue? [Y/N]:y
```

14.2.19 cpu-defend application-apperceive enable

Function

The **cpu-defend application-apperceive enable** command enables active link protection (ALP). After the ALP is enabled, the CAR values of protocol packets set using **linkup-car** can take effect.

The **undo cpu-defend application-apperceive enable** command disables ALP.

By default, ALP is enabled on FTP, IPv6 FTP, HTTP, HTTPS, IP-CLOUD, IKE, IPSEC-ESP, SSH, TELNET, and TFTP packets and disabled on BGP, BGP4+, ISIS, OSPF, and OSPFv3 packets.

Format

cpu-defend application-apperceive [**bgp** | **bgp4plus** | **ftp** | **ftpv6** | **http** | **https** | **ike** | **ip-cloud** | **ipsec-esp** | **isis** | **ospf** | **ospfv3** | **ssh** | **telnet** | **tftp**] **enable**

undo cpu-defend application-apperceive [**bgp** | **bgp4plus** | **ftp** | **ftpv6** | **http** | **https** | **ike** | **ip-cloud** | **ipsec-esp** | **isis** | **ospf** | **ospfv3** | **ssh** | **telnet** | **tftp**] **enable**

NOTE

- Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **bgp** parameter.
- Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6735-S, S6720-EI, and S6720S-EI support the **ike** parameter.
- Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **ipsec-esp** parameter.
- Only the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720S-LI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **ospf** parameter.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **bgp4plus** and **isis** parameter.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **ospfv3** parameter.
- Only the S200, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H support the **ip-cloud** parameter.

Parameters

Parameter	Description	Value
bgp	Enables ALP on BGP packets.	-
bgp4plus	Enables ALP on BGP4+ packets.	-
ftp	Enables ALP on FTP packets.	-
ftpv6	Enables ALP on IPv6 FTP packets.	-
http	Enables ALP on HTTP packets.	-
https	Enables ALP on HTTPS packets.	-
ike	Enables ALP on IKE packets.	-
ip-cloud	Enables ALP on IP-CLOUD packets.	-
ipsec-esp	Enables ALP on IPSEC-ESP packets.	-
isis	Enables ALP on ISIS packets.	-
ospf	Enables ALP on OSPF packets.	-
ospfv3	Enables ALP on OSPFv3 packets.	-
ssh	Enables ALP on SSH packets.	-
telnet	Enables ALP on TELNET packets.	-
tftp	Enables ALP on TFTP packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default CAR value of BGP, BGP4+, FTP, IPv6 FTP, HTTP, HTTPS, IP-CLOUD, ISIS, OSPFv3, OSPF, IKE, IPSEC-ESP, SSH, TFTP, or TELNET protocol is small. When a switch uses these protocols to transfer files or set up connections with other hosts or devices, the number of protocol packets sharply increases in a short period. When the packet rate exceeds the limit, the protocol packets are dropped. The switch may also undergo attacks of other protocols. This affects data transmission and causes service interruption.

You can run the **cpu-defend application-apperceive** command to enable ALP for above protocols, ensuring normal operation of these related services when attacks occur. When a connection is set up, the switch sends packets at the rate of the CPCAR value configured using the **linkup-car** command. The CPCAR value can be set as required.

Precautions

To enable the ALP function for a certain protocol, run the **cpu-defend application-apperceive enable** command to enable ALP globally. For example, before enabling ALP for the TFTP protocol, run the **cpu-defend application-apperceive enable** command, and then the **cpu-defend application-apperceive tftp enable** command to make the configuration take effect.

Example

Enable ALP on BGP packets and set the CIR value to 256 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] linkup-car packet-type bgp cir 256
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend application-apperceive enable
[HUAWEI] cpu-defend application-apperceive bgp enable
```

14.2.20 cpu-defend dynamic-adjust enable

Function

The **cpu-defend dynamic-adjust enable** command enables adaptive CPCAR adjustment for protocol packets.

The **undo cpu-defend dynamic-adjust enable** command disables adaptive CPCAR adjustment for protocol packets and restores the default CPCAR values of protocol packets.

By default, adaptive CPCAR adjustment for protocol packets is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.

Format

cpu-defend dynamic-adjust [**packet-type** { **arp-reply** | **arp-request** | **arp-request-uc** | **dhcp-client** | **dhcp-server** | **igmp** | **nd** | **pim** }] **enable**

undo cpu-defend dynamic-adjust [**packet-type** { **arp-reply** | **arp-request** | **arp-request-uc** | **dhcp-client** | **dhcp-server** | **igmp** | **nd** | **pim** }] **enable**

Parameters

Parameter	Description	Value
packet-type	Specifies the type of protocol packets. **NOTE** If this parameter is not specified, adaptive CPCAR adjustment for protocol packets is enabled or disabled globally.	-
arp-reply	Specifies ARP reply packets.	-
arp-request	Specifies ARP request packets.	-
arp-request-uc	Specifies unicast ARP request packets.	-
dhcp-client	Specifies the packets sent by DHCP clients.	-
dhcp-server	Specifies the packets sent by DHCP servers.	-
igmp	Specifies IGMP packets.	-
nd	Specifies IPv6 ND packets.	-
pim	Specifies PIM protocol packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default CPCAR values for protocol packets may not meet the dynamic requirements on the rate of sending protocol packets to the CPU. To resolve this problem, you can run this command to enable the adaptive CPCAR adjustment function for protocol packets.

After adaptive CPCAR adjustment is enabled for a specified type of protocol packets, the device periodically detects whether the protocol packets are lost. If packet loss occurs in the last detection period, the device adjusts the CPCAR value of the protocol packets according to the CPU usage. If the CPU usage is low, the device increases the CPCAR value. If the CPU usage is high, the device decreases the CPCAR value. The new CPCAR values must be within the allowed range. If packet loss occurs due to congestion in the queue of protocol packets, the device restores the default CPCAR value of the protocol packets. You can run the **display cpu-defend dynamic-adjust history-record** command to view the historical adaptive CPCAR adjustment records.

The following table lists the supported protocol packet types and the maximum CPCAR values allowed after adjustment.

Protocol Packet Type	Description	Maximum CPCAR Value After Adjustment
arp-reply	ARP reply packets	Twice the default value
arp-request	ARP request packets	Twice the default value
arp-request-uc	Unicast ARP request packets	Twice the default value
dhcp-client	Packets sent by DHCP clients	1.5 times the default value
dhcp-server	Packets sent by DHCP servers	1.5 times the default value
igmp	IGMP packets	Twice the default value
nd	IPv6 ND packets	Twice the default value
pim	PIM protocol packets	1.5 times the default value

Precautions

- This function takes effect only when the default CPCAR values of protocol packets are not manually modified.
- After adaptive CPCAR adjustment for protocol packets is enabled globally, this function takes effect for all supported types of protocol packets.
- If this command is configured together with the **cpu-defend dynamic-car enable** command for the same type of protocol packets, this command takes effect.

Example

Enable adaptive CPCAR adjustment for ARP request packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend dynamic-adjust packet-type arp-request enable
```

14.2.21 cpu-defend dynamic-car enable

Function

The **cpu-defend dynamic-car enable** command enables a switch to dynamically adjust the default CIR value for protocol packets.

The **undo cpu-defend dynamic-car enable** command disables a switch from dynamically adjusting the default CIR value for protocol packets.

By default, dynamic adjustment of the default CIR value is enabled globally, but the switch is disabled from dynamically adjusting the default CIR value for VRRP and ARP protocol packets.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend dynamic-car [**arp** | **vrrp**] **enable**

undo cpu-defend dynamic-car [**arp** | **vrrp**] **enable**

Parameters

Parameter	Description	Value
arp	Enables the switch to dynamically adjust the default CIR value for ARP protocol packets.	-
vrrp	Enables the switch to dynamically adjust the default CIR value for VRRP protocol packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A fixed default CIR value may not adapt to dynamic requirements on rate limiting for protocol packets. The **cpu-defend dynamic-car enable** command enables a switch to dynamically adjust the default CIR value for protocol packets.

If the default CIR value for a protocol has never been changed, the switch dynamically adjusts the default CIR value for the protocol packets based on service scale (for example, number of dynamic ARP entries) and CPU usage to meet various service requirements. For details, see **Table 14-19**.

Table 14-19 Default CPCAR adjustment for ARP packets

X = Number of ARP Entries	Adjusted CPCAR
X ≤ 512	Unchanged
512 < X ≤ 1024	128 kbit/s (remain unchanged if the default CIR is greater than 128 kbit/s)
1024 < X ≤ 3072	256 kbit/s
3072 < X ≤ 4096	512 kbit/s
X > 4096	512 kbit/s

Table 14-20 Default CPCAR adjustment for VRRP packets

X = Number of VRRP Groups	Adjusted CPCAR
X ≤ 200	192 kbit/s
200 < X ≤ 300	256 kbit/s
300 < X ≤ 400	320 kbit/s
400 < X ≤ 500	384 kbit/s
500 < X ≤ 600	448 kbit/s
600 < X ≤ 1000	512 kbit/s

NOTE

When the number of entries increases, the CPCAR value is dynamically increased. When the CPU usage is between 70% to 98%, the dynamic CPCAR adjustment stops. If the CPU usage is greater than 98%, the default CPCAR value is used.

Precautions

The switch dynamically adjusts the default CIR value for VRRP or ARP protocol packets only when the function is enabled globally and on VRRP or ARP protocol packets.

The default CIR value dynamically adjusted only takes effect when the CIR value of the protocol packet is not manually changed.

After the default CPCAR setting is modified for ARP, only the CIR value for ARP reply, Unicast ARP request, and ARP request packets is adjusted.

Example

Enable the switch to dynamically adjust the default CIR value for ARP protocol packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend dynamic-car enable
[HUAWEI] cpu-defend dynamic-car arp enable
```

14.2.22 cpu-defend host-car

Function

The **cpu-defend host-car** command specifies the packet type to which the user-level rate limiting is applied.

By default, the user-level rate limiting can apply to ARP Request, ARP Reply, ND, DHCP Request, DHCPv6 Request, and 8021x packets, but does not apply to IGMP and HTTPS-SYN packets.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend host-car { { **arp** | **dhcp-request** | **dhcpv6-request** | **igmp** | **nd** | **8021x** | **https-syn** } * | **all** }

Parameters

Parameter	Description	Value
arp	Applies user-level rate limiting to ARP packets.	-
dhcp-request	Applies user-level rate limiting to DHCP Request packets.	-
dhcpv6-request	Applies user-level rate limiting to DHCPv6 Request packets.	-
igmp	Applies user-level rate limiting to IGMP packets.	-
nd	Applies user-level rate limiting to ND packets.	-
8021x	Applies user-level rate limiting to 8021x packets.	-
https-syn	Applies user-level rate limiting to HTTPS-SYN packets.	-

Parameter	Description	Value
all	Applies user-level rate limiting to ARP, DHCP Request, DHCPv6 Request, IGMP, ND, 8021x, and HTTPS-SYN packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch limits the rates of the ARP, ND, DHCP Request, DHCPv6 Request, and 8021x packets received from user MAC addresses, including wired and wireless users, and discards excessive packets when the packet rates exceed the rate limit. If you need to limit the rate of only IGMP and HTTPS-SYN packets or packets of the specified types, specify the packet type.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- If the command is run multiple times, the user-level rate limiting applies to the packet type specified in the last command. For example, if the command specifying ARP and DHCP Request packets is run, and then the **cpu-defend host-car arp** command is run, the user-level rate limiting applies to only ARP packets.
- After the **cpu-defend host-car all** command is run, the configuration file displays **cpu-defend host-car 8021x arp dhcp-request dhcpv6-request https-syn igmp nd**.

Example

Apply user-level rate limiting to ARP, DHCP Request, DHCPv6 Request, IGMP, and ND packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car arp dhcp-request dhcpv6-request igmp nd
```

14.2.23 cpu-defend host-car drop-packet cir

Function

The **cpu-defend host-car drop-packet cir** command sets a rate limit for sending packets that are discarded due to user-level rate limiting to the CPU.

The **undo cpu-defend host-car drop-packet cir** command restores the default rate limit.

By default, the CIR and CBS for sending packets that are discarded due to user-level rate limiting to the CPU are 64 kbit/s and 12032 bytes, respectively.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend host-car drop-packet cir *cir-value* [**cbs** *cbs-value*]

undo cpu-defend host-car drop-packet cir

Parameters

Parameter	Description	Value
cir-value	Specifies the CIR value.	The value is an integer in the range from 64 to 4096, in kbit/s.
cbs *cbs-value*	Specifies the CBS value.	The value is an integer in the range from 10000 to 800000, in bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **undo cpu-defend host-car drop-packet monitor disable** command is run to enable monitoring for packets discarded due to user-level rate limiting, the discarded packets are sent to the CPU. You can run the **cpu-defend host-car drop-packet cir** command to adjust the rate limit for sending these discarded packets to the CPU.

Prerequisites

Monitoring for packets discarded due to user-level rate limiting has been enabled using the **undo cpu-defend host-car drop-packet monitor disable** command.

Example

Set the CIR and CBS for sending packets that are discarded due to user-level rate limiting to the CPU to 128 kbit/s and 16384 bytes, respectively.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car enable
```

```
[HUAWEI] undo cpu-defend host-car drop-packet monitor disable
[HUAWEI] cpu-defend host-car drop-packet cir 128 cbs 16384
```

14.2.24 cpu-defend host-car drop-packet monitor disable

Function

The **cpu-defend host-car drop-packet monitor disable** command disables monitoring for packets discarded due to user-level rate limiting.

The **undo cpu-defend host-car drop-packet monitor disable** command enables monitoring for packets discarded due to user-level rate limiting.

By default, monitoring for packets discarded due to user-level rate limiting is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend host-car drop-packet monitor disable

undo cpu-defend host-car drop-packet monitor disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After user-level rate limiting is enabled, the switch discards the excess packets if the rate of packets from the same source MAC address exceeds the rate limit within a specified period of time. To check the information about discarded packets, you can run the **cpu-defend host-car drop-packet monitor disable** command to enable monitoring for packets discarded due to user-level rate limiting.

Prerequisites

User-level rate limiting has been enabled using the **cpu-defend host-car enable** command.

Precautions

After you run the **cpu-defend host-car drop-packet monitor disable** command to disable monitoring for packets discarded due to user-level rate limiting, the **cpu-defend host-car drop-packet cir** command configuration is deleted.

Example

Enable monitoring for packets discarded due to user-level rate limiting.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car enable
[HUAWEI] undo cpu-defend host-car drop-packet monitor disable
```

14.2.25 cpu-defend host-car enable

Function

The **cpu-defend host-car enable** command enables user-level rate limiting.

The **undo cpu-defend host-car enable** command disables user-level rate limiting.

By default, user-level rate limiting is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend host-car enable

undo cpu-defend host-car enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User-side hosts are prone to virus attacks. Infected hosts may send a large number of protocol packets to network devices, causing a high CPU usage and degraded performance on the devices and affecting services. You can configure the user-level rate limiting to resolve this problem. User-level rate limiting identifies users by user MAC addresses and limits the rates of specified packets for both wired and wireless users. By default, the threshold for each user MAC address is 10 pps.

The user-level rate limiting is more precise than CPCAR (based on switches) and port attack defense (based on interfaces) because it is user-specific and has little impact on online users.

Precautions

- After you run the **undo cpu-defend host-car enable** command to disable user-level rate limiting, all configurations related to user-level rate limiting are deleted or restored to the default values.
- You are advised to disable user-level rate limiting on network-side ports of access switches and network interconnection interfaces of gateway switches.
- During user-level rate limiting, the system performs a hash calculation for the source MAC addresses of specified packets, and places the packets into different buckets. Therefore, multiple users may share the rate limit. When the traffic volume is heavy on the network, packets may be dropped. If you confirm that these users are authorized, run the **cpu-defend host-car mac-address** *mac-address* command to increase the rate threshold for the specified MAC addresses.

Example

Disable user-level rate limiting.

```
<HUAWEI> system-view
[HUAWEI] undo cpu-defend host-car enable
```

14.2.26 cpu-defend host-car pps

Function

The **cpu-defend host-car pps** command sets the rate limit for the user-level rate limiting.

The **undo cpu-defend host-car** command restores the default rate limit for the user-level rate limiting.

By default, the rate limit for the user-level rate limiting is 10 pps.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend host-car [**mac-address** *mac-address* | **car-id** *car-id*] **pps** *pps-value*

undo cpu-defend host-car { **mac-address** *mac-address* | **car-id** *car-id* }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Sets the rate limit for the specified MAC address.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.
car-id *car-id*	Sets the rate limit for the specified bucket.	The value is an integer that ranges from 0 to 8191.
pps *pps-value*	Indicates the rate limit.	The value is an integer that ranges from 1 to 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User-level rate limiting identifies users by user MAC addresses and limits the rates of specified packets (ARP, ND, DHCP Request, DHCPv6 Request, IGMP, 802.1X, and HTTPS-SYN packets) for both wired and wireless users. By default, the user-level rate limit is 10 pps. You can set a rate limit based on user.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- If the rate limit is too high, attacks cannot be prevented and CPU may be overloaded.
- If both the **cpu-defend host-car mac-address** *mac-address* **pps** *pps-value* and **cpu-defend host-car pps** *pps-value* commands are run, the rate limit for the specified MAC address is determined by the former command, and the rate limit for other MAC addresses is determined by the latter command.
- The user-level rate limiting performs a hash calculation for the source MAC addresses of specified packets, and places the packets into different buckets. When two user MAC addresses are mapped to the same bucket index, the two users share the same rate limit (in pps mode). If the two users modify the rate limit for the bucket simultaneously, the setting will be overwritten. To avoid this situation, the rate limit for the specified MAC address cannot be set upon hash conflict.
- When the **cpu-defend host-car mac-address** *mac-address* **pps** *pps-value* and **cpu-defend host-car pps** *pps-value* commands are run to configure the rate limit for multiple MAC addresses, the settings are displayed in the alphabetic order in the configuration file.

Example

Set the rate limit for MAC address 00e0-fc0b-000c to 20 pps.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car mac-address 00e0-fc0b-000c pps 20
```

14.2.27 cpu-defend policy

Function

The **cpu-defend policy** command creates an attack defense policy and displays the attack defense policy view.

The **undo cpu-defend policy** command deletes an attack defense policy.

By default, the **default** attack defense policy exists on the device and is applied to the device. The **default** attack defense policy cannot be deleted or modified.

Format

cpu-defend policy *policy-name*

undo cpu-defend policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy.	The value is a string of 1 to 31 case-insensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of packets including malicious attack packets are sent to the CPU on a network. If excess packets are sent to the CPU, the CPU usage becomes high and CPU performance deteriorates. The attack packets affect services and may even cause system breakdown. To solve the problem, create an attack defense policy and configure CPU attack defense and attack source tracing in the attack defense policy.

Precautions

The device supports a maximum of 13 attack defense policies, including the **default** attack defense policy. The **default** attack defense policy is generated in the system by default and is applied to the device. The **default** attack defense policy cannot be deleted or modified. The other 12 policies can be created, modified, and deleted.

The configuration in a user-defined attack defense policy overrides the configuration in the **default** attack defense policy. If no parameter is set in the user-defined attack defense policy, the configuration in the **default** attack defense policy is used.

When the **default** attack defense policy is used, protocol packets sent to the CPU are limited based on the default CIR value.

Example

Create an attack defense policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test]
```

14.2.28 cpu-defend-policy

Function

The **cpu-defend-policy** command applies an attack defense policy.

The **undo cpu-defend-policy** command cancels the application of an attack defense policy.

By default, the **default** attack defense policy is applied to the switch.

Format

The stack-incapable models support the following commands:

cpu-defend-policy *policy-name* **global**

undo cpu-defend-policy { *policy-name* **global** | **global** }

Other models support the following format:

cpu-defend-policy *policy-name* [**global**]

undo cpu-defend-policy [*policy-name*] [**global**]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy. ● If the **global** keyword is specified, the attack defense policy is applied to the switching chip. ● If the **global** keyword is not specified, the attack defense policy is applied to the CPU. Only the attack defense policies that limit the rates of packets sent to the CPU can be applied to the CPU. Other types of attack defense policies are not applicable to the CPU, so configuring such policies cannot protect the CPU.	The attack defense policy must already exist.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, you must apply the policy in the system view. Otherwise, the attack defense policy does not take effect.

Prerequisites

An attack defense policy has been created by using the **cpu-defend policy** command.

Example

Apply the attack defense policy named **test** to all devices.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend-policy test global
```

14.2.29 cpu-defend trap drop-packet

Function

The **cpu-defend trap drop-packet** command enables alarm reporting for packet loss caused by CPCAR exceeding.

The **undo cpu-defend trap drop-packet** command restores the default configuration.

By default, the system does not report alarms for packet loss caused by CPCAR exceeding.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

cpu-defend trap drop-packet

undo cpu-defend trap drop-packet

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the CPU, a switch limits the rate of protocol packets sent to the CPU based on the CPCAR. If the rate of protocol packets exceeds the CPCAR, excess protocol packets are dropped. As a result, the corresponding service may not run normally. To quickly detect packet loss caused by CPCAR exceeding, you can use this command to enable alarm reporting for this event. After this function is enabled, the switch checks for packet loss caused by CPCAR at 10-minute intervals. If the switch finds that the number of dropped packets of a protocol increases, the switch reports a packet loss alarm.

Precautions

After this alarm reporting function is enabled, the switch reports packet loss alarms based on protocol types. That is, if the rates of packets of multiple protocols exceed the CPCAR values set for these protocols, the switch reports an alarm for each protocol.

Example

Enable alarm reporting for packet loss caused by CPCAR exceeding.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend trap drop-packet
```

14.2.30 deny

Function

The **deny** command configures the device to discard packets sent to the CPU.

The **undo deny** command restores the default action taken for the packets sent to the CPU.

By default, the device does not discard packets sent to the CPU. Instead, the device limits the rate of packets sent to the CPU and user-defined flows using the default rate. You can check the CAR values of each type of packets using the **display cpu-defend configuration** command.

Format

deny { **packet-type** *packet-type* | **user-defined-flow** *flow-id* }

undo deny { **packet-type** *packet-type* | **user-defined-flow** *flow-id* }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the type of the packet to be discarded.	The supported packet type depends on the device.
user-defined-flow *flow-id*	Specifies the ID of the user-defined flow to be discarded. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter.	The value is an integer that ranges from 1 to 8.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, if the device receives attack packets of a specified type or a large number of packets sent to the CPU, run the **deny** command to configure the device to discard packets of the specified type sent to the CPU.

Precautions

If you run the **deny** command, and then the **car** command, the **car** command takes effect; if you run the **car** command, and then the **deny** command, the **deny** command takes effect. After the **undo deny** command is executed, the default action for packets sent to the CPU is restored, that is, CIR and CBS actions are performed.

To configure the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S, switch to discard BPDU, CDP, LNP, and VCMP packets, run the **deny packet-type bpdu-tunnel** command.

Example

Configure the drop action taken for ARP Reply packets to be sent to the CPU in the attack defense policy **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] deny packet-type arp-reply
```

14.2.31 description (attack defense policy view)

Function

The **description** command configures the description of an attack defense policy.

The **undo description** command deletes the description of an attack defense policy.

By default, no description is configured for an attack defense policy.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the content of a description.	It is a string of 1 to 63 case-sensitive characters with spaces.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an attack defense policy, for example, the usage or application scenario of the attack defense policy. The description is used to differentiate attack defense policies.

Precautions

If you run the **description** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

Example

Configure the description **defend_arp_attack** for the attack defense policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] description defend_arp_attack
```

14.2.32 display auto-defend attack-source

Function

The **display auto-defend attack-source** command displays the attack sources.

Format

display auto-defend attack-source [**history** [**begin** *begin-date begin-time*] [**slot** *slot-id*] | [**slot** *slot-id*] [**detail**]]

Parameters

Parameter	Description	Value
history	Displays the history attack source information. If **history** is not specified, all existing attack source information is displayed.	-
begin *begin-date begin-time*	Specifies the start time.	*begin-date* is in the format YYYY/MM/DD. *begin-time* is in the format HH:MM:SS. The value of YYYY/MM/DD ranges from 2000/1/1 to 2099/12/31. The value of HH:MM:SS ranges from 00:00:00 to 23:59:59.

Parameter	Description	Value
slot *slot-id*	- This parameter specifies the slot ID if stacking is not configured. - This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.
detail	Displays detailed information about the attack sources, including the type of attack packets. If **detail** is not specified, brief information about the attack sources is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display auto-defend attack-source** command displays the attack sources.

In a stack, the attack source list can be saved on each member switch. The **display auto-defend attack-source slot** *slot-id* command displays the attack source list on the specified member switch.

Example

Display the attack source list.

```
<HUAWEI> display auto-defend attack-source
 Attack Source User Table (slot 0):
 -------------------------------------------------------------------------------
 MacAddress       InterfaceName              Vlan:Outer/Inner    TotalPackets
 -------------------------------------------------------------------------------
 xxxx-xxxx-xxxx   GigabitEthernet0/0/1        100                1395
 -------------------------------------------------------------------------------
 Total: 1

 Attack Source Port Table (slot 0):
 ------------------------------------------------------------
 InterfaceName              Vlan:Outer/Inner    TotalPackets
 ------------------------------------------------------------
 GigabitEthernet0/0/1        100                605
 ------------------------------------------------------------
```

```
 Total: 1

 Attack Source IP Table (slot 0):
 ----------------------------------------------------------------------
 IPAddress                                TotalPackets
 ----------------------------------------------------------------------
 2001:db8:1::1                             1395
 ----------------------------------------------------------------------
 Total: 1
```

Display detailed information about the attack source list.

```
<HUAWEI> display auto-defend attack-source detail
 Attack Source User Table (slot 0):
 ----------------------------------------------------
 MAC Address                 xxxx-xxxx-xxxx
 Interface                 GigabitEthernet0/0/1
 VLAN: Outer/Inner             100
    ARP:                   1580
 Total                     1580
 ----------------------------------------------------
 Total: 1

 Attack Source Port Table (slot 0):
 ----------------------------------------------------
 Interface                 GigabitEthernet0/0/1
 VLAN: Outer/Inner             100
    ARP:                   790
 Total                     790
 ----------------------------------------------------
 Total: 1

 Attack Source IP Table (slot 0):
 -------------------------------------------------------------------------
 IP address                 2001:db8:1::1
    ARP:                   1580
 Total                     1580
  -------------------------------------------------------------------------
 Total: 1
```

Table 14-21 Description of the **display auto-defend attack-source** command output

Item	Description
Attack Source User Table (slot 0)	Source tracing information of device, which is distinguished according to the attack user.
Attack Source Port Table (slot 0)	Source tracing information of device, which is distinguished according to the attacked interface. **NOTE** The device does not support attack source tracing based on source interfaces and VLANs for Layer 3 Ethernet interfaces. Therefore, this field does not contain the attack source tracing information of Layer 3 Ethernet interfaces.
Attack Source IP Table (slot 0)	Source tracing information of device, which is distinguished according to the attacked interface.
IPAddress	User IP address.
MacAddress	MAC address of the user.
InterfaceName	Name of the interface that initiates the attack.

Item	Description
Interface	Name of the interface that initiates the attack.
Vlan:Outer/Inner	ID of the VLAN that an interface belongs to. **Outer** indicates the outer VLAN ID and **Inner** indicates the inner VLAN ID. **NOTE** This field displays - for the attack source tracing entries of Layer 3 Ethernet interfaces.
TotalPackets	Total number of packets received by the device.

Display history attack source information.

```
<HUAWEI> display auto-defend attack-source history

 S : start time
 E : end time

 Attack History User Table (slot 0):
 -------------------------------------------------------------------------------
 AttackTime          MacAddress     IFName        Vlan:O/I  Protocol    PPS
 -------------------------------------------------------------------------------
 S:2016-09-08 07:36:15 xxxx-xxxx-xxxx GE0/0/1        100      ARP         40
 E:-
 -------------------------------------------------------------------------------
 Total: 1

 Attack History Port Table (slot 0):
 ---------------------------------------------------------------
 AttackTime          IFName        Vlan:O/I  Protocol    PPS
 ---------------------------------------------------------------
 S:2016-09-08 07:36:37 GE0/0/1        100      ARP         40
 E:-
 ---------------------------------------------------------------
 Total: 1

 Attack History IP Table (slot 0):
 ---------------------------------------------------------------------------
 AttackTime          IPAddress                              Protocol
 PPS
 ---------------------------------------------------------------------------
 S:2016-09-08 07:36:15 2001:db8:1::1                          ARP
 E:-
 40
 ---------------------------------------------------------------------------
 Total: 1
```

Table 14-22 Description of the display auto-defend attack-source history command output

Item	Description
Attack History User Table (slot 0)	Information about attack sources on the device, which is distinguished according to attackers.
Attack History Port Table (slot 0)	Information about attack sources on the device, which is distinguished according to attacked interfaces.

Item	Description
Attack History IP Table (slot 0)	Information about attack sources on the device, which is distinguished according to attacked source IP addresses.
AttackTime	Attack time. ● S indicates start time. ● E indicates end time. If the attack is not ended when you display history attack source information, this field displays -.
MacAddress	User MAC address.
IPAddress	User IP address.
IFName	Name of the interface that initiates the attack.
Vlan:O/I	ID of the VLAN that an interface belongs to. The value O indicates the outer VLAN ID and the value I indicates the inner VLAN ID.
Protocol	Attack type.
PPS	Highest rate of attack packets.

14.2.33 display auto-defend configuration

Function

The **display auto-defend configuration** command displays the attack source tracing configuration.

Format

display auto-defend configuration [**cpu-defend policy** *policy-name*]

Parameters

Parameter	Description	Value
cpu-defend policy *policy-name*	Displays the attack source tracing configuration of a specified attack defense policy. ● If this parameter is specified, the configuration of the specified attack defense policy is displayed. ● If this parameter is not specified, the configurations of all attack defense policies are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After attack source tracing is configured in an attack defense policy, you can run the **display auto-defend configuration** command to view the attack source tracing configuration.

Example

Display the attack source tracing configuration.

```
<HUAWEI> display auto-defend configuration
 -------------------------------------------------------------------------
 Name  : test
 Related slot : <0>
 auto-defend                      : enable
 auto-defend attack-packet sample : 5
 auto-defend threshold            : 60 (pps)
 auto-defend alarm                : enable
 auto-defend trace-type           : source-mac source-ip
 auto-defend protocol             : arp icmp dhcp igmp tcp telnet 8021x nd dhcpv6 mld icmpv6 tcpv6
 auto-defend action               : deny (Expired time : 300 s)
 auto-defend whitelist 1          : acl number 2002
 -------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed information depends on the actual situation.

Table 14-23 Description of the **display auto-defend configuration** command output

Item	Description
Name	Name of an attack defense policy.
Related slot	ID of the stack to which the attack defense policy is applied.
auto-defend	Whether attack source tracing is enabled. To enable attack source tracing, run the **auto-defend enable** command.
auto-defend attack-packet sample	Packet sampling ratio for attack source tracing. To set the packet sampling ratio for attack source tracing, run the **auto-defend attack-packet sample** command.
auto-defend threshold	Checking threshold for attack source tracing. To set the checking threshold for attack source tracing, run the **auto-defend threshold** command.
auto-defend alarm	Whether the alarm function for attack source tracing is enabled. To enable the alarm function for attack source tracing, run the **auto-defend alarm enable** command.
auto-defend trace-type	Attack source tracing mode: ● source-mac: indicates attack source tracing based on source MAC addresses. ● source-ip: indicates attack source tracing based on source IP addresses. ● source-portvlan: indicates attack source tracing based on source ports+VLANs. To configure the attack source tracing mode, run the **auto-defend trace-type** command.
auto-defend protocol	Type of traced packets. To specify the types of protocol packets that the device monitors in attack source tracing, run the **auto-defend protocol** command.
auto-defend action	Action taken on the attack source. The value can be: ● deny (Expired time: 300s): indicates that the device discards all attack packets in 300s. ● error-down: indicates that the inbound interfaces of attack packets are shut down. To configure the **punish** action, run the **auto-defend action** command.

Item	Description
auto-defend whitelist 1	Whitelist for attack source tracing. For related commands, see **auto-defend whitelist**.

14.2.34 display auto-defend whitelist

Function

The **display auto-defend whitelist** command displays information about the attack source tracing whitelist.

Format

display auto-defend whitelist [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- On a standalone switch without the stacking function configured, this parameter specifies a slot ID. - In a stack system, this parameter specifies a stack ID.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the whitelist for attack source tracing is configured or when you locate faults on network, run the **display auto-defend whitelist** command to verify whitelist information. If no whitelist is configured, the command displays no whitelist information.

Example

Display information about the attack source tracing whitelist on the switch.

```
<HUAWEI> display auto-defend whitelist
 Protocol       Interface               IP              ACL      Status
-------------------------------------------------------------------------------
    DHCP         GE0/0/1                --               --       auto
    DHCP         GE0/0/2                --               --       auto
```

Table 14-24 Description of the **display auto-defend whitelist** command output

Item	Description
Protocol	Protocol type of the packets excluded from attack source tracing.
Interface	Interface on which inbound packets are excluded from attack source tracing.
IP	Source IP address of the packets excluded from attack source tracing. If not source IP address is specified in the whitelist rule, this field displays --.
ACL	ACL number specified in a manually configured whitelist rule. If the whitelist rule is automatically delivered, this field displays --.
Status	Type of the whitelist rule, which can be: ● **auto**: An automatically delivered whitelist rule is triggered by services. ● **manual**: You can run the **auto-defend whitelist** *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* } command in the attack defense policy view to manually configure an attack source tracing whitelist.

14.2.35 display auto-port-defend attack-source

Function

The **display auto-port-defend attack-source** command displays source tracing information on interfaces.

Format

display auto-port-defend attack-source [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- The value indicates the slot ID if stacking is not configured. - The value indicates the stack ID when stack is configured. If **slot** *slot-id* is not specified, the source tracing information on the interfaces of the master device (stack configured) or local device (stack not configured) is displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The source tracing information helps you locate attack sources.

Example

Display the source tracing information on the interfaces of the device.

```
<HUAWEI> display auto-port-defend attack-source
Attack source table on slot 0:
Total : 1
-------------------------------------------------------------------------------
Interface     VLAN Protocol     Expire(s)   PacketRate(pps)
LastAttackTime
-------------------------------------------------------------------------------
GE0/0/1     NA   arp-request  297        12             2013-07-06 17:36:54
-------------------------------------------------------------------------------
```

Table 14-25 Description of the **display auto-port-defend attack-source** command output

Item	Description
Attack source table on slot 0	Source tracing information on the interfaces of device.

Item	Description
Total	Number of source tracing records.
Interface	Name of the attacked interface.
VLAN	VLAN ID in attack packets. If the device does not support checking on VLAN IDs in attack packets, this field displays NA.
Protocol	Attack packet type.
Expire(s)	Remaining time of the aging time for port attack defense. **NOTE** If the **Expire(s)** field of an entry displays 0, this entry will be deleted after a certain period (a maximum of 10 seconds).
PacketRate(pps)	Rate of the last received attack packet.
LastAttackTime	Time when the last attack packet is received.

14.2.36 display auto-port-defend configuration

Function

The **display auto-port-defend configuration** command displays the configuration of port attack defense.

Format

display auto-port-defend configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the configuration of port attack defense, use this command.

Example

Display the configuration of port attack defense on the local device.

```
<HUAWEI> display auto-port-defend configuration
-------------------------------------------------------------------------------
 Name  : test
 Related slot : <0>
 Auto-port-defend                          : enable
 Auto-port-defend sample                   : 5
 Auto-port-defend aging-time               : 300 second(s)
 Auto-port-defend arp-request threshold    : 120 pps(enable)
 Auto-port-defend arp-request-uc threshold : 120 pps(enable)
 Auto-port-defend arp-reply threshold      : 120 pps(enable)
 Auto-port-defend dhcp threshold           : 120 pps(enable)
 Auto-port-defend icmp threshold           : 120 pps(enable)
 Auto-port-defend igmp threshold           : 120 pps(enable)
 Auto-port-defend ip-fragment threshold    : 30 pps(enable)
 Auto-port-defend nd threshold             : 120 pps(enable)
 Auto-port-defend alarm                    : disable
-------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed information depends on the actual situation.

Table 14-26 Description of the display auto-port-defend configuration command output

Item	Description
Name	Name of an attack defense policy.
Related slot	ID of the stack to which the attack defense policy is applied. In a non-stack environment, this field indicates that the attack defense policy is applied to the local device.
Auto-port-defend	Whether port attack defense is enabled. To enable the port attack defense function, run the **auto-port-defend enable** command.
Auto-port-defend sample	Sampling ratio for protocol packets. To set this parameter, run the **auto-port-defend sample** command.
Auto-port-defend aging-time	Aging time for port attack defense. To set this parameter, run the **auto-port-defend aging-time** command.
Auto-port-defend arp-request threshold	Whether port attack defense is applied to ARP Request packets and rate threshold. To set this parameter, run the **auto-port-defend protocol arp-request** and **auto-port-defend protocol arp-request threshold** *threshold* commands.

Item	Description
Auto-port-defend arp-request-uc threshold	Whether port attack defense is applied to Unicast ARP Request packets and rate threshold. To set this parameter, run the **auto-port-defend protocol arp-request-uc** and **auto-port-defend protocol arp-request-uc threshold** *threshold* commands.
Auto-port-defend arp-reply threshold	Whether port attack defense is applied to ARP Reply packets and rate threshold. To set this parameter, run the **auto-port-defend protocol arp-reply** and **auto-port-defend protocol arp-reply threshold** *threshold* commands.
Auto-port-defend dhcp threshold	Whether port attack defense is applied to DHCP packets and rate threshold. To set this parameter, run the **auto-port-defend protocol dhcp** and **auto-port-defend protocol dhcp threshold** *threshold* commands.
Auto-port-defend icmp threshold	Whether port attack defense is applied to ICMP packets and rate threshold. To set this parameter, run the **auto-port-defend protocol icmp** and **auto-port-defend protocol icmp threshold** *threshold* commands.
Auto-port-defend igmp threshold	Whether port attack defense is applied to IGMP packets and rate threshold. To set this parameter, run the **auto-port-defend protocol igmp** and **auto-port-defend protocol igmp threshold** *threshold* commands.
Auto-port-defend ip-fragment threshold	Whether port attack defense is applied to IP fragments and rate threshold. To set this parameter, run the **auto-port-defend protocol ip-fragment** and **auto-port-defend protocol ip-fragment threshold** *threshold* commands.
Auto-port-defend nd threshold	Whether port attack defense is applied to ND packets and rate threshold. To set this parameter, run the **auto-port-defend protocol nd** and **auto-port-defend protocol nd threshold** *threshold* commands.
Auto-port-defend alarm	Whether the report of port attack defense events is enabled. To set this parameter, run the **auto-port-defend alarm enable** command.

14.2.37 display auto-port-defend statistics

Function

The **display auto-port-defend statistics** command displays packet statistics about port attack defense.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display auto-port-defend statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	● The value indicates the slot ID when stacking is not configured. ● The value indicates the stack ID when stacking is configured. If **slot** *slot-id* is not specified, packet statistics on the master device (stack configured) or local device (stack not configured) are displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view statistics about the packets discarded and accepted in the port attack defense service. The statistics help you understand protocol packet processing status and promptly adjust the attack defense policy.

Example

Display packet statistics on the interfaces of the device.

```
<HUAWEI> display auto-port-defend statistics
Statistics on MPU:
-------------------------------------------------------------------------------
Protocol     Vlan Queue Cir(Kbps)  Pass(Packet/Byte)  Drop(Packet/
Byte)
-------------------------------------------------------------------------------
icmp         NA   2     256        23095              3
                           NA                NA
-------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 14-27 Description of the **display auto-port-defend statistics** command output

Item	Description
Statistics on MPU	Packet statistics on the interfaces of the device.
Protocol	Attack packet type.
Vlan	VLAN ID in attack packets. If the device does not support checking VLAN IDs in attack packets, this field displays **NA**.
Queue	Queue from which attack packets are sent.
Cir(Kbps)	Protocol rate limit. (When **slot** is not specified, the default CPCAR value is displayed if the manually configured CPCAR value is smaller than the default CPCAR value; the manually configured CPCAR value is displayed if the manually configured CPCAR value is greater than the default CPCAR value. When **slot** is specified, the default CPCAR value is displayed. However, the rate limit of protocol packets except DHCP packets cannot exceed 256 kbit/s when **slot** is specified.) To configure a CIR value, run the **car packet-type** *packet-type* **cir** *cir-value* command in the attack defense policy view.

Item	Description
Pass(Packet/Byte)	Number and bytes of attack packets that pass through the device. The value **23095** indicates the number of accepted packets. The value **NA** indicates that the device does not support statistics collection by byte.
Drop(Packet/Byte)	Number and bytes of attack packets discarded by the device. The value **3** indicates the number of discarded packets. The value **NA** indicates that the device does not support statistics collection by byte.

14.2.38 display auto-port-defend whitelist

Function

The **display auto-port-defend whitelist** command displays information about the interface attack defense whitelist.

Format

display auto-port-defend whitelist [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	• Specifies a slot ID if stacking is not configured. • Specifies a stack ID in a stack.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the whitelist for port attack defense is configured or when you locate faults on network, run the **display auto-port-defend whitelist** command to verify whitelist information. If no whitelist is configured, the command displays no whitelist information.

Example

Display information about the interface attack defense whitelist.

```
<HUAWEI> display auto-port-defend whitelist
 Protocol      Interface              IP                ACL      Status
--------------------------------------------------------------------------------
   --          Eth-Trunk0            --                --       auto
   --          GE0/0/1               --                --      manual
   --             --               --              2000     manual
```

Table 14-28 Description of the **display auto-port-defend whitelist** command output

Item	Description
Protocol	Protocol type of packets free from the interface attack defense action. If no packet protocol type is specified in the whitelist rule, this field displays --.
Interface	Interface free from the attack defense action. If the whitelist is configured based on ACL rules, this field displays --.
IP	Source IP address of packets free from the interface attack defense action. If the whitelist is configured based on interfaces or automatically delivered, this field displays --.
ACL	ACL number specified in a manually configured whitelist rule.
Status	Type of the whitelist rule, which can be: ● **auto**: An automatically delivered whitelist rule is triggered by services. ● **manual**: You can run the **auto-port-defend whitelist** *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* } command in the attack defense policy view to configure a whitelist for port attack defense.

14.2.39 display cpu-defend applied

Function

The **display cpu-defend applied** command displays the actual CAR values for the protocol packets delivered to the chip.

Format

display cpu-defend applied [**packet-type** *packet-type*] { **mcu** | **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
mcu	Indicates the main control board. **NOTE** Only the stack-capable models support the **mcu** parameter.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if a stack is configured.	The value must be set according to the device configuration.
all	Indicates all switches in a stack if stacking is enabled, or the switch itself if stacking is disabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The actual CAR values may be different from the configured CAR values. The possible causes are as follows:

- The CIR value specified in the **car packet-type** *packet-type* **cir** *cir-value* [**cbs** *cbs-value*] command is a consecutive range. However, the actual CIR value is discrete, depending on chip granularity. For example, if the CIR value range is set to 65 to 128 with the granularity 64 kbit/s, the actual CIR value may be 64 or 128, which depends on product models.

- The configured CIR value exceeds the chip capacity and the upper threshold. For example, the CIR value is set to 10000, but the chip does not support CIR value 10000. Then the actual CIR value cannot reach 10000.

You can run the **display cpu-defend applied** command to view the actual CAR values for protocol packets.

NOTE

When too much output information is to be displayed, specify the **begin**, **exclude**, or **include** parameter to display only the required information.

Example

Display the actual CAR values for ARP Request messages sent from the switch.

```
<HUAWEI> display cpu-defend applied packet-type arp-request slot 0
Applied Car on slot 0:
-------------------------------------------------------------------------------
Packet Type        Cir(Kbps)    Cbs(Byte) Applied Cir(Kbps) Applied Cbs(Byte)
-------------------------------------------------------------------------------
arp-request              65       10000              128            10000
-------------------------------------------------------------------------------
```

Table 14-29 Description of the **display cpu-defend applied** command output

Item	Description
Applied Car on slot 0	CAR value for protocol packets sent by a specified stack.
Packet Type	Packet type.
Cir(Kbps)	Configured committed information rate (CIR), in kbit/s. To set the CIR value, run the **car** and **linkup-car** commands.
Cbs(Byte)	Configured committed burst size (CBS) value, in bytes. To set the CBS value, run the **car** and **linkup-car** commands.
Applied Cir(Kbps)	Actual CIR value on the chip, in kbit/s.
Applied Cbs(Byte)	Actual CBS value on the chip, in bytes.

14.2.40 display cpu-defend configuration

Function

The **display cpu-defend configuration** command displays CAR configurations.

Format

The stack-incapable models support the following commands:

display cpu-defend configuration [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

Other models support the following format:

display cpu-defend configuration [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **mcu** }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device. **NOTE** The CAR configuration information about packet type IPv6 FTP is displayed when the packet type **ftp** is specified in the command.
all	Indicates all devices.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.
mcu	Indicates the main control board.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cpu-defend configuration** command to view the rate limit of protocol packets sent to the CPU. By default, the rate limit of protocol packets in the **default** policy is displayed.

In a stack, you can run the **cpu-defend-policy global** command to bind all switches to the same attack defense policy. Then you can run the **display cpu-defend configuration all** command to view the same CAR configuration of all switches in the stack.

Example

Display the CAR configurations.

```
<HUAWEI> display cpu-defend configuration all
Car configurations on mainboard.
----------------------------------------------------------------------
Packet Name         Status     Cir(Kbps)   Cbs(Byte)
----------------------------------------------------------------------
arp-miss            Enabled         64       12032
arp-reply           Enabled        256       48128
arp-request         Enabled        256       48128
bgp                 Enabled        384       72192
bgp-keepalive       Enabled        128       24064
bgp4plus            Enabled        256       48128
dhcpv6-reply        Enabled        256       48128
dhcpv6-request      Enabled        256       48128
dns                 Enabled         64       12032
fib-hit             Enabled         64       12032
fib-miss            Enabled         64       12032
ftp                 Enabled        512       96256
hop-limit           Enabled         64       12032
http                Enabled        512       96256
https               Enabled        512       96256
hw-tacacs           Enabled        128       24064
icmp                Enabled        128       24064
icmpv6              Enabled         64       12032
igmp                Enabled        256       48128
ip-cloud            Enabled        128       24064
isis                Enabled        256       48128
mdns-relay          Enabled        256       48128
mld                 Enabled        256       48128
mpls-fib-hit        Enabled        256       48128
mpls-ldp            Enabled        512       96256
mpls-one-label      Enabled        128       24064
mpls-ping           Enabled        128       24064
mpls-rsvp           Enabled        128       24064
mpls-ttl-expired    Enabled        128       24064
mpls-vccv-ping      Enabled        128       24064
nac-arp-reply       Enabled        128       24064
nac-arp-request     Enabled        128       24064
nac-nd              Enabled         64       12032
nd                  Enabled        128       24064
ntp                 Enabled        128       24064
ospf                Enabled        384       72192
ospfv3              Enabled        384       72192
pim                 Enabled        256       48128
pimv6               Enabled        128       24064
portal              Enabled        128       24064
radius              Enabled        128       24064
rip                 Enabled        256       48128
ripng               Enabled        256       48128
snmp                Enabled        128       24064
ssh                 Enabled        128       24064
tcp                 Enabled         64       12032
telnet              Enabled        128       24064
ttl-expired         Enabled         64       12032
vrrp                Enabled        128       24064
vrrp6               Enabled        128       24064
----------------------------------------------------------------------

Linkup Information:
--------------------------------------------------------------------------------
Packet Name : ftp
Cir(Kbps)/Cbs(Byte) : 4096/770048
SIP(SMAC) : 10.1.2.1
DIP(DMAC) : 10.1.3.1
Port(S/C) : 42372/22
--------------------------------------------------------------------------------
Car configurations on slot 0.
```

```
----------------------------------------------------------------------
Packet Name         Status     Cir(Kbps)   Cbs(Byte)   Queue  Port-Type
----------------------------------------------------------------------
8021x              Disabled        128       24064      3         NA
arp-mff            Disabled         64       12032      3         NA
arp-miss           Enabled          64       12032      3         NA
arp-reply          Enabled         128       24064      3        UNI
arp-request        Enabled         128       24064      3        UNI
bfd                Disabled         64       12032      5        NNI
bgp                Enabled         256       48128      5         NA
bgp-keepalive      Enabled         128       24064      5         NA
bgp4plus           Enabled         128       24064      5         NA
bpdu-tunnel        Disabled         64       12032      5         NA
cdp                Disabled        128       24064      5         NA
dhcp-client        Enabled         512       96256      3        NNI
dhcp-server        Enabled         512       96256      3        UNI
dhcpv6-reply       Enabled         256       48128      3        NNI
dhcpv6-request     Enabled         256       48128      3        UNI
dldp               Disabled        128       24064      5         NA
dns                Enabled          64       12032      5         NA
easy-operation     Disabled        128       24064      3         NA
eoam-1ag           Disabled        256       48128      5         NA
eoam-1ag-lblt      Disabled        128       24064      5         NA
eoam-3ah           Disabled         64       12032      5         NA
erps-port          Disabled         64       12032      5         NA
fib-hit            Enabled          64       12032      3         NA
fib-miss           Disabled         64       12032      3        UNI
ftp                Enabled          64       12032      3         NA
gre-keepalive      Enabled          64       12032      5         NA
gvrp               Disabled        128       24064      5         NA
hop-limit          Enabled          64       12032      2        NNI
http               Enabled          64       12032      3         NA
https              Enabled          64       12032      3         NA
hw-tacacs          Enabled          64       12032      3        NNI
icmp               Enabled         128       24064      3        UNI
icmp-ttl-expired   Disabled          0           0      3        UNI
icmpv6             Enabled          64       12032      3        NNI
igmp               Enabled         128       24064      3         NA
ip-cloud           Disabled         64       12032      3         NA
ipsec-ah           Disabled        256       48128      5         NA
ipsec-esp          Disabled        256       48128      5         NA
isis               Disabled        256       48128      5        NNI
lacp               Disabled        128       24064      7         NA
ldt                Enabled          64       12032      5         NA
lldp               Disabled        128       24064      5         NA
lnp                Enabled         128       24064      5         NA
loopbacktest       Disabled         64       12032      5         NA
mad                Disabled        128       24064      5         NA
mdns-relay         Disabled        256       48128      5         NA
mld                Disabled        128       24064      3        NNI
mpls-fib-hit       Enabled         128       24064      5         NA
mpls-ldp           Enabled         256       48128      5         NA
mpls-one-label     Enabled         128       24064      3         NA
mpls-ping          Enabled          64       12032      5         NA
mpls-rsvp          Enabled         128       24064      5         NA
mpls-ttl-expired   Enabled         128       24064      5         NA
mpls-vccv-ping     Disabled        128       24064      3         NA
nac-arp-reply      Disabled         64       12032      3         NA
nac-arp-request    Disabled         64       12032      3         NA
nac-dhcp           Disabled        256       48128      3         NA
nac-dhcpv6         Disabled        256       48128      3         NA
nac-nd             Disabled         64       12032      3         NA
nd                 Enabled          64       12032      5        UNI
ntdp               Enabled         128       24064      5         NA
ntp                Enabled          64       12032      5        NNI
ospf               Disabled        256       48128      5        NNI
ospf-hello         Disabled        256       48128      5        NNI
ospfv3             Disabled        256       48128      5        NNI
pim                Enabled         128       24064      5        NNI
```

```
pimv6            Disabled        64      12032      5        NNI
portal           Enabled         64      12032      3        NNI
pppoe            Disabled        128      24064      3        NA
radius           Enabled         64      12032      3        NNI
rip              Disabled        128      24064      5        NNI
ripng            Disabled        256      48128      5        NNI
rrpp             Disabled        64      12032      5        NA
sep-global       Disabled        128      24064      5        NA
sep-port         Disabled        128      24064      5        NA
smart-link       Disabled        64      12032      5        NA
snmp             Enabled         128      24064      3        NNI
ssh              Enabled         64      12032      5        NNI
stp              Disabled        64      12032      5        NA
tcp              Enabled         64      12032      3        NA
telnet           Enabled         64      12032      5        NA
ttl-expired      Enabled         64      12032      2        NA
udp-helper       Disabled        64      12032      3        NA
vbst             Disabled        64      12032      5        NA
vbst-trunk       Disabled        64      12032      5        NA
vcmp             Enabled         128      24064      3        NA
vpls-igmp        Disabled        64      12032      3        NA
vrrp             Disabled        64      12032      5        NA
vrrp6            Disabled        64      12032      5        NA
y1731            Disabled        256      48128      5        NA
----------------------------------------------------------------------

Linkup Information:
-------------------------------------------------------------------------------
Packet Name : ftp
Cir(Kbps)/Cbs(Byte) : 4096/770048
SIP(SMAC) : 10.1.2.1
DIP(DMAC) : 10.1.3.1
Port(S/C) : 42372/22
-------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 14-30 Description of the **display cpu-defend configuration** command output

Item	Description
Car configurations on slot 0	CAR configuration of a stack with a specified ID.
Car configurations on mainboard	CAR configurations on the device.
Packet Name	Packet type.
Status	Protocol packet status: - Enabled - Disabled
Cir(Kbps)	Committed Information Rate (CIR), in kbit/s. To set the CIR value, run the **car** and **linkup-car** commands.

Item	Description
Cbs(Byte)	Committed burst size (CBS), in bytes. To configure the CBS value, run the **car** and **linkup-car** commands.
Queue	Queue that protocol packets are sent to.
Port-Type	Port type. The value can be UNI, NNI, or ENI. To configure the port type, run the **port type** and **port-type** commands.
Linkup Information	Information about the protocol connection. **NOTE** This information is displayed only when association of protocols is triggered. For the S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S, the linkup information about packet type **http** is displayed when the packet type **fib-hit** is specified in the command.
SIP(SMAC)	Source IP address or source MAC address.
DIP(DMAC)	Destination IP address or destination MAC address.
Port(S/C)	Source/Destination port number.

14.2.41 display cpu-defend dynamic-adjust history-record

Function

The **display cpu-defend dynamic-adjust history-record** command displays historical adaptive CPCAR adjustment records of protocol packets.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this function.

Format

display cpu-defend dynamic-adjust history-record [**packet-type** { **arp-reply** | **arp-request** | **arp-request-uc** | **dhcp-client** | **dhcp-server** | **igmp** | **nd** | **pim** }] { **all** | **mcu** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
packet-type	Specifies the type of protocol packets. **NOTE** If this parameter is not specified, the historical adaptive CPCAR adjustment records of all supported types of protocol packets are displayed.	-
arp-reply	Specifies ARP reply packets.	-
arp-request	Specifies ARP request packets.	-
arp-request-uc	Specifies unicast ARP request packets.	-
dhcp-client	Specifies the packets sent by DHCP clients.	-
dhcp-server	Specifies the packets sent by DHCP servers.	-
igmp	Specifies IGMP packets.	-
nd	Specifies IPv6 ND packets.	-
pim	Specifies PIM protocol packets.	-
all	Specifies all devices in a stack if a stack is established or the local device if no stack is established.	-
mcu	Specifies the main control board.	-
slot *slot-id*	● Specifies a slot ID if stacking is not configured. ● Specifies a stack ID if stacking is configured.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After adaptive CPCAR adjustment for protocol packets is enabled, you can run this command to view the historical adaptive CPCAR adjustment records of protocol packets. The information includes the adjustment time, CPCAR adjustments, and reason for the adjustments.

You can use this command to check a maximum of 100 latest historical records.

Example

Display historical adaptive CPCAR adjustment records of protocol packets.

```
<HUAWEI> display cpu-defend dynamic-adjust history-record all
Dynamic-adjust history-record on mainboard:
-----------------------------------------------------------------------------------------

Adjustment time     Packet type     Default/Previous/Current(kbps) Reason
2019-04-22 11:00:41 arp-request-uc  384/672/720                CPCAR drop
packet
2019-04-22 10:59:41 arp-request-uc  384/624/672                CPCAR drop
packet
2019-04-22 10:58:41 arp-request-uc  384/576/624                CPCAR drop
packet
2019-04-22 10:57:41 arp-request-uc  384/528/576                CPCAR drop
packet
2019-04-22 10:56:41 arp-request-uc  384/480/528                CPCAR drop
packet
2019-04-22 10:55:41 arp-request-uc  384/432/480                CPCAR drop
packet
2019-04-22 10:54:41 arp-request-uc  384/384/432                CPCAR drop
packet
-----------------------------------------------------------------------------------------

Dynamic-adjust history-record on slot 0
-----------------------------------------------------------------------------------------

Adjustment time     Packet type     Default/Previous/Current(kbps) Reason
-----------------------------------------------------------------------------------------
```

Table 14-31 Description of the **display cpu-defend dynamic-adjust history-record** command output

Item	Description
Dynamic-adjust history-record on mainboard	Historical adaptive CPCAR adjustment records of protocol packets on the main control board.
Adjustment time	Time when the CPCAR value was adjusted.
Packet type	Type of protocol packets.

Item	Description
Default/Previous/ Current(kbps)	- **Default**: default CPCAR value (in kbit/s) - **Previous**: CPCAR value after the last adjustment (in kbit/s) - **Current**: current CPCAR value (in kbit/s)
Reason	Reason for the adjustment: - **CPCAR drop packet**: Packet loss occurred due to CPCAR exceeding. - **CPU queue drop packet**: Packet loss occurred in the CPU queue. - **CPU overload**: The CPU was overloaded. - **Set default**: CPCAR was restored to the default value.
Dynamic-adjust history-record on slot 0	Historical adaptive CPCAR adjustment records of protocol packets in a slot.

14.2.42 display cpu-defend dynamic-car history-record

Function

The **display cpu-defend dynamic-car history-record** command displays historical records on dynamic adjustment of the default CIR value of protocol packets.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display cpu-defend dynamic-car history-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the default CIR value is set, you can run this command to view the historical records of adjusting the CPCAR value of protocol packets from 64 kbit/s to a specific value.

The granularity of each adjustment is 64 kbit/s on the switch. If the default CPCAR value is greater than 64 kbit/s, the adjustments from 64 kbit/s to the default CPCAR value are only recorded but do not take effect.

You can use this command to check a maximum of 100 latest historical records.

Example

Display the historical records on dynamic adjustment of the default CIR value of protocol packets.

```
<HUAWEI> display cpu-defend dynamic-car history-record
 Global status : Enable
 -------------------------------------------------------------------------------
 Time                Protocol    Packet-type     Slot  CIR(Kbps)   Status
 -------------------------------------------------------------------------------
 2012-08-24 11:28:10  arp        arp-reply       0     128         Success
 2012-08-24 11:28:08  arp        arp-request     0     128         Success
 2012-08-24 11:27:37  arp        arp-reply       0     64          Success
 2012-08-24 11:27:37  arp        arp-request     0     64          Success
-------------------------------------------------------------------------------
```

Table 14-32 Description of the display cpu-defend dynamic-car history-record command output

Item	Description
Global status	The device is enabled to dynamically adjust the default CIR value of protocol packets. To enable the device to dynamically adjust the default CIR value of protocol packets, run the **cpu-defend dynamic-car enable** command.
Time	Timestamps of the default CIR value of protocol packets that is dynamically adjusted.
Protocol	Protocol name. To configure a protocol, run the **cpu-defend dynamic-car** [**arp** | **vrrp**] command.
Packet-type	Packet type.
Slot	ID of the stack where the default CIR value is dynamically adjusted. The value indicates the slot ID if stacking is not configured.

Item	Description
CIR(Kbps)	Dynamically adjusted default CIR value, in kbit/s. If the default CIR value restores to the original default CIR value, NA is displayed. **NOTE** When the rate of sending packets to the CPU is too large, the CPU becomes overloaded. The device restores the original default CIR value for protocol packets and this field is displayed as NA.
Status	Result of dynamic adjustment. The value can be: ● success: indicates that the adjustment succeeds. ● fail: indicates that the adjustment fails. ● conflict: indicates that the adjusted default CIR value conflicts the configured CIR value. The CIR value configured by users takes effect.

14.2.43 display cpu-defend host-car statistics

Function

The **display cpu-defend host-car statistics** command displays the number of packets discarded in user-level rate limiting.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display cpu-defend host-car [**mac-address** *mac-address*] **statistics** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Indicates the number of discarded packets from the specified MAC address.	-
slot *slot-id*	Indicates the number of packets discarded by the specified slot.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the number of packets discarded in the user-level rate limiting, run this command.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- If the number of discarded packets is 0, the index is not displayed.

Example

Display the number of packets discarded in the user-level rate limiting.

```
<HUAWEI> display cpu-defend host-car statistics
slot 0
car-id                          car-drop
----------------------------------------------
3192                              740385
3347                                   7
4133                              529474
4471                              529477
5075                              529476
5836                              529474
6046                             1001218
```

Table 14-33 Description of the display cpu-defend host-car statistics command output

Item	Description
slot	Slot ID.
car-id	Bucket ID for rate limiting.
car-drop	Number of dropped packets whose rate exceeds the CAR. To configure the CAR value, run the **cpu-defend host-car** [**mac-address** *mac-address* | **car-id** *car-id*] **pps** *pps-value* command.

14.2.44 display cpu-defend policy

Function

The **display cpu-defend policy** command displays the attack defense policy configuration.

Format

display cpu-defend policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specified attack defense policy. ● If *policy-name* is specified, information about the specified attack defense policy is displayed. ● If *policy-name* is not specified, information about all attack defense policies is displayed.	The attack defense policy must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an attack defense policy is created, you can run the **display cpu-defend policy** command to view the stack ID that the attack defense policy is applied to and configurations of the attack defense policy.

Example

Display information about all attack defense policies.

```
<HUAWEI> display cpu-defend policy
  ----------------------------------------------------------------
 Name  : default
 Related slot : <3>
  ----------------------------------------------------------------
 Name  : test
 Description : defend_arp_attack
 Related slot : <mcu>
```

Display information about the attack defense policy named **test**.

```
<HUAWEI> display cpu-defend policy test
 Description : defend_arp_attack
```

```
Related slot : <0>
Configuration :
  Whitelist 1 ACL number : 2002
  Blacklist 1 ACL number : 2001
  Car packet-type arp-request : CIR(128)  CBS(24064)
  Deny packet-type arp-reply
  Port-type eni packet-type arp-request
  Linkup-car packet-type  ftp : CIR(5000)  CBS(940000)
```

Table 14-34 Description of the display cpu-defend policy command output

Item	Description
Name	Name of an attack defense policy. To configure an attack defense policy, run the **cpu-defend policy** command.
Description	Description of an attack defense policy. To configure a description for an attack defense policy, run the **description** command.
Related slot	Slot ID or stack ID that an attack defense policy is applied to. When mcu is displayed, it indicates the main control board.
Whitelist 1 ACL number	Number of an ACL defined in whitelist 1. To configure a whitelist, run the **whitelist** command.
Blacklist 1 ACL number	Number of an ACL defined in blacklist 1. To configure a blacklist, run the **blacklist** command.
Car packet-type arp-request	CIR values of ARP Request packets. To set the CIR values for ARP Request packets, run the **car** command.
Deny packet-type arp-reply	ARP Reply packets are discarded. To configure the device to discard ARP Reply packets, run the **deny** command.
Port-type eni packet-type arp-request	ARP Request packets are sent to the CPU through ENI ports.
Linkup-car packet-type ftp	CIR values of FTP packets after an FTP connection is set up. To set the CIR values of FTP packets after an FTP connection is set up, run the **linkup-car** and **cpu-defend application-apperceive enable** commands.

14.2.45 display cpu-defend port-type

Function

The **display cpu-defend port-type** command displays physical interfaces of Network-to-Network Interface (NNI), User-to-Network Interface (UNI), and Enhanced Network Interface (ENI) types.

NOTE

Only the S6735-S, S6720S-EI and S6720-EI support this command.

Format

display cpu-defend port-type slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	• This parameter specifies the slot ID if stacking is not configured. • This parameter specifies the stack ID if a stack is configured.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After specifying interfaces types for sending protocol packets using the **port type** { **uni** | **eni** | **nni** } and **port-type** { **uni** | **eni** | **nni** } **packet-type** *type* commands, you can run the **display cpu-defend port-type** command to view types of interfaces on the device.

Example

Display interface types in stack 0.

```
<HUAWEI> display cpu-defend port-type slot 0
 Uni Port :
 Eni Port :
 Nni Port :GigabitEthernet0/0/1-22
```

Table 14-35 Description of the display cpu-defend port-type command output

Item	Description
Uni Port	The interface is a user-side interface on the device.
Eni Port	The interface is an interface connected to another switch or user.
Nni Port	The interface is a network-side interface on the device.

14.2.46 display cpu-defend rate

Function

The **display cpu-defend rate** command displays the rate of sending protocol packets to the CPU.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display cpu-defend rate [**packet-type** *packet-type*] { **all** | **slot** *slot-id* }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
all	Indicates all switches in a stack if stack is enabled, or the switch itself if stack is disabled.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stack is enabled.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cpu-defend rate** command to view the rate of sending protocol packets to the CPU when checking the configuration of an attack defense policy. In this way, you can determine which type of protocols may attack the CPU based on the rate.

NOTE

To ensure normal operation of other services and protect the CPU, the rate of incremental protocol packets is calculated only in a specified period after you run the **display cpu-defend rate** command and displayed on the terminal. After you run this command, a message is displayed to wait for a while.

Example

Display the rate of ARP Reply packets sent from the switch to the CPU.

```
<HUAWEI> display cpu-defend rate packet-type arp-reply slot 0
Info: Please wait for a moment....
Cpu-defend rate on slot 0:
-------------------------------------------------------------------------------
Packet Type          Pass(bps)    Drop(bps)       Pass(pps)       Drop(pps)
-------------------------------------------------------------------------------
arp-reply              49504       86496            91             159
-------------------------------------------------------------------------------
```

Table 14-36 Description of the **display cpu-defend rate** command output

Item	Description
Packet Type	Packet type.
Pass(bps)	Number of forwarded bits within one second.
Drop(bps)	Number of discarded bits within one second.
Pass(pps)	Number of forwarded packets within one second.
Drop(pps)	Number of discarded packets within one second.

14.2.47 display cpu-defend statistics

Function

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU.

Format

display cpu-defend statistics [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

NOTE

The S1720GW-E and S1720GWR-E do not support this command.

Parameters

Parameter	Description	Value
packet-type *packet-type*	Displays statistics about the specified type of packets. *packet-type* specifies the packet type. ● If *packet-type* is specified, statistics on the specified type of protocol packets are displayed. ● If *packet-type* is not specified, statistics on all protocol packets are displayed.	The value depends on the protocol types supported by the device. **NOTE** You can specify the **ftp** parameter to view IPv6 FTP packet statistics.
all	Displays packet statistics about all the member switches in a stack if stacking is enabled or on the local switch if stacking is disabled. If **all** and **slot** are not specified, the CAR statistics on the master switch in a stack are displayed.	-
slot *slot-id*	● Specifies the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value depends on the actual configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU, including the number of forwarded and discarded packets. This helps the network administrator configure attack defense policies.

Precautions

If neither **all** nor **slot** is specified, the CAR statistics on the master switch in a stack are displayed.

Example

Display CAR statistics on the switch. (S5731-H used as an example)

```
<HUAWEI> display cpu-defend statistics
 Statistics on slot 0:
-----------------------------------------------------------------------------
Packet Type         Pass(Packet/Byte)   Drop(Packet/Byte)  Last-dropping-time
-----------------------------------------------------------------------------
arp-miss                       0                0                 -
                            0                0
arp-reply                      0                0                 -
                            0                0
arp-request                     0                0                 -
                            0                0
......
```

Display CAR statistics on the switch. (S5720-LI used as an example)

```
<HUAWEI> display cpu-defend statistics
 Statistics on mainboard:
-----------------------------------------------------------------------------
Packet Type         Pass(Packet)       Drop(Packet)
-----------------------------------------------------------------------------
8021x                      0          0
arp-reply                  0          0
arp-request                 0          0
bpdu                       0          0
bpdu-tunnel                 0          0
capwap-ctrl                 0          0
dhcp-client                 0          0
dhcp-server                 0          0
eth-ring                   0          0
fib-hit                   0          0
ftp                       0          0
https                     0          0
icmp                       0          0
igmp                       0          0
ip-cloud                   0          0
lacp                      0          0
ldt                       0          0
lnp                       0          0
nd                        0          0
ospf                       0          0
pim                        0          0
pppoe                      0          0
rip                       0          0
sip                       0          0
telnet                     0          0
vrrp                      0          0
--------------------------------------------------------------------
```

Display CAR statistics about Telnet packets on the switch. (S5731-H used as an example)

```
<HUAWEI> display cpu-defend statistics packet-type telnet
 Statistics on slot 0:
-------------------------------------------------------------------------------
Packet Type          Pass(Packet/Byte)   Drop(Packet/Byte)  Last-dropping-time
-------------------------------------------------------------------------------
telnet                     3625354          5612376421  2020-04-13 12:05:37
                         377036776         583687147k
-------------------------------------------------------------------------------
 Linkup statistics on slot 0:
-------------------------------------------------------------------------------
Packet Type          Pass(Packet/Byte)   Drop(Packet/Byte)  Last-dropping-time
-------------------------------------------------------------------------------
telnet                           0                  0                  -
                               0                  0
-------------------------------------------------------------------------------
```

Display CAR statistics about Telnet packets on the switch. (S5720-LI used as an example)

```
<HUAWEI> display cpu-defend statistics packet-type telnet
 Statistics on mainboard:
-------------------------------------------------------------------------------
Packet Type          Pass(Packet)       Drop(Packet)
-------------------------------------------------------------------------------
telnet                     0           0
-------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 14-37 Description of the **display cpu-defend statistics** command output

Item	Description
Statistics on slot 0	CAR statistics about protocol packets on a specified switch or stack. **NOTE** On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, you cannot view packet statistics on interfaces of the master switch in a stack.
Statistics on mainboard	CAR statistics about protocol packets on the MCU.
Linkup statistics on slot 0	CAR statistics about protocol packets collected when the protocol connection is established.
Packet Type	Packet type.

Item	Description
Pass(Packet/Byte)	Number of passed packets or bytes. **NOTE** The S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S does not support packet statistics collection based on the number of bytes.
Drop(Packet/Byte)	Number of dropped packets or bytes. **NOTE** When the length exceeds 11 digits, the end of the value is displayed as **k**, indicating that the value is multiplied by 1000. When the length exceeds 14 digits, the end of the value is displayed as **m**, indicating that the value is multiplied by 1000000. When the length exceeds 17 digits, the end of the value is displayed as **g**, indicating that the value is multiplied by 1000000000. Statistics on discarded packets cannot be collected for the standby and slave switches in a stack, which cover the following switch models: S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S
Last-dropping-time	Last time statistics about dropped packets were collected.

14.2.48 host-car disable

Function

The **host-car disable** command disables user-level rate limiting on interfaces.

The **undo host-car disable** command enables user-level rate limiting on interfaces.

By default, user-level rate limiting is enabled on all interfaces.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

host-car disable

undo host-car disable

Parameters

None

Views

GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch performs user-level rate limiting on the users connecting to all interfaces. If you are sure that the users connecting to an interface are secure, you can disable user-level rate limiting on this interface.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- After user-level rate limiting is disabled on an interface, the switch does not limit the rate of packets received from the specified user MAC address and cannot protect the interface against attacks. In addition, the packets of the same type sent from other users may be affected.
- Disable user-level rate limiting on network-side interfaces to prevent DHCP and ARP packets from being discarded.

Example

Disable user-level rate limiting on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] host-car disable
```

14.2.49 linkup-car

Function

The **linkup-car** command sets the CPCAR value for packets of a protocol connection, including the Committed Information Rate (CIR) and Committed Burst Size (CBS).

The **undo linkup-car** command restores the default CPCAR rate limit.

Table 14-38 lists the default CIR and CBS values for the setup of BGP, BGP4+, FTP, IPv6 FTP, HTTP, HTTPS, IKE, IPSEC-ESP, ISIS, OSPF, OSPFv3, SSH, TELNET, and TFTP connections; the CIR and CBS for sending packets of IP-CLOUD connections are 2048 kbit/s and 385024 bytes respectively.

Format

linkup-car packet-type { **bgp** | **bgp4plus** | **ftp** | **ftpv6** | **http** | **https** | **ike** | **ip-cloud** | **ipsec-esp** | **isis** | **ospf** | **ospfv3** | **ssh** | **telnet** | **tftp** } **cir** *cir-value* [**cbs** *cbs-value*]

undo linkup-car packet-type { **bgp** | **bgp4plus** | **ftp** | **ftpv6** | **http** | **https** | **ike** | **ip-cloud** | **ipsec-esp** | **isis** | **ospf** | **ospfv3** | **ssh** | **telnet** | **tftp** }

NOTE

- Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **bgp** parameter.
- Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **https** parameter.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **bgp4plus** and **isis** parameter.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **ospfv3** parameter.
- Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6735-S, S6720-EI, and S6720S-EI support the **ike** parameter.
- Only the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **ipsec-esp** parameter.
- Only the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5720S-LI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **ospf** parameter.
- Only the S200, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H support the **ip-cloud** parameter.

Parameters

Parameter	Description	Value
bgp	Indicates that the protocol type is BGP.	-
bgp4plus	Indicates that the protocol type is BGP4+.	-
ftp	Indicates that the protocol type is FTP.	-

Parameter	Description	Value
ftpv6	Indicates that the protocol type is IPv6 FTP.	-
http	Indicates that the protocol type is HTTP.	-
https	Indicates that the protocol type is HTTPS.	-
ike	Indicates that the protocol type is IKE. This parameter does not take effect in non-NAT scenarios.	-
ip-cloud	Indicates that the protocol type is IP-CLOUD.	-
ipsec-esp	Indicates that the protocol type is IPSEC-ESP. **ipsec-esp** specified in the **linkup-car** command indicates the type of the protocol used by IPsec EVPN, and **ipsec-esp** specified in the **car** command indicates the type of the protocol used by OSPFv3.	-
isis	Indicates that the protocol type is ISIS.	-
ospf	Indicates the protocol type is OSPF.	-
ospfv3	Indicates the protocol type is OSPFv3.	-
ssh	Indicates the protocol type is SSH.	-
telnet	Indicates the protocol type is TELNET.	-
tftp	Indicates the protocol type is TFTP.	-
cir *cir-value*	Specifies the CIR value.	The value is an integer that ranges from 64 to 65535, in kbit/s.

Parameter	Description	Value
cbs *cbs-value*	Specifies the CBS value.	The value is an integer that ranges from 10000 to 4294967295, in bytes. If the **cbs** is not set, the default *cbs-value* is 188 times the *cir-value*.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default CPCAR value of BGP, BGP4+, FTP, IPv6 FTP, HTTP, HTTPS, IP-CLOUD, ISIS, OSPFv3, OSPF, IKE, IPSEC-ESP, SSH, TFTP, or TELNET protocol is small. When a switch uses these protocols to transfer files or set up connections with other hosts or devices, the number of protocol packets sharply increases in a short period. When the packet rate exceeds the limit, the protocol packets are dropped. The switch may also undergo attacks of other protocols. This affects data transmission and causes service interruption.

You can run the **cpu-defend application-apperceive** command to enable active link protection, ensuring normal operation of these protocols related services when attacks occur. When a connection is set up, the switch sends packets at the rate of the CPCAR value configured using the **linkup-car** command. The CPCAR value can be set as required.

Follow-up Procedure

Run the **cpu-defend application-apperceive enable** command to enable ALP to enable the rate limit set using the **linkup-car** command. By default, ALP is enabled on FTP, IPv6 FTP, HTTP, IP-CLOUD, HTTPS, IKE, IPSEC-ESP, TFTP, SSH, and TELNET packets and disabled on BGP, BGP4+, ISIS, OSPF, and OSPFv3 packets.

Precautions

You are advised to run the **display cpu-defend configuration** command to check the CIR value supported by the protocol being used before running the **linkup-car** command to set the rate limit.

BGP, BGP4+, ISIS, OSPF, and OSPFv3 are disabled when the configuration is initialized. You can set the rate limit using the **car** command before the protocols are enabled and the **linkup-car** command after connections are set up and ALP is enabled.

You can set a shared CPCAR value for packets of FTP, IPv6 FTP, SSH, TFTP connections on S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-

H, and S5736-S. For example, the **linkup-car packet-type ftp cir** *cir-value* [**cbs** *cbs-value*] command specifies the CPCAR value for FTP packets when an FTP connection is set up, and also specifies the CPCAR value for packets of IPv6 FTP, SSH, TFTP connections.

Table 14-38 Default CIR and CBS values

Product	CIR	CBS
SS1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI	• FTP, IPv6 FTP, HTTP, SSH, TFTP: 1024 kbit/s • IKE: 64 kbit/s • IPSEC-ESP: 320 kbit/s • OSPF: 512 kbit/s • TELNET: 64 kbit/s	• FTP, IPv6 FTP, HTTP, SSH, TFTP: 192512 bytes • IKE: 12032 bytes • IPSEC-ESP: 60160 bytes • OSPF: 96256 bytes • TELNET: 12032 bytes
S5720I-SI	• FTP, IPv6 FTP, HTTP, SSH, TFTP: 1024 kbit/s • IKE: 64 kbit/s • IPSEC-ESP: 320 kbit/s • TELNET: 64 kbit/s	• FTP, IPv6 FTP, HTTP, SSH, TFTP: 192512 bytes • IKE: 12032 bytes • IPSEC-ESP: 60160 bytes • TELNET: 12032 bytes
S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M	• FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 1536kbit/s • IKE: 64kbit/s • IPSEC-ESP: 800kbit/s • OSPF: 512kbit/s • TELNET: 64kbit/s	• FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 288768bytes • IKE: 12032bytes • IPSEC-ESP: 150400bytes • OSPF: 96256bytes • TELNET: 12032bytes
S500, S5735-S, S5735S-S, S5735-S-I	• BGP: 1024kbit/s • FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 1536kbit/s • IKE: 64kbit/s • IPSEC-ESP: 800kbit/s • OSPF: 512kbit/s • TELNET: 64kbit/s	• BGP: 192512bytes • FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 288768bytes • IKE: 12032bytes • IPSEC-ESP: 150400bytes • OSPF: 96256bytes • TELNET: 12032bytes

Product	CIR	CBS
S5735S-H, S5736-S	● BGP: 1024 kbit/s ● FTP, IPv6 FTP, HTTP, SSH, TFTP: 1536 kbit/s ● IKE: 64 kbit/s ● IPSEC-ESP: 4096 kbit/s ● OSPF: 512 kbit/s ● TELNET: 64 kbit/s	● BGP: 192512 bytes ● FTP, IPv6 FTP, HTTP, SSH, TFTP: 288768 bytes ● IKE: 12032 bytes ● IPSEC-ESP: 770048 bytes ● OSPF: 96256 bytes ● TELNET: 12032 bytes
S6735-S, S6720-EI, S6720S-EI	● BGP: 1024 kbit/s ● FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 1536 kbit/s ● IKE: 64 kbit/s ● IPSEC-ESP: 4096 kbit/s ● BGP4+, ISIS, OSPF, OSPFv3: 512 kbit/s ● TELNET: 64 kbit/s	● BGP: 192512 bytes ● FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 288768 bytes ● IKE: 12032 bytes ● IPSEC-ESP: 770048 bytes ● BGP4+, ISIS, OSPF, OSPFv3: 96256 bytes ● TELNET: 12032 bytes
S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S	● BGP: 1024kbit/s ● FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 1536kbit/s ● IPSEC-ESP: 800kbit/s ● BGP4+, ISIS, OSPF, OSPFv3: 512kbit/s ● TELNET: 64kbit/s	● BGP: 192512bytes ● FTP, IPv6 FTP, HTTP, HTTPS, SSH, TFTP: 288768bytes ● IPSEC-ESP: 150400bytes ● BGP4+, ISIS, OSPF, OSPFv3: 96256bytes ● TELNET: 12032bytes

Example

Set the CIR and CBS for BGP packets to 1000 kbit/s and 100000 bytes.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] linkup-car packet-type bgp cir 1000 cbs 100000
```

14.2.50 port type

Function

The **port type** command configures the interface type. The interface type can be Network-to-Network Interface (NNI), User-to-Network Interface (UNI), or Enhanced Network Interface (ENI).

The **undo port type** command cancels the configuration.

By default, the interface type is NNI.

NOTE

Only the S6735-S, S6720S-EI and S6720-EI support this command.

Format

port type { **uni** | **eni** | **nni** }

undo port type

Parameters

Parameter	Description	Value
uni	Indicates that the interface is a user-side interface on the device.	-
eni	Indicates that the interface is connected to another switch or user. An ENI supports all protocols that are supported by an UNI.	-
nni	Indicates that the interface is a network-side interface on the device. An NNI supports all protocol packets.	-

Views

40GE interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, protocol packets that can be sent to the CPU are controlled by an ACL. If protocol packets are sent to the device, packets received by interfaces cannot be differentiated.

If an interface is attacked and the user disables the device to send packets, packets cannot be sent from other interfaces, affecting communications of the device. If an interface is attacked and the user does not disable the device to send packets, attack packets occupy resources and valid packets cannot be sent.

For example, OSPF is enabled on an interface and OSPF packets are sent to the device. If a non-OSPF interface is attacked, attack packets will occupy resources and valid OSPF packets cannot be forwarded. As a result, OSPF negotiation becomes slow or fails.

The **port type** command specifies the interface types according to the interface location. Interfaces of different types support different protocols and send only the packets of the supported protocols to the CPU. This reduces the workload of the CPU and provides flexible ways to protect the CPU.

Precautions

If you run the **port type** command multiple times, only the latest configuration takes effect.

Follow-up Procedure

This command differentiates packets from different types of interfaces so that the attack packets are denied and valid packets are forwarded. If an attack occurs, you can run the **deny** command to discard packets of a specified type or run the **car** command to limit the rate of a specified type of protocol packets.

Example

Configure GE0/0/1 as an NNI.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port type nni
```

14.2.51 port-type

Function

The **port-type** command maps interfaces to protocol types. The type can be User-to-Network Interface (UNI), Enhanced Network Interface (ENI), or Network-to-Network Interface (NNI).

The **undo port-type** command cancels the configuration.

By default, the type of interface sending protocol packets to the CPU is displayed using the **display cpu-defend configuration** command.

NOTE

Only the S6735-S, S6720S-EI and S6720-EI support this command.

Format

port-type { **uni** | **eni** | **nni** } **packet-type** *packet-type*

undo port-type [**uni** | **eni** | **nni**] **packet-type** *packet-type*

Parameters

Parameter	Description	Value
uni	Indicates that the interface is a user-side interface on the device.	-

Parameter	Description	Value
eni	Indicates that the interface is connected to another switch or user. An ENI supports all protocols that are supported by an UNI.	-
nni	Indicates that the interface is a network-side interface on the device. An NNI supports all protocol packets.	-
packet-type *packet-type*	Specifies the protocol supported by an interface type. A protocol is mapped to only one interface type.	The supported packet type depends on the device.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, protocol packets that can be sent to the CPU are controlled by an ACL. If protocol packets are sent to the device, packets received by interfaces cannot be differentiated.

If an interface is attacked and the user disables the device to send packets, packets cannot be sent from other interfaces, affecting communications of the device. If an interface is attacked and the user does not disable the device to send packets, attack packets occupy resources and valid packets cannot be sent.

The **port-type** command maps interfaces to protocol types. The **port type** command specifies the interface types according to port locations. By using the two commands, the interfaces send only the packets of the supported protocols. This reduces the workload of CPU and provides ways to flexibly protect the CPU.

NOTE

Protocol packets are not supported by the UNI, ENI, or NNI interfaces. These protocol packets are sent to the CPU for processing from any interface on the device.

Procedure

After you run the **port type** command to configure interface types, run the **port-type** command to specify the protocols supported by the interfaces and the method to process the protocol packets.

Precautions

If you run the **port-type** command multiple times, only the latest configuration takes effect because a protocol is mapped to only one interface type.

Follow-up Procedure

This command differentiates packets from different types of interfaces so that the attack packets are denied and valid packets are forwarded. If an attack occurs, you can run the **deny** command to discard a specified type of packets. When receiving packets of the type, the interfaces discard these packets. You can also run the **car (attack defense policy view)** command to limit the rate of attack packets of a specified type.

Example

Configure UNI interfaces to send ARP Reply packets to the CPU.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] port-type uni packet-type arp-reply
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend-policy test global
```

14.2.52 reset auto-defend attack-source

Function

The **reset auto-defend attack-source** command clears information about attack sources.

Format

reset auto-defend attack-source [**history**] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
history	Deletes history attack source information. If **history** is not specified, all existing attack source information is deleted.	-
slot *slot-id*	- This parameter specifies the slot ID if stacking is not configured. - This parameter specifies the stack ID if stacking is enabled. If **slot** *slot-id* is not specified, information about attack sources is cleared.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the latest attack source information on the device, run the **reset auto-defend attack-source** command to delete the existing attack source information, wait for a period, and run the **display auto-defend attack-source** command.

To delete history attack source information, run the **reset auto-defend attack-source history** command.

Precautions

After the **reset auto-defend attack-source** command is run, information about attack sources is cleared and cannot be restored.

Example

Delete existing attack source information on the device.

```
<HUAWEI> system-view
[HUAWEI] reset auto-defend attack-source
```

14.2.53 reset auto-defend attack-source trace-type

Function

The **reset auto-defend attack-source trace-type** command clears the counter of packets traced after attack source tracing based on source MAC addresses, source IP addresses, or source ports+VLANs is configured.

Format

reset auto-defend attack-source trace-type { **source-mac** [*mac-address*] | **source-ip** [*ipv4-address* | **ipv6** *ipv6-address*] | **source-portvlan** [**interface** *interface-type interface-number* **vlan-id** *vlan-id* [**cvlan-id** *cvlan-id*]] } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
source-mac [*mac-address*]	Clears the counter of packets traced after attack source tracing based on source MAC addresses is configured. If *mac-address* is specified, the counter of traced packets sent from the specified MAC address is cleared.	The value of *mac-address* is in H-H-H format. An H contains 1 to 4 hexadecimal numbers.
source-ip [*ipv4-address* | **ipv6** *ipv6-address*]	Clears the counter of packets traced after attack source tracing based on source IP addresses is configured. If an ip-address is specified, the counter of traced packets sent from the specified IP address is cleared. ● *ipv4-address* specifies the IPv4 address of an interface. ● **ipv6** *ipv6-address* specifies the IPv6 address of an interface.	● The value of *ipv4-address* is in dotted decimal notation. ● The value of *ipv6-address* is in format X:X:X:X:X:X:X:X. The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters.
source-portvlan [**interface** *interface-type interface-number* **vlan-id** *vlan-id* [**cvlan-id** *cvlan-id*]]	Clears the counter of packets traced after attack source tracing based on source ports+VLANs is configured. If a port or VLAN is specified, the counter of traced packets sent from the specified port or VLAN is cleared. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● **vlan-id** *vlan-id* specifies the ID of the VLAN. ● **cvlan-id** *cvlan-id* specifies the inner VLAN ID in a QinQ packet.	*vlan-id* is an integer that ranges from 1 to 4094. *cvlan-id* is an integer that ranges from 1 to 4094.

Parameter	Description	Value
slot *slot-id*	- This parameter specifies the slot ID if stacking is not configured. - This parameter specifies the stack ID if stack is enabled.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view information about attack sources in a specified period, run the **reset auto-defend attack-source** command to clear existing information about attack sources and run the **display auto-defend attack-source** command. However, the **reset auto-defend attack-source** clears information about all attack sources. You can run the **reset auto-defend attack-source trace-type** command to clear information about specified attack sources.

Precautions

After the **reset auto-defend attack-source trace-type** command is run, information about attack sources is cleared and cannot be restored.

Example

Clear the counter of traced packets sent from IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] reset auto-defend attack-source trace-type source-ip 10.1.1.1
```

14.2.54 reset auto-port-defend statistics

Function

The **reset auto-port-defend statistics** command deletes packet statistics on port attack defense.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset auto-port-defend statistics [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Deletes packet statistics of port attack defense on the interfaces of all stacked switches in a stack environment or on all interfaces of the local switch in a non-stack environment. If **all** or **slot** *slot-id* is not specified, packet statistics on the master device (stack configured) or local device (stack not configured) are deleted.	-
slot *slot-id*	● The value indicates the slot ID if stacking is not configured. ● The value indicates the stack ID when stack is configured.	The value depends on the device configuration.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before viewing packet statistics of port attack defense in a certain period, delete existing packet statistics, and then run the **display auto-port-defend statistics** command to collect the latest statistics.

Precautions

The deleted packet statistics cannot be restored.

Example

Delete packet statistics on the interfaces of the device.

```
<HUAWEI> reset auto-port-defend statistics
```

14.2.55 reset cpu-defend dynamic-car history-record

Function

The **reset cpu-defend dynamic-car history-record** command clears history records on dynamic adjustment of the default CIR value of protocol packets.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset cpu-defend dynamic-car history-record

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **reset cpu-defend dynamic-car history-record** command to clear the previous records and run the **display cpu-defend dynamic-car history-record** command to view the history records on dynamic adjustment of the default CIR value of protocol packets in a specified period.

Precautions

The **reset cpu-defend dynamic-car history-record** command clears history records on dynamic adjustment of the default CIR value of protocol packets and the records cannot be restored.

Example

Clear the history records on dynamic adjustment of the default CIR value of protocol packets.

```
<HUAWEI> reset cpu-defend dynamic-car history-record
```

14.2.56 reset cpu-defend host-car statistics

Function

The **reset cpu-defend host-car statistics** command clears packet statistics in the user-level rate limiting.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset cpu-defend host-car [**mac-address** *mac-address*] **statistics** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Clears statistics on the packets from the specified MAC address.	-
slot *slot-id*	Clears packet statistics on the specified slot.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Before viewing the latest packet statistics in the user-level rate limiting, run this command to clear existing packet statistics.

NOTICE

Packet statistics cannot be restored after they are deleted. Exercise caution when you use the command.

Example

Clear packet statistics in user-level rate limiting.

```
<HUAWEI> reset cpu-defend host-car statistics
```

14.2.57 reset cpu-defend statistics

Function

The **reset cpu-defend statistics** command clears statistics on packets sent to the CPU.

Format

reset cpu-defend statistics [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

NOTE

The S1720GW-E and S1720GWR-E do not support this command.

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the protocol type of packets. *packet-type* specifies the packet type. ● If **packet-type** *packet-type* is specified, the statistics on the specified type of protocol packets are cleared. ● If **packet-type** *packet-type* is not specified, the statistics on all protocol packets are cleared.	The supported packet type depends on the device.
all	This parameter indicates all switches in a stack if stacking is enabled, or the switch itself if stack is disabled. If **all** and **slot** are not specified, the CAR statistics on the master switch in a stack are cleared.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view statistics on the packets sent to the CPU in a specified period, run the **reset cpu-defend statistics** command to clear existing statistics and run the **display cpu-defend statistics** command.

Precautions

The deleted packet statistics cannot be restored.

Example

Clear statistics on BGP packets sent to the CPU.

```
<HUAWEI> reset cpu-defend statistics packet-type bgp slot 0
```

14.2.58 user-defined-flow

Function

The **user-defined-flow** command configures a user-defined flow.

The **undo user-defined-flow** command deletes a user-defined flow.

By default, no user-defined flow is configured.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

user-defined-flow *flow-id* **acl** *acl-number*

undo user-defined-flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of the user-defined flow.	The value is an integer that ranges from 1 to 8.
acl *acl-number*	Specifies the number of an Access Control List (ACL). The ACL referenced by a user-defined flow on the device can be a basic ACL, an advanced ACL, or a Layer 2 ACL.	The value is an integer that ranges from 2000 to 4999. • 2000 to 2999: basic ACLs • 3000 to 3999: advanced ACLs • 4000 to 4999: Layer 2 ACLs

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When unknown attacks occur on the network, you can run the **user-defined-flow** command to bind an ACL rule with a user-defined flow. Then you can run the **car user-defined-flow** *flow-id* **cir** *cir-value* [**cbs** *cbs-value*] command to limit the rate of flows with the specific characteristic or run the **deny user-defined-flow** *flow-id* command to discard these flows.

Precautions

If an ACL containing the deny action is applied to the user-defined flow, packets matching the ACL are discarded.

The priority of user-defined flows is higher than that of dynamic link protection. That is, if a user-defined flow is configured on a device and packets match the user-defined flow, dynamic link protection does not take effect on the packets.

Example

Specify ACL 2001 as the rule of user-defined flow 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] user-defined-flow 2 acl 2001
```

14.2.59 whitelist

Function

The **whitelist** command configures a whitelist.

The **undo whitelist** command deletes a whitelist.

By default, no whitelist is configured.

Format

whitelist *whitelist-id* **acl** *acl-number*

undo whitelist *whitelist-id*

Parameters

Parameter	Description	Value
whitelist-id	Specifies the ID of a whitelist.	The value is an integer that ranges from 1 to 8.

Parameter	Description	Value
acl *acl-number*	Specifies the number of an Access Control List (ACL). The ACL referenced by a whitelist on the device can be a basic ACL, an advanced ACL, or a Layer 2 ACL.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can create a whitelist and add users with specified characteristic to the whitelist. The device processes packets sent from users in the whitelist first. You can set the attributes of the whitelist flexibly by defining ACL rules.

A maximum of 8 whitelists can be configured in an attack defense policy on the device.

Precautions

If an ACL containing the deny action is applied to the whitelist, packets sent from users in the whitelist are discarded.

For X series cards, the packets from users in the whitelist are preferentially sent to the CPU at a high rate, and the **display cpu-defend statistics** command cannot collect statistics on these packets.

Example

Specify ACL 2002 as the rule of whitelist 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] whitelist 2 acl 2002
```

14.3 MFF Configuration Commands

14.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.3.2 display mac-forced-forwarding

Function

The **display mac-forced-forwarding** command displays the MFF configuration.

Format

display mac-forced-forwarding { **network-port** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
network-port	Displays network interface information.	-
vlan *vlan-id*	Displays the MFF configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mac-forced-forwarding** command displays the MFF network interface information and MFF configuration in a specified VLAN.

NOTE

When the **user-bind static** command is executed to configure a static binding entry for a non-DHCP user, at least **ip-address** and **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*] must be specified. In this case, the MFF entry that has the same IP address and VLAN ID as the static binding entry can be deleted when the static binding entry is deleted.

Example

Display information about the MFF network interface.

```
<HUAWEI> display mac-forced-forwarding network-port
--------------------------------------------------------------------------------
```

```
VLAN ID                Network-ports
-------------------------------------------------------------------------------
VLAN 10                GigabitEthernet0/0/1
                       GigabitEthernet0/0/2
                       GigabitEthernet0/0/3
VLAN 100               GigabitEthernet0/0/4
                       GigabitEthernet0/0/5
```

Table 14-39 Description of the display mac-forced-forwarding network-port command output

Item	Description
VLAN ID	ID of the VLAN that the network interface belongs to.
Network-ports	Network interface.

Display the MFF configuration in VLAN 100.

```
<HUAWEI> display mac-forced-forwarding vlan 100
[Vlan 100] MFF host total count = 3
-------------------------------------------------------------------------------
Servers        192.168.1.2
               192.168.1.3
-------------------------------------------------------------------------------
User IP        User MAC          Gateway IP       Gateway MAC
-------------------------------------------------------------------------------
192.168.1.10   00e0-fc01-0001    192.168.1.254    00e0-fc02-0001
192.168.1.11   00e0-fc01-0002    192.168.1.254    00e0-fc02-0001
192.168.1.12   00e0-fc01-0003    192.168.1.252    00e0-fc02-0003
-------------------------------------------------------------------------------
```

Table 14-40 Description of the display mac-forced-forwarding vlan command output

Item	Description
MFF host total count	Number of users in VLAN 100.
Servers	IP addresses of servers in VLAN 100.
User IP	IP addresses of users in VLAN 100.
User MAC	MAC addresses of users in VLAN 100.
Gateway IP	Gateway IP address.
Gateway MAC	Gateway MAC address.

14.3.3 mac-forced-forwarding arp-trigger

Function

The **mac-forced-forwarding arp-trigger** command enables an EAN to add or update an MFF entry when receiving an ARP packet from a user.

The **undo mac-forced-forwarding arp-trigger** command disables an EAN from adding or updating an MFF entry when receiving an ARP packet from a user.

By default, the EAN does not add or update an MFF entry when receiving an ARP packet from a user.

Format

mac-forced-forwarding arp-trigger

undo mac-forced-forwarding arp-trigger

Parameters

N/A

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a data center, users and virtual machine (VM) servers are isolated at Layer 2 on EAN devices using MFF. If a VM connects to another EAN and does not send DHCP request packets after migrating between servers, the backup binding table may exist on the new EAN device and the original EAN may still reserve the MFF entry. This cannot ensure security of Layer 2 isolation and Layer 3 communication between users and servers. Run the **mac-forced-forwarding arp-trigger** command on the new EAN to enable it to check binding entries when receiving an ARP packet from the user. If an entry matches the user, the EAN updates the MFF entry. If no entry matches the user, the EAN adds a new entry. The EAN broadcasts the ARP packet to all network interfaces when receiving the first ARP packet regardless of whether the user entry exists.

Prerequisite

MFF has been enabled in the system view and VLAN view using the **mac-forced-forwarding enable** command.

Example

Enable the EAN to add or update the MFF entries when receiving an ARP packet from a user in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding arp-trigger
```

14.3.4 mac-forced-forwarding dumb-terminal-compatible

Function

The **mac-forced-forwarding dumb-terminal-compatible** command configures a device to forward the ARP packets from the gateway to dumb terminals.

The **undo mac-forced-forwarding dumb-terminal-compatible** command disables a device from forwarding the ARP packets from the gateway to dumb terminals.

By default, a device does not forward the ARP packets from gateway to dumb terminals.

Format

mac-forced-forwarding dumb-terminal-compatible

undo mac-forced-forwarding dumb-terminal-compatible

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MFF device connects to dumb terminals (which do not actively send ARP request packets or send ARP request packets at a long interval), the MFF device must transparently transmit the ARP packets from gateway to dumb terminals after the MFF entries are aged out; otherwise, the user ARP entries on gateway are aged out and user services are interrupted. Therefore, when the MFF device connects to dumb terminals, the MFF device needs to be configured to transparently transmit the ARP packets from gateway to dumb terminals.

Prerequisites

Global MFF has been enabled using the **mac-forced-forwarding enable** command.

Precautions

After the MFF device is configured to transparently transmit ARP packets to dumb terminals, run the **mac-forced-forwarding static-gateway** command to configure an IP address for the static gateway; otherwise, this function does not take effect.

After this function is enabled, the MFF device searches the static binding table when receiving ARP request packets from the gateway (configured using the **user-bind static** command):

- If the outbound interface is found in the static binding table, the device forwards the ARP request packets through this interface.
- If the outbound interface is not found in the static binding table, the device broadcasts the ARP request packets in the VLAN. In this situation, all users in the VLAN can receive the ARP packets.

Example

Configure a device to transparently transmit ARP packets from gateway to dumb terminals in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mac-forced-forwarding enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding dumb-terminal-compatible
```

14.3.5 mac-forced-forwarding enable

Function

The **mac-forced-forwarding enable** command enables MFF.

The **undo mac-forced-forwarding enable** command disables MFF.

By default, MFF is disabled.

Format

mac-forced-forwarding enable

undo mac-forced-forwarding enable

Parameters

None

Views

System view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Many networks require that the gateway monitor data traffic and isolate users. MFF isolates users at Layer 2 and connects users at Layer 3 on the same network segment. MFF enables traffic to be forwarded through the gateway. This implements traffic monitoring and accounting and ensures network security.

Precautions

You can run the **mac-forced-forwarding enable** command in the VLAN view and perform other configurations only after you enable MFF globally in the system view.

After MFF is disabled in the system view, other MFF configurations are automatically deleted.

MFF cannot be enabled in a VLAN where the super VLAN or VLANIF interface is configured.

MFF cannot be enabled in a sub-VLAN where the super VLAN and VLANIF interface are configured.

The MFF function is implemented based on ARP proxy, whereas the EAI function is implemented based on ARP request packet forwarding. Therefore, the two functions conflict with each other. If you have enabled both MFF and EAI in the same VLAN, the MFF function takes effect.

NOTE

When you enable MFF, if ACL resources are insufficient, the MFF function does not take effect.

MFF cannot be configured in the super-VLAN.

When DHCP relay is configured in a super VLAN, MFF cannot be enabled in its sub-VLANs.

Example

Enable MFF in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mac-forced-forwarding enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
```

14.3.6 mac-forced-forwarding gateway-detect

Function

The **mac-forced-forwarding gateway-detect** command enables timed gateway detection and sets the gateway detection interval.

The **undo mac-forced-forwarding gateway-detect** command disables timed gateway detection.

By default, timed gateway detection is enabled and the default gateway detection interval is 30s.

Format

mac-forced-forwarding gateway-detect [**interval** *interval-time*]

undo mac-forced-forwarding gateway-detect

Parameters

Parameter	Description	Value
interval *interval-time*	Indicates the gateway detection interval.	The value is an integer that ranges from 30 to 17280, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a practical network, services may be interrupted for a long time because the MFF-enabled device cannot immediately detect the gateway MAC address change. Timed gateway detection can solve this problem. After the detection function is enabled (enabled by default), the MFF-enabled device scans recorded gateway information every *interval-time* seconds. For each gateway recorded, the MFF-enabled device uses user information to construct an ARP request packet and sends it to the network interface. The MFF-enabled device then learns the gateway MAC address from the ARP reply packet. If the gateway MAC address changes, the MFF-enabled device immediately updates the gateway information and broadcasts gratuitous ARP packets to users. Users can update the gateway address.

Prerequisites

MFF has been enabled in a VLAN using the **mac-forced-forwarding enable** command.

Precautions

When detecting multiple gateway addresses, the MFF-enabled device sends an ARP reply packet with the first gateway address by default.

After MFF is enabled, timed gateway detection does not take effect if no ARP request packet is received from the user or gateway or if no user is authorized by the DHCP server to access the network.

If a gateway fails, traffic between users will be blocked. To avoid this situation, the device considers a gateway invalid if it does not receive a response from the gateway after five detection attempts. The device then deletes the MAC address entry of the invalid gateway. If the gateway detection interval is changed during a detection, the number of detection times is accumulated.

Example

Enable timed gateway detection in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mac-forced-forwarding enable
[HUAWEI-vlan10] mac-forced-forwarding gateway-detect
```

14.3.7 mac-forced-forwarding igmp-query discard

Function

The **mac-forced-forwarding igmp-query discard** command configures an MFF-enabled device to discard the IGMP Query messages from users when both MFF and IGMP snooping are enabled in a VLAN.

The **undo mac-forced-forwarding igmp-query discard** command disables an MFF-enabled device from discarding the IGMP Query messages from users when both MFF and IGMP snooping are enabled in a VLAN.

By default, an MFF-enabled device does not discard the IGMP Query messages from users when both MFF and IGMP snooping are enabled in a VLAN.

Format

mac-forced-forwarding igmp-query discard

undo mac-forced-forwarding igmp-query discard

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

After MFF and IGMP snooping are enabled in a VLAN, the IGMP Query messages are broadcast in the VLAN. To prevent IGMP Query message broadcasting, use the **mac-forced-forwarding igmp-query discard** command.

Example

Configure an MFF-enabled device to discard the IGMP Query messages from users in VLAN10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mac-forced-forwarding igmp-query discard
```

14.3.8 mac-forced-forwarding ipv6-isolate

Function

The **mac-forced-forwarding ipv6-isolate** command configures the user-side inbound interface on a device to discard IPv6 packets.

The **undo mac-forced-forwarding ipv6-isolate** command disables a device from discarding IPv6 packets from users.

By default, the user-side inbound interface on a device does not discard IPv6 packets from users.

Format

mac-forced-forwarding ipv6-isolate

undo mac-forced-forwarding ipv6-isolate

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **mac-forced-forwarding ipv6-isolate** command is used, the user-side inbound interface on a device discards the IPv6 packets from users to prevent IPv6 packets from being broadcast on the VLAN. If the device does not discard IPv6 packets, users can learn the MAC addresses of each other, which makes MFF user isolation function invalid.

Prerequisites

The MFF function has been enabled in the system view and the VLAN view.

The VLAN contains at least one network-side interface.

Example

Configure the user-side inbound interface on a device to discard IPv6 packets from users.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding ipv6-isolate
```

14.3.9 mac-forced-forwarding network-port

Function

The **mac-forced-forwarding network-port** command configures an interface as a network interface.

The **undo mac-forced-forwarding network-port** command restores the interface to be a user interface.

By default, an interface is a user interface.

Format

mac-forced-forwarding network-port

undo mac-forced-forwarding network-port

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make MFF in a VLAN effective, ensure that at least one network interface belongs to the VLAN. Therefore, configure network interfaces for MFF.

The interface that is connected to the gateway and other network devices is configured as a network interface.

Precautions

MFF has been enabled in the system view using the **mac-forced-forwarding enable** command. Regardless of whether MFF is enabled in the VLAN that an interface belongs to, the interface can be configured as a network interface.

Multiple interfaces can be configured as network interfaces.

Example

Configure GE0/0/1 as a network interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-forced-forwarding network-port
Info: This operation may take a few seconds. Please wait for a moment.....
```

14.3.10 mac-forced-forwarding network-port-arp-trigger

Function

The **mac-forced-forwarding network-port-arp-trigger** command enables the network interface on an EAN to delete an MFF entry when the network port receives an ARP packet.

The **undo mac-forced-forwarding network-port-arp-trigger** command disables the network interface on an EAN from deleting an MFF entry when the network port receives an ARP packet.

By default, the network interface on an EAN does not delete the MFF entry when receiving an ARP packet.

Format

mac-forced-forwarding network-port-arp-trigger

undo mac-forced-forwarding network-port-arp-trigger

Parameters

N/A

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a data center, users and VM servers are isolated at Layer 2 on EAN devices using MFF. If a VM connects to another EAN after migrating between servers, and the binding table on the original EAN is not aged out, the original EAN considers the VM an MFF host. If an attacker accesses users or sends ARP request packets using the IP address and MAC address of the VM, the original EAN allows the request. Attacks are not defended. After you run the **mac-forced-forwarding network-port-arp-trigger** command on the original EAN, the original EAN determines that the VM has migrated to another EAN and deletes the MFF entry mapping the VM when receiving ARP packets from this VM.

Prerequisites

MFF has been enabled in the system view and VLAN view using the **mac-forced-forwarding enable** command.

Example

Enable the network interface on an EAN to delete an MFF entry when receiving an ARP packet.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding network-port-arp-trigger
```

14.3.11 mac-forced-forwarding server

Function

The **mac-forced-forwarding server** command configures the IP address for a server on the MFF network.

The **undo mac-forced-forwarding server** command deletes the configured IP address of a server.

By default, no IP address is configured for servers.

Format

mac-forced-forwarding server *server-ip* &<1–10>

undo mac-forced-forwarding server { *server-ip* | **all** }

Parameters

Parameter	Description	Value
server-ip	Specifies the IP address for a server.	The value is in dotted decimal notation. **NOTE** This IP address must be a class A, B, or C address. If the IP address is a class A address, it cannot be in the format 0.x.x.x.
all	Specifies IP addresses for all servers.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to the gateway, application servers such as the DHCP, multicast, or another server may be deployed on a network. You can configure IP addresses for application servers and set a list of accessible application servers on the MFF-enabled device.

- When a network interface on the MFF-enabled device receives an ARP request from a specified application server, the MFF-enabled device responds with the user MAC address by default. The packets sent from the server to the user are directly forwarded without passing through the gateway.
- If the MFF-enabled device is configured to transparently transmit ARP request packets, the device responds with the gateway MAC address. The packets sent from the server to the user are forwarded through the gateway.

Prerequisites

MFF has been enabled in a VLAN using the **mac-forced-forwarding enable** command.

Precautions

When the number of configured servers reaches the upper limit 10, run the **undo mac-forced-forwarding server** { *server-ip* | **all** } command to delete unneeded servers before you configure new servers.

NOTE

This command is required only when the application servers and clients are in the same VLAN.

Example

Configure IP address 192.168.1.2 for a server in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding server 192.168.1.2
```

14.3.12 mac-forced-forwarding static-gateway

Function

The **mac-forced-forwarding static-gateway** command configures a static gateway IP address in a VLAN.

The **undo mac-forced-forwarding static-gateway** command cancels the configuration.

By default, no static gateway IP address is configured in a VLAN.

Format

mac-forced-forwarding static-gateway *ip-address* &<1-16>

undo mac-forced-forwarding static-gateway { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the static gateway IP address in a VLAN. A maximum of 16 static gateway IP addresses in a VLAN can be specified in this command.	The value is in dotted decimal notation. **NOTE** This IP address must be a class A, B, or C address. If the IP address is a class A address, it cannot be in the format 0.x.x.x.
all	Deletes all static gateway IP addresses in the VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The static gateway is applicable when users are configured with static IP addresses. These users cannot dynamically obtain gateway information through DHCP packets. In this case, configure a static gateway address for each VLAN. After you run the **mac-forced-forwarding static-gateway** command, the users who are not authorized by the DHCP server can use the static gateway address to access the network. The users who are authorized by the DHCP server can still access the original gateway.

Prerequisites

Global MFF has been enabled using the **mac-forced-forwarding enable** command.

Precautions

If a static gateway IP address is changed, users will fail to access the network. The MAC address in the ARP table on the client belongs to the old gateway. After a new gateway is configured, the ARP entry on client is not updated immediately (that is, the MAC address in ARP table is not updated to the new gateway's MAC address). Therefore, the user cannot access the network.

Example

Configure static gateway IP address 10.1.1.10 in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding static-gateway 10.1.1.10
```

14.3.13 mac-forced-forwarding user-detect transparent

Function

The **mac-forced-forwarding user-detect transparent** command enables transparent transmission of ARP request packets.

The **undo mac-forced-forwarding user-detect transparent** command disables transparent transmission of ARP request packets.

By default, transparent transmission of ARP request packets is disabled.

Format

mac-forced-forwarding user-detect transparent

undo mac-forced-forwarding user-detect transparent

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MFF networking, if the gateway performs accounting for users based on the online duration, the gateway must know whether a user is online at a specified moment. By default, the MFF-enabled device sends ARP reply packets in response to ARP request packets sent from the gateway. The MFF-enabled device can always send ARP reply packets as long as the MFF entry is not aged out. As a result, the gateway always considers users online even if they have gone offline.

To solve this problem, configure the MFF-enabled device to transparently transmit ARP request packets sent from the gateway to the user. Then, the MFF-enabled device does not respond to the ARP packets. If the gateway does not receive the ARP reply packet from a user, the gateway considers that the user has gone offline. The gateway can monitor the user status in a timely manner and correctly perform accounting.

Prerequisites

Global MFF has been enabled using the **mac-forced-forwarding enable** command.

Precautions

In other scenarios, use the default configuration.

Example

Enable transparent transmission of ARP request packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mac-forced-forwarding enable
[HUAWEI-vlan10] mac-forced-forwarding user-detect transparent
```

14.4 Attack Defense Configuration Commands

14.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.4.2 anti-attack abnormal enable

Function

The **anti-attack abnormal enable** command enables defense against malformed packet attacks.

The **undo anti-attack abnormal enable** command disables defense against malformed packet attacks.

The **anti-attack abnormal disable** command disables defense against malformed packet attacks.

By default, defense against malformed packet attacks is enabled.

Format

anti-attack abnormal enable

undo anti-attack abnormal enable

anti-attack abnormal disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The malformed packet attack is to send malformed IP packets to the system. If such an attack occurs, the system may break down when processing the malformed IP packets. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack abnormal enable** command to enable defense against malformed packets.

The device detects malformed packets after defense against malformed packets is enabled.

The device directly discards packets of the following types:

- Flood attacks from IP null payload packets
- Attacks from IGMP null payload packets
- LAND attacks
- Smurf attacks
- Attacks from packets with invalid TCP flag bits

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including malformed packets.

Example

Enable defense against malformed packet attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack abnormal enable
```

14.4.3 anti-attack enable

Function

The **anti-attack enable** command enables defense against all attack packets.

The **undo anti-attack enable** command disables defense against all attack packets.

The **anti-attack disable** command disables defense against all attack packets.

By default, defense against all attack packets is enabled.

Format

anti-attack enable

undo anti-attack enable

anti-attack disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different types of attacks on a network cause high device usage or system breakdown, affecting network services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack enable** command to enable defense against all attack packets.

Precautions

Running the **anti-attack enable** command is equivalent to running all of the following commands:

- **anti-attack abnormal enable**
- **anti-attack fragment enable**
- **anti-attack tcp-syn enable**
- **anti-attack udp-flood enable**
- **anti-attack icmp-flood enable**

Example

Enable defense against all attack packets.

```
<HUAWEI> system-view
[HUAWEI] anti-attack enable
```

14.4.4 anti-attack fragment enable

Function

The **anti-attack fragment enable** command enables defense against packet fragment attacks.

The **undo anti-attack fragment enable** command disables defense against packet fragment attacks.

The **anti-attack fragment disable** command disables defense against packet fragment attacks.

By default, defense against packet fragment attacks is enabled.

Format

anti-attack fragment enable

undo anti-attack fragment enable

anti-attack fragment disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends error packet fragments to a device, the device consumes a large number of resources to process the error packet fragments, affecting normal services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack fragment enable** command to enable defense against packet fragment attacks.

The device detects error packet fragments after defense against error packet fragments is enabled. If the device detects error packet fragments, the device limits the rate of these fragments to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including packet fragments.

Example

Enable defense against packet fragment attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack fragment enable
```

14.4.5 anti-attack fragment car

Function

The **anti-attack fragment car** command sets the rate limit of packet fragments.

The **undo anti-attack fragment car** command restores the rate limit of packet fragments.

By default, the rate limit of packet fragments is 155000000 bit/s.

Format

anti-attack fragment car cir *cir*

undo anti-attack fragment car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of packet fragments.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against packet fragment attacks is enabled, run the **anti-attack fragment car** command to set the rate limit of packet fragments. If the rate of received packet fragments exceeds the rate limit, the device discards excess packet fragments to ensure that the device CPU works properly.

Prerequisites

Defense against packet fragment attacks has been enabled using the **anti-attack fragment enable** command.

Example

Set the rate limit of packet fragments to 8000 bit/s.

```
<HUAWEI> system-view
[HUAWEI] anti-attack fragment enable
[HUAWEI] anti-attack fragment car cir 8000
```

14.4.6 anti-attack icmp-flood enable

Function

The **anti-attack icmp-flood enable** command enables defense against ICMP flood attacks.

The **undo anti-attack icmp-flood enable** command disables defense against ICMP flood attacks.

The **anti-attack icmp-flood disable** command disables defense against ICMP flood attacks.

By default, defense against ICMP flood attacks is enabled.

Format

anti-attack icmp-flood enable

undo anti-attack icmp-flood enable

anti-attack icmp-flood disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of ICMP request packets to the target host in a short time, the target host is busy with these ICMP request packets. As a result, the target host is overloaded and cannot process normal services. To prevent ICMP flood attacks, run the **anti-attack icmp-flood enable** command to enable defense against ICMP flood attacks.

The device detects ICMP flood attack packets after defense against ICMP flood attacks is enabled. If the device detects ICMP flood attack packets, the device limits the rate of these ICMP flood attack packets to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including ICMP flood attack packets.

Example

Enable defense against ICMP flood attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack icmp-flood enable
```

14.4.7 anti-attack icmp-flood car

Function

The **anti-attack icmp-flood car** command sets the rate limit of ICMP flood attack packets.

The **undo anti-attack icmp-flood car** command restores the default rate limit of ICMP flood attack packets.

By default, the rate limit of ICMP flood attack packets is 155000000 bit/s.

Format

anti-attack icmp-flood car cir *cir*

undo anti-attack icmp-flood car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of ICMP flood attack packets.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against ICMP flood attacks is enabled, run the **anti-attack icmp-flood car** command to set the rate limit of ICMP flood attack packets. If the rate of received ICMP flood attack packets exceeds the rate limit, the device discards excess ICMP flood attack packets to ensure that its CPU works properly.

Prerequisites

Defense against ICMP flood attacks has been enabled using the **anti-attack icmp-flood enable** command.

Example

Set the rate limit of ICMP flood attack packets to 8000 bit/s.

```
<HUAWEI> system-view
[HUAWEI] anti-attack icmp-flood enable
[HUAWEI] anti-attack icmp-flood car cir 8000
```

14.4.8 anti-attack tcp-syn enable

Function

The **anti-attack tcp-syn enable** command enables defense against TCP SYN flood attacks.

The **undo anti-attack tcp-syn enable** command disables defense against TCP SYN flood attacks.

The **anti-attack tcp-syn disable** command disables defense against TCP SYN flood attacks.

By default, defense against TCP SYN flood attacks is enabled.

Format

anti-attack tcp-syn enable

undo anti-attack tcp-syn enable

anti-attack tcp-syn disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An attacker sends a SYN packet to a target host to initiate a TCP connection but does not respond to the SYN-ACK sent from the target host. If the target host receives no ACK packet from the attacker, it keeps waiting for the ACK packet. A half-open connection is formed. The attacker keeps sending SYN packets, so many half-open connections are set up on the target host. This wastes a large number of resources. To prevent TCP SYN flood attacks, run the **anti-attack tcp-syn enable** command to enable defense against TCP SYN flood attacks.

The device detects TCP SYN flood attack packets after defense against TCP SYN flood attacks is enabled. If the device detects TCP SYN flood attack packets, the device limits the rate of these TCP SYN flood attack packets to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including TCP SYN flood attack packets.

Example

Enable defense against TCP SYN flood attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack tcp-syn enable
```

14.4.9 anti-attack tcp-syn car

Function

The **anti-attack tcp-syn car** command sets the rate limit at which TCP SYN packets are received.

The **undo anti-attack tcp-syn car** command restores the default rate limit at which TCP SYN packets are received.

By default, the rate limit at which TCP SYN packets are received is 155000000 bit/s.

Format

anti-attack tcp-syn car cir *cir*

undo anti-attack tcp-syn car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) at which TCP SYN packets are received.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against TCP SYN flood attacks is enabled, run the **anti-attack tcp-syn car** command to set the rate limit at which TCP SYN packets are received. If the rate of received TCP SYN attack packets exceeds the rate limit, the device discards excess TCP SYN flood attack packets to ensure that the device CPU works properly.

Prerequisites

Defense against TCP SYN flood attacks has been enabled using the **anti-attack tcp-syn enable** command.

Example

Set the rate limit at which TCP SYN packets are received to 8000 bit/s.

```
<HUAWEI> system-view
[HUAWEI] anti-attack tcp-syn enable
[HUAWEI] anti-attack tcp-syn car cir 8000
```

14.4.10 anti-attack udp-flood enable

Function

The **anti-attack udp-flood enable** command enables defense against UDP flood attacks.

The **undo anti-attack udp-flood enable** command disables defense against UDP flood attacks.

The **anti-attack udp-flood disable** command disables defense against UDP flood attacks.

By default, defense against UDP flood attacks is enabled.

Format

anti-attack udp-flood enable

undo anti-attack udp-flood enable

anti-attack udp-flood disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of UDP packets to the target host in a short time, the target host is busy with these UDP packets. As a result, the target host is overloaded and cannot process normal services. To prevent UDP flood attacks, run the **anti-attack udp-flood enable** command to enable defense against UDP flood attacks.

The device detects UDP flood attack packets after defense against UDP flood attacks is enabled. The device directly discards UDP flood attack packets.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including UDP flood attack packets.

Example

Enable defense against UDP flood attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack udp-flood enable
```

14.4.11 display anti-attack statistics

Function

The **display anti-attack statistics** command displays statistics about attack packets of a specified type.

If no parameter is specified, the **display anti-attack statistics** command displays statistics about attack packets of all types.

Format

display anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**]

Parameters

Parameter	Description	Value
abnormal	Displays statistics about malformed packets.	-
fragment	Displays statistics about defense against packet fragments.	-
tcp-syn	Displays statistics about defense against TCP SYN flood attacks.	-
udp-flood	Displays statistics about defense against UDP flood attacks.	-
icmp-flood	Displays statistics about defense against ICMP flood attacks.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display anti-attack statistics** command displays statistics on attack packets of the following types: malformed packet attack, packet fragment attack, TCP SYN flood attack, UDP flood attack, ICMP flood attack.

Example

Display attack defense statistics.

```
<HUAWEI> display anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum        DropPacketNum         PassPacketNum
        (H)        (L)        (H)        (L)        (H)        (L)
-------------------------------------------------------------------------------
URPF         0          0          0          0          0          0
Abnormal     0          0          0          0          0          0
Fragment     0          0          0          0          0          0
Tcp-syn      0          58         0          0          0          58
Udp-flood    0          0          0          0          0          0
Icmp-flood   0          0          0          0          0          0
-------------------------------------------------------------------------------
```

Table 14-41 Description of the display anti-attack statistics command output

Item	Description
Packets Statistic Information	Attack defense statistics.
AntiAtkType	Attack defense type: - URPF: URPF check (The device does not support this parameter.) - Abnormal: defense against malformed packets - Fragment: defense against packet fragments - Tcp-syn: defense against TCP SYN flood attacks - Udp-flood: defense against UDP flood attacks - Icmp-flood: defense against ICMP flood attacks
TotalPacketNum	Total number of packets.
DropPacketNum	Number of discarded packets.

Item	Description
PassPacketNum	Number of forwarded packets.
(H)	Highest-order bit display.
(L)	Lowest-order bit display.

14.4.12 reset anti-attack statistics

Function

The **reset anti-attack statistics** command clears attack defense statistics.

Format

reset anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**]

Parameters

Parameter	Description	Value
abnormal	Clears statistics about defense against malformed packets.	-
fragment	Clears statistics about defense against packet fragments.	-
tcp-syn	Clears statistics about defense against TCP SYN flood attacks.	-
udp-flood	Clears statistics about defense against UDP flood attacks.	-
icmp-flood	Clears statistics about defense against ICMP flood attacks.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If no attack defense is specified, statistics about all types of attack defense are cleared.

NOTICE

The cleared statistics cannot be restored. Exercise caution when you use the command.

Example

Clear statistics about defense against malformed packets.

```
<HUAWEI> reset anti-attack statistics abnormal
```

14.5 Traffic Suppression and Storm Control Configuration Commands

14.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.5.2 broadcast-suppression (interface view)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface in the inbound direction.

The **undo broadcast-suppression** command restores the default maximum traffic rate of broadcast packets that can pass through an interface in the inbound direction.

By default, the rate of broadcast packets is suppressed by bandwidth percentage, and the percentage rate limit is 10%.

Format

broadcast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }

undo broadcast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer and the value range is as follows: ● 40GE interface: 0 to 100 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S ● Other interfaces: 0 to 100

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 0 to 100000 ● GE interface: 0 or 16 to 1000000 for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, 0 to 1000000 for the others ● XGE interface: 0 or 16 to 10000000 for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, 0 to 10000000 for the others ● 25GE interface: 0 to 25000000 ● MultiGE interface: 0 to X, X indicates the negotiated bandwidth ● 40GE interface: 0 to 40000000 ● 100GE interface: 0 to 100000000 ● Port group: 0 to 100000000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer. For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: The value ranges from 10000 to 65535, in bytes. For other models: The value ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: - Ethernet interface: 0 to 148810 - GE interface: 0 to 1488100 - XGE interface: 0 to 14881000 - MultiGE interface: 0 to X. X indicates the negotiated bandwidth - 25GE interface: 0 to 37202500 - 40GE interface: 0 to 59524000 - 100GE interface: 0 to 148810000 - Port group: 0 to 148810000 **NOTE** - For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the configured value is less than 24, traffic suppression is performed based on 24. If the configured value is greater than or equal to 24, traffic suppression is performed based on the configured value. - When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, 100GE interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, port group view, Eth-Trunk member interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **broadcast-suppression** command to set the threshold of broadcast traffic that an interface allows to pass through. When the broadcast traffic rate reaches the rate limit, the system discards excess broadcast packets to control the traffic rate in a proper range.

Precautions

If the rate limit in bit/s is set for a type of packets on an interface, the rate limit in pps cannot be set for other types of packets on the same interface. In a similar manner, if the rate limit in pps is set for a type of packets on an interface, the rate limit in bit/s cannot be set for other types of packets on the same interface.

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

Set the broadcast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] broadcast-suppression packets 100000
```

14.5.3 broadcast-suppression block outbound

Function

The **broadcast-suppression block outbound** command blocks outgoing broadcast packets on an interface.

The **undo broadcast-suppression block outbound** command unblocks outgoing broadcast packets on an interface.

By default, an interface does not block outgoing broadcast packets.

Format

broadcast-suppression block outbound

undo broadcast-suppression block outbound

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

After an interface receives a broadcast packet, it broadcasts the packet to all users in the same VLAN. This may cause information leak. For example, if an unauthorized user is connected to an interface in a VLAN, an unauthorized user obtains a host's address from broadcast packets and uses the address to attack the host. To prevent information leak, use the **broadcast-suppression block outbound** command to block outgoing broadcast packets on an interface if users connected to the interface do not need to receive broadcast packets. For example, if users on an interface seldom change and require high security, you can use this command on the interface.

Precautions

The **broadcast-suppression block outbound** command is applicable only to interfaces on which users do not need to receive broadcast packets. This command will affect network operations if it is used on an interface where users need to receive broadcast packets.

Traffic suppression can be configured for incoming and outgoing packets on an interface, and the configurations are independent of each other. On an interface, you can use the **broadcast-suppression** command to limit the rate of incoming broadcast packets and use the **broadcast-suppression block outbound** command to block outgoing broadcast packets.

Example

Block outgoing broadcast packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] broadcast-suppression block outbound
```

14.5.4 broadcast-suppression (VLAN view)

Function

The **broadcast-suppression** command sets the rate limit for broadcast packets in a VLAN.

The **undo broadcast-suppression** command cancels broadcast packets suppression in a VLAN.

By default, broadcast packets are not suppressed in a VLAN.

Format

broadcast-suppression *threshold-value*

undo broadcast-suppression

Parameters

Parameter	Description	Value
threshold-value	Specifies the rate limit of broadcast packets.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

After you run the **broadcast-suppression** command, the device limits the rate of broadcast packets based on the configured rate limit. If the rate limit is exceeded, the device discards excess broadcast packets.

Example

Set the rate limit to 1000 kbit/s for broadcast packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] broadcast-suppression 1000
```

14.5.5 display flow-suppression interface

Function

The **display flow-suppression interface** command displays the traffic suppression configuration on an interface.

Format

display flow-suppression interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display the traffic suppression for broadcast, unknown multicast, known multicast, unknown unicast, and known unicast packets on the interface, including rate limiting mode and rate limit value.

Example

Display the traffic suppression configuration on GE0/0/1.

```
<HUAWEI> display flow-suppression interface gigabitethernet 0/0/1
 storm type         rate mode   set rate value
-------------------------------------------------------------------------------
 unknown-unicast    percent      percent: 90%
 multicast          percent      percent: 90%
 broadcast          percent      percent: 90%
 known-unicast      percent      percent: 100%
 known-multicast    percent      percent: 100%
-------------------------------------------------------------------------------
```

Table 14-42 Description of the display flow-suppression interface command output

Item	Description
storm type	Traffic type: - unknown-unicast: unknown unicast traffic - multicast: unknown multicast traffic - broadcast: broadcast traffic - known-unicast: known-unicast traffic - known-multicast: known-multicast traffic
rate mode	Type of the rate limit. - pps: packet mode - percent: percentage mode
set rate value	Configured rate limit. The rate can be set by the following commands: - **broadcast-suppression** - **multicast-suppression** - **unicast-suppression** - **known-unicast-suppression** - **known-multicast-suppression**

14.5.6 display storm-control

Function

The **display storm-control** command displays information about storm control on an interface.

Format

display storm-control [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. - *interface-type* specifies the type of the interface. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display the storm control for broadcast, unknown multicast, and unknown unicast packets on the interface, such as packet mode, storm control action, and packet status.

Example

Display information about storm control on GE0/0/1.

```
<HUAWEI> display storm-control interface gigabitethernet 0/0/1
PortName     Type      Rate      Mode Action   Punish-  Trap Log Int Last-
                    (Min/Max)            Status             Punish-Time
-----------------------------------------------------------------------------
GE0/0/1      Multicast 1000      Pps  Block    Normal   Off  On  90  -
                    /2000
GE0/0/1      Broadcast 1000      Pps  Block    Normal   Off  On  90  -
                    /2000
GE0/0/1      Unicast   1000      Pps  Block    Normal   Off  On  90  -
                    /2000
```

Table 14-43 Description of the display storm-control command output

Item	Description
PortName	Interface name.
Type	Packet type. ● Broadcast packets ● Unknown Multicast packets ● Unknown Unicast packets To configure the type of packets on which storm control is performed, run the **storm-control** command.
Rate	● Min: lower rate threshold ● Max: upper rate threshold To configure the rates, run the **storm-control** command.

Item	Description
Mode	Storm control mode. - Kbps: CIR in kbit/s - Pps: packets in pps - %: percentage in % To configure the storm control mode, run the **storm-control** command.
Action	Storm control action. - Block: blocks packets. - Err-down: shuts down the interface. - None: No action is configured. To configure a storm control action, run the **storm-control action** command.
Punish-Status	Status of the interface. - Block: When the rate of receiving packets is greater than the value of **MaxRate** and the storm control action is **block**, the status of the interface is **block**. - Normal: Packets are normally forwarded. - Err-down: When the rate of receiving packets is greater than the value of **MaxRate** and the storm control action is **error-down**, the status of the interface is **error-down**.
Trap	Whether the alarm function for storm control is enabled. - on: The alarm function for storm control is enabled. - off: The alarm function for storm control is disabled. To configure the alarm function for storm control, run the **storm-control enable trap** command.
Log	Whether the log function for storm control is enabled. - on: The log function for storm control is enabled. - off: The log function for storm control is disabled. To configure the alarm function for storm control, run the **storm-control enable log** command.
Int	Interval for detecting storms, in seconds. The default value is 5.
Last-Punish-Time	Last time storm control is performed.

14.5.7 icmp rate-limit

Function

The **icmp rate-limit** command sets the rate threshold of ICMP packets.

The **undo icmp rate-limit** command restores the default rate threshold of ICMP packets.

By default, the rate limits of ICMP packets in the system and on an interface depend on the product model. The value is 128 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and 190 on the other models, in pps.

Format

icmp rate-limit { **total** | **interface** *interface-type interface-number1* [**to** *interface-number2*] } **threshold** *threshold-value*

undo icmp rate-limit { **total** | **interface** *interface-type interface-number1* [**to** *interface-number2*] }

Parameters

Parameter	Description	Value
total	Specifies the total rate threshold in the system.	-
interface *interface-type interface-number1* **to** *interface-number2*	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • **to** *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces.	-

Parameter	Description	Value
threshold *threshold-value*	Specifies the rate threshold of ICMP packets.	The value ranges from 0 to 1000, in pps. **NOTE** The value 0 indicates that the rate of ICMP packets is not limited.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

A network often undergoes ICMP packet attacks. If a switch receives a large number of broadcast ICMP request packets on user-side interfaces, these packets are sent to the switch CPU for processing. Then the CPU usage becomes high, affecting other services on the switch. You can use the **icmp rate-limit** command to prevent the switch from being attacked by ICMP packets.

After the rate limit function is configured for ICMP packets on an interface, the system automatically discards excess ICMP packets when the number of ICMP packets sent by an interface every second exceeds the rate threshold.

Precautions

Before setting the rate threshold of ICMP packets, use the **icmp rate-limit enable** command to enable the rate limit function for ICMP packets.

Example

Set the rate threshold of ICMP packets on GE0/0/1 to GE0/0/5 to 20 pps.

```
<HUAWEI> system-view
[HUAWEI] icmp rate-limit interface gigabitethernet 0/0/1 to 0/0/5 threshold 20
```

14.5.8 icmp rate-limit enable

Function

The **icmp rate-limit enable** command enables the traffic suppression function for ICMP packets.

The **undo icmp rate-limit enable** command disables the traffic suppression function for ICMP packets.

By default, the traffic suppression function for ICMP packets is disabled.

Format

icmp rate-limit enable

undo icmp rate-limit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Attackers may send a large number of ICMP packets to attack a network. If the device sends all the received ICMP packets to the CPU for processing, a lot of CPU usage resources are occupied and other services may be abnormal. To prevent ICMP packet attacks, you can configure the device to suppress ICMP packets.

Before configuring traffic suppression for ICMP packets on an interface, run the **undo icmp-reply fast** command to disable the ICMP reply fast function.

Example

Enable the traffic suppression function for ICMP packets.

```
<HUAWEI> system-view
[HUAWEI] icmp rate-limit enable
```

14.5.9 known-multicast-suppression

Function

The **known-multicast-suppression** command sets the maximum traffic volume of known multicast packets that can pass through an interface.

The **undo known-multicast-suppression** allows all known multicast packets to pass.

By default, known multicast packets are not suppressed.

NOTE

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S do not support this command.

Format

known-multicast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }

undo known-multicast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer and the value range is as follows: - 40GE interface: 0 to 100 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S - Other interfaces: 0 to 100

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 0 to 100000 ● GE interface: 0 to 1000000 ● XGE interface: 0 to 10000000 ● 25GE interface: 0 to 25000000 ● MultiGE interface: 0 to X, X indicates the negotiated bandwidth ● 40GE interface: 0 to 40000000 ● 100GE interface: 0 to 100000000 ● Port group: 0 to 100000000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● XGE interface: 0 to 14881000 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● 25GE interface: 0 to 37202500 ● 40GE interface: 0 to 59524000 ● 100GE interface: 0 to 148810000 ● Port group: 0 to 148810000 **NOTE** ● For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the configured value is less than 24, traffic suppression is performed based on 24. If the configured value is greater than or equal to 24, traffic suppression is performed based on the configured value. ● When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, 100GE interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **known-multicast-suppression** command to set the threshold of known multicast traffic that an interface allows to pass through. When the known multicast traffic volume exceeds the threshold, the system discards the excess known multicast packets to control the traffic volume of known multicast packets to a proper range.

Precautions

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

known Set the maximum known multicast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] known-multicast-suppression packets 100000
```

14.5.10 known-unicast-suppression

Function

The **known-unicast-suppression** command sets the maximum traffic volume of known unicast packets that can pass through an interface.

The **undo known-unicast-suppression** allows all known unicast packets to pass.

By default, known unicast packets are not suppressed.

NOTE

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S do not support this command.

Format

known-unicast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }

undo known-unicast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer and the value range is as follows: • 40GE interface: 0 to 100 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S • Other interfaces: 0 to 100

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer, in kbit/s. The value range is as follows: - Ethernet interface: 0 to 100000 - GE interface: 0 to 1000000 - XGE interface: 0 to 10000000 - 25GE interface: 0 to 25000000 - MultiGE interface: 0 to X, X indicates the negotiated bandwidth - 40GE interface: 0 to 40000000 - 100GE interface: 0 to 100000000 - Port group: 0 to 100000000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● XGE interface: 0 to 14881000 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● 25GE interface: 0 to 37202500 ● 40GE interface: 0 to 59524000 ● 100GE interface: 0 to 148810000 ● Port group: 0 to 148810000 **NOTE** ● For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the configured value is less than 24, traffic suppression is performed based on 24. If the configured value is greater than or equal to 24, traffic suppression is performed based on the configured value. ● When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, 100GE interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **known-unicast-suppression** command to set the threshold of known multicast traffic that an interface allows to pass through. When the known unicast traffic rate exceeds the rate limit, the system discards excess known unicast packets to control the traffic volume in a proper range.

Precautions

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

#Set the maximum known unicast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] known-unicast-suppression packets 100000
```

14.5.11 multicast-suppression (interface view)

Function

The **multicast-suppression** command sets the maximum traffic volume of unknown multicast packets that can pass through an interface.

The **undo multicast-suppression** allows all unknown multicast packets to pass.

By default, unknown multicast packets are not suppressed.

Format

multicast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }

undo multicast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer and the value range is as follows: ● 40GE interface: 0 to 100 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S ● Other interfaces: 0 to 100

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 0 to 100000 ● GE interface: 0 or 16 to 1000000 for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, 0 to 1000000 for the others ● XGE interface: 0 or 16 to 10000000 for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, 0 to 10000000 for the others ● 25GE interface: 0 to 25000000 ● MultiGE interface: 0 to X, X indicates the negotiated bandwidth ● 40GE interface: 0 to 40000000 ● 100GE interface: 0 to 100000000 ● Port group: 0 to 100000000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer. For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: The value ranges from 10000 to 65535, in bytes. For other models: The value ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● XGE interface: 0 to 14881000 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● 25GE interface: 0 to 37202500 ● 40GE interface: 0 to 59524000 ● 100GE interface: 0 to 148810000 ● Port group: 0 to 148810000 **NOTE** ● For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the configured value is less than 24, traffic suppression is performed based on 24. If the configured value is greater than or equal to 24, traffic suppression is performed based on the configured value. ● When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, 100GE interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, port group view, Eth-Trunk member interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an increasing number of unknown multicast packets are transmitted on a network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **multicast-suppression** command to set the threshold of unknown multicast traffic that an interface allows to pass through. When the unknown multicast traffic volume exceeds the threshold, the system discards the excess unknown multicast packets to control the traffic volume of unknown multicast packets to a proper range.

Precautions

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

For S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, unknown multicast traffic suppression does not take effect on unknown multicast packets with the reserved addresses (224.0.0.x/24, 224.0.1.x/24, 239.x.x.x/8, and ff0x::/12).

Example

Set the maximum unknown multicast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-suppression packets 100000
```

14.5.12 multicast-suppression block outbound

Function

The **multicast-suppression block outbound** command configures an interface to block outgoing unknown multicast packets.

The **undo multicast-suppression block outbound** command cancels the configuration.

By default, outgoing unknown multicast packets are not blocked on an interface.

Format

multicast-suppression block outbound

undo multicast-suppression block outbound

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface receives an unknown multicast packet, the interface broadcasts the packet to all users in the same VLAN. This may cause information leak. For example, if an unauthorized user is connected to an interface in a VLAN, the unauthorized user obtains the host address in unknown multicast packets by listening to unknown multicast packets and uses the host address to attack the host. To prevent information leak, use the **multicast-suppression block outbound** command to block outgoing unknown multicast packets on an interface if users connected to the interface do not need to receive unknown multicast packets.

Precautions

The **multicast-suppression block outbound** command is applicable only to interfaces where users do not need to receive unknown multicast packets. This command will affect network operations if it is used on an interface where users need to receive unknown multicast packets.

Traffic suppression can be configured for incoming and outgoing packets on an interface, and the configurations are independent of each other. On an interface, you can use the **multicast-suppression** command to limit the rate of incoming unknown multicast packets and use the **multicast-suppression block outbound** command to block outgoing unknown multicast packets.

Example

Block outgoing unknown multicast packets onGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-suppression block outbound
```

14.5.13 storm-control

Function

The **storm-control** command enables storm control for broadcast packets, unknown multicast packets, and unknown unicast packets on an interface.

The **undo storm-control** command disables storm control.

By default, storm control is disabled on interfaces.

Format

storm-control { **broadcast** | **multicast** | **unicast** } **min-rate** *min-rate-value* **max-rate** *max-rate-value*

storm-control { **broadcast** | **multicast** | **unicast** } **min-rate cir** *min-rate-value-cir* **max-rate cir** *max-rate-value-cir* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

storm-control { **broadcast** | **multicast** | **unicast** } **min-rate percent** *min-rate-value-percent* **max-rate percent** *max-rate-value-percent* (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

undo storm-control { **broadcast** | **multicast** | **unicast** | **all-packets** }

Parameters

Parameter	Description	Value
broadcast	Enables storm control for broadcast packets.	-
multicast	Enables storm control for unknown multicast packets.	-
unicast	Enables storm control for unknown unicast packets.	-

Parameter	Description	Value
min-rate *min-rate-value*	Specifies the lower threshold in packet rate limit mode. If the value of *min-rate-value* is specified, packets received by an interface are forwarded when the rate of receiving packets is smaller than the value of *min-rate-value* in storm detection.	The value is an integer, in pps. The value range is as follows: ● Ethernet interface: 1 to 148810 ● GE interface: 1 to 1488100 ● MultiGE interface: 1 to X. X indicates the negotiated bandwidth ● XGE interface: 1 to 14881000 ● 25GE interface: 1 to 14881000 ● 40GE interface: 1 to 59524000 ● 100GE interface: 1 to 148810000 ● Port group: 1 to 148810000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group. The actual value range depends on the auto-negotiated rates.

Parameter	Description	Value
min-rate cir *min-rate-value-cir*	Specifies the lower threshold in byte rate limit mode. If the value of *min-rate-value-cir* is specified, packets received by an interface are forwarded when the rate of receiving packets is smaller than the value of *min-rate-value-cir* in storm detection.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 1 to 100000 ● GE interface: 1 to 1000000 ● XGE interface: 1 to 10000000 ● 25GE interface: 1 to 14881000 ● 40GE interface: 1 to 40000000 ● 100GE interface: 1 to 100000000 ● Port group: 1 to 100000000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group. The actual value range depends on the auto-negotiated rates.
min-rate percent *min-rate-value-percent*	Specifies the lower threshold in percentage rate limit mode. If the value of *min-rate-value-percent* is specified, packets received by an interface are forwarded when the rate of receiving packets is lower than the value of *min-rate-value-percent* in storm detection.	The value is an integer, in percentage. The value ranges from 1 to 100.

Parameter	Description	Value
max-rate *max-rate-value*	Specifies the upper threshold in packet rate limit mode. Storm control is performed on an interface when the rate of receiving packets on the interface is greater than the value of *max-rate-value* in storm detection.	The value is an integer, in pps. The value range is as follows: - Ethernet interface: 1 to 148810 - GE interface: 1 to 1488100 - MultiGE interface: 1 to X. X indicates the negotiated bandwidth - XGE interface: 1 to 14881000 - 25GE interface: 1 to 14881000 - 40GE interface: 1 to 59524000 - 100GE interface: 1 to 148810000 - Port group: 1 to 148810000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group. The actual value range depends on the auto-negotiated rates.

Parameter	Description	Value
max-rate cir *max-rate-value-cir*	Specifies the upper threshold in byte rate limit mode. If the value of *max-rate-value-cir* is specified, storm control is performed on an interface when the rate of receiving packets on the interface is greater than the value of *max-rate-value-cir* in storm detection.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 1 to 100000 ● GE interface: 1 to 1000000 ● XGE interface: 1 to 10000000 ● 25GE interface: 1 to 14881000 ● 40GE interface: 1 to 40000000 ● 100GE interface: 1 to 100000000 ● Port group: 1 to 100000000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group. The actual value range depends on the auto-negotiated rates.
max-rate percent *max-rate-value-percent*	Specifies the upper threshold in percentage rate limit mode. If the value of *max-rate-value-percent* is specified, storm control is performed on an interface when the rate of receiving packets on the interface is greater than the value of *max-rate-value-percent* in storm detection.	The value is an integer, in percentage. The value ranges from 1 to 100.

Parameter	Description	Value
all-packets	Disables storm control for all the broadcast packets, unknown multicast packets, and unknown unicast packets.	-

Views

Ethernet interface view, 40GE interface view, 100GE interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the average rate of receiving packets on an interface is greater than the value of *max-rate-value*, *max-rate-value-cir*, or *max-rate-value-percent* in storm detection, storm control is performed on the packets.

NOTE

The storm detection interval can be set using the **storm-control interval** command.

Storm control actions include **block** and **shutdown**, which can be configured using the **storm-control action** command. If the action is **block** on an interface, packets on the interface are unblocked when the rate of receiving packets on the interface is smaller than the value of *min-rate-value*, *min-rate-value-cir* or *min-rate-value-percent*; if the action is **shutdown** on an interface, run the **undo shutdown** command to enable the interface.

Precautions

For S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, when detecting unicast packets, a switch does not distinguish unknown unicast packets from known unicast packets. The packet rate detected is the sum of the rates of unknown and known unicast packets. When the storm control action is block, the switch blocks only the unknown unicast packets. This rule also applies to multicast packets.

You cannot configure storm control and traffic suppression simultaneously on an interface. For example, if you configure traffic suppression for unknown multicast packets, unknown unicast packets, or broadcast packets (including 100% traffic suppression for broadcast packets) on an interface, then you cannot configure storm control for broadcast packets simultaneously on the interface.

After storm control is configured on an interface, the device does not check the VLAN IDs of packets when performing check on the packets. That is, the device performs storm control on all the packets no matter whether the VLANs of the packets are allowed by the interface.

Example

Perform storm control on broadcast packets received on GE0/0/1. In the storm detection interval, perform storm control on packets when the rate of receiving packets on an interface is greater than 8000 pps and forward packets when the rate of receiving packets on an interface is smaller than 5000 pps.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control broadcast min-rate 5000 max-rate 8000
```

14.5.14 storm-control action

Function

The **storm-control action** sets the storm control action to **error-down** or **block**.

The **undo storm-control action** command cancels the configuration.

By default, no storm control action is configured.

Format

storm-control action { **block** | **error-down** }

undo storm-control action

NOTE

The following models do not support the **error-down** parameter:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S

Parameters

Parameter	Description	Value
block	Blocks packets.	-
error-down	Shuts down an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

You can control data packets and prevent flooding by running the **storm-control action** command to configure a storm control action and the **storm-control** command to set the upper and lower thresholds.

In a storm detection interval, when the average rate of receiving broadcast packets, unknown multicast packets, and unknown unicast packets is greater than the value of the specified upper threshold, packets are blocked or the interface is shut down.

If the storm control action on an interface is **block**, the interface is restored when the traffic falls below the lower threshold.

If the storm control action is **error-down**, the interface can be recovered using either of the following methods:

- Manual recovery (after an Error-Down event occurs):

  If a few interfaces need to be recovered, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.
- Automatic recovery (before an Error-Down event occurs):

  If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. To avoid this problem, run the **error-down auto-recovery cause storm-control interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. Run the **display error-down recovery** command to view information about automatic interface recovery.

  NOTE

  This method does not take effect on interfaces that are already in Error-Down state. It is effective only on interfaces that enter the Error-Down state after this configuration is complete.

Precautions

For S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, when detecting unicast packets, a switch does not distinguish unknown unicast packets from known unicast packets. The packet rate detected is the sum of the rates of unknown and known unicast packets. When the storm control action is block, the switch blocks only the unknown unicast packets. This rule also applies to multicast packets.

Example

Configure the storm control action is **block** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control action block
```

14.5.15 storm-control enable

Function

The **storm-control enable** command configures the system to record logs or report traps during storm control.

The **undo storm-control enable** command configures the system not to record logs or report traps during storm control.

By default, the system does not record logs or report traps.

Format

storm-control enable { **log** | **trap** }

undo storm-control enable { **log** | **trap** }

Parameters

Parameter	Description	Value
log	Enables the log function.	-
trap	Enables the trap function.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After storm control is configured, the switch monitors the broadcast, unknown multicast, and unknown unicast packets received on an interface. When the packet rate within a detection interval exceeds the upper limit, the switch executes the storm control action (block packets or shut down the interface) on the interface. This may affect services. You can configure the log or trap for storm control so that the administrator can quickly take actions to protect the switch.

- After the logging function is enabled for storm control, the storm control log information is recorded in the **STORMCTRL** log of the SECE module.
- After the trap function is enabled for storm control, the trap is SECE_1.3.6.1.4.1.2011.5.25.32.4.1.14.1 hwXQoSStormControlTrap.

Example

Enable the trap reporting function during storm control on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control broadcast min-rate 3000 max-rate 5000
[HUAWEI-GigabitEthernet0/0/1] storm-control action block
[HUAWEI-GigabitEthernet0/0/1] storm-control enable trap
```

14.5.16 storm-control interval

Function

The **storm-control interval** command sets the storm detection interval.

The **undo storm-control interval** command restores the default storm detection interval.

By default, the storm detection interval is 5s.

Format

storm-control interval *interval-value*

undo storm-control interval

Parameters

Parameter	Description	Value
interval-value	Specifies the storm detection interval.	The value is an integer that ranges from 1 to 180, in seconds. The default value is 5s.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Before using the **storm-control interval** command to set the storm detection interval, run the **storm-control** command in the interface view to configure storm control. Otherwise, the storm detection interval does not take effect.

Example

Configure storm control and set the storm detection interval to 10 seconds on GE0/0/1. Block broadcast packets when the rate of receiving broadcast packets is greater than 5000 pps and forward the packets when the rate of receiving broadcast packets is smaller than 3000 pps in 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control broadcast min-rate 3000 max-rate 5000
[HUAWEI-GigabitEthernet0/0/1] storm-control action block
[HUAWEI-GigabitEthernet0/0/1] storm-control interval 10
```

14.5.17 storm-control whitelist protocol

Function

The **storm-control whitelist protocol** command adds specified protocol packets to the traffic suppression and storm control whitelist.

The **undo storm-control whitelist protocol** command deletes specified protocol packets from the traffic suppression and storm control whitelist.

By default, no protocol packet is not added to the traffic suppression and storm control whitelist.

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S.

Format

storm-control whitelist protocol { **arp-request** | **bpdu** | **dhcp** | **igmp** | **rip** }*

undo storm-control whitelist protocol { **arp-request** | **bpdu** | **dhcp** | **igmp** | **rip** }*

Parameters

Parameter	Description	Value
arp-request	Adds ARP packets to the traffic suppression and storm control whitelist.	-
bpdu	Adds BPDU packets to the traffic suppression and storm control whitelist.	-
dhcp	Adds DHCP packets to the traffic suppression and storm control whitelist.	-
igmp	Adds IGMP packets to the traffic suppression and storm control whitelist.	-
rip	Adds RIP packets to the traffic suppression and storm control whitelist.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To free specified protocol packets from traffic suppression and storm control, you can run the **storm-control whitelist protocol** command to add these packets to the traffic suppression and storm control whitelist.

Precautions

- The **storm-control whitelist protocol** command configuration takes effect only on protocol packets in the inbound direction of an interface. It does not take effect on the packets that are blocked in the outbound direction of an interface using the **broadcast-suppression block outbound**, **multicast-suppression block outbound**, and **unicast-suppression block outbound**.
- The **storm-control whitelist protocol** command configuration does not take effect on broadcast packets that are suppressed using the **broadcast-suppression** command in the VLAN view.
- After the **qos lr inbound whitelist protocol** command is run to add specified protocol packets to the whitelist for inbound interface-based rate limiting, traffic suppression and storm control do not take effect on these protocol packets in the inbound direction of the corresponding interface.

Example

Add BPDU packets to the traffic suppression and storm control whitelist.

```
<HUAWEI> system-view
[HUAWEI] storm-control whitelist protocol bpdu
```

14.5.18 suppression mode

Function

The **suppression mode** command sets the global traffic suppression mode.

The **undo suppression mode** command restores the default traffic suppression mode.

By default, the global traffic suppression mode is **packets**.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S support this command.

Format

suppression mode { **by-packets** | **by-bits** }

undo suppression mode

Parameters

Parameter	Description	Value
by-packets	Sets the traffic suppression mode to **packets**.	-
by-bits	Sets the traffic suppression mode to **bits**.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default traffic suppression mode on an interface is **packets**. To precisely control traffic rate, run the **suppression mode** command in the system view to set the traffic suppression mode to **bits**.

Precautions

If the **packets** mode has been set on an interface and the **bits** mode is set in the system view, the device automatically converts the traffic rate values and suppresses traffic based on **bits**. For example, if the maximum rate of broadcast packets allowed by a GE interface is set to 1000 pps, the device converts the traffic rate value as follows: 1000 x 84 x 8 = 672000 bits = 672 Kbit. In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

If the traffic suppression mode set in the system view is **packets**, the **cir** parameter cannot be specified when you set the maximum traffic rate on an interface.

If the traffic suppression mode set in the system view is **bits**, the **packets** parameter cannot be specified when you set the maximum traffic rate on an interface.

Example

Set the traffic suppression mode to **by-bits**.

```
<HUAWEI> system-view
[HUAWEI] suppression mode by-bits
Warning: All Interface supression mode will be changed. Continue? [Y/N]:y
```

14.5.19 unicast-suppression (interface view)

Function

The **unicast-suppression** command sets the maximum traffic volume of unknown unicast packets that can pass through an interface.

The **undo unicast-suppression** allows all unknown unicast packets to pass.

By default, unknown unicast packets are not suppressed.

Format

unicast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }

undo unicast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer and the value range is as follows: • 40GE interface: 0 to 100 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S • Other interfaces: 0 to 100

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer, in kbit/s. The value range is as follows: - Ethernet interface: 0 to 100000 - GE interface: 0 or 16 to 1000000 for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, 0 to 1000000 for the others - XGE interface: 0 or 16 to 10000000 for the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, 0 to 10000000 for the others - 25GE interface: 0 to 25000000 - MultiGE interface: 0 to X, X indicates the negotiated bandwidth - 40GE interface: 0 to 40000000 - 100GE interface: 0 to 100000000 - Port group: 0 to 100000000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer. For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: The value ranges from 10000 to 65535, in bytes. For other models: The value ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● XGE interface: 0 to 14881000 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● 25GE interface: 0 to 37202500 ● 40GE interface: 0 to 59524000 ● 100GE interface: 0 to 148810000 ● Port group: 0 to 148810000 **NOTE** ● For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the configured value is less than 24, traffic suppression is performed based on 24. If the configured value is greater than or equal to 24, traffic suppression is performed based on the configured value. ● When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, 100GE interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, port group view, Eth-Trunk member interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an increasing number of unknown unicast packets are transmitted on the network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **unicast-suppression** command to set the threshold of unicast traffic that an interface allows to pass through. When the unknown unicast traffic rate exceeds the rate limit, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Precautions

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

#Set the maximum unknown unicast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] unicast-suppression packets 100000
```

14.5.20 unicast-suppression block outbound

Function

The **unicast-suppression block outbound** command configures an interface to block outgoing unknown unicast packets.

The **undo unicast-suppression block outbound** command cancels the configuration.

By default, an interface does not block outgoing unknown unicast packets.

Format

unicast-suppression block outbound

undo unicast-suppression block outbound

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface receives an unknown unicast packet, the interface broadcasts the packet to all users in the same VLAN. This may cause information leak. For example, if an unauthorized user is connected to an interface in a VLAN, the unauthorized user obtains a host's address from unknown unicast packets and uses the address to attack the host. To prevent information leak, use the **unicast-suppression block outbound** command to block unknown unicast packets on an interface if users connected to the interface do not need to receive broadcast packets. For example, if users on an interface seldom change and require high security, you can use this command on the interface.

Precautions

The **unicast-suppression block outbound** command is applicable only to interfaces where users do not need to receive unknown unicast packets. This command will affect network operations if it is used on an interface where users need to receive unknown packets.

Traffic suppression can be configured for incoming and outgoing packets on an interface, and the configurations are independent of each other. On an interface, use the **unicast-suppression** command to limit the rate of incoming unknown unicast packets and the **unicast-suppression block outbound** command to block outgoing unknown unicast packets.

Example

Block outgoing multicast packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] unicast-suppression block outbound
```

14.6 ARP Security Configuration Commands

14.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.6.2 arp anti-attack check user-bind alarm enable

Function

The **arp anti-attack check user-bind alarm enable** command enables the alarm function for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm enable** command disables the alarm function for ARP packets discarded by DAI.

By default, the alarm function for ARP packets discarded by DAI is disabled.

Format

arp anti-attack check user-bind alarm enable

undo arp anti-attack check user-bind alarm enable

Parameters

None

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, VLAN view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DAI is enabled, if you want to receive an alarm when a large number of ARP packets are discarded by DAI, you can run the **arp anti-attack check user-bind alarm enable** command. After the alarm function is enabled, the device sends an alarm when the number of discarded ARP packets exceeds the threshold.

Prerequisites

DAI has been enabled using the **arp anti-attack check user-bind enable** command in the corresponding view.

Follow-up Procedure

The alarm threshold is set by the **arp anti-attack check user-bind alarm threshold** command.

Precautions

If you run this command in multiple views, the configuration will take effect in the following sequence: BD view > interface view > VLAN view.

Example

Enable the alarm function for ARP packets discarded by DAI on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
```

14.6.3 arp anti-attack check user-bind alarm threshold

Function

The **arp anti-attack check user-bind alarm threshold** command sets the alarm threshold for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm threshold** command restores the default alarm threshold for ARP packets discarded by DAI.

By default, the alarm threshold for ARP packets discarded by DAI is 100 packets.

Format

arp anti-attack check user-bind alarm threshold *threshold*

undo arp anti-attack check user-bind alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the ARP packets discarded by DAI.	The value is an integer that ranges from 1 to 1000.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, VLAN view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to set the alarm threshold for ARP packets discarded by DAI. After the alarm threshold is set, the device sends an alarm when the number of ARP packets discarded by DAI exceeds this threshold.

Prerequisites

DAI has been enabled using the **arp anti-attack check user-bind enable** command in the corresponding view, and the alarm function for ARP packets discarded by DAI has been enabled using the **arp anti-attack check user-bind alarm enable** command in the corresponding view.

Precautions

The **arp anti-attack check user-bind alarm threshold** command takes effect in the system view only when DAI and the alarm function for ARP packets discarded by DAI are enabled in the interface, BD, or VLAN view. The global alarm threshold takes effect on all interfaces, BDs, or VLANs enabled with the two functions.

The priority configured in the interface, BD, or VLAN view is higher than that configured globally. If the alarm threshold on an interface is not configured, the global alarm threshold is used.

Example

Set the alarm threshold for ARP packets discarded by DAI on GE0/0/1 to 200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm threshold 200
```

14.6.4 arp anti-attack check user-bind check-item (interface view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries on an interface.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and VLAN ID.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
vlan	Indicates that the device checks VLAN IDs in ARP packets.	-

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and VLAN ID of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, use the **arp anti-attack check user-bind check-item** command to configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

Example

Configure GE0/0/1 to check IP addresses in ARP packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind check-item ip-address
```

14.6.5 arp anti-attack check user-bind check-item (VLAN or BD view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries in a VLAN or BD.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and interface number.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
interface	Indicates that the device checks interface numbers in ARP packets.	-

Views

VLAN view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled in the VLAN or BD using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

Example

Configure the device to check IP addresses in ARP packets from VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable
[HUAWEI-vlan100] arp anti-attack check user-bind check-item ip-address
```

14.6.6 arp anti-attack check user-bind enable

Function

The **arp anti-attack check user-bind enable** command enables dynamic ARP inspection (DAI) for an interface, BD, or VLAN to check ARP packets against binding entries.

The **undo arp anti-attack check user-bind enable** command disables DAI for an interface, BD, or VLAN.

By default, DAI is disabled for an interface, BD, or VLAN.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

Parameters

None

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, BD view, VLAN view

NOTE

DAI can be enabled in the BD view only for the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To defend against MITM attacks and prevent authorized users' data from being intercepted, run the **arp anti-attack check user-bind enable** command to enable DAI. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, BD, and VLAN ID of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

DAI can be enabled in the interface view, BD view, or VLAN view. When DAI is enabled in the interface view, the device checks all ARP packets received on the interface against binding entries. When DAI is enabled in the VLAN view or BD view, the device checks ARP packets received on interfaces belong to the VLAN or BD based on binding entries.

Follow-up Procedure

Run the **arp anti-attack check user-bind check-item (interface view)** or **arp anti-attack check user-bind check-item (VLAN or BD view)** command to configure check items for ARP packet check based on binding entries.

Precautions

When resources are sufficient, DAI can be enabled in a maximum of 400 VLANs.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable DAI on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
```

Enable DAI in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable
```

14.6.7 arp anti-attack entry-check enable

Function

The **arp anti-attack entry-check enable** command enables ARP entry fixing.

The **undo arp anti-attack entry-check enable** command disables ARP entry fixing.

By default, ARP entry fixing is disabled.

Format

arp anti-attack entry-check { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

undo arp anti-attack entry-check [**fixed-mac** | **fixed-all** | **send-ack**] **enable**

Parameters

Parameter	Description	Value
fixed-mac	Indicates ARP entry fixing in **fixed-mac** mode. When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry.	-
fixed-all	Indicates ARP entry fixing in **fixed-all** mode. When the MAC address, interface number, and VLAN ID of an ARP packet match those in the corresponding ARP entry, the device updates other information about the ARP entry.	-
send-ack	Indicates ARP entry fixing in **send-ack** mode. When the device receives an ARP packet with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user.	-

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To defend against ARP address spoofing attacks, enable ARP entry fixing. The **fixed-mac**, **fixed-all**, and **send-ack** modes are applicable to different scenarios and are mutually exclusive:

- The **fixed-mac** mode applies to networks where user MAC addresses are unchanged but user access locations often change. When a user connects to a different interface on the device, the device updates interface information in the ARP entry of the user timely.
- The **fixed-all** mode applies to networks where user MAC addresses and user access locations are fixed.
- The **send-ack** mode applies to networks where user MAC addresses and user access locations often change.

Precautions

After ARP entry fixing is enabled, the function that updates ARP entries when MAC address entries change (configured by the **mac-address update arp** command) becomes invalid.

In **send-ack** mode, the device can record a maximum of 100 ARP entries in the ARP Request packets intended to trigger ARP entry modification.

If you run the **arp anti-attack entry-check enable** command in the system view, ARP entry fixing is enabled on all interfaces. If you run the **arp anti-attack entry-check enable** command in the interface view, ARP entry fixing is enabled on the specified interface.

If ARP entry fixing is enabled globally and on a VLANIF interface simultaneously, the configuration on the VLANIF interface takes precedence over the global configuration.

Example

Enable ARP entry fixing and specify the **fixed-mac** mode.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack entry-check fixed-mac enable
```

14.6.8 arp anti-attack gateway-duplicate enable

Function

The **arp anti-attack gateway-duplicate enable** command enables ARP gateway anti-collision.

The **undo arp anti-attack gateway-duplicate enable** command disables ARP gateway anti-collision.

By default, ARP gateway anti-collision is disabled.

Format

arp anti-attack gateway-duplicate enable

undo arp anti-attack gateway-duplicate enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets with the source IP address being the gateway IP address on the LAN where the gateway is located, ARP entries on hosts in the LAN record the incorrect gateway address. As a result, all traffic from user hosts to the gateway is sent to the attacker and the attacker can intercept user data, causing network access failures of these hosts.

To defend against attacks from bogus gateways, run the **arp anti-attack gateway-duplicate enable** command to enable ARP gateway anti-collision on gateways to which user hosts directly connect. A gateway considers that an ARP gateway collision occurs when it receives an ARP packet meeting either of the following conditions:

- The source IP address of the ARP packet is the same as the IP address of the VLANIF interface matching the inbound interface of the packet.
- The source IP address of the ARP packet is the virtual IP address of the inbound interface, but the source MAC address is not the VRRP virtual MAC address.

The gateway generates an ARP anti-collision entry and discards the received ARP packets with the same source MAC address and VLAN ID as those of the ARP packet within a specified period of time. This function prevents ARP packets with a bogus gateway address from being broadcast in a VLAN.

Precautions

The device supports a maximum of 100 ARP anti-collision entries. When the maximum number is exceeded, the gateway cannot prevent new ARP gateway collision attacks.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable ARP gateway anti-collision.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack gateway-duplicate enable
```

14.6.9 arp anti-attack log-trap-timer

Function

The **arp anti-attack log-trap-timer** command sets the interval for sending ARP alarms.

The **undo arp anti-attack log-trap-timer** command restores the default setting.

The default interval for sending alarms is 0, indicating that the device does not send ARP alarms.

Format

arp anti-attack log-trap-timer *time*

undo arp anti-attack log-trap-timer

Parameters

Parameter	Description	Value
time	Specifies the interval for sending ARP alarms.	The value is an integer that ranges from 0 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limiting on ARP packets based on source IP addresses is enabled, if the number of ARP packets the device receives per second exceeds the limit, the device discards the excess ARP packets. The device considers the excess ARP packets as potential attacks. The device sends ARP alarms indicating potential attacks to the NMS. To avoid excessive alarms when ARP attacks occur, reduce the alarm quantity by setting a proper interval for sending alarms.

Precautions

In the insecure environment, you are advised to extend the interval for sending ARP alarms. This prevents excessive ARP alarms. In the secure environment, you are advised to shorten the interval for sending ARP alarms. This facilitates fault rectification in real time.

After the interval is set, the device discards alarms generates in this interval; therefore, some faults cannot be rectified in real time.

The command takes effect only on the alarm for ARP rate limit based on source IP addresses (corresponding to **arp speed-limit source-ip**). The other ARP alarms are generated at a fixed interval of 5 seconds.

Example

Set the interval for sending ARP alarms to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack log-trap-timer 20
```

14.6.10 arp anti-attack packet-check

Function

The **arp anti-attack packet-check** command enables ARP packet validity check and specifies check items.

The **undo arp anti-attack packet-check** command disables ARP packet validity check.

By default, ARP packet validity check is disabled.

Format

arp anti-attack packet-check { **ip** | **dst-mac** | **sender-mac** } *

undo arp anti-attack packet-check [**ip** | **dst-mac** | **sender-mac**] *

Parameters

Parameter	Description	Value
ip	Indicates ARP packet validity check based on the IP address.	-
dst-mac	Indicates ARP packet validity check based on the destination MAC address.	-
sender-mac	Indicates ARP packet validity check based on the source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To avoid ARP attacks, you can use the **arp anti-attack packet-check** command to enable ARP packet validity check on an access device or a gateway to filters out

ARP packets with invalid IP addresses or MAC addresses. The device checks validity of an ARP packet based on each or any combination of the following items:

- Source and destination IP addresses: The device checks the source and destination IP addresses in an ARP packet. If the source or destination IP address is all 0s, all 1s, or a multicast IP address, the device discards the packet as an invalid packet. The device checks both the source and destination IP addresses in an ARP Reply packet but checks only the source IP address in an ARP Request packet.
- Source MAC address: The device compares the source MAC address in an ARP packet with that in the Ethernet frame header. If they are the same, the packet is valid. If they are different, the device discards the packet.
- Destination MAC address: The device compares the destination MAC address in an ARP packet with that in the Ethernet frame header. If they are the same, the packet is valid. If they are different, the device discards the packet.

Precautions

Generally, packets with different source and destination MAC addresses in the ARP packet and Ethernet frame header are allowed by the ARP protocol. When an attack occurs, capture and analyze packets. If the attack is initiated by using inconsistent source or destination MAC addresses in the ARP packet and Ethernet frame header, enable ARP packet validity check based on the source or destination MAC address.

If you run the **arp anti-attack packet-check sender-mac** command multiple times, all the check items specified in these commands take effect.

Example

Enable ARP packet validity check and configures the device to check the source MAC address in an ARP packet.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack packet-check sender-mac
```

14.6.11 arp anti-attack rate-limit

Function

The **arp anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP packets globally, in a VLAN, or on an interface, and enables the function of discarding all ARP packets received from the interface when the rate of ARP packets exceeds the limit on an interface.

The **undo arp anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP packets globally, in a VLAN, or on an interface, and allows the device to send ARP packets to the CPU again.

By default, a maximum of 100 ARP packets are allowed to pass per second, and the function of discarding all ARP packets received from the interface when the rate of ARP packets exceeds the limit is disabled.

Format

System view, VLAN view

arp anti-attack rate-limit packet *packet-number* [**interval** *interval-value*]

undo arp anti-attack rate-limit

Interface view

arp anti-attack rate-limit packet *packet-number* [**interval** *interval-value* | **block-timer** *timer*] *

undo arp anti-attack rate-limit

Parameters

Parameter	Description	Value
packet *packet-number*	Specifies the maximum rate of sending ARP packets, that is, the number of ARP packets allowed to pass through in the rate limiting duration.	The value is an integer that ranges from 1 to 16384. The default value is 100.
interval *interval-value*	Specifies the rate limiting duration of ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.
block-timer *timer*	Specifies the duration for blocking ARP packets.	The value is an integer that ranges from 5 to 864000, in seconds.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, run the **arp anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP packets globally, in a VLAN, or on an interface. In the rate limiting duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

If the parameter **block-timer** *timer* is specified, the device discards all ARP packets received in the duration specified by *timer*.

Prerequisites

Rate limit on ARP packets has been enabled globally, in a VLAN, or on an interface using the **arp anti-attack rate-limit enable** command.

Precautions

If the maximum rate and rate limiting duration are configured in the system view, VLAN view, and interface view at the same time, the device uses the configurations in the interface view, VLAN view, and system view in order.

NOTE

The **arp anti-attack rate-limit** command takes effect only on ARP packets sent to the CPU for processing in **none-block** mode, and does not affect ARP packet forwarding by the chip. In **block** mode, the device discards subsequent ARP packets on an interface only when the number of ARP packets sent to the CPU exceeds the limit.

Example

Configure Layer 2 interface GE0/0/1 to allow 200 ARP packets to pass through in 10 seconds, and configure GE0/0/1 to discard all ARP packets in 60 seconds when the number of ARP packets exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit packet 200 interval 10 block-timer 60
```

Configure Layer 3 interface GE0/0/1 to allow 200 ARP packets to pass through in 10 seconds, and configure GE0/0/1 to discard all ARP packets in 60 seconds when the number of ARP packets exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit packet 200 interval 10 block-timer 60
```

14.6.12 arp anti-attack rate-limit alarm enable

Function

The **arp anti-attack rate-limit alarm enable** command enables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

The **undo arp anti-attack rate-limit alarm enable** command disables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

By default, the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit is disabled.

Format

arp anti-attack rate-limit alarm enable

undo arp anti-attack rate-limit alarm enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, if you want the device to generate alarms for excessive discarded ARP packets, run the **arp anti-attack rate-limit alarm enable** command. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command.

Example

Enable rate limit on ARP packets globally and enable the alarm function.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack rate-limit enable
[HUAWEI] arp anti-attack rate-limit alarm enable
```

Enable rate limit for the ARP packets on Layer 2 interface GE0/0/1 and enable the alarm function.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
```

Enable rate limit for the ARP packets on Layer 3 interface GE0/0/1 and enable the alarm function.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
```

14.6.13 arp anti-attack rate-limit alarm threshold

Function

The **arp anti-attack rate-limit alarm threshold** command sets the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.

The **undo arp anti-attack rate-limit alarm threshold** command restores the default alarm threshold.

By default, the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is 100.

Format

arp anti-attack rate-limit alarm threshold *threshold*

undo arp anti-attack rate-limit alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.	The value is an integer that ranges from 1 to 16384.

Views

System view, VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **arp anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp anti-attack rate-limit alarm enable** command.

Example

Enable rate limit on ARP packets globally, enable the alarm function, and set the alarm threshold to 50.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack rate-limit enable
[HUAWEI] arp anti-attack rate-limit alarm enable
[HUAWEI] arp anti-attack rate-limit alarm threshold 50
```

Enable rate limit for the ARP packets on Layer 2 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm threshold 50
```

Enable rate limit for the ARP packets on Layer 3 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm threshold 50
```

14.6.14 arp anti-attack rate-limit enable

Function

The **arp anti-attack rate-limit enable** command enables rate limit on ARP packets.

The **undo arp anti-attack rate-limit enable** command disables rate limit on ARP packets.

By default, rate limiting on ARP packets is disabled.

Format

arp anti-attack rate-limit enable

undo arp anti-attack rate-limit enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

You can run the **arp anti-attack rate-limit enable** command to enable rate limit on ARP packets. When the rate of ARP packets exceeds the limit, excess ARP packets are discarded. To set the rate limit and rate limiting duration of ARP packets, run the **arp anti-attack rate-limit** command.

After the optimized ARP reply function (disabled by default) is enabled using the **undo arp optimized-reply disable** command, rate limiting on ARP packets globally, in a VLAN, or on an Interface does not take effect.

Example

Enable rate limit on ARP packets globally.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack rate-limit enable
```

Enable rate limit for the ARP packets on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
```

Enable rate limit for the ARP packets on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
```

14.6.15 arp trust source

Function

The **arp trust source** command enables ARP gateway protection for the specified IP address.

The **undo arp trust source** command disables ARP gateway protection for the specified IP address.

By default, ARP gateway protection is disabled.

Format

arp trust source *ip-address*

undo arp trust source { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the protected gateway IP address.	The value is in dotted decimal notation.
all	Disables ARP gateway protection for all IP addresses in the current view.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker poses as a gateway to send ARP packets, other users on the network consider the attacker to be a gateway, causing a communication interruption between authorized users and gateway. This situation will also happen if a user incorrectly sets the host IP address as the gateway address. To prevent such bogus gateway attacks, configure ARP gateway protection on the device's interfaces connected to the gateway. When the ARP packets from a gateway address reach a device:

- The interfaces with gateway protection enabled can receive and forward the ARP packets.
- The interfaces without gateway protection enabled discard the ARP packets.

Precautions

A maximum of 8 protected gateway addresses can be specified on each interface, and 32 can be specified on the entire device. If the same gateway IP address is specified on different interfaces, the system considers that multiple protected gateway IP addresses have been configured.

Example

Enable ARP gateway protection on GE0/0/1 and set the protected gateway IP address to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp trust source 10.10.10.1
```

14.6.16 arp gratuitous-arp send enable

Function

The **arp gratuitous-arp send enable** command enables gratuitous ARP packet sending.

The **undo arp gratuitous-arp send enable** command disables gratuitous ARP packet sending.

By default, gratuitous ARP packet sending is disabled.

Format

arp gratuitous-arp send enable

undo arp gratuitous-arp send enable

Parameters

None

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets to other user hosts, ARP entries on the hosts record the incorrect gateway address. As a result, the gateway cannot receive data sent from the hosts. You can enable gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

By default, the device sends a gratuitous ARP packet every 60 seconds after this function is enabled. You can also set the interval using the **arp gratuitous-arp send interval** command.

Precautions

After you run the **arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is enabled on all VLANIF interfaces.

After you run the **undo arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is disabled on all VLANIF interfaces.

Example

Enable gratuitous ARP packet sending on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp gratuitous-arp send enable
```

14.6.17 arp gratuitous-arp send interval

Function

The **arp gratuitous-arp send interval** command sets the interval for sending gratuitous ARP packets.

The **undo arp gratuitous-arp send interval** command restores the default interval for sending gratuitous ARP packets.

By default, the interval for sending gratuitous ARP packets is 60 seconds.

Format

arp gratuitous-arp send interval *interval-time*

undo arp gratuitous-arp send interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for sending gratuitous ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds.

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device sends a gratuitous ARP packet every 60 seconds after gratuitous ARP sending is enabled. You can set the interval for sending gratuitous ARP packets using the **arp gratuitous-arp send interval** command.

If you set the interval in the system view, the configuration takes effect on all VLANIF interfaces. If you set the interval in both the system view and VLANIF interface view, the configuration on the VLANIF interface takes precedence over the global configuration.

Prerequisites

Gratuitous ARP packet sending has been enabled using the **arp gratuitous-arp send enable** command.

Example

Set the interval for sending gratuitous ARP packets to 100 seconds on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp gratuitous-arp send enable
[HUAWEI-Vlanif10] arp gratuitous-arp send interval 100
```

14.6.18 arp learning dhcp-trigger

Function

The **arp learning dhcp-trigger** command enables ARP learning triggered by DHCP.

The **undo arp learning dhcp-trigger** command disables ARP learning triggered by DHCP.

By default, ARP learning triggered by DHCP is disabled.

Format

arp learning dhcp-trigger

undo arp learning dhcp-trigger

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many DHCP users connect to a network device, the device needs to learn and maintain many ARP entries. This affects device performance.

To address this issue, you can configure ARP learning triggered by DHCP on the gateway. When the DHCP server assigns an IP address to a user, the device generates a DHCP snooping binding table and generates an ARP entry for the user based on the binding table. When DHCP snooping binding entries are deleted, ARP entries are also deleted.

Prerequisites

- DHCP has been enabled globally using the **dhcp enable** command in the system view.

- DHCP snooping has been enabled globally using the **dhcp snooping enable** command in the system view.
- DHCP snooping has been enabled using the **dhcp snooping enable** command in the view of the interface or VLAN through which a user goes online.

Precautions

When both VRRP and DHCP relay are configured on the network, neither the **dhcp snooping enable** command nor the **arp learning dhcp-trigger** command can be configured on the VRRP master and backup devices.

The VLANIF interface must be assigned an IP address on the same network segment as that of a user.

DHCP snooping for wireless users is deployed on APs. The AC enabled with DHCP snooping does not process DHCP packets of wireless users. Therefore, ARP learning takes effect only for wired users.

Example

Enable ARP learning triggered by DHCP on VLANIF 100 and assign an IP address on the same network segment as that of a user.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.0.1 255.255.255.0
[HUAWEI-Vlanif100] arp learning dhcp-trigger
```

14.6.19 arp learning disable

Function

The **arp learning disable** command disables an interface from learning dynamic ARP entries.

The **undo arp learning disable** command enables an interface to learn dynamic ARP entries.

By default, an interface is enabled to learn dynamic ARP entries.

Format

arp learning disable

undo arp learning disable

Parameters

None

Views

VLANIF interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security and facilitate management, you can enable an interface to learn or disable an interface from learning dynamic ARP entries. You can also use the **arp learning strict** or **arp learning strict** commands to strictly control ARP entry learning on an interface.

Precautions

If an interface is disabled from learning ARP entries, the network will be interrupted.

If an interface has learned some dynamic ARP entries, the system does not delete these entries after the interface is disabled from learning dynamic ARP entries. You can manually delete or reserve these learned dynamic ARP entries (deleted by the **reset arp** command).

Example

Disable VLANIF10 from learning dynamic ARP entries.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp learning disable
```

14.6.20 arp learning strict (interface view)

Function

The **arp learning strict** command enables strict ARP learning on the interface.

The **undo arp learning strict** command restores the global configuration on the interface.

By default, strict ARP learning is disabled on the interface.

Format

arp learning strict { **force-enable** | **force-disable** | **trust** }

undo arp learning strict

Parameters

Parameter	Description	Value
force-enable	Indicates that strict ARP learning is enabled.	-

Parameter	Description	Value
force-disable	Indicates that strict ARP learning is disabled.	-
trust	Indicates that the configuration of strict ARP learning is the same as the global configuration. **NOTE** The effect of the **trust** parameter is the same as the effect of the **undo arp learning strict** command.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself, but does not allow the device to learn the ARP entries for the ARP packets received from other devices. In this way, the device can defend against most ARP attacks.

Prerequisites

On an Ethernet interface working in Layer 2 mode, the **undo portswitch** command has been run to switch the interface to Layer 3 mode.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

Precautions

The configuration on an interface takes precedence over the global configuration.

When ARP attacks occur on many interfaces of the device, you can run the **arp learning strict** command to enable strict ARP learning globally.

Example

Enable strict ARP learning on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp learning strict force-enable
```

Enable strict ARP learning on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp learning strict force-enable
```

14.6.21 arp learning strict (system view)

Function

The **arp learning strict** command enables strict ARP learning.

The **undo arp learning strict** command disables strict ARP learning.

By default, strict ARP learning is disabled.

Format

arp learning strict

undo arp learning strict

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.

- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. In this way, the device can defend against most ARP attacks.

Precautions

The configuration on an interface takes precedence over the global configuration.

Example

Enable strict ARP learning.

```
<HUAWEI> system-view
[HUAWEI] arp learning strict
```

14.6.22 arp optimized-passby enable

Function

The **arp optimized-passby enable** command configures the device not to send ARP packets destined for other devices to the CPU.

The **undo arp optimized-passby enable** command configures the device to send ARP packets destined for other devices to the CPU.

By default, a device does not send ARP packets destined for other devices to the CPU.

Format

arp optimized-passby enable

undo arp optimized-passby enable

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface receives a large number of ARP packets whose destination IP addresses are different from the IP address of this interface and sends these ARP packets to the CPU for processing, the CPU usage is high and the CPU cannot process services properly.

To prevent this issue, you can configure the device to directly forward ARP packets destined for other devices without sending them to the CPU. This improves the device's capability of defending against ARP flood attacks.

Precautions

If any of the following configurations is performed, the configuration of disabling the device from sending ARP packets destined for other devices to the CPU does not take effect on a VLANIF interface:

- Run the **arp anti-attack gateway-duplicate enable** to enable ARP gateway anti-collision.
- Run the **arp ip-conflict-detect enable** command to enable IP address conflict detection.
- Run the **arp anti-attack check user-bind enable** command to enable the dynamic ARP inspection (DAI) function.
- Run the **dhcp snooping arp security enable** command to enable the egress ARP inspection (EAI) function.
- Run the **arp over-vpls enable** command to enable proxy ARP on a VPLS network.
- Run the **arp-proxy enable** command to enable routed proxy ARP.
- Run the **arp-proxy inner-sub-vlan-proxy enable** command to enable intra-VLAN proxy ARP.
- Run the **arp-proxy inter-sub-vlan-proxy enable** command to enable inter-VLAN proxy ARP.
- Perform an NAC-related configuration. For details, see the *User Access and Authentication Configuration Guide*.

Example

Configure the device to send ARP packets destined for other devices to the CPU.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo arp optimized-passby enable
```

14.6.23 arp optimized-reply disable

Function

The **arp optimized-reply disable** command disables the optimized ARP reply function.

The **undo arp optimized-reply disable** command enables the optimized ARP reply function.

By default, the optimized ARP reply function is enabled.

Format

arp optimized-reply disable

undo arp optimized-reply disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stack of multiple switches functions as an access gateway, the stack can receive a large number of ARP packets requesting for the stack's interface MAC address. If all these ARP Request packets are sent to the master switch, the CPU usage of the switch increases, and other services are affected.

To address the preceding problem, enable optimized ARP reply, which improves the switch's capability of defending against ARP flood attack. After this function is enabled, the stack performs the following operations:

- When receiving an ARP Request packet of which the destination IP address is the local interface address, the switch where the interface is located directly returns an ARP Reply packet.
- When a stack system receives an ARP Request packet of which the destination IP address is not the local interface address and intra-VLAN proxy ARP is enabled on the master switch, the switch where the interface is located checks whether the ARP Request packet meets the proxy condition. If so, the switch returns an ARP Reply packet. If not, the switch discards the packet.

NOTE

The optimized ARP reply function can be configured on a stand-alone fixed switch, but does not take effect.

By default, the optimized ARP reply function is enabled. After a device receives an ARP Request packet, the device checks whether an ARP entry corresponding to the source IP address of the ARP Request packet exists.

- If there is a corresponding ARP entry, the stack performs optimized ARP reply to this ARP Request packet.
- If there is no corresponding ARP entry, the stack does not perform optimized ARP reply to this ARP Request packet.

Precautions

- The optimized ARP reply function does not take effect for ARP Request packets with double VLAN tags.
- The optimized ARP reply function takes effect for ARP Request packets sent by wireless users.
- The optimized ARP reply function takes effect only for the ARP Request packets received by VLANIF interfaces, VBDIF interfaces, Eth-Trunk sub-interfaces, and physical sub-interfaces. The optimized ARP reply function does not take effect for the ARP Request packets sent from the VLANIF interfaces of super VLANs. The optimized ARP reply function takes effect for the ARP Request packets sent from the VLANIF interfaces of MUX VLANs, but it do not take effect when the ARP request packet carries the Group VLAN or Separate VLAN.

  NOTE

  The optimized ARP reply function takes effect only for the ARP Request packets received by the Eth-Trunk sub-interfaces and physical sub-interfaces of the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The optimized ARP reply function does not take effect globally or on interfaces after you run any of the following commands:
  - **ip address** *ip-address* { *mask* | *mask-length* } **sub**: configures secondary IP addresses for interfaces.
  - **arp anti-attack gateway-duplicate enable**: enables the ARP gateway anti-collision function.
  - **arp ip-conflict-detect enable**: enables IP address conflict detection.
  - **arp anti-attack check user-bind enable**: enables dynamic ARP inspection (DAI).

    NOTE

    When DAI is enabled in the physical interface view, the optimized ARP reply function does not take effect on the device where the physical interface resides. When DAI is enabled in the Eth-Trunk view or VLAN view, the optimized ARP reply function does not take effect globally.
  - **dhcp snooping arp security enable**: enables egress ARP inspection (EAI).
  - **arp over-vpls enable**: enables ARP proxy on the device on a VPLS network.
  - **arp-proxy enable**: configures the routed ARP proxy function.
  - **arp-proxy inter-sub-vlan-proxy enable** configures inter-VLAN proxy ARP function.
- After the optimized ARP reply function is enabled, the following functions become invalid:
  - ARP rate-limiting based on source MAC addresses (configured using the **arp speed-limit source-mac** command)
  - ARP rate-limiting based on source IP addresses (configured using the **arp speed-limit source-ip** command)
  - Global ARP rate-limiting, ARP rate-limiting in VLANs, as well as ARP rate-limiting on interfaces (configured using the **arp anti-attack rate-limit enable** command)

Example

Disable the optimized ARP reply function.

```
<HUAWEI> system-view
[HUAWEI] arp optimized-reply disable
```

14.6.24 arp over-vpls enable

Function

The **arp over-vpls enable** command enables ARP proxy on a device in a VPLS network.

The **undo arp over-vpls enable** command disables ARP proxy on a device in a VPLS network.

By default, ARP proxy is disabled on a device in a VPLS network.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Format

arp over-vpls enable

undo arp over-vpls enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent bogus ARP packets at the PW side from being broadcast to the AC side on a VPLS network, enable ARP proxy over VPLS on a PE.

ARP packets at the PW side are sent to the CPU for processing.

- If the ARP packets are ARP request packets and the destination IP addresses in the packets match DHCP snooping binding entries, the device constructs ARP reply packets based on the DHCP snooping binding entries and sends them to the requester at the PW side.

- If the ARP packets are not ARP request packets or the destination IP addresses in the packets match no DHCP snooping binding entry, the device forwards these ARP packets to the destination.

Precautions

Before using this command, ensure that DHCP snooping on the device in a VPLS network is enabled using the **dhcp snooping over-vpls enable** command.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

Example

Enable ARP proxy on a device in a VPLS network.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping over-vpls enable
[HUAWEI] arp over-vpls enable
```

14.6.25 arp snooping anti-attack check enable

Function

The **arp snooping anti-attack check enable** command enables ARP snooping detection on an interface.

The **undo arp snooping anti-attack check enable** command disables ARP snooping detection on an interface.

By default, ARP snooping detection is disabled on an interface.

Format

arp snooping anti-attack check enable

undo arp snooping anti-attack check enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group interface

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If forged ARP packets are sent in a man-in-the-middle (MITM) attack, two communicating devices learn an incorrect address mapping of each other and the data of authorized users is intercepted by the attacker. To prevent this problem, you can enable ARP snooping detection on the device. After ARP snooping detection is enabled, the device compares the source IP address, source MAC address, port number, and VLAN information in a received ARP packet with those in the ARP snooping table. If no ARP snooping entry with the same source IP address and VLAN information as the ARP packet is found, the device creates an ARP snooping entry. If an ARP snooping entry with the same source IP address and VLAN information is found and other information matches, the device determines that the user who sends the ARP packet is a valid user and allows the ARP packet to pass. If an ARP snooping entry with the same source IP address and VLAN information is found but other information does not match, the device discards the ARP packet.

Prerequisites

Before running this command, ensure that you have completed the following configurations:

1. Run the **arp snooping enable** command in the system view to enable ARP snooping globally.
2. Run the **arp snooping anti-attack entry-check enable** command in the system view to enable ARP snooping entry fixing.
3. Run the **arp snooping enable** command in the interface view to enable ARP snooping on an interface.

Example

Enable ARP snooping detection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] arp snooping enable
[HUAWEI] arp snooping anti-attack entry-check fixed-mac enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp snooping enable
[HUAWEI-GigabitEthernet0/0/1] arp snooping anti-attack check enable
```

14.6.26 arp snooping anti-attack entry-check enable

Function

The **arp snooping anti-attack entry-check enable** command enables ARP snooping entry fixing.

The **undo arp snooping anti-attack entry-check enable** command disables ARP snooping entry fixing.

By default, ARP snooping entry fixing is disabled.

Format

arp snooping anti-attack entry-check { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

undo arp snooping anti-attack entry-check [**fixed-mac** | **fixed-all** | **send-ack**] **enable**

Parameters

Parameter	Description	Value
fixed-mac	Indicates ARP snooping entry fixing in **fixed-mac** mode. When receiving an ARP packet, the device discards the packet if its MAC address does not match the MAC address in the corresponding ARP snooping entry. If the MAC address in the ARP packet matches that in the corresponding ARP snooping entry while the interface information does not match that in the ARP snooping entry, the device updates the interface information in the ARP snooping entry.	-
fixed-all	Indicates ARP snooping entry fixing in **fixed-all** mode. When the MAC address and interface information of an ARP packet match those in the corresponding ARP snooping entry, the device updates other information in the ARP snooping entry.	-

Parameter	Description	Value
send-ack	Indicates ARP snooping entry fixing in **send-ack** mode. When the device receives an ARP packet with a changed MAC address or different interface information, it does not immediately update the corresponding ARP snooping entry. Instead, the device sends a unicast ARP Request packet to the user corresponding to the original MAC address in the ARP snooping entry. If the device receives an ARP Reply packet from the user, the device does not update the ARP snooping entry. If the device does not receive an ARP Reply packet from the user, the device sends a unicast ARP Request packet to the user corresponding to the new MAC address. Regardless of whether the device receives an ARP Reply packet from this user, the device updates the ARP snooping entry based on the ARP packets sent from the user if this user continuously sends ARP Request packets to the device.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges ARP packets, the device learns incorrect ARP snooping entries. As a result, users cannot receive data packets. To prevent this problem, you can enable the ARP snooping entry fixing function on the device. Once the device enabled with this function learns an ARP snooping entry, it does not update the ARP snooping entry, only updates some information in the ARP snooping entry, or sends a unicast ARP Request packet to check the validity of the new ARP snooping entry. The device provides three ARP snooping entry fixing modes, which are applicable to different scenarios.

- **fixed-mac**: This mode applies to networks where user MAC addresses are unchanged but user access locations often change. When a user connects to a different interface on the device, the device updates interface information in the ARP snooping entry of the user timely.
- **fixed-all**: This mode applies to networks where user MAC addresses and user access locations are fixed.
- **send-ack**: This mode applies to networks where user MAC addresses and user access locations often change.

Prerequisites

ARP snooping has been enabled by running the **arp snooping enable** command in the system view.

Precautions

- An ARP snooping entry is created based on the source IP address and VLAN information of an ARP packet. Therefore, ARP snooping entry fixing is performed only when the source IP address and VLAN information of an ARP packet are the same as those in an existing ARP snooping entry.
- The three ARP snooping entry fixing modes are mutually exclusive.
- Before disabling ARP snooping entry fixing, ensure that ARP snooping detection is disabled on all interfaces.

Example

Enable ARP snooping entry fixing and specify the **fixed-mac** mode.

```
<HUAWEI> system-view
[HUAWEI] arp snooping enable
[HUAWEI] arp snooping anti-attack entry-check fixed-mac enable
```

14.6.27 arp snooping enable

Function

The **arp snooping enable** command enables ARP snooping.

The **undo arp snooping enable** command disables ARP snooping.

By default, ARP snooping is disabled on the device.

Format

arp snooping enable

undo arp snooping enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During video network O&M, the NMS needs to obtain the IP addresses and MAC addresses of NEs to draw a network topology for subsequent O&M. For LLDP-incapable NEs, you can configure the ARP snooping function on the access switch. This function enables the device to obtain the IP addresses and MAC addresses of NEs from the ARP packets sent from the NEs, and generate ARP snooping entries.

After ARP snooping is enabled, the device sends the received ARP packets to the CPU. The CPU analyzes the ARP packets to obtain the source IP address, source MAC address, VLAN ID, and inbound interface of the packets, and creates an ARP snooping entry to record user information.

After an ARP snooping entry is created, it ages after 900 seconds by default. An ARP snooping entry is created based on the source IP address and VLAN information of an ARP packet. If no ARP snooping entry matches the source IP address and VLAN information of a received ARP packet, the device creates a new ARP snooping entry. If the source IP address and VLAN information of a received ARP packet are the same as those in an existing ARP snooping entry, the device updates the MAC address and interface information in the entry and resets the aging timer.

Precautions

- You must enable ARP snooping in the system view, and then enable ARP snooping in a VLAN or on an interface.
- When a switch is managed by the analyzer, you need to enable ARP snooping globally and on an interface so that the analyzer can parse user access port information.

Example

Enable ARP snooping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] arp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp snooping enable
```

Enable ARP snooping in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] arp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp snooping enable
```

14.6.28 arp snooping detect default-ip

Function

The **arp snooping detect default-ip** command configures the source IP address of ARP probe packets sent by the device.

The **undo arp snooping detect default-ip** command restores the default setting.

By default, the source IP address of ARP probe packets is 0.0.0.0.

Format

arp snooping detect default-ip *ip-address*

undo arp snooping detect default-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address of ARP probe packets.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After generating ARP snooping entries, the device performs ARP probe on the entries that are about to be aged out. By default, the device sends ARP probe packets with the source IP address being 0.0.0.0. After a terminal obtains an IP address when going online, it also sends an ARP probe packet with the source IP address being all 0s to check whether the obtained IP address conflicts with other IP addresses. If the terminal receives an all-0 ARP packet, the terminal considers that an IP address conflict occurs and therefore re-applies for an IP address. In this case, you need to run this command to change the source IP address of the device's ARP probe packets to prevent terminals from repeatedly applying for IP addresses.

Configuration Impact

If this command is run more than once, the latest configuration overrides the previous one.

Precautions

You are advised to set the IP address to be different from the IP address of the user gateway.

Example

Set the source IP address of ARP probe packets to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] arp snooping detect default-ip 10.1.1.1
```

14.6.29 arp snooping detect ignored-ip

Function

The **arp snooping detect ignored-ip** command configures the device not to perform ARP probe for ARP snooping entries of a specified IP address.

The **undo arp snooping detect ignored-ip** command restores the default setting.

By default, the device performs ARP probe for ARP snooping entries of all IP addresses.

Format

arp snooping detect ignored-ip *ip-address*

undo arp snooping detect ignored-ip { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address for ARP probe.	The value is in dotted decimal notation.
all	Performs ARP probe for all IP addresses.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device performs ARP probe for the generated ARP snooping entries that are about to age. Specifically, it sends ARP probe packets with the source IP addresses being all 0s and the destination IP addresses being the IP addresses of the entries that are about to age. If the peer device is a gateway, it identifies the received ARP packets as gratuitous ARP packets sent by itself, performs IP address conflict detection, and frequently generates conflict alarms and logs. To prevent this problem, you can run the **arp snooping detect ignored-ip** command to configure the device not to perform ARP probe for ARP snooping entries of a specified IP address.

Example

Disable ARP probe for ARP snooping entries of the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] arp snooping detect ignored-ip 10.1.1.1
```

14.6.30 arp speed-limit source-mac

Function

The **arp speed-limit source-mac** command sets the maximum rate of ARP packets based on source MAC addresses.

The **undo arp speed-limit source-mac** command restores the default setting.

By default, the maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on source MAC addresses.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp speed-limit source-mac [*mac-address*] **maximum** *maximum*

undo arp speed-limit source-mac [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address. If this parameter is specified, the rate of ARP packets from the MAC address is limited. If this parameter is not specified, the rate of ARP packets from each MAC address is limited.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified MAC address.	The integer form, in pps, is as follows: ● S5731-S, S5731S-S: 0 to 16384 ● S5731-H, S5731S-H: 0 to 61440 ● S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S: 0 to 65536 ● S6735-S, S6720-EI, S6720S-EI: 0 to 131072 ● S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M: 0 to 4096 ● S5735-S, S5735S-S, S5735-S-I: 0 to 8180 ● S2730S-S: 0 to 2048

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed source MAC addresses but variable source IP addresses, the CPU is overloaded and ARP entries are exhausted. To prevent this problem, limit the rate of ARP packets based on source MAC addresses.

After the **arp speed-limit source-mac** command is run, the device collects statistics on ARP packets from a specified source MAC address. If the number of

ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source MAC address.

If the source MAC address is not specified, the rate of ARP packets from each MAC address is limited. If the rate of ARP packets from each source IP address is set using the **arp speed-limit source-ip** command at the same time and the rate is the same as that set using the **arp speed-limit source-mac** command, both commands take effect. When receiving ARP packets from a fixed source, the device limits the rate of these packets based on the maximum rate set by the **arp speed-limit source-mac** command.

After the optimized ARP reply function (disabled by default) is enabled using the **undo arp optimized-reply disable** command, rate limiting on ARP packets based on the source MAC address does not take effect.

Example

Set the maximum rate of ARP packets from any source MAC address to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-mac maximum 100
```

Set the maximum rate of ARP packets from a specified MAC address 0-0-1 to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-mac 0-0-1 maximum 50
```

14.6.31 arp speed-limit source-ip

Function

The **arp speed-limit source-ip** command sets the maximum rate of ARP packets based on the source IP address.

The **undo arp speed-limit source-ip** command restores the default setting.

By default, the device allows a maximum of 30 ARP packets from the same source IP address to pass through per second.

Format

arp speed-limit source-ip [*ip-address*] **maximum** *maximum*

undo arp speed-limit source-ip [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the rate of ARP packets from the IP address is limited. If this parameter is not specified, the rate of ARP packets from each IP address is limited.	The value is in dotted decimal notation.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified source IP address. **NOTE** If the rate of all ARP packets is limited, a large value is recommended because valid packets may be discarded if the value is small. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The integer form, in pps, is as follows: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720-LI, S5720S-LI: 0 to 2048 ● S5720I-SI, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M: 0 to 4096 ● S5735-S, S5735S-S, S5735-S-I: 0 to 8180 ● S5731-S, S5731S-S: 0 to 16384 ● S5731-H, S5731S-H: 0 to 61440 ● S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S: 0 to 65536 ● S5735S-H, S5736-S: 0 to 20000 ● S6735-S, S6720-EI, S6720S-EI: 0 to 131072

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed IP addresses (for example, the ARP packets with the same source IP addresses but frequently changing MAC addresses or outbound interfaces), the CPU is overloaded and cannot process other services. To prevent this problem, limit the rate of ARP packets based on the source IP address.

After the **arp speed-limit source-ip** command is run, the device collects statistics on ARP packets based on the source IP address. If the number of ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source IP address.

When you confirm that the network is secure, set the rate limit to 0 to increase ARP learning speed. After the rate limit is set to 0, the device does not limit the ARP packet rate based on source IP addresses.

If the source IP address is not specified, the rate of ARP packets from each IP address is limited. If the rate of ARP packets from each source MAC address is set using the **arp speed-limit source-mac** command at the same time and the rate is the same as that set using the **arp speed-limit source-ip** command, both commands take effect. When receiving ARP packets from a fixed source, the device limits the rate of these packets based on the maximum rate set by the **arp speed-limit source-mac** command.

After the optimized ARP reply function (disabled by default) is enabled using the **undo arp optimized-reply disable** command, rate limiting on ARP packets based on the source IP address does not take effect.

Example

Set the maximum rate of ARP packets from a source IP address to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-ip maximum 100
```

Set the maximum rate of ARP packets from a specified IP address 10.0.0.1 to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-ip 10.0.0.1 maximum 50
```

14.6.32 arp validate (interface view)

Function

The **arp validate** command enables MAC address consistency check in an ARP packet on an interface. This function compares the source and destination MAC addresses in ARP packets with those in the Ethernet frame header.

The **undo arp validate** command disables MAC address consistency check in an ARP packet on an interface.

By default, MAC address consistency check in an ARP packet is disabled.

Format

arp validate { **source-mac** | **destination-mac** } *

undo arp validate { **source-mac** | **destination-mac** } *

Parameters

Parameter	Description	Value
source-mac	Indicates that the device compares the source MAC address in a received ARP packet with that in the Ethernet frame header.	-
destination-mac	Indicates that the device compares the destination MAC address in a received ARP packet with that in the Ethernet frame header.	-

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, VE interface view

Default Level

2: Configuration level

Usage Guidelines

The MAC address consistency check function for ARP packets prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. This function is usually configured on gateways.

After the **arp validate** command is run, the gateway checks the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

When using this command, note the following points:

- If **source-mac** is specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks only the source MAC address consistency.
- If **destination-mac** is specified:

  - When receiving an ARP Request packet, the device does not check the destination MAC address consistency because the ARP Request packet is broadcast.
  - When receiving an ARP Reply packet, the device checks the destination MAC address consistency.
- If **source-mac** and **destination-mac** are specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks the source and destination MAC address consistency.

Example

Enable MAC address consistency check in an ARP packet on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp validate source-mac destination-mac
```

Enable MAC address consistency check in an ARP packet on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp validate source-mac destination-mac
```

14.6.33 arp-fake expire-time

Function

The **arp-fake expire-time** command sets the aging time of temporary ARP entries.

The **undo arp-fake expire-time** command restores the default aging time of temporary ARP entries.

By default, the aging time of temporary ARP entries is 3 seconds.

Format

arp-fake expire-time *expire-time*

undo arp-fake expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of temporary ARP entries.	The value is an integer that ranges from 1 to 36000, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

- In the aging time of temporary ARP entries:
  - Before receiving an ARP reply packet, the device discards the IP packets matching the temporary ARP entry and does not generate ARP Miss messages.
  - After receiving an ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages and temporary ARP entries are repeatedly generated

When a device undergoes an ARP Miss attack, you can run the **arp-fake expire-time** command to extend the aging time of temporary ARP entries to reduce the frequency of triggering ARP Miss messages and minimize the impact on the device.

Example

Set the aging time of temporary ARP entries to 10 seconds on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp-fake expire-time 10
```

Set the aging time of temporary ARP entries to 10 seconds on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-fake expire-time 10
```

14.6.34 arp-limit

Function

The **arp-limit** command sets the maximum number of ARP entries that an interface can dynamically learn.

The **undo arp-limit** command deletes the maximum number of ARP entries that an interface can dynamically learn.

By default, the maximum number of ARP entries that an interface can dynamically learn is the same as the number of ARP entries supported by the device.

Format

VLANIF interface, VBDIF interface, VE sub-interface, Layer 3 interface, and Ethernet sub-interface:

arp-limit maximum *maximum*

undo arp-limit

VE sub-interface, Layer 2 interface and port group:

arp-limit vlan *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*

undo arp-limit vlan *vlan-id1* [**to** *vlan-id2*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Layer 3 interfaces and sub-interfaces.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support VE sub-interfaces.

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN from which the maximum number of ARP entries an interface can dynamically learn is limited. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, the device limits the maximum number of ARP entries an interface dynamically learns from the VLAN *vlan-id1*. If **to** *vlan-id2* is specified, the device limits the maximum number of ARP entries an interface dynamically learns from each VLAN from *vlan-id1* to *vlan-id2*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Parameter	Description	Value
maximum *maximum*	Specifies the maximum number of ARP entries that an interface can dynamically learn.	The integer form, is as follows: - SS1720GW-E, S1720GWR-E, S2730S-S, S5720-LI, S5720S-LI: 1 to 2048 - S5720I-SI, S5735-L-I, S5735-L1,S300, S500, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M: 1 to 4096 - S5735-S, S5735S-S, S5735-S-I: 1 to 8000 - S5731-S, S5731S-S: 1 to 16384 - S5731-H, S5731S-H: 1 to 61440 - S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S: 1 to 65536 - S5735S-H, S5736-S: 1 to 20000 - S6735-S, S6720-EI, S6720S-EI: 1 to 131072

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent ARP entries from being exhausted by ARP attacks from a host connecting to an interface on the device, set the maximum number of ARP entries that the interface can dynamically learn. When the number of the ARP entries learned by a specified interface reaches the maximum number, no dynamic ARP entry can be added.

Precautions

If the number of ARP entries learned by an interface exceeds the maximum number, the device neither learns new ARP entries nor clears the learned ARP entries. Instead, the device asks users to delete the excess ARP entries.

If the **arp-limit vlan** *vlan-id1* **to** *vlan-id2* **maximum** *maximum* command is run more than once, the following situations are available:

- If **maximum** *maximum* is the same in multiple command instances, all configurations take effect. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 35 to 40 maximum 200** command are run, both configurations take effect. If the VLAN ranges specified in multiple command instances are overlapping, the system automatically merges the VLAN ranges. For example, if the **arp-limit vlan 50 to 80 maximum 200** command and then the **arp-limit vlan 70 to 100 maximum 200** command are run, both configurations take effect, and the system merges the configurations into **arp-limit vlan 50 to 100 maximum 200**.
- If **maximum** *maximum* is different in multiple command instances, the latest configuration overrides the previous one for the same VLAN range. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 15 to 25 maximum 300** command are run, the system automatically divides the configurations into **arp-limit vlan 10 to 14 maximum 200**, **arp-limit vlan 15 to 25 maximum 300**, and **arp-limit vlan 26 to 30 maximum 200**.

Example

Configure that VLANIF 10 can dynamically learn a maximum of 20 ARP entries.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp-limit maximum 20
```

Configure that Layer 3 interface GE0/0/1 can dynamically learn a maximum of 20 ARP entries.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-limit maximum 20
```

Configure that Layer 2 interface GE0/0/1 can dynamically learn a maximum of 20 ARP entries corresponding to VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-limit vlan 10 maximum 20
```

14.6.35 arp-miss anti-attack rate-limit

Function

The **arp-miss anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP Miss messages globally, in a VLAN, or on an interface.

The **undo arp-miss anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP Miss messages globally, in a VLAN, or on an interface.

By default, the device can process a maximum of 100 ARP Miss messages per second.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp-miss anti-attack rate-limit packet *packet-number* [**interval** *interval-value*]

undo arp-miss anti-attack rate-limit

Parameters

Parameter	Description	Value
packet *packet-number*	Specifies the maximum rate of ARP Miss messages, that is, the number of ARP Miss messages the device processes in the rate limiting duration.	The value is an integer that ranges from 1 to 16384. The default value is 100.
interval *interval-value*	Specifies the rate limiting duration of ARP Miss messages.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, you can set maximum rate and rate limiting duration of ARP Miss messages globally, in a VLAN, or on an interface. If the number of ARP Miss messages triggered by IP packets in the rate limiting duration exceeds the limit, the device does not process the excess ARP Miss packets and discards the IP packets triggering the excess ARP Miss messages.

Prerequisites

Rate limit on ARP Miss messages has been enabled globally, in a VLAN, or on an interface using the **arp-miss anti-attack rate-limit enable** command.

Precautions

If rate limit on ARP Miss messages is configured in the system view, VLAN view, and interface view, the device uses the configurations in the interface view, VLAN view, and system view in order.

Example

Configure the device to process a maximum of 200 ARP Miss messages triggered by IP packets from Layer 2 interface GE0/0/1 in 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit packet 200 interval 10
```

Configure the device to process a maximum of 200 ARP Miss messages triggered by IP packets from Layer 3 interface GE0/0/1 in 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit packet 200 interval 10
```

14.6.36 arp-miss anti-attack rate-limit alarm enable

Function

The **arp-miss anti-attack rate-limit alarm enable** command enables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

The **undo arp-miss anti-attack rate-limit alarm enable** command disables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

By default, the alarm function is disabled.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp-miss anti-attack rate-limit alarm enable

undo arp-miss anti-attack rate-limit alarm enable

Parameters

None

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, if you want that the device can generate alarms to notify the network administrator of a large number of discarded excess ARP Miss messages, run the **arp-miss anti-attack rate-limit alarm enable** command. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp-miss anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command.

Example

Enable the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
```

Enable the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
```

14.6.37 arp-miss anti-attack rate-limit alarm threshold

Function

The **arp-miss anti-attack rate-limit alarm threshold** command sets the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss packets exceeds the limit.

The **undo arp-miss anti-attack rate-limit alarm threshold** command restores the default alarm threshold.

By default, the alarm threshold for ARP Miss packets discarded is 100.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp-miss anti-attack rate-limit alarm threshold *threshold*

undo arp-miss anti-attack rate-limit alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.	The value is an integer that ranges from 1 to 16384, in pps.

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **arp-miss anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp-miss anti-attack rate-limit alarm enable** command.

Example

Enable rate limit on ARP Miss messages globally, enable the alarm function, and set the alarm threshold to 200.

```
<HUAWEI> system-view
[HUAWEI] arp-miss anti-attack rate-limit enable
```

```
[HUAWEI] arp-miss anti-attack rate-limit alarm enable
[HUAWEI] arp-miss anti-attack rate-limit alarm threshold 200
```

Enable rate limit on ARP Miss messages on Layer 2 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm threshold 200
```

Enable rate limit on ARP Miss messages on Layer 3 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm threshold 200
```

14.6.38 arp-miss anti-attack rate-limit enable

Function

The **arp-miss anti-attack rate-limit enable** command enables rate limit on ARP Miss messages globally, in a VLAN, or on an interface.

The **undo arp-miss anti-attack rate-limit enable** command disables rate limit on ARP Miss messages globally, in a VLAN, or on an interface.

By default, rate limit on ARP Miss messages is disabled globally, in a VLAN, or on an interface.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp-miss anti-attack rate-limit enable

undo arp-miss anti-attack rate-limit enable

Parameters

None

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, 25GE interface view, 100GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the CPU for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, configure rate limit on ARP Miss messages globally, in a VLAN, or on an interface. The device collects statistics on ARP Miss messages. If the number of ARP Miss messages generated within the rate limiting duration exceeds the threshold (the maximum number of ARP Miss messages), the gateway discards the IP packets triggering the excess ARP Miss messages.

Follow-up Procedure

Run the **arp-miss anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP Miss messages.

Example

Enable rate limit on ARP Miss messages on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
```

Enable rate limit on ARP Miss messages on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
```

14.6.39 arp-miss speed-limit source-ip

Function

The **arp-miss speed-limit source-ip** command sets the maximum number of ARP Miss messages based on source IP addresses and specifies the mode for processing ARP Miss packets.

The **undo arp-miss speed-limit source-ip** command restores the default setting.

By default, the device processes a maximum of 30 ARP Miss messages triggered by IP packets from the same source IP address per second.

If the number of ARP Miss messages triggered by IP packets from the same source IP address per second exceeds the limit, the device discards the excess ARP Miss messages, that is, the device discards the excess ARP Miss packets. The device then uses the **block** mode to discard all ARP Miss packets from the source IP address within 5 seconds by default.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

arp-miss speed-limit source-ip *ip-address* [**mask** *mask*] **maximum** *maximum* [**none-block** | **block timer** *timer*]

arp-miss speed-limit source-ip maximum *maximum*

undo arp-miss speed-limit source-ip [*ip-address* [**mask** *mask*]]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support [**none-block** | **block timer** *timer*].

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the maximum number of ARP Miss messages triggered by packets from this IP address is limited. If this parameter is not specified, the maximum number of ARP Miss messages triggered by packets from each IP address is limited.	The value is in dotted decimal notation.
mask *mask*	Specifies the mask of the IP address. If this parameter is specified, the maximum number of ARP Miss messages triggered by packets from IP addresses in the network segment is limited.	The value is an integer that ranges from 1 to 32.

Parameter	Description	Value
maximum *maximum*	Specifies the maximum number of ARP Miss messages based on the source IP address. **NOTE** If the maximum number of ARP Miss messages triggered by packets from each IP address is limited, a large value is recommended for this parameter because a small value may cause discarding of valid packets. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The integer form, in pps, is as follows: ● SS1720GW-E, S1720GWR-E, S2730S-S, S5720-LI, S5720S-LI: 0 to 2048 ● S5720I-SI, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M: 0 to 4096 ● S5735-S, S5735S-S, S5735-S-I: 0 to 8000 ● S5731-S, S5731S-S: 0 to 16384 ● S5731-H, S5731S-H: 0 to 61440 ● S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S: 0 to 65536 ● S5735S-H, S5736-S: 0 to 20000 ● S6735-S, S6720-EI, S6720S-EI: 0 to 131072 **NOTE** If the maximum rate of ARP Miss messages is set to 0, ARP Miss messages are not rate-limited based on source IP addresses.
none-block	Indicates that ARP Miss packets are processed in **none-block** mode. If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the CPU of the device discards the excess ARP Miss messages, that is, the CPU discards the excess ARP Miss packets.	-

Parameter	Description	Value
block timer *timer*	Indicates that ARP Miss packets are processed in **block** mode. If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device discards the excess ARP Miss messages and delivers an ACL to enable the chip to discard all packets that are sent from this source IP address within the period specified by *timer*. When the period specified by *timer* expires, the ACL ages out and the chip does not discard ARP Miss packets from the source IP address and sends them to the CPU for processing.	The value ranges from 5 to 864000, in seconds. The default value is 5 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack is initiated from the source IP address. If the ARP Miss message processing mode is set to **block**, the device discards excess ARP Miss packets from this source IP address and delivers an ACL to discard all subsequent packets sent from this source IP address. If the ARP Miss message processing mode is set to **none-block**, the device only discards excess ARP Miss packets.

The administrator can use the **arp-miss speed-limit source-ip** command to set the maximum number of ARP Miss packets and specify the mode for processing ARP Miss packets based on the actual network environment.

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack is initiated from the source IP address. The administrator can use the **arp-miss speed-limit source-ip** command to set the maximum number of ARP Miss messages that the device can process within a specified duration, protecting the system resources and ensuring proper running of other services.

Precautions

You can set the maximum number of ARP Miss messages for a maximum of 512 IP addresses.

If the ARP Miss packet processing mode is set to **none-block**, the device discards ARP Miss packets triggering excess ARP Miss messages to reduce CPU load. The non-block action can cause a high CPU usage, and the block action uses ACL resources. The default ARP Miss packet processing mode is recommended.

In the process of setting the maximum number of ARP Miss messages based on source IP addresses, if the ARP Miss packet processing mode is not specified, the device use the default processing mode **block**.

When the maximum number of ARP Miss packets exceeds the limit, the delivered ACL discards only the ARP Miss packets from the source IP address. Other packets can still be sent to the CPU.

A maximum of 16 ACLs can be delivered to the chip to discard ARP Miss packets from a specified IP address or network segment. When the device delivers 16 ACLs and all ACLs do not age out, and the number of ARP Miss packets from other IP addresses or network segments per second exceeds the limit, the device does not deliver any ACL to discard all subsequent packets and the CPU discards excess ARP packets.

NOTE

The S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S cannot deliver ACLs to discard ARP Miss packets.

Example

Set the maximum number of ARP Miss messages triggered by each source IP address per second to 60.

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip maximum 60
```

Set the maximum number of ARP Miss messages triggered by the IP address 10.0.0.1 per second to 100, and set the maximum number of ARP Miss messages triggered by other source IP addresses per second to 60.

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip maximum 60
[HUAWEI] arp-miss speed-limit source-ip 10.0.0.1 maximum 100
```

14.6.40 display arp anti-attack arpmiss-record-info

Function

The **display arp anti-attack arpmiss-record-info** command displays information recorded by the device when rate limit on ARP Miss messages is triggered.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display arp anti-attack arpmiss-record-info [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Displays the IP address of discarded ARP Miss packets.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After rate limit on ARP Miss messages is triggered, the device discards excess ARP Miss messages. You can run this command to view information recorded by the device when rate limit on ARP Miss messages is triggered. The information helps locate and rectify faults.

The device can record a maximum of 256 records about rate limit on ARP Miss messages. If a new round of rate limit on ARP Miss messages is triggered when the number of records reaches 256, the device takes the following actions:

1. If the source IP address of the attacker already exists in a record, the device updates the block time in the record using the discarding time of the new ARP Miss message.
2. If the source IP address of the attacker does not exist in any record, the device deletes the first record and adds a new record for this attacker.

Example

Display information recorded by the device when rate limit on ARP Miss messages is triggered.

```
<HUAWEI> display arp anti-attack arpmiss-record-info
Interface    IP address      Attack time          Block time          Aging-time
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
The number of record(s) in arp-miss table is 0
```

Table 14-44 Description of the display arp anti-attack arpmiss-record-info command output

Item	Description
Interface	Interface where ARP Miss packets are discarded.
IP address	Source IP address of discarded ARP Miss packets.
Attack time	First time when rate limit on ARP Miss messages is triggered, that is, time when the number of ARP Miss messages exceeds the limit.
Block time	Last time when the device discards the ARP Miss messages of the attacker.
Aging-time	Period during which the device discards ARP Miss packets. If the ARP Miss packet processing mode is set to **none-block**, the values of **Block time** and **Aging-time** are both 0. If the ARP Miss packet processing mode is set to **block**, the value of **Aging-time** is configured by the **arp-miss speed-limit source-ip** command, and the default value is 5 seconds.

14.6.41 display arp anti-attack configuration check user-bind

Function

The **display arp anti-attack configuration check user-bind** command displays the configuration of DAI in a VLAN or on an interface.

Format

display arp anti-attack configuration check user-bind [**vlan** [*vlan-id*] | **interface** [*interface-type interface-number*]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays DAI configuration in the specified VLAN. If *vlan-id* is not specified, the DAI configurations in all VLANs are displayed.	*vlan-id* is an integer that ranges from 1 to 4094.

Parameter	Description	Value
interface [*interface-type interface-number*]	Displays DAI on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If *interface-type interface-number* is not specified, the DAI configurations on all interfaces are displayed. If neither **vlan** [*vlan-id*] nor **interface** [*interface-type interface-number*] is specified, the DAI configurations in all VLANs and on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the configuration of DAI in a VLAN or on an interface, including whether the function is enabled, check items, whether the alarm function is enabled for discarded ARP packets, and alarm threshold.

Only after DAI and the alarm function are enabled, output of this command is displayed.

Example

Display DAI configuration on GE0/0/1.

```
<HUAWEI> display arp anti-attack configuration check user-bind interface gigabitethernet 0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 50
 arp anti-attack check user-bind check-item ip-address
```

Display ARP check configurations in all VLANs and on all interfaces.

```
<HUAWEI> display arp anti-attack configuration check user-bind
#
```

```
vlan 2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address
#
vlan 3
 arp anti-attack check user-bind enable
#
GigabitEthernet0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 50
 arp anti-attack check user-bind check-item ip-address
#
```

Table 14-45 Description of the display arp anti-attack configuration check user-bind command output

Item	Description
arp anti-attack check user-bind enable	DAI has been enabled. You can run the **arp anti-attack check user-bind enable** command to enable DAI.
arp anti-attack check user-bind alarm enable	The alarm function for ARP packets discarded by DAI has been enabled. You can run the **arp anti-attack check user-bind alarm enable** command to enable the alarm function.
arp anti-attack check user-bind alarm threshold 50	Alarm threshold of discarded ARP packets matching no binding entry. You can run the **arp anti-attack check user-bind alarm threshold** command to set the alarm threshold.
arp anti-attack check user-bind check-item ip-address	Only the IP address is checked during ARP packet check based on binding entries. You can run the **arp anti-attack check user-bind check-item** command or **arp anti-attack check user-bind check-item** command to specify the check item for ARP packet check based on binding entries.

14.6.42 display arp anti-attack configuration

Function

The **display arp anti-attack configuration** command displays the ARP anti-attack configuration.

Format

display arp anti-attack configuration { **arp-rate-limit** | **arp-speed-limit** | **entry-check** | **arpmiss-rate-limit** | **arpmiss-speed-limit** | **gateway-duplicate** | **log-trap-timer** | **packet-check** | **all** } (Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-

L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **arpmiss-rate-limit**, **arpmiss-speed-limit** and **gateway-duplicate**.)

Parameters

Parameter	Description	Value
arp-rate-limit	Displays the configuration of rate limit on ARP packets globally, in a VLAN, or on an interface.	-
arp-speed-limit	Displays the configuration of rate limit on ARP packets based on the source IP address or source MAC address.	-
entry-check	Displays the ARP entry fixing mode.	-
arpmiss-rate-limit	Displays the configuration of rate limit on ARP Miss messages globally, in a VLAN, or on an interface.	-
arpmiss-speed-limit	Displays the configuration of rate limit on ARP Miss messages based on the source IP address.	-
gateway-duplicate	Displays whether gateway anti-collision is enabled.	-
log-trap-timer	Displays the interval for sending ARP alarms.	-
packet-check	Displays whether ARP packet validity check is enabled.	-
all	Displays all ARP anti-attack configurations.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After all ARP anti-attack functions are configured, you can run this command to check all configurations.

Example

Display the configuration of rate limit on ARP packets based on the source IP address or source MAC address.

```
<HUAWEI> display arp anti-attack configuration arp-speed-limit
ARP speed-limit for source-MAC configuration:
MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 0
-------------------------------------------------------------------------------
The number of configured specified MAC address(es) is 0, spec is
512.
ARP speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
10.1.1.1            100
Others              0
-------------------------------------------------------------------------------
The number of configured specified IP address(es) is 1, spec is 512.
```

Display the configuration of rate limit on ARP Miss messages based on the source IP address.

```
<HUAWEI> display arp anti-attack configuration arpmiss-speed-limit
 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 -------------------------------------------------------------------------
 10.0.0.30/32        400
 Others              0
 -------------------------------------------------------------------------
 The number of configured specified IP address(es) is 1, spec is 512.
```

Display the ARP entry fixing mode.

```
<HUAWEI> display arp anti-attack configuration entry-check
 ARP anti-attack entry-check mode:
 Vlanif      Mode
-------------------------------------------------------------------------------
 All         send-ack
-------------------------------------------------------------------------------
```

Display all ARP anti-attack configurations.

```
<HUAWEI> display arp anti-attack configuration all
ARP anti-attack packet-check configuration:
-------------------------------------------------------------------------------
Sender-MAC checking function: disable
Dst-MAC checking function: disable
IP checking function: disable
-------------------------------------------------------------------------------

ARP gateway-duplicate anti-attack function: disabled

ARP anti-attack log-trap-timer: 0 second(s)
(The log and trap timer of speed-limit, default is 0 and means disabled.)

ARP anti-attack entry-check mode:
Vlanif      Mode
-------------------------------------------------------------------------------
```

```
All         disabled
-------------------------------------------------------------------------------

ARP rate-limit configuration:
-------------------------------------------------------------------------------
Global configuration:
Interface configuration:
  GigabitEthernet0/0/10 :
    arp anti-attack rate-limit enable
    arp anti-attack rate-limit packet 10 interval 1
VLAN configuration:
-------------------------------------------------------------------------------

ARP miss rate-limit configuration:
-------------------------------------------------------------------------------
Global configuration:
Interface configuration:
VLAN configuration:
-------------------------------------------------------------------------------

ARP speed-limit for source-MAC configuration:
MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 0
-------------------------------------------------------------------------------
The number of configured specified MAC address(es) is 0, spec is 512.

ARP speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 0
-------------------------------------------------------------------------------
The number of configured specified IP address(es) is 0, spec is 512.

ARP miss speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 500
-------------------------------------------------------------------------------
The number of configured specified IP address(es) is 0, spec is 512.
```

Table 14-46 Description of the display arp anti-attack configuration all command output

Item	Description
ARP anti-attack packet-check configuration	Whether ARP packet validity check is enabled. ● **Sender-mac checking function** indicates that the source MAC address is checked. ● **Dst-mac checking function** indicates that the destination MAC address is checked. ● **Ip checking function** indicates that the IP address is checked. You can run the **arp anti-attack packet-check** command to enable ARP packet validity check.
ARP gateway-duplicate anti-attack function	Whether ARP gateway anti-collision is enabled. You can run the **arp anti-attack gateway-duplicate enable** command to enable ARP gateway anti-collision.

Item	Description
ARP anti-attack log-trap-timer	Interval for sending ARP alarms You can run the **arp anti-attack log-trap-timer** command to set the interval for sending ARP alarms.
ARP anti-attack entry-check mode	ARP entry fixing mode. **Vlanif** specifies the interface to which the ARP entry fixing mode is applied. The modes include: - fixed-mac - fixed-all - send-ack - disabled You can run the **arp anti-attack entry-check enable** command to set the ARP entry fixing mode.
ARP rate-limit configuration	Configuration of rate limit on ARP packets. - **Global configuration** indicates the global configuration of rate limit on ARP packets. - **Interface configuration** indicates the configuration of rate limit on ARP packets on an interface. - **Vlan configuration** indicates the configuration of rate limit on ARP packets in a VLAN. You can run the **arp anti-attack rate-limit** command to configure rate limit on ARP packets.
ARP miss rate-limit configuration	Configuration of rate limit on ARP Miss messages. - **Global configuration** indicates the global configuration of rate limit on ARP Miss messages. - **Interface configuration** indicates the configuration of rate limit on ARP Miss messages on an interface. - **Vlan configuration** indicates the configuration of rate limit on ARP Miss messages in a VLAN. You can run the **anti-attack rate-limit** command to configure rate limit on ARP Miss messages.
ARP speed-limit for source-MAC configuration	Rate limit on ARP packets based on the source MAC address. You can run the **arp speed-limit source-mac** command to configure rate limit on ARP packets based on the source MAC address.
ARP speed-limit for source-IP configuration	Rate limit on ARP packets based on the source IP address. You can run the **arp speed-limit source-ip** command to configure rate limit on ARP packets based on the source IP address.

Item	Description
ARP miss speed-limit for source-IP configuration	Rate limit on ARP Miss messages based on source IP addresses. You can run the **arp-miss speed-limit source-ip** command to configure rate limit on ARP Miss messages based on the source IP address.
The number of configured specified MAC address(es) is 0, spec is 512.	Number (0) of the configured source MAC addresses based on which the rate of ARP packets or ARP Miss messages is limited, and the maximum value (512) allowed.
The number of configured specified IP address(es) is 1, spec is 512.	Number (1) of the configured source IP addresses based on which the rate of ARP packets or ARP Miss messages is limited, and the maximum value (512) allowed.
MAC-address	Rate limit on ARP packets based on a specified MAC address. ● **ALL** indicates all MAC addresses. ● **Others** indicates other MAC addresses except for the specified MAC address.
IP-address	Rate limit on ARP packets and ARP Miss messages based on a specified IP address. ● **ALL** indicates all IP addresses. ● **Others** indicates other IP addresses except for the specified IP address.
suppress-rate	Rate limit on ARP packets and ARP Miss messages. Value 0 indicates that the rate limit function is disabled for ARP packets and ARP Miss messages. You can run the **arp anti-attack rate-limit packet** *packet-number* command to configure the rate limit of ARP packets, and run the **arp-miss anti-attack rate-limit packet** *packet-number* command to configure the rate limit of ARP Miss messages.

14.6.43 display arp anti-attack gateway-duplicate item

Function

The **display arp anti-attack gateway-duplicate item** command displays ARP gateway anti-collision entries.

Format

display arp anti-attack gateway-duplicate item

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP gateway anti-collision is enabled, you can run this command to view ARP anti-collision entries.

Example

Display ARP gateway anti-collision entries.

```
<HUAWEI> display arp anti-attack gateway-duplicate item
 Interface              IP address       MAC address      VLANID   Aging time
-------------------------------------------------------------------------------
 GigabitEthernet0/0/1    10.1.1.1         00e0-fc12-3456  2        150
 GigabitEthernet0/0/2    10.1.1.2         00e0-fc12-3478  2        170
-------------------------------------------------------------------------------
The number of record(s) in gateway conflict table is 2
```

Table 14-47 Description of the display arp anti-attack gateway-duplicate item command output

Item	Description
Interface	Inbound interface of ARP packets.
IP address	IP address of the gateway.
MAC address	Source MAC address of ARP packets.
VLANID	VLAN ID of ARP packets.
Aging time	Aging time of entries. The maximum value is 180 seconds. This parameter cannot be configured.

14.6.44 display arp anti-attack packet-check statistics

Function

The **display arp anti-attack packet-check statistics** command displays the statistics on invalid ARP packets that are filtered out during ARP packet validity check.

Format

display arp anti-attack packet-check statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP packet validity check is enabled, if you want to view the statistics on invalid ARP packets that are filtered out, you can run this command.

Example

Display the statistics on invalid ARP packets that are filtered out in ARP packet validity check is displayed.

```
<HUAWEI> display arp anti-attack packet-check statistics
Number of ARP packet(s) checked:                        5
Number of ARP packet(s) dropped by sender-mac checking: 0
Number of ARP packet(s) dropped by dst-mac checking:    0
Number of ARP packet(s) dropped by src-ip checking:     2
Number of ARP packet(s) dropped by dst-ip checking:     0
```

Table 14-48 Description of the display arp anti-attack packet-check statistics command output

Item	Description
Number of ARP packet(s) checked	Number of ARP packets whose validity is checked.
Number of ARP packet(s) dropped by sender-mac checking	Number of invalid ARP packets that are filtered out because the source MAC address in the packet is different from that in the Ethernet frame header.
Number of ARP packet(s) dropped by dst-mac checking	Number of invalid ARP packets that are filtered out because the destination MAC address in the packet is different from that in the Ethernet frame header.
Number of ARP packet(s) dropped by src-ip checking	Number of invalid ARP packets with invalid source IP addresses that are filtered out.

Item	Description
Number of ARP packet(s) dropped by dst-ip checking	Number of invalid ARP packets with invalid destination IP addresses that are filtered out.

14.6.45 display arp anti-attack statistics check user-bind interface

Function

The **display arp anti-attack statistics check user-bind interface** command displays the statistics on discarded ARP packets matching no binding entry.

Format

display arp anti-attack statistics check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. Where, ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After dynamic ARP inspection (DAI) is enabled in the interface view, you can run this command to check statistics about discarded ARP packets matching no binding entry on the interface. If the alarm function for ARP packets discarded by

DAI is enabled, you can also check statistics about discarded ARP packets matching no binding entry on the interface after the latest alarm is generated.

Precautions

- If DAI is enabled only in the VLAN view, this command cannot be run to display statistics about discarded ARP packets matching no binding entry on the interfaces in the VLAN.
- This command cannot check statistics about discarded ARP packets matching no binding entry on the management interface.

Example

Display the statistics on discarded ARP packets matching no binding entry on GE0/0/1.

```
<HUAWEI> display arp anti-attack statistics check user-bind interface gigabitethernet 0/0/1
 Dropped ARP packet number is 966
 Dropped ARP packet number since the latest warning is 605
```

Table 14-49 Description of the display arp anti-attack statistics check user-bind interface command output

Item	Description
Dropped ARP packet number is 966	Number of discarded ARP packets matching no DHCP snooping binding entry.
Dropped ARP packet number since latest warning is 605	Statistics on discarded ARP packets matching no DHCP snooping binding entry after the latest alarm is generated.

14.6.46 display arp learning strict

Function

The **display arp learning strict** command displays strict ARP learning globally and on all interfaces.

Format

display arp learning strict

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After strict ARP learning is configured, you can run this command to check the configuration.

Example

Display strict ARP learning globally and on all interfaces.

```
<HUAWEI> display arp learning strict
The global configuration:arp learning strict
 Interface                          LearningStrictState
------------------------------------------------------------
 Vlanif100                          force-disable
 Vlanif200                          force-enable
------------------------------------------------------------
 Total:2
 Force-enable:1
 Force-disable:1
```

Table 14-50 Description of the display arp learning strict command output

Item	Description
The global configuration	Global strict ARP learning. The value **arp learning strict** indicates that strict ARP learning has been enabled. If the parameter is left blank, strict ARP learning is disabled. You can run the **arp learning strict** command to enable strict ARP learning.
Interface	Interface name.
LearningStrictState	Strict ARP learning. ● The value **force-enable** indicates that strict ARP learning is enabled. ● The value **force-disable** indicates that strict ARP learning is disabled. You can run the **arp learning strict** command to enable strict ARP learning.
Total	Total number of interfaces to which strict ARP learning is applied.
Force-enable	Number of the interfaces on which strict ARP learning is enabled.
Force-disable	Number of the interfaces on which strict ARP learning is disabled.

14.6.47 display arp optimized-passby status

Function

The **display arp optimized-passby status** command displays whether the device is configured not to send ARP packets destined for other devices to the CPU and whether the configuration takes effect.

Format

display arp optimized-passby status interface vlanif *vlanif-id* **slot** *slot-id*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
interface vlanif *vlanif-id*	Displays whether the device is configured not to send ARP packets destined for other devices to the CPU and whether the configuration takes effect on a specified VLANIF interface.	The value is an integer and the value range depends on the range of existing VLANIF interfaces. You can enter ? to obtain the range of VLANIF interface numbers.
slot *slot-id*	Displays whether the device is configured not to send ARP packets destined for other devices to the CPU and whether the configuration takes effect in a specified slot.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an interface receives a large number of ARP packets whose destination IP addresses are different from the IP address of this interface and sends these ARP packets to the CPU for processing, the CPU usage is high and the CPU cannot process services properly.

To prevent this issue, you can configure the device to directly forward ARP packets destined for other devices without sending them to the CPU. This improves the device's capability of defending against ARP flood attacks.

When the device is configured not to send ARP packets destined for other devices to the CPU, the configuration does not take effect if a conflict configuration exists on the device. You can use the **display arp optimized-passby status** command to check whether the device is configured not to send ARP packets destined for other devices to the CPU and whether the configuration takes effect. For details about conflict configurations, see **arp optimized-passby enable**.

Example

Display whether the device is configured not to send ARP packets destined for other devices to the CPU and whether the configuration takes effect on VLANIF 100.

```
<HUAWEI> display arp optimized-passby status interface Vlanif 100 slot 0
Current configuration:Enable
Actual        status:Inactive
Related configuration:
   NAC configuration (for example, dot1x enable)
```

Table 14-51 Description of the **display arp optimized-passby status** command output

Item	Description
Current configuration	Whether the device is configured not to send ARP packets destined for other devices to the CPU. ● Enable: The device is configured not to send ARP packets destined for other devices to the CPU. ● Disable: The device is configured to send ARP packets destined for other devices to the CPU.
Actual status	Whether the configuration of disabling the device from sending ARP packets destined for other devices to the CPU takes effect. ● Inactive ● Active
Related configuration	Conflict configuration. For details, see **arp optimized-passby enable**.

14.6.48 display arp optimized-reply statistics

Function

The **display arp optimized-reply statistics** command displays statistics on optimized ARP Reply packets.

Format

display arp optimized-reply statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- This parameter specifies the slot ID if stacking is not configured. - This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on optimized ARP Reply packets after the optimized ARP reply function is enabled on the device.

Example

Display statistics on optimized ARP Reply packets.

```
<HUAWEI> display arp optimized-reply statistics
Slot           Received          Processed            Dropped
---------------------------------------------------------------
0                    11                 9                 7
```

Table 14-52 Description of the display arp optimized-reply statistics command output

Item	Description
Slot	Stack ID.
Received	Number of ARP Request packets entering the processing procedure of the optimized ARP reply function.
Processed	Number of optimized ARP Reply packets.
Dropped	Number of ARP Request packets discarded.

14.6.49 display arp optimized-reply status

Function

The **display arp optimized-reply status** command displays the status of the optimized ARP reply function.

Format

display arp optimized-reply status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the status of the optimized ARP reply function.

Example

Check the status of the optimized ARP reply function.

```
<HUAWEI> display arp optimized-reply status
Current configuration:Disable
Actual         status:Inactive
Related configuration:
   arp optimized-reply disable
   arp anti-attack check user-bind enable
   arp anti-attack gateway-duplicate enable
```

Table 14-53 Description of the display arp optimized-reply status command output

Item	Description
Current configuration	Configuration of the optimized ARP reply function. - Enable - Disable To set this field, run the **arp optimized-reply disable** command.

Item	Description
Actual status	Status of the optimized ARP reply function. - Active - Inactive
Related configuration	Configuration that results in the invalid optimized ARP reply function. If the optimized ARP reply function has taken effect, this field is not displayed.

14.6.50 display arp packet statistics

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to view the statistics on ARP packets.

This command displays the ARP packet statistics on the active switch in a stack system.

Example

Display the statistics on ARP packets.

```
<HUAWEI> display arp packet statistics
ARP Pkt Received: sum 420066
ARP Received In Message-cache: sum 0
ARP-Miss Msg Received: sum 0
ARP Learnt Count: sum 5
ARP Pkt Discard For Limit: sum 0
ARP Pkt Discard For SpeedLimit: sum 0
```

```
ARP Pkt Discard For Proxy Suppress: sum 179578
ARP Pkt Discard For Other: sum 90347
ARP-Miss Msg Discard For SpeedLimit: sum 0
ARP Discard In Message-cache For SpeedLimit: sum 0
ARP-Miss Msg Discard For Other: sum 0
```

Table 14-54 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Received In Message-cache	Number of ARP packets received within each second when a switch encapsulates multiple ARP request packets into one packet.
ARP-Miss Msg Received	Total number of ARP Miss messages triggered by ARP Miss packets sent to the CPU.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit. To configure the maximum number of dynamic ARP entries that an interface can learn, run the **arp-limit** command.
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit. To configure a rate limit for ARP packets based on the source IP address, run the **arp speed-limit source-ip** command.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.
ARP-Miss Msg Discard For SpeedLimit	Number of ARP Miss messages discarded when the number of ARP Miss messages triggered by IP packets from a specified source IP address exceeds the limit.
ARP Discard In Message-cache For SpeedLimit	Number of ARP packets discarded due to software rate limit when a switch encapsulates multiple ARP request packets into one packet. To configure a rate limit for ARP Miss messages based on the source IP address, run the **arp-miss speed-limit source-ip** command.

Item	Description
ARP-Miss Msg Discard For Other	Number of the ARP Miss messages discarded due to other causes.

14.6.51 display arp-limit

Function

The **display arp-limit** command displays the maximum number of ARP entries that an interface can dynamically learn.

Format

display arp-limit [**interface** *interface-type interface-number*[*.subinterface-number*]] [**vlan** *vlan-id*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interface.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*[*.subinterface-number*]	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. • *subinterface-number* specifies the sub-interface number.	-
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the maximum number of ARP entries that an interface can dynamically learn is set, you can run this command to check the configuration.

If **interface** *interface-type interface-number*[*.subinterface-number*] and **vlan** *vlan-id* are specified, you can view the maximum number of ARP entries that the specified interface can dynamically learn in the specified VLAN. If the two parameters are not specified, the maximum number of ARP entries that each interface can dynamically learn is displayed.

Example

Display the number of ARP entries that each interface can dynamically learn.

```
<HUAWEI> display arp-limit
 Interface              LimitNum       VlanID         LearnedNum(Mainboard)
-------------------------------------------------------------------------
 Vlanif100              1000          0                0
 GigabitEthernet0/0/1    16384          10               0
 -------------------------------------------------------------------------
 Total:2
```

Table 14-55 Description of the display arp-limit command output

Item	Description
Interface	Interface name.
LimitNum	Maximum number of ARP entries that an interface can dynamically learn. To configure the maximum number of dynamic ARP entries that an interface can learn, run the **arp-limit** command.
VlanID	ID of the VLAN that the interface belongs to.
LearnedNum(Mainboard)	Number of ARP entries that an interface has learned.

14.6.52 display arp-miss speed-limit source-ip

Function

The **display arp-miss speed-limit source-ip** command displays the configuration of rate limit on ARP Miss message based on the source IP address.

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display arp-miss speed-limit source-ip

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP Miss rate limiting based on source IP address is configured, you can run this command to check the configuration.

Example

Display the configuration of rate limit on ARP Miss messages based on the source IP address.

```
<HUAWEI> display arp-miss speed-limit source-ip
 Slot     SuppressType   SuppressValue
 ---------------------------------------------------
 0        ARP-miss       600
```

Table 14-56 Description of the display arp-miss speed-limit source-ip command output

Item	Description
Slot	- The value indicates the slot ID if stacking is not configured. - The value indicates the stack ID if stacking is configured.
SuppressType	Suppression type.

Item	Description
SuppressValue	Maximum rate of ARP Miss messages from a specified source IP address. To configure a rate limit for ARP Miss messages based on the source IP address, run the **arp-miss speed-limit source-ip** command.

14.6.53 display arp snooping

Function

The **display arp snooping** command displays ARP snooping entries.

Format

display arp snooping { **all** \| **interface** *interface-type interface-number* \| **vlan** *vlan-id* \| **ip-address** *ip-address* \| **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays all ARP snooping entries.	-
interface *interface-type interface-number*	Displays the ARP snooping entry of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays the ARP snooping entry of a specified VLAN.	The value is an integer in the range from 1 to 4094.
ip-address *ip-address*	Displays the ARP snooping entry of a specified IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
mac-address *mac-address*	Displays the ARP snooping entry of a specified MAC address.	The value is a 12-digit hexadecimal number, in the format of H-H-H. Each H is 4 digits. If an H contains fewer than 4 digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP snooping is enabled, the device generates ARP snooping entries that contain the IP address, MAC address, VLAN ID, inbound interface, and aging time. You can run the **display arp snooping** command to view the ARP snooping entries.

Example

Display all ARP snooping entries.

```
<HUAWEI> display arp snooping all
VLAN/CEVLAN     IP ADDRESS     MAC ADDRESS     INTERFACE     EXPIRE(S)
---------------------------------------------------------------------
2/-            192.168.10.1   xxxx-xxxx-xxx1  Eth1/0/0      20
2/-            192.168.10.2   xxxx-xxxx-xxx2  Eth1/0/0      10
13/-            10.1.1.1       xxxx-xxxx-xxx3  Eth-Trunk0    18
12/10            172.16.1.1     xxxx-xxxx-xxx4  40GE5/0/4     5
---------------------------------------------------------------------
Total Count:4
```

Table 14-57 Description of the **display arp snooping** command output

Item	Description
VLAN/CEVLAN	VLAN information.
IP ADDRESS	IP address.
MAC ADDRESS	MAC address.

Item	Description
INTERFACE	Inbound interface.
EXPIRE(S)	Aging time.

14.6.54 reset arp anti-attack packet-check statistics

Function

The **reset arp anti-attack packet-check statistics** command clears the statistics on invalid ARP packets that are filtered out during ARP packet validity check.

Format

reset arp anti-attack packet-check statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to clear existing statistics, and run the **display arp anti-attack packet-check statistics** command to view the statistics on follow-up invalid ARP packets that are filtered out.

Example

Clear the statistics on invalid ARP packets that are filtered out in ARP packet validity check.

```
<HUAWEI> reset arp anti-attack packet-check statistics
```

14.6.55 reset arp anti-attack statistics check user-bind

Function

The **reset arp anti-attack statistics check user-bind** command clears the statistics on discarded ARP packets matching no binding entry.

Format

reset arp anti-attack statistics check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. Where, - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

User view, system view

Default Level

2: Configuration level

Usage Guidelines

After DAI is enabled and some ARP packets matching no binding entry are discarded, you can run this command to clear the statistics on the discarded ARP packets.

Example

Clear the statistics on discarded ARP packets on GE0/0/1.

```
<HUAWEI> reset arp anti-attack statistics check user-bind interface gigabitethernet 0/0/1
```

14.6.56 reset arp anti-attack statistics rate-limit

Function

The **reset arp anti-attack statistics rate-limit** command clears the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit.

Format

reset arp anti-attack statistics rate-limit

Parameters

None

Views

User view, system view

Default Level

2: Configuration level

Usage Guidelines

After rate limit on ARP packets is enabled globally, the device discards the excess packets when the rate of ARP packets exceeds the limit. You can run this command to clear the statistics on the discarded ARP packets.

Example

Clear the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit.

```
<HUAWEI> reset arp anti-attack statistics rate-limit
```

14.6.57 reset arp optimized-reply statistics

Function

The **reset arp optimized-reply statistics** command clears statistics on optimized ARP Reply packets.

Format

reset arp optimized-reply statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value must be set according to the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To collect statistics on optimized ARP Reply packets on the device, you can run the **reset arp optimized-reply statistics** [**slot** *slot-id*] command to clear statistics on optimized ARP Reply packets of the device.

Example

Clears statistics on optimized ARP Reply packets.

```
<HUAWEI> reset arp optimized-reply statistics
```

14.6.58 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics on the active switch in a stack system.

Example

Clear the statistics on all ARP packets.

```
<HUAWEI> reset arp packet statistics
```

14.6.59 reset arp snooping

Function

The **reset arp snooping** command clears ARP snooping entries.

Format

reset arp snooping { **all** | **interface** *interface-type interface-number* | **vlan** *vlan-id* | **ip-address** *ip-address* | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears all ARP snooping entries.	-
interface *interface-type interface-number*	Clears ARP snooping entries on an interface that has the specified interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Clears ARP snooping entries in a specified VLAN.	The value is an integer in the range from 1 to 4094.
ip-address *ip-address*	Clears ARP snooping entries of the specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Clears ARP snooping entries of the specified MAC address.	The value is in H-H-H format, in which H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four alphanumeric characters, 0s are added before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, and a multicast MAC address.

Views

User view

Default Level

3: Management level

Usage Guidelines

To view ARP snooping entries in a specified period, you need to generate new ARP snooping entries from a specified time. You can run the **reset arp snooping** command to clear ARP snooping entries.

Example

Clear ARP snooping entries.

```
<HUAWEI> reset arp snooping all
```

14.7 Port Security Configuration Commands

14.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.7.2 display mac-address sec-config

Function

The **display mac-address sec-config** command displays secure static MAC address entries.

Format

display mac-address sec-config [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the secure static MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays the secure static MAC address entries on a specified interface.	-

Parameter	Description	Value
verbose	Displays detailed information about secure static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After secure static MAC address entries are configured by the command **port-security mac-address**, you can run the **display mac-address sec-config** command to check these entries.

Example

Display all secure static MAC address entries.

```
<HUAWEI> display mac-address sec-config
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                   Learned-From        Type
-------------------------------------------------------------------------------
xxxx-xxxx-xxx1 100/-/-                       GE0/0/1             sec-config

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-58 Description of the display mac-address sec-config command output

Item	Description
MAC Address	Destination MAC address in a secure static MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or the ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **sec-config**, which indicates a secure static MAC address.

14.7.3 display mac-address security

Function

The **display mac-address security** command displays secure dynamic MAC address entries.

Format

display mac-address security [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays secure dynamic MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays secure dynamic MAC address entries with a specified outbound interface. - *interface-type* specifies the type of the outbound interface. - *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about secure dynamic MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface by using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. The learned secure dynamic MAC address entries are deleted after the device restarts.

After configuring the port security function, you can run the **display mac-address security** command to check whether the learned secure dynamic MAC address entries are correct.

Follow-up Procedure

If the displayed secure dynamic MAC address entries are invalid, run the **undo mac-address security** command to delete secure dynamic MUX MAC address entries.

Precautions

If you run the **display mac-address security** command without parameters, all secure dynamic MAC address entries are displayed.

If the MAC address table does not contain any secure dynamic MAC address entry, no information is displayed.

When the device has a large number of secure dynamic MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all secure dynamic MAC address entries.

```
<HUAWEI> display mac-address security
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                   Learned-From        Type
-------------------------------------------------------------------------------
xxxx-xxxx-xxx1 100/-/-                       GE0/0/1             security
xxxx-xxxx-xxx2 200/-/-                       GE0/0/2             security

-------------------------------------------------------------------------------
Total items displayed = 2
```

Display detailed information about all secure dynamic MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address security vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : xxxx-xxxx-xxx1          VLAN : 10
Learned-From: GE0/0/1               Type : security
Aging-Time  : 200s

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-59 Description of the display mac-address security command output

Item	Description
MAC Address	Destination MAC address in a secure dynamic MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or the ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **security**, which indicates a secure dynamic MAC address.
Aging-Time	How soon a secure dynamic MAC address entry will be aged out.

14.7.4 display mac-address sticky

Function

The **display mac-address sticky** command displays sticky VLAN MAC address entries.

Format

display mac-address sticky [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays sticky MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays sticky MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-

Parameter	Description	Value
verbose	Displays detailed information about sticky MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

After port security is enabled on an interface by using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. The learned secure dynamic MAC address entries are deleted after the switch restarts. If the sticky MAC function is also enabled on the interface by using the **port-security mac-address sticky** command, secure dynamic MAC address entries change to sticky MAC address entries. Sticky MAC address entries are not deleted after the switch restarts.

To check the sticky MAC configuration or the learned sticky MAC address entries, run the **display mac-address sticky** command.

Follow-up Procedure

If the displayed sticky MAC address entries are invalid, run the **undo mac-address sticky** command to delete sticky MAC address entries.

Precautions

If you run the **display mac-address sticky** command without parameters, all sticky MAC address entries are displayed.

If the MAC address table does not contain any sticky MAC address, no information is displayed.

When the switch has a large number of sticky MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.

- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all sticky MAC address entries.

```
<HUAWEI> display mac-address sticky
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                    Learned-From        Type
-------------------------------------------------------------------------------
xxxx-xxxx-xxx1 100/-/-                        GE0/0/1             sticky
xxxx-xxxx-xxx2 200/-/-                        GE0/0/2             sticky

-------------------------------------------------------------------------------
Total items displayed = 2
```

Display detailed information about all sticky MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address sticky vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : xxxx-xxxx-xxx1           VLAN : 10
Learned-From: GE0/0/1                 Type : sticky

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-60 Description of the display mac-address sticky command output

Item	Description
MAC Address	MAC address in a sticky MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or the ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **sticky**, which indicates a sticky MAC address.

14.7.5 display mac-address sticky-config

Function

The **display mac-address sticky-config** command displays MAC address entries of the Sticky-Config type.

Format

display mac-address sticky-config [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN.	The value is an integer in the range from 1 to 4094.
interface-type interface-number	Displays MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After secure static MAC address entries are configured using the **port-security mac-address sticky-config** command, you can run the **display mac-address sticky-config** command to check these entries.

Follow-up Procedure

After you run this command to check MAC address entries of the Sticky-Config type and consider that a MAC address entry is invalid, you can run the **undo port-security mac-address** [**sticky-config**] *mac-address* **vlan** *vlan-id* command to delete it.

Precautions

If you run the **display mac-address sticky-config** command without specifying any parameters, all MAC address entries of the Sticky-Config type are displayed.

If the MAC address table does not contain any MAC address of the Sticky-Config type, no information is displayed in the command output.

When the device has a large number of MAC address entries of the Sticky-Config type, it is recommended that you specify parameters in the command to filter the output information. If you do not specify these parameters, the following faults may occur:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all MAC address entries of the Sticky-Config type.

```
<HUAWEI> display mac-address sticky-config
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                    Learned-From        Type
-------------------------------------------------------------------------------
0022-0022-0033 100/-/-                      GE0/0/1            sticky-config
0000-0000-0001 200/-/-                      GE0/0/2            sticky-config
-------------------------------------------------------------------------------
Total items displayed = 2
```

Display detailed information about all MAC address entries of the Sticky-Config type in VLAN 10.

```
<HUAWEI> display mac-address sticky-config vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 0000-0000-0001           VLAN : 10
Learned-From: GE0/0/1                  Type : sticky-config

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-61 Description of the **display mac-address sticky-config** command output

Item	Description
MAC Address	MAC address in a MAC address entry of the Sticky-Config type.
VLAN/VSI/BD	ID of the VLAN, name of the virtual switch instance (VSI), or ID of the BD to which the MAC address belongs.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **sticky-config**, which indicates a MAC address of the Sticky-Config type.

14.7.6 display port-security

Function

The **display port-security** command displays the port security configuration.

Format

display port-security [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the port security configuration on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view information about interfaces configured with port security, including the number of MAC addresses that can be learned, number of learned MAC addresses, and actions configured on the interfaces.

After an interface enters the error-down state, you need to check the traffic that triggers this state. To facilitate troubleshooting, you can run this command to view the MAC address of the end user that triggers the error-down state of the interface and the VLAN to which the end user belongs.

Example

Display the port security configuration.

```
<HUAWEI> display port-security
Interface        MaxMacNum  CurrentMacNum  ProtectAction
InSecureMac:Vlan
Eth-Trunk17      1          0              Restrict       -
GE0/0/1     1          0            Shutdown       xxxx-xxxx-xxxx:100
GE0/0/2     1          0            Protect        -
```

Table 14-62 Description of the **display port-security** command output

Item	Description
Interface	Interface name.
MaxMacNum	Maximum number of MAC addresses that can be learned by the interface.
CurrentMacNum	Number of MAC addresses that have been learned by the interface.
ProtectAction	Action configured on the interface, which can be configured using the **port-security protect-action** command. Actions include: ● **Protect**: indicates that packets are discarded. ● **Restrict**: indicates that packets are discarded and a trap is generated. ● **Shutdown**: indicates that the interface is set to the error-down state and a trap is generated.
InSecureMac:Vlan	MAC address of the end user that triggers the **Shutdown** action and the VLAN to which the end user belongs after the action is set to **Shutdown**.

14.7.7 port-security aging-time

Function

The **port-security aging-time** command sets the aging time of secure dynamic MAC addresses on an interface.

The **undo port-security aging-time** command restores the default configuration.

By default, secure dynamic MAC addresses will not be aged out.

Format

port-security aging-time *time* [**type** { **absolute** | **inactivity** }]

undo port-security aging-time

NOTE

The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I do not support **inactivity** parameter.

Parameters

Parameter	Description	Value
time	Specifies the aging time of secure dynamic MAC addresses.	The value is an integer that ranges from 1 to 1440, in minutes.
type	Specifies the type of the aging time.	The default type is **absolute**, indicating the absolute aging time.
absolute	Indicates the absolute aging time. After the aging time of secure dynamic MAC addresses is set, the system calculates the lifetime of each MAC address every minute. If the lifetime of a MAC address plus 1 is greater than or equal to *time* minutes, the secure dynamic MAC address is aged immediately. If the lifetime is smaller than *time* minutes, the system determines whether to delete the secure dynamic MAC address after 1 minute.	-
inactivity	Indicates the relative aging time. After the relative aging time is set to *time* minutes, the system checks traffic from each secure dynamic MAC address every 1 minute. If there is traffic, the aging is not performed. If no traffic is received from a secure dynamic MAC address, this MAC address is aged out after *time* minutes.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **port-security enable** command to enable port security on an interface, MAC address entries learned by the interface are saved in the MAC address table as secure dynamic MAC addresses. The learned secure dynamic MAC addresses will not be aged by default. When the number of learned MAC addresses reaches the limit, the interface cannot learn new MAC addresses.

If MAC addresses learned by an interface can be trusted only for a certain period, run the **port-security aging-time** command to set the aging time of secure dynamic MAC addresses on the interface. Then secure dynamic MAC addresses can be aged out and the interface can learn new MAC addresses.

Prerequisites

Port security is enabled on the interface.

Precautions

If you run the **port-security aging-time** command multiple times in the same interface view, only the latest configuration takes effect.

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S: After an interface learns the secure dynamic MAC address of a user, the user connects to another interface (the original interface does not go Down) and the other interfaces continuously receive traffic with the source MAC address. The MAC address of the original interface is not aged out. As a result, the user cannot connect to the interface again. To solve this problem, you can set the aging time of secure dynamic MAC addresses on the interface.

Example

Set the aging time of secure dynamic MAC addresses on GE0/0/1 to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security aging-time 30
```

14.7.8 port-security enable

Function

The **port-security enable** command enables the port security function on an interface.

The **undo port-security enable** command disables the port security function on an interface.

By default, port security is disabled on an interface.

Format

port-security enable

undo port-security enable

Parameters

None

Views

GE interface view, Ethernet interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. By default, secure dynamic MAC addresses will not be aged out. If the aging time of secure dynamic MAC address entries is set, these entries will be aged out. After the device restarts, secure dynamic MAC address entries are lost and need to be relearned. You can also create secure static MAC addresses which do not age out.

Port security has the following functions:

- Prevent unauthorized guests from using their computers to connect to an enterprise network.
- Prevent employees of a company from moving their computers without permission.

Precautions

- The total number of MAC addresses on interfaces enabled with port security cannot exceed 4096. For example, if the numbers of MAC addresses learned on interfaces 1, 2, 3, and 4 are 1000 respectively, interface 5 can learn a maximum of 96 MAC addresses.
- The protection action, secure static MAC addresses, and sticky MAC function can be configured only after port security is enabled.
- Port security and MAC address limiting conflict on an interface; therefore, the **port-security enable** and **mac-limit maximum** commands cannot be used on the same interface.
- Port security and MUX VLAN conflict on an interface; therefore, the **port-security enable** and **port mux-vlan enable** commands are not advised to be used on the same interface.

- Port security and GVRP conflict on an interface; therefore, the **port-security enable** and **gvrp** commands cannot be used on the same interface.
- Port security and generating snooping MAC entries conflict on an interface; therefore, the **port-security enable** and **user-bind ip sticky-mac** commands cannot be used on the same interface.
- If port security is enabled after MAC address learning is disabled using the **mac-address learning disable** command, the dynamic port security function does not take effect. If port security is enabled before MAC address learning is disabled on an interface, the device no longer learns MAC addresses on the interface, but secure MAC addresses that have been learned are reserved (including secure static MAC addresses).
- When multiple NAC users are online under one interface, if you want to enable port security function on the interface, you need to first run the **port-security max-mac-num** command to set the maximum number of MAC addresses learned by the interface, and then run the **port-security enable** command. Otherwise, only one user is reserved and other users are logged out.
- When both NAC authentication and port security are enabled on an interface, MAC addresses that fail to be authenticated are not converted to secure MAC addresses. Instead, they are learned as authentication MAC addresses on the interface. After authentication succeeds, the MAC addresses are converted to secure MAC addresses.

Example

Enable port security on GigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] port-security enable
```

14.7.9 port-security mac-address

Function

The **port-security mac-address** command configures a static secure MAC address.

The **undo port-security mac-address** command deletes a static secure MAC address.

By default, no static secure MAC address is configured.

Format

port-security mac-address *mac-address* **vlan** *vlan-id*

undo port-security mac-address *mac-address* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a static secure MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits. The value cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer in the range from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view,MultiGE interface view,40GE interface view,100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries.

When the interface becomes Down or the device is reset, static secure MAC addresses are not affected, and dynamic secure MAC addresses need to be learned again. Static secure MAC addresses are not aged out. Static secure MAC addresses have a higher priority than dynamic secure MAC addresses.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

Running the **port-security mac-address** *mac-address* **vlan** *vlan-id* command multiple times configures multiple static secure MAC addresses.

A static secure MAC address cannot be a VRRP virtual MAC address or system MAC address.

Example

Configure a static secure MAC address entry on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security mac-address 00e0-fc12-3456 vlan 10
```

14.7.10 port-security mac-address sticky-config

Function

The **port-security mac-address** command configures a static secure MAC address of the Sticky-Config type.

The **undo port-security mac-address** command deletes a static secure MAC address of the Sticky-Config type.

By default, no static secure MAC address of the Sticky-Config type is configured.

Format

port-security mac-address sticky-config *mac-address* **vlan** *vlan-id*

undo port-security mac-address sticky-config *mac-address* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a static secure MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits. The value cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer in the range from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view,MultiGE interface view,40GE interface view,100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries.

When the interface becomes Down or the device is reset, static secure MAC addresses are not affected, and dynamic secure MAC addresses need to be learned again. Static secure MAC addresses are not aged out. Static secure MAC addresses have higher priority than dynamic secure MAC addresses. You can run this command to configure a static secure MAC address of the Sticky-Config type.

Prerequisites

1. Port security has been enabled using the **port-security enable** command.
2. The sticky MAC function on an interface has been enabled using the **port-security mac-address sticky** command.

Precautions

You can manually configure one or more static secure MAC address entries of the Sticky-Config type. You run the **port-security mac-address sticky-config** *mac-address* **vlan** *vlan-id* command multiple times to configure multiple static secure MAC address entries of the Sticky-Config type.

A static secure MAC address of the Sticky-Config type cannot be a VRRP virtual MAC address or a system MAC address.

Example

Configure a static secure MAC address entry of the Sticky-Config type on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security mac-address sticky
[HUAWEI-GigabitEthernet0/0/1] port-security mac-address sticky-config 00e0-fc12-3456 vlan 10
```

14.7.11 port-security mac-address sticky

Function

The **port-security mac-address sticky** command enables the sticky MAC function on an interface.

The **undo port-security mac-address sticky** command disables the sticky MAC function on an interface.

By default, the sticky MAC function is disabled on an interface.

Format

port-security mac-address sticky [*mac-address* **vlan** *vlan-id*]

undo port-security mac-address sticky [*mac-address* **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a sticky MAC address entry. **NOTE** This parameter is not supported in the port group view.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits. A MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN. **NOTE** This parameter is not supported in the port group view.	The value is an integer in the range from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view,MultiGE interface view,40GE interface view,100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries.

After the sticky MAC function is enabled on an interface, the dynamic MAC addresses learned by the interface change to sticky MAC addresses.

Before the number of sticky MAC addresses reaches the limit on the interface, the MAC addresses learned subsequently are still converted into sticky MAC addresses. When the number of sticky MAC addresses reaches the limit, non-sticky MAC addresses are discarded. In addition, the system determines whether to send a trap message based on the configuration of the interface protection mode.

After enabling the sticky MAC function on an interface using the **port-security mac-address sticky** command, you can run the **port-security mac-address sticky** *mac-address* **vlan** *vlan-id* command to manually configure a sticky MAC address entry.

The sticky MAC function has the following functions:

- Prevent non-employees from using their own computers to access the company intranet without the permission of the network administrator.
- Prevent employees from moving network devices or computers of the company without the permission of the network administrator.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

Running the **undo port-security mac-address sticky** command will convert the sticky MAC addresses on the interface into secure dynamic MAC addresses.

The configuration information is not displayed after you run the **port-security mac-address sticky** *mac-address* **vlan** *vlan-id* command to configure sticky MAC address entries.

Manually configured and auto-generated sticky MAC address entries are automatically saved in a .ztbl or .ctbl file every 10 minutes. Alternatively, you can run the **save** command to manually save them. The saved file is not discarded after the device restarts. The file name must be the same as that of the system configuration file. For example, if the name of the system configuration file is test.cfg, the name of the sticky MAC address entry file must be test.ctbl. Otherwise, sticky MAC address entries will fail to be restored after the device restarts.

If you run the **port-security mac-address sticky** *mac-address* **vlan** *vlan-id* command multiple times, multiple sticky MAC address entries are configured.

A sticky MAC address cannot be a VRRP virtual MAC address or a system MAC address.

Example

Enable the sticky MAC function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security mac-address sticky
```

14.7.12 port-security max-mac-num

Function

The **port-security max-mac-num** command sets the maximum number of secure MAC addresses that can be learned on an interface.

The **undo port-security max-mac-num** command restores the default maximum number of secure MAC addresses that can be learned on an interface.

By default, only one MAC address can be learned on an interface.

Format

port-security max-mac-num *max-number*

undo port-security max-mac-num

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of secure MAC addresses that can be learned by an interface.	The value is an integer that ranges from 1 to 1024.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security on an interface, you can run the **port-security max-mac-num** command to limit the number of MAC addresses that the interface can learn. If the switch receives packets with a nonexistent source MAC address after the number of secure MAC addresses reaches the limit, the switch considers that the packets are sent from an unauthorized user, regardless of whether the destination MAC address of packets is valid, and takes the action configured using the **port-security protect-action** command on the interface. This prevents untrusted users from accessing these interfaces, improving security of the switch and the network.

Precautions

- The total number of MAC addresses on interfaces enabled with port security cannot exceed 4096. For example, if the numbers of MAC addresses learned on interfaces 1, 2, 3, and 4 are 1000 respectively, interface 5 can learn a maximum of 96 MAC addresses.
- If the sticky MAC function is disabled, *max-number* limits the number of secure dynamic MAC addresses learned by the interface and secure static MAC addresses configured manually.
- If the sticky MAC function is enabled, *max-number* limits the number of sticky MAC addresses learned by the interface, and sticky MAC addresses and secure static MAC addresses configured manually.
- When multiple NAC users are online under one interface, if you want to enable port security function on the interface, you need to first run the **port-security max-mac-num** command to set the maximum number of MAC addresses learned by the interface, and then run the **port-security enable**

command. Otherwise, only one user is reserved and other users are logged out.

- If you run the **port-security max-mac-num** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the maximum number of MAC addresses that can be learned by GigabitEthernet0/0/1 to 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security max-mac-num 5
```

14.7.13 port-security protect-action

Function

The **port-security protect-action** command configures the protection action to be used when the number of learned MAC addresses on an interface exceeds the upper limit or static MAC address flapping is detected.

The **undo port-security protect-action** command restores the default protection action.

The default protection action is **restrict**.

Format

port-security protect-action { **protect** | **restrict** | **shutdown** }

undo port-security protect-action

Parameters

Parameter	Description	Value
protect	● The interface discards packets with source MAC addresses that are not in the MAC address table when the number of learned MAC addresses exceeds the upper limit. ● The interface discards packets with the flapping MAC address when static MAC address flapping occurs.	-

Parameter	Description	Value
restrict	● The interface discards packets with source MAC addresses that are not in the MAC address table and sends a trap message when the number of learned MAC addresses exceeds the upper limit. ● The interface discards packets with the flapping MAC address and sends a trap message when static MAC address flapping occurs.	-
shutdown	● The interface goes ERROR DOWN and sends a trap message when the number of learned MAC addresses exceeds the upper limit. ● The interface goes ERROR DOWN and sends a trap message when static MAC address flapping occurs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security, you can run the **port-security protect-action** command to configure the protection action performed on the interface when the number of learned MAC addresses on the interface exceeds the upper limit or static MAC address flapping is detected.

The default action **restrict** is recommended. If the action is set to **shutdown** on an interface connected to a downstream device, the interface discards packets from trusted MAC addresses. Select the **shutdown** action only when the interface is directly connected to a user terminal.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

The interface takes protection actions when detecting static MAC address flapping only after the **port-security static-flapping protect** command is executed.

If the protection action is set to **shutdown**, the interface automatically goes ERROR DOWN when the number of learned MAC addresses exceeds the limit or static MAC address flapping is detected. In addition, the interface status will not be automatically recovered. In this case, you can run the **error-down auto-recovery cause port-security interval** *interval-value* command in the system view to enable an interface in Error-Down state to come back up automatically.

If you run the **port-security protect-action** command multiple times in the same interface view, only the latest configuration takes effect.

If both port security and traffic policy-based VLAN translation are configured on the following switch models, an interface forwards protocol packets with source MAC addresses not in the MAC address table when the number of learned MAC addresses exceeds the limit: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S,

Example

Set the protection action on GE0/0/1 to **protect**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security protect-action protect
```

14.7.14 port-security static-flapping protect

Function

The **port-security static-flapping protect** command enables static MAC address flapping detection.

The **undo port-security static-flapping protect** command disables static MAC address flapping detection.

By default, static MAC address flapping detection is disabled.

Format

port-security static-flapping protect

undo port-security static-flapping protect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Secure MAC addresses are also static MAC addresses. When an interface receives a packet of which the source MAC address exists in the static MAC address table on another interface, the interface discards this packet. This will affect user services. For example, after the sticky MAC address function is enabled on GE0/0/1, PC1 is connected to the device through this interface. In this way, the MAC address of PC1 is stored in the static MAC address entry of GE0/0/1. If PC1 is then connected to the device through GE0/0/2, GE0/0/2 discards the packets sent from PC1. In this case, you can enable static MAC address flapping detection. The device then performs the configured action on GE0/0/2.

Precautions

Static MAC address flapping detection needs to be enabled only on the interfaces with port security enabled.

Example

Enable static MAC address flapping detection.

```
<HUAWEI> system-view
[HUAWEI] port-security static-flapping protect
```

14.7.15 undo mac-address security

Function

The **undo mac-address security** command deletes secure MAC address entries. Secure MAC address entries include dynamic and static secure MAC address entries and sticky MAC address entries.

Format

undo mac-address { **sec-config** | **security** | **sticky** } [*interface-type interface-number* | **vlan** *vlan-id*] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface in a secure MAC address entry to be deleted.	-
vlan *vlan-id*	Specifies the VLAN ID in a secure MAC address entry to be deleted.	The value is an integer that ranges from 1 to 4094.
sec-config	Deletes static secure MAC address entries.	-
security	Deletes dynamic secure MAC address entries, that is, MAC address entries learned by an interface enabled with port security.	-
sticky	Deletes sticky MAC address entries, that is, MAC address entries learned by an interface enabled with the sticky MAC function.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After port security is enabled on an interface, dynamic MAC address entries learned by the interface turn into secure MAC address entries. Secure MAC address entries are not aged out. After the number of MAC address entries learned by an interface reaches the limit, the interface cannot learn new MAC address entries. Packets matching no MAC address entry are broadcast, wasting bandwidth resources. This command can delete useless secure MAC address entries to release the MAC address table space.

You can delete some of secure MAC address entries as required. For example:

- If you do not specify *interface-type interface-number*, the command deletes MAC address entries of the specified type on all interfaces.
- If you do not specify **vlan** *vlan-id*, the command deletes MAC address entries of the specified type in all VLANs.

Example

Delete all static secure MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address sec-config
```

Delete all dynamic secure MAC address entries on gigabitethernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address security gigabitethernet 0/0/1
```

Delete all sticky MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address sticky
```

14.8 DHCP Snooping Configuration Commands

14.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.8.2 arp dhcp-snooping-detect enable

Function

The **arp dhcp-snooping-detect enable** command enables association between the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) snooping.

The **undo arp dhcp-snooping-detect enable** command disables association between ARP and DHCP snooping.

By default, association between ARP and DHCP snooping is disabled.

Format

arp dhcp-snooping-detect enable

undo arp dhcp-snooping-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP client sends a DHCP Release message to release its IP address, the DHCP snooping-enabled device immediately deletes the binding entry of the DHCP client. If a DHCP client is abnormally disconnected and cannot send a DHCP Release message, the DHCP snooping-enabled device cannot immediately delete the binding entry of the DHCP client.

If association between ARP and DHCP snooping is enabled using this command and no ARP entry corresponding to the IP address in the DHCP snooping binding entry is found, the DHCP snooping-enabled device performs an ARP probe on the IP address. If no user is detected for consecutive four times, the DHCP snooping-enabled device deletes the DHCP snooping binding entry corresponding to the IP address. (The probe interval is 20 seconds, and the probe times and probe interval are fixed values and cannot be modified.) If the DHCP snooping-enabled device supports the DHCP relay function, this device then sends a DHCP Release message in place of the DHCP client to notify the DHCP server to release the IP address.

Prerequisites

Before association between the ARP and DHCP snooping is enabled, ensure that an IP address configured on the device is on the same network segment as the IP address of the client for ARP probe.

Example

Enable association between ARP and DHCP snooping on the device.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] arp dhcp-snooping-detect enable
```

14.8.3 dhcp option82 append vendor-specific

Function

The **dhcp option82 append vendor-specific** command inserts the Sub9 suboption into Option 82.

The **undo dhcp option82 append vendor-specific** command restores the default configuration.

By default, Sub9 suboption is not inserted into the Option 82 field of DHCP messages.

Format

dhcp option82 append vendor-specific

undo dhcp option82 append vendor-specific

Parameters

None

Views

Interface view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **dhcp option82 append vendor-specific** command is run on a DHCP relay agent or DHCP snooping device, the device will insert the Sub9 suboption into the Option 82 field of a received DHCP message. When this DHCP message is forwarded to the DHCP server, the server obtains the DHCP client location information from the Sub9 suboption.

The Sub9 suboption has old and new formats. The old format contains the vendor ID, for example, hwid. The new format does not contain the vendor ID.

Both the **dhcp option82 append vendor-specific** and **dhcp option82 vendor-specific format** commands can insert the Sub9 into the Option 82 field of the DHCP message, except that the Sub9 formats are different:

- **dhcp option82 append vendor-specific**: inserts the Sub9 of the new format. The new format includes the location information such as the node identifier, node chassis ID, node slot ID, node port number, and user VLAN.
- **dhcp option82 vendor-specific format**: inserts the Sub9 of the old format. The old format includes the DHCP client information such as user IP address and device name.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- When both the **dhcp option82 append vendor-specific** and **dhcp option82 vendor-specific format** commands are run, the **dhcp option82 append vendor-specific** command takes effect.
- The Sub9 suboption can be inserted into Option 82 only when the Sub9 format is the same as the DHCP packet format. If the formats are different:
  - If the **dhcp option82 vendor-specific format** command has been run, the Sub9 of the new format cannot be inserted into Option 82.
  - If the **dhcp option82 append vendor-specific** command has been run, whether the Sub9 of the old format can be inserted depends on the Option 82 insertion method (which is configured using the **dhcp option82 enable** command).
    - When the Option 82 insertion method is Insert, the Sub9 is not inserted.
    - When the Option 82 insertion method is Rebuild, the Sub9 is reconstructed and then inserted into Option 82.

- The total length of the Option 82 field cannot exceed 255 bytes.

Example

Insert the Sub9 suboption into the Option 82 field of DHCP messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 append vendor-specific
```

14.8.4 dhcp option82 enable

Function

The **dhcp option82 enable** command enables a device to insert the Option 82 field to a DHCP message.

The **undo dhcp option82 enable** command disables a device from inserting the Option 82 field to a DHCP message.

By default, a device does not insert the Option 82 field to a DHCP message.

Format

In the interface view, BD view and port group view

dhcp option82 { **insert** | **rebuild** } **enable**

undo dhcp option82 { **insert** | **rebuild** } **enable**

In the VLAN view

dhcp option82 { **insert** | **rebuild** } **enable interface** *interface-type interface-number1* [**to** *interface-number2*]

undo dhcp option82 { **insert** | **rebuild** } **enable interface** *interface-type interface-number1* [**to** *interface-number2*]

Parameters

Parameter	Description	Value
insert	Enables a device to insert the Option 82 field to a DHCP message.	-
rebuild	Enables a device to forcibly insert the Option 82 field to a DHCP message.	-

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-number2*]	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	If this command is run in the VLAN view, the specified interface must have been added to the VLAN.

Views

VLAN view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

The device inserts the Option 82 field to a DHCP message in two modes:

- Insert mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device checks whether the Option 82 field contains the remote ID. If so, the device retains the Option 82 field; if not, the device inserts the remote ID.
- Rebuild mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device deletes the original Option 82 field and inserts the Option 82 field set by the administrator.

The device handles the reply packets from the DHCP server in the same way regardless of whether the Insert or Rebuild method is used.

- The DHCP reply packets contain Option 82:
  - If the DHCP request packets received by the device do not contain Option 82, the device deletes Option 82 from the DHCP reply packets, and forwards the packets to the DHCP client.
  - If the DHCP request packets contain Option 82, the device changes the Option 82 format in the DHCP reply packets into the Option 82 format in the DHCP request packets, and forwards the packets to the DHCP client.
- If the DHCP reply packets do not contain Option 82, the device directly forwards the packets.

NOTE

The physical interface can insert Option82 to the DHCP packets directly forwarded, but does not insert Option82 to the DHCP packets forwarded through a tunnel.

Prerequisites

DHCP snooping has been enabled on the device, or the device has been configured as a DHCP relay agent.

Precautions

- When receiving a DHCP Request message, the device checks whether the field GIADDR in the packet is 0. If so, the **dhcp option82 enable** command takes effect; if not, this command does not take effect.
- DHCP Option 82 must be configured on the user-side of a device; otherwise, the DHCP messages sent to the DHCP server will not carry Option 82.

Example

Enable the device to insert the Option 82 field to DHCP messages on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 insert enable
```

14.8.5 dhcp option82 encapsulation

Function

The **dhcp option82 encapsulation** command configures suboptions inserted into the DHCP Option 82 field.

The **undo dhcp option82 encapsulation** command restores the default suboptions inserted into the DHCP Option 82 field.

By default, the circuit-id (CID), remote-id (RID), subscriber-id (SID), and Sub9 suboptions are inserted into the DHCP Option 82 field in the system view.

By default, suboptions of the DHCP Option 82 field are not inserted in other views.

Format

dhcp option82 encapsulation { **circuit-id** | **remote-id** | **subscriber-id** | **vendor-specific-id** } *

undo dhcp option82 encapsulation

Parameters

Parameter	Description	Value
circuit-id	Inserts the circuit-id suboption.	-
remote-id	Inserts the remote-id suboption.	-

Parameter	Description	Value
subscriber-id	Inserts the subscriber-id (SID) suboption.	-
vendor-specific-id	Inserts the vendor-specific suboption in the Sub9 field.	-

Views

System view, VLAN view, interface view, BD view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This function applies to a DHCP relay agent or a DHCP snooping-enabled device. The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security. The administrator can run this command to configure the device to insert one or more of the circuit-id suboption, remote-id suboption, subscriber-id suboption, and vendor-specific suboption in the Sub9 field into the DHCP Option 82 field. After the command is run, suboptions that are not configured to be inserted are not inserted into the DHCP Option 82 field by default.

Prerequisites

The DHCP function has been enabled in the system view using the **dhcp enable** command.

Example

Insert the circuit-id suboption into the DHCP Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 encapsulation circuit-id
```

14.8.6 dhcp option82 format

Function

The **dhcp option82 format** command configures the format of the Option 82 field in a DHCP message.

The **undo dhcp option82 format** command restores the default format of the Option 82 field in a DHCP message.

By default, the Option 82 field in a DHCP message is in the format of **default**.

Format

dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }

undo dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format**

Parameters

Parameter	Description	Value
circuit-id	Indicates the circuit ID (CID) in the Option 82 field. If the CID is not specified, the format of the Option 82 field is **default**.	-
remote-id	Indicates the remote ID (RID) in the Option 82 field. If the RID is not specified, the format of the Option 82 field is **default**.	-
default	Indicates the default format of the Option 82 field. ● CID format: interface name:svlan.cvlan host name/0/0/0/0/0, in ASCII format ● RID format: device MAC address, in hexadecimal notation	-
common	Indicates the common format of the Option 82 field. ● CID format: {eth|trunk}slot ID/subcard ID/ port ID:svlan.cvlan host name0/0/0/0/0, in ASCII format ● RID format: device MAC address (6 bytes), in ASCII format	-
extend	Indicates the extended format of the Option 82 field. ● CID format: circuit-id type (0) + length (4) + S-VLAN ID (2 bytes) + slot ID (5 bits) + subslot ID (3 bits) + port (1 byte), in hexadecimal notation ● RID format: remote-id type (0) + length (6) + device MAC address (6 bytes), in hexadecimal notation In the CID and RID formats, the values without a unit are fixed values of the fields; the values with a unit indicate the field lengths.	-

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 82 field.	The value is a string of 1 to 255 characters. For details, see the description in "Usage Guideline."
vlan *vlan-id*	Indicates an outer VLAN ID. If a VLAN ID is specified, only the format of the Option 82 field in the DHCP messages sent from the specified VLAN is configured. If no VLAN is specified, the format of the Option 82 field in all the DHCP messages received by the interface is configured.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Indicates an inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of inserting the Option 82 field to DHCP messages is enabled, you can use the **dhcp option82 format** command to configure the format of the Option 82 field.

If you run the **dhcp option82 format** command in the system view, the command takes effect for all the DHCP messages on all the interfaces of the device.

You can use the following keywords to define the Option 82 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.

- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The keyword length can be configured only once.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 82 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.

- The contents in quotation marks (" ") are encapsulated in a character string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 82 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
  - All the spaces in a hexadecimal character string are ignored.
  - By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
  - A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- All Option82 fields configured in the system view or in the same interface view share a length of 1-255 bytes. If their total length exceeds 255 bytes, some Option82 information will be lost.
- There is no limit on the number of Option 82 fields configured on the device. However, a large number of Option 82 fields will occupy a lot of memory and

prolong the device processing time. To ensure device performance, you are advised to configure Option 82 fields based on the service requirements and device memory size.

Example

Configure the default format for the CID in the Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 circuit-id format default
```

Configure the extended format for the CID and RID in the Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 format extend
```

Configure the user-defined string for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 circuit-id format user-defined "%portname:%svlan.%cvlan %sysname"
```

Configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot %3subslot %8port
```

Configure the user-defined string for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 remote-id format user-defined %mac
```

On GE0/0/1, configure the default format for the CID in the Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 circuit-id format default
```

On GE0/0/1, configure the extended format for the CID and RID in the Option 82 field of DHCP messages from VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 vlan 10 format extend
```

On GE0/0/1, configure a user-defined format for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 circuit-id format user-defined "%portname:%svlan.
%cvlan %sysname"
```

On GE0/0/1, configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot
%3subslot %8port
```

On GE0/0/1, configure the user-defined format for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 remote-id format user-defined %mac
```

14.8.7 dhcp option82 subscriber-id format

Function

The **dhcp option82 subscriber-id format** command inserts the Sub6 suboption into the DHCP Option 82 field of DHCP messages and configures the format of the Sub6 suboption.

The **undo dhcp option82 subscriber-id format** command cancels the configuration of the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages.

By default, the Sub6 suboption is not inserted into the DHCP Option 82 field of DHCP messages.

Format

dhcp option82 subscriber-id format { **ascii** *ascii-text* | **hex** *hex-text* }

undo dhcp option82 subscriber-id format

Parameters

Parameter	Description	Value
ascii *ascii-text*	Specifies the ASCII character string in the Sub6 field.	The value is an ASCII character string and contains fewer than 129 characters.
hex *hex-text*	Specifies the HEX character string in the Sub6 field.	The value is in hexadecimal notation. The value can contain only digits 0 to 9, uppercase letters A to F, and lowercase letters a to f. If no space is included, the value length must be an even number smaller than 257.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an authentication system for wired Ethernet access based on DHCP, DHCP snooping, and Option82, a device can insert suboptions (suboption 1, suboption 2, suboption 6, and suboption 9) into the Option 82 field in DHCP Request messages. These suboptions in DHCP Request messages help locate user devices. Unauthorized users cannot access the network by using static IP addresses or stealing accounts of authorized users. You can run the **dhcp option82 subscriber-id format** command to configure the Sub6 suboption.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Configure the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages on GE0/0/1 and specify the ASCII character string in the Sub6 suboption.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 subscriber-id format ascii hw
```

14.8.8 dhcp option82 vendor-specific format

Function

The **dhcp option82 vendor-specific format** command configures the Sub9 field in the Option 82 field.

The **undo dhcp option82 vendor-specific format** command deletes the configuration of the Sub9 field inserted into the DHCP Option 82 field.

By default, the Sub9 field inserted into the Option 82 field is not configured.

Format

dhcp option82 vendor-specific format vendor-sub-option *sub-option-num* { **ascii** *ascii-text* | **hex** *hex-text* | **ip-address** *ip-address* &<1-8> | **sysname** }

undo dhcp option82 vendor-specific format vendor-sub-option *sub-option-num*

Parameters

Parameter	Description	Value
vendor-sub-option *sub-option-num*	Specifies the vendor-specific suboption in the Sub9 field.	The value is an integer that ranges from 1 to 255.
ascii *ascii-text*	Specifies the ASCII character string in the vendor-specific suboption in the Sub9 field.	The value is an ASCII character string and must be smaller than 129 characters.
hex *hex-text*	Specifies the HEX character string in the vendor-specific suboption in the Sub9 field.	The value is in hexadecimal notation. The value can contain only numerals 0 to 9, lowercase letters a to f, and uppercase letters A to F. If no space is included, the value length must be an even number smaller than 257.
ip-address *ip-address*	Specifies the IP address in the vendor-specific suboption in the Sub9 field.	-
sysname	Specifies the device name in the vendor-specific suboption in the Sub9 field.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In authentication for wired Ethernet access using DHCP, DHCP snooping, and Option 82, a device can insert suboptions (suboption 1, suboption 2, and suboption 9) to the Option 82 field in DHCP Request messages. These suboptions in DHCP Request messages carry information about user device locations. Unauthorized users cannot access the network by static IP addresses or embezzled accounts of authorized users. The **dhcp option82 vendor-specific format** command configures the suboptions in the Sub9 field.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Insert the device name to the vendor-specific suboption 1 in the Sub9 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 vendor-specific format vendor-sub-option 1 sysname
```

14.8.9 dhcp server detect

Function

The **dhcp server detect** command enables DHCP server detection.

The **undo dhcp server detect** command disables DHCP server detection.

By default, DHCP server detection is disabled.

Format

dhcp server detect

undo dhcp server detect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bogus DHCP servers exist on the network, they send incorrect information to DHCP clients, such as the incorrect gateway address, incorrect DNS server, and incorrect IP address. As a result, DHCP clients cannot access the network or access incorrect networks.

After DHCP server detection is enabled, a DHCP snooping-capable device checks and logs all the information about DHCP servers in the DHCP Reply messages, such as the addresses and interface numbers of DHCP servers. Based on logs, the network administrator checks for bogus DHCP servers on the network to maintain the network.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Enable detection of DHCP servers.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp server detect
```

14.8.10 dhcp snooping alarm dhcp-rate enable

Function

The **dhcp snooping alarm dhcp-rate enable** command enables the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.

The **undo dhcp snooping alarm dhcp-rate enable** command disables the device from generating an alarm when the number of discarded DHCP messages reaches the threshold.

By default, the device is disabled from generating an alarm when the number of discarded DHCP messages reaches the threshold.

Format

dhcp snooping alarm dhcp-rate enable [**threshold** *threshold*]

undo dhcp snooping alarm dhcp-rate enable [**threshold**]

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold. If the number of discarded DHCP messages reaches the threshold, an alarm is generated. For details, see the **dhcp snooping alarm dhcp-rate threshold**.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCP Request messages and Reply messages to the processing unit. If the rate of sending DHCP messages is high, processing efficiency of the processing unit is affected. After the **dhcp snooping check dhcp-rate enable** command is run, the device checks the rate of sending DHCP messages. DHCP messages that are sent in a specified rate are sent to the processing unit and those that exceed the rate are discarded.

If the number of discarded DHCP messages reaches the threshold, an alarm is generated. To set the alarm threshold, run the **dhcp snooping alarm dhcp-rate threshold** command.

If you run the **dhcp snooping alarm dhcp-rate enable** command in the system view, the command takes effect on all the interfaces of the device. If you run the **dhcp snooping alarm dhcp-rate enable** command in the interface view, the command only takes effect on the specified interface.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

In the system view, enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcp-rate enable
[HUAWEI] dhcp snooping alarm dhcp-rate enable
```

Enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-rate enable
```

14.8.11 dhcp snooping alarm dhcpv6-rate enable

Function

The **dhcp snooping alarm dhcpv6-rate enable** command enables a device to generate an alarm when the number of discarded DHCPv6 messages reaches the threshold.

The **undo dhcp snooping alarm dhcpv6-rate enable** command disables a device from generating an alarm when the number of discarded DHCPv6 messages reaches the threshold.

By default, a device is disabled from generating an alarm when the number of discarded DHCPv6 messages reaches the alarm threshold.

Format

dhcp snooping alarm dhcpv6-rate enable

undo dhcp snooping alarm dhcpv6-rate enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCPv6 messages to the processing unit. If the rate of sending DHCPv6 messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCPv6 messages to the processing unit using the **dhcp snooping check dhcpv6-rate enable** command, DHCPv6 messages that are sent in a specified rate are sent to the processing unit and those that exceed the rate are discarded.

If the **dhcp snooping alarm dhcpv6-rate enable** command is run, the device generates an alarm when the number of discarded DHCPv6 messages reaches the threshold. You can configure the alarm threshold using the **dhcp snooping alarm dhcpv6-rate threshold** command.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If the **dhcp snooping alarm dhcpv6-rate enable** command is run in the system view, the configuration takes effect for all the interfaces on the device. If this command is run in the interface view, the configuration takes effect only for the specified interface.

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

In the system view, enable the device to generate an alarm when the number of discarded DHCPv6 messages reaches the alarm threshold.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping alarm dhcpv6-rate enable
```

14.8.12 dhcp snooping alarm dhcp-rate threshold

Function

The **dhcp snooping alarm dhcp-rate threshold** command sets the alarm threshold for the number of discarded DHCP messages.

The **undo dhcp snooping alarm dhcp-rate threshold** command restores the default alarm threshold for the number of discarded DHCP messages.

By default, the global alarm threshold for the number of discarded DHCP messages is 100, and the alarm threshold for the number of discarded DHCP messages on an interface is the same as that configured in the system view.

Format

dhcp snooping alarm dhcp-rate threshold *threshold*

undo dhcp snooping alarm dhcp-rate threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold. If the number of discarded DHCP messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **dhcp snooping alarm dhcp-rate enable** command to enable a device to generate an alarm when the number of discarded DHCP messages reaches the threshold, you can set the alarm threshold using the **dhcp snooping alarm dhcp-rate threshold** command. An alarm is generated when the number of discarded DHCP messages reaches the threshold.

If the alarm threshold is set in the system view and interface view, the smaller value takes effect.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

Set the alarm threshold for the number of discarded DHCP messages on GE0/0/1 to 50.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-rate threshold 50
```

14.8.13 dhcp snooping alarm dhcpv6-rate threshold

Function

The **dhcp snooping alarm dhcpv6-rate threshold** command sets the alarm threshold for the number of discarded DHCPv6 messages.

The **undo dhcp snooping alarm dhcpv6-rate threshold** command restores the default setting.

By default, the alarm threshold for globally discarded DHCPv6 messages is 100 packets, and the alarm threshold for discarded DHCPv6 messages on an interface is the same as the configured value in the system view.

Format

dhcp snooping alarm dhcpv6-rate threshold *threshold*

undo dhcp snooping alarm dhcpv6-rate threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold. When the number of discarded DHCPv6 messages reaches the threshold, the device generates an alarm.	The value is an integer that ranges from 1 to 1000, in packets.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the device is enabled to generate an alarm when the number of discarded DHCPv6 messages reaches the threshold using the **dhcp snooping alarm dhcpv6-rate enable** command, you can run the **dhcp snooping alarm dhcpv6-rate threshold** *threshold* command to configure the alarm threshold for discarded DHCPv6 messages. The device generates an alarm when the number of discarded DHCPv6 messages reaches the configured alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

- If the **dhcp snooping alarm dhcpv6-rate threshold** command is run in the system view, the configuration takes effect for all the interfaces on the device. If this command is run in the interface view, the configuration takes effect only for the specified interface.
- If an alarm threshold is configured in the system view and interface view simultaneously, the smaller one takes effect.

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

Set the alarm threshold for discarded DHCPv6 messages to 500 packets in the system view.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping alarm dhcpv6-rate threshold 500
```

14.8.14 dhcp snooping alarm enable

Function

The **dhcp snooping alarm enable** command enables the alarm function for DHCP snooping.

The **undo dhcp snooping alarm enable** command disables the alarm function for DHCP snooping.

By default, the alarm function for DHCP snooping is disabled.

Format

dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** [**threshold** *threshold*]

undo dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** [**threshold**]

Interface view, port group view, VLAN view

dhcp snooping alarm dhcpv6-request enable

undo dhcp snooping alarm dhcpv6-request enable

Parameters

Parameter	Description	Value
dhcp-request	Generates an alarm when the number of DHCPv4 Request messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-

Parameter	Description	Value
dhcp-chaddr	Generates an alarm when the number of DHCPv4 Request messages discarded because the CHADDR field in the DHCP message does not match the source MAC address in the Ethernet frame header reaches the threshold.	-
dhcp-reply	Generates an alarm when the number of DHCPv4 Reply messages discarded by untrusted interfaces reaches the threshold.	-
dhcpv6-request	Generates an alarm when the number of DHCPv6 Request messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-
threshold *threshold*	Specifies an alarm threshold. When the number of discarded DHCPv4 messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view, bridge domain view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function is enabled, alarm messages are displayed if DHCP attacks occur and the number of discarded attack messages reaches the threshold. The minimum interval for sending alarms is 1 minute. You can run the **dhcp snooping alarm threshold** command to set the alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

By default, the device does not check the packets received by the client. Therefore:

- Before running the **dhcp snooping alarm** [**dhcp-request** | **dhcpv6-request**] **enable** command, run the **dhcp snooping check dhcp-request enable** command to enable the device to check DHCP messages against the DHCP snooping binding table.

- Before running the **dhcp snooping alarm dhcp-chaddr enable** command, run the **dhcp snooping check dhcp-chaddr enable** command to enable the device to check whether the CHADDR field is the same as the source MAC address in the header of a DHCPv4 Request message.

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

Enable DHCP snooping, dhcp-chaddr check, and the alarm function for packets discarded due to dhcp-chaddr check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr enable
```

14.8.15 dhcp snooping alarm threshold

Function

The **dhcp snooping alarm threshold** command sets the alarm threshold for the number of DHCP messages discarded by DHCP snooping.

The **undo dhcp snooping alarm threshold** command restores the default alarm threshold.

By default, an alarm is generated in the system when at least 100 DHCP snooping messages are discarded, and the alarm threshold on an interface is set using the **dhcp snooping alarm threshold** command in the system view.

Format

In the system view:

dhcp snooping alarm threshold *threshold*

undo dhcp snooping alarm threshold

In the interface view, VLAN view and BD view and port group view:

dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **threshold** *threshold*

undo dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **threshold**

In the interface view, VLAN view and port group view:

dhcp snooping alarm dhcpv6-request threshold *threshold*

undo dhcp snooping alarm dhcpv6-request threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCP snooping-discarded messages.	The value is an integer that ranges from 1 to 1000.
dhcp-request	Specifies the alarm threshold for the number of DHCPv4 Request messages discarded because they do not match the DHCP snooping binding entries.	-
dhcp-chaddr	Specifies the alarm threshold for the number of DHCP messages discarded because the CHADDR field in the DHCPv4 request messages does not match the source MAC address in the data frame header.	-
dhcp-reply	Specifies the alarm threshold for the number of DHCPv4 Response messages discarded by untrusted interfaces.	-
dhcpv6-request	Specifies the alarm threshold for the number of DHCPv6 Request messages discarded because they do not match the DHCP snooping binding entries.	-

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After trap for discarded DHCP messages is enabled, run the **dhcp snooping alarm threshold** command to specify the alarm threshold for the number of DHCP messages discarded by DHCP snooping. If the alarm threshold is not set on an interface, the interface uses the global alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

The DHCP snooping alarm function has been enabled using the **dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** | **dhcpv6-request** } **enable** command.

Precautions

If you run the **dhcp snooping alarm threshold** command in the system view, the command takes effect on all the interfaces of the device.

If you specify an alarm threshold for the number of DHCP messages discarded by DHCP snooping in the system view, an alarm is generated when the number of all the discarded DHCP messages reaches the threshold.

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

Set the global alarm threshold for the number of discarded DHCP messages to 200.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping alarm threshold 200
```

On GE0/0/1, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address. Set the alarm threshold to 1000.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr threshold 1000
```

14.8.16 dhcp snooping check dhcp-giaddr enable

Function

The **dhcp snooping check dhcp-giaddr enable** command enables the device to check whether the GIADDR field in DHCP messages is 0.

The **undo dhcp snooping check dhcp-giaddr enable** command disables the device from checking whether the GIADDR field in DHCP messages is 0.

By default, the device does not check whether the GIADDR field in DHCP messages is 0.

Format

In the system view:

dhcp snooping check dhcp-giaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping check dhcp-giaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

In the VLAN view and interface view:

dhcp snooping check dhcp-giaddr enable

undo dhcp snooping check dhcp-giaddr enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check whether the GIADDR field in DHCP messages sent from a specified VLAN is 0. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that the device obtains parameters such as MAC addresses for generating a binding table, DHCP snooping needs to be applied to Layer 2 access devices or the first DHCP relay agent from the device. Therefore, the GIADDR field in the DHCP messages received by the DHCP snooping-enabled device is 0. If the GIADDR field is not 0, the message is unauthorized and then discarded. This function is recommended if DHCP snooping is enabled on the DHCP relay agent.

In normal situations, the GIADDR field in DHCP messages sent by user PCs is 0. If the GIADDR field is not 0, the DHCP server cannot correctly allocate IP addresses. To prevent attackers from applying IP addresses with the DHCP messages containing a non-0 GIADDR field, you are advised to configure this function.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-giaddr enable** command in the VLAN view, the command takes effect on all the DHCP messages from the specified VLAN. If you run the **dhcp snooping check dhcp-giaddr enable** command in the interface view, the command takes effect on all the DHCP messages received by the specified interface.

Example

Enable the device to check whether the GIADDR field in DHCP messages from VLAN10 is 0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping check dhcp-giaddr enable
```

Enable the device to check whether the GIADDR field in DHCP messages received on GE0/0/1 is 0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-giaddr enable
```

14.8.17 dhcp snooping check dhcp-rate

Function

The **dhcp snooping check dhcp-rate** command sets the maximum rate of sending DHCP messages to the processing unit.

The **undo dhcp snooping check dhcp-rate** command restores the default maximum rate of sending DHCP messages to the processing unit.

By default, the maximum rate of sending global DHCP messages to the processing unit is 100 pps, which is the same as the maximum rate of sending DHCP messages on interfaces to the processing unit.

Format

In the system view:

dhcp snooping check dhcp-rate *rate* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping check dhcp-rate

In the VLAN view and interface view:

dhcp snooping check dhcp-rate *rate*

undo dhcp snooping check dhcp-rate

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of sending DHCP messages to the processing unit.	The value is an integer that ranges from 1 to 100, in pps.
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies the maximum rate of sending DHCP messages from a specified VLAN to the processing unit. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. If this parameter is not specified, the command takes effect on all the DHCP messages.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCP Request messages and Reply messages to the processing unit. If the rate of sending DHCP messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCP messages to the processing unit, run the **dhcp snooping check dhcp-rate** command to set the maximum rate of sending DHCP messages to the processing unit. DHCP messages that exceed the rate are discarded.

Prerequisites

The device has been enabled to check the rate of sending DHCP messages to the processing unit using the **dhcp snooping check dhcp-rate enable** command.

Precautions

If the maximum rates of sending DHCP messages to the processing unit are set in the system view, VLAN view, and interface view, the smallest value takes effect.

Example

In the system view, set the maximum rate of sending DHCP messages to the processing unit to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcp-rate enable
[HUAWEI] dhcp snooping check dhcp-rate 50
```

14.8.18 dhcp snooping check dhcpv6-rate

Function

The **dhcp snooping check dhcpv6-rate** command sets the maximum rate of sending DHCPv6 messages to the processing unit.

The **undo dhcp snooping check dhcpv6-rate** command restores the default maximum rate of sending DHCPv6 messages to the processing unit.

By default, the maximum rate of DHCPv6 messages sent to the processing unit is 100 pps.

Format

dhcp snooping check dhcpv6-rate *rate*

undo dhcp snooping check dhcpv6-rate

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of DHCPv6 messages sent to the processing unit.	The value is an integer that ranges from 1 to 400, in pps.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCPv6 messages to the processing unit. If the rate of sending DHCPv6 messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCPv6 messages to the processing unit, DHCPv6 messages that exceed the specified rate are discarded.

Before the maximum rate of DHCP messages sent to the DHCP message processing unit is configured, ensure that the **dhcp snooping check dhcpv6-rate enable** command has been executed to enable the device to check the rate of sending DHCPv6 messages to the processing unit. Otherwise, the configuration does not take effect.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

- If you run the **dhcp snooping check dhcpv6-rate** command in the system view, the configuration takes effect for all the interfaces on the device. If you run this command in the interface view, the configuration takes effect only for the specified interface. If you run this command in the VLAN view, the configuration takes effect for all the interfaces in this VLAN.
- If the maximum rates of sending DHCPv6 messages to the processing unit are set in the system view, VLAN view, and interface view simultaneously, the smallest value takes effect.

Example

In the system view, set the maximum rate of sending DHCPv6 messages to the processing unit to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcpv6-rate 50
```

14.8.19 dhcp snooping check dhcp-rate enable

Function

The **dhcp snooping check dhcp-rate enable** command enables the device to check the rate of sending DHCP messages to the processing unit.

The **undo dhcp snooping check dhcp-rate enable** command disables the device from checking the rate of sending DHCP messages to the processing unit.

By default, the device does not check the rate of sending DHCP messages to the processing unit.

Format

In the system view:

dhcp snooping check dhcp-rate enable [*rate*] [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping check dhcp-rate enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping check dhcp-rate enable [*rate*]

undo dhcp snooping check dhcp-rate enable

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of sending DHCP messages to the processing unit. For the function of *rate*, see the command **dhcp snooping check dhcp-rate**.	The value ranges from 1 to 100, in pps. The default value is 100.
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check the rate of sending DHCP messages from a specified VLAN to the processing unit. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. If this parameter is not specified, the command takes effect on all the DHCP messages.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCP Request messages and Reply messages to the processing unit. If the rate of sending DHCP messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCP messages to the processing unit, DHCP messages that exceed the specified rate are discarded.

The default maximum rate of sending DHCP messages is 100 pps. To set the maximum rate, run the **dhcp snooping check dhcp-rate** command.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

In the system view, enable the device to check the rate of sending DHCP messages to the processing unit.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcp-rate enable
```

In VLAN 10, enable the device to check the rate of sending DHCP messages to the processing unit.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping check dhcp-rate enable
```

14.8.20 dhcp snooping check dhcpv6-rate enable

Function

The **dhcp snooping check dhcpv6-rate enable** command enables the device to check the rate of sending DHCPv6 messages to the processing unit.

The **undo dhcp snooping check dhcpv6-rate enable** command disables the device from checking the rate of sending DHCPv6 messages to the processing unit.

By default, the device does not check the rate of DHCPv6 messages sent to the processing unit.

Format

dhcp snooping check dhcpv6-rate enable

undo dhcp snooping check dhcpv6-rate enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCPv6 messages to the processing unit. If the rate of sending DHCPv6 messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCPv6 messages to the processing unit, DHCPv6 messages that exceed the specified rate are discarded.

After the device is enabled to check the rate of sending DHCPv6 messages to the processing unit, the default maximum rate of sending DHCPv6 messages is set to 100 pps. To set the maximum rate, run the **dhcp snooping check dhcpv6-rate** command.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcpv6-rate enable** command in the system view, the configuration takes effect for all the interfaces on the device. If you run this command in the interface view, the configuration takes effect only for the specified interface. If you run this command in the VLAN view, the configuration takes effect for all the interfaces in this VLAN.

Example

In the system view, enable the device to check the rate of DHCPv6 messages sent to the processing unit.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcpv6-rate enable
```

14.8.21 dhcp snooping check dhcpv6-request mac

Function

The **dhcp snooping check dhcpv6-request mac** command enables the function of checking the validity of DHCPv6 messages based on MAC addresses.

The **undo dhcp snooping check dhcpv6-request mac** command disables the function of checking the validity of DHCPv6 messages based on MAC addresses.

By default, the function of checking the validity of DHCPv6 messages based on MAC addresses is disabled.

Format

dhcp snooping check dhcpv6-request mac

undo dhcp snooping check dhcpv6-request mac

Parameters

None

Views

System view, VLAN view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After binding entries are generated, the device searches for the binding entries based on the MAC address entry that is used as the key. The device checks whether the Request messages sent by the DHCPv6 client match any binding entry. If they match, the device forwards the messages; otherwise, the device discards the messages. This prevents unauthorized users from sending bogus DHCPv6 messages to extend the IP address lease or release IP addresses.

The rules for checking DHCPv6 Request messages based on binding entries are as follows:

- When receiving a DHCPv6 Request message, the device searches the dynamic binding table based on the user's MAC address. If no corresponding binding entry is found or the binding entry found is a temporary one, the device forwards the message. Otherwise, the device checks whether the VLAN ID, VPN instance, and interface information of the message match the corresponding binding entry. If so, the device forwards the message. If not, the device discards the message.
- When receiving a DHCPv6 Release or Decline message, the device checks whether the VLAN ID, VPN instance, and interface information of the message matches an entry in the dynamic binding table. If a match is found, the device forwards the message. Otherwise, the device discards the message.

Prerequisites

DHCPv6 snooping has been enabled on the device using the **dhcp snooping enable** command.

Follow-up Procedure

Run the **dhcpv6 snooping user-bind mac-conflict detect enable** command to enable DHCPv6 snooping to detect whether a user is online. If a user's DHCPv6 message fails the match check, the device detects whether the user is online. If the user is offline, the device deletes the DHCPv6 snooping entry of the offline user in a timely manner.

Precautions

If you run this command in the VLAN view, the command configuration takes effect only for the DHCPv6 messages from the specified VLAN. If you run this command in the interface view, the command configuration takes effect for all DHCPv6 messages on the specified interface.

This command cannot be used together with **dhcp snooping enable no-user-binding**; otherwise, online users may fail to go offline.

Example

Enable the function of checking the validity of DHCPv6 messages based on MAC addresses in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping check dhcpv6-request mac
```

14.8.22 dhcp snooping check dhcp-chaddr enable

Function

The **dhcp snooping check dhcp-chaddr enable** command enables the device to check whether the CHADDR field matches the source MAC address in the header of DHCP Request messages (DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, DHCP INFORM).

The **undo dhcp snooping check dhcp-chaddr enable** command disables the device from checking whether the CHADDR field matches the source MAC address in the header of

DHCP Request messages (DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, DHCP INFORM).

By default, the device does not check whether the CHADDR field is the same as the source MAC address in the header of DHCP Request messages (DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, DHCP INFORM).

Format

In the system view:

dhcp snooping check dhcp-chaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping check dhcp-chaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

In the VLAN view, BD view and interface view:

dhcp snooping check dhcp-chaddr enable

undo dhcp snooping check dhcp-chaddr enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check whether the CHADDR field matches the source MAC address in the header of a DHCP Request message. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, the CHADDR field in DHCP Request messages (DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, DHCP INFORM) matches the MAC address of the DHCP client that sends the message. The DHCP server identifies the client MAC address based on the CHADDR field in the DHCP Request messages (DHCP DISCOVER, DHCP REQUEST, DHCP DECLINE, DHCP RELEASE, DHCP INFORM). If attackers continuously apply for IP addresses by changing the CHADDR field in the DHCP Request message, addresses in the address pool on the DHCP server may be exhausted. As a result, authorized users cannot obtain IP addresses.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-chaddr enable** command in the VLAN view, the command takes effect on all the DHCP messages in the specified VLAN received by all the interfaces on the device. If you run the **dhcp snooping check dhcp-chaddr enable** command in the interface view, the command takes effect for all the DHCP messages received on the interface.

Example

Enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
```

14.8.23 dhcp snooping check dhcp-request enable

Function

The **dhcp snooping check dhcp-request enable** command enables the device to check DHCP messages against the DHCP snooping binding table.

The **undo dhcp snooping check dhcp-request enable** command disables the device from checking DHCP messages against the DHCP snooping binding table.

By default, the device does not check DHCP messages against the DHCP snooping binding table.

Format

System view:

dhcp snooping check dhcp-request enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping check dhcp-request enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

VLAN view, interface view, BD view:

dhcp snooping check dhcp-request enable

undo dhcp snooping check dhcp-request enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check DHCP messages from a specified VLAN against the DHCP snooping binding table.	The value is an integer in the range from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP snooping binding table is generated, the device checks DHCPv4 Request, DHCPv6 Request, or DHCPv4 Release messages against the DHCP snooping binding table. Only DHCP messages that match entries are forwarded, and those that do not match entries are discarded. This prevents unauthorized users from sending bogus DHCP packets to renew or release IP addresses.

The device checks DHCPv4 Request, DHCPv6 Request, or DHCPv4 Release messages against the DHCP snooping binding table based on the following rules:

- For a DHCPv4 Request message:
  a. Checks whether the destination MAC address is all Fs. If so, the device considers the message a broadcast message requesting a lease renewal or a broadcast message a user sends on the first login and directly forwards the message. If not, the device considers the user to have sent the DHCPv4 Request message to renew the IP address lease and checks the message against the DHCP snooping binding table.
  b. Checks whether the CHADDR field in the DHCPv4 Request message matches a DHCP snooping binding entry. If not, the device considers the user to have gone online for the first time and directly forwards the message. If so, the device checks whether the VLAN ID, IP address, and interface number of the message match any DHCP snooping binding entry. If all these fields match a DHCP snooping binding entry, the device forwards the message; otherwise, the device discards the message.
- When receiving a DHCPv4 Release message, the device checks whether the VLAN ID, IP address, MAC address, and interface number of the message match a dynamic DHCP snooping binding entry. If so, the device forwards the message; otherwise, the device discards the message.
- When receiving a DHCPv6 Request message, the device searches the DHCP snooping binding table based on the user's MAC address. If no corresponding binding entry is found or the binding entry found is a temporary one, the device forwards the message. Otherwise, the device considers the message as the one used for requesting a lease renewal and checks whether the VLAN ID, IP address, and interface number of the message match any binding entry. If so, the device forwards the message. If not, the device discards the message.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping enable** command in the VLAN view, the command takes effect for all the DHCP messages from the specified VLAN. If you run this command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

After defense against bogus DHCPv6 message attacks is configured using the **dhcp snooping check dhcpv6-request mac** command, the device does not check DHCPv6 messages against the DHCP snooping binding table when the **dhcp snooping check dhcp-request** command is executed.

Example

Enable the device to check DHCP messages against the DHCP snooping binding table in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping check dhcp-request enable
```

14.8.24 dhcp snooping check local-reply enable

Function

The **dhcp snooping check local-reply enable** command enables the device to check validity of DHCP reply messages with the CHADDR field being its local MAC address.

The **undo dhcp snooping check local-reply enable** command disables the device from checking validity of DHCP reply messages with the CHADDR field being its local MAC address.

By default, a device does not check validity of DHCP reply messages with the CHADDR field being its local MAC address.

Format

dhcp snooping check local-reply enable

undo dhcp snooping check local-reply enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a possibility that a device, as a DHCP client, obtains an IP address from an untrusted interface even if DHCP snooping is enabled. In this case, IP address validity cannot be ensured. To ensure security, you can enable the device to check validity of the received DHCP reply messages with the CHADDR field being its local MAC address: If the message is received from a trusted interface, the device keeps the message. If the message is received from an untrusted interface, the device discards the message.

Prerequisites

In the system view, run the **dhcp snooping enable** command to enable DHCP snooping.

Example

Enable the device to check whether DHCP reply messages with the CHADDR field being its local MAC address are received from trusted interfaces.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check local-reply enable
```

14.8.25 dhcp snooping check server-vlan enable

Function

The **dhcp snooping check server-vlan enable** command enables the DHCP snooping-enabled device to check VLAN information in DHCP Reply messages.

The **undo dhcp snooping check server-vlan enable** command disables the DHCP snooping-enabled device from checking VLAN information in DHCP Reply messages.

By default, the DHCP snooping-enabled device does not check VLAN information in DHCP Reply messages.

Format

dhcp snooping check server-vlan enable

undo dhcp snooping check server-vlan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the DHCP snooping-enabled device identifies devices by checking DHCP reply messages only based on MAC addresses. If devices cannot be identified based on MAC addresses, run the **dhcp snooping check server-vlan enable** command to enable the DHCP snooping-enabled device to identify devices by checking DHCP reply messages based on MAC addresses and VLAN IDs.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

DHCP server detection has been enabled using the **dhcp server detect** command.

Example

Enable the DHCP snooping-enabled device to check VLAN information in DHCP Relay messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp server detect
[HUAWEI] dhcp snooping check server-vlan enable
```

14.8.26 dhcp snooping deny enable

Function

The **dhcp snooping deny enable** command enables the function of discarding DHCP messages.

The **undo dhcp snooping deny enable** command disables the function of discarding DHCP messages.

By default, the function of discarding DHCP messages is disabled.

Format

dhcp snooping deny { **dhcp** | **dhcpv6** } **enable**

undo dhcp snooping deny { **dhcp** | **dhcpv6** } **enable**

Parameters

Parameter	Description	Value
dhcp	Indicates that the device processes DHCPv4 messages.	-
dhcpv6	Indicates that the device processes DHCPv6 messages.	-

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling DHCP snooping, you can prevent DHCP messages from being processed by using the **dhcp snooping deny enable** command to discard these messages.

Prerequisites

The **dhcp snooping enable** or **dhcp snooping trusted** command has been run on the specified interface or in the specified VLAN.

Precautions

If you run the **dhcp snooping deny enable** command in the system view, the function of discarding DHCP messages takes effect globally. If you run the **dhcp snooping deny enable** command in the VLAN view, the command takes effect for all DHCP messages in a specified VLAN received by all the interfaces on the device. If you run the **dhcp snooping deny enable** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

Example

Enable an interface that has been added to VLAN 10 to discard DHCPv4 messages in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping deny dhcp enable
```

14.8.27 dhcp snooping disable

Function

The **dhcp snooping disable** command disables DHCP snooping on an interface.

The **undo dhcp snooping disable** command cancels the configuration.

By default, if the **dhcp snooping enable** command is used on an interface or in a VLAN that an interface belongs to, DHCP snooping is enabled on this interface.

Format

dhcp snooping disable

undo dhcp snooping disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you run the **dhcp snooping enable** command to enable DHCP snooping in a VLAN, DHCP snooping is enabled on all the interfaces in the VLAN. If you do not run the **dhcp snooping enable** command to enable DHCP snooping on an interface, you cannot run the **undo dhcp snooping enable** command to disable DHCP snooping on the interface. To address this problem, run the **dhcp snooping disable** command to disable DHCP snooping on the interface. Users can properly go online from this interface, but no dynamic binding entry is generated.

Precautions

- The **dhcp snooping disable** command does not only disable DHCP snooping on an interface, but also clears the DHCP snooping configuration and the dynamic binding table. The **undo dhcp snooping enable** command, however, only disables DHCP snooping on the interface and does not clear the configuration or the dynamic binding table.
- The **undo dhcp snooping disable** command enables DHCP snooping on an interface. To enable DHCP snooping, run the **dhcp snooping enable** command.

Example

Disable DHCP snooping on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping disable
```

14.8.28 dhcp snooping enable

Function

The **dhcp snooping enable** command enables DHCP snooping.

The **undo dhcp snooping enable** command disables DHCP snooping.

By default, DHCP snooping is disabled on the device.

Format

In the system view:

dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view, BD view, and interface view:

dhcp snooping enable

undo dhcp snooping enable

Parameters

Parameter	Description	Value
ipv4	Indicates that the device processes only DHCPv4 messages.	-
ipv6	Indicates that the device processes only DHCPv6 messages.	-
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables DHCP snooping in a specified VLAN. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*.	The specified VLAN ID must exist.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

NOTE

Only the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S supports the BD view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP snooping is a security function to protect DHCP. When you run the **dhcp snooping enable** command to enable DHCP snooping on a device, the device can process both DHCPv4 and DHCPv6 messages. In practice, however, if the DHCP snooping device needs to process only DHCPv4 or DHCPv6 messages, you can run the **dhcp snooping enable ipv4** or **dhcp snooping enable ipv6** command, which improves CPU efficiency.

You must enable DHCP snooping in the system view before enabling DHCP snooping on an interface, in a BD, or in a VLAN.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Follow-up Procedure

After DHCP snooping is enabled on an interface connected to users, in a BD, or in a VLAN, run the **dhcp snooping trusted** command to configure the interface connected to the DHCP server as a trusted interface. Then a DHCP snooping binding table can be generated.

Precautions

The **dhcp snooping enable** command in the system view is the prerequisite for DHCP snooping-related functions. After the **undo dhcp snooping enable** command is run, all DHCP snooping-related configurations of the device are deleted. After DHCP snooping is enabled again using the **dhcp snooping enable** command, all DHCP snooping-related configurations of the device are restored to the default configurations.

If you run the **dhcp snooping enable** command in the VLAN view, the command takes effect for all the DHCP messages from the specified VLAN. If you run this command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

If both DHCP relay and VRRP are configured on a device, DHCP snooping cannot be enabled.

If the DHCP server is at the subordinate VLAN side and the DHCP client is at the principal VLAN side, DHCP snooping cannot be enabled.

If DHCP snooping is enabled on the device, do not configure 2:2 VLAN mapping. Otherwise, DHCP users cannot go online.

Example

Enable DHCP snooping globally and configure the device to process only IPv4 messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv4
```

Enable DHCP snooping on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
```

Enable DHCP snooping in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
```

Enable DHCP snooping in VLANs ranging from VLAN 20 to VLAN 25 in a batch.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan batch 20 to 25
[HUAWEI] dhcp snooping enable vlan 20 to 25
```

14.8.29 dhcp snooping enable no-user-binding

Function

The **dhcp snooping enable no-user-binding** command disables the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.

The **undo dhcp snooping enable no-user-binding** command restores the default setting.

By default, an interface generates DHCP snooping binding entries after DHCP snooping is enabled.

Format

System view:

dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

VLAN view and interface view:

dhcp snooping enable no-user-binding

undo dhcp snooping enable no-user-binding

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Disables the interfaces in the specified VLANs from generating DHCP snooping binding entries. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*.	The value is an integer in the range from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled on a device, the device generates DHCP snooping binding entries for users by default. If the number of binding entries on the device reaches the upper limit, new users cannot go online. In certain scenarios, for example, on a trusted DHCP network, if you do not want to limit the number of online users but want to record user location information, run the **dhcp snooping enable no-user-binding** command to disable the device from generating DHCP snooping binding entries.

When the command is executed in an interface view, the command takes effect for all DHCP users connected to the interface. When the command is executed in the VLAN view, the command takes effect for all the DHCP users belonging to this VLAN on all interfaces. When the command is executed in the system view, the command takes effect in the same way as it is executed in the VLAN view, except that multiple VLANs can be specified.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

After this command is executed, the device deletes the binding entries from the corresponding VLAN or interface.

If the DHCP snooping binding entry-dependent function such as IPSG or DAI is configured on the device, the corresponding function does not take effect after this command is run.

This command cannot be used together with **dhcp snooping check dhcp-request enable** and **dhcp snooping check dhcpv6-request mac**. Otherwise, online users may fail to go offline.

Example

In the system view, disable the interfaces in VLAN 10 and VLAN 20 from generating DHCP snooping binding entries.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping enable vlan 10 20
[HUAWEI] dhcp snooping enable no-user-binding vlan 10 20
```

In the VLAN view, disable the interfaces in VLAN 10 from generating DHCP snooping binding entries.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping enable no-user-binding
```

In the interface view, disable GE0/0/1 from generating DHCP snooping binding entries.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable no-user-binding
```

14.8.30 dhcp snooping max-user-number

Function

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface.

The **undo dhcp snooping max-user-number** command restores the default maximum number of DHCP snooping binding entries to be learned on an interface.

By default, the maximum number of DHCP snooping binding entries that can be learned on an interface is 512 for S1720GW-E, S1720GWR-E, and 2048 for S5720-LI, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, , S5735S-H, S5736-S, S6720S-S, and S5720I-SI, and 8192 for other models.

NOTE

The maximum number of DHCP snooping binding entries configured using this command is the sum of DHCPv4 snooping and DHCPv6 snooping binding entries.

Format

In the system view:

dhcp snooping max-user-number *max-user-number* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping max-user-number [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping max-user-number *max-user-number*

undo dhcp snooping max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of DHCP snooping binding entries that can be learned on an interface.	The value is an integer that ranges from 1 to 512 for S1720GW-E, S1720GWR-E, and from 1 to 2048 for S5720-LI, S2730S-S, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, , S5735S-H, S5736-S, S6720S-S, and S5720I-SI, and from 1 to 8192 for other models.

Parameter	Description	Value
		NOTE If the maximum number of DHCP snooping binding entries to be learned by interfaces is N in the system or VLAN view, for a stack, the value in system view and VLAN view ranges from 1 to N * Number of stacked devices. That is, by default, a maximum of N * Number of stacked devices DHCP users are allowed to access the entire device or VLAN. For S5720-LI, S2730S-S, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6720-EI, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720S-EI: A stack of these switches can learn a maximum of 9216 DHCP snooping binding entries. For example, a stack of two S5731-H switches can learn a maximum of 8192 DHCP snooping binding entries globally and in VLANs by default. When three of these switches set up a stack, the stack can learn a maximum of 9216 DHCP snooping binding entries globally and in VLANs by default.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the maximum number of DHCP snooping binding entries can be learned in a VLAN. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface. If the number of DHCP snooping binding entries reaches the maximum value, subsequent users cannot access.

When the command is executed in the system view, the value specified in this command is the total number of DHCP snooping binding entries to be learned by all interfaces on the device. If you run the **dhcp snooping max-user-number** command in the VLAN view, the command takes effect on all the interfaces in the VLAN. If you run the **dhcp snooping max-user-number** command in the system view, VLAN view and the interface view, the smallest value takes effect.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

The maximum number of DHCP snooping binding entries to be learned in a stack environment will still be valid if the stack is split. For example, the maximum number of DHCP snooping binding entries to be learned by interfaces is set to N in the system or VLAN view. After the stack splits, run the **display dhcp snooping** command. You will find that the maximum number of entries learned by interfaces in the system or VLAN view is still N (even if N is greater than the maximum number (M) of entries supported by a stand-along device). Pay attention to the following points:

- For the users requiring to go online: The users are allowed to go online when the number of binding entries on the device is smaller than M, and not allowed to go online when the number of binding entries on the device is equivalent to or larger than M.
- For online users: The users are kept online no matter whether the number of binding entries on the device is larger than M. However, if the number of binding entries is larger than M, the users cannot go online again after they go offline.
- Binding entries that have been backed up: After the device restarts, all binding entries on the device can be restored no matter whether the number of binding entries is smaller than M, and the users matching these binding entries can go online.

Example

Set the maximum number of DHCP users to 100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping max-user-number 100
```

Set the maximum number of DHCP users in VLAN 100 to 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI-vlan100] dhcp snooping max-user-number 100
```

14.8.31 dhcp snooping over-vpls enable

Function

The **dhcp snooping over-vpls enable** command enables DHCP snooping on the device on a Virtual Private LAN Service (VPLS) network.

The **undo dhcp snooping over-vpls enable** command disables DHCP snooping on the device on a VPLS network.

By default, DHCP snooping is disabled on the device on a VPLS network.

NOTE

Only the S6730-H, S6730S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5732-H, S5731S-H, and S5731-H support this command.

Format

dhcp snooping over-vpls enable

undo dhcp snooping over-vpls enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DHCP packets on a VPLS network are different from common DHCP packets. Therefore, DHCP snooping cannot take effect for the device on the VPLS network even if the function is enabled globally using the **dhcp snooping enable** command in the system view. To make DHCP snooping take effect for the device applied to the VPLS network, run the **dhcp snooping over-vpls enable** command to enable the function.

To enable DHCP snooping for the device on the VPLS network, enable it on the device closed to the user side so that the DHCP packets from the user side to the VPLS network can be controlled.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Precautions

The device management interfaces do not support DHCP snooping on a VPLS network.

When the device is applied to a VPLS network, you only need to run the **dhcp snooping over-vpls enable** command to enable DHCP snooping on the device and other DHCP snooping command have no changes.

Example

Enable DHCP snooping on the device on a VPLS network.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping over-vpls enable
```

14.8.32 dhcp snooping packet-flow log enable

Function

The **dhcp snooping packet-flow log enable** command enables the function of recording logs when DHCP messages are exchanged.

The **undo dhcp snooping packet-flow log enable** command disables the function of recoding logs when DHCP messages are exchanged.

By default, the function of recording logs when DHCP messages are exchanged is disabled.

NOTE

Only the following switch models support this command:

Format

dhcp snooping packet-flow log enable

undo dhcp snooping packet-flow log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of recording logs when DHCP messages are exchanged is enabled using the **dhcp snooping packet-flow log enable** command, the device records a **DHCP/6/SNP_RCV_MSG** log each time it receives a DHCP message. This log can be used in smart O&M and other scenarios. The network analyzer can perform smart analysis on whether the user obtains an IP address through this log.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Enable the function of recording logs when DHCP messages are exchanged.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping packet-flow log enable
```

14.8.33 dhcp snooping trusted

Function

The **dhcp snooping trusted** command configures an interface as a trusted interface.

The **undo dhcp snooping trusted** command configures an interface as an untrusted interface.

By default, all interfaces are untrusted interfaces.

Format

In the VLAN view:

dhcp snooping trusted interface *interface-type interface-number*

undo dhcp snooping trusted interface *interface-type interface-number*

In the interface view and BD view:

dhcp snooping trusted

undo dhcp snooping trusted

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface in a VLAN. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable DHCP clients to obtain IP addresses from authorized DHCP servers, DHCP snooping supports the trusted interface and untrusted interfaces. The trusted interface forwards DHCP messages while untrusted interfaces discard received DHCP ACK messages and DHCP Offer messages.

An interface directly or indirectly connected to the DHCP server trusted by the administrator needs to be configured as the trusted interface, and other interfaces are configured as untrusted interfaces. This ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

Prerequisites

In the system view, run the **dhcp snooping enable** command to enable DHCP snooping.

Precautions

If an interface has been configured as a DHCP trusted interface using the **dhcp snooping trusted** command, the device will not consider DHCP packets received by this interface as attack packets or perform attack defense operations on the DHCP packets received by this interface.

If you run the **dhcp snooping trusted** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping trusted** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

You are advised not to configured more than 15 trusted ports in a VLAN.

After an interface on which the **dhcp snooping trusted** command is run receives a DHCP Request message, it forwards the message to all other trusted interfaces. If there are no other trusted interfaces, it discards the message.

Example

Configure GE0/0/1 in VLAN 100 as the trusted interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping trusted interface gigabitethernet 0/0/1
```

Configure GE0/0/1 as the trusted interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping trusted
```

14.8.34 dhcp snooping user-alarm percentage

Function

The **dhcp snooping user-alarm percentage** command configures the alarm thresholds for the percentage of DHCP snooping binding entries.

The **undo dhcp snooping user-alarm percentage** command restores the default alarm thresholds for the percentage of DHCP snooping binding entries.

By default, the lower and upper alarm thresholds for the percentage of DHCP snooping binding entries are 50 and 100, respectively.

Format

dhcp snooping user-alarm percentage *percent-lower-value percent-upper-value*

undo dhcp snooping user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer in the range from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **dhcp snooping max-user-number** command to set the maximum number of DHCP snooping binding entries on an interface, you can run the **dhcp snooping user-alarm percentage** command to set the alarm thresholds for the percentage of DHCP snooping binding entries.

When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or exceeds the upper alarm threshold, the device generates an alarm. When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

Example

Set the lower alarm threshold for the DHCP user count percentage to 30 and the upper alarm threshold to 80.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping user-alarm percentage 30 80
```

14.8.35 dhcp snooping user-bind autosave

Function

The **dhcp snooping user-bind autosave** command enables local automatic backup of the DHCP snooping binding table.

The **undo dhcp snooping user-bind autosave** command disables local automatic backup of the DHCP snooping binding table.

By default, local automatic backup of the DHCP snooping binding table is disabled.

Format

dhcp snooping user-bind autosave *file-name* [**write-delay** *delay-time*]

undo dhcp snooping user-bind autosave

Parameters

Parameter	Description	Value
file-name	Specifies the path for storing the file that backs up the binding table and the file name. The file path and name supported by the device must be both entered.	The value is a string of 1 to 51 case-insensitive characters without spaces.
write-delay *delay-time*	Specifies the interval for local automatic backup of the DHCP snooping binding table. If this parameter is not specified, the backup interval is the default value.	The value is an integer that ranges from 60 to 4294967295, in seconds. By default, the interval for local automatic backup of the DHCP snooping binding table is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping user-bind autosave** command can retain the configured DHCP snooping binding entries after the device restarts. After a DHCP snooping binding table is generated, you can run the **dhcp snooping user-bind autosave** command to enable local automatic backup of the DHCP snooping binding table.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

This prevents data loss in the DHCP snooping binding table. The suffix of the file must be .tbl.

If the system restarts within one day after the system time is changed, immediately run the **dhcp snooping user-bind autosave** command again to back up the latest dynamic binding entries because it is not the time to update the binding table. If you do not run this command, the lease will be inconsistent with the current system time after the dynamic binding table is restored.

If a device where the DHCP snooping binding table is backed up is powered off and then restarted after the lease of DHCP snooping binding table expires, the DHCP snooping entries cannot be restored.

After this function is enabled, if the interface goes down, the DHCP snooping binding table on the interface will be deleted from the backup binding table file.

Example

Configure the device to back up the DHCP snooping binding table to the file **backup.tbl** in the flash every 5000 seconds.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind autosave flash:/backup.tbl write-delay 5000
```

14.8.36 dhcp snooping user-bind cache enable

Function

The **dhcp snooping user-bind cache enable** command enables the device to cache DHCPv4 and DHCPv6 binding entries.

The **undo dhcp snooping user-bind cache enable** command disables the device from caching DHCPv4 and DHCPv6 binding entries.

By default, the function of caching DHCP snooping binding entries is disabled.

Format

dhcp snooping user-bind cache enable

undo dhcp snooping user-bind cache enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device generates DHCP snooping binding entries for DHCP users. To prevent such entries from being lost immediately after the user interface is removed from the VLAN, run the **dhcp snooping user-bind cache enable** command to enable the device to cache the DHCP snooping binding entries.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Enable the function of caching DHCPv4 and DHCPv6 binding entries.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind cache enable
```

14.8.37 dhcp snooping user-bind ftp

Function

The **dhcp snooping user-bind ftp** command enables the device to automatically back up DHCP snooping binding entries on the remote FTP server.

The **undo dhcp snooping user-bind ftp** command disables the device from automatically backing up DHCP snooping binding entries on the remote FTP server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote FTP server.

Format

dhcp snooping user-bind ftp remotefilename *filename* **host-ip** *ip-address* [**port** *port-number*] **username** *username* **password** *password* [**write-delay** *delay-time*]

undo dhcp snooping user-bind ftp

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the remote FTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote FTP server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. By default, the port number is 21.
username *username*	Specifies the user name to connect to the FTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Parameter	Description	Value
password *password*	Specifies the password to connect to the FTP server.	The value is a string of case-sensitive characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the system backs up DHCP snooping binding entries every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind ftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote FTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The FTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp** command is recommended.

Example

Enable the device to automatically back up DHCP snooping binding entries to the **backup** file on the FTP server at 10.137.12.10 with the FTP user name **test** and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind ftp remotefilename backup host-ip 10.137.12.10 username test
password YsHsjx_202206
```

14.8.38 dhcp snooping user-bind ftp load

Function

The **dhcp snooping user-bind ftp load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote FTP server.

Format

dhcp snooping user-bind ftp load remotefilename *filename* **host-ip** *ip-address* [**port** *port-number*] **username** *username* **password** *password*

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote FTP server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. By default, the port number is 21.
username *username*	Specifies the user name to connect to the FTP server.	The value is a string of 1 to 64 characters without spaces.

Parameter	Description	Value
password *password*	Specifies the password to connect to the FTP server.	The value is a string of characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **dhcp snooping user-bind ftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote FTP server, you can run the **dhcp snooping user-bind ftp load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote FTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The FTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp load** command is recommended.

Example

Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote FTP server at 10.137.12.10 with the FTP user name **test** and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind ftp load remotefilename backup host-ip 10.137.12.10 username
test password YsHsjx_202206
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Downloading the file from the remote FTP server. Please wait...done.
 Total number of dynamic binding table in remote file: 30
 Recovering dynamic binding table, please wait for a moment....
```

```
10 successful, 20 failed.
Binding Collisions         :    20     Exceeds max limits      :     0
Invalid interfaces         :     0     Invalid vlans           :     0
Invalid snp configurations :     0     Expired leases          :     0
Parse failures             :     0
```

Table 14-63 Description of the **dhcp snooping user-bind ftp load** command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
m successful, *n* failed	*m* DHCP snooping binding entries are recovered successfully, and *n* DHCP snooping binding entries fail to be recovered.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.
Exceeds max limits	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlans	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Invalid snp configurations	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.
Expired leases	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

14.8.39 dhcp snooping user-bind http https

Function

The **dhcp snooping user-bind http https** command enables the device to automatically back up DHCP snooping binding entries on the remote HTTP or HTTPS server.

The **undo dhcp snooping user-bind http https** command disables the device from automatically backing up DHCP snooping binding entries on the remote HTTP or HTTPS server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote HTTP or HTTPS server.

Format

dhcp snooping user-bind http { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*] [**write-delay** *delay-time*]

dhcp snooping user-bind https ssl-policy *ssl-policy-name* { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*] [**write-delay** *delay-time*]

undo dhcp snooping user-bind { **http** | **https** }

Parameters

Parameter	Description	Value
ssl-policy *ssl-policy-name*	Specifies the name of the SSL policy used by the HTTPS protocol.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the HTTP or HTTPS server.	The value is a string of 1 to 64 case-sensitive characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the HTTP or HTTPS server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the HTTP or HTTPS server.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
url *url-string*	Specifies the URL of the HTTP or HTTPS server, in the format http://*server_location*/*file_location*, for example, http://10.1.1.1:70/32768snp.txt.	The value is a string of 1 to 200 case-sensitive characters without spaces.
username *username*	Specifies the user name to connect to the HTTP or HTTPS server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password *password*	Specifies the password to connect to the HTTP or HTTPS server.	The value is a string of case-sensitive characters without spaces. It can be a ciphertext password of 48 characters or a plaintext password of 1 to 16 characters. **NOTE** For security purposes, it is recommended that the password contains at least two types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least 8 characters.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the system backs up DHCP snooping binding entries every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind http https** command to enable the device to automatically back up DHCP snooping binding entries on the remote HTTP or HTTPS server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The HTTP protocol will bring risk to device security. The HTTPS protocol is recommended for file operations.

Example

Configure the device to automatically back up DHCP snooping binding entries to the **backup** file on the HTTP server at 10.1.1.1 with the HTTP user name **test** and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind http remotefilename backup host-ip 10.1.1.1 username test
password YsHsjx_202206
```

Configure the device to back up DHCP snooping binding entries to the HTTPS server at 10.1.1.1 and specify the SSL policy name as **s1**, backup file name as **backup**, HTTPS user name as **test**, and HTTPS password as **test@123**.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind https ssl-policy s1 remotefilename backup host-ip 10.1.1.1
username test password test@123
```

14.8.40 dhcp snooping user-bind http https load

Function

The **dhcp snooping user-bind http https load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote HTTP or HTTPS server.

Format

dhcp snooping user-bind http load { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*]

dhcp snooping user-bind https ssl-policy *ssl-policy-name* **load** { **remotefilename** *filename* **host-ip** *ip-address* [**port** *port-number*] | **url** *url-string* } [**username** *username* **password** *password*]

Parameters

Parameter	Description	Value
ssl-policy *ssl-policy-name*	Specifies the name of the SSL policy used by the HTTPS protocol.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the HTTP or HTTPS server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the HTTP or HTTPS server.	The value is an integer that ranges from 1 to 65535.
url *url-string*	Specifies the URL of the HTTP or HTTPS server, in the format http://*server_location*/*file_location*, for example, http://10.1.1.1:70/32768snp.txt.	The value is a string of 1 to 200 case-sensitive characters without spaces.
username *username*	Specifies the user name to connect to the HTTP or HTTPS server.	The value is a string of 1 to 64 characters without spaces.
password *password*	Specifies the password to connect to the HTTP or HTTPS server.	The value is a string of characters without spaces. It can be a ciphertext password of 48 characters or a plaintext password of 1 to 16 characters. **NOTE** For security purposes, it is recommended that the password contains at least two types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least 8 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **dhcp snooping user-bind http https** command to enable the device to automatically back up DHCP snooping binding entries on the remote HTTP or HTTPS server, you can run the **dhcp snooping user-bind http https load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote HTTP or HTTPS server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The HTTP protocol will bring risk to device security. The HTTPS protocol is recommended for file operations.

Example

Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote HTTP server at 10.1.1.1 with the HTTP user name **test** and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind http load remotefilename backup host-ip 10.1.1.1 username test
password YsHsjx_202206
Info: Downloading the file from the remote HTTP server. Please wait...done.
 Total number of dynamic binding table in remote file: 10
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 0 failed.
 Binding Collisions    :     0     Exceeds max limit     :     0
 Invalid interfaces    :     0     Invalid vlan          :     0
 Snooping not enable   :     0     Lease expired         :     0
 Parse failures        :     0
```

Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote HTTPS server at 10.1.1.1 and specify the SSL policy name as **s1**, HTTPS user name as **test**, and HTTPS password as **test@123**.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind https ssl-policy s1 load remotefilename backup host-ip 10.1.1.1
username test password test@123
Info: Downloading the file from the remote HTTPS server. Please wait...done.
 Total number of dynamic binding table in remote file: 10
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 0 failed.
 Binding Collisions    :     0     Exceeds max limit     :     0
 Invalid interfaces    :     0     Invalid vlan          :     0
 Snooping not enable   :     0     Lease expired         :     0
 Parse failures        :     0
```

Table 14-64 Description of the **dhcp snooping user-bind http https load** command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
m successful, *n* failed	*m* DHCP snooping binding entries are recovered successfully, and *n* DHCP snooping binding entries fail to be recovered.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.
Exceeds max limit	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlan	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Snooping not enable	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.
Lease expired	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

14.8.41 dhcp snooping user-bind sftp

Function

The **dhcp snooping user-bind sftp** command enables the device to automatically back up DHCP snooping binding entries on the remote SFTP server.

The **undo dhcp snooping user-bind sftp** command disables the device from automatically backing up DHCP snooping binding entries on the remote SFTP server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote SFTP server.

Format

dhcp snooping user-bind sftp remotefilename *filename* **host-ip** *ip-address* [**port** *port-number*] **username** *username* **password** *password* [**write-delay** *delay-time*]

undo dhcp snooping user-bind sftp

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the remote SFTP server.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote SFTP server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the SFTP server.	The value is an integer that ranges from 1 to 65535. By default, the port number is 22.
username *username*	Specifies the user name to connect to the SFTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Parameter	Description	Value
password *password*	Specifies the password to connect to the SFTP server.	The value is a string of case-sensitive characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the system backs up DHCP snooping binding entries every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind sftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote SFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The suffix of the file must be .tbl.

Example

Enable the device to automatically back up DHCP snooping binding entries to the **backup** file on the SFTP server at 10.137.12.10 with the SFTP user name **test** and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind sftp remotefilename backup host-ip 10.137.12.10 username test
password YsHsjx_202206
```

14.8.42 dhcp snooping user-bind sftp load

Function

The **dhcp snooping user-bind sftp load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote SFTP server.

Format

dhcp snooping user-bind sftp load remotefilename *filename* **host-ip** *ip-address* [**port** *port-number*] **username** *username* **password** *password*

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote SFTP server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the SFTP server.	The value is an integer that ranges from 1 to 65535. By default, the port number is 22.
username *username*	Specifies the user name to connect to the SFTP server.	The value is a string of 1 to 64 characters without spaces.
password *password*	Specifies the password to connect to the SFTP server.	The value is a string of characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **dhcp snooping user-bind sftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote SFTP server, you can run the **dhcp snooping user-bind sftp load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote SFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Example

Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote SFTP server at 10.137.12.10 with the SFTP user name **test** and password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind sftp load remotefilename backup host-ip 10.137.12.10 username
test password YsHsjx_202206
Info: Downloading the file from the remote SFTP server. Please wait...done.
 Total number of dynamic binding table in remote file: 30
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 20 failed.
 Binding Collisions         :   20    Exceeds max limits    :    0
 Invalid interfaces         :    0    Invalid vlans         :    0
 Invalid snp configurations :    0    Expired leases        :    0
 Parse failures             :    0
```

Table 14-65 Description of the **dhcp snooping user-bind sftp load** command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
m successful, *n* failed	*m* DHCP snooping binding entries are recovered successfully, and *n* DHCP snooping binding entries fail to be recovered.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.

Item	Description
Exceeds max limits	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlans	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Invalid snp configurations	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.
Expired leases	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

14.8.43 dhcp snooping user-bind tftp

Function

The **dhcp snooping user-bind tftp** command enables the device to automatically back up DHCP snooping binding entries on the remote TFTP server.

The **undo dhcp snooping user-bind tftp** command disables the device from automatically backing up DHCP snooping binding entries on the remote TFTP server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote TFTP server.

Format

dhcp snooping user-bind tftp remotefilename *filename* **host-ip** *ip-address* [**write-delay** *delay-time*]

undo dhcp snooping user-bind tftp

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the remote TFTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the TFTP server.	The value is in dotted decimal notation.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the interval for local automatic backup of the DHCP snooping binding table is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind tftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote TFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The TFTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp** command is recommended.

Example

Enable the device to automatically back up DHCP snooping binding entries to the **backup** file on the TFTP server at 10.137.12.10 at intervals of 5000s.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind tftp remotefilename backup host-ip 10.137.12.10 write-delay 5000
```

14.8.44 dhcp snooping user-bind tftp load

Function

The **dhcp snooping user-bind tftp load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote TFTP server.

Format

dhcp snooping user-bind tftp load remotefilename *filename* **host-ip** *ip-address*

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote TFTP server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **dhcp snooping user-bind tftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote TFTP server, you can run the **dhcp snooping user-bind tftp load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote TFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The TFTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp load** command is recommended.

Example

Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote TFTP server at 10.137.12.10.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind tftp load remotefilename backup host-ip 10.137.12.10
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
100%
TFTP: Downloading the file successfully.
656 byte(s) received in 1 second(s).
 Total number of dynamic binding table in remote file: 20
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 10 failed.
 Binding Collisions         :    10     Exceeds max limit    :     0
 Invalid interfaces         :     0     Invalid vlan         :     0
 Invalid snp configurations :     0     Expired leases       :     0
 Parse failures             :     0
```

Table 14-66 Description of the dhcp snooping user-bind tftp load command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.
Exceeds max limit	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlan	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Invalid snp configurations	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.
Expired leases	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.

Item	Description
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

14.8.45 dhcp snooping user-offline remove mac-address

Function

The **dhcp snooping user-offline remove mac-address** command enables the device to delete the MAC address entry of a user whose DHCP snooping binding entry is deleted.

The **undo dhcp snooping user-offline remove mac-address** command disables the device from deleting the MAC address entry of a user whose binding entry is deleted.

By default, the device does not delete the MAC address entry of a user whose DHCP snooping binding entry is deleted.

Format

dhcp snooping user-offline remove mac-address

undo dhcp snooping user-offline remove mac-address

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user goes offline but its MAC address entry is not aged, the device forwards the packet whose destination address is the IP address of the user based on the dynamic MAC address entry. After the **dhcp snooping user-offline remove mac-address** command is executed, the user MAC address entry is deleted when the DHCP snooping binding entry is deleted. With the function of discarding unknown unicast packets on the network-side interface, the device discards packets destined to offline users.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Enable the device to delete the MAC address entry of a user whose DHCP snooping binding entry is deleted.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-offline remove mac-address
```

14.8.46 dhcp snooping user-bind upload format ascii

Function

The **dhcp snooping user-bind upload format ascii** command configures DHCP snooping binding entries to be backed up in both ASCII and binary formats.

The **undo dhcp snooping user-bind upload format ascii** command restores the default configuration.

By default, DHCP snooping binding entries are backed up only in binary format when the automatic backup of DHCP snooping binding entries on the remote server is enabled.

Format

dhcp snooping user-bind upload format ascii

undo dhcp snooping user-bind upload format ascii

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, DHCP snooping binding entries are backed up only in binary format when the automatic backup of DHCP snooping binding entries on the remote server is enabled. Huawei switches can restore DHCP snooping binding entries in binary format. However, customers cannot read backup DHCP snooping binding entries in binary format. To resolve this problem, run the **dhcp snooping user-**

bind upload format ascii command to configure the device to back up DHCP snooping binding entries in ASCII and binary formats. Customers then can read DHCP snooping binding entries in ASCII format and store the entries to the local database.

Prerequisites

Backup of DHCP snooping binding entries must be enabled for the remote FTP, HTTP, HTTPS, SFTP, and TFTP servers. Otherwise, the configuration of the **dhcp snooping user-bind upload format ascii** command does not take effect.

Example

Enable the device to back up DHCP snooping binding entries to the file named **backup** on the FTP server at 10.137.12.10 with the FTP user name **test** and password YsHsjx_202206. DHCP snooping binding entries can be backed up in both ASCII and binary formats.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind ftp remotefilename backup host-ip 10.137.12.10 username test
password YsHsjx_202206
[HUAWEI] dhcp snooping user-bind upload format ascii
```

14.8.47 dhcp snooping user-transfer enable

Function

The **dhcp snooping user-transfer enable** command enables location transition for DHCP snooping users.

The **undo dhcp snooping user-transfer enable** command disables location transition for DHCP snooping users.

By default, location transition is enabled for DHCP snooping users.

Format

dhcp snooping user-transfer enable

undo dhcp snooping user-transfer enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a mobile user goes online through interface A, goes offline, and then goes online through interface B, the user sends a DHCP Discover message to apply an IP address. By default, if DHCP snooping is enabled on the device, the device allows the user to go online and updates the DHCP snooping binding entries. However, this may bring security risks. For example, if an attacker pretends an authorized user to send a DHCP Discover message, the authorized user cannot access the network after the DHCP snooping binding table is updated. To prevent such attacks, you can disable the DHCP snooping location transition function. After this function is disabled, the device discards the DHCP Discover messages sent by a user who has an entry in the DHCP snooping binding table (user's MAC address exists in the DHCP snooping binding table) through another interface.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Disable location transition for DHCP snooping users.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] undo dhcp snooping user-transfer enable
```

14.8.48 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 00e0-fc12-3456, the Interface-ID generated during the system parsing process is 0011.0022.00e0fc123456:vlanif100.	-
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: ● Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 14-67**. ● Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. ● Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

Table 14-67 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.

Keyword	Description
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 interface-id format user-defined "%mac"
```

14.8.49 dhcpv6 option18 format

Function

The **dhcpv6 option18 format** command configures the format of the Option 18 field in a DHCPv6 message.

The **undo dhcpv6 option18 format** command restores the default format of the Option 18 field in a DHCPv6 message.

By default, the format of the Option 18 field is not configured in a DHCPv6 message. If the function of adding the Option 18 field to DHCPv6 messages is enabled, DHCPv6 messages are encapsulated in the default format %portname:%svlan.%cvlan %sysname/0/%cssid/%slot/%subslot/%port.

Format

dhcpv6 option18 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option18 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 18 field.	The value is a string of 1 to 251 characters. The details about the user-defined format string are provided in the Usage Guidelines.
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** ● If a VLAN is specified, only the format of the Option 18 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 18 field in all DHCPv6 messages received by the interface is configured. ● If the format of the Option 18 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. ● This parameter is not supported in the VLAN view.	The value is an integer in the range from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer in the range from 1 to 4094.
all	Deletes all formats of the Option 18 field.	-

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **dhcpv6 option18** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 18 field to a DHCPv6 message, you can run the **dhcpv6 option18 format** command to configure the format of the Option 18 field in a DHCPv6 message.

You can use the following keywords to define the Option 18 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- duid: indicates the ID of the client. This keyword is valid only in the string format.
- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of a port, including eth and trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: specifies the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

If the Option 18 format is not customized, the following keywords are used for encapsulation by default:

- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.
- svlan: specifies the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- cssid: indicates the cluster ID. The value is 0 in non-cluster scenarios.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 18 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- "" indicates that the contents in the double quotation marks are encapsulated in ASCII format. Contents that are not enclosed in double quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

- A hexadecimal notation string can contain numerals, spaces, and % + keywords.
- In a hexadecimal notation string, numbers are encapsulated in the Option 18 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
- All the spaces in a hexadecimal character string are ignored.
- By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
- If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
- A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
- If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Precautions

After the **dhcpv6 snooping relay-information enable** command is run in the VLAN view, the **dhcpv6 option18 format** command does not take effect in the VLAN.

Example

Configure the format of the Option 18 field in a DHCPv6 message in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 option18 format user-defined "%length %svlan %5slot %3subslot %8port"
```

Configure the format of the Option 18 field in a DHCPv6 message on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 option18 format user-defined "%length %svlan %5slot
%3subslot %8port"
```

14.8.50 dhcpv6 option37 format

Function

The **dhcpv6 option37 format** command configures the format of the Option 37 field in a DHCPv6 message.

The **undo dhcpv6 option37 format** command restores the default format of the Option 37 field in a DHCPv6 message.

By default, the format of the Option 37 field is not configured in a DHCPv6 message. If the function of adding Option 37 to DHCPv6 messages is enabled, DHCPv6 messages are encapsulated in the default format: enterprise-id:%sysmac.

Format

dhcpv6 option37 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option37 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 37 field.	The value is a string of 1 to 247 characters. The details about the user-defined format string are provided in the Usage Guidelines.
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** • If a VLAN is specified, only the format of the Option 37 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 37 field in all DHCPv6 messages received by the interface is configured. • If the format of the Option 37 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. • This parameter is not supported in the VLAN view.	The value is an integer in the range from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer in the range from 1 to 4094.

Parameter	Description	Value
all	Deletes all formats of the Option 37 field.	-

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dhcpv6 option37** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 37 field to a DHCPv6 message, you can run the **dhcpv6 option37 format** command to configure the format of the Option 37 field in a DHCPv6 message.

You can use the following keywords to define the Option 37 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- duid: indicates the ID of the client. This keyword is valid only in the string format.
- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of a port, including eth and trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: specifies the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.

- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

If the Option 37 format is not customized, the following keywords are used for encapsulation by default:

- enterprise-id: indicates the enterprise code. The value is fixed at 2011: Huawei proprietary message.
- sysmac: indicates the system MAC address of the device.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 37 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- "" indicates that the contents in the double quotation marks are encapsulated in ASCII format. Contents that are not enclosed in double quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 37 field in hexadecimal notation. A number from 0 to 255

occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.

- All the spaces in a hexadecimal character string are ignored.
- By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
- If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
- A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
- If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Precautions

After the **dhcpv6 snooping relay-information enable** command is run in the VLAN view, the **dhcpv6 option37 format** command does not take effect in the VLAN.

Example

Configure the format of the Option 37 field in a DHCPv6 message in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 option37 format user-defined "%length %svlan %5slot %3subslot %8port"
```

Configure the format of the Option 37 field in a DHCPv6 message on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 option37 format user-defined "%length %svlan %5slot
%3subslot %8port"
```

14.8.51 dhcpv6 { option18 | option37 } enable

Function

The **dhcpv6** { **option18** | **option37** } **enable** command enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.

The **undo dhcpv6** { **option18** | **option37** } **enable** command disables the device from adding the Option 18 or Option 37 field to a DHCPv6 message.

By default, the device does not insert the Option 18 or Option 37 field to a DHCPv6 message.

Format

dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

undo dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

Parameters

Parameter	Description	Value
insert	Enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.	-
rebuild	Enables the device to modify the Option 18 or Option 37 field in a DHCPv6 message that carries either option; enables the device to forcibly insert the Option 18 or Option 37 field to a DHCPv6 message that does not carry either option.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The function of Option 18 or Option 37 is similar to that of Option 82 (see the **dhcp option82 enable** command). The Option 18 field contains the port number of a client and the Option 37 field contains the MAC address of a client. The device inserts the Option 18 or Option 37 field to a DHCPv6 Request message to notify the DHCP server of the DHCPv6 client location. As such, the DHCP server can properly assign an IP address and other configurations to the DHCPv6 client, ensuring DHCP client security.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcpv6** { **option18** | **option37** } **enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run this command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

After the **dhcpv6 snooping relay-information enable** command is run in the VLAN view, the **dhcpv6 { option18 | option37 } enable** command does not take effect in the VLAN.

Example

Insert the Option 37 field into DHCPv6 Request messages sent by GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 option37 insert enable
```

14.8.52 dhcpv6 remote-id format

Function

The **dhcpv6 remote-id format** command sets the format of the Remote-ID in DHCPv6 messages.

The **undo dhcpv6 remote-id format** command restores the default format of the Remote-ID in DHCPv6 messages.

By default, the default format of the Remote-ID in DHCPv6 messages is used.

Format

dhcpv6 remote-id format { **default** | **user-defined** *text* }

undo dhcpv6 remote-id format

Parameters

Parameter	Description	Value
default	Indicates to adopt the default format of the remote ID. The default format of the remote ID is %duid %portname:%04svlan.%04cvlan, where the values of the outer VLAN ID and inner VLAN ID are integers and composed of four characters. If the length is shorter than four characters, 0s are prefixed to the value. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is GE0/0/1, and the client DUID is 0003000180FB063545B3, the Remote-ID option generated during the system parsing process is 0003000180FB063545B3 GigabitEthernet 0/0/1:0011.0022.	-

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Remote-ID format. A user-defined format can be: - Format defined by keywords: The Remote-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Remote-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 14-68**. - Format defined by common character strings: The Remote-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Remote-ID can be directly defined as N8. - Mixed format: The Remote-ID is defined by both the keywords and common character strings. For	The value is a string of 3 to 247 case-sensitive characters with spaces.

Parameter	Description	Value
	example, the Remote-ID can be defined as %sysname N8.	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The Remote-ID records user access information such as the DUID of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Remote-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 remote-id format** command to configure the format of the Remote-ID inserted into DHCPv6 packets.

Table 14-68 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.

Keyword	Description
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

The DHCP function has been enabled using the **dhcp enable** command in the system view.

Follow-up Procedure

When the device functions as a DHCPv6 relay, you must run the **dhcpv6 remote-id insert enable** or **dhcpv6 remote-id rebuild enable** command to enable the function of inserting the Remote-ID into DHCPv6 relay packets after running the **dhcpv6 remote-id format** command to configure the Remote-ID format in DHCPv6 packets.

NOTE

When the device functions as an LDRA, the Remote-ID is inserted into DHCPv6 relay packets by default and the function does not need to be enabled.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:

- The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
- An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / . , < > `.
- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Set the customized format for the remote ID carried in DHCPv6 messages and encapsulate the MAC address of the device into the remote ID.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 remote-id format user-defined "%mac"
```

14.8.53 dhcpv6 snooping check relay-forward enable

Function

The **dhcpv6 snooping check relay-forward enable** command enables the function of discarding DHCPv6 Relay-Forward messages.

The **undo dhcpv6 snooping check relay-forward enable** command disables the function of discarding DHCPv6 Relay-Forward messages.

By default, the function of discarding DHCPv6 Relay-Forward messages is disabled.

Format

In the system view:

dhcpv6 snooping check relay-forward enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcpv6 snooping check relay-forward enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

In the VLAN view or interface view:

dhcpv6 snooping check relay-forward enable

undo dhcpv6 snooping check relay-forward enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Discards DHCPv6 Relay-Forward messages received in specified VLANs. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than the value of *vlan-id1*.	The value is an integer in the range from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCPv6 snooping needs to be deployed on access devices on a Layer 2 network or the first DHCPv6 relay agent. Therefore, the device that has DHCPv6 snooping configured should not receive the DHCPv6 Relay-Forward messages forwarded by the relay agent. If the device receives the DHCPv6 Relay-Forward messages, it considers the messages invalid and discards them.

Prerequisites

DHCPv6 snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping enable** command in the VLAN view, the command configuration takes effect only for the DHCP messages from the specified VLAN. If you run this command in the interface view, the command configuration takes effect for all DHCP messages on the specified interface.

Example

Enable the function of discarding DHCPv6 Relay-Forward messages in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 snooping check relay-forward enable
```

Enable the function of discarding DHCPv6 Relay-Forward messages on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 snooping check relay-forward enable
```

14.8.54 dhcpv6 snooping relay-information enable

Function

The **dhcpv6 snooping relay-information enable** command enables Lightweight DHCPv6 Relay Agent (LDRA) for DHCPv6 snooping.

The **undo dhcpv6 snooping relay-information enable** command disables LDRA.

By default, LDRA for DHCPv6 snooping is disabled.

Format

dhcpv6 snooping relay-information enable [**trust**]

undo dhcpv6 snooping relay-information enable [**trust**]

Parameters

Parameter	Description	Value
trust	Configures the device to trust the received Relay-Forward messages. If this parameter is not specified, the device does not trust the received Relay-Forward messages.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

In some scenarios, for example, interfaces in the same VLAN have different network access rights and QoS requirements, the DHCPv6 server must be able to detect user access locations, and assign corresponding access control and QoS policies. The DHCPv6 relay agent is usually configured on the gateway. The relay agent can record user access locations; however, if access devices are located between the relay agent and users, the relay agent cannot detect the access locations of users.

LDRA can meet the requirements of these scenarios. LDRA is configured on the user-side access device. The LDRA-enabled device can forward user access locations (such as the network-side interfaces on clients) to the DHCPv6 server. The DHCPv6 server delivers policies to users accordingly.

This command enables LDRA for DHCPv6 snooping and configures the handling methods for received Relay-Forward messages:

- Trust: The device forwards the received Relay-Forward messages to the DHCPv6 server. This method is usually used when multiple LDRA-enabled devices are directly connected. If the downstream LDRA-enabled device trusts the Relay-Forward messages from the upstream LDRA-enabled device, this method can be used.
- Untrust: The device discards the received Relay-Forward messages. This method is usually used when an LDRA-enabled device directly connects to users, and the users may send invalid Relay-Forward messages.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The LDRA function only records the client location information and forwards the information to the DHCPv6 server. The differentiated policies for IP address allocation, accounting, access control, and QoS are configured on the DHCPv6 server.

Example

Enable LDRA for DHCPv6 snooping in VLAN10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 snooping relay-information enable
```

14.8.55 dhcpv6 snooping user-bind detect confirm-client enable

Function

The **dhcpv6 snooping user-bind detect confirm-client enable** command enables the confirm-client probing function of DHCPv6 snooping.

The **undo dhcpv6 snooping user-bind detect confirm-client enable** command disables the confirm-client probing function of DHCPv6 snooping.

By default, the confirm-client probing function is enabled.

Format

dhcpv6 snooping user-bind detect confirm-client enable

undo dhcpv6 snooping user-bind detect confirm-client enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a binding entry is generated for a client using the DHCPv6 Confirm packet, this client is a confirm-client. When the client goes online again, it sends a DHCPv6 Confirm packet.

When a user-side interface receives the DHCPv6 Confirm packet, a DHCPv6 snooping binding entry is generated for the client. Because the DHCPv6 Confirm packet does not contain lease information, the binding entry of the client cannot be deleted immediately when the client goes offline. This occupies binding table space and new users may fail to go online.

After the confirm-client probing function is enabled, DHCPv6 snooping periodically sends DAD NS packets to detect whether the confirm-client is online. The DHCPv6 snooping entries are promptly deleted when the confirm-clients go offline.

Prerequisites

The **dhcp snooping enable ipv6** command has been executed to enable DHCPv6 snooping.

Example

Enable confirm-client probing of DHCPv6 snooping.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv6
[HUAWEI] dhcpv6 snooping user-bind detect confirm-client enable
```

14.8.56 dhcpv6 snooping user-bind detect retransmit

Function

The **dhcpv6 snooping user-bind detect retransmit** command sets the number of times and interval at which the DAD NS packets are sent for DHCPv6 snooping.

The **undo dhcpv6 snooping user-bind detect retransmit** command restores the default number of times and interval at which the DAD NS packets are sent for DHCPv6 snooping.

By default, a DAD NS packet is sent up to three times at the interval of 180 seconds.

Format

dhcpv6 snooping user-bind detect retransmit *times* **interval** *interval*

undo dhcpv6 snooping user-bind detect retransmit

Parameters

Parameter	Description	Value
times	Specifies the number of times a DAD NS packet is sent.	The value is an integer that ranges from 1 to 10.
interval *interval*	Specifies the interval for sending DAD NS packets.	The value is an integer that ranges from 60 to 86400, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of enabling DHCPv6 snooping to detect whether the confirm-client is online is enabled using the **dhcpv6 snooping user-bind detect confirm-client enable** command, the DHCPv6 snooping-enabled device will periodically send DAD NS packets to detect whether the confirm-client is online and delete the DHCPv6 snooping entry of the offline confirm-client. You can change the number of times and interval at which the DHCPv6 snooping-enabled device sends DAD NS packets as required.

Prerequisites

The **dhcp snooping enable ipv6** command has been executed to enable DHCPv6 snooping.

Example

Set the number of times and interval at which the DAD NS packets are sent to 2 and 60 seconds, respectively.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv6
[HUAWEI] dhcpv6 snooping user-bind detect retransmit 2 interval 60
```

14.8.57 dhcpv6 snooping user-bind mac-conflict detect enable

Function

The **dhcpv6 snooping user-bind mac-conflict detect enable** command enables DHCPv6 snooping for detecting whether a user is online.

The **undo dhcpv6 snooping user-bind mac-conflict detect enable** command disables DHCPv6 snooping from detecting whether a user is online.

By default, DHCPv6 snooping is disabled from detecting whether a user is online.

Format

dhcpv6 snooping user-bind mac-conflict detect enable

undo dhcpv6 snooping user-bind mac-conflict detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After binding entries are generated, you can run the **dhcp snooping check dhcpv6-request mac** command to enable the function of checking the validity of DHCPv6 messages based on MAC addresses. Then the device searches for the binding entries based on the MAC address entry that is used as the key. The device checks whether the Request messages sent by the DHCPv6 client match any binding entry. If they match, the device forwards the messages; otherwise, the device discards the messages. This prevents unauthorized users from sending bogus DHCPv6 messages to extend the IP address lease or release IP addresses. When determining that a DHCPv6 message is invalid, the device discards it. In this case, you can enable the function of detecting whether DHCPv6 users are online. DHCPv6 snooping then sends DAD NS packets at an interval of 3 seconds for three times to detect whether a DHCPv6 user is online. If no response packet is received from the DHCPv6 user within the timeout period, the device considers that the user is offline and deletes the DHCPv6 snooping entry of the offline user.

Prerequisites

1. The **dhcp snooping enable ipv6** command has been run to enable DHCPv6 snooping globally.
2. The **dhcp snooping check dhcpv6-request mac** command has been run to enable the function of checking the validity of DHCPv6 messages based on MAC addresses.

Example

Enable DHCPv6 snooping for detecting whether a user is online.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
```

```
[HUAWEI] dhcp snooping enable ipv6
[HUAWEI] dhcpv6 snooping user-bind mac-conflict detect enable
```

14.8.58 display dhcp option82 configuration

Function

The **display dhcp option82 configuration** command displays the DHCP Option 82 configuration.

Format

display dhcp option82 configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP Option 82 configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP Option 82 configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can properly assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

After the Option 82 field is inserted to a DHCP message, run the **display dhcp option82 configuration** command to display the DHCP Option 82 configuration.

Example

Display all the DHCP Option82 configurations.

```
<HUAWEI> display dhcp option82 configuration
#
dhcp option82 vendor-specific format vendor-sub-option 1 ascii 22
#
interface GigabitEthernet0/0/1
 dhcp option82 subscriber-id format ascii 222
 dhcp option82 insert enable
 dhcp option82 encapsulation circuit-id
 dhcp option82 append vendor-specific
 dhcp option82 circuit-id format common
#
```

Table 14-69 Description of the **display dhcp option82 configuration** command output

Item	Description
interface *ifn*	Option 82 configuration on interface *ifn*.
dhcp option82 vendor-specific format vendor-sub-option *i* ascii *text1*	The Sub9 of the old format is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **dhcp option82 vendor-specific format** command.
dhcp option82 subscriber-id format ascii *text2*	The Sub6 suboption is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **dhcp option82 subscriber-id format** command.
dhcp option82 insert enable	The function of inserting Option 82 to DHCP messages is enabled and the insertion method is configured: ● dhcp option82 rebuild enable: Rebuild mode ● dhcp option82 insert enable: Insert mode To specify the parameter, run the **dhcp option82 enable** command.
dhcp option82 encapsulation circuit-id	The suboption inserted into the Option 82 field of DHCP messages is configured. To specify the parameter, run the **dhcp option82 encapsulation** command.
dhcp option82 append vendor-specific	The Sub9 of the new format is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **dhcp option82 append vendor-specific** command.

Item	Description
dhcp option82 circuit-id format common	Format of the circuit-id suboption. To specify the parameter, run the **dhcp option82 format** command.

14.8.59 display dhcp snooping

Function

The **display dhcp snooping** command displays DHCP snooping running information.

Format

display dhcp snooping [**interface** *interface-type interface-number* | **vlan** *vlan-id* | **bridge-domain** *bd-id*]

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP snooping running information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays DHCP snooping running information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
bridge-domain *bd-id*	Displays DHCP snooping running information in a specified BD.	The BD ID must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp snooping** command displays DHCP snooping running information. If no interface or VLAN is specified, global DHCP snooping running information is displayed. If an interface or a VLAN ID is specified, DHCP snooping running information of the interface or VLAN is displayed.

Example

Display global DHCP snooping running information.

```
<HUAWEI> display dhcp snooping
 DHCP snooping global running information   :
 DHCPv4 snooping                           : Enable
 DHCPv6 snooping                           : Enable
 Static user max number                    : 1024
 Current static user number                : 1
 Dhcp user(dhcpv4/dhcpv6/nd) max number     : 4096
 Dhcp user(dhcpv4/dhcpv6) max number        : 3000
 Nd user max number                        : 1000
 Current dhcpv4 user number                 : 0
 Current dhcpv6 user number                 : 0
 Current nd user number                    : 0
 Arp dhcp-snooping detect                  : Disable  (default)
 Alarm threshold                           : 100      (default)
 Check dhcp-rate                           : Disable  (default)
 Dhcp-rate limit(pps)                      : 100      (default)
 Alarm dhcp-rate                           : Disable  (default)
 Alarm dhcp-rate threshold                 : 100      (default)
 Discarded dhcp packets for rate limit      : 0
 Bind-table autosave                       : Disable  (default)
 Client position transfer allowed          : Enable   (default)
 DHCPv6 confirm-client online detection     : Enable   (default)
 DHCPv6 client online detection times       : 3        (default)
 DHCPv6 client online detection interval    : 180      (default)
 Check dhcpv6-rate                         : Disable  (default)
 Dhcpv6-rate limit(pps)                    : 100      (default)
 Alarm dhcpv6-rate                         : Enable
 Alarm dhcpv6-rate threshold               : 10
 Discarded dhcpv6 packets for rate limit    : 0
 DHCP snooping packet-flow log             : Disable  (default)

 DHCP snooping running information for interface GigabitEthernet0/0/1   :
 DHCP snooping                             : Enable
 Trusted interface                         : No
 Dhcp user(dhcpv4/dhcpv6/nd) max number     : 4096
 Current dhcpv4 user number                 : 0
 Current dhcpv6 user number                 : 0
 Current nd user number                    : 0
 Check dhcp-giaddr                         : Enable
 Check dhcp-chaddr                         : Disable  (default)
 Alarm dhcp-chaddr                         : Disable  (default)
 Check dhcp-request                        : Disable  (default)
 Alarm dhcp-request                        : Disable  (default)
 Check dhcp-rate                           : Enable
 Dhcp-rate limit(pps)                      : 100
 Alarm dhcp-rate                           : Enable
 Alarm dhcp-rate threshold                 : 100
 Discarded dhcp packets for rate limit      : 0
 Alarm dhcp-reply                          : Disable  (default)
 Check dhcpv6-rate                         : Enable
 Dhcpv6-rate limit(pps)                    : 100
 Alarm dhcpv6-rate                         : Enable
 Alarm dhcpv6-rate threshold               : 10
 Discarded dhcpv6 packets for rate limit    : 0
 Alarm dhcpv6-request                      : Enable
 Alarm dhcpv6-request threshold            : 100
```

```
Discarded dhcpv6 packets for check request : 0
DHCPv6 snooping check relay-forward        : Enable
Check dhcpv6-request                       : Disable  (default)
```

Table 14-70 Description of the **display dhcp snooping** command output

Item	Description
DHCPv4 snooping	Whether DHCPv4 snooping is enabled globally. To enable DHCP snooping, run the **dhcp snooping enable** command.
DHCPv6 snooping	Whether DHCPv6 snooping is enabled globally. To enable DHCP snooping, run the **dhcp snooping enable** command.
DHCP snooping	Whether DHCP snooping is enabled on an interface or in a VLAN. To enable DHCP snooping, run the **dhcp snooping enable** command.
Static user max number	Maximum number of static users.
Current static user number	Number of current static users.
Dhcp user(dhcpv4/dhcpv6/nd) max number	Shared specifications of the DHCPv4 snooping, ND snooping, and DHCPv6 snooping binding tables.
Dhcp user(dhcpv4/dhcpv6) max number	Maximum number of DHCPv4 snooping and DHCPv6 snooping users that can be set using a command. To configure this item, run the **dhcp snooping max-user-number** command. If this command is not configured, the item is not displayed.
Nd user max number	Maximum number of ND snooping users that can be set using a command. To configure this item, run the **nd snooping max-user-number** command. If this command is not configured, the item is not displayed.
Current dhcpv4 user number	Number of currently online DHCPv4 users.
Current dhcpv6 user number	Number of currently online DHCPv6 users.
Current nd user number	Number of currently online ND users.

Item	Description
Arp dhcp-snooping detect	Whether association between ARP and DHCP snooping is enabled. To enable association between ARP and DHCP snooping, run the **arp dhcp-snooping-detect enable** command.
Alarm threshold	Global alarm threshold for the number of discarded DHCP snooping messages. To set the global alarm threshold for the number of discarded DHCP snooping messages, run the **dhcp snooping alarm threshold** command.
Check dhcp-rate	Whether a device is enabled to check the rate of sending DHCP messages. To enable the device to check the rate of sending DHCP messages, run the **dhcp snooping check dhcp-rate enable** command.
Dhcp-rate limit(pps)	Rate limit of DHCP messages, in pps. To set the rate limit of DHCP messages, run the **dhcp snooping check dhcp-rate** command.
Alarm dhcp-rate	Whether trap for checking the rate of sending DHCP messages to the processing unit is enabled. To enable trap for checking the rate of sending DHCP messages to the processing unit, run the **dhcp snooping alarm dhcp-rate enable** command.
Alarm dhcp-rate threshold	Alarm threshold for the number of discarded DHCP messages. An alarm is generated if the number of discarded DHCP messages reaches the alarm threshold. To set the alarm threshold for the number of discarded DHCP messages, run the **dhcp snooping alarm dhcp-rate threshold** command.
Discarded dhcp packets for rate limit	Number of discarded DHCP messages whose rate exceeds the rate limit.

Item	Description
Bind-table autosave	Whether a device is enabled to save the DHCP snooping binding table. To enable the device to save the binding table, run the **dhcp snooping user-bind autosave** command.
Client position transfer allowed	Whether location transition is enabled for DHCP snooping users. To enable location transition for DHCP snooping users, run the **dhcp snooping user-transfer enable** command.
DHCPv6 confirm-client online detection	Whether the confirm-client probing function of DHCPv6 snooping is enabled. To configure the confirm-client probing function of DHCPv6 snooping, run the **dhcpv6 snooping user-bind detect confirm-client enable** command.
DHCPv6 client online detection times	Number of times that the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online. To configure the number of times that the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online, run the **dhcpv6 snooping user-bind detect retransmit** command.
DHCPv6 client online detection interval	Interval at which the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online. To configure the number of times that the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online, run the **dhcpv6 snooping user-bind detect retransmit** command.
Check dhcpv6-rate	Whether a device is enabled to check the rate of sending DHCPv6 messages. To enable a device to check the rate of sending DHCPv6 messages, run the **dhcp snooping check dhcpv6-rate enable** command.

Item	Description
Dhcpv6-rate limit(pps)	Rate limit of DHCPv6 messages, in pps. To configure the rate limit of DHCPv6 messages, run the **dhcp snooping check dhcpv6-rate** command.
Alarm dhcpv6-rate	Whether a device is enabled to generate an alarm when the rate of sending DHCPv6 messages to the processing unit exceeds the alarm threshold. To enable the device to generate an alarm when the rate of sending DHCPv6 messages to the processing unit exceeds the alarm threshold, run the **dhcp snooping alarm dhcpv6-rate enable** command.
Alarm dhcpv6-rate threshold	Alarm threshold for the number of discarded DHCPv6 messages. An alarm is generated if the number of discarded DHCPv6 messages reaches the alarm threshold. To configure the alarm threshold for the number of discarded DHCPv6 messages, run the **dhcp snooping alarm dhcpv6-rate threshold** command.
Discarded dhcpv6 packets for rate limit	Number of discarded DHCPv6 messages whose rate exceeds the rate limit.
DHCP snooping packet-flow log	Whether the log function is enabled for DHCP message exchange: ● Enable: The function is enabled. ● Disable: The function is disabled. To configure this function, run the **dhcp snooping packet-flow log enable** command.
Trusted interface	Whether an interface is a trusted interface. To configure an interface as a trusted interface, run the **dhcp snooping trusted** command.

Item	Description
Check dhcp-giaddr	Whether a device is enabled to check the GIADDR field in a DHCP Request message. To enable the device to check the GIADDR field in a DHCP Request message, run the **dhcp snooping check dhcp-giaddr enable** command.
Check dhcp-chaddr	Whether a device is enabled to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header. To enable the device to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header, run the **dhcp snooping check dhcp-chaddr enable** command.
Alarm dhcp-chaddr	Whether a device is enabled to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold. To enable the device to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold, run the **dhcp snooping alarm enable** command.
Check dhcp-request	Whether an interface is enabled to check DHCP Request messages. To enable the interface to check DHCP Request messages, run the **dhcp snooping check dhcp-request enable** command.

Item	Description
Alarm dhcp-request	Whether a device is enabled to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold. To enable the device to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold, run the **dhcp snooping alarm enable** command.
Alarm dhcp-reply	Whether a device is enabled to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface. To enable the device to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface, run the **dhcp snooping alarm enable** command.
Alarm dhcpv6-request	Whether a device is enabled to generate an alarm when an interface discards a DHCPv6 Request message from an untrusted interface. To enable the device to generate an alarm when an interface discards a DHCPv6 Request message from an untrusted interface, run the **dhcp snooping alarm enable** command.
Alarm dhcpv6-request threshold	Alarm threshold for the number of discarded DHCPv6 Request messages that are received from untrusted interfaces. To configure the alarm threshold, run the **dhcp snooping alarm threshold** command.
Discarded dhcpv6 packets for check request	Number of discarded DHCPv6 messages whose rate exceeds the rate limit.
DHCPv6 snooping check relay-forward	Whether the function of discarding DHCPv6 Relay-Forward messages is enabled. To configure this function, run the **dhcpv6 snooping check relay-forward enable** command.

Item	Description
Check dhcpv6-request	Whether the function of checking the validity of DHCPv6 messages based on MAC addresses is enabled. To configure this function, run the **dhcp snooping check dhcpv6-request mac** command.

14.8.60 display dhcp snooping configuration

Function

The **display dhcp snooping configuration** command displays the DHCP snooping configuration.

Format

display dhcp snooping configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number* | **bridge-domain** *bd-id*]

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP snooping configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP snooping configuration on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
bridge-domain *bd-id*	Displays DHCP snooping running information in a specified BD.	The BD ID must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping configuration is complete, run the **display dhcp snooping configuration** command to view the DHCP snooping configuration. If no VLAN or interface is specified, all the DHCP snooping configurations are displayed. If a VLAN or an interface is specified, only the DHCP snooping configuration in the VLAN or on the interface is displayed.

Example

Display all the DHCP snooping configurations.

```
<HUAWEI> display dhcp snooping configuration
#
dhcp snooping enable
#
vlan 3
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
#
```

14.8.61 display dhcp snooping statistics

Function

The **display dhcp snooping statistics** command displays statistics about received DHCP messages.

Format

display dhcp snooping statistics { **bridge-domain** *bd-id* | **global** | **interface** *interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [**interface** *interface-type interface-number*] }

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
bridge-domain *bd-id*	Displays DHCP snooping statistics in a specified BD.	The value is an integer that ranges from 1 to 16777215.
global	Displays all DHCP snooping statistics on the device.	-
vlan *vlan-id*	Displays DHCP snooping statistics in a specified VLAN.	The value is an integer in the range from 1 to 4094.
interface *interface-type interface-number*	Displays DHCP snooping statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view statistics about the received DHCP messages of all types, run the **display dhcp snooping statistics** command.

Example

Display DHCP snooping statistics on a specified interface.

```
<HUAWEI> display dhcp snooping statistics interface gigabitethernet 0/0/1
 DHCP Snooping Statistics:
 Dropped by mac-address check:   0
 Dropped by untrust reply:       0
 Dropped by request check:       0
 Dropped by requestv6 check:     0
 Dropped by no trust port:       0
 Dropped by deny dhcp:           0
```

Display DHCP snooping statistics in a specified BD.

```
<HUAWEI> display dhcp snooping statistics bridge-domain 300
 DHCP Snooping Statistics:
```

```
  Dropped by mac-address check:   0
  Dropped by untrust reply:       0
  Dropped by request check:       0
  Dropped by requestv6 check:     0
  Dropped by no trust port:       0
 Dropped by deny dhcp:            0
```

Display all DHCP snooping statistics on the device.

```
<HUAWEI> display dhcp snooping statistics global
 DHCP Snooping Statistics:

 Client Request:
  Dhcp Discover:                  0
  Dhcp Request:                   0
  Dhcp Decline:                   0
  Dhcp Release:                   0
  Dhcp Inform:                    0
 Server Reply:
  Dhcp Offer:                     0
  Dhcp Ack:                       0
  Dhcp Nak:                       0
 Drop Packet:
  Dropped by mac-address check:   0
  Dropped by untrust reply:       0
  Dropped by request conflict:    0
  Dropped by no trust port:       0
  Dropped by deny dhcp:           0
 Delete DHCP snooping table:
  Receive release packet:         0
  Receive decline packet:         0
  Lease expired:                  0
  User command:                   0
  Client transfers:               0
  Interface down:                 0
  Arp detect:                     0
  Ucm notify:                     0
 Terminal Identity:
  Single upload count:            0
  Batch get count:                0
  Batch upload count:             0
```

Table 14-71 Description of the **display dhcp snooping statistics** command output

Item	Description
DHCP Snooping Statistics	DHCP snooping statistics.
Client Request	Number of messages sent by DHCP clients: - DHCP Discover messages - DHCP Request messages - DHCP Decline messages - DHCP Release messages - DHCP Inform messages

Item	Description
Server Reply	Number of messages sent by the DHCP server: - DHCP Offer messages - DHCP ACK messages - DHCP NAK messages
Drop Packet	Number of discarded messages.
Dropped by mac-address check	Number of discarded DHCP messages whose MAC address is different from the CHADDR field.
Dropped by untrust reply	Number of untrusted reply messages that are discarded.
Dropped by request check	Number of DHCP Request messages discarded on an interface due to mismatch of any DHCP snooping binding entry.
Dropped by requestv6 check	Number of DHCPv6 Request messages discarded on an interface due to mismatch of any DHCPv6 snooping binding entry.
Dropped by request conflict	Number of packets that are discarded because the client and server MAC addresses conflict.
Dropped by untrust relay-forw	Number of untrusted Relay-Forward messages that are discarded.
Dropped by no trust port	Number of messages discarded because no trusted interface is configured.
Dropped by deny dhcp	Number of DHCP messages discarded because the function of discarding DHCP messages is enabled.
Dropped by relay-forward check	Number of discarded DHCPv6 Relay-Forward messages.
Delete DHCP snooping table	Number of DHCP snooping binding entries deleted by the device.
Receive release packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP Release messages.
Receive decline packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP Decline messages.
Lease expired	Number of DHCP snooping binding entries deleted by the device because of lease expiry.

Item	Description
User command	Number of DHCP snooping binding entries deleted using commands.
Client transfers	Number of DHCP snooping binding entries deleted because the client connects to another interface on the device.
Interface down	Number of DHCP snooping binding entries deleted because the port is shut down.
Arp detect	Number of DHCP snooping binding entries deleted due to ARP probe.
Ucm notify	Number of times the UCM module requests DHCP snooping to delete user binding entries.
Terminal Identity	Terminal identity.
Single upload count	Number of times that the DHCP snooping module reports a single user entry.
Batch get count	Number of times that the device requests to obtain entry information in a batch from the DHCP snooping module.
Batch upload count	Number of times that the DHCP snooping module reports entry information in a batch.

14.8.62 display dhcp snooping user-bind

Function

The **display dhcp snooping user-bind** command displays information about the DHCP snooping dynamic binding table.

Format

display dhcp snooping user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* | **bridge-domain** *bd-id* } * | **all** } [**verbose**]

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries mapping a specified interface. In the preceding information: - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays binding entries mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays binding entries mapping a specified MAC address.	The value is in H-H-H format. Each H is a hexadecimal number of 4 digits.
vlan *vlan-id*	Displays binding entries mapping a specified VLAN ID.	The value is an integer in the range from 1 to 4094.
bridge-domain *bd-id*	Displays DHCP snooping running information in a specified BD.	The BD ID must already exist.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table. A binding entry contains the MAC address, IP address, interface connecting to the DHCP client, and ID of the VLAN to which the interface belongs. You can run the **display dhcp snooping user-bind** command to view the DHCP snooping binding table.

Example

Display information about the DHCP snooping binding table.

- Display information about all binding entries.

```
<HUAWEI> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address       MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Interface      Lease
--------------------------------------------------------------------------------
10.1.28.141      00e0-fc12-3456  10                        GE0/0/1        2008.10.17-07:31
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

- Display detailed information about the DHCP snooping binding table by specifying the **verbose** parameter.

```
<HUAWEI> display dhcp snooping user-bind all verbose
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address     : 10.10.21.254
 MAC Address    : 00e0-fc12-3456
 Bridge-domain : 1
 VSI            : --
 VLAN(O/I/P)    : 10  /--  /--
 Interface      : GE0/0/1
 Renew time     : 2020.08.26-11:58
 Expire time    : 2019.08.27-11:58
 Cache time     : 2022.10.27-23:32
 Gateway        : 10.10.21.1
 Server-ip      : 10.10.21.1
 Discover time : 2020.08.26-11:58:20:920
 Ack time       : 2020.08.26-11:58:23:660
 Option12       : Tesgine2000
 Option55       : 1 15 3 6 44 46 47 43 77
 Option60       : DEC
 OptionList     : 12 50 53 54 55 60 61 255
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 14-72 Description of the **display dhcp snooping user-bind** command output

Item	Description
DHCP Dynamic Bind-table	DHCP snooping dynamic binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	O indicates the outer VLAN ID; I indicates the inner VLAN ID; P indicates the mapped VLAN ID.
IP Address	User IP address.
MAC Address	User MAC address.

Item	Description
VSI	Name of the VPN instance that the online user belongs to. **NOTE** If **verbose** is not specified, only one of VSI, (BD-VLAN), and VLAN (O/I/P) is displayed.
VLAN (O/I/P)	Outer VLAN ID, inner VLAN ID, or mapped VLAN ID of the online user. **NOTE** If **verbose** is not specified, only one of VSI, (BD-VLAN), and VLAN (O/I/P) is displayed.
(BD-VLAN)	BD and the VLAN to which the BD is bound. **NOTE** If **verbose** is not specified, only one of VSI, (BD-VLAN), and VLAN (O/I/P) is displayed.
Bridge-domain	Broadcast domain.
Interface	Interface through which a user goes online.
Renew time	Entry update time.
Expire time	Aging time of entries.
Cache time	Cache time of entries.
IPSG Status	IPv4 effective indicates that IPv4 packet check takes effect. slot: <3> indicates that the slot ID is 3.
Lease	Time when the lease of the IP address used by a user expires.
Gateway	Gateway IP address.
Server-ip	IP addresses of the DHCP server.
Discover time	Time when the access device receives a DHCP request message.
Ack time	Time when the access device receives a DHCP ACK message.
Option12	DHCP Option 12 information carried by a user packet. This field is displayed only when a user packet carries this attribute.
Option55	DHCP Option 55 information carried by a user packet. This field is displayed only when a user packet carries this attribute.
Option60	DHCP Option 60 information carried by a user packet. This field is displayed only when a user packet carries this attribute.

Item	Description
OptionList	DHCP Option information carried by a user packet. This field is displayed only when a user packet carries this attribute.

14.8.63 display dhcpv6 snooping statistics

Function

The **display dhcpv6 snooping statistics** command displays DHCPv6 snooping statistics.

Format

display dhcpv6 snooping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display DHCPv6 snooping statistics.

```
<HUAWEI> display dhcpv6 snooping statistics
DHCPV6 Snooping Statistics:
--------------------------------------------------------------------------------
 DHCPV6 packets received from clients:
   Solicit                 : 3
   Request                 : 3
   Renew                   : 36
   Rebind                  : 0
   Inform                  : 0
   Release                 : 2
   Confirm                 : 394213
   Decline                 : 0
   Relay-forward           : 0
 DHCPV6 packets received from servers:
   Advertise               : 3
   Reply                   : 43
   Relay-reply             : 0
 DHCPV6 Packets Dropped:
```

```
  LDRA distrust relay-forward    : 0
  Src mac conflict with server   : 0
  Not allow client transfer      : 0
  Fake server                    : 0
  Reach savi user max number     : 0
  Reach dhcp user max number     : 0
  untrust relay-forw             : 0
  relay-forward check            : 0
  Check dhcpv6-request mac       : 0
  Deny dhcpv6                    : 0
 DHCPV6 snooping user-bind table deleted:
  Receive release packet         : 2
  Receive decline packet         : 0
  Exceed lifetime                : 0
  User command                   : 0
  Client transfer                : 0
  Interface down                 : 1
  Confirm-reply with error code  : 0
  Confirm-client offline         : 2
  Check mac client offline       : 0
 DAD NS packets sent to clients   : 16
 NA packets received from clients : 0
-------------------------------------------------------------------------------
```

Table 14-73 Description of the **display dhcpv6 snooping statistics** command output

Item	Description
DHCPV6 Snooping Statistics	DHCPv6 snooping statistics.
DHCPV6 packets received from clients	Number of DHCPv6 packets received from clients.
Solicit	Number of received Solicit packets.
Request	Number of received Request packets.
Renew	Number of received Renew packets.
Rebind	Number of received Rebind packets.
Inform	Number of received Inform packets.
Release	Number of received Release packets.
Confirm	Number of received Confirm packets.
Decline	Number of received Decline packets.
Relay-forward	Number of received Relay-Forward packets.
DHCPV6 packets received from servers	Number of DHCPv6 packets received from servers.
Advertise	Number of received Advertise packets.
Reply	Number of received Reply packets.
Relay-reply	Number of received Relay-reply packets.
DHCPV6 Packets Dropped	Number of discarded DHCPv6 packets.

Item	Description
LDRA distrust relay-forward	Number of Relay-Forward packets discarded by the LDRA untrusted port from the upstream LDRA.
Src mac conflict with server	When the source MAC address of a DHCPv6 packet from a client conflicts with the DHCPv6 server's MAC address, the DHCPv6 packet is discarded. The field indicates the number of DHCPv6 packets discarded for this reason.
Not allow client transfer	After clients are not allowed to change access interfaces, if a DHCPv6 snooping binding entry of a client exists on the original interface and the client attempts to change the access interface, the DHCPv6 packets from this client are discarded. The field indicates the number of DHCPv6 packets discarded for this reason. To configure this item, run the **undo dhcp snooping user-transfer enable** command.
Fake server	Number of packets discarded by the DHCP snooping-enabled interface from the DHCPv6 server. To configure this item, run the **dhcp snooping enable** command.
Reach savi user max number	Number of packets from clients discarded because the maximum number of SAVI binding entries that can be learned by the interface is reached.
Reach dhcp user max number	Number of packets from clients discarded because the maximum number of DHCP snooping binding entries that can be learned by the interface is reached.
untrust relay-forw	Number of Relay-Forward packets discarded by an LDRA untrusted interface.
relay-forward check	Number of discarded DHCPv6 Relay-Forward packets after the **dhcpv6 snooping check relay-forward enable** command is executed.
Check dhcpv6-request mac	Number of DHCPv6 packets that are discarded after the function of checking the validity of DHCPv6 packets based on MAC addresses is enabled.

Item	Description
Deny dhcpv6	Number of DHCPv6 messages discarded because the function of discarding DHCPv6 messages is enabled.
DHCPV6 snooping user-bind table deleted	Number of deleted DHCPv6 snooping binding entries.
Receive release packet	Number of binding entries deleted after receiving Release packets.
Receive decline packet	Number of binding entries deleted after receiving Decline packets.
Exceed lifetime	Number of binding entries that are aged out (the lease time is the same as that on client).
User command	Number of binding entries deleted using the **reset dhcp snooping user-bind** command.
Client transfer	After a client disconnects from one interface and connects to another one, the binding entry of the client on the original interface is deleted. The field indicates the number of binding entries deleted on original interfaces.
Interface down	Number of binding entries deleted because the interface physical status becomes Down.
Confirm-reply with error code	After a Confirm packet is received, a binding entry is generated. If a Reply packet in which the status code is not 0 is received within the timeout period (10 seconds), the generated binding entry is deleted. The field indicates the number of binding entries deleted for this reason.
Confirm-client offline	After the confirm-client probing function is enabled, an NA packet is returned for every DAD NS packet. If no NA packet is received when the maximum number of retransmission times of a DAD NS packet is reached, the binding entry is deleted. The field indicates the number of binding entries deleted for this reason.

Item	Description
Check mac client offline	Number of binding entries deleted because the device detects that users have gone offline after DHCPv6 snooping is enabled for detecting whether users are online.
DAD NS packets sent to clients	Number of DAD NS packets sent for confirm-client probing.
NA packets received from clients	Number of NA packets received from confirm-client probing.

14.8.64 display dhcpv6 snooping user-bind

Function

The **display dhcpv6 snooping user-bind** command displays the DHCPv6 snooping binding table.

Format

display dhcpv6 snooping user-bind { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **confirm-client** | **all** } [**verbose**]

display dhcpv6 snooping user-bind ipv6-prefix { *prefix/prefix-length* | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer in the range from 1 to 4094.
ipv6-prefix	Displays an IPv6 suffix binding entry.	-
prefix/*prefix-length*	Displays the binding entry mapping a specified IPv6 prefix.	*prefix* is a 32-digit hexadecimal number, in the format of X:X::X:X. *prefix-length* is an integer that ranges from 1 to 128.
confirm-client	Displays the DHCPv6 snooping binding entries generated using DHCPv6 Confirm packets.	-
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table. If the parameter is not specified, brief information about the binding table is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table. A binding entry contains the MAC address, IP address, interface connecting to the DHCP client, and ID of the VLAN to which the interface belongs. You can run the **display dhcpv6 snooping user-bind** command to view the DHCPv6 snooping binding table.

If prefix delegation (PD) users exist on the network, the device generates an IPv6 prefix binding entry. The **display dhcpv6 snooping user-bind ipv6-prefix** command displays IPv6 prefix binding entries.

If a DHCPv6 snooping user is going online, running the **display dhcpv6 snooping user-bind** command generates a binding entry with an empty address. If the user goes online successfully, the binding entry is updated. If the user fails to go online, the binding entry ages and disappears.

Example

Display the DHCPv6 binding table.

- Display all binding entries.

```
<HUAWEI> display dhcpv6 snooping user-bind all
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                    MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Lease
--------------------------------------------------------------------------------
FC00:1::1                    00e0-fc12-3456  500 /--  /--    2008.10.01-00:26
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

- Display detailed information about the DHCPv6 binding table.

```
<HUAWEI> display dhcpv6 snooping user-bind all verbose
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : FC00:1::1
 MAC Address : 00e0-fc12-3456
 VSI         : --
 VLAN(O/I/P) : 500 /--  /--
 Interface   : GE0/0/1
 Renew time  : 2008.10.01-00:27
 Expire time : 2008.10.03-00:27
 Cache time  : 2022.10.03-00:27
 IPSG Status : ineffective
 DadTimerId  : --
 DadPktNum   : --
 User State  : BOUND
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

Display the IPv6 prefix binding table.

- Display all binding entries.

```
<HUAWEI> display dhcpv6 snooping user-bind ipv6-prefix all
PD Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IPv6 Prefix                   MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Lease
--------------------------------------------------------------------------------
FC00:2::/36                   00e0-fc12-3456  500 /--  /--    2008.10.03-00:30
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

- Display detailed information about the IPv6 prefix binding table by specifying the **verbose** parameter.

```
<HUAWEI> display dhcpv6 snooping user-bind ipv6-prefix all verbose
PD Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : FC00:2::/36
 MAC Address : 00e0-fc12-3456
 VSI         : --
 VLAN(O/I/P) : 500 /--  /--
 Interface   : GE0/0/1
```

```
 Lease       : 2008.10.03-00:30
 User State  : BOUND
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

Table 14-74 Description of the **display dhcpv6 snooping user-bind** command output

Item	Description
DHCPV6 Dynamic Bind-table	DHCPv6 snooping dynamic binding table.
PD Dynamic Bind-table	IPv6 prefix binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: VLAN mapping
IP Address	User IPv6 address.
IPv6 Prefix	User IPv6 prefix.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to. **NOTE** If **verbose** is not specified, only one of VSI, (BD-VLAN), and VLAN (O/I/P) is displayed.
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or mapped VLAN ID of the online user. **NOTE** If **verbose** is not specified, only one of VSI, (BD-VLAN), and VLAN (O/I/P) is displayed.
(BD-VLAN)	BD and the VLAN to which the BD is bound. **NOTE** If **verbose** is not specified, only one of VSI, (BD-VLAN), and VLAN (O/I/P) is displayed.
Interface	Interface through which a user goes online.
Lease	Time when the lease of the IP address used by a user expires.
IPSG Status	Whether the binding table is effective for IP packet check that has been enabled. ● IPv6 effective slot: <0> indicates that the binding table is effective for IPv6 packet checking in slot 0. ● ineffective This field is invalid if IP packet check is disabled.
Renew time	Entry update time.

Item	Description
Expire time	Entry expiration time.
Cache time	Cache time of entries.
DadTimerId	Client probing timer ID.
DadPktNum	Remaining number of times a DAD NS packet can be transmitted.
User State	Status of a DHCPv6 snooping binding entry is as follows: ● START ● DETECTION ● BOUND ● LIVE ● DELETE ● CONFIRM ● TESTING_VP

14.8.65 reset dhcp snooping statistics

Function

The **reset dhcp snooping statistics** command clears DHCP snooping statistics.

Format

reset dhcp snooping statistics { **bridge-domain** *bd-id* | **global** | **interface** *interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [**interface** *interface-type interface-number*] }

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
bridge-domain *bd-id*	Clears DHCP snooping statistics in a specified BD.	The value is an integer that ranges from 1 to 16777215.
global	Clears global DHCP snooping statistics.	-

Parameter	Description	Value
interface *interface-type interface-number*	Clears DHCP snooping statistics on the specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vlan *vlan-id*	Clears DHCP snooping statistics in the specified VLAN. *vlan-id* specifies a VLAN ID.	*vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If statistics are collected after DHCP snooping is enabled, you can run the **reset dhcp snooping statistics** command to clear the statistics.

Precautions

If both **interface** and **vlan** are specified, the specified interface must have been added to the specified VLAN. The **reset dhcp snooping statistics** command is used to clear DHCP snooping statistics in the VLAN to which the specified interface is added.

Example

Clear DHCP snooping statistics on GE0/0/1.

```
<HUAWEI> reset dhcp snooping statistics interface gigabitethernet 0/0/1
```

14.8.66 reset dhcp snooping user-bind

Function

The **reset dhcp snooping user-bind** command clears DHCP snooping binding entries.

Format

reset dhcp snooping user-bind [**vlan** *vlan-id* | **interface** *interface-type interface-number*] * [**ipv4** | **ipv6**]

reset dhcp snooping user-bind [**ip-address** [*ip-address*] | **ipv6-address** [*ipv6-address*] | **vpls** *vpls-name*]

reset dhcp snooping user-bind bridge-domain *bd-id*

reset dhcp snooping user-bind [**ipv6-prefix** [*prefix/prefix-length*]]

NOTE

Only the , S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H support **vpls** parameter.

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears DHCP snooping binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Clears DHCP snooping binding entries mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
bridge-domain *bd-id*	Clears DHCP snooping binding entries in a specified BD.	The BD ID must already exist.
ipv4 or **ip-address**	Clears DHCP snooping binding entries mapping IPv4 addresses.	-
ipv6-address, **ipv6** or **ipv6-prefix**	Clears DHCP snooping binding entries mapping IPv6 addresses or IPv6 prefixes. ● **ipv6** indicates that DHCP snooping binding entries mapping IPv6 addresses or IPv6 prefixes are cleared. ● **ipv6-address** indicates that DHCP snooping binding entries mapping IPv6 addresses are cleared. ● **ipv6-prefix** indicates that DHCP snooping binding entries mapping IPv6 prefixes are cleared.	-

Parameter	Description	Value
ip-address	Clears DHCP snooping binding entries mapping a specified IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Clears DHCP snooping binding entries mapping a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix/*prefix-length*	Clears DHCP snooping binding entries mapping a specified IPv6 prefix. - *prefix* specifies the IPv6 prefix. - *prefix-length* specifies the IPv6 prefix length.	*prefix* is a 32-digit hexadecimal characters in the format of X:X::X:X. *prefix-length* is an integer that ranges from 1 to 128.
vpls *vpls-name*	Clears DHCP snooping binding entries mapping a specified VPLS name.	The value must be an existing VPLS name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the mapping DHCP snooping binding entries are generated after DHCP users log in. The **reset dhcp snooping user-bind** command clears binding entries mapping a specified parameter. If no parameter is specified, all the binding entries are cleared.

Precautions

If both **interface** *interface-type interface-number* and **vlan** *vlan-id* are configured, the interface specified by **interface** *interface-type interface-number* must have been added to the VLAN specified by **vlan** *vlan-id*. In this case, the command clears the DHCP snooping binding entries on a specified interface belonging to a certain VLAN.

Example

Clear DHCP snooping binding entries in VLAN 100.

```
<HUAWEI> reset dhcp snooping user-bind vlan 100
```

14.8.67 reset dhcpv6 snooping statistics

Function

The **reset dhcpv6 snooping statistics** command deletes DHCPv6 snooping statistics.

Format

reset dhcpv6 snooping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

When you locate faults in DHCPv6 services, you need to collect statistics on DHCPv6 snooping packets and deleted entries within a certain period of time. Before collecting statistics using the **display dhcpv6 snooping statistics** command, run the **reset dhcpv6 snooping statistics** command to delete historical statistics.

Example

Delete DHCPv6 snooping statistics.

```
<HUAWEI> reset dhcpv6 snooping statistics
```

14.9 ND Snooping Configuration Commands

14.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.9.2 display nd snooping configuration

Function

The **display nd snooping configuration** command displays the ND snooping configuration.

Format

display nd snooping configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

ND snooping configuration includes whether ND snooping is enabled or disabled and information about ND snooping trusted interfaces.

To view ND snooping configuration, run the **display nd snooping configuration** command.

Example

Display ND snooping configuration.

```
<HUAWEI> display nd snooping configuration
#
nd snooping enable
#
interface GigabitEthernet0/0/1
 nd snooping trusted
#
```

14.9.3 display nd snooping prefix

Function

The **display nd snooping prefix** command displays prefix management entries of users.

Format

display nd snooping [**static** | **dynamic**] **prefix** [**verbose**]

Parameters

Parameter	Description	Value
static	Displays statically configured prefix management entries.	-
dynamic	Displays dynamically generated prefix management entries.	-
verbose	Displays details about prefix management entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A device can establish a prefix management table which can be used to implement duplicate address detection for users with IPv6 addresses and establish a dynamic ND snooping binding table. A prefix management entry can be statically configured or dynamically generated.

- Dynamic generation: The device obtains an RA packet received from an ND snooping trusted interface and automatically generates a prefix management entry based on the RA packet.
- Static configuration: When a gateway device does not send RA packets, you can run the **nd snooping static-prefix** command to configure a static prefix management entry.

You can run the **display nd snooping prefix** command to check prefix management entries.

Example

Display prefix management entries of users.

```
<HUAWEI> display nd snooping prefix
prefix-table:
Prefix                       Length     Valid-Time    Vlan(O/I)/BD     Prefix-
Type
--------------------------------------------------------------------------------
FC00:1::                      64       -        10  /24/-      static
FC00:2::                      64       2592000      1   /-/-      dynamic
--------------------------------------------------------------------------------
Prefix table total count:       2        Print count:         2
```

Table 14-75 Description of the **display nd snooping prefix** command output

Item	Description
prefix-table	Prefix management table of users.
Prefix	Prefix. The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.
Length	Prefix length. The value is an integer that ranges from 1 to 128.
Valid-Time	Valid lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Vlan(O/I)/BD	VLAN or BD information in a prefix management entry.
Prefix-Type	Type of a prefix management entry. The value can be: ● static: The prefix management entry is statically configured. ● dynamic: The prefix management entry is dynamically generated.
Prefix table total count	Total number of entries in the prefix management table.
Print count	Number of displayed prefix management entries.

Display prefix management entries of users.

```
<HUAWEI> display nd snooping prefix verbose
prefix-table:
-------------------------------------------------------------------------------
 Prefix                  : FC00:1::
 Prefix Length           : 64
 Valid Lifetime(sec)     : -
 Preferred Lifetime(sec) : -
 Interface               : -
 VLAN ID(Outer/Inner)    : 10/24
 Prefix Type             : static
-------------------------------------------------------------------------------
 Prefix                  : FC00:2::
 Prefix Length           : 64
 Valid Lifetime(sec)     : 2592000
 Preferred Lifetime(sec) : 2592000
 Interface               : GE0/0/1
 VLAN ID(Outer/Inner)    : 1/-
 Prefix Type             : dynamic
-------------------------------------------------------------------------------
Prefix table total count:      2          Print count:         2
```

Table 14-76 Description of the **display nd snooping prefix verbose** command output

Item	Description
prefix-table	Prefix management table of users.
Prefix	Prefix. The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.
Prefix Length	Prefix length. The value is an integer that ranges from 1 to 128.
Valid Lifetime(sec)	Valid lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Preferred Lifetime(sec)	Preferred lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Interface	Interface information in a prefix management entry.
VLAN ID(Outer/Inner)	VLAN information in a prefix management entry.
Prefix-Type	Type of a prefix management entry. The value can be: ● static: The prefix management entry is statically configured. ● dynamic: The prefix management entry is dynamically generated.
Prefix table total count	Total number of entries in the prefix management table.
Print count	Number of printed entries.

14.9.4 display nd snooping statistics

Function

The **display nd snooping statistics** command displays statistics about the ND snooping packets received, sent, and discarded by the device.

Format

display nd snooping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ND snooping is enabled, the device records statistics on the received, sent, and discarded ND snooping packets to facilitate maintenance.

Example

Display statistics on the ND snooping packets received, sent, and discarded on the device.

```
<HUAWEI> display nd snooping statistics
Input: total 203 packets, discarded 14 packets
  ns                                        :       178
  na                                        :        21
  rs                                        :         4
  ra                                        :         0
  other                                     :         0
Drop Packet:
  The local link address is incorrect           :         7
  It does not match the binding table            :         1
  The destination IP address is incorrect        :         6
Output: total 50 packets
  ns                                        :         50
```

Table 14-77 Description of the **display nd snooping statistics** command output

Item	Description
Input: total *n* packets, discarded *m* packets	Number (*n*) of ND packets received by the device and number (*m*) of discarded ND packets.
ns	Number of sent or received NS packets on a device.
na	Number of received NA packets.
rs	Number of received RS packets.
ra	Number of received RA packets.
other	Number of received other packets.
Drop Packet	Number of dropped packets. The displayed information varies according to the packet drop reasons.
The local link address is incorrect	Number of packets dropped due to incorrect link-local address.

Item	Description
It does not match the binding table	Number of packets dropped because the packets do not match the binding entries.
The destination IP address is incorrect	Number of packets dropped due to incorrect destination IP addresses.
Output: total *x* packets	Number (*x*) of ND packets sent by a device.

14.9.5 display nd snooping user-bind

Function

The **display nd snooping user-bind** command displays the ND snooping dynamic binding table.

Format

display nd snooping user-bind all [**verbose**]

display nd snooping user-bind { **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* | **bridge-domain** *bd-id* } * [**verbose**]

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
all	Displays all ND snooping dynamic binding entries.	-
verbose	Displays detailed information about ND snooping dynamic binding entries.	-
ipv6-address *ipv6-address*	Displays information about the IPv6 address in the ND snooping dynamic binding table.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
mac-address *mac-address*	Displays information about the MAC address in the ND snooping dynamic binding table.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
vlan *vlan-id*	Displays information about the VLAN in the ND snooping dynamic binding table.	The value is an integer ranging from 1 to 4094.
interface *interface-type interface-number*	Displays interface information in the ND snooping dynamic binding table. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
bridge-domain *bd-id*	Displays information about the BD in the ND snooping dynamic binding table.	The value is an integer ranging from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ND snooping dynamic binding entry includes the source IPv6 address and source MAC address of a user, and the VLAN that a user belongs to. You can run the **display nd snooping user-bind** command to view details in the ND snooping dynamic binding table.

Example

Display all ND snooping dynamic binding entries.

```
<HUAWEI> display nd snooping user-bind all
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                    MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Lease
-----------------------------------------------------------------------------------------
FC00:1::2                    00e0-fc12-3456  10  /--  /--            2011.05.06-20:09
-----------------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Display detailed information about ND snooping dynamic binding entries.

```
<HUAWEI> display nd snooping user-bind all verbose
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
------------------------------------------------------------------------------------------
 IP Address     : FE80::6BD:70FF:FEE0:733
```

```
 MAC Address   : 00e0-fc12-3456
 Bridge-domain : 50
 VSI           : --
 VLAN(O/I/P)   : 200 /--  /--
 Interface     : GE0/0/1
 Renew time    : 2019.10.28-15:02
 Expire time   : 2019.10.28-16:02
 DadTimerId    : --
 DadPktNum     : --
 User State    : BOUND
--------------------------------------------------------------------------------
Print count:          1          Total count:          1
```

Table 14-78 Description of the **display nd snooping user-bind** command output

Item	Description
ND Dynamic Bind-table	ND snooping dynamic binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	O indicates the outer VLAN ID; I indicates the inner VLAN ID; P indicates the mapped VLAN ID.
IP Address	IPv6 address of a user.
MAC Address	MAC address of a user.
Bridge-domain	Broadcast domain.
VSI	VPN instance that a user belongs to.
VLAN(O/I/P)	Inner VLAN ID, outer VLAN ID, or VLAN mapping information of the online user. **NOTE** The ND snooping binding table does not contain VLAN mapping information. Therefore, no value is displayed in the P field.
Interface	User access interface.
User State	Status of an ND snooping dynamic binding entry is as follows: ● START: The binding entry is being created and is in the initialization state. ● DETECTION: The system is performing detection for the binding entry to check whether the user is online. ● BOUND: The binding entry has been successfully created.

14.9.6 nd snooping alarm binding-table check enable

Function

The **nd snooping alarm binding-table check enable** command enables the alarm function for checking packets against the ND snooping binding table.

The **undo nd snooping alarm binding-table check enable** command disables the alarm function for checking packets against the ND snooping binding table.

By default, the alarm function for checking packets against the ND snooping binding table is disabled.

Format

nd snooping alarm binding-table check enable

undo nd snooping alarm binding-table check enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After ND protocol packet validity check is enabled using the **nd snooping check enable** command, the device checks the NA, NS, and RS packets received from untrusted interfaces against the ND snooping binding table and discards the packets that do not match the binding table. If the number of discarded packets exceeds the threshold, the corresponding alarm is generated. The minimum interval for sending alarm messages is 1 minute. You can run the **nd snooping alarm binding-table check threshold** command to set the alarm threshold.

Prerequisites

ND snooping has been enabled on the device using the **nd snooping enable** command.

Precautions

To ensure that alarms can be properly reported, you need to run the **snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **display snmp-agent trap feature-name dhcp all** command.

Example

Enable the alarm function for checking packets against the ND snooping binding table on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping alarm binding-table check enable
```

14.9.7 nd snooping alarm binding-table check threshold

Function

The **nd snooping alarm binding-table check threshold** command configures the alarm threshold for the number of ND snooping-discarded packets.

The **undo nd snooping alarm binding-table check threshold** command restores the default alarm threshold.

By default, the global alarm threshold for the number of ND snooping-discarded packets is 100, and the alarm threshold for the number of ND snooping-discarded packets on an interface is the value configured in the system view.

Format

nd snooping alarm binding-table check threshold *threshold*

undo nd snooping alarm binding-table check threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of ND snooping-discarded packets.	The value is an integer that ranges from 1 to 1000.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function for checking packets against the ND snooping binding table is enabled using the **nd snooping alarm binding-table check enable** command, you can run the **nd snooping alarm binding-table check threshold** command to configure the alarm threshold for the number of ND snooping-discarded packets.

Prerequisites

ND snooping has been enabled on the device using the **nd snooping enable** command.

Precautions

If this command is run in the system view, it takes effect on all the interfaces of the device.

Example

Set the alarm threshold for the number of ND snooping-discarded packets on GE0/0/1 to 1000.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping alarm binding-table check threshold 1000
```

14.9.8 nd snooping check enable

Function

The **nd snooping check enable** command enables ND protocol packet validity check.

The **undo nd snooping check enable** command disables ND protocol packet validity check.

By default, ND protocol packet validity check is disabled.

Format

nd snooping check { **na** | **ns** | **rs** } **enable**

undo nd snooping check { **na** | **ns** | **rs** } **enable**

Parameters

Parameter	Description	Value
na	Enables validity check for Neighbor Advertisement (NA) packets.	-
ns	Enables validity check for Neighbor Solicitation (NS) packets.	-
rs	Enables validity check for Router Solicitation (RS) packets.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ND packet validity check prevents forged NA/NS/RS packets.

After ND packet validity check is enabled, the device verifies the NA/NS/RS packets received by untrusted interfaces against the ND snooping binding table, to determine whether the NA/NS/RS packets are sent from valid users in the VLAN on the interface. The device forwards the ND packets from valid users and drops invalid ND packets.

Prerequisites

ND snooping has been enabled globally using the **nd snooping enable** command.

Example

Enable NA packet validity check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping check na enable
```

14.9.9 nd snooping check dad-ns retransmit-rate rate

Function

The **nd snooping check dad-ns retransmit-rate rate** command configures the maximum retransmission rate of DAD NS packets.

The **undo nd snooping check dad-ns retransmit-rate rate** command restores the default retransmission rate of DAD NS packets.

By default, the maximum retransmission rate of DAD NS packets is 50 packets per second.

Format

nd snooping check dad-ns retransmit-rate rate *rate-value*

undo nd snooping check dad-ns retransmit-rate rate

Parameters

Parameter	Description	Value
rate-value	Specifies the maximum retransmission rate of DAD NS packets.	The value is an integer that ranges from 1 to 100, in packet per second. The default value is 50.

Views

System view, VLAN view, Eth-Trunk view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the ND snooping binding entry is not established, an untrusted interface on a device forwards a DAD NS packet after receiving it. After the **nd snooping check dad-ns retransmit-rate enable** command is configured, the device checks the retransmission rate of DAD NS packets. You can run the **nd snooping check dad-ns retransmit-rate rate** *rate-value* command to configure the retransmission rate of DAD NS packets. If the number of DAD NS packets retransmitted per second exceeds the value of the *rate-value* parameter, the device directly discards excessive packets instead of forwarding these packets.

Prerequisites

ND snooping has been enabled using the **nd snooping enable** command in the system view.

Example

Set the retransmission rate of DAD NS packets to 60 packets per second in the system view.

```
<HUAWEI> system-view
[HUAWEI] nd snooping check dad-ns retransmit-rate rate 60
```

14.9.10 nd snooping check dad-ns retransmit-rate enable

Function

The **nd snooping check dad-ns retransmit-rate enable** command enables the function of checking the retransmission rate of DAD NS packets.

The **undo nd snooping check dad-ns retransmit-rate enable** command disables the function of checking the retransmission rate of DAD NS packets.

By default, the function of checking the retransmission rate of DAD NS packets is disabled.

Format

nd snooping check dad-ns retransmit-rate enable

undo nd snooping check dad-ns retransmit-rate enable

Parameters

None

Views

System view, VLAN view, Eth-Trunk view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an untrusted interface on a device receives a DAD NS packet, the interface forwards the packet for the duplicate address detection and bogus user check. To avoid the situation that the remote interface cannot receive packets forwarded by the local device because of packet loss when the ND snooping binding entry is not established, configure the untrusted interface on the local device to forward a DAD NS packet after receiving it. By default, a device does not control the retransmission rate of DAD NS packets. When excessive packets are received, packet retransmission may affect normal operation of network services. To solve this problem, you can run the **nd snooping check dad-ns retransmit-rate enable** command to enable the function of checking the retransmission rate of DAD NS packets. After this function is enabled, the device limits the retransmission rate of DAD NS packets.

You can run the **nd snooping check dad-ns retransmit-rate rate** *rate-value* command to configure the retransmission rate of DAD NS packets. If the number of DAD NS packets retransmitted per second exceeds the value of the *rate-value* parameter, the device directly discards excessive packets instead of forwarding these packets.

Prerequisites

ND snooping has been enabled using the **nd snooping enable** command in the system view.

Example

Enable the function of checking the retransmission rate of DAD NS packets in the system view.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] nd snooping check dad-ns retransmit-rate enable
```

14.9.11 nd snooping disable

Function

The **nd snooping disable** command disables ND snooping on an interface.

The **undo nd snooping disable** command restores the default configuration.

By default, ND snooping is disabled on an interface.

Format

nd snooping disable

undo nd snooping disable

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6735-S, S6730-S, and S6730S-S support this command.

Parameters

None.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If ND snooping is enabled in a specific VLAN using the **nd snooping enable** command, ND snooping is enabled on all the interfaces in this VLAN. The **nd snooping enable** command is configured in the VLAN, and interfaces in the VLAN do not have the command configuration. Therefore, the **undo nd snooping enable** command cannot disable ND snooping on a specific interface in this VLAN. To solve this problem, run the **nd snooping disable** command on this interface to disable ND snooping on it.

Precautions

- Running the **nd snooping disable** command will disable ND snooping on an interface and clear the ND snooping configuration and the dynamic ND snooping binding table. Running the **undo nd snooping enable** command will disable ND snooping on an interface will the dynamic ND snooping binding table, but will not clear the ND snooping configuration.
- Running the **undo nd snooping disable** command on an interface will disable ND snooping on the interface. To enable ND snooping on the interface, run the **nd snooping enable** command.

Example

Disable ND snooping on GE0/0/1 that has been added to VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] nd snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping disable
```

14.9.12 nd snooping enable

Function

The **nd snooping enable** command enables ND snooping.

The **undo nd snooping enable** command disables ND snooping.

By default, ND snooping is disabled.

Format

nd snooping enable

undo nd snooping enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

ND provides powerful functions but has no security mechanism. Attackers often use ND to attack network devices. Common ND attacks are as follows:

- An attacker uses the IP address of host A to send NS, NA, or RS packets to host B or the gateway. Host B or the gateway then modifies their ND entries. As a result, all packets sent from host B or the gateway to host A are sent to the attacker.
- An attacker uses the gateway IP address to send RA packets to hosts. Then the hosts incorrectly set IPv6 parameters and modify their ND entries.

To prevent ND attacks, enable ND snooping on the device. The device detects NS packets in the DAD process to establish an ND snooping dynamic binding table that includes source IPv6 addresses, source MAC addresses, VLANs, and inbound ports. When receiving ND packets, the device checks the validity of ND packets based on the ND snooping binding table and checks whether the user is an authorized user in the VLAN that the port receiving ND packets belongs to. The device forwards valid ND packets and discards invalid ND packets to defend against ND attacks from bogus hosts or gateways.

NOTE

By default, the system reports a port-Up event 2 seconds after a user-side interface transits from Down to Up state. If ND snooping is enabled before the port-Up event is reported, the system cannot generate the ND snooping entry of the user connected to this interface. To avoid this problem, run the **carrier up-hold-time** *interval* command to change the delay in reporting the port-Up event to 0.

Example

Enable ND snooping globally and on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping enable
```

14.9.13 nd snooping enable dhcpv6 only

Function

The **nd snooping enable dhcpv6 only** command enables ND snooping in the DHCPv6 Only scenario.

The **undo nd snooping enable** command disables ND snooping in the DHCPv6 Only scenario.

By default, ND snooping is disabled in the DHCPv6 Only scenario.

Format

nd snooping enable dhcpv6 only

undo nd snooping enable

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device checks the validity of ND protocol packets against the IPv6 static binding table, DHCPv6 dynamic binding table, and ND snooping binding table. The IPv6 static binding table is manually configured by the administrator, the DHCPv6 dynamic binding table is automatically generated by extracting information from DHCPv6 Reply packets, and the ND snooping binding table is automatically generated by extracting information from DAD NS packets. At the same time, the ND protocol packet validity check function depends on the ND snooping function (including enabling ND snooping and configuring ND snooping trusted interfaces). In the DHCPv6 Only scenario, users are only allowed to obtain IPv6 addresses using DHCPv6 and IPv6 addresses that are privately configured by users and automatically generated using the PD address prefix are considered as invalid addresses. In this scenario, ND snooping is disabled to prevent ND snooping binding entries from being generated for such invalid addresses. In this case, the ND protocol packet validity check function cannot be performed, so that address spoofing attacks may exist on the network.

To resolve this problem, you can run the **nd snooping enable dhcpv6 only** and **nd snooping trusted dhcpv6 only** commands to enable the ND snooping function in the DHCPv6 Only scenario. After the **nd snooping enable dhcpv6 only** command is configured, no ND snooping binding entry is generated for the IPv6 global unicast addresses that are manually configured by users and automatically generated using the PD address prefixes. The device checks the validity of ND protocol packets against the IPv6 static binding table and DHCPv6 dynamic binding table.

Prerequisites

ND snooping has been enabled globally using the **nd snooping enable** command.

Precautions

- In the DHCPv6 Only scenario, ND snooping binding entries are generated for the IPv6 link-local addresses that are manually configured by users and automatically generated. To be specific, only records corresponding to the IPv6 link-local addresses exist in the ND snooping binding table in the DHCPv6 Only scenario.
- IPv6 addresses obtained using DHCPv6 PD also apply to the DHCPv6 Only scenario.

Example

Enable ND snooping globally and on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping enable dhcpv6 only
```

14.9.14 nd snooping max-user-number

Function

The **nd snooping max-user-number** command sets the maximum number of ND snooping dynamic binding entries to be learned by an interface.

The **undo nd snooping max-user-number** command restores the default maximum number of ND snooping dynamic binding entries to be learned by an interface.

By default, the maximum number of ND snooping binding entries that can be learned on an interface is 512 for S200, S1720GW-E, S1720GWR-E, and 2048 for S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, S6735-S, and 8192 for other models.

Format

nd snooping max-user-number *max-user-number*

undo nd snooping max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of ND snooping dynamic binding entries to be learned by an interface.	The value is an integer that ranges from 1 to 512 for S1720GW-E, S1720GWR-E, and from 1 to 2048 for S5720-LI, S2730S-S, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, , S5735S-H, S5736-S, S6720S-S, and S5720I-SI, and from 1 to 8192 for other models.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a lot of users go online through an interface, the device consumes many ND snooping dynamic binding entries to process the NS packets. To prevent this problem, you can set the maximum number of ND snooping dynamic binding entries to be learned by an interface. If the number of the ND snooping dynamic binding entries learned by an interface reaches the maximum number, no entry can be added.

You can set the maximum number ND snooping entries in the system view or interface view. The configuration in the system view is valid for all interfaces. The settings in the interface view only take effect on the specified interface. If the settings are performed in both the interface view and system view, the smaller value is adopted.

Prerequisites

Before setting the maximum number of ND snooping dynamic binding entries to be learned by an interface, ensure that ND snooping has been enabled in the system view using the **nd snooping enable** command.

Example

Set the maximum number of ND snooping binding entries to 200 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping max-user-number 200
```

14.9.15 nd snooping static-prefix

Function

The **nd snooping static-prefix** command configures a static prefix management entry.

The **undo nd snooping static-prefix** command deletes a configured static prefix management entry.

By default, no static prefix management entry is configured on a device.

Format

nd snooping static-prefix *ipv6-address/prefix-length* [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

undo nd snooping static-prefix *ipv6-address/prefix-length* [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

Parameters

Parameter	Description	Value
ipv6-address/prefix-length	Specifies the IPv6 address prefix. Descriptions of each part in this parameter are as follows: - *ipv6-address*: Specifies an IPv6 address. - *prefix-length*: Specifies the IPv6 address prefix length.	- *ipv6-address*: The total length of the value is 128 bits. The string is divided into eight groups, each of which consists of four hexadecimal digits. The address is in the X:X:X:X:X:X:X:X format. - *prefix-length*: The value is an integer that ranges from 1 to 128.
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** By default, the outer VLAN ID is 1 and no inner VLAN is configured.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving an NS packet from a user, a device can generate a dynamic ND snooping binding entry only after the value of the **Target Address** field in the packet matches the user's prefix management entry. The device obtains an RA packet received from an ND snooping trusted interface and automatically generates a prefix management entry based on the RA packet. However, if a gateway device does not send RA packets, the device cannot automatically generate a prefix management entry and then cannot establish a corresponding dynamic ND snooping binding entry, affecting services. In this case, you can run the **nd snooping static-prefix** *ipv6-address/prefix-length* [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] command to manually configure a prefix management entry.

Prerequisites

ND snooping has been enabled using the **nd snooping enable** command in the system view.

Precautions

The total number of statically configured and dynamically generated prefix management entries cannot exceed the maximum number of entries allowed on a device. Otherwise, no prefix management entry can be further statically configured or dynamically generated.

Example

Configure a static prefix management entry with the IPv6 address prefix FC00:1::/64.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] nd snooping static-prefix fc00:1::/64
```

14.9.16 nd snooping trusted

Function

The **nd snooping trusted** command configures the trusted interface.

The **undo nd snooping trusted** command restores the trusted interface to an untrusted interface.

Format

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

nd snooping trusted

undo nd snooping trusted

VLAN view

nd snooping trusted interface *interface-type interface-number*

undo nd snooping trusted interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the trusted interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ND snooping classifies interfaces connected to IPv6 nodes into trusted and untrusted interfaces. The trusted interfaces connect to trusted IPv6 nodes and untrusted interfaces connect to untrusted IPv6 nodes. By default, all interfaces are untrusted.

- You must configure the interface connected to a trusted IPv6 node as a trusted interface so that the device can forward the ND packets received by this interface. In addition, the device creates a prefix management table according to the received RA packet to help network administrators manage IPv6 addresses.
- The interface connected to an untrusted IPv6 node must be configured as an untrusted interface. The device discards the RA packets received by the untrusted interface to prevent RA attacks.

NOTE

Generally, the interface connecting to the gateway is configured as the trusted interface, and other interfaces are all untrusted interfaces.

Prerequisites

ND snooping has been enabled using the **nd snooping enable** command in the system view.

Precautions

After the **nd snooping trusted** command is executed, ND snooping is enabled on the interface.

When you run the **nd snooping trusted** command in the VLAN view, the specified interface must belong to the VLAN.

Example

Configure GE0/0/1 as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping trusted
```

Configure GE0/0/1 in VLAN 10 as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] nd snooping trusted interface gigabitethernet 0/0/1
```

14.9.17 nd snooping trusted dhcpv6 only

Function

The **nd snooping trusted dhcpv6 only** command configures the interfaces in the DHCPv6 Only scenario as ND snooping trusted interfaces.

The **undo nd snooping trusted** command restores the interfaces to untrusted.

By default, all interfaces are untrusted.

Format

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

nd snooping trusted dhcpv6 only

undo nd snooping trusted

VLAN view

nd snooping trusted interface *interface-type interface-number* **dhcpv6 only**

undo nd snooping trusted interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface that will be configured as an ND snooping trusted interface in the DHCPv6 Only scenario. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, BD view

Default Level

2: Configuration level

Usage Guidelines

The device checks the validity of ND protocol packets against the IPv6 static binding table, DHCPv6 dynamic binding table, and ND snooping binding table. The IPv6 static binding table is manually configured by the administrator, the DHCPv6 dynamic binding table is automatically generated by extracting information from DHCPv6 Reply packets, and the ND snooping binding table is automatically generated by extracting information from DAD NS packets. At the same time, the ND protocol packet validity check function depends on the ND snooping function (including enabling ND snooping and configuring ND snooping trusted interfaces). In the DHCPv6 Only scenario, users are only allowed to obtain IPv6 addresses using DHCPv6 and IPv6 addresses that are privately configured by users and automatically generated using the PD address prefix are considered as invalid addresses. In this scenario, ND snooping is disabled to prevent ND snooping binding entries from being generated for such invalid addresses. In this case, the ND protocol packet validity check function cannot be performed, so that address spoofing attacks may exist on the network.

To resolve this problem, you can run the **nd snooping enable dhcpv6 only** and **nd snooping trusted dhcpv6 only** commands to enable the ND snooping function in the DHCPv6 Only scenario. After the **nd snooping trusted dhcpv6 only** command is configured, no prefix management entry is generated when the trusted interface receives an RA packet, which is different from the **nd snooping trusted** command. This is because the prefix management entries need to be matched before the corresponding ND snooping binding entries are generated for the IPv6 addresses excluding the IPv6 link-local addresses. However, only records corresponding to the IPv6 link-local addresses exist in the ND snooping binding table in the DHCPv6 Only scenario. Therefore, the prefix management entries do not need to be generated.

Example

Configure GE0/0/1 as an ND snooping trusted interface.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping trusted dhcpv6 only
```

Configure GE0/0/1 as an ND snooping trusted interface in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] nd snooping trusted interface gigabitethernet 0/0/1 dhcpv6 only
```

14.9.18 nd snooping user-alarm percentage

Function

The **nd snooping user-alarm percentage** command configures the alarm thresholds for the percentage of ND snooping dynamic binding entries.

The **undo nd snooping user-alarm percentage** command restores the default alarm thresholds for the percentage of ND snooping dynamic binding entries.

By default, the lower alarm threshold for the percentage of ND snooping dynamic binding entries is 50, and the upper alarm threshold for the percentage of ND snooping dynamic binding entries is 100.

Format

nd snooping user-alarm percentage *percent-lower-value percent-upper-value*

undo nd snooping user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of ND snooping dynamic binding entries.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of ND snooping dynamic binding entries.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **nd snooping max-user-number** command to set the maximum number of ND snooping dynamic binding entries on an interface, you can run the **nd snooping user-alarm percentage** command to set the alarm thresholds for the percentage of ND snooping dynamic binding entries.

When the percentage of learned ND snooping dynamic binding entries against the maximum number of ND snooping dynamic entries allowed by the device reaches or exceeds the upper alarm threshold, the device generates an alarm. When the percentage of learned ND snooping dynamic binding entries against the maximum number of ND snooping dynamic entries allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm. The alarm information helps network administrators monitor the status of ND snooping binding table in real time.

Example

Set the lower alarm threshold for the percentage of ND snooping dynamic binding entries to 30 and the upper alarm threshold to 80.

```
<HUAWEI> system-view
[HUAWEI] nd snooping user-alarm percentage 30 80
```

14.9.19 nd snooping wait-time life-time

Function

The **nd snooping wait-time life-time** command configures the wait time for a device to send an NS packet to detect the user status and the lifetime of an ND snooping binding entry when a device detects the user status.

The **undo nd snooping wait-time life-time** command restores the default settings.

By default, the wait time for a device to send an NS packet to detect the user status is 250 milliseconds and the lifetime of an ND snooping binding entry when a device detects the user status is 500 milliseconds.

Format

nd snooping wait-time *wait-time* **life-time** *life-time*

undo nd snooping wait-time life-time

Parameters

Parameter	Description	Value
wait-time	Specifies the wait time for a device to send an NS packet to detect the user status.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 250 milliseconds.
life-time	Specifies the lifetime of an ND snooping binding entry when a device detects the user status.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 500 milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device updates the ND snooping binding table by detecting the received NA packets. If an ND snooping binding entry exists and the device receives an NA packet with the IP address the same as that in the corresponding entry and inbound port number different from that in the entry, the NA packet conflicts with the entry. The device is then triggered to send an NS packet to detect whether the user corresponding to the entry is online. You can run the **nd snooping wait-time** *wait-time* **life-time** *life-time* command to configure the wait time for a device to send an NS packet to detect the user status and the lifetime of an ND snooping binding entry when a device detects the user status.

- If the entry is within the lifetime and the device receives an NA packet from the port corresponding to the entry, the user corresponding to the entry is still online and the device updates the IP address lease in the corresponding entry.
- If the entry is within the lifetime and the device does not receive an NA packet from the port corresponding to the entry, the user corresponding to the entry is offline and the device updates the user's IP address lease time in the entry and updates the port number in the entry to that in the previously received NA packet.

Prerequisites

ND snooping has been enabled using the **nd snooping enable** command in the system view.

Precautions

After the device receives an NA packet conflicting with an ND snooping binding entry and user status detection is enabled, periodic user status detection is suspended.

Example

Set the wait time for a device to send an NS packet to detect the user status to 300 milliseconds and the lifetime of an ND snooping binding entry when a device detects the user status to 2000 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] nd snooping wait-time 300 life-time 2000
```

14.9.20 nd user-bind detect

Function

The **nd user-bind detect** command configures the number of times and interval for sending NS packets to detect the user status.

The **undo nd user-bind detect** command restores the default setting.

After automatic user status detection is enabled for users mapping ND snooping dynamic binding entries, the default number of detection times is 2, and the default detection interval is 1000 milliseconds.

Format

nd user-bind detect retransmit *retransmit-times* **interval** *retransmit-interval*

undo nd user-bind detect retransmit interval

Parameters

Parameter	Description	Value
retransmit *retransmit-times*	Specifies the number of times for sending NS packets to detect the user status.	The value is an integer ranging from 1 to 10. The default value is 2.
interval *retransmit-interval*	Specifies the interval for sending NS packets to detect the user status.	The value is an integer ranging from 1 to 10000, in milliseconds. The default value is 1000 milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After automatic user status detection for users mapping ND snooping dynamic binding entries is enabled, the device sends NS packets to users based on the configured detection times and interval. If no NA packet is returned from a user after NS packets are sent for configured times, the device considers the user to be offline and deletes the mapping ND snooping dynamic binding entry.

You can run the **nd user-bind detect** command to change the number of times and interval for sending NS packets to detect the user status. On a small network with good network quality, the user returns an NA packet quickly. In this scenario, you can set the interval for sending NS packets to a small value. On a large network with poor network quality, the user returns an NA packet slowly. You can set the interval to a large value to prevent the device from sending the next NS packet before receiving the NA packet. You can change the interval based on the actual network environment.

Prerequisites

Automatic user status detection for users mapping ND snooping dynamic binding entries has been enabled using the **nd user-bind detect enable** command.

Precautions

After you run the **nd user-bind detect enable** command, the device sends an NS packet after a period of time. The maximum value of this period is 20 seconds.

Example

Set the number of times for sending NS packets to 10, and the interval for sending NS packets to 1000 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] nd user-bind detect enable
[HUAWEI] nd user-bind detect retransmit 10 interval 1000
```

14.9.21 nd user-bind detect enable

Function

The **nd user-bind detect enable** command enables the function for automatically detecting status of users mapping ND snooping dynamic binding entries.

The **undo nd user-bind detect enable** command disables the function for automatically detecting status of users mapping ND snooping dynamic binding entries.

By default, the function for automatically detecting status of users mapping ND snooping dynamic binding entries is disabled.

Format

nd user-bind detect enable

undo nd user-bind detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After ND snooping is enabled, the device snoops NS packets in the DAD process to establish ND dynamic binding entries. The aging time of an ND snooping dynamic binding table depends on the IPv6 address lease. If the address lease does not expire but the user is offline, the ND snooping dynamic entry mapping the user cannot be deleted, which occupies binding entry resources on the device.

To prevent this problem, you can enable the automatic user status detection for users mapping ND snooping dynamic binding entries on the device. After this function is enabled, the device sends NS packets to the user according to the detection times (n) specified in **nd user-bind detect** and detection interval. If the device receives no NA packet from the user after sending the NS packets n times, the device considers the user to be offline and deletes the dynamic ND snooping binding entry matching the user.

Precautions

After you run the **nd user-bind detect enable** command, the device sends an NS packet after a period of time. The maximum value of this period is 20 seconds.

Example

Enable the function for automatically detecting status of users mapping ND snooping dynamic binding entries.

```
<HUAWEI> system-view
[HUAWEI] nd user-bind detect enable
```

14.9.22 reset nd snooping prefix

Function

The **reset nd snooping prefix** command clears prefix management entries of users.

Format

reset nd snooping prefix [*ipv6-address*/*prefix-length*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the prefix length.	The value is an integer ranging from 1 to 128. If the global unicast address needs to be set in EUI-64 format, the value of *prefix-length* ranges from 1 to 64.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The ND server that functions as the gateway router sends RA packets periodically to instruct users to update prefixes. The switch that functions as the access device establishes prefix management entries based on RA packets to maintain and manage user prefixes.

Generally, do not delete prefix management entries of users manually. Run the **reset nd snooping prefix** command to delete prefix management entries of users if the following requirements are met:

- The user lease does not expire and the prefix management table cannot age automatically.
- The user is no longer connected to the network.

Precautions

After a prefix management entry is deleted, the switch cannot establish the ND snooping dynamic binding table for new users with the prefix management entry.

Example

Delete the prefix management entry with the prefix address being fc00:1::1 and the prefix length being 64.

```
<HUAWEI> reset nd snooping prefix fc00:1::1/64
```

14.9.23 reset nd snooping statistics

Function

The **reset nd snooping statistics** command deletes statistics on ND snooping packets.

Format

reset nd snooping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Use Scenario

After ND snooping is enabled, the device records statistics on the sent and received ND packets. This command deletes the statistics on ND packets.

Precautions

Deleted statistics cannot be restored. Exercise caution.

Example

Delete statistics on ND snooping packets.

```
<HUAWEI> reset nd snooping statistics
```

14.9.24 reset nd snooping user-bind

Function

The **reset nd snooping user-bind** command clears ND snooping dynamic binding entries on the device.

Format

reset nd snooping user-bind [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* | **bridge-domain** *bd-id*]

NOTE

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720-EI, S6735-S, S6720S-EI support the **bridge-domain** parameter.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface in the ND snooping dynamic binding entry to be cleared. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Specifies the IPv6 address in the ND snooping dynamic binding entry to be cleared.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
mac-address *mac-address*	Specifies the MAC address in the ND snooping dynamic binding entry to be cleared.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Specifies the VLAN ID in the ND snooping dynamic binding entry to be cleared.	The value is an integer ranging from 1 to 4094.
bridge-domain *bd-id*	Specifies the BD ID in the ND snooping dynamic binding entry to be cleared.	The value is an integer ranging from 1 to 16777215.

Views

User view

Default Level

3: Management level

Usage Guidelines

You need to manually delete ND snooping dynamic binding entries if the following requirements are met:

- The ND snooping dynamic binding entry does not reach the aging time, so the entry cannot age automatically.
- The user is no longer connected to the network.
- The user VLAN or interface information changes.

The networking environment change may lead to the change in the VLAN or interface information, while the ND snooping dynamic binding entry mapping a user does not age out and cannot update in real time. As a result, the device discards valid ND packets that do not match the old ND snooping dynamic binding entries. Before changing the networking environment, clear all ND snooping dynamic binding entries manually so that a device generates a new ND snooping dynamic binding table based on the new networking environment.

Example

Delete the ND snooping dynamic binding entry that contains the IPv6 address being fc00:1::1.

```
<HUAWEI> reset nd snooping user-bind ipv6-address fc00:1::1
```

Delete the ND snooping dynamic binding entry that contains the MAC address being 00e0-fc11-2222.

```
<HUAWEI> reset nd snooping user-bind mac-address 00e0-fc11-2222
```

14.10 IPv6 RA Guard Configuration Command

14.10.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support IPv6 RA Guard.

14.10.2 display nd raguard policy

Function

The **display nd raguard policy** command displays the configuration of an IPv6 RA guard policy.

Format

display nd raguard policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of the IPv6 RA guard policy with the specified name.	The value must be the name of an existing IPv6 RA guard policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the matching rules configured in a specified IPv6 RA guard policy, run the **display nd raguard policy** command. RA messages can be forwarded only when they match all rules.

Example

Display the IPv6 RA guard policy configured on the device.

```
<HUAWEI> display nd raguard policy
-----------------------------------------------
   ID        nd-raguard-policy name
    0        p1
    1        p2
    2        p3
-----------------------------------------------
   Total 3, printed 3
```

Table 14-79 Description of the **display nd raguard policy** command output

Item	Description
ID	ID.
nd-raguard-policy name	Name of an IPv6 RA guard policy.
Total *m*, printed *n*	There are a total of *m* entries and *n* entries are printed.

Display the configuration of the IPv6 RA guard policy named **p1**.

```
<HUAWEI> display nd raguard policy p1
ND raguard policy: p1
  if-match source-mac-address acl 4000
  if-match ipv6-source-address acl 2000
  if-match ra-prefix acl 2000
  hop-limit minimum 10
  hop-limit maximum 20
```

```
router-preference maximum medium
managed-address-flag on
other-config-flag on
```

Table 14-80 Description of the **display nd raguard policy** *policy-name* command output

Item	Description
ND raguard policy	Name of an IPv6 RA guard policy. To set the value, run the **nd raguard policy** command.
if-match source-mac-address acl	Number of the Layer 2 ACL that is used to match the source MAC address of RA messages. To set the value, run the **if-match source-mac-address** command.
if-match ipv6-source-address acl	Number of the basic ACL6 that is used to match the source IPv6 address of RA messages. To set the value, run the **if-match ipv6-source-address** command.
if-match ra-prefix acl	Number of the basic ACL6 that is used to match the IPv6 prefix of RA messages. To set the value, run the **if-match prefix** command.
hop-limit minimum	Minimum hop limit used to match RA messages. To set the value, run the **hop-limit minimum** command.
hop-limit maximum	Maximum hop limit used to match RA messages. To set the value, run the **hop-limit maximum** command.
router-preference maximum	Highest route preference used to match RA messages: ● high: high preference ● medium: medium preference ● low: low preference To set the value, run the **router-preference maximum** command.

Item	Description
managed-address-flag	M flag used to match RA messages: - on: The M flag is set to 1. - off: The M flag bit is set to 0. To set the value, run the **managed-address-flag** command.
other-config-flag	O flag used to match RA messages: - on: The O flag is set to 1. - off: The O flag bit is set to 0. To set the value, run the **other-config-flag** command.

14.10.3 display nd raguard statistic

Function

The **display nd raguard statistic** command displays statistics about RA messages discarded by interfaces.

Format

display nd raguard statistic [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about RA messages discarded by a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the interface role of an interface is a host interface or when an IPv6 RA guard policy is applied to an interface and RA messages received on the interface do not match the rules configured in the policy, the interface discards RA messages. The device supports the display of discarded RA message statistics based on interfaces.

Example

Display statistics about RA messages discarded by a specified interface.

```
<HUAWEI> display nd raguard statistic
RA messages dropped by RA guard:
Interface              Dropped
Eth-trunk10              1221
```

Table 14-81 Description of the **display nd raguard statistic** command output

Item	Description
Interface	Interface that discards RA messages.
Dropped	Number of discarded RA messages.

14.10.4 hop-limit

Function

The **hop-limit** command configures a rule to match RA messages against the maximum and minimum hop limits in RA messages.

The **undo hop-limit** command restores the default hop limits.

By default, the maximum and minimum hop limits in an RA message are 255 and 1 respectively.

Format

hop-limit { **maximum** *max-value* | **minimum** *min-value* }

undo hop-limit { **maximum** | **minimum** }

Parameters

Parameter	Description	Value
maximum *max-value*	Specifies the maximum hop limit used to match RA messages.	The value is an integer in the range from 1 to 255.
minimum *min-value*	Specifies the minimum hop limit used to match RA messages.	The value is an integer in the range from 1 to 255.

NOTE

In the same IPv6 RA guard policy, if both *max-value* and *min-value* are configured, *min-value* must be less than or equal to *max-value*.

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

The **Hop Limit** field in an RA message indicates the maximum number of hops that the message can pass through. The value is decremented by 1 each time the message passes through a device. The message is discarded when the field value is 0. After the maximum or minimum hop limit is configured in the IPv6 RA guard policy view, the interface to which the policy is applied forwards only the RA messages whose hop limit is within the configured range and discards those whose hop limit is outside the configured range.

Example

In the IPv6 RA guard policy **p1**, set the maximum and minimum hop limits in RA messages to 10 and 5 respectively.

```
<HUAWEI> system-view
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] hop-limit maximum 10
[HUAWEI-nd-raguard-policy-p1] hop-limit minimum 5
```

14.10.5 if-match source-mac-address

Function

The **if-match source-mac-address** command configures an ACL to match RA messages against the source MAC address in RA messages.

The **undo if-match source-mac-address** command deletes the ACL used to match RA messages against the source MAC address in RA messages.

By default, no ACL is configured to match RA messages against the source MAC address in RA messages.

Format

if-match source-mac-address acl *acl-number*

undo if-match source-mac-address acl

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of a Layer 2 ACL.	The value is an integer in the range from 4000 to 4999.

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ACL is configured in an IPv6 RA guard policy to match RA messages against the source MAC address in RA messages, the interface to which the policy is applied checks the source MAC address of the received RA messages and forwards only the RA messages that match the ACL.

Precautions

- If the ACL specified as a matching rule is not created, no rule is configured in the ACL, or the rule configured in the ACL is not a source MAC address, RA messages will not match against the ACL.
- In the matching process, the permit and deny actions configured in the ACL are ignored, and the focus is only on the rule configured in the ACL. That is, RA messages are forwarded as long as they match the rule.

Example

In the IPv6 RA guard policy **p1**, configure the switch to forward RA messages with the source MAC address 0001-0001-0001 or 0022-0022-0022.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule 1 permit source-mac 0001-0001-0001
[HUAWEI-acl-L2-4001] rule 2 permit source-mac 0022-0022-0022
[HUAWEI-acl-L2-4001] quit
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] if-match source-mac-address acl 4001
```

14.10.6 if-match ipv6-source-address

Function

The **if-match ipv6-source-address** command configures an ACL to match RA messages against the source IPv6 address in RA messages.

The **undo if-match ipv6-source-address** command deletes the ACL used to match RA messages against the source IPv6 address in RA messages.

By default, no ACL is configured to match RA messages against the source IPv6 address in RA messages.

Format

if-match ipv6-source-address acl *acl-number*

undo if-match ipv6-source-address acl

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of a basic ACL6.	The value is an integer in the range from 2000 to 2999.

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ACL is configured in an IPv6 RA guard policy to match RA messages against the source IPv6 address in RA messages, the interface to which the policy is applied checks whether the source IPv6 address of the received RA messages is within the network segment configured in the ACL and forwards only the RA messages that match the ACL.

Precautions

- If the ACL specified as a matching rule is not created, no rule is configured in the ACL, or the rule configured in the ACL is not a source IP address or prefix, RA messages will not match against the ACL.
- In the matching process, the permit and deny actions configured in the ACL are ignored, and the focus is only on the rule configured in the ACL. That is, RA messages are forwarded as long as they match the rule.

Example

In the IPv6 RA guard policy **p1**, configure the switch to forward RA messages with the source IPv6 address FC00:1::10/64.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule 1 permit source fc00:1::/64
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] if-match ipv6-source-address acl 2000
```

14.10.7 if-match prefix

Function

The **if-match prefix** command configures an ACL to match RA messages against the IPv6 prefix in RA messages.

The **undo if-match prefix** command deletes the ACL used to match RA messages against the IPv6 prefix in RA messages.

By default, no ACL is configured to match RA messages against the IPv6 prefix in RA messages.

Format

if-match prefix acl *acl-number*

undo if-match prefix acl

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of a basic ACL6.	The value is an integer in the range from 2000 to 2999.

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an ACL is configured in an IPv6 RA guard policy to match RA messages against the IPv6 prefix in RA messages, the interface to which the policy is applied checks whether the IPv6 prefix of the received RA messages is within the network segment configured in the ACL and forwards the RA messages only when the messages match the ACL. Otherwise, the interface discards the messages.

Precautions

- If the ACL specified as a matching rule is not created, no rule is configured in the ACL, or the rule configured in the ACL is not a source IP address or prefix, RA messages will not match against the ACL.
- In the matching process, the permit and deny actions configured in the ACL are ignored, and the focus is only on the rule configured in the ACL. That is, RA messages are forwarded as long as they match the rule.

Example

In the IPv6 RA guard policy **p1**, configure the switch to forward RA messages with the IPv6 prefix FC00:1::/64.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule 1 permit source fc00:1::/64
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] if-match prefix acl 2000
```

14.10.8 managed-address-flag

Function

The **managed-address-flag** command configures a rule to match RA messages against the M flag in RA messages.

The **undo managed-address-flag** command deletes the rule used to match RA messages against the M flag in RA messages.

By default, no rule is configured to match RA messages against the M flag in RA messages.

Format

managed-address-flag { **on** | **off** }

undo managed-address-flag

Parameters

Parameter	Description	Value
on	Indicates that the M flag is set to 1.	-
off	Indicates that the M flag is set to 0.	-

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

The M flag in an RA message determines whether users use stateful autoconfiguration to obtain IPv6 addresses. When the M flag is set to 1, a user obtains an IPv6 address using stateful autoconfiguration (for example, a DHCPv6 server). When the M flag is set to 0, a user obtains an IPv6 address using stateless autoconfiguration. That is, an IPv6 address is generated for the user according to the prefix information advertised by the router and the link-layer address of the user.

After a rule is configured to match RA messages against the M flag in RA messages in the IPv6 RA guard policy view, the interface to which the policy is applied checks the M flag in the received RA messages and forwards the messages only when the messages match the rule. Otherwise, the interface discards the messages.

Example

In the IPv6 RA guard policy **p1**, set the matching rule of the M flag to **on**. That is, users obtain IPv6 addresses using stateful autoconfiguration.

```
<HUAWEI> system-view
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] managed-address-flag on
```

14.10.9 nd raguard role

Function

The **nd raguard role** command configures an interface role for IPv6 RA guard.

The **undo nd raguard role** command deletes the interface role configured for IPv6 RA guard.

By default, no interface role is configured for IPv6 RA guard.

Format

nd raguard role { **host** | **router** }

undo nd raguard role

Parameters

Parameter	Description	Value
host	Specifies the interface role as a host interface.	-
router	Specifies the interface role as a router interface.	-

Views

Layer 2 Ethernet interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Administrators can configure an interface role based on the network location of interfaces. If an interface is connected to a user host, administrators can configure the interface role of the interface as a host interface. If the interface is connected to a router, administrators can configure the interface role of the interface as a router interface.

- If the interface role of the interface is a router interface, the system forwards the RA messages received by the interface.
- If the interface role of the interface is a host interface, the system discards the RA messages.

Example

On GE0/0/1, configure the interface role as a router interface for IPv6 RA guard.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd raguard role router
```

14.10.10 nd raguard policy

Function

The **nd raguard policy** command creates an IPv6 RA guard policy and displays the IPv6 RA guard policy view.

The **undo nd raguard policy** command deletes a created IPv6 RA guard policy.

By default, no IPv6 RA guard policy is created.

Format

nd raguard policy *policy-name*

undo nd raguard policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPv6 RA guard policy.	The value is a string of 1 to 31 case-insensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure an IPv6 RA guard policy for an interface to filter RA messages in the following situations:

- The type of the device or terminal connected to the interface cannot be determined. That is, no interface role can be configured for the interface to help determine whether to discard or forward RA messages.
- The interface is connected to a router and needs to filter RA messages based on specific conditions instead of forwarding RA messages immediately.

Follow-up Procedure

Configure a matching rule in the IPv6 RA guard policy view and run the **nd raguard attach-policy** command to apply the IPv6 RA guard policy to an interface.

Example

Create an IPv6 RA guard policy named **p1**.

```
<HUAWEI> system-view
[HUAWEI] nd raguard policy p1
```

14.10.11 nd raguard attach-policy

Function

The **nd raguard attach-policy** command binds an IPv6 RA guard policy to an interface.

The **nd raguard attach-policy** command unbinds an IPv6 RA guard policy from an interface.

By default, no IPv6 RA guard policy is applied to an interface.

Format

nd raguard attach-policy *policy-name*

undo nd raguard attach-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPv6 RA guard policy.	The value must be the name of an existing IPv6 RA guard policy.

Views

Layer 2 Ethernet interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After an IPv6 RA guard policy is bound to an interface, the interface filters received RA messages based on the matching rules configured in the policy.

Example

Bind the IPv6 RA guard policy **p1** to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd raguard policy p1
```

```
[HUAWEI-nd-raguard-policy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd raguard attach-policy p1
```

14.10.12 nd raguard log enable

Function

The **nd raguard log enable** command enables the IPv6 RA guard log function.

The **nd raguard log enable** command disables the IPv6 RA guard log function.

By default, the IPv6 RA guard log function is disabled.

Format

nd raguard log enable

undo nd raguard log enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The IPv6 RA guard log function records RA message processing information to meet the audit requirements of administrators. After this function is enabled, the device generates the ND_RAGUARD/3/ND_RAGUARD_DROP log when detecting invalid RA messages. The log content includes the name of the attacked interface, source IP address and source MAC address of RA messages, and total number of RA messages discarded on the interface.

The IPv6 RA guard logs generated by the device are sent to the information center module for processing. The configuration of the information center module determines the output rules and output directions of the logs. For details about the information center, see Information Center Configuration in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.

Example

Enable the IPv6 RA guard log function.

```
<HUAWEI> system-view
[HUAWEI] nd raguard log enable
```

14.10.13 other-config-flag

Function

The **other-config-flag** command configures a rule to match RA messages against the O flag in RA messages.

The **undo other-config-flag** command deletes the rule used to match RA messages against the O flag in RA messages.

By default, no rule is configured to match RA messages against the O flag in RA messages.

Format

other-config-flag { **on** | **off** }

undo other-config-flag

Parameters

Parameter	Description	Value
on	Indicates that the O flag is set to 1.	-
off	Indicates that the O flag is set to 0	-

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

The O flag in an RA message determines whether users use stateful autoconfiguration to obtain information other than IPv6 addresses. When the O flag is set to 1, a user obtains information other than an IPv6 address using stateful autoconfiguration (for example, a DHCPv6 server). When the O flag is set to 0, a user obtains information other than an IPv6 address using stateless autoconfiguration.

After a rule is configured to match RA messages against the O flag in RA messages in the IPv6 RA guard policy view, the interface to which the policy is applied checks the O flag in the received RA messages and forwards the messages only when the messages match the rule. Otherwise, the interface discards the messages.

Example

In the IPv6 RA guard policy **p1**, set the matching rule of the O flag to **on**. That is, users obtain information other than IPv6 addresses using stateful autoconfiguration.

```
<HUAWEI> system-view
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] other-config-flag on
```

14.10.14 router-preference maximum

Function

The **router-preference maximum** command configures a rule to match RA messages against the highest route preference in RA messages.

The **undo router-preference maximum** command deletes the rule used to match RA messages against the highest route preference in RA messages.

By default, no rule is configured to match RA messages against the highest route preference in RA messages.

Format

router-preference maximum { **high** | **medium** | **low** }

undo router-preference maximum

Parameters

Parameter	Description	Value
high	Sets the highest route preference in RA messages to high preference.	-
medium	Sets the highest route preference in RA messages to medium preference.	-
low	Sets the highest route preference in RA messages to low preference.	-

Views

IPv6 RA guard policy view

Default Level

2: Configuration level

Usage Guidelines

RA messages carry the route preference field. Route preferences are classified into high preference (with the value 1), medium preference (with the value 0), and low preference (with the value 3). After receiving an RA message, a host updates its default route list and selects a route in descending order of the route preference.

After a rule is configured in an IPv6 RA guard policy to match RA messages against the highest route preference in RA messages, the interface to which the policy is applied checks the route preference of the received RA messages and forwards the RA messages only when the route preference of the messages is lower than or equal to that configured in the rule. Otherwise, the interface discards the messages.

Example

In the IPv6 RA guard policy **p1**, set the highest route preference used to match RA messages to medium preference.

```
<HUAWEI> system-view
[HUAWEI] nd raguard policy p1
[HUAWEI-nd-raguard-policy-p1] router-preference maximum medium
```

14.10.15 reset nd raguard statistic

Function

The **reset nd raguard statistic** command clears statistics about RA messages discarded by interfaces.

Format

reset nd raguard statistic [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about RA messages discarded by a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect statistics about RA messages discarded on interfaces within a certain period, run the **reset nd raguard statistic** command to clear the existing statistics and then run the **display nd raguard statistic** command.

Example

Clear statistics about RA messages discarded by interfaces.

```
<HUAWEI> reset nd raguard statistic
```

14.11 PPPoE+ Configuration Commands

14.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.11.2 display pppoe intermediate-agent information encapsulation

Function

The **display pppoe intermediate-agent information encapsulation** command displays the fields and vendor ID added to PPPoE packets.

Format

display pppoe intermediate-agent information encapsulation

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the fields and vendor ID added to PPPoE packets, you can run **display pppoe intermediate-agent information encapsulation** command to view the information.

Example

Display the fields and vendor ID added to PPPoE packets.

```
<HUAWEI> display pppoe intermediate-agent information encapsulation
 The vendor id is: 2011
 Encapsulation content contains: Circuit-id and Remote-id
```

Table 14-82 Description of the display pppoe intermediate-agent information encapsulation command output

Item	Description
The vendor id is	Vendor ID added to PPPoE packets. You can run the **pppoe intermediate-agent information vendor-id** *vendor-id* command to set this parameter.
Encapsulation content contains	Fields added to PPPoE packets. You can run the **pppoe intermediate-agent information encapsulation** { **circuit-id** | **remote-id** } * command to set this parameter.

14.11.3 display pppoe intermediate-agent information format

Function

The **display pppoe intermediate-agent information format** command displays formats of circuit ID and remote ID that are configured globally.

Format

display pppoe intermediate-agent information format

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After PPPoE+ is enabled globally, you can run the **display pppoe intermediate-agent information format** command to check whether the configuration of the circuit ID or remote ID added to PPPoE packets is correct.

Example

Display formats of circuit ID and remote ID that are configured globally.

```
<HUAWEI> display pppoe intermediate-agent information format
 The current information format :
  Circuit ID : EXTEND
  Remote  ID : COMMON
```

```
For example:
 interface GigabitEthernet0/0/1 SVLAN:200 CVLAN:100
 The PPPOE Intermediate Agent information is as follows:
 Circuit ID:00 04 00 c8 00 00
 Remote  ID:0022-0033-0044
```

Table 14-83 Description of the **display pppoe intermediate-agent information format** command output

Item	Description
Circuit ID	Format of the circuit ID - COMMON: indicates the standard fill format. - EXTEND: indicates the extended fill format. - USER DEFINE: indicates user-defined fill format. You can run the **pppoe intermediate-agent information format** command to set this parameter. If the **portdescription** keyword is specified in the user-defined circuit-id and no interface description is configured, the **Circuit ID** in **For example** displays **portdescription**.
Remote ID	Format of the remote ID - COMMON: indicates the standard fill format. - EXTEND: indicates the extended fill format. - USER DEFINE: indicates user-defined fill format. You can run the **pppoe intermediate-agent information format** command to set this parameter. Remote IDs vary according to devices. If the **portdescription** keyword is specified in the user-defined **remote-id** and no interface description is configured, the **Remote ID** in **For example** displays **portdescription**.

14.11.4 display pppoe intermediate-agent information policy

Function

The **display pppoe intermediate-agent information policy** command displays the global policy for processing original fields in PPPoE packets at the user side and PPPoE server side.

Format

display pppoe intermediate-agent information policy

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pppoe intermediate-agent information policy** command displays the global policy for processing original fields in PPPoE packets at the user side and PPPoE server side.

Example

Display the global policy for processing original information fields in PPPoE packets at the user side and PPPoE server side.

```
<HUAWEI> display pppoe intermediate-agent information policy
The current information Policy :REPLACE
The current ignore-reply Policy:ENABLE
```

Table 14-84 Description of the display pppoe intermediate-agent information policy command output

Item	Description
The current information Policy	Global policy for processing original information fields in PPPoE packets at the user side: ● DROP: removes original information fields from PPPoE packets. ● REPLACE: replaces original fields in PPPoE packets according to the field format. ● KEEP: reserves the content and format of original fields in PPPoE packets. You can run the **pppoe intermediate-agent information policy (system view)** command to set this parameter.
The current ignore-reply Policy	Global policy for processing PPPoE reply packets sent by the PPPoE server: ● ENABLE: indicates that the device does not process PPPoE reply packets sent by the PPPoE server. ● DISABLE: indicates that the device processes PPPoE reply packets sent by the PPPoE server. You can run the **pppoe intermediate-agent information ignore-reply** command to set this parameter.

14.11.5 pppoe intermediate-agent information enable

Function

The **pppoe intermediate-agent information enable** command enables PPPoE+ globally.

The **undo pppoe intermediate-agent information enable** command disables PPPoE+.

By default, PPPoE+ is disabled.

Format

pppoe intermediate-agent information enable

undo pppoe intermediate-agent information enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After PPPoE+ is enabled globally, the device can add information about the interface connected to the PPPoE client such as the slot ID/subcard ID/interface number to PPPoE packets. The user account and access interface information are both authenticated, preventing user account embezzling.

After the **pppoe intermediate-agent information enable** command is executed in the system view, PPPoE+ is enabled on all interfaces.

NOTE

If PPPoE+ is enabled on the device that has no ACL resources, the system displays the following message "Warning: Allocate acl resources failed." In this case, PPPoE+ does not work.

After PPPoE+ is enabled in a VPLS scenario, traffic cannot be forwarded.

Example

Enable PPPoE+ globally.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
```

14.11.6 pppoe intermediate-agent information encapsulation

Function

The **pppoe intermediate-agent information encapsulation** command configures fields added to PPPoE packets.

The **undo pppoe intermediate-agent information encapsulation** command restores the default fields added to PPPoE packets.

By default, the device adds the **circuit-id** and **remote-id** fields to PPPoE packets.

Format

pppoe intermediate-agent information encapsulation { **circuit-id** | **remote-id** } *

undo pppoe intermediate-agent information encapsulation

Parameters

Parameter	Description	Value
circuit-id	Indicates the circuit ID (CID).	-
remote-id	Indicates the remote ID (RID).	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PPPoE+ is enabled, the device adds the **circuit-id** and **remote-id** fields to PPPoE packets by default. If the remote non-Huawei PPPoE server can identify only the **circuit-id** or **remote-id** field, run the **pppoe intermediate-agent information encapsulation** command to configure the device only to add the **circuit-id** or **remote-id** fields to PPPoE packets.

Prerequisites

The PPPoE+ function has been enabled by running the **pppoe intermediate-agent information enable** command in the system view.

Example

Configure the device only to add the **circuit-id** field to PPPoE packets.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information encapsulation circuit-id
```

14.11.7 pppoe intermediate-agent information format

Function

The **pppoe intermediate-agent information format** command configures the format of fields added to PPPoE packets.

The **undo pppoe intermediate-agent information format** command restores the format of fields added to PPPoE packets to default values.

By default, the format of fields **circuit-id** and **remote-id** added to PPPoE packets is **common**.

Format

pppoe intermediate-agent information [**vlan** *vlan-id*] [**ce-vlan** *cevlan-id*] **format** { **circuit-id** | **remote-id** } { **common** | **extend** | **user-defined** *text* }

undo pppoe intermediate-agent information format all

undo pppoe intermediate-agent information [**vlan** *vlan-id*] [**ce-vlan** *cevlan-id*] **format** { **circuit-id** | **remote-id** }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Indicates the outer VLAN ID. **NOTE** This parameter is not supported in the system view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *cevlan-id*	Indicates the end inner VLAN ID. **NOTE** This parameter is not supported in the system view.	The value is an integer that ranges from 1 to 4094.
circuit-id	Indicates the circuit ID (CID).	-
remote-id	Indicates the remote ID (RID).	-

Parameter	Description	Value
common	Indicates the standard fill format. ● CID format: {eth|trunk}slot ID/subcard ID/port ID:svlan.cvlan host name0/0/0/0/0, in ASCII format ● RID format: device MAC address (6 bytes), in ASCII format	-
extend	Indicates the extended format. ● CID format: circuit-id type (0) + length (4) + S-VLAN ID (2 bytes) + slot ID (5 bits) + subslot ID (3 bits) + port (1 byte), in hexadecimal notation ● RID format: remote-id type (0) + length (6) + MAC address (6 bytes), in hexadecimal notation In the format of the CID or RID, the values in parentheses without a unit are fixed values of the fields, and the values in parentheses with a unit indicate the length of the corresponding fields.	-
user-defined *text*	Indicates the user-defined format.	The *text* parameter specifies a user-defined format, and the value is a string of 1 to 127 characters. The details about the customized format string are provided in Precautions.

Parameter	Description	Value
all	Indicates the all format of fields. **NOTE** This parameter is not supported in the system view.	-

Views

System view and interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PPPoE+ is enabled globally, the default policy for processing user-side PPPoE packets is **replace**. The device replaces original information fields in the PPPoE packets received at the user side with those in common format. You can run the **pppoe intermediate-agent information format** command to change the format of information fields.

When the policy for processing user-side PPPoE packets is **replace** and the **pppoe intermediate-agent information format** command is executed, all interfaces add fields in a specified format to received PPPoE packets in the system view.

When the **pppoe intermediate-agent information format** command is configured, the device uses the following matching rules to encapsulate the information fields in PPPoE packets:

- For a double-tagged packet, the device matches the VLAN IDs in both the outer and inner VLAN tags. If the match fails, the device matches the VLAN ID in the inner VLAN tag, followed by that in the outer VLAN tag. If the match still fails, the device considers the packet does not carry a VLAN ID, and does not encapsulate the packet.
- For a single-tagged packet, the device matches the VLAN ID in the outer VLAN tag. If the match fails, the device considers the packet does not carry a VLAN ID, and does not encapsulate the packet.

If the **pppoe intermediate-agent information format** command is configured in both the interface and system views, the configuration in the interface view takes effect.

NOTE

Fields in PPPoE Intermediate-Agent Information packets support the following formats: **common**, **extend**, and **user-defined**. The formats are the same as those of DHCP Option 82. For description of the three parameters, see **dhcp option82 format**.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Precautions

You can use the following keywords to define the format. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port. For example, GigabitEthernet0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is valid in ASCII or hexadecimal notation.
- iftype: indicates the type of an interface. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of an interface. In ASCII format, the value is expressed as H-H-H in hexadecimal notation, and the value is a number of six bytes.
- Slot: specifies the slot ID. This keyword is valid in ASCII or hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII or hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII or hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 0 to 4095. This keyword is valid in ASCII or hexadecimal notation.
- cvlan: indicates the inner VLAN ID. The value ranges from 0 to 4095. This keyword is valid in ASCII or hexadecimal notation.
- n: specifies the value of the svlan or cvlan keyword if the outer VLAN tag or inner VLAN tag does not exist. The n keyword is on the left of the svlan or cvlan keyword. If the corresponding VLAN does not exist, the default value of the svlan or cvlan keyword is 4096 in ASCII format and is all Fs in hexadecimal notation. If the keyword n is added to the left of the svlan or cvlan keyword, the svlan or cvlan keyword is set to 0. This keyword is valid in ASCII or hexadecimal notation.
- length: indicates the total length of the keywords following the length keyword.
- portdescription: indicates the interface description. It is available only in ASCII format.

NOTE

Separators must be added between keywords; otherwise, they cannot be parsed. The separators cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number between the % symbol and a keyword indicates the length of the keyword. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the length of the corresponding keyword in bits.

- The [] symbol indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the [] symbol is added to information fields only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nested [] symbols.
- The \ symbol is an escape character. The %, \, and [] symbols following the escape character indicate themselves. For example, \\ represents \.
- The content in quotation marks (" ") is expressed in a character string, and the content outside the quotation marks are expressed in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain letters, numerals, and symbols ! @ # $ % ^ & * () _ + | - = \ [] {} ; : '" / . , <> `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, space characters, %, and the keywords.
  - In a hexadecimal notation string, numbers are encapsulated in information fields. A number in the range of 0-255 occupies one byte; a number in the range of 256-65535 occupies two bytes; a number in the range of 65536-4294967295 occupies four bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by space characters; otherwise, they are considered as a number.
  - All the space characters in a hexadecimal character string are ignored.
  - By default, each slot ID, subslot ID, port number, and VLAN ID in a hexadecimal notation string occupy two bytes. The length field occupies one byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the specified length of a keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal character string can contain only the keywords whose values are numbers. Other keywords, such as the port name, cannot be added to the hexadecimal character string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate to the string in the ASCII format, add the string into a pair of quotation marks. For example, the slot ID is 3, and the port ID is 4. If the format string is %slot %port, the value of the string after encapsulation is a hexadecimal number 00030004. If the format string is "%slot %port", the value of the string after encapsulation is 3 4.
  - A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

Configure the extended format for the **remote-id** field added to PPPoE packets.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information format remote-id extend
```

Configure the user-defined format for the **circuit-id** field added to PPPoE packets and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information format circuit-id user-defined "%portname:%svlan.
%cvlan %sysname"
```

Configure the extended format for the **remote-id** field added to PPPoE packets on GE1/0/1.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] pppoe intermediate-agent information format remote-id extend
```

14.11.8 pppoe intermediate-agent information ignore-reply

Function

The **pppoe intermediate-agent information ignore-reply** command configures the device whether to directly forward PPPoE reply packets sent by the PPPoE server.

The **undo pppoe intermediate-agent information ignore-reply** command restores the default policy for processing PPPoE packets sent by the PPPoE server.

By default, the device does not process PPPoE reply packets sent by the PPPoE server.

Format

pppoe intermediate-agent information ignore-reply { **disable** | **enable** }

undo pppoe intermediate-agent information ignore-reply

Parameters

Parameter	Description	Value
disable	Indicates that the device processes PPPoE reply packets sent by the PPPoE server.	-
enable	Indicates that the device does not process PPPoE reply packets sent by the PPPoE server.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the device does not process PPPoE reply packets and directly forwards them to the PPPoE client. Only when the PPPoE client cannot identify PPPoE packets that the device directly forwards, the device needs to process the PPPoE reply packets sent by the PPPoE server to ensure communication between the PPPoE server and PPPoE client. The PPPoE reply packets are processed as follows:

- When the policy for processing original fields in PPPoE packets is **replace** or **keep**:
  - If fields are not contained in PPPoE reply packets sent by the PPPoE server, the device directly forwards PPPoE reply packets.
  - If fields are contained in PPPoE reply packets sent by the PPPoE server and the format and content are consistent with those of the fields added to the user-side PPPoE packets, the device removes the original fields from PPPoE packets and forwards the packets. If the format and content are different from those of the fields added to the user-side PPPoE packets, the device directly forwards PPPoE reply packets.
- When the policy for processing original fields in PPPoE packets is **drop**, the device directly forwards the PPPoE packets:

Precautions

The **pppoe intermediate-agent information ignore-reply** command takes effect only after PPPoE+ is enabled globally. To modify the configuration, disable PPPoE+ globally first.

If the device is configured to process the PPPoE reply packets sent by the PPPoE server, the user access rate is reduced when the PPPoE server sends a large number of PPPoE+ packets.

Example

Configure the device to process PPPoE reply packets sent by the PPPoE server.

```
<HUAWEI> system-view
[HUAWEI] undo pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information ignore-reply disable
[HUAWEI] pppoe intermediate-agent information enable
```

14.11.9 pppoe intermediate-agent information policy (interface view)

Function

The **pppoe intermediate-agent information policy** command configures the policy for a specified interface to process original fields in user-side PPPoE packets.

The **undo pppoe intermediate-agent information policy** command restores the default policy for a specified interface to process original fields in user-side PPPoE packets.

By default, the policy configured on an interface to process original fields in user-side PPPoE packets is **replace**.

Format

pppoe intermediate-agent information policy { **drop** | **replace** | **keep** }

undo pppoe intermediate-agent information policy

Parameters

Parameter	Description	Value
drop	Removes the original fields from PPPoE packets.	-
replace	Replaces original fields in PPPoE packets according to the field format.	-
keep	Reserves the content and format of original fields in PPPoE packets.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the policy for processing original fields in user-side PPPoE packets is configured, the device can add information about the interface connected to the PPPoE client such as the slot ID/subcard ID/interface number, VLAN ID, and MAC address to PPPoE packets. The user account and access interface information are both authenticated, preventing user account embezzling. If received PPPoE packets contain fields related to the interface that connected to the PPPoE client, the device removes or reserves original fields as required.

You can run the **pppoe intermediate-agent information policy (system view)** command to configure the PPPoE packet processing policy for all interfaces in the system view. To use a different policy on a specified interface, run the **pppoe intermediate-agent information policy** command. In this case, the policy for processing PPPoE packets on the interface depends on the interface configuration.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Example

Configure GE0/0/1 to replace original fields in the received PPPoE packets with the circuit ID and remote ID of the local device.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] pppoe intermediate-agent information policy replace
```

14.11.10 pppoe intermediate-agent information policy (system view)

Function

The **pppoe intermediate-agent information policy** command configures the policy for all interfaces to process original fields in user-side PPPoE packets.

The **undo pppoe intermediate-agent information policy** command restores the policy for all interfaces to process original fields in user-side PPPoE packets.

By default, the policy configured on all interfaces to process original fields in user-side PPPoE packets is **replace**.

Format

pppoe intermediate-agent information policy { **drop** | **replace** | **keep** }

undo pppoe intermediate-agent information policy

Parameters

Parameter	Description	Value
drop	Removes the original fields from PPPoE packets.	-
replace	Replaces original information fields in PPPoE packets according to the field format.	-
keep	Reserves the content and format of original fields in PPPoE packets. If a PPPoE packet does not contain the fields, the device adds the fields to the packet according to the configuration.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the policy for processing original fields in user-side PPPoE packets is configured, the device can add information about the interface connected to the PPPoE client such as the slot ID/subcard ID/interface number, VLAN ID, and MAC address to PPPoE packets. The user account and access interface information are both authenticated, preventing user account embezzling. If received PPPoE packets contain fields related to the interface that connected to the PPPoE client, the device removes or reserves original fields as required.

After the command is executed, the policy for processing PPPoE packets takes effect on all interfaces. To configure a policy on a specified interface, run the **pppoe intermediate-agent information policy (interface view)** command. In this case, the policy for processing PPPoE packets on the interface depends on the interface configuration.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Example

Configure all interfaces to replace original fields in the received PPPoE packets with the circuit ID and remote ID of the local device.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information policy replace
```

14.11.11 pppoe intermediate-agent information vendor-id

Function

The **pppoe intermediate-agent information vendor-id** command sets the vendor ID that the device adds to PPPoE packets.

The **undo pppoe intermediate-agent information vendor-id** command restores the default vendor ID that the device adds to PPPoE packets.

The default vendor ID that the device adds to PPPoE packets is 2011.

Format

pppoe intermediate-agent information vendor-id *vendor-id*

undo pppoe intermediate-agent information vendor-id

Parameters

Parameter	Description	Value
vendor-id *vendor-id*	Specifies a vendor ID added to PPPoE packets.	The value is an integer ranging from 0 to 4294967295. The default value is 2011.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After PPPoE+ is enabled, the device must negotiate with the PPPoE server using PPPoE packets containing the vendor ID. By default, the device adds vendor ID 2011 to PPPoE packets. If the device is connected to a non-Huawei PPPoE server, the vendor ID may not be 2011; for example, the vendor ID is 3561. In this case, run the **pppoe intermediate-agent information vendor-id** *vendor-id* command to set the vendor ID to be the same as that in PPPoE packets sent from the non-Huawei PPPoE server.

Prerequisites

Example

Set the vendor ID added to PPPoE packets to 3561.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information vendor-id 3561
```

14.11.12 pppoe uplink-port trusted

Function

The **pppoe uplink-port trusted** command configures an interface as a trusted interface.

The **undo pppoe uplink-port trusted** command restores an interface to be untrusted.

By default, all interfaces are untrusted interfaces.

Format

pppoe uplink-port trusted

undo pppoe uplink-port trusted

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent bogus PPPoE servers and the security risk caused by PPPoE packets forwarded to non-PPPoE service interfaces, the interface connecting the device and the PPPoE server must be configured as the trusted interface. Then PPPoE protocol packets are forwarded to the PPPoE server through the trusted interface only. In addition, only the PPPoE protocol packets received on the trusted interface can be forwarded to the PPPoE client.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Precautions

The trusted interface controls PPPoE protocol packets at the PPPoE discovery stage only. PPPoE service packets at the PPPoE session stage are not controlled.

If the trusted interface is configured on the device that has no ACL resources, the system displays the following message "Warning: Allocate acl resources failed." In this case, the trusted interface fails to be configured.

Example

Configure GE0/0/1 as the PPPoE trusted interface.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] pppoe uplink-port trusted
```

14.12 IP Source Guard Configuration Commands

14.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.12.2 display dhcp static user-bind

Function

The **display dhcp static user-bind** command displays information about a static binding table.

Format

display dhcp static user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries mapping a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays the binding entry mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to view information about a configured static binding table. The information includes the IP address, MAC address, VLAN information, and interface information.

Example

Display information about the static binding table.

```
<HUAWEI> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address           MAC Address   VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.1.1.1           00e0-fc02-0003 10 /-- /--      GE0/0/1
--------------------------------------------------------------------------------
Print count:      1     Total count:      1
```

Display detailed information about the static binding table.

```
<HUAWEI> display dhcp static user-bind all verbose
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.21.21.254
 MAC Address : --
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : GE0/0/1
 IPSG Status : IPv4 effective slot: <0>
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 14-85 Description of the **display dhcp static user-bind** command output

Item	Description
DHCP static Bind-table	Static DHCP binding entries. To configure a static DHCP binding table, run the **user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VSI that the online user belongs to.
VLAN(O/I/P)	Inner VLAN ID, outer VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

Item	Description
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: - IPv4 effective slot: <0> indicates that the binding table is effective for IPv4 packet checking in slot 0. - Ineffective This field is invalid if IP packet checking is not enabled.

14.12.3 display dhcpv6 static user-bind

Function

The **display dhcpv6 static user-bind** command displays the IPv6 binding table.

Format

display dhcpv6 static user-bind { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

display dhcpv6 static user-bind ipv6-prefix { *prefix/prefix-length* | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 32-digit hexadecimal number, in the format of X:X::X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.

Parameter	Description	Value
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
ipv6-prefix	Displays an IPv6 prefix binding entry.	-
prefix/*prefix-length*	Displays the binding entry mapping a specified IPv6 prefix.	*prefix* is a 32-digit hexadecimal number, in the format of X:X::X:X. *prefix-length* is an integer that ranges from 1 to 128.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to view information about a configured DHCPv6 static binding table. The information includes the IPv6 address, MAC address, VLAN information, and interface information. If prefix delegation (PD) users exist on the network, the device generates an IPv6 prefix binding entry. The **display dhcpv6 static user-bind ipv6-prefix** command displays the static IPv6 prefix binding entries.

Example

Display the DHCPv6 static binding table.

```
<HUAWEI> display dhcpv6 static user-bind all
DHCPV6 static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                      MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Interface
--------------------------------------------------------------------------------
fc00:1::1                     0001-0002-0003  10  /--  /--    --
--------------------------------------------------------------------------------
Print count:          1          Total count:          1
```

Display detailed information about the DHCPv6 static binding table.

```
<HUAWEI> display dhcpv6 static user-bind all verbose
DHCPV6 static Bind-table:
-------------------------------------------------------------------------------
 IP Address  : fc00:1::1
 MAC Address : 0001-0002-0003
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : --
 IPSG Status : IPv6 effective slot: <0>
-------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Display the IPv6 prefix static binding table.

```
<HUAWEI> display dhcpv6 static user-bind ipv6-prefix all
PD static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IPv6 Prefix                     MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Interface
-------------------------------------------------------------------------------
fc00:1000::12/32                0001-0002-0003  10  /--  /--    --
-------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 14-86 Description of the display dhcpv6 static user-bind command output

Item	Description
DHCPV6 static Bind-table	Static DHCPv6 binding entries. To configure a static DHCPv6 binding table, run the **user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - map vlan	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Map VLAN
IPv6 Prefix	User IPv6 prefix.
IP Address	User IPv6 address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
(BD-VLAN)	BD and the VLAN to which the BD is bound.
Interface	User access interface.

Item	Description
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: ● IPv6 effective slot: <0> indicates that the binding table is effective for IPv6 packet checking in slot 0. ● ineffective This field is invalid if IP packet checking is not enabled.

14.12.4 display ip source check user-bind

Function

The **display ip source check user-bind** command displays the IPSG configurations.

Format

display ip source check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the IP packet check configuration on a specified interface. The interface is specified by the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ip source check user-bind** command displays the IP packet check configuration on an interface, including IP packet check items and the alarm function of IP packet check.

Example

Display the IP packet check configuration on GE0/0/1.

```
<HUAWEI> display ip source check user-bind interface gigabitethernet 0/0/1
 ipv4 source check user-bind enable
 ipv6 source check user-bind enable
 ip source check user-bind check-item ip-address
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
```

Table 14-87 Description of the display ip source check user-bind command output

Item	Description
ipv4 source check user-bind enable	IPv4 packet check is enabled.
ipv6 source check user-bind enable	IPv6 packet check is enabled.
ip source check user-bind check-item ip-address	IP packet check items. An IP packet check item can contain the IP address, MAC address, VLAN ID, and interface number. To specify check items, run the **ip source check user-bind check-item (interface view)** or **ip source check user-bind check-item (VLAN view)** commands.
ip source check user-bind alarm enable	Alarm function of IP packet check is enabled. To enable the alarm function of IP packet check, run the **ip source check user-bind alarm enable** command.
ip source check user-bind alarm threshold 200	Alarm threshold for IP packet check. To set the alarm threshold for IP packet check, run the **ip source check user-bind alarm threshold** command.

14.12.5 display mac-address snooping

Function

The **display mac-address snooping** command displays snooping MAC address entries generated based on the snooping binding table.

Format

display mac-address snooping [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the static MAC address entry on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays all the static MAC address entries on all the interfaces in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
verbose	Displays detailed information about static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **user-bind ip sticky-mac** command in the interface view, the device generates snooping MAC address entries based on the snooping binding table. A snooping MAC address entry includes the user MAC address and VLAN ID. The **display mac-address snooping** command displays snooping MAC address entries generated based on the snooping binding table. If no interface or VLAN is specified, all the snooping MAC address entries generated based on the snooping binding table are displayed.

Example

Display the snooping MAC address entries generated based on the snooping binding table on the device.

```
<HUAWEI> display mac-address snooping
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                       Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc02-0602 10/-/-                            GE0/0/1             snooping
-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-88 Description of the **display mac-address snooping** command output

Item	Description
MAC Address	User MAC address.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or ID of the BD that the user belongs to.
Learned-From	Port number.
Type	Type of a MAC address entry, including: ● static: indicates a static MAC address entry. ● blackhole: indicates a blackhole MAC address entry. ● dynamic: indicates a dynamic MAC address entry. ● security: indicates a security MAC address entry. ● sticky: indicates a sticky MAC address entry. ● snooping: indicates a MAC address entry generated based on the snooping binding table.

14.12.6 ip anti-attack source-ip equals destination-ip drop

Function

The **ip anti-attack source-ip equals destination-ip drop** command enables the device to discard IP packets with the same source and destination IP addresses.

The **undo ip anti-attack source-ip equals destination-ip drop** command disables the device from discarding IP packets with the same source and destination IP addresses.

By default, the device does not discard IP packets with the same source and destination IP addresses.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ip anti-attack source-ip equals destination-ip drop

undo ip anti-attack source-ip equals destination-ip drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, IP packets with the same source and destination IP addresses can be forwarded. When you determine that the IP packets are attack packets, you can use the **ip anti-attack source-ip equals destination-ip drop** command to enable the device to discard the IP packets.

Precautions

On the following models, the device discards IP packets with the same source and destination IP addresses:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S

Example

Enable the device to discard IP packets with the same source and destination IP addresses.

```
<HUAWEI> system-view
[HUAWEI] ip anti-attack source-ip equals destination-ip drop
```

14.12.7 ip source check user-bind alarm enable

Function

The **ip source check user-bind alarm enable** command enables the alarm function of IP packet check.

The **undo ip source check user-bind alarm enable** command disables the alarm function of IP packet check.

By default, the alarm function of IP packet check is disabled.

Format

ip source check user-bind alarm enable

undo ip source check user-bind alarm enable

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip source check user-bind alarm enable** command enables the log and alarm function for IP packet check. If the number of discarded packets reaches the threshold, the device sends an alarm to the NMS device.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command on the interface.

Follow-up Procedure

Run the **ip source check user-bind alarm threshold** command to set the alarm threshold.

Precautions

If the alarm function of IP packet check is enabled both in the VLAN view and in the view of the interface added to the VLAN, it takes effect in the view where it was first enabled. To change the order in which the function takes effect, disable it in the view where it has taken effect, and then enable it in the desired view.

Example

Enable the alarm function for IP packet check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind alarm enable
```

14.12.8 ip source check user-bind alarm threshold

Function

The **ip source check user-bind alarm threshold** command sets the alarm threshold for IP packet check.

The **undo ip source check user-bind alarm threshold** command restores the default alarm threshold for IP packet check.

By default, the alarm threshold is 100.

Format

ip source check user-bind alarm threshold *threshold*

undo ip source check user-bind alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies an alarm threshold for IP packet check.	The value is an integer that ranges from 1 to 1000.

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of IP packet check is enabled, run the **ip source check user-bind alarm threshold** command to set the alarm threshold for IP packet check.

Prerequisites

The alarm function of IP packet check has been enabled using the **ip source check user-bind alarm enable** command.

Example

Set the alarm threshold for IP packet check to 200 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind alarm enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind alarm threshold 200
```

14.12.9 ip source check user-bind check-item (interface view)

Function

The **ip source check user-bind check-item** command configures IP packet check items on an interface.

The **undo ip source check user-bind check-item** command restores the default IP packet check items.

By default, the check items contain the IP address, MAC address, VLAN and interface information..

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
vlan	Checks whether VLAN information of an IP packet matches a binding entry.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (interface view)** command to specify items in the IP packet to be checked on a specified interface. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP packet contain the source IP address, source MAC address, and VLAN information. Interface information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the interface view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

Example

Enable IP packet check on GE0/0/1 to check whether the IP address in the IP packet matches the binding entry.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind check-item ip-address
```

14.12.10 ip source check user-bind check-item (VLAN view)

Function

The **ip source check user-bind check-item** command configures IP packet check items in a VLAN.

The **undo ip source check user-bind check-item** command restores the default IP packet check items in a VLAN.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
interface	Checks whether interface information of an IP packet matches a binding entry.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (VLAN view)** command to configure IP packet check items in a specified VLAN. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP packet contain the source IP address, source MAC address, and interface information. VLAN information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the VLAN view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

Example

Enable IP packet check in VLAN 100 and check whether the IP address in the IP packet matches the binding entry.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] ip source check user-bind enable
[HUAWEI-vlan100] ip source check user-bind check-item ip-address
```

14.12.11 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP packet check.

The **undo ip source check user-bind enable** command disables IP packet check.

By default, IP packet check is disabled.

Format

ip source check user-bind enable

undo ip source check user-bind enable

ipv4 source check user-bind enable

undo ipv4 source check user-bind enable

ipv6 source check user-bind enable

undo ipv6 source check user-bind enable

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unauthorized users often send bogus packets with the source IP address and MAC address of authorized users to access or attack the network. Then authorized users cannot access stable and secure networks. To address this problem, you can configure IP packet check.

When IP packet check is enabled, the device checks the IP address, MAC address, VLAN information, and interface information against the binding table. You can run the **ip source check user-bind check-item** or **ip source check user-bind check-item** command to specify IP packet check items. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded.

Prerequisites

The IP packet check is based by binding table. So,

- The dynamic DHCP snooping binding table has been generated for DHCP users.
- The static binding table has been configured manually for users using static IP addresses.
- The dynamic ND snooping binding table has been generated for users dynamically obtaining IPv6 addresses through Stateless Address Autoconfiguration.

Precautions

After IP packet check is enabled using the **ip source check user-bind enable** command, the device checks the source IPv4 and IPv6 addresses of users' IP packets. The configuration file is displayed as follows:

```
ipv4 source check user-bind enable
ipv6 source check user-bind enable
```

To check only IPv4 or IPv6 packets, run the **ipv4 source check user-bind enable** or **ipv6 source check user-bind enable** command.

Example

Enable IPv4 and IPv6 packet check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
```

Enable IPv4 packet check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv4 source check user-bind enable
```

14.12.12 user-bind static

Function

The **user-bind static** command configures a static binding table.

The **undo user-bind static** command deletes a static binding table.

By default, no static binding table is configured.

Format

user-bind static { { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

undo user-bind static [{ **ip-address** { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-address** [*start-ip* [**to** *end-ip*]] &<1-10> | **ipv6-prefix** [*prefix/prefix-length*] } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface connected to a user in a static binding entry. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
ip-address	Indicates the static IPv4 address.	-
ipv6-address	Indicates the static IPv6 address.	-

Parameter	**Description**	**Value**
start-ip [**to** *end-ip*]	Specifies the user IP address in a static binding entry. - *start-ip* specifies the first IP address. - **to** *end-ip* specifies the last IP address. The value of *end-ip* must be larger than the value of *start-ip*. *start-ip* and *end-ip* identify a VLAN range. If **to** *end-ip* is not specified, only the start IP address is added to the static binding entry. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	The IPv4 address is in dotted decimal notation in the format of X.X.X.X. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix *prefix/prefix-length*	Specifies the prefix of an IPv6 address	The prefix consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. *prefix-length* is an integer that ranges from 1 to 128.
mac-address *mac-address*	Specifies the user MAC address in a static binding entry.	The value is in hexadecimal notation. The value is in the format of H-H-H.
vlan *vlan-id*	Specifies the user VLAN ID in a static binding entry.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN tag of a QinQ packet in a static binding entry.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When DHCP snooping is enabled, a dynamic binding table is automatically generated for dynamic users. However, a static binding table cannot be generated for static users. If IP source guard is enabled but no static binding table is available, the device discards all static users' forwarding packets. To enable the device to forward static users' packets, run the **user-bind static** command to configure a static binding table.

Precautions

After a static binding table is configured and IP source guard is enabled, the device performs a match check on IP packets based on the configured binding entries. If the match check fails, the device discards the IP packets.

Example

Configure a static binding entry for a user in VLAN 2 with the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 10.1.1.1 vlan 2
```

14.12.13 user-bind ip sticky-mac

Function

The **user-bind ip sticky-mac** command enables the device to generate snooping MAC entries.

The **undo user-bind ip sticky-mac** command disables the device from generating snooping MAC entries.

By default, the device does not generate snooping MAC entries.

Format

user-bind ip sticky-mac

undo user-bind ip sticky-mac

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the users with unauthorized MAC addresses from attacking the network, run the **user-bind ip sticky-mac** command to configure the device to generate snooping MAC entries on the interface that is prone to attack. After the device is configured to generate snooping MAC entries, it translates the dynamic MAC entries learned by the interface into snooping MAC entries (snooping MAC entries are a type of static MAC entries) based on the DHCP snooping binding table and ND snooping binding table, or generates snooping MAC entries based on the static binding entries.

After the configuration is complete, the interface forwards only the IP packets of which the source MAC addresses are included in the static MAC entries (static and snooping), and discards other IP packets.

NOTE

- To view MAC entry information on the device, see **display mac-address**.
- If a binding entry is modified, the matching snooping MAC entry is also modified.

Prerequisites

Before using the **user-bind ip sticky-mac** command, ensure that the DHCP snooping function has been enabled by the **dhcp snooping enable** command.

Precautions

- To ensure correct packet forwarding for authorized static users on an interface, you can run the **user-bind static** command to configure static binding entries, which generate static MAC entries, or run the **mac-address static** command to configure static MAC entries.
- When configuring a static binding entry, specify the MAC address, VLAN ID, and interface number. The VLAN ID must already exist on the device. If you do not specify the three parameters, a snooping MAC entry cannot be generated based on this static binding entry.
- To allow DHCPv6 users to go online, enable both DHCP snooping and ND snooping.
- To check whether the snooping MAC address entries are successfully delivered, you can use **display mac-address summary** to check the total number of snooping MAC address entries. If the snooping MAC address entries fail to be delivered, the possible cause is a hash conflict.
- The **user-bind ip sticky-mac** command cannot be used together with the following commands.

Command	Description
dot1x enable	Enables 802.1X authentication on an interface.
mac-authen	Enables MAC address-based authentication on an interface.
authentication-profile (Interface view or VAP profile view)	Applies an authentication profile to the interface or VAP profile.
mac-address learning disable (Interface view and VLAN view)	Enables MAC address learning.

Command	Description
mac-limit	Sets the maximum number of MAC addresses to be learned.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Enables VLAN mapping.
port-security enable	Enables port security.

Example

Configure the GE0/0/1 interface to generate snooping MAC entries based on the snooping binding table.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] user-bind ip sticky-mac
```

14.13 SAVI Configuration Commands

14.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.13.2 savi max dad-delay

Function

The **savi max dad-delay** command sets the time for listening to an NA packet responding to address conflicts.

The **undo savi max dad-delay** command restores the default setting.

By default, the time for listening to an NA packet responding to address conflicts is 2 seconds.

Format

savi max dad-delay *value*

undo savi max dad-delay

Parameters

Parameter	Description	Value
value	Specifies the time for listening to an NA packet responding to address conflicts.	The value is an integer that ranges from 1 to 100, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **savi max dad-delay** command is applicable only for SLAAC-Only scenarios and DHCPv6+SLAAC scenarios.

- In SLAAC-Only scenarios:

  When obtaining an IP address in SLAAC mode, an ND client generates the IPv6 address based on the prefix in the RA packet. After the IPv6 address is generated, the ND client sends an NS packet to check whether duplicate addresses exist on the network. When detecting the NS packet in the DAD process from the ND client, the device generates an ND snooping entry, sets the entry to the detect state, and listens to the mapping NA packet.

  - If a mapping NA packet is detected in the configured listening period, IPv6 address conflict occurs and the device deletes this ND snooping entry.
  - If no mapping NA packet is detected in the configured listening period, the IPv6 address is available and the device sets the ND snooping entry to the bound state. The device deletes the ND snooping entry only when the entry ages out. If automatic user status detection for users mapping ND snooping dynamic binding entries is enabled using the **nd user-bind detect enable** command on the device, and no NA packet is returned from the user after NS packets are sent for times configured using the **nd user-bind detect retransmit** *retransmit-times* **interval** *retransmit-interval* command, the device considers the user to be offline and deletes the mapping ND snooping entry.
- In DHCPv6+SLAAC scenarios:
  - The procedure for processing packets by SAVI in SLAAC mode is the same as that in SLAAC-Only scenarios.
  - When obtaining an IP address in DHCPv6 mode, a DHCPv6 client may send an NS packet to check whether duplicate addresses exist on the network. When detecting the NS packet in the DAD process from the DHCPv6 client, the device sets the mapping DHCPv6 snooping entry to the detect state, and listens to the mapping NA packet.

  - If a mapping NA packet is detected in the configured listening period, IPv6 address conflict occurs and the device deletes this DHCPv6 snooping entry.
  - If no mapping NA packet is detected in the configured listening period, the IPv6 address is available and the device sets the DHCPv6 snooping entry to the bound state.

When the DHCPv6 Snooping entry is in detection state, the device deletes this entry after detecting the NA packets within the time of listening on NA packets with response address conflicts. When the DHCPv6 Snooping entry is in bound state, the device deletes this entry after detecting the DHCPv6 Decline or DHCPv6 Release packets sent from the DHCPv6 clients.

Prerequisites

The SAVI function has been enabled using the **savi enable** command.

Precautions

This command is used together with ND snooping and DHCPv6 snooping.

Example

Set the time for listening to an NA packet responding to address conflicts to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] savi enable
[HUAWEI] savi max dad-delay 5
```

14.13.3 savi max dad-prepare-delay

Function

The **savi max dad-prepare-delay** command sets the time for listening to the duplicate address detection performed by the DHCPv6 client.

The **undo savi max dad-prepare-delay** command restores the default setting.

By default, the time for listening to the duplicate address detection performed by the DHCPv6 client is 2 seconds.

Format

savi max dad-prepare-delay *value*

undo savi max dad-prepare-delay

Parameters

Parameter	Description	Value
value	Specifies the time for listening to the duplicate address detection performed by the DHCPv6 client.	The value is an integer that ranges from 1 to 100, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **savi max dad-prepare-delay** command is applicable only for DHCPv6-Only scenarios and DHCPv6+SLAAC scenarios.

After detecting that the DHCPv6 client obtains the IPv6 address, the device detects whether the DHCPv6 client sends an NS packet for duplicate address detection.

- In DHCPv6-Only scenarios:
  - If no NS packet in the DAD process is detected in the configured listening period, the device sets the DHCPv6 snooping entry to the bound state. It indicates that the DHCPv6 does not perform the duplicate address detection on the obtained IPv6 address or no duplicate IPv6 address exists.
  - If an NS packet in the DAD process is detected in the configured listening period, the device does not change the status of the mapping DHCPv6 snooping entry. The device sets the DHCPv6 snooping entry to the bound state only when the listening period expires.

  In DHCPv6-Only scenarios, when detecting the DHCPv6 Decline packet or DHCPv6 Release packet from the DHCPv6 client, the device deletes the corresponding DHCPv6 snooping entry.
- In DHCPv6+SLAAC scenarios:
  - If no NS packet in the DAD process is detected in the configured listening period, the device sets the DHCPv6 snooping or ND snooping entry to the bound state. It indicates that the client does not perform the duplicate address detection on the obtained IPv6 address or no duplicate IPv6 address exists, and the client can use this IPv6 address.
  - If an NS packet in the DAD process is detected in the configured listening period, the device sets the mapping DHCPv6 snooping or ND snooping entry to the detection state, and listens to the mapping NA packet. For the listening method, see **savi max dad-delay**.

Prerequisites

The SAVI function has been enabled using the **savi enable** command.

Precautions

This command is used together with ND snooping and DHCPv6 snooping.

Example

Set the time for listening to the duplicate address detection performed by the DHCPv6 client to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] savi enable
[HUAWEI] savi max dad-prepare-delay 5
```

14.13.4 savi max-binding-table

Function

The **savi max-binding-table** command sets the maximum number of SAVI binding entries on an interface.

The **undo savi max-binding-table** command restores the default maximum number of SAVI binding entries on an interface.

By default, the maximum number of SAVI binding entries is the same as the number of binding entries supported by the device.

Format

savi max-binding-table *max-number*

undo savi max-binding-table

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of SAVI binding entries on an interface.	The value is an integer that varies depending on product models.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SAVI binding table is a set of the ND snooping binding table and DHCPv6 snooping binding table. When the sum of ND snooping binding entries and DHCPv6 snooping binding entries on an interface reaches the configured maximum number of SAVI binding entries, subsequent users cannot connect to the network. After the maximum number of SAVI binding entries is set, the device does not process many ND packets and DHCPv6 packets with invalid source addresses to defend against attacks.

Prerequisites

Ensure that SAVI has been enabled globally using the **savi enable** command.

Example

Set the maximum number of SAVI binding entries on the GE0/0/1 to 8.

```
<HUAWEI> system-view
[HUAWEI] savi enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] savi max-binding-table 8
```

14.13.5 savi enable

Function

The **savi enable** command enables the SAVI function.

The **undo savi enable** command disables the SAVI function.

By default, the SAVI function is disabled.

Format

savi enable

undo savi enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the SAVI function is enabled, the device checks the validity of the source addresses in the ND, DHCPv6, and IPv6 data packets based on the bindings between IP addresses and ports and filters out invalid packets. The bindings between IP addresses and ports are generated based on ND snooping and DHCPv6 snooping.

Precautions

The SAVI function must be used together with ND snooping, DHCPv6 snooping, or IP source guard.

After the SAVI function is enabled, only when both ND snooping and IP source guard are enabled or both DHCPv6 snooping and IP source guard are enabled on an interface, the device checks the validity of the source addresses in IPv6 data packets received on this interface.

Example

Enable the SAVI function.

```
<HUAWEI> system-view
[HUAWEI] savi enable
```

14.14 URPF Configuration Commands

14.14.1 Command Support

Only the following switch models support URPF:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

14.14.2 urpf (interface view)

Function

The **urpf** command enables URPF on an interface and configures the URPF mode.

The **undo urpf** command disables URPF on an interface.

By default, URPF is disabled on an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

For the S6735-S, S6720-EI, and S6720S-EI, only Layer 2 Ethernet interfaces support URPF strict check.

Format

urpf { **loose** | **strict** } [**allow-default-route**]

undo urpf

Parameters

Parameter	Description	Value
loose	Indicates URPF check in loose mode. A packet passes the check as long as the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet is not required to be the same as the outbound interface of the route.	-
strict	Indicates URPF check in strict mode. A packet passes the check only when the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet should be the same as the outbound interface of the route.	-
allow-default-route	Allows the route to the source IP address of the packet to be configured as the default route. If this parameter is not configured, the device does not allow the route to the source IP address of the packet to be configured as the default route during the URPF check.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Denial of Service (DoS) attack disables users from connecting to a server. DoS attacks aim to occupy many resources by sending a large number of connection requests to a specified server. The attacked server cannot respond to authorized users.

URPF searches for the route to the source IP address in the routing table based on the source IP address of the packet, and checks whether the inbound interface of the packet is the same as the outbound interface of the route. If no route to the source IP address of the packet exists in the routing table, or the inbound interface of the packet is different from the outbound interface of the route, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

In a complicated networking environment, asymmetric routes may exist. That is, the routes recorded on the local end and remote end are different. A URPF-enabled device on this network may discard the packets transmitted along the correct path, but forward the packets transmitted along incorrect paths. The device provides the following two URPF modes to solve this problem:

- **Strict mode**

  In strict mode, a packet passes the check only when the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet should be the same as the outbound interface of the route.

  If route symmetry is ensured, you are advised to use the URPF strict mode. For example, if there is only one path between two network edge devices, URPF strict mode can be used to ensure network security.

- **Loose mode**

  In loose mode, a packet passes the check as long as the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet is not required to be the same as the outbound interface of the route.

  If route symmetry is not ensured, you are advised to use the URPF loose mode. For example, if there are multiple paths between two network edge devices, URPF loose mode can be used to ensure network security and prevent the packets transmitted along the correct path from being discarded.

Prerequisites

For the S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, and S6720S-EI, configurations on the interface take effect only after global URPF is enabled using the **urpf** command.

Precautions

In the Eth-Trunk interface view, this command conflicts with the **service type tunnel**, **service type multicast-tunnel**, or **service type vxlan-tunnel** command and cannot be run in the same Eth-Trunk interface view.

For the S6720-EI, S6735-S and S6720S-EI, even if no default route is configured, the **urpf loose allow-default-route** command takes effect when the resource allocation mode is set to **enhanced-ipv4** or **ipv4-ipv6 6:1** using the **assign resource-mode** command. The device allows the route to the source IP address of the packet to be configured as the default route during the URPF loose check.

For the S5735-S-I, only URPF check in loose mode is supported. For the S5735-S and S5735S-S, V200R019C10 and later versions support only URPF check in loose mode. If URPF check in strict mode is configured in V200R019C00, the configuration will be changed to URPF check in loose mode after the version is upgraded to V200R019C10 or later.

Example

Enable URPF strict check on a Layer 2 interface GE0/0/1 and allow the route to the source IP address of the packet to be configured as the default route.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] urpf strict allow-default-route
```

Enable URPF loose check on a Layer 3 interface GE0/0/2 and allow the route to the source IP address of the packet to be configured as the default route.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] undo portswitch
[HUAWEI-GigabitEthernet0/0/2] urpf loose allow-default-route
```

14.14.3 urpf (system view)

Function

The **urpf** command enables global URPF.

The **undo urpf** command disables global URPF.

By default, the switch does not enable global URPF.

NOTE

Only S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6735-S, S6720-EI, and S6720S-EI support this command.

Format

For S5720I-SI, S5735S-H, S6720S-S, and S5736-S:

urpf [**slot** *slot-id*]

undo urpf [**slot** *slot-id*]

For S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, and S6720S-EI:

urpf slot *slot-id* [**based-logic-port**]

undo urpf slot *slot-id* [**based-logic-port**]

Parameters

Parameter	Description	Value
slot *slot-id*	- Specifies the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	Set the value according to the device configuration.
based-logic-port	- If this parameter is specified, URPF check configured on logical interfaces takes effect, including VLANIF interfaces and subinterfaces, and URPF check configured on Ethernet interfaces does not take effect, including Layer 2 and Layer 3 Ethernet interfaces. - If this parameter is not specified, URPF check configured on Ethernet interfaces takes effect, and URPF check configured on logical interfaces does not take effect.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Denial of Service (DoS) attack disables users from connecting to a server. DoS attacks aim to occupy many resources by sending a large number of connection requests to a specified server. The attacked server cannot respond to authorized users.

URPF searches for the route to the source IP address in the routing table based on the source IP address of the packet, and checks whether the inbound interface of the packet is the same as the outbound interface of the route. If no route to the source IP address of the packet exists in the routing table, or the inbound interface of the packet is different from the outbound interface of the route, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

In a complicated networking environment, asymmetric routes may exist. That is, the routes recorded on the local end and remote end are different. A URPF-enabled device on this network may discard the packets transmitted along the correct path, but forward the packets transmitted along incorrect paths. The device provides the following two URPF modes to solve this problem:

- **Strict mode**

  In strict mode, a packet passes the check only when the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet should be the same as the outbound interface of the route.

  If route symmetry is ensured, you are advised to use the URPF strict mode. For example, if there is only one path between two network edge devices, URPF strict mode can be used to ensure network security.

- **Loose mode**

  In loose mode, a packet passes the check as long as the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet is not required to be the same as the outbound interface of the route.

  If route symmetry is not ensured, you are advised to use the URPF loose mode. For example, if there are multiple paths between two network edge devices, URPF loose mode can be used to ensure network security and prevent the packets transmitted along the correct path from being discarded.

Precautions

- Enabling or disabling global URPF will affect packet forwarding in a short period of time.
- The S5720I-SI, S5735S-H, S6720S-S, and S5736-S only support URPF strict check.
- For the S5720I-SI, S5735S-H, S6720S-S, and S5736-S, after a stack is set up, if **slot** *slot-id* is not specified when the **urpf (system view)** command is executed, URPF takes effect only on the master switch.

- For the S6720-EI and S6720S-EI, the number of FIB entries are reduced by half if URPF is enabled. You are advised to enable URPF before services are deployed. If you need to enable URPF after services are deployed, configure URPF when less traffic is transmitted and ensure that network requirements are met if the number of FIB entries is reduced by half.
- If both the **urpf slot** *slot-id* and **urpf slot** *slot-id* **based-logic-port** commands are executed, the last configured one takes effect.

Follow-up Procedure

For the S5735-S, S5735S-S, S5735-S-I, S6735-S, S6720-EI, and S6720S-EI, run the **urpf(interface view)** command to enable URPF on an interface and configure the URPF mode.

Example

Enable global URPF on the device.

```
<HUAWEI> system-view
[HUAWEI] urpf slot 0
Warning: Changing the global URPF status may interrupt some services for several seconds and FIB entries
supported may be reduced. Continue? [Y/N]:y
```

Change URPF from Ethernet interface-based to logical interface-based.

```
<HUAWEI> system-view
[HUAWEI] urpf slot 0 based-logic-port
Warning: Changing the global URPF status may interrupt some services for several seconds and FIB entries
supported may be reduced. Continue? [Y/N]: y
Warning: The global URPF mode will be changed from physical interface-based to logical interface-based.
The URPF configuration on all Layer 2 or Layer 3 physical interfaces of the card will become invalid. Are
you sure to continue? [Y/N]: y
```

Change URPF from logical interface-based to Ethernet interface-based.

```
<HUAWEI> system-view
[HUAWEI] urpf slot 0
Warning: Changing the global URPF status may interrupt some services for several seconds and FIB entries
supported may be reduced. Continue? [Y/N]: y
Warning: The global URPF mode will be changed from logical interface-based to physical interface-based.
The URPF configuration on all sub-interfaces or VLANIF interfaces of the card will become invalid. Are you
sure to continue? [Y/N]: y
```

14.15 Keychain Configuration Commands

14.15.1 Command Support

Only the following switch models support Keychain:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

14.15.2 algorithm

Function

The **algorithm** command configures the authentication algorithm of a key.

The **undo algorithm** command deletes the authentication algorithm of a key.

By default, no authentication algorithm is configured.

Format

algorithm { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** | **sm3** }

undo algorithm

Parameters

Parameter	Description	Value
hmac-md5	Specifies HMAC-MD5 as the authentication algorithm.	-
hmac-sha-256	Specifies HMAC-SHA-256 as the authentication algorithm.	-
hmac-sha1-12	Specifies HMAC-SHA1-12 as the authentication algorithm.	-
hmac-sha1-20	Specifies HMAC-SHA1-20 as the authentication algorithm.	-
md5	Specifies MD5 as the authentication algorithm.	-
sha-1	Specifies SHA-1 as the authentication algorithm.	-
sha-256	Specifies SHA-256 as the authentication algorithm.	-
simple	Indicates that the configured key is used for packet authentication.	-
sm3	Specifies SM3 as the authentication algorithm.	-

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. A keychain consists of multiple keys, each of which needs to be configured with an authentication algorithm. Different keys are valid within different time periods, ensuring dynamic change of keychain authentication algorithms.

Packets are authenticated and encrypted based on the authentication algorithm and key string associated with a specified key. This improves the packet transmission security.

The characteristics of each authentication algorithm are as follows:

- MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length.
- SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. Then, 0s are added to make up a 512-bit message.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.
- SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code.
- SM3: The 256-bit SM3 message digest is calculated based on the entered message of any length. All the 256 bits are used as the authentication code.

Prerequisites

key-id has been configured.

Precautions

SHA-1 has low security, for higher security purposes, you are advised to specify the **hmac-sha-256** or **sha2-256** parameter.

Keys configured on the sender and receiver of packets must correspond to the same authentication and encryption algorithms. Otherwise, packet transmission fails for not passing the authentication.

If algorithm is not configured, key will never be active.

Different protocols support different algorithms.

- RIP supports MD5 and simple.
- BGP and BGP4+ support MD5.
- IS-IS supports HMAC-MD5 and simple.
- OSPF supports MD5, simple and HMAC-MD5.
- MSDP supports MD5.
- MPLS LDP supports MD5. MPLS TE supports HMAC-MD5.

Example

Specify sha-256 as the authentication algorithm of key-id 1.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] key-id 1
[HUAWEI-keychain-test-keyid-1] algorithm sha-256
```

14.15.3 default send-key-id

Function

The **default send-key-id** command configures a particular key as the default send key for that keychain.

The **undo default send-key-id** command deletes default send key.

By default, no key is configured as default send key.

Format

default send-key-id

undo default send-key-id

Parameters

None

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key sting dynamically. This can reduce the workload of changing the algorithm and key manually. A keychain consists of multiple authentication keys, each of which is valid within different time periods. When a key becomes valid, the authentication algorithm corresponding to the key is used, and packets passing the authentication will be sent or received.

If a key for packet sending is not configured in a keychain or no key for packet sending is valid within a certain period, protocol packets cannot be authenticated and encrypted. As a result, protocol packet transmission fails. To address such a problem, configure a default key for packet sending. If no key is valid, the default key for packet sending is used.

Precautions

Each keychain can have only one default key for packet sending.

- If the default key for packet sending is an existing key, the authentication and encryption algorithms, and key corresponding to the key are used.
- If the default key for packet sending is a newly created key, configure the authentication and encryption algorithms.

Example

Configure the key-1 as default send key in keychain test.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] key-id 1
[HUAWEI-keychain-test-keyid-1] default send-key-id
```

14.15.4 display keychain

Function

The **display keychain** command displays the configuration of a specified keychain.

Format

display keychain *keychain-name* [**key-id** *key-id*]

Parameters

Parameter	Description	Value
keychain-name	Displays the configuration of a keychain with a specified name.	The keychain must already exist.

Parameter	Description	Value
key-id *key-id*	Displays the configuration of a specified key in the keychain.	The key must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To troubleshoot a keychain authentication failure or collect required information before configuration, run the **display keychain** command to view configurations of a specified keychain.

Example

Display the configuration of keychain **test** when no key ID is configured for the keychain.

```
<HUAWEI> display keychain test
 Keychain Information:
 ---------------------
 Keychain Name              : test
   Timer Mode               : Absolute
   Time Type                : Lmt
   Receive Tolerance(min)   : 0
   TCP Kind                 : 254
   TCP Algorithm IDs        :
     HMAC-MD5               : 5
     HMAC-SHA1-12           : 2
     HMAC-SHA1-20           : 6
     HMAC-SHA-256           : 7
     SHA-256                : 8
     MD5                    : 3
     SHA1                   : 4
 Number of Key IDs          : 0
 Active Send Key ID         : None
 Active Receive Key IDs     : None
 Default send Key ID        : Not configured
```

Display the configuration of keychain **test** when a key ID is configured for the keychain.

```
<HUAWEI> display keychain test
 Keychain Information:
 ---------------------
 Keychain Name              : test
   Timer Mode               : Absolute
   Time Type                : Lmt
   Receive Tolerance(min)   : 100
   TCP Kind                 : 182
   TCP Algorithm IDs        :
     HMAC-MD5               : 5
     HMAC-SHA1-12           : 2
     HMAC-SHA1-20           : 6
```

```
    HMAC-SHA-256          : 7
    SHA-256               : 8
    MD5                   : 3
    SHA1                  : 4
 Number of Key IDs         : 1
 Active Send Key ID        : 1
 Active Receive Key IDs    : 01
 Default send Key ID       : 1

 Key ID Information:
 -------------------
 Key ID                   : 1
   Key string              : ******
   Algorithm               : MD5
   SEND TIMER              :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
   RECEIVE TIMER           :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active

 Key ID                   : 2
   Key string              : -
   Algorithm               : -
   SEND TIMER              :
     Status                : Inactive
   RECEIVE TIMER           :
     Status                : Inactive
```

Display the configuration of key-id 1 in the keychain **test**.

```
<HUAWEI> display keychain test key-id 1
 Keychain Information:
 ---------------------
 Keychain Name             : test
   Timer Mode              : Absolute
   Time Type               : Lmt
   Receive Tolerance(min)  : 100
   TCP Kind                : 182
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     HMAC-SHA-256          : 7
     SHA-256               : 8
     MD5                   : 3
     SHA1                  : 4

 Key ID Information:
 -------------------
 Key ID                   : 1
   Key string              : ******
   Algorithm               : MD5
   SEND TIMER              :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
   RECEIVE TIMER           :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
   DEFAULT SEND KEY ID INFORMATION
     Default               : Configured
     Status                : Inactive
```

Table 14-89 Description of the display keychain command output

Item	Description
Keychain Name	Name of a keychain. To set the keychain name, run the **keychain** command.
Timer Mode	Time mode of a keychain. ● Absolute: The keychain takes effect in an absolute time range. ● Daily periodic: The keychain is valid on a daily basis. ● Weekly periodic: The keychain is valid on a weekly basis. ● Monthly periodic: The keychain is valid on a monthly basis. ● Yearly periodic: The keychain is valid on a yearly basis. To set the time mode, run the **keychain** command.
Time Type	Specifies the timing type of the keychain.
Receive Tolerance(min)	Receive tolerance time configured for a keychain. To set the receive tolerance time, run the **receive-tolerance** command.
TCP Kind	TCP kind value configured for a keychain. To set the TCP kind value, run the **tcp-kind** command.

Item	Description
TCP Algorithm IDs	TCP algorithm ID configured for a keychain. The characteristics of each authentication algorithm are as follows: ● MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length. ● SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. Then, 0s are added to make up a 512-bit message. ● HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. ● HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. ● SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code. ● SM3: The 256-bit SM3 message digest is calculated based on the entered message of any length. All the 256 bits are used as the authentication code. To set the TCP algorithm ID, run the **tcp-algorithm-id** command.
Number of Key IDs	Number of key IDs.
Active Send Key ID	ID of the active send key.

Item	Description
Active Receive Key IDs	ID of the active receive key.
Default send Key ID	ID of the default send key.
Key ID	Key configured in a keychain. To set the key ID, run the **key-id** command.
Key string	Key string configured for the key. To set the key string, run the **key-string** command.

Item	Description
Algorithm	Algorithm configured for the key. To set the algorithm for a key, run the **algorithm** command. The characteristics of each authentication algorithm are as follows: ● MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length. ● SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. Then, 0s are added to make up a 512-bit message. ● HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. ● HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. ● SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code. ● SM3: The 256-bit SM3 message digest is calculated based on the entered message of any length. All the 256 bits are used as the authentication code.

Item	Description
SEND TIMER	Send time of a key. To set the send time of a key, run the **send-time** command.
Start time	Time when a key becomes valid.
End time	Time when a key becomes invalid.
Status	Status of send/receive keys: ● Active ● Inactive
RECEIVE TIMER	Receive time of a key. To set the receive time of a key, run the **receive-time** command.
DEFAULT SEND KEY ID INFORMATION	Information about the default send key.
Default	Configuration of the default send key: ● Not configured ● Configured
Status	Status of the default send key: ● Active ● Inactive

14.15.5 keychain

Function

The **keychain** command creates a new set of keychain rules or displays the keychain view.

The **undo keychain** command deletes the keychain configuration.

By default, no keychain is configured.

Format

keychain *keychain-name* { **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } } }

undo keychain *keychain-name*

Parameters

Parameter	Description	Value
keychain-name	Specifies the keychain name. All the applications identify the set of keychain rules by keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
mode	Indicates the time mode of a keychain. **NOTE** ● The time mode of a keychain must be specified when a keychain is created. ● You do not need to specify the time mode for a created keychain.	-
absolute	Indicates that the given keychain is non-periodic.	-
periodic	Indicates that the given keychain is periodic.	-
daily	Indicates that the given keychain is day-periodic.	-
weekly	Indicates that the given keychain is week-periodic.	-
monthly	Indicates that the given keychain is month-periodic.	-
yearly	Indicates that the given keychain is year-periodic.	-

Views

System view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

There are two keychain time modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

Follow-up Procedure

Run the **key-id** command to configure a key. If the key is not configured, the keychain cannot authenticate and encrypt protocol packets.

The time mode of a key must be the same as the time mode of the keychain.

Precautions

A keychain supports a maximum of 64 keys.

The **keychain** *keychain-name* command displays a specific keychain view. If the keychain specified by *keychain-name* does not exist, the **keychain** *keychain-name* command cannot be executed. To create a keychain, run the **keychain** *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } } command.

Example

Configure the keychain **test** and enter keychain view.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test]
```

14.15.6 key-id

Function

The **key-id** command creates a new set of key-ids or displays the key-id view.

The **undo key-id** command deletes the key-id configuration.

By default, no key-id is configured.

Format

key-id *key-id*

undo key-id *key-id*

Parameters

Parameter	Description	Value
key-id	Specifies the key identification number of a keychain.	The integer value ranges from 0 to 63.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key string dynamically. This can reduce the workload of manually changing the algorithm and key.

The dynamic change of the keychain authentication algorithm is implemented based on the keys. Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Follow-up Procedure

After key-id is specified, perform the following operations:

- Run the **algorithm** command to configure an algorithm used by the key.
- Run the **key-string** command to specify a key string.
- Run the **send-time** command to specify the send time of the key.
- Run the **receive-time** command to specify the receive time of the key.

Precautions

A **key-id** represents a key on the device.

A keychain supports 64 keys, but only one key takes effect during one period.

No active key can be used to authenticate and encrypt protocol packets at the intervals of keys. Therefore, run the **default send-key-id** command to specify a default key.

The time mode of the key must be the same as the time mode of Keychain.

Example

Configure key-id 1.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
```

```
[HUAWEI-keychain-test] key-id 1
[HUAWEI-keychain-test-keyid-1]
```

14.15.7 key-string

Function

The **key-string** command specifies a key used for keychain authentication.

The **undo key-string** command deletes a key used for keychain authentication.

By default, no key is configured for keychain authentication.

Format

key-string { **plain** *plain-text* | [**cipher**] *cipher-text* }

undo key-string

Parameters

Parameter	Description	Value
plain *plain-text*	Indicates the plain text used for authentication. The configured text will be stored as unencrypted text and displayed as unencrypted text. **NOTE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is case-sensitive and ranges from 1 to 255 characters. Spaces are not supported. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.
cipher	Specifies the cipher key string used for encryption and decryption.	-

Parameter	Description	Value
cipher-text	Indicates the cipher text used for authentication.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 255 characters in plaintext or a string of 20 to 392 characters in ciphertext. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Precautions

An authentication key configured in cipher text mode will be also displayed in cipher text mode. Therefore, remember the plaintext key string when configuring the key in cipher text mode.

If the authentication key is not configured, the corresponding key remains in inactive state.

Example

Configure the key string **test@1234**.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] key-id 1
[HUAWEI-keychain-test-keyid-1] key-string cipher test@1234
```

14.15.8 receive-time

Function

The **receive-time** command configures a key as a receive key for the specified interval of time.

The **undo receive-time** command deletes the receive time configuration.

By default, no receive time is configured.

Format

receive-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

receive-time daily *start-time* **to** *end-time*

receive-time day { *start-day-name* **to** *end-day-name* | *day-name* &<1-7> }

receive-time date { *start-date-value* **to** *end-date-value* | *date-value* &<1-31> }

receive-time month { *start-month-name* **to** *end-month-name* | *month-name* &<1-12> }

undo receive-time

Parameters

Parameter	Description	Value
start-time	Specifies the start receive time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specifies the start date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the receive time in minutes.	The value ranges from 1 to 26280000.
infinite	Indicates that the key will be acting as an active receive key forever from the configured start time.	-
to	Indicates a separator.	-

Parameter	Description	Value
end-time	Specifies the end receive time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start time.
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily receive time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end receive day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end receive date of the month.	The value ranges from 2 to 31. The end date must be later than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-

Parameter	Description	Value
start-month-name	Specifies the month of the year to be configured as the start receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
end-month-name	Specifies the end receive month. The end month must be greater than the start month.	The end month must be later than the start month. It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
month-name &<1-12>	Specifies the month of the year to be configured as the receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different keys for packet sending and receiving to be valid within different time periods.

When the system time is within the specified interval, the receive key is in active state.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which receive keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys can be active at the same time. The device will select a key for decryption based on the received packet.

Example

Configure the time for packet receiving with the timing mode as absolute and range as infinite.

```
<HUAWEI> system-view
[HUAWEI] keychain one mode absolute
[HUAWEI-keychain-one] key-id 5
[HUAWEI-keychain-one-keyid-5] receive-time 14:52 2014-11-1 duration infinite
```

Configure the time for packet receiving with the timing mode as absolute.

```
<HUAWEI> system-view
[HUAWEI] keychain two mode absolute
[HUAWEI-keychain-two] key-id 5
[HUAWEI-keychain-two-keyid-5] receive-time 14:52 2014-11-1 to 14:52 2040-10-1
```

Configure the time for packet receiving with the timing mode as daily periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain three mode periodic daily
[HUAWEI-keychain-three] key-id 5
[HUAWEI-keychain-three-keyid-5] receive-time daily 14:52 to 18:10
```

Configure the time for packet receiving with the timing mode as weekly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain four mode periodic weekly
[HUAWEI-keychain-four] key-id 5
[HUAWEI-keychain-four-keyid-5] receive-time day mon
```

Configure the time for packet receiving with the timing mode as monthly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain five mode periodic monthly
[HUAWEI-keychain-five] key-id 5
[HUAWEI-keychain-five-keyid-5] receive-time date 12 to 25
```

Configure the time for packet receiving with the timing mode as yearly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain six mode periodic yearly
[HUAWEI-keychain-six] key-id 5
[HUAWEI-keychain-six-keyid-5] receive-time month oct to dec
```

14.15.9 receive-tolerance

Function

The **receive-tolerance** command sets receive tolerance for all the receive keys in the keychain.

The **undo receive-tolerance** command deletes the receive tolerance configuration.

By default, no receive tolerance is configured.

Format

receive-tolerance { *value* | **infinite** }

undo receive-tolerance

Parameters

Parameter	Description	Value
value	Specifies the receive tolerance value for a keychain.	The integer value ranges from 1 to 14400 in minutes.
infinite	Indicates that the receive tolerance is infinite. That is, the receive key is always valid.	-

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key string dynamically. Each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm is used.

Due to the networking environment or clock asynchronization on the packet sender and receiver, packets may be delayed. The receiver may receive a packet sent from the sender after its key for packet receiving becomes invalid. As a result, the receiver discards the packet and packet transmission is interrupted. To address this problem, set a tolerance time to ensure that the validity period of the receive key on the receiver expires after all packets sent from the sender reach the receiver.

Implementation Procedure

After a tolerance time is set, the tolerance time is added to the start time and end time when the key ID for packet receiving becomes valid.

Precautions

A tolerance time is required for each keychain. The configured tolerance time takes effect for all keys in the keychain.

Example

Configure the receive tolerance time as 570 minutes.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] receive-tolerance 570
```

14.15.10 send-time

Function

The **send-time** command configures a key as a send key at a specified interval.

The **undo send-time** command deletes the send time configuration.

By default, no send-time is configured.

Format

send-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

send-time daily *start-time* **to** *end-time*

send-time day { *start-day-name* **to** *end-day-name* | *day-name* &<1-7> }

send-time date { *start-date-value* **to** *end-date-value* | *date-value* &<1-31> }

send-time month { *start-month-name* **to** *end-month-name* | *month-name* &<1-12> }

undo send-time

Parameters

Parameter	Description	Value
start-time	Specifies the start send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specify the start date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the send time, in minutes.	The value ranges from 1 to 26280000.
infinite	Indicates that the key will act as a send key forever from the configured start time.	-
to	Indicates a separator.	-
end-time	Specifies the end send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start time.

Parameter	Description	Value
end-date	Specifies the end date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily send time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end send day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end date of the month to be configured as the send date for the given key.	The value ranges from 2 to 31. The end date must be greater than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-
start-month-name	Specifies the month of the year to be configured as the start send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

Parameter	Description	Value
end-month-name	Specifies the end send month. The end month must be greater than the start month.	It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. The end month must be later than the start month.
month-name &<1-12>	Specifies the month of the year to be configured as the send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different send and receive keys to be valid within different time periods.

When the system is within the send time range of the key, the device will use the algorithm and key of the configured key to encrypt the packet.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which send keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys cannot be active at the same time. Only one key takes effect during a period in a keychain.

Example

Configure the time for packet sending with the timing mode as absolute.

```
<HUAWEI> system-view
[HUAWEI] keychain one mode absolute
[HUAWEI-keychain-one] key-id 5
[HUAWEI-keychain-one-keyid-5] send-time 14:52 2014-11-1 to 14:52 2040-10-1
```

Configure the time for packet sending with the timing mode as daily periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain two mode periodic daily
[HUAWEI-keychain-two] key-id 5
[HUAWEI-keychain-two-keyid-5] send-time daily 14:52 to 18:10
```

Configure the time for packet sending with the timing mode as weekly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain three mode periodic weekly
[HUAWEI-keychain-three] key-id 5
[HUAWEI-keychain-three-keyid-5] send-time day mon
```

Configure the time for packet sending with the timing mode as monthly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain four mode periodic monthly
[HUAWEI-keychain-four] key-id 5
[HUAWEI-keychain-four-keyid-5] send-time date 12
```

Configure the time for packet sending with the timing mode as yearly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain five mode periodic yearly
[HUAWEI-keychain-five] key-id 5
[HUAWEI-keychain-five-keyid-5] send-time month apr
```

Configure the time for packet sending with the timing mode as yearly periodic, and a few months are available.

```
<HUAWEI> system-view
[HUAWEI] keychain six mode periodic yearly
[HUAWEI-keychain-six] key-id 5
[HUAWEI-keychain-six-keyid-5] send-time month oct to dec
```

14.15.11 tcp-algorithm-id

Function

The **tcp-algorithm-id** command specifies an algorithm ID to represent a TCP authentication algorithm supported by the keychain.

The **undo tcp-algorithm-id** command restores the default settings.

By default, mapping between the TCP authentication algorithm and algorithm ID supported by IANA is used.

Format

tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** } *algorithm-id*

undo tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** }

Parameters

Parameter	Description	Value
hmac-md5	Specifies the HMAC-MD5 authentication algorithm.	-
hmac-sha-256	Specifies the HMAC-SHA-256 authentication algorithm.	-
hmac-sha1-12	Specifies the HMAC-SHA1-12 authentication algorithm.	-
hmac-sha1-20	Specifies the HMAC-SHA1-20 authentication algorithm.	-
md5	Specifies the MD5 authentication algorithm.	-
sha-1	Specifies the SHA-1 authentication algorithm.	-
sha-256	Specifies the SHA-256 authentication algorithm.	-
algorithm-id	Specifies the algorithm ID to represent a TCP authentication algorithm.	The value ranges from 1 to 63. Default algorithm IDs for algorithm types are: **md5** is 3, **hmac-sha-256** is 7, **hmac-md5** is 5, **hmac-sha1-12** is 2, **hmac-sha1-20** is 6 and **sha-256** is 8.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

The TCP connection is authenticated using the authentication algorithm specified by the algorithm ID. The algorithm ID is not defined by IANA. Different vendors use different algorithm IDs to identify authentication algorithms. When two devices of different vendors are connected, ensure that algorithm IDs configured on the two devices are the same.

The characteristics of each authentication algorithm are as follows:

- MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length.
- SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. Then, 0s are added to make up a 512-bit message.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.
- SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code.
- SM3: The 256-bit SM3 message digest is calculated based on the entered message of any length. All the 256 bits are used as the authentication code.

Prerequisites

Before configuring algorithm IDs for the communicating parties, run the **tcp-kind** command to configure TCP types for the communicating parties.

Precautions

SHA-1 has low security, for higher security purposes, you are advised to specify the **hmac-sha-256** or **sha2-256** parameter.

Each algorithm has a unique algorithm ID. And the algorithm IDs configured for the two communication devices must be identical.

Example

Specify 1 as the algorithm ID of **hmac-sha-256**.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] tcp-algorithm-id hmac-sha-256 1
```

14.15.12 tcp-kind

Function

The **tcp-kind** command specifies the option type in the TCP enhanced authentication option.

The **undo tcp-kind** command restores the default TCP kind value.

By default, the default kind value is 254.

Format

tcp-kind *kind-value*

undo tcp-kind

Parameters

Parameter	Description	Value
kind-value	Specifies the TCP kind value to be used for that keychain.	The value ranges from 28 to 255.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

TCP connection request packets carry enhanced authentication options and are authenticated by a specified authentication algorithm. Different vendors use different kind values to specify the enhanced authentication option. Kind values configured for the communicating parties must be the same.

Follow-up Procedure

After configuring the same TCP kind value for the communicating parties, run the **tcp-algorithm-id** command to specify TCP algorithm IDs for the communicating parties.

Precautions

Communicating parties using the keychain authentication must establish a TCP connection when configuring the kind value. Otherwise, the TCP authentication does not take effect.

If TCP connection request packets carry enhanced authentication options, the kind value must be specified in the packets.

Example

Configure the TCP kind value as 252 for the keychain **test**.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] tcp-kind 252
```

14.15.13 time mode

Function

The **time mode** command configures the time mode for Keychain.

The **undo time mode** command restores the default time mode for Keychain.

By default, the time mode of Keychain is Local Mean Time (LMT).

Format

time mode { **utc** | **lmt** }

undo time mode

Parameters

Parameter	Description	Value
utc	Specifies that the configured time is in Universal Time Coordinated (UTC) format.	-
lmt	Specifies that the configured time is in LMT format.	-

Views

Keychain view

Default Level

2: Configuration level

Usage Guidelines

Each keychain consists of multiple key IDs that are valid within different time periods and each key ID is configured with an authentication algorithm. When a key ID becomes valid, the corresponding authentication algorithm is used, ensuring the dynamic change of authentication algorithms. Configure different key IDs for packet sending and receiving to be valid within different time periods.

To configure the time mode for Keychain, run the **time mode** command. You can configure UTC or LMT for Keychain based on the network planning. Ensure that the time mode remains the same on the entire network.

Example

Configure the time mode for Keychain as UTC.

```
<HUAWEI> system-view
[HUAWEI] keychain test mode absolute
[HUAWEI-keychain-test] time mode utc
```

14.16 MPAC Configuration Commands

14.16.1 Command Support

Only the following switch models support MPAC:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

14.16.2 description (MPAC policy)

Function

The **description** command configures the description for an MPAC policy.

The **undo description** command deletes the description of an MPAC policy.

By default, an MPAC policy does not have a description.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an MPAC policy.	The value is a string of 1 to 255 case-sensitive characters with spaces supported.

Views

MPAC policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure description for a created MPAC policy, use the **description** command. The descriptions facilitate MPAC policy management on the device.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Example

Configure a description for an MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test
[HUAWEI-service-sec-test] description SwitchA-GE0/0/1 to SwitchB-GE0/0/1
```

14.16.3 display service-security binding

Function

The **display service-security binding** command displays the MPAC policies bound to an interface or bound globally.

Format

display service-security binding { **ipv4** | **ipv6** } [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ipv4	Indicates the IPv4 MPAC policy.	-
ipv6	Indicates the IPv6 MPAC policy.	-
interface *interface-type interface-number*	Indicates the interface to which MPAC policies are bound.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check information about bound MPAC policies, run this command.

The **display service-security binding** { **ipv4** | **ipv6** } command displays all MPAC policies bound to interfaces and bound globally.

The **display service-security binding** { **ipv4** | **ipv6** } **interface** *interface-type interface-number* command displays the MPAC policies bound to a specified interface.

Example

Display all IPv4 MPAC policies bound on the device.

```
<HUAWEI> display service-security binding ipv4
Configured  : Global
Policy Name : test

Interface  : GigabitEthernet0/0/1
Policy Name: A1

Interface  : Eth-Trunk1
Policy Name: A2
```

Display the IPv4 MPAC policies bound to GE0/0/1.

```
<HUAWEI> display service-security binding ipv4 interface GigabitEthernet 0/0/1
Interface  : GigabitEthernet0/0/1
Policy Name: A1
```

Table 14-90 Description of the display service-security binding command output

Item	Description
Configured	The MPAC policy bound globally. This field has a fixed value of **Global**. If no MPAC policy is bound globally, this field is not displayed.
Interface	Interface to which MPAC policies are bound.
Policy Name	Name of an MPAC policy.

14.16.4 display service-security policy

Function

The **display service-security policy** command displays MPAC policy configurations.

Format

display service-security policy { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Displays the specified IPv4 MPAC policy.	-
ipv6	Displays the specified IPv6 MPAC policy.	-
security-policy-name	Specifies the name of an MPAC policy to be displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An MPAC policy protects device security by controlling the packets destined for the CPUs.

To check the MPAC rules, step, and description configured on a device, run the **display service-security policy** command.

Example

Display all IPv4 MPAC policy configurations on a device.

```
<HUAWEI> display service-security policy ipv4
Policy Name : A1
Step        : 5

Policy Name : test
Description : RouterA-GE0/0/1 to ROUTERB-GE0/0/1
Step        : 5
 rule 5 permit protocol udp source-port 3503
```

Display the configuration of the IPv4 MPAC policy **test**.

```
<HUAWEI> display service-security policy ipv4 test
Policy Name : test
Step        : 5
 rule 5 permit protocol tcp source-ip 127.1.1.1 0 source-port 1000
 rule 10 permit protocol ip source-ip 10.10.1.0 0.0.0.255
```

Table 14-91 Description of the display service-security policy command output

Item	Description
Policy Name	Name of an MPAC policy.
Description	Description of an MPAC policy.
Step	Step between two MPAC rule IDs.
rule	MPAC rules.

14.16.5 display service-security statistics

Function

The **display service-security statistics** command displays statistics about matched rules in MPAC policies.

Format

display service-security statistics { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Displays statistics about matched rules in IPv4 MPAC policy.	-
ipv6	Displays statistics about matched rules in IPv6 MPAC policy.	-
security-policy-name	Indicates the name of an MPAC policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An MPAC policy protects device security by controlling the packets destined for the CPUs.

The **display service-security statistics** command displays MPAC policy information and how many times MPAC rules are matched.

Example

Display statistics about matched rules in all IPv4 MPAC policies.

```
<HUAWEI> display service-security statistics ipv4
Policy Name : A1
Step        : 5

Policy Name : beijing
Description : mpac policy for ipv4
Step        : 2
 rule 2 permit protocol any (0 times matched)
 rule 4 deny protocol any (0 times matched)
 rule 6 permit protocol bgp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (1 times matched)
 rule 12 permit protocol ftp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 14 permit protocol ip source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 16 permit protocol ldp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 20 permit protocol ntp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 22 permit protocol ospf source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 24 permit protocol rip source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 26 permit protocol rsvp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 28 permit protocol snmp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 30 permit protocol ssh source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 32 permit protocol tcp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 34 permit protocol telnet source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 36 permit protocol tftp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 38 permit protocol udp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)

Policy Name : test
Step        : 5
 rule 5 permit protocol tcp source-ip 127.1.1.1 0 source-port 1000 (10 times matched)
 rule 10 permit protocol ip source-ip 10.10.1.0 0.0.0.255 (1 times matched)
```

Display statistics about matched rules in the IPv4 MPAC policy named **test**.

```
<HUAWEI> display service-security statistics ipv4 test
Policy Name : test
Step        : 5
 rule 5 permit protocol tcp source-ip 127.1.1.1 0 source-port 1000 (10 times matched)
 rule 10 permit protocol ip source-ip 10.10.1.0 0.0.0.255 (1 times matched)
```

Table 14-92 Description of the display service-security statistics command output

Item	Description
Policy Name	Name of an MPAC policy.
Description	Description of an MPAC policy.
Step	Step between two MPAC rule IDs.
rule	MPAC rules.
(0 times matched)	Number of times the MPAC rules are matched.

14.16.6 reset service-security counters

Function

The **reset service-security counters** command deletes MPAC policy statistics.

Format

reset service-security counters { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Deletes IPv4 MPAC policy statistics.	-
ipv6	Deletes IPv6 MPAC policy statistics.	-
security-policy-name	Specifies the name of an MPAC policy to be deleted.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If excess MPAC policy statistics are generated on a device and you want to view new MPAC information, run the **reset service-security counters** to delete the existing statistics first.

With the *security-policy-name* parameter specified, you can delete statistics about the specified IPv4 or IPv6 MPAC policy. Without the *security-policy-name* parameter specified, you can delete statistics about all IPv4 or IPv6 MPAC policies.

Precautions

All existing MPAC policy statistics will be deleted after this command is executed.

Example

Delete statistics about the IPv4 MPAC policy **test**.

```
<HUAWEI> reset service-security counters ipv4 test
```

14.16.7 rule (MPAC policy)

Function

The **rule** command adds a rule to the MPAC policy view.

The **undo rule** command deletes a rule or some configurations from the MPAC policy view.

By default, an MPAC policy does not have a rule.

Format

rule [*rule-id*] { **permit** | **deny** } **protocol** { *protocol-number* | **ftp** | **ssh** | **snmp** | **telnet** | **tftp** | **bgp** | **ldp** | **rsvp** | **ospf** | **rip** | **ntp** | **lsp-ping** | **dhcp-c** | **dhcp-r** | **ip** } [[**source-ip** { *source-ipv4-address* { *source-ipv4-mask* | 0 } | **any** }] | [**destination-ip** { *destination-ipv4-address* { *destination-ipv4-mask* | 0 } | **any** }]] *

rule [*rule-id*] { **permit** | **deny** } **protocol** { **tcp** | *tcp-protocol-number* | **udp** | *udp-protocol-number* } [[**source-port** *source-port-number*] | [**destination-port** *destination-port-number*] | [**source-ip** { *source-ipv4-address* { *source-ipv4-mask* | 0 } | **any** }] | [**destination-ip** { *destination-ipv4-address* { *destination-ipv4-mask* | 0 } | **any** }]] *

rule [*rule-id*] { **deny** | **permit** } **protocol** { **any** | **isis** }

rule [*rule-id*] { **permit** | **deny** } **protocol** { *protocol-number* | **ftp** | **ssh** | **snmp** | **telnet** | **tftp** | **bgp** | **ldp** | **rsvp** | **ospf** | **rip** | **ntp** | **lsp-ping** | **dhcp-c** | **dhcp-r** | **ip** } [[**source-ip** { *source-ipv6-address source-ipv6-prefix-length* | *source-ipv6-address/prefix-length* | **any** }] | [**destination-ip** { *destination-ipv6-address destination-ipv6-prefix-length* | *destination-ipv6-address/prefix-length* | **any** }]] *

rule [*rule-id*] { **permit** | **deny** } **protocol** { **tcp** | *tcp-protocol-number* | **udp** | *udp-protocol-number* } [[**source-port** *source-port-number*] | [**destination-port** *destination-port-number*] | [**source-ip** { *source-ipv6-address source-ipv6-prefix-length* | *source-ipv6-address/prefix-length* | **any** }] | [**destination-ip** { *destination-ipv6-address destination-ipv6-prefix-length* | *destination-ipv6-address/prefix-length* | **any** }]] *

undo rule *rule-id* [**source-ip** | **destination-ip** | **source-port** | **destination-port**] *

Parameters

Parameter	Description	Value
rule-id	Indicates the MPAC rule ID.	The value is an integer that ranges from 0 to 4294967294.

Parameter	Description	Value
deny	Prevents protocol packets matching the rules from being sent to the CPU.	-
permit	Allows the protocol packets matching the rules to be sent to the CPU.	-
protocol	Specifies the protocol name or number.	-
tcp	Indicates the Transmission Control Protocol (TCP).	-
tcp-protocol-number	Indicates the TCP protocol number.	It has a fixed value of 6.
udp	Indicates the User Datagram Protocol (UDP).	-
udp-protocol-number	Indicates the UDP protocol number.	It has a fixed value of 17.
source-port *source-port-number*	Specifies the source port number of protocol packets.	The value is an integer that ranges from 1 to 65535.
destination-port *destination-port-number*	Specifies the destination port number of protocol packets.	The value is an integer that ranges from 1 to 65535.
protocol-number	Specifies a protocol number.	The value is an integer that ranges from 1 to 255.
ftp	Indicates the File Transfer Protocol (FTP).	-
ssh	Indicates the Secure Shell (SSH) protocol.	-
snmp	Indicates the Simple Network Management Protocol (SNMP).	-
telnet	Indicates the Telnet protocol.	-
tftp	Indicates the Trivial File Transfer Protocol (TFTP).	-

Parameter	Description	Value
bgp	Indicates the Border Gateway Protocol (BGP).	-
ldp	Indicates the Label Distribution Protocol (LDP).	-
rsvp	Indicates the Resource Reservation Protocol (RSVP).	-
ospf	Indicates the Open Shortest Path First (OSPF) protocol.	-
rip	Indicates the Routing Information Protocol (RIP).	-
ntp	Indicates the Network Time Protocol (NTP).	-
lsp-ping	Indicates the Label Switched Path (LSP)-PING protocol.	-
dhcp-c	Indicates the Dynamic Host Configuration Protocol-C (DHCP-C) protocol.	-
dhcp-r	Indicates the DHCP-R protocol.	-
ip	Indicates the Internet Protocol (IP).	-
source-ip	Indicates the source address of protocol packets.	-
source-ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
source-ipv4-mask | 0	Specifies the mask of the source IPv4 address. The protocol packets from the specified subnet are allowed to be sent to the CPU or discarded. 0 Specifies the source host name. The protocol packets from the specified host are allowed to be sent to the CPU or discarded.	The value is in dotted decimal notation.
destination-ip	Indicates the destination address of protocol packets.	-
destination-ipv4-address	Specifies a destination IPv4 address.	The value is in dotted decimal notation.
destination-ipv4-mask | 0	Specifies the mask of the destination IPv4 address. The protocol packets destined for the specified subnet are sent to the CPU or discarded. 0 Specifies the destination host name. The protocol packets destined for the specified host are sent to the CPU or discarded.	The value is in dotted decimal notation.
any	Indicates any IP address.	-
isis	Indicates the Intermediate System to Intermediate System (IS-IS) protocol.	-
source-ipv6-address	Specifies a source IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source-ipv6-prefix-length	Specifies the prefix length of a source IPv6 address.	The value is an integer that ranges from 1 to 128.

Parameter	Description	Value
source-ipv6-address/ prefix-length	Specifies the source IPv6 address and prefix length.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X/M. M is an integer that ranges from 1 to 128.
destination-ipv6-address	Specifies a destination IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
destination-ipv6-prefix-length	Specifies the prefix length of a destination IPv6 address.	The value is an integer that ranges from 1 to 128.
destination-ipv6-address/ prefix-length	Specifies the destination IPv6 address and prefix length.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X/M. M is an integer that ranges from 1 to 128.

Views

MPAC policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To match specific users or packets, run the **rule** command with the protocol name or five packet attributes specified.

The MPAC matching rules for TCP/UDP are described in **Table 14-93**.

Table 14-93 Description of the MPAC matching rules for TCP/UDP

Protocol	TCP/UDP	Description
FTP	TCP	The source/destination port number is 21.
SSH	TCP	The source/destination port number is 22.

Protocol	TCP/UDP	Description
Telnet	TCP	The source/destination port number is 23.
BGP	TCP	The source/destination port number is 179.
LDP	TCP/UDP	TCP: The source/destination port number is 646. UDP: The destination port number is 646.
DHCP-R	UDP	IPv4: The destination port number is 67. IPv6: The destination port number is 547.
DHCP-C	UDP	IPv4: The destination port number is 68. IPv6: The destination port number is 546.
NTP	UDP	The destination port number is 123.
SNMP	UDP	The destination port number is 161.
RIP	UDP	IPv4: The destination port number is 520. IPv6: The destination port number is 521.
LSP-PING	UDP	The source/destination port number is 3503.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Precautions

- The MPAC rules configured in the service6-sec policy view do not support ISIS.
- Exercise caution when using the **rule** [*rule-id*] **deny protocol any** command. If this command is executed in the system view, no protocol packets can be sent to the CPU, causing the device to be out of management.
- If a whitelist is configured for an MPAC IPv6 policy, run the **rule permit protocol** *58* command to allow ICMPv6 packets to pass.

Example

Add a rule to an MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test
```

```
[HUAWEI-service-sec-test] rule 5 permit protocol udp source-port 3503 destination-ip 127.0.0.1
255.255.255.255
```

14.16.8 service-security binding

Function

The **service-security binding** command binds an MPAC policy to an interface.

The **undo service-security binding** command unbinds an MPAC policy from an interface.

By default, no MPAC policy is applied to an interface.

Format

service-security binding { **ipv4** | **ipv6** } *security-policy-name*

undo service-security binding { **ipv4** | **ipv6** }

NOTE

The **ipv6** parameter is not supported in the subinterface view.

Parameters

Parameter	Description	Value
ipv4	Binds an IPv4 MPAC policy to an interface.	-
ipv6	Binds an IPv6 MPAC policy to an interface.	-
security-policy-name	Specifies the name of an MPAC policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

Ethernet interface view, Ethernet sub-interface view, GE interface view, MultiGE interface view, MultiGE sub-interface view, GE sub-interface view, XGE interface view, 25GE interface view, XGE sub-interface view, 25GE sub-interface view, 40GE interface view, 40GE sub-interface view, 100GE interface view, 100GE sub-interface view, Eth-Trunk interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some attackers may pose as authorized users to send protocol packets to network devices or control these devices. Such attacks affect network running. You can configure MPAC on network devices to allow the specified protocol packets to be sent to the CPUs or discard these packets, improving device security and reliability.

After an MPAC policy is created, run the **service-security binding** command to bind it to interfaces.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Example

Create an IPv4 MPAC policy and apply it to an interface.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test
[HUAWEI-service-sec-test] rule 5 permit protocol tcp source-port 1000 source-ip 127.1.1.1 0
[HUAWEI-service-sec-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] service-security binding ipv4 test
```

Create an IPv6 MPAC policy and apply it to an interface.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 test1
[HUAWEI-service6-sec-test1] rule 10 deny protocol tcp
[HUAWEI-service6-sec-test1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] service-security binding ipv6 test1
```

14.16.9 service-security global-binding

Function

The **service-security global-binding** command binds an MPAC policy to a device globally.

The **undo service-security global-binding** command unbinds an MPAC policy from a device.

By default, no MPAC policy is globally applied.

Format

service-security global-binding { **ipv4** | **ipv6** } *security-policy-name*

undo service-security global-binding { **ipv4** | **ipv6** }

Parameters

Parameter	Description	Value
ipv4	Binds an IPv4 MPAC policy to a device globally.	-
ipv6	Binds an IPv6 MPAC policy to a device globally.	-
security-policy-name	Specifies the name of an MPAC policy to be bound.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some attackers may pose as authorized users to send protocol packets to network devices or control these devices. Such attacks affect network running. You can configure MPAC on network devices to allow the specified protocol packets to be sent to the CPUs or discard these packets, improving device security and reliability.

After an MPAC policy is created, run the **service-security global-binding** command to bind it to a device globally.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Example

Create an IPv4 MPAC policy and apply it to a device globally.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test
[HUAWEI-service-sec-test] rule 5 permit protocol tcp source-port 1000 source-ip 127.1.1.1 0
[HUAWEI-service-sec-test] quit
[HUAWEI] service-security global-binding ipv4 test
```

Create an IPv6 MPAC policy and apply it to a device globally.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 test1
[HUAWEI-service6-sec-test1] rule 10 deny protocol tcp
[HUAWEI-service6-sec-test1] quit
[HUAWEI] service-security global-binding ipv6 test1
```

14.16.10 service-security policy

Function

The **service-security policy** command creates an MPAC policy and displays its view.

The **undo service-security policy** command deletes an MPAC policy.

By default, no MPAC policy exists on a device.

Format

service-security policy { **ipv4** | **ipv6** } *security-policy-name*

undo service-security policy { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Creates an IPv4 MPAC policy and displays its view.	-
ipv6	Creates an IPv6 MPAC policy and displays its view.	-
security-policy-name	Specifies the name of an MPAC policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Some attackers may pose as authorized users to send protocol packets to network devices or control these devices. Such attacks affect network running. You can configure MPAC on network devices to allow the specified protocol packets to be sent to the CPUs or discard these packets, improving device security and reliability.

Example

Create an IPv4 MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test
[HUAWEI-service-sec-test]
```

Create an IPv6 MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 test1
[HUAWEI-service6-sec-test1]
```

14.16.11 step (MPAC policy)

Function

The **step** command sets the step between two MPAC rule IDs.

The **undo step** command restores the default step between MPAC rule IDs.

By default, the step between two MPAC rule IDs is 5.

Format

step *step-value*

undo step

Parameters

Parameter	Description	Value
step-value	Specifies the step between two MPAC rule IDs.	The value is an integer that ranges from 1 to 20.

Views

MPAC policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A step is an increment between neighboring MPAC rule IDs automatically allocated by the system. For example, if the step is 5, the system allocates MPAC rules with IDs 5, 10, 15, 20...

To allow insertion of new rules, set a step for MPAC rule IDs by using the **step** command.

Prerequisites

MPAC policies have been created using the **service-security policy** command.

Configuration Impact

After you set a step, all the rule IDs in the MPAC policy are re-arranged using the new step.

Precautions

Setting the step only changes rule IDs, but will not change the rule priorities.

Example

Set the step for MPAC rule IDs to 10.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test
[HUAWEI-service-sec-test] step 10
```

14.17 Traffic Isolation Between the Service and Management planes Configuration Commands

14.17.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.17.2 management-plane isolate enable

Function

The **management-plane isolate enable** command enables management plane separation.

The **undo management-plane isolate enable** command disables the function.

By default, management plane separation is enabled.

Format

management-plane isolate enable

undo management-plane isolate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **management-plane isolate enable** command enables separation of the management plane to prevent unauthorized users from attacking the management network through the service network. After the command is run, the switch prevents unauthorized users from accessing the management interface through a service interface. That is, if the destination address of a packet received by a service interface is the management interface address, the user cannot access the switch. The access from the management interface to service interface is not restricted.

Precautions

- Disabling this function may cause the management network port to be attacked. Therefore, you are advised not to disable this function.
- The **management-port isolate enable** and **management-plane isolate enable** command functions are different. The **management-port isolate enable** command isolates traffic between the management and service interfaces by marking the network segment routes with the outbound interfaces being the management interface as the blackhole route, whereas the **management-plane isolate enable** command isolates service interfaces from the management interface by marking the host and broadcast routes with the outbound interfaces being the management interface as the blackhole route.
- When a version earlier than V200R005C02 (except V200R005C00SPC500) is upgraded to V200R005C02, a version later than V200R005C02, or V200R005C00SPC500, the **undo management-plane isolate enable** configuration is automatically generated.

Example

Enables management plane separation.

```
<HUAWEI> system-view
[HUAWEI] management-plane isolate enable
```

14.17.3 management-port isolate enable

Function

The **management-port isolate enable** command isolates management interfaces from service interfaces.

The **undo management-port isolate enable** command disables the function.

By default, management interface separation is enabled.

Format

management-port isolate enable

undo management-port isolate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **management-port isolate enable** command enables separation of the management interface to prevent unauthorized users from attacking the packet forwarding service. After the command is run, the switch forbids packet exchange between the management and service interfaces. That is, the packets received by the management interface will not be sent out through a service interface, and the packets received by a service interface will not be sent out through the management interface.

Precautions

- Disabling this function may cause the management network port to be attacked. Therefore, you are advised not to disable this function.
- For the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, when disabling this function, also run the **arp-miss message-cache disable** command to disable the function of packetizing ARP Miss messages. Otherwise, disabling management interface separation cannot take effect. After management interface separation is disabled, the device needs to send ICMP unreachable and redirection packets, which however cannot be sent when the function of packetizing ARP Miss messages is enabled.
- The interval between management-port isolate enable and undo management-port isolate enable command must be longer than 30 seconds.
- When a version earlier than V200R005C02 (except V200R005C00SPC500) is upgraded to V200R005C02, a version later than V200R005C02, or V200R005C00SPC500, the **undo management-port isolate enable** configuration is automatically generated.

Example

Isolate management interfaces from service interfaces.

```
<HUAWEI> system-view
[HUAWEI] management-port isolate enable
```

14.18 Security Risk Commands

14.18.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.18.2 display security risk

Function

The **display security risk** command displays security risks in the system and suggested solutions for the risks.

Format

display security risk [**trap-info**] [**feature** *feature-name*] [**level** { **high** | **medium** | **low** }]

Parameters

Parameter	Description	Value
trap-info	Displays alarm information of security risk.	-
feature *feature-name*	Displays security risks of a specified feature.	Enumerated type. The value depends on the registered module.
level high	Displays security risks of High level.	-
level medium	Displays security risks of Medium level.	-
level low	Displays security risks of Low level.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Protocols have different security performances, and some protocols may have security risks. Run the **display security risk** command to identify security risks in the system. Then clear the security risks according to the repair action in the command output. For example, if SNMPv1 is configured, the **display security risk** command output will prompt for the use of SNMPv3.

You can filter the security risks by specifying the security level, feature, or both.

Precautions

The security risks that are displayed vary with user levels. The system administrators can view all security risks in the system. Other users can only view the security risks matching their levels.

Example

Display security risks in the system.

```
<HUAWEI> display security risk
Risk level       : high
Feature name     : SNMP
Risk information : SNMPv1/SNMPv2c is enabled.
Repair action    : Use SNMPv3.

Risk level       : high
Feature name     : TELNET
Risk information : None authentication is configured for Telnet
users.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : CONSOLE
Risk information : No authentication is configured, password authentication is configured but no password
is specified, or none auth
entication is configured on the console interface.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : TELNET
Risk information : The Telnet server function is used.
Repair action    : Use Stelnet.
```

Display security risks of the TELNET feature.

```
<HUAWEI> display security risk feature telnet
Risk level       : high
Feature name     : TELNET
Risk information : None authentication is configured for Telnet
users.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : TELNET
Risk information : The Telnet server function is used.
Repair action    : Use Stelnet.
```

Display security risks of Medium level.

```
<HUAWEI> display security risk level medium
Risk level       : medium
Feature name     : CONSOLE
Risk information : No authentication is configured, password authentication is configured but no password
is specified, or none auth
entication is configured on the console interface.
Repair action    : Use AAA authentication.
```

```
Risk level       : medium
Feature name     : TELNET
Risk information : The Telnet server function is used.
Repair action    : Use Stelnet.
```

NOTE

The command output provided here is used for reference only. The actual output information depends on the situation.

Table 14-94 Description of the **display security risk** command output

Item	Description
Risk level	Security risk level. It can be any value of the following: ● high; ● medium; ● low.
Feature name	Feature name.
Risk information	Information about the security risks.
Repair action	Suggested solutions for the security risks.

14.19 PKI Configuration Commands

14.19.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support PKI.

14.19.2 auto-enroll

Function

The **auto-enroll** command enables automatic certificate enrollment and update.

The **undo auto-enroll** command disables automatic certificate enrollment and update.

By default, the automatic certificate enrollment and update are disabled.

Format

auto-enroll [*percent*] [**regenerate** [*key-bit*]] [**updated-effective**]

undo auto-enroll [**updated-effective**]

Parameters

Parameter	Description	Value
percent	Specifies the percentage of the certificate's validity period after which a new certificate is requested automatically.	The value is an integer that ranges from 10 to 100. The default value is 100. When the old certificate expires, the system requests a new certificate.
regenerate	Indicates the RSA key pair will be generated during certificate updates.	-
key-bit	Specifies the number of bits in the RSA key pair generated during certificate updates.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.
updated-effective	Indicates that the certificate takes effect immediately after being updated. By default, an updated certificate takes effect only after the old one expires.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Automatic certificate enrollment: When the certificates are unavailable, will expire, or have expired, an entity automatically requests a new certificate or renews the certificate using the Simple Certification Enrollment Protocol (SCEP).

By default, the automatic certificate enrollment and update function is disabled. When a certificate has expired, you must request a certificate for an entity manually. You can still request a certificate for an entity manually when the automatic certificate enrollment and update function is enabled.

Precautions

- If you do not specify **regenerate**, the system uses the original RSA key pairs during automatic updates.
- If you specify **regenerate**, the system generates new RSA key pairs during certificate updates for certificate requests and overwrites the original certificates and RSA key pairs with the new ones.
- After this command is run, the device checks whether the certificate has expired every 60 minutes. If the certificate has expired, the device updates it.

Example

Enable automatic certificate enrollment and update for the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] auto-enroll 50 regenerate
```

14.19.3 ca id

Function

The **ca id** command specifies a certificate authority (CA) trusted by a PKI realm.

The **undo ca id** command deletes the CA trusted by a PKI realm.

By default, no trusted CA is configured in a PKI realm.

Format

ca id *ca-name*

undo ca id

Parameters

Parameter	Description	Value
ca-name	Specifies the name of a CA trusted by a PKI realm.	The value is a string of 1 to 64 case-sensitive characters.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After the **ca id** command is executed to specify the CA trusted by the device, the device's local certificate is requested, obtained, revoked, or queried through the CA.

Example

Specify the CA **root_ca** trusted by the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] ca id root_ca
```

14.19.4 cdp-url

Function

The **cdp-url** command configures the CRL distribution point (CDP) URL.

The **undo cdp-url** command deletes the configured CDP URL.

By default, no CDP URL is configured.

Format

cdp-url [**esc**] *url-addr*

cdp-url from-ca

undo cdp-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-addr	Specifies the CDP URL.	The value is a string starting with http:// and consisting of 1 to 128 case-sensitive characters without spaces.
from-ca	Specifies that the CDP URL address is obtained from the CA certificate.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity needs to use HTTP to update CRL, it must set up a connection with the HTTP server based on CDP URL, and obtain the CRL from the HTTP server. By default, a PKI entity locates and downloads CRL based on the method (HTTP) in the CDP information of the local certificate. If you do not want to download CRL based on the CDP URL in the local certificate, run this command to configure the PKI entity to obtain CDP URL from the CA certificate or manually configure the CDP URL.

When CRL is automatically updated by SCEP, you can also manually configure a CDP URL address.

Precautions

Manually configuring a CDP URL address overwrites the CDP carried in the certificate. If the certificate does not contain CDP information and no CDP URL address is manually configured, the device requests the CRL from the CA server using SCEP.

Keyword **esc** only supports the URLs that include the question mark (?) in ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\\x3f**.

Example

Set the CDP URL to http://10.1.1.1/certenroll/ca_root.crl.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl scep
[HUAWEI-pki-realm-d1] cdp-url http://10.1.1.1/certenroll/ca_root.crl
```

Set the CDP URL to **http://www.***.com/certenroll/ca_root.crl**.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl scep
[HUAWEI-pki-realm-d1] cdp-url http://www.***.com/certenroll/ca_root.crl
```

14.19.5 certificate-check

Function

The **certificate-check** command sets the method of checking whether a certificate in the PKI realm is revoked.

The **undo certificate-check** command cancels the method of checking whether a certificate in the PKI realm is revoked.

By default, the method of checking whether a certificate in the PKI realm is revoked is **crl**.

Format

certificate-check { { **crl** | **ocsp** } * [**none**] | **none** }

undo certificate-check

NOTE

Only devices in NETCONF mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
crl	Sets the check method to Certificate Revocation List (CRL).	-
ocsp	Sets the check method to Online Certificate Status Protocol (OCSP).	-
none	Indicates that the system does not check whether a certificate is revoked.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the PKI entity validates the peer certificate, for example, whether the peer certificate has expired and whether it is added to CRL. In this case, you can run the **certificate-check** command to check the peer certificate status.

The system supports the following methods to check whether a certificate in the PKI realm is revoked:

- CRL
  - If the CA server can function as a CDP, the certificate issued by CA contains the CDP information about obtaining the certificate CRL. The PKI

entity then uses the specified method (HTTP) to find the CRL from the specified location and download the CRL. If the CDP URL is configured in the PKI realm, the PKI entity obtains the CRL from the specified URL.

  - If the CA does not support CDPs and no CDP URL is configured on the PKI entity, the PKI entity uses the SCEP protocol to obtain the CRL.

- OCSP

  The PKI entity can use OCSP to check certificate status online, and you do not need to frequently download CRLs.

  When two PKI entities use certificates to perform IPsec negotiation, they check the peer certificate status through OCSP in real time.

- None

  This mode is used when no CRL or OCSP server is available to the PKI entity or the PKI entity does not need to check the peer certificate status. In this mode, the PKI entity does not check whether a certificate has been revoked.

Select the following configurations:

- If the **certificate-check crl** command is configured for a certificate, the CRL mode is used.
- If the **certificate-check ocsp** command is configured for a certificate, the OCSP mode is used.
- If the **certificate-check crl none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check crl ocsp** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check ocsp crl** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check crl ocsp none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp crl none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check none** command is configured for a certificate, the certificate is regarded as valid.

Precautions

After the **certificate-check crl** command is configured, if the device does not have the CRL file, the device fails the certificate verification, and the certificate becomes invalid.

If **certificate-check** is set to **none**, the system does not check whether a certificate is revoked, which poses security risks. Therefore, this method is not recommended.

Example

Set the certificate check method to **crl none** in PKI realm **test**. If the CRL mode is unavailable, the certificate is regarded as valid.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] certificate-check crl none
```

14.19.6 certificate auto-update enable

Function

The **certificate auto-update enable** command enables CMPv2-based automatic certificate update.

The **undo certificate auto-update enable** command disables CMPv2-based automatic certificate update.

By default, the CMPv2-based automatic certificate update is disabled.

Format

certificate auto-update enable

undo certificate auto-update enable

Parameters

None

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If a certificate obtained through CMPv2 is about to expire, run this command to enable CMPv2-based automatic certificate update to ensure certificate validity. After the command is executed, the system performs checks (for example, referenced PKI entity, URL for the CMPv2 server, RSA key pair for CMPv2-based certificate application). The configuration is successful only when the conditions are met.

When the system detects that the remaining validity period of the local certificate has reached the value specified in **certificate update expire-time**, the system automatically initiates the certificate update request and decides whether to create an RSA key pair based on the **cmp-request rsa local-key-pair** configuration. After the new certificate is obtained, the system replaces the previous certificate and RSA key pair with the new ones. The replacement files include the files in device storage, certificate in memory, and configuration used in IKE negotiation.

Example

Enable CMPv2-based automatic certificate update.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] certificate auto-update enable
```

14.19.7 certificate update expire-time

Function

The **certificate update expire-time** command specifies when the certificate starts to update. The time is represented by a percentage of the total validity period.

The **undo certificate update expire-time** command restores the default certificate update time.

By default, the certificate is automatically updated when the validity period is only 50% left.

Format

certificate update expire-time *valid-percent*

undo certificate update expire-time

Parameters

Parameter	Description	Value
valid-percent	Specifies the remaining percentage of the validity period.	The value is an integer that ranges from 10 to 100. The default value is 50.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If the automatic certificate update through CMPv2 is enabled, the system sends an update request to the CMPv2 server when the specified updated time is reached.

This command sets the time (percentage of the total validity period) to update the certificate.

Example

Enable the automatic certificate update when the used time is 60% of the validity period of the certificate.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] certificate update expire-time 60
```

14.19.8 cmp-request authentication-cert

Function

The **cmp-request authentication-cert** command configures the certificate for identity authentication in the request through CMPv2.

The **undo cmp-request authentication-cert** command deletes the certificate for identity authentication in the request through CMPv2.

By default, no certificate for identity authentication in the request through CMPv2 is configured.

Format

cmp-request authentication-cert *cert-name*

undo cmp-request authentication-cert

Parameters

Parameter	Description	Value
cert-name	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command to configure the certificate for identity authentication if you need to apply for a certificate through CMPv2. For different requests through CMPv2, the required certificates are as follows:

- For Initialization Requests (IR), the required certificate is an external identity certificate.
- For certification requests (CR), the required certificate is the one that the CA has already issued to the device.
- For the key update requests (KUR), the required certificate is the one that the CA has already issued to the device and is also the one to be updated.

Prerequisites

An identity authentication in the request through CMPv2 exists.

Example

Configure the certificate for identity authentication in the request through CMPv2.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request authentication-cert bb.cer
```

14.19.9 cmp-request ca-name

Function

The **cmp-request ca-name** command sets a CA name for the CMP session.

The **undo cmp-request ca-name** command deletes the CA name of the CMP session.

By default, no CA name is configured for a CMP session.

Format

cmp-request ca-name *ca-name*

undo cmp-request ca-name

Parameters

Parameter	Description	Value
ca-name	Indicates the name of the CA and is the field of subject in the CA certificate.	The value starts and ends with the quotation mark (") and is a string of 1 to 128 characters (including the quotation marks). A comma (,) is used to separate adjacent fields in the string.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

A trusted authority enrolls and issues certificates to entities. Therefore, a trusted CA name must be configured.

The field order in the CA name must be the same as that in the actual CA certificate. Otherwise, the server regards the name as incorrect.

Example

Set the CA name for CMP session **test**.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request ca-name "C=cn,ST=beijing,L=shangdi,O=BB,OU=BB,CN=BB"
```

14.19.10 cmp-request entity

Function

The **cmp-request entity** command sets the entity name used to apply for certificate through CMPv2.

The **undo cmp-request entity** command deletes the entity name used to apply for certificate through CMPv2.

By default, the entity name used to apply for certificate through CMPv2 is not configured.

Format

cmp-request entity *entity-name*

undo cmp-request entity

Parameters

Parameter	Description	Value
entity-name	Specifies the entity name for certificate application through CMPv2.	The value must be an existing PKI entity name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To apply for a certificate through CMPv2, create a CMP session and specify the entity name in the CMP session.

Prerequisites

1. A PKI entity has been created using the **pki entity** command.
2. A PKI entity common name has been created using the **common-name** command.

Precautions

The specified entity can be referenced only by one CMP session or PKI realm.

Example

Set the entity name the device uses when applying for a certificate through CMPv2 to **entity1**.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] common-name test1
[HUAWEI-pki-entity-entity1] quit
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request entity entity1
```

14.19.11 cmp-request message-authentication-code

Function

The **cmp-request message-authentication-code** command configures the reference value and secret value of the message authentication code (MAC).

The **undo cmp-request message-authentication-code** command deletes the reference value and secret value of the MAC.

By default, the reference value and secret value of the MAC are not configured.

Format

cmp-request message-authentication-code *reference-value secret-value*

undo cmp-request message-authentication-code

Parameters

Parameter	Description	Value
reference-value	Specifies the reference value of the MAC.	The value is a string of 1 to 128 case-sensitive characters without spaces and question marks. If the character string is enclosed in double quotation marks, it can contain spaces.

Parameter	Description	Value
secret-value	Specifies the secret value of the MAC.	The length of the plaintext ranges from 1 to 128. The length of the encrypted ciphertext ranges from 48 to 188. The value is a case-sensitive character string without question marks.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

When a device is configured to use MAC for initial request (IR), you need to check the reference value and secret value of the MAC from the CMPv2 server in out-of-band mode, and then run this command to set the values on the device.

Example

Configure the reference value and secret value of the MAC.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request message-authentication-code 1234 YsHsjx_202206
```

14.19.12 cmp-request origin-authentication-method

Function

The **cmp-request origin-authentication-method** command configures the authentication method used for initial request (IR) through CMPv2.

The **undo cmp-request origin-authentication-method** command restores the default authentication method used for IR through CMPv2.

By default, the authentication method used for IR through CMPv2 is MAC.

Format

cmp-request origin-authentication-method { **message-authentication-code** | **signature** }

undo cmp-request origin-authentication-method

Parameters

Parameter	Description	Value
message-authentication-code	Indicates the MAC method for the IR.	-
signature	Indicates the signature method for the IR.	-

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

During the IR using CMPv2, a security protection measure needs to be taken:

- After you select the MAC method, run the **cmp-request message-authentication-code** command to configure the reference value and secret value. The device uses the reference value and secret value to protect messages during the IR.
- After you select the signature method, run the **cmp-request authentication-cert** command to configure the external certificate. The device uses the external certificate to protect signatures during the IR.

Example

Configure the authentication method used for IR through CMPv2.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request origin-authentication-method signature
```

14.19.13 cmp-request realm

Function

The **cmp-request realm** command specifies a PKI realm to which the CMPv2 server certificate belongs.

The **undo cmp-request realm** command deletes the specified PKI realm.

By default, no PKI realm is specified for the CMP server certificate.

Format

cmp-request [**https**] **realm** *realm-name*

undo cmp-request realm

Parameters

Parameter	Description	Value
https	Specifies the communication mode with the CMPv2 server to HTTPS.	-
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The value must be an existing PKI realm name. **NOTE** If the specified PKI realm is the default realm, there may be security risks.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When applying for a certificate through CMPv2, run the **cmp-request realm** command to specify the PKI realm to which the CMPv2 server certificate belongs.

By default, the device uses HTTP to communicate with the CMPv2 server. To improve the security, you can specify **https** to use HTTPS for communication.

Prerequisites

A PKI realm has been created using the **pki realm** command.

Precautions

If the device communicates with the CMPv2 server using HTTPS, the *url-addr* parameter must start with **https://** when the **cmp-request server url** *url-addr* command is to configure the server URL.

Example

Set a PKI realm name of the CMPv2 server certificate to **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request realm abc
```

14.19.14 cmp-request rsa local-key-pair

Function

The **cmp-request rsa local-key-pair** command configures the RSA key pair used for certificate application through CMPv2.

The **undo cmp-request rsa local-key-pair** command deletes the RSA key pair used for certificate application through CMPv2.

By default, the RSA key pair used to apply for certificate through CMPv2 is not configured.

Format

cmp-request rsa local-key-pair *key-name* [**regenerate** [*key-bit*]]

undo cmp-request rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.
regenerate	Indicates that the RSA key pair is updated together with certificate update.	-
key-bit	Specifies the bits of the RSA key pair generated during the certificate update.	The value is an integer that ranges from 3072 to 4096. The default value is 3072. After the WEAKEA plug-in is installed, the value is an integer that ranges from 2048 to 4096. A key of less than 3072 bits has security risks. You are advised to use a key of 3072 bits or more.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CMPv2 is used to apply for a certificate, the certificate request message sent by the PKI entity to CA must contain public key information. Therefore, you need to configure an RSA key pair for certificate application through CMPv2. Note the following during the configuration:

- If **regenerate** is unspecified, the system uses the original RSA key pairs during automatic updates.
- If **regenerate** is specified, the system generates new RSA key pairs during certificate updates for the application for certificates and overwrites the original certificates and RSA key pairs with the new ones.

Prerequisites

The RSA key pair for certificate application has been created using the **pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **pki import rsa-key-pair** command.

Precautions

One RSA key pair can be referenced only by one CMP session.

Example

Configure the RSA key pair to be referenced by CMP session **test** and update the RSA key pair during the certificate update.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:4096
 Generating key-pairs...
........................+++
................................................................................
........+++
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request rsa local-key-pair test regenerate 4096
```

14.19.15 cmp-request server url

Function

The **cmp-request server url** command specifies the URL address of a CMPv2 server.

The **undo cmp-request server url** command deletes the URL address of a CMPv2 server.

By default, the URL of a CMPv2 server is not configured.

Format

cmp-request server url [**esc**] *url-addr*

undo cmp-request server url

Parameters

Parameter	Description	Value
esc	Specifies the entering of URLs in the ASCII code.	-
url-addr	Specifies the URL of the CMPv2 server.	The value is a string starting with **http://** or **https://** and consisting of 1 to 128 case-insensitive characters without spaces.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Configure a URL for the CMPv2 server before certificate application. Then the PKI entity sends a request message to the server's URL. The device can communicate with the server through HTTPS for higher security. In this case, *url-addr* must start with **https://**.

A user cannot enter command lines that include a question mark (?). Therefore, keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\\\x3f**.

Example

Set the URL of the CMPv2 server for CMP session **test** to **http://10.1.1.1:8080**.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request server url http://10.1.1.1:8080
```

Set the URL of the CMPv2 server for CMP session **test** to **http://www.***.com?page1\x3f**.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request server url esc http://www.***.com\x3fpage1\\x3f
```

14.19.16 cmp-request signature-algorithm

Function

The **cmp-request signature-algorithm** command configures a signature algorithm for CMPv2-based certificate application.

The **undo cmp-request signature-algorithm** command restores the default configuration.

By default, the signature algorithm used for CMPv2-based certificate application is SHA-256.

Format

cmp-request signature-algorithm [**sha1** | **sha256**]

undo cmp-request signature-algorithm

NOTE

The system software does not contain the **sha1** parameter. To use this parameter, you need to install the WEAKEA plug-in. However, the SHA-1 algorithm is less secure. For security purposes, you are advised to specify the **sha256** parameter. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Parameters

Parameter	Description	Value
sha1	Specifies the SHA-1 authentication algorithm.	-
sha256	Specifies the SHA-256 authentication algorithm.	-

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When applying for or updating a local certificate for a PKI entity using CMPv2, you can run the **cmp-request signature-algorithm** [**sha1** | **sha256**] command in the CMP session view to change the signature algorithm depending on the support of the CA server.

Precautions

After the system software is upgraded to V200R022C00 or later versions, the default signature algorithm used for CMPv2-based certificate application is SHA-1. However, this algorithm is insecure. For security purposes, you are advised to use the SHA-256 authentication algorithm.

Example

Set the signature algorithm to SHA-256 for CMPv2-based certificate application.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request signature-algorithm sha256
```

14.19.17 cmp-request timeout

Function

The **cmp-request timeout** command sets the timeout interval for communication between the device and CMPv2 server.

The **undo cmp-request timeout** command restores the default setting.

By default, the timeout interval for communication between the device and CMPv2 server is 30 seconds.

Format

cmp-request timeout *timeout*

undo cmp-request timeout

Parameters

Parameter	Description	Value
timeout	Specifies the timeout interval for communication with the CMPv2 server.	The value is an integer in the range from 0 to 60, in seconds. The default value is 30. The value 0 indicates that the communication is always attempted.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If it takes a long time for a device to communicate with the CMPv2 server for applying for a certificate, certificate application resources are occupied. As a result, other CMP sessions fail to obtain certificates. To avoid this, you can run the **cmp-request timeout** *timeout* command to set a proper timeout interval to release certificate application resources in time.

Example

Set the timeout interval for communication between the device and CMPv2 server to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request timeout 10
```

14.19.18 cmp-request verification-cert

Function

The **cmp-request verification-cert** command configures the certificate file for verifying the CA response signature.

The **undo cmp-request verification-cert** command deletes the certificate file for verifying the CA response signature.

By default, no certificate file for verifying the CA response signature is configured.

Format

cmp-request verification-cert *cert-file-name*

undo cmp-request verification-cert

Parameters

Parameter	Description	Value
cert-file-name	Specifies the certificate file name.	The value must be an existing certificate file name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is executed, the device uses the configured certificate to verify the CA response signature. This command configures the CA certificate.

If this command is not executed and the CA response mode is signature, the device constructs a certificate chain based on the certificates in the response messages sent by the device itself and CA to verify the CA response signature. If the MAC mode is set, the device uses the MAC to verify the CA response signature. That is, this command does not take effect.

Prerequisites

The certificate file for verifying the CA response signature exists.

Example

Configure the certificate file for verifying the CA response signature.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] cmp-request verification-cert aa.der
```

14.19.19 common-name

Function

The **common-name** command configures a common name for a PKI entity.

The **undo common-name** command cancels the configuration.

By default, a PKI entity does not have a common name.

Format

common-name *common-name*

undo common-name

Parameters

Parameter	Description	Value
common-name	Specifies the common name of a PKI entity.	The value is a string of 1 to 64 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

After a PKI entity is created, a common name must be configured to uniquely identify the PKI entity.

After the common name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the common name of the PKI entity.

Example

Set the common name to **test** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] common-name test
```

14.19.20 country (PKI entity view)

Function

The **country** command configures a country code for a PKI entity.

The **undo country** command deletes the country code of a PKI entity.

By default, no country code is configured for a PKI entity.

Format

country *country-code*

undo country

Parameters

Parameter	Description	Value
country-code	Specifies the country code of a PKI entity.	A country code must be two-character long. If the entered country code contains lower case letters, the system automatically changes the lower case letters into upper case letters when you create a certificate request file. You can query country codes in ISO3166. For example, CN is the legitimate country code of China, and US is the legitimate country code of the USA.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure the country code for the PKI entity, which is used as an alias of the entity.

After the country code is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this country code. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the country code of the PKI entity.

Example

Configure the country code to CN for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] country CN
```

14.19.21 crl auto-update enable

Function

The **crl auto-update enable** command enables the automatic CRL update function.

The **undo crl auto-update enable** command disables the automatic CRL update function.

By default, automatic CRL update is enabled.

Format

crl auto-update enable

undo crl auto-update enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To configure the automatic CRL update function, enable the function first.

Example

Enable the automatic CRL update function.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl auto-update enable
```

14.19.22 crl cache

Function

The **crl cache** command configures the device to use the cached CRL.

The **undo crl cache** command configures the device to retrieve the latest CRL each time.

By default, the PKI realm is allowed to use cached CRLs.

Format

crl cache

undo crl cache

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The system overwrites the CRL in memory with the cached URL for certificate verification. If the PKI realm is not allowed to use cached CRL, the system must download the latest CRL every time to overwrite the CRL in memory.

Example

Allow the device to use the cached CRL in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] crl cache
```

14.19.23 crl http

Function

The **crl http** command enables automatic CRL update using HTTP.

By default, the CRL is updated automatically using HTTP.

Format

crl http

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using HTTP, and ensure that there is sufficient space in the device storage for the CRL file.

Example

Configure automatic CRL update using HTTP.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl http
```

14.19.24 crl scep

Function

The **crl scep** command configures a device to use SCEP to automatically update a CRL.

By default, a device uses HTTP to automatically update a CRL.

Format

crl scep

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using SCEP, and ensure that there is sufficient space in the device storage for the CRL file.

Example

Use SCEP to automatically update a CRL.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl scep
```

14.19.25 crl update-period

Function

The **crl update-period** command sets the interval for automatic CRL update.

The **undo crl update-period** command restores the default interval for automatic CRL update.

By default, the automatic CRL update interval is 8 hours.

Format

crl update-period *interval*

undo crl update-period

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a CRL is automatically updated.	The value is an integer that ranges from 1 to 720, in hours.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The CRL update interval is the interval at which a PKI entity using a certificate downloads a CRL from the CRL storage server. The CA/RA does not issue the CRL to an entity. Instead, the entity initiates CRL query to obtain a CRL.

Example

Set the interval at which a CRL is automatically updated to 21 hours.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl update-period 21
```

14.19.26 display pki ca-capability

Function

The **display pki ca-capability** command displays the CA capabilities of a PKI realm.

Format

display pki ca-capability realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Indicates the name of a PKI realm.	The PKI realm name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display pki ca-capability** command displays the CA capabilities of a PKI realm.

Example

Display the CA capabilities of the PKI realm **asdf**.

```
<HUAWEI> display pki ca-capability realm asdf
PKI CA Capabilities :
  GetNextCACert      :  ----
  POSTPKIOperation   :  ----
```

```
Renewal           :  ----
SHA-512           :  ----
SHA-256           :  ----
SHA-1             :  ----
DES3              :  ----
```

Table 14-95 Description of the **display pki ca-capability** command output

Item	Description
PKI CA Capabilities	PKI CA capabilities.
GetNextCACert	Get next CA certificate.
POSTPKIOperation	Post PKI operation messages.
Renewal	Certificate renewal.
SHA-512	SHA-512 algorithm.
SHA-256	SHA-256 algorithm.
SHA-1	SHA-1 algorithm.
DES3	DES3 algorithm.

14.19.27 display pki cert-req

Function

The **display pki cert-req** command displays the content of a certificate request file.

Format

display pki cert-req filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate request file.	The certificate request file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays content of a certificate request file, including the subject, public key algorithm, key modulus, attributes, and signature algorithm.

Example

Display the content of a certificate request file named **test.req**.

```
<HUAWEI> display pki cert-req filename test.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:01:cf:95:bb:fb:35:f0:3e:cd:1d:10:9e:11:
                    08:2e:77:48:ba:1b:e6:00:1b:43:30:56:f9:9a:6b:
                    ed:8b:fe:3e:03:57:38:02:48:88:e3:9b:39:d0:1c:
                    2b:8f:6a:9b:91:17:9b:ce:cb:fc:87:40:78:39:08:
                    1c:53:c3:71:cc:db:64:6f:ec:5a:cd:33:a5:68:5e:
                    e6:52:61:ad:a1:58:55:f0:a0:0f:db:ab:05:eb:a4:
                    fe:e1:68:61:8c:af:2c:3a:34:95:d2:41:ee:09:e7:
                    b0:fc:59:d9:f4:12:00:de:ab:14:b6:a3:fe:29:75:
                    f7:dd:7b:aa:03:81:fc:ae:41:8c:e4:ad:e3:d9:65:
                    d4:be:a0:c1:e0:43:8a:91:ad:20:7b:6f:12:25:6e:
                    0d:67:7d:4c:fe:8d:1b:6d:f3:96:07:31:ed:73:d3:
                    71:6b:51:18:64:bd:41:d6:18:2d:2d:86:b7:fa:26:
                    eb:cc:cb:a3:0f:0b:61:22:fd:dd:5f:b4:4d:9b:7d:
                    bc:fa:af:e6:95:d7:27:f1:60:31:56:83:58:2c:40:
                    1a:5e:6a:94:63:aa:70:2f:9b:00:e0:a3:9e:fb:73:
                    62:5e:1c:3c:5f:48:42:7c:26:8f:5f:cf:39:b9:5d:
                    25:90:8e:6c:e0:04:ec:e2:1b:1f:a8:0d:d2:ef:20:
                    41:79
                Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :******
        Requested Extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.1.1.1, DNS:example.com, email:test@example.com
    Signature Algorithm: sha256WithRSAEncryption
         71:e7:c0:5f:36:c9:16:eb:fc:0c:8e:d1:4f:3d:ee:25:6b:47:
         65:86:4b:89:ec:22:01:42:a5:0e:5c:aa:01:0a:57:a9:25:ba:
         1b:59:6d:77:5f:74:80:3b:af:f9:37:75:97:9a:ca:80:73:8b:
         36:14:2c:4b:9a:2f:53:5c:5b:4a:93:31:88:94:0f:4d:58:84:
         36:41:e8:a8:6c:cd:f0:bb:9f:51:50:b2:a4:40:f4:ec:37:c5:
         42:08:69:b5:c5:fd:af:3d:8a:aa:47:53:d3:ce:bc:76:ec:47:
         ca:36:90:0b:49:2b:2f:04:c4:1f:f1:12:b6:99:d0:f8:33:d8:
         08:d0:32:ac:ee:34:0f:07:ef:72:9f:6b:71:80:3e:8d:37:cc:
         ca:b5:c1:56:3d:65:c7:e6:99:1b:2b:53:01:69:f5:8a:18:05:
         d1:b1:48:3e:50:e0:4c:7f:db:dc:b7:cd:a2:37:f9:96:cd:0d:
         ee:61:c2:80:61:6b:99:c0:76:0d:ab:2c:46:ce:b7:aa:6a:12:
         72:b7:6f:64:cc:78:b7:16:bd:c5:32:45:79:42:cf:4c:28:91:
         ce:cd:7d:da:eb:2b:3a:cf:90:1f:61:5e:02:25:fe:3c:82:66:
         d4:e8:c7:f8:5e:84:2c:f6:b2:f0:ba:ee:7a:c1:9b:d4:68:02:
         a4:e3:27:89
```

Table 14-96 Description of the **display pki cert-req** command output

Item	Description
Certificate Request	Information about a certificate request file.

Item	Description
Data	Data of a certificate request file.
Version	Version of a certificate request file.
Subject	Subject of a certificate request file. The subject includes the following attributes: ● C: country code of a PKI entity. It is configured using the **country(PKI entity view)** command. ● ST: name of the state or province to which a PKI entity belongs. It is configured using the **state(PKI entity view)** command. ● L: geographic area where a PKI entity is located. It is configured using the **locality** command. ● O: organization to which a PKI entity belongs. It is configured using the **organization** command. ● OU: department to which a PKI entity belongs. It is configured using the **organization-unit** command. ● CN: common name of a PKI entity. It is configured using the **common-name** command.
Subject Public Key Info	Information about the subject public key of a certificate request file.
Public Key Algorithm	Public key algorithm.
Public-Key	RSA public key. It is configured using the **rsa local-key-pair** command.
Modulus	Key modulus.
Exponent	Key exponent.
Attributes	Attributes of a certificate request file.
challengePassword	The challenge password used in certificate application. It is configured using the **pki enroll-certificate** command.
Requested Extensions	Certificate request extension.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.

Item	Description
IP Address	IP address of a PKI entity. It is configured using the **ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **fqdn** command.
email	Email address of a PKI entity. It is configured using the **email** command.
Signature Algorithm	Signature algorithm. It is configured using the **enrollment-request signature message-digest-method** command.

14.19.28 display pki certificate

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

NOTE

Only devices in NETCONF mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Displays content about the CA certificate.	-
local	Displays content about the local certificate.	-
ocsp	Displays content about the Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the CA certificate, local certificate, and OCSP server's certificate, including signature algorithm, issuer, validity period, subject, and subject public key.

Example

Display information about the CA certificate.

```
<HUAWEI> display pki certificate ca realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Jun  4 14:58:17 2015 GMT
            Not After : Jun  4 15:07:10 2020 GMT
        Subject: CN=ca_root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:5f:2a:93:cb:66:18:59:8c:26:80:db:cd:73:
                    d5:68:92:1b:04:9d:cf:33:a2:73:64:3e:5f:fe:1a:
                    53:78:0e:3d:e1:99:14:aa:86:9b:c3:b8:33:ab:bb:
                    76:e9:82:f6:8f:05:cf:f6:83:8e:76:ca:ff:7d:f1:
                    bc:22:74:5e:8f:4c:22:05:78:d5:d6:48:8d:82:a7:
                    5d:e1:4c:a4:a9:98:ec:26:a1:21:07:42:e4:32:43:
                    ff:b6:a4:bd:5e:4d:df:8d:02:49:5d:aa:cc:62:6c:
                    34:ab:14:b0:f1:58:4a:40:20:ce:be:a5:7b:77:ce:
                    a4:1d:52:14:11:fe:2a:d0:ac:ac:16:95:78:34:34:
                    21:36:f2:c7:66:2a:14:31:28:dc:7f:7e:10:12:e5:
                    6b:29:9a:e8:fb:73:b1:62:aa:7e:bd:05:e5:c6:78:
                    6d:3c:08:4c:9c:3f:3b:e0:e9:f2:fd:cb:9a:d1:b7:
                    de:1e:84:f4:4a:7d:e2:ac:08:15:09:cb:ee:82:4b:
                    6b:bd:c6:68:da:7e:c8:29:78:13:26:e0:3c:6c:72:
                    39:c5:f8:ad:99:e4:c3:dd:16:b5:2d:7f:17:e4:fd:
                    e4:51:7a:e6:86:f0:e7:82:2f:55:d1:6f:08:cb:de:
                    84:da:ce:ef:b3:b1:d6:b3:c0:56:50:d5:76:4d:c7:
                    fb:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C5
            X509v3 CRL Distribution Points:
```

```
                Full Name:
                  URI:http://vasp-e6000-127.china.example.com/CertEnroll/ca_root.
crl
                  URI:file://\\vasp-e6000-127.china.example.com\CertEnroll\ca_roo
t.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
         52:21:46:b8:67:c8:c3:4a:e7:f8:cd:e1:02:d4:24:a7:ce:50:
         be:33:af:8a:49:47:67:43:f9:7f:79:88:9c:99:f5:87:c9:ff:
         08:0f:f3:3b:de:f9:19:48:e5:43:0e:73:c7:0f:ef:96:ef:5a:
         5f:44:76:02:43:83:95:c4:4e:06:5e:11:27:69:65:97:90:4f:
         04:4a:1e:12:37:30:95:24:75:c6:a4:73:ee:9d:c2:de:ea:e9:
         05:c0:a4:fb:39:ec:5c:13:29:69:78:33:ed:d0:18:37:6e:99:
         bc:45:0e:a3:95:e9:2c:d8:50:fd:ca:c2:b3:5a:d8:45:82:6e:
         ec:cc:12:a2:35:f2:43:a5:ca:48:61:93:b9:6e:fe:7c:ac:41:
         bf:88:70:57:fc:bb:66:29:ae:73:9c:95:b9:bb:1d:16:f7:b4:
         6a:da:03:df:56:cf:c7:c7:8c:a9:19:23:61:5b:66:22:6f:7e:
         1d:26:92:69:53:c8:c6:0e:b3:00:ff:54:77:5e:8a:b5:07:54:
         fd:18:39:0a:03:ac:1d:9f:1f:a1:eb:b9:f8:0d:21:25:36:d5:
         06:de:33:fa:7b:c8:e9:60:f3:76:83:bf:63:c6:dc:c1:2c:e4:
         58:b9:cb:48:15:d2:a8:fa:42:72:15:43:ef:55:63:39:58:77:
         e8:ae:0f:34

Pki realm name: abc
Certificate file name: abc_ca.cer
Certificate peer name: -
```

Table 14-97 Description of the **display pki certificate** command output

Item	Description
The x509 object type is certificate	X.509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

Item	Description
Subject	Subject of a certificate. For details about the attributes that are not mentioned below, see the *Equipment Identifier Specification of Wireless Local Area Network*. - C: country code of a PKI entity. - ST: name of the state or province to which a PKI entity belongs. - L: geographic area where a PKI entity is located. - O: organization to which a PKI entity belongs. - OU: department to which a PKI entity belongs. - CN: common name of a PKI entity. - DC: forcible domain. - ASUE: user equipment.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Key Usage	X509v3 key usage.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 CRL Distribution Points	CRL distribution points (CDP).
Full Name	Full name of the CDP.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

14.19.29 display pki certificate enroll-status

Function

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Format

display pki certificate enroll-status [**realm** *realm-name*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Example

Display the certificate enrollment status.

```
<HUAWEI> display pki certificate enroll-status realm abc
 Certificate Request Transaction 1
    Status: Pending
    Key Usage: ENC&SIG
    Entity name: test
    Remain polling count: 1
    Next polling after : 35 seconds
<HUAWEI> display pki certificate enroll-status realm abc
 info: No certificate request transaction in realm abc.
```

Table 14-98 Description of the **display pki certificate enroll-status** command output

Item	Description
Certificate Request Transaction	Certificate enrollment request process.
Status	Certificate enrollment status. Pending: A certificate is being enrolled.

Item	Description
Key Usage	Functions of a certificate public key: - ENC: The public key is used for encryption. - SIG: The public key is used for signature.
Entity name	Entity name.
Remain polling count	Number of times a certificate enrollment request can be initiated again.
Next polling after	Next time a certificate enrollment request is initiated.
No certificate request transaction	There is no certificate enrollment request process.

14.19.30 display pki certificate filename

Function

The **display pki certificate filename** command displays the content of a certificate.

Format

display pki certificate filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about the certificate including signature algorithm, issuer, validity period, subject, and subject public key.

Example

Display information about the certificate **ca.cer**.

```
<HUAWEI> display pki certificate filename ca.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f3:a3:3a:46:f6:09:8d:18
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
        Validity
            Not Before: May 16 11:48:04 2017 GMT
            Not After : May 14 11:48:04 2027 GMT
        Subject: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:ba:cc:ef:2f:55:9c:d0:09:c5:1b:d2:52:63:92:
                    c8:f0:88:ed:1b:88:f1:e4:3c:90:07:85:01:8c:d5:
                    80:d9:91:ef:64:e9:79:0c:7d:0e:b9:6c:00:a2:72:
                    e2:1b:aa:9b:2d:11:6b:6f:2d:de:5d:58:22:cf:9e:
                    2f:7d:f1:ad:71:e9:25:0e:bc:26:f1:77:57:02:3d:
                    7f:09:8f:49:63:ae:11:75:57:65:a0:bd:9c:94:c6:
                    df:21:f7:c8:5a:4d:5e:f8:5e:84:b0:b0:fd:a6:c7:
                    e0:78:d1:1c:8a:55:d9:e9:66:1c:e5:4e:ce:88:dd:
                    fa:0f:60:d0:7e:86:a1:ec:b1:34:aa:f7:dd:72:c6:
                    0a:90:c7:4a:6b:a0:86:01:30:b6:6f:23:ff:ce:ae:
                    39:fb:de:18:ce:2f:b9:d7:17:09:8c:29:19:34:7a:
                    69:75:dc:ee:bf:2e:d4:93:fb:f6:a6:5b:f8:2a:6d:
                    fe:bd:f4:8b:30:49:5c:a8:94:76:12:9d:64:78:4a:
                    48:d3:2d:63:da:0a:79:b2:ee:8e:2d:5a:a0:71:99:
                    cf:b9:68:77:d3:d9:cf:12:64:80:bb:42:8c:28:1f:
                    d9:bf:7c:4b:8f:39:1e:dc:92:a4:ff:8e:b3:02:58:
                    c5:79:96:f2:a1:f9:17:cb:ea:49:57:b0:b0:3c:af:
                    db:19
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                83:08:A4:F4:BC:EC:1B:B6:7D:B0:27:F6:10:47:77:AA:2A:66:59:D5
            Netscape Cert Type:
                SSL CA
    Signature Algorithm: sha256WithRSAEncryption
         1e:6b:2a:76:7e:8e:b0:0e:72:4e:02:53:b0:77:0d:13:28:4e:
         c3:e5:f8:0b:76:fd:56:2c:e6:5b:d1:f8:48:19:17:95:1a:79:
         5e:d9:50:b9:68:bd:36:c4:ce:7b:ce:0c:98:55:b1:44:9f:20:
         66:66:33:3c:b5:40:ad:50:c8:64:1c:07:0e:08:42:72:88:35:
         d4:af:f0:8d:5d:64:90:5d:ec:f0:5c:07:76:10:ed:9b:22:18:
         ef:44:4e:c2:29:32:40:68:fe:04:dc:0e:f6:2b:25:c2:73:f5:
         9b:64:df:25:56:c6:bb:6e:a4:2f:07:b3:9d:c0:18:60:72:cb:
         51:62:94:ee:f7:21:0a:a0:92:58:a1:bf:c8:30:0e:0c:0a:91:
         cb:f4:8f:07:52:ba:df:25:88:8a:b3:3f:f0:68:fa:4c:b7:31:
         c8:97:e0:49:08:8a:74:fc:c2:90:d7:3c:0b:00:38:90:3b:19:
         ab:66:96:24:1f:86:b9:62:49:6d:9c:2d:02:99:38:bb:96:b6:
         dd:0f:3c:6e:24:7b:3d:1e:77:58:e7:46:2b:42:cc:14:6a:a4:
         16:45:ed:3c:b1:d6:30:94:c0:30:d0:46:fa:bc:da:9a:2b:f1:
         fa:f3:df:1b:84
```

Table 14-99 Description of the **display pki certificate filename** command output

Item	Description
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.
Subject	Subject of a certificate. The subject includes the following attributes: ● C: country code of a PKI entity. ● ST: name of the state or province to which a PKI entity belongs. ● L: geographic area where a PKI entity is located. ● O: organization to which a PKI entity belongs. ● OU: department to which a PKI entity belongs. ● CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
RSA Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trusted.
X509v3 Key Usage	X.509v3 key usage.
X509v3 Subject Key Identifier	Identifier of a subject key.
Netscape Cert Type	Netscape certificate type.

14.19.31 display pki cmp statistics

Function

The **display pki cmp statistics** command displays CMP session statistics.

Format

display pki cmp statistics [**session** *session-name*]

Parameters

Parameter	Description	Value
session *session-name*	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays CMP session statistics, including the number of sent IR packets, sent CR packets, sent KUR packets, and received IP packets.

If a CMP session is specified, the statistics of the session are displayed. If no CMP session is specified, the statistics of all sessions are displayed.

Example

Display the statistics of the CMP session **test**.

```
<HUAWEI> display pki cmp statistics session test
 CMP Context Name: test
  Initialization request      : 0
  Certification request       : 0
  Key update request          : 0
 PKI Status:
  Accepted                    : 0
  Granted with modifications : 0
  Rejection                   : 0
  Waiting                     : 0
  Revocation warning          : 0
  Revocation notification     : 0
  Key update warning          : 0
```

Table 14-100 Description of the **display pki cmp statistics** command output

Item	Description
CMP Context Name	Name of a CMP session.
Initialization request	Total number of initialization requests sent during the session.
Certification request	Total number of certificate requests sent during the session.
Key update request	Total number of key update requests sent during the session.
PKI Status	Status of the PKI realm.
Accepted	Number of received certificate applications.
Granted with modifications	The certificate server returns an application request, but the change needs to be confirmed.
Rejection	The certificate server rejects the application request.
Waiting	The certificate server has not handled the application request.
Revocation warning	The certificate is about to be revoked.
Revocation notification	The certificate has been revoked.
Key update warning	The certificate key has been updated.

14.19.32 display pki credential-storage-path

Function

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

By default, the certificate file is stored in **flash:/**.

Format

display pki credential-storage-path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

Example

Display the default path where a PKI certificate is stored.

```
<HUAWEI> display pki credential-storage-path
 The pki credential-storage-path is flash:/ .
```

14.19.33 display pki crl

Function

The **display pki crl** command displays the content of the CRL in the device.

Format

display pki crl { **realm** *realm-name* | **filename** *filename* }

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm associated with the CRL.	The PKI realm name must already exist.
filename *filename*	Specifies the file name of the certificate to be imported.	The certificate file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about local CRL, including signature algorithm, issuer, update time, revoked certificate, CRL sequence number, and revocation time.

Example

Display information about the CRL associated with the PKI realm **abc**.

```
<HUAWEI> display pki crl realm abc
 The x509 object type is CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /CN=ca_root
        Last Update: Dec 15 08:24:28 2015 GMT
        Next Update: Dec 22 20:44:28 2015 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 CRL Number:
                365
            1.3.6.1.4.1.311.21.4:
151222083428Z   .
Revoked Certificates:
    Serial Number: 28C63371000000003E04
        Revocation Date: Dec 15 08:34:27 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 28C2AB44000000003E01
        Revocation Date: Dec 15 08:30:35 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2364247C000000003D48
        Revocation Date: Dec 14 07:29:05 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 23627E0F000000003D47
        Revocation Date: Dec 14 07:27:29 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2360F397000000003D46
        Revocation Date: Dec 14 07:25:48 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Signature Algorithm: sha1WithRSAEncryption
         7a:71:54:d1:66:13:6f:9f:62:03:ac:9a:5f:42:10:15:87:46:
         e2:a1:49:0f:44:19:ce:ed:6f:c3:0e:9f:31:fe:62:d5:08:0b:
         a4:a7:7e:80:4d:9a:5b:a9:55:5c:1a:73:30:62:48:e1:28:0e:
         5b:bd:ae:04:7e:83:36:43:62:fc:f7:12:0d:f9:f6:ac:2b:be:
         9c:50:6c:67:19:43:12:31:67:c2:06:31:97:e1:34:75:1c:87:
         53:5f:e6:15:a1:33:ad:00:e7:14:68:59:05:67:28:78:a0:91:
         49:7b:ab:87:9f:9e:53:18:4b:54:53:1c:b7:1c:2d:3e:b3:57:
         63:95:1d:01:29:9e:6c:41:07:40:2d:28:d8:82:7b:d6:22:e6:
         0d:0c:4c:af:84:96:8e:f1:29:28:d4:9e:1c:37:3b:1b:2e:34:
         a7:15:e3:29:d1:c0:69:0a:7f:24:b1:ce:00:f1:b3:da:ef:8a:
         1b:14:36:f9:14:6c:b0:66:86:a8:92:95:fc:e3:78:aa:d6:d0:
         cb:4d:26:b4:bc:41:c4:47:19:d0:2a:0c:ac:c6:aa:95:c2:03:
```

```
        33:8a:39:45:3e:c3:ad:46:7d:8a:03:4d:08:e2:d0:9a:ae:39:
        fa:8d:61:d0:1c:6c:03:d4:48:2e:4d:37:60:a1:06:a4:ea:c8:
        0d:20:59:c2

Pki realm name: abc
CRL file name: abc.crl
```

Table 14-101 Description of the **display pki crl** command output

Item	Description
The x509 object type is CRL	x509 object type is CRL.
Certificate Revocation List (CRL)	Information about the CRL.
Signature Algorithm	Algorithm of signature.
Issuer	Information of issuer.
Last Update	Last time the CRL has been updated.
Next Update	Next time the CRL will be updated.
CRL extensions	CRL extended attribute.
X509v3 Authority Key Identifier	X.509v3 authority key identifier.
X509v3 CRL Number	X.509v3 CRL number.
Revoked Certificates	Certificate that is revoked.
Serial Number	Serial number of the CRL.
Revocation Date	Date when the certificate was revoked.
CRL entry extensions	CRL entry extensions.
X509v3 CRL Reason Code	Reason why CRL is revoked.
Signature Algorithm	Signature algorithm. It is configured using the **enrollment-request signature message-digest-method** command.
Pki realm name	PKI realm name. It is configured using the **pki realm(system view)** command.
CRL file name	CRL file name. It is configured using the **pki import-crl** command.

14.19.34 display pki entity

Function

The **display pki entity** command displays information about PKI entities.

Format

display pki entity [*entity-name*]

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity. If the *entity-name* parameter is not specified, information about all entities is displayed.	The value must be an existing PKI entity name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about PKI entities, including names, common names, countries, province, and location where the entities reside, and organizations to which entities belong.

Example

Display information about all PKI entities.

```
<HUAWEI> display pki entity
PKI Entity Information:

  Entity Name       : a
  Common name       : chi
  Country           : -
  State             : A
  Locality          : -
  Organization      : A
  Organization unit: -
  FQDN              : www. e
  IP address        : -
  Email             : -
  Serial-number     : -
 Total Number: 1
```

Table 14-102 Description of the **display pki entity** command output

Item	Description
PKI Entity Information	Information of the PKI entity.
Entity Name	Entity name. It is configured using the **pki entity** command.

Item	Description
Common name	Common name of the entity. It is configured using the **common-name** command.
Country	Country where a PKI entity resides. It is configured using the **country (PKI entity view)** command.
State	Province where a PKI entity resides. It is configured using the **state (PKI entity view)** command.
Locality	Location of a PKI entity. It is configured using the **locality** command.
Organization	Organization to which a PKI entity belongs. It is configured using the **organization** command.
Organization unit	Organization unit to which a PKI entity belongs. It is configured using the **organization-unit** command.
FQDN	FQDN name of a PKI entity. It is configured using the **fqdn** command.
IP address	IP address of a PKI entity. It is configured using the **ip-address** command.
Email	Email address. It is configured using the **email** command.
Serial-number	Serial number of the entity. It is configured using the **serial-number** command.

14.19.35 display pki ocsp cache statistics

Function

The **display pki ocsp cache statistics** command displays statistics about cached OCSP responses.

Format

display pki ocsp cache statistics

NOTE

This command is available only on NETCONF-supporting switch models.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command shows statistics about cached OCSP responses, including the maximum number of OCSP responses that can be cached, cache update interval, and number of cached responses.

Example

Display statistics about cached OCSP responses.

```
<HUAWEI> display pki ocsp cache statistics

==================================================
   OCSP Cache Function: Enable
   OCSP Cache Max Number: 2
   OCSP Cache Refresh Interval: 5 minutes
   OCSP Cache Current Number: 0
==================================================
```

Table 14-103 Description of the **display pki ocsp cache statistics** command output

Item	Description
OCSP Cache Function	Whether OCSP caching is enabled. - Enable - Disable It is configured using the **pki ocsp response cache enable** command.
OCSP Cache Max Number	Maximum size of OCSP cache. It is configured using the **pki ocsp response cache number** command.

Item	Description
OCSP Cache Refresh Interval	OCSP cache update interval. It is configured using the **pki ocsp response cache refresh interval** command.
OCSP Cache Current Number	Number of cached OCSP responses.

14.19.36 display pki ocsp cache detail

Function

The **display pki ocsp cache detail** displays the detail information of the OCSP cache.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

display pki ocsp cache detail

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view detail information of the OCSP cache.

Example

Display the detail information of the OCSP cache.

```
<HUAWEI> display pki ocsp cache detail
=====================================================
Cache Hash Status Info:
num_items              = 0
num_nodes              = 8
num_alloc_nodes        = 16
num_expands            = 0
num_expand_reallocs    = 0
num_contracts          = 0
```

```
num_contract_reallocs = 0
num_hash_calls        = 0
num_comp_calls        = 0
num_insert            = 0
num_replace           = 0
num_delete            = 0
num_no_delete         = 0
num_retrieve          = 0
num_retrieve_miss     = 0
num_hash_comps        = 0
Cache Hash Node Status Info:

node      0 ->   0
node      1 ->   0
node      2 ->   0
node      3 ->   0
node      4 ->   0
node      5 ->   0
node      6 ->   0
node      7 ->   0
Cache Hash Node Usage Status Info:

0 nodes used out of 8
0 items
====================================================
```

Table 14-104 Description of the **display pki ocsp cache detail** command output

Item	Description
Cache Hash Status Info	Hash status of the OCSP cache.
num_items	Number of available hash elements.
num_nodes	Number of requested hash nodes.
num_alloc_nodes	Maximum number of hash nodes that can be expanded.
num_expands	Number of hash node expansion application times.
num_expand_reallocs	Number of expanded hash nodes.
num_contracts	Number of hash node reduction times.
num_contract_reallocs	Number of reduced hash nodes.
num_hash_calls	Number of times the hash function is invoked.
num_comp_calls	Number of times the hash comparison function is invoked.
num_insert	Number of inserted hash nodes.
num_replace	Number of replaced hash nodes.
num_delete	Number of deleted hash nodes.
num_no_delete	Number of undeleted hash nodes.

Item	Description
num_retrieve	Number of times the hash nodes in the OCSP cache are matched.
num_retrieve_miss	Number of times the hash nodes in the OCSP cache are not matched.
num_hash_comps	Number of times the hash nodes in the OCSP cache are compared.
Cache Hash Node Status Info	Hash node status in the OCSP cache. For example, **node 0 -> 0** indicates that the number 0 node is unused; **node 0 -> 1** indicates that the number 0 node is in use.
Cache Hash Node Usage Status Info	Hash node use status in the OCSP cache.
n nodes used out of 8	There are 8 hash nodes, and n nodes are in use.
n items	nth hash element.

14.19.37 display pki ocsp server down-information

Function

The **display pki ocsp server down-information** command displays the Down state information of the OCSP server recorded on the device.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

display pki ocsp server down-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is Down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to Down. In this case, the device will not send OCSP requests to the URL within 10 minutes.

Example

Display the Down state information of the OCSP server.

```
<HUAWEI> display pki ocsp server down-information

=====================================================

  Server URL: http://10.1.1.1/ocsp
  Timeout Times: 1
  Last timeout until now: 5 seconds
=====================================================
```

Table 14-105 Description of the **display pki ocsp server down-information** command output

Item	Description
Server URL	URL of an unreachable OCSP server. It is configured using the **ocsp url** command.
Timeout Times	Connection timeouts.
Last timeout until now	Time elapsed since the last connection timeout and now.

14.19.38 display pki peer-certificate

Function

The **display pki peer-certificate** command displays the imported certificates of the remote device.

Format

display pki peer-certificate { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate.	The value must be an existing peer certificate file name.

Parameter	Description	Value
all	Displays brief information about all certificates of the remote device.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about imported certificates of the remote device, including signature algorithm, issuer, validity period, subject, public key, and PKI realm.

Example

Display brief information about all certificates of the remote device.

```
<HUAWEI> display pki peer-certificate all
  Peer certificate name :abcd
  Serial Number:
    12 19 3c d3 00 00 00 00 04 9a
  Subject:
    CN=a

Total Number: 1
```

Display detailed information about the certificate **abcd** of the remote device.

```
<HUAWEI> display pki peer-certificate name abcd
The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:19:3c:d3:00:00:00:00:04:9a
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=CA_ROOT
        Validity
            Not Before: Feb 19 13:00:22 2013 GMT
            Not After : Feb 19 13:10:22 2014 GMT
        Subject: CN=a
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (512 bit)
                Modulus:
                    00:b9:8b:47:65:a9:99:ed:58:b2:63:74:65:56:d1:
                    08:bb:1d:8f:4e:ed:72:a2:4a:ef:d8:45:3d:53:db:
                    c8:eb:df:53:9e:5f:c7:96:46:65:14:1a:ab:72:e9:
                    a2:71:c8:7a:f0:51:0c:cc:39:bb:14:75:7d:f1:bc:
                    88:2c:a7:2e:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

```
            X509v3 Subject Key Identifier:
                E2:5B:8A:03:58:01:C8:E3:14:BC:18:5B:F9:BD:00:68:5B:D1:90:4E
            X509v3 Authority Key Identifier:
                keyid:CE:BA:CA:39:C7:AD:6A:CB:85:17:D0:8A:8E:28:02:0B:52:D4:D9:2
B

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://10.1.1.1:8080/CertEnroll/CA_ROOT.crl

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=CA_ROOT,CN=AIA,CN=Public%20Key%20Ser
vices,CN=Services,CN=Configuration,DC=esap,DC=com?cACertificate?base?objectClass
=certificationAuthority
                CA Issuers - URI:http://www.example.com/CertEnroll/www.example.com
_CA_ROOT.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
         bb:8b:77:af:ae:df:2e:0c:bd:7a:29:6e:76:23:ad:7d:69:6d:
         0d:16:d9:18:82:ad:4f:52:b3:cd:1c:1a:fc:34:00:33:36:8d:
         47:2a:20:24:52:b7:02:75:cc:ab:3b:4c:f8:2a:a9:a9:4f:46:
         fb:c2:21:00:c1:b5:c2:67:0c:b1:99:2a:62:7b:71:4d:e7:c2:
         93:29:bb:ec:b1:e9:28:82:2f:77:61:ec:28:66:35:cb:5f:15:
         04:73:77:d8:26:91:7b:a2:56:74:51:33:0b:f1:04:28:24:b2:
         71:58:ad:5c:f8:96:17:0d:f7:b7:5f:4b:b9:ed:09:79:bc:54:
         21:c5:9b:90:f7:7b:21:aa:5a:aa:6f:51:e4:79:ce:b8:35:8b:
         19:90:51:94:e6:c2:61:f8:24:46:85:4c:a9:69:bd:8a:ef:c2:
         64:b8:19:ab:0b:6b:ec:34:41:8d:43:43:44:d1:1b:4c:4a:23:
         cd:40:52:7a:2e:8c:5d:b6:62:55:93:45:c8:3e:de:b1:51:82:
         d0:bb:7c:b8:09:7b:97:08:7b:93:17:40:a8:6f:2d:ed:f4:3e:
         36:10:2a:20:e3:47:e1:fb:ad:fe:97:73:a7:53:d0:f8:52:ca:
         b6:0e:e8:f1:df:6c:7a:37:39:bb:82:f9:03:c9:4a:71:65:df:
         6f:37:e6:b7

Pki realm name: -
Certificate file name: -
Certificate peer name: abcd
```

Table 14-106 Description of the **display pki peer-certificate** command output

Item	Description
Peer certificate name	Peer certificate name.
The x509 object type is certificate	X.509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

Item	Description
Subject	Subject of the certificate.
Subject Public Key Info	Public key of the certificate.
Public Key Algorithm	Algorithm of the Public key.
Public-Key	Information about the RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Authority Information Access	Authority information access.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

14.19.39 display pki realm

Function

The **display pki realm** command displays PKI realm information.

Format

display pki realm [*realm-name*]

Parameters

Parameter	Description	Value
realm-name	Displays detailed information about a PKI realm. If the parameter is left blank, information about all PKI realms is displayed.	The PKI realm name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays details about PKI realms, including PKI realm name, associated CA, CA certificate subject name, URL of the certificate enrolled through SCEP, PKI entity name, digital fingerprint algorithm of CA certificate, and digital fingerprint of CA certificate.

Example

Display information about all PKI realms.

```
<HUAWEI> display pki realm abc
 Realm Name : abc
 CA ID: CA_ROOT
 CA Name: "/CN=ca_root"
 Enrollment URL: http://10.136.7.196:8080/certsrv/mscep/mscep.dll
 Certificate Request Interval(Minutes): 1
 Certificate Request Times: 5
 Enrollment Mode: RA
 Enrollment Method: SCEP
 Entity Name: abc
 CA Certificate Fingerprint Arithmetic: sha256
 CA Certificate Fingerprint: e71add0744360e91186b828412d279e06dcc15a4ab4bb3d1384
2820396b526a0
 OCSP Nonce: Enable
 OCSP URL: -
 Method for Getting CRL: HTTP
 CDP URL: -
 Certificate Revocation Check Method: -
 RSA Key Name: abc
 Auto-enroll: Enable
 Auto-enroll Percent: 100%
 Auto-enroll Regenerate: Enable
 Auto-enroll Regenerate Key-size: 2048
 Auto-enroll Updated-effective: Disable
 Password Cipher: Enable
 Password: ******
 Crl Update-period(Hours): 8
 Crl Cache: Enable
 Key-usage: -
```

```
Vpn-instance: -
Source IP: -
Enrollment-request Signature Message-digest-method: SHA256

Total Number: 1
```

Table 14-107 Description of the **display pki realm** command output

Item	Description
Realm Name	PKI realm name. It is configured using the **pki realm (system view)** command.
CA ID	ID of the CA associated with the PKI realm.
CA Name	Subject name of a CA certificate.
Enrollment URL	URL of the certificate enrolled on the SCEP server. It is configured using the **enrollment-url** command.
Certificate Request Interval(Minutes)	Interval between two certificate enrollment status queries.
Certificate Request Times	Maximum number of certificate enrollment status queries.
Enrollment Mode	Certificate enrollment mode (whether enrolled through RA). It is configured using the **enrollment-url** command.
Enrollment Method	Certificate enrollment method, including: ● SCEP: obtains certificate from CA using the SCEP protocol. ● Self-Signed: obtains certificate using self-signature.
Entity Name	PKI entity name. It is configured using the **entity** command.
CA Certificate Fingerprint Arithmetic	Fingerprint algorithm of the CA certificate. It is configured using the **fingerprint** command.
CA Certificate Fingerprint	Digital fingerprint of the CA certificate. It is configured using the **fingerprint** command.
OCSP Nonce	Whether a nonce extension is added to the OCSP request sent by a PKI entity. ● Enable: A nonce extension is added to the OCSP request sent by a PKI entity. ● Disable: A nonce extension is not added to the OCSP request sent by a PKI entity. It is configured using the **ocsp nonce enable** command.
OCSP URL	OCSP server's URL. It is configured using the **ocsp url** command.

Item	Description
Method for Getting CRL	Method of obtaining CRL. - SCEP: updates the CRL automatically using SCEP. It is configured using the **crl scep** command. - HTTP: updates the CRL automatically using HTTP. It is configured using the **crl http** command.
CDP URL	URL of the CDP. It is configured using the **cdp-url** command.
Crl Cache	Whether the PKI realm is allowed to use the CRL in cache. - Enable: The PKI realm is allowed to use the CRL in cache. - Disable: The PKI realm is not allowed to use the CRL in cache. To configure whether to allow the PKI realm to use the CRL in cache, run the **crl cache** command.
Certificate Revocation Check Method	Certificate status check method. It is configured using the **certificate-check** command.
RSA Key Name	RSA key. It is configured using the **rsa local-key-pair** command.
Auto-enroll	Whether automatic certificate enrollment is enabled: - Enable: Automatic certificate enrollment is enabled. - Disable: Automatic certificate enrollment is disabled. It is configured using the **auto-enroll** command.
Auto-enroll Percent	The percentage of the certificate's validity period. It is configured using the **auto-enroll** command.
Auto-enroll Regenerate	Whether the RSA key pair will be generated during certificate updates: - Enable: The RSA key pair will be generated during certificate updates. - Disable: The RSA key pair will not be generated during certificate updates. It is configured using the **auto-enroll** command.
Auto-enroll Regenerate Key-size	RSA key length. It is configured using the **auto-enroll** command.

Item	Description
Auto-enroll Updated-effective	Whether the certificate takes effect immediately after being updated. - Enable: The certificate takes effect immediately after being updated. - Disable: The certificate does not take effect immediately after being updated. It is configured using the **auto-enroll** command.
Password Cipher	Whether the challenge password can be used: - Enable: The challenge password can be used. - Disable: The challenge password cannot be used.
Password	Password used to apply for or revoke a certificate. It is configured using the **password (PKI realm view)** command.
Crl Update-period(Hours)	CRL update interval. It is configured using the **crl update-period** command.
Key-usage	Purpose information carried in a certificate request packet. It is configured using the **key-usage** command.
Vpn-instance	VPN to which the PKI realm is added. It is configured using the **vpn-instance** command.
Source IP	Source IP address used by the device to communicate with the PKI server. It is configured using the **source** command.
Enrollment-request Signature Message-digest-method	Digest method used for the enrollment request packet of signed certificate. It is configured using the **enrollment-request signature message-digest-method** command.

14.19.40 display pki rsa local-key-pair

Function

The **display pki rsa local-key-pair** command displays RSA key pairs and public keys.

Format

display pki rsa local-key-pair { **pem** | **pkcs12** } *filename* [**password** *password*]

display pki rsa local-key-pair [**name** *key-name*] **public** [**temporary**]

NOTE

The **pem** *file-name* parameter is supported only when the WEAKEA plug-in is installed. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Parameters

Parameter	Description	Value
pem	Indicates that the file format is PEM.	-
pkcs12	Indicates that the file format is PKCS12.	-
filename	Specifies the name of the file that contains the RSA key pair.	The file name must already exist.
password *password*	Specifies the decryption password for the RSA key pair file. The value must be the same as the password configured using the **pki export rsa-key-pair** command.	The value must be the name of an existing decryption password of the RSA key pair.
name *key-name*	Specifies the RSA key pair name.	The RSA key pair name must already exist.
temporary	Displays information about the RSA key pair saved in the temporary zone.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about the RSA key pair and public key, including key pair creation time, key pair name, whether the key can be exported, and public key information.

If *key-name* is not specified, all RSA key pairs and public keys are displayed. If *key-name* is specified, the specified RSA key pair and public key are displayed.

Example

Display information about all RSA key pairs.

```
<HUAWEI> display pki rsa local-key-pair public

====================================================
Time of Key pair created: 17:43:42  2016/4/18
Key Name: abc
Key Index: 0
Key Modules: 2048 bit
Key Exportable: Yes
Key Type: RSA signature key
====================================================
Key code:
30820109
  02820100
    C23344E1 B2C2D653 EB134011 9266C6CC 7C18C45F
    440AF31F 98B29D4C D436757B F6785BB5 09EFA2A1
    09FDBB24 62F1914D 4F10678F 3BE8E3C0 E6F02FC9
    AFE2ADDE 98E07D2C A5732288 A5280D2B 6A785F59
    A8D19D37 9B80F7EF 1B15FB77 BD9C54D0 01AF270F
    90258F65 1A631282 50002C4F 23EF0482 1F62E356
    AC700041 B31AB3B4 5C7EB4C0 AFF2E5AF 3DDA4F4E
    F5B86502 08BA7AFE 37204C67 7149AE52 1462F25E
    16B777E8 E71BCFBE 0E9E02A7 C5FE6120 304BE6C3
    CEB2575A EA24EBB6 BA420994 C50F3662 D8F24F25
    0D833865 5A127754 2E954F7F 16292DAA AF9D2371
    E669ADFF 4EA9FFF8 CE8488D7 344EBCEB AAA74116
    B30EF506 C64A726E B1013CB4 E8FA6707
  0203
    010001
```

Table 14-108 Description of the **display pki rsa local-key-pair** command output

Item	Description
Time of Key pair created	Time when the RSA key pair is created.
Key Name	Name of a key pair. It is configured using the **pki rsa local-key-pair create** command.
Key Index	Index of the key.
Key Modules	Number of bits of the key.
Key Exportable	Whether the key can be exported.
Key Type	Type of the key.
Key code	Public key in the RSA key pair.

14.19.41 email

Function

The **email** command configures an email address for a PKI entity.

The **undo email** command cancels the configuration.

By default, no email address is configured for a PKI entity.

Format

email *email-address*

undo email

Parameters

Parameter	Description	Value
email-address	Specifies the email address of a PKI entity.	The value is a string of 1 to 128 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an email address for the PKI entity, which is used as an alias of the entity.

After the email address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this email address. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the email address of the PKI entity.

Example

Set the email address to **test@example.com** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] email test@example.com
```

14.19.42 enrollment self-signed

Function

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm.

The **undo enrollment self-signed** command restores the default certificate obtaining method.

By default, self-signed certificate obtaining in the PKI realm is not configured.

Format

enrollment self-signed

undo enrollment self-signed

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm. The device can use the self-signed certificate obtained from the PKI realm to support default HTTPS functions. The certificate issuer name is in the format: device name-Self-Signed-Certificate-ESN.

Prerequisites

The RSA key pair has been configured by using the **rsa local-key-pair** command.

Precautions

The device generates a self-signed certificate only when the PKI domain is applied to the service.

The device does not support lifecycle management for self-signed certificates. For example, self-signed certificates cannot be registered, updated, or revoked on the device. To ensure security of the device and certificates, it is recommended the user's certificate be used.

To configure self-signed certificate obtaining, delete the certificate in the PKI realm.

After the **enrollment self-signed** command is run, the device will not generate certificate expiration logs when its self-signed certificate expires.

Example

Configure self-signed certificate obtaining in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] enrollment self-signed
```

14.19.43 enrollment-request signature message-digest-method

Function

The **enrollment-request signature message-digest-method** command configures the digest algorithm used to sign certificate enrollment requests.

The **undo enrollment-request signature message-digest-method** command restores the default digest algorithm used to sign certificate enrollment requests.

By default, the digest algorithm used to sign certificate enrollment requests is **sha-256**.

Format

enrollment-request signature message-digest-method { **md5** | **sha1** | **sha-256** | **sha-384** | **sha-512** }

undo enrollment-request signature message-digest-method

Parameters

Parameter	Description	Value
md5	Specifies the digest algorithm used to sign certificate enrollment requests to MD5.	-
sha1	Specifies the digest algorithm used to sign certificate enrollment requests to SHA1.	-
sha-256	Specifies the digest algorithm used to sign certificate enrollment requests to SHA2-256.	-
sha-384	Specifies the digest algorithm used to sign certificate enrollment requests to SHA2-384.	-
sha-512	Specifies the digest algorithm used to sign certificate enrollment requests to SHA2-512.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

In SCEP local certificate application mode, after a CA server receives a certificate enrollment request from a PKI entity, the CA server requests a signature for authentication, and generates a local certificate only after the authentication is successful.

For security purposes, SHA2 is recommended. You are not advised to configure MD5 and SHA1.

Example

Set the digest algorithm used to sign certificate enrollment requests to **sha-384**.

```
<HUAWEI> system-view
[HUAWEI] pki realm e
[HUAWEI-pki-realm-e] enrollment-request signature message-digest-method sha-384
```

14.19.44 enrollment-url

Function

The **enrollment-url** command configures the URL of the CA server.

The **undo enrollment-url** command deletes the URL of the CA server.

By default, the URL of the CA server is not configured.

Format

enrollment-url [**esc**] *url* [**interval** *minutes*] [**times** *count*] [**ra**]

undo enrollment-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url	Specifies the URL of the CA server. The URL is in the format of *http://server_location/ca_script_location*. *server_location* can use only the IP address format and domain name resolution. *ca_script_location* is the path where CA server host's application script is located, for example, **http://10.137.145.158:8080/certsrv/mscep/mscep.dll**.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.

Parameter	Description	Value
interval *minutes*	Specifies the interval between two certificate enrollment status queries.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 1.
times *count*	Specifies the maximum number of certificate enrollment status queries.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
ra	Configures an RA to authenticate a PKI entity's identity information during local certificate application. By default, a CA authenticates a PKI entity's identity information during local certificate application.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The URL refers to the address provided by a CA server for certificate application. For example, a CA server running Windows Server 2008 uses a URL address in the format http://host:port/certsrv/mscep/mscep.dll, in which *host* indicates the IP address of the CA server and *port* indicates the port number.

The keyword **esc** supports the entering of URLs that include the question mark (?) in ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\\x3f**.

Example

Create a PKI realm **test** and configure the URL in HTTP mode for the CA server.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] enrollment-url http://10.13.14.15:8080/certsrv/mscep/mscep.dll ra
```

14.19.45 entity

Function

The **entity** command specifies a PKI entity that applies for a certificate.

The **undo entity** command cancels a PKI entity.

By default, no PKI entity is specified.

Format

entity *entity-name*

undo entity

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value must be an existing PKI entity name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity requests the local certificate in the PKI realm, the device encapsulates the configuration of the specified PKI entity into the certificate request.

Prerequisites

1. The specified PKI entity has been configured by using the **pki entity** command.
2. The common name of the PKI entity has been configured using the **common-name** command.

Precautions

A PKI realm can be bound to only one PKI entity.

Example

Bind the PKI entity **a** to the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki entity a
[HUAWEI-pki-entity-a] common-name test
[HUAWEI-pki-entity-a] quit
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] entity a
```

14.19.46 fingerprint

Function

The **fingerprint** command configures the CA certificate fingerprint used in CA certificate authentication.

The **undo fingerprint** command deletes the CA certificate fingerprint used in CA certificate authentication.

By default, no CA certificate fingerprint is configured for CA certificate authentication.

Format

fingerprint { **md5** | **sha1** | **sha256** } *fingerprint*

undo fingerprint

Parameters

Parameter	Description	Value
md5	Sets the digital fingerprint algorithm to MD5.	-
sha1	Sets the digital fingerprint algorithm to SHA1.	-
sha256	Sets the digital fingerprint algorithm to SHA256.	-

Parameter	Description	Value
fingerprint	Specifies the digital fingerprint value. This value needs to be obtained from the CA server offline. For example, from a CA server running Windows Server 2008, you can obtain the digital fingerprint at http://*host*:*port*/certsrv/mscep_admin/, in which *host* indicates the server's IP address and *port* indicates the port number.	The digital fingerprint value is a hexadecimal string of case-insensitive characters. ● An MD5 fingerprint consists of 32 characters (16 bytes). ● An SHA1 fingerprint consists of 40 characters (20 bytes). ● An SHA256 fingerprint consists of 64 characters (32 bytes).

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When obtaining a CA certificate, the device uses an algorithm to calculate the CA certificate fingerprint and compares the CA certificate fingerprint with the configured fingerprint. If the two values are the same, the device receives the CA certificate. When verifying a certificate, the device uses the public key of the CA certificate to authenticate the digital signature. If the digital signature can be decrypted, the certificate is verified.

Precautions

You can configure an algorithm to calculate the CA certificate fingerprint. If you run the **fingerprint** command multiple times in the same PKI realm view, only the latest configuration takes effect.

The MD5 and SHA1 algorithms have a low security level. SHA256 is recommended.

Example

Configure the CA certificate fingerprint used in CA certificate authentication.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
```

```
[HUAWEI-pki-realm-test] fingerprint sha256
e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
```

14.19.47 fqdn

Function

The **fqdn** command configures a fully qualified domain name (FQDN) for a PKI entity.

The **undo fqdn** command cancels the configuration.

By default, no FQDN is configured for a PKI entity.

Format

fqdn *fqdn-name*

undo fqdn

Parameters

Parameter	Description	Value
fqdn-name	Specifies the FQDN of a PKI entity.	The value is a string of 1 to 255 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an FQDN for the PKI entity, which is used as an alias of the entity.

An FQDN is the unique identifier of a PKI entity. It consists of a host name and a domain name, and can be translated into an IP address. A sample of an FQDN is www.example.com.

After the FQDN is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this FQDN. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the FQDN of the PKI entity.

Example

Set the FQDN to **example.com** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] fqdn example.com
```

14.19.48 ip-address

Function

The **ip-address** command configures an IP address for a PKI entity.

The **undo ip-address** command deletes the configuration.

By default, a PKI entity does not have an IP address.

Format

ip-address { *ipv4-address* | *interface-type interface-number* }

undo ip-address

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a PKI entity.	The value is in dotted decimal notation.
interface-type interface-number	Specifies an interface IP address of a PKI entity. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To facilitate applicant identification, configure an IP address for the PKI entity, which is used as an alias of the PKI entity.

After an IP address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this IP address. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device IP address.

Example

Set an IP address 10.1.1.1 for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] ip-address 10.1.1.1
```

14.19.49 key-usage

Function

The **key-usage** command configures the purpose description for a certificate public key.

The **undo key-usage** command deletes the purpose description of a certificate public key.

By default, a certificate public key does not have a purpose description.

Format

key-usage { **ike** | **ssl-client** | **ssl-server** } *

undo key-usage { **ike** | **ssl-client** | **ssl-server** } *

Parameters

Parameter	Description	Value
ike	Specifies the usage of a key as ike. That is, the key is used to set up an IPSec tunnel.	-
ssl-client	Specifies the usage of a key as ssl-client. That is, the key is used by the SSL client to set up an SSL session.	-
ssl-server	Specifies the usage of a key as ssl-server. That is, the key is used by the SSL server to set up an SSL session.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To improve certificate security, you can add the usage information of a key to the certificate request packet sent from the device to the CA server.

After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the usage information of the key.

For example, when setting up an SSL session, the SSL client adds a digital signature and encrypts the key by using the certificate. After you specify the usage of a key as ssl-client by using the **key-usage ssl-client** command, the certificate generated by the CA server carries the usage information, including a digital signature and encrypted key. If you use this key to encrypt data, the key will be invalid.

Example

Specify the usage of a key as ssl-client.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] key-usage ssl-client
```

14.19.50 locality

Function

The **locality** command configures a locality name for a PKI entity.

The **undo locality** command cancels the configuration.

By default, a PKI entity does not have a locality name.

Format

locality *locality-name*

undo locality

Parameters

Parameter	Description	Value
locality-name	Specifies the locality name of a PKI entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a locality name for the PKI entity, which is used as an alias of the entity.

After the locality name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this locality name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the locality name of the PKI entity.

Example

Set the locality name to **Beijing** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] locality Beijing
```

14.19.51 ocsp nonce enable

Function

The **ocsp nonce enable** command adds a nonce extension to the OCSP request sent by a PKI entity.

The **undo ocsp nonce enable** command cancels the configuration.

By default, the OCSP request sent by a PKI entity contains a nonce extension.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

ocsp nonce enable

undo ocsp nonce enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To improve security and reliability of communication between a PKI entity and OCSP server, this command adds a nonce extension (a random value) to the OSCP request sent by the PKI entity. If the nonce extension values on the PKI entity and OCSP server are different, communication fails.

Example

Add a nonce extension to the OCSP request sent by a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] ocsp nonce enable
```

14.19.52 ocsp signature enable

Function

The **ocsp signature enable** command enables the function of signing OCSP request packets.

The **undo ocsp signature enable** command disables the function of signing OCSP request packets.

By default, the function of signing OCSP request packets is disabled.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

ocsp signature enable

undo ocsp signature enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

When the certificate check mode is set to OCSP, the device sends OCSP request packets to the OCSP server. To improve access security, run the **ocsp signature enable** command to enable the function of signing OCSP request packets.

Example

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] ocsp signature enable
```

14.19.53 ocsp url

Function

The **ocsp url** command configures the Uniform Resource Locator (URL) address for an Online Certificate Status Protocol (OCSP) server.

The **undo ocsp url** command deletes the URL address of an OCSP server.

By default, an OCSP server does not have a URL address.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

ocsp url [**esc**] *url-address*

undo ocsp url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-address	Indicates the OCSP server's URL address.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP does not contain the AIA option, run this command to configure the OCSP server's URL. If the certificate contains the AIA option, run the **ocsp-url from-ca** command to configure the PKI entity to obtain OSCP server's URL from the AIA option.

The keyword **esc** supports the entering of URLs that include the question mark (?) in ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?). Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\\) to \x3f and enter **http://www.***.com\x3fpage1\\\\x3f**.

Example

Set the OCSP server's URL address to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] ocsp url http://10.1.1.1
```

14.19.54 ocsp-url from-ca

Function

The **ocsp-url from-ca** command configures a PKI entity to obtain the OCSP server's URL from the Authority Info Access (AIA) option in a CA certificate.

The **undo ocsp-url from-ca** command disables a PKI entity from obtaining the OCSP server's URL from the AIA option in a CA certificate.

By default, a PKI entity does not obtain OCSP server's URL from a CA certificate's AIA option.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

ocsp-url from-ca

undo ocsp-url from-ca

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP contains the AIA option, run this command to configure the PKI entity to obtain OSCP server's URL from the AIA option. If the certificate does not contain the AIA option, run the **ocsp url** command to configure the OCSP server's URL.

Example

Configure a PKI entity to obtain OCSP server's URL from a CA certificate's AIA option.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] ocsp-url from-ca
```

14.19.55 organization-unit

Function

The **organization-unit** command configures the department name for a PKI entity.

The **undo organization-unit** command restores the default setting.

By default, no department name is configured for a PKI entity.

Format

organization-unit *organization-unit-name*

undo organization-unit

Parameters

Parameter	Description	Value
organization-unit-name	Specifies the department name for a PKI entity.	The department name is a string of 1 to 31 case-sensitive characters. Names of departments are separated by commas (,). The total length of all department names ranges from 1 to 191. The characters can be letters, integers, apostrophe ('), equal sign (=), brackets (), plus sign (+), comma (,), minus sign (-), dot (.), slash (/), colon (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a department name for the PKI entity, which is used as an alias of the entity.

After the department name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this department name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the department name of the PKI entity.

Example

Configure the department name of a PKI entity to **Group1,Sale**.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] organization-unit Group1,Sale
```

14.19.56 organization

Function

The **organization** command configures a PKI entity's organization name.

The **undo organization** command deletes a PKI entity's organization name.

By default, a PKI entity does not have an organization name.

Format

organization *organization-name*

undo organization

Parameters

Parameter	Description	Value
organization-name	Specifies the organization name of a PKI entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an organization name for the PKI entity, which is used as an alias of the entity.

After the organization name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this organization name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the organization name of the PKI entity.

Example

Set the organization name of a PKI entity to **org1**.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] organization org1
```

14.19.57 password (PKI realm view)

Function

The **password** command sets the challenge password used for certificate application through SCEP, which is also used to revoke a certificate.

The **undo password** command deletes the challenge password used for certificate application through SCEP.

By default, no challenge password is configured.

Format

password cipher *password*

undo password

Parameters

Parameter	Description	Value
cipher *password*	Specifies the challenge password used for certificate application through SCEP. The password is displayed in ciphertext.	The value is a string of case-sensitive characters. It cannot contain question marks (?). *password* is in plaintext that contains 1 to 64 characters or in ciphertext that contains 48 to 108 characters. **NOTE** To improve communication security, it is recommended that the password contain at least three types of lowercase letters, uppercase letters, numerals, and special characters, and contain at least 8 characters.

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

When a PKI entity uses SCEP to apply for a certificate from a CA, the CA needs to verify the challenge password of the entity. The CA accepts the certificate application request only when the challenge password is correct. You need to run this command to set a challenge password for the PKI entity.

The challenge password is also used to revoke a certificate. It avoids misoperations in certificate revocation.

Example

Set the challenge password used to apply for certificate through SCEP.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] password cipher YsHsjx_202206
```

14.19.58 pki cmp certificate-request session

Function

The **pki cmp certificate-request session** command configures a device to send a certificate request (CR) to the CMPv2 server based on CMP session information.

Format

pki cmp certificate-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device has a certificate issued by a CA, the device can send a CR to apply for a certificate for another device.

After this command is executed, the system checks whether the configuration in the CMP session can be used for certificate application. If not, the system displays an error message. If so, the system initiates the CR according to the configuration. The obtained certificate is saved in a file on the CF card or Hda1, but not imported to the memory.

NOTE

The device does not support the message authentication code mode. If the CMP session mode is set to message authentication code, the system displays an error message.

Prerequisites

A CMP session has been created using the **pki cmp session** command.

Example

Send a CR to the CMPv2 server.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] quit
[HUAWEI] pki cmp certificate-request session test
 Info: Initializing configuration.
 Info: Creatting certification request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending certification request packet.
 Info: Waitting for certification response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

14.19.59 pki cmp initial-request session

Function

The **pki cmp initial-request session** command configures a device to send an initial request (IR) to the CMPv2 server based on CMP session information.

Format

pki cmp initial-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the command is executed, the system checks whether the configuration in the CMP session can be used for certificate application. If not, the system displays an error message. If so, the system performs an IR according to the configuration. The obtained certificate is saved in a file on the CF card or Hda1, but not imported to the memory. If the server issues the CA certificate during the response period, the CA certificate is also saved in a file.

Prerequisites

A CMP session has been created using the **pki cmp session** command.

Example

Send an IR to the CMPv2 server.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] quit
[HUAWEI] pki cmp initial-request session test
 Info: Initializing configuration.
 Info: Creatting initial request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending initial request packet.
 Info: Waitting for initial response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

14.19.60 pki cmp keyupdate-request session

Function

The **pki cmp keyupdate-request session** command configures a device to send a key update request (KUR) to the CMPv2 server based on CMP session information.

Format

pki cmp keyupdate-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device has a certificate issued by a CA, the device can send a KUR to update the certificate.

After the command is executed, the system checks whether the configuration in the CMP session can be used for certificate update application. If not, the system displays an error message. If so, the system initiates a KUR according to the configuration. The updated certificate is saved in a file on the device storage, but not imported to the memory.

NOTE

The device does not support the message authentication code mode. If the CMP session mode is set to message authentication code, the system displays an error message.

Prerequisites

A CMP session has been created using the **pki cmp session** command.

Example

Send a KUR to the CMPv2 server.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] quit
[HUAWEI] pki cmp keyupdate-request session test
 Info: Initializing configuration.
 Info: Creatting key update request packet.
 Info: Connectting to CMPv2 server.
 Error: CMPv2 server connect failed.
 Info: CMPv2 operation finish.
```

14.19.61 pki cmp session

Function

The **pki cmp session** command creates a CMP session and displays the CMP session view, or displays the view of an existing CMP session.

The **undo pki cmp session** command deletes a CMP session.

By default, no CMP session exists.

Format

pki cmp session *session-name*

undo pki cmp session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value is a string of 1 to 63 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before choosing CMPv2 for certificate application, run the **pki cmp session** command to create a CMP session. CMPv2 configuration is performed in the CMP session view.

Example

Create the CMP session **test** and enter the CMP session view.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test]
```

14.19.62 pki create-certificate

Function

The **pki create-certificate** command creates a self-signed certificate.

Format

pki create-certificate self-signed filename *file-name*

Parameters

Parameter	Description	Value
self-signed	Creates a self-signed certificate.	-
filename *file-name*	Specifies the name of a certificate file.	The value is a string of 1 to 64 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a self-signed certificate or local certificate is generated by the device, the certificate file is saved in the storage device as a PEM file. You can export the certificate for other devices to use. This simplifies certificate issue process.

When you run the **pki create-certificate** command, the system asks you to enter certificate information, for example, PKI entity parameters, certificate file name, certificate validity period, and RSA key length.

Precautions

The device does not provide lifecycle management for self-signed certificates. For example, self-signed certificates cannot be updated or revoked on the device. To ensure security of the device and certificates, a local certificate is recommended.

Example

Create a self-signed certificate **test**.

```
<HUAWEI> system-view
[HUAWEI] pki create-certificate self-signed filename test
```

14.19.63 pki delete replaced-file to recycle-bin enable

Function

The **pki delete replaced-file to recycle-bin enable** command moves overwritten files to the recycle bin.

The **undo pki delete replaced-file to recycle-bin enable** command cancels moving overwritten files to the recycle bin.

By default, overwritten files are permanently deleted.

Format

pki delete replaced-file to recycle-bin enable

undo pki delete replaced-file to recycle-bin enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Overwritten files are permanently deleted by default and cannot be restored. If you want to restore overwritten files in case that new files are unavailable, run the **pki delete replaced-file to recycle-bin enable** command to move these files to the recycle bin.

The **pki delete replaced-file to recycle-bin enable** command applies only to the following scenarios:

- The existing certificates have been overwritten using the **pki get-certificate** command.
- The existing certificates and CRL have been overwritten using the **pki http** command.
- The existing certificates have been overwritten using the **pki cmp initial-request session** command.
- The existing certificates have been overwritten using the **pki cmp certificate-request session** command.
- The existing certificates have been overwritten using the **pki cmp keyupdate-request session** command.
- The existing CRL has been overwritten using the **pki get-crl** command.
- The existing certificates have been overwritten using the **pki enroll-certificate** command.
- The existing certificates have been overwritten using the **pki create-certificate** command.
- The existing certificates have been overwritten using the **pki export-certificate** command.
- The existing RSA key pair has been overwritten using the **pki export rsa-key-pair** command.
- The existing certificates have been overwritten using the **pki import-certificate peer** command.
- The existing CRL has been overwritten using the **pki import-crl** command.
- The existing RSA key pair and certificates have been overwritten using the **pki import rsa-key-pair** command.

Example

Enable the function of moving overwritten files to the recycle bin.

```
<HUAWEI> system-view
[HUAWEI] pki delete replaced-file to recycle-bin enable
```

14.19.64 pki delete-certificate

Function

The **pki delete-certificate** command deletes a certificate from the memory.

Format

pki delete-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

NOTE

Only devices in NETCONF mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Deletes a CA certificate.	-
local	Deletes a local certificate.	-
ocsp	Deletes an Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the name of the PKI realm to which a certificate belongs.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the certificate expires or you want to apply for a new certificate, run this command to delete the CA certificate, OCSP server certificate, or local certificate from the memory.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

Deleting a certificate may interrupt certificate-related services.

Updating the security engine signature database requires the default_ca.cer certificate in the default domain. Therefore, if the security engine has been enabled using the **defence engine enable** command, deleting the certificate in the default domain will fail. To delete the certificate in the default domain, run the **update server** command to replace the certificate for updating the security engine signature database with another certificate.

Example

Delete the local certificate from the memory.

```
<HUAWEI> system-view
[HUAWEI] pki delete-certificate local realm abc
```

14.19.65 pki delete-crl

Function

The **pki delete-crl** command deletes a CRL from the memory.

Format

pki delete-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm that the certificate belongs to.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a CRL expires, run this command to delete a CRL file from the memory. This command will not delete the CRL files in storage card.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Example

Delete the CRL of PKI realm **abc** from the memory.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
```

```
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki delete-crl realm abc
```

14.19.66 pki enroll-certificate

Function

The **pki enroll-certificate** command configures manual certificate enrollment.

Format

pki enroll-certificate realm *realm-name* [**pkcs10** [**filename** *filename*]] [**password** *password*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of a PKI realm.	The PKI realm name must already exist.
pkcs10	Uses the PKCS#10 format to display the local certificate request information. It can be used to request certificates in offline mode.	-
filename *filename*	Saves the certificate request information in a specified file. The certificate request information is saved in the file in PKCS#10 format and is sent to the CA in outband mode.	The value is a string of 1 to 64.

Parameter	Description	Value
password *password*	Indicates a challenge password, which is used to request certificates in online mode. When the CA server processes the certificate request using the challenge password, you must set a challenge password on the entity, and the challenge password must be the same as the password configured on the CA server.	The value is a string of case-sensitive characters without question marks (?) or spaces. It can be a plain-text string of 1 to 64 characters or a cipher-text string of 48 to 108 characters. **NOTE** To improve certificate security, it is recommended that a password consist of at least two of the following: lowercase letters, uppercase letters, numerals and special characters. In addition, the password must contain at least eight characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Manual certificate application is online or offline.

- Online mode (in-band mode)

  The device requests certificates online by communicating with the CA server through SCEP. Then the device stores the obtained certificates on the flash.

- Offline mode (outband mode)

  The device generates a certificate request file. The administrator sends the file to the CA server using methods such as disks and emails.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

- If **pkcs10** is specified, an entity applies to a CA for a certificate in offline mode. The entity saves the certificate request information in a file in PKCS#10 format and sends the file to the CA in outband mode.
- If **pkcs10** is not specified, an entity applies to a CA for a certificate in online mode.

- In online mode, a PKI entity obtains a CA certificate and imports it to memory, and then obtains a local certificate and imports it to memory.
- After the **enrollment self-signed** command is used in the PKI realm, it is not allowed to use the **pki enroll-certificate** command to configure manual certificate enrollment.

Example

Enroll a certificate for the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki enroll-certificate realm abc
```

14.19.67 pki entity

Function

The **pki entity** command creates a PKI entity and displays the PKI entity view, or displays the view of an existing PKI entity.

The **undo pki entity** command deletes a PKI entity.

By default, no PKI entity is configured.

Format

pki entity *entity-name*

undo pki entity *entity-name*

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value is a string of 1 to 64 case-sensitive characters without spaces or slashes (/).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A PKI entity refers to the applicant or user of a certificate. A PKI entity is required when you use PKI features. After a PKI entity is created, you can configure attributes for it, for example, common name, country code, email address, FQDN, IP address, geographic area, organization, department, state, and province. These attributes include identity information of the PKI entity. The identity information will be added to the subject of a PKI entity.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Example

Configure a PKI entity **entity1** and enter the PKI entity view.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1]
```

14.19.68 pki export-certificate

Function

The **pki export-certificate** command exports a certificate to the device storage.

Format

pki export-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name* { **pem** | **pkcs12** }

NOTE

Only devices in NETCONF mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Exports a CA certificate.	-
local	Exports a local certificate.	-
ocsp	Exports the Online Certificate Status Protocol (OCSP) certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate.	The PKI realm name must already exist.
pem	Exports a certificate in PEM format.	-
pkcs12	Exports a certificate in P12 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To copy a certificate to another device, run the **pki export-certificate** command to export a certificate to the flash of the local device first, and then transfer the certificate to another device using a file transfer protocol.

Before using this command, run the **display pki certificate** command to view information about certificates on the device.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

When the exported certificate file does not contain a private key, the device does not encrypt this file.

If the exported certificate is in PEM format, you need to install the WEAKEA plug-in to export the certificate containing a private key. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

When you export the private key, the system asks you to enter the private key file name. If the private key file name and the certificate file name are the same, the private key and certificate are stored in the same file. If they are different, they are stored in different files.

When you export the private key, the system asks you to enter the private key file format and set the password. The password will be used when you run the **pki import-certificate** command to import this private key.

After the **enrollment self-signed** command is used in the PKI realm, you cannot use the **pki export-certificate** command to export certificates to files.

Example

Export the local certificate in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki export-certificate local realm abc pem
 Please enter the name of certificate file <length 1-127>: aa
 If you only export the certificate, do not export the private key.
 You can directly enter empty of private key file.
 Please enter the name of private key file <length 1-127>:
 Info: Succeeded in exporting the certificate.
```

14.19.69 pki export rsa-key-pair

Function

The **pki export rsa-key-pair** command exports the RSA key pair to the flash and allows the export of the associated certificate.

Format

pki export rsa-key-pair *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* **aes** | **pkcs12** *file-name* } **password** *password*

NOTE

The **pem** *file-name* parameter is supported only when the WEAKEA plug-in is installed. For details about how to install the WEAKEA plug-in, see "WEAKEA Configuration" in the *CLI-based Configuration Guide*.

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value must be an existing RSA key pair name.
and-certificate *certificate-name*	Indicates that the certificate related to the RSA key pair are exported.	The value must be an existing certificate file name.
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.

Parameter	Description	Value
aes	Sets the encryption algorithm to AES if a file is exported in the PEM format. The default value is AES.	-
password *password*	Specifies the encryption password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 8 to 32 case-sensitive characters without question marks (?). For security purposes, a password must meet the minimum strength requirements, that is, the password needs to contain at least three types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To transfer or back up an RSA key pair, run this command to generate the PEM or PKCS12 file carrying this RSA key pair (which may include the certificate) in the flash.

Before using this command, run the **display pki rsa local-key-pair** command to view information about the RSA key pairs on the device.

Prerequisites

The RSA key pair has been created and configured to be exportable using the **pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **pki import rsa-key-pair** command.

Precautions

The RSA key pair is sensitive information. Delete and destroy the exported RSA key pair on the device or storage device immediately after you do not need it.

The system software does not contain the **3des** and **des** parameters. To use these parameters, you need to install the WEAKEA plug-in. However, this algorithm is less secure. For security purposes, you are advised to use other algorithms.

Example

Export the RSA key pair **key1** in PEM format to the **aaa.pem** file with the AES encryption mode after installing the WEAKEA plug-in.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create key1 exportable
 Info: The name of the new key-pair will be: key1
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
......+++
...................+++
[HUAWEI] pki export rsa-key-pair key1 pem aaa.pem aes password YsHsjx_202206
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting the RSA key pair in PEM format.
```

14.19.70 pki file-format

Function

The **pki file-format** command sets the format for the saved certificate request, certificate, and CRL.

By default, the device stores certificate request, certificate, and CRL in PEM format.

Format

pki file-format { **der** | **pem** }

Parameters

Parameter	Description	Value
der	Indicates that the format of a certificate request file is DER.	-
pem	Indicates that the format of a certificate request file is PEM.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the format for the saved certificate request, certificate, and CRL, for example, to use the certificate and CRL obtained through CMPv2, SCEP, run the **pki file-format** command.

However, the certificate and CRL obtained through HTTP are downloaded directly and are not saved in the format configured using this command. The created self-signed certificate or local certificate can only be saved in PEM format.

Example

Set the format of saved certificate request, certificate, and CRL to DER.

```
<HUAWEI> system-view
[HUAWEI] pki file-format der
```

14.19.71 pki get-certificate

Function

The **pki get-certificate** command downloads a certificate to the device storage.

Format

pki get-certificate ca realm *realm-name*

Parameters

Parameter	Description	Value
ca	Specifies a CA or RA certificate to be obtained.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be obtained.	The value must be an existing PKI realm name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you request a local certificate for the PKI entity through SCEP, run this command to download a CA certificate to the device storage, and request a local certificate using the encrypted CA public key.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

After obtaining a CA certificate, the device automatically imports the certificate to the device memory.

If the same certificate exists on the device, delete the existing one; otherwise, the certificate cannot be obtained.

Example

Obtain the CA certificate in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki get-certificate ca realm abc
```

14.19.72 pki get-crl

Function

The **pki get-crl** command updates CRL immediately.

Format

pki get-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of the CRL.	The value must be an existing PKI realm name, which is a string of 1 to 52 case-insensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CRL status is checked periodically when it is updated automatically. If the CRL on the device is likely to expire, configure this command to update CRL immediately.

After this command is executed, the new CRL replaces the old CRL in the storage, and is automatically imported to the memory to replace the old one.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Example

Configure CRL immediate update.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] quit
[HUAWEI] pki get-crl realm test
```

14.19.73 pki http

Function

The **pki http** command configures a device to use HTTP to download a CA certificate, local certificate, or CRL.

Format

pki http [**esc**] *url-address save-name*

Parameters

Parameter	Description	Value
esc	Specifies the URL in ASCII code.	-
url-address	Specifies the URL of the CA certificate, local certificate, or CRL.	The value is a string of 1 to 128 case-sensitive characters.
save-name	Specifies the name of a CA certificate, local certificate, or CRL saved on the flash of the device.	The value is a string of 1 to 64 case-insensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Before you configure a device to use HTTP to download a CA certificate, local certificate, or CRL, ensure that the flash of the device has enough space to accommodate the CA certificate, local certificate, or CRL.

The keyword **esc** supports the entering of URLs that include the question mark (?) in ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?). Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\\) to **\x3f** and enter **http://www.***.com\x3fpage1\\\x3f**.

Example

Configure a device to use HTTP to download a local certificate.

```
<HUAWEI> system-view
[HUAWEI] pki http http://10.1.1.1/test.cer local.cer
```

Configure a device to use HTTP to download a local certificate.

```
<HUAWEI> system-view
[HUAWEI] pki http esc http://www.***.com\x3fpage1\\x3f local.cer
```

14.19.74 pki import-certificate

Function

The **pki import-certificate** command imports a certificate to the device memory.

Format

pki import-certificate { **ca** | **local** } **realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] [**replace**] [**no-check-validate**] [**no-check-hash-alg**]

pki import-certificate { **ca** | **local** } **realm** *realm-name* **pkcs12 filename** *filename* [**no-check-validate**] [**no-check-hash-alg**] **password** *password*

pki import-certificate ocsp realm *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*]

pki import-certificate ocsp realm *realm-name* **pkcs12 filename** *filename* **password** *password*

NOTE

Only devices in NETCONF mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Imports a CA certificate. For example, when the device works as an SSL proxy, import the SSL proxy CA certificate and use the private key in the certificate to sign the SSL client certificate again.	-
local	Imports a local certificate.	-
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The PKI realm name must already exist. **NOTE** The domain name cannot contain spaces. Otherwise, the certificate cannot be imported.
der	Imports a certificate in DER format.	-
pkcs12	Imports a certificate in PKCS12 format.	-
pem	Imports a certificate in PEM format.	-
filename *filename*	Specifies the name of the imported certificate.	The file name must already exist.
replace	Deletes the original certificate and RSA key pair and imports the new certificate when there are repeated certificates in the domain. **NOTE** If the RSA key pair of the original certificate is not referenced by other domains, the certificate and key pair are deleted. If the RSA key pair of the original certificate is referenced by other domains or a CMP session, only the original certificate is deleted but the key pair is not deleted.	-
no-check-validate	Indicates whether to perform validity check on the validity period of the imported certificate.	-
no-check-hash-alg	Indicates whether to check the hash algorithm used for the signature of the imported certificate.	-
ocsp	Imports the Online Certificate Status Protocol (OCSP) server's certificate.	-

Parameter	Description	Value
password *password*	Specifies the decryption password of the certificate. The password is the same as the password configured using the **pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a certificate is saved to the storage, run this command to import the certificate to the memory for it to take effect.

The device supports the following certificate import modes:

- terminal: Import or copy the certificate file of the peer to the local device. That is, you can open the PEM certificate file using a text tool and copy the certificate content to the local device.
- file: The **filename** parameter is specified to import the certificate file of the peer.

Multiple certificates can be imported on the device, including the CA certificate, local certificate, and private key.

NOTE

If you do not know the format of the certificate you want to import, configure each format in turn and check whether the certificate is successfully imported.

Prerequisites

The PKI realm has been created using the **pki realm (system view)** command, and the certificate file already exists on the storage device.

Precautions

If a certificate file contains a key pair file, the **pki import-certificate** command imports only the certificate file, but not the key pair file. To import the key pair file, run the **pki import rsa-key-pair** command after the **pki import-certificate** command, or run the **pki import rsa-key-pair** command to import the certificate and key pair files simultaneously.

It is not recommended that multiple local certificates be imported into the same PKI realm. Otherwise, certificate-related services may use the certificates that do not match the services, causing services to become unavailable.

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_local.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported should be less than 50 characters, so the total certificate file name does not exceed 64 characters, and the certificate file cannot be imported to the storage component.

The device supports the import of digital certificates generated through the RSA encryption algorithm or SM2 key hash algorithm.

Example

Import a local certificate to the PKI realm **abc** in file transfer mode.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki import-certificate local realm abc pem filename local.cer
 Info: Succeeded in importing the certificate.
```

14.19.75 pki import-certificate peer

Function

The **pki import-certificate peer** command imports a certificate of the remote device to the device memory.

Format

pki import-certificate peer *peer-name* { **der** | **pem** | **pkcs12** } **filename** [*filename*]

pki import-certificate peer *peer-name* **pkcs12 filename** *filename* **password** *password*

Parameters

Parameter	Description	Value
peer-name	Specifies the name of a peer certificate. A certificate cannot be imported to multiple peers.	The value is a string of 1 to 32 case-insensitive characters without spaces. If the character string is enclosed in double quotation marks, it can contain spaces.
der	Imports a certificate of the remote device in DER format.	-
pem	Imports a certificate of the remote device in PEM format.	-

Parameter	Description	Value
pkcs12	Imports a certificate of the remote device in P12 format.	-
filename *filename*	Imports a certificate of the remote device in file mode.	The value is an existing certificate name of the remote device.
password *password*	Specifies the decryption password of the certificate. The password is the same as the password configured using the **pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Where digital envelop authentication is used, configure the public key of the remote device. The public key can be obtained from the public and private key management module or certificate of the remote device.

Prerequisites

The certificate file of the remote device must already exist on the storage device.

Precautions

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported cannot exceed 50 characters. Otherwise, the total certificate file name will exceed 64 characters, and the certificate file cannot be imported to the storage component.

You can import a peer certificate generated using the RSA encryption algorithm or SM2 key hash algorithm to the device.

Example

Import the certificate **aa.pem** of the remote device in the file mode.

```
<HUAWEI> system-view
[HUAWEI] pki import-certificate peer abcd pem file aa.pem
 Info: Succeeded in importing the peer certificate.
```

14.19.76 pki import-crl

Function

The **pki import-crl** command imports the CRL to the memory.

Format

pki import-crl realm *realm-name* **filename** *file-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name.	The value must be an existing PKI realm name.
filename *file-name*	Specifies the name of an imported certificate or CRL file. The certificates only support PEM and DER formats.	The value must be an existing certificate or CRL file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the CRL that is obtained in out-of-band mode or is updated manually, run this command to import the CRL to the memory.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command and the CRL file has been downloaded using HTTP.

Example

Import the CRL in the PKI realm to the memory.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
```

```
[HUAWEI] pki http esc http://www.***.com\x3fpage1\\x3f abc.crl
[HUAWEI] pki import-crl realm abc filename abc.crl
```

14.19.77 pki import rsa-key-pair

Function

The **pki import rsa-key-pair** command imports the RSA key pair to the device memory.

Format

pki import rsa-key-pair *key-name* [**include-cert realm** *realm-name*] { **pem** | **pkcs12** } *file-name* [**exportable**] [**password** *password*]

pki import rsa-key-pair *key-name* **der** *file-name* [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is enclosed in double quotation marks (" "), the character string can contain spaces.
include-cert	Indicates that the certificates in the file will be imported.	-
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The value must be an existing PKI realm name.
pem *file-name*	Indicates that the RSA key pair to be imported is in the PEM format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
pkcs12 *file-name*	Indicates that the RSA key pair to be imported is in the PKCS12 format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.

Parameter	Description	Value
der *file-name*	Indicates that the RSA key pair to be imported is in the DER format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
exportable	Indicates that the imported RSA key pair can be exported.	-
password *password*	Specifies the decryption password of the RSA key pair. The password is the same as the password configured using the **pki export rsa-key-pair** command.	The value must be the name of an existing decryption password of the RSA key pair. **NOTE** If the RSA key pair file does not have a decryption password, you need to enter any character. Otherwise, the import will fail.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to use the RSA key pair generated by other entities. After the configuration, the imported RSA key pair can be referenced by the PKI module for operations such as signing.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

If you do not know the format of the key pair you want to import, configure each format in turn and check whether the key pair is successfully imported.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

Import the RSA key pair **aaa.pem**. In the system, the RSA key pair is named **key-1**, is marked **exportable** and has the decryption password YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] pki import rsa-key-pair key-1 pem aaa.pem exportable password YsHsjx_202206
 Info: Succeeded in importing the RSA key pair in PEM format.
```

14.19.78 pki key enhance enable

Function

The **pki key enhance enable** command enables the PKI module to use the enhanced key algorithm for encryption and decryption.

The **undo pki key enhance enable** command disables the PKI module from using the enhanced key algorithm for encryption and decryption.

By default, the PKI module is enabled to use the enhanced key algorithm for encryption and decryption.

Format

pki key enhance enable

undo pki key enhance enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In V200R020C00SPC300 and later versions, the PKI module uses the enhanced key algorithm for encryption and decryption by default. The enhanced key algorithm is incompatible with the key algorithm used by the PKI module in versions earlier than V200R020C00SPC300. Therefore, before downgrading a device from V200R020C00SPC300 or a later version to a version earlier than V200R020C00SPC300, run the **undo pki key enhance enable** command to disable this function so that the PKI module uses the same key algorithm before and after the device downgrade, ensuring service continuity.

Precautions

When a device is upgraded from a version earlier than V200R020C00SPC300 to V200R020C00SPC300 or a later version, the **undo pki key enhance enable** command is automatically added to the configuration file of the device to ensure upgrade compatibility.

Example

Before a device is downgraded from V200R020C00SPC300 or a later version to a version earlier than V200R020C00SPC300, disable the PKI module from using the enhanced key algorithm for encryption and decryption so that the key algorithms before and after the downgrade are the same.

```
<HUAWEI> system-view
[HUAWEI] undo pki key enhance enable
 Warning: The current operation has security risks. You are not advised to perform this operation.
```

14.19.79 pki match-rsa-key

Function

The **pki match-rsa-key** command configures a device to search for the RSA key pair associated with a specific certificate.

Format

pki match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
certificate-filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to check the RSA key pair corresponding to a certificate. After configuration, the system searches for all the local RSA key pairs, compares them with the specified certificate and outputs the matched RSA key pair name once it is searched out.

Example

Configure a device to search for the RSA key pair that matches the certificate file **local.cer**.

```
<HUAWEI> system-view
[HUAWEI] pki match-rsa-key certificate-filename local.cer
 Info: The file local.cer contains certificates 1.
 Info: Certificate 1 from file local.cer matches RSA key rsa2.key.
```

14.19.80 pki ocsp response cache enable

Function

The **pki ocsp response cache enable** command enables a PKI entity to cache OCSP responses.

The **undo pki ocsp response cache enable** command disables a PKI entity from caching OCSP responses.

By default, OCSP response caching is disabled on a PKI entity.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

pki ocsp response cache enable

undo pki ocsp response cache enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After you enable a PKI entity to cache OCSP responses, the PKI entity first searches its cache for the certificate revocation status. If the search fails, the PKI entity sends a request to the OCSP server. In addition, the PKI entity caches valid OCSP responses for subsequent query. OCSP responses have a validity period. With OCSP response caching enabled, a PKI entity refreshes the cached OCSP responses every minute to clear expired OCSP responses.

Example

Enable a PKI entity to cache OCSP responses.

```
<HUAWEI> system-view
[HUAWEI] pki ocsp response cache enable
```

14.19.81 pki ocsp response cache number

Function

The **pki ocsp response cache number** command sets the maximum number of OCSP responses that can be cached on a PKI entity.

The **undo pki ocsp response cache number** command restores the default maximum number of OCSP responses that can be cached on a PKI entity.

By default, the maximum number of OCSP responses that can be cached on a PKI entity is 2.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

pki ocsp response cache number *number*

undo pki ocsp response cache number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of OCSP responses that can be cached on a PKI entity.	The value is an integer in the range from 1 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

A PKI entity caches valid OCSP responses for subsequent query. If the number of cached OCSP responses reaches the value specified by *number*, the PKI entity stops caching OCSP responses.

Example

Set the maximum number of OCSP responses that can be cached on a PKI entity to 3.

```
<HUAWEI> system-view
[HUAWEI] pki ocsp response cache number 3
```

14.19.82 pki ocsp response cache refresh interval

Function

The **pki ocsp response cache refresh interval** command sets the interval at which the OCSP response cache is refreshed.

The **undo pki ocsp response cache refresh interval** command restores the default interval at which a PKI entity refreshes the OCSP response cache.

By default, the interval at which a PKI entity refreshes the OCSP response cache is 5 minutes.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

pki ocsp response cache refresh interval *interval*

undo pki ocsp response cache refresh interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the OCSP response cache is refreshed.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

A PKI entity refreshes the OCSP response cache periodically and deletes the OCSP responses that have expired based on the *interval* value.

Example

Set the interval at which the OCSP response cache is refreshed to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] pki ocsp response cache refresh interval 30
```

14.19.83 pki realm (system view)

Function

The **pki realm** command creates a PKI realm and displays the PKI realm view, or displays the view of an existing PKI realm.

The **undo pki realm** command deletes a PKI realm.

By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

Format

pki realm *realm-name*

undo pki realm *realm-name*

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces or slashes (/).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PKI realm is a set of identity information required when a PKI entity enrolls a certificate.

Precautions

A PKI realm configured on a device is unavailable to certificate authorities (CAs) or other devices.

When a certificate is requested using a PKI realm, the system names the certificate file *PKI realm name***_local.cer**. Therefore, ensure that the name of a created PKI realm does not exceed 50 characters. Otherwise, the certificate file name may exceed 64 characters and cannot be saved on a storage device.

The name of a CRL file requested using a PKI realm is suffixed with .crl. Therefore, ensure that the name of a created PKI realm does not exceed 52 characters. Otherwise, the CRL file name may exceed 64 characters and cannot be saved on a storage device.

Example

Create a PKI realm named **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc]
```

14.19.84 pki release-certificate peer

Function

The **pki release-certificate peer** command releases a certificate of the remote device.

Format

pki release-certificate peer { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate to be released.	The value must be an existing peer certificate file name.
all	Releases all certificates of the remote device.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the specified certificate of the remote device is not required, run the **pki release-certificate peer** command to release the certificate of the remote device.

Before using this command, run the **display pki peer-certificate** command to view the certificate information of the remote device.

Prerequisites

The **pki import-certificate peer** command has been used to import the certificate of the remote device.

Example

Release the certificate **test** of the remote device.

```
<HUAWEI> system-view
[HUAWEI] pki release-certificate peer name test
 Info: Succeeded in releasing the peer certificate.
```

14.19.85 pki rsa local-key-pair create

Function

The **pki rsa local-key-pair create** command creates the specified RSA key pair.

Format

pki rsa local-key-pair create *key-name* [**modulus** *modulus-size*] [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be created.	The value is a string of 1 to 64 case-sensitive characters without question marks (?) and spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
modulus *modulus-size*	Specifies the size of the RSK key pair.	The value is an integer that ranges from 3072 to 4096. The default value is 3072. After the WEAKEA plug-in is installed, the value is an integer that ranges from 2048 to 4096. A key of less than 3072 bits has security risks. You are advised to use a key of 3072 bits or more.
exportable	Indicates that the new RSA key pair can be exported from the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a PKI entity requests a certificate from the CA, the certificate enrollment request that it sends contains information such as the public key. Run this command to create the RSA key pair for the certificate request.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Precautions

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_localx.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

The RSA key pair referenced by PKI realms cannot be overwritten. They can be overwritten only after the reference relationship is removed.

If the name of the new RSA key pair is the same as that of a pair on the device, the system prompts the user to decide whether to overwrite the existing pair.

Example

Create 4096-bit RSA key pair **test**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 3072 to 4096.
 Input the bits in the modules:4096
 Generating key-pairs...
......+++
.......+++
```

14.19.86 pki rsa local-key-pair destroy

Function

The **pki rsa local-key-pair destroy** command deletes the specified RSA key pair.

Format

pki rsa local-key-pair destroy *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be deleted.	The value must be the name of an existing key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It is recommended that you run this command to destroy the specified RSA key pair if it is leaked, damaged, unused, or lost.

After this command is executed, the specified RSA key pair is deleted from the active device and the standby device.

Prerequisites

The RSA key pair has been created using the **pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **pki import rsa-key-pair** command.

Precautions

The RSA key pair in the creation process cannot be deleted.

The RSA key pair referenced by a PKI realm or CMP session cannot be deleted. They can be deleted only after the reference relationship is removed.

Example

Delete the RSA key pair **test**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
```

```
.........................+++
[HUAWEI] pki rsa local-key-pair destroy test
 Warning: The name of the key pair to be deleted is test.
 Are you sure you want to delete the key pair? [y/n]:y
 Info: Delete RSA key pair success.
```

14.19.87 pki set-certificate expire-prewarning

Function

The **pki set-certificate expire-prewarning** command sets the expiration warning date for the local certificate and the CA certificate in the memory.

The **undo pki set-certificate expire-prewarning** command restores the default expiration warning date for the local certificate and the CA certificate in the memory.

By default, the expiration warning date for the local certificate and the CA certificate in the memory is 90 days.

Format

pki set-certificate expire-prewarning *day*

undo pki set-certificate expire-prewarning

Parameters

Parameter	Description	Value
day	Specifies the expiration warning date.	The value is an integer that ranges from 7 to 180. By default, the value is 90.

Views

System view

Default Level

3: Management level

Usage Guidelines

After this command is executed, you will be prompted the expiration of a certificate in advance. If the system detects that a certificate in the memory is to expire in less than *day*, the device sends an expiration warning to the user.

Example

Set the expiration warning date for the local certificate and the CA certificate in the memory as 30 days.

```
<HUAWEI> system-view
[HUAWEI] pki set-certificate expire-prewarning 30
```

14.19.88 pki validate ocsp-server-certificate enable

Function

The **pki validate ocsp-server-certificate enable** command enables the function that uses the OCSP server certificate to verify OCSP server packets.

The **undo pki validate ocsp-server-certificate enable** command disables the function that uses the OCSP server certificate to verify OCSP server packets.

By default, the function that uses the OCSP server certificate to verify OCSP server packets is enabled.

Format

pki validate ocsp-server-certificate enable

undo pki validate ocsp-server-certificate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For security purposes, you are advised to enable the function that uses the OCSP server certificate to verify OCSP server packets. If OCSP server packets fail the verification, the device discards these packets.

Precautions

If the imported OCSP server certificate is not the correct one, OCSP server packets fail the verification, causing the local certificate to become unavailable. To prevent this problem, import the correct OCSP server certificate. If no OCSP server certificate can be obtained, run the **undo pki validate ocsp-server-certificate enable** command to disable the function that uses the OCSP server certificate to verify OCSP server packets.

Example

Enable the function that uses the OCSP server certificate to verify OCSP server packets.

```
<HUAWEI> system-view
[HUAWEI] pki validate ocsp-server-certificate enable
```

14.19.89 pki validate-certificate

Function

The **pki validate-certificate** command allows you to verify the validity of a CA certificate or a local certificate.

Format

pki validate-certificate { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Checks validity of the CA certificate.	-
local	Checks validity of the local certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an end entity verifies a peer certificate, it checks the status of the peer certificate. For example, the end entity checks whether the peer certificate has expired and whether the certificate is in a CRL.

To verify the validity of a CA certificate or a local certificate, run the **pki validate-certificate** command.

Prerequisites

A PKI realm has been configured using the **pki realm (system view)** command.

Precautions

The **pki validate-certificate ca** command allows you to verify only the root CA certificate, but not subordinate CA certificates. When multiple CA certificates are imported on a device, you can use only the **pki validate-certificate local** command to verify the validity of subordinate certificates.

Example

Configure the device to check validity of the local certificate using CRL.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] certificate-check crl
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki validate-certificate local realm abc
 Info: It will take a few seconds or more to validate specified certificate. Please wait a moment.
 Info: Local encryption certificate is valid.
 Info: It will take a few seconds or more to validate specified certificate. Please wait a moment.
 Info: Local signature certificate is valid.
```

14.19.90 reset pki cmp statistics

Function

The **reset pki cmp statistics** command clears the statistics on CMP sessions.

Format

reset pki cmp statistics [**session** *session-name*]

Parameters

Parameter	Description	Value
session *session-name*	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

If a CMP session is specified, this command will clear the statistics of the session. If no CMP session is specified, this command will clear the statistics of all sessions.

Example

Clear statistics on the CMP session **test**.

```
<HUAWEI> reset pki cmp statistics session test
```

14.19.91 reset pki ocsp response cache

Function

The **reset pki ocsp response cache** command resets an OCSP response cache.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

reset pki ocsp response cache

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The PKI entity caches valid OCSP responses for future searches. If the number of cached OCSP responses reaches the maximum value, no more OCSP responses can be cached. To ensure that the latest OCSP responses can be cached, you can run this command to clear the OCSP response cache first.

Example

Reset an OCSP response cache.

```
<HUAWEI> reset pki ocsp response cache
```

14.19.92 reset pki ocsp server down-information

Function

The **reset pki ocsp server down-information** command clears Down state information of the OCSP server recorded on the device.

NOTE

This command is available only on NETCONF-supporting switch models.

Format

reset pki ocsp server down-information [**url** [**esc**] *url-addr*]

Parameters

Parameter	Description	Value
url [**esc**] *url-addr*	Specifies the OCSP server's URL address. If no URL address is specified, clear Down state information of all OCSP servers. If the **esc** parameter is specified, the URL address in ASCII format is supported.	The value is a string starting with http:// and consisting of 1 to 128 case-sensitive characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is Down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to Down. In this case, the device will not send OCSP requests to the URL within 10 minutes. However, this mechanism may falsely set the state of a transiently disconnected server to Down. Using this command, the user can manually clear the falsely reported Down state of the OCSP server so that the device can send OCSP requests to the server.

The keyword **esc** supports the entering of URLs that include the question mark (?) in ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Clear the OCSP server Down information of the specified URL.

```
<HUAWEI> reset pki ocsp server down-information
```

14.19.93 rsa local-key-pair

Function

The **rsa local-key-pair** command configures the RSA key pair used to request a certificate using SCEP or in offline mode.

The **undo rsa local-key-pair** command deletes the RSA key pair used to request a certificate using SCEP or in offline mode.

By default, the system does not configure the RSA key pair used to request a certificate using SCEP or in offline mode.

Format

rsa local-key-pair *key-name*

undo rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PKI entity that requests a certificate from the CA using SCEP or in offline PKCS#10 mode must contain a public key. Run this command to configure the RSA key pair.

Prerequisites

The RSA key pair for certificate application has been created using the **pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **pki import rsa-key-pair** command.

Precautions

- An RSA key pair can be referenced by only one PKI realm.

Example

Configure the RSA key pair that is referenced by the PKI realm **test**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.........................+++
```

```
.................................................................................
........+++
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] rsa local-key-pair test
```

14.19.94 serial-number

Function

The **serial-number** command adds the serial number of a device to a PKI entity.

The **undo serial-number** command restores the default setting.

By default, the serial number of a device is not added to a PKI entity.

Format

serial-number

undo serial-number

Parameters

None

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To further identify the applicant, add the serial number of the device to the PKI entity.

After the serial number of the device is added to a PKI entity, the certificate request packet sent by the device to the CA server carries this serial number. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device serial number.

Example

Add the serial number of the device to a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] serial-number
```

14.19.95 source

Function

The **source** command configures the source address used in TCP connection setup.

The **undo source** command restores the default setting.

By default, the device uses an outbound interface's IP address as the source IP address used in TCP connection setup.

Format

source { **interface** *interface-type interface-number* | *ip-address* }

undo source

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface's IP address as the source IP address used in TCP connection setup. - *interface-type* indicates the interface type. - *interface-number* indicates the interface number.	-
ip-address	Specifies the source address used in TCP connection setup.	An IPv4 address is in dotted decimal notation, whereas an IPv6 address is in colon-separated hexadecimal notation. **NOTE** The CMP session view does not support the configuration of an IPv6 address. The value is in dotted decimal notation.

Views

PKI realm view or CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device needs to establish a TCP connection with an SCEP or OCSP server, you must run the **source** command to specify the source IP address used in TCP connection setup.

In the multi-output scenario, if the interfaces for sending and receiving a TCP packet are different, the IP address in the received TCP packet is different from the IP address of the receiving interface. Then the TCP packet is dropped, and the TCP connection is torn down. In this situation, you can run this command to specify the loopback interface address.

Precautions

If the source interface used in TCP connection setup has been specified, the source interface must be a Layer 3 interface with an IP address configured.

The VPN instance bound to the interface specified by the **source interface** command in the CMP session view must be the same as the VPN instance configured in the **vpn-instance**. If they are inconsistent, either **source interface** or **vpn-instance**, which is configured later, cannot be executed successfully.

Example

Configure the IP address of VLANIF 100 as the source address used in TCP connection setup.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.136.2.25 24
[HUAWEI-Vlanif100] quit
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] source interface vlanif 100
```

14.19.96 state (PKI entity view)

Function

The **state** command configures a state or province name for a PKI entity.

The **undo state** command deletes the configuration.

By default, no state or province name is configured for a PKI entity.

Format

state *state-name*

undo state

Parameters

Parameter	Description	Value
state-name	Specifies the state or province name of a PKI entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a state or province name for a PKI entity.

After the state or province name is configured for a PKI entity, the certificate request packet sent by the device to the CA server contains this province name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the state or provision name of the PKI entity.

Example

Configure the province name to **Jiangsu** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] state Jiangsu
```

14.19.97 undo pki cmp poll-request session

Function

The **undo pki cmp poll-request session** command cancels CMP polling requests.

Format

undo pki cmp poll-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the server cannot deliver the results immediately after the client initiates certificate-related requests, the server requires the client to send the requests in polling mode until the server deliver the final result. The process duration varies with the actual situation. To cancel the process, run the command. Then the certificate-related request is also canceled.

Prerequisites

A CMP session has been created using the **pki cmp session** command.

Example

Cancel CMP polling requests.

```
<HUAWEI> system-view
[HUAWEI] pki cmp session test
[HUAWEI-pki-cmp-session-test] quit
[HUAWEI] undo pki cmp poll-request session test
```

14.19.98 vpn-instance

Function

The **vpn-instance** command adds a PKI realm to a specified VPN.

The **undo vpn-instance** command unbinds a PKI realm from a specified VPN.

By default, a PKI realm is not added to any VPN.

Format

PKI realm view

vpn-instance *vpn-instance-name*

undo vpn-instance

CMP session view

vpn-instance { **vpn-name** *vpn-instance-name* }

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

PKI realm view or CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain and verify certificates, the device needs to communicate with the CA or SCEP server. When the CA or SECP server is in a VPN, add the PKI realm to the specified VPN.

Prerequisites

1. A VPN instance has been created using the **ip vpn-instance** command.
2. The RD has been configured using the **route-distinguisher** command.

Precautions

The VPN instance bound to the interface specified by the **source** command in the CMP session view must be the same as the VPN instance configured in the **vpn-instance**. If they are inconsistent, either **source** or **vpn-instance**, which is configured later, cannot be executed successfully.

Example

Add a PKI realm to the VPN named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] route-distinguisher 22:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] vpn-instance vrf1
```

14.20 OLC Configuration Commands

14.20.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

14.20.2 cpu-overload-control

Function

The **cpu-overload-control** command configures the CPU usage thresholds and adjustment factor of the leak rate.

The **undo cpu-overload-control** command restores the default CPU usage thresholds and adjustment factor of the leak rate.

By default, the level-1 CPU usage threshold is 95%, the level-2 CPU usage threshold is 98%, and the adjustment factor of the leak rate is 10.

Format

cpu-overload-control { **threshold1** *threshold1–value* | **threshold2** *threshold2–value* | **adjustfactor** *adjustfactor–value* } * **slot** *slot-id*

undo cpu-overload-control { **threshold1** *threshold1–value* | **threshold2** *threshold2–value* | **adjustfactor** *adjustfactor–value* } * **slot** *slot-id*

Parameters

Parameter	Description	Value
threshold1 *threshold1–value*	Specifies the level-1 CPU usage threshold.	The value is an integer in the range from 70 to 95, in percentages.
threshold2 *threshold2–value*	Specifies the level-2 CPU usage threshold.	The value is an integer in the range from 71 to 100, in percentages.
adjustfactor *adjustfactor–value*	Specifies the adjustment factor of the leak rate.	The value is an integer in the range from 1 to 1000.
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Only when the CPU usage reaches the OLC start threshold (the same as the level-1 CPU usage threshold), the OLC function is started to lower the leak rate so that the rate of packets sent to the CPU is lowered. When the CPU usage reaches the level-2 CPU usage threshold, the system lowers the leak rate twice as fast. When the CPU usage falls below the OLC stop threshold (the level-1 CPU usage threshold minus 20%), the OLC function is stopped. The adjustment factor specifies the frequency at which the leak rate is adjusted. The smaller the adjustment factor, the faster the adjustment frequency, and vice versa. A smaller adjustment factor will allow the system to adjust more quickly to service changes but may lead t o flapping of the leak rate. The default leak rate is recommended.

Example

Set the level-1 CPU usage threshold to 90%, level-2 CPU usage threshold to 95%, and adjustment factor of the leak rate to 15 in slot 0.

```
<HUAWEI> system-view
[HUAWEI] cpu-overload-control threshold1 90 threshold2 95 adjustfactor 15 slot 0
```

14.20.3 cpu-overload-control alarm disable

Function

The **cpu-overload-control alarm disable** command disables the OLC alarm function.

The **undo cpu-overload-control alarm disable** command enables the OLC alarm function.

By default, the OLC alarm function is enabled.

Format

cpu-overload-control alarm disable

undo cpu-overload-control alarm disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the OLC alarm function is enabled. When the CPU usage is greater than the OLC start threshold or lower than the OLC stop threshold, an alarm is generated to notify users of the CPU running status and the status of the OLC function.

When the service traffic of monitored protocols or tasks on the live network is light and the CPU usage remains stably low, you can disable the OLC alarm function.

Example

Enable the OLC alarm function.

```
<HUAWEI> system-view
[HUAWEI] undo cpu-overload-control alarm disable
```

14.20.4 cpu-overload-control bucket-weight

Function

The **cpu-overload-control bucket-weight** command configures the weight of a protocol or task leaky bucket.

The **undo cpu-overload-control bucket-weight** command restores the default weight of a protocol or task leaky bucket.

The default weight of the leaky bucket is 90 for 8021x-1st, 200 for 8021x-other, 290 for arp-request, arp-reply, icmp, dhcp, arp-miss, igmp, ttl-expired, ip-frag, fib-hit, icmpv6, dhcpv6, mld, and nd, 250 for cos-4, 240 for cos-3, 200 for cos-2, 150 for cos-1, 100 for cos-0, and 2500 for acl and arpa tasks.

Format

cpu-overload-control { **packet-type** *packet-type* | **task** *task-name* } **bucket-weight** *bucket-weight-value* **slot** *slot-id*

undo cpu-overload-control { **packet-type** *packet-type* | **task** *task-name* } **bucket-weight** *bucket-weight-value* **slot** *slot-id*

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a protocol type.	The value is of the enumerated type: - 8021x-1st: first fragment of an 802.1X packet - 8021x-other: non-first fragments of an 802.1X packet - arp-request: ARP Request packet - arp-reply: ARP Reply packet - icmp: ICMP packet - dhcp: DHCP packet - arp-miss: ARP Miss packet - igmp: IGMP packet - ttl-expired: IPv4 TTL-expired packet - ip-frag: IP fragment - fib-hit: packet matching a route - icmpv6: ICMPv6 packet - dhcpv6: DHCPv6 packet - mld: MLD packet - nd: IPv6 neighbor discovery packet - cos-4: packet with priority 4 or higher (excluding whitelisted protocol packets) - cos-3: packet with priority 3 (excluding whitelisted protocol packets) - cos-2: packet with priority 2 (excluding whitelisted protocol packets) - cos-1: packet with priority 1 (excluding

Parameter	Description	Value
		whitelisted protocol packets) - cos-0: packet with priority 0 (excluding whitelisted protocol packets) **NOTE** S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S do not support arp-miss parameter.
task *task-name*	Specifies a task name.	The value is of the enumerated type: - acl: indicates the ACL task. - arpa: indicates the ARP broadcast task.
bucket-weight-value	Specifies the weight of the leaky bucket for the protocol or task.	The value is an integer in the range from 50 to 5000.
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Each protocol or task for which OLC is enabled is associated with a bottom leaky bucket. By default, the device assigns each leaky bucket a weight based on priorities of the monitored protocols and tasks. The weight of a leaky bucket determines its weighted water level (that is, the number of tokens that it can apply for). You can run this command to configure weights of the leaky buckets for monitored protocols and tasks based on service requirements.

Example

Set the weight of the leaky bucket for the DHCP protocol to 500 in slot 0.

```
<HUAWEI> system-view
[HUAWEI] cpu-overload-control packet-type dhcp bucket-weight 500 slot 0
```

14.20.5 cpu-overload-control disable

Function

The **cpu-overload-control disable** command disables the OLC function.

The **undo cpu-overload-control disable** command enables the OLC function.

By default, the OLC function is enabled.

Format

cpu-overload-control disable slot *slot-id*

undo cpu-overload-control disable slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a complex live network, the CPU may be overloaded if a large amount of service traffic is sent to the CPU or the CPU is attacked by unauthorized services. CPU overload will affect both the device's performance and its ability to process services.

OLC monitors certain CPU-bound protocol packets and tasks. According to the priorities of different services, OLC rate-limits the monitored protocol packets and tasks if the CPU usage exceeds a certain threshold. In this way, OLC not only reduces consumption of CPU resources but also prevents CPU overload from affecting normal processing of other services.

When the service traffic of monitored protocols or tasks on the live network is light and the CPU usage remains stably low, you can disable the OLC function.

Precautions

The OLC function configured for a protocol or task takes effect only after the OLC function is enabled.

Example

Enable the OLC function in slot 0.

```
<HUAWEI> system-view
[HUAWEI] undo cpu-overload-control disable slot 0
```

14.20.6 cpu-overload-control packet-type disable

Function

The **cpu-overload-control packet-type disable** command disables the OLC function for a monitored protocol.

The **undo cpu-overload-control packet-type disable** command enables the OLC function for a monitored protocol.

By default, the OLC function is enabled for all monitored protocols.

Format

cpu-overload-control packet-type *packet-type* &<1-20> **disable slot** *slot-id*

undo cpu-overload-control packet-type *packet-type* &<1-20> **disable slot** *slot-id*

Parameters

Parameter	Description	Value
packet-type	Specifies a protocol type.	The value is of the enumerated type: - 8021x-1st: first fragment of an 802.1X packet - 8021x-other: non-first fragments of an 802.1X packet - arp-request: ARP Request packet - arp-reply: ARP Reply packet - icmp: ICMP packet - dhcp: DHCP packet - arp-miss: ARP Miss packet - igmp: IGMP packet - ttl-expired: IPv4 TTL-expired packet - ip-frag: IP fragment - fib-hit: packet matching a route - icmpv6: ICMPv6 packet - dhcpv6: DHCPv6 packet - mld: MLD packet - nd: IPv6 neighbor discovery packet - cos-4: packet with priority 4 or higher (excluding whitelisted protocol packets) - cos-3: packet with priority 3 (excluding whitelisted protocol packets) - cos-2: packet with priority 2 (excluding whitelisted protocol packets) - cos-1: packet with priority 1 (excluding

Parameter	Description	Value
		whitelisted protocol packets) - cos-0: packet with priority 0 (excluding whitelisted protocol packets) **NOTE** S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S do not support arp-miss parameter. One or more of the preceding protocol types can be selected.
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the OLC function is enabled for all monitored protocols to prevent CPU overload caused by a large number of CPU-bound packets of a certain protocol or attacks from unauthorized services. When the service traffic of a monitored protocol on the live network is light, you can disable the OLC function for the protocol.

Precautions

The OLC function configured for a protocol takes effect only after the OLC function is enabled.

Example

Enable the OLC function for the DHCP protocol in slot 0.

```
<HUAWEI> system-view
[HUAWEI] undo cpu-overload-control packet-type dhcp disable slot 0
```

14.20.7 cpu-overload-control task enable

Function

The **cpu-overload-control task enable** command enables OLC for a specified monitoring task.

The **undo cpu-overload-control task enable** command disables OLC for a specified monitoring task.

By default, OLC is disabled for all monitoring tasks.

Format

cpu-overload-control task *task-name* &<1-2> **enable slot** *slot-id*

undo cpu-overload-control task *task-name* &<1-2> **enable slot** *slot-id*

Parameters

Parameter	Description	Value
task-name	Specifies the task name.	The value is of the enumerated type: - acl: indicates the ACL task. - arpa: indicates the ARP broadcast task. You can select one or two of the preceding task names.
slot *slot-id*	Specifies the slot ID.	The value must be the ID of an existing chip on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, OLC is disabled for ACL tasks and ARP broadcast tasks. To prevent CPU overload due to a type of tasks sending a large number of packets to the CPU, you can enable OLC for this type of tasks.

Precautions

OLC of the monitoring task takes effect only after the function is enabled.

Example

Enable OLC for ACL tasks in slot 0.

```
<HUAWEI> system-view
[HUAWEI] cpu-overload-control task acl enable slot 0
```

14.20.8 display cpu-overload-control configuration

Function

The **display cpu-overload-control configuration** command displays the OLC configuration.

Format

display cpu-overload-control configuration [**packet-type** *packet-type* | **task** *task-name*] **slot** *slot-id*

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a protocol type.	The value is of the enumerated type: - 8021x-1st: first fragment of an 802.1X packet - 8021x-other: non-first fragments of an 802.1X packet - arp-request: ARP Request packet - arp-reply: ARP Reply packet - icmp: ICMP packet - dhcp: DHCP packet - arp-miss: ARP Miss packet - igmp: IGMP packet - ttl-expired: IPv4 TTL-expired packet - ip-frag: IP fragment - fib-hit: packet matching a route - icmpv6: ICMPv6 packet - dhcpv6: DHCPv6 packet - mld: MLD packet - nd: IPv6 neighbor discovery packet - cos-4: packet with priority 4 or higher (excluding whitelisted protocol packets) - cos-3: packet with priority 3 (excluding whitelisted protocol packets) - cos-2: packet with priority 2 (excluding whitelisted protocol packets) - cos-1: packet with priority 1 (excluding

Parameter	Description	Value
		whitelisted protocol packets) - cos-0: packet with priority 0 (excluding whitelisted protocol packets) **NOTE** S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S do not support arp-miss parameter. If this parameter is not specified, the OLC configuration in the specified slot is displayed.
task *task-name*	Specifies a task name.	The value is of the enumerated type: - acl: indicates the ACL task. - arpa: indicates the ARP broadcast task. If this parameter is not specified, the OLC configuration in the specified slot is displayed.
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view the OLC configuration of a specified protocol, task, or slot, including the weight of the leaky bucket, OLC function status, CPU usage thresholds, and adjustment factor of the leak rate.

Example

Display the OLC configuration of the DHCP protocol in slot 0.

```
<HUAWEI> display cpu-overload-control configuration packet-type dhcp slot 0
---------------------------------
Protocol         Weight   Enable
---------------------------------
dhcp              290      Y
---------------------------------
```

Table 14-109 Description of the **display cpu-overload-control configuration packet-type** command output

Item	Description
Protocol	Protocol type.
Weight	Weight of the leaky bucket for the protocol. For details, see **cpu-overload-control bucket-weight**.
Enable	Whether the OLC function is enabled for the protocol: ● Y: enabled ● N: disabled For details, see **cpu-overload-control packet-type disable**.

Display the OLC configuration of the ACL task in slot 0.

```
<HUAWEI> display cpu-overload-control configuration task ACL slot 0
---------------------------------
Task             Weight   Enable
---------------------------------
acl               2500     N
---------------------------------
```

Table 14-110 Description of the **display cpu-overload-control configuration task** command output

Item	Description
Task	Task name.
Weight	Weight of the leaky bucket for the task. For details, see **cpu-overload-control bucket-weight**.

Item	Description
Enable	Whether the OLC function is enabled for the task: - Y: enabled - N: disabled For details, see **cpu-overload-control task enable**.

Display the OLC configuration in slot 0.

```
<HUAWEI> display cpu-overload-control configuration slot 0
CPU OLC Status: enable.
Alarm Status  : enable.
Low  Threshold: 95%.
High Threshold: 98%.
Adjustfactor  : 10.
Total Weight  : 10000.
---------------------------------
Task             Weight   Enable
---------------------------------
arpa               2500     N
acl               2500     N
---------------------------------
---------------------------------
Protocol         Weight   Enable
---------------------------------
8021x              290
  8021x-1st          90     Y
  8021x-other       200     Y
arp-request         290     Y
arp-reply          290     Y
icmp               290     Y
dhcp               290     Y
arp-miss            290     Y
igmp               290     Y
ttl-expired         290     Y
ip-frag            290     Y
fib-hit            290     Y
icmpv6              290     Y
dhcpv6              290     Y
nd                 290     Y
mld                290     Y
cos-4              250     Y
cos-3              240     Y
cos-2              200     Y
cos-1              150     Y
cos-0              100     Y
---------------------------------
```

Table 14-111 Description of the **display cpu-overload-control configuration** command output

Item	Description
CPU OLC Status	Whether the OLC function is enabled: - enable - disable For details, see **cpu-overload-control disable**.

Item	Description
Alarm Status	Whether the OLC alarm function is enabled: ● enable ● disable For details, see **cpu-overload-control alarm disable**.
Low Threshold	Level-1 CPU usage threshold. For details, see **cpu-overload-control**.
High Threshold	Level-2 CPU usage threshold. For details, see **cpu-overload-control**.
Adjustfactor	Adjustment factor of the leak rate. For details, see **cpu-overload-control**.
Total Weight	Total weights of all protocol or task leaky buckets.
Task	Task name.
Protocol	Protocol type.
Weight	Weight of the leaky bucket for the protocol or task. For details, see **cpu-overload-control bucket-weight**.
Enable	Whether the OLC function is enabled for the protocol or task. For details, see **cpu-overload-control packet-type disable** and **cpu-overload-control task enable**.

14.20.9 display cpu-overload-control statistics

Function

The **display cpu-overload-control statistics** command displays OLC statistics.

Format

display cpu-overload-control statistics [**packet-type** *packet-type* | **task** *task-name*] **slot** *slot-id*

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a protocol type.	The value is of the enumerated type: ● 8021x-1st: first fragment of an 802.1X packet ● 8021x-other: non-first fragments of an 802.1X packet ● arp-request: ARP Request packet ● arp-reply: ARP Reply packet ● icmp: ICMP packet ● dhcp: DHCP packet ● arp-miss: ARP Miss packet ● igmp: IGMP packet ● ttl-expired: IPv4 TTL-expired packet ● ip-frag: IP fragment ● fib-hit: packet matching a route ● icmpv6: ICMPv6 packet ● dhcpv6: DHCPv6 packet ● mld: MLD packet ● nd: IPv6 neighbor discovery packet ● cos-4: packet with priority 4 or higher (excluding whitelisted protocol packets) ● cos-3: packet with priority 3 (excluding whitelisted protocol packets) ● cos-2: packet with priority 2 (excluding whitelisted protocol packets) ● cos-1: packet with priority 1 (excluding

Parameter	Description	Value
		whitelisted protocol packets) - cos-0: packet with priority 0 (excluding whitelisted protocol packets) **NOTE** S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S do not support arp-miss parameter. If this parameter is not specified, OLC statistics in the specified slot are displayed.
task *task-name*	Specifies a task name.	The value is of the enumerated type: - acl: indicates the ACL task. - arpa: indicates the ARP broadcast task. If this parameter is not specified, OLC statistics in the specified slot are displayed.
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view OLC statistics of a specified protocol, task, or slot, including the number of protocol packets leaving or dropped by the leaky bucket, total running time of a task, and delay in processing a task.

Example

Display OLC statistics of the DHCP protocol in slot 0.

```
<HUAWEI> display cpu-overload-control statistics packet-type dhcp slot 0
-------------------------------------------------------------------------------
Protocol     Total pass     Total drop       Average pass     Average drop
             (packet)       (packet)         (packet)         (packet)
-------------------------------------------------------------------------------
dhcp         0              0                0                0
-------------------------------------------------------------------------------
```

Display OLC statistics of the ACL task in slot 0.

```
<HUAWEI> display cpu-overload-control statistics task ACL slot 0
-------------------------------------------------------------------------------
Task         Total Runtime  Total Delaytime  Average Runtime  Average Delaytime
               (ms)           (ms)             (ms)             (ms)
-------------------------------------------------------------------------------
acl          0              0                0                0
-------------------------------------------------------------------------------
```

Display OLC statistics in slot 0.

```
<HUAWEI> display cpu-overload-control statistics slot 0
-------------------------------------------------------------------------------
Task         Total Runtime  Total Delaytime  Average Runtime  Average Delaytime
               (ms)           (ms)             (ms)             (ms)
-------------------------------------------------------------------------------
arpa         3170           0                0                0
acl          0              0                0                0
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Protocol     Total Pass     Total Drop       Average Pass     Average Drop
             (packet)       (packet)         (packet)         (packet)
-------------------------------------------------------------------------------
8021x-1st    0              0                0                0
8021x-other  0              0                0                0
arp-request  0              0                0                0
arp-reply    0              0                0                0
icmp         0              0                0                0
dhcp         0              0                0                0
arp-miss     0              0                0                0
igmp         0              0                0                0
ttl-expired  0              0                0                0
ip-frag      0              0                0                0
fib-hit      0              0                0                0
icmpv6       0              0                0                0
dhcpv6       0              0                0                0
nd           0              0                0                0
mld          0              0                0                0
cos-4        0              0                0                0
cos-3        0              0                0                0
cos-2        0              0                0                0
cos-1        0              0                0                0
cos-0        0              0                0                0
-------------------------------------------------------------------------------
```

Table 14-112 Description of the **display cpu-overload-control statistics** command output

Item	Description
Task	Task name.
Total Runtime	Total running time of the task, in milliseconds.
Total Delaytime	Total delay in processing the task, in milliseconds.
Average Runtime	Running time of the task in the last second, in milliseconds.
Average Delaytime	Delay in processing the task in the last second, in milliseconds.
Protocol	Protocol type.
Total Pass	Total number of protocol packets leaving the leaky bucket.
Total Drop	Total number of protocol packets dropped by the leaky bucket.
Average Pass	Number of protocol packets leaving the leaky bucket in the last second.
Average Drop	Number of protocol packets dropped by the leaky bucket in the last second.

14.20.10 reset cpu-overload-control statistics

Function

The **reset cpu-overload-control statistics** command clears OLC statistics.

Format

reset cpu-overload-control statistics [**packet-type** *packet-type* | **task** *task-name*] **slot** *slot-id*

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a protocol type.	The value is of the enumerated type: - 8021x-1st: first fragment of an 802.1X packet - 8021x-other: non-first fragments of an 802.1X packet - arp-request: ARP Request packet - arp-reply: ARP Reply packet - icmp: ICMP packet - dhcp: DHCP packet - arp-miss: ARP Miss packet - igmp: IGMP packet - ttl-expired: IPv4 TTL-expired packet - ip-frag: IP fragment - fib-hit: packet matching a route - icmpv6: ICMPv6 packet - dhcpv6: DHCPv6 packet - mld: MLD packet - nd: IPv6 neighbor discovery packet - cos-4: packet with priority 4 or higher (excluding whitelisted protocol packets) - cos-3: packet with priority 3 (excluding whitelisted protocol packets) - cos-2: packet with priority 2 (excluding whitelisted protocol packets) - cos-1: packet with priority 1 (excluding

Parameter	Description	Value
		whitelisted protocol packets) - cos-0: packet with priority 0 (excluding whitelisted protocol packets) **NOTE** S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S do not support arp-miss parameter. If this parameter is not specified, OLC statistics in the specified slot are cleared.
task *task-name*	Specifies a task name.	The value is of the enumerated type: - acl: indicates the ACL task. - arpa: indicates the ARP broadcast task. If this parameter is not specified, OLC statistics in the specified slot are cleared.
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain OLC statistics in a specified period to locate faults of monitored protocols or tasks, you can run the **reset cpu-overload-control statistics** command to clear the previous OLC statistics of a specified protocol, task, or slot, and then run the **display cpu-overload-control statistics** command after a period of time to view the OLC statistics.

Precautions

The deleted OLC statistics cannot be restored. Therefore, exercise caution when running this command.

Example

Clear OLC statistics of the DHCP protocol in slot 0.

```
<HUAWEI> reset cpu-overload-control statistics packet-type dhcp slot 0
```

Clear OLC statistics of the ACL task in slot 0.

```
<HUAWEI> reset cpu-overload-control statistics task acl slot 0
```

Clear OLC statistics in slot 0.

```
<HUAWEI> reset cpu-overload-control statistics slot 0
```

14.21 ECA Configuration Commands

14.21.1 Command Support

Only the following switch models support ECA:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

14.21.2 defence engine enable

Function

The **defence engine enable** command enables the IAE.

The **undo defence engine enable** command disables the IAE.

By default, the IAE is disabled.

Format

defence engine enable

undo defence engine enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To configure the ECA function, you need to run the **defence engine enable** command to enable the IAE.

Precautions

To enable the IAE in a stack, reserve at least 20 MB storage space on each member device.

Example

Enable the IAE.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
```

14.21.3 decoding uri-cache

Function

The **decoding uri-cache enable** command enables the URI cache function.

The **decoding uri-cache disable** command disables the URI cache function.

By default, the URI cache function is enabled.

Format

decoding uri-cache enable

decoding uri-cache disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If no threat is detected from the corresponding session traffic after the URI cache function is enabled, the system will not inspect the session traffic with the same URI in a period of time. If all traffic must be inspected, disable the URI cache function.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the URI cache function.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] decoding uri-cache enable
```

14.21.4 display decoding statistics

Function

The **display decoding statistics** command displays decoding statistics.

Format

display decoding statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view statistics about the decoding function, including the event statistics, traffic statistics, and file statistics of each application.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display IPS statistics.

```
<HUAWEI> display decoding statistics
Decoding statistic on slot 0 cpu 0 :
-----------------------------------------------------------------------------
Decoding Statistic Table
-----------------------------------------------------------------------------
 Traffic statistic:
-----------------------------------------------------------------------------
   Total Traffic  :                             0
 ----------------------------------------------------------------------------
   Application                   Traffic
 ----------------------------------------------------------------------------
   HTTP                           0
   FTP                            0
   SMTP                           0
   POP3                           0
   NFS                            0
   SMB                            0
   IMAP                           0
   OTHER                          0
-----------------------------------------------------------------------------

 File statistic:
-----------------------------------------------------------------------------
   Total File  :                                0
 ----------------------------------------------------------------------------
   Application                   File
 ----------------------------------------------------------------------------
 ---- More ----
```

Table 14-113 Description of the **display decoding statistics** command output

Item	Description
Decoding statistic on slot 0 cpu 0	Displays decoding statistic from a specific slot ID and CPU ID.
Decoding Statistic Table	Decoding statistic table
Traffic statistic	Traffic statistics.
Total Traffic	All traffic.
Application	Application name.
Traffic	Traffic of the current application protocol.
File statistic	File statistics.
Total File	Total number of files.
Application	Application name.

Item	Description
File	Number of files of the current application protocol.

14.21.5 display engine information

Function

The **display engine information** command displays the running status of the Intelligent Awareness Engine (IAE) and the version of the SA signature database.

Format

display engine information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the IAE's running status and the version of the SA signature database, run the **display engine information** command.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the IAE's running status and the version of the SA signature database.

```
<HUAWEI> display engine information
==============================================================================
VSP Software Version               : V200R020C00SPC700B005
==============================================================================
Engine on CPU 0 in slot 0:
==============================================================================
  Engine Status                    : Ready
  Compile Status                   : Commit Succeeded
  SA Signature Database Version    : 2018041202
------------------------------------------------------------------------------
```

Table 14-114 Description of the **display engine information** command output

Item	Description
VSP Software Version	Software version of the VSP.
Engine on CPU *X* in slot *Y*	Engine information on CPU *X* in slot *Y*.
Engine Status	Engine status, which can be: ● Not Run: The engine is not running. ● Initializing: The engine is initializing. ● Ready: The engine is ready.
Compile Status	Compilation status, which can be: ● Idle ● Committing ● Commit Succeeded ● Commit Failed ● Commit Time Out ● Updating ● Update Succeeded ● Update Failed ● Update Time Out
SA Signature Database Version	Version of the SA signature database.

14.21.6 display engine session statistics

Function

The **display engine session statistics** command displays session statistics for the engine.

Format

display engine session statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The session statistics of the specified virtual system or all systems can be viewed only in the root system. In a virtual system, you can view only the session statistics of the virtual system.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Displays session statistics for the engine.

```
<HUAWEI> display engine session statistics

Engine session statistic on slot 0 cpu 0 :
------------------------------------------------------------------------------

  Engine Session Statistic Information of All Threads:
------------------------------------------------------------------------------
  Total Current Sessions              :            0
  Total Current UDP Sessions          :            0
  Total Current TCP Sessions          :            0
  Total Blocked Sessions              :            0
  Total Current Free Sessions         :        10000
  Total Current Buffered TCP Segments  :            0
  Total Out-of-sequence TCP Segments   :            0
  Total Overlapping TCP Segments      :            0
  Total Current Free TCP Segments     :         1000
------------------------------------------------------------------------------
  Engine Session Statistic Information of Each Thread:
------------------------------------------------------------------------------
  T00: NgeSess       0, sent:           0 rcv:           0 lost:           0
```

Table 14-115 Description of the **display engine session statistics** command output

Item	Description
Engine Session Statistic Information of All Threads	Session statistics for the engines used by all threads
Total Current Sessions	Total number of all sessions
Total Current UDP Sessions	Total number of UDP sessions
Total Current TCP Sessions	Total number of TCP sessions

Item	Description
Total Blocked Sessions	Total number of blocked sessions
Total Current Free Sessions	Total number of idle session nodes
Total Current Buffered TCP Segments	Total number of cached TCP segments
Total Out-of-sequence TCP Segments	Total number of out-of-sequence TCP segments
Total Overlapping TCP Segments	Total number of overlapped TCP segments
Total Current Free TCP Segments	Total number of TCP segments that can be cached
Engine Session Statistic Information of Each Thread	Session statistics for the engine used by each thread
NgeSess	Number of sessions
sent	Number of sent packets
rcv	Number of received packets
lost	Number of discarded packets

14.21.7 display engine session statistics app-type

Function

The **display engine session statistics app-type** command displays application statistics about an ECA session.

Format

display engine session statistics app-type [**slot** *slot-id*]

display engine session statistics interface [*interface-type interface-number*] **app-type**

Parameters

Parameter	Description	Value
slot *slot-id*	Displays application statistics about the ECA sessions in the specified slot. If the slot ID is not specified, application statistics about ECA sessions in all slots are displayed.	The value varies depending on the device configuration.

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays application statistics about the ECA sessions on the specified interface. If the interface type and number are not specified, application statistics about ECA sessions on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check application statistics about an ECA session and know about service traffic distribution, you can run the **display engine session statistics app-type** command.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

ECA session statistics may be inaccurate because collection of these statistics depends on NetStream packet statistics, which have no impact on the ECA function.

Example

Display application statistics about the ECA sessions on GE0/0/1.

```
<HUAWEI> display engine session statistics interface gigabitethernet 0/0/1 app-type
 GigabitEthernet0/0/1
 ------------------------------------------------------------------------------------
  App-Name                     Connect-Packet        Connect-Byte         Percent
 ------------------------------------------------------------------------------------
  Telnet                    8933              750614              80.05%
  HTTPS                       547              182102              19.42%
  HTTP                       51               4923               0.52%
 ------------------------------------------------------------------------------------
 Total:3
```

Table 14-116 Description of the **display engine session statistics app-type** command output

Item	Description
App-Name	Application name.
Connect-Packet	Number of connection packets.
Connect-Byte	Number of connection bytes.
Percent	Percentage of the application.
Total	Total number of applications.

14.21.8 display engine session statistics interface

Function

The **display engine session statistics interface** command displays ECA session flow statistics on a specified interface.

Format

display engine session statistics interface *interface-type interface-number* **flow** { **by-time** | **by-packet** }

Parameters

Parameter	Description	Value
interface-type interface-number	Displays ECA session flow statistics on an interface with the specified interface type and number.	-
flow	Displays ECA session flow statistics.	-
by-time	Displays ECA session flow statistics in descending order of time.	-
by-packet	Displays ECA session flow statistics in descending order of packet quantity.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check ECA session flow statistics on a specified interface and know about traffic distribution, run the **display engine session statistics interface** command.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display ECA session flow statistics on GE0/0/1 in descending order of packet quantity.

```
<HUAWEI> display engine session statistics interface gigabitethernet 0/0/1 flow by-packet

------------------------------------------------------------------------------------------------------------------------
--
 Source-ip       Destination-ip  Sport Dport Connect-Packet       Connect-Byte        Percent  App-name

------------------------------------------------------------------------------------------------------------------------
--
 192.168.240.32  192.168.40.2     4671  443   166                  101803              21.58%  HTTPS
 192.168.240.32  192.168.40.2     4679  443   69                  19140               4.05%   HTTPS
 192.168.240.32  192.168.40.2     4680  443   65                  15281               3.24%   HTTPS
 192.168.240.32  192.168.40.2     4682  443   59                  10532               2.23%   HTTPS
 192.168.240.32  192.168.40.2     4681  443   57                  8774               1.86%   HTTPS
 192.168.240.32  192.168.40.2     4683  443   56                  8710               1.84%   HTTPS
 192.168.240.32  192.168.40.2     4668  80    51                 4923               1.04%   HTTP
 192.168.40.84   192.168.40.2    54657 23    50                 4180               0.88%   Telnet
 192.168.40.84   192.168.40.2    54001 23    48                 4052               0.85%   Telnet
 192.168.40.84   192.168.40.2    50167 23    48                 4052               0.85%   Telnet
 192.168.40.84   192.168.40.2    52973 23    48                 4052               0.85%   Telnet
 192.168.40.84   192.168.40.2    52507 23    48                 4052               0.85%   Telnet
 192.168.40.2    192.168.240.188  23    39069 29                  2379               0.50%   Telnet
 192.168.40.84   192.168.40.2    52795 23    26                 2154               0.45%   Telnet
 192.168.40.84   192.168.40.2    51293 23    26                 2154               0.45%   Telnet
 192.168.40.84   192.168.40.2    53587 23    26                 2154               0.45%   Telnet
 192.168.40.84   192.168.40.2    49800 23    26                 2154               0.45%   Telnet
 192.168.40.84   192.168.40.2    50838 23    26                 2154               0.45%   Telnet
 192.168.40.2    192.168.40.84   23    52504 26                 2154               0.45%   Telnet
 192.168.40.84   192.168.40.2    52156 23    26                 2154               0.45%   Telnet
 192.168.40.84   192.168.40.2    54008 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    53553 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    49613 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    52435 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    52162 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    54290 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    53615 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    52442 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    50025 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    55381 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    51757 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    54892 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    55012 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    53311 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    52677 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    54313 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    51857 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    54850 23    25                 2090               0.44%   Telnet
 192.168.40.84   192.168.40.2    51344 23    24                 2026               0.42%   Telnet
 192.168.40.84   192.168.40.2    51184 23    24                 2026               0.42%   Telnet
 192.168.40.84   192.168.40.2    51319 23    24                 2026               0.42%   Telnet
 192.168.40.84   192.168.40.2    54185 23    24                 2026               0.42%   Telnet
```

```
192.168.40.84  192.168.40.2    52334 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53589 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52935 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52390 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50833 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54575 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52362 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52472 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53839 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51372 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51346 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50740 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50172 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50218 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51166 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53613 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51337 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51101 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54111 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54558 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50318 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51311 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51602 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51865 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51768 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53686 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53287 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51639 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52556 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52239 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51778 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52295 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    49713 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    49483 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53465 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52740 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    49424 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53369 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    55403 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51936 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50185 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54811 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50231 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51497 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53594 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52648 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51562 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    49833 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51465 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50220 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    49674 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53279 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    51992 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52575 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54275 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50561 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54997 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54541 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    55463 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50370 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53237 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    54070 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53798 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53764 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    55483 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    50659 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52069 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    52020 23    24              2026            0.42%   Telnet
192.168.40.84  192.168.40.2    53019 23    24              2026            0.42%   Telnet
```

```
 192.168.40.84   192.168.40.2    52896 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54381 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    53206 23    24                2026             0.42%   Telnet
 192.168.40.2    192.168.40.84   23    49498 24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    50960 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    52508 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    51848 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    52338 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54717 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    51666 23    24                2026             0.42%   Telnet
 192.168.40.2    192.168.40.84   23    54773 24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54763 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    55417 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    49952 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    50241 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    51389 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54166 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    52830 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54164 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    49412 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    49863 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    50044 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    53317 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    52065 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    49885 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    55114 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    53650 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    50195 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    49206 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54817 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    51190 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    52735 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    52385 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54527 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    54331 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    51671 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    55068 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    53631 23    24                2026             0.42%   Telnet
 192.168.40.84   192.168.40.2    53010 23    24                2026             0.42%   Telnet

-----------------------------------------------------------------------------------------------------------------------------------
--
 Total:150
```

Table 14-117 Description of the **display engine session statistics interface** command output

Item	Description
Source-ip	Source IP address of an ECA session flow.
Destination-ip	Destination IP address of an ECA session flow.
Sport	Source port number of an ECA session flow.
Dport	Destination port number of an ECA session flow.
Connect-Packet	Number of connection packets of an ECA session flow.
Connect-Byte	Number of connection bytes of an ECA session flows.
Percent	Percentage of an ECA session flow.
App-name	Application name of an ECA session flow.
Total	Total number of ECA session flows.

14.21.9 display engine session table

Function

The **display engine session table** command displays the details about the IPv4 session table of an engine.

Format

display engine session table [**source-ip** *source-ip-address* | **source-port** *source-port-number* | **destination-ip** *destination-ip-address* | **destination-port** *destination-port-number* | **protocol** { **tcp** | **udp** } | [**application** *application-name*]]* [**verbose**] [**slot** *slot-id* **cpu** *cpu-id* [**thread** *thread-id*]]

Parameters

Parameter	Description	Value
source-ip *source-ip-address*	Indicates a source IP address.	The value is in dotted decimal notation.
source-port *source-port-number*	Indicates a source port.	The value is an integer that ranges from 0 to 65535.
destination-ip *destination-ip-address*	Indicates a destination IP address.	The value is in dotted decimal notation.
destination-port *destination-port-number*	Indicates a destination port.	The value is an integer that ranges from 0 to 65535.
protocol	Specifies the protocol in a session table.	-
tcp	Indicates a TCP session.	-
udp	Indicates a UDP session.	-
application *application-name*	Specifies an application name.	-
verbose	Displays session details.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.

Parameter	Description	Value
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.
thread *thread-id*	Indicates a thread ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In a virtual system, you can view only the session statistics of the virtual system. The session information of the specified virtual system or all systems can be viewed only in the root system.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display details about the IPv4 session table of an engine.

```
<HUAWEI> display engine session table verbose
Engine session table on slot 0 cpu 0 :
-------------------------------------------------------------------------------
VSys:0 Vpn:0 Thread:0 UDP 10.0.0.1:80-->10.0.0.2:132 ttl:20 left-time:132 app: (45,QQ)
-------------------------------------------------------------------------------
```

Table 14-118 Description of the **display engine session table verbose** command output

Item	Description
Engine session table on slot 0 cpu 0	Engine session table on a specified slot and CPU
VSys	Name of a virtual system
Vpn	Name of a VPN instance
Thread	Thread ID
UDP	UDP

Item	Description
TCP	TCP
10.0.0.1:80-->10.0.0.2:132	Source address (10.0.0.1), source port (80), destination address (10.0.0.2), and destination port (132)
ttl	Aging time of a session
left-time	Remaining aging time of a session
app: (45,QQ)	Port number (45) and protocol (QQ) of the application

14.21.10 display engine statistics

Function

The **display engine statistics** command displays IAE engine statistics.

Format

display engine statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display engine statistics.

```
<HUAWEI> display engine statistics
Engine statistic on slot 0 cpu 0 :
------------------------------------------------------------------------------
Engine Statistic Table
------------------------------------------------------------------------------
 Event statistic:
------------------------------------------------------------------------------
   Total Alert Events  :          0
   Total Block Events  :          0
 -----------------------------------------------------------------------------
   Application                        Alert Events          Block Events
 -----------------------------------------------------------------------------
------------------------------------------------------------------------------

 Traffic statistic:
------------------------------------------------------------------------------
   Total Traffic  :               0
 -----------------------------------------------------------------------------
   Application                              Traffic
 -----------------------------------------------------------------------------
   DECODING                                          0
------------------------------------------------------------------------------

 File statistic:
------------------------------------------------------------------------------
   Total File  :               0
 -----------------------------------------------------------------------------
   Application                                File
 -----------------------------------------------------------------------------
   DECODING                                          0
------------------------------------------------------------------------------
```

Table 14-119 Description of the **display engine statistics** command output

Item	Description
Engine Statistic Table	Engine statistics table
Event statistic	Event statistics
Total Alert Events	Total number of alarm events
Total Block Events	Total number of block events
Application	Feature name
Alert Events	Number of alarm events corresponding to a feature
Block Events	Number of block events corresponding to a feature
Traffic statistic	Traffic statistics
Total Traffic	Total volume of traffic
Traffic	Volume of traffic processed in a feature
File statistic	File statistics

Item	Description
Total File	File size
File	Size of files processed in a feature
DECODING	Number of decoding.

14.21.11 display flow-probe metadata-collect information

Function

The **display flow-probe metadata-collect information** command displays configuration information about the function of metadata collection through the ECA flow probe.

Format

display flow-probe metadata-collect information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display configuration information about the function of metadata collection through the ECA flow probe.

```
<HUAWEI> display flow-probe metadata-collect information
 Flow-Probe Metadata-Collect Information on slot 0 cpu 0:
--------------------------------------------------------------------------------
  Global Config:
--------------------------------------------------------------------------------
  Enable                          : Yes
  Transfer Method                 : UDP
  Server IP                       : 0.0.0.0
  Server Port                     : 8514
  Source IP                       : 0.0.0.0
  Source Port                     : 0
  Source VPN Index                : 0
```

```
Source VPN Name              : -
Metadata aging time          : 300
Metadata Cache Max(Current number): 131072(0)
```

Table 14-120 Description of the **display flow-probe metadata-collect information** command output

Item	Description
Flow-Probe Metadata-Collect Information on slot 0 cpu 0	Metadata collection information through the ECA flow probe of in the specified slot and CPU.
Global Config	Global configuration.
Enable	Whether the function of metadata collection through the ECA flow probe is enabled: ● Yes: Enable ● No: Disable
Transfer Method	Transfer mode of metadata collected through the ECA flow probe, which can only be UDP.
Server IP	IP address of the peer HiSec Insight server.
Server Port	Port number of the peer HiSec Insight server.
Source IP	Source IP address of the packet sent from the ECA flow probe metadata to the HiSec Insight server.
Source Port	Source port of the packet sent from the ECA flow probe metadata to the HiSec Insight server.
Source VPN Index	VPN instance index of the packet sent from the ECA flow probe metadata to the HiSec Insight server.
Source VPN Name	VPN instance name of the packet sent from the ECA flow probe metadata to the HiSec Insight server.
Metadata aging time	Aging time of the ECA flow probe metadata.
Metadata Cache Max(Current number)	Max cache of the ECA flow probe metadata(Current number)

14.21.12 display flow-probe metadata-collect statistics

Function

The **display flow-probe metadata-collect statistics** command displays statistics about the function of metadata collection through the ECA flow probe.

Format

display flow-probe metadata-collect statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays statistics of metadata collection through the ECA flow probe in the specified slot.	The value range depends on the device configuration.
cpu *cpu-id*	Displays statistics of metadata collection through the ECA flow probe in the specified CPU.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display statistics about the function of metadata collection through the ECA flow probe.

```
<HUAWEI> display flow-probe metadata-collect statistics
 Flow-Probe Metadata-Collect Statistic Table (slot 0 cpu 0)
-------------------------------------------------------------------------------
  Statistics Information:
-------------------------------------------------------------------------------
  Engine Send By UDP                    : 0
  Engine UDP Send To Forward Success    : 0
  Engine UDP Send To Forward Fail       : 0
-------------------------------------------------------------------------------
```

Table 14-121 Description of the **display flow-probe metadata-collect statistics** command output

Item	Description
Flow-Probe Metadata-Collect Statistic Table (slot 0 cpu 0)	Statistics table for the metadata collection through the ECA flow probe in the specified slot and CPU.
Statistics Information	Statistics information for the metadata collection through the ECA flow probe.
Engine Send By UDP	Number of times UDP packets are sent.
Engine UDP Send To Fpath Success	Number of times that UDP packets are successfully sent.
Engine UDP Send To Fpath Fail	Number of times that UDP packets fail to be sent.

14.21.13 display fragment-reassemble configuration

Function

The **display fragment-reassemble configuration** command displays the global fragment reassembly configuration.

Format

display fragment-reassemble configuration [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the global fragment reassembly configuration.

```
<HUAWEI> display fragment-reassemble configuration
Fragment Reassembly statistics on slot 0 cpu 0 :
----------------------------------------------------------------------------
Fragment Reassembly Configuration:
-----------------------------------------------------------
  enable                : on
  overflow-mode         : forward
  overlap-mode          : consistency
  time-out(s)           : 5
  packet-cache(packets) : 255
  total-cache(packets)  : 1000
  defense-check         : off
  pass-through          : off
-----------------------------------------------------------
```

Table 14-122 Description of the **display fragment-reassemble configuration** command output

Item	Description
Fragment Reassembly statistics on slot 0 cpu 0	Fragment Reassembly statistics on a specific slot and CPU
Fragment Reassembly Configuration	Global fragment reassembly configuration
enable	State of the fragment reassembly function. ● on: The function is enabled. ● off: The function is disabled.
overflow-mode	Method for handling packets arriving at a full buffer in fragment reassembly: ● discard: Packets arriving at a full buffer are discarded. ● forward: Packets arriving at a full buffer are forwarded straight through.
overlap-mode	Policy to handle overlapping fragments: **consistency** indicates that overlapping fragments are processed based whether the overlapping parts have the same content.

Item	Description
time-out(s)	Fragment reassembly timeout in seconds
packet-cache(packets)	Fragment buffer size (in number of packets) for each packet
total-cache(packets)	Total buffer size in number of packets
defense-check	Status of the fragment attack defense function: ● on: The function is enabled. ● off: The function is disabled.
pass-through	Status of the fragment reassembly pass-through mode: ● on: The pass through mode is enabled. ● off: The pass through mode is disabled.

14.21.14 display fragment-reassemble session table

Function

The **display fragment-reassemble session table** command displays information about the IPv4/IPv6 fragmented packet-specific session table.

Format

display fragment-reassemble session table [**source-ip** *source-ip-address* | **destination-ip** *destination-ip-address*] * [**slot** *slot-id* **cpu** *cpu-id*]

display fragment-reassemble ipv6 session table [**source-ip** *source-ipv6-address* | **destination-ip** *destination-ipv6-address*] * [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
source-ip *source-ip-address*	Specifies the source IPv4 address.	The value is in dotted decimal notation.
destination-ip *destination-ip-address*	Specifies the destination IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
ipv6	Displays statistics on the fragment reassembly of IPv6 packets.	-
source-ip *source-ipv6-address*	Specifies the source IPv6 address.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
destination-ip *destination-ipv6-address*	Specifies the destination IPv6 address.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the IPv4 fragmented packet-specific session table.

```
<HUAWEI> display fragment-reassemble session table
Fragment Reassembly statistics on slot 0 cpu 0 :
------------------------------------------------------------------------------------------------------------------
  VSys:0 Vpn:0 10.1.1.1-->1.1.1.1(363) ttl:5 left-time:4 frag-num:32 flags:(first 1,last 0,overflow 0,result 0)

  VSys:0 Vpn:0 10.1.1.1-->1.1.1.1(363) ttl:5 left-time:3 frag-num:32 flags:(first 1,last 0,overflow 0,result 0)
------------------------------------------------------------------------------------------------------------------
```

Table 14-123 Description of the **display fragment-reassemble session table** command output

Item	Description
Fragment Reassembly statistics on slot 0 cpu 0	Fragment Reassembly statistics on a specific slot and CPU
VSys	Name of a virtual system
Vpn	Name of a VPN instance
ttl	Aging time of a fragment session
left-time	Remaining aging time of a fragment session
frag-num	Number of fragments
flags:(first 1,last 0,overflow 0,result 0)	Fragment flag, which can be: ● first: first fragment ● last: last fragment ● overflow: fragment cache overflow ● result: reassembly result

14.21.15 display fragment-reassemble statistics

Function

The **display fragment-reassemble statistics** command displays statistics on the fragment reassembly of IP packets.

Format

display fragment-reassemble [**ipv6**] **statistics** [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
ipv6	Displays statistics on the fragment reassembly of IPv6 packets.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display statistics on the fragment reassembly of IP packets.

```
<HUAWEI> display fragment-reassemble statistics
Fragment Reassembly statistics on slot 0 cpu 0 :
------------------------------------------------------------------------------
Fragment Reassembly Statistics:
------------------------------------------------------------
  Total fragments              : 0
  Total cached fragments       : 0
  Total error packets          : 0
  Total discarded fragments    : 0
  Complete overlap processing : 0
  Partial overlap processing  : 0
  Total current sessions       : 0
  Total free sessions          : 1000
------------------------------------------------------------
```

Table 14-124 Description of the **display fragment-reassemble statistics** command output

Item	Description
Fragment Reassembly statistics on slot *X* cpu *Y*	Fragment reassembly statistics on CPU *Y* in slot *X*.
Fragment Reassembly Statistics	Statistics on fragment reassembly.
Total fragments	Number of received fragments.
Total cached fragments	Number of cached fragments.
Total error packets	Number of packets with error fragments.
Total discarded fragments	Number of discarded fragments.
Complete overlap processing	Complete overlap processing.
Partial overlap processing	Partial overlap processing
Total current sessions	Total number of current sessions.
Total free sessions	Total number of free sessions.

14.21.16 display stream-reassemble configuration

Function

The **display stream-reassemble configuration** command displays the global TCP stream reassembly configuration.

Format

display stream-reassemble configuration [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the global TCP stream reassembly configuration.

```
<HUAWEI> display stream-reassemble configuration
Stream reassemble configuration on slot 0 cpu 0 :
-------------------------------------------------------------------------------
Stream Reassembly Configuration:
-------------------------------------------------------------
  enable                : on
  overflow-mode         : discard
  overlap-mode          : overwrite
  session-cache(KB)     : 16
  total-cache(packets)  : 1000
  timestamp-check       : true
  tcp-option check      : true
  defense-check         : on
  session-timeout(s)    : 60
  enhanced-mode         : on
-------------------------------------------------------------
```

Table 14-125 Description of the **display stream-reassemble configuration** command output

Item	Description
Stream reassemble configuration on slot 0 cpu 0	TCP stream reassembly configuration on slot 0 cpu 0.
enable	Indicates the state of the TCP stream reassembly function. ● on: The function is enabled. ● off: The function is disabled.
overflow-mode	Indicates the method for handling packets arriving at a full buffer in stream reassembly. ● discard: Packets arriving at a full buffer are discarded. ● forward: Packets arriving at a full buffer are forwarded straight through.
overlap-mode	Indicates the policy to handle overlapping packets: ● overwrite: Indicate overwrite the original overlapped part. ● preserve: Indicate preserve the original overlapped part.
session-cache(KB)	Indicates the buffer size in KB for each session in TCP stream reassembly.
total-cache(packets)	Global buffer size in number of packets in stream reassembly.
timestamp-check	Indicates the state of the timestamp check function. ● true: The function is enabled. ● false: The function is disabled.
tcp-option check	Indicates the state of the TCP option check function. ● true: The function is enabled. ● false: The function is disabled.
defense-check	Indicates the status of the TCP attack defense function: ● on: The function is enabled. ● off: The function is disabled.

Item	Description
session-timeout(s)	Indicates the timeout of out-of-sequence TCP packet inspection, in seconds.
enhanced-mode	Status of enhanced traffic reassembly: ● on: The function is enabled. ● off: The function is disabled.

14.21.17 display update configuration

Function

The **display update configuration** command displays the update configuration of the application identification signature database.

Format

display update configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the update configuration of the application identification signature database.

```
<HUAWEI> display update configuration
Update Configuration Information:
------------------------------------------------------------
  Update Server              : sec.huawei.com
  Update Port                : 443
  Proxy State                : Disable
  Proxy Server               : -
  Proxy Port                 : -
  Proxy User                 : -
```

```
 Proxy Password              : -
 SA-SDB:
   Application Confirmation  : Disable
   Schedule Update           : Enable
   Schedule Update Frequency : Daily
   Schedule Update Time      : 04:16
------------------------------------------------------------
```

Table 14-126 Description of the **display update configuration** command output

Item	Description
Update Configuration Information	Update configuration of the application identification signature database.
Update Server	IP address or domain name of the update server. The default domain name is that of the update center.
Update Port	Port number of the update server.
Proxy State	Whether the proxy server is enabled. The value can be: ● Enable: The proxy server is enabled. ● Disable: The proxy server is disabled.
Proxy Server	IP address or domain name of the proxy server.
Proxy Port	Port number of the proxy server.
Proxy User	User name of the proxy server.
Proxy Password	Password of the proxy server.
SA-SDB	Update configuration of the application identification signature database.
Application Confirmation	Whether manual installation confirmation is enabled. The value can be: ● Enable: Confirmation is required before the installation of the update file. ● Disable: The update file is automatically installed.
Schedule Update	Whether the scheduled update function is enabled. The value can be: ● Enable ● Disable
Schedule Update Frequency	Scheduled update frequency. The value can be: ● Weekly ● Daily ● Hourly
Schedule Update Time	Scheduled update time

14.21.18 display update host source

Function

The **display update host source** command displays the interface and source IP address configurations used in online updating the application identification signature database.

Format

display update host source

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **update host source** command configures the source interface and IP address, and **display update host source** command displays the configurations.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the interface and source address configurations used in online updating the application identification signature database.

```
<HUAWEI> display update host source
----------------------------------------------------------------
Source IP Information:
        IP address                : 10.1.1.1
        vpn-instance               : -
Source Interface Information:
        interface name            : GigabitEthernet0/0/1
----------------------------------------------------------------
```

Table 14-127 Description of the **display update host source** command output

Item	Description
Source IP Information	Source IP address information.

Item	Description
IP address	IP address.
vpn-instance	VPN instance name.
Source Interface Information	Source interface information.
interface name	Interface name.

14.21.19 display update information all-sdb

Function

The **display update information all-sdb** command displays the last record on application identification signature database updates.

Format

display update information all-sdb

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the last record on application identification signature database updates.

```
<HUAWEI> display update information all-sdb
  Current Update Status:  Idle.
-----------------------------------------------------------------------------------------------
  SA-SDB latest update finish time           : 04:16:13 2018/07/03
  SA-SDB latest update result              : Error: Failed to perform DNS resolution.
-----------------------------------------------------------------------------------------------
```

Table 14-128 Description of the **display update information all-sdb** command output

Item	Description
Current Update Status	Current status of the update server, including: - Idle: indicates that no signature database is being updated. - Version Loading: indicates that the version is being loaded. - Live Updating: indicates live update. - Local Updating: indicates the local update. - Version Rollbacking: indicates that version rollback is being performed. - Stop Updating: indicates that the update is being stopped. - Version Applying: indicates that the version is being downloaded. - Version Restoring: indicates that the default version is being restored. - Version Uninstalling: indicates that the version is being uninstalled. - Update check: indicates that the update is being checked. - Engine start loading: indicates that the engine start is being loaded.
SA-SDB	Application identification signature database.
latest update finish time	Last update time of the application identification signature database.
latest update result	Last update result of the application identification signature database.
SA-SDB	Application identification signature database.

14.21.20 display update status

Function

The **display update status** command displays the update status of the application identification signature database.

Format

display update status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

View the current update status of the application identification signature database.

```
<HUAWEI> display update status
  Current Update Status: Idle.
```

Table 14-129 Description of the **display update status** command output

Item	Description
Current Update Status	Current update status of the application identification signature database consist of update type and update status. Update type: - Idle: indicates that no signature database is being updated. - Version Load: indicates that the version is being loaded. - Online Update: indicates online update. - Local Update: indicates the local update. - Version Rollback: indicates the version rollback. - Stop Update: indicates that the update is stopped. - Version Apply: indicates that the version is applied. - Version Restore: indicates that the default version is restored. - Version Uninstall: indicates that the version is being uninstalled. - Update check: indicates that the update is checked. - Engine start loading: indicates that the engine start is being loaded. Update status: - Ready to load The Update Package: indicates that the update package will be loaded soon. - Verify The Authority: indicates that permission is being verified. - Obtain The Update Package: indicates that the update package is being obtained. - Load The Update Package: indicates that the update package is being loaded. - Merge The Incremental Package: indicates that the incremental package is being merged. - Retry The Update: indicates that the update is being retried. For example: - Online Update, Obtain The Update Package.: indicates online update and an update package is being downloaded. - Version Rollback, Load The Update Package: indicates version rollback and a rollback package is being loaded.

Item	Description
	● Version Apply, Verify The Authority.: indicates that the version is being applied and the permission is being verified. ● Local Update, Load The Update Package: indicates local update and an update package is being loaded.

14.21.21 display version sa-sdb

Function

The **display version sa-sdb** command displays the version of the application identification signature database.

Format

display version sa-sdb

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

View the version of the application identification signature database.

```
<HUAWEI> display version sa-sdb
SA SDB Update Information List:
----------------------------------------------------------------
  Current Version:
    Signature Database Version    : 2018041202
    Signature Database Size(byte) : 871104
    Update Time                   : 17:47:51 2018/06/30
    Issue Time of the Update File : 17:03:54 2018/04/12

  Backup Version:
    Signature Database Version    :
    Signature Database Size(byte) : 0
    Update Time                   : 00:00:00 0000/00/00
```

```
  Issue Time of the Update File : 00:00:00 0000/00/00
------------------------------------------------------------------
```

Table 14-130 Description of the **display version sa-sdb** command output

Item	Description
SA SDB Update Information List	Update information list of the application identification signature database.
Current Version	Current version information about the engine or the application identification signature database.
Signature Database Version	Version of the engine or the application identification signature database.
Signature Database Size(byte)	Size of the engine or the application identification signature database(byte).
Update Time	Date and time when the application identification signature database was upgraded to this version
Issue Time of the Update File	Date and time when the file for the upgrade package to this version was released
Backup Version	Source version of the engine or the application identification signature database for rollbacks.

14.21.22 ec-analytics enable

Function

The **ec-analytics enable** command enables the ECA function on an interface.

The **undo ec-analytics enable** command disables the ECA function on an interface.

By default, the ECA function is disabled.

Format

ec-analytics enable [**inbound** | **outbound**]

undo ec-analytics enable [**inbound** | **outbound**]

Parameters

Parameter	Description	Value
inbound	Enables ECA traffic in the inbound direction.	-
outbound	Enables ECA for traffic in the outbound direction.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, VLANIF interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

To analyze encrypted traffic on a network and identify malicious communications in the encrypted traffic, you can run the **ec-analytics enable** command on an interface to enable the ECA function.

Precautions

- If the traffic direction is not specified, ECA is performed for traffic in both direction by default.
- If it is confirmed that firewalls have been deployed at the network egress, you are advised to enable ECA only for traffic in the inbound direction.
- When ECA is enabled on both upstream and downstream interfaces, only upstream interfaces take effect.

Example

Enable the ECA function for traffic in the inbound direction of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ec-analytics enable inbound
```

14.21.23 ec-analytics enhanced-mode disable

Function

The **ec-analytics enhanced-mode disable** command disables the ECA enhanced mode.

The **undo ec-analytics enhanced-mode disable** command enables the ECA enhanced mode.

By default, the ECA enhanced mode is enabled.

Format

ec-analytics enhanced-mode disable

undo ec-analytics enhanced-mode disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In ECA enhanced mode, 50 packets are sent to the IAE for each ECA session flow, improving accuracy of encrypted traffic identification. However, the processing performance of the IAE deteriorates if it has to process enormous packets. When the device performance is limited, you can disable the ECA enhanced mode. After that, only 20 packets are sent to the IAE for each ECA session flow.

Precautions

You are advised to enable the ECA enhanced mode when the device performance meets requirements.

Example

Enable the ECA enhanced mode.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] undo ec-analytics enhanced-mode disable
```

14.21.24 ec-analytics whitelist

Function

The **ec-analytics whitelist** command configures an ECA whitelist. ECA is not performed for the whitelist traffic.

The **undo ec-analytics whitelist** command deletes an ECA whitelist.

By default, no ECA whitelist is configured on a device.

Format

ec-analytics whitelist acl *acl-number*

undo ec-analytics whitelist acl *acl-number*

Parameters

Parameter	Description	Value
acl *acl-number*	Adds the specified ACL number to the ECA whitelist.	The value is an integer in the range from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **ec-analytics whitelist** command to add trusted network traffic to the whitelist so that ECA is not performed for such traffic.

Precautions

Advanced ACLs are applied in the ECA whitelist and only the 5-tuple information is supported.

When the ECA whitelist is configured, a maximum of 32 ACL rules with small rule numbers take effect.

Example

Add ACL 3000 to the ECA whitelist to prevent ECA from being performed for traffic with the source IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule permit ip source 10.1.1.1 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] ec-analytics whitelist acl 3000
```

14.21.25 engine configuration commit

Function

The **engine configuration commit** command commits the configuration of security policies.

Format

engine configuration commit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Newly configured security policies or the modified security policies do not take effect until you run the **engine configuration commit** command to commit the configuration. To save time, commit the configurations in batches after you have completed all security policy configurations.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Commit the security policy configurations.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] engine configuration commit
```

14.21.26 engine enhanced-detection

Function

The **engine enhanced-detection** command configures the engine to work in enhanced detection mode.

The **undo engine enhanced-detection** command configures the engine to work in common detection mode.

By default, the engine works in common detection mode.

Format

engine enhanced-detection

engine enhanced-detection protocol { **rtsp** | **others** }

undo engine enhanced-detection

undo engine enhanced-detection protocol { **rtsp** | **others** }

Parameters

Parameter	Description	Value
protocol rtsp	Configures the engine to work in enhanced detection mode for RTSP.	By default, the engine works in enhanced detection mode for RTSP.

Parameter	Description	Value
protocol others	Configures the engine to work in enhanced detection mode for protocols excluding RTSP.	By default, the engine works in common detection mode for protocols excluding RTSP.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you configure the engine to work in enhanced detection mode, the detection capability of the device will be enhanced, and the detection speed will be decreased.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Configure the engine to work in enhanced detection mode.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] engine enhanced-detection
```

14.21.27 engine pass-through enable

Function

The **engine pass-through enable** command enables the pass-through mode of the engine.

The **undo engine pass-through enable** command disables the pass-through mode of the engine.

By default, the pass-through mode of the engine is disabled.

Format

engine pass-through enable [**slot** *slot-id* **cpu** *cpu-id*]

undo engine pass-through enable [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the pass-through mode of the engine is enabled, the system generates events, such as debugging information or log during service processing, but does not perform actual actions. Even a block action is configured for a service, the system does not block traffic but records the service event state.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the pass-through mode of the engine.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] engine pass-through enable
```

14.21.28 engine session timeout active

Function

The **engine session timeout active** command sets the active flow aging time of an ECA session.

The **undo engine session timeout active** command restores the default active flow aging time of an ECA session.

By default, the active flow aging time of an ECA session is 60 seconds.

Format

engine session timeout active *time*

undo engine session timeout active

Parameters

Parameter	Description	Value
time	Specifies the active flow aging time of an ECA session.	The value is an integer in the range from 1 to 300, in seconds. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After ECA is configured on a device, the ECA session flow table ages out after a certain period. The flow table that is aged out is encapsulated and then sent to the HiSec Insight server as metadata. Active flow aging of ECA enables the device to periodically output the statistics about the flows that persist for a long period.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the active flow aging time of an ECA session to 15 seconds.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] engine session timeout active 15
```

14.21.29 engine session timeout inactive

Function

The **engine session timeout inactive** command sets the inactive flow aging time of an ECA session.

The **undo engine session timeout inactive** command restores the default inactive flow aging time of an ECA session.

By default, the inactive flow aging time of an ECA session is 15 seconds.

Format

engine session timeout inactive *time*

undo engine session timeout inactive

Parameters

Parameter	Description	Value
time	Specifies the inactive flow aging time of an ECA session.	The value is an integer in the range from 1 to 300, in seconds. The default value is 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After ECA is configured on a device, the ECA session flow table ages out after a certain period. The flow table that is aged out is encapsulated and then sent to the HiSec Insight server as metadata. Inactive flow aging of ECA requires the device to export statistics about the flows that persist for a short period. Once adding packets to a flow stops, the device exports flow statistics to conserve memory space.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the inactive flow aging time of an ECA session to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] engine session timeout active 10
```

14.21.30 flow-probe metadata-collect aging-time

Function

The **flow-probe metadata-collect aging-time** command configures the aging time of ECA flow probe metadata entries.

The **undo flow-probe metadata-collect aging-time** command restores the default aging time of ECA flow probe metadata entries.

By default, the aging time of ECA flow probe metadata entries is 300 seconds.

Format

flow-probe metadata-collect aging-time *time*

undo flow-probe metadata-collect aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time of ECA flow probe metadata entries.	The value is an integer in the range from 0 to 1200, in seconds. The default value is 300.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the aging time of ECA flow probe metadata entries to adjust the rate of sending packets to the HiSec Insight server.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the aging time of ECA flow probe metadata entries to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] flow-probe metadata-collect aging-time 10
```

14.21.31 flow-probe metadata-collect enable

Function

The **flow-probe metadata-collect enable** command enables the function of metadata collection through the ECA flow probe.

The **undo flow-probe metadata-collect enable** command disables the function of metadata collection through the ECA flow probe.

By default, the function of metadata collection through the ECA flow probe is enabled.

Format

flow-probe metadata-collect enable

undo flow-probe metadata-collect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the function of metadata collection through the ECA flow probe.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] flow-probe metadata-collect enable
```

14.21.32 flow-probe metadata-collect server

Function

The **flow-probe metadata-collect server** command configures the IP address and port number of the HiSec Insight server.

The **undo flow-probe metadata-collect server** command deletes the configured IP address and restores the configured port number to the default value.

By default, the IP address of the HiSec Insight server is not specified and the default port number is 8514.

Format

flow-probe metadata-collect server ip *ip-address* [**port** *port-number*]

undo flow-probe metadata-collect server

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IP address of the HiSec Insight server.	The value is an IPv4 address in dotted decimal notation.
port *port-number*	Specifies the port number of the HiSec Insight server.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default port number of the peer HiSec Insight server connected to the flow probe metadata collector is subject to the metadata collection and transmission mode. Currently, the switch only supports UDP for metadata transmission, and the default port number is 8514.

When configuring the IP address of the HiSec Insight server:

- If the HiSec Insight server is of the standard version, the IP address is the data dispatcher management plane IP address of the HiSec Insight server. Multiple data dispatcher management plane IP addresses may exist. You can select any one of them.
- If the HiSec Insight server is of the small-scale edition, the IP address is the Big Data cluster server management plane IP address of the HiSec Insight server. Multiple Big Data cluster server management plane IP addresses may exist. You can select any one of them.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the IP address and port number of the HiSec Insight server to **10.1.1.1** and **10** respectively.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] flow-probe metadata-collect server ip 10.1.1.1 port 10
```

14.21.33 flow-probe metadata-collect source

Function

The **flow-probe metadata-collect source** command configures the source IP address and VPN instance name of the packet sent from the ECA flow probe metadata to the HiSec Insight server.

The **undo flow-probe metadata-collect source** command restores the configured source IP address and VPN instance name to the default values.

By default, the source IP address of the packet sent from the ECA flow probe metadata to the HiSec Insight is empty.

Format

flow-probe metadata-collect source { **ip** *ip-address* **port** *port-number* | **vpn-instance** *vpn-instance-name* } *

undo flow-probe metadata-collect source

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the source IP address of the packet sent from the ECA flow probe metadata to the HiSec Insight server.	The value is in dotted decimal notation.
port *port-number*	Specifies the source port number of the packet sent from the ECA flow probe metadata to the HiSec Insight server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name of the packet sent from the ECA flow probe metadata to the HiSec Insight server.	The value must be the name of an existing VPN instance.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the source IP address of the packet sent from the ECA flow probe metadata to the HiSec Insight server, ensure that the IP address is the device interface IP address and that this interface IP address is reachable to the HiSec Insight server.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the source IP address and source port number of the packet sent from the ECA flow probe metadata to the HiSec Insight server to **10.1.1.1** and **port 1** respectively.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] flow-probe metadata-collect source ip 10.1.1.1 port 1
```

14.21.34 fragment-reassemble enable

Function

The **fragment-reassemble enable** command enables fragment reassembly.

The **undo fragment-reassemble enable** command disables fragment reassembly.

By default, fragment reassembly is enabled.

Format

fragment-reassemble enable

undo fragment-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If fragment reassembly is disabled, fragments will not be reassembled and will not be inspected. Meanwhile, TCP stream reassembly may also fail.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable fragment reassembly.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] fragment-reassemble enable
```

14.21.35 fragment-reassemble overflow-mode

Function

The **fragment-reassemble overflow-mode** command configures the action to take on fragments that overflow the cache.

The **undo fragment-reassemble overflow-mode** command restores the default action to take on fragments that overflow the cache.

By default, the system forwards the fragments that overflow the cache to ensure services.

Format

fragment-reassemble overflow-mode { **discard** | **forward** }

undo fragment-reassemble overflow-mode

Parameters

Parameter	Description	Value
discard	Discards the fragments that overflow the cache.	-
forward	Forwards the fragments that overflow the cache.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the action is set to **discard**, the system discards the fragments that overflow the cache, which may interrupt services.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Configure the action to take on fragments that overflow the cache to **discard**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] fragment-reassemble overflow-mode discard
```

14.21.36 fragment-reassemble user-configure

Function

The **fragment-reassemble user-configure** command configures user-defined items for the fragment reassembly function.

The **undo fragment-reassemble user-configure** command cancels the configuration of user-defined items for the fragment reassembly function.

By default, all user-defined items of the fragment reassembly function are disabled.

Format

fragment-reassemble user-configure { **defense-check** | **pass-through** }

undo fragment-reassemble user-configure { **defense-check** | **pass-through** }

Parameters

Parameter	Description	Value
defense-check	Indicates fragment attack defense.	-
pass-through	Indicates the pass through mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the pass through mode is enabled (using the **fragment-reassemble user-configure pass-through** command), in some special fragment traffic scenarios (for example, the fragments completely overlap, and the overlapped part has the same content), the system will regard the traffic as abnormal traffic and will not reassemble the fragments. If the fragment attack defense function has been enabled (using the **fragment-reassemble user-configure defense-check** command), the abnormal fragments will be discarded. If the fragment attack defense function has not been enabled, the system will forward the fragments. After the pass through mode is disabled, the system assembles the fragments based on the normal processing flow.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the fragment attack defense function.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] fragment-reassemble user-configure defense-check
```

14.21.37 reset decoding statistics

Function

The **reset decoding statistics** command clears decoding statistics.

Format

reset decoding statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Clear decoding statistics.

```
<HUAWEI> reset decoding statistics
```

14.21.38 reset engine session statistics

Function

The **reset engine session statistics** command clears the session statistics of the engine.

Format

reset engine session statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Use caution before you decide to run this command. Once the session statistics of the engine are cleared, they cannot be restored.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Clear the session statistics of the engine.

```
<HUAWEI> reset engine session statistics
```

14.21.39 reset engine session statistics app-type

Function

The **reset engine session statistics app-type** command clears application statistics about an ECA session.

Format

reset engine session statistics app-type [**slot** *slot-id*]

reset engine session statistics interface [*interface-type interface-number*] **app-type**

Parameters

Parameter	Description	Value
slot *slot-id*	Clears application statistics about ECA sessions in a specified slot.	The value varies depending on the device configuration.
interface *interface-type interface-number*	Clears application statistics about ECA sessions on a specified interface. If the interface type and number are not specified, application statistics about ECA sessions on all interfaces are displayed.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **reset engine session statistics app-type** command to clear application statistics about ECA sessions.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Clear application statistics about ECA sessions on slot 0.

```
<HUAWEI> reset engine session statistics app-type slot 0
```

14.21.40 reset engine session statistics flow

Function

The **reset engine session statistics flow** command clears ECA session flow statistics.

Format

reset engine session statistics interface *interface-type interface-number* **flow** { **by-time** | **by-packet** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears ECA session flow statistics on a specified interface.	-
by-time	Clears ECA session flow statistics displayed in descending order of time.	-
by-packet	Clears ECA session flow statistics displayed in descending order of packet quantity.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **reset engine session statistics interface** command to clear ECA session flow statistics on a specified interface.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Clear ECA session flow statistics displayed in descending order of packet quantity on GE0/0/1.

```
<HUAWEI> reset engine session statistics interface gigabitethernet 0/0/1 flow by-packet
```

14.21.41 reset engine session table

Function

The **reset engine session table** command clears the session information of the engine.

Format

reset engine session table [**source** *source-ip-address* | **destination** *destination-ip-address* | **destination-port** *destination-port-number* | **protocol** { **tcp** | **udp** }] * [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IPv4 address.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IPv4 address.	The value is in dotted decimal notation.
destination-port *destination-port-number*	Specifies the destination port number.	The value is an integer ranging from 0 to 65535.
protocol	Indicates a protocol.	-
tcp	Indicates Transmission Control Protocol (TCP).	-
udp	Indicates User Datagram Protocol (UDP).	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no parameter is specified, all session information of the engine is cleared after you run the **reset engine session table** command.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

Use caution before you decide to run this command. Clearing the session information of the engine adversely affects the service operating.

Example

Clear all session information of the engine.

```
<HUAWEI> reset engine session table
Warning: Reseting session table will affect the engine's normal service. Continue? [Y/N]: y
```

14.21.42 reset engine statistics

Function

The **reset engine statistics** command clears engine statistics.

Format

reset engine statistics [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Clear engine statistics.

```
<HUAWEI> reset engine statistics
```

14.21.43 reset flow-probe metadata-collect statistics

Function

The **reset flow-probe metadata-collect statistics** command resets statistics about the function of metadata collection through the ECA flow probe.

Format

reset flow-probe metadata-collect statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you run the **display flow-probe metadata-collect statistics** command to view statistics about the function of metadata collection through the ECA flow probe, you can run the **reset flow-probe metadata-collect statistics** command to reset the statistics and collect statistics again. Cleared statistics cannot be restored. Exercise caution when you run this command.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Reset statistics about the function of metadata collection through the ECA flow probe.

```
<HUAWEI> reset flow-probe metadata-collect statistics
```

14.21.44 reset fragment-reassemble statistics

Function

The **reset fragment-reassemble statistics** command clears statistics on fragment reassembly.

Format

reset fragment-reassemble [**ipv6**] **statistics** [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
ipv6	Clears statistics of IPv6 packets on fragment reassembly.	-
slot *slot-id*	Specifies a slot ID.	The value range depends on the device configuration.
cpu *cpu-id*	Specifies a CPU ID.	The value range depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Clear statistics on fragment reassembly.

```
<HUAWEI> reset fragment-reassemble statistics
```

14.21.45 stream-reassemble enable

Function

The **stream-reassemble enable** command enables TCP stream reassembly.

The **undo stream-reassemble enable** command disables TCP stream reassembly.

By default, TCP stream reassembly is enabled.

Format

stream-reassemble enable

undo stream-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If TCP stream reassembly is disabled, TCP packets will not be reassembled and will not be inspected. Meanwhile, security inspections based on TCP streams may also fail.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable TCP stream reassembly.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble enable
```

14.21.46 stream-reassemble enhanced-mode

Function

The **stream-reassemble enhanced-mode** command enables the enhanced traffic reassembly mode.

The **undo stream-reassemble enhanced-mode** command disables the enhanced traffic reassembly mode.

By default, the enhanced traffic reassembly mode is disabled.

Format

stream-reassemble enhanced-mode

undo stream-reassemble enhanced-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command is used to enable the enhanced traffic reassembly mode in the bypass deployment scenario. After this mode is enabled, sequence number reassembly is supported when TCP data packets and three-way handshake packets are out of order.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the enhanced traffic reassembly mode.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble enhanced-mode
```

14.21.47 stream-reassemble overflow-mode

Function

The **stream-reassemble overflow-mode** command configures the action for cache overflow during TCP stream reassembly.

The **undo stream-reassemble overflow-mode** command restores the default action for cache overflow during TCP stream reassembly.

By default, the action for cache overflow during TCP stream reassembly is **forward**.

Format

stream-reassemble overflow-mode { **discard** | **forward** }

undo stream-reassemble overflow-mode

Parameters

Parameter	Description	Value
discard	Discards the packets that overflow the cache.	-
forward	Forwards the fragments that overflow the cache.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the action for cache overflow during TCP stream reassembly to **forward**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble overflow-mode forward
```

14.21.48 stream-reassemble overlap-mode

Function

The **stream-reassemble overlap-mode** command configures the action for overlapping packets during TCP stream reassembly.

The **undo stream-reassemble overlap-mode** command restores the default action for overlapping packets during TCP stream reassembly.

By default, the action for the overlapping packets during TCP stream reassembly is **preserve**.

Format

stream-reassemble overlap-mode { **preserve** | **overwrite** }

undo stream-reassemble overlap-mode

Parameters

Parameter	Description	Value
preserve	Preserves overlapping packets.	-
overwrite	Overwrites overlapping packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the action for the overlapping packets during TCP stream reassembly to **preserve**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble overlap-mode preserve
```

14.21.49 stream-reassemble session-cache

Function

The **stream-reassemble session-cache** command configures the maximum cache for each session during TCP stream reassembly for out-of-order packets.

The **undo stream-reassemble session-cache** command restores the default values.

By default , the maximum cache for each session during TCP stream reassembly for out-of-order packets is 128 KB.

Format

stream-reassemble session-cache *session-cache-value*

undo stream-reassemble session-cache

Parameters

Parameter	Description	Value
session-cache-value	Specifies the maximum cache for a session.	The value is an integer ranging from 0 to 256, in KB. The default value is 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the *session-cache-value* is 0 or the size of a single session exceeds the *session-cache-value*, the stream reassembly for out-of-order packets becomes invalid.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the maximum cache for each session to 16 KB during stream reassembly.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble session-cache 16
```

14.21.50 stream-reassemble session-timeout

Function

The **stream-reassemble session-timeout** command set the timeout time for out-of-sequence TCP packet inspection.

The **undo stream-reassemble session-timeout** command restores the default setting.

By default, the timeout time for out-of-sequence TCP packet inspection is 10 seconds.

Format

stream-reassemble session-timeout *session-timeout-value*

undo stream-reassemble session-timeout

Parameters

Parameter	Description	Value
session-timeout-value	Specifies the timeout time.	The value is an integer ranging from 0 to 1200, in seconds. The default value is 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, out-of-sequence TCP packet inspection is enabled on the switch.

- When *session-timeout-value* is 0, out-of-sequence TCP packet inspection is disabled.
- When *session-timeout-value* is greater than 0 and the time when TCP packets are out of order is smaller than or equal to *session-timeout-value*, the switch will attempt to reassemble traffic.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the timeout time for out-of-sequence TCP packet inspection to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble session-timeout 20
```

14.21.51 stream-reassemble tcp-option check

Function

The **stream-reassemble tcp-option check** command enables the TCP option check function.

The **undo stream-reassemble tcp-option check** command disables the TCP option check function.

By default, the TCP option check function is disabled.

Format

stream-reassemble tcp-option check

undo stream-reassemble tcp-option check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is enabled, the engine directly discards packets with abnormal TCP options.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the TCP option check function.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble tcp-option check
```

14.21.52 stream-reassemble timestamp check

Function

The **stream-reassemble timestamp check** command enables timestamp check of TCP flow reassembly.

The **undo stream-reassemble timestamp check** command disables timestamp check of TCP flow reassembly.

By default, the timestamp check function is disabled.

Format

stream-reassemble timestamp check

undo stream-reassemble timestamp check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you enable timestamp check of TCP flow reassembly, the device verifies the timestamp option of TCP packets. If the option is incorrect, the device discards the packets.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable timestamp check of TCP flow reassembly.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble timestamp check
```

14.21.53 stream-reassemble user-configure defense-check

Function

The **stream-reassemble user-configure defense-check** command enables the TCP attack defense function.

The **undo stream-reassemble user-configure defense-check** command disables the TCP attack defense function.

By default, the TCP attack defense function is disabled.

Format

stream-reassemble user-configure defense-check

undo stream-reassemble user-configure defense-check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this function is enabled, the switch directly discards abnormal TCP packets.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the TCP attack defense function.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] stream-reassemble user-configure defense-check
```

14.21.54 update abort

Function

The **update abort** command aborts the update process of the application identification signature database.

Format

update abort

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In online/immediate updates, the device needs to connect to the update center. If the network rate is too low and impacts the services and device performance, you can run the **update abort** command to abort the update and then retry updating when appropriate. In update retires, you cannot perform other update operations. If you need to use another update method, run the **update abort** command to abort the update process first.

Prerequisites

The **update abort** command can only be used for online/immediate updates or update retries.

Example

Abort the immediate update process.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update online sa-sdb
[HUAWEI] update abort
```

14.21.55 update apply sa-sdb

Function

The **update apply sa-sdb** command installs the downloaded update files of the application identification signature database.

By default, the upgrade file is automatically installed after being downloaded in an online upgrade scenario. If manual installation confirmation has been enabled, the upgrade file need to be manually installed.

Format

update apply sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If manual installation confirmation has been enabled by the **update confirm sa-sdb enable** command, run the **update apply sa-sdb** command to install the update files.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Install the application identification signature database update files.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update apply sa-sdb
```

14.21.56 update confirm sa-sdb enable

Function

The **update confirm sa-sdb enable** command enables manual confirmation of the application identification signature database installation.

The **undo update confirm sa-sdb enable** command disables manual confirmation of the application identification signature database installation.

By default, the manual confirmation of the application identification signature database installation is disabled.

Format

update confirm sa-sdb enable

undo update confirm sa-sdb enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In an online upgrade scenario, the upgrade file is automatically installed after being downloaded by default. To make the upgrade file not to be automatically installed after being downloaded, run the **update confirm sa-sdb enable** command to enable manual confirmation of the application identification signature database installation and run the **update apply sa-sdb** command to manually install the upgrade file.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable manual confirmation for the application identification signature database installation.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update confirm sa-sdb enable
```

14.21.57 update download-server aging-time

Function

The **update download-server aging-time** command specifies the aging time of the download server.

The **undo update download-server aging-time** command prevents the download server from aging.

By default, the aging time of the download server is 7 days.

Format

update download-server aging-time *age-time*

undo update download-server aging-time

Parameters

Parameter	Description	Value
age-time	Aging time of the download server	The value is an integer ranging from 1 to 360, in days. The default value is 7.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the download server is normal and has not been expired, you do not need to re-obtain the IP address of the download server. You need to re-obtain the IP address of the download server when the server has expired or is abnormal. You can use this command to adjust the aging time of the download server.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the aging time of the download server to 10 days.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update download-server aging-time 10
```

14.21.58 update force apply sa-sdb

Function

The **update force apply sa-sdb** command forcibly installs the downloaded update files of the application identification signature database.

Format

update force apply sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you run the **update apply sa-sdb** command to download update files, the update fails in case of insufficient system memory. In this case, you can run the **update force apply sa-sdb** command to forcibly install downloaded update files.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

Running the **update force apply sa-sdb** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

Example

Forcibly install the application identification signature database update files.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update force apply sa-sdb
```

14.21.59 update force local sa-sdb

Function

The **update force local sa-sdb** command configures forcible manual update of the local application identification signature database.

Format

update force local sa-sdb file *filename*

Parameters

Parameter	Description	Value
file *filename*	Indicates the file used for the update. You must upload the update files to the device memory before the update.	The absolute path of a file is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you run the **update local sa-sdb** command to update the application identification signature database locally, the update fails in case of insufficient system memory. In this case, you can run the **update force local sa-sdb** command to forcibly update the local application identification signature database.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

Running the **update force local sa-sdb** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

Example

Forcibly update the local application identification signature database using file hda1:/cnc_h10010000_2017111500.zip.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update force local sa-sdb file hda1:/cnc_h10010000_2017111500.zip
```

14.21.60 update force online sa-sdb

Function

The **update force online sa-sdb** command forcibly configures the immediate updates of the application identification signature database.

Format

update force online sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you run the **update online sa-sdb** command to immediately update the application identification signature database, the update fails in case of insufficient system memory. In this case, you can run the **update force online sa-sdb** command to immediately update the application identification signature database.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

Running the **update force online sa-sdb** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

Example

Forcibly update the application identification signature database.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update force online sa-sdb
```

14.21.61 update force restore sdb-default sa-sdb

Function

The **update force restore sdb-default sa-sdb** command forcibly restores the application identification signature database to the factory default version.

Format

update force restoresdb-default sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you run the **update restore sdb-default sa-sdb** command to restore the application identification signature database to the default version, the restore fails if the system memory is insufficient. In this case, you can attempt to run the **update force restore sdb-default sa-sdb** command to forcibly restore the application identification signature database to the default version.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

- After you run the **update force restore sdb-default sa-sdb** command, the application identification signature database files corresponding to the rollback version and download version of the application identification signature database will be deleted.
- Running the **update force restore sdb-default sa-sdb** command causes the IAE not to take effect within a short period, resets all IAE-related session tables, and interrupts some services. Therefore, exercise caution when running this command.

Example

Forcibly restore the application identification signature database to the factory default version.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update force restore sdb-default sa-sdb
```

14.21.62 update force rollback sa-sdb

Function

The **update force rollback sa-sdb** command forcibly rolls back the version of the application identification signature database.

Format

update force rollback sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you run the **update rollback sa-sdb** command to roll back the version of the application identification signature database, the rollback fails in case of insufficient system memory. In this case, you can run the **update force rollback sa-sdb** command to forcibly roll back the version of the application identification signature database.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

Running the **update force rollback sa-sdb** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

Example

Forcibly roll back the version of the application identification signature database.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update force rollback sa-sdb
```

14.21.63 update host source

Function

The **update host source** command specifies the source IP address of online update request packets.

The **undo update host source** command deletes the specified source IP address of online update request packets.

By default, the system searches a route based on the IP address of the update center and uses the IP address of the outgoing interface as the source IP address of update request packets.

Format

update host source { *interface-type interface-number* | **ip** *ip-address* [**vpn-instance** *vpn-instance*] }

undo update host source [**ip**]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the IP address of the source interface of online update request packets.	-
ip *ip-address*	Specifies the source IP address of online update request packets.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the name of a VPN instance.	The name is a string of 1 to 31 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device connects to the Internet through a VPN instance, these commands are mandatory. If the commands are not configured, the update will fail.

- When **update host source** *interface-type interface-number* is configured, the interface must be bound to the corresponding VPN instance name.
- When the **update host source ip** *ip-address* command is configured, **vpn-instance** *vpn-instance* must be specified.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

Instructions on these commands are as follows:

- The interface specified in the **update host source** *interface-type interface-number* command is not necessarily the outgoing interface of update request packets. This command actually specifies the IP address of a specific interface as the source IP address. To send update request packets, the system checks the route information to determine the outgoing interface.

  Do not specify an interface that is bound to a virtual system. Otherwise, the update will fail.
- If the interface has multiple IP addresses, run the **update host source ip** *ip-address* command to set the source IP address of update request packets and ensure that the device can receive the reply packets. Otherwise, the online update may fail.
- When both **update host source** *interface-type interface-number* and **update host source ip** *ip-address* [**vpn-instance** *vpn-instance*] are configured, the system preferentially uses the specified IP address as the source IP address of update request packets. That is, the **update host source** *interface-type interface-number* command does not take effect.

NOTE

After configuring this command, the device performs remote URL query within the VPN that the interface belongs to.

Example

Set the IP address of the interface used for online update to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet1/0/0] quit
[HUAWEI] update host source gigabitethernet 0/0/1
```

Set the source IP address of online update request packets to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update host source ip 10.1.1.1
```

14.21.64 update local sa-sdb

Function

The **update local sa-sdb** command configures manual update of the local application identification signature database.

Format

update local sa-sdb file *filename*

Parameters

Parameter	Description	Value
file *filename*	Specifies the update file. You must upload the update files to the device memory before the update.	The absolute path of a file is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device cannot connect to the network, download the update files from the security center to a PC and upload the files to the device memory. Then run the **update local** command to update the application identification signature database.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Manually update the local application identification signature database using file hda1:/cnc_h10010000_2017111500.zip.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update local sa-sdb file hda1:/cnc_h10010000_2017111500.zip
```

14.21.65 update online sa-sdb

Function

The **update online sa-sdb** command configures the immediate updates of the application identification signature database.

Format

update online sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The online update modes of the application identification signature database include scheduled update and immediate update. Generally, scheduled update is used. In some case, the application identification signature database needs to be updated to the latest version immediately. If the scheduled update period does not expire, you can run the **update online sa-sdb** command to start immediate update. Before the update, you need to check whether the domain name or IP address of the update center (sec.huawei.com) is accessible.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Update the application identification signature database immediately.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update online sa-sdb
```

14.21.66 update proxy

Function

The **update proxy** command sets the IP address or domain name of the proxy server.

The **undo update proxy** command deletes the proxy server setting.

By default, no IP address or domain name is configured for the proxy server.

Format

update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* [**password** *password*]]

undo update proxy

Parameters

Parameter	Description	Value
domain *domain-name*	Indicates the domain name of the proxy server.	The value is a string of 1 to 64 characters. It cannot contain spaces.
ip *ip-address*	Indicates the IP address of the proxy server.	The value is in dotted decimal notation.
port *port-number*	Indicates the port number of the proxy server.	The value is an integer in the range from 1 to 65535. The default value is 80.
user *user-name*	Indicates the user name for logging in to the proxy server.	The user name is a string and must have been set on the proxy server. If the user name does not contain spaces, it ranges from 1 to 32 characters. If the user name contains spaces, it ranges from 3 to 34 characters, and must be enclosed with double quotation marks (""), for example, "user for test".
password *password*	Indicates the password for logging in to the proxy server.	The password is a string and must be the same as the password corresponding to the user name of the proxy server. ● If the password does not contain spaces, it ranges from 1 to 32 characters. If the password contains spaces, it ranges from 3 to 34 characters, and must be enclosed with double quotation marks (""). ● The password cannot contain only asterisks (*).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

After the password for logging in to the proxy server is configured, you need to reconfigure the password if a version earlier than V200R021C10 is upgraded to V200R021C10 or later, or V200R021C10 or later is downgraded to a version earlier than V200R021C10.

Example

Configure the proxy server.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update proxy ip 192.168.2.33 port 8080 user test password Hello!123
```

14.21.67 update proxy enable

Function

The **update proxy enable** command enables the application identification signature database proxy update function.

The **undo update proxy enable** command disables the application identification signature database proxy update function.

By default, the application identification signature database proxy update function is disabled.

Format

update proxy enable

undo update proxy enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **update proxy enable** command used for updating the application identification signature database through a proxy server.

After this function is enabled, you must run the **update proxy** command to set the proxy server. Otherwise, the device cannot connect to the update server through the proxy server.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Precautions

During the application identification signature database update through a proxy server, HTTP will be used, causing security risks. You are advised to update the application identification signature database in local or direct update mode.

Example

Enable the application identification signature proxy update function.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update proxy enable
```

14.21.68 update restore engine

Function

The **update restore engine** command restores the engine to the factory default version.

Format

update restore engine

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Restore the engine to the factory default version.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update restore engine
```

14.21.69 update restore sdb-default sa-sdb

Function

The **update restore sdb-default sa-sdb** command restores the application identification signature database to the factory default version.

Format

update restore sdb-default sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you run the **update restore sdb-default sa-sdb** command, the application identification signature database files corresponding to the rollback version and download version of the application identification signature database will be deleted. Therefore, exercise caution when running this command.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Restore the application identification signature database to the factory default version.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update restore sdb-default sa-sdb
```

14.21.70 update rollback sa-sdb

Function

The **update rollback sa-sdb** command rolls back the version of the application identification signature database.

Format

update rollback sa-sdb

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run the **update rollback sa-sdb** command to roll back the current version of the application identification signature database to an earlier version. Only one earlier version is available for version rollback. If you run the **update rollback sa-sdb** command a second time, the version of the application identification signature database is rolled back to the current version again.

NOTE

The version rollback function is unavailable before the second update is complete.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Roll back the version of the application identification signature database.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update rollback sa-sdb
```

14.21.71 update schedule enable

Function

The **update schedule enable** command enables scheduled update time for the application identification signature database.

The **undo update schedule enable** command disables scheduled update time for the application identification signature database.

By default, scheduled update time for the application identification signature database is enabled.

Format

update schedule sa-sdb enable

undo update schedule sa-sdb enable

Parameters

Parameter	Description	Value
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Enable the scheduled update time function for the application identification signature database.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update schedule sa-sdb enable
```

14.21.72 update schedule retry-download interval

Function

The **update schedule retry-download interval** command sets the retry interval for downloading the application identification signature database for scheduled update.

The **undo update schedule retry-download interval** command restores the default interval.

By default, the retry interval for downloading the application identification signature database for scheduled update is 3600 seconds.

Format

update schedule retry-download interval *interval-value*

undo update schedule retry-download interval

Parameters

Parameter	Description	Value
interval-value	Specifies the retry interval for downloading the application identification signature database for scheduled update.	The value is an integer ranging from 300 to 3600, in second. The default value is 3600.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In case of scheduled update, if the update server is busy, the application identification signature database may fail to be download, causing an update failure. Then, the device will retry downloading the application identification signature database. The **update schedule retry-download interval** command is used to set the retry interval for downloading the application identification signature database.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the retry interval for downloading the application identification signature database for scheduled update to 1800s.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update schedule retry-download interval 1800
```

14.21.73 update schedule retry-load interval

Function

The **update schedule retry-load interval** command sets the retry interval for loading the application identification signature database for scheduled update.

The **undo update schedule retry-load interval** command restores the default interval.

By default, the retry interval for loading the application identification signature database for scheduled update is 3600 seconds.

Format

update schedule retry-load interval *interval-value*

undo update schedule retry-load interval

Parameters

Parameter	Description	Value
interval-value	Specifies the retry interval for loading the application identification signature database for scheduled update.	The value is an integer ranging from 300 to 3600, in second. The default value is 3600.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In case of scheduled update, if the memory of the device is insufficient, the device may fail to load the downloaded application identification signature database. Then, the device will retry loading the application identification signature database. The **update schedule retry-load interval** command is used to set the retry interval for loading the application identification signature database.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the retry interval for loading the application identification signature database for scheduled update to 1800s.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update schedule retry-load interval 1800
```

14.21.74 update schedule

Function

The **update schedule** command sets scheduled update time for the signature database.

By default, the scheduled update time for the signature database is not set.

Format

update schedule [**sa-sdb**] [{ **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*]

Parameters

Parameter	Description	Value
sa-sdb	Indicates scheduled update time of the application identification signature database.	-
daily	Indicates daily update of an application identification signature database.	-
weekly { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** }	Indicates weekly update of an application identification signature database.	-

Parameter	Description	Value
time	Specifies the time in a day for the scheduled update of the application identification signature database.	The format is **hh:mm**. The hour and minute are separated by a colon (:). The **hh** value is an integer ranging from 0 to 23 and the **mm** value is an integer ranging from 0 to 59.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If time is not specified, the **update schedule** can update the application identification signature database daily at any point during the time range 22:00 to 08:00.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Configure a scheduled update of the application identification signature database at 02:00 every Wednesday.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update schedule weekly Wed 02:00
```

Configure a scheduled update of the application identification signature database at 03:00 every day.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update schedule daily 03:00
```

14.21.75 update server

Function

The **update server** command sets the IP address or domain name of the update server.

The **undo update server** command deletes the IP address or domain name of the update server.

By default, the domain name of the update server is sec.huawei.com.

Format

update server { { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] | **ca-certificate** *ca-certificate-name* }

undo update server

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of the update server.	The value is a string of 1 to 64 characters, spaces not supported.
ip *ip-address*	Specifies the IP address of the update server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the update server.	The value is an integer ranging from 1 to 65535.
ca-certificate *ca-certificate-name*	Specifies the CA certificate name of the update server.	The value is a string of 1 to 64 characters. The value must be the name of an existing CA certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the domain name of the update server is sec.huawei.com, the HTTP port number is 80 and the HTTPS port number is 443.

Prerequisites

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Set the IP address of the update server to 10.1.1.1 and port number to 86.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] update server ip 10.1.1.1 port 86
```

14.22 Network Deception Configuration Commands

14.22.1 Command Support

Only the following switch models support deception:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

14.22.2 deception

Function

The **deception** command creates and enters the deception view.

The **undo deception** command deletes the deception view.

By default, no deception view exists on the switch.

Format

deception

undo deception

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the deception function, run this command to create and enter the deception view first.

Precautions

The **undo deception** command will delete all deception configurations. Therefore, confirm your operation before using this command.

Example

Create and enter the deception view.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception]
```

14.22.3 deception aci enable

Function

The **deception aci enable** command enables the Access Control Isolation (ACI) deception function.

The **undo deception aci enable** command disables the ACI deception function.

The ACI deception function is disabled by default.

Format

deception aci detect-network { **id** *id-number* | **all** } **enable**

undo deception aci detect-network { **id** *id-number* | **all** } **enable**

Parameters

Parameter	Description	Value
id *id-number*	Specifies the ID of a network segment to be detected.	The value is an integer ranging from 1 to 50.
all	Specifies all network segments to be detected.	-

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

ACI is an isolation scheme for controlling intranet communication through DNS access. After this function is enabled, the source or destination address in the detected network segment must be accessed through the domain name. If the IP address is directly accessed or the IP address that does not exist is accessed, traffic is deceived to the Decoy.

The DecoySensor parses DNS reply packets and establishes mappings between the source addresses of DNS request packets and the IP addresses corresponding to the domain names in DNS reply packets (that is, the ACI table). Subsequent TCP SYN packets and ICMP ping packets will match the ACI table. Traffic that fails to match the table is deceived to the Decoy for in-depth interactive detection.

ACI also supports the configuration of an ACI suffix using the **deception aci suffix** command. The default value is **aci**. An ACI suffix functions as an intranet access key. For example, if the IP address of the server in the detected network segment is 192.168.1.1, the server must be accessed through **192.168.1.1.aci** if the default ACI suffix is used. If the IP address of the server is directly accessed or the IP address with an incorrect ACI suffix is accessed, traffic is deceived to the Decoy for in-depth interactive detection.

The ACI deception function takes effect only after the deception function is enabled using **deception enable**.

Example

Enable the ACI deception function.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception aci detect-network all enable
```

14.22.4 deception aci lack decoy

Function

The **deception aci lack decoy** command sets the policy used in the case of a full ACI table to deceive.

The **undo deception aci lack decoy** sets the policy used in the case of a full ACI table to permit.

The policy used in the case of a full ACI table is permit by default.

Format

deception aci lack decoy

undo deception aci lack decoy

Parameters

None

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

The ACI table is space-limited. If there are a large number of intranet DNS requests and the ACI table cannot store new mappings, traffic will be deceived or permitted based on the configuration of this command.

To prevent a full ACI table, you can run the **deception aci timeout** command to set a shorter aging time for ACI entries.

Example

Set the policy used in the case of a full ACI table to deceive.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception aci lack decoy
 Warning: If the configured ACI resources are insufficient, the default action is decoy which affects services.
Continue? [Y/N]:y
```

14.22.5 deception aci suffix

Function

The **deception aci suffix** command sets an ACI suffix.

The **undo deception aci suffix** command restores the default ACI suffix.

The ACI suffix is **aci** by default.

Format

deception aci suffix *suffix-value*

undo deception aci suffix

Parameters

Parameter	Description	Value
suffix-value	Specifies the ACI suffix.	The value is a string of at most eight characters, including letters, digits, and hyphens (-). It must start with a letter.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

An ACI suffix functions as an intranet access key. For example, if the IP address of the server in the detected network segment is 192.168.1.1, the server must be accessed only through **192.168.1.1.aci** if the default ACI suffix is used. If the IP address of the server is directly accessed or the IP address with an incorrect ACI suffix is accessed, traffic is deceived to the Decoy or discarded.

After the ACI suffix is changed, you need to run the **reset deception aci** command to update the ACI entries. Otherwise, the old ACI suffix becomes invalid only after the ACI entries age. After the ACI entries are updated, the access initiated by a terminal is deceived when the DNS record of the terminal does not age. Therefore, change the ACI suffix when no service traffic exists.

Example

Set the ACI suffix to **testaci**.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception aci suffix testaci
```

14.22.6 deception aci timeout

Function

The **deception aci timeout** command sets the aging time of ACI entries.

The **undo deception aci timeout** command restores the default aging time of ACI entries.

By default, the aging time of ACI entries is 60s. When a new DNS reply packet arrives, the corresponding ACI entry is updated.

Format

deception aci timeout *timeout-value*

undo deception aci timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the aging time of ACI entries.	The value is an integer ranging from 10 to 300, in seconds.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

The DecoySensor replaces the TTL in the DNS reply packet with the aging time configured in this command. The DNS TTL is the cache time of the DNS entries recorded by the terminal. After the time expires, the terminal initiates a DNS request again. After receiving the DNS reply packet, the DecoySensor updates the aging time of the corresponding ACI entry to ensure that the DNS entry recorded by the terminal and the ACI entry on the DecoySensor are aged or updated at the same time.

The ACI table is space-limited. If there are a large number of intranet DNS requests and the ACI table cannot store new mappings, traffic will be deceived or permitted based on the configuration of the **deception aci lack decoy** command. You can run the **deception aci timeout** command to set a shorter aging time for ACI entries.

If the intranet access is stable and there is a small number of DNS requests, you can set a longer aging time of ACI entries for better performance.

Example

Set the aging time of ACI entries to 100s.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception aci timeout 100
```

14.22.7 deception arp-request rate

Function

The **deception arp-request rate** command sets an IP address scanning threshold.

The **undo deception arp-request rate** command restores the IP address scanning threshold to the default value.

By default, the IP address scanning threshold is 10 times per 10 seconds.

Format

deception arp-request rate *rate-number*

undo deception arp-request rate

Parameters

Parameter	Description	Value
rate-number	Specifies an IP address scanning threshold.	The value is an integer in the range from 1 to 20000, in **"times per 10 seconds"**.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

If the frequency of scanning a destination IP address by a source IP address reaches the specified threshold, the switch considers the event to be a suspected attack. Once the switch detects that the scanned IP address is offline, it immediately lures the traffic to the Decoy for further detection.

Example

Set the IP address scanning threshold to 20 times per 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception arp-request rate 20
```

14.22.8 deception decoy-network

Function

The **deception decoy-network** command configures a bait network segment.

The **undo deception decoy-network** command deletes a bait network segment.

By default, no bait network segment is configured on the switch.

Format

deception decoy-network id *id-number* **destination** *ip-address* [*mask*] [**destination-port** *port* &<1-20>] [**vpn-instance** *vpn-instance-name*]

undo deception decoy-network { **all** | **id** *id-number* }

Parameters

Parameter	Description	Value
id *id-number*	Specifies the ID of a bait network segment.	The value is an integer in the range from 1 to 50.
destination *ip-address* [*mask*]	• *ip-address* specifies an IP address. • *mask* specifies the subnet mask of the bait network segment.	The value is in dotted decimal notation.
destination-port *port*	Specifies the destination TCP port number. **NOTE** If this parameter is specified, traffic will be lured immediately if this TCP port is scanned or the IP address corresponding to the TCP port is scanned.	The value is an integer in the range from 1 to 65535.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance for the bait network segment.	The VPN instance must be an existing one on the device.
all	Specifies all bait network segments.	-

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a bait network segment is configured, the switch does not detect whether the IP addresses on the bait network segment are online. If an IP address or TCP port on the bait network segment is scanned, the switch lures the scanning traffic to the Decoy for further attack detection. Therefore, you can add some idle IP addresses to the bait network segment.

Precautions

A deception whitelist configured using the **deception whitelist** command takes precedence over a bait network segment:

- If an IP address is in both the deception destination IP address whitelist and the bait network segment, the switch ignores IP address scanning and TCP port scanning on the IP address and does not lure the traffic destined for the IP address.
- If scanning is initiated by a whitelisted address and the scanned IP address is on the bait network segment, the switch does not lure the traffic.

A bait network segment cannot contain the device management address and any network segment (0.0.0.0). Otherwise, the devices cannot be managed remotely.

Example

Add 10.1.1.11 to the bait network segment.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception decoy-network id 1 destination 10.1.1.11
```

14.22.9 deception detect-network

Function

The **deception detect-network** command sets a network segment detected by the deception system.

The **undo deception detect-network** command deletes the detected network segment.

By default, no detected network segment is configured on the switch.

Format

deception detect-network id *id-number ip-address mask* [**vpn-instance** *vpn-instance-name*]

undo deception detect-network { **all** | **id** *id-number* }

Parameters

Parameter	Description	Value
id *id-number*	Specifies the ID of a detected network segment.	The value is an integer in the range from 1 to 50.
ip-address	Specifies the IP address of the detected network segment.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the detected network segment.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the detected network segment.	The VPN instance must be an existing one on the device.
all	Indicates that all network segments are detected for deception.	-

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The detected network segment is protected by the deception system:

- IP address scanning: Deception is triggered only when the destination IP address of scanning packets is on the detected network segment.
- TCP port scanning: Deception is triggered when the source or destination IP address of scanning packets is on the detected network segment.

Precautions

If you have configured a bait network segment using the **deception decoy-network** command, deception is triggered when the IP addresses on the bait network segment are scanned, with no need to configure these IP addresses in the detected network segment.

Example

Configure the deception system to detect the network segment **10.1.1.0/24**.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception detect-network id 1 10.1.1.0 255.255.255.0
```

14.22.10 deception dns enable

Function

The **deception dns enable** command enables the unknown-domain-name deception function.

The **undo deception dns enable** command disables the unknown-domain-name deception function.

The unknown-domain-name deception function is disabled by default.

Format

deception dns enable

undo deception dns enable

Parameters

None

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

After the unknown-domain-name deception function is enabled, the DecoySensor identifies DNS requests on the network. When DNS requests are quickly sent from the same source IP address, it is suspected that domain name scanning is performed for obtaining the real intranet IP address. When the rate of domain name scans reaches the threshold and related information in the DNS reply packet indicates that the domain name does not exist, the DecoySensor automatically constructs and returns a DNS reply packet. The IP address in the DNS reply packet is the IP address in the bait network segment and is in the same network segment as the source address for sending the DNS request packet. The subsequent access and attack to this IP address will be deceived to the Decoy for in-depth interactive detection.

The deception operation is performed only after a bait network segment that is the same as the detected network segment is configured using **deception decoy-network**. If the bait network segment is not configured, the DecoySensor sends only domain name scan threshold-crossing logs.

The unknown-domain-name deception function takes effect only after the deception function is enabled using **deception enable**.

Example

Enable the unknown-domain-name deception function.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception dns enable
```

14.22.11 deception dns-request rate

Function

The **deception dns-request rate** command sets the domain name scan threshold.

The **undo deception dns-request rate** command restores the default domain name scan threshold.

By default, the domain name scan threshold is 5 scans per second.

Format

deception dns-request rate *rate-number*

undo deception dns-request rate

Parameters

Parameter	Description	Value
rate-number	Specifies the domain name scan threshold.	The value is an integer ranging from 1 to 20000, in scans per second.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

When the rate of domain name scans sent from the same source IP address reaches the threshold and related information carried in the DNS reply packet indicates that the domain name does not exist, the DecoySensor determines that it is an attack. The DecoySensor automatically constructs and returns a DNS reply packet. The IP address corresponding to the domain name in the constructed DNS reply packet is the IP address in the bait network segment, and is in the same network segment as the source address for sending the DNS request packet. The subsequent access and attack to this IP address will be deceived to the Decoy.

Example

Set the domain name scan threshold to 300 scans per second.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception dns-request rate 300
```

14.22.12 deception enable

Function

The **deception enable** command enables the deception function.

The **undo deception enable** command disables the deception function.

By default, the deception function is disabled.

Format

deception enable

undo deception enable

Parameters

None

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After deception is enabled, the DecoySensor identifies IP address and TCP port scanning activities on the network and lures suspicious traffic to the Decoy. If the configuration is incorrect, normal network traffic may be affected. Before enabling deception, run the **display this** command in the deception view to confirm the deception configuration.

Prerequisites

- The optimized ARP reply function has been disabled using the **arp optimized-reply disable** command, and the VLANIF interface has been configured to send ARP packets destined for other devices to the CPU using the **undo arp optimized-passby enable** command.
- You have configured **deception detect-network** or **deception decoy-network**, or both of them. Otherwise, the deception function does not take effect.

Example

Enable the deception function.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception enable
```

14.22.13 deception decoy

Function

The **deception decoy** command sets a Decoy IP address.

The **undo deception decoy** command deletes a Decoy IP address.

By default, no Decoy IP address is configured on the switch.

Format

deception decoy destination *destination-ip* [**source** *source-ip*] [**vpn-instance** *vpn-instance-name*] [**backup destination** *destination-ip* [**source** *source-ip*] [**vpn-instance** *vpn-instance-name*]]

undo deception decoy

Parameters

Parameter	Description	Value
source *source-ip*	Specifies the IP address used by a switch to connect to a Decoy. If this parameter is not specified, the IP address of the outbound interface is used.	The value is in dotted decimal notation.

Parameter	Description	Value
destination *destination-ip*	Specifies a Decoy IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the Decoy.	The VPN instance must be an existing one on the device.
backup	Indicates the standby Decoy.	-

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting suspected attack traffic, the switch lures the traffic to a Decoy for further checks. Therefore, you must first run this command to configure the IP address of the Decoy.

If communication between the switch and active Decoy is abnormal, the switch sends the log and deceived traffic to the standby Decoy that can communicate with the switch.

Precautions

A switch cannot use the virtual IP address of a VRRP group or the IP address of the management network interface to connect to a Decoy.

Example

Set the Decoy IP address to **10.1.1.1**.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception decoy destination 10.1.1.1
```

14.22.14 deception ip-state detect rate

Function

The **deception ip-state detect rate** command configures the frequency of scanning IP addresses by the switch.

The **undo deception ip-state detect rate** command restores the default frequency of scanning IP addresses by the switch.

By default, the switch scans IP addresses 30 times per second.

Format

deception ip-state detect rate *rate-number*

undo deception ip-state detect rate

Parameters

Parameter	Description	Value
rate-number	Specifies the frequency of scanning IP addresses by the switch.	The value is an integer in the range from 1 to 4096, in **"times per second"**.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

The switch initiates IP address scanning on the network segment to be detected to check whether IP addresses are online. If the scanning frequency is too high, the network is affected. If the scanning frequency is too low, the switch takes a long time to learn about the online status of IP addresses. You need to configure a proper IP address scanning frequency based on the site requirements and live network quality.

Example

Set the frequency of scanning IP addresses by the switch to 40 times per second.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception ip-state detect rate 40
```

14.22.15 deception mac-address aging-time

Function

The **deception mac-address aging-time** command configures the interval at which the switch sends an ARP broadcast packet.

The **undo deception mac-address aging-time** command restores the default interval at which the switch sends an ARP broadcast packet.

By default, the switch sends an ARP broadcast packet at an interval of 290 seconds.

Format

deception mac-address aging-time *aging-time*

undo deception mac-address aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the interval at which the switch sends an ARP broadcast packet.	The value is an integer in the range from 10 to 1000000, in seconds.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

To perform spoofing on IP address scanning, the switch constructs a virtual MAC address and sends it to the scanning source. The scanning source then incorrectly considers that the IP address to be scanned is online, and the switch diverts subsequent traffic from the scanning source to a Decoy for attack detection. The Layer 2 switch records an ARP entry of the scanned IP address and virtual MAC address. To prevent packets destined for the scanned IP address from being broadcast on the network after the entry is aged out, the switch periodically sends an ARP broadcast packet that contains the mapping between the scanned IP address and the virtual MAC address to the Layer 2 switch. You can run the **deception mac-address aging-time** command to adjust the interval at which the switch sends an ARP broadcast packet.

Example

Set the interval at which the switch sends an ARP broadcast packet to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception mac-address aging-time 300
```

14.22.16 deception mode strict

Function

The **deception mode strict** command enables the strict deception mode.

The **undo deception mode** command disables the strict deception mode.

By default, the strict deception mode is not used.

Format

deception mode strict

undo deception mode

Parameters

None

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

Fixed networking and stable servers are prerequisites for the strict deception mode. After the strict deception mode is set, the switch immediately lures the traffic destined for offline IP addresses or unopened TCP ports to the Decoy for further detection.

In non-strict mode, deception is performed only when the following conditions are met:

- The IP scanning or TCP port scanning frequency initiated by an IP address reaches the specified threshold.
- An offline IP address or unopened TCP port is scanned.

Example

Enable the strict deception mode.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception mode strict
```

14.22.17 deception syn-connect rate

Function

The **deception syn-connect rate** command sets a TCP port scanning threshold.

The **undo deception syn-connect rate** command restores the TCP port scanning threshold to the default value.

By default, the TCP port scanning threshold is 100 times per second.

Format

deception syn-connect rate *rate-number*

undo deception syn-connect rate

Parameters

Parameter	Description	Value
rate-number	Specifies a TCP port scanning threshold.	The value is an integer in the range from 1 to 20000, in **"times per second"**.

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

If the frequency of scanning a TCP port by a source IP address reaches the specified threshold, the switch considers the event to be a suspected attack. Once the switch detects that the scanned TCP port is unopened, it immediately lures the traffic to the Decoy for further detection.

Example

Set the TCP port scanning threshold to 200 times per second.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception syn-connect rate 200
```

14.22.18 deception whitelist

Function

The **deception whitelist** command sets a deception whitelist.

The **undo deception whitelist** command deletes a deception whitelist.

By default, there is no deception whitelist.

Format

deception whitelist id *id-number* { **destination** | **source** } *ip-address* [*mask*] [**vpn-instance** *vpn-instance-name*]

undo deception whitelist { **all** | **id** *id-number* }

Parameters

Parameter	Description	Value
id *id-number*	Specifies a whitelist ID.	The value is an integer in the range from 1 to 50.
destination	Indicates the destination IP address whitelist.	-
source	Indicates the source IP address whitelist.	-
ip-address [*mask*]	Adds a specified IP address or IP address segment to the deception whitelist. ● *ip-address* specifies an IP address. ● *mask* specifies the subnet mask of the IP address segment.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the whitelisted IP address.	The VPN instance must be an existing one on the device.
all	Indicates all whitelists.	-

Views

Deception view

Default Level

2: Configuration level

Usage Guidelines

You can configure destination IP address whitelists and source IP address whitelists:

- Source IP address whitelist: If the source IP address of scanning packets is in the source IP address whitelist, the device does not lure the scanning packets sent from this IP address to the Decoy. The addresses of devices that proactively detect the network (such as the NMS) can be whitelisted to prevent deception.
- Destination IP address whitelist: If the destination IP address of scanning packets is in the destination IP address whitelist, the device does not lure the scanning packets sent to this IP address to the Decoy. The addresses of devices that do not respond to ARP requests or port connection requests (such as traditional printers) can be whitelisted to prevent deception.

Example

Add 10.1.1.10 to destination IP address whitelist.

```
<HUAWEI> system-view
[HUAWEI] deception
[HUAWEI-deception] deception whitelist id 1 destination 10.1.1.10
```

14.22.19 display deception aci

Function

The **display deception aci** command displays the ACI table.

Format

display deception aci [**source** *ip-address*]

Parameters

Parameter	Description	Value
source *ip-address*	Specifies the source IP address in an ACI entry.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The DecoySensor parses DNS reply packets and establishes mappings between the source addresses of DNS request packets and the IP addresses corresponding to the domain names in DNS reply packets (that is, the ACI table). Subsequent TCP SYN packets and ICMP ping packets will match the ACI table. Traffic that fails to match the table is deceived to the Decoy for in-depth interactive detection.

If the number of current entries approaches the upper limit, run the **deception aci timeout** command to set a shorter aging time for ACI entries.

Example

Display the ACI table.

```
<HUAWEI> display deception aci
 ------------------------------------------------------------------------------------------------------
 Current total number = 1
 ------------------------------------------------------------------------------------------------------
 source          destnation       time    vpn-instance
 ------------------------------------------------------------------------------------------------------
 192.168.1.1      172.16.2.1       192     public
```

Table 14-131 Description of the **display deception aci** command output

Item	Description
source	Source IP address initiating a DNS request
destnation	IP address corresponding to the domain name in the DNS reply packet
time	Remaining lifetime of the entry
vpn-instance	VPN instance to which the source IP address belongs

14.22.20 display deception arp-proxy

Function

The **display deception arp-proxy** command displays the interface IP address of the switch and the target IP addresses in the proxy ARP requests sent to the switch in the online IP address table.

Format

display deception arp-proxy

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The switch cannot scan its interface IP address and the target IP addresses in the proxy ARP requests sent to the switch. Therefore, the switch may lure the traffic destined for these IP addresses to a Decoy. To solve this problem, after the switch receives ARP requests destined for these IP addresses, the switch returns ARP reply packets, and the management plane instructs the deception module to add the target IP addresses in ARP requests to the online IP address table.

Example

Display the interface IP address of the switch and the target IP addresses in the proxy ARP requests sent to the switch in the online IP address table.

```
<HUAWEI> display deception arp-proxy
---------------------------------------------------------------------------------------------------------
```

```
Current total number = 1

-----------------------------------------------------------------------------------------------------------
ip-address       vlan   vpn-instance
10.1.1.1         10     default
-------------------------------------------------------------------------------
```

Table 14-132 Description of the **display deception arp-proxy** command output

Item	Description
Current total number	Number of entries.
ip-address	Interface IP address of the switch or the target IP address in the proxy ARP request sent to the switch.
vlan	VLAN ID corresponding to the IP address.
vpn-instance	VPN instance to which the IP address belongs.

14.22.21 display deception arp-request

Function

The **display deception arp-request** command displays the IP address scanning behavior detected by the switch.

Format

display deception arp-request [**source** *ip-address*]

Parameters

Parameter	Description	Value
source *ip-address*	Specifies the source IP address that initiates IP address scanning.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the IP address scanning behavior detected by the switch, so that you can configure a more accurate IP address canning threshold using the **deception arp-request rate** command. If an IP address is scanned at a lower frequency than the threshold specified by the **deception arp-**

request rate command but have been scanned for many times, the scanning behavior may be an attack.

Example

Display the IP address scanning behavior detected by the switch.

```
<HUAWEI> display deception arp-request
-------------------------------------------------------------------------------------------------
Current total number = 2

-------------------------------------------------------------------------------------------------
source          rate(num/10s)    number       vlan   vpn-instance
-------------------------------------------------------------------------------------------------
10.1.1.1        4                231          10     public
10.1.1.2        1                280          10     public
-------------------------------------------------------------------------------
```

Table 14-133 Description of the **display deception arp-request** command output

Item	Description
Current total number	Number of entries.
source	Source IP address that initiates IP scanning.
rate(num/10s)	IP address scanning frequency, in **"times per 10 seconds"**.
number	Number of IP address scanning times.
vlan	VLAN to which the source IP address belongs.
vpn-instance	VPN instance of the source IP address.

14.22.22 display deception config-flow

Function

The **display deception config-flow** command displays the configuration flow table.

Format

display deception config-flow [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a detected network segment, bait network segment, or deception whitelist is configured, a configuration flow table is generated. If the preceding configuration is changed, the switch checks whether the deceived traffic meets the conditions of configuration flow tables and determines whether to lure the traffic to the Decoy.

Example

Display the configuration flow table.

```
<HUAWEI> display deception config-flow

Slot: 0
------------------------------------------------------------------------------------------------------
CFG Flow ID 1 information:
------------------------------------------------------------------------------------------------------
Priority        :0
Action          :1
Causeid         :16384
Vpn-instance    :
Source IP       :10.10.11.11/255.255.255.255
------------------------------------------------------------------------------------------------------
CFG Flow ID 2 information:
------------------------------------------------------------------------------------------------------
Priority        :1
Action          :4
Causeid         :4096
Vpn-instance    :
Destination IP  :192.168.1.0/255.255.255.240
------------------------------------------------------------------------------------------------------
CFG Flow ID 3 information:
------------------------------------------------------------------------------------------------------
Priority        :3
Action          :8
Causeid         :1
Vpn-instance    :
Destination IP  :10.10.10.0/255.255.255.0
------------------------------------------------------------------------------------------------------
CFG Flow ID 4 information:
------------------------------------------------------------------------------------------------------
Priority        :3
Action          :8
Causeid         :1
Vpn-instance    :
Source IP       :10.10.10.0/255.255.255.0
------------------------------------------------------------------------------------------------------
CFG Flow ID 5 information:
------------------------------------------------------------------------------------------------------
Priority        :3
Action          :8
Causeid         :1
Vpn-instance    :
Destination IP  :192.168.1.0/255.255.255.0
------------------------------------------------------------------------------------------------------
```

```
CFG Flow ID 6 information:
-----------------------------------------------------------------------------------------------------
Priority        :3
Action          :8
Causeid         :1
Vpn-instance    :
Source IP       :192.168.1.0/255.255.255.0
-----------------------------------------------------------------------------------------------------
CFG Flow ID 7 information:
-----------------------------------------------------------------------------------------------------
Priority        :0
Action          :1
Causeid         :16384
Vpn-instance    :
Destination IP  :10.10.10.22/255.255.255.255
```

Table 14-134 Description of the **display deception config-flow** command output

Item	Description
Slot	Slot ID.
CFG Flow ID *n* information	Information about configuration flow table *n*.
Priority	Priority of the configuration flow entry. The value is in the range from 0 to 10, and a smaller value indicates a higher priority. If a flow matches multiple configuration flow entries, the configuration flow entry with the highest priority takes effect.
Action	Action taken on the packets matching the configuration flow entry: ● 1: Deception check is not performed on the packets. ● 2: The packets are discarded. ● 4 and 8: Deception check is performed on the packets.
Causeid	Type of packets. The value in 2^i, in which i can be as follows: ● 0: packets matching the deception detected network segment ● 12: packets matching the bait network segment ● 14: packets matching the deception whitelist
Vpn-instance	VPN instance.
Destination IP	Destination IP address of traffic.
Destination Port	Destination TCP port number of traffic.
Source IP	Source IP address of traffic.

14.22.23 display deception decoy-network

Function

The **display deception decoy-network** command displays a bait network segment.

Format

display deception decoy-network [**id** *id-number*]

Parameters

Parameter	Description	Value
id *id-number*	Specifies the ID of a bait network segment.	The value is an integer in the range from 1 to 50.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a bait network segment using the **deception decoy-network** command, you can run the **display deception decoy-network** command to check whether the bait network segment is correctly configured.

Example

Display all bait network segments.

```
<HUAWEI> display deception decoy-network
------------------------------------------------------------------------------------------------------------
Current total number = 1

------------------------------------------------------------------------------------------------------------
Decoy-network ID 1 information:
------------------------------------------------------------------------------------------------------------
source/mask              :any
destination/mask           :192.168.1.0/255.255.255.240
destination-port          :
vpn-instance             :
```

Table 14-135 Description of the **display deception decoy-network** command output

Item	Description
Current total number	Number of entries.

Item	Description
Decoy-network ID *i* information	Information about the bait network segment whose ID is *i*.
source/mask	Source IP address and subnet mask.
destination/mask	Destination IP address and subnet mask.
destination-port	Destination port number.
vpn-instance	VPN instance of the destination IP address.

14.22.24 display deception detect-network

Function

The **display deception detect-network** command displays the network segments detected for deception.

Format

display deception detect-network [**id** *id-number*]

Parameters

Parameter	Description	Value
id *id-number*	Specifies the ID of a detected network segment.	The value is an integer in the range from 1 to 50.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a detected network segment using the **deception detect-network** command, you can run the **display deception detect-network** command to check whether the detected network segment is correctly configured.

Example

Display the network segments detected for deception.

```
<HUAWEI> display deception detect-network
-------------------------------------------------------------------------------------------------------
```

```
Current total number = 1

---------------------------------------------------------------------------------------------------
id   ip-address/mask(For both source and destination)        vpn-
instance
---------------------------------------------------------------------------------------------------
1    192.168.10.0/255.255.255.0
```

Table 14-136 Description of the **display deception detect-network** command output

Item	Description
Current total number	Number of entries.
id	ID of a detected network segment.
ip-address/mask	IP address and subnet mask of the detected network segment.
vpn-instance	VPN instance of the detected network segment.

14.22.25 display deception dns

Function

The **display deception dns** command displays the domain name scan status.

Format

display deception dns [**source** *ip-address*]

Parameters

Parameter	Description	Value
source *ip-address*	Specifies the source IP address initiating the domain name scan.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By observing the domain name scan status, network administrators can set a more accurate domain name scan threshold using the **deception dns-request rate** command.

If the **rate** of a source address is low and does not reach the threshold but the **number** is large, a very patient hacker may be hidden behind this address.

Example

Display domain name scan status.

```
<HUAWEI> display deception dns
 -----------------------------------------------------------------------------
 Current total number = 2
 -----------------------------------------------------------------------------
 source           number    rate(num/s)    error-aci      vpn-instance
 -----------------------------------------------------------------------------
 192.168.1.1      4          231          0             public
 192.168.1.2      1          280          0             public
 -----------------------------------------------------------------------------
 recent request dns domain :
 www.huawei.com
 192.168.1.3.aci
```

Table 14-137 Description of the **display deception dns** command output

Item	Description
source	Source IP address initiating the domain name scan
number	Number of domain name scans
rate(num/s)	Rate of domain name scans, in scans per second
error-aci	Number of ACI suffix mismatches in DNS requests in ACI format
vpn-instance	VPN instance to which the source IP address belongs
recent request dns domain	Domain name in the latest request. A maximum of five domain names can be recorded

14.22.26 display deception flow

Function

The **display deception flow** command displays the deception flow table.

Format

display deception flow [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In the deception flow table, you can view the traffic that meets certain conditions and will be sent to the deception module. The deception module then determines whether to lure the traffic to the Decoy based on the scanned IP address and TCP port.

Precautions

When a detected network segment, bait network segment, or deception whitelist is configured, a deception flow table is generated.

Example

Display the deception flow table.

```
<HUAWEI> display deception flow

Slot: 0
--------------------------------------------------------------------------------
Flow ID 1 information:
--------------------------------------------------------------------------------
Status          :Valid
Destination mac :0050-568c-1bbc
Vpn-instance    :
--------------------------------------------------------------------------------
Flow ID 2 information:
--------------------------------------------------------------------------------
Status          :Valid
Vpn-instance    :
Eth_type        :Arp
--------------------------------------------------------------------------------
Flow ID 4 information:
--------------------------------------------------------------------------------
Status          :Valid
Vpn-instance    :
Protocol        :Tcp
Tcp_flag        :Syn
--------------------------------------------------------------------------------
Flow ID 5 information:
--------------------------------------------------------------------------------
Status          :Valid
Vpn-instance    :
Protocol        :Tcp
Tcp_flag        :Syn | Ack
--------------------------------------------------------------------------------
Flow ID 6 information:
--------------------------------------------------------------------------------
Status          :Valid
Vpn-instance    :
Protocol        :Tcp
Tcp_flag        :Rst | Ack
```

Table 14-138 Description of the **display deception flow** command output

Item	Description
Slot	Slot ID.
Flow ID *n* information	Information about deception flow table *n*.
Status	Whether the deception flow entry is valid: ● Valid ● Invalid
Vpn-instance	VPN instance to which the inbound interface of the scanning packets belongs.
Destination mac	MAC address used by the switch to perform ARP spoofing on IP address scanning in a suspected attack.
Destination IP	Destination IP address of scanning packets.
Destination Port	Destination port number of scanning packets.
Source IP	Source IP address of scanning packets.
Protocol	Transport layer protocol type of scanning packets.
Eth_type	Layer 2 protocol type of scanning packets.
Tcp_flag	TCP flag.

14.22.27 display deception decoy status

Function

The **display deception decoy status** command displays the registration status of a DecoySensor on a Decoy.

Format

display deception decoy status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A DecoySensor initiates registration to a Decoy. If the registration succeeds:

- The registration status changes from **INIT** to **ALIVE**.
- The Decoy informs the DecoySensor of a port list for which the deception service is provided. Only the traffic whose destination ports in the list can be lured to the Decoy for further detection.
- The DecoySensor and Decoy send heartbeat packets to each other every 5 seconds. If the DecoySensor does not receive heartbeat packets from the Decoy within 60 seconds, its registration status changes to **INIT**. If the Decoy does not receive heartbeat packets from the DecoySensor within 60 seconds, it sends a deregistration packet to the DecoySensor. After the DecoySensor receives the packet, its registration status changes to **INIT**.

Example

Display the registration status of a DecoySensor on a Decoy.

```
<HUAWEI> display deception decoy status
 Decoy register status information:
   Register status                                   : alive
   Decoy select                                      : master
   Online time                                       : 37062(s)
   Send heartbeat timeout                                  : 0(s)
   Receive heartbeat timeout                               : 5(s)
 Decoy register port information:
   445      80       8080      443       22
   3389      21       3306      6379
```

Table 14-139 Description of the **display deception decoy status** command output

Item	Description
Decoy register status information	Registration status of a DecoySensor on a Decoy.
Register status	Registration status: ● init: Unregistered ● alive: Successfully registered
Decoy select	Currently connected Decoy ● master: Active ● backup: Standby
Online time	Duration of the connection to the Decoy.
Send heartbeat timeout	Period after the DecoySensor sent the last heartbeat packet, in seconds.
Receive Heartbeat timeout	Period after the DecoySensor received the last heartbeat packet, in seconds.
Decoy register port information	Port information of the deception service provided by the Decoy.

Item	Description
Decoy nonsupport port statistics	Port statistics not supported by the Decoy.

14.22.28 display deception instance

Function

The **display deception instance** command checks whether the deception process is normal.

Format

display deception instance

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Check whether the deception process is normal.

```
<HUAWEI> display deception instance
-------------------------------------------------------------------------------------------------------------

Instance        Slot      Cpu       State
-------------------------------------------------------------------------------------------------------------

decpt           *         *         normal
-------------------------------------------------------------------------------------------------------------

Current total number = 1
```

Table 14-140 Description of the **display deception instance** command output

Item	Description
Instance	Name of the deception process.

Item	Description
Slot	Slot ID.
Cpu	CPU ID.
State	Status: ● normal ● abnormal
Current total number	Total number of processes.

14.22.29 display deception interface

Function

The **display deception interface** command displays information about all deception-enabled interfaces.

Format

display deception interface

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view information about all deception-enabled interfaces, including the interface name, VLAN ID, and election status of interfaces for detecting IP address scanning. If a detected network segment has been configured using the **deception detect-network** command, the deception function can be configured only on the interfaces whose IP addresses are on the detected network segment.

Precautions

Interfaces whose IP addresses are not on the detected network segment cannot detect IP address scanning or participate in the election.

Example

Display information about all deception-enabled interfaces.

```
<HUAWEI> display deception interface
------------------------------------------------------------------------------------------------------
Current total number = 0
------------------------------------------------------------------------------------------------------
name                    ip-address         vlan   election-state   master-ip     vpn-instance
------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------
```

Table 14-141 Description of the **display deception interface** command output

Item	Description
name	Interface name.
ip-address	IP address of the interface.
vlan	VLAN to which the interface belongs.
election-state	Election status of the interface for detecting IP address scanning: ● master: If the device of the interface is elected as the active DecoySensor, it detects IP scanning on the network. ● slave: If the device of the interface is elected as a standby DecoySensor, it does not detect IP scanning on the network. ● init: Election is ongoing. ● --: The interface address is not in the detected network segment, so the interface does not participate in election.
master-ip	IP address of the active DecoySensor on the network segment.
vpn-instance	VPN instance of the interface.

14.22.30 display deception ip-redirect

Function

The **display deception ip-redirect** command displays information about deceived traffic due to the scanning of offline IP addresses.

Format

display deception ip-redirect [**source-ip** *ip-address*] [**destination-ip** *ip-address*] [**destination-port** *port*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Specifies the source IP address of the deceived traffic.	The value is in dotted decimal notation.
destination-ip *ip-address*	Specifies the destination IP address of the deceived traffic.	The value is in dotted decimal notation.
destination-port *port*	Specifies the destination port of the deceived traffic.	The value is an integer in the range from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about deceived traffic due to the scanning of offline IP addresses.

```
<HUAWEI> display deception ip-redirect
--------------------------------------------------------------------------------
Current total number = 1
--------------------------------------------------------------------------------
source          destination     port  out-vlan  vpn-instance  left-time(s) packets
--------------------------------------------------------------------------------
10.1.1.1        10.1.1.2         *      10       public        432          0
--------------------------------------------------------------------------------
```

Table 14-142 Description of the **display deception ip-redirect** command output

Item	Description
Current total number	Number of entries.
source	Source IP address of the deceived traffic.
destination	Destination IP address of the deceived traffic.
port	Destination port number of the deceived traffic.

Item	Description
out-vlan	VLAN ID of the deceived traffic.
vpn-instance	VPN instance of the deceived traffic.
left-time(s)	Remaining time before an entry ages, in seconds. The aging time is 10 minutes. If no traffic matches the entry within the aging time, the entry is deleted. If traffic matches the entry within the aging time, the aging time is updated.
packets	Number of the deceived packets.

14.22.31 display deception ip-state

Function

The **display deception ip-state** command displays the online status of IP addresses scanned by the switch.

Format

display deception ip-state [*ip-address*] [**verbose**]

Parameters

Parameter	Description	Value
ip-address	Displays the online status of a specified IP address.	The value is in dotted decimal notation.
verbose	Displays the detailed online status of IP addresses.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A switch checks the online status of IP addresses every 30 minutes. If traffic destined for address A is deceived, the interval for checking the online status of address A is shortened to 10 to 110 seconds to minimize the adverse impact on network services. The interval depends on the number of the deceived source addresses. More source addresses result in a longer interval.

The **display deception ip-state** command output does not contain the IP address online status if the **deception detect-network** command is not used to set any detected network segment.

Precautions

The IP addresses scanned by the DecoySensor must be on the detected network segment, and the DecoySensor has an IP address belonging to this network segment.

The **reset deception ip-state** command clears the IP address online status and immediately initiates the check on the online status of IP addresses.

Example

Display the online status of IP addresses scanned by the switch.

```
<HUAWEI> display deception ip-state
----------------------------------------------------------------------------------------------------
Current total number = 0

----------------------------------------------------------------------------------------------------
ip-address       state     vlan    vpn-instance
----------------------------------------------------------------------------------------------------
```

Display the detailed online status of IP addresses scanned by the switch.

```
<HUAWEI> display deception ip-state verbose
----------------------------------------------------------------------------------------
10.1.1.1 information:
----------------------------------------------------------------------------------------
state               :online
vlan                :10
vpn-instance        :
proxy_flag          :1
on2off_flag         :0
redirect_num        :0
----------------------------------------------------------------------------------------
Total displayed = 1
```

Table 14-143 Description of the **display deception ip-state** command output

Item	Description
Current total number	Number of entries.
ip-address information	Detailed information about the IP address.
ip-address	IP address.
state	Online status of the IP address: ● online ● offline
vlan	VLAN to which the IP address belongs.
vpn-instance	VPN instance of the IP address.

Item	Description
proxy_flag	Whether the IP address is learned through proxy ARP: ● 0: No ● 1: Yes
on2off_flag	Whether the IP address changes from online to offline: ● 0: No ● 1: Yes
redirect_num	Number of the deceived source IP addresses that scanned this IP address.

14.22.32 display deception port-redirect

Function

The **display deception port-redirect** command displays information about deceived traffic due to the scanning of unopened TCP ports.

Format

display deception port-redirect [**source-ip** *ip-address*] [**destination-ip** *ip-address*] [**destination-port** *port*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Specifies the source IP address of the deceived traffic.	The value is in dotted decimal notation.
destination-ip *ip-address*	Specifies the destination IP address of the deceived traffic.	The value is in dotted decimal notation.
destination-port *port*	Specifies the destination port of the deceived traffic.	The value is an integer in the range from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If it is found that deceived traffic is normal service traffic, run the **reset deception port-redirect** command to delete the corresponding entry from the deception flow table to release the traffic.

Example

Display information about deceived traffic due to the scanning of unopened TCP ports.

```
<HUAWEI> display deception port-redirect
---------------------------------------------------------------------------------------------------
Current total number = 0

---------------------------------------------------------------------------------------------------
source          destination     port   out-vlan vpn-instance  packets  left-
time(s)
---------------------------------------------------------------------------------------------------
```

Table 14-144 Description of the **display deception port-redirect** command output

Item	Description
Current total number	Number of entries.
source	Source IP address of the deceived traffic.
destination	Destination IP address of the deceived traffic.
port	Destination TCP port of the deceived traffic.
out-vlan	VLAN of the deceived traffic.
vpn-instance	VPN instance of the deceived traffic.
packets	Number of the deceived packets
left-time(s)	Remaining time before an entry ages, in seconds. The aging time is 10 minutes. If no traffic matches the entry within the aging time, the entry is deleted. If traffic matches the entry within the aging time, the aging time is updated.

14.22.33 display deception port-state

Function

The **display deception port-state** command displays the port openness status of a service host.

Format

display deception port-state [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a service host is busy, it responds with the RST-ACK packet even to normal TCP access. As a result, the DecoySensor incorrectly considers that the host port is not opened and deceives normal traffic. The DecoySensor records the port openness status based on the SYN-ACK packet returned by the service host and saves the record for 24 hours, until the record ages naturally or updated when a new SYN-ACK packet is generated. During this period, even if the DecoySensor receives the RST-ACK packet from the corresponding port, it does not deceive the traffic.

The DecoySensor records only the port openness status for TCP access requests whose destination IP addresses are in the detected network segment. The prerequisite for the DecoySensor to record the port openness status is that the in-depth interaction services must be supported by the Decoy.

The **reset deception port-state** command clears the current port openness status.

Examples

Display the port openness status of a service host.

```
<HUAWEI> display deception port-state
  --------------------------------------------------------------------------------
 Current total number = 2
--------------------------------------------------------------------------------
ip-address    :192.168.1.1
vpn-instance  :public port    state   time_out(h)
80      open    24
8080    open    24
445     open    24

ip-address    :192.168.1.2
vpn-instance  :public
port    state   time_out(h)
80      open    24
8080    open    24
445     open    2
```

Table 14-145 Description of the **display deception port-state** command output

Item	Description
ip-address	IP address of a service host
vpn-instance	VPN instance to which the IP address belongs
port	Port
state	Port openness status - open: Open
time_out(h)	Expiration time The new SYN-ACK packet will update the expiration time. If the expiration time is not updated within 24 hours, the service may have stopped working.

14.22.34 display deception statistics

Function

The **display deception statistics** command displays deception statistics.

Format

display deception statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To clear deception statistics, run the **reset deception statistics** command. Then, run the **display deception statistics** command to view deception statistics in this period.

Example

Display deception statistics.

```
<HUAWEI> display deception statistics
Dataplane normal statistics information:
  Receive local ip pkts                        : 9466
```

```
  Receive arp request pkts                    : 143087
  Receive arp reply pkts                    : 8671
  Receive don't need check pkts                   : 9471
  Receive from decoy pkts                    : 18605
  Receive from decoy reg acks                  : 14884
  Receive from decoy heartbeats                   : 3721
  Constructor arp request pkts                 : 8216
  Constructor arp reply pkts                  : 3860
  Send to decoy pkts                      : 14884
  Send to decoy regs                      : 14884
  Send channel success pkts                   : 12076
Dataplane discard statistics information:
  Send to decoy failed logs                  : 226
  VPN header illegal packets discarded                : 14884
Dataplane error statistics information:
```

Table 14-146 Description of the **display deception statistics** command output

Item	Description
Mgmtplane statistics information	Statistics about the management plane.
Rpc msg send success	Number of RPC messages that have been successfully sent.
Rpc msg recv success	Number of RPC messages that have been successfully received.
Rpc msg send instance not exist	Number of RPC messages that fail to be sent because the instance does not exist.
Rpc msg recv poll failed	Statistics about message query failures on the receiver.
Receive RPC msg	Number of received RPC messages.
Send RPC msg success	Number of RPC messages that have been successfully sent.
Dataplane normal statistics information	Statistics on normal packets
ReceiveRPCmsg	Number of received RPC messages
SendRPCmsgsuccess	Number of RPC messages that have been successfully sent
Receive total pkts	Number of received packets
Receive VLAN pkts	Number of received packets with VLAN tags
Receive local ip pkts	Number of packets destined for the local device or packets sent from the local device
Receive arp request pkts	Number of received ARP requests
Receive arp reply pkts	Number of received ARP replies

Item	Description
Receive offline ip icmp pkts	Number of received ICMP packets whose destination IP addresses are offline
Receive offline ip tcp pkts	Number of received TCP packets whose destination IP addresses are offline
Receive tcp syn pkts	Number of received SYN packets
Receive tcp syn ack pkts	Number of received SYN ACK packets
Receive tcp rst pkts	Number of received RST packets
Receive tcp decoy network pkts	Number of received packets that match the bait network segment
Receive don't need check pkts	Number of packets that do not need to be checked
Receive match acl	Number of packets that match ACLs
Receive from decoy pkts	Number of received packets from the Decoy
Receive arp consult pkts	Number of received ARP negotiation packets
Receive arp notify enable pkts	Number of received ARP notification enabling packets
Receive arp notify undo enable pkts	Number of received ARP notification disabling packets
Receive from decoy forward pkts	Number of received packets forwarded by the Decoy
Receive from decoy reg acks	Number of received registration reply packets from the Decoy
Receive from decoy update decoy ports	Number of packets received from the Decoy for updating the honeypot service port
Receive from decoy heartbeats	Number of received heartbeat packets from the Decoy
Receive total dns pkts	Number of received DNS packets
Receive dns request aci pkts	Number of received DNS packets with the ACI suffix
Receive aci syn pkts	Number of received SYN packets matching ACI entries
Constructor arp request pkts	Number of constructed ARP requests
Constructor arp reply pkts	Number of constructed ARP replies

Item	Description
Send to decoy pkts	Number of packets sent to the Decoy
Send to decoy forward pkts	Number of packets forwarded to the Decoy
Send to decoy regs	Number of registration packets sent to the Decoy
Send to decoy heartbeats	Number of heartbeat packets sent to the Decoy
Send to decoy logs	Number of log packets sent to the Decoy
Add ip state to decoy	Number of IP address status adding messages sent to the Decoy
Delete ip state to decoy	Number of IP address status deleting messages sent to the Decoy
Update ip state to decoy	Number of IP address status updating messages sent to the Decoy
Send to decoy iplist	Number of IP status packets sent to the Decoy
Send to decoy redirect	Number of packets redirected to the Decoy
Send scan reply to decoy	Number of scan response packets sent to the Decoy
Send channel success pkts	Number of packets successfully sent through the channel
Constructor icmp reply pkts	Number of constructed ICMP replies
Constructor tcp syn pkts	Number of constructed TCP SYN packets
Constructor arp consult pkts	Number of constructed ARP negotiation packets
Constructor arp notify enable pkts	Number of constructed ARP notification enabling packets
Constructor arp notify undo enable pkts	Number of constructed ARP notification disabling packets
Dns answer query pkts for aci	Number of DNS request packets responded using the ACI function
Dns answer respond pkts	Number of DNS reply packets modified using the ACI function
Aci forward syn pkts	Number of SYN packets forwarded using the ACI function
Aci decoy syn pkts	Number of SYN packets discarded or deceived using the ACI function

Item	Description
Send subnet	Number of times that subnet information is sent to the Decoy
Subnet add	Number of subnet information adding messages sent to the Decoy
Subnet del	Number of subnet information deleting messages sent to the Decoy
Dataplane discard statistics information	Statistics on discarded packets
Send RPC msg failed	Number of RPC messages that fail to be sent
Run RPC msg failed	Number of RPC message errors
Send channel failed pkts	Number of packets discarded due to transmission failures on the channel
Arp malloc node failed pkts	Number of packets discarded due to ARP table node application failures
Ip port table malloc node failed pkts	Number of packets discarded due to port table node application failures
Attack weight table malloc node failed pkts	Number of packets discarded due to attack weight table node application failures.
Arp redirect node exhaustion	Number of times when the ARP table node is full.
Get port info failed pkts	Number of packets discarded due to interface information obtaining failures
Hash length limit pkts	Number of packets discarded due to long hash table chains
Send to decoy failed pkts	Number of packets that fail to be sent to the Decoy
Send to decoy failed forward pkts	Number of packets that fail to be forwarded to the Decoy
Send to decoy failed regs	Number of registration packets that fail to be sent to the Decoy
Send to decoy failed heartbeats	Number of heartbeat packets that fail to be sent to the Decoy
Send to decoy failed logs	Number of log packets that fail to be sent to the Decoy
Send to decoy failed iplist	Number of IP status packets that fail to be sent to the Decoy

Item	Description
Send to decoy failed redirect	Number of packets that fail to be redirected to the Decoy
Send to attacker failed pkts	Number of packets that fail to be sent to the attacker
Smbuf malloc failed	Number of packets discarded due to Smbuf application failures
ARP header illegal packets discarded	Number of packets discarded due to invalid ARP headers
IP header illegal packets discarded	Number of packets discarded due to invalid IP headers
IP frag packets discarded	Number of discarded IP fragments
TCP header illegal packets discarded	Number of packets discarded due to invalid TCP headers
VPN header illegal packets discarded	Number of packets discarded due to invalid VPN headers
Arp extend type illegal packets discarded	Statistics of packets discarded due to invalid ARP extended types
Log cache num limit not merge	Number of logs that are not merged when the number of cached logs reaches the upper limit
Log cache num limit not send	Number of logs that are not sent when the number of cached logs reaches the upper limit
Aci node exhaustion	Number of ACI entry creation failures due to insufficient ACI cache resources
Aci source ip limit add fail	Number of ACI entry creation failures due to the limit on the number of source addresses that can be cached
Dns node exhaustion	Number of DNS entry creation failures due to insufficient DNS cache resources
Send subnet fai	Number of times that subnet information fails to be sent.
Smbuf pool exhaustion	Number of Smbuf resource application failures due to Smbuf resource exhaustion
Smbuf pool head null	Number of Smbuf resource application failures due to an empty Smbuf resource head
Smbuf pool bad safemask	Number of Smbuf resource application failures due to an incorrect header verification value of the Smbuf resource

Item	Description
Smbuf pool bad free flag	Number of Smbuf resource application failures due to an incorrect release verification value of the Smbuf resource
Dataplane error statistics information	Error statistics

14.22.35 display deception syn-connect

Function

The **display deception syn-connect** command displays the TCP port scanning behavior detected by the switch.

Format

display deception syn-connect [**source-ip** *ip-address*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Specifies the source IP address that initiates TCP port scanning.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the TCP port scanning behavior detected by the switch, so that you can configure a more accurate TCP port scanning threshold using the **deception syn-connect rate** command. If a TCP port is scanned at a lower frequency than the threshold specified by the **deception syn-connect rate** command but have been scanned for many times, the scanning behavior may be an attack.

Example

Display the TCP port scanning behavior detected by the switch.

```
<HUAWEI> display deception syn-connect
----------------------------------------------------------------------------------------------------
```

```
Current total number = 0

----------------------------------------------------------------------------------------------------
source           rate(num/s)number    vlan   vpn-instance
----------------------------------------------------------------------------------------------------
```

Table 14-147 Description of the **display deception syn-connect** command output

Item	Description
Current total number	Number of entries.
source	Source IP address that initiates TCP port scanning.
rate(num/s)	TCP port scanning frequency, in **"times per second"**.
number	Number of TCP port scanning times.
vlan	VLAN to which the source IP address belongs.
vpn-instance	VPN instance of the source IP address.

14.22.36 display deception version

Function

The **display deception version** command displays the DecoySensor version.

Format

display deception version

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The DecoySensor and Decoy need to be used together, and they can communicate with each only when their versions are the same.

Example

Display the DecoySensor version.

```
<HUAWEI> display deception version
Version 1.1.0
```

Table 14-148 Description of the **display deception version** command output

Item	Description
Version	DecoySensor version.

14.22.37 display deception whitelist

Function

The **display deception whitelist** command displays the deception whitelist.

Format

display deception whitelist [**id** *id-number*]

Parameters

Parameter	Description	Value
id *id-number*	Specifies a whitelist ID.	The value is an integer in the range from 1 to 50.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a deception whitelist using the **deception whitelist** command, you can run the **display deception whitelist** command to check whether the deception whitelist is correctly configured.

Example

Display deception whitelists.

```
<HUAWEI> display deception whitelist
--------------------------------------------------------------------------------
Current total number = 1

--------------------------------------------------------------------------------
Whitelist ID 1 information:
--------------------------------------------------------------------------------
source/mask              :192.168.10.10/255.255.255.255
```

```
destination/mask         :any
vpn-instance             :
```

Table 14-149 Description of the **display deception whitelist** command output

Item	Description
Current total number	Number of entries.
Whitelist ID *i* information	Information about the whitelist whose ID is *i*.
source/mask	Source IP address and subnet mask.
destination/mask	Destination IP address and subnet mask.
vpn-instance	VPN instance of the IP address.

14.22.38 reset deception aci

Function

The **reset deception aci** command updates ACI entries.

Format

reset deception aci

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After the ACI suffix is changed, you need to update the ACI entries. Otherwise, the old ACI suffix becomes invalid only after the ACI entries age.

After the ACI entries are updated, the access initiated by a terminal is deceived when the DNS record of the terminal does not age. Therefore, change the ACI suffix when no service traffic exists.

Example

Update ACI entries.

```
<HUAWEI> reset deception aci
  Warning:Reseting aci table will affect the normal service. Continue? [Y/N]:y
```

14.22.39 reset deception arp-proxy

Function

The **reset deception arp-proxy** command clears the interface IP address of the switch and the target IP addresses in the proxy ARP requests sent to the switch in the online IP address table.

Format

reset deception arp-proxy

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

None

Example

Clear the interface IP address of the switch and the target IP addresses in the proxy ARP requests sent to the switch in the online IP address table.

```
<HUAWEI> reset deception arp-proxy
```

14.22.40 reset deception ip-state

Function

The **reset deception ip-state** command updates the online status of IP addresses on the network where the switch is located.

Format

reset deception ip-state

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset deception ip-state** command clears the IP address online status and immediately initiates the check on the online status of IP addresses. There are two exceptions:

- If traffic destined for address A is deceived, the online status of address A is not cleared.
- The online status of IP addresses learned through proxy ARP is not cleared.

Example

Update the online status of IP addresses on the network where the switch is located.

```
<HUAWEI> reset deception ip-state
```

14.22.41 reset deception port-redirect

Function

The **reset deception port-redirect** command clears information about deceived traffic that scanned unopened TCP ports and stops port deception.

Format

reset deception port-redirect [**source-ip** *ip-address*] [**destination-ip** *ip-address*] [**destination-port** *port*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Specifies the source IP address of the deceived traffic.	The value is in dotted decimal notation.
destination-ip *ip-address*	Specifies the destination IP address of the deceived traffic.	The value is in dotted decimal notation.
destination-port *port*	Specifies the destination TCP port of the deceived traffic.	The value is an integer in the range from 1 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

If it is found that deceived traffic is normal service traffic based on the **display deception port-redirect** command, run the **reset deception port-redirect** command to delete the corresponding entry from the deception flow table to release the traffic.

Example

Clear information about deceived traffic that scanned unopened TCP ports and stop port deception.

```
<HUAWEI> reset deception port-redirect
```

14.22.42 reset deception port-state

Function

The **reset deception port-state** command updates the port openness status of a service host.

Format

reset deception port-state

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The DecoySensor records the port openness status based on the SYN-ACK packet returned by the service host and saves the record for 24 hours, until the record ages naturally or updated when a new SYN-ACK packet is generated. During this period, even if the DecoySensor receives the RST-ACK packet from the corresponding port, it does not deceive the traffic.

If the service openness status of the service host is updated, update the record in a timely manner.

Examples

Update the port openness status of a service host.

```
<HUAWEI> reset deception port-state
```

14.22.43 reset deception statistics

Function

The **reset deception statistics** command clears deception statistics.

Format

reset deception statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

To clear deception statistics, run the **reset deception statistics** command. Then, run the **display deception statistics** command to view deception statistics in this period.

Example

Clear deception statistics.

```
<HUAWEI> reset deception statistics
```

14.23 Terminal Anti-Spoofing Configuration Commands

14.23.1 Command Support

Only the following models support terminal anti-spoofing:

S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

14.23.2 display terminal configuration

Function

The **display terminal configuration** command displays the manually entered terminal information.

Format

display terminal configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **terminal** command to manually enter terminal information, you can run the **display terminal configuration** command to check the manually entered terminal information.

Example

Display the manually entered terminal information.

```
<HUAWEI> display terminal configuration
-------------------------------------------------------------------------------------------
MAC Address     IP Address      Mask            Interface               Category
-------------------------------------------------------------------------------------------
00e0-fc11-1111  10.10.1.1       -               -                       printer
00e0-fc11-1112  10.10.1.2       255.255.255.0   -                       printer
-------------------------------------------------------------------------------------------
Total items displayed = 2
```

Table 14-150 Description of the **display terminal configuration** command output

Item	Description
MAC Address	MAC address of a terminal.
IP Address	IP address of a terminal.
Mask	Subnet mask of a terminal's IP address.
Interface	Access interface of a terminal.

Item	Description
Category	Type of a terminal.
Total items displayed	Total number of entries.

14.23.3 display terminal information

Function

The **display terminal information** command displays terminal entries.

Format

display terminal information { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays entry information about all terminals.	-
mac-address *mac-address*	Displays entry information about the terminal with a specified MAC address.	The value must be an existing terminal MAC address in the terminal table. The value is in H-H-H format. An H is a 4-digit hexadecimal number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view terminal entries, including the MAC address, type, access interface, anomaly detection result, isolation status, and aging time of the terminal.

The device generates an entry for a terminal only when the terminal information manually entered using the **terminal** command matches the ARP packets sent by the terminal. Then you can run this command to view the terminal entry.

Example

Display entries of all terminals.

```
<HUAWEI> display terminal information all
Status: N - Normal,     F - Flow abnormal      U - Unknown
        IP - Ip abnormal, INT - Interface abnormal
        INTIP - Interface and ip abnormal
-------------------------------------------------------------------------------------------
MAC Address    Category  Ip Address     Interface           Status Isolation Inspect  Expire(minute)
-------------------------------------------------------------------------------------------
00e0-fc11-1111 Printer   10.1.10.1     GigabitEthernet0/0/1     N     No      Enable          30
00e0-fc22-2222 Ip-camera  10.1.20.1     GigabitEthernet0/0/2     N     No      Enable          24
-------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 14-151 Description of the **display terminal information** command output

Item	Description
MAC Address	MAC address of a terminal.
Category	Terminal type. The options are as follows: ● Printer: printer ● Ip-camera: IP camera ● Voip-phone: IP phone
Ip Address	IP address of a terminal.
Interface	Access interface of a terminal.
Status	Anomaly detection result of a terminal. The options are as follows: ● N: The terminal is normal. ● F: The traffic of the terminal is abnormal. ● U: No detection result is obtained after the terminal is de-isolated. ● IP: The IP address of the terminal is abnormal. ● INT: The access interface of the terminal is abnormal. ● INTIP: Both the access interface and IP address of the terminal are abnormal.
Isolation	Isolation status of a terminal. The options are as follows: ● Yes: The terminal is isolated. ● No: The terminal is not isolated.
Inspect	Whether terminal anomaly detection is enabled. The options are as follows: ● Enable: The function is enabled. ● Disable: The function is disabled.

Item	Description
Expire(minute)	● When the value of **Isolation** is **Yes**, this field indicates the remaining time of the isolation action, in minutes. When the remaining time is 0, the entry is deleted. ● When the value of Isolation is **No**, this field indicates the remaining time before a terminal entry is aged, in minutes. When the remaining time is 0, the entry is deleted.

14.23.4 display terminal-inspect abnormal-reason

Function

The **display terminal-inspect abnormal-reason** command displays the terminal anomaly cause.

Format

display terminal-inspect abnormal-reason { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays the anomaly causes of all terminals.	-
mac-address *mac-address*	Displays the anomaly cause of the terminal with a specified MAC address.	The value is in H-H-H format. An H is a 4-digit hexadecimal number. The value must be an existing terminal MAC address in the terminal table.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the anomaly cause of a terminal.

Prerequisites

The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.

Example

Display the anomaly causes of all terminals.

```
<HUAWEI> display terminal-inspect abnormal-reason all
---------------------------------
MAC            AbnormalReason
---------------------------------
00e0-fc11-1111 stream-model
00e0-fc11-1112 stream-model
---------------------------------
Total: 2, printed: 2
```

Table 14-152 Description of the **display terminal-inspect abnormal-reason** command output

Item	Description
MAC	MAC address of a terminal.
Abnormal-reason	Anomaly cause. ● stream-model: The actual traffic behavior of the terminal does not comply with the traffic behavior model of the terminal type.
Total	Total number of entries.
printed	Number of displayed entries.

14.23.5 display terminal-inspect cache-data

Function

The **display terminal-inspect cache-data** command displays terminal traffic data cached on the device.

Format

display terminal-inspect cache-data [**mac-address** *mac-address*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of a terminal.	The value must be the MAC address of an existing terminal. The value is in H-H-H format. An H is a 4-digit hexadecimal number.

Views

All view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the **terminal-inspect cache-data** command is run to enable the traffic data caching function for a terminal, you can run the **display terminal-inspect cache-data** command to view the traffic data of the terminal.

Prerequisites

1. The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.
2. The **terminal-inspect cache-data** command has been run in the system view to enable the traffic data caching function for a terminal.

Precautions

A maximum of 128 terminal traffic data records can be displayed on the device, and the latest 128 records are saved in time sequence.

Example

Display terminal traffic data cached on the device.

```
<HUAWEI> display terminal-inspect cache-data
MAC: 00e0-fc11-1111
-------------------------------------------------------------------------------------
TimeStamp SrcMac         DstMac         SrcPort DstPort Protocol       Byte Packet
-------------------------------------------------------------------------------------
     8743 00e0-fc11-1111 00e0-fc22-2222       0    1000       17      34688    271
-------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 14-153 Description of the **display terminal-inspect cache-data** command output

Item	Description
MAC	MAC address of a terminal.
TimeStamp	Time stamp of the first packet.
SrcMac	Source MAC address of packets.
DstMac	Destination MAC address of packets.
SrcPort	Source port number of packets.
DstPort	Destination port number of packets.
Protocol	5-tuple protocol identifier of traffic.
Byte	Total number of bytes.
Packet	Total number of packets.
Total	Total number of entries.
printed	Number of printed entries.

14.23.6 display terminal-inspect category

Function

The **display terminal-inspect category** command displays the types of terminals for which terminal anomaly detection is enabled.

Format

display terminal-inspect category

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the terminal anomaly detection function is enabled, you can run this command to view the terminal types.

Prerequisites

The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.

Example

Display the types of terminals for which terminal anomaly detection is enabled.

```
<HUAWEI> display terminal-inspect category
--------------------
Id Category
--------------------
 1 ip-camera
 2 voip-phone
--------------------
Total: 2
```

Table 14-154 Description of the **display terminal-inspect category** command output

Item	Description
Id	Terminal ID.
Category	Terminal type.
Total	Total number of terminal types.

14.23.7 display terminal-inspect result

Function

The **display terminal-inspect result** command displays the terminal anomaly detection result.

Format

display terminal-inspect result { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays anomaly detection results of all terminals.	-

Parameter	Description	Value
mac-address *mac-address*	Displays the anomaly detection result of the terminal with a specified MAC address.	The value must be an existing terminal MAC address in the terminal table. The value is in H-H-H format. An H is a 4-digit hexadecimal number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the comprehensive anomaly detection result of the traffic behavior model of a terminal, including the update time of the detection result, MAC address of the terminal, and detection result.

Example

Display the anomaly detection results of all terminals.

```
<HUAWEI> display terminal-inspect result all
--------------------------------------------
Mac-address    Time                Result
--------------------------------------------
00e0-fc11-1111 2021-04-29 13:10:07  abnormal
00e0-fc22-2222 2021-04-29 13:10:07  abnormal
--------------------------------------------
Total: 2, printed: 2
```

Table 14-155 Description of the **display terminal-inspect result** command output

Item	Description
Time	Time when the detection result is updated.
Mac-address	MAC address of a terminal.
Result	Anomaly detection result. The options are as follows: ● inspecting: Detection is in progress and no detection result is available. ● normal: The terminal is normal. ● abnormal: The terminal is abnormal. **NOTE** If a terminal has detection results, the result of the last detection is displayed when you perform the detection again.

Item	Description
Total	Total number of entries.

14.23.8 display terminal-inspect supervised abnormal-reason

Function

The **display terminal-inspect supervised abnormal-reason** command displays the anomaly degree of terminal detection indicators.

Format

display terminal-inspect supervised abnormal-reason { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Specifies all terminals.	-
mac-address *mac-address*	Specifies the MAC address of a terminal.	The value is in H-H-H format. An H is a 4-digit hexadecimal number. The value must be an existing terminal MAC address in the terminal table.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate terminal anomaly problems, you can run this command to check the anomaly degree of terminal detection indicators for further analysis. Exercise caution when running the **display terminal-inspect supervised abnormal-reason all** command. Excessive information output affects system performance.

Example

Display the anomaly degree of detection indicators for the terminal whose MAC address is 00e0-fc11-1111.

```
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose] display terminal-inspect supervised abnormal-reason mac-address 00e0-fc11-1111
UpstreamTrafficRate: upstream traffic rate of a terminal
DownstreamTrafficRate: downstream traffic rate of a terminal
TotalTrafficRate: total traffic rate of a terminal
DestinationPort: destination port number in packets sent by a terminal
Ratio: ratio of the upstream traffic rate to the downstream traffic rate of a terminal
-------------------------------------------------------------------------------------------------------------------------
MAC              UpstreamTrafficRate     DownstreamTrafficRate      TotalTrafficRate      DestinationPort
Ratio
00e0-fc11-1111                 82%                      1%                   4%                  4%       9%
-------------------------------------------------------------------------------------------------------------------------
Total: 1, printed: 1
```

Table 14-156 Description of the **display terminal-inspect supervised abnormal-reason** command output

Item	Description
MAC	MAC address of a terminal.
UpstreamTrafficRate	Upstream traffic rate of a terminal.
DownstreamTrafficRate	Downstream traffic rate of a terminal.
TotalTrafficRate	Total traffic rate of a terminal.
DestinationPort	Number of the destination port to which packets are sent.
Ratio	Anomaly degree of the ratio of the upstream traffic rate to the downstream traffic rate for a terminal.
Total	Total number of MAC addresses.
printed	Number of printed entries.

14.23.9 display terminal-inspect terminal-list

Function

The **display terminal-inspect terminal-list** command displays the list of terminals under anomaly detection.

Format

display terminal-inspect [**category** *category-name*] **terminal-list**

Parameters

Parameter	Description	Value
category *category-name*	Specifies a terminal type.	The value is of the enumerated type: • ip-camera: IP camera • printer: printer • Voip-phone: IP phone

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the terminals that are enabled with anomaly detection and are not isolated.

Prerequisites

The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.

Example

Display the list of all terminals under anomaly detection.

```
<HUAWEI> display terminal-inspect terminal-list
------------------------------
MAC            Category
------------------------------
00e0-fc11-1111 ip-camera
00e0-fc22-2222 voip-phone
------------------------------
Total: 2, printed: 2
```

Table 14-157 Description of the **display terminal-inspect terminal-list** command output

Item	Description
MAC	MAC address of a terminal.
Category	Terminal type. The options are as follows: • printer: printer • ip-camera: IP camera • Voip-phone: IP phone

Item	Description
Total	Total number of entries.
printed	Number of displayed entries.

14.23.10 display terminal-isolate configuration

Function

The **display terminal-isolate configuration** command displays the configuration of a terminal isolation policy.

Format

display terminal-isolate { **apply** | **exclude** } **configuration**

Parameters

Parameter	Description	Value
apply	Displays the terminal isolation policy applied to the device.	-
exclude	Displays the whitelist configured in a terminal isolation policy. The device does not apply the isolation policy to whitelisted terminals.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a terminal isolation policy is configured, you can run this command to view the configuration of the terminal isolation policy.

Example

Display the terminal isolation policy applied to the device.

```
<HUAWEI> display terminal-isolate apply configuration
------------------------------------------------------------------------------------------
Category       MAC Address    Block         Period(minutes) Template Name
------------------------------------------------------------------------------------------
printer        00e0-fc11-1111 YES           35              test1
printer        00e0-fc22-2222 NO             20              test2
```

```
--------------------------------------------------------------------------------------------
Total items = 2
```

Display the whitelist configured in a terminal isolation policy.

```
<HUAWEI> display terminal-isolate exclude configuration
------------------------------
Category       MAC Address
------------------------------
printer        00e0-fc33-3333
------------------------------
Total items = 1
```

Table 14-158 Description of the **display terminal-isolate configuration** command output

Item	Description
Category	Terminal type.
MAC Address	MAC address of a terminal. If the MAC address of a terminal is not specified when you configure the terminal isolation policy, **NA** is displayed.
Block	Whether the isolation action of the terminal is block.
Period(minutes)	Aging time of the configured isolation action, in minutes. This parameter is configured using the **terminal-isolate period** command.
Template Name	Name of an isolation template.
Total items	Total number of entries.

14.23.11 reset terminal-inspect cache-data

Function

The **reset terminal-inspect cache-data** command clears the terminal traffic data cached on the device.

Format

reset terminal-inspect cache-data

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the latest terminal traffic data, run the **reset terminal-inspect cache-data** command to clear the cached terminal traffic data. After a period of time, run the **display terminal-inspect cache-data** command to view the cached terminal traffic data.

Prerequisites

1. The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.
2. The **terminal-inspect cache-data** command has been run in the system view to enable the traffic data caching function for a terminal.

Example

Clear the terminal traffic data cached on the device.

```
<HUAWEI> reset terminal-inspect cache-data
```

14.23.12 terminal

Function

The **terminal** command allows you to manually enter terminal information.

The **undo terminal** command deletes the manually entered terminal information.

By default, no terminal information is manually entered on the device.

Format

terminal { **mac-address** *mac-address* [**ip-address** *ip-address* | **interface** *interface-type interface-number*] | **ip-address** *ip-address* { *mask* | *mask-length* } | **interface** { *interface-type interface-number* &<1-8> | *interface-type interface-number1* **to** *interface-number2* } } **category** { **printer** | **voip-phone** | **ip-camera** }

undo terminal { **mac-address** *mac-address* | **ip-address** *ip-address* { *mask* | *mask-length* } | **interface** { *interface-type interface-number* &<1-8> | *interface-type interface-number* **to** *interface-number* } }

undo terminal { **mac-address** | **ip-address** | **interface** } **all**

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of a terminal.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter less than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
ip-address *ip-address*	Specifies the IP address of a terminal.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of an IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IP address.	The value is an integer ranging from 0 to 32, but the mask length of an IP address cannot be set to 0.
interface	Specifies the access interface of a terminal.	-
interface-type interface-number	Specifies the type and number of an interface.	The interface type cannot be set to Eth-Trunk.
interface-type interface-number1 **to** *interface-number2*	Specifies the type and number of an interface. *interface-number1* and *interface-number2* specify an interface range. *interface-number1* specifies the number of the first interface, and *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than that of *interface-number1*.	The interface type cannot be set to Eth-Trunk. In a stack, *interface-number1* and *interface-number2* cannot reside on different devices. That is, the slot IDs of the interfaces corresponding to *interface-number1* and *interface-number2* must be the same.

Parameter	Description	Value
category	Specifies a terminal type.	-
printer	Sets the terminal type to printer.	-
voip-phone	Sets the terminal type to IP phone.	-
ip-camera	Sets the terminal type to IP camera.	-
mac-address	Deletes all terminal MAC addresses.	-
ip-address	Deletes all terminal IP addresses.	-
interface	Deletes all terminal access interfaces.	-
all	Deletes all the manually entered terminal information.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to manually enter the MAC address, IP address, type, and access interface of a terminal.

Precautions

If different terminals have the same MAC address, their information cannot be recorded.

The device generates an entry for a terminal only when the terminal information manually entered using the **terminal** command matches the ARP packets sent by the terminal and terminal anomaly detection has been enabled globally using the **terminal-inspect flow enable** command. Then you can run the **display terminal information** command to view the terminal entry information.

You can run this command to manually enter the access interface information of a terminal only when the device is directly connected to the terminal. Otherwise, the terminal may be incorrectly identified.

Example

Manually enter the following terminal information: The terminal MAC address is 00e0-fc11-1111, the IP address is 10.1.1.1, and the terminal type is printer.

```
<HUAWEI> system-view
[HUAWEI] terminal mac-address 00e0-fc11-1111 ip-address 10.1.1.1 category printer
```

Delete all the manually entered terminal information.

```
<HUAWEI> system-view
[HUAWEI] undo terminal all
```

14.23.13 terminal-inspect cache-data

Function

The **terminal-inspect cache-data** command enables the traffic data caching function for a terminal.

The **undo terminal-inspect cache-data** command disables the traffic data caching function for a terminal.

By default, the traffic data caching function is disabled for a terminal.

Format

terminal-inspect cache-data mac-address *mac-address* [**max-num** *max-num*]

undo terminal-inspect cache-data mac-address *mac-address* [**max-num** *max-num*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of a terminal.	The value must be the MAC address of an existing terminal. The value is in H-H-H format. An H is a 4-digit hexadecimal number.
max-num *max-num*	Specifies the maximum number of traffic data entries that can be cached. If this parameter is not specified, a maximum of 128 entries can be cached.	The value is an integer ranging from 1 to 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the algorithm used for terminal anomaly detection is incorrect, engineers need to analyze the original traffic data to locate the problem. To view the traffic data of a terminal, run the **terminal-inspect cache-data** command to enable the traffic data caching function for the terminal. If you want to delete the cached traffic data of a terminal and disable the device from caching the traffic data of the terminal, run the **undo terminal-inspect cache-data** command to disable the traffic data caching function for the terminal.

Prerequisites

The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.

Follow-up Procedure

Run the **display terminal-inspect cache-data** command to view the terminal traffic data.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Enable the traffic data caching function for the terminal whose MAC address is 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] terminal-inspect cache-data mac-address 00e0-fc12-3456
```

14.23.14 terminal-inspect category

Function

The **terminal-inspect category** command enables terminal anomaly detection for a specified type of terminal.

The **undo terminal-inspect category** command disables terminal anomaly detection for a specified type of terminal.

By default, anomaly detection is not directed at a specific type of terminal.

Format

terminal-inspect category { **printer** | **voip-phone** | **ip-camera** } [[**exclude**] **mac-address** *mac-address*]

undo terminal-inspect category { **printer** | **voip-phone** | **ip-camera** } [[**exclude**] **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
printer	Sets the terminal type to printer.	-
voip-phone	Sets the terminal type to IP phone.	-
ip-camera	Sets the terminal type to IP camera.	-
exclude	Whitelist a terminal, for which terminal anomaly detection is not performed.	-
mac-address *mac-address*	Specifies the MAC address of a terminal.	The value must be an existing terminal MAC address in the terminal table. The value is in H-H-H format. An H is a 4-digit hexadecimal number.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **terminal-inspect category** command to enable terminal anomaly detection for a specified type of terminal. After this command is configured, the device compares the traffic behavior model with the actual traffic behavior of the terminal to determine whether the traffic behavior of the terminal is abnormal.

The following uses printers as an example to describe how to use the **terminal-inspect category** command:

- Run the **terminal-inspect category printer** command to enable terminal anomaly detection for all printers.
- Run the **terminal-inspect category printer mac-address** *mac-address* command to enable terminal anomaly detection for the printer with a specified MAC address.
- After you run the **terminal-inspect category printer** command to enable terminal anomaly detection for all printers, run the **terminal-inspect category printer exclude mac-address** *mac-address* command to disable terminal anomaly detection for the printer with a specified MAC address.

Precautions

- The **terminal-inspect category** command takes effect only when the following conditions are met:
    a. The **terminal-inspect flow enable** command has been run in the system view to enable terminal anomaly detection globally.
    b. A terminal entry is generated on the device for the terminal to be detected. The device generates the corresponding terminal entry only when terminal anomaly detection is enabled globally and the terminal information manually entered using the **terminal** command matches the ARP packets sent by the terminal. You can run the **display terminal information** command to view the terminal entry information.
- Before running the **terminal-inspect category** { **printer** | **voip-phone** | **ip-camera** } **exclude mac-address** *mac-address* command, ensure that anomaly detection has been enabled for all terminals of the specified type.

  Using printers as an example, before running the **terminal-inspect category printer exclude mac-address** *mac-address* command, you must run the **terminal-inspect category printer** command.
- If anomaly detection has been enabled for all terminals of a certain type, you cannot run the **terminal-inspect category** { **printer** | **voip-phone** | **ip-camera** } **mac-address** *mac-address* command to enable this function for a terminal of this type with a specified MAC address.

  Using printers as an example, after the **terminal-inspect category printer** command is run, the **terminal-inspect category printer mac-address** *mac-address* command is not supported.
- When anomaly detection has been enabled for a terminal of a certain type with a specified MAC address and if you run the **terminal-inspect category** { **printer** | **voip-phone** | **ip-camera** } command to enable anomaly detection for all terminals of this type, the device deletes the configuration of enabling anomaly detection for the terminal of this type with the specified MAC address.

  Using printers as an example, if you run the **terminal-inspect category printer** command after the **terminal-inspect category printer mac-address** *mac-address* command, the device deletes the **terminal-inspect category printer mac-address** *mac-address* command configuration.

Example

Enable terminal anomaly detection for all printers.

```
<HUAWEI> system-view
[HUAWEI] terminal-inspect category printer
```

14.23.15 terminal-inspect flow enable

Function

The **terminal-inspect flow enable** command enables terminal anomaly detection globally.

The **undo terminal-inspect flow** disables terminal anomaly detection.

By default, terminal anomaly detection is disabled globally.

Format

terminal-inspect flow enable

undo terminal-inspect flow

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **terminal-inspect flow enable** command to enable terminal anomaly detection globally.

After terminal anomaly detection is enabled globally, the device sends the ARP packet received from a terminal to the CPU, and checks whether the IP address and access interface of the terminal are abnormal based on the terminal entry. The device generates an entry for a terminal only when the terminal information manually entered by the administrator matches the ARP packet sent by the terminal and the device sends the ARP packet to the CPU.

Precautions

- The **terminal-inspect flow enable** command is mutually exclusive with the following commands:
  - **s-ipfpm measure flow** (enables packet loss and delay measurement)
  - **s-ipfpm measure auto-detect** (enables automatic in-band flow measurement)
  - **ip netstream** (enables IPv4 traffic statistics collection on the inbound and outbound interfaces)
  - **ipv6 netstream** (enables IPv6 traffic statistics collection on the inbound and outbound interfaces)

  - **service-awareness enable** (enables service awareness)
  - **ec-analytics enable** (enables ECA)

Example

Enable terminal anomaly detection globally.

```
<HUAWEI> system-view
[HUAWEI] terminal-inspect flow enable
```

14.23.16 terminal-isolate category

Function

The **terminal-isolate category** command configures a terminal isolation policy for a specified type of terminal.

The **undo terminal-isolate category** command restores the default setting.

The **undo terminal-isolate all** command deletes all isolation policies and whitelists bound to all terminals.

By default, no terminal isolation policy is configured.

Format

terminal-isolate category { **printer** | **voip-phone** | **ip-camera** } { [**mac-address** *mac-address*] **apply template** *template-name* | **exclude mac-address** *mac-address* }

undo terminal-isolate category { **printer** | **voip-phone** | **ip-camera** } { [**mac-address** *mac-address*] **apply template** *template-name* | **exclude mac-address** *mac-address* }

undo terminal-isolate { **apply** | **exclude** } **all**

Parameters

Parameter	Description	Value
printer	Sets the terminal type to printer.	-
voip-phone	Sets the terminal type to IP phone.	-
ip-camera	Sets the terminal type to IP camera.	-

Parameter	Description	Value
mac-address *mac-address*	Specifies the MAC address of a terminal.	The value must be an existing terminal MAC address in the terminal table. The value is in H-H-H format. An H is a 4-digit hexadecimal number.
apply	Applies an isolation template to a terminal. If **apply** is specified but **mac-address** *mac-address* is not specified, the isolation template is applied to all terminals of the specified type.	-
template *template-name*	Specifies the name of an isolation template.	The value must be the name of an existing isolation template. The isolation template name is configured using the **terminal-isolate template** command.
exclude	Whitelists a terminal. The device does not apply the isolation policy to whitelisted terminals.	-
all	Deletes all isolation policies and whitelists bound to terminals.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement the terminal isolation action configured in a terminal isolation template for abnormal terminals of a specified type, run the **terminal-isolate category** { **printer** | **voip-phone** | **ip-camera** } [**mac-address** *mac-address*] **apply template** *template-name* command to apply the configured isolation template to all terminals of this type. Then if a terminal of this type does not need to be isolated, you can run the **terminal-isolate category** { **printer** | **voip-phone** | **ip-camera** } **exclude mac-address** *mac-address* command to add the terminal to the isolation whitelist.

Precautions

Before running the **terminal-isolate category** { **printer** | **voip-phone** | **ip-camera** } [**mac-address** *mac-address*] **apply template** *template-name* command, run the **terminal-isolate template** command to create a terminal isolation template. To make the terminal isolation template take effect, you must run the **terminal-isolate action** command in the terminal isolation template to configure a terminal isolation action.

Example

Apply the isolation template named **test** to all printers. In the isolation template, set the terminal isolation action to **block**.

```
<HUAWEI> system-view
[HUAWEI] terminal-isolate template test
[HUAWEI-terminal-isolate-test] terminal-isolate action block
[HUAWEI-terminal-isolate-test] quit
[HUAWEI] terminal-isolate category printer apply template test
```

Delete all isolation policies bound to terminals.

```
<HUAWEI> system-view
[HUAWEI] undo terminal-isolate apply all
```

14.23.17 terminal-isolate template

Function

The **terminal-isolate template** command creates a terminal isolation template and displays the terminal isolation template view.

The **undo terminal-isolate template** command deletes a terminal isolation template.

By default, no terminal isolation template is created.

Format

terminal-isolate template *template-name*

undo terminal-isolate template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a terminal isolation template.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces, question marks (?), or double quotation marks (").

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a terminal isolation policy, you need to create a terminal isolation template, configure a terminal isolation action and the aging time of the action in the terminal isolation template view, and run the **terminal-isolate category** command to bind the terminal isolation template to a specified type of terminal.

Follow-up Procedure

1. Run the **terminal-isolate action** command in the terminal isolation template view to configure a terminal isolation action.
2. (Optional) Run the **terminal-isolate period** command in the terminal isolation template view to set the aging time of the terminal isolation action.
3. Run the **terminal-isolate category** { **printer** | **voip-phone** | **ip-camera** } [**mac-address** *mac-address*] **apply template** *template-name* command in the system view to apply the terminal isolation template to a specified type of terminal.

Example

Create a terminal isolation template named **test**.

```
<HUAWEI> system-view
[HUAWEI] terminal-isolate template test
```

14.23.18 terminal-isolate action

Function

The **terminal-isolate action** command configures a terminal isolation action.

The **undo terminal-isolate action** command restores the default setting.

By default, no terminal isolation action is configured, meaning that the device does not isolate spoofed terminals.

Format

terminal-isolate action block

undo terminal-isolate action block

Parameters

Parameter	Description	Value
block	Specifies the terminal isolation action to **block**, that is, blocking packets.	-

Views

Terminal isolation template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a terminal isolation policy, you need to run the **terminal-isolate template** command to create a terminal isolation template, configure a terminal isolation action in the terminal isolation template view, and run the **terminal-isolate category** command to bind the terminal isolation template to a specified type of terminal.

When the terminal isolation action is set to block, the device discards packets from spoofed terminals identified by the device.

Follow-up Procedure

Run the **terminal-isolate category** { **printer** | **voip-phone** | **ip-camera** } [**mac-address** *mac-address*] **apply template** *template-name* command in the system view to apply the terminal isolation template to a specified type of terminal.

Example

In the isolation template named **test**, set the terminal isolation action to **block**.

```
<HUAWEI> system-view
[HUAWEI] terminal-isolate template test
[HUAWEI-terminal-isolate-test] terminal-isolate action block
```

14.23.19 terminal-isolate period

Function

The **terminal-isolate period** command sets the aging time of a terminal isolation action.

The **undo terminal-isolate period** command restores the default setting.

By default, the aging time is not configured for a terminal isolation action, meaning that a terminal isolation action does not age.

Format

terminal-isolate period *period-time*

undo terminal-isolate period

Parameters

Parameter	Description	Value
period-time	Specifies the aging time of a terminal isolation action.	The value is an integer ranging from 1 to 1440, in minutes.

Views

Terminal isolation template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a terminal isolation policy, you need to run the **terminal-isolate template** command to create a terminal isolation template, configure a terminal isolation action and the aging time of the action in the terminal isolation template view, and run the **terminal-isolate category** command to bind the terminal isolation template to a specified type of terminal.

By default, the aging time is not configured for a terminal isolation action, meaning that the device always implements the configured terminal isolation action for the identified spoofed terminals. To prevent abnormal terminals from being isolated after recovery, you can run the **terminal-isolate period** command to set the aging time of the terminal isolation action. When the aging time arrives, the device re-identifies whether the terminal is a spoofed terminal and determines whether to implement the configured terminal isolation action.

Prerequisites

The **terminal-isolate action** command has been run in the terminal isolation template view to configure a terminal isolation action.

Follow-up Procedure

Run the **terminal-isolate category** { **printer** | **voip-phone** | **ip-camera** } [**mac-address** *mac-address*] **apply template** *template-name* command in the system view to apply the terminal isolation template to a specified type of terminal.

Example

Configure an isolation template named **test**, set the terminal isolation action to **block**, and set the aging time of the terminal isolation action to 60 minutes. Apply the isolation template named **test** to all printers.

```
<HUAWEI> system-view
[HUAWEI] terminal-isolate template test
[HUAWEI-terminal-isolate-test] terminal-isolate action block
[HUAWEI-terminal-isolate-test] terminal-isolate period 60
[HUAWEI-terminal-isolate-test] quit
[HUAWEI] terminal-isolate category printer apply template test
```

14.24 Terminal Identification Configuration Commands

14.24.1 Command Support

Only the following models support terminal identify:

S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

14.24.2 display terminal identify result

Function

The **display terminal identify result** command displays the terminal identification result.

Format

display terminal identify result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the terminal identification result, including the update time of the identification result, MAC and IP addresses of the terminal, and identification result.

Example

Display the identification result of all terminals.

```
<HUAWEI> display terminal identify result
-------------------------------------------------------------------------------------------
IP            MAC             Category  Vendor    Model              Time
-------------------------------------------------------------------------------------------
1.1.1.1  xxxx-xxxx-xxx1 IP Camera xx1      M2220-In            2023-01-31:19-07-05
1.1.1.2  xxxx-xxxx-xxx2 IP Camera xx2      IPC-HDW1020C        2023-01-31:19-07-10
1.1.1.3  xxxx-xxxx-xxx3 IP Camera xx3      DS-2CD3386FWDV2-IS  2023-01-31:19-01-32
1.1.1.4  xxxx-xxxx-xxx4 IP Camera xx4      TL-IPC435H(P)-S2.8  2023-01-31:19-06-50
-------------------------------------------------------------------------------------------
Total: 4, printed: 4
-------------------------------------------------------------------------------------------
```

Table 14-159 Description of the **display terminal identify result** command output

Item	Description
IP	IP address of a terminal.
MAC	MAC address of a terminal.
Category	Terminal type.
Vendor	Vendor of a terminal.
Model	Terminal model.
Time	Time when the identification result is updated.

14.24.3 terminal-identify enable

Function

The **terminal-identify enable** command enables global terminal identification.

The **undo terminal-identify enable** command disables global terminal identification.

By default, global terminal identification is disabled.

Format

terminal-identify enable

undo terminal-identify enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **terminal-identify enable** command is used to enable global terminal identification. After global terminal identification is enabled, the device sends the ARP packets from the matching terminals to the CPU based on configurations of the **terminal-monitoring source-ip** command and scans the terminals. In addition, the device periodically scans terminals based on the network segment and detection interval configured using the **terminal-scan source-ip** command.

Example

Enable global terminal identification.

```
<HUAWEI> system-view
[HUAWEI] terminal-identify enable
```

14.24.4 terminal-monitoring source-ip

Function

The **terminal-monitoring source-ip** command enables terminal identification triggered when terminals in a specified domain go online.

The **undo terminal-monitoring source-ip** command disables terminal identification triggered when terminals in a specified domain go online.

By default, terminal identification triggered when terminals in a specified domain go online is disabled.

Format

terminal-monitoring source-ip *ip-address* { **vlan** *vlan-id* | **bridge-domain** *bd-id* | **monitor-ip** *ip-address* { *mask* | *mask-length* } } **vendor** { { *vendors* } * | **all** } **category** *ip-camera*

undo terminal-monitoring source-ip *ip-address* { **vlan** *vlan-id* | **bridge-domain** *bd-id* | **monitor-ip** *ip-address* { *mask* | *mask-length* } }

Parameters

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address.	The value must be the IP address of the local host in dotted decimal notation.
vlan *vlan-id*	Indicates the VLAN ID.	The value is an integer that ranges from 1 to 4094.
bridge-domain *bd-id*	Indicates the bridge domain ID.	The value is an integer that ranges from 1 to 16777215.
monitor-ip *ip-address* { *mask* | *mask-length* }	Indicates the IP address range.	• *ip-address*: indicates an IP address, in dotted decimal notation. • *mask*: indicates the mask of an IP address, in dotted decimal notation. • *mask-length*: indicates the mask length, which is an integer that ranges from 0 to 32.
vendor { { *vendors* } ***** **|** *all* **}**	Indicates the device vendor.	The value is a character string.
category *ip-camera*	Indicates the terminal type.	The value is a character string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **terminal-monitoring source-ip** command, you can enable terminal identification triggered when terminals in a specified domain go online. When a terminal goes online, the device identifies the terminal by performing proactive detection based on the configured domain, terminal vendor, and ARP packets sent by the terminal.

Take the cameras of vendor *xx* as an example. The **terminal-monitoring source-ip** command can be used in the following ways:

- Run the **terminal-monitoring source-ip** *ip-address* **vlan** *vlan-id* **vendor** *xx* **category** *ip-camera* command to enable the device (source IP address: **source-ip** *ip-address*) to detect the cameras of vendor *xx* in the specified VLAN (**vlan** *vlan-id*).
- Run the **terminal-monitoring source-ip** *ip-address* **bridge-domain** *bd-id* **vendor** *xx* **category** *ip-camera* command to enable the device (source IP address: **source-ip** *ip-address*) to detect the cameras of vendor *xx* in the specified bridge domain (*bd-id*).
- Run the **terminal-monitoring source-ip** *ip-address* **monitor-ip** *ip-address* { *mask* | *mask-length* } **vendor** *hikvision* **category** *ip-camera* command to enable the device (source IP address: **source-ip** *ip-address*) to detect the cameras of vendor *xx* on the specified IP network segment.

Prerequisites

1. Run the **terminal-identify enable** command in the system view to enable global terminal identification.
2. The specified source IP address, VLAN ID, and bridge domain ID exist on the local host.

Precautions

When you have run this command for multiple times, the latest configuration takes precedence if the source IP address, VLAN ID, and bridge domain ID are the same while different vendors are set.

Example

Enable the device with the source IP address **10.1.1.1** to perform terminal identification triggered when cameras of all vendors in VLAN 20 go online.

```
<HUAWEI> system-view
[HUAWEI] terminal-monitoring source-ip 2.2.2.1 vlan 20 vendor all category ip-camera
```

14.24.5 terminal-scan source-ip

Function

The **terminal-scan source-ip** command enables terminal identification for terminals in a specified domain.

The **undo terminal-scan source-ip** command disables terminal identification for terminals in a specified domain.

By default, terminal identification is disabled for terminals in any domain.

Format

terminal-scan source-ip *ip-address* { **vlan** *vlan-id* | **bridge-domain** *bd-id* } [**scan-ip** *ip-address* { *mask* | *mask-length* }] [**period** *period-time*] **vendor** { { *vendors* } * | **all** } **category** *ip-camera*

undo terminal-scan source-ip *ip-address* { **vlan** *vlan-id* | **bridge-domain** *bd-id* }

Parameters

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address.	The value must be the IP address of the local host in dotted decimal notation.
vlan *vlan-id*	Indicates the VLAN ID.	The value is an integer that ranges from 1 to 4094.
bridge-domain *bd-id*	Indicates the bridge domain ID.	The value is an integer that ranges from 1 to 16777215.
scan-ip *ip-address* { *mask* | *mask-length* }	Indicates the IP address range.	● *ip-address*: indicates an IP address, in dotted decimal notation. ● *mask*: indicates the mask of an IP address, in dotted decimal notation. ● *mask-length*: indicates the mask length, which is an integer that ranges from 0 to 32.
period *period-time*	Indicates the detection interval.	The value is an integer that ranges from 1 to 65535, in minutes. The default value is 30.
vendor { { *vendors* } * | **all** }	Indicates the device vendor.	The value is a character string.
category *ip-camera*	Indicates the terminal type.	The value is a character string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **terminal-scan source-ip** command enables terminal identification for terminals in a specified domain. After this command is executed, the device periodically detects and identifies terminal information based on the configured network segment and terminal vendor.

Take the cameras of vendor *xx* as an example. The **terminal-scan source-ip** command can be used in the following ways:

- Run the **terminal-scan source-ip** *ip-address* **vlan** *vlan-id* **scan-ip** *ip-address mask* **period** *20* **vendor** *xx* **category** *ip-camera* command to enable the device (source IP address: **source-ip** *ip-address*) to detect the cameras of vendor *xx* in the specified VLAN (**vlan** *vlan-id*) at an interval of 20 minutes. Only cameras on the specified network segment (**scan-ip** *ip-address*) are identified.
- Run the **terminal-scan source-ip** *ip-address* **bridge-domain** *bd-id* **scan-ip** *ip-address mask* **period** *30* **vendor** *xx* **category** *ip-camera* command to enable the device (source IP address: **source-ip** *ip-address*) to detect the cameras of vendor *xx* in the specified bridge domain (*bd-id*) at an interval of 30 minutes.

Prerequisites

1. Run the **terminal-identify enable** command in the system view to enable global terminal identification.
2. The specified source IP address, VLAN ID, and bridge domain ID exist on the local host.

Precautions

When you have run this command for multiple times, the latest configuration takes precedence if the source IP address, VLAN ID, and bridge domain ID are the same while different IP address ranges, detection intervals, and vendors are set.

Example

Enable the device with the source IP address **10.1.1.1** to identify cameras of all vendors in VLAN 20 at an interval of 20 minutes.

```
<HUAWEI> system-view
[HUAWEI] terminal-scan source-ip 10.1.1.1 vlan 20 period 20 vendor all category ip-camera
```

14.25 WEAKEA Command Reference

14.25.1 ah authentication-algorithm

Function

The **ah authentication-algorithm** command specifies the authentication algorithm for AH protocol.

NOTE

All models support this command, except S200 and S1730S-S1.

Format

ah authentication-algorithm md5

Parameters

Parameter	Description	Value
md5	Specifies MD5 as the authentication algorithm.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use AH protocol to authenticate packets, preventing packets from being intercepted or modified, you can run the **ah authentication-algorithm** command to configure the authentication algorithm for AH protocol.

Prerequisite

The protocol of this IPSec proposal has been configured to AH using the **transform** command.

Precautions

The authentication algorithms on both IPSec peers must be identical.

Example

Configure the IPSec proposal **prop1** to use the AH protocol, and specify **MD5** as the authentication algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform ah
[HUAWEI-ipsec-proposal-prop1] ah authentication-algorithm md5
```

14.25.2 dh

Function

The **dh** command specifies a DH group used for IKE negotiation.

NOTE

All models support this command, except S200 and S1730S-S1.

Format

dh { **group1** | **group2** | **group5** }

Parameters

Parameter	Description	Value
group1	Uses the 768-bit DH group in IKE negotiation phase 1.	-
group2	Uses the 1024-bit DH group in IKE negotiation phase 1.	-
group5	Uses the 1536-bit DH group in IKE negotiation phase 1.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DH algorithm is a public key algorithm. Two communicating parties calculate a shared key based on data exchanged between them, without transmitting the key. A third party (such as a hacker) cannot calculate the actual key even if it obtains all exchanged data for key calculation.

Precautions

Both ends of an IPSec tunnel must be configured with the same DH group. Otherwise, the negotiation fails.

Example

Specify the **1024-bit DH group** in IKE negotiation phase 1.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] dh group2
```

14.25.3 esp authentication-algorithm

Function

The **esp authentication-algorithm** command configures the authentication algorithm for ESP protocol.

NOTE

All models support this command, except S200 and S1730S-S1.

Format

esp authentication-algorithm md5

Parameters

Parameter	Description	Value
md5	Specifies MD5 as the authentication algorithm.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use ESP protocol to authenticate and encrypt packets, preventing packets from being intercepted or modified, you can run the **esp authentication-algorithm** command to configure the authentication algorithm for ESP protocol.

Prerequisite

The protocol of this IPSec proposal has been configured to ESP using the **transform** command.

Precautions

The authentication algorithms on both IPSec peers must be identical.

The authentication algorithm and encryption algorithm for ESP protocol cannot be both set to **NULL**.

Example

Configure the IPSec proposal **prop1** to use the ESP protocol, and specify **MD5** as the authentication algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform esp
[HUAWEI-ipsec-proposal-prop1] esp authentication-algorithm md5
```

14.25.4 esp encryption-algorithm

Function

The **esp encryption-algorithm** command configures the encryption algorithm for ESP protocol.

NOTE

All models support this command, except S200 and S1730S-S1.

Format

esp encryption-algorithm des

Parameters

Parameter	Description	Value
des	Specifies DES as the encryption algorithm.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use ESP protocol to authenticate and encrypt packets, preventing packets from being intercepted or modified, you can run the **esp encryption-algorithm** command to configure the encryption algorithm for ESP protocol.

Prerequisite

The protocol of this IPSec proposal has been configured to ESP using the **transform** command.

Precautions

The encryption algorithms on both IPSec peers must be identical.

The authentication algorithm and encryption algorithm for ESP protocol cannot be both set to **NULL**.

Example

Configure the IPSec proposal **prop1** to use the AH protocol, and specify **DES** as the encryption algorithm.

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal prop1
[HUAWEI-ipsec-proposal-prop1] transform esp
[HUAWEI-ipsec-proposal-prop1] esp encryption-algorithm des
```

14.25.5 load-module weakea

Function

The **load-module weakea** command loads the WEAKEA plug-in from the system software.

Format

load-module weakea

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before installing the WEAKEA plug-in, run the **load-module weakea** command in the user view to load the WEAKEA plug-in (for example, *xxx***WEAKEA.mod**) from the system software to the plug-in installation directory **$_install_mod**.

Follow-up Procedure

Run the **install-module** *file-name* [**next-startup**] command in the user view to install the plug-in. *file-name* specifies the plug-in file name.

Precautions

If the WEAKEA plug-in exists in the plug-in installation directory **$_install_mod**, delete the original WEAKEA plug-in. Otherwise, this command cannot be executed successfully.

Example

Load the WEAKEA plug-in from the system software.

```
<HUAWEI> load-module weakea
```

14.25.6 pfs

Function

The **pfs** command enables PFS when the local end initiates IPSec tunnel negotiation.

NOTE

All models support this command, except S200 and S1730S-S1.

Format

pfs { **dh-group1** | **dh-group2** | **dh-group5** }

Parameters

Parameter	Description	Value
dh-group1	Uses the 768-bit DH group.	-
dh-group2	Uses the 1024-bit DH group.	-
dh-group5	Uses the 1536-bit DH group.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

When the local end initiates negotiation, there is an additional DH exchange in IKEv1 phase 2 or IKEv2 CREATE_CHILD_SA exchange. The additional DH exchange ensures security of the IPSec SA key and improves communication security.

Example

Enable PFS (using the **1024-bit DH group**) when the local end initiates IPSec tunnel negotiation.

```
<HUAWEI> system-view
[HUAWEI] ipsec efficient-vpn evpn mode client
[HUAWEI-ipsec-efficient-vpn-evpn] pfs dh-group2
```

14.25.7 pki export rsa-key-pair

Function

The **pki export rsa-key-pair** command exports the RSA key pair to the device flash memory and supports the export of the associated certificate.

Format

pki export rsa-key-pair *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* [**3des** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of an RSA key pair on the device.	The value must be an existing RSA key pair name.
and-certificate *certificate-name*	Indicates that the certificate associated to the RSA key pair will be exported.	The value must be an existing certificate file name.
pem *file-name*	Indicates that the RSA key pair will be exported in PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters. Spaces and question marks (?) are not supported. If the file path is included, the value is a string of 1 to 127 characters, for example, **flash:/8ab3/ab3.pem**.
pkcs12 *file-name*	Indicates that the RSA key pair will be exported in PKCS12 format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **des**	Sets the encryption algorithm to DES or 3DES if the RSA key pair is exported in PEM format.	-

Parameter	Description	Value
password *password*	Specifies the encryption password for the RSA key pair file. This password protects the exported RSA key pair file and is required when you import the RSA key pair file.	The value is a string of 8 to 32 case-sensitive characters without question marks (?). For security purposes, a password must meet the minimum strength requirements, that is, the password needs to contain at least three types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before transferring or backing up an RSA key pair, run this command to enable the device to generate the PEM or PKCS12 file carrying this RSA key pair (which may include the certificate) in its flash memory.

Before using this command, run the **display pki rsa local-key-pair** command to view RSA key pair information on the device.

Prerequisites

The RSA key pair has been created and configured to be exportable using the **pki rsa local-key-pair create** command, or it has been imported to the device memory and configured to be exportable using the **pki import rsa-key-pair** command.

Precautions

The RSA key pair is sensitive information. Delete and destroy the exported RSA key pair on the device or storage device immediately after you do not need it.

Example

Export the RSA key pair **key1** to the file **aaa.pem** and set the encryption mode to DES.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create key1 exportable
 Info: The name of the new key-pair will be: key1
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
......+++
...................+++
[HUAWEI] pki export rsa-key-pair key1 pem aaa.pem DES password YsHsjx_202206
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting the RSA key pair in PEM format.
```

14.25.8 set cipher-suite

Function

The **set cipher-suite** command configures cipher suites for a customized SSL cipher suite policy.

Format

set cipher-suite { **tls12_ck_rsa_aes_256_cbc_sha256** | **tls1_ck_dhe_dss_with_aes_128_sha** | **tls1_ck_dhe_dss_with_aes_256_sha** | **tls1_ck_dhe_rsa_with_aes_128_sha** | **tls1_ck_dhe_rsa_with_aes_256_sha** | **tls1_ck_rsa_with_aes_128_sha** | **tls1_ck_rsa_with_aes_256_sha** }

Parameters

Parameter	Description	Value
tls12_ck_rsa_aes_256_cbc_sha256	Configures the TLS12_CK_RSA_AES_256_CBC_SHA256 cipher suite.	-
tls1_ck_dhe_dss_with_aes_128_sha	Configures the TLS1_CK_DHE_DSS_WITH_AES_128_SHA cipher suite.	-
tls1_ck_dhe_dss_with_aes_256_sha	Configures the TLS1_CK_DHE_DSS_WITH_AES_256_SHA cipher suite.	-
tls1_ck_dhe_rsa_with_aes_128_sha	Configures the TLS1_CK_DHE_RSA_WITH_AES_128_SHA cipher suite.	-

Parameter	Description	Value
tls1_ck_dhe_rsa_with_aes_256_sha	Configures the TLS1_CK_DHE_RSA_WITH_AES_256_SHA cipher suite.	-
tls1_ck_rsa_with_aes_128_sha	Configures the TLS1_CK_RSA_WITH_AES_128_SHA cipher suite.	-
tls1_ck_rsa_with_aes_256_sha	Configures the TLS1_CK_RSA_WITH_AES_256_SHA cipher suite.	-

Views

Customized SSL cipher suite policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure cipher suites for a customized SSL cipher suite policy, run the **set cipher-suite** command.

Precautions

If a customized SSL cipher suite policy is being referenced by an SSL policy, the cipher suites in the customized cipher suite policy can be added, modified, or partially deleted. Deleting all of the cipher suites is not allowed.

Example

Configure the **tls12_ck_rsa_aes_256_cbc_sha256** cipher suite for the customized SSL cipher suite policy named **cipher1**.

```
<HUAWEI> system-view
[HUAWEI] ssl cipher-suite-list cipher1
[HUAWEI-ssl-cipher-suite-cipher1] set cipher-suite tls12_ck_rsa_aes_256_cbc_sha256
```

14.25.9 ssh client cipher

Function

The **ssh client cipher** command configures an encryption algorithm list for an SSH client.

The **undo ssh client cipher** command restores the default encryption algorithm list of an SSH client.

By default, an SSH client supports all encryption algorithms.

Format

ssh client cipher { **des_cbc** | **3des_cbc** | **aes128_cbc** | **aes256_cbc** } *

undo ssh client cipher

Parameters

Parameter	Description	Value
des_cbc	Specifies the CBC DES encryption algorithm.	-
3des_cbc	Specifies the CBC 3DES encryption algorithm.	-
aes128_cbc	Specifies the CBC AES128 encryption algorithm.	-
aes256_cbc	Specifies the CBC AES256 encryption algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

An SSH server and a client need to negotiate an encryption algorithm for the packets exchanged between them. You can run the **ssh client cipher** command to configure an encryption algorithm list for the SSH client. After the SSH server receives a packet from the client, the server matches the encryption algorithm list of the client against its local list and selects the first matched encryption algorithm. If no encryption algorithm matches, the negotiation fails.

Example

Configure CBC encryption algorithms for an SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client cipher aes128_cbc aes256_cbc
```

14.25.10 ssh client hmac

Function

The **ssh client hmac** command configures an HMAC algorithm list for an SSH client.

The **undo ssh client hmac** command restores the default HMAC algorithm list of an SSH client.

By default, an SSH client supports all HMAC algorithms.

Format

ssh client hmac { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256_96** } *

undo ssh client hmac

Parameters

Parameter	Description	Value
md5	Specifies the HMAC MD5 algorithm.	-
md5_96	Specifies the HMAC MD5_96 algorithm.	-
sha1	Specifies the HMAC SHA1 algorithm.	-
sha1_96	Specifies the HMAC SHA1_96 algorithm.	-
sha2_256_96	Specifies the HMAC SHA2_256_96 algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

An SSH server and a client need to negotiate an HMAC algorithm for the packets exchanged between them. You can run the **ssh client hmac** command to configure an HMAC algorithm list for the SSH client. After the SSH server receives a packet from the client, the server matches the list of the client against its local list and selects the first matched HMAC algorithm. If no matched HMAC algorithms, the negotiation fails.

Example

Configure the HMAC **sha2_256_96** algorithm for an SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client hmac sha2_256_96
```

14.25.11 ssh client key-exchange

Function

The **ssh client key-exchange** command configures a key exchange algorithm list for an SSH client.

The **undo ssh client key-exchange** command restores the default configuration.

By default, an SSH client supports all key exchange algorithms.

Format

ssh client key-exchange { **dh_group14_sha1** | **dh_group1_sha1** | **dh_group_exchange_sha1** }*

undo ssh client key-exchange

Parameters

Parameter	Description	Value
dh_group14_sha1	Adds the Diffie-hellman-group14-sha1 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group1_sha1	Adds the Diffie-hellman-group1-sha1 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group_exchange_sha1	Adds the Diffie-hellman-group-exchange-sha1 algorithm to the key exchange algorithm list of an SSH client.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The client and server negotiate the key exchange algorithm used for packet transmission. You can run the **ssh client key-exchange** command to configure a key exchange algorithm list for the SSH client. The SSH server compares the configured key exchange algorithm list with the counterpart sent by the client and then selects the first matched key exchange algorithm for packet transmission. If the key exchange algorithm list sent by the client does not match any algorithm in the key exchange algorithm list configured on the server, the negotiation fails.

Example

Configure key exchange algorithm lists **dh_group1_sha1** on the SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client key-exchange dh_group1_sha1
```

14.25.12 ssh server cipher

Function

The **ssh server cipher** command configures an encryption algorithm list for an SSH server.

The **undo ssh server cipher** command restores the default encryption algorithm list of an SSH server.

By default, an SSH server supports all encryption algorithms.

Format

ssh server cipher { **des_cbc** | **3des_cbc** | **aes128_cbc** | **aes256_cbc** } *

undo ssh server cipher

Parameters

Parameter	Description	Value
des_cbc	Specifies the CBC DES encryption algorithm.	-
3des_cbc	Specifies the CBC 3DES encryption algorithm.	-
aes128_cbc	Specifies the CBC AES128 encryption algorithm.	-
aes256_cbc	Specifies the CBC AES256 encryption algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

An SSH server and a client need to negotiate an encryption algorithm for the packets exchanged between them. You can run the **ssh server cipher** command to configure an encryption algorithm list for the SSH server. After the SSH server receives a packet from the client, the server matches the encryption algorithm list of the client against its local list and selects the first matched encryption algorithm. If no matched encryption algorithms, the negotiation fails.

Example

Configure CBC encryption algorithms for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server cipher aes256_cbc aes128_cbc
```

14.25.13 ssh server compatible-ssh1x enable

Function

The **ssh server compatible-ssh1x enable** command enables an SSH server to be compatible with earlier versions.

The **undo ssh server compatible-ssh1x enable** command disables an SSH server from being compatible with earlier versions.

By default, this function is disabled on unconfigured devices. After a device is upgraded, whether an SSH server is allowed to be compatible with earlier versions is determined by the configuration in the configuration file.

Format

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **ssh server compatible-ssh1x enable** command applies to scenarios where a client and a server negotiate with each other on a working version. After a TCP connection is set up between a client and a server, the client negotiates with the server on a version that both the client and server support.

The server compares its own version with that sent by the client and determines whether it can work with the client.

- If the protocol version on the client is earlier than 1.3 or later than 2.0, version negotiation fails and the server disconnects from the client.
- If the protocol version on the client is later than or equal to 1.3 and earlier than 1.99, the SSH1.5 server module is invoked, and the SSH1.X process is performed when the SSH1.X-compatible mode is configured. When the SSH1.X-incompatible mode is configured, version negotiation fails, and the server disconnects from the client.
- If the protocol version on the client is 1.99 or 2.0, the SSH2.0 server module is invoked, and the SSH2.0 process is performed.

Precautions

- If the SSH server is enabled to be compatible with earlier SSH versions, a device prompts a security risk.
- The device can only function as the SSH client of v2.0. When the device functions as the SSH server, it allows SSH clients of v1.x and v2.0 to log in.
- The configuration takes effect upon the next login.
- SSH2.0 has an extended structure and supports more authentication modes and key exchange methods than SSH1.X. SSH 2.0 can eliminate the security risks that SSH 1.X has. SSH 2.0 is more secure and therefore is recommended.
- If a device has empty configuration, the device delivers the **undo ssh server compatible-ssh1x enable** command to disable the SSH server's compatibility with earlier versions. If a device is upgraded, the SSH server's compatibility with earlier versions is the same as that in the configuration file.

NOTE

Currently, protocols support SSH versions as follows:

- STelnet: The device supports SSH v1.99. That is SSH1 (SSH1.x) and SSH2 (SSH2.0) are supported. By default, SSH2 (SSH2.0) is supported.
- SFTP: Only SSH2 (SSH2.0) is supported.
- SCP: Only SSH2 (SSH2.0) is supported.

Example

Enable an SSH server to be compatible with earlier versions.

```
<HUAWEI> system-view
[HUAWEI] ssh server compatible-ssh1x enable
Warning: SSHv1 is not a secure protocol, and it is recommended to use SSHv2.
```

14.25.14 sshd server

Function

The **sshd server** command configures the algorithms that can be used by a switch to establish a NETCONF session with a third-party controller.

The **undo sshd server** command deletes the algorithms that can be used by a switch to establish a NETCONF session with a third-party controller.

The algorithms that can be configured by this command have low security. By default, the switch does not support these algorithms when establishing a NETCONF session with a third-party controller.

NOTE

All models support this command, except S1720GW-E, S1720GWR-E, S200, and S1730S-S1.

Format

sshd server cipher { **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **aes128-gcm@openssh.com | aes256-gcm@opensscom** } *

sshd server hmac { **hmac-md5** | **hmac-md5-etm@openssh.com** | **hmac-sha1** | **hmac-sha1-etm@openssh.com** } *

sshd server hostkey *hostkey*

sshd server key-exchange { **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** | **diffie-hellman-group1-sha1** | **diffie-hellman-group14-sha1** | **diffie-hellman-group-exchange-sha1** } *

sshd server hostkey-algorithms ssh-rsa

undo sshd server { **cipher** | **hmac** | **hostkey** | **key-exchange** | **hostkey-algorithms** }

Parameters

Parameter	Description	Value
cipher	Specifies an encryption algorithm.	-
aes128-cbc	Specifies the **aes128-cbc** algorithm.	-
aes192-cbc	Specifies the **aes192-cbc** algorithm.	-
aes256-cbc	Specifies the **aes256-cbc** algorithm.	-
aes128-gcm@openssh.com	Specifies the **aes128-gcm@openssh.com** algorithm.	-
aes256-gcm@openssh.com	Specifies the **aes256-gcm@openssh.com** algorithm.	-
hmac	Specifies an authentication algorithm.	-
hmac-md5	Specifies the **hmac-md5** algorithm.	-

Parameter	Description	Value
hmac-md5-etm@openssh.com	Specifies the **hmac-md5-etm@openssh.com** algorithm.	-
hmac-sha1	Specifies the **hmac-sha1** algorithm.	-
hmac-sha1-etm@openssh.com	Specifies the **hmac-sha1-etm@openssh.com** algorithm.	-
hostkey *hostkey*	Specifies a key file.	The key file must exist on the device.
key-exchange	Specifies a key exchange algorithm.	-
ecdh-sha2-nistp256	Specifies the **ecdh-sha2-nistp256** algorithm.	-
ecdh-sha2-nistp384	Specifies the **ecdh-sha2-nistp384** algorithm.	-
diffie-hellman-group1-sha1	Specifies the **diffie-hellman-group1-sha1** algorithm.	-
diffie-hellman-group14-sha1	Specifies the **diffie-hellman-group14-sha1** algorithm.	-
diffie-hellman-group-exchange-sha1	Specifies the **diffie-hellman-group-exchange-sha1** algorithm.	-
hostkey-algorithms	Specifies a key algorithm.	-
ssh-rsa	Specifies the **ssh-rsa** algorithm.	-

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

The algorithms that can be configured by this command have low security. By default, the switch does not support these algorithms when establishing a

NETCONF session with a third-party controller. You are advised not to use these algorithms.

Example

Configure the **aes128-cbc** encryption algorithm that can be used by the switch to establish a NETCONF session with a third-party controller.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] sshd server cipher aes128-cbc
Warning: Insecure encryption algorithms will be enabling and the SSH connection may be teared down. Continue? [Y/N]:y
```

14.25.15 ssh server hmac

Function

The **ssh server hmac** command configures an HMAC algorithm list for an SSH server.

The **undo ssh server hmac** command restores the default HMAC algorithm list of an SSH server.

By default, an SSH server supports all HMAC algorithms.

Format

ssh server hmac { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256_96** } *

undo ssh server hmac

Parameters

Parameter	Description	Value
md5	Specifies the HMAC MD5 algorithm.	-
md5_96	Specifies the HMAC MD5_96 algorithm.	-
sha1	Specifies the HMAC SHA1 algorithm.	-
sha1_96	Specifies the HMAC SHA1_96 algorithm.	-
sha2_256_96	Specifies the HMAC SHA2_256_96 algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

An SSH server and a client need to negotiate an HMAC algorithm for the packets exchanged between them. You can run the **ssh server hmac** command to configure an HMAC algorithm list for the SSH server. After the server receives a packet from the client, the server matches the list of the client against its local list and selects the first matched HMAC algorithm. If no matched HMAC algorithms, the negotiation fails.

Example

Configure the HMAC **sha2_256_96** algorithm for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server hmac sha2_256_96
```

14.25.16 ssh server key-exchange

Function

The **ssh server key-exchange** command configures a key exchange algorithm list on an SSH server.

The **undo ssh server key-exchange** command restores the default configuration.

By default, an SSH server supports all key exchange algorithms.

Format

ssh server key-exchange { **dh_group14_sha1** | **dh_group1_sha1** | **dh_group_exchange_sha1** }*

undo ssh server key-exchange

Parameters

Parameter	Description	Value
dh_group14_sha1	Adds the Diffie-hellman-group14-sha1 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group1_sha1	Adds the Diffie-hellman-group1-sha1 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group_exchange_sha1	Adds the Diffie-hellman-group-exchange-sha1 algorithm to the key exchange algorithm list of an SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

An SSH server and a client need to negotiate a key exchange algorithm for the packets exchanged between them. You can run the **ssh server key-exchange** command to configure a key exchange algorithm list for the SSH server. After the server receives a packet from the client, the server matches the key exchange algorithm list of the client against its local list and selects the first matched key exchange algorithm. If no matched key exchange algorithms, the negotiation fails.

Example

Configure key exchange algorithm lists **dh_group1_sha1** on the SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server key-exchange dh_group1_sha1
```

14.25.17 ssl minimum version

Function

The **ssl minimum version** command configures a minimum SSL version for an SSL policy.

Format

ssl minimum version tls1.0

Parameters

Parameter	Description	Value
tls1.0	Sets the minimum SSL version to TLS1.0 for an SSL policy.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

To configure a minimum SSL version for an SSL policy, run the **ssl minimum version** command so that service modules can flexibly adopt the SSL policy.

Example

Configure the minimum SSL version for the SSL policy **ftp_server** to be TLS1.0.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] ssl minimum version tls1.0
```

15 QoS Commands

15.1 MQC Configuration Commands

15.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.1.2 classifier behavior

Function

The **classifier behavior** command binds a traffic behavior to a traffic classifier in a traffic policy.

The **undo classifier** command unbinds a traffic behavior from a traffic classifier in a traffic policy.

By default, no traffic classifier or traffic behavior is bound to a traffic policy.

Format

classifier *classifier-name* **behavior** *behavior-name*

undo classifier *classifier-name*

Parameters

Parameter	Description	Value
classifier-name	Specifies the name of a traffic classifier.	The value must be the name of an existing traffic classifier.
behavior-name	Specifies the name of a traffic behavior.	The value must be the name of an existing traffic behavior.

Views

Traffic policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To take an action for packets of a certain type, use a traffic classifier to group the packets into one class and use a traffic behavior to define an action. Then associate the traffic classifier with the traffic behavior and bind them to a traffic policy.

Prerequisites

- A traffic classifier has been created using the **traffic classifier** command.
- A traffic behavior has been created using the **traffic behavior** command.
- A traffic policy has been created using the **traffic policy** command.

Precautions

You can dynamically add, modify, or delete the bound traffic classifiers, traffic behaviors, or binding of traffic classifiers and traffic behaviors in a traffic policy that has been applied to the system, a VLAN, or an interface.

NOTICE

Dynamically updating the traffic classifiers and traffic behaviors in a traffic policy makes the traffic policy ineffective for a short time. Confirm the operation before you use this command.

In a traffic policy, one traffic classifier can be bound to only one traffic behavior; each traffic policy supports a maximum of 256 pairs of traffic classifiers and traffic behaviors.

Example

Bind the traffic classifier **c1** to the traffic behavior **b1** in the traffic policy **p1**, and apply the traffic policy to GE0/0/1 in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark 8021p 2
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet0/0/1] quit
```

Bind the traffic classifier **c1** to the new traffic behavior **newb1** in the traffic policy **p1** that has been applied to GE0/0/1 in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior newb1
[HUAWEI-trafficpolicy-p1] quit
```

15.1.3 display acl division

Function

The **display acl division** command displays division rules based on the VLAN ID range in a delivered traffic classification rule or port number range in a delivered ACL rule.

Format

display acl division *start-id* **to** *end-id*

Parameters

Parameter	Description	Value
start-id	Specifies the start VLAN ID or port number.	The value is an integer that ranges from 0 to 65535.

Parameter	Description	Value
to *end-id*	Specifies the end VLAN ID or port number.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*] command is used to configure a traffic classification rule defining a VLAN ID range, or the **rule (advanced ACL view)** or **rule (advanced ACL6 view)** command is used with the protocol as TCP or UDP and the port number range specified, run the **display acl resource** command to view occupied ACL resources. The system divides a rule into multiple rules. The **display acl division** command displays division rules based on the VLAN ID range or port number range.

Example

Display division rules based on VLAN 10 to VLAN 20 or PORT10 to PORT20.

```
<HUAWEI> display acl division 10 to 20
 Range: 10 to 20;  Total rules: 4
 ---------------------------------------------------------
  [ 1]:Value = 10     Mask = 0xfffe  Range[   10,   11]
  [ 2]:Value = 12     Mask = 0xfffc  Range[   12,   15]
  [ 3]:Value = 16     Mask = 0xfffc  Range[   16,   19]
  [ 4]:Value = 20     Mask = 0xffff  Range[   20,   20]
```

Table 15-1 Description of the **display acl division** command output

Item	Description
Range	Input VLAN ID range or port number range.
Total rules	Number of division rules based on the VLAN ID range or port number range.
[1]	ID of the division rule.
Value	Start VLAN ID of the division rule.
Mask	Mask of the VLAN ID in the division rule.
Range	Division rule range.

15.1.4 display traffic behavior

Function

The **display traffic behavior** command displays the traffic behavior configuration on the device.

Format

display traffic behavior user-defined [*behavior-name*]

Parameters

Parameter	Description	Value
user-defined [*behavior-name*]	Displays the configuration of a specified traffic behavior. If the name of a traffic behavior is not specified, the configuration of all traffic behaviors is displayed.	The value must be the name of an existing traffic behavior.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic behavior** command displays the configuration of a specified traffic behavior or all traffic behaviors. The command output helps you check the traffic behavior configuration and locate faults.

Precautions

If no traffic behavior is created, the system displays the following information after this command is executed:

```
Info: There is no behavior exists.
```

If the specified traffic behavior name is incorrect, the system displays the following information after this command is executed:

```
Info: The behavior does not exist.
```

Example

Display the configuration of all traffic behaviors.

```
<HUAWEI> display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: tb1
      Committed Access Rate:
        CIR 1000 (Kbps), CBS 125000 (Byte)
        PIR 1000 (Kbps), PBS 125000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Remark:
        Remark 8021p 1
Total behavior number is 1
```

Table 15-2 Description of the **display traffic behavior user-defined** command output

Item	Description
Behavior	Traffic behavior name. To create a traffic behavior, run the **traffic behavior** command.
Committed Access Rate	CAR. To configure an action taken for packets whose rate exceeds the CAR, run the **car (traffic behavior view)** command.
CIR	Committed information rate (CIR). To set the CIR, run the **car (traffic behavior view)** command.
PIR	Peak information rate (PIR). To set the PIR, run the **car (traffic behavior view)** command.
CBS	Committed burst size (CBS). To set the CBS, run the **car (traffic behavior view)** command.
PBS	Peak burst size (PBS). To set the PBS, run the **car (traffic behavior view)** command.
Green Action	Action taken for green packets. To configure an action taken for green packets, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Red Action	Action taken for red packets. To configure an action taken for red packets, run the **car (traffic behavior view)** command.
Remark	Re-marking action. To configure re-marking, run the **remark** command.
Total behavior number is 1	Total number of created traffic behaviors.

15.1.5 display traffic classifier

Function

The **display traffic classifier** command displays the traffic classifier configuration on the device.

Format

display traffic classifier user-defined [*classifier-name*]

Parameters

Parameter	Description	Value
user-defined [*classifier-name*]	Displays the configuration of a specified traffic classifier. If the name of a traffic classifier is not specified, the configuration of all traffic classifiers is displayed.	The value must be the name of an existing traffic classifier.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic classifier** command displays the configuration of a specified traffic classifier or all traffic classifiers. The command output helps you check the traffic classifier configuration and locate faults.

Precautions

If no traffic classifier is created, the system displays the following information after this command is executed:

```
Info: There is no classifier exists.
```

If the specified traffic classifier name is incorrect, the system displays the following information after this command is executed:

```
Info: The classifier does not exist.
```

Example

Display the configuration of all traffic classifiers on the device.

```
<HUAWEI> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: AND
    Rule(s) : if-match vlan-id 120

   Classifier: c2
    Operator: AND
    Rule(s) : if-match vlan-id 110

   Classifier: c3
    Operator: AND
    Rule(s) : if-match vlan-id 100

Total classifier number is 3
```

Table 15-3 Description of the **display traffic classifier user-defined** command output

Item	Description
Classifier	Traffic classifier name. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.
Total classifier number is	Total number of created traffic classifiers.

15.1.6 display traffic policy

Function

The **display traffic policy** command displays the traffic policy configuration on the device.

Format

display traffic policy { **interface** [*interface-type interface-number* [*.subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]

display traffic policy ap-group [*ap-group*] [**outbound**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support **ssid-profile** and **ap-group**.

Parameters

Parameter	Description	Value
interface [*interface-type interface-number* [.*subinterface-number*]]	Displays the traffic policy configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* [.*subinterface-number*] specifies the interface or sub-interface number.	-
vlan [*vlan-id*]	Displays the traffic policy configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
ssid-profile [*ssid-profile-name*]	Displays the traffic policy configuration in a specified SSID profile.	The value must be the name of an existing SSID profile.
ap-group [*ap-group*]	Displays the traffic policy configuration in a specified AP group.	The value must be the name of an existing AP group.
global	Displays the traffic policy configuration in the system.	-
inbound	Displays the traffic policy configuration in the inbound direction.	-
outbound	Displays the traffic policy configuration in the outbound direction.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy** command displays the configuration of a specified traffic policy or all traffic policies. The command output helps you check the traffic policy configuration and locate faults.

Example

Display the configuration of the traffic policy applied to GE0/0/1 .

```
<HUAWEI> display traffic policy interface gigabitethernet 0/0/1

 Interface: GigabitEthernet0/0/1

 Direction: Inbound

 Policy: p1
   Classifier: c1
    Operator: AND
    Rule(s) :
       if-match acl 5500
       if-match 8021p 6
       if-match acl 3001
   Behavior: b1
     Statistic enable

     Committed Access Rate:
       CIR 1000 (Kbps), CBS 125000 (Byte)
       PIR 1000 (Kbps), PBS 125000 (Byte)
       Green Action   : pass
       Yellow Action  : pass
       Red Action     : discard
```

Table 15-4 Description of the **display traffic policy interface** command output

Item	Description
Interface	Interface to which the traffic policy is applied.
Direction	Direction to which a traffic policy is applied. To apply a traffic policy, run the **traffic-policy (interface view)** command.
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.
Behavior	Traffic behavior bound to the traffic classifier. To create a traffic behavior, run the **traffic behavior** command.

Item	Description
Committed Access Rate	CAR. To configure CAR, run the **car (traffic behavior view)** command.
CIR 100 (Kbps), CBS 9000 (Byte) PIR 40000 (Kbps), PBS 200000 (Byte)	Parameters in the QoS CAR profile, including the CIR, PIR, CBS, and PBS. To configure CAR parameters, run the **car (traffic behavior view)** command.
Green Action	Action taken for green packets. To configure an action taken for green packets, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Red Action	Action taken for red packets. To configure an action taken for red packets, run the **car (traffic behavior view)** command.

Display the traffic policy in the SSID profile named test on the S5732-H.

```
<HUAWEI> display traffic policy ssid-profile test inbound
  Ssid-profile: test

  Direction: Inbound

  Policy: 1
    Classifier: 1
     Operator: AND
     Rule(s) :
        if-match vlan-id 100
    Behavior: 1
      Permit
```

Table 15-5 Description of the **display traffic policy ssid-profile** command output

Item	Description
Ssid-profile	SSID profile to which the traffic policy is applied.
Direction	Direction to which a traffic policy is applied. To apply a traffic policy, run the **traffic-policy (SSID profile view)** command.
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.

Item	Description
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.
Behavior	Traffic behavior bound to the traffic classifier. To create a traffic behavior, run the **traffic behavior** command.
Permit	Allows packets matching the rule in the traffic classifier to pass. To allow or disallow packets matching the rule in the traffic classifier to pass, run the **deny | permit** command.

15.1.7 display traffic policy statistics

Function

The **display traffic policy statistics** command displays packet statistics in the specified object or each object to which a traffic policy has been applied.

Format

display traffic policy statistics { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* [*.subinterface-number*] | **vlan** *vlan-id* | **ssid-profile** *ssid-profile-name* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]

display traffic policy statistics ap-group *ap-group* **outbound** [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]

display traffic policy statistics policy-name *policy-name*

display traffic policy statistics all

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support **ssid-profile** *ssid-profile-name* and **ap-group** *ap-group*.

Parameters

Parameter	Description	Value
global	Displays packet statistics in the system to which a traffic policy has been applied.	-
slot *slot-id*	Displays packet statistics on a specified device to which a traffic policy has been applied. *slot-id* specifies the slot ID of the device.	The value range depends on the device configuration.
interface *interface-type interface-number* [.*subinterface-number*]	Displays packet statistics on a specified interface to which a traffic policy has been applied. - *interface-type* specifies the interface type. - *interface-number* [.*subinterface-number*] specifies the interface or sub-interface number.	-
vlan *vlan-id*	Displays packet statistics in a specified VLAN to which a traffic policy has been applied. *vlan-id* specifies the ID of the VLAN.	The value is an integer that ranges from 1 to 4094.
ssid-profile *ssid-profile-name*	Displays packet statistics in a specified SSID profile to which a traffic policy has been applied. *ssid-profile-name* specifies the name of the SSID profile.	The value must be the name of an existing SSID profile.
ap-group *ap-group*	Displays packet statistics in a specified AP group to which a traffic policy has been applied. *ap-group* specifies the name of the AP group .	The value must be the name of an existing AP group.

Parameter	Description	Value
inbound	Displays packet statistics in the inbound direction to which a traffic policy has been applied.	-
outbound	Displays packet statistics in the outbound direction to which a traffic policy has been applied.	-
verbose	Displays detailed packet statistics.	-
classifier-base	Displays statistics on packets matching a specified traffic classifier. If this parameter is specified, statistics on packets matching all traffic classifiers in the traffic policy are displayed.	-
rule-base	Displays statistics on packets matching a rule. If this parameter is specified, statistics on packets matching all rules are displayed.	-
class *classifier-name*	Specifies the name of a traffic classifier. If this parameter is specified, statistics on packets matching the specified traffic classifier or rules in the specified traffic classifier are displayed. If this parameter is not specified, statistics on packets matching all traffic classifiers are displayed.	The value must be the name of an existing traffic classifier.
policy-name *policy-name*	Displays packet statistics in each object to which the specified traffic policy is applied.	The value must be the name of an existing traffic policy.

Parameter	Description	Value
all	Displays packet statistics in each object to which a traffic policy has been applied, including packet statistics in the inbound or outbound directions in the system, on each interface, in each VLAN, and in each SSID profile.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy statistics** command displays packet statistics in the specified object or each object to which a traffic policy has been applied. The command output helps you check statistics on forwarded and discarded packets and locate faults.

Precautions

If no traffic policy is applied, the system displays the following information after this command is executed:

```
Info: The Policy is not applied in this view.
```

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays the following information after this command is executed:

```
Info: Statistic has not been enabled.
```

If the **rule-base** parameter is specified in this command to display packet statistics matching a rule in a traffic classifier and ACL rules are modified or deleted at the same time, ACL rule statistics that are displayed in pagination mode are inaccurate. To obtain accurate ACL rule statistics, run this command after ACL rules are modified or deleted.

On the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S, packetstatistics are collected only in the outbound direction of interfaces.

Example

Display packet statistics on GE0/0/1 in the inbound direction to which a traffic policy has been applied.

```
<HUAWEI> display traffic policy statistics interface gigabitethernet 0/0/1 inbound

 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Board : 0
---------------------------------------------------------------------
 Matched          |      Packets:                            0
                  |      Bytes:                              0
                  |      Rate(pps):                          0
                  |      Rate(bps):                          0
---------------------------------------------------------------------
   Passed         |      Packets:                            0
                  |      Bytes:                              0
                  |      Rate(pps):                          0
                  |      Rate(bps):                          0
---------------------------------------------------------------------
   Dropped        |      Packets:                            0
                  |      Bytes:                              0
                  |      Rate(pps):                          0
                  |      Rate(bps):                          0
---------------------------------------------------------------------
     Filter       |      Packets:                            0
                  |      Bytes:                              0
---------------------------------------------------------------------
     Car          |      Packets:                            0
                  |      Bytes:                              0
---------------------------------------------------------------------
```

Display statistics on incoming packets matching a rule after the traffic policy is applied to the system.

```
<HUAWEI> display traffic policy statistics global inbound verbose rule-base
 Global :
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Classifier: c1 operator and
 Behavior: b1
 if-match 8021p 5
 Board : 0
---------------------------------------------------------------------
 Passed           |      Packets:                            0
                  |      Bytes:                              0
                  |      Rate(pps):                          0
                  |      Rate(bps):                          0
---------------------------------------------------------------------
 Dropped          |      Packets:                            0
                  |      Bytes:                              0
                  |      Rate(pps):                          0
                  |      Rate(bps):                          0
---------------------------------------------------------------------
```

Display statistics on incoming packets matching a traffic classifier in the traffic policy that has been applied to GE0/0/1.

```
<HUAWEI> display traffic policy statistics interface gigabitethernet 0/0/1 inbound verbose classifier-base class c1

 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Classifier: c1 operator and
```

```
Behavior: b1
Board : 0
---------------------------------------------------------------------
Matched         |      Packets:                          0
                |      Bytes:                          0
                |      Rate(pps):                        0
                |      Rate(bps):                        0
---------------------------------------------------------------------
  Passed        |      Packets:                          0
                |      Bytes:                          0
                |      Rate(pps):                        0
                |      Rate(bps):                        0
---------------------------------------------------------------------
  Dropped       |      Packets:                          0
                |      Bytes:                          0
                |      Rate(pps):                        0
                |      Rate(bps):                        0
---------------------------------------------------------------------
    Filter      |      Packets:                          0
                |      Bytes:                          0
---------------------------------------------------------------------
    Car         |      Packets:                          0
                |      Bytes:                          0
---------------------------------------------------------------------
```

Display statistics about incoming packets matching rules after the traffic policy is applied to GigabitEthernet 0/0/1.

```
<HUAWEI> display traffic policy statistics interface GigabitEthernet 0/0/1 inbound verbose rule-base
Interface: GigabitEthernet0/0/1
Traffic policy inbound: tp2
Rule number: 2
Current status: success
Statistics interval: 300
---------------------------------------------------------------------
Classifier: c2 operator and
Behavior: b1
Board : 0
rule 15 permit ip source 10.154.128.6 0 (match-counter 0)
---------------------------------------------------------------------
Passed          |      Packets:                          0
                |      Bytes:                          -
                |      Rate(pps):                        0
                |      Rate(bps):                        -
---------------------------------------------------------------------
Dropped         |      Packets:                          0
                |      Bytes:                          -
                |      Rate(pps):                        0
                |      Rate(bps):                        -
---------------------------------------------------------------------
rule 70 permit ip source 10.10.12.0 0.0.0.31 (match-counter 0)
---------------------------------------------------------------------
Passed          |      Packets:                   13,528
                |      Bytes:                          -
                |      Rate(pps):                        0
                |      Rate(bps):                        -
---------------------------------------------------------------------
Dropped         |      Packets:                          0
                |      Bytes:                          -
                |      Rate(pps):                        0
                |      Rate(bps):                        -
---------------------------------------------------------------------
```

Table 15-6 Description of the **display traffic policy statistics** command output

Item	Description
Interface	Interface to which the traffic policy is applied.
Global	System to which the traffic policy is applied.
Vlan	VLAN to which the traffic policy is applied.
Ssid-profile	SSID profile to which the traffic policy is applied.
Ap-group	AP group to which the traffic policy is applied.
Traffic policy inbound	Applied traffic policy.
Rule number	Number of valid rules in the traffic classifier.
Current status	Traffic policy status.
Statistics interval	Interval for collecting traffic statistics. To set the interval for collecting traffic statistics, run the **traffic statistics interval** command.
Classifier	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior name. To create a traffic behavior, run the **traffic behavior** command.
Board	ID of the switch to which the traffic policy is applied. When you query the statistics on an Eth-Trunk, the system displays only the statistics on the switch where member interfaces in the Eth-Trunk are located.
Matched	Numbers of packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Passed	Numbers of forwarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.

Item	Description
Dropped	Numbers of discarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. The discarded packets include the filtered packets and packets dropped by CAR.
Filter	Numbers of filtered packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Car	Numbers of packets and bytes that match traffic classification rules and are discarded by CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. To configure CAR, run the **car (traffic behavior view)** command.
Packets	Number of packets. If the information is displayed as -, the statistics on this item cannot be collected.
Bytes	Number of bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(pps)	Rate, in pps. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(bps)	Rate, in bit/s. If the information is displayed as -, the statistics on this item cannot be collected.
match-counter 0	Number of times packets match ACL rules. **NOTE** FTP, TFTP, Telnet, SNMP, HTTP, routing, and multicast packets match software ACL rules, and the number of times packets match software ACL rules can be checked using a command. Other packets match hardware ACL rules, and the number of times packets match hardware ACL rules can be checked using other methods. For example, to view the number of times packets match ACL rules after a traffic policy is applied, run the **statistic enable (traffic behavior view)** command to enable traffic statistics in the traffic behavior and run the **display traffic policy statistics** command to check statistics.

15.1.8 display traffic policy user-defined

Function

The **display traffic policy user-defined** command displays the user-defined traffic policy configuration.

Format

display traffic policy user-defined [*policy-name* [**classifier** *classifier-name*]]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specified user-defined traffic policy. If this parameter is not specified, the configuration of all user-defined traffic policies is displayed.	The value must be the name of an existing traffic policy.
classifier *classifier-name*	Displays the configuration of a traffic behavior bound to a specified traffic classifier in a traffic policy. If this parameter is not specified, the traffic policy configuration is displayed.	The value must be the name of an existing traffic classifier.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy user-defined** command displays the configuration of a specified traffic policy or all traffic policies. The command output helps you check the traffic policy configuration and locate faults.

Precautions

If no traffic policy is created, the system displays the following information after the **display traffic policy user-defined** command is executed:

```
Info: There is no policy exists.
```

If the specified traffic policy name is incorrect, the system displays the following information after the **display traffic policy user-defined** command is executed:

```
Info: The policy does not exist.
```

Example

Display the user-defined traffic policy configuration.

```
<HUAWEI> display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: tb1
      Remark:
        Remark 8021p 0
      Committed Access Rate:
        CIR 10000 (Kbps), CBS 1250000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard

Total policy number is 1
```

Table 15-7 Description of the **display traffic policy user-defined** command output

Item	Description
User Defined Traffic Policy Information	User-defined traffic policy configuration.
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To create a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior associated with the traffic classifier in the traffic policy. To create a traffic behavior, run the **traffic behavior** command.
Committed Access Rate	CAR. To configure the CAR, run the **car (traffic behavior view)** command.
Green Action	Action taken for green packets. To configure an action taken for green packets, run the **car (traffic behavior view)** command.

Item	Description
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Red Action	Action taken for red packets. To configure an action taken for red packets, run the **car (traffic behavior view)** command.
Remark	Re-marking action. To configure re-marking, run the **remark** command.
Total policy number is	Total number of created traffic policies.

15.1.9 display traffic-applied

Function

The **display traffic-applied** command displays information about ACL-based simplified and MQC-based traffic policies applied in various views.

Format

display traffic-applied [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]

display traffic-applied [**ssid-profile** [*ssid-profile-name*] | **traffic-profile** [*traffic-profile-name*]] { **inbound** | **outbound** }

display traffic-applied ap-group [*ap-group*] **outbound**

display traffic-applied brief

display traffic-applied record

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support **ssid-profile** and **ap-group**.

Parameters

Parameter	Description	Value
interface [*interface-type interface-number*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If this parameter is not specified, information about ACL-based simplified and MQC-based traffic policies applied to the system or a VLAN is displayed.	-
vlan [*vlan-id*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified VLAN. If this parameter is not specified, information about ACL-based simplified and MQC-based traffic policies applied to the system or an interface is displayed.	The value is an integer that ranges from 1 to 4094.
ssid-profile [*ssid-profile-name*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified SSID profile.	The value must be the name of an existing SSID profile.
ap-group [*ap-group*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified AP group.	The value must be the name of an existing AP group.

Parameter	Description	Value
traffic-profile [*traffic-profile-name*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified traffic profile.	The value must be the name of an existing traffic profile.
inbound	Displays information about ACL-based simplified and MQC-based traffic policies applied in the inbound direction.	-
outbound	Displays information about ACL-based simplified and MQC-based traffic policies applied in the outbound direction.	-
verbose	Displays detailed information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, or an interface.	-
brief	Displays brief information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, an interface, an SSID profile, or a traffic profile.	-
record	Displays information about all ACL-based simplified traffic policies applied to the device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display traffic-applied** command displays information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, or an interface.

Example

Display information about globally applied ACL-based simplified and MQC-based traffic policies in the inbound direction.

```
<HUAWEI> display traffic-applied inbound
------------------------------------------------------------
Policy applied inbound global
  Policy:    p1
------------------------------------------------------------
```

Table 15-8 Description of the **display traffic-applied inbound** command output

Item	Description
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.

Display the configuration of all ACL-based simplified traffic policies on the device.

```
<HUAWEI> display traffic-applied record
---------------------------------------------------------------------------
*interface GigabitEthernet0/0/1
 traffic-filter inbound acl 3000
  slot 0: success

---------------------------------------------------------------------------
*system
 traffic-filter inbound acl 3001
  slot 0: success

 traffic-filter outbound acl 3002
  slot 0: success

---------------------------------------------------------------------------
```

Table 15-9 Description of the **display traffic-applied record** command output

Item	Description
interface GigabitEthernet0/0/1	Interface where the ACL-based simplified traffic policy has been applied.
traffic-filter inbound acl 3000	Configuration of the ACL-based simplified traffic policy that has been applied. For details, see **ACL-based Simplified Traffic Policy Commands**.

Item	Description
slot	Slot where the ACL-based simplified traffic policy has been applied. The value is 0 in a non-stack scenario. In a stack scenario, the value depends on the device configuration.
success	Status of the ACL-based simplified traffic policy that has been applied: ● success: The ACL-based simplified traffic policy has been applied successfully. ● fail: The ACL-based simplified traffic policy fails to be applied.
system	Configuration of the ACL-based simplified traffic policy that has been applied globally.

15.1.10 display traffic-policy applied-record

Function

The **display traffic-policy applied-record** command displays traffic policy records.

Format

display traffic-policy applied-record [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the record of a specified traffic policy. If this parameter is not specified, records of all the applied traffic policies are displayed.	The value must be the name of an existing traffic policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-policy applied-record** command displays a record of an applied traffic policy or records of all applied traffic policies, including the view, interface number, and direction that the traffic policy/policies is/are applied to, traffic policy status on an SSID profile, and number of times the traffic policy/policies is/are applied. The command output helps you check traffic policy records and locate faults.

Precautions

If no traffic policy is created, the system does not display any information after this command is executed.

If the specified traffic policy name is incorrect, the system displays the following information after this command is executed:

```
Info: Traffic policy does not exist.
```

Example

Display the record of the traffic policy **p1** in a non-stack scenario.

```
<HUAWEI> display traffic-policy applied-record p1
-------------------------------------------------
  Policy Name:   p1
  Policy Index:  0
     Classifier:c1     Behavior:b1
-------------------------------------------------
 *interface GigabitEthernet0/0/1
    traffic-policy p1 inbound
      slot 0    :  success (support sharing)
 *vlan 100
    traffic-policy p1 inbound
      slot 0    :  success
 *system
    traffic-policy p1 global inbound
      slot 0    :  success
 *ssid-profile test
    traffic-policy p1 inbound
      slot 0    :  success
 *ap-group test
    traffic-policy p1 outbound
      slot 0    :  success
-------------------------------------------------
  Policy total applied times: 5.
```

Display the record of the traffic policy **p1** in a stack scenario.

```
<HUAWEI> display traffic-policy applied-record p1
-------------------------------------------------
  Policy Name:   p1
  Policy Index:  1
     Classifier:c1     Behavior:b1
-------------------------------------------------
 *system
    traffic-policy p1 global inbound
      slot 2  :  success
      slot 1  :  success
      slot 0  :  success
 *system
    traffic-policy p1 global outbound
      slot 2  :  success
      slot 1  :  success
```

```
     slot 0  :  success
-------------------------------------------------
 Policy total applied times: 2.
```

Table 15-10 Description of the **display traffic-policy applied-record** command output

Item	Description
Policy Name	Traffic policy name. To configure a traffic policy, run the **traffic policy** command.
Policy Index	Traffic policy index.
Classifier	Traffic classifier name. To configure a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior name. To configure a traffic behavior, run the **traffic behavior** command.
interface GigabitEthernet0/0/1	Interface to which the traffic policy is applied. To apply a traffic policy to an interface, run the **traffic-policy (interface view)** command.
traffic-policy p1 inbound	Inbound direction to which the traffic policy **p1** is applied.
traffic-policy p1 outbound	Outbound direction to which the traffic policy **p1** is applied.
slot	Status of the traffic policy applied to the specified slot. ● success (support sharing): The traffic policy is applied successfully, and resources occupied by the traffic policy that is applied to the inbound direction of an interface can be shared by other interfaces to which the same traffic policy that is applied in the inbound direction in the slot. ● success: The traffic policy is applied successfully, but resources occupied by the traffic policy that is applied to an interface cannot be shared by other interfaces in the slot. ● fail: The traffic policy fails to be applied.
vlan	VLAN to which the traffic policy is applied. To apply a traffic policy to a VLAN, run the **traffic-policy (VLAN view)** command.
system	System to which the traffic policy is applied. To apply a traffic policy to the system, run the **traffic-policy global** command.

Item	Description
ssid-profile	SSID profile to which the traffic policy is applied. To apply a traffic policy to an SSID profile, run the **traffic-policy (SSID profile view)** command. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support SSID profiles.
ap-group	AP group to which the traffic policy is applied. To apply a traffic policy to an AP group, run the **traffic-policy (AP Group view)** command. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the AP group view.
Policy total applied times	Number of times the traffic policy is applied.

15.1.11 if-match 8021p

Function

The **if-match 8021p** command configures a matching rule based on the 802.1p priority of VLAN packets in a traffic classifier.

The **undo if-match 8021p** command deletes a matching rule based on the 802.1p priority of VLAN packets in a traffic classifier.

By default, a matching rule based on the 802.1p priority of VLAN packets is not configured in a traffic classifier.

Format

if-match 8021p *8021p-value* &<1-8>

undo if-match 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority in VLAN packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match 8021p** command to classify traffic based on the 802.1p priority in VLAN packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

For a Layer 2 network, run the **if-match 8021p** command; for a Layer 3 network, run the **if-match dscp** command.

After the **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id**, and **remark vlan-id** commands are used, the system modifies VLAN tags of packets according to the re-marking configuration. These actions are called VLAN-based actions.

Regardless of whether the relationship between traffic classification rules is AND or OR, if you enter multiple values of 802.1p priorities, the packet that matches one 802.1p priority matches a rule.

If you run the **if-match 8021p** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the 802.1p priority of 1 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match 8021p 1
```

15.1.12 if-match acl

Function

The **if-match acl** command configures a matching rule based on an Access Control List (ACL) in a traffic classifier.

The **undo if-match acl** command deletes a matching rule based on an ACL.

By default, a matching rule based on an ACL is not configured in a traffic classifier.

Format

if-match [**ipv6**] **acl** { *acl-number* | *acl-name* }

undo if-match [**ipv6**] **acl** { *acl-number* | *acl-name* }

Parameters

Parameter	Description	Value
ipv6	Indicates that IPv6 ACLs are matched. If this parameter is not specified, IPv4 ACLs are matched.	-
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 5999, and the value of an ACL6 ranges from 2000 to 3999. ● ACLs numbered 2000 to 2999 are basic ACLs, which are used to classify all packets. ● ACLs numbered 3000 to 3999 are advanced ACLs, which are used to classify packets based on Layer 3 information. ● ACLs numbered 4000 to 4999 are Layer 2 ACLs, which are used to classify packets based on the source MAC address, destination MAC address, and packet type. ● ACLs numbered 5000 to 5999 are user-defined ACLs.
acl-name	Specifies the name of an ACL.	The value must be the name of an existing ACL.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To classify packets based on the interface that receives packets, source IP address, destination IP address, protocol over IP, source and destination TCP port numbers, ICMP type and code, and source and destination MAC addresses, ARP packets, reference an ACL in a traffic classifier. You must first define an ACL and configure rules in the ACL, and then run the **if-match acl** command to configure a matching rule based on the ACL so that the device processes packets matching the same rule in the same manner.

Prerequisites

The following operations must have been performed:

- Create an ACL and configure rules in the ACL.
- Create a traffic classifier using the **traffic classifier** command.

Precautions

Regardless of whether the relationship between rules in a traffic classifier is AND or OR, if an ACL contains multiple rules, the packet that matches one ACL rule matches the ACL.

Only the S6720-EI, S6735-S, and S6720S-EI support traffic classifiers with advanced ACLs containing the **ttl-expired** field.

You can configure multiple ACL rules in a traffic classifier to match different types of packets.

If the **vpn-instance** parameter is specified in an ACL rule, a traffic policy that defines a traffic classifier matching this ACL rule does not take effect.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, and S500, S5735-S-I, S5735S-S, if a traffic policy is applied to the outbound direction and the relationship between rules in a traffic classifier is AND:

- Rules for matching the source IPv6 address and those for matching the destination IPv6 address cannot be configured in the same traffic classifier.
- Rules for matching IPv6 information (for example, **if-match protocol ipv6** and **if-match ipv6 acl**) and those for matching the source MAC address, destination MAC address, source IPv6 address, or destination IPv6 address of packets cannot be configured in the same traffic classifier. (ACL6 rules can be used to match the source or destination IPv6 address of packets.)
- Rules for matching IPv4 information (IP address and UDP port number) and those for matching some Layer 2 information (for example, **if-match source-mac**, **if-match destination-mac**, and **if-match l2-protocol** { **mpls** | **rarp** | *protocol-value* }) cannot be configured in the same traffic classifier.

On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, and S500, S5735-S-I, S5735S-S, if a traffic policy is applied to the outbound direction, and an ACL6 rule for matching the source IPv6 address of packets and an ACL6 rule for matching the destination IPv6 address of packets are respectively configured in two traffic classifiers:

- If the traffic behaviors corresponding to the two traffic classifiers do not conflict, the two traffic classifiers and their corresponding traffic behaviors take effect.
- If the traffic behaviors corresponding to the two traffic classifiers conflict, the traffic behavior and traffic classifier defining the ACL6 rule for matching the source IPv6 address of packets take effect.

MTU-exceeded UDP packets will be fragmented. Only the first fragmented packet contains UDP information, and the other fragmented packets cannot be matched against ACL rules based on UDP information. Therefore, a traffic policy that contains **if-match acl** for matching UDP information does not take effect on fragmented packets. For example, if traffic policing is configured for traffic that contains a large number of fragmented packets and these fragmented packets do not match the UDP port number in an ACL rule, traffic policing is not performed on the fragmented packets. As a result, the actual rate is higher than the rate limit.

For S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, on devices for which the resource mode of extended entry space cannot be configured, ACL6 rules can define only the protocol number, source port number, destination port number, source IPv6 address, and destination IPv6 address. Additionally, ACL6-based traffic policies that contain these ACL6 rules cannot be applied to sub-interfaces and VLANIF interfaces.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, if the **first-fragment** parameter is specified in an ACL rule, a traffic policy defining this ACL rule can be applied only to the inbound direction.

Example

Configure a matching rule based on ACL 2046 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] acl 2046
[HUAWEI-acl-basic-2046] rule permit source any
[HUAWEI-acl-basic-2046] quit
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match acl 2046
```

15.1.13 if-match any

Function

The **if-match any** command configures a matching rule based on all data packets in a traffic classifier.

The **undo if-match any** command deletes a matching rule based on all data packets in a traffic classifier.

By default, a matching rule based on all data packets is not configured in a traffic classifier.

Format

if-match any

undo if-match any

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To process all the data packets in the same manner, you can run the **if-match any** command to configure a matching rule based on all data packets in a traffic classifier.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

After the **if-match any** command is run, only the matching rule configured using this command takes effect, and the other matching rules in the same traffic classifier will become ineffective.

Example

Configure a matching rule based on all data packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match any
```

15.1.14 if-match cvlan-8021p

Function

The **if-match cvlan-8021p** command configures a matching rule based on the 802.1p priority in the inner tag of QinQ packets in a traffic classifier.

The **undo if-match cvlan-8021p** command deletes a matching rule based on the 802.1p priority in the inner tag of QinQ packets in a traffic classifier.

By default, a matching rule based on the 802.1p priority in the inner tag of QinQ packets is not configured in a traffic classifier.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

if-match cvlan-8021p *8021p-value* &<1-8>

undo if-match cvlan-8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in the inner tag of QinQ packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of QinQ packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match cvlan-8021p** command to classify packets based on the 802.1p priority in the inner tag of QinQ packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match cvlan-8021p** command is valid for only the double-tagged packets.

If you enter multiple 802.1p priorities in the inner tag of packets in the command, a packet matches a rule as long as it matches one of the 802.1p priorities in the inner tag of packets, regardless of whether the relationship between traffic classification rules is AND or OR.

If you run the **if-match cvlan-8021p** command multiple times in the same traffic classifier view, only the latest configuration takes effect.

Example

Configure a matching rule based on the inner 802.1p priority of 1 in QinQ packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match cvlan-8021p 1
```

15.1.15 if-match cvlan-id

Function

The **if-match cvlan-id** command configures a matching rule based on VLAN IDs in the inner and outer tags of QinQ packets in a traffic classifier. You can specify the VLAN ID range in the inner tag.

The **undo if-match cvlan-id** command deletes a matching rule based on VLAN IDs in the inner and outer tags of QinQ packets in a traffic classifier.

By default, a matching rule based on the VLAN ID in the inner and outer tags of QinQ packets is not configured in a traffic classifier.

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

if-match cvlan-id *start-cvlan-id* [**to** *end-cvlan-id*] [**vlan-id** *vlan-id*]

undo if-match cvlan-id *start-cvlan-id* [**to** *end-cvlan-id*] [**vlan-id** *vlan-id*]

Parameters

Parameter	Description	Value
start-cvlan-id [**to** *end-cvlan-id*]	Specifies the VLAN ID in the inner tag of a QinQ packet.	• *start-cvlan-id* specifies the start VLAN ID in the inner tag. The value is an integer that ranges from 1 to 4094. • *end-cvlan-id* specifies the end VLAN ID in the inner tag. The value is an integer that ranges from 1 to 4094. The value of *end-cvlan-id* must be larger than the value of *start-cvlan-id*. If **to** *end-cvlan-id* is not specified, only the VLAN ID specified by *start-cvlan-id* is matched.
vlan-id *vlan-id*	Specifies the VLAN ID in the outer tag of a QinQ packet. If this parameter is not specified, only the VLAN ID in the inner tag of a QinQ packet is matched.	The value is an integer that ranges from 1 to 4094.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match cvlan-id** command to classify packets based on the VLAN ID in the inner tag of QinQ packets or VLAN IDs in inner and outer tags of QinQ packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match cvlan-id** command is valid only for the double-tagged packets.

On the S6720-EI, if a traffic policy contains the traffic classifier defining the **if-match cvlan-id** *start-cvlan-id* [**to** *end-cvlan-id*] **vlan-id** *vlan-id* matching rule, IPv6 ACL resources are occupied. To display information about IPv6 ACL resources, run the **display acl resource** command.

Example

Configure a matching rule based on the VLAN ID of 100 in the inner tag of QinQ packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match cvlan-id 100
```

Configure a matching rule based on the inner VLAN ID in the range of 100 to 200 and outer VLAN ID 300 of QinQ packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match cvlan-id 100 to 200 vlan-id 300
```

15.1.16 if-match destination-mac

Function

The **if-match destination-mac** command configures a matching rule based on the destination MAC address in a traffic classifier.

The **undo if-match destination-mac** command deletes a matching rule based on the destination MAC address in a traffic classifier.

By default, a matching rule based on the destination MAC address is not configured in a traffic classifier.

Format

if-match destination-mac *mac-address* [*mac-address-mask*]

undo if-match destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
mac-address-mask	Specifies the mask of the destination MAC address. Similar to the mask of the IP address, the value F indicates that the destination MAC address is matched and the value 0 indicates that the destination MAC address is not matched. The mask of the MAC address determines a group of MAC addresses. The device can accurately match certain bits in the destination MAC address using the mask of the MAC address. In practice, you can set these bits to F in the mask of the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be 0-0-0.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match destination-mac** command to configure a matching rule based on the destination MAC address in a traffic classifier so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match destination-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, and S500, S5735-S-I, S5735S-S, if a traffic policy is applied to the outbound direction and the relationship between rules in a traffic classifier is AND:

- Rules for matching the source IPv6 address and those for matching the destination IPv6 address cannot be configured in the same traffic classifier.
- Rules for matching IPv6 information (for example, **if-match protocol ipv6** and **if-match ipv6 acl**) and those for matching the source MAC address, destination MAC address, source IPv6 address, or destination IPv6 address of packets cannot be configured in the same traffic classifier. (ACL6 rules can be used to match the source or destination IPv6 address of packets.)
- Rules for matching IPv4 information (IP address and UDP port number) and those for matching some Layer 2 information (for example, **if-match source-mac**, **if-match destination-mac**, and **if-match l2-protocol** { **mpls** | **rarp** | *protocol-value* }) cannot be configured in the same traffic classifier.

Example

Configure a matching rule based on the destination MAC address of 00eo-fc12-3456 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match destination-mac 00eo-fc12-3456
```

Configure a matching rule based on the destination MAC address of XXeo-fXX2-3456 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match destination-mac 00eo-fc12-3456 00ff-f00f-ffff
```

15.1.17 if-match discard

Function

The **if-match discard** command configures a matching rule based on drop packets in a traffic classifier.

The **undo if-match discard** command deletes a matching rule based on drop packets in a traffic classifier.

By default, no matching rule based on drop packets is configured in a traffic classifier.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

if-match discard

undo if-match discard

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After packets reach the device, invalid packets are discarded. You can run the **if-match discard** command to configure the device to match discarded packets, take action for the discarded packets such as traffic statistics collection and mirroring, and analyze them.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, both the traffic classifier defining **if-match discard** and traffic classifiers defining other matching rules (excluding **if-match application**) take effect. Examples are as follows:

- A packet matches two pairs of traffic classifiers and traffic behaviors defined in the same traffic policy, and only one traffic classifier contains **if-match discard**. (The other traffic classifier does not contain **if-match discard** or **if-match application**.) In this case, both pairs of traffic classifiers and traffic behaviors take effect for the packet.
- A packet matches two traffic policies, and a traffic classifier contains **if-match discard** in only one of the traffic policies. (The other traffic policy does not contain **if-match discard** or **if-match application**.) In this case, both traffic policies take effect for the packet.

Example

Configure a matching rule based on discarded packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match discard
```

15.1.18 if-match double-tag

Function

The **if-match double-tag** command configures a matching rule based on double tags of packets in a traffic classifier.

The **undo if-match double-tag** command deletes a matching rule based on double tags of packets in a traffic classifier.

By default, a matching rule based on double tags of packets is not configured in a traffic classifier.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

if-match double-tag

undo if-match double-tag

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match double-tag** command to classify traffic based on double tags so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Example

Configure a matching rule based on double tags of packets in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match double-tag
```

15.1.19 if-match dscp

Function

The **if-match dscp** command configures a matching rule based on the Differentiated Services Code Point (DSCP) priority of packets in a traffic classifier.

The **undo if-match dscp** command deletes a matching rule based on the DSCP priority of packets in a traffic classifier.

By default, a matching rule based on the DSCP priority of packets is not configured in a traffic classifier.

Format

if-match dscp *dscp-value* &<1-8>

undo if-match dscp

Parameters

Parameter	Description	Value
dscp *dscp-value*	Specifies the DSCP priority.	The value can be a DiffServ code, an integer ranging from 0 to 63, or the name of the DSCP service type such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The values corresponding to service types are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match dscp** command to classify packets based on the DSCP priority of packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

For a Layer 2 network, run the **if-match 8021p** command; for a Layer 3 network, run the **if-match dscp** command.

if-match dscp can match both IPv4 and IPv6 packets.

If you enter multiple DSCP priorities in the command, a packet matches a rule as longs as it matches one of the DSCP priorities, regardless of whether the relationship between traffic classification rules is AND or OR.

If the relationship between rules in a traffic classifier is AND, the **if-match dscp** and **if-match ip-precedence** commands cannot be used in the traffic classifier simultaneously.

In a version earlier than V200R009C00, if **if-match dscp** *dscp-value* is configured in the traffic classifier on the switch, the traffic classifier can only match IPv4 packets. After the switch is upgraded to V200R009C00 and later versions, the traffic classifier can match IPv4 and IPv6 packets.

If you run the **if-match dscp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the DSCP priority of 1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match dscp 1
```

15.1.20 if-match flow-id

Function

The **if-match flow-id** command configures a matching rule based on the flow ID in a traffic classifier.

The **undo if-match flow-id** command deletes a matching rule based on the flow ID in a traffic classifier.

By default, no matching rule based on the flow ID is configured in a traffic classifier.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

if-match flow-id *flow-id*

undo if-match flow-id

Parameters

Parameter	Description	Value
flow-id	Specifies a flow ID.	The value is an integer that ranges from 1 to 15.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a traffic policy is applied to different interfaces or VLANs, to save ACL resources, you can run the **if-match flow-id** command to classify packets based on the flow ID so that the device processes packets matching the same flow ID in the same manner.

Assume that *M* ACLs are configured on the device to distinguish services, and each ACL contains *N* ACL rules. Traffic classifiers classify packets based on ACL rules, and the traffic policy containing the ACL rules is applied to *X* interfaces. If the actions of re-marking flow IDs and matching rules based on the flow IDs are not configured, applying the traffic policy occupies $M \times N \times X$ ACL resources. If the actions of re-marking flow IDs and matching rules based on flow IDs are configured, applying the traffic policy occupies only $M \times (N + X)$ ACL resources.

Prerequisites

The following operations must have been performed before this command is used:

- Run the **remark flow-id** command in the traffic behavior view to configure an action of re-marking the flow ID.
- Run the **traffic classifier** command in the system view to create a traffic classifier.

Precautions

It is recommended that the traffic classifier containing **if-match flow-id** and the traffic behavior containing **remark flow-id** be bound to different traffic policies.

The traffic policy containing **if-match flow-id** can be only applied to an interface, a VLAN, a VLANIF interface, or the system in the inbound direction.

If you run the **if-match flow-id** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the flow ID of 1 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match flow-id 1
```

15.1.21 if-match inbound-interface

Function

The **if-match inbound-interface** command configures a matching rule based on an inbound interface in a traffic classifier.

The **undo if-match inbound-interface** command deletes a matching rule based on an inbound interface in a traffic classifier.

By default, a matching rule based on an inbound interface is not configured in a traffic classifier.

Format

if-match inbound-interface *interface-type interface-number*

undo if-match inbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an inbound interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match inbound-interface** command to classify traffic based on an inbound interface so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

A traffic policy containing **if-match inbound-interface** cannot be applied to an interface.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the inbound interface in this command cannot be an Eth-Trunk member interface.

A traffic policy containing the **if-match inbound-interface** rule can only be applied to the inbound direction.

If you run the **if-match inbound-interface** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the inbound interface of GE0/0/1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match inbound-interface gigabitethernet 0/0/1
```

15.1.22 if-match ip-precedence

Function

The **if-match ip-precedence** command configures a matching rule based on the IP precedence of packets in a traffic classifier.

The **undo if-match ip-precedence** command deletes a matching rule based on the IP precedence of packets in a traffic classifier.

By default, a matching rule based on the IP precedence of packets is not configured in a traffic classifier.

Format

if-match ip-precedence *ip-precedence-value* &<1-8>

undo if-match ip-precedence

Parameters

Parameter	Description	Value
ip-precedence-value	Specifies the IP precedence.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match ip-precedence** command to classify packets based on the IP precedence so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

After the **if-match ip-precedence** command is run, IP precedences are listed in ascending order.

If you enter multiple IP precedences in the **if-match ip-precedence** command, a packet matches a rule as long as it matches one of the IP precedence values, regardless of whether the relationship between traffic classification rules is AND or OR.

In a traffic classifier where the relationship between rules is AND, the **if-match dscp** and **if-match ip-precedence** commands cannot be used simultaneously.

If you run the **if-match ip-precedence** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the IP precedence of 1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match ip-precedence 1
```

15.1.23 if-match l2-protocol

Function

The **if-match l2-protocol** command configures a matching rule based on the Layer 2 protocol type in a traffic classifier.

The **undo if-match l2-protocol** command deletes a matching rule based on the Layer 2 protocol type in a traffic classifier.

By default, a matching rule based on the Layer 2 protocol type is not configured in a traffic classifier.

Format

if-match l2-protocol { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }

undo if-match l2-protocol

Parameters

Parameter	Description	Value
arp	Indicates that ARP packets are classified.	The value of **arp** corresponds to 0x0806.
ip	Indicates that IP packets are classified.	The value of **ip** corresponds to 0x0800.
mpls	Indicates that MPLS packets are classified.	The value of **mpls** corresponds to 0x8847.

Parameter	Description	Value
rarp	Indicates that RARP packets are classified.	The value of **rarp** corresponds to 0x8035.
protocol-value	Specifies the value of a protocol type.	The value ranges from 0x0000 to 0xFFFF in hexadecimal notation and must start with 0x. If the value of *protocol-value* is smaller than 0x0600, the Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) fields in the Logical Line Control (LLC) protocol packets are matched.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match l2-protocol** command to classify packets based on the Layer 2 protocol type so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The device supports Layer 2 protocols including ARP, IP, MPLS, and RARP.

If you run the **if-match l2-protocol** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

If the relationship between rules in a traffic classifier is AND, and both the **if-match l2-protocol arp** and **if-match protocol** { **ip** | **ipv6** } commands are configured in this traffic classifier, of the two, only the **if-match l2-protocol arp** command takes effect.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, and S500, S5735-S-I, S5735S-S, if a traffic policy is applied to the outbound direction and the relationship between rules in a traffic classifier is AND:

- Rules for matching the source IPv6 address and those for matching the destination IPv6 address cannot be configured in the same traffic classifier.
- Rules for matching IPv6 information (for example, **if-match protocol ipv6** and **if-match ipv6 acl**) and those for matching the source MAC address, destination MAC address, source IPv6 address, or destination IPv6 address of packets cannot be configured in the same traffic classifier. (ACL6 rules can be used to match the source or destination IPv6 address of packets.)
- Rules for matching IPv4 information (IP address and UDP port number) and those for matching some Layer 2 information (for example, **if-match source-mac**, **if-match destination-mac**, and **if-match l2-protocol** { **mpls** | **rarp** | *protocol-value* }) cannot be configured in the same traffic classifier.

Example

Define a matching rule based on the protocol type of ARP in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match l2-protocol arp
```

15.1.24 if-match mpls-exp

Function

The **if-match mpls-exp** command configures a matching rule based on the EXP priority of MPLS packets in a traffic classifier.

The **undo if-match mpls-exp** command deletes a matching rule based on the EXP priority of MPLS packets in a traffic classifier.

By default, a matching rule based on the EXP priority of MPLS packets is not configured in a traffic classifier.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6720-EI, S6720S-EI, S6730S-H, S5731-S, S5731S-S, S6730-S, S6730S-S, and S6730-H support this command.

Format

if-match mpls-exp *exp-value* &<1-8>

undo if-match mpls-exp

Parameters

Parameter	Description	Value
exp-value	Specifies the EXP priority of MPLS packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of MPLS packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match mpls-exp** command to classify MPLS packets based on the EXP priority so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you enter multiple values of EXP priorities in the command, a packet matches the traffic classifier as long as it matches one of the EXP priorities, regardless of whether the relationship between traffic classification rules is AND or OR.

If a traffic classifier in the traffic policy contains **if-match mpls-exp**, the traffic policy cannot be applied to the outbound direction on the S6720-EI and S6720S-EI.

If you run the **if-match mpls-exp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the EXP priority of 1 or 4 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match mpls-exp 1 4
```

15.1.25 if-match outbound-interface

Function

The **if-match outbound-interface** command configures a matching rule based on an outbound interface in a traffic classifier.

The **undo if-match outbound-interface** command deletes a matching rule based on an outbound interface in a traffic classifier.

By default, a matching rule based on an outbound interface is not configured in a traffic classifier.

NOTE

The S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S6720S-S, and S5735S-S do not support this command.

Format

if-match outbound-interface *interface-type interface-number*

undo if-match outbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an outbound interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match outbound-interface** command to classify packets based on an outbound interface so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

A traffic policy containing **if-match outbound-interface** cannot be applied to an interface.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, the outbound interface in this command cannot be an Eth-Trunk member interface.

A traffic policy containing the **if-match outbound-interface** rule can only be applied to the outbound direction on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6730-H, S6730S-H, S6730-S, and S6730S-S.

If you run the **if-match outbound-interface** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the outbound interface of GE0/0/1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match outbound-interface gigabitethernet 0/0/1
```

15.1.26 if-match protocol

Function

The **if-match protocol** command configures a matching rule based on a protocol in a traffic classifier.

The **undo if-match protocol** command deletes a matching rule based on a protocol in a traffic classifier.

By default, a matching rule based on a protocol is not configured in a traffic classifier.

Format

if-match protocol { **ip** | **ipv6** }

undo if-match protocol

Parameters

Parameter	Description	Value
ip	Specifies an IP protocol.	-
ipv6	Specifies an IPv6 protocol.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match protocol** command to classify packets based on a protocol so that the device processes packets of the same protocol in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

Currently, the device supports IPv4 and IPv6.

If you run the **if-match protocol** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

If the relationship between rules in a traffic classifier is AND, and both the **if-match protocol** and **if-match l2-protocol arp** commands are configured in this traffic classifier, of the two, only the **if-match l2-protocol arp** command takes effect.

Example

Configure a matching rule based on the IP protocol in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match protocol ip
```

15.1.27 if-match source-mac

Function

The **if-match source-mac** command configures a matching rule based on the source MAC address in a traffic classifier.

The **undo if-match source-mac** command deletes a matching rule based on the source MAC address in a traffic classifier.

By default, a matching rule based on the source MAC address is not configured in a traffic classifier.

Format

if-match source-mac *mac-address* [*mac-address-mask*]

undo if-match source-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
mac-address-mask	Specifies the mask of the source MAC address. Similar to the mask of the IP address, the mask of the MAC address determines a group of MAC addresses. The device can accurately match certain bits in the source MAC address using the mask of the MAC address. In practice, you can set these bits to F in the mask of the source MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be 0-0-0.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match source-mac** command to classify packets based on the source MAC address so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match source-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, and S500, S5735-S-I, S5735S-S, if a traffic policy is applied to the outbound direction and the relationship between rules in a traffic classifier is AND:

- Rules for matching the source IPv6 address and those for matching the destination IPv6 address cannot be configured in the same traffic classifier.
- Rules for matching IPv6 information (for example, **if-match protocol ipv6** and **if-match ipv6 acl**) and those for matching the source MAC address, destination MAC address, source IPv6 address, or destination IPv6 address of packets cannot be configured in the same traffic classifier. (ACL6 rules can be used to match the source or destination IPv6 address of packets.)
- Rules for matching IPv4 information (IP address and UDP port number) and those for matching some Layer 2 information (for example, **if-match source-mac**, **if-match destination-mac**, and **if-match l2-protocol** { **mpls** | **rarp** | *protocol-value* }) cannot be configured in the same traffic classifier.

Example

Configure a matching rule based on the source MAC address of 00e0-fc12-3456 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match source-mac 00e0-fc12-3456
```

Configure a matching rule based on the source MAC address of XXe0-fXX2-3457 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match source-mac 00e0-fc12-3457 00ff-f00f-ffff
```

15.1.28 if-match tcp

Function

The **if-match tcp** command configures a matching rule based on the SYN Flag in the TCP packet header in a traffic classifier.

The **undo if-match tcp** command deletes a matching rule based on the SYN Flag in the TCP packet header in a traffic classifier.

By default, a matching rule based on the SYN Flag in the TCP packet header is not configured in a traffic classifier.

Format

if-match tcp syn-flag { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }

undo if-match tcp syn-flag

Parameters

Parameter	Description	Value
syn-flag	Specifies the SYN Flag in the TCP packet header.	-
syn-flag-value	Specifies the SYN Flag in the TCP packet header.	The value is an integer that ranges from 0 to 63.
ack	Indicates that the SYN Flag type in the TCP packet header is ACK.	-
fin	Indicates that the SYN Flag type in the TCP packet header is FIN.	-
psh	Indicates that the SYN Flag type in the TCP packet header is PSH.	-
rst	Indicates that the SYN Flag type in the TCP packet header is RST.	-
syn	Indicates that the SYN Flag type in the TCP packet header is SYN.	-
urg	Indicates that the SYN Flag type in the TCP packet header is URG.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match tcp** command to classify packets based on the SYN Flag in the TCP packet header so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match tcp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the SYN Flag of psh in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match tcp syn-flag psh
```

15.1.29 if-match vlan-id

Function

The **if-match vlan-id** command configures a matching rule based on the VLAN ID of packets in a traffic classifier.

The **undo if-match vlan-id** command deletes a matching rule based on the VLAN ID of packets in a traffic classifier.

By default, a matching rule based on the VLAN ID of packets is not configured in a traffic classifier.

Format

if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]

undo if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]

NOTE

Only the S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **cvlan-id** *cvlan-id* parameter.

Parameters

Parameter	Description	Value
start-vlan-id [**to** *end-vlan-id*]	Specifies the outer VLAN ID.	• *start-vlan-id* specifies the start outer VLAN ID. The value of *start-vlan-id* is an integer that ranges from 1 to 4094. • *end-vlan-id* specifies the end outer VLAN ID. The value of *end-vlan-id* is an integer that ranges from 1 to 4094. The value of *end-vlan-id* must be larger than the value of *start-vlan-id*. If **to** *end-vlan-id* is not specified, only the VLAN ID specified by *start-vlan-id* is matched.
cvlan-id *cvlan-id*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match vlan-id** command to classify packets based on the VLAN ID so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

On the S6720-EI, if a traffic policy contains the traffic classifier defining the **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] **cvlan-id** *cvlan-id* matching rule, IPv6 ACL resources are occupied. To display information about IPv6 ACL resources, run the **display acl resource** command.

Example

Configure a matching rule based on VLAN 2 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match vlan-id 2
```

15.1.30 if-match vxlan

Function

The **if-match vxlan** command configures a matching rule based on inner information of VXLAN packets in a traffic classifier.

The **undo if-match vxlan** command deletes a matching rule based on inner information of VXLAN packets from a traffic classifier.

By default, a matching rule based on inner information of VXLAN packets is not configured in a traffic classifier.

Format

if-match vxlan [**transit**] **vni** *vni-id*

undo if-match vxlan [**transit**] **vni** *vni-id*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command. On a VXLAN-incapable switch, the **transit** parameter must be set so that passerby packets can be transparently transmitted.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support VXLAN.

Parameters

Parameter	Description	Value
transit	Indicates that VXLAN packets on the transmission device are matched. If this parameter is not specified, a traffic policy containing this traffic classifier takes effect only on a VXLAN decapsulation device.	-

Parameter	Description	Value
vni *vni-id*	Specifies the VNI ID for matching VXLAN packets.	The value is an integer that ranges from 1 to 16777215.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VNI is similar to a VLAN ID on a traditional network, and it identifies a VXLAN segment. You can use the **if-match vxlan** command to classify packets based on the inner information of VXLAN packets so that the device processes packets matching the same traffic classifier in the same manner.

Precautions

- A traffic policy containing this traffic classifier cannot be applied in the outbound direction.
- If a traffic classifier contains this matching rule, it supports only traffic behaviors of traffic policing, packet filtering, and traffic statistics.

Example

Configure a matching rule based on VNI 10 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match vxlan transit vni 10
```

15.1.31 remark flow-id

Function

The **remark flow-id** command configures an action of re-marking the flow ID in a traffic behavior.

The **undo remark flow-id** command deletes the configuration.

By default, an action of re-marking the flow ID is not configured in a traffic behavior.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

remark flow-id *flow-id*

undo remark flow-id

Parameters

Parameter	Description	Value
flow-id	Specifies a flow ID.	The value is an integer that ranges from 1 to 15.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a traffic policy is applied to different interfaces or VLANs, to save ACL resources, you can run the **if-match flow-id** command to classify packets based on the flow ID so that the device processes packets matching the same flow ID in the same manner. Before the device classifies packets based on the flow ID, use the **remark flow-id** command to configure an action of re-marking the flow ID in a traffic behavior.

Assume that *M* ACLs are configured on the device to distinguish services, and each ACL contains *N* ACL rules. Traffic classifiers classify packets based on ACL rules, and the traffic policy containing the ACL rules is applied to *X* interfaces. If the actions of re-marking flow IDs and matching rules based on the flow IDs are not configured, applying the traffic policy occupies $M \times N \times X$ ACL resources. If the actions of re-marking flow IDs and matching rules based on flow IDs are configured, applying the traffic policy occupies only $M \times (N + X)$ ACL resources.

Follow-up Procedure

Run the **traffic classifier** command to configure a traffic classifier and run the **if-match flow-id** command in the traffic classifier view to create a matching rule based on the flow ID.

Precautions

It is recommended that the traffic classifier containing **if-match flow-id** and the traffic behavior containing **remark flow-id** be bound to different traffic policies.

The traffic policy containing **remark flow-id** can be only applied to an interface, a VLAN, or the system in the inbound direction.

remark flow-id, **statistic enable**, and **car** cannot be configured in the same traffic behavior.

If you run the **remark flow-id** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

On the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, a traffic policy containing **remark flow-id** does not take effect for MPLS packets.

Example

Configure the device to re-mark the flow ID with 4 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark flow-id 4
```

15.1.32 reset traffic policy statistics

Function

The **reset traffic policy statistics** command clears statistics on packets matching a traffic policy that has been applied to the specified object or each object.

Format

reset traffic policy statistics { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* [*.subinterface-number*] | **vlan** *vlan-id* | **ssid-profile** *ssid-profile-name* } { **inbound** | **outbound** }

reset traffic policy statistic ap-group *ap-group* **outbound**

reset traffic policy statistics policy-name *policy-name*

reset traffic policy statistics all

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support **ssid-profile** *ssid-profile-name* and **ap-group** *ap-group*.

Parameters

Parameter	Description	Value
global	Clears statistics on packets matching a traffic policy in the system.	-
slot *slot-id*	Clears statistics on packets matching a traffic policy on a specified device. *slot-id* specifies the slot ID of the device.	The value range depends on the device configuration.
interface *interface-type interface-number* [*.subinterface-number*]	Clears statistics on packets matching a traffic policy on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* [*.subinterface-number*] specifies the interface or sub-interface number.	-
vlan *vlan-id*	Clears statistics on packets matching a traffic policy in a specified VLAN. *vlan-id* specifies the ID of the VLAN.	The value is an integer that ranges from 1 to 4094.
ssid-profile *ssid-profile-name*	Clears statistics on packets matching a traffic policy in a specified SSID profile. *ssid-profile-name* specifies the name of the SSID profile.	The value must the name of an existing SSID profile.
ap-group *ap-group*	Clears statistics on packets matching a traffic policy in a specified AP group. *ap-group* specifies the name of the AP group .	The value must be the name of an existing AP group.
inbound	Clears traffic statistics in the inbound direction.	-

Parameter	Description	Value
outbound	Clears traffic statistics in the outbound direction.	-
policy-name *policy-name*	Clears statistics on packets matching the specified traffic policy in each object.	The value must be the name of an existing traffic policy.
all	Clears statistics on packets matching a traffic policy in each object, including statistics on packets in the inbound and outbound directions in the system, on each interface, in each VLAN, and in each SSID profile.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before re-collecting statistics on packets matching a traffic policy in the specified object or each object, run the **reset traffic policy statistics** command to clear existing packet statistics. Then run the **display traffic policy statistics** command to view packet statistics.

Precautions

The traffic policies that can be deleted from the device every second are limited. If many traffic policies are applied to the device, it may take a long time to delete the traffic policies.

The cleared traffic statistics cannot be restored. Exercise caution when you use the command.

If no traffic policy is applied, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Error: The Policy is not applied in this view.
```

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Info: Statistic has not been enabled.
```

Example

Clear traffic statistics on GE0/0/1 in the inbound direction to which a traffic policy has been applied.

```
<HUAWEI> reset traffic policy statistics interface gigabitethernet 0/0/1 inbound
```

15.1.33 rule-deny skip-action

Function

The **rule-deny skip-action** command creates an action for making the deny action in an ACL or ACL6 ineffective in a traffic behavior.

The **undo rule-deny skip-action** command cancels the configuration.

By default, no action for making the deny action in an ACL or ACL6 ineffective is created in a traffic behavior.

Format

rule-deny skip-action

undo rule-deny skip-action

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a traffic classifier contains an ACL or ACL6 rule that defines the deny action, traffic matching the deny action is discarded.

To prevent such traffic from being discarded, run the **rule-deny skip-action** command in the traffic behavior view. The switch does not take other actions (except traffic statistics collection) defined in the traffic behavior for traffic matching the deny action.

Precautions

If both the **rule-deny skip-action** and **statistic enable** commands are configured in a traffic behavior, traffic matching the deny action in the ACL or ACL6 is forwarded based on the original forwarding path and statistics on the traffic are collected.

If the **rule-deny skip-action** command is configured in a traffic behavior and **logging** is specified in the ACL or ACL6 rule that defines the deny action, the following situations may occur:

- When the traffic policy is applied to the inbound direction on the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6730-H, S6730S-H, or S6720S-EI, traffic matching the deny action in the ACL or ACL6 rule is forwarded based on the original forwarding path, and IP addresses of packets matching the rule are logged. On the other models, traffic matching the deny action in an ACL or ACL6 is discarded, and IP addresses of packets matching the rule are logged.
- When the traffic policy is applied to the outbound direction, traffic matching the deny action in the ACL or ACL6 is forwarded based on the original forwarding path, but IP addresses of packets matching the rule are not logged.

Example

Create an action for making the deny action in an ACL ineffective in traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule deny ip source 192.168.10.1 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match acl 3000
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] rule-deny skip-action
```

15.1.34 traffic behavior

Function

The **traffic behavior** command creates a traffic behavior and displays the traffic behavior view, or directly displays the view of an existing traffic behavior.

The **undo traffic behavior** command deletes a traffic behavior.

By default, no traffic behavior is created in the system.

Format

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Parameters

Parameter	Description	Value
behavior-name	Specifies the name of a traffic behavior.	The value is a string of 1 to 64 case-sensitive characters, spaces and question marks (?) not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A traffic classifier is used to differentiate services and must be associated with a flow control or resource allocation action such as packet filtering, traffic policing, and re-marking. The actions constitute a traffic behavior. The **traffic behavior** command creates a traffic behavior.

Follow-up Procedure

Configure an action in the traffic behavior view. For example, run the **car (traffic behavior view)** command to configure the traffic policing action.

Precautions

To delete a traffic behavior, unbind the traffic policy containing the traffic behavior from the system, an interface, or a VLAN where the traffic policy is applied and unbind the traffic behavior from the traffic classifier. To modify only actions in a traffic behavior, you do not need to unbind the traffic policy containing the traffic behavior from the system, an interface, or a VLAN.

On the device, a maximum of 256 traffic behaviors can be created and multiple traffic actions can be configured in a traffic behavior.

Example

Create the traffic behavior **b1** and enter the traffic behavior view.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1]
```

15.1.35 traffic classifier

Function

The **traffic classifier** command creates a traffic classifier and displays the traffic classifier view, or directly displays the view of an existing traffic classifier.

The **undo traffic classifier** command deletes a traffic classifier.

By default, no traffic classifier is created in the system.

Format

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

Parameters

Parameter	Description	Value
classifier-name	Specifies the name of a user-defined traffic classifier.	The value is a string of 1 to 64 case-sensitive characters, spaces and question marks (?) not supported. When double quotation marks are used around the string, spaces are allowed in the string.
operator	Specifies the relationship between rules in a traffic classifier. If this parameter is not specified, the relationship between rules is OR by default.	-

Parameter	Description	Value
and	Indicates that the relationship between rules is AND. After this parameter is specified, the following situations occur: - If a traffic classifier contains ACL rules, packets match the traffic classifier only when the packets match one ACL rule and all the non-ACL rules. - If a traffic classifier does not contain ACL rules, packets match the traffic classifier only when the packets match all the non-ACL rules.	-
or	Indicates that the relationship between rules is OR. After this parameter is specified, packets match a traffic classifier if the packets match one or more rules.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A traffic classifier classifies traffic of a certain type using matching rules. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior (see **traffic behavior**) to a traffic policy and apply the traffic policy.

A traffic classifier can be created based on Layer 2 information such as the 802.1p priority in the VLAN ID, 802.1p priority in the C-VLAN ID, VLAN ID, C-VLAN ID, or

Layer 2 protocol type, and Layer 3 information such as the DSCP priority or IP priority, or ACLs.

Follow-up Procedure

Define rules in the traffic classifier. For example, run the **if-match 8021p** command to define rules based on the 802.1p priority in the VLAN tag.

Precautions

To delete a traffic classifier, unbind the traffic policy containing the traffic classifier from the system, an interface, or a VLAN where the traffic policy is applied and unbind the traffic classifier from the traffic behavior.

A maximum of 512 traffic classifiers can be created on the device.

After the relationship between rules in a traffic classifier is changed, the system checks whether rules conflict. When the relationship between rules is changed from OR to AND and multiple rules are configured, for example, matching rules based on the 802.1p priority in the inner VLAN tag, DSCP priority, IP precedence, and VLAN ID, the rules may conflict and the traffic policy cannot take effect. If the relationship between rules is changed from AND to OR, the traffic policy still takes effect but services may be affected because more packets are matched. Exercise caution when you change the relationship between rules.

Example

Create a traffic classifier **c1** and enter the traffic classifier view.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1]
```

15.1.36 traffic policy

Function

The **traffic policy** command creates a traffic policy and specifies the matching order of traffic classifiers in the traffic policy.

The **undo traffic policy** command deletes a traffic policy.

By default, no traffic policy is created in the system.

Format

traffic policy *policy-name* [**match-order** { **auto** | **config** }] [**atomic**]

undo traffic policy *policy-name*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **match-order** { **auto** | **config** }.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value is a string of 1 to 64 case-sensitive characters, spaces and question marks (?) not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be f, fa, fas, fast, fast-, fast-m, fast-mo, fast-mod, or fast-mode.
match-order	Specifies the matching order of traffic classifiers in the traffic policy. By default, the matching order of traffic classifiers in a traffic policy is **config**.	-

Parameter	Description	Value
auto	Indicates that the matching order depends on priorities of traffic classifier types. For the S6735-S, S6720-EI and S6720S-EI: If a traffic policy is applied to the inbound direction, traffic classifiers based on the following information are matched in descending order of priority: Layer 2 and IPv4 Layer 3 information > advanced ACL6 > basic ACL6 > IPv4 Layer 3 information > Layer 2 information > user-defined ACL information. For other models: Traffic classifiers based on the following information are in descending order of priority: Layer 2 and IPv4 Layer 3 information > advanced ACL6 > basic ACL6 > Layer 2 information > IPv4 Layer 3 information > user-defined ACL information. If this parameter is specified, fewer ACL resources are consumed.	-
config	Indicates that the matching order depends on the sequence in which traffic classifiers were bound to traffic behaviors. If this parameter is specified, more ACL resources are consumed.	-

Parameter	Description	Value
atomic	Indicates the atomic attribute of a traffic policy. After this parameter is specified, if a traffic policy references an ACL and the ACL is applied to a specified object, dynamically updating the ACL does not interrupt services.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are obtained based on Layer 2 information, Layer 3 information, or ACLs. To implement differentiated services for service flows of packets, bind a traffic classifier and a traffic behavior to the created traffic policy and apply the traffic policy. You can use the **traffic policy** command to create a traffic policy. A maximum of 256 traffic policies can be created on the device.

Pre-configuration Tasks

A traffic classifier and a traffic behavior have been created.

Follow-up Procedure

- Run the **classifier behavior** command in the traffic policy view to associate the traffic policy with a traffic classifier and a traffic behavior.
- Run the **traffic-policy global**, **traffic-policy (interface view)**, **traffic-policy (VLAN view)**, or **traffic-policy (VLANIF interface view)** command to apply the traffic policy to the system, an interface, or a VLAN for the created traffic policy to take effect.

Precautions

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, no matter whether the traffic policy defines the **auto** or **config** matching order, traffic classifiers bound to the traffic policy always take effect in the **config** matching order.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, and S6720S-EI, when the traffic policy that defines the **config** matching order is applied to the inbound direction, traffic classifiers bound to the traffic policy take effect in the **config** matching order. When the traffic policy is applied to the outbound direction, even if the matching order is **config**, traffic classifiers bound to the traffic policy still take effect in the **auto** matching order.

For the S6735-S, S6720-EI and S6720S-EI, when any of the following actions is defined in a traffic action of a traffic policy, even if the matching order is **config**, traffic classifiers bound to the traffic policy still take effect in the **auto** matching order:

- **mac-address learning disable**
- **remark 8021p**
- **remark cvlan-id**
- **remark flow-id**

For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I, when any of the following actions is defined in a traffic behavior of a traffic policy, even if the matching order is **config**, traffic classifiers bound to the traffic policy still take effect in the **auto** matching order:

- **remark 8021p**
- **remark flow-id**
- **remark cvlan-id**
- **remark vlan-id**
- **redirect ip-nexthop**

You cannot directly modify the atomic attribute of a created traffic policy. To modify the atomic attribute, delete the traffic policy, and then recreate the traffic policy with the atomic attribute being specified or deleted.

The atomic attribute is valid for the traffic policy only containing the **permit** or **deny** action. If the traffic policy in which the atomic attribute is specified contains other actions in addition to **permit** or **deny**, applying the traffic policy will cause a failure to deliver the configuration.

For the traffic policy with specified atomic attribute, when the ACL configuration is being updated dynamically, ensure that the device has sufficient ACL resources. Otherwise, the updated ACL configuration will fail to be delivered.

If the atomic attribute is specified for a traffic policy and the device is downgraded from the current version to a version earlier than V200R011C10, the traffic policy configuration cannot be restored during device restart.

If the traffic policy that you want to delete has been applied to the system, an interface, or a VLAN, run the **undo traffic-policy** command to unbind the traffic policy in the corresponding view. Then run the **undo traffic policy** command in the system view to delete the traffic policy. The traffic policy that is not applied can be deleted directly.

When **rule** is configured in the traffic policy and **permit ip** is specified, many ARP Miss packets may be sent to the CPU. As a result, the device is disconnected.

Example

Create a traffic policy **p1**, and associate the traffic classifier **c1** with the traffic behavior **b1** in the traffic policy.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark 8021p 2
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
```

Delete the traffic policy **p1** that has been applied to the inbound indirection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo traffic-policy p1 inbound
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] undo traffic policy p1
```

15.1.37 traffic statistics interval

Function

The **traffic statistics interval** command sets the interval at which the system measures the rates of forwarded and discarded packets in a queue.

The **undo traffic statistics interval** command restores the default interval.

By default, the system measures the rates of forwarded and discarded packets in a queue at intervals of 300s.

Format

traffic statistics interval *time-value*

undo traffic statistics interval [*time-value*]

Parameters

Parameter	Description	Value
time-value	Specifies the interval at which the system measures the rates of forwarded and discarded packets in a queue.	The value is an integer that ranges from 30 to 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device is managed by a network management system (NMS), the MIB module checks the rates of forwarded and discarded packets in each queue at intervals and sends the rates to the NMS. You can view the rates of forwarded and discarded packets in each queue to analyze network performance or locate faults. The MIB module calculates the average rates forwarded and discarded packets during an interval configured by this command.

Example

Set the interval at which the system measures the rates of forwarded and discarded packets in a queue to 100s.

```
<HUAWEI> system-view
[HUAWEI] traffic statistics interval 100
```

15.1.38 traffic statistics mode by-bytes

Function

The **traffic statistics mode by-bytes** command enables byte-based traffic statistics in a traffic policy.

The **undo traffic statistics mode by-bytes** command disables byte-based traffic statistics in a traffic policy.

By default, the byte-based traffic statistics function is not enabled in a traffic policy.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI support this command.

Format

traffic statistics mode by-bytes

undo traffic statistics mode by-bytes

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the traffic statistics function is defined in a traffic policy, the switch collects traffic statistics by packet by default. To collect traffic statistics by byte, run the **traffic statistics mode by-bytes** command. Then the **display traffic policy statistics** command displays the packet rate by byte.

Example

Enable byte-based traffic statistics in a traffic policy.

```
<HUAWEI> system-view
[HUAWEI] traffic statistics mode by-bytes
```

15.1.39 traffic-policy (interface view)

Function

The **traffic-policy** command applies a traffic policy to an interface.

The **undo traffic-policy** command deletes a traffic policy from an interface.

By default, no traffic policy is applied to an interface.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

undo traffic-policy [*policy-name*] { **inbound** | **outbound** }

NOTE

Traffic policies can be applied only to the inbound direction of sub-interfaces on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

NOTE

- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Layer 2 Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Layer 3 Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be f, fa, fas, fast, fast-, fast-m, fast-mo, fast-mod, or fast-mode.
inbound	Applies a traffic policy to the inbound direction.	-
outbound	Applies a traffic policy to the outbound direction.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, MultiGE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, port group view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a created traffic policy to an interface.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

If a traffic classifier in the traffic policy contains **if-match mpls-exp**, the traffic policy cannot be applied to the outbound direction on the S6735-S, S6720-EI and S6720S-EI.

Each direction on an interface can be configured with only one traffic policy. A single traffic policy can be applied to both directions on one or more interfaces.

After a traffic policy is applied to an interface, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

If the traffic policy that you want to delete has been applied to an interface, run the **undo traffic-policy** command to unbind the traffic policy from the interface. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Run the **undo traffic-policy** { **inbound** | **outbound** } command without *policy-name* specified to delete the traffic policy that has been applied to an interface and has the following names: i, in, inb, inbo, inbou, inboun, inbound, o, ou, out, outb, outbo, outbou, outboun, and outbound.

After setting the tunneling protocol of a tunnel interface to GRE, you can apply a traffic policy to the inbound direction of the tunnel interface. For details about how to configure GRE, see GRE Configuration in *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - VPN*.

A traffic policy does not take effect on a Layer 2 VXLAN sub-interface, a Dot1q termination sub-interface, or a sub-interface in BGP AD mode. You are advised to configure a traffic policy that defines a traffic classifier containing a matching rule based on the flow ID on the main interface.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
```

15.1.40 traffic-policy (AP group view)

Function

traffic-policy command applies a traffic policy to an AP group.

undo traffic-policy command deletes a traffic policy from an AP group.

By default, no traffic policy is applied to an AP group.

Format

traffic-policy *policy-name* **outbound**

undo traffic-policy [*policy-name*] **outbound**

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy.
outbound	Applies a traffic policy to the outbound direction of an AP group.	-

Views

AP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a traffic policy to an AP group.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

The traffic policy applied to an AP group takes effect only for downstream broadcast, unknown-unicast, and multicast (BUM) traffic.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the outbound direction in the AP group named test.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-group name test
[HUAWEI-wlan-ap-group-test] traffic-policy p1 outbound
```

15.1.41 traffic-policy (SSID profile view)

Function

traffic-policy command applies a traffic policy to an SSID profile.

undo traffic-policy command deletes a traffic policy from an SSID profile.

By default, no traffic policy is applied to an SSID profile.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

undo traffic-policy [*policy-name*] { **inbound** | **outbound** }

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H, and S6730-H support this command.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction of an SSID profile.	-
outbound	Applies a traffic policy to the outbound direction of an SSID profile.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a traffic policy to an SSID profile.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

Only one traffic policy can be applied to each direction in an SSID profile, but a traffic policy can be applied to different directions in different SSID profiles.

NOTE

After a traffic policy is applied to an SSID profile, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, priority of the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

If the traffic policy that you want to delete has been applied to an SSID profile, run the **undo traffic-policy** command to unbind the traffic policy from the SSID profile. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Run the **undo traffic-policy** { **inbound** | **outbound** } command without *policy-name* specified to delete the traffic policy that has been applied to an SSID profile and has the following names: i, in, inb, inbo, inbou, inboun, inbound, o, ou, out, outb, outbo, outbou, outboun, and outbound.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction in the SSID profile named test.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] traffic-policy p1 inbound
```

15.1.42 traffic-policy (VLAN view)

Function

The **traffic-policy** command applies a traffic policy to a VLAN.

The **undo traffic-policy** command deletes a traffic policy from a VLAN.

By default, no traffic policy is applied to a VLAN.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

undo traffic-policy [*policy-name*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction of a VLAN.	-
outbound	Applies a traffic policy to the outbound direction of a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a traffic policy to a VLAN.

Prerequisites

A traffic policy has been created using the **traffic policy** command.

Precautions

After a traffic policy is applied to a VLAN, the traffic policy takes effect for packets received and sent in the VLAN.

If a traffic classifier in the traffic policy contains **if-match mpls-exp**, the traffic policy cannot be applied to the outbound direction on the S6735-S, S6720-EI and S6720S-EI.

If a traffic policy has been applied to a VLAN, you are not allowed to delete the traffic policy or its traffic classifier and traffic behavior.

After a traffic policy is applied to a VLAN, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

To delete the traffic policy that has been applied, run the **undo traffic-policy** command in the corresponding view to unbind the traffic policy and then run the **undo traffic policy** command in the system view to delete the traffic policy.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] vlan 100
[HUAWEI-vlan100] traffic-policy p1 inbound
```

15.1.43 traffic-policy (VLANIF interface view)

Function

The **traffic-policy** command applies a traffic policy to a VLANIF interface.

The **undo traffic-policy** command deletes a traffic policy from a VLANIF interface.

By default, no traffic policy is applied to a VLANIF interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

undo traffic-policy [*policy-name*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction.	-
outbound	Applies a traffic policy to the outbound direction.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a created traffic policy to a VLANIF interface.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

Each direction of a VLANIF interface can be configured with only one traffic policy. A single traffic policy can be applied to both directions on one or more VLANIF interfaces.

A traffic policy cannot be applied to a VLANIF interface corresponding to the super-VLAN or MUX VLAN.

On the S6720-EI, S6735-S, and S6720S-EI, a traffic policy applied to a VLANIF interface takes effect only for unicast packets and Layer 3 multicast packets on the VLANIF interface.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, a traffic policy applied to a VLANIF interface takes effect only for unicast packets on the VLANIF interface.

A traffic policy cannot be applied to the inbound direction of a VLANIF interface when the bound traffic behaviors define the following actions:

- **remark vlan-id**
- **remark cvlan-id**
- **remark 8021p**
- **remark flow-id**
- **mac-address learning disable**

A traffic policy cannot be applied to the outbound direction of a VLANIF interface when the bound traffic behaviors define the following actions:

- **remark flow-id**
- **mac-address learning disable**

After a traffic policy is applied to a VLANIF interface, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

If the traffic policy that you want to delete has been applied to a VLANIF interface, run the **undo traffic-policy** command to unbind the traffic policy from the VLANIF interface. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Run the **undo traffic-policy inbound** command without *policy-name* specified to delete the traffic policy that has been applied to a VLANIF interface and has the following names: i, in, inb, inbo, inbou, inboun, and inbound.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] traffic-policy p1 inbound
[HUAWEI-Vlanif100] quit
```

15.1.44 traffic-policy fast-mode enable

Function

The **traffic-policy fast-mode enable** command enables fast delivery of ACL rules.

The **undo traffic-policy fast-mode enable** command disables fast delivery of ACL rules.

By default, fast delivery of ACL rules is disabled.

Format

traffic-policy fast-mode enable

undo traffic-policy fast-mode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many ACL rules are applied in the system view, and then some of them are applied in the interface view, it takes a long time to deliver ACL rules. As a result, the ACL rules are slow to take effect, and the CPU usage is high. To speed up ACL delivery, run the **traffic-policy fast-mode enable** command.

Precautions

After the **traffic-policy fast-mode enable** command is run:

- ACL rules in effect may be invalid temporarily.
- The statistics on traffic policies are cleared.
- The device performance deteriorates.

Example

Enable fast delivery of ACL rules.

```
<HUAWEI> system-view
[HUAWEI] traffic-policy fast-mode enable
```

15.1.45 traffic-policy global

Function

The **traffic-policy global** command applies a traffic policy to the system.

The **undo traffic-policy global** command deletes a traffic policy that is applied to the system.

By default, no traffic policy is applied to the system.

Format

traffic-policy *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]

undo traffic-policy [*policy-name*] **global** { **inbound** | **outbound** } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction.	-
outbound	Applies a traffic policy to the outbound direction.	-

Parameter	Description	Value
slot *slot-id*	On a stacked device, if *slot-id* is not specified, the traffic policy can be applied to all devices in the stack.	The value is fixed at 0 on a non-stacked device, and specifies the stack ID on a stacked device. **NOTE** If the value of *slot-id* is specified in the **undo traffic-policy** command, it must be the same as the ID of the specified slot to which the traffic policy is applied.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy.

You can use the **traffic policy global** command to apply a traffic policy to the system.

Prerequisites

A traffic policy has been created using the **traffic policy** command.

Precautions

If a traffic policy has been applied, you cannot directly change the traffic policy or its traffic classifier and traffic behavior.

If a traffic classifier in the traffic policy contains **if-match mpls-exp**, the traffic policy cannot be applied to the outbound direction on the S6735-S, S6720-EI and S6720S-EI.

After a traffic policy is applied, you cannot directly delete the traffic policy or the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

Run the **undo traffic-policy global** { **inbound** | **outbound** } command without *policy-name* specified to delete the traffic policy that has been applied to an interface and has the following names: g, gl, glo, glob, globa, and global.

The traffic policy that has the following names cannot be applied to the system: f, fa, fas, fast, fast-, fast-m, fast-mo, fast-mod, and fast-mode.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] traffic-policy p1 global inbound
```

15.1.46 traffic rate statistics enable

Function

The **traffic rate statistics enable** command enables traffic rate statistics collection in a traffic policy.

The **undo traffic rate statistics enable** command disables traffic rate statistics collection in a traffic policy.

By default, traffic rate statistics collection is enabled in a traffic policy.

Format

traffic rate statistics enable

undo traffic rate statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the traffic statistics function is configured in a traffic policy and more than 60K traffic classification rules are configured, memory resources may be insufficient. To release memory resources, run the **undo traffic rate statistics enable** command to disable traffic rate statistics collection in the traffic policy.

Precautions

After traffic rate statistics collection is disabled in a traffic policy, the **display traffic policy statistics** command can still display the number of packets and bytes, but traffic rates are all displayed as -.

This command is valid for traffic policies configured after traffic rate statistics collection is enabled or disabled, and traffic rate statistics collection is not disabled in traffic policies that have been configured before this command is executed.

Before you disable traffic rate statistics collection in a traffic policy, traffic statistics are displayed as follows:

```
<HUAWEI> display traffic policy statistics global slot 0 inbound
 Global :
 Traffic policy inbound: test
 Rule number: 0
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Board : 0
---------------------------------------------------------------------
 Matched          |      Packets:                            0
                  |      Bytes:                          0
                  |      Rate(pps):                        0
                  |      Rate(bps):                        0
---------------------------------------------------------------------
   Passed         |      Packets:                          0
                  |      Bytes:                          0
                  |      Rate(pps):                        0
                  |      Rate(bps):                        0
---------------------------------------------------------------------
   Dropped        |      Packets:                          0
                  |      Bytes:                          0
                  |      Rate(pps):                        0
                  |      Rate(bps):                        0
---------------------------------------------------------------------
     Filter       |      Packets:                        0
                  |      Bytes:                          0
---------------------------------------------------------------------
     Car          |      Packets:                        0
                  |      Bytes:                          0
---------------------------------------------------------------------
```

After you disable traffic rate statistics collection in a traffic policy, traffic statistics are displayed as follows:

```
<HUAWEI> display traffic policy statistics global slot 0 inbound
 Global :
 Traffic policy inbound: testp
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Board : 0
---------------------------------------------------------------------
 Matched          |      Packets:                            0
                  |      Bytes:                          0
                  |      Rate(pps):                        -
                  |      Rate(bps):                        -
---------------------------------------------------------------------
   Passed         |      Packets:                          0
                  |      Bytes:                          0
                  |      Rate(pps):                        -
                  |      Rate(bps):                        -
---------------------------------------------------------------------
```

```
 Dropped        |      Packets:                          0
              |      Bytes:                          0
              |      Rate(pps):                          -
              |      Rate(bps):                          -
-------------------------------------------------------------------
    Filter      |      Packets:                          0
              |      Bytes:                          0
-------------------------------------------------------------------
    Car         |      Packets:                          0
              |      Bytes:                          0
-------------------------------------------------------------------
```

Example

Disable traffic rate statistics collection in a traffic policy.

```
<HUAWEI> system-view
[HUAWEI] undo traffic rate statistics enable
```

15.2 Priority Mapping Commands

15.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.2.2 8021p-inbound

Function

The **8021p-inbound** command maps the 802.1p priority of incoming VLAN packets in a DiffServ domain to the PHB and colors the packets.

The **undo 8021p-inbound** command restores the default mapping.

Table 15-11 lists the default mappings from the 802.1p priorities to PHBs and colors of incoming VLAN packets in a DiffServ domain.

Table 15-11 Mappings from 802.1p priorities to PHBs and colors of incoming packets in the DiffServ domain

802.1p Priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green

802.1p Priority	PHB	Color
6	CS6	green
7	CS7	green

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S:

8021p-inbound *8021p-value* **phb** *service-class* [**green** | **yellow** | **red**]

undo 8021p-inbound [*8021p-value*]

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S:

8021p-inbound *8021p-value* **phb** *service-class*

undo 8021p-inbound [*8021p-value*]

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
phb *service-class*	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates that packets are colored green.	-
yellow	Indicates that packets are colored yellow.	-
red	Indicates that packets are colored red.	-

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

To implement QoS scheduling on incoming VLAN packets, you can use the **8021p-inbound** command to map the 802.1p priorities of the packets to the PHBs and colors. After a DiffServ domain is bound to the inbound interface of packets, the device forwards the packets to queues based on PHBs of the packets. Congestion management is implemented. Packets are scheduled according to their colors after a discard template is configured, avoiding congestion.

Precautions

- The color is used to determine whether packets are discarded during flow control, and is independent of the mapping from internal priorities to queues.
- The CoS values of packets are mapped to the corresponding internal priorities and the packets are colored accordingly. If no mapping from 802.1p priorities to CoS values is specified, the device uses the default mappings of the system.
- If you do not specify the parameter *8021p-value* when running the **undo 8021p-inbound** command, all the mapping between 802.1p priorities and CoS values is restored.
- The DiffServ domain **default** exists by default. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, only the DiffServ domain **default** is supported.

Example

For devices excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In DiffServ domain **ds1**, map the 802.1p priority 2 of the incoming VLAN packets to PHB AF1 and mark the packets yellow.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] 8021p-inbound 2 phb af1 yellow
```

For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In the default DiffServ domain, map the 802.1p priority 2 of the incoming VLAN packets to PHB AF1.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain default
[HUAWEI-dsdomain-default] 8021p-inbound 2 phb af1
```

15.2.3 8021p-outbound

Function

The **8021p-outbound** command maps the PHB and color of outgoing VLAN packets in a DiffServ domain to the 802.1p priority.

The **undo 8021p-outbound** command restores the default mapping.

Table 15-12 lists the default mappings from the PHBs and colors to 802.1p priorities of outgoing VLAN packets in a DiffServ domain.

Table 15-12 Mappings from PHBs and colors to 802.1p priorities of outgoing VLAN packets in the DiffServ domain

PHB	Color	802.1p Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6

PHB	Color	802.1p Priority
CS7	green	7
CS7	yellow	7
CS7	red	7

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S:

8021p-outbound *service-class* { **green** | **yellow** | **red** } **map** *8021p-value*

undo 8021p-outbound [*service-class* { **green** | **yellow** | **red** }]

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S:

8021p-outbound *service-class* **map** *8021p-value*

undo 8021p-outbound [*service-class*]

Parameters

Parameter	Description	Value
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates green packets.	-
yellow	Indicates yellow packets.	-
red	Indicates red packets.	-
map *8021p-value*	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

After QoS scheduling is performed on VLAN packets, you can use the **8021p-outbound** command to map the PHB and color of the packets in a DiffServ domain to the 802.1p priority. After the DiffServ domain is bound to the outbound interface of the VLAN packets, the downstream device implements QoS scheduling according to the 802.1p priority.

Precautions

If you do not specify the parameters *service-class* and *color* when running the **undo 8021p-outbound** command, the default mappings from CoS values and colors to 802.1p priorities are restored.

The DiffServ domain **default** exists by default. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, only the DiffServ domain **default** is supported.

Example

For devices excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In DiffServ domain **ds1**, map PHB AF1 of the outgoing yellow VLAN packets to 802.1p priority 2.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] 8021p-outbound af1 yellow map 2
```

For devices excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In the default DiffServ domain, map PHB AF1 of the outgoing VLAN packets to 802.1p priority 2.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain default
[HUAWEI-dsdomain-default] 8021p-outbound af1 map 2
```

15.2.4 dei enable

Function

The **dei enable** command maps the drop eligible indicator (DEI) field in a VLAN tag to the drop priority.

The **undo dei enable** command cancels the configuration of the DEI field in a VLAN tag as the drop priority.

By default, the DEI field in a VLAN tag is not used as the drop priority.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

dei enable

undo dei enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Eth-Trunk member interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The DEI is also called the Canonical Format Indicator (CFI) field in a VLAN tag and its value is 0 or 1. The DEI field in a VLAN tag is used as the drop priority of packets in certain situations. When the rate of packets on certain devices exceeds the CIR value, the DEI field is set to 1. In this case, the drop priority of the packets is high. When congestion occurs, subsequent devices first discard the packets whose DEI field is 1.

Precautions

After the **dei enable** command is run, the DEI field in the VLAN tag is mapped to the drop priority:

- The DEI field in the VLAN tag is mapped to the drop priority (packet color) on the inbound interface as follows:
  - When the DEI field is 0, packets are colored green.
  - When the DEI field is 1, packets are colored yellow.
- The drop priority is mapped to the DEI field on the outbound interface as follows:
  - Green and yellow packets correspond to DEI 0.
  - Red packets correspond to DEI 1.

The **dei enable** command cannot be configured on both an Eth-Trunk and its member interfaces.

To configure the DEI field in a VLAN tag as the drop priority on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

Configure the DEI field in the VLAN tag as the drop priority on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dei enable
```

15.2.5 diffserv domain

Function

The **diffserv domain** command creates a DiffServ domain and displays the DiffServ domain view, or displays an existing DiffServ domain view.

The **undo diffserv domain** command deletes a specified DiffServ domain.

By default, the system defines a DiffServ mode named **default**.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

diffserv domain { **default** | *ds-domain-name* }

undo diffserv domain *ds-domain-name*

Parameters

Parameter	Description	Value
default	Indicates the default DiffServ domain preset in the system.	-

Parameter	Description	Value
ds-domain-name	Specifies the name of a DiffServ domain.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be n, no, non, or none. **NOTE** The value cannot be --. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the *ds-domain-name* parameter cannot be specified.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

A DiffServ domain defines the mapping between the packet priority and PHB/colors packets for managing and avoiding congestion. You can run the **display diffserv domain** command to view the mappings and packet colors defined in the DiffServ domain.

A DiffServ domain defines the mapping between the PHBs/colors and packet priorities (802.1p and DSCP). When binding a DiffServ domain to an interface, you can run the **trust** command to configure 802.1p or DSCP priority mapping on the interface.

Precautions

The DiffServ domain **default** exists by default. In addition to this domain, the device allows a maximum of 7 DiffServ domains. (On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, only the DiffServ domain **default** is supported.) You can only change the mapping for the DiffServ domain **default**, but cannot delete the domain.

Example

Create DiffServ domain **d1** and display the corresponding DiffServ domain view.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain d1
[HUAWEI-dsdomain-d1]
```

15.2.6 display diffserv domain

Function

The **display diffserv domain** command displays the DiffServ domain configuration.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S:

display diffserv domain [**all** | **name** *ds-domain-name*]

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S:

display diffserv domain name default

Parameters

Parameter	Description	Value
all	Displays configurations of all DiffServ domains.	-
name *ds-domain-name*	Displays the detailed configuration of a specified DiffServ domain.	The value must the name of an existing DiffServ domain. **NOTE** The DiffServ domain **default** exists by default. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, only the DiffServ domain **default** is supported.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Scenario

After creating a DiffServ domain and configuring the mappings in the DiffServ domain, you can use the **display diffserv domain** command to view the configuration of the DiffServ domain.

If no optional parameter is specified, this command displays configurations of all DiffServ domains on the device.

Example

Display the configuration of DiffServ domain **d1** (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S).

```
<HUAWEI> display diffserv domain name d1
diffserv domain name:d1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb ef green
 8021p-inbound 6 phb cs6 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 8021p-outbound be yellow map 0
 8021p-outbound be red map 0
 8021p-outbound af1 green map 1
 8021p-outbound af1 yellow map 1
 8021p-outbound af1 red map 1
 8021p-outbound af2 green map 2
 8021p-outbound af2 yellow map 2
 8021p-outbound af2 red map 2
 8021p-outbound af3 green map 3
 8021p-outbound af3 yellow map 3
 8021p-outbound af3 red map 3
 8021p-outbound af4 green map 4
 8021p-outbound af4 yellow map 4
 8021p-outbound af4 red map 4
 8021p-outbound ef green map 5
 8021p-outbound ef yellow map 5
 8021p-outbound ef red map 5
 8021p-outbound cs6 green map 6
 8021p-outbound cs6 yellow map 6
 8021p-outbound cs6 red map 6
 8021p-outbound cs7 green map 7
 8021p-outbound cs7 yellow map 7
 8021p-outbound cs7 red map 7
 ip-dscp-inbound 0 phb be green
 ip-dscp-inbound 1 phb be green
 ip-dscp-inbound 2 phb be green
 ip-dscp-inbound 3 phb be green
 ip-dscp-inbound 4 phb be green
 ip-dscp-inbound 5 phb be green
```

```
ip-dscp-inbound 6 phb be green
ip-dscp-inbound 7 phb be green
ip-dscp-inbound 8 phb af1 green
ip-dscp-inbound 9 phb be green
ip-dscp-inbound 10 phb af1 green
ip-dscp-inbound 11 phb be green
ip-dscp-inbound 12 phb af1 yellow
ip-dscp-inbound 13 phb be green
ip-dscp-inbound 14 phb af1 red
ip-dscp-inbound 15 phb be green
ip-dscp-inbound 16 phb af2 green
ip-dscp-inbound 17 phb be green
ip-dscp-inbound 18 phb af2 green
ip-dscp-inbound 19 phb be green
ip-dscp-inbound 20 phb af2 yellow
ip-dscp-inbound 21 phb be green
ip-dscp-inbound 22 phb af2 red
ip-dscp-inbound 23 phb be green
ip-dscp-inbound 24 phb af3 green
ip-dscp-inbound 25 phb be green
ip-dscp-inbound 26 phb af3 green
ip-dscp-inbound 27 phb be green
ip-dscp-inbound 28 phb af3 yellow
ip-dscp-inbound 29 phb be green
ip-dscp-inbound 30 phb af3 red
ip-dscp-inbound 31 phb be green
ip-dscp-inbound 32 phb af4 green
ip-dscp-inbound 33 phb be green
ip-dscp-inbound 34 phb af4 green
ip-dscp-inbound 35 phb be green
ip-dscp-inbound 36 phb af4 yellow
ip-dscp-inbound 37 phb be green
ip-dscp-inbound 38 phb af4 red
ip-dscp-inbound 39 phb be green
ip-dscp-inbound 40 phb ef green
ip-dscp-inbound 41 phb be green
ip-dscp-inbound 42 phb be green
ip-dscp-inbound 43 phb be green
ip-dscp-inbound 44 phb be green
ip-dscp-inbound 45 phb be green
ip-dscp-inbound 46 phb ef green
ip-dscp-inbound 47 phb be green
ip-dscp-inbound 48 phb cs6 green
ip-dscp-inbound 49 phb be green
ip-dscp-inbound 50 phb be green
ip-dscp-inbound 51 phb be green
ip-dscp-inbound 52 phb be green
ip-dscp-inbound 53 phb be green
ip-dscp-inbound 54 phb be green
ip-dscp-inbound 55 phb be green
ip-dscp-inbound 56 phb cs7 green
ip-dscp-inbound 57 phb be green
ip-dscp-inbound 58 phb be green
ip-dscp-inbound 59 phb be green
ip-dscp-inbound 60 phb be green
ip-dscp-inbound 61 phb be green
ip-dscp-inbound 62 phb be green
ip-dscp-inbound 63 phb be green
ip-dscp-outbound be green map 0
ip-dscp-outbound be yellow map 0
ip-dscp-outbound be red map 0
ip-dscp-outbound af1 green map 10
ip-dscp-outbound af1 yellow map 12
ip-dscp-outbound af1 red map 14
ip-dscp-outbound af2 green map 18
ip-dscp-outbound af2 yellow map 20
ip-dscp-outbound af2 red map 22
ip-dscp-outbound af3 green map 26
ip-dscp-outbound af3 yellow map 28
```

```
ip-dscp-outbound af3 red map 30
ip-dscp-outbound af4 green map 34
ip-dscp-outbound af4 yellow map 36
ip-dscp-outbound af4 red map 38
ip-dscp-outbound ef green map 46
ip-dscp-outbound ef yellow map 46
ip-dscp-outbound ef red map 46
ip-dscp-outbound cs6 green map 48
ip-dscp-outbound cs6 yellow map 48
ip-dscp-outbound cs6 red map 48
ip-dscp-outbound cs7 green map 56
ip-dscp-outbound cs7 yellow map 56
ip-dscp-outbound cs7 red map 56
mpls-exp-inbound 0 phb be green
mpls-exp-inbound 1 phb af1 green
mpls-exp-inbound 2 phb af2 green
mpls-exp-inbound 3 phb af3 green
mpls-exp-inbound 4 phb af4 green
mpls-exp-inbound 5 phb ef green
mpls-exp-inbound 6 phb cs6 green
mpls-exp-inbound 7 phb cs7 green
mpls-exp-outbound be green map 0
mpls-exp-outbound be yellow map 0
mpls-exp-outbound be red map 0
mpls-exp-outbound af1 green map 1
mpls-exp-outbound af1 yellow map 1
mpls-exp-outbound af1 red map 1
mpls-exp-outbound af2 green map 2
mpls-exp-outbound af2 yellow map 2
mpls-exp-outbound af2 red map 2
mpls-exp-outbound af3 green map 3
mpls-exp-outbound af3 yellow map 3
mpls-exp-outbound af3 red map 3
mpls-exp-outbound af4 green map 4
mpls-exp-outbound af4 yellow map 4
mpls-exp-outbound af4 red map 4
mpls-exp-outbound ef green map 5
mpls-exp-outbound ef yellow map 5
mpls-exp-outbound ef red map 5
mpls-exp-outbound cs6 green map 6
mpls-exp-outbound cs6 yellow map 6
mpls-exp-outbound cs6 red map 6
mpls-exp-outbound cs7 green map 7
mpls-exp-outbound cs7 yellow map 7
mpls-exp-outbound cs7 red map 7
```

Table 15-13 Description of the **display diffserv domain name d1** command output

Item	Description
diffserv domain name	Name of the DiffServ domain. To create a DiffServ domain, run the **diffserv domain** command.
8021p-inbound	Mapping from the 802.1p priority of incoming VLAN packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **8021p-inbound** command.
8021p-outbound	Mapping from the PHB and color of outgoing VLAN packets in a DiffServ domain to the 802.1p priority. To configure the mapping, run the **8021p-outbound** command.

Item	Description
ip-dscp-inbound	Mapping from the DSCP priority of incoming IP packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **ip-dscp-inbound** command.
ip-dscp-outbound	Mapping from the PHB and color of outgoing IP packets in a DiffServ domain to the DSCP priority. To configure the mapping, run the **ip-dscp-outbound** command.
mpls-exp-inbound	Mapping from the EXP priority of incoming MPLS packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **mpls-exp-inbound** command.
mpls-exp-outbound	Mapping from the PHB and color of outgoing MPLS packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **mpls-exp-outbound** command.

Display configurations of all DiffServ domains on the device.

```
<HUAWEI> display diffserv domain
  index      DS name
 --------------------------------------
    0        default
    1        ds1
    2        ds2
 --------------------------------------
 Total 8, Used 3
```

Table 15-14 Description of the **display diffserv domain** command output

Item	Description
index	Index of the DiffServ domain.
DS name	Name of the DiffServ domain. To create a DiffServ domain, run the **diffserv domain** command.
Total	Total number of DiffServ domains supported by the device.
Used	Number of created DiffServ domains on the device.

15.2.7 display qos local-precedence-queue-map

Function

The **display qos local-precedence-queue-map** command displays the mapping between local precedences and queues.

Format

display qos local-precedence-queue-map

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **qos local-precedence-queue-map** command, you can configure the mapping between local precedences and queues. Then you can run the **display qos local-precedence-queue-map** command to display the configuration.

Example

Display the mapping between local precedences and queues.

```
<HUAWEI> system-view
[HUAWEI] qos local-precedence-queue-map af3 2
[HUAWEI] display qos local-precedence-queue-map
 Current configurations of mapping between local-precedence and queue:
  local-precedence value: be     queue index: 0
  local-precedence value: af1    queue index: 1
  local-precedence value: af2    queue index: 2
  local-precedence value: af3    queue index: 2
  local-precedence value: af4    queue index: 4
  local-precedence value: ef     queue index: 5
  local-precedence value: cs6    queue index: 6
  local-precedence value: cs7    queue index: 7
```

Table 15-15 Description of the **display qos local-precedence-queue-map** command output

Item	Description
local-precedence value	Local priority.
queue index	Queue index mapping the local precedence. To configure the mapping between local precedences and queues, run the **qos local-precedence-queue-map** command.

15.2.8 display qos map-table

Function

The **display qos map-table** command displays the mapping between priorities.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and, S6720S-S support this command.

Format

display qos map-table [**dscp-dot1p** | **dscp-dp** | **dscp-dscp**]

Parameters

Parameter	Description	Value
dscp-dot1p	Specifies the name of the mapping table. That is, the mapping from DSCP priorities to 802.1p priorities.	-
dscp-dp	Specifies the name of the mapping table. That is, the mapping between the DSCP priority and the drop precedence is displayed.	-
dscp-dscp	Specifies the name of the mapping table. That is, the mapping between DSCP priorities.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before and after configuring the mapping between priorities, you can use the **display qos map-table** command to check whether the priority mapping is correct.

Example

Display the mapping between the current DSCP priorities and Dot1p priorities.

```
<HUAWEI> display qos map-table dscp-dot1p
Input DSCP       Dot1P
------------------------
0               0
1               0
2               0
3               0
4               0
5               0
6               0
7               0
......
```

Display all the mappings between the current priorities.

```
<HUAWEI> display qos map-table
Input DSCP       Dot1P   DP      DSCP
----------------------------------------
0               0       0       0
1               0       0       1
2               0       0       2
3               0       0       3
4               0       0       4
5               0       0       5
6               0       0       6
7               0       0       7
......
```

Table 15-16 Description of the **display qos map-table** command output

Item	Description
Input DSCP	Input DSCP priority. The value is an integer that ranges from 0 to 63. To set the input DSCP priority, run the **input (DSCP mapping table view)** command.
Dot1P	Output 802.1p priority. The value is an integer that ranges from 0 to 7. To set the output 802.1p priority, run the **input (DSCP mapping table view)** command.
DP	Output drop priority that corresponds to a color. The value is 0, 1, or 2. ● 0: green ● 1: yellow ● 2: red To set the output drop priority, run the **input (DSCP mapping table view)** command.
DSCP	Output DSCP priority. The value is an integer that ranges from 0 to 63. To set the output DSCP priority, run the **input (DSCP mapping table view)** command.

NOTE

A larger value indicates a higher priority.

15.2.9 input (DSCP mapping table view)

Function

The **input** command sets the mapping in a DSCP mapping table.

The **undo input** command restores the default mapping in a DSCP mapping table.

Table 15-17 lists the default mapping from DSCP priorities to 802.1p priorities and from DSCP priorities to drop priorities. The default mapping from DSCP priorities to DSCP priorities remains unchanged.

Table 15-17 Default mapping from DSCP priorities to 802.1p priorities and from DSCP priorities to drop priorities

Input DSCP	Output Dot1p	Output DP
0-7	0	0
8-15	1	0
16-23	2	0
24-31	3	0
32-39	4	0
40-47	5	0
48-55	6	0
56-63	7	0

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and, S6720S-S support this command.

Format

input { *input-value1* [**to** *input-value2*] } &<1-10> **output** *output-value*

undo input { **all** | { *input-value1* [**to** *input-value2*] } &<1-10> }

Parameters

Parameter	Description	Value
input-value1	Specifies the start DSCP priority that is entered.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *input-value2*	Specifies the end DSCP priority that is entered.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority. The value of *input-value2* must be greater than the value of *input-value1* and the two values determine the DSCP range.
output *output-value*	Specifies the output 802.1p priority, output drop precedence, or output DSCP value.	The current mapping table view determines the value of **output-value**. The value ranges are as follows: The value ranges from 0 to 7 in the dscp-dot1p view. The value ranges from 0 to 2 in the dscp-dp view. ● The drop priority 0 corresponds to green packets. ● The drop priority 1 corresponds to yellow packets. ● The drop priority 2 corresponds to red packets. The value ranges from 0 to 63 in the dscp-dscp view. A larger value indicates a higher priority.
all	Indicates all mappings in the DSCP mapping table.	-

Views

DSCP mapping table view

Default Level

2: Configuration level

Usage Guidelines

You must run the **qos map-table** command to enter the corresponding DSCP mapping table view before running the **input** command.

The **input** command modifies the mapping from DSCP priorities to Dot1p priorities, from DSCP priorities to drop priorities, and from DSCP priorities to DSCP priorities in the DSCP table.

After running the **input** command, you can run the **display qos map-table** command to view the current DSCP mapping.

Example

Set the mapping in the DSCP mapping table: Level 0 to level 7 in the DSCP mapping table are mapped to level 0 of 802.1p priority.

```
<HUAWEI> system-view
[HUAWEI] qos map-table dscp-dot1p
[HUAWEI-dscp-dot1p] input 0 to 7 output 0
```

15.2.10 ip-dscp-inbound

Function

The **ip-dscp-inbound** command maps the DSCP priority of incoming IP packets in a DiffServ domain to the PHB and colors the packets.

The **undo ip-dscp-inbound** command restores the default mapping.

Table 15-18 lists the default mappings from the DSCP priorities to PHBs and colors of incoming IP packets in a DiffServ domain.

Table 15-18 Mappings from DSCP priorities to PHBs and colors of incoming IP packets in the DiffServ domain

DSCP	PHB	Color	DSCP	PHB	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green

DSCP	PHB	Color	DSCP	PHB	Color
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S:

ip-dscp-inbound *dscp-value* **phb** *service-class* [**green** | **yellow** | **red**]

undo ip-dscp-inbound [*dscp-value*]

S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S:

ip-dscp-inbound *dscp-value* **phb** *service-class*

undo ip-dscp-inbound [*dscp-value*]

Parameters

Parameter	Description	Value
dscp-value	Specifies the DSCP priority of IP packets.	The value is an integer that ranges from 0 to 63.
phb *service-class*	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates that packets are colored green.	-
yellow	Indicates that packets are colored yellow.	-
red	Indicates that packets are colored red.	-

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

To implement QoS scheduling for incoming IP packets carrying DSCP priorities, use the **ip-dscp-inbound** command to configure mappings from DSCP priorities of packets to PHBs and color the packets. After a DiffServ domain is bound to the inbound interface of packets, the device forwards the packets to queues based on PHBs of the packets. Congestion management is implemented. Packets are scheduled according to their colors after a discard template is configured, avoiding congestion.

Precautions

- The color is used to determine whether packets are discarded during flow control, and is independent of the mapping from internal priorities to queues.
- The CoS values of packets are mapped to the corresponding internal priorities and the packets are colored accordingly. If no mapping from DSCP priorities to CoS values is specified, the device uses the default mappings of the system.
- If you do not specify the parameter *dscp-value* when running the **undo ip-dscp-inbound** command, all mappings from DSCP priorities to CoS values is restored.
- The DiffServ domain **default** exists by default. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, only the DiffServ domain **default** is supported.

Example

For devices excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In DiffServ domain **ds1**, map DSCP priority 8 of the incoming IP packets to PHB AF1 and mark the packets yellow.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] ip-dscp-inbound 8 phb af1 yellow
```

For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In the DiffServ domain, map DSCP priority 8 of the incoming IP packets to PHB AF1.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain default
[HUAWEI-dsdomain-default] ip-dscp-inbound 8 phb af1
```

15.2.11 ip-dscp-outbound

Function

The **ip-dscp-outbound** command maps the PHB and color of outgoing IP packets in a DiffServ domain to the DSCP priority.

The **undo ip-dscp-outbound** command restores the default mapping.

Table 15-19 lists the default mappings from the PHBs and colors to DSCP priorities of outgoing IP packets in a DiffServ domain.

Table 15-19 Mappings from PHBs and colors to DSCP priorities of outgoing IP packets in the DiffServ domain

PHB	Color	DSCP
BE	green	0
BE	yellow	0

PHB	Color	DSCP
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

ip-dscp-outbound *service-class* { **green** | **yellow** | **red** } **map** *dscp-value*

undo ip-dscp-outbound [*service-class* { **green** | **yellow** | **red** }]

Parameters

Parameter	Description	Value
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates green packets.	-
yellow	Indicates yellow packets.	-
red	Indicates red packets.	-
map *dscp-value*	Specifies the DSCP priority of IP packets.	The value is an integer that ranges from 0 to 63.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

After QoS scheduling is performed on the IP packets, you can use the **ip-dscp-outbound** command to map the PHB and color of IP packets in a DiffServ domain to the DSCP priority. After the DiffServ domain is bound to the outbound interface of the IP packets, the downstream device implements QoS scheduling according to the DSCP priority.

Precautions

If you do not specify the parameters *service-class* and colors when running the **undo ip-dscp-outbound** command, the default mappings from CoS values and colors to DSCP priorities are restored.

The DiffServ domain **default** exists by default. On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, only the DiffServ domain **default** is supported.

Example

For devices excluding the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In DiffServ domain **ds1**, map PHB AF1 of the outgoing yellow IP packets to DSCP priority 8.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] ip-dscp-outbound af1 yellow map 8
```

For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S: In the DiffServ domain, map PHB AF1 of the outgoing yellow IP packets to DSCP priority 8.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain default
[HUAWEI-dsdomain-default] ip-dscp-outbound af1 yellow map 8
```

15.2.12 port priority

Function

The **port priority** command configures the priority for an interface.

The **undo port priority** command restores the default priority of an interface.

By default, the priority of an interface is 0.

Format

port priority *priority-value*

undo port priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of an interface.	The value is an integer that ranges from 0 to 7. The default value is 0. A larger value indicates a higher priority of an interface.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The 802.1p priority is determined by the 3-bit priority 802.1p field contained in a VLAN tag. The 802.1p priority is used to ensure QoS in the DiffServ model.

If an interface receives untagged packets, the interface priority is added to packets during the internal forwarding.

If an interface is configured to trust the 802.1p priority using the **trust 8021p** command, the interface adds the 802.1p priority to the received untagged packets. The device then searches for the internal priority (represented by a PHB and color) mapping the 802.1p priority and marks packets with the internal priority.

Precautions

- The **port priority** command is invalid if the current interface is a member interface of an Eth-Trunk.
- If you run the **port priority** command multiple times in the same interface view, only the latest configuration takes effect.
- When an interface switches to Layer 3 mode through the **undo portswitch** command, you cannot configure a priority for the Ethernet interface. This Ethernet interface uses priority 0.

Example

Set the priority of GE0/0/1 to 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port priority 1
```

15.2.13 qos local-precedence-queue-map

Function

The **qos local-precedence-queue-map** command configures the default mappings between local precedences and queues.

The **undo qos local-precedence-queue-map** command restores the default mappings between local precedences and queues.

Table 15-20 lists the default mappings between local precedences and queues.

Table 15-20 Mappings between local precedences and queues

Local Precedence	Queue Index
BE	0
AF1	1
AF2	2
AF3	3
AF4	4
EF	5
CS6	6
CS7	7

Format

qos local-precedence-queue-map *local-precedence queue-index*

undo qos local-precedence-queue-map [*local-precedence*]

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support the mapping configuration between local precedences and queues cannot be configured.

Parameters

Parameter	Description	Value
local-precedence	Specifies the name of the local precedence.	The value can be **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The device sends packets to the specified queue according to the mapping between local precedences and queues.

To make traffic across the entire network achieve consistent QoS, ensure that all the stations keep consistent mapping between local precedences and queues.

Precautions

If you run the **qos local-precedence-queue-map** command multiple times in the system view, only the latest configuration takes effect.

Example

Map packets with local precedence AF3 to queue 2.

```
<HUAWEI> system-view
[HUAWEI] qos local-precedence-queue-map af3 2
```

15.2.14 qos map-table

Function

The **qos map-table** command displays the DSCP mapping table view.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S5736-S, and, S6720S-S support this command.

Format

qos map-table { **dscp-dot1p** | **dscp-dp** | **dscp-dscp** }

Parameters

Parameter	Description	Value
dscp-dot1p	Displays the dscp-dot1p view. The dscp-dot1p table contains the mapping between DSCP priorities and 802.1p priorities.	-
dscp-dp	Displays the dscp-dp view. The dscp-dp table contains the mapping between DSCP priorities and drop precedences.	-
dscp-dscp	Displays the dscp-dscp view. The dscp-dscp table contains the mapping between DSCP priorities and DSCP priorities.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before mapping received packets based on the DSCP priority, run the **qos map-table** command to enter the priority mapping table view.

Follow-up Procedure

Run the **input** (DSCP priority mapping table view) command to configure the mapping.

Example

Enter the dscp-dot1p view.

```
<HUAWEI> system-view
[HUAWEI] qos map-table dscp-dot1p
[HUAWEI-dscp-dot1p]
```

15.2.15 qos phb marking dscp enable (interface view)

Function

The **qos phb marking dscp enable** command enables PHB mapping for DSCP priorities in outgoing packets on an interface.

The **undo qos phb marking dscp enable** command disables PHB mapping for DSCP priorities in outgoing packets on an interface.

By default, PHB mapping is enabled for DSCP priorities in outgoing packets on an interface.

NOTE

This command is supported only on the following: S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, S6735-S, S6720-EI, and S6720S-EI.

Format

qos phb marking dscp enable

undo qos phb marking dscp enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **undo qos phb marking dscp enable** command is used on an interface of the edge node of the DiffServ domain, PHB mapping is disabled for DSCP priorities in outgoing packets on the interface connected to the device that does not belong to the DiffServ domain.

Precautions

The **trust upstream none** command disables PHB mapping on an interface. After this command is configured, the system does not perform PHB mapping for incoming and outgoing packets on the interface. Unlike the **trust upstream none** command, after the **undo qos phb marking dscp enable** command is used, the system does not perform PHB mapping for DSCP priorities in outgoing packets on the interface but performs PHB mapping for DSCP priorities in incoming packets on the interface.

The **undo qos phb marking dscp enable** and **trust upstream none** commands cannot be used simultaneously.

After the **undo qos phb marking dscp enable** command is used, DSCP priorities in packets are not mapped. However, 802.1p priorities in packets are still mapped. After the **undo qos phb marking enable** command is used, DSCP and 802.1p priorities in packets are not mapped.

If the **qos phb marking enable** command is configured on an interface and then the **trust dscp** or **qos phb marking dscp enable** command is configured on the interface, PHB mapping is performed for DSCP priorities in outgoing packets on the interface.

Example

Disable PHB mapping for DSCP priorities in outgoing packets on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo qos phb marking dscp enable
```

15.2.16 qos phb marking 8021p enable

Function

The **qos phb marking 8021p enable** command enables PHB mapping for 802.1p priorities in outgoing packets on an interface.

The **undo qos phb marking 8021p enable** command disables PHB mapping for 802.1p priorities in outgoing packets on an interface.

By default, PHB mapping for 802.1p priorities in outgoing packets is disabled on an interface, and outgoing packets are mapped based on the 802.1p priority (default configuration of the **trust** command).

NOTE

This command is supported only on the following: S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, S6735-S, S6720-EI, and S6720S-EI.

Format

qos phb marking 8021p enable

undo qos phb marking 8021p enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Typically, **undo qos phb marking 8021p enable** is configured on the device that functions as the edge node of the DiffServ domain to disable PHB mapping for 802.1p priorities in outgoing packets on an interface. If the downstream device needs to use the 802.1p priorities in packets, you can configure the **qos phb marking 8021p enable** command to perform PHB mapping for 802.1p priorities in outgoing packets on an interface.

Precautions

- The **trust upstream none** command is used to disable PHB mapping on an interface. After this command is configured, the system does not perform PHB mapping for incoming and outgoing packets on the interface.
- If the **undo qos phb marking enable** command is configured, the system does not perform PHB mapping for 802.1p priorities in outgoing packets on an interface.
- The **qos phb marking 8021p enable** command is mutually exclusive with the **trust upstream none** and **undo qos phb marking enable** commands.
- If the **qos phb marking enable** command is configured on an interface and then the **trust 8021p outer** or **qos phb marking 8021p enable** command is configured on the interface, the device performs PHB mapping for 802.1p priorities in outer VLAN tags of outgoing packets on the interface.

Example

Enable PHB mapping for 802.1p priorities in outgoing packets on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos phb marking 8021p enable
```

15.2.17 qos phb marking enable

Function

The **qos phb marking enable** command enables PHB mapping for outgoing packets on an interface.

The **undo qos phb marking enable** command disables PHB mapping for outgoing packets on an interface.

By default, PHB mapping is enabled for outgoing packets on an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

qos phb marking enable

undo qos phb marking enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

After the **undo qos phb marking enable** command is executed on the interface of the edge node in a DiffServ domain, PHB mapping is disabled on the interface connected to a device that does not belong to the DiffServ domain.

Precautions

- The **trust upstream none** command is executed to disable PHB mapping on an interface. After the **trust upstream none** command is executed, the system does not perform PHB mapping for incoming and outgoing packets on the interface. Unlike the **trust upstream none** command, after the **undo qos phb marking enable** command is executed, the system does not perform PHB mapping for outgoing packets on the interface but performs PHB mapping for incoming packets on the interface.
- The **undo qos phb marking enable** and **trust upstream none** commands cannot be executed simultaneously.

Example

Disable PHB mapping for outgoing packets on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo qos phb marking enable
```

15.2.18 remark 8021p

Function

The **remark 8021p** command configures an action of re-marking the 802.1p priority in VLAN packets in a traffic behavior.

The **undo remark 8021p** command deletes the configuration.

By default, no action of re-marking the 802.1p priority in VLAN packets is configured in a traffic behavior.

Format

remark 8021p [*8021p-value* | **inner-8021p**]

NOTE

inner-8021p is supported only on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-S, S5735-S-IS6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

undo remark 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority in VLAN packets. If the value is not specified, the default value 0 is used.
inner-8021p	Inherits the 802.1p priority in the inner tag.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the inner 802.1p priority in VLAN packets, run the **remark 8021p** command to configure the device to re-mark the inner 802.1p priority in VLAN packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing 802.1p priority re-marking.

Precautions

If a traffic policy containing **remark 8021p** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream Layer 2 device processes the packets based on the re-marked priority.

A traffic policy containing **remark 8021p inner-8021p** can be applied only to the inbound direction, except for the following models: S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S. For the S6735-S, S6720-EI, and S6720S-EI, if a traffic policy contains **remark 8021p inner-8021p**, the PRI field (802.1p priority) in single-tagged packets is changed to 0. In this case, you can configure **if-match double-tag** in a traffic classifier to change the 802.1p priority only of double-tagged packets.

If a traffic policy containing **remark 8021p** is applied to the outbound direction on an interface, the VLAN of the interface must work in tag mode.

When a traffic classifier defines **if-match ipv6 acl** { *acl-number* | *acl-name* }, **remark 8021p** [*8021p-value* | **inner-8021p**] cannot be configured on the following models: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

If selective QinQ, VLAN mapping, flow ID re-marking, 802.1p priority re-marking, or MAC address learning disabling is configured in a traffic behavior, the S5731-H, S5731-S, S5731S-H, S6730S-H, and S5731S-S do not support the following actions in the traffic behavior: traffic statistics collection, traffic mirroring, redirection, PBR, DSCP priority re-marking, internal priority re-marking, destination MAC address re-marking, traffic policing, and hierarchical traffic policing; the S5732-H, S6730-H, S6730-S, and S6730S-S do not support the following actions in the traffic behavior: traffic mirroring, redirection, PBR, DSCP priority re-marking, internal priority re-marking, destination MAC address re-marking, traffic policing, and hierarchical traffic policing.

On the S6720-EI, S6735-S, and S6720S-EI, if flow ID re-marking, re-marking of the inner VLAN tag in QinQ packets, MAC address learning disabling, or redirection of packets to a VPN instance is configured in a traffic behavior, the following actions cannot be defined in the traffic behavior: traffic statistics collection, traffic mirroring, redirection, PBR, DSCP priority re-marking, internal priority re-marking, destination MAC address re-marking, traffic policing, and hierarchical traffic policing.

If both the **trust 8021p** command and the traffic policy containing **remark 8021p** are used in the outbound direction on the interface of packets, the 802.1p priority specified by the **trust 8021p** command is the re-marked value. This is because the **remark 8021p** command takes precedence over the **trust 8021p** command.

On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S, if a traffic policy containing **remark 8021p** and a traffic policy containing **remark dscp** are applied to the inbound direction of an interface, and the **trust 8021p** or **trust dscp** command is configured in the outbound direction of the interface, the DSCP and 802.1p values of the packet are the values after re-marking.

The **remark 8021p** command configured on a Layer 3 routed sub-interface or termination sub-interface does not take effect.

The **remark 8021p** and **remark local-precedence** commands cannot be used in the same traffic behavior.

On the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the **remark 8021p** and **remark dscp** commands cannot be used in the same traffic behavior.

If you run the **remark 8021p** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the 802.1p priority of VLAN packets with 4 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark 8021p 4
```

15.2.19 remark 8021p (QoS profile view)

Function

The **remark 8021p** command configures the device to re-mark 802.1p priorities in VLAN packets in a QoS profile.

The **undo remark 8021p** command cancels the configuration.

By default, the device does not re-mark 802.1p priorities in VLAN packets in a QoS profile.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

remark 8021p *8021p-value*

undo remark 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device needs to provide differentiated services based on 802.1p priorities in VLAN packets, run the **remark 8021p** command to configure the device to re-mark 802.1p priorities in VLAN packets in a QoS profile.

Precautions

If you run the **remark 8021p** command in the same QoS profile view multiple times, only the latest configuration takes effect.

Example

Configure the device to re-mark the 802.1p priority in VLAN packets with 4 in the QoS profile **test**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name test
[HUAWEI-qos-test] remark 8021p 4
```

15.2.20 remark dscp

Function

The **remark dscp** command configures an action of re-marking the DSCP priority in IP packets in a traffic behavior.

The **undo remark dscp** command deletes the configuration.

By default, an action of re-marking the DSCP priority in IP packets is not configured in a traffic behavior.

Format

remark dscp { *dscp-name* | *dscp-value* }

undo remark dscp

Parameters

Parameter	Description	Value
dscp-name	Specifies the DSCP priority name in IP packets.	The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.
dscp-value	Specifies the DSCP priority in IP packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the DSCP priority, run the **remark dscp** command to configure the device to re-mark the DSCP priority in IP packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing DSCP priority re-marking.

Precautions

If a traffic policy containing **remark dscp** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream Layer 3 device or above processes the packets based on the re-marked priority.

If the traffic policy containing **remark dscp** and the **trust dscp** command are used in the outbound direction on the interface of packets, the **remark dscp** command changes DSCP priorities in packets because the **remark dscp** command takes precedence over the **trust dscp** command.

On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, and S5735S-S, if a traffic policy containing

remark 8021p and a traffic policy containing **remark dscp** are applied to the inbound direction of an interface, and the **trust 8021p** or **trust dscp** command is configured in the outbound direction of the interface, the DSCP and 802.1p values of the packet are the values after re-marking.

The **remark dscp** and **remark ip-precedence** commands cannot be used in the same traffic behavior.

On the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the **remark 8021p** and **remark dscp** commands cannot be used in the same traffic behavior.

If you run the **remark dscp** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

After the **remark dscp** { *dscp-name* | *dscp-value* } command is configured in the traffic behavior view, the system maps the packet priority to a local priority based on the DSCP priority and sends the packet to a queue based on the mapped priority. If the **remark local-precedence** { *local-precedence-name* | *local-precedence-value* } command is also configured, the system sends packets to queues based on the priority configured using this command.

Example

Re-mark the DSCP priority in IP packets with 56 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark dscp 56
```

15.2.21 remark dscp (QoS profile view)

Function

The **remark dscp** command configures the device to re-mark DSCP priorities in IP packets in a QoS profile.

The **undo remark dscp** command cancels the configuration.

By default, the device does not re-mark DSCP priorities in IP packets in a QoS profile.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

remark dscp *dscp-value* { **inbound** | **outbound** }

undo remark dscp { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
dscp-value	Specifies the DSCP priority in IP packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
inbound	Specifies the DSCP priority in incoming IP packets.	-
outbound	Specifies the DSCP priority in outgoing IP packets.	-

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device needs to provide differentiated services based on DSCP priorities in IP packets, run the **remark dscp** command to configure the device to re-mark DSCP priorities in IP packets in a QoS profile.

Precautions

When the device processes IPv6 packets, or when the device uses the direct forwarding mode to process IPv4 packets, the **remark dscp** command cannot be used to re-mark DSCP priorities in these packets.

When packets match both outbound DSCP priority re-marking and outbound priority mapping that are configured on the device, only outbound priority mapping takes effect.

On the device that uses an earlier version of V200R011C10, the DSCP priority re-marking direction cannot be specified. When the device that uses an earlier version of V200R011C10 is upgraded to V200R011C10, the device re-marks DSCP priorities of incoming packets by default.

If you run the **remark dscp** command in the same QoS profile view multiple times, only the latest configuration takes effect.

Example

Configure the device to re-mark the DSCP priority in incoming IP packets with 56 in the QoS profile **test**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name test
[HUAWEI-qos-test] remark dscp 56 inbound
```

15.2.22 remark ip-precedence

Function

The **remark ip-precedence** command configures an action of re-marking the IP precedence in IP packets in a traffic behavior.

The **undo remark ip-precedence** command deletes the configuration.

By default, an action of re-marking the IP precedence in IP packets is not configured in a traffic behavior.

Format

remark ip-precedence *ip-precedence*

undo remark ip-precedence

Parameters

Parameter	Description	Value
ip-precedence	Specifies the IP precedence.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the downstream device needs to provide differentiated services based on the IP precedence, run the **remark ip precedence** command to configure the device to re-mark the IP precedence in IP packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing IP precedence re-marking.

Precautions

After the re-marking action is configured, the device still processes outgoing packets based on the original priority but the downstream Layer 3 device or above processes the packets based on the re-marked priority.

A traffic policy containing the **remark ip-precedence** action can be only used in the inbound direction.

The **remark dscp** and **remark ip-precedence** commands cannot be used in the same traffic behavior.

If you run the **remark ip-precedence** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the IP precedence in IP packets with 6 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark ip-precedence 6
```

15.2.23 remark local-precedence

Function

The **remark local-precedence** command configures an action of re-marking the internal priority in packets in a traffic behavior.

The **undo remark local-precedence** command deletes the configuration.

By default, an action of re-marking the internal priority in packets is not configured in a traffic behavior.

Format

remark local-precedence { *local-precedence-name* | *local-precedence-value* } [**green** | **yellow** | **red**]

undo remark local-precedence

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **green**, **yellow**, and **red**.

Parameters

Parameter	Description	Value
local-precedence-name	Specifies the internal priority name.	The value can be **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.

Parameter	Description	Value
local-precedence-value	Specifies the internal priority value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
green	Indicates that the green color corresponds to an internal priority.	-
yellow	Indicates that the yellow color corresponds to an internal priority.	-
red	Indicates that the red color corresponds to an internal priority.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the internal priority of packets, run the **remark local-precedence** command to configure the device to re-mark the internal priority of packets so that the device can provide QoS based on the re-marked priority.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing internal priority re-marking.

Precautions

Re-marking the internal priority only affects QoS processing of packets on the device.

The **remark 8021p** and **remark local-precedence** commands cannot be used in the same traffic behavior.

A traffic policy containing the **remark local-precedence** action can be only used in the inbound direction.

If you run the **remark local-precedence** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the internal priority of packets with 2 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark local-precedence 2
```

15.2.24 trust

Function

The **trust** command specifies the priority to be mapped for packets.

The **undo trust** command cancels the configuration.

By default:

- The S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI process packets based on the mapping of the 802.1p priority.
- The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S process packets based on the mapping of the outer 802.1p priority.

Format

trust { **8021p** | **dscp** } (S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI)

undo trust { **8021p** | **dscp** } (S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI)

trust { **8021p** { **inner** | **outer** } | **dscp** } (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S)

undo trust (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Parameters

Parameter	Description	Value
8021p	Maps packets based on the 802.1p priority.	-
inner	Maps packets based on the inner 802.1p priority.	-

Parameter	Description	Value
outer	Maps packets based on the outer 802.1p priority.	-
dscp	Maps packets based on the DSCP priority.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Eth-Trunk member interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device does not trust any packet priority, packets enter queue 0 and 802.1p priorities in the packets are set to 0. Differentiated services cannot be provided. After the **trust** command is used, the device searches for the mapping table based on the priority in packets, re-marks the inner priority in packets, and sends packets to queues.

To set the same priority to be trusted on multiple interfaces, you can perform the configuration on a port group to reduce the workload.

Precautions

By default, the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, and S5720-LI in a version earlier than V200R013C00 do not trust priorities of packets. If the **trust** command is not executed to change the switches to trust 802.1p or DSCP priority of packets, the switches will process packets based on the mapping of the 802.1p priority after they are updated to V200R013C00 and later versions.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI, when the **trust dscp** and **trust 8021p** commands are configured on the same interface:

- The interface trusts DSCP priorities if IPv4 packets are received.
- The interface trusts 802.1p priorities if VLAN packets are received.

If both a traffic policy containing **remark 8021p** or **remark dscp** and the **trust 8021p** or **trust dscp** command are configured in the outbound interface of packets, only the traffic policy containing **remark 8021p** or **remark dscp** takes effect, and the **trust 8021p** or **trust dscp** command does not take effect.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if you run the **trust 8021p inner**, **trust 8021p outer**, and **trust dscp** commands multiple times on the same interface, only the latest configuration takes effect.

The **trust** command cannot be configured on both an Eth-Trunk and its member interfaces.

This command can be delivered in Layer 3 mode.

Example

Configure GE0/0/1 to trust DSCP priorities.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trust dscp
```

15.2.25 trust upstream

Function

The **trust upstream** { **default** | *ds-domain-name* } command applies a DiffServ domain to an interface.

The **trust upstream none** command disables the priority mapping on an interface.

The **undo trust upstream** command restores the default settings.

By default, no DiffServ domain is bound to an interface. The priority mappings on the interface are the same as those of the DiffServ domain **default**.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

trust upstream { **default** | *ds-domain-name* | **none** }

undo trust upstream

Parameters

Parameter	Description	Value
default	Indicates the default DiffServ domain preset in the system.	-
ds-domain-name	Specifies the name of a DiffServ domain applied to an interface.	The value must the name of an existing DiffServ domain.

Parameter	Description	Value
none	Indicates that none DiffServ domain is applied to an interface, and the priorities in packets are not trusted.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Eth-Trunk member interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To map priorities of the packets sent from the upstream device to PHBs according to the mappings defined in a DiffServ domain, run the **trust upstream** command to apply the DiffServ domain to the inbound interface of the packets. The system then maps priorities of packets to PHBs according to the mappings defined in the DiffServ domain.

To map PHBs of the packets sent to the downstream device to priorities according to the mappings defined in a DiffServ domain, run the **trust upstream** command to apply the DiffServ domain to the outbound interface of the packets. The system then maps PHBs of packets to the priorities according to the mappings defined in the DiffServ domain.

Prerequisites

A DiffServ domain has been created.

Precautions

- After the **trust upstream** command is executed on an interface, the system maps the priorities of packets on the interface to the following values according to the mappings defined in the DiffServ domain:
  - PHB
  - Packet color

  For default mappings from 802.1p priorities to PHBs and colors, from PHBs and colors to 802.1p priorities, from EXP priorities to PHBs and colors, from PHBs and colors to EXP priorities, from DSCP priorities to PHBs and colors, and from PHBs and colors to DSCP priorities, see the **8021p-inbound**, **8021p-outbound**, , **mpls-exp-inbound**, **mpls-exp-outbound**, **ip-dscp-inbound**, and **ip-dscp-outbound** commands.

- After the **trust upstream none** command is executed, the system performs no priority mapping on packets passing the interface.
- To change the DiffServ domain bound to an interface, run the **undo trust upstream** command to unbind the original DiffServ domain from the interface, and then run the **trust upstream** command to apply the new DiffServ domain to the interface.
- If you run the **trust upstream** command multiple times in the same interface view, only the latest configuration takes effect.
- The **trust upstream** command cannot be configured on both an Eth-Trunk and its member interfaces.
- To apply a DiffServ domain to multiple interfaces, you can perform the configuration on the port group to reduce the workload.

Example

Apply DiffServ domain **ds1** to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trust upstream ds1
```

15.3 Traffic Policing, Traffic Shaping, and Interface-based Rate Limiting Commands

15.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.3.2 assign car-resource

Function

The **assign car-resource** command configures the CAR resource allocation mode.

The **undo assign car-resource** command restores the default CAR resource allocation mode.

By default, the **enhanced** CAR resource allocation mode is used, where CAR resources are allocated in a contiguous manner.

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I.

Format

assign car-resource { **enhanced** | **normal** } [**slot** *slot-id*]

undo assign car-resource [**slot** *slot-id*]

Parameters

Parameter	Description	Value
enhanced	Sets the CAR resource allocation mode to **enhanced**.	-
normal	Sets the CAR resource allocation mode to **normal**. In this mode, CAR resources are allocated in a non-contiguous manner.	-
slot *slot-id*	● Specifies the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured. If *slot-id* is not specified, the CAR resource allocation mode of all stacked switches is displayed.	The value must be set according to the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the **car (traffic behavior view)** command is used to configure a traffic policing policy, CAR resources are occupied. By default, the device uses the **enhanced** CAR resource allocation mode, where CAR resources are allocated in a contiguous manner. However, in some scenarios, for example, scenarios with heavy traffic, traffic may be rate-limited inaccurately. In this case, you can change the CAR resource allocation mode to **normal**, where CAR resources are allocated in a non-contiguous manner.

Precautions

- After configuring the CAR resource allocation mode, save the configuration, and restart the device for the configuration to take effect.
- After the CAR resource allocation mode is changed from **enhanced** to **normal**, the number of available CAR resources is halved.

Example

Change the CAR resource allocation mode to **enhanced**.

```
<HUAWEI> system-view
[HUAWEI] assign car-resource enhanced
```

15.3.3 car (traffic behavior view)

Function

The **car** command configures traffic policing in a traffic behavior.

The **undo car** command deletes traffic policing from a traffic behavior.

By default, traffic policing is not configured in a traffic behavior.

Format

car [**aggregation**] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green pass**] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, and S5720S-LI)

car [**aggregation**] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**coupling-flag** *flag-value*] [**mode** { **color-blind** | **color-aware** }] [**green pass**] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] (S5735S-H, S5735-S, S5735S-S, S6720S-S, and S5736-S)

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**coupling-flag** *flag-value*] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] (S6735-S, S6720-EI, S6720S-EI)

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**coupling-flag** *flag-value*] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**service-class** *class* **color** *color*] } | **yellow** { **discard** | **pass** [**service-class** *class* **color** *color*] } | **red** { **discard** | **pass** [**service-class** *class* **color** *color*] }]* (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

car [**aggregation**] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value*] }] (S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S)

undo car

Parameters

Parameter	Description	Value
aggregation	Indicates aggregated CAR. Aggregated CAR can be applied to multiple interfaces, and traffic on the interfaces is restricted by aggregated CAR.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the minimum CIR is 16 kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the minimum PIR is 16 kbit/s. The PIR must be greater than or equal to the CIR. By default, the PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. By default, the CBS is 125 times the CIR. **NOTE** If the default CBS is smaller than 4000 because the CIR is small, the device uses the CBS of 4000. If the default CBS is larger than 4294967295 because the CIR is large, the device uses the CBS of 4294967295.

Parameter	Description	Value
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 125 times the CIR. If the PIR is set, the default PBS is 125 times the PIR. **NOTE** If the default PBS is smaller than 4000 because the CIR or PIR is small, the device uses the PBS of 4000. If the default PBS is larger than 4294967295 because the CIR or PIR is large, the device uses the PBS of 4294967295.
share	Indicates level-1 aggregated CAR. If level-1 aggregated CAR is defined in a traffic behavior, and a traffic classifier defining multiple matching rules is bound to this traffic behavior, traffic matching the traffic classifier shares the rate limit.	-
coupling-flag *flag-value*	Specifies the MEF meter algorithm. The following models support both the MEF0 and MEF1 algorithms: S6720S-S, S5731-S, S5731S-S, S5731-H, S5731S-H, S5732-H, S6730-H, S6730-S, S6730S-S, S6730S-H, S5735S-H, and S5736-S. The following models support only the MEF0 algorithm: S6735-S, S6720-EI, and S6720S-EI.	The value is 0 for the S6735-S, S6720-EI, and S6720S-EI and can be 0 or 1 for the other models.
mode	Specifies the color mode for traffic policing.	-

Parameter	Description	Value
color-blind	Specifies the color-blind mode. In color-blind mode, the original packet color does not affect the traffic policing action.	-
color-aware	Specifies the color-aware mode. In color-aware mode, the original packet color affects the traffic policing action.	-
green **yellow** **red**	Specifies the packet color. The packet color is determined by the CBS and PBS. By default, green packets and yellow packets are allowed to pass through, and red packets are discarded.	-
discard	Discards packets.	If the action specified for green packets is **discard**, the action specified for yellow and red packets must be **discard**. If the action specified for yellow packets is **discard**, the action specified for red packets must be **discard**.
pass	Allows packets to pass through.	-
remark-8021p *8021p-value*	Re-marks the 802.1p priorities of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
remark-dscp *dscp-value*	Re-marks the DSCP priority of packets.	The value is an integer that ranges from 0 to 63.
service-class *class*	Specifies the class of service (CoS).	The value can be **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.
color *color*	Specifies the color corresponding to the CoS.	The value can be **green**, yellow, or **red**.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow-based traffic policing controls traffic that matches traffic classification rules and discards the excess traffic to limit traffic within a proper range and to protect network resources.

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate so that the outgoing traffic rate is limited within a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

Traffic policing based on traffic policies controls rates of packets of different types.

The packet color is determined by the CBS and PBS:

- When the size of a packet is smaller than the CBS, the packet is colored green.
- When the size of a packet is greater than or equal to the CBS but smaller than the PBS, the packet is colored yellow.
- When the size of a packet is greater than or equal to the PBS, the packet is colored red.

After traffic policing is configured, the device counts forwarded and discarded packets.

If level-1 aggregated CAR is defined in a traffic behavior, and a traffic classifier defining multiple matching rules is bound to this traffic behavior, traffic matching the traffic classifier shares the rate limit. If level-1 aggregated CAR is not configured in a traffic behavior, the device limits the rate of traffic based on rules.

Prerequisites

A traffic behavior has been created using the **traffic behavior** command.

Precautions

When a traffic policy containing traffic policing actions is applied to an interface, you must use the **undo traffic-policy** command to unbind the traffic policy if you need to change traffic policing parameters.

If a traffic behavior defines the **car** command with **remark-8021p** *8021p-value* or **remark-dscp** *dscp-value* specified on the S6720S-S, S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, and S5736-S, a traffic policy containing this traffic behavior can only be applied in the inbound direction.

For the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, S6720S-S: If aggregated CAR is configured by specifying the **aggregation** parameter, a traffic policy containing this traffic behavior can only be applied in the inbound direction.

If a traffic behavior defines the **car** command with **share** specified, a traffic policy containing this traffic behavior can only be applied in the inbound direction.

The **aggregation** and **share** parameters cannot be specified simultaneously in one traffic behavior.

For the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S, S6720S-S: If a traffic policy defining aggregated CAR and traffic statistics collection is applied to multiple interfaces, the system collects traffic statistics on all these interfaces. Traffic statistics on any one of the interfaces are the sum traffic statistics of all these interfaces.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

When you use a traffic policy for rate limiting and apply the traffic policy in the Eth-Trunk interface view, if the Eth-Trunk interface contains several member interfaces, these member interfaces share the bandwidth specified by the rate limit.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if traffic policing and traffic statistics collection are configured in the same traffic behavior, only the following statistics are correct: numbers of packets and bytes that match the bound traffic classifier and on the packet rate, namely, values of **Packets**, **Bytes**, **Rate(pps)**, and **Rate(bps)** in **matched** in the **display traffic policy statistics** command output.

For the S6735-S, S6720-EI, S6720S-EI, the **car** command containing **remark-dscp** *dscp-value* and the **remark dscp** command cannot be configured in the same traffic behavior.

For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if the **car** command containing **remark-dscp** *dscp-value* and the **remark dscp** command are configured in the same traffic behavior, only the **car** command takes effect after the corresponding traffic policy is applied. The re-marked DSCP priority of a packet depends on the **car** command configuration.

Example

Configure traffic policing in the traffic behavior **b1** as follows: Set the CIR to 1000 kbit/s, permit green and yellow packets to pass through, re-mark the 802.1p priority of green packets with 7, re-mark the DSCP priority of yellow packets with 20, and discard red packets.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] car cir 1000 green pass remark-8021p 7 yellow pass remark-dscp 20 red discard
```

Configure level-1 aggregated CAR in the traffic behavior **b2** as follows: Set the CIR to 100 kbit/s for incoming data flows with destination IP addresses in 192.168.1.0/24 and 192.168.2.0/24 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl number 4999
[HUAWEI-acl-L2-4999] rule 5 permit destination 192.168.1.0 0.0.0.255
[HUAWEI-acl-L2-4999] rule 10 permit destination 192.168.2.168 0
[HUAWEI-acl-L2-4999] rule 15 permit destination 192.168.2.0 0.0.0.255
[HUAWEI-acl-L2-4999] quit
[HUAWEI] traffic classifier c2 operator or
[HUAWEI-classifier-c2] if-match acl 4999
[HUAWEI-classifier-c2] quit
[HUAWEI] traffic behavior b2
[HUAWEI-behavior-b2] car cir 100 pir 100 cbs 18800 pbs 31300 share green pass yellow pass red discard
[HUAWEI-behavior-b2] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p2 inbound
```

If level-1 aggregated CAR is not configured, configure the traffic behavior **b2** in the preceding example as follows: Limit the rate of incoming data flows destined for 192.168.2.168 on GE0/0/1 to 100 kbit/s, and limit the total rate of incoming data flows destined for 192.168.1.0/24 and 192.168.2.0/24 (excluding 192.168.2.168) to 100 kbit/s, respectively.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b2
[HUAWEI-behavior-b2] car cir 100 pir 100 cbs 18800 pbs 31300 green pass yellow pass red discard
```

15.3.4 car (QoS profile view)

Function

The **car** command configures traffic policing in a QoS profile.

The **undo car** command deletes the traffic policing configuration from the QoS profile.

By default, traffic policing is not configured in a QoS profile.

Format

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] { **inbound** | **outbound** }

undo car { **inbound** | **outbound** }

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

The S6720-EI, S6735-S, and S6720S-EI do not support inbound traffic policing.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR must be greater than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default CBS is 188 times the CIR. If the PIR is set, the default CBS is 125 times the CIR.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 313 times the CIR. If the PIR is set, the default PBS is 125 times the PIR.
inbound	Indicates inbound traffic policing.	-
outbound	Indicates outbound traffic policing.	-

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing discards excess traffic to limit traffic within a proper range and to protect network resources.

The **car** command configures traffic policing in a QoS profile.

Follow-up Procedure

Apply the QoS profile in the AAA domain view.

Precautions

When the traffic policing rate is larger than the maximum bandwidth of an interface, traffic policing does not take effect on the interface. Set the CIR and PIR to be smaller than the rate of an interface.

When the CBS is smaller than the number of bytes in a packet, the device directly discards the packet.

Example

Create a QoS profile named **huawei** in which the CIR is set to 10000 kbit/s, the CBS is set to 10240 bytes, and the PBS is set to 10240 bytes.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] car cir 10000 cbs 10240 pbs 10240 inbound
```

15.3.5 car share

Function

The **car share** command configures aggregated CAR in a traffic behavior.

The **undo car share** command cancels aggregated CAR in a traffic behavior.

By default, aggregated CAR is not configured in a traffic behavior.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

car *car-name* **share**

undo car [*car-name*] **share**

Parameters

Parameter	Description	Value
car-name	Specifies the name of a CAR profile.	The value must the name of an existing CAR profile.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple traffic classifiers are defined in a traffic policy and traffic behaviors associated with the traffic classifiers define CAR (using the **car cir** command) and aggregated CAR, the system limits the rates of flows using the configured CAR, aggregates the flows, and limits the rate of the aggregated traffic using the aggregated CAR in sequence. This process is called hierarchical traffic policing.

Hierarchical traffic policing multiplexes traffic statistics and controls services in a fine-granular manner. For example, hierarchical traffic policing limits the service traffic of level-1 and level-2 users or traffic of level-1 and level-2 user groups.

Prerequisites

A QoS CAR profile has been configured using the **qos car** command.

Precautions

The traffic policy defining the aggregated CAR action can only be used in the inbound direction.

After aggregated CAR is configured, all the rules in the traffic classifiers bound to the same traffic behavior share the CAR index. The system aggregates all the flows matching these traffic classifiers and uses CAR to limit the rate of the flows. If the traffic classifiers define both Layer 2 and Layer 3 information, the aggregated CAR configuration is invalid.

A traffic policy limits the traffic rate using the aggregated CAR only in the current applied object. For example, when the traffic policy **p1** defining the aggregated CAR is applied to **interface1** and **interface2**, the aggregated CAR applies to traffic on **interface1** and **interface2** respectively, without affecting each other.

Example

Configure aggregated CAR in the traffic behavior **tb1**.

```
<HUAWEI> system-view
[HUAWEI] qos car qoscar1 cir 2000
[HUAWEI] traffic behavior tb1
[HUAWEI-behavior-tb1] car cir 1000 pir 123456
[HUAWEI-behavior-tb1] car qoscar1 share
```

15.3.6 display car-resource configuration

Function

The **display car-resource configuration** command displays the CAR resource allocation mode.

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, and S5735-S-I.

Format

display car-resource configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the CAR resource allocation mode that is used currently and to be used after the next startup of the device.

Example

Display the CAR resource allocation mode on a device.

```
<HUAWEI> display car-resource configuration
Slot      Current Mode    Next Mode
- - - - - - - - - - - - - - - - - - - - - - -
0         enhanced        enhanced
1         enhanced        enhanced
-------------------------------------------------------------------------------
```

Table 15-21 Description of the **display car-resource configuration** command output

Item	Description
Slot	Slot ID.
Current Mode	CAR resource allocation mode that is used currently.
Next Mode	CAR resource allocation mode to be used after the next startup of the device. To configure the CAR resource allocation mode, run the **assign car-resource** command.

15.3.7 display qos-profile

Function

The **display qos-profile** command displays the configured QoS profile information.

Format

display qos-profile [**name** *profile-name* | **all**]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a QoS profile.	The value must the name of an existing QoS profile.
all	Indicates all QoS profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos-profile** command displays the configuration of a specified QoS profile or all QoS profiles. The command output helps you check the QoS profile configuration and locate QoS faults.

Example

Display the configurations of all QoS profiles.

```
<HUAWEI> display qos-profile all
Qos-profile[0]: huawei
---------------------------------------------
IcarConfiged      :      0
IcarCir           :      0
IcarPir           :      0
IcarCbs           :      0
IcarPbs           :      0
```

```
EcarConfiged       :        0
EcarCir            :        0
EcarPir            :        0
EcarCbs            :        0
EcarPbs            :        0
StatisticEn        :        0
Remark8021p        :        0
8021pValue         :        0
RemarkDscp inbound  :        0
DscpValue inbound   :        0
RemarkDscp outbound :        0
DscpValue outbound  :        0
---------------------------------------------
```

NOTE

The **display qos-profile** command on the S6735-S, S6720-EI and S6720S-EI does not display **Remark8021p**, **8021pValue**, **RemarkDscp**, or **DscpValue**.

Table 15-22 Description of the **display qos-profile all** command output

Item	Description
Qos-profile[0]	Name of a QoS profile. The number in bracket is the index that the system assigns to the QoS profile. To create a QoS profile, run the **qos-profile** command.
IcarConfiged	Whether inbound traffic policing is configured: ● 0: Inbound traffic policing is not configured. ● 1: Inbound traffic policing is configured. To configure inbound traffic policing in a QoS profile, run the **car (QoS profile view)** command.
IcarCir	CIR in the inbound direction. To change the value, run the **car (QoS profile view)** command.
IcarPir	PIR in the inbound direction. To change the value, run the **car (QoS profile view)** command.
IcarCbs	CBS in the inbound direction. To change the value, run the **car (QoS profile view)** command.
IcarPbs	PBS in the inbound direction. To change the value, run the **car (QoS profile view)** command.

Item	Description
EcarConfiged	Whether outbound traffic policing is configured: ● 0: Outbound traffic policing is not configured. ● 1: Outbound traffic policing is configured. To configure outbound traffic policing in a QoS profile, run the **car (QoS profile view)** command.
EcarCir	CIR in the outbound direction. To change the value, run the **car (QoS profile view)** command.
EcarPir	PIR in the outbound direction. To change the value, run the **car (QoS profile view)** command.
EcarCbs	CBS in the outbound direction. To change the value, run the **car (QoS profile view)** command.
EcarPbs	PBS in the outbound direction. To change the value, run the **car (QoS profile view)** command.
StatisticEn	Whether the traffic statistics function is configured: ● 0: The traffic statistics function is not configured. ● 1: The traffic statistics function is configured. To configure the traffic statistics function in a QoS profile, run the **statistic enable (QoS profile view)** command.
Remark8021p	Whether 802.1p priority re-marking is configured: ● 0: 802.1p priority re-marking is not configured. ● 1: 802.1p priority re-marking is configured. To configure 802.1p priority re-marking in a QoS profile, run the **remark 8021p (QoS profile view)** command.

Item	Description
8021pValue	Re-marked 802.1p priority. To change the value, run the **remark 8021p (QoS profile view)** command.
RemarkDscp inbound	Whether to re-mark the DSCP priority of incoming packets: - 0: DSCP priority re-marking is not configured. - 1: DSCP priority re-marking is configured. To configure DSCP priority re-marking in a QoS profile, run the **remark dscp (QoS profile view)** command.
DscpValue inbound	Re-marked DSCP priority of incoming packets. To change the value, run the **remark dscp (QoS profile view)** command.
RemarkDscp outbound	Whether to re-mark the DSCP priority of outgoing packets: - 0: DSCP priority re-marking is not configured. - 1: DSCP priority re-marking is configured. To configure DSCP priority re-marking in a QoS profile, run the **remark dscp (QoS profile view)** command.
DscpValue outbound	Re-marked DSCP priority of outgoing packets. To change the value, run the **remark dscp (QoS profile view)** command.

Display the summary configurations of all QoS profiles.

```
<HUAWEI> display qos-profile
       index                  qos-profile name
-------------------------------------------------------------------
       0                      huawei
-------------------------------------------------------------------
 Total   64     Used   1
```

Table 15-23 Description of the **display qos-profile** command output

Item	Description
index	Index that the system assigns to a QoS profile.

Item	Description
qos-profile name	Name of a QoS profile.
Total	Maximum number of QoS profiles that can be configured.
Used	Number of used QoS profiles.

15.3.8 display qos car

Function

The **display qos car** command displays the QoS CAR profile configuration.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display qos car { **all** | **name** *car-name* }

Parameters

Parameter	Description	Value
all	Displays the configurations of all QoS CAR profiles.	-
name *car-name*	Displays the configuration of a specified QoS CAR profile.	The value must the name of an existing QoS CAR profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos car** command displays the configurations of all QoS CAR profiles or a specified QoS CAR profile. The command output helps you check the QoS CAR profile configuration and locate QoS faults.

Precautions

If you do not use the **qos car** command to create a QoS CAR profile, no information is displayed after the **display qos car** command is executed.

Example

Display the configurations of all QoS CAR profiles.

```
<HUAWEI> display qos car all
  ----------------------------------------------------------------
   CAR Name     : qoscar1
   CAR Index    : 0
    car cir 8000 (Kbps) pir 10000 (Kbps) cbs 1000000 (byte) pbs 1250000 (byte)
  ----------------------------------------------------------------
   CAR Name     : qoscar2
   CAR Index    : 1
    car cir 5000 (Kbps) pir 8000 (Kbps) cbs 625000 (byte) pbs 1000000 (byte)
  ----------------------------------------------------------------
   CAR Name     : car1
   CAR Index    : 2
    car cir 1000 (Kbps) cbs 188000 (byte)
```

Display the configuration of the QoS CAR profile named **car1**.

```
<HUAWEI> display qos car name car1
  ----------------------------------------------------------------
   CAR Name     : car1
   CAR Index    : 2
    car cir 1000 (Kbps) cbs 188000 (byte)
```

Table 15-24 Description of the **display qos car** command output

Item	Description
CAR Name	QoS CAR profile name. To configure a QoS CAR profile, run the **qos car** command.
CAR Index	Index of the QoS CAR profile.
car cir 8000 (Kbps) pir 10000 (Kbps) cbs 1000000 (byte) pbs 1250000 (byte)	Parameters of the QoS CAR profile, including the CIR, PIR, CBS, and PBS. To set parameters in a QoS CAR profile, run the **qos car** command.

15.3.9 display qos configuration

Function

The **display qos configuration** command displays the QoS configuration on an interface.

Format

display qos configuration interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface [*interface-type interface-number*]	Displays the QoS configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the QoS configurations on all the interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos configuration** command displays QoS configurations on a specified interface or all interfaces. The command output helps you check the QoS configuration and locate QoS faults.

Example

Display the QoS configuration on GE0/0/1 of the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, or S5720-LI.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
 ------------------------------------------------------------------------
 Trust flag            | 8021p
 Port priority         | 0
 Schedule-profile        |
 Tail-drop-profile       |
 Port lr             | outbound, cir = , cbs =
 Port lr             | inbound, cir = , cbs =
 ------------------------------------------------------------------------
 queue-index | configuration |
 ------------------------------------------------------------------------
```

```
0           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
1           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
2           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
3           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
4           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
5           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
6           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
7           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
```

Display the QoS configuration on GE0/0/1 of the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, or S5735S-S.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
----------------------------------------------------------------------------
Trust flag                  | dscp
DS name                     | default
DEI enable                  | disable
PHB marking                 | enable
Port priority               | 0
Tail-drop-profile           |
Port lr                     | outbound, cir = , cbs =
Port lr                     | inbound, cir = , cbs =
----------------------------------------------------------------------------
queue-index | configuration |
----------------------------------------------------------------------------
0           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
1           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
2           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
3           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
----------------------------------------------------------------------------
4           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
```

```
 --------------------------------------------------------------------------
 5           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
 --------------------------------------------------------------------------
 6           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
 --------------------------------------------------------------------------
 7           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
 --------------------------------------------------------------------------
```

Display the QoS configuration on GE0/0/1 of the S6735-S, S6720-EI or S6720S-EI.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
 --------------------------------------------------------------------------
 Trust flag                  | dscp
 DS name                      |
 DEI enable                  | disable
 PHB marking                  | enable
 Port priority               | 0
 Port wred                   |
 Port lr                     | outbound, cir = , cbs =
 Port lr                     | inbound, cir = , cbs =
 --------------------------------------------------------------------------
 queue-index | configuration |
 --------------------------------------------------------------------------
 0           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
 --------------------------------------------------------------------------
 1           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
 --------------------------------------------------------------------------
 2           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
 --------------------------------------------------------------------------
 3           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
 --------------------------------------------------------------------------
 4           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
 --------------------------------------------------------------------------
 5           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
 --------------------------------------------------------------------------
 6           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
```

```
            | wred          |
            | length        |
------------------------------------------------------------------------
7           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | wrr, weight = 1
            | wred          |
            | length        |
------------------------------------------------------------------------
```

Display the QoS configuration on GE0/0/1 of the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
------------------------------------------------------------------------
Trust flag                  | outer 8021p
DS name                     |
DEI enable                  | disable
Port priority               | 0
PHB marking                 | enable
Port wred                   |
Port lr                     | outbound, cir = , cbs =
Port lr                     | inbound, cir = , cbs =
TM enable                   | disable
------------------------------------------------------------------------
queue-index | configuration |
------------------------------------------------------------------------
0           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
1           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
2           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
3           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
4           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
5           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
6           | shaping       | cir = , cbs =
            |               | pir = , pbs =
            | schedule      | pq
            | wred          |
            | length        |
------------------------------------------------------------------------
```

```
7          | shaping       | cir = , cbs =
           |               | pir = , pbs =
           | schedule      | pq
           | wred          |
           | length        |
------------------------------------------------------------------------------
```

Table 15-25 Description of the **display qos configuration** command output

Item	Description
Trust flag	Type of the external priority (802.1p priority, DSCP priority, or IP precedence) mapped to the internal priority (DiffServ level and color). To change the value, run the **trust** command.
DS name	DiffServ domain name. To create a DiffServ domain, run the **diffserv domain** command.
DEI enable	Whether the function that DEI field in a VLAN tag is mapped to the drop priority is enabled. ● enable: The function is enabled. ● disable: The function is disabled. To set the function that DEI field in a VLAN tag is mapped to the drop priority, run the **dei enable** command.
PHB marking	Whether PHB mapping is enabled for outgoing packets on the interface. ● enable: PHB mapping is enabled for outgoing packets on the interface. ● disable: PHB mapping is disabled for outgoing packets on the interface. To set PHB mapping, run the **qos phb marking enable** command.
Port priority	Default 802.1p priority added to untagged packets by the interface. To change the value, run the **port priority** command.
Port wred	Name of the WRED drop profile applied to the interface. To apply a WRED drop profile to an interface, run the **qos wred** command.
Schedule-profile	Name of the scheduling profile applied to the interface. To apply a scheduling profile to an interface, run the **qos schedule-profile (interface view)** command.
Tail-drop-profile	Name of the tail drop profile applied to the interface. To apply a tail drop profile to an interface, run the **qos tail-drop-profile (interface view)** command.

Item	Description
Port lr	Traffic shaping rate on the interface. To configure traffic shaping rate on an interface, run the **qos lr outbound** or **qos lr inbound** command.
TM enable	Whether the traffic manager (TM) is enabled to buffer and schedule packets. ● enable: The TM is enabled to buffer and schedule packets. ● disable: The TM is disabled from buffering and scheduling packets. To enable the TM, run the **qos traffic-manage enable** command.
queue-index	Interface queue index.
configuration	Interface queue configuration.
shaping	Traffic shaping configuration of the interface queue. To configure traffic shaping on an interface, run the **qos queue shaping** command.
cir	Committed information rate (CIR). To change the value, run the **qos queue shaping** command.
cbs	Committed burst size (CBS). To change the value, run the **qos queue shaping** command.
pir	Peak information rate (PIR). To change the value, run the **qos queue shaping** command.
pbs	Peak burst size (PBS). To change the value, run the **qos queue shaping** command.
schedule	Scheduling mode of the interface queue. To set the scheduling mode of interface queues, run the **qos { pq | wrr | drr }** command.
wred	WRED drop profile bound to an interface queue. To bind a WRED drop profile to an interface queue, run the **qos queue wred** command.
weight	Scheduling weight of a queue. To set the scheduling weight of a queue, run the **qos queue drr** or **qos queue wrr** command.
length	Interface queue length. This field cannot be modified on the switch and is empty in the command output.

15.3.10 display qos lr

Function

The **display qos lr** command displays the rate limit configuration on an interface.

Format

display qos lr { **inbound** | **outbound** } **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
inbound	Displays the rate limit configuration in the inbound direction on an interface.	-
outbound	Displays the rate limit configuration in the outbound direction on an interface.	-
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos lr** command displays the rate limit configuration on a specified interface. The command output helps you check the rate limit on an interface and locate faults.

Precautions

If you do not use the **qos lr inbound** or **qos lr outbound** command to configure the rate limit on an interface, no information is displayed after the **display qos lr** command is executed.

Example

Set the CIR of data packets to be sent from the GE0/0/1 to 20000 kbit/s and the CBS to 375000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos lr outbound cir 20000 cbs 375000
[HUAWEI-GigabitEthernet0/0/1] quit
```

Display the rate limit configuration on the GE0/0/1.

```
<HUAWEI> display qos lr outbound interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 lr outbound:
  cir: 20000 Kbps, cbs: 375000 Byte
```

Table 15-26 Description of the **display qos lr** command output

Item	Description
cir	Committed information rate (CIR). To set the CIR, run the **qos lr inbound** or **qos lr outbound** command.
cbs	Committed burst size (CBS). To set the CBS, run the **qos lr inbound** or **qos lr outbound** command.

15.3.11 display qos statistics

Function

The **display qos statistics** command displays traffic statistics on an interface where rate limiting is performed in the inbound direction.

Format

display qos statistics interface *interface-type interface-number* **inbound**

display qos statistics inbound all [**nonzero**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays traffic statistics on a specified interface where rate limiting is performed. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
inbound	Displays traffic statistics in the inbound direction.	-
all	Displays traffic statistics on all interfaces where rate limiting is performed.	-
nonzero	Displays traffic statistics on all interfaces where rate limiting is performed and the statistics are not 0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display qos statistics** command to view statistics on forwarded and discarded packets and check whether rate limiting takes effect. The command output helps you locate faults.

Prerequisites

The **qos lr inbound** command has been executed to configure rate limiting in the inbound direction on an interface.

Precautions

If the **qos lr inbound** command is not used, the system displays the following message after the **display qos statistics interface** *interface-type interface-number* **inbound** command is executed:

```
Info: There is no rate limited configuration inbound in the interface.
```

Example

Display traffic statistics on GE0/0/1 where rate limiting is performed in the inbound direction. (S5732-H)

```
<HUAWEI> display qos statistics interface gigabitethernet 0/0/1 inbound
------------------------------------------------------------
 Item                                     Value
------------------------------------------------------------
 Passed packets                             0
 Passed bytes                              0
 Dropped packets                             0
 Dropped bytes                              0
------------------------------------------------------------
```

Display traffic statistics on GE0/0/1 where rate limiting is performed in the inbound direction. (S5735-S)

```
<HUAWEI> display qos statistics interface gigabitethernet 0/0/1 inbound
------------------------------------------------------------
 It has not reached the threshold of ingress bandwidth.
------------------------------------------------------------
```

Table 15-27 Description of the **display qos statistics** command output

Item	Description
Passed packets	Number of forwarded packets.
Passed bytes	Number of forwarded bytes.
Dropped packets	Number of discarded packets.
Dropped bytes	Number of discarded bytes.
It has not reached the threshold of ingress bandwidth.	On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the following information may be displayed in the **display qos statistics** command output: ● The rate limit is not reached: It has not reached the threshold of ingress bandwidth. ● The rate limit is reached: It has reached the threshold of ingress bandwidth.

15.3.12 qos car

Function

The **qos car** command creates a QoS CAR profile and sets parameters in the QoS CAR profile.

The **undo qos car** command deletes a QoS CAR profile.

By default, no QoS CAR profile is created.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

qos car *car-name* **cir** *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

undo qos car *car-name*

Parameters

Parameter	Description	Value
car-name	Specifies the name of a QoS CAR profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be c, ci, or cir.
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR must be greater than or equal to the CIR. By default, the PIR is equal to the CIR.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. By default, the CBS is 188 times the CIR if the PIR is not set and is 125 times the CIR if the PIR is set.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. By default, the PBS is 125 times the PIR.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing controls traffic by monitoring the rate of traffic, and discards excess traffic to limit traffic within a proper range and to protect network resources.

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate so that the outgoing traffic rate is limited within a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

The packet color is determined by **cbs** *cbs-value* and **pbs** *pbs-value* of this command:

- When the size of a packet is smaller than the CBS, the packet is colored green.
- When the size of a packet is greater than or equal to the CBS but smaller than the PBS, the packet is colored yellow.
- When the size of a packet is greater than or equal to the PBS, the packet is colored red.

Precautions

A maximum of 512 QoS CAR profiles can be created on the switch.

When the traffic shaping rate is greater than the maximum rate of an interface, traffic policing is not performed on the interface. You need to set the CIR or PIR to be smaller than the maximum rate of the interface.

When the CBS is smaller than the number of bytes in a packet, packets of this type are discarded.

To prevent a device failure to identify the packet color, you are advised to set the PBS to be larger than the CBS.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

The granularity of traffic policing may increase with the CBS. For the S6735-S, S6720-EI and S6720S-EI, if the CIR is far smaller than the CBS (for example, the CIR is set to 1000 kbit/s and CBS is set to 1000000 bytes), rate limiting may be inaccurate.

Example

Create a QoS CAR profile named **qoscar1**, and set the CIR to 10000 kbit/s and the CBS to 10240 bytes.

```
<HUAWEI> system-view
[HUAWEI] qos car qoscar1 cir 10000 cbs 10240
```

15.3.13 qos-car exclude-interframe

Function

The **qos-car exclude-interframe** command configures the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic policing rate or rate limit.

The **undo qos-car exclude-interframe** command configures the device to count the inter-frame gap and preamble of packets when the device calculates the traffic policing rate or rate limit.

By default, the device calculates the inter-frame gap and preamble of packets when the device calculates the traffic policing rate or rate limit.

Format

qos-car exclude-interframe

undo qos-car exclude-interframe

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When traffic policing or rate limiting is configured on an interface, the device calculates the inter-frame gap and preamble of packets for the traffic policing rate or rate limit. As a result, the rate is inaccurate. After the **qos-car exclude-interframe** command is used, the device does not count the inter-frame gap and preamble of packets for the traffic policing rate or rate limit.

The **qos-car exclude-interframe** command affects calculation of the traffic policing rate and inbound rate limit. When the **car (traffic behavior view)** and **qos lr inbound** commands are used to configure traffic policing and inbound rate limiting, the device does not count the inter-frame gap and preamble for the traffic policing rate or rate limit.

Precautions

Before this command is used, the following formula is used to calculate the traffic policing rate or rate limit:

Traffic policing rate/Rate limit = (Original packet length + Inter-frame gap + Preamble) x Number of packets forwarded per second

The inter-frame gap and preamble occupy 20 bytes.

After this command is used, the following formula is used to calculate the traffic policing rate or rate limit:

Traffic policing rate/Rate limit = Original packet length x Number of packets forwarded per second

Example

Configure the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic policing rate.

```
<HUAWEI> system-view
[HUAWEI] qos-car exclude-interframe
```

15.3.14 qos-profile

Function

The **qos-profile** command creates a QoS profile and displays its view, or directly displays the view of an existing QoS profile.

The **undo qos-profile** command deletes a QoS profile.

By default, no QoS profile is configured on the device.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

qos-profile name *profile-name*

undo qos-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a QoS profile.	The value is a string of 1 to 64 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be --.
all	Indicates all QoS profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can define QoS configurations in a QoS profile to implement such functions as traffic policing, priority re-marking, and traffic statistics.

Follow-up Procedure

- Define parameters in the QoS profile, including parameters of traffic policing, priority re-marking, and traffic statistics.
- Apply the QoS profile in the specified view.

Precautions

The **undo qos-profile all** command only deletes the QoS profiles that are not applied.

The switch supports a maximum of 64 QoS profiles.

Example

Create a QoS profile named **huawei** and enter the QoS profile view.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei]
```

15.3.15 qos-shaping exclude-interframe

Function

The **qos-shaping exclude-interframe** command configures the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

The **undo qos-shaping exclude-interframe** command configures the device to count the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

By default, the device counts the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

Format

qos-shaping exclude-interframe

undo qos-shaping exclude-interframe

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After traffic shaping is configured on an interface, the device counts the inter-frame gap and preamble of packets for the traffic shaping rate. As a result, the rate is inaccurate. After the **qos-shaping exclude-interframe** command is used, the device does not calculate the inter-frame gap and preamble of packets for the traffic shaping rate.

The **qos-shaping exclude-interframe** command affects calculation of the traffic shaping rate and outbound rate limit. When the **qos queue shaping** and **qos lr outbound** commands are used to configure traffic shaping and outbound rate limiting, the device does not count the inter-frame gap and preamble for the traffic shaping rate.

Precautions

Before this command is used, the following formula is used to calculate the traffic shaping rate:

Traffic shaping rate = (Original packet length + Inter-frame gap + Preamble) x Number of packets forwarded per second

The inter-frame gap and preamble occupy 20 bytes.

After this command is used, the following formula is used to calculate the traffic shaping rate:

Traffic shaping rate = Original packet length x Number of packets forwarded per second

Example

Configure the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

```
<HUAWEI> system-view
[HUAWEI] qos-shaping exclude-interframe
```

15.3.16 qos lr inbound

Function

The **qos lr inbound** command configures traffic policing in the inbound direction on an interface.

The **undo qos lr inbound** command cancels traffic policing in the inbound direction on an interface.

By default, traffic policing is not configured in the inbound direction on an interface.

Format

qos lr inbound cir *cir-value* [**cbs** *cbs-value*]

undo qos lr inbound

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer. The value range differs depending on the interface type: - Interfaces in a port group: 64 to 100000000 - Other interfaces: 64 to X, where X indicates the maximum rate supported by the interface Unit: kbit/s

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 4000 to 4294967295, in bytes. If this parameter is not specified, the CBS is 125 times the CIR by default. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, CloudEngine S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the maximum CBS is 65535 bytes. On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI, the maximum value of the CBS is 65535 granularities. Each granularity depends on the CIR: ● When the CIR is in the range of 64 kbit/s to 1023 kbit/s, each granularity is 1 byte. ● When the CIR is in the range of 1024 kbit/s to 10230 kbit/s, each granularity is 8 bytes. ● When the CIR is in the range of 10231 kbit/s to 102300 kbit/s, each granularity is 64 bytes. ● When the CIR is in the range of 102301 kbit/s to 1023000 kbit/s, each granularity is 512 bytes. ● When the CIR is in the range of 1023001 kbit/s to 10000000 kbit/s, each granularity is 4096 bytes.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. In this case, the data traffic rate needs to be limited. After the traffic policing rate for incoming packets on an interface is set by using the **qos lr inbound** command, if the rate of packets received by the interface is larger than the traffic policing rate and the queue buffer is full, the packets exceeding the rate limit are discarded.

Precautions

When interface-based 802.1X authentication is configured and the RADIUS server delivers the rate limit, the interface does not support the rate limit.

If both the IPSG function and inbound interface-based rate limiting are configured on an interface of the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI, both IPSG and interface-based rate-limiting configurations take effect as long as the configurations do not conflict. Otherwise, only the IPSG configuration takes effect.

The **traffic-limit (interface view)** command limits the rate of packets matching an ACL, whereas the **qos lr inbound** command limits the rate of all packets on an interface. If both of them are configured:

- On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI, the **qos lr inbound** command takes effect.
- On the S6735-S, S6720-EI, and S6720S-EI, rate limiting is inaccurate.
- On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, the actual rate limit is the smaller CIR between CIR values configured using the two commands.

Configuring the **qos lr inbound** command occupies system resources. If system resources are insufficient, the configuration fails.

If you run the **qos lr inbound** command multiple times on the same interface, only the latest configuration takes effect.

If you need to set the same traffic policing rate on multiple interfaces, you can perform the configuration on a port group to reduce the workload.

The granularity of traffic shaping may increase with the CBS. For the S6735-S, S6720-EI and S6720S-EI, if the CIR is far smaller than the CBS (for example, the CIR is set to 1000 kbit/s and CBS is set to 1000000 bytes), rate limiting may be inaccurate.

If the rate range configured in a version earlier than V200R019C10 exceeds the maximum rate supported by an interface, the corresponding command in the configuration file of the source version can still be delivered after the version is upgraded to V200R019C10 or a later version. However, the maximum rate supported by the interface takes effect.

Example

Set the CIR of data packets received by the GE0/0/1 to 20000 kbit/s and the CBS to 375000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos lr inbound cir 20000 cbs 375000
[HUAWEI-GigabitEthernet0/0/1] quit
```

15.3.17 qos lr inbound whitelist protocol

Function

The **qos lr inbound whitelist protocol** command adds protocol packets to the whitelist for inbound interface-based rate limiting.

The **undo qos lr inbound whitelist protocol** command cancels the configuration.

By default, no protocol packet is added to the whitelist for inbound interface-based rate limiting.

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S support this command.

Format

qos lr inbound whitelist protocol { **arp-request** | **bpdu** | **dhcp** | **igmp** | **rip** }*

undo qos lr inbound whitelist protocol { **arp-request** | **bpdu** | **dhcp** | **igmp** | **rip** }*

Parameters

Parameter	Description	Value
arp-request	Indicates ARP request packets and Neighbor Solicitation (NS) messages.	-
bpdu	Indicates BPDUs.	-

Parameter	Description	Value
dhcp	Indicates DHCP and DHCPv6 packets.	-
igmp	Indicates IGMP packets, including IPv4 IGMP, IPv6 MLDv1, IPv6 MLDv2, and PIM packets.	-
rip	Indicates RIP and OSPF packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the traffic policing rate for incoming packets on an interface is set by using the **qos lr inbound** command, if the rate of packets received by the interface is larger than the traffic policing rate and the queue buffer is full, the packets exceeding the rate limit are discarded. To make the **qos lr inbound** command ineffective to one or more types of protocol packets (for example, DHCP packets, ARP request packets, and NS messages), you can run the **qos lr inbound whitelist protocol** command to add the protocol packets to the whitelist for inbound interface-based rate limiting. Then, the switch will not rate-limit incoming packets of these protocols on all interfaces.

Precautions

After the **qos lr inbound whitelist protocol** command is run to add protocol packets to the whitelist for inbound interface-based rate limiting, incoming packets of these protocols are exempted from traffic suppression and storm control.

Example

Add DHCP and DHCPv6 packets to the whitelist for inbound interface-based rate limiting.

```
<HUAWEI> system-view
[HUAWEI] qos lr inbound whitelist protocol dhcp
```

15.3.18 qos lr outbound

Function

The **qos lr outbound** command configures traffic shaping in the outbound direction on an interface.

The **undo qos lr outbound** command cancels traffic shaping in the outbound direction on an interface.

By default, traffic shaping is not configured in the outbound direction on an interface.

Format

qos lr outbound cir *cir-value* [**cbs** *cbs-value*]

undo qos lr outbound

NOTE

cbs *cbs-value* is not supported on the S5731-H, S5731-S, S5731S-H, and S5731S-S.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Interfaces in a port group: 64 to 100000000 ● Other interfaces: 64 to X, where X indicates the maximum rate supported by the interface

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 4000 to 4294967295, in bytes. If this parameter is not specified, the CBS is 125 times the CIR by default. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, CloudEngine S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the maximum CBS is 65535 bytes.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large amount of data flows are sent from the upstream device to its downstream device, to prevent congestion or packet loss, run the **qos lr outbound** command to configure traffic shaping on the outbound interface of the device to limit the traffic and burst traffic transmitted over a connection so that packets are sent at an even rate.

Similar to traffic policing, traffic shaping limits the traffic rate. When traffic policing is used, the system directly discards the packets whose rate is larger than the traffic policing rate. Traffic shaping, however, buffers the packets whose rate is larger than the traffic shaping rate. When there are sufficient tokens in the token bucket, the device forwards buffered packets at an even rate. Traffic shaping increases the delay, whereas traffic policing does not.

Precautions

When interface-based NAC authentication is configured and the RADIUS server delivers the rate limit, the interface does not support the rate limit.

If you need to set the same traffic shaping rate on multiple interfaces, you can perform the configuration on a port group to reduce the workload.

If both traffic shaping and queue shaping (configured by using the **qos queue shaping** command) are configured on an interface, the CIR of traffic shaping cannot be lower than the sum of CIR values of all the queues on the interface; otherwise, the traffic shaping result may be incorrect. For example, the queue with a lower priority may occupy the bandwidth of the queue with a higher priority.

Traffic shaping uses the buffer mechanism, thereby increasing the delay.

If you run the **qos lr outbound** command multiple times on the same interface, only the latest configuration takes effect.

After traffic shaping is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

On the S6720S-S, S5735S-H, and S5736-S, the **cbs** *cbs-value* parameter specified in the **qos lr outbound** command does not take effect and has a fixed value of 132000, in bytes.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, and S5720-LI, the maximum value of **cbs** *cbs-value* specified in the **qos lr outbound** command is 16380000, in bytes, even if the specified value is greater than 16380000.

The granularity of traffic policing may increase with the CBS. For the S6735-S, S6720-EI and S6720S-EI, if the CIR is far smaller than the CBS (for example, the CIR is set to 1000 kbit/s and CBS is set to 1000000 bytes), rate limiting may be inaccurate.

If the rate range configured in a version earlier than V200R019C10 exceeds the maximum rate supported by an interface, the corresponding command in the configuration file of the source version can still be delivered after the version is upgraded to V200R019C10 or a later version. However, the maximum rate supported by the interface takes effect.

Example

Set the CIR of data packets sent by the GE0/0/1 to 20000 kbit/s and the CBS to 375000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos lr outbound cir 20000 cbs 375000
[HUAWEI-GigabitEthernet0/0/1] quit
```

15.3.19 qos lr pps

Function

The **qos lr pps** command rate-limits incoming traffic on a management network interface.

The **undo qos lr pps** command disables rate limiting for incoming traffic on a management network interface.

By default, the rate limit on the management interface is 1000 pps.

NOTE

Only switches with management network interfaces support this command.

Format

qos lr pps *packets*

undo qos lr

Parameters

Parameter	Description	Value
packets	Specifies the maximum number of packets that are allowed to pass per second.	• S6720S-S, S5736-S, and S5735S-H: The value is an integer that ranges from 1 to 2500, in pps. • Other models: The value is an integer that ranges from 1 to 3000, in pps.

Views

MEth interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If there is heavy traffic on the management interface caused by malicious attacks or network exceptions, the CPU is overloaded and services are interrupted. To prevent this problem, run the **qos lr pps** command to rate-limit incoming traffic on a management network interface.

Configuration Impact

If a small rate limit is used, FTP and Telnet functions may be affected.

If you run the **qos lr pps** command multiple times on the same interface, only the latest configuration takes effect.

In a stack, only the management interface of the master switch can reach the value specified by the **qos lr pps** command.

Example

Set the rate limit of MEth0/0/1 to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] interface meth 0/0/1
[HUAWEI-MEth0/0/1] qos lr pps 100
```

15.3.20 qos queue shaping

Function

The **qos queue shaping** command enables traffic shaping for a queue on a specified interface and sets traffic shaping parameters.

The **undo qos queue shaping** command restores the default scheduling parameters of each queue on an interface.

The following table describes the default scheduling parameters on an interface.

Format

qos queue *queue-index* **shaping cir** *cir-value* **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]

undo qos queue *queue-index* **shaping**

NOTE

For the S5731-H, S5731-S, S5731S-H, and S5731S-S, only **pir** *pir-value* takes effect.

Parameters

Parameter	Description	Value
queue-index	Specifies the queue index.	The value is an integer that ranges from 0 to 7.
cir *cir-value*	Specifies the committed information rate (CIR) of a queue.	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Interfaces in a port group: 0 to 10000000 ● Other interfaces: 0 to X (the actual maximum rate supported by such an interface) The default value is the maximum bandwidth of an interface.

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR) of a queue.	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Interfaces in a port group: 64 to 10000000 ● Other interfaces: 64 to X (the actual maximum rate supported by such an interface) The default value is the maximum bandwidth of an interface. The PIR must be greater than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, CloudEngine S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the maximum CBS is 65535 bytes.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, the maximum PBS is 65535 bytes.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the traffic rate of an interface on a downstream device is lower than that of the connected interface on the upstream device, traffic congestion may occur on the interface of the downstream device. You can configure traffic shaping for queues on the outbound interface of the upstream device and adjust the transmit rate of the interface.

The **qos queue shaping** command configures traffic shaping on packets of a specific service on an interface.

Prerequisites

Priority mapping based on simple traffic classification has been configured to map packet priorities to PHBs and colors, or internal priority re-marking based on complex traffic classification has been configured so that packets of different services enter different queues.

Precautions

If traffic shaping is configured both on an interface queue and an interface (using the **qos lr outbound** command), the CIR of the interface cannot be lower than the sum of CIR values of all the queues on the interface; otherwise, traffic shaping result may be incorrect. For example, the queue with a lower priority may occupy the bandwidth of the queue with a higher priority.

It is recommended that the CBS be 120 times the CIR.

After traffic shaping is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

When interface queue shaping is configured on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, only *pir* and *pbs* take effect, and the maximum value of *pbs* is 16380000.

If you run the **qos queue shaping** command multiple times on the same interface, only the latest configuration takes effect.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, after traffic shaping is configured, statistics on the number of discarded packets in the **display qos queue statistics** command output may be incorrect upon heavy traffic bursts.

If the rate range configured in a version earlier than V200R019C10 exceeds the maximum rate supported by an interface, the corresponding command in the configuration file of the source version can still be delivered after the version is upgraded to V200R019C10 or a later version. However, the maximum rate supported by the interface takes effect.

Example

Set the CIR of queue 4 on the GE0/0/1 to 10000 kbit/s and the PIR to 20000 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos queue 4 shaping cir 10000 pir 20000
[HUAWEI-GigabitEthernet0/0/1] quit
```

15.3.21 reset qos statistics

Function

The **reset qos statistics** command clears traffic statistics on an interface where rate limiting is performed in the inbound direction.

Format

reset qos statistics interface *interface-type interface-number* **inbound**

reset qos statistics inbound all

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears traffic statistics on a specified interface where rate limiting is performed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
inbound	Clears traffic statistics in the inbound direction.	-
all	Clears traffic statistics on all interfaces where rate limiting is performed.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting traffic statistics on an interface where rate limiting is performed in the inbound direction, run the **reset qos statistics** command to clear existing traffic statistics. Then run the **display qos statistics** command to view the traffic statistics.

Prerequisites

The **qos lr inbound** command has been executed to configure rate limiting in the inbound direction on an interface.

Precautions

If the **qos lr inbound** command is not used, the system displays the following error message when you run the **reset qos statistics interface** *interface-type interface-number* **inbound** command:

```
Error: There is no rate limited configuration inbound in the interface.
```

The cleared statistics cannot be restored. Exercise caution when you use this command.

Example

Clear traffic statistics on GE0/0/1 where rate limiting is performed in the inbound direction.

```
<HUAWEI> reset qos statistics interface gigabitethernet 0/0/1 inbound
```

15.4 Congestion Avoidance and Congestion Management Commands

15.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.4.2 color

Function

The **color** command sets parameters of a WRED drop file, including the upper drop threshold, lower drop threshold, and maximum drop probability.

The **undo color** command restores the default settings of a WRED drop profile.

By default, the upper drop threshold, lower drop threshold, and maximum drop probability of a WRED drop profile are all 100.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

color { **green** | **non-tcp** | **red** | **yellow** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*

undo color { **green** | **non-tcp** | **red** | **yellow** }

NOTE

Only the S6735-S, S6720-EI, and S6720S-EI support the **non-tcp** parameter.

Parameters

Parameter	Description	Value
green	Sets WRED parameters for green packets.	-
non-tcp	Sets WRED parameters for non-TCP packets.	-
red	Sets WRED parameters for red packets.	-
yellow	Sets WRED parameters for yellow packets.	-
low-limit *low-limit-percentage*	Specifies the lower drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, the switch starts to discard packets.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 100.
high-limit *high-limit-percentage*	Specifies the upper drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, the switch discards all subsequent packets.	The value is an integer that ranges from *low-limit-percentage* to 100, in percentage. The default value is 100.
discard-percentage *discard-percentage*	Specifies the maximum drop probability.	The value is an integer that ranges from 1 to 100, in percentage. The default value is 100.

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets enter a switch, the switch colors packets based on the mappings defined in a DiffServ domain. The system processes the packets of different colors based on the WRED configuration:

- When the queue length reaches the lower drop threshold, the switch discards some packets.
- When the queue length reaches the upper drop threshold, the switch discards all subsequent packets in the queue.

When congestion occurs, the switch first discards packets with the highest drop probability.

Precautions

If multiple interfaces are congested and packets cannot be forwarded at the line rate on some interfaces on the S5731-H, S5731-S, S5731S-H, and S5731S-S, you can run the **display qos queue statistics** command to check queues in which packets are discarded on the congested interfaces and run the **color** command to decrease the upper drop threshold, lower drop threshold, and maximum drop probability. This ensures that packets can be properly forwarded at the line rate on all interfaces.

If you run the **color** command multiple times in the same drop profile view, only the latest configuration takes effect.

Example

Configure WRED drop profile **wred1** in which the lower drop threshold, upper drop threshold, and maximum drop probability of green packets are set to 80, 100, and 10 for green packets, to 60, 80, and 20 for yellow packets, and to 40, 60, and 40 for red packets.

```
<HUAWEI> system-view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
```

15.4.3 display drop-profile

Function

The **display drop-profile** command displays the WRED drop profile configuration.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display drop-profile [**all** | **name** *drop-profile-name*]

Parameters

Parameter	Description	Value
all	Displays detailed information about all WRED drop profiles.	-
name *drop-profile-name*	Displays detailed information about a WRED drop profile with the specified name.	The value must be the name of an existing WRED drop profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display drop-profile** command to view the number of configured WRED drop profiles and all configuration of a specified WRED drop profile.

Precautions

If the **all** and **name** *drop-profile-name* parameters are not specified, brief information about all WRED drop profiles is displayed.

Example

Display brief information about all WRED drop profiles on the switch.

```
<HUAWEI> display drop-profile
        index                   drop-profile name
-------------------------------------------------------------------
        0                     default
        1                     dp1
-------------------------------------------------------------------
 Total   64     Used   2
```

Display detailed information about the WRED drop profile named **dp1**.

```
<HUAWEI> display drop-profile name dp1
Drop-profile[1]: dp1
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     60          90          20
Yellow    100         100         100
Red       100         100         100
Non-tcp   100         100         100
-------------------------------------------------------------------
```

Display detailed information about all WRED drop profiles on the switch.

```
<HUAWEI> display drop-profile all
Drop-profile[0]: default
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     100         100         100
Yellow    100         100         100
Red       100         100         100
Non-tcp   100         100         100
-------------------------------------------------------------------
Drop-profile[1]: dp1
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     60          90          20
Yellow    100         100         100
Red       100         100         100
Non-tcp   100         100         100
-------------------------------------------------------------------
```

Table 15-28 Description of the **display drop-profile** command output

Item	Description
index	WRED drop profile index.
drop-profile name	WRED drop profile name. To configure a WRED drop profile, run the **drop-profile** command.
Queue depth	Length of a queue. To configure the length of a queue, run the **queue-depth (WRED drop profile view)** command. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this field.
Total	Total number of WRED drop profiles that can be configured on the switch.
Used	Number of configured WRED drop profiles.
Drop-profile[1]	WRED drop profile name in which 1 indicates the drop profile index.

Item	Description
Color	Color of packets: ● Green ● Yellow ● Red ● Non-tcp To set the color of packets, run the **color** command.
Low-limit	Lower drop threshold, in percentage. To set the lower drop threshold, run the **color** command.
High-limit	Upper drop threshold, in percentage. To set the upper drop threshold, run the **color** command.
Discard-percentage	Maximum drop probability, in percentage. To set the maximum drop probability, run the **color** command.

15.4.4 display qos micro-burst peak-buffer verbose interface

Function

The **display qos micro-burst peak-buffer verbose interface** command displays the peak buffer usage and the buffer usage of queues on an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display qos micro-burst peak-buffer verbose interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays buffer information on a specified interface. - *interface-type* specifies an interface type. - *interface-number* specifies an interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos micro-burst peak-buffer verbose interface** *interface-type interface-number* command displays the peak buffer usage and the buffer usage of queues on an interface.

Prerequisites

1. The microburst detection function has been enabled on the switch by running the **qos micro-burst detection** [**enhanced**] **enable slot** *slot-id* command in the system view.
2. The microburst detection function has been enabled on an interface by running the **qos micro-burst detection enable** command in the interface view.

Example

In default microburst detection mode, display the peak buffer usage and the buffer usage of queues on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos micro-burst detection enable slot 0
[HUAWEI] interface gigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos micro-burst detection enable
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] quit
<HUAWEI> display qos micro-burst peak-buffer verbose interface GigabitEthernet 0/0/1
--------------------------------------------------------------------------------------------------------------
P-Buffer     Queue0    Queue1    Queue2    Queue3    Queue4    Queue5    Queue6    Queue7
DateTime
(KB)           (KB)      (KB)      (KB)      (KB)      (KB)      (KB)      (KB)      (KB)
```

```
---------------------------------------------------------------------------------------------------------------
4099            0        0        0        0      4099        0        0        0  2019-08-27 08:43:17
---------------------------------------------------------------------------------------------------------------
```

Table 15-29 Description of the **display qos micro-burst peak-buffer verbose interface** command output

Item	Description
P-Buffer(KB)	Peak value of the buffer usage on the interface.
Queue0(KB)	Buffer usage of queue 0.
Queue1(KB)	Buffer usage of queue 1.
Queue2(KB)	Buffer usage of queue 2.
Queue3(KB)	Buffer usage of queue 3.
Queue4(KB)	Buffer usage of queue 4.
Queue5(KB)	Buffer usage of queue 5.
Queue6(KB)	Buffer usage of queue 6.
Queue7(KB)	Buffer usage of queue 7.
DateTime	Time when the device recorded the entry.

15.4.5 display qos micro-burst statistics interface

Function

The **display qos micro-burst statistics interface** command displays statistics about microburst detection on an interface.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display qos micro-burst statistics interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

In default microburst detection mode, the packet sampling interval is 5 ms. In enhanced microburst detection mode, the packet sampling interval is 1 ms.

The microburst detection period is 5 minutes. That is, key performance indicators of an interface are collected every 5 minutes and related entries are generated. You can run the **display qos micro-burst statistics interface** *interface-type interface-number* command to view statistics collected within the most recent 300 minutes after microburst detection is enabled on an interface, including the average rate of burst traffic, maximum rate of burst traffic, number of discarded packets, average buffer usage on the interface, peak buffer usage on the interface, and entry generation time.

Prerequisites

1. The microburst detection function has been enabled on the device by running the **qos micro-burst detection** [**enhanced**] **enable slot** *slot-id* command in the system view.
2. The microburst detection function has been enabled on an interface by running the **qos micro-burst detection enable** command in the interface view.

Precautions

The average buffer usage and peak buffer usage on an interface cannot be checked on the S5731-H, S5731-S, S5731S-S, and S5731S-H.

Example

In default microburst detection mode, display microburst detection statistics on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos micro-burst detection enable slot 0
[HUAWEI] interface gigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos micro-burst detection enable
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] quit
<HUAWEI> display qos micro-burst statistics interface GigabitEthernet 0/0/1
----------------------------------------------------------------------------------------------------
A-Rate          P-Rate          Discard         A-Buffer        P-Buffer              DateTime
(bps)           (bps)          Packets            (KB)            (KB)
----------------------------------------------------------------------------------------------------
840385600       845712000         29956755            2503            2507      2019-09-28 14:54:43
840561600       845712000         13524346            2503            2507      2019-09-28 14:49:43
----------------------------------------------------------------------------------------------------
```

Table 15-30 Description of the **display qos micro-burst statistics interface** command output

Item	Description
A-Rate(bps)	Average rate of packets forwarded to an interface from any other interfaces on the same device, in bit/s.
P-Rate(bps)	Peak rate of packets forwarded to an interface from any other interfaces on the same device, in bit/s.
Discard Packets	Number of discarded packets.
A-Buffer(KB)	Average buffer usage, in kilobytes.
P-Buffer(KB)	Peak buffer usage, in kilobytes.
DateTime	Time when an entry is generated.

15.4.6 display qos micro-burst status all

Function

The **display qos micro-burst status all** command displays information about all interfaces enabled with microburst detection and packet loss information on the interfaces.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display qos micro-burst status all [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display qos micro-burst status all** [**slot** *slot-id*] command to view information about all interfaces enabled with microburst detection and packet loss information on the interfaces.

Prerequisites

1. The microburst detection function has been enabled on the switch by running the **qos micro-burst detection** [**enhanced**] **enable slot** *slot-id* command in the system view.
2. The microburst detection function has been enabled on an interface by running the **qos micro-burst detection enable** command in the interface view.

Example

In default microburst detection mode, display all interfaces enabled with microburst detection and packet loss information on the interfaces.

```
<HUAWEI> system-view
[HUAWEI] qos micro-burst detection enable slot 0
[HUAWEI] interface gigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos micro-burst detection enable
[HUAWEI-GigabitEthernet0/0/1] quit
<HUAWEI> display qos micro-burst status all
Slot 0                  Mode:default(5ms)
------------------------------------------
Interface               Discard(Packets)
------------------------------------------
GigabitEthernet0/0/1                 0
```

Table 15-31 Description of the **display qos micro-burst status all** command output

Item	Description
Slot	ID of a slot enabled with microburst detection.
Mode	Microburst detection mode: - default(5ms): In default mode, the packet sampling interval is 5 ms. - enhanced(1ms): In enhanced mode, the packet sampling interval is 1 ms.
Interface	Interface enabled with microburst detection.
Discard(Packets)	Number of discarded packets.

15.4.7 display qos queue statistics

Function

The **display qos queue statistics** command displays queue-based traffic statistics on an interface.

Format

display qos queue statistics interface *interface-type interface-number* [**queue** *queue-index*]

display qos queue statistics all

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
interface *interface-type interface-number*	Displays queue-based traffic statistics on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
all	Displays queue-based traffic statistics on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether packets in each queue on an interface are forwarded or discarded due to congestion, run this command to check statistics on each queue on the interface.

To collect queue-based statistics within a certain period, first run the **reset qos queue statistics** command to clear the existing statistics.

The function of displaying queue-based traffic statistics is unavailable to stack ports.

Example

Display queue-based traffic statistics on the GE0/0/1 on the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

```
<HUAWEI> display qos queue statistics interface gigabitethernet 0/0/1
--------------------------------------------------------
 Queue ID          : 0
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
--------------------------------------------------------
 Queue ID          : 1
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
--------------------------------------------------------
 Queue ID          : 2
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
```

```
 Dropped Bytes      : 4,956,144,598
 Dropped Rate(bps) : 106,976
----------------------------------------------------------
 Queue ID          : 3
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
----------------------------------------------------------
 Queue ID          : 4
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
----------------------------------------------------------
 Queue ID          : 5
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
----------------------------------------------------------
 Queue ID          : 6
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
----------------------------------------------------------
 Queue ID          : 7
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
----------------------------------------------------------
```

Table 15-32 Description of the **display qos queue statistics** command output (S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S)

Item	Description
Queue ID	Queue index.
CIR(kbps)	Committed information rate (CIR). By default, the CIR is displayed as 0. If the CIR is configured for queue shaping, the configured CIR is displayed. To set the CIR, run the **qos queue shaping** command.
PIR(kbps)	Peak information rate (PIR). By default, the PIR is displayed as 1000000. If the PIR is configured for queue shaping, the configured PIR is displayed. To set the PIR, run the **qos queue shaping** command.
Used Length(byte)	Maximum number of bytes to be cached in a queue on an interface.
Passed Packets	Number of forwarded packets.
Passed Rate(pps)	Rate of forwarded packets, in pps.
Passed Bytes	Number of forwarded bytes.
Passed Rate(bps)	Rate of forwarded bytes, in bit/s.
Dropped Packets	Number of discarded packets.
Dropped Rate(pps)	Rate of discarded packets, in pps.
Dropped Bytes	Number of discarded bytes.
Dropped Rate(bps)	Rate of discarded bytes, in bit/s.

Display queue-based traffic statistics on GE0/0/1 on the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S6720S-S, and S5735S-S.

```
<HUAWEI> display qos queue statistics interface gigabitethernet 0/0/1
------------------------------------------------------------
 Queue ID          : 0
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
```

```
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
----------------------------------------------------------
 Queue ID          : 1
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
----------------------------------------------------------
 Queue ID          : 2
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
----------------------------------------------------------
 Queue ID          : 3
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
----------------------------------------------------------
 Queue ID          : 4
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
----------------------------------------------------------
 Queue ID          : 5
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
----------------------------------------------------------
 Queue ID          : 6
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 6
 Passed Rate(pps)  : 0
```

```
 Passed Bytes      : 3,042
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
------------------------------------------------------------
 Queue ID          : 7
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
------------------------------------------------------------
```

Table 15-33 Description of the **display qos queue statistics** command output (S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S6720S-S, and S5735S-S)

Item	Description
Queue ID	Queue index.
CIR(kbps)	Committed information rate (CIR). By default, the CIR that is displayed as 0. If the CIR is configured for queue shaping, the configured CIR is displayed. To set the CIR, run the **qos queue shaping** command.
PIR(kbps)	Peak information rate (PIR). By default, the PIR that is displayed as 1000000. If the PIR is configured for queue shaping, the configured PIR is displayed. To set the PIR, run the **qos queue shaping** command.
Passed Packets	Number of forwarded packets.
Passed Rate(pps)	Rate of forwarded packets, in pps.
Passed Bytes	Number of forwarded bytes. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, this field is not supported and is displayed as -.

Item	Description
Passed Rate(bps)	Rate of forwarded bytes, in bit/s. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, this field is not supported and is displayed as -.
Dropped Packets	Number of discarded packets.
Dropped Rate(pps)	Rate of discarded packets, in pps.
Dropped Bytes	Number of discarded bytes. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, this field is not supported and is displayed as -.
Dropped Rate(bps)	Rate of discarded bytes, in bit/s. **NOTE** On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, this field is not supported and is displayed as -.

15.4.8 drop-profile

Function

The **drop-profile** command creates a WRED drop profile and displays the WRED drop profile view, or displays the existing WRED drop profile view.

The **undo drop-profile** command deletes a WRED drop profile.

By default, the system provides a WRED drop profile named **default**.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

drop-profile *drop-profile-name*

undo drop-profile *drop-profile-name*

Parameters

Parameter	Description	Value
drop-profile-name	Specifies the name of a WRED drop profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A WRED drop profile defines WRED parameters for packets of different priorities. After the WRED drop profile is applied to an interface or queues on an interface, congestion avoidance is implemented. The **drop-profile** command creates a WRED drop profile or displays the WRED drop profile view.

Precautions

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support a maximum of 16 WRED drop profiles, and other switches support a maximum of 64 WRED drop profiles, including the default drop profile. The default drop profile can be modified but cannot be deleted.

Follow-up Procedure

1. Set parameters for the WRED drop profile.

   Run the **color** command in the WRED drop profile view to set WRED parameters for packets of different priorities.
2. Apply the WRED drop profile to an interface or queues on an interface.

Example

Create a WRED drop profile named **drop1** and enter the WRED drop profile view.

```
<HUAWEI> system-view
[HUAWEI] drop-profile drop1
[HUAWEI-drop-drop1]
```

15.4.9 qos burst-mode (interface view)

Function

The **qos burst-mode** command configures a burst traffic buffer mode on an interface.

The **undo qos burst-mode** command restores the default burst traffic buffer mode on an interface.

By default, an interface uses the standard mode.

NOTE

Only the S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

qos burst-mode { **enhanced** | **extreme** }

undo qos burst-mode { **enhanced** | **extreme** }

Parameters

Parameter	Description	Value
enhanced	Indicates the enhanced burst traffic buffer mode.	-
extreme	Indicates the extreme burst traffic buffer mode.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The buffer size on an interface is small, and traffic on the live network is not always stable. When the traffic rate on an interface reaches 50% to 60% of the interface bandwidth, packet loss may occur. The burst traffic buffer mode enables an interface to occupy more available buffer space in the system to process burst traffic, improving a switch's packet processing performance.

The device buffer is allocated in static and dynamic modes. By default, each interface is allocated some static buffer space for the basic buffer requirement. The remaining buffer space is used as the dynamic buffer for a switch.

In standard mode, an interface can occupy only some dynamic buffer space on the switch.

In enhanced mode, an interface can occupy only some dynamic buffer space on the switch, and more dynamic buffer space than that in standard mode.

In extreme mode, an interface occupies the dynamic buffer space as well as static buffer space on interfaces in non-extreme mode.

Precautions

The **qos burst-mode (interface view)** and **qos queue buffer shared-ratio** commands cannot be used on the same interface.

When the enhanced mode is used, the **qos burst-mode (interface view)** and **qos burst-mode (system view)** commands cannot be used together.

The **extreme** mode is not recommended because forwarding of other interfaces may be affected and QoS results such as scheduling and shaping results may be incorrect.

The **extreme** mode is used only when the switch uses one or two interfaces. This mode takes effect only when it is configured globally and on an interface. If the **extreme** mode is configured globally but is not configured on an interface, traffic forwarding may be abnormal and multicast packets may fail to be obtained. If the **extreme** mode is configured on an interface but is not configured globally, the **extreme** mode does not take effect.

When the **extreme** mode is configured globally, the interface where the **extreme** mode is not configured cannot be used as a service interface.

Example

Configure the enhanced burst traffic buffer mode on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos burst-mode enhanced
```

15.4.10 qos burst-mode (system view)

Function

The **qos burst-mode** command configures a burst traffic buffer mode on a switch.

The **undo qos burst-mode** command restores the default burst traffic buffer mode on a switch.

By default, the switch uses the standard mode.

NOTE

Only the S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

qos burst-mode { **enhanced** | **extreme** } **slot** *slot-id*

undo qos burst-mode { **enhanced** | **extreme** } **slot** *slot-id*

Parameters

Parameter	Description	Value
enhanced	Indicates the enhanced burst traffic buffer mode.	-
extreme	Indicates the extreme burst traffic buffer mode.	-
slot *slot-id*	The default value of *slot-id* is 0 on a non-stacked switch. *slot-id* specifies the stack ID.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

By default, the buffer size on an interface is small. When the traffic rate on an interface reaches 50% to 60% of the interface bandwidth, packet loss occurs on the interface. After the burst traffic buffer mode is configured on a switch, all interfaces on the switch can occupy more buffer space in the system to process burst traffic, improving a switch's packet processing performance.

The device buffer is allocated in static and dynamic modes. By default, each interface is allocated some static buffer space for the basic buffer requirement. The remaining buffer space is used as the dynamic buffer for a switch.

In standard mode, an interface can occupy only some dynamic buffer space on the switch.

In enhanced mode, an interface can occupy only some dynamic buffer space on the switch, and more dynamic buffer space than that in standard mode.

In extreme mode, an interface occupies the dynamic buffer space as well as static buffer space on interfaces in non-extreme mode.

Precautions

The **qos burst-mode (system view)** and **qos queue buffer shared-ratio** commands cannot be used on the switch simultaneously.

The **extreme** mode is not recommended because forwarding of other interfaces may be affected and QoS results such as scheduling and shaping results may be incorrect.

The **extreme** mode is used only when the switch uses one or two interfaces. This mode takes effect only when it is configured globally and on an interface. If the **extreme** mode is configured globally but is not configured on an interface, traffic forwarding may be abnormal and multicast packets may fail to be obtained. If the **extreme** mode is configured on an interface but is not configured globally, the **extreme** mode does not take effect.

When the **extreme** mode is configured globally, the interface where the **extreme** mode is not configured cannot be used as a service interface.

Example

Configure the enhanced burst traffic buffer mode in slot 0.

```
<HUAWEI> system-view
[HUAWEI] qos burst-mode enhanced slot 0
```

15.4.11 qos dynamic-buffer enable

Function

The **qos dynamic-buffer enable** command enables dynamic queue buffer adjustment.

The **undo qos dynamic-buffer enable** command disables dynamic queue buffer adjustment.

By default, the device does not dynamically adjust the queue buffer.

NOTE

This command is available only on the following switch models:

S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S

Format

qos dynamic-buffer enable

undo qos dynamic-buffer enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos dynamic-buffer enable** command to enable dynamic queue buffer adjustment. This ensures that a queue has sufficient buffer space, preventing packets from being discarded. To configure the interval for dynamically adjusting the queue buffer, run the **qos dynamic-buffer interval** command; to configure the maximum buffer size of a queue for which dynamic buffer adjustment is enabled, run the **qos dynamic-buffer maximum** command.

Precautions

This command takes effect only when multicast entries exist.

Example

Enable the dynamic queue buffer adjustment function.

```
<HUAWEI> system-view
[HUAWEI] qos dynamic-buffer enable
```

15.4.12 qos dynamic-buffer interval

Function

The **qos dynamic-buffer interval** command configures the interval for dynamically adjusting the queue buffer.

The **undo qos dynamic-buffer interval** command restores the default interval for dynamically adjusting the queue buffer.

By default, the device dynamically adjusts the queue buffer at an interval of 100 ms.

NOTE

This command is available only on the following switch models:

S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S

Format

qos dynamic-buffer interval *interval-value*

undo qos dynamic-buffer interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for dynamically adjusting the queue buffer.	The value is an integer in the range from 1 to 10000, in milliseconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos dynamic-buffer enable** command to enable dynamic queue buffer adjustment. This ensures that a queue has sufficient buffer space, preventing packets from being discarded. You can run the **qos dynamic-buffer interval** command to configure the interval for dynamically adjusting the queue buffer. A shorter interval indicates that the device performs dynamic adjustment of the queue buffer more frequently.

Precautions

This command takes effect only after the **qos dynamic-buffer enable** command is run to enable dynamic queue buffer adjustment.

Example

Set the interval for dynamically adjusting the queue buffer to 1000 ms.

```
<HUAWEI> system-view
[HUAWEI] qos dynamic-buffer interval 1000
```

15.4.13 qos dynamic-buffer maximum

Function

The **qos dynamic-buffer maximum** command configures the maximum buffer size of a queue for which dynamic buffer adjustment is enabled.

The **undo qos dynamic-buffer maximum** command restores the default maximum buffer size of a queue for which dynamic buffer adjustment is enabled.

By default, the maximum buffer size of a queue for which dynamic buffer adjustment is enabled is 320 cells. The size of a cell is 128 bytes.

NOTE

This command is available only on the following switch models:

S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S

Format

qos dynamic-buffer maximum *maximum*

undo qos dynamic-buffer maximum

Parameters

Parameter	Description	Value
maximum	Specifies the maximum buffer size of a queue for which dynamic buffer adjustment is enabled.	The value is an integer in the range from 10 to 3500, in cells. The size of a cell is 128 bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos dynamic-buffer enable** command to enable dynamic queue buffer adjustment. This ensures that a queue has sufficient buffer space, preventing packets from being discarded. You can run the **qos dynamic-buffer maximum** command to configure the maximum buffer size of a queue for which dynamic buffer adjustment is enabled.

Precautions

This command takes effect only after the **qos dynamic-buffer enable** command is run to enable dynamic queue buffer adjustment.

Example

Set the maximum buffer size of a queue for which dynamic buffer adjustment is enabled to 100, in cells.

```
<HUAWEI> system-view
[HUAWEI] qos dynamic-buffer maximum 100
```

15.4.14 qos micro-burst detection enable

Function

The **qos micro-burst detection enable** command enables microburst detection.

The **undo qos micro-burst detection enable** command disables microburst detection.

By default, microburst detection is disabled on a switch and interfaces.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

System view:

qos micro-burst detection [**enhanced**] **enable slot** *slot-id*

undo qos micro-burst detection [**enhanced**] **enable slot** *slot-id*

Interface view:

qos micro-burst detection enable

undo qos micro-burst detection enable

Parameters

Parameter	Description	Value
enhanced	Enables microburst detection in enhanced mode. If this parameter is not specified, microburst detection in default mode is enabled.	-
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

System view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To detect microbursts on an outbound interface, you must enable microburst detection on a switch and interfaces. This helps locate packet loss caused by microbursts.

In default microburst detection mode, the packet sampling interval is 5 ms. In enhanced microburst detection mode, the packet sampling interval is 1 ms.

Precautions

Before enabling microburst detection on an interface, you must enable this function on the slot where the interface resides.

In default microburst detection mode, microburst detection can be enabled on multiple interfaces on a switch. In enhanced microburst detection mode, microburst detection can be enabled on only one interface on a switch.

To change the mode of microburst detection, you must delete the existing microburst detection configuration from the switch.

Example

Enable microburst detection in default mode in slot 0 on the switch, and enable microburst detection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos micro-burst detection enable slot 0
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos micro-burst detection enable
```

15.4.15 qos { pq | wrr | drr }

Function

The **qos** { **pq** | **wrr** | **drr** } command configures a scheduling mode for queues on an interface.

The **undo qos** { **pq** | **wrr** | **drr** } command restores the default scheduling mode of queues on an interface.

By default, the scheduling mode of queues on an interface of the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S is WDRR, and the scheduling mode of queues on an interface of other models is WRR.

Format

qos { **pq** | **wrr** | **drr** }

undo qos { **pq** | **wrr** | **drr** }

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command in interface mode.

Only the S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI support this command using a schedule template.

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support **wrr**.

Parameters

Parameter	Description	Value
pq	Indicates the PQ scheduling mode.	-
wrr	Indicates the WRR scheduling mode.	-
drr	Indicates the WDRR scheduling mode.	-

Views

GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view, Scheduling profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs on a network, configure a combination of queue scheduling modes to adjust the delay and jitter of various service packets as follows:

- Packets of delay-sensitive services, such as the voice and video services, are processed preferentially.
- Among the delay-insensitive services, such as the email service, the packets with the same priority are processed equally and the packets with different priorities are processed based on their weights.

The switch supports PQ+WRR and PQ+WDRR. When a combination of queue scheduling modes is used, the switch first schedules the packets in queues using PQ scheduling. When all packets in the queues using PQ scheduling are sent out, the switch schedules the packets in queues using WRR or WDRR scheduling. Packets from the queues using PQ scheduling are scheduled based on packet priorities.

Precautions

- Before configuring a queue scheduling mode, map packet priorities to PHBs and colors or re-mark local priorities of packets. The packets of different priorities enter different queues.
- To set the same queue scheduling mode on multiple interfaces, perform the configuration on a port group to reduce the workload.
- When the scheduling mode of queues on an interface is set to PQ+WRR or PQ +WDRR, a queue can use only one scheduling mode. If you set multiple scheduling modes for a queue, only the latest configuration takes effect.
- If the queue scheduling mode is set to WDRR or WRR on an interface on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735-S-I, and S5735S-S, other interfaces on the switch use the same queue scheduling mode as this interface.
- On the S6720S-S, S5735S-H, and S5736-S, the WRR scheduling changed from WDRR scheduling takes effect only after the switch runs for a period with traffic transmitted.
- For GE interfaces (including XGE interfaces configured with GE optical modules) on the S5731-H, S5731-S, S5731S-H, and S5731S-S, if severe congestions occur, queue scheduling is inaccurate on these interfaces, and traffic forwarding may even be interrupted in some low-priority queues. To prevent this, you are advised to configure congestion avoidance.

Example

Set the scheduling mode of queues on GE0/0/1 of the S5732-H to PQ.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos pq
```

Set the scheduling mode of queues on GE0/0/1 of the S5720-LI to WDRR.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos drr
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
```

15.4.16 qos queue buffer shared-ratio

Function

The **qos queue buffer shared-ratio** command sets the maximum ratio of the dynamic buffer occupied by a queue on an interface.

The **undo qos queue buffer shared-ratio** command restores the default maximum ratio of the dynamic buffer occupied by a queue on an interface.

By default, the maximum ratio of the dynamic buffer occupied by a queue on an interface of the S6735-S, S6720-EI and S6720S-EI is 20%.

NOTE

Only the S6735-S, S6720-EI and S6720S-EI support this command.

Format

qos queue *queue-index* **buffer shared-ratio** *ratio-value*

undo qos queue *queue-index* **buffer shared-ratio**

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
ratio-value	Specifies the maximum ratio of the dynamic buffer occupied by a queue on an interface, in percentage.	The value is an integer that ranges from 1 to 90.

Views

GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the buffer of an interface is small. When the traffic rate on an interface reaches 50% to 60% of the interface bandwidth, packets are lost on the interface. The switch uses static and dynamic modes to allocate the buffer. The switch allocates specified static buffer to each interface, and the remaining buffer is used as the dynamic buffer. When there is heavy burst traffic in a queue on an interface, you can run the **qos queue buffer shared-ratio** command to increase the maximum ratio of the dynamic buffer occupied by the queue. The switch allocates larger dynamic buffer to the queue to reduce packet loss on the queue.

Precautions

The available dynamic buffer on each interface is limited. When a queue on an interface occupies more dynamic buffer, there is less dynamic buffer that can be occupied by other queues on the interface. As a result, the queues' capability to forward burst traffic is lowered.

The **qos queue buffer shared-ratio** and **qos burst-mode (system view)** commands cannot be configured on the switch simultaneously.

The **qos queue buffer shared-ratio** and **qos burst-mode (interface view)** commands cannot be configured on the same interface simultaneously.

Example

Set the maximum ratio of the dynamic buffer occupied by queue 3 on the GE0/0/1 to 35%.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos queue 3 buffer shared-ratio 35
```

15.4.17 qos queue drr

Function

The **qos queue drr** command sets the WDRR weight of queues that participate in WDRR scheduling.

The **undo qos queue drr** command restores the default WDRR weight of queues that participate in WDRR scheduling.

By default, the WDRR weight of queues that participate in WDRR scheduling is 1.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command in interface mode.

Format

qos queue *queue-index* **drr weight** *weight*

undo qos queue *queue-index* **drr**

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
weight *weight*	Specifies a WDRR weight.	The value is an integer that ranges from 0 to 127.

Views

GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view, Scheduling profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WDRR schedules packets based on the packet length used as the weight. If the packet length is too long, WDRR allows the negative weight value so that long packets can be scheduled. In the next round, the queue with the negative weight value is not scheduled until its weight value becomes positive.

WDRR offsets the disadvantages of PQ scheduling and WRR scheduling. In PQ scheduling, packets in queues with lower priorities cannot be scheduled for a long time if congestion occurs. In WRR scheduling, bandwidth is allocated improperly when the packet length of each queue is different or variable.

When WDRR scheduling is used, set the weight for each queue. The switch schedules queues in turn according to the weights.

Precautions

When WDRR scheduling is applied and the weight of a queue is set to 0, the queue uses PQ scheduling and the scheduling mode is PQ+WDRR.

For the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI:

- When configuring the PQ+WDRR scheduling mode, ensure that queues with weight 0 (queues using PQ scheduling) are consecutively configured, without being interrupted by the configuration of the queues using WDRR scheduling.
- If PQ+WDRR scheduling is used and the numbers of the queues using PQ scheduling are consecutive (for example, queue 0, queues 0 and 1, and queues 0 to 2), the device schedules packets in queues using PQ scheduling after scheduling for the packets in queues using WDRR scheduling is completed.

On the S6735-S, S6720-EI and S6720S-EI, if the queue scheduling mode is changed or the weight is changed during queue scheduling, packet loss occurs within 20 ms.

To set the same WDRR weight on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

Set the WDRR weight of queue 4 on GE0/0/1 of the S5732-H to 9.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos drr
[HUAWEI-GigabitEthernet0/0/1] qos queue 4 drr weight 9
```

Set the WDRR weight of queue 4 on GE0/0/1 of the S5720-LI to 9.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos drr
[HUAWEI-qos-schedule-profile-test] qos queue 4 drr weight 9
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
```

15.4.18 qos queue low-limit high-limit

Function

The **qos queue low-limit high-limit** command sets the upper and lower limits for buffering packets in a queue.

The **undo qos queue low-limit high-limit** command restores the default values of the upper and lower limits for buffering packets in a queue.

By default, the upper and lower limits for buffering packets in a queue are 78 and 68 buffer units, respectively. Each buffer unit is 360 bytes.

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S support this command.

Format

qos queue *queue-index* **low-limit** *low-limit-pages* **high-limit** *high-limit-pages*

undo qos queue *queue-index* [**low-limit** *low-limit-pages* **high-limit** *high-limit-pages*]

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer in the range from 0 to 7.
low-limit *low-limit-pages*	Specifies the lower limit for buffering packets in a queue.	The value is an integer in the range from 1 to 5000. Each buffer unit is 360 bytes.
high-limit *high-limit-pages*	Specifies the upper limit for buffering packets in a queue.	The value is an integer in the range from the value of **low-limit** *low-limit-pages* to 5000. Each buffer unit is 360 bytes.

Views

Tail drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs, a switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos queue low-limit high-limit** command to set the upper limit and lower limit for buffering packets in a specified queue on an interface so that the queue has sufficient buffer, preventing packet loss.

When the size of packets in the queue buffer is always lower than or equal to the lower limit (**low-limit** *low-limit-pages*), the switch does not discard any packet. When the size of packets in the buffer increases and is greater than the lower limit:

- If the size of packets in the queue buffer is always less than or equal to the upper limit (**high-limit** *high-limit-pages*), the switch does not discard any packet.
- If the size of packets in the buffer increases gradually or even exceeds the upper limit, the switch discards the packets in the buffer until the size of packets in the queue does not exceed the lower limit.

Prerequisites

A tail drop profile has been created using the **qos tail-drop-profile (system view)** command. Only one tail drop profile can be created on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S.

Example

Create a global tail drop profile named **test**, and set the lower limit and upper limit to 100 and 120 buffer units, respectively, for queue 0.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 0 low-limit 100 high-limit 120
```

15.4.19 qos queue max-buffer

Function

The **qos queue max-buffer** command sets the maximum number of bytes in all packets to be cached in a queue.

The **undo qos queue max-buffer** command restores the default maximum number of bytes in all packets to be cached in a queue.

The **qos queue green max-buffer** command sets the maximum number of bytes in green packets to be cached in a queue.

The **undo qos queue green max-buffer** command restores the default maximum number of bytes in green packets to be cached in a queue.

By default, the maximum buffer size of all packets in a queue is 24 and the maximum buffer size of green packets in a queue is 12, in cells. The size of a cell is 128 bytes.

NOTE

Only the S1720GW-E, S1720GWR-E, S300, S500, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6720S-S, and S5736-S support this command.

Format

qos queue *queue-index* **max-buffer** *cell-number* [**green max-buffer** *cell-number*]

undo qos queue *queue-index* **max-buffer** [*cell-number* **green max-buffer** *cell-number* | **green max-buffer**]

qos queue *queue-index* **green max-buffer** *cell-number*

undo qos queue *queue-index* **green max-buffer**

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
max-buffer *cell-number*	Specifies the maximum number of bytes in all packets to be cached in a queue.	The value is an integer, in cells. The value range is as follows: ● S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, and S5720-LI: from 1 to 5444. ● S5735S-H, S6720S-S, and S5736-S from 1 to 10000. The size of a cell is 128 bytes.
green max-buffer *cell-number*	Specifies the maximum number of bytes in green packets to be cached in a queue.	The value is an integer, in cells. The value range is as follows: ● S5735S-H, S6720S-S, and S5736-S: from 1 to 10000. ● Other models except the S5735S-H, S6720S-S, and S5736-S: from 1 to 5444. The size of a cell is 128 bytes.

Views

Tail drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos queue max-buffer** command to set the maximum number of bytes in all packets or green packets to be cached in a queue so that the queue has sufficient buffer, preventing packet loss.

Prerequisites

A tail drop profile has been created using the **qos tail-drop-profile (system view)** command.

Precautions

You can also use the **qos queue max-length** command to set the maximum number of packets to be cached in a queue. If the maximum number of bytes or packets is reached, the device considers that congestion occurs and will discard subsequent packets.

Example

Create a global tail drop profile named **test**, and then set the maximum buffer size of all packets in a BE queue for the global tail drop profile to 100, in cells.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 0 max-buffer 100
```

15.4.20 qos queue max-length

Function

The **qos queue max-length** command sets the maximum number of packets allowed in a queue.

The **undo qos queue max-length** command restores the default maximum number of packets allowed in a queue.

The **qos queue green max-length** command sets the maximum number of green packets allowed in a queue.

The **undo qos queue green max-length** command restores the default maximum number of green packets allowed in a queue.

By default, the maximum buffer size of all packets in a queue is 22 and the maximum buffer size of green packets in a queue is 11, in packets.

NOTE

Only the S1720GW-E, S1720GWR-E, S300, S500, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6720S-S, and S5736-S support this command.

Format

qos queue *queue-index* **max-length** *packet-number* [**green max-length** *packet-number*]

undo qos queue *queue-index* **max-length** [*packet-number* **green max-length** *packet-number* | **green max-length**]

qos queue *queue-index* **green max-length** *packet-number*

undo qos queue *queue-index* **green max-length**

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
max-length *packet-number*	Specifies the maximum number of packets allowed in a queue.	The value is an integer, in packets. The value range is as follows: ● S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, and S5720-LI: from 1 to 5134. ● S5735S-H, S6720S-S, and S5736-S from 1 to 10000.
green max-length *packet-number*	Specifies the maximum number of green packets to be cached in a queue.	The value is an integer, in packets. The value range is as follows: ● S5735S-H, S6720S-S, and S5736-S: from 1 to 10000. ● Other models except the S5735S-H, S6720S-S, and S5736-S: from 1 to 5134.

Views

Tail drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos queue max-length** command to set the maximum number of packets to be cached in a specified queue on an interface so that the queue has sufficient buffer, preventing packet loss.

Prerequisites

A tail drop profile has been created using the **qos tail-drop-profile (system view)** command.

Precautions

You can also run the **qos queue max-buffer** command to set the maximum number of bytes in all packets to be cached in a queue. If the maximum number of bytes or packets is reached, the device considers that congestion occurs and will discard subsequent packets.

Example

Create a global tail drop template named **test** and set the maximum number of packets to be cached in queue 0 for the global tail drop template to 200.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 0 max-length 200
```

15.4.21 qos queue statistics interval

Function

The **qos queue statistics interval** command sets the interval for checking the rate of discarded packets in a queue.

The **undo qos queue statistics interval** command restores the default interval.

By default, the rate of discarded packets in a queue is checked every 300 seconds.

Format

qos queue statistics interval *interval-value*

undo qos queue statistics interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for checking the rate of discarded packets in a queue.	The value is an integer that ranges from 60 to 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch is managed by a network management system (NMS), the MIB module checks the rate of discarded packets in each queue at intervals and sends the rate to the NMS. You can view the rate of discarded packets in each queue to analyze network performance or locate faults. The **qos queue statistics interval** command sets the interval. The MIB module calculates the average rate at which packets in a queue are discarded at an interval.

Example

Set the interval for checking the rate of discarded packets in a queue to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] qos queue statistics interval 100
```

15.4.22 qos queue wred

Function

The **qos queue wred** command applies a Weighted Random Early Detection (WRED) drop profile to the system or an interface queue.

The **undo qos queue wred** command deletes a WRED drop profile from the system or an interface queue.

By default, no WRED drop profile is applied to the system or an interface queue.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

A WRED drop profile cannot be applied to interfaces 1 to 12 on the S5732-H48S6Q, S5732-H48UM2CC, S5732-H48XUM2CC, and S6730-H48X6C.

Format

qos queue *queue-index* **wred** *drop-profile-name*

undo qos queue *queue-index* **wred**

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
drop-profile-name	Specifies the name of a WRED drop profile.	The value must be the name of an existing WRED drop profile.

Views

System view, GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Tail drop technology processes all packets in the same manner without classifying the packets. When the queue length reaches its maximum value, the packets that were added last (at the tail of the queue) are discarded. This packet drop policy may cause global TCP synchronization. As a result, TCP connections cannot be set up.

Random Early Detection (RED) and WRED are used to avoid global TCP synchronization.

RED and WRED randomly discard packets to prevent global TCP synchronization. When packets of a TCP connection are discarded, packets of other TCP connections can still be sent at a high rate, ensuring bandwidth use efficiency.

Prerequisites

A WRED drop profile has been created using the **drop-profile** command.

Precautions

On the switch, you can apply a WRED drop profile to an interface, the system, or a queue on an interface.

If a WRED drop profile is applied to the system and an interface simultaneously, the WRED drop profile applied to the interface takes effect. After a WRED drop profile is applied to the system, it takes effect on all the interfaces.

If you apply a WRED drop profile to an interface and a queue on an interface simultaneously, the system matches the packets with the profiles applied to the queue and interface in sequence. Then the switch performs congestion avoidance on the packets that match the WRED drop profile.

To apply the same WRED drop profile to queues with the same index on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

Create a WRED drop profile named **wred1** and apply it to queue 1 on the GE0/0/1.

```
<HUAWEI> system view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[HUAWEI-drop-wred1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos queue 1 wred wred1
```

15.4.23 qos queue wrr

Function

The **qos queue wrr** command sets the WRR weight of queues that participate in WRR scheduling.

The **undo qos queue wrr** command restores the default WRR weight of queues that participate in WRR scheduling.

By default, the WRR weight of queues that participate in WRR scheduling is 1.

Format

qos queue *queue-index* **wrr weight** *weight*

undo qos queue *queue-index* **wrr**

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this command.

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, and S6720S-EI support this command in interface mode.

Only the S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI support this command using a schedule template.

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.

Parameter	Description	Value
weight *weight*	Specifies a WRR weight.	The value is an integer that ranges from 0 to 127.

Views

GE interface view, XGE interface view, 40GE interface view, 100GE interface view, port group view, Scheduling profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Weighted Round Robin (WRR) ensures that packets in all the queues are scheduled in turn.

When using WRR scheduling, set the weight for each queue. The switch schedules queues in turn according to the weights.

Precautions

When WRR scheduling is applied and the weight of a queue is set to 0, the queue uses PQ scheduling and the scheduling mode is PQ+WRR.

For the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI:

- When configuring the PQ+WRR scheduling mode, ensure that queues with weight 0 (queues using PQ scheduling) are consecutively configured, without being interrupted by the configuration of the queues using WRR scheduling.
- If PQ+WRR scheduling is used and the numbers of the queues using PQ scheduling are consecutive (for example, queue 0, queues 0 and 1, and queues 0 to 2), the device schedules packets in queues using PQ scheduling after scheduling for the packets in queues using WRR scheduling is completed.

On the S6735-S, S6720-EI and S6720S-EI, if the queue scheduling mode is changed or the weight is changed during queue scheduling, packet loss occurs within 20 ms.

To set the same WRR weight on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

Set the WRR weight of queue 4 on GE0/0/1 of the S5720-LI to 9.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
```

```
[HUAWEI-qos-schedule-profile-test] qos wrr
[HUAWEI-qos-schedule-profile-test] qos queue 4 wrr weight 9
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
[HUAWEI-GigabitEthernet0/0/1] quit
```

15.4.24 qos schedule-profile (interface view)

Function

The **qos schedule-profile** command applies a global scheduling profile to an interface.

The **undo qos schedule-profile** command deletes a global scheduling profile from an interface.

By default, no global scheduling profile is applied to an interface.

NOTE

Only the S1720GW-E, S1720GWR-E, S300, S500, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6720S-S, and S5736-S support this command.

Format

qos schedule-profile *profile-name*

undo qos schedule-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a scheduling profile.	The value must be the name of an existing scheduling profile.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos schedule-profile (system view)** command to create a global scheduling profile, you can run the **qos schedule-profile** command in the interface view to apply the global scheduling profile to an interface to perform queue scheduling.

Example

Create a global scheduling profile named **test**, set the queue scheduling mode to PQ, and then apply the global scheduling profile to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos pq
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
```

15.4.25 qos schedule-profile (system view)

Function

The **qos schedule-profile** command creates a global scheduling profile and displays the scheduling profile view.

The **undo qos schedule-profile** command deletes a created global scheduling profile.

By default, no global scheduling profile is created.

NOTE

Only the S1720GW-E, S1720GWR-E, S300, S500, S5720I-SI, S5720-LI, S5720S-LI, S5735S-H, S6720S-S, and S5736-S support this command.

Format

qos schedule-profile *profile-name*

undo qos schedule-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a scheduling profile.	The value is a string of 1 to 31 case-insensitive characters without spaces. **NOTE** A maximum of six scheduling profiles are allowed; otherwise, the system displays an error message.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos schedule-profile** command in the system view to create a global scheduling profile, you can run the **qos { pq | wrr | drr }** command in the scheduling profile view to configure a queue scheduling mode. You can apply a global scheduling profile to a physical interface to perform queue scheduling.

Example

Create a global scheduling profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test]
```

15.4.26 qos tail-drop-profile (interface view)

Function

The **qos tail-drop-profile** command applies a tail drop profile to an interface.

The **undo qos tail-drop-profile** command deletes a tail drop profile from an interface.

By default, no tail drop profile is applied to an interface.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S support this command.

Format

qos tail-drop-profile *profile-name*

undo qos tail-drop-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a tail drop profile.	The value must be the name of an existing tail drop profile.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos tail-drop-profile (system view)** command to create a global tail drop profile, run the **qos tail-drop-profile** command in the interface view to apply the global tail drop profile to an interface to drop packets at the end of a queue.

Example

Create a global tail drop profile named **test**, set the maximum length of green packets in queue 1 for the global tail drop profile to 10, and then apply the global tail drop profile to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 1 green max-length 10
[HUAWEI-tail-drop-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos tail-drop-profile test
```

15.4.27 qos tail-drop-profile (system view)

Function

The **qos tail-drop-profile** command creates a global tail drop profile and displays the tail drop profile view.

The **undo qos tail-drop-profile** command deletes a global tail drop profile.

By default, no global tail drop profile is created.

NOTE

Only the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S6720S-S, S5735S-S, S5735-S-I, S5735S-H, and S5736-S support this command.

Format

qos tail-drop-profile *profile-name*

undo qos tail-drop-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a tail drop profile.	The value is a string of 1 to 16 case-insensitive characters, without spaces. **NOTE** - For the S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, CloudEngine S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, a maximum of one tail drop profile is allowed; otherwise, the system displays an error message. - For other models, a maximum of six tail drop profiles are allowed; otherwise, the system displays an error message.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos tail-drop-profile** command in the system view to create a tail drop profile, you can run the **qos queue max-length** or **qos queue max-buffer** command in the tail drop profile view to configure a queue. You can apply a global tail drop profile to a physical interface to drop packets at the end of a queue.

Example

Create a global tail drop profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test]
```

15.4.28 qos traffic-manage enable

Function

The **qos traffic-manage enable** command enables the traffic manager (TM) to buffer and schedule packets.

The **undo qos traffic-manage enable** command disables the TM from buffering and scheduling packets.

By default, the TM is enabled to buffer and schedule packets.

NOTE

Only the S5731-S, S5731S-S, S5731-H, and S5731S-H support this command.

Format

qos traffic-manage enable

undo qos traffic-manage enable

Parameters

None

Views

GE interface view, XGE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the TM is enabled to buffer and schedule packets. When heavy traffic needs to be forwarded on all interfaces, the device cannot ensure lossless forwarding. You can run the **undo qos traffic-manage enable** command to disable the TM from buffering and scheduling packets.

Configuration Note

After the **undo qos traffic-manage enable** command is executed, the switch does not support HQoS.

After the **undo qos traffic-manage enable** command is executed, the buffer of the device is greatly reduced.

Example

Configure the TM not to buffer and schedule packets on the GE0/0/1.

```
<HUAWEI> system view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo qos traffic-manage enable
```

15.4.29 qos wred

Function

The **qos wred** command applies a WRED drop profile to an interface.

The **undo qos wred** command deletes a WRED drop profile from an interface.

By default, no WRED drop profile is applied to an interface.

NOTE

Only the S6735-S, S6720-EI and S6720S-EI support this command.

Format

qos wred *drop-profile-name*

undo qos wred

Parameters

Parameter	Description	Value
drop-profile-name	Specifies the name of a WRED drop profile.	The value must be the name of an existing WRED drop profile.

Views

GE interface view, XGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WRED drop profile is applied to an interface, congestion avoidance is implemented on the interface.

Prerequisites

Before applying a WRED drop profile, run the **drop-profile** command to create a WRED drop profile.

Precautions

A WRED drop profile can be applied to an interface or a queue.

If you apply WRED drop profiles to an interface and to a queue on the interface, the system first matches the packets with the profiles applied to the queue and interface in sequence. The system performs congestion avoidance for the packets that match the WRED drop profiles.

To configure the same WRED drop profile on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

Create a WRED drop profile named **wred1** and apply it to the GE0/0/1.

```
<HUAWEI> system view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[HUAWEI-drop-wred1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos wred wred1
[HUAWEI-GigabitEthernet0/0/1] quit
```

15.4.30 qos wred high-limit

Function

The **qos wred high-limit** command configures the Weighted Random Early Detection (WRED) threshold for all port queues.

The **undo qos wred high-limit** command cancels the configuration.

By default, the WRED threshold for all port queues is 100.

NOTE

This command is available only on the S5731-H, S5731-S, S5731S-H, and S5731S-S.

Format

qos wred slot *slot-id* **high-limit** *high-limit-percentage*

undo qos wred slot *slot-id* **high-limit**

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Parameter	Description	Value
high-limit-percentage	Specifies the WRED threshold. When the percentage of the packet count in a queue to the queue length reaches this value, the switch discards all subsequent packets.	The value is an integer in the range from 1 to 100, in percentage.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WRED randomly discards packets based on drop parameters. When packets enter a switch, the switch marks the packets with corresponding colors based on the mappings defined in the DiffServ domain. Then the switch processes the packets of different colors according to the WRED configuration.

To avoid congestion, you can configure WRED and set the same threshold for packets of different colors in all port queues. This simplifies configuration.

Precautions

If the WRED threshold is set and the WRED drop profile is also applied to a port queue, the WRED drop profile applied to the port queue takes effect.

Example

Set the WRED threshold to 90 for all port queues in slot 0.

```
<HUAWEI> system view
[HUAWEI] qos wred slot 0 high-limit 90
```

15.4.31 queue-depth (WRED drop profile view)

Function

The **queue-depth** command sets the length of a queue.

The **undo queue-depth** command restores the default length of a queue.

By default, the system uniformly manages the lengths of queues.

Format

queue-depth *queue-depth-value*

undo queue-depth

📖 **NOTE**

Only the S5731-S, S5731S-S, S5731-H, and S5731S-H support this command.

Parameters

Parameter	Description	Value
queue-depth-value	Specifies the queue length.	The value is an integer that ranges from 1024 to 805306368, in bytes.

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets entering interface queues are processed based on parameters in a WRED drop profile, the percentage of the packet length to the queue length needs to be calculated. When the percentage reaches the lower drop threshold, the switch discards packets based on the drop probability. When the percentage reaches the upper drop threshold, the switch discards all subsequent packets. You can adjust the queue length to optimize the congestion avoidance effect.

Prerequisites

A WRED drop profile has been created and the WRED drop profile view has been displayed.

Precautions

When a small queue length is used, the delay of packets passing a queue is shortened but the queue buffer capability is lowered. When a large queue length is used, the queue buffer capability is improved but the delay of packets passing a queue is extended. In addition, when congestion occurs in a queue, many buffer resources are occupied. In this case, packets in other queues may be discarded due to insufficient buffer resources.

Example

Configure WRED drop profile **wred1** and set the queue length to 2000 bytes.

```
<HUAWEI> system-view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] queue-depth 2000
```

15.4.32 reset qos queue statistics

Function

The **reset qos queue statistics** command clears queue-based traffic statistics on an interface.

Format

reset qos queue statistics interface *interface-type interface-number*

reset qos queue statistics all

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears queue-based traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
all	Clears queue-based traffic statistics on all interfaces.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect queue-based statistics within a certain period, first run the **reset qos queue statistics** command to clear the existing statistics.

Precautions

The cleared queue-based statistics cannot be restored. Therefore, exercise caution when you run the command.

Example

Clear queue-based traffic statistics on the GE0/0/1.

```
<HUAWEI> reset qos queue statistics interface gigabitethernet 0/0/1
```

15.4.33 stack-port qos { pq | wrr | drr }

Function

The **stack-port qos** { **pq** | **wrr** | **drr** } command configures a scheduling mode of queues on an interface of the stack.

The **undo stack-port qos** { **pq** | **wrr** | **drr** } command restores the default scheduling mode of queues on an interface of the stack.

By default, the queue scheduling mode of queues is priority queuing (PQ).

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

stack-port qos { **pq** | **wrr** | **drr** }

undo stack-port qos { **pq** | **wrr** | **drr** }

NOTE

The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support WRR scheduling mode.

Parameters

Parameter	Description	Value
pq	Indicates the PQ scheduling mode.	-
wrr	Indicates the Weighted Round Robin (WRR) scheduling mode.	-
drr	Indicates the Weighted Deficit Round Robin (WDRR) scheduling mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the stack is configured, stack protocol packets and packets between chassis are exchanged on the stack interface. If a large number of packets are exchanged, congestion may occur on the stack interface. As a result, core services such as video and voice services cannot be processed in a timely manner. You can set the scheduling mode on the stack interface so that services with the same priority are processed in the same manner and services with different priorities are processed based on weights.

Precautions

Before setting the scheduling mode of queues, configure priority mapping based on simple traffic classification to map packet priorities to per-hop behaviors (PHBs) and colors or configure internal priority re-marking based on complex traffic classification so that packets of different services enter different queues.

Example

Set the queue scheduling mode on the stack interface to WDRR.

```
<HUAWEI> system view
[HUAWEI] stack-port qos drr
```

15.4.34 stack-port qos queue

Function

The **stack-port qos queue** command configures the WRR or WDRR weight for queues on an interface of the stack.

The **undo stack-port qos queue** command restores the default WRR or WDRR weight for queues on a stack interface.

By default, the WRR or WDRR weight for queues on an interface of the stack is 1.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

stack-port qos queue *queue-index* { **wrr** | **drr** } **weight** *weight*

undo stack-port qos queue *queue-index* { **wrr** | **drr** } [**weight** *weight*]

NOTE

The WRR weight of queues cannot be set on the stack interface of the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
wrr	Indicates the WRR weight.	-
drr	Indicates the WDRR weight.	-
weight *weight*	Specifies the WRR or WDRR weight.	The value is an integer. The value range is 0 to 127.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using WRR or WDRR scheduling, you can set the weight for each queue. Then the switch schedules queues in turn based on the weights. If the weight of a queue is set to 0, the queue uses PQ scheduling. In this case, PQ+WRR or PQ +WDRR is used.

Prerequisites

The **stack-port qos** { **pq** | **wrr** | **drr** } command has been executed to configure the WRR or WDRR scheduling mode of queues on a stack interface.

Example

Set the WDRR weight for queue 1 on the stack interface to 30.

```
<HUAWEI> system view
[HUAWEI] stack-port qos queue 1 drr weight 30
```

15.4.35 stack-port qos schedule-profile

Function

The **stack-port qos schedule-profile** command applies a scheduling profile to a stack interface.

The **undo stack-port qos schedule-profile** command deletes a scheduling profile from a stack interface.

NOTE

The following switches support this command:

- S5720I-SI (excluding the S5720I-10X-PWH-SI-AC and S5720I-6X-PWH-SI-AC), S5720-LI, and S5720S-LI
- S5735S-H, S5736-S, S6720S-S
- S5735-S, S5735S-S

Format

stack-port qos schedule-profile *profile-name*

undo stack-port qos schedule-profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a scheduling profile.	The value must be the name of an existing scheduling profile.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **qos schedule-profile** *profile-name* command is used to create a scheduling profile globally, run this command to apply the scheduling profile. Then the switch schedules traffic on the stack interface based on the scheduling mode defined in the scheduling profile.

Example

Create a scheduling profile named **test** globally, set the queue scheduling mode to PQ, and apply the scheduling profile to the system.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos pq
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] stack-port qos schedule-profile test
```

15.5 Filtering Configuration Commands

15.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.5.2 deny | permit

Function

The **deny** | **permit** command configures access control for service packets based on traffic classifiers.

- The **deny** command prevents service flows that match a specified rule from passing through.
- The **permit** command forwards packets matching traffic classification rules according to the original policy.

The **undo** { **deny** | **permit** } command cancels access control for service packets based on traffic classifiers.

By default, a switch does not control service packets based on traffic classifiers.

Format

deny | **permit**

undo { **deny** | **permit** }

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device implements access control using a traffic policy. That is, you can use a traffic policy containing **deny** | **permit** on the device so that the device provides the firewall function to filter out specified types of packets. The **deny** | **permit** command only filters data packets, but does not process control packets such as STP BPDUs sent to the CPU.

Precautions

When you specify a packet filtering action for packets matching an ACL, if the ACL rule defines **permit**, the device processes packets according to the action (**deny** or **permit**) in the traffic behavior. If the ACL rule defines **deny**, the device discards packets regardless of whether **deny** or **permit** is configured in the traffic behavior.

When you specify the packet filtering action for packets matching an ACL to **deny** or **permit**, if the ACL rule contains the **logging** field, logs are recorded when packets are discarded or forwarded.

If a traffic policy in which the **deny** behavior is defined is applied to the outbound direction on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, control packets of ICMP, OSPF, BGP, RIP, SNMP, and Telnet sent by the CPU are discarded. This affects relevant protocol functions.

In the same traffic behavior, the deny action cannot be used with other traffic actions. Before adding other traffic actions such as re-marking to a traffic behavior, ensure that the traffic behavior does not contain the deny action. If the traffic behavior contains the deny action, configure the permit action before configuring other traffic actions.

Example

Configure a traffic policy **p1** to prevent the packets from VLAN 2 to pass through GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match vlan-id 2
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] deny
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
```

15.6 Redirection Configuration Commands

15.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.6.2 redirect cpu

Function

The **redirect cpu** command configures an action of redirecting packets to the CPU in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to the CPU is not configured in a traffic behavior.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

redirect cpu

undo redirect

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to the CPU.

Precautions

The traffic policy that contains the redirection action can only be applied to the system, an interface, or a VLAN.

NOTICE

After the traffic policy containing **redirect cpu** is used, the traffic matching the traffic classification rule is redirected to the CPU, causing CPU performance to deteriorate. Exercise caution when you run the **redirect cpu** command.

Example

Redirect packets to the CPU in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect cpu
```

15.6.3 redirect interface

Function

The **redirect interface** command configures an action of redirecting packets to an interface in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, no action of redirecting packets to an interface is configured in a traffic behavior.

Format

redirect interface *interface-type interface-number* [**forced**]

undo redirect

NOTE

Tunnel interfaces do not support **forced**.

Only the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the action of redirecting packets to a tunnel interface.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface to which packets are redirected. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
forced	Directly discards packets when the interface is in Down state.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **redirect interface** command configures an action of redirecting packets to an interface in a traffic behavior. For example, packets can be redirected to a firewall for security check.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to an interface.

Precautions

The traffic policy that contains the redirection action can only be applied to the system, an interface, or a VLAN in the inbound direction.

For the S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, packets can be redirected to physical interfaces and Eth-Trunk interfaces in Layer 2 or Layer 3 mode. For other models, packets can be redirected only to physical interfaces and Eth-Trunk interfaces in Layer 2 mode.

The packets that are redirected to an interface will be discarded if the VLAN of the packets on the interface is not allowed.

Example

Redirect packets to GE0/0/1 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect interface gigabitethernet 0/0/1
```

15.6.4 redirect vpn-instance

Function

The **redirect vpn-instance** command configures an action of redirecting packets to a VPN instance in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, no action of redirecting packets to a VPN instance is configured in a traffic behavior.

NOTE

The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735-S, S500, S5735-S-I, S5735S-L, S5735S-L1, S5735S-S, and S5735S-L-M do not support this command.

Format

redirect vpn-instance *vpn-instance-name*

undo redirect

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance to which packets are redirected.	The value must be an existing VPN instance name.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **redirect vpn-instance** command configures an action of redirecting packets to a VPN instance in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to an interface.

Precautions

The traffic policy that contains the redirection action can only be applied to the system, an interface, or a VLAN in the inbound direction.

Example

Redirect packets to the VPN instance named **vpn1** in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect vpn-instance vpn1
```

15.7 Statistics Configuration Commands

15.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.7.2 statistic enable (traffic behavior view)

Function

The **statistic enable** command enables the traffic statistics function in a traffic behavior.

The **undo statistic enable** command disables the traffic statistics function in a traffic behavior.

By default, the traffic statistics function in a traffic behavior is disabled.

Format

statistic enable

undo statistic enable

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the statistics on packets matching a traffic policy, you can use the **statistic enable** command to enable the statistics function. After the statistics function is enabled, you can use the **display traffic policy statistics** command to view the statistics.

Precautions

If only **statistic enable** is configured in a traffic behavior, the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI support packet-based traffic statistics but not byte-based traffic statistics. After the **traffic statistics mode by-bytes** command is configured in the system view and traffic statistics is configured in a traffic policy, the switches support byte-based traffic statistics.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if a traffic policy defining traffic statistics is applied to an Eth-Trunk in the outbound direction, traffic statistics does not take effect for the packets sent by the CPU. In this case, you can configure traffic statistics or port mirroring in the inbound direction on the interface connected to the Eth-Trunk.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the traffic statistics collection function.

Example

Enable the statistics function in traffic behavior **test**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior test
[HUAWEI-behavior-test] statistic enable
```

15.7.3 statistic enable (QoS profile view)

Function

The **statistic enable** command enables traffic statistics in a QoS profile.

The **undo statistic enable** command disables traffic statistics in a QoS profile.

By default, the traffic statistics function is disabled in a QoS profile.

Format

statistic enable

undo statistic enable

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Parameters

None

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **statistic enable** command collects traffic statistics of successfully authenticated online users.

Precautions

When users connected to the device through an Eth-Trunk go online through Portal authentication, the S6720-EI, S6735-S, and S6720S-EI cannot provide traffic statistics for the users.

Example

Enable traffic statistics in the QoS profile **test**

```
<HUAWEI> system-view
[HUAWEI] qos-profile name test
[HUAWEI-qos-test] statistic enable
```

15.8 ACL-based Simplified Traffic Policy Commands

15.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

15.8.2 display traffic-statistics

Function

The **display traffic-statistics** command displays ACL-based traffic statistics.

Format

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*]] [**secure**]

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound acl** *user-acl* [**rule** *rule-id*]

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *bas-acl* | *adv-acl* | *user-acl* } [**rule** *rule-id*]]

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]] [**secure**]

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]]

display traffic-statistics interface inbound [**secure**]

display traffic-statistics interface outbound

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl ipv6** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays ACL-based traffic statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays ACL-based traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If *interface-type interface-number* is not specified, ACL-based traffic statistics on all interfaces are displayed.	-
inbound	Displays ACL-based traffic statistics in the inbound direction.	-
outbound	Displays ACL-based traffic statistics in the outbound direction.	-
acl { *bas-acl* | *adv-acl* | *user-acl* }	Displays traffic statistics on packets matching a specified ACL. • *bas-acl* specifies a basic ACL. • *adv-acl* specifies an advanced ACL. • *user-acl* specifies a user-defined ACL.	The value is an integer. The value ranges are as follows: • The value of *bas-acl* ranges from 2000 to 2999. • The value of *adv-acl* ranges from 3000 to 3999. • The value of *user-acl* ranges from 5000 to 5999.
acl { *acl-name* | *l2-acl* }	Displays traffic statistics on packets matching a specified ACL. • *acl-name* specifies the name of an ACL. • *l2-acl* specifies the number of a Layer 2 ACL.	• The value of *acl-name* must be the name of an existing ACL. • The value of *l2-acl* is an integer that ranges from 4000 to 4999.

Parameter	Description	Value
acl ipv6	Displays traffic statistics based on the IPv6 ACL.	-
rule *rule-id*	Displays traffic statistics on packets matching a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
secure	Displays traffic statistics on packets based on packet filtering policies configured through the **traffic-secure (interface view)** or **traffic-secure (system view)** command.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-statistics** command displays ACL-based traffic statistics on an interface or in a VLAN. The command output helps you learn about forwarded and discarded packets matching the ACL and locate faults.

Prerequisites

The traffic statistics function has been enabled using the **traffic-statistic (interface view)** or **traffic-statistic (system view)** command.

Precautions

Before running the **display traffic-statistics** command to display traffic statistics on packets based on packet filtering policies configured through the **traffic-secure (interface view)** command, you must specify the **secure** parameter in the **traffic-statistic (interface view)** command.

Before running the **display traffic-statistics** command to display traffic statistics on packets based on packet filtering policies configured through the **traffic-secure (system view)** command, you must specify the **secure** parameter in the **traffic-statistic (system view)** command.

On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, if traffic policing and traffic statistics collection based on the same ACL are configured, only statistics on the number of packets matching an ACL, namely, value of **matched** in the **display traffic-statistics** command output, are correct.

Example

Display statistics on packets matching ACL 3009 in the inbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl 3009
[HUAWEI-acl-adv-3009] rule 1 permit ip
[HUAWEI-acl-adv-3009] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-statistic inbound acl 3009
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] display traffic-statistics interface gigabitethernet 0/0/1 inbound acl 3009
--------------------------------------------------------------------------------
Interface GigabitEthernet0/0/1
 ACL:3009 Rule:1
     matched:0 packets, passed:0 packets, dropped:0 packets
```

Table 15-34 Description of the **display traffic-statistics** command output

Item	Description
ACL	ACL number.
Rule	ACL rule ID.
matched	Number of packets matching the ACL.
passed	Number of forwarded packets.
dropped	Number of discarded packets.

15.8.3 reset traffic-statistics

Function

The **reset traffic-statistics** command clears ACL-based traffic statistics.

Format

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*]] [**secure**]

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound acl** *user-acl* [**rule** *rule-id*]

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *bas-acl* | *adv-acl* | *user-acl* } [**rule** *rule-id*]]

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **inbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]] [**secure**]

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] **outbound** [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]]

reset traffic-statistics { **interface** | **vlan** } **inbound** [**secure**]

reset traffic-statistics { **interface** | **vlan** } **outbound**

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl ipv6** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears ACL-based traffic statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Clears ACL-based traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If *interface-type interface-number* is not specified, ACL-based traffic statistics on all interfaces are cleared.	-
inbound	Clears ACL-based traffic statistics in the inbound direction.	-
outbound	Clears ACL-based traffic statistics in the outbound direction.	-

Parameter	Description	Value
acl { *bas-acl* | *adv-acl* | *user-acl* }	Clears traffic statistics on packets matching a specified ACL. ● *bas-acl* specifies a basic ACL. ● *adv-acl* specifies an advanced ACL. ● *user-acl* specifies a user-defined ACL.	The value is an integer. The value ranges are as follows: ● The value of *bas-acl* ranges from 2000 to 2999. ● The value of *adv-acl* ranges from 3000 to 3999. ● The value of *user-acl* ranges from 5000 to 5999.
acl { *acl-name* | *l2-acl* }	Clears traffic statistics on packets matching a specified ACL. ● *acl-name* specifies the name of an ACL. ● *l2-acl* specifies the number of a Layer 2 ACL.	● The value of *acl-name* must be the name of an existing ACL. ● The value of *l2-acl* is an integer that ranges from 4000 to 4999.
acl ipv6	Clears traffic statistics based on the IPv6 ACL.	-
rule *rule-id*	Clears traffic statistics on packets matching a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
secure	Clears traffic statistics on packets based on packet filtering policies configured through the **traffic-secure (interface view)** or **traffic-secure (system view)** command.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before re-collecting ACL-based traffic statistics, run the **reset traffic-statistics** command to clear existing statistics. Then run the **display traffic-statistics** command to view ACL-based traffic statistics.

Precautions

After the **reset traffic-statistics** command is executed, statistics are cleared and cannot be restored. Exercise caution when you use this command.

Example

Clear statistics about incoming packets that match rule 5 in the ACL named **test** on GE0/0/1.

```
<HUAWEI> reset traffic-statistics interface gigabitethernet 0/0/1 inbound acl test rule 5
```

15.8.4 traffic-delete fast-mode enable

Function

The **traffic-delete fast-mode enable** command enables the device to rapidly delete ACL-based simplified traffic policies.

The **undo traffic-delete fast-mode enable** command disables the device from rapidly deleting ACL-based simplified traffic policies.

By default, the device is disabled from rapidly deleting ACL-based simplified traffic policies.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

traffic-delete fast-mode enable

undo traffic-delete fast-mode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple ACL-based simplified traffic policies are configured and the ACL contains a large number of rules, it takes a long time for the device to delete the traffic policies. To solve the problem, run the **traffic-delete fast-mode enable** command to enable the device to rapidly delete ACL-based simplified traffic policies.

Precautions

After the **traffic-delete fast-mode enable** command is executed, the traffic policy statistics are cleared.

After the **traffic-delete fast-mode enable** command is used, if you configure a new ACL-based simplified traffic policy, the original ACL-based simplified traffic policy becomes invalid temporarily and takes effect only when the new ACL-based simplified traffic policy is applied successfully.

Example

Enable the device to rapidly delete ACL-based simplified traffic policies.

```
<HUAWEI> system-view
[HUAWEI] traffic-delete fast-mode enable
```

15.8.5 traffic-filter (interface view)

Function

The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.

The **undo traffic-filter** command cancels the configuration.

By default, no ACL is applied to an interface to filter packets on the interface.

Format

Use the following command in the inbound direction on an interface:

traffic-filter inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

undo traffic-filter inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following command in the inbound direction on a tunnel interface:

traffic-filter inbound acl { *adv-acl* | *ucl-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter inbound acl { *adv-acl* | *ucl-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

ACL-based packet filtering can be configured on the tunnel interface in the inbound direction only on the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Use the following command in the outbound direction on an interface:

traffic-filter outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

undo traffic-filter outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-filter { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-filter { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction on an interface.	-
outbound	Configures ACL-based packet filtering in the outbound direction on an interface.	-
acl	Filters packets based on the IPv4 ACL.	-
ipv6	Filters packets based on the IPv6 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer in the range from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer in the range from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer in the range from 4000 to 4999.
user-acl	Filters packets based on a specified user-defined ACL.	The value is an integer in the range from 5000 to 5999.

Parameter	Description	Value
ucl-acl	Filters packets based on a specified user ACL.	The value is an integer in the range from 6000 to 9999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The value is an integer in the range from 0 to 4294967294.

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed on an interface, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

If the **traffic-filter (system view)** and **traffic-filter (interface view)** commands are used simultaneously, and the associated ACLs are non-user-defined ACLs, the **traffic-filter (interface view)** command takes effect.

When the deny action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can only be associated with the **traffic-mirror (interface view)**, **traffic-mirror (system view)**, **traffic-statistic (interface view)**, or **traffic-statistic (system view)** command. If the ACL rule is associated with other simplified traffic policies, the simplified traffic policies may not take effect.

When the permit action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can be associated with other simplified traffic policies.

When the ACL rule containing the **logging** field is associated with the **traffic-filter** command, logs are recorded when packets are discarded or forwarded.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based packet filtering on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based packet filtering is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based packet filtering.

If an ACL rule defines **deny** and **traffic-filter** based on the ACL is applied to the outbound direction on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, when packets match the ACL rule, control packets of ICMP, OSPF, BGP, RIP, SNMP, and Telnet sent by the CPU are discarded. This affects relevant protocol functions.

Example

On the GE0/0/1, configure packet filtering based on the ACL that rejects packets with source IP address 192.168.0.2/32.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 deny ip source 192.168.0.2 0
```

```
[HUAWEI-acl-adv-3000] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-filter inbound acl 3000
```

15.8.6 traffic-filter (system view)

Function

The **traffic-filter** command configures ACL-based packet filtering globally or in a VLAN.

The **undo traffic-filter** command cancels ACL-based packet filtering globally or in a VLAN.

By default, ACL-based packet filtering is not configured globally or in a VLAN.

NOTE

When ACL-based packet filtering is implemented in the system or in a VLAN, the ACL number is in the range of 2000 to 5999. When ACL-based packet filtering is implemented for user access control on the NAC network, the ACL number is in the range of 6000 to 9999. See **traffic-filter acl**.

Format

To configure ACL-based packet filtering in the inbound direction on a switch, use the following command:

traffic-filter [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

traffic-filter inbound acl [**ipv6**] *ucl-acl*

undo traffic-filter inbound acl [**ipv6**] *ucl-acl*

To configure ACL-based packet filtering in the outbound direction on a switch, use the following command:

traffic-filter [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] {*bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based packet filtering in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Configures ACL-based packet filtering in the inbound direction.	-
outbound	Configures ACL-based packet filtering in the outbound direction. **NOTE** Packet filtering based on the user-defined ACL cannot be applied to the outbound direction.	-
acl	Filters packets based on the IPv4 ACL.	-
ipv6	Filters packets based on the IPv6 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Filters packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Specifies the name of an ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed on the device, the device filters packets matching an ACL rule:

- If the action in the ACL rule is **deny**, the device discards packets matching the rule.
- If the action in the ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-filter (system view)** and **traffic-filter (interface view)** commands are used simultaneously, and the associated ACLs are non-user-defined ACL, the **traffic-filter (interface view)** command takes effect.

When the deny action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can only be associated with the **traffic-mirror (interface view)**, **traffic-mirror (system view)**, **traffic-statistic (interface view)**, or **traffic-statistic (system view)** command. If the ACL rule is associated with other simplified traffic policies, the simplified traffic policies may not take effect.

When the permit action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can be associated with other simplified traffic policies.

When the ACL rule containing the **logging** field is associated with the **traffic-filter** command, logs are recorded when packets are discarded or forwarded.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based packet filtering on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based packet filtering is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based packet filtering.

If an ACL rule defines **deny** and **traffic-filter** based on the ACL is applied to the outbound direction on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, when packets match the ACL rule, control packets of ICMP, OSPF, BGP, RIP, SNMP, and Telnet sent by the CPU are discarded. This affects relevant protocol functions.

Example

Configure ACL-based packet filtering in VLAN 100. The ACL rejects packets with source IP address 192.168.0.2/32.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] acl name test 3000
[HUAWEI-acl-adv-test] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-test] quit
[HUAWEI] traffic-filter vlan 100 inbound acl name test
```

15.8.7 traffic-limit (interface view)

Function

The **traffic-limit** command configures ACL-based traffic policing on an interface.

The **undo traffic-limit** command cancels ACL-based traffic policing on an interface.

By default, ACL-based traffic policing is not configured on an interface.

Format

Use the following command in the inbound direction on a switch interface:

traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following command in the outbound direction on a switch interface:

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]] (S6735-S, S6720-EI, S6720S-EI)

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S)

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the inbound direction on a switch interface, use the following command:

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-*

value **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the outbound direction on a switch interface, use the following command:

traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-*

value **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Performs traffic policing for packets in the inbound direction of an interface.	-
outbound	Performs traffic policing for packets in the outbound direction of an interface.	-
acl	Performs traffic policing for packets based on the IPv4 ACL.	-
ipv6	Performs traffic policing for packets based on the IPv6 ACL.	-
bas-acl	Performs traffic policing for packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Performs traffic policing for packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Performs traffic policing for packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Performs traffic policing for packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.

Parameter	Description	Value
name *acl-name*	Performs traffic policing for packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Performs traffic policing for packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be greater than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. The default CBS is 125 times the CIR. If the CIR multiplied by 125 is smaller than 4000, the default CBS is 4000.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 125 times the CIR. If the PIR is set, the default PBS is 125 times the PIR. If the CIR or PIR multiplied by 125 is smaller than 4000, the default PBS is 4000.
green	Performs traffic policing for green packets. By default, green packets are allowed to pass through.	-

Parameter	Description	Value
yellow	Performs traffic policing for yellow packets. By default, yellow packets are allowed to pass through.	-
red	Performs traffic policing for red packets. By default, red packets are discarded.	-
remark-8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7.
remark-dscp *dscp-value*	Re-marks the DSCP priority in packets.	The value is an integer that ranges from 0 to 63.
drop	Indicates that packets are discarded.	-
pass	Indicates that packets are allowed to pass through.	-

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-limit** command is executed on an interface, the device limits the rate and remarks the 802.1p or DSCP priority of packets matching an ACL.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

If the **traffic-limit (system view)** and **traffic-limit (interface view)** commands are used simultaneously, the **traffic-limit (interface view)** command takes effect.

When the **traffic-limit (interface view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, the traffic rate is limited.

If the **traffic-limit** command with the same ACL rule specified is executed two or more times in the interface view, the system displays the following information:

```
Error:Sacl does not support config the same acl or rule repeatedly.
```

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based traffic policing on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based traffic policing is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic policing.

Example

Configure ACL-based traffic policing in the inbound direction on GE0/0/1, set the CIR to 10000 kbit/s for packets matching ACL 3000, configure GE0/0/1 to allow green packets, yellow packets, and red packets to pass through, and re-mark the DSCP priority of red packets with 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-limit inbound acl 3000 cir 10000 green pass yellow pass red
pass remark-dscp 5
```

15.8.8 traffic-limit (system view)

Function

The **traffic-limit** command configures ACL-based traffic policing globally or in a VLAN.

The **undo traffic-limit** command cancels ACL-based traffic policing globally or in a VLAN.

By default, ACL-based traffic policing is not configured globally or in a VLAN.

Format

To configure ACL-based traffic policing in the inbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

To configure ACL-based traffic policing in the outbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]] (S6735-S, S6720-EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp**

dscp-value] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the inbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-*

value] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the outbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI)

undo traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
inbound	Performs traffic policing for packets in the inbound direction.	-
outbound	Performs traffic policing for packets in the outbound direction.	-
acl	Performs traffic policing for packets based on the IPv4 ACL.	-
ipv6	Performs traffic policing for packets based on the IPv6 ACL.	-
bas-acl	Performs traffic policing for packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Performs traffic policing for packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Performs traffic policing for packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Performs traffic policing for packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Performs traffic policing for packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Performs traffic policing for packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be greater than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. The default CBS is 125 times the CIR. If the CIR multiplied by 125 is smaller than 4000, the default CBS is 4000.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 125 times the CIR. If the PIR is set, the default PBS is 125 times the PIR. If the CIR or PIR multiplied by 125 is smaller than 4000, the default PBS is 4000.
green	Performs traffic policing for green packets. By default, green packets are allowed to pass through.	-
yellow	Performs traffic policing for yellow packets. By default, yellow packets are allowed to pass through.	-
red	Performs traffic policing for red packets. By default, red packets are discarded.	-

Parameter	Description	Value
remark-8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7.
remark-dscp *dscp-value*	Re-marks the DSCP priority in packets.	The value is an integer that ranges from 0 to 63.
drop	Indicates that packets are discarded.	-
pass	Indicates that packets are allowed to pass through.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-limit** command is executed on the device, the device limits the rate and remarks the 802.1p or DSCP priority of packets matching an ACL.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-limit (interface view)** and **traffic-limit (system view)** commands are used simultaneously, the **traffic-limit (interface view)** command takes effect.

When the **traffic-limit (system view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, the traffic rate is limited.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based traffic policing on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based traffic policing is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic policing.

Example

In the inbound direction in VLAN 100, configure traffic policing based on ACL 3000, set the CIR to 10000 kbit/s, and configure the device to permit green and yellow packets to pass through and to discard red packets.

```
<HUAWEI> system-view
[HUAWEI] traffic-limit vlan 100 inbound acl 3000 cir 10000 green pass yellow pass red drop
```

15.8.9 traffic-mirror (interface view)

Function

The **traffic-mirror** command configures ACL-based flow mirroring on an interface.

The **undo traffic-mirror** command cancels ACL-based flow mirroring on an interface.

By default, ACL-based flow mirroring is not configured on an interface.

Format

To configure a single ACL, use the following command:

traffic-mirror inbound { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-mirror inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Mirrors packets in the inbound direction on an interface.	-
acl	Mirrors packets based on the IPv4 ACL.	-
ipv6	Mirrors packets based on the IPv6 ACL.	-
bas-acl	Mirrors packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Mirrors packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Mirrors packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Mirrors packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Mirrors packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Mirrors packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.

Parameter	Description	Value
to observe-port *o-index*	Specifies the index of the observing port to which packets are mirrored.	The value is an integer and the value range depends on the product model: - S1720GW-E, S1720GWR-E, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, and S5720-LI: 1 - S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1 to 8

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **traffic-mirror** command is configured, the device can perform flow mirroring or remote flow mirroring, without affecting traffic forwarding.

Prerequisites

An observing port has been created through the **observe-port (local mirroring)** or **observe-port (remote mirroring)** command.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

If the **traffic-mirror (system view)** and **traffic-mirror (interface view)** commands are used simultaneously, the **traffic-mirror (interface view)** command takes effect.

Example

Configure ACL-based flow mirroring in the inbound direction on GE0/0/1, and mirror the packets matching ACL 3000 to the observing port with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-mirror inbound acl 3000 to observe-port 1
```

15.8.10 traffic-mirror (system view)

Function

The **traffic-mirror** command configures ACL-based flow mirroring globally or in a VLAN.

The **undo traffic-mirror** command cancels ACL-based flow mirroring globally or in a VLAN.

By default, ACL-based flow mirroring is not configured globally or in a VLAN.

Format

To configure a single ACL, use the following command:

traffic-mirror [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-mirror [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
inbound	Mirrors packets in the inbound direction.	-
acl	Mirrors packets based on the IPv4 ACL.	-
ipv6	Mirrors packets based on the IPv6 ACL.	-
bas-acl	Mirrors packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Mirrors packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Mirrors packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Mirrors packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Mirrors packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Parameter	Description	Value
rule *rule-id*	Mirrors packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
to observe-port *o-index*	Specifies the index of the observing port to which packets are mirrored.	The value is an integer and the value range depends on the product model: • S1720GW-E, S1720GWR-E, S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S, and S5720-LI: 1 • S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: 1 to 8

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **traffic-mirror** command is configured, the device can perform flow mirroring or remote flow mirroring, without affecting traffic forwarding.

Prerequisites

An observing port has been created through the **observe-port (local mirroring)** or **observe-port (remote mirroring)** command.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-mirror (interface view)** and **traffic-mirror (system view)** commands are used simultaneously, the **traffic-mirror (interface view)** command takes effect.

Example

Configure ACL-based flow mirroring in the inbound direction in VLAN 100, and mirror the packets matching ACL 3000 to the observing port with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] traffic-mirror vlan 100 inbound acl 3000 to observe-port 1
```

15.8.11 traffic-redirect (interface view)

Function

The **traffic-redirect** command configures ACL-based redirection on an interface.

The **undo traffic-redirect** command cancels ACL-based redirection on an interface.

By default, ACL-based redirection is not configured on an interface.

Format

To configure a single ACL, use the following command:

traffic-redirect inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following command on a tunnel interface:

traffic-redirect inbound acl { *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **interface tunnel** *interface-number* [**force**]

undo traffic-redirect inbound acl { *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect inbound acl *ucl-acl* **interface tunnel** *interface-number* [**force**]

undo traffic-redirect inbound acl *ucl-acl*

NOTE

ACL-based redirection can be configured in the inbound direction of a tunnel interface only on the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-redirect inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vpn-instance** *vpn-instance-name*.

Parameters

Parameter	Description	Value
inbound	Redirects packets in the inbound direction on an interface.	-

Parameter	Description	Value
acl	Redirects packets based on the IPv4 ACL.	-
ipv6	Redirects packets based on the IPv6 ACL.	-
bas-acl	Redirects packets based on a specified basic ACL.	The value is an integer in the range from 2000 to 2999.
adv-acl	Redirects packets based on a specified advanced ACL.	The value is an integer in the range from 3000 to 3999.
l2-acl	Redirects packets based on a specified Layer 2 ACL.	The value is an integer in the range from 4000 to 4999.
user-acl	Redirects packets based on a specified user-defined ACL.	The value is an integer in the range from 5000 to 5999.
ucl-acl	Redirects packets based on a user ACL.	The value is an integer in the range from 6000 to 9999.
name *acl-name*	Redirects packets based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Redirects packets based on a specified ACL rule.	The value is an integer in the range from 0 to 4294967294.
cpu	Redirects packets to the CPU.	-
interface *interface-type interface-number*	Redirects packets to a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
remote	Redirects packets to a remote next hop.	-
vpn-instance *vpn-instance-name*	Redirects packets to a VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
ip-nexthop *ip-nexthop*	Redirects packets to a next-hop IPv4 address.	The value is in dotted decimal notation.
ipv6-nexthop *ipv6-nexthop*	Redirects packets to a next-hop IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv6-nexthop link-local *link-local-address* **interface** *interface-type interface-number*	Redirects packets to the IPv6 link-local address of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. When the link-local address is configured, the IPv6 address prefix should match FE80::/10.	The link-local address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-redirect** command is executed on an interface, the device redirects packets matching an ACL to the CPU, a specified interface, or a specified next-hop address.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

If the **traffic-redirect (system view)** and **traffic-redirect (interface view)** commands are used simultaneously, the **traffic-redirect (interface view)** command takes effect.

When the **traffic-redirect (interface view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is redirected.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, if traffic matching **traffic-redirect (interface view)** also matches **traffic-secure (interface view)** or **traffic-secure (system view)**, **traffic-redirect (interface view)** takes effect. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the ACL defines the permit action, **traffic-secure (interface view)** or **traffic-secure (system view)** and **traffic-redirect (interface view)** take effect.

Before redirecting packets to an IPv6 address using this command, run the **ipv6 neighbor** command to configure a static neighbor.

Redirection to a next hop only takes effect on L3 traffic for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735-S-I, and S5735S-S.

NOTICE

If packets are redirected to the CPU, a large number of packets will be sent to the CPU, affecting normal services. Exercise caution when you configure redirection to the CPU.

Example

Configure ACL-based redirection in the inbound direction on GE0/0/1, and redirect packets matching ACL 3000 to GE0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-redirect inbound acl 3000 interface gigabitethernet 0/0/2
```

15.8.12 traffic-redirect (system view)

Function

The **traffic-redirect** command configures ACL-based redirection globally or in a VLAN.

The **undo traffic-redirect** command cancels ACL-based redirection globally or in a VLAN.

By default, ACL-based redirection is not configured globally or in a VLAN.

NOTE

When ACL-based redirection is implemented in the system or in a VLAN, the ACL number is in the range of 2000 to 5999. When ACL-based redirection is implemented on the NAC network, the ACL number is in the range of 6000 to 9999. See **traffic-redirect acl**.

Format

To configure a single ACL, use the following command:

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-redirect [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | { [**remote**] { [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } } }

traffic-redirect [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } **ipv6-nexthop link-local** *link-local-address* **interface** *interface-type interface-number*

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vpn-instance** *vpn-instance-name*.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
inbound	Redirects packets to the inbound direction.	-
acl	Redirects packets based on the IPv4 ACL.	-
ipv6	Redirects packets based on the IPv6 ACL.	-
bas-acl	Redirects packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Redirects packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Redirects packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Redirects packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.

Parameter	Description	Value
name *acl-name*	Redirects packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Redirects packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
cpu	Redirects packets to the CPU.	-
interface *interface-type interface-number*	Redirects packets to a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
remote	Redirects packets to a remote next hop.	-
vpn-instance *vpn-instance-name*	Redirects packets to a VPN instance.	The value must be an existing VPN instance name.
ip-nexthop *ip-nexthop*	Redirects packets to a next-hop IPv4 address.	The value is in dotted decimal notation.
ipv6-nexthop *ipv6-nexthop*	Redirects packets to a next-hop IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-nexthop link-local *link-local-address* **interface** *interface-type interface-number*	Redirects packets to the IPv6 link-local address of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. When the link-local address is configured, the IPv6 address prefix should match FE80::/10.	The link-local address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-redirect** command is executed on the device, the device redirects packets matching an ACL to the CPU, a specified interface, or a specified next hop address.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-redirect (interface view)** and **traffic-redirect (system view)** commands are used simultaneously, the **traffic-redirect (interface view)** command takes effect.

When the **traffic-redirect (system view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is redirected.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, if traffic matching **traffic-redirect (system view)** also matches **traffic-secure (interface view)** or **traffic-secure (system view)**, **traffic-redirect (system view)** takes effect. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the ACL defines the permit action, **traffic-secure (interface view)** or **traffic-secure (system view)** and **traffic-redirect (system view)** take effect.

Before redirecting packets to an IPv6 address using this command, run the **ipv6 neighbor** command to configure a static neighbor.

Redirection to a next hop only takes effect on L3 traffic for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735-S-I, and S5735S-S.

NOTICE

If packets are redirected to the CPU, a large number of packets will be sent to the CPU, affecting normal services. Exercise caution when you configure redirection to the CPU.

Example

Configure ACL-based redirection in the inbound direction in VLAN 100, and redirect packets matching ACL 3000 to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] traffic-redirect vlan 100 inbound acl 3000 interface gigabitethernet 0/0/1
```

15.8.13 traffic-remark (interface view)

Function

The **traffic-remark** command configures ACL-based re-marking on an interface.

The **undo traffic-remark** command cancels ACL-based re-marking on an interface.

By default, ACL-based re-marking is not configured on an interface.

Format

To configure ACL-based re-marking in the inbound direction on a switch interface, use the following command:

traffic-remark inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

To configure ACL-based re-marking in the outbound direction on a switch interface, use the following command:

traffic-remark outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the inbound direction on a switch interface, use the following command:

traffic-remark inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the outbound direction on a switch interface, use the following command:

traffic-remark outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

Parameters

Parameter	Description	Value
inbound	Re-marks packets in the inbound direction.	-
outbound	Re-marks packets in the outbound direction.	-

Parameter	Description	Value
acl	Re-marks packets based on the IPv4 ACL.	-
ipv6	Re-marks packets based on the IPv6 ACL.	-
bas-acl	Re-marks packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Re-marks packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Re-marks packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Re-marks packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Re-marks packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Re-marks packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
cvlan-id *cvlan-id*	Re-marks the inner VLAN tag in QinQ packets. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **cvlan-id** *cvlan-id*.	The value is an integer that ranges from 1 to 4094.
destination-mac *mac-address*	Re-marks the destination MAC address in packets. **NOTE** Only the S6735-S, S6720-EI and S6720S-EI support **destination-mac** *mac-address*.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
dscp { *dscp-name* | *dscp-value* }	Re-marks the DSCP service type in packets.	The value can be an integer in the range of 0 to 63, or DSCP service name, for example, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values corresponding to DSCP service names are as follows: • af11: 10 • af12: 12 • af13: 14 • af21: 18 • af22: 20 • af23: 22 • af31: 26 • af32: 28 • af33: 30 • af41: 34 • af42: 36 • af43: 38 • cs1: 8 • cs2: 16 • cs3: 24 • cs4: 32 • cs5: 40 • cs6: 48 • cs7: 56 • default: 0 • ef: 46 By default, the *dscp-value* is 0.
local-precedence *local-precedence-value*	Re-marks the local IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
ip-precedence *ip-precedence-value*	Re-marks the IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
vlan-id *vlan-id*	Re-marks the VLAN ID in packets.	The value is an integer that ranges from 1 to 4094.

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-remark** command is executed on an interface, the device re-marks packets matching an ACL, for example, 802.1p priority, inner VLAN tag in QinQ packets, destination MAC address, DSCP service type, local IP precedence, IP precedence, and VLAN ID.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied

to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

- The destination MAC address and VLAN ID in packets cannot be re-marked.

If the **traffic-remark (system view)** and **traffic-remark (interface view)** commands are used simultaneously, the **traffic-remark (interface view)** command takes effect.

When the **traffic-remark (interface view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is re-marked.

Outbound ACL-based re-marking on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based re-marking is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based re-marking.

Example

Configure ACL-based re-marking in the inbound direction on GE0/0/1, and re-mark the VLAN ID in packets from source MAC address 0-0-1 with 100.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule 5 permit source-mac 0-0-1
[HUAWEI-acl-L2-4001] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-remark inbound acl 4001 rule 5 vlan-id 100
```

15.8.14 traffic-remark (system view)

Function

The **traffic-remark** command configures ACL-based re-marking globally or in a VLAN.

The **undo traffic-remark** command cancels ACL-based re-marking globally or in a VLAN.

By default, ACL-based re-marking is not configured globally or in a VLAN.

Format

To configure ACL-based re-marking in the inbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-**

mac *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark inbound acl { **name** *acl-name* | *ucl-acl* } **local-precedence** *local-precedence-value*

NOTE

The function of re-marking the internal priority of packets based on a user ACL is available only on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S.

To configure ACL-based re-marking in the outbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the inbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the outbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based re-marking in a specified VLAN.	The value is an integer in the range from 1 to 4094.
inbound	Re-marks packets in the inbound direction.	-
outbound	Re-marks packets in the outbound direction.	-
acl	Re-marks packets based on the IPv4 ACL.	-
ipv6	Re-marks packets based on the IPv6 ACL.	-
bas-acl	Re-marks packets based on a specified basic ACL.	The value is an integer in the range from 2000 to 2999.
adv-acl	Re-marks packets based on a specified advanced ACL.	The value is an integer in the range from 3000 to 3999.
l2-acl	Re-marks packets based on a specified Layer 2 ACL.	The value is an integer in the range from 4000 to 4999.

Parameter	Description	Value
user-acl	Re-marks packets based on a specified user-defined ACL.	The value is an integer in the range from 5000 to 5999.
ucl-acl	Specifies the user ACL for re-marking packets based on a user ACL.	The value is an integer in the range from 6000 to 9999.
name *acl-name*	Re-marks packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Re-marks packets based on a specified ACL rule.	The value is an integer in the range from 0 to 4294967294.
8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
cvlan-id *cvlan-id*	Re-marks the inner VLAN tag in QinQ packets. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **cvlan-id** *cvlan-id*.	The value is an integer in the range from 1 to 4094.
destination-mac *mac-address*	Re-marks the destination MAC address in packets. **NOTE** Only the S6735-S, S6720-EI and S6720S-EI support **destination-mac** *mac-address*.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
dscp { *dscp-name* | *dscp-value* }	Re-marks the DSCP priority in packets.	The value can be an integer in the range of 0 to 63, or DSCP service name, for example, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values corresponding to DSCP service names are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46 By default, the *dscp-value* is 0.
local-precedence *local-precedence-value*	Re-marks the local IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
ip-precedence *ip-precedence-value*	Re-marks the IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
vlan-id *vlan-id*	Re-marks the VLAN ID in packets.	The value is an integer in the range from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-remark** command is executed on a device, the device re-marks packets matching an ACL rule, for example, 802.1p priority, inner VLAN tag in QinQ packets, destination MAC address, DSCP service type, local precedence, IP precedence, and VLAN ID.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If both the **traffic-remark (interface view)** and **traffic-remark (system view)** commands are used, the **traffic-remark (interface view)** command takes effect.

When both the **traffic-remark (system view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is re-marked.

Outbound ACL-based re-marking on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based re-marking is configured, and the ACL is based on VLAN IDs.

- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based re-marking.

Example

Configure ACL-based re-marking in the inbound direction in VLAN 100, and re-mark the VLAN ID in packets from source MAC address 0-0-1 with 101.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule 5 permit source-mac 0-0-1
[HUAWEI-acl-L2-4001] quit
[HUAWEI] traffic-remark vlan 100 inbound acl 4001 rule 5 vlan-id 101
```

15.8.15 traffic-secure (interface view)

Function

The **traffic-secure** command configures ACL-based packet filtering on an interface.

The **undo traffic-secure** command cancels ACL-based packet filtering on an interface.

By default, ACL-based packet filtering is not configured on an interface.

Format

To configure a single ACL, use the following command:

traffic-secure inbound acl { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure inbound acl { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-secure inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Filters packets in the inbound direction.	-
acl	Filters packets based on the IPv4 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.

Parameter	Description	Value
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-secure** command is executed on an interface, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, if traffic matching **traffic-secure (interface view)** also matches **traffic-redirect (interface view)** or **traffic-redirect (system view)**, **traffic-redirect (interface view)** or **traffic-redirect (system view)** takes effect. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the ACL defines the permit action, **traffic-redirect (interface view)** or **traffic-redirect (system view)** and **traffic-secure (interface view)** take effect.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands except **traffic-redirect (interface view)** and **traffic-redirect (system view)**.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands.

If both **traffic-secure** and other ACL-based simplified traffic policy commands need to be configured on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and the ACL is based on the inner 802.1p priority, inner VLAN ID, or port range, configure the **traffic-secure** command, and then configure other ACL-based simplified traffic policy commands.

Example

Configure the traffic filtering action on GE0/0/1 to discard the packets with source address 192.168.0.2 and mirror the packets with destination address 192.168.1.3 to the observing interface with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] acl name test 3001
[HUAWEI-acl-adv-test] rule 5 permit ip destination 192.168.1.3 0
```

```
[HUAWEI-acl-adv-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-secure inbound acl 3000
[HUAWEI-GigabitEthernet0/0/1] traffic-mirror inbound acl 3001 to observe-port 1
```

15.8.16 traffic-secure (system view)

Function

The **traffic-secure** command configures ACL-based packet filtering globally or in a VLAN.

The **undo traffic-secure** command cancels ACL-based packet filtering globally or in a VLAN.

By default, ACL-based packet filtering is not configured globally or in a VLAN.

Format

To configure a single ACL, use the following command:

traffic-secure [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-secure [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based packet filtering in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Filters packets in the inbound direction.	-
acl	Filters packets based on the IPv4 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.

Parameter	Description	Value
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-secure** command is executed on the device, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, if traffic matching **traffic-secure (system view)** also matches **traffic-redirect (interface view)** or **traffic-redirect (system view)**, **traffic-redirect (interface view)** or **traffic-redirect (system view)** takes effect. On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, if the ACL defines the permit action, **traffic-redirect (interface view)** or **traffic-redirect (system view)** and **traffic-secure (system view)** take effect.

On the S1720GW-E, S1720GWR-E, S5720I-SI, S5720S-LI, S5735S-H, S5736-S, S6720S-S, and S5720-LI, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands except **traffic-redirect (interface view)** and **traffic-redirect (system view)**.

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands.

If both **traffic-secure** and other ACL-based simplified traffic policy commands need to be configured on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and the ACL is based on the inner 802.1p priority, inner VLAN ID, or port range, configure the **traffic-secure** command, and then configure other ACL-based simplified traffic policy commands.

Example

Configure the traffic filtering action globally to discard the packets with source address 192.168.0.2 and mirror the packets with destination address 192.168.1.3 to the observing interface with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] acl name test 3001
[HUAWEI-acl-adv-test] rule 5 permit ip destination 192.168.1.3 0
[HUAWEI-acl-adv-test] quit
[HUAWEI] traffic-secure inbound acl 3000
[HUAWEI] traffic-mirror inbound acl 3001 to observe-port 1
```

15.8.17 traffic-statistic (interface view)

Function

The **traffic-statistic** command configures ACL-based traffic statistics on an interface.

The **undo traffic-statistic** command cancels ACL-based traffic statistics on an interface.

By default, the ACL-based traffic statistics function is not configured on an interface.

Format

Use the following command in the inbound direction on an interface:

traffic-statistic inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* | *l2-acl* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* | *l2-acl* } [**rule** *rule-id*] [**secure**]

traffic-statistic inbound acl { **ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* } | *user-acl* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic inbound acl { **ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* } | *user-acl* } [**rule** *rule-id*]

Use the following command in the inbound direction on a tunnel interface:

traffic-statistic inbound acl { *adv-acl* | *ucl-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic inbound acl { *adv-acl* | *ucl-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

ACL-based traffic statistics collection can be configured in the inbound direction of a tunnel interface only on the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Use the following command in the outbound direction on an interface:

traffic-statistic outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

undo traffic-statistic outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics collection function is used in the inbound direction on an interface, use the following command:

traffic-statistic inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**secure**]

traffic-statistic inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**secure**]

traffic-statistic inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**secure**]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics collection function is used in the outbound direction on an interface, use the following command:

traffic-statistic outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Collects statistics on packets in the inbound direction.	-
outbound	Collects statistics on packets in the outbound direction.	-
acl	Collects statistics on packets based on the IPv4 ACL.	-
ipv6	Collects statistics on packets based on the IPv6 ACL.	-
bas-acl	Collects statistics on packets based on a specified basic ACL.	The value is an integer in the range from 2000 to 2999.
adv-acl	Collects statistics on packets based on a specified advanced ACL.	The value is an integer in the range from 3000 to 3999.
l2-acl	Collects statistics on packets based on a specified Layer 2 ACL.	The value is an integer in the range from 4000 to 4999.
user-acl	Collects statistics on packets based on a specified user-defined ACL.	The value is an integer in the range from 5000 to 5999.
ucl-acl	Collects statistics on packets based on a specified user ACL.	The value is an integer in the range from 6000 to 9999.

Parameter	Description	Value
name *acl-name*	Collects statistics on packets based on a specified named ACL. *acl-name* specifies the name of an ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Collects statistics on packets based on a specified ACL rule.	The value is an integer in the range from 0 to 4294967294.
by-bytes	Collects statistics on packets based on the number of bytes. **NOTE** By default, traffic statistics are collected based on the number of packets. After **by-bytes** is specified, traffic statistics are collected based on the number of bytes.	-
secure	Collects statistics on packets based on packet filtering policies configured through the **traffic-secure (interface view)** command.	-

Views

VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Tunnel interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-statistic** command is executed on an interface, the device collects statistics on packets matching an ACL. After the statistics collection function is configured, you can use the **display traffic-statistics** command to view the statistics.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support ACL-based simplified traffic policy configuration on a VLANIF interface.

- The VLAN corresponding to the VLANIF interface cannot be a Super-VLAN or MUX VLAN.
- For the S6735-S, S6720-EI and S6720S-EI, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.
- For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, an ACL-based simplified traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.

If the **traffic-statistic (system view)** and **traffic-statistic (interface view)** commands are used simultaneously, the **traffic-statistic (interface view)** command takes effect.

When the action in an ACL rule is **permit** or **deny**, the ACL can be associated with the **traffic-statistic** command, but **deny** does not take effect. That is, only traffic statistics are collected.

Outbound ACL-based traffic statistics collection on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based traffic statistics collection is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic statistics collection.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, ifIf **traffic-statistic** is applied to an Eth-Trunk in the outbound direction, traffic statistics does not take effect for the packets sent by the CPU. In this case, you can configure traffic statistics or port mirroring in the inbound direction on the interface connected to the Eth-Trunk.

Example

Configure the ACL-based traffic statistics function in the inbound direction on GE0/0/1 to collect statistics on packets matching rule 1 in ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-statistic inbound acl 3000 rule 1
```

15.8.18 traffic-statistic (system view)

Function

The **traffic-statistic** command configures ACL-based traffic statistics globally or in a VLAN.

The **undo traffic-statistic** command cancels ACL-based traffic statistics globally or in a VLAN

By default, the ACL-based traffic statistics function is not configured globally or in a VLAN.

Format

Use the following command in the inbound direction on a switch:

traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* | *l2-acl* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* | *l2-acl* } [**rule** *rule-id*] [**secure**]

traffic-statistic [**vlan** *vlan-id*] **inbound acl** { **ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* } | *user-acl* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** { **ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* } | *user-acl* } [**rule** *rule-id*]

Use the following command in the outbound direction on a switch:

traffic-statistic [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics function is used in the inbound direction on a switch, use the following command:

traffic-statistic [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**secure**]

traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**secure**]

traffic-statistic [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**] [**secure**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**secure**]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics function is used in the outbound direction on a switch, use the following command:

traffic-statistic [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based packet statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Collects statistics on packets in the inbound direction.	-
outbound	Collects statistics on packets in the outbound direction.	-
acl	Collects statistics on packets based on the IPv4 ACL.	-
ipv6	Collects statistics on packets based on the IPv6 ACL.	-
bas-acl	Collects statistics on packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Collects statistics on packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Collects statistics on packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.

Parameter	Description	Value
user-acl	Collects statistics on packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Collects statistics on packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Collects statistics on packets based on a specified ACL rule.	The value is an integer that ranges from 0 to 4294967294.
by-bytes	Indicates that traffic statistics are collected based on the number of bytes. **NOTE** By default, traffic statistics are collected based on the number of packets. After **by-bytes** is specified, traffic statistics are collected based on the number of bytes.	-
secure	Collects statistics on packets based on packet filtering policies configured through the **traffic-secure (system view)** command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-statistic** command is executed on the device, the device collects statistics on packets matching an ACL. After the statistics function is configured, you can use the **display traffic-statistics** command to view the statistics.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-statistic (interface view)** and **traffic-statistic (system view)** commands are used simultaneously, the **traffic-statistic (interface view)** command takes effect.

When the action in an ACL rule is **permit** or **deny**, the ACL can be associated with the **traffic-statistic** command, but **deny** does not take effect. That is, only traffic statistics are collected.

Outbound ACL-based traffic statistics collection on an interface does not take effect on the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S5735S-H, S5736-S, S6720S-S, and S5720S-LI if:

- Outbound ACL-based traffic statistics collection is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic statistics collection.

Example

Configure the ACL-based traffic statistics function in the inbound direction in VLAN 100 to collect statistics on packets matching rule 1 in ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] traffic-statistic vlan 100 inbound acl 3000 rule 1
```

15.9 HQoS Commands

15.9.1 Command Support

Only the following switch model supports HQoS:

S5731-S, S5731S-S, S5731-H, S5731S-H

15.9.2 color (flow queue WRED drop profile view)

Function

The **color** command configures upper and lower drop thresholds and maximum drop probability in a flow queue WRED drop profile based on the packet color.

The **undo color** command restores default parameters in a flow queue WRED drop profile.

By default, the upper and lower drop thresholds and maximum drop probability for green, yellow, and red packets are 100.

Format

color { **green** | **yellow** | **red** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*

undo color { **green** | **yellow** | **red** }

Parameters

Parameter	Description	Value
green	Indicates WRED parameters for green packets.	-
yellow	Indicates WRED parameters for yellow packets.	-
red	Indicates WRED parameters for red packets.	-
low-limit *low-limit-percentage*	Specifies the lower drop threshold, in percentage. When the percentage of the packet length to the queue length reaches this value, the device discards packets based on the drop probability.	The value is an integer that ranges from 0 to 100. The default value is 100.
high-limit *high-limit-percentage*	Specifies the upper drop threshold, in percentage. When the percentage of the packet length to the queue length reaches this value, the device starts to discard all subsequent packets.	The value is an integer that ranges from *low-limit-percentage* to 100. The default value is 100.
discard-percentage *discard-percentage*	Specifies the maximum drop probability.	The value is an integer that ranges from 1 to 100. The default value is 100.

Views

Flow queue WRED drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets enter queues, the device colors packets based on the mapping defined in a DiffServ domain. The device processes packets entering flow queues based on parameters in a flow queue WRED drop profile. When the percentage of the packet length to the queue length reaches the lower drop threshold, the device discards packets based on the drop probability. When the percentage of the packet length to the queue length reaches the upper drop threshold, the device discards all subsequent packets.

Prerequisites

A flow queue WRED drop profile has been created and the flow queue WRED drop profile view has been displayed.

Example

Configure flow queue WRED drop profile **wred1**, set the lower drop threshold, upper drop threshold, and maximum drop probability for green packets to 80%, 100%, and 10%, set the lower drop threshold, upper drop threshold, and maximum drop probability for yellow packets to 60%, 80%, and 20%, and set the lower drop threshold, upper drop threshold, and maximum drop probability for red packets to 40%, 60%, and 40%.

```
<HUAWEI> system-view
[HUAWEI] flow-wred-profile wred1
[HUAWEI-flow-wred-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-flow-wred-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-flow-wred-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
```

15.9.3 display flow-queue-profile

Function

The **display flow-queue-profile** command displays the flow queue profile configuration.

Format

display flow-queue-profile [**name** *flow-queue-profile-name* | **all**]

Parameters

Parameter	Description	Value
name *flow-queue-profile-name*	Displays detailed information about a specified flow queue profile.	The value must be the name of an existing flow queue profile.
all	Displays detailed information about all flow queue profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display flow-queue-profile** command to view the number of configured flow queue profiles and all the configuration of the specified flow queue profile.

Precautions

If **all** and **name** *flow-queue-profile* are not specified, brief information about all flow queue profiles is displayed.

Example

Display brief information about all flow queue profiles.

```
<HUAWEI> display flow-queue-profile
       index                  flow-queue-profile name
--------------------------------------------------------------------
       0                     default
       1                     flow1
--------------------------------------------------------------------
 Total   128     Used   2
```

Display detailed information about flow queue profile **flow1**.

```
<HUAWEI> display flow-queue-profile name flow1
Flow-queue-profile[1]: flow1
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     WFQ(50)          50%            wred1
1     PQ               None           default
2     PQ               None           default
3     PQ               None           default
4     PQ               None           default
5     PQ               None           default
6     PQ               None           default
7     PQ               None           default
---------------------------------------------------------------------------
```

Display detailed information about all flow queue profiles.

```
<HUAWEI> display flow-queue-profile all
Flow-queue-profile[0]: default
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     PQ               None           default
1     PQ               None           default
2     PQ               None           default
3     PQ               None           default
4     PQ               None           default
5     PQ               None           default
6     PQ               None           default
7     PQ               None           default
---------------------------------------------------------------------------
```

```
Flow-queue-profile[1]: flow1
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     WFQ(50)         50%           wred1
1     PQ             None          default
2     PQ             None          default
3     PQ             None          default
4     PQ             None          default
5     PQ             None          default
6     PQ             None          default
7     PQ             None          default
------------------------------------------------------------------------
```

Table 15-35 Description of the **display flow-queue-profile** command output

Item	Description
index	Index of the flow queue profile.
flow-queue-profile name	Name of the flow queue profile. To create a flow queue profile, run the **flow-queue-profile** command.
Total	Total number of flow queue profiles.
Used	Number of configured flow queue profiles.
Flow-queue-profile[1]	Name of the flow queue profile. The value 1 is the index of the flow queue profile. To create a flow queue profile, run the **flow-queue-profile** command.
Queue	Index of the flow queue, which corresponds to the local priority of packets.
Schedule(Weight)	Scheduling mode or weight of the flow queue. To set the scheduling mode and weight of a flow queue, run the **qos queue (flow queue profile view)** command.
Shaping	Traffic shaping rate or percentage of the flow queue. To set the traffic shaping and percentage of a flow queue, run the **qos queue (flow queue profile view)** command.
flow-wred-profile	Name of the WRED drop profile bound to the flow queue. To bind a WRED drop profile to a flow queue, run the **qos queue (flow queue profile view)** command.

15.9.4 display flow-wred-profile

Function

The **display flow-wred-profile** command displays the configuration of flow queue WRED drop profiles.

Format

display flow-wred-profile [**name** *flow-wred-profile-name* | **all**]

Parameters

Parameter	Description	Value
name *flow-wred-profile-name*	Displays detailed information about a specified flow queue WRED drop profile.	The value must be the name of an existing flow queue WRED drop profile.
all	Displays detailed information about all flow queue WRED drop profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display flow-wred-profile** command to view the number of configured flow queue WRED drop profiles and all the configuration of the specified flow queue WRED drop profile.

Precautions

If **all** and **name** *flow-wred-profile-name* are not specified, brief information about all flow queue WRED drop profiles is displayed.

Example

Display brief information about all flow queue WRED drop profiles.

```
<HUAWEI> display flow-wred-profile
        index                    flow-wred-profile name
----------------------------------------------------------------
```

```
      0                    default
      1                    wred1
----------------------------------------------------------------------
 Total   128     Used    2
```

Display detailed information about flow queue WRED drop profile **wred1**.

```
<HUAWEI> display flow-wred-profile name wred1
Flow-wred-profile[1]: wred1
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
----------------------------------------------------------------------
```

Display detailed information about all flow queue WRED drop profiles.

```
<HUAWEI> display flow-wred-profile all
Flow-wred-profile[0]: default
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     100         100         100
Yellow    100         100         100
Red       100         100         100
----------------------------------------------------------------------
Flow-wred-profile[1]: wred1
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
----------------------------------------------------------------------
```

Table 15-36 Description of the display flow-wred-profile command output

Item	Description
index	Index of the flow queue WRED drop profile.
flow-wred-profile name	Name of the flow queue WRED drop profile. To create a flow queue WRED drop profile, run the **flow-wred-profile** command.
Total	Total number of flow queue WRED drop profiles.
Used	Number of configured flow queue WRED drop profiles.
Flow-wred-profile[1]	Name of the flow queue WRED drop profile. The value 1 is the index of the flow queue WRED drop profile. To create a flow queue WRED drop profile, run the **flow-wred-profile** command.

Item	Description
Queue depth	Queue length. To set the queue length, run the **queue-depth (flow queue WRED drop profile view)** command.
Color	Packet color. To set the packet color, run the **color (flow queue WRED drop profile view)** command.
Low-limit	Lower drop threshold in the flow queue WRED drop profile, in percentage. To set the lower drop threshold in a flow queue WRED drop profile, run the **color (flow queue WRED drop profile view)** command.
High-limit	Upper drop threshold in the flow queue WRED drop profile, in percentage. To set the upper drop threshold in a flow queue WRED drop profile, run the **color (flow queue WRED drop profile view)** command.
Discard-percentage	Maximum drop probability in the flow queue WRED drop profile, in percentage. To set the maximum drop probability in a flow queue WRED drop profile, run the **color (flow queue WRED drop profile view)** command.

15.9.5 display traffic-user-queue statistics

Function

The **display traffic-user-queue statistics** command displays traffic statistics on subscriber queues.

Format

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** { *bas-acl* | *adv-acl* } [**acl** { *l2-acl* | **name** *acl-name* }]

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** *l2-acl* [**acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }]

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl name** *acl-name* [**acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* }]

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays traffic statistics on subscriber queues on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
outbound	Displays traffic statistics on subscriber queues in the outbound direction on an interface.	-
acl	Displays traffic statistics on subscriber queues based on IPv4 ACLs.	-
ipv6	Displays traffic statistics on subscriber queues based on IPv6 ACLs.	-
bas-acl	Displays traffic statistics on subscriber queues based on basic ACLs.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Displays traffic statistics on subscriber queues based on advanced ACLs.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Displays traffic statistics on subscriber queues based on Layer 2 ACLs.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Displays traffic statistics on subscriber queues based on named ACLs. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-user-queue statistics** command displays traffic statistics on subscriber queues based on ACLs on an interface. The command output helps you learn about forwarded and discarded packets matching ACLs and locate faults.

Prerequisites

The **traffic-user-queue** command has been executed to create a subscriber queue based on ACLs to implement HQoS.

Example

Display traffic statistics on subscriber queues based on ACL 3009 in the outbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl 3009
[HUAWEI-acl-adv-3009] rule 1 permit ip
[HUAWEI-acl-adv-3009] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-user-queue outbound acl 3009 pir 2000
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] display traffic-user-queue statistics interface gigabitethernet 0/0/1 outbound acl 3009
-------------------------------------------------------------------------------
 Interface: GigabitEthernet0/0/1
-------------------------------------------------------------------------------
    Queue ID     |                   Statistics information
-------------------------------------------------------------------------------
       0         |         packets: pass:                        0
                 |                  drop:                        0
                 |         bytes:   pass:                        0
                 |                  drop:                        0
-------------------------------------------------------------------------------
    Queue ID     |                   Statistics information
-------------------------------------------------------------------------------
       1         |         packets: pass:                        0
                 |                  drop:                        0
                 |         bytes:   pass:                        0
                 |                  drop:                        0
-------------------------------------------------------------------------------
    Queue ID     |                   Statistics information
-------------------------------------------------------------------------------
       2         |         packets: pass:                        0
                 |                  drop:                        0
                 |         bytes:   pass:                        0
                 |                  drop:                        0
-------------------------------------------------------------------------------
    Queue ID     |                   Statistics information
-------------------------------------------------------------------------------
       3         |         packets: pass:                        0
                 |                  drop:                        0
                 |         bytes:   pass:                        0
                 |                  drop:                        0
-------------------------------------------------------------------------------
    Queue ID     |                   Statistics information
-------------------------------------------------------------------------------
       4         |         packets: pass:                        0
                 |                  drop:                        0
                 |         bytes:   pass:                        0
                 |                  drop:                        0
-------------------------------------------------------------------------------
    Queue ID     |                   Statistics information
-------------------------------------------------------------------------------
```

```
       5        |          packets: pass:                       0
                |                  drop:                        0
                |          bytes:    pass:                      0
                |                  drop:                        0
-------------------------------------------------------------------------------
   Queue ID     |                    Statistics information
-------------------------------------------------------------------------------
       6        |          packets: pass:                       0
                |                  drop:                        0
                |          bytes:    pass:                      0
                |                  drop:                        0
-------------------------------------------------------------------------------
   Queue ID     |                    Statistics information
-------------------------------------------------------------------------------
       7        |          packets: pass:                       0
                |                  drop:                        0
                |          bytes:    pass:                      0
                |                  drop:                        0
-------------------------------------------------------------------------------
```

Table 15-37 Description of the **display traffic-user-queue statistics** command output

Item	Description
Queue ID	Index of the flow queue.
packets	Number of collected packets. pass indicates the number of forwarded packets, and drop indicates the number of discarded packets.
bytes	Number of collected bytes. pass indicates the number of forwarded bytes, and drop indicates the number of discarded bytes.

15.9.6 flow-queue-profile

Function

The **flow-queue-profile** command creates a flow queue profile or displays the view of an existing flow queue profile.

The **undo flow-queue-profile** command deletes the created flow queue profile.

By default, the system predefines a flow queue profile **default**.

Format

flow-queue-profile *flow-queue-profile-name*

undo flow-queue-profile *flow-queue-profile-name*

Parameters

Parameter	Description	Value
flow-queue-profile-name	Specifies the name of a flow queue profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring congestion management and traffic shaping parameters of a flow queue, you can run the **flow-queue-profile** *flow-queue-profile-name* command to create a flow queue profile and define parameters in the profile. To set the same scheduling mode and weight for different flow queues, reference the same flow queue profile.

Precautions

The flow queue profile **default** cannot be modified or deleted.

Follow-up Procedure

Configure congestion management and traffic shaping parameters of a flow queue and reference the flow queue WRED drop profile in the flow queue profile view.

Example

Create flow queue profile **test**.

```
<HUAWEI> system-view
[HUAWEI] flow-queue-profile test
[HUAWEI-flow-queue-test]
```

15.9.7 flow-wred-profile

Function

The **flow-wred-profile** command creates a flow queue WRED drop profile or displays the view of an existing flow queue WRED drop profile.

The **undo flow-wred-profile** command deletes the created flow queue WRED drop profile.

By default, the system predefines a flow queue WRED drop profile **default**.

Format

flow-wred-profile *flow-wred-profile-name*

undo flow-wred-profile *flow-wred-profile-name*

Parameters

Parameter	Description	Value
flow-wred-profile-name	Specifies the name of a flow queue WRED drop profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring WRED parameters of a flow queue, you can run the **flow-wred-profile** *flow-wred-profile-name* command to create a flow queue WRED drop profile and define parameters in the profile. To use the same upper and lower drop thresholds and maximum drop probability for different flow queues, reference the same flow queue WRED drop profile.

Precautions

The flow queue WRED drop profile **default** cannot be modified or deleted.

Follow-up Procedure

Configure WRED parameters of the flow queue and queue length in the flow queue WRED drop profile view.

Example

Create flow queue WRED drop profile **test**.

```
<HUAWEI> system-view
[HUAWEI] flow-wred-profile test
[HUAWEI-flow-wred-test]
```

15.9.8 qos queue (flow queue profile view)

Function

The **qos queue** command sets the scheduling mode, traffic shaping rate, and referenced flow queue WRED drop profile.

The **undo qos queue** command restores the default scheduling mode, traffic shaping rate, and referenced flow queue WRED drop profile.

By default, a flow queue uses PQ scheduling, PIR of a subscriber queue as the traffic shaping rate, and flow queue WRED drop profile **default**.

Format

qos queue *queue-index* { { **pq** | **wfq weight** *weight-value* } | { **shaping** { *shaping-value* | **shaping-percentage** *shaping-percentage-value* } } | { **flow-wred-profile** *flow-wred-profile-name* } } *

undo qos queue *queue-index* { { **pq** | **wfq** } | **shaping** | **flow-wred-profile** } *

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a flow queue.	The value is an integer that ranges from 0 to 7.
pq	Indicates PQ scheduling.	-
wfq	Indicates WFQ scheduling.	-
weight *weight-value*	Specifies the weight of WFQ scheduling.	The value is an integer that ranges from 1 to 100.
shaping *shaping-value*	Specifies the traffic shaping rate.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Parameter	Description	Value
shaping-percentage *shaping-percentage-value*	Specifies the traffic shaping percentage, that is, percentage of the traffic shaping rate to the PIR of a subscriber queue.	The value is an integer that ranges from 1 to 100.
flow-wred-profile *flow-wred-profile-name*	Specifies the name of a flow queue WRED drop profile.	The value must be the name of an existing flow queue WRED drop profile.

Views

Flow queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage packets in a flow queue, run this command to set the scheduling mode, traffic shaping rate, and referenced flow queue WRED drop profile.

Prerequisites

A flow queue profile has been created and the flow queue profile view has been displayed.

Precautions

The scheduling mode, traffic shaping rate, and flow queue WRED drop profile can be configured in any sequence. You can configure the scheduling mode, traffic shaping rate, and flow queue WRED drop profile independently or a combination of them.

Example

Configure flow queue profile **flow1** where the WFQ weight of flow queue 0 is 50%, the traffic shaping percentage is 50%, and referenced flow queue WRED drop profile is **wred1**.

```
<HUAWEI> system-view
[HUAWEI] flow-queue-profile flow1
[HUAWEI-flow-queue-flow1] qos queue 0 wfq weight 50 shaping shaping-percentage 50 flow-wred-profile wred1
```

15.9.9 queue-depth (flow queue WRED drop profile view)

Function

The **queue-depth** command sets the length of a flow queue.

The **undo queue-depth** command restores the default length of a flow queue.

By default, the length of a flow queue is 1048576 bytes.

Format

queue-depth *queue-depth-value*

undo queue-depth

Parameters

Parameter	Description	Value
queue-depth-value	Specifies the length of a flow queue.	The value is an integer that ranges from 1024 to 67092480, in bytes. The default value is 1048576.

Views

Flow queue WRED drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets entering flow queues are processed based on parameters in a flow queue WRED drop profile, the percentage of the packet length to the flow queue length needs to be calculated. When the percentage reaches the lower drop threshold, the device discards packets based on the drop probability. When the percentage reaches the upper drop threshold, the device discards all subsequent packets. You can adjust the flow queue length to optimize the congestion avoidance effect.

Prerequisites

A flow queue WRED drop profile has been created and the flow queue WRED drop profile view has been displayed.

Precautions

When a small flow queue length is used, the delay of packets passing a queue is shortened but the queue buffer capability is lowered. When a large flow queue length is used, the queue buffer capability is improved but the delay of packets passing a queue is extended. In addition, when congestion occurs in a flow queue, many buffer resources are occupied. In this case, packets in other flow queues may be discarded due to insufficient buffer resources. Therefore, the default flow queue length is recommended.

Example

Configure flow queue WRED drop profile **wred1** and set the flow queue length to 2000 bytes.

```
<HUAWEI> system-view
[HUAWEI] flow-wred-profile wred1
[HUAWEI-flow-wred-wred1] queue-depth 2000
```

15.9.10 reset traffic-user-queue statistics

Function

The **reset traffic-user-queue statistics** command clears traffic statistics on subscriber queues.

Format

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** { *bas-acl* | *adv-acl* } [**acl** { *l2-acl* | **name** *acl-name* }]

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** *l2-acl* [**acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }]

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl name** *acl-name* [**acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* }]

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears traffic statistics on subscriber queues on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
outbound	Clears traffic statistics on subscriber queues in the outbound direction on an interface.	-

Parameter	Description	Value
acl	Clears traffic statistics on subscriber queues based on IPv4 ACLs.	-
ipv6	Clears traffic statistics on subscriber queues based on IPv6 ACLs.	-
bas-acl	Clears traffic statistics on subscriber queues based on basic ACLs.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Clears traffic statistics on subscriber queues based on advanced ACLs.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Clears traffic statistics on subscriber queues based on Layer 2 ACLs.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Clears traffic statistics on subscriber queues based on named ACLs. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before re-collecting traffic statistics on subscriber queues in a given period of time, run this command to clear existing traffic statistics on subscriber queues.

Precautions

The cleared traffic statistics on subscriber queues cannot be restored. Exercise caution when you run this command.

Example

Clear traffic statistics on subscriber queues based on ACL 3009 in the outbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl 3009
```

```
[HUAWEI-acl-adv-3009] rule 1 permit ip
[HUAWEI-acl-adv-3009] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-user-queue outbound acl 3009 pir 2000
[HUAWEI-GigabitEthernet0/0/1] return
<HUAWEI> reset traffic-user-queue statistics interface gigabitethernet 0/0/1 outbound acl 3009
```

15.9.11 sac-profile (system view)

Function

The **sac-profile** command creates an SAC profile and displays its view, or directly displays the view of an existing SAC profile.

The **undo sac-profile** command deletes an SAC profile.

By default, no SAC profile is configured on a device.

NOTE

Only the S5731-S, S5731S-S, S5731-H, and S5731S-H support this command.

Format

sac-profile name *profile-name*

undo sac-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Indicates the name of an SAC profile.	The value is a string of 1 to 35 case-insensitive characters without spaces. If the string is enclosed in double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure an SAC profile and perform QoS configurations for users using the profile, for example, re-marking internal priorities based on user ACLs.

Follow-up Procedure

- Set parameters for the SAC profile, for example, internal priority re-marked based on a user ACL.
- Apply the SAC profile in the specified view. For example, in the WLAN scenario, apply an SAC profile in the service scheme view to re-mark the internal priority of packets, so that the device can schedule packets based on the re-marked priority.

Precautions

A device supports a maximum of 31 SAC profiles.

Example

Create an SAC profile named **huawei** and enter the SAC profile view.

```
<HUAWEI> system-view
[HUAWEI] sac-profile name huawei
[HUAWEI-sac-profile-huawei]
```

15.9.12 sac-profile (service scheme view)

Function

The **sac-profile** command binds an SAC profile to a service scheme.

The **undo sac-profile** command unbinds an SAC profile from a service scheme.

By default, no SAC profile is bound to a service scheme.

NOTE

Only the S5731-S, S5731S-S, S5731-H, and S5731S-H support this command.

Format

sac-profile *profile-name*

undo sac-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an SAC profile.	The value must be the name of an existing SAC profile.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

After creating a service scheme using the **service-scheme (AAA view)** command, you can run the **sac-profile** command to bind an SAC profile to the service scheme. The user assigned with the service scheme will have the attributes in the SAC profile.

Example

Bind the SAC profile **abc** to the service scheme **huawei**.

```
<HUAWEI> system-view
[HUAWEI] sac-profile name abc
[HUAWEI-sac-profile-abc] quit
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme huawei
[HUAWEI-aaa-service-huawei] sac-profile abc
```

15.9.13 traffic-user-queue (interface view)

Function

The **traffic-user-queue** command creates a subscriber queue on an interface to implement HQoS.

The **undo traffic-user-queue** command deletes a subscriber queue on an interface.

By default, no subscriber queue is configured on an interface.

Format

If a single ACL is used, use the following command:

traffic-user-queue outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name*]

undo traffic-user-queue outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } }

If both Layer 2 and Layer 3 ACLs are configured, use the following command:

traffic-user-queue outbound acl { *l2-acl* | **name** *acl-name* } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name*]

undo traffic-user-queue outbound acl { *l2-acl* | **name** *acl-name* } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }

traffic-user-queue outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } **acl** { *l2-acl* | **name** *acl-name* } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name*]

undo traffic-user-queue outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } **acl** { *l2-acl* | **name** *acl-name* }

Parameters

Parameter	Description	Value
outbound	Creates a subscriber queue in the outbound direction on an interface to implement HQoS scheduling.	-
acl	Creates a subscriber queue based on IPv4 ACLs to implement HQoS scheduling.	-
ipv6	Creates a subscriber queue based on IPv6 ACLs to implement HQoS scheduling.	-
bas-acl	Creates a subscriber queue based on basic ACLs to implement HQoS scheduling.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Creates a subscriber queue based on advanced ACLs to implement HQoS scheduling.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Creates a subscriber queue based on Layer 2 ACLs to implement HQoS scheduling.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Creates a subscriber queue based on named ACLs to implement HQoS scheduling. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
pir *pir-value*	Specifies the peak information rate (PIR) of a subscriber queue, which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Parameter	Description	Value
flow-queue-profile *flow-queue-profile-name*	Specifies the name of the referenced flow queue profile.	The value must be the name of an existing flow queue profile.

Views

GE interface view, XGE interface view, 25GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Multiple users can be differentiated based on ACL rules. When different scheduling and shaping parameters need to be set for different users and differentiated services need to be provided for different service traffic of the same user, run the **traffic-user-queue** command to configure multiple subscriber queues, set different scheduling modes and traffic shaping rates, and reference different flow queue profiles to implement fine-granular scheduling.

Prerequisites

The **acl (system view)** or **acl name** command has been executed to create an ACL.

Example

Create a subscriber queue based on ACLs on the GE0/0/1 to implement HQoS.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-user-queue outbound acl 3000 pir 1000 flow-queue-profile
flow1
```

15.9.14 user-queue (qos-profile view)

Function

The **user-queue** command creates a subscriber queue in a QoS profile to implement HQoS.

The **undo user-queue** command deletes a subscriber queue from a QoS profile.

By default, no subscriber queue is configured in a QoS profile.

Format

user-queue { **pir** *pir-value* | **flow-queue-profile** *flow-queue-profile-name* } *

undo user-queue

Parameters

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR) of a subscriber queue, which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 10000000, in kbit/s.
flow-queue-profile *flow-queue-profile-name*	Specifies the name of the referenced flow queue profile. If the name of the referenced flow queue profile is not specified, the flow queue profile **default** is used.	The value must be the name of an existing flow queue profile.

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure HQoS for authentication users to implement fine-granular scheduling, run the **user-queue** command to create subscriber queues, set different traffic shaping rates, and reference different flow queue profiles.

Prerequisites

A QoS profile has been created using the **qos-profile** command.

The user-defined flow queue profile and flow mapping profile have been created using the **flow-queue-profile** command respectively. If the user-defined flow queue profile and flow mapping profile are not required, use the default ones.

Example

Configure a user queue in the QoS profile **huawei** to implement HQoS.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] user-queue pir 1000 flow-queue-profile flow1
```

15.10 SAC Configuration Commands

15.10.1 Command Support

Only the following switch models support SAC:

S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

15.10.2 application name cache type aging-time

Function

The **application name cache type aging-time** command sets the aging time of the entry associated with pre-defined application identification.

The **undo application name cache type aging-time** command restores the default setting.

By default, the aging time of the entry generated upon application identification acceleration is 3600 seconds. In the entry generated upon multi-channel application identification, the aging time of FTP is 15 seconds, other application is 300 seconds.

Format

application name *name* **cache type** { **acceleration aging-time** *aging-time* | **multi-channel aging-time** *aging-time* }

undo application name *name* **cache type** { **acceleration** | **multi-channel** } **aging-time**

Parameters

Parameter	Description	Value
name	Specifies the name of a predefined application.	The value must be the name of an existing application.
acceleration aging-time *aging-time*	Specifies the aging time of the entry generated upon application identification acceleration.	The value is an integer ranging from 1 to 60,000, in seconds. The default value is 3600 seconds.

Parameter	Description	Value
multi-channel aging-time *aging-time*	Specifies the aging time of the entry generated upon multi-channel application identification.	The value is an integer ranging from 1 to 60,000, in seconds. The default value of FTP is 15 seconds, The default value of other applications is 300 seconds.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

The **application name cache type aging-time** command sets the aging time of the entry associated with the identification of predefined applications.

Example

Set the aging time of the entry associated with HTTPS acceleration identification to 5000 seconds and that of the entry associated with SFTP data channel application identification to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] application name HTTPS cache type acceleration aging-time 5000
[HUAWEI-sa] application name SFTP cache type multi-channel aging-time 100
```

15.10.3 category sub-category

Function

The **category sub-category** command configures the category and subcategory of user-defined applications.

The **undo category** command restores the default category and subcategory of user-defined applications.

The default category and subcategory of a user-defined application are **General** and **Other** respectively.

Format

category *category* **sub-category** *sub-category*

undo category

Parameters

Parameter	Description	Value
category	Specifies the category of an application.	See **Table 15-38**.
sub-category	Specifies the subcategory of an application.	See **Table 15-38**.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

One category contains multiple subcategories, but one subcategory belongs to only one category.

The device divides applications into the following categories and subcategories, as shown in **Table 15-38**.

Table 15-38 Category and subcategory of applications

Category	Subcategory	Description
Business_Systems	Auth_Service	Authentication service
	CloudService	Cloud service
	Data_Backup	Data backup
	Database	Database
	E_Government	Electronic government
	Electronic_Business	Electronic business
	Email	Email
	Enterprise_Application	Enterprise application
	File_Access	File access
	Finance	Finance
	Industrial	Industrial
	Internet_Conferencing	Internet conferencing
	Life_Services	Life service
	Remote_Access	Remote access control

Category	Subcategory	Description
	Remote_Desktop	Remote desktop
	Video_Surveillance	Video surveillance
	Wealth_Investment	Wealth investment
	WebMail	Web mail
Entertainment	Blog_Microblog	Microblog
	Forum_Community	Forum community
	Game	Game software
	Instant_Messaging	IM software
	Live_Streaming	Live streaming
	Media_Sharing	Applications for online videos
	Online_Media	Online media
	PeerCasting	P2P web video
	Personals_Dating	Personals dating
	Press_Media	Press media
	RSS_Feed	RSS feed
	Social_Networks	Social networks
	VoIP	VOIP
	WireLess	Wireless terminal application
General_Internet	AppStore	App store
	Browser_Plugin	Website plug-ins
	Cloud_Notes	Cloud notes
	FileShare_P2P	P2P file sharing
	File_Sharing	Fire sharing
	IM_File_Transfer	Applications for IM file transfer
	Internet_Reading	Internet reading
	Map_GPS	GPS map
	Network_Storage	Network storage
	Photo_Sharing	Photo sharing

Category	Subcategory	Description
	Resource_Library	Resource library
	Search_Engines	Search engines
	Software_Update	Software update
	Utility	Utility
	Web_Browsing	Web browsing
Network	Encrypted_Tunnel	Tunneling applications
	IP_Protocol	IP-layer protocols
	Infrastructure	Basic network protocols
	Network_Admin	Network administration
	Proxy	Proxy software
	Security_Risk	Security risk
General	General_UDP	General UDP applications
	General_TCP	General TCP applications
	Other	Other general applications

Example

Configure the category and subcategory of user-defined application **abc** to **Business_Systems** and **Database** respectively.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] category Business_Systems sub-category Database
```

15.10.4 data-model

Function

The **data-model** command specifies the data model of a user-defined application.

The **undo data-model** command restores the default data model of a user-defined application.

The default data model of user-defined applications is **unassigned**.

Format

data-model { **unassigned** | **client-server** | **browser-based** | **networking** | **peer-to-peer** }

undo data-model

Parameters

Parameter	Description	Value
unassigned	Indicates that no model is specified for data transmission.	-
client-server	Indicates applications using the Client/Server (C/S) model, such as client games.	-
browser-based	Indicates web applications, such as web games.	-
networking	Indicates common networking applications, such as HTTP and HTTPS.	-
peer-to-peer	Indicates peer-to-peer applications, such as Thunder and BT.	-

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the data model of user-defined application **UD_abc** to **client-server**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] data-model client-server
```

15.10.5 description (user-defined application rule view)

Function

The **description** command configures the description of a user-defined application rule.

The **undo description** command deletes the description of a user-defined application rule.

By default, the user-defined application rule has no description information.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined application rule.	The value is a case-sensitive string of 1 to 128 characters. Spaces are supported.

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Add description **test** for user-defined application rule **rule1**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] rule name rule1
[HUAWEI-sa-user-defined-app-UD_abc-rule-rule1] description test
```

15.10.6 description (user-defined application view)

Function

The **description** command configures the description of a user-defined application.

The **undo description** command deletes the description of a user-defined application.

By default, the user-defined application has no description information.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined application.	The value is a case-sensitive string of 1 to 128 characters. Spaces are supported.

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Add description **test** for user-defined application **UD_abc**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] description test
```

15.10.7 detect max-bytes

Function

The **detect max-bytes** command specifies the maximum number of bytes to be detected by the SA module.

The **undo detect max-bytes** command restores the maximum number of bytes detected by the SA module to the default value.

By default, the maximum number of bytes is 2048.

Format

detect max-bytes *max-bytes*

undo detect max-bytes

Parameters

Parameter	Description	Value
max-bytes	Specifies the maximum number of bytes to be detected.	The value is an integer ranging from 1 to 10240.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

This command is used to specify the maximum number of bytes detected by the SA module to prevent certain applications from evading the detection by using small packets. In common cases, the default maximum value can meet the requirement. If the value is too large, the device performance may deteriorate. If the value is too small, the device may fail to detect certain applications.

Example

Set the maximum number of bytes to be detected by the SA module to 4096.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] detect max-bytes 4096
```

15.10.8 detect max-packets

Function

The **detect max-packets** command specifies the maximum number of packets to be detected by the SA module.

The **undo detect max-packets** command restores the maximum number of packets detected by the SA module to the default value.

By default, the maximum number of packets is 8.

Format

detect max-packets *max-packets*

undo detect max-packets

Parameters

Parameter	Description	Value
max-packets	Specifies the maximum number of packets in a session.	The value is an integer ranging from 1 to 64.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

The specified maximum number of packets to be detected covers both directions in a session.

Example

Set the maximum number of packets to be detected by the SA module to **20**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] detect max-packets 20
```

15.10.9 detect max-time

Function

The **detect max-time** command sets the maximum duration in which the SA module detects sessions.

The **undo detect max-time** command restores the maximum duration to the default value.

By default, the maximum duration is 1 minute.

Format

detect max-time *max-time*

undo detect max-time

Parameters

Parameter	Description	Value
max-time	Specifies the maximum session detection duration.	The value is an integer ranging from 0 to 60, in minutes.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum duration in which the SA module detects sessions to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] detect max-time 5
```

15.10.10 detect uni-direction

Function

The **detect uni-direction** command configures the unidirectional detection on the SA module.

The **undo detect uni-direction** command restores to the default detection mode, namely, bidirectional detection.

By default, the SA module works in bidirectional detection mode.

Format

detect uni-direction

undo detect uni-direction

Parameters

None

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

SA detection falls into unidirectional detection and bidirectional detection. If the device is deployed in unidirectional mode, use the **detect uni-direction** command to configure the unidirectional detection mode of the SA module.

Example

Configure the unidirectional detection mode of the SA module.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] detect uni-direction
```

15.10.11 display application

Function

The **display application** command displays information about applications in the system.

Format

display application [**pre-defined** | **user-defined** | **name** *name*]

Parameters

Parameter	Description	Value
pre-defined	Indicates all predefined applications.	-
user-defined	Indicates all user-defined applications.	-
name *name*	Specifies the name of an application.	The value must be the name of an existing application.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

The actual information about each application varies depending on the device.

Example

Display information about all applications.

```
<HUAWEI> display application
Service Awareness Signature Database Information:
Total Applications: 544
-------------------------------------------------------------------------------------------------------------------------------
 AppID Name                         Category              Sub-category               RiskLevel State
 1     BT                        General_Internet       FileShare_P2P              4        activated
 2     PPLive                     Entertainment          Peercasting               5        activated
 3     Thunder                     General_Internet        FileShare_P2P              5        activated
 5     FTP                        Network               Infrastructure            3        activated
 7     eDonkey_eMule                   General_Internet         FileShare_P2P              5        activated
 9     QQLive                      Entertainment          Peercasting               5        activated
 11    Fasttrack                   General_Internet        FileShare_P2P              5        activated
 12    PPStream                     Entertainment          Peercasting               5        activated
 14    DirectConnect                 General_Internet        FileShare_P2P              3        activated
 15    KuGoo                       Entertainment          Peercasting               5        activated
 16    Fring_VoIP                   Entertainment          VoIP                     4        activated
 18    POCO                        General_Internet        FileShare_P2P              5        activated
 20    Maze                        General_Internet        FileShare_P2P              3        activated
 22    UUSee                       Entertainment          Peercasting               4        activated
 23    Vagaa                       General_Internet        FileShare_P2P              4        activated
 25    QQDownLoad                     General_Internet         FileShare_P2P              4        activated
 27    Filetopia                   General_Internet        FileShare_P2P              5        activated
 28    Soulseek                    General_Internet        FileShare_P2P              5        activated
 31    KooWo                       Entertainment          Peercasting               4        activated
 32    FengXing                    Entertainment          Peercasting               5        activated
 34    DoPool                      Entertainment          Peercasting               3        activated
 35    FlashGet                    General_Internet        FileShare_P2P              5        activated
 39    Fs2You                      General_Internet        FileShare_P2P              5        activated
 41    QQ_VoIP                      Entertainment          VoIP
...
```

Table 15-39 Description of the **display application** command output

Item	Description
Total Applications	Total number of applications.
AppID	Application ID.
Name	Application name.
Category	Category to which an application belongs.
Sub-category	Subcategory to which an application belongs.
RiskLevel	Risk level of an application.

Item	Description
State	Status of an application. A predefined application can be in either of the following states: ● activated: indicates that the application takes effect. ● disabled: indicates that the application is disabled.

Display information about the predefined application **BT**.

```
<HUAWEI> display application name bt
Application bt Information:
--------------------------------------------------------------------------------------
  Application ID      : 1
  Application Name    : BT
  Category            : General_Internet
  Sub-category        : FileShare_P2P
  Software            : Other
  Risk Level          : 4
  Label               : "Productivity-Loss", "Data-Loss", "Bandwidth-Consuming",
                        "Evasive", "Tunneling", "P2P-Based"
  State               : activated
  DataModel           : peer-to-peer
  Description         : BitTorrent (BT) is a P2P protocol for multi-point downloading an
                        d can be used for many different kinds of applications. The clie
                        nt downloads and uploads data at the same time. Example: BitTorr
                        ent, BitSpirit and BitComet.

  Total Rule Number   : 0

--------------------------------------------------------------------------------------
```

Table 15-40 Description of the **display application name** *name* command output

Item	Description
Application *name* Information	Application *name* information.
Application ID	Application ID.
Application Name	Application name.
Category	Category to which an application belongs.
Sub-category	Subcategory to which an application belongs.
Software	Name of the software corresponding to the application. This item is displayed only for predefined applications.
Risk Level	Risk level of the application.
Label	Label of the application.

Item	Description
State	Status of the application. A predefined application can be in either of the following states: - activated: indicates that the application takes effect. - disabled: indicates that the application is disabled.
DataModel	Data transmission mode: - unassigned - client-server - browser-based - networking - peer-to-peer
Description	Description of the application.
Total Rule Number	Number of rules. For predefined applications, the value is fixed to 0.

15.10.12 display application name aging-time

Function

The **display application name aging-time** command displays the aging time of the entry associated with application identification.

Format

display application name *name* **aging-time**

Parameters

Parameter	Description	Value
name	Specifies the name of an application.	The value must be the name of an existing application.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Display the aging time of the entry associated with SFTP identification.

```
<HUAWEI> display application name SFTP aging-time
Aging Time:
-------------------------------------------------------------------------------
  Application Name                  : sftp
  Acceleration Aging-time(sec)       : 300
  Multi-channel Aging-time(sec)      : 15
-------------------------------------------------------------------------------
```

Table 15-41 Description of the **display application name aging-time** command output

Item	Description
Aging Time	The aging time of the entry associated with the identification of predefined applications.
Application Name	Name of an application.
Acceleration Aging-time(sec)	Aging time of the entry generated upon application identification acceleration.
Multi-channel Aging-time(sec)	Aging time of the entry generated upon multi-channel application identification. If the queried application is not a multi-channel application, **-** is displayed.

15.10.13 display engine session application

Function

The **display engine session application** command displays application identification entries.

Format

display engine session application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the service awareness (SA) function is configured, the switch identifies application packets and generates application identification entries. You can run the **display engine session application** command to check application identification entries on the switch.

Prerequisites

1. The resource allocation mode has been set to **sac** or **enhanced-sac**. To check the current resource allocation mode of the switch and the resource allocation mode specified using the **assign resource-mode** command, run the **display resource-mode configuration** command. If the resource allocation mode is not **sac** or **enhanced-sac**, run the **assign resource-mode sac** | **enhanced-sac** command to change the resource allocation mode to **sac** or **enhanced-sac**, save the configuration, and restart the switch.
2. The **defence engine enable** command has been run to enable the IAE. When the IAE is enabled, the application signature database is loaded automatically.
3. The **service-awareness enable** command has been run to enable the SA function on the interface.

Example

Display application identification entries generated after the switch identifies application packets.

```
<HUAWEI> display engine session application
Source IP       Destination IP  SPort  DPort  ProtocolID AppName      AppID  Expire(S)
----------------------------------------------------------------------------------------
10.10.1.1       10.20.1.1       51918  23     6          Telnet       415    300
----------------------------------------------------------------------------------------
Total:1
```

Table 15-42 Description of the **display engine session application** command output

Item	Description
Source IP	Source IP address.
Destination IP	Destination IP address.
SPort	Source port number.
DPort	Destination port number.

Item	Description
ProtocolID	Protocol ID.
AppName	Application name.
AppID	Application ID.
Expire(S)	Aging time, in seconds.
Total	Total number of application identification entries.

15.10.14 if-match application

Function

The **if-match application** command configures a matching rule based on the application name in a traffic classifier.

The **undo if-match application** command deletes a matching rule based on the application name in a traffic classifier.

By default, no matching rule based on the application name is configured in a traffic classifier.

Format

if-match application name *appname*

undo if-match application name

Parameters

Parameter	Description	Value
name *appname*	Specifies the name of an application.	The value is a string of characters. The value depends on the applications supported in the signature database. To check the supported application names, run the **display application** command.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match application** command to classify packets based on the application name of packets. This ensures that the switch processes packets matching the same traffic classifier identically.

Precautions

If you run the **if-match application** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

A traffic policy containing such a traffic classifier can be applied only to the inbound direction globally or on a physical or a VLANIF interface.

Both the traffic classifier defining **if-match application** and traffic classifiers defining other matching rules (excluding **if-match discard**) can take effect. Examples are as follows:

- A packet matches two pairs of traffic classifiers and traffic behaviors defined in the same traffic policy, and only one traffic classifier contains **if-match application**. (The other traffic classifier does not contain **if-match discard** or **if-match application**.) In this case, both pairs of traffic classifiers and traffic behaviors take effect for the packet.
- A packet matches two traffic policies, and a traffic classifier contains **if-match application** in only one of the traffic policies. (The other traffic policy does not contain **if-match discard** or **if-match application**.) In this case, both traffic policies take effect for the packet.

Example

Configure a matching rule based on the application name **BT** in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match application name BT
```

15.10.15 ip-address (user-defined application rule view)

Function

The **ip-address** command sets the IPv4 address in a user-defined application rule.

The **undo ip-address** command deletes the IPv4 address in a user-defined application rule.

Format

ip-address *ip-address* [*mask* | *mask-length*]

undo ip-address { *ip-address* [*mask* | *mask-length*] | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
mask	Specifies the subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 1 to 32.
all	Deletes all IPv4 addresses.	-

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set a single IPv4 address in a user-defined application rule or set the subnet mask or mask length to specify a network segment.

After you configure the IPv4 address, the SA engine will use the transport layer protocol and ports, that is, the 3-tuple to match the network packets. If you know the destination 3-tuple of the detecting flow, you can configure a user-defined 3-tuple to accelerate the application identification. For example, if you have a server, you can configure a 3-tuple rule according to the IPv4 address, port, and protocol of the server, so the rule can identify all the accessing flow to this server. At least one IPv4 address or one port should be in the 3-tuple rule. Note that the IPv4 address set here is only the destination IPv4 address.

Precautions

- The total number of IPv4 and IPv6 addresses in a user-defined application rule cannot be larger than four.
- If an IPv4 address with a mask is configured, the executed command is recorded in the configuration file, but the masked IPv4 address takes effect in the actual configuration. For example, if the **ip address 1.1.1.1 8** command is executed, this command is recorded in the configuration file. However, the actual configuration that takes effect is **ip address 1.0.0.0 8**.

Example

Set the IPv4 address in user-defined application rule **rule1** to **10.1.1.1**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] rule name rule1
[HUAWEI-sa-user-defined-app-rule-rule1] ip-address 10.1.1.1
```

15.10.16 label (User-defined application view)

Function

The **label** command specifies the label of a user-defined application.

The **undo label** command cancels the label of a user-defined application.

Format

label *label-name* &<1-8>

undo label [*label-name*]

Parameters

Parameter	Description	Value
label-name	Specify the label of the user-defined application.	For details about the label dimensions and names, see **Table 15-43**.

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

You can specify one or more labels to a user-defined application. No more than 8 labels are supported.

Table 15-43 lists the label dimensions and names.

Table 15-43 Label dimensions and names

Label Dimension	Label Name
Other-Dimension	Database, Business-Applications
Technology-Dimension	Mobile-Supported, Cloud-Based, Encrypted-Communications, P2P-Based, HTTP-Based, Tunneling

Label Dimension	Label Name
Function-Dimension	Network-Storage, Social-Applications, Plays-Game, Browses-Web, Speech, Sends-Mail, Supports-IM, Supports-Video, Supports-VoIP, Supports-File-Transfer
Risk-Dimension	The following label may bring risk to the network. After you configure the risk features, the system automatically calculates the risk level (1 to 5) of the application. Applications with a higher risk level bring about more risks to the network. ● **Exploitable**: indicates that the application has known vulnerabilities. ● **Malware-Vehicle**: indicates applications used by malware. For example, malware can use an application to launch attacks or listen data. ● **Productivity-Loss**: indicates applications compromising work efficiency, for example, applications for entertainment, news, and videos. ● **Bandwidth-Consuming**: indicates applications consuming network bandwidth, such as BT. ● **Evasive**: indicates applications that use ports or protocols for malicious purposes, such as evading firewall inspection. Proxy software is a typical example of such protocols. ● **Data-Loss**: indicates applications for transferring files and uploading texts. Using such applications may cause information leaks.

Example

Configure a matching rule based on the application name **BT** in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] label P2P-Based Encrypted-Communications Business-Applications
```

15.10.17 port (user-defined application rule view)

Function

The **port** command specifies a port in a user-defined application rule.

The **undo port** command deletes the port in a user-defined application rule.

Format

port *port*

undo port { *port* | **all** }

Parameters

Parameter	Description	Value
port	Specifies a port in a user-defined application rule.	The value is an integer ranging from 1 to 65535.
all	Deletes all port.	-

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can specify a maximum of 4 ports in a user-defined application rule.

After you configure the port, the SA engine will use the transport layer protocol and ports, that is, the 3-tuple to match the network packets. If you know the destination 3-tuple of the detecting flow, you can configure a user-defined 3-tuple to accelerate the application identification. For example, if you have a server, you can configure a 3-tuple rule according to the IP address, port, and protocol of the server, so the rule can identify all the accessing flow to this server. At least one IP address or one port should be in the 3-tuple rule. Note that the port number set here is only the destination port number.

Example

Set the port in user-defined application rule **rule1** to 80.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] rule name rule1
[HUAWEI-sa-user-defined-app-rule-rule1] port 80
```

15.10.18 port-identification packet-number-threshold

Function

The **port-identification packet-number-threshold** command sets the threshold of packet quantity for port identification in the SA module.

The **undo port-identification packet-number-threshold** command restores the default threshold of packet quantity for port identification in the SA module.

By default, the threshold of packet quantity is 16.

Format

port-identification packet-number-threshold *packets*

undo port-identification packet-number-threshold

Parameters

Parameter	Description	Value
packets	Specifies the number of packets.	The value is an integer ranging from 1 to 64.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

If packets exceeding the threshold are sent to the IAE and their applications cannot be identified, the SA module identifies the application by port. A high threshold compromises the application identification performance while a low threshold increases the false positive rate. The default value (16) is recommended.

Example

Set the threshold of packet quantity for port identification in the SA module to 32.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] port-identification packet-number-threshold 32
```

15.10.19 protocol (user-defined application rule view)

Function

The **protocol** command specifies a transport-layer protocol.

The **undo protocol** command restores the default setting.

The default transport-layer protocol in a user-defined application rule is any. That is, the rule applies to both TCP and UDP packets.

Format

protocol { **tcp** | **udp** }

undo protocol

Parameters

Parameter	Description	Value
port	Indicates the Transmission Control Protocol (TCP).	-
all	Indicates the User Datagram Protocol (UDP).	-

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the transport-layer protocol in a user-defined application rule to TCP.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] rule name rule1
[HUAWEI-sa-user-defined-app-rule-rule1] protocol tcp
```

15.10.20 rule name (user-defined application view)

Function

The **rule name** command creates a user-defined application rule, and displays the user-defined application view.

The **undo rule** command deletes a user-defined application rule.

Format

rule name *name*

undo rule { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a rule.	The value is a case-sensitive character string. The value is a case-sensitive string of 1 to 32 characters. Enclose the name with double quotation marks ("") if the name contains spaces, for example, "user for test". The name that contains spaces has 3 to 34 characters. The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot have any double quotation marks ("). In addition, the name cannot be **any** or **all**.
all	Deletes all user-defined application rules.	-

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

If the specified user-defined application rule does not exist, a new application rule is created and the application rule view is displayed. If the specified user-defined application rule exists, the view of the specified user-defined application rule is displayed.

The device uses the 3-tuple, keyword, or the combination to creates rules. The 3-tuple can be the destination 3-tuple (server address, protocol, and port) or source 3-tuple (user source address, protocol, and source port). The keyword indicates the signature of the application data packets or data flow. The signature uniquely identifies the application.

- You can run the **ip-address (user-defined application rule view)**, **port (user-defined application rule view)**, and **protocol (user-defined application rule view)** commands to specify the 3-tuple of an application. After you configure the 3-tuple and commit the configuration, the device uses the destination 3-tuple to match the first packet of a flow. If a match is found, the application of the traffic is the application specified in the 3-tuple. If no match is found, the device uses the source 3-tuple to match the first packet. If a match is found, the application of the traffic is the application specified in the 3-tuple. If no match is found, the application of the traffic is not the application specified in the 3-tuple.

If you use the 3-tuple to configure user-defined application rules, ensure that one rule contains at least one IP address or port.

- You can run the **signature (user-defined application rule view)** command to specify the keyword of an application.

You can configure multiple rules for one user-defined application. These rules are logically ORed. Data flows or packets are of the application once they match one of the rules.

When the number of user-defined application rules on the device exceeds the maximum value but the number of user-defined applications does not exceed the maximum value, you can create user-defined applications but cannot create user-defined application rules.

Example

Create rule **rule1** for user-defined application **UD_abc** and access the rule view.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] rule name rule1
[HUAWEI-sa-user-defined-app-UD_abc-rule-rule1]
```

15.10.21 sa

Function

The **sa** command displays the SA view.

Format

sa

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, you must run the **defence engine enable** command to enable the IAE.

Example

Access the SA view.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa]
```

15.10.22 sa cache enable

Function

The **sa cache enable** command enables application identification acceleration.

The **undo sa cache enable** command disables application identification acceleration.

By default, application identification acceleration is disabled.

Format

sa cache [**risk-level** { **low** | **high** }] **enable**

undo sa cache enable

Parameters

Parameter	Description	Value
risk-level	Indicates the risk level of the SA cache.	-
low	Indicates that the risk level is low.	-
high	Indicates that the risk level is high.	-

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

After application identification acceleration is enabled, the system generates an association entry for an identified application. The follow-up traffic matching the entry is identified as the application without additional application identification, which accelerates application identification.

You can set parameter **risk-level** to control the risk level of the SA module acceleration identification. If **risk-level** is set to low, high-risk acceleration cache entries are not generated. If **risk-level** is set to high or no risk level is specified, low-risk and high-risk acceleration cache entries are generated.

Application identification acceleration applies only to predefined applications of non-multi-channel protocols.

NOTE

Enabling application identification acceleration increases the efficiency but also the false positive rate. If the acceleration cache risk is set to high, the false positive rate is also high.

Example

Enable application identification acceleration.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] sa cache enable
```

15.10.23 service-awareness enable

Function

The **service-awareness enable** command enables the service awareness (SA) function.

The **undo service-awareness enable** command disables the SA function.

By default, the SA function is disabled.

Format

service-awareness enable

undo service-awareness enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, VLANIF interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traditional traffic classification technologies only check the content at Layer 4 and lower layers in packets, for example, source IP address, destination IP address, source port number, destination port number, and service type. It cannot analyze applications in packets. SA is a traffic detection and control technology based on the application layer. Apart from the IP packet header, SA can analyze the content of the application layer.

To identify the application of the traffic passing through an interface, run this command to enable SA on the interface.

Precautions

- The resource allocation mode has been set to **sac** or **enhanced-sac** for the slot corresponding to the interface. To check the current resource allocation mode of the switch and the resource allocation mode specified using the **assign resource-mode** command, run the **display resource-mode configuration** command. If the resource allocation mode is not **sac** or **enhanced-sac**, run the **assign resource-mode sac** | **enhanced-sac** command to change the resource allocation mode to **sac** or **enhanced-sac**, save the configuration, and restart the switch.
- In versions earlier than V200R022C10, SAC takes effect only on access-side interfaces but not tunnel-side interfaces in VXLAN scenarios. This limitation does not apply to V200R022C10 and later versions.

Example

Enable SA on VLANIF 10.

```
<HUAWEI> system view
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] service-awareness enable
```

15.10.24 signature (user-defined application rule view)

Function

The **signature** command configures a user-defined application signature.

The **undo signature** command deletes a user-defined application signature.

Format

signature context { **flow** | **packet** } **direction** { **request** | **response** | **both** } **plain-string** *plain-string* [**field** *field*]

undo signature

Parameters

Parameter	Description	Value
context	Indicates signature context.	-
flow	Indicates flow-based matching.	-
packet	Indicates packet-based matching.	-
direction	Indicates that the detection direction.	-

Parameter	Description	Value
request	Indicates that the detection direction is the request direction.	-
response	Indicates that the detection direction is the response direction.	-
both	Indicates that the detection direction is both directions.	-
plain-string *plain-string*	Specifies a plain-text string.	The value is a case-sensitive string of 3 to 128 characters. If the keyword contains any space and question mark (?), the value is a string of 5 to 130 characters and must be enclosed with double quotation marks (""), for example, "GET w?". If the keyword contains quotation marks, replace the quotation marks with \x22, for example, to set keyword **abc"d**, enter **abc\x22d**.
field *field*	Specifies a protocol field to search for a signature.	The **General-payload** field can be searched.

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can configure only one signature for each user-defined application rule.

Example

Configure a plain-text string for the signature in user-defined application rule **rule1**, configure flow-based matching mode, and set the detection direction to **request**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-sa-user-defined-app-UD_abc] rule name rule1
[HUAWEI-sa-user-defined-app-rule-rule1] protocol tcp
[HUAWEI-sa-user-defined-app-rule-rule1] signature context flow direction request plain-string abc field
General-payload
```

15.10.25 user-defined-application name

Function

The **user-defined-application name** command creates a user-defined application and displays its view.

The **undo user-defined-application name** command deletes a user-defined application.

Format

user-defined-application name *name* [**id** *id*]

undo user-defined-application { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a user-defined application.	The value is a case-sensitive character string, and must begin with **UD_**. The length of a name without spaces ranges from 4 to 32 characters. The length of a name with spaces ranges from 6 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "UD_user for test"). The name cannot contain question marks (?), commas (,), or hyphens (-). If the name does not contain any space, it also cannot have any double quotation marks (").
id *id*	Specifies the ID of a user-defined application.	The value is an integer that ranges from 60000 to 60511.
all	Indicates all user-defined applications.	-

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

If the name you specify does not exist, a user-defined application is created and the user-defined application view is displayed. If the specified name exists, the user-defined application view is displayed directly.

Example

Create a user-defined application **UD_abc**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable
[HUAWEI] sa
[HUAWEI-sa] user-defined-application name UD_abc
[HUAWEI-app-UD_abc] user-defined-application name UD_abc
```

16 Network Management and Monitoring Commands

16.1 SNMP Configuration Commands

16.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.1.2 bulk-file

Function

The **bulk-file** command creates a bulk file for bulk statistics collection and displays the bulk file view. If the specified bulk file exists, the command displays the bulk file view directly.

The **undo bulk-file** command deletes a bulk file.

By default, no bulk file is configured in the system.

Format

bulk-file *file-name*

undo bulk-file *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a bulk file.	The value is a string of 1 to 31 characters. It can only contain digits, letters, underscores (_), and hyphens (-).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before creating a bulk file, run the **bulk-stat enable** command to enable bulk statistics collection.

Before deleting a bulk file, ensure that the bulk file exists and the bulk statistics collection task has been stopped. If the bulk file does not exist or the bulk statistics collection task is still running, the system displays an error message.

Example

Create a bulk file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
```

```
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable]
```

16.1.3 bulk-stat enable

Function

The **bulk-stat enable** command enables the bulk statistics collection function.

The **undo bulk-stat enable** command disables the bulk statistics collection function.

By default, the bulk statistics collection function is disabled.

Format

bulk-stat enable

undo bulk-stat enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the system to collect statistics about multiple objects on the local device, generate a statistics file, and send the file to the NMS through FTP or TFTP, use the **bulk-stat enable** command to enable the bulk statistics collection function.

When disabling the bulk statistics collection function, you need to confirm your action in interactive mode.

Example

Enable the bulk statistics collection function.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
```

Disable the bulk statistics collection function.

```
<HUAWEI> system-view
[HUAWEI] undo bulk-stat enable
Warning: All bulk stat configuration will be deleted. Continue? [Y/N]:y
```

16.1.4 clear configuration snmp-agent trap enable

Function

The **clear configuration snmp-agent trap enable** command deletes alarm configurations related to one or all functions in a batch and restores the default alarm functions.

Format

clear configuration snmp-agent trap enable [**feature-name** *feature-name*]

Parameters

Parameter	Description	Value
feature-name *feature-name*	Deletes configurations of the trap function of a feature.	The value is the name of a feature that has been supported by the device.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a feature trap function is enabled or disabled using the **snmp-agent trap enable feature-name** *feature-name* [**trap-name** *trap-name*] command, the trap functions of all features are enabled using the **snmp-agent trap enable** command, or the trap functions of all features are disabled using the **snmp-agent trap disable** command. To delete the configurations, run the **clear configuration snmp-agent trap enable** command.

Configuration Impact

- When the trap function is enabled or disabled globally, running the **clear configuration snmp-agent trap enable feature-name** *feature-name* command deletes configurations of the trap function of the feature specified by *feature-name* and restores the status of the trap function to be the same as that of the global trap function.
- When the global trap function is in the default state, running the **clear configuration snmp-agent trap enable feature-name** *feature-name* command deletes configurations of the trap function of the feature specified by *feature-name* and restores the status of the trap function to be the default status.

- Running the **clear configuration snmp-agent trap enable** command deletes configurations of the trap functions of all features and restores all feature alarm functions to the default status.

Example

Delete configurations of the trap functions of all features.

```
<HUAWEI> system-view
[HUAWEI] clear configuration snmp-agent trap enable
```

16.1.5 collect enable

Function

The **collect enable** command enables an existing bulk file.

The **undo collect enable** command disables an existing bulk file.

By default, no bulk file is enabled.

Format

collect enable

undo collect enable

Parameters

None

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a bulk file is created, it is in Stop state and does not participate in data collection and scheduling. After you run the **collect enable** command to enable the bulk file, the bulk file transitions to Ready state and can participate in data collection and scheduling. The **undo collect enable** command disables the bulk file and sets the file state to Stop.

Precautions

Before running the **collect enable** command in a bulk file, run the **transfer** command to configure the primary upload path for the bulk file.

The interval between running the **undo collect enable** and **collect enable** commands in a bulk file must be at least 10 seconds. If the interval is less than 10 seconds, the **collect enable** configuration files.

You can change the maximum number of retransmissions, collection interval, upload interval, and upload holding time, and delete the primary URL for a bulk file only when the bulk file is disabled.

The **collect enable** command takes effect only when the collection interval, upload interval, and upload holding time meet the following requirements: The upload interval is an integral multiple of the collection interval, and the upload holding time is smaller than or equal to the upload interval.

Example

Enable the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer primary protocol ftp username user password pwd host 10 path
folder/bulkstat1
[HUAWEI-bulk-file-iftable] collect enable
```

16.1.6 collect interval

Function

The **collect interval** command sets the statistics collection interval for a bulk file.

The **undo collect interval** command restores the default statistics collection interval.

By default, the statistics collection interval is 5 minutes.

Format

collect interval *interval*

undo collect interval

Parameters

Parameter	Description	Value
interval	Specifies statistics collection interval of a bulk file.	The value can be 5, 10, 15, or 30, in minutes.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

The file upload interval configured using the **transfer interval** command must be an integral multiple of the statistics collection interval configured using this command.

Before changing the statistics collection interval, run the **undo collect enable** command to disable the statistics collection function.

Example

Set the statistics collection interval to 10 minutes for the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] collect interval 10
```

16.1.7 display bulk-stat

Function

The **display bulk-stat** command displays the configuration of the bulk statistics collection function.

Format

display bulk-stat [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a bulk file.	The value is a string of 1 to 31 characters. It can only contain digits, letters, underscores (_), and hyphens (-).

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bulk-stat** command displays the configuration of the bulk statistics collection function, including:

- Maximum number of bulk files
- Number of configured bulk files

- Maximum number of instances that can be collected within 5 minutes
- Basic configurations and status of configured bulk files

The **display bulk-stat** *file-name* command displays detailed information about the bulk file with the specified file name, including:

- File name, storage mode, and format of the bulk file
- Statistics collection interval and upload interval of the bulk file
- The primary URL and secondary URL where the bulk file will be uploaded
- Maximum number of retransmissions of the bulk file
- Storage time of the bulk file
- Current status of the bulk file
- Objects included in the bulk file

Example

Display the configuration of the bulk statistics collection function.

```
<HUAWEI> display bulk-stat
bulk statistic info:
--------------------------------
max bulk file number : 10
current bulk file number: 10
current bulk object number: 2000
max data item per 5 minutes: 40000
--------------------------------
index  bulk file name          collect(min)  transfer(min) status
--------------------------------------------------------------------------------------------------------------
 1     bulk1                  5           5             running
 2     bulk2                  5           15             ready
 3     bulk3                  5           10             stop
 4     bulk4                  5           15             ready
--------------------------------------------------------------------------------------------------------------
```

Table 16-1 Description of the **display bulk-stat** command output

Item	Description
max bulk file number	Maximum number of bulk files.
current bulk file number	Number of configured bulk files.
current bulk object number	Number of configured statistics objects.
max data item per 5 minutes	Maximum number of instances that can be collected within 5 minutes.
index	Index of a configured bulk file.
bulk file name	Name of a configured bulk file. You can run the **bulk-file** command to configure this parameter.
collect(min)	Statistics collection interval of a configured bulk file. You can run the **collect interval** command to configure this parameter.

Item	Description
transfer(min)	Upload interval of a configured bulk file. You can run the **transfer interval** command to configure this parameter.
status	Status of a configured bulk file. The value can be: ● ready: The bulk file is ready for batch performance statistics collection. ● running: The system is collecting performance statistics and writing data in the bulk file. ● stop: The system has finished collecting performance statistics in the current collection interval.

Display detailed information about bulk file **iftable**.

```
<HUAWEI> display bulk-stat iftable
bulk file iftable:
--------------------------------
storage: ephemeral
format: bulkASCII
collect interval: 5 min
transfer interval: 15 min
primary transfer URL: sftp://user:password@host/folder/bulkstat1
secondary transfer URL: sftp://10.1.0.1/tftpboot/user/bulkstat1
transfer retry times: 3
file remain time: 15 min
status: running
last transfer success time: 2006-11-29 11:15
last transfer fail time: NULL
total object number: 2
--------------------------------
index: 1
class: single
OID: 1.3.6.1.2.1.10.94.1.1.10.1.1.0.1
start index: NULL
instance number: NULL
--------------------------------
index: 2
class: column
OID:  1.3.6.1.2.1.10.94.1.1.10.1.2
start index: 1
instance number: 3
```

Table 16-2 Description of the **display bulk-stat iftable** command output

Item	Description
storage	Storage mode of the bulk file. Currently, only the ephemeral storage mode is supported.
format	Format of the bulk file.

Item	Description
collect interval	Statistics collection interval of the bulk file. You can run the **collect interval** command to configure this parameter.
transfer interval	Upload interval of the bulk file. You can run the **transfer interval** command to configure this parameter.
transfer retry times	Maximum number of retransmissions of the bulk file. You can run the **transfer retry** command to configure this parameter.
primary transfer URL	Primary URL where the bulk file will be uploaded. You can run the **transfer** command to configure this parameter.
secondary transfer URL	Secondary URL where the bulk file will be uploaded. You can run the **transfer** command to configure this parameter.
file remain time	Storage time of the bulk file. You can run the **transfer remain-time** command to configure this parameter.
last transfer success time	Time of the last file upload success.
last transfer fail time	Time of the last file upload failure.
total object number	Total number of objects in the bulk file.
index	Index of an object.
class	Type of an object. The value can be: ● single: a single statistics object ● column: bulk statistics object
OID	OID of an object.
start index	● When the value of **class** is **single**, the parameter is displayed **NULL**. ● When the value of **class** is **column**, this parameter indicates the start instance index. You can run the **object** command to configure this parameter.

Item	Description
instance number	- When the value of **class** is **single**, the parameter is displayed **NULL**. - When the value of **class** is **column**, this parameter indicates the number of consecutive instances collected from the start instance index. You can run the **object** command to configure this parameter.

16.1.8 display snmp dynamic-control threshold

Function

The **display snmp dynamic-control threshold** command displays the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

Format

display snmp dynamic-control threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **set snmp dynamic-control threshold** command is used to configure the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks. The **display snmp dynamic-control threshold** command is used to check the current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

Example

Check the current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

```
<HUAWEI> display snmp dynamic-control threshold
Info: The current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks
is 60%.
```

Table 16-3 Description of the **display snmp dynamic-control threshold** command output

Item	Description
The current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is *threshold*.	When the CPU usage reaches the value specified by *threshold*, the device reduces resources for scheduling SNMP tasks.

16.1.9 display snmp-agent

Function

The **display snmp-agent** command displays the engine ID of the local or remote SNMP agent.

Format

display snmp-agent { **local-engineid** | **remote-engineid** }

Parameters

Parameter	Description	Value
local-engineid	Displays the engine ID of the local SNMP agent.	-
remote-engineid	Displays the engine ID of a remote SNMP agent.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the SNMP agent function is enabled, you can run the **display snmp-agent** { **local-engineid** | **remote-engineid** } command to view the engine ID of the local or remote SNMP agent.

The engine ID of the SNMP agent uniquely identifies an SNMP agent in a management domain. The engine ID of the SNMP agent is an important component of the SNMP agent. It schedules and processes SNMP messages, implements security authentication, access control and so on.

Prerequisites

Before running the **display snmp-agent** { **local-engineid** | **remote-engineid** } command to view the engine ID of the local or remote SNMP agent, you need to run the **snmp-agent** command to enable the SNMP agent function.

Precautions

To configure an engine ID for the local SNMP agent, you can run the **snmp-agent local-engineid** command.

Example

Display the engine ID of the local SNMP agent.

```
<HUAWEI> display snmp-agent local-engineid
   SNMP local EngineID: 800007DB03360102101100
```

Table 16-4 Description of the **display snmp-agent local-engineid** command output

Item	Description
SNMP local EngineID	The engine ID of the local SNMP agent.

16.1.10 display snmp-agent community

Function

The **display snmp-agent community** command displays the configured community name.

Format

display snmp-agent community [**read** | **write**] *

Parameters

Parameter	Description	Value
read	Displays the name of a community with read-only permission.	-
write	Displays the name of a community with read and write permission.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

When configuring a management entity, you can use the **display snmp-agent community** command to check the community name configured on the current agent.

If the parameter **read** or **write** is not specified, the names of all communities are displayed.

You have to configure the community name using the **snmp-agent community** command before you run the **display snmp-agent community** command.

Example

Display the current community name.

```
<HUAWEI> display snmp-agent community
   Community name: %^%#.T|&Whvyf$<Gd"I,wXi5SP_6~Nakk6<<+3H:N-h@aJ6d,l0md%HCeAY8~>X=>xV
\JKNAL=124r839v<*%^%#
       Group name: %^%#.T|&Whvyf$<Gd"I,wXi5SP_6~Nakk6<<+3H:N-h@aJ6d,l0md%HCeAY8~>X=>xV
\JKNAL=124r839v<*%^%#
       Alias name:huawei
       Acl:2001
       Storage type: nonVolatile
```

Table 16-5 Description of the **display snmp-agent community** command output

Item	Description
Community name	Name of a community.
Group name	Name of a group.
Alias name	Alias name for a community
Acl	The ACL takes effect on both IPv4 and IPv6 networks.
Ipv4 acl	The ACL takes effect on only IPv4 network.
Ipv6 acl	The ACL takes effect on only IPv6 network.
Storage type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.

16.1.11 display snmp-agent extend error-code status

Function

The **display snmp-agent extend error-code status** command allows you to check whether the function of sending extended error codes to the NMS is enabled on the device.

Format

display snmp-agent extend error-code status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

If the NMS does not receive the extended error codes sent from the device, you can run the **display snmp-agent extend error-code status** command to check whether the function of sending extended error codes to the NMS is enabled on the device.

Example

Display whether the function of sending extended error codes to the NMS is enabled on the device.

```
<HUAWEI> display snmp-agent extend error-code status
Extend error-code status: enabled
```

Table 16-6 Description of the display snmp-agent extend error-code status command output

Item	Description
Extend error-code status	Whether the function of sending extended error codes to the NMS is enabled on the device: • enabled: The function is enabled. • disabled: The function is disabled. You can run the **snmp-agent extend error-code enable** command to configure this parameter.

16.1.12 display snmp-agent group

Function

The **display snmp-agent group** command displays information about SNMP user groups.

Format

display snmp-agent group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays information about a specified SNMP user group. If this parameter is not specified, the system displays information about all SNMP user groups.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When configuring a management object according to the SNMP user group, you can run the **display snmp-agent group** command to view information about the SNMP user group, such as the group name and security model.

Prerequisites

An SNMP user group has been configured using the **snmp-agent group** command.

Example

Display information about all SNMP user groups.

```
<HUAWEI> display snmp-agent group
   Group name: testgroup
       Security model: v3 AuthPriv
       Readview: ViewDefault
       Writeview: dnsmib
       Notifyview: dnsmib
       Storage type: nonVolatile
       Acl: 2001
```

Table 16-7 Description of the **display snmp-agent group** command output

Item	Description
Group name	Name of the SNMP user group.
Security model	Security mode of the SNMP user group: ● v3 AuthPriv: SNMP packets need to be authenticated and encrypted. ● v3 AuthnoPriv: SNMP packets only need to be authenticated. ● v3 noAuthnoPriv: SNMP packets neither need to be authenticated nor encrypted.
Readview	Name of a MIB view with read-only permission of the SNMP user group.
Writeview	Name of a MIB view with read and write permission of the SNMP user group.
Notifyview	Name of a MIB view name with notification permission of the SNMP user group.
Storage-type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.
Acl	The ACL takes effect on both IPv4 and IPv6 networks.
Ipv4 acl	The ACL takes effect on only IPv4 network.
Ipv6 acl	The ACL takes effect on only IPv6 network.

16.1.13 display snmp-agent heartbeat configuration

Function

The **display snmp-agent heartbeat configuration** command displays the configuration of sending heartbeat packets to the NMS.

Format

display snmp-agent heartbeat configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the NMS cannot initiatively obtain the status of the device, run the **snmp-agent heartbeat enable** command to enable the device to send heartbeat packets to the NMS. The device then periodically sends heartbeat packets to the NMS to notify the NMS of its status. To check whether the device is enabled to send heartbeat packets to the NMS, run the **display snmp-agent heartbeat configuration** command.

Example

Display the configuration of sending heartbeat packets to the NMS.

```
<HUAWEI> display snmp-agent heartbeat configuration
SNMP agent heartbeat configuration:
 Status   :     Enabled
 Interval :     60(s)
```

Table 16-8 Description of the **display snmp-agent heartbeat configuration** command output

Item	Description
SNMP agent heartbeat configuration	Configuration of sending heartbeat packets to the NMS.
Status	Whether the device is enabled to send heartbeat packets to the NMS: ● Enabled: The function is enabled. ● Disabled: The function is disabled. You can run the **snmp-agent heartbeat enable** command to configure this parameter.
Interval	The interval at which the device sends heartbeat packets to the NMS. You can run the **snmp-agent heartbeat interval** command to configure this parameter.

16.1.14 display snmp-agent inform

Function

The **display snmp-agent inform** command displays parameters for sending traps to the NMS through Inform packets and statistics about the Inform packets.

Format

display snmp-agent inform [**address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** { *security-name* | **cipher** *security-name* }]

Parameters

Parameter	Description	Value
address udp-domain *ip-address*	Specifies the IP address of the NMS, with the transmission domain of the target host being based on the User Datagram Protocol (UDP). **NOTE** The IP address specified by **address** and the security name specified by **securityname** together identify an NMS.	The value is dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which the NMS belongs. **NOTE** On the VPN, the VPN instance specified by **vpn-instance**, IP address, and security name together identify an NMS.	The value must be an existing VPN instance name.
params	Indicates information about the NMS.	-
securityname *security-name*	Specifies the user security name displayed on the NMS.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32 or 56 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 or 56 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display snmp-agent inform** command displays parameters for sending traps to the NMS through Inform packets and statistics about the Inform packets:

- Number of times Inform packets are retransmitted when the device receives no acknowledgement message from the NMS.
- Timeout period for the acknowledgement from the NMS in response to Inform packets.
- Number of Inform packets retransmitted to the NMS.
- Number of Inform packets in the Inform buffer to be acknowledged by the NMS.
- Number of traps sent through Inform packets to the NMS.
- Number of Inform packets discarded when the Inform buffer is full.
- Number of retransmitted Inform packets that are not acknowledged.
- Number of packets acknowledged by the NMS.

If no parameter is specified in the **display snmp-agent inform** command, global parameters for sending traps through Inform packets, all NMS parameters, and packet statistics mode are displayed.

Example

Displays global parameters for sending traps through Inform packets, all NMS parameters, and packets statistics mode.

```
<HUAWEI> display snmp-agent inform
Global config: resend-times 3, timeout 15s, pending 39
Global status: current notification count 1
Target-host ID: VPN instance/IP-Address/Domain/Security name
-/10.1.1.1/-/%^%#O>tf1ssv|~v3.\IY}|@Gk,:%/IX{!OrFazE#1lxR%^%#:
    Config: resend-times 3, timeout 15s
    Status: retries 0, pending 0, sent 0, dropped 0, failed 0, confirmed 0
```

Table 16-9 Description of the **display snmp-agent inform** command output

Item	Description
Global config	Global Inform parameters: - resend-times: indicates the number of times Inform packets are retransmitted when the device receives no acknowledgement message from the NMS. - timeout: indicates timeout period for the acknowledgement from the NMS in response to Inform packets, in seconds. - pending: indicates the number of Inform packets in the Inform buffer to be acknowledged by the NMS. You can run the **snmp-agent inform** command to configure these parameters.
Global status	Statistics about global Inform packets.
Target-host ID: VPN instance/IP-Address/Domain/Security name	You can run the **snmp-agent inform address** command to configure these parameters (except Domain).
Config	Inform packet parameters of the NMS: - resend-times: indicates the number of times Inform packets are retransmitted when the device receives no acknowledgement message from the NMS. - timeout: Indicates timeout period for the acknowledgement from the NMS in response to Inform packets. You can run the **snmp-agent inform address** command to configure these parameters.

Item	Description
Status	Statistics about Inform packets from the switch to the NMS: ● retries: Number of Inform packets retransmitted to the NMS. ● pending: indicates the number of Inform packets in the Inform buffer to be acknowledged by the NMS. ● sent: Number of traps sent through Inform packets to the NMS. ● dropped: Number of Inform packets discarded when the Inform buffer is full. ● failed: Number of retransmitted Inform packets that are not acknowledged. ● confirmed: Number of packets acknowledged by the NMS.

16.1.15 display snmp-agent mib-view

Function

The **display snmp-agent mib-view** command displays the current MIB view.

Format

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

Parameters

Parameter	Description	Value
exclude	Displays all MIB views that have excluded MIB subtrees configured.	-
include	Displays all MIB views that have included MIB subtrees configured.	-
viewname *view-name*	Displays a specified MIB view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **snmp-agent mib-view** command creates or updates a MIB view. To check the current MIB view, you can run the **display snmp-agent mib-view** command.

Precautions

The **snmp-agent** command has been run to enable the SNMP Agent. Otherwise, an error message is displayed.

Example

Display the current MIB view.

```
<HUAWEI> display snmp-agent mib-view
   View name:ViewDefault
       MIB Subtree:internet
       Subtree mask:F0(Hex)
       Storage-type: nonVolatile
       View Type:included
       View status:active
```

Table 16-10 Description of the **display snmp-agent mib-view** command output

Item	Description
View name	MIB view name. You can run the **snmp-agent mib-view** command to configure this parameter.
MIB Subtree	MIB subtree. You can run the **snmp-agent mib-view** command to configure this parameter.
Subtree mask	MIB subtree mask.
Storage type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.

Item	Description
View Type	Whether the MIB subtree can be accessed by a MIB view: ● included: The MIB subtree can be accessed by a MIB view. ● excluded: The MIB subtree cannot be accessed by a MIB view. You can run the **snmp-agent mib-view** command to configure this parameter.
View status	Indicates the status of the MIB view.

16.1.16 display snmp-agent notification-log

Function

The **display snmp-agent notification-log** command displays information saved in the trap log buffer.

Format

display snmp-agent notification-log [**info** | **logtime** *starttime* **to** *endtime* | **size** *size*]

Parameters

Parameter	Description	Value
info	Displays parameters of trap logs recorded by the device and statistics about trap logs.	-
logtime *starttime* **to** *endtime*	Specifies the start time and end time of trap logs to be displayed: ● *starttime*: specifies the start time of trap logs. ● *endtime*: specifies the end time of trap logs.	The value is in the HH:MM:SS YYYY/MM/DD format, where HH:MM:SS indicates the hour, minute, and second and YYYY/MM/DD indicates the year, month, and day. HH ranges from 0 to 23; MM and SS range from 0 to 59. YYYY ranges from 2000 to 2099; MM ranges from 1 to 12; DD ranges from 1 to 31. The end time must be later than the start time.

Parameter	Description	Value
size *size*	Specifies the number of latest trap logs to be displayed.	The value is an integer that ranges from 1 to 5000.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use any of the following methods to view logs in the trap log buffer using the **display snmp-agent notification-log** command:

- Specify the start time and end time of trap logs to be displayed.
- Specify the number of latest trap logs to be displayed.
- Specify no parameter to view all trap logs.

Example

Display parameters of trap logs recorded by the device and statistics about trap logs.

```
<HUAWEI> display snmp-agent notification-log info
Notification log information :
Notification Admin Status: enable
GlobalNotificationsLogged: 0
GlobalNotificationsBumped: 0
GlobalNotificationsLimit: 500
GlobalNotificationsAgeout: 24
Total number of notification log(s): 0
```

Table 16-11 Description of the **display snmp-agent notification-log info** command output

Item	Description
Notification log information	Parameters of trap logs recorded by the device and statistics about trap logs.
Notification Admin Status	Whether the function of recording trap logs is enabled on the device: - enable: The function is enabled. - disable: The function is disabled. You can run the **snmp-agent notification-log enable** command to configure this parameter.
GlobalNotificationsLogged	Number of trap logs recorded currently.

Item	Description
GlobalNotificationsBumped	Number of logs recording discarded traps.
GlobalNotificationsLimit	Maximum number of trap logs that can be saved. You can run the **snmp-agent notification-log** command to configure this parameter.
GlobalNotificationsAgeout	Aging time of trap logs. You can run the **snmp-agent notification-log** command to configure this parameter.
Total number of notification log(s)	Total number of recorded trap logs.

Display the latest 20 trap logs. (In this example, only one trap log is available in the system.)

```
<HUAWEI> display snmp-agent notification-log size 20
 Total number of notifications log(s) : 1

LogTable :
  LogIndex= 12
  LogTime= 229323
  LogDateAndTime= 2007/3/8 10:28:16
  LogEngineID= 000007DB7F00000100004CFB
  LogEngineTAddress= 192.168.39.1/162
  LogEngineTDomain= snmpUDPDomain
  LogContextEngineID= null
  LogContextName= null
  LogNotificationID= 1.3.6.1.4.1.2011.6.10.2.1
LogVariableTable :
  LogVariableIndex= 1
  LogVariableOID= 1.3.6.1.2.1.1.3
  LogVariableValueType= TimeTicksLogVariableValue = 229323
  LogVariableIndex= 2
  LogVariableOID= 1.3.6.1.6.3.1.1.4.1
  LogVariableValueType= OidLogVariableValue = 1
  LogVariableIndex= 3
  LogVariableOID= 1.3.6.1.4.1.2011.6.10.1.1.7.1.3.29
  LogVariableValueType= Integer32LogVariableValue = 1
  LogVariableIndex= 4
  LogVariableOID= 1.3.6.1.4.1.2011.6.10.1.1.7.1.4.29
  LogVariableValueType= Integer32LogVariableValue = 3
  LogVariableIndex= 5
  LogVariableOID= 1.3.6.1.4.1.2011.6.10.1.1.7.1.5.29
  LogVariableValueType= Integer32LogVariableValue = 2
```

Table 16-12 Description of the **display snmp-agent notification-log size 20** command output

Item	Description
LogTable	Log table.
LogIndex	Index of the log.

Item	Description
LogTime	Difference between the time when the log was recorded and the time when the system started. The unit is 10 ms.
LogDateAndTime	Absolute date and time when the log was recorded.
LogEngineID	Engine ID of the SNMP message recorded in the log.
LogEngineTAddress	IP address and port number of the SNMP message recorded in the log.
LogEngineTDomain	Transmission type of the SNMP message recorded in the log.
LogContextEngineID	Engine ID of context of the SNMP message recorded in the log.
LogContextName	Secure user name, IP address, and VPN instance name.
LogNotificationID	OID of the trap object recorded in the log.
LogVariableTable	Variable table of the log.
LogVariableIndex	Index of a variable.
LogVariableOID	OID of a variable.
LogVariableValueType	Value type of a variable.
LogVariableValue	Value of a variable.

16.1.17 display snmp-agent notify-filter-profile

Function

The **display snmp-agent notify-filter-profile** command displays information about a specified trap filter profile or all trap filter profiles.

Format

display snmp-agent notify-filter-profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a trap filter profile.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent notify-filter-profile** command to view information about configured trap filter profiles. The command can display all the configured trap filter profiles or a specified trap file profile.

Example

Display information about configured trap filter profiles.

```
<HUAWEI> display snmp-agent notify-filter-profile
  Notify-filter name:snmpv2
  Notify-filter Subtree:snmpV2
  Notify-filter Subtree mask:F8(Hex)
  Notify-filter Storage-type:nonVolatile
  Notify-filter Type:included
  Notify-filter status:active
```

Table 16-13 Description of the **display snmp-agent notify-filter-profile** command output

Item	Description
Notify-filter name	Name of a trap filter profile. You can run the **snmp-agent notify-filter-profile** command to configure this parameter.
Notify-filter Subtree	Filtered MIB subtree. You can run the **snmp-agent notify-filter-profile** command to configure this parameter.
Notify-filter Subtree mask	Mask of a MIB subtree.

Item	Description
Notify-filter Storage-type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.
Notify-filter Type	Whether traps of the MIB subtree are sent to the NMS: ● included: Traps of the MIB subtree are sent to the NMS. ● excluded: Traps of the MIB subtree are not sent to the NMS. You can run the **snmp-agent notify-filter-profile** command to configure this parameter.
Notify-filter status	Status of a trap filter profile.

16.1.18 display snmp-agent statistics

Function

The **display snmp-agent statistics** command displays statistics about SNMP packets on the switch.

Format

display snmp-agent statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

In an SNMP management system, the NMS and the SNMP Agent exchange SNMP messages as follows:

- The NMS acts as a manager to send an SNMP Request message to the SNMP Agent.
- The SNMP Agent searches the MIB on the device for the required information and sends an SNMP Response message to the NMS.

- When the trap triggering conditions are met, the SNMP Agent sends a trap to the NMS to report the event occurring on the device. In this manner, the network administrator can process the event occurring on the network in time.

You can run the **display snmp-agent statistics** command to analyze the statistics about SNMP packets exchanged between the NMS and SNMP Agent, facilitating fault location.

NOTE

If large number of messages are received in short period, a great number of CPU resources are occupied. The number of received messages depends on the frequency at which the NMS sends the Request messages.

Example

Display the statistics about SNMP packets on the switch.

```
<HUAWEI> display snmp-agent statistics
  0 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used a SNMP community name not known
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  7 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  0 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status
  0 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 GetRequest-PDU accepted and processed
  0 GetNextRequest-PDU accepted and processed
  0 GetResponse-PDU accepted and processed
  0 SetRequest-PDU accepted and processed
  0 Trap-PDU accepted and processed
  0 Inform-PDU sent
  0 Inform ACK PDUs failed to be processed
  0 Inform ACK PDUs successfully processed
```

Table 16-14 Description of the **display snmp-agent statistics** command output

Item	Description
Messages delivered to the SNMP entity	Total number of received SNMP messages
Messages which were for an unsupported version	Number of SNMP messages with version errors
Messages which used a SNMP community name not known	Number of SNMP messages with community name errors
Messages which represented an illegal operation for the community supplied	Number of SNMP messages with authority errors corresponding to community name
ASN.1 or BER errors in the process of decoding	Number of SNMP messages with encoding errors

Item	Description
Messages passed from the SNMP entity	Total number of sent SNMP messages
SNMP PDUs which had badValue error-status	Number of SNMP messages with bad values
SNMP PDUs which had genErr error-status	Number of SNMP messages with general errors
SNMP PDUs which had noSuchName error-status	Number of SNMP messages with requests for non-existing MIB objects
SNMP PDUs which had tooBig error-status	Number of SNMP messages with Too_big errors
MIB objects retrieved successfully	Number of variables requested by NMS
MIB objects altered successfully	Number of variables set by NMS
GetRequest-PDU accepted and processed	Number of received SNMP Get-request messages
GetNextRequest-PDU accepted and processed	Number of received SNMP GetNext-request messages
GetResponse-PDU accepted and processed	Number of sent SNMP Get-response messages
SetRequest-PDU accepted and processed	Number of received SNMP Set-request messages
Trap-PDU accepted and processed	Number of sent SNMP Trap messages
Inform-PDU sent	Number of sent SNMP Inform messages
Inform ACK PDUs failed to be processed	Number of SNMP Inform messages received with no acknowledgement
Inform ACK PDUs successfully processed	Number of SNMP Inform messages received with acknowledgement

16.1.19 display snmp-agent statistics mib

Function

The **display snmp-agent statistics mib** command displays statistics about the NMS's operations on MIB objects.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display snmp-agent statistics mib [[**vpn-instance** *vpn-instance-name*] { **address** *ipv4-address* | **ipv6** *ipv6-address* }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.
address *ipv4-address*	Specifies an IPv4 address.	-
ipv6 *ipv6-address*	Specifies an IPv6 address.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An NMS performs operations on MIB objects to manage devices. To check these operation statistics, run the **display snmp-agent statistics mib** command. The command output displays names, access frequencies, and handling dates of MIB objects.

If no NMS is specified, the **display snmp-agent statistics mib** command displays statistics about the operations performed by all NMSs (that is, IPv4+VPN, IPv6+VPN, IPv4, and IPv6 NMSs) on MIB objects.

Follow-up Procedure

If the NMS accesses a great amount of MIB node information and statistics do not need to be saved, run the **reset snmp-agent statistics mib** command to delete the statistics.

Example

Display all statistics about the NMS's operations on MIB objects.

```
<HUAWEI> display snmp-agent statistics mib
-------------------------------------------------------------------------------------
ip address:192.168.1.4, total mib node number:9
   SUMMARY:    Total set:0,Total get:9,Total get-next:75
-------------------------------------------------------------------------------------
MibNode                    Set       Get       GetNext    MaxTime MinTime
AveTime

ifEntry                  0         0         75        0       0       0
ifNumber                   0         1         0         0       0       0
sysContact                 0         1         0         0       0       0
sysDescr                 0         1         0         0       0       0
sysLocation                0         1         0         0       0       0
sysName                    0         1         0         0       0       0
sysObjectID                0         1         0         0       0       0
sysServices              0         1         0         0       0       0
sysUpTime                  0         2         0         0       0       0
```

Display the statistics about the operations performed by the NMS with the IP address of 192.168.1.3 in the VPN instance **aa**.

```
<HUAWEI> display snmp-agent statistics mib vpn-instance aa address 192.168.1.3
-------------------------------------------------------------------------------------
vpn instance:aa, ip address:192.168.1.3, total mib node number:
1
   SUMMARY:    Total set:0,Total get:1,Total get-next:0
-------------------------------------------------------------------------------------
MibNode                    Set       Get       GetNext    MaxTime MinTime
AveTime

sysDescr                 0         1         0         0       0       0
```

Table 16-15 Description of the **display snmp-agent statistics mib** command output

Item	Description
ip address	IP address of the NMS.
vpn instance	VPN instance name
total mib node number	Total number of MIB objects accessed by the NMS.
SUMMARY	Abstract of statistics about the NMS's operations on MIB objects.
Total set	Total number of Set operations performed on all MIB objects.
Total get	Total number of Get operations performed on all MIB objects.
Total get-next	Total number of GetNext operations performed on all MIB objects.
MibNode	MIB object name.
Set	Number of the Set operations performed on a specified MIB object.
Get	Number of the Get operations performed on a specified MIB object.

Item	Description
GetNext	Number of the GetNext operations performed on a specified MIB object.
MaxTime	Maximum time for an operation performed on MIB objects, in milliseconds.
MinTime	Minimum time for an operation performed on MIB objects, in milliseconds.
AveTime	Average time for an operation performed on MIB objects, in milliseconds.

16.1.20 display snmp-agent sys-info

Function

The **display snmp-agent sys-info** command displays SNMP information about the device, including contact information of device maintenance personnel, physical location of the device, and SNMP version running on the device.

Format

display snmp-agent sys-info [**contact** | **location** | **version**] *

Parameters

Parameter	Description	Value
contact	Displays contact information of device maintenance personnel.	-
location	Displays the physical location of the device.	-
version	Displays the SNMP version running on the device.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent sys-info** command to display SNMP information about the device, including:

- Contact information of device maintenance personnel
- Physical location of the device
- SNMP version running on the device

If no parameter is specified, all information is displayed.

Example

Display all SNMP information about the device.

```
<HUAWEI> display snmp-agent sys-info
   The contact person for this managed node:
           R&D Beijing, Huawei Technologies Co.,
Ltd.

   The physical location of this node:
           Beijing China

   SNMP version running in the system:
           Polling: SNMPv1:disable, SNMPv2c:disable,
SNMPv3:enable
           Trap   : SNMPv1:disable, SNMPv2c:enable,
SNMPv3:disable
```

Display the SNMP version running on the device.

```
<HUAWEI> display snmp-agent sys-info version
   SNMP version running in the system:
           Polling: SNMPv1:disable, SNMPv2c:disable,
SNMPv3:enable
           Trap   : SNMPv1:disable, SNMPv2c:enable,
SNMPv3:disable
```

Display contact information of device maintenance personnel.

```
<HUAWEI> display snmp-agent sys-info contact
   The contact person for this managed node:
           R&D Beijing, Huawei Technologies Co.,
Ltd.
```

Display the physical location of the device.

```
<HUAWEI> display snmp-agent sys-info location
  The physical location of this node:
           Beijing China
```

Table 16-16 Description of the **display snmp-agent sys-info** command output

Item	Description
The contact person for this managed node	Contact information of device maintenance personnel, which is useful in event of emergencies. You can run the **snmp-agent sys-info** command to configure this parameter.
The physical location of this node	Physical location of the device. You can run the **snmp-agent sys-info** command to configure this parameter.

Item	Description
SNMP version running in the system	SNMP version running on the device. The value can be any combination of SNMPv1, SNMPv2c, and SNMPv3. When multiple versions are configured, the NMS manages the device using multiple SNMP versions. You can run the **snmp-agent sys-info** command to configure this parameter.
Polling	● SNMPv1: The function status is **enable** only when SNMPv1 is enabled and an SNMPv1 community name is configured. Otherwise, it is **disable**. ● SNMPv2: The function status is **enable** only when SNMPv2 is enabled and an SNMPv2 community name is configured. Otherwise, it is **disable**. ● SNMPv3: The function status is **enable** only when SNMPv3 is enabled and an SNMPv3 user name (excluding remote-engineid users) is configured. Otherwise, it is **disable**.
Trap	● SNMPv1: The trap host status is **enable** only when SNMPv1 is enabled and a trap host is configured. Otherwise, it is **disable**. ● SNMPv2: The trap host status is **enable** only when SNMPv2 is enabled and a trap host is configured. Otherwise, it is **disable**. ● SNMPv3: The trap host status is **enable** only when SNMPv3 is enabled and a trap host is configured. Otherwise, it is **disable**.

16.1.21 display snmp-agent target-host

Function

The **display snmp-agent target-host** command displays the configurations of destination hosts of all alarms.

Format

display snmp-agent target-host

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent target-host** command to display the configurations of destination hosts of all traps, including IP addresses of the hosts, modes in which traps are sent, security name used to send traps, and SNMP versions. At present, the system can save the configuration of a maximum of 20 destination hosts. Therefore, the **display snmp-agent target-host** command can view the configuration of a maximum of 20 destination hosts.

Example

Display the configurations of destination hosts of all alarms.

```
<HUAWEI> display snmp-agent target-host
Target-host NO. 1
-----------------------------------------------------------
  IP-address    : 10.1.2.1
  Domain        : -
  Source interface : -
  VPN instance  : -
  Security name : %^%#uq/!YZfvW4*vf[~C|.:Cl}UqS(vXd#wwqR~5M(rU%%^%#
  Port          : 162
  Type          : trap
  Version       : v2c
  Level         : No authentication and privacy
  NMS type      : HW NMS
  With ext-vb:  : No
-----------------------------------------------------------
```

Table 16-17 Description of the **display snmp-agent target-host** command output

Parameter	Description
Target-host NO	Target host number, which is generated based on the sequence in which the target host is configured. You can run the **snmp-agent target-host inform** or **snmp-agent target-host trap** command to configure parameters of the target host.
IP-address	IP address of the target host.
Domain	Domain name of the target host.
Source interface	Source interface that sends traps.
VPN instance	VPN instance to which the target host belongs.
Security name	Security name used to send traps.
Port	UDP port number used to send traps.

Parameter	Description
Type	Mode in which traps are sent: ● trap ● inform
Version	SNMP version: ● v1 ● v2c ● v3
Level	Security mode of packets: ● Authentication: Packets only need to be authenticated. ● Privacy: Packets need to be authenticated and encrypted. ● No authentication and privacy: Packets need neither to be authenticated nor encrypted.
NMS type	Type of the target host: ● NMS: indicates a network management system, which can be a Huawei NMS or an NMS from another vendor. ● HW NMS: indicates a Huawei NMS. The traps sent to the Huawei NMS can contain more detailed information.
With ext-vb	Whether the trap sent to the target host carries extended bound variables: ● No ● Yes

16.1.22 display snmp-agent trap all

Function

The **display snmp-agent trap all** command displays whether the switch is enabled to send alarms of all features to the NM station.

Format

display snmp-agent trap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap all** command to check whether the switch is enabled to send alarms of specified features to the NMS. You can configure this function by running **snmp-agent trap enable**, **snmp-agent trap enable feature-name**, and **snmp-agent trap disable**.

Example

Check whether the switch is enabled to send alarms of specified features to the NMS.

```
<HUAWEI> display snmp-agent trap all
------------------------------------------------------------------------------
Feature name: INFO
Trap number : 2
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwICLogFileAging                on                       on
hwICLogBufferLose               on                       on
------------------------------------------------------------------------------
---- More ----
```

Table 16-18 Description of the display snmp-agent trap all command output

Item	Description
Feature name	Name of the feature that generates alarms.
Trap number	Number of alarms generated by this feature.
Trap name	Name of the alarm.
Default switch status	Default status of the alarm: ● on: The switch is enabled to send this alarm to the NMS. ● off: The switch is disabled to send this alarm to the NMS.
Current switch status	Current status of the alarm: ● on: The switch is enabled to send this alarm to the NMS. ● off: The switch is disabled to send this alarm to the NMS. This status can be configured using the **snmp-agent trap enable feature-name** command.

16.1.23 display snmp-agent trap feature-name all

Function

The **display snmp-agent trap feature-name all** command displays whether the device is enabled to send alarms of specified features to the NMS.

Format

display snmp-agent trap feature-name *feature-name* **all**

Parameters

Parameter	Description	Value
feature-name	Specifies the feature that generates alarms.	acle, adpvxlan, arp, asmngtrap, bfd, bgp, cfgmgr, clkm, configuration, datasync, dhcp, dldp, easyoperatrap, efm, emdi, entityexttrap, entitymib, entitytrap, eoam-1ag, eoam-y1731, erps, error-down, etrunk, fm, ftp_server, gtl, hgmp, hsb-trap, http, ifnet, ifpdt, igmp, info, ip, ipfpm, iplpm, ipsec, ipv6, isis, l2bptnl, l2if, l2ifppi, l2vpn, l3mb, l3vpn, lacp, lbdt, ldp, line, lldptrap, loopdetect, mad, mcast, mid_aaa, mid_am, mid_eapol, mid_web, mld, mpls, mpls_lspm, mpls_rsvp, mrm, msdp, mstp, ntp, ospf, ospfv3, pim, pim-std, pki, pm, ptp, qose, radius, rip, rm, rmon, rrpp, securitytrap, sindex, snmp, srmtrap, sspadp, stack, swithsrvres, sysres, system, tcp, trunk, tunnel-te, uni-topomng, uni-tplm, uni-vermng, unimbrtrap, usbloadtrap, vbst, vcmp, vfs, vplsoam, vrrp, wlan

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name all** command to check whether the switch is enabled to send alarms of specified features to the NMS. You can use the **snmp-agent trap enable feature-name** command to enable this function.

Precautions

- The feature name asmngtrap, uni-topomng, uni-tplm, uni-vermng, and unimbrtrap are supported only on the SVF parent.
- The feature name etrunk is supported only on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The feature name igmp, mld, mrm, msdp, pim-std, and pim are supported only on the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The feature name gtl takes effect only on the device that loads the license control item.
- If the IS-IS trap function is enabled before a version upgrade, you need to run the **snmp-agent trap enable feature-name isis** command to re-enable the trap function after the version upgrade. Otherwise, the previous configuration is lost.

Example

Display the status of the ARP alarms.

```
<HUAWEI> display snmp-agent trap feature-name arp all
------------------------------------------------------------------------------
Feature name: ARP
Trap number : 4
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwEthernetARPSpeedLimitAlarm     on                        on
hwEthernetARPThresholdExceedAlarm
                               on                      on
hwEthernetARPThresholdResumeAlarm
                               on                      on
hwEthernetARPIPConflictEvent     on                        on
```

Table 16-19 Description of the display snmp-agent trap feature-name all command output

Item	Description
Feature name	Name of the feature that generates alarms.
Trap number	Number of alarms generated by this feature.
Trap name	Name of the alarm. For details about the alarm, see the Alarm Handling.
Default switch status	Default status of the alarm: ● on: The switch is enabled to send this alarm to the NMS. ● off: The switch is disabled to send this alarm to the NMS.

Item	Description
Current switch status	Current status of the alarm: ● on: The switch is enabled to send this alarm to the NMS. ● off: The switch is disabled to send this alarm to the NMS. This status can be configured using the **snmp-agent trap enable feature-name** command.

16.1.24 display snmp-agent usm-user

Function

The **display snmp-agent usm-user** command displays information about an SNMPv3 user.

Format

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Parameters

Parameter	Description	Value
engineid *engineid*	Displays information about an SNMPv3 user with a specified SNMP entity engine ID.	-
group *group-name*	Displays the SNMPv3 user belonging to a specified user group.	-
username *user-name*	Displays information about a specified SNMPv3 user.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent usm-user** command to display the SNMPv3 user information configured through the **snmp-agent usm-user** command. The

SNMPv3 user here refers to the remote user that carries out SNMPv3 management. The displayed information about an SNMPv3 user includes the user name, authentication protocol, encryption algorithm, and user group to which the SNMPv3 user belongs.

Example

Display information about all current SNMPv3 users.

```
<HUAWEI> display snmp-agent usm-user
   User name: myuser01
       Engine ID: 800007DB03360102101100 active
       Authentication Protocol: sha2-256
       Privacy Protocol: aes256
       Group name: mygroup
       Ipv4 acl : 2000
       Ipv6 acl : 2004
<HUAWEI> display snmp-agent usm-user
   User name: myuser02
       Engine ID: 800007DB03360102101100 active
       Authentication Protocol: sha2-256
       Privacy Protocol: aes256
       Group name: mygroup
       Acl: 2000
```

Table 16-20 Description of the **display snmp-agent usm-user** command output

Item	Description
User name	SNMPv3 user name.
Engine ID	Local SNMP engine ID.
active	Status of the SNMPv3 user.
Authentication Protocol	Authentication algorithm used for the SNMPv3 user.
Privacy Protocol	Encryption algorithm used for the SNMPv3 user.
Group name	User group to which the SNMPv3 user belongs.
Acl	The ACL takes effect on both IPv4 and IPv6 networks.
Ipv4 acl	The ACL takes effect on only IPv4 network.
Ipv6 acl	The ACL takes effect on only IPv6 network.

16.1.25 enable snmp trap updown

Function

The **enable snmp trap updown** command enables an interface to send a trap to the NMS when the protocol status of the interface changes.

The **undo enable snmp trap updown** command disables an interface from sending a trap to the NMS when the protocol status of the interface changes.

By default, an interface sends a Trap message to the NMS when the protocol status of the interface changes.

Format

enable snmp trap updown

undo enable snmp trap updown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enable snmp trap updown** command is used to enable an interface to send a Trap message to the NMS when the protocol status of the interface changes, which helps the NMS monitor the interface status in real time.

Precautions

By default, the function of sending a Trap message to the NMS when the protocol status of the interface changes is enabled. If an interface alternates between Up and Down, it will frequently send Trap messages to the NMS, causing the NMS to be busy processing these Trap messages. In this case, you can run the **undo enable snmp trap updown** command to disable the interface from sending trap messages to the NMS.

Example

Disable an interface from sending a trap to the NMS when the protocol status of the interface changes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo enable snmp trap updown
```

16.1.26 format (bulk file view)

Function

The **format** command configures the format for a bulk file.

The **undo format** command restores the default format of a bulk file.

By default, the format of a bulk file is bulkascii (text format).

Format

format bulkascii

undo format

Parameters

Parameter	Description	Value
bulkascii	Indicates the text format.	-

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Currently, the system supports only the text format of bulk files. The command can be upgraded to support more file formats, such as word and xml.

Example

Set the format of the bulk file **iftable** to bulkascii.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] format bulkascii
```

16.1.27 object

Function

The **object** command creates a statistics object for a bulk file.

The **undo object** command deletes a statistics object.

By default, no statistics object exists in a bulk file.

Format

object *oid* **class** { **single** | **column** [**start-index** *start-index*] [**instance-number** *instance-number*] }

undo object *oid* **class** { **single** | **column** }

Parameters

Parameter	Description	Value
oid	Specifies the OID of a statistics object. The value is a numeric string of 1 to 127 characters, in dotted notation.	-
class single	Creates a single statistics object.	-
class column	Creates a bulk statistics object.	-
start-index *start-index*	Specifies the start instance index when the object type is set to **column**. The value is a numeric string of 1 to 127 characters, in dotted notation. The value 0 indicates that the system collects statistics from the first instance in the column. The default value is 0.	-
instance-number *instance-number*	Specifies the number of consecutive instances to be collected from the start instance when the object type is set to **column**. The value is an integer that ranges from 0 to 65535. The value 0 indicates that the system stops collecting statistics at the end of the column. If the instance range specified by the *start-index* and *instances-number* parameters is beyond the actual instance range, the system collects statistics within the actual instance range. The default value is 0.	-

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **object** *oid* **class single** command creates a statistics object for the data item of a single instance. In this command, the *oid* parameter must contain the instance index. When the instance index is set to 0, the data item is a scalar quantity. When the instance index is set to a non-0 value, the data item is an instance in the column. If the object has been configured in the bulk file, the system displays an error message indicating that the OID already exists.

The **object** *oid* **class column start-index** *start-index* **instance-number** *instance-number* command creates a bulk statistics object to collect statistics about some or all types of instances in a column. You must specify the *start-index* and *instances-number* parameters to specify the start instance index and the number of instances. If the instance range specified by the *start-index* and *instances-number* parameters is beyond the actual instance range, the system collects statistics within the actual instance range. If the object has been configured in the bulk file, the system displays an error message indicating that the OID already exists.

Precautions

The configuration of **object** or **undo object** takes effect in the next collection interval.

The OID specified in the command must exist in the MIB tree. If the specified OID exists in the bulk file, the system displays a message indicating that the OID has been configured. Delete this OID and then reconfigure it.

Example

Add a single statistics object to the bulk file **ifOutOctets**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file ifOutOctets
[HUAWEI-bulk-file-ifOutOctets] object 1.3.6.1.2.1.2.2.1.16.1 class single
```

Add a bulk statistics object to the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] object 1.3.6.1.2.1.2.2.1.16 class column start-index 1 instance-number 10
```

16.1.28 reset snmp-agent statistics mib

Function

The **reset snmp-agent statistics mib** command clears statistics about the NMS's operations on MIB objects.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset snmp-agent statistics mib [**address** *ipv4-address* | **ipv6** *ipv6-address* | **vpn-instance** *vpn-instance-name* **address** *ipv4-address*]

Parameters

Parameter	Description	Value
address *ipv4-address*	Specifies an IPv4 address.	-

Parameter	Description	Value
ipv6 *ipv6-address*	Specifies an IPv6 address.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An NMS performs operations on MIB objects to manage devices. You can run the **display snmp-agent statistics mib** command to check the operation statistics.

If the NMS accesses a great amount of MIB node information and statistics do not need to be saved, run the **reset snmp-agent statistics mib** command to delete the statistics.

If no NMS is specified, the **reset snmp-agent statistics mib** command clears statistics about the operations performed by all NMSs (that is, IPv4+VPN, IPv6+VPN, IPv4, and IPv6 NMSs) on MIB objects.

Precautions

Operation statistics cannot be restored after they are cleared. Exercise caution when running the **reset snmp-agent statistics mib** command.

Example

Clear all statistics about the NMS's operations on MIB objects.

```
<HUAWEI> reset snmp-agent statistics mib
```

16.1.29 set snmp dynamic-control threshold

Function

The **set snmp dynamic-control threshold** command configures the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

The **undo set snmp dynamic-control threshold** command restores the default setting.

By default, a device reduces resources for scheduling SNMP tasks when the CPU usage reaches 75%.

Format

set snmp dynamic-control threshold *threshold*

undo set snmp dynamic-control threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the CPU usage threshold.	The value is an integer that ranges from 30 to 90, in percentage.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is 75%. That is, a device reduces resources for scheduling SNMP tasks when the CPU usage exceeds 75%. This reduces CPU usage of SNMP tasks. You can run the **set snmp dynamic-control threshold** command to change the CPU usage threshold based on your site scenario.

Example

Set the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks to 60%.

```
<HUAWEI> system-view
[HUAWEI] set snmp dynamic-control threshold 60
Info: The CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is set to
60%. That is, when the system CPU usage exceeds 70%, the device reduces resources for scheduling SNMP
tasks. Continue?[Y/N]:y
```

16.1.30 snmp-agent

Function

The **snmp-agent** command enables the SNMP agent function.

The **undo snmp-agent** command disables the SNMP agent function.

By default, the SNMP agent function is disabled.

Format

snmp-agent

undo snmp-agent

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before configuring SNMP, you need to enable the SNMP agent function.

By executing the **snmp-agent** command with any parameter enables the SNMP agent function. For example, if you execute the **snmp-agent community** command, the community name gets created and also SNMP agent function is enabled.

Precautions

After the **snmp-agent** command is executed, both the IPv4 and IPv6 services are enabled for the SNMP agent. By default, the switch listens on the IP address 0.0.0.0, that is, all IP addresses. This default setting is a threat to data confidentiality. You are advised to run the **snmp-agent protocol source-interface** *interface-type interface-number* command to specify the source interface that receives and responds to SNMP requests from the NMS.

Example

Enable the SNMP agent function.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent
```

Disable the SNMP agent function.

```
<HUAWEI> system-view
[HUAWEI] undo snmp-agent
```

16.1.31 snmp-agent acl

Function

The **snmp-agent acl** command configures an SNMP ACL.

The **undo snmp-agent acl** command deletes the configured SNMP ACL.

By default, no SNMP ACL is configured.

Format

snmp-agent acl { *acl-number* | *acl-name* }

snmp-agent acl-ipv4 { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }]

snmp-agent acl-ipv6 { *acl-number* | *acl-name* }

undo snmp-agent acl

Parameters

Parameter	Description	Value
acl	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When using the NMS to manage devices, you can run the **snmp-agent acl** command to configure an SNMP ACL on the devices and restrict the NMS's access to the devices to enhance network security.

Precautions

- The SNMP ACLs take precedence over ACLs based on SNMP community names, SNMP groups, and SNMP users.
- To specify the same ACL on both IPv4 and IPv6 networks, you can only run the **snmp-agent acl** { *acl-number* | *acl-name* } command. For example, to allow the NMS that matches ACL 2000 to access the device using SNMP on

both IPv4 and IPv6 networks, run the **snmp-agent acl 2000** command instead of the **snmp-agent acl-ipv4 2000 acl-ipv6 2000** command.

- If this command is run more than once, the latest configuration overrides the previous one.

Example

Configure SNMP ACL 2000 to allow NM stations that match rules defined in ACL 2000 to access the device using SNMP.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-basic-2000] rule permit source 192.168.10.10 0
[HUAWEI-basic-2000] quit
[HUAWEI] snmp-agent acl 2000
```

16.1.32 snmp-agent blacklist ip-block disable

Function

The **snmp-agent blacklist ip-block disable** command disables the SNMP blacklist function.

The **undo snmp-agent blacklist ip-block disable** command enables the SNMP blacklist function.

By default, the SNMP blacklist function is enabled.

Format

snmp-agent blacklist ip-block disable

undo snmp-agent blacklist ip-block disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the SNMP blacklist function is enabled, if an SNMP user fails to connect to the device, the IP address used by the user is recorded in the SNMP blacklist on the device; that is, the IP address is locked. Within the locking period, the SNMP user cannot connect to the device.

If the connection fails to be established several times in succession, the device locks the IP address for 8 seconds on the first attempt, 16 seconds on the second attempt, and 32 seconds on the third attempt. Any subsequent failed attempts result in the IP address being locked for 5 minutes. When the locking period arrives, the IP address is automatically unlocked.

Precautions

After the SNMP blacklist function is disabled, the IP addresses of SNMP users who fail to connect to the device are not locked. The device is vulnerable to attacks and cracking by unauthorized users, affecting device security. Therefore, you are advised to enable the IP blacklist function.

After the SNMP blacklist function is disabled, locked IP addresses are unlocked immediately.

Example

Enable the SNMP blacklist function.

```
<HUAWEI> system-view
[HUAWEI] undo snmp-agent blacklist ip-block disable
```

16.1.33 snmp-agent community

Function

The **snmp-agent community** command configures the SNMPv1 or SNMPv2c read-write community name.

The **undo snmp-agent community** command is used to delete the configuration of the community name.

By default, the community name is not configured.

Format

snmp-agent community { **read** | **write** } { *community-name* | **cipher** *community-name* } [**mib-view** *view-name* | **acl** { *acl-number* | *acl-name* } | **alias** *alias-name*] *

snmp-agent community { **read** | **write** } [**cipher**] *community-name* [**mib-view** *view-name*] **acl-ipv4** { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }] [**alias** *alias-name*]

snmp-agent community { **read** | **write** } [**cipher**] *community-name* [**mib-view** *view-name*] **acl-ipv6** { *acl-number* | *acl-name* } [**alias** *alias-name*]

undo snmp-agent community *community-name*

undo snmp-agent community { **read** | **write** } [**cipher**] *community-name*

Parameters

Parameter	Description	Value
read	Indicates that the community with a specified name has the read-only rights in the specified view.	-
write	Indicates that the community with a specified name has the read-write rights in the specified view.	-
community-name	Specifies the name of a community. The community name is displayed in cipher text in the configuration file.	The value is a string of 8 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cipher *community-name*	Specifies the community name in plain text or in cipher text. The community name is displayed in cipher text in the configuration file.	The value is a string of 8 to 32, 44, 56, 80 or 88 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 8 to 31 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32, 44, 56, 80 or 88 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.
mib-view *view-name*	Specifies a MIB view that the community name can access.	It is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
acl	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-

Parameter	Description	Value
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
alias *alias-name*	Specifies the alias name for a community. The alias names of communities are stored in plain text in the configuration file.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **snmp-agent community** command is used on SNMPv1 and SNMPv2c networks. The community is a combination of the NMS and SNMP agent and is identified by a community name. The community name functions as a password for authentication during device communication in a community. Devices can communicate if the community name of the NMS and that of the SNMP agent are the same. The **snmp-agent community** command configures a community name on a device so that the NMS can communicate with the device. Parameters of the **snmp-agent community** command set the access permission, ACL, and accessible MIB views of a community name.

When running the **snmp-agent community** command, you can select parameters based on the networking requirements.

- To grant the NMS read-only permission in the specified view, configure **read**.
- To grant the NMS read-write permission in the specified view, configure **write**.
- To allow specified NMSs using this community name have the rights of ViewDefault, omit **mib-view** *view-name*.

- To allow all NMSs using this community name to manage specified objects on a managed device, omit **acl** *acl-number*.
- To allow specified NMSs using this community name to manage specified objects on a managed device, configure **mib-view** and **acl**.
- The community name will be saved in encrypted format in the configuration file. To facilitate identification of community names, specify the **alias** *alias-name* parameter to set the alias names for the communities. The alias names are stored in plain text in the configuration file.

NOTE

When both community name and ACL are configured, the NMS verifies the community name before accessing the device, and then checks the ACL rules. If the community name does not exist, the packet is discarded and a log indicating that the community name is wrong is printed. The ACL rule is not checked. That is, the ACL rule is checked only when the community name exists.

Precautions

- The device checks the complexity of community names in simple text rather than in ciphertext. The device has the following requirements for community name complexity:
  - The minimum length of a community name is determined by the **set password min-length** command. By default, a password contains 8 characters.
  - The community name includes at least two kinds of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ?).

  If a community name fails the complexity check, the community name cannot be configured. To disable the complexity check for a community name, run the **snmp-agent community complexity-check disable** command, and then the length of community names in simple text ranges from 1 to 32. However, if a community name is simple and does not meet complexity requirements, it is prone to be attacked and cracked by unauthorized users, which affects device security. Therefore, enabling complexity check of community names is recommended.
- Only one type of permission can be configured for a community. If a community has both the read-only and read-write permission configured, the permission configured later takes effect.
- If you specify the parameter **mib-view** or **acl** when running the **snmp-agent community** command, configure the MIB view and ACL rule. If the default MIB view is deleted, the NMS using this community name cannot communicate with managed devices. To continue to use this community name, specify an existing MIB view.
- The community name is saved in cipher text in the configuration file. To delete a community name, run the **undo snmp-agent community** *community name in plain text* or **undo snmp-agent community** *community name in plain text* command. To view a community name in cipher text, run the **display snmp-agent community** command.
- When a user with a level lower than the level configured using this command queries the password configured using the **display this** command, the password is displayed as asterisks (******).

- To specify the same ACL on both IPv4 and IPv6 networks, you can only run the **snmp-agent community** { **read** | **write** } { *community-name* | **cipher** *community-name* } **acl** { *acl-number* | *acl-name* } command.
- If the **snmp-agent community** command is run more than once to specify an ACL for the same SNMP community, the latest configuration overrides the previous one.
- If you forget the configured SNMP community name, run this command to configure a new one.

Example

Set the name of a community to **comaccess1** and configure the read-only rights for the community.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent community read comaccess1
```

Set the name of a community to **comaccess2** and configure the read-write rights for the community.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent community write comaccess2
```

16.1.34 snmp-agent community complexity-check disable

Function

The **snmp-agent community complexity-check disable** command disables the complexity check of a community name.

The **undo snmp-agent community complexity-check disable** command enables the complexity check of a community name.

By default, the device enables the complexity check of a community name.

Format

snmp-agent community complexity-check disable

undo snmp-agent community complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device checks the complexity of community names in simple text rather than in ciphertext. The device has the following requirements for community name complexity:

- The minimum length of a community name is determined by the **set password min-length** command. By default, a password contains 8 characters.
- The community name includes at least two kinds of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ?).

Precautions

To ensure the security of SNMP community names, enable the complexity check for community names. If a community name fails the complexity check, the community name cannot be configured. The complexity check can also be disabled for a community name. However, if a community name is simple and does not meet complexity requirements, it is prone to be attacked and cracked by unauthorized users, which affects device security.

Example

Disable the complexity check for community names.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent community complexity-check disable
```

16.1.35 snmp-agent community plaintext enable

Function

The **snmp-agent community plaintext enable** command enables SNMPv1 and SNMPv2c community names to be displayed in plaintext.

The **undo snmp-agent community plaintext enable** command enables SNMPv1 and SNMPv2c community names to be displayed in ciphertext.

By default, SNMPv1 and SNMPv2c community names are displayed in ciphertext.

Format

snmp-agent community plaintext enable

undo snmp-agent community plaintext enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage scenario

After you run the **snmp-agent community plaintext enable** command, the community name is displayed in plaintext after you run the **snmp-agent community** { **read** | **write** } *community-name* command to specify a plaintext community name.

Precautions

The existing community names are not affected after you run the **snmp-agent community plaintext enable** command. But the configured community names displayed in plaintext will be encrypted and displayed in ciphertext after you run the **undo snmp-agent community plaintext enable** command.

To ensure the security of community names, enable SNMPv1 and SNMPv2c community names to be displayed in ciphertext.

Example

Enable SNMPv1 and SNMPv2c community names to be displayed in ciphertext.

```
<HUAWEI> system-view
[HUAWEI] undo snmp-agent community plaintext enable
```

16.1.36 snmp-agent extend error-code enable

Function

The **snmp-agent extend error-code enable** command enables the device to send extended error codes to the NMS.

The **undo snmp-agent extend error-code enable** command disables the function of sending extended error codes to the NMS.

By default, the function of sending extended error codes to the NMS is disabled.

Format

snmp-agent extend error-code enable

undo snmp-agent extend error-code enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

With the increasing number of features and scenarios supported by the system, the current types of SNMP standard error codes can hardly meet requirements in diversified scenarios. Therefore, the extended error code is introduced. The extended error code can define more scenarios for the NMS to correctly analyze the fault type of the current NE.

If both the NMS and managed device are Huawei products, error codes are extended and more scenarios are defined after the function of sending extended error codes is enabled. As a result, users are enabled to locate and troubleshoot faults quickly and accurately.

Support of the MIB for the extended error code:

- For the MIB that supports the extended error code, you can enable the SNMP extended error code function and use Huawei NMS to provide the NMS with various error codes.
- For the MIB that does not support the extended error code, after the SNMP extended error code function is enabled, NMS of either Huawei or other vendors can obtain only the standard error code.

Example

Enable the device to send extended error codes to the NMS.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent extend error-code enable
```

16.1.37 snmp-agent group

Function

The **snmp-agent group** command creates an SNMP group by mapping SNMP users to SNMP views.

The **undo snmp-agent group** command deletes a specified SNMP user group.

By default, no SNMP group is configured.

Format

snmp-agent group v3 *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* [**acl** { *acl-number* | *acl-name* }]

snmp-agent group v3 *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* **acl-ipv4** { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }]

snmp-agent group v3 *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* **acl-ipv6** { *acl-number* | *acl-name* }

undo snmp-agent group v3 *group-name* { **authentication** | **privacy** | **noauthentication** }

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP group uses the security mode in SNMPv3.	-
group-name	Specifies the name of an SNMP group.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
authentication | **privacy** | **noauthentication**	Indicates the security level of the SNMP group. ● **authentication**: authenticates SNMP messages without encryption. ● **privacy**: authenticates and encrypts SNMP messages. ● **noauthentication**: not authenticate or encrypt SNMP messages.	To ensure security, it is recommended that you set the security level of the SNMP group to **privacy**.
read-view *read-view*	Specifies a read-only view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *read-view* specified by the **snmp-agent mib-view** command.

Parameter	Description	Value
write-view *write-view*	Specifies a read-write view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *write-view* is specified by the **snmp-agent mib-view** command.
notify-view *notify-view*	Specifies a notify view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *notify-view* is specified by the **snmp-agent mib-view** command.
acl	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SNMPv1 and SNMPv2c have serious defects in terms of security. The security authentication mechanism used by SNMPv1 and SNMPv2c is based on the community name. In this mechanism, the community name is transmitted in plain text. You are not advised to use SNMPv1 and SNMPv2c on untrusted networks.

By adopting the user-based security model, SNMPv3 eradicates the security defects in SNMPv1 and SNMPv2c and provides two services, authentication and privacy. The SNMP group name and security name determine an SNMP group. SNMPv3 defines the following security levels:

- noAuthNoPriv
- AuthNoPriv
- AuthPriv

NOTE

The security authentication level noAuthPriv does not exist. This is because the generation of a key is based on the authentication information and product information.

The **snmp-agent group** command can be used to configure the following:

- Authentication
- Privacy
- Access rights for users of SNMP group
- Bind the SNMP group to a MIB view

Parameters are selected based on the following rules:

- To enhance security, configure the parameter **authentication** or **privacy**.
  - If the **noauthentication** parameter is set, SNMP messages are not authenticated or encrypted. This applies to the environment that is secure and has a fixed administrator.
  - To authenticate SNMP messages without encryption, configure the parameter **authentication**. This mode is applicable to secure networks managed by many administrators who may frequently perform operations on the same device. Authentication allows only the administrators with permission to access the device.
  - To authenticate and encrypt SNMP messages, configure the parameter **privacy**. This mode is applicable to insecure networks managed by many administrators who may frequently perform operations on the same device. Authentication and encryption allow only specified administrators to access the device and encrypts data before the transmission. This prevents data from being tampered or leaked.
- To grant the NMS read-only permission in the specified view, configure **read-view**. To grant the NMS read-write permission in the specified view, configure **write-view**. To filter unnecessary alarms, configure **notify-view**. After this parameter is configured, only alarms generated on MIB objects specified by **notify-view** are delivered to the NMS.

  By default, the read-only view of an SNMP group is the ViewDefault view, and the names of the read-write view and inform view are not specified.

- To allow specified NMSs in the same SNMPv3 group to access the device, configure **acl**.

Configuration Impact

When you run the **undo snmp-agent group** command to delete an SNMP user group, you delete all SNMP users in the SNMP user group.

Precautions

To receive trap messages specified in *notify-view*, you need to ensure the target host for receiving SNMP traps is specified through the **snmp-agent target-host trap** command.

If non authentication and non encryption, or authentication and non encryption is configured for an SNMPv3 group, these modes bring security risks. To improve system security, delete the group and create a group with authentication and encryption.

To specify the same ACL on both IPv4 and IPv6 networks, you can only run the **snmp-agent group v3** *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* **acl** { *acl-number* | *acl-name* } command.

If the **snmp-agent group** command is run more than once to specify an ACL for the same SNMP user group, the latest configuration overrides the previous one.

Example

Create an SNMPv3 group named **Johngroup** to authenticate and encrypt SNMP messages, and set the read-only view of the SNMPv3 group to public.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent
[HUAWEI] snmp-agent mib-view excluded public 1.3.6.1.2.1
[HUAWEI] snmp-agent group v3 Johngroup privacy read-view public
```

Create an SNMPv3 group named **Johngroup** to authenticate and encrypt SNMP messages, and set the write-only view of the SNMPv3 group to private.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent
[HUAWEI] snmp-agent mib-view included private 1.3.6.1.2.1
[HUAWEI] snmp-agent group v3 Johngroup privacy write-view private
```

16.1.38 snmp-agent heartbeat enable

Function

The **snmp-agent heartbeat enable** command enables the device to send heartbeat packets to the NMS.

The **undo snmp-agent heartbeat enable** command disables the device from sending heartbeat packets to the NMS.

By default, the device does not send heartbeat packets to the NMS.

Format

snmp-agent heartbeat enable

undo snmp-agent heartbeat enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the NMS cannot initiatively obtain the status of the device, run the **snmp-agent heartbeat enable** command to enable the device to send heartbeat packets (corresponding trap: hwEntityHeartbeatTrap) to the NMS. The device then periodically sends heartbeat packets to the NMS to notify the NMS of its status.

Example

Enable the device to send heartbeat packets to the NMS.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent heartbeat enable
```

16.1.39 snmp-agent heartbeat interval

Function

The **snmp-agent heartbeat interval** command sets the interval at which the device sends heartbeat packets to the NMS.

The **undo snmp-agent heartbeat interval** command restores the interval at which the device sends heartbeat packets to the NMS to the default interval.

By default, the device sends heartbeat packets to the NMS at an interval of 60 seconds.

Format

snmp-agent heartbeat interval *interval*

undo snmp-agent heartbeat interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the device sends heartbeat packets to the NMS.	The value is an integer that ranges from 60 to 86400, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the device to send heartbeat packets to the NMS, you can use the **snmp-agent heartbeat interval** command to set the interval at which heartbeat packets are sent. On a stable network, increase the interval to reduce the bandwidth consumed for periodic transmission of heartbeat packets.

Prerequisites

The device has been enabled to send heartbeat packets to the NMS using the **snmp-agent heartbeat enable** command.

Example

Configure the device to send heartbeat packets to the NMS at an interval of 180 seconds.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent heartbeat interval 180
```

16.1.40 snmp-agent inform

Function

The **snmp-agent inform** command sets global parameters of informs, including the timeout period for waiting for inform ACK messages, number of times to retransmit informs, and maximum number of informs to be confirmed in the inform buffer.

The **undo snmp-agent inform** command restores the default setting.

By default, the timeout waiting period for inform ACK messages is 15 seconds, the number of times to retransmit informs is 3, and the maximum number of informs in the inform buffer is 39.

Format

snmp-agent inform { **timeout** *seconds* | **resend-times** *times* | **pending** *number* } *

undo snmp-agent inform { **timeout** | **resend-times** | **pending** } *

Parameters

Parameter	Description	Value
timeout *seconds*	Specifies the timeout period for waiting for inform ACK messages from the NMS.	The value is an integer ranging from 1 to 1800, in seconds. The default value is 15 seconds.
resend-times *times*	Specifies the times to retransmit informs in the case that no inform ACK message is returned from the NMS.	The value is an integer ranging from 0 to 10. The default value is 3.
pending *number*	Specifies the maximum number of informs to be confirmed in the inform buffer.	The value is an integer ranging from 1 to 2048. The default value is 39.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After sending an inform, the SNMP agent waits for an inform ACK message from the NMS. You can run the **snmp-agent inform** command to set parameters **timeout**, **resend-times**, and **pending** of the inform.

These three parameters mutually affect each other. For example, if the timeout period for waiting for inform ACK messages prolongs or the times to retransmit informs increase, but the maximum number of informs to be confirmed is not changed, the number of informs to be confirmed is increased, causing the inform buffer to be quickly filled up.

Once the inform buffer is filled up, the earliest inform in the inform buffer is deleted each time a new inform enters the queue. The deleted informs are not retransmitted to the NMS. To avoid this problem, you can increase the maximum number of informs to be confirmed in the inform buffer.

You can configure the **snmp-agent inform** command to contain the parameter **timeout**, **resend-times**, or **pending** according to the network condition.

- When a large number of informs are dropped on the network, you can run the **snmp-agent inform pending** *number* command to increase the inform buffer.
- When the transmission speed on the network is low, you can increase the timeout period. Increasing the timeout period will increase the waiting time of informs in the inform buffer. You can also run the **snmp-agent inform** { **timeout** *seconds* | **pending** *number* } * command to increase the inform.

- When the transmission speed on the network is high, you can run the **snmp-agent inform timeout** *seconds* command to reduce the timeout period.
- When informs are transmitted on an unreliable network, you can increase the retransmission times. In this case, the informs in the inform buffer need to wait for a longer time to be confirmed. You can run the **snmp-agent inform** { **resend-times** *times* | **pending** *number* } * command to increase the inform buffer.

Prerequisites

Parameters for sending informs take effect only after the IP address of the target host for receiving informs is configured using the **snmp-agent target-host inform** command.

Precautions

You need to configure only parameters for sending informs using the **snmp-agent inform** command; you do not need to configure parameters for sending traps.

You must set the parameters **timeout**, **resend-times**, and **pending** according to the network condition. Otherwise, the SNMP working efficiency is greatly affected.

Example

Set the times to retransmit an inform to 5 and the maximum number of informs waiting to be confirmed in the inform buffer to 100.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent inform resend-times 5 pending 100
```

16.1.41 snmp-agent inform address

Function

The **snmp-agent inform address** command sets parameters for sending informs, including the timeout period for waiting for inform ACK messages from the NMS and times to retransmit an inform.

The **undo snmp-agent inform address** command restores the default setting for a particular inform host.

By default, the timeout waiting period for inform ACK messages is 15 seconds and the number of times to retransmit informs is 3.

Format

snmp-agent inform { **timeout** *seconds* | **resend-times** *times* } * **address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** { *security-name* | **cipher** *security-name* }

undo snmp-agent inform { **timeout** [*seconds*] | **resend-times** [*times*] } * **address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
timeout *seconds*	Specifies the timeout period for waiting for inform ACK messages from the NMS.	The value is an integer ranging from 1 to 1800, in seconds. The default value is 15, which is equal to the global timeout period configured using the **snmp-agent inform** command.
resend-times *times*	Specifies the number of times that informs are retransmitted when no inform ACK message is returned from the NMS.	The value is an integer ranging from 0 to 10. The default value is 3, which is equal to the global retransmission times configured using the **snmp-agent inform** command.
address	Indicates the address of the target host for receiving SNMP traps. **NOTE** The IP address specified by **address** and the security name specified by **securityname** together identify a host.	The value is dotted decimal notation.
udp-domain *ip-address*	Specifies the IP address of a specified target host, with the transmission domain based on UDP.	The value is dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name. The parameter **vpn-instance** is optional. On a VPN network, you need to use the VPN instance specified by **vpn-instance**, IP address, and security name to identify a target host.
params	Indicates information about the target host that generates SNMP notifications.	-

Parameter	Description	Value
securityname *security-name*	Displays the name of the target host for receiving informs on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. For SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32, 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use both the **snmp-agent inform address** command and the **snmp-agent inform** command to set parameters according to the network condition.

- When a large number of Inform messages are dropped on the network, you are recommended to run the **snmp-agent inform pending** *number* command to lengthen the trap queue and then the **snmp-agent inform address** command to specify the destination IP address and name of the target host.
- When the transmission speed on the network is low, you are recommended to increase the timeout period. Increasing the timeout period will surely increase the waiting time of informs in the trap queue for confirmation. In this case, you are also recommended to run the **snmp-agent inform** { **timeout** *seconds* | **pending** *number* } * command to lengthen the trap queue and then the **snmp-agent inform address** command to specify the destination address and the displayed user name.
- When the transmission speed on the network is high, you are recommended to run the **snmp-agent inform timeout** *seconds* **address udp-domain** *ip-address* **params securityname** *security-name* command to reduce the timeout period.
- When informs are transmitted on an unreliable network, you are recommended to increase the retransmission times. In this case, the informs in the trap queue need to wait for a longer time to be confirmed. This requires you to run the **snmp-agent inform** { **resend-times** *times* | **pending** *number* } * command to lengthen the trap queue and then the **snmp-agent inform address** command to specify the destination address and the displayed user name.

Prerequisites

Parameters for sending informs take effect only after the IP address of the target host for receiving informs is configured using the **snmp-agent target-host inform** command.

Precautions

- You need to configure only parameters for sending informs using the **snmp-agent inform address** command; you do not need to configure parameters for sending traps.
- You must set the parameters **timeout** and **resend-times** according to the network condition. Otherwise, the SNMP working efficiency is greatly affected.
- The priority set for the **timeout** and **resend-times** parameters using the **snmp-agent inform address** command is higher than that set for the **timeout** and **resend-times** parameters using the **snmp-agent inform** command. If both parameters in Inform mode and parameters using the **snmp-agent inform address** command are configured, parameters using the

snmp-agent inform address command take effect for a specified destination host.

- For SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Set the times to retransmit an inform to the target host (with the IP address of 10.1.1.1 and the security name of ABC) to 10.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent inform resend-times 10 address udp-domain 10.1.1.1 params securityname ABC
```

16.1.42 snmp-agent local-engineid

Function

The **snmp-agent local-engineid** command sets an engine ID for the local SNMP agent.

The **undo snmp-agent local-engineid** command restores the engine ID of the local SNMP agent to the default value.

By default, the device uses an internal algorithm to automatically generate an engine ID for a device. The engine ID consists of the enterprise number and the device information.

Format

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

Parameters

Parameter	Description	Value
engineid	Specifies the engine ID of the local SNMP agent.	The value is string of 10 to 64 hexadecimal digits. It cannot be all 0s or all Fs.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **snmp-agent local-engineid** command to set an engine ID for the local SNMP agent for identification.

The SNMP engine ID uniquely identifies an SNMP agent in a management domain. The SNMP engine ID is an important component of the SNMP agent. It schedules and processes SNMP messages, and implements security authentication and access control. You can use the **display snmp-agent local-engineid** command to check the engine ID of the local SNMP entity.

When setting an engine ID, you need to comply with the following rules:

- The length of the octet strings varies. The first four octets are set to the binary equivalent of the agent, which is SNMP management private enterprise number and is assigned by the Internet Assigned Numbers Authority (IANA). The engine ID of Huawei devices is 2011 in decimal notation. The first digit is in binary format, and has a fixed value 1. Therefore, the engine ID in hexadecimal format is 800007DB.
- The device information can be configured manually. It is recommended that the IP address or MAC address of the device be used as the device information to uniquely identify the device.

Precautions

- After the SNMP agent function is enabled using the **snmp-agent** command, the system automatically adopts the default engine ID for the local SNMP agent.
- If the local engine ID is set or changed, the existing SNMPv3 user with this engine ID is deleted.

Example

Set the engine ID of the local SNMP agent to 800007DB03360102101100.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent local-engineid 800007DB03360102101100
```

16.1.43 snmp-agent mib-view

Function

The **snmp-agent mib-view** command creates or updates a MIB view.

The **undo snmp-agent mib-view** command cancels the configuration of the current MIB view.

By default, the device has the MIB view ViewDefault with OID of 1.3.6.1.

For SNMPv1 and SNMPv2c, you can access the Viewdefault view by default. For SNMPv3, you must specify the MIB views that can be accessed by running the **snmp-agent group** command; if no new MIB view is created, you can specify the default MIB view ViewDefault in this command.

Format

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree*

undo snmp-agent mib-view *view-name* [*oid-tree*]

undo snmp-agent mib-view [**excluded** | **included**] *view-name* [*oid-tree*]

Parameters

Parameter	Description	Value
excluded	Indicates that the MIB view excludes the MIB subtree.	-
included	Indicates that the MIB view includes the MIB subtree.	-
view-name	Specifies the MIB view name.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
oid-tree	Specifies the OID for the MIB subtree. *oid-tree* can be the OID (such as 1.4.5.3.1) or the name (such as system) of the subtree.	It is a string of 1 to 255 case-sensitive characters without spaces. **NOTE** It must be a valid MIB subtree.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Most SNMP configuration commands contain the parameter *view-name*. The **snmp-agent mib-view** command is used to create or update a view. You cannot modify or delete the default ViewDefault MIB view.

In the **snmp-agent mib-view** command, the parameter *view-name* can be displayed as an OID or an object name.

- Displaying the parameter *view-name* as an OID: **snmp-agent mib-view included myview 1.3.6.1.2.1**.
- Displaying the parameter *view-name* as an object name: **snmp-agent mib-view excluded myview system.7**.

NOTE

To uniquely identify object identifiers in SNMP messages, SNMP uses a hierarchical naming structure to distinguish object identifiers from each other. This is a tree-like structure, with the nodes (such as {1.3.6.1.2.1}) representing object identifiers. The MIB is a collection of standard variables on monitored network devices.

You can select parameters based on the following rules:

- **excluded**: If a few MIB objects on the device or some objects in the current MIB view do not or no longer need to be managed by the NM station, **excluded** needs to be specified in the command to exclude these MIB objects.
- **included**: If a few MIB objects on the device or some objects in the current MIB view need to be managed by the NM station, **included** needs to be specified in the command to include these MIB objects.

If you forget which information you have configured for a MIB view, you can run the **display snmp-agent mib-view** command to check it.

Precautions

When you run the **snmp-agent mib-view** command for multiple times to define the MIB view, the new configuration overwrites the original configuration if the values of *view-name* and *oid-tree* are the same; the new and original configurations both take effect if the values of *view-name* and *oid-tree* are different. The system can store a maximum of 256 MIB view configurations, among which there are four default views.

If both the **include** and **exclude** parameters are configured for MIB objects that have an inclusion relationship, whether to include or exclude the lowest MIB object will be determined by the parameter configured for the lowest MIB object. For example, the snmpV2, snmpModules, and snmpUsmMIB objects are from top down in the MIB table. If the **exclude** parameter is configured for snmpUsmMIB objects and **include** is configured for snmpV2, snmpUsmMIB objects will still be excluded.

Example

Create MIB view **mib2view** that includes all mib-2 objects and the subtree with the OID as 1.3.6.1.2.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent mib-view included mib2view 1.3.6.1.2.1
```

16.1.44 snmp-agent notification-log

Function

The **snmp-agent notification-log** command sets the aging time of trap logs and the maximum number of trap logs that can be saved in the trap log buffer.

The **undo snmp-agent notification-log** command restores the default configuration.

By default, the aging time of trap logs is 24 hours, and a maximum of 500 trap logs can be saved in the trap log buffer.

Format

snmp-agent notification-log { **global-ageout** *ageout* | **global-limit** *limit* } *

undo snmp-agent notification-log { **global-ageout** [*ageout*] | **global-limit** [*limit*] } *

Parameters

Parameter	Description	Value
global-ageout *ageout*	Specifies the aging time of trap logs.	The value can be 0 or an integer that ranges from 12 to 36, in hours. The default value is 24. The value 0 indicates that trap logs are never aged out.
global-limit *limit*	Specifies the maximum number of trap logs that can be saved in the trap log buffer.	The value is an integer that ranges from 1 to 5000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a device sends the alarms propagated through Inform messages, the target host is required to respond with Inform ACK messages. In the following two situations, the alarms propagated through Inform messages are logged and the alarm logs are cached in the log buffer to help the target host synchronize the alarms generated in the event of host or link failures:

- No Inform ACK message is returned when the number of times to resend the Inform message in the alarm queue reaches the set threshold.
- Inform messages will be discarded because the number of logged Inform messages reaches the maximum that the alarm queue can support.

The maximum number of alarm logs in a log buffer is fixed (500 by default) to prevent a device from being burdened with excessive alarm logs. Alarm logs are aged periodically (24 hours by default) to ensure alarm logs remain up-to-date.

Precautions

- Only Inform logs are saved to the log buffer; trap logs are not saved to the log buffer.
- If notification logs in the log buffer do not need to be aged, you can set the aging time of these notification logs to 0.

- If the number of notification logs saved to the log buffer within the aging time exceeds the limit, new notification logs can still be saved but overwrites the earlier logs in the log buffer.
- The maximum number of alarm logs specified in the **snmp-agent notification-log** command cannot occupy more memory than the memory occupied by the log buffer. If the size of the log buffer is excessively large, more network resources are consumed. You are therefore recommended to set the size of the log buffer to a reasonable value.

Example

Set the aging time of trap logs to 36 hours.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notification-log global-ageout 36
```

Set the maximum number of trap logs that can be saved in the trap log buffer to 1000.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notification-log global-limit 1000
```

16.1.45 snmp-agent notification-log enable

Function

The **snmp-agent notification-log enable** command enables the notification logging function.

The **undo snmp-agent notification-log enable** command disables the notification logging function.

By default, the notification logging function is disabled.

Format

snmp-agent notification-log enable

undo snmp-agent notification-log enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the route from a network element to the NMS is unreachable because of a link failure between the network element and NMS, the network element does not send any SNMP notifications to the NMS. If the notification logging function is enabled, the network element records trap logs. When the link between the network element and NMS recovers, the NMS can obtain the trap logs recorded when the link was faulty.

After the notification logging function is enabled, the system records informs in trap logs in either of the following conditions:

- No ACK message is received after an inform in the notification queue is retransmitted the specified number of times.
- Earliest informs are discarded because the number of notifications in the notification queue exceeds the limit. The system records the discarded informs in trap logs.

Precautions

Only informs are recorded in trap logs, and traps are not recorded.

Example

Enable the notification logging function.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notification-log enable
```

16.1.46 snmp-agent notify-filter-profile

Function

The **snmp-agent notify-filter-profile** command creates or updates a trap filter profile.

The **undo snmp-agent notify-filter-profile** command deletes a trap filter profile.

By default, no trap is filtered.

Format

snmp-agent notify-filter-profile { **included** | **excluded** } *profile-name oid-tree*

undo snmp-agent notify-filter-profile [**included** | **excluded**] *profile-name*

Parameters

Parameter	Description	Value
included	Includes the specified MIB subtree.	-
excluded	Excludes the specified MIB subtree.	-

Parameter	Description	Value
profile-name	Specifies the name of a trap filter profile.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
oid-tree	Specifies the OID for the MIB subtree. *oid-tree* can be the OID (such as 1.4.5.3.1) or the name (such as system) of the subtree.	The value is a string of 1 to 255 case-sensitive characters without spaces. **NOTE** It must be a valid MIB subtree.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To filter trap messages sent to a target host, run the **snmp-agent notify-filter-profile** command to add the MIB objects to be filtered to a filter profile to limit the number of MIB objects that can send trap messages to the NMS. After the filter profile is configured using the **snmp-agent notify-filter-profile** command, only the trap messages generated by eligible MIB objects are sent to the NMS.

Precautions

- If no trap filter profile is configured, all traps are sent to the destination host.
- The **snmp-agent notify-filter-profile** command creates or updates a trap filter profile. The value of *oid-tree* can be an OID or a subtree name. An OID can contain asterisks (*) as wildcards. An asterisk (*) cannot be placed at the beginning or end of the OID string.
- In Include filtering mode of an alarm, OIDs of all bound variables in the alarm must be specified in this command. Otherwise, the filtering fails.
- In Exclude filtering mode of an alarm, only the OID of the alarm or that of any bound variable need to be specified in this command.

Example

Configure a trap filter profile named **tmp**.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notify-filter-profile included tmp 1.3.6.1.*.4
```

16.1.47 snmp-agent packet contextengineid-check enable

Function

The **snmp-agent packet contextengineid-check enable** command enables the device to check consistency between the contextEngineID on the NMS and the local engine ID.

The **undo snmp-agent packet contextengineid-check enable** command disables the device from checking consistency between the contextEngineID on the NMS and the local engine ID.

By default, the device does not check consistency between the contextEngineID on the NMS and the local engine ID.

Format

snmp-agent packet contextengineid-check enable

undo snmp-agent packet contextengineid-check enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device does not check consistency between the contextEngineID on the NMS and the local engine ID, the NMS can connect to the device even if the contextEngineID is different from the local engine ID.

To improve system security, run the **snmp-agent packet contextengineid-check enable** command to enable the device to check consistency between the contextEngineID on the NMS and the local engine ID.

Configuration Impact

After this function is enabled, an NMS cannot connect to the device if the contextEngineID on the NMS is different from the local engine ID.

Precautions

This consistency check function applies only to SNMPv3.

Example

Enable the consistency check between the contextEngineID and local engine ID.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent packet contextengineid-check enable
```

16.1.48 snmp-agent packet max-size

Function

The **snmp-agent packet max-size** command sets the maximum size of an SNMP message.

The **undo snmp-agent packet max-size** command restores the default setting.

By default, the maximum size of an SNMP message is 12000 bytes.

Format

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

Parameters

Parameter	Description	Value
byte-count	Specifies the maximum size of an SNMP message that the SNMP agent can receive and send.	The value is an integer that ranges from 484 to 17940, in bytes. The default value is 12000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You are recommended to run the **snmp-agent packet max-size** command to set the maximum size of an SNMP message that the SNMP agent receives or sends according to the network condition.

By increasing the maximum size of an SNMP message, you can prevent the NMS from obtaining the incomplete information about the device status.

By decreasing the maximum size of an SNMP message, you can prevent the NMS or device from discarding an SNMP message because its size exceeds the processing capability of the NMS or device.

Precautions

You need to increase the size of an SNMP message according to the network condition. Otherwise, the transmission efficiency of SNMP messages is affected.

Generally, the default value is recommended.

The maximum size set through the **snmp-agent packet max-size** command takes effect for the SNMP messages of all SNMP versions.

Example

Set the maximum size of an SNMP message that the SNMP agent can receive or send to 1042 bytes.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent packet max-size 1042
```

16.1.49 snmp-agent packet-priority

Function

The **snmp-agent packet-priority** command sets the priority of SNMP messages.

The **undo snmp-agent packet-priority** command restores the default priority of SNMP messages.

By default, the priority of SNMP messages is 6.

Format

snmp-agent packet-priority { **snmp** | **trap** } *priority-level*

undo snmp-agent packet-priority { **snmp** | **trap** }

Parameters

Parameter	Description	Value
snmp	Sets the priority of common SNMP messages (excluding trap messages), including: ● Get-Response packets ● Set-Response packets	-
trap	Sets the priority of SNMP trap messages, including: ● Trap packets ● Inform packets	-

Parameter	Description	Value
priority-level	Specifies the priority of SNMP messages.	The value is an integer that ranges from 0 to 7. The default value is 6. The value 0 indicates the lowest priority, and the value 7 indicates the highest priority.

Views

System view

Default Level

3: Management level

Usage Guidelines

SNMP messages may be lost if the number of SNMP messages on a network exceeds the processing capability of the NMS. Run the **snmp-agent packet-priority** command to set the transmission priority of SNMP messages to ensure that the NMS can process important messages first. This command can be used in the following situations:

- To prevent traps from being discarded, increase the priority of SNMP trap messages so that traps can be successfully sent to the NMS.
- To improve reliability of MIB operations performed on the device by the NMS, increase the priority of common SNMP messages, excluding SNMP trap messages.
- When the network is severely congested and traps are generated frequently, reduce the priority of all SNMP messages, including SNMP trap messages.

Example

Set the priority of common SNMP messages to 5.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent packet-priority snmp 5
```

16.1.50 snmp-agent protocol get-bulk timeout

Function

The **snmp-agent protocol get-bulk timeout** command configures a get-bulk operation timeout period.

The **undo snmp-agent protocol get-bulk timeout** command restores the default get-bulk operation timeout period.

The default get-bulk operation timeout period is 2 seconds.

Format

snmp-agent protocol get-bulk timeout *time*

undo snmp-agent protocol get-bulk timeout

Parameters

Parameter	Description	Value
time	Specifies a get-bulk operation timeout period.	The value is an integer ranging from 0 to 600, in seconds. **NOTE** The value 0 indicates that a get-bulk operation never expires.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A get-bulk operation allows an NMS to query information about multiple managed devices at a time, equaling multiple get-next operations.

If an NMS requests many data through a get-bulk operation, a long time is required to obtain the data. You can run the **snmp-agent protocol get-bulk timeout** command to change the get-bulk operation timeout period.

Precautions

You are not advised to change the get-bulk operation timeout period. The default get-bulk operation timeout period is recommended. To reconfigure a get-bulk operation timeout period, you must ensure that the configured period is less than an NMS's timeout period.

Example

Set the get-bulk operation timeout period to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol get-bulk timeout 10
```

16.1.51 snmp-agent protocol ipv6 source-ip

Function

The **snmp-agent protocol ipv6 source-ip** command configures an IPv6 address for receiving and responding to NMS requests.

The **undo snmp-agent protocol ipv6 source-ip** command restores the default configuration.

By default, no IPv6 address can be used to receive or respond to NMS requests.

Format

snmp-agent protocol ipv6 source-ip *ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo snmp-agent protocol ipv6 source-ip

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no IPv6 address can be used to receive or respond to NMS requests. When a device needs to establish a connection with the NMS, you can run the **snmp-agent protocol ipv6 source-ip** command to specify an IPv6 address for the device to receive and respond to NMS requests.

Precautions

- After the **snmp-agent protocol ipv6 source-ip** command is run, the NMS can communicate with the device only through the specified IPv6 address.

Therefore, ensure that there are reachable routes between the NMS and the specified IPv6 address.

- If you run this command multiple times, only the latest configuration takes effect.

Example

Configure 1::1 as a IPv6 address for receiving and responding to NM station requests.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol ipv6 source-ip 1::1
```

16.1.52 snmp-agent protocol server disable

Function

The **snmp-agent protocol server disable** command disables the SNMP IPv4 or IPv6 listening port.

The **undo snmp-agent protocol server disable** command enables the SNMP IPv4 or IPv6 listening port.

By default, the SNMP IPv4 or IPv6 listening port is disabled.

Format

snmp-agent protocol server [**ipv4** | **ipv6**] **disable**

undo snmp-agent protocol server [**ipv4** | **ipv6**] **disable**

Parameters

Parameter	Description	Value
ipv4	Disables the SNMP IPv4 listening port.	-
ipv6	Disables the SNMP IPv6 listening port.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable alarm sending to the NMS without performing the Get/Set operation, SNMP port listening is not required. To disable the SNMP IPv4 or IPv6 listening port, run the **snmp-agent protocol server disable** command.

This command helps separately manage and control SNMP IPv4 and IPv6 listening ports.

If **ipv4** or **ipv6** is not selected, both SNMP IPv4 and IPv6 listening ports are disabled.

Precautions

After you disable the SNMP IPv4 or IPv6 listening port using the **snmp-agent protocol server disable** command, SNMP no longer processes SNMP packets. Exercise caution when you disable the SNMP IPv4 or IPv6 listening port.

Example

Disable the SNMP IPv4 listening port.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol server ipv4 disable
```

16.1.53 snmp-agent protocol source-interface

Function

The **snmp-agent protocol source-interface** command configures an interface for receiving and responding to NMS requests.

The **undo snmp-agent protocol source-interface** command restores the default configuration.

By default, no interface can receive or respond to NMS requests.

Format

snmp-agent protocol source-interface *interface-type interface-number*

undo snmp-agent protocol source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no interface can receive or respond to NMS requests. When a device needs to establish a connection with the NMS, you can run the **snmp-agent protocol source-interface** command to specify an interface on the device to receive and respond to NMS requests.

Prerequisites

The interface to be configured as the interface must have been created, and a valid IP address must have been assigned to this interface. If the interface to be configured as the interface is not created or a valid IP address is not assigned to the interface, the **snmp-agent protocol source-interface** command will not take effect. If a valid IP address is assigned to the interface, the **snmp-agent protocol source-interface** command will take effect automatically.

Precautions

- If the interface on which the **snmp-agent protocol source-interface** command is configured is deleted, or an address is changed or deleted on the interface, SNMP configurations will not be affected.
- After SNMP is bound to the interface, SNMP listens only this interface, through which the NMS communicates with the device. If the interface or its IP address is deleted, SNMP will stop receiving IP packets, and therefore communication between the NMS and devices will interrupt. After the interface's IP address is changed, the NMS can communicate with devices only through the new IP address.
- If you run this command multiple times, only the latest configuration takes effect.

Example

Configure loopback 1 for receiving and responding to NMS requests.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol source-interface Loopback 1
```

16.1.54 snmp-agent protocol source-status

Function

The **snmp-agent protocol source-status** command enables all interfaces or IPv6 addresses to receive and respond to NMS requests.

The **undo snmp-agent protocol source-status** command restores the default configuration.

By default, no interface or IPv6 address can be used to receive or respond to NMS requests.

Format

snmp-agent protocol source-status [**ipv6**] **all-interface**

undo snmp-agent protocol source-status [**ipv6**] **all-interface**

Parameters

Parameter	Description	Value
ipv6	Enables all IPv6 addresses to receive and respond to NMS requests.	-
all-interface	Enables all interfaces to receive and respond to NMS requests.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For security purposes, no interface or IPv6 address can be used to receive or respond to NMS requests by default. When a device needs to establish a connection with the NMS, you can run any one of the following commands to allow the device to receive and respond to NMS requests:

- **snmp-agent protocol source-status**: Enables all interfaces or IPv6 addresses to receive and respond to NMS requests.
- **snmp-agent protocol source-interface**: Enables a specified interface to receive and respond to NMS requests.
- **snmp-agent protocol ipv6 source-ip**: Enables a specified IPv6 address to receive and respond to NMS requests.

Precautions

- Assume that on a switch running a version earlier than V200R020C00, the **snmp-agent** command is configured to enable the SNMP agent function, and the **snmp-agent protocol source-interface** and **snmp-agent protocol ipv6 source-ip** commands are not configured. After the switch is upgraded to V200R020C00 or a later version, the **snmp-agent protocol source-status all-interface** and **snmp-agent protocol source-status ipv6 all-interface** commands are automatically added to the configuration file.
- When the **snmp-agent protocol source-status** command is configured, all interfaces or IPv6 addresses can receive and respond to NMS requests, increasing system security risks. Therefore, this configuration is not recommended. You are advised to specify an interface or IPv6 address to receive and respond to NMS requests.

Example

Enable all interfaces to receive and respond to NMS requests.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol source-status all-interface
```

16.1.55 snmp-agent protocol server message queue

Function

The **snmp-agent protocol server message queue** command configures the size of a packet queue that can be received by an SNMP agent.

The **undo snmp-agent protocol server message queue** command restores the default size.

By default, the packet queue that can be received by an SNMP agent contains 30 packets.

Format

snmp-agent protocol server message queue *message-queue*

undo snmp-agent protocol server message queue

Parameters

Parameter	Description	Value
message-queue	Specifies the size of a packet queue.	The value is an integer ranging from 10 to 100.

Views

System view

Default Level

3: Management level

Usage Guidelines

If some packets are discarded when the number of packets in the packet queue that can be received by an SNMP agent has reached the upper limit, run the **snmp-agent protocol server message queue** command to adjust the queue size.

Example

Configure the packet queue that can be received by an SNMP agent to contain 50 packets at most.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol server message queue 50
```

16.1.56 snmp-agent statistics mib disable

Function

The **snmp-agent statistics mib disable** command disables the statistics function about the NMS's operations on MIB objects.

The **undo snmp-agent statistics mib disable** command restores the default statistics status.

By default, the statistics function about the NMS's operations on MIB objects is enabled.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

snmp-agent statistics mib disable

undo snmp-agent statistics mib disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An NMS performs operations on MIB objects to manage devices. Currently, SNMP supports the statistics function about these operations.

By default, the statistics function is enabled. To disable this function due to some reasons, for example, high CPU usage caused by collecting statistics about the NMS accessing MIB objects, run the **snmp-agent statistics mib disable** command.

Follow-up Procedure

Run the **display snmp-agent statistics mib** command to check statistics about the NMS's operations on MIB objects.

If the NMS accesses a great amount of MIB node information and statistics do not need to be saved, run the **reset snmp-agent statistics mib** command to delete the statistics.

Precautions

After you run the **snmp-agent statistics mib disable** command, the statistics function is disabled, but statistics that have been collected are not deleted.

Example

Disable the statistics function about the NMS's operations on MIB objects.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent statistics mib disable
```

16.1.57 snmp-agent sys-info

Function

The **snmp-agent sys-info** command sets the SNMP system information.

The **undo snmp-agent sys-info** command restores the default setting.

By default, the system maintenance information is " R&D Beijing, Huawei Technologies Co., Ltd.", the system location is "Beijing China", and the version is SNMPv3.

Format

snmp-agent sys-info { **contact** *contact* | **location** *location* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

undo snmp-agent sys-info { **contact** | **location** | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

Parameters

Parameter	Description	Value
contact *contact*	Indicates contact information of system maintenance.	The value is a string of 1 to 225 case-sensitive characters that can contain spaces.
location *location*	Indicates the location of a device.	The value is a string of 1 to 255 case-sensitive characters that can contain spaces.

Parameter	Description	Value
version { { **v1** | **v2c** | **v3** } * | **all** }	Indicates the SNMP version. - **v1**: SNMPv1 is enabled. - **v2c**: SNMPv2c is enabled. - **v3**: SNMPv3 is enabled. - **all**: SNMPv1, SNMPv2c, and SNMPv3 are enabled. **NOTE** This parameter can be repeatedly configured. If a device runs multiple SNMP versions, the NMS can use any one of them to manage the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the contact information for the managed node, you can run the **snmp-agent sys-info contact** command in the system. If a device fails, maintenance personnel can contact the vendor for device maintenance.

To configure the physical location of the node, you can run the **snmp-agent sys-info location** command in the system.

To configure features in a specified version, you can run the **snmp-agent sys-info version** command to set the corresponding SNMP version in the system. SNMPv1 or SNMPv2c is not secure enough. Using SNMPv3 is recommended.

SNMPv1:

- Community-name-based access control
- MIB-view-based access control

SNMPv2c:

- Community-name-based access control
- MIB-view-based access control
- Supporting Inform messages

Besides inheriting basic SNMPv2c operations, SNMPv3 defines a management architecture, which introduces a User-based Security Model (USM) to provide users with a more secure access mechanism.

- User group

- Group-based access control
- User-based access control
- Authentication and encryption mechanisms

NOTE

Use **display snmp-agent sys-info** command to view the information of the system maintenance, the physical location of the node and the SNMP version.

Precautions

A lack of authentication capabilities in SNMPv1 and SNMPv2c results in vulnerability to security threats, so SNMPv3 is recommended.

Example

Set the contact information of the system maintenance as "call Operator at 010-12345678".

```
<HUAWEI> system-view
[HUAWEI] snmp-agent sys-info contact call Operator at 010-12345678
```

Set the location of a device as "shanghai China".

```
<HUAWEI> system-view
[HUAWEI] snmp-agent sys-info location shanghai China
```

Set the current SNMP version used by the system to v3.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent sys-info version v3
```

16.1.58 snmp-agent target-host inform

Function

The **snmp-agent target-host inform** command sets the target host for receiving Inform messages.

The **undo snmp-agent target-host** command cancels the target host set to receive Inform messages.

By default, the target host for receiving Inform messages is not set.

Format

snmp-agent target-host inform address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name* | **public-net**]] * **params securityname** { *security-name* | **cipher** *security-name* } **v2c** [**notify-filter-profile** *profile-name* | **ext-vb**] *

snmp-agent target-host inform address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name* | **public-net**]] * **params securityname** *security-name* **v3** [**authentication** | **privacy**] [**notify-filter-profile** *profile-name* | **ext-vb**] *

undo snmp-agent target-host *ip-address* **securityname** { *security-name* | **cipher** *security-name* } [**vpn-instance** *vpn-instance-name*]

undo snmp-agent target-host inform address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name* | **public-net**]] * **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
address	Specifies the IP address of a specified target host.	-
udp-domain *ip-address*	Specifies the IP address of a specified target host, with the transmission domain being based on UDP.	It is dotted decimal notation.
udp-port *port-number*	Specifies the UDP port of the specified target host for receiving Inform messages.	The value is an integer ranging from 0 to 65535. The default value is 162.
source *interface-type interface-number*	Specifies the source interface of the device for sending Inform messages.	-
vpn-instance *vpn-instance-name*	Specifies VPN instance to which the target host belongs.	The value must be an existing VPN instance name.
public-net	Indicates the target host is on the public network.	-
params	Indicates information about the target host that generates SNMP notifications.	-

Parameter	Description	Value
securityname *security-name*	Specifies the user security name displayed on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. Ensure that the *security-name* value is the same as the created user name; otherwise, the NMS cannot access the device. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.
v2c	Indicates the SNMP version is SNMPv2c.	-
v3	Indicates the SNMP version is SNMPv3.	-
authentication | **privacy**	Specifies the security mode. ● **authentication**: authenticates SNMP messages without encryption. ● **privacy**: authenticates and encrypts SNMP messages. This parameter takes effect only in SNMPv3.	-

Parameter	Description	Value
notify-filter-profile *profile-name*	Specifies the filtering view name.	The filtering view must exist.
ext-vb	Indicates that traps sent to a target host carry extended bound variables. If a Huawei data communication device extends the trap objects defined in the public MIB, you can configure this parameter to determine whether traps sent to the NMS carry extended bound variables. ● If this parameter is not configured, the traps sent from the Huawei data communication device do not carry extended bound variables. If you are using a third-party NMS tool, you are not advised to configure this parameter, which ensures that the NMS tool can receive alarms sent from the Huawei device. By default, a trap sent from a Huawei data communication device does not carry extended bound variables. ● If this parameter is configured, the traps sent from the Huawei data communication device carry extended bound variables. If you are using a Huawei NMS tool, you are advised to configure this parameter, which allows you to view more information carried in a trap.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After sending an Inform message, the device waits for an Inform ACK message from the NMS and will retransmit the same Inform message only when no Inform ACK message is received from the NMS within the specified period. If the SNMP agent does not receive the inform ACK message from the NMS during the retransmission period, the SNMP agent deletes this inform message from the trap queue. This ensures that the NMS can receive the SNMP Inform messages to the maximum extent.

If there are multiple target hosts, you need to run the **snmp-agent target-host inform** command on each target host. If the **snmp-agent target-host inform** command is executed for multiple times on the target host, only the last successful operation takes effect.

The rules for selecting the target host are as follows:

- If the **public-net** parameter is specified, the system accesses the target host on the public network.
- If the **vpn-instance** *vpn-instance-name* parameter is specified, the system accesses the target host in the specified VPN instance.
- If both the **public-net** and **vpn-instance** *vpn-instance-name* parameters are not specified:
  a. If the **source** *interface-type interface-number* parameter is specified and a VPN instance is bound to the specified interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the specified interface, the system accesses the target host on the public network.
  b. If the **snmp-agent trap source** command is run to configure a source interface for sending trap packets and a VPN instance is bound to the interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the interface, the system accesses the target host on the public network.
  c. If the **set net-manager vpn-instance** command is run to configure a network management VPN instance, the system accesses the target host in this VPN instance.
  d. If none of the preceding conditions is met, the system accesses the target host on the public network.

Configuration Impact

The transmission of Inform messages, however, consumes more resources than that of traps.

Precautions

The **snmp-agent notify-filter-profile** command is used to create or update the trap filtering information. The NMS filters trap messages according to the profile and sends only the eligible trap messages to the target host. If **notify-filter-profile** is not configured, all trap messages are sent to the target host.

Ensure that the security level of a trap host is not higher than that of the user specified by **securityname** and not lower than that of the user group. Otherwise, the trap host cannot send trap messages properly. The user security level can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: noauthentication (no authentication or encryption)

When SNMPv3 is used to send Inform messages, run the **snmp-agent remote-engineid usm-user v3** command to configure a remote SNMPv3 user whose remote engine ID must be the same as the engine ID of the destination host.

The **securityname** configuration of an SNMPv2c alarm host is displayed in ciphertext, whereas the **securityname** configuration of an SNMPv3 alarm host is displayed in simple text. For SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Configure alarms to be sent in inform mode, set the security name of the host to 123 and protocol version to SNMPv3, and send alarms to the NMS host with the IP address of 192.168.10.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
[HUAWEI] snmp-agent target-host inform address udp-domain 192.168.10.1 params securityname 123
v3
```

16.1.59 snmp-agent target-host trap

Function

The **snmp-agent target-host trap** command configures the target host for receiving SNMP traps.

The **undo snmp-agent target-host** command deletes the target host configuration for receiving SNMP traps.

By default, the target host is not set.

Format

snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**public-net** | **vpn-instance** *vpn-instance-name*]] * **params securityname** *security-name* [[**v1** | **v2c** | **v3** [**authentication** | **privacy**]] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**public-net** | **vpn-instance** *vpn-instance-name*]] * **params securityname cipher** *security-name* [[**v1** | **v2c**] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

undo snmp-agent target-host *ip-address* **securityname** { *security-name* | **cipher** *security-name* } [**vpn-instance** *vpn-instance-name*]

undo snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**public-net** | **vpn-instance** *vpn-instance-name*]] * **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
address	Specifies the IP address of a specified target host.	-
udp-domain *ip-address*	Specifies the IP address of a specified target host, with the transmission domain being based on UDP.	-
udp-port *port-number*	Specifies the UDP port of the specified target host for receiving Trap messages.	The value is an integer ranging from 0 to 65535. The default value is 162.
source *interface-type interface-number*	Specifies the source interface of the device for sending Trap messages.	-
public-net	Specifies VPN instance to which the target host belongs.	-
vpn-instance *vpn-instance-name*	Indicates the target host is on the public network.	The value must be an existing VPN instance name.

Parameter	Description	Value
params securityname *security-name*	Specifies the user security name displayed on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. Ensure that the *security-name* value is the same as the created user name; otherwise, the NMS cannot access the device. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.
v1 | **v2c** | **v3**	Indicates the SNMP version. ● **v1**: SNMPv1. ● **v2c**: SNMPv2c. ● **v3**: SNMPv3. If this parameter is not specified, the default version is SNMPv1.	-

Parameter	Description	Value
authentication | **privacy**	Specifies the security mode. - **authentication**: authenticates packets without encryption. - **privacy**: authenticates and encrypts SNMP messages. This parameter takes effect only in SNMPv3.	-
private-netmanager	Indicates the Huawei NMS as the target host receiving a trap. When a Huawei NMS is deployed and this parameter is configured, a trap sent to the NMS contains more information, such as the trap type, sequence of the trap, and sending time.	-
notify-filter-profile *profile-name*	Specifies the filtering view name. If the trap filtering is not configured using the parameter **notify-filter-profile**, all traps will be sent to the destination host.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ext-vb	Indicates that traps sent to a target host carry extended bound variables. If a Huawei data communication device extends the trap objects defined in the public MIB, you can configure this parameter to determine whether traps sent to the NMS carry extended bound variables. - If this parameter is not configured, the traps sent from the Huawei data communication device do not carry extended bound variables. If you are using a third-party NMS tool, you are not advised to configure this parameter, which ensures that the NMS tool can receive alarms sent from the Huawei device. By default, a trap sent from a Huawei data communication device does not carry extended bound variables. - If this parameter is configured, the traps sent from the Huawei data communication device carry extended bound variables. If you are using a Huawei NMS tool, you are advised to configure this parameter, which allows you to view more information carried in a trap.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SNMP notifications can be classified into traps and inform messages. Trap messages are less reliable than inform messages because the NMS does not send any acknowledgment when it receives a trap. In this case, the sender cannot verify whether the trap has been received. Informs are configured with an acknowledgment mechanism and therefore are reliable.

To configure multiple target hosts, you must run the **snmp-agent target-host trap** command on each target host. If you run the **snmp-agent target-host trap** command for multiple times on a host, only the latest configuration takes effect. For example, if you configure the trap function for a host that has been configured with trap, the second configuration takes effect.

The rules for selecting the target host are as follows:

- If the **public-net** parameter is specified, the system accesses the target host on the public network.
- If the **vpn-instance** *vpn-instance-name* parameter is specified, the system accesses the target host in the specified VPN instance.
- If both the **public-net** and **vpn-instance** *vpn-instance-name* parameters are not specified:
  a. If the **source** *interface-type interface-number* parameter is specified and a VPN instance is bound to the specified interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the specified interface, the system accesses the target host on the public network.
  b. If the **snmp-agent trap source** command is run to configure a source interface for sending trap packets and a VPN instance is bound to the interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the interface, the system accesses the target host on the public network.
  c. If the **set net-manager vpn-instance** command is run to configure a network management VPN instance, the system accesses the target host in this VPN instance.
  d. If none of the preceding conditions is met, the system accesses the target host on the public network.

Configuration Impact

No matter whether a trap sent from the SNMP agent reaches the NMS, the SNMP agent deletes the trap to reduce the resource consumption.

Precautions

Ensure that the security level of a trap host is not higher than that of the user specified by **securityname** and not lower than that of the user group. Otherwise, the trap host cannot send trap messages properly. The user security level can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: noauthentication (no authentication or encryption)

If the SNMP trap function has been enabled, to ensure that SNMPv3-running devices normally send trap messages, **notify-view** *notify-view* must be configured in the **snmp-agent group** command for the user group to which **securityname** belongs to allow the devices to have the right to send trap messages.

For SNMPv1 and SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Allow the SNMP agent to send SNMP traps to the target host with the IP address of 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
[HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname comaccess
```

Allow the SNMP agent to send SNMP traps to the Huawei NMS with the IP address of 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
[HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname comaccess
private-netmanager
```

16.1.60 snmp-agent target-host trap ipv6

Function

The **snmp-agent target-host trap ipv6** command configures a target host to receive SNMP trap messages.

The **undo snmp-agent target-host ipv6** command deletes the configuration of a target host to receive SNMP trap messages.

By default, the target host that receives SNMP trap messages is not set.

Format

snmp-agent target-host trap ipv6 address udp-domain *ipv6-address* [**udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname** *security-name* [[**v1** | **v2c** | **v3** [**authentication** | **privacy**]] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

snmp-agent target-host trap ipv6 address udp-domain *ipv6-address* [**udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname cipher** *security-name* [[**v1** | **v2c**] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

undo snmp-agent target-host ipv6 *ipv6-address* **securityname** { *security-name* | **cipher** *security-name* } [**vpn-instance** *vpn-instance-name*]

undo snmp-agent target-host trap ipv6 address udp-domain *ipv6-address* [**udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
ipv6 address	Sets the IPv6 address of the target host used to receive SNMP trap messages.	-
udp-domain	Indicates that trap messages are sent to the target host through the User Datagram Protocol (UDP).	-
ipv6-address	Specifies the IPv6 address of the target host.	-
udp-port *port-number*	Specifies the port number used to receive trap messages.	The value is an integer that ranges from 0 to 65535. The default value is 162.
vpn-instance *vpn-instance-name*	Specifies a VPN instance name. If the **vpn-instance** *vpn-instance-name* parameter is not specified, the system accesses the target host on the public network. The device cannot send traps to a target host on the VPN interface specified by the **set net-manager vpn-instance** command.	The **vpn-instance** parameter is optional. If **vpn-instance** is configured, the VPN instance specified by **vpn-instance** *vpn-instance-name*, IP address, and security name specified by **securityname** *security-string* form a 3-tuple to identify a host on a VPN.

Parameter	Description	Value
params securityname *security-name*	Specifies the SNMP security name that is displayed as the user name on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.

Parameter	Description	Value
v1 | **v2c** | **v3**	Specifies the SNMP version. ● **v1**: indicates SNMPv1. ● **v2c**: indicates SNMPv2c. ● **v3**: indicates SNMPv3. If no SNMP version is specified, SNMPv1 is used by default.	-
authentication | **privacy**	Specifies the security mode for SNMP trap messages. ● **authentication**: indicates that the SNMP trap messages are authenticated but not encrypted. ● **privacy**: indicates that SNMP trap messages are authenticated and encrypted.	-
private-netmanager	Indicates that the target host is a Huawei NMS. Specify this parameter when a Huawei NMS is used. This parameter enables trap messages sent to the NMS to contain more information, including types, sequence numbers, and transmission time of trap messages.	-
notify-filter-profile *profile-name*	Specifies the name of a trap filter profile.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ext-vb	Indicates that trap messages sent to a target host carry extended bound variables. If alarm objects defined in public MIBs are extended on a Huawei data communication device, you can use **ext-vb** to determine whether the trap messages sent to the NMS carry extended bound variables. ● If **ext-vb** is not specified, trap messages sent from the device do not carry extended bound variables. When a third-party NMS is used, you are advised not to specify the **ext-vb** parameter so that the third-party NMS can receive trap messages from Huawei data communication devices. By default, trap messages sent from a Huawei data communication device do not carry extended bound variables. ● If **ext-vb** is specified, trap messages sent from the device carry extended bound variables. This parameter is recommended when a Huawei NMS is used so that more information can be transmitted in trap messages.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is used to configure an IPv6 NMS host so that traps can be sent to the host using the IPv6 protocol.

Precautions

Ensure that the security level of a trap host is not higher than that of the user specified by **securityname** and not lower than that of the user group. Otherwise, the trap host cannot send trap messages properly. The user security level can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: noauthentication (no authentication or encryption)

For SNMPv1 and SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Configure an IPv6 NMS host that uses SNMP v3. Set the security name to Test and configure traps to be authenticated and encrypted.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[HUAWEI] snmp-agent target-host trap ipv6 address udp-domain FC00::1 params securityname Test
v3 privacy
```

16.1.61 snmp-agent trap disable

Function

The **snmp-agent trap disable** command disables the trap function for all features.

The **undo snmp-agent trap disable** command restores the trap function for all features to the default status.

By default, the **display snmp-agent trap all** command can be used to view the status of the trap function for all features.

Format

snmp-agent trap disable

undo snmp-agent trap disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the trap function for all modules, run the **snmp-agent trap enable** command. To enable the trap function for a specified module, run the **snmp-agent trap enable feature-name** command.

- To disable the trap function for all modules, run the **snmp-agent trap disable** command.
- To restore the trap function for all features to the default status, run the **undo snmp-agent trap disable** or **undo snmp-agent trap enable** command.

NOTE

To disable the trap function for a specified module, run the **undo snmp-agent trap enable feature-name** command.

Example

Disable the trap function for all features.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap disable
```

16.1.62 snmp-agent trap enable

Function

The **snmp-agent trap enable** command enables the switch to send traps.

The **undo snmp-agent trap enable** command restores the default setting.

The default configuration of the **snmp-agent trap enable** command can be checked by the **display snmp-agent trap all** command.

Format

snmp-agent trap enable

undo snmp-agent trap enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

- To enable the trap function for all modules, run the **snmp-agent trap enable** command.

- To disable the trap function for all modules, run the **snmp-agent trap disable** command.
- To enable the trap function for a specified module, run the **snmp-agent trap enable feature-name** *feature-name* command.
- To disable the trap function for a specified module, run the **undo snmp-agent trap enable feature-name** *feature-name* command.
- To enable a specified trap for a specified module, run the **snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name* command.
- To disable a specified trap for a specified module, run the **undo snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name* command.
- To restore the default trap status of all modules, run the **undo snmp-agent trap disable** or **undo snmp-agent trap enable** command.

The **snmp-agent trap enable** command must be used together with the **snmp-agent target-host inform** command or **snmp-agent target-host trap** command.

To enable a device to send traps, you need to run at least the **snmp-agent target-host inform** command or **snmp-agent target-host trap** command on the device to specify the destination address of the traps.

Example

Enable the switch to send traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
```

16.1.63 snmp-agent trap enable feature-name

Function

The **snmp-agent trap enable feature-name** command enables a specified trap for a specified feature.

The **undo snmp-agent trap enable feature-name** command disables a specified trap for a specified feature.

The default configuration of the **snmp-agent trap enable feature-name** command can be checked using the **display snmp-agent trap all** command.

Format

snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the feature that generates traps.	acle, adpvxlan, arp, asmngtrap, bfd, bgp, cfgmgr, clkm, configuration, datasync, dhcp, dldp, easyoperatrap, efm, emdi, entityexttrap, entitymib, entitytrap, eoam-1ag, eoam-y1731, erps, error-down, etrunk, fm, ftp_server, gtl, hgmp, hsb-trap, http, ifnet, ifpdt, igmp, info, ip, ipfpm, iplpm, ipsec, ipv6, isis, l2bptnl, l2if, l2ifppi, l2vpn, l3mb, l3vpn, lacp, lbdt, ldp, line, lldptrap, loopdetect, mad, mcast, mid_aaa, mid_am, mid_eapol, mid_web, mld, mpls, mpls_lspm, mpls_rsvp, mrm, msdp, mstp, ntp, ospf, ospfv3, pim, pim-std, pki, pm, ptp, qose, radius, rip, rm, rmon, rrpp, securitytrap, sindex, snmp, srmtrap, sspadp, stack, swithsrvres, sysres, system, tcp, trunk, tunnel-te, uni-topomng, uni-tplm, uni-vermng, unimbrtrap, usbloadtrap, vbst, vcmp, vfs, vplsoam, vrrp, wlan
trap-name *trap-name*	Specifies the name of a trap.	For details about the alarm, see the Alarm Handling.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If **trap-name** *trap-name* is not specified, the switch enables all traps about a specified feature after the **snmp-agent trap enable feature-name** *feature-name* command is used.

You can run the **display snmp-agent trap feature-name all** command to check the configuration result.

Precautions

- The feature name asmngtrap, uni-topomng, uni-tplm, uni-vermng, and unimbrtrap are supported only on the SVF parent.
- The feature name etrunk is supported only on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H,

S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

- The feature name igmp, mld, mrm, msdp, pim-std, and pim are supported only on the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The feature name gtl takes effect only on the device that loads the license control item.
- If the IS-IS trap function is enabled before a version upgrade, you need to run the **snmp-agent trap enable feature-name isis** command to re-enable the trap function after the version upgrade. Otherwise, the previous configuration is lost.

Example

Enable the switch to send the fallingalarm trap about RMON to the NMS.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name rmon trap-name fallingalarm
```

16.1.64 snmp-agent trap life

Function

The **snmp-agent trap life** command sets the lifetime of trap messages. When the lifetime expires, the trap messages are discarded.

The **undo snmp-agent trap life** command cancels the current settings.

By default, the lifetime of trap messages is 300 seconds.

Format

snmp-agent trap life *seconds*

undo snmp-agent trap life

Parameters

Parameter	Description	Value
seconds	Specifies the lifetime of trap messages.	The value is an integer that ranges from 1 to 2592000, in seconds. The default value is 300.

Views

System view

Default Level

3: Management level

Usage Guidelines

Any trap messages are discarded after the duration expires. The trap messages are no longer reserved or sent.

Example

Set the lifetime of trap messages to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap life 60
```

16.1.65 snmp-agent trap queue-size

Function

The **snmp-agent trap queue-size** command sets the queue length of the trap messages sent to a target host.

The **undo snmp-agent trap queue-size** command cancels the current settings.

The default value is 1000.

Format

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Parameters

Parameter	Description	Value
size	Specifies the queue length of trap messages.	The value is an integer that ranges from 1 to 1000. The default value is 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a large number of trap messages need to be sent in a certain period of time, packets will be lost if the queue length of trap messages is insufficient. The queue length can be adjusted to reduce the packet loss ratio.

When the lifetime of trap messages is long, the queue length of trap messages needs to be lengthened. If the queue length is not lengthened, packet loss will occur.

Example

Set the queue length of the trap messages sent to the target host to 200.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap queue-size 200
```

16.1.66 snmp-agent trap start-trap resend disable

Function

The **snmp-agent trap start-trap resend disable** command disables the function of resending device cold-start or warm-start traps.

The **undo snmp-agent trap start-trap resend disable** command restores the default status of the function of resending device cold-start or warm-start traps.

By default, the function of resending device cold-start or warm-start traps is enabled.

Format

snmp-agent trap start-trap resend disable

undo snmp-agent trap start-trap resend disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

SNMP uses the resending mechanism for device cold-start or warm-start traps. This mechanism works in the following way:

- The system resends a cold-start or warm-start trap for three consecutive times to ensure that the trap can be sent to the destination.
- The first trap that the device sends must be a cold-start or warm-start trap. If another alarm is generated before the cold-start or warm-start trap, the system buffers that alarm and sends it only after the cold-start or warm-start trap is sent. The system also resends the buffered alarm for three consecutive times.

If the function of resending device cold-start or warm-start traps is not required any more, run the **snmp-agent trap start-trap resend disable** command to disable it.

Example

Disable the function of resending device cold-start or warm-start traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap start-trap resend disable
```

16.1.67 snmp-agent trap source

Function

The **snmp-agent trap source** command sets the source interface from which traps are sent.

The **undo snmp-agent trap source** command removes the set source interface configuration.

By default, source interface is not set.

Format

snmp-agent trap source *interface-type interface-number*

undo snmp-agent trap source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface that sends traps.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **snmp-agent trap source** command to specify the type and number of the interface on the device from which traps are sent. The system specifies the IP address of this interface as the source IP address of traps. In this way, the trap source can be identified on the NMS.

Precautions

The source interface that sends traps must have an IP address; otherwise, the commands will fail to take effect. To ensure device security, it is recommended that you set the source IP address to the local loopback address.

The source interface in traps on the device must be the same as the source interface specified on the NM station. Otherwise, the NM station cannot receive traps.

Example

Specify the IP address of VLANIF100 as the source address of traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap source vlanif 100
```

16.1.68 snmp-agent trap source-port

Function

The **snmp-agent trap source-port** command configures the number of the source port that sends trap messages.

The **undo snmp-agent trap source-port** command restores the default number of the source port that sends trap messages.

By default, the source port that sends trap messages is a random port.

Format

snmp-agent trap source-port *port-num*

undo snmp-agent trap source-port

Parameters

Parameter	Description	Value
port-num	Specifies the number of the source port that sends trap messages.	The value is an integer ranging from 1025 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve security of network packets, run the **snmp-agent trap source-port** command to configure the source port that sends trap messages. Therefore, the user firewall filters packets based on the port number.

Precautions

By default, a random port is used to send trap messages, and no configuration file is generated. After you configure a specific source port, the corresponding configuration file is generated. If you delete the specified source port, no configuration file is generated.

If a device sends packets to the NMS in Inform mode and the **snmp-agent trap source-port** command is run to change the source port number, SNMP uses the new source port instead of the original port to receive response packets from the NMS. As a result, packets are retransmitted.

Example

Set the number of the source port that sends SNMP agent trap messages to **1057**.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap source-port 1057
```

16.1.69 snmp-agent trap type

Function

The **snmp-agent trap type** command configures the device to send ENTITYTRAP traps or BASETRAP traps.

The **undo snmp-agent trap type** command restores the default configuration.

By default, the device sends BASETRAP traps.

Format

snmp-agent trap type { **base-trap** | **entity-trap** }

undo snmp-agent trap type

Parameters

Parameter	Description	Settings
base-trap	Configures the device to send BASETRAP traps.	-
entity-trap	Configures the device to send ENTITYTRAP traps.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two types of traps for the hardware of the switch: BASETRAP and ENTITYTRAP.

- The BASETRAP traps are sent when faults occur, so they are classified based on fault types. For example, the same BASETRAP trap is sent when a Power Module or a fan is removed.
- The ENTITYTRAP traps are classified based on hardware types. For example, different ENTITYTRAP traps are sent when a Power Module is removed and when a fan is removed.

The functions of the two types of traps are similar. Select one type of traps based on your requirements.

Precautions

The following conditions must be met; otherwise, the device does not send BASETRAP traps to the NMS:

- The trap type is set to base-trap using the **snmp-agent trap type** command.
- The BASETRAP trap function is enabled.

The following conditions must be met; otherwise, the device does not send ENTITYTRAP traps to the NMS:

- The trap type is set to entity-trap using the **snmp-agent trap type** command.
- The ENTITYTRAP trap function is enabled.

You can run the **clear alarm active** command to clear the alarms that are generated before the alarm type is changed.

After NETCONF is enabled on a device, the device sends traps only based on entity-trap.

Example

Configure the device to send BASETRAP traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap type base-trap
```

16.1.70 snmp-agent udp-port

Function

The **snmp-agent udp-port** command sets the listening port of the SNMP agent.

The **undo snmp-agent udp-port** command restores the default listening port of the SNMP agent.

By default, the listening port of the SNMP agent is 161.

Format

snmp-agent udp-port *port-num*

undo snmp-agent udp-port

Parameters

Parameter	Description	Value
port-num	Specifies the listening port of the SNMP agent.	The value is 161 or an integer that ranges from 1025 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The SNMP agent is a proxy process running on a network device. By default, the SNMP agent listens on port 161 to respond to instructions sent from the NMS. In this manner, the NMS can manage the network device. Fixing the listing port may threaten network security. For example, if all attack packets are sent to this listening port, the network is congested.

To improve device security, run the **snmp-agent udp-port** command to change the listening port of the SNMP agent.

Configuration Impact

After you run this command, the SNMP agent listens on the new port number. The original SNMP connection with the NMS is torn down, and the NMS must use the new port number to connect to the device.

Precautions

- Before configuring the listening port of the SNMP agent, run the **snmp-agent protocol source-interface** or **snmp-agent protocol source-status** command to enable the network device to receive and respond to NMS request packets.
- The listening port configured on the NMS must be the same as that specified by the **snmp-agent udp-port** command. Otherwise, the NMS cannot connect to the device.

Example

Set the listening port of the SNMP agent to 1057.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent udp-port 1057
```

16.1.71 snmp-agent usm-user

Function

The **snmp-agent usm-user** command creates an SNMPv3 user.

The **undo snmp-agent usm-user** command deletes an SNMPv3 user.

By default, no SNMPv3 user exists on a device.

Format

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* [**group** *group-name* | **acl** { *acl-number* | *acl-name* }] *

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **authentication-mode** { **md5** | **sha** | **sha2-256** } [**localized-configuration cipher** *password* | **cipher** *password*]

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } [**localized-configuration cipher** *password* | **cipher** *password*]

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **group** *group-name* **acl-ipv4** { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }]

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **group** *group-name* **acl-ipv6** { *acl-number* | *acl-name* }

undo snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* [**group** | **acl** | **authentication-mode** | **privacy-mode**]

Parameters

Parameter	Description	Value
remote-engineid *engineid*	Specifies the ID of the engine associated with a user. **remote-engineid** *engineid* must be set to the engine ID of the destination host that receives alarms. The engine IDs of the source and destination hosts must be different.	The value is string of 10 to 64 hexadecimal digits. It cannot be all 0s or all Fs.
v3	Indicates that the security mode in SNMPv3 is adopted.	-
user-name	Specifies the name of an SNMPv3 user.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
group *group-name*	Specifies the SNMPv3 user group to which the SNMPv3 user belongs.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
authentication-mode	Sets the authentication mode. Authentication is a process in which the SNMP agent (or the NMS) confirms that the message is received from an authorized NMS (or SNMP agent) and the message is not changed during transmission.	-
md5 | **sha** | **sha2-256**	Specifies the authentication algorithm. ● **md5**: Specifies HMAC-MD5-96 as the authentication algorithm. ● **sha**: Specifies HMAC-SHA-96 as the authentication algorithm. ● **sha2-256**: Specifies HMAC-SHA2-256-192 as the authentication algorithm. **NOTE** For higher security purposes, you are advised to specify the **sha2-256** parameter.	-
privacy-mode	Specifies the authentication with encryption. The system adopts the cipher block chaining (CBC) code of the data encryption standard (DES) and uses 128-bit privKey to generate the key. The NMS uses the key to calculate the CBC code and then adds the CBC code to the message while the SNMP agent fetches the authentication code through the same key and then obtains the actual information. Like the identification authentication, the encryption requires the NMS and the SNMP agent to share the same key to encrypt and decrypt the message.	-

Parameter	Description	Value
des56 | **aes128** | **aes192** | **aes256** | **3des**	Specifies DES-56, AES-128, AES-192, AES-256, or 3DES as the encryption algorithm. **NOTE** For higher security purposes, the DES-56 or 3DES algorithm is not recommended. If the DES-56 or 3DES algorithm is used, do not use passwords composed of repeated character strings. For example, in *str*n*, *str* is a repeated character string and *n* indicates the number of times this string repeats. Otherwise, the passwords containing any times of *str* can pass authentication. For example, if the password is **Huawei@123Huawei@123**, passwords **Huawei@123Huawei@123**, and **Huawei@123Huawei@123Huawei@123** can all pass authentication.	-
localized-configuration	Specifies the localized password configuration mode. **NOTE** After authentication and encryption passwords are configured through MIB, this keyword is displayed in the commands recorded in configuration files. After authentication and encryption passwords are configured through command line, you are not advised to use this keyword. If this keyword is used, the cipher text passwords configured later use the local format. As a password with the **localized-configuration** keyword is related to the engine ID, copying configurations with this keyword from one device to another causes the password to be invalid.	-

Parameter	Description	Value
cipher *password*	Specifies the password.	The value is a case-insensitive string without spaces. It must be in cipher text format with 32 to 108 characters. ● The password should not contain repeated character strings such as abc123abc123abc123 and **123abc**123abc. ● The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Special characters do not include the question mark (?) and space. ● The password entered in interactive mode is not displayed on the screen.
acl	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.

Parameter	Description	Value
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SNMPv1 and SNMPv2c have serious defects in terms of security. The security authentication mechanism used by SNMPv1 and SNMPv2c is based on the community name. In this mechanism, the community name is transmitted in plain text. You are not advised to use SNMPv1 and SNMPv2c on untrusted networks. By adopting the user-based security model, SNMPv3 eradicates the security defects in SNMPv1 and SNMPv2c and provides two services, authentication and encryption. SNMPv3 can provide higher security and confidentiality than SNMPv1 and SNMPv2c. The following table lists the difference between SNMPv1, SNMPv2c, and SNMPv3:

Table 16-21 Comparison in the security of SNMP of different versions

Protocol version	User Checksum	Encryption	Authentication
v1	Adopts the community name.	None	None
v2c	Adopts the community name.	None	None
v3	Adopts user name-based encryption/ decryption.	Yes	Yes

The **snmp-agent group** command can be used to configure the authentication, encryption, and access rights for an SNMPv3 user group. The **snmp-agent group** command can be used to configure the rights for SNMPv3 users in a specified SNMPv3 user group and bind the SNMPv3 user group to a MIB view. The MIB view is created through the **snmp-agent mib-view** command. For details, see the usage guideline of this command. After an SNMPv3 user group is configured, the

MIB-view-based access control is configured for the SNMPv3 user group. Users cannot access objects in the MIB view through the SNMPv3 user group. The purpose of adding SNMPv3 users to an SNMPv3 user group is to ensure that SNMPv3 users in an SNMPv3 user group have the same security level and access control list. When you run the **snmp-agent usm-user** command to configure a user in an SNMPv3 user group, you configure the MIB-view-based access rights for the user. If an SNMPv3 user group is configured with the AuthPriv access rights, you can configure the authentication mode and encryption mode when configuring SNMPv3 users. Note that the authentication keys and encryption passwords configured on the NMS and the SNMP agent should be the same; otherwise, authentication fails.

To ensure that the NMS correctly receives the alarm in Inform mode sent by the switch, run the **snmp-agent remote-engineid** *engineid* **usm-user v3** *user-name* command to specify the NMS engine ID on the host. After the command is run, the host encapsulates the NMS engine ID in the Authoritative Engine ID field of the SNMPv3 alarm packet before sending the alarm in Inform mode. After receiving the alarm, the NMS compares the engine ID carried in the received packet with its own engine ID. If the two IDs match, the NMS sends a response to the alarm host. If the two IDs do not match, the NMS discards the packet.

When the NMS and device are in an insecure network environment, for example, a network prone to attacks, it is recommended that you configure different authentication password and encryption password to improve security.

Configuration Impact

If an SNMP agent is configured with a remote user, the engine ID is required during the authentication. If the engine ID changes after the remote user is configured, the remote user becomes invalid.

Precautions

The security level of the SNMPv3 user must be higher than or equal to the security level of the SNMPv3 user group to which the SNMPv3 user belongs. The security level can be (in descending order): AuthPriv (authentication and encryption), authNoPriv (authentication without encryption), and noAuthNoPriv (neither authentication nor encryption). If the user security level is set to neither authentication nor encryption, the user only has the read-only permission within MIB-2 (OID: 1.3.6.1.2.1).

To add an SNMPv3 user to an SNMPv3 user group, ensure that the SNMPv3 user group is valid.

If you run the **snmp-agent usm-user** command multiple times, only the latest configuration takes effect.

Keep your user name and plain-text password well when creating the user. The plain-text password is required when the NMS accesses the device.

When a user with a level lower than the level configured using this command queries the password configured using the **display this** command, the password is displayed as asterisks (******).

To specify the same ACL on IPv4 and IPv6 networks, you can only run the **snmp-agent** [**remote-engineid** *engineid*] **usm-user v3** *user-name* **acl** { *acl-number* | *acl-name* } command.

If the **snmp-agent usm-user** command is run more than once to specify an ACL for the same SNMPv3 user, the latest configuration overrides the previous one.

Example

Configure an SNMPv3 user with user name **u1**, group name **g1**, authentication mode **sha2-256**, authentication password **8937561bc**, encryption mode **aes128**, and encryption password **68283asd**.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent usm-user v3 u1 group g1
[HUAWEI] snmp-agent usm-user v3 u1 authentication-mode sha2-256
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[HUAWEI] snmp-agent usm-user v3 u1 privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
[HUAWEI]
```

16.1.72 snmp-agent usm-user password complexity-check disable

Function

The **snmp-agent usm-user password complexity-check disable** command disables the complexity check for SNMPv3 user passwords.

The **undo snmp-agent usm-user password complexity-check disable** command enables the complexity check for SNMPv3 user passwords.

By default, the complexity check is enabled for SNMPv3 user passwords.

Format

snmp-agent usm-user password complexity-check disable

undo snmp-agent usm-user password complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the complexity check is enabled for SNMPMv3 user passwords, a newly-configured SNMPv3 user password needs to meet the requirements for the complexity check. After complexity check is disabled for SNMPv3 user passwords, the complexity of the passwords is not checked.

The requirements for the complexity of SNMPv3 user passwords are as follows:

- The password cannot be the same as the user name and cannot be the same as the user name in reverse order.
- The minimum length of a password is configured by using the **set password min-length** command. By default, a password contains 8 characters at least.
- A password includes at least two kinds of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding question marks (?) and spaces).

Precautions

- After complexity check is disabled for SNMPv3 user passwords, if a configured SNMPv3 user password is simple and does not meet the complexity requirements, the password may be easily attacked and cracked down by unauthorized users, affecting device security. Therefore, enabling the complexity check for SNMPv3 user passwords is recommended.
- In the configuration restoration stage, complexity check is not performed for SNMPv3 user passwords.
- Enabling the complexity check for SNMPv3 user passwords does not affect the SNMPv3 user passwords that have been configured.

Example

Disable the complexity check for SNMPv3 user passwords.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent usm-user password complexity-check disable
```

16.1.73 storage

Function

The **storage** command configures the storage mode for a bulk file.

The **undo storage** command restores the default storage mode for a bulk file.

By default, a bulk file is stored in ephemeral mode.

Format

storage ephemeral

undo storage

Parameters

Parameter	Description	Value
ephemeral	Indicates the ephemeral storage mode in which the bulk file is deleted after a specified period.	-

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Currently, the device supports only the ephemeral storage mode, which is the default storage mode. This command can be upgraded to support more storage modes.

Example

Set the storage mode of the bulk file **iftable** to ephemeral.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] storage ephemeral
```

16.1.74 transfer

Function

The **transfer** command configures the method of uploading a statistics file.

The **undo transfer** command removes the configured statistics file uploading method.

By default, a statistics file is not uploaded.

Format

transfer { **primary** | **secondary** } **protocol** { **tftp** | { { **ftp** | **sftp** } **username** *user-name* **password** *password* } } { **host** *host-name* } [**path** *destination-path*]

undo transfer { **primary** | **secondary** }

Parameters

Parameter	Description	Value
primary	Indicates the primary method of uploading a statistics file.	-
secondary	Indicates the secondary method of uploading a statistics file.	-
protocol	Indicates the protocol used by uploading a statistics file.	-
tftp	Specifies uploading a statistics file using TFTP.	-
ftp	Specifies uploading a statistics file using FTP.	-
sftp	Specifies uploading a statistics file using SFTP.	-
username *user-name*	Specifies the user name for uploading a statistics file using FTP or SFTP.	The value is a string of 1 to 64 characters.
password *password*	Specifies the user password for uploading a statistics file using FTP or SFTP.	In plaintext mode, the value is a string of 1 to 16 characters. In ciphertext mode, the value is a string of 32 or 48characters.
host *host-name*	Specifies the host name of the server.	The value is a string of 1 to 20 characters.
path *destination-path*	Specifies the destination folder for uploaded files.	The value is a string of 1 to 64 characters.

Views

Bulk-file view

Default Level

2: Configuration level

Usage Guidelines

Primary and secondary methods of uploading statistics files are supported. If the primary method fails, the secondary method is adopted.

You must configure a primary before enabling a statistics file. The secondary is optional.

You can modify a primary or secondary but cannot delete a primary when a statistics file is enabled; however, you can delete or configure a secondary when a statistics file is enabled.

Using SFTP as the upload mode is recommended to enhance security.

Example

Configure a primary method of uploading the statistics file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer primary protocol sftp username user password pwd host host-name
path folder/bulkstat1
```

Configure a secondary method of uploading the statistics file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer secondary protocol tftp host 10.1.0.1 path folder/bulkstat2
```

Remove the configured secondary method of uploading the statistics file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] undo transfer secondary
```

16.1.75 transfer interval

Function

The **transfer interval** command sets the upload interval for a bulk file.

The **undo transfer interval** command restores the default upload interval for a bulk file.

By default, the upload interval for a bulk file is 5 minutes.

Format

transfer interval *interval*

undo transfer interval

Parameters

Parameter	Description	Value
interval	Specifies the upload interval for a bulk file.	The value can be 5, 10, 15, or 30, in minutes.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

The upload interval for a bulk file must be longer than or equal to the statistics collection interval of the bulk file, and is an integral multiple.

The upload interval for a bulk file can be changed only when the bulk file is disabled.

Example

Set the upload interval to 15 minutes for the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer interval 15
```

16.1.76 transfer remain-time

Function

The **transfer remain-time** command sets the upload holding time for a bulk file.

The **undo transfer remain-time** command restores the default upload holding time for a bulk file.

By default, the upload holding time for a bulk file is 5 minutes.

Format

transfer remain-time *remain-time*

undo transfer remain-time

Parameters

Parameter	Description	Value
remain-time	Specifies the upload holding time for a bulk file.	The value is an integer that ranges from 1 to 30, in minutes.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an upload interval expires, the compressed bulk file must be retained for a period to ensure enough time for the file to be uploaded. This period is the upload holding time.

When the network quality is high and the file transfer is fast, you can reduce the upload holding time. When the network quality is low and the file transfer is slow, increase the upload holding time to improve file transfer reliability.

Precautions

To ensure that only one copy of a bulk file is uploaded to the server, set *remain-time* to be smaller than or equal to the file upload interval.

Example

Set the upload holding time to 10 minutes for bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer remain-time 10
```

16.1.77 transfer retry

Function

The **transfer retry** command sets the maximum number of retransmissions for a bulk file.

The **undo transfer retry** command restores the default maximum number of retransmissions for a bulk file.

By default, the maximum number of retransmissions for a bulk file is 5.

Format

transfer retry *retry-times*

undo transfer retry

Parameters

Parameter	Description	Value
retry-times	Specifies the maximum number of retransmissions for a bulk file.	The value is an integer that ranges from 0 to 5.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

The maximum number of retransmissions for a bulk file can be changed only when the bulk file is disabled.

If *retry-times* is set to 0 for a bulk file, the system does not retransmit the bulk file when the file fails to be uploaded.

Example

Set the maximum number of retransmissions to 1 for the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer retry 1
```

16.2 RMON and RMON2 Configuration Commands

16.2.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support RMON and RMON2.

16.2.2 display rmon alarm

Function

The **display rmon alarm** command displays information about RMON alarm function.

Format

display rmon alarm [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays information about the RMON alarm entry with the specified index. If no index is specified, information about all alarms is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the RMON alarm thresholds using the **rmon alarm** command, you can run this command to view the configured alarm variables, sampling interval, thresholds, alarm triggering condition, and last sampled value.

Example

Display the RMON alarm configurations.

```
<HUAWEI> display rmon alarm
Alarm table 1 owned by creator is valid.
  Samples delta value       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval         : 5(sec)
  Rising threshold          : 1000 (linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  Latest value              : 0
```

Table 16-22 Description of the display rmon alarm command output

Item	Description
Alarm table *entry-number* owned by *owner* is *status*.	The current status of the alarm entry *entry-number* created by *owner* is *status*. ● *entry-number*: alarm entry index, corresponding to the alarmIndex object in alarmTable. ● *owner*: creator of the entry, corresponding to the alarmOwner object in alarmTable. ● *status*: row status of the alarm entry with the specified index, corresponding to the alarmStatus in alarmTable: undercreation(invalid), valid(valid), invalid(no valid trap). You can run the **rmon alarm** command to configure *entry-number* and *owner*.

Item	Description
Samples delta value	Alarm variable, namely, monitored MIB object, corresponding to the alarmVariable object in alarmTable. You can run the **rmon alarm** command to configure this parameter.
Sampling interval	Sampling interval, in seconds, corresponding to the alarmInterval object in alarmTable. You can run the **rmon alarm** command to configure this parameter.
Rising threshold	Rising threshold of the alarm table, corresponding to the alarmRisingThreshold object in alarmTable. When the sampled value reaches or exceeds the rising threshold, an alarm is generated. You can run the **rmon alarm** command to configure this parameter.
Falling threshold	Falling threshold of the alarm table, corresponding to the alarmFallingThreshold object in alarmTable. When the sampled value reaches or falls below the falling threshold, an alarm is generated. You can run the **rmon alarm** command to configure this parameter.
When startup enables	Condition that triggers alarms for the first time, corresponding to the alarmStartupAlarm object in alarmTable. When the sampled value exceeds the rising threshold or falls below the falling threshold, an alarm is generated. The values are: ● risingOrFallingAlarm: generating an alarm when the sampled value exceeds the rising threshold or falls below the falling threshold ● risingAlarm: generating an alarm when the sampled value exceeds the rising threshold ● fallingAlarm: generating an alarm when the sampled value falls below the falling threshold You can run the **rmon alarm** command to configure this parameter.
Latest value	Latest sampled value, corresponding to the alarmValue object in alarmTable.

16.2.3 display rmon event

Function

The **display rmon event** command displays information about RMON events.

Format

display rmon event [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays the configuration of the RMON event with the specified index. If no index is specified, information about all events is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the trap or log function for RMON events, you can run this command to view the configured event description, whether events trigger traps and logs, and latest event.

Example

Display the RMON event configurations.

```
<HUAWEI> display rmon event
Event table 1 owned by Test is valid.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.69th.
```

Table 16-23 Description of the display rmon event command output

Item	Description
Event table *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. ● *entry-number*: event entry index, corresponding to the eventIndex object in eventTable. ● *owner*: creator of the entry, corresponding to the eventOwner object in eventTable. ● *status*: row status of the event entry with the specified index, corresponding to the eventStatus in eventTable: undercreation(invalid), valid(valid), invalid(no valid event). You can run the **rmon event** command to configure *entry-number* and *owner*.
Description	Event description, corresponding to the eventDescription object in eventTable. You can run the **rmon event** command to configure this parameter.
Will cause log when triggered	Whether events trigger traps or logs, corresponding to the eventType object in eventTable. The actions associated with events are as follows: ● none: no action is taken. ● log: a log is recorded when an event is triggered. ● trap: a trap is sent to the NMS when an event is triggered. ● log-trap: a log is recorded and a trap is sent to the NMS when an event is triggered. You can run the **rmon event** command to configure this parameter.
last triggered at	Latest event time, corresponding to the eventLastTimeSent object in eventTable.

16.2.4 display rmon eventlog

Function

The **display rmon eventlog** command displays details about RMON event logs.

Format

display rmon eventlog [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays the log with the specified index. If no index is specified, information about all event logs is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you use the **rmon event** command to specify that a log is recorded for a certain event, the event record is stored in the LogTable. The command output includes event index, current event status, time the event triggers a log (calculated based on the number of seconds elapsed since system initialization or startup), and event description.

Example

Display the log of RMON event 1.

```
<HUAWEI> display rmon eventlog 1
Event table 1 owned by User is valid.
  Generates eventLog 1.1 at 0days 00h:00m:07s.43th.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1, less than or equal to 100 with alarm
value 0. Alarm sample type is delta.
  Generates eventLog 1.2 at 0days 00h:02m:26s.43th.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1, greater than or equal to 1000 with alarm
value 10443. Alarm sample type is delta.
```

Table 16-24 Description of the display rmon eventlog command output

Item	Description
Event table *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. ● entry-number: event log entry index, corresponding to the logEventIndex object in LogTable. ● owner: creator of the entry, corresponding to the eventOwner object in eventTable. ● status: row status of the event entry with the specified index, corresponding to the eventStatus in eventTable: undercreation(invalid), valid(valid), invalid(no valid event log).
Generates eventLog at	Log creation time (time elapsed since system startup), corresponding to the logTime object in LogTable.
Description	Event description, corresponding to the logDescription object in LogTable.

16.2.5 display rmon history

Function

The **display rmon history** command displays RMON history sampling information.

Format

display rmon history [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RMON history sampling information on the specified Ethernet interface. If this parameter is not specified, RMON history sampling information on all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring RMON history statistics on an interface using the **rmon history** command, the system samples packets on the interface periodically. The **display rmon history** command can display history sampling information, including the number of sampled packets, history sampling interval, latest sampling information, Ethernet interface usage, number of CRC error packets, and total number of packets.

Example

Display RMON history sampling information.

```
<HUAWEI> display rmon history
History control entry 1 owned by Creator is valid
  Samples interface     : GigabitEthernet0/0/1<ifIndex.402653698>
  Sampling interval     : 30(sec) with 10 buckets max
  Last Sampling time    : 0days 00h:09m:43s.00th
  Latest sampled values :
  octets               :645       , packets           :7
  broadcast packets    :7         , multicast packets :0
  undersize packets    :6         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
```

Display RMON history sampling information on the specified interface.

```
<HUAWEI> display rmon history gigabitethernet 0/0/1
History control entry 1 owned by Creator is valid
  Samples interface     : GigabitEthernet0/0/1<ifIndex.402653698>
  Sampling interval     : 30(sec) with 10 buckets max
  Last Sampling time    : 0days 00h:09m:43s.00th
  Latest sampled values :
  octets               :645       , packets           :7
  broadcast packets    :7         , multicast packets :0
  undersize packets    :6         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
  History record:
  Record No.1 (Sample time: 0days 00h:02m:30s.01th)
  octets               :0         , packets           :0
  broadcast packets    :0         , multicast packets :0
  undersize packets    :0         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
```

Table 16-25 Description of the display rmon history command output

Item	Description
History control entry *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. - *entry-number*: history control table entry index, corresponding to the historyControlIndex object in historyControlTable. - *owner*: creator of the entry, corresponding to the historyControlOwner object in historyControlTable. - *status*: row status of the history control table entry with the specified index, corresponding to the historyControlStatus in historyControlTable: undercreation(invalid), valid(valid), invalid(no valid historical sampling information). You can run the **rmon history** command to configure *entry-number* and *owner*.
Samples interface	Sampled interface.
Sampling interval	Sampling interval, in seconds, corresponding to the historyControlInterval object in historyControlTable. The system samples packets on the interface at this interval. You can run the **rmon history** command to configure this parameter.
Last Sampling time	Latest sampling time, corresponding to the etherHistoryIntervalStart object in etherHistoryTable.
Latest sampled values	Latest sampling result.
octets	Number of bytes received in a sampling interval, corresponding to the etherHistoryOctets object in etherHistoryTable.
packets	Number of packets received in a sampling interval, corresponding to the etherHistoryPkts object in etherHistoryTable.
broadcast packets	Number of broadcast packets received in a sampling interval, corresponding to the etherHistoryBroadcastPkts object in etherHistoryTable.
multicast packets	Number of multicast packets received in a sampling interval, corresponding to the etherHistoryMulticastPkts object in etherHistoryTable.
undersize packets	Number of undersize packets received in a sampling interval, corresponding to the etherHistoryUndersizePkts object in etherHistoryTable.

Item	Description
oversize packets	Number of large packets received in a sampling interval, corresponding to the etherHistoryOversizePkts object in etherHistoryTable.
fragments packets	Number of undersize and CRC error packets received in a sampling interval, corresponding to the etherHistoryFragments object in etherHistoryTable.
jabbers packets	Number of large and CRC error packets received in a sampling interval, corresponding to the etherHistoryJabbers object in etherHistoryTable.
CRC alignment errors	Number of CRC error packets received in a sampling interval, corresponding to the etherHistoryCRCAlignErrors object in etherHistoryTable.
collisions	Number of collision packets received in a sampling interval, corresponding to the etherHistoryCollisions object in etherHistoryTable.
Dropped packet	Number of packets discarded in a sampling interval, corresponding to the etherHistoryDropEvents object in etherHistoryTable.
utilization	Bandwidth usage in a sampling interval, corresponding to the etherHistoryUtilization object in etherHistoryTable.
History record	History sampling result.

16.2.6 display rmon prialarm

Function

The **display rmon prialarm** command displays information about RMON extended alarm function.

Format

display rmon prialarm [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays information about the RMON extended alarm entry with the specified index. If this parameter is not specified, all RMON extended alarm information is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring RMON extended alarm function using the **rmon prialarm** command, you can run this command to view sampling interval, rising and falling thresholds, alarm triggering condition, and latest sampled value.

Example

Display the RMON extended alarm configurations.

```
<HUAWEI> display rmon prialarm
Prialarm table 1 owned by Test is valid.
  Samples absolute value    : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 3)
  Falling threshold         : 100(linked with event 3)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever
  Latest value              : 557
```

Table 16-26 Description of the display rmon prialarm command output

Item	Description
Prialarm table *entry-number* owned by *owner* is *status*.	The current status of the extended alarm entry *entry-number* created by *owner* is *status*. ● *entry-number*: extended alarm entry index. ● *owner*: creator of the entry. ● *status*: row status of the extended alarm entry with the specified index: undercreation(invalid), valid(valid), invalid(no valid extended alarm information). You can run the **rmon prialarm** command to configure *entry-number* and *owner*.
Samples *type* value	The sampling type is *type*. The value of *type* can be: ● absolute: absolute value sampling ● delta: variable value sampling ● changeratio: change rate of sampled values (Change rate = Value change/Sampling interval) This field is followed by an alarm variable. You can run the **rmon prialarm** command to configure this parameter.

Item	Description
Sampling interval	Interval at which traffic is sampled, in seconds. You can run the **rmon prialarm** command to configure this parameter.
Rising threshold	Alarm rising threshold. You can run the **rmon prialarm** command to configure this parameter.
Falling threshold	Alarm falling threshold. You can run the **rmon prialarm** command to configure this parameter.
linked with event *entry-number*	Associate with the row with index *entry-number*. You can run the **rmon prialarm** command to configure this parameter.
When startup enables	Condition that triggers alarms for the first time. The values are: ● risingOrFallingAlarm: generating an alarm when the sampled value exceeds the rising threshold or falls below the falling threshold ● risingAlarm: generating an alarm when the sampled value exceeds the rising threshold ● fallingAlarm: generating an alarm when the sampled value falls below the falling threshold You can run the **rmon alarm** command to configure this parameter.
This entry will exist	Aging time of the extended alarm entry. An entry may be valid permanently or in a certain period. You can run the **rmon prialarm** command to configure this parameter.
Latest value	Latest sampling result.

16.2.7 display rmon statistics

Function

The **display rmon statistics** command displays RMON Ethernet statistics.

Format

display rmon statistics [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RMON Ethernet statistics on the specified Ethernet interface. If this parameter is not specified, RMON Ethernet statistics on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you configure Ethernet statistics using the **rmon statistics** command, the system collects packet statistics on Ethernet interfaces. The command output includes communication information generated since statistics function is enabled. The command output helps you locate faults.

When the device restarts, all statistics are cleared.

Example

Display RMON Ethernet statistics.

```
<HUAWEI> display rmon statistics
Statistics entry 1 owned by Creator is valid.
  Interface : GigabitEthernet0/0/1<ifIndex.402653698>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersize packets   :0         , oversize packets :0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

Table 16-27 Description of the display rmon statistics command output

Item	Description
Statistics entry *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. ● entry-number: Ethernet statistics entry, corresponding to the etherStatsIndex object in etherStatsTable. ● owner: creator of the entry, corresponding to the etherStatsOwner object in etherStatsTable. ● status: row status of the Ethernet statistics entry with the specified index, corresponding to the etherStatsStatus in etherStatsTable: undercreation(invalid), valid(valid), invalid(no valid statistics information). You can run the **rmon statistics** command to configure *entry-number* and *owner*.
Interface	Interface where statistics are collected, corresponding to the etherStatsDataSource object in etherStatsTable, followed by the interface OID.
Received	Number of received packets.
octets	Number of received octets.
packets	Number of received packets, corresponding to the etherStatsPkts object in etherStatsTable.
broadcast packets	Number of received broadcast packets, corresponding to the etherStatsBroadcastPkts object in etherStatsTable.
multicast packets	Number of received multicast packets, corresponding to the etherStatsMulticastPkts object in etherStatsTable.
undersize packets	Number of received undersize packets, corresponding to the etherStatsUndersizePkts object in etherStatsTable.
oversize packets	Number of received large packets, corresponding to the etherStatsOversizePkts object in etherStatsTable. **NOTE** The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S cannot collect statistics on the packets of which the lengths range from 1518 to **n**. **n** is the maximum frame length allowed by the interface, and can be set using the **jumboframe enable** command.
fragments packets	Number of received undersize and CRC error packets, corresponding to the etherStatsFragments object in etherStatsTable.

Item	Description
jabbers packets	Number of received large and CRC error packets, corresponding to the etherStatsJabbers object in etherStatsTable. **NOTE** The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this item.
CRC alignment errors	Number of received CRC error packets, corresponding to the etherStatsCRCAlignErrors object in etherStatsTable.
collisions	Number of received collision packets, corresponding to the etherStatsCollisions object in etherStatsTable.
Dropped packet	Number of discarded packets, corresponding to the etherStatsDropEvents object in etherStatsTable.
Packets received according to length	Number of received packets with different lengths, corresponding to the etherStatsPkts64Octets, etherStatsPkts65to127Octets, etherStatsPkts128to255Octets, etherStatsPkts256to511Octets, etherStatsPkts512to1023Octets, and etherStatsPkts1024to1518Octets objects in etherStatsTable. **NOTE** In classified packet statistics on the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, 1024-1518 includes the packets longer than 1518. On the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, or S6720S-S, this field is displayed 0.

16.2.8 display rmon2 hlhostcontroltable

Function

The **display rmon2 hlhostcontroltable** command displays information about entries in hlHostControlTable.

Format

display rmon2 hlhostcontroltable [**index** *ctrl-index*] [**verbose**]

Parameters

Parameter	Description	Value
ctrl-index	Indicates the entry index, which uniquely identifies an entry in the host control table.	The value is an integer that ranges from 1 to 65535.
verbose	Displays details about the host control table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you use the **rmon2 hlhostcontroltable** command to create a protocol directory table, you can run the **display rmon2 hlhostcontroltable** command to view the configurations.

If no entry index is specified, the configuration of the entire table is displayed.

Example

Display information about the entry with index 123 in the host control table.

```
<HUAWEI> display rmon2 hlhostcontroltable index 123
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
status - hlhostcontrolstatus

index datasource                droppedfrm inserts    Deletes    maxentries       status
123   Vlanif10                 0          0          0          50               active
```

Display detailed information about the entry with index 123 in the host control table.

```
<HUAWEI> display rmon2 hlhostcontroltable index 123 verbose
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
owner - hlhostcontrolowner
status - hlhostcontrolstatus
index       :   123
datasource  :   Vlanif10
droppedfrm  :   0
inserts     :   0
Deletes     :   0
```

```
maxentries :   50
owner      :   china
status     :   active
```

Table 16-28 Description of the **display rmon2 hlhostcontroltable** command output

Item	Description
index	Index of an entry in the hlHostControlTable. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
datasource	Source interface of data. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
droppedfrm	Number of the frames that are received on the statistics interface but not added into nlHost entries.
inserts	Times add nlHost entries are added to nlHostTable.
Deletes	Times nlHost entries are deleted from nlHostTable.
maxentries	Maximum number of entries that hlHostControlTable contains. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
owner	Owner of the entry in the hlHostControlTable. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
status	Status of the entry in the hlHostControlTable: ● active: running normally ● not in service: invalid You can run the **rmon2 hlhostcontroltable** command to configure this parameter.

16.2.9 display rmon2 nlhosttable

Function

The **display rmon2 nlhosttable** command displays information about entries in the nlHostTable.

Format

display rmon2 nlhosttable [**hostcontrolindex** *ctrl-index*] [**timemark** *time-value*] [**protocoldirlocalindex** *protocol-local-index*] [**hostaddress** *ip-address*]

Parameters

Parameter	Description	Value
hostcontrolindex *ctrl-index*	Specifies the index number. A *ctrl-index* uniquely identifies an entry in the hlHostControlTable.	It is an integer ranging from 1 to 65535.
timemark *time-value*	Enables the time filter.	The value is in the range of 0 to 4294967295. The entries in the nlHostTable with the ChgTm value being larger than this value are displayed.
protocoldirlocalindex *protocol-local-index*	Identifies the network layer protocol of the nlHostAddress.	Its value ranges from 1 to 2147483647.
hostaddress *ip-address*	Checks the traffic on a specified host.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After statistics function is configured on an interface, you can view traffic statistics using this command. A maximum of 5000 rows can be displayed for each protocol on an interface.

Example

Display information about the entry with index 1 in the host table.

```
<HUAWEI> display rmon2 nlhosttable hostcontrolindex 1 protocoldirlocalindex 2 hostaddress
10.110.94.177
Abbreviation:
HIdx - hlHostControlIndex
PIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIdx Addr          InPkts  OutPkts InOctes OutOctes OutMac       ChgTm                         CrtTm
1     2    10.110.94.177  59      68      3240    3821         0        0 days 00h:01m:29s.09th(8909)  0 days 00h:
01m:01s.13th(6113)
```

Table 16-29 Description of the display rmon2 nlhosttable command output

Item	Description
HIdx	Index of the host control table.
PIdx	Protocol directory index.
Addr	Host address. It is the source address of the incoming IP packets on the monitored interface and destination address of the outgoing IP packets on the interface.
InPkts	Number of incoming packets on the monitored interface.
OutPkts	Number of outgoing packets on the monitored interface.
InOctes	Number of incoming bytes on the monitored interface.
OutOctes	Number of outgoing bytes on the monitored interface.
OutMac	Number of outgoing non-unicast packets on the monitored interface.
ChgTm	Entry time filter in the host control table.
CrtTm	Customized time filter.

16.2.10 display rmon2 protocoldirtable

Function

The **display rmon2 protocoldirtable** command displays all entries in the protocolDirTable.

Format

display rmon2 protocoldirtable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you use the **rmon2 protocoldirtable** command to configure statistics on IP packets, you can run the **display rmon2 protocoldirtable** command to view the configurations.

Example

Display entries in the protocolDirTable.

```
<HUAWEI> display rmon2 protocoldirtable
protocolDirId              :   8.0.0.0.1.0.0.8.0
protocolDirParameters      :   2.0.0
protocolDirLocalIndex      :   2
protocolDirDescr           :   ww
protocolDirAddressMapConfig:   not supported
protocolDirHostConfig      :   supported on
protocolDirMatrixConfig    :   not supported
protocolDirOwner           :   test
protocolDirStatus          :   active
```

Table 16-30 Description of the display rmon2 protocoldirtable command output

Item	Description
protocolDirId	Protocol directory ID. Currently, RMON2 only supports IP protocol, so the protocol directory ID is fixed at 8.0.0.0.1.0.0.8.0.
protocolDirParameters	Protocol directory parameter. The value is fixed at 2.0.0.
protocolDirLocalIndex	Local protocol directory index.
protocolDirDescr	Indicates the description of the protocol directory table. You can run the **rmon2 protocoldirtable** command to configure this parameter.
protocolDirAddressMapConfig	Whether protocol directory address mapping is supported. This function is not supported currently.
protocolDirHostConfig	Whether the configuration of protocol directory host is supported: ● not supported: The device does not monitor the network-layer host table of the protocol, and this value cannot be changed. ● supported on: The device can monitor the network-layer host table of the protocol, and the monitoring function is enabled. ● supported off: The device can monitor the network-layer host table of the protocol, but the monitoring function is disabled. You can run the **rmon2 protocoldirtable** command to configure this parameter.

Item	Description
protocolDirMatrixConfig	Whether protocol directory matrix is supported. This function is not supported currently.
protocolDirOwner	Indicates the owner. You can run the **rmon2 protocoldirtable** command to configure this parameter.
protocolDirStatus	Protocol directory status. ● active: running normally ● not in service: invalid You can run the **rmon2 protocoldirtable** command to configure this parameter.

16.2.11 rmon alarm

Function

The **rmon alarm** command adds an entry to the alarm table.

The **undo rmon alarm** command deletes an entry from the alarm table.

Format

rmon alarm *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**startup-alarm** { **falling** | **rising** | **risingorfalling** }] [**owner** *owner-name*]

undo rmon alarm *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
alarm-OID	Specifies the OID of a monitored object.	The name is a string of 1 to 256 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
sampling-time	Specifies the sampling interval.	The value is an integer that ranges from 5 to 65535, in seconds.
absolute	Indicates that the sample type is absolute. The value is the sampled value at the end of the period.	-
changeratio	Indicates that the sample type is changeratio. The value is Changing value/Sampling interval.	-
delta	Indicates that the sample type is delta. The value is the difference between the samples at the beginning and end of the period.	-
rising-threshold *threshold-value1*	Specifies the rising threshold of sampled value.	The value is an integer that ranges from 1 to 2147483647.
event-entry1	Indicates the event index corresponding to the rising threshold.	The value is an integer that ranges from 1 to 65535.
falling-threshold *threshold-value2*	Specifies the falling threshold of sampled value.	The value is an integer that ranges from 0 to 2147483646.
event-entry2	Indicates the event index corresponding to the falling threshold.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
startup-alarm { **falling** | **rising** | **risingorfalling** }	Specifies the condition of sending an alarm when the system data is sampled for the first time. ● **falling**: an alarm is sent when the sampled value falls below the lower threshold value. ● **rising**: an alarm is sent when the sampled value exceeds the upper threshold value. ● **risingorfalling**: an alarm is sent when the sampled value exceeds the upper threshold value or the lower threshold value. **NOTE** An alarm is sen no matter whether the following sampled value exceeds the upper threshold value or the lower threshold value.	-
owner *owner-name*	Indicates the owner of the alarm.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor system running status, run the **rmon alarm** command to configure an alarm table and add an entry to the alarm table. After the command is executed, the RMON alarm function is enabled. The system obtains information about the monitored object at the specified interval, and compares the obtained value with the configured threshold. Then the system triggers the event according to the following table, and records log or sends a trap to the NMS.

Situation	Action
The sampled value is greater than or equal to the configured rising threshold *threshold-value1*.	Trigger *event-entry1*.
The sampled value is smaller than or equal to the configured falling threshold *threshold-value2*.	Trigger *event-entry2*.

Prerequisites

Before configuring alarm function for the specified object, run the **rmon event** command to define the associated events. Otherwise, events cannot be triggered even if alarms are generated.

If the alarm variables configured in RMON alarm function are MIB variables defined in the statistics group or history group, the Ethernet statistics function or history statistics function must be configured on the monitored Ethernet interface first. Otherwise, alarm entries cannot be created.

Example

Monitor the alarm threshold of etherStatsBroadcastPkts.1 (1.3.6.1.2.1.16.1.1.1.6.1) and sample the absolute value with an interval of 30 seconds. When the sampled value is greater than or equal to the upper threshold 500, event 1 is triggered. When the sampled value is less than or equal to the lower threshold 100, event 2 is triggered. The **creator** parameter indicates the owner that creates the event.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon statistics 1 owner creator
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] rmon event 1 log
[HUAWEI] rmon event 2 trap public
[HUAWEI] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 500 1 falling-threshold
100 2 owner creator
```

16.2.12 rmon event

Function

The **rmon event** command adds an entry to the event table.

The **undo rmon event** command deletes an entry from the event table.

Format

rmon event *entry-number* [**description** *string*] { **log** | **trap** *object* | **log-trap** *object* | **none** } [**owner** *owner-name*]

undo rmon event *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
description *string*	Specifies the event description.	The value is a string of 1 to 127 characters.
log	Records a log for the event.	-
trap	Sends a trap to the NMS.	-
object	Specifies the community name of the NMS receiving the trap.	The value is a string of 1 to 127 characters.
log-trap	Records a log and sends a trap to the NMS for the event.	-
none	Indicates that no action is taken for the event.	-
owner *owner-name*	Indicates the creator of the event entry.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command specifies whether to record a log or send a trap for events. When an error occurs in the system, the RMON alarm function triggers the corresponding event. You can run the **rmon event** command to configure an event table and add an entry to the table. The entry specifies whether to record a log or send a trap to the NMS for the event.

Prerequisites

The **rmon alarm** command is executed to configure the alarm objects. Otherwise, no alarm will trigger the event.

Example

Send a trap to the NMS for event 10.

```
<HUAWEI> system-view
[HUAWEI] rmon event 10 trap public
```

16.2.13 rmon history

Function

The **rmon history** command adds an entry to the history control table.

The **undo rmon history** command deletes an entry from the history control table.

Format

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]

undo rmon history *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
buckets *number*	Indicates the maximum number of records in the history control table.	The value is an integer that ranges from 1 to 10.
interval *sampling-interval*	Specifies the sampling interval.	The value is an integer that ranges from 5 to 3600, in seconds.
owner *owner-name*	Indicates the owner of the entry in the history control table.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect statistics on the specified interface at an interval and save the statistics for future retrieval, run the **rmon history** command to configure a history control table and add an entry to the table. The system can periodically collect statistics on each type of traffic, including bandwidth usage, number of error packets, and total number of packets.

Precautions

The number of stored records is determined by the **buckets** *number* parameter. When the number of records in the table reaches the maximum, the system overwrites the old records with new ones. Statistics include the number of packets, broadcast packets, and multicast packets received by the interface within a sampling interval. You can run the **display rmon history** command to view history sampling results.

In versions earlier than V200R019C00, this command cannot be configured on Eth-Trunk member interfaces. Starting from V200R019C00, this command can be configured on Eth-Trunk member interfaces.

Example

Configure a history control table and add an entry with index 1 to the table. Set the maximum number of entries in the table to 10, sampling interval to 5 seconds, and creator to **user1**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

16.2.14 rmon prialarm

Function

The **rmon prialarm** command adds an entry to the extended alarm table.

The **undo rmon prialarm** command deletes an entry from the extended alarm table.

Format

rmon prialarm *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *owner-name*]

undo rmon prialarm *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
prialarm-formula	Specifies the formula for calculating an alarm variable. The alarm variable in the formula is identified by an OID. The OID value starts with a dot, for example, (.1.3.6.1.2.1.2.1.10.1)*8. The calculation formula is defined by user. The calculation result is a long integer. Ensure that the length of calculation result in each step cannot exceed the limit; otherwise, the calculation result is incorrect.	The value is a string of 1 to 256 characters.
description-string	Specifies the alarm description.	The value is a string of 1 to 256 characters.
sampling-interval	Specifies the sampling interval.	The value is an integer that ranges from 10 to 65535, in seconds.
absolute	Indicates that the sample type is absolute. The value is the sampled value at the end of the period.	-
changeratio	Indicates that the sample type is changeratio. The value is Changing value/Sampling interval.	-
delta	Indicates that the sample type is delta. The value is the difference between the samples at the beginning and end of the period.	-
rising-threshold *threshold-value1*	Specifies the alarm rising threshold.	The value is an integer that ranges from 1 to 2147483647.
event-entry1	Indicates the entry number of the event corresponding to the rising threshold in the event table.	The value is an integer that ranges from 1 to 65535.
falling-threshold *threshold-value2*	Specifies the alarm falling threshold.	The value is an integer that ranges from 0 to 2147483646.
event-entry2	Indicates the entry number of the event corresponding to the falling threshold in the event table.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
entrytype	Indicates the lifetime type of an alarm entry.	-
cycle *entry-period*	Indicates the lifetime of an alarm entry.	The value is an integer that ranges from 11 to 2147483646.
forever	Indicates that the alarm entry is valid permanently.	-
owner *owner-name*	Indicates the owner of the extended alarm variable.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The extended alarm function can compute the alarm variables and compare the result with the specified threshold.

After the extended alarm function is enabled, the system performs the following operations:

1. Samples the alarm variables in the extended alarm formula at the specified sampling interval.
2. Calculates the sampled value using the defined formula.
3. Compares the calculation result with the thresholds and takes actions according to the following table.

Situation	Action
The sampled value is greater than or equal to the configured rising threshold *threshold-value1*.	Trigger *event-entry1*.
The sampled value is smaller than or equal to the configured falling threshold *threshold-value2*.	Trigger *event-entry2*.

To use more alarm functions, run the **rmon prialarm** command to configure the extended alarm table and add an entry to the table.

Prerequisites

Before configuring extended alarm function for the specified object, run the **rmon event** command to define the associated events. Otherwise, events cannot be triggered even if alarms are generated. When the sampled value exceeds the rising threshold or falls below the falling threshold, whether to record a log or send a trap to the NMS is determined by the **rmon event** command.

Example

Monitor broadcast and multicast packets: Set the sampling interval to 10 seconds and sample type to absolute. Trigger event 3 when the sample value reaches or exceeds 100000 and when the sample value reaches or falls below 100. Set the lifetime of the entry to forever and the owner to **Test**.

```
<HUAWEI> system-view
[HUAWEI] rmon prialarm 1 .1.1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 10
absolute rising-threshold 100000 3 falling-threshold 100 3 entrytype forever owner Test
```

16.2.15 rmon statistics

Function

The **rmon statistics** command adds an entry to the statistics table.

The **undo rmon statistics** command deletes an entry from the statistics table.

Format

rmon statistics *entry-number* [**owner** *owner-name*]

undo rmon statistics *entry-number*

Parameters

Parameter	Description	Value
entry-number	Indicates the row index corresponding to the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
owner *owner-name*	Indicates the owner name.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To keep collecting statistics on the current interface, run the **rmon statistics** command to configure a statistics table and add an entry to the table. This command monitors usage of Ethernet interfaces and collects statistics on errors, including the number of collision packets, CRC error packets, undersize and large packets, timeout packets, fragments, broadcast packets, multicast packets, and unicast packets.

Prerequisites

The **rmon-statistics enable** command is executed to enable RMON statistics function on the interface. If the command is not executed, the statistics result is 0.

Precautions

In versions earlier than V200R019C00, this command cannot be configured on Eth-Trunk member interfaces. Starting from V200R019C00, this command can be configured on Eth-Trunk member interfaces.

Example

Configure a statistics table on GigabitEthernet0/0/1 and add an entry with index 20 to the table.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon statistics 20 owner creater
```

16.2.16 rmon2 hlhostcontroltable

Function

The **rmon2 hlhostcontroltable** command creates or changes an entry in the hlHostControlTable.

The **undo rmon2 hlhostcontroltable** command deletes an entry from the hlHostControlTable or from the whole table.

Format

rmon2 hlhostcontroltable index *ctrl-index* [**datasource interface** *interface-type interface-number*] [**maxentry** *maxentry-value*] [**owner** *owner-name*] [**status** { **active** | **inactive** }]

undo rmon2 hlhostcontroltable [**index** *ctrl-index*]

Parameters

Parameter	Description	Value
ctrl-index	Indicates the entry index, which uniquely identifies an entry in the host control table.	The value is an integer that ranges from 1 to 65535.
datasource interface *interface-type interface-number*	Identifies an interface and a subnet, corresponding to hlHostControlDataSource. The parameter value, namely, the interface index, is the data source defining the entry. In this command, the data source is represented by interface type and number.	-
maxentry *maxentry-value*	Indicates the maximum number of entries in the host table.	The value is an integer that ranges from 1 to 100000. The default value is 50. If the host table contains too many entries, system performance is degraded. The default settings of host table are recommended.
owner *owner-name*	Indicates the owner.	The value is a string of 1 to 127 characters and cannot be empty.
status	Indicates the status of an entry in the host control table, corresponding to hlHostControlStatus.	-
active	Indicates that the hlHostControlStatus value in the host control table is active and this entry is available.	-
inactive	Indicates that the hlHostControlStatus value in the host control table is not in service and this entry is inactive and unavailable.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor traffic on the subnet connected to an interface of the managed device, run the **rmon2 hlhostcontroltable** command and specify the interface.

Precautions

When creating an entry, specify the **datasource interface** parameter to identify the interface, which specifies the subnet. The parameter value, namely, the interface index, is the data source defining the entry. Enter the interface type and number in the command. Only one entry can be created for each interface in the host control table.

The parameter **status** in the **display rmon2 hlhostcontroltable** command output matches the hlhostcontrolstatus value, which indicates the entry status.

- When the hlhostcontrolstatus value is set to **inactive**, all related entries in the host table are deleted automatically.
- When the hlhostcontrolstatus value is set to **active**, you cannot change the hlhostcontroldatasource and hlhostcontrolnlmaxdesiredentries values.
- If an interface that corresponds to the hlhostcontroldatasource in an entry is deleted, the entry is deleted at the same time.

Example

Create an entry in the host control table.

```
<HUAWEI> system-view
[HUAWEI] rmon2 hlhostcontroltable index 1 datasource interface gigabitethernet 0/0/1 maxentry 100
owner test status active
```

Set the hlHostControlStatus value in the host control table to **inactive**.

```
<HUAWEI> system-view
[HUAWEI] rmon2 hlhostcontroltable index 1 status inactive
```

16.2.17 rmon2 protocoldirtable

Function

The **rmon2 protocoldirtable** command creates or modifies an entry in the protocolDirTable.

The **undo rmon2 protocoldirtable** command deletes an entry from the protocolDirTable. If optional parameters are not specified, the entire table is deleted.

Format

rmon2 protocoldirtable protocoldirid *protocol-id* **parameter** *parameter-value* [**descr** *description-string*] [**host** { **notsupported** | **supportedon** | **supportedoff** }] [**owner** *owner-name*] [**status** { **active** | **inactive** }]

undo rmon2 protocoldirtable [**protocoldirid** *protocol-id* **parameter** *parameter-value*]

Parameters

Parameter	Description	Value
protocoldirid *protocol-id*	Indicates the protocol ID. Only IP protocol is supported currently.	The value is fixed at 8.0.0.0.1.0.0.8.0.
parameter *parameter-value*	Indicates the protocol parameter.	The value is fixed at 2.0.0.
descr *description-string*	Indicates the description of the protocol directory table.	The value is a string of 1 to 64 characters.
host { **notsupported** | **supportedon** | **supportedoff** }	Indicates the configuration of protocol directory host, corresponding to protocolDirHostConfig in the **display rmon2 protocoldirtable** command output. ● **notsupported**: Indicates that the device does not monitor the network-layer host table of the protocol, and this value cannot be changed. ● **supportedon**: Indicates that the device can monitor the network-layer host table of the protocol, and the monitoring function is enabled. ● **supportedoff**: Indicates that the device can monitor the network-layer host table of the protocol, but the monitoring function is disabled.	-
owner *owner-name*	Indicates the owner.	The value is a string of 1 to 127 characters.

Parameter	Description	Value
status { **active** | **inactive** }	Indicates the entry status, corresponding to the protocolDirStatus value in the **display rmon2 protocoldirtable** command output. ● **active**: Indicates that the protocolDirStatus value in the host control table is active and this entry is available. ● **inactive**: Indicates that the protocolDirStatus value in the host control table is not in service and this entry is inactive and unavailable.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor statistics on IP packets, run this command.

RMON2 supports only statistics on IP packets on an Ethernet interface. A protocol occupies an entry, so there is only one entry in the table.

Precautions

When running the **rmon2 protocoldirtable** command, you must set the description and protocols supported by the host. That is, the **descr** and **host** parameters are mandatory.

The parameter **status** in the **display rmon2 protocoldirtable** command output matches the protocolDirStatus value, which indicates the entry status.

- When the **status** parameter is set to **active**, the **descr** value cannot be modified. The value of **host** (corresponding to the protocolDirHostConfig value, indicating the protocol directory host configuration) can be modified. This parameter indicates whether to monitor the network-layer host table of the protocol.
  - If the **host** value is set to **notsupported**, the **host** value cannot be modified.
  - If the **host** value is not **notsupported**, the value can be switched between **supportedon** and **supportedoff**.
  - When the **host** value is changed from **supportedon** to **supportedoff**, the corresponding entry in the host control table is deleted.

- When the status is **inactive**, all related entries in the host table are deleted.

Example

Create an entry in the protocol directory table.

```
<HUAWEI> system-view
[HUAWEI] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 descr test host
supportedon owner test status active
```

Set the protocolDirStatus value in the protocol directory table to not in service.

```
<HUAWEI> system-view
[HUAWEI] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 status inactive
```

Set the protocolDirHostConfig value in the protocol directory table to supportedoff.

```
<HUAWEI> system-view
[HUAWEI] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 host supportedoff
```

16.2.18 rmon-statistics enable

Function

The **rmon-statistics enable** command enables RMON statistics function on an interface.

The **undo rmon-statistics** command disables RMON statistics function on an interface.

By default, RMON statistics function is disabled on interfaces.

Format

rmon-statistics enable

undo rmon-statistics

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Port-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the statistics function is not enabled on an interface, statistics in the statistics table and history table are 0.

Precautions

In versions earlier than V200R019C00, this command cannot be configured on Eth-Trunk member interfaces. Starting from V200R019C00, this command can be configured on Eth-Trunk member interfaces.

After the interface mode is changed from Layer 2 to Layer 3 by using the **undo portswitch** command, the device does not support the **rmon-statistics enable** command.

Example

Enable RMON statistics function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon-statistics enable
```

16.3 LLDP Configuration Commands

16.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.3.2 cdp clear neighbor

Function

The **cdp clear neighbor** command clears CDP neighbors in the system or on an interface of the device.

Format

cdp clear neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of the interface whose CDP neighbors are to be cleared. In the command: ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface. If no interface is specified, this command clears CDP neighbors on all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to obtain the latest CDP neighbor information of interfaces, use the **cdp clear neighbor** command to clear existing CDP neighbors. When an interface receives new CDP packets, new CDP neighbors are generated.

Prerequisites

The LLDP function has been enabled globally and on interfaces, and the **lldp compliance cdp receive** command has been run to enable CDP-compatible LLDP on interfaces.

Example

Clear CDP neighbors on all the interfaces.

```
<HUAWEI> cdp clear neighbor
Warning: This command will clear CDP neighbor information of all the ports. Continue? [Y/N]:y
```

16.3.3 display cdp local

Function

The **display cdp local** command displays local CDP information on a specified interface or all interfaces.

Format

display cdp local [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the CDP local information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the command displays CDP local information on all the interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check CDP information on a specified interface or all interfaces, run the **display cdp local** information.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display CDP local information on all the interfaces.

```
<HUAWEI> display cdp local
Remote Table Statistics:
-----------------------------------------------------------------------
Remote Table Last Change Time   :0 days, 23 hours, 21 minutes, 37 seconds
Remote Neighbors Added          :0
Remote Neighbors Deleted        :0
```

```
Remote Neighbors Dropped        :0
Remote Neighbors Aged           :0
Total Neighbors                 :1

Port information:
-------------------------------------------------------------------------
Interface GigabitEthernet0/0/1:
CDP Status              :enabled              (default is disabled)
Total Neighbors         :1
Interface GigabitEthernet0/0/2:
CDP Status              :enabled      (default is disabled)
Total Neighbors         :0
  ---- More ----
```

Table 16-31 Description of the **display cdp local** command output.

Item	Description
Remote Table Statistics	Statistics about CDP neighbors.
Remote Table Last Change Time	Time of the latest update of the CDP neighbor table.
Remote Neighbors Added	Number of added CDP neighbors.
Remote Neighbors Deleted	Number of deleted CDP neighbors.
Remote Neighbors Dropped	Number of CDP neighbors that are deleted because of insufficient storage memory.
Remote Neighbors Aged	Number of CDP neighbors that are deleted by the aging mechanism.
Total Neighbors	Total number of CDP neighbors.
Port information	Local CDP information on all interfaces of the switch.
Interface *x*	Local CDP information on the *x* interface.
CDP Status	Whether LLDP compatibility with CDP is enabled on the interface: ● enabled ● disabled You can run the **lldp compliance cdp receive** command to configure this parameter.
Total Neighbors	Total number of CDP neighbors on the interface.

16.3.4 display cdp neighbor

Function

The **display cdp neighbor** command displays information about CDP neighbors of all interfaces or a specified interface.

Format

display cdp neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about CDP neighbors of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the command displays information about CDP neighbors of all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command enables you to know which CDP neighbors the local device has, Layer 2 information about the neighbors, and to which interfaces the neighbors connect. You can also use this command to check whether the Layer 2 information is configured correctly on the neighbors.

Prerequisites

LLDP has been enabled globally using the **lldp enable** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display information about CDP neighbors of all the interfaces.

```
<HUAWEI> display cdp neighbor
GigabitEthernet0/0/1 has 1 neighbor(s):
```

```
Neighbor index :1
Device ID                :ME3400
Port ID                  :GigabitEthernet0/4
Version                  :SCCP75.8-3-3SR2S
Platform                 :cisco ME-3400EG-2CS-A
Capabilities             :host
MacAddress               :b4a4-e3cf-e984
Discovered time          :0 days, 22 hours, 33 minutes, 36 seconds
Expired time             :122 s
Power drawn              :12000 mw
Power request ID         :39308
Power management ID      :2
Power request levels     :12000 mw 0 mw
  ---- More ----
```

Table 16-32 Description of the **display cdp neighbor** command output

Item	Description
m has *n* neighbor(s)	The interface *m* has *n* CDP neighbors.
Neighbor index	Index of a CDP neighbor.
Device ID	ID of the CDP neighbor.
Port ID	Interface of the CDP neighbor connecting to the switch.
Version	Version of the CDP neighbor.
Platform	Software platform of the CDP neighbor.
Capabilities	Type of the CDP neighbor: ● router ● trans-bridge ● switch ● host ● igmp ● repeater ● phone ● other
MacAddress	MAC address of the CDP neighbor.
Discovered time	Time when the CDP neighbor was discovered, that is, the time difference between the system time when the device discovers the CDP neighbor and the startup time of the switch.
Expired time	The aging time remaining of CDP neighbor, in seconds.
Power drawn	Power set on the source.
Power request ID	Requested power ID.
Power management ID	ID used to manage power. The ID is the number of times the power is changed.

Item	Description
Power request levels	Requested power level. The maximum power among the negotiated power values is selected.

16.3.5 display cdp neighbor brief

Function

The **display cdp neighbor brief** command displays brief information about CDP neighbors of the device.

Format

display cdp neighbor brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to quickly view brief information about CDP neighbors connected to a switch, such as CDP neighbor names and interfaces on which CDP neighbor relationships are set up.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display brief information about CDP neighbors.

```
<HUAWEI> display cdp neighbor brief
Local Intf       Neighbor Dev             Neighbor Intf            Exptime(s)
GE0/0/1          ME3400                   GE0/0/4                  144
```

Table 16-33 Description of the **display cdp neighbor brief** command output

Item	Description
Local Intf	Local interface of the switch that sets up a CDP neighbor relationship with a peer device.
Neighbor Dev	Name of a CDP neighbor. If the name of an LLDP neighbor contains more than 24 characters, only the first 21 characters plus an ellipsis (...) are displayed. This display format cannot be changed. For example, if the name of an LLDP neighbor is **Huawei123456789123456789123456789**, this field is displayed **Huawei123456789123456...**.
Neighbor Intf	Interface of a peer device that sets up a CDP neighbor relationship with the switch.
Exptime(s)	Time left before a CDP neighbor relationship expires, in seconds.

16.3.6 display cdp neighbor device-id

Function

The **display cdp neighbor device-id** command displays the name of a CDP neighbor.

Format

display cdp neighbor device-id

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the name of a CDP neighbor contains more than 24 characters, the **display cdp neighbor brief** command cannot display the complete name of the CDP neighbor. In this case, run the **display cdp neighbor device-id** command instead.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display the name of a CDP neighbor.

```
<HUAWEI> display cdp neighbor device-id
Local Interface  Neighbor Interface  Neighbor Device
GE0/0/3          GE0/0/1             Edge1i-11111111111111111111111111111111111111111111
```

Table 16-34 Description of the **display cdp neighbor device-id** command output

Item	Description
Local Interface	Local interface of the switch that sets up a CDP neighbor relationship with a peer device.
Neighbor Interface	Interface of a peer device that sets up a CDP neighbor relationship with the switch.
Neighbor Device	Name of a CDP neighbor. A maximum of 255 characters can be displayed in this field.

16.3.7 display cdp statistics

Function

The **display cdp statistics** command displays statistics about CDP packets received.

Format

display cdp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about CDP packets received by a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, the command displays statistics about CDP packets received by all the interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When you need to locate an LLDP fault on a switch according to statistics about CDP packets received, run the **display cdp statistics** command.

NOTE

To check statistics about CDP packets received in a specified period of time, run the **reset cdp statistics** command to clear the historical CDP packet statistics. Wait for the specified period of time, and then run the **display cdp statistics** command to check the new CDP packet statistics.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display statistics about CDP packets received by all interfaces.

```
<HUAWEI> display cdp statistics
CDP statistics global Information:
Statistics for GigabitEthernet0/0/1:
Total frames received:    30
Total frames discarded:   0
Total frames error:       0
Last cleared time:        never
  ---- More ----
```

Table 16-35 Description of the **display cdp statistics** command output

Item	Description
CDP statistics global Information	Statistics about CDP packets received by the switch.
Statistics for *x*	Statistics about CDP packets received by the *x* interface.
Total frames received	Number of received CDP packets by this interface.
Total frames discarded	Number of discarded CDP packets by this interface.
Total frames error	Number of received CDP error packets by this interface.

Item	Description
Last cleared Time	Time when the statistics about CDP packets received on this interface are cleared last time: ● If the statistics about CDP packets on this interface have been cleared, the time is displayed. ● If the statistics about CDP packets on this interface have never been cleared, **never** is displayed.

16.3.8 display lldp device-classifier information

Function

The **display lldp device-classifier information** command displays LLDP neighbor information on a switch.

Format

display lldp device-classifier information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a switch has multiple types of LLDP neighbors and needs to deliver different configurations to different types of LLDP neighbors, configure the Python script in advance and run the **lldp device-classifier enable** command to enable the switch to automatically execute the Python script after the LLDP neighbor changes. If the switch detects that a specified type of LLDP neighbor is added or deleted on an interface, the switch automatically delivers the predefined configuration in the Python script, reducing the configuration workload. You can run the **display lldp device-classifier information** command to view LLDP neighbor information on the switch, including the LLDP neighbor type.

Prerequisites

The **lldp device-classifier enable** command has been executed to enable the switch to automatically execute the Python script after the LLDP neighbor changes.

Example

Display LLDP neighbor information on a switch.

```
<HUAWEI> display lldp device-classifier information
Capability codes:
    (T) Telephone, (B) Bridge, (R) Router
    (W) WLAN Access Point, (O) Other

Local Intf    Trigger Source    Capability        Exptime(s)
GE0/0/1       LLDP Packet       B,R               149
GE0/0/2       LLDP Packet       B,R               120
```

Table 16-36 Description of the **display lldp device-classifier information** command output

Item	Description
Capability codes/Capability	LLDP neighbor type: - (T) Telephone: IP phone - (B) Bridge: switch - (R) Router: router - (W) WLAN Access Point: AP - (O) Other: others
Local Intf	Interface of the switch that detects the LLDP
Trigger Source	Method used by the switch to detect the LLDP neighbor - LLDP Packet: through LLDP packets. - CDP Packet: through CDP packets. The **lldp compliance cdp receive** command must have been executed to enable CDP-compatible LLDP on the interface.
Exptime(s)	Remaining time of the LLDP neighbor on the switch, in seconds

16.3.9 display lldp local

Function

The **display lldp local** command displays the global LLDP information or the LLDP information on a specified interface.

Format

display lldp local [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the LLDP information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays LLDP information on all the interfaces with LLDP enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp local** command displays the global LLDP information or the LLDP information on an interface.

- The global LLDP information includes system information, MED system information, system configuration, and data statistics on the peer device.
- The LLDP information on an interface includes the interface information and MED interface information.

To verify the LLDP information and Layer 2 information of the system and interfaces, run this command.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display the global LLDP information, S5735-S24T4X is used as an example.

```
<HUAWEI> display lldp local
System information
-----------------------------------------------------------------------
Chassis type   :MAC address
Chassis ID     :00e0-11fc-1710
System name    :HUAWEI
```

```
System description  :Huawei Switch S5735-S24T4X
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5720 V200R023C00)
Copyright (C) 2000-2019 HUAWEI TECH Co., Ltd.
System capabilities supported   :bridge router
System capabilities enabled     :bridge router
LLDP Up time   :2023-02-28 11:53:20

MED system information
---------------------------------------------------------------------------
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :VER.B
FirmwareRev       :NA
SoftwareRev       :Version 5.170 V200R023C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
---------------------------------------------------------------------------
LLDP Status                     :enabled            (default is enabled)
LLDP Message Tx Interval        :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                  (default is 4)
LLDP Refresh Delay              :2                  (default is 2s)
LLDP Tx Delay                   :2                  (default is 2s)
LLDP Notification Interval      :5                  (default is 5s)
LLDP Notification Enable        :enabled            (default is enabled)
Management Address              :IP:10.10.10.1  MAC:000b-09e6-3da1

Remote Table Statistics:
---------------------------------------------------------------------------
Remote Table Last Change Time   :0 days, 0 hours, 4 minutes, 15
seconds
Remote Neighbors Added          :5
Remote Neighbors Deleted        :0
Remote Neighbors Dropped        :0
Remote Neighbors Aged           :0
Total Neighbors                 :5

Port information:
---------------------------------------------------------------------------
Interface GigabitEthernet0/0/1:
LLDP Enable Status       :enabled            (default is enabled)
Total Neighbors          :1

Port ID subtype     :Interface name
Port ID             :GigabitEthernet0/0/1
Port description    :GigabitEthernet0/0/1

Port and protocol VLAN ID(PPVID)   :0
Port and protocol VLAN supported   :No
Port and protocol VLAN enabled     :No
Port VLAN ID(PVID)  :1
VLAN name of VLAN 1:VLAN 0001
VLAN name of VLAN 3:VLAN 0003
VLAN name of VLAN 4:VLAN 0004
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class          :PD
PSE power supported       :No
PSE power enabled         :No
PSE pairs control ability:No
Power pairs               :Unknown
```

```
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :1526

EEE support              :Yes
Transmit Tw              :16
Receive Tw               :16
Fallback Receive Tw      :65535
Echo Transmit Tw         :16
Echo Receive Tw          :16

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID           :0
Media policy L2 priority      :0
Media policy Dscp             :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0.2(w)

  ---- More ----
```

Table 16-37 Description of the **display lldp local** command output.

Item	Description
System information	Global LLDP information.
Chassis type	Type of the Device ID: ● Chassis component: chassis alias ● Interface alias: interface alias ● Port component: interface or backplane alias ● MAC address: MAC address ● Network address: network address ● Interface name: name of the interface ● Locally assigned: name of the local device
Chassis ID	Device ID.
System name	Name of the device.
System description	Description of the device.
Huawei Versatile Routing Platform Software	-
VRP (R) software, Version	Versions of the VRP and the software of the device.
Copyright (C) 2000-2013 HUAWEI TECH Co., Ltd.	Huawei copyright.

Item	Description
System capabilities supported	Capabilities supported of the local device, including: ● bridge: bridge device ● router: router
System capabilities enabled	Capabilities enabled on the local device.
LLDP Up time	Time when LLDP is enabled.
MED system information	MED TLV information of the device.
Device class	Type of the device.
MED inventory information of master board	-
HardwareRev	Hardware version of the device.
FirmwareRev	Firmware version of the device.
SoftwareRev	Software version of the device.
SerialNum	Serial number of the device. **NOTE** If the decimal value of a serial number is not in the range of 32 to 126, the serial number is displayed in octal notation.
Manufacturer name	Name of the manufacturer.
Model name	Name of a model.
Asset tracking identifier	Asset tracking ID.
System configuration	Global LLDP configuration.
LLDP Status	Whether LLDP is enabled globally on the switch: ● Enabled ● Disabled You can run the **lldp enable (system view)** command to configure this parameter.
default is *x*	Default value *x*.
LLDP Message Tx Interval	Interval for sending LLDP packets of the device, in seconds. You can run the **lldp message-transmission interval** command to configure this parameter.

Item	Description
LLDP Message Tx Hold Multiplier	Hold time multiplier of local device information stored on neighbors. You can run the **lldp message-transmission hold-multiplier** command to configure this parameter.
LLDP Refresh Delay	Delay in re-enabling the LLDP function on the switch, in seconds. You can run the **lldp restart-delay** command to configure this parameter.
LLDP Tx Delay	Delay in sending LLDP packets on the switch, in seconds. You can run the **lldp message-transmission delay** command to configure this parameter.
LLDP Notification Interval	Delay in sending the neighbor change traps to the NMS on the switch, in seconds. You can run the **lldp trap-interval** command to configure this parameter.
LLDP Notification Enable	Whether the function of sending LLDP traps to the NMS is enabled on the switch: ● enabled ● disabled You can run the **snmp-agent trap enable feature-name lldptrap** command to configure this parameter.
Management Address	LLDP management address of the switch. You can run the **lldp management-address** command to configure this parameter. If an invalid management address is used, the inactive field is added for this address. For example, if 10.1.1.1 is an invalid management address, the displayed information is as follows: Management Address :IP:10.10.10.1, 10.1.1.1 (inactive) MAC: 000b-09e6-3da1
Remote Table Statistics	Statistics about LLDP neighbors.
Remote Table Last Change Time	Time that elapsed since the latest modification of remote data.
Remote Neighbors Added	Number of added LLDP neighbors.
Remote Neighbors Deleted	Number of deleted LLDP neighbors.
Remote Neighbors Dropped	Number of devices that do not set up LLDP neighbor relationships because the number of neighbors has reached the maximum value.

Item	Description
Remote Neighbors Aged	Number of LLDP neighbors that are aged out and deleted.
Total Neighbors	Number of LLDP neighbors.
Port information	LLDP information on the interface.
LLDP Enable Status	Whether LLDP is enabled on the interface: ● Enabled ● Disabled You can run the **lldp enable (system view)** and **lldp enable (interface view)** commands to configure this parameter.
Total Neighbors	Number of LLDP neighbors on the interface.
Port ID subtype	Type of the interface ID. ● Interface alias: interface alias ● Port component: interface or backplane alias ● MAC address: MAC address ● Network address: network address ● Interface name: name of the interface ● Agent circuit ID: circuit ID of the DHCP agent ● Locally assigned: name of the local device
Port ID	Interface ID.
Port description	Interface description.
Port and protocol VLAN ID(PPVID)	Protocol VLAN ID of a port.
Port and protocol VLAN supported	Whether PPVID is supported: ● Yes: PPVID is supported. ● No: PPVID is not supported.
Port and protocol VLAN enabled	Whether PPVID is enabled: ● Yes: PPVID is enabled. ● No: PPVID is disabled.
Port VLAN ID(PVID)	The default VLAN ID of the interface.
VLAN name of VLAN 1 VLAN name of VLAN 3 VLAN name of VLAN 4	Name of a VLAN to be advertised, which is configured using the **lldp tlv-enable dot1-tlv** command. If no VLAN name is specified, the default VLAN name is advertised and displayed.
Protocol identity	Protocol ID.

Item	Description
Auto-negotiation supported	Whether the interface supports auto-negotiation: - Yes - No
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: - Yes - No You can run the **negotiation auto** command to configure this parameter.
OperMau	Rate and duplex mode of the interface.
Power port class	PoE type of the interface: - PSE: power-sourcing equipment - PD: powered device
PSE power supported	Whether the PSE power is supported. - Yes: PSE power is supported. - No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. - Yes: enabled - No: disabled
PSE pairs control ability	Whether the PSE twisted pair control is supported. - Yes: PSE twisted pair control is supported. - No: PSE twisted pair control is not supported.
Power pairs	PoE remote power supply mode. - Signal: power supply mode of signal lines - Spare: power supply mode of spare signal lines - Unknown: an unknown remote power supply mode
Port power classification	PD power control level on the interface: - Class0: indicates level 1. - Class1: indicates level 2. - Class2: indicates level 3. - Class3: indicates level 4. - Class4: indicates level 5. - Unknown: indicates an unknown level.

Item	Description
Link aggregation supported	Whether the interface supports link aggregation. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Link aggregation enabled	Whether link aggregation is enabled on the interface. ● Yes: enabled ● No: disabled
Aggregation port ID	ID of an aggregated interface, If link aggregation is disabled, the value of this field is 0.
Maximum frame Size	Maximum size of a frame supported by the interface. You can run the **jumboframe enable** command to configure this parameter.
EEE support	Whether the interface supports energy efficient Ethernet (EEE): ● Yes ● No
Transmit Tw	Amount of time the sender waits before starting sending data after leaving lower power consumption mode (LPI mode).
Receive Tw	Amount of time the receiver expects the sender to wait before starting sending data after leaving LPI mode.
Fallback Receive Tw	Additional information provided to the sender.
Echo Transmit Tw	Transmit Tw value specified in the Echo message sent from the remote end.
Echo Receive Tw	Receive Tw value specified in the Echo message sent from the remote end.
MED port information	-

Item	Description
Media policy type	Type of the media policy: ● Voice ● Voice Signaling ● Guest Voice ● Guest Voice Signaling ● Softphone Voice ● Video Conferencing ● Streaming Video ● Video Signaling ● Unknown
Unknown Policy	Whether the type of the media policy is unknown: ● Yes: unknown ● Defined: known ● Unknown indicates that the Media policy VlanID, Media policy L2 priority and Media policy Dscp value fields are ignored.
VLAN tagged	Whether to add tag to the packets of the voice VLAN: ● Yes: Adds a VLAN tag to packets of the voice VLAN. ● No: Not to add a VLAN tag to packets of the voice VLAN.
Media policy VlanID	ID of the voice VLAN.
Media policy L2 priority	802.1p priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type: ● PSE: power-sourcing equipment ● PD: powered device ● Unknown: an unknown power supply type Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.
PoE PSE power source	Type of the PSE: ● Primary: indicates primary power supply. ● Backup: indicates backup power supply. ● Unknown: indicates an unknown type of PSE. Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.

Item	Description
Port PSE Priority	PSE priority of an interface: - Unknown: indicates an unknown priority. - Critical: indicates the highest priority. - High: indicates the medium priority. - Low: indicates the lowest priority. Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.
Port Available power value	Port power supply. Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.

16.3.10 display lldp neighbor

Function

The **display lldp neighbor** command displays information about neighboring device of all interfaces or a specified interface.

Format

display lldp neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about neighboring devices of a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If no interface is specified, the command displays information about neighboring devices of all interfaces with LLDP enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Using this command, you can know which neighboring devices are connected to the local device, to which interfaces the neighboring devices are connected, layer 2 information about the neighbors, and whether LLDP configuration is correct.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display information about neighbor devices of interfaces GigabitEthernet0/0/1. (The neighbor is a switch.)

```
<HUAWEI> display lldp neighbor interface gigabitethernet0/0/1
GigabitEthernet0/0/1 has 1 neighbor(s):

Neighbor index : 1
Chassis type   :MAC address
Chassis ID     :00e0-11fc-1710
Port ID type   :Interface name
Port ID        :GigabitEthernet0/0/1
Port description    :GigabitEthernet0/0/1
System name         :HUAWEI
System description  :S5735-S24T4X
Huawei Versatile Routing Platform Software
VRP (R) software,Version 5.160 (S5720 V200R023C00)
Copyright (C) 2000-2019 HUAWEI TECH CO., LTD
System capabilities supported   :bridge router
System capabilities enabled     :bridge router
Management address type  :ipv4
Management address value : 127.0.0.1
OID  :0.6.15.43.6.1.4.1.2011.5.25.41.1.2.1.1.1.
Expired time   :104s

Device 0 infomation:
  Device serial number :21980115830123456789
  Device model name    :S5735-S24T4X
Device 1 infomation:
  Device serial number :21980115790123456789
  Device model name    :S5735-S24T4X
Port VLAN ID(PVID)  :1
Port and protocol VLAN ID(PPVID)   :0
Port and protocol VLAN supported   :No
Port and protocol VLAN enabled     :No
VLAN name of VLAN  1: VLAN 0001
Protocol identity   :

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)
```

```
Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown
Power type                 :Type 2 PD
Power source                :PSE
Power priority              :Low
PD requested power value    :60.0(w)
PSE allocated power value   :60.0(w)
PD requested power mode A value  :30.0(w)
PD requested power mode B value  :30.0(w)
Power class                      :6
Power typex                      :Type 3 PSE
PSE allocated power mode A value :0.0(w)
PSE allocated power mode B value :0.0(w)
PSE maximum available power      :0.0(w)
PSE power pairsx                 :Unknown
PSE Autoclass support            :PSE does not supports Autoclass
PD 4PID                          :PD does not supports powering of both Modes
PD Load                          :PD is single-signature or dual-signature and power demand on Mode A and
Mode B are not electrically isolated
Autoclass completed              :Autoclass idle
Autoclass request                :Autoclass idle
Power down                       :Not power down
Power capability                 :AF AT BT_60 BT_90
Power-up mode                    :AT

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

EEE support              :Yes
Transmit Tw              :16
Receive Tw               :16
Fallback Receive Tw      :65535
Echo Transmit Tw         :16
Echo Receive Tw          :16

MED Device information
Device class   :Network Connectivity

HardwareRev       :LE02MCUA VER.AVER.BVER.A
FirmwareRev       :151NA
SoftwareRev       :Version 5.160 V200R023C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID      :0
Media policy L2 priority :6
Media policy Dscp        :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0.2(w)
```

Display information about neighbor devices of interfaces GigabitEthernet0/0/2. (The neighbor is an AP.)

```
<HUAWEI> display lldp neighbor interface gigabitethernet0/0/2
GigabitEthernet0/0/2 has 1 neighbor(s):
```

```
Neighbor index :1
Chassis type   :MAC address
Chassis ID     :00e0-11fc-8670
Port ID type   :Interface name
Port ID        :MultiGE0/0/1
Port description    :HUAWEI, AP Series, MultiGE0/0/1
Interface
System name         :e483-2696-8670
System description  :Huawei AP AirEngine8760-X1-PRO
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AirEngine8760-X1-PRO V200R022C10SPC100)
Copyright (C) 2011-2020 Huawei Technologies
Co.,Ltd

System capabilities supported   :wlanAccessPoint
System capabilities enabled     :wlanAccessPoint
Management address type  :ipv4
Management address value :169.254.1.1
OID  :0.6.15.43.6.1.4.1.2011.5.25.41.1.2.1.1.1.
Expired time   :105s

Device 0 infomation:
  Device serial number :
2102353GSG10LB000165
  Device model name    :AirEngine8760-X1-PRO

Port VLAN ID(PVID)  :1
VLAN name of VLAN  1:VLAN1

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class            :PD
PSE power supported         :No
PSE power enabled           :No
PSE pairs control ability   :No
Power pairs                 :Spare
Port power classification   :Class7
Power type                  :Type 2 PD
Power source                :PSE
Power priority              :Low
PD requested power value    :71.3(w)
PSE allocated power value   :71.3(w)
PD requested power mode A value  :35.6(w)
PD requested power mode B value  :35.6(w)
Power class                      :0
Power typex                      :Type 4 dual-signature PD
PSE allocated power mode A value :0.0(w)
PSE allocated power mode B value :0.0(w)
PSE maximum available power      :0.0(w)
PSE power pairsx                 :Unknown
PSE power status                 :Unknown
PD power status                  :Powered single-signature PD
Dual-signature power class mode A:Single-signature PD or 2-pair only
PSE
Dual-signature power class mode B:Single-signature PD or 2-pair only
PSE
PSE Autoclass support            :PSE does not supports
Autoclass
PD 4PID                          :PD supports powering of both Modes
PD Load                          :PD is single-signature or dual-signature and power demand on Mode A and
Mode B are not electricall
y isolated
Autoclass completed              :Autoclass idle
Autoclass request                :Autoclass idle
Power down request               :YES
Power down timer                 :1s
```

```
Power capability           :AT BT_60 BT_90
Power-up mode               :BT_90

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0

Maximum frame Size       :1800
```

Table 16-38 Description of the **display lldp neighbor** command output

Item	Description
Neighbor index	Index of a neighbor.
Chassis type	ID sub-types of a neighboring device: ● Chassis component: chassis alias ● Interface alias: interface alias ● Port component: interface or backplane alias ● MAC address: MAC address ● Network address: network address ● Interface name: name of the interface ● Locally assigned: name of the local device
Chassis Id	ID of a neighboring device.
Port ID type	ID sub-type of a neighboring interface: ● Interface alias: interface alias ● Port component: interface or backplane alias ● MAC address: MAC address ● Network address: network address ● Interface name: name of the interface ● Agent circuit ID: circuit ID of the DHCP agent ● Locally assigned: name of the local device
Port Id	ID of a neighbor interface.
Port description	Description of a neighboring interface.
System name	System name of a neighboring device.
System description	Description of a neighboring device.

Item	Description
System capabilities supported	Capabilities of a neighboring device (at least one capability is supported): ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station
System capabilities enabled	Capabilities enabled on a neighboring device (This field is a subset of the system capabilities supported field, and at least one capability must be enabled). ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point (AP) ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station
Management address type	Neighbor management address type of a neighbor.
Management address value	Neighbor management address of a neighbor.
OID	Neighbor management address OID.
Expired time	Aging time of a neighbor.
Device 0 infomation Device 1 infomation	Neighbor device information. This field is displayed only when there are multiple neighbors.
Device serial number	Serial number of a neighbor.
Device model name	Model of a neighbor.
Port VLAN ID(PVID)	VLAN ID of an interface.
Port and protocol VLAN ID(PPVID)	Protocol VLAN ID of a port.

Item	Description
Port and protocol VLAN supported	Whether PPVID is supported: - Yes: PPVID is supported. - No: PPVID is not supported.
Port and protocol VLAN enabled	Whether PPVID is enabled: - Yes: PPVID is enabled. - No: PPVID is disabled.
VLAN name of VLAN 1	Name of VLAN 1.
Protocol identity	Protocol ID.
Auto-negotiation supported	Whether the interface supports auto-negotiation: - Yes: Auto-negotiation is supported. - No: Auto-negotiation is not supported.
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: - Yes: enabled. - No: disabled.
OperMau	Transmission rate and duplex mode of the interface.
Power port class	PoE type: - PSE: power-sourcing equipment. - PD: powered device.
PSE power supported	Whether the PSE power is supported. - Yes: PSE power is supported. - No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. - Yes: enabled. - No: disabled.
PSE pairs control ability	Whether the PSE control is supported. - Yes: PSE control is supported. - No: PSE control is not supported.
Power pairs	PoE remote power supply mode. - Signal: power supply mode of signal lines. - Spare: power supply mode of spare signal lines. - Unknown: an unknown remote power supply mode.

Item	Description
Port power classification	PD power control level on the interface: - Class0: indicates level 1. - Class1: indicates level 2. - Class2: indicates level 3. - Class3: indicates level 4. - Class4: indicates level 5. - Class5: indicates level 6. - Class6: indicates level 7. - Class7: indicates level 8. - Unknown: indicates an unknown control level.
Power type	The power supply type: - Type 1 PD: indicates the PD that does not support IEEE 802.3at. - Type 1 PSE: indicates the PSE that does not support IEEE 802.3at. - Type 2 PD: indicates the PD that supports IEEE 802.3at. - Type 2 PSE: indicates the PSE that supports IEEE 802.3at.
Power source	The power supply source.
Power priority	The power supply priority of an interface: - low - high - Critical - unknown
PD requested power value	Power requested by the PD.
PSE allocated power value	Power allocated by the PSE to the PD.
PD requested power mode A value	Power in alternative A mode requested by the PD.
PD requested power mode B value	Power in alternative B mode requested by the PD.
Power class	- When the power type is PD this field shall be set to the requested Class of the PD. - When the power type is PSE this field shall be set to the PSEs assigned Class.

Item	Description
Power typex	- Type 1 PSE - Type 1 PD - Type 2 PSE - Type 2 PD - Type 3 PSE - Type 3 single-signature PD - Type 4 PSE - Type 4 PD - Type 4 single-signature PD - Type 3 dual-signature PD - Type 4 dual-signature PD
PSE power status	- 2-pair powering - 4-pair powering single-signature PD - 4-pair powering dual-signature PD - Unknown
PD power status	- Powered single-signature PD - 2-pair powered dual-signature PD - 4-pair powered dual-signature PD - Unknown
Dual-signature power class mode A	- Class1 - Class2 - Class3 - Class4 - Class5 - Single-signature PD or 2-pair only PSE - Unknown
Dual-signature power class mode B	- Class1 - Class2 - Class3 - Class4 - Class5 - Single-signature PD or 2-pair only PSE - Unknown
PSE allocated power mode A value	Power allocated by the PSE to the PD in alternative A mode.
PSE allocated power mode B value	Power allocated by the PSE to the PD in alternative B mode.

Item	Description
PSE maximum available power	The highest power the PSE can grant to the PD.
PSE power pairsx	The power supply modes that the PSE supports: ● Alternative A ● Alternative B ● Alternative A and Alternative B ● Unknown
PSE Autoclass support	Whether PSE supports Autoclass: ● PSE supports Autoclass ● PSE does not support Autoclass
PD 4PID	● PD supports powering of both Modes ● PD does not support powering of both Modes
PD Load	● PD is dual-signature and power demand on Mode A and Mode B are electrically isolated ● PD is single-signature or dual-signature and power demand on Mode A and Mode B are not electrically isolated
Autoclass completed	Whether Autoclass is completed: ● Autoclass measurement completed ● Autoclass idle
Autoclass request	Whether the interface has received Autoclass request: ● PD requests Autoclass measurement ● Autoclass idle
Power down	Whether the interface powers down.
Power down request	Whether the interface sends a power-off request. ● YES ● NO
Power down timer	Time when the interface stops supplying power. This field is displayed only when **Power down request** is **YES**.
Power capability	Power supply mode supported by the PD: ● AF: 802.3af ● AT: 802.3at ● BT_60: 802.3bt with the 60 W supply power ● BT_90: 802.3bt with the 90 W supply power

Item	Description
Power-up mode	Power supply mode used by the PD. The setting **--** indicates that the PD does not notify the switch of the power supply mode in use.
Link aggregation supported	Whether link aggregation is supported on the interface. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Link aggregation enabled	Whether link aggregation is enabled on an interface. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Aggregation port ID	ID of an aggregated interface, If link aggregation is disabled, the value of this field is 0.
Maximum frame Size	Maximum size of a frame supported by the interface.
EEE support	Whether the interface supports energy efficient Ethernet (EEE).
Transmit Tw	Amount of time the sender waits before starting sending data after leaving lower power consumption mode (LPI mode).
Receive Tw	Amount of time the receiver expects the sender to wait before starting sending data after leaving LPI mode.
Fallback Receive Tw	Additional information provided to the sender.
Echo Transmit Tw	Transmit Tw value specified in the Echo message sent from the remote end.
Echo Receive Tw	Receive Tw value specified in the Echo message sent from the remote end.
Device class	Type of the MED device.
HardwareRev	Hardware version of the device.
FirmwareRev	Firmware version of the device.
SoftwareRev	Software version of the device.
SerialNum	Serial number of the device. **NOTE** If the decimal value of a serial number is not in the range of 32 to 126, the serial number is displayed in octal notation.

Item	Description
Manufacturer name	Name of the manufacturer.
Model name	Name of a model.
Asset tracking identifier	Asset tracking ID.
Media policy type	Type of the media policy: ● Voice. ● Voice Signaling. ● Guest Voice. ● Guest Voice Signaling. ● Softphone Voice. ● Video Conferencing. ● Streaming Video. ● Video Signaling. ● unknown indicates that the type of the media policy is unknown.
Unknown Policy	Whether the type of the media policy is unknown: ● Yes: unknown ● Defined: known ● Unknown indicates that the Media policy VlanID, Media policy L2 priority and Media policy Dscp value fields are ignored.
VLAN tagged	Whether to add tag to the packets of the voice VLAN: ● Yes: Adds a VLAN tag to packets of the voice VLAN. ● No: Not to add a VLAN tag to packets of the voice VLAN.
Media policy VlanID	ID of the voice VLAN.
Media policy L2 priority	802.1p priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type: ● PSE: power-sourcing equipment. ● PD: powered device. ● Unknown: indicates an unknown power supply type.

Item	Description
PoE PSE power source	Type of the PSE: ● Primary: indicates primary power supply. ● Backup: indicates backup power supply. ● Unknown: indicates an unknown type of PSE.
Port PSE Priority	PSE priority of an interface: ● Unknown: indicates an unknown priority. ● Critical: indicates the highest priority. ● High: indicates the medium priority. ● Low: indicates the lowest priority.
Port Available power value	Port power supply

16.3.11 display lldp neighbor brief

Function

The **display lldp neighbor brief** command displays brief information about neighbors of the device.

Format

display lldp neighbor brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To quickly view brief information about the LLDP neighbors of a switch and the interfaces connected to neighbors, run this command.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.

2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display brief information about LLDP neighbors of the switch.

```
<HUAWEI> display lldp neighbor brief
Local Intf   Neighbor Dev             Neighbor Intf            Exptime(s)
GE0/0/1      Huawei                  GE0/0/1                  103
```

Table 16-39 Description of the **display lldp neighbor brief** command output

Item	Description
Local Intf	Local interface on which the LLDP neighbor relationship is established with a peer device.
Neighbor Dev	Name of an LLDP neighbor. If the name of an LLDP neighbor contains more than 24 characters, only the first 21 characters plus an ellipsis (...) are displayed. This display format cannot be changed. For example, if the name of an LLDP neighbor is **Huawei123456789123456789123456789**, this field is displayed **Huawei123456789123456...**. To view the complete neighbor name, run the **display lldp neighbor system-name** command.
Neighbor Intf	Interface of a peer device on which the LLDP neighbor relationship is established.
Exptime	Time left before an LLDP neighbor relationship expires, in seconds.

16.3.12 display lldp neighbor system-name

Function

The **display lldp neighbor system-name** command displays the name of an LLDP neighbor.

Format

display lldp neighbor system-name

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the name of an LLDP neighbor contains more than 24 characters, the **display lldp neighbor brief** command cannot display the complete name of the LLDP neighbor. In this case, run the **display lldp neighbor system-name** command instead.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display the name of an LLDP neighbor.

```
<HUAWEI> display lldp neighbor system-name
Local Interface  Neighbor Interface  Neighbor Device
GE0/0/3         GE0/0/1           Edge1i-11111111111111111111111111111111111111111111
```

Table 16-40 Description of the **display lldp neighbor system-name** command output

Item	Description
Local Interface	Local interface on which the LLDP neighbor relationship is established with a peer device.
Neighbor Interface	Interface of a peer device on which the LLDP neighbor relationship is established.
Neighbor Dev	Name of an LLDP neighbor. A maximum of 255 characters can be displayed in this field.

16.3.13 display lldp statistics

Function

The **display lldp statistics** command displays statistics about LLDP packets sent and received by all or a specified interface.

Format

display lldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type* *interface-number*	Displays statistics about LLDP packet sent and received by a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays statistics about LLDP packets on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To display the LLDP packet statistics within a specified period of time, run the **reset lldp statistics** command to clear the existing statistics first, and then run the **display lldp statistics** command to display the new statistics.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

When you query statistics about all interfaces, no information about LLDP-disabled interfaces is displayed. When you query statistics about an LDDP-disabled interface, the system displays a message indicating that LLDP is not enabled on this interface.

Example

Display the statistics about LLDP packets sent and received by all interfaces.

```
<HUAWEI> display lldp statistics
LLDP statistics global Information:
```

```
Statistics for GigabitEthernet0/0/1:
Transmitted Frames Total: 2839
Received Frames Total:    2728      Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0
```

Table 16-41 Description of the **display lldp statistics** command output

Item	Description
LLDP statistics global Information	Statistics about LLDP packets.
Statistics for *x*	Statistics about LLDP packets received and sent by the *x* interface.
Transmitted Frames Total	Number of sent LLDP packets.
Received Frames Total	Number of received LLDP packets.
Frames Discarded Total	Number of discarded LLDP packets.
Frames Error Total	Number of received errored LLDP packets.
TLVs Discarded Total	Number of discarded TLVs.
TLVs Unrecognized Total	Number of unknown TLVs.
Neighbors Expired Total	Number of aged-out neighbors.

16.3.14 display lldp tlv-config

Function

The **display lldp tlv-config** command displays optional TLVs that can be sent with LLDP packets on all or a specified interface.

Format

display lldp tlv-config [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays optional TLVs supported by a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number. If no interface is specified, the command displays optional TLVs on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp tlv-config** command displays the TLVs supported by the specified interface or all interfaces, and thus you can know whether the required TLVs are enabled and unneeded TLVs are disabled.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display Optional TLVs that can be sent with LLDP packets on GigabitEthernet0/0/1.

```
<HUAWEI> display lldp tlv-config interface gigabitethernet 0/0/1

LLDP tlv-config of port [GigabitEthernet0/0/1]:
-----------------------------------------------------
Name                          Status    Default
-----------------------------------------------------

Basic optional TLV:
-----------------------------------
Port Description TLV              Yes       Yes
```

```
System Name TLV                  Yes       Yes
System Description TLV           Yes       Yes
System Capabilities TLV          Yes       Yes
Management Address TLV           Yes       Yes

IEEE 802.1 extend TLV:
----------------------------------
Port VLAN ID TLV                 Yes       Yes
Port And Protocol VLAN ID TLV    Yes       Yes
VLAN Name TLV                    Yes       Yes
Protocol Identity TLV            No        No

IEEE 802.3 extend TLV:
----------------------------------
MAC-Physic TLV                   Yes       Yes
Power Via MDI TLV                Yes       Yes
Link Aggregation TLV             Yes       Yes
Maximum Frame Size TLV           Yes       Yes
EEE TLV                          Yes       Yes

LLDP-MED extend TLV:
----------------------------------
Capabilities TLV                 Yes       Yes
Extended Power Via MDI TLV       Yes       Yes
Inventory TLV                    Yes       Yes
Network Policy TLV               Yes       Yes
Location Identification TLV      No        No

LLDP Legacy config TLV:
----------------------------------
Poe TLV                          Yes       Yes
Device Sn And Model TLV          Yes       Yes
Pnp TLV                          Yes       Yes
----------------------------------
   Start Vlanid TLV              Yes       Yes
   Link Aggregation TLV          Yes       Yes
   Device Type TLV               Yes       Yes
```

Table 16-42 Description of the **display lldp tlv-config** command output

Item	Description
Name	Type of TLV.
Status	Whether the interface is configured to send the TLVs of the specified type.
Default	Whether the TLVs of the specified types are sent on an interface by default.
Basic optional TLV	Basic TLVs that can be sent on an interface.
Port Description TLV	Interface description TLV.
System Name TLV	System name TLV.
System Description TLV	System description TLV.
System Capabilities TLV	TLV indicating the system capability set.
Management Address TLV	Management address TLV.

Item	Description
IEEE 802.1 extend TLV	Type of the IEEE 802.1 organizational-specific TLVs that can be sent on an interface.
Port VLAN ID TLV	PVID TLV.
Port And Protocol VLAN ID TLV	Port and protocol VLAN ID TLV.
VLAN Name TLV	VLAN name TLV.
Protocol Identity TLV	Protocol ID TLV.
IEEE 802.3 extend TLV	IEEE 802.3 organizational-specific TLVs that can be sent on an interface.
MAC-Physic TLV	TLV indicating physical attributes of an interface.
Power Via MDI TLV	Power capability TLV.
Link Aggregation TLV	Link aggregation TLV.
Maximum Frame Size TLV	Maximum frame length TLV.
LLDP-MED extend TLV	LLDP MED TLV.
Capabilities TLV	TLV indicating MED capability sets.
Extended Power Via MDI TLV	TLV indicating the extended power supply capabilities.
Inventory TLV	Inventory information, including Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model name TLV, and Asset id TLV.
Network Policy TLV	Network policy TLV.
Location Identification TLV	Location ID TLV.
EEE TLV	EEE capability TLV.
LLDP Legacy config TLV	Legacy TLV configuration.
Poe TLV	PoE power TLV.
Device Sn And Model TLV	Device SN and model TLV.
Pnp TLV	PnP TLV.
Start Vlanid TLV	Initial VLAN TLV.
Link Aggregation TLV	Link aggregation TLV.
Device Type TLV	Device type TLV.

16.3.15 ip domain-name

Function

The **ip domain-name** command adds a suffix to a device name.

The **undo ip domain-name** command deletes the suffix of a device name.

By default, a device name does not have a suffix.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support this command.

Format

ip domain-name *domain-name*

undo ip domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the suffix of a device name.	The value is a string of 1 to 255 characters without spaces. It contains digits, letters, hyphens (-), underscores (_), and dots (.).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device name and a suffix form a fully qualified domain name (FQDN). If you need to add a suffix to a device name, run the **ip domain-name** command. In this situation, the System Name TLV in an LLDP packet is in "device name.suffix" format. For example, if the device name is **HUAWEI** and suffix is **area1**, the System Name TLV in an LLDP packet is **HUAWEI.area1**.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Set the device name suffix to **area1**.

```
<HUAWEI> system-view
[HUAWEI] ip domain-name area1
```

16.3.16 lldp auto-vlan sensor ap

Function

The **lldp auto-vlan sensor ap** command configures a switch to identify Huawei Fit APs using LLDP and adds the interfaces receiving the LLDP packets from APs to the specified VLAN.

The **undo lldp auto-vlan** command disables this function.

By default, this function is disabled.

Format

lldp auto-vlan *vlan-id* **sensor ap**

undo lldp auto-vlan *vlan-id* **sensor ap**

lldp auto-vlan tagged { *vlan-id1* [**to** *vlan-id2*] }&<1-10> **sensor ap**

undo lldp auto-vlan tagged { *vlan-id1* [**to** *vlan-id2*] }&<1-10> **sensor ap**

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN to which the interfaces receiving LLDP packets from APs are added in untagged mode.	The value is an integer that ranges from 1 to 4094.
tagged	Indicates that the interfaces receiving LLDP packets from APs are added to a VLAN in tagged mode.	-
vlan-id1 [**to** *vlan-id2*]	Specifies the VLAN to which the interfaces receiving LLDP packets from APs are added in tagged mode.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switch is connected to a Huawei Fit AP, the interfaces connected to the AP must be added to the AP's management VLAN in untagged mode and to the AP's service VLAN in tagged mode. If many APs are connected to the switch, the configuration is complex. To facilitate operation, run the **lldp auto-vlan** *vlan-id* **sensor ap** command to enable the switch to automatically add the interfaces receiving LLDP packets from an AP to the AP's management VLAN in untagged mode, and run the **lldp auto-vlan tagged** { *vlan-id1* [**to** *vlan-id2*] }&<1-10> **sensor ap** command to add these interfaces to the AP's service VLAN in tagged mode.

You can run the **display port vlan** [*interface interface-number* | **active**] command to view information about the VLANs to which interfaces are automatically added.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Precautions

- The ID of the VLAN to which interfaces are added in untagged mode cannot be the same as the ID of the VLAN to which the interfaces are added in tagged mode.
- The VLAN specified in the command can be an existing VLAN or created after this command is executed, but cannot be the control VLAN for SEP/RRPP/ERPS.
- After an interface is added in untagged mode to a specified VLAN, the original PVID of the interface becomes invalid. When the LLDP neighbor information of the interface ages (for example, the connected AP goes offline), the original PVID configuration takes effect again and the interface is automatically removed from the VLAN.
- If the VLAN to which an interface is added in tagged mode is the same as that manually configured on the interface, the manually configured VLAN takes effect.
- An interface can be automatically added to a VLAN in tagged mode only when the interface type is trunk or hybrid.

Example

Add the interfaces receiving LLDP packets from an AP to the management VLAN 100 in untagged mode and to the service VLAN 200 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] lldp enable
[HUAWEI] lldp auto-vlan 100 sensor ap
[HUAWEI] lldp auto-vlan tagged 200 sensor ap
```

16.3.17 lldp clear neighbor

Function

The **lldp clear neighbor** command clears LLDP neighbors in the system or on an interface of the device.

Format

lldp clear neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of the interface whose LLDP neighbors to be cleared. In the command: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, this command clears LLDP neighbors on all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to obtain the latest LLDP neighbor information of interfaces, use the **lldp clear neighbor** command to clear existing LLDP neighbors. When an interface receives new LLDP packets, new LLDP neighbors are generated.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Example

Clear LLDP neighbors of all interfaces.

```
<HUAWEI> lldp clear neighbor
Warning: This command will clear the neighbor information of all the ports. Continue? [Y/N]:y
```

16.3.18 lldp compliance cdp receive

Function

The **lldp compliance cdp receive** command enables CDP-compatible LLDP on an interface.

The **undo lldp compliance cdp receive** command disables CDP-compatible LLDP on an interface.

By default, CDP-compatible LLDP is disabled on an interface.

Format

lldp compliance cdp receive

undo lldp compliance cdp receive

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Neighbors may use other proprietary protocols but LLDP, for example, CDP. To ensure that the local device can discover and identify the neighbors, you can use this command to enable CDP-compatible LLDP on an interface.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

Example

Enable CDP-compatible LLDP on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp compliance cdp receive
```

16.3.19 lldp compliance cdp txrx

Function

The **lldp compliance cdp txrx** command enables an interface to exchange information with CDP-capable devices.

The **undo lldp compliance cdp txrx** command disables an interface from exchanging information with CDP-capable devices.

By default, an interface cannot exchange information with CDP-capable devices.

Format

lldp compliance cdp txrx

undo lldp compliance cdp txrx

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some IP phones send proprietary protocol packets but not DHCP packets to apply for IP addresses. After you run the **lldp compliance cdp txrx** command on an interface, the switch can identify proprietary protocol packets sent from such the IP phone connected to the interface and respond to the proprietary protocol packets. In addition, the switch assigns the voice VLAN configured on the LLDP module to the IP phone.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

When a switch connects the IP phones of some vendors, you are advised to run the **lldp tlv-enable med-tlv network-policy voice-vlan vlan** *vlan-id* command to specify the voice VLAN ID in the MED TLVs advertised from the interface.

Example

Enable GigabitEthernet0/0/1 to exchange information with CDP-capable voice devices.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable med-tlv network-policy voice-vlan vlan 10
[HUAWEI-GigabitEthernet0/0/1] lldp compliance cdp txrx
```

16.3.20 lldp device-classifier enable

Function

The **lldp device-classifier enable** command enables the switch to automatically execute the Python script after the LLDP neighbor changes.

The **undo lldp device-classifier enable** command disables the switch from automatically executing the Python script after the LLDP neighbor changes.

By default, the switch is enabled to automatically execute the Python script after the LLDP neighbor changes.

Format

lldp device-classifier enable

undo lldp device-classifier enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a switch has multiple types of LLDP neighbors and needs to deliver different configurations to different types of LLDP neighbors, configure the Python script in advance and run the **lldp device-classifier enable** command to enable the switch to automatically execute the Python script after the LLDP neighbor changes. If the switch detects that a specified type of LLDP neighbor is added or deleted on an interface, the switch automatically delivers the predefined configuration in the Python script, reducing the configuration workload.

Prerequisites

1. The Python script automatically executed after the LLDP neighbor changes has been prepared, uploaded, and installed, and the Python script assistant has been configured. For details, see "**Configuring OPS**" in OPS Configuration in *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.
2. LLDP has been enabled globally using the **lldp enable (system view)** command.

Example

Enable the switch to automatically execute the Python script after the LLDP neighbor changes.

```
<HUAWEI> system-view
[HUAWEI] lldp device-classifier enable
```

16.3.21 lldp dot3-tlv power

Function

The **lldp dot3-tlv power** command sets the standard to which the 802.3 Power Via MDI TLV sent by an interface conforms.

The **undo lldp dot3-tlv power** command restores the default configuration.

By default, the 802.3 Power Via MDI TLV conforms to 802.1ab.

Format

lldp dot3-tlv power { **802.1ab** [**force**] | **802.3at** }

undo lldp dot3-tlv power { **802.1ab force** | **802.3at** }

Parameters

Parameter	Description	Value
802.1ab	Indicates that the 802.3 Power Via MDI TLV sent by the interface conforms to 802.1ab.	-
802.3at	Indicates that the 802.3 Power Via MDI TLV sent by the interface conforms to 802.3at.	-

Parameter	Description	Value
force	Indicates that the 802.3 Power Via MDI TLV sent by the interface must conform to 802.1ab.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.3 Power Via MDI TLV has the following formats:

- 802.1ab format: [TLV type | TLV information string length | 802.3 OUI | 802.3 subtype | MDI power support | PSE power pair | power class]
- 802.3at format: [TLV type | TLV information string length | 802.3 OUI | 802.3 subtype | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]

Based on 802.1ab, 802.3at extends three fields: t**ype/source/priority**, **PD requested power value**, and **PSE allocated power value**.

If a PD requires higher power than the PoE switch can supply, run the **lldp dot3-tlv power 802.1ab force** command to specify that 802.3 Power Via MDI TLV sent by the interface must conform to 802.1ab, so as to reduce the power required by the PD.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

Before selecting a format of the 802.3 Power Via MDI TLV, you must know the TLV format supported by the neighbors. The TLV format on the local device must be the same as that on the neighbors. You are advised to retain the default configuration of the switch. That is, interfaces send 802.3 Power Via MDI TLV conforming to 802.1ab. The switch can then adapt to 802.3 Power Via MDI TLV conforming to 802.1ab or 802.3at based on the remote device and correctly communicates with the remote device.

An Ethernet interface supports the **lldp dot3-tlv power** command no matter whether it works in Layer 2 or Layer 3 mode.

An interface that is already configured with the **poe power auto-neg enable** command do not support the **lldp dot3-tlv power 802.1ab force** and **lldp dot3-tlv power 802.3at** commands.

Example

Configure the interface to send the 802.3 Power Via MDI TLV conforming to 802.3at.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp dot3-tlv power 802.3at
```

16.3.22 lldp enable (interface view)

Function

The **lldp enable** command enables LLDP on an interface.

The **undo lldp enable** command disables LLDP on an interface.

After LLDP is enabled in the system view, all interfaces are enabled with LLDP.

Format

lldp enable

undo lldp enable

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After LLDP is enabled on an interface, the interface exchanges LLDP packets with LLDP-enabled neighbors. The interface receives status information from the neighbors and sends the local status information to the neighbors. The NMS then obtains the status information for topology discovery.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Precautions

LLDP can be enabled in the system view and the interface view.

- After LLDP is enabled in the system view, all interfaces are enabled with LLDP.
- After LLDP is disabled in the system view, all LLDP settings are restored to the default settings except the setting of LLDP trap. Therefore, LLDP is also disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.
- If LLDP needs to be disabled on some interfaces, enable LLDP globally first, and run the **undo lldp enable** command on these interfaces. To re-enable LLDP on these interfaces, run the **lldp enable** command in the views of these interfaces.

The **lldp enable (interface view)** command can be executed only on an Ethernet interface, regardless of whether it works at Layer 2 or Layer 3 mode, but not on a logical interface such as a VLANIF or Eth-Trunk interface. For an Eth-Trunk interface, LLDP can only be enabled on its member interfaces. LLDP-enabled interfaces and LLDP-disabled interfaces can exist in the same Eth-Trunk.

Example

Disable LLDP on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo lldp enable
```

16.3.23 lldp enable (system view)

Function

The **lldp enable** command enables LLDP globally.

The **undo lldp enable** command disables LLDP globally.

By default, LLDP is enabled globally.

Format

lldp enable

undo lldp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the Layer 2 link status or analyze network topology, run the **lldp enable** command.

Configuration Impact

After LLDP is enabled globally, the device sends its own status information to LLDP-enabled neighbors and receives the status information from the neighbors.

Precautions

After the global LLDP is disabled, the LLDP configuration is deleted from all interfaces.

The interval between enabling LLDP globally and disabling LLDP cannot be shorter than 10 seconds; otherwise, an error message is displayed.

LLDP can be enabled in the system view and the interface view.

- After LLDP is enabled in the system view, all interfaces are enabled with LLDP.
- After LLDP is disabled in the system view, all LLDP settings are restored to the default settings except the setting of LLDP trap. Therefore, LLDP is also disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.

For the device running a version earlier than V200R011C10SPC200:

- By default, LLDP is disabled globally, and the configuration file does not have the **undo lldp enable** configuration. After the device is upgraded to V200R011C10SPC200 or a later version, the configuration file has the **undo lldp enable** configuration.
- If **lldp enable** has been executed to enable LLDP globally, the configuration file has the **lldp enable** configuration. After the device is upgraded to V200R011C10SPC200 or a later version, the configuration file no longer has the **lldp enable** configuration.

The status of global LLDP does not change after the device is upgraded.

Example

Enable LLDP globally.

```
<HUAWEI> system-view
[HUAWEI] lldp enable
```

Disable LLDP globally.

```
<HUAWEI> system-view
[HUAWEI] undo lldp enable
Warning: This command will delete the configurations of LLDP on all the ports.Continue?[Y/N]:y
```

16.3.24 lldp management-address

Function

The **lldp management-address** command configures the LLDP management IP address.

The **undo lldp management-address** command restores the default setting.

By default, the system automatically obtains the management IP address.

Format

lldp management-address *ip-address*

undo lldp management-address

Parameters

Parameter	Description	Value
ip-address	Specifies the management IP address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The management IP address is carried in the management address TLV field of the LLDP packet. It is used by the NMS to identify and manage devices. A management address identifies a device, facilitating the layout of the network topology and network management. To allocate a management address to a neighbor, run the **lldp management-address** command.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

The management IP address to be allocated must be a valid unicast IP address existing on the device.

Configuration Impact

After the configuration, the management IP address is added to the management address TLV field of the LLDP packet. The NMS then identifies the device according to the management IP address.

Precautions

If no management address is configured or an invalid management address is configured, the system sets an IP address in the address list as the management address. The system selects the IP address in the following sequence: IP address of the device connected to the iMaster NCE-Campus, loopback interface address, management port address, VLANIF interface address, VBDIF interface address, Layer 3 Ethernet interface address, and Sub-interface. Among the IP addresses of the same type, the system selects the smallest one. If the system fails to find a management IP address, the bridge MAC address is used as the management address.

Example

Set the LLDP management IP address to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] lldp management-address 10.10.10.1
```

16.3.25 lldp message-transmission delay

Function

The **lldp message-transmission delay** command sets the LLDP packet transmission delay.

The **undo lldp message-transmission delay** command restores the default LLDP packet transmission delay.

By default, the LLDP packet transmission delay is 2 seconds.

Format

lldp message-transmission delay *delay*

undo lldp message-transmission delay [*delay*]

Parameters

Parameter	Description	Value
delay	Specifies the LLDP packet transmission delay.	The value is an integer ranging from 1 to 8192, in seconds. The default value is 2 seconds. The *delay* value depends on the *interval* value in **lldp message-transmission interval**. The *delay* value must be equal to or smaller than a quarter of the *interval* value.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the interface sends an LLDP packet to the neighbor when the device status changes frequently. After the LLDP packet transmission delay is set on the device, the LLDP-enabled interfaces send LLDP packets to neighbors after a delay (the delay is the same as or longer than the delay you specified). The interfaces may send LLDP packets at different time points.

If the device status changes frequently, extend the delay in preventing the device from frequently sending packets to the neighbors. A delay suppresses the network topology flapping.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Configuration Impact

The LLDP packet transmission delay must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency when the local device status frequently changes. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time when the local device status frequently changes. However, if the value is too small, LLDP packets are exchanged frequently, increasing the system load.
- The default value is recommended.

Precautions

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- The value of *delay* ranges from 1 to 8192.
- The value of *delay* must be smaller than or equal to a quarter of *interval*. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to four times the new *delay* value, and then increase the *delay* value.

NOTE

If the *interval* value is smaller than four times the *delay* value, the system displays an error message when you run the **undo lldp message-transmission delay** command. To run the **undo lldp message-transmission delay** command in this case, increase the *interval* value to at least four times the *delay* value first.

Example

Set the LLDP packet transmission delay to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] lldp message-transmission delay 5
```

16.3.26 lldp message-transmission hold-multiplier

Function

The **lldp message-transmission hold-multiplier** command sets the hold time multiplier of device information stored on neighbors.

The **undo lldp message-transmission hold-multiplier** command restores the default hold time multiplier of device information stored on neighbors.

The default hold time multiplier is 4.

Format

lldp message-transmission hold-multiplier *hold*

undo lldp message-transmission hold-multiplier [*hold*]

Parameters

Parameter	Description	Value
hold	Specifies the hold time multiplier of device information on neighbors.	The value is an integer ranging from 2 to 10. The default value is 4.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The time multiplier is used to calculate how long a packet can be saved on a neighboring node. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

TTL is the device information storage time. It is the smaller value between 65535 and (*interval* x *hold*).

interval indicates the interval at which the device sends LLDP packets to neighbors. This parameter is set by **lldp message-transmission interval**. *hold* indicates the hold time multiplier of device information on neighbors.

After the LLDP function is disabled on the device, its neighbors wait until the TTL of the device information expires, and then delete the device information. This prevents network topology flapping.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Configuration Impact

The hold time multiplier of device information on neighbors must be set to a proper value.

- A large value of *hold* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *hold* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the hold time multiplier of device information on neighbors to 5.

```
<HUAWEI> system-view
[HUAWEI] lldp message-transmission hold-multiplier 5
```

16.3.27 lldp message-transmission interval

Function

The **lldp message-transmission interval** command sets the LLDP transmission interval.

The **undo lldp message-transmission interval** command restores the default LLDP transmission interval.

The default LLDP transmission interval is 30 seconds.

Format

lldp message-transmission interval *interval*

undo lldp message-transmission interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the LLDP transmission interval.	The value is an integer ranging from 5 to 32768, in seconds. The default value is 30 seconds. The *interval* value depends on the *delay* value in **lldp message-transmission delay**. The value of *interval* must be equal to or greater than four times the value of *delay*. Otherwise, an error occurs in the configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the LLDP status of the device keeps unchanged or the device does not discover new neighbors, the interface sends LLDP packets to the neighbors at a certain interval. After the LLDP transmission interval is set on the device, the LLDP enabled interfaces send LLDP packets to neighbors at this interval. The interfaces may send LLDP packets at different time points.

If you want to change the network topology detection frequency, run the **lldp message-transmission interval** command to change the LLDP transmission interval.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Configuration Impact

The LLDP transmission interval must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.

- A short interval increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time. However, if the interval is too short, LLDP packets are exchanged frequently, increasing the system load.

Precautions

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *delay*.

- The value of *interval* ranges from 5 to 32768.
- The value of *interval* must be equal to or greater than four times the value of *delay*. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be equal to or smaller than a quarter of the new *interval* value, and then reduce the *interval* value.

NOTE

If the *delay* value is greater than a quarter of the *interval* value, the system displays an error message when you run the **undo lldp message-transmission interval** command. To run the **undo lldp message-transmission interval** command in this case, reduce the *delay* value to be equal to or smaller than a quarter of *interval* first.

Example

Set the LLDP transmission interval to 35 seconds.

```
<HUAWEI> system-view
[HUAWEI] lldp message-transmission interval 35
```

16.3.28 lldp restart-delay

Function

The **lldp restart-delay** command sets the delay in re-enabling the LLDP function on an interface.

The **undo lldp restart-delay** command restores the default delay in re-enabling the LLDP function on an interface.

The default delay is 2 seconds.

Format

lldp restart-delay *delay*

undo lldp restart-delay [*delay*]

Parameters

Parameter	Description	Value
delay	Specifies the delay in re-enabling the LLDP function on an interface.	The value is an integer ranging from 1 to 10, in seconds. The default value is 2 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before LLDP is re-enabled on an interface. The delay suppresses the topology flapping caused by the frequent LLDP status changes.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Configuration Impact

The delay in re-enabling the LLDP function on an interface must be set properly.

- A large value of *delay* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *delay* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the delay in re-enabling the LLDP function on an interface to 3 second.

```
<HUAWEI> system-view
[HUAWEI] lldp restart-delay 3
```

16.3.29 lldp tlv-enable (MEth interface view)

Function

The **lldp tlv-enable** command sets the TLVs that can be sent by the MEth interface.

The **undo lldp tlv-enable** command sets the TLVs disabled on the MEth interface.

By default, the MEth interface can advertise all TLVs except the Location Identification TLV.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } & <1-10> | **elin-address** *Tel-Number* } }

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** [**civic-address** | **elin-address**] }

Parameters

Parameter	Description	Value
all	Indicates to advertise all basic TLV.	-
management-address	Indicates to advertise Management-address TLV.	-
port-description	Indicates to advertise Port Description TLV.	-
system-capability	Indicates to advertise System Capabilities TLV.	-
system-description	Indicates to advertise System Description TLV.	-
system-name	Indicates to advertise System Name TLV.	-
all	Indicates to advertise all MED TLVs except the Location Identification TLV.	-
capability	Indicates to advertise MED Capabilities TLV.	-
inventory	Indicates to advertise Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV, and Asset ID TLV.	-
location-id	Indicates to advertise Location Identification TLV.	-

Parameter	Description	Value
civic-address *device-type country-code* { *ca-type ca-value* } & <1-10>	Indicates to advertise the common address information of the network devices encapsulated in Location Identification TLV. ● *device-type* specifies the type of the device. The value is an integer that ranges from 0 to 2. 0 indicates that the device is a DHCP server. 1 indicates that the device is a switch. 2 indicates that the device is an MED endpoint. ● *country-code* specifies the country code. For the value range, see ISO 3166. ● { *ca-type ca-value* }&<1-10> specifies the address information. *ca-type* specifies the type of address information. The value is an integer that ranges from 0 to 255. *ca-value* specifies the content of the address information. The value is a string of 1-250 characters. **<1-10>** indicates that the preceding parameters can be entered 10 times.	-
elin-address *Tel-Number*	Advertises the emergency phone number encapsulated in Location Identification TLV.	The value is a string of 10 to 25 numerals. Each numeral ranges from 0 to 9.

Views

MEth interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. LLDPDUs supported by the management interface includes basic TLVs and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

- If the **all** parameter is not specified, all the available TLVs of the specified type can be advertised except the Location Identification TLV. If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.
- You can specify the other types of MED TLVs only after specifying the MED Capabilities TLV.

  To disable the MED Capabilities TLV, first disable the other types of MED TLVs.

Example

Configure The MEth interface to advertise the MED Capabilities TLV.

```
<HUAWEI> system-view
[HUAWEI] interface meth 0/0/1
[HUAWEI-MEth0/0/1] lldp tlv-enable med-tlv capability
```

16.3.30 lldp tlv-enable basic-tlv

Function

The **lldp tlv-enable basic-tlv** command sets the basic TLVs that can be sent by an interface.

The **undo lldp tlv-enable basic-tlv** command set the basic TLVs disabled on an interface.

By default, an interface can advertise all basic TLVs.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

Parameters

Parameter	Description	Value
all	Indicates to advertise all basic TLVs.	-
management-address	Indicates to advertise Management-address TLV.	-
port-description	Indicates to advertise Port Description TLV.	-
system-capability	Indicates to advertise System Capabilities TLV.	-
system-description	Indicates to advertise System Description TLV.	-
system-name	Indicates to advertise System Name TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

Example

Configure GigabitEthernet0/0/1 to advertise all basic TLVs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable basic-tlv all
```

16.3.31 lldp tlv-enable dot1-tlv

Function

The **lldp tlv-enable dot1-tlv** command sets to advertise TLVs defined by the IEEE 802.1 working group.

The **undo lldp tlv-enable dot1-tlv** command sets the TLVs defined by the IEEE 802.1 working group disabled on an interface.

By default, an interface advertises all TLVs defined by the IEEE 802.1 working group, except Protocol Identity TLV.

Format

lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [{ *vlan-id* [**to** *vlan-id1*] } &<1-14>] | **protocol-identity** }

undo lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [{ *vlan-id* [**to** *vlan-id1*] } &<1-14>] | **protocol-identity** }

Parameters

Parameter	Description	Value
all	Indicates to advertise all TLVs defined by the IEEE 802.1 working group.	-
port-vlan-id	Indicates to advertise Port VLAN ID TLV. The VLAN ID is the default VLAN ID on the interface.	-

Parameter	Description	Value
protocol-vlan-id [*vlan-id*]	Indicates to advertise Port And Protocol VLAN ID TLV. If *vlan-id* is not specified, the interface does not support protocol VLAN TLVs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
vlan-name [{ *vlan-id* [**to** *vlan-id1*] } &<1-14>]	Indicates to advertise VLAN Name TLV. If no VLAN ID is specified, the default VLAN ID is used. ● *vlan-id* specifies the start VLAN ID. ● **to** *vlan-id1* specifies the end VLAN ID. The value of *vlan-id1* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id* is an integer that ranges from 1 to 4094. The value of *vlan-id1* is an integer that ranges from 1 to 4094.
protocol-identity	Indicates to advertise Protocol Identity TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.

NOTE

An Ethernet interface working in Layer 3 mode does not support the TLVs defined in IEEE 802.1.

Example

Configure GigabitEthernet0/0/1 to advertise the port VLAN TLV in the IEEE 802.1 format.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable dot1-tlv port-vlan-id
```

16.3.32 lldp tlv-enable dot3-tlv

Function

The **lldp tlv-enable dot3-tlv** command sets to advertise the TLVs defined by the IEEE 802.3 working group.

The **undo lldp tlv-enable dot3-tlv** command sets the TLVs defined by the IEEE 802.3 working group disabled on an interface.

By default, an interface advertises all TLVs defined by the IEEE 802.3 working group.

Format

lldp tlv-enable dot3-tlv { **all** | **eee** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

undo lldp tlv-enable dot3-tlv { **all** | **eee** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

Parameters

Parameter	Description	Value
all	Indicates to advertise all TLVs defined by the IEEE 802.3 working group.	-
eee	Indicates to advertise EEE (Energy Efficient Ethernet) TLV. EEE is supported only when the switch has only one neighbor.	-

Parameter	Description	Value
link-aggregation	Indicates to advertise Link Aggregation TLV.	-
mac-physic	Indicates to advertise MAC/PHY Configuration/Status TLV.	-
max-frame-size	Indicates to advertise Maximum Frame Size TLV.	-
power	Indicates to advertise Power Via MDI TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

Example

Configure GigabitEthernet0/0/1 to advertise the Link Aggregation TLV in the IEEE 802.3 format.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable dot3-tlv link-aggregation
```

16.3.33 lldp tlv-enable legacy-tlv esn

Function

The **lldp tlv-enable legacy-tlv esn** command enables the LLDPDUs sent by a device to carry ESN information.

The **undo lldp tlv-enable legacy-tlv esn** command disables the LLDPDUs sent by a device from carrying ESN information.

By default, the LLDPDUs sent by a switch carries ESN information.

Format

lldp tlv-enable legacy-tlv esn

undo lldp tlv-enable legacy-tlv esn

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

You can run the **undo lldp tlv-enable legacy-tlv esn** command to disable the LLDPDUs sent by a device from carrying ESN information.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command in the system view.
2. LLDP has been enabled on an interface using the **lldp enable** command in the interface view.

Example

Disable GE 0/0/2 from sending LLDPDUs carrying ESN information.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEIGigabitEthernet0/0/2] undo lldp tlv-enable legacy-tlv esn
```

16.3.34 lldp tlv-enable legacy-tlv poe

Function

The **lldp tlv-enable legacy-tlv poe** command enables the LLDPDUs sent by a device to carry the PoE power flag.

The **undo lldp tlv-enable legacy-tlv poe** command disables the LLDPDUs sent by a device from carrying the PoE power flag.

By default, the LLDPDUs sent by a switch carries the PoE power flag.

NOTE

This command is supported only on the following switch models:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731-S, S5731S-S, S5732-H, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-H, S5735S-S, S5735-S-I, S5736-S

Format

lldp tlv-enable legacy-tlv poe

undo lldp tlv-enable legacy-tlv poe

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

You can run the **undo lldp tlv-enable legacy-tlv poe** command to disable the LLDPDUs sent by a device from carrying the PoE power flag.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command in the system view.

2. LLDP has been enabled on an interface using the **lldp enable** command in the interface view.

Example

Disable GE 0/0/2 from sending LLDPDUs carrying the PoE power flag.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEIGigabitEthernet0/0/2] undo lldp tlv-enable legacy-tlv poe
```

16.3.35 lldp tlv-enable med-tlv

Function

The **lldp tlv-enable med-tlv** command sets to advertise the MED TLVs.

The **undo lldp tlv-enable med-tlv** command sets the MED TLVs disabled on an interface.

By default, an interface advertises all types of MED TLVs except the Location Identification TLV and Network Policy TLV.

NOTE

Although the interface does not advertise Network Policy TLV, Network Policy TLV is still enabled.

Format

lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } &<1-10> | **elin-address** *Tel-Number* } | **network-policy** [**voice-vlan** { **vlan** *vlan-id* [**cos** *cvalue* | **dscp** *dvalue*]* | **8021p** [**cos** *cvalue* | **dscp** *dvalue*]* | **untagged** }] | **power-over-ethernet** }

undo lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** [**civic-address** | **elin-address**] | **network-policy** [**voice-vlan** { **vlan** | **cos** | **dscp** | **8021p** | **untagged** }] | **power-over-ethernet** }

Parameters

Parameter	Description	Value
all	Indicates that all MED TLVs except Location Identification TLV and Network Policy TLV are advertised.	-
capability	Indicates to advertise MED Capabilities TLV.	-

Parameter	Description	Value
inventory	Indicates to advertise Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV, and Asset ID TLV.	-
location-id	Indicates to advertise Location Identification TLV.	-
civic-address *device-type country-code* { *ca-type ca-value* } & <1-10>	Indicates to advertise the common address information of the network devices encapsulated in Location Identification TLV. ● *device-type* specifies the type of the device. The value is an integer that ranges from 0 to 2. 0 indicates that the device is a DHCP server. 1 indicates that the device is a switch. 2 indicates that the device is an MED endpoint. ● *country-code* specifies the country code. For the value range, see ISO 3166. ● { *ca-type ca-value* }&<1-10> specifies the address information. *ca-type* specifies the type of address information. The value is an integer that ranges from 0 to 255. *ca-value* specifies the content of the address information. The value is a string of 1-250 characters. **<1-10>** indicates that the preceding parameters can be entered 10 times.	-
elin-address *Tel-Number*	Advertises the emergency phone number encapsulated in Location Identification TLV.	The value is a string of 10 to 25 numerals. Each numeral ranges from 0 to 9.

Parameter	Description	Value
network-policy	Advertises Network Policy TLV. Network Policy TLV is used to exchange VLAN configurations between network devices and terminal devices. A switch uses the TLV to advertise voice VLAN ID and voice stream priority to an IP phone. Then the IP phone forwards packets according to the received voice VLAN ID and priority, ensuring the voice quality. **NOTE** An Ethernet interface working in Layer 3 mode does not support the Network Policy TLV.	-
voice-vlan	Encapsulates the voice VLAN ID when advertising Network Policy TLV.	-
vlan *vlan-id*	Specifies the voice VLAN ID.	The value is an integer that ranges from 1 to 4094.
cos *cvalue*	Specifies the CoS priority. The CoS priority is the PRI (Priority) field in an 802.1Q VLAN frame. This field is 3 bits long and ensures that high-priority data packets are forwarded first when congestion occurs.	The value is an integer that ranges from 0 to 7. The default value is 5. A larger value indicates a higher priority.
dscp *dvalue*	Sets the DSCP priority. The first six bits of the Type of Service (ToS) field in an IPv4 packet header are used as the DiffServ Code Point (DSCP). DSCP is used in the DiffServ model to provide QoS guarantee on an IP network. The operations performed by the traffic controller on the gateway are determined only by these six bits.	The value is an integer that ranges from 0 to 63. The default value is 46.
8021p	Sets the voice VLAN ID to VLAN 0.	-
untagged	Configures voice devices to send untagged voice data packets.	-

Parameter	Description	Value
power-over-ethernet	Advertises Extended Power via MDI TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent. Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs. Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

- When the supported TLVs are MED TLVs, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs except Location Identification TLV. If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.
- You can specify the other types of MED TLVs only after specifying the MED Capabilities TLV. To disable the MED Capabilities TLV, first disable the other types of MED TLVs.
- To disable the 802.3 MAC/PHY Configuration/Status TLVs, first disable the MED Capabilities TLV.
- The 802.3 MAC/PHY Configuration/Status TLVs are automatically advertised after the MED Capabilities TLV is advertised.

- If you disable the MED TLVs using the command with the **all** parameter, the 802.3 MAC/PHY Configuration/Status TLVs are not disabled automatically.
- When the switch detects that the LLDP packet sent by an LLDP neighbor on an interface contains any type of MED TLV, the switch advertises all MED TLVs that can be advertised on the interface to the LLDP neighbor. However, the LLDP neighbor may support only parts of MED TLVs advertised by the switch, leading to an LLDP negotiation failure. You can run the **undo lldp tlv-enable med-tlv** command to enable the interface not to advertise the MED TLV that is not supported by the LLDP neighbor. For example, if a terminal does not support the 802.3af standard, that is, Extended Power-via-MDI TLV cannot be identified, run the **undo lldp tlv-enable med-tlv power-over-ethernet** command on the interface connected to the terminal to enable the interface not to advertise Extended Power-via-MDI TLV.
- The voice VLAN configured using the **lldp tlv-enable med-tlv network-policy voice-vlan** command has a higher priority than the voice VLAN authorized by the authentication server.

Example

Configure GigabitEthernet0/0/1 to advertise the MED Capabilities TLV.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable med-tlv capability
```

16.3.36 lldp trap-interval

Function

The **lldp trap-interval** command sets the delay in sending neighbor change traps to the NMS.

The **undo lldp trap-interval** command restores the default delay in sending neighbor change traps to the NMS.

By default, the device sends a neighbor change trap to the NMS after a 5-second delay.

Format

lldp trap-interval *interval*

undo lldp trap-interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the delay in sending traps.	The value is an integer ranging from 5 to 3600, in seconds. The default value is 5 seconds. The default value is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the device sends LLDP traps about neighbor information changes to the NMS. When neighbor information changes frequently, you can prolong the delay. In this way, the device will not frequently send traps to the NMS, and the network topology flapping is suppressed.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Configuration Impact

After the delay is set on the device, LLDP-enabled interfaces send LLDP traps to neighbors after a delay (the delay is the same as or longer than the delay you specified). The interfaces may send LLDP traps at different time points.

Precautions

The delay takes effect for the lldpRemTablesChange trap generated when a neighbor is added, aged, or discarded (a new neighbor is discarded if the number of neighbors on an interface or switch has reached the upper limit).

Example

Set the delay in sending neighbor change traps to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] lldp trap-interval 6
```

16.3.37 reset cdp statistics

Function

The **reset cdp statistics** command clears statistics about CDP packets that all interfaces receive and send or CDP packets that a specified interface receives and sends.

Format

reset cdp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Interface on which statistics about CDP packets are to be cleared. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, CDP packet information about all interfaces is cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to quickly locate and process a CDP fault, you must calculate the numbers of CDP packets sent and received by a device for a specified period. Before collecting specific CDP packet statistics, you can run the **reset cdp statistics** command to clear existing statistics about CDP packets.

Prerequisites

LLDP has been globally enabled using the **lldp enable** command in the system view and LLDP has been configured to be compatible with CDP on interfaces using the **lldp compliance cdp receive** command.

Follow-up Procedure

After running the **reset cdp statistics** command to clear existing statistics about CDP packets, you can run the **display cdp statistics** command to check statistics about CDP packets sent and received by a device for a specific period.

Precautions

If you do not set the **interface** parameter when running the **reset cdp statistics** command, statistics about CDP packets sent and received by all interfaces are cleared. Exercise caution when running this command.

Example

Display statistics about CDP packets that all interfaces receive and send.

```
<HUAWEI> reset cdp statistics
```

16.3.38 reset lldp statistics

Function

The **reset lldp statistics** command clears LLDP packet statistics on all interfaces or on a specified interface.

Format

reset lldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface where the LLDP statistics you want to reset. In the command: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, LLDP packet statistics of all interfaces are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To troubleshoot LLDP faults, you may need to view LLDP packet statistics within a certain period of time. In this case, you must run the **reset lldp statistics** command to clear existing LLDP packet statistics, and run the **display lldp statistics** command to view the new LLDP packet statistics.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Example

Clear LLDP packet statistics on all interfaces.

```
<HUAWEI> reset lldp statistics
Warning: This Command will clear LLDP statistics of all the ports. Continue? [Y/N]:y
```

Clear LLDP packet statistics of GigabitEthernet0/0/1.

```
<HUAWEI> reset lldp statistics interface gigabitethernet 0/0/1
```

16.4 Performance Management Commands

16.4.1 Command Support

Only the following switch models support Performance Management:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

16.4.2 binding

Function

The **binding** command binds an instance to a performance statistics collection task.

The **undo binding** command unbinds an instance from a performance statistics collection task.

By default, no instance is bound to a performance statistics collection task.

Format

binding instance-type *instance-type* **all**

binding instance-type *instance-type* **instance** *instance-name* &<1-5>

undo binding instance-type *instance-type* { **all** | **instance** *instance-name* &<1-5> }

Parameters

Parameter	Description	Value
instance-type *instance-type*	Specifies the type of an instance bound to a performance statistics collection task.	The enumerated values include: - **ipfpm**: collects IP FPM statistics. - **uni-mng-as-port**: collects statistics on an AS port. - **wlan-ap**: collects AP statistics: - **wlan-radio**: collects statistics about a specified AP radio. - **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. - **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.
all	Binds all instances. When **all** is specified, *instance-type* can only be **ipfpm**.	-

Parameter	Description	Value
instance *instance-name*	Specifies the name of an instance of a specific type.	The value is a string of 1 to 255 case-insensitive characters. - When *instance-type* is **ipfpm**, the *instance-name* value is configured using the **instance (IPFPM-MCP view)** command. - When *instance-type* is **uni-mng-as-port**, the *instance-name* value is AS name +interface number, for example, as1 gigabitethernet0/0/1. - When *instance-type* is **wlan-ap**, the *instance-name* value is ap-id. For example, 1 indicates AP 1. - When *instance-type* is **wlan-radio**, the *instance-name* value is ap-id.radio-id. For example, 0.1 indicates radio 1 of AP 0. - When *instance-type* is **wlan-ssid**, the *instance-name* value is ap-id.radio-id.SSID name length.SSID name ASCII code. For example, 1.0.5.98.99.100.101.102 indicates the SSID with the name bcdef and name length 5 of radio 0 of AP 1. - When *instance-type* is **wlan-ap-wiredport**, the *instance-name* value is ap-id.port type x 100+port number. For example, 0.101 indicates FE port 1 of AP 0. The port type can be 1 (an FE port) or 2 (a GE port). The port number ranges from 0 to 99.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **binding** command is used to bind an instance to a performance statistics task so that the system can collect the performance statistics about the instance. Multiple instances can be bound to a performance statistics collection task.

Prerequisites

The traffic statistics function has been enabled using the **statistics enable** command. Otherwise, the **binding** command cannot take effect.

Precautions

If multiple performance statistics tasks are bound to the same interface to collect interface statistics, the peak values of the tasks are inaccurate.

If **instance-type** is set to **uni-mng-as-port**, performance statistics on interfaces of the AS are collected. The interval for collecting traffic statistics on interfaces configured by the **set flow-stat interval** *interval-time* command must be shorter than the interval for collecting performance statistics configured by the **statistics-cycle** *cycle* command. If the value of *interval-time* is greater than the value of *cycle*, performance statistics on interfaces are incorrect. This is because the statistics about the rate and bandwidth usage on interfaces remain the same within the interval specified by *interval-time*.

Example

Bind all instances in IP FPM to performance statistics collection task **task1**.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] quit
[HUAWEI-nqa-ipfpm-mcp] quit
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] binding instance-type ipfpm all
```

16.4.3 display pm brief

Function

The **display pm brief** command displays brief PM information.

Format

display pm brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After PM is configured, you can run the **display pm brief** command to view brief PM information, such as the PM status, number of performance statistics tasks, number of performance statistics files.

NOTE

Number of Active Statistics Objects in the output of the **display pm brief** command shows the number of current statistics objects. When this number exceeds 10000, you are advised to run the **statistics-cycle** command to set the statistics collection period to 30 minutes or longer, and run the s**ample-interval** command to set the sampling period to 5 minutes or longer.

Example

Display brief PM information.

```
<HUAWEI> display pm brief
Statistics Status                  : disable
Statistics Start Time              : -
Number of Statistics Tasks         : 2
Number of Active Statistics Objects : 0
Number of Configured Pm Servers     : 0
Number of Statistics Files         : 0
Statistics Files Saved Directory    : /pmdata/
```

Table 16-43 Description of the **display pm brief** command output

Item	Description
Statistics Status	Whether the performance statistics function is enabled: ● enable: enabled ● disable: disabled You can run the **statistics enable** command to configure this parameter.
Statistics Start Time	Time when the performance statistics function starts.
Number of Statistics Tasks	Number of performance statistics tasks.
Number of Active Statistics Objects	Number of current performance statistics objects.
Number of Configured Pm Servers	Number of configured PM servers.
Number of Statistics Files	Number of performance statistics files.
Statistics Files Saved Directory	Path where performance statistics files are saved.

16.4.4 display pm measure-info

Function

The **display pm measure-info** command displays information about performance statistics counters.

Format

display pm measure-info [**instance-type** *instance-type*]

Parameters

Parameter	Description	Value
instance-type *instance-type*	Specifies the type of an instance bound to a performance statistics task.	The enumerated values include: ● **ipfpm**: collects IP FPM statistics. ● **uni-mng-as-port**: collects statistics on an AS port. ● **wlan-ap**: collects AP statistics: ● **wlan-radio**: collects statistics about a specified AP radio. ● **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. ● **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running the **measure disable** command to configure performance statistics counters for instances of a specific type, run the **display pm measure-info** command to view information about available performance statistics counters, including the name, type, maximum value, and minimum value of each counter.

Example

Display information about performance statistics counters of the instance of the IPFPM type.

```
<HUAWEI> display pm measure-info instance-type ipfpm
Total instance types: 1, total measures: 10
-------------------------------------------------------------------------------
Instance Type: ipfpm, Measures Count: 10
  Measure Name                 : forward-loss-ratio-max
  Measure Type                 : Maximum
  Measure Counter Size(bits)   : 32
  Measure MaxValue             : 100000000
  Measure MinValue             : -100000000

  Measure Name                 : forward-loss-ratio-min
  Measure Type                 : Minimum
  Measure Counter Size(bits)   : 32
  Measure MaxValue             : 100000000
  Measure MinValue             : -100000000

  Measure Name                 : forward-loss-pkts-inc
  Measure Type                 : Increase
  Measure Counter Size(bits)   : 64
  Measure MaxValue             : 9223372036854775807
  Measure MinValue             : -9223372036854775808
......
```

Table 16-44 Description of the **display pm measure-info** command output

Item	Description
Total instance types	Total types of measurement instances.
total measures	Total statistics counters.
Instance Type	Type of an instance.
Measures Count	Number of a performance statistics counter.
Measure Name	Name of a performance statistics counter.
Measure Type	Type of a performance statistics counter. The value can be: ● Increase: Accumulated performance statistics are compared with the counter. ● Actual: The currently collected performance statistics are compared with the counter. ● Maximum: The maximum performance statistics are compared with the counter. ● Minimum: The minimum performance statistics are compared with the counter. ● Average: The average performance statistics are compared with the counter.
Measure Counter Size(bits)	Size of a performance statistics counter, 32 bits or 64 bits.
Measure MaxValue	Maximum value of a performance statistics counter.
Measure MinValue	Minimum value of a performance statistics counter.

16.4.5 display pm statistics

Function

The **display pm statistics** command displays the collected performance statistics.

Format

display pm statistics *task-name* **data-index** *index* [**instance-type** *instance-type* [**measure** *measure-name* | **instance** *instance-name* &<1-5>] *]

Parameters

Parameter	Description	Value
task-name	Displays the performance statistics of a specified performance statistics collection task.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.
data-index *index*	Displays the performance statistics collected at a specified interval.	The value is an integer that ranges from 0 to 16. ● If the value is 0, the current performance statistics are displayed. ● If the value is larger than 0, the performance statistics collected in one or more cycles are displayed. The smaller the value, the latest the statistics. If a short performance statistics collection cycle (5, 10, 15, 30, or 60 minutes) is set, the value of *index* ranges from 1 to 16. If a long performance statistics collection cycle (1440 minutes) is set, the value of *index* ranges from 1 to 3.

Parameter	Description	Value
instance-type *instance-type*	Specifies the type of an instance bound to a performance statistics collection task.	The enumerated values include: - **ipfpm**: collects IP FPM statistics. - **uni-mng-as-port**: collects statistics on an AS port. - **wlan-ap**: collects AP statistics: - **wlan-radio**: collects statistics about a specified AP radio. - **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. - **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.
measure *measure-name*	Specifies the name of a statistics counter.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.
instance *instance-name*	Specifies the name of an instance.	The value is a string of 1 to 255 case-insensitive characters. - When *instance-type* is **ipfpm**, the *instance-name* value is configured using the **instance (IPFPM-MCP view)** command. - When *instance-type* is **uni-mng-as-port**, the *instance-name* value is AS name+interface number, for example, as1 gigabitethernet0/0/1. - When *instance-type* is **wlan-ap**, the *instance-name* value is ap-id. For example, 1 indicates AP 1. - When *instance-type* is **wlan-radio**, the *instance-name* value is ap-id.radio-id. For example, 0.1 indicates radio 1 of AP 0. - When *instance-type* is **wlan-ssid**, the *instance-name* value is ap-id.radio-id.SSID name length.SSID name ASCII code. For example, 1.0.5.98.99.100.101.102 indicates the SSID with the name bcdef and name length 5 of radio 0 of AP 1. - When *instance-type* is **wlan-ap-wiredport**, the *instance-name* value is ap-id.port type x 100+port number. For example, 0.101 indicates FE port 1 of AP 0. The port type can be 1 (an FE port) or 2 (a GE port). The port number ranges from 0 to 99.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the current or historical performance statistics, run the **display pm statistics** command. The system can display the current performance statistics and historical performance statistics collected in a maximum of 16 cycles.

Prerequisites

- An instance has been bound to the current performance statistics using **binding** command.
- Performance statistics has been enabled for the current performance statistics task using **statistics enable** command.

Precautions

To display the performance statistics, confirm that the performance statistics task is running.

Example

Display the current performance statistics of the performance statistics collection task **task1**.

```
<HUAWEI> display pm statistics task1 data-index 0
Total measures count: 10
-------------------------------------------------------------------------------
Instance Type        : ipfpm
Instance Name        : 1
Measure Name         : forward-loss-ratio-max
Measure Data         : 0
Valid Flag           : no statistics
Timestamp            : 2014-04-15 11:17:00

......
```

Table 16-45 Description of the **display pm statistics** command output

Item	Description
Total measures count	Number of a performance statistics counter.
Instance Type	Type of an instance bound to a performance statistics collection task.
Instance Name	Name of an instance bound to a performance statistics collection task.

Item	Description
Measure Name	Name of a performance statistics counter.
Measure Data	Statistics counter.
Valid Flag	Valid flag of the performance statistics. The value can be: ● no statistics: The performance statistics are not collected. ● valid: The performance statistics are valid. ● incredible value: The performance statistics are not reliable. ● measure not configured: The statistics counter is disabled.
Timestamp	Time when the performance statistics are collected.

16.4.6 display pm statistics-file

Function

The **display pm statistics-file** command displays performance statistics files.

Format

display pm statistics-file [*task-name*]

Parameters

Parameter	Description	Value
task-name	Displays the performance statistics files generated for a performance statistics task.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a performance statistics task starts, the system automatically generates performance statistics files for the task. To view the performance statistics files generated for the performance statistics task, run the **display pm statistics-file** command.

Example

Display performance statistics files for all performance statistics tasks.

```
<HUAWEI> display pm statistics-file
Total files count: 1
-------------------------------------------------------------------------------
Task Name: test
  test20130701150001.txt
```

Table 16-46 Description of the **display pm statistics-file** command output

Item	Description
Total files count	Number of performance statistics files.
Task Name	Name of a performance statistics task. You can run the **statistics-task** command to configure this parameter.
test20130701150001.txt	Name of the performance statistics file.

16.4.7 display pm statistics-task

Function

The **display pm statistics-task** command displays information about a performance statistics collection task.

Format

display pm statistics-task [*task-name*]

Parameters

Parameter	Description	Value
task-name	Displays the information about a specified performance statistics collection task.	The performance statistics collection task must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check information about a performance statistics collection task, including the running status of the task, statistics collection cycle, and type of the instance bound to the task.

Example

Display information about performance statistics collection tasks.

```
<HUAWEI> display pm statistics-task
Total task count: 1
--------------------------------------------------------------------------------
Task Name                : task1
Task State               : ready
Record-file Status       : enable
Threshold Alarm Status   : disable
Task Cycle               : 15 minutes
Sample Interval          : 3 minutes
Instance Type            : -
Record Interval(cycle)   : 4
File Format              : text
File Name Prefix         : task1
File Transfer Mode       : passive
Current File Name        : -
```

Table 16-47 Description of the **display pm statistics-task** command output

Item	Description
Total task count	Number of performance statistics collection tasks.
Task Name	Name of a performance statistics collection task. The task name is specified in the **statistics-task** *task-name* command.
Task State	Running status of a performance statistics collection task.
Record-file Status	Whether performance statistics file generation is enabled. The value can be: ● enable: This function is enabled. ● disable: This function is not enabled. This function is configured using the **record-file disable** command.
Threshold Alarm Status	Whether the threshold alarm function is enabled. The value can be: ● enable: This function is enabled. ● disable: This function is not enabled. This function is configured using the **threshold-alarm enable** command.
Task Cycle	Performance statistics collection cycle configured in a performance statistics collection task. This parameter is configured using the **statistics-cycle** *cycle* command.

Item	Description
Sample Interval	Sampling interval configured in a performance statistics collection task. This parameter is configured using the **sample-interval** *interval* command.
Instance Type	Type of an instance bound to a performance statistics collection task. This parameter is configured using the **binding instance-type** *instance-type* { **all** | **instance** *instance-name* &<1-5> } command.
Record Interval(cycle)	Interval at which the system generates performance statistics files. This parameter is configured using the **record-interval** *interval* command.
File Format	Format of performance statistics files.
File Name Prefix	Name prefix of a performance statistics file.
File Transfer Mode	Mode in which statistics files are uploaded to the performance management server. The value can be: ● active: The device automatically uploads statistics files to the performance management server, this function is configured using the **upload auto** command. ● passive: The device uploads statistics files to the performance management server following the instructions from the command line interface or network management system, this function is configured using the **upload** command.
Current File Name	Name of the current performance statistics file.

16.4.8 measure disable

Function

The **measure disable** command disables statistics counters in a performance statistics task.

The **undo measure disable** or **measure enable** command enables statistics counters in a performance statistics task.

By default, all statistics counters of the instance bound to the performance statistics collection task are measured.

Format

measure disable [*measure-name*]

undo measure disable [*measure-name*]

measure enable [*measure-name*]

Parameters

Parameter	Description	Value
measure-name	Specifies the name of a statistics counter in a performance statistics collection task.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the type of the instance bound to a performance statistics task is specified, statistics counters of instances of the specified type are enabled by default. The **measure disable** command can be used to disable some or all statistics counters.

After you run the **measure disable** [*measure-name*] command, some or all statistics counters are disabled. To add one or more counters that have been disabled to the performance statistics task again, run the **measure enable** [*measure-name*] or **undo measure disable** [*measure-name*] command to enable these counters.

Prerequisites

An instance has been bound to a performance statistics task using the **binding instance-type** *instance-type-name* **instance** *instance-name* command.

The performance statistics function has been enabled using the **statistics enable** command.

Example

Disable measurement of the forward-loss-ratio-max counter for ipfpm instances.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] binding instance-type ipfpm all
[HUAWEI-pm-statistics-task1] measure disable forward-loss-ratio-max
```

16.4.9 path

Function

The **path** command configures the destination path to save performance statistics files on the PM server.

The **undo path** command deletes the configured destination path.

By default, performance statistics files are uploaded to the default path on a PM server.

Format

path *destination-path*

undo path

Parameters

Parameter	Description	Value
destination-path	Specifies the destination path to save performance statistics files on the PM server.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To upload performance statistics files to a specific path on the PM server, run the **path** command to specify the destination path.

Precautions

The specified destination path must exist in the performance management server. Otherwise, the statistics file cannot be uploaded to the server.

Example

Specify the destination path to save performance statistics on the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] path d:/pmdata
```

16.4.10 pm

Function

The **pm** command displays the PM view.

Format

pm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the performance statistics function of PM, run the **pm** command to display the PM view.

Example

Display the PM view.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm]
```

16.4.11 pm-server

Function

The **pm-server** command creates a process serving the PM server and displays the view of the PM server created in the process. If there is an existing PM server view, the **pm-server** command displays the PM server view without creating a process.

The **undo pm-server** command deletes the created process.

By default, no process serving the PM server is created.

Format

pm-server *server-name*

undo pm-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of the process serving the PM server.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To upload generated performance statistics files to the PM server, run the **pm-server** command to create a process serving the PM server.

Follow-up Procedure

Configure the IP address and port number for the PM server, and user name and password for logging in to the PM server. Performance statistics files are uploaded to the PM server using FTP or SFTP.

Precautions

If a device is enabled to upload performance statistics files to a PM server, the process serving the PM server cannot be deleted.

Example

Create a process named **server1** to serve the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1]
```

16.4.12 protocol (PM server view)

Function

The **protocol** command configures the parameters for connecting to a PM server.

The **undo protocol** command deletes the parameters for connecting to a PM server.

By default, no PM server connection parameter is configured.

Format

protocol { **ftp** | **sftp** } **ip-address** *ip-address* [**port** *port-number* | { **net-manager-vpn** | **vpn-instance** *vpn-instance-name* }] *

undo protocol

Parameters

Parameter	Description	Value
ftp	Uses the FTP protocol to upload performance statistics files.	-
sftp	Uses the SFTP protocol to upload performance statistics files.	-
ip-address *ip-address*	Specifies the IP address of the PM server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number.	The value is an integer that ranges from 1 to 65535. The default port number is 21 (using FTP) or 22 (using SFTP).
net-manager-vpn	Indicates the network management VPN.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To upload statistics files to a PM server, use this command to configure connection parameters, including the transfer protocol, IP address, and port number of the PM server.

If the PM server uses a private IP address, you can use the **net-manager-vpn** parameter to specify a network management VPN or use the **vpn-instance** *vpn-instance-name* parameter to specify a VPN instance to upload a performance statistics file.

Precautions

Using FTP to upload performance statistics files is insecure. Therefore, using SFTP is recommended.

Example

Configure the device to upload performance statistics files to the SFTP server with the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] protocol sftp ip-address 10.1.1.1
```

16.4.13 record-file disable

Function

The **record-file disable** command disables performance statistics file generation.

The **undo record-file disable** command restores performance statistics file generation.

By default, a performance statistics file is automatically generated and saved on the device. A maximum of four performance statistics files can be generated for each performance statistics collection task.

Format

record-file disable

undo record-file disable

Parameters

None

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

To save system resources, reduce system cost and operations on storage devices, and prolong the lifespan of storage devices during performance statistics collection, run the **record-file disable** command to prevent performance statistics files from being generated.

The system-generated file name is named in the format of "name of a performance statistics task+time that a performance statistics file is generated", and is saved in the text format. Each performance statistics collection task can generate a maximum of four statistics files. If more than four statistics files are generated, the new file replaces the earliest one.

Example

Disable performance statistics file generation.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] record-file disable
```

16.4.14 record-interval

Function

The **record-interval** command sets the number of performance statistics collection cycles after which the system generates a statistics file.

The **undo record-interval** command restores the default number of performance statistics collection cycles.

By default:

- If a short performance statistics collection cycle (5, 10, 15, 30, or 60 minutes) is set, the system generates a statistics file after four cycles.
- If a long performance statistics collection cycle (1440 minutes) is set, the system generates a statistics file after one cycle.

Format

record-interval *interval*

undo record-interval

Parameters

Parameter	Description	Value
interval	Specifies the number of performance statistics collection cycles.	The value is an integer. The value range depends on the performance statistics collection cycle: ● If a short performance statistics collection cycle is set, the value of *interval* ranges from 1 to 16, and the default value is 4. ● If a long performance statistics collection cycle is set, the value of *interval* ranges from 1 to 3, and the default value is 1.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure a performance statistics collection task, the system periodically saves collected performance data to statistics files. To set the interval at which the system generates statistics files, run the **record-interval** command. Then the system generates performance statistics files every *cycle* x *interval* minutes, and automatically saves the performance data in the files. The system generates a maximum of four statistics files for each performance statistics collection task, and saves performance statistics files to the path flash: /pmdata by default.

Prerequisites

1. The performance statistics function has been enabled using the **statistics enable** command.
2. The *cycle* has been set using the **statistics-cycle** command.

Example

Configure the system to save performance data to a statistics file every three performance statistics collection cycles. If the performance statistics collection cycle is 5 minutes, the system saves a performance data to a statistics file every 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics enable
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] statistics-cycle 5
Warning: All data of the statistics task will be deleted. Continue? [Y/N]: y
[HUAWEI-pm-statistics-task1] record-interval 3
Warning: This operation will cause some data to be lost. Continue? [Y/N]: y
```

16.4.15 reset pm current-data

Function

The **reset pm current-data** command deletes the collected performance statistics.

Format

reset pm current-data [**instance-type** *instance-type* [**measure** *measure-name* | **instance** *instance-name* &<1-5>] *]

Parameters

Parameter	Description	Value
instance-type *instance-type*	Deletes the performance statistics about instances of a specified type. If **instance-type** *instance-type* is not specified, the system deletes the performance statistics about instances of all types.	The enumerated values include: - **ipfpm**: collects IP FPM statistics. - **uni-mng-as-port**: collects statistics on an AS port. - **wlan-ap**: collects AP statistics: - **wlan-radio**: collects statistics about a specified AP radio. - **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. - **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.
measure *measure-name*	Deletes the performance statistics about a specified counter.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.

Parameter	Description	Value
instance *instance-name*	Deletes the performance statistics about a specified instance.	The value is a string of 1 to 255 case-insensitive characters. ● When *instance-type* is **ipfpm**, the *instance-name* value is configured using the **instance (IPFPM-MCP view)** command. ● When *instance-type* is **uni-mng-as-port**, the *instance-name* value is AS name +interface number, for example, as1 gigabitethernet0/0/1. ● When *instance-type* is **wlan-ap**, the *instance-name* value is ap-id. For example, 1 indicates AP 1. ● When *instance-type* is **wlan-radio**, the *instance-name* value is ap-id.radio-id. For example, 0.1 indicates radio 1 of AP 0. ● When *instance-type* is **wlan-ssid**, the *instance-name* value is ap-id.radio-id.SSID name length.SSID name ASCII code. For example, 1.0.5.98.99.100.101.102 indicates the SSID with the name bcdef and name length 5 of radio 0 of AP 1. ● When *instance-type* is **wlan-ap-wiredport**, the *instance-name* value is ap-id.port type x 100+port number. For example, 0.101 indicates FE port 1 of AP 0. The port type can be 1 (an FE port) or 2 (a GE port). The port number ranges from 0 to 99.

Views

Performance statistics collection task view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete the collected performance statistics and collect new performance statistics, run the **reset pm current-data** command.

Precautions

Performance statistics cannot be restored after being deleted. Confirm your action before using this command.

Example

Delete the collected performance statistics.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] reset pm current-data
```

16.4.16 retry

Function

The **retry** command sets the number of retransmissions for a performance statistics file.

The **undo retry** command restores the number of retransmissions for a performance statistics file to the default value.

The default number of retransmissions for a performance statistics file is 3.

Format

retry *retry-times*

undo retry

Parameters

Parameter	Description	Value
retry-times	Sets the number of retransmissions for a performance statistics file.	The value is an integer ranging from 1 to 3. The default value is 3.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

The system generates performance statistics files and transmits these files to a PM server. To set the number of retransmissions for a performance statistics file, run the **retry** command.

Example

Set the number of retransmissions for a performance statistics file to 2.

```
<HUAWEI> system-view
[HUAWEI] pm
```

```
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] retry 2
```

16.4.17 sample-interval

Function

The **sample-interval** command configures the sampling interval for a performance statistics task.

The **undo sample-interval** command restores the default setting.

By default, the sampling interval varies with the performance statistics interval as follows:

- If the interval at which the performance statistics are collected is 5 minutes, the default sampling interval is 1 minute.
- If the interval at which the performance statistics are collected is 10 minutes, the default sampling interval is 2 minutes.
- If the interval at which the performance statistics are collected is 15 minutes, the default sampling interval is 3 minutes.
- If the interval at which the performance statistics are collected is 30 minutes, the default sampling interval is 5 minutes.
- If the interval at which the performance statistics are collected is 60 minutes, the default sampling interval is 5 minutes.
- If the interval at which the performance statistics are collected is 1440 minutes, the default sampling interval is 15 minutes.

Format

sample-interval *interval*

undo sample-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the performance statistics collected in a performance statistics task is sampled.	The value can be 1, 2, 3, 5, 10, 15, 30, or 60, in minutes: ● If the interval at which performance statistics are collected is 5 minutes, the sampling interval is 1 minute by default and can be set to 1 minute or 5 minutes. ● If the interval at which performance statistics are collected is 10 minutes, the sampling interval is 2 minutes by default and can be set to 1, 2, 5, or 10 minutes. ● If the interval at which performance statistics are collected is 15 minutes, the sampling interval is 3 minutes by default and can be set to 1, 3, 5, or 15 minutes. ● If the interval at which performance statistics are collected is 30 minutes, the sampling interval is 5 minutes by default and can be set to 1, 2, 3, 5, 10, 15, or 30 minutes. ● If the interval at which performance statistics are collected is 60 minutes, the sampling interval is 5 minutes by default and can be set to 1, 2, 3, 5, 10, 15, 30, or 60 minutes. ● If the interval at which performance statistics are collected is 1440 minutes, the sampling interval is 15 minutes by default and can be set to 1, 2, 3, 5, 10, 15, 30, or 60 minutes.

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

After the statistics task is configured, the system collects statistics at a specified sampling interval. The shorter the sampling interval, the more accurate the statistics. However, more system resources are consumed.

Example

Set the sampling interval to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] pm
```

```
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] sample-interval 5
```

16.4.18 statistics enable

Function

The **statistics enable** command enables the performance statistics function.

The **undo statistics enable** command disables the performance statistics function.

By default, the performance statistics function is disabled.

Format

statistics enable

undo statistics enable

Parameters

None

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect performance statistics, run the **statistics enable** command to enable the performance statistics function.

Precautions

After the **undo statistics enable** command is run, the performance statistics task that is running will be stopped. Therefore, exercise caution when you run this command.

Example

Enable the performance statistics function.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics enable
```

16.4.19 statistics-cycle

Function

The **statistics-cycle** command configures the performance statistics collection interval for a performance statistics task.

The **undo statistics-cycle** command restores the default setting.

The default interval is 15 minutes.

Format

statistics-cycle *cycle*

undo statistics-cycle

Parameters

Parameter	Description	Value
cycle	Specifies the performance statistics collection interval for a performance statistics task.	The value can be 5, 10, 15, 30, 60, or 1440, in minutes. The default value is 15 minutes. The system defines the interval 1440 minutes as a long interval and the interval 5, 10, 15, 30, or 60 minutes as a short interval.

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A specific performance statistics collection interval is set for each performance statistics task. After the performance statistics collection interval is set, bind an instance to the performance statistics task and enable statistics counter measurement so that the system can collect performance statistics at the specified interval. If the statistics interval is set to a small value, the obtained performance statistics are more accurate but more system resources are consumed.

Configuration Impact

Running the **statistics-cycle** command in the performance statistics task view has the following impacts:

- Performance statistics of the performance statistics task are deleted.

- The default interval at which the system generates performance statistics files is used. In the case of a short statistics collection interval, the system generates a performance statistics file every four performance statistics collection intervals; in the case of a long statistics collection interval, the system generates a performance statistics file every one performance statistics collection interval.

Prerequisites

The performance statistics function has been enabled using the **statistics enable** command.

Example

Set the performance statistics collection interval for the performance statistics task named **task1** to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] statistics-cycle 5
Warning: All data of the statistics task will be deleted. Continue? [Y/N]: y
```

16.4.20 statistics-task

Function

The **statistics-task** command creates a performance statistics task or displays the performance statistics task view.

The **undo statistics-task** command deletes a performance statistics task.

By default, no performance statistics task is created.

Format

statistics-task *task-name*

undo statistics-task *task-name*

Parameters

Parameter	Description	Value
task-name	Specifies the name of a performance statistics task.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A performance statistics task is the minimum statistics collection unit of PM. Before configuring the performance statistics function, run the **statistics-task** command to create a performance statistics task. Only one performance statistics collection interval can be configured for each performance statistics task. After a performance statistics task is configured, enable statistics counter measurement for the task.

Precautions

- A maximum of 16 performance statistics tasks can be configured.
- After the **undo statistics-task** command is run to delete a performance statistics task, performance statistics and performance statistics files of the task are deleted.

Prerequisites

The performance statistics function has been enabled using the **statistics enable** command.

Example

Configure a performance statistics task named **task1**.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1]
```

16.4.21 threshold-alarm enable

Function

The **threshold-alarm enable** command enables the threshold alarm.

The **undo threshold-alarm enable** command disables the threshold alarm.

By default, the threshold alarm function is disabled.

Format

threshold-alarm enable

undo threshold-alarm enable

Parameters

None

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The threshold alarm function enables users to learn the device operating status in a timely manner so that the device maintenance level can be promoted. To monitor the running data, run the command to enable the threshold alarm.

Precautions

After the **undo threshold-alarm enable** command is run, the threshold alarm function will be disabled and threshold alarms will be cleared. Exercise caution before operation.

Follow-up Procedure

After the command is run, run the **threshold-alarm measure** command to configure monitoring rules for the threshold alarm. Otherwise, the threshold alarm function will not take effect.

Example

Enable the threshold alarm function.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] threshold-alarm enable
```

16.4.22 threshold-alarm measure

Function

The **threshold-alarm measure** command creates monitoring rules for threshold alarms.

The **undo threshold-alarm measure** command deletes monitoring rules for threshold alarms.

By default, no monitoring rules are created for threshold alarms about performance statistics tasks.

Format

threshold-alarm measure *measure-name* **operation** { **ge** | **le** } **trigger-value** *trigger-value-val* **clear-value** *clear-value-val*

undo threshold-alarm measure *measure-name* **operation** { **ge** | **le** }

Parameters

Parameter	Description	Value
measure-name	Specifies the threshold monitoring indicator The indicator name is predefined by each feature.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.
operation { **ge** | **le** }	Specifies the type of triggering a threshold alarm.	Enumerated value: ge or le ● ge: the system triggers an alarm if the monitored indicator value is greater than or equal to the threshold value ● le: the system triggers an alarm if the monitored indicator value is less than or equal to the threshold value.
trigger-value *trigger-value-val*	Specifies the threshold information when the alarm is triggered.	The value is an integer, and the value range is determined by *measure-name*.
clear-value *clear-value-val*	Specifies the threshold information when the alarm is cleared.	The value is an integer, and the value range is determined by *measure-name*.

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The threshold alarm function is used for the system to periodically monitor the device operating status. If an alarm condition is triggered, the alarm will be sent to the NMS and cleared after the alarm condition is cleared.

The **threshold-alarm measure** command configures threshold monitoring rules for current performance statistics tasks. The **threshold-alarm measure** command configures the alarm triggering type, threshold for triggering an alarm and threshold for clearing an alarm based on the instance type and indicators of the threshold monitoring instance.

Prerequisites

Before the **threshold-alarm measure** command is run, run the **binding instance-type** *instance-type* { **all** | **instance** *instance-name* &<1-5> } command to bind a threshold monitoring instance, and run the **threshold-alarm enable** command to enable the threshold alarm function. Otherwise, alarms will not be sent.

Example

Create threshold monitoring rules.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] binding instance-type ipfpm all
[HUAWEI-pm-statistics-task1] threshold-alarm enable
[HUAWEI-pm-statistics-task1] threshold-alarm measure forward-loss-ratio-max operation ge trigger-
value 1000 clear-value 10
```

16.4.23 upload

Function

The **upload** command configures the device to upload performance statistics files to a PM server.

Format

upload *request-name* **file** *filename* &<1-16>

Parameters

Parameter	Description	Value
request-name	Specifies the name of a request for uploading performance statistics files.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.
file *filename*	Specifies the name of a performance statistics file.	The value is a string of 1 to 255 case-insensitive characters without spaces. The file name can contain the file path. If multiple files are specified, separate them with spaces.

Views

PM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system periodically generates performance statistics files based on the collected performance statistics. You can manually upload the statistics files to a PM server.

Prerequisites

A request for uploading performance statistics files to the PM server has been created using the **upload-config** *request-name* **server** *server-name* command.

Follow-up Procedure

View the performance statistics on the PM server.

Example

Configure the device to upload performance statistics file to the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server ftpserver
[HUAWEI-pm-server-ftpserver] quit
[HUAWEI-pm] upload-config req1 server ftpserver
[HUAWEI-pm] upload req1 file stream20130703103001.txt
```

16.4.24 upload auto

Function

The **upload auto** command enables a device to automatically upload performance statistics files to a server.

The **undo upload auto** command disables a device from automatically uploading performance statistics files to a server.

By default, a device does not automatically upload performance statistics files to a server.

Format

upload auto *request-name*

undo upload auto

Parameters

Parameter	Description	Value
request-name	Specifies the name of a request for uploading performance statistics files to a server.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system periodically generates performance statistics files based on the collected performance statistics. To enable the device to automatically upload performance statistics files to the PM server at a specific interval, run the **upload auto** command.

Prerequisites

A request for uploading performance statistics files to the PM server has been created using the **upload-config** *request-name* **server** *server-name* command.

Example

Configure the device to automatically upload statistics files to a PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server ftpserver
[HUAWEI-pm-server-ftpserver] quit
[HUAWEI-pm] upload-config req1 server ftpserver
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] upload auto req1
```

16.4.25 upload-config

Function

The **upload-config** command creates a request for uploading performance statistics files to a specified PM server.

The **undo upload-config** command deletes a request for uploading performance statistics files to a specified PM server.

By default, no request for uploading performance statistics files is available on a device.

Format

upload-config *request-name* **server** *server-name*

undo upload-config *request-name*

Parameters

Parameter	Description	Value
request-name	Specifies the name of a request for uploading performance statistics files.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.
server *server-name*	Specifies the name of the process serving the PM server.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to upload performance statistics files to a PM server, run the **upload-config** command to create a file uploading request.

Prerequisites

A PM server process has been created using the **pm-server** *server-name* command.

Follow-up Procedure

Enable the device to upload performance statistics files to the PM server.

- Run the **upload** *request-name* **file** *filename* &<1-16> command in the PM view to manually upload statistics files to the PM server.
- Run the **upload auto** *request-name* command in the performance statistics collection task view to configure the device to automatically upload statistics files to the PM server.

Example

Create a request for uploading statistics files to a PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server ftpserver
[HUAWEI-pm-server-ftpserver] quit
[HUAWEI-pm] upload-config req1 server ftpserver
```

16.4.26 username password

Function

The **username password** command configures the user name and password for logging in to the PM server.

The **undo username** command deletes the user name and password for logging in to the PM server.

By default, no user name and password for logging in to the PM server are configured.

Format

username *user-name* **password** *password*

undo username

Parameters

Parameter	Description	Value
user-name	Specifies the user name for logging in to a PM server.	The name is a string of 1 to 255 case-sensitive characters without spaces.
password	Specifies the password for logging in to a PM server.	The value is a string of 1 to 128 characters or a string of 32 to 200 characters. The password can be in plain or cipher text. ● The password in plain text is a string of 1 to 128 case-sensitive characters without spaces. ● The password in cipher text is a string of 32 to 200 characters. The password is displayed in ciphertext in the configuration file regardless of whether it is input in plain or cipher text. **NOTE** A 24-character ciphertext password configured in an earlier version is also supported in this version.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

To log in to a PM server for upload performance statistics files to the PM server, run the **username password** command to configure the user name and password.

Example

Configure the user name and password for logging in to the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] username admin password Pwd@123
```

16.5 iPCA Configuration Commands

16.5.1 Command Support

Only the following switch models support iPCA:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S

16.5.2 ach

Function

The **ach** command creates an Atomic Closed Hop (ACH) and displays the ACH view. If the ACH already exists, the command displays the ACH view directly.

The **undo ach** command deletes an ACH and all configurations in the ACH view.

By default, no ACH is created.

Format

ach *ach-id*

undo ach *ach-id*

Parameters

Parameter	Description	Value
ach-id	Specifies an ACH ID.	The value is an integer ranging from 1 to 2147483647.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACH consists of two target logical ports (TLPs) and is used to identify a segment between two specified devices on the network. In IP FPM hop-by-hop measurement, you need to specify the ACH for the target flow in a measurement instance and configure the direction and measurement points for the target flow in the ACH view. You can create an ACH and enter the ACH view by running the **ach** command.

Prerequisites

The **instance** command has been run to configure an IP FPM instance on an MCP.

Example

Create an ACH.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
```

16.5.3 authentication-mode (IPFPM-DCP view)

Function

The **authentication-mode** command configures the authentication mode and password on a Data Collecting Point (DCP).

The **undo authentication-mode** command deletes the authentication mode and password on a DCP.

By default, no authentication mode or password is configured on a DCP.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to encrypt and authenticate packets sent by a DCP to the MCP.	-

Parameter	Description	Value
key-id *key-id*	Specifies the ID of the authentication password configured on a DCP.	The value is an integer that ranges from 1 to 64.
cipher	Specifies the cipher-text authentication password on a DCP.	-
password	Specifies the authentication password on a DCP.	The value is a case-sensitive character string without spaces. ● The value is a string of 1 to 255 characters in plain text. ● The value is a string of 32 to 392 characters in cipher text.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Example

Configure the authentication mode and password on a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] authentication-mode hmac-sha256 key-id 1 cipher test12
```

16.5.4 authentication-mode (IPFPM-DCP instance view)

Function

The **authentication-mode** command configures the authentication mode and password for a measurement instance on a DCP.

The **undo authentication-mode** command deletes the authentication mode and password of a measurement instance on a DCP.

By default, no authentication mode or password is configured for a measurement instance on a DCP.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to encrypt and authenticate packets sent by a DCP to the MCP.	-
key-id *key-id*	Specifies the ID of the authentication password configured for a measurement instance.	The value is an integer that ranges from 1 to 64.
cipher	Specifies the cipher-text authentication password for a measurement instance.	-
password	Specifies the authentication password for a measurement instance.	The value is a case-sensitive character string without spaces. ● The value is a string of 1 to 255 characters in plain text. ● The value is a string of 32 to 392 characters in cipher text.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding high security, when iPCA is used to measure network-level packet loss, enable authentication. After the same authentication mode and password are configured on the MCP and DCPs, the MCP accepts the packets only from authenticated DCPs. This improves network security and reliability of packet loss measurement. The **authentication-mode** command configures the authentication mode and password for a measurement instance on a DCP.

Prerequisites

A measurement instance has been created on the DCP using the **instance** command.

Precautions

If the **authentication-mode** command is not used to configure the authentication mode and password, all measurement instances of the DCP use the authentication mode and password configured by the **authentication-mode (IPFPM-DCP view)** command.

Example

Configure the authentication mode and password for a measurement instance.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] authentication-mode hmac-sha256 key-id 1 cipher test12
```

16.5.5 authentication-mode (IPFPM-MCP view)

Function

The **authentication-mode** command configures the authentication mode and password on the Measurement Control Point (MCP).

The **undo authentication-mode** command deletes the authentication mode and password on the MCP.

By default, no authentication mode or password is configured on the MCP.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256 key-id *key-id*

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to decrypt and authenticate packets sent by a DCP to the MCP.	-
key-id *key-id*	Specifies the ID of the authentication password configured on the MCP.	The value is an integer that ranges from 1 to 64.

Parameter	Description	Value
cipher	Specifies the cipher-text authentication password configured on the MCP.	-
password	Specifies the authentication password configured on the MCP.	The value is a case-sensitive character string without spaces. ● The value is a string of 1 to 255 characters in plain text. ● The value is a string of 32 to 392 characters in cipher text.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding high security, when iPCA is used to measure network-level packet loss, enable authentication. After the same authentication mode and password are configured on the MCP and DCPs, the MCP accepts the packets only from authenticated DCPs. This improves network security and reliability of packet loss measurement. The **authentication-mode** command configures the authentication mode and password on the MCP.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

The MCP and DCP must be configured with the same authentication mode and password; otherwise, the MCP cannot obtain packet loss measurement from the DCP.

Example

Configure the authentication mode and password on the MCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] authentication-mode hmac-sha256 key-id 1 test12
```

16.5.6 color-flag loss-measure

Function

The **color-flag loss-measure** command configures the color bit used in network-level packet loss measurement.

The **undo color-flag** command restores the default color bit used in network-level packet loss measurement.

By default, bit 6 in the ToS field is used as the color bit for network-level packet loss measurement. The default configuration is recommended.

Format

color-flag loss-measure { **tos-bit** *tos-bit* | **flags-bit0** }

undo color-flag

Parameters

Parameter	Description	Value
tos-bit *tos-bit*	Specifies a bit in the range of bits 3 to 7 in the ToS field of IP packets as the color bit for network-level packet loss measurement.	The value is an integer that ranges from 3 to 7.
flags-bit0	Specifies bit 0 in the Flags field of IP packets as the color bit for network-level packet loss measurement.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before deploying Packet Conservation Algorithm for Internet (iPCA) to implement network-level packet loss measurement, run this command to configure the color bit. You can select a color bit according to the actual situation and network planning.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Precautions

All devices on a network must use the same color bit setting. When the DS field is used to provide differentiated service, it is not recommended that you configure bits 3-5 as color bits because the measurement result may be inaccurate.

When both network-level and device-level packet loss measurements are enabled on a device, the color bits must be differentiated.

Example

Configure bit 3 in the ToS field as the color bit for network-level packet loss measurement.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] color-flag loss-measure tos-bit 3
```

16.5.7 dcp

Function

The **dcp** command associates the DCP ID with a measurement instance on the MCP.

The **undo dcp** command disassociates the DCP ID from a measurement instance on the MCP.

By default, no DCP ID is associated with a measurement instance on the MCP.

Format

dcp *dcp-id*

undo dcp [*dcp-id*]

Parameters

Parameter	Description	Value
dcp-id	Specifies the DCP ID to be associated with a measurement instance.	The value is in dotted decimal notation.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each measurement instance of the MCP contains one or more DCP IDs. The MCP checks whether the statistics data is complete based on the DCP ID, so the DCP ID must be specified for a measurement instance created on the MCP. The **dcp** command associates the DCP ID with a measurement instance on the MCP.

Prerequisites

A measurement instance has been created on the MCP using the **instance** command.

Precautions

The DCP ID associated with the measurement instance on the MCP must be the same as the DCP ID configured by the **dcp id** command on the DCP.

The **undo dcp** command without *dcp-id* specified deletes all DCP IDs associated with a measurement instance.

Example

Associate a DCP ID with measurement instance 1 on the MCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] dcp 10.1.1.1
```

16.5.8 dcp id

Function

The **dcp id** command sets the DCP ID.

The **undo dcp id** command deletes the DCP ID.

By default, no DCP ID is configured.

Format

dcp id *dcp-id*

undo dcp id

Parameters

Parameter	Description	Value
dcp-id	Specifies the DCP ID. It is recommended that you configure the router ID of the device as the DCP ID.	The value is in dotted decimal notation.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MCP communicates with a DCP, the DCP encapsulates statistics data collected from Target Logical Ports (TLPs) in a packet and sends the packet with the DCP ID as the source IP address. After receiving the packet sent from the DCP, the MCP compares the DCP ID in the packet with the DCP ID configured by the **dcp** command:

- If the two DCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two DCP IDs are different, the MCP considers the packet invalid and discards it.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Precautions

Each DCP has a unique ID on the network. It is recommended that you configure the router ID of the device as the DCP ID. The DCP ID must be the same as the DCP ID in the measurement instance configured by the **dcp** command on the MCP.

Example

Set the DCP ID.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] dcp id 10.1.1.1
```

16.5.9 description (IPFPM-DCP instance view)

Function

The **description** command configures the description for a measurement instance on a DCP.

The **undo description** command deletes the description of a measurement instance on a DCP.

By default, no description is configured for a measurement instance on a DCP.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a measurement instance.	The value is a string of 1 to 64 case-sensitive characters with spaces supported.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. The **description** command configures the description for a measurement instance on a DCP, which helps you understand the function of the measurement instance.

It is recommended that the **description** command be used to configure the description for a measurement instance in the following situations:

- Many measurement instances are configured, and it is difficult to differentiate functions of each measurement instance.
- The interval for using the same measurement instance is too long, and functions of measurement instances change.

Precautions

If an IP FPM instance is configured but does not have a description, it may be misused.

Example

Configure the description for measurement instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] description NanJinToHeFei
```

16.5.10 description (IPFPM-MCP instance view)

Function

The **description** command configures the description for a measurement instance on the MCP.

The **undo description** command deletes the description of a measurement instance on the MCP.

By default, no description is configured for a measurement instance on the MCP.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a measurement instance.	The value is a string of 1 to 64 case-sensitive characters with spaces supported.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. The **description** command configures the description for a measurement instance on a DCP, which helps you understand the function of the measurement instance.

It is recommended that the **description** command be used to configure the description for a measurement instance in the following situations:

- Many measurement instances are configured, and it is difficult to differentiate functions of each measurement instance.
- The interval for using the same measurement instance is too long, and functions of measurement instances change.

Precautions

If an IP FPM instance is configured but does not have a description, it may be misused.

Example

Configure the description for measurement instance 1 on the MCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] description NanJinToHeFei
```

16.5.11 display ipfpm dcp

Function

The **display ipfpm dcp** command displays the DCP configuration in the IP Flow Performance Measurement (FPM) system.

Format

display ipfpm dcp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the DCP configuration.

Example

Display the DCP configuration.

```
<HUAWEI> display ipfpm dcp

Specification Information(Main Board):
 Max Instance Number                    : 512
 Max 10s Instance Number                : 512
 Max 1s Instance Number                 : 1
 Max TLP Number                         : 512
 Max TLP Number Per Instance            : 8

Configuration Information:
 DCP ID                                 : 10.1.1.1
 Loss-measure Flag                      : tos-bit6(default)
 Authentication Mode                    : --
 Test Instances MCP ID                  : 10.2.2.2
 Test Instances MCP Port                : 65030(default)
 Current Instance Number                : 1
```

Table 16-48 Description of the **display ipfpm dcp** command output

Item	Description
Specification Information(Main Board)	Specification information of the main board.
Max Instance Number	Maximum number of measurement instances supported.
Max 10s Instance Number	Maximum number of measurement instances at intervals of 10s.
Max 1s Instance Number	Maximum number of measurement instances at intervals of 1s.
Max TLP Number	Maximum number of TLPs supported.

Item	Description
Max TLP Number Per Instance	Maximum number of TLPs supported by each measurement instance.
Configuration Information	DCP configuration.
DCP ID	DCP ID. To configure this parameter, run the **dcp id** command.
Loss-measure Flag	Color bit used in packet loss measurement: ● tos-bit3: bit 3 in the ToS field ● tos-bit4: bit 4 in the ToS field ● tos-bit5: bit 5 in the ToS field ● tos-bit6: bit 6 in the ToS field ● tos-bit7: bit 7 in the ToS field ● flag-bit0: bit 0 in the Flags field To configure this parameter, run the **color-flag loss-measure** command.
Authentication Mode	Authentication mode on the DCP: ● hmac-sha256: HMAC-SHA256 encrypted authentication ● --: non-authentication To configure the authentication mode on a DCP, run the **authentication-mode** command.
Test Instances MCP ID	ID of the MCP corresponding to the DCP.
Test Instances MCP Port	UDP port number used by the DCP to communicate with the MCP.
Current Instance Number	Number of measurement instances.

16.5.12 display ipfpm mcp

Function

The **display ipfpm mcp** command displays the MCP configuration and status in the IP Flow Performance Measurement (FPM) system.

Format

display ipfpm mcp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the MCP configuration and status.

Example

Display the MCP configuration.

```
<HUAWEI> display ipfpm mcp
Specification Information:
 Max Instance Number                       :128
 Max DCP Number Per Instance               :128
 Max ACH Number Per Instance               :36
 Max TLP Number Per ACH                    :16

Configuration Information:
 MCP ID                                    :10.1.1.1
 Status                                    :Active
 Protocol Port                             :65030(default)
 Current Instance Number                   :1
```

Table 16-49 Description of the display ipfpm mcp command output

Item	Description
Specification Information	Specifications of the MCP.
Max Instance Number	Maximum number of measurement instances supported by the MCP.
Max DCP Number Per Instance	Maximum number of DCPs supported by each measurement instance on the MCP.
Max ACH Number Per Instance	Maximum number of ACHs supported by each measurement instance on the MCP.
Max TLP Number Per ACH	Maximum number of TLPs supported by ACH on the MCP.
Configuration Information	MCP configuration.
MCP ID	MCP ID. To set the MCP ID, run the **mcp id** command on the MCP.

Item	Description
Status	MCP status: - Active: The MCP works properly. - Deleting: The **undo nqa ipfpm mcp** command is being used to disable global MCP.
Protocol Port	UDP port number through which the DCP and MCP communicate with each other. To configure the UDP port number through which the DCP and MCP communicate with each other, run the **protocol udp port** command.
Current Instance Number	Total number of measurement instances.

16.5.13 display ipfpm statistic-type

Function

The **display ipfpm statistic-type** command displays packet loss statistics of a specified measurement instance in the IP Flow Performance Measurement (FPM) system.

Format

display ipfpm statistic-type loss instance *instance-id* [**ach** *ach-id*]

Parameters

Parameter	Description	Value
loss	Displays packet loss statistics.	-
instance *instance-id*	Displays packet loss statistics of a specified measurement instance.	The value is an integer that ranges from 1 to 16777214.
ach *ach-id*	Displays hop-by-hop performance statistics for an Atomic Closed Hop (ACH).	The value is an integer ranging from 1 to 2147483647.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The packet loss statistics of a specified measurement instance include the indicators such as the number of discarded packets, number of discarded bytes, and packet loss ratio. To view packet loss statistics of a specified measurement instance, run the **display ipfpm statistic-type** command.

To locate and diagnose network faults when network performance deteriorates, run the **display ipfpm statistic-type** command with **ach** configured to check statistics for a specified ACH.

Precautions

This command can be only executed on the MCP.

The first statistics record obtained through the IP FPM may be inaccurate, so do not use the first statistics record to determine network performance.

If the packet loss ratio is a negative value, the service packets may be unknown unicast packets or the color bits on devices participating in measurement may be different.

Example

Display packet loss statistics of measurement instance 1.

```
<HUAWEI> display ipfpm statistic-type loss instance 1
Latest loss statistics of forward flow:
Unit: p - packet, b - byte
------------------------------------------------------------------------------------------
 Period              Loss(p)              LossRatio(p)  Loss(b)             LossRatio(b)
------------------------------------------------------------------------------------------
 136118757           20                  20.000000% 2000                  20.000000%
 136118756           20                  20.000000% 2000                  20.000000%
 136118755           20                  20.000000% 2000                  20.000000%
 136118753           20                  20.000000% 2000                  20.000000%
 136118752           20                  20.000000% 2000                  20.000000%
 136118751           20                  20.000000% 2000                  20.000000%
 136118750           20                  20.000000% 2000                  20.000000%
 136118749           20                  20.000000% 2000                  20.000000%
 136118748           20                  20.000000% 2000                  20.000000%
 136118747           20                  20.000000% 2000                  20.000000%
 136118746           20                  20.000000% 2000                  20.000000%
 136118745           20                  20.000000% 2000                  20.000000%

Latest loss statistics of backward flow:
Unit: p - packet, b - byte
------------------------------------------------------------------------------------------
 Period              Loss(p)              LossRatio(p)  Loss(b)             LossRatio(b)
------------------------------------------------------------------------------------------
 136118757           20                  20.000000% 2000                  20.000000%
 136118756           20                  20.000000% 2000                  20.000000%
 136118755           20                  20.000000% 2000                  20.000000%
 136118753           20                  20.000000% 2000                  20.000000%
 136118752           20                  20.000000% 2000                  20.000000%
 136118751           20                  20.000000% 2000                  20.000000%
 136118750           20                  20.000000% 2000                  20.000000%
 136118749           20                  20.000000% 2000                  20.000000%
 136118748           20                  20.000000% 2000                  20.000000%
 136118747           20                  20.000000% 2000                  20.000000%
 136118746           20                  20.000000% 2000                  20.000000%
 136118745           20                  20.000000% 2000                  20.000000%
```

Table 16-50 Description of the **display ipfpm statistic-type** command output

Item	Description
Latest loss statistics of forward flow	-
Latest loss statistics of backward flow	-
Period	Measurement interval.
Loss(p)	Number of discarded packets.
LossRatio(p)	Packet loss ratio.
Loss(b)	Number of discarded bytes.
LossRatio(b)	Packet loss ratio of bytes.

16.5.14 display iplpm configuration brief

Function

The **display iplpm configuration brief** command displays the brief configuration of device-level packet loss measurement (including measurement on the entire device and direct link).

Format

display iplpm configuration brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view parameters of device-level packet loss measurement, run this command.

Example

Display the brief configuration of device-level packet loss measurement.

```
<HUAWEI> display iplpm configuration brief
Configuration information:
```

```
------------------------------------------------------------------
Loss-measure flag              : flags-bit0(default)
Global loss-measure interval(s) : 10(default)
Global loss-measure status      : disable
Global loss-measure alarm       : disable
Loss-measure board number       : 1
Loss-measure board list         : 0
Loss-measure port number        : 9
Loss-measure port list          : GigabitEthernet0/0/1
                                  GigabitEthernet0/0/2
                                  GigabitEthernet0/0/3
                                  GigabitEthernet0/0/4
                                  GigabitEthernet0/0/5
                                  GigabitEthernet0/0/6
                                  GigabitEthernet0/0/7
                                  GigabitEthernet0/0/8
                                  GigabitEthernet0/0/9
------------------------------------------------------------------
```

Table 16-51 Description of the display iplpm configuration brief command output

Item	Description
Configuration information	Configuration of device-level packet loss measurement.
Loss-measure flag	Color bit for packet loss measurement. To configure the color bit, run the **iplpm loss-measure color-flag** command. ● tos-bit6: bit 6 in the ToS field ● tos-bit7: bit 7 in the ToS field ● flags-bit0: bit 0 in the Flags field The value default indicates that the default color bit is used.
Global loss-measure interval(s)	Measurement interval of packet loss measurement on the device. To set the measurement interval, run the **iplpm global loss-measure interval** command. The value default indicates that the default measurement interval is used.
Global loss-measure status	Whether packet loss measurement on the device is enabled. To packet loss measurement for a device, run the **iplpm global loss-measure enable** command. ● enable ● disable
Global loss-measure alarm	Whether the alarm and clear alarm of packet loss ratio are enabled. To enable the alarm and clear alarm of packet loss ratio, run the **iplpm global loss-measure alarm enable** command. ● enable ● disable

Item	Description
Loss-measure board number	Number of devices that support device-level packet loss measurement.
Loss-measure board list	List of slot numbers of devices that support device-level packet loss measurement. The value -- indicates that no device supports device-level packet loss measurement.
Loss-measure port number	Number of interfaces where packet loss measurement for direct links is enabled.
Loss-measure port list	List of interfaces where packet loss measurement for direct links is enabled. The value -- indicates that no interface is enabled with packet loss measurement for direct links.

16.5.15 display iplpm loss-measure statistics global

Function

Run the **display iplpm loss-measure statistics global** command displays the packet loss measurement result on a device.

Format

display iplpm loss-measure statistics global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the packet loss measurement result on a device, including the number of discarded packets, packet loss ratio, and error information.

Example

Display the packet loss measurement result on a device.

```
<HUAWEI> display iplpm loss-measure statistics global
Latest global loss statistics:
```

```
-------------------------------------------------------------------------------
StartTime(DST)        Loss Packets          LossRatio        ErrorInfo
-------------------------------------------------------------------------------
2014-06-12 18:47:30   344127                4.513519%        OK
2014-06-12 18:47:20   381085                4.513196%        OK
2014-06-12 18:47:10   381192                4.513290%        OK
2014-06-12 18:47:00   381339                4.513341%        OK
2014-06-12 18:46:50   381465                4.513392%        OK
2014-06-12 18:46:40   381444                4.513487%        OK
2014-06-12 18:46:30   381129                4.513309%        OK
-------------------------------------------------------------------------------
```

Table 16-52 Description of the **display iplpm loss-measure statistics global** command output

Item	Description
Latest global loss statistics	Latest statistics about packet loss measurement on the device.
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Loss Packets	Number of discarded packets in the current measurement interval.
LossRatio	Packet loss ratio in the current measurement interval.
ErrorInfo	Error code about packet loss measurement in the current measurement interval: ● OK: There is no error, and the packet loss measurement result is normal. ● Incomplete: The statistics data is incomplete. The possible reason is the inter-chassis communication error. Part of statistics on the standby or slave switch cannot be sent to the master switch.

16.5.16 display iplpm loss-measure statistics history-record

Function

The **display iplpm loss-measure statistics history-record** command displays the historical records of packet loss measurement on a device and a direct link.

Format

display iplpm loss-measure statistics history-record { **global** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
global	Displays the historical records of packet loss measurement on a device.	-
interface *interface-type interface-number*	Displays the historical records of packet loss measurement on a direct link.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the measurement interval is 1s, 10s, or 60s, the system summarizes statistics results in each measurement interval every 5 minutes to obtain the maximum and minimum packet loss ratios within 5 minutes. When the measurement interval is 600s, the system summarizes statistics results in each measurement interval every 60 minutes to obtain the maximum and minimum packet loss ratios within 60 minutes. The system saves a maximum of four summarized records. You can run this command to view historical records.

Example

Display the historical records of packet loss measurement on a device.

```
<HUAWEI> display iplpm loss-measure statistics history-record global
Latest global history record(every 5 minutes):
-------------------------------------------------------------------------
 Record no                    : 29
 Period(DST)                  : 2014-03-19 16:20:10 to 2014-03-19 16:25:10
 Valid statistic data number    : 30
 Maximum loss ratio             : 0.000000%
 Minimum loss ratio             : 0.000000%
 Total loss packets             : 0
 Total receive packets          : 0

 Record no                    : 28
 Period(DST)                  : 2014-03-19 16:15:10 to 2014-03-19 16:20:10
 Valid statistic data number    : 30
 Maximum loss ratio             : 0.000000%
 Minimum loss ratio             : 0.000000%
 Total loss packets             : 0
 Total receive packets          : 0

 Record no                    : 27
 Period(DST)                  : 2014-03-19 16:10:10 to 2014-03-19 16:15:10
 Valid statistic data number    : 30
 Maximum loss ratio             : 0.000000%
 Minimum loss ratio             : 0.000000%
 Total loss packets             : 0
 Total receive packets          : 0
```

```
 Record no                    : 26
 Period(DST)                  : 2014-03-19 16:05:10 to 2014-03-19 16:10:10
 Valid statistic data number    : 30
 Maximum loss ratio             : 0.000000%
 Minimum loss ratio             : 0.000000%
 Total loss packets             : 0
 Total receive packets          : 0

--------------------------------------------------------------------------
```

Display the historical records of packet loss measurement on a direct link of GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics history-record interface gigabitethernet 0/0/1
Latest history record of interface GigabitEthernet0/0/1(every 5 minutes):
------------------------------------------------------------------------------
 Record no                    : 29
 Period(DST)                  : 2014-03-19 16:20:10 to 2014-03-19 16:25:10
 Valid statistic data number    : 30
 Maximum forward loss ratio     : 0.000000%
 Minimum forward loss ratio     : 0.000000%
 Total forward loss packets     : 0
 Total forward receive packets  : 0
 Maximum backward loss ratio    : 20.000000%
 Minimum backward loss ratio    : 19.980020%
 Total backward loss packets    : 6000
 Total backward receive packets : 30001

 Record no                    : 28
 Period(DST)                  : 2014-03-19 16:15:10 to 2014-03-19 16:20:10
 Valid statistic data number    : 30
 Maximum forward loss ratio     : 0.000000%
 Minimum forward loss ratio     : 0.000000%
 Total forward loss packets     : 0
 Total forward receive packets  : 0
 Maximum backward loss ratio    : 20.079920%
 Minimum backward loss ratio    : 19.980020%
 Total backward loss packets    : 6001
 Total backward receive packets : 30003

 Record no                    : 27
 Period(DST)                  : 2014-03-19 16:10:10 to 2014-03-19 16:15:10
 Valid statistic data number    : 30
 Maximum forward loss ratio     : 0.000000%
 Minimum forward loss ratio     : 0.000000%
 Total forward loss packets     : 0
 Total forward receive packets  : 0
 Maximum backward loss ratio    : 20.039880%
 Minimum backward loss ratio    : 19.960080%
 Total backward loss packets    : 6001
 Total backward receive packets : 30005

 Record no                    : 26
 Period(DST)                  : 2014-03-19 16:05:10 to 2014-03-19 16:10:10
 Valid statistic data number    : 30
 Maximum forward loss ratio     : 0.000000%
 Minimum forward loss ratio     : 0.000000%
 Total forward loss packets     : 0
 Total forward receive packets  : 0
 Maximum backward loss ratio    : 20.059880%
 Minimum backward loss ratio    : 19.980020%
 Total backward loss packets    : 6001
 Total backward receive packets : 30004
-----------------------------------------------------------------------------------
```

Table 16-53 Description of the **display iplpm loss-measure statistics history-record** command output

Item	Description
Latest global history record(every 5 minutes)	Latest statistics about packet loss measurement in every five minutes on the device.
Latest history record of interface *x* (every 5 minutes)	Latest statistics about packet loss measurement on a direct link of the *x* interface in every five minutes.
Record no	Historical record ID.
Period(DST)	Time historical records were generated (standard DST).
Valid statistic data number	Number of valid historical statistics records.
Maximum loss ratio	Maximum packet loss ratio of the device.
Minimum loss ratio	Minimum packet loss ratio of the device.
Total loss packets	Total number of packets discarded by the device.
Total receive packets	Total number of packets received by the device.
Maximum forward loss ratio	Maximum packet loss ratio of a forward flow (a forward flow is sent by the local device interface and received by the remote device interface).
Minimum forward loss ratio	Minimum packet loss ratio of a forward flow.
Total forward loss packets	Total number of discarded packets of a forward flow.
Total forward receive packets	Total number of received packets (including the number of discarded packets) of a forward flow.
Maximum backward loss ratio	Maximum packet loss ratio of a backward flow (a backward flow is sent by the remote device interface and received by the local device interface).
Minimum backward loss ratio	Minimum packet loss ratio of a backward flow.
Total backward loss packets	Total number of discarded packets of a backward flow.
Total backward receive packets	Total number of received packets (including the number of discarded packets) of a backward flow.

16.5.17 display iplpm loss-measure statistics interface

Function

The **display iplpm loss-measure statistics interface** command displays the packet loss measurement result on the direct link of a specified interface.

Format

display iplpm loss-measure statistics interface *interface-type interface-number* [**forward** | **backward**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the packet loss measurement result on the direct link of a specified interface.	-
forward	Displays the packet loss measurement result of a forward flow on the direct link of a specified interface. A forward flow is sent by the local device interface and received by the remote device interface.	-
backward	Displays the packet loss measurement result of a backward flow on the direct link of a specified interface. A backward flow is sent by the remote device interface and received by the local device interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the packet loss measurement result in the forward and backward directions, including the number of discarded packets and packet loss ratio.

Example

Display the packet loss measurement result on the direct link of GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics interface gigabitethernet 0/0/1
Latest forward loss statistics of interface GigabitEthernet0/0/1:
--------------------------------------------------------------------------------------------------------

 StartTime(DST)        Forward Loss Packets  Forward LossRatio
ErrorInfo
--------------------------------------------------------------------------------------------------------
```

```
 2014-03-19 15:50:50    200               19.980020%        OK
 2014-03-19 15:50:40    200               20.000000%        OK
 2014-03-19 15:50:30    200               19.980020%        OK
 2014-03-19 15:50:20    200               20.020020%        OK
 2014-03-19 15:50:10    200               20.000000%        OK
 2014-03-19 15:50:00    200               19.980020%        OK
--------------------------------------------------------------------------------------------------------
Latest backward loss statistics of interface
GigabitEthernet0/0/1:
---------------------------------------------------------------------------------------------------------

 StartTime(DST)        Backward Loss Packets  Backward LossRatio
ErrorInfo
---------------------------------------------------------------------------------------------------------

 2014-03-19 15:50:50    0                  0.000000%         OK
 2014-03-19 15:50:40    0                  0.000000%         OK
 2014-03-19 15:50:30    0                  0.000000%         OK
 2014-03-19 15:50:20    0                  0.000000%         OK
 2014-03-19 15:50:10    0                  0.000000%         OK
 2014-03-19 15:50:00    0                  0.000000%         OK
------------------------------------------------------------------------------------------------------------
```

Table 16-54 Description of the **display iplpm loss-measure statistics interface** command output

Item	Description
Latest forward loss statistics of interface *x*	Latest statistics about packet loss measurement of a forward target flow on the direct link of the *x* interface (a forward flow is sent by the local device interface and received by the remote device interface).
Latest backward loss statistics of interface *x*	Latest statistics about packet loss measurement of a backward target flow on the direct link of the *x* interface (a backward flow is sent by the remote device interface and received by the local device interface).
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Forward Loss Packets	Number of discarded packets of a forward flow in the current measurement interval.
Forward LossRatio	Packet loss ratio of a forward flow in the current measurement interval.
Backward Loss Packets	Number of discarded packets of a backward flow in the current measurement interval.
Backward LossRatio	Packet loss ratio of a backward flow in the current measurement interval.

Item	Description
ErrorInfo	Error code about packet loss measurement in the current measurement interval: - Init: The device is in initialized state and there is no statistics data. - OK: There is no error, and the packet loss measurement result is normal. - NoRecvData: The local end does not receive statistics data from the remote end. The possible causes may be that the packet loss measurement on a direct link is not enabled on the remote device or the direct link becomes faulty or there is a forwarding node on the link. - DataErr: The local end receives error statistics data from the remote end. - DiffAuth: The authentication modes or passwords on both ends are different. - DiffIntvl: The measurement intervals on both ends are different. - ASynClock: The time on both ends is asynchronous. When this code occurs, check the NTP configuration. - PortIsDown: The interface is Down.

16.5.18 display iplpm loss-measure statistics port-flow interface

Function

The **display iplpm loss-measure statistics port-flow interface** command displays statistics about discarded packets on an interface.

Format

display iplpm loss-measure statistics port-flow interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics about discarded packets on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you find packet loss on an interface in the packet loss measurement result on the direct link in the **display iplpm loss-measure statistics interface** command output, you can run the **display iplpm loss-measure statistics port-flow interface** command to check the statistics data. Then you can check whether the fault on the local interface causes packet loss.

Example

Display statistics about discarded packets on GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics port-flow interface gigabitethernet 0/0/1
Latest port loss statistics of interface GigabitEthernet0/0/1:
--------------------------------------------------------------------------------
 StartTime(DST)         Output Packets Loss Ratio     Input Packets Loss Ratio
--------------------------------------------------------------------------------
 2014-04-01 18:09:40    0.000000%                   0.000000%
 2014-04-01 18:09:30    0.000000%                   0.000000%
 2014-04-01 18:09:20    0.000000%                   0.000000%
 2014-04-01 18:09:10    0.000000%                   0.000000%
---------------------------------------------------------------------------------
```

Table 16-55 Description of the **display iplpm loss-measure statistics port-flow interface** command output

Item	Description
Latest port loss statistics of interface *x*	Latest statistics about packet loss measurement on the *x* interface.
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Output Packets Loss Ratio	Packet loss rate of packets sent from the local interface and received by the peer interface during the current statistics interval.
Input Packets Loss Ratio	Packet loss rate of packets sent from the peer interface and received by the local interface during the current statistics interval.

16.5.19 display iplpm loss-measure statistics qos-queue interface

Function

The **display iplpm loss-measure statistics qos-queue interface** command displays statistics about sent packets in QoS queues on an interface.

Format

display iplpm loss-measure statistics qos-queue interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics about sent packets in QoS queues on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you find packet loss on an interface in the packet loss measurement result on the direct link in the **display iplpm loss-measure statistics interface** command output, you can run the **display iplpm loss-measure statistics qos-queue interface** command to check the statistics about sent packets in QoS queues on an interface. Then you can check whether congestion in queues causes packet loss.

Example

Display statistics about sent packets in QoS queues on GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics qos-queue interface gigabitethernet 0/0/1
Latest qos queue loss statistics of interface
GigabitEthernet0/0/1:
-------------------------------------------------------------------------------

StartTime(DST): 2014-03-19 16:25:10
 Queue0   : 0.000000%          Queue1: 0.000000%
 Queue2   : 0.000000%          Queue3: 0.000000%
 Queue4   : 0.000000%          Queue5: 0.000000%
 Queue6   : 0.000000%          Queue7: 0.000000%
 UserQueue: 0.000000%

StartTime(DST): 2014-03-19 16:25:00
 Queue0   : 0.000000%          Queue1: 0.000000%
```

```
Queue2   : 0.000000%          Queue3: 0.000000%
Queue4   : 0.000000%          Queue5: 0.000000%
Queue6   : 0.000000%          Queue7: 0.000000%
UserQueue: 0.000000%

--------------------------------------------------------------------------------
```

Table 16-56 Description of the display iplpm loss-measure statistics qos-queue interface command output

Item	Description
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Queue0-Queue7	Packet loss ratios of queues 0 to 7 in the measurement interval, which is used for reference only.
UserQueue	Packet loss ratio of the subscriber queue on the interface in the current measurement interval. The value of this field can be obtained only when HQoS is configured, and is used for reference only.

16.5.20 flow (IPFPM-DCP instance view)

Function

The **flow** command configures a target flow in a measurement instance on a DCP.

The **undo flow** command deletes the target flow from a measurement instance on a DCP.

By default, no target flow is configured in a measurement instance on a DCP.

Format

Define a unidirectional flow.

- When the protocol of a target flow is TCP or UDP, run the following command:

  flow { **forward** | **backward** } { **protocol** { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] } *

- When the protocol of a target flow is not TCP or UDP, run the following command:

  flow { **forward** | **backward** } { **protocol** *protocol-number* | **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] } *

Define a bidirectional symmetrical flow.

- When the protocol of a target flow is TCP or UDP, run the following command:

  flow bidirectional { **protocol** { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] } *

- When the protocol of a target flow is not TCP or UDP, run the following command:

  flow bidirectional { **protocol** *protocol-number* | **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] } *

Cancel the configured target flow.

undo flow { **forward** | **backward** | **bidirectional** }

Parameters

Parameter	Description	Value
forward	Indicates the forward flow.	-
backward	Indicates the backward flow.	-
protocol { **tcp** | **udp** }	Indicates that the protocol of a target flow is TCP or UDP.	-
source-port *src-port-number1*	Specifies the start source port number of a target flow.	The value is an integer that ranges from 1 to 65535.
src-port-number2	Specifies the end source port number of a target flow.	The value is an integer that ranges from 1 to 65535. *src-port-number2* must be larger than *src-port-number1*.
destination-port *dest-port-number1*	Specifies the start destination port number of a target flow.	The value is an integer that ranges from 1 to 65535.
dest-port-number2	Specifies the end destination port number of a target flow.	The value is an integer that ranges from 1 to 65535. *dest-port-number2* must be larger than *dest-port-number1*.
dscp *dscp-value*	Specifies the value of a Differentiated Services CodePoint (DSCP) of a target flow.	The value is an integer that ranges from 0 to 63.
source *src-ip-address*	Specifies the source IP address of a target flow. Only unicast IP addresses are supported.	The value is in dotted decimal notation.

Parameter	Description	Value
src-mask-length	Specifies the mask length of the source IP address of a target flow.	The value is an integer that ranges from 1 to 32.
destination *dest-ip-address*	Specifies the destination IP address of a target flow. Only unicast IP addresses are supported.	The value is in dotted decimal notation.
dest-mask-length	Specifies the mask length of the destination IP address of a target flow.	The value is an integer that ranges from 1 to 32.
protocol *protocol-number*	Specifies the protocol type of a target flow.	The value is an integer ranging from 1 to 5, 7 to 16, or 18 to 255. **NOTE** The value 6 indicates TCP and the value 17 indicates UDP.
bidirectional	Indicates the bidirectional symmetrical flow. **NOTE** If the target flow is symmetrical bidirectional, set *src-ip-address* to specify a source IP address and *dest-ip-address* to specify a destination IP address for the target flow.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The target flow must be specified before each measurement.

A target flow is the objective in iPCA measurement, and can be defined by any combinations of source IP address, destination IP address, protocol type, DSCP value, source port number, and destination port number. Specifying more attributes can make the target flow accurate. Therefore, it is recommended that you specify more attributes to improve precision of measurement results.

Precautions

An instance can have only one target flow configured, either unidirectional or bidirectional. A bidirectional target flow is logically two unidirectional flows in opposite directions.

- If the target flow in an instance is unidirectional, you can specify **forward** to configure a forward flow or **backward** to configure a backward flow.
- If the target flow in an instance is bidirectional, two situations are available:
  - If the bidirectional target flow is symmetrical, you can specify **bidirectional** to configure the bidirectional target flow characteristics, and you must specify the source and destination IP addresses. By default, the characteristics specified are used for the forward flow, and the reverse of those are used for the backward flow. Specifically, the source and destination IP addresses and port numbers specified for the forward flow are used respectively as the destination and source IP addresses and port numbers for the backward flow.
  - If the bidirectional target flow is asymmetrical, you must configure **forward** and **backward** in two command instances to configure the forward and backward flow characteristics.

Target flows in different IP FPM instances cannot have the same characteristics. The forward and backward target flows in an IP FPM instance cannot have the same characteristics neither.

Example

Configure a target flow of measurement instance 1 on a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] flow bidirectional protocol udp source-port 1025 source 10.1.1.1
destination 10.2.2.2
```

16.5.21 flow (IPFPM-MCP-ACH view)

Function

The **flow** command configures the target flow direction in the Atomic Closed Hop (ACH) view.

The **undo flow** command deletes the target flow direction in the ACH view.

By default, no direction is configured for target flows in the ACH view.

Format

flow { **forward** | **backward** }

undo flow

Parameters

Parameter	Description	Value
forward	Indicates the forward target flow.	-
backward	Indicates the backward target flow.	-

Views

IPFPM-MCP-ACH view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **flow** command in IP FPM hop-by-hop performance statistics scenarios.

Prerequisites

The **ach** command has been run to create an ACH and display the ACH view.

Example

Configure the forward target flow in the ACH view.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
[HUAWEI-nqa-ipfpm-mcp-instance-1-ach-1] flow forward
```

16.5.22 in-group

Function

The **in-group** command creates a Target Logical Port (TLP) in-group for the target flow.

The **undo in-group** command deletes a TLP in-group or deletes a TLP from a TLP in-group.

By default, no TLP in-group is configured for the target flow.

Format

in-group dcp *dcp-id* **tlp** *tlp-id*

undo in-group [**dcp** *dcp-id* **tlp** *tlp-id*]

Parameters

Parameter	Description	Value
dcp *dcp-id*	Specifies a DCP to which TLPs in a TLP in-group belongs.	This value is in dotted decimal notation.
tlp *tlp-id*	Indicates a TLP in a TLP in-group.	The value is an integer ranging from 1 to 16777215.

Views

IPFPM-MCP-ACH view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IP FPM hop-by-hop performance statistics scenarios, a hop is a set of links and interfaces that service packets travel through, from one measurement point or group to the next measurement point or group, and therefore is represented by (TLP in-group, TLP out-group). Performance statistics are implemented on the TLP in-point or in-group through which service packets enter a network and the TLP out-point or out-group through which service packets leave the network.

Prerequisites

The **ach** command has been run to create an ACH and display the ACH view.

Example

Create a TLP in-group for the target flow.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
[HUAWEI-nqa-ipfpm-mcp-instance-1-ach-1] in-group dcp 10.1.1.1 tlp 100
```

16.5.23 instance (IPFPM-DCP view)

Function

The **instance** command creates an IPFPM-DCP instance and displays the IPFPM-DCP instance view, or directly displays the view of an existing IPFPM-DCP instance.

The **undo instance** command deletes an IPFPM-DCP instance.

By default, no IPFPM-DCP instance is created on a DCP.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IPFPM-DCP instance.	The value is an integer that ranges from 1 to 8355838.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCP collects statistics data based on measurement instances. Each measurement instance consists of the target flow, TLP, and measurement interval. The MCP reports measurement results based on measurement instances. The MCP summarizes and analyzes statistics data of the same measurement instance on all DCPs, and reports measurement results of target flows.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Follow-up Procedure

Run the **flow** command to configure a target flow, run the **tlp** command to configure the TLPs of the measurement instance, and run the **interval** command to configure the measurement interval.

Precautions

To measure packet loss for a specified service flow, create the same measurement instance on the MCP and DCP.

Example

Create IPFPM-DCP instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
```

16.5.24 instance (IPFPM-MCP view)

Function

The **instance** command creates an IPFPM-MCP instance and displays the IPFPM-MCP instance view, or directly displays the view of an existing IPFPM-MCP instance.

The **undo instance** command deletes an IPFPM-MCP instance.

By default, no IPFPM-MCP instance is created on the MCP.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IPFPM-MCP instance.	The value is an integer that ranges from 1 to 8355838.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCP collects statistics data based on measurement instances. Each measurement instance consists of the target flow, TLP, and measurement interval. The MCP reports measurement results based on measurement instances. The MCP summarizes and analyzes statistics data of the same measurement instance on all DCPs, and reports measurement results of target flows.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

To measure packet loss for a specified service flow, create the same measurement instance on the MCP and DCP.

Example

Create IPFPM-MCP instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
```

16.5.25 interval (IPFPM-DCP instance view)

Function

The **interval** command sets the measurement interval of a measurement instance on a DCP.

The **undo interval** command restores the default measurement interval of a measurement instance on a DCP.

By default, the measurement interval of a measurement instance on a DCP is 10 seconds.

Format

interval *interval*

undo interval

Parameters

Parameter	Description	Value
interval	Specifies the measurement interval of a measurement instance on a DCP.	The value is of the enumerated type and can be 1, 10, 60, or 600, in seconds.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The measurement interval of a measurement instance on a DCP is the interval at which a TLP collects statistics on packets or bytes and records the timestamp of packet receiving or sending. It is also the interval at which a DCP reports statistics data to the MCP. A shorter interval indicates a higher frequency at which a DCP reports statistics data to the MCP, so the interval adjustment affects the performance of the DCP and MCP.

Considering factors such as the clock synchronization offset, maximum transmission delay, and device performance, you can run this command to change the measurement interval.

Precautions

The measurement intervals of the same measurement instances on all DCPs must be the same; otherwise, the statistics data will be empty.

The measurement interval of a measurement instance cannot be changed when the measurement instance is running. If the measurement interval of a running measurement instance is changed, the statistics reported by MCP may be inaccurate. To change the measurement interval, run the **measure disable** command in the IPFPM-MCP instance view to disable the measurement, and then run the **measure enable** command to enable the measurement.

Example

Set the measurement interval of measurement instance 1 to 60s.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] interval 60
```

16.5.26 ipfpm tlp

Function

The **ipfpm tlp** command binds a Target Logical Port (TLP) to an interface in a measurement instance on a DCP.

The **undo ipfpm tlp** command unbinds a TLP from an interface in a measurement instance on a DCP.

By default, an interface is not bound to a TLP in a measurement instance on a DCP.

Format

ipfpm tlp *tlp-id*

undo ipfpm tlp { *tlp-id* | **all** }

Parameters

Parameter	Description	Value
tlp-id	Specifies the ID of a TLP.	The value is an integer that ranges from 1 to 16777215.
all	Cancels the binding between all TLPs and interfaces.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing packet loss measurement, run this command to bind a TLP to an interface.

Prerequisites

A Layer 2 or Layer 3 interface can be bound to a TLP. You can run the **undo portswitch** command to switch the interface to Layer 3 mode.

Precautions

A TLP can be bound to only one interface on the DCPs associated with an MCP, and an interface can bound only one TLP.

Example

Bind GE0/0/1 to TLP 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipfpm tlp 100
```

16.5.27 iplpm global loss-measure alarm enable

Function

The **iplpm global loss-measure alarm enable** command enables the alarm and clear alarm of the packet loss ratio for device-level packet loss measurement.

The **undo iplpm global loss-measure alarm enable** command restores the default setting.

By default, the alarm and clear alarm of the packet loss ratio are disabled.

Format

iplpm global loss-measure alarm enable

undo iplpm global loss-measure alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After this command is used, the alarm threshold and clear alarm threshold of the packet loss ratio are 5% and 1%.

- If the packet loss ratio in five consecutive measurement intervals exceeds the alarm threshold, the device reports the hwIpfpmLossRatioExceed alarm to the NMS to notify the link fault in real time.
- If the packet loss ratio in five consecutive measurement intervals falls below or is equivalent to the clear alarm threshold, the device reports the hwIpfpmLossRatioRecovery alarm to the NMS to notify link recovery in real time.

Example

Enable the alarm and clear alarm of the packet loss ratio for device-level packet loss measurement.

```
<HUAWEI> system-view
[HUAWEI] iplpm global loss-measure alarm enable
```

16.5.28 iplpm global loss-measure enable

Function

The **iplpm global loss-measure enable** command enables packet loss measurement for a device.

The **undo iplpm global loss-measure enable** command disables packet loss measurement for a device.

By default, packet loss measurement for a device is disabled.

Format

iplpm global loss-measure enable

undo iplpm global loss-measure enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To measure the packet loss of a switch, run this command to enable packet loss measurement for the switch.

Example

Enable packet loss measurement for a device.

```
<HUAWEI> system-view
[HUAWEI] iplpm global loss-measure enable
```

16.5.29 iplpm global loss-measure interval

Function

The **iplpm global loss-measure interval** command configures the device-level packet loss measurement interval.

The **undo iplpm global loss-measure interval** command restores the default device-level packet loss measurement interval.

By default, the device-level packet loss measurement interval is 10s.

Format

iplpm global loss-measure interval *interval*

undo iplpm global loss-measure interval

Parameters

Parameter	Description	Value
interval	Specifies the device-level packet loss measurement interval.	The value is of the enumerated type and can be 1, 10, 60, or 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device-level packet loss measurement interval refers to the period from received packet statistics collection to sent packet statistics collection. To ensure accuracy of statistics data, run the **undo iplpm global loss-measure enable** command to disable device-level packet loss measurement in the system view before changing the measurement interval.

Example

Set the device-level packet loss measurement interval to 60s.

```
<HUAWEI> system-view
[HUAWEI] iplpm global loss-measure interval 60
```

16.5.30 iplpm link authentication-mode

Function

The **iplpm link authentication-mode** command configures the authentication mode and password for packet loss measurement on a direct link.

The **undo iplpm link authentication-mode** command deletes the authentication mode and password.

By default, no authentication mode or password is configured for packet loss measurement on a direct link.

Format

iplpm link authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo iplpm link authentication-mode

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to authenticate packets between devices.	-
key-id *key-id*	Specifies the ID of the authentication password.	The value is an integer that ranges from 1 to 64.
cipher	Specifies the cipher-text authentication password.	-
password	Specifies the authentication password.	The value is a character string without spaces. ● The value is a string of 1 to 255 characters in plain text. ● The value is a string of 32 to 392 characters in cipher text.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After packet loss measurement is configured on a direct link, statistics data on received and sent packets on an interface at one end is sent to an interface at the other end and summarized for packet loss measurement. This command is used to authenticate communication packets on the direct link, improving security.

Precautions

- When the authentication mode and password are configured on an interface, packets encapsulated with local statistics data sent from the interface are authenticated. Therefore, both interfaces of the direct link must be configured with the same authentication mode and password.
- For security purposes, it is recommended that the authentication password contain at least 16 characters.

Example

Set the authentication mode to hmac-sha256 and password to **YsHsjx_202206** in cipher text for packet loss measurement on a direct link on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link authentication-mode hmac-sha256 key-id 1 cipher
YsHsjx_202206
```

16.5.31 iplpm link loss-measure alarm enable

Function

The **iplpm link loss-measure alarm enable** command enables the alarm and clear alarm of the packet loss ratio for packet loss measurement on a direct link.

The **undo iplpm link loss-measure alarm enable** command restores the default setting.

By default, the packet loss alarm and clear alarm are disabled for packet loss measurement on a direct link.

Format

iplpm link loss-measure alarm enable

undo iplpm link loss-measure alarm enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

After this command is used, the alarm threshold and clear alarm threshold of the packet loss ratio are 5% and 1%.

- If the packet loss ratio in five consecutive measurement intervals exceeds the alarm threshold, the device reports the hwIpfpmLossRatioExceed alarm to the NMS to notify the link fault in real time.
- If the packet loss ratio in five consecutive measurement intervals falls below the clear alarm threshold, the device reports the hwIpfpmLossRatioRecovery alarm to the NMS to notify link recovery in real time.

Example

On the GE0/0/1, enable the alarm and clear alarm of the packet loss ratio for packet loss measurement on a direct link.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link loss-measure alarm enable
```

16.5.32 iplpm link loss-measure enable

Function

The **iplpm link loss-measure enable** command enables packet loss measurement on the direct link.

The **undo iplpm link loss-measure enable** command disables packet loss measurement on the direct link.

By default, packet loss measurement is disabled on the direct link.

Format

iplpm link loss-measure enable

undo iplpm link loss-measure enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

To accurately locate packet loss on a link, run the **iplpm link loss-measure enable** command to enable packet loss measurement on the direct link between two devices.

This function must be enabled on both device interfaces of the direct link.

Example

On the GE0/0/1, enable packet loss measurement on the direct link.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link loss-measure enable
```

16.5.33 iplpm link loss-measure interval

Function

The **iplpm link loss-measure interval** command configures the interval for packet loss measurement on the direct link.

The **undo iplpm link loss-measure interval** command restores the default interval for packet loss measurement on the direct link.

By default, the interval for packet loss measurement on the direct link is 10s.

Format

iplpm link loss-measure interval *interval*

undo iplpm link loss-measure interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for packet loss measurement on the direct link.	The value is an integer that can be 1, 10, 60, or 600, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

The interval for packet loss measurement on the direct link refers to the period from received packet statistics collection to sent packet statistics collection on a specified interface. To ensure accuracy of statistics data, run the **undo iplpm link loss-measure enable** command to disable packet loss measurement on the direct link in the interface view before changing the measurement interval.

Example

On the GE0/0/1, set the interval for packet loss measurement on the direct link to 60s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link loss-measure interval 60
```

16.5.34 iplpm loss-measure color-flag

Function

The **iplpm loss-measure color-flag** command configures the color bit used in device-level packet loss measurement.

The **undo iplpm loss-measure color-flag** command restores the default color bit used in device-level packet loss measurement.

By default, bit 0 in the Flags field is used as the color bit for device-level packet loss measurement. The default configuration is recommended.

Format

iplpm loss-measure color-flag { **tos-bit** *tos-bit* | **flags-bit0** }

undo iplpm loss-measure color-flag

Parameters

Parameter	Description	Value
tos-bit *tos-bit*	Specifies bit 6 or 7 in the ToS field of IP packets as the color bit for device-level packet loss measurement.	The value is 6 or 7.
flags-bit0	Specifies bit 0 in the Flags field of IP packets as the color bit for device-level packet loss measurement.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Device-level packet loss measurement contains measurement on the entire device and direct link. Before deploying Packet Conservation Algorithm for Internet (iPCA) to implement device-level packet loss measurement, run this command to configure the color bit. You can select a color bit according to the actual situation and network planning.

Precautions

Before changing the color bit for device-level packet loss measurement, run the **undo iplpm global loss-measure enable** command in the system view to disable device-level packet loss measurement. If packet loss measurement is configured on the direct link, run the **undo iplpm link loss-measure enable** command in the interface view to disable packet loss measurement on the direct link and ensure that the color bits on both devices of the direct link are changed to be the same.

When both network-level and device-level packet loss measurements are enabled on a device, the color bits must be differentiated.

Example

Configure bit 7 in the ToS field as the color bit for device-level packet loss measurement.

```
<HUAWEI> system-view
[HUAWEI] iplpm loss-measure color-flag tos-bit 7
```

16.5.35 loss-measure enable

Function

The **loss-measure enable** command enables statistics collection based on the time range for a measurement instance on a DCP.

The **undo loss-measure enable** command disables statistics collection for a measurement instance on a DCP.

By default, statistics collection based on the time range is disabled for a measurement instance on a DCP.

Format

loss-measure enable [**mid-point**] [**time-range** *time-range*]

undo loss-measure enable [[**mid-point**] **time-range** [*time-range*]]

Parameters

Parameter	Description	Value
mid-point	Enables on-demand packet loss measurement for mid-points. If this parameter is configured, on-demand packet loss measurement is enabled for all mid-points. If this parameter is not configured, on-demand packet loss measurement is enabled for all measurement points. **NOTE** The mid-point is only applied to hop-by-hop measurement.	-
time-range *time-range*	Specifies the time range for statistics collection.	The value is 5, 10, 15, or 30, in minutes. The default value is 10 minutes.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP FPM performance statistics serve as a reliable reference for assessing IP network performance and therefore are useful for fault diagnosis and service statistics. To monitor on-demand packet loss performance in a specified period or diagnose network faults and locate faulty nodes when network performance deteriorates, run the **loss-measure enable** command.

Prerequisites

An IP FPM model has been established, including configuring a DCP and MCP, binding a TLP to a physical interface, and creating a target flow and IP FPM instance.

Precautions

This command is not recorded in the configuration file after being executed.

After device restart, statistics collection based on the time range becomes invalid, and needs to be reconfigured.

Statistics collection based on the time range and continual statistics collection cannot be enabled simultaneously.

Example

Enable statistics collection based on the time range for a measurement instance on a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] loss-measure enable time-range 30
```

16.5.36 loss-measure enable continual

Function

The **loss-measure enable continual** command enables continual statistics collection for a measurement instance on a DCP.

The **undo loss-measure enable continual** command disables continual statistics collection for a measurement instance on a DCP.

By default, continual statistics collection is disabled for a measurement instance on a DCP.

Format

loss-measure enable continual

undo loss-measure enable continual

Parameters

None

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you are unaware of network performance degrading and want to continuously monitor packet loss on the network, run the **loss-measure enable continual** command to enable continual statistics collection.

Prerequisites

An IP FPM model has been established, including configuring a DCP and MCP, binding a TLP to a physical interface, and creating a target flow and IP FPM instance.

Precautions

Continual statistics collection and statistics collection based on the time range cannot be enabled simultaneously.

Example

Enable continual statistics collection for a measurement instance on a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] loss-measure enable continual
```

16.5.37 loss-measure ratio-threshold

Function

The **loss-measure ratio-threshold** command configures the alarm and clear alarm thresholds of the packet loss ratio for a measurement instance on the MCP.

The **undo loss-measure ratio-threshold** command restores the default setting.

By default, the alarm and clear alarm thresholds of the packet loss ratio are not configured for a measurement instance on the MCP. That is, no alarm is generated for packet loss.

Format

loss-measure ratio-threshold upper-limit *upper-limit* **lower-limit** *lower-limit*

undo loss-measure ratio-threshold

Parameters

Parameter	Description	Value
upper-limit *upper-limit*	Specifies the alarm threshold for the packet loss ratio.	The value is a string of 1 to 10 digits and in the range of 0.000001 to 100. The value is accurate to six decimal places, in percentage.
lower-limit *lower-limit*	Specifies the clear alarm threshold for the packet loss ratio.	The value is a string of 1 to 10 digits and in the range of 0.000001 to 100. The value is accurate to six decimal places, in percentage. *lower-limit* must be smaller than or equal to *upper-limit*.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm and clear alarm thresholds of the packet loss ratio are configured for a measurement instance on the MCP:

- If the packet loss ratio in five consecutive measurement intervals exceeds the alarm threshold, the MCP reports the hwIpfpmLossRatioExceed alarm to the NMS to notify the link fault in real time.
- If the packet loss ratio in five consecutive measurement intervals falls below the clear alarm threshold, the MCP reports the hwIpfpmLossRatioRecovery alarm to the NMS to notify link recovery in real time.

To facilitate operation and maintenance, you are advised to run this command to configure the alarm and clear alarm thresholds of the packet loss ratio for a measurement instance on the MCP according to network performance.

Precautions

If you run the **loss-measure ratio-threshold** command multiple times, only the latest configuration takes effect.

This command only configures the alarm and clear alarm thresholds of the packet loss ratio for a measurement instance on the MCP. The hwIpfpmLossRatioExceed and hwIpfpmLossRatioRecovery alarms are triggered only when the alarm and clear alarm functions are enabled and the packet loss ratio in five consecutive measurement intervals reaches the threshold.

Example

Set the alarm and clear alarm thresholds of the packet loss ratio to 10% and 5.5% for measurement instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] loss-measure ratio-threshold upper-limit 10 lower-limit 5.5
```

16.5.38 mcp (IPFPM-DCP view)

Function

The **mcp** command associates the MCP ID with all measurement instances of a DCP.

The **undo mcp** command disassociates the MCP ID from all measurement instances of a DCP.

By default, no MCP ID is associated with a measurement instance of a DCP.

Format

mcp *mcp-id* [**port** *port-number*] [**vpn-instance** *vpn-instance-name* | **net-manager-vpn**]

undo mcp

Parameters

Parameter	Description	Value
mcp-id	Specifies the MCP ID associated with all measurement instances of a DCP. It is recommended that you configure the router ID of the device as the MCP ID.	The value is in dotted decimal notation.
port *port-number*	Specifies the UDP port number through which the DCP and MCP communicate with each other.	The value is an integer that ranges from 1024 to 65535. The default value is 65030 and is recommended.
vpn-instance *vpn-instance-name*	Specifies the VPN instance where the DCP and MCP communicate with each other.	The value must be an existing VPN instance name.
net-manager-vpn	Specifies the manager VPN where the DCP and MCP communicate with each other.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the IP Flow Performance Measurement (FPM) system, each measurement instance belongs to an MCP. Before a DCP sends statistics data of a measurement instance from TLPs to the MCP, you must associate the MCP ID with the measurement instance. The **mcp** command associates the MCP ID with all measurement instances of a DCP.

A DCP encapsulates statistics data collected from Target Logical Ports (TLPs) and MCP ID associated with all measurement instances on the DCP in a packet, and sends the packet with the MCP ID as the destination IP address. After receiving the packet sent from the DCP, the MCP compares the MCP ID in the packet with the MCP ID configured by the **mcp id** command:

- If the two MCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two MCP IDs are different, the MCP considers the packet invalid and discards it.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

NOTE

If the DCP is required to send statistics data to the MCP through a specified VPN instance or manager VPN, the VPN instance must have been created on the DCP before you run the **mcp** command with **vpn-instance** *vpn-instance-name* or **net-manager-vpn** specified.

Precautions

The MCP ID must be an IP address that DCPs can reach and must be the same as the MCP ID configured by the **mcp id** command on the MCP.

The UDP port number through which the DCP and MCP communicate with each other must be the same as the UDP port number configured by the **protocol udp port** command.

The **mcp** command associates the MCP ID with all measurement instances on the DCP. However, if some measurement instances on the DCP have been associated with the MCP ID configured by the **mcp** command, the measurement instances still use the MCP ID in the IPFPM-DCP instance view.

Example

Associate the MCP ID with all measurement instances of a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] mcp 10.1.1.1
```

16.5.39 mcp (IPFPM-DCP instance view)

Function

The **mcp** command associates the MCP ID with a measurement instance of a DCP.

The **undo mcp** command disassociates the MCP ID from a measurement instance of a DCP.

By default, no MCP ID is associated with a measurement instance of a DCP.

Format

mcp *mcp-id* [**port** *port-number*] [**vpn-instance** *vpn-instance-name* | **net-manager-vpn**]

undo mcp

Parameters

Parameter	Description	Value
mcp-id	Specifies the MCP ID associated with a measurement instance of a DCP. It is recommended that you configure the router ID of the device as the MCP ID.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port-number*	Specifies the UDP port number through which the DCP and MCP communicate with each other.	The value is an integer that ranges from 1024 to 65535. The default value 65030 is recommended.
vpn-instance *vpn-instance-name*	Specifies the VPN instance where the DCP and MCP communicate with each other.	The value is a string of 1 to 31 case-sensitive characters without spaces.
net-manager-vpn	Specifies the manager VPN where the DCP and MCP communicate with each other.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a DCP sends statistics data of a measurement instance from TLPs to the MCP, you must associate the MCP ID with the measurement instance. The **mcp** command associates the MCP ID with a measurement instance of a DCP.

A DCP encapsulates statistics data collected from Target Logical Ports (TLPs) and MCP ID associated with a measurement instance of the DCP in a packet, and sends the packet with the MCP ID as the destination IP address. After receiving the packet sent from the DCP, the MCP compares the MCP ID in the packet with the MCP ID configured by the **mcp id** command:

- If the two MCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two MCP IDs are different, the MCP considers the packet invalid and discards it.

Prerequisites

A measurement instance has been created on the DCP using the **instance** command.

Precautions

The MCP ID must be an IP address that DCPs can reach and must be the same as the MCP ID configured by the **mcp id** command on the MCP.

The UDP port number through which the DCP and MCP communicate with each other must be the same as the UDP port number configured by the **protocol udp port** command.

The VPN instance has been created on the DCP before you configure **vpn-instance** *vpn-instance-name* or **net-manager-vpn** to allow the DCP to report the statistics to the MCP through the specified VPN or management VPN.

Example

Associate the MCP ID with a measurement instance of a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] mcp 10.1.1.1
```

16.5.40 mcp id

Function

The **mcp id** command configures the MCP ID in the IP Flow Performance Measurement (FPM) system.

The **undo mcp id** command deletes the MCP ID.

By default, no MCP ID is configured.

Format

mcp id *mcp-id*

undo mcp id

Parameters

Parameter	Description	Value
mcp-id	Specifies the MCP ID. It is recommended that you configure the router ID of the device as the MCP ID.	The value is in dotted decimal notation.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MCP communicates with a DCP, the DCP encapsulates statistics data collected from TLPs and MCP ID associated with a measurement instance by the **mcp** command in a packet, and sends the packet with the MCP ID as the destination IP address. After receiving the packet sent from the DCP, the MCP compares the MCP ID in the packet with the MCP ID of the device:

- If the two MCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two MCP IDs are different, the MCP considers the packet invalid and discards it.

This command configures the MCP ID.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

The MCP ID must be an IP address that a DCP can reach and must be the same as the MCP ID configured by the **mcp** command on the DCP. If you have changed the MCP ID, you must change the MCP ID associated with measurement instances on the DCP; otherwise, the DCP cannot communicate with the MCP.

Example

Set the MCP ID.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] mcp id 10.1.1.1
```

16.5.41 measure disable (IPFPM-MCP instance view)

Function

The **measure disable** command disables measurement of all indicators in a measurement instance on the MCP.

Both the **undo measure disable** and **measure enable** commands enable measurement of all indicators in a measurement instance on the MCP.

By default, measurement of all indicators is enabled in a measurement instance on the MCP.

Format

measure disable

measure enable

undo measure disable

Parameters

None

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

If the MCP receives error data during the DCP configuration update, you can run the **measure disable** command to disable measurement of all indicators in a measurement instance on the MCP. When the DCP configuration update is complete, run the **undo measure disable** or **measure enable** command to enable measurement of all indicators in a measurement instance on the MCP so that data of the measurement instance is more accurate.

Example

Disable measurement of all indicators in measurement instance 1 on the MCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] measure disable
```

16.5.42 nqa ipfpm dcp

Function

The **nqa ipfpm dcp** command enables global DCP and displays the IPFPM-DCP view, or directly displays the IPFPM-DCP view if global DCP has been enabled.

The **undo nqa ipfpm dcp** command disables global DCP.

By default, global DCP is disabled.

Format

nqa ipfpm dcp

undo nqa ipfpm dcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing packet loss measurement for service traffic, run the **nqa ipfpm dcp** command to enable global DCP and enter the IPFPM-DCP view.

Follow-up Procedure

Run the **dcp id** command to set the DCP ID.

Precautions

DCP and MCP functions can be configured on the same device.

Example

Enable global DCP and enter the IPFPM-DCP view.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp]
```

16.5.43 nqa ipfpm mcp

Function

The **nqa ipfpm mcp** command enables global MCP and displays the IPFPM-MCP view, or directly displays the IPFPM-MCP view if global MCP has been enabled.

The **undo nqa ipfpm mcp** command disables global MCP.

By default, global MCP is disabled.

Format

nqa ipfpm mcp

undo nqa ipfpm mcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing packet loss measurement for service traffic, run the **nqa ipfpm mcp** command to enable global MCP and enter the IPFPM-MCP view.

Follow-up Procedure

Run the **mcp id** command to set the MCP ID.

Precautions

MCP and DCP functions can be configured on the same device.

Example

Enable global MCP and enter the IPFPM-MCP view.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp]
```

16.5.44 out-group

Function

The **out-group** command creates a Target Logical Port (TLP) out-group for the target flow.

The **undo out-group** command deletes a TLP out-group or deletes a TLP from a TLP out-group.

By default, no TLP out-group is configured for the target flow.

Format

out-group dcp *dcp-id* **tlp** *tlp-id*

undo out-group [**dcp** *dcp-id* **tlp** *tlp-id*]

Parameters

Parameter	Description	Value
dcp *dcp-id*	Indicates a DCP to which TLPs in a TLP out-group belongs.	This value is in dotted decimal notation.
tlp *tlp-id*	Indicates a TLP in a TLP out-group.	The value is an integer ranging from 1 to 16777215.

Views

IPFPM-MCP-ACH view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To measure the packet loss or delay of service packets leaving a network, run the **out-group** command. In IP FPM hop-by-hop performance statistics scenarios, a hop is a set of links and interfaces that service packets travel through, from one measurement point or group to the next measurement point or group, and therefore is represented by (TLP in-group, TLP out-group). Performance statistics are implemented on the TLP in-point or in-group through which service packets enter a network and the TLP out-point or out-group through which service packets leave the network.

Prerequisites

The **ach** command has been run to create an ACH and display the ACH view.

Example

Create a TLP out-group for the target flow.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
[HUAWEI-nqa-ipfpm-mcp-instance-1-ach-1] out-group dcp 10.1.1.1 tlp 100
```

16.5.45 protocol udp port

Function

The **protocol udp port** command configures the UDP port number through which the DCP and MCP communicate with each other.

The **undo protocol udp port** command restores the default UDP port number through which the DCP and MCP communicate with each other.

By default, the DCP and MCP communicate with each other through UDP port 65030. The default configuration is recommended.

Format

protocol udp port *port-number*

undo protocol udp port

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number through which the DCP and MCP communicate with each other.	The value is an integer that ranges from 1024 to 65535.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCP uses UDP and default port 65030 to send statistics data to the MCP. To change the UDP port number, run this command.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

The UDP port number of the DCP must be the same as the UDP port number configured by the **mcp (IPFPM-DCP instance view)** command on the DCP. If a UDP port number is changed on an MCP, it must be changed for all DCPs associated with this MCP in an IP FPM instance. Otherwise, the MCP cannot process the statistics reported by the DCPs.

Example

Specify UDP port 1024 through which the DCP and MCP communicate with each other.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] protocol udp port 1024
```

16.5.46 tlp

Function

The **tlp** command configures Target Logical Ports (TLPs) of an IP FPM instance and their roles.

The **undo tlp** command deletes TLPs of a measurement instance.

By default, no TLP of a measurement instance is configured.

Format

tlp *tlp-id* { **in-point** | **out-point** } { **ingress** | **egress** }

tlp *tlp-id* **mid-point flow** { **forward** | **backward** | **bidirectional** } { **ingress** | **egress** }

undo tlp *tlp-id*

Parameters

Parameter	Description	Value
tlp-id	Specifies the ID of a TLP.	The value is an integer that ranges from 1 to 16777215.

Parameter	Description	Value
in-point	Indicates the in-point TLP. An in-point TLP colors a target flow.	-
out-point	Indicates the out-point TLP. An out-point TLP removes the color flag from a target flow.	-
ingress	Indicates the ingress TLP. An ingress TLP only receives packets.	-
egress	Indicates the egress TLP. An egress TLP only sends packets.	-
mid-point	Indicates the TLP as a mid-point.	-
flow	Indicates the target flow.	-
forward	Indicates the forward target flow.	-
backward	Indicates the backward target flow.	-
bidirectional	Indicates the bidirectional target flows.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To locate faults in IP FPM performance statistics scenarios, run the **tlp** command to configure TLPs in an IP FPM instance. TLPs are measurement points along the path of the target flow and compile and output the statistics. TLPs can be in-points, mid-points, or out-points.

Precautions

- A TLP that functions as the in-point for the forward target flow is the out-point for the backward target flow. The TLP role specified in the **tlp** command applies only to the forward target flow, and the reverse of the specified role is used for the backward target flow.
- Mid-points apply only to IP FPM hop-by-hop performance statistics scenarios. Therefore, you must configure **flow** to specify the target flow direction when specifying a TLP as a mid-point.

- A TLP cannot function as both the in-point and out-point for the same unidirectional target flow.
- After an in-point is specified, the packets that match corresponding rules are modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Configure TLP 100 and its role for measurement instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
```

16.6 iPCA 2.0 Configuration Commands

16.6.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support iPCA 2.0.

16.6.2 display s-ipfpm configuration

Function

The **display s-ipfpm configuration** command displays the iPCA 2.0 configuration.

Format

display s-ipfpm configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the iPCA 2.0 configuration is complete, you can run this command to check whether the configuration is correct.

Example

Display the iPCA 2.0 configuration (S5732-H is used as an example).

```
<HUAWEI> display s-ipfpm configuration
Global measure interval(s)              : 60(default)
Global measure color-flag               : Flags-bit0(default)
Report loss reason                      : disable(default)

Total flow(s) of five tuple             : 2
Total flow(s) of application            : 2
Total flow(s) of UCL group              : 1
Total flow(s) of UCL group and application : 1
Total measure interface(s)/VAP(s)       : 5

Five tuple flow list(s):
--------------------------------------------------------------------------------
Flow  Protocol  SrcPort      DstPort      SrcIp/Mask         DstIp/Mask
--------------------------------------------------------------------------------
10    -         -            -            10.0.0.0/8         20.0.0.0/8
11    UDP       10000-20000  30000        1.0.0.0/8          11.11.11.11/32
--------------------------------------------------------------------------------
Total: 2

Application flow list(s):
--------------------------------------------------------------------------------
Flow  Application
--------------------------------------------------------------------------------
1000  rtp
1002  ftp, tcp, rtp, qq
--------------------------------------------------------------------------------
Total: 2

UCL group flow list(s):
------------------------------------------------------------------------------------------------------------------------

Flow  GroupId  GroupName                        Status
------------------------------------------------------------------------------------------------------------------------

777   11       NA                               Active
------------------------------------------------------------------------------------------------------------------------

Total: 1

UCL group and application flow list(s):
------------------------------------------------------------------------------------------------------------------------

Flow  GroupId  GroupName                        Status    Application
------------------------------------------------------------------------------------------------------------------------
666   11       NA                               Active    UD_DDP
------------------------------------------------------------------------------------------------------------------------

Total: 1

Measure list(s):
I: In-Point,  O: Out-Point, M: Mid-Point
ING: Ingress, EGR: Egress,  B: Bidirectional
--------------------------------------------------------------------------------
Interface/VAPProfileName               Flow  AutoDetect  Direction
--------------------------------------------------------------------------------
GigabitEthernet0/0/10                  10    -           I/ING/B
GigabitEthernet0/0/11                  -     YES         M/EGR/B
GigabitEthernet0/0/12                  11    -           O/ING/B
test                                   10    -           I/ING/B
```

```
test1                          11    -           I/ING/B
-------------------------------------------------------------------------------
Total: 5
```

Table 16-57 Description of the **display s-ipfpm configuration** command output

Item	Description
Global measure interval(s)	Packet loss and delay measurement interval. To configure this parameter, run the **s-ipfpm measure interval** command.
Global measure color-flag	Color bit for packet loss and delay measurement. To configure this parameter, run the **s-ipfpm measure color-flag** command.
Report loss reason	Whether the device reports the packet loss cause to the analyzer. To configure this parameter, run the **s-ipfpm report-loss-reason enable** command.
Total flow(s) of five tuple	Number of measurement flow tables based on 5-tuple.
Total flow(s) of application	Number of measurement flow tables based on applications.
Total flow(s) of UCL group	Number of measurement flow tables based on UCL groups.
Total flow(s) of UCL group and application	Number of measurement flow tables based on UCL groups and applications.
Total measure interface(s)/VAP(s)	Number of interfaces and VAP profiles enabled with packet loss and delay measurement.
Five tuple flow list(s)	5-tuple information of the measurement flow. To configure this parameter, run the **s-ipfpm flow** command.
Flow	Measurement flow ID.
Protocol	Protocol type of the measurement flow.
SrcPort	Source port number of the measurement flow.
DstPort	Destination port number of the measurement flow.
SrcIp/Mask	Source IP address of the measurement flow.
DstIp/Mask	Destination IP address of the measurement flow.

Item	Description
Total	Total number of measurement flows.
Application flow list(s)	Information about measurement flows based on applications. To configure this parameter, run the **s-ipfpm flow application** command.
Application	Application name.
UCL group flow list(s)	Information about measurement flows based on UCL groups. To configure this parameter, run the **s-ipfpm flow source-ucl-group** command.
UCL group and application flow list(s)	Information about measurement flows based on UCL groups and applications. To configure this parameter, run the **s-ipfpm flow source-ucl-group** command.
GroupId	UCL group ID.
GroupName	UCL group name. If no UCL group is configured, **NA** is displayed.
Status	Whether a UCL group has been created. To create a UCL group, run the **ucl-group (system view)** command. ● Active: The UCL group has been created. ● Inactive: The UCL group has not been created.
Interface/VAPProfileName	Name of the interface on which packet loss and delay measurement is enabled using the **s-ipfpm measure flow** (interface view) command and name of the VAP profile in which packet loss and delay measurement is enabled using the **s-ipfpm measure flow** (VAP profile view) command.
Flow	Measurement flow ID.
AutoDetect	Whether automatic in-band flow measurement is enabled on an interface. To configure this function, run the **s-ipfpm measure auto-detect** command.
Direction	Measurement point and measurement direction.

16.6.3 s-ipfpm clear color-flag ingress

Function

The **s-ipfpm clear color-flag ingress** command enables the function of clearing the packet color bit in the ingress direction of an interface.

The **undo s-ipfpm clear color-flag ingress** command disables the function of clearing the packet color bit in the ingress direction of an interface.

By default, the function of clearing the packet color bit in the ingress direction of an interface is disabled on the device.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

This command can be configured in the VAP profile view only on the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

Format

s-ipfpm clear color-flag ingress

undo s-ipfpm clear color-flag ingress

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, VAP profile view

Default Level

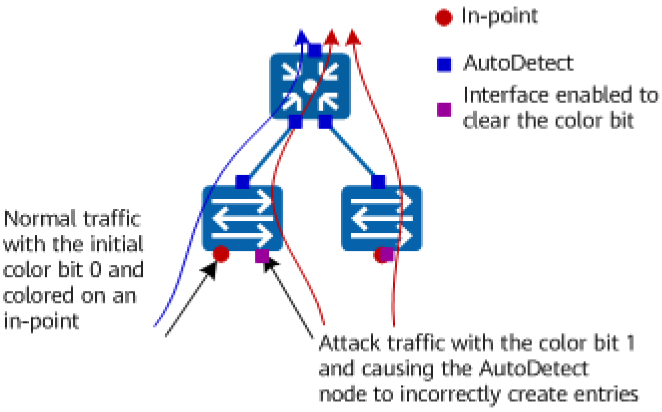
2: Configuration level

Usage Guidelines

After automatic in-band flow measurement is configured on a downstream device, the downstream device automatically creates a measurement entry and performs measurement for the packets with color bit 1. When an attack occurs on the network (the color bit of attack packets is set to 1) or the color bit of other service packets on the upstream device is set to 1, the measurement data on the downstream device is incorrect. In this case, you can run this command on the inbound interface of packets on the upstream device to enable the function of clearing the packet color bit in the ingress direction. After this function is enabled, the color bit in incoming packets is set to 0, and measurement is not performed for the packets after they are forwarded to the downstream device.

In **Figure 16-1**, on the left device, the interface that receives attack traffic is different from the interface configured as an in-point. The attack traffic is forwarded to the downstream AutoDetect node based on a forwarding entry. In this case, you need to enable the function of clearing the packet color bit in the ingress direction of the inbound interface that receives the attack traffic on the upstream device. On the right device, the interface that receives attack traffic is the same as the interface configured as an in-point. You need to enable the function of clearing the packet color bit in the ingress direction on this interface. In this way, normal traffic is colored on the in-point, and attack traffic is not colored, ensuring that the downstream device performs measurement only for normal traffic.

Figure 16-1 Attack traffic processing



Example

Enable the function of clearing the packet color bit in the ingress direction of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] s-ipfpm clear color-flag ingress
```

16.6.4 s-ipfpm flow

Function

The **s-ipfpm flow** command configures a measurement flow.

The **undo s-ipfpm flow** command deletes a configured measurement flow.

By default, no measurement flow is configured.

Format

s-ipfpm flow *flow-id* { **source** *src-ip-address src-mask-length* | **destination** *dest-ip-address dest-mask-length* | **protocol** { { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

undo s-ipfpm flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 0 to 1023. When a measurement flow is specified by application name, the value is in the range from 512 to 1023.
source *src-ip-address*	Specifies the source IP address of a measurement flow. The value can only be a unicast IP address.	The value is in dotted decimal notation.
src-mask-length	Specifies the mask length of the source IP address of a measurement flow.	The value is an integer in the range from 1 to 32.
destination *dest-ip-address*	Specifies the destination IP address of a measurement flow. The value can only be a unicast IP address.	The value is in dotted decimal notation.
dest-mask-length	Specifies the mask length of the destination IP address of a measurement flow.	The value is an integer in the range from 1 to 32.
protocol { **tcp** | **udp** }	Indicates that the protocol type of a measurement flow is TCP or UDP.	-
source-port *src-port-number1*	Specifies the start source port number of a measurement flow.	The value is an integer in the range from 1 to 65535.
src-port-number2	Specifies the end source port number of a measurement flow.	The value is an integer in the range from 1 to 65535. The value of *src-port-number2* must be greater than that of *src-port-number1*.
destination-port *dest-port-number1*	Specifies the start destination port number of a measurement flow.	The value is an integer in the range from 1 to 65535.

Parameter	Description	Value
dest-port-number2	Specifies the end destination port number of a measurement flow.	The value is an integer in the range from 1 to 65535. The value of *dest-port-number2* must be greater than that of *dest-port-number1*.
protocol-number	Specifies a protocol number for a measurement flow.	The value is an integer in the range from 1 to 5, 7 to 16, or 18 to 255. The values 6 and 17 indicate TCP and UDP, respectively.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. A measurement flow is a key element for configuring iPCA 2.0. Before each measurement, you must configure a measurement flow.

A measurement flow can be defined by any combinations of the source IP address, destination IP address, protocol type, source port number, and destination port number. The device generates accurate 5-tuple matching rules for measurement based on the configured parameters.

Precautions

- All devices on a network must have the same measurement flow configuration.
- If a measurement flow is used by an interface, it cannot be deleted.
- WLAN services can use only measurement flows with IDs 0 to 127. Therefore, if WLAN services are configured on a network, you are advised not to use measurement flows with IDs 0 to 127 for other services.
- The source and destination port numbers of a measurement flow cannot be both configured as port number ranges.
- The source IP address/mask length and destination IP address/mask length of a measurement flow cannot be the same.

Example

Configure a measurement flow with the source port number 3, destination port number 10, source IP address 1.1.1.1/24, destination IP address 2.2.2.2/24, and protocol type TCP for packet loss and delay measurement.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 2 protocol tcp source-port 3 destination-port 10 source 1.1.1.1 24 destination
2.2.2.2 24
```

16.6.5 s-ipfpm flow application

Function

The **s-ipfpm flow application** command configures a measurement flow based on an application name.

The **undo s-ipfpm flow** command deletes a measurement flow configured based on an application name.

By default, a measurement flow based on an application name is not configured on the device.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm flow *flow-id* **application** { *app-name* } &<1-16>

undo s-ipfpm flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 512 to 1023.
application *app-name*	Specifies the application name corresponding to a measurement flow.	The value is a string of 1 to 64 case-insensitive characters. If the application name contains spaces, it must be enclosed in double quotation marks, for example, "user for test". A maximum of 16 application names can be configured at a time, and multiple application names configured at a time can be the same.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. A measurement flow is a key element for configuring iPCA 2.0. Before each measurement, you must configure a measurement flow.

A measurement flow can be specified based on an application name so that the device performs measurement for traffic of the application.

Precautions

- All devices on a network must have the same measurement flow configuration.
- If a measurement flow is used by an interface, the measurement flow cannot be deleted.

Follow-up Procedure

Run the **s-ipfpm measure flow** command to enable traffic measurement in the interface view.

Example

Configure the device to perform measurement for packets of the application named **QQLive**.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 533 application QQLive
```

16.6.6 s-ipfpm flow source-ucl-group

Function

The **s-ipfpm flow source-ucl-group** command configures a measurement flow based on a UCL group or a UCL group and an application.

The **undo s-ipfpm flow** command deletes a measurement flow configured based on a UCL group or a UCL group and an application.

By default, a measurement flow based on a UCL group or a UCL group and an application is not configured on the device.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm flow *flow-id* **source-ucl-group** { *group-index* | **name** *group-name* } &<1-16>

s-ipfpm flow *flow-id* **application** { *app-name* } &<1-16> **source-ucl-group** { *group-index* | **name** *group-name* }

undo s-ipfpm flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 512 to 1023.
group-index	Specifies the index of a source UCL group.	The value is an integer in the range from 1 to 64000.
name *group-name*	Specifies the name of a source UCL group.	The value must be the name of an existing UCL group. A maximum of 16 UCL group indexes and UCL group names can be configured at a time, and multiple UCL group indexes and UCL group names configured at a time can be the same.
application *app-name*	Specifies the name of an application.	The value is a string of 1 to 64 case-insensitive characters. If the application name contains spaces, it must be enclosed in double quotation marks, for example, "user for test". A maximum of 16 application names can be configured at a time, and multiple application names configured at a time can be the same.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. A measurement flow is a key element for configuring iPCA 2.0. Before each measurement, you must configure a measurement flow.

A measurement flow can be specified based on a UCL group or a UCL group and an application so that the device performs measurement for traffic of all users in the UCL group.

Precautions

- All devices on a network must have the same measurement flow configuration.
- If a measurement flow is used by an interface, the measurement flow cannot be deleted.
- If a UCL group index is not created, this command can be configured when the UCL group index is specified. If a UCL group name is not configured, this command cannot be configured when the UCL group name is specified. After a UCL group name is configured in a measurement flow, the UCL group name cannot be deleted.

Follow-up Procedure

Run the **s-ipfpm measure flow** command to enable traffic measurement in the interface view.

Example

Configure the device to perform measurement for packets of users in the UCL group with index 10.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 533 source-ucl-group 10
```

16.6.7 s-ipfpm measure application

Function

The **s-ipfpm measure application** command enables packet loss and delay measurement based on the application name in the VAP profile view.

The **undo s-ipfpm measure application** command disables packet loss and delay measurement based on the application name in the VAP profile view.

By default, packet loss and delay measurement based on the application name is disabled in the VAP profile view.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure application { *app-name* } &<1-16>

undo s-ipfpm measure application { *app-name* } &<1-16>

Parameters

Parameter	Description	Value
application *app-name*	Specifies the name of an application for which packet loss and delay measurement is performed.	The application name must exist in the application signature database. A maximum of 16 application names can be configured at a time.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an application on a wireless network has poor user experience (for example, video freezing or voice discontinuity) or you want to monitor the network transmission quality of an application in real time, you can enable packet loss and delay measurement for the application on the switch.

Precautions

- Before configuring this command, you must run the **defence engine enable ap-group** { **all** | **name** *ap-group-name* } command to enable the security engine function for an AP group.
- This command cannot be configured after the **s-ipfpm measure flow** command is run in the VAP profile view to enable packet loss and delay measurement.
- After the **s-ipfpm measure application** command is configured to enable packet loss and delay measurement based on an application name in the VAP profile view, user packets corresponding to the application name will be modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Configure packet loss and delay measurement for the application named **baidu**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable ap-group name test
Info: Make sure the group name of AP exists. Continue? [Y/N]:y
It will take several minutes to load the signature lib, please wait....
Info: The signature lib load successful.
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] s-ipfpm measure application baidu
```

16.6.8 s-ipfpm measure color-flag

Function

The **s-ipfpm flow** command configures a color bit for packet loss and delay measurement.

The **undo s-ipfpm measure color-flag** command restores the default color bit for packet loss and delay measurement.

By default, bit 0 in the Flags field of the IP header is used as the color bit for packet loss and delay measurement on the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and bit 5 in the ToS field of the IP header is used as the color bit for packet loss and delay measurement on other models.

Format

s-ipfpm measure color-flag { **tos-bit** *tos-bit* | **flags-bit0** }

undo s-ipfpm measure color-flag

Parameters

Parameter	Description	Value
tos-bit *tos-bit*	Specifies a bit in the ToS field of the IP header as the color bit for packet loss and delay measurement.	The value is an integer in the range from 3 to 7 for the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S and in the range from 3 to 5 for other models.
flags-bit0	Specifies bit 0 in the Flags field of the IP header as the color bit for packet loss and delay measurement.	This parameter is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. You can run this command to specify the color bit for packet loss and delay measurement. You can select a proper color bit based on your requirements and network planning.

Precautions

- All devices on a network must use the same color bit setting.
- When the DS field is used to provide differentiated services for QoS, it is not recommended that you configure bits 3 to 5 in the ToS field as color bits because the packet loss and delay measurement result may be inaccurate.
- When bits 3 to 5 in the ToS field are used as color bits, you must run the **dynamic flow inspection disable** command in the VAP profile view to disable the Deep Flow Inspection (DFI) function on a VAP. Otherwise, the measurement function is abnormal because the DFI function on a VAP will decolor color bits 3 to 5 in the ToS field.
- If the Explicit Congestion Notification (ECN) function is configured on a device on the network, bits 6 and 7 in the ToS field cannot be used as color bits because the ECN function uses these two bits. If they are used as color bits, a switch sends packets with the color bits to a downstream device, affecting the ECN function.

Example

Configure bit 3 in the ToS field as the color bit for packet loss and delay measurement.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm measure color-flag tos-bit 3
```

16.6.9 s-ipfpm measure interval

Function

The **s-ipfpm measure interval** command configures the packet loss and delay measurement interval.

The **undo s-ipfpm measure interval** command restores the default packet loss and delay measurement interval.

By default, the packet loss and delay measurement interval is 60 seconds.

Format

s-ipfpm measure interval *interval*

undo s-ipfpm measure interval

Parameters

Parameter	Description	Value
interval	Specifies the packet loss and delay measurement interval.	The value can be 10 or 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packet loss or delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. You can run this command to specify the packet loss and delay measurement interval on a device.

Precautions

- The measurement interval must be the same on all devices configured with measurement flows. Otherwise, there is no measurement data.
- The measurement interval cannot be changed during measurement. To change the measurement interval, you are advised to disable the measurement flows bound to all interfaces first. Otherwise, the packet loss and delay data calculated in subsequent measurement intervals may be incorrect.
- On a large network, changing the measurement interval to 10 seconds affects the measurement performance. Therefore, exercise caution when changing the measurement interval.

Example

Set the packet loss and delay measurement interval to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm measure interval 60
```

16.6.10 s-ipfpm measure auto-detect

Function

The **s-ipfpm measure auto-detect** command enables automatic in-band flow measurement on an interface.

The **undo s-ipfpm measure auto-detect** command disables automatic in-band flow measurement on an interface.

By default, automatic in-band flow measurement is disabled on an interface.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm measure auto-detect { **out-point** | **mid-point** } { **ingress** | **egress** } [**bidirectional**]

undo s-ipfpm measure auto-detect

Parameters

Parameter	Description	Value
out-point	Indicates that a measurement point for automatic in-band flow measurement is an out-point. An out-point removes the color bit from a measurement flow.	-
mid-point	Indicates that a measurement point for automatic in-band flow measurement is a mid-point.	-
ingress	Indicates that measurement is performed in the ingress direction. On this measurement point, the system measures the packets received by the interface.	-
egress	Indicates that measurement is performed in the egress direction. On this measurement point, the system measures the packets sent by the interface.	-
bidirectional	Indicates that measurement is performed in both the ingress and egress directions. When this parameter is specified, a backward flow configuration is added based on reversal of the measurement flow information and measurement direction.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packet loss and delay measurement is performed for a specified flow or application, measurement needs to be performed on all devices on the forwarding path. In this case, you need to specify the 5-tuple information or application name of the flow on all devices. If a large number of flows or applications need to be measured, the configuration workload is heavy. To simplify the configuration, you can specify the 5-tuple or application name of the flow only on the in-point node and enable automatic in-band flow measurement on the mid-point and out-point nodes. After automatic in-band flow measurement is enabled on the mid-point and out-point nodes, the devices automatically create measurement entries based on the packet coloring on the in-point node to perform traffic measurement.

Precautions

- When automatic in-band flow measurement is configured, if the resource allocation mode is not **enhanced-sipfpm**, measurement flows occupy ACL resources, and the number of measurement flows is limited by the number of ACL resources on the device. When the **enhanced-sipfpm** mode is configured, measurement flows do not occupy ACL resources, which meets the requirements in scenarios where a large number of measurement flows are configured.
- This command can be run on a Layer 2 or Layer 3 interface, but not on a stack interface.

Example

Configure GE0/0/1 as a mid-point to perform automatic in-band flow measurement in the ingress direction.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] s-ipfpm measure auto-detect mid-point ingress
```

16.6.11 s-ipfpm measure flow (interface view)

Function

The **s-ipfpm measure flow** command enables packet loss and delay measurement on an interface.

The **undo s-ipfpm measure flow** command disables packet loss and delay measurement from an interface.

By default, packet loss and delay measurement is disabled on an interface.

Format

s-ipfpm measure flow *flow-id* { **in-point** | **out-point** | **mid-point** } { **ingress** | **egress** } [**bidirectional**]

undo s-ipfpm measure flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 0 to 1023.
in-point	Indicates that a measurement point is an in-point. An in-point colors a measurement flow.	-
out-point	Indicates that a measurement point is an out-point. An out-point removes the color bit from a measurement flow.	-
mid-point	Indicates that a measurement point is a mid-point.	-
ingress	Indicates that measurement is performed in the ingress direction. On this measurement point, the system measures the packets received by the interface.	-
egress	Indicates that measurement is performed in the egress direction. On this measurement point, the system measures the packets sent by the interface.	-
bidirectional	Indicates that measurement is performed in both the ingress and egress directions. When this parameter is specified, a backward flow configuration is added based on reversal of the measurement flow information and measurement direction.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor network transmission quality in real time to quickly detect abnormal traffic and locate faults, you can enable packet loss and delay measurement on interfaces of devices.

Precautions

- Measurement can be performed only for incoming traffic on interfaces for the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S,S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S ,S6735-S, S6720-EI, S6720S-S, and S6720S-EI.
- This command can be run on a Layer 2 or Layer 3 interface, but not on a stack interface.
- The 5-tuple ranges of multiple measurement flows bound to the same interface cannot overlap.
- Measurement is performed for tunnel packets based on the inner 5-tuple of the packets.
- If the **s-ipfpm flow source-ucl-group** command has been run to configure a measurement flow based on a UCL group or based on a UCL group and application, you can only specify the **in-point** and **ingress** parameters when you run the **s-ipfpm measure flow** command to enable packet loss and delay measurement on an interface.
- After an interface is configured as an in-point using the **s-ipfpm measure flow** *flow-id* **in-point** { **ingress** | **egress** } [**bidirectional**] command, the packets that arrive at the interface and match corresponding rules are modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Configure GE0/0/1 as an in-point and enable packet loss and delay measurement in its ingress direction.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 33 protocol tcp source-port 3 destination-port 10 source 1.1.1.1 24 destination
2.2.2.2 24
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] s-ipfpm measure flow 33 in-point ingress
```

16.6.12 s-ipfpm measure flow (VAP profile view)

Function

The **s-ipfpm measure flow** command enables packet loss and delay measurement in the VAP profile view.

The **undo s-ipfpm measure flow** command disables packet loss and delay measurement in the VAP profile view.

By default, packet loss and delay measurement is disabled in the VAP profile view.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure flow *flow-id* { **in-point** | **out-point** | **mid-point** } { **ingress** | **egress** } [**bidirectional**]

undo s-ipfpm measure flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 0 to 127.
in-point	Indicates that a measurement point is an in-point. An in-point colors a measurement flow.	-
out-point	Indicates that a measurement point is an out-point. An out-point removes the color bit from a measurement flow.	-
mid-point	Indicates that a measurement point is a mid-point.	-
ingress	Indicates the ingress direction of a measurement flow. On this measurement point, the system measures the packets received by the AP.	-
egress	Indicates the egress direction of a measurement flow. On this measurement point, the system measures the packets sent by the AP.	-
bidirectional	Indicates that a measurement flow is a bidirectional flow. When this parameter is specified, a backward flow configuration is added based on reversal of the 5-tuple and measurement direction.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor wireless network transmission quality in real time in a native AC scenario to quickly detect abnormal traffic and locate faults, you can enable packet loss and delay measurement in the VAP profile view.

Precautions

- A maximum of 64 measurement flows can be bound to a VAP profile.
- The 5-tuple ranges of multiple measurement flows bound to the same VAP profile cannot overlap.
- Measurement is performed for tunnel packets based on the inner 5-tuple of the packets.
- After an in-point is specified using the **s-ipfpm measure flow** *flow-id* **in-point** { **ingress** | **egress** } [**bidirectional**] command, the packets that match corresponding rules are modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Enable packet loss and delay measurement in the VAP profile view.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 1 protocol tcp destination-port 5
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-vap-prof-test] s-ipfpm measure flow 1 in-point ingress
```

16.6.13 s-ipfpm measure max-user-flow

Function

The **s-ipfpm measure max-user-flow** command sets the maximum number of iPCA 2.0 measurement flows for each user.

The **undo s-ipfpm measure max-user-flow** command restores the default maximum number of iPCA 2.0 measurement flows for each user.

By default, the maximum number of iPCA 2.0 measurement flows for each user is not limited but depends on device specifications.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure max-user-flow *limit-number*

undo s-ipfpm measure max-user-flow

Parameters

Parameter	Description	Value
limit-number	Specifies the maximum number of iPCA 2.0 measurement flows for each user.	The value is an integer that ranges from 100 to 400.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent a single user from occupying excessive iPCA 2.0 flow entries, you can run this command to set the maximum number of iPCA 2.0 measurement flows for each user.

Example

Set the maximum number of iPCA 2.0 measurement flows for each user to 100.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys
[HUAWEI-wlan-ap-system-prof-apsys] s-ipfpm measure max-user-flow 100
```

16.6.14 s-ipfpm measure ucl-group

Function

The **s-ipfpm measure ucl-group** command specifies a UCL group or a "UCL group + application" combination for iPCA 2.0 measurement.

The **undo s-ipfpm measure ucl-group** command deletes a UCL group or a "UCL group + application" combination for iPCA 2.0 measurement.

By default, iPCA 2.0 measurement is not specified for any UCL group on a VAP.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* & <1-16>]

undo s-ipfpm measure ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* & <1-16>]

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer that ranges from 1 to 64000.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.
application *application-name*	Specifies an application for which iPCA 2.0 measurement is performed.	The application name must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform UCL group–based iPCA 2.0 measurement based on a VAP, run this command to specify a UCL group or a "UCL group + application" combination on the VAP.

You can specify a UCL group so that the device can perform iPCA 2.0 measurement for applications of users in the specified UCL group. You can also specify a "UCL group + application" combination, so that the device can perform iPCA 2.0 measurement for the specified application of users in the specified UCL group.

Precautions

A maximum of 128 applications, UCL groups, and "UCL group + application" combinations (including 16 applications at most) can be specified for iPCA 2.0 measurement.

If the parameter **application** *application-name* is specified, you need to enable the security engine function (using the **defence engine enable ap-group** { **all** | **name** *ap-group-name* } command) for the AP group.

Example

Specify a "UCL group + application" combination for iPCA 2.0 measurement in the VAP profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] s-ipfpm measure ucl-group 1 application welink
```

16.6.15 s-ipfpm report-loss-reason enable

Function

The **s-ipfpm report-loss-reason enable** command enables the device to report the packet loss cause to the analyzer.

The **undo s-ipfpm report-loss-reason enable** command disables the device from reporting the packet loss cause to the analyzer.

By default, the device is disabled from reporting the packet loss cause to the analyzer.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm report-loss-reason enable

undo s-ipfpm report-loss-reason enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

iPCA 2.0 enables devices to report flow measurement information to the analyzer. The analyzer can determine the number of packets discarded on each device for fault locating. However, the packet loss cause cannot be obtained, and maintenance personnel need to manually locate the cause. To address this issue, you can run this command to enable the device to report the packet loss cause to the analyzer. When detecting that packet loss occurs, the device automatically reports the number of lost packets, number of lost bytes, and last packet loss cause in a period to the analyzer. The analyzer directly displays the packet loss cause, helping maintenance personnel quickly locate faults.

Example

Enable the device to report the packet loss cause to the analyzer.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm report-loss-reason enable
```

16.7 NQA Configuration Commands

16.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.7.2 agetime

Function

The **agetime** command sets the aging time of an NQA test instance.

The **undo agetime** command restores the default aging time of an NQA test instance.

The default aging time of an NQA test instance is 0, indicating that the test instance is not aged.

Format

agetime *hh:mm:ss*

undo agetime

Parameters

Parameter	Description	Value
hh:mm:ss	Specifies the aging time.	*hh* ranges from 0 to 23; *mm* ranges from 0 to 59; *ss* ranges from 0 to 59.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent endless running of a test instance, you need to age the test instance periodically. The **agetime** command can be used to configure the aging time to change the survival time of a test instance in the system.

- The aging time is started when the NQA test instance is in the inactive state. When the aging time expires, the system deletes the NQA test instance automatically.
- The aging time is reset when the NQA test instance is in the active state.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

The aging time of a running test instance cannot be changed.

Example

Set the aging time of NQA test instance **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] agetime 1:0:0
```

16.7.3 clear-records

Function

The **clear-records** command clears statistics on NQA test instances.

Format

clear-records

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After each test instance is complete, test results and historical information will be recorded in result and historical tables respectively. You can run the following commands to view the corresponding data and assess the network quality.

- The **display nqa results** command displays the results of an NQA test instance.
- The **display nqa history** command displays the historical records of an NQA test instance.

After several test instances are performed to detect network quality, there may be too many records in the statistics table. In this case, you can run the **clear-records** command to clear historical records and result records of an NQA test instance.

Configuration Impact

Statistics cannot be restored after being cleared using the **clear-records** command.

Precautions

Clearing statistics on the ongoing test is forbidden.

Before running the command, ensure that the test type specified by the **test-type** command exists.

Example

Clear all statistics on NQA test instance **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] clear-records
```

16.7.4 community read cipher

Function

The **community read cipher** command configures the community name for SNMP test.

The **undo community** command deletes the community name of SNMP test.

By default, the community name for SNMP test is public.

Format

community read cipher *community-name*

undo community

Parameters

Parameter	Description	Value
community-name	Specifies the community name for SNMP test.	The value is a string of case-sensitive characters without command line characters such as spaces and question marks. The length ranges from 1 to 32 for plain text and ranges from 32 to 68 for cipher text. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A community, uniquely identified by a community name, defines administrative relationships between NMSs and SNMP agents. The community name acts like a password to regulate access to an SNMP agent. An NMS can access an SNMP agent only if the community name carried in the SNMP request sent by the NMS is the same as the community name configured on the SNMP agent.

When the SNMP versions on agents are SNMPv1 or SNMPv2c, the community name must be configured using the **community read cipher** command, and the community name must be a read-only community name on SNMP agents. When the SNMP versions on agents are SNMPv3, the community name does not need to be configured because SNMPv3 does not support community names.

Prerequisites

The NQA test instance has been configured using the **nqa** command, and the test instance type has been set to SNMP using the **test-type** command.

Example

Set the community name for SNMP test.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test1
[HUAWEI-nqa-user-test1] test-type snmp
[HUAWEI-nqa-user-test1] community read cipher Tester-123
```

16.7.5 datafill

Function

The **datafill** command configures pad characters in an NQA test instance.

The **undo datafill** command deletes the pad characters in an NQA test instance.

By default, there are no padding characters in an NQA test instance.

Format

datafill *fillstring*

undo datafill

Parameters

Parameter	Description	Value
fillstring	Specifies the pad characters for NQA test packets.	The value is a string of 1 to 230 case-sensitive characters with spaces supported. The question mark (?) is not supported. The default value is 0 (an empty pad character).

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test, you need to simulate actual datagrams to obtain more accurate statistics. The **datasize** command can be used to set the size of the Data field. To differentiate packets sent from different test instances, add the specified characters to identify the test packets.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type can be one of the following:

- UDP
- UDP Jitter
- ICMP
- Trace
- Path Jitter
- Path MTU

Configuration Impact

After the **datafill** command is run, the following situations may occur:

- If the length of the data packet sent from the test instance is shorter than the configured pad character, only the forepart of the pad character can be used.
- If the length of the data packet sent from the test instance is larger than the configured pad character, the pad character is repeated in sequence until the data packet is successfully padded.

For example, the pad character is set to **abcd**. If the length of the test packet is 3, only **abc** is used to pad the test packet. If the length of the test packet is 6, **abcdab** is used to pad the test packet.

Precautions

The pad character of a running test instance cannot be changed.

Example

Set the pad characters of the test named **user test** to **abcd**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] datafill abcd
```

16.7.6 datasize

Function

The **datasize** command sets the size of the NQA test packet.

The **undo datasize** command restores the size of the NQA test packet.

The default size is 0, which indicates that the test packet does not carry data information.

Format

datasize *size*

undo datasize

Parameters

Parameter	Description	Value
size	Specifies the size of the NQA test packet.	The value is an integer that ranges from 0 to 8100, in bytes. If the configured size of a packet is smaller than the default size of a packet, the configured size is invalid and the packet is forwarded based on its default size. **NOTE** Only for MAC ping test instance, the value ranges from 95 to 9000, in bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **datasize** command to set the size of the data field of a test packet. This ensures that the size of the test packet is closer to the size of the actual data packet and the obtained statistics are more accurate.

For example, if a UDP jitter test instance is used to detect voice over IP (VoIP) services, you can run the **datasize** command to set the size of the NQA test packet to the same size as the actual voice packet. This enables a simulation of the actual traffic that occurs in a period of time.

To simulate a voice data flow with the transmission rate of 64 kbit/s, you can set the size of the voice packet to 172 bytes (160-byte payload + 12-byte RTP header + 28-byte IP header and UDP header) and set the interval for sending the voice packet to 20 ms. In this manner, 3000 packets can be sent in one minute.

Prerequisites

The test type has been specified using the **test-type** command.

The **datasize** command is applicable only to the LSP Ping, LSP Jitter, PWE3 Ping, ICMP, MAC Ping, Path Jitter, Trace, UDP, and UDP Jitter test instances.

Precautions

You cannot change the size of the running test packets.

Example

Set the size of the packets to 100 bytes in the test instance named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] datasize 100
```

16.7.7 description (NQA view)

Function

The **description** command configures description of an NQA test instance.

The **undo description** command deletes the description of an NQA test instance.

By default, no description is configured for an NQA test instance.

Format

description *string*

undo description

Parameters

Parameter	Description	Value
string	Specifies the description of an NQA test instance.	The value is a string of 1 to 230 case-sensitive characters with spaces.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command can be used to briefly describe the test instance to help maintenance. Generally, the test item or the test objective of a test instance is described.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

If the description of a test instance has been configured, running the **description** command will override the previous configuration.

Precautions

The description of a running test instance cannot be changed.

Example

Set the description of the test named **user test** to fortest.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] description fortest
```

16.7.8 destination-address

Function

The **destination-address** command specifies the destination address of an NQA test instance.

The **undo destination-address** command deletes the destination address of an NQA test instance.

By default, destination address is not configured for an NQA test instance.

Format

destination-address ipv4 *ipv4-address* [**lsp-masklen** *masklen* | **lsp-loopback** *loopback-address*] * [**vpn-frr-path**]

destination-address ipv6 *ipv6-address*

destination-address mac *mac-address*

destination-address remote-mep mep-id *rmep-id*

destination-address url *urlstring*

undo destination-address

Parameters

Parameter	Description	Value
ipv4 *ipv4-address*	Specifies an IPv4 destination address.	The IPv4 address is in dotted decimal notation.
lsp-masklen *masklen*	Specifies the mask length of an LSP's IPv4 address prefix.	The value is an integer that ranges from 0 to 32.
lsp-loopback *loopback-address*	Specifies a 127/8 IP address in the MPLS echo request packet header.	-

Parameter	Description	Value
vpn-frr-path	Indicates that the connectivity of the backup VPN FRR LSP will be checked.	-
mac *mac-address*	Specifies a unicast MAC address.	The value is a 12-digit hexadecimal number, in the format of H-H-H. Each H is 4 digits.
remote-mep mep-id *rmep-id*	Specifies the ID of a remote MEP.	The value is an integer that ranges from 1 to 8191.
ipv6 *ipv6-address*	Specifies an IPv6 destination address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
url *urlstring*	Specifies a destination URL address.	The value is a string of 1 to 230 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NQA detects service features by creating test instances. In NQA, two test ends are called an NQA client and an NQA server. An NQA test is initiated by the NQA client. For a test instance, the server is specified using the destination IP address configured with the **destination-address** command.

For example, to detect whether the peer device is reachable, run the **nqa** command to create an NQA test instance, set the test type to ICMP, and then run the **destination-address** command to configure the IP address of the peer device as the destination IP address. After that, you can start the test instance. Based on the response packet, you can know whether the peer device is reachable.

Precautions

- The Label Switched Path (LSP) parameters can be configured only for the LSP test instances.
- The **mac** and **remote-mep mep-id** parameters can be configured only for MAC ping test instances.
- Only the destination addresses of HTTP, trace, and DNS test instances can be URL addresses. For the HTTP test instances, only absolute URL addresses are supported.
- The destination addresses of DNS test instances cannot be IPv4 addresses, and the destination URL addresses must contain dots (.); otherwise, the test will fail.
- When a URL is specified as the destination address of an NQA test instance, the NQA test instance cannot be bound to a VPN instance. Otherwise, the test fails.
- You cannot change the destination address of a running test instance.

Example

Configure the destination address for test instance **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] destination-address ipv4 10.1.1.1
```

16.7.9 destination-port

Function

The **destination-port** command configures the destination port number for an NQA test.

The **undo destination-port** command restores the default setting.

The default port numbers for test instances of different types are as follows:

- TCP and UDP: 7
- HTTP: 80
- FTP: 21
- Trace: 33434
- Jitter: No default value is available, and the destination port number must be configured.

NOTE

A port number larger than 10000 is recommended for a jitter test instance. A small port number may be conflict with the default port number of a protocol, causing a test failure.

Format

destination-port *port-number*

undo destination-port

Parameters

Parameter	Description	Value
port-number	Specifies the destination port number.	The value is integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NQA detects service features by creating test instances. In NQA, two test ends are called an NQA client and an NQA server. An NQA test is initiated by the NQA client. After test instances are configured with commands on the client, NQA places different types of test instances into various test queues. After the test starts, a response packet is returned. Carriers can then know the operating status about protocols by analyzing the received response packet.

For a test instance, the port for accessing the server is specified using the destination port number configured with the **destination-port** command on the client.

For example, to detect whether the TCP service runs normally on the peer device using a TCP test instance, perform the following configurations:

- On the server: Configure the TCP server used for NQA tests, including the supported client IP address and the TCP port number opened to the client.
- On the client:
  - Create an NQA test instance and set its type to TCP.
  - Configure the IP address of the server as the destination IP address and configure the opened TCP port number on the server as the destination port number.
  - Start the test instance.

Precautions

In the case of a TCP test instance and a UDP test instance, the configured destination port number must be the same as the opened port number on the server.

This command applies to only the FTP, HTTP, TCP, Trace, UDP, and UDP Jitter test instances.

You cannot change the destination port number of the test that is being performed.

Example

Set the destination port number to 2020 for the test instance named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] destination-port 2020
```

16.7.10 discovery-pmtu-max

Function

Using the **discovery-pmtu-max** command, you can specify the maximum value for the range of a path MTU test.

Using the **undo discovery-pmtu-max** command, you can restore the default maximum value for the range of a path MTU test.

By default, the maximum value for the range of a path MTU test is 1500 bytes.

Format

discovery-pmtu-max *pmtu-max*

undo discovery-pmtu-max

Parameters

Parameter	Description	Value
pmtu-max	Specifies the maximum value for the range of a path MTU test.	It is an integer ranging from 48 to 9198, in bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **discovery-pmtu-max** command is available only in the path MTU test.

Precautions

For the running test instance, the **discovery-pmtu-max** command cannot be used to change the range of the MTU test.

Example

The maximum value for the range of a specified path MTU test is 1800 bytes.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pathmtu
[HUAWEI-nqa-user-test] discovery-pmtu-max 1800
```

16.7.11 display nqa history

Function

The **display nqa history** command displays the history records about an NQA test.

Format

display nqa history [**test-instance** *admin-name test-name*]

Parameters

Parameter	Description	Value
test-instance	Indicates NQA test instances.	-
admin-name	Specifies the name of the administrator for an NQA test instance.	The value must be the name of an existing NQA test instance administrator.
test-name	Specifies the name of an NQA test instance.	The value must be the name of an existing NQA test instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

NQA provides NQA test instances to test network operation conditions, to export statistics, and to effectively cut costs. NQA measures the performance of different protocols running on the network.

The **display nqa history** command helps you understand the network status by displaying the operation statistics about each test packet, including the status and round-trip delay.

NOTE

No history record about the failed UDP Jitter test instances exists.

Precautions

If no optional parameter is specified, all history records of an NQA test instance are displayed.

When NQA test result table and historical table are displayed in a split screen, latest results are displayed to improve user experience.

Example

Display the history records about an NQA test.

```
<HUAWEI> display nqa history
 NQA entry(admin, rtp) history:
 Index  T/H/P     Response Status       Address       Time
 1       1/1/1     1157ms  success       10.2.1.2       2012-07-15 10:16:38.188
 2       2/1/1     3000ms  success       10.2.1.2       2012-07-15 10:18:2.922
 NQA entry(admin, http) history:
 Index  T/H/P     Response Status       Address       Time
 1       1/1/1     0ms     busy          UnKnown        2012-07-15 11:16:39.915
 2       1/1/2     0ms     busy          UnKnown        2012-07-15 11:16:39.978
 3       1/1/3     0ms     busy          UnKnown        2012-07-15 11:16:39.40
```

Table 16-58 Description of the **display nqa history** command output

Item	Description
NQA entry(admin, rtp) history	The history records about an NQA test instance: - admin: administrator of an NQA test instance. - rtp: name of an NQA test instance. You can run the **nqa** command to configure this parameter.
Index	Index of a test record.
T/H/P	- T: Times, which indicates the sequence of the test for a test instance. - H: Hop, which indicates the sequence of the hop. - P: Probe, which indicates the sequence of the probe.
Response	Period from the time when a probe packet is sent to the time when a response packet is received.

Item	Description
Status	Probe status: ● success: indicates that the probe succeeds. ● timeout: indicates that the probe times out and no response packet is received. ● busy: indicates that the resources are insufficient and the probe packet fails to be sent. When Status is busy, the value of the Response field is 0 ms. ● drop: indicates that the probe packet is discarded because of no link is available. When Status is busy, the value of the Response field is 0 ms.
Address	Destination IP address of an NQA test instance.
Time	Time when the response packet is received.

16.7.12 display nqa results

Function

The **display nqa results** command displays NQA test results.

Format

display nqa results [**test-instance** *admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
test-instance	Indicates an NQA test instance.	-
admin-name	Specifies the name of the administrator for an NQA test instance.	The value must be the name of an existing NQA test instance administrator.
test-name	Specifies the name of an NQA test instance.	The value must be the name of an existing NQA test instance.
verbose	Displays detailed information. **NOTE** Only ICMP, UDP, ICMP Jitter, Path MTU, and UDP Jitter test instances support the query of details.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

NQA test results cannot be displayed automatically on the terminal. To view NQA test results, run the **display nqa results** command.

If no test instance is specified, the test result of the test instance is displayed in the corresponding test instance view, and the test result of all test instances is displayed in the system view or other views irrelevant to test instances. If a test instance is specified, the test result of only this test instance is displayed.

The output of the **display nqa results** command contains the following two parts:

- Universal test results: This part does not vary according to the test instance type.
- Detailed statistics of each test: Statistics items in this part vary according to the test instance type.

Precautions

The **display nqa results** command only displays the result of a test instance that has been completed.

When NQA test result table and historical table are displayed in a split screen, latest results are displayed to improve user experience.

By default, the unit of the delay statistics field in the result table is millisecond. The **timestamp-unit** command specifies the unit of delay statistics fields in result tables of the UDP Jitter and ICMP Jitter test instances.

When you run the **display nqa results** command to check the results of a single UDP Jitter or ICMP Jitter test instance:

- If the value of **SendProbe** is 0, no test packet has been sent, and **Packet Loss Ratio** is displayed as 100% (default value).
- If the value of **SendProbe** is not 0 and the value of **Packet Loss Ratio** is 100%, all test packets have been lost.

Example

Display the results of an NQA ICMP test.

```
<HUAWEI> display nqa results test-instance admin icmp
  NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
```

```
  Operation sequence errors number:0   RTT Status errors number:0
  Destination ip address:10.138.77.21
  Min/Max/Average Completion Time: 2/2/2
  Sum/Square-Sum  Completion Time: 6/12
  Last Good Probe Time: 2012-07-02 17:09:18.1
  Lost packet ratio: 0 %
```

Display detailed results of an NQA ICMP test.

```
<HUAWEI> display nqa results test-instance admin icmp verbose
 NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
 1 . Test 1 result   The test is finished
  Send operation times: 3              Receive response times: 3
  Completion:success                   RTD OverThresholds number: 0
  Attempts number:1                    Drop operation number:0
  Disconnect operation number:0        Operation timeout number:0
  System busy operation number:0       Connection fail number:0
  Operation sequence errors number:0   RTT Status errors number:0
  Destination ip address:10.138.77.21
  Min/Max/Average Completion Time: 2/2/2
  Sum/Square-Sum  Completion Time: 6/12
  Last Good Probe Time: 2012-07-02 17:09:18.1
  Lost packet ratio: 0 %
  Detailed result information:
```

Table 16-59 Description of the **display nqa results test-instance admin icmp** and **display nqa results test-instance admin icmp verbose** command output

Item	Description
NQA entry(admin, icmp)	NQA test items: - admin: indicates the administrator or creator of the NQA test instance. - icmp: indicates the name of the NQA test instance. You can run the **nqa** command to configure this parameter.
testflag	Test flag. - active: indicates that the test is running. Checking the result of a running test is invalid. - inactive: indicates that the test is complete. At this time, the actual test result is displayed.
testtype	Test type. You can run the **test-type** command to configure this parameter.
1 . Test 1 result	Sequence number of test results. Test results are numbered based on the time when the tests are complete.
The test is finished	Test status: - finished: indicates that the test is complete. - running: indicates that the test is running.
Send operation times	Number of sent packets.

Item	Description
Receive response times	Number of received response packets.
Completion	Completing status of the test: - success: indicates that the test is complete successfully. - no result: indicates that the test is running, so no test result is obtained or no test result is obtained after the test. - failed: indicates that the test fails.
RTD OverThresholds number	Number of times that the round-trip delay (RTD) threshold is exceeded.
Attempts number	Test times.
Drop operation number	Number of system resource allocation failures.
Disconnect operation number	Number of forcible disconnections.
Operation timeout number	Number of timeout operations during the test.
System busy operation number	Number of conflict operations.
Connection fail number	Number of times that the local end fails to establish connections with the peer.
Operation sequence errors number	Number of received disordered packets.
RTT Status errors number	Number of RTT status errors.
Destination ip address	Destination IP address of the test. You can run the **destination-address** command to configure this parameter.
Min/Max/Average Completion Time	Minimum/Maximum/Average time taken to complete the test.
Sum/Square-Sum Completion Time	Sum/square sum of the time taken to complete the test.
Last Good Probe Time	Time at which the last probe is complete.
Lost packet ratio	Packet loss ratio.
Detailed result information	Displays detailed result information.

Display the result of an NQA UDP Jitter test.

```
<HUAWEI> display nqa results test-instance admin jitter
 NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                        ResponseProbe:0
   Completion:failed                   RTD OverThresholds number:0
   OWD OverThresholds SD number:0       OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:0/0/0/0          RTT Square Sum:0
   NumOfRTT:0                          Drop operation number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   System busy operation number:0       Operation timeout number:60
   Min Positive SD:0                   Min Positive DS:0
   Max Positive SD:0                   Max Positive DS:0
   Positive SD Number:0                  Positive DS Number:0
   Positive SD Sum:0                   Positive DS Sum:0
   Positive SD Square Sum:0              Positive DS Square Sum:0
   Min Negative SD:0                   Min Negative DS:0
   Max Negative SD:0                   Max Negative DS:0
   Negative SD Number:0                  Negative DS Number:0
   Negative SD Sum:0                   Negative DS Sum:0
   Negative SD Square Sum:0              Negative DS Square Sum:0
   Min Delay SD:0                      Min Delay DS:0
   Avg Delay SD:0                      Avg Delay DS:0
   Max Delay SD:0                      Max Delay DS:0
   Delay SD Square Sum:0                 Delay DS Square Sum:0
   Packet Loss SD:0                    Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:0
   Average of Jitter SD:0              Average of Jitter DS:0
   Jitter out value:0.0000000           Jitter in value:0.0000000
   NumberOfOWD:0                         Packet Loss Ratio: 100%
   OWD SD Sum:0                          OWD DS Sum:0
   ICPIF value: 0                    MOS-CQ value: 0
   TimeStamp unit: ms                   Packet Rewrite Number: 0
   Packet Rewrite Ratio: 0%              Packet Disorder Number: 0
   Packet Disorder Ratio: 0%             Fragment-disorder Number: 0
   Fragment-disorder Ratio: 0%           Jitter OverThresholds SD number:0
   Jitter OverThresholds DS number:0    OverallOverThresholds number:0
   Start time: 2014-09-01 10:47:57+08:00
   End time: 2014-09-01 10:48:01+08:00
```

Table 16-60 Description of the **display nqa results test-instance admin jitter** command output

Item	Description
NQA entry(admin, jitter)	NQA test items: - admin: indicates the name of the administrator for an NQA test instance. - jitter: indicates the name of the NQA test instance.
testflag	Test flag: - active: indicates that the test is running. Checking the test result during the operation is invalid. - inactive: indicates that the test is complete. At this time, the actual test result is displayed.
testtype	Test type.

Item	Description
SendProbe	Number of sent probes.
ResponseProbe	Number of received response probes.
Completion	Completing status of the test: ● success: indicates that the test is complete successfully. ● no result: indicates that the test is running, so no test result is obtained or no test result is obtained after the test. ● failed: indicates that the test fails.
RTD OverThresholds number	Number of times that the RTD threshold is exceeded.
OWD OverThresholds SD number	Number of times that the one-way delay (OWD) threshold (from the source to the destination) is exceeded.
OWD OverThresholds DS number	Number of times that the OWD threshold (from the destination to the source) is exceeded.
Min/Max/Avg/Sum RTT	Minimum/Maximum/Average/Sum of the RTT.
RTT Square Sum	RTT square sum of the probes.
NumOfRTT	Number of RTTs.
Drop operation number	Number of system resource allocation failures.
Operation sequence errors number	Serial number of the error packets received by the client.
RTT Stats errors number	Number of RTT status errors.
System busy operation number	Number of conflict operations.
Operation timeout number	Number of timeout operations during the test.
Min Positive SD	Minimum positive jitter from the source to the destination.
Min Positive DS	Minimum positive jitter from the destination to the source.
Max Positive SD	Maximum positive jitter from the source to the destination.
Max Positive DS	Maximum positive jitter from the destination to the source.

Item	Description
Positive SD Number	Number of the positive jitter from the source to the destination.
Positive DS Number	Number of the positive jitter from the destination to the source.
Positive SD Sum	Sum of the positive jitter from the source to the destination.
Positive DS Sum	Sum of the positive jitter from the destination to the source.
Positive SD Square Sum	Square sum of the positive jitter from the source to the destination.
Positive DS Square Sum	Square sum of the positive jitter from the destination to the source.
Min Negative SD	Minimum negative jitter from the source to the destination.
Min Negative DS	Minimum negative jitter from the destination to the source.
Max Negative SD	Maximum negative jitter from the source to the destination.
Max Negative DS	Maximum negative jitter from the destination to the source.
Negative SD Number	Number of the negative jitter from the source to the destination.
Negative DS Number	Number of the negative jitter from the destination to the source.
Negative SD Sum	Sum of the negative jitter from the source to the destination.
Negative DS Sum	Sum of the negative jitter from the destination to the source.
Negative SD Square Sum	Square sum of the negative jitter from the source to the destination.
Negative DS Square Sum	Square sum of the negative jitter from the destination to the source.
Min Delay SD	Minimum delay from the source to the destination.
Min Delay DS	Minimum delay from the destination to the source.
Avg Delay SD	Average delay from the source to the destination.
Avg Delay DS	Average delay from the destination to the source.
Max Delay SD	Maximum delay from the source to the destination.

Item	Description
Max Delay DS	Maximum delay from the destination to the source.
Delay SD Square Sum	Square sum of the delay jitter from the source to the destination.
Delay DS Square Sum	Square sum of the delay jitter from the destination to the source.
Packet Loss SD	Maximum number of lost packets from the source to the destination.
Packet Loss DS	Maximum number of lost packets from the destination to the source.
Packet Loss Unknown	Number of packets lost at an unknown direction.
Average of Jitter	Average jitter.
Average of Jitter SD	Average jitter from the source to the destination.
Average of Jitter DS	Average jitter from the destination to the source.
Jitter out value	Jitter in sending packets.
Jitter in value	Jitter in receiving packets.
NumberOfOWD	Number of OWD packets.
Packet Loss Ratio	Packet loss ratio.
OWD SD Sum	Sum of OWD from the source to the destination.
OWD DS Sum	Sum of OWD from the destination to the source.
MOS-CQ value	Average estimate of VoIP performance.
ICPIF value	Advantage factor.
TimeStamp unit	Unit of the timestamp.
Packet Rewrite Number	Number of rewritten packets.
Packet Rewrite Ratio	Percentage of rewritten packets to total packets.
Packet Disorder Number	Number of out-of-order packets.
Packet Disorder Ratio	Percentage of out-of-order packets to total packets.
Fragment-disorder Number	Number of out-of-order fragmented packets.
Fragment-disorder Ratio	Percentage of out-of-order fragmented packets to total packets.
Jitter OverThresholds SD number	Number of times that a test instance is successfully performed with the jitter exceeding the specified threshold from the source to the destination.

Item	Description
Jitter OverThresholds DS number	Number of times that a test instance is successfully performed with the jitter exceeding the specified threshold from the destination to the source.
OverallOverThresholds number	Number of times that a test instance is successfully performed with any of the delays from the source to the destination or from the destination to the source, the bi-directional delay, the jitters from the source to the destination or from the destination to the source exceeding the set threshold.
Start time	Time when the test began.
End time	Time when the test ended.

16.7.13 display nqa-agent

Function

The **display nqa-agent** command displays the status and configuration of the specified or all NQA test instances on an NQA client.

Format

display nqa-agent [*admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 characters.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters.
verbose	Indicates detailed information about the client status of an NQA test.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the test instances are configured on an NQA client, run the **display nqa-agent** command to view the status and configuration of the specified or all NQA test instances on an NQA client.

Example

Display the status and configuration of all NQA test instances on an NQA client.

```
<HUAWEI> display nqa-agent
nqa test-instance admin ftp
 test-type ftp
 ftp-operation get
 nqa status : normal
nqa test-instance admin icmp
 nqa status : normal
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.10.10.10
 destination-port 100
 nqa status : normal
```

Table 16-61 Description of the **display nqa-agent** command output

Item	Description
nqa test-instance admin icmp test-type icmp destination-address ipv4 192.168.1.2 nqa status : normal	The administrator of NQA test instance **icmp** is **admin**. Configurations of this test instance include the following: ● test-type ● destination-address ● nqa status You can run the **nqa** command to configure an NQA test instance. Configurations of different NQA test instances are not the same. For details, see **Configuring an NQA Test Instance**.

16.7.14 display nqa-server

Function

The **display nqa-server** command displays information about NQA servers.

Format

display nqa-server

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display nqa-server** command can display information about NQA servers, including the maximum number of configurable NQA servers and the number and types of configured NQA servers.

Example

Display the information about NQA servers.

```
<HUAWEI> display nqa-server
NQA Server Max:100                    NQA Server Num:3
NQA Concurrent TCP Server:1              NQA Concurrent UDP Server:2
 nqa-server tcpconnect 10.1.1.1 2000    ACTIVE
 nqa-server udpecho 10.1.1.1 2000       ACTIVE
 nqa-server udpecho 10.1.1.1 6000       ACTIVE
```

Table 16-62 Description of the display nqa-server command output

Item	Description
NQA Server Max	Maximum number of NQA servers that can be configured.
NQA Server Num	Number of current NQA servers.
NQA Concurrent TCP Server	Number of the configured TCP servers.
NQA Concurrent UDP Server	Number of the configured UDP servers.
nqa-server	Running servers.
ACTIVE	Status of the NQA server.

16.7.15 dns-server

Function

The **dns-server** command configures the IP address of the domain name service (DNS) server in the NQA test.

The **undo dns-server** command deletes the configured IP address of the DNS server.

By default, the IP address of the DNS server is not configured.

Format

dns-server ipv4 *ip-address*

undo dns-server

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies an IPv4 address for the DNS server.	The value is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using a DNS test instance to detect the rate of resolving a given DNS name to an IP address, configure a DNS server first.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The test instance can only be a DNS or HTTP test instance.

Precautions

The DNS server configuration of a running test instance cannot be changed.

Example

Set the IP address of the DNS server to 10.1.1.1 in the test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type dns
[HUAWEI-nqa-user-test] dns-server ipv4 10.1.1.1
```

16.7.16 fail-percent

Function

The **fail-percent** command sets the failure percentage for the NQA test instance.

The **undo fail-percent** command deletes the configured failure percentage for the NQA test instance.

By default, the failure percentage is 100%. That is, the test is regarded as a failure only when all the probes fail.

Format

fail-percent *percent*

undo fail-percent

Parameters

Parameter	Description	Value
percent	Specifies the percentage of failed probes.	The value is an integer that ranges from 1 to 100.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, multiple probes are sent to test probe packets. Statistics obtained from multiple probe tests show the network quality.

In actual scenarios, however, a probe test may fail because of interference in the network. In addition, a failure in a probe test does not mean that the NQA test fails. The **fail-percent** command can be used to set failure percentage to check whether an NQA test fails or not. If the number of failure probe packets to the total number of probe packets reaches a specified percentage, the NQA test is considered as a failure.

For example, the number of sent packets set in the **probe-count** command is 10, but seven of them are lost during the probe test, the following situations occur:

- If the failure percentage is set to 80, the probe test is considered a success.
- If the failure percentage is set to 60, the probe test is considered a failure.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type of test instances that are not supported is as follows:

- FTP
- Trace
- LSP Trace
- PWE3 Trace
- DNS
- Path Jitter
- Path MTU

Precautions

The failure percentage of a running test instance cannot be changed.

Example

Set the percentage of the failed probes to 10% in the test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] fail-percent 10
```

16.7.17 frequency

Function

The **frequency** command sets the interval at which an NQA test instance is automatically performed.

The **undo frequency** command deletes the configured interval at which an NQA test instance is automatically performed.

By default, the interval at which an NQA test instance is automatically performed is not configured. That is, the test is performed once.

Format

frequency *interval*

undo frequency

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an NQA test instance is automatically performed.	The value is an integer that ranges from 1 to 604800, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **start** command to set the start time and end time of an NQA test. If you need to perform period test from the start time to the end time in a test instance, run the **frequency** command to set the interval at which an NQA test instance is automatically performed. After that, the NQA test is automatically performed once at each configured interval. Configuring the interval of periodic NQA test avoids time-consuming manual operations.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

If the master/slave switchover is performed on the NQA client before the test instance (group) is complete, the following situations may occur:

- If the interval for automatically performing the test is not set, the test stops after the master/slave switchover.
- If the interval for automatically performing the test instance is set, the test is performed from the next period after the master/slave switchover.

Precautions

- The frequency of a running test instance cannot be changed.
- In a trace, Path MTU, LSP trace, or PWE3 trace test, the configured **frequency** must be greater than or equal to 60s.
- The configured **frequency** cannot be less than the **timeout** value, otherwise, the test instance will start failed. If the configured **frequency** is smaller than or equal to (**probe-count** - 1) x **interval** + **timeout** + 1, the test result may be **no result**. For the test instance supporting the **jitter-packetnum** parameter, the number of sent packets is **probe-count** x **jitter-packetnum** packets.
- In an FTP test instance, the configured **frequency** must be 2s greater than the **timeout** value; otherwise, the FTP test instance may fail.

Example

Set the interval at which test instance **user test** is automatically performed to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] frequency 20
```

16.7.18 ftp-filename

Function

The **ftp-filename** command configures the file name and file path for an NQA FTP test instance.

The **undo ftp-filename** command deletes the file name and file path for an NQA FTP test instance.

By default, no file name and file path are configured.

Format

ftp-filename *file-name*

undo ftp-filename

Parameters

Parameter	Description	Value
file-name	Specifies the name and path of the operation file in an FTP test instance.	The value is a string of 1 to 230 characters.

Views

NQA view

Default Level

3: Management level

Usage Guidelines

The **ftp-filename** command is valid only for FTP test instances.

You cannot change the file path and file name of a running test instance.

If no file path is specified, the system searches for the file in the current path.

The file name cannot end with any forward slashes (/) or backward slashes (\).

The file name includes but is not limited to the extension name, such as .txt.

NOTE

Various FTP servers may support files with the file name in different length ranges. Before you configure this command, ensure that the target FTP server supports the length of the specified file name. Otherwise, NQA test results may fail to be transmitted using FTP.

Example

Set the FTP path and file name of test instance **user test** to **D:\abc** and **abc.txt** respectively.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type ftp
[HUAWEI-nqa-user-test] ftp-filename D:\abc\abc.txt
```

16.7.19 ftp-filesize

Function

The **ftp-filesize** command sets the size of the file used in an NQA FTP test instance.

The **undo ftp-filesize** command restores the default size of the file used in an NQA FTP test instance.

By default, the size of the file used in the FTP test is 1000 Kbytes.

Format

ftp-filesize *size*

undo ftp-filesize

Parameters

Parameter	Description	Value
size	Specifies the size of the file used in the FTP test.	The value is an integer that ranges from 1 to 10000, in Kbytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You cannot change the configured size of the file when the test is running.

If specifying the size of the upload file is adopted, the FTP client automatically generates the file name **nqa-ftp-test.txt**. If the test is performed several times, the newly uploaded file replaces the previous one.

The type of the test instance has been set to **ftp** using the **test-type** command.

Example

Set the size of the file to 1024 bytes in the FTP upload test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type ftp
[HUAWEI-nqa-user-test] ftp-filesize 1024
```

16.7.20 ftp-operation

Function

The **ftp-operation** command sets the operation mode for an NQA FTP test instance.

The **undo ftp-operation** command restores the default operation mode of an NQA FTP test instance.

By default, the operation mode of an FTP test instance is **get**.

Format

ftp-operation { **get** | **put** }

undo ftp-operation put

Parameters

Parameter	Description	Value
get	Indicates that the client downloads a file from the server and the download speed is recorded.	-
put	Indicates that the client uploads a local file or a created file to the server and the upload speed is recorded.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP download test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

The **ftp-operation** command can be used to specify the FTP operation mode as **put** or **get**. A connection with the FTP server is set up using the IP address, the user name, and the password of the FTP server, and the time to set up FTP connection is recorded.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The operation mode of a running test instance cannot be changed.

Example

Perform a test named **user test** to obtain the FTP download speed.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type ftp
[HUAWEI-nqa-user-test] ftp-operation get
```

16.7.21 ftp-password

Function

The **ftp-password** command sets a password for logging in to the FTP server in an NQA FTP test instance.

The **undo ftp-password** command deletes the configured password for logging in to the FTP server.

By default, no password is set for FTP test instances.

Format

ftp-password { *password* | **cipher** *cipher-password* }

undo ftp-password

Parameters

Parameter	Description	Value
password	Specifies the password for logging in to the FTP server in an FTP test instance.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. ● If the password is plaintext, the length ranges from 1 to 32. ● If the password is ciphertext, the length ranges from 32 to 68. ● If the password length is 32 and the configured ciphertext password can be decrypted successfully, the configured ciphertext password takes effect. If the configured ciphertext password cannot be decrypted, the plaintext password is used after passing the validity check. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
cipher *cipher-password*	Specifies the password for logging in to the FTP server in an FTP test instance.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. ● If the password is plaintext, the length ranges from 1 to 32. ● If the password is ciphertext, the length ranges from 32 to 68. ● If the password length is 32 and the configured ciphertext password can be decrypted successfully, the configured ciphertext password takes effect. If the configured ciphertext password cannot be decrypted, the plaintext password is used after passing the validity check. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **ftp-password** command can be used to set the specified user and password. Only the user who enters the authorized user name and password is authorized to access the network.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The password of a running test instance cannot be changed.

Example

Set the password for logging in to the FTP server to **Tester-123**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type ftp
[HUAWEI-nqa-user-test] ftp-password Tester-123
```

16.7.22 ftp-username

Function

The **ftp-username** command sets the user name for logging in to the FTP server in an FTP test instance.

The **undo ftp-username** command deletes the configured user name for logging in to the FTP server.

By default, no user name is set for FTP test instances.

Format

ftp-username *name*

undo ftp-username

Parameters

Parameter	Description	Value
name	Specifies the user name for logging in to the FTP server.	The value is a string of 1 to 255 case-sensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **ftp-username** command can be used to set the specified user in an FTP test. Only the user who enters the authorized user name and password is authorized to access the network.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The user name of a running test instance cannot be changed.

Example

Set the user name for logging in to the FTP server to **user1**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type ftp
[HUAWEI-nqa-user-test] ftp-username user1
```

16.7.23 http-operation

Function

The **http-operation** command sets the operation mode for an NQA HTTP test instance.

By default, the operation mode of the HTTP test instance is GET.

Format

http-operation get

Parameters

Parameter	Description	Value
get	Obtains data from the HTTP server.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

This command applies only to the HTTP test.

You cannot change the operation mode of a running HTTP test instance.

Example

Set the operation mode of HTTP test instance **user test** to **get**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type http
[HUAWEI-nqa-user-test] http-operation get
```

16.7.24 http-url

Function

The **http-url** command configures the uniform resource locator (URL) and version information for an HTTP test instance.

The **undo http-url** command deletes the configured URL and version information.

By default, no URL or version information is configured for an HTTP test instance.

Format

http-url *deststring* [*verstring*]

undo http-url

Parameters

Parameter	Description	Value
deststring	Specifies the name of the web page used for an HTTP test.	The value is a string of 1 to 230 case-insensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
verstring	Specifies the HTTP version.	The total length of *verstring* should be equal to or shorter than 7 characters. It can be set to v1.0 or 1.1. The default HTTP version is v1.0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HTTP1.0 and HTTP1.1 are supported in this test instance.

Precautions

The **http-url** command applies only to HTTP test instances. You cannot change the URL of a running HTTP test instance.

When running the **http-url** command, you need to specify a domain name or a server's IP address; otherwise, the test instance fails.

Example

Set the URL of HTTP test instance **user test** to **http://www.***.com**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type http
[HUAWEI-nqa-user-test] http-url http://www.***.com
```

16.7.25 icmp-jitter-mode

Function

The **icmp-jitter-mode** command specifies the mode of an ICMP jitter test.

The **undo icmp-jitter-mode** command restores the default mode of an ICMP jitter test.

By default, the ICMP jitter test is in **icmp-timestamp** mode.

Format

icmp-jitter-mode { **icmp-echo** | **icmp-timestamp** }

undo icmp-jitter-mode

Parameters

Parameter	Description	Value
icmp-echo	Configures the ICMP jitter test to use ICMP Echo messages.	-
icmp-timestamp	Configures the ICMP jitter test to use ICMP Timestamp messages.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **icmp-jitter-mode** command can only be used to configure the mode for ICMP jitter or path jitter tests.

Example

Configure the ICMP jitter test to use ICMP Echo messages.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin icmpjitter
[HUAWEI-nqa-admin-icmpjitter] test-type icmpjitter
[HUAWEI-nqa-admin-icmpjitter] icmp-jitter-mode icmp-echo
```

16.7.26 interval (NQA view)

Function

The **interval** command sets the interval at which NQA test packets are sent.

The **undo interval** command restores the default setting.

By default, the intervals for sending test packets in various tests are as follows:

- For UDP Jitter, Path Jitter, and ICMP Jitter test instance, the interval is 50 milliseconds on the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S and is 100 milliseconds for other devices.
- The interval is 4 seconds for other test instances.

Format

interval { **milliseconds** *interval* | **seconds** *interval* }

undo interval

Parameters

Parameter	Description	Value
milliseconds *interval*	Sets the interval at which packets are sent, in milliseconds. **NOTE** If the configured interval is a multiple of 1000 milliseconds, the system will automatically convert milliseconds into seconds.	The value is an integer that ranges from 20 to 60000.
seconds *interval*	Sets the interval at which packets are sent, in seconds.	The value is an integer that ranges from 1 to 60, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, multiple probes are sent. Statistics obtained from multiple probe tests show the network quality. Probe packets (or probes) are sent at a specified interval.

- If the network quality is poor, the interval at which packets are sent must be increased. Otherwise, the network performance may deteriorate.
- If the network quality is good, the interval at which are sent can be decreased to shorten the waiting time.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The **interval** command is valid only for the ICMP, ICMP Jitter, Path Jitter, SNMP, LSP Jitter, LSP Ping, PWE3 Ping, TCP, UDP, or UDP Jitter test instances.

Configuration Impact

- Packets can be sent at interval of milliseconds only in UDP Jitter, Path Jitter, or ICMP Jitter test instances. The interval at which packets are sent must be greater than the timeout period set using the **timeout** command in all test instances except the UDP Jitter, Path Jitter, or ICMP Jitter test instance.
- If the interval for sending packets has been configured, running the **interval** command will override the previous configuration.

Precautions

The interval for sending packets of a running test instance cannot be changed.

Example

Set the interval for sending test packets to 1000 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] interval milliseconds 1000
```

16.7.27 ip-forwarding

Function

The **ip-forwarding** command configures packets to be forcibly forwarded using IP on the first node.

The **undo ip-forwarding** command disables packets from being forcibly forwarded using IP on the first node.

Format

ip-forwarding

undo ip-forwarding

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

When a fault occurs on the network, you can first run the **ping** command to check network connectivity. On an MPLS network, if a fault occurs but the control layer fails to detect the fault, the ping operation fails. To fast identify whether the fault occurs on the MPLS network or on the IP network, you can configure IP packets to be forcibly forwarded using IP on the first node. This can help you fast locate the fault.

NOTE

Only ICMP test instances support this configuration.

If you configure both the **ip-forwarding** and **sendpacket passroute** commands, the **sendpacket passroute** command takes effect. Therefore, the device sends packets without searching the routing table.

Example

Configure packets to be forwarded using IP.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] ip-forwarding
```

16.7.28 jitter-packetnum

Function

The **jitter-packetnum** command sets the number of packets sent in each probe test instance.

The **undo jitter-packetnum** command restores the default number of packets sent in each probe test instance.

By default, 20 test packets are sent in each probe.

Format

jitter-packetnum *number*

undo jitter-packetnum

Parameters

Parameter	Description	Value
number	Specifies the number of test packets sent in each probe in the jitter test (**probe-count**).	The value is an integer that ranges from 1 to 3000. The default value is 20.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, the **jitter-packetnum** command can be used to set the number of consecutive packets to simulate the actual traffic of a data in a specified period of time. This helps simulate services more accurately.

For example, the **jitter-packetnum** command can be used to set the number of consecutive packets to 3000 and an interval of 20 ms to send packets. In this way, G.711 traffic can be simulated within one minute to detect VoIP services in UDP jitter test instances.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The number of sent packets can be configured only for UDP Jitter, LSP jitter, Path Jitter, and ICMP Jitter test instances.

Configuration Impact

- In UDP Jitter, LSP jitter, Path Jitter, and ICMP Jitter test instances, the number of sent packets = **jitter-packetnum** x **probe-count**, but the product cannot exceed 3000.
- If the number of probe packets has been set, running the **jitter-packetnum** command will override the previous configuration.

Precautions

The number of probe packets of a running test instance cannot be changed.

Example

Perform 3 probes in the test named **user test** and send 1000 packets in each probe.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] probe-count 3
[HUAWEI-nqa-user-test] jitter-packetnum 1000
```

16.7.29 local-pw-id

Function

Using the **local-pw-id** command, you can set the ID of the local end of a PW or a VC.

Using the **undo local-pw-id** command, you can delete the configured ID of the local end of a PW or a VC.

By default, **local-pw-id** is not configured.

Format

local-pw-id *local-pw-id*

undo local-pw-id

Parameters

Parameter	Description	Value
local-pw-id	Specifies the ID of the local end of a PW or a VC.	The value is a decimal integer. ● When the test instance is of PWE3Ping, the value of *local-pw-id* is an integer that ranges from 1 to 4294967295, and only the VC type of LDP is supported. ● When the test instance is of PWE3Trace: when the VC type is LDP, the value of *local-pw-id* is an integer that ranges from 1 to 4294967295; when the VC type is BGP, the value of *local-pw-id* is an integer that ranges from 0 to 65534.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PWE3 ping and PWE3 trace test instances can be used in the following scenarios:

Connectivity and faulty node detections for a single-hop PW. After the **local-pw-id** command is run in the NQA view to configure the local PW ID or VC ID, you can specify a PW for the detection.

Connectivity and faulty node detections for a multi-hop PW. After the **local-pw-id** command is run in the NQA view to configure the local PW ID or VC ID, you need to specify the destination address.

- If the **label-type** parameter is set to **control-word**, run the **remote-pw-id** *remote-pw-id* command to configure the remote PW ID.
- If the **label-type** parameter is set to **label-alert** or **normal**, run the **destination-address ipv4** *ipv4-address* [**lsp-masklen** *masklen* | **lsp-masklen** *masklen* **lsp-loopback** *loopback-address* | **lsp-loopback** *loopback-address* **lsp-masklen** *masklen*] command to configure the destination address for PWE3 ping and PWE3 trace test instances.

Prerequisites

Before running the **local-pw-id** command, you must set the NQA test type to PWE3 Trace or PWE3 Ping in the NQA view.

Precautions

The *local-pw-id* value must be the same as the **VC ID** value in the **display mpls l2vc** command output; otherwise, the test may fail.

Example

Set the ID of the local end of a PW to 100 in the NQA view.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] local-pw-id 100
```

16.7.30 local-pw-type

Function

Using the **local-pw-type** command, you can configure the PW type of the local end.

Using the **undo local-pw-type** command, you can cancel setting the PW type of the local end.

By default, the PW type of the local end is Ethernet.

Format

local-pw-type *local-pw-type*

undo local-pw-type

Parameters

Parameter	Description	Value
local-pw-type	Specifies the PW type of the local end.	Currently, encapsulation types **ethernet**, **ip-interworking** and **vlan**are supported. By the default, the value is **ethernet**.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **local-pw-type** command is used to configure a PW encapsulation type for the local PE. The PW encapsulation type configured for the local PE must be the same as the PW encapsulation type for the remote PE.

Prerequisites

Before configuring the **local-pw-type** command, configure the test type of NQA test instances as PWE3 trace or PWE3 ping in the NQA view.

Precautions

The *local-pw-type* value must be the same as the **VC type** value in the **display mpls l2vc** command output; otherwise, the test may fail.

Example

In the NQA view, configure the local pw-type as VLAN.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] local-pw-type vlan
```

16.7.31 label-type

Function

Using the **label-type** command, you can configure the label type.

Using the **undo label-type** command, you can cancel the operation of configuring the label type.

By default, the label type is **control-word**.

Format

label-type { **control-word** | { **label-alert** | **normal** } [**no-control-word**] }

undo label-type

Parameters

Parameter	Description	Value
control-word	Indicates that the control word option is encapsulated in MPLS Echo Request packets.	-
label-alert	Indicates that the router alert option is encapsulated in MPLS Echo Request packets.	-
normal	Indicates that neither control words nor router alert options are encapsulated in MPLS Echo Request packets.	-
no-control-word	Indicates that the control word option is not encapsulated in MPLS Echo Request packets. This parameter can be used in NQA PWE3 ping and NQA PWE3 trace tests.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The usage scenarios of the label types are as follows:

- **control-word**:
  - If the encapsulation type is set to **control-word**, at a switch node on a multi-hop PW, the MPLS Echo Request packets are not delivered to the CPU for processing until the TTL of the label times out. In this case, the source obtains little PW information. This type, however, ensures system performance and the source cannot learn information on the downstream interfaces of the switch node. You should use this type when there are a great number of packets.
  - Only **control-word** is supported when the vc-type is BGP and lsp-version is draft6.
- **label-alert**:

  - If the encapsulation type is set to **label-alert**, at a switch node on a multi-hop PW, the MPLS Echo Request packets are delivered to the CPU for processing. In this case, the source can obtain more PW information. The system performance is greatly affected when there are a great number of packets. You can use this type to obtain details about the switch node when test instances are few.
  - Only **control-word** or **label-alert** is supported when the vc-type is BGP and lsp-version is rfc4379.
- In the case that a device communicates with Huawei devices running earlier versions and the label alert or normal mode is adopted, the **no-control-word** option must be carried in the test packets.
- **normal** is unsupported when the lsp-version is draft6.

Prerequisites

Before running the **label-type** command, you must set the test type to PWE3 Trace or PWE3 Ping in the NQA view; otherwise, **label-type** cannot be specified.

Precautions

The **label-type** value must be the same as the **local VCCV** value in the **display mpls l2vc** command output; otherwise, the test may fail.

Example

Configure the encapsulation type of test packets as **label-alert** in the NQA view.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] label-type label-alert
```

16.7.32 lsp-exp

Function

The **lsp-exp** command configures the LSP EXP value of MPLS Echo Request packets in an NQA test instance.

Using the **undo lsp-exp** command, you can restore the default setting.

By default, LSP EXP is 0.

Format

lsp-exp *exp*

undo lsp-exp

Parameters

Parameter	Description	Value
exp	Specifies the LSP EXP value of an NQA test instance.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MPLS experimental bits (EXP) field is a 3-bit field in the MPLS header used to mark the precedence of MPLS packets.

Test packets are added to different queues according to their LSP EXP values, so that

- Congestion on the link can be avoided.
- Specified queue can be detected.

Precautions

This command applies to only the LSP test.

You cannot change the configured LSP EXP value when the test is performed.

Example

Set the LSP EXP value to 5.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-exp 5
```

16.7.33 lsp-nexthop

Function

The **lsp-nexthop** command is used to configure the IP address of the next hop in the case that load balancing is enabled.

Using the **undo lsp-nexthop** command, you can cancel the current setting.

By default, the next-hop IP address of any link that participates in load balancing.

Format

lsp-nexthop *nexthop-ip-address*

undo lsp-nexthop

Parameters

Parameter	Description	Value
nexthop-ip-address	Specifies the next hop address.	It is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two conditions must be met before you use the command:

- **lsp-type** is IPv4
- **lsp-version** is RFC4379

You can use the **lsp-nexthop** command to configure the IP address of the next hop. Test instance type supported as following:

- LSP Ping
- LSP Trace
- LSP Jitter

Precautions

A running test instance cannot be configured with the next hop address.

Example

Specify the next hop address for the LSP Ping test instance whose LSP type is IPv4 and lsp-version is rfc4379.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-type ipv4
[HUAWEI-nqa-user-test] lsp-version rfc4379
[HUAWEI-nqa-user-test] lsp-nexthop 10.1.2.20
```

16.7.34 lsp-replymode

Function

Using the **lsp-replymode** command, you can set the reply mode for the LSP test.

Using the **undo lsp-replymode** command, you can restore the default setting.

By default, UDP packets are used.

Format

lsp-replymode { **no-reply** | **udp** }

undo lsp-replymode

Parameters

Parameter	Description	Value
no-reply	Indicates that the LSP test is not responded.	If the **no-reply** parameter is specified in the command, the destination does not respond to NQA probe packets. This configuration is used to collect the statistics on or process received probe packets on the destination host, and no response packets need to be sent. Meanwhile, the NQA test instance fails because the client does not receive response packets.
udp	Indicates that IPv4 UDP packets are used to respond to the LSP test.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **lsp-replymode** command, you can set the reply mode for the LSP test. The supported test instances are:

- LSP Ping
- LSP Trace
- LSP Jitter

- PWE3 Ping
- PWE3 Trace

Precautions

lsp-replymode no-reply indicates the unidirectional test. If the client displays timeout, it indicates that the test succeeds; or the client displays that the LSP is non-existent.

You cannot change the reply mode of the currently performed LSP test.

Example

Set the reply mode of the test named **user test** to sending UDP packets.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-replymode udp
```

16.7.35 lsp-tetunnel

Function

The **lsp-tetunnel** command configures the TE tunnel used in an NQA LSP test.

The **undo lsp-tetunnel** command deletes the configured TE tunnel.

By default, no TE tunnel is configured for an LSP test instance.

Format

lsp-tetunnel tunnel *interface-number* [**hot-standby** | **primary**]

undo lsp-tetunnel

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the tunnel interface number.	-
hot-standby	Indicates the hot-standby tunnel of the TE tunnel.	-
primary	Indicates the primary tunnel of the TE tunnel.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hot standby: An ordinary backup CR-LSP is set up immediately after a primary CR-LSP is set up. The ordinary backup CR-LSP takes over traffic if the primary CR-LSP fails. After the primary CR-LSP recovers, traffic switches back.

CR-LSP backup can be configured to allow traffic to switch from a primary CR-LSP to a backup CR-LSP, providing end-to-end protection.

An NQA LSP test instance can check the reachability of the following LSPs and collect SLA statistics:

- MPLS TE tunnel: Run the **lsp-tetunnel** *interface-type interface-number* command to configure an interface number for an MPLS TE tunnel.
- Hot-standby MPLS CR-LSP: Run the **lsp-tetunnel** *interface-type interface-number* **hot-standby** command to configure an interface number for a hot-standby MPLS CR-LSP.
- Primary MPLS TE tunnel: Run the **lsp-tetunnel** *interface-type interface-number* **primary** command to configure an interface number for a primary MPLS TE tunnel.

Prerequisites

Before using the **lsp-tetunnel** command to configure the TE tunnel in an NQA LSP test instance, perform the following operations:

- Run the **interface tunnel** *interface-number* command to create a tunnel interface.
- Run the **lsp-type te** command to set the NQA LSP test type to TE.

Precautions

LSP Jitter test instances cannot test the hot-standby tunnel of a TE tunnel.

You cannot change the TE tunnel when the LSP test is performed.

Example

Configure the TE tunnel of the test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] quit
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-type te
[HUAWEI-nqa-user-test] lsp-tetunnel tunnel 1
```

Configure the CR-LSP hot-standby tunnel of the test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] quit
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-type te
[HUAWEI-nqa-user-test] lsp-tetunnel tunnel 1 hot-standby
```

16.7.36 lsp-type

Function

Using the **lsp-type** command, you can configure the LSP test type.

Using the **undo lsp-type** command, you can cancel configuring the LSP test type.

By the default, the value of lsp-type is ipv4.

Format

lsp-type { **ipv4** | **te** | **ipv4-vpn** }

undo lsp-type

Parameters

Parameter	Description	Value
ipv4	Sets the test type to IPv4 LSP ping/trace/jitter.	-
te	Sets the type to LSP ping/trace/jitter of the TE tunnel.	-
ipv4-vpn	Sets the LSP test type to IPv4 L3VPN.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **lsp-type** command can be used to configure the LSP test type of an NQA test instance to detect an LDP or a TE tunnel.

- If **ipv4** is configured, the NQA test instance is used to detect the connectivity of a specified LDP LSP. The destination address of the test instance is configured using the **destination-address** command.
- If **te** is configured, the NQA test instance is used to detect the connectivity of a specified TE tunnel. The destination address of the test instance is configured using the **lsp-tetunnel** command.
- If the **ipv4-vpn** parameter is set, the NQA test case is used to test LSPs on a BGP-based L3VPN network.
  - To test a primary LSP on a BGP-based L3VPN network, specify the destination address using the **destination-address lsp-masklen** *masklen* command.

  - To test a primary LSP on a BGP-based L3VPN network, specify the destination address using the **destination-address lsp-masklen** *masklen* **vpn-frr-path** command.

Prerequisites

- If the LSP test type is set to IPv4, the NQA test instance type must be set to LSP ping, LSP trace, or LSP jitter.
- If the LSP test type is set to TE, the NQA test instance type must be set to LSP ping, LSP trace, or LSP jitter.
- If the LSP test type is set to IPv4 L3VPN, the NQA test instance type must be set to LSP ping.

Precautions

The type of an LSP test that is running cannot be changed.

After the **lsp-type** command is configured, the **destination-address**, **lsp-tetunnel**, and **lsp-version** commands cannot be configured.

Example

Set the type of the test named **user test** to Ipv4 LSP ping.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-type ipv4
```

16.7.37 lsp-version

Function

Using the **lsp-version** command, you can configure the protocol that is used by the LSP test instance.

Using the **undo lsp-version** command, you can restore the default setting.

By default, draft6 is adopted.

Format

lsp-version { **rfc4379** | **draft6** }

undo lsp-version

Parameters

Parameter	Description	Value
rfc4379	Indicates that the protocol defined in RFC 4379 is adopted.	-
draft6	Indicates that Draft-ietf-mpls-lsp-ping-06 is adopted.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **lsp-version** command can be used to specify the protocol that is used by the LSP test instance.

Prerequisites

If **draft6** or **rfc4379** is specified in the **lsp-version** command, specify **lspping**, **lsptrace**, **lspjitter**, **pwe3ping**, or **pwe3trace** in the **test-type** command.

NOTE

The protocol adopted by a running LSP test instance cannot be changed.

Example

Configure the LSP test instance to use the protocol defined in RFC 4379.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type lspping
[HUAWEI-nqa-user-test] lsp-version rfc4379
```

16.7.38 md

Function

Using the **md** command, you can specify the Maintenance Domain (MD) and Maintenance Association (MA) of the NQA test packet to be sent. This command takes effect only in the MAC Ping test instance.

Using the **undo md** command, you can remove the specified MD from the NQA test packet to be sent.

By default, no MD is specified.

Format

md *md-name* **ma** *ma-name*

undo md

Parameters

Parameter	Description	Value
md-name	Specifies an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces.

Parameter	Description	Value
ma-name	Specifies an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to specify the MD and MA of an MAC Ping test instance. This command has the same effect as the operation of checking the connectivity fault in the MA view. Before running this command, you need to create an MD and MA, and set the test type to macping.

You cannot modify the MD and MA when the test instance is running. The total length of *ma-name* and *md-name* combination cannot be greater than 44 characters.

Example

Set the test type of an NQA test instance to MAC Ping and specify the MD name to "mdcustomer" and the MA name to "macustomer".

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type macping
[HUAWEI-nqa-user-test] md mdcustomer ma macustomer
```

16.7.39 mep

Function

Using the **mep** command, you can configure the MEP ID for an NQA test instance.

Using the **undo mep** command, you can delete the MEP ID configured for an NQA test instance.

By default, the MEP ID for an NQA test instance is 0.

Format

mep mep-id *mep-id*

undo mep

Parameters

Parameter	Description	Value
mep-id	Specifies the MEP ID of an NQA test instance.	The value is an integer ranging from 1 to 8191.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Before starting an NQA test instance, you need to run the **mep-id** *mep-id* command to configure the EOAM module. Otherwise, the normal operation of the NQA test instance will be affected.

This command is available for NQA MAC ping test instances.

Example

Set the MEP ID of an NQA MAC ping test instance to 1.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance test macping
[HUAWEI-nqa-test-macping] test-type macping
[HUAWEI-nqa-test-macping] mep mep-id 1
```

16.7.40 nexthop

Function

The **nexthop** configures a next hop address for NQA test packets.

The **undo nexthop** deletes the configured next hop address for the NQA test packets.

By default, the next hop address for the NQA test packets is obtained by searching the routing table.

Format

nexthop ipv4 *ip-address*

undo nexthop

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies a next hop address for NQA test packets.	The value is in dotted decimal notation. **NOTE** The specified next hop must be the physical interface directly connected to the device that sends the NQA test packets.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario that an NQA test instance is associated with static routes, if a link becomes faulty, the NQA test instance detects this fault and then the static routes associated with the NQA test instance become Down. After the link recovers, the NQA test instance attempts to send ICMP test packets over the static routes. Because these static routes are still Down, the NQA test instance still fails to detect link connectivity. Traffic fails to be forwarded.

The **nexthop** command configures a next hop address for the NQA test packets, which ensures that the packets are forwarded when the link recovers from the fault, and the static routes associated with the NQA test instance are Up.

Prerequisites

Only the NQA ICMP test instance allows you to specify a next hop address for NQA test packets.

Precautions

After you configure a next hop address for an NQA ICMP test instance, the test instance packets will be sent based on the address.

You can also run the **source-interface** command to specify an outbound interface through which the NQA ICMP test instance packets are sent to the specified next hop address. To guarantee that the test packets are sent, the following two conditions must be met:

- The specified next hop address matches the outbound interface.
- The specified outbound interface cannot be the member interface of a logical interface.

Example

Configure a next hop address for NQA ICMP test packets.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] nexthop ipv4 10.1.1.1
```

16.7.41 nqa

Function

The **nqa** command creates an NQA test instance and enters the NQA view.

The **undo nqa** command deletes an NQA test instance.

Format

nqa test-instance *admin-name test-name*

undo nqa { **test-instance** *admin-name test-name* | **all-test-instance** }

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 characters without question marks (?), spaces, or hyphens (-). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters without question marks (?), spaces, or hyphens (-). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-test-instance	Specifies all NQA test instances.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA is an integrated network test function. NQA test instances can accurately detect network running status, collect test statistics, and reduce costs.

NQA measures the performance of different protocols running on the network. NQA allows enterprise users to collect network operation indexes in real time, such as total delay of the HTTP, TCP connection delay, DNS resolution delay, file transmission delay, FTP connection delay, and DNS resolution error ratio.

To check these performance indexes, you can create NQA test instances. The two ends of an NQA test are called the NQA client and NQA server. The NQA client is responsible for initiating an NQA test. After receiving packets, the NQA server sends response messages to the NQA client. You can learn about the running status of a corresponding network according to the returned packets.

Configuration Impact

After the **undo nqa all-test-instance** command is run, all NQA test instances except the running test instance will be deleted.

Precautions

A running test instance cannot be deleted.

Example

Create a test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test]
```

16.7.42 nqa-jitter tag-version

Function

The **nqa-jitter tag-version** command sets the packet version for a UDP Jitter test instance.

The **undo nqa-jitter tag-version** command restores the default packet version for a UDP Jitter test instance.

By default, the packet version of a UDP Jitter test instance is 1.

Format

nqa-jitter tag-version *version-number*

undo nqa-jitter tag-version

Parameters

Parameter	Description	Value
version-number	Specifies the packet version for a UDP Jitter test instance.	The value can be 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Version 1 does not support unidirectional packet loss statistics.

Version 2 produces more accurate packet statistics, which helps network administrators to locate network faults and detect malicious attacks towards the network. After version 2 and collecting the packet loss across a unidirectional link are enabled, you can view the packet loss across the link from the source end to the destination end, from the destination end to the source end, or in an unknown direction in the test results.

Therefore, configuring version 2 is recommended.

Configuration Impact

If the packet version of a UDP Jitter test instance has been configured, running the **nqa-jitter tag-version** command will override the previous configuration.

Precautions

No matter the version number of the UDP Jitter test packet is 1 or 2, you need to run the **nqa-server udpecho** command to configure the NQA server. Otherwise, the UDP Jitter test instance will fail due to timeout.

Example

Set the packet version of a UDP Jitter test instance to 2.

```
<HUAWEI> system-view
[HUAWEI] nqa-jitter tag-version 2
```

16.7.43 nqa-server tcpconnect

Function

The **nqa-server tcpconnect** command configures the IP address and port number for the TCP server in an NQA TCP test instance.

The **undo nqa-server tcpconnect** command deletes the IP address and port number configured for the TCP server in an NQA TCP test instance.

By default, no IP address or port number is configured for the TCP server in an NQA TCP test instance.

Format

nqa-server tcpconnect [**vpn-instance** *vpn-instance-name*] *ip-address port-number*

undo nqa-server tcpconnect { **all** | [**vpn-instance** *vpn-instance-name*] *ip-address port-number* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the TCP server belongs. **NOTE** This parameter is invalid when a loopback address is specified as the TCP server address.	The value must be an existing VPN instance name.
all	Indicates all TCP listening addresses and port numbers.	-
ip-address	Specifies the IP address of the TCP server for monitoring TCP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the TCP server for monitoring TCP services.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA TCP test is used to detect the rate at which a TCP connection is set up between an NQA client and a TCP server through the three-way handshake. In a

TCP test instance, a TCP server needs to be configured on the server end to respond to probe packets.

Perform the following steps on the client to configure TCP server parameters:

- Run the **destination-address** command to configure the destination address of an NQA test instance or the IP address of the TCP server.
- Run the **destination-port** command to configure the destination port number of an NQA test instance, or the port number of the TCP server.

If the client and the server are connected through a VPN, you need to specify the VPN instance name.

Configuration Impact

Running the **undo nqa-server tcpconnect all** command will delete the IP address and port number of the TCP server.

Precautions

A TCP server is configured only in a TCP test instance.

Example

Create a TCP server for an NQA test instance with the IP address as 10.10.10.1 and the port number as 5000.

```
<HUAWEI> system-view
[HUAWEI] nqa-server tcpconnect 10.10.10.1 5000
```

16.7.44 nqa-server udpecho

Function

The **nqa-server udpecho** command configures the IP address and port number for the UDP server in an NQA test.

The **undo nqa-server udpecho** command deletes the IP address and port number configured for the UDP server in an NQA test.

By default, no IP address or port number is configured for the UDP server in an NQA test.

Format

nqa-server udpecho [**vpn-instance** *vpn-instance-name*] { *ip-address* | **ipv6** *ipv6-address* } *port-number*

undo nqa-server udpecho { [**vpn-instance** *vpn-instance-name*] { *ip-address* | **ipv6** *ipv6-address* } *port-number* | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the server belongs. **NOTE** This parameter is invalid when a loopback address is specified as the UDP server address.	The value is a string of 1 to 31 characters.
all	Specifies a server for all NQA test instances.	-
ip-address	Specifies the IP address of the server for monitoring UDP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the server for monitoring UDP services.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.
ipv6 *ipv6-address*	Specifies the IPv6 address of the server for monitoring UDP services.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a UDP server.

UDP packets are transmitted in a UDP Jitter test. The test is used to obtain the packet delay, jitter, and packet loss ratio by comparing timestamps in the request and response packets. A UDP server needs to be configured for an NQA test to respond to probe packets.

If the local IPv4 address cannot be predicted because of dynamic address allocation by DHCP, specify the **auto-address** keyword to configure the UDP service on the NQA server to automatically monitor all IPv4 addresses.

Configuration Impact

Running the **undo nqa-server udpecho all** command will delete the IP address and port number of the UDP server for all NQA UDP test instances.

Precautions

If the client and the server are connected through a VPN, you need to specify the VPN instance name.

No matter the version number of the UDP Jitter test packet is 1 or 2, you need to configure the NQA server. Otherwise, the UDP Jitter test instance will fail due to timeout.

Example

Create an NQA UDP monitoring server with the IP address 10.10.10.2 and the port number 6000.

```
<HUAWEI> system-view
[HUAWEI] nqa-server udpecho 10.10.10.2 6000
```

16.7.45 peer-address (NQA view)

Function

The **peer-address** command specifies a peer IP address for an NQA PWE3 ping or trace test instance.

The **undo peer-address** command restores the default setting.

By default, no peer IP address is specified for an NQA PWE3 ping or trace test instance.

Format

peer-address *peer-address*

undo peer-address *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies a peer IP address for an NQA PWE3 ping or trace test instance.	The value is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

For an NQA PWE3 ping or trace test instance, if the primary and secondary VCs are configured with the same VC ID, the **peer-address** command must be configured to specify a peer IP address. This configuration determines a unique PW for the NQA test.

Example

Specify 10.1.1.1 as the peer IP address of an NQA PWE3 ping test instance.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pwe3ping
[HUAWEI-nqa-user-test] peer-address 10.1.1.1
```

16.7.46 probe-count

Function

The **probe-count** command sets the number of probes for an NQA test instance.

The **undo probe-count** command restores the default number of probes for an NQA test instance.

By default, the number of probes for an NQA test instance is 3.

Format

probe-count *number*

undo probe-count

Parameters

Parameter	Description	Value
number	Specifies the number of probes in an NQA test instance.	The value is an integer that ranges from 1 to 15. The default value is 3. **NOTE** The number of probes in a trace test instance cannot be more than 10.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NQA test consists of multiple probes. By default, if one or more probes are successful in an NQA test, the test is considered successful. If all probes fail, the test is considered a failure. The number of probes in an NQA test is based on the network quality.

- If the network to be tested is a reliable network, the number of probes can be set relatively small because the probe can be successful after a small number of probe packets are sent.
- If the network to be tested is an unreliable network, the number of probes can be set relatively large because the probe can be successful only after a large number of probe packets are sent.

You can also detect the network quality based on statistics obtained from multiple probes. For example,

- If the probe test is successful after a small number of probes packets are sent, the network quality is good.
- If the probe test is successful after a large number of probes packets are sent, the network quality is poor.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type of test instances that are not supported is as follows:

- FTP
- DNS

Configuration Impact

- In UDP Jitter test instances, ICMP Jitter test instances, Path Jitter test instances, LSP Jitter test instances, the number of sent packets = **probe-count** x **jitter-packetnum**, but the product cannot exceed 3000.
- If the number of probes has been configured, running the **probe-count** command will override the previous configuration.

Precautions

The number of probes of a running test instance cannot be changed.

Example

Set the number of probes to 6 in NQA test instance **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] probe-count 6
```

16.7.47 probe-failtimes

Function

The **probe-failtimes** command sets the threshold for the number of traps to be sent when the NQA test fails. That is, test packet fragmentation is not allowed.

The **undo probe-failtimes** command restores the default threshold for the number of traps to be sent when the NQA test fails.

By default, one trap is sent for each probe failure.

Format

probe-failtimes *times*

undo probe-failtimes

Parameters

Parameter	Description	Value
times	Specifies the threshold for the number of traps to be sent when the NQA test fails, that is, the number of continuous probe failures.	The value is an integer that ranges from 1 to 15. The default value is 1.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA probe test is used to check whether response packets are received in a probe. If the number of continuous probe failures reaches the specified value, the system sends a trap to the specified NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command. Path jitter and Path MTU test are not supported.

Follow-up Procedure

Run the **send-trap probefailure** command to enable the system to send a trap to the NMS after a probe fails. Otherwise, the trap cannot be sent to the NMS after a probe fails.

Precautions

This configuration of a running test instance cannot be changed.

If the test instance does not support **probe-count**, you are advised to set **probe-failtimes** to 1; otherwise, traps cannot be sent.

If the test instance supports **probe-count**, you are advised to set **probe-failtimes** to be smaller or equivalent to probe-count; otherwise, traps cannot be sent.

Example

Set the number of continuous probe failures to 10 in the test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type tcp
[HUAWEI-nqa-user-test] probe-failtimes 10
```

16.7.48 records

Function

The **records** command sets the maximum number of history records and the maximum number of test results for NQA test instances.

The **undo records** command restores the default maximum number of history records and the default maximum number of test results for NQA test instances.

By default, the number of history records is 50, and the number of test results is 5.

Format

records { **history** *number* | **result** *number* }

undo records { **history** | **result** }

Parameters

Parameter	Description	Value
history *number*	Specifies the maximum number of history records.	The value is an integer that ranges from 0 to 1000. The default value is 50.
result *number*	Specifies the maximum number of test results.	The value is an integer that ranges from 1 to 10. The default value is 5.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **records** command to set the maximum number of history records and the maximum number of test results for NQA test instances.

By default, a test instance supports 50 history records. You need to limit the number of history records on the device. In addition, you need to set the number of allowed remaining history records that can be added. The configured maximum number of history records cannot exceed the sum of the total default number of history records and the remaining number of history records.

Precautions

The type of a test instance has been specified using the **test-type** command. Path MTU test is not supported.

This configuration of a running test instance cannot be changed.

Example

Set the maximum number of history records to 30 for test instance **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] records history 30
```

16.7.49 remote-pw-id

Function

Using the **remote-pw-id** command, you can configure the ID of the remote end of a PW or a VC.

Using the **undo remote-pw-id** command, you can remove the configured ID of the remote end of a PW or a VC.

When the VC type is LDP, **remote-pw-id** defaults to be 0.

Format

remote-pw-id *remote-pw-id*

undo remote-pw-id

Parameters

Parameter	Description	Value
remote-pw-id	Specifies the ID of the remote end of a PW or a VC.	The value is a decimal integer. ● In the case of a PWE3 ping test instance, the value of *remote-pw-id* is an integer that ranges from 1 to 4294967295, and only the VC type of LDP is supported. The default value is 0, indicating that the ID of the remote end of a PW is not configured. ● In the case of a PWE3 trace: if the VC type is LDP, the value of *remote-pw-id* is an integer that ranges from 1 to 4294967295. The default value is 0; if the VC type is BGP, the value of *remote-pw-id* is an integer that ranges from 0 to 65534.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before running the **remote-pw-id** command, you must set the test type to PWE3 Trace or PWE3 Ping in the NQA view.

Precautions

You cannot configure the **remote-pw-id** command after setting **lsp-version** to **rfc4379**.

The *remote-pw-id* value must be the same as the **VC ID** value in the **display mpls l2vc remote-info verbose** command output; otherwise, the test may fail.

Example

In the NQA view, configure the ID of the remote end of a PW to 100, the administrator to admin, and the test type to PWE3 trace.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] remote-pw-id 100
```

16.7.50 restart (NQA view)

Function

The **restart** command restarts the current running test instance.

Format

restart

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Function of the **restart** command is the same as that of the **start now** command.

Example

Restart the test instance named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] destination-port 8000
[HUAWEI-nqa-user-test] destination-address ipv4 10.1.1.1
[HUAWEI-nqa-user-test] restart
```

16.7.51 sendpacket passroute

Function

The **sendpacket passroute** command enables test packets to be sent without searching the routing table.

The **undo sendpacket passroute** command restores the default setting.

By default, the test packet is sent according to the routing table.

Format

sendpacket passroute

undo sendpacket passroute

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The type of a test instance has been specified using the **test-type** command. The type of test instances that are supported is as follows:

- ICMP
- TCP
- UDP
- HTTP
- UDP Jitter
- FTP
- SNMP
- Trace

Precautions

You cannot change this configuration of a running test instance.

If you configure both the **sendpacket passroute** and **source-interface** commands, the **source-interface** command takes effect. In this scenario, packets are sent from the interface specified using the **source-interface** command.

After the **sendpacket passroute** command is executed, the device sends test packets without searching the routing table. However, the configurations of **ttl** and **ip-forwarding** become invalid.

Example

Enable test packets to be sent without searching the routing table.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] sendpacket passroute
```

16.7.52 send-trap

Function

The **send-trap** command configures conditions for sending traps.

The **undo send-trap** command deletes the previous configuration.

By default, the device is disabled from sending traps.

Format

send-trap { **all** | { **probefailure** | **rtd** | **testcomplete** | **testfailure** | **testresult-change** } * }

undo send-trap { **all** | { **probefailure** | **rtd** | **testcomplete** | **testfailure** | **testresult-change** } * }

Parameters

Parameter	Description	Value
all	Indicates that a trap is sent in any of the following situations: ● The RTD exceeds the threshold. ● NQA probes fail. ● An NQA test succeeds. ● NQA tests fail.	-
probefailure	Indicates that a trap is sent when the number of probe failures reaches the threshold. **NOTE** This parameter does not apply to the UDP Jitter and ICMP Jitter test instances.	-
rtd	Indicates that a trap is sent when the RTD exceeds the threshold.	-
testcomplete	Indicates that a trap is sent when a test succeeds.	-
testfailure	Indicates that a trap is sent when the number of test failures reaches the threshold.	-
testresult-change	Indicates that a trap is sent when the probe result changes. **NOTE** This function supports only ICMP test instances.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traps are generated no matter whether the NQA test succeeds or fails. You can determine whether traps are sent to the NMS by enabling or disabling the trap function.

The device sends traps to the NMS in any of the following situations:

- The RTD exceeds the threshold.

  If the RTD exceeds the threshold, the device sends a trap to the NMS using the configured address.
- NQA probes fail.

  When no response packet is received after a specified number of continuous test packets are sent, the device sends a trap to the NMS using the configured address.
- An NQA test succeeds.

  When the device receives a response packet from a destination address, the device sends a trap to the NMS using the configured address.
- NQA tests fail.

  When the number of continuous test failures reaches the maximum number, the device sends a trap to the NMS using the configured address.

You can run the **send-trap** command to configure conditions for sending traps. When a condition is met, the device sends a trap to the NMS.

probefailure indicates that a trap is sent when the number of probe sending failures reaches the threshold set using the **probe-failtimes** command within a detection period. **testfailure** indicates that all probes fail to be sent within a detection period. When the number of detection failures reaches the threshold set using the **test-failtimes** command, a trap is sent. For example, if three probes are sent in a detection period and probe-failtimes and test-failtimes are set to 1, the alarm specified by probefailure is triggered when one probe fails to be sent and two probes are successfully sent. If all the three probes fail to send packets, the alarm specified by testfailure is triggered.

Prerequisites

The type of a test instance has been specified using the **test-type** command. Path jitter and Path MTU test are not supported.

The route between the device and NMS is reachable, and related configurations are complete. The host where traps are sent is configured using the **snmp-agent target-host trap** command; otherwise, traps cannot be sent to the NMS.

Precautions

You cannot change this configuration of a running test instance.

Example

Configure the test instance **user test** to send a trap when the test fails.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
```

```
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] send-trap testfailure
```

16.7.53 sender-address

Function

The **sender-address** command configures the source IP address in the multi-hop PW scenario.

The **undo sender-address** command restores the default setting.

By default, no source IP address is configured.

Format

sender-address ipv4 *ip-address*

undo sender-address

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies a source IPv4 address.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When PWE3 ping is performed in the multi-hop PW scenario, and the *lsp-version* is **rfc4379**, the **sender-address** command specifies a source IP address. The value is a routable address on the same public network with the address of the destination PE. Usually, the source IP address is the address of the adjacent SPE or UPE.

Precautions

After the **sender-address** command is run, the LSP version cannot be set to **draft6**.

Example

Set the source IP address of the PWE3 ping test instance in the multi-hop PW scenario to 10.1.1.1.

```
<HUAWEI> system-view
```

```
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pwe3ping
[HUAWEI-nqa-user-test] lsp-version rfc4379
[HUAWEI-nqa-user-test] sender-address ipv4 10.1.1.1
```

16.7.54 set-df

Function

The **set-df** command configures the DF (Don't Fragment) field of the test packet. This field prevents packets from being fragmented.

The **undo set-df** command restores the default setting.

By default, packet fragmentation is allowed.

Format

set-df

undo set-df

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two hosts need to communicate with each other over multiple networks, the smallest MTU value of the networks is the path MTU value. Packets can be transmitted normally over multiple networks only after the path MTU value is obtained.

If the DF bit of a packet is not configured, and the length of the packet is longer than the MTU value, the packet will be fragmented into several fragments that are shorter than the path MTU value. As a result, the path MTU cannot be detected by sending packets with increasing lengths. To detect the path MTU value, run the **set-df** command to prohibit packet fragmentation. Then, increase the length of packets sent along the path to find the path MTU value.

Prerequisites

The type of a test instance has been set to Trace using the **test-type trace** command.

Precautions

The configuration of the DF bit for packets in a running test instance cannot be changed.

Example

Set the test packet sent without being fragmented.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type trace
[HUAWEI-nqa-user-test] set-df
```

16.7.55 source-address

Function

The **source-address** command sets the source IP address for a test instance.

The **undo source-address** command restores the default setting.

By default, the IP address of the interface where packets are sent functions as the source IP address of a test instance.

Format

source-address ipv4 *ipv4-address*

source-address ipv6 *ipv6-address*

undo source-address

Parameters

Parameter	Description	Value
ipv4 *ipv4-address*	Specifies the IPv4 source address for the NQA test instance.	The value is in dotted decimal notation.
ipv6 *ipv6-address*	Specifies the IPv6 source address for the NQA test instance. **NOTE** Only ICMP, trace, and jitter tests support IPv6 source addresses.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the test packets are transmitted to the destination address, the source address of the NQA test instance is used as the destination address. The **source-address** command is used to configure the source IP address for the NQA test. If no source IP address is configured, the system specifies the IP address that sends test packets as the source IP address.

Prerequisites

The type of a test instance has been specified using the **test-type** command. However, the test type cannot be PWE3 trace, PWE3 ping, or MAC ping.

Precautions

The configuration of the source IP address of the running test instance cannot be changed.

Example

Set the source IP address to 10.1.1.1 for test instance **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] source-address ipv4 10.1.1.1
```

16.7.56 source-interface

Function

The **source-interface** command configures the source interface for an NQA test instance.

The **undo source-interface** command cancels the configuration.

By default, no source interface is configured for an NQA test instance.

Format

source-interface *interface-type interface-number*

undo source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface for an NQA test instance.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After test packets reach the destination address, the destination end sends response packets to the client end. After the **source-interface** command is used to configure the source interface for an NQA test instance, there are the following scenarios:

- If the **source-address** command is run to specify the source IP address, the test packets are sent from the specified source interface, but the response packets are received from the configured source IP address.
- If no source IP address is specified for an NQA test instance, the IP address of the source interface will be used as the source IP address of the NQA test instance. In this scenario, the initiated and responded packets are both transmitted over the outbound interface specified by the **source-interface** command.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The source interface can be configured only for ICMP, ICMP Jitter, UDP Jitter, Path MTU, and MAC Ping test instances.

Precautions

The configuration of the source interface of a running test instance cannot be changed.

The source interface of an NQA test instance must be an interface with an IP address configured; otherwise, the command cannot take effect.

The source interface cannot be a link aggregation interface or a member interface in load balancing scenario; otherwise, the command cannot take effect.

Example

Set the source interface of test instance **user test** to vlanif 100.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] source-interface vlanif 100
```

16.7.57 source-port

Function

The **source-port** command configures the source port for an NQA test instance.

The **undo source-port** command restores the default setting.

No default source port number is specified, port numbers are randomly allocated by the system.

Format

source-port *port-number*

undo source-port

Parameters

Parameter	Description	Value
port-number	Specifies the source port number for an NQA test instance.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a source port number is specified in an NQA test instance, NQA test packets can be regulated more accurately, which prevents the probe packets from being filtered by rules such ACL. The **source-port** command can be used to configure the source port for this NQA test instance:

- If no source port number is specified for an NQA test instance, a port number is selected at random to receive or send NQA test packets.
- If source port number is specified for an NQA test instance, the specified port number is used to receive and send NQA test packets.

Prerequisites

The test instance type has been specified using the **test-type** command. The source port can be configured for FTP, HTTP, SNMP, UDP Jitter, TCP, and UDP test instances.

Precautions

The port specified in the **source-port** command must be available; otherwise, the probe fails.

Ports in the range from 61441 (excluded) to 65535 are reserved and cannot be used. Otherwise, the probe fails.

You cannot change this configuration of a running test instance.

Example

Set the source port number of test instance **user test** to 3000.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type tcp
[HUAWEI-nqa-user-test] source-port 3000
```

16.7.58 start

Function

The **start** command sets the start mode and end mode for an NQA test instance.

The **undo start** command stops a running NQA test instance or restores the configuration of start mode and end mode of an unperformed NQA test instance.

By default, the test instance stops automatically after test packets are sent.

Format

start at [*yyyy/mm/dd*] *hh:mm:ss* [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }]

start delay { **seconds** *second* | *hh:mm:ss* } [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }]

start now [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }]

undo start

Parameters

Parameter	Description	Value
start at [*yyyy/mm/dd*] *hh:mm:ss*	Performs a test instance at a specified time. **NOTE** The configured time must be later than the time on the device.	-
start delay { **seconds** *second* | *hh:mm:ss* }	Specifies a delay in performing a test instance.	- **seconds** *second*: specifies a delay in performing a test instance. The value is an integer ranging from 1 to 86399, in seconds. - *hh:mm:ss*: specifies a delay in performing a test instance. If *hh:mm:ss* is specified, the system automatically sets the moment in seconds. For example, 1:0:0 indicates that a test instance starts in one hour (3600 seconds).

Parameter	Description	Value
start now	Performs a test instance immediately.	-
end at [*yyyy/mm/dd*] *hh:mm:ss*	Stops a test instance at a specified time.	-
end delay { **seconds** *second* | *hh:mm:ss* }	Specifies a delay in stopping a test instance. This delay is set based on the current system time. For example: If **start at 9:00:00 end delay seconds 60** is run at 8:59:40, then, a test instance starts at 9:00:00 and ends at 9:00:40.	● **seconds** *second*: specifies a delay in stopping a test instance. The value is an integer ranging from 6 to 86399 in seconds. ● *hh:mm:ss*: specifies a delay in stopping a test instance. For example, 1:0:0 stands for a 3600-second delay from the current system time till the time that the test instance stops. **NOTE** The delay in stopping a test instance must be set to at least 6s later than the delay in performing the test instance.
end lifetime { **seconds** *second* | *hh:mm:ss* }	Specifies the lifetime of an NQA test instance (starting from the moment that the NQA test instance starts). For example: If **start delay seconds 60 end lifetime seconds 120** is run at 9:00:00, then, a test instance lasts for 120s as it starts at 09:01:00 and ends at 09:03:00.	● **seconds** *second*: sets the life time of a test instance in seconds. The value is an integer ranging from 6 to 86399 in seconds. ● *hh:mm:ss*: sets the lifetime of a test instance. For example, 1:0:0 indicates that the lifetime of a test instance is 3600s starting from the moment a test instance starts.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring test instances and relevant attributes, you need to manually set the start and end modes for the test instances. The types of start and end modes are as follows:

- Start modes:
  - Starting a test instance at a specified time
  - Starting a test instance immediately
  - Starting a test instance after a certain delay
- End modes:
  - Ending a test instance at a specified time
  - Ending a test instance immediately
  - Ending a test instance after a certain delay
  - Ending a test instance after all test packets are sent

You can set the start and end modes as required.

Precautions

If the number of the running test instances reaches the maximum value defined by the system, the **start** command is invalid.

For the same test instance, the **start now** command can be used again only when the previous configuration is complete. Although this command has been run and configurations have been saved, this **start now** command will not be restored and needs to be run again after the device is restarted.

When starting a test instance at a specified time, the time must be later than the current time on the device.

If no end time is configured, the test cannot stop automatically. You need to stop it manually using the **stop** command.

Example

Perform the test 10 hours later.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] destination-address ipv4 10.1.1.1
[HUAWEI-nqa-user-test] destination-port 4000
[HUAWEI-nqa-user-test] start delay 10:00:00
```

16.7.59 step (NQA view)

Function

Using the **step** command, you can set the value of the incremental step for the packet length in the path MTU test.

Using the **undo step** command, you can delete the current setting.

By default, the value of the incremental step is 10.

Format

step *step*

undo step

Parameters

Parameter	Description	Value
step	Specifies the value of the incremental step.	It is an integer ranging from 1 to 512, in bytes. The default value is 10 bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **step** command is run to set the value of the incremental step for the packet length, only when the test type is configured as the path MTU test.

Example

Set the value of the incremental step for the packet length in the path MTU test to 50 bytes.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pathmtu
[HUAWEI-nqa-user-test] step 50
```

16.7.60 stop

Function

The **stop** command stops an NQA test instance.

Format

stop

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to stop only the running NQA test instances, that is, test instances in active state.

Example

Stop the test instance named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] stop
```

16.7.61 test-failtimes

Function

The **test-failtimes** command sets the number of consecutive test failures in an NQA test.

The **undo test-failtimes** command restores the default setting.

By default, a trap message is sent for each test failure.

Format

test-failtimes *times*

undo test-failtimes

Parameters

Parameter	Description	Value
times	Specifies the number of consecutive test failures in an NQA test.	The value is an integer that ranges from 1 to 15. The default value is 1.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NQA test consists of multiple probe tests. By default, if one or more probe tests are successful in an NQA test, the test is considered successful. If all probe tests fail, the test is considered failed. If the number of consecutive test failures reaches the specified value, the system will send a trap to the specified NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command. Path jitter and Path MTU test are not supported.

Follow-up Procedure

Run the **send-trap testfailure** command to send a trap to the NMS after an NQA test fails. Otherwise, the trap cannot be sent to the NMS after an NQA test fails.

Precautions

This configuration of a running test instance cannot be changed.

Example

Set the number of consecutive test failures to 10.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] test-failtimes 10
```

16.7.62 test-type

Function

The **test-type** command configures the test type for an NQA test instance.

The **undo test-type** command cancels the test type configured for an NQA test instance.

By default, no test type is configured.

Format

test-type { **dns** | **ftp** | **http** | **icmp** | **icmpjitter** | **jitter** | **lspjitter** | **lspping** | **lsptrace** | **macping** | **pathjitter** | **pwe3ping** | **pwe3trace** | **snmp** | **tcp** | **trace** | **udp** | **pathmtu** }

undo test-type

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **lspjitter**, **lspping**, **lsptrace**, **pwe3ping**, and **pwe3trace**.

Parameters

Parameter	Description	Value
dns	Specifies a DNS test.	-
ftp	Specifies an FTP service test.	-
http	Specifies an HTTP service test.	-

Parameter	Description	Value
icmp	Specifies an ICMP test.	-
icmpjitter	Specifies an ICMP jitter test, which can detect the jitter on the network.	-
jitter	Specifies a UDP jitter test, which can detect the jitter during UDP packet transmission.	-
lspjitter	Specifies an LSP jitter test.	-
lspping	Specifies an LSP ping test.	-
lsptrace	Specifies an LSP trace route test.	-
macping	Specifies a MAC ping test.	-
pathjitter	Specifies a path jitter test, which can detect the hop-by-hop jitter during the ICMP packet transmission.	-
pwe3ping	Specifies a PWE3 ping test.	-
pwe3trace	Specifies a PWE3 trace test.	-
snmp	Specifies an SNMP test.	-
tcp	Specifies a TCP test.	-
trace	Specifies a trace test.	-
udp	Specifies a UDP test.	-
pathmtu	Specifies a path MTU test to find the minimum MTU value on the network.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

- After an NQA test instance is created, a test type needs to be specified for it as other parameters are configured based on the test instance type. To configure the test type for an NQA test instance, run the **test-type** command.
- You cannot change the type of a running test instance.
- An ICMP test is usually conducted to check the connectivity. However, it cannot accurately test the link delay. Therefore, to test link delay or other link performance, you are advised to conduct an ICMP jitter or UDP jitter test.

Example

Configure the test type of an NQA test instance as TCP.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type tcp
```

16.7.63 timestamp-unit

Function

The **timestamp-unit** command sets the unit of timestamp for an NQA test instance.

The **undo timestamp-unit** command restores the default setting.

By default, the unit of timestamp for an NQA test instance is millisecond.

Format

timestamp-unit { **millisecond** | **microsecond** }

undo timestamp-unit microsecond

Parameters

Parameter	Description	Value
millisecond	Sets the unit of timestamp for an NQA test instance to millisecond.	-
microsecond	Sets the unit of timestamp for an NQA test instance to microsecond.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

This command applies to the ICMP Jitter and UDP Jitter tests.

Example

Set the unit of timestamp for an NQA test instance to microsecond.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] timestamp-unit microsecond
```

16.7.64 threshold

Function

The **threshold** command sets the RTD threshold.

The **undo threshold** command deletes the RTD threshold.

By default, no threshold is set.

Format

threshold rtd *rtd-value*

undo threshold rtd

Parameters

Parameter	Description	Value
rtd *rtd-value*	Sets the RTD threshold.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The type of a test instance has been specified using the **test-type** command. Path jitter and Path MTU test are test is not supported.

Example

Set the RTD threshold to 2 ms.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] threshold rtd 2
```

16.7.65 timeout

Function

The **timeout** command sets the timeout period for a probe of an NQA test instance.

The **undo timeout** command restores the default timeout period for a probe of an NQA test instance.

By default, the timeout period for FTP test instances is 15 seconds and that for other test instances is 3 seconds.

Format

timeout *time*

undo timeout

Parameters

Parameter	Description	Value
time	Specifies the timeout period for a probe.	The value is an integer that ranges from 1 to 60, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The timeout period refers to the waiting time after a probe is sent. If no response packet is received when the timeout period expires, the test fails. The timeout period is set based on the actual networking.

On an unstable network with a low transmission rate, you need to prolong the timeout period for sending probe packets to ensure that response packets can be received.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

- You are advised to set the timeout period based on the round-trip time (RTT) value. Ensure that the timeout period set by the **timeout** command is longer than the RTT value.
- The timeout period set by the **timeout** command must be smaller than or equal to the interval of automatic tests set by the **interval** command. Otherwise, the tests fail due to timeout of test packets.

Precautions

You cannot change this configuration of a running test instance.

In an ICMP test instance, if the following conditions are met, the Completion field in the test results will be displayed as **no result**:

- The system CPU usage exceeds 90% and the configured timeout period is less than 6s.
- **frequency** configured ≤ (**probe-count** - 1) × **interval** + 6.

Example

Set the timeout period of the test instance named **user test** to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type jitter
[HUAWEI-nqa-user-test] timeout 20
```

16.7.66 tos

Function

The **tos** command sets the ToS value for an NQA test packet.

The **undo tos** command restores the default ToS value of an NQA test packet.

By default, the ToS value is 0.

Format

tos *value*

undo tos

Parameters

Parameter	Description	Value
value	Specifies the ToS value of a packet.	The value is an integer that ranges from 0 to 255. The default value is 0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ToS field contains a precedence sub-field and a ToS sub-field. The precedence sub-field indicates the priority of a packet and the ToS sub-field is seldom used. All the bits in the ToS sub-field must be set to 0. You can set the priority of probe packets by setting the ToS value. When a large number of packets are received, packets of high priorities are processed preferentially.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The following types of test instances are supported:

- FTP
- HTTP
- ICMP
- ICMP Jitter
- UDP Jitter
- SNMP
- TCP
- UDP

Configuration Impact

If you run the **tos** command multiple times, only the latest configuration takes effect.

Precautions

The ToS value of a running test instance cannot be changed.

Example

Set the ToS value for the test instance named **user test** to 10.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] tos 10
```

16.7.67 tracert-hopfailtimes

Function

The **tracert-hopfailtimes** command sets the number of consecutive failed hops indicating a failed trace test instance.

The **undo tracert-hopfailtimes** command restores the default number of consecutive failed hops indicating a failed trace test instance.

By default, five consecutive failed hops indicate a failed trace test instance.

Format

tracert-hopfailtimes *times*

undo tracert-hopfailtimes

Parameters

Parameter	Description	Value
times	Specifies the number of consecutive failed hops indicating a failed trace test instance.	The value is an integer that ranges from 1 to 255.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **tracert-hopfailtimes** command only takes effect for trace test instances.

You cannot change this configuration of a running test instance.

Example

Set the number of consecutive failed hops indicating a failed trace test instance to 6.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type trace
[HUAWEI-nqa-user-test] tracert-hopfailtimes 6
```

16.7.68 tracert-livetime

Function

The **tracert-livetime** command sets the time to live (TTL) value for trace test instances in an NQA test.

The **undo tracert-livetime** command restores the default TTL value for trace test instances in an NQA test.

By default, the initial TTL value is 1 and the maximum TTL value is 30.

Format

tracert-livetime first-ttl *first-ttl* **max-ttl** *max-ttl*

undo tracert-livetime

Parameters

Parameter	Description	Value
first-ttl *first-ttl*	Specifies the initial TTL value of a packet.	The value is an integer that ranges from 1 to 255. The default value is 1.
max-ttl *max-ttl*	Specifies the maximum TTL value of a packet.	The value is an integer that ranges from 1 to 255. The value of *max-ttl* must be greater than the value of *first-ttl*. By default, the maximum TTL value is 30.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **tracert-livetime** command takes effect only for trace test instances.

You cannot change this configuration of a running test instance.

Example

Set the initial TTL value of the test instance named **user test** to 5 and the maximum TTL value to 20.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type trace
[HUAWEI-nqa-user-test] tracert-livetime first-ttl 5 max-ttl 20
```

16.7.69 ttl

Function

The **ttl** command sets the TTL value for the test packets of an NQA test instance.

The **undo ttl** command restores the default setting.

The default TTL value is 30.

Format

ttl *number*

undo ttl

Parameters

Parameter	Description	Value
number	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default TTL value is 30.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent test packets from being transmitted endlessly, the test instance must be performed within certain hops.

When a test packet is created, you can run the **ttl** command to set the TTL value. When the test packet is transmitted along Layer 3 routing devices, each Layer 3 routing device decrements the TTL value by one when the packet arrives. When the TTL value is 0, the Layer 3 routing device discards the test packet and sends an error message to the sending end. This prevents test packets from being transmitted endlessly.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type of test instances that are not supported is as follows:

- DNS
- Trace
- MAC Ping
- Path Jitter
- Path MTU

Configuration Impact

If you run the **ttl** command multiple times, only the latest configuration takes effect.

Precautions

The type of a running test instance cannot be changed.

Example

Set the TTL value for the test packets of a test instance named **user test** to 10.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
```

```
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] ttl 10
```

16.7.70 ttl-copymode

Function

Using the **ttl-copymode** command, you can specify the TTL propagation mode (pipe or uniform) for a multi-hop PW detection.

Using the **undo ttl-copymode** command, you can cancel the TTL propagation mode configured in the NQA view.

By default, the TTL propagation mode varies with products.

Format

ttl-copymode { **pipe** | **uniform** }

undo ttl-copymode

Parameters

Parameter	Description	Value
pipe	Sets the TTL propagation mode to pipe.	-
uniform	Sets the TTL propagation mode to uniform.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

During the detection of a multi-hop PW, if the default TTL propagation mode on different devices is different, you need to specify the TTL propagation mode on the first hop of the PW. This command is used to detect PWE3 networks and BGP/ MPLS IP VPN networks.

The TTL propagated in pipe and uniform modes is processed in different manners:

- When receiving a packet carrying the TTL propagated in pipe mode, the system strips the outer tag of the packet, decreases the TTL in the inner tag by 1, and then sets the TTL in the outer tag to 255.
- When receiving a packet carrying the TTL propagated in uniform mode, the system maps the TTL in the outer tag to the inner tag, decreases the TTL in the inner tag by 1, and then sets the TTL in the outer tag to the value of the TTL in the inner tag.

NOTE

The **ttl-copymode** command makes sense only in the Trace test instances. In the case of a trace test instance, you need to first run the **vpn-instance** *vpn-instance-name* command to bind the NQA trace test instance with a VPN instance.

Example

Configure the TTL propagation mode of packets in the NQA trace test instance as pipe.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin trace
[HUAWEI-nqa-admin-trace] test-type trace
[HUAWEI-nqa-admin-trace] vpn-instance voice
[HUAWEI-nqa-admin-trace] ttl-copymode pipe
```

16.7.71 undo no-control-word

Function

Using the **undo no-control-word** command, you can enable the control-word option.

By default, the control-word is used in packet encapsulation.

Format

undo no-control-word

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The control-word option carries control-word information in each encapsulated packet. The information is used for packet sequence verification, packet fragmentation, and packet reassembling on the forwarding plane.

By default, the control-word is used in packet encapsulation. If a non-huawei device does not support control-word information in the packet structure, the **label-type** { { **label-alert** | **normal** } **no-control-word** } command can be used on the Huawei device to remove the control-word option from each packet sent to the non-huawei device to facilitate their interworking.

If a non-huawei device supports control-word information in the packet structure, the **undo no-control-word** command can be used on the Huawei device to restore the Huawei packet structure.

NOTE

Only PWE3 Ping and PWE3 Trace test instances support the **undo no-control-word** command.

Example

Enable the control-word option.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pwe3ping
[HUAWEI-nqa-user-test] label-type label-alert no-control-word
[HUAWEI-nqa-user-test] undo no-control-word
```

16.7.72 vc-type

Function

Using the **vc-type** command, you can configure the type of the protocol used for setting up an L2VPN VC in the NQA view.

Using the **undo vc-type** command, you can delete the protocol type configured in the NQA view.

By default, the type of the protocol used for setting up an L2VPN VC is LDP.

Format

vc-type { **ldp** | **bgp** }

undo vc-type

Parameters

Parameter	Description	Value
ldp	Propagates inner labels by using LDP as the signaling protocol.	-
bgp	Propagates inner labels by using BGP as the signaling protocol.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vc-type** command is used to configure the signaling protocol for an NQA test instance to be identical with that for the PW on the network to be tested.

Prerequisites

For the **vc-type ldp** command, ensure that the test instance is of the following type:

- PWE3 Ping
- PWE3 Trace

For the **vc-type bgp** command, ensure that the test instance is of the following type:

- PWE3 Trace

Precautions

The signaling type of a running test instance cannot be changed.

Example

In the NQA view, configure BGP to be the type of the protocol used for setting up an L2VPN VC.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] vc-type bgp
```

16.7.73 vpn-instance (NQA view)

Function

The **vpn-instance** command configures the VPN instance that an NQA test instance belongs to.

The **undo vpn-instance** command deletes the configured VPN instance.

By default, no VPN instance is configured.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance that an NQA test instance belongs to.	The value must be an existing VPN instance name.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **vpn-instance** command applies to FTP, HTTP, ICMP, ICMP Jitter, Path Jitter, SNMP, TCP, trace, UDP, Path MTU, and UDP Jitter test instances.

In a PWE3 Trace test instance, if the protocol type of the L2VPN VC is set to BGP by the **vc-type** command, you can run the **vpn-instance** command to specify a VPN instance name for the PWE3 Trace test instance.

You cannot change this configuration of a running test instance.

Example

Set the VPN instance for an NQA test instance named **user test** to vrf1.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] vpn-instance vrf1
```

16.8 Service Diagnosis Configuration Commands

16.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.8.2 display trace information

Function

The **display trace information** command displays information about service diagnosis.

Format

display trace information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring service diagnosis, you can run this command to view global information about service diagnosis, such as the number of diagnosis instances and the number of diagnosis objects created on the device.

Example

Display information about service diagnosis.

```
<HUAWEI> display trace information
Trace Information:
-------------------------------------------------------------
Trace Enable                          : Enable
Debug info level                      : Brief
Debug fill-instance                   : Off
Debug quit-instance                   : Off
Debug output information              : Off
Syslog Source IP Address              : -
Terminal process enable               : On
Authentication duration threshold     : 10s
AAA duration threshold                : 5s
CM duration threshold                 : 5s

The sum of all the instances          : 0
The startID of the instance table     : -
Alloc instance times                  : 9
Free instance times                   : 9
The sum of all the objects            : 2
-------------------------------------------------------------
```

Table 16-63 Description of the **display trace information** command output

Item	Description
Trace Information	Information about service diagnosis.

Item	Description
Trace Enable	Status of service diagnosis. - Disable: Service diagnosis is disabled. - Enable: Service diagnosis is enabled. This field can be modified using the **trace enable** command.
Debug info level	Output level of service diagnosis information. - Brief: brief service diagnosis information. - Detail: detailed service diagnosis information. This field can be modified using the **trace enable** command.
Debug fill-instance	Debugging status of the **fill-instance** module. - Off: disabled - On: enabled
Debug quit-instance	Debugging status of the **quit-instance** module. - Off: disabled - On: enabled
Debug output information	Debugging status of the **output information** module. - Off: disabled - On: enabled
Syslog Source IP Address	Source IP address of the interface for exporting diagnosis information to the log server. To set this parameter, run the **trace syslog source** command.
Terminal process enable	Whether the function of logging the network access process and interaction packets of terminals is enabled. - Disable: This function is disabled. - Enable: This function is enabled. To configure this function, run the **trace object process enable** command.
Authentication duration threshold	Threshold of the processing time for the access module during terminal authentication.
AAA duration threshold	Threshold of the processing time for the AAA module during terminal authentication.
CM duration threshold	Threshold of the processing time for the CM module during terminal authentication.
The sum of all the instances	Total number of diagnosis instances.

Item	Description
The startID of the instance table	Start ID of the instance table.
Alloc instance times	Number of the allocated diagnosis instances.
Free instance times	Number of the released diagnosis instances.
The sum of all the objects	Total number of diagnosis objects.

16.8.3 display trace instance

Function

The **display trace instance** command displays diagnosis instances on a device.

Format

display trace instance [*instance-start-id* [*instance-end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **cid** *cid*] [**process-wlan**]

NOTE

The **process-wlan** keyword is only supported by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Parameters

Parameter	Description	Value
instance-start-id	Specifies the ID of the first instance whose information is displayed, that is, start ID.	The value varies according to different devices.
instance-end-id	Specifies the ID of the last instance whose information is displayed, that is, end ID.	The value varies according to different devices. **NOTE** The *instance-end-id* value must be larger than the *instance-start-id* value.
mac-address *mac-address*	Specifies a MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
cid *cid*	Specifies the diagnosis instance CID.	The value varies according to different devices.
process-wlan	Specifies the WLAN sub-core.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify no parameter, all diagnosis instances are displayed in sequence. Each time you run this command, 10 diagnosis instances are displayed. For example, all diagnosis instances have been created on the device. When you run the **display trace instance** command for the first time, information about diagnosis instances 0 to 9 is displayed. When you run this command again, information about instances 10 to 19 is displayed. This process is repeated until information about all the diagnosis instances is displayed. If you specify the value of *instance-start-id*, information about 10 diagnosis instances from this ID is displayed.

To view information about diagnosis instances within a specified range, run the **display trace instance** *instance-start-id instance-end-id* command to specify the start and end IDs of diagnosis instances.

Example

Display information about diagnosis instances on the interface with the IP address of 10.10.10.1.

```
<HUAWEI> display trace instance ip-address 10.10.10.1
Trace Instance:
------------------------------------------------------------
  ID            : 0
  MAC Address    : 00e0-fc12-3456
  IP Flag        : -
  Session ID     : -
```

```
IP Address     : 10.10.10.1
VRF Index      : -
CID            : 100
User Name      : -
Interface      : -
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : dot1x
Modules online : EAPoL  :0    WEBS   :0      WEB    :0      AAA    :0
                 CM     :0    TM     :0      SAM    :0      RADIUS :1
                 DHCPS  :0    DHCPC  :0      DHCPR  :0      DHCPP  :0
                 TACACS :0    AM     :0      SAVI   :0      WLAN_AC:0
-------------------------------------------------------------
Total 1, 1 printed
```

Table 16-64 Description of the display trace instance command output

Item	Description
ID	ID of the diagnosis instance.
MAC Address	MAC address of the interface.
IP Flag	Flag of the IP address.
Session ID	ID of the session, only valid for PPPoX users.
IP Address	IP address of the interface.
VRF Index	User VPN instance index.
CID	User connect ID.
User Name	User name.
Interface	Interface index.
QinQ VLAN ID	QinQ VLAN ID.
User VLAN ID	User VLAN ID.
Access Mode	User access mode, including dot1x, mac-authen, portal, and wlan. To set the user access mode, run the **trace object** command.
Modules online	User status on a module. User status can be: ● 0: The user is offline on the module. ● 1: The user is online on the module.

16.8.4 display trace object

Function

The **display trace object** command displays the configuration about a service diagnosis object.

Format

display trace object [*service-object-id*]

Parameters

Parameter	Description	Value
service-object-id	Specifies the ID of a diagnosis object.	The value is an integer that ranges from 0 to 3.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify *service-object-id*, configurations about all diagnosis objects are displayed.

Example

Display configurations about all diagnosis objects.

```
<HUAWEI> display trace object
Trace Object Syslog Server:
  SSL_Policy     : test
  Port           : 6514
Trace Object:
------------------------------------------------------------
  Object ID      : 0
  Slot           : -
  MAC Address    : -
  IP Flag        : -
  Session ID     : -
  IP Address     : 10.1.1.1
  VRF Index      : -
  CID            : -
  User Name      : -
  Interface      : -
  QinQ VLAN ID   : -
  User VLAN ID   : -
  Access Mode    : -
  User Tunnel ID : -
  Output         : command line ( User-Intf 4 )

  Object ID      : 1
  Slot           : -
  MAC Address    : 00e0-fc01-0101
  IP Flag        : -
  Session ID     : -
  IP Address     : -
  VRF Index      : -
  CID            : -
  User Name      : -
  Interface      : -
```

```
 QinQ VLAN ID   : -
 User VLAN ID   : -
 Access Mode    : -
 User Tunnel ID : -
 Output         : file ( flash:/a.txt )

 Object ID      : 2
 Slot           : -
 MAC Address    : 00e0-fc01-0101
 IP Flag        : -
 Session ID     : -
 IP Address     : 10.2.2.2
 VRF Index      : -
 CID            : -
 User Name      : -
 Interface      : -
 QinQ VLAN ID   : -
 User VLAN ID   : -
 Access Mode    : -
 User Tunnel ID : -
 Output         : server ( 10.10.10.10 )

------------------------------------------------------------
 Total 3, 3 printed
```

Table 16-65 Description of the **display trace object** command output

Item	Description
Object ID	ID of a diagnosis object. This parameter is automatically generated from 0 in sequence of creation time.
Slot	Slot ID of the device.
MAC Address	MAC address. To set this parameter, run the **trace object** command.
IP Flag	Flag of the IP address.
Session ID	ID of the session, only valid for PPPoX users.
IP Address	IP address of the interface. To set this parameter, run the **trace object** command.
VRF Index	User VRF index.
CID	User CID.
User Name	User name. To set this parameter, run the **trace object** command.
Interface	Interface index. To set this parameter, run the **trace object** command.
QinQ VLAN ID	QinQ VLAN ID. To set this parameter, run the **trace object** command.
User VLAN ID	User VLAN ID. To set this parameter, run the **trace object** command.

Item	Description
Access Mode	User access mode, including dot1x, mac-authen, portal, and wlan. To set this parameter, run the **trace object** command.
Output	Direction in which the device exports diagnosis information. To set this parameter, run the **trace object** command. - Command line (User-Intf X): Diagnosis information is displayed on the screen of a configuration terminal. **NOTE** When the configuration terminal is online, X displays the absolute number of the user interface (the absolute number can be checked using the **display users** command). When the configuration terminal is offline, X displays offline. - file: Diagnosis information is exported to files. - server: Diagnosis information is exported to a log server.
Trace Object Syslog Server	Diagnosis information is exported to a log server.
SSL_Policy	Name of an SSL policy. To set this parameter, run the **ssl policy** command. This field is displayed only when the device is enabled to export diagnosis information to a log server and the **trace object output syslog-server** command is run to enable the device to export diagnosis information to the log server using the TLS protocol.
Port	Port number of the log server. This field is displayed only when the device is enabled to export diagnosis information to a log server and the **trace object output syslog-server** command is run to enable the device to export diagnosis information to the log server using the TLS protocol.
Total 3, 3 printed	Total number of created diagnosis objects and number of displayed objects.

16.8.5 reset trace instance

Function

The **reset trace instance** command clears all the diagnosis instances on a device.

Format

reset trace instance

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After service diagnosis is enabled and a diagnosis object is created on a device, the device creates a diagnosis instance when a user matching the attributes of the diagnosis object gets online. If the device diagnoses services of multiple users, it creates a diagnosis instance for each user, which occupies a large amount of system resources. Therefore, the device needs to delete the diagnosis instance of a user when the user goes online successfully or fails to go online. Additionally, the device provides an aging mechanism for service diagnosis. When the aging time is reached, the device automatically deletes diagnosis instances to reclaim resources.

In addition to the preceding two methods for automatically clearing diagnosis instances, you can run the **reset trace instance** command to clear all the diagnosis instances.

NOTICE

After all the diagnosis instances are cleared using the **reset trace instance** command, properly running diagnosis instances are also deleted. Exercise caution when you run the **reset trace instance** command.

Example

Clear all diagnosis instances on the device.

```
<HUAWEI> system-view
[HUAWEI] reset trace instance
```

16.8.6 save trace information

Function

The **save trace information** command saves diagnosis information in the buffer area as a file.

Format

save trace information

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After you specify the parameter **file** *file-name* in the **trace object** command to save diagnosis information as files to the default root directory on the storage device, the system saves diagnosis information in the buffer area until the buffer is full. To prevent data loss, the system automatically saves diagnosis information in the buffer area as the file *file-name*. Before the buffer becomes full, to view real-time diagnosis information, run the **save trace information** command to save diagnosis information in the buffer area as a file.

Prerequisites

The device has been configured to export diagnosis information as a file using the **trace object** command.

Example

Save diagnosis information as a file.

```
<HUAWEI> system-view
[HUAWEI] save trace information
```

16.8.7 trace enable

Function

The **trace enable** command enables service diagnosis.

The **undo trace enable** command disables service diagnosis.

By default, service diagnosis is disabled.

Format

trace enable [**brief**]

undo trace enable

Parameters

Parameter	Description	Value
brief	Configures the device to output brief service diagnosis information.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

It is difficult to locate problems during user access based on debugging information on existing networks because multiple users may get online or offline simultaneously and debugging information about a specified user cannot be displayed. Service diagnosis provided by the switch allows maintenance personnel to customize attributes and create diagnosis objects to diagnose information about services of specified users. To enable service diagnosis, run the **trace enable** command.

Service diagnosis information can be displayed in two methods:

- The **trace enable brief** command configures the device to output brief service diagnosis information.
- The **trace enable** command configures the device to output detailed service diagnosis information.

Follow-up Procedure

After service diagnosis is enabled, run the **trace object** command to create a diagnosis object. After an ID is generated for the diagnosis object, the system starts diagnosis services.

Precautions

Service diagnosis affects system performance. Therefore, enable service diagnosis only when fault locating is required. After locating faults, immediately run the **undo trace enable** command to disable service diagnosis.

The **trace enable** command is not recorded in the configuration file. Therefore, run the **trace enable** command again after the device restarts to make service diagnosis take effect.

Example

Enable the service diagnosis function and configure the device to output brief service diagnosis information.

```
<HUAWEI> system-view
[HUAWEI] trace enable brief
```

16.8.8 trace object

Function

The **trace object** command creates a diagnosis object.

The **undo trace object** command deletes a diagnosis object.

By default, no diagnosis object is created. If you do not specify the direction at which information is exported, the default direction is the CLI.

Format

trace object { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** } } * [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

undo trace object { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** } } * [**output** { **command-line** | **file** [*file-name*] | **syslog-server** [*syslog-server-ip*] }]

undo trace object { *service-object-id* | **all** }

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support **access-mode wlan**.

Parameters

Parameter	Description	Value
mac-address *mac-address*	Creates a diagnosis object based on the MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 1 to 4 digits. If an H contains fewer than 4 digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0. The MAC address cannot be set to FFFF-FFFF-FFFF or 0000-0000-0000.
ip-address *ip-address*	Creates a diagnosis object based on the IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Creates a diagnosis object based on the interface.	-
user-vlan *user-vlan-id*	Creates a diagnosis object based on the user VLAN.	The value is an integer that ranges from 1 to 4094.
qinq-vlan *qinq-vlan-id*	Creates a diagnosis object based on the QinQ VLAN ID.	The value is an integer that ranges from 1 to 4094.
user-name *user-name*	Creates a diagnosis object based on the user name.	The value is a string of 1 to 253 case-insensitive characters without spaces.
access-mode	Creates a diagnosis object based on the access mode.	-
dot1x	Creates a diagnosis object based on the dot1x access mode.	-
mac-authen	Creates a diagnosis object based on the mac-authen access mode.	-
portal	Creates a diagnosis object based on the Portal access mode.	-
wlan	Creates a diagnosis object based on the WLAN access mode.	-
output	Specifies the direction in which the device exports diagnosis information.	-
command-line	Exports diagnosis information to the CLI.	-

Parameter	Description	Value
file *file-name*	Exports diagnosis information as a file. **NOTE** It is recommended that you export the diagnosis information to a specified file.	The value of *file-name* is a string of 1 to 63 case-insensitive characters without spaces.
syslog-server *syslog-server-ip*	Exports diagnosis information to a log server.	*syslog-server-ip* specifies the IP address of the log server, which is in dotted decimal notation.
service-object-id	Specifies the ID of a diagnosis object to be deleted. **NOTE** Diagnosis object IDs are generated based on sequence in which the diagnosis objects are created. The ID starts from 0. To view all created diagnosis objects, run the **display trace object** command.	The value is an integer that ranges from 0 to 3.
all	Deletes all diagnosis objects.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

When locating faults of DHCP, AAA, or NAC service during user access, maintenance personnel can create diagnosis objects to trace services and locate the faults.

Users with different services have different attributes. Create diagnosis objects for different services based on different attributes.

- DHCP service: based on the MAC address.
- AAA and NAC services: based on the MAC address, IP address, user name, user VLAN ID, or access mode.

NOTE

To ensure that you can diagnose the entire DHCP service process, create a diagnosis object based on the MAC address. You can run the **trace object mac-address** *mac-address* [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }] command to create a diagnosis object for the DHCP service.

Service diagnosis supports only common AAA users.

Prerequisites

Service diagnosis has been enabled using the **trace enable** command.

Precautions

If a diagnosis object is created based on the MAC address or IP address, various service processes can be diagnosed generally. If a diagnosis object is created based on other parameters, service diagnosis may fail to be performed because the parameters may not be obtained in service processes. Therefore, you are advised to create a diagnosis object based on the MAC address or IP address.

When the **slot** parameter is used for service diagnosis, if a user switches between the pre-authentication connection and authentication success states and authorization information (including ACL, VLAN, or authentication event authorization) is not changed in the switching process, no service diagnosis information will be output. In this situation, you can use the user name or interface for service diagnosis.

The diagnosis output file cannot exceed 5 MB. The excessive diagnosis information is not recorded.

You can run the **undo trace object** command to delete diagnosis objects in any of the following modes:

- Delete diagnosis objects based on the object attributes. Run the **undo trace object** { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** } } * [**output** { **command-line** | **file** [*file-name*] | **syslog-server** [*syslog-server-ip*] }] command. For example, assume that diagnosis objects 1 (10.10.10.1) and 2 (10.10.10.1+00e0-fc12-3456) have been created. To delete diagnosis objects based on the IP address, run the **undo trace object ip-address 10.10.10.1** command. Diagnosis objects 1 and 2 are deleted.
- Delete diagnosis objects based on the object ID. Run the **undo trace object** *service-object-id* command to delete a specified diagnosis object. You can view the object ID using the **display trace object** command
- Delete all diagnosis objects using the **undo trace object all** command.

Example

Create a diagnosis object on the interface with IP address 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] trace object ip-address 10.10.10.1
```

16.8.9 trace object duration threshold

Function

The **trace object duration threshold** command sets time thresholds for logging the network access process and interaction packets of terminals.

The **undo trace object duration threshold** command cancels the settings of time thresholds for logging the network access process and interaction packets of terminals.

By default, the time threshold for logging temporary entries of the access module during terminal authentication (specified by **authentication**) is 10s; the time threshold for logging user entries of the AAA module during terminal authentication (specified by **aaa**) is 5s; the time threshold for logging the authorization entries delivered by the CM module during terminal authentication (specified by **cm**) is 5s.

Format

trace object { **authentication** | **cm** | **aaa** } **duration threshold** *value*

undo trace object { **authentication** | **cm** | **aaa** } **duration threshold**

Parameters

Parameter	Description	Value
authentication	Specifies the time threshold for logging temporary entries of the access module during terminal authentication.	-
aaa	Specifies the time threshold for logging user entries of the AAA module during terminal authentication.	-
cm	Specifies the time threshold for logging the authorization entries delivered by the CM module during terminal authentication.	-
value	Specifies the time threshold.	The value is an integer in the range from 3 to 180, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate maintenance and fault locating, you can enable the function of recording the abnormal network access process and interaction packets of terminals in diagnostic log files. However, logs are generated only for the terminals with the network access time exceeding the time thresholds, regardless of whether the terminals are successfully authenticated or fail the authentication. To modify the time thresholds, run the **trace object duration threshold** command.

Prerequisites

The function of logging the abnormal network access process and interaction packets of terminals has been enabled using the **trace object process enable** command.

Precautions

The configuration of the **trace object duration threshold** command is not recorded in the configuration file. Therefore, the function will be disabled after the device is restarted.

Example

In the system view, set the time threshold for logging temporary entries of the access module during terminal authentication to 12s.

```
<HUAWEI> system-view
[HUAWEI] trace object process enable
[HUAWEI] trace object authentication duration threshold 12
```

16.8.10 trace object output syslog-server

Function

The **trace object output syslog-server** command configures the device to export diagnosis information to a log server through TLS.

The **undo trace object output syslog-server** command disables the device from exporting diagnosis information to a log server through TLS.

By default, diagnosis information is not exported to a log server through TLS.

Format

trace object output syslog-server ssl-policy *policy-name* [**port** *port num*]

undo trace object output syslog-server

Parameters

Parameter	Description	Value
ssl-policy *policy-name*	Specifies the name of an SSL policy used to export diagnosis information to a log server. **NOTE** The SSL policy must already exist on the device. If no SSL policy is available, run the **ssl policy** command to create one.	The value is the name of an SSL policy that has been created.
port *port num*	Specifies the port number of a log server.	The value is an integer in the range from 1024 to 65535. The default port number is 6514.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **trace syslog source** command is run, the device transfers diagnosis information to a log server. However, this transfer mode is insecure. In scenarios with high security requirements, you can run the **trace object output syslog-server** command to enable the device to transfer log files to the log server using the TLS protocol.

Prerequisites

A diagnosis object has been created and the device has been enabled to export diagnosis information to a log server using the **trace object** command.

Precautions

The configuration of the **trace object output syslog-server** command is not recorded in the configuration file. Therefore, the function will be disabled after the device is restarted.

If diagnosis information cannot be exported to a log server after the **trace object output syslog-server** command is run, the device automatically puts the log server to the quiet state. The quiet period is 10 minutes. The device does not send diagnosis information to the log server until the quiet period times out. If you want to cancel the quiet state in advance, run the **undo trace enable** or **undo trace object** command. To enable the device to send diagnosis information to the log server again, run the **trace enable** or **trace object** command accordingly.

Example

In the system view, enable the device to export diagnosis information to a log server through TLS.

```
<HUAWEI> system-view
[HUAWEI] ssl policy btr_syslog
[HUAWEI] trace object mac-address 00e0-fc03-0405 output syslog-server 192.168.1.1
[HUAWEI] trace object output syslog-server ssl-policy btr_syslog port 6514
```

16.8.11 trace object process enable

Function

The **trace object process enable** command enables the function of logging the abnormal network access process and interaction packets of terminals.

The **undo trace object process enable** command disables the function of logging the abnormal network access process and interaction packets of terminals.

By default, the function of logging the abnormal network access process and interaction packets of terminals is disabled.

Format

trace object process enable

undo trace object process enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

It is difficult to locate network access issues of terminals on the live network based on debugging information. To facilitate maintenance and fault locating, you can run the **trace object process enable** command to enable the function of recording the abnormal network access process and interaction packets of terminals in a diagnostic log file.

Precautions

The configuration the **trace object process enable** command is not recorded in the configuration file. Therefore, the function will be disabled after the device is restarted.

Example

In the system view, enable the function of logging the abnormal network access process and interaction packets of terminals.

```
<HUAWEI> system-view
[HUAWEI] trace object process enable
```

16.8.12 trace syslog source

Function

The **trace syslog source** command sets the source interface from which the device exports diagnosis information to a log server.

The **undo trace syslog source** command cancels the configuration of the source interface from which the device exports diagnosis information to a log server.

By default, no interface is specified to export diagnosis information to the log server.

Format

trace syslog source *interface-type interface-number*

undo trace syslog source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After you specify an interface for exporting diagnosis information to a log server, the system specifies the IP address of this interface as the source IP address of service diagnosis packets. In this way, the log server can identify the source of diagnosis information.

Prerequisites

The device has been configured to export diagnosis information to a log server using the **trace object** command.

Precautions

The **trace syslog source** command is not recorded in the configuration file. After the device restarts, the configured source interface for exporting diagnosis information is invalid. To set the source interface, run the **trace syslog source** command again.

Example

Set VLANIF100 as the source interface for exporting diagnosis information to the log server.

```
<HUAWEI> system-view
[HUAWEI] trace syslog source vlanif 100
```

16.9 Mirroring Configuration Commands

NOTE

The device supports the mirroring function, which is mainly used for network monitoring and fault management and may use user communication information. Huawei will not collect or save user communication information independently. You must use this function in compliance with applicable laws and regulations. Ensure that your customers' privacy is protected when you are using or saving communication information.

16.9.1 Command Support

Model	Port Mirroring	Traffic Mirroring	VLAN Mirroring	MAC Address Mirroring
S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S	Supported	Only local inbound traffic mirroring is supported.	Supported	Supported
S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I	Supported	Only inbound traffic mirroring is supported.	Supported	Supported

Model	Port Mirroring	Traffic Mirroring	VLAN Mirroring	MAC Address Mirroring
S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S	Supported	Supported	Supported	Supported
S6735-S, S6720-EI, S6720S-EI	Supported	Supported	Supported	Supported

16.9.2 display observe-port

Function

The **display observe-port** command displays the observing port configuration.

Format

display observe-port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After observing ports are configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view, you can run the **display observe-port** command to check detailed information about the configured observing ports.

Example

Display the observing port configuration.

```
<HUAWEI> display observe-port
  ----------------------------------------------------------------------
```

```
Index          : 1
Untag-packet   : No
Forwarding     : Yes
Packet-length  : 1000
Interface      : GigabitEthernet0/0/1
----------------------------------------------------------------------
Index          : 2
Untag-packet   : No
Forwarding     : Yes
Packet-length  : 1000
Interface-range: GigabitEthernet0/0/2
Vlan           : 20
----------------------------------------------------------------------
Index          : 3
Untag-packet   : No
Forwarding     : Yes
Packet-length  : 1000
Interface-range: GigabitEthernet0/0/3 to GigabitEthernet0/0/5
----------------------------------------------------------------------
```

Display the observing port configuration (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S).

```
<HUAWEI> display observe-port
  ----------------------------------------------------------------------
  Index          : 2
  Untag-packet   : No
  Forwarding     : Yes
  Dynamic-alloc  : No
  Interface      : GigabitEthernet0/0/2
  ----------------------------------------------------------------------
  Index          : 3
  Untag-packet   : No
  Forwarding     : Yes
  Dynamic-alloc  : No
  Interface      : GigabitEthernet1/0/3
  ----------------------------------------------------------------------
  Index          : 4
  Untag-packet   : No
  Forwarding     : Yes
  Dynamic-alloc  : Yes
  Interface      : XGigabitEthernet1/0/3
  ----------------------------------------------------------------------
```

Table 16-66 Description of the **display observe-port** command output

Item	Description
Index	Index of an observing port.
Untag-packet	Whether to remove VLAN tags of original traffic.
Forwarding	Forwarding parameter value: ● Yes: An observing port can forward data packets. ● No: An observing port does not forward data packets.
Packet-length	Length of the truncated mirrored packet. If the mirrored packet length is not specified when an observing port is configured, this field is not displayed.
Interface	A single observing port.
Interface-range	The observing ports in an observing port group.

Item	Description
Vlan	Layer 2 remote mirroring VLAN.
Dynamic-alloc	Whether the function of dynamically applying for observing port resources is enabled.

16.9.3 display port-mirroring

Function

The **display port-mirroring** command displays the mirroring configuration.

Format

display port-mirroring

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After observing ports and mirrored ports are configured on the switch, you can run the **display port-mirroring** command to check detailed mirroring configuration on the switch.

Example

Display the mirroring configuration.

```
<HUAWEI> display port-mirroring
 ----------------------------------------------------------------------
  Observe-port 1 : GigabitEthernet0/0/1
  Observe-port 2 : GigabitEthernet0/0/2
  Observe-port 3 : GigabitEthernet0/0/3
  Observe-port 4 : GigabitEthernet0/0/4
  ----------------------------------------------------------------------
  Port-mirror:
  ----------------------------------------------------------------------
       Mirror-port               Direction  Observe-port
  ----------------------------------------------------------------------
  1    GigabitEthernet0/0/15     Inbound    Observe-port 1
  ----------------------------------------------------------------------
  Stream-mirror:
  ----------------------------------------------------------------------
```

```
    Behavior                Direction  Observe-port
-------------------------------------------------------------------
1    b1                     -          Observe-port 2
-------------------------------------------------------------------
Vlan-mirror:
-------------------------------------------------------------------
Mirror-vlan             Direction     Observe-port
-------------------------------------------------------------------
10                      Inbound       Observe-port 3
-------------------------------------------------------------------
Mac-mirror:
-------------------------------------------------------------------
Mirror-mac       Vlan    Direction     Observe-port
-------------------------------------------------------------------
xxxx-xxxx-xxxx   10      Inbound       Observe-port 4
-------------------------------------------------------------------
```

Table 16-67 Description of the **display port-mirroring** command output

Item	Description
Port-mirror	Port mirroring configuration.
Mirror-port	Mirrored port. This parameter is configured using the **port-mirroring to observe-port** command.
Direction	Direction of mirrored packets: ● Inbound ● Outbound This parameter is configured using the **port-mirroring to observe-port** command.
Observe-port	Observing port to which mirrored packets are sent. This parameter is configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command.
Stream-mirror	Traffic mirroring configuration.
Behavior	Traffic behavior of traffic mirroring. ● In MQC-based traffic mirroring, this parameter is configured using the **mirroring to observe-port** command. ● In ACL-based traffic mirroring, this parameter is configured using the **traffic-mirror** or **traffic-mirror** command.
Vlan-mirror	VLAN mirroring configuration.
Mirror-vlan	VLAN ID in VLAN mirroring. This parameter is configured using the **mirroring to observe-port** command.
Mac-mirror	MAC address mirroring configuration.
Mirror-mac	MAC address in MAC address mirroring. This parameter is configured using the **mac-mirroring** command.

Item	Description
Vlan	VLAN in which MAC address mirroring is used.

16.9.4 mac-mirroring

Function

The **mac-mirroring** command copies packets with a specified MAC address to a specified observing port.

The **undo mac-mirroring** command restores the default configuration.

By default, packets with a specified MAC address are not copied to a specified observing port.

Format

mac-mirroring *mac-address* **to observe-port** *observe-port-index* **inbound**

undo mac-mirroring *mac-address* [**to observe-port** *observe-port-index*] **inbound**

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits.
observe-port-index	Specifies the index of the observing port.	The specified observing port must exist.

Views

VLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In MAC address mirroring, you can run the **mac-mirroring** command to copy packets received with a specified source or destination MAC address in a specified VLAN to a specified observing port.

Prerequisites

An observing port has been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Example

Copy packets received of which the source or destination MAC address is 00e0-fc00-0001 in VLAN 3 to the observing port with index 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] vlan 3
[HUAWEI-vlan3] mac-mirroring 00e0-fc00-0001 to observe-port 1 inbound
```

16.9.5 mirroring to observe-port (VLAN view)

Function

The **mirroring to observe-port** command copies packets received in a specified VLAN to a specified observing port.

The **undo mirroring** command restores the default configuration.

By default, packets received in a VLAN are not copied to any observing port.

Format

mirroring to observe-port *observe-port-index* **inbound**

undo mirroring [**to observe-port** *observe-port-index*] **inbound**

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of the observing port.	The specified observing port must exist.

Views

VLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In VLAN mirroring, you can run the **mirroring to observe-port** command to copy packets on all the active ports in a specified VLAN to observing ports.

Prerequisites

Observing ports have been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Precautions

For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-SX series cards, copying packets received in a specified VLAN to a specified observing port may affect the device forwarding performance (for example, some packets may be discarded during line-rate forwarding when all interfaces are fully loaded). Therefore, exercise caution when using this function.

Example

Copy packets received in VLAN 10 to the observing port with index 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] vlan 10
[HUAWEI-vlan10] mirroring to observe-port 1 inbound
```

16.9.6 mirroring to observe-port (traffic behavior view)

Function

The **mirroring to observe-port** command copies traffic that matches rules to observing ports.

The **undo mirroring** command cancels copying traffic that matches rules to observing ports.

By default, the switch does not copy traffic that matches rules to observing ports.

Format

mirroring to observe-port *observe-port-index*

undo mirroring

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of the observing port.	The specified observing port must exist.

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In traffic mirroring, you can run the **mirroring to observe-port** command to copy traffic that matches rules to specified observing ports.

Prerequisites

Observing ports have been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Precautions

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if selective QinQ, VLAN mapping, flow ID re-marking, 802.1p priority re-marking, or MAC address learning disabling is configured in a traffic behavior, traffic mirroring is not supported.

On the S6720-EI, S6735-S, and S6720S-EI, if flow ID re-marking, re-marking of the inner VLAN tag in QinQ packets, MAC address learning disabling, or redirection of packets to a VPN instance is configured in a traffic behavior, traffic mirroring is not supported.

Example

Copy traffic that matches rules to observing ports with index 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] traffic behavior tb1
[HUAWEI-behavior-tb1] mirroring to observe-port 1
```

16.9.7 observe-port (local observing port)

Function

The **observe-port** command configures local observing ports.

The **undo observe-port** command deletes local observing ports.

By default, no local observing ports are configured.

Format

Configure a single local observing port

observe-port [*observe-port-index*] **interface** *interface-type interface-number* [**untag-packet**] [**truncate packet** *packet-length*]

Configure a local observing port group

observe-port [*observe-port-index*] **interface-range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-n> [**untag-packet**] [**truncate packet** *packet-length*] (Only supported by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S; n in &<1-n> is 4 on an S6735-S, S6720-EI, and S6720S-EI and 8 on an S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.)

observe-port *observe-port-index* **interface-range** { **add** | **delete** } *interface-type interface-number* (Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

undo observe-port *observe-port-index*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **truncate packet** *packet-length*.

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The value is an integer. The value ranges from 1 to 8 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, ranges from 1 to 4 on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, and ranges from 1 to 6 on other devices.
interface-type interface-number	Specifies the type and number of an interface.	-
add	Adds observing ports to the observing port group.	-
delete	Deletes observing ports from the observing port group.	-
untag-packet	Removes VLAN tags of original traffic. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter. Each original packet can have at most two VLAN tags removed.	-

Parameter	Description	Value
truncate	Truncates packets to be mirrored.	-
packet *packet-length*	Specifies the length of packets to be mirrored.	The value is an integer in the range from 64 to 1023, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an observing port is directly connected to a monitoring host, you can run the **observe-port** command to configure a local observing port. There are two modes for configuring observing ports: configure a single observing port and configure an observing port group. Observing port group is often used in 1:N mirroring to simplify the configuration and save observing port indexes. This is because an observing port group occupies only one observing port index regardless of how many ports are configured in the group.

Precautions

- The management interface cannot be configured as an observing port.
- If you configure observing ports without specifying *observe-port-index*, the system selects the smallest unused indexes and assigns the indexes to the observing ports in sequence.
- In 1:N mirroring, if you configure packets (in the inbound or outbound direction) on a mirrored port to be copied to an observing port group, the packets cannot be copied to other observing ports.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, both Ethernet ports and Eth-Trunks can be configured as observing ports. On other devices, only Ethernet ports can be configured as observing ports.
- An observing port in blocked state can still forward mirrored traffic.
- You must dedicate observing ports for mirroring use and do not configure other services on them to prevent mirrored traffic and other service traffic from affecting each other. Do not configure any member port of an Eth-Trunk as an observing port. If you must do so, ensure that the bandwidth of service traffic on this port and the bandwidth occupied by the mirrored traffic do not exceed the bandwidth limit of the port. For the S6735-S, you are advised not

to modify the VLAN configuration on observing ports. Otherwise, VLAN information in the mirrored packets is incorrect.

Example

Configure GigabitEthernet0/0/1 as a local observing port.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
```

Configure GigabitEthernet0/0/1 through GigabitEthernet0/0/3 as a local observing port group.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface-range gigabitethernet 0/0/1 to gigabitethernet 0/0/3
```

16.9.8 observe-port (Layer 2 remote observing port)

Function

The **observe-port** command configures Layer 2 remote observing ports.

The **undo observe-port** command deletes Layer 2 remote observing ports.

By default, no Layer 2 remote observing ports are configured.

Format

Configure a single Layer 2 remote observing port:

observe-port [*observe-port-index*] **interface** *interface-type interface-number* **vlan** *vlan-id* [**truncate packet** *packet-length*]

Configure a Layer 2 remote observing port group:

observe-port [*observe-port-index*] **interface-range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-n> **vlan** *vlan-id* [**truncate packet** *packet-length*](Only supported by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S; n in &<1-n> is 4 on an S6735-S, S6720-EI, and S6720S-EI and 8 on an S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.)

observe-port *observe-port-index* **interface-range** { **add** | **delete** } *interface-type interface-number* (Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

undo observe-port *observe-port-index*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **truncate packet** *packet-length*.

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The value is an integer. The value ranges from 1 to 8 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, ranges from 1 to 4 on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, and ranges from 1 to 6 on other devices.
interface-type interface-number	Specifies the type and number of an interface.	-
add	Adds observing ports to the observing port group.	-
delete	Deletes observing ports from the observing port group.	-
vlan *vlan-id*	Specifies the Layer 2 remote mirroring VLAN.	The value is an integer in the range from 1 to 4094.
truncate	Truncates packets to be mirrored.	-
packet *packet-length*	Specifies the length of packets to be mirrorred.	The value is an integer in the range from 64 to 1023, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In Layer 2 remote mirroring, a monitoring device and the device where an observing port resides are connected through a Layer 2 network. The device where the observing port resides adds a specified VLAN tag to mirrored packets, and then the observing port broadcasts the mirrored packets in the Layer 2 remote mirroring VLAN so that the monitoring device can receive the mirrored packets. There are two modes for configuring observing ports: configure a single observing port and configure an observing port group. Observing port group is often used in 1:N mirroring to simplify the configuration and save observing port indexes. This is because an observing port group occupies only one observing port index regardless of how many ports are configured in the group.

Precautions

- The management interface cannot be configured as an observing port.
- If you configure observing ports without specifying *observe-port-index*, the system selects the smallest unused indexes and assigns the indexes to the observing ports in sequence.
- In 1:N mirroring, if you configure packets (in the inbound or outbound direction) on a mirrored port to be copied to an observing port group, the packets cannot be copied to other observing ports.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, both Ethernet ports and Eth-Trunks can be configured as observing ports. On other devices, only Ethernet ports can be configured as observing ports.
- An observing port in blocked state can still forward mirrored traffic.
- You must dedicate observing ports for mirroring use and do not configure other services on them to prevent mirrored traffic and other service traffic from affecting each other. Do not configure any member port of an Eth-Trunk as an observing port. If you must do so, ensure that the bandwidth of service traffic on this port and the bandwidth occupied by the mirrored traffic do not exceed the bandwidth limit of the port. For the S6735-S, you are advised not to modify the VLAN configuration on observing ports. Otherwise, VLAN information in the mirrored packets is incorrect.
- An Eth-Trunk on the S6735-S, S6720-EI, and S6720S-EI can meet at most three of the following conditions simultaneously:
  - The Eth-Trunk is a Layer 2 interface, or the working mode of the Eth-Trunk is changed from Layer 3 to Layer 2 using the **portswitch** or **portswitch batch** command.
  - The Eth-Trunk is configured as a Layer 2 remote observing port using the **observe-port** command.
  - The operating mode of the spanning tree protocol is set to VBST on the switch using the **stp mode** command.
  - VBST is enabled on the Eth-Trunk using the **stp enable** command.
- The **mac-address learning disable** command must be run in the VLAN view to disable the MAC address learning function in VLANs on all the intermediate devices between the monitoring device and the observing port. Otherwise, mirrored traffic will be discarded on the intermediate devices.

Example

Configure GigabitEthernet0/0/1 as a Layer 2 remote observing port.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1 vlan 10
```

Configure GigabitEthernet0/0/1 through GigabitEthernet0/0/3 as a Layer 2 remote observing port group.

```
<HUAWEI> system-view
[HUAWEI] observe-port 2 interface-range gigabitethernet 0/0/1 to gigabitethernet 0/0/3 vlan 10
```

16.9.9 observe-port dynamic-allocation enable

Function

The **observe-port dynamic-allocation enable** command enables the function of dynamically applying for observing port resources.

The **undo observe-port dynamic-allocation enable** command restores the default configuration.

By default, the function is disabled.

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S.

Format

observe-port *observe-port-index* **dynamic-allocation enable**

undo observe-port *observe-port-index* **dynamic-allocation enable**

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The value is an integer in the range from 2 to 4. The observing port with index 1 does not support the function of dynamically applying for observing port resources.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, when the same observing port is configured for outbound mirroring and inbound mirroring and multiple mirrored ports reside on the same switch, only one copy of the same packets is mirrored to the observing port. To resolve this problem, run the **observe-port dynamic-allocation enable** command to enable the observing port to dynamically apply for hardware resources.

Precautions

- In a stack, you can also configure the mirrored ports and observing port on different member switches to prevent this problem, without the need of running this command.
- You need to run this command before running the **observe-port** [*observe-port-index*] **interface** command to create an observing port.
- After the **observe-port dynamic-allocation enable** command is configured, observing port resources are occupied only when the **port-mirroring to observe-port** command is configured on mirrored ports. If both inbound mirroring and outbound mirroring are configured on a mirrored port, one observing port resource is occupied for each direction.

Example

Enable the function of dynamically applying for observing port resources.

```
<HUAWEI> system-view
[HUAWEI] observe-port 2 dynamic-allocation enable
[HUAWEI] observe-port 2 interface gigabitethernet 0/0/1
```

16.9.10 observe-port forwarding disable

Function

The **observe-port forwarding disable** command disables an observing port from forwarding data packets.

The **undo observe-port forwarding disable** command restores the default configuration.

By default, an observing port can forward data packets.

Format

observe-port *observe-port-index* **forwarding disable**

undo observe-port *observe-port-index* **forwarding disable**

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The specified observing port must exist.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You must dedicate observing ports for mirroring use and do not configure other services on them to prevent mirrored traffic and other service traffic from affecting each other. However, the observing port is still capable of forwarding data packets by default. You can run the **observe-port forwarding disable** command to disable an observing port from forwarding data packets.

Precautions

If an observing port is an Eth-Trunk interface, this function cannot be configured for this observing port.

Example

Disable the observing port with index 1 from forwarding data packets.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 forwarding disable
```

16.9.11 port-mirroring to observe-port

Function

The **port-mirroring to observe-port** command configures a mirrored port and bind it to an observing port. That is, copy packets on the mirrored port to a specified observing port.

The **undo port-mirroring** command restores the default configuration.

By default, there are no mirrored ports on the device.

Format

port-mirroring to observe-port *observe-port-index* { **both** | **inbound** | **outbound** }

undo port-mirroring [**to observe-port** *observe-port-index*] { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of observing ports.	The specified observing port must exist.
both	Copies inbound and outbound packets on a mirrored port to observing ports.	-
inbound	Copies inbound packets on a mirrored port to observing ports.	-
outbound	Copies outbound packets on a mirrored port to observing ports.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In port mirroring, you can run the **port-mirroring to observe-port** command to copy packets that pass through a mirrored port to specified observing ports.

Prerequisites

Observing ports have been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Precautions

- To prevent mirrored packets from being lost, ensure that mirrored and monitoring ports have the same port type and bandwidth.
- Both physical interfaces and Eth-Trunks can be configured as mirrored ports. If an Eth-Trunk is configured as a mirrored port, its member ports cannot be configured as observing ports.
- A mirrored port can be bound to either observing ports or observing port groups.

Example

Configure port mirroring for inbound packets on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/2
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
```

16.10 Packet Capture Configuration Commands

16.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.10.2 capture-packet

Function

The **capture-packet** command captures service packets matching specified rules.

Format

capture-packet { **interface** *interface-type interface-number* | **acl** { *ipv4-acl* | **ipv6** *ipv6-acl* } } * [**vlan** *vlan-id* | **cvlan** *cvlan-id*] * **destination** { **file** *file-name* | **terminal** } * [**car cir** *car-value* | **time-out** *time-out-value* | **packet-num** *number* | **packet-len** *length* | { **inbound** | **outbound** }] *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **cvlan** *cvlan-id* and **car cir** *car-value* parameters.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **inbound** and **outbound** parameters. If the **inbound** and **outbound** parameters are not specified, the switch captures both incoming and outgoing packets on the interface. Other switch models capture only incoming packets on the interface.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Captures packets on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Parameter	Description	Value
acl { *ipv4-acl* | **ipv6** *ipv6-acl* }	Captures packets matching a specified ACL or ACL6. **NOTE** The specified ACL or ACL6 must exist and contain ACL rules. The destination IPv6 address should not be specified in rules of the ACL6 for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S. Otherwise, packets will fail to be captured.	- *ipv4-acl*: The value is an integer in the range from 2000 to 5999 for the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 2000 to 4999 for other models. - **ipv6** *ipv6-acl*: The value is an integer in the range from 2000 to 3999.
vlan *vlan-id*	Captures packets from a specified VLAN.	The value is an integer in the range from 1 to 4094.
cvlan *cvlan-id*	Captures packets with a specified inner VLAN ID.	The value is an integer in the range from 1 to 4094.
destination	Indicates the destination to which captured packet information is sent.	-
file *file-name*	Saves captured packet information to a file. The file name extension must be **.cap**.	The value is a string of 5 to 63 characters that cannot contain the following special characters: ~ * : / \ ' " < >
terminal	Displays captured packet information on a terminal.	-
car cir *car-value*	Specifies the rate at which packets are captured.	The value is an integer in the range from 8 to 256, in kbit/s. The default value is 64 kbit/s.

Parameter	Description	Value
time-out *time-out-value*	Specifies the timeout period for packet capture. The system stops capturing packets after the specified timeout period elapses.	- When only **file** *file-name* is specified: The value is an integer in the range from 1 to 86400, in seconds. The default timeout period is 60s. - When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 300, in seconds. The default timeout period is 60s.
packet-num *number*	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	- When only **file** *file-name* is specified: The value is an integer in the range from 1 to 10000. The default value is 100. - When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 1000. The default value is 100.
packet-len *length*	Specifies the length of captured packets.	The value is an integer in the range from 20 to 64, in bytes. The default value is 64 bytes.
inbound	Captures incoming packets on the interface.	-
outbound	Captures outgoing packets on the interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an error occurs in service traffic forwarding (for example, the traffic status does not match the traffic model), you can configure the switch to capture service packets for analysis so that the switch can quickly identify invalid packets.

Precautions

- Currently, packets on the management interface, logical stack ports, and stack member ports cannot be captured.
- If the IP addresses of ARP packets on the control plane match the IP addresses in a basic or advanced ACL, these ARP packets can also be captured.
- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- Different packet capture instances cannot be executed simultaneously. That is, a new packet capture instance can be executed only when the previous one is complete.
- The system limits the rate of captured packets. The default rate limit is 64 kbit/s. If the rate of packets exceeds the limit, some packets may be discarded.
- The device cannot capture the packets of fast ICMP reply, BFD, 802.1ag, and VBST.
- When an S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S discards the packets that it cannot forward, packets may not be captured in some situations. It is recommended that you obtain packets in other ways, such as mirroring.
- For the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, the VLAN ID in the packets captured using this command is not the original VLAN ID but the VLAN ID replaced during Layer 3 forwarding. However, the packets can be forwarded normally without affecting services.
- In an SVF system, an Eth-Trunk bound to a fabric port does not support service packet capture.

Example

Capture packets on the interface GigabitEthernet0/0/1, saves them to the capture.cap file, and display them on the terminal (on a switch that supports capture of outgoing packets on an interface).

```
<HUAWEI> system-view
[HUAWEI] capture-packet interface gigabitethernet 0/0/1 destination file capture.cap terminal
[HUAWEI]
  Packet(inbound): 1
```

```
-------------------------------------------------------
ff ff ff ff ff ff 00 00 c1 02 01 02 81 00 00 58
08 00 45 00 00 52 00 00 00 00 40 72 c8 33 58 01
01 02 58 01 01 03 00 01 02 03 04 05 06 07 08 09
0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19
-------------------------------------------------------

Packet(outbound): 1
-------------------------------------------------------
ff ff ff ff ff ff 00 00 c1 02 01 02 08 00 45 00
00 52 00 00 00 00 40 72 c8 33 58 01 01 02 58 01
01 03 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
-------------------------------------------------------

-----------------packet getting report-----------------
file:  flash:/capture.cap
packets getting: interface GigabitEthernet0/0/1
acl: -
vlan: -  cvlan: -
car: 64kbps timeout: 60s
packets: 100 (expected)
        1 (inbound actual) 1 (outbound actual)
length without tunnel header: 64 (expected)
-------------------------------------------------------
```

Capture packets on the interface GigabitEthernet0/0/1, saves them to the capture.cap file, and display them on the terminal (on a switch that does not support capture of outgoing packets on an interface).

```
<HUAWEI> system-view
[HUAWEI] capture-packet interface gigabitethernet 0/0/1 destination file capture.cap terminal
[HUAWEI]
  Packet: 1
  -------------------------------------------------------
  01 80 c2 00 00 00 00 e0 09 87 78 90 81 00 00 01
  00 69 42 42 03 00 00 03 02 7c 80 00 00 e0 09 87
  78 90 00 00 00 00 80 00 00 e0 09 87 78 90 80 23
  00 00 14 00 02 00 0f 00 00 00 40 00 72 67 31 00
  -------------------------------------------------------
  Packet: 2

  -------------------------------------------------------
  01 80 c2 00 00 00 00 e0 09 87 78 90 81 00 00 01
  00 69 42 42 03 00 00 03 02 7c 80 00 00 e0 09 87
  78 90 00 00 00 00 80 00 00 e0 09 87 78 90 80 23
  00 00 14 00 02 00 0f 00 00 00 40 00 72 67 31 00
  -------------------------------------------------------

  -----------------packet getting report-----------------
  file:  flash:/capture.cap
  packets getting: interface GigabitEthernet0/0/1
  acl: -
  vlan: -  cvlan: -
  car: 64kbps timeout: 60s
  packets: 100 (expected) 2 (actual)
  length without tunnel header: 64 (expected)
  -------------------------------------------------------
```

Table 16-68 Description of the **capture-packet** command output

Item	Description
Packet(inbound): *i*	*i*th captured (incoming/outgoing) packet. ● inbound: incoming packet ● outbound: outgoing packet

Item	Description
file	Local path that stores captured packets. If **NULL** is displayed, captured packets are displayed to the terminal.
packets getting	- Specific interface name: Packets on this interface are captured. - global: Packets matched a specified ACL or ACL6 are captured.
acl	ACL number matched by captured packets.
acl ipv6	ACL6 number matched by captured packets.
vlan	VLAN ID of captured packets.
cvlan	Inner VLAN ID of captured packets.
car	Rate of captured packets.
timeout	Timeout period of packet capture. The system stops capturing packets after the specified timeout period elapses.
packets	- expected: number of packets expected to be captured - actual: actual number of captured packets - inbound actual: actual number of captured incoming packets - outbound actual: actual number of captured outgoing packets
length without tunnel header	Length of captured packets, excluding the length of tunnel headers.

16.10.3 capture-packet cpu

Function

The **capture-packet cpu** command captures packets sent to the CPU.

Format

capture-packet cpu [**vlan** *vlan-id* | **acl** { *ipv4-acl* | **ipv6** *ipv6-acl* }] * **destination** { **file** *file-name* | **terminal** } * [**time-out** *time-out-value* | **packet-num** *number* | **packet-len** *length*] *

Parameters

Parameter	Description	Value
vlan *vlan-id*	Captures packets from a specified VLAN.	The value is an integer that ranges from 1 to 4094.
acl { *ipv4-acl* | **ipv6** *ipv6-acl* }	Captures packets matching a specified ACL or ACL6. **NOTE** The specified ACL or ACL6 must exist and contain ACL rules. The destination IPv6 address should not be specified in rules of the ACL6 for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S. Otherwise, packets will fail to be captured.	● *ipv4-acl*: The value is an integer in the range from 2000 to 5999 for the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 2000 to 4999 for other models. ● **ipv6** *ipv6-acl*: The value is an integer in the range from 2000 to 3999.
destination	Indicates the destination to which captured packet information is sent.	-
file *file-name*	Saves captured packet information to a file. The file name extension must be **.cap**.	The value is a string of 5 to 63 characters that cannot contain the following special characters: ~ * : / \ ' " < >
terminal	Displays captured packet information on a terminal.	-

Parameter	Description	Value
time-out *time-out-value*	Specifies the timeout period for packet capture. The system stops capturing packets after the specified timeout period elapses.	● When only **file** *file-name* is specified: The value is an integer in the range from 1 to 86400, in seconds. The default timeout period is 60s. ● When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 300, in seconds. The default timeout period is 60s.
packet-num *number*	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	● When only **file** *file-name* is specified: The value is an integer in the range from 1 to 10000. The default value is 100. ● When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 1000. The default value is 100.
packet-len *length*	Specifies the length of captured packets.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 64 bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a CPU fault occurs (for example, the CPU usage is high), configure the packet capture function to capture packets sent to the CPU for analysis. This allows the switch to process invalid packets promptly, ensuring that the CPU works properly.

Precautions

- If the IP addresses of ARP packets on the control plane match the IP addresses in a basic or advanced ACL, these ARP packets can also be captured.
- Running this command will increase the CPU usage. Therefore, you are not advised to run this command if the CPU usage is higher than the specified value in a Warning message.
- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- Different packet capture instances cannot be executed simultaneously. That is, a new packet capture instance can be executed only when the previous one is complete.
- The system limits the rate of captured packets. The default rate limit is 64 kbit/s. If the rate of packets exceeds the limit, some packets may be discarded.

Example

Capture the packets to be sent to the CPU, save them to the **abc.cap** file, and display them on the terminal.

```
<HUAWEI> system-view
[HUAWEI] capture-packet cpu destination file flash:/abc.cap
[HUAWEI]
  Packet: 1
  -------------------------------------------------------
  01 80 c2 00 00 0e 00 e0 09 87 78 90 81 00 00 01
  88 cc 02 07 04 00 e0 09 87 78 90 04 16 05 47 69
  67 61 62 69 74 45 74 68 65 72 6e 65 74 34 2f 30
  2f 32 36 06 02 00 78 08 15 47 69 67 61 62 69 74
  -------------------------------------------------------

  Packet: 2
  -------------------------------------------------------
  01 80 c2 00 00 0e 00 e0 09 87 78 90 81 00 00 01
  88 cc 02 07 04 00 e0 09 87 78 90 04 16 05 47 69
  67 61 62 69 74 45 74 68 65 72 6e 65 74 34 2f 30
  2f 32 36 06 02 00 78 08 15 47 69 67 61 62 69 74
  -------------------------------------------------------

  ------------------packet getting report-----------------------
  file: flash:/abc.cap
  packets getting: cpu
  acl: -
  vlan: -  cvlan: -
  car: -- timeout: 60s
  packets: 100 (expected) 2 (actual)
  length without tunnel header: 64 (expected)
  -------------------------------------------------------
```

Table 16-69 Description of the **capture-packet cpu** command output

Item	Description
Packet: *i*	*i*th captured packet.

Item	Description
file	Local path that stores captured packets. If **NULL** is displayed, captured packets are displayed on a terminal, instead of being saved to a specified file.
packets getting	The system captures the packets to be sent to the CPU.
acl	ACL number matched by captured packets.
acl ipv6	ACL6 number matched by captured packets.
vlan	VLAN ID of captured packets.
cvlan	Inner VLAN ID of captured packets.
car	Rate of captured packets.
timeout	Timeout period of packet capture. The system stops capturing packets after the specified timeout period elapses.
packets	● expected: number of packets expected to be captured ● actual: actual number of captured packets
length without tunnel header	Length of captured packets, excluding the length of tunnel headers.

16.10.4 capture-packet stop

Function

The **capture-packet stop** command stops capturing service packets.

Format

capture-packet stop

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you need to update service packet capture parameters or no longer need to capture service packets after running the **capture-packet** command, you can run the **capture-packet stop** command to stop capturing service packets.

Example

Stop capturing service packets.

```
<HUAWEI> system-view
[HUAWEI] capture-packet stop
```

16.11 NetStream Configuration Commands

NOTE

NetStream collects statistics and analyzes service traffic. During service provisioning, personal data may be involved. You have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

16.11.1 Command Support

Only the following switch models support NetStream:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

16.11.2 collect counter

Function

The **collect counter** command allows the flexible flow statistics exported to the NetStream Collector (NSC) to contain the number of bytes and packets.

The **undo collect counter** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the number of bytes or packets.

Format

collect counter { **bytes** | **packets** }

undo collect counter { **bytes** | **packets** }

Parameters

Parameter	Description	Value
bytes	Indicates that the flexible flow statistics exported to NSC contain the number of bytes.	-

Parameter	Description	Value
packets	Indicates that the flexible flow statistics exported to NSC contain the number of packets.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether flexible flow statistics contain the number of bytes and packets.

Precaution

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

The command can be run multiple times, and all the configurations take effect.

Example

Configure the flexible flow statistics template **record1** to export the flexible flow statistics containing the number of packets to the NSC.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect counter packets
```

16.11.3 collect interface

Function

The **collect interface** command allows the flexible flow statistics exported to the NSC to contain the indexes of inbound and outbound interfaces.

The **undo collect interface** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the index of inbound or outbound interface.

Format

collect interface { **input** | **output** }

undo collect interface { **input** | **output** }

Parameters

Parameter	Description	Value
input	Indicates that the flexible flow statistics exported to the NSC contain the index of inbound interface.	-
output	Indicates that the flexible flow statistics exported to the NSC contain the index of outbound interface.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether flexible flow statistics exported to the NSC contain indexes of inbound and outbound interfaces.

Precaution

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

The command can be run multiple times, and all the configurations take effect.

Example

Configure the flexible flow statistics template **record1** to export the flexible flow statistics containing the inbound interface index to the NSC.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect interface input
```

16.11.4 collect ip bgp-next-hop

Function

The **collect ip bgp-next-hop** command configures the flexible flow statistics exported to the NSC to contain the BGP next hop information of a flow.

The **undo collect ip bgp-next-hop** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the BGP next hop information of a flow.

Format

collect ip bgp-next-hop

undo collect ip bgp-next-hop

Parameters

None

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether the flexible flow statistics exported to the NSC contain the BGP next hop information of a flow.

To enable the flexible flow statistics sent to the NSC to contain the BGP next hop information, you also need to run the **collect ip bgp-next-hop** and **ip netstream export version 9 bgp-nexthop** commands.

Precautions

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Configure the flexible flow statistics exported to the NSC to contain the BGP next hop information of a flow.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect ip bgp-next-hop
```

16.11.5 collect ip next-hop

Function

The **collect ip next-hop** command configures the flexible flow statistics exported to the NSC to contain the next hop information of a flow.

The **undo collect ip next-hop** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the next hop information of a flow.

Format

collect ip next-hop

undo collect ip next-hop

Parameters

None

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether the flexible flow statistics exported to the NSC contain the next hop information of a flow.

Precautions

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Configure the flexible flow statistics exported to the NSC to contain the next hop information of a flow.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect ip next-hop
```

16.11.6 collect ip tcp-flag

Function

The **collect ip tcp-flag** command configures the flexible flow statistics exported to the NSC to contain the TCP flags of a flow.

The **undo collect ip tcp-flag** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the TCP flags of a flow.

Format

collect ip tcp-flag

undo collect ip tcp-flag

Parameters

None

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether the flexible flow statistics exported to the NSC contain the TCP flags of a flow.

Precautions

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Configure the flexible flow statistics exported to the NSC to contain the TCP flags of a flow.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect ip tcp-flag
```

16.11.7 display ip netstream record

Function

The **display ip netstream record** command displays the configuration of a flexible flow statistics template.

Format

display ip netstream record { **all** | **name** *record-name* } [**vxlan inner-ip**]

Parameters

Parameter	Description	Value
all	Displays configurations of all flexible flow statistics templates.	-
name *record-name*	Displays the configuration of a flexible flow statistics template specified by *record-name*.	The flexible flow statistics template must be existed.
vxlan inner-ip	Displays configurations of VXLAN flexible flow statistics templates.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After you create and configure a flexible flow statistics template using the **ip netstream record** command, you can run the **display ip netstream record** command to view the configuration of the template.

Example

Display the configuration of the flexible flow statistics template **test0**.

```
<HUAWEI> display ip netstream record name test0
ip netstream record test0
 match ip source-address
 match ip destination-address
 match vlan input
```

Table 16-70 Description of the **display ip netstream record** command output

Item	Description
ip netstream record *record-name*	The flexible flow statistics template is *record-name*. You can run the **ip netstream record** command to configure this parameter.
match *x*	This template aggregates packets based on *x*. For the meaning and configuration of *x*, see the **match** command in the flexible flow statistics template view.

16.11.8 display ip netstream statistics

Function

The **display ip netstream statistics** command displays the NetStream flow statistics.

Format

display ip netstream statistics slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the actual configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After NetStream is configured, you can run the **display ip netstream statistics** command to view NetStream statistics.

Precautions

After each statistics item in the command output reaches the maximum value, it is reset to 0. To ensure accurate statistics about NetStream flows, you are advised to run the **reset ip netstream statistics** command to clear statistics about current NetStream flows before running the **display ip netstream statistics** command.

Example

Display the NetStream flow statistics on the device.

```
<HUAWEI> display ip netstream statistics slot 0
 =====Netstream statistics:=====
 Origin/Flexible ingress entries  : 572
 Origin/Flexible ingress packets  : 56122
 Origin/Flexible ingress octets   : 6762976
 Origin/Flexible egress entries   : 57
 Origin/Flexible egress packets   : 3588
 Origin/Flexible egress octets    : 394680
 Origin/Flexible total entries    : 629
 Handle origin entries            : 620
 Handle As aggre entries          : 12
 Handle ProtPort aggre entries    : 11
 Handle SrcPrefix aggre entries   : 10
 Handle DstPrefix aggre entries   : 15
 Handle Prefix aggre entries      : 7
 Handle AsTos aggre entries       : 6
 Handle ProtPortTos aggre entries : 5
 Handle SrcPreTos aggre entries   : 5
 Handle DstPreTos aggre entries   : 4
 Handle PreTos aggre entries      : 1
 Record test handle entries : 0
 VXLAN-Record test handle entries : 0
```

Table 16-71 Description of the **display ip netstream statistics** command output

Item	Description
Netstream statistics	NetStream statistics.
Origin/Flexible ingress entries	Total number of incoming original flows or flexible flows.
Origin/Flexible ingress packets	Total number of packets in incoming original flows or flexible flows.
Origin/Flexible ingress octets	Total number of bytes in incoming original flows or flexible flows.
Origin/Flexible egress entries	Total number of outgoing original flows or flexible flows.
Origin/Flexible egress packets	Total number of packets in outgoing original flows or flexible flows.
Origin/Flexible egress octets	Total number of bytes in outgoing original flows or flexible flows.
Origin/Flexible total entries	Total number of original flows or flexible flows of the real-time statistics.
Handle origin entries	Number of processed incoming and outgoing original flows.
Handle As aggre entries	Number of processed incoming and outgoing AS aggregation flows.
Handle ProtPort aggre entries	Number of processed incoming and outgoing protocol-port aggregation flows.

Item	Description
Handle SrcPrefix aggre entries	Number of processed incoming and outgoing source-prefix aggregation flows.
Handle DstPrefix aggre entries	Number of processed incoming and outgoing destination-prefix aggregation flows.
Handle Prefix aggre entries	Number of processed incoming and outgoing prefix aggregation flows.
Handle AsTos aggre entries	Number of processed incoming and outgoing AS-ToS aggregation flows.
Handle ProtPortTos aggre entries	Number of processed incoming and outgoing protocol-port-ToS aggregation flows.
Handle SrcPreTos aggre entries	Number of processed incoming and outgoing source-prefix-ToS aggregation flows.
Handle DstPreTos aggre entries	Number of processed incoming and outgoing destination-prefix-ToS aggregation flows.
Handle PreTos aggre entries	Number of processed incoming and outgoing prefix-ToS aggregation flows.
Record test handle entries	Number of flows processed using the flexible flow statistics template **test**.
VXLAN-Record test handle entries	Number of flows processed using the VXLAN flexible flow statistics template **test**.

16.11.9 display netstream

Function

The **display netstream** command displays the NetStream configurations.

Format

display netstream { **all** | **global** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays all the NetStream configurations, including: ● NetStream configurations in the system view ● NetStream configurations in the aggregation view ● NetStream configurations in the flexible flow statistics template view ● NetStream configurations in the interface view	-
global	Displays the global NetStream configurations, including: ● NetStream configurations in the system view ● NetStream configurations in the aggregation view ● NetStream configurations in the flexible flow statistics template view	-
interface *interface-type interface-number*	Displays the NetStream configurations on a specified interface. The parameter *interface-type interface-number* specifies the interface type and number.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the NetStream configurations for both IPv4 and IPv6 flows.

Example

Display all the NetStream configurations.

```
<HUAWEI> display netstream all
system
ip netstream export version 9
ip netstream export source 10.1.1.1
ip netstream export host 10.0.0.2 6000 vpn-instance test
ip netstream export host 10.5.5.5 6000
ipv6 netstream export version 9
ipv6 netstream export host 10.0.0.3 6000 vpn-instance test12
ip netstream record test
ip netstream record test1 vxlan inner-ip
ip netstream aggregation destination-prefix
 enable
 export version 9
ip netstream aggregation protocol-port
 export version 9

slot 0
GigabitEthernet0/0/1
 ip netstream inbound
```

Table 16-72 Description of the **display netstream all** command output

Item	Description
system	Global NetStream configurations.
ip netstream export version *version*	The field *version* indicates the version of the exported packets carrying IPv4 original flow statistics. This field is displayed only when the **ip netstream export version** command has been executed. If the version retains the default setting, this field is not displayed.
ip netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The *ip-address* field indicates the destination address of the exported packets carrying IPv4 flow statistics. The *port-number* field is the UDP port. The *vpn-instance-name* field is the name of the VPN instance to which the specified destination address belongs. This field is displayed only when the **ip netstream export host** command has been executed in the system view.
ip netstream export source *ip-address*	The field *ip-address* indicates the source address of the exported packets carrying IPv4 flow statistics. This field is displayed only when the **ip netstream export source** command has been executed. If the source address is not specified, the outbound interface IP address is used.

Item	Description
ipv6 netstream export version *version*	The field *version* indicates the version of the exported packets carrying IPv6 original flow statistics. This field is displayed only when the **ipv6 netstream export version** command has been executed. If the version retains the default setting, this field is not displayed.
ipv6 netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The *ip-address* field indicates the destination address of the exported packets carrying IPv6 flow statistics. The *port-number* field is the UDP port. The *vpn-instance-name* field is the name of the VPN instance to which the specified destination address belongs. This field is displayed only when the **ipv6 netstream export host** command has been executed in the system view.
ip netstream record *record-name*	The flexible flow statistics template is *record-name*. This field is displayed only when the **ip netstream record** command has been executed in the system view. If the flexible flow statistics template is not specified, this field is not displayed.
ip netstream record *record-name* vxlan inner-ip	The VXLAN flexible flow statistics template is *record-name*. This field is displayed only when the **ip netstream record** command has been executed in the system view.

Item	Description
ip netstream aggregation destination-prefix	Destination-prefix aggregation method. This field is displayed only when the **ip netstream aggregation** command has been executed to set the aggregation method. Currently, the following aggregation methods are supported: ● **as**: AS aggregation ● **as-tos**: AS-ToS aggregation ● **destination-prefix**: destination-prefix aggregation ● **destination-prefix-tos**: destination-prefix-ToS aggregation ● **prefix**: prefix aggregation ● **prefix-tos**: prefix-ToS aggregation ● **protocol-port**: protocol-port aggregation ● **protocol-port-tos**: protocol-port-ToS aggregation ● **source-prefix**: source-prefix aggregation ● **source-prefix-tos**: source-prefix-ToS aggregation
enable	The destination-prefix aggregation method is enabled. This field is displayed only when the **enable** command has been executed in the aggregation view.
export version *version*	The field *version* indicates the version format of the exported packets carrying aggregation flow statistics. If the version retains the default setting, this field is not displayed. This field is displayed only when the **export version** command has been executed.
slot *x*	NetStream configurations on the card in slot *x*.
GigabitEthernet0/0/1 ip netstream inbound	The flow statistics function is enabled for incoming packets on GigabitEthernet0/0/1. This field is displayed only when the **ip netstream** command has been executed in the interface view.

16.11.10 display netstream cache ip aggregation

Function

The **display netstream cache ip aggregation** command displays details about IPv4 aggregation flow statistics on a device.

Format

display netstream cache ip aggregation { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** } **slot** *slot-id*

Parameters

Parameter	Description	Value
as	Specifies the AS aggregation. It classifies flows based on source AS number, destination AS number, inbound interface index, and outbound interface index.	-
as-tos	Specifies the AS-ToS aggregation. It classifies flows based on source AS number, destination AS number, inbound interface index, outbound interface index, and ToS.	-
destination-prefix	Specifies the destination-prefix aggregation. It classifies flows based on destination AS number, destination mask length, destination prefix, and outbound interface index.	-
destination-prefix-tos	Specifies the destination-prefix-ToS aggregation. It classifies flows based on destination AS number, destination mask length, destination prefix, outbound interface index, and ToS.	-
prefix	Specifies the prefix aggregation. It classifies flows based on source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix, inbound interface index, and outbound interface index.	-
prefix-tos	Specifies the prefix-ToS aggregation. It classifies flows based on source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix, inbound interface index, outbound interface index, and ToS.	-
protocol-port	Specifies the protocol-port aggregation. It classifies flows based on protocol number, source port, and destination port.	-
protocol-port-tos	Specifies the protocol-port-ToS aggregation. It classifies flows based on protocol number, source port, destination port, ToS, inbound interface index, and outbound interface index.	-

Parameter	Description	Value
source-prefix	Specifies the source-prefix aggregation. It classifies flows based on source AS number, source mask length, source prefix, and inbound interface index.	-
source-prefix-tos	Specifies the source-prefix-ToS aggregation. It classifies flows based on source AS number, source mask length, source prefix, ToS, and inbound interface index.	-
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv4 aggregation flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display detailed statistics about flows aggregated based on protocol and port on the device.

```
<HUAWEI> display netstream cache ip aggregation protocol-port slot 0
NetStream cache information:
--------------------------------------------------------------------------------
 Protocol   SrcPort   DstPort   Direction  Streams     Packets     Octets
--------------------------------------------------------------------------------
 114        0         0         IN         200         50688       5271552
--------------------------------------------------------------------------------
............
```

Table 16-73 Description of the **display netstream cache ip aggregation** command output

Item	Description
NetStream cache information	NetStream flow information.
Protocol	Protocol number of packets.
SrcPort	Source port number of packets.
DstPort	Destination port number of packets.
Direction	Packet sampling direction: ● IN: inbound direction ● OUT: outbound direction
Streams	Number of flows.
Packets	Number of packets.
Octets	Number of octets in packets.

16.11.11 display netstream cache ip record

Function

The **display netstream cache ip record** command displays details about IPv4 flexible flow statistics on a device.

Format

display netstream cache ip record *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **source mac-address** *mac-address* | **protocol** *protocol-type* | **tos** *tos-number* | **ttl** *ttl-number* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**]

NOTE

If the **destination mac-address** *mac-address*, **source mac-address** *mac-address*, **ttl** *ttl-number*, or **vlan** *vlan-id* parameter is specified, the **verbose** parameter must be specified too.

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	It must be an existing template name on the device.

Parameter	Description	Value
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ip *ip-address*	Specifies the destination IP address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
destination mac-address *mac-address*	Specifies the destination MAC address of packets.	-
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ip *ip-address*	Indicates the source IP address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
source mac-address *mac-address*	Specifies the source MAC address of packets.	-
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.
ttl *ttl-number*	Specifies the TTL value of packets.	The value is an integer that ranges from 1 to 255.
vlan *vlan-id*	Specifies the VLAN ID of packets.	The value is an integer that ranges from 1 to 4094.
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv4 flexible flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display IPv4 flexible flow statistics on the device.

```
<HUAWEI> display netstream cache ip record record1 slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
--------------------------------------------------------------------------------
 SrcIP                DstIP              L4 Info            DstAS     Direction
 SrcIf                DstIf              TCP Flags          SrcAS     ToS
 NextHop              BGPNextHop         Octets             Packets   TTL
 SMAC                 DMAC               VLAN
--------------------------------------------------------------------------------
 255.255.255.255      255.255.255.255    0:0:0              100       OUT
 GE0/0/10             GE0/0/11           0:0:0:0:0:0        --        0
 10.1.1.1             10.1.1.1           528                4         20
 00:e0:fc:12:23:56    00:e0:fc:12:23:33  60
--------------------------------------------------------------------------------
```

Table 16-74 Description of the **display netstream cache ip record** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets, including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets, including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.

Item	Description
SrcIP	Source IP address of packets.
DstIP	Destination IP address of packets.
DstAS	Destination AS number of packets.
Direction	Packet sampling direction: ● IN: inbound direction. ● OUT: outbound direction.
SrcIf	Source interface of packets.
DstIf	Destination interface of packets.
SrcAS	Source AS number of packets.
ToS	ToS field of packets.
NextHop	Next hop address.
BGPNextHop	Address of the BGP next hop.
Octets	Number of octets in packets.
Packets	Number of packets.
TTL	TTL value of packets.
SMAC	Source MAC address of packets.
DMAC	Destination MAC address of packets.
VLAN	VLAN ID of packets.

16.11.12 display netstream cache vxlan record

Function

The **display netstream cache vxlan record** command displays detailed VXLAN flexible flow statistics.

Format

display netstream cache vxlan inner-ip [ipv6] record *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **source mac-address** *mac-address* | **protocol** *protocol-type* | **tos** *tos-number* | **ttl** *ttl-number* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**]

NOTE

When **destination mac-address** *mac-address*, **source mac-address** *mac-address*, **ttl** *ttl-number*, or **vlan** *vlan-id* is specified, the **verbose** parameter must also be specified.

Parameters

Parameter	Description	Value
ipv6	Displays detailed IPv6 information about VXLAN flexible flows. If this parameter is not specified, detailed IPv4 information about VXLAN flexible flows is displayed by default.	-
record-name	Specifies the name of a flexible flow statistics template.	It must be an existing template name on the switch.
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ip *ip-address*	Specifies the destination IP address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer in the range 0 to 65535.
destination mac-address *mac-address*	Specifies the destination MAC address of packets.	-
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ip *ip-address*	Specifies the source IP address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer in the range 0 to 65535.
source mac-address *mac-address*	Specifies the source MAC address of packets.	-
protocol *protocol-type*	Specifies the packet protocol type.	The value is an integer in the range from 0 to 255.

Parameter	Description	Value
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer in the range from 0 to 255.
ttl *ttl-number*	Specifies the TTL value of packets.	The value is an integer in the range from 1 to 255.
vlan *vlan-id*	Indicates the VLAN ID of packets.	The value is an integer in the range from 1 to 4094.
slot *slot-id*	Specifies a slot ID.	The value depends on the actual configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays detailed real-time VXLAN flexible flow statistics.

Precautions

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display detailed IPv4 information about VXLAN flexible flows on the switch.

```
<HUAWEI> display netstream cache vxlan inner-ip record record1 slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
        TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
--------------------------------------------------------------------------------
 SrcIP             DstIP             L4 Info          DstAS      Direction
 SrcIf            DstIf            TCP Flags          SrcAS      ToS
 NextHop              BGPNextHop           Octets           Packets   TTL
 SMAC                DMAC               VLAN              VNI
--------------------------------------------------------------------------------
 255.255.255.255      255.255.255.255    0:0:0             100       OUT
 GE0/0/10            GE0/0/11           0:0:0:0:0:0       --        0
 10.1.1.1           10.1.1.1           528               4         20
 00:e0:fc:12:23:56    00:e0:fc:12:23:33  60
--------------------------------------------------------------------------------
```

Table 16-75 Description of the **display netstream cache vxlan record** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets, including the source port number, destination port number, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of a packet, including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIP	Source IP address of packets.
DstIP	Destination IP address of packets.
DstAS	Destination AS number of packets.
Direction	Packet sampling direction: ● IN: inbound direction ● OUT: outbound direction
SrcIf	Source interface of packets.
DstIf	Destination interface of packets.
SrcAS	Source AS number of packets.
ToS	ToS value of packets.
NextHop	Next-hop IP address in a route.
BGPNextHop	IP address of the BGP next hop.
Octets	Number of octets in packets.
Packets	Number of packets.
TTL	TTL value of packets.
SMAC	Source MAC address of packets.
DMAC	Destination MAC address of packets.
VLAN	VLAN ID of packets.
VNI	VNI ID of packets.

16.11.13 display netstream cache ip origin

Function

The **display netstream cache ip origin** command displays details about IPv4 original flow statistics on a device.

Format

display netstream cache ip origin [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**]

Parameters

Parameter	Description	Value
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ip *ip-address*	Specifies the destination IP address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ip *ip-address*	Indicates the source IP address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv4 original flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display details about IPv4 original flow statistics on the device.

```
<HUAWEI> display netstream cache ip origin slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
--------------------------------------------------------------------------------
 SrcIf              SrcIP/Mask           DstIP/Mask           L4 Info
 ToS                Direction            SrcAS                DstAS
 DstIf              TCP Flags            Octets               Packets
 NextHop            BGPNextHop
--------------------------------------------------------------------------------
 GE0/0/5            10.1.1.2/--          10.1.1.1/--          0:0:114
 0                  IN                   --                   --
 --                 0:0:0:0:0:0          5200                 50
 --                 --
--------------------------------------------------------------------------------
..........................
```

Table 16-76 Description of the **display netstream cache ip origin** command output

Item	Description
NOTE	Note.

Item	Description
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets: including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets: including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIf	Source interface of packets.
SrcIP/Mask	Source IP address and mask of packets.
DstIP/Mask	Destination IP address and mask of packets.
ToS	ToS of packets.
Direction	Packet sampling direction: ● IN: inbound direction ● OUT: outbound direction
SrcAS	Source AS number of packets.
DstAS	Destination AS number of packets.
DstIf	Destination interface of packets.
Octets	Number of octets in packets.
Packets	Number of packets.
NextHop	Next hop address.
BGP NextHop	BGP next hop address.

16.11.14 display netstream cache ipv6 record

Function

The **display netstream cache ipv6 record** command displays details about IPv6 flexible flow statistics on a device.

Format

display netstream cache ipv6 record *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ipv6** *ipv6-address* | **destination port** *port-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source ipv6** *ipv6-address* | **source port** *port-number* | **source mac-address** *mac-address* | **flowlabel** *flowlabel* | **protocol** *protocol-type* | **tos** *tos-number* | **ttl** *ttl-number* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**]

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	It must be an existing template name on the device.
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ipv6 *ipv6-address*	Specifies the destination IPv6 address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
destination mac-address *mac-address*	Specifies the destination MAC address of packets.	-
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ipv6 *ipv6-address*	Specifies the source IPv6 address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
source mac-address *mac-address*	Specifies the source MAC address of packets.	-
flowlabel *flowlabel*	Specifies the flow label of packets.	The value is an integer that ranges from 0 to 1048575.
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.
ttl *ttl-number*	Specifies the TTL value of packets.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
vlan *vlan-id*	Specifies the VLAN ID of packets.	The value is an integer that ranges from 1 to 4094.
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv6 flexible flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display IPv6 flexible flow statistics on the device.

```
<HUAWEI> display netstream cache ipv6 record test slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
--------------------------------------------------------------------------------
 SrcIP                                   SrcIf               L4 Info
 DstIP                                   DstIf               ToS
 NextHop                                    SrcAS               DstAS
 BGPNextHop                                    FlowLabel           Direction
 TCP Flags                                 Octets              Packets
 SMAC                                      VLAN                TTL
 DMAC
--------------------------------------------------------------------------------
 FC00:1::2                                 GE0/0/10            0:0:0
 FC00:3::2                                 GE0/0/11            0
 FC00:2::2                                  --                 --
 FC00:2::2                                      0                  OUT
 0:0:0:0:0:0                               6204                47
 00:e0:fc:12:34:56                            60                  20
 00:e0:fc:12:34:78
--------------------------------------------------------------------------------
```

Table 16-77 Description of the **display netstream cache ipv6 record** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets, including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets, including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIP	Source IPv6 address of packets.
SrcIf	Source interface of packets.
DstIP	Destination IPv6 address of packets.
DstIf	Destination interface of packets.
ToS	ToS of packets.
NextHop	Next hop address.
SrcAS	Source AS number of packets.
DstAS	Destination AS number of packets.
BGPNextHop	Address of the BGP next hop.
FlowLabel	IPv6 flow label.
Direction	Packet sampling direction: ● IN: inbound direction. ● OUT: outbound direction.
Octets	Number of octets in packets.
Packets	Number of packets.
SMAC	Source MAC address of packets.
VLAN	VLAN ID of packets.
TTL	TTL value of packets.
DMAC	Destination MAC address of packets.

16.11.15 display netstream cache ipv6 origin

Function

The **display netstream cache ipv6 origin** command displays details about IPv6 original flow statistics on a device.

Format

display netstream cache ipv6 origin [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ipv6** *ipv6-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ipv6** *ipv6-address* | **source port** *port-number* | **flowlabel** *flowlabel* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**]

Parameters

Parameter	Description	Value
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ipv6 *ipv6-address*	Specifies the destination IPv6 address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ipv6 *ipv6-address*	Specifies the source IPv6 address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
flowlabel *flowlabel*	Specifies the flow label of packets.	The value is an integer that ranges from 0 to 1048575.
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.

Parameter	Description	Value
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv6 original flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display details about IPv6 original flow statistics on the device.

```
<HUAWEI> display netstream cache ipv6 origin slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
-------------------------------------------------------------------------------
 SrcIf            TCP Flags        SrcIP/Mask
 DstIf            ToS              DstIP/Mask
 L4 Info          FlowLable        NextHop
 SrcAS            DstAS            BGP NextHop
 Direction        Octets           Packets
-------------------------------------------------------------------------------
 GE0/0/5          0:0:0:0:0:0      FEC0::801:200:0:A01:102/--
 --               0                FEC0::801:200:0:C108:101/--
 0:0:59           0                --
 --               --               --
 IN               3821896          36749
-------------------------------------------------------------------------------
.........................
```

Table 16-78 Description of the **display netstream cache ipv6 origin** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets: including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets: including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIf	Source interface of packets.
SrcIP/Mask	Source IPv6 address and mask of packets.
DstIf	Destination interface of packets.
ToS	Service type of packets.
DstIP/Mask	Destination IPv6 address and mask of packets.
FlowLable	IPv6 flow label.
NextHop	Next hop address.
SrcAS	Source AS number of packets.
DstAS	Destination AS number of packets.
BGP NextHop	BGP next hop address.
Direction	Packet sampling direction: ● IN: inbound direction ● OUT: outbound direction
Octets	Number of octets in packets.
Packets	Number of packets.

16.11.16 enable

Function

The **enable** command enables the aggregation function in the aggregation view.

The **undo enable** command disables the aggregation function in the aggregation view.

By default, the aggregation function is disabled.

Format

enable

undo enable

Parameters

None

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

The **enable** command takes effect only in the NetStream aggregation view. Flow statistics are exported according to the configured aggregation method only after you run the **enable** command in the aggregation view.

Example

Enable destination address prefix aggregation.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation destination-prefix
[HUAWEI-aggregation-dstpre] enable
```

16.11.17 export version

Function

The **export version** command configures the version of exported packets carrying aggregation flow statistics.

The **undo export version** command restores the default setting.

By default, the aggregation flow statistics are exported in the version of V8.

Format

export version *version*

undo export version

Parameters

Parameter	Description	Value
version	Specifies the version number of exported packets carrying aggregation flow statistics.	The value of *version* is set to 8 or 9. The default is 8.

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

The format of exported packets in V8 is fixed and is not easy to expand. The format of exported packets in V9 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

V9 is supported by most NSCs for its advantages. It is recommended that you set the version of exported packets carrying aggregation flow statistics to V9.

Example

Set the version number of exported packets carrying aggregation flow statistics to V9.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation as
[HUAWEI-aggregation-as] export version 9
```

16.11.18 ip netstream

Function

The **ip netstream** command enables IPv4 flow statistics collection on the inbound and outbound interfaces.

The **undo ip netstream** command restores the default setting.

By default, statistics collection for IPv4 flows is disabled on the inbound and outbound interfaces.

Format

ip netstream { **inbound** | **outbound** }

undo ip netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables flow statistics collection on the inbound interface.	-
outbound	Enables flow statistics collection on the outbound interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To export IPv4 flow statistics, you must run the **ip netstream** command to enable the IPv4 flow statistics collection function on the interface.

Precautions

- When the IPv4 and IPv6 flow statistics collection function is enabled on the interface, statistics about unicast and multicast packets are collected.
- After the statistics collection function is enabled for IPv4 and IPv6 flows, the statistics are independent of each other.
- Currently, the flow statistics collection function can be enabled only on the main interface. If the NetStream function is enabled on the main interface but you do not set a sampling ratio using the **ip netstream sampler** command, the main interface uses the sampling ratio of 1:1000. If you set the sampling ratio, the interface uses this sampling ratio.

Example

Enable the flow statistics collection function for the incoming IPv4 packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip netstream inbound
```

16.11.19 ip netstream aggregation

Function

The **ip netstream aggregation** command configures the aggregation method and displays the aggregation view.

Format

ip netstream aggregation { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }

Parameters

Parameter	Description	Value
as	Specifies the AS aggregation. It classifies flows based on: • Source AS number • Destination AS number • Inbound interface index • Outbound interface index	-
as-tos	Specifies the AS-ToS aggregation. It classifies flows based on: • Source AS number • Destination AS number • Inbound interface index • Outbound interface index • ToS	-

Parameter	Description	Value
destination-prefix	Specifies the destination-prefix aggregation. It classifies flows based on: ● Destination AS number ● Destination mask length ● Outbound interface index ● Destination prefix	-
destination-prefix-tos	Specifies the destination-prefix-ToS aggregation. It classifies flows based on: ● Destination AS number ● Destination mask length ● Destination prefix ● ToS ● Outbound interface index	-
prefix	Specifies the prefix aggregation. It classifies flows based on: ● Source and destination AS numbers ● Source and destination mask lengths ● Source and destination prefixes ● Inbound interface index ● Outbound interface index	-

Parameter	Description	Value
prefix-tos	Specifies the prefix-ToS aggregation. It classifies flows based on: • Source and destination AS numbers • Source and destination mask lengths • Source and destination prefixes • ToS • Inbound interface index • Outbound interface index	-
protocol-port	Specifies the protocol-port aggregation. It classifies flows based on: • Protocol number • Source port number • Destination port number	-
protocol-port-tos	Specifies the protocol-port-ToS aggregation. It classifies flows based on: • Protocol number • Source port number • Destination port number • ToS • Inbound interface index • Outbound interface index	-

Parameter	Description	Value
source-prefix	Specifies the source-prefix aggregation. It classifies flows based on: ● Source AS number ● Source mask length ● Source prefix ● Inbound interface index	-
source-prefix-tos	Specifies the source-prefix-ToS aggregation. It classifies flows based on: ● Source AS number ● Source mask length ● Source prefix ● ToS ● Inbound interface index	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

NetStream aggregation groups the original flows with the same attributes together. The aggregation flow statistics collection and original flow statistics collection are different. The original flow statistics collection is on the basis of sampled packets, while the aggregation flow statistics collection is on the basis of original flows. Therefore, the aggregation flow statistics collection generates less data.

Follow-up Procedure

Run the **enable** command in the aggregation view to enable the device to export flow statistics according to the configured aggregation method.

Example

Configure the NetStream AS aggregation method.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation as
[HUAWEI-aggregation-as]
```

Configure the NetStream destination-prefix aggregation method.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation destination-prefix
[HUAWEI-aggregation-dstpre]
```

16.11.20 ip netstream export host

Function

The **ip netstream export host** command configures the destination IP address and destination UDP port number for the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export host** command deletes the configured destination IP address and destination UDP port number for the exported packets carrying IPv4 flow statistics.

By default, no destination IP address and destination UDP port number are configured in the system view or aggregation view for the exported packets carrying IPv4 flow statistics.

Format

ip netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

undo ip netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IPv4 address of the exported packets carrying IPv4 flow statistics.	-
port-number	Specifies the destination UDP port number of the exported packets carrying IPv4 flow statistics.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified destination address belongs.	The value is the name of an existing VPN instance.

Views

System view, NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After finishing data collection, the NDE sends the collected data to the NSC. This command specifies the destination address of the collected data, that is, the NSC IP address.

Precautions

When you run the **ip netstream export host** command in the system view, this command configures the destination address for the exported packets carrying IPv4 original flow statistics and IPv4 flexible flow statistics; when you run this command in the aggregation view, this command configures the destination address for the exported packets carrying IPv4 aggregation flows. The exported packets carrying aggregation flow statistics preferentially use the destination address configured in the aggregation view. If the destination address is not configured in the aggregation view, the exported packets carrying aggregation flow statistics use the destination address configured in the system view.

You can configure two destination addresses in the system view or aggregation view to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ip host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of addresses is exceeded and the configuration fails.

Example

Set the destination IP address for the exported packets carrying original flow statistics to 10.1.1.1, and UDP port number to 222.

```
<HUAWEI> system-view
[HUAWEI] ip netstream export host 10.1.1.1 222
```

Set the destination IP address for the exported packets carrying aggregation flow statistics to 10.2.2.1, and UDP port number to 255.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation as
[HUAWEI-aggregation-as] ip netstream export host 10.2.2.1 255
```

16.11.21 ip netstream export index-switch

Function

The **ip netstream export index-switch** command sets the number of digits in the interface index contained in an exported packet carrying IPv4 flow statistics.

The **undo ip netstream export index-switch** command restores the default configuration.

By default, the number of digits in interface indexes is 16.

Format

ip netstream export index-switch *index-switch*

undo ip netstream export index-switch

Parameters

Parameter	Description	Value
index-switch	Specifies the number of digits in the index of a specified interface.	The value is 16 or 32. The default value is 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream export index-switch** command to set the number of digits in the interface index to 16 or 32.

The number of digits in an interface index contained in exported packets must be the same as the number of digits in an interface index that can be parsed by the NMS. For example, if the NMS can parse the 32-digit interface index, set the number of digits in an interface index contained in exported packets to 32.

Precautions

The number of digits in the interface index can be changed to 32 only when the NMS supports 32-digit interface index. If the number of digits in an interface index contained in exported packets is different from the number of digits in an interface index supported by the NMS, the NMS cannot identify NetStream packets sent by the device.

This command is valid for V9. Before changing 16-digit interface indexes to 32-digit interface indexes, ensure that:

- The version of exported packets of original flows is V9.
- The version of exported packets carrying aggregation flow statistics is V9.

When the 32-digit interface index is used, the version of exported packets of original flows cannot be changed from V9 to V5, and the version of exported packets carrying aggregation flow statistics cannot be changed from V9 to V8.

Example

Change the number of digits in the interface index contained in an exported packet carrying IPv4 flow statistics from 16 to 32.

```
<HUAWEI> system-view
[HUAWEI] ip netstream export version 9
[HUAWEI] ip netstream export index-switch 32
```

16.11.22 ip netstream export source

Function

The **ip netstream export source** command configures the source address for the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export source** command deletes the configured source address for the exported packets carrying IPv4 flow statistics.

By default, no source address is configured in the system view or aggregation view for the exported packets carrying IPv4 flow statistics.

Format

ip netstream export source *ip-address*

undo ip netstream export source

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address of the exported packets carrying IPv4 flow statistics.	The parameter must be set to an existing IP address on the device.

Views

System view, NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS identifies the data source according to the source IP address in NetStream packets, you need to specify the source IP address for NetStream packets.

Precautions

NetStream prefers the source IP address configured in the aggregation view. If no source address is specified in an aggregation method, the source address configured in the system view is used.

This command must be performed; otherwise, the source address of output packets may be 0.0.0.0, and the output packets may be discarded during transmission or cannot be parsed by the NetStream server.

Example

In the system view, set the source address for the exported packets carrying IPv4 flow statistics to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ip netstream export source 10.1.1.1
```

In the aggregation view, set the source address for the exported packets carrying IPv4 flow statistics to 10.2.2.2.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation as
[HUAWEI-aggregation-as] ip netstream export source 10.2.2.2
```

16.11.23 ip netstream export template timeout-rate

Function

The **ip netstream export template timeout-rate** command configures the interval at which the switch sends the NetStream export template to the NetStream server when IPv4 original or flexible flow statistics is exported in NetStream V9.

The **undo ip netstream export template timeout-rate** command restores the default setting.

By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes.

Format

ip netstream export template timeout-rate *timeout-interval*

undo ip netstream export template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

When IPv4 original or flexible flow statistics is exported in NetStream V9, the NetStream server can parse the exported packets in V9 only after receiving the NetStream export template from the switch. By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes. You can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Configure the switch to send the NetStream export template to the NetStream server at the interval of 10 minutes when IPv4 original or flexible flow statistics is exported in NetStream V9.

```
<HUAWEI> system-view
[HUAWEI] ip netstream export template timeout-rate 10
```

16.11.24 ip netstream export version

Function

The **ip netstream export version** command configures the version number and AS option of the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export version** command restores the default setting.

By default, the version number of the exported packets carrying IPv4 original flow statistics is 5 and no AS option is used. The version number of the exported packets carrying IPv4 flexible flow statistics is 9. Packets of V9 have no AS option and do not carry BGP next hop information.

Format

ip netstream export version *version* [**origin-as** | **peer-as**] [**bgp-nexthop**]

undo ip netstream export version

Parameters

Parameter	Description	Value
version	Specifies the version number of exported packets carrying IPv4 flow statistics.	The value of *version* is set to 5 or 9.

Parameter	Description	Value
origin-as	Specifies the AS number recorded in the statistics as the original AS number.	-
peer-as	Specifies the AS number recorded in the statistics as the peer AS number.	-
bgp-nexthop	Configures the statistics to carry BGP next hop information. Currently, only V9 supports the exported packets carrying BGP next hop information.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

The format of exported packets in V5 is fixed and is not easy to expand. The format of exported packets in V9 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

V9 is supported by most NSCs for its advantages. It is recommended that you set the version of exported packets carrying aggregation flow statistics to V9.

Precautions

- Only one version can be specified on a device. The versions configured on all the devices on the network must be the same as the version configured on the NMS.
- The AS option is used according to the actual situation of the AS configured on each device. The AS option affects only the packet statistics result, but does not affect the flows. The AS option is encapsulated in the AS option field carried in the NetStream packets sent to the NMS.
- To enable flexible flow statistics to be sent to the NSC to contain BGP next hop information, run the **collect ip bgp-next-hop** and **ip netstream export**

version 9 bgp-nexthop commands. Otherwise, the function does not take effect.

Example

Set the version of the exported packets carrying IPv4 flow statistics to V9 and AS option to **peer-as**.

```
HUAWEIsystem-viewHUAWEIip netstream export version 9 peer-as
```

16.11.25 ip netstream record

Function

The **ip netstream record** command creates a flexible flow statistics template or displays the view of an existing flexible statistics template.

The **undo ip netstream record** command deletes a specified flexible flow statistics template.

By default, no flexible flow statistics template exists.

Format

ip netstream record *record-name* [**vxlan inner-ip**]

undo ip netstream record *record-name* [**vxlan inner-ip**]

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	The value is a string of 1 to 32 case-insensitive characters without spaces or the following special characters: / \ : * ? " < > | @ ' %
vxlan inner-ip	Create a VXLAN flexible flow statistics template or enter the view of an existing VXLAN flexible flow statistics template. If this parameter is not specified, an IPv4 flexible flow statistics template is created by default or the view of an existing IPv4 flexible flow statistics template is displayed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You need to create a flexible flow statistics template before exporting flexible flow statistics.

Precautions

Each switch supports a maximum of 16 IPv4 flexible flow statistics templates and 16 VXLAN flexible flow statistics templates. To configure a 17th flexible flow statistics template, run the **undo ip netstream record** command to delete an existing one first.

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Create the flexible flow statistics template named **abc**.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record abc
[HUAWEI-record-abc]
```

16.11.26 ip netstream sampler

Function

The **ip netstream sampler** command configures the packet sampling function for IPv4 packets on an interface.

The **undo ip netstream sampler** command restores the default setting.

By default, an interface uses the packet-based regular sampling and the sampling ratio is 1000.

Format

ip netstream sampler fix-packets *packet-interval* { **inbound** | **outbound** }

undo ip netstream sampler [**fix-packets** *packet-interval*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Indicates the sampling ratio for packet-based regular sampling.	The value is an integer that ranges from 1 to 65535. **NOTE** For the S5731-H, S5731-S, S5731S-H, and S5731S-S, setting the sampling ratio to 1 affects the forwarding performance and can be performed on a maximum of eight interfaces. For details about how to calculate a sampling ratio, see NetStream Packet Sampling under the "NetStream Configuration" chapter in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Network Management and Monitoring*.
inbound	Samples incoming traffic on an interface.	-
outbound	Samples outgoing traffic on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can set an interval for sampling packets so that only statistics about sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces NetStream impact on device performance.

Precautions

You must run the **ip netstream sampler** command together with the **ip netstream** command. If you run only the **ip netstream sampler** command, the command does not take effect.

If you run the **ip netstream sampler** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the packet-based regular sampling ratio for incoming IPv4 packets on GE0/0/1 to 1200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip netstream sampler fix-packets 1200 inbound
[HUAWEI-GigabitEthernet0/0/1] ip netstream inbound
```

16.11.27 ip netstream tcp-flag enable

Function

The **ip netstream tcp-flag enable** command configures the aging of NetStream traffic according to the FIN flag or the RST flag in the TCP packet header.

The **undo ip netstream tcp-flag enable** command restores the default setting.

By default, NetStream flows are not aged according to the FIN or RST flag in the TCP packet header.

Format

ip netstream tcp-flag enable

undo ip netstream tcp-flag enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The FIN or RST flag in a TCP packet indicates that the TCP connection is terminated. When receiving a packet with the FIN or RST flag, the device immediately ages the corresponding NetStream flow. If the **ip netstream tcp-flag enable** command is not run, NetStream flows are aged by following other criteria, for example, inactive aging time or bytes overflow.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Only original flows can be aged according to the FIN or RST flag in the TCP packet header.

Example

Configure the aging of original flows according to the FIN or RST flag in the TCP packet header.

```
<HUAWEI> system-view
[HUAWEI] ip netstream tcp-flag enable
```

16.11.28 ip netstream timeout active

Function

The **ip netstream timeout active** command configures the active flow aging time.

The **undo ip netstream timeout active** command restores the default setting.

By default, the active flow aging time is 200 seconds.

Format

ip netstream timeout active *active-interval*

undo ip netstream timeout active

Parameters

Parameter	Description	Value
active-interval	Specifies the active aging time.	The value is an integer that ranges from 1 to 300, in seconds. The default is 200.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the active time (from flow creation time to the current time) of a flow exceeds the specified active aging time, the flow is exported to the destination.

To quickly detect the status of an active flow, set the active time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the active time to a large value.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the active aging time to 240 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip netstream timeout active 240
```

16.11.29 ip netstream timeout inactive

Function

The **ip netstream timeout inactive** command configures the inactive aging time.

The **undo ip netstream timeout inactive** command restores the default setting.

By default, the inactive aging time is 30 seconds.

Format

ip netstream timeout inactive *inactive-interval*

undo ip netstream timeout inactive

Parameters

Parameter	Description	Value
inactive-interval	Specifies the inactive aging time.	The value is an integer that ranges from 1 to 300, in seconds. The default is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the inactive time (from the last packet receiving time to the current time) of an original or flexible flow exceeds the specified inactive aging time, the flow is exported to the destination.

To quickly detect the status of an inactive flow, set the inactive time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the inactive time to a large value.

Precautions

The inactive aging time that is configured using the **ip netstream timeout inactive** command applies to both IPv4 and IPv6 flows.

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the inactive aging time to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip netstream timeout inactive 20
```

16.11.30 ipv6 netstream

Function

The **ipv6 netstream** command enables IPv6 flow statistics collection on the inbound and outbound interfaces.

The **undo ipv6 netstream** command restores the default setting.

By default, statistics collection for IPv6 flows is disabled on the inbound and outbound interfaces.

Format

ipv6 netstream { **inbound** | **outbound** }

undo ipv6 netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables IPv6 flow statistics collection on the inbound interface.	-
outbound	Enables IPv6 flow statistics collection on the outbound interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To export IPv6 flow statistics, you must run the **ipv6 netstream** command to enable IPv6 flow statistics collection on the inbound interface.

Precautions

- When the IPv4 and IPv6 flow statistics collection function is enabled on the interface, statistics about unicast and multicast packets are collected.
- After the statistics collection function is enabled for IPv4 and IPv6 flows, the statistics are independent of each other.
- Currently, flow statistics collection can be enabled only on main interfaces. If statistics collection is enabled on an interface but you do not set a sampling ratio using the **ipv6 netstream sampler** command, the interface uses the sampling ratio of 1:1000. If you have set the sampling ratio, the interface uses this sampling ratio.

Example

Enable statistics collection for the incoming IPv6 flows on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv6 netstream inbound
```

16.11.31 ipv6 netstream export host

Function

The **ipv6 netstream export host** command configures the destination IP address and destination UDP port number for the exported packets carrying IPv6 flow statistics.

The **undo ipv6 netstream export host** command deletes the configured destination IP address and destination UDP port number for the exported packets carrying IPv6 flow statistics.

By default, no destination IP address or destination UDP port number is configured in the system view for the exported packets carrying IPv6 flow statistics.

Format

ipv6 netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

undo ipv6 netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IPv4 address of the exported packets carrying IPv6 flow statistics.	-
port-number	Specifies the destination UDP port number of the exported packets.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified destination address belongs.	The value is the name of an existing VPN instance.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After finishing data collection, the NDE sends the collected data to the NSC. This command specifies the destination address of the collected data, that is, the NSC IP address.

Precautions

The **netstream export ipv6 host** command configures the destination address for the exported packets carrying IPv6 original flows and flexible flows.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo ipv6 netstream export host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of addresses is exceeded and the configuration fails.

Example

Set the destination IP address for the exported packets carrying IPv6 original flows to 10.1.1.1, and UDP port number to 222.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export host 10.1.1.1 222
```

16.11.32 ipv6 netstream export index-switch

Function

The **ipv6 netstream export index-switch** command sets the number of digits in the interface index contained in an exported packet carrying IPv6 flow statistics.

The **undo ipv6 netstream export index-switch** command restores the default setting.

By default, an interface index contains 16 digits.

Format

ipv6 netstream export index-switch *index-switch*

undo ipv6 netstream export index-switch

Parameters

Parameter	Description	Value
index-switch	Specifies the digit of the interface index.	The value is an integer that can be 16 or 32. The default is 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ipv6 netstream export index-switch** command to set the number of digits in the interface index to 16 or 32.

Set the type of the interface index contained in exported packets the same as the type of the interface index that can be parsed by the NMS. For example, if the NMS can parse the 32-digit interface index, set the type of the interface index contained in exported packets to 32-digit interface index.

Prerequisites

The interface index length in exported packets can be set to 32 bits only when the NMS supports 32-bit interface index; otherwise, the NMS cannot identify the NetStream packets.

Example

Change the interface index type of the exported packets carrying IPv6 flow statistics from 16-digit to 32-digit.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export index-switch 32
```

16.11.33 ipv6 netstream export source

Function

The **ipv6 netstream export source** command configures the source address for the exported packets carrying IPv6 flow statistics.

The **undo ipv6 netstream export source** command deletes the configured source address for the exported packets carrying IPv6 flow statistics.

By default, no source address is configured on the device for the exported packets carrying IPv6 flow statistics.

Format

ipv6 netstream export source *ip-address*

undo ipv6 netstream export source

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address of the exported packets carrying IPv6 flow statistics.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS identifies the data source according to the source IP address in NetStream packets, you need to specify the source IP address for NetStream packets.

Precautions

This command must be performed; otherwise, the source address of output packets may be 0.0.0.0, and the output packets may be discarded during transmission or cannot be parsed by the NetStream server.

Example

In the system view, set the source address for the exported packets carrying IPv6 flow statistics to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export source 10.1.1.1
```

16.11.34 ipv6 netstream export template timeout-rate

Function

The **ipv6 netstream export template timeout-rate** command configures the interval at which the switch sends the NetStream export template to the NetStream server when IPv6 original or flexible flow statistics is exported in NetStream V9.

The **undo ipv6 netstream export template timeout-rate** command restores the default setting.

By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes.

Format

ipv6 netstream export template timeout-rate *timeout-interval*

undo ipv6 netstream export template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

When IPv6 original or flexible flow statistics is exported in NetStream V9, the NetStream server can parse the exported packets in V9 only after receiving the NetStream export template from the switch. By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes. You can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Configure the switch to send the NetStream export template to the NetStream server at the interval of 10 minutes when IPv6 original or flexible flow statistics is exported in NetStream V9.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export template timeout-rate 10
```

16.11.35 ipv6 netstream export version

Function

The **ipv6 netstream export version** command configures the version number and AS option of the exported packets carrying IPv6 flow statistics.

The **undo ipv6 netstream export version** command restores the default setting.

By default, the version number of the exported packets carrying IPv6 flow statistics is not specified.

Format

ipv6 netstream export version *version* [**origin-as** | **peer-as**]

undo ipv6 netstream export version

Parameters

Parameter	Description	Value
version	Specifies the version of exported packets.	Only V9 is supported.
origin-as	Specifies the AS number recorded in the statistics as the original AS number.	-
peer-as	Specifies the AS number recorded in the statistics as the peer AS number.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

Precautions

The AS option is used according to the actual situation of the AS configured on each device. The AS option affects only the packet statistics result, but does not affect the flows. The AS option is encapsulated in the AS option field carried in the NetStream packets sent to the NMS.

Example

Set the version of exported packets carrying IPv6 flow statistics to V9 and AS to **peer-as**.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export version 9 peer-as
```

16.11.36 ipv6 netstream sampler

Function

The **ipv6 netstream sampler** command configures packet sampling for IPv6 packets on an interface.

The **undo ipv6 netstream sampler** command restores the default setting.

By default, an interface uses the packet-based regular sampling and the sampling ratio is 1000.

Format

ipv6 netstream sampler fix-packets *packet-interval* { **inbound** | **outbound** }

undo ipv6 netstream sampler [**fix-packets** *packet-interval*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Indicates the sampling ratio for packet-based regular sampling.	The value is an integer that ranges from 1 to 65535. **NOTE** For the S5731-H, S5731-S, S5731S-H, and S5731S-S, setting the sampling ratio to 1 affects the forwarding performance and can be performed on a maximum of eight interfaces. For details about how to calculate a sampling ratio, see NetStream Packet Sampling under the "NetStream Configuration" chapter in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Network Management and Monitoring*.
inbound	Samples incoming traffic on an interface.	-
outbound	Samples outgoing traffic on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can set an interval for sampling packets so that only statistics about sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces impact of NetStream on device performance.

Precautions

You must run the **ipv6 netstream sampler** command together with the **ipv6 netstream** command. If you run only the **ipv6 netstream sampler** command, the command does not take effect.

If you run the **ipv6 netstream sampler** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the packet-based regular sampling interval for incoming IPv6 packets on GE0/0/1 to 1200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv6 netstream inbound
[HUAWEI-GigabitEthernet0/0/1] ipv6 netstream sampler fix-packets 1200 inbound
```

16.11.37 mask

Function

The **mask** command sets the aggregation mask length.

The **undo mask** command restores the default setting.

By default, no aggregation mask is configured.

Format

mask { **source** | **destination** } **minimum** *mask-length*

undo mask { **source** | **destination** }

Parameters

Parameter	Description	Value
source	Indicates the aggregation mask of the source address. It is used in the following aggregation methods: prefix, prefix-ToS, source-prefix, and source-prefix-ToS.	-
destination	Indicates the aggregation mask of the destination address. It is used in the following aggregation methods: prefix, prefix-ToS, destination-prefix, or destination-prefix-ToS.	-
mask-length	Specifies the aggregation mask length.	The value is an integer that ranges from 1 to 32.

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system uses the larger value between the set mask and the largest mask in the FIB table. If the aggregation mask is not configured, the system uses the mask in the FIB table for aggregation.

Precaution

Aggregation masks are applied to six aggregation methods: **destination-prefix**, **destination-prefix-tos**, **prefix**, **prefix-tos**, **source-prefix**, and **source-prefix-tos**.

Example

Set the aggregation mask length in the source-prefix aggregation method to 24.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation source-prefix
[HUAWEI-aggregation-srcpre] mask source minimum 24
```

16.11.38 match (Flexible Flow Statistics Template View)

Function

The **match** command configures aggregation keywords for flexible flow statistics.

The **undo match** command deletes aggregation keywords configured for flexible flow statistics.

By default, no aggregation keyword for flexible flow statistics is configured in a flexible flow statistics template.

Format

match ip { **protocol** | **dscp** | **source-address** | **destination-address** | **source-port** | **destination-port** | **flow-label** | **ttl** }

match { **vlan** | **source-mac** | **destination-mac** } { **input** | **output** }

undo match ip { **protocol** | **dscp** | **source-address** | **destination-address** | **source-port** | **destination-port** | **flow-label** | **ttl** }

undo match { **vlan** | **source-mac** | **destination-mac** } { **input** | **output** }

Parameters

Parameter	Description	Value
ip	Aggregates statistics based on packet information at the network layer or transport layer.	-
protocol	Aggregates statistics based on the protocol type.	-
dscp	Aggregates statistics based on the DSCP priority.	-
source-address	Aggregates statistics based on the source IP address.	-
destination-address	Aggregates statistics based on the destination IP address.	-
source-port	Aggregates statistics based on the source port number.	-
destination-port	Aggregates statistics based on the destination port number.	-
flow-label	Aggregates statistics based on the IPv6 flow label.	-
ttl	Aggregates statistics based on the TTL value.	-
vlan	Aggregates statistics based on the VLAN ID.	-
source-mac	Aggregates statistics based on the source MAC address.	-
destination-mac	Aggregates statistics based on the destination MAC address.	-

Parameter	Description	Value
input	Aggregates statistics about incoming packets. **NOTE** If this parameter is specified, the flexible flow statistics template can be applied only to the inbound direction of an interface.	-
output	Aggregates statistics about outgoing packets. **NOTE** If this parameter is specified, the flexible flow statistics template can be applied only to the outbound direction of an interface.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During exporting of flexible flow statistics, you can run the **match** command to configure aggregation keywords for flexible flow statistics.

Precautions

If you run this command multiple times, you can obtain a collection of multiple aggregation keywords. However, the **input** and **output** keywords cannot coexist in a flexible flow statistics template, regardless of whether the aggregation keywords before **input**/**output** are the same.

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Set the flexible flow statistics template **abc123** to aggregate flows based on the source port number.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record abc123
[HUAWEI-record-abc123] match ip source-port
```

16.11.39 port ip netstream record

Function

The **port ip netstream record** command applies a flexible flow statistics template to an interface.

The **undo port ip netstream record** command unbinds a specified flexible flow statistics template from an interface.

By default, no flexible flow statistics template is applied to an interface.

Format

port ip netstream record *record-name* [**vxlan inner-ip**] [**inbound** | **outbound**]

undo port ip netstream record [*record-name* [**vxlan inner-ip**] [**inbound** | **outbound**]]

NOTE

If neither **inbound** nor **outbound** is configured, the flexible flow statistics template is applied to both the inbound and outbound directions of an interface.

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	The value must be the name of an existing flexible flow statistics template.
inbound	Applies the flexible flow statistics template to the inbound direction of an interface.	-
outbound	Applies the flexible flow statistics template to the outbound direction of an interface.	-
vxlan inner-ip	Applies a VXLAN flexible statistics template to an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a flexible flow statistics template is configured, run the **port ip netstream record** command to apply the template to an interface.

The interface then aggregates flows based on the configured aggregation keywords, collects flow statistics, and exports aged flows to the NSC.

Prerequisites

A flexible flow statistics template has been created using the **ip netstream record** command, and at least one aggregation keyword has been configured using the **match** command in the flexible flow statistics template view.

Precautions

- If the **vlan** parameter is configured in the flexible flow statistics template, it is recommended that the template be applied to Layer 2 Ethernet interfaces.
- If the **input** parameter is configured in the flexible flow statistics template, the template can be applied only to the inbound direction of an interface. If the **output** parameter is configured in the flexible flow statistics template, the template can be applied only to the outbound direction of an interface.
- The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.
- Each direction of an interface can have only one flexible flow statistics template applied. The templates applied to the inbound and outbound directions of an interface can be the same or different. To change a flexible flow statistics template, run the **undo port ip netstream record** command to delete the existing template.

Example

Configure the flexible flow statistics template **abc1** (aggregating flows based on the source and destination IP addresses, collecting statistics about the number of packets, and exporting the inbound interface index). Apply the template to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record abc1
[HUAWEI-record-abc1] match ip source-address
[HUAWEI-record-abc1] match ip destination-address
[HUAWEI-record-abc1] collect counter packets
[HUAWEI-record-abc1] collect interface input
[HUAWEI-record-abc1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port ip netstream record abc1
```

16.11.40 refresh netstream template

Function

The **refresh netstream template** command immediately refreshes the NetStream export template.

By default, the template is refreshed every 30 minutes.

Format

refresh netstream template

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After a NetStream server restarts, you need to run this command to enable the device to immediately resend the NetStream export template. Only the V9 template supports this command.

Example

Refresh the NetStream export template.

```
<HUAWEI> refresh netstream template
```

16.11.41 reset ip netstream cache

Function

The **reset ip netstream cache** command forcibly ages all the flows in the cache.

Format

reset ip netstream cache slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the actual configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the original flows in the cache and export the flow statistics.

NOTE

If you run the **reset ip netstream cache** command on the device before the inactive aging time is reached, the NDE does not export the flow statistics to the NSC.

Example

Age all the flows forcibly in slot 0.

```
<HUAWEI> system-view
[HUAWEI] reset ip netstream cache slot 0
```

16.11.42 reset ip netstream statistics

Function

The **reset ip netstream statistics** command deletes NetStream flow statistics.

Format

reset ip netstream statistics slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the actual configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When diagnosing and locating network faults, collect flow statistics in a specified period. Before statistics collection starts, you can run this command to delete historical statistics.

Precautions

The **reset ip netstream statistics** command deletes all NetStream statistics. The statistics cannot be restored after being deleted. Therefore, confirm the action before running this command.

You can run this command multiple times at any interval.

Example

Delete NetStream statistics in slot 0.

```
<HUAWEI> reset ip netstream statistics slot 0
```

16.11.43 template timeout-rate

Function

The **template timeout-rate** command configures the interval at which the switch sends the NetStream export template to the NetStream server when IPv4 aggregation flow statistics is exported in NetStream V9.

The **undo template timeout-rate** command restores the default setting.

By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes.

Format

template timeout-rate *timeout-interval*

undo template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

When IPv4 aggregation flow statistics is exported in NetStream V9, the NetStream server can parse the exported packets in V9 only after receiving the NetStream export template from the switch. By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes. You can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Configure the switch to send the NetStream export template to the NetStream server at the interval of 10 minutes when IPv4 aggregation flow statistics is exported in NetStream V9.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation source-prefix
[HUAWEI-aggregation-srcpre] template timeout-rate 10
```

16.12 sFlow Configuration Commands

NOTE

sFlow collects statistics and analyzes service traffic. During service provisioning, personal data may be involved. You have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

16.12.1 Command Support

Only the following switch models support sFlow:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-S, S6735-S, S6720-EI, S6720S-EI

16.12.2 display sflow

Function

The **display sflow** command displays the sFlow configuration on a specified device.

Format

display sflow [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the sFlow information on a device, where *slot-id* specifies the slot ID of the device. If this parameter is not configured, the global sFlow configuration is displayed.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the sFlow function, you can use the **display sflow** command to verify the configuration.

The **display sflow** command shows the sFlow configuration, which helps you locate faults.

Example

Display the sFlow configuration on a specified device.

```
<HUAWEI> display sflow slot 0
sFlow Version 5 Information:
----------------------------------------------------------------------------
Agent Information:

     IP Address: 192.168.1.206(CLI)
 Address family: IPV4
   Vpn-instance: NA
----------------------------------------------------------------------------
```

```
Collector Information:

   Collector ID: 1
     IP Address: 192.168.1.194
 Address family: IPV4
   Vpn-instance: NA
           Port: 6343
  Datagram size: 1500
       Time out: NA
    Description: zjm-pc
-------------------------------------------------------------------------------
Port on slot 0 Information:

Interface: GE0/0/1
  Flow-sample collector: 1            Counter-sample collector  : 1
  Flow-sample rate(1/x): 2048         Counter-sample interval(s): 10
  Flow-sample maxheader: 64
  Flow-sample direction: IN,OUT
<HUAWEI> display sflow slot 0
sFlow Version 5 Information:
-------------------------------------------------------------------------------
Agent Information:

     IP Address: 192.168.1.20(Auto)
 Address family: IPV4
   Vpn-instance: NA
 Related collector: 1
-------------------------------------------------------------------------------
Collector Information:

   Collector ID: 1
     IP Address: 192.168.1.94
 Address family: IPV4
   Vpn-instance: NA
           Port: 6343
  Datagram size: 1400
       Time out: NA
    Description: NA
-------------------------------------------------------------------------------
Port on slot 0 Information:

Interface: GE0/0/2
 Flow-sample collector: NA           Counter-sample collector  : NA
 Flow-sample rate(1/x): 257          Counter-sample interval(s): 2
 Flow-sample maxheader: 512
 Flow-sample direction: IN
```

Table 16-79 Description of the **display sflow** command output

Item	Description
sFlow Version 5 Information	Configuration information about sFlow V5.
Agent Information	Configuration of the sFlow Agent.

Item	Description
IP Address	IP address of the sFlow Agent. To configure this parameter, run the **sflow agent** command. The string in the parentheses next to the IP address can be: - CLI: Indicate that this IP address is specified using the **sflow agent** command. - Auto: Indicate that the sFlow agent uses the IP address of the outbound interface in the route to the sFlow collector as the sFlow agent IP address.
Address family	Address family of the sFlow Agent: - IPV4: IPv4 address family - IPV6: IPv6 address family To configure this parameter, run the **sflow agent** command.
Vpn-instance	VPN instance of the sFlow Agent. To configure this parameter, run the **sflow agent** command. The value will be NA if this parameter is not configured in the **sflow agent** command.
Related collector	Collector ID corresponding to the IP address automatically selected by the sFlow agent.
Collector Information	Configuration of the sFlow Collector.
Collector ID	ID of the sFlow Collector. To configure this parameter, run the **sflow collector** command.
IP Address	IP address of the sFlow Collector. To configure this parameter, run the **sflow collector** command.
Address family	Address family of the sFlow collector: - IPV4: IPv4 address family - IPV6: IPv6 address family To configure this parameter, run the **sflow collector** command.
Vpn-instance	VPN instance of the sFlow Collector. To configure this parameter, run the **sflow collector** command. The value will be NA if this parameter is not configured in the **sflow collector** command.
Port	Port number of the sFlow Collector. To configure this parameter, run the **sflow collector** command.
Datagram size	Maximum length of sFlow packets sent to the sFlow Collector. To configure this parameter, run the **sflow collector** command.

Item	Description
Time out	Aging time of the sFlow Collector. To configure this parameter, run the **sflow collector** command. The value will be NA if this parameter is not configured or is set to 0 in the **sflow collector** command.
Description	Description of the sFlow Collector. To configure this parameter, run the **sflow collector** command. The value will be NA if this parameter is not configured in the **sflow collector** command.
Port on slot 0 Information	sFlow configuration on the interface in slot 0.
Interface	sFlow-enabled interface. To configure this parameter, run the **sflow flow-sampling collector** command.
Flow-sample collector	sFlow Collector that receives flow sampling data. To configure this parameter, run the **sflow flow-sampling collector** command.
Counter-sample collector	sFlow Collector that receives counter sampling data. To configure this parameter, run the **sflow counter-sampling collector** command.
Flow-sample rate(1/x)	Flow sampling rate. To configure this parameter, run the **sflow flow-sampling rate** command.
Counter-sample interval(s)	Counter sampling interval. To configure this parameter, run the **sflow counter-sampling interval** command.
Flow-sample maxheader	The maximum bytes of data that can be copied from a sampled packet in flow sampling. To configure this parameter, run the **sflow flow-sampling max-header** command.
Flow-sample direction	Flow sampling direction: ● IN: Enable flow sampling in the inbound direction. ● OUT: Enable flow sampling in the outbound direction. ● IN,OUT: Enable flow sampling in both inbound direction and outbound direction. To configure this parameter, run the **sflow flow-sampling** command.

16.12.3 display sflow statistics

Function

The **display sflow statistics** command displays sFlow statistics.

Format

display sflow statistics [**slot** *slot-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a device.	The value is an integer and must be set according to the device configuration.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display sflow statistics** command displays sFlow statistics, including the sampling mode, number of sampled packets, sequence number of sent packets, and number of discarded sFlow packets because of expiration. You can use the command output to locate faults.

Example

Display sFlow statistics.

```
<HUAWEI> display sflow statistics
sFlow Version 5 statistic Information:
--------------------------------------------------------------------------
Collector 1 Current sample sequence:22388
--------------------------------------------------------------------------
Port on slot 0 statistic Information:

Interface: GE0/0/1
Flow-sample sequence    : 7         Counter-sample sequence : 44778
Flow-sample inbound pool: 28000       Flow-sample outbound pool: 4000
--------------------------------------------------------------------------
```

Table 16-80 Description of the **display sflow statistics** command output

Item	Description
sFlow Version 5 statistic Information	sFlow sampling of sFlow version 5.

Item	Description
Collector 1 Current sample sequence	Sampling sequence number of the sFlow collector.
Port on slot 0 statistic Information	sFlow sampling information on slot 0.
Interface: GE0/0/1	sFlow-enabled interface.
Flow-sample sequence	Sequence number for flow sampling on an interface.
Counter-sample sequence	Sequence number for counter sampling on an interface.
Flow-sample inbound pool	Number of incoming packets for flow sampling on an interface.
Flow-sample outbound pool	Number of outgoing packets for flow sampling on an interface.

16.12.4 sflow agent

Function

The **sflow agent** command creates an sFlow agent and specifies an IP address for the sFlow agent or updates the IP address of the existing sFlow agent.

The **undo sflow agent** command deletes the IP address of an sFlow agent.

By default, an sFlow agent uses the IP address of the outbound interface in the route to the sFlow collector as the sFlow agent IP address of sFlow packets.

Format

sflow agent { **ip** [**vpn-instance** *vpn-instance-name*] *ip-address* | **ipv6** [**vpn-instance** *vpn-instance-name*] *ipv6-address* }

undo sflow agent { **ip** [**vpn-instance** *vpn-instance-name*] *ip-address* | **ipv6** [**vpn-instance** *vpn-instance-name*] *ipv6-address* }

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IPv4 address of an sFlow agent.	The value is in dotted decimal notation and is a valid unicast address except 127.X.X.X.

Parameter	Description	Value
ipv6 *ipv6-address*	Specifies an IPv6 address of the sFlow agent.	The value is an IPv6 unicast address, which is a 32-digit hexadecimal number.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

sFlow is a traffic monitoring technique that collects and analyzes traffic statistics. An sFlow agent encapsulates traffic statistics into sFlow packets and sends the sFlow packets to specified sFlow collectors. To send the sFlow packets to a certain sFlow collector, configure an IP address for the sFlow agent as the source address of sFlow packets. The sFlow collector analyzes and displays the traffic statistics based on the traffic in the received sFlow packets. Network administrators can view the traffic statistics on a specified interface based on the IP address of the sFlow agent and interface number.

Prerequisites

- The IP address configured as the source address must exist on the device.
- A VPN instance has been created if the sFlow agent is located on a private network.

Configuration Impact

If you run the **sflow agent** command multiple times, only the latest configuration takes effect.

Precautions

A maximum of two sFlow agents can be configured in the system, and each VPN instance of an address family supports only one agent. The IP address of an agent must be a valid unicast IP address of an interface. If an IPv6 address is specified for an agent, the IPv6 address must be a global unicast address, but cannot be a link-local address.

Example

Configure an IPv4 address for the sFlow agent.

```
<HUAWEI> system-view
[HUAWEI] sflow agent ip 192.168.100.10
```

Configure an IPv6 address for the sFlow agent.

```
<HUAWEI> system-view
[HUAWEI] sflow agent ipv6 FC00::1
```

16.12.5 sflow collector

Function

The **sflow collector** command creates an sFlow collector and sets or modifies optional parameters for the sFlow collector.

The **undo sflow collector** command restores default values of optional parameters of the sFlow collector or deletes the sFlow collector.

By default, no sFlow collector is configured.

Format

sflow collector *collector-id* { **ip** [**vpn-instance** *vpn-instance-name*] *ip-address* | **ipv6** [**vpn-instance** *vpn-instance-name*] *ipv6-address* } [**datagram-size** *datagram-size* | **port** *port-num* | **time-out** *time*] * [**description** *description*]

sflow collector *collector-id* { **datagram-size** *datagram-size* | **port** *port-num* } * [**description** *description*]

undo sflow collector *collector-id* [**datagram-size** | **port** | **description**] *

Parameters

Parameter	Description	Value
collector-id	Specifies the ID of an sFlow collector. This ID is used when you specify the collector in subsequent sFlow configuration.	The value is an integer that can be 1 or 2.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies an IPv4 address of the sFlow collector.	The value is a value unicast IP address in X.X.X.X format, dotted decimal notation. The value cannot be 127.X.X.X.

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address for the sFlow collector.	The value is a 32-digit hexadecimal number in the format of X:X:X:X:X:X:X:X and is a valid global IPv6 unicast address.
datagram-size *datagram-size*	Specifies the maximum length of sFlow packets sent from an sFlow agent to an sFlow collector.	The value is an integer, in bytes. It ranges from 1024 to 8100. The default value is 1400.
port *port-num*	Specifies the UDP destination port number of sFlow packets.	The value is an integer that ranges from 1 to 65535. The default value is 6343.
description *description*	Specifies the description of an sFlow collector.	The value is a string of 1 to 255 case-sensitive characters without spaces.
time-out *time*	Specifies the aging time of an sFlow collector.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0, indicating that the sFlow collector is not aged out. If the default value is used, the aging time cannot be changed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage scenario

sFlow is a traffic monitoring technique that collects and analyzes traffic statistics. An sFlow agent encapsulates traffic statistics into sFlow packets and sends the sFlow packets to all sFlow collectors. To send the sFlow packets to a certain sFlow collector, configure an sFlow collector used to receive sFlow packets and analyze traffic of sFlow packets. When both flow sampling and counter sampling are configured on an interface of an sFlow agent, the sFlow agent sends the flow sampling data and counter sampling data to one or two sFlow collectors. Because sFlow packets are sampled quickly and the number of sFlow packets sent every second is limited, run the **sflow collector** command with **datagram-size length** specified to set the maximum length of sFlow packets so that an sFlow packet carries more sampled data. This reduces the number of sent sFlow packets.

NOTE

When you create an sFlow collector, specify the ID and IP address for the sFlow collector. If the aging time of the sFlow collector is not set, the sFlow collector is not aged out by default and the aging time cannot be changed.

Prerequisites

- There is a reachable route between an sFlow agent and an sFlow collector.
- A VPN instance has been created if the sFlow collector is located on a private network.

Configuration Impact

If you run the **sflow collector** command multiple times on the same address family and VPN instance, only the latest configuration takes effect.

Precautions

A maximum of two sFlow collectors can be configured in the system.

Example

Configure an IPv4 address for the sFlow collector, and set the aging time of the sFlow collector to 100s.

```
<HUAWEI> system-view
[HUAWEI] sflow collector 1 ip 192.168.100.10 time-out 100
```

Configure an IPv6 address for the sFlow collector, and set the aging time of the sFlow collector to 100s.

```
<HUAWEI> system-view
[HUAWEI] sflow collector 1 ipv6 FC00::1 time-out 100
```

16.12.6 sflow counter-sampling collector

Function

The **sflow counter-sampling collector** command specifies the target sFlow collector that receives counter sampling data.

The **undo sflow counter-sampling collector** command deletes the target sFlow collector.

By default, no target sFlow collector is specified.

Format

sflow counter-sampling collector { *collector-id* | **all** }

undo sflow counter-sampling collector { *collector-id* | **all** }

Parameters

Parameter	Description	Value
collector-id	Specifies the ID of the target sFlow collector that receives counter sampling data.	The value is an integer that can be 1 or 2. **NOTE** The value of *collector-id* is set using the **sflow collector** command.
all	Indicates all the configured sFlow collectors.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

Counter sampling is based on time. An sFlow agent periodically obtains traffic statistics on an interface, encapsulates the traffic statistics into sFlow packets, and sends them to an sFlow collector. When multiple sFlow collectors are configured, you can run the **sflow counter-sampling collector** command to specify the target sFlow collector to receive the counter sampling data. Each interface can send sFlow sampling data to a maximum of two sFlow collectors.

When you run the **sflow counter-sampling collector** command to specify the first target sFlow collector on an interface, counter sampling is enabled on the interface. When you run the **undo sflow counter-sampling collector** command to delete the last target sFlow collector on an interface, counter sampling is disabled on the interface.

Prerequisites

An sFlow collector has been created using the **sflow collector** command.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces.

Example

Specify sFlow collector 1 to receive counter sampling data.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow counter-sampling collector 1
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and specify sFlow collector 1 to receive counter sampling data for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow counter-sampling collector 1
```

16.12.7 sflow counter-sampling interval

Function

The **sflow counter-sampling interval** command sets the counter sampling interval on an interface.

The **undo sflow counter-sampling interval** command restores the default counter sampling interval on an interface.

By default, the counter sampling interval on an interface is 10s.

Format

sflow counter-sampling interval *interval*

undo sflow counter-sampling interval

Parameters

Parameter	Description	Value
interval *interval*	Specifies the counter sampling interval.	The value is an integer that ranges from 2 to 3600, in seconds. The default value is 10.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

Counter sampling is based on time. An sFlow agent periodically obtains traffic statistics on an interface, encapsulates the traffic statistics into sFlow packets, and sends them to an sFlow collector. You can run the **sflow counter-sampling interval** command to set an appropriate counter sampling interval.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces. If you run the **sflow flow-sampling rate** command multiple times, only the latest configuration takes effect.

Example

Set the counter sampling interval to 100s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow counter-sampling interval 100
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and set the counter sampling interval to 100s for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow counter-sampling interval 100
```

16.12.8 sflow flow-sampling

Function

The **sflow flow-sampling** command enables flow sampling in a specified direction on an interface.

The **undo sflow flow-sampling** command disables flow sampling in a specified direction on an interface.

By default, flow sampling is enabled in both directions on an interface.

Format

sflow flow-sampling { **inbound** | **outbound** }

undo sflow flow-sampling { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables flow sampling in the inbound direction.	-
outbound	Enables flow sampling in the outbound direction.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

You can specify the direction in which flow sampling is performed. Flow sampling can be performed in both inbound and outbound directions.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces. If you run the **sflow flow-sampling rate** command multiple times, only the latest configuration takes effect.

Example

Enable flow sampling in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling inbound
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and enable flow sampling in the inbound direction of the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling inbound
```

16.12.9 sflow flow-sampling collector

Function

The **sflow flow-sampling collector** command specifies the target sFlow collector that receives flow sampling data.

The **undo sflow flow-sampling collector** command deletes the target sFlow collector that receives flow sampling data.

By default, no target sFlow collector is specified.

Format

sflow flow-sampling collector { *collector-id* | **all** }

undo sflow flow-sampling collector { *collector-id* | **all** }

Parameters

Parameter	Description	Value
collector-id	Specifies the ID of the target sFlow collector that receives flow sampling data.	The value is an integer that can be 1 or 2.
all	Indicates all the configured sFlow collectors.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

An sFlow agent samples packets in a direction of an interface based on a sampling rate, analyzes packets, encapsulates sampled packets and analysis result into sFlow packets, and then sends the sFlow packets to an sFlow collector. When multiple sFlow collectors are configured, you can run the **sflow flow-sampling collector** command to specify one or two to receive sFlow packets. Each interface can send sFlow sampling packets to a maximum of two collectors.

When you run the **sflow flow-sampling collector** command to specify the first target sFlow collector on an interface, flow sampling is enabled on the interface. When you run the **undo sflow flow-sampling collector** command to delete the last target sFlow collector on an interface, flow sampling is disabled on the interface.

Prerequisites

An sFlow collector has been created using the **sflow collector** command.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces.

Example

Specify sFlow collector 1 to receive the flow sampling data.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling collector 1
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and specify sFlow collector 1 to receive flow sampling data for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling collector 1
```

16.12.10 sflow flow-sampling max-header

Function

The **sflow flow-sampling max-header** command sets the maximum bytes of data that can be copied from a sampled packet in flow sampling.

The **undo sflow flow-sampling max-header** command restores the default maximum bytes of data.

By default, a maximum of 64 bytes of data can be copied from a sampled packet in flow sampling.

Format

sflow flow-sampling max-header *length*

undo sflow flow-sampling max-header

Parameters

Parameter	Description	Value
length	Specifies the maximum bytes of data that can be copied from a sampled packet.	The unit is byte. The value is an integer that ranges from 18 to 512. The default value is 64.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

An sFlow agent samples packets in a direction of an interface based on a sampling rate, analyzes packets, encapsulates sampled packets and analysis result into sFlow packets, and then sends the sFlow packets to an sFlow collector. The datagram size of sFlow packets is set using the **sflow collector** [**datagram-size** *datagram-size*] command. If only the information carried in the packet header is required, run the **sflow flow-sampling max-header** command to set the maximum length of data starting from the original packet header that can be copied from a sampled packet.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces.

Example

Set the maximum length of data starting from the original packet header that can be copied from a sampled packet to 256 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling max-header 256
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and set the maximum length of data starting from the original packet header that can be copied from a sampled packet to 256 bytes for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling max-header 256
```

16.12.11 sflow flow-sampling rate

Function

The **sflow flow-sampling rate** command sets the sampling rate on an interface.

The **undo sflow flow-sampling rate** command restores the default sampling rate on an interface.

By default, the sampling rate on a 40GE interface is 1/20480 and on other types of interfaces is 1/2048.

Format

sflow flow-sampling rate *rate*

undo sflow flow-sampling rate

Parameters

Parameter	Description	Value
rate *rate*	Specifies the sampling rate in the format of 1/*rate*. *rate* specifies the number of packets out of which the interface will sample a packet.	The *rate* is an integer that ranges from 256 to 65535 on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, and ranges from 256 to 1048576 on other devices.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

An sFlow agent samples packets in a direction of an interface based on a sampling rate, analyzes packets, encapsulates sampled packets and analysis result into sFlow packets, and then sends the sFlow packets to an sFlow collector. You can run the **sflow flow-sampling rate** command to set the sampling rate to limit the number of sampled packets.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces. If you run the **sflow flow-sampling rate** command multiple times, only the latest configuration takes effect.

Example

Set the sampling rate to 1/3072.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling rate 3072
```

Configure a port group **pg1** that has member ports of GE0/0/2 and GE0/0/3, and set the sampling rate to 1/3072 for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
```

```
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling rate 3072
```

16.13 Ping and Tracert Configuration Commands

16.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.13.2 ping

Function

The **ping** command checks whether a specified IPv4 address is reachable and exports corresponding statistics.

Format

ping [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | { **-f** | **ignore-mtu** } | **-h** *ttl-value* | **-nexthop** *nexthop-ip-address* | **-i** *interface-type interface-number* | **-m** *time* | **-n** | **-name** | **-p** *pattern* | **-q** | **-r** | { **-s** *packetsize* | **-range** [**min** *min-size* | **max** *max-size* | **step** *step-size*] * } | **-system-time** | **-t** *timeout* | **-tos** *tos-value* | **-v** | **-vpn-instance** *vpn-instance-name*] * *host* [**ip-forwarding**]

Parameters

Parameter	Description	Value
ip	Indicates the IPv4 protocol. If **ip** is not specified, the IPv4 protocol is used.	-
-a *source-ip-address*	Specifies the source IP address of the ICMP Echo Request message. If the source IP address is not specified, the IP address of the outbound interface is used as the source IP address of the ICMP Echo Request message.	The value is in dotted decimal notation.

Parameter	Description	Value
-c *count*	Specifies the number of times for sending ICMP Echo Request messages. The **ping** command labels each ICMP Echo Request message with a sequence ID that starts from 1 and is increased by 1. By default, five ICMP Echo Request messages are sent. You can set the number of ICMP Echo Request messages to send by specifying the parameter *count*, that is, performing a Ping test with multiple Ping packets. In the case of poor network quality, you can set this parameter to a comparatively large value to check the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-d	Indicates that the socket works in debug mode.	By default, the socket works in non-debug mode.
-f	Indicates that packets are not fragmented during transmission. **NOTE** After this parameter is specified, ICMP packets are not fragmented. If the ICMP packet size exceeds the link MTU, the ICMP packet is discarded. If you do not want ICMP packets to be discarded, do not specify this parameter or increase the link MTU.	-
-h *ttl-value*	Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 device that the message reaches sends an ICMP timeout message to the source host, indicating that the destination host is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 255.

Parameter	Description	Value
-nexthop *nexthop-ip-address*	Specifies an IP address for the next hop. If you have specified this parameter, the device no longer searches the routing table before sending ICMP Echo Response packets. This process prevents ping failures caused by incorrect routing entries. **NOTE** The specified next hop address must be the next hop address of a directly connected physical interface. When you specify a next hop address, you can configure **-i** *interface-type interface-number* to specify an outbound interface. The following conditions must be met to ensure a test success: the specified next hop address must match the outbound interface; the specified outbound interface cannot be a logical interface's member interface. If you have specified a next hop address, you cannot specify a VPN.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the outbound interface for sending ICMP Echo Request packets. **NOTE** In load balancing scenarios, if an interface is specified to send ICMP Echo Request packets, all packets are sent from the interface and load balancing is not performed. The interface specified to send ICMP Echo Request packets must be a Layer 3 interface, such as a VLANIF interface.	-

Parameter	Description	Value
-m *time*	Specifies the time to wait before sending the next ICMP Echo Request message. Each time the source sends an ICMP Echo Request message using the **ping** command, the source waits a period of time (500 ms by default) before sending the next ICMP Echo Request message. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 500, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 500.
-n	Uses the value of *host* as the IP address to spare domain name resolution.	-
-name	Displays the name of the destination host.	-
-p *pattern*	Specifies pad characters for ICMP Echo Request messages. By configuring pad characters for ICMP Echo Request messages, you can identify a specific message among the large number of received ICMP Echo Reply messages.	The value is a hexadecimal integer that ranges from 0 to FFFFFFFF. By default, the padding starts from 0x01, and continues in ascending order.
-q	Displays only the statistics. If the **ping** command carries this parameter, the system displays only the statistics information such as the number of sent and received packets, packet loss rate, and minimum, average, and maximum RTTs of the packet.	By default, the system displays all statistics information.

Parameter	Description	Value
-r	Records the route along which an IP packet is forwarded. When **-r** is specified, during the transmission of an IP packet, the IP address of each Layer 3 device that the IP packet passes through is added to the Options field. When the IP packet reaches the destination, all IP addresses recorded in the Options field are copied to the ICMP Echo Reply message. In addition, the IP address of each Layer 3 device that the returned IP packet passes through is added to the message. When the ping program receives the ICMP Echo Reply message, IP addresses of the passed Layer 3 devices are displayed.	By default, the route along which an IP packet is forwarded is not recorded.
-s *packetsize*	Specifies the length of an ICMP Echo Request message, excluding the IP header and ICMP header, that is, performing a Ping test with large-sized Ping packets.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.

Parameter	Description	Value
-range	Enables the device to send ICMP Echo Request messages with variable payload lengths. **NOTE** The command execution takes a long period if a large number of ICMP Echo Request messages need to be sent. If you want to terminate the command execution, press **Ctrl+C**. To change the number of ICMP Echo Request messages to be sent, change the values of **min** *min-size* and **max** *max-size*. The value of **min** *min-size* must be smaller than that of **max** *max-size*. If both the **-range** and **-c** *count* parameters are specified, the device sends ICMP Echo Request messages of the same payload length for the number of times specified by the **-c** *count* parameter.	• If the **-range** parameter is not specified, the payload length of an ICMP Echo Request message is equal to the length specified by the **-s** *packetsize* parameter. The default value is 56, in bytes. • If the **-range** parameter is specified, the payload length of the first ICMP Echo Request message is **min** *min-size*, and that of the second ICMP Echo Request message is **min** *min-size* plus **step** *step-size*. The payload length increases incrementally by **step** *step-size* for subsequent ICMP Echo Request messages until **max** *max-size* is reached. After that, the device will not send ICMP Echo Request messages any more. By default, the payload length of an ICMP Echo Request message ranges from 56 to 9600 bytes, and the step length is 1 byte.
min *min-size*	Specifies the minimum payload length of an ICMP Echo Request message.	The value is an integer ranging from 20 to 9600, in bytes. The default value is 56.
max *max-size*	Specifies the maximum payload length of an ICMP Echo Request message.	The value is an integer ranging from 20 to 9600, in bytes. The default value is 9600.

Parameter	Description	Value
step *step-size*	Specifies the step length of an ICMP Echo Request message.	The value is an integer ranging from 1 to 1000, in bytes. The default value is 1.
-system-time	Displays the system time when the ping packet is sent.	-
-t *timeout*	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent. After the **ping** command is run, the source sends an ICMP Echo Request message to a destination and waits for an ICMP Echo Reply message. If the destination, after receiving the ICMP Echo Request message, returns an ICMP Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMP Echo Reply message within the specified period, the source displays that the message times out. Normally, the source receives an ICMP Echo Reply message within 1 to 10 seconds after sending an ICMP Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000. The minimum timeout period is 200 ms. If the specified timeout period is less than 200 ms, the device uses 200 ms as the timeout period.
-tos *tos-value*	Specifies the ToS value of the sent ICMP Echo Request messages. The ToS value is used to set the packet priority.	The value is an integer that ranges from 0 to 255. The default value is 0.
-v	● If **-v** is not specified, the system displays only the ICMP Echo Reply messages received by the local user. ● If **-v** is specified, the system displays all received ICMP Echo Reply messages.	-

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ignore-mtu	Indicates that the system does not check the interface MTU when a packet is sent.	-
host	Specifies the domain name or IP address of the destination host.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation.
ip-forwarding	Indicates that the ping packets are forcibly forwarded through IP on the first node.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping** command is a common debugging tool for testing the network connectivity by transmitting ICMP Echo messages. It can detect the following items:

- Availability of the remote device
- Round-trip delay in communication between the local and remote devices
- Packet loss rate

You can run the **ping** command to check the network connectivity or line quality in the following scenarios:

- Scenario 1: Check the protocol stack on the local device. You can run the **ping** *loopback-address* command to check whether the TCP/IP protocol stack works properly on the local device.

- Scenario 2: Check whether the destination host is reachable on an IP network. You can run the **ping** *host* command to send an ICMP Echo Request message to the destination host. If a reply is received, the destination host is reachable.
- Scenario 3: In the case of an unstable network, you can run the **ping -c** *count* **-t** *timeout host* command to check the quality of the network between the local device and the peer. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.
- Scenario 4: Check the path. You can run the **ping -r** *host* command to obtain information about nodes along the path from the local device to the peer.
- Scenario 5: Check the path MTU. You can run the **ping -f -s** *packetsize host* command to prevent ICMP message fragmentation and set the length of an ICMP message so as to obtain the path MTU through multiple probes.
- Scenario 6: Check whether the peer is reachable on a Layer 3 VPN. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **ping** *host* command to check whether the peer is reachable. When a VPN instance name is specified, you can run the **ping -vpn-instance** *vpn-instance-name host* command to send an ICMP Echo Request message to the peer. If the peer returns an ICMP Echo Reply message, the peer is reachable.

Prerequisite

- Before running the **ping** command, ensure that the ICMP module is working properly.
- If **-vpn-instance** is specified, ensure that the VPN module is working properly.

Precautions

- If an intermediate device is disabled from responding to ICMP messages, detection on this node fails.
- If a fault occurs in the ping process, you can press **Ctrl+C** to terminate the ping operation.
- To ensure security, do not **ping** the broadcast address, such as XX.XX.XX.255.
- When the destination host is unreachable, the system displays "Request time out", which indicates that the ICMP Echo Request message times out.
- The **ping** command is typically used to check network connectivity and link quality, and cannot be used to evaluate the forwarding latency of a switch. If the pinged IP address is not the local switch's, the switch forwards the ICMP packet according to routing entries, without sending them to the CPU. If the pinged IP address is the local switch's, the switch sends the ICMP packets to the CPU for processing. In this case, you can run the **icmp-reply fast** command on the switch to enable the fast ICMP reply function. With this function, the switch directly processes the ICMP packets destined for its own IP address on interfaces, without sending the packets to the CPU. This minimizes the ping latency.
- When the ping command is used, packet statistics are collected only in the outbound direction of interfaces on the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S.

Example

Check whether the host at 10.1.1.2 is reachable.

```
<HUAWEI> ping 10.1.1.2
  PING 10.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 10.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Check whether the host at 10.1.1.4 is reachable, set the transmission count to 8, and set the period for waiting for an ICMP Echo Reply message to 4000 ms.

```
<HUAWEI> ping -c 8 -t 4000 10.1.1.4
  PING 10.1.1.4: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.4: bytes=56 Sequence=1 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=2 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=3 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=4 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=5 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=6 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=7 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=8 ttl=255 time=32 ms
  --- 10.1.1.4 ping statistics ---
    8 packet(s) transmitted
    8 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 32/32/32 ms
```

Enable the device to send ICMP Echo Request messages with variable payload lengths.

```
<HUAWEI> ping -range min 56 max 60 192.168.1.9
  PING 192.168.1.9: 56-60  data bytes, press CTRL_C to break
    Reply from 192.168.1.9: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 192.168.1.9: bytes=57 Sequence=2 ttl=255 time=60 ms
    Reply from 192.168.1.9: bytes=58 Sequence=3 ttl=255 time=80 ms
    Reply from 192.168.1.9: bytes=59 Sequence=4 ttl=255 time=80 ms
    Reply from 192.168.1.9: bytes=60 Sequence=5 ttl=255 time=50 ms

  --- 192.168.1.9 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/70/80 ms
```

Check whether the host at 10.1.1.10 is reachable.

```
<HUAWEI> ping 10.1.1.10
ping 10.1.1.10
  PING 10.1.1.10: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.10: bytes=56 Sequence=1 ttl=128 time=1 ms
    Reply from 10.1.1.10: bytes=56 Sequence=1 ttl=64 time=1 ms (DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=2 ttl=128 time=1
ms
    Reply from 10.1.1.10: bytes=56 Sequence=2 ttl=64 time=1 ms
(DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=3 ttl=128 time=1 ms
    Reply from 10.1.1.10: bytes=56 Sequence=3 ttl=64 time=1 ms (DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=4 ttl=128 time=1
ms
    Reply from 10.1.1.10: bytes=56 Sequence=4 ttl=64 time=1 ms
```

```
(DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=5 ttl=128 time=1
ms

  --- 10.1.1.10 ping statistics ---
    5 packet(s) transmitted
    9 packet(s) received
    4 duplicates
    -- somebody's printing up packets
    round-trip min/avg/max = 1/0/1 ms
```

Table 16-81 Description of the ping command output

Item	Description
PING x.x.x.x	Reachability of the destination host with the IP address as *x.x.x.x* is tested.
x data bytes	Length of a sent ICMP Echo Request message.
press CTRL_C to break	The ongoing ping test is terminated after you press **Ctrl+C**.
Reply from x.x.x.x	The destination host responds to the ICMP Echo Request message with an ICMP Echo Reply message that contains the following items: ● bytes: indicates the length of the ICMP Echo Reply message. ● Sequence: indicates the sequence number of the ICMP Echo Reply message. ● ttl: indicate the TTL value of the ICMP Echo Reply message. ● time: indicates the RTT, in milliseconds. If no ICMP Echo Reply message is received after the timeout period, the system displays "Request time out". **NOTE** If a received packet ends with (DUP!), the device has received the Echo Reply messages with repeated sequence number.

Item	Description
x.x.x.x ping statistics	Statistics collected after the ping test on the destination host. The statistics include the following information: ● packet(s) transmitted: indicates the number of sent ICMP Echo Request messages. ● packet(s) received: indicates the number of received ICMP Echo Reply messages. ● duplicates: indicates that the device has received the Echo Reply messages with repeated sequence number. ● % packet loss: indicates the percentage of unresponded messages to total sent messages. ● -- somebody's printing up packets: indicates that the number of received Echo Reply messages is larger than the number of send Echo Request messages. ● round-trip min/avg/max: indicates the minimum, average, and maximum RTTs. The unit is ms. (On an IPv4 network, round-trip min/avg/max is not displayed if the ping fails. On an IPv6 network, round-trip min/avg/max = 0/0/0 ms is displayed if the ping fails.)

16.13.3 ping ipv6

Function

The **ping ipv6** command checks whether a specified IPv6 address is reachable and exports corresponding statistics.

Format

ping ipv6 [**-a** *source-ipv6-address* | **-c** *count* | **-h** *ttl-value* | **-m** *time* | **-name** | **-s** *packetsize* | **-t** *timeout* | **-tc** *traffic-class-value* | **vpn-instance** *vpn-instance-name*] * *host* [**-i** *interface-type interface-number*]

Parameters

Parameter	Description	Value
-a *source-ipv6-address*	Specifies a source IPv6 address for sending ICMPv6 Echo Request messages. If no source IPv6 address is specified, the IPv6 address of the outbound interface is used as the source address for sending ICMPv6 Echo Request messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
-c *count*	Specifies the number of times for sending ICMPv6 Echo Request messages. You can increase the number of outgoing packets to detect the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-h *ttl-value*	Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 switch that the message reaches sends an ICMPv6 timeout message to the source host, indicating that the destination host is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 255.
-m *time*	Specifies the time to wait before sending the next ICMPv6 Echo Request message. Each time the source sends an ICMPv6 Echo Request message using the **ping ipv6** command, the source waits a period of time (2000 ms by default) before sending the next ICMPv6 Echo Request message. You can set the time to wait before sending the next ICMPv6 Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.

Parameter	Description	Value
-name	Displays the name of the destination host.	-
-s *packetsize*	Specifies the length of an ICMPv6 Echo Request message, excluding the IP header and ICMPv6 header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-t *timeout*	Specifies the timeout period to wait for an ICMPv6 Echo Reply message after an ICMPv6 Echo Request message is sent. After the **ping ipv6** command is run, the source sends an ICMPv6 Echo Request message to a destination and waits for an ICMPv6 Echo Reply message. If the destination, after receiving the ICMPv6 Echo Request message, returns an ICMPv6 Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMPv6 Echo Reply message within the specified period, the source displays that the message times out. Normally, the source receives an ICMPv6 Echo Reply message within 1 to 10 seconds after sending an ICMPv6 Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000. The minimum timeout period is 200 ms. If the specified timeout period is less than 200 ms, the device uses 200 ms as the timeout period.
-tc *traffic-class-value*	Specifies the traffic classification in the ICMPv6 Echo Request message. To configure traffic control for ICMPv6 packets, set the parameter *traffic-class-value*.	The value is an integer that ranges from 0 to 255. The default value is 0.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance for the IPv6 address family.	The value must be an existing VPN instance name.

Parameter	Description	Value
host	Specifies the host name or IPv6 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The IPv6 address is a 32–bit string in hexadecimal format, namely, the format X:X:X:X:X:X:X:X.
-i *interface-type interface-number*	Specifies the outbound interface for sending ICMPv6 Echo Request messages.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping ipv6** command is a widely used debugging tool for checking network connectivity and host reachability on an IPv6 network by transmitting ICMPv6 messages. It can detect the following items:

- Availability of the remote device
- Round-trip delay in communication between the local and remote devices
- Packet loss rate

You can run the **ping ipv6** command to check the IPv6 network connectivity or line quality in the following scenarios:

- Check the protocol stack on the local device. You can run the **ping ipv6** *IPv6-loopback-address* command to check whether the TCP/IP protocol stack works properly on the local device.
- Check whether the destination IPv6 host is reachable on an IPv6 network. You can run the **ping ipv6** *host* command to send an ICMPv6 Echo Request message to the destination host. If a reply is received, the destination host is reachable.
- Check whether the peer is reachable on a Layer 3 VPN. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **ping ipv6** *host* command to check whether the peer is reachable. When a VPN instance name is specified, you can run the **ping ipv6**

vpn-instance *vpn-instance-name host* command to send an ICMPv6 Echo Request message to the peer. If the peer returns an ICMPv6 Echo Reply message, the peer is reachable.

- In the case of an unstable network, you can run the **ping ipv6 -c** *count* **-t** *timeout host* command to check the quality of the network between the local device and the peer. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.

Prerequisites

- Before running the **ping ipv6** command, ensure that the ICMPv6 module is working properly.
- If **-vpn-instance** is specified, ensure that the VPN module is working properly.

Precautions

- If an intermediate device is disabled from responding to ICMPv6 messages, detection on this node fails.
- If the IPv6 address of the destination host maps the local address, specify the name of the local outbound interface through which the ICMPv6 Echo Request message is sent. Otherwise, reply to the **ping ipv6** command times out.
- When the destination host is unreachable, the system displays "Request time out" indicating that the ICMPv6 Echo Request message times out and displays statistics collected by the IPv6 ping test.
- If a fault occurs in the IPv6 ping process, you can press **Ctrl+C** to terminate the IPv6 ping operation.

Example

Check whether the host with the IPv6 address as FC00::1 is reachable.

```
<HUAWEI> ping ipv6 FC00::1
 PING FC00::1 : 56  data bytes, press CTRL_C to break
    Reply from FC00::1
    bytes=56 Sequence=1 hop limit=64 time=115 ms
    Reply from FC00::1
    bytes=56 Sequence=2 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=3 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=4 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=5 hop limit=64 time=1 ms
  ---FC00::1 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max=1/23/115 ms
```

Table 16-82 Description of the ping ipv6 command output

Item	Description
PING HH:HH::HH:H	IPv6 address of the destination host.

Item	Description
x data bytes	Length of a sent ICMPv6 Echo Request message.
press CTRL_C to break	The ongoing IPv6 ping test is terminated after you press **Ctrl+C**.
Reply from HH:HH::HH:H	The destination host responds to the ICMPv6 Echo Request message with an ICMPv6 Echo Reply message that contains the following items: ● bytes: indicates the length of the ICMPv6 Echo Reply message. ● sequence: indicates the sequence number of the ICMPv6 Echo Reply message. ● hop limit: indicates the TTL of the ICMPv6 Echo Reply message. ● time: indicates the RTT, in milliseconds. If no ICMPv6 Echo Reply message is received after the timeout period, the system displays "Request time out".
HH:HH::HH:H ping statistics	Statistics collected after the IPv6 ping test on the destination host. The statistics include the following information: ● packet(s) transmitted: indicates the number of sent ICMPv6 Echo Request messages. ● packet(s) received: indicates the number of received ICMPv6 Echo Reply messages. ● % packet loss: indicates the percentage of unresponded messages to total sent messages. ● round-trip min/avg/max: indicates the minimum, average, and maximum RTTs.

16.13.4 tracert

Function

The **tracert** command checks the path of packets from the source to the destination, checks network connectivity, and locates a network fault.

Format

tracert [**-a** *source-ip-address* | **-f** *first-ttl* | **-m** *max-ttl* | **-name** | **-p** *port* | **-q** *nqueries* | **-v** | **-vpn-instance** *vpn-instance-name* [**pipe**] | **-w** *timeout* | **-s** *packetsize*] * *host*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **-v**.

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source address of a probe packet. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address for sending tracert packets.	The value is in dotted decimal notation.
-f *first-ttl*	Specifies the initial TTL. The TTL field is carried in the IP header. It indicates the lifetime of packets and specifies the maximum hops that packets can pass through. The TTL value is set on the source and reduced by 1 each time the packet passes through a hop. When the TTL value is reduced to 0, the packet is discarded. At the same time, an ICMP Timeout message is sent to notify the source host. If *first-ttl* is specified and the number of hops is smaller than the value of *first-ttl*, no ICMP Timeout packet is sent to the source host when the packet passes through these hops. If *max-ttl* is specified, the value of *first-ttl* must be smaller than the value of *max-ttl*.	The value is an integer that ranges from 1 to 255. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL. Usually, the maximum TTL is set to the number of hops the packet passes through. You need to use this parameter to change the TTL. If *first-ttl* is specified, the value of *max-ttl* must be greater than the value of *first-ttl*.	The value is an integer that ranges from 1 to 255. The default value is 30.
-name	Displays the host name of each hop.	-
-p *port*	Specifies the UDP port number of the destination. Before specifying the UDP port number of the destination, ensure that the port is not in use; otherwise, the tracert fails.	The value is an integer that ranges from 0 to 65535. The default value is 33434.

Parameter	Description	Value
-q *nqueries*	Specifies the number of probe packets to be sent each time. In the case of poor network quality, you can set this parameter to a comparatively large value to ensure that the probe packet can reach the destination.	The value is an integer that ranges from 1 to 65535. The default value is 3.
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet.	By default, the MPLS label carried in the ICMP Time Exceeded is not displayed. Instead, only the path information carried in the ICMP Time Exceeded and Port-Unreachable packets is displayed.
-vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the destination address belongs.	The value must be an existing VPN instance name.
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire MPLS domain is considered as one hop and the IP TTL of the probe packet is reduced by one on the ingress node and egress node respectively.	-
-w *timeout*	Specifies the timeout period to wait for a reply. If a tracert packet times out when reaching a gateway, an asterisk (*) is displayed. In the case of poor network quality and a low network transmission rate, you are advised to prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5000.
-s *packetsize*	Specifies the UDP payload of packets to be sent in the **tracert** command.	The value is an integer that ranges from 12 to 9600, in bytes. The default value is 12.

Parameter	Description	Value
host	Indicates the domain name or IPv4 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

During routine system maintenance, you can run the **ping** command to check network connectivity. If the ping fails, run the **tracert** command to locate the fault on the network.

You can specify different parameters in the **tracert** command for different scenarios:

- To check information about nodes between the source and the destination, run the **tracert** *host* command.
- To check information about nodes between the source and the destination on a Layer 3 VPN, run the **tracert -vpn-instance** *vpn-instance-name host* command. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **tracert** *host* command to check whether the peer is reachable. To check information about nodes between the source and the destination in a specified VPN instance, run the **tracert -vpn-instance** *vpn-instance-name host* command.
- On an unstable network, you can run the **tracert -q** *nqueries* **-w** *timeout host* command to check information about nodes between the source and the destination. If the network is unreliable, set the packet transmission count (**-q**) and timeout (**-w**) to the upper limits. This makes the test result accurate.
- To check information about nodes along a segment of a path, run the **tracert -f** *first-ttl* **-m** *max-ttl host* command that has initial TTL and maximum TTL specified.

Prerequisite

- The UDP module of each node is working properly; otherwise, the tracert operation fails.
- If **-vpn-instance** is specified, ensure that the VPN module of each node is working properly.
- The ICMP module of each node is working properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert** command is as follows:

1. The source sends a packet with the TTL being 1. After the TTL times out, the first hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
2. The source sends a packet with the TTL being 2. After the TTL times out, the second hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
3. The source sends a packet with the TTL being 3. After the TTL times out, the third hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
4. The preceding process proceeds until the packet reaches the destination.

When receiving an IPv4 packet, each destination hop cannot find the port specified in the packet, and returns an ICMP Port Unreachable message, indicating that the destination port is unreachable and the tracert ends. In this manner, the result of each probe is displayed on the source, according to which you can find the path from the source to the destination.

Configuration Impact

If a fault occurs when you run the **tracert** command, the following information may be displayed:

- !H: The host is unreachable.
- !N: The network is unreachable.
- !: The port is unreachable.
- !P: The protocol type is incorrect.
- !F: The packet is incorrectly fragmented.
- !S: The source route is incorrect.

Precautions

Once **-r** is specified, the outputs of both the **tracert** and **ping** commands show information about nodes between the source and the destination. Differences between the outputs of the **tracert** and **ping** commands are as follows:

- If the **ping** command times out on a transit node, a timeout packet is returned and the command output displays no path information.
- If the **tracert** command times out on a transit node, the command output displays " * * * " indicating that the tracert times out on the node but the tracert is not interrupted.

By default, each hop sends three probe packets. If load balancing is implemented, the same hop may correspond to different nodes. In this case, if the IP address in a probe packet is different from that in the previous probe packet, information in the later probe packet is displayed. If the IP address in a probe packet is the same as that in the previous probe packet, information in the previous probe packet is displayed.

Example

Tracert the gateways from the source host to the destination host with the IP address being 10.1.1.11.

```
<HUAWEI> tracert 10.1.1.11
traceroute to 10.1.1.11 (10.1.1.11), max hops: 30, packet length: 40, press CTRL_C to break
1 10.3.112.1   10 ms 10 ms 10 ms
2 10.32.216.1  19 ms 19 ms 19 ms
3 * * *
4 * * *
5 * * *
6 * * *
7 10.1.1.11   339 ms 279 ms 279 ms
```

Table 16-83 Description of the tracert command output

Item	Description
traceroute to	Tracert to a destination IP address.
max hops	Maximum TTL value.
packet length	Length of a sent packet.
1 10.3.112.1 10 ms 10 ms 10 ms	The integer 1 indicates the first hop gateway. Each hop increments the hop count. By default, the maximum hop count is 30. "10.3.112.1" is the gateway address of the first hop. The IPv4 address following the serial number of each hop is the gateway address of the hop. "10 ms 10 ms 10 ms" indicates the difference between the time when the three UDP packets are sent and when corresponding ICMP Time Exceeded or ICMP Port Unreachable messages are received. Tracert is used to test connectivity. When a switch is a hop in a tracert test, tracert packets are be sent to the CPU for processing. This causes a time difference, but it does not mean the link delay.

Item	Description
* * *	No ICMP Time Exceeded message or ICMP Port Unreachable message is returned within a specified period on the Nth hop. By default, an ICMP Time Exceeded message or ICMP Port-unreachable message should be returned within 5000 ms.

16.13.5 tracert ipv6

Function

The **tracert ipv6** command checks the path of packets from the source to the destination, checks IPv6 network connectivity, and locates a network fault.

Format

tracert ipv6 [**-f** *first-hop-limit* | **-m** *max-hop-limit* | **-p** *port-number* | **-q** *probes* | **-w** *timeout* | **vpn-instance** *vpn-instance-name* | **-a** *source-ipv6-address* | **-s** *packetsize* | **-name** | **-v**] * *host*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **-v**.

Parameters

Parameter	Description	Value
-f *first-hop-limit*	Specifies the initial hop-limit. Carried in the IPv6 header, the hop-limit (time to live) indicates the lifetime of IPv6 packets and specifies the maximum number of hops that the IPv6 packets can pass through. The hop-limit field in IPv6 packets is similar to the TTL field in the IPv4 packets. The hop-limit value is set on the source and reduced by 1 each time the packet passes through a Layer 3 device. When the hop-limit value is reduced to 0 on a Layer 3 device, the Layer 3 device discards the packet and sends an ICMPv6 Timeout message to the source. If *first-hop-limit* is specified and the number of hops is smaller than the specified value, the hop-limit value will be greater than 0 after the packet passes through all the nodes. Therefore, no ICMPv6 Timeout message is sent to the source. If *max-hop-limit* is specified, the value of *first-hop-limit* must be smaller than the value of *max-hop-limit*.	The value is an integer that ranges from 1 to 255. The default value is 1.
-m *max-hop-limit*	Specifies the maximum hop-limit. Usually, the maximum hop-limit is set to the number of hops that a packet passes through. To change the hop-limit value, you need to use this parameter. If *first-hop-limit* is specified, the value of *max-hop-limit* must be greater than the value of *first-hop-limit*.	The value is an integer that ranges from 1 to 255. The default value is 30.

Parameter	Description	Value
-p *port-number*	Specifies the UDP port number of the destination. - If no UDP port number is specified for the destination, when you run the **tracert ipv6** command, a port with the port number greater than 32768 is randomly chosen for the destination to receive tracert packets. - Before specifying the UDP port number for the destination, ensure that the port is not in use; otherwise, the tracert fails.	The value is an integer that ranges from 1 to 65535. The default value is 33434.
-q *probes*	Specifies the number of tracert packets sent each time. In the case of poor network quality, you can set *probes* to a comparatively large value to ensure that tracert packets can reach the destination.	The value is an integer that ranges from 1 to 65535. The default value is 3.
-w *timeout*	Sets the timeout period to wait for a reply. If a tracert packet times out when reaching a gateway, an asterisk (*) is displayed. In the case of poor network quality and a low network transmission rate, you are advised to prolong the timeout period.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 5000.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance for the IPv6 address family.	The value must be an existing VPN instance name.
-a *source-ipv6-address*	Specifies the source address of a tracert packet. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address for sending tracert packets.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
-s *packetsize*	Specifies the size of IPv6 probe packets in the **tracert ipv6** command.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-name	Displays the name of the destination host.	-
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet.	By default, the MPLS label carried in the ICMP Time Exceeded is not displayed. Instead, only the path information carried in the ICMP Time Exceeded and Port-Unreachable packets is displayed.
host	Specifies the host name or IPv6 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The IPv6 address is a 32–bit string in hexadecimal format, namely, the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When a fault occurs on the network and the peer is an IPv6 device, you can run the **ping ipv6** command to check network connectivity based on the reply message, and then run the **tracert ipv6** command to locate the fault.

You can specify different parameters in the **tracert ipv6** command for different scenarios:

- To check information about nodes between the source and the IPv6 destination, run the **tracert ipv6** *host* command.

- To check information about nodes between the source and the IPv6 destination on a Layer 3 VPN, run the **tracert ipv6 vpn-instance** *vpn-instance-name host* command. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **tracert ipv6** *host* command to check whether the peer is reachable. To check information about nodes between the source and the IPv6 destination in a specified VPN instance, run the **tracert ipv6 vpn-instance** *vpn-instance-name host* command.
- On an unstable network, you can run the **tracert ipv6 -q** *probes* **-w** *timeout host* command to check information about nodes between the source and the IPv6 destination. If the network is unreliable, set the packet transmission count (**-q**) and timeout (**-w**) to the upper limits. This makes the test result accurate.
- To check information about nodes along a segment of a path, run the **tracert ipv6 -f** *first-hop-limit* **-m** *max-hop-limit host* command that has initial hop-limit and maximum hop-limit specified.

Prerequisites

- The UDP module of each node is working properly; otherwise, the IPv6 tracert operation fails.
- The VPN module of each node is working properly if **vpn-instance** is specified.
- The ICMPv6 module of each node is working properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert ipv6** command is as follows:

- The source sends a packet with the hop-limit being 1. After the hop-limit times out, the first hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The source sends a packet with the hop-limit being 2. After the hop-limit times out, the second hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The source sends a packet with the hop-limit being 3. After the hop-limit times out, the third hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The preceding process proceeds until the packet reaches the destination.

When receiving an IPv6 packet, each destination hop cannot find the port specified in the IPv6 packet, and therefore returns an ICMPv6 Port Unreachable message, indicating that the destination port is unreachable and the IPv6 tracert ends. In this manner, the result of each probe is displayed on the source, according to which you can find the path from the source to the destination.

Configuration Impact

If a fault occurs when you run the **tracert ipv6** command, the following information may be displayed:

- !H: The host is unreachable.
- !N: The network is unreachable.

- !: The port is unreachable.
- !P: The protocol type is incorrect.
- !F: The packet is incorrectly fragmented.
- !S: The source route is incorrect.

Precautions

By default, the ICMPv6 module is automatically enabled after you enable the IPv6 module.

Example

Set the number of packets to be sent to 5 and timeout period to 8000 ms, and tracert the gateways from the source to the destination at FC00::3.

```
<HUAWEI> tracert ipv6 -q 5 -w 8000 FC00::3
traceroute to FC00::3 30 hops max,60 bytes packet
1 FC00:1::3 26 ms 23 ms 26 ms 30 ms 29 ms
2 FC00::3 3020 ms 3024 ms 4040 ms 6820 ms 5584 ms
```

Table 16-84 Description of the tracert ipv6 command output

Item	Description
traceroute to HH:HH::HH:H	IPv6 address of the destination host.
x hops max	Maximum hop-limit value.
x bytes packet	Length of a tracert packet.
1 2	Sequence number of the received ICMPv6 Echo Reply message.
HH:HH::HH:H	Address of the IPCMPv6 Echo Reply message.
26 ms 23 ms 26 ms 30 ms 29 ms	RTT, in milliseconds.

16.14 TWAMP Light Configuration Commands

16.14.1 Command Support

Only the following switch models support TWAMP Light, and only TWAMP Light Responder function is supported:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S

16.14.2 display twamp-light responder test-session

Function

The **display twamp-light responder test-session** command displays real-time measurement session information on the TWAMP Light Responder.

Format

display twamp-light responder test-session [**verbose** | *session-id*]

Parameters

Parameter	Description	Value
verbose	Displays details about all measurement sessions on the TWAMP Light Responder.	-
session-id	Displays details about the specified measurement session on the TWAMP Light Responder.	The value is an integer that ranges from 1 to 5.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the performance measurement function is enabled, you can run this command to view measurement session information on the TWAMP Light Responder if you want to check the measurement session configuration or locate the fault in measurement.

Example

Display the summary of all measurement sessions.

```
<HUAWEI> display twamp-light responder test-session
Total number  : 2
-------------------------------------------------------------------------------
  ID    Local-IP       Local-Port     Remote-IP       Remote-Port
-------------------------------------------------------------------------------
   1    10.1.1.2           10000     10.2.2.2            20000
   2    10.1.1.3           10001     10.2.2.3            20001
```

Display details about all measurement sessions.

```
<HUAWEI> display twamp-light responder test-session verbose
Session ID                    : 1
Local IP                      : 10.1.1.2
Local Port                    : 10000
Remote IP                     : 10.2.2.2
```

```
Remote Port                : 20000
Mode                       : unauthenticated
VPN Instance               : test
Description                : -

Session ID                 : 2
Local IP                   : 10.1.1.3
Local Port                 : 10001
Remote IP                  : 10.2.2.3
Remote Port                : 20001
Mode                       : unauthenticated
VPN Instance               : shuai
Description                : -
```

Display details about the specified measurement session.

```
<HUAWEI> display twamp-light responder test-session 1
Session ID                 : 1
Local IP                   : 10.1.1.2
Local Port                 : 10000
Remote IP                  : 10.2.2.2
Remote Port                : 20000
Mode                       : unauthenticated
VPN Instance               : test
Description                : -
```

Table 16-85 Description of the **display twamp-light responder test-session** command output

Item	Description
Total number	Total number of sessions.
ID/Session ID	Session ID.
Local-IP/Local IP	IP address of the session Responder.
Local-Port/Local Port	UDP port number of the session Responder.
Remote-IP/Remote IP	IP address of the session Sender.
Remote-Port/Remote Port	UDP port number of the session Sender.
Mode	Authentication mode. The value **unauthenticated** indicates that authentication is disabled.
VPN Instance	VPN instance name. If the VPN instance name is not specified, the value of this field is empty.
Description	Session description.

16.14.3 nqa twamp-light

Function

The **nqa twamp-light** command creates the TWAMP Light service and displays the TWAMP-Light view. If the TWAMP-Light service already exists, the TWAMP-Light view is directly displayed.

The **undo nqa twamp-light** command deletes the TWAMP Light service.

By default, the TWAMP Light service is not configured.

Format

nqa twamp-light

undo nqa twamp-light

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using a simple structure of TWAMP, TWAMP Light lowers the requirements on the Responder. TWAMP Light measures bidirectional network performance between any nodes on the network. When the TWAMP Light service is required, run the **nqa twamp-light** command to create the TWAMP Light service.

Precautions

After you run the **undo nqa twamp-light** command, the device automatically deletes all TWAMP Light roles, sessions, and measurement services.

Example

Create the TWAMP Light service.

```
<HUAWEI> system-view
[HUAWEI] nqa twamp-light
[HUAWEI-twamp-light]
```

16.14.4 responder

Function

The **responder** command enables the TWAMP Light Responder function and displays the TWAMP-Light-Responder view. If the Responder function has been enabled, the TWAMP-Light-Responder view is directly displayed.

The **undo responder** command disables the TWAMP Light Responder function.

By default, the TWAMP Light Responder function is disabled.

Format

responder

undo responder

Parameters

None

Views

TWAMP-Light view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, run the **Responder** command on the Responder to display the TWAMP-Light-Responder view and create a measurement session. Then the Controller starts the measurement service based on the session configuration.

Precautions

After the TWAMP Light Responder is deleted, the packet loss rate is displayed as 100%, which is inaccurate.

Example

Enable the TWAMP Light Responder function.

```
<HUAWEI> system-view
[HUAWEI] nqa twamp-light
[HUAWEI-twamp-light] responder
[HUAWEI-twamp-light-responder]
```

16.14.5 test-session (TWAMP-Light-Responder view)

Function

The **test-session** command creates a TWAMP Light measurement session on the Responder.

The **undo test-session** command deletes a TWAMP Light measurement session on the Responder.

By default, no TWAMP Light measurement session is created on the Responder.

Format

test-session *session-id* **local-ip** *local-ip-address* **remote-ip** *remote-ip-address* **local-port** *local-port* **remote-port** *remote-port* [**vpn-instance** *vpn-instance-name*] [**description** *description*]

undo test-session *session-id* [**local-ip** *local-ip-address* **remote-ip** *remote-ip-address* **local-port** *local-port* **remote-port** *remote-port* [**vpn-instance** *vpn-instance-name*] [**description** *description*]]

Parameters

Parameter	Description	Value
session-id	Specifies the ID of the measurement session.	The value is an integer that ranges from 1 to 5.
local-ip *local-ip-address*	Specifies the IP address of the Responder.	The value is in dotted decimal notation.
remote-ip *remote-ip-address*	Specifies the IP address of the Sender.	The value is in dotted decimal notation.
local-port *local-port*	Specifies the UDP port number of the Responder.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
remote-port *remote-port*	Specifies the UDP port number of the Sender.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.
description *description*	Indicates the description of the specified measurement session. To configure description for a measurement session, specify the **description** parameter. The description facilitates session management and operation.	The value is a string of 3 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

TWAMP-Light-Responder view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the TWAMP Light service is created, you need to create a TWAMP Light measurement session on the Responder and configure measurement instance information, including the Sender's IP address, Responder's IP address, Sender's UDP port number, Responder's UDP port number, and VPN instance name.

Precautions

- A maximum of 5 measurement sessions can be created on a Responder.
- The created session starts measurement only when the measurement starts on the Controller.
- After a session is created, its parameters cannot be modified. To modify a session, delete it and create it again.
- The IP address must be a unicast address. By default, the DSCP field in a sent packet is 0 and the packet padding length is 128.
- The UDP port of the sender must be a port that is not occupied.
- The VPN instance must exist. When the VPN instance is deleted, the related measurement instance is also deleted.

Example

Create a TWAMP Light measurement session on the Responder.

```
<HUAWEI> system-view
[HUAWEI] nqa twamp-light
[HUAWEI-twamp-light] responder
[HUAWEI-twamp-light-responder] test-session 1 local-ip 192.168.10.1 remote-ip 192.168.10.2 local-port
3000 remote-port 3001
```

16.15 NETCONF Configuration Commands

16.15.1 Command Support

NETCONF Mode	Product Model
NETCONF over SSH Callhome	S200, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H

NETCONF Mode	Product Model
NETCONF over SSH	All models except S1720GW-E, S1720GWR-E, and S1720X-E

16.15.2 ap manage-mode force-tradition

Function

The **ap manage-mode force-tradition** command sets the AP management mode to the local AC mode.

The **undo ap manage-mode force-tradition** command sets the AP management mode to the same as that on the switch. That is, if the NETCONF mode is enabled on the switch, the AP is managed by iMaster NCE-Campus; if the NETCONF mode is disabled on the switch, the AP is locally managed by the switch.

By default, the AP management mode is the same as that on the switch.

Format

ap manage-mode force-tradition

undo ap manage-mode force-tradition

Parameters

None

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After NETCONF is enabled on a switch (with the native AC function enabled), Fit APs are managed by iMaster NCE-Campus by default. AP entries delivered by iMaster NCE-Campus take effect, and cloud management license resources are consumed. Additionally, the switch no longer supports the commands listed in **Table 16-86**. To locally manage APs (using local AP entries and local license resources), run the **ap manage-mode force-tradition** command to set the AP management mode to the local AC mode. Then, the commands become available on the switch.

Precautions

When a Fit AP is managed by iMaster NCE-Campus, running the **ap manage-mode force-tradition** command on the switch will disconnect the Fit AP from iMaster NCE-Campus. In this case, deleting the entry of this AP on iMaster NCE-Campus will delete the corresponding AP entry on the switch synchronously. To enable the AP to go online on the switch, you need to manually confirm the AP by running the **ap-confirm** { **all** | **mac** *ap-mac* | **sn** *ap-sn* } command on the switch.

Table 16-86 Commands that are not supported by the switch in NETCONF mode

Command	Function Description
ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** } **undo ap auth-mode**	Configures the AP authentication mode. For a switch in NETCONF mode, the AP authentication mode is SN authentication.
ap blacklist mac *ap-mac1* [**to** *ap-mac2*] **undo ap blacklist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **all** }	Adds APs to an AP blacklist, or deletes APs from an AP blacklist.
ap modify *ap-id* **mac** *ap-mac*	Modifies the MAC address of an AP.
ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] } **undo ap whitelist** { **mac** { *ap-mac1* [**to** *ap-mac2*] | **all** } | **sn** { *ap-sn1* [**to** *ap-sn2*] | **all** } }	Adds APs to an AP whitelist, or deletes APs from an AP whitelist.
ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }	Confirms unauthorized APs and allows them to go online.
ap-name *ap-name*	Configures an AP name.
ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*	Changes the name of an AP.

Example

Set the AP management mode to the local AC mode.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] ap manage-mode force-tradition
```

16.15.3 assign arp netconf number

Function

The **assign arp netconf number** command sets the number of ARP entries reserved for NETCONF.

The **undo assign arp netconf number** command restores the default setting.

By default, no ARP entry is reserved for NETCONF.

Format

assign arp netconf number *number-value*

undo assign arp netconf number

Parameters

Parameter	Description	Value
number-value	Specifies the number of ARP entries reserved for NETCONF.	The value is an integer in the range from 0 to 2000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If ARP entries are used up by due to forged packet attacks, the switch cannot communicate with the NMS. To prevent this situation, you can set the number of ARP entries reserved for NETCONF communication between the switch and NMS. When the number of remaining ARP entries on a device is less than or equal to the number of ARP entries reserved for NETCONF, only ARP entries in the NETCONF scenario can be delivered.

Precautions

- When you run the **management-vlan** command in the NETCONF view to configure a management VLAN of a switch, the switch automatically delivers the **assign arp netconf number** command to set the number of ARP entries reserved for NETCONF to 200. If you then run the **undo management-vlan** command, the switch automatically delivers the **undo assign arp netconf number** command to restore the default setting.
- When you run the **source ip** command in the NETCONF view to configure a VLANIF interface for the switch to communicate with the NMS, the switch automatically delivers the **assign arp netconf number** command to set the number of ARP entries reserved for NETCONF to 200. If you then run the **undo source ip** command, the switch automatically delivers the **undo assign arp netconf number** command to restore the default setting.
- After you run this command to manually configure the number of ARP entries reserved for NETCONF and then run the **management-vlan** or **source ip** command, the system will not automatically deliver the configuration of the

number of reserved ARP entries. If you run this command to set the number of ARP entries reserved for NETCONF to 200 and then run the **undo management-vlan** or **undo source ip** command, the switch automatically delivers the **undo assign arp netconf number** command to restore the default setting; if you run this command to set the number of ARP entries reserved for NETCONF to another value and then run the **undo management-vlan** or **undo source ip** command, the system will not deliver the **undo assign arp netconf number** command to restore the default setting.

Example

Set the number of ARP entries reserved for NETCONF to 1000.

```
<HUAWEI> system-view
[HUAWEI] assign arp netconf number 1000
```

16.15.4 backup ip address (callhome template view)

Function

The **backup ip address** command configures the IPv4 address and port number of a standby NMS that communicates with a switch through NETCONF.

The **undo backup ip** command deletes the IPv4 address and port number of a standby NMS that communicates with a switch through NETCONF.

By default, no standby NMS's IPv4 address and port number are configured for communicating with a switch through NETCONF.

Format

backup ip address *ip-address* **port** *port-number*

undo backup ip address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the standby NMS.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the standby NMS.	The value is an integer in the range from 1 to 65535.

Views

Callhome template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a disaster recovery scenario, you can run the **backup ip address** command to configure the IPv4 address and port number of the standby NMS that communicates with a switch through NETCONF. If the active NMS breaks down or is disconnected, services can be automatically switched to the standby NMS, ensuring service continuity.

Precautions

Assume that a switch has registered with one copy of iMaster NCE-Campus and gone online. If the switch needs to register with another copy of iMaster NCE-Campus, clear the switch configuration, run the **reset netconf db-configuration** command to clear database information from the switch, and restart the switch as prompted.

Example

Set the IP address and port number of the standby NMS that communicates with the switch through NETCONF to 10.1.2.1 and 830, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] callhome Test123
[HUAWEI-netconf-callhome-Test123] backup ip address 10.1.2.1 port 830
```

16.15.5 bootstrap

Function

The **bootstrap** command configures information about the primary Bootstrap server.

The **undo bootstrap** command deletes information about the primary Bootstrap server.

Format

bootstrap { **ip-address** *ip-address* | **domain** *domain* } **port** *port-number* **voucher-type** { **esn** | **ip-or-domain** } **always-trust**

undo bootstrap

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the Bootstrap server IP address, which is the southbound IP address of iMaster NCE-Campus.	The value is in dotted decimal notation.

Parameter	Description	Value
domain *domain*	Specifies the Bootstrap server domain name, which is the southbound domain name of iMaster NCE-Campus.	The value is a string of 3 to 128 characters.
port *port-number*	Specifies the port number of a Bootstrap server.	The value is an integer in the range from 1 to 65535. Currently, the value is fixed at 30217.
voucher-type esn	Specifies that the voucher type is the device ESN.	-
voucher-type ip-or-domain	Specifies that the voucher type is the Bootstrap server address.	-
always-trust	Specifies that the voucher returned by the Bootstrap server is trusted by default.	-

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switch registers with the iMaster NCE-Campus, the switch needs to obtain Lite CA information from a Bootstrap server to authenticate iMaster NCE-Campus. In this scenario, you need to run the **bootstrap** command to configure information about the Bootstrap server.

Example

Configure Bootstrap server information. Assume that the southbound IP address of iMaster NCE-Campus is 1.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] bootstrap ip-address 1.1.1.1 port 30217 voucher-type ip-or-domain always-trust
```

16.15.6 backup bootstrap

Function

The **backup bootstrap** command configures information about the backup Bootstrap server.

The **undo backup bootstrap** command deletes information about the backup Bootstrap server.

Format

backup bootstrap { **ip-address** *ip-address* | **domain** *domain* } **port** *port-number* **voucher-type** { **esn** | **ip-or-domain** } **always-trust**

undo backup bootstrap

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the Bootstrap server IP address, which is the secondary southbound IP address of iMaster NCE-Campus.	The value is in dotted decimal notation.
domain *domain*	Specifies the Bootstrap server domain name, which is the secondary southbound domain name of iMaster NCE-Campus.	The value is a string of 3 to 128 characters.
port *port-number*	Specifies the port number of a Bootstrap server.	The value is an integer in the range from 1 to 65535. Currently, the value is fixed at 30217.
voucher-type esn	Specifies that the voucher type is the device ESN.	-
voucher-type ip-or-domain	Specifies that the voucher type is the Bootstrap server address.	-
always-trust	Specifies that the voucher returned by the Bootstrap server is trusted by default.	-

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a disaster recovery scenario, you can run the **backup bootstrap** command to configure information about the standby Bootstrap server. If the primary Bootstrap server breaks down or is disconnected, services are automatically switched to the backup Bootstrap server, ensuring service continuity.

Example

Configure standby Bootstrap server information. Assume that the secondary southbound IP address of iMaster NCE-Campus is 1.1.2.1.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] backup bootstrap ip-address 1.1.2.1 port 30217 voucher-type ip-or-domain always-trust
```

16.15.7 callhome

Function

The **callhome** command creates a callhome template and enters the callhome template view.

The **undo callhome** command deletes a callhome template.

By default, there is no callhome template on a switch.

Format

callhome *callhome-name*

undo callhome *callhome-name*

Parameters

Parameter	Description	Value
callhome-name	Specifies the name of a callhome template.	The value is a string of 1 to 31 case-sensitive characters excluding spaces. If the string is enclosed in double quotation marks ("), the string can contain spaces.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If iMaster NCE-Campus needs to configure and manage a switch in NETCONF over SSH Callhome mode, you must run the **callhome** command to create a callhome template so that the switch can proactively set up a NETCONF connection with iMaster NCE-Campus.

Follow-up Procedure

Run the **ip address** command in the callhome template view to configure the IPv4 address and port number for the NMS.

Precautions

Only one callhome template can be created on a switch. Before creating a new callhome template, delete the existing one by running the **undo callhome** *callhome-name* command. After the command is run, communication between the switch and NMS is interrupted.

Example

Create the callhome template **Test123** and display the callhome template view.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] callhome Test123
[HUAWEI-netconf-callhome-Test123]
```

16.15.8 card register-permit

Function

The **card register-permit** command configures a slot-to-card name mapping.

The **undo card register-permit** command disables the slot-to-card name mapping.

By default, the name of the card that can be installed in a specific slot is not specified. That is, any card can be installed in the slot.

Format

card register-permit card-id *card-id* **card-name** *card-name*

undo card register-permit card-id *card-id*

Parameters

Parameter	Description	Value
card-id *card-id*	Specifies the slot ID of a card.	The value is in the format of *Slot ID*/CARD+*Card slot ID* and is case-insensitive, for example, 1/CARD1. The slot ID is in the range 0 to 8 and the card slot ID is in the range 1 to 4.
card-name *card-name*	Specifies the name of a card.	The value is a string of 1 to 32 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In NETCONF over SSH Callhome mode, you need to specify the name of the card that can be installed in a specific slot on iMaster NCE-Campus before registering the switch with iMaster NCE-Campus. The switch can register with iMaster NCE-Campus successfully only when the required cards are installed in their corresponding slots. If the name of the card installed in a specific slot is inconsistent with that configured on iMaster NCE-Campus, the switch will set this card to the **PowerOff** state.

In NETCONF over SSH mode, after enabling the NETCONF function on the switch, run the **card register-permit** command to specify the name of the card that can be installed in a specific slot. If the name of the card installed in a specific slot is inconsistent with the configured one, the switch will set this card to the **PowerOff** state. When the NETCONF function is disabled, the slot-to-card name mappings will be automatically cleared.

Example

Specify the name of the card that can be installed on card slot 1 of the switch in slot 1 after the NETCONF function is enabled on the switch.

```
<HUAWEI> system-view
[HUAWEI] card register-permit card-id 1/card1 card-name ES5D21Q02Q00
```

16.15.9 certificate identity

Function

The **certificate identity** command configures a unique common name (CN) for the iMaster NCE-Campus's certificate, which will be used for certificate uniqueness verification.

The **undo certificate identity** command cancels the CN configuration for the iMaster NCE-Campus's certificate.

By default, no CN is configured for the iMaster NCE-Campus's certificate; that is, the switch does not verify the CN of the iMaster NCE-Campus's certificate.

Format

certificate identity *common-name*

undo certificate identity

Parameters

Parameter	Description	Value
common-name	Specifies a unique CN for the iMaster NCE-Campus's certificate.	The value can be either of the following: • A string of 1 to 64 case-insensitive characters in cleartext, with spaces not supported • A string of 48 to 108 characters in ciphertext

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

When a switch registers with iMaster NCE-Campus for authentication, bidirectional certificate authentication is performed over an SSH channel established between them to ensure secure data transmission. However, if an attacker obtains the iMaster NCE-Campus's certificate and pretends to be iMaster NCE-Campus to communicate with the switch, the switch cannot identify this forged iMaster NCE-Campus, posing security risks.

To address this issue, you can run the **certificate identity** command on the switch to specify the CN of the iMaster NCE-Campus's certificate for certificate uniqueness verification. When the switch registers with iMaster NCE-Campus again, it compares the CN in the iMaster NCE-Campus's certificate with the locally configured one, and goes online only when the CNs are the same.

Example

Configure a CN for the iMaster NCE-Campus's certificate on the switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] certificate identity device-naas.huawei.com
```

16.15.10 controller backup ip-address

Function

The **controller backup ip-address** command configures an IP address of the standby iMaster NCE-Campus.

The **undo controller backup ip-address** command deletes the IP address of the standby iMaster NCE-Campus.

By default, no IP address of the standby iMaster NCE-Campus is configured.

Format

controller backup ip-address *ip-address* **port** *port-number*

undo controller backup ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the standby iMaster NCE-Campus.	The value is in dotted decimal notation.
port *port-number*	Specifies a port number.	The value is an integer in the range from 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The switch needs to register with iMaster NCE-Campus for authentication in NETCONF over SSH Callhome mode. Before registration authentication, the switch needs to obtain the IP address of iMaster NCE-Campus for communication with iMaster NCE-Campus. The switch can obtain the IP address of iMaster NCE-Campus through DHCP or the registration query center, or you can configure an IP address for iMaster NCE-Campus using the **controller ip-address** command.

In a disaster recovery scenario, you can run the **controller backup ip-address** command to configure the IP address of the standby iMaster NCE-Campus. When the active iMaster NCE-Campus breaks down or is disconnected, services are automatically switched to the standby iMaster NCE-Campus, ensuring service continuity.

Precautions

- If the switch obtains the IP addresses of iMaster NCE-Campus using all the three methods, the IP addresses are sorted in descending order of priority as follows: IP address obtained using DHCP, IP address configured using the command, and IP address obtained through the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **controller ip-address** command and the **controller url** command are configured on the switch, only the latest command takes effect. That is, the switch registers with iMaster NCE-Campus using either the IP address of iMaster NCE-Campus or the IP address resolved from the URL of iMaster NCE-Campus.
- If a switch that has registered with a iMaster NCE-Campus registers with another iMaster NCE-Campus, the device configurations will change. Exercise caution when performing this operation.
- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset netconf db-configuration** command. To clear the configuration of this command, run the **undo controller backup ip-address**, **undo netconf**, or **reset factory-configuration** command.

Example

Configure the IP address of the standby iMaster NCE-Campus on a switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] controller backup ip-address 10.1.1.1 port 10020
```

16.15.11 controller ip-address

Function

The **controller ip-address** command configures an IP address for iMaster NCE-Campus.

The **undo controller ip-address** command deletes the IP address configured for iMaster NCE-Campus.

By default, no IP address is configured for iMaster NCE-Campus on a switch.

Format

controller ip-address *ip-address* **port** *port-number*

undo controller ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for iMaster NCE-Campus.	The value is in dotted decimal notation.
port *port-number*	Specifies a port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The switch needs to register with iMaster NCE-Campus for authentication in NETCONF over SSH Callhome mode. Before registration authentication, the switch needs to obtain the IP address of iMaster NCE-Campus for communication with iMaster NCE-Campus. The switch can obtain the IP address of iMaster NCE-Campus through DHCP or the registration query center, or you can configure an IP address for iMaster NCE-Campus using the **controller ip-address** command.

Precautions

- If the switch obtains the IP addresses of iMaster NCE-Campus using all the three methods, the IP addresses are sorted in descending order of priority as follows: IP address obtained using DHCP, IP address configured using the command, and IP address obtained through the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **controller ip-address** command and the **controller url** command are configured on the switch, only the latest command takes effect. That is, the switch registers with iMaster NCE-Campus using either the IP address of iMaster NCE-Campus or the IP address resolved from the URL of iMaster NCE-Campus.
- If a switch that has registered with a iMaster NCE-Campus registers with another iMaster NCE-Campus, the device configurations will change. Exercise caution when performing this operation.

- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset netconf db-configuration** command. To clear the configuration of this command, run the **undo controller ip-address**, **undo netconf**, or **reset factory-configuration** command.

Example

Configure an IP address for iMaster NCE-Campus.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] controller ip-address 10.1.1.1 port 10020
```

16.15.12 controller url

Function

The **controller url** command configures a URL for iMaster NCE-Campus.

The **undo controller url** deletes the URL configured for iMaster NCE-Campus.

By default, no URL is configured for iMaster NCE-Campus on the switch.

Format

controller url *url-string* **port** *port-number*

undo controller url

Parameters

Parameter	Description	Value
url-string	Specifies a URL for iMaster NCE-Campus.	The value is a string of 3 to 128 case-sensitive characters. If you need to set one or more consecutive spaces, enclose the URL in double quotation marks (").
port *port-number*	Specifies a port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In NETCONF over SSH Callhome mode, the switch needs to register with iMaster NCE-Campus for authentication. Before registration authentication, the switch needs to obtain the IP address of iMaster NCE-Campus for communication with iMaster NCE-Campus. The switch can obtain the IP address of iMaster NCE-Campus through DHCP or the registration query center or obtain the IP address by resolving the URL configured using the **controller url** command.

Precautions

- If the switch obtains the URL of iMaster NCE-Campus using all the three methods, the URLs are sorted in descending order of priority as follows: URL obtained using DHCP, URL configured using the command, and URL obtained through the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **controller url** command and the **controller ip-address** or **controller backup ip-address** command are configured on the switch, only the latest command takes effect. That is, the switch registers with iMaster NCE-Campus using either the IP address of iMaster NCE-Campus or the IP address resolved from the URL of iMaster NCE-Campus.
- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset netconf db-configuration** command. To clear the configuration of this command, run the **undo controller url**, **undo netconf**, or **reset factory-configuration** command.

Example

Configure a URL for iMaster NCE-Campus on the switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] controller url controller.huawei.com port 10020
```

16.15.13 display netconf alarm active

Function

The **display netconf alarm active** command displays the active alarms reported by the switch to NMS.

Format

display netconf alarm active

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the NETCONF function is enabled on a switch, you can run the **display netconf alarm active** command to view the active alarms reported by the switch.

Example

Display the active alarms reported by the switch to NMS.

```
<HUAWEI> display netconf alarm active
A/B/C/D/E/F/G
A=Sequence, B=Alarm type, C=Generating time
D=Name, E=Level, F=OID, G=Description

  1/equipmentAlarm/2019-08-27T02:15:42Z/hwPowerInvalid/critical/1.3.6.1.4.1.2011.5.25.219.2.5.5/Power
supply is unavailable for some reason.
(Index=67207181, EntityPhysicalIndex=67207181, PhysicalName="POWER Card 0/PWR2",
EntityTrapFaultID=136973)
  2/equipmentAlarm/2019-08-27T02:15:59Z/hwPowerInvalid/critical/1.3.6.1.4.1.2011.5.25.219.2.5.5/Power
supply is unavailable for some reason.
(Index=68255757, EntityPhysicalIndex=68255757, PhysicalName="POWER Card 1/PWR2",
EntityTrapFaultID=136973)
```

Table 16-87 Description of the **display netconf alarm active** command output

Item	Description
A/B/C/D/E/F/G	Alarm format.
A=Sequence	Alarm sequence number.
B=Alarm type	Alarm type.
C=Generating time	Time when an alarm was generated
D=Name	Alarm name.
E=Level	Alarm severity.
F=OID	Alarm OID.
G=Description	Alarm description.

16.15.14 display netconf configuration

Function

The **display netconf configuration** command displays the information of iMaster NCE-Campus.

Format

display netconf configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information of iMaster NCE-Campus (such as the IP address), run the **display netconf configuration** command.

This command cannot display the information of iMaster NCE-Campus obtained through DHCP or the registration query center.

Example

Display the information of iMaster NCE-Campus.

```
<HUAWEI> display netconf configuration
--------------- Configuration begin---------------
controller ip-address 10.1.1.1 port 10020
controller ip-address 192.168.2.2 port 10020 (redirected)
CLI permission: allowed
Current startup rdb file: configbackup/2022-06-23_startup.rdb
--------------- Configuration end-----------------
```

Table 16-88 Description of the **display netconf configuration** command output

Item	Description
controller ip-address 10.1.1.1 port 10020	The configured IP address and port number of iMaster NCE-Campus are 10.1.1.1 and 10020 respectively. If the information is marked with **redirected**, the switch has been redirected from iMaster NCE-Campus with which it just registers to another iMaster NCE-Campus for management.
CLI permission	Whether commands except those for configuring the whitelist can be configured on the device. ● denied ● allowed (default value) You can change the value only through the iMaster NCE-Campus.
Current startup rdb file	Database file that takes effect currently.

16.15.15 display netconf connect-status

Function

The **display netconf connect-status** command displays the NETCONF configuration on a switch.

Format

display netconf connect-status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the NETCONF configuration on a switch, run the **display netconf connect-status** command.

Example

Display the NETCONF configuration on the switch.

```
<HUAWEI> display netconf connect-status
----------------------------------------------------------------------------------------------------
Netconf status                 : enable
Upload alarm status            : enable
----------------------------------------------------------------------------------------------------
Controller address source      : --
Controller URL                 : --
Controller IP address          : --
Controller port                : --
Backup controller URL          : --
Backup controller IP address   : 10.1.1.1
Backup controller port         : 10020
Management VLAN                : --
Management IP address          : --
Register phase                 : --
Register status                : --
----------------------------------------------------------------------------------------------------
Netconf src-ip                 : 192.168.10.1
Netconf src-ipv6               : --
Netconf src-port               : 830
Controller information         :
----------------------------------------------------------------------------------------------------
No Mode     Name                        IP                      Port  Connected  RegisterStatus
----------------------------------------------------------------------------------------------------
1  callhome aa                       192.168.30.1(Master)      10020 N
Unregistered
2  ssh      -                           -                       -     N          -
```

```
3  ssh      -                              -                        -     N          -
----------------------------------------------------------------------------------------------------------
Bootstrap information
  Address source               : User-configured
  Main URL                     : https://1.1.1.1:30217(Active)
  Backup URL                   : --
----------------------------------------------------------------------------------------------------------
```

Table 16-89 Description of the **display netconf connect-status** command output

Item	Description
Netconf status	Status of the NETCONF function: ● **enable**: The function is enabled. ● **disable**: The function is disabled. To configure the NETCONF function, run the **netconf** command.
Upload alarm status	Whether the switch is configured to send alarms to the NMS: ● **enable**: The switch is configured to send alarms to the NMS. ● **disable**: The switch cannot send alarms to the NMS.
Controller address source	Source from which the iMaster NCE-Campus address is obtained. ● **User-defined configuration**: indicates that the address is defined by the user. ● **Allocated by Register Center**: indicates that the address is obtained from the registration query center. ● **Allocated by DHCP**: indicates that the address is obtained through DHCP. ● **Allocated by controller**: indicates that the IP address is obtained from iMaster NCE-Campus. ● --: indicates that the iMaster NCE-Campus address is not obtained.
Controller URL	URL of iMaster NCE-Campus. To configure the URL for iMaster NCE-Campus, run the **controller url** command. If no URL is configured or obtained, this parameter value is --.
Controller IP address	IP address of iMaster NCE-Campus. To configure the IP address for iMaster NCE-Campus, run the **controller ip-address** command. If no IP address is configured or obtained, this parameter value is --.

Item	Description
Controller port	Port number of iMaster NCE-Campus. To configure the port number of iMaster NCE-Campus, run the **controller ip-address** command. If no port number is configured or obtained, this parameter value is -.
Backup controller URL	URL of the standby iMaster NCE-Campus. The value can be obtained only through Option 148. If no value is obtained, the parameter value is **--**.
Backup controller IP address	IP address of the standby iMaster NCE-Campus. To configure this parameter, run the **controller backup ip-address** command. If no IP address is configured or obtained, the parameter value is **--**.
Backup controller port	Port number of the standby iMaster NCE-Campus. To configure this parameter, run the **controller backup ip-address** command. If no port number is configured or obtained, the parameter value is **--**.
Management VLAN	Management VLAN ID used when the switch communicates with iMaster NCE-Campus. The management VLAN can be configured using the **management-vlan (NETCONF view)** command. If **Management VLAN (Dynamic)** is displayed in the command output, the management VLAN is automatically negotiated using the PNP protocol. The management VLAN statically configured using the **management-vlan** command in the NETCONF view has a higher priority than the management VLAN dynamically negotiated using PNP.
Management IP address	IP address of the VLANIF interface corresponding to the management VLAN used when the switch communicates with iMaster NCE-Campus. This IP address can be dynamically allocated by the DHCP server, or it can be the static IP address configured for the VLANIF interface corresponding to the management VLAN. If no IP address is dynamically allocated or configured on the VLANIF interface, this parameter value is --.

Item	Description
Register phase	Current registration phase of the switch. - **DHCP**: The switch is requesting an IP address from a DHCP server. - **registering**: The switch has obtained an IP address from a DHCP server and is registering with iMaster NCE-Campus. - **registered**: The switch has registered with iMaster NCE-Campus. - **aborted**: The process of registering the switch with iMaster NCE-Campus is terminated using the **netconf register abort** command.
Register status	Current registration status of the switch. **NOTE** If the TCP connection between the switch and iMaster NCE-Campus is disconnected, it takes the switch 3 minutes to detect the disconnection. The switch changes from **registered** to **unregistered** state only after detecting the disconnection.
Netconf src-ip	IPv4 address of the switch. To configure the IPv4 address of the switch, run the **source ip** command.
Netconf src-ipv6	IPv6 address of the switch. To configure the IPv6 address of the switch, run the **source ipv6-address** command.
Netconf src-port	Port number used by the switch. To configure the port number, run the **source ip** command.
Controller information	Information about the connected NMS.
No	Connection number.
Mode	NETCONF mode: - **callhome**: NETCONF over SSH Callhome - **ssh**: NETCONF over SSH
name	Name of a callhome template. This parameter is not supported in NETCONF over SSH mode and the parameter value will be a hyphen (-) in this mode. To configure the name of a callhome template, run the **callhome** command.
IP	IPv4 address of the NMS. To configure the IPv4 address of the NMS in NETCONF over SSH Callhome mode, run the **ip address** command in the callhome template view.

Item	Description
Port	- This parameter is the port number used by the NMS in NETCONF over SSH Callhome mode. To configure the port number, run the **ip address** command in the callhome template view. - This parameter is the port number used by both the switch and NMS in NETCONF over SSH mode. To configure the port number, run the **source ip** or **source ipv6-address** command.
Connected	Whether the NMS has set up a NETCONF connection with the switch: - **Y**: The NMS has set up a NETCONF connection with the switch. - **N**: The NMS has not set up a NETCONF connection with the switch.
RegisterStatus	Status of the switch on iMaster NCE-Campus. This field is supported only when the NETCONF mode is callhome. - Unregistered: The switch is offline. - Registered: The switch is online. - -: This field is not supported.
Bootstrap information	Bootstrap information.
Address source	Method used to obtain Bootstrap information.
Main URL	Primary address, including the IP address/domain name and port number. If **(Active)** is contained in the value, the device has set up a connection with this address.
Backup URL	Backup address, including the IP address/domain name and port number. If **(Active)** is contained in the value, the device has set up a connection with this address.

16.15.16 display netconf offline-record

Function

The **display netconf offline-record** command displays the reason for the switch to go offline.

Format

display netconf offline-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a switch goes offline, you can run the **display netconf offline-record** command to check the reason. Only the latest five records will be displayed.

Example

Display the reason for the switch to go offline.

```
<HUAWEI> display netconf offline-record
--------------------------------------------------------------------------------
Time                      Error Info
--------------------------------------------------------------------------------
2019/10/12 11:13:10       Connect lost
2019/10/12 11:05:53       Connect lost
2019/10/12 10:58:32       Board reset by VRP command or net 
manager
2019/10/12 10:58:30       Connect lost
--------------------------------------------------------------------------------
```

Table 16-90 Description of the **display netconf offline-record** command output

Item	Description
Time	Time when the switch went offline.

Item	Description
Error Info	Reason for the switch to go offline. ● Connect lost ● The stackid is inconsistent and setting failed due to fabric port member configuration ● Board reset by VRP for unknown reason ● Board reset by VRP for registering failure ● Board reset by VRP interface management module ● Board reset by VRP command or net manager ● Board reset by VRP for not ready when slave switching to master ● Board reset by VRP for schedule ● Board reset by ISSU for switch-prepare or switch-age failed ● Board reset by NSR ● Board reset by PATCH for restore patch number error ● Board reset by PATCH for restore patch file error ● Board reset by PATCH for effect after restore running ● Board reset by NSF ● Board reset by ISIS for purging LSP error ● Board reset by OSPF for aging LSA error ● Board reset by PATCH for the patch is not empty ● Board reset by PATCH for the patch filename or status is incorrect ● Board reset by PATCH for the insufficient space or file occupation ● Board reset by PATCH for the patch file fails to be synchronized ● Board reset by PATCH after the patch is successfully synchronized ● Board reset by PATCH due to patch restoration preprocessing failure

16.15.17 display netconf register-fail-record

Function

The **display netconf register-fail-record** command displays records about failed registrations with iMaster NCE-Campus.

Format

display netconf register-fail-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After this command is executed, a maximum of five registration failure records can be displayed.

If there are multiple registration failures caused by the same reason, only the corresponding registration failure record is updated, which will not overwrite registration failure records with other reasons.

Example

Display records about failed registrations with iMaster NCE-Campus.

```
<HUAWEI> display netconf register-fail-record
----------------------------------------------------------------------------
Time                     Error Info
----------------------------------------------------------------------------
2019/11/09 23:21:02        Failed to apply IP address
2019/11/09 23:12:13        Failed to create TCP link to controller (192.168.1.1)
2022/07/09 22:21:02        Failed to obtain the Lite CA certificate from the bootstrap server
2022/09/09 22:21:02        Failed to obtain local certificate (192.168.1.1)
----------------------------------------------------------------------------
```

Table 16-91 Description of the **display netconf register-fail-record** command output

Item	Description
Time	Registration failure time.

Item	Description
Error Info	Reason for the registration failure. The IP address in this parameter value is the IP address of iMaster NCE-Campus with which the switch failed to register. Possible reasons are as follows: ● Manage VLAN is physical down ● Change to tradition work mode failed ● Failed to apply IP address ● No DNS information in DHCP options ● No controller IP or URL information ● Failed to get IP address of controller ● Failed to create TCP link to controller ● Failed to get register result from controller ● Controller certificate authentication failed ● Controller ESN check failed ● Device is not authorized ● Device type and ESN does not match ● Failed to connect registration center ● The configuration of the device is inconsistent with that of the controller: For example, the stack configuration exists on the device, but not on the controller. ● The slot number of the device is inconsistent with that on the controller ● The controller failed to verify the sitecode ● Failed to obtain the Lite CA certificate from the bootstrap server ● Failed to obtain local certificate ● Others

16.15.18 display netconf { rsa | dsa } local-key-pair public

Function

The **display netconf { rsa | dsa } local-key-pair public** command displays the public key in the local RSA or DSA key pair.

Format

display netconf { rsa | dsa } local-key-pair public

Parameters

Parameter	Description	Value
rsa	Displays the public key in the local RSA key pair.	-
dsa	Displays the public key in the local DSA key pair.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to display the public key in the RSA or DSA key pair on a switch, and then copy the public key to the RSA or DSA public key on the controller. In this way, the public keys on the switch and controller are the same, ensuring successful authentication.

Example

Display the public key in the local DSA key pair.

```
<HUAWEI> display netconf dsa local-key-pair public
The DSA public key:
ssh-dss AAAAB3NzaC1kc3MAAACBAOAWWAtGClBH4qhgm0+ntDTZVW/tR8R9Vn
+rXVA8GFWM5TVUJWXFWghy4QTJqmvg+ca0znn+c2hDGDhx1yhRsduKWmOBAzIQE/
1OYhMLdK0vRmceyYtSTfVNCbtAwJNOM0JPBlbim/
vjp3aX3iRn6EPU7bYaJ3A8KEUZlVKh7YU5AAAAFQCQ8znriZRmpyoAVK68YPNDnKzkGQAAAIA8f1ELwIJC9J73z
g6an2Hz7P3zDAqDv2mnvOuvKEbVWY3IVNhCHaX39yBl0PT2rWmXzHI6nJWEPiuoW/
eJpDxNwV1OCgSN4mhG90/
iOJkLKqF6UENdQWXNKbjLHYKTkKXSnpi2ibqEzrqnbkzIVbaf2a8nBDrh1CHKRhw1dQChggAAAIA7TGIupodUc1
Enn3rzTNch5rL0CKL9znjFG+lyeJU39fDWSOVfgWfz4ehs48/5Zco6H9wj1seLxh3pVXYLqJvRDR6B0g/
68T3aEYEKGoHeRYC3sU80lXb8s0VFae90ohOf89ULyfVt7HVE+QKkExQIj9sAo8KbR3gNkb84PM+Z9g==
root@root
```

16.15.19 display work-mode

Function

The **display work-mode** command displays the working mode of the switch.

Format

display work-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display work-mode** command to view the working mode of a switch.

Example

Display the working mode of the switch.

```
<HUAWEI> display work-mode
Current work-mode        : NETCONF
Work-mode before upgrade: Cloud-mng
```

Table 16-92 Description of the **display work-mode** command output

Item	Description
Current work-mode	Working mode of the switch: - NETCONF: NETCONF is enabled. - Tradition: NETCONF is disabled.
Work-mode before upgrade	Working mode of the switch before the upgrade. **Cloud-mng** indicates cloud-based management. This field is displayed only when a switch working in cloud-based management mode is upgraded to V200R019C00 or a later version.

16.15.20 ip address (callhome template view)

Function

The **ip address** command configures the IPv4 address and port number used by the NMS that communicates with a switch through NETCONF.

The **undo ip address** command deletes the IPv4 address and port number used by the NMS that communicates with a switch through NETCONF.

By default, no IPv4 address and port number have been configured for the NMS with which the switch communicates through NETCONF.

Format

ip address *ip-address* **port** *port-number*

undo ip address

Parameters

Parameter	Description	Value
ip-address	IPv4 address of the NMS.	The value is in dotted decimal notation.
port *port-number*	Port number used by the NMS.	The value is an integer in the range 1 to 65535.

Views

Callhome template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch in NETCONF over SSH Callhome mode, you must run the **ip address** command to configure the IPv4 address and port number for the NMS so that the switch can proactively set up a NETCONF connection with the NMS.

Precautions

If a switch that has registered with a iMaster NCE-Campus needs to register with another iMaster NCE-Campus, restart the switch before the re-registration.

Example

Set the IP address and port number used by the NMS to communicate with the switch through NETCONF to 10.1.2.1 and 10020, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] callhome Test123
[HUAWEI-netconf-callhome-Test123] ip address 10.1.2.1 port 10020
```

16.15.21 lldp tlv-enable legacy-tlv pnp

Function

The **lldp tlv-enable legacy-tlv pnp** command configures an interface to advertise PnP TLVs.

The **undo lldp tlv-enable legacy-tlv pnp** command disables an interface from advertising PnP TLVs.

By default, an interface advertises all PnP TLVs.

Format

lldp tlv-enable legacy-tlv pnp { **all** | **startup-vlan** | **startup-link-aggregation** | **device-type** }

undo lldp tlv-enable legacy-tlv pnp { **all** | **startup-vlan** | **startup-link-aggregation** | **device-type** }

Parameters

Parameter	Description	Value
all	Advertises all PnP TLVs.	-
startup-vlan	Specifies the PnP TLVs to be advertised to VLAN IDs.	-
startup-link-aggregation	Specifies the PnP TLVs to be advertised to the Eth-Trunk flag and LACP mode flag.	-
device-type	Specifies the PnP TLVs to be advertised to device types.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view, port group view

Default Level

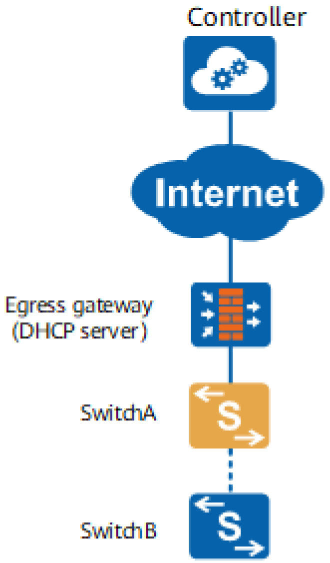
2: Configuration level

Usage Guidelines

- **Scenario 1: All switches on a CloudCampus network can be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-2**, SwitchA and SwitchB are both switches. SwitchB is newly connected to the network when the VLAN for the IP address pool of the DHCP server is not VLAN 1. After SwitchB is connected to the network, by default, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of iMaster NCE-Campus. However, SwitchB fails to obtain the information because the VLAN for the IP address pool of the DHCP server is not VLAN 1.

Figure 16-2 CloudCampus networking



To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain related information from the DHCP server.

SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

- SwitchA has registered with iMaster NCE-Campus successfully.
- iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
- iMaster NCE-Campus has delivered the function of transmitting the PnP VLAN ID to the downstream device to SwitchA, and the configuration file contains the **pnp startup-vlan send enable** command.
- SwitchA is enabled to send LLDPDUs containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** or **undo lldp tlv-enable legacy-tlv pnp all** command, the function of sending LLDPDUs containing the PnP VLAN ID to the downstream device is disabled. You can enable the function on iMaster NCE-Campus.

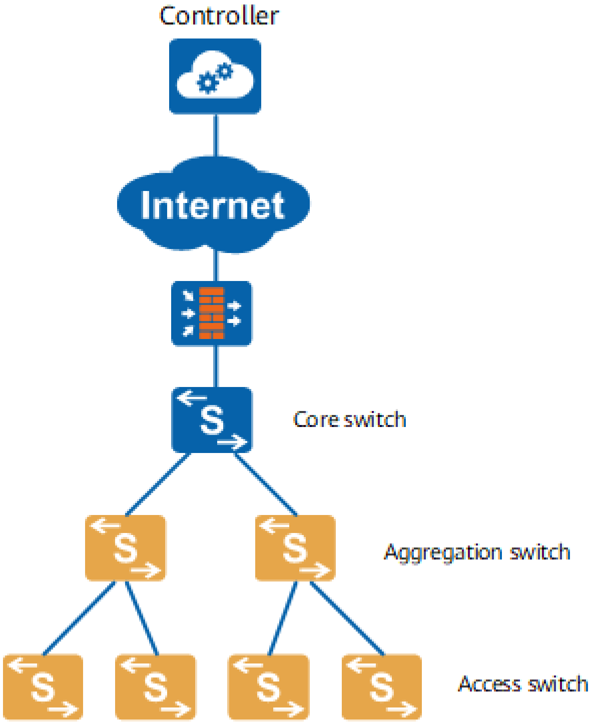
SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function on iMaster NCE-Campus.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on iMaster NCE-Campus and delivered to a switch after the switch has registered with iMaster NCE-Campus.

- **Scenario 2: On a CloudCampus network, some switches cannot be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-3**, the access and aggregation switches can be managed by iMaster NCE-Campus. The core switch is not managed by iMaster NCE-Campus. When the management VLAN is changed on iMaster NCE-Campus from VLAN 1 (default) to VLAN 2, the core switch needs to notify its downstream switches of the new management VLAN ID.

  Figure 16-3 CloudCampus networking



  Configure PnP VLAN auto-negotiation on the core switch so that the core switch can notify its downstream switches of the new management VLAN ID. This process consists of the following operations:

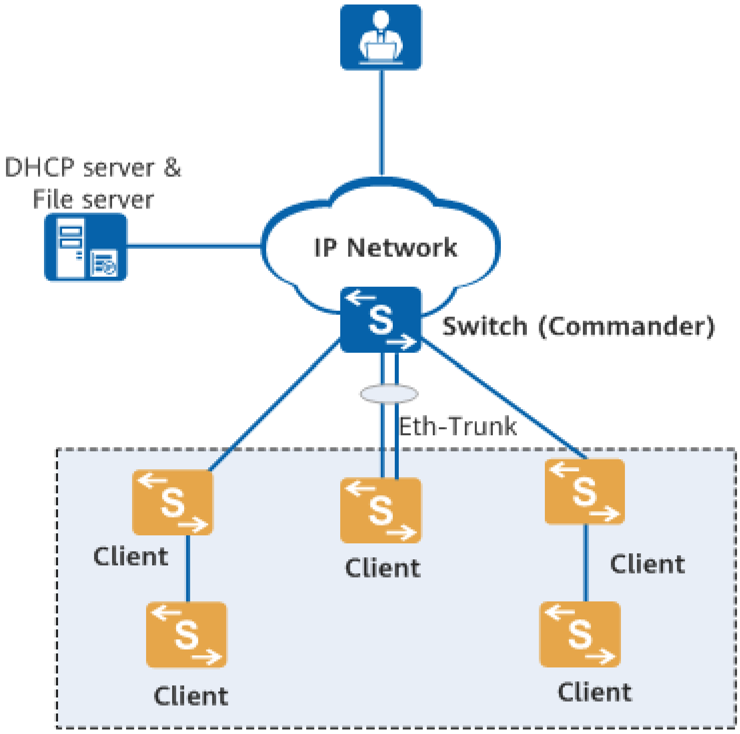
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation**

enable command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

- **Scenario 3: Zero-touch deployment using EasyDeploy**

  In **Figure 16-4**, when EasyDeploy is used for zero touch deployment, the Commander needs to notify a client of the new VLAN ID if the Commander does not use VLAN 1 to communicate with the client.

  Figure 16-4 EasyDeploy networking diagram



- Configure PnP VLAN auto-negotiation on the Commander to enable the Commander to notify clients of the new VLAN ID. This process consists of the following operations:
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

Example

Enable a switch to send LLDPDUs containing PnP VLAN information to downstream devices.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable legacy-tlv pnp startup-vlan
```

16.15.22 management-vlan (NETCONF view)

Function

The **management-vlan** command configures the VLAN used by the switch to communicate with a DHCP server. This VLAN is the management VLAN of the switch.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID used by the switch to communicate with a DHCP server.	The value is an integer in the range 1 to 4094.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In NETCONF over SSH Callhome mode, the switch can obtain the IP address of iMaster NCE-Campus using DHCP. The request sent by the switch to the DHCP server to obtain the IP address of iMaster NCE-Campus is transmitted over VLAN 1. After the switch passes registration authentication, iMaster NCE-Campus changes the VLAN ID used by the switch to communicate with the DHCP server again. After the switch restarts, to ensure that it continues to use the configured VLAN to communicate with the DHCP server, you can configure the management VLAN on the switch.

Precautions

- This command cannot be configured if the **source ip-address** command has been executed in the SMI view to configure the IPv4 address used by the switch to communicate with the NMS (such as the analyzer iMaster NCE-CampusInsight).
- The management VLAN of the switch cannot be the same as the management VLAN of the CAPWAP tunnel.
- When you disable NETCONF in the system view or delete the management VLAN in the NETCONF view, the system displays a message asking you whether to retain the **ip address dhcp-alloc** configuration. Exercise caution when you choose to delete the configuration.
- Assume that a static IP address has been configured for a VLANIF interface. When you run the **management-vlan** command to configure the VLAN corresponding to this VLANIF interface as the management VLAN, the device displays a message indicating that users in the management VLAN will be unable to go online through DHCP. Exercise caution when running this command.

Example

Set the management VLAN ID of the switch to 2.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] management-vlan 2
```

16.15.23 netconf

Function

The **netconf** command enables the NETCONF function and enters the NETCONF view.

The **undo netconf** command disables the NETCONF function.

By default, NETCONF is disabled on a switch.

Format

netconf

undo netconf

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch using NETCONF, run the **netconf** command on the switch to enable the NETCONF function.

Precautions

- After the **undo netconf** command is executed on the switch to disable the NETCONF function, all NETCONF configurations, all the database information, and the **card register-permit** configuration on the switch are deleted, leading to communication interruption between the switch and NMS.
- Before running the **netconf** command to enable the NETCONF function, ensure that port 830 and ports 55552 to 55807 are not in use. Otherwise, NETCONF cannot be enabled.
- Before running the **netconf** command to enable the NETCONF function, ensure that the fixed IP address 169.254.2.1 that is automatically configured for a virtual management interface is not in use. Otherwise, NETCONF cannot be enabled.
- If Eth-Trunk 0 has been created on a switch, Eth-Trunk auto-negotiation will become abnormal after you enable the NETCONF function using the **netconf** command.
- When you disable NETCONF in the system view or delete the management VLAN in the NETCONF view, the system will prompt you to delete the **ip address dhcp-alloc** configuration. Exercise caution when you choose to delete the configuration.
- For the S6735-S, S6720-EI and S6720S-EI, when you run the **netconf** command to enable NETCONF, the device automatically delivers the **unknown-unicast load-balance enhanced lbid** command and displays a message indicating that enabling NETCONF will automatically disable LNP, enable STP, and configure load balancing for broadcast, unknown unicast, and multicast packets (BUM packets). Exercise caution when performing this operation. If the S6735-S, S6720-EI or S6720S-EI running a version earlier than V200R021C10 is enabled with NETCONF and then is upgraded to V200R021C10 or later, the switch does not automatically deliver the **unknown-unicast load-balance enhanced lbid** command for upgrade compatibility purposes.

Example

Enable the NETCONF function and display the NETCONF view.

```
<HUAWEI> system-view
[HUAWEI] netconf
```

16.15.24 netconf config enhanced

Function

The **netconf config enhanced** command sets the configuration mode of a switch to enhanced mode.

The **undo netconf config enhanced** command restores the default configuration mode of a switch.

By default, the default configuration mode is used on a switch.

Format

netconf config enhanced

undo netconf config enhanced

Parameters

None

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

When the default configuration mode is used on a switch, the switch limits the number of objects in the packets sent from iMaster NCE-Campus. If the number of objects in the packets sent from iMaster NCE-Campus exceeds this limit, the switch returns an error message indicating that the configuration fails to be delivered.

To remove this limit, run the **netconf config enhanced** command on the switch to enable the enhanced configuration mode.

In versions earlier than V200R022C10, a switch does not limit the number of nodes in packets issued by iMaster NCE-Campus packets. After the switch is upgraded to V200R022C10 or a later version, the **netconf config enhanced** configuration is automatically added to the configuration file to ensure that the switch still has no such a limitation after the upgrade.

NOTICE

The enhanced configuration mode of a switch affects system stability, which may cause device exceptions. Therefore, use this function under the guidance of technical support engineers.

Example

Set the switch configuration mode to default mode.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] undo netconf config enhanced
```

16.15.25 netconf alarm upload enable

Function

The **netconf alarm upload enable** command enables the switch to report alarms to the NMS.

The **undo netconf alarm upload enable** command disables the switch from reporting alarms to the NMS.

By default, a switch is enabled to report alarms to the NMS.

Format

netconf alarm upload enable

undo netconf alarm upload enable

Parameters

None

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

If a switch reports a large number of alarms to the NMS, the CPU usage of the switch is high. As a result, services cannot be configured on the switch. To prevent this problem, you can run the **undo netconf alarm upload enable** command to disable the device from reporting alarms to the NMS.

Example

Disable the device from reporting alarms to the NMS.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] undo netconf alarm upload enable
```

16.15.26 netconf register abort

Function

The **netconf register abort** command terminates a switch's registration with iMaster NCE-Campus.

The **undo netconf register abort** command resumes a switch's registration with iMaster NCE-Campus.

By default, a switch registers with iMaster NCE-Campus normally.

Format

netconf register abort

undo netconf register abort

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a switch fails to register with iMaster NCE-Campus, log in to the switch through SSH to view the registration status. If the registration process is not terminated, the DHCP server may re-assign an IP address to the switch, which will cause the SSH login process to terminate. To prevent this problem, log in to the switch and then run the **netconf register abort** command to terminate the registration process.

After this command is executed, the registration process stops for 30 minutes and then resumes. To view the registration status, run the **display netconf connect-status** command.

Precautions

- The **netconf register abort** command cannot be executed repeatedly.
- Do not run this command when the switch has registered with iMaster NCE-Campus successfully.
- The command configuration is not recorded to the configuration file and the command will become ineffective after the switch restarts.
- If this command is run and iMaster NCE-Campus displays the device status as registered, the actual registration status is subject to the **display netconf connect-status** command output.

Example

Terminate the switch's registration with iMaster NCE-Campus.

```
<HUAWEI> system-view
[HUAWEI] netconf register abort
```

16.15.27 pnp disable

Function

The **pnp disable** command disables PnP negotiation on an interface.

The **undo pnp disable** command enables PnP negotiation on an interface.

By default, PnP negotiation is enabled on an interface of a switch.

Format

pnp disable

undo pnp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a campus solution scenario, newly connected switches can go online through a PnP VLAN. By default, PnP negotiation is enabled on interfaces. If a new downstream access switch is planned not to use a PnP VLAN to register with and go online on iMaster NCE-Campus, you can disable PnP negotiation on the interface connected to the downstream switch.

Precautions

This command cannot be configured in the Eth-Trunk 0 interface view.

Example

Disable PnP on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] pnp disable
```

16.15.28 pnp startup-link-aggregation enable

Function

The **pnp startup-link-aggregation enable** command enables a switch to inform its downstream device of the need to establish an Eth-Trunk.

The **undo pnp startup-link-aggregation enable** command disables a switch from informing its downstream device of the need to establish an Eth-Trunk.

By default, a switch is disabled from informing its downstream device of the need to establish an Eth-Trunk.

Format

pnp startup-link-aggregation enable

undo pnp startup-link-aggregation enable

Parameters

None

Views

Eth-Trunk interface view

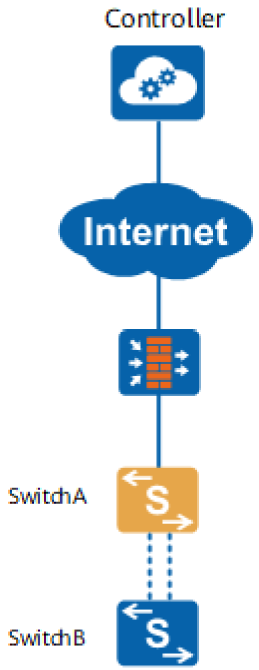
Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 16-5 CloudCampus network diagram



As shown in **Figure 16-5**, the new switch, SwitchB, is connected to its upstream device, SwitchA, through two links. When SwitchB and SwitchA negotiate the PnP VLAN, if SwitchA is enabled to inform its downstream device of the need to establish an Eth-Trunk, SwitchB adds two links to the Eth-Trunk and sets the Eth-Trunk mode based on whether the Eth-Trunk mode of SwitchA is LACP.

The auto-negotiated Eth-Trunk can only be Eth-Trunk0, which is reserved on iMaster NCE-Campus and cannot be used by other services.

Precautions

- Running this command on uplink interfaces is not recommended, as it will cause connection failures.
- Only the following configurations are allowed on the physical uplink port of the downstream device when this port is added to Eth-Trunk 0 through auto-negotiation. If any other configurations exist on the physical uplink port, it cannot be automatically added to Eth-Trunk 0.
  - **trust dscp**
  - **port link-type trunk**
  - **description** *description*
- After a switch registers with iMaster NCE-Campus, you are advised to fix the auto-negotiated Eth-Trunk through iMaster NCE-Campus. This prevents the configuration from becoming invalid after the switch goes offline from the controller.

Example

Enable the function of transmitting the flag indicating whether to establish an Eth-Trunk to downstream devices.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] pnp startup-link-aggregation enable
```

16.15.29 pnp startup-link-aggregation receive enable

Function

The **pnp startup-link-aggregation receive enable** command enables Eth-Trunk auto-negotiation.

The **undo pnp startup-link-aggregation receive enable** command disables Eth-Trunk auto-negotiation.

By default, Eth-Trunk auto-negotiation is enabled.

Format

pnp startup-link-aggregation receive enable

undo pnp startup-link-aggregation receive enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device goes online through a negotiated PnP VLAN and the network of the upstream device becomes stable, you can run the **undo pnp startup-link-aggregation receive enable** command on the downstream device to disable Eth-Trunk auto-negotiation. Then, the device will not accept new Eth-Trunk auto-negotiation requests. In this way, the configuration of Eth-Trunk 0 and its member interfaces remain unchanged, preventing flapping of the upstream device from affecting local services. If Eth-Trunk auto-negotiation is not disabled, the connection between the device and controller will be unstable when Eth-Trunk members are added or deleted.

Precautions

After Eth-Trunk auto-negotiation is disabled, if the networking mode of the upstream device changes, you need to enable Eth-Trunk auto-negotiation again.

Example

Disable Eth-Trunk auto-negotiation.

```
<HUAWEI> system-view
[HUAWEI] undo pnp startup-link-aggregation receive enable
```

16.15.30 pnp startup-vlan

Function

The **pnp startup-vlan** command configures a wired PnP VLAN ID for wired devices.

The **undo pnp startup-vlan** command deletes a wired PnP VLAN ID.

By default, no wired PnP VLAN ID is configured on a switch.

Format

pnp startup-vlan *vlan-id*

undo pnp startup-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a wired PnP VLAN ID.	The value is an integer in the range 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

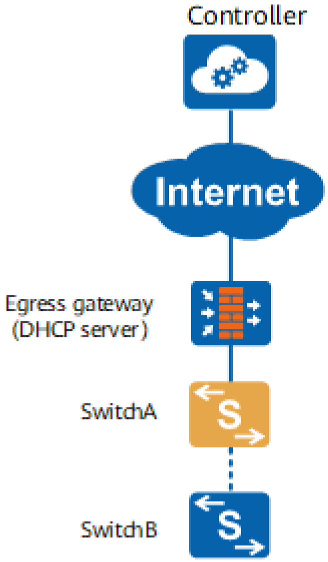
Usage Scenario

There are two types of PnP VLANs: wired and wireless PnP VLANs. Switches obtain management IP addresses through the wired PnP VLAN. When a switch has APs connected, the switch automatically changes the PVID of interfaces connected to the APs to the wireless PnP VLAN ID. For switches, PnP VLAN negotiation involves both wired and wireless PnP VLANs. The PnP VLAN applies to the following scenarios:

- **Scenario 1: All switches on a CloudCampus network can be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-6**, SwitchA and SwitchB are both switches. SwitchB is newly connected to the network when the VLAN for the IP address pool of the DHCP server is not VLAN 1. After SwitchB is connected to the network, by default, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of iMaster NCE-Campus. However, SwitchB fails to obtain the information because the VLAN for the IP address pool of the DHCP server is not VLAN 1.

Figure 16-6 CloudCampus networking



To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain related information from the DHCP server.

SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

- SwitchA has registered with iMaster NCE-Campus successfully.
- iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
- iMaster NCE-Campus has delivered the function of transmitting the PnP VLAN ID to the downstream device to SwitchA, and the configuration file contains the **pnp startup-vlan send enable** command.
- SwitchA is enabled to send LLDPDUs containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** or **undo lldp tlv-enable legacy-tlv pnp all** command, the function of sending LLDPDUs containing the PnP VLAN ID to the downstream device is disabled. You can enable the function on iMaster NCE-Campus.

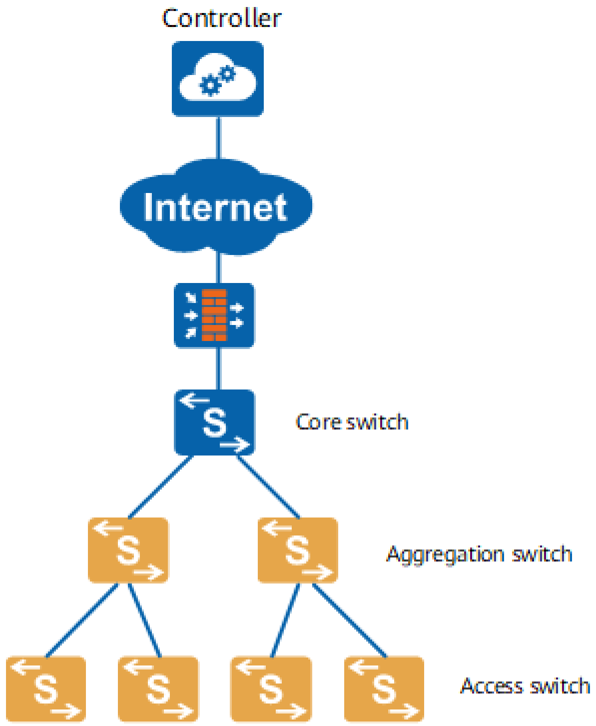
SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function on iMaster NCE-Campus.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on iMaster NCE-Campus and delivered to a switch after the switch has registered with iMaster NCE-Campus.

- **Scenario 2: On a CloudCampus network, some switches cannot be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-7**, the access and aggregation switches can be managed by iMaster NCE-Campus. The core switch is not managed by iMaster NCE-Campus. When the management VLAN is changed on iMaster NCE-Campus from VLAN 1 (default) to VLAN 2, the core switch needs to notify its downstream switches of the new management VLAN ID.

  Figure 16-7 CloudCampus networking



  Configure PnP VLAN auto-negotiation on the core switch so that the core switch can notify its downstream switches of the new management VLAN ID. This process consists of the following operations:

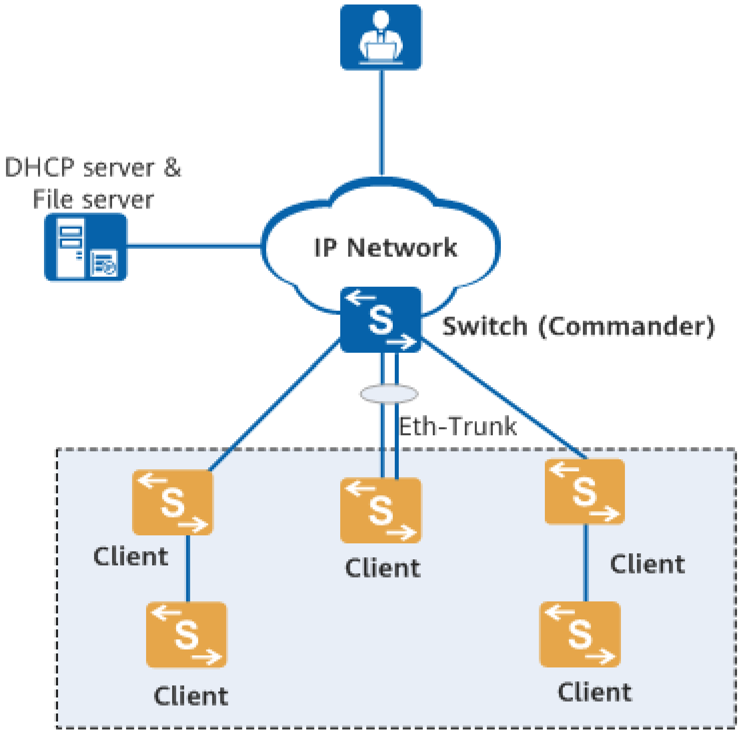
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices

of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

- **Scenario 3: Zero-touch deployment using EasyDeploy**

  In **Figure 16-8**, when EasyDeploy is used for zero touch deployment, the Commander needs to notify a client of the new VLAN ID if the Commander does not use VLAN 1 to communicate with the client.

Figure 16-8 EasyDeploy networking diagram



- Configure PnP VLAN auto-negotiation on the Commander to enable the Commander to notify clients of the new VLAN ID. This process consists of the following operations:
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

Precautions

- If the management VLAN of a switch is set to VLAN 1 through iMaster NCE-Campus or a command, the switch automatically goes online in the PNP VLAN. If the management VLAN configured through iMaster NCE-Campus or a command is not VLAN 1, the switch uses the management VLAN to send a request to the DHCP server. Even if the request fails, the switch does not use the PNP VLAN to send a request to the DHCP server. Therefore, ensure that the switch can communicate with the DHCP server through the management VLAN. Otherwise, the switch cannot go online.
- The wired PnP VLAN must have been created and cannot be the reserved VLAN of a stack, the control VLAN of RRPP/ERPS/SEP or the management VLAN of a CAPWAP tunnel in an SVF system.
- The wired and wireless PnP VLANs can be the same or different.
- If a wired PnP VLAN is configured and no wireless PnP VLAN is configured (using the **pnp wireless startup-vlan** command), the PVID of the interface connecting the switch to an AP is changed to the wired PnP VLAN.

Example

Configure the PnP VLAN ID.

```
<HUAWEI> system-view
[HUAWEI] pnp startup-vlan 2
```

16.15.31 pnp wireless startup-vlan

Function

The **pnp wireless startup-vlan** command configures a wireless PnP VLAN ID for APs.

The **undo pnp wireless startup-vlan** command deletes a wireless PnP VLAN ID.

By default, no wireless PnP VLAN ID is configured on a switch.

Format

pnp wireless startup-vlan *vlan-id*

undo pnp wireless startup-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a wireless PnP VLAN ID.	The value is an integer in the range 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a smart campus network, wired devices (such as switches) and wireless devices (such as APs) can use different management VLANs to facilitate maintenance and management. The wired and wireless devices can obtain management VLANs through the wired and wireless PnP VLANs, respectively.

- When all devices on the network can be managed by iMaster NCE-Campus, you can pre-configure wired and wireless PnP VLANs on iMaster NCE-Campus. After switches successfully register with iMaster NCE-Campus, iMaster NCE-Campus automatically delivers the wired and wireless PnP VLANs to the switches. When a switch identifies that the downstream device is an AP, it automatically changes the PVID of the interface connected to the AP to the wireless PnP VLAN ID and add the interface to the wireless PnP VLAN ID .
- If some switches on the network cannot be managed by iMaster NCE-Campus, you can manually configure wired and wireless PnP VLANs on these switches, which will deliver the PnP VLANs to downstream devices.

The device can obtain a wireless PnP VLAN in multiple ways. A wireless PnP VLAN configured using a command takes precedence over that negotiated with the upstream device. If no wireless PnP VLAN is specified or negotiated with the upstream devices, a wired PnP VLAN is used as a wireless PnP VLAN. To be specific, the device determines the PnP VLAN to be used as the wireless PnP VLAN in descending order of priority as follows:

1. Wireless PnP VLAN configured using the **pnp wireless startup-vlan** command
2. Wired PnP VLAN configured using the **pnp startup-vlan** command
3. Wireless PNP VLAN negotiated with the upstream device
4. Wired PnP VLAN negotiated with the upstream device

Precautions

- The VLAN used as the wireless PnP VLAN must have been created and cannot be the reserved VLAN of a stack, the control VLAN of RRPP/ERPS/SEP, or the management VLAN of a CAPWAP tunnel in an SVF system.
- The wired and wireless PnP VLANs can be the same or different.
- When a switch identifies that the downstream device is an AP, the switch adds the interconnection interface to the PnP VLAN. However, no corresponding configuration is added to the configuration file, and this interface cannot be removed from the PnP VLAN by manually adding the interface to the PnP VLAN and then removing the interface from the PnP VLAN.
- If a wired PnP VLAN is configured and no wireless PnP VLAN is configured (using the **pnp wireless startup-vlan** command), the PVID of the interface connecting the switch to an AP is changed to the wired PnP VLAN.

Example

Configure a wireless PnP VLAN ID.

```
<HUAWEI> system-view
[HUAWEI] pnp wireless startup-vlan 2
```

16.15.32 pnp startup-vlan receive enable

Function

The **pnp startup-vlan receive enable** command enables a switch to receive the PnP VLAN negotiation packets sent by its upstream device.

The **undo pnp startup-vlan receive enable** command disables a switch from receiving the PnP VLAN negotiation packets sent by its upstream device.

By default, a switch is enabled to receive the PnP VLAN negotiation packets from its upstream device.

Format

pnp startup-vlan receive enable

undo pnp startup-vlan receive enable

Parameters

None

Views

System view

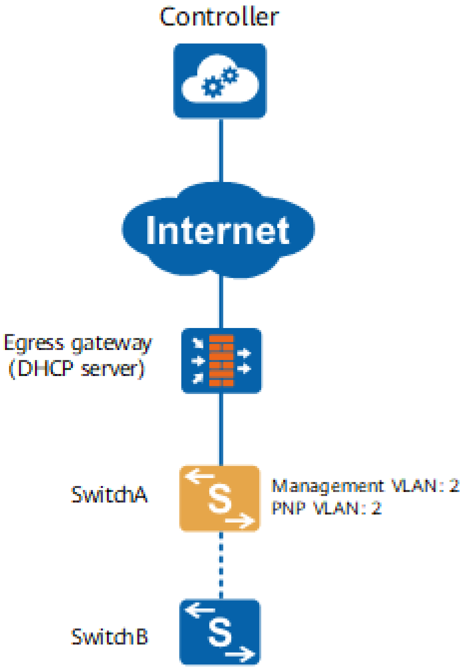
Default Level

2: Configuration level

Usage Guidelines

On a campus network shown in **Figure 16-9**, the VLAN for the IP address pool of the DHCP server is not VLAN 1 and SwitchB is newly connected to the network. After SwitchB is connected to the network, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of controller. The VLAN for the IP address pool of the DHCP server is not VLAN 1. As a result, SwitchB cannot obtain the related information.

Figure 16-9 Campus network diagram



To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain the related information from the DHCP server.

SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

- If NETCONF is enabled on SwitchA:
  - SwitchA has registered with iMaster NCE-Campus successfully.
  - iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
  - iMaster NCE-Campus has delivered to SwitchA the function of transmitting the PnP VLAN ID to its downstream device, and the configuration file contains the **pnp startup-vlan send enable** command.
  - SwitchA is enabled to send LLDP packets containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** command, the function of sending LLDP packets containing the PnP VLAN ID to the downstream device is disabled. You can enable the function on iMaster NCE-Campus.
- If NETCONF is not enabled on SwitchA:
  - SwitchA has a PnP VLAN ID configured using the **pnp startup-vlan** *vlan-id* command.
  - The **pnp startup-vlan send enable** command has been configured on SwitchA to transmit PnP VLAN information to its downstream device.
  - SwitchA is enabled to send LLDP packets containing PnP VLAN information to its downstream device. This function is enabled by default.

If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** command, the function of sending LLDP packets containing the PnP VLAN ID to the downstream device is disabled. You can run the **lldp tlv-enable legacy-tlv pnp startup-vlan** command to enable this function.

SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function by running **pnp startup-vlan receive enable** command.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on controller and delivered to a switch after the switch has registered with controller. If the switch does not register with controller, perform preconfiguration on the switch.

Example

Enable the downstream device to receive the PnP VLAN negotiation packets sent by the upstream device.

```
<HUAWEI> system-view
[HUAWEI] pnp startup-vlan receive enable
```

16.15.33 pnp startup-vlan send enable

Function

The **pnp startup-vlan send enable** command enables the device to transmit the PnP VLAN ID to its downstream device.

The **undo pnp startup-vlan send enable** command disables the device from transmitting the PnP VLAN ID to its downstream device.

By default, a switch does not transmit the PnP VLAN ID to its downstream device.

Format

pnp startup-vlan send enable

undo pnp startup-vlan send enable

Parameters

None

Views

System view

Default Level

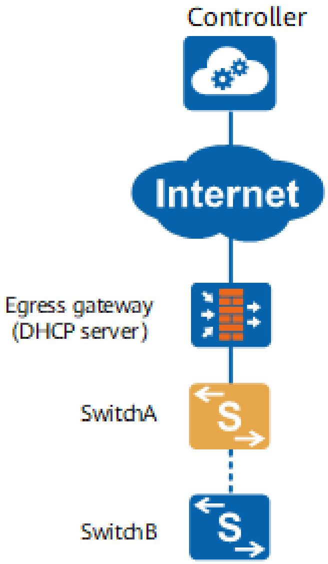
2: Configuration level

Usage Guidelines

- **Scenario 1: All switches on a CloudCampus network can be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-10**, SwitchA and SwitchB are both switches. SwitchB is newly connected to the network when the VLAN for the IP address pool of the DHCP server is not VLAN 1. After SwitchB is connected to the network, by default, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of iMaster NCE-Campus. However, SwitchB fails to obtain the information because the VLAN for the IP address pool of the DHCP server is not VLAN 1.

  Figure 16-10 CloudCampus networking

  To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain related information from the DHCP server.

  SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

  - SwitchA has registered with iMaster NCE-Campus successfully.
  - iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
  - iMaster NCE-Campus has delivered the function of transmitting the PnP VLAN ID to the downstream device to SwitchA, and the configuration file contains the **pnp startup-vlan send enable** command.
  - SwitchA is enabled to send LLDPDUs containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** or **undo lldp tlv-enable legacy-tlv pnp all** command, the function of sending LLDPDUs containing the PnP VLAN ID to the

downstream device is disabled. You can enable the function on iMaster NCE-Campus.

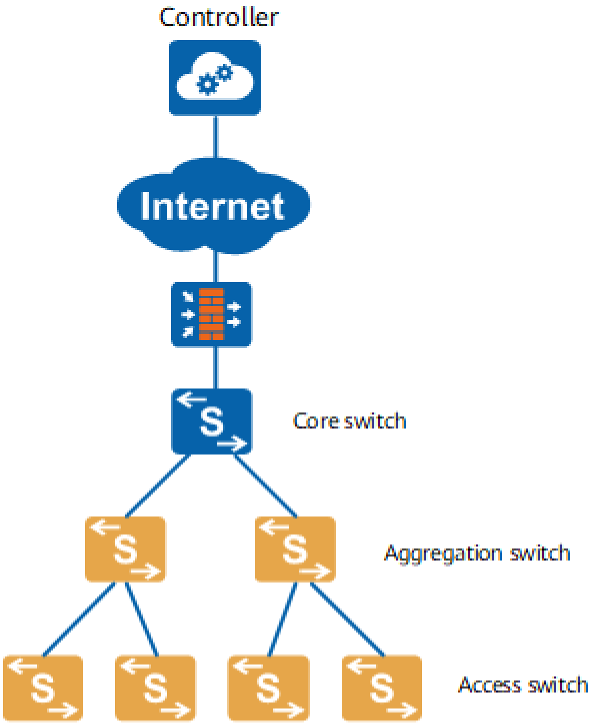
SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function on iMaster NCE-Campus.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on iMaster NCE-Campus and delivered to a switch after the switch has registered with iMaster NCE-Campus.

- **Scenario 2: On a CloudCampus network, some switches cannot be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-11**, the access and aggregation switches can be managed by iMaster NCE-Campus. The core switch is not managed by iMaster NCE-Campus. When the management VLAN is changed on iMaster NCE-Campus from VLAN 1 (default) to VLAN 2, the core switch needs to notify its downstream switches of the new management VLAN ID.

  Figure 16-11 CloudCampus networking



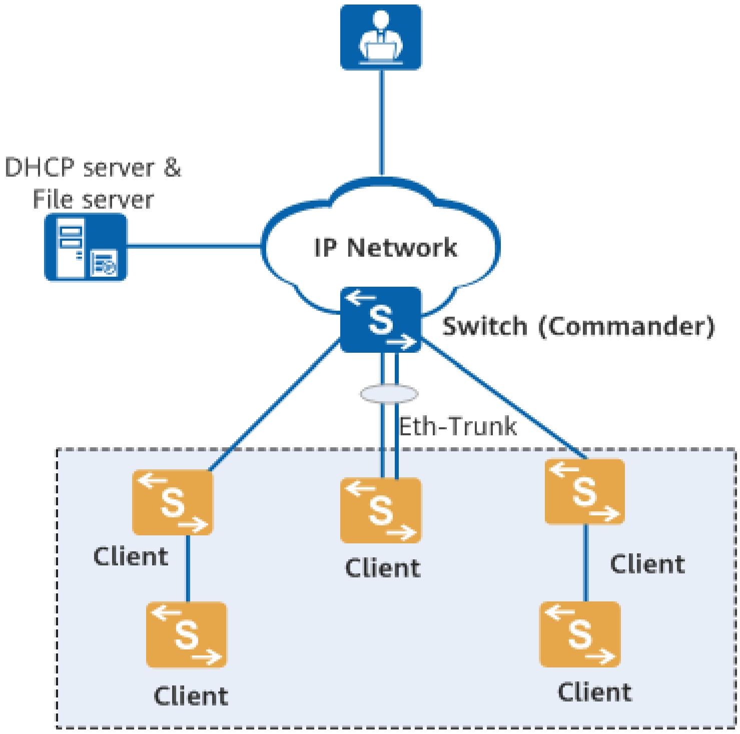
  Configure PnP VLAN auto-negotiation on the core switch so that the core switch can notify its downstream switches of the new management VLAN ID. This process consists of the following operations:

  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.

  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.
- **Scenario 3: Zero-touch deployment using EasyDeploy**

  In Figure 16-12, when EasyDeploy is used for zero touch deployment, the Commander needs to notify a client of the new VLAN ID if the Commander does not use VLAN 1 to communicate with the client.

  Figure 16-12 EasyDeploy networking diagram



- Configure PnP VLAN auto-negotiation on the Commander to enable the Commander to notify clients of the new VLAN ID. This process consists of the following operations:
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.

  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

Example

Enable a switch to transmit the PnP VLAN ID to its downstream devices.

```
<HUAWEI> system-view
[HUAWEI] pnp startup-vlan send enable
```

16.15.34 redirected-controller backup ip-address

Function

The **redirected-controller backup ip-address** command configures the redirected IP address and port number of the standby iMaster NCE-Campus.

The **undo redirected-controller backup ip-address** command deletes the redirected IP address and port number of the standby iMaster NCE-Campus.

By default, no redirected IP address and port number of the standby iMaster NCE-Campus are configured on a switch.

Format

redirected-controller backup ip-address *ip-address* **port** *port-number*

undo redirected-controller backup ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies a redirected IP address.	The value is in dotted decimal notation.
port *port-number*	Specifies a redirected port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Assume that a switch has successfully registered with iMaster NCE-Campus through DHCP. After a restart, the switch will use DHCP to obtain the IP address of iMaster NCE-Campus for registration. If you want the switch to use the IP address already obtained during the previous registration, fix the IP address on iMaster NCE-Campus. Then, iMaster NCE-Campus delivers this command to the switch, and the switch executes this command to save the IP address of iMaster NCE-Campus.

Precautions

- After a restart, the switch can obtain the address of iMaster NCE-Campus using different methods (listed in descending order of priority): configured in the callhome template view on the switch, from the redirection information of iMaster NCE-Campus configured on the switch, through DHCP, using commands, or in the registration query center.
- When the following conditions are met, a switch regenerate the redirection configuration command: (1) iMaster NCE-Campus delivers redirection information to the switch to fix the IP address of iMaster NCE-Campus on the switch; (2) the **undo redirected-controller backup ip-address** command is run on the switch to delete redirection information ; (3) the configuration is saved and the switch is restarted.

Example

Configure the redirected IP address and port number of the standby iMaster NCE-Campus on a switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] redirected-controller backup ip-address 10.1.1.2 port 10020
```

16.15.35 redirected-controller ip-address

Function

The **redirected-controller ip-address** command configures the redirection IP address and port number of iMaster NCE-Campus.

The **undo redirected-controller ip-address** command deletes the redirection IP address and port number of iMaster NCE-Campus.

By default, no redirection IP address and port number are configured for iMaster NCE-Campus on a switch.

Format

redirected-controller ip-address *ip-address* **port** *port-number*

undo redirected-controller ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the redirection IP address.	The value is in dotted decimal notation.
port *port-number*	Specifies the redirection port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Assume that a switch has successfully registered with iMaster NCE-Campus through DHCP. After a restart, the switch will use DHCP to obtain the IP address of iMaster NCE-Campus for registration. If you want the switch to use the IP address already obtained during the previous registration, fix the IP address on iMaster NCE-Campus. Then, iMaster NCE-Campus delivers this command to the switch, and the switch executes this command to save the IP address of iMaster NCE-Campus.

Precautions

- After a restart, the switch can obtain the address of iMaster NCE-Campus using different methods (listed in descending order of priority): configured in the callhome template view on the switch, from the redirection information of iMaster NCE-Campus configured on the switch, through DHCP, using commands, or in the registration query center.
- When the following conditions are met, a switch regenerate the redirection configuration command: (1) iMaster NCE-Campus delivers redirection information to the switch to fix the IP address of iMaster NCE-Campus on the switch; (2) the **undo redirected-controller ip-address** command is run on the switch to delete redirection information ; (3) the configuration is saved and the switch is restarted.

Example

Configure the redirection IP address and port number of iMaster NCE-Campus on the switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] redirected-controller ip-address 10.1.1.2 port 10020
```

16.15.36 reset cloud-mng work-mode

Function

The **reset cloud-mng work-mode** command clears the cloud-based management flag in the flash memory of a switch.

Format

reset cloud-mng work-mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Since V200R019C00, you no longer need to change the working mode of a switch to cloud-mng to implement cloud-based management. Instead, you can enable NETCONF on the switch to implement cloud-based management. However, after a switch working in cloud-mng mode is upgraded from an earlier version to V200R019C10 or a later version, the cloud-based management flag still exists in the flash memory of the switch. As a result, the LNP, VCMP, and OPS functions do not take effect.

To resolve this problem, run the **reset cloud-mng work-mode** command to clear the cloud-based management flag in the flash memory of the switch.

- When you run the **undo netconf** command on a switch that originally worked in cloud-mng mode before the upgrade, the following message is displayed to prompt you to run the **reset cloud-mng work-mode** command to restore the LNP, VCMP, and OPS functions:
  ```
  Info: After the device is upgraded in cloud management mode, execute 'reset cloud-mng work-mode'
  to restore the LNP, VCMP, and OPS functions.
  ```
  When you run the **reset cloud-mng work-mode** command, the switch displays the following message indicating that this operation will delete the saved configuration and the device will restart. Exercise caution when performing this operation.
  ```
  Warning: The action will delete the saved configuration and reboot. Continue? [Y/N]:
  ```
- When you run the **reset cloud-mng work-mode** command on a switch that did not work in cloud-mng mode before the upgrade, the following message is displayed indicating that this operation is not required:
  ```
  Info: Current status is not upgrade from Cloud-mng mode.
  ```

Example

Clear the cloud-based management flag in the flash memory of a switch.

```
<HUAWEI> reset cloud-mng work-mode
```

16.15.37 reset netconf db-configuration

Function

The **reset netconf db-configuration** command clears the database configuration.

Format

reset netconf db-configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To stop providing network services, run the **reset netconf db-configuration** command to clear all database configuration.

Precautions

After the **reset netconf db-configuration** or **reset saved-configuration** command is run, the **assign trunk** command configuration is cleared, that is, the default configuration is restored.

NOTICE

After the **reset netconf db-configuration** command is executed, the system asks whether you want to restart the switch. If you enter Y, the switch restarts and clears all the database and configuration file information. Confirm your action.

Example

Clear the database configuration on a switch.

```
<HUAWEI> system-view
[HUAWEI] reset netconf db-configuration
```

```
Warning: This operation will clear the database and saved configuration and restart the device. Continue?
[Y/N]:
```

16.15.38 reset netconf register-fail-record

Function

The **reset netconf register-fail-record** command clears records about failed registrations with iMaster NCE-Campus.

Format

reset netconf register-fail-record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **reset netconf register-fail-record** command to clear records about failed registries with iMaster NCE-Campus. Confirm the action before running this command.

Example

Clear records about failed registrations with iMaster NCE-Campus.

```
<HUAWEI> reset netconf register-fail-record
Warning: This command will clear the registration failures. Continue? [Y/N]: y
```

16.15.39 { rsa | dsa } local-key-pair create (NETCONF view)

Function

The **{ rsa | dsa } local-key-pair create** command creates a local RSA or DSA key pair.

Format

{ rsa | dsa } local-key-pair create

Parameters

Parameter	Description	Value
rsa	Creates a local RSA key pair.	-
dsa	Creates a local DSA key pair.	-

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

You can run this command to create a local RSA or DSA key pair. If the local RSA or DSA key pair already exists, the system displays a message asking you whether to create a new one.

Example

Create a local DSA key pair.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] dsa local-key-pair create
```

16.15.40 set netconf db-configuration-file

Function

The **set netconf db-configuration-file** command configures a NETCONF database file used by the system.

NOTE

This command is supported only in scenarios where the device is registered with iMaster NCE-Campus.

Format

set netconf db-configuration-file *database-file*

Parameters

Parameter	Description	Value
database-file	Specifies a database file. The file must already exist. **NOTE** You must specify a database file in the **flash:/** directory on the active device.	The value is a string of 5 to 64 characters in the format of [*drive-name*] [*file-name*]. It cannot contain spaces. - If *drive-name* is not specified, the default flash memory name is used. - The value of *file-name* cannot contain special characters including | ; & $ < > ' ! \ and must use .rdb as the file name extension.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the database file is abnormal due to misoperations or system exceptions, you can run the **set netconf db-configuration-file** command to manually specify a valid database file. To view the currently effective database file, run the **display netconf configuration** command.

NOTICE

When you run this command, the system displays a message indicating that the device will be disconnected from iMaster NCE-Campus for a short period of time. After you enter **Y**, the device is disconnected for a short period of time and then reconnects to iMaster NCE-Campus. Therefore, exercise caution when running this command.

Prerequisites

The configurations in the database file must be the same as those in the configuration file. Therefore, before running this command, configure the corresponding configuration file and make it take effect by using one of the following methods:

- Run the **startup saved-configuration** command to configure the configuration file used by the system, and then restart the system for the configuration file to take effect. You are advised to use the backup configuration file in the backup directory.
- Manually supplement configurations in the configuration file and make the configurations take effect.

Precautions

- When you run this command to configure a database file, the system checks the file content. If the file content is invalid, the command configuration fails and the configurations in the configuration file may be lost. To ensure validity of the database file, you are advised to use the backup database file.
- The database file specified in this command cannot exceed 30 MB or be named **startup.rdb**. Otherwise, the configuration fails.
- This command cannot be executed repeatedly in a short period of time.

Example

Specify **2022-06-23_startup.rdb** as the system datastore file.

```
<HUAWEI> set netconf db-configuration-file configbackup/2022-06-23_startup.rdb
Warning: Configure the corresponding CFG file first. This operation will activate the database configuration
file and make the device go offline for a short period of time, Continue? [Y/
N]:y
Info: The operation is in progress. Please wait........................Done.
```

16.15.41 source ip

Function

The **source ip** command configures the IPv4 address and port number used by a switch to communicate with the NMS through NETCONF.

The **undo source ip** command deletes the IPv4 address and port number used by a switch to communicate with the NMS through NETCONF.

By default, no IPv4 address and port number are configured for a switch to communicate with the NMS through NETCONF.

Format

source ip { *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* } [**port** *port-number*]

undo source ip

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a switch.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which the IPv4 address or interface of the switch belongs.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the interface to which the IPv4 address used by the switch belongs.	The interface must be an existing Layer 3 interface on the switch. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.
port *port-number*	● This parameter is the port number used by the switch in NETCONF over SSH Callhome mode. ● This parameter is the port number used by both the switch and NMS in NETCONF over SSH mode.	The value is 830 or an integer in the range 55552 to 55807. The default value is 830.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch using NETCONF, run the **source ip** command to configure the IPv4 address and port number used by the switch to communicate with the NMS, regardless of whether the NETCONF over SSH or NETCONF over SSH Callhome mode is used.

Precautions

- You cannot run this command if you have run the **source ip-address** command in the SMI view to configure the IPv4 address used by the switch to communicate with an NMS (for example, iMaster NCE-CampusInsight).

- When you run the **source ip** command to configure or change the port number for IPv4 communication between the switch and NMS, the port number for IPv6 communication between the two systems configured using the **source ipv6-address** command will be changed accordingly.
- Changing the IPv4 address or port number will cause communication interruption between the switch and NMS.

Example

Set the IPv4 address and port number used by the switch to communicate with the NMS through NETCONF to 10.1.1.1 and 55555, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] source ip 10.1.1.1 port 55555
```

16.15.42 source ipv6-address

Function

The **source ipv6-address** command configures the IPv6 address and port number used by a switch to communicate with the NMS through NETCONF.

The **undo source ipv6-address** command deletes the IPv6 address and port number used by a switch to communicate with the NMS through NETCONF.

By default, no IPv6 address and port number are configured for a switch to communicate with the NMS using NETCONF.

Format

source ipv6-address { *ipv6-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* } [**port** *port-number*]

undo source ipv6-address

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a switch.	The total length of the value is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format of X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which the IPv6 address or interface of the switch belongs.	The value must be an existing VPN instance name.

Parameter	Description	Value
interface *interface-type* *interface-number*	Specifies the interface to which the IPv6 address used by the switch belongs.	The interface must be an existing Layer 3 interface on the switch. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.
port *port-number*	Specifies the port number used by the switch and NMS.	The value is 830 or an integer in the range 55552 to 55807. The default value is 830.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch using an IPv6 address in NETCONF over SSH mode, run the **source ipv6-address** command to configure the IPv6 address and port number of the switch.

Precautions

When you run the **source ipv6-address** command to configure or change the port number for IPv6 communication between the switch and NMS, the port number for IPv4 communication between the two systems configured using the **source ip** command will be changed accordingly.

Changing the IPv6 address or port number will cause communication interruption between the switch and NMS.

Example

Set the IPv6 address and port number used by the switch to communicate with the NMS through NETCONF to FC00::1 and 55555, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] source ipv6-address FC00::1 port 55555
```

16.15.43 user assign { rsa | dsa } public-key

Function

The **user** *user-name* **assign { rsa | dsa } public-key public-key-name** command assigns an existing RSA or DSA public key to a specified user.

The **undo user** *user-name* **assign { rsa | dsa } public-key** command deletes the mapping between a user and an RSA or DSA public key.

By default, no RSA or DSA public key is assigned to a user.

Format

user *user-name* **assign { rsa | dsa } public-key** *public-key-name*

undo user *user-name* **assign { rsa | dsa } public-key**

Parameters

Parameter	Description	Value
user-name	Specifies a NETCONF user name.	The value is a string of 1 to 25 case-insensitive characters without spaces. **NOTE** If the string is enclosed in quotation marks, the string can contain spaces.
rsa	Assigns an RSA public key to a specified user.	-
dsa	Assigns a DSA public key to a specified user.	-
public-key-name	Specifies the name of an RSA or DSA public key.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** If the string is enclosed in double quotation marks ("), the string can contain spaces.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

When a controller acting as a NETCONF client needs to log in to the switch acting as the NETCONF server in RSA or DSA mode, you can run this command to assign an RSA or DSA public key to a specified user. If multiple public keys are assigned to a user, the last assigned public key takes effect.

Example

Assign the DSA public key **key1** to the NETCONF user named **test123**.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] user test123 assign dsa public-key key1
```

16.16 O&M information reporting Configuration Commands

16.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.16.2 collect dynamic mac disable

Function

The **collect dynamic mac disable** command disables the device from reporting dynamic MAC address information to an NMS.

The **undo collect dynamic mac disable** command enables the device to report dynamic MAC address information to an NMS.

By default, the function of reporting dynamic MAC address information to an NMS is enabled in the system view, but not the interface view.

Format

collect dynamic mac disable

undo collect dynamic mac disable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, Multi-GE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After being connected to an NMS (for example, a controller or analyzer), the device also reports information about online users who go online after successful authentication or without authentication to NMS. The information about users who go online without authentication includes dynamic MAC addresses learned by the device. Layer 2 network devices usually learn a large number of dynamic MAC addresses, which will be sent to the NMS if the **collect-item user-data enable** command is configured. As a result, large amounts of resources on the NMS will be occupied. To reduce the usage of NMS resources, you can run the **collect dynamic mac disable** command to disable the device from reporting dynamic MAC address information to the NMS.

Precautions

- The device reports dynamic MAC address information to an NMS only when the **undo collect dynamic mac disable** command is run in both the system view and interface view.
- This command does not take effect on the device's interface connected to the NMS.
- In a policy association scenario, ASs cannot report dynamic MAC address information to the NMS.

Example

Disable all interfaces on the device from reporting dynamic MAC address information to the NMS.

```
<HUAWEI> system-view
[HUAWEI] collect dynamic mac disable
```

16.16.3 collect-item enable (SMI view)

Function

The **collect-item enable** command enables the switch to report collected information to iMaster NCE-CampusInsight.

The **undo collect-item enable** command disables the switch from reporting collected information to iMaster NCE-CampusInsight.

By default, the switch does not report any collected information to iMaster NCE-CampusInsight.

Format

collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** | **media-quality** | **application-statistics-data** | **sipfpm-data** } **enable**

undo collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** | **media-quality** | **application-statistics-data** | **sipfpm-data** } **enable**

Parameters

Parameter	Description	Value
device-data	Enables the switch to report device data to iMaster NCE-CampusInsight.	-
fiber-module	Enables the switch to report optical module information to iMaster NCE-CampusInsight.	-
poe	Enables the switch to report PoE data to iMaster NCE-CampusInsight.	-
user-data	Enables the switch to report traffic statistics collection of wired users to iMaster NCE-CampusInsight.	-
device-status	Enables the switch to report device status information to iMaster NCE-CampusInsight.	-
media-quality	Enables the switch to report application-based poor-QoE monitoring information, audio, and video data to iMaster NCE-CampusInsight.	-
application-statistics-data	Enables the switch to report application traffic statistics to iMaster NCE-CampusInsight.	Only the following models support this parameter: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S
sipfpm-data	Enables the switch to report packet loss and delay measurement information to iMaster NCE-CampusInsight.	-

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Based on your networking requirements, you can enable the switch to report collected information to iMaster NCE-CampusInsight. You can run this command for multiple times to enable the switch to report different types of data to iMaster NCE-CampusInsight. For details about the information that can be collected, see KPI.

Example

Enable the switch to report optical module information to iMaster NCE-CampusInsight.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] collect-item fiber-module enable
```

16.16.4 collect-item interval (SMI view)

Function

The **collect-item interval** command sets the interval at which the switch collects KPI information.

The **undo collect-item interval** command restores the default interval at which the switch collects KPI information.

By default, the interval for collecting KPI information about the total number of bad blocks in the NAND flash and the total number of erase times in the NOR flash is 60 minutes, and the interval for collecting other KPI information is 5 minutes.

Format

collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** } **interval** *interval*

undo collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** } **interval**

Parameters

Parameter	Description	Value
device-data	Enables the switch to report device data to iMaster NCE-CampusInsight.	-
fiber-module	Enables the switch to report optical module information to iMaster NCE-CampusInsight.	-

Parameter	Description	Value
poe	Enables the switch to report PoE data to iMaster NCE-CampusInsight.	-
user-data	Enables the switch to report traffic statistics collection of wired users to iMaster NCE-CampusInsight.	-
device-status	Enables the switch to report device status information to iMaster NCE-CampusInsight.	-
interval *interval*	Specifies the interval at which the switch collects KPI information.	The value is an integer in the range from 1 to 1440, in minutes.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Based on your networking requirements, you can set the interval at which the switch collects KPI information. For details about the information that can be collected, see KPI.

Example

Enable the switch to report optical module information to the iMaster NCE-CampusInsightand set the interval at which the switch collects such information to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] collect-item fiber-module enable
[HUAWEI-smi-server] collect-item fiber-module interval 3
```

16.16.5 collect-item syslog enable (SMI view)

Function

The **collect-item syslog enable** command configures the device to report logs and alarms to an NMS.

The **undo collect-item syslog enable** command disables the device from reporting logs and alarms to an NMS.

By default, the device does not report logs and alarms to an NMS.

Format

collect-item syslog { **aaa** | **acl** | **am** | **arp** | **basetrap** | **bgp** | **defd** | **dhcp** | **dldp** | **dot1x** | **efm** | **emdi** | **entitytrap** | **errdown** | **gtl** | **ifnet** | **ifpdt** | **ipca** | **l2ifppi** | **l3adp** | **lbdt** | **mcast** | **mpls** | **mstp** | **nac** | **nvo3** | **ospf** | **poe** | **portal** | **rumng** | **ruupgrade** | **sea** | **sece** | **shell** | **srm** | **web** | **gtl** | **qose** | **entityexttrap** | **fsp** | **mad** } **enable**

undo collect-item syslog { **aaa** | **acl** | **am** | **arp** | **basetrap** | **bgp** | **defd** | **dhcp** | **dldp** | **dot1x** | **efm** | **emdi** | **entitytrap** | **errdown** | **gtl** | **ifnet** | **ifpdt** | **ipca** | **l2ifppi** | **l3adp** | **lbdt** | **mcast** | **mpls** | **mstp** | **nac** | **nvo3** | **ospf** | **poe** | **portal** | **rumng** | **ruupgrade** | **sea** | **sece** | **shell** | **srm** | **web** | **am** | **qose** | **entityexttrap** | **fsp** | **mad** } **enable**

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can report data of the eMDI and iPCA modules to an NMS.

Parameters

Parameter	Description	Value
aaa	Configures the device to report data of the AAA module to an NMS.	-
acl	Configures the device to report data of the ACL module to an NMS.	-
am	Configures the device to report data of the AM module to an NMS.	-
basetrap	Configures the device to report data of the BASETRAP module to an NMS.	-
bgp	Configures the device to report data of the BGP module to an NMS.	-
defd	Configures the device to report data of the DEFD module to an NMS.	-
dhcp	Configures the device to report data of the DHCP module to an NMS.	-
dldp	Configures the device to report data of the DLDP module to an NMS.	-
dot1x	Configures the device to report data of the DOT1X module to an NMS.	-

Parameter	Description	Value
efm	Configures the device to report data of the EFM module to an NMS.	-
emdi	Configures the device to report data of the eMDI module to an NMS.	-
entitytrap	Configures the device to report data of the ENTITYTRAP module to an NMS.	-
errdown	Configures the device to report data of the ErrorDown module to an NMS.	-
gtl	Configures the device to report data of the GTL module to an NMS.	-
ifnet	Configures the device to report data of the IFNET module to an NMS.	-
ifpdt	Configures the device to report data of the IFPDT module to an NMS.	-
ipca	Configures the device to report data of the iPCA module to an NMS.	-
l2ifppi	Configures the device to report data of the L2IFPPI module to an NMS.	-
l3adp	Configures the device to report data of the L3MB module to an NMS.	-
lbdt	Configures the device to report data of the LBDT module to an NMS.	-
mcast	Configures the device to report data of the MCAST module to an NMS.	-
mpls	Configures the device to report data of the MPLS module to an NMS.	-
mstp	Configures the device to report data of the MSTP module to an NMS.	-
nac	Configures the device to report data of the NAC module to an NMS.	-

Parameter	Description	Value
nvo3	Configures the device to report data of the NVO3 module to an NMS.	-
ospf	Configures the device to report data of the OSPF module to an NMS.	-
poe	Configures the device to report data of the PoE module to an NMS.	-
portal	Configures the device to report data of the Portal module to an NMS.	-
qose	Configures the device to report data of the QoS module to an NMS.	-
rumng	Configures the device to report data of the RUMNG module to an NMS.	-
ruupgrade	Configures the device to report data of the RUUPGRADE module to an NMS.	-
sea	Configures the device to report data of the SEA module to an NMS.	-
sece	Configures the device to report data of the SECE module to an NMS.	-
shell	Configures the device to report data of the SHELL module to an NMS.	-
srm	Configures the device to report data of the SRM module to an NMS.	-
web	Configures the device to report data of the WEB module to an NMS.	-
entityexttrap	Configures the device to report data of the ENTITYEXTTRAP module to an NMS.	-
arp	Configures the device to report data of the ARP module to an NMS.	-
fsp	Configures the device to report data of the FSP module to an NMS.	-

Parameter	Description	Value
mad	Configures the device to report data of the MAD module to an NMS.	-

Views

SMI view

Default Level

3: Management level

Usage Guidelines

You can run this command to configure the device to report logs and alarms to an NMS. You can run the command multiple times to configure the device to report multiple types of data to the NMS. For the device information that can be collected, see Logs and Alarms.

Example

Configure the device to report data of the ACL module to an NMS.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] collect-item syslog acl enable
```

16.16.6 keepalive (SMI view)

Function

The **keepalive** command configures connection parameters between the switch and iMaster NCE-CampusInsight.

The **undo keepalive** command restores the default settings of connection parameters between the switch and iMaster NCE-CampusInsight.

By default, the switch and iMaster NCE-CampusInsight send heartbeat packets to each other at an interval of 5 minutes, the switch reconnects to iMaster NCE-CampusInsight at an interval of 5 minutes, and the maximum number of reconnection attempts is 0.

Format

keepalive { **interval** *interval* | **retry-interval** *retry-interval* | **retry-number** *retry-number* } *

undo keepalive { **interval** | **retry-interval** | **retry-number** } *

Parameters

Parameter	Description	Value
interval *interval*	Sets the interval at which the switch and iMaster NCE-CampusInsight send heartbeat packets to each other.	The value is an integer in the range from 5 to 60, in minutes.
retry-interval *retry-interval*	Sets the interval at which the switch reconnects to iMaster NCE-CampusInsight after port disconnection for the first time.	The value is an integer in the range from 5 to 60, in minutes.
retry-number *retry-number*	Sets the maximum number of attempts the switch reconnects to iMaster NCE-CampusInsight after port disconnection for the first time.	The value is an integer in the range from 0 to 10. The default value is 0, which indicates that the switch attempts to reconnect to iMaster NCE-CampusInsight until the reconnection succeeds.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

According to the network stability, you can adjust connection parameters between the switch and iMaster NCE-CampusInsight as required, such as the interval at which the switch and iMaster NCE-CampusInsight send heartbeat packets to each other and the maximum number of reconnection attempts. If the network condition is poor, set the maximum number of reconnection attempts to a smaller value and the reconnection interval to a large value to consume less network resources.

Example

Set the interval at which the switch reconnects to iMaster NCE-CampusInsight to 10 minutes and the maximum number of reconnection attempts to 5.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] keepalive retry-interval 10 retry-number 5
```

16.16.7 max-packet-size (SMI view)

Function

The **max-packet-size** command sets the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight.

The **undo max-packet-size** command restores the default maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight.

By default, the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight is 5 KB.

Format

max-packet-size *size*

undo max-packet-size

Parameters

Parameter	Description	Value
size	Specifies the maximum packet size.	The value is an integer in the range from 5 to 15, in KB.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

According to the network condition, you can run this command to set the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight. If the network condition is poor, set the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight to a smaller value to reduce packet loss.

Example

Set the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight to 10 KB.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] max-packet-size 10
```

16.16.8 monitor application name

Function

The **monitor application name** command enables application-based poor-QoE monitoring for a specified application.

The **undo monitor application name** command disables application-based poor-QoE monitoring.

By default, application-based poor-QoE monitoring is disabled for an application.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

monitor application name *appname*

undo monitor application name *appname*

Parameters

Parameter	Description	Value
appname	Specifies the name of an application.	The value is a string of characters. The value depends on the applications supported in the signature database. To check the supported application names, run the **display application** command.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor the quality of applications, you can configure the application-based poor-QoE monitoring function. After this function is configured, the device reports the application quality at a specific statistical interval. Application-based poor-QoE monitoring information reporting supports applications that use TCP or UDP-RTP as well as user-defined applications. Poor-QoE monitoring information can be reported for the following applications that use UDP-RTP: Skype_VoIP (Skype multimedia chat), Fetion_VoIP (Fetion multimedia chat), RTP, WhatsAPP, eSpace_VoIP (eSpace multimedia chat), WeLink_VideoCall (WeLink video call), Microsoft Teams, WebEx_VoIP (WebEx multimedia chat), and Hangouts.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Precautions

When poor-QoE monitoring based on users and applications has been configured using the **monitor source ucl-group** command, you cannot run the **monitor application name** command to configure application-based poor-QoE monitoring.

Example

Enable application-based poor-QoE monitoring for the application named **RTP**.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] monitor application name RTP
```

16.16.9 monitor application period

Function

The **monitor application period** command configures an application-based poor-QoE monitoring interval.

The **undo monitor application period** command restores the default application-based poor-QoE monitoring interval.

By default, the application-based poor-QoE monitoring interval is 10 seconds.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

monitor application period *period-value*

undo monitor application period

Parameters

Parameter	Description	Value
period-value	Specifies the maximum packet size.	The value is of the enumerated type, and can only be 2, 5, 10, 30, and 60, in seconds.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the application-based poor-QoE monitoring interval based on your network conditions. To obtain the application quality in a timely manner, you can configure a small monitoring interval.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Example

Set the application-based poor-QoE monitoring interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] monitor application period 30
```

16.16.10 monitor source ucl-group

Function

The **monitor source ucl-group** command is used to configure poor-QoE monitoring based on users or users and applications.

The **undo monitor source ucl-group** command deletes the configuration of poor-QoE monitoring based on users or users and applications.

By default, poor-QoE monitoring based on users or users and applications is not configured.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

monitor source ucl-group { *group-index* | **name** *group-name* } [**application name** *appname*]

undo monitor source ucl-group { *group-index* | **name** *group-name* } [**application name** *appname*]

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer in the range from 1 to 64000.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.
application name *appname*	Specifies the name of an application.	The value is a string of characters. The value depends on the applications supported in the signature database. To check the supported application names, run the **display application** command. A maximum of 16 application names can be configured at a time.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the intelligent O&M solution, the administrator wants to obtain information about the network quality experienced by users. A campus network has a large number of access users. During user access authentication, users with the same network access rights are added to the same UCL group. In this way, user-based network quality monitoring can be implemented based on the UCL group.

After you run this command to configure poor-QoE monitoring based on UCL groups or UCL groups and applications, the device periodically reports quality information about users or users and applications to the NMS.

Pre-configuration Tasks

The **emdi** command has been run to enable the eMDI function.

Precautions

- Poor-QoE monitoring can be performed for a maximum of 128 UCL groups.
- After you run the **monitor application name** command to perform poor-QoE monitoring on an application, you cannot run this command to perform poor-QoE monitoring based on users and applications.

Example

Configure poor-QoE monitoring for users in UCL group 10.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] monitor source ucl-group 10
```

16.16.11 report-interval (SMI view)

Function

The **report-interval** command sets the interval at which the switch reports KPI information to iMaster NCE-CampusInsight.

The **undo report-interval** command restores the default interval at which the switch reports KPI information to iMaster NCE-CampusInsight.

By default, the switch reports KPI information to iMaster NCE-CampusInsight at an interval of 1 minute.

Format

report-interval *interval*

undo report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the switch reports KPI information to iMaster NCE-CampusInsight.	The value is an integer in the range from 1 to 5, in minutes.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

According to the actual device and network resource usage and iMaster NCE-CampusInsight's requirements for the information collection precision, you can run this command to set the interval at which the switch reports KPI information to iMaster NCE-CampusInsight. A shorter interval indicates that KPI information is reported more frequently, the information collection precision is higher, and more device and network resources are occupied. A longer interval signifies that less information is collected by the switch within the same time period, the information collection precision is lower, but less device and network resources are occupied.

Example

Set the interval at which the switch reports KPI information to iMaster NCE-CampusInsight to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] report-interval 5
```

16.16.12 rtp-media monitor-period

Function

The **rtp-media monitor-period** command sets the monitoring period of media streams.

The **undo rtp-media monitor-period** command restores the default monitoring period of media streams.

By default, the monitoring period of media streams is 10 seconds.

Format

rtp-media monitor-period *period-value*

undo rtp-media monitor-period [*period-value*]

Parameters

Parameter	Description	Value
period-value	Specifies the monitoring period of media streams.	The value is of the enumerated type, and can only be 10, 30, and 60, in seconds.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor service quality of voice and video applications transported over RTP, run the **sea** command to enable the SEA function to detect SIP sessions, and use the eMDI function to detect dynamic indicators of RTP streams. To adjust the monitoring period of media streams, run the **rtp-media monitor-period** command.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Example

Set the monitoring period of media streams to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] rtp-media monitor-period 30
```

16.16.13 rtp-media monitor-type

Function

The **rtp-media monitor-type** command sets the type of media streams to be monitored.

The **undo rtp-media monitor-type** command deletes the type of media streams to be monitored.

By default, the type of media streams to be monitored is not configured.

Format

rtp-media monitor-type { **audio** | **video** } *

undo rtp-media monitor-type { **audio** | **video** } *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **video**.

Parameters

Parameter	Description	Value
audio	Sets the type of media streams to be monitored to audio.	-
video	Sets the type of media streams to be monitored to video.	-

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor service quality of audio and video applications transported over RTP in real time, you must run the **rtp-media monitor-type** command to set the type of media streams to be monitored after enabling the SEA function using the **sea** command.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Precautions

O&M information reporting for audio and video services takes effect only for unencrypted SIP packets without any tunnel header in IPv4 scenarios.

Example

Set the type of media streams to be monitored to audio.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] rtp-media monitor-type audio
```

16.16.14 sea

Function

The **sea** command enables the service experience analysis (SEA) function for users and applications and displays the SEA view.

The **undo sea** command disables the SEA function and deletes the SEA view.

By default, the SEA function is disabled.

Format

sea

undo sea

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor the quality of applications (such as audio and video applications) in real time during intelligent O&M of campus networks, run the **sea** command to enable the SEA function.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Follow-up Procedure

Run the **rtp-media monitor-type** { **audio** | **video** } * command to configure the type of media streams to be monitored or run the **monitor application name** *appname* command enables application-based poor-QoE monitoring for a specified application.

Example

Enable the SEA function and display the SEA view.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea]
```

16.16.15 server backup ip-address (SMI view)

Function

The **server backup ip-address** command configures the IPv4 address and port number of the standby analyzer connected to a switch.

The **undo server backup ip-address** command deletes the IPv4 address and port number of the standby analyzer connected to the switch.

By default, no standby analyzer's IPv4 address and port number are configured.

Format

server backup ip-address *ip-address* [**port** *port-number*]

undo server backup ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the standby analyzer.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port-number*	Specifies the port number of the standby analyzer.	The value is an integer in the range from 0 to 65535. The default value is 0.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you configure analyzers connected to a switch for intelligent O&M, you can run the **server backup ip-address** command to configure the IPv4 address and port number of the standby analyzer. When the active analyzer breaks down or is disconnected, services can be automatically switched to the standby analyzer, ensuring service continuity.

Prerequisites

The IPv4 address of the active analyzer connected to the switch has been configured using the **server ip-address** command.

Precautions

There is no limitation on the sequence in which you delete the active and standby analyzer configurations.

Example

Configure the IPv4 address and port number of the standby analyzer.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] server ip-address 1.1.1.1 port 111
[HUAWEI-smi-server] server backup ip-address 2.2.2.2 port 222
```

16.16.16 server ip-address (SMI view)

Function

The **server ip-address** command configures the IPv4 address and port number of connected iMaster NCE-CampusInsight.

The **undo server ip-address** command deletes the IPv4 address and port number of connected iMaster NCE-CampusInsight.

By default, the IPv4 address and port number of connected iMaster NCE-CampusInsight are not configured on the switch.

Format

server ip-address *ip-address* [**port** *port-number*]

undo server ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of iMaster NCE-CampusInsight.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of iMaster NCE-CampusInsight.	The value is an integer in the range from 0 to 65535. The default value is 0.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

To implement intelligent O&M, the switch needs to establish a NETCONF connection with iMaster NCE-CampusInsight and periodically reports KPI information to iMaster NCE-CampusInsight. To enable interoperability between the switch and iMaster NCE-CampusInsight, run the **server ip-address** command on the switch to configure the IPv4 address and port number of iMaster NCE-CampusInsight.

Example

Set the IP address and port number of iMaster NCE-CampusInsight to 10.1.2.1 and 27371, respectively.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] server ip-address 10.1.2.1 port 27371
```

16.16.17 smi-server

Function

The **smi-server** command creates and displays the switch maintenance insight (SMI) view.

The **undo smi-server** command deletes the SMI view.

By default, no SMI view is created on a switch.

Format

smi-server

undo smi-server

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The switch needs to interconnect with iMaster NCE-CampusInsight to implement O&M information reporting. You can run the **smi-server** command to enter the SMI view, and configure the IP address and port number used by connected iMaster NCE-CampusInsight in the SMI view.

Follow-up Procedure

Run the **server ip-address (SMI view)** command to configure the IPv4 address and port number of iMaster NCE-CampusInsight.

Precautions

Deleting the SMI view using the **undo smi-server** command will delete all O&M information reporting configurations from the switch. Therefore, exercise caution when deleting the SMI view.

Example

Create and display the SMI view.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server]
```

16.16.18 source ip-address (SMI View)

Function

The **source ip-address** command configures the IPv4 address used by the switch to communicate with an NMS.

The **undo source ip-address** command deletes the configuration of the IPv4 address used by the switch to communicate with an NMS.

By default, no IPv4 address is configured for the switch to communicate with an NMS.

Format

source ip-address *ip-address* [**vpn-instance** *vpn-instance-name*]

undo source ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a switch.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you want an NMS (for example, iMaster NCE-CampusInsight) to monitor and analyze KPIs or traffic statistics of a switch, you must run this command to configure the IPv4 address used by the switch to communicate with the NMS.

Precautions

- When the **source ip** or **management-vlan** command is run in the NETCONF view, the switch connects to iMaster NCE-Campus in joint deployment mode. For configuration consistency purposes, you cannot run this command to configure the IP address used by the switch to communicate with iMaster NCE-CampusInsight.
- Changing the IPv4 address will interrupt the communication between the switch and NMS.

Example

Set the IPv4 address used by the switch to communicate with an NMS to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] source ip-address 10.1.1.1
```

16.17 eMDI Configuration Commands

16.17.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.17.2 display emdi

Function

The **display emdi** command displays the eMDI specifications, current eMDI configuration, and running status of eMDI instances.

Format

display emdi

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the eMDI specifications, current eMDI configuration, and running status of eMDI instances.

```
<HUAWEI> display emdi

Specification Information(Main Board):
 Max Instance Number                    : 16
 Max UDP Instance Number                  : 16
 Max TCP Instance Number                 : 8
 Max Static Instance Number              : 16
 Max Dynamic Instance Number               : 16
```

```
Configuration Information:
 Current Instance Number                  : 0
 Current Running Instance Number          : 0
 Current UDP Instance Number              : 0
 Current TCP Instance Number              : 0
 Current Static Instance Number           : 0
 Current Dynamic Instance Number          : 0

Specification and Configuration Information(IO Board
0):
 Max Instance Number                      : 16
 Current Instance Number                  : 0
```

Table 16-93 Description of the **display emdi** command output

Item	Description
Specification Information(Main Board)	Specifications of the switch.
Max Instance Number	Maximum number of eMDI instances supported by the switch.
Max UDP Instance Number	Maximum number of eMDI instances for monitoring UDP packets.
Max TCP Instance Number	Maximum number of eMDI instances for monitoring TCP packets.
Max Static Instance Number	Maximum number of eMDI instances that can be statically configured.
Max Dynamic Instance Number	Maximum number of eMDI instances that can be dynamically configured.
Configuration Information	Configuration on the switch.
Current Instance Number	Number of eMDI instances configured on the switch.
Current Running Instance Number	Number of eMDI instances that have been started.
Current UDP Instance Number	Number of eMDI instances that are monitoring UDP packets.
Current TCP Instance Number	Number of eMDI instances that are monitoring TCP packets.
Current Static Instance Number	Number of eMDI instances that have been statically configured.
Current Dynamic Instance Number	Number of eMDI instances that have been dynamically configured.
Specification and Configuration Information(IO Board 0)	Device specifications and configuration information.

16.17.3 display emdi statistics instance

Function

The **display emdi statistics instance** command displays statistics about an eMDI instance.

Format

display emdi statistics instance *instance-id* [**verbose** | **abnormal**]

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an eMDI instance.	The value is an integer that ranges from 1 to 5120 for S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 4112 for other models.
verbose	Displays detailed statistics about an eMDI instance.	-
abnormal	Displays exception statistics collected by an eMDI instance. ● For service traffic transmitted over UDP, an exception occurs if the value of **RTP-LR** field in the command output is not 0. ● For service traffic transmitted over TCP, an exception occurs if the value of **UPLR** or **DPLR** in the command output is not 0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the latest 60 statistical records of an eMDI instance.

Example

Display statistics about eMDI instance 1 that monitors UDP flows.

```
<HUAWEI> display emdi statistics instance 1
Instance ID : 1       Monitor Period(s) : 10    Protocol : UDP
---------------------------------------------------------------------------
       Record        Monitor       RTP-LR       RTP-SER       Jitter
        Time         Status      (1/100000)    (1/100000)      (us)
 2018-09-17:16-17-00  Normal         152          151           2
 2018-09-17:16-17-10  Normal         152          151           2
 2018-09-17:16-17-20  Normal         152          151           2
```

Display statistics about eMDI instance 2 that monitors TCP flows.

```
<HUAWEI> display emdi statistics instance 2
Instance ID : 2       Monitor Period(s) : 10    Protocol : TCP
------------------------------------------------------------------------------
       Record        Monitor       MFR          DPLR          UPLR      DRTT
       Time          Status       (bps)      (1/100000)   (1/100000)    (us)
------------------------------------------------------------------------------
 2018-09-17:16-17-00  Normal       4865656118     151          2        2
 2018-09-17:16-17-10  Normal       4866005390     151          2        2
 2018-09-17:16-17-20  Normal       4871215641     151          2        2
```

Display detailed statistics about eMDI instance 3 that monitors UDP flows.

```
<HUAWEI> display emdi statistics instance 3 verbose
Instance ID : 3      Monitor Period(s) : 10    Protocol : UDP
---------------------------------------------------------------------------
Originated From Slot 0
Record Time        : 2018-09-17:17-02-00   Monitor Status    : Abnormal
Received Packets  : 3850                 Rate pps          : 128
Received Bytes    : 5390000                Rate bps          : 1437333
Lost Packets      : 32261                RTP-LR(1/100000)   : 89338
Disordered Packets: 0                    RTP-SER(1/100000) : 0
RTP-LP            : 35                 Average Jitter(us): 8540
Maximum Jitter(us): 8815                   Minimum Jitter(us)  : 8262
```

Display detailed statistics about eMDI instance 4 that monitors TCP flows.

```
<HUAWEI> display emdi statistics instance 4 verbose
Instance ID : 4       Monitor Period(s) : 10    Protocol : TCP
---------------------------------------------------------------------------
Originated From Slot 0
Record Time       : 2018-09-17:15-27-00   Monitor Status : Normal
Received Packets : 95                    Rate pps       : 9
Received Bytes   : 12510                 Rate bps(MFR)  : 10008
UPLC             : 0                  UPLR(1/100000) : 0
DPLC             : 0                  DPLR(1/100000) : 0
DRTT(us)         : 8396412
```

Display exception statistics about eMDI instance 5 that monitors UDP flows.

```
<HUAWEI> display emdi statistics instance 5 abnormal
Instance ID : 5       Monitor Period(s) : 30    Protocol : UDP
---------------------------------------------------------------------------
Originated From Slot 0
Record Time        : 2018-09-17:17-02-00   Monitor Status    : Abnormal
Received Packets  : 3850                 Rate pps          : 128
Received Bytes    : 5390000                Rate bps          : 1437333
Lost Packets      : 32261                RTP-LR(1/100000)   : 89338
Disordered Packets: 0                    RTP-SER(1/100000) : 0
RTP-LP            : 35                 Average Jitter(us): 8540
Maximum Jitter(us): 8815                   Minimum Jitter(us)  : 8262
```

Display exception statistics about eMDI instance 6 that monitors TCP flows.

```
<HUAWEI> display emdi statistics instance 6 abnormal
Instance ID : 6       Monitor Period(s) : 30    Protocol : TCP
```

```
------------------------------------------------------------------------------
Originated From Slot 0
Record Time      : 2018-09-17:15-27-00   Monitor Status : Abnormal
Received Packets : 95                    Rate pps       : 9
Received Bytes   : 12510                 Rate bps(MFR)  : 10008
UPLC             : 95                    UPLR(1/100000) : 100000
DPLC             : 0                     DPLR(1/100000) : 0
DRTT(us)         : 8396412
```

Table 16-94 Description of the **display emdi statistics instance** command output

Item	Description
Instance ID	ID of an eMDI instance.
Monitor Period(s)	Monitoring interval of an eMDI instance.
Protocol	Transport layer protocol.
Record Time	Time when a record is generated.
Monitor Status	Status of an eMDI instance: ● Normal ● Abnormal. This problem is caused by loss of packets to be sent to the CPU on the eMDI-enabled switch.
RTP-LR(1/100000)	Packet loss rate of RTP packets.
RTP-SER(1/100000)	Out-of-order rate of RTP packets.
Jitter(us)	Jitter of RTP packets.
MFR(bps)	Average bit rate.
DPLR(1/100000)	Downstream packet loss rate.
UPLR(1/100000)	Upstream packet loss rate.
DRTT(us)	Average downstream two-way delay, in microseconds.
Originated From Slot	ID of the slot where the card having eMDI instance started is located.
Received Packets	Number of the received packets.
Rate pps	Rate at which packets are received, in pps.
Received Bytes	Total number of received bytes.
Rate bps	Rate at which packets are received, in bps.
Lost Packets	Number of lost packets.
Disordered Packets	Number of out-of-order packets.

Item	Description
RTP-LP	Maximum number of consecutively lost RTP packets.
Average Jitter(us)	Average jitter, in microseconds.
Maximum Jitter(us)	Maximum jitter, in microseconds.
Minimum Jitter(us)	Minimum jitter, in microseconds.
Rate bps(MFR)	Average rate at which packets are received, in bps.
UPLC	Number of the lost upstream packets.
DPLC	Number of the lost downstream packets.

16.17.4 emdi

Function

The **emdi** command enables the eMDI function and displays the eMDI view.

The **undo emdi** command disables the eMDI function.

By default, the eMDI function is disabled.

Format

emdi

undo emdi

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To use eMDI to monitor network quality and demarcate faults, you must run this command to enable eMDI before performing other related operations.

Example

Enable the eMDI function.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi]
```

16.17.5 alarm threshold

Function

The **alarm threshold** command configures an alarm threshold for an eMDI instance.

The **undo alarm threshold** command restores the default alarm threshold for an eMDI instance.

By default, the alarm threshold for an eMDI instance is 100.

Format

alarm { **rtp-lr** | **rtp-ser** | **dplr** | **uplr** } **threshold** *threshold-value*

undo alarm { **rtp-lr** | **rtp-ser** | **dplr** | **uplr** } **threshold** [*threshold-value*]

Parameters

Parameter	Description	Value
rtp-lr	Specifies the alarm threshold of the packet loss rate for RTP packets (transported over UDP).	-
rtp-ser	Specifies the alarm threshold of the out-of-order rate for RTP packets (transported over UDP).	-
dplr	Specifies the alarm threshold of the downstream TCP packet loss rate.	-
uplr	Specifies the alarm threshold of the upstream TCP packet loss rate.	-
threshold *threshold-value*	Specifies the alarm threshold value.	The value is an integer in the range from 1 to 100000 (unit: 1/100,000).

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When eMDI is used to monitor quality and demarcate faults of video or audio services, you can run this command to configure the alarm threshold for an eMDI instance. When an indicator such as the out-of-order packet rate or packet loss rate monitored by the eMDI instance reaches the threshold for three consecutive times, an alarm is reported to the NMS. If the indicator no longer reaches the threshold within the following 60 consecutive monitoring intervals, the alarm is automatically cleared.

The switch supports alarms about the packet loss rate, out-of-order rate, and multi-flow detection for RTP packets (transported over UDP), as well as the downstream and upstream TCP packet loss rates. If the out-of-order rate of RTP packets transported over UDP is higher than the packet loss rate, the eMDI instance determines that multiple flows exist.

Prerequisites

A target flow has been configured in the eMDI instance using the **flow ipv4 udp** command or **flow ipv4 tcp** command.

Precautions

After an eMDI instance is started using the **start** command, the alarm threshold for the eMDI instance cannot be modified. To modify the alarm threshold, run the **stop** command to stop the eMDI instance first.

Example

Set the alarm threshold of the downstream packet loss rate to 1000 in eMDI instance 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] flow ipv4 tcp source 10.0.0.1 destination 10.2.2.2
[HUAWEI-emdi-instance-1] alarm dplr threshold 1000
```

16.17.6 emdi instance

Function

The **emdi instance** command creates an eMDI instance and displays the eMDI instance view. If an eMDI instance has been created, the system displays the view of the eMDI instance.

The **undo emdi instance** command deletes a specified eMDI instance.

By default, no eMDI instance is created.

Format

emdi instance *instance-id*

undo emdi instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an eMDI instance to be created.	The value is an integer in the range from 1 to 4096.

Views

eMDI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An eMDI instance is a basic unit for eMDI to collect statistics about target flows. Each eMDI instance is composed of multiple elements, such as the target flow and monitoring interval. After the eMDI function is enabled, you must run this command to create an eMDI instance for quality monitoring and fault demarcation of video or audio services.

Precautions

- You can create one or more eMDI instances. The number of eMDI instances that can concurrently run a device depends on the product model, which can be queried using the **display emdi** command.
- An eMDI instance can monitor only one target flow.

Example

Create an eMDI instance with the ID of 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1]
```

16.17.7 monitor-period

Function

The **monitor-period** command sets the monitoring interval of an eMDI instance.

The **undo monitor-period** command restores the default monitoring interval of an eMDI instance.

By default, the monitoring interval of an eMDI instance is 60 seconds.

Format

monitor-period *period-value*

undo monitor-period [*period-value*]

Parameters

Parameter	Description	Value
period-value	Specifies the monitoring interval of an eMDI instance.	The value is of the enumerated type and can be set to 10, 30, or 60, in seconds.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When eMDI is used to monitor quality and demarcate faults of video or audio services, an eMDI instance obtains monitoring data from the device at a specified interval.

Precautions

After an eMDI instance is started, its monitoring interval cannot be modified. To modify the monitoring interval, run the **stop** command to stop the eMDI instance first.

Example

Set the monitoring interval of eMDI instance 1 to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] monitor-period 10
```

16.17.8 end lifetime

Function

The **end lifetime** command sets the lifetime of an eMDI instance.

The **undo end lifetime** command restores the default lifetime of an eMDI instance.

By default, the lifetime of an eMDI instance is 1 hour.

Format

end lifetime { **seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days* }

undo end lifetime [**seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days*]

Parameters

Parameter	Description	Value
seconds *seconds*	Specifies the lifetime of an eMDI instance, in seconds.	The value is an integer in the range from 300 to 604800.
minutes *minutes*	Specifies the lifetime of an eMDI instance, in minutes.	The value is an integer in the range from 5 to 10080.
hours *hours*	Specifies the lifetime of an eMDI instance, in hours.	The value is an integer in the range from 1 to 168.
days *days*	Specifies the lifetime of an eMDI instance, in days.	The value is an integer in the range from 1 to 7.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

eMDI is a one-off monitoring activity and does not need to run for a long time. You can run this command to configure the lifetime of an eMDI instance. After the eMDI instance is started, it stops automatically when its lifetime expires.

Precautions

After an eMDI instance is started, its lifetime cannot be modified. To modify the lifetime, run the **stop** command to stop the eMDI instance first.

Example

Set the lifetime of eMDI instance 1 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] end lifetime seconds 300
```

16.17.9 flow ipv4 tcp

Function

The **flow ipv4 tcp** command configures a target TCP flow to be monitored by an eMDI instance.

The **undo flow ipv4 tcp** command deletes a target TCP flow monitored by an eMDI instance.

By default, no target flow is configured in an eMDI instance.

Format

flow ipv4 tcp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number*]*

undo flow ipv4 tcp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number*]*

undo flow

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IP address of a target flow.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IP address of a target flow.	The value is in dotted decimal notation.
vlan *vlan-id*	Specifies the VLAN ID of a target flow.	The value is an integer in the range from 1 to 4094.
source-port *source-port-number*	Specifies the source port number of a target flow.	The value is an integer in the range from 1 to 65535.
destination-port *destination-port-number*	Specifies the destination port number of a target flow.	The value is an integer in the range from 1 to 65535.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a key element in an eMDI instance, a target flow to be monitored must be configured before the eMDI instance is started.

A target flow is the object monitored by an eMDI instance, and can be defined by any combinations of multiple attributes such as source IP address, destination IP address, VLAN ID, source port number, and destination port number. Specifying more attributes makes the target flow more accurate. Therefore, it is recommended that you specify more attributes to improve precision of monitoring results.

Precautions

- An eMDI instance can monitor only one target flow. If multiple target flows are configured in an eMDI instance, only the last configured one takes effect.
- In a video surveillance scenario, specify the number of the port connected to IPCs to ensure uniqueness of the target flow. Otherwise, the monitoring results will be affected in multi-flow scenarios.
- After an eMDI instance is started, the target flow monitored by the eMDI instance cannot be modified. To modify the target flow, run the **stop** command to stop the eMDI instance first.
- If 0.0.0.0 is specified by **source** *source-ip-address* or **destination** *destination-ip-address*, the source or destination IP address of the target flow can be any IP address. Examples are as follows:
  - If *source-ip-address* is set to 0.0.0.0 and *destination-ip-address* is set to 10.1.1.1, flows sourced from any IP address and destined for 10.1.1.1 are monitored.
  - If *source-ip-address* is set to 10.1.1.1 and *destination-ip-address* is set to 0.0.0.0, flows sourced from 10.1.1.1 and destined for any IP address are monitored.
  - If both *source-ip-address* and *destination-ip-address* are set to 0.0.0.0, the system does not check the source or destination IP addresses of the target flow to be monitored.

Example

Set the source and destination IP addresses of the target TCP flow to be monitored by eMDI instance 2 to 10.0.0.1 and 10.0.0.2, respectively.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 2
[HUAWEI-emdi-instance-2] flow ipv4 tcp source 10.0.0.1 destination 10.0.0.2
```

16.17.10 flow ipv4 udp

Function

The **flow ipv4 udp** command configures a target UDP flow to be monitored by an eMDI instance.

The **undo flow ipv4 udp** command deletes the target UDP flow monitored by an eMDI instance.

By default, no target flow is configured in an eMDI instance.

Format

flow ipv4 udp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number* | **pt** *pt-value* | **clock-rate** *clock-rate-value*]*

undo flow ipv4 udp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number* | **pt** *pt-value* | **clock-rate** *clock-rate-value*]*

undo flow

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IP address of a target flow.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IP address of a target flow.	The value is in dotted decimal notation.
vlan *vlan-id*	Specifies the VLAN ID of a target flow.	The value is an integer in the range from 1 to 4094.
source-port *source-port-number*	Specifies the source port number of a target flow.	The value is an integer in the range from 1 to 65535.
destination-port *destination-port-number*	Specifies the destination port number of a target flow.	The value is an integer in the range from 1 to 65535.
pt *pt-value*	Specifies the payload type of a target flow.	The value is an integer in the range from 25 to 127.
clock-rate *clock-rate-value*	Specifies the clock rate of a target flow.	The value is of the enumerated type and can be set to 8000, 16000, or 90000, in Hz. The default value is 90000.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a key element in an eMDI instance, a target flow to be monitored must be configured before the eMDI instance is started.

A target flow is the object monitored by eMDI, and can be defined by any combinations of multiple attributes such as source IP address, destination IP address, VLAN ID, source port number, and destination port number. Specifying more attributes makes the target flow more accurate. Therefore, it is recommended that you specify more attributes to improve precision of monitoring results.

Precautions

- An eMDI instance can monitor only one target flow. If multiple target flows are configured in an eMDI instance, only the last configured one takes effect.
- In a video surveillance scenario, specify the number of the port connected to IPCs to ensure uniqueness of the target flow. Otherwise, the monitoring results will be affected in multi-flow scenarios.
- In an IPTV scenario, specify the **pt** *pt-value* parameter to ensure uniqueness of a target flow. Otherwise, the monitoring results will be affected in multi-flow scenarios.
- After an eMDI instance is started, the target flow monitored by the eMDI instance cannot be modified. To modify the target flow, run the **stop** command to stop the eMDI instance first.

Example

Set the source and destination IP addresses of the target UDP flow to be monitored by eMDI instance 1 to 10.0.0.1 and 10.0.0.2, respectively.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] flow ipv4 udp source 10.0.0.1 destination 10.0.0.2
```

16.17.11 reset emdi statistics instance

Function

The **reset emdi statistics instance** command clears the statistics about an eMDI instance.

Format

reset emdi statistics instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an eMDI instance.	The value is an integer that ranges from 1 to 5120 for S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 4112 for other models.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To obtain the latest monitoring results of an eMDI instance, you can run this command to clear historical monitoring results of the eMDI instance, and then run the **display emdi statistics instance** command to obtain the latest ones.

Example

Clear statistics about eMDI instance 1.

```
<HUAWEI> reset emdi statistics instance 1
```

16.17.12 start

Function

The **start** command starts an eMDI instance.

Format

start

Parameters

None

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an eMDI instance is created and a target flow is configured, you can run this command to start the eMDI instance to monitor quality and demarcate faults of video or audio services.

Prerequisites

A target flow has been configured for an eMDI instance using the **flow ipv4 tcp** or **flow ipv4 udp** command.

Precautions

After an eMDI instance is started, all parameters in the eMDI instance cannot be modified. To modify the parameters, run the **stop** command to stop the eMDI instance first.

Example

Start eMDI instance 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] flow ipv4 udp source 10.0.0.1 destination 10.0.0.2
[HUAWEI-emdi-instance-1] start
```

16.17.13 stop

Function

The **stop** command stops an eMDI instance immediately.

Format

stop

Parameters

None

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

You can stop an eMDI instance in either of the following situations:

- Stop execution of the eMDI instance immediately.
- Modify the target flow, monitoring interval, lifetime, or alarm threshold of the eMDI instance.

Example

Stop eMDI instance 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] stop
```

16.17.14 stop all

Function

The **stop all** command stops all eMDI instances immediately.

Format

stop all

Parameters

None

Views

eMDI view

Default Level

2: Configuration level

Usage Guidelines

If eMDI instances have completed fault demarcation before their lifetime expires, you can run this command to stop all the eMDI instances.

Example

Stop all eMDI instances.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] stop all
```

17 Free Mobility Commands

17.1 Free Mobility Configuration Commands

17.1.1 Command Support

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the commands in this chapter.

17.1.2 display group-policy status

Function

The **display group-policy status** command displays the status of the controller associated with the device.

Format

display group-policy status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **group-policy controller** command, you can run this command to check the status of the controller associated with the device.

Example

Display the status of the controller associated with the device.

```
<HUAWEI> display group-policy status
Controller IP address: 192.168.1.1
Controller port: 5222
Backup controller IP address: -
Backup controller port: -
Source IP address: 192.168.10.1
State: not connected
Connected controller: master
Device protocol version: 2
Controller protocol version: -
```

Table 17-1 Description of the **display group-policy status** command output

Item	Description
Controller IP address	IP address of the master controller. To configure the IP address of the master controller, run the **group-policy controller** command.
Controller port	Port number of the master controller that exchanges packets with the device. To configure the port number of the master controller, run the **group-policy controller** command.
Backup controller IP address	IP address of the backup controller. To configure the IP address of the backup controller, run the **group-policy controller** command.
Backup controller port	Port number of the backup controller that exchanges packets with the device. To configure the port number of the backup controller, run the **group-policy controller** command.
Source IP address	Source IP address that the device uses to communicate with the controller. To configure the source IP address, run the **group-policy controller** command.

Item	Description
State	Status of the connection between the device and controller. ● disabled: indicates that the free mobility function is disabled. ● not connected: indicates that the device and controller are not connected. ● working: indicates that the device and controller have been connected.
Connected controller	Controller connected to the device. ● master: indicates the master controller. ● slave: indicates the backup controller. ● none: indicates that the device and controller are not connected.
Device protocol version	Protocol version number of the device.
Controller protocol version	Protocol version number of the controller. The parameter displays - when the device is not registered on the controller.

17.1.3 group-policy controller

Function

The **group-policy controller** command enables the free mobility function.

The **undo group-policy controller** command restores the default configuration.

By default, the free mobility function is disabled.

NOTE

This command is supported only when the device interoperates with Agile Controller-Campus.

Format

group-policy controller *ip-address1* [*port-number1*] [**backup** *ip-address2* [*port-number2*]] **password** *password* [**src-ip** *ip-address3*] [**vpn-instance** *vpn-instance-name*]

undo group-policy controller

Parameters

Parameter	Description	Value
ip-address1 [*port-number1*]	Specifies the IP address of the active controller and the port number for exchanging packets between the active controller and device. If no port number is configured, the default port number 5222 is used.	*ip-address1*: The value is in dotted decimal notation. *port-number1*: The value is an integer in the range from 1 to 65535.
backup *ip-address2* [*port-number2*]	Specifies the IP address of the standby controller and the port number for exchanging packets between the standby controller and device. If no port number is configured, the default port number 5222 is used.	*ip-address2*: The value is in dotted decimal notation. *port-number2*: The value is an integer in the range from 1 to 65535.
password *password*	Specifies the password for connecting the device to controllers.	The password configured on the device must be the same as that configured on controllers. The password configured on a controller needs to meet the following rules: ● The length should be between 8 to 32 characters. (The password can be a plain text of 8 to 32 characters or a cipher text of 48 to 68 characters.) ● The password must contain at least two types of the following characters: digits, uppercase letters, lowercase letters, and special characters. ● The password cannot contain more than two consecutive identical characters. ● The password cannot be the same as the user name or the reverse of the user name.

Parameter	Description	Value
src-ip *ip-address3*	Specifies the source IP address that the device uses to communicate with a controller. If this parameter is not configured, the device selects one of its own IP addresses to communicate with the controller.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which the specified source IP address belongs.	The value must be the name of an existing VPN instance.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The free mobility function allows a user to obtain the same network access policy regardless of the user's location and IP address used. In addition, user access policies only need to be uniformly deployed and managed on controllers, simplifying network deployment.

After the free mobility function is enabled using the **group-policy controller** command on an access device, the device can connect to the specified controller. After you deploy network access policies for users on the controller, the controller delivers the policies to devices. The devices then can control users' network access rights.

Precautions

This command cannot be run on a device if a controller delivers services to the device.

Example

Enable the free mobility function, and set the controller IP address to 10.1.1.11 and the connection password to YsHsjx_202207.

```
<HUAWEI> system-view
[HUAWEI] group-policy controller 10.1.1.11 password YsHsjx_202207
```

17.1.4 group-policy version

Function

The **group-policy version** command configures the user group version or user group policy version used for free mobility.

Format

group-policy { **user-group** | **user-group-policy** } **version** *version*

Parameters

Parameter	Description	Value
user-group	Specifies a user group.	-
user-group-policy	Specifies a user group policy.	-
version *version*	Specifies a version.	The value is an integer that ranges from 0 to 4294967295. **NOTE** The version needs to be obtained from the controller database. The configured version must be consistent with the version obtained from the controller database. Otherwise, the switch configuration is inconsistent with the controller configuration or the controller configuration fails to be delivered to the switch.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a switch is connected to the controller and has free mobility configured, the switch's user group version and user group policy version used for free mobility are restored to 0 if the **group-policy controller** command configuration is deleted incorrectly from the switch. In this situation, the switch and controller have inconsistent user group versions and user group policy versions used for free mobility. This inconsistency leads to a failure to deliver the free mobility configuration from the controller to the switch even though the **group-policy**

controller command is configured again on the switch. To address this issue, run the **group-policy version** command on the switch to configure the user group version and user group policy version used for free mobility. This configuration can restore the function that delivers the free mobility configuration from the controller to the switch.

Precautions

- The **group-policy version** command can be used to restore communication between a switch and the controller only when the **group-policy controller** command configuration is deleted incorrectly. Do not use the **group-policy version** command when the switch communicates with the controller normally.
- If you run the **group-policy version** command multiple times, only the latest configuration takes effect.
- The **group-policy version** command configuration is not recorded in the configuration file after this command is executed. To verify the command configuration, run the **display group-policy health** command in the diagnostic view. In the command output, **CMDC_CONTROLLER_UGSYNINCREMET_CONTROL** indicates the user group version, and **CMDC_CONTROLLER_UGPSYNINCREMET_CONTROL** indicates the user group policy version.

Example

Set the user group version used for free mobility to 20.

```
<HUAWEI> system-view
[HUAWEI] group-policy user-group version 20
```

17.1.5 ip-group service timer heart-beat

Function

The **ip-group service timer heart-beat** command configures the interval for sending IP-GROUP channel heartbeat packets.

The **undo ip-group service timer heart-beat** command restores the default configuration.

By default, IP-GROUP channel heartbeat packets are sent at an interval of 5 minutes.

NOTE

This command is supported only when the device interoperates with iMaster NCE-Campus.

Format

ip-group service timer heart-beat *interval*

undo ip-group service timer heart-beat

Parameters

Parameter	Description	Value
interval	Specifies the interval at which IP-GROUP channel heartbeat packets are sent.	The value is an integer in the range from 1 to 1440, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an IP-GROUP channel is established, you can run the **ip-group service timer heart-beat** command to set the interval for sending IP-GROUP channel heartbeat packets. In this way, the device periodically sends heartbeat packets to the controller to detect connectivity of the IP-GROUP channel.

Precautions

If you want to modify the configuration after the IP-GROUP channel is established, run the **undo ip-group service ip-address** command to delete the IP-GROUP channel first.

Example

Set the interval for sending IP-GROUP channel heartbeat packets to 6 minutes.

```
<HUAWEI> system-view
[HUAWEI] ip-group service timer heart-beat 6
```

17.1.6 ip-group service timer reconnection

Function

The **ip-group service timer reconnection** command configures an IP-GROUP channel reconnection interval.

The **undo ip-group service timer reconnection** command restores the default configuration.

By default, the IP-GROUP channel reconnection interval is 1 minute.

NOTE

This command is supported only when the device interoperates with iMaster NCE-Campus.

Format

ip-group service timer reconnection *interval*

undo ip-group service timer reconnection

Parameters

Parameter	Description	Value
interval	Specifies the IP-GROUP channel reconnection interval.	The value is an integer in the range from 1 to 255, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the IP-GROUP channel fails, the device periodically attempts to set up an IP-GROUP channel with a controller at the specified interval.

Precautions

If you want to modify the configuration after the IP-GROUP channel is established, run the **undo ip-group service ip-address** command to delete the IP-GROUP channel first.

Example

Set the IP-GROUP channel reconnection interval to 2 minutes.

```
<HUAWEI> system-view
[HUAWEI] ip-group service timer reconnection 2
```

17.1.7 ip-group service timer down-delay

Function

The **ip-group service timer down-delay** command configures a delay in responding to the IP-GROUP channel interruption event.

The **undo ip-group service timer down-delay** command restores the default configuration.

By default, the delay in responding to the IP-GROUP channel interruption event is 30 seconds.

NOTE

This command is supported only when the device interoperates with iMaster NCE-Campus.

Format

ip-group service timer down-delay *interval*

undo ip-group service timer down-delay

Parameters

Parameter	Description	Value
interval	Specifies a delay in responding to the IP-GROUP channel interruption event.	The value is an integer in the range from 0 to 600, in seconds. The value 0 indicates that the device responds to the IP-GROUP channel interruption event without any delay.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the IP-GROUP channel between the device and controller is interrupted, the device responds with certain actions, for example, emergency processing. If the IP-GROUP channel is interrupted frequently within a short time, the device resources are affected. To prevent this problem, set a delay in responding to the IP-GROUP channel interruption event.

Precautions

If you want to modify the configuration after the IP-GROUP channel is established, run the **undo ip-group service ip-address** command to delete the IP-GROUP channel first.

Example

Set the delay in responding to the IP-GROUP channel interruption event to 35 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip-group service timer down-delay 35
```

17.1.8 ip-group service timer up-delay

Function

The **ip-group service timer up-delay** command configures a delay in responding to the IP-GROUP channel Up event.

The **undo ip-group service timer up-delay** command restores the default configuration.

By default, the delay in responding to the IP-GROUP channel Up event is 30 seconds.

NOTE

This command is supported only when the device interoperates with iMaster NCE-Campus.

Format

ip-group service timer up-delay *interval*

undo ip-group service timer up-delay

Parameters

Parameter	Description	Value
interval	Specifies a delay in responding to the IP-GROUP channel Up event.	The value is an integer in the range from 0 to 600, in seconds. The value 0 indicates that the device responds to the IP-GROUP channel Up event without any delay.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the IP-GROUP channel between the device and controller goes Up, the device responds with certain actions, for example, switching from emergency processing to normal processing. If the IP-GROUP channel goes Up frequently within a short time, the device resources are affected. To prevent this problem, set a delay in responding to the IP-GROUP channel Up event.

Precautions

If you want to modify the configuration after the IP-GROUP channel is established, run the **undo ip-group service ip-address** command to delete the IP-GROUP channel first.

Example

Set the delay in responding to the IP-GROUP channel Up event to 35 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip-group service timer up-delay 35
```

17.1.9 ip-group service ip-address

Function

The **ip-group service ip-address** command configures an IP address of a controller.

The **undo ip-group service ip-address** command deletes the IP address of a controller.

By default, no controller IP address is configured on the device.

NOTE

This command is supported only when the device interoperates with iMaster NCE-Campus.

Format

ip-group service ip-address *ip-address* [**port** *port-number*] **pki-realm-name** *pki-realm-name* [**backup**]

undo ip-group service ip-address [*ip-address* [**backup**]]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a controller.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of a controller.	The value is an integer in the range from 1 to 65535. The default value is 50304.
pki-realm-name *pki-realm-name*	Specifies the name of a PKI realm.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Parameter	Description	Value
backup	Specifies the IP address of the backup controller. If **backup** is not specified, the IP address of the primary controller is configured. If *ip-address* is not specified in the **undo** command, all controller IP addresses are removed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before the device sets up an IP-GROUP channel with a controller, you need to configure the IP address and port number of the controller on the device, so that the device can send packets to the controller.

Precautions

If the default PKI realm is bound, security risks exist.

If only the IP address of the backup controller is configured and the IP address of the primary controller is not configured, the device does not establish a link with the backup controller.

Example

Configure the IP address and port number of a controller.

```
<HUAWEI> system-view
[HUAWEI] ip-group service ip-address 10.1.1.1 port 50304 pki-realm-name abc
```

18 VXLAN Commands

18.1 VXLAN Configuration Commands

18.1.1 Command Support

Only the S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6720S-EI, and S6720-EI support VXLAN.

18.1.2 advertise l2vpn evpn

Function

The **advertise l2vpn evpn** command enables a device to advertise IP routes imported to a VPN instance to the BGP-EVPN address family.

The **undo advertise l2vpn evpn** command restores the default configuration.

By default, a device is disabled from advertising IP routes imported to a VPN instance to the BGP-EVPN address family.

Format

advertise l2vpn evpn

undo advertise l2vpn evpn

Parameters

None

Views

BGP-VPN instance IPv4 address family view or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, when you need to establish VTEP tunnels through IP prefix routes and advertise host routes, run the **advertise l2vpn evpn** command to enable a device to advertise IP routes imported to a VPN instance to the BGP-EVPN address family. In this way, the routes imported to the VPN instance can be sent to the EVPN address family and then sent to the remote VTEP through the EVPN peer relationship.

Example

Enable a device to advertise IP routes imported to VPN instance **vpna** to the BGP-EVPN address family.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] ipv4-family vpn-instance vpna
[HUAWEI-bgp-vpna] advertise l2vpn evpn
```

18.1.3 arp broadcast disable (VBDIF interface view)

Function

The **arp broadcast disable** command disables the ARP broadcast function on a VBDIF interface.

The **undo arp broadcast disable** command enables the ARP broadcast function on a VBDIF interface.

By default, ARP broadcast is enabled on a VBDIF interface.

Format

arp broadcast disable

undo arp broadcast disable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

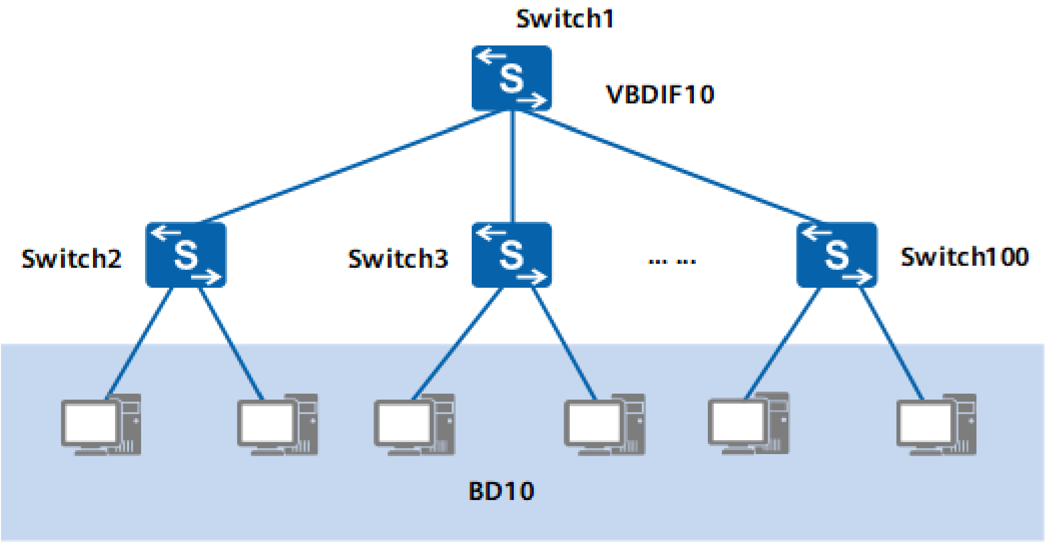
Usage Guidelines

Usage Scenario

By default, a VBDIF interface broadcasts ARP packets in a BD. However, in the large Layer 2 aggregation scenario shown in **Figure 18-1**, hosts on the user side are connected to aggregation switch 1 through switches 2-100, and the VBDIF interface is created on switch 1 as the user gateway, allowing hosts on the user side to communicate with external devices. The default ARP broadcast packet processing of the VBDIF interface can cause ARP packet flooding on the user side, which occupies large amounts of resources on the user side and affects normal user services. In addition, when a large number of ARP packets are broadcasted, the performance of switch 1 is affected.

To ensure normal user services and aggregation gateway performance in the large Layer 2 aggregation scenario, you can run this command to disable ARP broadcast on the VBDIF interface of an aggregation gateway.

Figure 18-1 Networking in the Layer 2 aggregation scenario



Precautions

Disabling a VBDIF interface from broadcasting ARP packets has impacts on the following scenarios: (Exercise caution before you run this command.)

- ARP proxy scenario. After a VBDIF interface is disabled from broadcasting ARP packets, the proxy does not forward ARP request packets from a host to their destinations even if all proxy conditions are met. As a result, ARP proxy fails.
- Scenarios in which hosts send unicast packets. For example, in **ping** operations, ICMP request packets must be encapsulated with MAC addresses mapped to the destination IP addresses. If a host does not have ARP entries, it has to send ARP request packets to learn the MAC address mapped to the destination IP address. However, the VBDIF interface is disabled from broadcasting ARP packets, and therefore cannot send ARP request packets. Consequently, the host cannot obtain the MAC address mapped to the destination IP address, causing a **ping** operation failure. This problem also occurs in other scenarios in which hosts send unicast packets.
- Strict ARP learning scenarios. In a strict ARP learning scenario, a device learns MAC addresses of only ARP reply packets in response to ARP request packets that it sends. If the VBDIF interface is disabled from broadcasting ARP

packets, it cannot actively send ARP request packets. As a result, strict ARP learning fails.

Example

Disable the ARP broadcast function on VBDIF interface 10.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] arp broadcast disable
```

18.1.4 arp broadcast-suppress enable

Function

The **arp broadcast-suppress enable** command enables ARP broadcast suppression in a BD.

The **undo arp broadcast-suppress enable** command disables ARP broadcast suppression in a BD.

By default, ARP broadcast suppression is disabled in a BD.

Format

arp broadcast-suppress [**mismatch-discard**] **enable**

undo arp broadcast-suppress [**mismatch-discard**] **enable**

Parameters

Parameter	Description	Value
mismatch-discard	Indicates that the device drops ARP request packets that do not match any entries in the ARP broadcast suppression table.	-

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a gateway receives a large number of ARP request packets within a short period and broadcasts the ARP request packets in a BD, excessive ARP request packets are forwarded. As a result, excessive network resources are used, traffic congestion may occur, and network performance may decline. ARP broadcast suppression can effectively ease the pressure on the gateway in handling ARP packets. After receiving an ARP request packet, the gateway searches the ARP broadcast suppression table that contains the mapping between the IP address and MAC address of each destination device.

- If a matching entry is found, the gateway replaces the broadcast MAC address in the received ARP request packet with the MAC address of the destination device, and then sends the request packet out through the interface matching the destination MAC address.
- If no matching entry is found:
  - The gateway broadcasts the ARP request packet in the BD if the **mismatch-discard** parameter is not set in the **arp broadcast-suppress enable** command.
  - The gateway drops the ARP request packet if the **mismatch-discard** parameter is set in the **arp broadcast-suppress enable** command.

Precautions

- When ARP broadcast suppression is configured in a VXLAN scenario and a large number of users exist, the gateway receives too many ARP packets and the packet rate exceeds the default CAR value. In this case, you can run the **car packet-type** { *vpls-arp* | *arp-request* } **cir** *cir-value* [**cbs** *cbs-value*] command to adjust the CAR value for ARP request packets. In this scenario, the CAR values specified using the arp-request and vpls-arp parameters share the same CAR resources. If the corresponding VBDIF interface is created on the device and the interface uses an IPv4 address and is Up, specify the arp-request parameter to adjust the CAR value. In other cases, specify the vpls-arp parameter to adjust the CAR value. You can run the **display cpu-defend configuration** command to view the CAR value for packets. If the CAR value is adjusted improperly, network services are affected. To adjust the CAR value for packets, contact technical support personnel.
- If the **arp broadcast-suppress enable** command is configured to enable ARP broadcast suppression in a BD and the **broadcast-suppression** command is configured to enable broadcast suppression in the BD, ARP broadcast suppression in the BD has a higher priority.

Example

Enable ARP broadcast suppression in BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] arp broadcast-suppress enable
```

Enable ARP broadcast suppression in BD 20 and configure the switch to discard ARP request packets if no matching entry is found in the ARP broadcast suppression table.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 20
[HUAWEI-bd20] arp broadcast-suppress mismatch-discard enable
```

18.1.5 arp collect host enable

Function

The **arp collect host enable** enables BGP EVPN to collect host information.

The **undo arp collect host enable** command disables BGP EVPN from collecting host information.

By default, BGP EVPN is disabled from collecting host information.

Format

arp collect host enable

undo arp collect host enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

When tenants communicate for the first time, they broadcast ARP request packets to each other. The ARP request packets are broadcasted in the Layer 2 network. To prevent broadcast storms caused by broadcasted ARP request packets, you can enable ARP broadcast suppression on the VXLAN Layer 2 gateway. However, ARP broadcast suppression relies on the host information table (containing the host IP address, MAC address, VTEP address, and VNI ID) on a Layer 3 gateway.

To allow a Layer 2 gateway to obtain the host information table, run this command in the VBDIF interface view to enable BGP EVPN to collect host information.

In VXLAN (BGP EVPN) scenarios, when VXLAN gateways advertise IRB routes to each other, run the **arp collect host enable** command for host information collection.

Example

Enable BGP EVPN on VBDIF interface 10 to collect host information.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] arp collect host enable
```

18.1.6 arp distribute-gateway enable

Function

The **arp distribute-gateway enable** command enables the distributed gateway function.

The **undo arp distribute-gateway enable** command disables the distributed gateway function.

By default, the distributed gateway function is disabled.

Format

arp distribute-gateway enable

undo arp distribute-gateway enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a gateway to function as a distributed gateway and learn only the ARP packets sent by a user-side host, run the **arp distribute-gateway enable** command to enable the distributed gateway function. After this function is enabled:

- The gateway processes only ARP packets sent by user-side hosts.
- The gateway deletes the network-side ARP entries that have been learned.

Precautions

After the distributed gateway function is enabled:

- Static ARP entries on the tunnel side fail to be configured on the gateway.
- If multiple gateways have the same IP address in the distributed scenario, this gateway does not report an ARP conflict.

Example

Enable the distributed gateway function on VBDIF interface 10.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] arp distribute-gateway enable
```

18.1.7 arp static bridge-domain

Function

The **arp static bridge-domain** command configures a static ARP entry on an interface of a VXLAN network.

The **undo arp static bridge-domain** command deletes a static ARP entry configured on an interface of a VXLAN network.

By default, no static ARP entry is configured on an interface of a VXLAN network.

Format

arp static *ip-address mac-address* **bridge-domain** *bd-id* [**vid** *vlan-id1* [**cevid** *vlan-id2*]] **interface** *interface-type interface-number.subnum*

undo arp static *ip-address mac-address* **bridge-domain** *bd-id* [**vid** *vlan-id1* [**cevid** *vlan-id2*]] **interface** *interface-type interface-number.subnum*

arp static *ip-address mac-address* **bridge-domain** *bd-id* [**vid** *vlan-id3*] **interface** *interface-type interface-number*

undo arp static *ip-address mac-address* **bridge-domain** *bd-id* [**vid** *vlan-id3*] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
bd-id	Specifies a BD ID.	The value is an integer that ranges from 1 to 16777215.
vid *vlan-id1*	Specifies the outer VLAN ID in the packet received by a sub-interface.	The value is an integer that ranges from 1 to 4094.
cevid *vlan-id2*	Specifies the inner VLAN ID in the packet received by a sub-interface.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number.subnum*	Specifies a sub-interface.	-
vid *vlan-id3*	Specifies the VLAN ID in the packet received by a interface.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static ARP entries are manually configured and maintained. They will not be aged out or overridden by dynamic ARP entries. Therefore, you can run the **arp static bridge-domain** command on an interface of a VXLAN network to configure static ARP entries to increase communication security. Static ARP entries enable the local device and a specified device to communicate with each other using only specified MAC addresses. Attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

Prerequisites

The outbound interface has been added to a VLAN and bound to a BD.

Precautions

- If a static ARP entry already exists, the new configuration cannot be delivered.
- The specified *ip-address* must be in the same network segment as the outbound interface address in the ARP entry.
- To specify the **vid** *vlan-id* and **cevid** *vlan-id* parameters, set the same encapsulation type as that on the interface first.
- When you configure a static ARP entry on an interface of the S6720-EI, S6735-S, and S6720S-EI, you must configure a static MAC address entry for the MAC address in the ARP entry. Otherwise, the switch will broadcast traffic from this MAC address.

Example

On the outbound interface GE0/0/1, configure a static ARP entry with the IP address and MAC address 10.1.1.2 and aaaa-fccc-1212, respectively.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] l2 binding vlan 10
```

```
[HUAWEI-bd10] quit
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ip address 10.1.1.1 255.255.255.0
[HUAWEI-Vbdif10] quit
[HUAWEI] arp static 10.1.1.2 aaaa-fccc-1212 bridge-domain 10 vid 10 interface GigabitEthernet 0/0/1
```

18.1.8 arp static vni

Function

The **arp static vni** command configures a static ARP entry for a VXLAN tunnel.

The **undo arp static vni** command deletes a static ARP entry of a VXLAN tunnel.

By default, no static ARP entry is configured for a VXLAN tunnel.

Format

arp static *ip-address mac-address* **vni** *vni-id* { **source-ip** *ip-address1* **peer-ip** *ip-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* }

undo arp static *ip-address mac-address* **vni** *vni-id* { **source-ip** *ip-address1* **peer-ip** *ip-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* }

NOTE

Only the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, and S5731-H support the **source-ipv6** and **peer-ipv6** parameters.

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vni-id	Specifies the VNI ID.	The value is an integer that ranges from 1 to 16777215.
source-ip *ip-address1*	Specifies the IP address of the source VTEP.	The value is in dotted decimal notation.
peer-ip *ip-address2*	Specifies the IP address of the destination VTEP.	The value is in dotted decimal notation.

Parameter	Description	Value
source-ipv6 *ipv6-address1*	Specifies the IPv6 address of the source VTEP.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
peer-ipv6 *ipv6-address2*	Specifies the IPv6 address of the destination VTEP.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static ARP entries are manually configured and maintained. They will not be aged out or overridden by dynamic ARP entries. Running the **arp static vni** command on a device to configure static ARP entries for a VXLAN tunnel increases communication security. Static ARP entries enable the local device and a specified device to communicate with each other using only specified MAC addresses. Attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

Prerequisites

A VXLAN tunnel and a Layer 3 gateway have been configured.

Precautions

- If a static ARP entry already exists, the new configuration cannot be delivered.
- The specified IP address must be in the same network segment as the outbound interface address in the ARP entry.
- When the VXLAN tunnel is created dynamically, the device does not support to configure a static ARP entry on a VXLAN tunnel-side interface.

Example

Configure a static ARP entry for a VXLAN tunnel that maps the IP address 10.0.0.2 to the MAC address aaaa-fccc-1212.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] vxlan vni 5000
```

```
[HUAWEI-bd10] quit
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ip address 10.0.0.10 255.255.255.0
[HUAWEI-Vbdif10] quit
[HUAWEI] interface nve 1
[HUAWEI-Nve1] source 10.1.1.1
[HUAWEI-Nve1] vni 5000 head-end peer-list 10.2.2.2
[HUAWEI-Nve1] quit
[HUAWEI] arp static 10.0.0.2 aaaa-fccc-1212 vni 5000 source-ip 10.1.1.1 peer-ip 10.2.2.2
```

18.1.9 arp-proxy local enable

Function

The **arp-proxy local enable** command enables local ARP proxy, realizing interconnection between isolated hosts in a BD.

The **undo arp-proxy local enable** command disables local ARP proxy.

By default, local ARP proxy is disabled.

Format

arp-proxy local enable

undo arp-proxy local enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

On a VXLAN, a BD is a broadcast domain. The member interfaces in a BD broadcast the broadcast, unknown unicast, and multicast (BUM) packets within the BD. To minimize broadcast traffic, network administrators usually run the **isolate enable** command or configure port isolation on the access side to enable access-side isolation. In this way, the access users of the BD are isolated and do not support Layer 2 interconnection. However, with the increase of user services, users have a growing demand for interconnection. To satisfy the demand, network administrators can enable local ARP proxy on a VBDIF interface so that isolated users in a BD can communicate with each other.

Example

Enable local ARP proxy on VBDIF interface 10.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] arp-proxy local enable
```

18.1.10 bridge-domain (Layer 2 sub-interface view)

Function

The **bridge-domain** command associates a Layer 2 sub-interface with a BD.

The **undo bridge-domain** command restores the default settings.

By default, no Layer 2 sub-interface is associated with a BD.

Format

bridge-domain *bd-id*

undo bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of the BD that is associated with a Layer 2 sub-interface.	The value is an integer that ranges from 1 to 16777215.

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

On the access side, two methods are available for creating a large Layer 2 BD.

- Based on VLAN: You can associate one or multiple VLANs with a BD to add users in these VLANs to the BD. This VLAN-based mode implements larger-granularity control, but is easy to configure. It applies to VXLAN deployment on a live network.
- Based on encapsulation mode: The device sends packets of different encapsulation modes to different Layer 2 sub-interfaces based on the VLAN tags contained in the packets. You can bind a Layer 2 sub-interface to a BD to add specified users to the BD. This mode implements refined and flexible control but requires more complex configuration. It applies to VXLAN deployment on a new network.

To create a BD based on encapsulation mode, create a Layer 2 sub-interface first. Then run the **encapsulation (Layer 2 sub-interface view)** command to configure a supported encapsulation mode on the sub-interface. After you run the **bridge-domain (Layer 2 sub-interface view)** command to associate a Layer 2 sub-interface with a BD, packets containing the same VLAN tag from different LANs can communicate at Layer 2.

Prerequisites

- Run the command **bridge-domain** to create the BD.
- Run the command **interface** to create the Layer 2 VXLAN sub-interface.

Precautions

One Layer 2 sub-interface can be associated with only one BD.

For the BD that is associated with the Layer 2 sub-interface using **default** encapsulation, the VBDIF interface of this BD cannot be created on the device.

Example

Associate Layer 2 sub-interface GE0/0/1.1 with BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] quit
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1 mode l2
[HUAWEI-GigabitEthernet0/0/1.1] bridge-domain 10
```

18.1.11 bridge-domain (system view)

Function

The **bridge-domain** command creates a bridge domain (BD) and displays the BD view, or directly displays the view of an existing BD view.

The **undo bridge-domain** command deletes a BD.

By default, no BD is created.

Format

bridge-domain *bd-id*

undo bridge-domain *bd-id*

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of a BD.	The value is an integer that ranges from 1 to 16777215.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

BDs are Layer 2 bridge domains on a large Layer 2 network constructed using VXLAN. VXLAN packets can be forwarded at Layer 2 within a BD through a VXLAN tunnel.

After you run the **bridge-domain** command to create a BD, you can complete other VXLAN configurations in the BD.

Example

Create BD 10 and enter the view of BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10]
```

18.1.12 broadcast-suppression (BD view)

Function

The **broadcast-suppression** command enables broadcast traffic suppression in a bridge domain (BD).

The **undo broadcast-suppression** command disables broadcast traffic suppression in a BD.

By default, broadcast traffic suppression is disabled in a BD.

Format

broadcast-suppression cir *cir-value* [**cbs** *cbs-value*]

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. If the **cbs** is not set, the default *cbs-value* is 125 times the *cir-value*.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

When a large number of broadcast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected. You can run the **broadcast-suppression** command to enable broadcast traffic suppression in a BD and configure the maximum number of broadcast packets that can pass through a BD. When the broadcast traffic volume exceeds the specified threshold, the system discards excess broadcast packets.

Example

Set the CIR value for broadcast traffic in BD 10 to 100 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] broadcast-suppression cir 100
```

18.1.13 description (EVPN instance view)

Function

The **description** command specifies the description of the current EVPN instance.

The **undo description** command deletes the description of the current EVPN instance.

By default, no description is specified for an EVPN instance.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of an EVPN instance.	The value is a string of 1 to 242 case-sensitive characters with spaces supported.

Views

EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To record the purpose of creating an EVPN instance and the CEs with which the EVPN instance is associated, you can run the **description** command to specify the description of the EVPN instance.

To check the description of an EVPN instance, run the **display evpn vpn-instance** command.

Precautions

If you run the **description** command several times, the latest configuration overrides the previous configurations.

Example

Specify the description of an EVPN instance named evn10.

```
<HUAWEI> system-view
[HUAWEI] evpn vpn-instance evn10 bd-mode
[HUAWEI-evpn-instance-evn10] description OnlyForAB
```

18.1.14 description (BD view)

Function

The **description** command configures the description of a bridge domain (BD).

The **undo description** command deletes the description of a BD.

By default, no description is configured for a BD.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the BD description.	The value is a string of 1 to 80 case-sensitive characters without question marks.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

If you have configured multiple BDs using the **bridge-domain (system view)** command, run the **description** command in the corresponding BD view to configure the description for each BD. BD description helps you quickly understand the function of each BD, facilitating service management.

Example

Configure description **vxlan** for BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] description vxlan
```

18.1.15 display arp broadcast-suppress user bridge-domain

Function

The **display arp broadcast-suppress user bridge-domain** command displays the ARP broadcast suppression table of a BD.

Format

display arp broadcast-suppress user bridge-domain { *bd-id* [*ip-address*] | **all** }

display arp broadcast-suppress user statistics { **bridge-domain** *bd-id* | **all** }

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of the BD of the ARP broadcast suppression table to be queried.	The value is an integer that ranges from 1 to 16777215.

Parameter	Description	Value
ip-address	Specifies the IP address of the ARP broadcast suppression table to be queried.	The value is in dotted decimal notation.
statistics	Displays ARP entry statistics.	-
all	Displays ARP entry in all BDs.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

ARP broadcast suppression can effectively ease the pressure on the gateway in handling ARP packets. When receiving an ARP request packet, the gateway searches for the host information about the device corresponding to the destination IP address (the IP address and MAC address mapping table of the destination device, also known as the ARP broadcast suppression table).

To display the ARP broadcast suppression table of a BD, run this command.

Example

Display the ARP broadcast suppression table of BD 10.

```
<HUAWEI> display arp broadcast-suppress user bridge-domain 10
-------------------------------------------------------------------------------
Flag     IP Address       MAC Address       VNI         VTEP Address
-------------------------------------------------------------------------------
local    10.1.1.11        00e0-fc00-0022    10          10.4.1.1
remote   10.1.1.12        00e0-fc98-15db    10          10.3.3.3
-------------------------------------------------------------------------------
Total: 2
```

Table 18-1 Description of the **display arp broadcast-suppress user bridge-domain** command output

Item	Description
Flag	ARP broadcast suppression entry type • local: ARP entry of the local access device • remote: ARP entry of the remote access device

Item	Description
IP Address	IP address of an ARP broadcast suppression entry
MAC Address	MAC address of an ARP broadcast suppression entry
VNI	Layer 2 VNI that an ARP broadcast suppression entry belongs
VTEP Address	IP address of the source VTEP of an ARP broadcast suppression entry
Total	Total number of ARP broadcast suppression entries in a BD

Display statistics on the ARP broadcast suppression table of BD 10.

```
<HUAWEI> display arp broadcast-suppress user statistics bridge-domain 10
Total: 2     Local: 1        Remote: 1
```

Table 18-2 Description of the **display arp broadcast-suppress user bridge-domain** command output

Item	Description
Total	Total number of ARP broadcast suppression entries
Local	Total number of ARP broadcast suppression entries learned from the local end
Remote	Total number of ARP broadcast suppression entries learned from the remote end

18.1.16 display bgp evpn group

Function

The **display bgp evpn group** command displays information about BGP EVPN peer groups.

Format

display bgp evpn group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Configuring BGP peer groups simplifies BGP network configuration and improves the route advertisement efficiency.

The **display bgp group** command displays the information about the peer group, including information about the peers in the peer group and configuration information about the peer group. This command is used in the following scenarios:

- Verify the configuration after running the **group** command to configure a peer group.
- Verify the configuration after running the **peer group** command to add a peer to the peer group.
- Verify the configuration after running the **undo peer group** command to delete a peer from a peer group.
- Verify the configuration after modifying the configuration of a peer group.

Example

Display the information about EVPN peer group **eg1**.

```
<HUAWEI> display bgp evpn group eg1

 BGP peer-group: eg1
 Remote AS: 100
 Authentication type configured: None
 Type : internal
 Configured hold timer value: 180
 Keepalive timer value: 60
 Connect-retry timer value: 32
 Minimum route advertisement interval is 0 seconds
 Connect-interface has been configured
 Tracking has been enabled, and the delay is 9s
 PeerSession Members:
   4.4.4.4            5.5.5.5

 Peer Preferred Value: 0
 No routing policy is configured
```

```
Peer Members:
 Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

 4.4.4.4         4         100        4        7     0 00:00:39 Established      2
 5.5.5.5         4         100        4        7     0 00:00:31 Established      2
```

Table 18-3 Description of the **display bgp evpn group** command output

Item	Description
BGP peer-group	Name of a BGP peer-group
Remote AS	Number of the AS where a peer group resides
Authentication type configured	BGP authentication type configured. The value can be the following: ● MD5 ● Keychain (kk), in which kk indicates the name of the configured keychain authentication ● None: no BGP authentication
Type	Type of a peer group: ● internal: The peer group is an IBGP peer group. ● external: The peer group is an EBGP peer group.
Configured hold timer value	Value of the Hold timer, in the unit of seconds
Keepalive timer value	Value of the Keepalive timer, in the unit of seconds
Connect-retry timer value	Value of the Connect-retry timer, in the unit of seconds
Minimum route advertisement interval	Minimum interval between route advertisements
PeerSession Members	Peers that set up sessions
Peer Preferred Value	Preferred value of a peer
Peer Members	Indicating that the following information is about peers
Peer	IP address of a peer
V	BGP version
As	Number of the AS where a member of a peer group resides
MsgRcvd	Number of received messages

Item	Description
MsgSent	Number of sent messages
OutQ	Number of messages to be sent to peers
Up/Down	Period of time during which a BGP session keeps the current state

Item	Description
State	BGP state mechanism: - Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. - Idle(Admin): indicates that the peer relationship is shut down inactively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. - Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. - Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer

Item	Description
	with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established.

Item	Description
	● Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PrefRcv	Indicates the number of route prefixes received by the local peer from the remote peer.

18.1.17 display bgp evpn peer

Function

The **display bgp evpn peer** command displays information about BGP EVPN peers.

Format

display bgp evpn peer [*ipv4-address* **verbose** | **verbose**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer to be displayed.	It is in dotted decimal notation.
verbose	Indicates to display detailed peer information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To query the following information about BGP EVPN peers, run the **display bgp evpn peer** command:

- Status of BGP EVPN connections
- Information about a BGP EVPN peer
- Whether BGP peers are successfully configured using the **peer enable** command
- Whether BGP peers are successfully deleted using the **undo peer enable** command

Precautions

By specifying **verbose**, you can query more BGP peer information, such as the BGP timer information, number of received and transmitted routes, capabilities supported by the peer, number of received and transmitted BGP information messages, and enabled configurations.

Example

Display the information about BGP EVPN peers.

```
<HUAWEI> display bgp evpn peer

 BGP local router ID : 6.6.6.6
 Local AS number : 100
 Total number of peers : 2              Peers in established state : 2

  Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  4.4.4.4         4         100        6        9     0 00:02:19 Established       2
  5.5.5.5         4         100        6        9     0 00:02:11 Established       2
```

Table 18-4 Description of the **display bgp evpn peer** command output

Item	Description
BGP Local router ID	Indicates the ID of the BGP local router. **NOTE** If two ends have the same BGP local router ID, no BGP peer relationship can be established between them. In this situation, run the **router id** command in the BGP view on either end to change the BGP local router ID. Changing it to the IP address of a loopback interface is recommended.
local AS number	Indicates the local AS number.
Total number of peers	Indicates the number of the peer.
Peers in established state	Indicates the number of the peer in established state.
Peer	Indicates the IP address of the peer.
V	Indicates the BGP version.
AS	Indicates the number of the AS where a member of a peer group resides.

Item	Description
MsgRcvd	Indicates the number of received messages.
MsgSent	Indicates the number of sent messages.
OutQ	Indicates the number of messages to be sent to peers.
Up/Down	Indicates the period of time during which a BGP session keeps the current state.

Item	Description
State	Indicates the BGP state mechanism: ● Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. ● Idle(Admin): indicates that the neighbor relationship is shut down initiatively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. ● No neg: The negotiation of the capabilities of the BGP peer's address family is not successful. ● Idle(Ovlmt): indicates that the neighbor relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP neighbor relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP neighbor relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP neighbor relationship will not be reestablished. ● Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer

Item	Description
	with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. ● Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PrefRcv	Indicates the number of route prefixes sent from the peer.

Display the detailed information about a BGP EVPN peer.

```
<HUAWEI> display bgp evpn peer 4.4.4.4 verbose

         BGP Peer is 4.4.4.4,  remote AS 100
         Type: IBGP link
         BGP version 4, Remote router ID 4.4.4.4
         Update-group ID: 0
         BGP current state: Established, Up for 00h04m51s
         BGP current event: KATimerExpired
         BGP last state: OpenConfirm
         BGP Peer Up count: 2
         Received total routes: 2
         Received active routes total: 2
         Received mac routes: 0
         Advertised total routes: 2
         Port:  Local - 65472    Remote - 179
```

```
    Configured: Connect-retry Time: 32 sec
    Configured: Min Hold Time: 0 sec
    Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
    Received  : Active Hold Time: 180 sec
    Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
    Peer optional capabilities:
    Peer supports bgp multi-protocol extension
    Peer supports bgp route refresh capability
    Peer supports bgp 4-byte-as capability
    Address family IPv4 Unicast: received
    Address family L2VPN EVPN: advertised and received
Received: Total 8 messages
         Update messages              2
         Open messages                1
         KeepAlive messages           5
         Notification messages        0
         Refresh messages             0
Sent: Total 11 messages
         Update messages              4
         Open messages                1
         KeepAlive messages           6
         Notification messages        0
         Refresh messages             0
Authentication type configured: None
Last keepalive received: 2018-03-29 20:52:33+00:00
Last keepalive sent    : 2018-03-29 20:52:33+00:00
Last update    received: 2018-03-29 20:48:33+00:00
Last update    sent    : 2018-03-29 20:48:41+00:00
Minimum route advertisement interval is 0 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Connect-interface has been configured
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
Tracking has been enabled, and the delay is 9s
```

Table 18-5 Description of the **display bgp evpn peer** command output

Item	Description
BGP Peer is 4.4.4.4	IP addresses of the BGP peer
remote AS 100	AS number of the BGP peer
Type	BGP link type, which can be **IBGP Link** or **EBGP Link**.
BGP version	BGP version (current version: BGP4)
Remote router ID	Router ID of the peer
Update-group ID	Update the peer group ID

Item	Description
BGP current state	Current BGP status: ● Idle: BGP denies any connection request. This is the initial status of BGP. After BGP receives a start event, BGP initiates a TCP connection to a peer, starts the ConnectRetry timer, and listens to the TCP messages from the peer. BGP then enters the Connect state. ● Idle(Admin): The neighbor relationship is shut down initiatively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the down state through the MIB, the neighbor is in this state. ● No neg: The negotiation of the capabilities of the BGP peer's address family is not successful. ● Idle(Ovlmt): The BGP neighbor relationship is interrupted because the number of routes exceeds the upper threshold (configured by running the **peer route-limit** command). When this happens, the neighbor is in this state. If the **reset bgp** command is not run, the BGP neighbor relationship is not reestablished. ● Connect: BGP waits for the TCP connection establishment to complete before performing further operations. – If the TCP connection is successfully established, BGP stops the ConnectRetry timer and sends an Open message to the peer. BGP then enters the Opensent state. – If the TCP connection fails to be established, BGP resets the ConnectRetry timer and listens to the TCP connection initiated by the peer. BGP then enters the Active state. – If the ConnectRetry timer expires, BGP restarts the ConnectRetry timer and attempts to establish a TCP connection with the peer again. At this time, BGP remains in the Connect state. ● Active: BGP attempts to establish a TCP connection. This is the intermediate status of BGP. – If the TCP connection is successfully established, BGP resets the ConnectRetry timer and sends an Open message to the peer. BGP then enters the Opensent state.

Item	Description
	– If the ConnectRetry timer expires, BGP restarts the ConnectRetry timer and enters the Connect state. – If BGP attempts to establish a TCP session with an unknown IP address but fails, BGP resets the ConnectRetry timer and remains in the Active state. ● OpenSent: BGP has sent an Open message to the peer and waits for an Open message from the peer. – If BGP receives a correct Open message, BGP enters the OpenConfirm state. – If BGP receives an incorrect Open message, BGP sends a Notification message to the peer and enters the Idle state. – If BGP receives a TCP connection teardown message, BGP resets the ConnectRetry timer and listens to the TCP connection initiated by the peer. BGP then enters the Active state. ● OpenConfirm: BGP waits for a Notification or Keepalive message. – If BGP receives a Notification or TCP connection teardown message, BGP enters the Idle state. – If BGP receives a Keepalive message, BGP enters the Established state. ● Established: BGP peers can exchange Update, Notification, and Keepalive messages. – If BGP receives an Update or Keepalive message, BGP remains in the Established state. – If BGP receives a Notification message, BGP enters the Idle state.
BGP current event	Current BGP event
BGP last state	Status of the last BGP stage, which can be Idle, Idle(Admin), Idle(Ovlmt), Connect, Active, OpenSent, OpenConfirm, or Established.
BGP Peer Up count	Number of times the BGP peer alternates between Up and Down
Received total routes	Number of route prefixes received
Received active routes total	Number of active route prefixes received
Received mac routes	Number of MAC routes received

Item	Description
Advertised total routes	Number of route prefixes sent
Port	Port number - Local: local port number, which is fixed to 179 because BGP uses TCP as the transport layer protocol - Remote: peer port number
Configured	Timers that are locally configured: - Connect-retry Time: ConnectRetry interval for a peer or peer group, in the unit of seconds. When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. - Min Hold Time: minimum hold time configured on the local device, in seconds. - Active Hold Time: hold time, in seconds. If BGP does not receive any KeepAlive message from the peer in the hold time, BGP considers that the peer is Down and then instructs other peers to remove the routes that are sent from the device. - Keepalive Time: interval for sending KeepAlive messages to the peer, in seconds. BGP peers send KeepAlive messages at intervals to show that they are working normally.
Received: Active Hold Time	Hold time of the peer
Negotiated	Timer negotiated by peers: - Active Hold Time: hold time agreed between the BGP peers after capability negotiation - Keepalive Time: Keepalive message transmission interval agreed between the BGP peers after capability negotiation
Peer optional capabilities	Capability supported by peers (optional) - Peer supports bgp multi-protocol extension: Indicates the BGP peer supports BGP multi-protocol extension - Peer supports bgp route refresh capability: Indicates the BGP peer supports BGP route refresh - Peer supports bgp 4-byte-as capability: Indicates the BGP peer supports BGP 4-byte AS numbers

Item	Description
Address family IPv4 Unicast	IPv4 unicast address family
Address family L2VPN EVPN	BGP EVPN address family
Received	Number of messages received from a peer: ● Total: total number of messages received from the peer ● Update messages: number of Update messages ● Open messages: number of Open messages ● KeepAlive messages: number of Keepalive messages ● Notification messages: number of Notification messages ● Refresh messages: number of route-refresh messages
Sent	Number of messages sent to the peer: ● Total: total number of messages ● Update messages: number of Update messages ● Open messages: number of Open messages ● KeepAlive messages: number of Keepalive messages ● Notification messages: number of Notification messages ● Refresh messages: number of route-refresh messages
Authentication type configured	BGP authentication type configured. The value can be the following: ● Message digest 5 (MD5) ● Keychain (kk): kk indicates the name of the configured keychain authentication. ● None: No BGP authentication is configured.

Item	Description
Last keepalive received	Indicates the time when the Keepalive message is received last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through the **clock daylight-saving-time** command.
Last keepalive sent	Time when the Keepalive message is sent last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through the **clock daylight-saving-time** command.
Last update received	Time when the Update message is received last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through the **clock daylight-saving-time** command.

Item	Description
Last update sent	Time when the Update message is sent last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through the **clock daylight-saving-time** command.
Minimum route advertisement interval is 30 seconds	Minimum route advertisement intervals. The default minimum route advertisement intervals are as follows: ● The minimum interval for advertising EBGP routes is 30 seconds. ● The minimum interval for advertising IBGP routes is 15 seconds.
Optional capabilities	(Optional) Capabilities of the peer
Peer Preferred Value	Preferred value of the peer
Routing policy configured	Whether a routing policy has been configured

18.1.18 display bgp evpn routing-table

Function

The **display bgp evpn routing-table** command displays information about BGP EVPN routes.

Format

display bgp evpn all routing-table statistics

display bgp evpn all routing-table [**inclusive-route** [*inclusive-route*] | **mac-route** [*mac-route*] | **prefix-route** [*prefix-route*]]

display bgp evpn route-distinguisher *route-distinguisher* **routing-table** { **inclusive-route** [*inclusive-route*] | **mac-route** [*mac-route*] | **prefix-route** [*prefix-route*] }

Parameters

Parameter	Description	Value
all	Displays all route information.	-
statistics	Displays route statistics.	-
route-distinguisher *route-distinguisher*	Displays information about EVPN routes with a specified RD.	RD has the following four formats: - 16-bit AS number:32-bit user-defined number. For example, 101:3. The AS number is an integer ranging from 0 to 65535, and the user-defined number is an integer ranging from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. - Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295, and a user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. - 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that both range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. - 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535.
inclusive-route	Displays the information about inclusive multicast routes.	-

Parameter	Description	Value
inclusive-route	Specifies an inclusive multicast route.	The format is M:L:X.X.X.X: ● M: 0 (fixed) ● L: mask length of the source address of the device originating the route ● X.X.X.X: source address of the device originating the route
mac-route	Displays the information about MAC advertisement routes.	-
mac-route	Specifies a MAC advertisement route.	The format is E:M:H-H-H:L:X.X.X.X or E:M:H-H-H:L:[X:X::X:X]: ● E: ID of the VLAN to which the MAC address belongs ● M: 48 (MAC address length) ● H-H-H: MAC address. H is a 4-digit hexadecimal number, such as 00e0 and fc01. If you enter fewer than four alphanumeric characters, 0s are added before the input digits. For example, if e0 is entered, 00e0 is specified. ● L: mask length of the IP address corresponding to the MAC address ● X.X.X.X: IP address corresponding to the MAC address ● X:X::X:X indicates the IPv6 address corresponding to the MAC address.
prefix-route	Displays the information about an IP prefix route.	-
prefix-route	Specifies an IP prefix route.	The format is L:X.X.X.X:M or L:[X:X::X:X]:M: ● L: 0 (fixed) ● X.X.X.X: host IP address ● M: host IP address and mask ● X:X::X:X indicates the IPv6 address of host routes.
statistics	Displays route statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, you can run this command to view EVPN route information and statistics on the device.

Example

Display all BGP EVPN routing information.

```
<HUAWEI> display bgp evpn all routing-table
Local AS number :100

 BGP Local router ID is 10.35.99.225
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 EVPN address family:
 Number of Mac Routes : 2
 Route Distinguisher: 1:1


       Network(EthTagId/MacAddrLen/MacAddr/IpAddrLen/IpAddr)   NextHop
 *>     0:48:a4dc-be0f-99a6:0:0.0.0.0                          9.9.9.9
 *>     0:48:a4dc-be0f-99a6:32:9.9.9.9                         9.9.9.9

 VPN-Instance vpn1, Router ID 10.35.99.225:

 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  9.9.9.9/32         9.9.9.9                   100        0      ?

 EVPN address family:
 Number of Inclusive Multicast Routes : 1
 Route Distinguisher: 1:1


       Network(EthTagId/IpAddrLen/OriginalIp)                  NextHop
 *>     0:32:9.9.9.9                                     9.9.9.9

 EVPN address family:
 Number of Ip Prefix Routes : 2
 Route Distinguisher: 1:1


       Network(EthTagId/IpPrefix/IpPrefixLen)                  NextHop
 *>     0:9.9.9.0:24                                     9.9.9.9
 *>     0:[2001:db8:1::]:64                                 9.9.9.9

 VPN-Instance vpn1, Router ID 10.35.99.225:

 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  9.9.9.0/24         9.9.9.9         0         100         0         ?
```

```
 VPN-Instance vpn1, Router ID 10.35.99.225:

 Total Number of Routes: 1

 *>  Network   : 2001:db8:1::                    PrefixLen  : 64
     NextHop   : ::FFFF:9.9.9.9                 LocPrf     :
     MED       :                                PrefVal    : 0
     Label     : 5010
     Path/Ogn  :200 100 ?
```

Table 18-6 Description of the **display bgp evpn all routing-table** command output

Item	Description
Local AS number	Local AS number
BGP Local router ID	Router ID of the local device
Number of Mac Routes	Number of MAC advertisement routes
Route Distinguisher	Route distinguisher
Network	Reachable address
NextHop	Next hop
VPN-Instance	VPN instance name
Router ID	Router ID
Total Number of Routes	Total number of routes
EVPN address family	BGP EVPN address family
MED	Multi-exit discriminator of route
LocPrf	Local priority
PrefVal	Value preferred by the protocol
Path/Ogn	AS path attribute and origin attribute of the route
Number of Inclusive Multicast Routes	Number of inclusive multicast routes
Number of Ip Prefix Routes	Number of IP prefix routes
PrefixLen	Mask length
Label	Label value

Display statistics information about all BGP EVPN routes.

```
<HUAWEI> display bgp evpn all routing-table statistics
Total number of routes from all PE: 5
Number of Mac Routes: 2
Number of Inclusive Multicast Routes: 1
Number of Ip Prefix Routes: 2
```

Table 18-7 Description of the **display bgp evpn all routing-table statistics** command output

Item	Description
Total number of routes from all PE	Total number of routes
Number of Mac Routes	Number of MAC routes
Number of Inclusive Multicast Routes	Number of inclusive multicast routes
Number of Ip Prefix Routes	Number of IP prefix routes

18.1.19 display bgp evpn routing-table peer statistics

Function

The **display bgp evpn routing-table peer statistics** command displays statistics about received and advertised BGP EVPN routes.

Format

display bgp evpn routing-table peer statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To display the statistics of the received and advertised BGP EVPN routes, run this command.

Example

Display the statistics about the received and advertised BGP EVPN routes.

```
<HUAWEI> display bgp evpn routing-table peer statistics

 BGP local router ID : 6.6.6.6
 Local AS number : 100
 Total number of peers : 2              Number of Peers in established state : 2

  Peer                   Received routes            Advertised routes
```

```
4.4.4.4              2                   2
5.5.5.5              2                   2
```

Table 18-8 Description of the **display bgp evpn routing-table peer statistics** command output

Item	Description
BGP local router ID	Local router ID
Local AS number	AS number
Total number of peers	Total number of peers
Number of Peers in established state	Number of peers in the established state
Peer	IP address of a peer
Received routes	Total number of routes received from the peer
Advertised routes	Total number of routes advertised to the peer

18.1.20 display bgp evpn update-peer-group

Function

The **display bgp evpn update-peer-group** command displays the BGP update group information about an EVPN address family.

Format

display bgp evpn update-peer-group [**index** *update-peer-group-index*]

Parameters

Parameter	Description	Value
index *update-peer-group-index*	Specifies the index of a BGP update peer-group.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, you can run this command to view the update group information about an EVPN address family.

Example

Display the update group information about an EVPN address family.

```
<HUAWEI> display bgp evpn update-peer-group

 The EVPN instance's update peer group number : 1
 Keep buffer update peer group number : 0
 BGP Version : 4

 Group ID : 0
 Group Type : internal
 Addr Family : L2-EVPN
 AdvMinTimeVal : 0
 Total Peers : 2
 Leader Peer : 5.5.5.5
 Peers List : 5.5.5.5          4.4.4.4
```

Display information about the BGP update peer-group with the index 0 in the EVPN address family.

```
<HUAWEI> display bgp evpn update-peer-group index 0

 Group ID : 0
 BGP Version : 4
 Group Type : internal
 Addr Family : L2-EVPN
 AdvMinTimeVal : 0
 Total Peers : 1
 Leader Peer : 1.1.1.1

 Total format packet number : 85
 Total send packet number : 85
 Total replicate packet number : 0
 The replication percentages(%) : 0

 Peers List : 1.1.1.1
```

Table 18-9 Description of the **display bgp evpn update-peer-group** command output

Item	Description
The EVPN instance's update peer group number	Number of update groups in an EVPN instance
Keep buffer update peer group number	Number of packets in update groups saved in the batch buffer
BGP Version	BGP version
Group ID	ID of the update group

Item	Description
Group Type	Type of the update group, which can be one of the following: - external: EBGP peer group. - internal: IBGP peer group. - external-confed: EBGP update group in the confederation - internal-confed: IBGP update group in the confederation - unknown: unknown type
Addr Family	Address family
AdvMinTimeVal	Minimum interval for sending Update packets with the same route prefix
Total Peers	Total number of peers in an update group
Leader Peer	Representative of an update-group
Total format packet number	Number of Update messages of a single peer sends in the update peer-group
Total send packet number	Number of Update messages sent to all BGP peers in the update peer-group
Total replicate packet number	Absolute value of the difference between Total send packet number and Total format packet number, that is, absolute value of the difference between the number of Update messages that are sent to all peers in the update peer-group and the number of Update messages sent to a single peer in the update peer-group
The replication percentages(%)	Percentage of the number of replicated Update messages to the total number of sent Update messages, that is, (Total send packet number – Total format packet number)/Total send packet number
Peers List	List of peers

18.1.21 display bridge-domain

Function

The **display bridge-domain** command displays the BD configuration.

Format

display bridge-domain [*bd-id* [**brief** | **verbose**]]

Parameters

Parameter	Description	Value
bd-id	Displays the configuration of a specified BD. If this parameter is not specified, the device displays the configuration of all BDs.	The value is an integer that ranges from 1 to 16777215.
brief	Displays brief BD configuration.	-
verbose	Displays detailed BD configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After BDs are created on a device, you can run the **display bridge-domain** command to view the configuration of a specified BD or all BDs.

Example

Display the configuration of all BDs.

```
<HUAWEI> display bridge-domain
STAT: Statistics;
--------------------------------------------------------------------------------

BDID     State    STAT        Description
--------------------------------------------------------------------------------
10       down    disable     vxlan
20       up      disable     vxlan
--------------------------------------------------------------------------------
The total number of bridge-domains is : 2
```

Display the detailed configuration of BD 10.

```
<HUAWEI> display bridge-domain 10 verbose
Bridge-domain ID   :10
Description        :vxlan
State              :Down
Statistics         :Disable
Broadcast-suppression       CIR(kbit/s) :-           CBS(byte) :-
Multicast-suppression       CIR(kbit/s) :10000000   CBS(byte) :4294967295
Unknown-unicast-suppression CIR(kbit/s) :0           CBS(byte) :655355
--------------------------------------------------------------------------------
```

```
Interface                          State
-------------------------------------------------------------------------------
GigabitEthernet1/0/1.1                down
-------------------------------------------------------------------------------
VLAN                               State
-------------------------------------------------------------------------------
2                                down
3                                down
10                               down
-------------------------------------------------------------------------------
```

Table 18-10 Description of the **display bridge-domain** command output

Item	Description
BDID/Bridge-domain ID	ID of a BD. To set the BD ID, run the **bridge-domain** command in the system view.
State	BD status: ● up: The BD is bound to a Layer 2 sub-interface, VLAN, or VNI, and at least one of the bound Layer 2 sub-interface, VLAN, and VNI is Up. ● down: The BD is not bound to a Layer 2 sub-interface, VLAN, or VNI; alternatively, the BD is bound to a Layer 2 sub-interface, VLAN, or VNI and the bound Layer 2 sub-interface, VLAN, and VNI are Down.
STAT/Statistics	Whether traffic statistics collection is enabled for the BD: ● disable ● enable
Description	BD description. To configure the description of a BD, run the **description (BD view)** command.
The total number of bridge-domains is	Total number of BDs on the device.
Broadcast-suppression CIR(kbit/s) CBS(byte)	CIR and CBS in a BD specified by the broadcast suppression function. The unit is kbit/s and byte, respectively.
Multicast-suppression CIR(kbit/s) CBS(byte)	CIR and CBS in a BD specified by the multicast suppression function. The unit is kbit/s and byte, respectively.
Unknown-unicast-suppression CIR(kbit/s) CBS(byte)	CIR and CBS in a BD specified by the unknown unicast suppression function. The unit is kbit/s and byte, respectively.

Item	Description
Interface State	Member interface in a BD and its status. - up: The link layer protocol of the interface is in the Up state. - down: The link layer protocol of the interface is Down.
VLAN State	Status of the VLAN associated with the BD. - up - down The status of a VLAN is determined by the status of member interfaces in the VLAN. A VLAN is Up only when at least one member interface in the VLAN is Up.

18.1.22 display bridge-domain statistics

Function

The **display bridge-domain statistics** command displays packet statistics in a BD.

Format

display bridge-domain *bd-id* **statistics**

Parameters

Parameter	Description	Value
bd-id	Displays packet statistics in a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display bridge-domain statistics** command to view packet statistics in a BD. The information helps you locate faults and simplifies VXLAN network maintenance.

Before using this command to view packet statistics in a BD, run the **statistics enable** command in the BD view to enable packet statistics collection in the BD.

Example

Display packet statistics in BD 10.

```
<HUAWEI> display bridge-domain 10 statistics
Total:
-------------------------------------------------------------------------
Item              Packets                      Bytes
-------------------------------------------------------------------------
Inbound            10                          1520
Outbound            10                           1520
-------------------------------------------------------------------------
```

Table 18-11 Description of the **display bridge-domain statistics** command output

Item	Description
Slot	Slot ID.
Item	Statistical item.
Packets	Number of packets.
Bytes	Number of bytes.
Inbound	Statistics on packets going in to a BD.
Outbound	Statistics on packets leaving a BD.

18.1.23 display evpn mac routing-table

Function

The **display evpn mac routing-table** command displays the MAC routing entries of the BGP EVPN function.

Format

display evpn mac routing-table { **all-vpn-instance** | **vpn-instance** *evpn-instance-name* [*mac-address*] }

Parameters

Parameter	Description	Value
all-vpn-instance	Displays the MAC routing entries of all the EVPN instances.	–
vpn-instance *evpn-instance-name*	Displays the MAC routing entry of a specified EVPN instance.	The EVPN instance must already exist on the device.

Parameter	Description	Value
mac-address	Displays the MAC routing entry of a specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check MAC routing entries of the BGP EVPN function, run this command.

Example

Display MAC routing entries of all the EVPN instances.

```
<HUAWEI> display evpn mac routing-table all-vpn-instance
EVPN-Instance Name : evpn10
-------------------------------------------------------------------------------
Flag     MAC Address      Serial number    VNI         VTEP Address
-------------------------------------------------------------------------------
local    0000-5e00-5311  0               1002        10.1.1.1
remote   0000-5e00-5322  0               1002        10.2.2.2
-------------------------------------------------------------------------------
Total Num: 2 Local Num: 1 Remote Num : 1
```

Table 18-12 Description of the **display evpn mac routing-table** command output

Item	Description
EVPN-Instance Name	EVPN instance where a MAC routing entry resides.
Flag	Flag of the MAC routing entry type: ● remote: The MAC routing entry is remotely obtained. ● local: The MAC routing entry is locally obtained.
MAC Address	MAC address of a MAC routing entry.
Serial number	Serial number of a MAC routing entry.
VNI	Layer 2 VNI to which a MAC routing entry belongs.

Item	Description
VTEP Address	VTEP IP address of a MAC routing entry.
Total Num	Total number of MAC routing entries.
Local Num	Total number of MAC routing entries locally obtained.
Remote Num	Total number of MAC routing entries remotely obtained.

18.1.24 display evpn vpn-instance

Function

The **display evpn vpn-instance** command displays the configurations of EVPN instances.

Format

display evpn vpn-instance [**verbose**] [*evpn-instance-name*]

Parameters

Parameter	Description	Value
verbose	Displays detailed information.	-
evpn-instance-name	Specifies the name of an EVPN instance.	The value is the name of an existing VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, EVPN instances need to be configured. After EVPN instances are configured, you can run this command to query the configurations of EVPN instances.

If *evpn-instance-name* is not specified, this command displays the information about all configured EVPN instances on the device.

Example

Display the brief information about all EVPN instances configured on the device.

```
<HUAWEI> display evpn vpn-instance
 Total EVPN-Instances configured      : 1
  VPN-Instance Name               RD
---------------------------------------------------------
  vn10                           10:1
```

Table 18-13 Description of the **display evpn vpn-instance** command output

Item	Description
Total EVPN-Instances configured	Total number of EVPN instances configured on the local end.
VPN-Instance Name	Name of the EVPN instance.
RD	RD of the EVPN instance IPv4 address family.

Display detailed information about all EVPN instances.

```
<HUAWEI> display evpn vpn-instance verbose
 Total EVPN-Instances configured      : 1

 EVPN-Instance Name and ID : vn10, 1
 Bridge-domain Number : 1
  Bridge-domain List : bridge-domain 10 source 1.1.1.1
  Route Distinguisher : 10:1
  Export VPN Targets : 1:1 100:1
  Import VPN Targets : 100:1
```

Table 18-14 Description of the **display evpn vpn-instance** command output

Item	Description
Total EVPN-Instances configured	Total number of EVPN instances configured on the local end.
EVPN-Instance Name and ID	Name and ID of the EVPN instance. The ID is assigned by the system, which facilitates indexing.
Bridge-domain Number	Number of BDs bound to an EVPN instance
Bridge-domain List	BDs bound to an EVPN and IP address of the source VTEP
Route Distinguisher	RD of the EVPN instance IPv4 address family
Export VPN Targets	Route Target list in the outbound direction

Item	Description
Import VPN Targets	Route Target list in the inbound direction

18.1.25 display evpn vpn-instance bridge-domain

Function

The **display evpn vpn-instance bridge-domain** command displays the information about the BD bound to an EVPN instance.

Format

display evpn vpn-instance bridge-domain

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, EVPN instances need to be configured and bound to BDs. After EVPN instances are configured and bound to BDs, you can run this command to display the information about the BDs bound to EVPN instances.

Example

Display the information about the BD bound to an EVPN.

```
<HUAWEI> display evpn vpn-instance bridge-domain
 Total EVPN-Instances configured      : 1

 EVPN-Instance Name and ID : vn10, 1
 Bridge-domain Number : 1
  Bridge-domain List : bridge-domain 10 source 1.1.1.1
```

Table 18-15 Description of the **display evpn vpn-instance bridge-domain** command output

Item	Description
Total EVPN-Instances configured	Total number of EVPN instances configured on the device
EVPN-Instance Name and ID	Name and ID of the EVPN instance. The ID is assigned by the system, which facilitates indexing.
Bridge-domain Number	Total number of BDs to which this EVPN instance is bound
Bridge-domain List	IP address of the BD to which the EVPN instance is bound and the local VTEP

18.1.26 display evpn vpn-instance import-vt

Function

The **display evpn vpn-instance import-vt** command displays the information about the EVPN instance that matches an import route target (IRT).

Format

display evpn vpn-instance import-vt *ivt-value*

Parameters

Parameter	Description	Value
ivt-value	Specifies the value of the import VPN-target attribute. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device is configured with multiple EVPN instances, you can run this command to display the EVPN instances to which the EVPN route with a specified VPN target can be imported.

Example

Display the information about the EVPN instance that matches an IRT.

```
<HUAWEI> display evpn vpn-instance import-vt 100:1
 The number of EVPN-Instances matched the import-vt 100:1 : 1
  EVPN-Instance Name and ID : bd10,1
```

Table 18-16 Description of the **display evpn vpn-instance import-vt** command output

Item	Description
The number of EVPN-Instances matched the import-vt	Total number of EVPN instances that matches an IRT
EVPN-Instance Name and ID	Name and ID of the EVPN instance. The ID is assigned by the system, which facilitates indexing.

18.1.27 display evpn vpn-instance peer-list

Function

The **display evpn vpn-instance peer-list** command displays the information about the remote peer of an EVPN instance.

Format

display evpn vpn-instance *evpn-instance-name* **peer-list**

Parameters

Parameter	Description	Value
evpn-instance-name	Specifies the name of an EVPN instance.	The value must be the name of an existing EVPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, you can run this command to query the information about the remote peer of an EVPN instance.

Example

Query the information about the remote peer of EVPN instance **vn10**.

```
<HUAWEI> display evpn vpn-instance vn10 peer-list
 Total EVPN-Instance Name and Peer-list Number : vn10, 1
  Remote VNI         Peer-Address       State
-------------------------------------------------
  10                 1.1.1.1            Active
```

Table 18-17 Description of the **display evpn vpn-instance peer-list** command output

Item	Description
Total EVPN-Instance Name and Peer-list Number	EVPN instance name and total number of the peers of the EVPN instance
Remote VNI	Layer 2 VNI carried by the peer
Peer-Address	Peer IP address
State	Connection status ● Active ● Inactive

18.1.28 display evpn vpn-instance tunnel-info

Function

The **display evpn vpn-instance tunnel-info** command displays the information about the tunnels constructed through EVPN instances.

Format

.

display evpn vpn-instance [**verbose**] **tunnel-info**

Parameters

Parameter	Description	Value
verbose	Displays detail information	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, the device constructs dynamic Layer 2 VXLAN tunnels through the routes between EVPN instances. You can run this command to display the information about the tunnels constructed through EVPN instances.

Example

Display the information about the tunnels constructed through EVPN instances.

```
<HUAWEI> display evpn vpn-instance tunnel-info
 Total EVPN-Instances Tunnel          : 2
  Remote VNI         Peer-Address
--------------------------------------
  10                 1.1.1.1
  20                 2.2.2.2
```

Table 18-18 Description of the **display evpn vpn-instance tunnel-info** command output

Item	Description
Total EVPN-Instances Tunnel	Number of tunnels constructed through EVPN instances
Remote VNI	Layer 2 VNI carried by the peer
Peer-Address	Peer IP address

Display the detailed information about the tunnels constructed through EVPN instances.

```
<HUAWEI> display evpn vpn-instance verbose tunnel-info
 Total EVPN-Instances Tunnel          : 2

 Remote VNI 10         Peer-Address 1.1.1.1
  Export VPN Targets : 1:1 100:1

 Remote VNI 20         Peer-Address 2.2.2.2
  Export VPN Targets : 1:1 200:1
```

Table 18-19 Description of the **display evpn vpn-instance tunnel-info** command output

Item	Description
Total EVPN-Instances Tunnel	Number of tunnels constructed through EVPN instances
Remote VNI	Layer 2 VNI carried by the peer
Peer-Address	Peer IP address
Export VPN Targets	Export RT list

18.1.29 display interface nve

Function

The **display interface nve** command displays Network Virtualization Edge (NVE) interface information.

Format

display interface nve [*nve-number* | **main**]

Parameters

Parameter	Description	Value
nve-number	Specifies the number of an NVE interface. If *nve-number* is not specified, information about all NVE interfaces is displayed.	The value is 1.
main	Displays the running status and statistics of the main interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the NVE interface status or locate an NVE interface fault on the VXLAN network, run the **display interface nve** command to check the running status and statistics of the NVE interface.

Example

Display the running status of the NVE interface.

```
<HUAWEI> display interface nve 1
Nve1 current state : UP
Line protocol current state : UP
Description:
Route Port
Internet protocol processing : disabled
Current system time: 2017-03-28 19:50:24
```

Table 18-20 Description of the **display interface nve** command output

Item	Description
Nve1 current state	Physical status of the NVE interface. The physical status of the successfully created NVE interface is always Up.
Line protocol current state	Link layer protocol status of the NVE interface. The link layer protocol status of the successfully created NVE interface is always Up.
Description	Description of the NVE interface.

Item	Description
Route Port	The interface is a Layer 3 interface.
Internet protocol processing	This field displays only **disabled**, and the interface cannot be configured with an IP address.
Current system time	System time.

18.1.30 display interface vbdif

Function

The **display interface vbdif** command displays the status, configuration, and statistics of a VBDIF interface.

Format

display interface vbdif [*bd-id* | **main**]

Parameters

Parameter	Description	Value
bd-id	Displays the status, configuration, and statistics of a VBDIF interface with a specified BD ID. If no BD ID is specified, the status, configuration, and statistics of all VBDIF interfaces are displayed.	The BD ID of a VBDIF interface must already exist.
main	Displays the running status and statistics of the main interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor an interface or locate an interface fault, you can use the **display interface vbdif** command to view the interface status, interface configuration, and traffic statistics on the interface. The information helps you locate faults in the system or on an interface.

Prerequisites

The specified VBDIF interface has been created.

Example

Display information of VBDIF interface with BD ID 20.

```
<HUAWEI> display interface vbdif 20
Vbdif20 current state : UP
Line protocol current state : UP
Last line protocol up time : 2015-07-08 11:25:34
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.20.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
0000-5e00-0101
Current system time: 2015-07-08 14:09:59
    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Table 18-21 Description of the **display interface vbdif** command output

Item	Description
Vbdif20 current state	Physical status of a VBDIF interface. ● UP: The physical status of the interface is Up. ● DOWN: The physical status of the interface is Down. ● Administratively down: The administrator has run the **shutdown** command on the VBDIF interface.
Line protocol current state	Link-layer protocol status of a VBDIF interface. ● UP: The link-layer protocol of the interface is Up. ● DOWN: The link-layer protocol of the interface is Down, or no IP address is assigned to the interface.
Last line protocol up time	Last time the link-layer protocol of an interface goes Up. **NOTE** This field is displayed only when the link-layer protocol status is Up.
Description	Description of a VBDIF interface. The description helps you learn the functions of the interface.
Route Port	Layer 3 interface.
The Maximum Transmit Unit is	Maximum transmit unit (MTU) of an interface. The default MTU is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.
Internet Address is	IP address of an interface. If no IP address is configured for the current interface, the command output is displayed as "Internet protocol processing: disabled."

Item	Description
IP Sending Frames' Format is	Format of the Ethernet frames sent by a VBDIF interface. The default value is **PKTFMT_ETHNT_2**. A VBDIF interface can identify the received Ethernet frames of the following formats: ● PKTFMT_ETHNT_2 ● Ethernet_SNAP ● 802.2 ● 802.3
Hardware address is	Physical address of an interface.
Current system time	System time.
Input bandwidth utilization	Number of packets received by the interface.
Output bandwidth utilization	Number of packets sent by the interface

18.1.31 display mac-address bridge-domain

Function

The **display mac-address bridge-domain** command displays MAC address entries of a BD.

Format

display mac-address [*mac-address*] **bridge-domain** *bd-id* [**verbose**]

Parameters

Parameter	Description	Value
mac-address	Displays an entry with a specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
bd-id	Displays MAC address entries of a specified BD.	The value is an integer that ranges from 1 to 16777215.
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of a switch stores MAC addresses of other devices. The switch queries the MAC address table to quickly locate the outbound interface for data forwarding. You can run the **display mac-address bridge-domain** command to view MAC address entries of a specified BD.

Follow-up Procedure

If any MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address static** command to add a correct one.

Example

Display MAC address entries of BD 20.

```
<HUAWEI> system-view
[HUAWEI] display mac-address bridge-domain 20
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                      Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc12-0006 -/-/20                        GE0/0/23.5          static

-------------------------------------------------------------------------------
Total items displayed = 1
```

Display detailed information about MAC address entries of BD 20.

```
<HUAWEI> system-view
[HUAWEI] display mac-address bridge-domain 20 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc12-0006         BD   : 20
Learned-From: GE0/0/23.5             Type : static

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 18-22 Description of the **display mac-address bridge-domain** command output

Item	Description
MAC Address	MAC address.
VLAN/VSI/BD	ID of the VLAN, name of the virtual switch instance (VSI), or ID of the BD to which the MAC address belongs.
Learned-From	Interface on which a MAC address is learned.

Item	Description
Type	Type of a MAC address entry: ● static: a static MAC address entry, which is manually configured and will not be aged out. ● blackhole: a blackhole MAC address entry, which is manually configured and will not be aged out.

18.1.32 display mac-address evpn

Function

The **display mac-address evpn** command displays information about MAC address entries of the EVPN type.

Format

display mac-address evpn bridge-domain *bd-id* [**verbose**]

Parameters

Parameter	Description	Value
bridge-domain *bd-id*	Displays information about MAC address entries of the EVPN type in a specified BD.	The value is an integer that ranges from 1 to 16777215.
verbose	Displays detailed information about MAC address entries of the EVPN type.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A device stores other devices' MAC addresses learned by itself into the MAC address table. The device queries the MAC address table to quickly locate the outbound interface for data forwarding.

Follow-up Task

You can run this command to check information about MAC address entries of the EVPN type. If any learned MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address static** command to add a correct one.

Example

Display information about MAC address entries in BD 10.

```
<HUAWEI> display mac-address evpn bridge-domain 10
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                      Learned-From        Type
-------------------------------------------------------------------------------
00e0-fc12-3456 -/-/10                           192.0.2.10          evpn

-------------------------------------------------------------------------------
Total items displayed = 1
```

Display detailed information about MAC address entries in BD 10.

```
<HUAWEI> display mac-address evpn bridge-domain 10 verbose
-------------------------------------------------------------------------------
MAC Address : 00e0-fc12-3456        BD   : 10
Learned-From: 192.0.2.10            Type : evpn


-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 18-23 Description of the **display mac-address evpn** command output

Item	Description
MAC Address	MAC address information.
VLAN/VSI/BD	ID of the VLAN, name of the virtual switch instance (VSI), or ID of the BD to which the MAC address belongs.
BD	Number of the BD to which an entry belongs.
Learned-From	Remote VTEP IP address of a VXLAN tunnel that learns the MAC address entry of the EVPN type.
Type	MAC address entry type.

18.1.33 display nd multicast-suppress user bridge-domain

Function

The **display nd multicast-suppress user bridge-domain** command displays the ND multicast suppression table of a BD.

Format

display nd multicast-suppress user bridge-domain *bd-id* [*ipv6-address*]

display nd multicast-suppress user statistics { **bridge-domain** *bd-id* | **all** }

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of the BD of the ND multicast suppression table to be queried.	The value is an integer that ranges from 1 to 16777215.
ipv6-address	Specifies the IP address of the ND multicast suppression table to be queried.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
statistics	Displays ND multicast suppression entry statistics.	-
all	Displays ND multicast suppression entry statistics in all BDs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

ND multicast suppression can effectively ease the pressure on the gateway in handling NS packets. When receiving an NS request packet, the gateway searches for the host information about the device corresponding to the destination IP address (the IPv6 address and MAC address mapping table of the destination device, also known as the ARP broadcast suppression table).

To display the ND multicast suppression table of a BD, run this command.

Example

Display the ND multicast suppression table of BD 10.

```
<HUAWEI> display nd multicast-suppress user bridge-domain 10
------------------------------------------------------------------------------
IPv6 Address : FC00:1::10
MAC Address  : 0487-ea01-0506   VNI : 10         Serial number : 0
VTEP Address : 10.2.2.2         Flag : local
VPN Instance :vpn1
------------------------------------------------------------------------------
Total Num: 1 Local Num: 1 Remote Num : 0
```

Table 18-24 Description of the **display nd multicast-suppress user bridge-domain** command output

Item	Description
IPv6 Address	IPv6 address of an NS multicast suppression entry
MAC Address	MAC address of an NS multicast suppression entry
VNI	Layer 2 VNI that an NS multicast suppression entry belongs
Serial number	Serial number of an NS multicast suppression entry
VTEP Address	IP address of the source VTEP of an NS multicast suppression entry
Flag	NS multicast suppression entry type ● local: NS multicast suppression entry of the local access device ● remote: NS multicast suppression entry of the remote access device
VPN Instance	VPN instance bound to the gateway to which the NS multicast suppression entries belong
Total Num	Total number of NS multicast suppression entries in a BD
Local Num	Total number of NS multicast suppression entries learned from the local end in a BD
Remote Num	Total number of NS multicast suppression entries learned from the remote end in a BD

Display statistics on the NS multicast suppression table of BD 10.

```
<HUAWEI> display nd multicast-suppress user statistics bridge-domain 10
Total: 1     Local: 1         Remote: 0
```

Table 18-25 Description of the **display nd multicast-suppress user bridge-domain** command output

Item	Description
Total	Total number of NS multicast suppression entries

Item	Description
Local	Total number of NS multicast suppression entries learned from the local end
Remote	Total number of NS multicast suppression entries learned from the remote end

18.1.34 display vxlan encapsulation

Function

The **display vxlan encapsulation** command displays VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface.

Format

display vxlan encapsulation interface *interface-type interface-number* [**bridge-domain** *bd-id* | **default** | **dot1q** [**vid** *pe-vid*] | **qinq** [**vid** *vlan-vid* [**ce-vid** *ce-vid*]] | **untag**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays VXLAN encapsulation information about a specified Layer 2 sub-interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
bridge-domain *bd-id*	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by BD ID.	The BD ID must exist.
default	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **default**.	-
dot1q	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **Dot1q**.	-

Parameter	Description	Value
vid *pe-vid*	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by VLAN ID in packets with the flow encapsulation mode **Dot1q**.	The VLAN ID must exist.
qinq	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **QinQ**.	-
vid *vlan-vid* [**ce-vid** *ce-vid*]	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by VLAN ID in packets with the flow encapsulation mode **QinQ**. ● *vlan-vid* specifies the outer VLAN ID. ● *ce-vid* specifies the inner VLAN ID.	The VLAN ID must exist.
untag	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **untag**.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vxlan encapsulation** command to view VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface as well as the bindings between the sub-interface and BD.

Example

Display VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface.

```
<HUAWEI> display vxlan encapsulation interface gigabitethernet 0/0/1
----------------------------------------------------------------------------------------------------
Interface                  EncapType          PeVid          CeVid          BD-ID        RewriteType
----------------------------------------------------------------------------------------------------
GigabitEthernet0/0/1.1       qinq              4093           4093          16000        pop default
----------------------------------------------------------------------------------------------------
Total number to display is 1.
```

Table 18-26 Description of the **display vxlan encapsulation** command output

Item	Description
Interface	Name of the Layer 2 sub-interface.
EncapType	Flow encapsulation type of the Layer 2 sub-interface. ● qinq ● dot1q ● default ● untag To configure the flow encapsulation type, run the **encapsulation** command in the Layer 2 sub-interface view.
PeVid	VLAN ID of packets with the flow encapsulation type **Dot1q** or outer VLAN ID of packets with the flow encapsulation type **QinQ**. To configure the VLAN ID, run the **encapsulation** command in the Layer 2 sub-interface view.
CeVid	Inner VLAN ID of packets with the flow encapsulation type **QinQ**. To configure the VLAN ID, run the **encapsulation** command in the Layer 2 sub-interface view.
BD-ID	BD. To configure the BD, run the **bridge-domain** command in the Layer 2 sub-interface view.
RewriteType	Type of the operation of removing VLAN tags in packets: ● pop default: Indicate the default operation of removing VLAN tags in packets. ● pop single: Remove one VLAN tag. ● pop double: Remove double VLAN tags. ● pop none: Do not remove any VLAN tag. To configure the operation type, run the **rewrite pop** command.
Total number to display is	Total number of encapsulation data records about Layer 2 sub-interfaces of a main interface.

18.1.35 display vxlan peer

Function

The **display vxlan peer** command displays the IP address of the destination VXLAN tunnel endpoint (VTEP) of a Virtual Network Identifier (VNI).

Format

display vxlan peer [**vni** *vni-id*]

Parameters

Parameter	Description	Value
vni *vni-id*	Displays the IP address of the destination VTEP of a specified VNI.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing VXLAN configuration, you can run the **display vxlan peer** command to view information about the source and destination IP address bound to the VNI.

Precautions

Before running the **display vxlan peer** command, ensure that the device has been configured with VNIs. Otherwise, the command output is meaningless.

Example

Display the IP address of the destination VTEP of a specified VNI.

```
<HUAWEI> display vxlan peer
 Vni ID       Source                 Destination           Type
 ---------------------------------------------------------------
 10           10.1.1.2               10.1.1.3              static
 10           10.1.1.2               10.1.1.4              static
 11           10.1.1.2               10.1.1.5              static&l2 dynamic
 ---------------------------------------------------------------
 Number of peers :
 Total: 3   Static: 3   L2 dynamic: 1   L3 dynamic: 0
```

Table 18-27 Description of the **display vxlan peer** command output

Item	Description
Vni ID	VNI ID. To configure or modify a VNI ID, run the **vxlan vni** command in the BD view. For a Layer 3 VXLAN tunnel, the **Vni ID** field displays **-**.
Source	IP address of the source VTEP. To configure or modify the IP address of the source VTEP, run the **source** command in the NVE interface view.

Item	Description
Destination	IP address of the destination VTEP. To configure or modify the IP address of the destination VTEP, run the **vni head-end peer-list** command.
Type	IP address configuration mode of the destination VTEP: - static: The IP address is manually configured. - l2 dynamic: Layer 2 VXLAN tunnel IP addresses are dynamically generated through the BGP protocol. - l3 dynamic: Layer 3 VXLAN tunnel IP addresses are dynamically generated through the BGP protocol. To configure the IP address configuration mode, run the **vni head-end peer-list** command.
Number of peers	Number of IP addresses of destination VTEPs on the device: - Total: indicates the number of IP addresses of destination VTEPs (If the Type field displays a combination of multiple types, such as static&l2 dynamic, the number of IP addresses of destination VTEPs is counted as 1). - Static: indicates the number of IP addresses of static destination VTEPs. - L2 dynamic: indicates the number of IP addresses of Layer 2 dynamic destination VTEPs. - L3 dynamic: indicates the number of IP addresses of Layer 3 dynamic destination VTEPs.

18.1.36 display vxlan statistics

Function

The **display vxlan statistics** command displays VXLAN tunnel packet statistics.

Format

display vxlan statistics source *source-ip-address* **peer** *peer-ip-address* [**vni** *vni-id*]

display vxlan statistics source *source-ipv6-address* **peer** *peer-ipv6-address* [**vni** *vni-id*]

NOTE

Only the S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, S5731-H, and S6730-S support the **source** and **peer** parameters configured as IPv6 address.

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the IPv4 address of the source VTEP.	The value is in dotted decimal notation.
peer *peer-ip-address*	Specifies the IPv4 address of the destination VTEP.	The value is in dotted decimal notation.
source *source-ipv6-address*	Specifies the IPv6 address of the source VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
peer *peer-ipv6-address*	Specifies the IPv6 address of the destination VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vxlan statistics** command to view VXLAN tunnel packet statistics. The information helps you locate faults and simplifies VXLAN network maintenance.

Before using this command to view VXLAN tunnel packet statistics, run the **vxlan statistics enable** command on an NVE interface to enable statistics collection on VXLAN tunnel packets.

Example

Display statistics on VXLAN tunnel packets, with 10.10.1.1 and 10.1.1.1 as the source and destination VTEP IP addresses.

```
<HUAWEI> display vxlan statistics source 10.10.1.1 peer 10.1.1.1
Total:
---------------------------------------------------------------------------
Item              Packets                     Bytes
---------------------------------------------------------------------------
Inbound             5                          760
Outbound             5                          760
---------------------------------------------------------------------------
```

Table 18-28 Description of the **display vxlan statistics** command output

Item	Description
Item	Statistical item.
Packets	Number of packets.
Bytes	Number of bytes.
Inbound	Packet statistics in the inbound direction of the VXLAN tunnel.
Outbound	Packet statistics in the outbound direction of the VXLAN tunnel.

18.1.37 display vxlan tunnel

Function

The **display vxlan tunnel** command displays information about VXLAN tunnels.

Format

display vxlan tunnel [*tunnel-id*] [**verbose**]

Parameters

Parameter	Description	Value
tunnel-id	Displays information about the VXLAN tunnel with a specified ID. If this parameter is not specified, the device displays information about all VXLAN tunnels.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays detailed VXLAN tunnel information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VXLAN tunnels are established, you can run the **display vxlan tunnel** command to view VXLAN tunnel information.

Example

Display VXLAN tunnel information.

```
<HUAWEI> display vxlan tunnel
 Tunnel ID       Source              Destination         State     Type
 ---------------------------------------------------------------------------
 4026531841      10.1.1.2            10.1.1.4            up        static
 ---------------------------------------------------------------------------
 Number of vxlan tunnel :
 Total: 1   Static: 1   L2 dynamic: 0   L3 dynamic: 0
```

Display detailed VXLAN tunnel information.

```
<HUAWEI> display vxlan tunnel verbose
 Tunnel ID       : 4026531841
 Source          : 10.1.1.2
 Destination     : 10.1.1.4
 State           : up
 Reason          : -
 Type            : static
 ---------------------------------------------------------------------------
 Number of vxlan tunnel :
 Total: 1   Static: 1   L2 dynamic: 0   L3 dynamic: 0
```

Table 18-29 Description of the **display vxlan tunnel** command output

Item	Description
Tunnel ID	ID of a VXLAN tunnel. After a VXLAN tunnel is established, the ID is automatically generated by the device.
Source	Source IP address of the VXLAN tunnel. To configure the source IP address, run the **source** command in the NVE interface view.
Destination	Destination IP address of the VXLAN tunnel.
State	Status of a VXLAN tunnel: ● up: The VXLAN tunnel is reachable. ● down: The VXLAN tunnel is unreachable.
Reason	Reason why the VXLAN tunnel is Down: ● no license: No valid license is available. ● no route: Routes are unreachable.

Item	Description
Type	IP address configuration mode of the destination VTEP: - static: The IP address is manually configured. - l2 dynamic: Layer 2 VXLAN tunnel IP addresses are dynamically generated through the BGP protocol. - l3 dynamic: Layer 3 VXLAN tunnel IP addresses are dynamically generated through the BGP protocol. To configure the IP address configuration mode, run the **vni head-end peer-list** command.
Number of vxlan tunnel	Total number of VXLAN tunnels on the device. - Total: indicates the number of VXLAN tunnels. - Static: indicates the number of static VXLAN tunnels. - L2 dynamic: indicates the number of Layer 2 dynamic VXLAN tunnels. - L3 dynamic: indicates the number of Layer 3 dynamic VXLAN tunnels.

18.1.38 display vxlan vni

Function

The **display vxlan vni** command displays the VXLAN configuration of a specified VNI or all VNIs.

Format

display vxlan vni [*vni-id* [**verbose**]]

Parameters

Parameter	Description	Value
vni-id	Displays VXLAN information about a specified VNI. If this parameter is not specified, the device displays VXLAN configuration of all VNIs.	The value is an integer that ranges from 1 to 16777215.
verbose	Displays detailed VXLAN information about a specified VNI.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Applications

After VXLAN is configured, you can run the **display vxlan vni** command to view information about BDs associated with VNIs and VNI status.

Precautions

Before running the **display vxlan vni** command, ensure that the device has been configured with VNIs. Otherwise, the command output is meaningless.

Example

Display VXLAN information about all VNIs.

```
<HUAWEI> display vxlan vni
 VNI               BD-ID            State
 -----------------------------------------
 10                10               up
 50                50               up
 -----------------------------------------
 Number of vxlan vni bound to BD is : 2

 VNI               VRF-ID
 -----------------------------------------
 20                5
 -----------------------------------------
 Number of vxlan vni bound to VPN is : 1
```

Display detailed VXLAN information about VNI 10.

```
<HUAWEI> display vxlan vni 10 verbose
 BD ID               :10
 State               :up
 Source              :10.1.1.2
 Source IPv6 Address :-
 UDP Port            :4789
 Peer List           :10.1.1.1 10.1.1.3
 IPv6 Peer List      :-
```

Display detailed VXLAN information about VNI 20.

```
<HUAWEI> display vxlan vni 20 verbose
 VRF-ID              :5
```

Table 18-30 Description of the **display vxlan vni** command output

Item	Description
VNI	ID of a VNI. To configure or modify a VNI ID, run the **vxlan vni** command.
BD-ID (BD ID)	ID of the BD associated with a VNI. To configure or modify a BD ID, run the **bridge-domain (system view)** command.

Item	Description
State	VNI status: - up - down To ensure that the VNI status is up, the corresponding VXLAN tunnel must exist and be up for the VNI. If the VNI status is down, check whether **Source** and **Peer List** in this command output are the same as **Source** and **Destination** in the output of the **display vxlan tunnel** command. - If they are different, no VXLAN tunnel exists for the specified VNI. Run the **source (NVE interface view)** or **vni head-end peer-list** command to change the source or destination IP address of the VXLAN tunnel to ensure that the corresponding VXLAN tunnel exists for the VNI. - If they are the same, collect related configuration and contact technical support personnel.
Number of vxlan vni bound to BD is	Number of existing VNIs bound to BDs.
VRF-ID	VPN instance ID.
Number of vxlan vni bound to VPN is	Number of existing VNIs bound to VPN instances.
Source	IP address of the source VTEP. To configure the IP address of the source VTEP, run the **source** command in the NVE interface view.
Source IPv6 Address	IPv6 address of the source VTEP. To configure the IPv6 address of the source VTEP, run the **source** command in the NVE interface view.
UDP Port	Destination UDP port. The port number is fixed as 4789.
Peer List	IP address of the destination VTEP. To configure the IP address of the destination VTEP, run the **vni head-end peer-list** command.
IPv6 Peer List	IPv6 address of the destination VTEP. To configure the IPv6 address of the destination VTEP, run the **vni head-end peer-list** command.

18.1.39 encapsulation (Layer 2 sub-interface view)

Function

The **encapsulation** command configures the encapsulation mode of packets allowed to pass a Layer 2 sub-interface.

The **undo encapsulation** command deletes the encapsulation mode of packets allowed to pass a Layer 2 sub-interface.

By default, the encapsulation mode of packets allowed to pass a Layer 2 sub-interface is not configured.

Format

encapsulation { **dot1q vid** *low-pe-vid* [**to** *high-pe-vid*] | **default** | **untag** | **qinq vid** *low-vlan-vid* [**to** *high-vlan-vid*] **ce-vid** *low-ce-vid* [**to** *high-ce-vid*] }

undo encapsulation { **dot1q vid** *low-pe-vid* [**to** *high-pe-vid*] | **default** | **untag** | **qinq vid** *low-vlan-vid* [**to** *high-vlan-vid*] **ce-vid** *low-ce-vid* [**to** *high-ce-vid*] }

Parameters

Parameter	Description	Value
dot1q	Sets encapsulation mode of packets allowed to pass a Layer 2 sub-interface to Dot1q. This mode enables a Layer 2 sub-interface to receive packets with a VLAN tag.	-
vid *low-pe-vid* [**to** *high-pe-vid*]	Specifies the outer VLAN ID in packets allowed to pass a Layer 2 sub-interface in Dot1q encapsulation mode. ● *low-pe-vid*: specifies the start VLAN ID. ● *high-pe-vid*: specifies the end VLAN ID. *high-pe-vid* must be greater than or equal to *low-pe-vid*. *high-pe-vid* and *low-pe-vid* define a range of VLAN IDs. ● If you do not specify **to** *high-pe-vid*, *low-pe-vid* specifies the single VLAN ID carried in packets.	The value is an integer that ranges from 2 to 4094.
default	Sets the encapsulation mode of packets allowed to pass a Layer 2 sub-interface to default. This mode enables a Layer 2 sub-interface to receive all packets, regardless of whether they contain VLAN tags.	-

Parameter	Description	Value
untag	Sets the encapsulation mode of packets allowed to pass a Layer 2 sub-interface to untag. This mode enables a Layer 2 sub-interface to receive packets without VLAN tags.	-
qinq	Sets encapsulation mode of packets allowed to pass a Layer 2 sub-interface to QinQ. This mode enables a Layer 2 sub-interface to receive packets with double VLAN tags.	-
vid *low-vlan-vid* [**to** *high-vlan-vid*]	Specifies the outer VLAN ID in double-tagged packets allowed to pass a Layer 2 sub-interface in QinQ encapsulation mode. ● *low-vlan-vid*: specifies the start VLAN ID. ● *high-vlan-vid*: specifies the end VLAN ID. *high-vlan-vid* must be greater than or equal to *low-vlan-vid*. *high-vlan-vid* and *low-vlan-vid* define a range of VLAN IDs. ● If you do not specify **to** *high-vlan-vid*, *low-vlan-vid* specifies the single VLAN ID carried in packets.	The value is an integer that ranges from 2 to 4094.
ce-vid *low-ce-vid* [**to** *high-ce-vid*]	Specifies the inner VLAN ID in double-tagged packets allowed to pass a Layer 2 sub-interface in QinQ encapsulation mode. ● *low-ce-vid*: specifies the start VLAN ID in an inner tag. ● *high-ce-vid*: specifies the end VLAN ID in an inner tag. *high-ce-vid* must be greater than or equal to *low-ce-vid*. *high-ce-vid* and *low-ce-vid* define a range of VLAN IDs in an inner VLAN tag. ● If you do not specify **to** *high-ce-vid*, *low-ce-vid* specifies the single VLAN ID in the inner VLAN tag carried in packets.	The value is an integer that ranges from 1 to 4094.

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VXLAN network, a Layer 2 sub-interface functions as a VXLAN service access point to forward data packets in a BD.

Packets passing through a physical interface may contain one or two VLAN tags or no VLAN tag. After you run the **encapsulation** command in a Layer 2 sub-interface view to configure the encapsulation mode, the sub-interface can forward only specified types of packets.

Prerequisites

Run the command **interface** *interface-type interface-number.subnum* **mode l2** to create a VXLAN Layer 2 sub-interface

Precautions

When configuring an encapsulation mode on a Layer 2 sub-interface, pay attention to the following points:

- The VLAN ID in **dot1q** mode or outer VLAN ID in **qinq** mode cannot be the same as the allowed VLAN of the corresponding main interface or the global VLAN.
- On the same main interface, the VLAN ID in **dot1q** mode and the outer VLAN ID in **qinq** mode must be different.
- After NAC authentication is configured on the main interface, the traffic encapsulation type on a Layer 2 sub-interface cannot be set to **default**.
- When the encapsulation mode of a Layer 2 sub-interface is **default**, the corresponding main interface cannot be added to any VLAN, including VLAN 1.
- Before the encapsulation mode of a Layer 2 sub-interface is set to **default**, the main interface has only one sub-interface.
- After the encapsulation mode of a Layer 2 sub-interface is set to **default**, no other sub-interface can be created on the main interface.
- When the encapsulation mode of a Layer 2 sub-interface is set to **untag**, the corresponding main interface cannot be added to VLAN 1, and other sub-interfaces of the main interface cannot be set to **untag**.
- You can configure only one encapsulation mode for each Layer 2 sub-interface. If an encapsulation mode has been configured for a Layer 2 sub-interface, run the **undo encapsulation** command to delete the original mode before you configure another mode.
- Before configuring a VLAN segment on a Dot1q or QinQ Layer 2 sub-interface, you must run the **rewrite pop none** command.

Example

Set the encapsulation mode of packets allowed to pass Layer 2 sub-interface GE0/0/1.1 to Dot1q and the outer VLAN ID in the packets to 10.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1 mode l2
[HUAWEI-GigabitEthernet0/0/1.1] encapsulation dot1q vid 10
```

18.1.40 evpn binding vpn-instance

Function

The **evpn binding vpn-instance** command binds an EVPN instance to a BD.

The **undo evpn binding vpn-instance** command unbinds an EVPN instance from a BD.

By default, no EVPN instance is bound to a BD.

Format

evpn binding vpn-instance *vpn-instance*

undo evpn binding vpn-instance

Parameters

Parameter	Description	Value
vpn-instance	Specifies an EVPN instance name.	The value must be an existing EVPN instance name.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where VXLAN is deployed through BGP EVPN, VXLAN BDs need to be bind to EVPN instances so that VXLAN tunnels can be dynamically created through BGP EVPN. You can run this command to bind an EVPN instance to a BD.

Precautions

Only one EVPN instance can be bound to a BD.

Example

Bind EVPN instance **evn10** to BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] evpn binding vpn-instance evn10
```

18.1.41 evpn mac-route enable

Function

The **evpn mac-route enable** command enables the MAC route function for BGP EVPN.

The **undo evpn mac-route enable** command disables the MAC route function for BGP EVPN.

By default, the MAC route function is disabled for BGP EVPN.

Format

evpn mac-route enable

undo evpn mac-route enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On a VXLAN network, if unidirectional isolation from the VXLAN access side to the tunnel side is enabled on a device using the **isolate remote enable** command, the device cannot learn MAC addresses through the received tunnel-side data packets. In this scenario, if communication between the access side and the tunnel side needs to be achieved, run the **evpn mac-route enable** command to enable the MAC route function for BGP EVPN. In this case, MAC address learning can be implemented and communication between the access side and the tunnel side can be achieved.

Example

Enable the MAC route function for BGP EVPN on the device.

```
<HUAWEI> system-view
[HUAWEI] evpn mac-route enable
```

18.1.42 evpn vpn-instance bd-mode

Function

The **evpn vpn-instance bd-mode** command creates an EVPN instance, and displays the EVPN instance view.

The **undo evpn vpn-instance bd-mode** command deletes an EVPN instance.

By default, no EVPN instance is created on a device.

Format

evpn vpn-instance *vpn-instance* **bd-mode**

undo evpn vpn-instance *vpn-instance* **bd-mode**

Parameters

Parameter	Description	Value
vpn-instance	Specifies an EVPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In the scenario where VXLAN is deployed through BGP EVPN, EVPN instances need to be created so that routes can be advertised between EVPN instances through the BGP protocol. You can run this command to create EVPN instances.

Example

Create EVPN instance **evn10**.

```
<HUAWEI> system-view
[HUAWEI] evpn vpn-instance evn10 bd-mode
[HUAWEI-evpn-instance-evn10]
```

18.1.43 export route-policy evpn

Function

The **export route-policy evpn** command associates the current VPN instance IPv4 or IPv6 address family with an export routing policy to filter EVPN routes to be advertised by the VPN instance IPv4 or IPv6 address family.

The **undo export route-policy evpn** command cancels the association between the IPv4 or IPv6 address family of a VPN instance and an export routing policy.

By default, the IPv4 or IPv6 address family of a VPN instance is not associated with any export routing policy.

Format

export route-policy *policy-name* **evpn**

undo export route-policy *policy-name* **evpn**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the export routing policy to be associated with the VPN instance IPv4 or IPv6 address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the IPv4 or IPv6 address family of a VPN instance adds all EVPN-VPN targets in the export EVPN-VPN target list to EVPN routes to be advertised by the IPv4 or IPv6 address family of the VPN instance to the EVPN address family. To control route export more precisely, run the **export route-policy** *policy-name* **evpn**command, specify the export routing policy to filter the routes to be advertised, and set attributes for eligible routes.

Prerequisites

- An RD has been configured for the IPv4 or IPv6 address family of the VPN instance by running the **route-distinguisher** *route-distinguisher* command.
- If no associated routing policy exists, a routing policy needs to be configured by running the **route-policy** command.

Precautions

- The IPv4 or IPv6 address family of a VPN instance can be associated with only one export routing policy. If the **export route-policy evpn** command is run more than once, the latest configuration overrides the previous one.
- The export routing policy configured using the **export route-policy evpn** command does not affect the export routing policy associated with another VPN instance using the **export route-policy** *policy-name* command.

Example

Associate the IPv4 address family of VPN instance **vrf1** with an export routing policy **policy-2** to filter EVPN routes to be advertised by the IPv4 address family of the VPN instance to the other VPN instances.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] export route-policy policy-2 evpn
```

18.1.44 hub-mode enable (VXLAN)

Function

The **hub-mode enable** command sets the access side mode to hub.

The **undo hub-mode enable** command cancels the hub mode on the access side.

By default, the access side mode is not set to hub.

NOTE

Only the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, and S5731-H switches support this command.

Format

hub-mode enable

undo hub-mode enable

Parameters

None

Views

VLAN view, Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

On a VXLAN, users connected to the same BD can directly communicate with each other. If the **isolate enable** command is run in the BD to isolate users on the access side. To enable users connected to a BD through a VLAN or a Layer 2 sub-interface to communicate with other users in the BD, you can run the **hub-mode enable** command in the VLAN or Layer 2 sub-interface view to set the access side mode to hub.

Example

Set the access side mode of VLAN 10 to hub.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] hub-mode enable
```

Set the access-side mode of Layer 2 sub-interface GE0/0/1.1 to hub.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1.1 mode l2
[HUAWEI-GigabitEthernet0/0/1.1] hub-mode enable
```

18.1.45 import route-policy evpn

Function

The **import route-policy evpn** command associates the IPv4 or IPv6 address family of a VPN instance with an import routing policy to filter EVPN routes imported.

The **undo import route-policy evpn** command cancels the association between the IPv4 or IPv6 address family of a VPN instance and an import routing policy.

By default, the IPv4 or IPv6 address family of a VPN instance is not associated with any import routing policy.

Format

import route-policy *policy-name* **evpn**

undo import route-policy *policy-name* **evpn**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the import routing policy to be associated with the IPv4 or IPv6 address family of a VPN instance.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance matches the export EVPN-VPN targets of the routes against the import EVPN-VPN targets of the IPv4 or IPv6 address family of the VPN instance to determine whether to import these IPv4 or IPv6 address family routes. To control EVPN route import more precisely, run the **import route-policy** *policy-name* **evpn** command to associate the VPN instance with an import routing policy and set attributes for eligible routes.

Prerequisites

- An RD has been configured for the IPv4 or IPv6 address family of the VPN instance by running the **route-distinguisher** *route-distinguisher* command.
- If no associated routing policy exists, a routing policy needs to be configured by running the **route-policy** command.

Precautions

- The IPv4 or IPv6 address family of a VPN instance can be associated with only one import routing policy. If the **import route-policy evpn** command is run several times, the latest configuration overrides the previous configurations.
- The import routing policy configured using the **import route-policy evpn** command does not affect the import routing policy applied to the VPN instance using the **import route-policy** *policy-name* command.

Example

Associate the IPv4 address family of VPN instance **vrf1** with an import routing policy **policy-1** to filter EVPN routes to be advertised by other VPN instances to the IPv4 address family of the VPN instance.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] import route-policy policy-1 evpn
```

18.1.46 interface nve

Function

The **interface nve** command creates a Network Virtualization Edge (NVE) interface and displays the NVE interface view.

The **undo interface nve** command deletes a specified NVE interface.

By default, no NVE interface is created.

Format

interface nve *nve-number*

undo interface nve *nve-number*

Parameters

Parameter	Description	Value
nve-number	Specifies the number of an NVE interface.	The value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fully use advantages of server virtualization, you can deploy VXLAN to connect to multiple tenants. VXLAN tunnel information needs to be configured on an NVE interface, so the **interface nve** command needs to be executed to create the NVE interface.

Precautions

After a VXLAN tunnel is configured, running the **undo interface nve** command will delete the specified NVE interface and all the configuration of the NVE interface.

Example

Create an NVE interface.

```
<HUAWEI> system-view
[HUAWEI] interface nve 1
```

18.1.47 interface vbdif

Function

The **interface vbdif** command creates a VBDIF interface and displays the VBDIF interface view, or displays the view of an existing VBDIF interface.

The **undo interface vbdif** command deletes a VBDIF interface.

By default, no VBDIF interface is created.

Format

interface vbdif *bd-id*

undo interface vbdif *bd-id*

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of a BD.	The value is an integer that ranges from 1 to 16777215.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP routes are required for communication between VXLAN networks on different network segments and between VXLAN and non-VXLAN networks.

To enable the communication, run the **interface vbdif** command to create a VBDIF interface for each BD and assign an IP address to the VBDIF interface. A VBDIF interface is a Layer 3 logical interface and can be configured with an IP address.

Prerequisites

- The specified BD has been created.
- If a BD contains user-side interfaces of the **default** subinterface type or the subinterface with **rewrite pop none**, the VBDIF interface cannot be configured in this BD.

Example

Create a VBDIF interface for BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] quit
[HUAWEI] interface vbdif 10
```

18.1.48 ipv6 nd collect host enable

Function

The **ipv6 nd collect host enable** command enables BGP EVPN to collect host IPv6 information.

The **undo ipv6 nd collect host enable** command disables BGP EVPN from collecting host IPv6 information.

By default, BGP EVPN is disabled from collecting host IPv6 information on a device.

Format

ipv6 nd collect host enable

undo ipv6 nd collect host enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a Layer 3 gateway to obtain the host information table, run the command in the VBDIF interface view so that EVPN can collect host IPv6 information.

In distributed VXLAN gateway deployment (BGP EVPN mode), if the VXLAN gateways advertise IRBv6 or ND routes to each other, run the command to advertise host IPv6 routes.

Prerequisites

IPv6 has been enabled in the VBDIF interface view using the **ipv6 enable** command.

Example

On VBDIF 10, enable BGP EVPN to collect host IPv6 information.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ipv6 enable
[HUAWEI-Vbdif10] ipv6 nd collect host enable
```

18.1.49 ipv6 nd distribute-gateway enable

Function

The **ipv6 nd distribute-gateway enable** command enables the IPv6 distributed gateway function on an interface.

The **undo ipv6 nd distribute-gateway enable** command disables the IPv6 distributed gateway function on an interface.

By default, IPv6 distributed gateway is disabled on an interface.

Format

ipv6 nd distribute-gateway enable

undo ipv6 nd distribute-gateway enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want a distributed gateway to learn ND packets only from hosts on the user side, run the **ipv6 nd distribute-gateway enable** command. After distributed gateway is enabled:

- The gateway processes only ND packets received from user hosts and generates host routes.
- The gateway deletes the ND packets learned from the network side and the hosts routes for the ND packets.

Prerequisites

IPv6 has been enabled in the VBDIF interface view using the **ipv6 enable** command.

Configuration Impact

After distributed gateway is enabled:

- Tunnel-side static ND entries cannot be configured on the gateway.
- In a distribution scenario, if multiple gateways use the same IPv6 address, the gateways do not report the address conflict.

Example

Enable IPv6 distributed gateway on VBDIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ipv6 enable
[HUAWEI-Vbdif10] ipv6 nd distribute-gateway enable
```

18.1.50 ipv6 nd multicast-suppress enable

Function

The **ipv6 nd multicast-suppress enable** command enables NS multicast suppression in a BD.

The **undo ipv6 nd multicast-suppress enable** command disables NS multicast suppression in a BD.

By default, NS multicast suppression is disabled in a BD.

Format

ipv6 nd multicast-suppress [**mismatch-discard**] **enable**

undo ipv6 nd multicast-suppress [**mismatch-discard**] **enable**

Parameters

Parameter	Description	Value
mismatch-discard	Indicates that the device drops NS packets that do not match any entries in the NS multicast suppression table.	-

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a network device receives an NS message to implement address resolution, the device forwards the NS message within its own BD. This NS message is received only by the nodes with the last 24 bits the same as the multicast address. If a device receives a large number of NS messages within a specified period, forwarding these NS messages uses excessive network resources and leads to network congestion and deteriorated network performance. As a result, user services are affected.

To resolve this problem, run the ipv6 nd multicast-suppress enable command to enable NS multicast suppression. With NS multicast suppression enabled, upon receipt of an NS message, a device checks whether the NS message contains information about the end user. If so, the device simply implements converts multicast streams to unicast streams. If not, the device forwards the NS message based on the original process. This reduces or suppresses message flooding occurred during address resolution.

Precautions

- When NS multicast suppression is configured in the VXLAN scenario with a large number of users and the NS packets received by the gateway exceeds the committed access rate (CAR), run the **car packet-type** *vpls-arp* **cir** *cir-value* [**cbs** *cbs-value*] command to adjust the CAR of the NS request packets. In the VXLAN scenario, the CAR for NS request packets is the same as that for vpls-arp packets. You can run the **display cpu-defend configuration** command to query the CAR. If the central processor CAR (CPCAR) is adjusted to an improper value, network services are affected. To adjust the CPCAR for packets, contact Huawei technical support.
- If the **ipv6 nd multicast-suppress enable** command is configured to enable NS multicast suppression in a BD and the **multicast-suppress enable** command is configured to enable multicast suppression in the BD, NS multicast suppression in the BD has a higher priority.

Example

Enable NS multicast suppression in BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] ipv6 nd multicast-suppress enable
```

Enable NS multicast suppression in BD 20 and configure the switch to discard ARP request packets if no matching entry is found in the NS multicast suppression table.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 20
[HUAWEI-bd20] ipv6 nd multicast-suppress mismatch-discard enable
```

18.1.51 ipv6 nd proxy enable

Function

The **ipv6 nd proxy enable** command enables routed proxy ND on an interface.

The **undo ipv6 nd proxy enable** command disables routed proxy ND on an interface.

By default, routed proxy ND is disabled on an interface.

Format

ipv6 nd proxy enable

undo ipv6 nd proxy enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two hosts physically belong to different network segments and no gateway is configured, run the **ipv6 nd proxy enable** command on the VBDIF interface of the device that connects the two hosts. This command enables routed proxy ND, which parses IPv6 addresses between the hosts.

Prerequisites

IPv6 has been enabled in the VBDIF interface view using the **ipv6 enable** command.

Precautions

After routed proxy ND is configured on an interface, the device counts the number of received NS unicast packets twice. As a result, the number of NS packets displayed in the **display cpu-defend statistics packet-type nd** command output may be greater than the actual number of NS packets sent to the CPU.

Example

Enable routed proxy ND on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ipv6 enable
[HUAWEI-Vbdif10] ipv6 nd proxy enable
```

18.1.52 ipv6 nd proxy local enable

Function

The **ipv6 nd proxy local enable** command enables intra-BD local proxy ND on an interface.

The **undo ipv6 nd proxy local enable** command disables intra-BD local proxy ND on an interface.

By default, intra-BD local proxy ND is disabled on an interface.

Format

ipv6 nd proxy local enable

undo ipv6 nd proxy local enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the overlay network of a VXLAN network is an IPv6 network, if two hosts belong to the same BD but they are isolated, to enable the hosts to communicate with each other, run the **ipv6 nd proxy local enable** command on the VBDIF interface. The command enables intra-BD local proxy ND on the interface.

Prerequisites

IPv6 has been enabled in the VBDIF interface view using the **ipv6 enable** command.

Precautions

After routed proxy ND is configured on an interface, the device counts the number of received NS unicast packets twice. As a result, the number of NS packets displayed in the **display cpu-defend statistics packet-type nd** command output may be greater than the actual number of NS packets sent to the CPU.

Example

Enable intra-BD local proxy ND on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ipv6 enable
[HUAWEI-Vbdif10] ipv6 nd proxy local enable
```

18.1.53 ipv6 neighbor (VXLAN)

Function

The **ipv6 neighbor** command configures a static IPv6 neighbor entry on an interface of a VXLAN network.

The **undo ipv6 neighbor** command deletes a static IPv6 neighbor entry configured on an interface of a VXLAN network.

By default, no static IPv6 neighbor entry is configured on an interface of a VXLAN network.

Format

ipv6 neighbor *ipv6-address mac-address* **vni** *vni-id* { **source-ip** *ipv4-address1* **peer-ip** *ipv4-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* }

undo ipv6 neighbor *ipv6-address mac-address* **vni** *vni-id* { **source-ip** *ipv4-address1* **peer-ip** *ipv4-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* }

ipv6 neighbor *ipv6-address mac-address* { **vid** *vlan-id1* [**cevid** *vlan-id2*] } **interface** *interface-type interface-num.subnum*

undo ipv6 neighbor *ipv6-address mac-address* { **vid** *vlan-id1* [**cevid** *vlan-id2*] } **interface** *interface-type interface-num.subnum*

ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id3* **interface** *interface-type interface-num*

undo ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id3* **interface** *interface-type interface-num*

NOTE

Only the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, and S5731-H support the **source-ipv6** and **peer-ipv6** parameters.

Parameters

Parameter	Description	Value
ipv6-address	Specifies a destination IPv6 address.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.
source-ip *ipv4-address1*	Specifies the IP address of the source VTEP.	The value is in dotted decimal notation.
peer-ip *ipv4-address2*	Specifies the IP address of the destination VTEP.	The value is in dotted decimal notation.
source-ipv6 *ipv6-address1*	Specifies the IPv6 address of the source VTEP.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
peer-ipv6 *ipv6-address2*	Specifies the IPv6 address of the destination VTEP.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
vid *vlan-id1*	Specifies the outer VLAN ID in the packet received by a interface.	The value is an integer that ranges from 1 to 4094.
cevid *vlan-id2*	Specifies the inner VLAN ID in the packet received by a interface.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number.subnum*	Specifies an L2 sub-interface.	-
vid *vlan-id3*	Specifies the VLAN ID in the packet received by a interface.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies an interface.	-

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VXLAN, if a Layer 3 gateway on a VXLAN is not enabled to send ND protocol packets, run the ipv6 neighbor command to configure a static IPv6 neighbor entry. To filter out invalid ND protocol packets, you can also run this command to bind the destination IPv6 addresses of these packets to nonexistent MAC addresses. To configure a static IPv6 neighbor entry for a VXLAN tunnel:

To configure static IPv6 neighbor entries on the VXLAN tunnel side, run the **ipv6 neighbor** *ipv6-address mac-address* **vni** *vni-id* { **source-ip** *ipv4-address1* **peer-ip** *ipv4-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* } command. If the current device has an access-side L2 sub-interface added to a BD, run the **ipv6 neighbor** *ipv6-address mac-address* { **vid** *vlan-id1* [**cevid** *vlan-id2*] } **interface** *interface-type interface-num.subnum* command to configure a static

IPv6 neighbor entry for the sub-interface. If the current device has an access-side interface added to a BD based a VLAN, run the **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id3* **interface** *interface-type interface-num* command to configure a static IPv6 neighbor entry for the interface.

Prerequisites

The IPv6 function has been enabled on a VBDIF interface using the **ipv6 enable** command.

In addition, before configuring a static IPv6 neighbor entry for the VXLAN tunnel side, ensure that a VNI ID has been associated with a BD using the **vxlan vni** command in the BD view on a VBDIF interface.

Precautions

- If the IPv6 address or MAC address specified in the **ipv6 neighbor** command is incorrect, communication with this neighbor fails.
- When the VXLAN tunnel is created dynamically, the device does not support to configure a static IPv6 neighbor entry on a VXLAN tunnel-side interface by the command **ipv6 neighbor** *ipv6-address mac-address* **vni** *vni-id* { **source-ip** *ipv4-address1* **peer-ip** *ipv4-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* }.

Example

Configure a static IPv6 neighbor entry for a VXLAN tunnel-side interface, and set the IP address to fc00:1::10 and MAC address to aaaa-fccc-1212.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] vxlan vni 5000
[HUAWEI-bd10] quit
[HUAWEI] interface nve 1
[HUAWEI-Nve1] source 10.1.1.1
[HUAWEI-Nve1] vni 5000 head-end peer-list 10.2.2.2
[HUAWEI-Nve1] quit
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ipv6 enable
[HUAWEI-Vbdif10] ipv6 address fc00:1::1/64
[HUAWEI-Vbdif10] ipv6 neighbor fc00:1::10 aaaa-fccc-1212 vni 5000 source-ip 10.1.1.1 peer-ip 10.2.2.2
[HUAWEI-Vbdif10] quit
```

Configure a static IPv6 neighbor entry in which the outbound interface is GE0/0/1, and set the IP address to fc00:1::11 and MAC address to aaaa-fccc-1212.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] l2 binding vlan 10
[HUAWEI-bd10] quit
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] ipv6 enable
[HUAWEI-Vbdif10] ipv6 address fc00:1::1/64
[HUAWEI-Vbdif10] ipv6 neighbor fc00:1::11 aaaa-fccc-1212 vid 10 interface GigabitEthernet 0/0/1
[HUAWEI-Vbdif10] quit
```

18.1.54 isolate enable (BD View)

Function

The **isolate enable** command enables isolation of users connected to an access-side BD.

The **undo isolate enable** command disables isolation of users connected to an access-side BD.

By default, isolation of users connected to an access-side BD is disabled.

NOTE

Only the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, and S5731-H switches support this command.

Format

isolate enable

undo isolate enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

In a VXLAN, users connected to the same BD can communicate. To isolate users connected to a BD, you can run the **isolate enable** command.

Example

Enables isolation of users connected to BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] isolate enable
```

18.1.55 isolate remote enable (BD view)

Function

The **isolate remote enable** command configures unidirectional isolation from the access side to the tunnel side in a BD.

The **undo isolate remote enable** command disables unidirectional isolation from the access side to the tunnel side in a BD.

By default, unidirectional isolation from the access side to the tunnel side is disabled in a BD.

NOTE

Only the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, and S5731-H support this command.

Format

isolate remote enable

undo isolate remote enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

On a VXLAN network, users in the same BD can directly communicate with each other. To isolate unidirectional traffic from the access side to the tunnel side in a BD, run this command in the BD view.

Example

Configure isolation from the access side to the tunnel side in BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] isolate remote enable
```

18.1.56 l2 binding vlan

Function

The **l2 binding vlan** command associates a specified VLAN with a BD.

The **undo l2 binding vlan** command restores the default settings.

By default, a VLAN is not associated with a BD.

Format

l2 binding vlan *vlan-id*

undo l2 binding vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094. Currently, VLAN 1 cannot be associated with a BD.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

On the access side, two methods are available for creating a large Layer 2 BD.

- Based on VLAN: You can associate one or multiple VLANs with a BD to add users in these VLANs to the BD. This VLAN-based mode implements larger-granularity control, but is easy to configure. It applies to VXLAN deployment on a live network.
- Based on encapsulation mode: The device sends packets of different encapsulation modes to different Layer 2 sub-interfaces based on the VLAN tags contained in the packets. You can bind a Layer 2 sub-interface to a BD to add specified users to the BD. This mode implements refined and flexible control but requires more complex configuration. It applies to VXLAN deployment on a new network.

After you run this command to associate specified VLANs with a BD, different VLANs associated with the same BD form a large Layer 2 network. Users belong to these VLANs can communicate at Layer 2 through VXLAN tunnels.

Prerequisites

The VLAN to be bound to the BD has been created using the **vlan** command.

Precautions

- One VLAN can be associated with only one BD, but one BD can be associated with multiple VLANs.
- After a global VLAN is associated with a BD, you need to add corresponding interfaces to the VLAN.

- If a VLAN is configured as a voice VLAN on the S6735-S, S6720-EI, S6720S-EI, the VLAN cannot be associated with a BD.
- In NAC authentication scenarios, if there are online users in a VLAN, running the **undo l2 binding vlan** command to unbind the VLAN from a BD makes the users go offline.
- If a VLAN is an ISP VLAN authorized to users and users exist in the VLAN on the device, the VLAN cannot be associated with a BD.
- If a VLAN is used as the management VLAN of a Fit AP, it is not recommended that the VLAN be associated with a BD.

Example

Associate VLAN 10 with BD 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] l2 binding vlan 10
```

18.1.57 l2vpn-family evpn

Function

The **l2vpn-family evpn** command enables and displays the BGP-EVPN address family view.

The **undo l2vpn-family evpn** command disables the BGP-EVPN address family view.

By default, the BGP-EVPN address family view is disabled.

Format

l2vpn-family evpn

undo l2vpn-family evpn

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Before performing configurations in the BGP-EVPN address family view, run the **l2vpn-family evpn** command in the BGP view to enable and display the BGP-EVPN address family view.

Example

Enable and display the BGP-EVPN address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn]
```

18.1.58 l3-interface virtual-mac compression

Function

The **l3-interface virtual-mac compression disable** command disables the virtual MAC address compression function. After the virtual MAC address compression function is disabled for a VBDIF interface on the S6720-EI, S6735-S and S6720S-EI, the device can still forward packets with destination MAC addresses in the range of 0000-5e00-0100 to 0000-5e00-01ff at Layer 2 when a MAC address is configured for the VBDIF interface.

The **l3-interface virtual-mac compression enable** command enables the virtual MAC address compression function. After a MAC address is configured for a VBDIF interface on the S6720-EI, S6735-S and S6720S-EI, the device cannot forward packets with destination MAC addresses in the range of 0000-5e00-0100 to 0000-5e00-01ff at Layer 2.

The **undo l3-interface virtual-mac compression disable** command restores the default setting of the virtual MAC address compression function.

By default, the virtual MAC address compression function is enabled.

NOTE

This command is supported only by the S6720-EI, S6735-S and S6720S-EI.

Format

l3-interface virtual-mac compression disable

l3-interface virtual-mac compression enable

undo l3-interface virtual-mac compression disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In a distributed gateway scenario where multiple Layer 3 gateways need to be simulated into one gateway, you need to run the **mac-address** command to configure the same MAC address for VBDIF interfaces on different Layer 3 gateways. In this way, terminals connect to the same gateway, ensuring normal traffic forwarding and VM migration. By default, the virtual MAC address compression function is enabled on the S6720-EI, S6735-S and S6720S-EI. After a MAC address is configured for a VBDIF interface, the device cannot forward packets with destination MAC addresses in the range of 0000-5e00-0100 to 0000-5e00-01ff at Layer 2. To enable the device to forward packets with destination MAC addresses in the range of 0000-5e00-0100 to 0000-5e00-01ff at Layer 2, run the **l3-interface virtual-mac compression disable** command to disable the virtual MAC address compression function.

Example

Disable the virtual MAC address compression function on the device.

```
<HUAWEI> system-view
[HUAWEI] l3-interface virtual-mac compression disable
```

18.1.59 mac rib-only

Function

The **mac rib-only** command configures a device not to deliver MAC address entries after receiving remote MAC routes.

The **undo mac rib-only** command configures a device to deliver MAC address entries after receiving remote MAC routes.

By default, a device is triggered to deliver MAC address entries after receiving remote MAC routes.

Format

mac rib-only

undo mac rib-only

Parameters

None

Views

EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a Layer 3 VXLAN gateway, if Layer 2 unicast traffic forwarding is not involved, you can run the **mac rib-only** command to configure a device not to deliver local MAC address entries after receiving VNI ID-based MAC routes advertised by the EVPN peer, saving forwarding entry resources.

Precautions

When this command is configured in an EVPN instance bound to a BD, the BD does not deliver MAC address entries after receiving remote MAC routes. Therefore, in this scenario, MAC address flapping in this BD does not depend on the MAC routes advertised by the remote BGP peer.

Example

Configure a device not to deliver MAC address entries after receiving remote MAC routes in evpn10.

```
<HUAWEI> system-view
[HUAWEI] evpn vpn-instance evpn10 bd-mode
[HUAWEI-evpn-instance-evpn10] mac rib-only
```

18.1.60 mac-address update host enable

Function

The **mac-address update host enable** command enables user host information update triggered by a MAC address entry change.

The **undo mac-address update host enable** command disables user host information update triggered by a MAC address entry change.

By default, user host information update triggered by a MAC address entry change is disabled.

Format

mac-address update host enable

undo mac-address update host enable

Parameters

None

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If user hosts migrate between different gateways in a distributed VXLAN gateway scenario and do not send gratuitous ARP or NA packets after the migration, you can run the **mac-address update host enable** command to configure the switch to be triggered to send ARP or NS requests to update user host information by changes in the user hosts' MAC address entries on the switch before and after the migration. This configuration ensures that user hosts can successfully go online after the migration.

Precautions

When the distributed gateway is the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, or S5731-H, the switch cannot learn a user host's MAC address from Layer 3 packets (the destination MAC address of the packets is the MAC address of the switch) sent by the user host. Therefore, the switch cannot be triggered to update user host information by Layer 3 traffic send by user hosts in this scenario. In this scenario, the switch can only be triggered to update user host information by Layer 2 traffic (the destination MAC address of the packets is not the MAC address of the switch) send by user hosts.

Example

Enable user host information update triggered by a MAC address entry change on VBDIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] mac-address update host enable
[HUAWEI-Vbdif10] quit
```

18.1.61 mac-address static bridge-domain

Function

The **mac-address static bridge-domain** command configures a static MAC address entry on a VXLAN access-side interface.

The **undo mac-address static bridge-domain** command deletes a static MAC address entry on a VXLAN access-side interface.

By default, no static MAC address entry is configured on a VXLAN access-side interface.

Format

mac-address static *mac-address interface-type interface-number.subnum* **bridge-domain** *bd-id* { **default** | **untag** | **vid** *vlan-id1* [**ce-vid** *vlan-id2*] }

undo mac-address static *mac-address interface-type interface-number.subnum* **bridge-domain** *bd-id* { **default** | **untag** | **vid** *vlan-id1* [**ce-vid** *vlan-id2*] }

mac-address static *mac-address interface-type interface-number* **bridge-domain** *bd-id* **vid** *vlan-id3*

undo mac-address static *mac-address interface-type interface-number* **bridge-domain** *bd-id* **vid** *vlan-id3*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in the static MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
interface-type interface-number.subnum	Specifies that the outbound interface in the static MAC address entry is a Layer 2 sub-interface.	-
bd-id	Specifies the BD to which the outbound interface belongs.	The value is an integer that ranges from 1 to 16777215.
default	Specifies that the outbound interface allows packets of the **default** type to pass.	-
untag	Specifies that the outbound interface allows packets of the **untag** type to pass.	-
vid *vlan-id1*	Specifies the outer VLAN ID in the packets allowed to pass the outbound interface.	The value is an integer that ranges from 1 to 4094.
ce-vid *vlan-id2*	Specifies the inner VLAN ID in the packets allowed to pass the outbound interface.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Specifies that the outbound interface in the static MAC address entry is a specified interface.	-
vid *vlan-id3*	Specifies the ID of the VLAN to which the outbound interface belongs.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device creates a MAC address table by learning source MAC addresses, the device cannot distinguish packets from authorized and unauthorized users. This threatens network security. If an unauthorized user uses the MAC address of an authorized user as the source MAC address of attack packets and connects to another interface of the device, the device learns an incorrect MAC address entry. The device incorrectly forwards the packets to the unauthorized user. Actually, the packets should be forwarded to the authorized user. You can run the **mac-address static bridge-domain** command to add a static MAC address entry to the MAC address table on the VXLAN access side. The static MAC address entry binds the MAC address to a specified interface, which prevents unauthorized users from intercepting data of authorized users. In addition, a manually configured static MAC address entry improves the unicast packet forwarding efficiency and saves bandwidth.

Prerequisites

- The interface has been added to a BD.

Example

Configure a static MAC address entry on a VXLAN access-side interface. In the entry, the destination MAC address is 00e0-fc12-3456 and the flow encapsulation type of the outbound interface is **dot1q**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bridge-domain 20
[HUAWEI-bd20] quit
[HUAWEI] interface gigabitethernet 0/0/1.1 mode l2
[HUAWEI-GigabitEthernet0/0/1.1] encapsulation dot1q vid 6
[HUAWEI-GigabitEthernet0/0/1.1] bridge-domain 20
[HUAWEI-GigabitEthernet0/0/1.1] quit
[HUAWEI] mac-address static 00e0-fc12-3456 GigabitEthernet 0/0/1.1 bridge-domain 20 vid 6
```

Configure a static MAC address entry on the VXLAN access-side interface. In the entry, the destination MAC address is 00e0-fc12-3457 and the outbound interface is added to a BD by the VLAN.

```
<HUAWEI> system-view
[HUAWEI] vlan 8
[HUAWEI-vlan8] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] port hybrid tagged vlan 8
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] bridge-domain 30
```

```
[HUAWEI-bd30] l2 binding vlan 8
[HUAWEI-bd30] quit
[HUAWEI] mac-address static 00e0-fc12-3457 GigabitEthernet 0/0/1 bridge-domain 30 vid 8
```

18.1.62 mac-address static bridge-domain vni

Function

The **mac-address static bridge-domain vni** command configures a static MAC address entry on a VXLAN tunnel-side interface.

The **undo mac-address static bridge-domain vni** command deletes a static MAC address entry on a VXLAN tunnel-side interface.

By default, no static MAC address entry is configured on a VXLAN tunnel-side interface.

Format

mac-address static *mac-address* **bridge-domain** *bd-id* { { **source** *ip-address1* **peer** *ip-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* } } **vni** *vni-id*

undo mac-address static *mac-address* **bridge-domain** *bd-id* { { **source** *ip-address1* **peer** *ip-address2* } | { **source-ipv6** *ipv6-address1* **peer-ipv6** *ipv6-address2* } } **vni** *vni-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in the static MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
bd-id	Specifies the BD to which the outbound interface belongs.	The value is an integer that ranges from 1 to 16777215.
source *ip-address1*	Specifies the source IP address of the VXLAN tunnel.	The value is in dotted decimal notation.
peer *ip-address2*	Specifies the remote IP address of the VXLAN tunnel.	The value is in dotted decimal notation.

Parameter	Description	Value
source-ipv6 *ipv6-address1*	Specifies the source IPv6 address of the VXLAN tunnel.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
peer-ipv6 *ipv6-address2*	Specifies the remote IPv6 address of the VXLAN tunnel.	The value consists of 128 bits, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format of X:X:X:X:X:X:X:X.
vni-id	Specifies the ID of a VXLAN tunnel.	The value is an integer that ranges from 1 to 16777215.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device creates a MAC address table by learning source MAC addresses, the device cannot distinguish packets from authorized and unauthorized users. This threatens network security. If an unauthorized user uses the MAC address of an authorized user as the source MAC address of attack packets and connects to another interface of the device, the device learns an incorrect MAC address entry. The device incorrectly forwards the packets to the unauthorized user. Actually, the packets should be forwarded to the authorized user. You can run the **mac-address static bridge-domain vni** command to add a static MAC address entry to the MAC address table on the VXLAN tunnel side. The static MAC address entry binds the MAC address to a specified interface, which prevents unauthorized users from intercepting data of authorized users. In addition, a manually configured static MAC address entry improves the unicast packet forwarding efficiency and saves bandwidth.

Prerequisites

- A VXLAN tunnel has been created.
- When the VXLAN tunnel is created dynamically, the device does not support to configure a static MAC address entry on a VXLAN tunnel-side interface.

Precautions

If a static MAC address entry is configured on a VXLAN tunnel-side interface and the VXLAN tunnel is Down, the static MAC address entry is not displayed in the output of the **display mac-address** command. When the VXLAN tunnel is Up, the static MAC address entry is displayed in the output of the **display mac-address** command.

Example

On a VXLAN tunnel-side interface, configure a static MAC address entry with the destination MAC address 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 20
[HUAWEI-bd20] vxlan vni 2000
[HUAWEI-bd20] quit
[HUAWEI] interface nve 1
[HUAWEI-Nve1] source 10.1.1.2
[HUAWEI-Nve1] vni 2000 head-end peer-list 10.1.2.2
[HUAWEI-Nve1] quit
[HUAWEI] mac-address static 00e0-fc12-3456 bridge-domain 20 source 10.1.1.2 peer 10.1.2.2 vni 2000
```

18.1.63 mac-address (VBDIF interface view)

Function

The **mac-address** command configures the MAC address of a VBDIF interface.

The **undo mac-address** command restores the default MAC address of a VBDIF interface.

By default, the MAC address of a VBDIF interface is the system MAC address.

Format

mac-address *mac-address*

undo mac-address

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a VBDIF interface.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number, such as 00e0 or fc01. If you enter fewer than four alphanumeric characters, 0s are added before the input digits. For example, if e0 is entered, 00e0 is specified. A MAC address cannot be set to all 0s or all 1s. The MAC address of a VBDIF interface ranges from 0000-5e00-0100 to 0000-5e00-01ff.

Views

VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a distributed gateway scenario, multiple Layer 3 gateways are simulated into one gateway. You need to run the **mac-address** command to configure the same MAC address for the VBDIF interfaces on these Layer 3 gateways to ensure normal traffic forwarding and VM migration. Using the same MAC address, the Layer 3 gateways act like one gateway for terminals.

Precautions

- After the MAC address of a VBDIF interface is changed, the switch proactively sends gratuitous ARP packets to update the mapping relationship between MAC addresses and ports.
- The MAC address configured for a VBDIF interface cannot be the same as the virtual MAC address of a VRRP group on the switch. You can run the **display vrrp** and **display vrrpv6** commands to view virtual MAC addresses of VRRP groups configured on the switch.

Example

Set the MAC address of VBDIF interface 10 to 0000-5e00-0101.

```
<HUAWEI> system-view
[HUAWEI] interface vbdif 10
[HUAWEI-Vbdif10] mac-address 0000-5e00-0101
```

18.1.64 mac-route no-advertise

Function

The **mac-route no-advertise** command configures a device not to advertise local MAC routes.

The **undo mac-route no-advertise** command configures a device to advertise local MAC routes.

By default, a device advertises local MAC routes.

Format

mac-route no-advertise

undo mac-route no-advertise

Parameters

None

Views

EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a Layer 3 VXLAN gateway, if Layer 2 unicast traffic forwarding is not involved, you can run the **mac-route no-advertise** command to configure the gateway not to advertise local MAC routes. In this case, the remote gateway cannot receive MAC routes, saving the memory for learning unnecessary MAC routes.

Precautions

When this command is configured in an EVPN instance bound to a BD, the corresponding MAC routes in the BD are no longer externally advertised. Therefore, in this scenario, MAC address flapping on the device where the corresponding BGP peer resides does not depend on the MAC routes advertised by the local device.

Example

Configure a device not to advertise local MAC routes in evpn10.

```
<HUAWEI> system-view
[HUAWEI] evpn vpn-instance evpn10 bd-mode
[HUAWEI-evpn-instance-evpn10] mac-route no-advertise
```

18.1.65 multicast-suppression (BD view)

Function

The **multicast-suppression** command enables multicast traffic suppression in a BD.

The **undo multicast-suppression** command disables multicast traffic suppression in a BD.

By default, multicast traffic suppression is disabled in a BD.

Format

multicast-suppression cir *cir-value* [**cbs** *cbs-value*]

undo multicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. If the **cbs** is not set, the default *cbs-value* is 125 times the *cir-value*.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

When a large number of multicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected. You can run the **multicast-suppression** command to enable multicast traffic suppression in a BD and configure the maximum number of multicast packets that can pass through a BD. When the multicast traffic volume exceeds the specified threshold, the system discards excess multicast packets.

Example

Set the CIR value for multicast traffic in BD 10 to 100 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] multicast-suppression cir 100
```

18.1.66 peer advertise

Function

The **peer advertise** command configures a device to advertise ARP, integrated routing and bridging (IRB), ND, or IRBv6 routes to its BGP EVPN peers.

The **undo peer advertise** command restores the default configurations.

By default, a device cannot advertise ARP, IRB, ND, or IRBv6 routes to its BGP EVPN peers.

Format

peer { *ipv4-address* | *group-name* } **advertise** { **arp** | **irb** }

undo peer { *ipv4-address* | *group-name* } **advertise** { **arp** | **irb** }

peer { *ipv4-address* | *group-name* } **advertise** { **nd** | **irbv6** }

undo peer { *ipv4-address* | *group-name* } **advertise** { **nd** | **irbv6** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
arp	Specifies the ARP routes to be advertised.	-
irb	Specifies the IRB routes to be advertised.	-
nd	Specifies the ND routes to be advertised.	-
irbv6	Specifies the IRBv6 routes to be advertised.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the overlay network is an IPv4 network, to allow a device to advertise ARP or IRB routes to its BGP EVPN peers, run the **peer advertise** command. This command allows VTEPs to implements ARP broadcast suppression on networks. If you specify **irb**, VTEPs can also transmit host routes.

When the overlay network is an IPv6 network, to allow a device to advertise ND or IRBv6 routes to its BGP EVPN peers, run the **peer advertise** command. This command allows VTEPs to implements NS broadcast suppression on networks. If you specify **irbv6**, VTEPs can also transmit host routes.

Precautions

You cannot specify both **arp** and **irb** in the same BGP-EVPN address family view.

You cannot specify both **nd** and **irbv6** in the same BGP-EVPN address family view.

Example

Configure a device to advertise ARP routes to its BGP EVPN peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] peer 1.1.1.1 advertise arp
```

18.1.67 peer advertise route-reoriginated

Function

The **peer advertise route-reoriginated** command enables a device to advertise IP prefix routes re-encapsulated by the EVPN address family to a BGP EVPN peer.

The **undo peer advertise route-reoriginated** command restores the default configuration.

By default, the local device does not advertise IP prefix routes re-encapsulated by the EVPN address family to a BGP EVPN peer.

Format

peer { *ipv4-address* | *group-name* } **advertise route-reoriginated evpn ip**

undo peer { *ipv4-address* | *group-name* } **advertise route-reoriginated evpn ip**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP EVPN peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a BGP EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
evpn	Re-encapsulates the received EVPN routes.	-
ip	Re-encapsulates the IP prefix routes in the received EVPN routes.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In three-segment VXLAN scenarios, to re-encapsulate EVPN routes received from a DC into IP prefix routes and then send them to the BGP EVPN peer in another DC, run the **peer advertise route-reoriginated** command. This configuration allows communication between VMs in different DCs.

During EVPN route re-encapsulation, a border leaf node receives an EVPN route from a DC and changes the route next hop to the VTEP address of the leaf node. Additionally, the leaf node replaces the source MAC address in the gateway MAC attribute of the host route with its own MAC address and the L3VNI with that of an L3VPN instance.

Prerequisites

The device has been enabled to add a regeneration flag to the routes received from BGP EVPN peers using the **peer** { *ipv4-address* | *group-name* } **import reoriginate** command.

Example

Enable a device to advertise regenerated IP prefix routes to a BGP EVPN peer.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 2.2.2.2 as-number 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] peer 2.2.2.2 enable
[HUAWEI-bgp-af-evpn] peer 2.2.2.2 import reoriginate
[HUAWEI-bgp-af-evpn] peer 2.2.2.2 advertise route-reoriginated evpn ip
```

18.1.68 peer enable (BGP-EVPN address family view)

Function

The **peer enable** command enables a device to exchange route information with a peer or peer group in the address family view.

The **undo peer enable** command disables a device from exchanging route information with a peer or peer group.

By default, only the peers of the BGP-IPv4 unicast address family are automatically enabled.

Format

peer { *group-name* | *ipv4-address* } **enable**

undo peer { *group-name* | *ipv4-address* } **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, only the peers of the BGP-IPv4 unicast address family are automatically enabled. After the **peer as-number** command is run in the BGP view, the system automatically runs the **peer enable** command to enable a peer. In the BGP EVPN address family view, the **peer enable** command must be manually run to enable a peer.

Prerequisites

The **peer as-number** command has been run to create a peer or peer group.

Example

Configure a peer and enable the peer in the BGP-EVPN address family view.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 1.1.1.2 as-number 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] peer 1.1.1.2 enable
```

18.1.69 peer import reoriginate

Function

The **peer import reoriginate** command enables a device to add a regeneration flag to the routes received from BGP EVPN peers.

The **undo peer import reoriginate** command restores the default configuration.

By default, a device does not add a regeneration flag to the routes received from BGP EVPN peers.

Format

peer { *ipv4-address* | *group-name* } **import reoriginate**

undo peer { *ipv4-address* | *group-name* } **import reoriginate**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP EVPN peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a BGP EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a three-segment VXLAN scenario, by default, an edge node that connects to a carrier network does not re-encapsulate the routes received from BGP EVPN peers, causing the EVPN routes to be terminated on the edge node. As a result, the EVPN routes from one DC cannot be advertised to the BGP EVPN peers of another DC. To address this problem, run the **peer import reoriginate** command to enable the edge node to add a regeneration flag to the routes received from BGP EVPN peers. The edge node then re-encapsulates the EVPN routes received from one DC before sending them to another DC for inter-DC VM communication.

Prerequisites

A device has been enabled to exchange routes with a specified peer or peer group using the **peer** { *group-name* | *ipv4-address* } **enable** command.

Example

Enable a device to add a regeneration flag to the routes received from BGP EVPN peers.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] peer 1.1.1.1 as-number 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] peer 1.1.1.1 enable
[HUAWEI-bgp-af-evpn] peer 1.1.1.1 import reoriginate
```

18.1.70 peer mac-limit

Function

The **peer mac-limit** command limits the number of MAC advertisement routes received from a peer.

The **undo peer mac-limit** command restores the default configuration.

By default, the number of MAC advertisement routes received from a peer is not limited.

Format

peer { *group-name* | *ipv4-address* } **mac-limit** *number* [**idle-forever** | **idle-timeout** *times*]

undo peer { *group-name* | *ipv4-address* } **mac-limit**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
number	Specifies the maximum number of MAC advertisement routes received from a peer.	The value is an integer, the value varies according to different devices.
idle-forever	Indicates that a terminated connection is not automatically re-established after the number of routes exceeds the maximum limit.	-
idle-timeout *times*	Specifies a timer for automatically re-establishing a terminated connection after the number of routes exceeds the maximum limit. No connection will be automatically re-established before the timer expires.	The value is an integer that ranges from 1 to 1200, in minutes.

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP-EVPN instance may import many invalid MAC advertisement routes from peers. In this case, To prevent these routes from occupying a large proportion of MAC advertisement routes, run the **peer mac-limit** command to configure the maximum number of MAC advertisement routes allowed to be received from each peer.

Precautions

- After this command is run, excessive routes in the BGP-EVPN address family view may be discarded.
- When the number of MAC advertisement routes exceeds the maximum limit, run the **undo peer mac-limit** command. The device then receives routes from each peer and adds them to the EVPN routing table.

Example

Configure the maximum number of MAC advertisement routes received by a device from peer 2.2.2.2 as 1000.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] peer 2.2.2.2 mac-limit 1000
```

18.1.71 peer route-policy (BGP-EVPN address family view)

Function

The **peer route-policy** command specifies a routing policy for filtering routes received from an EVPN peer or peer group or routes to be advertised to an EVPN peer or peer group.

The **undo peer route-policy** command deletes a specified routing policy.

By default, no routing policy is used for filtering routes received from an EVPN peer or peer group or routes to be advertised to an EVPN peer or peer group.

Format

peer { *group-name* | *ipv4-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* } **route-policy** *route-policy-name* { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of an EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of an EVPN peer.	The value is in dotted decimal notation.
route-policy-name	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a routing policy to routes to be imported from an EVPN peer or peer group.	-
export	Applies a routing policy to routes to be advertised to an EVPN peer or peer group.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a routing policy is created, the **peer route-policy** command is run to apply a routing policy to an EVPN peer or peer group so that the routes advertised to or received from the peer or peer group can be controlled. To be specific, only the necessary routes are received from or advertised to the peer or peer group. In this manner, route management is implemented, the scale of the routing table is reduced, and fewer network resources are consumed.

Prerequisites

- The ability to exchange EVPN routes with the peer or a group has been enabled using the **peer** { *group-name* | *ipv4-address* } **enable**.
- The corresponding routing policy has been established. By default, nonexistent routing policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the

system view and a nonexistent routing policy is referenced using this command, all routes are advertised to neighbors or all routes are received.

Precautions

If a routing policy is specified for an EVPN peer, all the peers in the EVPN peer group inherit the configuration.

Example

Apply routing policy **test-rp** to the routes received from EVPN peer 1.1.1.9.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] peer 1.1.1.9 enable
[HUAWEI-bgp-af-evpn] peer 1.1.1.9 route-policy test-rp import
```

18.1.72 policy vpn-target (BGP-EVPN address family view)

Function

The **policy vpn-target** command enables a device to filter received EVPN routes by the EVPN-VPN target.

The **undo policy vpn-target** command cancels EVPN-VPN target-based filtering of received EVPN routes.

By default, EVPN-VPN target-based filtering of received EVPN routes is enabled.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

After EVPN-VPN target-based filtering is enabled, only EVPN routes whose export EVPN-VPN target attribute matches the import EVPN-VPN target attribute are received.

Example

Enable a device to implement EVPN-VPN target-based filtering for received EVPN routes.

```
<HUAWEI> system-view
[HUAWEI] bgp 100
[HUAWEI-bgp] l2vpn-family evpn
[HUAWEI-bgp-af-evpn] policy vpn-target
```

18.1.73 port nvo3 mode access

Function

The **port nvo3 mode access** command configures an interface as a VXLAN access-side interface to allow common IP packets carrying the destination UDP port number 4789 of VXLAN packets to enter a VXLAN network.

The **undo port nvo3 mode access** command restores the default setting.

By default, an interface is not configured as a VXLAN access-side interface and cannot forward common IP packets carrying the destination UDP port number 4789 of VXLAN packets to a VXLAN network.

NOTE

Only the S6720-EI, S6735-S, and S6720S-EI switches support this command.

Format

port nvo3 mode access

undo port nvo3 mode access

Parameters

None

Views

XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if an access-side interface is on an S6720-EI, S6735-S, or S6720S-EI and the VXLAN function is configured, when the interface receives common IP packets carrying the destination UDP port number 4789 of VXLAN packets, the packets are discarded due to VXLAN decapsulation. In scenarios where common IP packets carrying the destination UDP port number 4789 of VXLAN packets need to enter a VXLAN network or other transparent transmission scenarios (such as QinQ and

VLAN mapping scenarios), you can run the **port nvo3 mode access** command on an interface to configure the interface as a VXLAN access-side interface. In this case, the interface can forward the received packets with UDP port number 4789.

Precautions

After the **port nvo3 mode access** command is configured on an interface, the interface cannot perform VXLAN decapsulation for received VXLAN-encapsulated packets. Therefore, this command can only be used on access-side interfaces.

Example

Specify XGE0/0/1 as a VXLAN access-side interface.

```
<HUAWEI> system-view
[HUAWEI] interface XGigabitEthernet 0/0/1
[HUAWEI-XGigabitEthernet0/0/1] port nvo3 mode access
```

18.1.74 refresh bgp evpn

Function

The **refresh bgp evpn** command soft resets an EVPN connection.

Format

refresh bgp evpn { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

Parameters

Parameter	Description	Value
all	Soft resets all EVPN connections.	-
ipv4-address	Specifies the IPv4 address of an EVPN peer.	The value is in dotted decimal notation.
group *group-name*	Specifies the name of an EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Specifies the EVPN peer of an EBGP connection.	-
internal	Specifies the EVPN peer of an IBGP connection.	-
export	Triggers a soft reset in the export direction.	-
import	Triggers a soft reset in the import direction.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **refresh bgp evpn** command to manually soft reset an EVPN connection. EVPN soft resets can update the EVPN routing table without interrupting a BGP connection and apply new filtering policies.

If a policy application delay time is configured:

- When the routing policy is set to neighbor import by running the **peer route-policy import** command, you can run the **refresh bgp evpn all** command to trigger BGP to re-apply the routing policy.
- When the routing policy is set to neighbor export by running the **peer route-policy export** command, the routing policy is not re-applied even if the **refresh bgp evpn all** command is run.

Example

Soft reset all BGP-EVPN connections in the import direction to make new configurations take effect.

```
<HUAWEI> refresh bgp evpn all import
```

18.1.75 reset bgp evpn

Function

The **reset bgp evpn** command resets the BGP connections of a BGP EVPN address family.

Format

reset bgp evpn { **all** | *as-number-plain* | *as-number-dot* | **group** *group-name* | *ipv4-address* }

Parameters

Parameter	Description	Value
all	Resets all BGP connections of a BGP EVPN address family.	-
as-number-plain	Specifies an integral AS number.	The value is an integer that ranges from 1 to 4294967295.

Parameter	Description	Value
as-number-dot	Specifies an AS number in dotted notation.	The value is in the format of x.y, where x and y are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the connection with a specified BGP peer.	The value is in dotted decimal notation.
group *group-name*	Resets the connection with a specified BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

When the BGP EVPN configuration is changed, you can run the **reset bgp evpn** command to make the new configuration take effect immediately.

NOTICE

After the command is run, the TCP connection established by the BGP device is reset and the corresponding peer relationship is re-established. Therefore, exercise caution before you run this command.

Example

Reset all BGP connections of a BGP EVPN address family.

```
<HUAWEI> reset bgp evpn all
```

18.1.76 reset bridge-domain statistics

Function

The **reset bridge-domain statistics** command clears packet statistics in a BD.

Format

reset bridge-domain *bd-id* **statistics**

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of a BD packet statistics of which are to be deleted.	The value is an integer that ranges from 1 to 16777215.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you collect packet statistics in a specified BD within a specific period, run the **reset bridge-domain statistics** command to clear the existing statistics in the BD to ensure statistics accuracy.

Precautions

Packet statistics cannot be restored after you clear them; therefore, exercise caution before you run the **reset bridge-domain statistics** command.

Example

Clear packet statistics in BD 10.

```
<HUAWEI> reset bridge-domain 10 statistics
```

18.1.77 reset vxlan statistics

Function

The **reset vxlan statistics** command clears VXLAN tunnel packet statistics.

Format

reset vxlan statistics source *source-ip-address* **peer** *peer-ip-address* [**vni** *vni-id*]

reset vxlan statistics source *source-ipv6-address* **peer** *peer-ipv6-address* [**vni** *vni-id*]

NOTE

Only the S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, S5731-H, and S6730-S support the **source** and **peer** parameters configured as IPv6 address.

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the IPv4 address of the source VTEP.	The value is in dotted decimal notation.
peer *peer-ip-address*	Specifies the IPv4 address of the destination VTEP.	The value is in dotted decimal notation.
source *source-ipv6-address*	Specifies the IPv6 address of the source VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
peer *peer-ipv6-address*	Specifies the IPv6 address of the destination VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you collect VXLAN tunnel packet statistics within a specific period, run the **reset vxlan statistics** command to clear the existing statistics to ensure statistics accuracy.

Precautions

Packet statistics cannot be restored after you clear them; therefore, exercise caution before you run the **reset vxlan statistics** command.

Example

Clear statistics on VXLAN tunnel packets, with 10.10.1.1 and 10.1.1.1 as the source and destination VTEP IP addresses.

```
<HUAWEI> reset vxlan statistics source 10.10.1.1 peer 10.1.1.1
```

18.1.78 rewrite pop

Function

The **rewrite pop** command enables the device to remove VLAN tags from packets received by Layer 2 sub-interfaces.

The **undo rewrite pop** command disables the device from removing VLAN tags from packets received by Layer 2 sub-interfaces.

By default, the device removes two VLAN tags from packets received by Layer 2 sub-interfaces that use QinQ encapsulation, removes one VLAN tag from packets received by Layer 2 sub-interfaces that use Dot1q encapsulation.

Format

rewrite pop { **single** | **double** | **none** }

undo rewrite pop { **single** | **double** | **none** }

Parameters

Parameter	Description	Value
single	Configures the device to remove one VLAN tag from received packets. This parameter can only be configured on Layer 2 sub-interfaces that use Dot1q encapsulation and no VLAN segment can be configured for Layer 2 sub-interfaces.	-
double	Configures the device to remove one VLAN tag from received packets. This parameter can only be configured on Layer 2 sub-interfaces that use QinQ encapsulation and no VLAN segment can be configured for Layer 2 sub-interfaces.	-
none	Configures the device not to remove VLAN tags from received packets. That is, the device transparently transmits received packets without modifying them. This parameter can only be configured on Layer 2 sub-interfaces that use QinQ or Dot1q encapsulation.	-

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a Layer 2 sub-interface with the encapsulation type being Dot1q or QinQ is configured as a VXLAN service access point on a VXLAN, to enable the sub-interface to remove the VLAN tag from received packets, run the **rewrite pop** command.

Precautions

Before running the **encapsulation** command to configure a VLAN segment on a Dot1q or QinQ Layer 2 sub-interface, you must run the **rewrite pop** command to specify the operation of removing VLAN tags as **none**.

Example

Configure the device to remove two VLAN tags from packets received by a Layer 2 sub-interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1 mode l2
[HUAWEI-GigabitEthernet0/0/1.1] rewrite pop double
```

18.1.79 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for an EVPN instance address family.

By default, no RD is configured for an EVPN instance address family.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD. The RD can be in the following forms: ● 2-byte AS number: 4-byte user-defined number, for example, 101:3. The AS number ranges from 0 to 65535, and the user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● Integral 4-byte AS number: 2-byte user-defined number, for example, 0:3 or 65537:3. The AS number ranges from 65536 to 4294967295, and the user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. The 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535, and the user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4 address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535.	-

Views

EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an EVPN instance is created, run this command to configure an RD in the EVPN instance view.

Different EVPN instances may have the same route prefix. RDs can be configured for EVPN instances so that EVPN routes sent to the peer device are added with RD attributes. In this way, EVPN routes are unique globally and Rx devices can easily distinguish EVPN instances.

Precautions

After you configure the RD for an EVPN instance address family, the RD cannot be modified or deleted. When you need to modify an RD, delete the corresponding EVPN instance and reconfigure the RD.

Example

Configure an RD for EVPN instance **evn1**.

```
<HUAWEI> system-view
[HUAWEI] evpn vpn-instance evn1 bd-mode
[HUAWEI-evpn-instance-evn1] route-distinguisher 22:1
```

18.1.80 service type vxlan-tunnel

Function

The **service type vxlan-tunnel** command configures an Eth-Trunk as a VXLAN loopback interface.

The **undo service type vxlan-tunnel** command cancels the configuration.

By default, an Eth-Trunk is not a VXLAN loopback interface.

NOTE

Only the S6720-EI, S6735-S, and S6720S-EI switches support this command.

Format

service type vxlan-tunnel

undo service type vxlan-tunnel

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The S6720-EI, S6735-S, and S6720S-EI switches can decapsulate received VXLAN packets and forward them at Layer 3 only after a VXLAN loopback interface is configured on them. As a result, you need to configure an Eth-Trunk as the VXLAN loopback interface when the S6720-EI, S6735-S, and S6720S-EI switches function as the Layer 3 VXLAN gateway.

Follow-up Procedure

Run the **trunkport** command to add member interfaces to the VXLAN loopback interface.

Precautions

- After an Eth-Trunk is configured as a VXLAN loopback interface, STP is automatically disabled on the Eth-Trunk. The Eth-Trunk then does not support STP configuration commands. After the configuration is canceled, STP is automatically enabled on the Eth-Trunk.
- Only one Eth-Trunk on a switch can be configured as the VXLAN loopback interface. VXLAN packets from all VBDIF interfaces are encapsulated and decapsulated by this loopback interface.
- An Eth-Trunk containing member interfaces cannot be configured as a VXLAN loopback interface.
- The configurations allowed on an Eth-Trunk to be configured as a loopback interface include **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **traffic-policy (interface view)**, and **trust**. If other configurations exist on the Eth-Trunk, the Eth-Trunk cannot be configured as a loopback interface.
- After an Eth-Trunk is configured as a loopback interface, the Eth-Trunk supports only the following configurations: **authentication open ucl-policy enable**, **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **statistic enable (interface view)**, **traffic-policy (interface view)**, **vcmp disable**, and **trust**.
- Before running the **undo service type vxlan-tunnel** command, delete all the member interfaces of the Eth-Trunk interface and all VBDIF interfaces on the device.

Example

Configure Eth-Trunk 1 as a VXLAN loopback interface.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-Trunk 1
[HUAWEI-Eth-Trunk1] service type vxlan-tunnel
```

18.1.81 set vxlan resource super-mode

Function

The **set vxlan resource super-mode** command sets the super VXLAN resource mode.

The **undo set vxlan resource super-mode** command restores the default VXLAN resource mode.

By default, the device supports 4095 BDs.

NOTE

Only the S5731S-H, S6730-H, S6730S-H, S5731-H, and S5732-H support this command.

Format

set vxlan resource super-mode

undo set vxlan resource super-mode

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When VXLAN is configured, the device supports 4095 BDs by default. If you want more than 4095 BDs, run the **set vxlan resource super-mode** command to set the super VXLAN resource mode. After this command is configured, the device supports 16000 BDs.

Precautions

- After setting the super VXLAN resource mode, save the configuration and then restart the device to make the configuration take effect.
- When the super VXLAN resource mode is configured, the forwarding performance of some services may degrade, such as the IP multicast, VPLS, VLAN mapping, Layer 3 traffic forwarding of sub-interfaces, and VLAN stacking services.

Example

Set the super VXLAN resource mode.

```
<HUAWEI> system-view
[HUAWEI] set vxlan resource super-mode
```

18.1.82 source (NVE interface view)

Function

The **source** command configures an IP address for the source VXLAN tunnel endpoint (VTEP) of a VXLAN tunnel.

The **undo source** command deletes the IP address of the source VTEP of a VXLAN tunnel.

By default, no IP address is configured for the source VTEP of a VXLAN tunnel.

Format

source *ip-address*

undo source [*ip-address*]

source *ipv6-address*

undo source [*ipv6-address*]

NOTE

Only the S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, S5731-H, and S6730-S support the *ipv6-address* parameter.

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a source VTEP.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a source VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

NVE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

To establish a VXLAN tunnel, configure IP addresses for the source and destination VTEPs.

To configure an IP address for a source VTEP, run this command. When access service packets reach a Network Virtualization Edge (NVE), the VTEP encapsulates the packets based on the IP addresses of source and destination VTEPs and forwards them.

Precautions

- You can specify the IP address of a physical interface or a loopback interface as the IP address of the source VTEP. The address of a loopback interface is recommended.

- Generally, the NVE interfaces of different devices must be configured with different VTEP addresses; otherwise, traffic forwarding errors may occur.
- The IP address of a VBDIF interface cannot be configured as the IP address of the source VTEP of a VXLAN tunnel.

Follow-up Procedure

After running the **source** command, you can run the **vni head-end peer-list** command to configure an IP address for the destination VTEP.

Example

Set the IP address of the source VTEP of a VXLAN tunnel to 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] interface nve 1
[HUAWEI-Nve1] source 10.1.1.2
```

18.1.83 statistics enable (BD view)

Function

The **statistics enable** command enables statistics collection in a BD.

The **undo statistics enable** command disables statistics collection in a BD.

By default, statistics collection is disabled in a BD.

Format

statistics enable

undo statistics enable

Parameters

None

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Packet statistics in a BD provide information about the number of packets going into and leaving a BD.

To view packet statistics in a BD, run the **statistics enable** and **display bridge-domain statistics** commands in sequence. The information helps you locate faults.

Example

Enable packet statistics collection in BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] statistics enable
```

18.1.84 undo mac-address bridge-domain

Function

The **undo mac-address bridge-domain** command deletes MAC address entries of a BD.

Format

undo mac-address bridge-domain *bd-id*

Parameters

Parameter	Description	Value
bd-id	Deletes MAC address entries of a specified BD.	The value is an integer that ranges from 1 to 16777215.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The MAC address table space is limited on a device. If the number of MAC address entries reaches the upper limit, the device cannot learn new MAC address entries before some entries in the MAC address table are aged out. In this case, the device broadcasts packets from new users, wasting network resources. To solve the problem, you can run the **undo mac-address bridge-domain** command to manually delete unnecessary MAC address entries of a specified BD.

Example

Delete MAC address entries of BD 20.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address bridge-domain 20
```

18.1.85 unknown-unicast-suppression (BD view)

Function

The **unknown-unicast-suppression** command enables unknown unicast traffic suppression in a BD.

The **undo unknown-unicast-suppression** command disables unknown unicast traffic suppression in a BD.

By default, unknown unicast traffic suppression is disabled in a BD.

Format

unknown-unicast-suppression cir *cir-value* [**cbs** *cbs-value*]

undo unknown-unicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 0 to 10000000, in kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. If the **cbs** is not set, the default *cbs-value* is 125 times the *cir-value*.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

When a large number of unknown unicast packets are transmitted on the network, a lot of network resources are occupied, and services on the network are affected. You can run the **unknown-unicast-suppression** command to enable unknown unicast traffic suppression in a BD and configure the maximum number of unknown unicast packets that can pass through a BD. When the unknown unicast traffic volume exceeds the specified threshold, the system discards excess unknown unicast packets.

Example

Set the CIR value for unknown unicast traffic in BD 10 to 100 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] unknown-unicast-suppression cir 100
```

18.1.86 vni head-end peer-list

Function

The **vni head-end peer-list** command configures an ingress replication list that contains the IP addresses of those remote VTEPs for a VXLAN network identifier (VNI).

The **undo vni head-end peer-list** command deletes the ingress replication list of a VNI.

By default, no ingress replication list is configured for any VNI.

Format

vni *vni-id* **head-end peer-list** *ip-address* &<1-10>

undo vni *vni-id* [**head-end peer-list** *ip-address* &<1-10>]

vni *vni-id* **head-end peer-list** *ipv6-address* &<1-10>

undo vni *vni-id* [**head-end peer-list** *ipv6-address* &<1-10>]

vni *vni-id* **head-end peer-list protocol bgp**

undo vni *vni-id* **head-end peer-list protocol bgp**

NOTE

Only the S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, S5731-H, and S6730-S support the **head-end peer-list** parameter configured as IPv6 address.

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.
ip-address	Specifies the IPv4 address of a remote VTEP.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a remote VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
protocol bgp	Specifies BGP for establishing Layer 2 VXLAN tunnels.	-

Views

NVE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the ingress of a VXLAN tunnel receives broadcast, unknown unicast, and multicast (BUM) packets, it replicates these packets and sends a copy to each VTEP in the ingress replication list. The ingress replication list is a collection of remote VTEP IP addresses to which the ingress of a VXLAN tunnel should send replicated BUM packets.

If a source VTEP on a VXLAN connects to multiple remote VTEPs on the same VXLAN segment, run the **vni head-end peer-list** command to configure an ingress replication list that contains the IP addresses of those remote VTEPs. After the source NVE receives BUM packets, the local VTEP sends a copy of the BUM packets to every VTEP in the list.

If an underlay network is an IPv6 network, run the **vni head-end peer-list** *ipv6-address* &<1-10> command to configure an ingress replication list that contains IPv6 addresses of remote VTEPs, which is used to forward BUM traffic.

To use BGP to dynamically establish Layer 2 VXLAN tunnels, run the **vni** *vni-id* **head-end peer-list protocol bgp** command.

Precautions

- You need to run the **vni head-end peer-list** command to configure the corresponding VTEP address even if the source VTEP matches only one destination VTEP.
- Run the **ping** command to check whether a reachable route exists between two ends of the tunnel. If there is a reachable route, the tunnel can be established and packets can be normally forwarded. If the two devices have a route to each other but the route is unreachable, the tunnel can still go Up but packets cannot be forwarded.
- Currently, the device can forward BUM packets only through ingress replication. To establish a VXLAN tunnel between the device and a non-Huawei device, ensure that ingress replication is also configured on the non-Huawei device. Otherwise, the VXLAN tunnel cannot be established.

Example

Configure an ingress replication list for VNI 10, with the remote VTEPs' IP addresses being 10.1.1.1 and 10.1.1.3.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] vxlan vni 10
[HUAWEI-bd10] quit
[HUAWEI] interface nve 1
[HUAWEI-Nve1] vni 10 head-end peer-list 10.1.1.1 10.1.1.3
```

18.1.87 vpn-target (EVPN instance view)

Function

The **vpn-target** command configures the export or import VPN target extended community attribute for an EVPN instance address family.

The **undo vpn-target** command deletes the VPN target extended community attribute for the EVPN instance address family.

By default, no export or import VPN target extended community attribute list is configured for the EVPN instance address family.

Format

vpn-target *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

Parameters

Parameter	Description	Value
vpn-target	Adds a VPN target to the VPN target extended community attribute list of the EVPN instance address family. The forms of VPN targets are as follows: - 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535, and the user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. - IPv4 address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535. - Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. The AS number ranges from 65536 to 4294967295, and the user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. - 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. The 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535, and the user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0.0.	-
both	Adds a VPN target to the import or export VPN target extended community attribute list of the EVPN instance address family. If keywords **both**, **export-extcommunity**, and **import-extcommunity** are not specified, **both** is used by default.	-
export-extcommunity	Adds a VPN target to the export VPN target extended community attribute list of the EVPN instance address family.	-
import-extcommunity	Adds a VPN target to the import VPN target extended community attribute list of the EVPN instance address family.	-
all	Deletes all the VPN targets of the EVPN instance address family.	-

Views

EVPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a local device advertises EVPN routes to other devices, the EVPN routes carry all VPN target attributes in the export VPN target attribute list of the local EVPN instance. Only when the VPN target attribute carried in an EVPN route is included in the import VPN target attribute list, the route can be added to the EVPN instance routing table.

NOTE

You can run the **vpn-target** command to add VPN targets to the VPN target extended community attribute list of an EVPN instance through more than one time. A maximum of eight VPN targets can be added at one time. To configure more VPN targets for an EVPN instance, you can run the **vpn-target** command multiple times.

Prerequisites

The RD of the EVPN instance has been configured by running the **route-distinguisher** command.

Precautions

If this command is not run, all received EVPN routes cannot be added to the local EVPN instance routing table.

If all the VPN targets of an EVPN instance are deleted using the **undo vpn-target** command, all routes learned by the EVPN instance are deleted.

Example

Add 3:3 to the export VPN target extended community attribute list and 4:4 to the import VPN target extended community attribute list of EVPN instance **evn3**.

```
<HUAWEI> system-view
[HUAWEI] evpn vpn-instance evn3 bd-mode
[HUAWEI-evpn-instance-evn3] route-distinguisher 100:1
[HUAWEI-evpn-instance-evn3] vpn-target 3:3 export-extcommunity
[HUAWEI-evpn-instance-evn3] vpn-target 4:4 import-extcommunity
```

18.1.88 vpn-target evpn

Function

The **vpn-target evpn** command configures the export or import VPN target extended community attribute when a VPN instance address family advertises routes to an EVPN instance.

The **undo vpn-target** command deletes the VPN target extended community attribute from a VPN instance address family.

By default, no export or import VPN target extended community attribute list is configured for a VPN instance address family.

Format

vpn-target *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] **evpn**

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] [**evpn**] }

Parameters

Parameter	Description	Value
vpn-target	Adds a VPN target to the VPN target extended community attribute list of the VPN instance address family. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535, and the user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● IPv4 address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number: 2-byte user-defined number, for example, 65537:3. The AS number ranges from 65536 to 4294967295, and the user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation: 2-byte user-defined number, for example, 0.0:3 or 0.1:0. The 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 0 to 65535, and the user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0.0.	-
both	Adds a VPN target to the import or export VPN target extended community attribute list of the VPN instance address family. If keywords **both**, **export-extcommunity**,and **import-extcommunity**are not specified, **both** is used.	-
export-extcommunity	Adds a VPN target to the export VPN target extended community attribute list of the VPN instance address family.	-

Parameter	Description	Value
import-extcommunity	Adds a VPN target to the import VPN target extended community attribute list of the VPN instance address family.	-
all	Deletes all the VPN targets of the VPN instance address family.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure a VPN instance on a device, you must run the **vpn-target evpn** command to configure a VPN target attribute of EVPN routes for the address family of the VPN instance.

The VPN target controls route learning of EVPN routes. A VPN target attribute is either an import one or an export one. An export VPN target is carried in a EVPN route to be advertised to a remote MP-BGP peer. When receiving a EVPN route, a peer compares the received VPN target attribute with the import VPN target attribute to determine whether the EVPN route can be added to the routing table of the local VPN instance address family.

In the VXLAN deployed through BGP EVPN scenario, to add EVPN routes to the routing table of an VPN instance, run the **vpn-target** command to configure the corresponding VPN target.

Prerequisites

The **route-distinguisher** command have been run to configure the VPN instance RD.

Precautions

A VPN target configured using the **vpn-target evpn** command will not overwrite any previously configured VPN target. If the number of configured VPN targets has reached the maximum limit, no VPN target can be added by running the **vpn-target evpn** command.

After a VPN target is configured for the address family of a VPN instance, only the routes that match the VPN target are accepted by the address family of the VPN instance.

If all the VPN targets of the address family of a VPN instance are deleted using the **undo vpn-target evpn** command, all EVPN routes learned by the address family of the VPN instance from other VPN instances are deleted.

Multiple VPN targets can be configured for the address family of a VPN instance. The **vpn-target evpn** command can configure a maximum of eight VPN targets at a time. To configure more VPN targets in the VPN instance view, run the **vpn-target evpn** command multiple times. When EVPN routes are advertised between VPN instances, if one of the VPN targets carried in the EVPN routes matches the import VPN target of the address family of a local VPN instance, the routes are added to the routing table of the local VPN instance.

Example

Add 3:3 to the export VPN target EVPN list and 4:4 to the import VPN target evpn list of VPN instance **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] ipv4-family
[HUAWEI-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity evpn
[HUAWEI-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity evpn
```

18.1.89 vxlan fragment-reassemble enable

Function

The **vxlan fragment-reassemble enable** command enables the function of reassembling fragmented VXLAN packets.

The **undo vxlan fragment-reassemble enable** command disables the function of reassembling fragmented VXLAN packets.

By default, the function of reassembling fragmented VXLAN packets is disabled.

NOTE

Only the S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, and S5731-H support this command.

Format

vxlan fragment-reassemble enable

undo vxlan fragment-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switch receives fragmented VXLAN packets in a VXLAN scenario, it does not reassemble the fragmented packets by default. To reassemble fragmented VXLAN packets, run the **vxlan fragment-reassemble enable** command to enable the function of reassembling fragmented VXLAN packets.

If the function of reassembling fragmented VXLAN packets is disabled on a switch, the switch generates the ADPVXLAN_1.3.6.1.4.1.2011.5.25.227.2.1.40 hwNotsuppDecapVxlanFragPackets alarm when receiving fragmented VXLAN packets.

Precautions

- Enabling the function of reassembling fragmented VXLAN packets may affect processing of other IP packets. Therefore, exercise caution when using this command.
- If the system software of a switch is upgraded from V200R011C10 to V200R012C00 or a later version and the **interface nve** and **vxlan vni (BD view)** commands are configured on the switch before the upgrade, the function of reassembling fragmented VXLAN packets is enabled after the upgrade. If the **interface nve** and **vxlan vni (BD view)** commands are not configured on the switch before the upgrade, the function of reassembling fragmented VXLAN packets is disabled after the upgrade.

Example

Enable the function of reassembling fragmented VXLAN packets.

```
<HUAWEI> system-view
[HUAWEI] vxlan fragment-reassemble enable
```

18.1.90 vxlan regularly-refresh

Function

The **vxlan regularly-refresh** command sets the interval at which VXLAN-related entries are updated periodically, the interval between two rounds of updates, and the number of entries updated in each round.

The **undo vxlan regularly-refresh** command restores the default configuration.

By default, the interval at which VXLAN-related entries are updated periodically is 1 minute, the interval between two rounds of updates is 1 second, and the number of entries updated in each round is 50.

Format

vxlan regularly-refresh { **interval** *interval* | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* }

undo vxlan regularly-refresh { **interval** | **entry-number** | **cycle-interval** }

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval between two rounds of VXLAN-related entry updates.	The value is an integer in the range from 1 to 300, in seconds.
entry-number *entry-number*	Specifies the number of VXLAN-related entries updated in each round.	The value is an integer in the range from 1 to 100.
cycle-interval *cycle-interval*	Specifies the interval at which VXLAN-related entries are updated periodically.	The value is an integer in the range from 1 to 1440, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports periodic update of VXLAN-related entries to ensure the real-timeliness and validity of the underlying forwarding data. Periodic update of VXLAN-related entries consumes system resources, including CPU and memory resources. A longer update interval and a smaller number of updated entries have less impact on other services in the system. You can flexibly configure the interval at which VXLAN-related entries are updated periodically and the number of updated entries based on system resource usage.

Prerequisites

Before running this command, ensure that periodic update of VXLAN-related entries has been enabled. By default, this function is enabled. If this function is disabled, run the **undo vxlan regularly-refresh disable** command in the system view to enable it.

Example

Set the interval between two rounds of VXLAN-related entry updates to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] vxlan regularly-refresh interval 5
```

18.1.91 vxlan regularly-refresh disable

Function

The **vxlan regularly-refresh disable** command disables periodic update of VXLAN-related entries.

The **undo vxlan regularly-refresh disable** command enables periodic update of VXLAN-related entries.

By default, periodic update of VXLAN-related entries is enabled.

Format

vxlan regularly-refresh disable

undo vxlan regularly-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device updates VXLAN-related entries for the first time 30 minutes after it is powered on, and the update is performed periodically at an interval of 1 minute to ensure the correctness of underlying data. Periodic update of VXLAN-related entries consumes system resources. If the CPU usage is high in a short period of time due to periodic update of VXLAN-related entries and the processing of normal services is affected, you can run the **vxlan regularly-refresh** { **interval** *interval* | **entry-number** *entry-number* | **cycle-interval** *cycle-interval* } command to prolong the periodic update interval and the interval between two rounds of updates, and reduce the number of entries updated in each round to reduce system resource consumption. If the CPU usage remains high, run the **vxlan regularly-refresh disable** command to immediately disable periodic update of VXLAN-related entries.

Precautions

Disabling periodic update of VXLAN-related entries may cause a failure to rectify certain hardware faults in a timely manner. Exercise caution when running the **vxlan regularly-refresh disable** command.

Example

Enables periodic update of VXLAN-related entries.

```
<HUAWEI> system-view
[HUAWEI] undo vxlan regularly-refresh disable
```

18.1.92 vxlan statistics enable

Function

The **vxlan statistics enable** command enables statistics collection on VXLAN tunnel packets.

The **undo vxlan statistics enable** command disables statistics collection on VXLAN tunnel packets.

By default, statistics collection on VXLAN tunnel packets is disabled.

Format

vxlan statistics peer *peer-ip-address* [**vni** *vni-id*] **enable**

undo vxlan statistics peer *peer-ip-address* [**vni** *vni-id*] **enable**

vxlan statistics peer *peer-ipv6-address* [**vni** *vni-id*] **enable**

undo vxlan statistics peer *peer-ipv6-address* [**vni** *vni-id*] **enable**

NOTE

Only the S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S6730-H, S6730S-H, S5731-H, and S6730-S support the **source** and **peer** parameters configured as IPv6 address.

Parameters

Parameter	Description	Value
peer *peer-ip-address*	Specifies the IPv4 address of the destination VTEP.	The value is in dotted decimal notation.
peer *peer-ipv6-address*	Specifies the IPv6 address of the destination VTEP.	The address is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vni *vni-id*	Specifies a VNI ID. If **vni** *vni-id* is specified, the device collects packet statistics based on the VXLAN tunnel and VNI. If **vni** *vni-id* is not specified, the device collects packet statistics based on the VXLAN tunnel only.	The value is an integer that ranges from 1 to 16777215.

Views

NVE interface view

Default Level

2: Configuration level

Usage Guidelines

VXLAN tunnel packet statistics provide information about the number of packets going into and leaving a VXLAN tunnel.

To view VXLAN tunnel packet statistics, run the **vxlan statistics enable** and **display vxlan statistics** commands in sequence.

Packet statistics collection based on the VXLAN tunnel and VNI and packet statistics collection based on the VXLAN tunnel are mutually exclusive. For example, if the **vxlan statistics peer 10.1.1.1 vni 10 enable** command is configured, do not configure the **vxlan statistics peer 10.1.1.1 enable** command. If the **vxlan statistics peer 10.1.1.1 enable** command is configured, do not configure the **vxlan statistics peer 10.1.1.1 vni 10 enable** command.

Example

Enable statistics collection on VXLAN tunnel packets with 10.1.1.1 as the destination VTEP IP address.

```
<HUAWEI> system-view
[HUAWEI] interface nve 1
[HUAWEI-Nve1] vxlan statistics peer 10.1.1.1 enable
```

18.1.93 vxlan tunnel-status track exact-route

Function

The **vxlan tunnel-status track exact-route** command enables subscription to the status of the exact route to a VXLAN tunnel destination.

The **undo vxlan tunnel-status track exact-route** command disables subscription to the status of the exact route to a VXLAN tunnel destination.

By default, subscription to the status of the exact route to a VXLAN tunnel destination is disabled.

Format

vxlan tunnel-status track exact-route

undo vxlan tunnel-status track exact-route

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, a VXLAN tunnel is considered Up if its source IP address and the network segment where its destination IP address resides are reachable. In the real-world situation, when multiple destination IP addresses share the same network segment, this network segment is reachable if only one such destination IP address is reachable. As such, a VXLAN tunnel may be incorrectly considered Up even if its destination IP address is unreachable. Network problems then cannot be immediately identified. To resolve this problem, run the **vxlan tunnel-status track exact-route** command to enable subscription to the status of the exact route to a VXLAN tunnel destination. The VXLAN tunnel is then reported Up only when the exact route to the VTEP destination IP address is reachable.

NOTE

The VXLAN tunnel status can be checked by running the **display vxlan tunnel** command.

Example

Enable subscription to the status of the exact route to a VXLAN tunnel destination.

```
<HUAWEI> system-view
[HUAWEI] vxlan tunnel-status track exact-route
```

18.1.94 vxlan vni (BD view)

Function

The **vxlan vni** command associated a specified VNI with a BD.

The **undo vxlan vni** command restores the default settings.

By default, no VNI is associated with a BD.

Format

vxlan vni *vni-id*

undo vxlan vni *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Similar to VLAN ID, VNI is used to distinguish VXLAN segments.

On the VXLAN network, one VXLAN segment is a large Layer 2 BD; therefore, VNI and BD have a one-to-one mapping relationship.

You can run this command to configure the mapping relationship between VNIs and BDs. In this way, the VTEP can forward received packets through a correct VXLAN tunnel based on the mapping between BDs and VNIs.

Example

Set the mapping between VNI 10 and BD 10.

```
<HUAWEI> system-view
[HUAWEI] bridge-domain 10
[HUAWEI-bd10] vxlan vni 10
```

18.1.95 vxlan vni (VPN instance view)

Function

The **vxlan vni** command configures the VXLAN VNI corresponding to a VPN instance.

The **undo vxlan vni** command restores the default settings.

By default, no VNI is configured for a VPN instance.

Format

vxlan vni *vni-id*

undo vxlan vni *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To isolate tenants at Layer 3, VPN is generally used. In a distributed VXLAN gateway scenario, to implement Layer 3 communication through a Layer 3 gateway, the Layer 3 gateway must be bound to a VPN instance.

The Layer 3 gateway assigns a VNI to each subnet and a Layer 3 VNI to each tenant identified by a VPN instance. To bind a VNI to a VPN instance, run the **vxlan vni** command. During Layer 3 communication through the Layer 3 gateway, the VNI ID bound to the VPN instance is transmitted to the remote Layer 3 gateway through the VXLAN tunnel. The remote Layer 3 gateway identifies VPNs based on tenants' VNI IDs to determine whether tenants belong to the same VPN for communication or isolation purposes.

Precautions

- A VNI can be bound only to one VPN instance.
- The VNI bound to a VPN instance cannot be bound to a BD.

Example

Configure the ID of the VNI corresponding to VPN instance **vpn1** as **10**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] vxlan vni 10
```

19 Upgrade-compatible Commands Reference

This chapter describes upgrade-compatible commands of each feature of all fixed switches. Upgrade-compatible commands are supported in earlier versions, but are deleted in the new version or have the command format changed. They exist to prevent configuration loss or impact on other configurations after the upgrade.

Due to version evolution, there may be changes on upgrade-compatible commands supported by some products. This chapter does not describe the differences.

Upgrade-compatible commands are classified into two types based on user operations:

- You can write these commands to the configuration file but cannot run them in the CLI after the device restarts.
- You can run these commands by entering commands in their complete format.

NOTE

You are not advised to use upgrade-compatible commands to perform operations on the device. If required, perform operations under the guidance of technical support personnel.

19.1 Basic Configuration Compatible Commands

19.1.1 set authentication password simple (upgrade-compatible command)

Function

The **set authentication password simple** command sets the simple format for a local authentication password.

Format

set authentication password simple *password*

Parameters

Parameter	Description	Value
password	Specifies a password.	The value is a string of 1 to 16 characters. The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Special character except the question mark (?) and space.

Views

User view

Default Level

3: Management level

Task Name and Operations

Task Name	Operations
telnet-server	write

Usage Guidelines

It is replaced by the **set authentication password** command.

This command is saved in simple text after it is configured, which brings security risks. Saving the command configuration in ciphertext is recommended.

19.1.2 certificate load (upgrade-compatible command)

Function

The **certificate load** command loads a digital certificate in the Secure Sockets Layer (SSL) policy view.

The **undo certificate load** command unloads a digital certificate for the SSL policy.

By default, no digital certificate is loaded for the SSL policy.

Format

Load a PEM digital certificate for the SSL policy.

certificate load pem-cert *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*

Load a PFX digital certificate for the SSL policy.

certificate load pfx-cert *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac** *mac-code* | **key-file** *key-filename* } **auth-code** *auth-code*

Load a PEM certificate chain for the SSL policy.

certificate load pem-chain *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*

Parameters

Parameter	Description	Value
pem-cert	Loads a PEM digital certificate for the SSL policy. A PEM digital certificate has a file name extension .pem. A PEM digital certificate transfers text data between systems.	-

Parameter	Description	Value
cert-filename	Specifies the name of a certificate file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
key-pair	Specifies the key pair type.	-
dsa	Sets the key pair type to DSA.	-
rsa	Sets the key pair type to RSA.	-
key-file *key-filename*	Specifies the key pair file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code *auth-code*	Specifies the authentication code of the key pair file. The authentication code verifies user identity to ensure that only authorized clients access the server.	When the authentication code is in plain text, the value is a string of 1 to 31 case-sensitive characters without any space.
pfx-cert	Loads a PFX digital certificate for the SSL policy. A PFX digital certificate has a file name extension .pfx. A digital certificate can be converted from the PFX format to another format.	-
mac *mac-code*	Specifies a message authentication code. The message authentication code ensures the packet data reliability and security.	When the authentication code is in plain text, the value is a string of 1 to 31 case-sensitive characters without any space.
pem-chain	Specifies a PEM certificate chain.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SSL security mechanism includes:

- Data transmission security: Uses the symmetric key algorithm to encrypt data.
- Message integrity: uses the multiplexed analog component (MAC) algorithm to ensure message integrity.
- Identity authentication mechanism: authenticates users based on the digital signatures and certificates.

The Certificate Authority (CA) issues PEM, ASN1, and PFX digital certificates that provide user identity information. Based on digital certificates, users establish trust relationships with partners who require high security.

A digital certificate data includes the applicant information such as the applicant's name, applicant's public key, digital signature of the CA that issues the certificate, and the certificate validity period. A certificate chain can be released when a certificate is sent so that the receiver can have all certificates in the certificate chain.

Prerequisites

Before running the **certificate load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

- You can load a certificate or certificate chain for only one SSL policy. Before loading a certificate or certificate chain, you must unload the existing certificate or certificate chain.
- When you configure an SSL policy to load a certificate or certificate chain, ensure that the maximum length of the key pair in the certificate or certificate chain is 2048 bits. If the length of the key pair exceeds 2048 bits, the certificate file or certificate chain file cannot be uploaded to the device.

Example

Load a PEM digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] certificate load pem-cert servercert.pem key-pair dsa key-file
serverkey.pem auth-code YsHsjx_202206
```

Load a PFX digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pfx-cert servercert.pfx key-pair dsa key-file
serverkey.pfx auth-code %$%$"DlqKik*GE*~`u4H+LFJ(K-=%$%$
```

Load a PEM certificate chain for the SSL policy.

```
<HUAWEI> system-view
```

```
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pem-chain chain-servercert.pem key-pair dsa key-file chain-servercertkey.pem auth-code YsHsjx_202206
```

19.1.3 set device usb-deployment password (upgrade-compatible command)

Function

The **set device usb-deployment password** command sets an authentication password for USB-based deployment.

Format

set device usb-deployment password *password*

Parameters

Parameter	Description	Value
password	Specifies the authentication password for USB-based deployment.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

A user with a level lower than the management level cannot query the password configured using this command. If this user query the configuration file, the password is displayed as asterisks (******).

19.1.4 set save-configuration backup-to-server server (upgrade-compatible command)

Function

The **set save-configuration backup-to-server server** command specifies the server where the system periodically saves the configuration file.

The **undo set save-configuration backup-to-server server** command cancels the server where the system periodically saves the configuration file.

By default, the system does not periodically save configurations to the server.

Format

set save-configuration backup-to-server server *server-ip* [**transport-type** { **ftp** | **sftp** }] **path** *path* **user** *user-name* **password** *password*

set save-configuration backup-to-server server *server-ip* **user** *user-name* **password** *password* [**path** *path*]

undo set save-configuration backup-to-server server [*server-ip*]

Parameters

Parameter	Description	Value
server *server-ip*	Specifies the IP address of the server where the system periodically saves the configuration file.	-
transport-type	Specifies the mode in which the configuration file is transmitted to the server.	The value can be **ftp** or **sftp**.
user *user-name*	Specifies the name of the user who saves the configuration file on the server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password *password*	Specifies the password of the user who saves the configuration file on the server.	The value is a string of 1 to 16 or 32 case-sensitive characters without spaces.
path *path*	Specifies the relative save path on the server.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to periodically save the configuration file to the server.

Precautions

If the mode in which the configuration file is transmitted to the server is not specified, FTP is used.

If the specified path on the server does not exist, configuration files cannot be sent to the server. The system then sends an alarm message indicating the transmission failure to the NMS, and the transmission failure is recorded as a log message on the device.

The user name and password must be the same as those used in FTP or SFTP login mode.

Example

Specify the server to which the system periodically sends the configuration file, and set the transmission mode to FTP.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration backup-to-server server 10.1.1.1 transport-type ftp path d:/ftp user
huawei password huawei@1234
```

19.1.5 set save-configuration (upgrade-compatible command)

Function

Using the **set save-configuration** command, you can enable automatic saving of configurations.

Using the **undo set save-configuration** command, you can disable automatic saving of configurations.

By default, automatic saving of configurations is not enabled.

Format

set save-configuration nochange-time *nochange-time*

undo set save-configuration nochange-time [*nochange-time*]

Parameters

Parameter	Description	Value
nochange-time *nochange-time*	Specifies a period and configures the system to automatically save configurations if no configurations are changed over the specified period.	The value is an integer ranging from 30 to 43200, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

If **nochange-time** *nochange-time* is specified in the command, the system automatically saves configurations if no configuration changes in the period specified by *nochange-time*.

If the interval from the time of the last configuration to the current time is shorter than the set interval, the system cancels the current automatic saving operation.

Example

Configure the system to automatically save configurations at 60-minute intervals if no configuration changes in the period.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration nochange-time 60
```

19.1.6 smart-upgrade information (upgrade-compatible command)

Function

The **smart-upgrade information** command sets the contact phone number and email address for smart upgrade.

The **undo smart-upgrade information** command deletes the configured contact number and email address for smart upgrade.

By default, no contact phone number or email address is configured for smart upgrade.

Format

smart-upgrade information telephone *phonevalue* **email** *emailvalue*

undo smart-upgrade information telephone

Parameters

Parameter	Description	Value
phonevalue	Specifies a mobile phone number.	The value is a string of 1 to 21 characters. The value can contain the plus sign (+) and digits (0 to 9), and cannot contain spaces. The plus sign (+) can be used only at the beginning of a character string. If a character string starts with a plus sign (+), the maximum string length is 21. If a character string starts with a digit, the maximum string length is 20.

Parameter	Description	Value
emailvalue	Specifies the email address.	The value is a string of 1 to 128 case-sensitive characters. The following characters are supported: letters, digits, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), and underscore (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

If smart upgrade fails on a switch, the switch can notify the user of the upgrade result based on the contact phone number and email address provided by the user.

NOTE

The contact information is used only for emergency contact upon an upgrade failure.

Example

Set the contact phone number and email address for smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade information telephone 111111111 email abcd@huawei.com
Privacy Policy

Your privacy is important to us.
When enabling the automatic upgrade function for Huawei devices, you may, at your discretion,
provide your personal information such as the telephone number, mobile number, and email address on the
Command Line Interface (CLI).
This information will be used to notify you immediately of the upgrade result after the automatic upgrade
function is enabled.
By agreeing to these terms and conditions, you are authorizing Huawei to collect and process the
aforementioned personal information provided by you for the stated purpose.
Your information may be transferred to a third party of Huawei or affiliated company of Huawei for the
purpose of providing the aforementioned service for you.
The information you provide will be stored on the servers of Huawei and its affiliates.
The information may be transmitted outside your country or region and accessed, stored, and processed in
another country or region, including China.
Huawei is committed to protecting your personal information and preventing the information from being
used without authorization.
For more details, please refer to the full privacy policy at https://www.huawei.com/en/privacy-policy.

Do you agree to these terms and conditions? [Y/N]:y
Info: Set the phone and email successfully.
```

19.1.7 snmp-agent trap enable configuration (upgrade-compatible command)

Function

The **snmp-agent trap enable configuration** command enables the trap function of the Configuration module.

By default, the trap function of the Configuration module is disabled.

Format

snmp-agent trap enable configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name configuration** command.

19.1.8 snmp-agent trap enable ssh (upgrade-compatible command)

Function

The **snmp-agent trap enable ssh** command enables the trap function of the SSH module.

By default, the alarm function of the SSH module is disabled.

Format

snmp-agent trap enable ssh

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.1.9 snmp-agent trap enable system (upgrade-compatible command)

Function

The **snmp-agent trap enable system** command enables the trap function of the system module.

By default, the trap function of the system module is enabled.

Format

snmp-agent trap enable system

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name system** command.

19.1.10 snmp-agent trap enable flash (upgrade-compatible command)

Function

The **snmp-agent trap enable flash** command enables the trap function of the flash module.

By default, the trap function of the flash module is disabled.

Format

snmp-agent trap enable flash

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name vfs** { **hwflhopernotification** | **hwflhsyncfailnotification** | **hwflhsyncsuccessnotification** } command.

19.1.11 super password (upgrade-compatible command)

Function

The **super password** command sets the password used to change a user from a lower level to a higher level.

By default, the system does not set the password used to change a user from a lower level to a higher level.

Format

super password [**level** *user-level*] **simple** *simple-password*

Parameters

Parameter	Description	Value
level *user-level*	Specifies a user level.	The value is an integer that ranges from 1 to 15. By default, the system sets passwords for users of level 3.
simple *simple-password*	Specifies the simple password for changing a user level.	The value is a string of 1 to 16 case-sensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device makes it possible to switch a user from a lower level to a higher level. To prevent illegal intrusion of unauthorized users, when a user switches to a higher user level, the system authenticates the user identity by requiring the user to input the password for the higher user level.

- If the **cipher** *cipher-password* parameter is not specified, the system starts the interactive password setting mode. Enter a plain text password of 6 to 16 characters. The requirements for the password are the same as the requirements for the plain text password configured when the **cipher** keyword is specified. The password you enter will not be displayed on the device. You can press **CTRL_C** to cancel the password setting.
- The password is in plain or cipher text and displayed on the device when the **cipher** *cipher-password* parameter is specified. When you run the **super** command to switch the user level, the password must be entered in plain text.
- Whether the password is entered in **cipher** or interactive mode, the password is saved in cipher text to the configuration file. Therefore, the password cannot be obtained from the system after it is set. Keep the password secure.
- This command is saved in simple text after it is configured, which brings security risks. Saving the command configuration in ciphertext is recommended.

Example

Set the password used when low-level users switch to level 10 to YsHsjx_202206.

```
<HUAWEI> system-view
[HUAWEI] super password level 10 simple YsHsjx_202206
```

19.1.12 trusted-ca load (upgrade-compatible command)

Function

The **trusted-ca load** command loads the trusted CA file for the SSL policy for the FTP client.

By default, no trusted CA file is loaded for the SSL policy.

Format

Load the trusted CA file for the SSL policy in PFX format.

trusted-ca load pfx-ca *ca-filename* **auth-code** { *auth-code* | **cipher** *auth-code* }

Parameters

Parameter	Description	Value
pfx-ca	Load the trusted CA file for the SSL policy in PFX format.	-
ca-filename	Specifies the name of the trusted CA file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code *auth-code*	Specifies the verification code for the trusted CA file in PFX format. The authentication code verifies user identity to ensure that only authorized users can log in to the server.	When the authentication code is in plain text, the value is a string of 1 to 31 case-sensitive characters without any space.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

CAs that are widely trusted in the world are called root CAs. Root CAs can authorize other lower-level CAs. The identity information about a CA is provided in the file of a trusted CA. To ensure the communication security and verify the server validity, you must run the **trusted-ca load** command to load the trusted CA file.

Prerequisites

Before running the **trusted-ca load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

A maximum of four trusted CA files can be loaded for an SSL policy.

Example

Load the trusted CA file for the SSL policy in PFX format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load pfx-ca servercert.pfx auth-code cipher 123456
```

19.2 Device Management Compatible Commands

19.2.1 cpu-usage threshold (upgrade-compatible command)

Function

The **cpu-usage threshold** command sets the upper and lower CPU usage alarm thresholds.

Format

cpu-usage threshold [**unit** *unit-id*] { **high** | **low** } *threshold-value*

Parameters

Parameter	Description	Value
high	Specifies the upper CPU usage alarm threshold.	-
low	Specifies the lower CPU usage alarm threshold.	-
unit *unit-id*	• Specifies the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured.	The value range depends on the device configuration.

Parameter	Description	Value
threshold-value	Specifies the alarm threshold of CPU usage.	- The value is an integer that ranges from 2 to 100 when specifies the upper CPU usage alarm threshold. - The value is an integer that ranges from 1 to 99 when specifies the lower CPU usage alarm threshold.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the CPU usage is not within the allowed range, a log is recorded. You can conveniently know CPU usage through log information.

19.2.2 display autosave config (upgrade-compatible command)

Function

The **display autosave config** command displays the configuration about the autosave function, including the status of the autosave function, time for autosave check, threshold of the CPU usage, and interval during which configurations are not changed.

Format

display autosave config

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the autosave function is configured, you can run the **display autosave config** command to check whether the configured parameters are correct. You can also run this command to check whether the parameters about the autosave function are properly configured when autosave cannot function normally. If not, run the **set save-configuration** command to adjust the parameters to restore the normal state of the autosave function.

Example

Display the configuration about the autosave function.

```
<HUAWEI> display autosave config
Auto save function status: enable
Auto save checking interval: 60 minutes
The threshold of the CPU usage: 50%
The interval of the configuration not changing: 30 minutes
```

Table 19-1 Description of the display autosave config command output

Item	Description
Auto save function status	Indicates the status of the autosave function: ● Enable ● Disable
Auto save checking interval	Indicates the time for autosave check.
The threshold of the CPU usage	Indicates the threshold of the CPU usage during the autosave operation.
The interval of the configuration not changing	Indicates the interval during which system configurations are not changed.

19.2.3 display fault-management (upgrade-compatible command)

Function

The **display fault-management** command displays the contents of an alarm message, active alarm message, or event.

Format

display fault-management { **alarm** | **active-alarm** | **event** } [**sequence-number** *sequence-number*]

Parameters

Parameter	Description	Value
alarm	Displays information about alarms.	-
active-alarm	Displays information about active alarms.	-
event	Displays information about events.	-
sequence-number *sequence-number*	Specifies the number of an alarm message, active alarm message, or event.	The value is an integer ranging from 0 to 2147483647. When the value is 0, information about all alarm messages, active messages, or events is displayed.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command helps you obtain the contents of all alarm messages or one alarm message on a device.

Example

Display the contents of active alarm messages in the system.

```
<HUAWEI> display fault-management active-alarm
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2008-10-13 01:49:45+08:00/-/0x41932001/hwLldpEnabled/Warning/Sta
rt/OID: 1.3.6.1.4.1.2011.5.25.134.2.1 Global LLDP is enabled.
  2/Independent/2008-10-13 01:50:06+08:00/-/0x41932000/lldpRemTablesChange/Warni
ng/Start/OID: 1.0.8802.1.1.2.0.0.1 Neighbor information is changed. (LldpStatsRe
mTablesInserts=1, LldpStatsRemTablesDeletes=0, LldpStatsRemTablesDrops=0, LldpSt
atsRemTablesAgeouts=0)
  5/Independent/2008-10-13 02:22:52+08:00/-/0x40c12014/hwPortPhysicalEthHalfDupl
exAlarm/Minor/Start/OID 1.3.6.1.4.1.2011.5.25.129.2.5.11 The port works in half
duplex mode. (EntityPhysicalIndex=10, BaseTrapSeverity=3, BaseTrapProbableCause=
1024, BaseTrapEventType=8, EntPhysicalName=GigabitEthernet0/0/5, RelativeResourc
e=interface GigabitEthernet0/0/5)
```

19.2.4 display fault-management alarm information (upgrade-compatible command)

Function

The **display fault-management alarm information** command displays registration information about an alarm message.

Format

display fault-management alarm information [*alarm-name*]

Parameters

Parameter	Description	Value
alarm-name	Specifies the name of an alarm message.	The value is a case-sensitive string of 1 to 256 characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Check registration information about the alarm message named linkUp.

```
<HUAWEI> display fault-management alarm information linkUp
*********************************
  AlarmName: linkUp
  AlarmType: Resume Alarm
  AlarmLevel: Cleared
  Suppress Period: NA
  CauseAlarmName: linkDown
  Match VB Name: ifIndex
*********************************
```

Table 19-2 Description of the display fault-management alarm information command output

Item	Description
AlarmName	Name of an alarm message
AlarmType	Type of an alarm

Item	Description
AlarmLevel	Level of an alarm
Suppress Period	Suppress period of an alarm
CauseAlarmName	Name of the corresponding root alarm
Match VB Name	Contents of the matching rule set for the alarm messages

19.2.5 dual-active detect mode direct (upgrade-compatible command)

Function

The **dual-active detect mode direct** command enables DAD in direct mode on a specified interface.

By default, DAD is disabled on an interface in a stack.

Format

dual-active detect mode direct

Parameters

None

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DAD in direct mode applies to a stack containing two DAD-supporting member switches.

Prerequisites

The stack containing two member switches is running properly, and DAD in relay mode is not configured for the stack.

Precautions

Disabling DAD in direct mode on an interface restores the forwarding function on the interface. If a loop exists on the network, a broadcast storm occurs.

The **dual-active detect mode direct** command performs the same function as the **mad detect mode direct** command.

Example

Configure DAD in direct mode on GigabitEthernet1/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dual-active detect mode direct
Warning: This command will block the port, and no other configuration running on this port is
recommended. Continue?[Y/N]:y
```

19.2.6 dual-active detect mode relay (upgrade-compatible command)

Function

The **dual-active detect mode relay** command enables DAD in relay mode on a specified interface.

By default, DAD is disabled on an interface in a stack.

Format

dual-active detect mode relay

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure DAD in relay mode only when a stack containing two member switches is configure with an inter-chassis Eth-Trunk and a proxy device supports the relay function.

Prerequisites

The stack containing two member switches is running properly, and DAD in direct mode is not configured for the stack.

Precautions

The **dual-active detect mode relay** command performs the same function as the **mad detect mode relay** command.

Example

Configure DAD in relay mode on Eth-Trunk 10.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] dual-active detect mode relay
```

19.2.7 dual-active exclude (upgrade-compatible command)

Function

The **dual-active exclude** command excludes specified interfaces of a stack from shutdown.

By default, only physical member ports are excluded from shutdown.

Format

dual-active exclude interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] }	Specifies the type and number of an interface: • *interface-type* specifies the type of the interface. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the second interface.	The value of *interface-number2* must be larger than that of *interface-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **mad exclude** command.

19.2.8 dual-active relay (upgrade-compatible command)

Function

The **dual-active relay** command enables the relay function on a specified interface of a proxy device.

By default, the relay function is disabled on an interface.

Format

dual-active relay

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

In DAD in relay mode, you need to use the **dual-active relay** command to configure the relay function on a specified Eth-Trunk interface of a proxy device. Member interfaces of the Eth-Trunk interface forward DAD packets to each other so that member switches can exchange DAD packets.

It is replaced by the **mad relay** command.

Example

Enable the relay function on Eth-Trunk 10 of a proxy device.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] dual-active relay
```

19.2.9 dual-active restore (upgrade-compatible command)

Function

The **dual-active restore** command restores the blocked interfaces of the standby switch that enters the Recovery state after its stack splits.

Format

dual-active restore

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a stack splits, if the active switch fails, you can restore the blocked interfaces of the standby switch that enters the Recovery state to make the standby switch to take over the active role.

Precautions

When the active switch is working properly, do not use this command. Otherwise, DAD detects a dual-active scenario again and blocks all service interfaces, causing interface status flapping.

It is replaced by the **mad restore** command.

Example

Restore all the blocked interfaces of the standby switch that enters the Recovery state after its stack splits.

```
<HUAWEI> system-view
[HUAWEI] dual-active restore
```

19.2.10 fault-management alarm (upgrade-compatible command)

Function

The **fault-management alarm** command configures the type or severity of an alarm message or event.

The **undo fault-management alarm** command cancels the type or severity of an alarm message or event.

Format

fault-management alarm *alarm-name* **level** *alarm-level*

undo fault-management alarm *alarm-name* [**level**]

Parameters

Parameter	Description	Value
alarm *alarm-name*	Specifies the name of an alarm message or event.	The value is a case-sensitive string of 1 to 64 characters without spaces.

Parameter	Description	Value
level *alarm-level*	Specifies the severity of an alarm message or event: 1. Critical: indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported. For example, when a managed object becomes totally out of service, its capability must be restored. 2. Major: indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported. For example, when there is a severe degradation in the capability of a managed object, its full capability must be restored. 3. Minor: indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported. For example, when the detected alarm condition is not currently degrading the capacity of the managed object. 4. Warning: indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault. 5. Indeterminate: indicates that the severity level cannot be determined. 6. Cleared: indicates the clearing of one or more previously reported alarms. This alarm clears all alarms for this managed object that have the same alarm type, possible causes and fault symptoms (if given). Multiple associated notifications may be cleared by using the Correlated notifications parameter.	The value is a character string. In the X.733 standard, according to the severity and emergency, alarm messages are classified into six levels. The more serious event an alarm message indicates, the smaller *alarm-level* is. **Critical** indicates the alarm severity 1, whereas **Cleared** indicates the alarm severity 6.

Views

System view

Default Level

3: Management level

Usage Guidelines

Alarm messages are classified into root alarm messages and resume-alarm messages. All the alarms are saved on the device.

Events are classified into critical events and events. Critical events are saved on a device and can be obtained by the NMS. Events are not saved on a device.

The **fault-management alarm** command can be used to promote or degrade the level of an alarm message according to the severity and emergency of the alarm message.

Example

Set the alarm severity of the alarm message named hwCfgManEventlog to major.

```
<HUAWEI> system-view
[HUAWEI] fault-management alarm hwCfgManEventlog level major
```

19.2.11 poe af-inrush enable (upgrade-compatible command)

Function

The **poe af-inrush enable** command changes the power supply standards of interfaces from 802.3at to 802.3af.

The **undo poe af-inrush enable** command restores the power supply standards of interfaces to 802.3at.

By default, interfaces comply with 802.3at.

Format

poe af-inrush enable [**slot** *slot-id*]

undo poe af-inrush enable [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, it is replaced by the **poe af-inrush enable** command in the interface view.

19.2.12 reset fault-management (upgrade-compatible command)

Function

The **reset fault-management** command clears all alarm messages.

Format

reset fault-management { **active-alarm** | **event** } [**sequence-number** *sequence-number*]

Parameters

Parameter	Description	Value
active-alarm	Clears information about active alarms.	-
event	Clears event information.	-
sequence-number *sequence-number*	Specifies the number of an alarm message.	The value is an integer ranging from 0 to 2147483647. If the value is 0, it indicates that all alarm messages are cleared.

Views

System view

Default Level

3: Management level

Usage Guidelines

If *sequence-number* is not specified, the system clears all the alarm messages on the device.

NOTICE

After this command is run, all alarm messages on a device are cleared and cannot be restored.

Example

Clear all active alarm messages.

```
<HUAWEI> system-view
[HUAWEI] reset fault-management active-alarm
```

19.2.13 ntp-service authentication-keyid (upgrade-compatible command)

Function

The **ntp-service authentication-keyid** command sets NTP authentication key.

The **undo ntp-service authentication-keyid** command removes NTP authentication key.

By default, no authentication key is set.

Format

ntp-service authentication-keyid *key-id* **authentication-mode** { **md5** | **hmac-sha256** } **plain** *password-plain*

undo ntp-service authentication-keyid *key-id*

Parameters

Parameter	Description	Value
key-id	Indicates the key number.	Key ID is an integer and ranges from 1 to 4294967295.
authentication-mode md5	Indicates MD5 authentication mode.	-
authentication-mode hmac-sha256	Indicates HMAC-SHA256 authentication mode.	-

Parameter	Description	Value
plain *password-plain*	Indicates that the configured password is displayed in plain text, and specifies the password. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks.	The password is a string of 1 to 255 case-sensitive characters without spaces.

Views

System view

Default Level

2: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **ntp-service authentication-keyid**.

19.3 Interface Management Compatible Commands

19.3.1 Ethernet Interface Compatible Commands

19.3.1.1 error-shutdown auto-recovery cause efm-threshold-event (upgrade-compatible command)

Function

The **error-shutdown auto-recovery cause efm-threshold-event** command enables an interface in error-shutdown state to go Up.

NOTE

An interface enters the error-shutdown state after being shut down due to an error.

Format

error-shutdown auto-recovery cause efm-threshold-event

Parameters

Parameter	Description	Value
cause	Indicates the cause for an interface in error-down state.	-
efm-threshold-event	Indicates that a threshold crossing event occurs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. You can associate an EFM crossing event with an interface. Then the system sets the administrative status of the interface to Down. In this manner, all services on the interface are interrupted.

By default, an interface can only be resumed by a network administrator after being shut down. To configure the interface to restore to the Up state automatically, run the **error-down auto-recovery** command to set an auto recovery.

Example

Set the auto recovery after an EFM threshold crossing event is associated with an interface.

```
<HUAWEI> system-view
[HUAWEI] error-shutdown auto-recovery cause efm-threshold-event
```

19.3.1.2 error-shutdown auto-recovery interval (upgrade-compatible command)

Function

The **error-shutdown auto-recovery interval** command sets the auto recovery delay.

NOTE

An interface enters the error-shutdown state after being shut down due to an error.

Format

error-shutdown auto-recovery interval *interval-value*

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the auto recovery delay.	The value is an integer that ranges from 30 to 86400, in seconds. ● A smaller value indicates a higher frequency at which an interface alternates between Up and Down states. ● A larger value indicates longer traffic interruption.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an interface can only be resumed by a network administrator after being shut down. To configure the interface to restore to the Up state automatically, run the **error-shutdown auto-recovery interval** command to set an auto recovery delay. After the delay, the interface goes Up automatically.

Example

Set the auto recovery delay to 50s.

```
<HUAWEI> system-view
[HUAWEI] error-shutdown auto-recovery interval 50
```

19.3.1.3 port-down holdoff-timer (upgrade-compatible command)

Function

Using the **port-down holdoff-timer** command, you can set the delay in reporting a port status change event.

Format

port-down holdoff-timer *interval*

Parameters

Parameter	Description	Value
interval	Specifies the delay timer.	The value is an integer. The value can be 0 or in the range of 50 to 50000, in milliseconds.

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the cable connected to an interface is faulty, the interface status may change frequently. When this occurs, the system frequently updates the matching entries. If link backup is configured on the interface, active/standby switchovers occur frequently. To prevent frequent status change, you can use the **port-down holdoff-timer** command to set the delay in reporting a port status change event.

If an interface is connected to a wavelength division multiplexing device, the interface becomes Down when a protective switchover occurs on the wavelength division multiplexing device, and services are interrupted. To prevent service interruption, you can set the delay in reporting a port Down event.

Configuration Impact

If you run the **port-down holdoff-timer** command multiple times in the same interface view, only the latest configuration takes effect.

It is replaced by the **carrier** { **up-hold-time** | **down-hold-time** } *interval* command.

Example

Set the delay in reporting a port status change event to 1000 milliseconds on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-down holdoff-timer 1000
```

19.3.1.4 snmp-agent trap enable port (upgrade-compatible command)

Function

The **snmp-agent trap enable port** command enables the system to generate an alarm when the inbound or outbound bandwidth usage on all Ethernet sub-interfaces exceeds the threshold.

Format

snmp-agent trap enable port { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Enables the system to generate an alarm when the inbound bandwidth usage on all Ethernet sub-interfaces exceeds the threshold.	-
output-rate	Enable the system to generate an alarm when the outbound bandwidth usage on all Ethernet sub-interfaces exceeds the threshold.	-

Views

System review

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

If the threshold for the inbound or outbound bandwidth usage has been configured on an Ethernet sub-interface, you can enable the system to generate an alarm when the threshold is exceeded. This allows you to determine whether the device is functioning normally.

After the configuration is complete, the system generates an alarm when the bandwidth usage exceeds or falls below the threshold.

Example

None

19.4 Ethernet Switching Compatible Commands

19.4.1 MAC Compatible Commands

19.4.1.1 mac-address blackhole (upgrade-compatible command)

Function

Using the **mac-address blackhole** command, you can add a blackhole MAC address entry.

Format

mac-address blackhole *mac-address* [*interface-type interface-number*] **vlan** *vlan-id1* [**ce-vlan** *vlan-id2*]

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in a MAC address entry.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
interface-type interface-number	Specifies the outbound interface in a MAC address entry. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
vlan *vlan-id1*	Specifies the VLAN ID in the outer VLAN tag.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **mac-address blackhole** command.

19.4.1.2 mac-address static (upgrade-compatible command)

Function

Using the **mac-address static** command, you can add a static MAC address entry.

Format

mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id1*

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in a MAC address entry.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
interface-type interface-number	Specifies the outbound interface in a MAC address entry. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
vlan *vlan-id1*	Specifies the VLAN ID in the VLAN tag.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **mac-address static vlan**, **mac-address static vlanif**, and **mac-address static vsi** command.

19.4.2 Link Aggregation Compatible Commands

19.4.2.1 mode lacp-static (upgrade-compatible command)

Function

The **mode** command configures the LACP mode of an Eth-Trunk.

Format

mode lacp-static

Parameters

none

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mode lacp** command.

19.4.2.2 lacp e-trunk system-id (Eth-Trunk interface view) (upgrade-compatible command)

Function

The **lacp e-trunk system-id** command configures the Link Aggregation Control Protocol (LACP) system ID of an E-Trunk.

The **undo lacp e-trunk system-id** command deletes the LACP system ID of an E-Trunk.

By default, the LACP system ID is the Ethernet MAC address of the device.

Format

lacp e-trunk system-id *mac-address*

undo lacp e-trunk system-id

Parameters

Parameter	Description	Value
system-id *mac-address*	Specifies the LACP system ID of the E-Trunk.	The value is in the format of H-H-H. An H contains 1 to 4 hexadecimal digits, such as 00e0 and fc01. If an H contains fewer than four digits, 0s are padded ahead. For example, if an H is specified as e0, it is displayed as 00e0. The LACP system ID cannot be all 0s or all Fs. **NOTE** The LACP system ID cannot be all 0s. If the value is all Fs, it indicates that the LACP system ID is restored to the default.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **lacp system-id** *mac-address* command.

19.4.2.3 snmp-agent trap enable eth-trunk (upgrade-compatible command)

Function

The **snmp-agent trap enable eth-trunk** command enables the Simple Network Management Protocol (SNMP) trap function on an Eth-Trunk.

The **undo snmp-agent trap enable eth-trunk** command disables the SNMP trap function on an Eth-Trunk.

By default, the SNMP trap function is disabled on an Eth-Trunk.

Format

snmp-agent trap enable eth-trunk

undo snmp-agent trap enable eth-trunk

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If the SNMP trap function is enabled on an Eth-Trunk, the system sends a trap to the network management system (NMS) server in case of when the following exceptions occur:

- The negotiation of the LAG fails.
- The bandwidth of the LAG is lost. For example, if the lower threshold of the number of active interfaces is set by using the **least active-linknumber** command and if the number of active interfaces is smaller than this value, the Eth-Trunk becomes Down and the system sends the trap.
- Part of the bandwidth of the LAG is lost. When one of active interfaces fails, the system sends the trap because the number of active interfaces is reduced.

Example

Enable the SNMP trap function on an Eth-Trunk so that the trap can be sent to the NMS server promptly when the status of the LAG changes.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable eth-trunk
```

19.4.3 VLAN Compatible Commands

19.4.3.1 port mux-vlan enable (upgrade-compatible command)

Function

The **port mux-vlan enable** command enables the MUX VLAN function on an interface.

The **undo port mux-vlan enable** command disables the MUX VLAN function on an interface.

By default, the MUX VLAN function is disabled on an interface.

Format

port mux-vlan enable

undo port mux-vlan enable

Parameters

None

Views

GE interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **port mux-vlan enable vlan** command.

19.4.4 Voice VLAN Compatible Commands

19.4.4.1 voice-vlan enable (upgrade-compatible command)

Function

The **voice-vlan enable** command enables the voice VLAN function on an interface.

By default, the voice VLAN function is disabled on an interface.

Format

voice-vlan enable

Parameters

None

Views

GE interface view, Ethernet interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **voice-vlan** *vlan-id* **enable** command.

19.4.5 GVRP Compatible Commands

19.4.5.1 garp leaveall timer (upgrade-compatible command)

Function

The **garp leaveall timer** command sets the GARP LeaveAll timer.

Format

garp leaveall timer *timer-value*

Parameters

Parameter	Description	Value
timer-value	Specifies the value of the GARP LeaveAll timer.	The value is an integer that ranges from 65 to 32765 and that can be exactly divided by 5, in centiseconds. The value of the LeaveAll timer must be greater than the values of Leave timers on all the interfaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. Then the LeaveAll timer restarts.

Devices on a network may have different settings for the LeaveAll timer. In this case, all the devices use the smallest LeaveAll timer value on the network. When the LeaveAll timer of a device expires, the device sends LeaveAll messages to other devices. After other devices receive the LeaveAll messages, they reset their LeaveAll timers. Therefore, only the LeaveAll timer with the smallest value takes effect even if devices have different settings for the LeaveAll timer.

Prerequisites

Before setting GARP timers on an interface, you must enable GVRP globally.

Precautions

The Leave timer length on an interface is restricted by the global LeaveAll timer length. When configuring the global LeaveAll timer, ensure that all the interfaces that have a GARP Leave timer configured are working properly.

Example

Set the LeaveAll timer to 510 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] garp leaveall timer 510
```

19.4.6 STP Compatible Commands

19.4.6.1 snmp-agent trap enable mstp (upgrade-compatible command)

Function

The **snmp-agent trap enable mstp** command enables the trap function for the MSTP module.

Format

snmp-agent trap enable mstp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name mstp** command in the system view.

19.4.6.2 snmp-agent trap enable feature-name mstp (upgrade-compatible command)

Function

The **snmp-agent trap enable feature-name mstp** command enables the trap function for the MSTP module.

By default, the trap function is disabled for the MSTP module.

Format

snmp-agent trap enable feature-name mstp trap-name { **nnewroot** | **ntopologychange** }

undo snmp-agent trap enable feature-name mstp trap-name { **nnewroot** | **ntopologychange** }

Parameters

Parameter	Description	Value
trap-name	Enables the traps of spanning tree protocol events of specified types.	-
nnewroot	Enables the device to send trap when the current device is elected as the root bridge.	-
ntopologychange	Enables the device to send trap when the topology changes.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name mstp trap-name** { **newroot** | **topologychange** } command in the system view.

19.4.6.3 stp tc-protection (upgrade-compatible command)

Function

The **stp tc-protection** command enables the trap function for the Topology Change (TC) BPDU protection.

The **undo stp tc-protection** command disables the trap function for the TC BPDU protection.

By default, the trap function for the TC BPDU protection is disabled.

Format

stp tc-protection

undo stp tc-protection

Parameters

None

Views

System view or MST process region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The TC attack defense function is enabled by default, you can run the **stp tc-protection interval** command to set the time that a device needs to process the maximum number of TC BPDUs which is configured using the **stp tc-protection threshold** command. If there are packets exceeding the maximum number, the switch processes the packets after the time specified in the **stp tc-protection interval** command expires. For example, if the time is set to 10 seconds and the maximum number is set to 5, when a switch receives TC BPDUs, the switch processes only the first 5 TC BPDUs within 10 seconds and processes the other TC BPDUs after the time expires. In this way, the device does not frequently update its MAC address entries and ARP entries, reducing CPU usage.

To learn about detailed processing information on TC BPDUs, run the **stp tc-protection** command to enable the trap function for the TC BPDU protection.

After the function is enabled, MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.15 hwMstpiTcGuarded and MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.16 hwMstpProTcGuarded are generated.

Precautions

The trap function for the TC BPDU protection takes effect only when the **snmp-agent trap enable feature-name mstp** and **stp tc-protection** are both run.

19.4.7 L2PT Compatible Commands

19.4.7.1 bpdu-tunnel (upgrade-compatible command)

Function

The **bpdu-tunnel** command configures an interface to forward or discard BPDUs.

By default, an interface discards the received BPDUs.

Format

bpdu-tunnel { **enable** | **disable** }

Parameters

Parameter	Description	Value
enable | **disable**	Indicates the action that an interface performs on BPDUs. - **enable**: The interface discards BPDUs. - **disable**: The interface forwards BPDUs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel stp** { **enable** | **disable** } command.

19.4.7.2 bpdu-tunnel enable (upgrade-compatible command)

Function

The **bpdu-tunnel enable** command enables Layer 2 protocol tunneling on an interface.

Format

bpdu-tunnel { **all** | *protocol-type* &<1-15> } **enable**

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol. You can specify multiple protocols in the command.	-

Views

Ethernet interface view, XGE interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel** { **all** | { *protocol-type* } &<1-15> | **user-defined-protocol** *protocol-name* } **enable** command.

19.4.7.3 bpdu-tunnel group-mac (upgrade-compatible command)

Function

The **bpdu-tunnel group-mac** command enables the switch to replace the multicast destination MAC address of Layer 2 protocol packets with a specified multicast MAC address.

Format

bpdu-tunnel *protocol-type* **group-mac** *group-mac*

Parameters

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol.	The value is a string of 1 to 31.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel** *protocol-type* **group-mac** *group-mac* command.

19.4.7.4 bpdu-tunnel stp group-mac (upgrade-compatible command)

Function

Using the **bpdu-tunnel stp group-mac** command, you can replace the global well-known MAC address of the STP BPDU packets with a multicast MAC address.

Format

bpdu-tunnel stp group-mac *group-mac*

Parameters

Parameter	Description	Value
group-mac *group-mac*	Specifies the multicast MAC address that replaces the well-known global MAC address of the BPDU packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel stp group-mac** *group-mac* command.

19.4.7.5 bpdu-tunnel stp vlan (upgrade-compatible command)

Function

Using the **bpdu-tunnel stp vlan** command, you can configure the interface to accept the BPDU packets whose tag values range from *low-vid* to *high-vid*.

Using the **undo bpdu-tunnel stp vlan** command, you can cancel the configuration.

By default, an interface does not accept the tagged BPDU packets.

Format

bpdu-tunnel stp vlan { *low-vid* [**to** *high-vid*] } &<1-10>

undo bpdu-tunnel stp vlan { *low-vid* [**to** *high-vid*] } &<1-10>

Parameters

Parameter	Description	Value
low-vid	Specifies the start VLAN ID of the BPDU packets that can be accepted by the interface.	The value is a decimal integer ranging from 1 to 4094. It must be smaller than *high-vid*.
high-vid	Specifies the end VLAN ID of the BPDU packets that can be accepted by the interface.	The value is a decimal integer ranging from 1 to 4094. It must be greater than *low-vid*.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel stp** { **vlan** *low-id* [**to** *high-id*] } &<1-10> command.

19.4.7.6 bpdu-tunnel vlan (upgrade-compatible command)

Function

The **bpdu-tunnel vlan** command enables VLAN-based Layer 2 protocol tunneling on an interface.

Format

bpdu-tunnel { **all** | *protocol-type* &<1-15> } **vlan** { *low-id* [**to** *high-id*] } &<1-10>

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol. You can specify multiple protocols in the command.	-
low-id	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be smaller than the end VLAN ID.
high-id	Specifies the end VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be greater than the start VLAN ID.

Views

Ethernet interface view, XGE interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel vlan** command.

19.4.7.7 l2protocol-tunnel user-defined-protocol (upgrade-compatible command)

Function

The **l2protocol-tunnel user-defined-protocol** command defines the characteristics of a Layer 2 protocol whose packets are transparently transmitted, including the protocol name, Ethernet encapsulation type, destination MAC address of packets, multicast MAC address replacing the destination multicast MAC address of packets, and priority of packets.

By default, there is no user-defined characteristics of a Layer 2 protocol whose packets are transparently transmitted.

Format

l2protocol-tunnel user-defined-protocol *protocol-name* **protocol-mac** *protocol-mac* **encape-type** { **ethernetii protocol-type** *protocol-type* | **llc dsap** *dsap-value* **ssap** *ssap-value* | **snap protocol-type** *protocol-type* } **group-mac** { *group-mac* | **default-group-mac** } [**priority** *priority-id*]

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a user-defined Layer 2 protocol whose packets are transparently transmitted.	The name is a string of 1 to 31 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
protocol-mac *protocol-mac*	Specifies the destination multicast MAC address of the Layer 2 protocol packets that are transparently transmitted. This MAC address must be an ordinary MAC address that has not been used on the devices.	The address is in the format of H-H-H, H indicating a 4-bit hexadecimal number.

Parameter	Description	Value
encape-type	Defines the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **ethernetii**: indicates Ethernet_II, the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **llc**:: indicates Logical Link Control (LLC), the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **snap**: indicates Sub-Network Access Protocol (SNAP), the encapsulation format for Layer 2 protocol packets that are transparently transmitted. When transparently-transmitted Layer 2 protocol packets carry the same protocol MAC address and protocol type, you can use the parameter **encap-type** to define different encapsulation formats to differentiate these packets.	-
protocol-type *protocol-type*	Specifies the value of Ethernet encapsulation type.	The value is a hexadecimal number ranging from 0600 to FFFF.
dsap *dsap-value*	Specifies the destination service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.
ssap *ssap-value*	Specifies the source service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination multicast MAC address of the Layer 2 protocol packets that are transparently transmitted. The address must be an ordinary MAC address, which cannot be the MAC address of bridge protocol data units (BPDUs), the MAC address of Smart Link protocol packets, or a special MAC address.	The address is in the format of H-H-H, H indicating a 4-bit hexadecimal number.

Parameter	Description	Value
default-group-mac	Specifies the default MAC address of a multicast group, which is 0100-0ccd-cdd0. This parameter can simplify the configuration and reduce the configuration error. For example: Most Layer 2 protocols can be classified by types. Default MAC addresses of Layer 2 protocols in the same type are the same. In this case, you can attach the parameter **default-group-mac** to the **l2protocol-tunnel user-defined-protocol** command to reduce the configuration workload and the probability of configuration error.	-
priority *priority-id*	Specifies the priority of the Layer 2 protocol packets that are transparently transmitted.	The value is an integer that ranges from 1 to 7. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel user-defined-protocol** command.

19.5 IP Service Compatible Commands

19.5.1 DHCP Upgrade-compatible Commands

19.5.1.1 expired (upgrade-compatible command)

Function

The **expired** command sets the lease for IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer ranging from 0 to 999, in days. The default value is 1.
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer ranging from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer ranging from 0 to 59, in minutes. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **expired-hide** command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment. Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, configure **expired** as **unlimited** to set the IP address lease of the specified global address pool to unlimited. If some hosts such as a portable computer just need to user temporary IP addresses, set the IP address lease of the specified global address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts or half of its IP address lease has passed, the DHCP client sends a DHCP Request packet to the DHCP server to renew the lease. If the IP address can still be assigned to the client, the DHCP server informs a renewed IP address lease to the client. If the IP address can no longer be assigned to this client, the DHCP server informs the client that the IP address lease cannot be renewed and it needs to apply for another IP address.

Prerequisites

Run the **ip pool** command to create a global IP address pool and the **dhcp enable** command to globally enable the DHCP server function.

Precautions

Different IP address leases can be specified for different global IP address pools on a DHCP server. In a global IP address pool, all addresses have the same lease.

Example

Specify the IP address lease of the global address pool global1 to 1 day 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] expired  day 1 hour 2 minute 30
```

19.5.1.2 dhcp server expired (upgrade-compatible command)

Function

The **dhcp server expired** command sets the lease for IP addresses in an interface IP address pool.

By default, the lease of IP addresses is one day.

Format

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

Parameters

Parameter	Description	Value
day	Specifies the number of days in the IP address lease.	The value is an integer ranging from 0 to 999, in days. The default value is 1.
hour	Specifies the number of hours in the IP address lease.	The value is an integer ranging from 0 to 23, in hours. The default value is 0.
minute	Specifies the number of minutes in the IP address lease.	The value is an integer ranging from 0 to 59, in minutes. The default value is 0.

Parameter	Description	Value
unlimited	Indicates that the IP address lease is unlimited.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server expired** command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment. Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, run the **dhcp server expired unlimited** command to set the IP address lease of the specified VLANIF interface address pool to unlimited. If some hosts such as a portable computer just need to user temporary IP addresses, run the **dhcp server expired** command to set the IP address lease of the specified VLANIF interface address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts or half of its IP address lease has passed, the DHCP client sends a DHCP Request packet to the DHCP server to renew the lease. If the IP address can still be assigned to the client, the DHCP server informs the client of a renewed IP address lease. If the IP address can no longer be assigned to this client, the DHCP server informs the client that the IP address lease cannot be renewed.

Prerequisites

Run the **dhcp enable** command to globally enable the DHCP function. Run the **dhcp select interface** command in the VLANIF interface view to enable the interface IP address pool.

Precautions

Different IP address leases can be specified for different interface IP address pools on a DHCP server. In an interface IP address pool, all IP addresses have the same lease.

Example

Set the IP address lease of the IP address pool on VLANIF 100 to 2 days 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server expired day 2 hour 2 minute 30
```

19.5.1.3 dhcp server forbidden-ip (upgrade-compatible command)

Function

The **dhcp server forbidden-ip** command specifies the range of IP addresses that cannot be assigned to clients by the DHCP server.

By default, the system does not configure the range of IP addresses that cannot be assigned to clients by the DHCP server.

Format

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address that cannot be automatically assigned.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address that cannot be automatically assigned. If *end-ip-address* is not specified, only *start-ip-address* cannot be assigned to clients.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server forbidden-ip** command applies to DHCP servers. In an IP address pool, some IP addresses need to be reserved for other services, and some IP addresses are statically assigned to certain hosts (such as the DNS server) and cannot be automatically assigned to clients. You can run the **dhcp server**

forbidden-ip command to specify the range of the IP addresses that cannot be automatically assigned to clients from the IP address pool.

Precautions

- The excluded IP address must be in the IP address pool range.
- The excluded IP address or IP address segment cannot be automatically assigned to clients from a local address pool.
- If you run the **dhcp server forbidden-ip** command multiple times, you can specify multiple IP addresses or IP address segments that cannot be automatically assigned to clients from the specified address pool.

Example

Configure that IP addresses in the address pool 10.10.10.10 to 10.10.10.20 cannot be automatically assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp server forbidden-ip 10.10.10.10 10.10.10.20
```

19.5.1.4 dhcp server ip-pool

Function

The **dhcp server ip-pool** command creates a global IP address pool.

The **undo dhcp server ip-pool** command deletes a global IP address pool.

By default, no global IP address pool is created.

Format

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of a global IP address pool.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

This function equals to the **ip pool** *ip-pool-name* command.

19.5.1.5 dhcp server ping

Function

The **dhcp server ping** command sets the maximum number of ping packets to be sent and the maximum response time of a ping packet.

By default, a DHCP server does not send any ping packet.

Format

dhcp server ping { **packets** *number* | **timeout** *milliseconds* } *

Parameters

Parameter	Description	Value
packets *number*	Specifies the maximum number of ping packets to be sent.	The value is an integer that ranges from 0 to 10.
timeout *milliseconds*	Specifies the maximum response time of a ping packet.	The value is an integer that ranges from 0 to 10000, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **dhcp server ping** { **packet** *number* | **timeout** *milliseconds* } * command.

Example

Set the maximum number of ping packets to be sent to 5.

```
<HUAWEI> system-view
[HUAWEI] dhcp server ping packets 5
```

19.5.1.6 dns-suffix

Function

The **dns-suffix** command configures the domain name suffix to be assigned by the DHCP server to a DHCP client.

By default, no domain name suffix is configured for a DHCP client.

Format

dns-suffix *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name suffix to be assigned to a DHCP client.	The value is a string of 1 to 63 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, it is replaced by the **domain-name** *domain-name* command.

19.5.1.7 ip relay address (upgrade-compatible command)

Function

Using the **ip relay address** command, you can configure DHCP server addresses on a VLANIF interface enabled with DHCP relay.

Using the **undo ip relay address** command, you can delete the configured DHCP server addresses.

By default, no DHCP server address is configured on a VLANIF interface enabled with DHCP relay.

Format

ip relay address *ip-address*

undo ip relay address { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.
all	Deletes all the DHCP server addresses configured on an interface.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip relay address** command is applicable to DHCP relay agents. When a DHCP client needs to send a DHCP request packet to a DHCP server on a different network segment by using a DHCP relay agent, run the **ip relay address** command on the DHCP relay agent to configure a DHCP server address.

Prerequisites

DHCP relay has been enabled on the VLANIF interface by using the **dhcp select relay** command.

Precautions

If you run the **ip relay address** command multiple times, multiple DHCP server addresses are configured.

Example

Configure DHCP server addresses 10.2.2.2 on VLANIF100 enabled with DHCP relay.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] ip relay address 10.2.2.2
```

19.5.1.8 lease (upgrade-compatible command)

Function

The **lease** command sets the lease for IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

lease *day* [*hour* [*minute*]]

Parameters

Parameter	Description	Value
day	Specifies the number of days in the IP address lease.	The value is an integer ranging from 0 to 999, in days. The default value is 1.
hour	Specifies the number of hours in the IP address lease.	The value is an integer ranging from 0 to 23, in hours. The default value is 0.
minute	Specifies the number of minutes in the IP address lease.	The value is an integer ranging from 0 to 59, in minutes. The default value is 0.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

After the upgrade, it is replaced by the **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } command.

Example

Specify the IP address lease of the global address pool **global1** to 1 day.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] lease 1
```

19.5.1.9 static-bind mac-address

Function

The **static-bind mac-address** command binds a MAC address to a global IP address pool.

Format

static-bind mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, it is replaced by the **static-bind** *ip-address* **mac-address** *mac-address* command.

19.5.1.10 dhcpv6 relay destination (upgrade-compatible command)

Function

The **dhcpv6 relay destination** command enables the DHCPv6 relay function on interfaces and configures the IPv6 address of the DHCPv6 server or next-hop relay agent.

By default, the DHCPv6 relay function is disabled on an interface.

Format

dhcpv6 relay destination *ipv6-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of the outbound interface of relay messages.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a client applies to a DHCPv6 server on a different network segment for an IPv6 address, you need to deploy a relay agent between the client and the DHCPv6 server. In this manner, the relay agent transmits DHCPv6 messages exchanged between the client and the DHCPv6 server.

19.6 IP Multicast Compatible Commands

19.6.1 MLD Snooping Compatible Commands

19.6.1.1 mld-snooping group-policy (interface view) (upgrade-compatible command)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy on an interface.

Format

mld-snooping group-policy *acl6-number* **vlan** *vlan-id mld-version* [**default-permit**]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 to 3999.
vlan *vlan-id*	Applies the IPv6 multicast group policy to a specified VLAN on an interface.	The value is an integer that ranges from 1 to 4094.
mld-version	Specifies an MLD version. The multicast group policy is applied only to the MLD messages of this version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. ● 1: MLDv1 ● 2: MLDv2
default-permit	Configures the multicast group policy to permit all groups by default. That is, if the referenced ACL has no rules, the multicast group policy allows hosts in the VLAN to join all groups.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

Prevent MLDv2 hosts in VLAN 10 on GE0/0/1 from joining IPv6 multicast group ff1c::3/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule deny source ff1c::3/32
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mld-snooping group-policy 2000 vlan 10 2 default-permit
```

19.6.1.2 mld-snooping group-policy (VLAN view) (upgrade-compatible command)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy in a VLAN.

Format

mld-snooping group-policy *acl6-number mld-version* [**default-permit**]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 to 3999.
mld-version	Applies the multicast group policy only to the MLD messages of the specified version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 3. ● 1: MLDv1 ● 2: MLDv2

Parameter	Description	Value
default-permit	Configures the multicast group policy to permit all groups by default. That is, if the referenced ACL has no rules, the multicast group policy allows hosts in the VLAN to join all groups.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

Prevent MLDv2 hosts in VLAN 4 from joining IPv6 multicast group ff1e::1/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule deny source ff1e::1/32
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping group-policy 2001 2 default-permit
```

19.7 MPLS compatible command

19.7.1 explicit-path (upgrade-compatible command)

Function

Using the **explicit-path** command, you can configure an explicit path of a tunnel.

By default, no explicit path of a tunnel is configured.

Format

explicit-path *path-name* { **enable** | **disable** }

Parameters

Parameter	Description	Value
path-name	Indicates the name of an explicit path.	The value is a string of 1 to 31 characters.
enable	Enables the explicit path of a tunnel.	-
disable	Disables the explicit path of a tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can configure an explicit path only after MPLS TE is enabled.

The addresses of the hops along the explicit path cannot overlap or loops cannot occur. If a loop occurs, CSPF detects the loop and fails to calculate the path.

When the explicit path is in use, you cannot perform the following operations:

- Run the **explicit-path** *path-name* **disable** command to disable the explicit path.
- Run the **undo explicit-path** command to delete the explicit path.

Example

Create an explicit path named **path1**.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] explicit-path path1 enable
[HUAWEI-explicit-path-path1]
```

19.7.2 mpls rsvp-te authentication handshake (upgrade-compatible command)

Function

The **mpls rsvp-te authentication handshake** command configures the RSVP-TE handshake mechanism and sets a local password.

The **undo mpls rsvp-te authentication handshake** command deletes the RSVP-TE handshake mechanism configuration.

By default, no RSVP-TE handshake mechanism is configured.

Format

mpls rsvp-te authentication handshake *local-secret*

undo mpls rsvp-te authentication handshake

Parameters

Parameter	Description	Value
local-secret	Specifies the local password.	The value is a string of 8 to 40 characters without spaces. It has no default value.

Views

Interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism and sets the local password.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication handshake** command can be used to configure the RSVP-TE handshake mechanism and sets the local password to prevent anti-replay and improve network security.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* } command in the interface view or the MPLS RSVP-TE neighbor view.

Precautions

local-secret is valid only on the local device and can be different from *local-secret* configured on neighbors.

Example

Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication handshake 12345678
```

Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication handshake 12345678
```

19.7.3 mpls rsvp-te send-message (upgrade-compatible command)

Function

The **mpls rsvp-te send-message** command configures the formats of objects in a sent message.

The **undo mpls rsvp-te send-message** command restores the default configuration.

By default, the formats of objects in the sent message are not configured.

Format

mpls rsvp-te send-message suggest-label exclude

undo mpls rsvp-te send-message suggest-label exclude

Parameters

Parameter	Description	Value
suggest-label exclude	Indicates that an RSVP message does not carry the suggest-label object.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls rsvp-te send-message** command controls the formats of objects in the messages sent by nodes. If required, you can use this command to adjust the transmission of messages so that downstream nodes can use the carried object format in processing.

Precautions

The modification takes effect only for new LSPs.

Configurations of the four formats of objects in a sent message can take effect simultaneously.

Example

Exclude the suggest-label object from a message.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message suggest-label exclude
```

19.7.4 mpls te max-reservable-bandwidth (upgrade-compatible command)

Function

The **mpls te max-reservable-bandwidth** command sets the maximum reservable bandwidth of a link.

The maximum reservable bandwidth of a link is not configured by default.

Format

mpls te max-reservable-bandwidth *bw-value* [**bc1** *bc1-bw-value*]

Parameters

Parameter	Description	Value
bw-value	Specifies the maximum reservable link bandwidth.	The value is an integer ranging from 0 to 40000000, in kbit/s. The default value is 0.
bc1 *bc1-bw-value*	Specifies the maximum reservable bandwidth for a BC1 link.	The value is an integer ranging from 0 to 40000000, in kbit/s. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **mpls te bandwidth max-reservable-bandwidth** command.

19.7.5 mpls te bypass-tunnel bandwidth (upgrade-compatible command)

Function

Using the **mpls te bypass-tunnel bandwidth** command, you can configure the bypass LSP bandwidth.

By default, no bypass LSP bandwidth is configured.

Format

mpls te bypass-tunnel bandwidth { *bandwidth* | { **bc0** | **bc1** } { *bandwidth* | **un-limited** } }

Parameters

Parameter	Description	Value
bandwidth	Specifies the bandwidth that the bypass tunnel can protect.	The value is an integer that ranges from 1 to 32000000, in kbit/s.
bc0	Indicates the BC0 bandwidth (global bandwidth) that the bypass tunnel can protect.	-
bc1	Indicates the BC1 bandwidth (subaddress pool bandwidth) that the bypass tunnel can protect.	-
un-limited	Indicates that there is no limit on the total bandwidth that can be protected.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The total bandwidth of LSPs protected by the bypass tunnel is not more than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system selects a single bypass tunnel through the best-fit algorithm.

The total bandwidth of all the LSPs protected by the bypass tunnel is not greater than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system determines the bypass tunnel through the best-fit algorithm.

Example

Configure Tunnel1 to protect the LSPs that use the BC0 bandwidth and set no limit on the bandwidth to be protected.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bypass-tunnel bandwidth bc0 un-limited
[HUAWEI-Tunnel1] mpls te commit
```

19.7.6 mpls te protect-switch manual (upgrade-compatible command)

Function

The **mpls te protect-switch manual** command sends a manual switchover request to a specified tunnel.

By default, no manual switching request for a specified tunnel is configured.

Format

mpls te protect-switch manual [**work-lsp** | **protect-lsp**]

Parameters

Parameter	Description	Value
work-lsp	Switches traffic manually to the primary tunnel.	-
protect-lsp	Switches traffic manually to a protection tunnel.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **mpls te protect-switch manual** command.

19.7.7 snmp-agent trap enable (MPLS) (upgrade-compatible command)

Function

The **snmp-agent trap enable** command enables SNMP traps with a related parameter.

The **undo snmp-agent trap enable** command disables SNMP traps with a related parameter.

Format

snmp-agent trap enable { **static-lsp** | **ldp** | **lsp** [**mplsxcup** | **mplsxcdown**] | **tunnel-ps** | **te** { **tunnel-reop** | **te-frr** [**private**] | **hot-standby** | **ordinary** | **bandwidth-change** } | [**te**] **tunnel** }

undo snmp-agent trap enable { **static-lsp** | **ldp** | **lsp** [**mplsxcup** | **mplsxcdown**] | **tunnel-ps** | **te** { **tunnel-reop** | **te-frr** [**private**] | **hot-standby** | **ordinary** | **bandwidth-change** } | [**te**] **tunnel** }

Parameters

Parameter	Description	Value
static-lsp	Enables the trap of static LSPs.	-
ldp	Enables LDP traps.	-
lsp mplsxcup	Enables the mplsXCUp trap.	-
lsp mplsxcdown	Enables the mplsXCDown trap.	-
tunnel-ps	Enables the TE protection switching trap.	-
te tunnel-reop	Enables trap of the TE route re-optimization.	-
te te-frr	Enables the public trap of TE FRR.	-
te-frr private	Enables the private trap of TE FRR.	-
te hot-standby	Enables the trap of the hot-standby CR-LSP.	-
te ordinary	Enables the trap of the ordinary CR-LSP.	-
bandwidth-change	Enables the system to send related private traps when the tunnel bandwidth changes.	-
tunnel	Enables the trap of the tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the trap function is disabled in the process of the MPLS LSP establishment.

To check the status of an LSP, run the **snmp-agent trap enable lsp** { **mplsxcup** | **mplsxcdown** } command when mplsXCUp or mplsXCDown is enabled.

After the **undo snmp-agent trap enable** command is run, information about mplsXCUp or mplsXCDown is not displayed, and the status of the trap is unchanged. When you run the **snmp-agent trap enable** command again, information about the restored trap is displayed.

Example

Enable the private trap of TE FRR.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable te te-frr private
```

Enable the mplsXCUp trap.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable lsp mplsxcup
 Warning: Enabling the alarm function will lead to the generation of excessive a
larms. Continue? [Y/N]
```

19.7.8 snmp-agent trap enable feature-name ldp (upgrade-compatible command)

Function

The **snmp-agent trap enable feature-name ldp** command enables the trap for the MPLS LDP module.

The **undo snmp-agent trap enable feature-name ldp** command disables the trap for the MPLS LDP module.

By default, the trap is disabled for the MPLS LDP module.

Format

snmp-agent trap enable feature-name ldp trap-name { **session-down** | **session-up** }

undo snmp-agent trap enable feature-name ldp trap-name { **session-down** | **session-up** }

Parameters

Parameter	Description	Value
trap-name	Enables the trap of MPLS LDP events of a specified type.	-
session-down	Enables the trap of the event that an LDP session goes Down in the MIB.	-
session-up	Enables the trap of the event that an LDP session goes Up in the MIB.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **snmp-agent trap enable feature-name ldp** command to enable the LDP session trap. Currently, all traps of the MPLS LDP module are non-excessive trap. The frequent LDP session status changes do not trigger a large number of traps.

Example

Enable the trap of the event that an LDP session is reestablished.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name ldp trap-name session-up
```

19.7.9 static-cr-lsp ingress bandwidth (upgrade-compatible command)

Function

Using the **static-cr-lsp ingress bandwidth** command, you can configure a static CR-LSP and specify its bandwidth on the ingress LSR.

By default, no static CR-LSP on the ingress LSR is configured.

Format

static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* } **destination** *destination-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* **bandwidth** { **bc0** | **bc1** } *bandwidth*

Parameters

Parameter	Description	Value
tunnel-interface tunnel *interface-number*	Specifies the tunnel interface of a static CR-LSP. *interface-number* indicates the tunnel interface number.	-
tunnel-name	Specifies the name of a CR-LSP.	The name is a string of 1 to 19 case-sensitive characters, spaces and abbreviation not supported. If you use the **interface Tunnel 2** command to create a tunnel interface for a static CR-LSP, the tunnel name in the **static-cr-lsp ingress** command must be formatted as "Tunnel2", otherwise, the tunnel cannot be created. There is no such a limit for the transit node and egress node.
destination *destination-address*	Specifies the destination IP address of a static CR-LSP.	-
nexthop *next-hop-address*	Specifies the next-hop IP address of a static CR-LSP.	-
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outgoing interface. This parameter is only applicable to a P2P link.	-
out-label *out-label*	Specifies the value of an outgoing label.	*out-label* is an integer ranging from 16 to 1048575.
bc0	Specifies BC0 bandwidth of a static CR-LSP.	-
bc1	Specifies BC1 bandwidth of a static CR-LSP.	-
bandwidth	Specifies the bandwidth required by a CR-LSP.	The value ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions.

Example

Configure the static CR-LSP named Tunnel1, with the destination IP address being 10.1.3.1, the next-hop address being 10.1.1.2, the outgoing label being 237, and the required bandwidth being 20 kbit/s from BC0 on the ingress.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp ingress tunnel-interface Tunnel 1 destination 10.1.3.1 nexthop 10.1.1.2 out-
label 237 bandwidth bc0 20
```

19.7.10 static-cr-lsp transit bandwidth (upgrade-compatible command)

Function

Using the **static-cr-lsp transit bandwidth** command, you can configure a static CR-LSP and specify its bandwidth on a transit LSR.

By default, no static CR-LSP on a transit LSR is configured.

Format

static-cr-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* **bandwidth** { **bc0** | **bc1** } *bandwidth* [**description** *description*]

Parameters

Parameter	Description	Value
lsp-name	Specifies the CR-LSP name.	The name is a string of 1 to 19 case-sensitive characters, spaces not supported.
incoming-interface *interface-type interface-number*	Specifies the name of an incoming interface.	-
in-label *in-label*	Specifies the value of an incoming label.	An integer ranging from 16 to 1023
nexthop *next-hop-address*	Specifies the next-hop address.	-
outgoing-interface *interface-type interface-number*	Specifies the name of an outgoing interface.	-

Parameter	Description	Value
out-label *out-label*	Specifies the value of an outgoing label.	An integer ranging from 16 to 1048575.
bc0	Obtains the bandwidth from BC0.	-
bc1	Obtains the bandwidth from BC1.	-
bandwidth	Specifies the bandwidth required by a CR-LSP.	The value ranges from 0 to 4000000000, in kbit/s. The default value is 0.
description *description*	Specifies the description information.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions.

Example

Configure the static CR-LSP named tunnel34, with the incoming interface being VLANIF10, the incoming label being 123, the outgoing interface being VLANIF20, the outgoing label as 253, the required BC0 bandwidth being 20 kbit/s on the transit node.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp transit tunnel34 incoming-interface vlanif 10 in-label 123 outgoing-interface
vlanif 20 out-label 253 bandwidth bc0 20
```

19.7.11 undo mpls te auto-frr (upgrade-compatible command)

Function

The **undo mpls te auto-frr** command disables MPLS TE Auto FRR in the interface view.

Format

undo mpls te auto-frr

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mpls te auto-frr block** command.

19.8 VPN compatible command

19.8.1 display ipv6 prefix-limit statistics (upgrade-compatible command)

Function

The **display ipv6 prefix-limit statistics** command displays the statistics of the prefix limits of IPv6 VPN instances.

Format

display ipv6 prefix-limit { **all-vpn6-instance** | **vpn6-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn6-instance	Indicates all IPv6 VPN instances.	-
vpn6-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified IPv6 VPN instance.

Example

Display the statistics of the prefix limits of all IPv6 VPN instances.

```
<HUAWEI> display ipv6 prefix-limit all-vpn6-instance statistics
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0               0            0               0              0
STATIC        0               0            0               0              0
OSPFv3       11               3            1               0              5
IS-IS       106               0            1               0              5
RIPng        98               0            1               1              5
BGP           2               0            1               1              5
------------------------------------------------------------------------------
IPv6 VPN instance name: VPN123

         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0               0            0               0              0
STATIC        0               0            0               0              0
OSPFv3       11               3            1               0              5
IS-IS       106               0            1               0              5
RIPng        98               0            1               1              5
BGP           2               0            1               1              5
```

Table 19-3 Description of the display ipv6 prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

Display the statistics of the prefix limit of the IPv6 VPN instance named **vrf1**.

```
<HUAWEI> display ipv6 prefix-limit vpn6-instance vrf1 statistics
------------------------------------------------------------------------------
```

```
IPv6 VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0              0           0             0            0
STATIC         0              0           0             0            0
OSPFv3        11              3           1             0            5
IS-IS        106              0           1             0            5
RIPng         98              0           1             1            5
BGP            2              0           1             1            5
```

19.8.2 display ipv6 vpn-instance (upgrade-compatible command)

Function

The **display ipv6 vpn6-instance** command displays information about an IPv6 VPN instance.

Format

display ipv6 vpn6-instance [**brief** | **verbose**] [*vpn6-instance-name*]

Parameters

Parameter	Description	Value
brief	Displays summary information about an IPv6 VPN instance.	-
verbose	Displays detailed information about the IPv6 VPN instances and their associated interfaces.	-
vpn6-instance-name	Specifies the name of an IPv6 VPN instance.	The name is a string of 1 to 31 case-sensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a VPN instance is configured, you can check the configuration of the instance by using the **display ipv6 vpn6-instance** command. You can also use this command to view the VPN instances configured on the local device.

When no parameters are specified, the command displays brief information about all the configured VPN instances.

Example

View brief information about all the configured IPv6 VPN instances.

```
<HUAWEI> display ipv6 vpn6-instance
 Total VPN-Instances configured      : 3
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 1

  VPN-Instance Name              RD                   Address-family
  vpn1
  vpna                       100:1                IPv4
  vpna                       100:3                IPv6
  vpnb                       100:2                IPv4
```

Table 19-4 Description of the display ip vpn-instance command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name	Name of the VPN instance.
RD	RD of the VPN instance IPv4 address family or IPv6 address family.
Creation Time	Time when an IPv4 or IPv6 address family is enabled for the VPN instance.
Address-family	Address family enabled for the VPN instance. The address family can be: ● Null, if no address family is enabled. ● ipv4, if only the IPv4 address family is enabled. ● ipv6, if only the IPv6 address family is enabled.

```
<HUAWEI> display ipv6 vpn6-instance brief
 Total VPN-Instances configured      : 3
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 1

  VPN-Instance Name              RD                   Address-family
  vpn1
  vpna                       100:1                IPv4
  vpna                       100:3                IPv6
  vpnb                       100:2                IPv4
```

View detailed information about all IPv6 VPN instances.

```
<HUAWEI> display ipv6 vpn-instance verbose
 Total VPN-Instances configured      : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 1

 VPN-Instance Name and ID : vpna, 6
  Description : vpna-1
  Service ID : 12
  Interfaces : Vlanif10
 Address family ipv4
  Create date : 2012/12/3 15:36:20 UTC+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Route Distinguisher : 100:1
  Export VPN Targets :  1:1
  Import VPN Targets :  1:1
  Label Policy : label per instance
  Per-Instance Label : 1024
  IP FRR Route Policy : 20
  VPN FRR Route Policy : 12
  Import Route Policy : 10
  Export Route Policy : 20
  Tunnel Policy : bindTE
  Maximum Routes Limit : 2000
  Threshold Routes Limit : 80%
  Maximum Prefixes Limit : 1024
  Threshold Prefixes Limit : 50%
  Install Mode : route-unchanged
  Log Interval : 10
 Address family ipv6
  Create date : 2012/12/3 15:36:20 UTC+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Log Interval : 5
```

Table 19-5 Description of the display ip vpn-instance verbose command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name and ID	Name and ID of the VPN instance. The ID is assigned by the system, which facilitates indexing.
Description	Description of the VPN instance. This field is displayed in the command output only when the **description (VPN instance view)** command is used.

Item	Description
Service ID	Service ID of the VPN instance. This item is displayed only after the **service-id (VPN instance view)** command is run in the VPN instance view.
Interfaces	Interfaces bound to the VPN instance. This field is displayed only after the **ip binding vpn-instance** command is configured on these interfaces.
Address family ipv4	Information about the IPv4 address family enabled for the VPN instance.
Address family ipv6	Information about the IPv6 address family enabled for the VPN instance.
Create date	Time when the VPN instance is created.
Up time	Period during which the VPN instance maintains in the Up state.
Route Distinguisher	RD of the VPN instance IPv4 address family or IPv6 address family
Export VPN Targets	Route Target list in the outbound direction. To set the VPN target, run the **vpn-target** command.
Import VPN Targets	Route Target list in the inbound direction. To set the VPN target, run the **vpn-target** command.
Label Policy	Label policy: ● label per instance: indicates that the same label is allocated to routes of a VPN instance. This field is displayed in the command output only when the **apply-label per-instance** command is run in the VPN instance view. ● label per route: indicates that each route of a VPN instance is assigned a label. Label allocation for routes of a VPN instance is implemented in this mode.

Item	Description
Per-Instance Label	Label value used when all VPN routes of the VPN instance address family share one label. This field is displayed only after the **apply-label per-instance** command is run in the VPN instance address family view.
IP FRR Route Policy	IP FRR route policy used for the address family. This item is displayed only after the **ip frr** command is run in the VPN instance IPv4 address family view.
VPN FRR Route Policy	VPN FRR route policy used for the address family. This item is displayed only after the **vpn frr** command is run in the VPN instance IPv4 address family view.
Import Route Policy	Import Route-Policy applied to the VPN instance. This field is displayed only after the **import route-policy** command is run in the VPN instance address family view.
Export Route Policy	Export Route-Policy applied to the VPN instance. This field is displayed only after the **export route-policy** command is run in the VPN instance address family view.
Tunnel Policy	Tunnel policy applied to the VPN instance. This field is displayed only after the **tnl-policy** command is run in the VPN instance address family view.
Maximum Routes Limit	Maximum number of routes supported by the current address family. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Threshold Routes Limit	Percentage of the maximum number of routes specified for the current address family. When the maximum number of routes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.

Item	Description
Maximum Prefixes Limit	Maximum number of prefixes supported by the current address family of the VPN instance. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Threshold Prefixes Limit	Percentage of the maximum number of prefixes specified for the current address family of the VPN instance. When the maximum number of prefixes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Install Mode	Method of processing routes. The **prefix limit** command can be used to specify the route processing method when the threshold is lowered due to the number of route prefixes exceeding the upper threshold. ● If **route-unchanged** is configured, routes in the routing information base (RIB) table remain unchanged. ● If **route-unchanged** is not configured, all routes in the RIB table are deleted and the routes are re-installed in the RIB table.
Log Interval	Interval for displaying log messages when the number of VPN instance routes exceeds the maximum value. The default interval is 5 seconds. The value can be set by the command **limit-log-interval**.

19.8.3 ipv6 binding vpn6-instance (upgrade-compatible command)

Function

The **ipv6 binding vpn6-instance** command binds the current interface to an IPv6 VPN instance.

The **undo ipv6 binding vpn6-instance** command unbinds the current interface from an IPv6 VPN instance.

By default, an interface is a public network interface and is not bound to any IPv6 VPN instance.

Format

ipv6 binding vpn6-instance *vpn6-instance-name*

undo ipv6 binding vpn6-instance *vpn6-instance-name*

Parameters

Parameter	Description	Value
vpn6-instance-name	Specifies the name of an IPv6 VPN instance.	The name is a string of 1 to 31 case-sensitive characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After an IPv6 VPN instance is created, the device interfaces belonging to the IPv6 VPN instance need to be bound to the instance; otherwise, the interfaces are public network interfaces.

After an interface is bound to an IPv6 VPN instance or an interface is unbound from an IPv6 VPN instance, the Layer 3 features such as the IPv6 address and IPv6 routing protocol configured on this interface are deleted.

19.8.4 ipv6 vpn6-instance (upgrade-compatible command)

Function

The **ipv6 vpn6-instance** command creates an IPv6 VPN instance and displays the IPv6 VPN instance view.

The **undo ipv6 vpn6-instance** command deletes a specified IPv6 VPN instance.

By default, no IPv6 VPN instance exists.

Format

ipv6 vpn6-instance *vpn6-instance-name*

undo ipv6 vpn6-instance *vpn6-instance-name*

Parameters

Parameter	Description	Value
vpn6-instance-name	Specifies the name of an IPv6 VPN instance.	The name is a string of 1 to 31 case-sensitive characters without any spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After this command is run, an IPv6 VPN instance is created and the IPv6 VPN instance view is displayed.

19.8.5 link-alive (upgrade-compatible command)

Function

The **link-alive** command enables the link-alive function on a GRE tunnel.

The **undo link-alive** command disables the link-alive function on a GRE tunnel.

By default, the link-alive function is disabled on a GRE tunnel.

Format

link-alive [**period** *period*] [**retry-times** *retry-times*]

undo link-alive

Parameters

Parameter	Description	Value
period	Specifies the interval for sending link-alive packets.	The value is an integer that ranges from 1 to 32767, in seconds. The default value is 5.
retry-times *retry-times*	Specifies the tunnel-unreachable counter value.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The link-alive function takes effect on a GRE tunnel immediately after you run the **link-alive** command on the tunnel interface. After you run the **undo link-alive** command, the link-alive function immediately becomes invalid. The source end of a GRE tunnel periodically sends link-alive packets. The tunnel-unreachable counter increases by 1 every time a link-alive packet is sent. If the source end does not receive any response packet when the tunnel-unreachable counter value reaches *retry-times*, the source end considers the remote end unreachable.

Example

Enable the link-alive function on a GRE tunnel and retain the default parameter values.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] link-alive
```

Disable the link-alive function on a GRE tunnel.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo link-alive
```

Enable the link-alive function on a GRE tunnel. Set the interval for sending link-alive packets to 12 seconds and retain the default tunnel-unreachable counter value.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] link-alive period 12
```

Enable the link-alive function on a GRE tunnel. Set the interval for sending link-alive packets to 12 seconds and the tunnel-unreachable counter to 4.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] link-alive period 12 retry-times 4
```

19.8.6 snmp-agent trap enable feature-name l3vpn (upgrade-compatible command)

Function

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for the L3VPN module.

The **undo snmp-agent trap enable feature-name l3vpn** command disables the trap function for the L3VPN module.

By default, the trap function for the L3VPN module is disabled.

Format

snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_mid_exceed

undo snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_mid_exceed

Parameters

Parameter	Description	Value
trap-name	Enables the traps of L3VPN events of specified types.	-
l3vpn_mib_trap_mid_exceed	Enables the trap of the event indicating that the number of private route prefixes exceeds the middle threshold.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for L3VPN modules.

Example

Enable the trap of the event indicating that the number of private route prefixes exceeds the middle threshold in the system view.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_mid_exceed
```

19.8.7 snmp-agent trap enable l3vpn (upgrade-compatible command)

Function

The **snmp-agent trap enable l3vpn** command enables the device to send the L3VPN trap message.

The **undo snmp-agent trap enable l3vpn** command prohibits the device from sending the L3VPN trap message.

By default, the L3VPN trap message cannot be sent.

Format

snmp-agent trap enable l3vpn

undo snmp-agent trap enable l3vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Permit the device to send the L3VPN trap message.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable l3vpn
```

19.8.8 sa authentication-hex (upgrade-compatible command)

Function

The **sa authentication-hex** command sets an authentication in hexadecimal format or cipher text for Security Associations (SAs).

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } **plain** *hex-plain-key*

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-

Parameter	Description	Value
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa authentication-hex** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa authentication-hex** command.	-
plain	Indicates the plain text used for authentication.	-
hex-plain-key	Specifies the plain text key.	The value is in hexadecimal notation. ● If authentication algorithm Message Digest 5 (MD5) is used, the length of the key is 16 bytes. ● If authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used, the length of the key is 20 bytes. ● If authentication algorithm SHA2-256 is used, the length of the key is 32 bytes. **NOTE** The MD5 and SHA-1 authentication algorithms have security risks; therefore, you are advised to use SHA-256 preferentially.

Views

SA view

Default Level

3: Management level

Usage Guidelines

This command is upgrade compatible and can be executed during configuration recovery. Users cannot manually configure this command.

After the upgrade, this command is no longer supported, and it is replaced by the **sa authentication-hex** command.

19.8.9 sa encryption-hex (upgrade-compatible command)

Function

The **sa encryption-hex** command configures an encryption key for manual Security Association (SA) in hexadecimal format.

Format

sa encryption-hex { **inbound** | **outbound** } { **ah** | **esp** } **plain** *hex-plain-key*

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa encryption-hex** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa encryption-hex** command.	-
plain	Indicates the plaintext used for authentication.	-

Parameter	Description	Value
hex-plain-key	Specifies the plaintext key.	The value is in hexadecimal notation. ● If encryption algorithm Data Encryption Standard (DES) is used, the length of the key is 8 bytes. ● If encryption algorithm Triple Data Encryption Standard (3DES) is used, the length of the key is 24 bytes. ● If encryption algorithm Advanced Encryption Standard 128 (AES-128) is used, the length of the key is 16 bytes. ● If encryption algorithm AES-192 is used, the length of the key is 24 bytes. ● If encryption algorithm AES-256 is used, the length of the key is 32 bytes. **NOTE** The DES and 3DES encryption algorithms have security risks; therefore, you are advised to use AES-128, AES-192 or AES-256 preferentially.

Views

SA view

Default Level

3: Management level

Usage Guidelines

This command is upgrade compatible and can be executed during configuration recovery. Users cannot manually configure this command.

After the upgrade, this command is no longer supported, and it is replaced by the **sa encryption-hex** command.

19.8.10 sa string-key (upgrade-compatible command)

Function

The **sa string-key** command configures an authentication key in the string format.

Format

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } **plain** *string-plain-key*

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa string-key** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa string-key** command.	-
plain	Indicates the plaintext used for authentication.	-
string-plain-key	Specifies the plaintext key.	The value is a string of 1 to 127 case-sensitive characters.

Views

SA view

Default Level

3: Management level

Usage Guidelines

This command is upgrade compatible and can be executed during configuration recovery. Users cannot manually configure this command.

After the upgrade, this command is no longer supported, and it is replaced by the **sa string-key** command.

19.9 WLAN Compatible Commands

19.9.1 agc-threshold low

Function

The **agc-threshold low** command sets the receiver sensitivity threshold of an AP.

The **undo agc-threshold low** command restores the default receiver sensitivity threshold of an AP.

By default, the receiver sensitivity threshold of an AP is –128 dBm.

Format

agc-threshold low *low-threshold*

undo agc-threshold low

Parameters

Parameter	Description	Value
low-threshold	Specifies the receiver sensitivity threshold of an AP.	The value is an integer that ranges from –128 to –40, in dBm.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the configuration is restored, this command is restored to **rx-sensitivity** *threshold*.

19.9.2 anti-attack broadcast-flood blacklist disable (upgrade-compatible command)

Function

The **anti-attack broadcast-flood blacklist disable** command disables the broadcast flood blacklist function.

The **undo anti-attack broadcast-flood blacklist disable** command enables the broadcast flood blacklist function.

By default, the broadcast flood blacklist function is disabled.

Format

anti-attack broadcast-flood blacklist disable

undo anti-attack broadcast-flood blacklist disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the broadcast flood blacklist function is enabled, the device considers traffic with a rate higher than that specified in **anti-attack broadcast-flood sta-rate-threshold** *sta-rate-threshold* a broadcast flood attack and adds the STA to the blacklist.

Prerequisites

The broadcast flood detection function has been enabled using the **undo anti-attack broadcast-flood sta-rate-threshold** command.

19.9.3 anti-attack broadcast-flood blacklist enable (upgrade-compatible command)

Function

The **anti-attack broadcast-flood blacklist enable** command enables the broadcast flood blacklist function.

The **undo anti-attack broadcast-flood blacklist enable** command disables the broadcast flood blacklist function.

By default, the broadcast flood blacklist function is disabled.

Format

anti-attack broadcast-flood blacklist enable

undo anti-attack broadcast-flood blacklist enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.4 anti-attack broadcast-flood disable (upgrade-compatible command)

Function

The **anti-attack broadcast-flood disable** command disables the broadcast flood detection function.

The **undo anti-attack broadcast-flood disable** command enables the broadcast flood detection function.

By default, the broadcast flood detection function is enabled.

Format

anti-attack broadcast-flood disable

undo anti-attack broadcast-flood disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.5 anti-attack broadcast-flood sta-rate-threshold (upgrade-compatible command)

Function

The **anti-attack broadcast-flood sta-rate-threshold** command sets the broadcast flood threshold.

The **undo anti-attack broadcast-flood sta-rate-threshold** command restores the default broadcast flood threshold.

By default, the broadcast flood threshold is 10 pps.

Format

anti-attack broadcast-flood sta-rate-threshold *sta-rate-threshold*

undo anti-attack broadcast-flood sta-rate-threshold

Parameters

Parameter	Description	Value
sta-rate-threshold	Specifies the rate threshold of broadcast traffic from STAs.	The value is an integer that ranges from 5 to 5000, in pps.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.6 ap-location (upgrade-compatible command)

Function

ap-location command sets the latitude and longitude of an AP.

By default, no latitude or longitude is configured for an AP.

Format

ap-location longitude { **e** | **w** } *longitude-value* **latitude** { **s** | **n** } *latitude-value*

ap-location latitude { **s** | **n** } *latitude-value* **longitude** { **e** | **w** } *longitude-value*

Parameters

Parameter	Description	Value
longitude e *longitude-value*	Specifies the east longitude value of an AP.	The value supports two formats: degrees, minutes, and seconds (DMS) and decimal degrees (DD). ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the east longitude value of an AP can be set to **longitude e** 120-45-23 in DMS format and **longitude e** 120.756333333 in DD format.
longitude w *longitude-value*	Specifies the west longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the west longitude value of an AP can be set to **longitude w** 120-45-23 in DMS format and **longitude w** 120.756333333 in DD format.
latitude s *latitude-value*	Specifies the south longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the south longitude value of an AP can be set to **latitude s** 78-45-23 in DMS format and **latitude s** 78.756333333 in DD format.

Parameter	Description	Value
latitude n *latitude-value*	Specifies the north longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the north longitude value of an AP can be set to **latitude n** 78-45-23 in DMS format and **latitude n** 78.756333333 in DD format.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the longitude and latitude of an AP for easily locating it.

19.9.7 calibrate auto-channel-select disable (upgrade-compatible command)

Function

The **calibrate auto-channel-select disable** command disables automatic channel selection.

The **undo calibrate auto-channel-select disable** command enables automatic channel selection.

By default, automatic channel selection is enabled.

Format

calibrate auto-channel-select disable

undo calibrate auto-channel-select disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Two channel selection modes are available:

- Automatic mode (enabling automatic channel selection): An AP automatically selects a proper channel based on the WLAN radio environment, removing the need to specify channels manually.
- Fixed mode (disabling automatic channel selection): Channels must be manually specified.

The automatic mode (automatic channel selection) is recommended because you do not need to specify a channel for each radio. The fixed mode provides users with an alternative way when they want to specify channels by themselves or to avoid frequent channel adjustment (this may cause intermittent service interruption).

If an AP needs radio calibration, automatic channel selection must be enabled.

NOTE

When automatic channel selection is enabled, the manually configured channels do not take effect to ensure that the radio works in the optimal channel environment.

19.9.8 calibrate auto-txpower-select disable (upgrade-compatible command)

Function

The **calibrate auto-txpower-select disable** command disables automatic transmit power selection.

The **undo calibrate auto-txpower-select disable** command enables automatic transmit power selection.

By default, automatic transmit power selection is enabled.

Format

calibrate auto-txpower-select disable

undo calibrate auto-txpower-select disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Two power selection modes are available:

- Automatic mode (enabling automatic transmit power selection): An AP automatically selects or adjusts the transmit power based on the WLAN radio environment, removing the need to specify AP power manually.
- Fixed mode (disabling automatic transmit power selection): The transmit power must be manually specified.

If an AP needs radio calibration, automatic transmit power selection must be enabled.

19.9.9 calibrate error-rate-threshold (upgrade-compatible command)

Function

The **calibrate error-rate-threshold** command sets the retransmission rate threshold.

The **undo calibrate error-rate-threshold** command restores the default retransmission rate threshold.

By default, the retransmission rate threshold is 60%.

Format

calibrate error-rate-threshold *error-rate-threshold*

undo calibrate error-rate-threshold

Parameters

Parameter	Description	Value
error-rate-threshold	Specifies the retransmission rate threshold.	The value is an integer that ranges from 20 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

The retransmission rate is the ratio of retransmitted packets to all packets sent by a radio.

The retransmission rate threshold determines whether the radio environment is normal. When the retransmission rate of a radio reaches the threshold, the system considers that the radio environment deteriorates. When this occurs, the system may start radio calibration or take measures to avoid signal interference.

19.9.10 calibrate noise-threshold (upgrade-compatible command)

Function

The **calibrate noise-threshold** command specifies the noise floor threshold for triggering radio calibration.

The **undo calibrate noise-threshold** command restores the default noise floor threshold for triggering radio calibration.

The default noise floor threshold for triggering radio calibration is -75 dBm.

Format

calibrate noise-threshold *threshold*

undo calibrate noise-threshold

Parameters

Parameter	Description	Value
noise-threshold *threshold*	Specifies the noise floor threshold for triggering radio calibration.	The value is an integer that ranges from -95 to 0, in dBm.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The noise floor indicates the noise strength in the current environment. A high noise floor value will make noise drown out valid data, affecting user services.

The noise floor threshold for triggering radio calibration can be used to determine whether the environment noise is normal. When detecting a noise floor value higher than the threshold, an AP reports a high noise floor message to the AC. The AC then performs radio calibration to avoid channels with high noise floor values to improve user experience.

19.9.11 calibrate policy (upgrade-compatible command)

Function

The **calibrate policy** command creates a radio calibration policy.

The **undo calibrate policy** command deletes a radio calibration policy.

By default, no radio calibration policy is created.

Format

calibrate policy noise

undo calibrate policy noise

Parameters

Parameter	Description	Value
noise	Indicates the noise floor mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Noise floor policy: When the noise floor of APs is high due to special external interference, service experience may deteriorate. With this radio calibration policy, the device takes actions to avoid interference. When detecting that the noise floor of the current channel exceeds the threshold for three consecutive times, an AP notifies the AC of the high noise floor. The AC then allocates another channel to the AP and does not allocate the current channel to the AP in 30 minutes.

Prerequisites

The noise floor threshold for triggering radio calibration has been specified using the **calibrate noise-floor-threshold** *threshold* command.

19.9.12 contain-mode (upgrade-compatible command)

Function

The **contain-mode** command sets the wireless intrusion protection system (WIPS) mode.

The **undo contain-mode** command deletes the WIPS mode.

By default, no WIPS mode is set.

Format

contain-mode all

undo contain-mode all

Parameters

Parameter	Description	Value
all	Sets WIPS against all unauthorized devices.	-

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.13 dot11r private

Function

The **dot11r private** command enables the Huawei's proprietary 802.11r function.

The **undo dot11r private** command disables the Huawei's proprietary 802.11r function.

By default, Huawei's proprietary 802.11r is disabled.

Format

dot11r private

undo dot11r private

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to the characteristics of Wi-Fi and different behaviors of different terminals on the WLAN, the actual roaming experience for the terminals varies. The roaming experience for latency-sensitive services such as audio, video, and gaming cannot be guaranteed. Roaming optimization policies are different for terminals and APs and may conflict with each other. Therefore, simply optimization for terminals or APs cannot solve the problem. AirEngine series APs (except the AirEngine 5760-10) are optimized for Huawei terminals running EMUI 10.0 or later. After the Huawei's proprietary 802.11r function is enabled, APs can carry the interworking IE in Beacon and Probe Response frames and perform roaming negotiation with Huawei terminals based on the specified frame format and interaction action. This function implements mutual trust and interworking between devices and pipes, reduces resource overheads during roaming negotiation, and effectively improves roaming experience.

Precautions

- Security policies supported by 802.11r include open system, WPA2+PSK+AES, WPA2+PPSK+AES, and WPA2+802.1X+AES.
- The 802.11r and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r function has been configured, the PMF function cannot be configured.

Example

Enable the Huawei's proprietary 802.11r function.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name ssid1
[HUAWEI-wlan-ssid-prof-ssid1] dot11r private
```

19.9.14 frame-format (serial profile view) (upgrade-compatible command)

Function

The **frame-format** command configures the format for serial frames on an IoT card interface.

The **undo frame-format** command restores the configured format for serial frames to the default value.

By default, the frame format is **frame-start-stop**.

Format

frame-format { **fixed-length** | **frame-start-stop** }

undo frame-format

Parameters

Parameter	Description	Value
fixed-length	Specifies a fixed frame length.	-
frame-start-stop	Specifies the start and stop flags for frames.	-

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.15 frame-length (serial profile view) (upgrade-compatible command)

Function

The **frame-length** command configures the length for serial frames on an IoT card interface.

The **undo frame-length** command restores the configured length for serial frames to the default value.

By default, the frame length is 512 bytes.

Format

frame-length *frame-length-value*

undo frame-length

Parameters

Parameter	Description	Value
frame-length-value	- If the frame format adopts a fixed length, this parameter is used for framing. - If the frame format is set to frame-start-stop, this parameter specifies the maximum frame length used to verify the validity of framing.	The value is an integer that ranges from 1 to 280, in bytes.

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.16 frame-start (serial profile view) (upgrade-compatible command)

Function

The **frame-start** command configures the start flag byte for serial frames on an IoT card slot.

The **undo frame-start** command restores the configured start flag byte to the default value.

By default, the start flag byte is aa.

Format

frame-start *frame-start-value*

undo frame-start

Parameters

Parameter	Description	Value
frame-start-value	Specifies the start flag byte of a frame.	The value ranges from 0 to ff.

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.17 frame-stop (serial profile view) (upgrade-compatible command)

Function

The **frame-stop** command configures the stop flag byte for serial frames on an IoT card slot.

The **undo frame-stop** command restores the configured stop flag byte to the default value.

By default, the stop flag byte is 7e.

Format

frame-stop *frame-stop-value*

undo frame-stop

Parameters

Parameter	Description	Value
frame-stop-value	Specifies the stop flag byte of a frame.	The value ranges from 0 to ff.

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.18 gap-threshold (upgrade-compatible command)

Function

The **gap-threshold** command sets the load difference threshold for load balancing based on the number of users in a static load balancing group.

The **undo gap-threshold** command restores the default load difference threshold for load balancing based on the number of users in a static load balancing group.

By default, the load difference threshold of a static load balancing group is 20%.

Format

gap-threshold *gap-threshold-value*

undo gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold-value*	Specifies the load difference threshold for load balancing based on the number of users in a static load balancing group.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the number of users on radios.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

After the load difference threshold for load balancing based on the number of users is configured using the **gap-threshold** command, an AP implements load balancing based on the difference between the number of users on different radios. The load balancing algorithm is as follows:

The AC calculates the load percentage of each radio in a load balancing group using the formula: Load percentage of a radio = (Number of associated users on the radio/Maximum number of users allowed on the radio) x 100%. The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a user requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold. If the difference is smaller than the threshold, the AC allows the user to associate with the radio. If not, the AC rejects the association request of the user. If users continue to send association requests to the AP and the maximum number of times the AP rejects users' association requests for a static load balancing group, the AP allows user access.

19.9.19 sta-number gap-threshold (upgrade-compatible command)

Function

The **sta-number gap-threshold** command sets the load difference threshold for load balancing based on the number of users in a static load balancing group.

The **undo sta-number gap-threshold** command restores the default load difference threshold for load balancing based on the number of users in a static load balancing group.

By default, the load difference threshold of a static load balancing group is 20%.

Format

sta-number gap-threshold *gap-threshold-value*

undo sta-number gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold-value*	Specifies the load difference threshold for load balancing based on the number of users in a static load balancing group.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the number of users on radios.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

After the load difference threshold for load balancing based on the number of users is configured using the **sta-number gap-threshold** command, an AP implements load balancing based on the difference between the number of users on different radios.

19.9.20 learn-client-address disable (VAP profile view) (upgrade-compatible command)

Function

learn-client-address disable command disables STA address learning.

undo learn-client-address disable command disables STA address learning.

By default, STA address learning is enabled.

Format

learn-client-address disable

undo learn-client-address disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a STA associates with an AP that has STA address learning enabled and obtains an IP address, the AP automatically reports the STA IP address to the AC to maintain the STA' IP address and MAC address binding entry

Prerequisites

- You have disabled the DHCP trusted interface by running **undo dhcp trust port** in the VAP profile view.
- Before disabling STA address learning, run the **undo learn-client-address dhcp-strict** command to disable strict STA IP address learning through DHCP.

Precautions

If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.

19.9.21 parity (serial profile view) (upgrade-compatible command)

Function

The **parity** command configures the parity bit for serial data on an IoT card slot.

The **undo parity** command restores the configured parity bit to the default value.

By default, the parity bit is set to **none** on an IoT card slot.

Format

parity { **none** | **odd** | **even** | **mark** | **space** }

undo parity

Parameters

Parameter	Description	Value
none	Indicates no parity.	-
odd	Indicates odd parity.	-
even	Indicates even parity.	-
mark	Indicates mark parity.	-
space	Indicates space parity.	-

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.22 serial-profile (WLAN view) (upgrade-compatible command)

Function

The **serial-profile** command creates a serial profile and displays the serial profile view.

The **undo serial-profile** command deletes a serial profile.

By default, serial profile **preset-enjoyor-toeap** is bound to an IoT card interface.

Format

serial-profile name *profile-name*

undo serial-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a serial profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Specifies all serial profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.23 serial-profile (IoT card interface view) (upgrade-compatible command)

Function

The **serial-profile** command binds a serial profile to an AP or AP group.

The **undo serial-profile** command deletes the serial profile bound to an AP or AP group.

By default, serial profile **preset-enjoyor-toeap** is bound to an AP group, and no serial profile is bound to an AP.

Format

serial-profile *profile-name*

undo serial-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a serial profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").

Views

IoT card interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.24 smart-roam enable (upgrade-compatible command)

Function

The **smart-roam enable** command enables smart roaming.

The **undo smart-roam enable** command disables smart roaming.

By default, smart roaming is disabled.

Format

smart-roam enable

undo smart-roam enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a traditional WLAN, when a STA is farther from an AP, the access rate of the STA becomes lower but the STA still associates with the AP without reinitiating a connection with the AP or roaming to another AP. This degrades user experience. To prevent this situation, configure the smart roaming function. When detecting that the SNR or access rate of a STA is lower than the specified threshold, the AP sends a Disassociation packet to the STA so that the STA can reconnect or roam to another AP.

19.9.25 speed (serial profile view) (upgrade-compatible command)

Function

The **speed** command configures the baud rate for serial communications on an IoT card slot.

The **undo speed** command restores the configured baud rate to the default value.

By default, the baud rate is 115,200 bit/s.

Format

speed *speed-value*

undo speed

Parameters

Parameter	Description	Value
speed-value	Specifies the baud rate for serial communication on an IoT card slot.	The unit is bit/s and the value can be: ● 9600 bit/s ● 19200 bit/s ● 38400 bit/s ● 57600 bit/s ● 115200 bit/s

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.26 start-threshold (upgrade-compatible command)

Function

The **start-threshold** command sets the start threshold for load balancing based on the number of users in a static load balancing group.

The **undo start-threshold** command deletes the configured start threshold for load balancing based on the number of users in a static load balancing group.

By default, the start threshold for load balancing based on the number of users in a static load balancing group is 10.

Format

start-threshold *start-threshold-value*

undo start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold-value*	Specifies the start threshold for load balancing based on the number of users in a static load balancing group.	The value is an integer that ranges from 1 to 40.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to set the start threshold for load balancing based on the number of users in a static load balancing group. If the load on a radio does not reach the start threshold, the device does not implement load balancing control on access STAs.

19.9.27 sta-load-balance dynamic gap-threshold (upgrade-compatible command)

Function

The **sta-load-balance dynamic gap-threshold** command sets the load difference threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic gap-threshold** command restores the default load difference threshold for dynamic load balancing based on the number of users.

By default, the load difference threshold of a dynamic load balancing group is 20%.

Format

sta-load-balance dynamic gap-threshold *gap-threshold*

undo sta-load-balance dynamic gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the load difference threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a user requests to connect to an AP, the AP will count the total number of access users on all radios. If the total number of access users does not exceed the start threshold, the AP does not implement dynamic load balancing. The AP implements dynamic load balancing only when the total number of access users on all radios exceeds the start threshold.

In dynamic load balancing mode, an AC uses a load balancing algorithm to determine whether to allow a user to associate with a radio. The load balancing algorithm is as follows:

When implementing dynamic load balancing, the AC calculates the load percentage of each radio in a load balancing group using the formula: Load percentage of a radio = (Number of associated users on the radio/Maximum number of users allowed on the radio) x 100%. The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a user requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold. If the difference is smaller than the threshold, the AC allows the user to associate with the radio. If not, the AC rejects the association request of the user. If the user continues sending association requests to this AP, the AC allows the user to associate with the AP when the number of consecutive association attempts of the user exceeds the maximum number of rejection times.

19.9.28 sta-load-balance dynamic sta-number gap-threshold (upgrade-compatible command)

Function

The **sta-load-balance dynamic sta-number** command sets the load difference threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic sta-number gap-threshold** command restores the default load difference threshold for dynamic load balancing based on the number of users.

By default, the load difference threshold of a dynamic load balancing group is 20%.

Format

sta-load-balance dynamic sta-number gap-threshold *gap-threshold*

undo sta-load-balance dynamic sta-number gap-threshold

Parameters

Parameter	Description	Value
gap-threshold *gap-threshold*	Specifies the load difference threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a user requests to connect to an AP, the AP will count the total number of access users on all radios. If the total number of access users does not exceed the start threshold configured, the AP does not implement dynamic load balancing. The AP implements dynamic load balancing only when the total number of access users on all radios exceeds the start threshold.

In dynamic load balancing mode, an AC uses a load balancing algorithm to determine whether to allow a user to associate with a radio.

19.9.29 sta-load-balance dynamic start-threshold (upgrade-compatible command)

Function

The **sta-load-balance dynamic start-threshold** command sets the start threshold for dynamic load balancing based on the number of users.

The **undo sta-load-balance dynamic start-threshold** command restores the default start threshold for dynamic load balancing based on the number of users.

By default, the start threshold for dynamic load balancing based on the number of users is 10.

Format

sta-load-balance dynamic start-threshold *start-threshold*

undo sta-load-balance dynamic start-threshold

Parameters

Parameter	Description	Value
start-threshold *start-threshold*	Specifies the start threshold for dynamic load balancing based on the number of users.	The value is an integer that ranges from 1 to 40.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a user requests to connect to an AP, the AP counts the total number of access users on all radios. If the number of access users on the requested radio does not exceed the start threshold, the AP does not implement dynamic load balancing based on the number of users. The AP implements dynamic load balancing based on the number of users only after the number of access users exceeds the start threshold.

19.9.30 stopbits (serial profile view) (upgrade-compatible command)

Function

The **stopbits** command configures stop bits for serial data on an IoT card slot.

The **undo stopbits** command restores the configured stop bits to the default value.

The default stop bit is 1.

Format

stopbits { **1** | **2** }

undo stopbits

Parameters

Parameter	Description	Value
1	Specifies one stop bit.	-
2	Specifies two stop bits.	-

Views

Serial profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.31 traffic-filter (AP wired port profile view) (upgrade-compatible command)

Function

The **traffic-filter** command configures ACL-based IPv4 packet filtering on an AP's wired interface.

The **undo traffic-filter** command cancels ACL-based IPv4 packet filtering configuration on an AP's wired interface.

By default, ACL-based IPv4 packet filtering is not configured on an AP's wired interface.

Format

traffic-filter { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based IPv4 packet filtering in the inbound direction.	-
outbound	Configures ACL-based IPv4 packet filtering in the outbound direction.	-
acl	Filters IPv4 packets based on a specified ACL.	-
acl-number	Specifies an ACL number.	The ACL must exist. The value is an integer that ranges from 3000 to 3031.
name *acl-name*	Filters IPv4 packets based on a named ACL. *acl-name* indicates the ACL name.	The ACL name must exist. The value range is the same as that of the *acl-number* parameter.

Views

AP wired port profile view

Default Level

3: Management level

Usage Guidelines

Usage scenario

The rules for an AP's wired interface to filter IPv4 packets based on ACLs are as follows:

- If the action in the ACL rule is **deny**, the device discards IPv4 packets matching the rule.
- If the action in the ACL rule is **permit**, the device allows IPv4 packets matching the rule to pass through.
- If no rule is matched, IPv4 packets are allowed to pass through.

Prerequisites

An ACL rule has been created by running the **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }] or **acl name** *acl-name acl-number* [**match-order** { **auto** | **config** }] command.

Precautions

The **traffic-filter** command can reference an ACL with no rule configured. You can configure a rule for the ACL after running this command.

You can configure IPv4 packet filtering based on only one ACL in one direction. If a referenced ACL needs to be replaced, configure a new ACL to overwrite the original one.

19.9.32 traffic-filter (traffic profile view) (upgrade-compatible command)

Function

The **traffic-filter** command configures ACL-based IPv4 packet filtering in a traffic profile.

The **undo traffic-filter** command cancels configuration of ACL-based IPv4 packet filtering in a traffic profile.

By default, ACL-based IPv4 packet filtering is not configured in a traffic profile.

Format

traffic-filter { **inbound** | **outbound** } **acl** { *acl-number1* | *acl-number2* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based IPv4 packet filtering in the inbound direction.	-
outbound	Configures ACL-based IPv4 packet filtering in the outbound direction.	-

Parameter	Description	Value
acl	Filters IPv4 packets based on a specified ACL.	-
acl-number	Specifies an ACL number.	The ACL must exist. The value is an integer that ranges from 3000 to 3031 and from 6000 to 6031. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs
name *acl-name*	Filters IPv4 packets based on a named ACL. *acl-name* indicates the ACL name.	The ACL name must exist. The value range is the same as that of the *acl-number* parameter.

Views

Traffic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed in the traffic profile view, the device filters packets matching a specified ACL rule:

- If the action in the ACL rule is **deny**, the device discards IPv4 packets matching the rule.
- If the action in the ACL rule is **permit**, the device allows IPv4 packets matching the rule to pass through.
- If no rule is matched, IPv4 packets are allowed to pass through.

Prerequisites

An ACL rule has been created by running the **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }] or **acl name** *acl-name acl-number* [**match-order** { **auto** | **config** }] command.

Precautions

The **traffic-filter** command can reference an ACL with no rule configured. You can configure a rule for the ACL after running this command.

You can configure IPv4 packet filtering based on only one ACL in one direction. If a referenced ACL needs to be replaced, configure a new ACL to overwrite the original one.

19.9.33 traffic-optimize broadcast-suppression enable (upgrade-compatible command)

Function

The **traffic-optimize broadcast-suppression enable** command enables rate limit for broadcast and multicast packets packets on an AP.

The **undo traffic-optimize broadcast-suppression enable** command disables rate limit for broadcast and multicast packets packets on an AP.

By default, rate limit for broadcast and multicast packets packets is disabled on an AP.

Format

traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **other** } **enable**

undo traffic-optimize broadcast-suppression { **all** | **arp** | **igmp** | **nd** | **other** } **enable**

Parameters

Parameter	Description	Value
all	Enables rate limit for all broadcast and multicast packets packets.	-
arp	Enables rate limit for ARP broadcast packets.	-
igmp	Enables rate limit for IGMP multicast packets.	-
nd	Enables rate limit for ND broadcast packets.	-
other	Enables rate limit for broadcast packets other than ARP and ND broadcast packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.34 traffic-optimize broadcast-suppression disable (AP system profile view)(upgrade-compatible command)

Function

The **traffic-optimize broadcast-suppression disable** command disables rate limit for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression disable** command enables rate limit for broadcast and multicast packets on an AP.

By default, rate limit for broadcast and multicast packets is enabled on an AP.

Format

traffic-optimize broadcast-suppression other disable

undo traffic-optimize broadcast-suppression other disable

Parameters

Parameter	Description	Value
other	Disables rate limit for broadcast packets other than ARP and ND broadcast packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.35 traffic-optimize broadcast-suppression rate-threshold (AP system profile view) (upgrade-compatible command)

Function

The **traffic-optimize broadcast-suppression rate-threshold** command sets a rate threshold for broadcast and multicast packets on an AP.

The **undo traffic-optimize broadcast-suppression rate-threshold** command restores the default threshold of broadcast and multicast packets on an AP.

The default rate threshold for ARP broadcast packets, ND broadcast packets, IGMP multicast packets, and other types of broadcast packets is 256 pps.

Format

traffic-optimize broadcast-suppression other rate-threshold *threshold-value*

undo traffic-optimize broadcast-suppression other rate-threshold

Parameters

Parameter	Description	Value
other	Specifies broadcast packets other than ARP and ND broadcast packets.	-
rate-threshold *threshold-value*	Specifies a rate threshold.	The value is an integer that ranges from 64 to 1024, in pps. The default value is 256.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.9.36 vht mcs-map (upgrade-compatible command)

Function

The **vht mcs-map** command configures the maximum MCS value corresponding to a specific number of 802.11ac spatial streams in the 5G radio profile.

The **undo vht mcs-map** command restores the default maximum MCS value corresponding to a specific number of 802.11ac spatial streams in the 5G radio profile.

By default, the maximum MCS value of the 802.11 ac radios is 9 in the 5G radio profile.

Format

vht mcs-map { **nss** *nss-value* { **max-mcs** *max-mcs-value* } } & <2-3>

undo vht mcs-map

Parameters

Parameter	Description	Value
nss *nss-value*	Specifies the number of spatial streams.	The value is an integer ranging from 1 to 4.
max-mcs *max-mcs-value*	Specifies the maximum MCS value corresponding to a specific number of spatial streams.	The value is an integer ranging from 7 to 9.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rates of 802.11ac radios depend on the index value of Modulation and Coding Scheme (MCS). A larger MCS value indicates a higher transmission rate.

- If *nss-value* is equal to or larger than the actual number of spatial streams supported by an AP, the maximum MCS value corresponding to all spatial streams of the AP is *max-mcs-value*.
- If *nss-value* is smaller than the actual number of spatial streams supported by an AP, only the maximum MCS value of configured spatial streams is *max-*

mcs-value. The maximum MCS value of the other spatial streams does not take effect.

For example, if *nss-value* is 2, and the AP supports 3 spatial streams. Only the maximum MCS value of spatial stream 1 and spatial stream 2 is *max-mcs-value*, and that of spatial stream 3 does not take effect.

Precautions

This configuration applies only to STAs associated with an AP in 802.11ac mode but does not take effect on STAs associated with the AP in other modes.

19.9.37 sniffer enable (upgrade-compatible command)

Function

The **sniffer enable** command enables and configures the working mode of an AP's built-in Bluetooth module.

The **undo sniffer enable** command disables the configured working mode of an AP's built-in Bluetooth module.

By default, the Bluetooth function of an AP's built-in Bluetooth module is disabled.

Format

sniffer enable

undo sniffer enable

Parameters

None

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the Bluetooth monitoring function, the built-in Bluetooth module of an AP will scan and obtain information about surrounding BLE devices, and reports the obtained information such as MAC addresses, RSSIs, BLE broadcast frame contents, and battery power.

After the Bluetooth monitoring function is enabled, an AP obtains battery power of surrounding Bluetooth devices at WLAN service off-peak time, for example, 2:00 am of the system time. Precisely configure the system time of an AC to ensure that WLAN services are not affected when the AC obtains battery power of Bluetooth devices.

The Bluetooth broadcast and Bluetooth monitoring functions can be enabled simultaneously for an AP's built-in Bluetooth module. When the two functions are enabled simultaneously, the AP's built-in Bluetooth module is also monitored.

After you run the **undo sniffer enable** command to disable the BLE monitoring function, the AC will trigger an alarm indicating that BLE devices are offline.

Follow-up Procedure

After the Bluetooth monitoring function is enabled, you are advised to run the **ble monitoring-list** command to add Bluetooth devices to the monitoring list for easy management. When a Bluetooth device in the monitoring list is offline or has low battery power, an alarm is triggered on the AC accordingly. If a Bluetooth device is not in the monitoring list, no such alarm will be triggered on the AC.

19.9.38 broadcasting-content (upgrade-compatible command)

Function

The **broadcasting-content** command configures the content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

The **undo broadcasting-content** command restores the default content of a BLE broadcast frame sent by an AP's built-in Bluetooth module.

By default, the UUID, Major, and Minor fields in a BLE broadcast frame sent by an AP's built-in Bluetooth module are null, and the RSSI calibration value is -65 dBm.

NOTE

Only the AP4050DN-E supports the Bluetooth broadcast function.

Format

broadcasting-content { **uuid** *uuid-value* | **major** *major-value* | **minor** *minor-value* | **reference-rssi** *reference-rssi-value* }*

undo broadcasting-content

Parameters

Parameter	Description	Value
uuid *uuid-value*	Specifies the UUID field in a BLE broadcast frame. UUID is the universally unique identifier of a BLE device.	The value is a string of 1 to 16 characters. The default value is null.
major *major-value*	Specifies the Major field in a BLE broadcast frame. This field specifies a major group and is combined with the Minor field to define information about a BEL device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.

Parameter	Description	Value
minor *minor-value*	Specifies the Minor field in a BLE broadcast frame. This field specifies a minor group and is combined with the Major field to define information about a BEL device, for example, location of a BLE device.	The value is a string of 1 or 2 characters. The default value is null.
reference-rssi *reference-rssi-value*	Specifies the RSSI calibration value of a BLE device. RSSI calibration value indicates the RSSI value of a BLE device measured at a distance of 1 m. It is used to estimate the distance between the BLE device and Bluetooth terminals.	The value is an integer that ranges from -97 to -50, in dBm. The default value is -65 that is measured when the transmit power of an APs' built-in Bluetooth module is 0 dBm.

Views

BLE profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the broadcast function of an AP's built-in Bluetooth module using the **broadcaster enable** command, you can run the **broadcasting-content** command to configure the content of BLE broadcast frames sent by the module.

Precautions

The RSSI calibration value in a BLE broadcast frame is set based on the actual measurement result.

After changing the transmit power of a built-in Bluetooth module using the **tx-power (BLE profile view)** command, you need to remeasure and reconfigure the RSSI calibration value. Therefore, you are advised to run the **tx-power (BLE profile view)** command to configure the transmit power of a built-in Bluetooth module before configuring the RSSI calibration value.

19.9.39 radio-5g-profile (upgrade-compatible command)

Function

The **radio-5g-profile** command binds a 5G radio profile to a 5G radio.

The **undo radio-5g-profile** command unbinds a 5G radio profile from a 5G radio.

By default, no 5G radio profile is applied in the AP view and AP radio view, but the 5G radio profile **default** is applied to the AP group view and AP group radio view.

Format

radio-5g-profile *profile-name*

undo radio-5g-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 5G radio profile.	The 5G radio profile must exist.

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 5G radio profile, bind it to a 5G radio so that the 5G radio profile can take effect.

Precautions

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

19.9.40 vap-profile (upgrade-compatible command)

Function

The **vap-profile** command binds a VAP profile to a radio.

The **undo vap-profile** command unbinds a VAP profile from a radio.

By default, no VAP profile is bound to a radio.

Format

vap-profile *profile-name* **wlan** *wlan-id*

undo vap-profile *profile-name* **wlan** *wlan-id*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a VAP profile.	The VAP profile must exist.
wlan *wlan-id*	Specifies the WLAN ID of a VAP.	The value is an integer that ranges from 1 to 16.

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VAP profile, bind it to a radio so that the VAP profile can take effect.

Precautions

After a VAP profile is bound to a radio, parameter settings in the VAP profile apply to the radio using the profile.

19.9.41 learn-client-address enable (AP wired port profile view) (upgrade-compatible command)

Function

The **learn-client-address enable** command enables terminal address learning on an AP's wired interface.

The **undo learn-client-address enable** command disables terminal address learning on an AP's wired interface.

By default, terminal address learning is disabled on an AP's wired interface.

Format

learn-client-address enable

undo learn-client-address enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After terminal address learning is enabled on an AP's wired interface, if a wired terminal connected to the AP wired interface successfully obtains an IP address, the AP automatically reports the IP address of the terminal to the AC, helping to maintain the ARP binding entries of wired terminals.

Prerequisites

You have disabled the DHCP trusted interface by running **undo dhcp trust port** in the AP wired port profile view.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

The AP wired interfaces added to an Eth-trunk interface do not support this function.

19.9.42 radio-2g-profile (upgrade-compatible command)

Function

The **radio-2g-profile** command binds a 2G radio profile to a 2G radio.

The **undo radio-2g-profile** command unbinds a 2G radio profile from a 2G radio.

By default, no 2G radio profile is applied in the AP view and AP radio view, but the 2G radio profile **default** is applied to the AP group view and AP group radio view.

Format

radio-2g-profile *profile-name*

undo radio-2g-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 2G radio profile.	The 2G radio profile must exist.

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 2G radio profile, bind it to a 2G radio so that the 2G radio profile can take effect.

Precautions

After a 2G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 2G radios in the AP group or the 2G radio of the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

19.9.43 master controller (upgrade-compatible command)

Function

The **master controller** command displays the configuration view of the Master Controller.

Format

master controller

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform configurations on the Master Controller, run the **master controller** command to enter the configuration view of the Master Controller.

Prerequisite

Run the **master-controller enable** command to enable the Master Controller role.

19.9.44 mu-mimo enable (upgrade-compatible command)

Function

The **mu-mimo enable** command enables MU-MIMO.

The **undo mu-mimo enable** command disables MU-MIMO.

By default, the MU-MIMO function is disabled.

Format

mu-mimo enable

undo mu-mimo enable

Parameters

None

Views

SSID profile view, WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Carrier sense multiple access with collision avoidance (CSMA-CA) allows an air interface channel to be occupied only by one STA, and other STAs cannot communicate with the AP. After MU-MIMO is enabled, STAs supporting MU-MIMO can form an MU group to simultaneously receive downlink data from the same air interface channel, improving channel efficiency and overall downlink throughput.

19.9.45 mpp-active-reselection enable (upgrade-compatible command)

Function

The **mpp-active-reselection enable** command enables active MPP reselection.

The **undo mpp-active-reselection** command disables active MPP reselection.

By default, active MPP reselection is disabled.

Format

mpp-active-reselection enable

undo mpp-active-reselection

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After active MPP reselection is enabled on an MP, the MP evaluates MPPs of the same Mesh ID and on the same channel based on the signal strength of Mesh links, the number of link hops, and the number of Mesh links. If a more preferable MPP is available, the MP selects the MPP as its Mesh gateway.

By default, active MPP reselection is disabled, and an MP can only passively reselect MPPs. When the minimum RSSI of all Mesh links on the optimal route to the current MPP is lower than the RSSI threshold of a Mesh link, the MPP reselection process is triggered.

Precautions

This configuration is invalid for the MPP.

In train-to-ground communication scenarios, this configuration takes effect only on vehicle-mounted APs working in client mode but not those working in Mesh handover mode. This is because in Mesh handover mode, vehicle-mounted APs use the link handover algorithm to select the MPP.

Active MPP reselection will cause service loss. Configure the function according to actual needs.

19.10 Reliability Compatible Commands

19.10.1 BFD Compatible Commands

19.10.1.1 bfd bind peer-ipv6 (upgrade-compatible command)

Function

The **bfd bind peer-ipv6** command creates a BFD6 session to test an IPv6 link.

By default, no BFD6 session is created to test an IPv6 link.

Format

bfd *bfd-name* **bind peer-ipv6** *peer-ipv6* [**vpn6-instance** *vpn6-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*]

Parameters

Parameter	Description	Value
bfd-name	Specifies a BFD6 session name.	The value is a string of 1 to 15 characters, spaces not supported.
peer-ipv6 *peer-ipv6*	Specifies the peer IPv6 address that is to be bound to a BFD6 session.	-
vpn6-instance *vpn6-instance-name*	Specifies the name of the VPN instance that is bound to a BFD6 session. If no VPN instance is specified, the peer IP address is regarded as a public IP address.	The value is a string of 1 to 31 characters.
interface *interface-type interface-number*	Specifies the local Layer 3 interface that is bound to a BFD6 session.	-

Parameter	Description	Value
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets. Generally, you do not need to configure this parameter. If no source IPv6 address is specified, the device specifies one based on the following situations: ● During BFD for IPv6 negotiation, the device searches for the IPv6 address of an outbound interface that connects to the peer in the local routing table as the source IPv6 address before sending BFD packets. ● During BFD for IPv6 detection, the device sets the source IPv6 address to a fixed value. **NOTE** BFD works with unicast reverse path forwarding (URPF). When URPF checks the source IPv6 address in received packets, you must manually set the source IPv6 address for the BFD packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **bfd** *bfd-name* **bind peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*] command.

Example

Create a BFD6 session named **test** to test the single-hop link.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd test bind peer-ipv6 2001:db8:1::1 vpn6-instance vpn1 interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-test] discriminator local 1
[HUAWEI-bfd-session-test] discriminator remote 2
[HUAWEI-bfd-session-test] commit
```

19.10.1.2 display bfd statistics session (upgrade-compatible command)

Function

The **display bfd statistics session** command displays BFD statistics.

Format

display bfd statistics session peer-ipv6 *peer-ipv6* [{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*]

Parameters

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays statistics about a BFD6 session bound to a specified peer IPv6 address.	-
{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*	Displays statistics about a BFD6 session bound to a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **display bfd statistics session peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] command.

19.10.1.3 display bfd session (upgrade-compatible command)

Function

The **display bfd session** command displays information about BFD sessions.

Format

display bfd session peer-ipv6 *peer-ipv6* [{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*] [**verbose**]

Parameters

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays the configuration of a BFD6 session bound to a specified peer IPv6 address.	-
{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*	Displays information about a BFD6 session bound to a specified VPN instance.	The value must be an existing VPN instance name.
verbose	Displays detailed information about the BFD6 configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **display bfd session peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**verbose**] command.

19.10.1.4 display bfd configuration (upgrade-compatible command)

Function

The **display bfd configuration** command displays configurations of BFD sessions.

Format

display bfd configuration peer-ipv6 *peer-ipv6* [{ **vpn-instance** | **vpn6-instance** } *vpn6-instance-name*] [**verbose**]

Parameters

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays the configuration of a BFD6 session bound to a specified peer IPv6 address.	-

Parameter	Description	Value
{ **vpn-instance** | **vpn6-instance** } *vpn6-instance-name*	Displays the configuration of a BFD6 session bound to a specified VPN instance	The value must be an existing VPN instance name.
verbose	Displays detailed information about BFD6 configurations.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **display bfd configuration peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**verbose**] command.

19.10.1.5 snmp-agent trap enable bfd (upgrade-compatible command)

Function

The **snmp-agent trap enable bfd** command enables the trap function for the BFD module.

By default, the trap function is disabled for the BFD module.

Format

snmp-agent trap enable bfd

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **snmp-agent trap enable feature-name bfd** command in the system view.

19.10.2 DLDP Compatible Commands

19.10.2.1 snmp-agent trap enable dldp (upgrade-compatible command)

Function

The **snmp-agent trap enable dldp** command enables the trap function for the DLDP module.

By default, the trap function is disabled for the DLDP module.

Format

snmp-agent trap enable dldp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name dldp** command.

19.10.2.2 dldp authentication-mode md5-compatible (upgrade-compatible command)

Function

The **dldp authentication-mode md5-compatible** command configures MD5-compatible authentication.

By default, DLDP packets are not authenticated.

Format

dldp authentication-mode md5-compatible *md5-password*

Parameters

Parameter	Description	Value
md5-compatible *md5-password*	Uses MD5-compatible to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices. *md5-password* specifies the MD5-compatible authentication password. **NOTE** To ensure security, the password is saved in cipher text in the configuration file.	The value is a string of 1 to 16 case-sensitive characters in plain text without any question mark (?) and space. **NOTE** During the upgrade, the device is compatible with the cipher-text passwords with different lengths before the upgrade.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

When the device that uses MD5 authentication is upgraded from V200R001 or V200R002 to V200R008 or later, to ensure compatibility, upgrade the DLDP authentication mode to MD5-compatible.

Running the **dldp authentication-mode md5-compatible** command is equivalent to running the **dldp authentication-mode** command in the system view.

19.10.3 Ethernet OAM Compatible Commands

19.10.3.1 ma format (upgrade-compatible command)

Function

The **ma** command creates an MA in an MD and displays the MA view. If the MA already exists, this command displays the MA view.

Format

ma *ma-name* **format** { **icc-based** | **string** }

Parameters

Parameter	Description	Value
ma-name	Specifies the name of an MA. Names of MAs in an MD are unique.	The value is a string of characters without spaces, hyphen (-), or question mark (?). The total length of the names of the MA and MD must be within 44 case-sensitive characters.
icc-based	Specifies an ICC-based MA name carried in CCMs to be sent. ITU carrier codes (ICCs) are assigned to network operators or service providers and maintained by ITU-T Telecommunication Standardization Bureau (TSB) in compliance with ITU-T M.1400 Recommendation.	-
string	Specifies a string-based MA name carried in CCMs to be sent.	-

Views

MD view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **ma** *ma-name* [**format** { **icc-based** *iccbased-ma-format-name* | **string** *ma-format-name* }] command.

19.10.3.2 cfm md format (upgrade-compatible command)

Function

Using the **cfm md** command, you can create an MD and enter the MD view. If the MD exists, you can use this command to enter the MD view.

Format

cfm md *md-name* **format** { **dnsname-and-mdname** | **mac-address** | **md-name** } [**level** *level*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 characters, which are case sensitive. The characters, such as ?, -, and space are excluded. The name of an MD is used to identify the MD. Different MDs on a device cannot have the same name. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
dnsname-and-mdname	Indicates the MD name in the format that a DNS name is followed by an MD name.	-
mac-address	Indicates the MD name in the format that a MAC address is followed by an MD name.	-
md-name	Indicates that the MA ID field of the sent packet contains the MD name.	-
level *level*	Specifies the level of the MD.	The value is an integer ranging from 0 to 7. The greater the value, the higher the priority. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **cfm md** *md-name* [**format** { **no-md-name** | **dns** *dns-md-format-name* | **mac-address** *mac-md-format-name* | **string** *string-md-format-name* }] [**level** *level*] command.

19.10.3.3 delay-measure one-way continual receive (upgrade-compatible command)

Function

The **delay-measure one-way continual receive** command configures a remote device to receive DMMs to implement proactive one-way frame delay measurement.

By default, the remote device enabled with proactive one-way frame delay measurement in the maintenance association (MA) is not configured to receive DMMs.

Format

delay-measure one-way continual receive

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **delay-measure one-way continual receive mep** *mep-id* command.

19.10.3.4 delay-measure one-way receive (upgrade-compatible command)

Function

Using the **delay-measure one-way receive** command, you can configure the DM frame receiving function on the remote end of the local device enabled with one-way frame delay measurement.

By default, the DM frame receiving function is not configured for the remote end in an MA.

Format

delay-measure one-way receive

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **delay-measure one-way receive mep** *mep-id* [**peer-ip** *peer-ip* [**vc-id** *vc-id*]].

19.10.3.5 delay-measure two-way receive (upgrade-compatible command)

Function

Using the **delay-measure two-way receive** command, you can enable DM frame reception on the remote MEP to implement the two-way frame delay measurement.

By default, DM frame reception is not configured on the remote MEP in an MA.

Format

delay-measure two-way receive

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **delay-measure two-way receive mep** *mep-id* [**8021p** { *8021p-value* } &<1-3>] [**peer-ip** *peer-ip* [**vc-id** *vc-id*]] command.

19.10.3.6 efm threshold-event trigger error-shutdown (upgrade-compatible command)

Function

Using the **efm threshold-event trigger error-shutdown** command, you can enable the error-triggered shutdown function on an interface. After this function is enabled, the interface is shut down when the number of EFM errored frames or errored codes reaches the threshold.

By default, the error-triggered shutdown function is disabled on an interface.

Format

efm threshold-event trigger error-shutdown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **efm threshold-event trigger error-down** command.

19.10.3.7 efm trigger if-net (upgrade-compatible command)

Function

The **efm trigger if-net** command associates EFM with an interface.

Format

efm trigger if-net

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **efm trigger if-down** command.

19.10.3.8 oam-bind ingress interface egress cfm md ma (upgrade-compatible command)

Function

The **oam-bind ingress interface egress cfm md ma** command configures an interface to report faults to Ethernet CFM.

Format

oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?).

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?). The total length of the names of the MA and MD must be within 44 characters.

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, it is replaced by the **oam-bind ingress interface** *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down** command.

19.10.3.9 oam-bind ingress interface egress efm interface (upgrade-compatible command)

Function

The **oam-bind ingress interface egress efm interface** command enables an interface to report faults to EFM OAM.

Format

oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. - *interface-type1* specifies the interface type. - *interface-number1* specifies the interface number.	-

Parameter	Description	Value
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, it is replaced by the **oam-bind ingress interface** *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down** command.

19.10.3.10 snmp-agent trap enable efm (upgrade-compatible command)

Function

The **snmp-agent trap enable efm** command enables the trap function for the EFM module.

By default, the trap function is disabled for the EFM module.

Format

snmp-agent trap enable efm

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name efm** command.

19.10.3.11 snmp-agent trap enable eoam-1ag (upgrade-compatible command)

Function

The **snmp-agent trap enable eoam-1ag** command enables the trap function for the Eoam-1ag module.

By default, the trap function is disabled for the Eoam-1ag module.

Format

snmp-agent trap enable eoam-1ag

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name eoam-1ag** command.

19.10.3.12 snmp-agent trap enable test-packet (upgrade-compatible command)

Function

The **snmp-agent trap enable test-packet** command enables an Ethernet OAM module to send traps to the NMS.

By default, an Ethernet OAM module is enabled to send traps to the NMS.

Format

snmp-agent trap enable test-packet

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **snmp-agent trap enable feature-name efm** command.

19.11 User Access and Authentication Compatible Commands

19.11.1 AAA Compatible Commands

19.11.1.1 adminuser-priority (upgrade-compatible command)

Function

The **adminuser-priority** command configures a user as an administrator to log in to the device and sets the administrator level during login.

Format

adminuser-priority *level*

Parameters

Parameter	Description	Value
level	Specifies the level of an administrator.	The value is an integer ranging from 0 to 15. After logging in to the device, a user can run only the commands of the same level or lower levels.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **admin-user privilege level** *level* command.

19.11.1.2 hwtacacs-server shared-key (upgrade-compatible command)

Function

The **hwtacacs-server shared-key** command configures the shared key of an HWTACACS server.

The **undo hwtacacs-server shared-key** command deletes the shared key of an HWTACACS server.

By default, no shared key of an HWTACACS server is configured.

Format

hwtacacs-server shared-key simple *key-string*

undo hwtacacs-server shared-key

Parameters

Parameter	Description	Value
simple	Indicates the shared key in simple text.	-
key-string	Specifies the shared key of an HWTACACS server.	The value is a string of 1 to 255 characters in plain text and a string of 20 to 392 characters in cipher text.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **hwtacacs-server shared-key** [**cipher**] *key-string* command.

19.11.1.3 local-user (upgrade-compatible command)

Function

The **local-user** command creates a local user and sets parameters of the local user.

By default, a local user exists in the system. The privilege of the user is **15**, and service type is **http**. The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

local-user *user-name* **password** { *key-string* [**old-password** *password*] | **simple** *simple-string* } [**access-limit** *max-number* | **idle-timeout** *minutes* [*seconds*] | **state** { **block** | **active** }] *

Parameters

Parameter	Description	Value
user-name	Specifies the user name. If the user name contains a delimiter "@", the character before "@" is the user name and the character after "@" is the domain name. If the value does not contain "@", the entire character string represents the user name and the domain name is the default one.	The value is a string of 1 to 64 characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Parameter	Description	Value

		NOTE
		- During local authentication or authorization, run the **authentication-mode** { **local** | **local-case** } or **authorization-mode** { **local** | **local-case** } command to configure case sensitivity for user names. If the parameter is set to **local**, user names are case-insensitive. If the parameter is set to **local-case**, user names are case-sensitive.
		- Note the following when configuring case sensitivity for user names:
		  - Only the user name is case-sensitive and the domain name is case-insensitive.
		  - For user security purposes, you cannot configure multiple local users with the user names that differ only in uppercase or lowercase. For example, after configuring ABC, you cannot configure Abc or abc as the user name.
		  - When a device is upgraded from V200R011C10 or an earlier version to a version later than V200R011C10, all local user names in the original configuration file are saved in lowercase. When a configuration file that is manually configured or generated using the third-party tool is used for configuration restoration, local user names that differ only in uppercase or lowercase are considered as one user name and the first one among these local user

Parameter	Description	Value
password *key-string*	Specifies the password of a local user. It is recommended that you set the user password when creating a user.	The value is a string of 1 to 256 case-sensitive characters without spaces.
old-password *password*	Specifies the old password of a local user. **NOTE** This parameter cannot be automatically displayed through the question mark help function and must be entered completely. It should be configured by the network administrator on the NMS and delivered to the device. It is not recommended that you directly specify this parameter on the device.	The value is the password used by the local user for the current login.
password simple *simple-string*	Specifies the password of a local user. It is recommended that you set the user password when creating a user.	The value is a string of 1 to 256 case-sensitive characters without spaces.
access-limit *max-number*	Specifies the number of connections that can be created with a specified user name. If this parameter is not specified, the number of connections that can be established by a specified user is not limited.	The value is an integer that varies according to the types and number of devices.

Parameter	Description	Value
idle-timeout *minutes* [*seconds*]	Specifies the timeout period for disconnection of the user. - *minutes* is the period when the user interface is disconnected in minutes. - *seconds* is the period when the user interface is disconnected in seconds. If this parameter is not specified, the device uses the user level configured by the **idle-timeout** command in the user view. If *minutes* [*seconds*] is set to **0 0**, the idle disconnection function is disabled.	- *minutes*: the value is an integer ranging from 0 to 35791 minutes. - *seconds*: the value is an integer ranging from 0 to 59 seconds.
state { **active** | **block** }	Specifies the status of a local user. - **active** indicates that a local user is in active state. - **block** indicates that a local user is in blocking state. If a user has established a connection with the device, when the user is set in blocking state, the connection still takes effect but the device rejects subsequent authentication requests from the user. If this parameter is not specified, the status of a local user is active.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **local-user** *user-name* { **password** { **cipher** | **irreversible-cipher** } *password* [**old-password***old-password*] | **access-limit** *max-number* | **ftp-directory** *directory* | **idle-timeout** *minutes* [*seconds*] | **privilege level** *level* | **state** { **block** | **active** } } * command.

19.11.1.4 local-user level (upgrade-compatible command)

Function

The **local-user level** command sets the level of a local user.

Format

local-user *user-name* **level** *level*

Parameters

Parameter	Description	Value
user-name	Specifies the user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
level	Specifies the user level.	The value is an integer that ranges from 0 to 15. A larger value indicates a higher level of a user. After logging in to the device, a user can run only the commands of the same level or lower levels.

Views

AAA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **local-user** *user-name* **privilege level** *level* command.

19.11.1.5 radius-attribute encap optimize (upgrade-compatible command)

Function

The **radius-attribute encap optimize disable** command disables RADIUS attribute encapsulation optimization.

The **radius-attribute encap optimize enable** command enables RADIUS attribute encapsulation optimization.

By default, the RADIUS attribute encapsulation optimization function is enabled.

Format

radius-attribute encap optimize { **enable** | **disable** }

undo radius-attribute encap optimize disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.11.1.6 radius-server accounting (upgrade-compatible command)

Function

The **radius-server accounting** command configures the RADIUS accounting server.

The **undo radius-server accounting** command deletes the configuration.

By default, no RADIUS accounting server is configured.

Format

radius-server accounting *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * **secondary**

radius-server accounting *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * **secondary**

undo radius-server accounting secondary

undo radius-server accounting *ip-address port* **source** { **loopback** | **ip-address** *ip-address* } **secondary**

undo radius-server accounting *ipv6-address port* **source** { **loopback** | **ip-address** *ipv6-address* } **secondary**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of a RADIUS accounting server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS accounting server is bound to.	The vpn-instance must already exist.
source loopback *interface-number*	Specifies the number of a loopback interface.	The loopback interface must already exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
source ip-address *ipv6-address*	Specifies the source IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
weight *weight-value*	Specifies the weight of a RADIUS accounting server.	The value is an integer that ranges from 0 to 100.
secondary	Specifies the configured accounting server as the secondary accounting server. If you do not configure this parameter, it indicates that you configure the primary accounting server.	-

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server accounting** *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * or **radius-server accounting** *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * command.

19.11.1.7 radius-server authentication (upgrade-compatible command)

Function

The **radius-server authentication** command configures a RADIUS authentication server.

The **undo radius-server authentication** command deletes the configured RADIUS authentication server.

By default, no RADIUS authentication server is specified.

Format

radius-server authentication *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * **secondary**

radius-server authentication *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * **secondary**

undo radius-server authentication secondary

undo radius-server authentication *ipv4-address port* **source** { **loopback** | **ip-address** *ipv4-address* } **secondary**

undo radius-server authentication *ipv6-address port* **source** { **loopback** | **ip-address** *ipv6-address* } **secondary**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of a RADIUS authentication server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authentication server is bound to.	The value is a string of 1 to 31 case-sensitive characters without spaces.
source loopback *interface-number*	Specifies the IP address of the loopback interface taken as the source IP address. *interface-number* specifies the number of a loopback interface.	The value is an integer that ranges from 0 to 1023.
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.

Parameter	Description	Value
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
weight *weight-value*	Specifies the weight of a RADIUS authentication server.	The value is an integer that ranges from 0 to 100.
secondary	Specifies the configured authentication server as the secondary accounting server. If you do not configure this parameter, it indicates that you configure the primary authentication server.	-

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server authentication** *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * or **radius-server authentication** *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * command.

19.11.1.8 radius-server authorization (upgrade-compatible command)

Function

The **radius-server authorization** command configures the RADIUS authorization server.

The **undo radius-server authorization** command deletes the configured RADIUS authorization server.

By default, no RADIUS authorization server is configured.

Format

radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* | **shared-key** { *key-string* | **simple** *simple-string* } } * [**ack-reserved-interval** *interval*]

undo radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a RADIUS authorization server.	The value is a valid unicast address in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authorization server is bound to.	The value is a string of 1 to 31 case-sensitive characters without spaces.
server-group *group-name*	Specifies the name of a RADIUS group corresponding to a RADIUS server template.	The value is a string of 1 to 32 case-sensitive characters without spaces.
shared-key *key-string*	Specifies the shared key in cipher text.	The value is a string of 32 characters in cipher text, for example, %$%$m^NF$L^SO%2@^y$T`^1'|lcZ%$%$, or a string of 1 to 16 characters in plain text, for example, 1234567.
shared-key simple *simple-string*	Specifies the shared key in plain text.	The value is a string of 1 to 16 case-sensitive characters, without spaces. By default, the key is converted to cipher text.

Parameter	Description	Value
ack-reserved-interval *interval*	Specifies the duration for retaining a RADIUS authorization response packet.	The value is an integer that ranges from 0 to 300, in seconds. By default, the value is 0s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server authorization** command.

19.11.1.9 radius-server shared-key (upgrade-compatible command)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

By default, the password is in cipher text. The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

radius-server shared-key { *key-string* | **simple** *simple-string* }

Parameters

Parameter	Description	Value
key-string	Specifies a cipher text password.	The value is a case-sensitive character string of 1 to 256 without spaces, quotation mark ("), and question mark (?).

Parameter	Description	Value
simple *simple-string*	Specifies a simple text password.	The value is a string of 1 to 16 case-sensitive characters, without spaces.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server shared-key cipher** *key-string* command.

19.11.1.10 radius-server testuser (upgrade-compatible command)

Function

Using the **radius-server testuser** command, you can create a user account for automatic detection in the RADIUS server template.

Using the **undo radius-server testuser** command, you can delete a user account for automatic detection.

By default, a user account for automatic detection in the RADIUS server template is not created.

Format

radius-server testuser username *username* **password** *password*

undo radius-server testuser

Parameters

Parameter	Description	Value
username *username*	Specifies a user name used for automatic detection.	The value is a string of 1 to 64 characters without spaces. It is case insensitive.

Parameter	Description	Value
password *password*	Specifies the user password for automatic detection.	The value is a character string of 1 to 16 characters without spaces, single quotation marks and question marks. It is case sensitive. If it is in cipher text, the password is a string of 32 characters.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server testuser username** *username* **password cipher** *password* command.

19.11.1.11 radius-server test-user (upgrade-compatible command)

Function

Using the **radius-server test-user** command, you can create a user account for automatic detection in the RADIUS server template.

Using the **undo radius-server test-user** command, you can delete a user account for automatic detection.

By default, a user account for automatic detection in the RADIUS server template is not created.

Format

radius-server test-user *username password*

undo radius-server test-user

Parameters

Parameter	Description	Value
username	Specifies a user name used for automatic detection.	The value is a string of 1 to 64 characters without spaces. It is case insensitive.
password	Specifies the user password for automatic detection.	The value is a character string of 1 to 16 characters without spaces, single quotation marks and question marks. It is case sensitive. If it is in cipher text, the password is a string of 32 characters.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server testuser username** *username* **password cipher** *password* command.

19.11.1.12 radius-server test-user detect interval (upgrade-compatible command)

Function

The **radius-server test-user detect interval** command sets the interval for automatic user status detection.

Format

radius-server test-user detect interval *interval-time*

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for automatic user status detection.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server detect-server interval interval** *interval* command.

19.11.1.13 radius-server user-name domain-included force (upgrade-compatible command)

Function

The **radius-server user-name domain-included force** command configures the device encapsulate the domain name in the user name in RADIUS packets to be sent to a RADIUS server.

Format

radius-server user-name domain-included force

Parameters

None

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server user-name domain-included** command.

19.11.1.14 remote-aaa-user authen-fail (upgrade-compatible command)

Function

The **remote-aaa-user authen-fail** command enables the remote AAA authentication account locking function, and sets the authentication retry interval, maximum number of consecutive authentication failures, and account locking period.

The **undo remote-aaa-user authen-fail** command disables the remote AAA authentication account locking function.

By default, the remote AAA account locking function is enabled, authentication retry interval is 5 minutes, maximum number of consecutive authentication failures is 30, and account locking period is 5 minutes.

Format

remote-aaa-user authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo remote-aaa-user authen-fail

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the authentication retry interval.	The value is an integer that ranges from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the maximum number of consecutive authentication failures.	The value is an integer that ranges from 3 to 65535.
block-time *block-time*	Specifies the account locking period.	The value is an integer that ranges from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **access-user remote authen-fail** command and **administrator remote authen-fail** command.

19.11.2 NAC Compatible Commands

19.11.2.1 authentication arp handshake

Function

The **authentication arp handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication arp handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

Format

authentication arp handshake

undo authentication arp handshake

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication handshake** command.

19.11.2.2 authentication handshake (upgrade-compatible command)

Function

The **authentication handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

Format

authentication handshake

undo authentication handshake

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication handshake** command in the authentication profile view.

19.11.2.3 authentication event action authorize (upgrade-compatible command)

Function

The **authentication event action authorize** command configures the device to assign network access policies to users before the users are authenticated.

The **undo authentication event action authorize** command deletes the configured network access policies.

By default, no network access right is granted to users before the users are authenticated.

Format

authentication event pre-authen action authorize service-scheme *service-scheme*

undo authentication event pre-authen action authorize

authentication event { **authen-fail** | **authen-server-down** } **action authorize service-scheme** *service-scheme* [**response-fail**]

undo authentication event { **authen-fail** | **authen-server-down** } **action authorize**

Parameters

Parameter	Description	Value
pre-authen	Configures the device to assign network access policies to users when the users establish pre-connections with the device.	-
authen-fail	Configures the device to assign network access policies to users when the authentication server sends authentication failure packets to the device.	-
authen-server-down	Configures the device to assign network access policies to users when the authentication server is Down and thereby the users fail to be authenticated.	-
response-fail	Configures the device to send authentication failure packets to users after assigning network access policies to the users. If this parameter is not specified, the device by default sends authentication success packets to users and therefore the users cannot know the fact that they fail to be authenticated. To solve this problem, specify this parameter so that the device will send authentication failure packets for the users to know their authentication results.	-

Parameter	Description	Value
service-scheme *service-scheme*	Specifies the name of the service scheme based on which network access policies are assigned to users.	The value is a string of 1 to 32 case-sensitive characters without spaces and the following: \ / : < > | @ ' % * " ?

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event pre-authen action authorize service-scheme** *scheme-name* and **authentication event** { **authen-fail** | **authen-server-down** } **action authorize service-scheme** *service-scheme* [**response-fail**] commands in the authentication profile view.

19.11.2.4 authentication event authen-server-up action re-authen (upgrade-compatible command)

Function

The **authentication event authen-server-up action re-authen** command enables the device to re-authenticate users when the authentication server changes from Down to Up.

The **undo authentication event authen-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the authentication server changes from Down to Up.

Format

authentication event authen-server-up action re-authen

undo authentication event authen-server-up action re-authen

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event authen-server-up action re-authen** command in the authentication profile view.

19.11.2.5 authentication event client-no-response action authorize (upgrade-compatible command)

Function

The **authentication event client-no-response action authorize** command configures the device to assign network access policies to users before the users are authenticated.

The **undo authentication event client-no-response action authorize** command deletes the configured network access policies.

By default, no network access right is granted to users before the users are authenticated.

Format

authentication event client-no-response action authorize service-scheme *service-scheme*

undo authentication event client-no-response action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Specifies the name of the service scheme based on which network access policies are assigned to users.	The value is a string of 1 to 32 case-sensitive characters without spaces and the following: \ / : < > | @ ' % * " ?

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event client-no-response action authorize service-scheme** *service-scheme* command in the 802.1X access profile view.

19.11.2.6 authentication event portal-server-down action authorize (upgrade-compatible command)

Function

The **authentication event portal-server-down action authorize** command configures network access policies for users when the Portal server is Down.

The **undo authentication event portal-server-down action authorize** command deletes the configured network access policies.

By default, no network access policy is configured for users when the Portal server is Down.

Format

authentication event portal-server-down action authorize service-scheme *service-scheme*

undo authentication event portal-server-down action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Specifies the name of the service scheme based on which network access policies are assigned to users.	The value is a string of 1 to 32 case-sensitive characters without spaces and the following: \ / : < > | @ ' % * " ?

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event portal-server-down action authorize service-scheme** *service-scheme* command in the Portal access profile view.

19.11.2.7 authentication event portal-server-up action re-authen (upgrade-compatible command)

Function

The **authentication event portal-server-up action re-authen** command enables the device to re-authenticate users when the Portal server changes from Down to Up.

The **undo authentication event portal-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the Portal server changes from Down to Up.

Format

authentication event portal-server-up action re-authen

undo authentication event portal-server-up action re-authen

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event portal-server-up action re-authen** command in the Portal access profile view.

19.11.2.8 authentication timer arp handshake-period

Function

The **authentication timer arp handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer arp** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer arp handshake-period *handshake-period*

undo authentication timer arp

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer that ranges from 5 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer handshake-period** *handshake-period* command.

19.11.2.9 authentication timer handshake-period (upgrade-compatible command)

Function

The **authentication timer handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer handshake-period** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer handshake-period *handshake-period*

undo authentication timer handshake-period

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer that ranges from 5 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer handshake-period** *handshake-period* command in the authentication profile view.

19.11.2.10 authentication timer authen-fail-user-aging (upgrade-compatible command)

Function

The **authentication timer authen-fail-user-aging** command configures the aging time for entries of the users who fail to be authenticated.

The **undo authentication timer authen-fail-user-aging** command restores the default aging time for entries of the users who fail to be authenticated.

By default, the aging time for entries of the users who fail to be authenticated is 23 hours.

Format

authentication timer authen-fail-user-aging *aging-time*

undo authentication timer authen-fail-user-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer authen-fail-aging** *aging-time* command in the authentication profile view.

19.11.2.11 authentication timer pre-authen-user-aging (upgrade-compatible command)

Function

The **authentication timer pre-authen-user-aging** command configures the aging time for pre-connection user entries.

The **undo authentication timer pre-authen-user-aging** command restores the default aging time for pre-connection user entries.

By default, the aging time for pre-connection user entries is 23 hours.

Format

authentication timer pre-authen-user-aging *aging-time*

undo authentication timer pre-authen-user-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer pre-authen-aging** *aging-time* command in the authentication profile view.

19.11.2.12 authentication timer re-authen (upgrade-compatible command)

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail to be authenticated.

The **undo authentication timer re-authen** command restores the default setting.

By default, pre-connection users and users who fail to be authenticated are re-authenticated at an interval of 60 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* }

undo authentication timer re-authen { **pre-authen** | **authen-fail** }

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value is an integer that ranges from 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail to be authenticated.	The value is an integer that ranges from 30 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer re-authen** { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* } command in the authentication profile view.

19.11.2.13 authentication device-type voice authorize (upgrade-compatible command)

Function

The **authentication device-type voice authorize** command enables voice terminals to go online without authentication.

The **undo authentication device-type voice authorize** command disables voice terminals from going online without authentication.

By default, voice terminals are disabled from going online without authentication.

Format

authentication device-type voice authorize [**service-scheme** *scheme-name*]

undo authentication device-type voice authorize [**service-scheme**]

Parameters

Parameter	Description	Value
service-scheme	Assigns network access rights to voice terminals based on a specified service scheme.	-
scheme-name	Specifies the name of the service scheme based on which network access rights are assigned to voice terminals.	The value must be an existing service scheme name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication device-type voice authorize service-scheme** *scheme-name* command in the authentication profile view.

19.11.2.14 authentication free-rule (upgrade-compatible command)

Function

The **authentication free-rule** command configures the NAC authentication-free rule for users.

The **undo authentication free-rule** command restores the default configuration.

By default, no NAC authentication-free rule is configured.

Format

authentication free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } *

undo authentication free-rule { *rule-id* | **all** }

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of the NAC authentication-free rule.	The value is an integer of which the range depends on product models
destination	Specifies the destination network resources that the authentication-free users can access.	-
source	Specifies the source information of the authentication-free users.	-
any	Specifies any condition. When **any** is used together with different keywords, the effect of the command is different.	-
ip *ip-address*	Specifies the IP address in the rule. This parameter can specify the source or destination address depending on the keyword.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of an IP address. This parameter can specify the source or destination address mask depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the IP address mask. This parameter can specify the source or destination address mask depending on the keyword.	The value is in dotted decimal notation.
tcp destination-port *port*	Specifies the TCP destination port number.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
udp destination-port *port*	Specifies the UDP destination port number.	The value is an integer that ranges from 1 to 65535.
interface *interface-type interface-number*	Specifies the type and number of the source interface in the rule. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies the VLAN ID of the source packet in the rule.	The value is an integer that ranges from 1 to 4094.
all	Specifies all rules.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **free-rule** *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } * command in the authentication-free rule profile view.

19.11.2.15 authentication mode (upgrade-compatible command)

Function

The **authentication mode** command configures the user access mode.

The **undo authentication mode** command restores the default user access mode.

By default, the user access mode is **multi-authen**.

Format

authentication mode { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number*] }

undo authentication mode [**multi-authen max-user**]

Parameters

Parameter	Description	Value
single-terminal	Specifies the interface to allow only one user to go online.	-
single-voice-with-data	Specifies the interface to allow only one data user and one voice user to go online. This mode applies to the scenario in which a data user connects to a network through a voice terminal.	-
multi-share	Specifies the interface to allow multiple users to go online. In this mode, the device only authenticates the first user. If the first user can be authenticated, the subsequent users share the same network access rights with the first user. If the first user goes offline, other users are also offline.	-
multi-authen	Specifies the interface to allow multiple users to go online. In this mode, the device authenticates each access user. If users can be authenticated, the users have their individual network access rights. If a user goes offline, other users are not affected.	-
max-user *max-user-number*	Specifies the maximum number of access users on the interface in **multi-authen** mode.	The value is an integer that depends on device types.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication mode** { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number*] } command in the authentication profile view.

19.11.2.16 authentication (upgrade-compatible command)

Function

The **authentication** command enables NAC authentication.

The **undo authentication** command disables NAC authentication.

By default, NAC authentication is disabled.

Format

Layer 2 interface view:

authentication { { **dot1x** | **mac-authen** } * [**portal**] | **portal** }

undo authentication { **dot1x** | **mac-authen** | **portal** } *

VLANIF interface view:

authentication { **mac-authen** [**portal**] | **portal** }

undo authentication { **mac-authen** | **portal** } *

Layer 3 interface view:

authentication portal

undo authentication portal

Parameters

Parameter	Description	Value
dot1x	Enables 802.1X authentication.	-
mac-authen	Enables MAC address authentication.	-
portal	Enables Portal authentication.	-

Views

VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x-access-profile** *access-profile-name*, **mac-access-profile** *access-profile-name*, and **portal-access-profile** *access-profile-name* commands in the authentication profile view.

19.11.2.17 authentication single-access (upgrade-compatible command)

Function

The **authentication single-access** command enables the device to allow users to access in only one authentication mode.

The **undo authentication single-access** command restores the default setting.

By default, the device allows users to access in different authentication modes.

Format

authentication single-access

undo authentication single-access

Parameters

None

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication single-access** command in the authentication profile view.

19.11.2.18 authentication trigger-condition dhcp dhcp-option (upgrade-compatible command)

Function

The **authentication trigger-condition dhcp dhcp-option** command enables the device to send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

The **undo authentication trigger-condition dhcp dhcp-option** command restores the default configuration.

By default, the device does not send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

Format

authentication trigger-condition dhcp dhcp-option *option-code*

undo authentication trigger-condition dhcp dhcp-option *option-code*

Parameters

Parameter	Description	Value
option-code	Specifies the option that the device sends to the authentication server.	The value is fixed as 82.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication trigger-condition dhcp dhcp-option** *option-code* command in the mac access profile view.

19.11.2.19 authentication trigger-condition (802.1X authentication) (upgrade-compatible command)

Function

The **authentication trigger-condition** command configures the packet types that can trigger 802.1X authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP packets can trigger 802.1X authentication.

Format

authentication trigger-condition { **dhcp** | **arp** } *

undo authentication trigger-condition [**dhcp** | **arp**] *

Parameters

Parameter	Description	Value
dhcp	Triggers 802.1X authentication through DHCP packets.	-
arp	Triggers 802.1X authentication through ARP packets.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication trigger-condition** { **dhcp** | **arp** } * command in the 802.1X access profile view.

19.11.2.20 authentication trigger-condition (MAC address authentication) (upgrade-compatible command)

Function

The **authentication trigger-condition** command configures the packet types that can trigger MAC address authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger MAC address authentication.

Format

authentication trigger-condition { **dhcp** | **arp** | **dhcpv6** | **nd** } *

undo authentication trigger-condition [**dhcp** | **arp** | **dhcpv6** | **nd**] *

Parameters

Parameter	Description	Value
dhcp	Triggers MAC address authentication through DHCP packets.	-
arp	Triggers MAC address authentication through ARP packets.	-
dhcpv6	Triggers MAC address authentication through DHCPv6 packets.	-
nd	Triggers MAC address authentication through ND packets.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication trigger-condition** { **dhcp** | **arp** | **dhcpv6** | **nd** } * command in the mac access profile view.

19.11.2.21 domain (upgrade-compatible command)

Function

The **domain** command configures the default domain or force domain for users.

The **undo domain** command deletes the configured default domain or force domain.

By default, no default domain or force domain is configured for users.

Format

Layer 2 interface view:

domain name *domain-name* [**dot1x** | **mac-authen** | **portal**] [**force**]

undo domain name *domain-name* [**dot1x** | **mac-authen** | **portal**] [**force**]

VLANIF interface view:

domain name *domain-name* [**mac-authen** | **portal**] [**force**]

undo domain name *domain-name* [**mac-authen** | **portal**] [**force**]

Layer 3 interface view:

domain name *domain-name* [**portal**] [**force**]

undo domain name *domain-name* [**portal**] [**force**]

System view (for all access authentication users):

domain *domain-name* **force** [**mac-address** *mac-address* **mask** *mask*]

undo domain *domain-name* **force** [**mac-address** *mac-address*]

System view (only for MAC address authentication users):

domain *domain-name* **mac-authen force**

undo domain *domain-name* **mac-authen force**

domain name *domain-name* **mac-authen force** [**mac-address** *mac-address* **mask** *mask*]

undo domain name *domain-name* **mac-authen force** [**mac-address** *mac-address*]

Parameters

Parameter	Description	Value
name *domain-name*	Specifies the name of the default domain or force domain. If no user authentication mode is specified, the default domain or force domain takes effect for all access authentication users.	The value must be an existing domain name on the device.

Parameter	Description	Value
mac-address *mac-address* **mask** *mask*	Specifies the MAC address range within which the MAC address authentication users use the forcible domain. ● **mac-address** *mac-address*: user MAC addresses. ● **mask** *mask*: masks of the MAC addresses. **NOTE** You can specify a maximum of 16 MAC address ranges.	The MAC address and mask are both in the format of H-H-H, in which H is a 4-digit hexadecimal number.
mac-address *mac-address*	User MAC addresses.	The MAC address and mask are both in the format of H-H-H, in which H is a 4-digit hexadecimal number.
dot1x	Specifies 802.1X authentication as the user authentication mode.	-
mac-authen	Specifies MAC address authentication as the user authentication mode.	-
portal	Specifies Portal authentication as the user authentication mode.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **access-domain** *domain-name* [**dot1x** | **mac-authen** | **portal**]* [**force**] command in the authentication profile view.

19.11.2.22 dot1x authentication-method (upgrade-compatible command)

Function

The **dot1x authentication-method** command sets the authentication mode for 802.1X users.

The **undo dot1x authentication-method** command restores the default authentication mode for 802.1X users.

By default, the global 802.1X user authentication mode is CHAP authentication and the 802.1X user authentication mode on interfaces is the same as the mode globally configured.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the CHAP-based EAP termination authentication mode.	-
pap	Indicates the PAP-based EAP termination authentication mode.	-
eap	Indicates that the EAP relay mode.	-

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x authentication-method** { **chap** | **pap** | **eap** } command in the 802.1X access profile view.

19.11.2.23 dot1x eap-notify-packet (upgrade-compatible command)

Function

The **dot1x eap-notify-packet** command enables the device to send an EAP packet code number to users.

The **undo dot1x eap-notify-packet** command disables the device from sending an EAP packet code number to users.

By default, the device is disabled from sending an EAP packet code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies an EAP packet code number sent to users.	The value is an integer that ranges from 5 to 255. The default value is 255.
data-type *type-number*	Specifies the data type in EAP packets sent to users.	The value is an integer that ranges from 1 to 255. The default value is 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x eap-notify-packet eap-code** *code-number* **data-type** *type-number* command in the 802.1X access profile view.

19.11.2.24 dot1x reauthenticate (upgrade-compatible command)

Function

The **dot1x reauthenticate** command enables periodic 802.1X re-authentication on an interface.

The **undo dot1x reauthenticate** command disables periodic 802.1X re-authentication on an interface.

By default, periodic 802.1X re-authentication is disabled on an interface.

Format

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x reauthenticate** command in the 802.1X access profile view.

19.11.2.25 dot1x retry (upgrade-compatible command)

Function

The **dot1x retry** command sets the maximum number of times an authentication request is sent to an 802.1X user.

The **undo dot1x retry** command restores the default setting.

By default, the device sends an authentication request to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the maximum number of times an authentication request is sent to an 802.1X user. The default value is recommended.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x retry** *max-retry-value* command in the 802.1X access profile view.

19.11.2.26 dot1x timer reauthenticate-period (upgrade-compatible command)

Function

The **dot1x timer reauthenticate-period** command sets the re-authentication interval for 802.1X authentication users.

The **undo dot1x timer reauthenticate-period** command restores the default re-authentication interval.

By default, the re-authentication interval is 3600 seconds.

Format

dot1x timer reauthenticate-period *reauthenticate-period-value*

undo dot1x timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for 802.1X address authentication users.	The value is an integer that ranges from 60 to 7200, in seconds.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x timer reauthenticate-period** *reauthenticate-period-value* command in the802.1X access profile view.

19.11.2.27 dot1x timer (upgrade-compatible command)

Function

The **dot1x timer** command sets values of timers used in 802.1X authentication.

The **undo dot1x timer** command restores the default settings of timers used in 802.1X authentication.

By default, the values of timers used in 802.1X authentication are not set.

Format

dot1x timer client-timeout *client-timeout-value*

undo dot1x timer client-timeout

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the timeout interval of the authentication response from the client. For details, see **dot1x retry**.	The value is an integer that ranges from 1 to 120, in seconds. By default, the timeout interval of the authentication response from the client is 5 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x timer** command in the 802.1X access profile view.

19.11.2.28 dot1x trigger dhcp-binding (upgrade-compatible command)

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-connection phase.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x trigger dhcp-binding** command in the dot1x access profile view.

19.11.2.29 dot1x unicast-trigger (upgrade-compatible command)

Function

The **dot1x unicast-trigger** command enables 802.1X authentication triggered by unicast packets.

The **undo dot1x unicast-trigger** command disables 802.1X authentication triggered by unicast packets.

By default, 802.1X authentication triggered by unicast packets is disabled.

Format

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x unicast-trigger** command in the 802.1X access profile view.

19.11.2.30 mac-authen offline dhcp-release (upgrade-compatible command)

Function

The **mac-authen offline dhcp-release** command enables the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

The **undo mac-authen offline dhcp-release** command restores the default configuration.

By default, the device does not clear user entries when receiving DHCP Release packets from MAC address authentication users.

Format

In the system view:

mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen offline dhcp-release

undo mac-authen offline dhcp-release

Parameters

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface. • *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number2* and *interface-number1* together specify an interface range.	-

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen offline dhcp-release** command in the mac access profile view.

19.11.2.31 mac-authen permit mac-address (upgrade-compatible command)

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen permit mac-address** *mac-address* **mask** { *mask* | *mask-length* } command in the mac access profile view.

19.11.2.32 mac-authen reauthenticate dhcp-renew (upgrade-compatible command)

Function

The **mac-authen reauthenticate dhcp-renew** command enables the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

The **undo mac-authen reauthenticate dhcp-renew** command restores the default setting.

By default, the device does not re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Format

mac-authen reauthenticate dhcp-renew

undo mac-authen reauthenticate dhcp-renew

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen reauthenticate dhcp-renew** command in the mac access profile view.

19.11.2.33 mac-authen reauthenticate (upgrade-compatible command)

Function

The **mac-authen reauthenticate** command enables periodic MAC address re-authentication on a specified interface.

The **undo mac-authen reauthenticate** command disables periodic MAC address re-authentication on a specified interface.

By default, periodic MAC address re-authentication is enabled on a specified interface.

Format

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen reauthenticate** command in the mac access profile view.

19.11.2.34 mac-authen timer reauthenticate-period (upgrade-compatible command)

Function

The **mac-authen timer reauthenticate-period** command sets the re-authentication interval for MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default re-authentication interval.

By default, the re-authentication interval is 1800 seconds.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for MAC address authentication users.	The value is an integer that ranges from 60 to 7200, in seconds.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command in the mac access profile view.

19.11.2.35 mac-authen username (upgrade-compatible command)

Function

The **mac-authen username** command configures the user name format for MAC address authentication.

The **undo mac-authen username** restores the default user name format.

By default, the MAC address without hyphens (-) is used as the user name and password for MAC address authentication.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** | **without-hyphen** } [**password cipher** *password*]] | **dhcp-option** *option-code* { **circuit-id** | **remote-id** } **password cipher** *password* }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** | **without-hyphen** } [**password cipher** *password*]] | **dhcp-option** *option-code* [**password cipher** *password*]]

Parameters

Parameter	Description	Value
fixed *username*	Specifies the fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive that do not contain spaces and question marks (?).
password cipher *password*	Specifies the password displayed in cipher text for MAC address authentication. ● The user with a fixed name can log in without a password if no password is set, which is not recommended. ● When a MAC address is used as the user name, the MAC address can be used as the password if no password is set. When local authentication is specified in the AAA authentication scheme, you must set a password. ● If the DHCP option is used as the user name, you must set a password. **NOTE** If fixed user names are configured in the VLANIF interface view, Eth-Trunk interface view or Port group view, the password must be set. If a MAC address is configured as the user name in the Port group view, the password cannot be set.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 8 characters.

Parameter	Description	Value
macaddress	Specifies that the user name in MAC address authentication is the MAC address.	-
format	Specifies the format of the MAC address.	-
with-hyphen	Specifies that the MAC address with hyphens is used as the user name, for example, 0005-e01c-02e3.	-
without-hyphen	Specifies that the MAC address without hyphens is used as the user name, for example, 0005e01c02e3.	-
dhcp-option *option-code*	Specifies the name of the MAC address authentication user to a specified DHCP option. ● **circuit-id**: Specifies the circuit ID in the DHCP Option82 as the user name in MAC address authentication. ● **remote-id**: Specifies the remote ID in the DHCP Option82 as the user name in MAC address authentication. **NOTE** In VLANIF interface view, the parameter does not support.	The value is an integer. In the current version, the value is fixed as 82.

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen username** command in the mac access profile view.

19.11.2.36 portal auth-network (upgrade-compatible command)

Function

The **portal auth-network** command configures a source subnet for Portal authentication.

The **undo portal auth-network** command restores the default source subnet for Portal authentication.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies the IP address of the source subnet for Portal authentication.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 1 to 32.
mask-address	Specifies the mask of the source subnet for Portal authentication.	The value is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **portal auth-network** *network-address* { *mask-length* | *mask-address* } command in the Portal access profile view.

19.11.2.37 portal https-redirect enable (upgrade-compatible command)

Function

The **portal https-redirect enable** command enables HTTPS redirection of Portal authentication.

The **undo portal https-redirect enable** command disables HTTPS redirection of Portal authentication.

By default, HTTPS redirection is enabled for wireless Portal authentication users and disabled for wired Portal authentication users.

Format

portal https-redirect enable

undo portal https-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication https-redirect enable** command.

19.11.2.38 portal local-server anonymous (interface view) (upgrade-compatible command)

Function

The **portal local-server anonymous** command enables anonymous login for users in built-in Portal authentication.

The **undo portal local-server anonymous** command disables anonymous login for users in built-in Portal authentication.

By default, anonymous login for users in built-in Portal authentication is disabled.

Format

portal local-server anonymous

undo portal local-server anonymous

Parameters

None

Views

VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **portal local-server anonymous** command in the Portal access profile view.

19.11.2.39 portal local-server ad-image load (upgrade-compatible command)

Function

The **portal local-server ad-image load** command loads an advertisement image file to the built-in Portal server login page.

The **undo portal local-server ad-image load** command deletes the advertisement image file loaded to the built-in Portal server login page.

By default, no advertisement image file is loaded to the built-in Portal server login page.

Format

portal local-server ad-image load *ad-image-file*

undo portal local-server ad-image load

Parameters

Parameter	Description	Value
ad-image-file	Specifies the name of an advertisement image file to be loaded to the built-in Portal server login page. The size of the advertisement image file must be equal to or less than 256 KB. A file of 670 x 405 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' " ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a blank area on the login page of the default page package used by the built-in Portal server. Users can customize this area by loading an advertisement image file. When the login page needs to be customized based on special requirements, the administrator can upload the user-defined advertisement image file to the device and run the **portal local-server ad-image load** command. After the advertisement image file is loaded, the user-defined advertisement images are displayed on the built-in Portal server login page for authentication.

Prerequisites

The user-defined advertisement image file has been uploaded to the device.

Example

Load the advertisement image file **ad.png** to the built-in Portal server login page.

```
<HUAWEI> system-view
[HUAWEI] portal local-server ad-image load flash:/ad.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.11.2.40 portal local-server anonymous (Portal access profile view) (upgrade-compatible command)

Function

The **portal local-server anonymous** command enables the anonymous login function for users authenticated through the built-in Portal server.

The **undo portal local-server anonymous** command disables the anonymous login function for users authenticated through the built-in Portal server.

By default, the anonymous login function is disabled for users authenticated through the built-in Portal server.

Format

portal local-server anonymous [**redirect-url** *url*]

undo portal local-server anonymous [**redirect-url**]

Parameters

Parameter	Description	Value
redirect-url *url*	Specifies the redirect URL. The URL is generally used to push advertisement information.	The value is a string of 1 to 200 case-sensitive characters without spaces and question marks (?). If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In places such as airports, hotels, cafes, and public recreation places, the anonymous login function allows users to access the network without entering the user name and password, facilitating network service provisioning.

After the anonymous login function is enabled, users are redirected to the login page the first time they access a web page. To connect to the network, users only need to accept terms in the license agreement and click **Login**.

If the **redirect-url** *url* parameter is specified, the web page corresponding to the specified URL will be automatically displayed when anonymous login users access web pages for the first time. This function can be used for advertisement push and users are unaware of the anonymous login process, improving user experience.

Precautions

When anonymous login is configured, it is recommended that you set AAA authentication mode to none authentication.

Example

In the Portal access template **p1**, configure the anonymous login function for users authenticated through the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] portal local-server anonymous
```

19.11.2.41 portal local-server authentication-method (upgrade-compatible command)

Function

The **portal local-server authentication-method** command configures the authentication mode for Portal users on the built-in Portal server.

The **undo portal local-server authentication-method** command restores the default authentication mode for Portal users on the built-in Portal server.

By default, the built-in Portal server uses CHAP to authenticate Portal users.

Format

portal local-server authentication-method { **chap** | **pap** }

undo portal local-server authentication-method

Parameters

Parameter	Description	Value
chap	Indicates that the built-in Portal server uses CHAP to authenticate Portal users.	-
pap	Indicates that the built-in Portal server uses PAP to authenticate Portal users.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Password Authentication Protocol (PAP) is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.

Challenge Handshake Authentication Protocol (CHAP) is a three-way handshake authentication protocol. It transmits only user names using RADIUS packets, but does not transmit passwords. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

Prerequisites

The built-in Portal server function has been enabled globally using the **portal local-server** command.

Example

Configure the built-in Portal server to use PAP to authenticate Portal users.

```
<HUAWEI> system-view
[HUAWEI] portal local-server authentication-method pap
```

19.11.2.42 portal local-server background-color (upgrade-compatible command)

Function

The **portal local-server background-color** command configures the background color of the built-in Portal server login page.

The **undo portal local-server background-color** command cancels the background color configured for the built-in Portal server login page.

By default, no background color of the built-in Portal server login page is configured.

Format

portal local-server background-color *background-color-value*

undo portal local-server background-color

Parameters

Parameter	Description	Value
background-color-value	Specifies the background color of the built-in Portal server login page.	The value is a string that ranges from #000000 to #FFFFFF in the RGB format. The hexadecimal code is used to indicate the page color, and the format is always #DEFABC (A-F and 0-9).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users can customize the login page of the default page package used by the built-in Portal server. The administrator can configure the background color of the login page.

Example

Configure the user-defined background color of the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server background-color #AABBCC
```

19.11.2.43 portal local-server background-image load (upgrade-compatible command)

Function

The **portal local-server background-image load** command loads a background image file to the built-in Portal server login page.

The **undo portal local-server background-image load** command deletes the background image file loaded to the built-in Portal server login page.

By default, the device has two background images **default-image0** and **default-image1**. The built-in Portal server uses **default-image0** as the background image by default.

Format

portal local-server background-image load { *background-image-file* | **default-image1** }

undo portal local-server background-image load

Parameters

Parameter	Description	Value
background-image-file	Specifies the name of the background image file to be loaded to the built-in Portal server login page. The size of the background image file must be equal to or less than 512 KB. A file of 1366 x 768 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' " ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.
default-image1	Loads the background image **default-image1** to the built-in Portal server login page.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users can customize the login page of the default page package used by the built-in Portal server. Users can customize background images or select the default ones. When the background image of the login page needs to be customized based on special requirements, the administrator can upload the user-defined background image file to the device and run the **portal local-server background-image load** command. After the image is loaded, the user-defined background image file is displayed on the built-in Portal server login page for authentication.

Prerequisites

The user-defined background image has been uploaded to the device.

Example

Load the background image file **bg.png** to the built-in Portal server login page.

```
<HUAWEI> system-view
[HUAWEI] portal local-server background-image load flash:/bg.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.11.2.44 portal local-server enable (Portal access profile view) (upgrade-compatible command)

Function

The **portal local-server enable** command enables the built-in Portal server function in a Portal access profile.

The **undo portal local-server enable** command restores the default setting.

By default, the built-in Portal server function is disabled in a Portal access profile.

Format

portal local-server enable

undo portal local-server enable

Parameters

None

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Portal authentication, the device needs to provide the IP address of the Portal server. The device supports external and built-in Portal servers. When the built-in Portal server is required to authenticate users, enable the built-in Portal server function globally and then run the **portal local-server enable** command in the Portal access profile. Then the built-in Portal server can be used to authenticate the users who use the Portal access profile.

Prerequisites

The built-in Portal server function has been enabled globally using the **portal local-server** command.

Example

In the Portal access profile **p1**, enable the built-in Portal server function.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.1.1 24
[HUAWEI-LoopBack1] quit
[HUAWEI] portal local-server ip 10.1.1.1
[HUAWEI] ssl policy s1
[HUAWEI-ssl-policy-s1] quit
[HUAWEI] portal local-server https ssl-policy s1
[HUAWEI] portal-access-profile name p1
[HUAWEI-portal-access-profile-p1] portal local-server enable
```

19.11.2.45 portal local-server enable (upgrade-compatible command)

Function

The **portal local-server enable** command enables built-in Portal authentication on an interface.

The **undo portal local-server enable** command disables built-in Portal authentication on an interface.

By default, built-in Portal authentication is disabled on an interface.

Format

In the system view:

portal local-server enable interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo portal local-server enable interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

portal local-server enable

undo portal local-server enable

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Specifies the interface type and number. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with the external Portal server, the built-in Portal server is easy to use, cost-effective, and easy to maintain. After built-in Portal authentication is enabled, the external Portal server is not required. After the built-in Portal server function is enabled using the **portal local-server** command, built-in Portal authentication must be enabled on the interface using the **portal local-server enable** command to authenticate users on the interface.

Prerequisites

Portal authentication has been enabled globally using the **portal local-server** command.

Precautions

It is recommended that you enable built-in Portal authentication on a VLANIF interface. The VLANIF interface of a super-VLAN does not support built-in Portal authentication.

Built-in Portal authentication of Layer 3 interfaces cannot be configured using this command in the system view.

If 802.1X authentication, MAC address authentication, MAC address bypass authentication or built-in Portal authentication is enabled on a Layer 2 interface, this command cannot be executed on the VLANIF interface of a VLAN to which the Layer 2 interface is added.

The **portal local-server enable** command cannot be used together with the following commands on the same interface.

Command	Function
mac-vlan enable	Enables MAC address-based VLAN assignment on an interface.
ip-subnet-vlan enable	Enables IP subnet-based VLAN assignment on an interface.

Example

Enable built-in Portal authentication on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.1.1 24
[HUAWEI-LoopBack1] quit
[HUAWEI] portal local-server ip 10.1.1.1
[HUAWEI] ssl policy s1
[HUAWEI-ssl-policy-s1] pki-realm default
[HUAWEI-ssl-policy-s1] quit
[HUAWEI] http secure-server ssl-policy s1
[HUAWEI] portal local-server https ssl-policy s1 port 1025
[HUAWEI] vlan batch 10
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] portal local-server enable
```

19.11.2.46 portal local-server ip (upgrade-compatible command)

Function

The **portal local-server ip** command configures an IP address for the built-in Portal server.

The **undo portal local-server ip** command deletes an IP address of the built-in Portal server.

By default, no IP address is configured for the built-in Portal server.

Format

portal local-server ip *ip-address*

undo portal local-server ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the built-in Portal server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device is used as a built-in Portal server, you can run the **portal local-server ip** command to configure an IP address for the built-in Portal server. Users are then redirected to the Portal server if they enter URLs that are not located in the free IP subnet.

NOTE

- The IP address assigned to the built-in Portal server must have a reachable route to the user.
- It is recommended that a loopback interface address be assigned to the built-in Portal server because the loopback interface is stable. Additionally, packets destined for loopback interfaces are not sent to other interfaces on the network; therefore, system performance is not deteriorated even if many users request to go online.
- After users go online through the built-in Portal server, if the interface address or interface (non-physical interface) matching the built-in Portal server's IP address is deleted, online users cannot go offline and offline users cannot go online. Therefore, exercise caution when you delete the interface address or interface.

Example

Assign the IP address 10.1.1.1 to the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.1.1 24
[HUAWEI-LoopBack1] quit
[HUAWEI] portal local-server ip 10.1.1.1
```

19.11.2.47 portal local-server keep-alive (upgrade-compatible command)

Function

The **portal local-server keep-alive** command configures the heartbeat detection interval and mode of the built-in Portal server.

The **undo portal local-server keep-alive** command cancels the configured heartbeat detection interval and mode of the built-in Portal server.

By default, the heartbeat detection function of the built-in Portal server is not configured.

Format

portal local-server keep-alive interval *interval-value* [**auto**]

undo portal local-server keep-alive

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the heartbeat detection interval of the built-in Portal server.	The value is an integer that ranges from 30 to 7200, in seconds.
auto	Specifies the automatic detection mode. If this parameter is not configured, the forcible detection mode is specified.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user closes the browser or an exception occurs, the device can detect the user's online state to determine whether to make the user go offline. The administrator can configure the heartbeat detection function of the built-in Portal server. If the device does not receive a heartbeat packet from the client within a specified period, the user is specified to go offline. The heartbeat detection mode of the built-in Portal server can be either of the following modes:

- Forcible detection mode: This mode is valid for all users. If the device does not receive a heartbeat packet from a user within a specified period, the device specifies the user to go offline.
- Automatic detection mode: The device checks whether the client browser supports the heartbeat program. If yes, the forcible detection mode is used for the user; if no, the device does not detect the user. You are advised to configure this mode to prevent users from going offline because the browser does not support the heartbeat program.

NOTE

Currently, the heartbeat program is supported by Internet Explorer 8, FireFox 3.5.2, Chrome 28.0.1500.72, and Opera 12.00 on Windows 7. A Java program must be installed and configured on the operating system.

Browsers using Java1.7 and later versions do not support the heartbeat program.

Precautions

When the forcible detection mode is configured, the device specifies users to go offline to prevent from failing to receive heartbeat packets for a long time during network congestion. In this scenario, the heartbeat detection interval must be increased.

If you run this command multiple times in the same view, only the latest configuration takes effect.

Example

Configure the automatic detection function of the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server keep-alive interval 60 auto
```

19.11.2.48 portal local-server load (upgrade-compatible command)

Function

The **portal local-server load** command loads a page file package to the built-in Portal server.

The **undo portal local-server load** command restores the default configuration.

By default, the built-in Portal server loads the default page file package **portalpage.zip**.

Format

portal local-server load *string*

undo portal local-server load

Parameters

Parameter	Description	Value
string	Specifies the name of the page file package to be loaded to the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' " ● *filename*: indicates the file name. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customized page file packages can be loaded to the built-in Portal server.

Prerequisites

The page file (.zip) has been uploaded from the PC to the device storage media.

Precautions

The default page file package can be modified but cannot be deleted. If it is deleted, the built-in Portal server fails to load the pages after startup.

This function is used by technical support personnel to develop limited page customization based on customer requirements and does not apply to customization by customers themselves.

Example

Load the page file **portalpage_01.zip** on the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server load portalpage_01.zip
Warning: Portal local server has been enabled, and this operation will affect online user, continue?[Y/N]:y
```

19.11.2.49 portal local-server logo load (upgrade-compatible command)

Function

The **portal local-server logo load** command loads a logo file to the built-in Portal server login page.

The **undo portal local-server logo load** command deletes the logo file loaded to the built-in Portal server login page.

By default, no logo file is loaded to the built-in Portal server login page.

Format

portal local-server logo load *logo-file*

undo portal local-server logo load

Parameters

Parameter	Description	Value
logo-file	Specifies the name of the logo file to be loaded to the built-in Portal server login page. The size of the logo file must be equal to or less than 128 KB. A file of 591 x 80 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' " ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a blank area on the login page of the default page package used by the built-in Portal server. Users can customize this area by loading a logo file. When the login page needs to be customized based on special requirements, the administrator can upload the user-defined logo file to the device and run the **portal local-server logo load** command. After the logo file is loaded, the user-defined logo is displayed on the built-in Portal server login page for authentication.

Prerequisites

The user-defined logo file has been uploaded to the device.

Example

Load the logo file **logo.png** to the built-in Portal server login page.

```
<HUAWEI> system-view
[HUAWEI] portal local-server logo load flash:/logo.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.11.2.50 portal local-server (upgrade-compatible command)

Function

The **portal local-server** command enables the built-in Portal server function.

The **undo portal local-server** command disables the built-in Portal server function.

By default, the built-in Portal server function is disabled.

Format

portal local-server https ssl-policy *policy-name* [**port** *port-num*]

undo portal local-server https

Parameters

Parameter	Description	Value
https	Configures the built-in Portal server to exchange authentication messages with users using the Hypertext Transfer Protocol Secure (HTTPS) protocol.	-
ssl-policy *policy-name*	Specifies the Secure Sockets Layer (SSL) policy used by the built-in Portal server.	The value must be the name of an existing SSL policy.
port *port-num*	Specifies the TCP port number used. If you do not specify a port number, the default port number is used.	The value can be 443 or any integer in the range of 1025 to 55535. By default, the port number is 443.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with an external Portal server, a built-in Portal server is easy to use, cost-effective, and easy to maintain. After a built-in Portal server is configured, Portal authentication can be implemented for users without an external Portal server. When using the **portal local-server** command to enable the built-in Portal server function, configure the built-in Portal server to exchange authentication messages with users using the HTTPS protocol. HTTPS is a secure extension of HTTP and uses the SSL protocol to guarantee secure communication. To enable the built-in Portal server to exchange authentication messages using HTTPS, you need to configure an SSL policy and load a digital certificate to the server.

Prerequisites

- The IP address of the built-in Portal server has been configured using the **portal local-server ip** command.
- An SSL policy has been configured using the **ssl policy** *policy-name* command in the system view, and a certificate has been loaded using the **certificate load** command in the SSL policy view.
- You have obtained a digital certificate for the SSL policy from an authorized certificate authority.

Precautions

When there are Portal authentication users online, you cannot disable the built-in Portal server function or change the SSL policy for the built-in Portal server.

Example

Enable the built-in Portal server function and configure the server to use the SSL policy **s1**.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.1.1 24
[HUAWEI-LoopBack1] quit
[HUAWEI] portal local-server ip 10.1.1.1
[HUAWEI] ssl policy s1
[HUAWEI-ssl-policy-s1] quit
[HUAWEI] portal local-server https ssl-policy s1
```

19.11.2.51 portal local-server page-text load (upgrade-compatible command)

Function

The **portal local-server page-text load** command loads the use instruction page file of the built-in Portal server.

The **undo portal local-server page-text load** command deletes the loaded use instruction page file of the built-in Portal server.

By default, no use instruction page file of the built-in Portal server is loaded.

Format

portal local-server page-text load *string*

undo portal local-server page-text load

Parameters

Parameter	Description	Value
string	Specifies the use instruction page file of the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [drive] [path] filename. - **drive** indicates the storage device name. - **path** indicates the directory or sub-directory. The directory name cannot contain the following characters: ~ * / \ : ' " - **filename** indicates the file name. The file name extension must be .txt or .html. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to customize the use instruction page, you can upload the customized use instruction page file to the device, and run this command to load the file. After the file is loaded, the hyperlink **Instruction for Use** is generated on the login page of the built-in Portal server, and users can click the hyperlink to access the use instruction page.

Prerequisite

The page file to be loaded has been uploaded to the device.

Precautions

When the to-be-loaded page is customized, the page length and width are fixed. After adjusting the page, the administrator must upload and load the modified page again.

Currently, only Chinese or English page files can be loaded on the device.

Example

Load the use instruction page file **page.html** to the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server page-text load flash:/page.html
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.11.2.52 portal local-server policy-text load (upgrade-compatible command)

Function

The **portal local-server policy-text load** command loads a disclaimer page file to the built-in Portal server.

The **undo portal local-server policy-text load** command deletes the loaded disclaimer page file.

By default, no disclaimer page file is loaded to the built-in Portal server.

Format

portal local-server policy-text load *string*

undo portal local-server policy-text load

Parameters

Parameter	Description	Value
string	Specifies the name of the disclaimer page file to be loaded to the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' " ● *filename*: indicates the file name. The file name extension must be .txt or .html. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To customize a disclaimer page, upload the disclaimer page file to the device and run this command to load the file. After the file is loaded, the hyperlink **Disclaimer** will be displayed on the login page. You can click the link to visit the disclaimer page.

Prerequisite

The disclaimer page file to be loaded has been uploaded to the device.

Precautions

Currently, only Chinese and English disclaimer page files can be loaded on the device.

Example

Load the disclaimer page file **policy.html** to the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server policy-text load policy.html
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.11.2.53 portal local-server timer session-timeout (upgrade-compatible command)

Function

The **portal local-server timer session-timeout** command configures the session timeout interval for built-in Portal authentication users.

The **undo portal local-server timer session-timeout** command restores the default session timeout interval for built-in Portal authentication users.

By default, the session timeout interval is 8 hours for built-in Portal authentication users.

Format

portal local-server timer session-timeout *interval*

undo portal local-server timer session-timeout

Parameters

Parameter	Description	Value
interval	Specifies the session timeout interval for built-in Portal authentication users.	The value is an integer that ranges from 1 to 720, in hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

When built-in Portal authentication is used for users and the device functions as a built-in Portal server, you can configure the session timeout interval for the users.

The users are disconnected after the specified session timeout interval. To connect to the network again, the users need to be re-authenticated.

Precautions

The session timeout interval for built-in Portal authentication users is calculated based on the device time. For example, if the session timeout interval is 6 hours and the device time is 2014-09-01 02:00:00 when a user was connected, the user should be disconnected at 2014-09-01 08:00:00. Therefore, ensure that the device time and time zone are correct after the session timeout interval is configured for users. If the device time is incorrect, users may fail to be connected or disconnected properly. You can run the **display clock** command to check the device time and the time zone.

Example

Set the session timeout interval to 10 hours for built-in Portal authentication users.

```
<HUAWEI> system-view
[HUAWEI] portal local-server timer session-timeout 10
```

19.11.2.54 portal local-server syslog-limit enable (upgrade-compatible command)

Function

The **portal local-server syslog-limit enable** command enables the log suppression function for users authenticated through the built-in Portal server.

The **undo portal local-server syslog-limit enable** command disables the log suppression function for users authenticated through the built-in Portal server.

By default, the log suppression function is enabled for users authenticated through the built-in Portal server.

Format

portal local-server syslog-limit enable

undo portal local-server syslog-limit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device generates logs when users authenticated through the built-in Portal server fail to go online or offline. If a user fails to go online or offline, the user attempts to go online or offline repeatedly, and the device generates a large number of logs within a short time. This results in a high failure rate in the statistics and degrades the system performance. You can run the **portal local-server syslog-limit enable** command to enable the log suppression function for users authenticated through the built-in Portal server. The device then only generates one log if a user fails to go online or offline within a suppression period (configured using the **portal local-server syslog-limit period** command).

Example

Enable the log suppression function for users authenticated through the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server syslog-limit enable
```

19.11.2.55 portal local-server syslog-limit period (upgrade-compatible command)

Function

The **portal local-server syslog-limit period** command configures the log suppression period for users authenticated through the built-in Portal server.

The **undo portal local-server syslog-limit period** command restores the default log suppression period.

By default, the log suppression period is 300 seconds for users authenticated through the built-in Portal server.

Format

portal local-server syslog-limit period *value*

undo portal local-server syslog-limit period

Parameters

Parameter	Description	Value
value	Specifies the log suppression period for users authenticated through the built-in Portal server.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device generates logs when users authenticated through the built-in Portal server fail to go online or offline. If a user fails to go online or offline, the user attempts to go online or offline repeatedly, and the device generates a large number of logs within a short time. This results in a high failure rate in the statistics and degrades the system performance. You can enable the log suppression function (configured using the **portal local-server syslog-limit enable** command) for users authenticated through the built-in Portal server. The device then only generates one log if a user fails to go online or offline within a suppression period.

Example

Set the log suppression period to 1000 seconds for users authenticated through the built-in Portal server.

```
<HUAWEI> system-view
[HUAWEI] portal local-server syslog-limit period 1000
```

19.11.2.56 portal timer offline-detect (upgrade-compatible command)

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **portal timer offline-detect** *time-length* command in the Portal access profile view.

19.11.2.57 url-parameter

Function

The **url-parameter** command sets parameters in a URL.

The **undo url-parameter** command deletes parameters in a URL.

By default, a URL does not carry parameters.

Format

url-parameter { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac* }*

undo url-parameter

NOTE

The command is only supported by the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

Parameters

Parameter	Description	Value
ac-ip *ac-ip-value*	Specifies the IP address of the ac carried in the URL and sets the parameter name displayed in the URL. In the wireless access scenario, the value of **ac-ip** carried in the URL is the CAPWAP gateway address.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
ac-mac *ac-mac-value*	Specifies the MAC address of the ac carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces or Chinese characters. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade. After the upgrade, this command is no longer supported, and it is replaced by the following command in the URL template view:

url-parameter { **device-ip** *device-ip-value* | **device-mac** *device-mac* }*

19.11.2.58 url (URL template view) (upgrade-compatible command)

Function

The **url** command configures the redirect URL or pushed URL.

The **undo url** command cancels the redirect URL or pushed URL.

By default, no redirect URL or pushed URL is configured.

Format

url [**ssid** *ssid*] [**push-only** | **redirect-only**] *url-string*

Parameters

Parameter	Description	Value
url-string	Specifies the redirect URL of the Portal server or pushed URL.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?).
ssid *ssid*	Specifies the SSID that users associate with.	The SSID must already exist.
push-only	Specifies the URL as a pushed URL.	-
redirect-only	Specifies the URL as a redirect URL.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

Set the redirect URL to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name huawei
[HUAWEI-url-template-huawei] url http://10.1.1.1
```

19.11.2.59 ucl-group (upgrade-compatible command)

Function

The **ucl-group** command creates a UCL group.

By default, no UCL group is created.

Format

ucl-group name *group-name* [**extend**]

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a UCL group.	The value is a string of 1 to 31 case-sensitive characters without spaces.
extend	Extends the maximum number of UCL groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

Create a UCL group named **abc**.

```
<HUAWEI> system-view
[HUAWEI] ucl-group name abc
```

19.11.2.60 voice-vlan (service scheme view) (upgrade-compatible command)

Function

The **voice-vlan** command configures a voice VLAN in a service scheme.

The **undo voice-vlan** command deletes the voice VLAN configured in the service scheme.

By default, no voice VLAN is configured in the service scheme.

Format

voice-vlan *vlan-id*

undo voice-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the voice VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

Configure voice VLAN 100 in the service scheme **huawei**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme huawei
[HUAWEI-aaa-service-huawei] voice-vlan 100
```

19.11.2.61 web-auth-server (interface view) (upgrade-compatible command)

Function

The **web-auth-server** command binds a Portal server template to an interface.

The **undo web-auth-server** command unbinds a Portal server template from an interface.

By default, no Portal server template is bound to an interface.

Format

- Layer 2 interface view

  web-auth-server *server-name* [*bak-server-name*] **direct**

  undo web-auth-server [*server-name* [*bak-server-name*] **direct**]
- VLANIF interface view

  web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

  undo web-auth-server [*server-name* [*bak-server-name*] { **direct** | **layer3** }]
- Routed main interface view

web-auth-server *server-name* [*bak-server-name*] **layer3**

undo web-auth-server [*server-name* [*bak-server-name*] **layer3**]

Parameters

Parameter	Description	Value
server-name	Specifies the name of the Portal server template.	The value must be an existing Portal server template name.
bak-server-name	Specifies the name of the secondary Portal server template. **NOTE** The name of the secondary Portal server template cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server template name.
direct	Specifies Layer 2 authentication as the Portal authentication mode. When there is no Layer 3 forwarding device between the user and device, the device can learn the user's MAC address. The device identifies the user using the MAC address.	-
layer3	Specifies Layer 3 authentication as the Portal authentication mode. Whether Layer 3 forwarding devices exist between the user and device, the device cannot learn the user's MAC address. The device identifies the user using the IP address uniquely.	-

Views

VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **web-auth-server** *server-name* [*bak-server-name*] { **direct** | **layer3** } command in the Portal access profile view.

19.12 Security Compatible Commands

19.12.1 ACL Compatible Commands

19.12.1.1 acl ipv6 (upgrade-compatible command)

Function

The **acl ipv6** command creates an ACL6 and enters the ACL6 view.

The **undo acl ipv6** command deletes an ACL.

Format

acl ipv6 [**number**] *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | [**number**] *acl6-number* | **name** *acl6-name* }

Parameters

Parameter	Description	Value
number *acl6-number*	Indicates the ID of an ACL6.	The value of *acl6-number* is an integer that ranges from 2000 to 3999. In these options, ● ACL6s numbered from 2000 to 2999 are basic ACL6s. ● ACL6s numbered from 3000 to 3999 are advanced ACL6s.
name *acl6-name*	Specifies a named ACL6.	The value of *acl6-name* is a string of 1 to 64 case-sensitive characters without spaces. The name starts with a letter (case-sensitive) and can contain letters, digits, and symbols such as the number sign (#), percentage symbol (%), and hyphen (-).

Parameter	Description	Value
all	Deletes all ACL6s.	-
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. ● **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6s are mainly used in QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services which packets need to be filtered.

Example

Create an ACL6 named test and numbered 3100.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3100 name test
[HUAWEI-acl6-adv-test]
```

19.12.1.2 acl (upgrade-compatible command)

Function

The **acl** command creates an ACL and enters the ACL view.

The **undo acl** command deletes a specified ACL.

Format

acl [**number**] *acl-number* [**name** *acl-name*]

undo acl { **all** | [**number**] *acl-number* | **name** *acl-name* }

Parameters

Parameter	Description	Value
number *acl-number*	Indicates the ID of an ACL.	The value of *acl-number* is an integer that ranges from 2000 to 5999. ● ACLs numbered from 2000 to 2999 are basic ACLs. ● ACLs numbered from 3000 to 3999 are advanced ACLs. ● ACLs numbered from 4000 to 4999 are Layer 2 ACLs. ● ACLs numbered from 5000 to 5999 are customized ACLs.

Parameter	Description	Value
name *acl-name*	Specifies a named ACL.	The value of *acl-name* is a string of 1 to 32 case-sensitive characters without spaces. The name starts with a letter (case-sensitive) and can contain letters, digits, and symbols such as the number sign (#), percentage symbol (%), and hyphen (-).
all	Deletes all ACLs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An ACL consists of a list of rules. Each rule contains a permit or deny clause. Before creating an ACL rule, you must create an ACL.

Example

Create an ACL named test and numbered 3100.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100 name test
[HUAWEI-acl-adv-test]
```

19.12.1.3 rule (advanced ACL6 view) (upgrade-compatible command)

Function

The **rule** command adds or modifies advanced ACL6 rules.

Format

rule [*rule-id*] { **deny** | **permit** } **ipv6-ah** [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

rule [*rule-id*] { **deny** | **permit** } **ipv6-esp** [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **dscp** *dscp* | **fragment** | **logging** | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

Parameters

Parameter	Description	Value
rule-id	Indicates the ID of an ACL6 rule.	The value ranges from 0 to 2047. ● If the ID of a rule is specified and the rule exists, the new rule is added to the rule with this ID, that is, the old rule is modified. ● If the rule associated with a rule ID does not exist, a rule can be created with this rule ID and its position in the ACL is determined by the rule ID. ● If no rule ID is specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order.
deny	Discards packets that do not match ACL rules.	-
permit	Allows packets to pass.	-
ipv6-ah	Indicates the protocol type.	-
ipv6-esp	Indicates the protocol type.	-
destination { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** }	Indicates the destination address and prefix of a packet.	*destination-ipv6-address* is expressed in hexadecimal notation. The value of *prefix-length* is an integer that ranges from 1 to 128. You can also use **any** to represent any destination address.

Parameter	Description	Value
destination *destination-ipv6-address* **postfix** *postfix-length*	Indicates the destination address and the length of destination address postfix.	*destination-ipv6-address* indicates the destination address and is expressed in hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.
dscp *dscp*	Specifies the value of a Differentiated Services CodePoint (DSCP).	The value ranges from 0 to 63.
fragment	Indicates that the rule is valid for only non-initial fragments.	-
logging	Indicates whether to record logs for packets that meet ACL rules.	Log contents include the ACL rule ID, pass or discard of packets, type of the protocol over IP, source or destination address, source or destination port number, and number of packets.
precedence *precedence*	Filters packets by priority.	The value is a name or a digit that ranges from 0 to 7.
source { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128. You can also use **any** to represent any source address.
source *source-ipv6-address* **postfix** *postfix-length*	Indicates the source address and the length of source address postfix.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.
time-range *time-name*	Specifies the time range only in which ACL6 rules are effective. *time-name* indicates the name of the time range.	The value is a string of 1 to 32 characters.
tos *tos*	Filters packets by Type of Service (ToS).	The value is a name or a digit that ranges from 0 to 15.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The vpn-instance must already exist.

Views

Advanced ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Advanced ACL6s classify data packets based on the source IP address, destination IP address, source port number, destination port number, and protocol type.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Create an advanced ACL6 with ID 3000 and configure a rule that allows only IPv6 ESP packets with the source IPv6 address xxxx:xxxx::xxxx and mask 64 to pass.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3000
[HUAWEI-acl6-adv-3000] rule 0 permit ipv6-esp source xxxx:xxxx::xxxx/64
```

19.12.2 Local Attack Defense Compatible Commands

19.12.2.1 blacklist (upgrade-compatible command)

Function

The **blacklist** command configures an ACL-based blacklist.

By default, no blacklist is configured.

Format

blacklist *blacklist-id* **acl** *acl-number* **soft-drop**

Parameters

Parameter	Description	Value
acl *acl-number*	Indicates the ACL ID. The ACL referenced by a blacklist on the device can be a basic ACL, an advanced ACL, or a Layer 2 ACL.	The value is an integer that ranges from 2000 to 4999.
soft-drop	Indicates that the blacklist is implemented through software.	-
blacklist-id	Specifies the number of an ACL6 referenced by a blacklist.	The value is an integer that ranges from 2000 to 3999. • 2000 to 2999: basic ACL6s • 3000 to 3999: advanced ACL6s

Views

System view, Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

A maximum of 8 blacklists can be configured in an attack defense policy on the device. You can set the attributes of a blacklist by defining ACL rules.

The packets sent from users in the blacklist are discarded after reaching the device.

Example

Reference ACL 2001 in the blacklist.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist acl 2001 soft-drop
```

19.12.2.2 car cpu-port (upgrade-compatible command)

Function

The **car cpu-port** command configures the CIR of all the packets to be sent to the CPU.

By default, the CIR value of all the packets to be sent to the CPU is 1024 kbit/s on the device.

Format

car cpu-port cir *cir-rate*

Parameters

Parameter	Description	Value
cir *cir-rate*	Sets the CIR of all the packets to be sent to the CPU.	The value is an integer that ranges from 64 to 2048, in kbit/s.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

The **car cpu-port** command limits the total rate of all protocol packets sent to the CPU. The **car packet-type** command limits the rate of packets of a specified protocol. However, the total CIR of packets of specified protocols cannot exceed the CIR of all the packets sent to the CPU.

When the CIR is exceeded, excess packets including unicast, multicast, and broadcast packets are not sent to the CPU. In addition, the unicast packets are discarded directly.

Example

Set the CIR of all the packets to be sent to the CPU to 512 kbit/s on the device.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] car cpu-port cir 512
```

19.12.2.3 deny (upgrade-compatible command)

Function

The **deny** command sets the discard action taken for packets sent to the CPU.

The **undo deny** command restores the default action taken for packets sent to the CPU.

By default, the device limits the rate of protocol packets and user-defined flows based on the CAR configuration.

Format

deny packet-type bpdu

deny packet-type ftp-dynamic

deny packet-type hotlimit

deny packet-type smlk-rrpp

deny packet-type nac-dhcp

undo deny packet-type bpdu

undo deny packet-type ftp-dynamic

undo deny packet-type hotlimit

undo deny packet-type smlk-rrpp

undo deny packet-type nac-dhcp

Parameters

Parameter	Description	Value
packet-type bpdu	Discards BPDU packets.	-
packet-type ftp-dynamic	Discards ftp-dynamic packets.	-
packet-type hotlimit	Discards hop-limit packets.	-
packet-type smlk-rrpp	Discards smlk-rrpp packets.	-
packet-type nac-dhcp	Discards nac-dhcp packets.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

If you run the **deny** and **car** commands for the same type of packets sent to the CPU, the command that runs later takes effect. The **undo deny** command restores the default action taken for packets sent to the CPU. After you run this command, the system limits the rate of packets sent to the CPU based on the configured CIR and CBS values.

Example

Set the discard action taken for bpdu packets sent to the CPU attack in defense policy test.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] deny packet-type bpdu
```

19.12.3 Attack Defense Compatible Commands

19.12.3.1 application-apperceive default drop (upgrade-compatible command)

Function

The **application-apperceive default drop** command enables the device to discard the received packets when no matching application layer association policy exists.

The **undo application-apperceive default drop** command enables the device to deliver the received packets to the upper layer though no matching application layer association policy exists.

By default, the device is enabled to deliver the received packets to the upper layer though no matching application layer association policy exists.

Format

application-apperceive default drop

undo application-apperceive default drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **application-apperceive default drop** command is run, if a protocol is not enabled in the system view nor in the interface view, the device discards all the packets of this protocol type.

Example

Enable the device to discard the received packets when no matching application layer association policy exists.

```
<HUAWEI> system-view
[HUAWEI] application-apperceive default drop
```

19.12.4 Traffic Suppression Compatible Commands

19.12.4.1 broadcast-suppression (upgrade-compatible command)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface.

The **undo broadcast-suppression** command restores the default traffic rate of broadcast packets that can pass through an interface.

Format

broadcast-suppression { *broadcast-pct* | **packets** *packets-per-second* }

undo broadcast-suppression

Parameters

Parameter	Description	Value
broadcast-pct	Specifies the maximum percentage of broadcast traffic on an interface.	The value ranges from 0 to 100. The default value is 100. By default, broadcast traffic is not suppressed on interfaces.
packets *packets-per-second*	Specifies the maximum number of broadcast packets allowed to pass through an interface per second.	The value of *packets-per-second* is an integer.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the traffic rate of broadcast packets exceeds the maximum value, the system discards excess broadcast packets to control the traffic rate and ensure normal operation of network services.

Example

Set the maximum percentage of broadcast traffic to 20% of interface bandwidth on Eth-Trunk1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] broadcast-suppression 20
```

19.12.4.2 multicast-suppression (upgrade-compatible command)

Function

The **multicast-suppression** command sets the maximum traffic rate of unknown multicast packets that can pass through an interface.

The **undo multicast-suppression** command restores the default traffic rate of unknown multicast packets that can pass through an interface.

Format

multicast-suppression { *multicast-pct* | **packets** *packets-per-second* }

undo multicast-suppression

Parameters

Parameter	Description	Value
multicast-pct	Specifies the maximum percentage of unknown multicast traffic on an Ethernet interface.	The value ranges from 0 to 100. The default value is 100. By default, unknown multicast traffic is not suppressed on interfaces.

Parameter	Description	Value
packets *packets-per-second*	Specifies the maximum number of unknown multicast packets allowed to pass through an interface per second.	The value of *packets-per-second* is an integer.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the traffic rate of unknown multicast packets exceeds the maximum value, the system discards excess unknown multicast packets to control the traffic rate and ensure normal operation of network services.

Example

Set the maximum percentage of unknown multicast traffic to 20% of interface bandwidth on Eth-Trunk1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] multicast-suppression 20
```

19.12.4.3 unicast-suppression (upgrade-compatible command)

Function

The **unicast-suppression** command sets the maximum traffic rate of unknown unicast packets that can pass through an interface.

The **undo unicast-suppression** command restores the default traffic rate of unknown unicast packets that can pass through an interface.

Format

unicast-suppression { *unicast-pct* | **packets** *packets-per-second* }

undo unicast-suppression

Parameters

Parameter	Description	Value
unicast-pct	Specifies maximum percentage of unknown unicast traffic on an Ethernet interface.	The value ranges from 0 to 100. The default value is 100. By default, unknown unicast traffic is not suppressed on interfaces.
packets *packets-per-second*	Specifies the maximum number of unknown unicast packets allowed to pass through an interface per second.	The value of *packets-per-second* is an integer.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the traffic rate of unknown unicast packets exceeds the maximum value, the system discards excess unknown unicast packets to control the traffic rate and ensure normal operation of network services.

Example

Set the maximum percentage of unknown unicast traffic to 20% of interface bandwidth on Eth-Trunk1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk1
[HUAWEI-Eth-Trunk1] unicast-suppression 20
```

19.12.4.4 storm-control action (upgrade-compatible command)

Function

The **storm-control action** sets the storm control action to **shutdown**.

The **undo storm-control action** command cancels the configuration.

By default, no storm control action is configured.

Format

storm-control action shutdown

undo storm-control action

Parameters

Parameter	Description	Value
shutdown	Shuts down an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **storm-control action error-down** command.

Example

Configure the storm control action is **shutdown** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control action shutdown
```

19.12.5 ARP Security Compatible Commands

19.12.5.1 arp anti-attack rate-limit (upgrade-compatible command)

Function

The **arp anti-attack rate-limit** command sets the maximum rate and rate limit duration of ARP packets globally, in a VLAN, or on an interface, enables the function of discarding all ARP packets received from the interface when the rate of ARP packets exceeds the limit on an interface.

The **undo arp anti-attack rate-limit** command restores the default maximum rate and rate limit duration of ARP packets globally, in a VLAN, or on an interface, and allows the device to send ARP packets to the CPU again.

By default, a maximum of 100 ARP packets are allowed to pass in 1 second, and the function of discarding all ARP packets received from the interface when the rate of ARP packets exceeds the limit is disabled.

Format

System view, VLAN view

arp anti-attack rate-limit *packet-number* [*interval-value*]

Interface view

arp anti-attack rate-limit *packet-number* [*interval-value* | **block timer** *timer*]*

undo arp anti-attack rate-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum rate of sending ARP packets, that is, the number of ARP packets allowed to pass through in the rate limit duration.	The value is an integer that ranges from 1 to 16384. The default value is 100.
interval-value	Specifies the rate limit duration of ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.
block timer *timer*	Specifies the duration for blocking ARP packets.	The value is an integer that ranges from 5 to 864000, in seconds.

Views

System view, VLAN view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, run the **arp anti-attack rate-limit** command to set the maximum rate and rate limit duration of ARP packets globally, in a VLAN, or on an interface. In the rate limit duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

If the parameter **block timer** *timer* is specified, the device discards all ARP packets received in the duration specified by *timer*.

Prerequisites

Rate limit on ARP packets has been enabled globally, in a VLAN, or on an interface using the **arp anti-attack rate-limit enable** command.

Precautions

If the maximum rate and rate limit duration are configured in the system view, VLAN view, and interface view, the device uses the configurations in the interface view, VLAN view, and system view in order.

If the maximum rate and rate limit duration are set globally or on an interface at the same time, the configurations on an interface and globally take effect in descending order of priority.

NOTE

The **arp anti-attack rate-limit** command takes effect only on ARP packets sent to the CPU for processing in **none-block** mode, and does not affect ARP packet forwarding by the chip. In **block** mode, only when the number of ARP packets sent to the CPU exceeds the limit, the device discards subsequent ARP packets on the interface.

Example

Configure GE0/0/1 to allow 200 ARP packet to pass through in 10 seconds, and configure GE0/0/1 to discard all ARP packets in 60 seconds when the number of ARP packets exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit 200 10 block timer 60
```

19.12.5.2 arp filter source (upgrade-compatible command)

Function

The **arp filter source** command enables ARP gateway protection for the specified IP address.

The **undo arp filter source** command disables ARP gateway protection for the specified IP address.

By default, ARP gateway protection is disabled.

Format

arp filter source *ip-address*

undo arp filter source { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the protected gateway IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
all	Disables ARP gateway protection for all IP addresses in the current view.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, it is replaced by the **arp trust source** command.

19.12.6 DHCP Snooping Compatible Commands

19.12.6.1 dhcp option82 format (upgrade-compatible command)

Function

The **dhcp option82 format** command configures the format of the Option 82 field in DHCP messages.

Format

dhcp option82 [**circuit-id** | **remote-id**] **format userdefined** *text*

Parameters

Parameter	Description	Value
circuit-id	Specifies the format of the circuit-id (CID).	-
remote-id	Specifies the format of the remote-id (RID).	-
userdefined *text*	Indicates the user-defined format of the Option 82 field.	*text* is the user-defined character string of the Option 82 field.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp option82 format** command to configure the format of the Option 82 field in DHCP messages.

Example

Configure the user-defined string for the CID in the Option 82 field and use the hexadecimal format to encapsulate the CID type (0, indicating the hexadecimal format), length (excluding the length of the CID type and the length keyword itself), outer VLAN ID, slot ID (5 bits), subslot ID (3 bits), and port number (8 bits).

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 circuit-id format userdefined 0 %length %svlan %5slot %3subslot %8port
```

19.12.6.2 dhcp snooping alarm { user-bind | mac-address | untrust-reply } enable (upgrade-compatible command)

Function

The **dhcp snooping alarm enable** command enables the alarm function for DHCP snooping.

The **undo dhcp snooping alarm enable** command disables the alarm function for DHCP snooping.

By default, the alarm function for discarded DHCP messages is disabled.

Format

dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** *threshold* }

undo dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** }

Parameters

Parameter	Description	Value
user-bind	Generates an alarm when the number of DHCP messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-

Parameter	Description	Value
mac-address	Generates an alarm when the number of DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address in the Ethernet frame header reaches the threshold.	-
untrust-reply	Generates an alarm when the number of DHCP Reply messages discarded by untrusted interfaces reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCP messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** [**threshold** *threshold*] command.

Example

On GE0/0/1, enable DHCP snooping, and enable the alarm function for DHCP snooping.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm user-bind enable
```

19.12.6.3 dhcp snooping bind-table autosave (upgrade-compatible command)

Function

The **dhcp snooping bind-table autosave** command configures a device to automatically back up DHCP snooping binding entries in a specified file.

Format

dhcp snooping bind-table autosave *file-name* [**write-delay** *delay-time*]

Parameters

Parameter	Description	Value
file-name	Specifies the path for storing the file that backs up DHCP snooping binding entries and the file name. You must specify both the path and name of the file supported by the system.	The value is a string of 1 to 51 characters.
write-delay *delay-time*	Specifies the interval for local automatic backup of the DHCP snooping binding table. If this parameter is not specified, the backup interval is the default value.	The value is an integer that ranges from 60 to 4294967295, in seconds. By default, the system backs up the DHCP snooping binding table every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping bind-table** command to back up DHCP snooping binding entries in a specified file.

Example

Configure a device to automatically back up DHCP snooping binding entries in the file **backup.tbl** in the flash memory.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping bind-table autosave flash:/backup.tbl
```

19.12.6.4 dhcp snooping check enable (upgrade-compatible command)

Function

The **dhcp snooping check enable** enables the device to check DHCP messages.

The **undo dhcp snooping check enable** disables the device from checking DHCP messages.

By default, the device does not check DHCP messages.

Format

In the system view:

dhcp snooping check { **user-bind** | **mac-address** } **enable vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

undo dhcp snooping check { **user-bind** | **mac-address** } **enable vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

In the VLAN view, Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view:

dhcp snooping check { **user-bind** | **mac-address** } **enable**

undo dhcp snooping check { **user-bind** | **mac-address** } **enable**

Parameters

Parameter	Description	Value
user-bind	Check DHCP messages against the DHCP snooping binding table.	-
mac-address	Compare the MAC address in DHCP ACK or DHCP Request messages with the CHADDR value.	-
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check the HCP messages from a specified VLAN to the processing unit. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

VLAN view, System view, Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the command is used, you can check DHCP messages against the DHCP snooping binding table or Compare the MAC address in DHCP ACK or DHCP Request messages with the CHADDR value.

Example

Enable the function of checking DHCP messages against the binding table in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping check user-bind enable
```

19.12.6.5 dhcp snooping check dhcp-rate alarm enable (upgrade-compatible command)

Function

The **dhcp snooping check dhcp-rate alarm enable** command enables the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.

By default, the device is disabled from generating an alarm when the number of discarded DHCP messages reaches the threshold.

Format

dhcp snooping check dhcp-rate alarm { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold for checking the rate of sending DHCP messages to the processing unit. An alarm is generated after the rate for sending DHCP messages is checked and the number of discarded DHCP messages reaches the alarm threshold.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the alarm function is enabled, the device sends a trap message when the number of discarded DHCP messages reaches the alarm threshold.

Example

In the system view, enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping check dhcp-rate alarm enable
```

19.12.6.6 dhcp snooping check dhcp-rate enable alarm dhcp-rate enable (upgrade-compatible command)

Function

Using the **dhcp snooping check dhcp-rate enable alarm dhcp-rate enable** command, you can:

- Enable the function of checking the rate of sending DHCP messages to the DHCP protocol stack.
- Set the rate limit of sending DHCP messages to the DHCP protocol stack.
- Enable the DHCP message discard alarm.
- Set the alarm threshold for discarded DHCP messages.

By default, the function of checking the rate of sending DHCP messages to the DHCP stack is disabled; the rate limit of sending DHCP messages to the DHCP stack is 100 pps; the DHCP message discard alarm is disabled; the alarm threshold for discarded DHCP messages is 100.

Format

dhcp snooping check dhcp-rate { **enable** | [**enable**] [**rate**] *rate* } **alarm dhcp-rate** { **enable** | [**enable**] **threshold** *threshold-value* }

Parameters

Parameter	Description	Value
[**rate**] *rate*	Specifies the rate limit of sending DHCP messages to the DHCP protocol stack.	The value ranges from 1 to 100, in pps. The default value is 100.
alarm dhcp-rate enable	Enables the DHCP message discard alarm.	-

Parameter	Description	Value
threshold *threshold-value*	Specifies the alarm threshold for discarded DHCP messages. After the function is enabled, an alarm is generated when the number of discarded DHCP messages reaches the alarm threshold on an interface.	The value ranges from 1 to 1000. The default value is 100.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the command is used, the DHCP message discard alarm is enabled. If the number of discarded messages reaches the alarm threshold, an alarm is generated.

Example

On GE 0/0/1, enable the function of checking the rate of sending DHCP messages, set the rate limit of sending DHCP messages to the DHCP protocol stack to 50 pps, enable the DHCP message discard alarm, and set the alarm threshold for discarded DHCP messages to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable
threshold 50
```

19.12.6.7 dhcp snooping check dhcp-rate enable alarm enable (upgrade-compatible command)

Function

Using the **dhcp snooping check dhcp-rate enable alarm enable** command, you can:

- Enable the function of checking the rate of sending DHCP messages to the processing unit.

- Set the rate limit of sending DHCP messages to the processing unit.
- Enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.
- Set the alarm threshold for the number of discarded DHCP messages.

By default, the device does not check the rate of sending DHCP messages to the processing unit; the maximum rate of sending DHCP messages to the processing unit is 100 pps; the device does not generate an alarm when the number of discarded DHCP messages reaches the threshold; the alarm threshold for the number of discarded DHCP messages is 100.

Format

dhcp snooping check dhcp-rate enable [[**rate**] *rate*] **alarm** [**dhcp-rate**] { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
[**rate**] *rate*	Specifies the rate limit of sending DHCP messages to the processing unit.	The value is an integer that ranges from 1 to 100, in pps. The default value is 100.
dhcp-rate	Generates an alarm when the number of discarded DHCP messages reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCP messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the command is used, the DHCP message discard alarm is enabled. If the number of discarded messages reaches the alarm threshold, an alarm is generated.

Example

Enable the function of checking the rate of sending DHCP messages to the processing unit, set the rate limit of sending DHCP messages to the processing unit to 50 pps, enable the DHCP message discard alarm, and set the alarm threshold for discarded DHCP messages to 50.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
```

19.12.6.8 dhcp snooping check { dhcp-request | dhcp-chaddr | dhcp-giaddr } enable alarm

Function

The **dhcp snooping check { dhcp-request | dhcp-chaddr | dhcp-giaddr | user-bind | mac-address } enable alarm enable** command enables the DHCP packet check and alarm function.

By default, the DHCP packet check and alarm function is disabled.

Format

dhcp snooping check { **dhcp-request** | **dhcp-chaddr** | **dhcp-giaddr** | **user-bind** | **mac-address** } **enable alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** | **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
dhcp-request or **user-bind**	Generates alarms when the number of DHCP packets that are discarded because they do not match the binding table reaches the threshold.	-
dhcp-chaddr or **mac-address**	Generates alarms when the number of DHCP packets that are discarded because the CHADDR field in the packets is different from the MAC address in the frame header reaches the threshold.	-
dhcp-reply or **untrust-reply**	Generates alarms when the number of DHCP server response packets discarded by untrusted interfaces reaches the threshold.	-

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold. The device generates alarm information when the number of discarded DHCP packets reaches the threshold.	The value is an integer that ranges from 1 to 1000.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

This function equals to the combination of the **dhcp snooping check dhcp-giaddr enable**, **dhcp snooping check dhcp-chaddr enable**, **dhcp snooping check dhcp-request enable**, and **dhcp snooping alarm** { **user-bind** | **mac-address** | **untrust-reply** } **threshold** *threshold* commands.

Example

Enable the **user-bind** check function on GE0/0/1. Set the alarm threshold to 1000 for the discarded packet in the **user-bind** check.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check user-bind enable alarm user-bind enable
threshold 100
```

19.12.6.9 dhcp snooping check enable alarm enable (upgrade-compatible command)

Function

The **dhcp snooping check enable alarm enable** command enables the DHCP packet check and alarm function.

By default, the DHCP packet check and alarm function is disabled.

Format

dhcp snooping check { **dhcp-request** | **dhcp-chaddr** | **dhcp-giaddr** } **enable alarm** { **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
dhcp-request	Matches DHCP packets with entries in the binding table.	-
dhcp-chaddr	Checks whether the MAC address and CHADDR field in DHCP packets are consistent.	-
dhcp-giaddr	Checks whether the GIADDR field in DHCP packets is not zero.	-
user-bind	Generates an alarm when the number of DHCP packets discarded because they do not match DHCP snooping binding entries reaches the threshold.	-
mac-address	Generates an alarm when the number of DHCP packets discarded because the CHADDR field in the DHCP packet does not match the source MAC address in the Ethernet frame header reaches the threshold.	-
untrust-reply	Generates an alarm when the number of DHCP Reply packets discarded by untrusted interfaces reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCP packets reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade. This function equals to the combination of the **dhcp snooping check dhcp-giaddr enable**, **dhcp snooping check dhcp-chaddr enable**, **dhcp snooping check dhcp-request enable**, and **dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **threshold** *threshold* commands.

19.12.6.10 dhcp snooping global max-user-number (upgrade-compatible command)

Function

The **dhcp snooping global max-user-number** command sets the maximum number of global DHCP users.

By default, the maximum number of global DHCP users is 1024.

Format

dhcp snooping global max-user-number *max-user-number*

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of global DHCP users.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp snooping global max-user-number** command takes effect only when DHCP snooping is enabled globally and is valid for only DHCP users. When the number of global DHCP users reaches the threshold set by this command, no more users can access.

You can use the **dhcp snooping global max-user-number** command to set the maximum number of global users.

Example

Set the maximum number of global DHCP users to 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping global max-user-number 100
```

19.12.6.11 dhcp snooping information circuit-id (upgrade-compatible command)

Function

The **dhcp snooping information circuit-id** command configures the Option 82 circuit-id format.

Format

System view:

dhcp snooping information circuit-id string *string*

Interface view:

dhcp snooping information [**vlan** *vlan-id*] **circuit-id string** *string*

Parameters

Parameter	Description	Value
string *string*	Specifies the circuit-id format.	The value is a string of 1 to 63 characters.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping information circuit-id** command to configure the Option 82 circuit-id format.

Example

Configure the Option 82 circuit-id format.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping information circuit-id string teststring
```

19.12.6.12 dhcp snooping information format (upgrade-compatible command)

Function

The **dhcp snooping information format** command configures the Option 82 field format.

Format

dhcp snooping information format { **hex** | **ascii** }

Parameters

Parameter	Description	Value
hex	Sets the Option 82 format to hexadecimal.	-
ascii	Sets the Option 82 format to ASCII.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping information format** command to configure the Option 82 field format.

Example

Set the Option 82 format to ASCII.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping information format ascii
```

19.12.6.13 dhcp snooping information remote-id (upgrade-compatible command)

Function

The **dhcp snooping information remote-id** command configures the Option 82 remote-id format.

Format

System view:

dhcp snooping information remote-id { **sysname** | **string** *string* }

Interface view:

dhcp snooping information [**vlan** *vlan-id*] **remote-id string** *string*

Parameters

Parameter	Description	Value
sysname	System name.	-
string *string*	Specifies the remote-id format.	The value is a string of 1 to 63 characters.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping information remote-id** command to configure the Option 82 remote-id format.

Example

Configure the Option 82 remote-id format.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping information remote-id string teststring
```

19.12.6.14 dhcp snooping max-user-number global (upgrade-compatible command)

Function

The **dhcp snooping max-user-number global** command sets the maximum number of global DHCP users.

By default, the maximum number of global DHCP users is 1024.

Format

dhcp snooping max-user-number *max-user-number* **global**

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of global DHCP users.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

The command takes effect only when DHCP snooping is enabled globally and is valid for only DHCP users. When the number of global DHCP users reaches the threshold set by this command, no more users can access. You can use the command to set the maximum number of global users.

Example

Set the maximum number of global DHCP users to 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping max-user-number 100 global
```

19.12.6.15 dhcp snooping sticky-mac (upgrade-compatible command)

Function

The **dhcp snooping sticky-mac** command enables the device to generate static MAC address entries based on dynamic DHCP snooping binding entries.

The **undo dhcp snooping sticky-mac** command disables the device from generating static MAC address entries based on dynamic DHCP snooping binding entries.

By default, the device is disabled to generate static MAC address entries based on dynamic DHCP snooping binding entries.

Format

dhcp snooping sticky-mac

undo dhcp snooping sticky-mac

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Dynamic MAC address entries are learned and generated by the device, and static MAC address entries are configured by command lines. A MAC address entry consists of the MAC address, VLAN ID, and port number of a DHCP client. The device implements Layer 2 forwarding based on MAC address entries.

After the **dhcp snooping sticky-mac** command is executed on an interface, the device generates static MAC address entries (snooping type) of DHCP users on the interface based on the corresponding dynamic binding entries, clears all the dynamic MAC address entries on the interface, disables the interface to learn dynamic MAC address entries, and enables the device to match the source MAC address based on MAC address entries. Then only the message with the source MAC address matching the static MAC address entry can pass through the interface; otherwise, messages are discarded. Therefore, the administrator needs to manually configure static MAC address entries (the static type) for non-DHCP users on the interface so that messages sent from non-DHCP users can pass through; otherwise, DHCP messages are discarded. This prevents attacks from non-DHCP users.

NOTE

- If a DHCP snooping binding entry is updated, the corresponding static MAC address entry is automatically updated.
- If you run the **dhcp snooping sticky-mac** command on the interface, DHCPv6 users cannot go online. Run the **nd snooping enable** command in the system view and interface view to enable ND snooping and the **savi enable** command in the system view to enable SAVI.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

The **dhcp snooping sticky-mac** command cannot be used with the following commands on an interface.

Command	Description
dot1x enable	Enables 802.1X authentication on an interface.
mac-authen	Enables MAC address authentication on an interface.
mac-address learning disable	Enables MAC address learning.
mac-limit	Sets the maximum number of MAC addresses to be learned.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Enables VLAN mapping.
port-security enable	Enables port security.

Example

Enable the device to generate static MAC address entries based on DHCP snooping binding entries on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping sticky-mac
```

19.12.6.16 dhcp snooping trusted interface no-user-binding (upgrade-compatible command)

Function

The **dhcp snooping trusted interface no-user-binding** command configures a trusted interface.

The **undo dhcp snooping trusted interface no-user-binding** command deletes a trusted interface.

By default, no trusted interface is configured.

Format

dhcp snooping trusted interface *interface-type interface-number* **no-user-binding**

undo dhcp snooping trusted interface *interface-type interface-number* **no-user-binding**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping trusted interface no-user-binding** command to configure a trusted interface in the VLAN view.

Before using this command:

- Enable DHCP snooping globally.
- Add the interface to a VLAN.

This command can only be used during a configuration restoration.

Example

Configure a trusted interface GE0/0/1 in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping trusted interface gigabitethernet 0/0/1 no-user-binding
```

19.12.6.17 dhcp snooping trusted no-user-binding (upgrade-compatible command)

Function

The **dhcp snooping trusted no-user-binding** command configures an interface as the trusted interface.

The **undo dhcp snooping trusted no-user-binding** command restores the default state of an interface.

By default, no trusted interface is configured.

Format

dhcp snooping trusted no-user-binding

undo dhcp snooping trusted no-user-binding

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When DHCP snooping is enabled on an interface, the interface is an untrusted interface by default. After you use the **dhcp snooping trusted no-user-binding** command in the interface view, the interface becomes a trusted interface.

This command can only be used during a configuration restoration.

Example

Configure a trusted interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping trusted no-user-binding
```

19.12.7 Keychain Upgrade-compatible Commands

19.12.7.1 receive-time (upgrade-compatible command)

Function

The **receive-time** command makes a key act as a receive-key for the specified interval of time.

The **undo receive-time** command deletes the receive-time configuration.

By default, no receive-time is configured.

Format

receive-time utc *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }

Parameters

Parameter	Description	Value
utc	Specifies that the given time is in Coordinated Universal Time (UTC) format.	-
start-time	Specifies the start receive time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specifies the start date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the receive time in minutes.	The value ranges from 1 to 26280000.
infinite	Specifies that the key will be acting as a active receive key forever from the configured start-time.	-
to	Acts as a separator.	-
end-time	Specifies the end receive time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end-time should be greater than the start-time.
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.

Views

key-id view

Default Level

2: Configuration Level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **receive-time** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } } command.

19.12.7.2 send-time (upgrade-compatible command)

Function

The **send-time** command makes a key act as a send key for the specified interval of time.

By default, no send-time is configured.

Format

send-time utc *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }

Parameters

Parameter	Description	Value
utc	Specifies that the given time is in Coordinated Universal Time (UTC) format.	-
start-time	Specifies the start send time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specify the start date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the send time in minutes.	The value ranges from 1 to 26280000.
infinite	Specifies that the key will be acting as a send key forever from the configured start-time.	-
to	Acts as a separator.	-
end-time	Specifies the end send time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end-time should be greater than the start-time.
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily send timing for the given key.	-

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **send-time** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } } command.

19.13 QoS Compatible Commands

19.13.1 count (upgrade-compatible command)

Function

Using the **count** command, you can enable the function of counting packets that match traffic classification rules.

By default, the counting function is disabled.

Format

count

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

When there are many traffic classification rules on the switch, you can run the **count** command to count the specific traffic. The counting start time is the time when the policy is applied.

Currently, the switch counts packets rather than bytes.

Example

Configure the traffic policy **p1** so that the switch counts packets that flow through GigabitEthernet 0/0/1. After a period of time, the switch displays the traffic statistics.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] count
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet0/0/1] display traffic policy interface gigabitethernet 0/0/1
  Interface: GigabitEthernet0/0/1

  Direction: Inbound

  Policy: p1
   Classifier: c1
     Rule(s) : if-match any
     Behavior: b1
      Count
        Matched : 10 (Packets)
```

19.14 Network Management Compatible Commands

19.14.1 SNMP Compatible Commands

19.14.1.1 snmp-agent group (upgrade-compatible command)

Function

The **snmp-agent group** command creates an SNMP group by mapping SNMP users to SNMP views.

The **undo snmp-agent group** command deletes a specified SNMP user group.

By default, no SNMP group is configured.

Format

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*] * [**acl** *acl-number*]

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP group uses the security mode in SNMPv3.	-
group-name	Specifies the name of an SNMP group.	It is a string of 1 to 32 case-sensitive characters without spaces.

Parameter	Description	Value
authentication | **privacy**	Indicates the security level of the SNMP group. - **authentication**: authenticates SNMP messages without encryption. - **privacy**: authenticates and encrypts SNMP messages.	To ensure security, it is recommended that you set the security level of the SNMP group to **privacy**.
read-view *read-view*	Specifies a read-only view.	It is a string of 1 to 32 case-sensitive characters without spaces. *read-view* specified by the **snmp-agent mib-view** command.
write-view *write-view*	Specifies a read-write view.	It is a string of 1 to 32 case-sensitive characters without spaces. *write-view* is specified by the **snmp-agent mib-view** command.
notify-view *notify-view*	Specifies a notify view.	It is a string of 1 to 32 case-sensitive characters without spaces. *notify-view* is specified by the **snmp-agent mib-view** command.
acl *acl-number*	Specifies a basic ACL. **NOTE** The ACL configured by the **acl** *acl-number* parameter takes effect on both IPv4 and IPv6 networks.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.1.2 snmp-agent trap enable (upgrade-compatible command)

Function

The **snmp-agent trap enable** command enables a specified trap for a specified feature.

The **undo snmp-agent trap enable** command disables a specified trap for a specified feature.

The default configuration of the **snmp-agent trap enable** command can be checked using the **display snmp-agent trap all** command.

Format

snmp-agent trap enable *feature-name*

undo snmp-agent trap enable *feature-name*

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the feature that generates traps.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.1.3 snmp-agent trap enable standard (upgrade-compatible command)

Function

Using the **snmp-agent trap enable standard** command, you can enable the trap function of standard SNMP.

Using the **undo snmp-agent trap enable standard** command, you can disable the trap function of standard SNMP.

By default, no trap messages are sent to a device.

Format

snmp-agent trap enable standard [**authentication** | **coldstart** | **warmstart** | **linkup** | **linkdown**] *

undo snmp-agent trap enable standard [**authentication** | **coldstart** | **warmstart** | **linkup** | **linkdown**] *

Parameters

Parameter	Description	Value
Authentication	Indicates that a trap message is sent when packets failed to be authenticated through SNMP.	-
Coldstart	Indicates that a trap message is sent when the system is cold started.	-
Warmstart	Indicates that a trap message is sent when the system is hot started.	-
Linkup	Indicates that a trap message is sent when the interface goes Up.	-
Linkdown	Indicates that a trap message is sent when the interface goes Down.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.1.4 snmp-agent usm-user (upgrade-compatible command)

Function

The **snmp-agent usm-user** command adds a user to an SNMP user group.

The **undo snmp-agent usm-user** command deletes a user from an SNMP user group.

By default, the SNMP user group has no users added.

NOTE

It is recommended that you deliver the **snmp-agent usm-user v3** *user-name group-name* **authentication-mode** { **md5** | **sha** } *password* [**privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } *encrypt-password*] [**acl** *acl-number*] to the switch from the NMS. Do not directly configure the command on the switch.

Format

snmp-agent usm-user v3 *user-name group-name* **simple** [**authentication-mode** { **md5** | **sha** } *password* [**privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } *encrypt-password*]] [**acl** *acl-number*]

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *password* [**privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } *encrypt-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* [**engineid** *engineid* | **local**]

Parameters

Parameter	Description	Value
v3	Indicates that the security mode in SNMPv3 is adopted.	-
user-name	Specifies the name of a user.	It is a string of 1 to 32 case-sensitive characters without spaces.
group-name	Specifies the name of the group to which a user belongs.	It is a string of 1 to 32 case-sensitive characters without spaces.
simple	Indicates the simple authentication.	-
cipher	Specifies that the password is in ciphertext, which is the default password type. If this parameter is specified, you can enter only a password in ciphertext. This type of password can be viewed using the configuration file.	-

Parameter	Description	Value
authentication-mode	Sets the authentication mode. **NOTE** Authentication is a process in which the SNMP agent (or the NMS) confirms that the message is received from an authorized NMS (or SNMP agent) and the message is not changed during transmission. RFC 2104 defines Keyed-Hashing for Message Authentication Code (HMAC), an effective tool that uses the security hash function and key to generate the message authentication code. This tool is widely used in the Internet. HMAC used in SNMP includes HWAC-MD5-96 and HWAC-SHA-96. The hash function of HWAC-MD5-96 is MD5 that uses 128-bit authKey to generate the key. The hash function of HWAC-SHA-96 is SHA-1 that uses 160-bit authKey to generate the key.	-
md5 | **sha**	Indicates the authentication protocol. ● **md5**: Specifies HMAC-MD5-96 as the authentication protocol. ● **sha**: Specifies HMAC-SHA-96 as the authentication protocol.	-

Parameter	Description	Value
password	Specifies the password for user authentication.	For plain-text password, the value is a string of 6 to 64 characters by default, and the minimum length is 6 characters. If the **set password min-length** command is run to set the minimum length of passwords to a value greater than 6, the minimum length is the value configured using the **set password min-length** command. For cipher-text password, the value is a string of 32 to 104 characters. **NOTE** The password cannot be the same as the user name or reverse of the user name. The password must contain at least two types of characters, including letters, digits, and special characters. The special characters cannot be question mark (?) or space.
privacy-mode	Specifies the authentication with encryption. The system adopts the cipher block chaining (CBC) code of the data encryption standard (DES) and uses 128-bit privKey to generate the key. The NMS uses the key to calculate the CBC code and then adds the CBC code to the message while the SNMP agent fetches the authentication code through the same key and then obtains the actual information. Like the identification authentication, the encryption requires the NMS and the SNMP agent to share the same key to encrypt and decrypt the message.	-

Parameter	Description	Value
des56 | **aes128** | **aes192** | **aes256** | **3des**	Indicates the encryption protocol.	-
encrypt-password	Indicates the encryption password.	For plain-text password, the value is a string of 6 to 64 characters by default, and the minimum length is 6 characters. If the **set password min-length** command is run to set the minimum length of passwords to a value greater than 6, the minimum length is the value configured using the **set password min-length** command. For cipher-text password, the value is a string of 32 to 104 characters. **NOTE** The password cannot be the same as the user name or reverse of the user name. The password must contain at least two types of characters, including letters, digits, and special characters. The special characters cannot be question mark (?) or space.
acl *acl-number*	Specifies the ACL number of the access view.	The value is an integer that ranges from 2000 to 2999.
engineid *engineid*	Specifies the ID of the engine associated with a user.	The value is a string of 10 to 64 case-insensitive characters without spaces.
local	Indicates the local entity user.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.2 NQA Compatible Commands

19.14.2.1 send-trap overthreshold (upgrade-compatible command)

Function

Using the **send-trap overthreshold** command, you can configure conditions for sending trap messages.

Using the **undo send-trap overthreshold** command, you can delete the previous configuration.

By default, the device is disabled from sending traps.

Format

send-trap overthreshold

undo send-trap overthreshold

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **send-trap rtd** command.

19.14.3 Mirror Compatible Commands

19.14.3.1 port-mirroring (upgrade-compatible command)

Function

The **port-mirroring** command configures a mirroring behavior on an interface.

Format

port-mirroring to observe-port *index*

Parameters

Parameter	Description	Value
index	Specifies the index of a global observing interface.	The value is integer.

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

Example

Mirror traffic to observing interface with index 1.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-traffic-behavior-b1] port-mirroring to observe-port 1
```